令和４年度　経済産業省委託
石油・ガス供給等に係る保安対策調査等事業

高圧ガス分野の新たな認定制度の検討に向けた調査
報告書

令和５年３月
高圧ガス保安協会

目次

0. 用語の定義 5
1. 調査概要 6
1.1 目的 6
1.2 調査内容等 6
2. 各事項の検討について 8
2.1 認定事業者及び自治体を対象としたアンケート調査及びヒアリングの実施 8
2.1.1 アンケート調査及びヒアリングの実施（事業所） 8
2.1.2 アンケート調査及びヒアリングの実施（自治体） 9
2.2 新認定制度の認定要件 12
2.2.1 経営トップのコミットメントについて 12
2.2.1.1 コンプライアンス体制、コーポレート・ガバナンスの確保検討の考慮事項 12
2.2.1.2 コンプライアンス体制、コーポレート・ガバナンスの確保の検討の視点 12
2.2.1.3 コンプライアンス体制、コーポレート・ガバナンスの確保の検討 12
2.2.1.4 検討結果 13
2.2.2 高度なリスク管理体制について 14
2.2.2.1 高度なリスク管理体制の検討の視点 14
2.2.2.2 高度なリスク管理体制の検討 14
2.2.2.3 検討結果 14
2.2.3 テクノロジーの活用の検討の視点 15
2.2.3.1 認定要件の軸について 15
2.2.3.2 A 認定、B 認定に求める要件案について 15
2.2.3.3 検討結果 16
2.2.4 サイバーセキュリティなど関連リスクへの対応について 18
2.2.4.1 サイバーセキュリティなど関連リスクへの対応の検討の視点 18
2.2.4.2 サイバーセキュリティなど関連リスクへの対応の検討 18
2.2.4.3 検討結果 18
2.3 新認定制度における特例措置 20
2.3.1 変更工事等の特例について 20
2.3.1.1 改正法における特例について 20
2.3.1.2 変更工事の特例における仕分けの切り口（考慮要素）について 20
2.3.1.3 上記の考慮要素を踏まえた分類方針（論点） 20
2.3.1.4 その他の論点 20
2.3.1.5 留意点等 21
2.3.2 変更工事等の特例の具体的な内容について 21
2.3.2.1 許可となるもの 21
2.3.2.2 事後届となるもの 22
2.3.2.3 記録保存となるもの 22
2.3.2.4 記録保存義務が掛からないもの 22
2.3.3 軽微な変更（記録保存）の対象の拡大等について 22
2.3.3.1 軽微な変更（記録保存）の対象の拡大について 22
2.3.4 保安検査時期の柔軟化について 23
2.3.5 定期自主検査の義務の廃止に伴う認定要件でのフォローについて 24
2.3.6 危害予防規定の届出義務・保安人員の選解任の届出義務の廃止 24
2.3.7 保安人員の柔軟化について 25
2.3.8 検討結果 25
2.4 新認定制度の審査方法等 28
2.4.1 新認定制度の審査方法等の検討の視点 28
2.4.2 更新申請時の審査の簡略化について 28
2.4.2.1 事故等の発生状況 28

2.4.2.2 法令違反について 29
2.4.2.3　大幅な変更の内容 29
2.4.3　審査基準案の作成について 29
2.4.4　検討結果 30
2.5　改正高圧法を踏まえ改正が必要となる下位法令の抽出等 33
2.5.1　認定取り消し後の保安検査期間等の猶予について 33
2.5.1.2　保安検査全体の実施期間の猶予について 33
2.5.1.3　認定によって認められている保安検査方法の有効期間の猶予 33
2.5.2　記録保存の方法について 34
2.5.2.1　電磁的方法による記録保存対象の拡大 34
2.5.2.2　クラウドの利用を前提とした「電磁的方法による保存等をする場合に確保するよう努めなければならない基準について」の改正の検討 34
2.5.2.3　記録保存が適切に実施できているかの確認方法 35
2.5.3　電磁的記録保存の方法についての再検討 36
2.5.3.1　クラウドの利用を前提とした「電磁的方法による保存等をする場合に確保するよう努めなければならない基準について」（電磁保存告示）の改正の検討 36
2.5.3.2　クラウドの利用を前提とした「経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則」（書面保存則）の改正の検討 36
2.5.4　製造施設ごとの認定申請、記録類等に関する規定について 37
2.5.4.1　コンビ則 40 条 2 項・47 条・49 条の 6 の規定の要否 37
2.5.4.2　記録保存とする記録に記載する項目の規定 37
2.5.4.3　完成検査の方法等について 38
2.5.4.4　危害予防規程の制改正の記録する項目の規定 38
2.5.4.5　保安人員の選解任に係る記録に記載する項目の規定 38
2.5.4.6　A 認定と B 認定をまとめて申請することを可とする規定を措置保安検査の時期について 38
2.6　立入検査 39
2.7　検討結果（検討中の項目を含む。）を踏まえた自治体への説明と意見交換 39
3.まとめ 39

0. 用語の定義

本報告書では、以下の略称等を使用する場合がある。

ただし、経済産業省の仕様書や本委員会以外の資料を引用する場合は、その資料に基づくことを原則とするため、用語の不整合が生じる場合がある。

略称	説明
法	高圧ガス保安法
政令	高圧ガス保安法施行令
コンビ則	コンビナート等保安規則
改正高圧法	高圧ガス保安法等の一部を改正する法律（令和 4 年 6 月 22 日公布）のうち、高圧ガス保安法の改正部分
高圧ガス保安室	経済産業省　産業保安グループ高圧ガス保安室
KHK	高圧ガス保安協会

1. 調査概要

1.1 目的

我が国の産業保安をめぐっては、近年、革新的なテクノロジーの進展、保安人材の不足・高齢化、電力・ガス供給構造の変化、災害の激甚化・頻発化、気候変動問題への対応の要請など、内外環境が大きく変化している。

このような状況の中、産業構造審議会保安・消費生活用製品安全分科会報告書「産業保安分野における当面の制度化に向けた取組と今後の重要課題（令和３年 12 月 21 日）」（以下「分科会報告書」という。）においては、高圧ガス分野においても、次のように現行の認定事業者制度（スーパー認定事業者制度を含む。）を見直すことが提言されている。

分科会報告書においては、保安レベルを下げることなく、むしろ、テクノロジーの活用により保安レベルを持続的に向上させる観点から、「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」については、行政の適切な監査・監督の下に、画一的な個別・事前規制によらず、事業者の保安力に応じた規制体系へ移行することとし、手続・検査のあり方をこれに見合った形に見直す措置を講じ、これにより、事業者の保安活動を、テクノロジーを活用しつつ自己リスク管理がなされた高度な領域に強力に押し上げていくことが必要であると結論が得られている。

分科会報告書の内容を踏まえ、高圧ガス保安法等の一部を改正する法律案が第 208 回通常国会に提出され、国会での審議を経て可決された。公布（令和４年６月２２日）より１年６カ月以内に施行される予定となっているところ、この法改正により新たに創設される認定高度保安実施者制度（以下「新認定制度」という。）を運用するために必要な下位法令、解釈等を準備する必要がある。

そこで本事業では、新認定制度の運用に必要な下位法令、解釈等の整備に必要な準備として、改正後の高圧ガス保安法（以下「改正高圧法」という。）を踏まえ改正が必要となる下位法令の抽出、新認定制度の認定要件・審査方法・特例措置等に係る詳細検討、自主保安高度化事業者制度の取り扱いなどについて経済産業省産業保安グループ高圧ガス保安室（以下「高圧ガス保安室」という。）と協力して検討した。

1.2 調査内容等

本事業の実施計画書（仕様書）による調査事項は以下のとおり。

① 改正高圧法を踏まえ改正が必要となる下位法令の抽出等

新認定制度の運用に必要な下位法令（政令・省令・告示・通達）やマニュアル等について抽出するとともに、ハネ改正が必要となる下位法令やマニュアル及びその該当箇所の内容についても抽出するとともに、変更後（ハネ改正後）の内容を整理する。

② 新認定制度の認定要件

新認定制度の要件は、スマート保安の促進の観点からテクノロジーの活用やサイバー対策を含む４つの要件（ⅰ経営トップのコミットメント、ⅱ高度なリスク管理体制、ⅲテクノロジーの活用、ⅳサイバーセキュリティなど関連リスクへの対応）で構成し、リスク管理レベル等に応じ、２つの措置（A 認定・B 認定）に差異化する。なお、特に上記ⅰは、現行スーパー認定事業者制度の要件に加え、コンプライアンス体制の整備（高圧ガス保安法についての法適合性確認能力（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。）、コーポレート・ガバナンスの確保を含むものとし、分科会報告書等を踏まえて検討する。

また、新認定制度において定期自主検査が不要となることを考慮し、現在、定期自主検査でのみ検査を行っている項目について、継続的に検査を行っていくことを担保するため、例えば、更新認定に当たって、継続的な改善事項とするなどの要件についても検討する。

③ 新認定制度の審査方法等

新認定制度の審査方法等にあっては、分科会報告書等を踏まえ、以下の項目について、具体的な方法、要件などを検討する。

・国の検査（現地検査）
・審査会審査

・国の一次的審査（更新の場合）
・認定の更新期間
・KHK 又は経済産業大臣の指定する者への意見聴取・調査依頼

④ 新認定制度における特例措置

新認定制度において、新たに設けられる以下の特例措置に関し、具体的な内容を検討する。

・設備のための施設等の変更の特例（製造のための施設等の変更に係る許可が必要な重要な変更、軽微な変更の工事の範囲等）
・軽微な変更の工事をしたとき等の記録保存の方法
・保安主任者、保安係員の選任区分の柔軟化

⑤ 立入検査

認定の更新期間の中間時点を目途に行う立入検査や抜き打ちで行う立入検査について、その実施体制、検査内容などについて、検討を行う。

2. 各事項の検討について

2.1　認定事業者及び自治体を対象としたアンケート調査及びヒアリングの実施

調査の検討にあたり、認定事業所や自治体における制度運用の実態を把握するため、アンケート調査及びヒアリングを実施した。

2.1.1　アンケート調査及びヒアリングの実施（事業所）

改正高圧ガス保安法による新たな認定制度の検討にあたり、事業者の意見や保安活動の実態等を把握するため、認定事業所が多く所属していると見込まれる石油連盟、石油化学工業協会及び日本化学工業会を通じ、アンケート調査を実施した。

① アンケート調査の内容（事業所）

アンケート調査表（事業所）（別添１）のとおり

② アンケート調査の方法

石油連盟、石油化学工業協会及び日本化学工業会を通じ、それぞれの団体に所属する事業所に対し、アンケート調査表を配布し、回収した。

③ アンケート調査の結果

認定事業者３７社、非認定事業者１３社から回答があった。

④ ヒアリングの実施

アンケート調査の回答があった事業所のうち、認定事業者を中心に、アンケート調査結果についてヒアリングを実施した。

⑤ ヒアリングの方法

アンケート調査の回答があった認定事業者のうち１２社に対し、訪問又は WEB によりヒアリングを実施した。

⑥ ヒアリングの結果（まとめ）

ヒアリングを実施した結果、次のような取り組みが見られた。

(1) 法令違反への対応について

・法令違反発生時の措置等については、連絡ルートや対応をルール化している。
・工事が発生した場合は、製造部門、設備部門、保安部門で複層的なチェックを行っている。
・チェック者の要件については、特に定めていないが、一定の経験者を確保するようジョブローテーションを行っている。
・コンプライアンス啓発・教育として、強化月間、e-learning の活用、他社事例の紹介などの機会を設けている。

(2) テクノロジーの活用について

・導入・検証しているテクノロジーとしては、①情報の電子化・可視化（ワイヤレスセンサー等）、②現場作業の効率化・信頼性向上（ウェアラブル端末による作業支援、ドローン、360°カメラ）、③意思決定の高度化（早期異常検知、運転操作の最適化、画像処理技術等）など。
・テクノロジーに関連する規制として、防爆規制の見直しが必要。危険場所の設定は複雑で、かつ一部の危険場所があると、立入禁止措置やドローン航行ルートの設定が困難。非防爆の携帯型端末も利用を促進したい。
・現行認定要件の外部モニターについては、不要ではないか。

(3) サイバーセキュリティについて

・業界別（石連、石化協）ガイドラインに沿って、セキュリティ対策を実施している。
・外部コンサルタント等の診断を受け、その結果をチェックリストに反映した上でセキュリティチェックに活用している。
・主なサイバーリスクとしては以下を想定し、対策を実施している。
  ・情報ネットワークから制御ネットワークへのウィルス等マルウェアの侵入
  ・USB 機器等外部機器から制御機器へのマルウェア侵入
  ・制御システムへのマルウェア感染のネットワークを通じた被害拡大
・データ保存としては、運転データ、運転操作履歴、アクセスログ等を一定期間（5５年

以上程度）は保存している

(4) 変更工事等に係る特例について

・重要な変更（事前許可）としては主に以下のとおり
製造施設の新規設置、処理能力・貯蔵能力の増減が一定程度（例えば 20%）を超える工事、プロセスフローの大幅な変更を伴う工事、耐震設計構造物に係る工事、耐圧部に直接関係する工事、ガス種の変更

・事後届となる変更としては主に以下のとおり
処理能力・貯蔵能力の増減が一定程度（例えば 20%）未満の工事、部品更新や散水配管の形状変更など高圧ガスの耐圧部に影響を与えない工事、コンビ則第 17 条などに記載のある完成検査を要しない変更の工事、設計範囲内の常用の圧力及び常用の温度の変更、配管のルート変更・材質変更

・記録保存（届出不要）となる変更は主に以下のとおり
現行の軽微な変更の範囲内の工事、仕様変更を伴わない配管・計器類の更新、熱交換器のプラグ打ち、チューブ交換、特定設備の変更の工事であって当該設備の処理能力・位置の変更を伴わない工事、高圧ガス設備（配管、バルブ、フランジ継手または付属機器類）の変更の工事であって当該設備の処理能力の変更を伴わない工事、同一特定設備内（や配管）にて過去実績のある材質や類似の構造への変更

(5) 保安人員の配置の柔軟化について

・特に柔軟化のニーズはない。（ラインの指揮命令系統とマッチしないため、指揮命令系統を変更するほどメリットを感じない。責任者に対して教育がモチベーションになっている。緊急事態を想定すると統合された責任者への負担が大きすぎる。等）

・製造装置を安全に緊急停止できる一括遮断システムや保安係員と保安主任者の技術力向上につながる教育システムと評価方法の導入が想定され、これら要件に応じた柔軟化の形態としては製造装置と配管接続され密接な関係にある貯蔵設備や充填設備などの区分の統合が想定される。

(6) 審査方法等について

・認定基準の公開と基準への適否の理解を要望。申請・準備書類については、現行の現地審査よりも要点に絞った簡素化、現地審査の手順の公開、審査期間（申請→大臣認定までの期間）の公開を要望。

・認定基準の簡素化と明確化をしてほしい。

・書類審査をメインとして、申請内容で確認が必要な項目については確認リストを提出して頂き、確認項目を絞ってヒアリング調査（現地又は書類）を実施してほしい。

・申請書類は変更点に限った記載を認めるなどして作成負荷を低減してほしい。

・事業所としては中間検査も認定制度と同レベルと捉えており、中間検査のための日程調整、各種準備などの負担が大きい。

・先進的な技術の導入について年々要求が過度になってきており、それに対応できる人材の確保が難しくなっている。認定基準として、革新的なテクノロジーを活用しなくても、本質的な保安が確保されていれば良しとする要件としてほしい。

(7) 認定取消後の猶予期間について

・事業所の規模や個々のプラントの事情によるため一律に決定できない。

・必要な猶予期間は、2〜3 カ月（小規模）、6 カ月〜1 年程度（中から大規模）
（開放検査等を行う協力会社の確保・手配によるものが大きい）

2.1.2 アンケート調査及びヒアリングの実施（自治体）

改正高圧ガス保安法による新たな認定制度の検討にあたり、自治体の意見や法執行の実態を把握するため、認定事業所を所管する自治体等にアンケート調査を実施した。

① アンケート調査の内容（自治体）
アンケート調査表（自治体）（別添２）のとおり

② アンケート調査の方法
認定事業所を有する地方自治体等に対し、アンケート調査表を配布し、回収した。

③ アンケート調査の結果

２０自治体から回答があった。

アンケート調査の回答があった自治体のうち、認定事業所を多く有する自治体（茨城県始め１０自治体）を対象として、アンケート調査結果についてヒアリングを実施した。

⑤　ヒアリングの方法

ヒアリング対象とした自治体に対し、訪問又はWEBによりヒアリングを実施した。

⑥　ヒアリングの結果（まとめ）

ヒアリングを実施した結果、次のような意見があった。

(1) 法令違反への対応について

・現状の認定事業所であっても、チェックから漏れて未届け等の事例が発生している。
・都道府県で法令解釈の認識違いが生じることを懸念。相談されればよいが、相談すらなくなると数年後に大きなズレとなる恐れあり。
・許可→事後届となった場合、事業者側から相談が増える恐れがあるが、事務が許可ではなくなるため、手数料収入はないが相談案件が増え、自治体の負担増となるのではないか。
・申請書作成者以外の複数者のチェックが必要かつ、一定の経験を持つ者（例えば 3 年以上）がチェックするような仕組みが必要ではないか。

(2) 変更工事等に係る特例について

・重要な変更（事前許可）としては主に以下のとおり
製造施設の新規設置、高圧ガス設備の新増設、処理能力・貯蔵能力の増加を伴う工事、耐震設計構造物に係る工事、ガス種の変更
・事後届となる変更としては主に以下のとおり
処理能力の変更（20%増減以内など）を伴う工事、配管のルート変更等、設計範囲内の常用の圧力及び常用の温度の変更、予備機への変更、安全弁の設定圧力の変更、継手類の変更（毒性ガスを除く）
・記録保存（届出不要）となる変更は主に以下のとおり
現行の軽微な変更の範囲内の工事、熱交換器チューブのプラグ打ち、チューブの取り換え
・その他留意点
  ・認定事業所においても届出を失念したケース、記録が適切に保存されていないものがあることから、いかに事業所が適切に管理できるかが課題。
  ・行政側が事業者側の誤り等をチェックしていたところ、届出不要として事業所に任せるのであれば、適切な基準の設定と適切な監査の実施が必要。
  ・認定事業所からの事後届出については、工事内容を示す書類の添付は不要としてほしい。届出をされれば内容に不備がなく適切に法令遵守されているかの確認をすべきとなるため、かかる時間・人件費が変更許可申請・完成検査書類の確認と何ら変わりがない。
  ・工事の区分については、明確な判断基準、Q&A 集、相談できる窓口など統一的な運用のための措置を希望する。
  ・災害発生時に事業所で取り扱っているガス種や処理能力、製造施設を把握しておく必要がある。発災場所周辺に高圧ガス施設があるかないか、どのようなガスを取り扱っているかは重要な情報であり、防災計画の策定や統計の作成も行っているため、処理量の増減やガスの種類については把握が必要。
  ・位置の変更がある場合の工事は、工事後に技術上の基準を満足しない場合があると対応が困難となるため、事前許可とすべき。

(3) 保安人員の配置の柔軟化について

・保安人員の考え方は、製造の様態で異なるものであり、リスクアセスメントを深く行うことや運転管理の体制、適正な配置等は各事業所が判断する要素が大きい。
・保安係員等が、製造施設の維持や監視、技術上の事項等について、現行体制と比べてレベルが落ちることなく、適切に管理する体制をとれることが要件となる。

(4) 審査方法等について

・緩和をするのであればその分の責務を果たすべきであり、現行の認定基準は過剰な部

分はなく、むしろ、クリアできるような要件が追加される必要があるのではないか。
・事業所の自主保安を促進させるため、行政が確認する回数が少なくなると、事故や法令違反が起きる可能性が高くなることが予想されるため、審査はより厳しくしていただきたい。
・保安確保のために設けられた事業所規程類について、現場末端従業員への浸透性の確認を強化すべきである。また、内部監査制度に基づく報告や事故後の対応、コンプライアンス違反に対する報告の提出を義務付けるべきである。
・技術的な部分だけでなく、法律全般の知識を有する職員の有無と、当該職員が変更工事や事故時の対応にどのように絡むのかを確認できる書類が必要。
・現行の認定制度においては常に新しい取り組みが求められているため、事業者への要求事項が雪だるま式に増加している点を改善すべき。
・現在の認定制度の認定方法よりも、なるべく簡素化することが望ましい。認定に当たっては、新制度の要件を満たしていることの確認を重視すべき。

(5) 認定取消後の猶予期間について
・認定取消し後、直ちに運転を停止させ開放検査等を実施し、健全性を確認するまでは運転を認めない。
・取り消しに当たっては手順を踏む必要があるため、取消になりそうな時点から準備を始めれば、検査時期の短縮は可能ではないか。
・一律に決められない。事業者からの検査計画の提出を見て相談しながら個々に判断することになる。
・行政側としては、1～2 カ月間で対応可能。事業者側からみれば、4 カ月～6 カ月、場合によっては、1 年以上かかるケースがあるのではないか。

2.2　新認定制度の認定要件

2.2.1　経営トップのコミットメントについて

2.2.1.1　コンプライアンス体制、コーポレート・ガバナンスの確保検討の考慮事項

新認定制度において、事業所に求めるコンプライアンス体制、コーポレート・ガバナンスの確保について、次の事項を考慮し検討した。

（コーポレート・ガバナンス）
・高圧ガス保安分野の特殊性
・審査コスト
・非上場企業への対応

（コンプライアンス・法適合性確認能力）
・現行の規定との差分
・高圧ガス保安分野の特殊性
・審査コスト
・過去の法令違反事例の活用
・高いコンプライアンスが求められる他法の例

2.2.1.2　コンプライアンス体制、コーポレート・ガバナンスの確保の検討の視点

コンプライアンス体制の整備、コーポレート・ガバナンスの確保の要件は、現行の認定制度の要件に経営トップによる保安の方針の明示等が含まれていることも踏まえ、以下の四つの視点で検討した。

①取締役等に保安についての責任とイニシアティブを持たせ、保安活動をトップダウンで推進できる体制の整備
②取締役等が、保安に対する責務を適切に果たしていることを監督する体制の整備
③行政手続漏れ等の法令違反を防止するためには、事業所内で複層的なチェック体制の構築
④法令違反時の組織的隠蔽等を防止する観点から、法令違反発生時の通報手順の明確化

上記に加え、法令遵守体制の整備を促すため、近年の認定取消し事例を踏まえ、認定取消の処分基準において、重大・悪質な法令違反が発覚した場合を明文化することも必要となる。

2.2.1.3　コンプライアンス体制、コーポレート・ガバナンスの確保の検討

・金融関係では上場企業にコーポレート・ガバナンスコードが求められているが、このコードそのものを認定要件として求めることは、本来の目的と異なり、高圧ガスの認定要件という観点から見ても過剰な認定要件となると考えられる。

　また、保安の確保の方策として、当該コードが要求されている上場企業と要求されていない非上場企業で認定要件上を分けることは適当ではないと考えられる。

　上記より、基本的には監視及び牽制機能の部分を強化することを要件として追加することを検討し、以下のような考え方で認定要件について検討した。

①保安についての責任とイニシアティブを持たせ、保安活動をトップダウンで推進すること。
②保安の確保及び法令順守に関して、第３者的な視点での確認が行われる体制を有すること。

　なお、具体例としては、社外取締役、監査役等が出席する会議への報告や本社の事業所監査における外部知見の活用が考えられるが、後者の本社の事業所監査における外部知見の活用については、ヒアリング結果において、本社の事業所監査では、事業所の実態に詳しい者が実務的な確認も含めて監査を行っており、単に外部有識者が監査に参画することが、必ずしも監査の実効性が向上に繋がるものではないとの意見も複数あったところから、本社の事業所監査における外部知見の活用については、追加的な認定要件としては不要とした。

（法適合確認能力等）
・現行、認定要件では、コンプライアンス遵守に関する法令窓口の設置については要件化されているが、高圧ガス保安法上の行政手続きや技術上の基準への適合について確認をすることについての法適合確認能力に対する要件は明確化されていないため、

　例えば、以下のような複層的なチェック等を行うための要求事項を具体的に検討した上で、追加する認定要件について検討を行った。

①法令上の手続きの要否、その場合の適合すべき基準が整理されていること。
②　①の手続きを行う場合の業務手順・チェック体制が構築されていること。

③チェックを行う者の資格要件が定められていること
④法令違反等があった場合の対応について明確に定めていること。
⑤法令・基準に関する情報収集及び最新版化を行っていること。
⑥　①～⑥を確実に行うための措置（電子データの蓄積、検索機能など）を行っていること。

2.2.1.4　検討結果

2.2.1.1～2.2.1.3 までの検討を踏まえ、コンプライアンス体制、コーポレート・ガバナンスの確保について検討を行い、次のとおり、高圧ガス小委員会の資料として、認定要件案がまとめられた。（図１、図２）。

なお、取締役や監査役については、指名委員会等設置会社などの会社の運営形態の多様化についても考慮し、各会社の運営形態に応じて、取締役や監査役に相当する者や機能も当該要件を充足することができるような認定要件案とした。

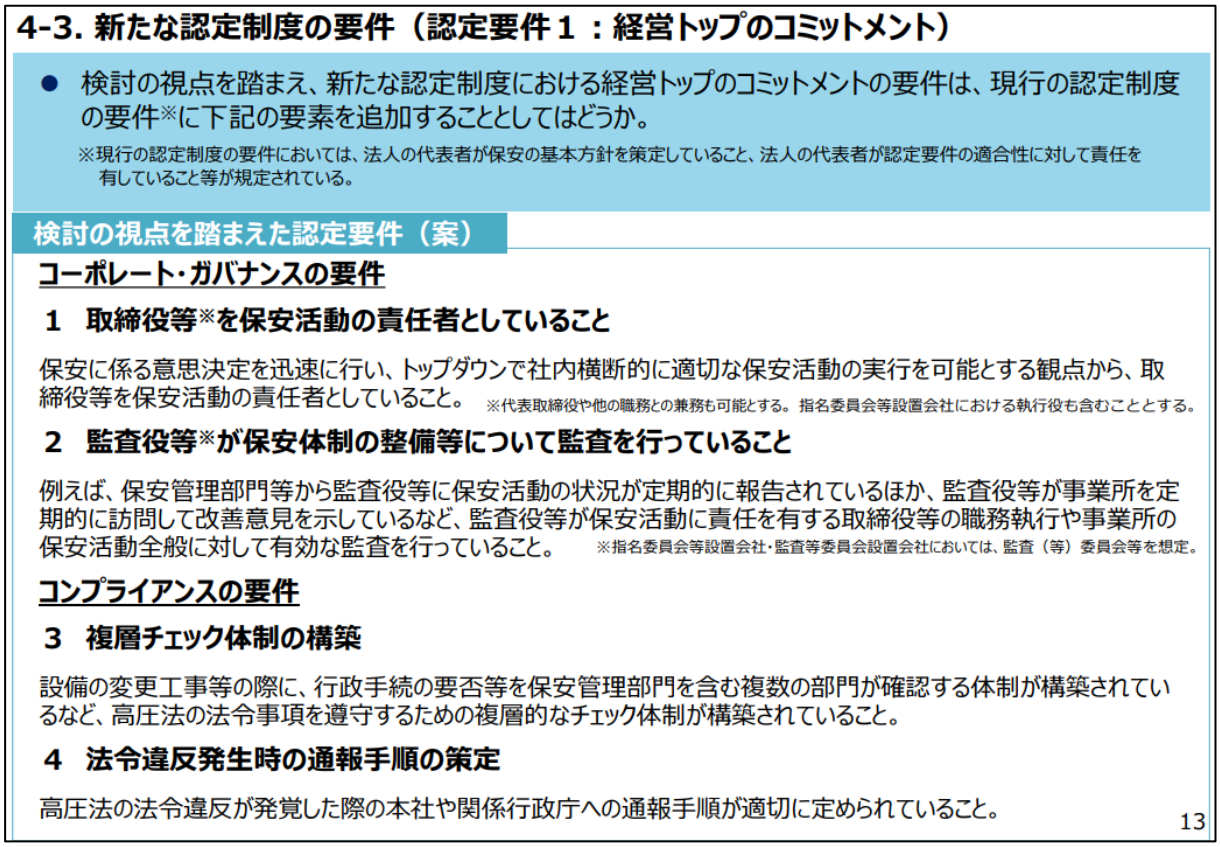
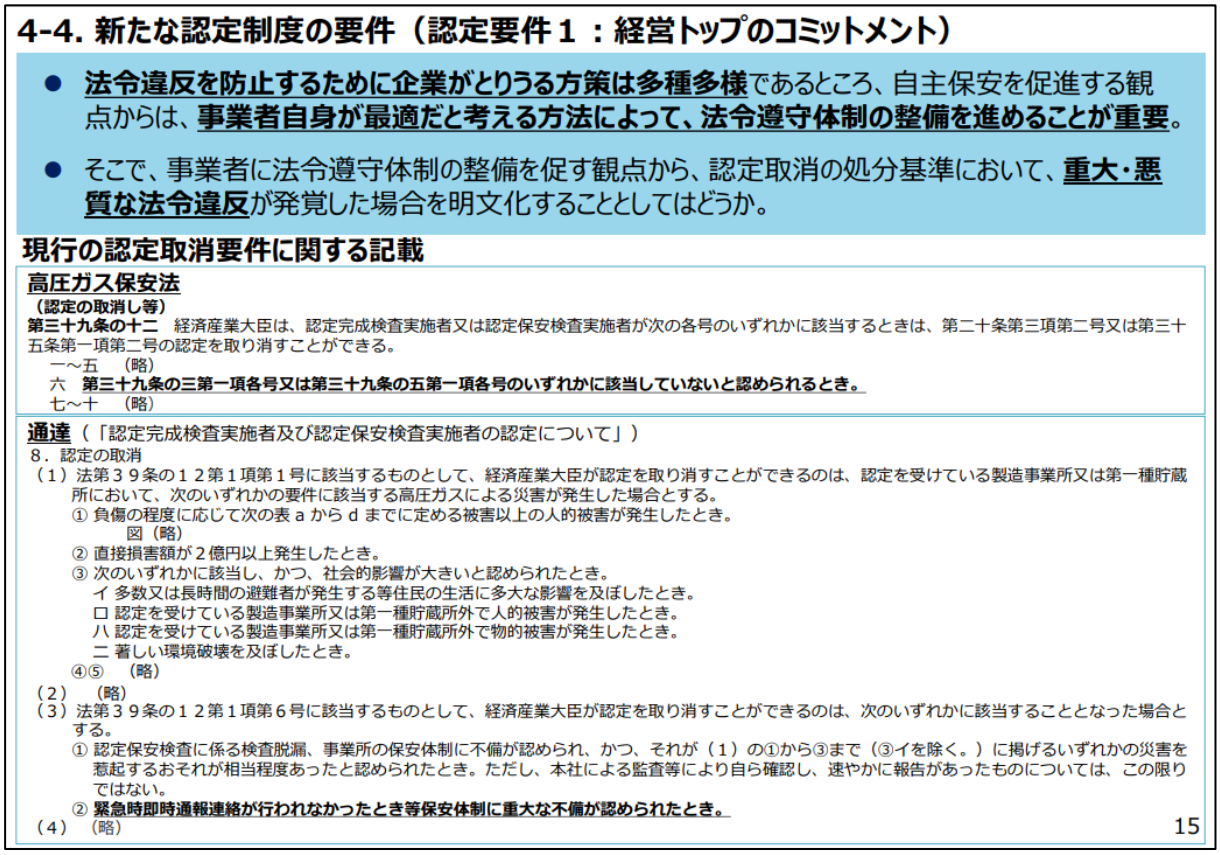


図１．高圧ガス保安法における新たな認定制度の詳細設計について（抜粋）
（2022 年 12 月 15 日開催第 23 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会　資料２）（以下「高圧ガス小委員会資料①」という。）



4-4. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

- **法令違反を防止するために企業がとりうる方策は多種多様**であるところ、自主保安を促進する観点からは、**事業者自身が最適だと考える方法によって、法令遵守体制の整備を進めることが重要**。
- そこで、事業者に法令遵守体制の整備を促す観点から、認定取消の処分基準において、**重大・悪質な法令違反**が発覚した場合を明文化することとしてはどうか。

現行の認定取消要件に関する記載

高圧ガス保安法
（認定の取消し等）
第三十九条の十二　経済産業大臣は、認定完成検査実施者又は認定保安検査実施者が次の各号のいずれかに該当するときは、第二十条第三項第二号又は第三十五条第一項第二号の認定を取り消すことができる。
一～五　（略）
六　**第三十九条の三第一項各号又は第三十九条の五第一項各号のいずれかに該当していないと認められるとき。**
七～十　（略）

通達（「認定完成検査実施者及び認定保安検査実施者の認定について」）
８．認定の取消
（１）法第３９条の１２第１項第１号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、認定を受けている製造事業所又は第一種貯蔵所において、次のいずれかの要件に該当する高圧ガスによる災害が発生した場合とする。
① 負傷の程度に応じて次の表ａからｄまでに定める被害以上の人的被害が発生したとき。
図（略）
② 直接損害額が２億円以上発生したとき。
③ 次のいずれかに該当し、かつ、社会的影響が大きいと認められたとき。
イ 多数又は長時間の避難者が発生する等住民の生活に多大な影響を及ぼしたとき。
ロ 認定を受けている製造事業所又は第一種貯蔵所外で人的被害が発生したとき。
ハ 認定を受けている製造事業所又は第一種貯蔵所外で物的被害が発生したとき。
ニ 著しい環境破壊を及ぼしたとき。
④⑤　（略）
（２）　（略）
（３）法第３９条の１２第１項第６号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、次のいずれかに該当することとなった場合とする。
① 認定保安検査に係る検査脱漏、事業所の保安体制に不備が認められ、かつ、それが（１）の①から③まで（③イを除く。）に掲げるいずれかの災害を惹起するおそれが相当程度あったと認められたとき。ただし、本社による監査等により自ら確認し、速やかに報告があったものについては、この限りではない。
② **緊急時即時通報連絡が行われなかったとき等保安体制に重大な不備が認められたとき。**
（４）（略）
15

図 2.　高圧ガス小委員会資料①（抜粋）

2.2.2　高度なリスク管理体制について

2.2.2.1　高度なリスク管理体制の検討の視点

高度なリスク管理体制について、以下の視点で検討した。

・A 認定については、現行のスーパー認定事業者相当のリスク管理体制を、B 認定については、現行通常認定事業者相当のリスク管理体制を求める。

2.2.2.2　高度なリスク管理体制の検討

A 認定については、現行のスーパー認定、B 認定については現行通常の現行の通常認定事業者相当のリスク管理体制を求めることについては、新たな認定制度においても現行認定要件レベルを維持することになる。

一方で、新たな認定制度においては、A 認定、B 認定に差はあるものの、双方に対して、高度なリスク管理体制が要求されることから、現行の通常認定では認定要件となっていない特定したリスクを低減する措置として、リスクマネジメントの認定要件を B 認定にも追加的に求めることとした。

なお、現行の通常認定事業者においては、現状は要件化されていなくとも特定したリスクを低減する措置は実施していることから、追加的な認定要件とはなるものの、事業者の運用実態に即した認定要件となっていると考えられる。

2.2.2.3　検討結果

2.2.2.1～2.2.2.2 の検討を踏まえ、高度なリスク管理体制について検討を行い、次のとおり、高圧ガス小委員会の資料として、認定要件案がまとめられた。（図３）。

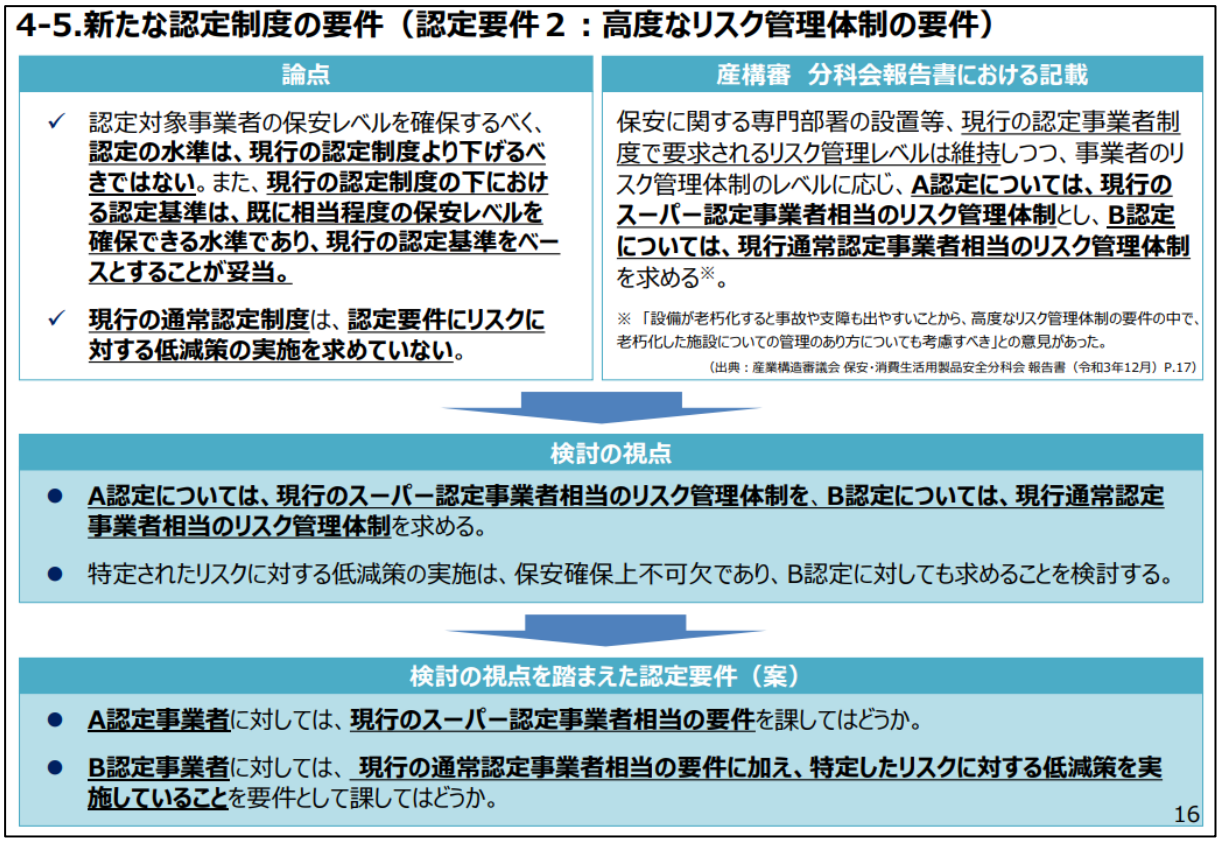


図 3.　高圧ガス小委員会資料①（抜粋）

2.2.3　テクノロジーの活用の検討の視点

今回の高圧法の改正においては、スマート保安（保安分野へのテクノロジー活用）の抜本的な促進を後押しすることが、重要な政策的目的の１つであることを踏まえ、高度な保安を行っている事業者に求められるテクノロジー要件の検討を行った。

2.2.3.1　認定要件の軸について

以下の軸を要件として再整理を行い、要件を検討した。

①テクノロジーの導入の程度

(1)導入計画→(2)トライアル検証→(3)導入→(4)効果検証→(5)改善

②テクノロジーの種類、段階

(1)異常検知、モニタリング技術、人の作業を代替する技術の導入

↓

(2)現状の状態を診断する技術の導入

↓

(3)予測する技術の導入

↓

(4)人の意思決定をサポート又は代替する技術の導入

③経営のコミットメント

＊①～③のについては、新規（新制度への移行も含む）、更新の違いも配慮した。

2.2.3.2　A 認定、B 認定に求める要件案について

（基本的な考え方）

①テクノロジーの導入の程度

基本的には、(1)導入計画→(2)トライアル検証→(3)導入→(4)効果検証→(5)改善はセットで考え、当該サイクルについては効果が期待できるものから、テクノロジーの進展に沿って、スピード感を持って対応していくことが重要であり、現行の認定要件である６カ月以上の検証については、認定要件から削除することとした。

なお、B 認定については、現行の通常認定ではテクノロジー要件は課していない点に留意

し、具体的には、高度なテクノロジーが完全に導入していることが認定要件として必須としないなどについて考慮してテクノロジーに係る認定要件の検討を行った。

・A 認定については、トップランナーの事業所であることを踏まえ、新規から導入等の計画に加え、一定程度技術の導入等まで求める。

・B 認定については、新規は導入等の計画の策定までを求め、更新は導入等を行った結果まで求める。

②テクノロジーの種類、段階

・A 認定については、予測や意思決定する技術等として(1)～(4)まで求める。（ただし、新規の場合は(3)、(4)は導入計画策定までとする。）

・B 認定は、(1)～（2）までを求める。（予測、意思決定の技術までは求めない。）

③経営のコミットメント

①、②を進める上でのドライビングフォースであり、A 認定、B 認定とも共通で求める。

①～③について表にまとめると以下のとおり

	新規		更新	
	A 認定	B 認定	A 認定	B 認定
①テクノロジーの導入の程度	①(1)～(5)	①(1)	①(1)～(5)	①(1)～(5)
②テクノロジーの種類、段階	②(1)～(4) ＊(3)、(4)については ①(1)までよい	②(1)、(2)	②(1)～(4)	②(1)、(2)
③経営のコミットメント	共通で求める。			

また、外部からのモニターの実施として、１年に１回の経済産業省への報告については、テクノロジー活用の進捗状況については全体として、スマート保安官民協議会等によって把握できることから、認定要件からは削除することとなった。

2.2.3.3　検討結果

2.2.3.1～2.2.3.2 の検討を踏まえ、高圧ガス小委員会の資料として、認定要件案がまとめられた。（図４、図５、図６）。

（図４）

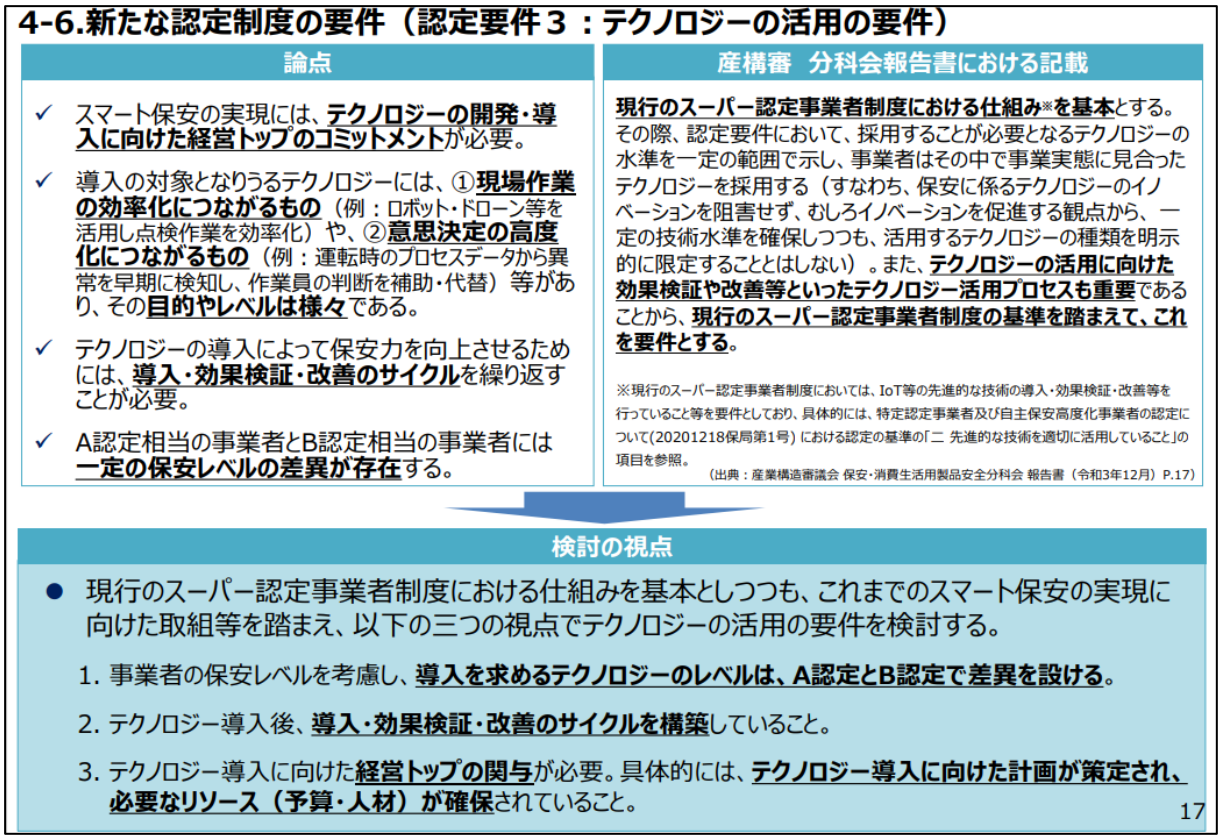


図 4.　高圧ガス小委員会資料①（抜粋）

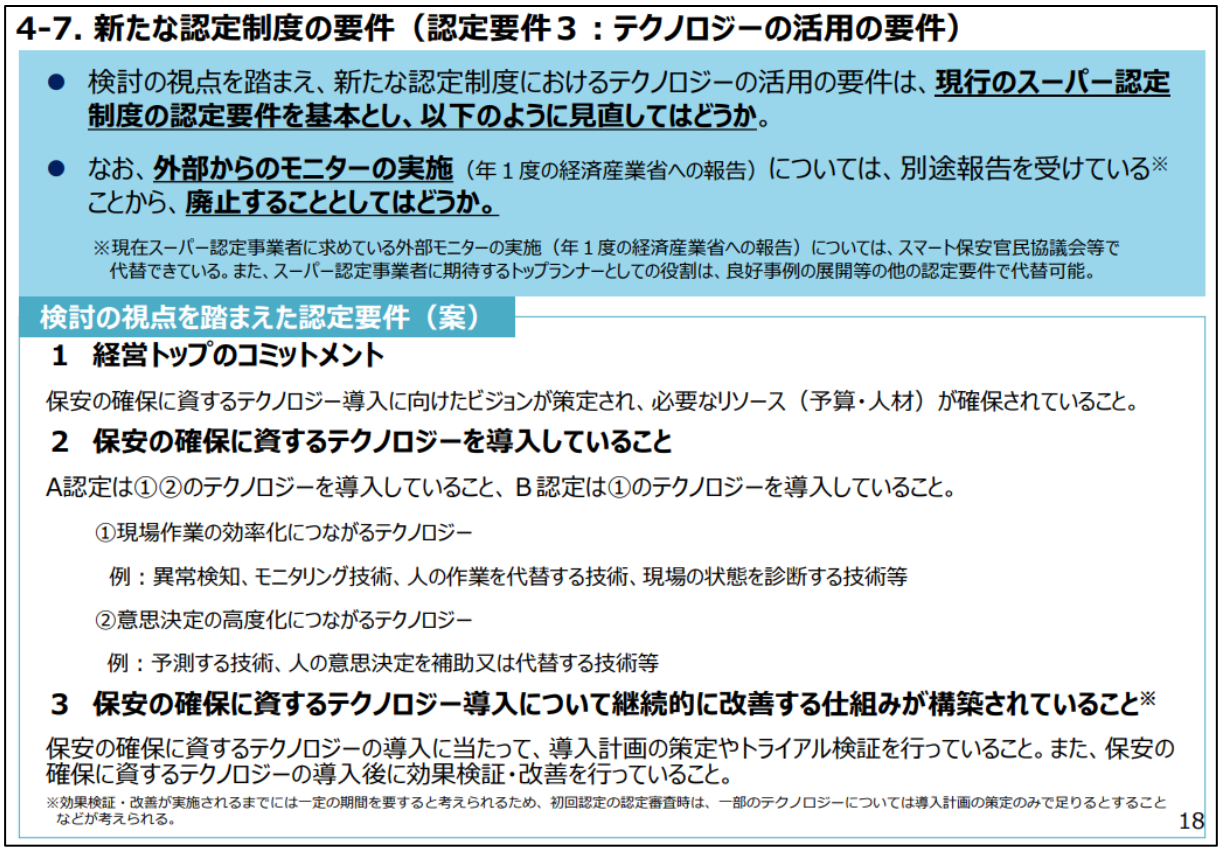


図 5.　高圧ガス小委員会資料①（抜粋）

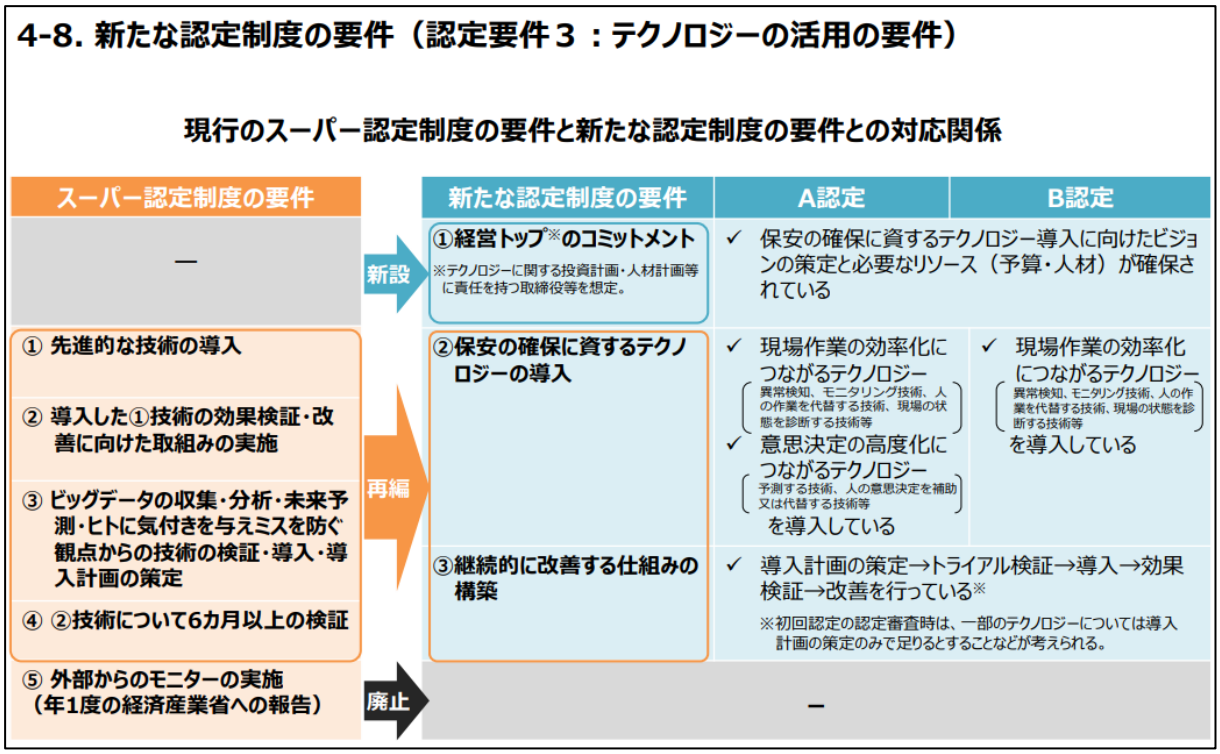


図 6.　高圧ガス小委員会資料①（抜粋）

2.2.4　サイバーセキュリティなど関連リスクへの対応について

2.2.4.1　サイバーセキュリティなど関連リスクへの対応の検討の視点

サイバーセキュリティなど関連リスクへの対応について、以下の視点で検討した。

・サイバーセキュリティなど関連リスクへの対応の要件は、組織や体制に着目した要件とする。具体的に は、 PDCA サイクルが構築されていることを要件とし、事業者が、技術の進展等に応じて自主的に、生産管理システム又はプラント制御システムに対するサイバー攻撃等のリスクへ対応する体制を維持・改善する仕組みがあることを確認する。

・本要件は新設の要件であるため、初回の認定審査時には一定の配慮を行う。

2.2.4.2　サイバーセキュリティなど関連リスクへの対応の検討

サイバーセキュリティについては、サイバーセキュリティ基本法で求められている重要インフラ事業者に対して、セキュリティの確保が努力義務として求められている。また、認定事業者においては、業界別ガイドラインが存在しない業種である事業者も存在している。

よって、単に業界別ガイドラインを認定要件とすると、業界別ガイドラインが存在しない業種である事業者に対しては、認定要件として適切でない場合も考えられる。

上記を踏まえ、サイバーセキュリティの認定要件については、その組織や体制に注目し、サイバーセキュリティにおける PDCA サイクルを構築していることを認定要件の基本とすることとした。

なお、サイバーセキュリティに関しては、日進月歩の分野であり、攻撃側の技術も常に高度化・巧妙化して中で、サイバーセキュリティに関するガイドライン見直しに伴い、認定要件も見直ししていく必要がある。

また、高圧ガス保安法におけるサイバーセキュリティは、高圧ガス事故を防止するためのサイバーセキュリティが求められており、例えば、単にサイバー攻撃によって顧客情報が漏えいしたが、爆発や火災事故等が発生しなかった場合は、高圧ガス保安法の法目的の対象ではないという考え方を踏まえて、サイバーセキュリティの認定要件の対象となるシステムは、プラントの運転等に密接に関係しているシステムとして、生産管理システム又はプラント制御システムとすることとした。

2.2.4.3　検討結果

2.2.4.1～2.2.4.2 の検討を踏まえ、高圧ガス小委員会の資料として、認定要件案がまとめられた。

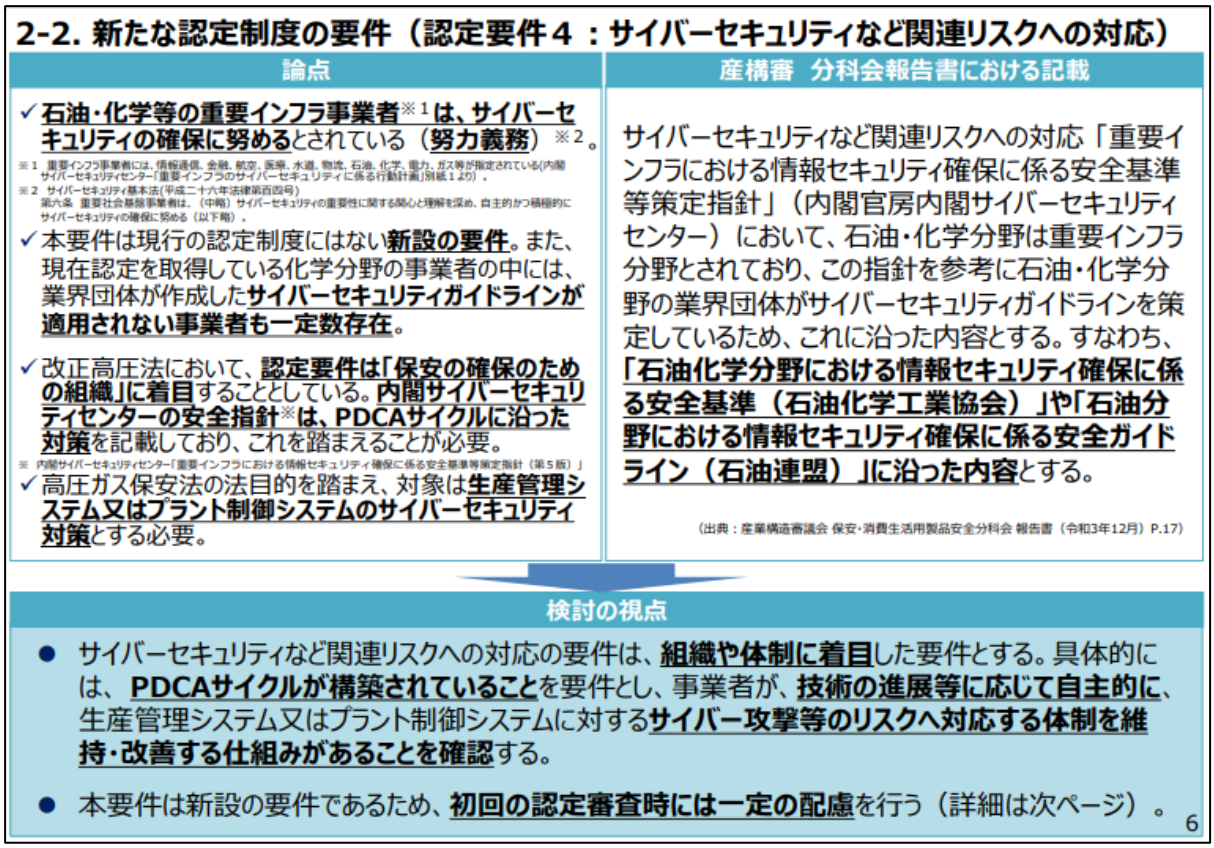


図 7. 高圧ガス保安法における新たな認定制度の詳細設計について②（抜粋）
（2023 年 2 月 24 日開催第 24 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会 資料１）（以下「高圧ガス委員会資料②」という。）

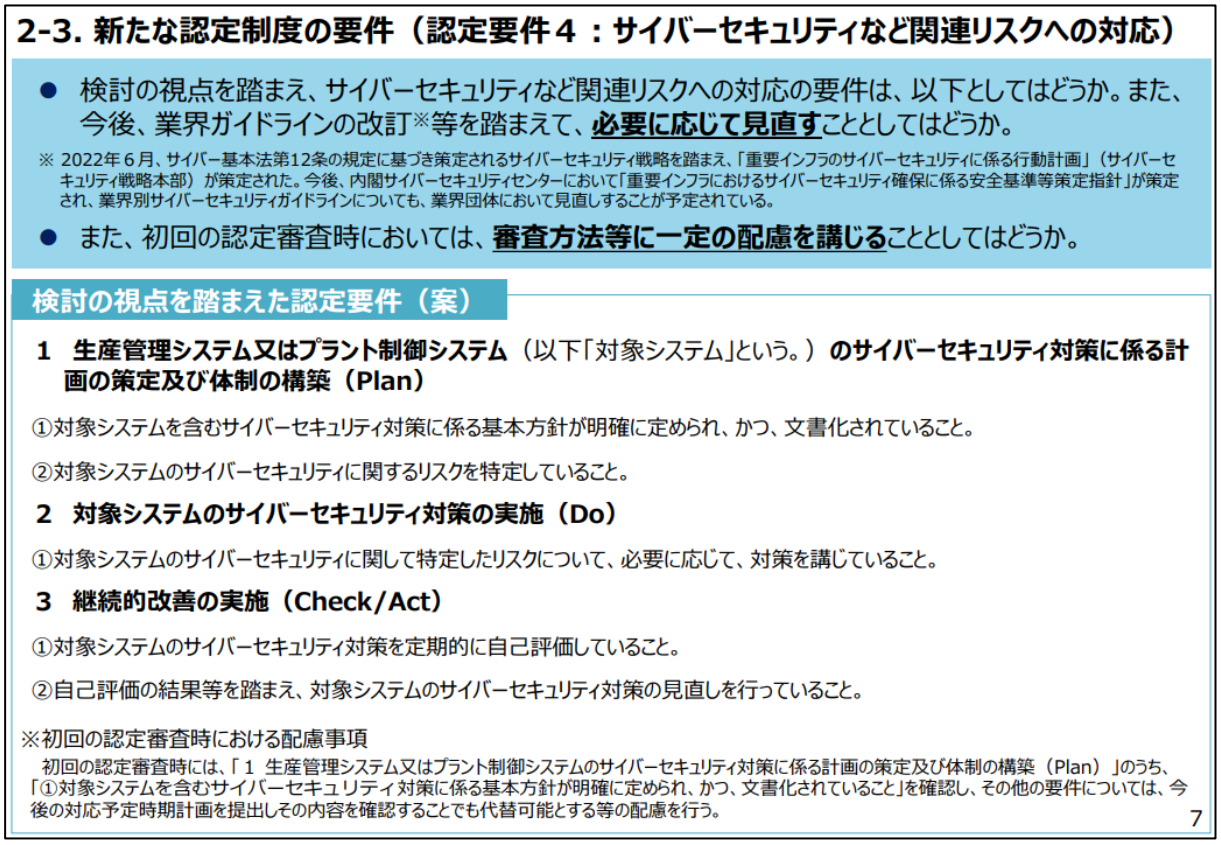


図 8. 高圧ガス委員会資料②

2.3　新認定制度における特例措置

新認定制度においては、変更工事の特例など、新たに設けられる特例措置に関して、具体的な内容を検討した。

2.3.1 変更工事等の特例について

2.3.1.1 改正法における特例について

改正法の特例については、法文上、以下のような構造となっており、特例の対象が限定されている点などに留意する必要がある。

①ガス種の変更は特例の対象外
②重要な変更以外の事後届出については完成検査が必要な場合あり
③非認定事業者には認められていない製造の方法について、事後届又は記録保存が可能
④認定完成検査記録は都道府県等への提出不要であり記録保存

2.3.1.2 変更工事の特例における仕分けの切り口（考慮要素）について

①工事が製造施設に与える影響
・工事の規模（製造施設の新設、増設（処理能力・貯蔵能力の増加・減少））
・工事の対象物（特定設備、耐震設計構造物、圧力容器、配管、継手、認定品、委託検査品など）
・製造の方法の変更（常用の圧力・温度の変更など）
・高圧ガスの種類（可燃性、毒性）
②事業者情報の把握の必要性（事故時・法令違反時に行政が迅速に対応する観点）
・処理能力・貯蔵能力の変更
・設備の位置の変更
・高圧ガスの種類の変更（特例は適用されず事前許可となるため把握可能）
③工事後の是正の可否（困難さ）
・位置の変更を伴う工事
・耐震設計構造物

2.3.1.3 上記の考慮要素を踏まえた分類方針（論点）

①一定の処理能力・貯蔵能力以内の変更を事後届以下として問題ないか。
→単純に処理能力等のみ（例 20%以上の増減）で規定した場合、②、③、④も事後届以下となることから、処理能力以外の条件が必要。
②耐震設計構造物の変更を事後届以下として問題ないか。
→耐震性能は重要。仮に耐震設計構造物上の誤りが発覚した場合、工事後の是正が困難な場合があることから、重要な変更とする。
③位置の変更を伴う工事を事後届以下として問題ないか。
→位置の変更を伴う工事は、保安距離などの変更がありえるため、工事後の是正が困難な場合がある。また、行政の防災計画にも関係するため、重要な変更とする。ただし、配管などの位置の変更は、事後届とする。
④認定品や委託検査品でないものを事後届以下として問題ないか。
→認定高度保安実施者の要件とメーカーの品質保証や第三者の検査を受検していることは関係がないため、認定品や委託検査品でないものは事後届以下としない。

2.3.1.4 その他の論点

①現行の許可工事→事後届とした場合にあっては、完成検査が必要となりうるが問題ないか。
→特定変更工事の範囲は、変更工事のうち軽微な変更と完成検査不要の工事を除くと解釈すれば、許可→事後届としても特定変更工事に該当するものは、完成検査が必要と解釈される。
技術上の基準が維持されているかについては、事業者で確認する必要がある。当該確認を完成検査として行うことについては事業者に課すことについては問題ない。なお、完成検査記録の届出は不要となっており、製造設備の運転には支障がないと考えられる。
②許可→事後届とした場合の自治体の運用は問題ないか。
・運用の統一性
→通達等に可能な限り明確に規定する。
・事後届となったとしても、確認するための自治体負担は変わらない。

→事後届として提出する書類を可能な限り簡素化する。ただし、事業者側で、詳細な工事記録が保存されているのが前提（記録保存義務は課せられていない）

③現行の軽微な変更→記録保存とする際、2.②の事業者情報の把握の必要性から、事後届とするものはないか。

→処理能力・貯蔵能力の変更（増減含む）を伴うものは事後届

→位置の変更（配管などは除く）を伴うものは事後届

＊この場合、特定変更工事の範囲に該当するものは完成検査もセットで行う必要あり

2.3.1.5 留意点等

・現行制度において届出とされている「軽微な変更」工事については、完成検査は不要とされている。一方、新認定制度において届出とされている「重要な変更以外の変更」工事については、特定変更工事に該当する場合にあっては、完成検査が必要となる。このため、特に現状の軽微変更を重要な変更以外の変更に加える場合には、現行よりも事業者の負担が増すこととなるため、事業者の混乱を招かないよう留意が必要。

・新制度での変更点（主な変更点：完成検査の記録は届出から記録保存へ変更・変更工事が事後届の場合でも完成検査が必要となる、等）を事業者に丁寧に周知する必要。

2.3.2 変更工事等の特例の具体的な内容について

2.3.1 の考慮要素等に基づいて、以下のとおり検討を行った。なお、考慮要素等については、現行の「①軽微な変更工事の対象となっているもの」、「②完成検査不要の工事となっているもの」にも考慮されていることも踏まえて検討を行った。

2.3.2.1 許可となるもの

① 重要な工事

(1) 新たに製造施設の追加を伴うもの

＊条文に規定する際には、(2)を満たさない又は新たな認定施設となっていないため、あえて規定する必要がないと考えられるが概念として記載。

(2) 変更の規模、処理能力の変更等が一定以上であるもの

【特定設備（特定設備検査規則の施行前に製造された設備であつて、特定設備に相当するものを含む。以下同じ）について】

・特定設備の増設又は移設、転用、再使用若しくはこれらの併用

・耐震設計構造物である特定設備の変更（耐震設計上の軽微な変更を除く）

＊現行の完成不要の工事は、耐震設計構造物である特定設備は除かれている。

・耐震構造物以外の特定設備の取り替え・変更（A 認定は事後届、B 認定は重要な工事とする。）

＊現行の軽微な変更では、特定設備の取り替え・変更はスーパー認定に限られている。

・特定設備検査規則に準じて行う協会の委託検査又は指定特定設備検査機関が行う検査に合格したものへの変更でないもの

・設置位置の変更を伴うもの

・２０％の範囲を超える処理能力の増減があるもの

＊現行の完成不要の工事の条件となっている。

【特定設備以外の高圧ガス設備】

・耐震設計構造物の変更を伴うもの（耐震設計上の軽微な変更を除く）

・設置位置の変更を伴うもの（配管等の変更を除く）

・認定品等（認定品、高圧ガス設備試験合格品、KHK 委託検査品）でないもの

・２０％の範囲を超える処理能力の増減があるもの

＊貯蔵能力の増減にあっては、現行の完成検査不要の工事にその概念がないため、規定していない。

② 許可となる製造の方法の変更

変更工事等により従来の設計条件を変えて行う常用の圧力及び常用の温度の変更

③ ガス種の変更

高圧ガスの種類に限らずガス種の変更は特例の対象外のため全て許可対象

2.3.2.2 事後届となるもの

①事後届となる工事

【特定設備について】

（A 認定事業所の特定設備の取り替え・変更に対してのみ適用）

・２０％以内の範囲で処理能力の増減があるもの
・耐震設計上の軽微な変更工事であるもの
・設置位置の変更を伴わないもの
・取り替えについては、同等以上の性能を有するものへの取替えに限る。
・変更については、特定設備検査規則に準じて行う協会の委託検査又は指定特定設備検査機関が行う検査に合格したものへの変更に限る。

【特定設備以外の高圧ガス設備】

（A 認定、B 認定共通）

・２０％以内の範囲で処理能力の増減があるもの
・耐震設計上の軽微な変更工事であるもの
・設置位置の変更を伴わないもの（配管等の変更を除く）
・認定品等であるもの

（B 認定のみ）

・配管等の変更において、設置位置の変更を伴う場合は、溶接等の現場加工を伴う場合は、管認定試験者が行う管認定工事によるものに限る。

＊スーパー認定事業所は、認定品以外でも設置位置の変更を伴う配管工事は、現行は、軽微変更であるが、通常認定事業所は、設置位置の変更を伴う配管工事は軽微変更の対象となっていない。

②事後届となる製造の方法の変更

設計条件以内の常用の圧力及び常用の温度の変更（１．（１）を伴うものは除く）

なお、変更工事について上記のような分類方法もあるが、同じ事後届の中で、完成検査を要するものと、完成検査を不要とするものが存在することにあることから、許可でないものに完成検査が要求されことになることから手続き上の混乱を招く可能性があり、「事後届となる変更工事については、特定変更工事以外の工事つまり完成検査不要工事と一致させる」こととし、重要な変更工事は、特定変更工事とすることとなった。

2.3.2.3 記録保存となるもの

①記録保存となる工事

現行の軽微な変更工事に該当するもの。ただし、処理能力の変更を伴うものについては、自治体の事故時の対応等の観点から、記録保存とはせずに、事後届出以上とする。

なお、現行の軽微な変更における通常認定、スーパー認定の差については、踏襲する。

②記録保存となる製造の方法の変更

常用の圧力・常用の温度の変更を伴わない製造の方法の変更に該当するもの。

ガスの種類が変更される場合は、遵守すべき技術上の基準の変更の可能性があるが、その場合は特例の対象外として許可の対象となるため

2.3.2.4 記録保存義務が掛からないもの

現行の軽微変更通達における許可及び届出の不要な工事については、記録保存義務が掛からないものとして整理した。

2.3.3 軽微な変更（記録保存）の対象の拡大等について

2.3.3.1 軽微な変更（記録保存）の対象の拡大について

認定保安高度事業者が行う軽微な変更にあっては、記録保存義務を課した上で、許可及び届出が不要であり、現行の軽微な変更であって、処理能力の変更を伴わないものにあっては、記録保存とすることを提案したところ。

これに加えて、事業者からの要望も踏まえつつ、記録保存とする対象を拡大することについて、検討を行った。

①基本的な考え方

事後届が特定変更工事以外（完成検査不要工事）となることから、事後届は、基本的には、取り替えの工事が対象となっており、設備に部分的に変更を加えるような工事は対象となっていない。

したがって、現行の許可であるものを軽微な変更（記録保存）に手続きのランクを変更する際には、記録保存に分類されることとなる。一方で、事後届が原則として取り替え工事に限定されていることから、記録保存とする取り替え工事以外の変更の拡大にあっては、限定的になるものと考えられる。

②軽微な変更の拡大（記録保存の拡大）等について

①のとおり、基本的には限定的な拡大となることを踏まえ、部品の取り替えであって、現行の軽微な変更に記載されている程度のもの又は高圧ガス設備の強度等に関係のない軽微な変更の拡大の対象とするとして検討した結果は、以下のとおり

【軽微な変更（記録保存）とするもの】

①熱交換器（エアフィンクーラーを含む）チューブの取替え

・現行は多管円筒形熱交換器の熱交換器のチューブの取替えに限定されているが、適切な設備管理等が行われるのであれば、熱交換器の型式を限定する必要はないと考えられる。

②フランジ継手以外の継手類の変更

・現行は認定事業者に認められている軽微な変更工事について、配管、バルブ又はフランジ継手から配管、バルブ又はフランジ継手への変更に限っているが、継手については、配管部品類であり、フランジ継手に限定する必要がないため。

③配管の撤去工事

・配管類の工事に附帯して発生する工事のものであることから、配管、バルブ又はフランジ継手から配管、バルブ又はフランジ継手と併せて、軽微な変更とする。

【手続き不要の工事とするもの】

①熱交換器のプラグ打ち

・劣化した熱交換器のチューブなどについて、機能しないように、チューブにプラグを打つ（蓋をする）ものであり、設備の全体の耐圧性能等の技術上の基準には影響がないと考えられるため。

②熱交換器のプラグ打ちに係るチューブの切断又は撤去

・①と同様に設備の耐圧性能等の技術上の基準には影響がないと考えられるため。

【その他通達等で明確にする項目】

①完成検査不要工事に該当する「第五条第一項第十九号の規定により製造することが適切であると経済産業大臣の認める者が製造したもの」の明確化

・軽微な変更工事には該当することが明確になっているが、上記の完成検査不要工事に KHK 高圧ガス設備試験品、KHK 委託検査品が適用されるのかが不明確なため、完成検査不要工事の解釈に規定。

2.3.4 保安検査時期の柔軟化について

保安検査については、改正高圧法においては、現時点では定期に行うことを基本とするものの、今後、CBM や常時監視等の導入が本格化することも想定し、新たな認定制度の認定事業者については、当該「定期に」との法律上の文言を削除されている。この場合において、検査の時期については、経済産業省令で定めるものとし、具体的には、現時点では、定期に行うことを基本としつつ、 CBM や常時監視等による場合には、それ以外の時期によことも可能とし得るよう措置する。

上記の基本的な考え方を踏まえて、現行の認定事業者においては、個別の保安検査の項目ごとには、検査方法やその実施時期については、保安検査を定める告示以外の方法でも検査可能な制度となっている。保安検査全体の時期については、その事業所の具体的な CBM や常時監視等を活用した検査方法等の状況も踏まえて、個別に認めていく必要があることから、経済産業大臣が個別に保安検査実施時期を認める制度とする。

2.3.5 定期自主検査の義務の廃止に伴う認定要件でのフォローについて

新たな認定制度において、認定高度保安事業者は、法第 35 条の２の定期自主検査の義務が除かれている。

これについて、保安検査と定期自主検査では対象となる設備の範囲が異なり、定期自主検査の対象範囲の方が広いことに加えて、自主検査自体は重要であり、認定審査においてフォローする必要がある。

なお、現行の認定要件でも、設備管理を担当する組織に一部自主的な検査についての規定がある。

基本的な考え方としては、当該自主検査は、法定で定めるものでなく、事業者自ら行うものであり、検査方法や検査時期に関しても制限はないが、認定要件又は評価の視点に追加し、適切に行われているかどうかについては、認定審査時に確認することとする。

【参考】

認定完成検査実施者及び認定保安検査実施者の
認定に係る事業所の体制の基準を定める告示（抜粋）

四 設備管理を担当する組織に関する事項。
イ 体制
(1) 運転管理を担当する組織と工事を担当する組織（コンビナート等保安規則別表第五又は別表第七の適用を受ける認定事業所にあっては、工事担当部門。）との引継ぎ及び引渡しに関する体制。
(2) 着工手順、火気使用作業、高所作業、槽内作業その他の工事管理に関する体制。
ロ 役割
(1) 設備補修に係る計画に沿って定期的に又は現場からの要請を受けて、高圧ガス設備を、目視又は検査機器により検査を行うこと及びその方法を定めること。
(2) 製造施設の新設、増設、変更に当たっての材料の選択、腐食、磨耗その他の保安上特に配慮すべき事項を定めること。
ハ 資格
設備管理を担当する組織に所属している者の五十パーセント以上が製造保安責任者免状又は必要な非破壊検査技術に関する資格を有していること（コンビナート等保安規則別表第七の適用を受ける認定事業者に限る。）。

2.3.6 危害予防規定の届出義務・保安人員の選解任の届出義務の廃止

①危害予防規程

改正保安法第 39 条の 23 に記載のとおり、危害予防規程が保存されていることを確認すればよいと考える。なお、危害予防規程が改正された場合には現行は届出が必要であることから、危害予防規程に記載されている改正履歴も確認を行う。

【参考】
高圧ガス保安法（令和四年法律第七十四号公布の日から一年六月を超えない範囲内において政令で定める日に施行予定の改正版）
第三十九条の二十三　認定高度保安実施者は、危害予防規程を定め、又は変更したときは、第二十六条第一項の規定にかかわらず、同項の規定による届出を要しない。この場合においては、経済産業省令で定めるところにより、当該危害予防規程を保存し、都道府県知事から提出を求められたときは、速やかにこれを提出しなければならない。

②保安人員の選解任（第 39 条の 24～26）

改正保安法第 39 条の 24～26 に記載のとおり、保安人員の選任又は解任に係る記録が保存されていることを確認する。

具体的には、選解任の履歴管理状況、資格者、経験を満たしている者が選任されていることを確認する。

【参考】

高圧ガス保安法（令和四年法律第七十四号公布の日から一年六月を超えない範囲内において政令で定める日に施行予定の改正版）
第三十九条の二十四
１（略）
２　認定高度保安実施者は、第二十七条の二第一項、第三項若しくは第四項の規定による保安統括者、保安技術管理者若しくは保安係員の選任又はその解任については、同条第五項又は第六項の規定にかかわらず、これらの規定による届出を要しない。この場合においては、経済産業省令で定めるところにより、当該選任又は解任に係る記録を作成し、これを保存しなければならない。

③クラウドの利用を前提とした「電磁的方法による保存等をする場合に確保するよう努めなければならない基準について」の改正の検討
「2.5.2　記録保存の方法について」を参照。

2.3.7 保安人員の柔軟化について

保安人員の柔軟化については、プロセスや運転管理体制が事業所ごとに異なり、一律に要件を定めることが難しいことから、区分を柔軟化するための特例の規定を設ける。

なお、一定の条件としては、一体区分の製造施設への監視と緊急事態への対応が適切なものなどとする。

また、改正高圧法においては、「区分ごとの配置を要しない」と法令上措置されていることから、「区分ごとに」という規定は設けないこととする。

【規定ぶりのイメージ】

コンビ則第 25 条に以下の規定を追加する。

・法第三十九条の二十四の規定により、認定高度保安実施者は、監視の方法、緊急事態への対応方法が適切であり、かつ、適切な保安管理が行えると経済産業大臣が認める方法で、甲種化学責任者免状、乙種化学責任者免状、丙種化学責任者免状、甲種機械責任者免状又は乙種機械責任者免状の交付を受けている者であつて、第三項に規定する高圧ガスの製造に関する経験を有する者のうちから、保安係員を選任することができる。

2.3.8　検討結果

2.3.1～2.3.7 の検討を踏まえ、次のとおり高圧ガス小委員会の資料として、新たな認定制度の特例案がまとめられた（図９、図１０、図１１、図１２、図１３）。

3-3. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- 新たな認定制度における製造施設の位置・設備等の変更の許可・届出等は、完成検査との関係（詳細は次ページ）を含め、**新制度の円滑な運用を確保する観点から、以下の分類**としてはどうか。
- その際、**「重要な変更」と「軽微な変更」の内容については、省令等において限定列挙**するとともに、**その他の変更を含め詳細な解釈についても通達等で可能な限り明らかにする**ことで、わかりやすい制度とする。

製造施設の位置・設備等の変更の許可・届出等の分類（案）

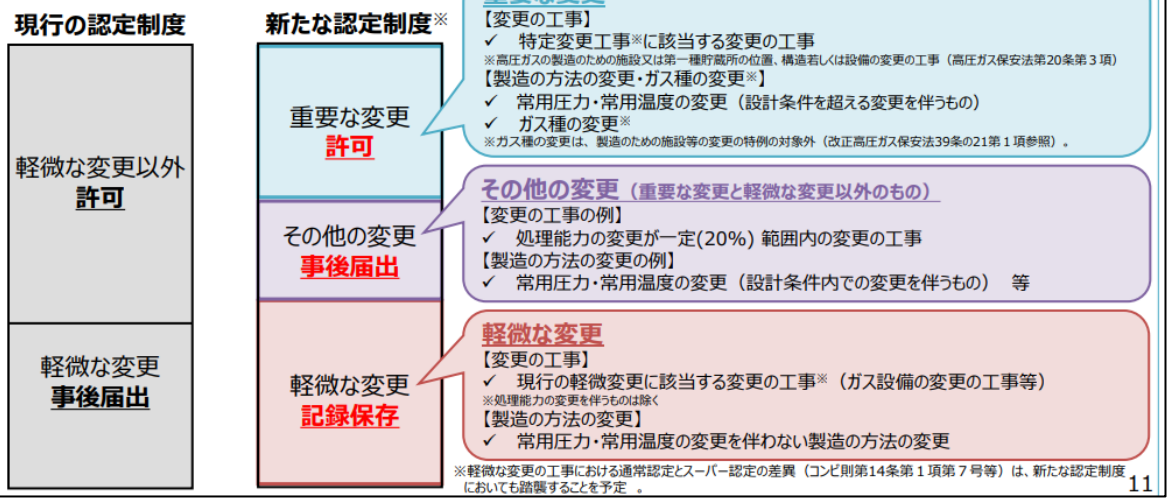


図９．高圧ガス委員会資料②（抜粋）

3-4. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- **製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係は、以下の整理**としてはどうか。
- なお、完成検査の検査記録は、現状届出義務となっているところ、**新たな認定制度においては記録保存義務**となるため、**完成検査終了後、速やかに運転を開始することができる。**

製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係

現行の認定制度

変更の工事			
軽微な変更以外の変更	特定変更工事※1	許可	完成検査必要（事後届出）
	特定変更工事以外の工事		完成検査不要
軽微な変更※2		事後届出	完成検査不要
製造の方法の変更・ガス種の変更			
軽微な変更以外の変更		許可	完成検査不要

新たな認定制度

変更の工事			
重要な変更	特定変更工事※1	許可	完成検査必要（記録保存）
その他の変更	特定変更工事以外の工事	事後届出	完成検査不要
軽微な変更※2		記録保存	完成検査不要
製造の方法の変更・ガス種の変更※3			
重要な変更	✓ガス種の変更※3 ✓常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）	許可	完成検査不要
その他の変更	✓常用圧力・常用温度の変更（設計条件内での変更を伴うもの）	事後届出	完成検査不要
軽微な変更	✓常用圧力・常用温度の変更を伴わない製造の方法の変更	記録保存	完成検査不要

※１ 高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）
※２ 軽微な変更の工事の範囲については、今後、必要に応じて見直すことを想定。
※３ ガス種の変更は製造のための施設等の変更の特例の対象外（改正高圧ガス保安法第39条の21第１項参照）。

12

図 10. 高圧ガス委員会資料②（抜粋）

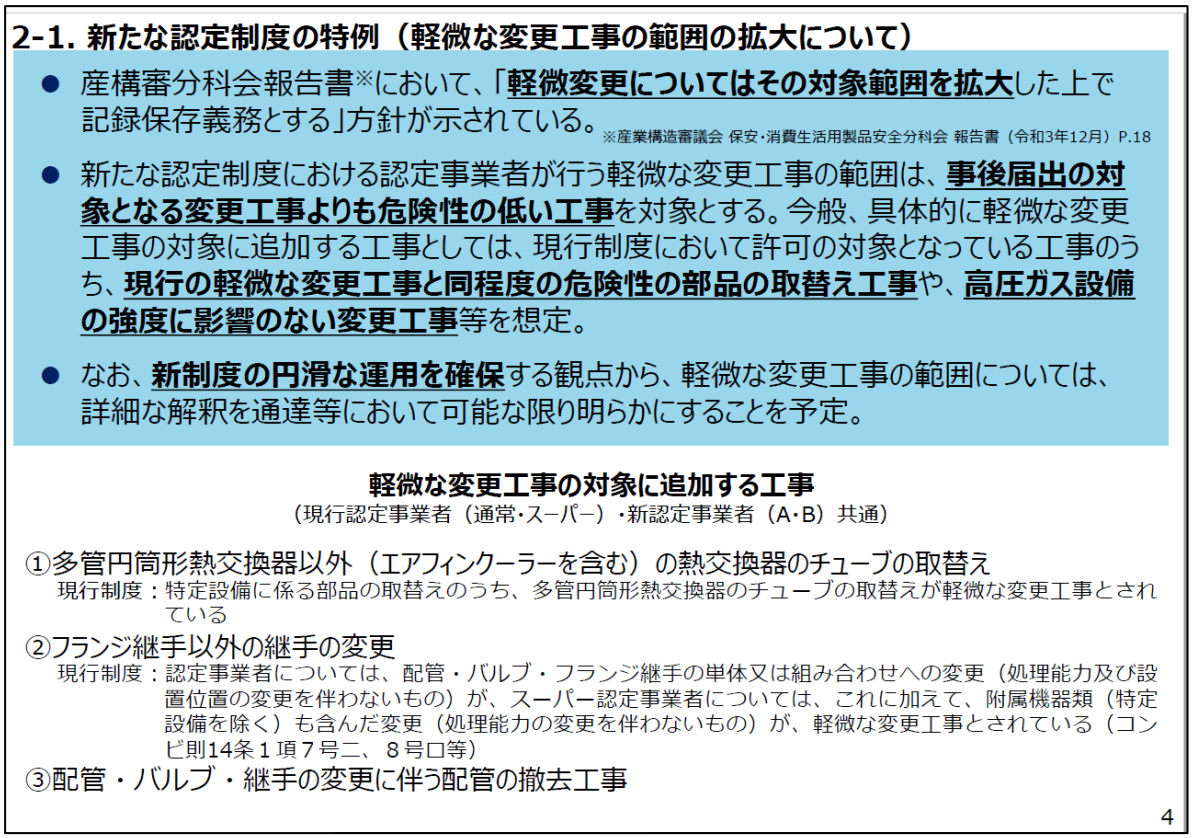


図 11.　高圧ガス保安法における新たな認定制度の詳細設計について③（抜粋）
（2023 年 3 月 24 日開催第 25 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会　資料３）（以下「高圧ガス小委員会資料③」という。）

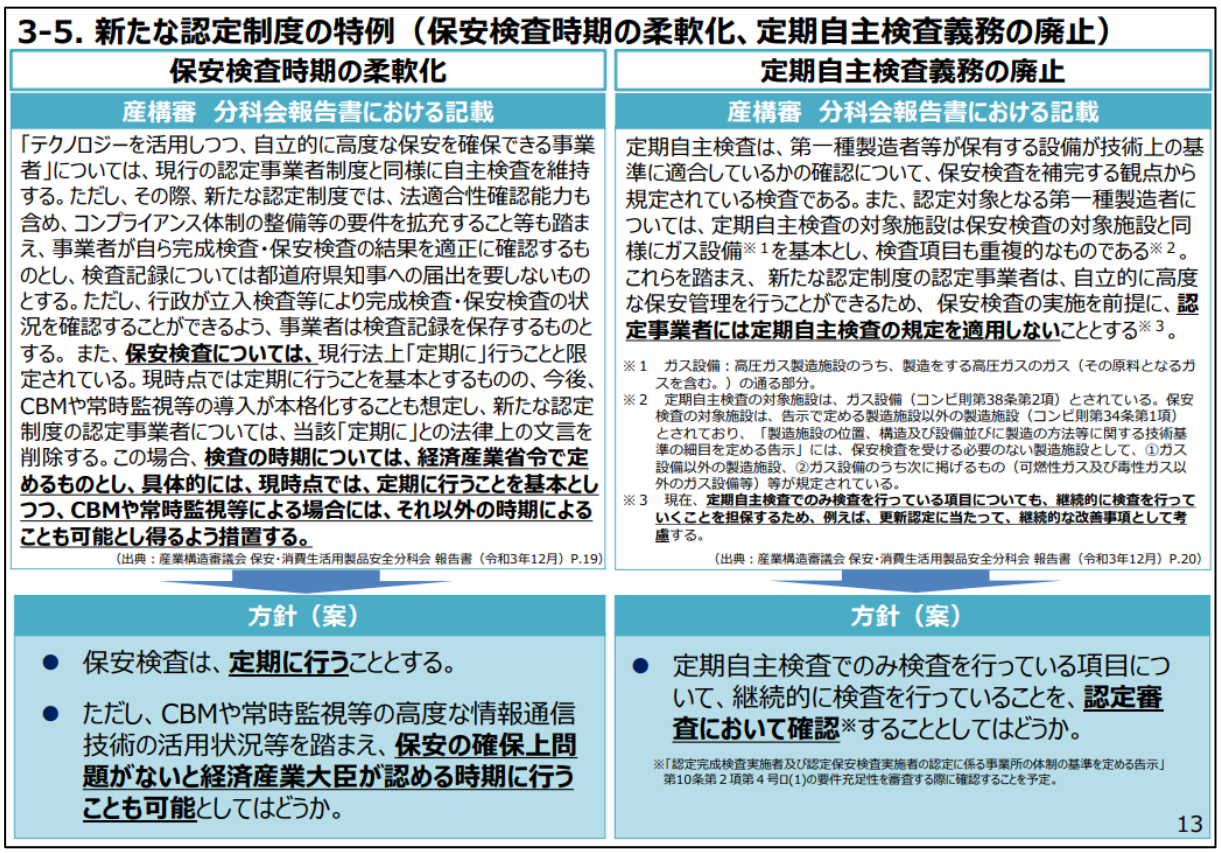


図 12.　高圧ガス委員会資料②（抜粋）

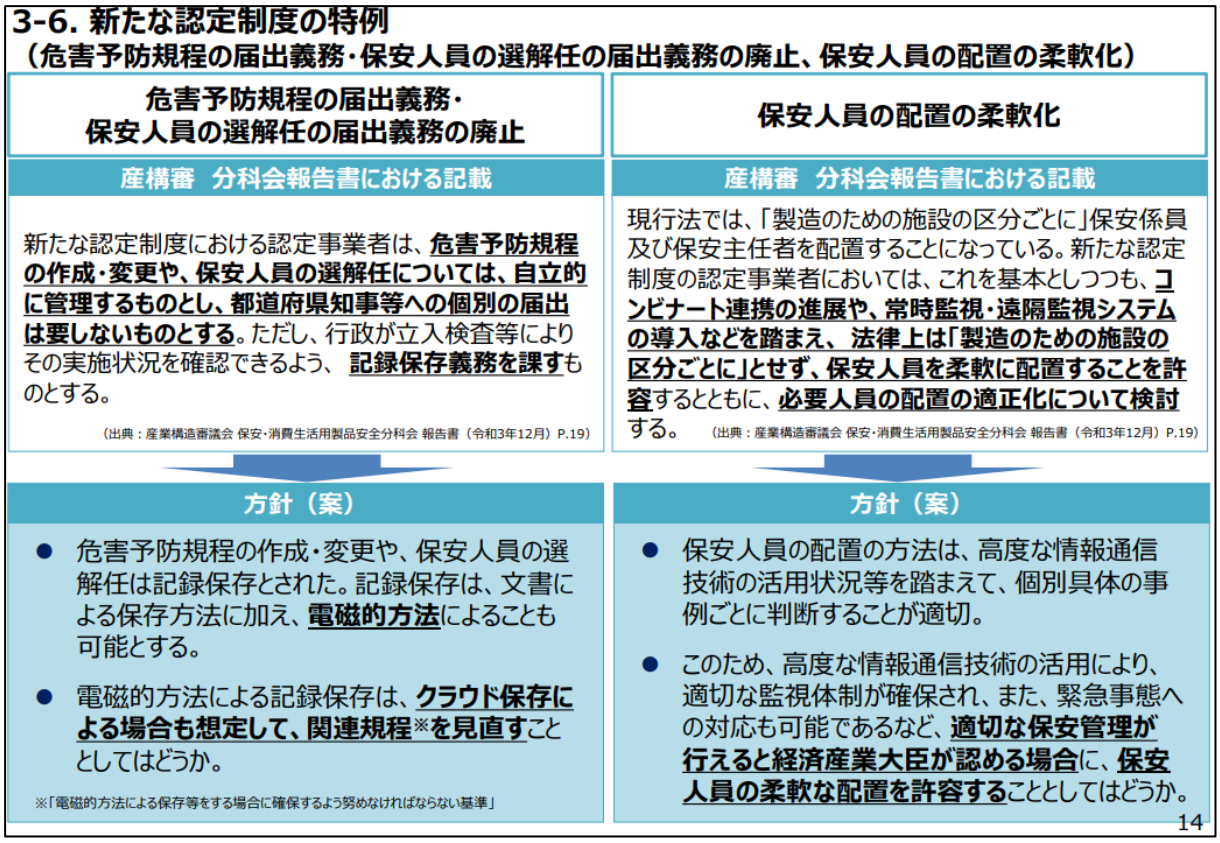


図 13.　高圧ガス委員会資料②（抜粋）

2.4　新認定制度の審査方法等

2.4.1　新認定制度の審査方法等の検討の視点

新認定制度の審査方法等について、以下の視点で検討した。

・新たな認定制度では、安全の確保及び向上を前提に、合理的かつ迅速な審査手続とする観点から、 国が（KHK 等への意見聴取・調査依頼、外部有識者からなる審査会審査などを活用しつつ）審査を 行うこととしており、以下のような見直しを行う方針。

① 審査プロセスの合理化（プロセスの合理化、申請書類・手数料の見直し、評価結果のランク付け廃止等）

② 審査基準の透明化（審査基準・審査会審査の議事要旨※の公開)

※企業の機密情報等を除いた上で作成。

2.4.2　更新申請時の審査の簡略化について

更新申請時の審査の簡略化の条件については、認定の審査を厳正に行うことを前提とし、更新審査後にA認定の場合は７年間、B認定の場合は５年間の認定のインセンティブを享受することを踏まえ、その対象は可能な限り限定的とすべきである。これに従って検討を行った。

なお、当該条件についてはA認定、B認定で共通とする。

2.4.2.1　事故等の発生状況

①高圧法・石災法の事故

A 級、B1 級事故以外であっても、繰り返し事故として B2 級以上の事故 が発生している事業所については、簡略化の対象外とする。

②労働災害

労働災害については、プラント内（高圧ガス製造施設以外も含む）において、死亡又は休業４日以上 の労働災害を発生させた事業所については、簡略化の対象外とする。対象は、従業員に加え、協力会社員も含むものとする。

＊休業災害が発生した場合、労働者死傷病報告を所轄労働基準監督署長に提出しなくてはならない（労働安全衛生法第１００条）。この場合、死亡又は休業４日以上の労働災害については、

遅滞なく、様式第２３号による報告書の提出が求められている（労働安全衛生法施行規則第９７条第１項)。

また、休業１日から３日の労働災害については、１月から３月まで、４月から６月まで、７月から９月まで及び１０月から１２月までの期間における当該事実について、様式第２４号による報告書をそれぞれの期間における最後の月の翌月末日までに提出しなければならない（同条第２項)。

なお、事業所における労働災害は、交通事故や躓きなど、事業所の安全管理とは希薄と考えられるものも発生しうることから、事業所の安全管理とは希薄と考えられる労働災害は②には含まないとする。

また、更新時に審査を簡略化できる事業所は特に優れた保安体制を有する事業所であることが適当であり、事業所全体の保安力を適切に評価する観点からは、高圧ガス製造施設以外で発生した労働災害も対象とする。

この高圧ガス製造施設以外の範囲については、例えば、危険物等を取り扱う製造プラントなどの区域内であり、計器室でない事務所や構内道路等製造現場に直接的に関係がないものを除くといった範囲などとなるが、今後の運用においては具体的な事業所の区域を踏まえつつ、その範囲を明確にする必要がある。

2.4.2.2 法令違反について

①違反の対象となる法令

原則として認定要件として求められる法適合確認能力は高圧ガス保安法に対しての確認能力であり、法令違反の対象としては、高圧ガス保安法 とする。

それ以外の法令は対象外とするが、2.4.3.1 のとおり、石災法の事故や、労安法上の労働災害の発生の有無が簡略化の条件に含まれていることから、他法令については単に法令違反を対象とするのではなく、事故等の結果を条件とすることで考慮することとしている。

②法令違反の件数等

高圧ガス製造施設において、以下の法令違反を起こした場合は、簡略化の対象外とする。

・公表された高圧法令違反：更新期間中に１件以上
・高圧法令違反（軽微なものも含む)：更新期間中に２件以上

【参考】法令違反の公表基準

① 死亡事故が発生したもの
② １００件を超えるような多数の法令違反を伴うもの（※１）
③ 国の行政処分（※２）が行われているもの
④ 国の行政文書による注意等が行われているもの

（※１）累積ではなく、一度の行政処分で対象とする法令違反件数
（※２）当該事案についての最終的な措置としての行政処分（認定取消し等）を指す。途中段階での行政処分（報告徴収や立入検査等）は含まない。

2.4.2.3 大幅な変更の内容

高圧ガス製造施設の追加があった場合にあっては、簡略化の対象外とする。

＊重要な工事又はガス種の変更があった場合を簡略化の対象外とするという考え方もあるが、事業所の適切な変更管理や法適合確認によって、その他の条件をクリアしているのであれば、単に重要な工事等があったことだけをもって簡略化の対象外とする必要性はないと考えられる。

一方で、製造施設の追加し、認定施設に追加する場合にあっては、管理体制も含めて新規申請と同様に審査を行う必要がある。

2.4.3 審査基準案の作成について

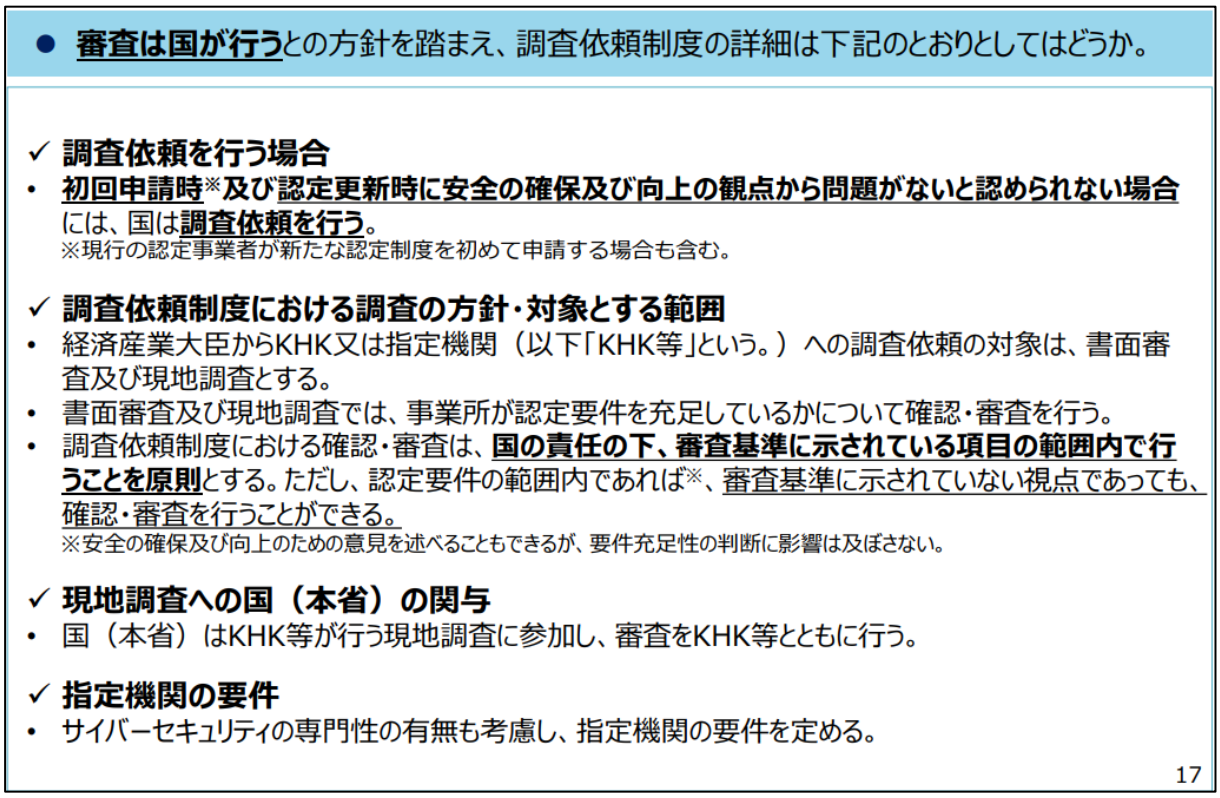
新たな認定制度における合理的かつ迅速な認定審査を行うため必要な審査基準について、現行の認定制度において、KHKが行っている事前調査で使用している調査用紙の審査基準（KHK作成）を元に、新たな認定要件を踏まえて、審査基準案を作成する。

審査基準案作成にあたっては、国による確認・審査が審査基準に示されている項目の範囲内で行われることを前提とし、審査基準の透明化のため、これを公開することとして作成する。

なお、事前調査で使用している調査用紙については、現行の事前調査で行っている評価結果ランク付けのため審査基準が規定されているが、評価ランク付けについては新たな認定制度においては廃止されることから、評価結果ランク付けのために規定されている審査基準については原則として削除する。

2.4.4　検討結果

2.4.1～2.4.3 の検討を踏まえ、次のとおり高圧ガス小委員会の資料として、新たな認定制度の審査方法等の案がまとめられた（図１４、図１５、図１６、図１７、図１８）。



● **審査は国が行う**との方針を踏まえ、調査依頼制度の詳細は下記のとおりとしてはどうか。

✓ **調査依頼を行う場合**

- **初回申請時※及び認定更新時に安全の確保及び向上の観点から問題がないと認められない場合**には、国は**調査依頼を行う**。
  ※現行の認定事業者が新たな認定制度を初めて申請する場合も含む。

✓ **調査依頼制度における調査の方針・対象とする範囲**

- 経済産業大臣からKHK又は指定機関（以下「KHK等」という。）への調査依頼の対象は、書面審査及び現地調査とする。
- 書面審査及び現地調査では、事業所が認定要件を充足しているかについて確認・審査を行う。
- 調査依頼制度における確認・審査は、**国の責任の下、審査基準に示されている項目の範囲内で行うことを原則**とする。ただし、認定要件の範囲内であれば※、審査基準に示されていない視点であっても、確認・審査を行うことができる。
  ※安全の確保及び向上のための意見を述べることもできるが、要件充足性の判断に影響は及ぼさない。

✓ **現地調査への国（本省）の関与**

- 国（本省）はKHK等が行う現地調査に参加し、審査をKHK等とともに行う。

✓ **指定機関の要件**

- サイバーセキュリティの専門性の有無も考慮し、指定機関の要件を定める。

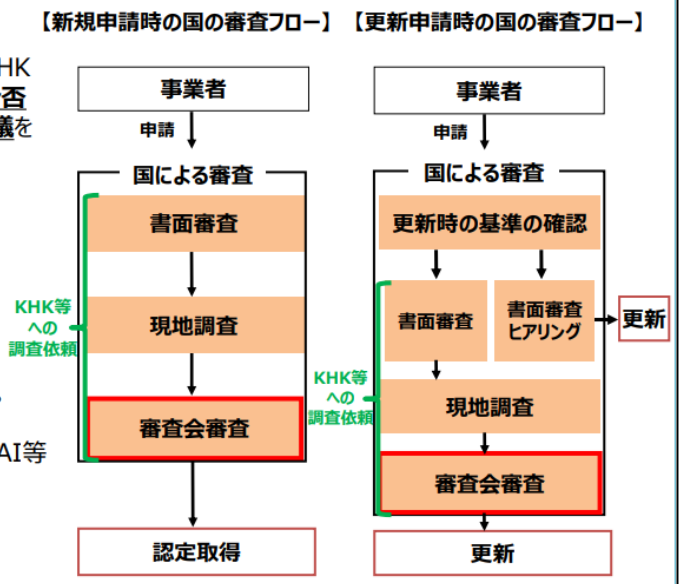
17

図 14.　高圧ガス委員会資料②（抜粋）

● 審査会審査の審査方法及び委員構成は、下記のとおりとしてはどうか。

✓ 審査会審査の審査方法

- ４半期に一度開催する。
- 国及び調査依頼制度に参加する専門機関（KHK等）から**書面審査と現地調査の審査結果（合否等）を報告**する。その後、**審査結果について審議**を行う。
- 申請者（事業者）は不参加とする。
- **議事要旨は公開**※する。
  ※企業の機微情報を除いた上で作成。



✓ 審査会審査の委員構成

- **委員**

以下の分野の**外部有識者１０名程度で構成**する。
【外部有識者の主な分野】
✓ 学識経験者（高圧ガス、安全工学、IoT･BD/AI等のテクノロジー、サイバーセキュリティ）
✓ 企業法務（コンプライアンス）
✓ 企業ＯＢ等（実務経験者）
✓ 高圧ガス保安協会（ＫＨＫ） 等

- **オブザーバー**

✓ 申請事業所を管轄する地方自治体

18

図 15. 高圧ガス委員会資料②（抜粋）

● **新たな認定制度**においては、**国による書面審査･ヒアリングにより認定の更新を認める制度を新たに導入**する。

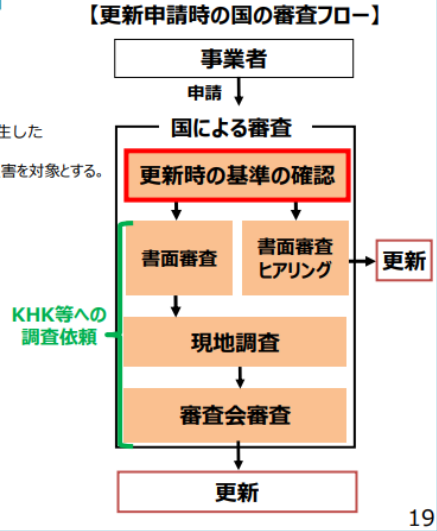
● その際、５年間（A認定の場合は７年間）の認定期間内に、**以下①～③の基準のいずれかに該当することとなった場合は、安全の確保及び向上の観点から問題がないと認められないと判断**し、現地調査及び審査会審査を行う。

更新時に現地調査･審査会審査を実施する場合の基準（案）

①事故や労働災害の有無
✓ **Ｂ２級**※１**以上の事故が発生**している事業所
✓ **死亡又は休業４日以上の労働災害**※２**が発生**している事業所
※１ 同一事業所において、Ａ級事故、Ｂ級事故又はＣ１級事故が発生した日から１年を経過しない間に発生したＣ１級事故（高圧ガスに係る事故に限る。）（「高圧ガス・石油コンビナート事故対応要領」３(2)）
※２ 従業員･協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

②法令違反の有無
✓ 高圧ガス保安法の法令違反が**２回**※３**以上**発生している事業所
（ただし以下の法令違反については**１回**）
① 死亡事故が発生したもの
② １００件を超えるような多数の法令違反を伴うもの
③ 国の行政処分が行われているもの
④ 国の行政文書による注意等が行われているもの
※３ 原則として、事業者からの報告数をカウントする。

③大幅な設備変更の有無
✓ **認定の対象に新たに高圧ガス製造施設を追加**する事業所※４
※４ 既存の認定施設において設備の変更工事が行われた場合、ガス種の変更等が行われた場合は含まない。



19

図 16. 高圧ガス委員会資料②（抜粋）

3-1.新たな認定制度の審査体制（高圧ガス小委員会での御指摘を踏まえた更新時の基準の変更点）

２月24日の事務局案における新たな認定制度の更新時に現地調査・審査会審査を実施する場合の基準の整理

- **新たな認定制度**においては、**国による書面審査・ヒアリングにより認定の更新を認める制度を新たに導入**する。
- ２月24日の事務局案では、労働災害は「**死亡又は休業４日以上の労働災害※が発生**している事業所」とすることを提示。

※ 従業員・協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

高圧ガス小委における御指摘事項

① 休業４日以上の労働災害には、**高齢者の腰痛、躓き、転倒等も含まれており**、こうした労災まで考慮すると、**高圧ガス製造施設の保安の維持・確保という制度趣旨から乖離**が生じる。
② **「休業４日以上の労働災害」の発生という基準は、範囲が広すぎる**。代替案として、重大労働災害の発生、としてはどうか。
③ 休業４日以上の労働災害は「プラント内（高圧ガス製造施設以外も含む）」で発生したものを対象としており、**高圧ガス製造設備以外の労働災害も考慮している点で厳しい**基準。重大事故を防止する観点から、災害等級・障害等級・強度率等の、より実態に即した基準の導入を検討いただきたい。

２月24日の事務局案の考え方

①新たな認定制度においては、合理的かつ迅速な認定審査へ移行しつつ、**安全確保を大前提に、認定審査を厳正に行う必要**がある。
②更新時の基準は、現地調査・審査会審査を省略する場合の基準であり、**認定更新が認められなくなるものではない**。
③分科会報告書において、認定更新時には、新規認定以降の事故の発生状況や法令違反（労安法等を含む）の有無等を踏まえることとしており、**労安法も考慮対象**の一つとしている。

御指摘を踏まえた修正案

- 労働安全衛生法において、**休業４日以上の労働災害**は、**遅滞ない報告が求められている**※1ほか、**ボイラー等の開放検査周期に係る認定制度の認定要件においても考慮**※2されている。また、更新時に現地調査・審査会審査が省略されるのは、特に優れた保安体制を備えた事業所のみを対象とすることが適切であるところ、**事業所全体の保安力を適切に評価する観点**からは、**高圧ガス製造施設以外で発生した労働災害も対象とすることが適切**。
- なお、高圧ガス小委員会での御指摘を踏まえて、交通事故や腰痛、躓き等の**事業所の安全管理と関係が希薄なものは除外することとしてはどうか。**

※1 労働安全衛生法第100条第1項、労働安全衛生規則第97条第1項
※2 「ボイラー等の開放検査周期に係る認定制度について」

7

図 17. 高圧ガス委員会資料③（抜粋）

3-2. 新たな認定制度の審査体制（審査基準の作成・公開）

- 認定審査の透明性を確保する観点から、すべての認定要件について、認定審査時の**評価の視点**と**確認する書類の例**を明らかにした**審査基準を作成し公開**する。
- 審査基準は、今後、関係者の意見を参考に、国が作成する。

審査基準のイメージ

認定の基準	確認する書類	評価の視点
● 法人の代表者によって、保安の確保に関する理念、基本方針等の諸施策が明確に定められ、かつ、文書化されていること。また、これらの諸施策が各事業所等の全ての就業者に理解され、実施され、かつ、維持されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 経営理念が記載されたもの ✓ 基本方針が記載されたもの ✓ 社員へイントラネット、カード等により配信・配布している又は社内掲示しているもの ✓ 保安に係る諸施策についての、経営層と現場従業員との対話やアンケート等の実績	● 法人の代表者によって、経営理念、基本方針が系統立って作成されており、本社の姿勢、保安活動への経営者のコミットメントが示されている。 ● 全ての就業者が経営理念等を理解できるような取り組みを行っている。
● 役員を長とする保安対策本部等が設置されており、保安管理の基本方針の決定、各事業所ごとの保安管理実績の検討等の実施について明確に定められ、文書化され、かつ、適切に実施されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 本部等の設置規程等 ✓ 保安管理の基本方針の決定及び各事業所ごとの保安管理実績の検討等が分かるもの	● 保安対策本部等が設置されており、組織、メンバー構成、設置目的等を示す規程・基準類が整備されている。 ● 取締役（指名委員会等設置会社においては執行役）が長となっている。 ● 保安対策本部等において、保安活動を定期的に計画し、その実績を評価している。
● 保安管理部門が設置されており、生産計画、設備管理計画等に当該部門の意見が十分に反映されることが、明確に定められ、文書化され、かつ、意見が十分反映されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 職務分掌規程等 ✓ 安全環境計画、生産計画及び設備管理計画等に保安管理部門の意見が反映されていることを示す会議議事録 ✓ 保安管理部門から社内外の保安関連情報（重大事故情報を含む）を展開し、それを踏まえて対応を行ったことを示すもの	● 保安管理部門が設置されている。 ● 安全環境計画、生産計画及び設備管理計画に保安管理部門の意見が反映されている。

9

図 18. 高圧ガス委員会資料③（抜粋）

2.5　改正高圧法を踏まえ改正が必要となる下位法令の抽出等

改正高圧法を踏まえ改正が必要となる下位法令の抽出に関連する事項について検討を行った。

2.5.1　認定取り消し後の保安検査期間等の猶予について

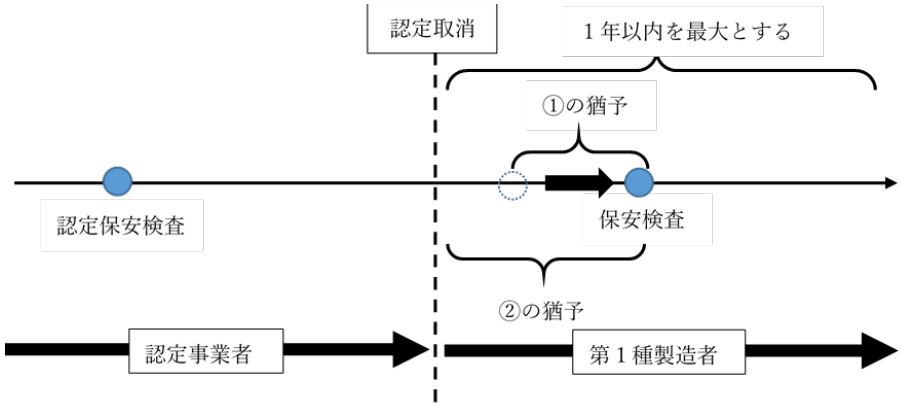
認定取り消し後の保安検査期間等の猶予については、プラント等により状況が異なるため一律に定めるのは難しいが、猶予期間を設けること考えた場合、認定取り消し後の違法状態を解消するには、以下の２つの猶予が必要となる。

①保安検査全体の実施期間の猶予

②認定によって認められている保安検査方法の有効期間の猶予

なお、虚偽の認定保安検査記録を作成した場合にあっては、過去の検査記録の信用性が失われており設備の健全性が確認できないことから、①及び②の猶予については認めない。

また、現行制度においても同様の規定を設ける。



2.5.1.2　保安検査全体の実施期間の猶予について

認定を取り消された日から最大１年以内を猶予することとする（期間としては最大で２年間空くことになる）。ただし、１年以内の猶予の中で、可能な限り速やかに検査を行う必要があることから、保安検査実施者となる都道府県等にその理由を添えて、検査計画を提出した場合のみ猶予を認める。１年以内に実施できないのであれば、休止届を提出するなどの対応が必要となる。

（規定ぶりのイメージ）

第一種製造者が法第三十九条の十二第一項又は法第三十九条の二十第一項の規定により認定を取り消された場合において、その第一種製造者が、次に掲げる事項を記載した書面を都道府県又は指定都市の長に提出したときは、その認定を取り消された日から１年以内の期間を限り、都道府県又は指定都市の長は、法第三十五条第一項の保安検査を猶予することができる。

一　猶予を必要とする理由

二　保安検査を速やかに行うための検査計画

前項の規定は、法第三十九条の十第三項、法第三十九条の十一第二項及び法第三十九条の二十七第一項の検査記録を作成せず、虚偽の検査記録を作成した場合においては、適用しない。

2.5.1.3　認定によって認められている保安検査方法の有効期間の猶予

認定によって認められている保安検査方法（開放検査周期の延長など）が認定の取り消し後、無効となることから、その保安検査方法の特例を猶予する必要がある。当該保安検査方法の猶予については、①と同様に最大１年以内の猶予の中で、可能な限り速やかに検査を行う必要があることから、保安検査実施者となる都道府県等にその理由を添えて、検査計画を提出した場合のみ猶予を認める。1 年以内に実施できないのであれば、休止届を提出するなどの対応が必要となる。

（規定ぶりのイメージ）

第一種製造者が法第三十九条の十二第一項又は法第三十九条の二十第一項の規定により認定を取り消された場合において、その第一種製造者が、次に掲げる事項を記載した書面を都道府県又は指定都市の長に提出し、前〇号の保安検査の方法を用いる場合（その認定を取り消された日から１年以内の期間に限る）。

イ　第二項で定める告示以外の保安検査の方法を用いる理由
ロ　保安検査を速やかに行うための検査計画
前号の規定は、法第三十九条の十第三項、法第三十九条の十一第二項及び法第三十九条の二十七第一項の検査記録を作成せず、虚偽の検査記録を作成した場合においては、適用しない。

＊前〇号とは、以下の現行制度の規定を及び新制度の条項指す。（以下コンビ則第３７条の場合）
（保安検査の方法）
第三十七条　法第三十五条第四項の経済産業省令で定める保安検査の方法は、開放検査、分解検査その他の各部の損傷、変形及び異常の発生状況を確認するために十分な方法並びに作動検査その他の機能及び作動の状況を確認するために十分な方法でなければならない。
２　前項の保安検査の方法は告示で定める。ただし、次の各号に掲げる場合はこの限りでない。
一　認定保安検査実施者が、法第三十五条第一項第二号の認定に係る特定施設について行う保安検査の方法であつて、同号の認定に当たり経済産業大臣が認めたものを用いる場合。
二　特定認定事業者が、令第十条ただし書の認定に係る特定施設について行う保安検査の方法であつて、次のいずれにも該当するものを用いる場合。
イ　製造設備の寿命等を勘案して、適切な時期に、肉厚測定検査及び開放検査を行う方法
ロ　少なくとも八年に一回は運転を停止した検査を行う方法
ハ　保安検査に係る責任者が前項に定める方法に適合すると認めた方法
以下　（略）

2.5.2　記録保存の方法について

新認定制度においては、事業者の記録保存の義務を課し、届出が不要となる規制の特例が措置される予定であることから、記録保存の方法について検討を行った。なお、検討に当たっては、今後、記録が電磁的に保存され、クラウドサービスを用いることや、設備管理システムなどシステム上に記録保存されることが、主流となっていくことも考慮した。

2.5.2.1　電磁的方法による記録保存対象の拡大

電磁的方法による記録保存は省令上（例：コンビ則第 38 条の２）においては、法第３５条の２の定期自主検査記録に限って規定していることから、今回の法改正により届出が不要になる記録は、電子的な保存を認めるよう対象を拡大する改正を行う必要がある。

2.5.2.2　クラウドの利用を前提とした「電磁的方法による保存等をする場合に確保するよう努めなければならない基準について」の改正の検討

複数の法令（例：国家戦略特別区域法、地方公共団体情報システム機構法）で、官民データ活用推進基本法における「クラウド・コンピューティング・サービス関連技術」の定義が引用されている。高圧ガス保安法関係法令等においても同様に当該定義を引用し、クラウド技術を利用する場合には、高圧ガス保安法で求める記録保存義務はサービス事業者の管理によることとする旨を明記すればよいのではないか。

（参考）官民データ活用推進基本法（平成二十八年法律第百三号）
第二条　１～３　（略）
４　この法律において「クラウド・コンピューティング・サービス関連技術」とは、インターネットその他の高度情報通信ネットワークを通じて電子計算機（入出力装置を含む。以下同じ。）を他人の情報処理の用に供するサービスに関する技術をいう。

具体的には、電磁保存告示に以下のような改正を加える。
①１　別表第２に掲げる保存等をする場合には、それぞれ別表第１に掲げる基準を確保するよう努めなければならない。「ただし、クラウド・コンピューティング・サービス関連技術に利用して保存等をする場合にあっては、クラウド・コンピューティング・サービス関連技術を提供する運用管理者における管理により基準を確保することができる。」
＊「」部分を追加
②用語の定義に、「クラウド・コンピューティング・サービス関連技術」を追加

なお、電磁保存告示において、記録の保存義務が課せられている事業者でなく、クラウドの運用

管理者において管理されていると考えらえる項目は、別添の黄色マーカー部の基準を参照

2.5.2.3　記録保存が適切に実施できているかの確認方法

記録保存については、例えば以下のような確認を行うことが必要であると考えられる。

・紙又は電磁的保存か
・記録の修正などの履歴管理はどのように行われているか。
・記録の作成における誤り、改ざん等を防止する措置は行われているか。

記録するべき事項については以下のとおり、

①完成検査・保安検査

現行のコンビ則第 48 条で規定する検査記録の項目と同様の事項が保存されていることを確認する。

(参考)

コンビナート等保安規則

第四十八条　法第三十九条の十第二項の経済産業省令で定める事項は、次の各号に掲げるものとする。

一　検査年月日
二　検査に係る責任者の氏名
三　検査をした特定変更工事の内容
四　特定変更工事の設備ごとの検査の方法、記録及びその結果の詳細

2　法第三十九条の十第三項で準用する同条第二項の経済産業省令で定める事項は、次の各号に掲げるものとする。

一　検査年月日
二　検査に係る責任者の氏名
三　検査をした特定施設
四　保安検査を行つた特定施設の設備ごとの検査の方法、記録及びその結果の詳細

②危害予防規程

改正保安法第 39 条の 23 に記載のとおり、危害予防規程が保存されていることを確認すればよいと考える。なお、危害予防規程が改正された場合には現行は届出が必要であることから、その改正履歴も確認する。

(参考)

高圧ガス保安法（令和四年法律第七十四号公布の日から一年六月を超えない範囲内において政令で定める日に施行予定の改正版）

第三十九条の二十三　認定高度保安実施者は、危害予防規程を定め、又は変更したときは、第二十六条第一項の規定にかかわらず、同項の規定による届出を要しない。この場合においては、経済産業省令で定めるところにより、当該危害予防規程を保存し、都道府県知事から提出を求められたときは、速やかにこれを提出しなければならない。

③保安人員の選解任（第 39 条の 24～26）

改正保安法第 39 条の 24～26 に記載のとおり、保安人員の選任又は解任に係る記録が保存されていることを確認すればよいと考える。

具体的には、先解任の履歴管理状況、資格者、経験を満たしている者が選任されていることを確認する。

(参考）高圧ガス保安法（令和四年法律第七十四号公布の日から一年六月を超えない範囲内において政令で定める日に施行予定の改正版）

第三十九条の二十四

1 （略）

2　認定高度保安実施者は、第二十七条の二第一項、第三項若しくは第四項の規定による保安統括者、保安技術管理者若しくは保安係員の選任又はその解任については、同条第五項又は

第六項の規定にかかわらず、これらの規定による届出を要しない。この場合においては、経済産業省令で定めるところにより、当該選任又は解任に係る記録を作成し、これを保存しなければならない。

2.5.3　電磁的記録保存の方法についての再検討

電磁的記録保存について、クラウドサービスを用いた場合に電磁保存告示の改正の要否について再度検討した。検討の際には、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（経済産業省）等を参考とした。
また、併せて書面保存則の改正の必要性について検討した。

2.5.3.1　クラウドの利用を前提とした「電磁的方法による保存等をする場合に確保するよう努めなければならない基準について」（電磁保存告示）の改正の検討

①ガイドラインにおける対応策と電磁保存告示の対応関係

ガイドラインにおける対応策は、以下に分類されるため、電磁保存告示との対応関係を調査し、色分けを行った。【別添３、別添４】

【電磁保存告示の対応策が、ガイドライン中のどの分類に該当するか】

A）クラウド利用者のための実施の手引（事業者が行う対応）
→水色マーカー
B）クラウド事業者の実施が望まれる事項（クラウドサービスの提供者が行う対応）
→黄色マーカー
A）と B）の両方が該当
→緑色マーカー
C)ガイドライン中の「管理策」に該当
→橙色マーカー

【ガイドラインの対応策が電磁保存告示に規定されているか】

D) ガイドラインの対応策のうち電磁保存告示に規定されているもの
→赤色マーカー

＊それぞれ、記載内容が異なるため、必ずしも対応関係が明確とならないことに留意

上記を参照し、クラウド利用者が対応するもの、クラウド事業者が対応するものに分割し、ガイドラインでの対応策に記載内容に準じた形で、クラウドを利用する際の基準とする場合の改正案を検討した。【別添５】

2.5.3.2　クラウドの利用を前提とした「経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則」（書面保存則）の改正の検討

①書面保存則上に規定されている高圧ガス保安法関連の記録類
・認定事業者の認定完成検査記録(法第 39 条の 10 第 2 項)
認定保安検査記録（同条第 3 項）
・第 1 種製造者等の帳簿（法第 60 条)
②書面保存則上で①の記録に適用される保存方法等の規定
・保存の方法
・電磁保存告示に定める基準の確保
・作成の方法
＊他法令は上記の他、縦覧等、交付等に関する規定が適用されているものある。
③改正の要否

書面保存則上の規定では、②で規定する方法等については、「民間事業者等の使用に係る電子計算機に備えられたファイル又は磁気ディスク、シー・ディー・ロムその他これらに準ずる方法」とされている。

法令上の解釈にもよるが、電子計算機の場所を限定しておらず、記録媒体もその他これらに準ずる方法と規定されていることから、クラウドサービスもこれに含まれているとすれば、特に改正は不要と考える。【別添６】

なお、参考として、他省庁が所管する書面保存則の状況を見ると、書面保存則上は特にクラウドについて明記していないが、書面保存則を補完するガイドラインにおいてクラウド利用の際の対応が記載されている。

（厚生労働省関係）
・医療情報システムの安全管理に関するガイドライン
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
（国土交通省関係）
・建築設計業務における設計図書の電磁的記録による作成と保存のガイドライン
https://www.jiima.or.jp/pdf/kenchiku_denshika_vol1_201712.pdf

2.5.4　製造施設ごとの認定申請、記録類等に関する規定について

製造施設ごとの認定、記録保存義務が課せられている記録保存の方法等について検討を行った。

2.5.4.1　コンビ則 40 条 2 項・47 条・49 条の 6 の規定の要否

初期設置の施設等を特例の対象から除外する規定の措置

初期設置の施設等を特例の対象から除外する規定の措置等について、完成検査と保安検査の申請区別がなくなったことに留意し、以下の規定を追加する。

【コンビ則第 40 条第 2 項の改正案】

1　（略）
2　前項の申請は、法第三十九の十二の認定に係る製造施設を明らかにして行わなければならない。
3　前項の製造施設は、継続して二年以上高圧ガスを製造しているものとする。

＊継続して 2 年以上の高圧ガスを製造している施設に限定しているため、製造施設の追加があった場合は、特例の対象外となることから、現行規定の特定変更工事に対する制限は不要。

【コンビ則第 47 条の改正案】

認定高度保安実施者が、製造施設を追加するために第四十条第一項の申請を行う場合にあつては、第四十条、第四十一条及び第四十四条第一項から第三項までの規定を準用する。ただし、第四十条第一項又は第四十四条第一項に掲げる認定申請書に添えなければならない書類のうち、施設の追加により内容の変更を及ぼすことのない書類の添付を省略することができる。

【コンビ則第 49 条の 6 改正案】

特定認定高度保安事業者が、製造施設を追加するために第四十条第一項の申請を行う場合にあつては、第四十九条の二及び第四十九条の三の規定を準用する。ただし、第四十九条の二第二項又は同条第三項に掲げる第四十九条の三の認定の基準に適合していることを説明する書類のうち、施設の追加により内容の変更を及ぼすことのない書類の添付を省略することができる。

＊現行規定は、スーパー認定は通常認定に要件を上乗せする規定となっているが、A 認定では、B 認定の要件を包含する A 認定全ての規定を満足するとした場合の規定ぶりとなっている。

2.5.4.2　記録保存とする記録に記載する項目の規定

改正高圧法 39 条の 21 第 2 項、第 3 項に規定される記録保存について、コンビ則 38 条第 5 項、48 条等を参照して、「工事に係る記録」（法 39 条の 21 第 2 項）「製造の方法の変更に係る記録」（第 3 項）に記載する項目を省令で規定することについて検討を行った。

【改正高圧法 39 条の 21 第 2 項の「工事に係る記録」に係る省令改正案】

一　製造施設の名称、変更工事の目的及び変更工事の内容
二　法第八条第一号の経済産業省令で定める技術上の基準への適合に関する事項
　＊変更後も技術上の基準に適合していることを確認できる資料という趣旨

【改正高圧法 39 条の 21 第 3 項の「製造の方法の変更に係る記録」の省令改正案】

一　製造施設の名称、製造の方法の変更の目的及び変更の内容
二　法第八第二号の経済産業省令で定める技術上の基準への適合に関する事項
　＊変更後も技術上の基準に適合していることを確認できる資料という趣旨

上記の記録類については、記録保存状況を立ち入り等で確認する際に最低限必要な書類として、変更工事等の内容等及びその変更工事等が技術基準に適合していることを確認するための書類と

している。

2.5.4.3　完成検査の方法等について

完成検査の方法等について、完成検査の方法の特例、完成検査記録の項目に関する規定について検討を行った。

【改正高圧法 39 条の 22 第 1 項の「完成検査の方法」】

完成検査の方法にあっては、設備設置や変更時として設備を停止した状態で行うものであり、別表 3 と同じ方法として、特に問題ないものと考えられる。なお、これまでの申請において完成検査の変更の特例については、特にニーズがないことに加え、設置時等には検査を確実に行っておく必要があることから、現在のところ完成検査に関する特例は不要とする。

【改正高圧法 39 条の 22 第 2 項の「完成検査の記録」】

完成検査の記録に関しては、新認定制度において、完成検査の方法等に変更がないことから、コンビ則 48 条第 1 項と同じ以下の記録保存を求める。

一　検査年月日
二　検査に係る責任者の氏名
三　検査をした特定変更工事の内容
四　特定変更工事の設備ごとの検査の方法、記録及びその結果の詳細

なお、保安検査についても同様にコンビ則 48 条第 2 項と同様の記録保存を求める。

一　検査年月日
二　検査に係る責任者の氏名
三　検査をした特定施設
四　保安検査を行つた特定施設の設備ごとの検査の方法、記録及びその結果の詳細

2.5.4.4　危害予防規程の制改正の記録する項目の規定

改正高圧法第 39 条の 23 に記載のとおり、危害予防規程が保存されていることを確認すればよいと考える。なお、危害予防規程の制改定された場合には現行は届出が必要であることから、危害予防規程に記載されている改正履歴も確認を行えるよう危害予防規程の保存を求める。

2.5.4.5　保安人員の選解任に係る記録に記載する項目の規定

保安人員の選任又は解任に係る記録に記載する項目を省令で規定することについて、具体的に記録すべき内容について検討を行った。

【保安人員の選任又は解任に係る記録】

立ち入り等において適切に選任又は解任がされていることを確認するため、以下の記録保存を求める。

一　選任した者の製造保安責任者免状の写し
二　高圧ガスの製造に関する経験に事項
三　保安管理組織図の変更履歴

2.5.4.6　A 認定と B 認定をまとめて申請することを可とする規定を措置保安検査の時期について

A 認定と B 認定を選択した際に、仮に A 認定に関する認定要件のみが不適だった場合に、B 認定も取得できなくならないようにしてほしいとの事業者から要望があったところを踏まえ、A 認定と B 認定の関係と認定に関する見なし規定について検討した。

コンビ則 49 条の 2 第 1 項の規定は、現行制度において、通常は法律が根拠、スーパー認定はその上乗せとして、政令が根拠となり、別の申請を同時に行うこととなっている。新たな認定制度においては、A、B 認定ともに改正高圧法第 39 条の 13 が根拠条項であるが、A 認定が上乗せであり、B 認定と同時に申請を行うのか、申請は 1 つで、A、B にルートが分かれるのかについて、省令以下の規定の仕方によって、このみなし規定の要否と方法が異なる。

つまり、前者の場合、A 認定が上乗せ規定としての A 認定制度とすると、A 認定及び B 認定を同時に申請した際に、仮に A 認定だけ不適合となった場合であっても B 認定は別の申請であるた

め、申請かんする見なし規定は不要となる。
後者の場合は、A 認定と B 認定がはじめから申請ルートが分かれているため、A 認定を申請して、仮に A 認定が不適合となった場合にあっては、B 認定の申請がなされていないため、その際に B 認定に対する見なし規定が必要となる。

【参考】
（政令改正案）
第十条の二　法第三十九条の十七第一項の政令で定める期間は、五年とする。ただし、法第三十九条第十三の認定を申請した者が、保安の確保に係る高度な方法を用い、かつ、当該方法を用いるために必要な経済産業省令で定める技術的能力及び実施体制を有すると経済産業大臣が認める場合は、七年とする。

2.6　立入検査
立入検査については、適時・適切な立入検査を行うとされているところであるが、現状の認定事業者に対しては、認定更新期間中の中間年を目途に国による中間立入検査が行われている。
この中間立入検査については、新たな認定制度でも引き続き行いつつ、重大な法令違反や事故等が発生した場合にあっては、個別事案の状況を勘案した上で、中間立入検査とは別に立入検査を行うことも重要である。
その際には、所管の地方自治体とも引き続き連携・協力して、適切な立入検査を行うこととする。

2.7　検討結果（検討中の項目を含む。）を踏まえた自治体への説明と意見交換
新認定制度の検討にあたり、アンケート調査及びヒアリングを実施した自治体に対して、新たな認定制度の創設に向けた検討状況を説明し、意見交換を行うため、第 24 回高圧ガス小委員会（令和５年２月２４日）後に、各自治体を訪問し説明及び意見交換を行った。

① 自治体への説明資料
- **本日意見交換させていただきたい事項（別添 7）**
- **高圧ガス保安法における新たな認定制度の詳細設計について（第 23・24 回 産業構造審議会 保安・消費生活用製品安全分科会高圧ガス小委員会 資料抜粋）（別添 8）**
- **軽微な変更工事の範囲の拡大について（別添 9）**
- **新認定制度における許認可手続き（イメージ）（別添 10）**

② 自治体への説明と意見聴取の方法
アンケート調査及びヒアリングを実施した自治体を訪問し、説明資料により高圧ガス保安室及び KHK が説明し、自治体担当者から意見を聴取した。

③ 自治体への説明と意見聴取の結果
自治体との意見交換とりまとめ（別添 11）のとおり

3.まとめ
高圧ガス保安法等の一部を改正する法律案が第 208 回通常国会に提出され、国会での審議を経て可決された。公布（令和４年６月２２日）された後の１年６ヶ月以内施行に向けて、新たな認定制度の詳細設計を行った。
具体的には、第 22 回の高圧ガス小委員会で示された以下のコンセプトに基づいて、経済産業省高圧ガス保安室と緊密な連携を取りつつ、認定要件、規制特例、審査体制等についての検討を行った。

・新認定制度の保安レベルの持続的向上や保安人材の枯渇問題の解消のため、テクノロジーを活用したスマート保安を推進する。
・厳正な認定審査のもと、テクノロジーを活用しつつ自立的に高度な保安を確保できると認められた事業者については、安全確保を大前提に、事業者の保安力に応じた規制体系へ移行するとともに、手続・検査の在り方をこれに見合った形に見直す。これにより、事業者・規制当局（国・自治体）のリソースを実質的な保安活動に配分することを可能とする。
・上記により、国全体の高圧ガス分野の保安力向上（重大・悪質な法令違反、重大事故の削減）

を目指す。

新たな認定制度におけるコンセプトについては、国会審議における附帯決議にも述べられているが、この制度の運用に当たっては、安全の確保を大前提とすること、認定審査を厳正に行うことが盛り込まれていることから、特にこれらの点について留意して検討を行った。

今後、政省令以下の公布・施行に向けた条文等の詳細について引き続き検討を行う必要がある。また、制度の運用開始に向けて、事業者・自治体に対して丁寧な説明を行い、新たな認定制度への円滑な移行を推進していくことも重要である。

添付資料一覧

１．自治体及び事業者向けアンケート及びヒアリング関係
・事業者向け
別添１　アンケート調査表（事業所）
・自治体向け
別添２　アンケート調査表（自治体）

２．電磁保存告示の改正関係
別添３　電磁的方法による保存等をする場合に確保するよう努めなければならない基準
別添４　クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013）
別添５　電磁保存告示　改正案
別添６　経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則

３．自治体への説明・意見交換関係
別添７　本日意見交換させていただきたい事項
別添８　高圧ガス保安法における新たな認定制度の詳細設計について（第 23・24 回 産業構造審議会 保安・消費生活用製品安全分科会高圧ガス小委員会 資料抜粋）
別添９　軽微な変更工事の範囲の拡大について
別添１０　新認定制度における許認可手続き（イメージ）
別添１１　自治体との意見交換とりまとめ

４．高圧ガス小委員会関係
別添１２　高圧ガス保安法における新たな認定制度の詳細設計について
（2022 年 12 月 15 日開催第 23 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会　資料２）
別添１３　高圧ガス保安法における新たな認定制度の詳細設計について②
（2023 年 2 月 24 日開催第 24 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会　資料１）
別添１４　高圧ガス保安法における新たな認定制度の詳細設計について③
（2023 年 3 月 24 日開催第 25 回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会　資料３）

別添１

新認定制度の設計に関するアンケート

Ⅰ　本社又は事業所の概要

1. 会社名：

2. 本社又は事業所名：

＊本社の場合は、「本社」とご記入ください。

3. 所在地：

4. 本件ご担当者様（ご回答後、ご連絡させていただく場合がございます。）

氏名：
部署：
役職：
E-Mail アドレス：
TEL：

5. 業種

a. 石油精製　b. 石油化学　c. 一般化学
d. その他（具体的にご記入ください）

回答欄	

6. 高圧ガス保安法適用規則

a. コンビナート等保安規則
b. 一般高圧ガス保安規則
c. その他（具体的にご記入ください。）

回答欄	

＜用語の説明＞

・改正法：高圧ガス保安法等の一部を改正する法律（令和 4 年法律第 74 号）による改正後の高圧ガス保安法

・法　　：高圧ガス保安法

Ⅱ　認定要件について

【質問 1】

① 本社の機関設計について、監査役会等会社、監査等委員会設置会社、指名委員会等設置会社のいずれかを採用していますか（自社が監査役会等会社、監査等委員会設置会社、指名委員会等設置会社でない場合でも、親会社がこれらの機関設計をとっている場合には、その旨を記載ください）。

② 上記のいずれも設置していない場合は、その理由と貴社で採用している機関設計を教えてください。また、監査役会設置会社、監査等委員会設置会社、指名委員会等設置会社とすることについての障壁があれば教えてください。

③ 上記機関設計以外で、コーポレート・ガバナンスについて、第三者的な視点で確認が行われる体制（監査役会の設置はないが、社会監査役を設置している等）を有している場合は、具体的な体制を教えてください。

【回答 1】	
①	
②	
③	

【質問 2】　（【質問 1】の①又は③記載の体制を有している場合のみ回答をお願いいたします。）

貴社において、監査役会・各監査役・監査委員会・三委員会の委員などの監督機関が保安に対してどのような監督を行っているか教えてください。（自社が監査役会等会社、監査等委員会設置会社、指名委員会等設置会社でなく、親会社がこれらの機関設計をとっている場合には、親会社のこれらの機関が保安に対してどのような監督を行っているかについて教えてください。）

【回答 2】

【質問 3】　（【質問 1】の①又は③記載の体制を有している場合のみ回答をお願いいたします。）

監査役会・各委員会などの監督機関において、保安に関して審議・議論がなされていますか。具体的にどのような議論がなされていますか。（自社が監査役会等会社、監査等委員会設置会社、指名委員会等設置会社でなく親会社がこれらの機関設計をとっている場合には、親会社の監査役会・各委員会における保安に関する審議・議論について教えてください。）

【回答 3】

【質問 4】

保安担当の役員（取締役又は取締役と同等の位置づけにある役員であり、執行役員は含まない。）は設置されていますか。保安担当の役員は具体的にどのような職務を担当していますか。

【回答 4】

【質問 5】

取締役等の保安に関する職務執行が適切に行われているか否かを監視する役割を果たす社内組織はありますか。当該組織がある場合、組織の位置づけや具体的な業務内容等について教えてください。

【回答 5】

【質問 6】

① 現行の認定制度においては、本社が１年に１回以上事業所及び検査管理組織に対して監査を実施することとなっています（コンビ則別表第５上欄一ロの項下欄第四号等）。この本社による監査について、監査のメンバーに会社員以外の外部の有識者は含まれていますか。

② 上記以外で、コンプライアンスについて、第三者的な視点で確認が行われる体制を有している場合は、具体的な体制を教えてください。

【回答 6】	
①	
②	

【質問 7】

① 内部通報制度は整備されていますか。また、現状どの程度活用されていますか。

② 内部通報制度の機能を向上させ、活用を促進するためには、どのような取組を行うことが効果的だと考えますか。

③ 内部通報制度の活用が進んでいない場合、活用の障害となっている事項及び有効な改善策は何だと考えますか。

【回答 7】	
①	
②	
③	

【質問 8】

① 法令違反が発覚した場合の具体的な対応手順が文書化され定められていますか。

② 定められている場合、どのような規程において、具体的にどのような対応手順をとることとしていますか。

③ このほか、法令違反が発覚した場合に適切な手続きをとるために実施している取組があれば御記載願います。

【回答 8】	
①	
②	
③	

【質問 9】

① （1）法令上の手続きの要否とその要件・基準（法令上の手続きが必要となる場合の要件・基準）、（2）法令手続きを行う場合の業務手順、（3）複層的なチェック体制（例：現場の運転管理・設備管理部門がチェックした後に、保安管理部門がチェックする）、（4）法令手続きのチェックを行う者の資格要件についてルールがありますか。

② このほか、法適合性確認能力（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）の確保のために実施している取組（教育制度等）があれば御記載願います。

【回答 9】	
①	
②	

【質問 10】

最新の法令情報を収集し、職員に周知・教育する取組を行っていますか。具体的にどのような取組を行っているか教えてください。

【回答 10】

【質問 11】

現行のスーパー認定事業所には、テクノロジーに関して、以下（1）から（5）の要件が求められています。

（1）先進的な技術（※1）を積極的に検証又は導入していること

（2）導入した技術について、その効果を適切に検証し、改善に向けた取組みを実施していること

（3）主要施設において、施設及び設備保全に関する分野並びに運転に関する分野のそれぞれについて

- ✓ ビッグデータの収集（※2）、ビッグデータの分析及び未来予測（※3）
- ✓ ヒトに気付きを与え、ミスを防ぐという観点（※4）から先進的な技術の検証及び導入を適切に行っており、先進的な技術の検証及び導入計画を適切に定めていること

（4）6ヶ月程度以上の検証

（5）外部からのモニターを適切に受けていること

① 保安の確保に向けて、現状活用しているテクノロジーについて幅広く教えてください。

② 今後の効果が期待できるテクノロジーや将来的なテクノロジー活用の展開・展望などについて幅広く教えてください。

③ 保安確保の観点から、上記(1)から(5)のうち、どの項目を行っていますか。行っている項目について、その項目ごとに具体的な取り組みを教えてください。また、現状先進的な技術を導入していない場合、将来的に導入および効果検証を行う予定はありますか。

（※1）先進的な技術とは、安全な操業や、設備内異常の早期かつ精度の良い検知又は予測を促進するための技術であって、安全に運転することを支援又は危険源の把握等を用意にするものをいう。（「特定認定事業者及び自主保安高度化事業者の認定について」（通達）より）

（※2）ビッグデータの収集とは、施設及び設備保全に関する分野並びに運転に関する分野等において、データの収集に努めていることをいう。

（※3）ビッグデータの分析及び未来予測とは、施設及び設備保全に関する分野並びに運転に関する分野等において、収集したビッグデータ等について分析し、異常予知等を含む保安の向上に活用していることをいう。

（※4）ヒトに気づきを与え、ミスを防ぐ観点とは、従業員に気づきを与え、ヒューマンエラーを防ぐ観点のことをいう。（「特定認定事業者及び自主保安高度化事業者の認定について」（通達）より）

【回答 11】	
①	
②	
③	

【質問 12】

保安を確保するためのサイバーセキュリティ対策として、具体的に何を実施していますか。

【回答 12】

【質問 13】

サイバーリスクとしては、具体的に何を想定していますか。

【回答 13】

【質問 14】

保安を確保するために導入しているテクノロジー（プラントの運転管理システム、設備管理システム等を含む）について、現状データログを保存していますか。

【回答 14】

Ⅲ　規制の特例について

【質問 15】

改正法（第 39 条の 21）において、変更工事の手続き（法第 14 条第 1 項）の特例として、新たな認定制度において、以下（1）から（3）の特例が措置されました。

（1）工事又は製造の方法の変更のうち重要な変更は「許可」

（2）（1）及び（3）以外の変更は「事後届」

（3）製造のための施設の位置、構造、設備、製造方法の変更のうち軽微な変更は「記録保存」

①　（1）の「重要な変更」として位置づけるべきものを教えてください（その理由も含む）。

②　（2）の「事後届」として位置づけるべきものを教えてください（その理由も含む）。

③　（3）の「軽微な変更」として位置づけるべきものを教えてください（その理由も含む）。

（※）なお、「軽微な変更」については、現行制度上、省令＊で定められており、それ以外に該当がある場合のみ記載をお願いいたします。

＊一般則第 15 条第 1 項、液石則第 16 条第 1 項、コンビ則第 14 条第 1 項、冷凍則第 17 条第 1 項

【回答 15】	
①	
②	
③	

【質問 16】

改正法（第 39 条の 24、第 39 条の 25）において、新たな認定制度において、保安係員と保安主任者の選任の区分の柔軟化の特例が措置されました。これにより、コンビナート連携や、常時監視・遠隔監視システムの導入によって、製造施設の区分ごとによらずに保安人員配置を柔軟化することが考えられますが、一方で保安係員と保安主任者には、複数の区分のプラントへの緊急対応も想定されます。また、プラント種類やその運転管理体制は事業者ごとに異なるものと考えられます。

その際、個別に事業者が具備すべき具体的な柔軟化の要件と要件に応じた柔軟化の形態（〇〇の区分と□□の区分の統合等）として想定されるものがあれば記載願います。

【回答 16】

Ⅳ　その他

【質問 17】

現行認定制度では、開放検査周期の延長など各保安検査項目に対する特例が認められており、今回の新制度においても同様の措置を講じることを予定しています。仮に、開放検査周期の延長などを行っていた状態で認定の取消しを受けた場合、非認定事業所として告示で定める保安検査方法により保安検査を受ける必要が生じます。このような場合に、取消し後、速やかに保安検査を受けるために必要な期間としては、どの程度の期間が考えられますか（例：取消し後 2 ヶ月など）。そのように考えられる理由についても教えてください。なお、開放検査周期の延長以外についても認定取り消しに伴い告示以外の保安検査方法が採用できなくなることや、新制度において【質問 16】の保安人員の特例を受けていた場合等も考慮してお答えください。

【回答 17】

【質問 18】　（認定事業所又はスーパー認定事業所ではない場合のみ回答をお願いいたします。）

認定・スーパー認定を取得しない理由（要件面などのボトルネックや、認定のインセンティブとして必要な特例など）を教えてください。

【回答 18】

【質問 19】　（認定事業所（スーパー認定事業所を除く。）のみ回答をお願いいたします。）

スーパー認定を取得しない理由（要件面などのボトルネックや、認定のインセンティブとして必要な特例など）を教えてください。

【回答 19】

【質問 20】

① 新認定制度の取得に際して、保安確保の観点から、改善（不要・過剰又は強化）すべきと考えられるもの（※例を参照）はありますか。ある場合は、その理由（例：具体的にどのような負担があり、それが改善されることによってどのようなメリットがあるか。）と改善すべき内容（具体的に、どの部分に改善の余地があると考えるか）について、具体的に記載願います。また、改善すべきと考えられるものが複数ある場合、その優先順位についても記載してください。

（※）例：認定基準、申請・準備書類、現地調査、審査期間、認定手数料 等

② 上記のほか、新認定制度に期待する事項があれば、教えてください。

【回答 20】	
①	
②	

＜アンケート調査にご協力いただき、誠にありがとうございました。＞

別添２

新認定制度の設計に関するアンケート

Ⅰ　自治体の概要

1. 自治体名：

2. 所在地：

3. 本件ご担当者様（ご回答後、ご連絡させていただく場合がございます。）

氏名：

部署：

役職：

E-Mail アドレス：

TEL：

＜用語の説明＞

・改正法：高圧ガス保安法等の一部を改正する法律（令和 4 年法律第 74 号）による改正後の高圧ガス保安法

・法　　：高圧ガス保安法

Ⅱ　認定要件について

【質問 1】

事業者の法適合性確認能力（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）・法令遵守体制について、問題だと感じている点があれば教えてください。その場合、そのように感じた経緯や具体的な理由についても教えてください。

【回答 1】

【質問 2】

各事業者の法適合性確認能力について、チェックの仕組み、チェック者の資格要件などの認定基準や求められる資質など必要と考えられる要素を教えてください。

【回答 2】

Ⅲ　規制の特例について

【質問 3】

改正法（第 39 条の 21）において、変更工事の手続き（法第 14 条第 1 項）の特例として、新たな認定制度において、以下（1）から（3）の特例が措置されました。

（1）工事又は製造の方法の変更のうち重要な変更は「許可」

（2）（1）及び（3）以外の変更は「事後届」

（3）製造のための施設の位置、構造、設備、製造方法の変更のうち軽微な変更は「記録保存」

①　（1）の「重要な変更」として位置づけるべきものを教えてください（その理由も含む）。

②　（2）の「事後届」として位置づけるべきものを教えてください（その理由も含む）。

③　（3）の「軽微な変更」として位置づけるべきものを教えてください（その理由も含む）。

（※）なお、「軽微な変更」については、現行制度上、省令＊で定められており、それ以外に該当がある場合のみ記載をお願いいたします。

＊一般則第 15 条第 1 項、液石則第 16 条第 1 項、コンビ則第 14 条第 1 項、冷凍則第 17 条第 1 項

【回答 3】	
①	
②	
③	

【質問 4】

施設の変更の特例について、自治体の事務処理等の観点から配慮してほしいことがあればご記載ください。そのほか、施設の変更の特例について留意点等があればご記載ください。

【回答 4】

【質問 5】

改正法（第 39 条の 24、第 39 条の 25）において、新たな認定制度において、保安係員と保安主任者の選任の区分の柔軟化の特例が措置されました。これにより、コンビナート連携や、常時監視・遠隔監視システムの導入によって、製造施設の区分ごとによらずに保安人員配置を柔軟化することが考えられますが、一方で保安係員と保安主任者には、複数の区分のプラントへの緊急対応も想定されます。また、プラント種類やその運転管理体制は事業者ごとに異なるものと考えられます。

その際、個別に事業者が具備すべき具体的な柔軟化の要件と要件に応じた柔軟化の形態（〇〇の区分と□□の区分の統合等）として想定されるものがあれば記載願います。また、この特例の適用に当たり留意点があれば教えてください。

【回答 5】

Ⅳ　その他

【質問 6】

現行認定制度では、開放検査周期の延長など各保安検査項目に対する特例が認められており、今回の新制度においても同様の措置を講じることを予定しています。仮に、開放検査周期の延長などを行っていた状態で認定の取消しを受けた場合、非認定事業所として告示で定める保安検査方法により保安検査を受ける必要が生じます。このような場合に、取消し後、速やかに保安検査を受けるために必要な期間としては、どの程度の期間が考えられますか（例：取消し後 2 ヶ月など）。そのように考えられる理由についても教えてください。

なお、開放検査周期の延長以外についても認定取り消しに伴い告示以外の保安検査方法が採用できなくなることや、新制度において【質問 5】の保安人員の特例を受けていた場合等も考慮してお答えください。

【回答 6】

【質問 7】

保安確保の観点から、不要・過剰又は強化すべきと考えられる認定要件や審査手続き・提出書類等はありますか。ある場合は、具体的に記載願います。

【回答 7】

【質問 8】

新制度において、事後的なチェック・監督を適切に行うための必要な措置として、立入検査のあり方（頻度、タイミング、メンバーなど）や、自治体における対応、国における対応について意見を教えてください。

【回答 8】

【質問 9】

新認定制度に期待する事項や留意点があれば、教えてください。

【回答 9】

＜アンケート調査にご協力いただき、誠にありがとうございました。＞

電磁的方法による保存等をする場合に確保するよう努めなければならない基準

（平成十七年三月二十九日　経済産業省・環境省告示第二号）

改正　平成一七年　五月一八日　経済産業省・環境省告示第　五号
同　一九年一〇月　一日　同　第　九号
同　二〇年　四月　一日　同　第　三号
同　二四年　九月一四日　同　第一三号
同　二八年　四月　一日　同　第　四号
同　二九年　三月二八日　同　第　二号

１　別表第２に掲げる保存等をする場合には、それぞれ別表第１に掲げる基準を確保するよう努めなければならない。

２　この基準において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）「情報システム」とは、ホストコンピュータ、端末機、通信関係装置、プログラム等の全部又は一部により構成され、電磁的方法による記録、保存等をするためのシステムをいう。

（２）「データ」とは、情報システムの入出力情報をいう。

（３）「プログラム」とは、プログラム言語により記述された命令の組合せをいう。

（４）「事務室」とは、端末機、サーバ、ワークステーション、パーソナルコンピュータ等を設置している室、店舗、配送センタ等をいう。

（５）「データ保管室」とは、データ、プログラム等を含んだ記録媒体等を保管する室をいう。

（６）「記録媒体」とは、データ、プログラム等を記録した機器、ディスク、磁気テープ、フィルム、カード等をいう。

附　則

この告示は、平成十七年四月一日から施行する。

附　則　（平成一七年五月一八日経済産業省・環境省告示第五号）

この告示は、海洋汚染及び海上災害の防止に関する法律等の一部を改正する法律の施行の日（平成十七年五月十九日）から施行する。

附　則　（平成一九年一〇月一日経済産業省・環境省告示第九号）

この告示は、平成十九年十月一日から施行する。

附　則　（平成二〇年四月一日経済産業省・環境省告示第三号）

この告示は、平成二十年四月一日から施行する。

改正文　（平成二四年九月一四日経済産業省・環境省告示第一三号）　抄

原子力規制委員会設置法の施行の日（平成二十四年九月十九日）から施行する。

改正文　（平成二八年四月一日経済産業省・環境省告示第四号）　抄

平成二十八年四月一日から施行する。

改正文　（平成二九年三月二八日経済産業省・環境省告示第二号）　抄

平成二十九年四月一日から施行する。

別表第１

基準
１　ログ ①情報システムには、データの保存及び更新時に保存及び更新の日時並びに実施者を記録する「ログデータ」の保存機能を設けること。 ②取得した「ログデータ」は安全な場所に保管し、保管方法等に係る運用管理規程を定めること。 ２　アクセス ①情報システムには、個人別のＩＤ、パスワード等の利用者登録、管理及び認証機能を設けること。 ②情報システムのうち、データの保管を行う機器に直接接続されたコンピュータが、公衆回線とのオンラインによって接続される場合には、アクセスするユーザ等の正当性を識別し認証する機能を設けること。 ③個人別のＩＤは、複数者で共用しないこと。 ④情報システムには、情報やシステムの機密度を区分し、アクセス権限を制御する機能を設けること。 ⑤情報システムは、ＩＤを付与された関係者以外の者が操作をしないよう周知徹底する等の措置をとること。 ⑥人事異動等で使わなくなったＩＤ及びパスワードは、直ちに無効化すること。 ３　バックアップ ①情報システムの保守、点検、改造等は、あらかじめ計画を設けた上で行い、バックアップ等当該行為の期間のデータ保護措置を講じること。 ②データを収蔵したデータ記録媒体は、当該媒体以外にバックアップを行い、当該媒体と異なる保管場所に保管すること。 ③データを収蔵したデータ記録媒体及びバックアップは、定期的に保管状況の点検を実施すること。 ４　セキュリティ対策等 ①外部から入手したソフトウェア、使用済記録媒体等は、ウイルス検査後に利用すること。 ②情報システムには、データのエラーの検出機能を設けること。 ③情報システムには、システムへの不正なアクセス及びデータの不正な変更を発見するソフトウェア機能を設けること。 ５　スキャナ（これに準ずる画像読取装置を含む。）による読取に係る取扱い ①作業責任者の明確化等スキャナによる読取に係る運用管理規程を定めること。 ②スキャナにより読み取り画像情報として電子化した文書に圧縮を施す際、圧縮方式を適切に設定すること。 ６　情報システムの運用管理 ①情報システムの管理には、管理責任者を定めること。 ②管理責任者は、以下の項目の管理規程を明文化して定め、関係者に周知徹底すること。 ・事務室及びデータ保管室への入退室管理 ・ＩＤ及びパスワードの付与及び廃止の管理 ・データ記録媒体の使用、保管、搬出入及び廃棄の管理

③情報システムの電源には、システムに無関係な機器の接続を禁止し、電源の誤切断を防止すること。
④データを収蔵したデータ記録媒体は、保管場所を定め、施錠して保管し、保管場所からの搬出入及び授受は管理記録を整備して行うこと。
⑤情報システムの非使用時には、施錠し又は機能を停止させること。
⑥情報処理機器及びソフトウェアは、正常作動を確認した上で情報システム上での運用を開始すること。

7　情報システムの点検・監査

①情報システムの自主点検又は内部検査を定期的に行うこと。
②第三者による情報システムの監査を定期的に行うこと。

別表第２

保存等
計量法施行規則（平成５年通商産業省令第６９号）第７７条の２第１項及び第８６条の２第１項の保存、指定定期検査機関、指定検定機関、指定計量証明検査機関及び特定計量証明認定機関の指定等に関する省令（平成５年通商産業省令第７２号）第４条の２第１項、第１２条の２第１項、第１８条及び第１８条の１０第１項の保存、特定工場における公害防止組織の整備に関する法律に基づく指定試験機関に関する省令(昭和６１年通商産業省令第４６号)第１０条の２第１項の保存、経済産業省関係化学物質の審査及び製造等の規制に関する法律施行規則（昭和４９年通商産業省令第４０号）第７条の２第１項の保存、化学兵器の禁止及び特定物質の規制等に関する法律施行規則（平成７年通商産業省令第４０号）第１５条の２第１項の保存、特定物質の規制等によるオゾン層の保護に関する法律施行規則（昭和６３年通商産業省令第８０号）第１３条の２第１項の保存、特定製品に係るフロン類の回収及び破壊の実施の確保等に関する法律に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則（平成１９年経済産業省・環境省令第８号）第４条第１項の保存、アルコール事業法施行規則（平成１２年通商産業省令第２０９号）第１０条第１項の保存、武器等製造法施行規則（昭和２８年通商産業省令第４３号）第２２条の２第１項の記録、対人地雷の製造の禁止及び所持の規制等に関する法律施行規則（平成１１年通商産業省令第１０号）第１１条第１項の記録、特定国際種事業に係る届出等に関する省令（平成７年総理府・通商産業省令第２号）第２条の２第１項の保存、絶滅のおそれのある野生動植物の種の保存に関する法律第３３条の８第１項に規定する認定機関に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令（平成１７年経済産業省・環境省令第３号）第４条第３項、ゴルフ場等に係る会員契約の適正化に関する法律施行規則（平成５年通商産業省令第２３号）第１２条の２第１項の備置き、特定商品等の預託等取引契約に関する法律施行規則（昭和６１年通商産業省令第７５号）第５条の２第１項の備置き、電気用品安全法施行規則（昭和３７年通商産業省令第８４号）第１２条第１項、第２８条第１項及び第３０条の保存、液化石油ガス器具等の技術上の基準等に関する省令（昭和４３年通商産業省令第２３号）第１４条第１項、第３０条第１項及び第３２条の保存、ガス用品の技術上の基準等に関する省令（昭和４６年通商産業省令第２７号）第１４条第１項、第３０条第１項及び第３２条の保存、経済産業省関係特定製品の技術上の基準等に関する省令（昭和４９年通商産業省令第１８号）第１５条第１項、第３２条第１項及び第３４条の保存、エネル

ギー管理士の試験及び免状の交付に関する規則（昭和５９年通商産業省令第１５号）第２５条第２項及び第４５条第１項の保存、エネルギー管理員の講習に関する規則（平成１１年通商産業省令第４８号）第１１条第１項の保存、鉱業法施行規則（昭和２６年通商産業省令第２号）第３０条の２第１項の備置き、石油及び可燃性天然ガス資源開発法施行規則（昭和２７年通商産業省令第４４号）第４４条の２第１項の作成、石油需給適正化法施行規則（昭和４９年通商産業省令第１号）第５条の２第１項の保存、揮発油等の品質の確保等に関する法律施行規則（昭和５２年通商産業省令第２４号）第６０条の２第１項の保存、石油の備蓄の確保等に関する法律施行規則（昭和５１年通商産業省令第２６号）第４３条第１項の保存、採石法施行規則（昭和２６年通商産業省令第６号）第９条の３第１項の保存、熱供給事業法施行規則（昭和４７年通商産業省令第１４３号）第２０条の２第１項の保存、特定放射性廃棄物の最終処分に関する法律施行規則（平成１２年通商産業省令第１５１号）第３０条第１項及び第４１条の保存、電気工事士法施行規則（昭和３５年通商産業省令第９７号）第１３条の１１の２第１項の保存、電気工事業の業務の適正化に関する法律施行規則（昭和４５年通商産業省令第１０３号）第１３条の２第１項の保存、電気事業法施行規則（平成７年通商産業省令第７７号）第４０条第１項、第９４条の８第１項、第１０３条の２第１項、第１１８条第１項、第１２６条第１項及び第１３２条の保存、電気事業者による新エネルギー等の利用に関する特別措置法施行規則（平成１４年経済産業省令第１１９号）第１９条第１項の保存、ガス事業法施行規則（昭和４５年通商産業省令第９７号）第１８条第１項、第２３条第１項、第４７条第１項、第５１条第１項、第７９条第１項、第９１条第１項、第１０５条第１項、第１１０条第１項（第１３１条第１項の規定において準用する場合を含む。）、第１２７条第１項、第１４５条第１項、第１６１条第１項、第１６６条第１項、第１８３条第１項（第２０６条の規定において準用する場合を含む。）及び第１９５条第１項の保存、火薬類取締法施行規則（昭和２５年通商産業省令第８８号）第８１条の１２の３第１項の保存、容器保安規則（昭和４１年通商産業省令第５０号）第５３条の２第１項及び第５６条の保存、冷凍保安規則（昭和４１年通商産業省令第５１号）第４４条の２第１項の保存、液化石油ガス保安規則（昭和４１年通商産業省令第５２号）第８１条の２第１項の保存、一般高圧ガス保安規則（昭和４１年通商産業省令第５３号）第８３条の２第１項の保存、特定設備検査規則（昭和５１年通商産業省令第４号）第７１条第１項及び第７５条の保存、コンビナート等保安規則（昭和６１年通商産業省令第８８号）第３８条の２第１項の保存、鉱山保安法施行規則（平成１６年経済産業省令第９６号）第５３条第１項の保存、金属鉱業等鉱害対策特別措置法施行規則（昭和４８年通商産業省令第６０号）第４３条の２第１項の保存、液化石油ガスの保安の確保及び取引の適正化に関する法律施行規則（平成９年通商産業省令第１１号）第１１８条の２第１項及び第１３１条の２第１項の保存、高圧ガス保安法に基づく指定試験機関等に関する省令（平成９年通商産業省令第２３号）第６８条第１項の保存、工業所有権に関する手続等の特例に関する法律施行規則（平成２年通商産業省令第４１号）第４９条の２第１項及び第５９条の２第１項の保存並びに経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則（平成１７年経済産業省令第３２号）第４条第４項の保存

別添 4

クラウドサービス利用のための
情報セキュリティマネジメントガイドライン

Information security management guidelines for the use of cloud computing services

2013 年度版

経 済 産 業 省

目　次

ページ

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版」の公表にあたって 1
0.1 背景 1
0.2 2013 年度版のポイント 1
0.3 2013 年度版における追補の概要 1
序文 3
0.1　一般 3
0.2　クラウドサービス及び情報セキュリティ 3
0.2.1　このガイドラインにおけるクラウドサービス及び情報とは何か 3
0.2.2　クラウドサービス利用のための情報セキュリティはなぜ必要か 4
0.2.3　クラウド利用者がセキュリティ要求事項を確立する方法 5
0.2.4　クラウド利用者の管理策の選択 5
0.3　このガイドラインの位置づけ及び構成 6
0.3.1　このガイドラインの位置づけ 6
0.3.2　このガイドラインの構成 6
1　適用範囲 7
2　引用規格 7
3　用語及び定義 8
4　クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント 11
4.1　クラウドサービス利用における情報セキュリティガバナンス 11
4.1.1　クラウドサービス利用がもたらす情報セキュリティガバナンスの変化 12
4.1.2　クラウドサービス利用における情報セキュリティガバナンスのフレームワーク 12
4.2　クラウドサービス利用における情報セキュリティマネジメント 14
4.2.1　クラウドサービス利用におけるリスクアセスメントの留意点 14
4.2.2　クラウドサービス利用におけるマネジメントシステムの改善に向けた留意点 15
4.2.3　このガイドラインの情報セキュリティ監査への活用 15
4.2.4　このガイドラインのサプライチェーンへの活用 15
5　セキュリティ基本方針 16
5.1　情報セキュリティ基本方針 16
5.1.1　情報セキュリティ基本方針文書 16
5.1.2　情報セキュリティ基本方針のレビュー 17
6　情報セキュリティのための組織 17
6.1　内部組織 17

6.1.1 情報セキュリティに対する経営陣の責任 18
6.1.2 情報セキュリティの調整 18
6.1.3 情報セキュリティ責任の割当て 18
6.1.4 情報処理設備の認可プロセス 19
6.1.5 秘密保持契約 20
6.1.6 関係当局との連絡 20
6.1.7 専門組織との連絡 21
6.1.8 情報セキュリティの独立したレビュー 21
6.2 外部組織 21
6.2.1 外部組織に関係したリスクの識別 22
6.2.2 顧客対応におけるセキュリティ 23
6.2.3 第三者との契約におけるセキュリティ 23
7 資産の管理 24
7.1 資産に対する責任 24
7.1.1 資産目録 24
7.1.2 資産の管理責任者 25
7.1.3 資産利用の許容範囲 25
7.2 情報の分類 25
7.2.1 分類の指針 26
7.2.2 情報のラベル付け及び取扱い 26
8 人的資源のセキュリティ 27
8.1 雇用前 27
8.1.1 役割及び責任 27
8.1.2 選考 27
8.1.3 雇用条件 27
8.2 雇用期間中 28
8.2.1 経営陣の責任 28
8.2.2 情報セキュリティの意識向上，教育及び訓練 28
8.2.3 懲戒手続 29
8.3 雇用の終了又は変更 29
8.3.1 雇用の終了又は変更に関する責任 29
8.3.2 資産の返却 29
8.3.3 アクセス権の削除 30
9 物理的及び環境的セキュリティ 30
9.1 セキュリティを保つべき領域 30
9.1.1 物理的セキュリティ境界 30

9.1.2 物理的入退管理策 31
9.1.3 オフィス，部屋及び施設のセキュリティ 31
9.1.4 外部及び環境の脅威からの保護 31
9.1.5 セキュリティを保つべき領域での作業 31
9.1.6 一般の人の立寄り場所及び受渡場所 32
9.2 装置のセキュリティ 32
9.2.1 装置の設置及び保護 32
9.2.2 サポートユーティリティ 32
9.2.3 ケーブル配線のセキュリティ 32
9.2.4 装置の保守 33
9.2.5 構外にある装置のセキュリティ 33
9.2.6 装置の安全な処分又は再利用 33
9.2.7 資産の移動 33
10 通信及び運用管理 33
10.1 運用の手順及び責任 33
10.1.1 操作手順書 34
10.1.2 変更管理 34
10.1.3 職務の分割 35
10.1.4 開発施設，試験施設及び運用施設の分離 35
10.2 第三者が提供するサービスの管理 36
10.2.1 第三者が提供するサービス 36
10.2.2 第三者が提供するサービスの監視及びレビュー 37
10.2.3 第三者が提供するサービスの変更に対する管理 37
10.3 システムの計画作成及び受入れ 38
10.3.1 容量・能力の管理 38
10.3.2 システムの受入れ 39
10.4 悪意のあるコード及びモバイルコードからの保護 40
10.4.1 悪意のあるコードに対する管理策 40
10.4.2 モバイルコードに対する管理策 41
10.5 バックアップ 41
10.5.1 情報のバックアップ 42
10.6 ネットワークセキュリティ管理 43
10.6.1 ネットワーク管理策 43
10.6.2 ネットワークサービスのセキュリティ 43
10.7 媒体の取扱い 44
10.7.1 取外し可能な媒体の管理 44

10.7.2 媒体の処分 44
10.7.3 情報の取扱手順 44
10.7.4 システム文書のセキュリティ 45
10.8 情報の交換 45
10.8.1 情報交換の方針及び手順 45
10.8.2 情報交換に関する合意 45
10.8.3 配送中の物理的媒体 45
10.8.4 電子的メッセージ通信 46
10.8.5 業務用情報システム 46
10.9 電子取引サービス 46
10.9.1 電子商取引 46
10.9.2 オンライン取引 46
10.9.3 公開情報 47
10.10 監視 47
10.10.1 監査ログ取得 47
10.10.2 システム使用状況の監視 48
10.10.3 ログ情報の保護 48
10.10.4 実務管理者及び運用担当者の作業ログ 49
10.10.5 障害のログ取得 49
10.10.6 クロックの同期 50
11 アクセス制御 50
11.1 アクセス制御に対する業務上の要求事項 50
11.1.1 アクセス制御方針 50
11.2 利用者アクセスの管理 51
11.2.1 利用者登録 51
11.2.2 特権管理 52
11.2.3 利用者パスワードの管理 52
11.2.4 利用者アクセス権のレビュー 53
11.3 利用者の責任 53
11.3.1 パスワードの利用 53
11.3.2 無人状態にある利用者装置 54
11.3.3 クリアデスク，クリアスクリーン方針 54
11.4 ネットワークのアクセス制御 54
11.4.1 ネットワークサービスの利用についての方針 54
11.4.2 外部から接続する利用者の認証 55
11.4.3 ネットワークにおける装置の識別 55

11.4.4 遠隔診断用及び環境設定用ポートの保護 55
11.4.5 ネットワークの領域分割 56
11.4.6 ネットワークの接続制御 56
11.4.7 ネットワークルーティング制御 57
11.5 オペレーティングシステムのアクセス制御 57
11.5.1 セキュリティに配慮したログオン手順 58
11.5.2 利用者の識別及び認証 58
11.5.3 パスワード管理システム 59
11.5.4 システムユーティリティの使用 59
11.5.5 セッションのタイムアウト 60
11.5.6 接続時間の制限 60
11.6 業務用ソフトウェア及び情報のアクセス制御 60
11.6.1 情報へのアクセス制限 61
11.6.2 取扱いに慎重を要するシステムの隔離 61
11.7 モバイルコンピューティング及びテレワーキング 62
11.7.1 モバイルのコンピューティング及び通信 62
11.7.2 テレワーキング 63
12 情報システムの取得，開発及び保守 63
12.1 情報システムのセキュリティ要求事項 63
12.1.1 セキュリティ要求事項の分析及び仕様化 63
12.2 業務用ソフトウェアでの正確な処理 64
12.2.1 入力データの妥当性確認 64
12.2.2 内部処理の管理 64
12.2.3 メッセージの完全性 64
12.2.4 出力データの妥当性確認 65
12.3 暗号による管理策 65
12.3.1 暗号による管理策の利用方針 65
12.3.2 かぎ（鍵）管理 65
12.4 システムファイルのセキュリティ 66
12.4.1 運用ソフトウェアの管理 66
12.4.2 システム試験データの保護 66
12.4.3 プログラムソースコードへのアクセス制御 66
12.5 開発及びサポートプロセスにおけるセキュリティ 67
12.5.1 変更管理手順 67
12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー 67
12.5.3 パッケージソフトウェアの変更に対する制限 68

12.5.4 情報の漏えい 68
12.5.5 外部委託によるソフトウェア開発 69
12.6 技術的ぜい弱性管理 69
12.6.1 技術的ぜい弱性の管理 69
13 情報セキュリティインシデントの管理 70
13.1 情報セキュリティの事象及び弱点の報告 70
13.1.1 情報セキュリティ事象の報告 70
13.1.2 セキュリティ弱点の報告 70
13.2 情報セキュリティインシデントの管理及びその改善 71
13.2.1 責任及び手順 71
13.2.2 情報セキュリティインシデントからの学習 71
13.2.3 証拠の収集 72
14 事業継続管理 73
14.1 事業継続管理における情報セキュリティの側面 73
14.1.1 事業継続管理手続への情報セキュリティの組込み 73
14.1.2 事業継続及びリスクアセスメント 74
14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施 74
14.1.4 事業継続計画策定の枠組み 75
14.1.5 事業継続計画の試験，維持及び再評価 75
15 順守 76
15.1 法的要求事項の順守 76
15.1.1 適用法令の識別 76
15.1.2 知的財産権（IPR） 77
15.1.3 組織の記録の保護 77
15.1.4 個人データ及び個人情報の保護 78
15.1.5 情報処理施設の誤用防止 78
15.1.6 暗号化機能に対する規制 78
15.2 セキュリティ方針及び標準の順守，並びに技術的順守 79
15.2.1 セキュリティ方針及び標準の順守 79
15.2.2 技術的順守点検 79
15.3 情報システムの監査に対する考慮事項 80
15.3.1 情報システムの監査に対する管理策 80
15.3.2 情報システムの監査ツールの保護 81
附属書 A（参考）クラウドサービス利用にかかわるリスク 82
附属書 B（参考）クラウドサービス利用におけるリスクアセスメントの実施例 89

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版」の公表にあたって

0.1 背景

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（以下，「初版」という。）の公表（2011 年 4 月 1 日）から約 2 年が経過した。この間，東日本大震災を背景とした事業継続の意識の高まり，政府機関並びに大手企業における情報セキュリティ事件・事故に伴う機密情報の流出及び大手金融機関における大規模システム障害の発生を契機にリスク対応の重要性が再認識されている。

クラウドサービスに着目すると，サービスの本格的な普及が進む中，国内外のクラウドサービスにおいて大規模な障害や障害対応過程における情報漏えいの発生など，リスクが顕在化した事例が見受けられるようになっている。一方，クラウドセキュリティに関する基準策定や国際標準策定が国内外で進められており，クラウドセキュリティに関する検討が深まっている。

クラウドサービスを取り巻くこのような環境の変化を踏まえ，「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版」（以下，「2013 年度版」という。）では，「クラウド利用者と事業者における信頼関係の強化に役立てる」ことに寄与するため，ガイドライン初版の内容を追補した。

0.2 2013 年度版のポイント

2013 年度版におけるポイントは次の 2 点である。

(1) 顕在化したリスクに対するセキュリティ要求事項の追加

昨今クラウドサービスにおいて顕在化したリスクを踏まえ，クラウド事業者に求められるセキュリティ要求事項を「クラウド事業者の実施が望まれる事項」に追加した。セキュリティ要求事項を明確化するにあたり，クラウドサービスにおける障害やトラブルなどのインシデント事例を分析するとともに，クラウド事業者に対してインタビュー調査を実施し，顕在化したリスクへの実際の対応及び自社では発生していないが想定されるリスクへの対応状況を調査した。

(2) 国際的な動向を踏まえた追補

クラウドサービスにおける情報セキュリティに関する国際会議などでの検討や海外政府の取組みなどの動向を踏まえて追補した。さらに，海外事業者へのインタビュー調査も踏まえて事業者の視点として反映した。

0.3 2013 年度版における追補の概要

(1) クラウドサービスにおける事業者の情報開示のあり方の反映

クラウドサービスの普及に伴い，クラウドサービスの本質に対する理解が深まっている。クラウドサービスの本質は，「標準的なサービスを多数の顧客に提供する」ことであり，従来のようなオンプレミスの情報システムの外部委託請負サービスとは異なるという点にある。2013 年度版では，次の考え方に基づき，初版の「クラウド利用者のための実施の手引」及び「クラウド事業者の実施が望まれる事項」を追補した。

a) 利用者への情報提供について事業者自らが方針を定めて利用者に提示し，利用者は提示された方

針及び方針に基づき提供された情報によってクラウドサービス利用に係るリスクを評価する。

b) クラウド事業者は，クラウド利用者との合意に基づき情報を開示する。

c) クラウド利用者には，クラウド事業者から情報を得た範囲で自らの責任においてリスクアセスメントを行い，対応や対策を決定する責任がある。

(2) 箇条書きへの変更

第三者評価などにおける客観的なチェックポイントをより明確にすべく，「クラウド利用者のための実施の手引」及び「クラウド事業者の実施が望まれる事項」において，箇条書きで示すことが適切な箇所については箇条書きに変更した。

(3) 例示の充実化

「クラウドサービスの関連情報」において，参考情報として例を示すことが有用な箇所については，クラウド事業者へのヒアリング調査なども踏まえて例示を充実させた。なお、参考情報の中に、『期待される』という表現で推奨事項を記載している。

序文

0.1　一般

クラウドコンピューティングは，「IT の所有」から「IT の利用」への転換を促すと予想され，その利用によって，組織が情報システムの構築・運用作業から解放されることが期待される。クラウドコンピューティングを利用することは，運用管理コストの低減，需要に応じた柔軟かつ迅速な調達に応えると同時に，大規模データ解析，最先端のアプリケーション利用が安価に実現できるため，IT 業界のみならず，農業や商業など，様々な業界からその普及，発展が期待されている。

そのような期待があるにもかかわらず，現時点で我が国でのクラウドコンピューティング利用は限定的である。その原因の一つとして，情報セキュリティに対する懸念がある。クラウドコンピューティングは，クラウド事業者の管理の下で他の利用者とコンピュータ資源を共有するため，情報の機密性・完全性・可用性にかかわる情報セキュリティについて懸念されているからである。

国内の組織の情報セキュリティには，国際的な規格（ISO/IEC 27002:2005）に準拠した JIS Q 27002:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範（以下「JIS Q 27002（実践のための規範）」という。）に基づく管理策の実施が推奨されており，実際に多く利用されている。JIS Q 27002（実践のための規範）には，第三者の提供するサービスの利用に関する管理策があるが，組織が IT を所有せずに全面的にクラウドコンピューティングを利用する場合には，この管理策が求める事項だけでは組織の情報セキュリティを確保するためには不足があるのが実情である。

そのため，クラウド利用者の視点から JIS Q 27002（実践のための規範）の各管理策を再考し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドラインを作成した。

このガイドラインには，組織がクラウドコンピューティングを全面的に利用する極限状態を想定し，①自ら行うべきこと，②クラウド事業者に対して求める必要のあること，さらに，③クラウドコンピューティング環境における情報セキュリティマネジメントの仕組みについて記載している。

組織において，このガイドラインを参考にクラウドコンピューティングに対応した情報セキュリティの仕組みを整備するとともに，クラウド利用者のみで行うことができない管理策を認識し，クラウド利用者がクラウド事業者に対して様々な情報を求める必要がある。

クラウド事業者においても，このガイドラインを参考に適切な情報を提供し，利用者との協力関係を向上することが望まれる。

このガイドラインの利活用によって，クラウド利用者がクラウドコンピューティングの利用にあった情報セキュリティ対策を実施し，クラウドコンピューティングの活用が促進されることが望まれる。

0.2　クラウドサービス及び情報セキュリティ

0.2.1　このガイドラインにおけるクラウドサービス及び情報とは何か

高速なネットワークの普及とともに，仮想化などの技術を利用してネットワーク上でコンピュータリソースを共有できるようになった。共有するコンピュータリソースは CPU，メモリ，ストレージ，ネットワーク，オペレーティングシステム，アプリケーションの実行環境，アプリケーション本体，データベースなど多岐にわたっており，組織内にコンピュータリソースをもつことなく，ネットワーク経由で様々な情

報処理サービスを利用できるようになった。

このガイドラインでは，クラウドコンピューティングを「共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態」と定義し，クラウドサービスをネットワークサービスの一つとして取り扱う。

クラウドサービスの中で，CPU，メモリ，ストレージ，ネットワークなどをサービスとして提供するものを IaaS，オペレーティングシステム，データベース，開発環境，実行環境を提供するものを PaaS，すぐに使えるアプリケーションを提供するものを SaaS と定義する。IaaS，PaaS，SaaS の区分については，商業的に提供するクラウド事業者によって定義が異なることもあり，このガイドラインの中で詳細な定義をするものではない。提供するリソースを目安としてクラウドサービスを IaaS，PaaS，SaaS に分類している。

JIS Q 27002（実践のための規範）序文 0.2.1 によれば，情報は，紙に印刷若しくは手書きされ，電磁的に保存され，郵便若しくは電磁的な手段によって伝達され，映写され，又は会話として話されるなど，多くの形態で存在することができる。一方，クラウドコンピューティングにおいて情報は，電磁的に保存され，電磁的な手段によって伝達されるのであり，紙，郵便，会話などの非電磁的な形態で存在することはない。

クラウドサービス利用を前提とするこのガイドラインにおいては，電磁的な形態にある情報のみを取り扱う。

0.2.2　クラウドサービス利用のための情報セキュリティはなぜ必要か

JIS Q 27002（実践のための規範）序文 0.2.2 によれば，情報セキュリティマネジメントには，組織内のすべての従業員の参加が最低条件として要求されるが，外部組織の参加は必ずしも要求されない。「外部組織の参加が必要な場合もある」とされるにとどまる。

組織事業の基礎を成す情報資産の多くを組織内に保持しつつ，補完的に外部組織を利用する場合と，その大部分を組織内から外部組織に移行した場合とでは，情報セキュリティにかかわる主要なリスクの所在とコントロールの方法は全く異なった様相を呈する。前者の場合は，組織は自らリスクを検知して，それを直接コントロールすることができるのに対し，後者の場合は外部組織を介してリスクを検知し，外部組織にコントロールをゆだねる。つまり，組織は自らの事業の基礎を成す情報セキュリティを間接的にしかコントロールすることができない。したがって，この場合の情報セキュリティマネジメントには，組織内すべての従業員の参加だけでなく，それ以上に外部組織の何らかの関与が最低条件として要求されることになろう。

外部組織が提供するクラウドサービスを利用するということは，情報を取り扱うプロセス，システム並びにネットワークという情報資産を自組織の外部に置くことを意味する。クラウド利用者は，外部組織であるクラウド事業者からこれらの情報資産を利用できるサービスの提供を受け，これを利用して組織事業の基礎を成す情報の大部分を保存し又は処理するものとすれば，外部組織に依拠せずに情報セキュリティのマネジメントをすることはできない。これがクラウドサービス利用のための情報セキュリティが求められる理由である。

0.2.3　クラウド利用者がセキュリティ要求事項を確立する方法

JIS Q 27002（実践のための規範）序文 0.2.3 によれば，組織が組織自体のセキュリティ要求事項を導出する方法の一つに，以下を挙げている。

a) 一つには，組織全体における事業戦略及び目的を考慮して，組織に対するリスクアセスメントを実施することによって得られるものである。リスクアセスメントによって資産に対する脅威を特定し，事故に対するぜい弱性及び事故の可能性を評価し，潜在的な影響を推定する。

前述のとおり，クラウドサービスを利用して，組織事業の基礎を成す情報の多くを保存し又は処理する組織は，資産の多くをクラウド事業者に依拠している。したがって，上記 a）の方法によって組織自体のセキュリティ要求事項を導出しようとすれば，組織内の資産だけでなく，クラウド事業者内のクラウドサービスの提供にかかわる「資産に対する脅威を特定し，事故に対するぜい弱性及び事故の可能性を評価し，潜在的な影響を推定」することになる。

しかし，クラウド事業者はクラウド利用者とは独立した組織である。クラウドサービスの提供にかかわる資産に対する脅威，ぜい弱性及び事故の可能性の評価に資するような，何らかの情報を開示するかどうかは，専らクラウド事業者自らの事業判断にゆだねられている。

したがって，クラウド利用者がセキュリティ要求事項を確立するには，クラウド利用者自らが行うリスクアセスメントに必要な情報を指定して，その情報を開示するよう，クラウド事業者に対して協力を要請することが望まれる。

0.2.4　クラウド利用者の管理策の選択

JIS Q 27001:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項（以下「JIS Q 27001（要求事項）」という。）を活用した情報セキュリティマネジメントシステムを構築している多くの組織が存在する。JIS Q 27001（要求事項）を満たす情報セキュリティマネジメントによれば，組織は，リスクアセスメントを行い，情報セキュリティの要求事項及びリスクを識別し，リスク対応の決定に基づいて，識別されたリスクを受容可能なレベルにまで確実に低減するように管理策を選択する。組織がクラウドサービスを導入するならば，クラウド事業者からリスクアセスメントに必要な情報の開示を受けて，情報セキュリティの管理と責任の変化を検討することから始まり，管理策の選択と実施に至る（図 1 参照）。

管理策について JIS Q 27001（要求事項）は，JIS Q 27002（実践のための規範）の管理目的及び管理策を引用し，規格の一部を構成している。JIS Q 27002（実践のための規範）の箇条 5～15 は，JIS Q 27001（要求事項）の附属書 A.5～15 までに規定した管理策を支える，導入への助言と最適な実施のための手引となっている。

したがって，JIS Q 27002（実践のための規範）に基づいたクラウドサービス利用のための実施の手引があれば，組織はより簡便に管理策の選択を行うことができる。

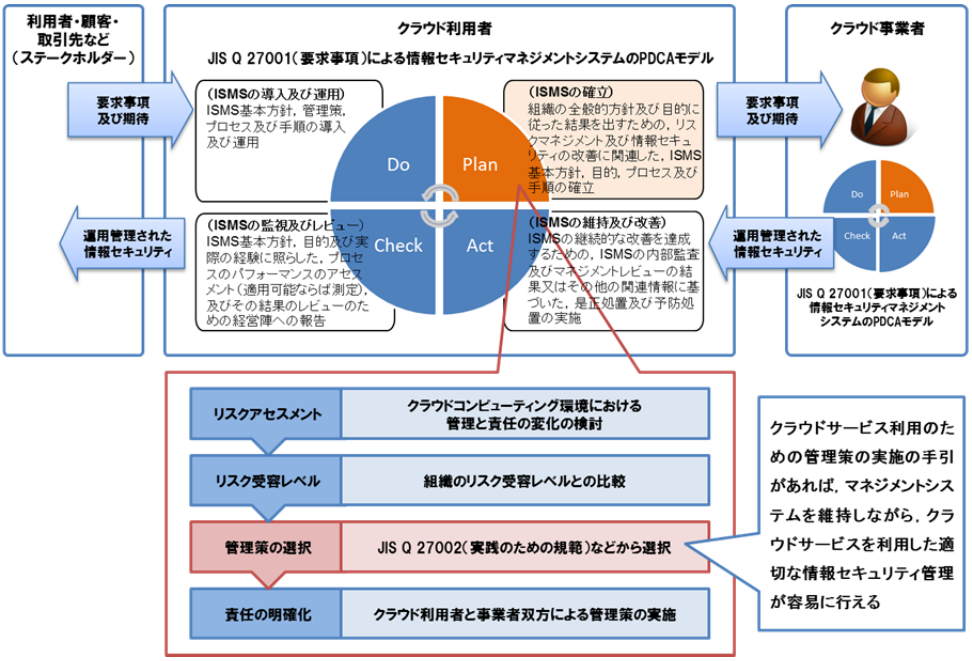


図 1　クラウドサービス利用にかかわる管理策の選択

0.3　このガイドラインの位置づけ及び構成

0.3.1　このガイドラインの位置づけ

このガイドラインは，クラウドサービスの利用にかかわるリスク対応のために JIS Q 27002（実践のための規範）から適切な管理策を選択し，導入するための助言とその最適な実施のための手引を提供する。JIS Q 27002（実践のための規範）がすべての組織に適用できることを意図しているのに対して，このガイドラインは，組織事業の基礎を成す情報資産の多くをクラウドサービスにゆだねる組織に適用できることを意図している。また，このガイドラインは JIS Q 27002（実践のための規範）の箇条 5～15 に記載された管理策の実施を支持し，管理目的を満たすための，クラウドサービス利用に着目した情報を提供する。

すなわち，このガイドラインは，JIS Q 27002（実践のための規範）に示された一般的原則の上に立ちながら，全面的にクラウドサービスを利用するという特殊な場合を想定するものである。

情報資産の多くを組織内に保持しつつ補完的にクラウドサービスを利用する場合には，組織内の情報資産については従来通りの管理策を実施し，クラウドサービス利用にかかわるプロセスについてはこのガイドラインを参考にして，適宜，必要となる管理策を選択することが望まれる。

0.3.2　このガイドラインの構成

このガイドラインの箇条 5～15 は，クラウド利用者が JIS Q 27002（実践のための規範）の箇条 5～15 の管理策を実施するための補足として活用できるように，次のように構成する。

目的

JIS Q 27002（実践のための規範）における目的をそのまま引用する。

管理策

JIS Q 27002（実践のための規範）における管理策をそのまま引用する。

クラウド利用者のための実施の手引

クラウドサービス利用において，クラウド利用者が実施する管理策を支持し，管理目的を満たすための情報を提供する。この手引にはすべての場合に適していないものもあるため，他の方法でその管理策を実施する方がより適切な場合もある。

クラウド事業者の実施が望まれる事項

クラウドサービス利用において，クラウド事業者の協力が必要となる管理策については，クラウド利用者が実施する管理策を支持し，管理目的を満たすために，クラウド事業者の実施が望まれる事項にかかわる情報を提供する。また，クラウド利用者が管理策を実施するにあたり事業者の協力が必要となる事項のみならず，クラウド事業者が自らの情報セキュリティマネジメントのために実施することが特に望まれる事項にかかわる情報についても提供する。

なお，クラウド事業者が実施する管理策として記載されている事項は，すべての場合に適していないものもあるため，他の方法でその管理策を実施する方がより適切な場合もある。

クラウドサービスの関連情報

クラウドサービス利用において考慮が必要と思われる関連情報（関連するクラウドサービスの種類，利用環境又は利用技術に関する情報など）を提供する。

なお，このガイドラインには，参考として附属書 A，B がある。附属書 A は，クラウドサービス利用にかかわるリスクを例示し，附属書 B は，クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

1　適用範囲

このガイドラインは，次の 2 点を満たす組織に対して適用される。

(1) 組織事業の基礎を成す情報資産の多くを，外部組織であるクラウド事業者が提供するクラウドサービスにゆだねようとする組織が，

(2) JIS Q 27002（実践のための規範）に規定された管理目的を達成するための管理策を実施しようとする場合

このガイドラインは，クラウドサービス利用の観点から，JIS Q 27002（実践のための規範）の「実施の手引」を補足した「クラウド利用者のための実施の手引」を提供し，クラウド事業者の協力が必要となる場合には「クラウド事業者の実施が望まれる事項」を提供する。クラウドサービスを利用しても，一般にその実施には影響がないと思われる管理策や，現時点の技術水準又は社会的な合意が形成されていない現況においてその実施を望むことが現実的でないと思われる事項については，「クラウド利用者のための実施の手引」又は「クラウド事業者の実施が望まれる事項」には記載していない。

2　引用規格

次に掲げる規格は，このガイドラインに引用されることによって，このガイドラインの規定の一部である，「目的」及び「管理策」をそのまま構成する。引用規格のうちで，西暦年を付記してあるものは，記

載の年の版を適用し，その後の改正版（追補を含む。）には適用しない。

JIS Q 27002:2006　情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範

注記　対応国際規格：ISO/IEC 17799:2005, Information technology―Security techniques―Code of practice for information security management （IDT）
なお，対応の程度を表す記号（IDT）は，ISO/IEC Guide 21 に基づき，一致していることを示す。

3　用語及び定義

このガイドラインで用いる主な用語及び定義は，次による。

3.1

資産 （asset）

組織にとって価値をもつもの（JIS Q13335-1:2006）。

3.2

可用性 （availability）

認可されたエンティティが要求したときに，アクセス及び使用が可能である特性（JIS Q13335-1:2006）。

3.3

クラウドコンピューティング（cloud computing）

共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態。

注記　これよりも広い定義が使われることもある。

例 1　（クラウドコンピューティングの定義の例）

1) クラウドコンピューティングとは，「ネットワークを通じて，情報処理サービスを，必要に応じて提供／利用する」形の情報処理の仕組み（アーキテクチャ）をいう。（経済産業省，「クラウドコンピューティングと日本の競争力に関する研究会報告書」，2010 年 8 月 16 日）。

2) Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, Special Publication 800-145 September 2011)

3.4

クラウドサービス（cloud service / cloud computing service）

クラウドコンピューティングを提供するサービス。

3.5

クラウド利用者 （cloud customer）

クラウドサービスを利用する組織。

3.6

クラウドサービスの利用者 （cloud user / cloud service user）

クラウド利用者（クラウドサービスを利用する組織）において，クラウドサービスを利用する者。

3.7

クラウド事業者 （cloud service provider）

クラウドサービスを提供する組織。ただし，クラウド事業者も，提供するサービスの様態によっては，クラウド利用者となる場合がある。

3.8

管理策 （control）

リスクを管理する手段（方針，手順，指針，実践又は組織構造を含む。）であり，実務管理的，技術的，経営的又は法的な性質をもつことがあるもの（JIS Q 27002:2006）。

3.9

指針 （guideline）

方針の中に設定された目標を達成するために成すべきこと及びその方法を明らかにした記述（JIS Q13335-1:2006）。

3.10

情報セキュリティガバナンス （information security governance）

社会的責任にも配慮したコーポレート・ガバナンスと，それを支えるメカニズムである内部統制の仕組みを，情報セキュリティの観点から企業内に構築・運用すること（経済産業省，「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」，平成 17 年 3 月）。

3.11

機密性 （confidentiality）

認可されていない個人, エンティティ又はプロセスに対して, 情報を使用不可又は非公開にする特性（JIS Q13335-1:2006）。

3.12

情報処理設備 （information processing facilities）

情報処理のシステム，サービス若しくは基盤のいかなるもの，又はそれらを収納する物理的場所（JIS Q 27002:2006）。

3.13

情報セキュリティ （information security）

情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい（JIS Q 27002:2006）。

3.14

情報セキュリティ監査 （information security audit）

情報セキュリティにかかわるリスクのマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキュリティ監査を行う主体が独立かつ専門的な

立場から，国際的にも整合性のとれた基準に従って検証又は評価し，もって保証を与えあるいは助言を行う活動（経済産業省，「情報セキュリティ監査研究会報告書」，2003 年 3 月 26 日）。

3.15

情報セキュリティ事象 （information security event）

システム，サービス又はネットワークにおける特定の状態の発生。特定の状態とは，情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関連するかもしれない未知の状況を示していることをいう（ISO/IEC TR 18044:2004）。

3.16

情報セキュリティインシデント （information security incident）

望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（ISO/IEC TR 18044:2004）。

3.17

情報セキュリティマネジメントシステム，ISMS （information security management system）

マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分（JIS Q 27001:2006）。

注記 マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。

3.18

IaaS （Infrastructure as a Service）

CPU，メモリ，ストレージ，ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス。

3.19

インフラ事業者 （infrastructure provider）

データセンター，ネットワークなどのインフラ資産を提供する事業者。

3.20

完全性 （integrity）

資産の正確さ及び完全さを保護する特性（JIS Q13335-1:2006）。

3.21

PaaS （Platform as a Service）

オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス。

3.22

リスク （risk）

事象の発生確率と事象の結果との組合せ（TR Q 0008:2003）。

3.23

リスク分析 （risk analysis）

リスク因子を特定するための，及びリスクを算定するための情報の系統的使用（TR Q 0008:2003）。

3.24

リスクアセスメント （risk assessment）

リスク分析からリスク評価までのすべてのプロセス（TR Q 0008:2003）。

3.25

リスク評価 （risk evaluation）

リスクの重大さを決定するために，算定されたリスクを与えられたリスク基準と比較するプロセス（TR Q 0008:2003）。

3.26

リスクマネジメント （risk management）

リスクに関して組織を指揮し管理する調整された活動。

注記 リスクマネジメントは一般にリスクアセスメント，リスク対応，リスクの受容及びリスクコミュニケーションを含む（TR Q 0008:2003）。

3.27

リスク対応 （risk treatment）

リスクを変更させるための方策を，選択及び実施するプロセス（TR Q 0008:2003）。

3.28

SLA （Service Level Agreement）

書面にしたサービス提供者と顧客との合意であって，サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）

3.29

SaaS （Software as a Service）

アプリケーションやデータベースをサービスとして提供するクラウドサービス。

3.30

第三者 （third party）

当該問題に関して，当事者と無関係であると認められる個人又は団体（ISO/IEC Guide 2:1996）。

注記 第三者には，構造的に，クラウド事業者が利用するクラウド事業者も含まれる。

3.31

脅威 （threat）

システム又は組織に損害を与える可能性があるインシデントの潜在的な原因（JIS Q13335-1:2006）。

3.32

ぜい弱性 （vulnerability）

一つ以上の脅威がつけ込むことができる，資産又は資産グループがもつ弱点（JIS Q13335-1:2006）。

4 クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント

4.1 クラウドサービス利用における情報セキュリティガバナンス

4.1.1　クラウドサービス利用がもたらす情報セキュリティガバナンスの変化

組織事業の基礎を成す情報及びその情報を取り扱うプロセス，システム並びにネットワークの多くを組織内に保持する場合，これらは経営陣によって管理できる。したがって，経営陣は，組織の情報セキュリティについて方向づけ（Direct）を与え，コミットメントを行い，PDCA の進捗・達成状況をモニタリング（Monitor）し，評価（Evaluate）し，利害関係者に報告（Report）することを通じて，組織の実効ある情報セキュリティガバナンスを確立することができる。

一方，クラウドサービス利用では，入力，演算，保存，出力という一連の情報処理プロセスのうち，主に入力と出力をクラウド利用者，演算と保存をクラウド事業者が分担するものとすれば，情報セキュリティガバナンスの主体は，互いに独立したクラウド利用者とクラウド事業者に分断される。

一般に，自組織の内部統制は，外部組織には及ばない。したがって，組織事業の基礎を成す情報資産の多くを外部組織にゆだねるクラウド利用者の経営陣は，組織の情報セキュリティにかかわる経営責任を全うすることができない。これを放置するならば，その組織の経営陣はその経営責任を，監査役はその監督責任を問われかねないため，情報セキュリティガバナンスは，クラウドサービスを利用するにあたって検討しなければならない大きな課題の一つとなっている。

4.1.2　クラウドサービス利用における情報セキュリティガバナンスのフレームワーク

クラウドサービス利用における情報セキュリティガバナンスの課題を解決するために，クラウド利用者とクラウド事業者の両経営陣がどのようなタスクを実施することが望ましいかを，情報セキュリティガバナンスのフレームワークで示されたモデルに従って示すことにする（図 2 参照）。

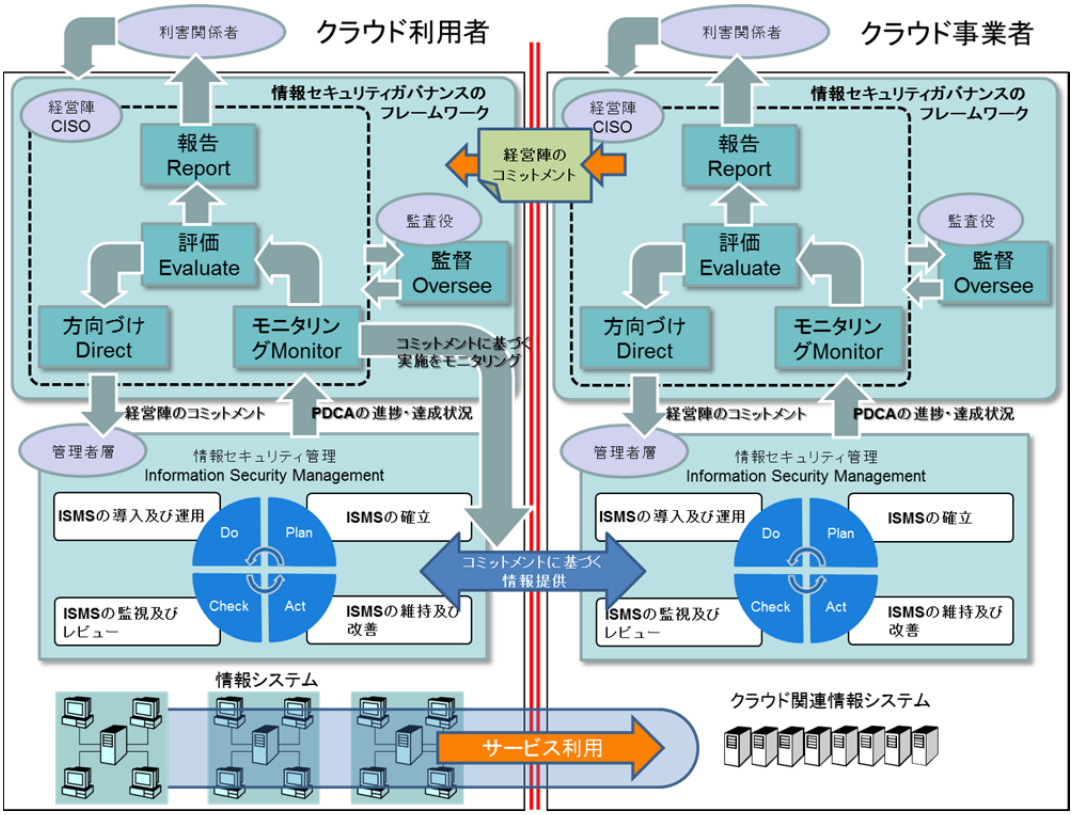


図 2　コミットメントに基づく情報セキュリティガバナンスのフレームワーク

クラウド事業者の経営陣は，クラウド利用者に対し，クラウドサービスの提供にかかわる情報セキュリティのガバナンス及びマネジメントに関するコミットメントを行う。このコミットメントはクラウド事業者の利害関係者たるクラウド利用者への報告（Report）の一部を成すが，一方的な報告ではなく，契約行為を含む双方向のコミットメントが望ましい。

このコミットメントに基づき，クラウド事業者はクラウド事業者の情報セキュリティガバナンスの報告（Report）を約束するとともに，クラウドの活動状況をクラウド利用者に提供することを約束する。

クラウド事業者によるクラウドの活動状況報告より，クラウド利用者は情報セキュリティ活動に必要な情報を入手し，理論的には自組織のシステムの延長のように，クラウドサービスを利用することが可能となる。例えば，クラウド利用者はクラウド事業者からクラウド事業者の情報セキュリティのマネジメントやコントロールにかかわる情報の提供を受け，これをクラウド利用者の点検（Check）の対象に含め，処置（Act）を検討する。処置にはクラウド利用者内で完結するものと，クラウド事業者による情報提供が必要なものがある。クラウド利用者は組織内で完結するものを解決するとともに，クラウド事業者による情報提供が必要な処置をクラウド事業者にフィードバックする。クラウド事業者は自組織内の処置（Act）に加え，クラウド利用者の要望である処置が可能かを検討する。

同様にクラウド利用者はクラウド事業者による情報提供を頼りに，クラウド利用者内の PDCA を実現できるようになる。もちろん，クラウド利用者とクラウド事業者は独立した経営主体であり，かつクラウド事業者は同時に多数のクラウド利用者から，時として矛盾する要望を受けることがあるので，おのずから情報提供の範囲には制約が生じ得る。クラウド利用者は，この制約を見定め受入れるか，又は別のクラウド事業者を求めるかの選択を迫られる場合もあるが，制約の存在を前提とした情報提供は可能であろう。

以上のような制約は存在するものの，一度クラウド利用者の PDCA サイクルが実現すると，クラウド利用者の経営陣の情報セキュリティガバナンス活動の基礎が形成される。クラウド利用者の経営陣は PDCA の進捗・達成状況をモニタリング（Monitor）することができるようになる。またクラウド利用者の経営陣は，クラウド事業者の経営陣から，彼らのコミットメントに基づく情報セキュリティガバナンス報告（Report）を受けることができる。クラウド利用者の経営陣は PDCA のモニタリング結果と，クラウド事業者の情報セキュリティガバナンス報告を基に評価（Evaluate）を行うとともに，クラウドを利用している組織としての報告（Report）を利害関係者に対して行うことができる。この利害関係者の中には，クラウド事業者も含まれる。この形態では，クラウド利用者の経営陣とクラウド事業者の経営陣は双方向に報告を行い，互いの状況を知ることとなる。

さらに，クラウド利用者の経営陣は評価（Evaluate）をベースに，情報セキュリティの経営陣のコミットメントとして，方向づけ（Direct）を行うことができる。この方向づけは，クラウド利用者の管理者の情報セキュリティ管理の入力となるとともに，一部はクラウド事業者への要望書となる。ここでもコミットメントに基づくクラウド利用者の限界が存在するが，クラウド利用者の経営陣の情報セキュリティガバナンス活動をベースとするクラウド事業者の経営陣への要望には，単なる PDCA に基づく要望以上の効力をもつと期待できる。クラウド利用者の経営陣は，方向づけの結果を，PDCA のモニタリングとクラウド事業者の情報セキュリティガバナンス報告から評価をし，最悪の場合，クラウド事業者を別に求めることになる。

以上の情報セキュリティガバナンスのフレームワークの有効性に対して監査役が監督（Oversee）を行う。

クラウド事業者の経営陣は，以上のコミットメントに基づくクラウド利用者に対する情報提供を可能とするための情報セキュリティガバナンスを確立していることをあらかじめ開示していることが望ましい。

4.2　クラウドサービス利用における情報セキュリティマネジメント

4.2.1　クラウドサービス利用におけるリスクアセスメントの留意点

JIS Q 27002（実践のための規範）4.1 によれば，リスクアセスメントは，セキュリティ要求事項及びリスク状況（例えば，資産，脅威，ぜい弱性，影響，リスク評価）の変化に対応できるように，定期的に及び重大な変化が発生したときに実施することが望ましい，とされている。つまり，リスクアセスメントでは，リスク状況の変化を把握することが重要である。

クラウドサービスを利用して組織事業の基礎を成す情報資産を組織内から外部組織に移行した場合には，次のようなリスク状況の変化に着目する必要がある。

クラウドコンピューティングで利用されている技術は，標準化された技術とは限らず，先進的な技術を自ら開発したクラウド事業者によってサービスが構築され，提供されている。そのため，当該事業者以外の専門家が対象技術そのものを評価し，ぜい弱性及び脅威を検証することは行われていない可能性があり，クラウドサービスを構成し，提供する技術そのものがぜい弱性を抱えているという懸念がある。クラウドサービスはクラウド利用者が機器構成内容や利用技術などを直接把握できず，これらの技術を客観的に検証することが難しいため，クラウドサービス上で問題が発生した際の対応計画を容易には構築できないということが情報セキュリティ上の問題とされている。

運用面においては，クラウド利用者とクラウド事業者との信頼関係や，データセンターの立地などにより，これまでのアウトソーシングに関連する情報セキュリティ問題だけではなく，コスト削減などに伴う情報管理の品質確保などの問題も併せて考慮しなければならない。

クラウドサービスを利用することにより直接管理できなくなったシステム，情報，監査ログなどを対象にして，情報セキュリティ対策の変化について検討することが望ましい。

また，クラウドサービスにかかわるリスクには，クラウド利用者自らが責任をもつにもかかわらず管理できない環境にある脅威及びぜい弱性が存在する。

例えば，クラウド利用者がクラウドサービスのすべての監査ログを入手することができないために，クラウドサービスの利用において問題が発生した場合，その原因を特定できず，再発防止のための対策を講じることができないというリスクが想定される。また，クラウドサービスの特徴であるマルチテナントの利用に起因するぜい弱性もある。自らの情報セキュリティ対策が十分であったとしても，実行環境となるゲスト OS が他のゲスト OS と同じハードウェア上に構成されている場合，他のゲスト OS が何らかの攻撃を受けた際に自らも不正アクセスや改ざんなどの被害を受ける可能性がある。

このようにシステムの管理主体がクラウド事業者にあることに起因して生じるぜい弱性については，クラウド利用者が技術的な対策を実施することが難しい。さらに，ネットワークに起因する脅威及びぜい弱性は，クラウドサービスに大きな影響を及ぼすリスクとなり得る。

4.2.2　クラウドサービス利用におけるマネジメントシステムの改善に向けた留意点

JIS Q 27001（要求事項）8.3 によれば，組織は，変化したリスクを特定し，大きく変化したリスクに注意を向けて，予防措置についての要求事項を特定しなければならない，とされている。情報セキュリティマネジメントシステムにおいては PDCA サイクルに基づいて，リスク状況の変化に伴う情報セキュリティ対策の見直しを行い，対策を検討することが求められている。

クラウドサービスではどのようなリスクの変化があり，どのような影響があるかを検討し，新たな情報セキュリティ対策の導入を計画することが望ましい。クラウドサービスの利用において変化するシステム環境，責任の所在，事故や事象の判断基準などを明確にすることで，適切なリスクマネジメントに向けた取組みが可能となる。

4.2.3　このガイドラインの情報セキュリティ監査への活用

JIS Q 27001（要求事項）を満たす情報セキュリティマネジメントによれば，点検（ISMS の監視及びレビュー）が要求される。クラウド事業者が適切な情報セキュリティ対策を実施しているかを点検するには，第三者の評価を利用することが効率的である。第三者の評価とは，情報セキュリティ関連の認定又は情報セキュリティ監査を指す。

しかしながら，クラウド事業者を国際的に認定する制度は整っておらず，これからのクラウド関連技術やビジネスモデルの発展を考慮すると，クラウド事業者に対する認定が実施されるのはまだ先になることが想定される。このような状況を踏まえると，情報セキュリティ監査によってクラウド事業者の情報セキュリティ管理状況の評価を知ることは有用だといえる。

このガイドラインはクラウド利用者が実施することが望ましい事項とクラウド事業者の実施が望まれる事項を示している。このガイドラインをクラウド利用者とクラウド事業者の両者が活用することにより，両者の関係において管理策が共有され，共有された管理策について情報セキュリティ監査を実施することができる（図 3 参照）。

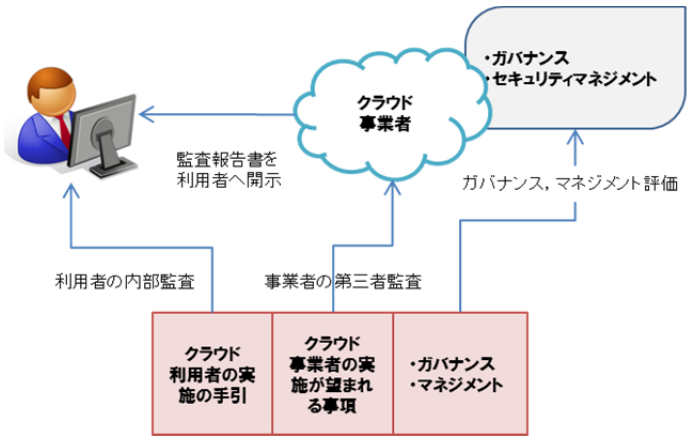


図 3　このガイドラインの監査への活用

4.2.4　このガイドラインのサプライチェーンへの活用

クラウドコンピューティングにおいては IaaS, PaaS 及び SaaS それぞれが関連しあってサプライチェー

ンを形成し，サービス全体を提供することがある。例えば，ある SaaS 事業者が PaaS 事業者のサービスを利用している場合，このガイドラインにおいては，その SaaS 事業者は PaaS の利用者となり，同様に PaaS 事業者が IaaS 事業者のクラウドサービスを利用している場合は，PaaS 事業者が IaaS の利用者となる。クラウドサービスを供給する側が利用する側に回ることで，サービスの供給と利用の連鎖が形成される（図 4 参照）。

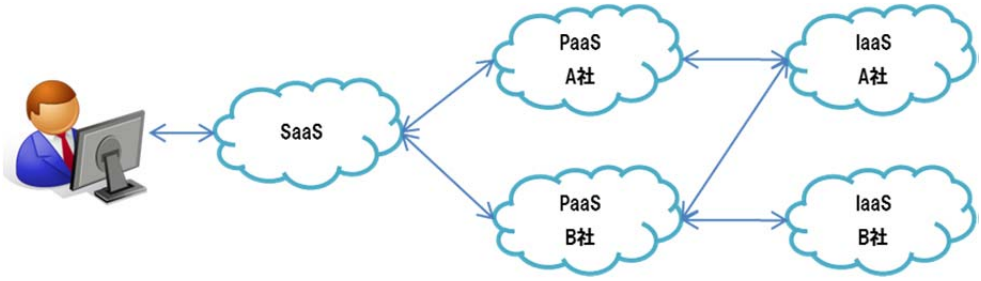


図 4　クラウド事業者のサプライチェーン

サプライチェーンを構成するクラウド事業者は自らの立場をクラウド利用者に置き換えて，このガイドラインの「クラウド利用者のための実施の手引」を自らの組織に活用できるだけでなく，「クラウド事業者の実施が望まれる事項」を自らが利用するクラウドサービスの供給者に対して要請し，サプライチェーンを形成するクラウド事業者の情報セキュリティマネジメントに活用することもできる。

5　セキュリティ基本方針

5.1　情報セキュリティ基本方針

目的：情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。

経営陣は，組織全体にわたる情報セキュリティ基本方針の発行及び維持を通じて，事業目的に沿った明確な情報セキュリティ基本方針の方向性を定め，情報セキュリティに対する支持及び責任を明示することが望ましい。

5.1.1　情報セキュリティ基本方針文書

管理策

情報セキュリティ基本方針文書は，経営陣によって承認され，全従業員及び関連する外部関係者に公表し，通知することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織の情報セキュリティ基本方針の適用範囲にクラウドコンピューティングの利用に関する事項を含めることが望ましい。クラウドコンピューティングの利用に関する情報セキュリティ基本方針は，リスクアセスメント及び次のような事項を考慮して定めることが望ましい。

a)　クラウドコンピューティング環境に保管するクラウド利用者組織の情報資産

b) クラウド事業者がアクセス及び管理するクラウド利用者組織の情報資産

c) クラウドコンピューティング環境においてクラウド利用者が実行するプロセス

d) クラウド利用者組織内のクラウドサービス利用者（一般利用者及び特権利用者）

クラウド利用者は，自らの情報セキュリティ基本方針とクラウド事業者の情報セキュリティ基本方針を比較し，その差異について検討することが望ましい。

クラウド利用者は，クラウド事業者が適切な情報セキュリティ基本方針に反しない管理を行っていることを確認し，その旨を経営陣（又は情報セキュリティ委員会）に報告することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，情報セキュリティ基本方針をクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者の情報セキュリティ管理状況に関する第三者による評価結果（例えば，ISMS 認証取得証明書，外部監査報告書及び内部監査報告書など）や，情報セキュリティ管理に関する取組みについてクラウド事業者が提供する情報（例えば，ホワイトペーパーなど）は，クラウド事業者が情報セキュリティ基本方針に基づき適切な管理を行っていることを確認するための参考となり得る。

5.1.2 情報セキュリティ基本方針のレビュー

管理策

情報セキュリティ基本方針は，あらかじめ定められた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当及び有効であることを確実にするためにレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスを利用することによって重大な変化が発生する場合に，情報セキュリティ基本方針が引き続き適切，妥当及び有効であることを確実にするためにレビューすることが望ましい。特に情報の安全管理について，クラウドサービスの利用によって，自ら管理できない情報が存在する可能性を考慮して，情報セキュリティ基本方針の見直しを行うことが望ましい。

6 情報セキュリティのための組織

6.1 内部組織

目的：組織内の情報セキュリティを管理するため。

組織内において情報セキュリティを導入し，その実施状態を統制するための管理上の枠組みを確立することが望ましい。

経営陣は，情報セキュリティ基本方針を承認し，セキュリティに対する役割を割り当て，組織全体にわたるセキュリティの実施を調整し，レビューすることが望ましい。

必要ならば，専門的な情報セキュリティの助言の出所を明らかにし，組織内で利用できるようにすることが望ましい。業界の動向に遅れないようにし，規格及び評価方法に目を配り，情報セキュリティインシデントに対処するときの適切な連絡窓口を確保するために，関係当局を含む，外部のセキュリティ専門家又はその一団との連絡網を築くことが望ましい。情報セキュリティに対して多角的に取り組むことが望ま

しい。

6.1.1　情報セキュリティに対する経営陣の責任

管理策

経営陣は，情報セキュリティの責任に関する明りょうな方向づけ，自らの関与の明示，責任の明確な割当て及び承認を通して，組織内におけるセキュリティを積極的に支持することが望ましい。

クラウド利用者のための実施の手引

経営陣は，クラウドサービスの利用における情報セキュリティについて組織を横断する役割及び責任を明確にし，組織全体としての責任者を割当て，承認することが望ましい。

クラウドサービスの関連情報

クラウドサービスを利用した場合でも，情報セキュリティ管理全般に関するクラウド利用者の経営陣の責任は変化しない。しかしながら，クラウドサービスの内容（例えば，システム構成，契約内容など）を把握し，どのようなリスクが伴うのかについては，クラウド利用者の経営陣は十分に理解しておくことが期待される。クラウドサービスの利用における責任の所在が明確になるように，クラウド利用者の経営陣は情報システム環境の全体像を把握しておくことが期待される。

6.1.2　情報セキュリティの調整

管理策

情報セキュリティ活動は，組織の中の，関連する役割及び職務機能をもつ様々な部署の代表が，調整することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用における組織の責任者を明確にし，情報セキュリティ委員会などの調整活動に参加させることが望ましい。クラウド利用者は，クラウドサービス利用における責任者を定め，情報セキュリティ管理者一覧などに追記することが望ましい。クラウドサービス利用におけるクラウド利用者の責任者は経営陣（又は情報セキュリティ委員会など）によって承認されることが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においては，情報システムの構築や利用に関する契約などが多者にわたる可能性があり，責任者を明確に決めて管理を行う必要がある。また，クラウドサービスに関する様々な情報を集約し様々な判断をする必要があるため，クラウドサービス利用における責任者は情報セキュリティ委員会などの組織の調整活動に参加することが期待される。

6.1.3　情報セキュリティ責任の割当て

管理策

すべての情報セキュリティ責任を，明確に定めることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用における情報セキュリティに関するクラウド利用者及びクラウド事業者の責任分界を確認することが望ましい。クラウド利用者は，情報セキュリティ責任について，クラウド利用者だけでは対応できない内容を明確にすることが望ましい。

クラウド利用者は，クラウド事業者の問合わせ窓口を確認し，窓口情報を最新に保つとともに，クラウ

ドサービス利用におけるリスクを識別・管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者，クラウド事業者及びインフラ事業者の間の責任分界を明確にし，文書化することが望ましい。

クラウド事業者は，クラウドサービスの情報セキュリティに関する窓口を明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおいては，情報セキュリティに関する一部の業務がクラウド事業者に委任される。しかしながら，情報セキュリティに関する全体の責任はクラウド利用者に残ったままであるため，クラウド事業者が情報セキュリティに関する業務を正しく実行していることを，クラウド利用者が判断することが期待される。また，個人が情報セキュリティに責任をもつ領域がクラウドサービスによって変化をする場合（例えば，ID 管理が一元化できずにパスワードの変更を個人が配慮して行わなければならないなど）には，クラウド利用者はその責任範囲を明確にし，クラウドサービスの利用者に伝えなければならない。

多くの場合には情報セキュリティ責任者は組織のすべての情報セキュリティに責任をもつが，クラウドサービスは多様性を有しており，これらのすべてを把握することは困難であることが想定される。このような場合は，情報セキュリティ責任者の補助としてクラウドセキュリティ責任者又は担当者を置くことを検討する必要がある。

データの管理責任，アクセス制御及びインフラ管理などに関する役割及び責任の定義が曖昧な場合，ビジネス上の若しくは法的な問題が引き起こされる恐れがある。

6.1.4　情報処理設備の認可プロセス

管理策

新しい情報処理設備に対する経営陣による認可プロセスを定め，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，新たに利用する機器などを経営陣が認可するプロセスに，クラウドサービスを含めることが望ましい。クラウド利用者は，クラウドサービスの利用認可プロセスを策定することが望ましい。クラウド利用者は，クラウドサービスの利用認可プロセスを文書化することが望ましい。クラウドサービスの利用認可プロセスは，クラウド利用者の経営陣によって承認されることが望ましい。また，セキュリティ要求事項を満たしていることを確認するために情報セキュリティ委員会からも承認を得ることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスの受入れを行うために必要な資料を作成し，提供することが望ましい。クラウド事業者は，SLA など，サービス開始前の合意事項を明確にすることが望ましい。クラウド事業者は， SLA など，サービス開始前の合意事項をクラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

IaaS や PaaS の利用においては，既存の情報システム調達及び構築の標準や手順が適用可能な場合があ

る。SaaS では，アプリケーションのカスタマイズがクラウド利用者にとって容易ではないために，これまでの認可プロセスの標準に合致しない場合もある。その場合は，受入れについての標準や手順を再度検討し，標準の変更又は特例措置の検討を行う必要がある。

6.1.5　秘密保持契約

管理策

情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報保護に対する組織の必要を反映する秘密保持契約をクラウド事業者と締結することが望ましい。クラウド利用者は，クラウド事業者との契約に必要な秘密保持契約の内容が含まれていることを確認することが望ましい。もし必要な事項が含まれていない場合は，別途，秘密保持契約を締結することが望ましい。クラウド利用者は，クラウド事業者との秘密保持契約に「保護される情報の定義」が記載されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者との契約時には秘密保持契約を締結することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においてはコンピュータ資源をネットワーク上（多くの場合はクラウド事業者のデータセンター）に配置しているが，データの所在などをクラウド利用者が特定することは技術的に難しい。クラウド利用者がすべての情報を適切に管理するためにも，重要な情報を双方が正しく認識し，協力しあうことが期待される。

6.1.6　関係当局との連絡

管理策

関係当局との適切な連絡体制を維持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者の監督官庁，管轄裁判所，関連団体，相談窓口などを確認することが望ましい。クラウド利用者は，利用するクラウド事業者の監督官庁，関連団体を調査し，事故発生時の連絡リストに追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスの情報セキュリティに関して関連する監督官庁などを明確にし，開示することが望ましい。クラウド事業者は，個人情報の保護に関して監督官庁などを明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウド利用者が複数のクラウド事業者と個別に契約し，複数のクラウドサービスを組み合わせて利用する場合には，それぞれのクラウド事業者の責任を明確にする必要がある。特に，様々なクラウドサービスを利用して一つのクラウドサービスとして提供する場合には，責任の切り分けが難しい場合もあるが，利用の前に責任分界点を明確にし，障害などに対応できるようにすることが期待される。

6.1.7　専門組織との連絡

管理策

情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持することが望ましい。

クラウドサービスの関連情報

クラウド利用者及びクラウド事業者は，次のような組織などを調査し，クラウドサービスに関する情報収集の対象とすることが期待される。

a) クラウドサービスを専門とする，又はクラウドサービスに関連する団体や組織
b) クラウドサービスの事業者団体
c) クラウドサービスに関連する省庁や団体
d) クラウドサービス関連のニュースソース

クラウドサービスでは，IaaS，PaaS，SaaS がサービスを共有して構成されている場合がある。例えば，複数の SaaS 事業者が同じ PaaS や IaaS を利用していたり，一つの SaaS 事業者が複数の PaaS を利用したりしている場合などがそれにあたる。この場合，クラウド事業者は，どのクラウド事業者のどのサービスを利用しているのかをクラウド利用者に開示することが望ましい。事前にこうした情報が開示されていれば，クラウド利用者は，あらかじめクラウドサービスやクラウド事業者の事故などが発生したときの影響と対策を検討することが可能になる。

6.1.8　情報セキュリティの独立したレビュー

管理策

情報セキュリティ及びその実施のマネジメントに対する組織の取組み（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）について，あらかじめ計画した間隔で，又はセキュリティの実施に重大な変化が生じた場合に，独立したレビューを実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティに関するマネジメントレビューにおいて，組織が保有する情報システムと同様に，クラウドサービスに関する事項を追加することが望ましい。クラウド利用者は，情報セキュリティに関するマネジメントレビューの計画書にクラウドサービスを追加することが望ましい。クラウド利用者は，リスクアセスメントに基づき，クラウドサービスを情報セキュリティ監査の対象に追加することが望ましい。

クラウドサービスの関連情報

クラウド利用者が，マネジメントレビューのための情報を提供する場合，クラウド事業者からクラウドサービスに関する情報を定期的に入手することが難しい場合がある。特にマルチテナントでクラウドサービスが展開されているクラウドサービスを利用している場合には，ログから得られる情報をクラウド事業者から提供してもらうために想定以上に時間を要する場合がある。そのため，事前にマネジメントレビューに必要な情報を精査し，それらの情報を得ることが可能であるかどうか，可能である場合は，必要な期間も併せてクラウド事業者に確認することが期待される。

6.2　外部組織

目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。

外部組織の製品又はサービスの導入によって，組織の情報及び情報処理施設のセキュリティが弱められることは望ましくない。

外部組織による組織の情報処理施設へのアクセス，並びに情報の処理及び通信を管理することが望ましい。

組織の情報及び情報処理施設へのアクセスを要求する外部組織との活動が業務上必要となる場合，又は外部組織との間で製品及びサービスの受入れ若しくは提供を行う場合には，セキュリティ関連事項を決定し，要求事項を管理するためにリスクアセスメントを実施することが望ましい。管理策は，その外部組織との間で合意し，契約書に明記することが望ましい。

6.2.1　外部組織に関係したリスクの識別

管理策

外部組織がかかわる業務プロセスからの，組織の情報及び情報処理施設に対するリスクを識別し，また，外部組織にアクセスを許可する前に適切な管理策を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，外部組織がかかわる業務プロセスの一つとしてクラウドサービスの利用を考慮することが望ましい。クラウド利用者は，業務プロセスへのクラウドサービスの関与と影響を特定することが望ましい。

クラウド利用者は，クラウドサービスの利用により生じる情報セキュリティに対するリスクを識別・検討し，必要に応じてクラウドサービスの利用を開始する前に管理策を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者の情報セキュリティに重大な影響を与えると考えられるリスクを定義し，クラウド利用者にその情報を提供することが望ましい。

クラウド事業者がクラウド利用者と合意した場合，クラウド事業者は，クラウドサービスにおける情報セキュリティ対策や作業状況に関する情報（例えば，データの完全消去作業の実施報告書）を提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者が開示する情報セキュリティ対策の内容は，多くの場合は限定的，抽象的なものであることに留意する。リスクを特定することが困難な場合に，クラウド利用者が実施できる有効な管理策の一つに情報の暗号化がある。

クラウド利用者は，組織の一般的な情報セキュリティリスクに加え，クラウド固有のリスクを情報セキュリティ リスクアセスメントプロセスの入力として含め，オンプレミスの情報システムとクラウドサービスとの間でリスクの違いを評価することが望ましい。なお，クラウドサービスにおいて考慮すべきリスクには次のようなものがある。

a) クラウド利用者の情報は，クラウド事業者が所有するハードウェアに格納されるため，クラウド

利用者は直接管理することができない。

b) クラウド事業者は，他のクラウド事業者が提供するクラウドサービスを利用してクラウドサービスを提供している場合があり，責任分界が曖昧である恐れがある。

c) 他のクラウド利用者と同一のコンピュータ環境を共用する場合があり，他のクラウド利用者の利用する環境との論理的な分割が適切に行われない恐れがある。

d) 一般的に，クラウドサービスの利用終了後，サービス利用中に使用されていたシステムリソースは再利用されるため，サービス利用終了後のデータ消去が適切に行われない場合，他のクラウド利用者によってデータがアクセスされる恐れがある。

情報セキュリティリスクは，クラウドサービスの利用によって高まる場合もあれば，低下する場合もある。クラウドサービスの利用においては，情報セキュリティ管理策の可視性及び情報セキュリティ管理レベルの達成度が限定されること，及び，リスクの識別が困難である傾向があることに留意する必要がある。

6.2.2 顧客対応におけるセキュリティ

管理策

顧客に組織の情報又は資産へのアクセスを許す前に，明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者が顧客に組織の情報又は資産へのアクセスを許可するために明確にしていたセキュリティ要求事項について，クラウドサービスを利用することによって変化するセキュティ要求事項を明確にし，明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。

クラウド利用者がセキュリティ要求事項の明確化を行うにあたっては，クラウドサービスの利用に伴い生じる顧客の作業及びリスクを識別することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド利用者が，クラウドサービスの利用に際してセキュリティ要求事項の順守状況を確認できるよう，クラウド事業者は，サービスの詳細に関する情報を提供することが望ましい。

クラウドサービスの関連情報

自らの顧客に内部統制報告の責任を負うクラウド利用者は，顧客に対して内部統制の報告を行うにあたり，クラウド事業者の情報セキュリティ監査報告書の入手が必要か否か，及び入手が可能かについてクラウドサービスの利用を開始する前に検討しておく必要がある。

クラウド利用者は，次の点について顧客に明示しておくことが期待される。

a) 個人情報保護法などの法令に基づき，利用者の同意なくクラウドコンピューティング環境上の情報への顧客のアクセスが制限される場合がある。

b) クラウド事業者は，他のクラウド利用者に情報が漏えいするリスクを完全に排除できない場合であっても，クラウド利用者に対してアクセスを付与する場合がある。

6.2.3 第三者との契約におけるセキュリティ

管理策

組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，

又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。

7　資産の管理

7.1　資産に対する責任

目的：組織の資産を適切に保護し，維持するため。

すべての資産を明らかにし，その管理責任者を指名することが望ましい。

管理責任者をすべての資産について明確にし，適切な管理策を維持する責任を割り当てることが望ましい。組織が適切と判断した場合には，管理責任者は具体的な管理策の実施を委任してもよいが，資産の適切な保護に関する責任は管理責任者にとどまる。

7.1.1　資産目録

管理策

すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドコンピューティング環境にある組織の資産を資産管理の適用範囲に含めることが望ましい。クラウド利用者は，資産目録にクラウドサービス名及びクラウド事業者名を追加することが望ましい。

クラウド利用者は，クラウド利用者による資産管理を支援する機能がクラウドサービスに付帯するかを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産に関する資産目録の一覧を取得できる機能をクラウド利用者に提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者は大規模な IaaS の上で PaaS や SaaS を展開している場合があり，クラウド利用者がクラウドサービスに関連するシステムのすべてを資産目録に詳細に記載することは困難である。また，データ管理のために様々なメタデータ（データに関する情報）などが付与されており，これらのすべてをクラウド利用者が管理することも困難である。しかしながら，クラウド利用者は，自らがクラウドコンピューティング環境においたデータやプログラムなどを資産目録に記載することは可能であり，これらをもれな

く記載することが期待される。

クラウドサービス環境にあるクラウド利用者の資産には，次のようなものがある。

a) 業務上の情報

b) 仮想化された装置

c) 仮想化されたストレージ

d) ソフトウェア

クラウド利用者の資産の種類はｑ，クラウドサービスに応じて多岐にわたる。例えば，SaaS 事業者が，提供する SaaS のインフラに IaaS を利用している場合，SaaS 事業者はクラウド利用者であり，SaaS において容量・能力及び資源などの監視・調整に使用するソフトウェアは，IaaS 事業者から見ると，自社の提供する IaaS サービス上にあるクラウド利用者の資産と解される場合がある。

7.1.2 資産の管理責任者

管理策

情報及び情報処理施設と関連する資産のすべてについて，組織の中に，その管理責任者を指定することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，資産目録の管理責任者の項目にクラウドサービスに関連する項目を追加することが望ましい。

資産の管理責任者は，クラウドコンピューティング環境上の資産に関して次の責任をもつことが望ましい。

a) 情報及び情報処理に関連する資産が適切に分類されていることを確実にする。

b) 複数のクラウドサービスを連携し情報処理を行う場合には，適切な処理を管理するための方針，プロセス及び手順を定め，定期的に見直す。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産の責任者を明確にし，顧客対応のエスカレーションプロセスに追加することが望ましい。

7.1.3 資産利用の許容範囲

管理策

情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用するクラウドサービスごとに，どの資産が利用可能か，リスクアセスメントを行い，利用の許容範囲を明確にすることが望ましい。クラウド利用者は，クラウドサービスごとに，資産の利用可能性について検討することが望ましい。

7.2 情報の分類

目的：情報の適切なレベルでの保護を確実にするため。

情報の必要性，優先順位及びその情報を取り扱う場合に期待する保護の程度を示すために，情報を分類することが望ましい。

情報の，取扱いに慎重を要する度合い及び重要性の度合いは様々である。情報によっては，保護レベルの引上げ又は特別な取扱いが必要なこともある。情報の分類体系は，一連の適切な保護レベルを定め，特別な取扱い方法の必要性を伝えるために利用することが望ましい。

7.2.1　分類の指針

管理策

情報は，組織に対しての価値，法的要求事項，取扱いに慎重を要する度合い及び重要性の観点から分類することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報分類の指針にクラウドサービスを考慮した分類項目を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，データの分類項目を明示することが望ましい。クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報がどのように分離されて管理されているかを明確にし，開示することが望ましい。

クラウドサービスの関連情報

データの分類項目の例として，以下のようなものがある。

－データのタイプ
－データ源の管轄裁判所
－コンテキスト（背景や位置づけなど）
－法的制約
－契約上の制約
－価値，機微性
－組織における重要度
－第三者による不正を防止する義務
－許可されない開示や誤用に関する事項
など

7.2.2　情報のラベル付け及び取扱い

管理策

情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで利用する資産についてもラベル付けやマーキングができる仕組みを作ることが望ましい。クラウド利用者は，ラベル付けやマーキングをクラウドサービスの利用者が実施できるように手順書を作成することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を分類するためにフォルダ分類やラベル付け機能を提供することが望ましい。クラウド事業者は，クラウド利用者との合意に基づき，ラベル付け機能について次の情報を提供することが望ましい。

a) ラベル付けを行うための機能

b) ラベル付けのカスタマイズを行うための機能

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を一時的に分類するためにマーキングなどの機能を提供することが望ましい。

クラウドサービスの関連情報

SaaS や PaaS では標準的なオペレーティングシステムではなく，クラウド事業者独自のオペレーティングシステムを利用している場合がある。その場合，情報管理において使い慣れたインタフェースを利用することができず，情報のラベル付けの手段で対応できないことがある。利用するクラウドサービスのインタフェースを正しく理解して，利用者が自らラベル付けやマーキングができるように手順を見直す必要がある。

8 人的資源のセキュリティ

8.1 雇用前

目的：従業員，契約相手及び第三者の利用者がその責任を理解し，求められている役割にふさわしいことを確実にするとともに，盗難，不正行為又は施設の不正使用のリスクを低減するため。

セキュリティの責任は，雇用に先立って，適切な職務定義書及び雇用条件において，言及することが望ましい。

従業員，契約相手及び第三者の利用者のすべての候補者について，十分に審査することが望ましい。特に，慎重を要する業務に就く者については，そうすることが望ましい。

従業員，契約相手及び情報処理施設の第三者の利用者は，セキュリティの役割及び責任についての契約書に署名することが望ましい。

8.1.1 役割及び責任

管理策

従業員，契約相手及び第三者の利用者のセキュリティの役割及び責任は，組織の情報セキュリティ基本方針に従って定め，文書化することが望ましい。

8.1.2 選考

管理策

従業員，契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は，関連のある法令，規則及び倫理に従って行うことが望ましい。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行われることが望ましい。

8.1.3 雇用条件

管理策

従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名することが望ましい。

8.2　雇用期間中

目的：従業員，契約相手及び第三者の利用者の，情報セキュリティの脅威及び諸問題，並びに責任及び義務に対する認識を確実なものとし，通常の業務の中で組織の情報セキュリティ基本方針を維持し，人による誤りのリスクを低減できるようにすることを確実にするため。

経営陣の責任は，組織内の構成員全体にセキュリティを適用することを確実にするために，明確にすることが望ましい。

起こり得るセキュリティリスクを最小とするために，すべての従業員，契約相手及び第三者の利用者にセキュリティ手順及び情報処理設備の正しい利用方法に関する十分なレベルの意識，教育及び訓練を与えることが望ましい。セキュリティ違反の取扱いに関する正式な懲戒手続を設けることが望ましい。

8.2.1　経営陣の責任

管理策

経営陣は，組織の確立された方針及び手順に従ったセキュリティの適用を，従業員，契約相手及び第三者の利用者に要求することが望ましい。

8.2.2　情報セキュリティの意識向上，教育及び訓練

管理策

組織のすべての従業員，並びに，関係するならば，契約相手及び第三者の利用者は，職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け，また，定めに従ってそれを更新することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，組織のすべての従業員，契約相手及び第三者の利用者を対象にした教育・訓練の範囲に，組織が保有する情報システムと同様に，クラウドサービスの情報セキュリティに関する事項を加えることが望ましい。クラウド利用者は，クラウドサービスの利用において必要な職務に関連する組織に対して，クラウドサービス利用に関する情報セキュリティの方針及び手順について，適切な意識向上のための教育・訓練の内容を盛り込むことが望ましい。

クラウドサービスの情報セキュリティに関する教育・訓練は，利用者のリテラシーレベルや認知度に応じた内容とし，次のような内容を追加することが望ましい。

a) クラウドサービス利用のための方針，基準及び手順などの規程類
b) クラウドサービスごとの情報セキュリティリスク及びその対策
c) クラウドサービスを使用するにあたり考慮すべきシステム及びネットワーク環境におけるリスク

クラウド利用者は，組織におけるクラウドサービス利用に関する教育，訓練及び意識向上プログラムの実施にあたり，利用するクラウドサービスの操作マニュアル，予防措置及び連絡先に関する情報提供を，

必要に応じてクラウド事業者に要求することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスに関する情報セキュリティ教育，訓練及び意識向上プログラムを実施するにあたり，自社が提供するクラウドサービスの操作マニュアル及び連絡先情報を必要に応じて提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者とクラウド事業者の作業が重複する点は，お互いにおいて，教育を行い，訓練を協調して行うことが期待される。

8.2.3 懲戒手続

管理策

セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスに携わる者を懲戒した場合に，利用者に情報セキュリティ上の影響がある場合は，懲戒の内容を連絡する必要があることに留意する。

8.3 雇用の終了又は変更

目的：従業員，契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。

責任者は，従業員，契約相手及び第三者の利用者の組織からの離脱を管理し，すべての装置の返却及びすべてのアクセス権の解除の完了を確実にすることが望ましい。

組織内の責任及び雇用の変更は，この箇条に沿って対応する責任又は雇用の終了として管理することが望ましい。また，新規の雇用は，8.1 に示すとおりに管理することが望ましい。

8.3.1 雇用の終了又は変更に関する責任

管理策

雇用の終了又は変更の実施に関する責任は，明確に定め，割り当てることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの提供終了や事業終了に伴う義務を明確に定義することが望ましい。

8.3.2 資産の返却

管理策

すべての従業員，契約相手及び第三者の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産すべてを返却することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，すべての従業員，契約相手及び第三者の利用者が，雇用，契約又は合意の終了時に返却する自らが所持する組織の資産に，クラウドサービスを加えることが望ましい。クラウド利用者は，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産をクラウド利用者が管理でき

る機能を，自らの資産の返却プロセスに組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，リモート環境から利用可能なクラウドサービスについては，資産の返却時期に特に留意する必要がある。

8.3.3　アクセス権の削除

管理策

すべての従業員，契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用者に対するアクセス権を，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することを，自らのアクセス権の管理プロセスに組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの利用者に対するアクセス権を，クラウド利用者が，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者との契約内容によっては，クラウドサービスの利用者との雇用，契約又は合意の終了後も，そのアクセス権を一定期間失効させることができない可能性があることに留意する必要がある。

9　物理的及び環境的セキュリティ

9.1　セキュリティを保つべき領域

目的：組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。

重要又は取扱いに慎重を要する情報処理設備は，適切なセキュリティ障壁及び入退管理を伴う明確なセキュリティ境界によって保護された，セキュリティが保たれた領域の中に設置することが望ましい。これらの設備は，認可されていないアクセス，損傷及び妨害から，物理的に保護することが望ましい。

取る保護は，識別されたリスクに相応することが望ましい。

9.1.1　物理的セキュリティ境界

管理策

情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界（例えば，壁，カード制

御による入口，有人の受付）を用いることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，複数のデータセンターを利用する場合にセキュリティの保護に差異が生じないように留意し，物理セキュリティ境界を用いることが期待される。

クラウド事業者は，クラウド利用者に対する情報提供に伴う情報セキュリティリスクを考慮し，取扱いに慎重を要する情報が露見しないよう，物理的セキュリティ境界及び関連する管理策に関する情報（例えば，データセンターの所在地，物理的アクセスの管理策など）の開示範囲を決定する必要がある。

9.1.2　物理的入退管理策

管理策

セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンターなどの間でデータを交換する場合，共通の物理的入退管理策が講じられたセキュリティエリアでデータが交換される必要があることに注意を要する。

9.1.3　オフィス，部屋及び施設のセキュリティ

管理策

オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，オフィス，部屋及び施設に対する物理的セキュリティに関する指針に差異が発生しないように留意することが期待される。

9.1.4　外部及び環境の脅威からの保護

管理策

火災，洪水，地震，爆発，暴力行為，及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し，適用することが望ましい。

9.1.5　セキュリティを保つべき領域での作業

管理策

セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し，適用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスを利用する場合に，セキュリティを保つべき領域が拡大しないか確認し，セキュリティを保つべき領域が拡大する場合は，作業に関する物理的な保護及び指針を設計し，適用することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスによって，クラウド利用者の利用環境を拡大させるような機能が存在する場合は，その機能を開示することが望ましい（例えば，モバイルコンピューティングからの利用が可能になる，など）。

9.1.6　一般の人の立寄り場所及び受渡場所

管理策

一般の人が立ち寄る場所（例えば，荷物などの受渡場所）及び敷地内の認可されていない者が立ち入ることもある場所を管理し，また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離すことが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンターなどの間でデータを交換する場合，一般の人の立寄り場所及び受渡場所に関する指針に差異が発生しないように留意することが期待される。

9.2　装置のセキュリティ

目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。

装置は，物理的及び環境的脅威から保護することが望ましい。

装置（構外で用いるもの及び移動するものを含む。）の保護は，情報への認可されていないアクセスのリスクを低減し，損失又は損傷から情報を保護するために必要である。装置の保護に関しては，装置の設置場所及び処分についても考慮することが望ましい。物理的な脅威から保護するため，また，サポート設備（例えば，電源，ケーブル配線施設）を保護するために，特別な管理策が要求される場合がある。

9.2.1　装置の設置及び保護

管理策

装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，機器や，データセンターなどの間でデータを交換する場合，装置の設置及び保護の管理策に差異が発生しないよう留意することが期待される。

9.2.2　サポートユーティリティ

管理策

装置は，サポートユーティリティの不具合による，停電，その他の故障から保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，機器や，データセンターなどの間でデータを交換する場合，サポートユーティリティの保護に差異が発生しないよう留意することが期待される。

9.2.3　ケーブル配線のセキュリティ

管理策

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受又は損傷から保護することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンター間でデータを交換する場合，データセンターごとのケーブル配線のセキュリティに差異が生じないように留意することが期待される。

9.2.4　装置の保守

管理策

装置は，可用性及び完全性を継続的に維持することを確実とするために，正しく保守することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，データセンター間でデータを交換する場合，データセンターごとの保守の差異が生じないように留意することが期待される。

9.2.5　構外にある装置のセキュリティ

管理策

構外にある装置に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用することが望ましい。

9.2.6　装置の安全な処分又は再利用

管理策

記憶媒体を内蔵した装置は，処分する前に，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又は問題が起きないように上書きしていることを確実にするために，すべてを点検することが望ましい。

クラウドの利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用を終了した場合，使用されていた機器などが再利用されることに留意することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，バックアップを含め，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを含む情報の取扱いに留意することが望ましい。クラウド事業者は，記憶媒体を内蔵した装置を処分する場合には，記録された情報を復元できないように安全に処分することが望ましい。また，記憶媒体を内蔵した装置を再利用する場合には，機密情報の漏えいに対する対策を実施することが望ましい。

9.2.7　資産の移動

管理策

装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい。

クラウドの利用者のための実施の手引

クラウド利用者は，クラウドサービスでは，事前にクラウド利用者の許可なく，データの物理的な所在が移動される可能性があることに留意することが望ましい。

10　通信及び運用管理

10.1　運用の手順及び責任

目的：情報処理設備の正確，かつ，セキュリティを保った運用を確実にするため。

すべての情報処理設備の管理及び運用のための責任体制及び手順を確立することが望ましい。この手順

には，適切な操作手順の策定を含む。

不注意又は故意によるシステムの不正使用のリスクを低減するために，適切ならば，職務の分割を実施することが望ましい。

10.1.1 操作手順書

管理策

操作手順は，文書化し，維持していくことが望ましい。また，その手順は，必要とするすべての利用者に対して利用可能とすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用するクラウドサービスの操作手順を作成することが望ましい。クラウド利用者は，手順書作成にあたり，クラウド事業者の情報提供方針を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がクラウドサービスの操作手順を作成する際の情報提供に関する方針を定め，クラウド利用者に提示することが望ましい。クラウド事業者による情報提供の例として，次のようなものがある。

a) 利用者向け操作手順書の提示

b) 問合せ窓口

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，サービスの変更が一斉に行われ，操作手順の変更が発生する可能性があることに留意することが期待される。

クラウド利用者が他のクラウドサービスを利用して内部又は外部の利用者にサービスを提供する場合（例えば，IaaS を利用して SaaS を提供する場合など），クラウド利用者は，サービス仕様及びサービスレベルの提供を維持するためにクラウド事業者に対して，システム及びサービスに関する変更情報を要求することが想定される。

10.1.2 変更管理

管理策

情報処理設備及びシステムの変更は，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者からクラウド利用者に影響が及ぶ情報処理設備及びシステムの変更の通知を受けた場合は，その影響を確認し，記録することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更において，クラウド利用者に影響を及ぼすものをあらかじめ定義し，クラウド利用者に通知することが望ましい。クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更においてクラウド利用者に通知する項目並びに変更履歴を，クラウドサービスの利用を検討する者及びクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，情報処理設備及びシステムの変更が一斉に行

われ，個別の環境や条件が考慮されない可能性に留意することが望ましい。クラウド利用者，クラウド事業者ともに，IaaS などで利用される仮想化環境では，資産調達と連動せずに機器（例えば，仮想マシンなど）やソフトウェアのライセンスなどの追加が可能になることに留意することが期待される。

クラウド事業者がクラウド利用者に通知する項目の例として，次のようなものがある。

a) システム変更の実施予定日時

b) システム変更の内容

- 新規ソフトウェアのインストール又はパッチの適用
- ハードウェア変更
- ネットワーク変更
- ソフトウェア変更
- サービスの変更
- サブプロバイダの変更
- システムの物理的な移動

c) 変更に関するリスク評価

d) システム変更の開始及び完了の通知

e) 事前の取決めに基づく確認又は承認

10.1.3 職務の分割

管理策

職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分割することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，分割すべき職務及び責任範囲を特定し，分割することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，クラウド利用者において分割することが望ましい職務及び責任範囲（例えば，ID の使用者と登録者など）を明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおいては，クラウド利用者にとって重要な処理であっても，職務の分割が技術的に実装されていない場合は，クラウド利用者は，職務の分割を運用で実装することが求められる場合がある。

10.1.4 開発施設，試験施設及び運用施設の分離

管理策

開発施設，試験施設及び運用施設は，運用システムへの認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，開発，試験及び運用環境を分離するため，必要に応じて仮想環境を利用することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，開発施設，試験施設及び運用施設の分離が，物理的に困難である可能性に留意することが期待される。

10.2 第三者が提供するサービスの管理

目的：第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。

組織は，提供されるサービスが第三者と同意したすべての要求事項を満たしていることを確実にするために，合意の実施状況を点検し，その合意への順守状況を監視し，また，順守状況の変化を管理することが望ましい。

10.2.1 第三者が提供するサービス

管理策

第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルが，第三者によって実施，運用及び維持されることを確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者が，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係するほかのクラウド事業者など。以下同じ。）が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルが，クラウド事業者によって実施，運用及び維持されることを，確実にしていることを確認することが望ましい。クラウド利用者は，クラウド事業者が，第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルによって，クラウド利用者が影響を受ける可能性についてあらかじめ考慮していることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供しているクラウドサービスにおいて利用している第三者が提供するサービスのうち，利用者の情報セキュリティ管理に影響のあるものを開示することが望ましい。

クラウド事業者は，第三者が提供するサービスにおけるセキュリティ管理策，サービスの定義及びサービスレベルをクラウド利用者が定期的にレビューできるよう，必要に応じて次のような情報を提供することが望ましい。

a) 情報セキュリティに係るサービス運用報告書
b) 情報セキュリティに係る監査報告書
c) サービスレベル報告書

クラウド事業者は，提供するクラウドサービスがサプライチェーンを形成する場合には，リスク管理に関する目標を他の事業者に提示し，各事業者に対してリスク管理の実施及び目標の達成を求めることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウド事業者の提供するクラウドサービスが特に依存する第三者サービスがないか（例えば，第三者のPaaS を利用した SaaS サービスであるか，など）留意することが期待される。

クラウド事業者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，お互いに実施したり，協同で実施したりすべきことに留意し，円滑な運用を図ることが期待される。

10.2.2 第三者が提供するサービスの監視及びレビュー

管理策

第三者が提供するサービス，報告及び記録は，常に監視し，レビューすることが望ましい。また，監査も定期的に実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者によって，第三者が提供するサービス，報告及び記録が，常に監視され，レビューされていることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて，クラウド事業者によって，第三者が提供するサービスが，監査されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供しているクラウドサービスについて，クラウド利用者に対して次のような情報提供を必要に応じて行うことが望ましい。

d) 第三者が提供するサービス，報告及び記録を，常に監視し，レビューしていることの開示
e) 第三者が提供するサービス，報告及び記録を，常に監視し，レビューした記録の明示
f) 第三者が提供するサービスを監査していることの開示
g) 第三者が提供するサービスを監査した結果をまとめた報告書などの提示

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウドサービスが連鎖していること（例えば，IaaS を利用した PaaS を利用した SaaS サービスである，など）に留意することが期待される。

10.2.3 第三者が提供するサービスの変更に対する管理

管理策

関連する業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，サービス提供の変更（現行の情報セキュリティ方針，手順及び管理策の保守・改善を含む。）を管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，クラウド事業者の利用する第三者のサービス提供の変更が影響を及ぼす可能性を確認することが望ましい。

クラウド利用者は，組織の情報セキュリティに影響を与える可能性のあるクラウド事業者の利用する第三者のサービス提供の変更について，クラウド利用者の変更管理プロセスに基づき，必要な対応を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，第三者のサービス提供の変更による影響を管理することが望ましい。

クラウド事業者は，組織の情報セキュリティに影響を与える可能性のある，クラウド事業者の利用する第三者のサービス提供の変更について，クラウド利用者への通知の方針を定め，クラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウド事業者が，第三者のサービスの変更に関してクラウド利用者に通知する事項の例として，次のようなものがある。

a) システム変更の実施予定日時
b) システム変更の内容
c) 変更に関するリスク評価
d) システム変更の開始及び完了の通知
e) 事前の取決めに基づく確認又は承認

クラウド利用者は，クラウドサービスの環境においては，様々な階層のサービスが複雑に作用するため，クラウドサービスが連鎖していること（例えば，IaaS を利用した PaaS を利用した SaaS サービスである，など）に留意することが期待される。

10.3 システムの計画作成及び受入れ

目的：システム故障のリスクを最小限に抑えるため。

必要とされるシステム性能を満たす十分な容量及び資源の可用性を確実にするためには，事前の計画及び準備を行う必要がある。

システムの過負荷のリスクを低減するために，将来の容量・能力の要求を予測することが望ましい。新しいシステムの運用上の要求事項を，その受入れ及び利用に先立って，設定し，文書化し，試験することが望ましい。

10.3.1 容量・能力の管理

管理策

要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整し，また，将来必要とする容量・能力を予測することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，要求されるシステム性能を満たすことを確実にするために，次の事項を実施することが望ましい。

a) クラウドサービスにおける容量・能力の限界値を把握する。
b) クラウドサービスにおける容量・能力の限界値が，要求されるシステム性能を満たすことを確認する。
c) クラウドサービスにおいて，資源の利用を監視・調整する仕組みがあることを確認し，現状の資

源の利用を監視・調整する仕組みに組み込む。

クラウド利用者は，将来必要とする容量・能力を予測する仕組みに，クラウドサービスを組み込むことが望ましい。クラウド利用者は，クラウドサービスの環境においては，契約形態に応じた容量・能力の割当ての変更や，容量・能力の利用に応じた課金について留意することが望ましい。クラウド利用者は，クラウドサービスの容量・能力の追加が，容易にできるか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，重大なインシデントを防ぐために，物理的な容量・能力の全体量を考慮して仮想化されたコンピューティング資源の全体量を監視し，適切に管理することが望ましい。

クラウド事業者は，クラウドサービスにおいて，システム全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握することが望ましい。

クラウドサービスの関連情報

10.3.2 クラウドサービスによっては，CPU 利用率などの急激な上昇・降下が発生し，サービスの安定稼働に影響を及ぼす場合がある。このような事象は原因を特定できないことも多く，特定のしきい値を設けた監視による完全な予測や事前対応が難しい。そのため，クラウド利用者は，クラウドサービスにおける CPU 利用率などの急激な上昇・降下に伴うリスクを評価した上でクラウドサービスを利用することが期待される。一方，クラウド事業者は，そのようなリスクをクラウド利用者が識別・評価できるよう，あらかじめ示しておくことが期待される。システムの受入れ管理策

新しい情報システム及びその改訂版・更新版の受入れ基準を確立し，また，開発中及びその受入れ前に適切なシステム試験を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，新規のクラウドサービスや，利用中のクラウドサービスの改訂版・更新版に関して，受入れ基準を確立し，開発中及びその受入れ前にシステム試験を実施し，結果をクラウド事業者に通知することが望ましい。

クラウド利用者は，クラウドサービスの選定にあたり，クラウド事業者に対して次の情報を求めることが望ましい。

a) SLA（アクセスネットワークの容量・能力及び冗長化を含む）

b) 試用に関する詳細（料金，試用期間及び免責事項を含む）

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの改訂版・更新版の提供プロセスを，クラウド利用者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，クラウド利用者へ改訂版・更新版の受入れ準備のための期間を提供することが望ましい（例えば，通知後一週間で運用環境に適用する，など）。クラウド事業者は，クラウド利用者が円滑にクラウドサービスの改訂版・更新版へ移行できるように，旧版との併用ができる期間を設けることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスにおいて，新しい情報システム及びその改訂版・更新版の提供は，

クラウド事業者によって，不定期に行われる可能性があることに留意することが期待される。

10.4 悪意のあるコード及びモバイルコードからの保護

目的：ソフトウェア及び情報の完全性を保護するため。

悪意のあるコード及び認可されていないモバイルコードの侵入を防止し，検出するために予防対策が必要となる。

ソフトウェア及び情報処理設備は，悪意のあるコード（例えば，コンピュータウィルス，ネットワークワーム，トロイの木馬，ロジック爆弾，スパイウェア）に対してぜい弱である。利用者には，悪意のあるコードの危険性を知らせることが望ましい。管理者は，適切な場合には，悪意のあるコードを防止し，検知し，取り除くための管理策を導入することが望ましく，また，モバイルコードを管理することが望ましい。

10.4.1 悪意のあるコードに対する管理策

管理策

悪意のあるコードから保護するために，検出，予防及び回復のための管理策，並びに利用者に適切に意識させるための手順を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，悪意のあるコードから情報やシステムを保護するために，検出，予防及び回復のための管理策だけでなく，クラウドサービスの利用者に対してクラウドサービス利用時の考慮事項を適切に意識させるための手順を策定して，実施することが望ましい。

クラウド利用者は，クラウドサービスにおいて，クラウド事業者が，悪意のあるコードからクラウド利用者を保護するために実施している次のような事項を確認することが望ましい。

a) 悪意のあるコードの検出，予防及び回復のための管理策

b) 悪意のあるコード及びその対策・対応について，クラウド利用者に適切に意識させるために実施している管理策とその実行結果

c) 悪意のあるコードに感染した場合のクラウド事業者における報告手順

クラウド利用者は，組織が実施している悪意のあるコード対策とクラウド事業者の悪意のあるコード対策を併せてリスク評価し，必要に応じて自ら追加の対策を実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの提供において，悪意のあるコードへのクラウド事業者の責任範囲と，クラウド利用者の責任範囲を明らかにすることが望ましい。クラウド事業者は，クラウドサービス内で，悪意のあるコードからクラウドサービスの利用者を保護するために，検出，予防及び回復のための管理策を実施し，また，クラウド利用者に適切に意識させるための手順を実施することが望ましい。

クラウドサービスの関連情報

クラウドサービスを構成する環境においては，様々な階層のサービスが複雑に関連するため，それぞれの階層において，悪意のあるコードへの独自の対策が行われている可能性がある。そのため，クラウド利用者とクラウド事業者は，それぞれの階層における対策方式や検出精度の違いから検出結果の違いが発生

する可能性に留意する必要がある。クラウド事業者は，ウイルス対策製品を導入した場合，パフォーマンスの問題や，可用性に影響を生じさせることに留意する必要がある。

10.4.2 モバイルコードに対する管理策

管理策

モバイルコードの利用が認可された場合は，認可されたモバイルコードが，明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また，認可されていないモバイルコードを実行できないようにすることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，マルウェア感染の拡大を防ぐため，特定のクラウド利用者に対するサービスの停止を含むモバイルコード利用の方針を定めることが望ましい。また，クラウド事業者は，クラウドサービスにおけるモバイルコード利用の方針をクラウド利用者に提示し，方針に対する協力を求めることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスにおいてモバイルコードを利用する場合，利用の可否をクラウド利用者が判断し，認可できるような仕組みを提示し，認可されたモバイルコードが，明確に定められたセキュリティ方針に従って動作することを確実にする方法をクラウド利用者に明示することが期待される。また，同時に，クラウド事業者は，クラウドサービスの環境において，認可されていないモバイルコードを実行できないようにする方法を，クラウド利用者に明示することが期待される。

クラウド利用者は，悪意のあるコードに関する次のような事項について，クラウド事業者の情報提供方針を確認することが期待される。

a) セキュリティ関連の設定及び使用されているオプション
b) セキュリティ管理策及び対象システムコンポーネント（例えば，ネットワーク，ゲスト OS レイヤなど）
c) ソフトウェア更新・パッチ適用に関するスケジュール及び情報（例えば，パッチの種類，パッチ適用の頻度及び対象システムなど）
d) ぜい弱性の検出，報告及び改善のための基準及び手順（例えば，ベンダーの公開情報，侵入テストツールなど）
e) 隣接する VM や VMM（Virtual Machine Monitor，仮想マシンモニタ／ハイパーバイザー）などの異なるクラウドコンポーネントの感染に備えたインシデント対応手順及び復旧手順
f) 利用者側で実装すべき悪意のあるコード対策
g) サービスレベル報告書に含まれる内容
   - 未対応のぜい弱性に関するパッチ情報及び管理策
   - 補完的統制に関する情報
   - 特定のぜい弱性に関する情報及び傾向（例えば，仮想化レイヤなどに対するぜい弱性の分類及び重要度スコアなど）

10.5 バックアップ

目的：情報及び情報処理設備の完全性及び可用性を維持するため。

データのバックアップ取得と時機を失しないデータ復旧の訓練とに関する，合意されたバックアップ方針及び戦略（14.1 参照）を実施するために，日常の作業手順を確立することが望ましい。

10.5.1 情報のバックアップ

管理策

情報及びソフトウェアのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定において，バックアップの必要性を確認することが望ましい。クラウド利用者は，自らが利用するクラウドサービスの特性を理解して，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定において，バックアップの可能性を確認することが望ましい。クラウド利用者は，自らが利用するクラウドサービスの特性を理解し，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定のバックアップ手順を，次の事項を考慮して策定することが望ましい。

a) クラウドサービスに付帯するバックアップ機能及び復元機能
b) 利用者自身が追加開発するバックアップ機能及び復元機能
c) バックアップデータの暗号化（暗号化の必要性を含む）
d) バックアップデータのローカルでの保管及び隔地保管
e) バックアップデータの保管期間

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者が行うべきバックアップ取得について明確にすることが望ましい。また，利用者自身によるバックアップ取得が必要な場合，バックアップ取得を支援する情報若しくは機能を提供することが望ましい。クラウド事業者は，利用者にバックアップ機能及び復元機能を提供する場合には，利用者が実施する手順を明確にすることが望ましい。

クラウドサービスの関連情報

クラウドサービスでは，クラウドサービスによってバックアップ不可能な情報がある点に留意する必要がある。クラウドサービス以外のシステム運用におけるバックアップ手順において，差分バックアップ，増分バックアップ，完全バックアップなど，バックアップ対象の特性に応じて使い分けている場合は，それぞれの手法による実施の可否を確認することが期待される。

IaaS サービスにおいては，作成された仮想イメージファイルを明示的にバックアップしておくことで，ある時点での環境を再現することができるが，バックアップを指定しない場合には再現することが難しい。クラウド事業者は，クラウド利用者が必要に応じて仮想イメージファイルをバックアップできる手段を用意しておくことが期待される。

PaaS サービスにおいては，作成したアプリケーションなどのソースファイルなどをバックアップすることができないこともある。アプリケーションの開発中など，頻繁に機能の追加や削除を行う場合に備えて，

開発途中の状態を維持できるかどうかを確認することが望ましい。また，実行環境や試験データなどが再現できるかどうかを確認することが期待される。

SaaS サービスでは，アプリケーションで利用するデータだけではなく，利用者アカウントの管理など，クラウドサービスの管理情報についてバックアップが可能かどうかを確認することが期待される。

10.6 ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護，及びネットワークを支える基盤の保護を確実にするため。

組織の境界を越えて広がることもあるネットワークのセキュリティ管理には，データの流れ，法的背景，監視，保護についての注意深い考慮が必要である。

公衆ネットワークを通過する，又は取扱いに慎重を要する情報の保護には，追加の管理策が要求される場合もある。

10.6.1 ネットワーク管理策

管理策

ネットワークを脅威から保護するために，また，ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために，ネットワークを適切に管理し，制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用に際して，ネットワークサービスに関する情報をクラウド事業者に求めることが望ましい。

クラウド利用者は，必要に応じて，私設網又は暗号化された通信経路を介してクラウドサービスを利用することが望ましい。

クラウド事業者の実施が望まれる事項

仮想化技術を用いて構築されたクラウドコンピューティング環境における仮想ネットワークは，物理ネットワーク上の仮想インフラ上に構成されており，物理・論理ネットワークのセキュリティポリシーが適切に調和していない場合，ネットワークのぜい弱性が生じ，システム停止やアクセス制御違反が発生する恐れがあるため，クラウド事業者は，物理ネットワークのセキュリティポリシーを考慮した仮想ネットワークのセキュリティポリシーを定めることが望ましい。また，クラウド事業者は，仮想ネットワークのセキュリティ設定マニュアルを定め，運用担当者に配付することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想化されたネットワークを通じての脅威が存在することを念頭におき，対策を行うことが望ましい。特に，IaaS においては，スイッチやファイアウォールもネットワークと同じホスト OS 上で，仮想化サービスとして提供されることがあるため，ホスト OS のぜい弱性が，スイッチングやフィルタリング，ブロッキングなどのネットワーク関連機能に影響を与える可能性に留意する必要がある。

10.6.2 ネットワークサービスのセキュリティ

管理策

すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について，

セキュリティ特性，サービスレベル及び管理上の要求事項を特定し，また，いかなるネットワークサービス合意書にもこれらを盛り込むことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスに含まれるすべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について，セキュリティ特性，サービスレベル及び管理上の要求事項に適合することを確認することが望ましい。クラウド利用者は，クラウドサービスに含まれるすべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を，クラウド事業者との合意書に盛り込むことが望ましい。クラウド利用者はクラウドービスに含まれるネットワークサービスが，セキュリティを保つ能力を見定め，常に監視することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスに含まれるすべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を，クラウド利用者と合意することが望ましい。クラウド事業者は，クラウド利用者と合意したクラウドサービスに含まれるネットワークサービスがセキュリティを保つ能力について，クラウド利用者が監視できる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおけるこれらの対策の実施を確実にすることが望ましい。クラウド事業者は，クラウドサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項が，適切に実行されていることを監査などで確認し，必要に応じてクラウド利用者に監査結果などを明示することが望ましい。

10.7 媒体の取扱い

目的：資産の認可されていない開示，改ざん，除去又は破壊，並びにビジネス活動の中断を防止するため。

媒体を管理し，かつ，物理的に保護することが望ましい。

認可されていない（情報）開示，改ざん，除去及び破壊から文書，コンピュータの媒体（例えば，テープ，ディスク），入力データ，出力データ及びシステムに関する文書を保護するために，適切な操作手順を確立することが望ましい。

10.7.1 取外し可能な媒体の管理

管理策

取外し可能な媒体の管理のための手順は，備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスのデータのバックップを媒体などで実施する場合には，その管理に留意する必要がある。

10.7.2 媒体の処分

管理策

媒体が不要になった場合は，正式な手順を用いて，セキュリティを保ち，かつ，安全に処分することが望ましい。

10.7.3 情報の取扱手順

管理策

情報の取扱い及び保管についての手順は，その情報を認可されていない開示又は不正使用から保護するために，確立することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上の組織の情報を認可されていない開示又は不正使用から保護するために，取扱い手順を確立することが望ましい。クラウド利用者は，作成したクラウドサービス上の情報の取扱い手順を，クラウドサービスの利用者に周知徹底することが望ましい。

10.7.4 システム文書のセキュリティ

管理策

システム文書は，認可されていないアクセスから保護することが望ましい。

10.8 情報の交換

目的：組織内部で交換した及び外部と交換した，情報及びソフトウェアのセキュリティを維持するため。

組織間での情報及びソフトウェアの交換は，正式な交換方針に基づいていること，情報交換に関する合意に沿って実施していること，また，いかなる関連法令をも順守していることが望ましい（箇条 15 参照）。

配送中の情報及び情報を格納した物理的媒体を保護するための手順及び標準を確立することが望ましい。

10.8.1 情報交換の方針及び手順

管理策

あらゆる形式の通信設備を利用した情報交換を保護するために，正式な交換方針，手順及び管理策を備えることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，情報交換の機能を含むクラウドサービスを提供する場合，この情報交換を保護するための機能を検討し，必要に応じて実装することが期待される。クラウド事業者は，クラウドサービスを利用した情報交換を保護するための機能及び利用手順を，クラウドサービスの利用を検討する者に明示することが期待される。クラウド事業者は，クラウドサービスを利用した情報交換を保護するための機能が適切に動作していることを監査などによって確認し，クラウド利用者にその実施の事実又は結果を明示することが期待される。クラウド利用者及びクラウド事業者は，クラウドサービスにおいて，通信経路が暗号化できず，データの改ざんチェック機能も備えていない機能がある可能性に留意する必要がある。

10.8.2 情報交換に関する合意

管理策

組織と外部組織との間の情報及びソフトウェアの交換について，両者間での合意が成立することが望ましい。

10.8.3 配送中の物理的媒体

管理策

情報を格納した媒体は，組織の物理的境界を越えた配送の途中における，認可されていないアクセス，不正使用又は破損から保護することが望ましい。

10.8.4 電子的メッセージ通信

管理策

電子的メッセージ通信に含まれた情報は，適切に保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能があることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを，クラウド事業者が監査していることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを監査などによって確認し，必要に応じてクラウド利用者に監査結果を明示することが望ましい。

10.8.5 業務用情報システム

管理策

業務用情報システムの相互接続と関連がある情報を保護するために，個別方針及び手順を策定し，実施することが望ましい。

10.9 電子取引サービス

目的：電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。

電子商取引サービス（オンライン取引を含む。）の利用に関連するセキュリティ上の影響及び管理策のための要求事項を考慮することが望ましい。公開されているシステムを通じて電子的に発行した情報の完全性及び可用性についても，考慮することが望ましい。

10.9.1 電子商取引

管理策

公衆ネットワークを経由する電子商取引に含まれる情報は，不正行為，契約紛争，認可されていない開示及び改ざんから保護することが望ましい。

10.9.2 オンライン取引

管理策

オンライン取引に含まれる情報は，次の事項を未然に防止するために，保護することが望ましい。

－不完全な通信

－誤った通信経路設定

－認可されていないメッセージの変更

－認可されていない開示

－認可されていない複製又は再生

10.9.3 公開情報

管理策

認可されていない変更を防止するために，公開システム上で利用可能な情報の完全性を保護することが望ましい。

10.10 監視

目的：認可されていない情報処理活動を検知するため。

システムを監視することが望ましく，また，情報セキュリティ事象を記録することが望ましい。

システム運用担当者の作業ログ及び障害ログは，情報システムの問題を識別することを確実とするために利用することが望ましい。

組織は，監視及び記録の活動に適用されるすべての関連した法的要求事項を順守することが望ましい。

システムの監視は，採用している管理策の有効性の点検及びアクセス方針モデルに対する適合性の確認のために利用することが望ましい。

10.10.1 監査ログ取得

管理策

利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを取得することが望ましく，また，将来の調査及びアクセス制御の監視を補うために，合意された期間，保持することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で取得されるクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログは，将来の調査及びアクセス制御の監視を補うために，適切な期間，保持されることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得される監査ログが，クラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録できていることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログが提供される方法，提供のタイミングについて，適切かどうか確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログが保持される期間が，将来の調査及びアクセス制御の監視を補うために適切かどうか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で取得するクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを特定し，取得する機能をクラウド利用者に提供することが望ましい。クラウド事業者は，クラウドサービス上で取得された監査ログは，クラウド利用者の将来の調査及びアクセス制御の監視を補うことを考慮し，保持する期間を定めることが望ましい。クラウド事業者は，クラウ

ドサービス上で取得する利用者の活動，例外処理及びセキュリティ事象を記録した監査ログについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログの提供方法，提供のタイミングについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログを保持する期間を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ログの取扱いについて，個別のクラウド利用者の要請に応じることができることを考慮することが期待される。監査ログの内容及び提供方法に関しては，クラウド利用者とクラウド事業者が合意した形式で実施することが期待される。

10.10.2 システム使用状況の監視

管理策

情報処理設備の使用状況を監視する手順を確立すること，及び監視活動の結果を定めに従ってレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの使用状況を監視する手順を確立することが望ましい。また，監視活動の結果を定めに従ってレビューすることが望ましい。

クラウド利用者は，クラウドコンピューティングサービスの利用状況の監視手順を策定するために，クラウド事業者に次のような事項を確認することが望ましい。

a) 利用状況の記録の種類

b) 利用状況の記録の表示方法

c) 利用状況の記録の保持期間

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で使用状況をクラウド利用者が監視できる機能を提供することが望ましい。

10.10.3 ログ情報の保護

管理策

ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確認するために，次のような情報をクラウド事業者に対して求めることが望ましい。

a) ログ情報の保護に関する方針

b) ログ情報の保護機能の概要

c) ログ情報の保護が適切に動作していることに関するクラウド事業者による監査の実施状況又は結果

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上のクラウド利用者のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確実にすることが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービス上でログ情報を一括して取得し，一括した改ざん防止を行っている場合，必要なログとして提供されるログの完全性が担保できない可能性があることに留意することが期待される。

10.10.4 実務管理者及び運用担当者の作業ログ

管理策

システムの実務管理者及び運用担当者の作業は，記録することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上に構築した利用者システムの実務管理者及び運用担当者の作業が，記録されていることを確認することが望ましい。クラウド利用者は，クラウドサービス上で記録された，システムの実務管理者及び運用担当者の作業の記録を，規定に従ってレビューすることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を，記録する機能を提供することが望ましい。クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を記録する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドコンピューティング環境に対する特権操作がクラウド利用者にゆだねられる場合，責任分界を明確にするために，クラウド事業者及びクラウド利用者双方の作業ログを取得・保管することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なときに必要なログが提供されない可能性に留意する必要がある。

クラウド利用者は，作業ログに関する仕様を確認したり，第三者タイムスタンプ及び WORM（Write-Once-Read-Many，書込み 1 回のみ可能かつ消去・変更不可）デバイスの否認防止機能の有無を確認することが期待される。

クラウド利用者は，クラウドサービスにおいて運用担当者のログが提供されない場合には，どのようなログをクラウド事業者が取得しているかについて情報提供を求めることが期待される。

10.10.5 障害のログ取得

管理策

障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上の障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を定めることが望ましい。クラウド

事業者は，クラウド利用者に障害のログを提供する機能を提供することが望ましい。クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウド利用者に提供する，障害のログの提供方法を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なログが提供されない可能性に留意する必要がある。

10.10.6 クロックの同期

管理策

組織又はセキュリティ領域内のすべての情報処理システム内のクロックは，合意された正確な時刻源と同期させることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差が発生するか確認することが望ましい。クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差を定期的に監視・記録し，時刻差が発生することによって，影響がある事項を洗い出し，管理策を検討することが望ましい。クラウド利用者は，分析などにおいて，ログに記録された時刻など，クラウドサービスの時刻の差を考慮することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させることが望ましい。クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させる仕組みを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，標準時の異なる複数の地域にまたがるシステムのクロックのずれに留意することが望ましい。クラウド事業者は，IaaS においては，仮想環境の時刻ずれのリスクに留意する必要がある。

11 アクセス制御

11.1 アクセス制御に対する業務上の要求事項

目的：情報へのアクセスを制御するため。

情報・情報処理設備及び業務プロセスへのアクセスにおいては，業務及びセキュリティの要求事項に基づいて管理することが望ましい。

アクセス制御規則には，情報を伝える範囲及びアクセスの認可に対する方針を考慮することが望ましい。

11.1.1 アクセス制御方針

管理策

アクセス制御方針は，アクセスについての業務上及びセキュリティの要求事項に基づいて確立し，文書

化し，レビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，既存のアクセス制御方針が，クラウドサービスが提供するアクセス制御機能で実現できるか確認することが望ましい。クラウド利用者は，クラウドサービスのアクセス権を既存のアクセス制御方針に組み込むことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおいて，利用者のアクセス制御機能を提供することが望ましい。クラウド事業者は，提供するクラウドサービスにおいてクラウド利用者が実施可能なアクセス制御機能について，クラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスのアクセス権を既存のアクセス制御方針に組み込む際に，クラウド利用者が考慮するポイントとして次のような事項がある。

a) アクセス制御に係る職務の分離（例えば，ID の使用者と登録者など）

b) アクセス権限付与に関する承認プロセス

c) クラウド利用者に付与されるアクセス制御権限

11.2 利用者アクセスの管理

目的：情報システムへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。

情報システム及びサービスへのアクセス権の割当てを管理するための正式の手順が備わっていることが望ましい。

この手順は，利用者アクセスのライフサイクル（すなわち，新しい利用者の初期登録から，情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除まで）におけるすべての段階を対象とすることが望ましい。アクセスの特権を与えると，システムの管理策ではその利用者を制御することができなくなる。適切な場合には，アクセス特権の付与を管理する必要性について，特別の注意を払うことが望ましい。

11.2.1 利用者登録

管理策

すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者の登録・登録削除についての正式な手順を備えることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者 ID の登録・削除についての正式な手順に，クラウドサービスの利用を考慮することが望ましい。クラウド利用者は，必要に応じてクラウド事業者に利用者 ID の登録・削除機能に関する情報を求め，クラウド事業者が提供する機能で組織の正式な手順が実現できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者のクラウドサービス利用者 ID の登録・削除機能を提供することが望ましい。また，このような機能について，必要に応じて次の情報を提供することが望ましい。

a) 利用者 ID 登録・削除の手順

b) 利用者 ID 登録・削除に必要な情報

c) 利用者の同一性検証の仕様

d) サービスの一部として利用者 ID 管理ツールを提供している場合は，利用者 ID 管理ツールの仕様

クラウドサービスの関連情報

クラウド利用者は，クラウドサービスの形態によっては，クラウドサービスの利用者 ID を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド提供者が登録を代行する場合など，様々な形態が存在することを考慮する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザが存在する場合や，クラウド利用者の環境にクラウド事業者が利用する利用者 ID を作成する必要がある場合は，クラウド利用者とクラウド提供者の間でその管理責任を明確に定義することが期待される。

11.2.2 特権管理

管理策

特権の割当て及び利用は，制限し，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，特権の割当て及び利用を管理する既存の仕組みが，クラウドサービス上で実現できるか確認し，クラウドサービス利用における特権を管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者に特権を付与する場合には，クラウド利用者がクラウドサービスにおける特権を管理する機能を提供することが望ましい。また，このような機能について，次のような情報をクラウド利用者に提供することが望ましい。

a) クラウド利用者の特権の種類及び役割

b) クラウド利用者の特権アカウント使用の監視・管理機能の仕様

c) クラウド利用者の特権アカウント使用に関するログ

クラウドサービスの関連情報

クラウド利用者はクラウドサービスの形態においては，特権を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド事業者が登録を実施するなど，様々な形態が存在することに留意する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザとして特権が存在する場合や，クラウド利用者の環境にクラウド事業者の特権を作成する必要がある場合は，クラウド利用者とクラウド事業者の間でその管理責任を明確に定義することが期待される。

11.2.3 利用者パスワードの管理

管理策

パスワードの割当ては，正式な管理プロセスによって管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，パスワードの割当てに関する既存の正式な管理プロセスが，クラウドサービスが提

供する機能で実現できるか確認することが望ましい。クラウド利用者は，クラウド事業者があらかじめ設定したパスワード（初期パスワードなど）を，システム又はソフトウェアのインストール後に変更することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理プロセスの機能について，次のような情報を提供することが望ましい。

a) パスワードの発行，変更及び再発行の手順

b) パスワード割当てにおける認証及び認証の仕組み（例えば，多要素認証を用いた認証方法など）

クラウドサービスの関連情報

クラウドサービスの利用者パスワードの管理機能は，利用するクラウドサービスの形態によっては，適切なインタフェースをクラウド利用者が設計する必要があることに留意する必要がある。

11.2.4 利用者アクセス権のレビュー

管理策

管理者は，正式なプロセスを使用して，利用者のアクセス権を定められた間隔でレビューすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，アクセス権を一覧化する機能の仕様について，クラウド事業者に情報を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用者のアクセス権をレビューする正式なプロセスが，クラウドサービスの機能で実現できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，クラウド利用者がアクセス権をレビューする機能を提供することが望ましい。

11.3 利用者の責任

目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。

認可されている利用者間の協力は，有効なセキュリティのために不可欠である。

利用者に，有効なアクセス制御を維持するための自分自身の責任を認識させることが望ましい。特にパスワードのセキュリティ及び利用者が利用する装置のセキュリティに関して，その責任を認識させることが望ましい。

クリアデスク・クリアスクリーン方針は，書類，媒体及び情報処理設備に対する認可されていないアクセス又は損傷のリスクを低減するために，実施することが望ましい。

11.3.1 パスワードの利用

管理策

パスワードの選択及び利用時に，正しいセキュリティ慣行に従うことを，利用者に要求することが望ま

しい。

クラウドサービスの関連情報

クラウド事業者は，クラウド利用者が，パスワードの選択及び利用をする際に，正しいセキュリティ慣行に従うことができる機能を提供することが期待される。クラウドサービスでは，複数のサービスを組み合わせて一つのパスワードを利用する場合があるので，クラウド事業者は，質の良いパスワードを用いることをクラウド利用者に助言することを考慮する必要がある。

11.3.2 無人状態にある利用者装置

管理策

利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にすることが望ましい。

クラウドサービスの関連情報

クラウド利用者は，共有環境でクラウドサービスを利用する場合には，認可されないアクセスについて留意する必要がある。

11.3.3 クリアデスク，クリアスクリーン方針

管理策

書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。

11.4 ネットワークのアクセス制御

目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。

内部及び外部のネットワークを利用したサービスへのアクセスを，制御することが望ましい。

ネットワーク及びネットワークサービスへの利用者のアクセスは，次の条件を確実にすることによって，ネットワークサービスのセキュリティを損なわないことが望ましい。

a) 組織のネットワークと他の組織が管理するネットワーク又は公衆ネットワークとの間に適切なインタフェースを備える。

b) 利用者及び装置に適切な認証機構を適用する。

c) 情報サービスへの利用者アクセスを制御する。

11.4.1 ネットワークサービスの利用についての方針

管理策

利用することを特別に認可したサービスへのアクセスだけを，利用者に提供することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，ネットワークサービスの利用に関する方針に，クラウドサービスの利用に関する考慮事項を含めることが望ましい。クラウド利用者は，適切なクラウドサービスの利用者のみクラウドサービスが利用できるようネットワークを構成する方針を定めることが望ましい。

クラウド利用者は，クラウドサービスのネットワークの利用に関する方針に次の事項を含めることを確実にすることが望ましい。

a) ネットワークアクセス制御方針

b) アクセス管理サービス方針

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう，クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想化ソフトウェア固有の課題（例えば，仮想マシンから他仮想マシンへの攻撃など，仮想化ソフトウェア内での攻撃）を考慮し，各仮想マシンの隔離設計に留意する必要がある。クラウド事業者は，隔離設計は，物理ネットワーク側での対応や，ゾーン機能やプライベート VLAN 機能などの機能を活用する方法や，同機能を有するサードパーティ製品の活用などに留意する必要がある。

11.4.2 外部から接続する利用者の認証

管理策

遠隔利用者のアクセスを管理するために，適切な認証方法を利用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，自らが管理していないネットワーク（公衆無線 LAN や携帯電話網による接続など）からクラウドサービスを利用する際に，適切な認証方法を利用することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を提供することが望ましい。クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を，クラウドサービスの利用を検討する者に明示することが望ましい。

11.4.3 ネットワークにおける装置の識別

管理策

特定の場所及び装置からの接続を認証するための手段として，自動の装置識別を考慮することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドサービスに接続する装置において，識別を可能にする機能（電子証明書や IC チップなどを利用した識別機能）を提供することが期待される。

11.4.4 遠隔診断用及び環境設定用ポートの保護

管理策

診断用及び環境設定用ポートへの物理的及び論理的なアクセスは，制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用者がクラウドサービスの遠隔診断用及び環境設定ポートを管理する場合には，厳密に管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスに遠隔診断用及び環境設定ポートが存在する場合は，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は, クラウドサービスのホスト OS 上で動作する仮想スイッチや仮想ファイアウォールなどの遠隔診断用及び環境設定ポートが存在する場合は，厳密に管理することが期待される。

11.4.5 ネットワークの領域分割

管理策

情報サービス，利用者及び情報システムは，ネットワーク上，グループごとに分割することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド事業者のネットワークにおける分離を要求する必要性について考慮することが望ましい。

クラウド利用者は，クラウドサービスのネットワークを分離するため，ネットワークを異なるドメインに分離する機能の使用について，必要に応じてクラウド事業者に情報を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用者のアクセス権限に基づいて，クラウドサービスのネットワークを論理的に分離することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，各クラウド利用者に割り当てたコンピューティング資源に，他のクラウド利用者や許可されていないユーザがアクセスできないように管理し，物理的な設定や移行にかかわらず，仮想環境の分離を確実にすることが望ましい。

ネットワーク若しくはインタフェースの分離がなされていない場合，クラウド事業者は，アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。

クラウド事業者は，クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために，クラウド環境における情報セキュリティについて評価を実施することが望ましい。

クラウドサービスの関連情報

クラウド事業者は, クラウドサービスのホスト OS 上で動作する仮想スイッチや仮想ファイアウォールなどのネットワークを構成に応じて論理的に分離する必要がある。

クラウド利用者がクラウド事業者にネットワークの分離を要求するケースとして，次のような場合が想定される。

a) クラウド環境内に同業他社が共存する場合

b) 規制要件によりネットワーク通信の分離・隔離が求められる場合

11.4.6 ネットワークの接続制御

管理策

共有ネットワーク，特に，組織の境界を越えて広がっているネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続能力を制限することが望ましい（11.1 参照）。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続を許可する範囲を制限することが望ましい。利用者のネットワークへのアクセス権は，アクセス制御方針の要求に従って，維持・更新することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを特定することが望ましい（例えば，電子メールなどのメッセージ通信，ファイル転送など）。クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，クラウドコンピューティングで利用できるサービスを増やすことで，他のゲストOSや，外部から受ける影響の増加に留意する必要がある。

11.4.7 ネットワークルーティング制御

管理策

コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，ルーティング制御の管理策をネットワークに対して実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，クラウドサービスを，ルーティング制御の管理策に加えることが望ましい。

クラウド事業者が，ホストOS上のネッワークルーティングを行う場合は，クラウド利用者は，その設定が，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反していないことを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，ホストOS上のネットワークルーティングについて，適切に設定することが望ましい。クラウド事業者は，ホストOS上のネットワークルーティングについて，適切に設定していることを利用者に明示することが望ましい。

クラウドサービスの関連情報

ホストOS上のネットワークルーティングについて，クラウド利用者が設定できる場合は，影響を考慮して設定する必要がある。

11.5 オペレーティングシステムのアクセス制御

目的：オペレーティングシステムへの，認可されていないアクセスを防止するため。

オペレーティングシステムにアクセスする者を，認可された利用者に限定するために，セキュリティ設備を用いることが望ましい。それらの設備は，次の能力をもつことが望ましい。

a) 既定のアクセス制御方針に従って認可されている利用者本人であることの認証

b) システムへの認証の成功及び失敗の記録

c) 特別なシステム特権の使用の記録

d) システムセキュリティ方針に違反したときの警告発信

e) 認証のための適切な手段の提供

f) 適切な場合，利用者の接続時間の制限

11.5.1 セキュリティに配慮したログオン手順

管理策

オペレーティングシステムへのアクセスは，セキュリティに配慮したログオン手順によって制御することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのオペレーティングシステムにログオンする場合，セキュリティに配慮したログオン手順によって制御されることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのオペレーティングシステムにクラウド利用者がログオンする場合，セキュリティに配慮したログオン手順で制御する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの形態においては，オペレーティングシステムが複数存在し，その利用者も異なる可能性があるため，クラウド事業者は，クラウド利用者の資産と権限に留意し，ログオン手順を定めることを求めることが期待される。

11.5.2 利用者の識別及び認証

管理策

すべての利用者は，各個人の利用ごとに一意な識別子（利用者 ID）を保有することが望ましい。また，利用者が主張する同一性を検証するために，適切な認証技術を選択することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスにおいて，すべてのクラウドサービスの利用者が，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるか確認することが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術の選択が可能であるかを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるようにすることが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術を選択することができる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるかどうか，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，選択できる認証技術を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ID 管理をするサービスが，クラウドサービス利用者 ID を個別に発行できるように設定することが期待される。クラウド事業者は，ID 管理をするサービスが，共有 ID を発行する場合は，

利用者が共有IDの利用者を個別に認識する必要があるか,検討が必要なことを明示することが期待される。

11.5.3 パスワード管理システム

管理策

パスワードを管理するシステムは，対話式とすることが望ましく，また，良質なパスワードを確実とするものが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのパスワードを管理するシステムが，対話式であり，また，良質なパスワードを確実とする機能があることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，対話式とすることが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，良質なパスワードを確実とすることが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，対話式であることを，開示することが望ましい。クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，良質なパスワードを確実とする機能があることを，利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，ID 管理をするサービスが，パスワード管理を適切に行われるように設定すると同時に，その設定を機能させるインタフェースを提供することが期待される。クラウド事業者は，ID 管理をするサービスのみを提供する場合は，パスワードの管理が適切に行われるように設定する手順や，その設定を機能させるインタフェースを作成するための手順を利用者に明示することが期待される。

11.5.4 システムユーティリティの使用

管理策

システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのシステム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用を，制限し，厳しく管理することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを特定することが望ましい。クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

システム管理者の利便性を重視するクラウドサービスの機能は，システム及びアプリケーションの管理策を無効化できるユーティリティプログラムである場合がある。クラウド利用者組織におけるクラウドサービス利用者に対しては，そのようなユーティリティプログラムの使用は制限し，厳密に管理することが

期待される。

11.5.5 セッションのタイムアウト

管理策

一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションが遮断されることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能を提供することが望ましい。クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能について開示することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，利用するクラウドサービスによっては，タイムアウトによる遮断をしてはならないサービスもあることに留意する必要がある。クラウド事業者は，仮想 OS の管理アクセス対応機能ではホスト OS へのアクセス制御において，セッションタイムアウトに未対応のものがあることに留意する必要がある。クラウド利用者は，セッションタイムアウトについて端末のスクリーンセイバーの制限など他の管理策を実施できることに留意する必要がある。

11.5.6 接続時間の制限

管理策

リスクの高い業務用ソフトウェアに対しては，更なるセキュリティを提供するために，接続時間の制限を利用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，利用におけるリスクが高いと判断したクラウドサービスに対しては，接続時間の制限を利用できるか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，利用におけるリスクが高いと判断されたクラウドサービスは，接続時間の制限を利用できる機能を提供することが望ましい。クラウド事業者は，リスクの高いクラウドサービスに対しては，接続時間の制限を利用できるかどうかを，開示することが望ましい。

クラウドサービスの関連情報

クラウド事業者は，仮想 OS の管理アクセス対応機能ではホスト OS へのアクセス制御において，管理アクセス通信の接続時間の制限が未対応のものがあることに留意する必要がある。クラウド利用者は，接続時間について端末の利用時間の制限など他の管理策を実施できることに留意する必要がある。

11.6 業務用ソフトウェア及び情報のアクセス制御

目的：業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。

業務用ソフトウェアシステムへのアクセス及びその中でのアクセスを制限するために，セキュリティ機能を用いることが望ましい。

業務用ソフトウェア及び情報への論理的アクセスは，認可されている利用者に制限することが望ましい。業務用ソフトウェアシステムは，次の条件を満たすことが望ましい。

a) 既定のアクセス制御方針に従って，情報及び業務用ソフトウェアシステム機能への利用者アクセスを制御する。

b) システム又は業務用ソフトウェアの制御を無効にできるユーティリティ，オペレーティングシステムのソフトウェア及び悪意のあるソフトウェアによる認可されていないアクセスから保護する。

c) 情報資源を共有しているほかの情報システムのセキュリティを脅かさない。

11.6.1 情報へのアクセス制限

管理策

利用者及びサポート要員による情報及び業務用ソフトウェアシステム機能へのアクセスは，既定のアクセス制御方針に従って制限することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用者及びクラウド利用者のサポート要員によるクラウドサービスへのアクセスを，既定のアクセス制御方針に従って制限することが望ましい。クラウド利用者は，複数のシステムや情報を内包できるクラウドサービスでは，その重要性に応じて，アクセス権を強固にする必要があることに留意し，必要な管理策を設定できるような機能を準備することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者におけるクラウドサービスへのアクセス制限の要求モデルを定めることが望ましい。クラウド事業者は，クラウド利用者が行える要件を定め，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

仮想マシンを操作するクライアントソフトウェアからは，ホスト OS のサービスコンソール部分だけでなくゲスト OS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施する必要があることに留意する必要がある。

11.6.2 取扱いに慎重を要するシステムの隔離

管理策

取扱いに慎重を要するシステムは，専用の（隔離された）コンピュータ環境をもつことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，取扱いに慎重を要するシステムを，クラウドコンピューティングを利用して，構築する場合には，専用の（隔離された）コンピュータ環境上に構築できることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，取扱いに慎重を要するシステムを，クラウドコンピューティング内に構築する場合

に備えて，専用の（隔離された）コンピュータ環境上に構築できる機能を提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，PaaS/IaaS 環境など，複数のシステムを内包できるクラウドサービス上では，そのシステムの重要性に応じて，アクセス権を強固にすることが期待される。クラウド事業者は，システム間の隔離をする管理策に留意する必要がある（仮想スイッチ上の arp スプーフィング防止機能など）。仮想マシンを操作するクライアントソフトウェアからは，ホスト OS のサービスコンソール部分だけでなくゲスト OS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施することが期待される。

11.7 モバイルコンピューティング及びテレワーキング

目的：モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため。

要求される保護は，これら特異な作業形態が引き起こすリスクに応じたものであることが望ましい。モバイルコンピューティングを用いるとき，保護されていない環境における作業のリスクを考慮し，適切な保護を施すことが望ましい。テレワーキングに関しては，組織は，テレワーキングを行う場所に保護を施し，この作業形態のために適切な取決めがあることを確実にすることが望ましい。

11.7.1 モバイルのコンピューティング及び通信

管理策

モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するために，正式な方針を備え，また，適切なセキュリティ対策を採用することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，クラウドサービスを加え，適切な情報セキュリティ対策を採用することが望ましい。クラウドサービスにおいてモバイルコンピューティングを利用できる機能がある場合は，クラウド利用者は，その機能がモバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，適合しているか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおいて，モバイルコンピューティングを利用できる機能を提供する場合は（一般的に，SaaS 又はアプリケーションレイヤにおけるサービスにおいて該当する），適切な情報セキュリティ対策を採用し，講じている情報セキュリティ対策を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

モバイルコンピューティング設備・通信設備 （例えば，ノート型コンピュータ，パームトップコンピュータ，ラップトップコンピュータ，IC カード，携帯電話） を用いる場合，業務情報が危険にさらされない

ことを確実にするために，特別な注意を払う必要がある。モバイルコンピューティング方針は，保護されていない環境におけるモバイルコンピューティング装置を用いた作業のリスクを考慮に入れる必要がある。クラウドサービスでは，スマートフォンなどの携帯端末での利用を前提として提供されている場合があるため，それらの端末の利用についても留意する必要がある。

11.7.2 テレワーキング

管理策

テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスをテレワーキングで利用する場合，テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。クラウドサービスにおいてテレワーキングを利用できる機能がある場合は，クラウド利用者は，その機能が，テレワーキングのための方針，運用計画及び手順に適合することを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウドサービスにおいてテレワーキングを利用する機能を提供する場合は，テレワーキングの適切な保護を実施することが望ましい。クラウド事業者は，提供するクラウドサービスにおいて，テレワーキングを利用する機能を提供する場合は，講じているセキュリティのための管理策を，クラウドサービスの利用を検討する者に明示することが望ましい。

12 情報システムの取得，開発及び保守

12.1 情報システムのセキュリティ要求事項

目的：セキュリティが情報システムに欠くことのできない部分であることを確実にするため。

情報システムには，オペレーティングシステム，システム基盤，業務用ソフトウェア，既成の製品，サービス及び利用者が開発したソフトウェアが含まれる。業務プロセスを支える情報システムの設計及び実装は，セキュリティへの影響が極めて大きい。セキュリティ要求事項は，情報システムを開発及び／又は実装する前に，特定し，合意することが望ましい。

すべてのセキュリティ要求事項は，プロジェクトの要求仕様検討段階で特定して，その正当性を実証し，合意した上で，情報システムの包括的な作業の一環として，文書化することが望ましい。

12.1.1 セキュリティ要求事項の分析及び仕様化

管理策

新しいシステム又は既存の情報システムの改善に関する業務上の要求事項を記述した文書では，セキュリティの管理策についての要求事項を仕様化することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，システム構築の標準を記載した規程にクラウドサービス利用時の項目を追加することが望ましい。クラウド利用者は，システム利用標準に外部のクラウドサービスを利用する場合に必要な項目を追加することが望ましい。クラウド利用者は，システム利用標準には組織のセキュリティ基本方針

とクラウド事業者のセキュリティ基本方針が組織のセキュリティ基本方針に反しないことを確認することが望ましい。

クラウド利用者は，クラウドサービスにおいて実施されている管理策が，組織のセキュリティ上の要求事項と整合しているかを分析・評価することが望ましい。この分析・評価の結果，情報セキュリティ要求事項を満たしていないと判断した場合，クラウドサービスの利用の制限や他の管理策の導入について検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスで実装（提供）している情報セキュリティ対策及び機能を列記し，開示することが望ましい。

クラウドサービスの関連情報

クラウド事業者によっては独自のオペレーティングシステムなどを利用している場合がある。この場合は標準的なオペレーティングシステムと違ってクラウド事業者からしかぜい弱性情報などを得ることができないことに留意すること。その場合，クラウド利用者は，クラウドサービスを単なるアウトソーシングと想定せずに，自らのシステムの一部としてクラウドサービスを把握し，クラウド事業者とのコミュニケーションをとりながら，情報セキュリティ対策を考慮することが期待される。

12.2 業務用ソフトウェアでの正確な処理

目的：業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。

利用者が開発した業務用ソフトウェアを含め，正しい処理を確実にするために，業務用ソフトウェアに適切な管理策を設計して組み入れることが望ましい。これらの管理策には，入力データ，内部処理及び出力データの妥当性確認を含めることが望ましい。

慎重な取扱いを要する，価値の高い，又は重要な情報を処理するシステム，又はそれらに影響を及ぼすシステムには，更なる管理策が必要となる場合もある。そのような管理策は，セキュリティ要求事項及びリスクアセスメントに基づいて決めることが望ましい。

12.2.1 入力データの妥当性確認

管理策

業務用ソフトウェアに入力するデータは，正確で適切であることを確実にするために，その妥当性を確認することが望ましい。

12.2.2 内部処理の管理

管理策

処理の誤り又は故意の行為によって発生する情報の破壊を検出するために，妥当性確認の機能を業務用ソフトウェアに組み込むことが望ましい。

12.2.3 メッセージの完全性

管理策

業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要

求事項を特定し，また，適切な管理策を特定し，実装することが望ましい。

12.2.4 出力データの妥当性確認

管理策

業務用ソフトウェアからの出力データは，保存する情報の処理が正しく，かつ，状況に対して適切であることを確実にするために，妥当性確認をすることが望ましい。

12.3 暗号による管理策

目的：暗号手段によって，情報の機密性，真正性又は完全性を保護するため。

暗号による管理策の利用に関する方針を策定することが望ましい。暗号技術の利用を支持するために，かぎ管理を備えることが望ましい。

12.3.1 暗号による管理策の利用方針

管理策

情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で利用する情報の暗号化機能が提供されていることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて提供されている情報の暗号化機能が，暗号による管理策の利用に関する方針に照らして適切であるか確認することが望ましい。

クラウド利用者は，クラウドサービスを利用するネットワーク経路が暗号化されていることを確認することが望ましい。クラウド利用者は，クラウドサービスで利用する情報がシステム上で暗号化されていることを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，暗号化に対応しているサービスを明確にし，クラウド利用者に明示することが望ましい。クラウド事業者は，暗号化されないサービスについて代替機能があれば明確にし，開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの暗号化では特殊なデータ管理を行っている場合が多く，組織の手順書に定めた暗号化技術が適用できない場合がある。そのため，クラウド利用者は，資産分類に従った機密性確保のための暗号化が実施できるかどうかを確認し，サービスの選択，付加機能の選択を行うことが期待される。

12.3.2 かぎ（鍵）管理

管理策

組織における暗号技術の利用を支持するために，かぎ管理を実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで管理すべき暗号かぎを識別し，かぎ管理手順を定めることが望ましい。

クラウド利用者は，クラウドサービスにおけるかぎ管理手順について，必要に応じて次のような情報を求めることが望ましい。

a) かぎの種類

b) かぎのライフサイクル（生成，変更，更新，保管，失効，回収，維持，破壊）の各プロセスにおける手順を含むかぎ管理システムの仕様

c) クラウド利用者側での実施が推奨される事項

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスにおけるかぎ管理をクラウド利用者が実施できるよう，かぎ管理に関する情報提供の方針を定め，クラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービス（特に SaaS）においては独自の認証を行っている場合があり，既に運用している認証とかぎ管理の仕組みとの連携がとれない場合がある。クラウド利用者は，システムの要求事項に適応したかぎ管理ができるかどうかを確認し，必要に応じて要求を満たす認証方式と連携して管理することが期待される。

12.4 システムファイルのセキュリティ

目的：システムファイルのセキュリティを確実にするため。

システムファイル及びプログラムソースコードへのアクセスを制御することが望ましい。IT プロジェクト及びサポート活動は，セキュリティを確保した上で実施することが望ましい。取扱いに慎重を要するデータが試験環境から漏えいすることを防止するように留意することが望ましい。

12.4.1 運用ソフトウェアの管理

管理策

運用システムにかかわるソフトウェアの導入を管理する手順を備えることが望ましい。

クラウドサービスの関連情報

PaaS では実行環境のみが提供され，試験運用のプログラムと本番運用のプログラムを区別することが難しい場合がある。そのように，試験運用と本番運用のプログラムを実行環境上で区別することができない場合には，実行時に試験運用のプログラムを削除するか，試験運用と本番運用で別のアカウントを取得し，個別に管理することが期待される。

12.4.2 システム試験データの保護

管理策

試験データは，注意深く選択し，保護し，管理することが望ましい。

12.4.3 プログラムソースコードへのアクセス制御

管理策

プログラムソースコードへのアクセスは，制限することが望ましい。

クラウドサービスの関連情報

PaaS ではスクリプト言語を利用しているものが多く，ソースをそのまま実行環境に置かざるをえないことが多い。クラウド利用者は，プログラムソースコードの保護の観点で，どのようにコードを管理するかを明確にし，新たな手順を作成することが期待される。

12.5 開発及びサポートプロセスにおけるセキュリティ

目的：業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。

プロジェクト及びサポート環境は，厳しく管理することが望ましい。

業務用ソフトウェアシステムに責任をもつ管理者は，プロジェクト又はサポート環境のセキュリティにも責任を負うことが望ましい。変更によってシステム又は運用環境のセキュリティが損なわれないことを点検するために，管理者は，提案されているすべてのシステム変更のレビューを，確実にすることが望ましい。

12.5.1 変更管理手順

管理策

変更の実施は，正式な変更管理手順の使用によって，管理することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，変更管理手順にクラウドサービスに関する内容を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの変更に関して，必要に応じて次の事項を実施することが望ましい。

a) システム変更の実施に関するクラウド利用者への通知

b) システム機能の追加・変更に関するクラウド利用者への通知

c) ソフトウェアの更新についての版数の管理

d) システム変更についての監査証跡・変更履歴の管理及び利用者への提示

クラウドサービスの関連情報

クラウドサービスの利用においてはスケーラビリティの確保が十分になされているとはいえ，マルチテナントであることを考慮すれば，ある一定時期に十分なサービスが得られない場合があることに留意すること。また，IaaS や PaaS の契約形態においては自動的に帯域を確保する機能を有していないものもある。スケーラビリティ以外の変更管理においても同様に，自動化されたシステムに依存せずに，クラウド利用者自らが管理できる手順を明確にすることが期待される。

12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー

管理策

オペレーティングシステムを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要な業務用ソフトウェアをレビューし，試験することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，オペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況を確認することが望ましい。クラウド利用者は，業務用ソフトウェアのレビュー手順にオペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況の確認を追加することが望ましい。クラウド利用者は，利用しているクラウドサービスが対応するオペレーティングシステムやウェブブラウザやクライアント（端末含む）の対応状況を確認することが望ましい。

クラウド利用者は，クラウドサービスのオペレーティングシステムに変更があった場合，クラウド利用者が管理するアプリケーションの技術的レビューを実施することが望ましい。

クラウド利用者が管理するアプリケーションに重大な影響を及ぼす可能性があるクラウドサービスのオペレーティングシステム変更については，クラウド事業者により情報が提供されることを確実にし，アプリケーションの技術レビューを実施することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンを明示することが望ましい。クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンに変更が生じる場合は，あらかじめクラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウドサービスのクラウド利用者側のインタフェースはウェブブラウザを利用することが多い。クラウドサービスではリッチインタフェースの実現のために様々な技術を提供している場合があるが，ブラウザの種類やバージョンによってはそれらの機能を活用できない場合がある。オペレーティングシステムのバージョンアップとともにクライアントのウェブブラウザがアップデートされることも考慮して，オペレーティングシステムアップデートの際には動作テストを行うことが期待される。

12.5.3 パッケージソフトウェアの変更に対する制限

管理策

パッケージソフトウェアの変更は，抑止し，必要な変更だけに限ることが望ましい。また，すべての変更は，厳重に管理することが望ましい。

12.5.4 情報の漏えい

管理策

情報の漏えいの可能性を抑止することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報漏えいが起きないように，クラウドサービスの利用手順を策定することが望ましい。クラウド利用者は，情報漏えいの可能性を考慮して，クラウドサービスの利用者にリスクと対策を周知することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおける情報漏えいに関する対策を行い，円滑なシステムの運用に支障のない範囲でクラウド利用者にその対策内容を開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスではデータを一つのサーバ上に保存するのではなく，複数のサーバ上に分散して配置され，更に冗長性を高めるために，分割されたデータが複製されて複数のサーバ上に配置されることも多い。そのため，データの移動や削除などに伴ってすべてのデータが完全に消去をされず，残存オブジェクトとしてデータの一部が残ってしまう可能性がある。そのため，資産分類において完全消去を前提としているデータについては取扱いに慎重を要する。

12.5.5 外部委託によるソフトウェア開発

管理策

組織は，外部委託したソフトウェア開発を監督し，監視することが望ましい。

12.6 技術的ぜい弱性管理

目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。

技術的ぜい弱性の管理は，効果的，体系的及び再現可能な方法で，その効果を確かめるための測定を伴って実施することが望ましい。これらの考慮は，利用しているオペレーティングシステム及びあらゆる業務用ソフトウェアに適用することが望ましい。

12.6.1 技術的ぜい弱性の管理

管理策

利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得することが望ましい。また，そのようなぜい弱性に組織がさらされている状況を評価し，それと関連するリスクに対処するために，適切な手段をとることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，技術的ぜい弱性についての情報収集について手順化し，利用しているクラウドサービスとの関連の有無を確認することが望ましい。クラウド利用者は，クラウド事業者から技術的ぜい弱性について情報を収集することが望ましい。クラウド利用者は，クラウド事業者以外の信頼できる情報源からぜい弱性について情報を収集することが望ましい。

クラウド利用者は，クラウドサービスにおける技術的ぜい弱性の管理について理解することが望ましい。クラウドサービスにおける技術的ぜい弱性の管理がクラウド利用者のセキュリティ要求事項に適合しない場合，クラウド利用者による対策の実施を検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，提供するクラウドサービスに関連するリスクについて情報収集を行うことが望ましい。クラウド事業者は，必要に応じてぜい弱性や脅威に関する情報をクラウド利用者に通知することが望ましい。

クラウドサービスの関連情報

クラウドサービスではクラウド事業者が独自技術を利用している事が多く，仕様が公開されていないためにクラウド利用者自らがぜい弱性に対応することが難しい。また，クラウド利用者同士の情報交換が難しいために，セキュリティ関連の情報についてクラウド事業者依存となる可能性が高い。クラウド利用者が，独自技術を利用してクラウドサービスを展開しているクラウド事業者と契約する際には，ぜい弱性に関する情報提供が行われるように要求することが期待される。また，クラウドサービスでは，クラウド事業者が用意したソフトウェアであっても，クラウド利用者にその管理権限と責任があり，クラウド事業者がそのソフトウェアの技術的ぜい弱性を管理しない場合がある。したがって，クラウド利用者は技術的ぜい弱性の管理責任にかかわるサービス内容及び契約内容を確認することが期待される。なお，技術的ぜい弱性の管理は，変更管理の従属機能とみなすことができるため，変更管理のプロセス（10.1.2）及び手順

（12.5.1）が利用できる。

13 情報セキュリティインシデントの管理

13.1 情報セキュリティの事象及び弱点の報告

目的：情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。

事象の報告及び段階的取扱いの正式な手順を備えることが望ましい。すべての従業員，契約相手及び第三者の利用者に，組織の資産のセキュリティに影響を及ぼす場合がある様々な形態の事象及び弱点についての報告手順を認識させておくことが望ましい。すべての従業員，契約相手及び第三者の利用者に，いかなる情報セキュリティの事象及び弱点も，できるだけすみやかに指定された連絡先に報告するよう要求することが望ましい。

13.1.1 情報セキュリティ事象の報告

管理策

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけすみやかに報告することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの利用者が利用中に気づいた事象について報告し，集約できる体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデントを定義することが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウドサービスの利用者が理解し，発生時に報告できるようにすることが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウド事業者に報告できる手順を策定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。

クラウドサービスの関連情報

組織事業の基礎を成す情報及びその情報を取り扱うプロセス，システム並びにネットワークの多くを，組織内に保持する場合と比べて，クラウドサービス利用においてはサーバの監視やログの取得が自由にできないことが多い。リアルタイム監視や膨大なログの解析といったことを前提としたインシデントレスポンスを行うことができない場合は，事前に取得できる情報を明確にし，それを前提に判断できる内容を情報セキュリティインシデントとして定義しなおすことが期待される。

13.1.2 セキュリティ弱点の報告

管理策

すべての従業員，契約相手並びに第三者の情報システム及びサービスの利用者に，システム又はサービスの中で発見した又は疑いをもったセキュリティ弱点は，どのようなものでも記録し，また，報告するよ

うに要求することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスのセキュリティ上の弱点に気づいた場合に記録し，報告する手順を策定することが望ましい。クラウド利用者は，当該サービスにおいてセキュリティ上の問題を発見した場合に，クラウド事業者に報告する手順を策定することが望ましい。

13.2 情報セキュリティインシデントの管理及びその改善

目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。

情報セキュリティの事象及び弱点の報告があったとき直ちに，それらを効果的に取り扱える責任体制及び手順を備えることが望ましい。情報セキュリティインシデントへの対応，並びに情報セキュリティインシデントの監視，評価及び包括的管理に対して，継続的改善の手続をとることが望ましい。

証拠が必要となる場合は，法的要求事項を順守することを確実にするために，証拠を収集することが望ましい。

13.2.1 責任及び手順

管理策

情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするために，責任体制及び手順を確立することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティインシデントに対する迅速な対応ができるように体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデント発生時の対応責任者を決めることが望ましい。クラウド利用者は，情報セキュリティインシデント対応の手順にクラウドサービスに関連する内容を追加することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスにおける重大な情報セキュリティインシデントを定義することが望ましい。また，インシデント対応についての情報提供の方針を定め，クラウド利用者に提示することが望ましい。

クラウド事業者は，他の事業者との合意に基づき，サプライチェーン上で重大な情報セキュリティインシデントが生じたときに共有すべき情報を文書化することが望ましい。

クラウドサービスの関連情報

クラウドサービスではサーバのリアルタイム監視や，ログの柔軟な管理が困難なため，情報セキュリティインシデントにクラウドサービスの利用者が最初に気づく可能性がある。このため，情報セキュリティインシデントのエスカレーション手順を見直し，クラウドサービスの利用者からの情報提供が行われやすい環境を考慮する必要がある。

13.2.2 情報セキュリティインシデントからの学習

管理策

情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの情報セキュリティインシデントについて記録し定量化することが望ましい。クラウド利用者は，クラウドサービスに関するセキュリティインシデントを記録し，定量化することが望ましい。クラウド利用者は，事故の発生や影響を軽減するために定量化した情報をクラウド事業者と共有することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド利用者が情報セキュリティインシデントを評価できるよう，クラウド事業者は，クラウド利用者との合意に基づき次の情報を提供することが望ましい。

a) 情報セキュリティインシデントの統計情報
b) 情報セキュリティインシデントによる影響
c) 情報セキュリティインシデントへの対応
d) 情報セキュリティインシデントへの予防策

クラウドサービスの関連情報

クラウドサービスではサーバの監視やログ管理が困難なために，クラウド利用者は，サーバ上の情報セキュリティインシデントに関する情報を自ら取得することが難しい。そのため，クラウド利用者は，クラウド事業者の情報を基に情報セキュリティインシデントの定量化を行い，情報セキュリティインシデントの予測などを行うことができる体制づくりを考慮する必要がある。

13.2.3 証拠の収集

管理策

情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定めている証拠に関する規則に従うために，証拠を収集，保全及び提出することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，情報セキュリティ事故が法的処置に及ぶ場合を想定して，必要な証拠の収集，保全を実施することが望ましい。また，クラウド事業者がそれらの情報を保管しているか確認することが望ましい。

クラウド事業者がクラウド利用者の法的証拠となり得る情報を管理する場合，クラウド利用者は，次の手順を実施することが望ましい。

1. クラウド利用者にとって法的証拠となり得る情報を明確にする
2. クラウド事業者によって管理されている情報が記録され，適切に保管されているかを確認する
3. クラウド事業者によって管理されている情報を収集・保持する
4. 収集した情報の中で、クラウド利用者にとって証拠として活用できる情報を識別し、保全する

クラウド利用者は，クラウド事業者がクラウド利用者にとって法的証拠となり得る情報を管理する場合，

クラウド事業者に情報を求めることが望ましい。
クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を取得することが望ましい。クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を必要期間保存することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，法的な証拠となる可能性がある情報については記録し，適切に保管しておくことが望ましい。クラウド事業者は，どのような記録がどの程度の期間保管されているかをクラウド利用者に明示することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においてはコスト削減のために保存データの容量を必要最低限にすることがある。そのため，外部の継続的証拠保全のためのサービス（e-discovery サービスやリモートジャーナリングサービスなど）を別途契約するなどの方法もある。

14 事業継続管理

14.1 事業継続管理における情報セキュリティの側面

目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。

組織への影響を最小に抑えるため，及び予防的管理策と回復のための管理策との組合せによって，情報及び情報処理施設に関連する資産の損失（例えば，自然災害，事故，装置の故障及び悪意による行為の結果の場合がある。）を受容可能なレベルにまで回復するために，事業継続管理手続を実施することが望ましい。この手続では，重要な業務プロセスを識別すること，並びに運用，要員配置，資材，配送及び設備といった点で関連する，情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。

災害，セキュリティ不具合及びサービス停止の結果，並びにサービスの可用性を，事業の影響分析の対象とすることが望ましい。必要不可欠な運用の時機を失しない再開を確実にするために，事業継続計画を策定し，実施することが望ましい。情報セキュリティは，組織の包括的な事業継続手続及びその他の管理手続の，必要不可欠な部分であることが望ましい。

事業継続管理には，リスクを特定して低減するための管理策のほか，リスクアセスメントの手続に加え，損害を与えるインシデントの影響を抑制するための管理策，及び業務プロセスに必要な情報が常に利用可能であることを確実にするための管理策を含むことが望ましい。

14.1.1 事業継続管理手続への情報セキュリティの組込み

管理策

組織全体を通じた事業継続のために，組織の事業継続に必要な情報セキュリティの要求事項を取り扱う，管理された手続を，策定し，維持することが望ましい。

14.1.2 事業継続及びリスクアセスメント

管理策

業務プロセスの中断を引き起こし得る事象は，そのような中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス利用が事業継続にどのような影響を及ぼすかを判断し，要求事項としてまとめることが望ましい。クラウド利用者は，クラウドサービスが関与する業務を特定することが望ましい。クラウド利用者は，クラウドサービスが関係する資産を特定し，クラウドサービス利用に関連する情報セキュリティインシデントが業務に及ぼす影響を特定し，クラウドサービスの利用に係る事業継続についてリスク識別し，評価することが望ましい。

クラウド利用者は，リスクアセスメントにおいてはクラウド事業者と調整し，技術的・運営的な背景なども検討することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスのサービスレベルについて中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおけるサービスレベルは SaaS, PaaS, IaaS がそれぞれ依存関係にある場合もあり，特に SaaS では高稼働率を実現することが難しい場合がある。そのため，業務において本来必要な稼働率を検討し（例えば，システムの最大許容停止時間及び目標復旧時間の設定），SLA などによって確認することが期待される。

14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施

管理策

重要な業務プロセスの中断又は不具合発生の後，運用を維持又は復旧するために，また，要求されたレベル及び時間内での情報の可用性を確実にするために，計画を策定し，実施することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，リスクアセスメントの結果に応じて，クラウドサービスにおける冗長化の状況を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図ることが望ましい。

クラウド事業者は，クラウドサービスの冗長化の状況を，クラウドサービスの利用を検討する者に明示することが望ましい。

クラウドサービスの関連情報

事業継続管理におけるクラウドサービスの関係は情報システムの稼働率だけではなく，クラウドサービス上で作成されたデータを他のシステムに持ち出すことができるか，また現在利用しているシステムからデータを容易に持ち込むことができるかなども検討することが期待される。さらに，システムの最大許容停止時間を考慮してこれらの課題に対して検討する必要がある。クラウドサービスを提供するシステムの

冗長化を図る観点として，次のようなものがある。

a) データのバックアップ

b) データセンター

c) サポートユーティリティ（例えば，電源，ケーブル配線施設やそれらのコントローラなど）

d) ハードウェア

e) クラウドプラットフォーム

f) クラウド制御システム

14.1.4 事業継続計画策定の枠組み

管理策

すべての計画が整合したものになることを確実にするため，情報セキュリティ上の要求事項を矛盾なく取り扱うため，また，試験及び保守の優先順位を特定するために，一つの事業継続計画の枠組みを維持することが望ましい。

14.1.5 事業継続計画の試験，維持及び再評価

管理策

事業継続計画が最新で効果的なものであることを確実にするために，定めに従って試験・更新することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，事業継続計画の試験及び更新において，クラウド事業者が関与可能かを確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者の事業継続計画の試験・更新に関する協力可否について，クラウド利用者との合意に基づき情報を提供することが望ましい。

クラウドサービスの関連情報

クラウド利用者は，サービス可用性について適切な条項を契約に規定し，クラウド利用者の事業継続計画の試験・更新に組み込むことが推奨される。

クラウド事業者は，リソースやインフラなどの高集約によるインシデントの影響の拡大がクラウドの特徴であることを踏まえ，クラウドサービス提供にかかわるクラウド事業者組織における教育訓練の内容を適時に見直し，障害対応要員の定期的及び必要に応じた教育・訓練を実施することが期待される。

クラウド利用者が事業継続に係るリスクアセスメントを実施する際に考慮すべき事項には，次のようなものがある。

a) クラウドサービスの障害などによる停止

b) 法執行機関の要請によるサービスの一時停止

c) クラウドサービスの終了

d) 財務状況の変化に伴うクラウド事業者の変更

クラウド事業者は，クラウド利用者の事業継続計画策定・実施に関連して，クラウド利用者との合意に基づき，次のような情報を提供することが望ましい。

a) クラウド事業者の災害復旧計画

b) システムの多重化など，可用性を確実にするための対策

c) クラウドサービスの目標復旧時間

15 順守

15.1 法的要求事項の順守

目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

情報システムの設計，運用，利用及び管理には，法令，規制及び契約上のセキュリティ要求事項が適用される場合がある。

特定の法的要求事項については，組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法律の定める要求事項は，国ごとに異なっており，また，一つの国で作成され別の国へ伝送される情報（すなわち，国境を越えたデータの流れ）についても異なる場合がある。

15.1.1 適用法令の識別

管理策

各情報システム及び組織について，すべての関連する法令，規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を，明確に定め，文書化し，また，最新に保つことが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドコンピューティングサービスに関する法執行機関が，複数の国／地域に関連し得ることを鑑み，クラウド事業者に対して情報提供を求めることが望ましい。クラウド利用者は，クラウドコンピューティングサービスに関する管轄裁判所について，クラウド事業者に対して情報提供を求めることが望ましい。

クラウド利用者は，クラウドサービスの利用目的に応じて，クラウド利用者自らが適用を受ける法令，規制及び契約上の要求事項などを洗い出すことが望ましい。クラウド利用者は，クラウドサービスの利用契約に定められた準拠法と裁判管轄を確認し，文書化することが望ましい。クラウド利用者は，クラウド事業者が適用を受ける法令を調査し，文書化することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，複数の国／地域の法執行機関がかかわるクラウドサービスを提供している場合，それらの国／地域についてクラウド利用者に知らせることが望ましい。クラウド事業者は，国家連合，国，州，地方自治体により法規制が異なるかを確認し，それぞれの国家連合，国，州，地方自治体の名称をクラウド利用者に明示することが望ましい。クラウド事業者は，関連する法規制について，それぞれの管轄裁判所の場所を明示することが望ましい。

クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。

クラウド事業者は，他のクラウド事業者が提供するクラウドサービスを利用している場合，利用しているクラウドサービスの裁判管轄及び適用を受ける法令・規制を確認・文書化し，最新に保つことが望ましい。

クラウド事業者は，クラウド利用者との合意に基づき，法令，規制及び契約上の要求事項が適用される地理的場所にクラウド利用者のデータが保持されていることを確実にするため，法的順守を監視することが望ましい。

クラウドサービスの関連情報

SaaS として契約しているクラウド事業者が国内企業であったとしても，そのバックボーンとなる PaaS や IaaS のクラウド事業者が海外の企業である場合もあるため，クラウド事業者が事業を行う国の法律や業界団体の慣習などについても洗い出し，検討することが期待される。

適用法令は，私法と公法を分けて識別することが望ましい。例えば，私人間に適用される法は「当事者が当該法律行為の当時に選択した地の法による」（法の適用に関する通則法第 7 条）である。つまり，契約時に準拠法を定めるのが一般的であるため，契約当事者間の適用法令が問題になることは少ない。一方，国家がかかわる公法の適用は，原則として属地的に定まる。外国法人でも日本国内において事業を行う限り，原則として国内法の適用を受け，逆に日本法人でも外国において事業を行う限り，外国法の適用を受けることがある。例えば，データセンターが外国にあっても我が国で事業を営む企業は，我が国の捜査機関の捜査を受け，外国のサーバ内の情報が差押えられることがあり，逆にデータセンターが国内にあっても外国で事業を営む企業は，その国の捜査機関の捜査を受け，我が国のサーバ内の情報が差押えられることがある。

15.1.2 知的財産権（IPR）

管理策

知的財産権が存在する可能性があるものを利用するとき，及び権利関係のあるソフトウェア製品を利用するときは，法令，規則及び契約上の要求事項の順守を確実にするための適切な手順を導入することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウド利用の目的に合せ，知的財産権の要求事項を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を，クラウド利用者に通知することが望ましい。

15.1.3 組織の記録の保護

管理策

重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービス上で利用する重要な記録は法令や規制に従って保護することが望ましい。クラウド利用者は，クラウドサービス上で利用する重要な記録は必要に応じて取り出せるように

保管することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，法令や規制に従って，クラウドサービス上の記録を保護することが望ましい。

クラウドサービスの関連情報

クラウドサービスでは，国内外問わず，様々なクラウド事業者を利用する事ができる。しかし，クラウド事業者の中には，特定国内における法律に対応できないクラウド事業者がある可能性もある。そのため，遵守すべき法律を考慮して記録の保管を適切に行うことができるクラウド事業者を選択するか，自ら記録を保管する体制を構築することが期待される。

15.1.4 個人データ及び個人情報の保護

管理策

個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスで個人情報を利用する際には，法令及び組織の個人情報護方針に従って利用できるように適切な手順を策定することが望ましい。

クラウド利用者は，クラウドサービスの利用目的に応じて，データ保護及び個人情報保護に係る，国内外の法令，規則及び契約上の要求事項を識別することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者がデータの保護及び個人情報保護に関する法規制を識別できるよう，自らのクラウドサービスに影響を及ぼす法的管轄に関する国／地域の情報を提供することが望ましい。

クラウドサービスの関連情報

個人情報保護法の要求事項及び当該要求事項の実現のために企業等が定める規程に対応できないクラウド事業者が存在するかもしれない。そのため，個人情報保護に関する基準や手順がクラウド事業者の提供するクラウドサービスに合致するかどうかを検討することが期待される。

15.1.5 情報処理施設の誤用防止

管理策

認可されていない目的のための情報処理施設の利用は，阻止することが望ましい。

15.1.6 暗号化機能に対する規制

管理策

暗号化機能は，関連するすべての協定，法令及び規制を順守して用いることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，暗号技術をクラウドサービス上で利用する際には，輸出規制などに抵触しないか確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウド利用者が輸出規制などに抵触しないよう，暗号化機能にかかわる法令などの情報をクラウド利用者に提供することが望ましい。

クラウドサービスの関連情報

暗号化技術については輸出規制などの問題もあり，海外のクラウド事業者のデータセンターに配置できない場合もある。クラウドサービス上で暗号化機能を利用する場合には，輸出規制などに抵触する可能性について十分に検討する必要がある。

15.2 セキュリティ方針及び標準の順守，並びに技術的順守

目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。

情報システムのセキュリティは，定めに従ってレビューすることが望ましい。

このようなレビューは，適切なセキュリティ方針及び技術的基盤と対照して行うことが望ましい。また適用されるセキュリティ実施標準及び文書化されたセキュリティ管理策を順守していることについて，情報システムを監査することが望ましい。

15.2.1 セキュリティ方針及び標準の順守

管理策

管理者は，セキュリティ方針及び標準類への順守を達成するために，自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスに関連する新しい規程や管理策が既存の規程や管理策同様に順守されるようにすることが望ましい。クラウド利用者は，クラウドサービスに関連する標準や手順が，既存の情報セキュリティ基本方針に合致しているかをレビューすることが望ましい。クラウド利用者は，クラウドサービスが情報セキュリティ基本方針に合致しない場合，原因を調査し，必要に応じて双方を是正することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，独立したレビュー及び評価（例えば，内部／外部監査，認証，ぜい弱性，ペネトレーションテストなど）を定期的に実施し，情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。また，クラウド事業者は，クラウド利用者の個別の監査要求に応える代わりに，クラウド利用者との合意に基づき，独立したレビュー及び評価の結果を提供することが望ましい。

クラウドサービスの関連情報

クラウドサービスの利用においては現在運用している管理策やセキュリティ要件に合致する機能を有していない場合が考えられる。特に SaaS においては，個別に機能の付加が容易ではないため，必要に応じてその他のサービスを利用したり，代替する機能を検討したりすることが望ましい。PaaS においても場合によってはこれまでに利用してきた API などが利用できないこともある。そのため，実行環境の制限などを十分に精査して，セキュリティを損なわないように標準などを見直すことが期待される。

15.2.2 技術的順守点検

管理策

情報システムを，セキュリティ実施標準の順守に関して，定めに従って点検することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検することが望ましい。クラウドサービスでは様々な機能がクラウド事業者主導で追加されることがあるため，クラウド利用者は，これらの機能が組織の技術的なセキュリティ要求事項に合致しているかを確認し，必要に応じて様々な機能の利用の可否を決定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検し，その結果を情報提供の方針に基づいてクラウド利用者に開示することが望ましい。

クラウドサービスの関連情報

SaaS では機能の追加がされた場合に，一般利用者権限で機能の利用が可能になる場合がある。クラウド利用者は，セキュリティ要求事項に合致しない機能は管理者権限で停止できるかどうかを確認し，必要に応じて機能の制限ができることを確認することが期待される。

15.3 情報システムの監査に対する考慮事項

目的：情報システムに対する監査手続の有効性を最大限にするため，及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。

情報システムの監査中には，運用システム及び監査ツールを保護するための管理策があることが望ましい。

監査ツールの完全性を守るため，及びその不正使用を防止するための保護も要求される。

15.3.1 情報システムの監査に対する管理策

管理策

運用システムの点検を伴う監査要求事項及び活動は，業務プロセスの中断のリスクを最小限に抑えるために，慎重に計画され，合意されることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドサービスの監査について方針を定めることが望ましい。クラウド利用者は，クラウドサービスを監査する場合において，全体的な業務プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドサービスの監査について方針を定め，監査を定期的に実施することが望ましい。クラウド事業者は，クラウドサービスを監査する場合において，全体的な業務プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。

また，クラウド事業者は，クラウド利用者との合意に基づき，利用者の情報システム監査実施に有用な情報を提供することが望ましい。

クラウドサービスの関連情報

クラウド事業者を監査対象に入れた場合，複数のデータセンターにデータが分散されていたり，実際のデータの所在がどのサーバにあるのかを特定することができないなど，物理的に幾つかの管理策に対して

監査が実施できないという問題に直面する可能性がある。そのため，クラウド事業者の監査についてはどのような監査を実施するか，あらかじめ監査項目や監査手順を明確にし，監査を実施することが期待される。

クラウド利用者は，利用するクラウドサービスについて自ら監査を実施する代わりに，クラウド事業者が提供する監査報告書を確認することができる。

15.3.2 情報システムの監査ツールの保護

管理策

情報システムを監査するツールの不正使用又は悪用を防止するために，それらのツールへのアクセスは，抑制することが望ましい。

附属書 A（参考）クラウドサービス利用にかかわるリスク

クラウドサービスの利用にかかわるセキュリティリスクを特定するため，先ずクラウドサービスと従来からある類似サービスとを比較する。

クラウドサービスは，共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理サービスである。これと類似のサービスには，データセンターにおけるアウトソーシングの一形態として，ハウジングサービス，ホスティングサービス，又はアプリケーションサービスなどがある。

クラウドサービスとこれら従来型の類似サービスは，どちらもネットワークを通じてデータセンターから提供され，ファシリティやコンピュータリソースを他者と共有することがある点で共通の特徴をもつ。クラウドサービスにかかわるリスクを検討する場合，これら従来型の類似サービスにおけるリスクは依然として存在する（図 5 参照）。

一方，クラウドサービスは，共有化されたコンピュータリソースをクラウド利用者の要求に応じて適宜・適切に配分するために仮想化技術や分散技術を駆使して提供されることが多いが，従来型の類似サービスは，必ずしもこれらの技術が用いられているとは限らない。これらの技術がクラウドサービスのみに用いられているわけではないが，仮想化・分散技術にかかわるリスクとその技術の運用にかかわるリスクは，クラウドサービスにおいて特に考慮すべきリスクであるといえよう。

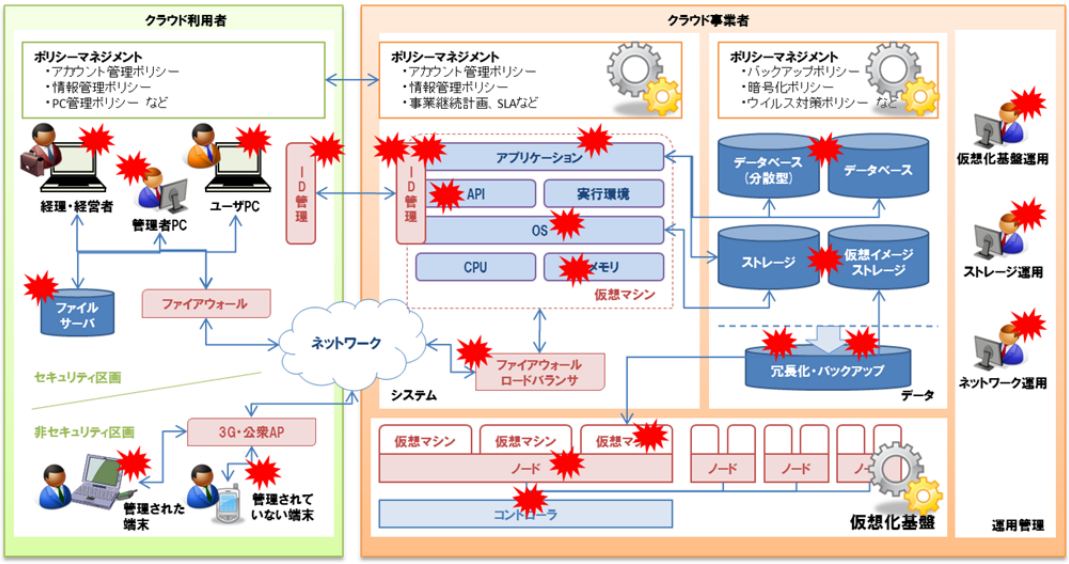


図 5　クラウドサービス利用にかかわるリスク

以下に，クラウドサービスにおいて考慮すべきリスクを例示する。セキュリティ以外の信頼性や稼働性に関するリスクについても参考までに含む。以下のリスクに関して，クラウド事業者は低減するべく努力をすることは当然のことであるが，クラウド利用者についてもリスクを認識し，クラウド事業者の対策を確認することが望ましい。

DoS 攻撃

クラウドサービスはネットワークで提供されるため，DoS 攻撃を受けた場合，すべてのサービスが停止してしまう可能性がある。DoS 攻撃を防御するための仕組がクラウド事業者に依存するため，クラウド利用者は対策を講じることができない。クラウド利用者は，このようにクラウド事業者しか対応できない問題については，あらかじめクラウド事業者に管理策を確認し，DoS 攻撃のリスクを受容するか検討を要する。

ID 管理

クラウドサービスによっては，クラウド利用者が既に利用している ID 管理とクラウドサービスにおける ID 管理を一元的に実施するためのインタフェースがない場合がある。その場合は，管理者の ID 管理に関する工数が増大し，一貫したセキュリティ対策及び管理を行うにあたってミスが発生する可能性が高くなる。そのためクラウド利用者は，ID 管理の連携ができるクラウドサービスを選ぶか，ID 管理が困難になるリスクを受容するか検討を要する。

アクセスポイント

公衆無線 LAN や 3G 回線などによる携帯電話網の普及によって，様々な場所からクラウドサービスを利用できるようになり，ネットワークにおけるアクセス制御が困難になっている。そのため，クラウド利用者は，アクセスポイントを制御できるクラウドサービスを選ぶか，あらかじめ，利便性はあがるが管理は困難になる，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

アクセス制御

利用するクラウドサービスによっては，あらかじめ定められたアクセス権限が，組織で想定するアクセス権とは異なり，アクセス制御が困難になる場合がある。そのため，クラウド利用者は，アクセス制御が管理できるクラウドサービスを選ぶか，あらかじめ，クラウドサービスが定めたアクセス制御を受入れることによるリスクを受容するか検討を要する。

アプリケーション

主に SaaS で提供されるアプリケーションはデスクトップ上で提供されるアプリケーションと違い，機能が制限されていることがある。例えば，デスクトップ用のアプリケーションデータをインポートした場合にすべての条件が反映されないような場合である。また，クラウドサービスで提供されるアプリケーション同士もデータの互換性が十分であるとはいえない。そのため，クラウド利用者は，互換性の高いクラウドサービスを選択するか，あらかじめ互換性に制限がある，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

インシデント管理

インシデント管理には様々な情報が必要になるが，クラウドサービス利用において自らが入手できる情報が制限される場合，クラウド利用者が主体となった対応ができなくなる可能性がある。特に，クラウド事業者が考えるインシデントやイベントのレベルと利用者組織のレベルが合致していないことにより，定められた対応がされなかったり，その発生によるビジネスに対する影響が明確にできなかったりする課題がある。そのため，クラウド利用者は，契約時にインシデントやイベントのレベルを合意するか，あらかじめクラウドサービスが定めたインシデントやイベントのレベルを受入れることによるリスクを受容するか検討を要する。

クラウド事業者の事業継続

クラウド事業者が何らかの理由により事業継続が困難となった場合，若しくは，クラウドサービス自体を戦略的に停止することになった場合，そのクラウド事業者が提供するクラウドサービス利用が制限され，クラウドサービス上の情報が利用できなくなり，クラウドサービス上に保存された情報が消失する可能性がある。そのため，クラウド利用者は通常の取引先としての信頼性の確認だけでなく，クラウドサービスを行う事業部の継続性も確認して，クラウドサービスの利用を決定し，また，クラウドサービスの停止はクラウド事業者が決定するというリスクを受容するか検討を要する。

システム運用・保守

クラウドサービスではシステム自体の保守をしなくても良いというのがメリットの一つではあるが，情報セキュリティの観点では業務の委託はできても責任をすべて委譲することはできない。クラウドを利用していない環境でのセキュリティ規程を満足させるために様々な情報が必要になる。

スケールアウト技術

クラウドコンピューティングにおけるスケールアウトという技術により，ハードウェアを仮想的に連携させ処理能力の高いハードウェアを形成することができる。ハードウェア単体における物理的な能力を超えた環境についての検証が十分できないことから，未知のトラブルが発生する可能性がある。新たな技術の導入に伴う未知のリスクは予知し難く，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

データセンターの所在

様々な国や場所にデータセンターが設置される場合の，データセンターに従事する従業者の経験やモラルなどによる情報の取扱いの差が，クラウド利用者の懸念事項として挙げられている。様々な国のネットワークの接続性などに伴って，サービスの質などの差による影響が出る可能性が考えられている。そのため，クラウド利用者は，あらかじめデータセンターの所在地の法規の適用にかかわる問題を認識してリスクを受容するかの検討を要する。

データセンターの物理環境

利用者からみたデータセンターのありようは大きく変化していないと考えられるが，クラウドサービスを提供するために新たな技術や運用形態（コンテナ式など）を利用したデータセンターが運営されており，クラウド事業者が経験していない問題が発生する可能性がある。クラウド利用者は，新たな技術や運用形態に起因するリスクの移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

ヘルプデスク

海外のクラウドサービスを利用している場合，ヘルプデスクサービスの対応言語が異なったり，時差や営業日の違いによってサービス日・時間帯が国内と異なる場合がある。そのため，クラウド利用者は，あらかじめ対応言語や対応時間などにかかわるリスクを受容するか検討を要する。

マルチテナント

一つのプラットフォーム上に複数の契約者が同居することにより，プラットフォームを狙った攻撃が実施された場合に対象ではないほかの契約者にも影響が及ぼされることになる。特にクラウドサービス環境においては，どの契約者とどの契約者が同じシステム内で同居しているかがわからないことが問題となる。そのため，クラウド利用者の管理の不備によって引き起こされるリスクについて検討した後，他の契約者の管理不備によって引き起こされるリスクについても検討を要する。

メモリ管理

クラウド事業者では物理的なメモリ管理などが実行できないために，メモリ保護に関するトラブルが発生した場合の問題について，ハードウェアが原因か，仮想化などによる技術的な問題かを切り分けを行うことが難しい。クラウド利用者は，このような技術的なトラブルに対するリスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

メンテナンスユーティリティ

システムの状況を知るためのユーティリティが提供されないことによって，情報を適宜入手することができないという課題がある。情報を入手できないことでトラブルの事前判断ができないだけではなく，経営面からみてITの活用状況がわからないなどの課題もある。そのため，クラウド利用者は，あらかじめ情報の把握が困難になるリスクを受容するか検討を要する。

ライセンス管理

クラウドサービスを前提に作成されていないソフトウェアのライセンス体系により，クラウドサービス上でソフトウェアがどのように利用されているのかを正確に把握できないことがある。そのため，ソフトウェア監査におけるトラブルへ発展することがある。クラウド環境を見越したライセンス体系をもつソフトウェアも増加しており，クラウド利用者は，利用するソフトウェアのライセンスの再確認や，場合によっては契約の再確認を要する。

リカバリー

クラウドサービスを利用して顧客向けサービスを提供しているような企業や組織においては，復旧計画を正確に顧客に知らせることができないという問題が発生する。SLA による復旧予定を通知できる場合は，それを通知するが，それ以外の場合は，通知は困難である。また，クラウドサービスが顧客向けサービスの唯一のインタフェースである場合は，通知自体も不可能になるため，クラウド利用者は代替策を講じるか，リスクを受容するか検討を要する。

ログ監視

サーバへのアクセスなどネットワークに関するログを取得することができないクラウドサービスでは，サーバのスキャニングなどが行われていることなど，自らの資産が危機にさらされているかもしれないという事実を知ることが難しく，事前に対策をすることができないという課題がある。そのため，クラウド利用者は，ログ監視と対応を行っているクラウドサービスを選ぶか，あらかじめスキャニングなどの認知は困難である，ということを認識してクラウドサービスを利用するリスクを受容するか検討を要する。

暗号化

クラウドサービスの多くは SSL/TLS を利用した暗号化通信を選択することができるが，対応していないサービスを提供している事業者や，クラウド事業者内の経路では暗号化通信を行っていない場合もある。そのような場合には，機密データや重要データのやり取りにおいて暗号化を規定しているにもかかわらず，クラウド事業者のネットワーク上でデータが暗号化されないという課題がある。クラウド利用者は，暗号化されないことのリスクを受容するか検討を要する。

仮想化対応

仮想化環境においては，CPU やメモリなどの利用が物理的に行われた場合とは異なる管理が行われることがある。また，ネットワークやストレージなども仮想化され単一機器と動作が異なる場合もあり，リスクを生む可能性がある。仮想化環境を前提としたアプリケーションの設計が行われていない場合，処理速度が低下するだけではなく，必要以上のコンピュータリソースを使用することで，クラウド本来のメリットであるコスト削減などに寄与しないという問題も考えられる。このような問題に対して，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

携帯電話・スマートフォン

携帯電話やスマートフォンは，PC に比べてセキュリティ対策を行うためのオプションが少なく，本格的な運用実績も少ないため，クラウドサービスが携帯電話やスマートフォンから利用できる場合は，トラブルに関する情報や対策についての十分な情報が得られないという課題がある。そのため，クラウド利用者は，携帯電話やスマートフォンによる利用を制御できるクラウドサービスを選ぶか，あらかじめ利便性はあがるが管理は困難になる，ということを認識してリスクを受容するか検討を要する。

最大許容停止時間

システムの最大許容停止時間について明確な指針が必要になる。最大許容停止時間は，クラウド事業者が定めるものであり，クラウド利用者は，クラウド事業者の定めに応じて復旧を待たねばならない。サービスにおける稼働率は SLA などの契約で定められるが，クラウド利用者は，最大許容停止時間の実態を確認するためにも過去のトラブルの状況などを問い合せ，これまでにどの程度サービスが停止したことがあるか，クラウド事業者の改善策によってその問題が解決しているかなどの確認を要する。

残存データ

メモリ上，ハードディスク上にデータが残ってしまった場合の処理について仮想化された環境で十分にこれらを制御することができるかどうか，可視化できない問題がある。そのため，クラウド利用者としては，クラウドサービスにおけるこれらの残存データの処理方法についてクラウド事業者が講じている技術的な処理方法についての情報を得るか，残存メモリ・残存オブジェクトが発生するリスクを受容するか検討を要する。

実行環境の制限

クラウドサービスでは提供される実行環境に制限がある場合が多い。アプリケーションによっては必要なライブラリが使えないことによって，動作しないことも考えられる。PaaS ベンダーによっては独自の開発言語やビジュアルエディタのみによる開発環境の提供により，他社のサービスを利用できないという問題が発生する。そのため，クラウド利用者は，汎用性のある実行環境を提供するクラウドサービスを選択するか，あらかじめ実行環境に制限があるリスクを受容するか検討を要する。

従量課金を利用した攻撃

クラウドサービスの契約形態によっては，利用したリソースに応じた使用料が課金される。この特性を利用して，処理を必要以上に増加させる攻撃が外部から行われることがある。DoS 攻撃のようにサービスの利用を妨げるのではなく，経済的に事業継続を不可能にする攻撃である。このような経済的な攻撃を EDoS（Economic Denial of Sustainability）と呼ぶことがある。クラウド利用者は，EDoS 攻撃により発生した使用料に関してクラウド事業者とあらかじめ取決めを交わすか検討を要する。

接続性

クラウドサービスは国内だけではなく，海外でも展開され，国内からの利用も増えている。国内外を問わず，事業者は様々な場所にクラウドサービスを提供するためのデータセンターを展開しており，かつそれらが連携して運用されている。そのため，ネットワーク構成が複雑になり，接続の信頼性を把握することができないという課題がある。そのため，クラウド利用者は，接続性にかかわるリスクの移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

相互運用性

クラウドサービスに関連する様々な標準化（技術，データ形式，サービス形態など）が行われていない現状では，アプリケーションのデータや作成されたシステムのイメージデータなどが，他のサービスで利用できなかったり，システム同士の連携ができなかったりという問題が発生する可能性がある。そのため，クラウド利用者は，相互運用性の高いクラウドサービスを選択するか，あらかじめ相互運用性にかかわるリスクを受容するか検討を要する。

中間者攻撃

データセンターが様々な場所で展開され，かつ連携していることを前提とした場合，1 対 1 の接続の場合に比べて中間者攻撃を受けやすくなっている。また，マッシュアップなどによってサービスが構成されている場合などは更に攻撃の機会が増えると考えられる。このような中間者攻撃に起因する被害の発生について，クラウド利用者は，リスク移転（利用料の減額など）が可能か，それともリスクを受容するか検討を要する。

分散管理

クラウドサービスでは冗長性や拡張性がそのメリットとして挙げられているが，反面これらのメリットを実現するための分散管理などの管理手法が，対象としている情報及びシステムの構造を複雑にし，クラウド利用者からの可視化を妨げており，情報やシステムの一元管理を実施しにくくしている。そのため，クラウド利用者は，クラウド事業者が使用する技術によっては，データの所在を明確に把握できないことによるリスクを受容するか検討を要する。

附属書 B（参考）クラウドサービス利用におけるリスクアセスメントの実施例

JIS Q 27002（実践のための規範）の管理目的及び管理策は，リスクアセスメントによって特定した要求事項を満たす形で実施することを意図している（図 6 参照）。情報セキュリティマネジメントにおいて，リスクアセスメントは，管理策を実施するリスク対応に先行するプロセスとして位置づけられるが，クラウドサービス利用におけるリスクアセスメントを実施した具体例はあまり知られていない。そこで，以下にクラウドサービス利用におけるリスクアセスメントの実施例を示す。

以下は，情報セキュリティマネジメント及びクラウドサービスに活用されている技術などを対象に，リスクが存在すると思われる要素を洗い出し，リスクアセスメントを実施したものである。

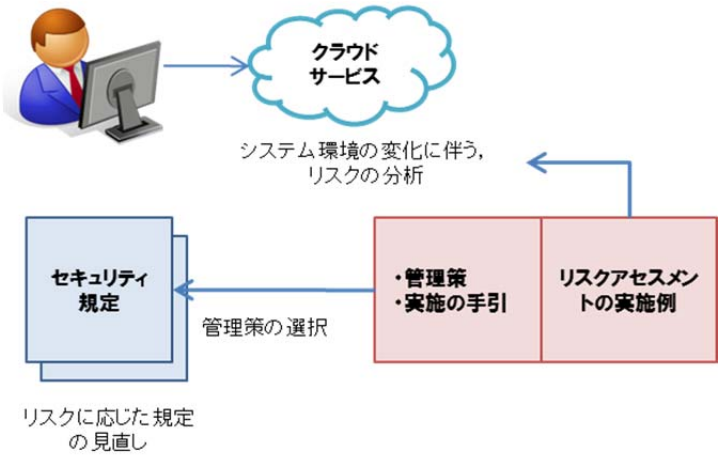


図 6　リスクアセスメントと管理策

クラウドコンピューティング環境とセキュリティリスク

クラウドコンピューティングでは，ネットワーク上に様々なリソースが配置されるとともに，管理主体がクラウド事業者にある。図 7 のようにクラウド環境の全体像を想定すると，管理対象を「クラウド利用者環境」，「クラウド事業者のシステム環境（仮想環境，データ環境）」，双方を接続する「ネットワーク」に分けることができる。また，運用環境においては「ID 管理」，「ログ管理」，「構成管理」，「物理的セキュリティ管理」に分類できる。

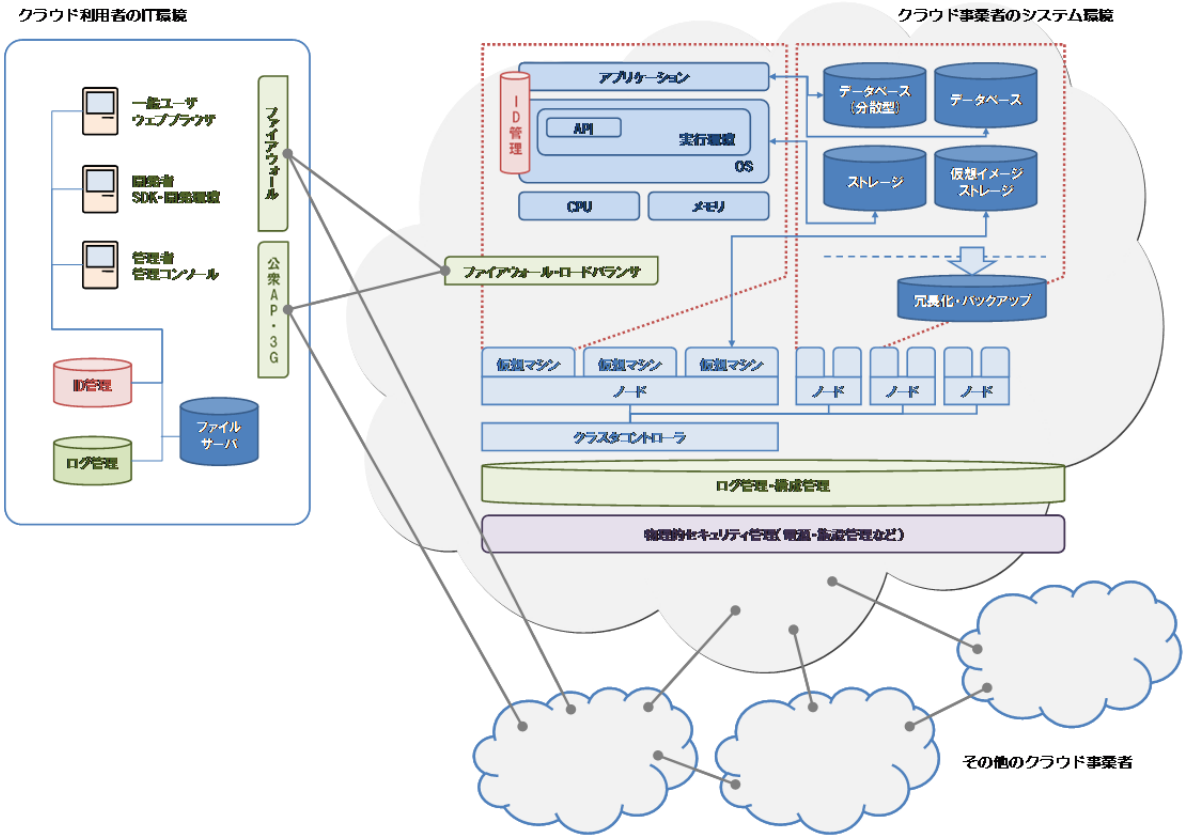


図 7　クラウド利用者からみたクラウドシステムの全体構成（例）

これらの分類を基に，クラウド利用者自らが管理したいにもかかわらず，自由に管理することができない管理対象，運用環境の部分は何かを精査することにより「プロセスに関するリスク」を洗い出すことができる。

組織内では，事故が発生した際に迅速に対応するために，情報セキュリティインシデントの検知機能や，インシデントを想定した回復策などを自ら用意することができた。しかしながら，クラウドコンピューティング環境においては，情報システムの停止の判断，侵入や不正アクセスの検知に関してクラウド事業者からの連絡を待つしかないこともある。

そのため，システムの停止にかかわるような事項については SLA などの契約によって対策を講じることができるが，日常的なシステム関連情報の収集は組織内ほど自由にはならない。

また，SLA の内容によっては短時間のサービス停止を対象としないなど，内容がクラウド事業者によって異なることがあり，個別に詳細を判断しなくてはいけない場合がある。組織内では自由に管理できたもので，ネットワーク上で自由に管理できないものにはデータが挙げられる。クラウドコンピューティング上で扱うデータを精査することにより「データに関するリスク」を洗い出すことができる。

クラウドコンピューティングによって取り扱われるデータの形態にはデータベース上のデータだけではなく，クラウドコンピューティング独自の分散技術を用いて管理されるもの，仮想化環境を構築するための仮想イメージデータ，それらのもととなる仮想イメージデータのテンプレートなどがある。

クラウドコンピューティング環境では, データが組織内のファイルサーバ上や個別の PC 上にあった場合のように機密レベルに応じて暗号化を行ったり，パスワードを付与したりという管理策を実施することができない場合もあり，データの管理方法について再度リスク分析を実施し，適切な管理策を選択する。
また，仮想化環境を構築する仮想イメージデータについてもクラウド利用者からは自由に扱うことが難しい。環境を構築する仮想イメージデータについての管理を適切に行うためにもクラウド事業者との連携を考慮する。

データ全般で考えれば，クラウド利用者は，バックアップの実施についても組織内のように管理することが難しい。バックアップのルールがクラウド事業者の定義による場合は，バックアップデータを，いつでも復旧できるような環境を構築することができない場合がある。その場合は，情報システムにおける事業継続管理において，データを自ら補完することを選択するか，サービス内容の検討を行うか，システム停止の受容レベルについて再度検討する。

クラウドコンピューティングではネットワーク経由でコンピュータリソースを利用するために，ネットワークの接続性と，十分な帯域が確保されていることが前提となる。組織が契約している外部ネットワークサービスに問題が発生した場合，コンピュータリソースの大半が利用できなくなるという問題もある。また, 組織のネットワークに問題がない場合でも, クラウド事業者のネットワークに問題が発生した場合, コンピュータリソースが利用できなくなる。

図 7 ではクラウド利用者とクラウド事業者，そしてクラウド事業者同士がネットワークを経由して接続されている様子を示している。サービスによってはクラウド事業者が連携して提供している場合もあれば, クラウド利用者が複数のクラウド事業者と契約して一つの業務システムを構築している場合もある。このような関係性を理解し，ネットワーク接続について精査することにより「ネットワークに関するリスク」を洗い出すことができる。

クラウド技術の一つである仮想化においては，それぞれの仮想環境を構築するために内部でネットワークが構築されている。それぞれの仮想環境を構成するハードウェア及びソフトウェアは暗号化通信又はネットワークの隔離を行うことにより経路上の安全を確保することができるが，クラウド利用者からは実施できない項目の一つとなっている。

管理的セキュリティの視点では，ID 管理，ログ管理，物理的セキュリティ管理などが，クラウド利用者にとって管理したくてもできない項目として挙げられることがある。

図 7 のように，クラウド上で提供されるアプリケーションやオペレーティングシステム，実行環境，API では, 単にシステム管理者への権限付与だけではなく, 利用者への ID が発行される場合がある。その際に, クラウド利用者が保有している ID 管理のシステムと整合性をとることができるか，またクラウド上の ID 管理がクラウド利用者の ID 管理のルールと適合するかどうかという問題がある。適切な情報セキュリティ管理を実施するために，クラウドサービスを利用するなら，クラウド事業者の ID 管理の方針を理解し，適合する。

同様の問題はログ管理においても考慮する。情報セキュリティインシデントに対する分析に際しては，ログを参照することが重要となるが，クラウド事業者が提供するログによっては，分析に足る情報が得られるとは限らない。

ID 管理やログ管理のようにクラウド利用者とクラウド事業者の双方が保有している場合は，整合をとる必要性について考慮する。

物理的セキュリティ管理はクラウド事業者の責任範囲であるが，データセンターによっては十分なサポートユーティリティが提供されないことがある。大規模なデータセンターの設営に対して，十分な電源が提供されない，災害によって十分なリソースが提供されないといった問題が考えられる。

データセンター内で業務を行う担当者の不正などについてはクラウドサービス以前と大きく変化はないが，データが集約されるクラウドサービスの環境では，影響の大きさを考慮しなければならない事項であり，クラウド事業者は人的な不正の発生を防ぐための物理的セキュリティを考慮する。

図 7 ではクラウドコンピューティング環境を簡単に示したが，実際には更に複雑な構造となっており，環境によっては新たな考慮事項が発生するかもしれない。しかしながら，基本的な形でのクラウドコンピューティング環境を把握しておくことにより，十分なリスクアセスメントを実施することができる。

リスクアセスメントの方法とマトリクスの活用例

本実施例では，提供されるリソースの変化，ユーザ環境，事業者におけるサービスにかかわるプレイヤーごとに，SaaS，PaaS，IaaS のそれぞれについて，管理情報及び取扱いデータにおける管理の可否について検討した。検討に当たっては，マトリクスを活用し，リスクを可視化する試みを行った。

なお，今回のリスクアセスメントにおいては，利用者組織を特定したわけではないため，情報資産の重要度や可用性，完全性，機密性が損なわれた場合の影響度については検討していない。

SaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実行した。

利用者側には「一般ユーザ」及び一般ユーザを管理する「ユーザ管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，SaaS で用意されている業務アプリケーションやオフィスアプリケーションを利用している。ユーザ管理者はそれら一般ユーザを管理するための ID を所有し，SaaS 事業者により用意されたユーザ管理インタフェースを利用できる権限をもつている。

クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発，緊急トラブルへの対応などを行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

この事例での SaaS 事業者はシステムのインフラも含めて自社で運用を行っており，他社の IaaS，PaaS といったサービスは利用していない。

表 1　SaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		SaaS利用者		クラウド事業者	
		一般ユーザ	ユーザ管理者	運用担当者	開発技術者
ユーザアプリケーション	操作	●	−	−	−
	設定	●	−	−	−
	ログ閲覧	−	●	−	−
ID管理	操作	−	●	−	−
	設定	−	●	−	−
	ログ閲覧	−	●	−	−
API	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
実行環境	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
OS	操作	−	−	●	−
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
ファイアウォール	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
仮想マシン	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●
ホストマシン	操作	−	−	−	●
	設定	−	−	−	●
	ログ閲覧	−	−	●	●

システム管理の側面から，リスクアセスメントを実施した（表 1 参照）。

一般的な SaaS においては，利用者組織はアプリケーションの利用と ID 管理のみが実施できるようになっている。ID 管理においては組織内のワークフローに対応するような役職による設定を行うことができず，機能のオンオフしかできない場合もある。

表では「API」以下の項目について利用者は直接操作，設定，ログ閲覧などができず，運用状況の把握などもクラウド事業者の報告が必要となる。つまり，情報システムの状態を詳細に把握できないという問題が発生する。

表 2　SaaS におけるデータ管理面における管理の可否（例）

対象データ（クラウド上）		SaaS利用者		クラウド事業者	
		一般ユーザ	ユーザ管理者	運用担当者	開発技術者
ユーザアプリケーションデータ	閲覧	●	－	－	－
	変更	●	－	－	－
	削除	－	●	－	－
	暗号化	－	●	－	－
	分類	●	－	－	－
ストレージデータ	閲覧	－	－	●	●
	変更	－	－	－	●
	削除	－	－	－	●
	暗号化	－	－	－	●
	分類	－	－	－	●
仮想イメージデータ（運用中）	閲覧	－	－	●	●
	変更	－	－	－	●
	削除	－	－	－	●
	暗号化	－	－	－	●
	分類	－	－	－	●
仮想イメージデータ（テンプレート）	閲覧	－	－	●	●
	変更	－	－	－	●
	削除	－	－	－	●
	暗号化	－	－	－	●
	分類	－	－	－	●
バックアップ	作成	－	－	●	●
	削除	－	－	●	●

次にデータ管理の側面からリスクアセスメントを実施した（表 2 参照）。

ユーザが管理できるのは SaaS で提供されているアプリケーションのデータのみであり，完全な削除という点では管理者のみが実施できるように設定されていることがある。利用者はデータ全体のバックアップを実施したり，アプリケーションの設定状況などのバックアップを実施することができない場合がある。

SaaS で提供されるアプリケーションそのものが特別な場合もあるので，一概に判断することはできないが，データのバックアップや移行ができないという問題が発生する。

SaaS においては以下の問題をリスクとして識別することができた（一部抜粋）。

- システム管理において，システムの状態を把握することができない
- ID 管理においてアプリケーションが提供した粒度での管理のみ実施できる

- ID 管理におけるトレーサビリティの確保が難しい
- アプリケーションデータのバックアップができない
- アプリケーションデータの移行ができない
- アプリケーションデータの完全削除ができない
- アプリケーションデータの暗号化を一般的な暗号化ツールを利用して実施できない

このように，システム管理におけるリスクの識別，データ管理におけるリスクの識別に役立てることができる。ここで識別されたリスクと情報資産の重要性及び影響度を照らし合わせ，組織に見合った管理策及び実施の手引の選択を行う。

以下，PaaS，IaaS についても同様にマトリクスを利用してリスクの識別を行う。

PaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実施した。

利用者側には「一般ユーザ」及び「アプリケーション開発者」，一般ユーザや開発者を管理する「ユーザ管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，PaaS を利用して開発された業務ソフトウェアやオフィスソフトウェアを利用している。アプリケーション開発者は PaaS により提供されている API を利用して業務ソフトウェアやオフィスソフトウェアを開発している。ユーザ管理者は一般ユーザ及び開発者を管理するための ID を所有し，PaaS 事業者により用意されたユーザ管理インタフェースを利用できる権限をもつている。クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」，サービスの「責任者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発を行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。

責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

表 3　PaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		PaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	ユーザ管理者	運用担当者	開発技術者	責任者
ユーザアプリケーション	操作	●	−	−	−	−	−
	設定	●	−	−	−	−	−
	ログ閲覧	−	−	●	−	−	−
ID管理	操作	−	−	●	−	−	−
	設定	−	−	●	−	−	−
	ログ閲覧	−	−	●	−	−	−
API	操作	−	●	−	−	−	−
	設定	−	●	−	−	−	−
	ログ閲覧	−	●	−	−	−	−
実行環境	操作	−	−	−	●	−	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
OS	操作	−	−	−	●	−	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
ファイアウォール	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
仮想マシン	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
ホストマシン	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−

PaaS 環境はクラウドサービスごとにシステム環境が異なり，統一的なリスクアセスメントを実施することが難しい。ここでは，API が提供されて，ユーザがそれを利用して自らのアプリケーションやシステムを構築するタイプの PaaS を対象に，システム管理におけるリスクの洗い出しを実施した（表 3 参照）。

SaaS 同様にプラットフォームとなる環境についての情報を直接得ることはできず，環境に応じてプラットフォームの変更などを行うことも難しい。

自らが作成したアプリケーションに関してはログを取得して分析するなど，問題解決のための情報は一部入手することができる。しかし，問題がプラットフォームにあると判断できたとしても，それを自らが修正できるわけではないので，サービス管理のすべてを実施できるということにはならない。

表 4　PaaS におけるデータ管理面における管理の可否（例）

対象データ(クラウド上)		PaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	ユーザ管理者	運用担当者	開発技術者	責任者
ユーザアプリケーションデータ	閲覧	●	−	−	−	−	−
	変更	●	−	−	−	−	−
	削除	−	−	●	−	−	−
	暗号化	−	−	●	−	−	−
	分類	●	−	−	−	−	−
ストレージデータ	閲覧	−	●	●	−	−	−
	変更	−	●	●	−	−	−
	削除	−	●	●	−	−	−
	暗号化	−	●	●	−	−	−
	分類	−	●	●	−	−	−
仮想イメージデータ（運用中）	閲覧	−	−	−	●	●	−
	変更	−	−	−	−	●	−
	削除	−	−	−	−	●	−
	暗号化	−	−	−	−	●	−
	分類	−	−	−	−	●	−
仮想イメージデータ（テンプレート）	閲覧	−	−	−	●	●	−
	変更	−	−	−	−	●	−
	削除	−	−	−	−	●	−
	暗号化	−	−	−	−	●	−
	分類	−	−	−	−	●	−
バックアップ	作成	−	−	−	●	●	−
	削除	−	−	−	●	●	−

データ管理においてはストレージデータまでを利用できることを前提に，データ管理におけるリスクの洗い出しを実施した（表 4 参照）。

ストレージデータとは，アプリケーションから利用するデータ領域ではなく，プログラムを保管したり，ログを保管することのできる比較的自由度の高いストレージに保存されたデータを指している。

バックアップの柔軟さについては SaaS よりは自由度が高いといえる。自らがアプリケーションを作成していることから，関連するデータのバックアップなどを実施することは可能な場合が多い。

プログラムのデプロイに関しては，実行環境によって異なるために一概にリスクとして捉えることができないが，本番環境とテスト環境を明確に分けて実施することができないものもあるため，組織の方針に応じて運用によって対応をする。

IaaS 利用時におけるリスク識別の実施例

以下のような組織を想定し，マトリクスを利用したリスクアセスメントを実行した。

利用者側には「一般ユーザ」及び「アプリケーション開発者」，OS などのシステムインフラを管理する「システム管理者」の役割が存在する。一般ユーザは一般ユーザ権限の ID を所有し，IaaS を利用して自社開発された業務ソフトウェアやオフィスソフトウェアを利用している。アプリケーション開発者は IaaS で提供される OS 上で業務ソフトウェアやオフィスソフトウェアを開発している。システム管理者は OS を管理するための特権 ID を所有し，IaaS 事業者により用意されたシステム管理インタフェースを利用できる権限をもつている。さらに，アプリケーション開発者により開発されたサービスの運用を行っている。

クラウド事業者にはサービス提供中のシステムの「運用担当者」，サービスを開発している「開発技術者」，サービスの「責任者」が存在する。運用担当者は運用のための ID を所有し，サービス提供中のシステムの運用管理を行っている。システムの安定的な動作を維持するためのログ管理など，あらかじめ決められた定型のオペレーション業務以外は行わない。開発技術者は提供中のサービスの機能拡張や新サービスの開発を行っており，特権 ID を使用可能であるが日常の運用管理は行っていない。責任者は提供中のサービスの動作やセキュリティに対しての責任を負っているがシステムを操作するための ID は所有していない。

この事例では利用者は IaaS を利用してアプリケーションを自社開発し，自社のユーザ専用にサービス提供を行っている。

表 5　IaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		IaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	システム管理者	運用担当者	開発技術者	責任者
ユーザアプリケーション	操作	●	−	−	−	−	−
	設定	●	−	−	−	−	−
	ログ閲覧	−	−	●	−	−	−
ID管理	操作	−	−	●	−	−	−
	設定	−	−	●	−	−	−
	ログ閲覧	−	−	●	−	−	−
API	操作	−	●	−	−	−	−
	設定	−	●	−	−	−	−
	ログ閲覧	−	●	−	−	−	−
実行環境	操作	−	−	●	−	−	−
	設定	−	−	●	−	−	−
	ログ閲覧	−	−	●	−	−	−
OS	操作	−	−	●	−	−	−
	設定	−	−	●	−	−	−
	ログ閲覧	−	−	●	−	−	−
ファイアウォール	操作	−	−	−	●	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
仮想マシン	操作	−	−	−	●	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−
ホストマシン	操作	−	−	−	−	●	−
	設定	−	−	−	−	●	−
	ログ閲覧	−	−	−	●	●	−

IaaS においては一般的なハウジングサービスレベルでの管理を実施することができる（表 5 参照）。また，サービスに大きな差異が生じるわけではないので，リスクアセスメントについては他の組織が実施した結果が大いに参考になる。

しかし，仮想化におけるマルチテナントなどが実施されている場合には，プラットフォームでの状況について正しく把握することができないことがある。

問題発生時に実施できる対応は多く，適切な管理を実施することで事業継続における問題は少なくなると言える。しかしながら，プラットフォーム全体が攻撃されてしまった場合などは自らが対応することはできない。仮想環境やネットワーク以外のほとんどの管理を行うことができる。

表 6　IaaS におけるデータ管理面における管理の可否（例）

対象データ(クラウド上)		IaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	システム管理者	運用担当者	開発技術者	責任者
ユーザアプリケーションデータ	閲覧	●	−	−	−	−	−
	変更	●	−	−	−	−	−
	削除	−	−	●	−	−	−
	暗号化	−	−	●	−	−	−
	分類	●	−	−	−	−	−
ストレージデータ	閲覧	−	●	●	−	−	−
	変更	−	●	●	−	−	−
	削除	−	●	●	−	−	−
	暗号化	−	●	●	−	−	−
	分類	−	●	●	−	−	−
仮想イメージデータ（テンプレート）	閲覧	−	−	●	−	−	−
	変更	−	−	●	−	−	−
	削除	−	−	●	−	−	−
	暗号化	−	−	●	−	−	−
	分類	−	−	●	−	−	−
仮想イメージデータ（運用中）	閲覧	−	−	−	−	●	−
	変更	−	−	−	−	●	−
	削除	−	−	−	−	●	−
	暗号化	−	−	−	−	●	−
	分類	−	−	−	−	●	−
バックアップ	作成	−	−	●	●	●	−
	削除	−	−	●	●	●	−

データ管理においても OS をインストールしたハードディスクの管理レベルの内容は実施可能であると考えても良い（表 6 参照）。仮想環境で展開されたシステムがイメージデータとして保存されることで，環境のバックアップは実施しやすくなっている。しかし，バックアップ対象が展開されたシステム全体であること，個々のファイルによる差分ではなく，イメージ全体の差分となるために，バックアップは毎回完全バックアップを取得しなければならないという点，ネットワーク上でバックアップをダウンロードしなくてはならない点など，バックアップ容量の大きさが実施を困難とさせている。

技術的な面を差し引けば，IaaS では従来のハウジングサービスを参考に管理策及び実施の手引の選択ができるといえる。

別添 5

電磁保存告示　改正案

クラウドサービスを利用する場合に確保に努めなくてはならない基準

１ ログ

①クラウド利用者は、クラウドサービス上で取得されるクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認すること。②クラウド利用者は、監査ログを取得した場合にあっては、監査ログは安全な場所に保管し、保管方法等に係る運用管理規程を定めること。

③クラウド事業者は、クラウドサービス上で取得するクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを特定し，取得する機能をクラウド利用者に提供すること。

２ アクセス

①クラウド利用者は、クラウドサービスが提供するアクセス制御機能が、個人別のＩＤ、パスワード等の利用者登録、管理及び認証機能及び情報やシステムの機密度を区分に応じたアクセス権限の制御機能を有しているかを確認すること。

②クラウド事業者は、提供するクラウドサービスにおいて、利用者のアクセス制御機能を提供すること。③クラウド利用者は、すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者 ID の登録・削除についての正式な手順に，クラウドサービスの利用を考慮すること

④クラウド利用者は、クラウドサービスにおいて、すべてのクラウドサービスの利用者が、各個人の利用ごとに一意な識別子(利用者 ID)を保有することができるか確認すること。

⑤クラウド事業者は、クラウドサービスにおいて、すべてのクラウドサービス利用者に、各個人の利用ごとに一意な識別子（利用者 ID）を保有することができるようにすること。

⑥クラウド利用者は、ＩＤを付与された関係者以外の者が操作をしないよう周知徹底する等の措置をとること。

３ バックアップ

①クラウド利用者は、自らが利用するクラウドサービスの特性を理解し、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定のバックアップ手順を次の事項を考慮して策定すること。

・クラウドサービスに付帯するバックアップ機能及び復元機能
・利用者自身が追加開発するバックアップ機能及び復元機能
・バックアップデータの暗号化（暗号化の必要性を含む）
・バックアップデータのローカルでの保管及び隔地保管
・バックアップデータの保管期間

②クラウド事業者は、クラウド利用者が行うべきバックアップ取得について明確にするこ

と。
③クラウド事業者は、利用者にバックアップ機能及び復元機能を提供する場合には、利用者が実施する手順を明確にすること。

4　セキュリティ対策等

①クラウド利用者は、クラウドサービスにおいて、クラウド事業者が、悪意のあるコードからクラウド利用者を保護するために実施している次のような事項を確認すること。
・悪意のあるコードの検出，予防及び回復のための管理策
・悪意のあるコード及びその対策・対応について，クラウド利用者に適切に意識させるために実施している管理策とその実行結果
・悪意のあるコードに感染した場合のクラウド事業者における報告手順。
②クラウド事業者は、クラウドサービス内で、悪意のあるコードからクラウドサービスの利用者を保護するために，検出，予防及び回復のための管理策を実施し、また，クラウド利用者に適切に意識させるための手順を実施すること。
③クラウド利用者は、クラウドサービスの利用に際して、ネットワークサービスに関する情報をクラウド事業者に求めること
④クラウド事業者は、物理ネットワークのセキュリティポリシーを考慮した仮想ネットワークのセキュリティポリシーを定めること。また，クラウド事業者は，仮想ネットワークのセキュリティ設定マニュアルを定め，運用担当者に配付すること。

5　スキャナ（これに準ずる画像読取装置を含む。）による読取に係る取扱い

①クラウド利用者は、作業責任者の明確化等スキャナによる読取に係る運用管理規程を定めること。
②クラウド利用者は、スキャナにより読み取り画像情報として電子化した文書に圧縮を施す際、圧縮方式を適切に設定すること。

6　情報システムの運用管理

①クラウド利用者は、クラウドサービスの利用に関する管理責任者を定めること。
②クラウド利用者の管理責任者は、以下の項目の管理規程を明文化して定め、関係者に周知徹底すること。
・事務室及びデータ保管室への入退室管理
・ＩＤ及びパスワードの付与及び廃止の管理
・データ記録媒体の使用、保管、搬出入及び廃棄の管理
③クラウド利用者は、ソフトウェアの正常作動を確認した上でクラウド上での運用を開始すること。

7　クラウドシステムの監査

①クラウド利用者は，クラウドサービスの監査について方針を定めること②クラウド事業者は、クラウドサービスの監査について方針を定め、監査を定期的に実施すること。
③クラウド利用者は、クラウドサービスにおいて、クラウド事業者によって、第三者が提供

するサービス、報告及び記録が、常に監視され、レビューされていることを確認すること

④クラウド事業者は，提供しているクラウドサービスについて，クラウド利用者に対して次のような情報提供を必要に応じて行うこと。

・第三者が提供するサービス、報告及び記録を、常に監視し、レビューしていることの開示

・ 第三者が提供するサービス、報告及び記録を、常に監視し、レビューした記録の明示

・第三者が提供するサービスを監査していることの開示

・第三者が提供するサービスを監査した結果をまとめた報告書などの提示

平成十七年経済産業省令第三十二号
経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則

民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成十六年法律第百四十九号）第三条第一項、第四条第一項及び第三項、第五条第一項並びに第六条第一項並びに民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行令（平成十七年政令第八号）第二条第一項の規定に基づき、経済産業省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則を次のように定める。

（趣旨）

第一条　民間事業者等が、経済産業省の所管する法令に係る保存等を、電磁的記録を使用して行う場合については、他の法律及び法律に基づく命令（告示を含む。）に特別の定めのある場合を除くほか、この省令の定めるところによる。

（定義）

第二条　この省令において使用する用語は、特別の定めのある場合を除くほか、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（以下「法」という。）において使用する用語の例による。

（法第三条第一項の主務省令で定める保存）

第三条　法第三条第一項の主務省令で定める保存は、別表第一の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の保存とする。

（電磁的記録による保存）

第四条　民間事業者等が、法第三条第一項の規定に基づき、別表第一の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の保存に代えて当該書面に係る電磁的記録の保存を行う場合は、次に掲げる方法のいずれかにより行わなければならない。

一　作成された電磁的記録を民間事業者等の使用に係る電子計算機に備えられたファイル又は磁気ディスク、シー・ディー・ロムその他これらに準ずる方法により一定の事項を確実に記録しておくことができる物（以下「磁気ディスク等」という。）をもって調製するファイルにより保存する方法

二　書面に記載されている事項をスキャナ（これに準ずる画像読取装置を含む。）により読み取ってできた電磁的記録を民間事業者等の使用に係る電子計算機に備えられたファイル又は磁気ディスク等をもって調製するファイルにより保存する方法

２　民間事業者等が、前項の規定に基づく電磁的記録の保存を行う場合は、必要に応じ電磁的記録に記録された事項を出力することにより、直ちに整然とした形式及び明瞭な状態で民間事業者等の使用に係る電子計算機その他の機器に表示及び書面を作成できなければならない。

３　別表第一の上欄に掲げる法令の同表の下欄に掲げる規定に基づき、同一内容の書面を二以上の事務所等（書面又は電磁的記録の保存が義務付けられている場所をいう。以下同じ。）に保存をしなければならないとされている民間事業者等が、第一項の規定に基づき、当該二以上の事務所等のうち、一の事務所等に当該書面に係る電磁的記録の保存を行うとともに、当該電磁的記録に記録されている事項を他の事務所等に備え付けた電子計算機の映像面に表示及び書面を作成できる措置を講じた場合は、当該他の事務所等に当該書面の保存が行われたものとみなす。

４　民間事業者等が、第一項の規定に基づく電磁的記録の保存を行う場合のうち、別表第二の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の保存に代えて当該書面に係る電磁的記録の保存を行う場合は、経済産業大臣が定める基準を確保するよう努めなければならない。

（法第四条第一項の主務省令で定める作成）

第五条　法第四条第一項の主務省令で定める作成は、別表第三の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の作成とする。

（電磁的記録による作成）

第六条　民間事業者等が、法第四条第一項の規定に基づき、別表第三の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の作成に代えて当該書面に係る電磁的記録の作成を行う場合は、民間事業者等の使用に係る電子計算機に備えられたファイルに記録する方法又は磁気ディスク等をもって調製する方法により作成を行わなければならない。

（作成において氏名等を明らかにする措置）

第七条　別表第三に掲げる規定に基づく作成において記載すべき事項とされた記名押印に代わるものであって、法第四条第三項に規定する主務省令で定めるものは、電子署名（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第一項に規定する電子署名をいう。）とする。

（法第五条第一項の主務省令で定める縦覧等）

第八条　法第五条第一項の主務省令で定める縦覧等は、別表第四の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の縦覧等とする。

（電磁的記録による縦覧等）

第九条　民間事業者等が、法第五条第一項の規定に基づき、別表第四の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の縦覧等に代えて当該書面に係る電磁的記録に記録されている事項の縦覧等を行う場合は、当該事項を民間事業者等の事務所に備え置く電子計算機の映像面における表示又は当該事項を記載した書類により行わなければならない。

（法第六条第一項の主務省令で定める交付等）

第十条　法第六条第一項の主務省令で定める交付等は、別表第五の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の交付等とする。

（電磁的記録による交付等）

第十一条　民間事業者等が、法第六条第一項の規定に基づき、別表第五の上欄に掲げる法令の同表の下欄に掲げる規定に基づく書面の交付等に代えて当該書面に係る電磁的記録に記録されている事項の交付等を行う場合は、次に掲げる方法により行わなければならない。

一　電子情報処理組織を使用する方法のうちイ又はロに掲げるもの

イ　民間事業者等の使用に係る電子計算機と交付等の相手方の使用に係る電子計算機とを接続する電気通信回線を通じて送信し、受信者の使用に係る電子計算機に備えられたファイルに記録する方法

ロ　民間事業者等の使用に係る電子計算機に備えられたファイルに記録された書面に記載すべき事項を電気通信回線を通じて交付等の相手方の閲覧に供し、当該相手方の使用に係る電子計算機に備えられたファイルに当該事項を記録する方法（法第六条第一項に規定する方法による交付等を受ける旨の承諾又は受けない旨の申出をする場合にあっては、民間事業者等の使用に係る電子計算機に備えられたファイルにその旨を記録する方法）

二　磁気ディスク等をもって調製するファイルに書面に記載すべき事項を記録したものを交付する方法

２　前項各号に掲げる方法は、交付等の相手方がファイルへの記録を出力することによる書面を作成することができるものでなければならない。

（電磁的方法による承諾）

第十二条　民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行令第二条第一項の規定により示すべき方法の種類及び内容は、次に掲げる事項とする。

一　前条第一項各号に掲げる方法のうち民間事業者等が使用するもの

二　ファイルへの記録の方式

附　則

（施行期日）

第一条　この省令は、平成十七年四月一日から施行する。

（罰則に関する経過措置）

第二条　この省令の施行前にした行為に対する罰則の適用については、なお従前の例による。

附　則　（平成一七年五月一八日経済産業省令第六一号）

この省令は、海洋汚染及び海上災害の防止に関する法律等の一部を改正する法律の施行の日（平成十七年五月十九日）から施行する。

附　則　（平成一七年八月二四日経済産業省令第八二号）　抄

（施行期日）

第一条　この省令は、法の施行の日（平成十七年十月一日）から施行する。

附　則　（平成一八年四月二八日経済産業省令第六三号）　抄

（施行期日）

第一条　この省令は、会社法の施行の日（平成十八年五月一日）から施行する。

附　則　（平成一九年一二月二五日経済産業省令第七七号）　抄

（施行期日）

第一条　この省令は、特定放射性廃棄物の最終処分に関する法律等の一部を改正する法律の施行の日（平成二十年四月一日）より施行する。

附　則　（平成二〇年三月二八日経済産業省令第二四号）　抄

この省令は、平成二十年四月一日から施行する。

附　則　（平成二一年六月二六日経済産業省令第三七号）　抄

（施行期日）

第一条　この省令は、特定商取引に関する法律及び割賦販売法の一部を改正する法律（以下「改正法」という。）の施行の日から施行する。

附　則　（平成二一年七月二八日経済産業省令第四二号）　抄

第一条　この省令は、経済連携協定に基づく特定原産地証明書の発給等に関する法律の一部を改正する法律の施行の日から施行する。

附　則　（平成二一年八月二八日経済産業省令第五〇号）

この省令は、消費者庁及び消費者委員会設置法（平成二十一年法律第四十八号）の施行の日（平成二十一年九月一日）から施行する。

附　則　（平成二二年六月二四日経済産業省令第三八号）　抄

（施行期日）

第一条　この省令は、法の施行の日から施行する。

附　則　（平成二四年九月一四日経済産業省令第六八号）

この省令は、原子力規制委員会設置法の施行の日（平成二十四年九月十九日）から施行する。

附　則　（平成二七年三月四日経済産業省令第九号）　抄

（施行期日）

第一条　この省令は、電気事業法の一部を改正する法律（以下「改正法」という。）の施行の日（平成二十七年四月一日）から施行する。

附　則　（平成二八年九月三〇日経済産業省令第九二号）　抄

（施行期日）

第一条　この省令は、原子力発電における使用済燃料の再処理等のための積立金の積立て及び管理に関する法律の一部を改正する法律（以下「改正法」という。）の施行の日（平成二十八年十月一日）から施行する。

附　則　（平成二九年三月二八日経済産業省令第一五号）　抄

（施行期日）

第一条　この省令は、電気事業法等の一部を改正する等の法律（以下「改正法」という。）附則第一条第五号に掲げる規定の施行の日（平成二十九年四月一日）から施行する。

別表第一（第三条関係）

法令名	規定
火薬類取締法（昭和二十五年法律第百四十九号）	第四十一条第一項及び第四十五条の三の九第二項（同条第三項において準用する場合を含む。）
高圧ガス保安法（昭和二十六年法律第二百四号）	第三十九条の十第二項（同条第三項において準用する場合を含む。）及び第六十条第一項
経済産業大臣の所管に属する公益法人の設立及び監督に関する規則（昭和二十六年通商産業省令第五十五号）	第七条
石油及び可燃性天然ガス資源開発法施行規則（昭和二十七年通商産業省令第四十四号）	第十七条の五
商工会議所法（昭和二十八年法律第百四十三号）	第十一条第一項及び第二項、第三十八条第一項（第八十条において準用する場合を含む。）並びに第三十九条第一項（第八十条において準用する場合を含む。）
ガス事業法（昭和二十九年法律第五十一号）	第百三十一条第一項（第百五十三条第二項及び第百五十五条第二項において準用する場合を含む。）
輸出入取引法施行令（昭和三十年政令第二百四十四号）	第七条第三項
商工会法（昭和三十五年法律第八十九号）	第三十七条第一項（第五十八条第三項において準用する場合を含む。）、第三十八条第一項並びに第五十七条第一項及び第五項

割賦販売法（昭和三十六年法律第百五十九号）	第十九条の二（第三十五条の三の六十二において準用する場合を含む。）
電気用品安全法（昭和三十六年法律第二百三十四号）	第三十七条第一項（第四十二条の三第二項において準用する場合を含む。）
電気事業法（昭和三十九年法律第百七十号）	第七十五条第一項（第九十六条において準用する場合を含む。）
液化石油ガスの保安の確保及び取引の適正化に関する法律（昭和四十二年法律第百四十九号）	第五十八条の二第一項（第六十三条第二項において準用する場合を含む。）及び第八十一条第一項
熱供給事業法施行規則（昭和四十七年通商産業省令第百四十三号）	第二十六条第二項
消費生活用製品安全法（昭和四十八年法律第三十一号）	第二十三条の二第一項（第二十九条第二項において準用する場合を含む。）
揮発油等の品質の確保等に関する法律（昭和五十一年法律第八十八号）	第十七条の十一第二項及び第十七条の十九第一項
エネルギー管理士の試験及び免状の交付に関する規則（昭和五十九年通商産業省令第十五号）	第二十条第一項
経済産業大臣の所管に属する公益信託の引受けの許可及び監督に関する規則（昭和六十年通商産業省令第十一号）	第四条
半導体集積回路の回路配置に関する法律（昭和六十年法律第四十三号）	第三十四条の二第一項及び第四十二条第一項

投資事業有限責任組合契約に関する法律（平成十年法律第九十号）	第八条第一項及び第二項
弁理士法（平成十二年法律第四十九号）	第五十五条第二項において準用する商法（明治三十二年法律第四十八号）第三十六条
特定放射性廃棄物の最終処分に関する法律（平成十二年法律第百十七号）	第六十五条第三項
経済連携協定に基づく特定原産地証明書の発給等に関する法律（平成十六年法律第百四十三号）	第七条第一項及び第二項並びに第七条の十第一項及び第二項
経済連携協定に基づく特定原産地証明書の発給等に関する法律施行規則（平成十七年経済産業省令第九号）	第十二条第一項及び第三項並びに第二十二条第一項及び第三項
クラスター弾等の製造の禁止及び所持の規制等に関する法律（平成二十一年法律第八十五号）	第十五条

別表第二（第四条第四項関係）

法令名	規定
高圧ガス保安法	第三十九条の十第二項（同条第三項において準用する場合を含む。）及び第六十条第一項
割賦販売法	第十九の二条（第三十五条の三の六十二において準用する場合を含む。）
液化石油ガスの保安の確保及び取引の適正化に関する法律	第八十一条第一項

熱供給事業法施行規則	第二十六条第二項
半導体集積回路の回路配置に関する法律	第四十二条第一項
クラスター弾等の製造の禁止及び所持の規制等に関する法律	第十五条

別表第三（第五条関係）

法令名	規定
火薬類取締法	第四十一条第一項及び第四十五条の三の九第二項（同条第三項において準用する場合を含む。）
高圧ガス保安法	第三十九条の十第二項（同条第三項において準用する場合を含む。）及び第六十条第一項
商工会議所法	第十条第一項及び第五項、第二十五条、第六十条の三第一項、第六十条の五第一項並びに第六十八条
商工会法	第二十八条、第五十二条の三第一項、第五十二条の五第一項、第五十五条の十六及び第五十七条第六項
割賦販売法	第十九条の二（第三十五条の三の六十二において準用する場合を含む。）
商店街振興組合法	第六十六条第一項及び第七十四条第一項
液化石油ガスの保安の確保及び取引の適正化に関する法律	第八十一条第一項
熱供給事業法施行規則	第二十六条第一項

半導体集積回路の回路配置に関する法律	第四十二条第一項
投資事業有限責任組合契約に関する法律	第三条第二項及び第八条第一項
弁理士法	第五十五条第二項において準用する商法第三十二条及び第三十三条
特定放射性廃棄物の最終処分に関する法律	第六十五条第一項及び第二項

別表第四（第八条関係）

法令名	規定
商工会議所法	第三十八条第二項（第八十条において準用する場合を含む。）及び第三十九条第三項（第八十条において準用する場合を含む。）
ガス事業法	第百三十一条第二項（第百五十三条第二項及び第百五十五条第二項において準用する場合を含む。）
輸出入取引法施行令	第七条第三項
商工会法	第三十七条第二項（第五十八条第三項において準用する場合を含む。）、第三十八条第三項並びに第五十七条第三項及び第五項
電気用品安全法	第三十七条第二項（第四十二条の三第二項において準用する場合を含む。）
電気事業法	第七十五条第二項（第九十六条において準用する場合を含む。）
液化石油ガスの保安の確保及び取引の適正化に関する法律	第五十八条の二第二項（第六十三条第二項において準用する場合を含む。）

消費生活用製品安全法	第二十三条の二第二項（第二十九条第二項において準用する場合を含む。）
揮発油等の品質の確保等に関する法律	第十七条の十九第二項
エネルギー管理士の試験及び免状の交付に関する規則	第二十条第二項
半導体集積回路の回路配置に関する法律	第三十四条の二第二項及び第四十八条第一項
投資事業有限責任組合契約に関する法律	第八条第三項
特定放射性廃棄物の最終処分に関する法律施行規則	第八条第一項（第十三条第二項及び第十四条第二項において準用する場合を含む。）

別表第五（第十条関係）

法令名	規定
商工会議所法	第三十九条第一項及び第二項（第八十条において準用する場合を含む。）
ガス事業法	第百三十一条第二項（第百五十三条第二項及び第百五十五条第二項において準用する場合を含む。）
商工会法	第三十八条第一項及び第二項並びに第五十七条第一項及び第二項
電気用品安全法	第三十七条第二項（第四十二条の三第二項において準用する場合を含む。）
商店街振興組合法	第五十五条第三項

電気事業法	第七十五条第二項（第九十六条において準用する場合を含む。）
液化石油ガスの保安の確保及び取引の適正化に関する法律	第五十八条の二第二項（第六十三条第二項において準用する場合を含む。）
消費生活用製品安全法	第二十三条の二第二項（第二十九条第二項において準用する場合を含む。）
揮発油等の品質の確保等に関する法律	第十七条の十九第二項
エネルギー管理士の試験及び免状の交付に関する規則	第二十条第二項
半導体集積回路の回路配置に関する法律	第三十四条の二第二項及び第四十八条第一項

本日意見交換させていただきたい事項

別添７

- 高圧ガス保安法における新たな認定制度の円滑な運用を確保するため、詳細な制度設計を産業構造審議会高圧ガス小委員会において議論しております。
- 特に、コンビナートが多く立地する都道府県・政令市の皆様との意見交換を通じ、行政の目線で、資料全体について御意見やお気付きの点があれば、ご指摘いただきたいと考えております。
- その際、特に下記の項目については、皆様の事務とも密接に関係すると考えており、積極的に御意見いただきたいと考えております。

1. 新たな認定制度の特例（資料①5.全般）
2. 設備変更等の特例措置（資料②、資料③）
   - ✓ 事後届出案件に係る都道府県・政令市における取り扱い（審査の有無等）
   - ✓ 事後届出時の添付書類の取り扱い（特に許可から事後届出となる手続について、添付書類の簡素化を検討する点）
   - ✓ 解釈を国から通達・ガイドライン・QA等の形式で示した場合における、都道府県・政令市における取り扱い（遵守頂く場合に、何か懸念があるか。）
3. 現地調査への同席、審査会審査へのオブザーバー参加（資料①6-1、6-4）

経済産業省

別添８

都道府県・政令市との意見交換用　資料①

高圧ガス保安法における
新たな認定制度の詳細設計について

（第23・24回 産業構造審議会 保安・消費生活用製品安全分科会
高圧ガス小委員会 資料抜粋）

2023年3月

経済産業省産業保安グループ

高圧ガス保安室

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の特例

６．新たな認定制度の審査体制

７．新たな認定制度の認定の更新期間

８．A認定事業者向けの特例措置

1-1. 高圧ガス保安法等の一部を改正する法律（※）の概要

※高圧ガス保安法、ガス事業法、電気事業法、情報処理の促進に関する法律。令和４年６月22日に公布。

令和４年12月
経済産業省
産業保安グループ

背景

✓ 近年、産業保安分野において、**革新的なテクノロジーの進展**、**保安人材の不足**、**電力の供給構造の変化**、**災害の激甚化・頻発化**、**気候変動問題への対応の要請**など、様々な環境変化が生じており、これらを踏まえた**保安規制の見直し**が必要。

法律の概要

✓ （１）スマート保安※の促進、（２）新たな保安上のリスク分野への対応／災害対策・レジリエンスの強化、（３）カーボンニュートラル実現に向けた保安規制の整備の３つを柱に、**高圧ガス保安法**、**ガス事業法**、**電気事業法**等の改正を行う。

※ スマート保安：産業保安分野におけるIoT、ビッグデータ・ＡＩ、ドローン等の活用を通じた安全性と効率性の向上。「人の力・技術」との連携・融合。

（１）スマート保安の促進

✓ **「認定高度保安実施事業者制度」の創設【高圧・ガス・電力】**

「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」を厳格に審査・認定し、安全の確保を前提に、その保安力に応じ、手続や検査の在り方を見直す。

- 許可・事前届出を**事後届出・記録保存へ**
- **国等と事業者双方が行う検査を事業者による検査のみに**
- 常時監視・遠隔監視の普及を踏まえ、**検査時期や保安人員の配置を柔軟化**　等

⇨ **テクノロジーの活用促進により、保安レベルの向上と人材不足への対処**



ドローン・IoTによる点検



ビッグデータ・AIによる異常予兆検知・運転最適化

（２）新たな保安上のリスク分野への対応／災害対策・レジリエンスの強化

✓ **太陽光・風力発電設備の保安規制の見直し【電力】**

小規模な太陽光・風力発電設備※を、「小規模事業用電気工作物」と位置付け、基礎情報の届出や使用前の自己確認等の対象とする。

※出力が10kW以上50kW未満の太陽光・20kW未満の風力発電設備

- **設備の設置者の基礎情報の届出義務**（設備の種類、設置場所及び管理者等）
- **技術基準維持義務**、**使用前自己確認**（事業者が設備の安全性を事前に確認）等

＜太陽光パネルの崩落＞



＜風車の羽根の脱落＞



令和3年4月～12月末までに報告された小出力発電設備の事故件数は**158件**。

✓ **ガス事業者間の災害時の連携強化【ガス】**

災害時におけるガス事業者間の連携計画の事前策定を義務付け。

※電気事業法における災害時連携計画と同様の仕組みを導入。

（３）カーボンニュートラル実現に向けた保安規制の整備

✓ **燃料電池自動車の規制の一元化【高圧】**

高圧ガス保安法と道路運送車両法の両法が適用される燃料電池自動車等について規制を一元化（高圧ガス保安法から適用除外）。

✓ **「登録適合性確認機関」による確認制度の創設【電力】**

今後導入が進む風力発電設備について、安全かつ迅速な審査を行うため、工事計画届出の審査について、専門機関（「登録適合性確認機関」）が技術基準の適合性を確認する仕組みとする。



1-2. スマート保安を進めるための制度的環境整備のあり方 （“保安のテクノロジー化／デジタライゼーション”を進めるために）

出典:産構審保安・消費生活用製品安全分科会報告書（令和3年12月） の概要　P.4

テクノロジーの革新的進展
（IoT、BD・AI、ドローン等）

深刻な保安人材の枯渇
熟練の保安人材の不足
若年層の雇用困難化

保安体制の成熟化した産業分野・事業者

画一的・詳細な個別規制
膨大な届出・許可等の手続
高圧ガス：24万件／年
電力：22万件／年
都市ガス：1.4万件／年

保安レベルの持続的向上（保安イノベーション）と保安人材の枯渇の問題への対処のため、「スマート保安」を強力に推し進めるための制度的環境整備が必要である。

保安体制の成熟化した従来的な産業保安分野においては、自立的に高度な保安を確保できる事業者に対して、保安レベルに見合った合理的な規制のあり方を検討すべきである。

限りある行政リソースを新たなリスク分野に展開する必要

テクノロジーを前提に高度な保安を実現するためのメリハリある規制体系

保安レベルを下げることなく、むしろ、テクノロジーの活用により保安レベルを持続的に向上させるため、**「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」**については、行政の適切な監査・監督の下に、画一的な個別・事前規制によらず、**事業者の保安力に応じた規制体系へ移行**することとし、**手続・検査のあり方**をこれに見合った形に**見直す**措置を講じる（テクノロジーの活用を抜本的に促進しつつ、保安能力に見合う形で規制を適正化するスキーム（認定制度））。これにより、事業者の保安活動をテクノロジーを活用しつつ自己リスク管理がなされた高度な領域に強力に押し上げていくことが必要である。

電力　都市ガス　高圧ガス

前提１（安全の確保とメリハリある規制）

○テクノロジーを活用しつつ、「自立的に高度な保安を確保できる事業者」のみが対象

○行政が法令遵守状況等を立入検査により厳格にチェックすることや、重大事故や法令違反などが発生した場合には、その原因・内容・対応等を精査したうえで、機動的に認定の取消を実施することなど、安全確保のための行政による実効的な監督等を行う。

○高圧ガス保安法の現行「認定事業者制度」(高圧ガス保安法第3章の2)については、発展的に解消する。

前提２（事業者に対する環境整備）

テクノロジー化を目指す事業者が技術・人材面での支援を受けられるための環境整備

○産業横断的な技術支援／人材育成支援の取組推進

※関係機関との連携・取組強化　等

1．高圧ガス保安法における新たな認定制度の概要

2．主な審議事項と施行に向けたスケジュール

3．新たな認定制度のコンセプト

4．新たな認定制度の要件

5．新たな認定制度の特例

6．新たな認定制度の審査体制

7．新たな認定制度の認定の更新期間

8．A認定事業者向けの特例措置

2-1. 主な審議事項と施行に向けたスケジュール

- **2023年12月頃の施行に向けて**、**新たな認定制度の詳細設計について、三回にわたる産業構造審議会高圧ガス小委員会における審議へ経て、制度の大枠を固める**予定。
- これを踏まえ、政令・省令等を準備し、**本年６月頃の公布、同12月頃の施行に向けた準備を進めていく**。

主な審議事項

制度総論	制度コンセプト・対応方針
	ターゲット
認定要件	要件の全体像
	要件１：経営トップのコミットメント
	要件２：高度なリスク管理体制
	要件３：テクノロジーの活用
	要件４：サイバーセキュリティなど関連リスクへの対応
認定特例	規制の特例措置
	A認定事業者向け特例措置
認定審査	審査体制
	認定更新期間

施行に向けたスケジュール（想定）

◇2022年
12月15日　高圧ガス小委員会①
主な審議事項：青枠の項目

◇2023年
２月頃　　高圧ガス小委員会②
主な審議項目：点線の項目
小委員会①の審議事項の深堀り

３月頃　　高圧ガス小委員会③
主な審議項目：とりまとめ※
※必要に応じて追加開催

◇2023年６月頃　　政令・省令等の公布

◇2023年12月頃　　施行

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の特例

６．新たな認定制度の審査体制

７．新たな認定制度の認定の更新期間

８．A認定事業者向けの特例措置

3-1. 新たな認定制度のコンセプト（目的）と具体的方針

- **新たな認定制度の導入に当たっては、国全体の高圧ガス分野の保安力向上を図ることを目的に、以下のような具体的方針の下、詳細設計を進めていく。**

新たな認定制度のコンセプト（目的）

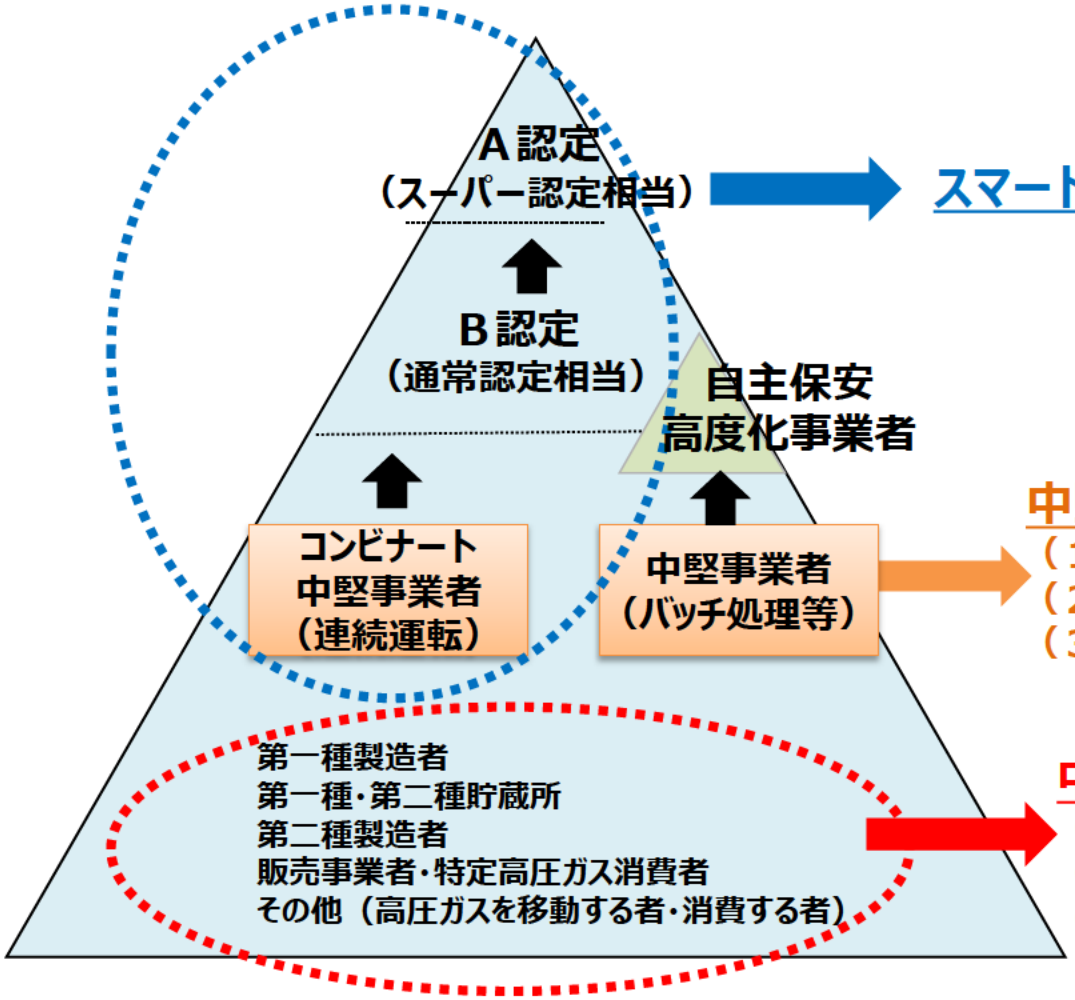
- 新認定制度の保安レベルの持続的向上や保安人材の枯渇問題の解消のため、**テクノロジーを活用したスマート保安を推進**する。
- 厳正な認定審査のもと、**テクノロジーを活用しつつ自立的に高度な保安を確保できると認められた事業者**については、**安全確保を大前提**に、**事業者の保安力に応じた規制体系へ移行**するとともに、**手続・検査の在り方をこれに見合った形に見直す。**これにより、**事業者・規制当局（国・自治体）のリソースを実質的な保安活動に配分することを可能**とする。
- 上記により、**国全体の高圧ガス分野の保安力向上（重大・悪質な法令違反、重大事故の削減）を目指す。**

具体的方針

1. 認定要件に**テクノロジー導入の要件を設け**、**保安分野へのテクノロジー導入を促進**する。
2. **合理的かつ迅速な認定審査へ移行**しつつ、**安全確保を大前提**に、**認定審査を厳正に行う**。
   併せて、**認定事業者に対する特例を拡充**する。
3. **テクノロジーを活用しつつ自立的に高度な保安を確保できる事業者（認定事業者）の増加**を目指す。

3-2. 新たな認定制度の対象事業者のイメージ

- **新たな認定制度の主な対象事業者は、現行認定制度の認定事業者の他、連続運転を行うコンビナートの中堅事業者**を想定。



スマート保安の促進を念頭に置いた新たな認定制度

中堅事業者における保安レベル向上のための対策
（１）スマート保安に向けた新技術導入支援
（２）スマート保安導入のための人材育成支援
（３）自主保安高度化事業者制度（非連続運転）

中小事業者における保安レベル向上のための対策
（１）“中小事業者向けインセンティブ制度”（省令事項）
（２）簡易アプリの開発・普及、許可・手続等のデジタル化
（３）中小事業者のデジタル化支援　等

（参考）現行高圧ガス保安法の認定制度の概要

高
保安力
低

スーパー認定

認定の要件

通常認定の要件に加えて、以下の取組が必要

① **高度なリスクアセスメント**の実施
② **IoT、ビッグデータ**等の**新技術の導入**
③ **高度な教育**の実施
④ **連続運転期間、検査手法の適切な評価体制の整備**
⑤ **第三者機関**によるアドバイスを実施

規制の合理化内容

①**連続運転期間・・・8年以下（事業者が自由に設定した期間）**
　<リスク・ベースドメンテナンス（リスクに応じた柔軟な保全）>
②完成・保安検査・・・**事業者自らが検査**
③検査方法・・・**事業者が自由に設定した方法**
④設置・変更工事・・・許可不要な**軽微変更範囲の更なる拡大**
　（熱交換器など、特定設備の取替え等）
⑤認定期間・・・**7年間**
⑥保安力の見える化・・・**スーパー認定マークを活用**

通常認定

認定の要件

① **リスクアセスメント**の実施。
② **PDCAサイクル**による保安体制の継続的改善
③ **教育訓練**の実施
④ **検査組織**の設置
⑤ **保安・運転・設備管理組織**の設置　等

規制の合理化内容

①**連続運転期間・・・4年間等（大臣に認められた期間）**
②完成・保安検査・・・**事業者自らが検査**
③検査方法・・・**大臣に認められた方法**
④設置・変更工事・・・許可不要な**軽微変更範囲の拡大**
　（特定設備の管台の取替え等）
⑤認定期間・・・**5年間**
⑥保安力の見える化・・・**認定マークを活用**

自主保安高度化事業者

認定の要件

① **リスクアセスメント**の実施
② **PDCAサイクル**による保安体制の継続的改善

規制の合理化内容

①**連続運転期間・・・１年間（1年に1度運転を停止して検査）**
②完成・保安検査・・・**都道府県が検査（保安検査猶予期間（3カ月））**
③検査方法・・・**告示に定められた方法（KHKS）**
④設置・変更工事・・・許可不要な**軽微変更範囲の拡大**
⑤認定期間・・・**5年間**　⑥保安力の見える化・・・**認定マークを活用**

通常の事業所

①**連続運転期間・・・1年間（1年に1度運転を停止して検査）**
②完成・保安検査・・・**都道府県が検査**
③検査方法・・・**告示に定められた方法（KHKS）**
④設置・変更工事・・・**軽微な変更を除き、都道府県の許可**

高
事業者の自由度
低

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の特例

６．新たな認定制度の審査体制

７．新たな認定制度の認定の更新期間

８．A認定事業者向けの特例措置

4-1. 新たな認定制度の要件（総論）

- 新たな認定制度の要件（改正高圧法第39条の14第1項）は、スマート保安の促進の観点から、サイバー対策を含む**４つの要件で構成**する。**これまでの審議会での整理を基本とするものの、追加・拡充する要件については、審議を通じ具体化**していく必要。
- また、安全確保・事業者の保安能力の適正な判断を前提に、**認定基準の大括り化、簡素化、明確化**についても、併せて検討する。

出典:産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.８

（※）下記の表における赤字の下線部及び赤枠は、新たな制度的措置の認定基準において、現行の認定基準から拡充するものを示す。

	A 認 定	B 認 定
①経営トップのコミットメント	現行スーパー認定事業者制度の要件に加え、 コンプライアンス体制の整備（注1）、コーポレート・ガバナンスの確保	
②高度なリスク管理体制	現行スーパー認定事業者相当	現行通常認定事業者相当
③テクノロジーの活用	現行スーパー認定事業者制度における仕組み（注2）を基本とする ※認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用。	
④サイバーセキュリティなど関連リスクへの対応	各業界におけるサイバーセキュリティガイドライン（注3）に沿った内容とする	

（注1）高圧ガス保安法についての**法適合性確認能力**（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。
（注2）特定認定事業者及び自主保安高度化事業者の認定について (20201218保局第1号) における認定の基準 「二 先進的な技術を適切に活用していること」の項目を参照。
（注3）「重要インフラにおける情報セキュリティ確保に係る安全基準等作成指針」（内閣官房内閣サイバーセキュリティセンター）を参考に業界団体が定める「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」、「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」。

4-2. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

論点

- ✓ 認定事業者による法令違反の発覚等を踏まえ、**会社全体の運営の健全性を確認することが必要**。
- ✓ **規制の特例の見直しにより**、事業者の自主保安に委ねられる領域が拡大※１することを踏まえ、事業者が**法適合性確認能力※２を有することを確認**することが必要。

※１　新たな認定制度の認定事業者においては、その保安確保能力を踏まえ、ガス種の変更又は製造能力が一定以上変更される場合など重要な変更については許可制を維持しながらも、軽微変更についてはその対象範囲を拡大した上で記録保存義務とされた。
※２　設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力。

産構審　分科会報告書における記載

現行のスーパー認定事業者制度の要件（経営トップによる保安の方針の明示等）に加え、**コンプライアンス体制の整備、コーポレート・ガバナンスの確保といった要件を拡充**し、特にコンプライアンス体制の整備については、**高圧ガス保安法についての法適合性確認能力（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していること等を確認**する。

※「コンプライアンス・ガバナンス」の観点からは、運営側の責任者の明確化、社内監視体制の整備とその責任者の明確化が重要である。その際、例えば、上場企業の場合には、上場審査基準の活用や、上場企業でない場合には、公益通報者保護法に基づく内部通報制度の整備と遵守といったようなところも考慮すべき」との意見があった。当該意見を踏まえつつ、「法適合性確認能力」の具体的審査項目については、金融関連法制やインフラ関係の業法等、高いコンプライアンスが求められる、他法の例も参考に策定（法令順守に関する組織や体制、第三者や相互の監視体制、内部通報制度の完備方針・マニュアルの整備、社内教育体制等）する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- **コンプライアンス体制の整備、コーポレート・ガバナンスの確保の要件は、**現行の認定制度の要件に経営トップによる保安の方針の明示等が含まれていることも踏まえ、**以下の四つの視点で検討する**。

1. **取締役等に保安についての責任とイニシアティブを持たせ、保安活動をトップダウンで推進できる体制の整備**が必要。
2. また、**取締役等が、保安に対する責務を適切に果たしていることを監督する体制の整備**が必要。
3. 行政手続漏れ等の法令違反を防止するためには、**事業所内で複層的なチェック体制を構築すること**が不可欠。
4. また、法令違反時の組織的隠蔽等を防止する観点から、**法令違反発生時の通報手順が明確に定められていること**が必要。

- 上記に加え、**認定取消の処分基準において、重大・悪質な法令違反が発覚した場合を明文化**することによって、法令遵守体制の整備を促す。

4-3. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

- 検討の視点を踏まえ、新たな認定制度における経営トップのコミットメントの要件は、現行の認定制度の要件※に下記の要素を追加することとしてはどうか。

※現行の認定制度の要件においては、法人の代表者が保安の基本方針を策定していること、法人の代表者が認定要件の適合性に対して責任を有していること等が規定されている。

検討の視点を踏まえた認定要件（案）

コーポレート・ガバナンスの要件

１　取締役等※を保安活動の責任者としていること

保安に係る意思決定を迅速に行い、トップダウンで社内横断的に適切な保安活動の実行を可能とする観点から、取締役等を保安活動の責任者としていること。　※代表取締役や他の職務との兼務も可能とする。指名委員会等設置会社における執行役も含むこととする。

２　監査役等※が保安体制の整備等について監査を行っていること

例えば、保安管理部門等から監査役等に保安活動の状況が定期的に報告されているほか、監査役等が事業所を定期的に訪問して改善意見を示しているなど、監査役等が保安活動に責任を有する取締役等の職務執行や事業所の保安活動全般に対して有効な監査を行っていること。　※指名委員会等設置会社・監査等委員会設置会社においては、監査（等）委員会等を想定。

コンプライアンスの要件

３　複層チェック体制の構築

設備の変更工事等の際に、行政手続の要否等を保安管理部門を含む複数の部門が確認する体制が構築されているなど、高圧法の法令事項を遵守するための複層的なチェック体制が構築されていること。

４　法令違反発生時の通報手順の策定

高圧法の法令違反が発覚した際の本社や関係行政庁への通報手順が適切に定められていること。

（参考）現行の認定制度における本社の体制の要件

（コンビナート等保安規則　別表第5（第41条第1項関係））

一　本社の体制について

イ　保安に係る基本姿勢

一　法人の代表者によつて、保安の確保に関する理念、基本方針等の諸施策が明確に定められ、かつ、文書化されていること。また、これらの諸施策が各事業所等の全ての就業者に理解され、実施され、かつ、維持されていること。

二　法人の代表者が、本社及び事業所をこの表に定める基準に適合させる責任を有することが明確に定められ、かつ、文書化されていること。

ロ　保安管理

一　役員を長とする保安対策本部等が設置されており、保安管理の基本方針の決定、各事業所ごとの保安管理実績の検討等の実施について明確に定められ、文書化され、かつ、適切に実施されていること。

二　保安管理部門が設置されており、生産計画、設備管理計画等に当該部門の意見が十分に反映されることが明確に定められ、文書化され、かつ、意見が十分反映されていること。

三　保安管理部門の長は、申請その他認定に関する業務を統括し、認定業務の責任者となることが明確に定められ、かつ、文書化されていること。

四　本社が、一年に一回以上事業所及び検査管理（認定完成検査の実施状況の不備及び検査結果がこの規則の基準に適合していない場合の改善勧告をいう。以下この表において同じ。）を行う組織に対し、この表に定める基準に適合しているかどうかについて監査を実施することが明確に定められ、文書化され、かつ、適切に実施されていること。

五　本社又は事業所における法令違反等に関する報告の受付等の業務を行う組織が、独立して設置されており、かつ、適切に運営されていること。

4-4. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

- **法令違反を防止するために企業がとりうる方策は多種多様**であるところ、自主保安を促進する観点からは、**事業者自身が最適だと考える方法によって、法令遵守体制の整備を進めることが重要**。
- そこで、事業者に法令遵守体制の整備を促す観点から、認定取消の処分基準において、**重大・悪質な法令違反**が発覚した場合を明文化することとしてはどうか。

現行の認定取消要件に関する記載

高圧ガス保安法

（認定の取消し等）

第三十九条の十二　経済産業大臣は、認定完成検査実施者又は認定保安検査実施者が次の各号のいずれかに該当するときは、第二十条第三項第二号又は第三十五条第一項第二号の認定を取り消すことができる。

一～五　（略）

六　**第三十九条の三第一項各号又は第三十九条の五第一項各号のいずれかに該当していないと認められるとき。**

七～十　（略）

通達（「認定完成検査実施者及び認定保安検査実施者の認定について」）

８．認定の取消

（１）法第３９条の１２第１項第１号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、認定を受けている製造事業所又は第一種貯蔵所において、次のいずれかの要件に該当する高圧ガスによる災害が発生した場合とする。

① 負傷の程度に応じて次の表 a から d までに定める被害以上の人的被害が発生したとき。

図（略）

② 直接損害額が２億円以上発生したとき。

③ 次のいずれかに該当し、かつ、社会的影響が大きいと認められたとき。

イ 多数又は長時間の避難者が発生する等住民の生活に多大な影響を及ぼしたとき。

ロ 認定を受けている製造事業所又は第一種貯蔵所外で人的被害が発生したとき。

ハ 認定を受けている製造事業所又は第一種貯蔵所外で物的被害が発生したとき。

ニ 著しい環境破壊を及ぼしたとき。

④⑤　（略）

（２）　（略）

（３）法第３９条の１２第１項第６号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、次のいずれかに該当することとなった場合とする。

① 認定保安検査に係る検査脱漏、事業所の保安体制に不備が認められ、かつ、それが（１）の①から③まで（③イを除く。）に掲げるいずれかの災害を惹起するおそれが相当程度あったと認められたとき。ただし、本社による監査等により自ら確認し、速やかに報告があったものについては、この限りではない。

② **緊急時即時通報連絡が行われなかったとき等保安体制に重大な不備が認められたとき。**

（４）　（略）

4-5.新たな認定制度の要件（認定要件２：高度なリスク管理体制の要件）

論点

- ✓ 認定対象事業者の保安レベルを確保するべく、**認定の水準は、現行の認定制度より下げるべきではない**。また、**現行の認定制度の下における認定基準は、既に相当程度の保安レベルを確保できる水準であり、現行の認定基準をベースとすることが妥当。**
- ✓ **現行の通常認定制度**は、**認定要件にリスクに対する低減策の実施を求めていない**。

産構審　分科会報告書における記載

保安に関する専門部署の設置等、現行の認定事業者制度で要求されるリスク管理レベルは維持しつつ、事業者のリスク管理体制のレベルに応じ、**A認定については、現行のスーパー認定事業者相当のリスク管理体制**とし、**B認定については、現行通常認定事業者相当のリスク管理体制**を求める※。

※「設備が老朽化すると事故や支障も出やすいことから、高度なリスク管理体制の要件の中で、老朽化した施設についての管理のあり方についても考慮すべき」との意見があった。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- **A認定については、現行のスーパー認定事業者相当のリスク管理体制を、B認定については、現行通常認定事業者相当のリスク管理体制**を求める。
- 特定されたリスクに対する低減策の実施は、保安確保上不可欠であり、B認定に対しても求めることを検討する。

検討の視点を踏まえた認定要件（案）

- **A認定事業者**に対しては、**現行のスーパー認定事業者相当の要件**を課してはどうか。
- **B認定事業者**に対しては、**現行の通常認定事業者相当の要件に加え、特定したリスクに対する低減策を実施していること**を要件として課してはどうか。

4-6.新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

論点

- ✓ スマート保安の実現には、**テクノロジーの開発・導入に向けた経営トップのコミットメント**が必要。
- ✓ 導入の対象となりうるテクノロジーには、①**現場作業の効率化につながるもの**（例：ロボット・ドローン等を活用し点検作業を効率化）や、②**意思決定の高度化につながるもの**（例：運転時のプロセスデータから異常を早期に検知し、作業員の判断を補助・代替）等があり、その**目的やレベルは様々**である。
- ✓ テクノロジーの導入によって保安力を向上させるためには、**導入・効果検証・改善のサイクル**を繰り返すことが必要。
- ✓ A認定相当の事業者とB認定相当の事業者には**一定の保安レベルの差異が存在**する。

産構審　分科会報告書における記載

現行のスーパー認定事業者制度における仕組み※を基本とする。その際、認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用する（すなわち、保安に係るテクノロジーのイノベーションを阻害せず、むしろイノベーションを促進する観点から、一定の技術水準を確保しつつも、活用するテクノロジーの種類を明示的に限定することとはしない）。また、**テクノロジーの活用に向けた効果検証や改善等といったテクノロジー活用プロセスも重要**であることから、**現行のスーパー認定事業者制度の基準を踏まえて、これを要件とする**。

※現行のスーパー認定事業者制度においては、IoT等の先進的な技術の導入・効果検証・改善等を行っていること等を要件としており、具体的には、特定認定事業者及び自主保安高度化事業者の認定について(20201218保局第1号) における認定の基準の「二 先進的な技術を適切に活用していること」の項目を参照。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- 現行のスーパー認定事業者制度における仕組みを基本としつつも、これまでのスマート保安の実現に向けた取組等を踏まえ、以下の三つの視点でテクノロジーの活用の要件を検討する。

1. 事業者の保安レベルを考慮し、**導入を求めるテクノロジーのレベルは、A認定とB認定で差異を設ける**。
2. テクノロジー導入後、**導入・効果検証・改善のサイクルを構築**していること。
3. テクノロジー導入に向けた**経営トップの関与**が必要。具体的には、**テクノロジー導入に向けた計画が策定され、必要なリソース（予算・人材）が確保**されていること。

4-7. 新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

- 検討の視点を踏まえ、新たな認定制度におけるテクノロジーの活用の要件は、**現行のスーパー認定制度の認定要件を基本とし、以下のように見直してはどうか**。
- なお、**外部からのモニターの実施**（年１度の経済産業省への報告）については、別途報告を受けている※ことから、**廃止することとしてはどうか。**

※現在スーパー認定事業者に求めている外部モニターの実施（年１度の経済産業省への報告）については、スマート保安官民協議会等で代替できている。また、スーパー認定事業者に期待するトップランナーとしての役割は、良好事例の展開等の他の認定要件で代替可能。

検討の視点を踏まえた認定要件（案）

１　経営トップのコミットメント

保安の確保に資するテクノロジー導入に向けたビジョンが策定され、必要なリソース（予算・人材）が確保されていること。

２　保安の確保に資するテクノロジーを導入していること

A認定は①②のテクノロジーを導入していること、B 認定は①のテクノロジーを導入していること。

①現場作業の効率化につながるテクノロジー

例：異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等

②意思決定の高度化につながるテクノロジー

例：予測する技術、人の意思決定を補助又は代替する技術等

３　保安の確保に資するテクノロジー導入について継続的に改善する仕組みが構築されていること※

保安の確保に資するテクノロジーの導入に当たって、導入計画の策定やトライアル検証を行っていること。また、保安の確保に資するテクノロジーの導入後に効果検証・改善を行っていること。

※効果検証・改善が実施されるまでには一定の期間を要すると考えられるため、初回認定の認定審査時は、一部のテクノロジーについては導入計画の策定のみで足りるとすることなどが考えられる。

4-8. 新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

現行のスーパー認定制度の要件と新たな認定制度の要件との対応関係

スーパー認定制度の要件		新たな認定制度の要件	A認定	B認定
—	新設	①経営トップ※のコミットメント ※テクノロジーに関する投資計画・人材計画等に責任を持つ取締役等を想定。	✓ 保安の確保に資するテクノロジー導入に向けたビジョンの策定と必要なリソース（予算・人材）が確保されている	
① 先進的な技術の導入 ② 導入した①技術の効果検証・改善に向けた取組みの実施 ③ ビッグデータの収集・分析・未来予測・ヒトに気付きを与えミスを防ぐ観点からの技術の検証・導入・導入計画の策定 ④ ②技術について6カ月以上の検証	再編	②保安の確保に資するテクノロジーの導入	✓ 現場作業の効率化につながるテクノロジー（異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等） ✓ 意思決定の高度化につながるテクノロジー（予測する技術、人の意思決定を補助又は代替する技術等） を導入している	✓ 現場作業の効率化につながるテクノロジー（異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等） を導入している
		③継続的に改善する仕組みの構築	✓ 導入計画の策定→トライアル検証→導入→効果検証→改善を行っている※ ※初回認定の認定審査時は、一部のテクノロジーについては導入計画の策定のみで足りるとすることなどが考えられる。	
⑤ 外部からのモニターの実施（年1度の経済産業省への報告）	廃止	–		

4-9. 新たな認定制度の要件（認定要件４：サイバーセキュリティなど関連リスクへの対応）

論点

- ✓**石油・化学等の重要インフラ事業者**※1**は、サイバーセキュリティの確保に努める**とされている（**努力義務**）※2。

※1　重要インフラ事業者には、情報通信、金融、航空、医療、水道、物流、石油、化学、電力、ガス等が指定されている(内閣サイバーセキュリティセンター「重要インフラのサイバーセキュリティに係る行動計画」別紙１より）。
※2　サイバーセキュリティ基本法(平成二十六年法律第百四号)
第六条　重要社会基盤事業者は、（中略）サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める（以下略）。

- ✓本要件は現行の認定制度にはない**新設の要件**。また、現在認定を取得している化学分野の事業者の中には、業界団体が作成した**サイバーセキュリティガイドラインが適用されない事業者も一定数存在**。
- ✓改正高圧法において、**認定要件は「保安の確保のための組織」に着目**することとしている。**内閣サイバーセキュリティセンターの安全指針**※**は、PDCAサイクルに沿った対策**を記載しており、これを踏まえることが必要。

※　内閣サイバーセキュリティセンター「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」

- ✓高圧ガス保安法の法目的を踏まえ、対象は**生産管理システム又はプラント制御システムのサイバーセキュリティ対策**とする必要。

産構審　分科会報告書における記載

サイバーセキュリティなど関連リスクへの対応「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（内閣官房内閣サイバーセキュリティセンター）において、石油・化学分野は重要インフラ分野とされており、この指針を参考に石油・化学分野の業界団体がサイバーセキュリティガイドラインを策定しているため、これに沿った内容とする。すなわち、**「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」**や**「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」に沿った内容**とする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- サイバーセキュリティなど関連リスクへの対応の要件は、**組織や体制に着目**した要件とする。具体的には、**PDCAサイクルが構築されていること**を要件とし、事業者が、**技術の進展等に応じて自主的に**、生産管理システム又はプラント制御システムに対する**サイバー攻撃等のリスクへ対応する体制を維持・改善する仕組みがあることを確認**する。
- 本要件は新設の要件であるため、**初回の認定審査時には一定の配慮**を行う（詳細は次ページ）。

4-10. 新たな認定制度の要件（認定要件４：サイバーセキュリティなど関連リスクへの対応）

- 検討の視点を踏まえ、サイバーセキュリティなど関連リスクへの対応の要件は、以下としてはどうか。また、今後、業界ガイドラインの改訂※等を踏まえて、**必要に応じて見直す**こととしてはどうか。

※ 2022年６月、サイバー基本法第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、「重要インフラのサイバーセキュリティに係る行動計画」（サイバーセキュリティ戦略本部）が策定された。今後、内閣サイバーセキュリティセンターにおいて「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」が策定され、業界別サイバーセキュリティガイドラインについても、業界団体において見直しすることが予定されている。

- また、初回の認定審査時においては、**審査方法等に一定の配慮を講じる**こととしてはどうか。

検討の視点を踏まえた認定要件（案）

1　生産管理システム又はプラント制御システム（以下「対象システム」という。）**のサイバーセキュリティ対策に係る計画の策定及び体制の構築（Plan）**

①対象システムを含むサイバーセキュリティ対策に係る基本方針が明確に定められ、かつ、文書化されていること。

②対象システムのサイバーセキュリティに関するリスクを特定していること。

2　対象システムのサイバーセキュリティ対策の実施（Do）

①対象システムのサイバーセキュリティに関して特定したリスクについて、必要に応じて、対策を講じていること。

3　継続的改善の実施（Check/Act）

①対象システムのサイバーセキュリティ対策を定期的に自己評価していること。

②自己評価の結果等を踏まえ、対象システムのサイバーセキュリティ対策の見直しを行っていること。

※初回の認定審査時における配慮事項

初回の認定審査時には、「１ 生産管理システム又はプラント制御システムのサイバーセキュリティ対策に係る計画の策定及び体制の構築（Plan）」のうち、「①対象システムを含むサイバーセキュリティ対策に係る基本方針が明確に定められ、かつ、文書化されていること」を確認し、その他の要件については、今後の対応予定時期計画を提出しその内容を確認することでも代替可能とする等の配慮を行う。

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の特例

６．新たな認定制度の審査体制

７．新たな認定制度の認定の更新期間

８．A認定事業者向けの特例措置

5-1. 新たな認定制度の特例（総論）

- **新たな認定制度の認定事業者に対しては**、製造施設の位置・設備等の変更の手続や危害予防規程・保安人員に関する手続等について、**事業者の保安力に応じて、届出等の手続の不要化や事業者自身による検査等を柔軟に措置（記録保存義務は維持）**。

製造施設の位置・設備等の変更の許可・届出

- 現行法では、軽微変更を除き、製造施設の位置・設備等の変更（設備変更）には都道府県知事又は政令指定都市の長の許可が必要

- 新たな認定制度の認定事業者においては、その保安確保能力を踏まえ、**ガス種の変更又は製造能力が一定以上変更される場合など重要な変更**については、**許可制を維持**
- **軽微変更**については、その対象範囲を拡大した上で**記録保存義務**とする
- **それら以外の変更**は、事故時・法令違反時に行政が迅速に対応することを可能とするため、**行政による事業者情報の把握の観点から、事後届出**とする

完成検査・保安検査

- 現行の認定事業者制度と同様に**自主検査**を維持
- その際、新たな認定制度では、法適合性確認能力も含め、コンプライアンス体制の整備等の要件を拡充すること等も踏まえ、**事業者が自ら完成検査・保安検査の結果を適正に確認**するものとし、検査記録については都道府県知事への**届出を要しない**こととする
- ただし、行政が立入検査等により確認できるよう、**検査記録を保存**
- 保安検査については、**定期に行うことを基本としつつ**、**CBMや常時監視等**による場合には、**それ以外の時期によることも可能**とし得るよう措置

保安人員（保安係員等）の配置

- 現行法では、「製造のための施設の区分ごとに」保安人員を配置

- 新たな認定制度の認定事業者においては、これを基本としつつも、コンビナート連携の進展や、常時監視・遠隔監視システムの導入などを踏まえ、法律上は「製造のための施設の区分ごとに」とせず、**保安人員の柔軟な配置**を許容し、**必要人員の配置の適正化について検討**

危害予防規程の届出・保安人員（保安係員等）の選解任の届出

- 新たな認定制度における認定事業者は、危害予防規程の作成・変更や、保安人員の選解任については、自立的に管理するものとし、**記録保存**とする

定期自主検査

- 定期自主検査は、保安検査を補完する検査であり、その対象施設は保安検査の対象施設と同様にガス設備が基本／検査項目も重複的
- 自立的に高度な保安管理を行うことができるため、保安検査の実施を前提に、認定事業者には**定期自主検査の規定を適用しない**

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.９より抜粋

5-2. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

論点

- ✓ **ガス種の変更又は製造能力が一定以上変更される場合など、製造施設に与える影響が大きい工事や製造の方法の変更**については、安全性を確保する観点から、許可とすることが妥当。
- ✓ **軽微変更については記録保存とするものの、処理能力の変更を伴うものについては、事故時・法令違反時に行政が迅速に対応することを可能とする観点から、事後届出とすることが妥当。**
- ✓ 誤解を防止し、新制度の円滑な運用を確保する観点から、制度全体について**分かりやすさを確保**する必要。

産構審　分科会報告書における記載

現行法では、認定事業者・非認定事業者を問わず、軽微変更を除き、製造施設の位置・設備等の変更（設備変更）には都道府県知事又は政令指定都市の長の許可を受ける必要がある。**新たな認定制度の認定事業者においては**、その保安確保能力を踏まえ、**ガス種の変更又は製造能力が一定以上変更される場合など重要な変更については許可制を維持**しながらも、**軽微変更についてはその対象範囲を拡大した上で記録保存義務**とする。**それら以外の変更**については、事故時・法令違反時に行政が迅速に対応することを可能とするため、**行政による事業者情報の把握の観点から、事後届出（速やかに／変更後30日以内）**とすることとする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.18）

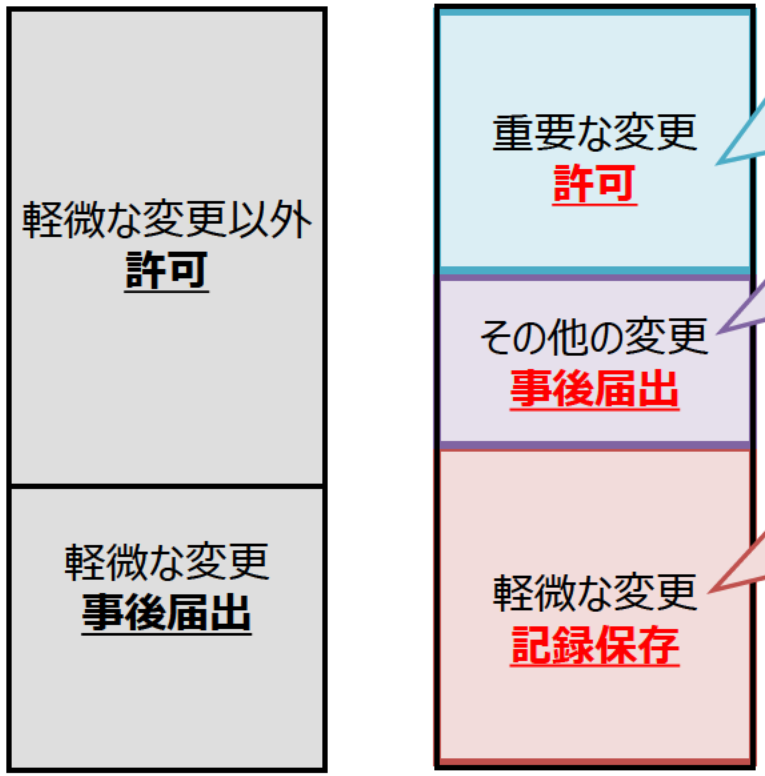
検討の視点

- 製造施設の位置・設備等の変更の許可・届出等の特例の検討に際しては、以下の三つの視点を考慮する。
  - ✓ **工事の規模や製造施設に与える影響の大小**
  - ✓ **行政が事業者情報を把握する必要性**
  - ✓ **制度運用上の分かりやすさ**

5-3. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- 新たな認定制度における製造施設の位置・設備等の変更の許可・届出等は、完成検査との関係（詳細は次ページ）を含め、**新制度の円滑な運用を確保する観点から、以下の分類**としてはどうか。
- その際、**「重要な変更」と「軽微な変更」の内容については、省令等において限定列挙**するとともに、**その他の変更を含め詳細な解釈についても通達等で可能な限り明らかにする**ことで、わかりやすい制度とする。

製造施設の位置・設備等の変更の許可・届出等の分類（案）



重要な変更

【変更の工事】
- ✓ 特定変更工事※に該当する変更の工事

※高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）

【製造の方法の変更・ガス種の変更※】
- ✓ 常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）
- ✓ ガス種の変更※

※ガス種の変更は、製造のための施設等の変更の特例の対象外（改正高圧ガス保安法39条の21第１項参照）。

その他の変更（重要な変更と軽微な変更以外のもの）

【変更の工事の例】
- ✓ 処理能力の変更が一定(20%) 範囲内の変更の工事

【製造の方法の変更の例】
- ✓ 常用圧力・常用温度の変更（設計条件内での変更を伴うもの） 等

軽微な変更

【変更の工事】
- ✓ 現行の軽微変更に該当する変更の工事※（ガス設備の変更の工事等）

※処理能力の変更を伴うものは除く

【製造の方法の変更】
- ✓ 常用圧力・常用温度の変更を伴わない製造の方法の変更

※軽微な変更の工事における通常認定とスーパー認定の差異（コンビ則第14条第１項第７号等）は、新たな認定制度においても踏襲することを予定 。

5-4. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- **製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係は、以下の整理**としてはどうか。
- なお、完成検査の検査記録は、現状届出義務となっているところ、**新たな認定制度においては記録保存義務**となるため、**完成検査終了後、速やかに運転を開始することができる**。

製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係

現行の認定制度

変更の工事			
軽微な変更以外の変更	特定変更工事※1	**許可**	**完成検査必要**（事後届出）
	特定変更工事以外の工事		完成検査不要
軽微な変更※2		**事後届出**	完成検査不要
製造の方法の変更・ガス種の変更			
軽微な変更以外の変更		**許可**	完成検査不要

新たな認定制度

変更の工事			
重要な変更	特定変更工事※1	**許可**	**完成検査必要**（記録保存）
その他の変更	特定変更工事以外の工事	**事後届出**	完成検査不要
軽微な変更※2		**記録保存**	完成検査不要
製造の方法の変更・ガス種の変更※3			
重要な変更	✓ガス種の変更※3 ✓常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）	**許可**	完成検査不要
その他の変更	✓常用圧力・常用温度の変更（設計条件内での変更を伴うもの）	**事後届出**	完成検査不要
軽微な変更	✓常用圧力・常用温度の変更を伴わない製造の方法の変更	**記録保存**	完成検査不要

※1　高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）
※2　軽微な変更の工事の範囲については、今後、必要に応じて見直すことを想定。
※3　ガス種の変更は製造のための施設等の変更の特例の対象外（改正高圧ガス保安法第39条の21第１項参照）。

5-5. 新たな認定制度の特例（保安検査時期の柔軟化、定期自主検査義務の廃止）

保安検査時期の柔軟化

産構審　分科会報告書における記載

「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」については、現行の認定事業者制度と同様に自主検査を維持する。ただし、その際、新たな認定制度では、法適合性確認能力も含め、コンプライアンス体制の整備等の要件を拡充すること等も踏まえ、事業者が自ら完成検査・保安検査の結果を適正に確認するものとし、検査記録については都道府県知事への届出を要しないものとする。ただし、行政が立入検査等により完成検査・保安検査の状況を確認することができるよう、事業者は検査記録を保存するものとする。また、**保安検査については、**現行法上「定期に」行うことと限定されている。現時点では定期に行うことを基本とするものの、今後、CBMや常時監視等の導入が本格化することも想定し、新たな認定制度の認定事業者については、当該「定期に」との法律上の文言を削除する。この場合、**検査の時期については、経済産業省令で定めるものとし、具体的には、現時点では、定期に行うことを基本としつつ、CBMや常時監視等による場合には、それ以外の時期によることも可能とし得るよう措置する。**

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 保安検査は、**定期に行う**こととする。
- ただし、CBMや常時監視等の高度な情報通信技術の活用状況等を踏まえ、**保安の確保上問題がないと経済産業大臣が認める時期に行うことも可能**としてはどうか。

定期自主検査義務の廃止

産構審　分科会報告書における記載

定期自主検査は、第一種製造者等が保有する設備が技術上の基準に適合しているかの確認について、保安検査を補完する観点から規定されている検査である。また、認定対象となる第一種製造者については、定期自主検査の対象施設は保安検査の対象施設と同様にガス設備※1を基本とし、検査項目も重複的なものである※2。これらを踏まえ、新たな認定制度の認定事業者は、自立的に高度な保安管理を行うことができるため、保安検査の実施を前提に、**認定事業者には定期自主検査の規定を適用しない**こととする※3。

※1　ガス設備：高圧ガス製造施設のうち、製造をする高圧ガスのガス（その原料となるガスを含む。）の通る部分。

※2　定期自主検査の対象施設は、ガス設備（コンビ則第38条第2項）とされている。保安検査の対象施設は、告示で定める製造施設以外の製造施設（コンビ則第34条第1項）とされており、「製造施設の位置、構造及び設備並びに製造の方法等に関する技術基準の細目を定める告示」には、保安検査を受ける必要のない製造施設として、①ガス設備以外の製造施設、②ガス設備のうち次に掲げるもの（可燃性ガス及び毒性ガス以外のガス設備等）等が規定されている。

※3　現在、**定期自主検査でのみ検査を行っている項目についても、継続的に検査を行っていくことを担保するため、例えば、更新認定に当たって、継続的な改善事項として考慮**する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.20）

方針（案）

- 定期自主検査でのみ検査を行っている項目について、継続的に検査を行っていることを、**認定審査において確認**※することとしてはどうか。

※「認定完成検査実施者及び認定保安検査実施者の認定に係る事業所の体制の基準を定める告示」第10条第２項第４号ロ(1)の要件充足性を審査する際に確認することを予定。

5-6. 新たな認定制度の特例
（危害予防規程の届出義務・保安人員の選解任の届出義務の廃止、保安人員の配置の柔軟化）

危害予防規程の届出義務・保安人員の選解任の届出義務の廃止

産構審　分科会報告書における記載

新たな認定制度における認定事業者は、**危害予防規程の作成・変更や、保安人員の選解任については、自立的に管理するものとし、都道府県知事等への個別の届出は要しないものとする**。ただし、行政が立入検査等によりその実施状況を確認できるよう、**記録保存義務を課す**ものとする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 危害予防規程の作成・変更や、保安人員の選解任は記録保存とされた。記録保存は、文書による保存方法に加え、**電磁的方法**によることも可能とする。
- 電磁的方法による記録保存は、**クラウド保存による場合も想定して、関連規程※を見直す**こととしてはどうか。

※「電磁的方法による保存等をする場合に確保するよう努めなければならない基準」

保安人員の配置の柔軟化

産構審　分科会報告書における記載

現行法では、「製造のための施設の区分ごとに」保安係員及び保安主任者を配置することになっている。新たな認定制度の認定事業者においては、これを基本としつつも、**コンビナート連携の進展や、常時監視・遠隔監視システムの導入などを踏まえ、法律上は「製造のための施設の区分ごとに」とせず、保安人員を柔軟に配置することを許容**するとともに、**必要人員の配置の適正化について検討**する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 保安人員の配置の方法は、高度な情報通信技術の活用状況等を踏まえて、個別具体の事例ごとに判断することが適切。
- このため、高度な情報通信技術の活用により、適切な監視体制が確保され、また、緊急事態への対応も可能であるなど、**適切な保安管理が行えると経済産業大臣が認める場合**に、**保安人員の柔軟な配置を許容する**こととしてはどうか。

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の特例

６．新たな認定制度の審査体制

７．新たな認定制度の認定の更新期間

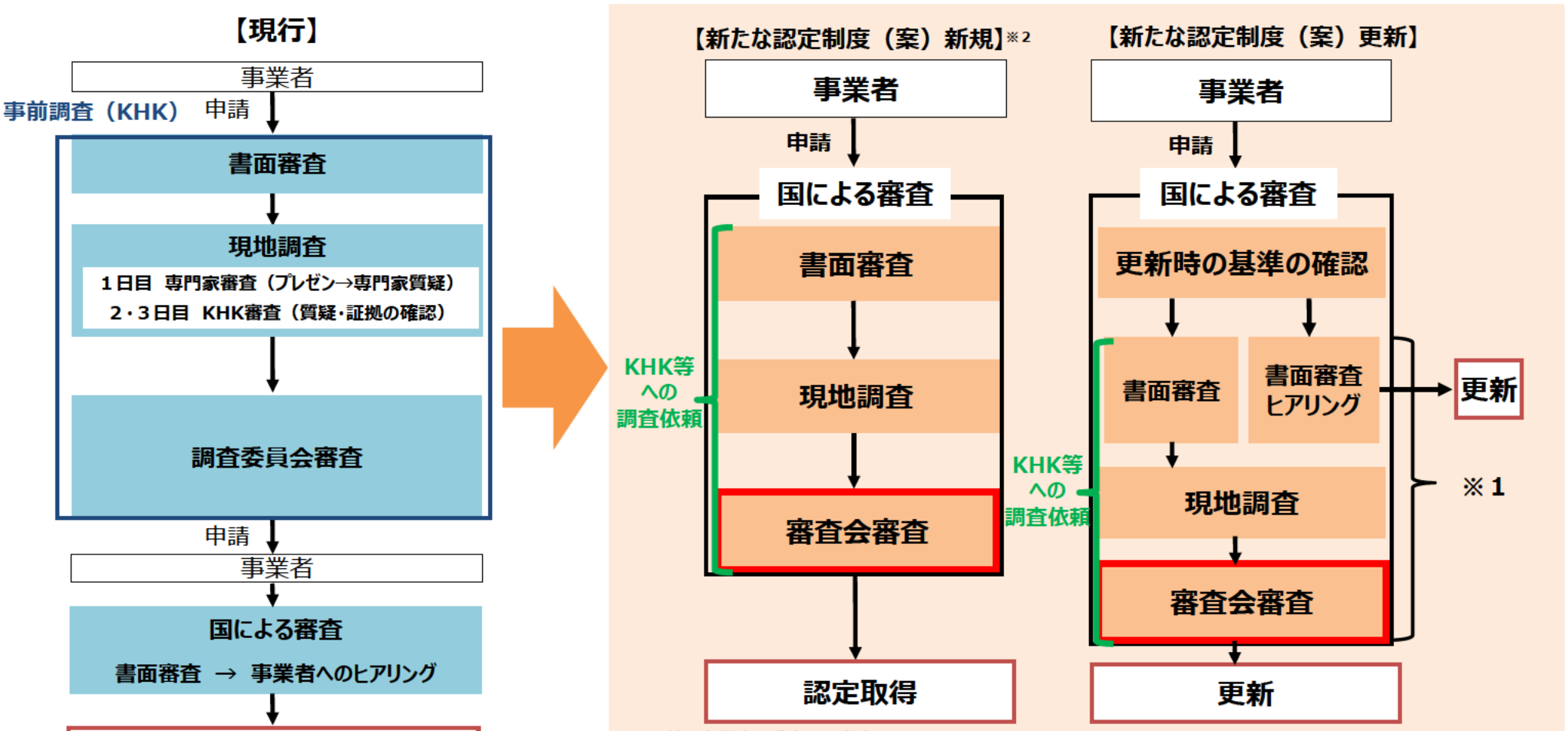
８．A認定事業者向けの特例措置

6-1. 新たな認定制度における認定審査のコンセプト

- 新たな認定制度では、**安全の確保及び向上を前提に、合理的かつ迅速な審査手続とする観点**から、**国が**（KHK等への意見聴取・調査依頼、外部有識者からなる審査会審査などを活用しつつ）**審査を行う**こととしており、以下のような見直しを行う方針。

  ① **審査プロセスの合理化（プロセスの合理化、申請書類・手数料の見直し、評価結果のランク付け廃止等）**

  ② **審査基準の透明化（審査基準・審査会審査の議事要旨※の公開）** ※企業の機密情報等を除いた上で作成。



※1　特に変更点を重点的に審査

※2　新規でA・B認定を受ける場合（但し、現行認定を受けている者の新制度認定審査では、特に変更点を重点的に審査）

6-2. 新たな認定制度における審査プロセスに関する今後の論点

- 新たな認定制度における審査体制について、下記の論点を検討する。

論点①　調査依頼制度の詳細

- ✓ **対象とする範囲**
- ✓ **指定機関の要件**
- ✓ **初回申請時の扱い**

【産構審分科会報告書における記載】

国は、国の検査及び審査会審査を行う案件のうち、必要と認めたときは、その範囲を定めて、KHK又は指定機関に意見を聴取し、又は調査を依頼できるものとする。KHK等の調査が行われた場合、国の検査は、その範囲で省略され、重複の検査・調査は行わない。KHK等が一部の調査を行う場合、運用上は、国とKHK 等は一緒に（一回で）検査・調査を行う。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

論点②　審査会審査の詳細

- ✓ **審査方法**
- ✓ **委員構成**

【産構審分科会報告書における記載】

〇新規認定：全数を国の検査及び審査会審査（注）を行う。

○更新：国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況等を踏まえ安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査（注）を行う。

（注）審査会審査：外部有識者（KHK、高圧ガスやIoT等のテクノロジーに関する学識経験者等）からなる審査会で行う審査

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.24 図21）

論点③　更新時に現地調査・審査会審査を実施する場合の基準

- ✓ **認定更新時に、現地調査・審査会審査を実施する場合の基準**

【産構審分科会報告書における記載】

更新では、国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況や法令違反（労安法等含む）、行政指導等の有無、また、大幅な変更（設備構成・製造能力・ガス種等）の有無等を踏まえ、安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査を行うものとする。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

6-3. 論点① 調査依頼制度の詳細について

● **審査は国が行う**との方針を踏まえ、調査依頼制度の詳細は下記のとおりとしてはどうか。

✓ 調査依頼を行う場合

- **初回申請時**※及び**認定更新時に安全の確保及び向上の観点から問題がないと認められない場合**には、国は**調査依頼を行う**。
  ※現行の認定事業者が新たな認定制度を初めて申請する場合も含む。

✓ 調査依頼制度における調査の方針・対象とする範囲

- 経済産業大臣からKHK又は指定機関（以下「KHK等」という。）への調査依頼の対象は、書面審査及び現地調査とする。
- 書面審査及び現地調査では、事業所が認定要件を充足しているかについて確認・審査を行う。
- 調査依頼制度における確認・審査は、**国の責任の下、審査基準に示されている項目の範囲内で行うことを原則**とする。ただし、認定要件の範囲内であれば※、審査基準に示されていない視点であっても、確認・審査を行うことができる。
  ※安全の確保及び向上のための意見を述べることもできるが、要件充足性の判断に影響は及ぼさない。

✓ 現地調査への国（本省）の関与

- 国（本省）はKHK等が行う現地調査に参加し、審査をKHK等とともに行う。

✓ 指定機関の要件

- サイバーセキュリティの専門性の有無も考慮し、指定機関の要件を定める。

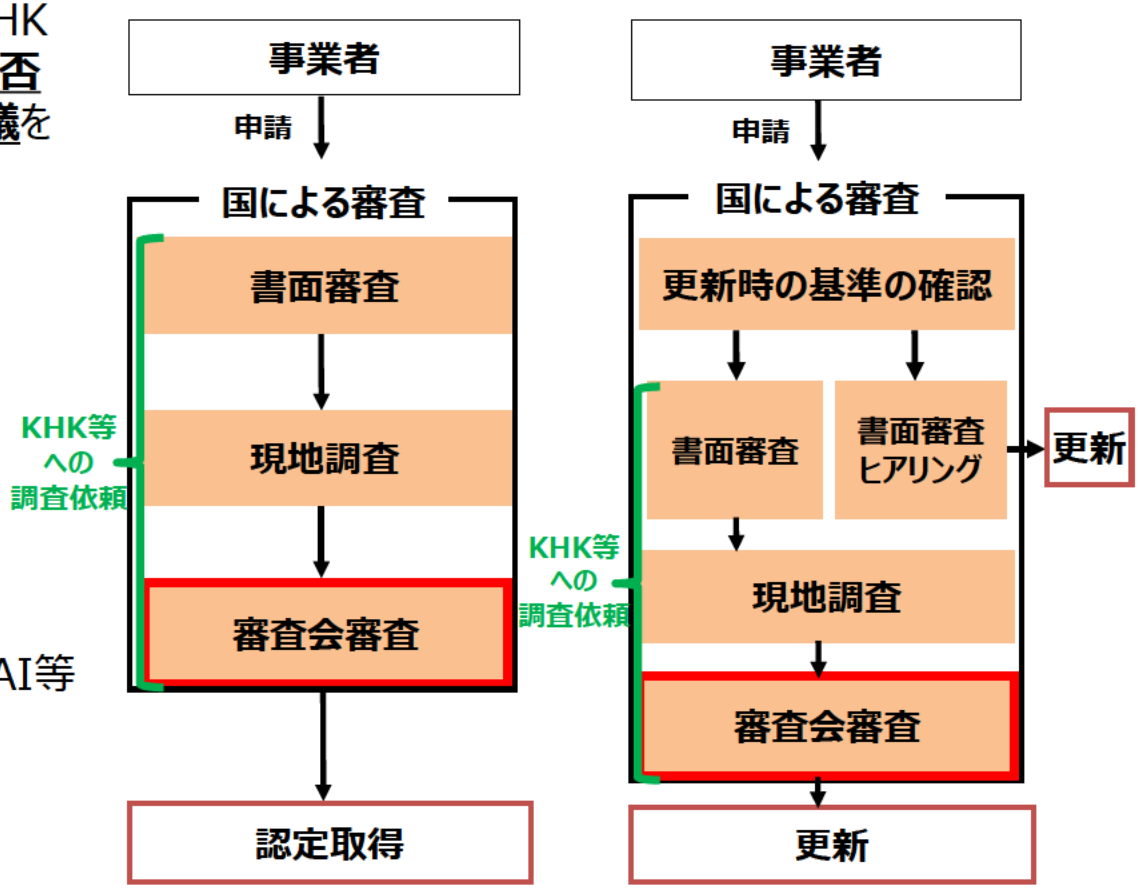
6-4. 論点② 審査会審査の詳細

● 審査会審査の審査方法及び委員構成は、下記のとおりとしてはどうか。

✓ 審査会審査の審査方法

- ４半期に一度開催する。
- 国及び調査依頼制度に参加する専門機関（KHK等）から**書面審査と現地調査の審査結果（合否等）を報告**する。その後、**審査結果について審議**を行う。
- 申請者（事業者）は不参加とする。
- **議事要旨は公開**※する。
  ※企業の機微情報を除いた上で作成。

【新規申請時の国の審査フロー】 【更新申請時の国の審査フロー】



✓ 審査会審査の委員構成

- **委員**

以下の分野の**外部有識者１０名程度で構成**する。
【外部有識者の主な分野】
✓ 学識経験者（高圧ガス、安全工学、IoT・BD/AI等のテクノロジー、サイバーセキュリティ）
✓ 企業法務（コンプライアンス）
✓ 企業ＯＢ等（実務経験者）
✓ 高圧ガス保安協会（ＫＨＫ） 等

- **オブザーバー**

✓ 申請事業所を管轄する地方自治体

6-5. 論点③ 更新時に現地調査・審査会審査を実施する場合の基準

- **新たな認定制度**においては、**国による書面審査・ヒアリングにより認定の更新を認める制度を新たに導入**する。
- その際、５年間（A認定の場合は７年間）の認定期間内に、**以下①～③の基準のいずれかに該当することとなった場合は、安全の確保及び向上の観点から問題がないと認められないと判断**し、現地調査及び審査会審査を行う。

更新時に現地調査・審査会審査を実施する場合の基準（案）

①事故や労働災害の有無

✓ **Ｂ２級※１以上の事故が発生**している事業所

✓ **死亡又は休業４日以上の労働災害※２が発生**している事業所

※１ 同一事業所において、Ａ級事故、Ｂ級事故又はＣ１級事故が発生した日から１年を経過しない間に発生したＣ１級事故（高圧ガスに係る事故に限る。）（「高圧ガス・石油コンビナート事故対応要領」３(2)）

※２ 従業員・協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

②法令違反の有無

✓ 高圧ガス保安法の法令違反が**２回※３以上**発生している事業所
（ただし以下の法令違反については**１回**）

① 死亡事故が発生したもの
② １００件を超えるような多数の法令違反を伴うもの
③ 国の行政処分が行われているもの
④ 国の行政文書による注意等が行われているもの

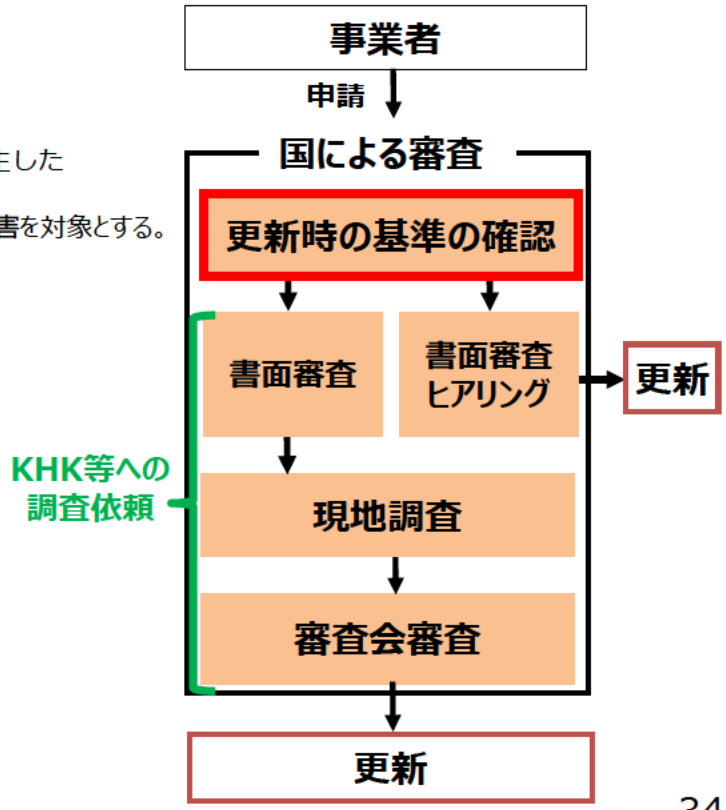
※３ 原則として、事業者からの報告数をカウントする。

③大幅な設備変更の有無

✓ **認定の対象に新たに高圧ガス製造施設を追加**する事業所※４

※４ 既存の認定施設において設備の変更工事が行われた場合、ガス種の変更等が行われた場合は含まない。

【更新申請時の国の審査フロー】



1．高圧ガス保安法における新たな認定制度の概要

2．主な審議事項と施行に向けたスケジュール

3．新たな認定制度のコンセプト

4．新たな認定制度の要件

5．新たな認定制度の特例

6．新たな認定制度の審査体制

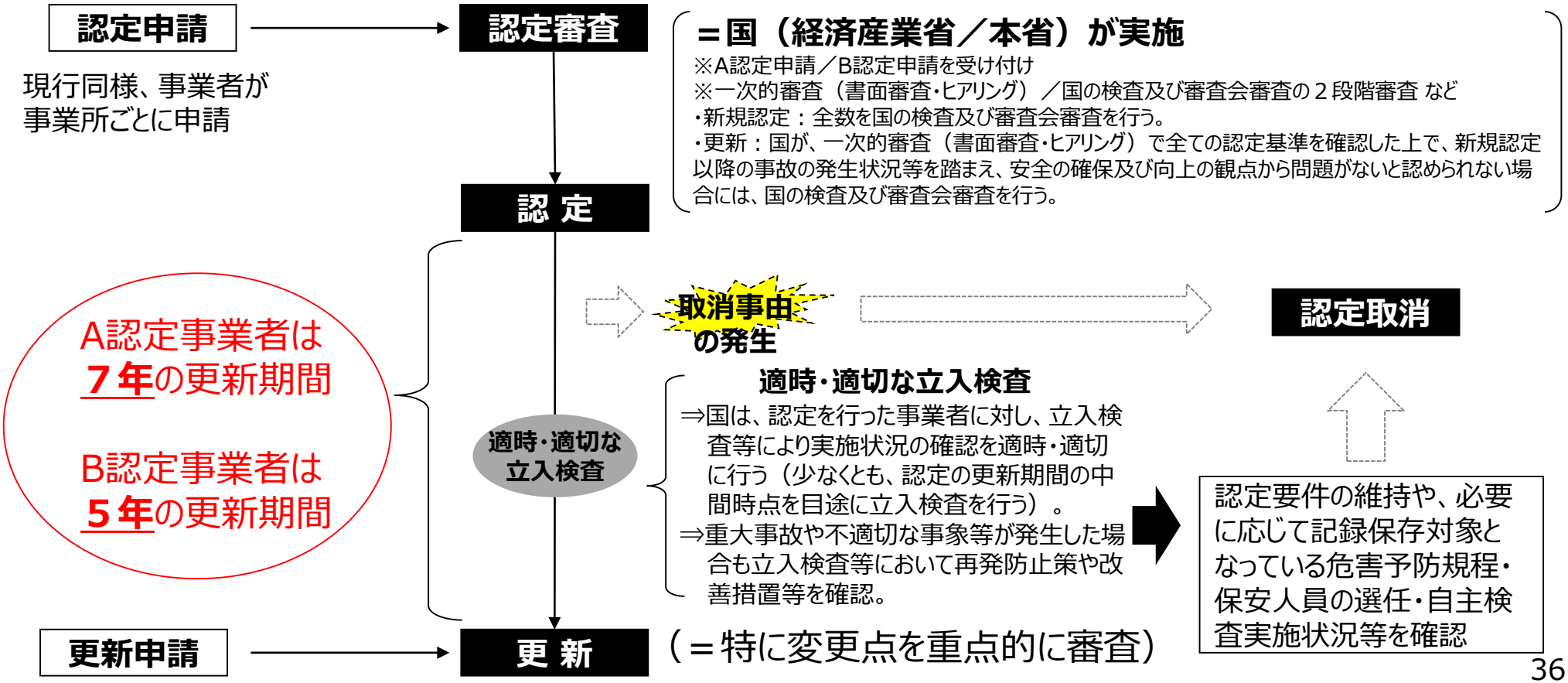
7．新たな認定制度の認定の更新期間

8．A認定事業者向けの特例措置

7-1. 新たな認定制度の認定の更新期間について

- 新たな認定制度における認定の更新期間については、①新制度では一部の要件が拡充されるものの、要件の大部は現行制度と同等の保安レベルを求めるものであること、②特例の範囲が現行制度よりも拡充されること、③近年の認定事業所の重大事故・法令違反の状況を考慮する必要があることを踏まえ 、現行認定制度同様、**A認定（スーパー認定相当）7年、B認定（通常認定相当） 5年としてはどうか。**

＜認定から更新までのフロー図＞



1．高圧ガス保安法における新たな認定制度の概要

2．主な審議事項と施行に向けたスケジュール

3．新たな認定制度のコンセプト

4．新たな認定制度の要件

5．新たな認定制度の特例

6．新たな認定制度の審査体制

7．新たな認定制度の認定の更新期間

8．A認定事業者向けの特例措置

8-1. A認定事業者に係る検査面での制度的措置（ふり返り）

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）**において、**A認定事業者には**、手続面での制度的措置に加え、**検査面での制度的措置を拡充し**、比例原則・リスクベースに基づき、**認定事業者間で制度的措置を差異化**することとされた。

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.11

①CBM（Condition Based Maintenance）の円滑化

●例えば、高圧ガス小委員会等で技術的検証を行い、以下について検討する。
- 現行の減肉判断：単純腐食に加え、クラック・クリープも対象
- CBMの考え方を用いた検査方法の拡大の検討：計測器類・遮断弁等

●KHKへの腐食環境や厚さ測定等のデータ提出義務を廃止

②検査等に係る基準・規格の柔軟化

－採用する基準・規格（海外規格等）の大臣認定制を導入する。
（採用する基準・規格の複線化・複相化の円滑化）

※具体的には、例えば、通達（補足1）において、肉厚測定検査及び開放検査を行う方法について「KHK/PAJ/JPCA S0851(2014)（補足2）又はこれと同等の基準」を用いることになっているが、「これと同等の基準」について、事業者自らの判断に加え、大臣が認定することにより、検査等に係る基準・規格を柔軟に選択できるようにすることが含まれる。また、肉厚測定の間隔（現行4年以内）及び検査時期設定係数（現行0.8）のあり方については、事業者において、その能力や設備管理の実態等に応じ、一定の範囲で決定できるなど仕組みの柔軟化を図る方向で検討する。その際、「一定の範囲」については、肉厚測定の間隔及び検査時期設定係数に関して事業者が選択しうる最大の値のあり方等について、B認定との差異化も考慮しつつ、技術的な検証を踏まえて検討する。

（補足1）「特定認定事業者及び自主保安高度化事業者の認定について」20201218保局第1号
（補足2）高圧ガス設備の供用適性評価に基づく耐圧性能及び強度に係る次回検査時期設定基準

（注１）A認定の認定時、採用する基準・規格のリストを添付し、同時に採用する基準・規格の認定を受けることも可能とする方向で検討する。

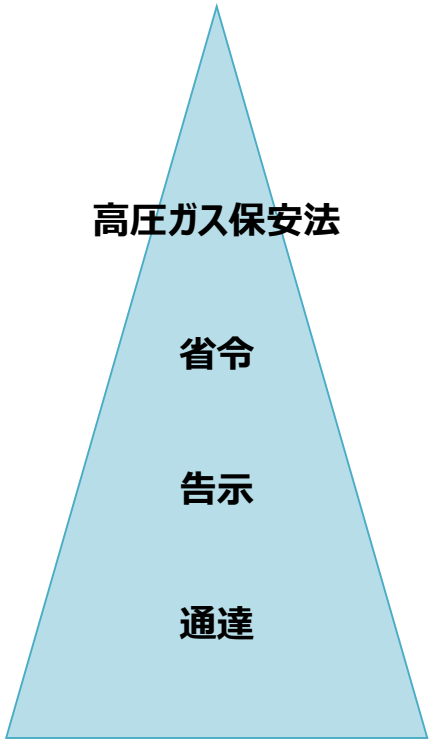
（注２）なお、B認定においては、引き続き、KHK/PAJ/JPCA S0851(2014)によることとするものの、技術的な検証を踏まえ、肉厚測定の間隔（現行最大2年⇒例えば4年）及び検査時期設定係数（現行0.5⇒例えば最大0.8）の柔軟化措置を講じる方向で検討する。

8-2. A認定事業者向けの特例措置（検査等に係る基準・規格の柔軟化のための新たな仕組みの導入）

- **現行のスーパー認定事業者（A認定相当）**には、**検査等に係る基準・規格の自由選択制が導入**されている。
- しかしながら、**事業者自らの判断により検査等に係る基準・規格を自由に導入することは積極的には活用されず**、**事業者は、実質的に法令で定められた基準・規格に従って保安業務を行っているのが実態**。
- このため、広く民間の先端の技術的知見を取り込み、一層民間規格の活用を促進する観点から、国・高圧ガス保安協会を中心とした従来の基準策定機能に加え、**A認定事業者による検査等に係る基準・規格の自由選択性が実質的に機能する仕組みを導入**することとしてはどうか。

【現行の高圧ガス保安法における検査方法】

- 現行のスーパー認定事業者は、**自由な検査方法を選択することができる**。



（法）高圧ガス保安法　第三十五条

4　第一項の都道府県知事、協会又は指定保安検査機関が行う**保安検査の方法は、経済産業省令で定める。**

（省令）コンビナート等保安規則

第三十七条　法第三十五条第四項の経済産業省令で定める**保安検査の方法は、開放検査、分解検査その他の各部の損傷、変形及び異常の発生状況を確認するために十分な方法並びに作動検査その他の機能及び作動の状況を確認するために十分な方法**でなければならない。

2　前項の**保安検査の方法は告示で定める。ただし、次の各号に掲げる場合はこの限りでない。**

一　（略）

二　**特定認定事業者が**、令第十条ただし書の認定に係る特定施設について行う保安検査の方法であつて、**次のいずれにも該当するものを用いる場合。**

イ　製造設備の寿命等を勘案して、適切な時期に、肉厚測定検査及び開放検査を行う方法

ロ　少なくとも八年に一回は運転を停止した検査を行う方法

ハ　保安検査に係る責任者が前項に定める方法に適合すると認めた方法

（告示）保安検査の方法を定める告示

保安検査の方法は、次の表の上欄に掲げる区分に応じ、それぞれ同表の下欄に掲げるものとする。

製造施設	保安検査の方法
四 コンビナート等保安規則の適用を受ける製造施設	四 高圧ガス保安協会規格ＫＨＫＳ ０８５０―３ （２０１７）保安検査基準

（通達）「特定認定事業者及び自主保安高度化事業者の認定について」

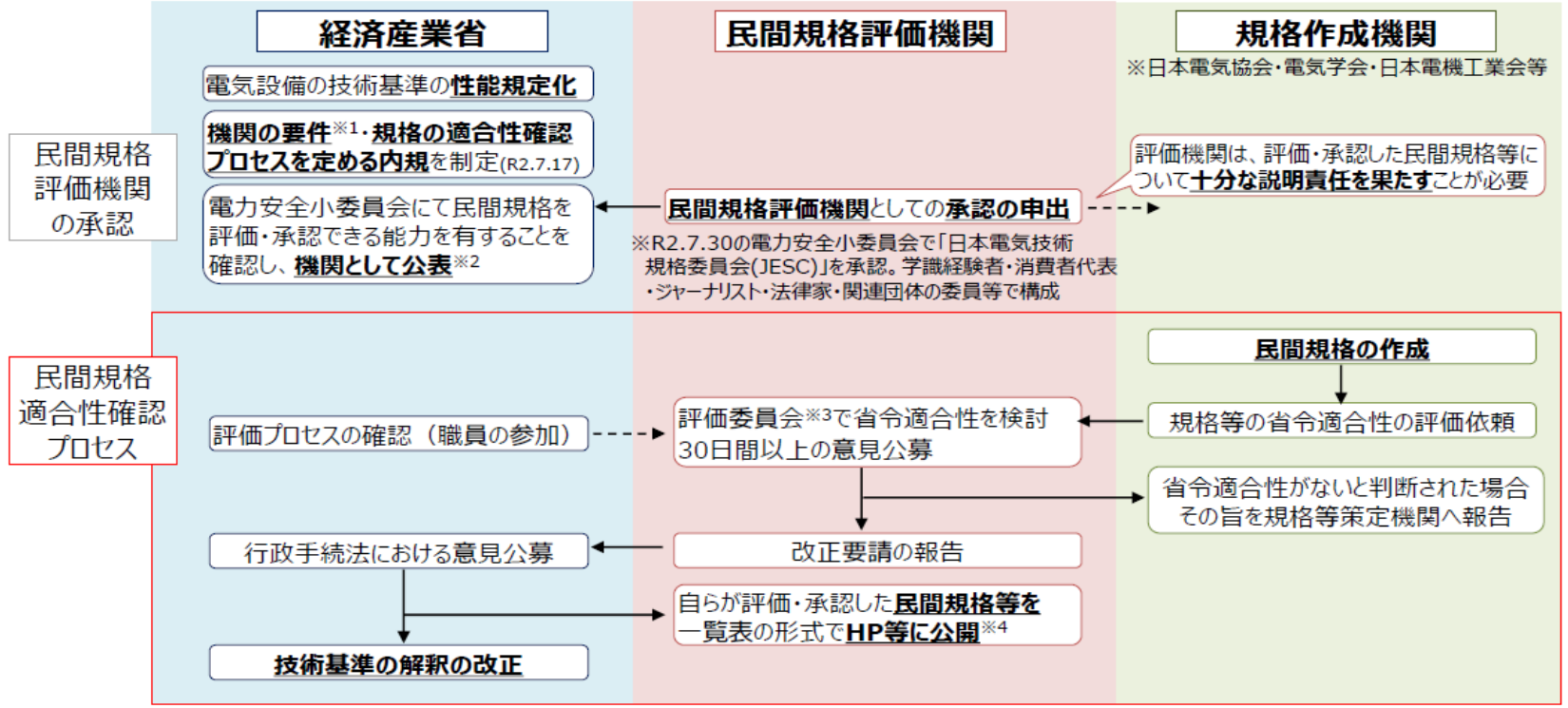
肉厚測定検査及び開放検査を行う方法について「KHK/PAJ/JPCA S0851(2022)又は**これと同等の基準**」を用いることになっている

8-3. A認定事業者向けの特例措置（電力分野を参考とした新たな仕組みの導入）

- **電気事業法における電気設備の技術基準への民間規格の取り込みを参考に、高圧ガス保安法上の検査等に係る基準・規格の自由な選択を促す仕組みを導入してはどうか。**
- 具体的には、**A認定事業者を対象に、国が定める要件を満たす民間規格評価機関が承認した検査等に係る基準・規格であれば、高圧ガス保安法上の適切な検査方法と認めることとする仕組みを導入してはどうか。**

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）P.65　図64

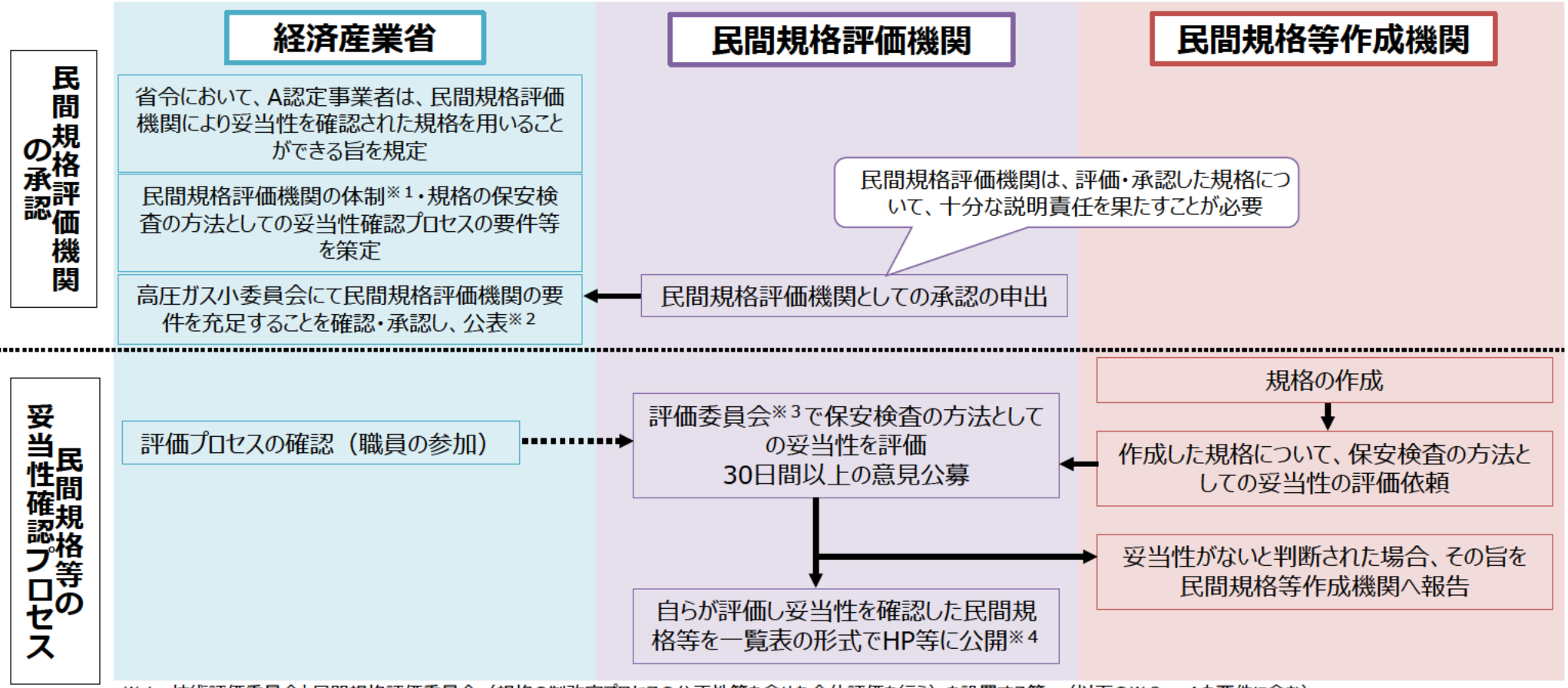
【電気事業法における電気設備の技術基準への民間規格の取り込み】



※1 技術評価委員会と民間規格評価委員会（規格の制改定プロセスの公正性等を含めた全体評価を行う）を設置する等。（以下の※2~4も要件に含む）
※2 適切な評価の実施は、国の職員による**評価委員会への立会い**、**１年ごとの定期報告**(評価の実施状況についての**有識者による外部評価**)等により確認
※3 民間規格等に係る**技術分野に加え**、**消費者問題、法律、ジャーナリズム等の幅広い分野の専門家から構成**
※4 規格として承認された日から**少なくとも五年に一回は、改正、廃止又は確認**が行われるよう適切に管理

8-4. A認定事業者向けの特例措置（電力分野を参考とした新たな仕組みの導入）

- 第23回高圧ガス小委員会において、**A認定事業者を対象に、国が定める要件を満たす民間規格評価機関が承認した検査等に係る基準・規格であれば、高圧ガス保安法上の適切な検査方法と認めることとする仕組みを導入**する方針が了承された。
- 本仕組みを実現するため、**民間規格評価機関の要件を定める**ことが必要。



※1　技術評価委員会と民間規格評価委員会（規格の制改定プロセスの公正性等を含めた全体評価を行う）を設置する等。（以下の※２～４も要件に含む）
※2　国は、承認した民間規格評価機関の活動について、年に１回高圧ガス小委員会に報告し、当該民間規格評価機関が民間規格等を適切に評価・承認できることを確認。
※3　民間規格等に係る技術分野に加え、消費者問題、法律、ジャーナリズム等の幅広い分野の専門家から構成。
※4　規格として承認された日から少なくとも五年に一回は、改正、廃止又は確認が行われるよう適切に管理。

8-5. 民間規格評価機関の承認・要件適合性の確認

- 国は、**候補となる機関が民間規格評価機関の要件を満たすことを確認し、承認する**。
- 国は、承認した民間規格評価機関について、民間規格等の**妥当性確認プロセスが要件に従い運営されていることを確認**し、**必要があると認められる場合は改善指導等**を行う。
- 民間規格評価機関は、**年１回以上の外部評価**を受け、**妥当性確認プロセスが適切に運営されていることを自ら確認**し、必要に応じて改善策を講じる。

➢ 国による民間規格評価機関の承認

- 国は、高圧ガス小委員会において、候補となる機関が民間規格評価機関の要件を満たしているかどうかを確認し、承認する。
- 国は、国の審議会の議事録や、民間規格評価機関の要件等について確認した内容をホームページ等で広く公開する。

➢ 国による確認

- 国は、年に１回、民間規格評価機関の活動について高圧ガス小委員会に報告し、当該民間規格評価機関が民間規格等を適切に評価できることを確認する。

➢ 外部機関による評価

- 民間規格評価機関は、妥当性確認プロセスが適切に運営されていることを自ら確認するため（PDCAサイクルの構築）、外部評価を受け、その結果に基づく改善等を定期的に行う。

8-6. 民間規格評価機関における民間規格等の妥当性確認プロセス①

- 民間規格評価機関は、**技術評価委員会**（技術的な側面の評価を行う）及び**民間規格評価委員会**（規格の制改定プロセスの公平性、客観性及び透明性等を含めた全体的な評価を行う）を設置するなど、民間規格等の妥当性確認のための**十分かつ確実な評価体制を構築**する。

➢ 評価の方法

- 民間規格等の評価に当たっては、技術的な側面の評価を行う技術評価委員会と民間規格制改定プロセスの公平性、客観性及び透明性等を含めた全体評価を行う民間規格評価委員会を設置する。また、評価対象となる民間規格等に応じた適切な審議回数を確保することなどにより、十分な評価が行われるようにする。
- 評価対象となる民間規格等の作成に関与した専門家は評価に関与すべきではなく、これが確実に担保される措置を講じる。

➢ 技術評価委員会

- 民間規格等の技術的な側面の評価にあたっては、専門家、民間規格等を使用する事業者等（業界団体、エンジ会社、メーカー、検査会社等）も加える等、評価対象となる民間規格等に関係するできるだけ幅広い者の参加を必要とする。

➢ 民間規格評価委員会

- 民間規格等の評価にあたっては、規格内容の技術分野の専門家に加え、消費者問題、法律及びジャーナリズムを含む幅広い観点から評価を行う専門家の参加を必要とする。

8-7.民間規格評価機関における民間規格等の妥当性確認プロセス②

- 民間規格評価機関は、**民間規格等の保安検査の方法としての妥当性について評価**を行う。
- 民間規格評価機関は、妥当性を確認した民間規格等をリストに掲載し、**公開**する。
- **国は**、技術評価委員会と民間規格評価委員会への立合い等により、**民間規格評価機関における民間規格等の妥当性確認プロセス全体を確認する**。

➢ 評価の観点

- 民間規格評価機関は、当該民間規格等が技術の動向や関連する最新の知見を適切に踏まえているか等を踏まえた評価を行い、結果を評価書にとりまとめる。

➢ 妥当性を確認した民間規格等のリストへの掲載

- 民間規格評価機関は、評価書をとりまとめ、保安検査の方法としての妥当性を確認した民間規格等を、民間規格評価機関が公開する「民間規格評価機関が承認した民間規格等」のリストに掲載する。

➢ 妥当性確認プロセスにおける国の関与

- 国は、民間規格評価機関における民間規格等の妥当性確認プロセス全体について、技術評価委員会と民間規格評価委員会への立会い等により確認する。

8-8. その他検査面での制度的措置の見直し事項①

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の整理を踏まえ**、以下の検査面での制度的措置の見直しを行うこととしてはどうか。

① B認定を対象とした肉厚測定の間隔等の見直し

現行の規定

- 現行の通常認定では、次回検査時期の設定について、KHK/PAJ/JPCA S 0851(2022)（以下「KHKS」という。）によることができると規定されているが、現行の通達※において、以下①～③等の読み替えを行い、KHKSよりも厳格な運用を行っている。

  ① 肉厚測定の間隔（肉厚測定検査における次回検査時期までの間隔。KHKS上最大4年とされているところ、通達により最大2年に厳格化。）
  ② 検査時期設定係数（次回検査時期を算出する際に余寿命に乗じる数値。KHKS上最大0.8とされているところ、通達により0.5に厳格化。）
  ③ 肉厚測定回数（減肉速度の算定時に必要とされる肉厚測定の回数。KHKS上計3回分とされているところ、通達により計5回分に厳格化。）

※「認定完成検査実施者及び認定保安検査実施者の認定について」

見直し理由

- 通達においてKHKSを厳格に読み替える旨の運用を行った背景としては、本制度導入当時（2011年）、肉厚測定の間隔を１年以上に延長することが初めての試みであったことから、慎重を期す必要があるとの判断に基づくもの。
- **当該規定の制定から既に10年以上が経過し、この間、技術的不都合や安全性への懸念は生じていないことから、これを見直し、KHKSで定められている基準を適用する**ことが適切。

見直し後の措置

- B認定（通常認定相当）では、KHKSを現行の厳格に読み替える旨の運用は見直し、次回検査時期の設定について、KHKSによることができることとする。

8-9. その他検査面での制度的措置の見直し事項②

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の整理を踏まえ**、以下の検査面での制度的措置の見直しを行うこととしてはどうか。

② KHKへの腐食環境や厚さ測定等のデータ提出義務の廃止

現行の規定

- 現行のスーパー認定事業者のうちCBM認定を受けている事業者に対しては、腐食環境や肉厚測定等のデータを定期的に高圧ガス保安協会に提出する義務が課せられている。

※「特定認定事業者及び自主保安高度化事業者の認定について」

見直し理由

- 腐食環境や肉厚測定等のデータ提出義務を課すこととした背景は、本制度導入当時（2019年）、開放検査の実施時期の設定についての柔軟化措置を講じることが初めての試みであったところ、制度導入初期は慎重な運用を期す必要があるとの判断に基づくもの。
- **当該規定の制定から一定期間が経過し、この間、技術的不都合や安全性への懸念は生じていないことから、これを廃止する**ことが適切。

見直し後の措置

- 高圧ガス保安協会への腐食環境や肉厚測定等のデータの提出義務は廃止する。

軽微な変更工事の範囲の拡大について

- 産構審分科会報告書※において、「**軽微変更についてはその対象範囲を拡大**した上で記録保存義務とする」方針が示されている。

※産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.18

- 新たな認定制度において、**事後届出の対象となる変更工事は、取替えの工事等の特定変更工事以外の工事**としたことを踏まえ、認定事業者が行う軽微な変更工事の対象に新たに追加する工事は、**部品の取替えの工事等**とすることを想定。具体的には、**現行の軽微な変更の工事と同程度の危険性の部品の取替え工事**や、**高圧ガス設備の強度に影響のない変更工事**等を、新たに軽微な変更工事の対象に追加する。
- なお、**新制度の円滑な運用を確保する観点から、**詳細な解釈を通達等において可能な限り明らかにすることを予定。

軽微な変更工事の対象に追加するもの

①多管円筒形熱交換器以外（エアフィンクーラーを含む）のチューブの交換
②フランジ継手以外の継手類の変更
③　②に伴う配管の撤去工事

（参考）手続き不要の工事※とするもの
①熱交換器のプラグ打ち
②熱交換器のプラグ打ちに係るチューブの切断又は撤去
※通達「高圧ガス保安法第 14 条第 1 項及び第 4 項、第 19 条第 1 項及び第 4 項並びに 第 24 条の 4 第 1 項に基づく軽微な変更の工事の取扱いについて」において記載することを予定。

○新認定制度における許認可手続き（イメージ）

資料③　別添10

変更の内容	現行制度における手続き			新制度における手続き（案）	
	特定認定事業者 （認定完成検査実施者）	認定完成検査実施者	認定保安検査実施者	A認定を受けた者	B認定を受けた者
特定変更工事に該当する変更の工事	許可 完成検査実施 （事後届出）	許可 完成検査実施 （事後届出）	許可 完成検査受検	許可 完成検査実施 （記録保存）	許可 完成検査実施 （記録保存）
製造の方法の変更 （常用圧力・温度の変更（設計条件を超える変更を伴うもの））	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要
製造の方法の変更 （常用圧力・温度の変更（設計条件内での変更を伴うもの））	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	事後届出	事後届出
製造の方法の変更 （常用圧力・温度の変更を伴わないもの）	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	（記録保存）	（記録保存）
ガス種の変更	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要
完成検査不要工事（処理能力の変更が一定（20%)範囲内の変更の工事等）	許可 完成検査不要	許可 完成検査不要	許可 完成検査不要	事後届出	事後届出
［以下現行軽微な変更の工事(拡大検討前）］					
処理能力、性能、技術基準、製造計画書等の記載事項に変更がないものへの取替（すみ肉溶接で告示で定める母材）（コ14①-6）（通3）	事後届出	事後届出	許可 完成検査受検	（記録保存）	（記録保存）
管台（ノズル）の取替 処理能力の変更がなく、同等以上の性能かつ特定設備の基準適合のものへの取替（すみ肉溶接で告示で定める母材）コ14①-7イ)(通4)	事後届出	許可 完成検査実施／完成検査不要 （事後届出）	許可 完成検査受検	（記録保存）	許可 完成検査実施／完成検査不要 （記録保存）
特定設備の取替え 処理能力の変更がなく、同等以上の性能かつ特定設備検査合格のものへの取替(コ14①-7ロ)(通4)	事後届出	許可 完成検査不要	許可 完成検査不要	（記録保存）	許可 完成検査不要 （記録保存）
特定設備の変更 処理能力及び設置位置の変更がない特定設備の変更（保安上特段の支障がない（KHK委託検査品等に限る。）（コ14①-7ハ)(通5)	事後届出	許可 完成検査実施／完成検査不要 （事後届出）	許可 完成検査受検	（記録保存）	許可 完成検査実施／完成検査不要 （記録保存）
高圧ガス設備（特定設備以外）の変更 処理能力の変更がない高圧ガス設備（配管、バルブ、フランジ継手、附属機器類）の変更(コ14①-7ニ)(通6)	事後届出	許可 完成検査実施／完成検査不要 （事後届出）	許可 完成検査受検	（記録保存）	許可 完成検査実施／完成検査不要 （記録保存）
高圧ガス設備（特定設備以外）の変更 処理能力の変更がなく認定品又は保安上特段の支障がないもの（処理能力及びＰ＆ＩＤに変更がない）への変更（コ14①-8イ)(通6)	事後届出	事後届出	事後届出	（記録保存）	（記録保存）
高圧ガス設備（特定設備以外）の変更 処理能力及び位置の変更がない高圧ガス設備（配管、バルブ、フランジ継手）の変更(コ14①-8ロ)（通6）	事後届出	事後届出	事後届出	（記録保存）	（記録保存）
ガス設備（特定設備以外）の変更 処理能力、性能、技術基準、製造計画書等の記載事項に変更がないものへの取替(コ14①-8ハ)（通3）	事後届出	事後届出	事後届出	（記録保存）	（記録保存）
上記以外の軽微な変更の工事（処理能力の変更を伴うもの）	事後届出	事後届出	事後届出	事後届出	事後届出
上記以外の軽微な変更の工事（処理能力の変更を伴わないもの）	事後届出	事後届出	事後届出	（記録保存）	（記録保存）

別添１１

〇新認定制度の自治体説明における主な質疑

2023/3/22
高圧ガス保安協会

質問及び回答
１．高圧ガス保安法における新たな認定制度の概要
・事業所へのヒアリングはしたのか？　その反応をお聞きしたい。（自治体） ⇒ヒアリングはしている。テクノロジー、要件に関する反応は、追加的な対応が必要なものはあるが、概ね妥当な内容という感じである。ただ、現在認定を取っていない事業所にとっては、ハードルが高いとは思うし、アンケートを見る限りあまり関心は高くない。（KHK）
・この制度が上手くまわっているときはよいが、もし、認定取消案件が発生した場合、行政負担が一気に増加するおそれがあるので、例えば年に１回の報告制度等を組み入れ、事務量を把握できるような制度にならないか（自治体） ⇒行政側の負担については考慮すべきで有り、しっかり受け止めたい。法令違反が発生する背景として制度のわかりにくさもあるかと思うので、その辺がないように努めたい。また行政手続きの DX 化も進めて、併せて法令違反が起きないシステム作りに努めたい。（METI） ⇒定期的な報告を制度上に組み込むことは難しいかもしれない。立検等で確認するなどが現実的な対応かと思う。（KHK）
・現行のスーパー認定事業者が新しい認定のインセンティブを享受するためには新しい認定を取得しなければならないということか。（自治体） ⇒そのとおり。再度、新制度下での認定の再取得が必要となる。既存の認定事業所については、認定更新の時期を捉えて徐々に新制度に切り替わってゆくものと思われる。施行直後は準備等の関係で併存する現行制度での更新を選択する場合もあると思うが、この場合には新しい認定のインセンティブは適用されない。（METI）
・今般の制度改正は、保安人材の枯渇もきっかけのひとつである。新制度の特例に、保安人員の配置の柔軟化があり、発災時等における緊急時対応を行う保安係員等の配置を、個別具体の事例ごとに判断することとなるが、判断基準はどういったものか。自動放水による消火等、技術導入が要件か。保安人材を合理化した場合、許認可の他に防災等のリスクに消防が対応することとなることを懸念している。（自治体） ⇒具体的には個別の事案について検討が必要であるが、技術が活用され、緊急事対応にも対応できることが重要である。自治体及び事業者にアンケートを取っている中では、今現在は個別事案が出てきていない。（METI）
２．主な審議事項と施行に向けたスケジュール
・今年の末に施行となるが、A 認定 B 認定の切り替わりは更新時ということでよいか。（自治体） ⇒新制度を（更新期限前に）前倒しで申請することも制度上は可能であるが、更新のタイミングで切換えが多いと思う。１２月に施行されると３年間は（新制度・現行制度の）どちらも申請できるという経過措置期間が確保されている。来年の１月２月に期限を迎える場合、新制度で間に合わないというところであれば、現行制度での申請となることが考えられる。ある程度時間が経つと新制度が増えてくると思う。（METI）
・次回更新が制度の移行期間になる場合には、旧制度か新制度かを事業者が選択できるという理解で良いか（自治体） ⇒そのとおり。ただし、旧制度の有効期限は 2030 年までという制限があるので、徐々に新制度に切り替わっていくものと思われる（METI）
・現行の認定を取得している事業所でも、新制度で申請しようとする場合は、新規の申請となるという理解で良いか？（自治体） ⇒そのとおり。現行制度で認定を取得している事業所でも新制度では新規の申請となる。なお、今年の年末から新制度を施行する予定であり、現行制度の認定の有効期限を迎える事業所から順次切り替えが進むものと思うが、移行期間中は現行制度での更新申請も可能となっている。（METI）
・認定の単位は、施設単位ではなく、事業所単位という理解で良いか？（自治体） ⇒事業所単位の認定となることで間違いはないが、認定施設の選択をなくすと全ての施設が認定要件を満たさないと認定できなくなるということも問題があるので、申請上は認定施設を選択できる制度としたい。（KHK）
・関連する質問となるが、その場合、認定事業所であっても、非認定施設については、認定事業所としてのインセンティブ（許認可の手続き緩和策等）は適用されないということでよいか。（自治体） ⇒そのように考える。（KHK）
３．新たな認定制度のコンセプト
・認定事業者に緊張感を持ってもらうためには、インセンティブを与えるだけでなく、厳しく接することも必要であり、認定取消の要件を厳しくすることも必要ではないか。高圧ガスの事故だけでなく、関連法令の違反を対象とすることは考えられないか。実際問題として昨年県下で発生した事故の多くが他法令の事故であり、同一事業所で連続して発生している。認定事業所として問題があるのではないか。（自治体） ⇒あくまで保安法上の制度の話なので、どこまで他法令での事象を対象とするかは議論の分かれるところである。悪質なものは取り消さなければならないとは思うが、取消を乱発することには慎重な議論が必要。他の自治体との話でも、もし認定が取り消された場合には、自治体で検査する体制を組むことが難しいという話も出た。（METI）
・資料 P8 の中小事業所における保安レベル向上のための対策について具体的に伺いたい。（自治体） ⇒当該箇所は今回の法令改正の対象でないため、本日の資料では説明していないが、中小事業所向けの施策については別途予算措置をしており、来年度以降も引き続き検討する予定である。具体的には日本能率協会で実施しているスマート保安講座の受講の補助事業や手続きデジタル化のためのアプリの開発等を考えている。（METI） ⇒軽微変更の条文を読めば、自主保安高度化事業者制度を上手く活用すれば、手続き関係の合理化等に有効に活用できるのもの（例：認定品への変更は軽微変更等）もあるので、県としても同制度は引き続き継続していただきたいと考えている。県としても中小事業所の保安力活用が今後の課題と捉えており、保安の取組状況の把握を進めるとともに、その裾野を広げて行きたいと考えているので、国としてもご支援をお願いしたい。（自治体） ⇒中小事業所向けの更なるインセンティブの付与については今後も検討していきたいと考えている。（METI）
４．新たな認定制度の要件
・P11 について、今回 B 認定についてテクノロジー活用の分野が入っているが、現在、通常認定の事業者が新制度で B 認定を取得したい場合は、テクノロジーの要件を満たさない場合は認定されないという理解でよいか。（自治体） ⇒初回申請時にテクノロジーの全て PDCA ができているのかということについて、導入計画が策定されていることなどを確認することになると思われる。それでもできない方は個別に見ていかないといけないが、一定の配慮をしたとしても要件を満たされなければ認定は取れないということになる。

（METI）

・テクノロジーの活用がすぐに難しいということで、段階的にということになると、（申請のタイミングが）遅くなるにつれて（認定の要件が）難しくなってくるのか。（現行制度において）複数の県に事業所をもつ方が、他県で認定を受けたところがあり、そのくらいのものを準備していたら、その後、上乗せを求められたという話もあった。よりテクノロジーが発達すればその分求められるテクノロジーも高度になっていくという認識でよいか。（自治体）

⇒結果的に陳腐化したもので認定大丈夫かというと、この制度も過去２５年間運用されている中で、時代の変化に対応してきており、当然その点は見直しされることもあると思う。事業者の方が全く予見できない等、場所による違いも出てくると思うので、P32 にあるような審査基準を作っていきたいと思う。認定要件に対応する具体的な審査の視点、何を確認していくのかを明らかにさせていただく。その中で審査していくが、審査基準が陳腐化していけば見直しが必要と考える。国の全体の審査基準なので、準備期間はあるかもしれないが全体の中で底上げしていくことであり、何を求めていくのかを議論した上で明らかにしてく。審査の透明化を図る中で必要があれば審査基準の見直しをしていく。なので、見えない中で急に要求されるということはないが、時代の中で適宜見直しをしていく（METI）

・こちらは定期的な５年１０年に一度見直ししていくのか、適宜見直ししていくのか。（自治体）

⇒両方ありうる。個別事案が生じるとその都度見直ししなければならないと思う。また、定期的に全体のオーバーホールをしていく必要もある。一方、サイバーのような別のトラックで見直しが進んでいるものもあり、適宜見直しをしていく。（METI）

・法律の読み違いにより行っていなかった場合、法令違反になるかどうかというのはどのように判断するのか。（自治体）

⇒一律に申し上げられないが、事実認定しないとどういう背景でということもあるので判断できない。個々に何が背景なのか、どういった形で事案が起きてしまったか、個々の事案を確定していかないと一律には言えないと思う。ただ認定基準に照らして、悪質性とかこれまでの認定取消の事案等ケースバイケースで見ていくしかないと思う。最終的に是正が必要なら許可等をとっていただくのが現行制度の運用となっている。それに基づく処分が取り消しなのか注意なのかはケースバイケースの判断となる。（METI）

・前の説明をいただいたときに、法令違反は機動的な措置をということがあったので基準等が決められているかと思ったが、ケースバイケースということなのか。（自治体）

⇒機動的なというところはＰ３６のとおりであるが、具体的な取り消し基準のところは認定取消事案を受けて具体化していくというのが今の取り組みかなと思っている。「機動的な」というのは法令違反があれば、そこに対する立入検査、報告徴収等、そういうところで受けていくのかと思っている。（METI）

・法令違反の有無については、ケースバイケースで一律に決められないので、報告徴収等で情報を集めて判断するということになるのか。（自治体）

⇒そのとおり（METI）

・p3 スマート保安の推進に関し、懸念を感じていることがある。昨年県下で 17 件の事故が発生したが、その半分が人的要因に起因するものであった。以前であれば設備要因による事故が 7 割を占めていたが、最近は知識不足、経験不足という人的ミスによる事故が増えている気がする。スマート保安によりますます人が少なくなっていくことを心配する。（自治体）

⇒ご懸念事項はもっともなことと思う。高圧ガスの分野に限らず、今後全体的に人が減って行くであろう事は間違いのないことであり、これを踏まえ、スマート保安の導入を進めることは必要と考えているが、決してご懸念の事項をないがしろにするつもりない。その点についても引き続き検討したい。（METI）

⇒企業は営利活動であるので、スマート化の推進が単に人の削減という方向に進まないこと期待する。（自治体）

・ｐ11 サイバーセキュリティへの対応について、各業界のガイドラインに従うということであるが、業界によっての違いが出てくることはないか。以前、環境アセスのガイドラインが各官庁から出された際に、それぞれのガイドラインの内容が違い大きかった。やる方が迷うことがないような配慮が必要である。（自治体）

⇒各業界のガイドラインは、内閣サイバーセキュリティセンターの指針を参考として定められているものである。業界によって対象やその対策が異なってくるので多少の違いは出てくるとは思うが、全く別のものになることはないと考える。（METI）

⇒環境アセスのガイドラインについては、各官庁の立場も違いもあって内容にばらつきがあったのではないかと思うが、サイバーセキュリティ対策についてはそのようなことは少ないと思う。（KHK）

・p12　法適合性確認能力については、誰がどのように判定するのか。事業所の担当者の能力に依存する部分も多いと思うが、継続性という観点からどのように考えるか（自治体）

⇒ご指摘の点は、令和 3 年度の報告書における検討事項であり、結論として複層チェック体制を構築していることを認定要件とした。ご指摘のように担当者の経験等によるものも大きいとは思うが、どのような人を配置するのかというのは事業所の判断によるものであり、それを基準に盛り込むことは難しい面もあって、人の対応というよりも制度の整備という観点で捉え、全体としてわかりやすい制度の構築を行っている。一方で、法令違反があれば認定を取り消されることもあるので、事業所にとってより慎重な対応が求められることにはなると思うし、更新時のインセンティブとして法令違反の有無により審査体制が異なってくるという制度を導入している。（METI）

・p15,p23　事業者自身が最適と考える方法で法令遵守体制の整備を進めることが重要とあるが、事業者と行政の判断に隔たりがある場合はどうなるか。（自治体）

⇒p15 と p23 とでは多少意味合いが違うので、別々に考えた方が良い。p15 については、複層チェックにはいろいろなやり方があると思うので、これについては事業者が最適と考える方法を採用すれば良いと考える。ただし、法令違反が起きた場合には、その結果として事業所の判断に誤りがあれば、認定取消に繋がることもあるので、事業所は慎重な判断が求められる。一方、p23 は、認定の特例として柔軟な保安人員の配置を認めようというものであり、これからの技術進歩に合わせたものにするためには、法律に技術的な要件を規定するのではなく、その要件を省令に委任する方式にするための措置として設けたものである。よって現時点で具体的な事例を想定して設けたものでなく、今後事業者から具体的に要望が出てくれば個別具体的に判断をすることになる。（METI）

・ｐ21　継続的に PDCA サイクルを廻すため、あえて課題点を残している事業所もあるという話も聞いたことがあり、これでは方向性が間違っている気がする。PDCA サイクルを廻すことに重きを置きすぎるのも問題はないか、（自治体）

⇒ご指摘はごもっともではあるが、ある意味サイバーセキュリティについては新しい取り組みであり、これからもまだまだ進歩が必要で、完成された世界ではないという認識。PDCA サイクルを廻すために課題を積み残すという考え方はあり得ないのではないか。（KHK）

・資料①P12　法適合性確認能力とは、法令遵守、保安の観点で重要な能力と考える。一方で、許認可手続きにおける事業者との接触からは、事業者にとってこれらを適切に具備することは難しいのではないかと考えるが、審査時の適否の判断基準はどのように考えるか。（自治体）

⇒今般新たに明確化したコンプライアンス体制（複層的なチェック体制等）の要件を満たすことの他、認定取消の厳格な処分基準を併せて考えている。認定制度の特例等も分かりやすくし、違反が発生しにくい制度設計も重要と考える。(METI)

・法適合性確認能力とは、法律そのものの他、材料、設備等の例示基準への適合の判断等、技術的知見も必要である。認定事業所が変更工事を行う際に、事後届出や記録保存で処理する工事は、原則、行政と協議することなく進めるのか。(自治体)

⇒将来的に事業所で判断可能となるとかもしれないが、行政とコミュニケーションをとることが必要と考える他、コンプライアンス体制に係る要件については適否を慎重に判断することが必要である。(METI)

・行政側では人員要求の際に、事務の有無が重要であり、事前相談は事務としてカウントされないことから、人員が削減されてしまうことが課題である。(自治体)

⇒データ活用による手続きの効率化も検討したい。(METI)

⇒許可申請に係る手数料収入が減少すると、行政側の人員が削減される。軽微変更届出について、これまでは事前相談で不備を是正指導していたこと、指摘事項のない申請は少ないことから、許可⇒事後届出に簡素化される変更工事があると、人員不足から関係書類をこれまでのように充分審査する時間が確保できず、技術基準の違反が発生するものと思慮。立入検査を行い、最悪の場合は違反として処理することになるし、保安に懸念が生じる。法適合性能力は厳格に審査頂きたい。(自治体)

・資料①P16　老朽化への対応　発災時に LP ガスの漏洩をバルブ閉止により止めようと試みたが固着により止まらない等の事案があるので、そのような不適切な設備がないか確認して頂きたい。新たな技術導入により事態を覚知できること等を要件として頂きたい。(自治体)

⇒そういうリスク日常点検や法定検査により拾い上げなければならない。必要なものには予算をとって対策すべきである。(KHK)

・認定要件にあるコンプライアンスの要件であるが、現状の認定制度とは大きく異なってくるのか？ (自治体)

⇒基本的には、現行制度の要件と大きく異なるものではない。(KHK)

・重大・悪質な法令違反とはどのようなものを指すのか (自治体)

⇒何が重大なのかについては、出てきた事例毎に判断することになるが、組織的隠蔽等が考えられる。(METI)

・新認定制度でインセンティブが広がるということは、取消要件についても、より厳にするべきと思われるが？ (自治体)

⇒現行の制度においても重大・悪質な違反があれば認定取消が可能な体制となっており、新認定制度においても取消要件の考え方を大きく変えるつもりはない。ただし、あまりふわっとしていると困るので、立入検査を活用するなど緊張感を伴った制度にしたいと考えている。(METI)

・保安の確保に資するテクノロジーの活用状況は、判断基準が難しいのではないかと思うが、具体的にはどのように考えているか？ (自治体)

⇒ご指摘のとおり難しい面もあるので、数値で○○以上ないとだめとかの判断基準を考えているわけではない。会社としての意思決定判断に繋がっていくものなので、会社トップとしてリソース配分をコミットメントしていることを何らかの形で示して貰うことが必要と考えている。(METI)

・取消要件の「緊急時即時通報連絡が行われなかった時」(資料 P15) とはどのようなことを想定しているのか。単に連絡が遅れただけで認定取消は少し厳しく感じる。(自治体)

⇒本表現は、現行通達にもあるものであり、その考え方自体を変えるものではない。先の四国で発生した取消事例では、法令違反をしていたことが取り消し事由となっていたのだが、「緊急時即時通報連絡が行われなかったとき等」の“等”に含まれるものと解しており、いろいろな状況をすべて列挙することはできないので、あくまでも保安体制に重大な不備があったかどうかが判断基準となると考える。なお、過去の事例を見ても単に通報がなかったからという事由で取消しとなったものはなく、事故が発生したとか、記録の改竄が行われていたということで、保安体制に重大な不備があったとされているようである。(METI)

・サイバーセキュリティ対策については、行政的には直接関係の薄い世界の話でもあり、戸惑いもある。具体的には、事業者は既にサイバーセキュリティ対策の仕組みを構築して実行しておく必要があるのか、それとも構想段階で良いのか。(自治体)

⇒ご指摘の点はそのとおり。基本は各業界のサイバーセキュリティのガイドラインに沿っていることを確認することが基本姿勢であるが、ガイドラインが努力義務の域を超えていないことや、認定事業所の中には、サイバーセキュリティ基本法の対象となる重要インフラに該当しない業界の事業所もあることから、認定要件としてどこまで義務を課すか考慮する必要もあって検討してきた。結果として、サイバーセキュリティ対策は必要であり、PDCA はしっかり廻して貰いたいが、初回の認定審査時には一定の配慮を講じるということにしている。(資料 p21) (METI)

・認定の取消要件にある法令違反の考え方はどうなるか (自治体)

⇒認定の取消要件については、資料 P15 にまとめたように保安体制に重大な不備が認められたときということになるとは思うが、個々の事例で判断をせざるを得ないと考える (METI)

⇒当該制度で、都道府県の関与が薄まる分、厳しく対応する必要があると考える。(KHK)

⇒軽い事故でも多発・連発するような事業所は体制に問題があり、会社の認識を改めさせる必要があると思う。(自治体)

5．新たな認定制度の特例

・P25 新たな認定制度の特例について、許可と軽微な変更が３つに分かれるが、軽微変更は様式に基づいて提出していたが、事後の届出についても新たに様式を作成されるのか。(自治体)

⇒事後届出の様式は新しく作成する。(METI)

・処理能力の変更が一定の範囲内の変更とは、どこを基準と考えるのか。設備ごとか、施設ごとか、事業所ごとなのか。(自治体)

⇒完成検査不要の工事と同じなので設備ごとである。告示記載の考え方と同じ。(KHK)

・重要な工事、軽微な工事とその他の工事は省令等に列挙するとともに通達で明らかになるということだが、現在都道府県ごとに詳細については異なる運用をしている旨コンビナート会議等で話を伺っているが、認定に関しては一律の基準になっていくという認識でよいか。(自治体)

⇒自治体ごとに対応の差があるところはなるべく解釈を明らかにしていき、大きな差異がないようにしていくが、通達で全てを明らかにすることは難しいので、細かい運用の差異が生じてしまうことは考えられるが、大きな差異は法令違反を招くのでそれは避けられるよう国として工夫をしていきたい。(METI)

・他の都道府県との判定の違いは一律国に相談していくのか。又は都道府県で運用するのか。(自治体)

⇒明確に方向性が決まっていない。具体的にどの点が異なる点なのかを明らかにしていく必要がある。可能な限り明らかにしていくが、それでも埋められない部分はどんな違いがあるのかを明らかにしないといけない。何が原因なのか、場合によっては一律化、一本化することが可能なのかを丁寧に議論していかないといけない。もし運用の中に何らかの背景があるということなら、時間をかけて丁寧な議論が必要と考える。そういった中で国が全部決めて

いくこともやり方の一つだが、できる限り埋めていきたい。(METI)
・県特有かもしれないが、経験のない職員が配属されると、認定事業者がいうのであればという判断をしてしまうこともあるかもしれないので、各都道府県で差異がないように AB 認定は一律の判断がよいと思う。質問されたときの窓口も検討してほしい。(自治体) ⇒KHK も相談を受けている。水素スタンドの運用方針統一の仕事もしている。国と並んで KHK にも遠慮なくご相談いただければと思う。この県はこのように運用といった内容を調べてご提示することは可能と思うが、最終的には地方自治体の権限でやっていると思うので、強制は難しい。(KHK)
・そういった質問が都道府県から KHK や METI に連絡があって、どのように回答した、どのような根拠で回答したかという一覧、検索できるものがあると重複する質問もなくなると思うし、判断もしやすくなる。そういったものはあるのか。(自治体) ⇒統一的に受け取ったものを整理する形にはなっていない。基本的にはお問い合わせいただくことになる。多い事例があれば統一的な手当てが必要ではないかと思うので国とも相談して、そういった形で整理していくことはありうる。(KHK) ・調べられるところがあると迅速な判断ができるし、同じ質問もなくなると思う。あると便利かと思うのでご検討いただきたいと思う。(自治体)
・資料２の軽微な変更の工事の拡大については認定事業者のみか。(自治体) ⇒認定事業者を対象にしたもの。新認定制度に限らず現行の認定事業者に対しても拡大することを予定している。(METI)
・コンビ則第１４条の後半の号に書かれているような形で認定事業所、スーパー認定事業者は軽微な変更となるという認識でよいか。(自治体) ⇒そのとおり。ただし、一部のものは通達に書く形になると思う。(METI)
・今後新認定制度の場合、ほとんどのものが記録保存となり、都道府県にでてこないが、何らかの確認する方法があるのか。または確認せずに事業所に委ねることになるのか。(自治体) ⇒記録保存の方法としてはある程度基準を示していこうと思う。(METI) ⇒その確認は認定更新の現地調査とか、中間立入でサンプル的に基準に従った記録が確保されているところを、電子保存であれば画面等により、ある程度ランダムに確認していくというのもやり方としてはあると思う。(METI)
・軽微な変更、設備ごと２０%以内の変更なら都道府県に届出はなく、中間立入の際や更新時に情報を得ない限り出てこないということでよいか。(自治体) ⇒そのとおり。(METI)
・中間立入や更新の際に、記録保存のリストを提出していただくことは可能か。特定変更工事以外は何もわからない。特定変更工事も許可を出しただけで、いつ完成した、技術上の基準にどう適合したのかが確認できないというのが、(都道府県にとって)宙ぶらりんの状態になるのかと懸念するところ。(自治体) ⇒許可対象の特定変更工事と事後届対象の工事は都道府県に提出される。処理量２０%以内であっても、処理能力の変更は記録保存にしないので、事後届以上となる。定期的な内容の報告等は手当されていないので、自治体が確認したいのですがということにとどまると思う。工事の一覧を提出するような手当する予定はない。(KHK)
・資料３の一番上の許可については、完成検査の結果は各都道府県にでてこないのか。(自治体) ⇒そのとおり（KHK)
・今までだと届出がでてきたが、許可したものがどうなったか把握できない状況になるが。(自治体) ⇒制度上はそのとおり。制度的には許可したものが許可どおり完成検査をしたのか事業所にお任せし、その記録が確認できるようにしていただくようになっている。許可したものが完成したのかは制度的に（都道府県は）把握できない。(KHK)
・特定変更工事は大きな工事に該当するので、(完成検査の記録は）記録保存ではなく運転開始後の事後届も可能であったと思うが記録保存にした理由は。(自治体) ⇒そういう指摘もあったかもしれないが、一昨年の議論では伺っていなかった。(METI)
・都道府県からすると許可を出すが、宙ぶらりんとなるので、必要に応じて報告徴収を各都道府県としてかけるということになるのか。(自治体) ⇒事故防止の観点からそのようなやり方もありうる。(METI)
・今回、記録保存という制度ができる。変更許可申請は必要だが、完成検査不要の場合には記録保存というものもできる。記録保存でも構わないが、この場合、許可をした自治体側では当該工事はいつ終了したか把握できないので、何らかの形で連絡を入れて頂ければありがたい。前回申請の工事が終了しているのかどうか判らない状態で、次の申請がくるというのは自治体としては心配である。(自治体) ⇒制度として手当てしていない。自治体の運用としてそのようなことが可能かどうか確認する必要はあるが、ご要望としてそのような指摘があったと言うことは承っておく。(METI)
・変更工事許認可手続きについて、付属機器類、液面計流量計、圧力計の材質変更等細かな変更が、許可、事後届出、軽微変更等判断ができるような規定になるか。(自治体) ⇒軽微変更と重要な変更は例示列挙し、それ以外の工事は事後届になる。それ以外は、事後届になる。(KHK)
・資料①P24　軽微変更の様式では工事完了日の欄がないため、工事完了から届出までに何日を要したのか確認できない。法適合性確認能力を求めていることからも、それらが確認できる様式とするべき。(自治体) ⇒拝承。手続きの電子化等把握のしやすさも併せて検討する。(METI)
・資料③最下段　上記以外の工事の具体的なものは何か。(自治体) ⇒撤去の工事だけであるが、処理能力の変更を伴わないもの以外を想定。(KHK)
・資料①P25　許可が事後届出になる工事がある。届出受理以降に不備が見つかると是正が大変であるため、規定を分かりやすくして頂きたい。法適合性確認能力としてこれらの振分けが適切にできるかの確認は要件か？（自治体） ⇒振分ける能力を直接審査するわけではないが、分かりやすい制度、チェック体制等を求める制度設計とし、周知、オンデマンドを含む研修の活用等、多方面での工夫が必要と考える。(METI)
・法 74 条により公安委員会への通報。施行令１７条で報告案件が決まっているが、事後届け出は何条に基づくのか？（自治体） ⇒特例の事後届けでは５条の事務ではなく別に規定される予定。(KHK) **・細かい工事（７号の２）も適切に分類できるように、省令、通達等で明確にして頂きたい。(自治体)**
・省令、通達に書き切れない工事が想定されるため、重要な変更、軽微な変更等の根本の考え方を示して頂けると運用しやすい。(自治体)

・記録保存された記録類は立入検査時に確認するのか。（自治体） ⇒そのとおり。中間立入、自治体の立入時に抜き打ちで確認頂くことを想定している。（METI）
・資料③事後届の根拠は、法第１４条に基づくか。（自治体） ⇒法第１４条とは別で、認定事業所の改正法に基づく事務となる。（METI）
・柔軟な人員配置について、大臣が認める場合とは、認定の審査の際に併せて審議するのか。それとも認定取得とは別に手続きが必要となるのか（自治体） ⇒制度的には別なものにはなるが、具体的な運用方法は現時点で確定していない。実態運用としては、認定審査の際に一緒に審議することもあり得ると思うが、認定審査には時間的制約もあるので、そのようなことが可能かどうかの議論をしたわけではない。具体的要望が出てきた時点で検討することとしたい。（METI）
・軽微変更の考え方が変わり、対象範囲の判断を事業所に任せる部分が出てくるかと思うが、もしも事業所と行政との見解が異なれば、結果的に無許可変更事例が出てくることも考えられるが、その場合の責任はどうなるのか（自治体） ⇒対象範囲の判断等は最終的には行政すべき問題ではあるが、まずは制度的に対象範囲を明確にし、見解の相違が起きないようにすることが重要と考える。今回は、許可・届出の区分を従来の 2 区分から 3 区分に変えようとしているが、許可が必要となる重要な変更工事及び記録保存に移行する軽微な変更工事の範囲を具体的に明確化することで、それ以外の工事を事後届出が必要な工事とする考え方で整理している。どうしてもグレーゾーンは残るかもしれないが、これまでの事例を見ても故意な事故隠しは別として、事業者が独自の考えのみで突っ走るとも考えにくく、事前に行政側に相談があるとは思うが、国としても適宜説明会の開催等、なるべく明確化を図りたい。（METI）
・資料②　現行は、通達のみで軽微変更を定めているものがある。今後省令の改正を行うと思うので、今後は通達のみで規定するやり方は止めて欲しい。（自治体） ⇒他の自治体からも同様な指摘、要望があるので整理したい。（METI）
・P25 について、重要な変更な工事は特定変更工事で、その他は事後届となり、処理能力が２０%以内の工事というのがあるが、処理能力の変更と特定変更工事（２０%以内であれば）があるがそれはその他の工事に該当するのか。（自治体） ⇒２０%以内の工事が全てその他の変更の工事となるわけではない。現在の完成検査不要工事は取替え等、別途条件がある。それもこの条件がかかる。（KHK）
・重要な変更工事＝特定変更工事だと、ほとんどの変更許可はかわらないと思うが特定変更工事以外で県に出てくる変更許可は特定設備の取り替えなどしかなくて、あまり事業所のメリットとならないのではないか。ちょっとした配管改造もスーパー認定でなければ重要な変更工事になるかと思う。（自治体） ⇒これを検討する際に複雑な場合分けがあるとわかりにくいので、基本的な考え方として許可と事後届の境目を P26 にある完成検査必要工事と不要と分類したので、今の特定変更工事とくらべて大きく変わらないというのはご意見のとおり。（KHK） ・2 年前に METI の課長からお伺いしたときはもう少し広がるのかなと思っていたので、広がらないのであれば我々としては良いのかなと思う。確認がよくできるので。（自治体）
・特定変更工事の定義は、認定事業者以外にとっては現行と変わらないと思うが、認定事業者は法令で定義されるのか、又は省令等で定義されるのか。（自治体） ⇒基本的には特定変更工事の定義は変えるつもりはなく現行法上の定義のまま、認定事業者に適用される。（METI）
・軽微変更についても、認定事業者以外はかわらないと思うが、認定事業者に限定される旨はどこに定義されるのか。（自治体） ⇒基本的に軽微な変更の工事の範囲は、省令に規定する予定。一部は通達で詳細をお示しする。（METI）
・定期自主検査の話であるが、定期自主検査について認定事業者は不要とあり、現在の検査組織は検査しないが、検査管理組織が全てを検査するというイメージか。（自治体） ⇒保安検査に対する検査組織と検査管理組織の関与は変わらず、自主検査の義務だけが除かれている。自主検査と保安検査の範囲が違うので、そこは認定要件のなかで引き続きフォローしていくという方針として記載されている。検査管理組織が見ないというのはあくまで検査管理組織と検査組織は保安検査のための組織であり、定期自主検査のデータを保安検査に流用するということはあったが、保安検査に対する検査組織、検査管理組織の関わりはかわらないと理解している。（KHK）
・事業所によっては一部の製造施設を県の保安検査の対象としていて、すべてを認定保安検査としていない事業所があるが、新しい制度でもそのようにできるのか。そうなると定期自主検査をしない事業者に対して、今、県の保安検査は定期自主検査に立ち会うとか定期自主検査の記録を見て保安検査を実施することになっている。県自体が保安検査を実施することになると、そのような予算を持っていないので開放検査の費用等どうなるのか教えていただきたい。（自治体） ⇒法律上は事業所認定となっているが、製造施設は申請の中で選択するような形を予定している。このためそこに上がっていない製造施設は、認定のメリットは享受できない形になる。もともと認定要件を満たすのが難しいとかそこまでメリットを感じないという製造施設もある。もちろん全部認定対象としている事業所もある。その部分は引き続き選べる形で残すよう省令以下で手当てする予定。（KHK） ・残った施設については定期自主検査を法令どおり実施すると理解した。（自治体）
・（「本日意見交換させていただきたい事項」の３ポツ目２．の）3 番目の解釈を国から示す場合の取り扱いだが、遵守はしていこうと思うが、示される前の案の段階で意見なり、確認させていただけると意見を言いやすいが、正式に決まってからだと言いにくいので、事前に示していただけるとありがたい。（自治体）
・その他の変更について、先ほどの質問で、その他の変更が少ないのであればよいが、すごく増えると予想していたので、すごく増える場合の懸念として、現在でも事前に法令違反、間違いがないか県に事前に相談される場合が多々ある。これが事後届け出となると、法令にあっていないとなると設備を止めてやり直さなければならない場合もありし、法令違反と言われてしまうこともあり、事業者にとってはリスクが増えるのではないかと思う。先ほど認定の更新の要件でも法令違反を問題にするという話もあったので、事業者はますます県に対して事前に確認してほしいといってくる可能性がある。事後届となっている部分を事業者によっては、事前に出して県に見てもらえないかと考える事業者もあると思うので、事前にも届出できる制度はないのかと思った。（意見として）（自治体）
・記録保存はどこかのタイミングで確認するのか。（自治体）

⇒一つは認定更新のとき。その他は認定期間の期中の立入検査で確認するやり方がある。その他は制度を運用してから考えさせていただきたい。その中で保存されているのかは見させていただくことになるかと思う。(METI)
・軽微変更に関連し、特定変更工事は許可で、現行では現場溶接加工等を伴うものは完成検査の対象となっているが、新制度ではその他変更の事後届出ということになるのか。(自治体) ⇒重要な変更として省令に位置付けられれば許可となるが、それに該当しない場合には、その他の変更として事故届という扱いになる。(KHK)
・軽微変更が記録保存となると自治体は把握できなくなる。これまでであれば、明確な判断が難しい場合には事前相談等があり、その場で指導することもあったが、今後はその判断に行政が関与せず、事業所に委ねることになるという不安はある。(自治体) ⇒認定要件のひとつとして、法適合確認能力を有することを求めており、事業所側できちんと判断できる仕組みがあるので、事業所の判断に委ねることで問題はないと思うが、今後も行政に対するその種の相談はあるとは思うので、引き続きご対応願えればと思う。(KHK) ⇒一方で、その手の相談がいくら出てきても自治体として、人員要求のための工数にはカウントできないので、事務負担のみが増えるという悩みもある。(自治体)
・自治体による対応の違いについては、これまでもブロック会議等で検討してきているが、必ずしも統一的見解が示されないケースもあるので、その点は新認定制度が導入されることによって何か変わるものなのか気になっている。(自治体) ⇒その点については、新認定制度導入により自治体の自治事務の範囲が変わるものではないので、従来どおり自治体の判断が必要になってくると思われる。ご指摘のとおり地域格差がなくなることが理想であり、また、事業所側からも同様の要望も出ているので、その辺を中心に見直していきたいと考えている。(METI) ⇒今回参考に明示したプラグ打ちの扱いなどが比較的簡単に統一できそうな案件ではあるが、必ずしも結論の出にくいものや認定制度内の議論だけでは収まらないものあるので、時間を掛けて調整する必要があろう。(KHK)
・現行制度と新制度では軽微変更の考え方が異なってくるが、両制度が併存する期間はそれぞれ別の運用をすることになるのか（自治体） ⇒省令の書きぶりにもよる。現行の軽微変更工事の範囲は、コンビ則 14 条に規定しているが、同条の規定を変更する場合には、現行制度及び新制度の両方に影響することになり、軽微変更についてはそういう視点での見直しも行うことになると思うが、新制度だけに適用したい部分もあり、これに対しては、現状別の条文で規定する予定であり、この場合には現行制度の運用と新制度での運用が異なってくることもあると思う。(KHK) ⇒軽微変更の考え方は自治体によって異なっている面があるので、できるだけ統一できるような制度の構築を期待する。(自治体)
・定期自主検査義務が廃止されることにより、検査組織、検査管理組織との関係に弊害が出るおそれはないか（自治体） ⇒もともと定期自主検査は、保安係員の管理下で自主的に行う検査であり、検査組織、検査管理組織が関係するのは保安検査であるため、混乱は起きないものと考える。現行制度でも言えることではあるが、認定事業所の場合、保安検査も定期自主検査も事業者自らの責任で行う制度となっており、検査内容の重複があることから、今回この点を整理したものである。(KHK)
・CBM、常時監視という技術活用状況を踏まえ、保安検査周期を柔軟化したいという説明があった。設備対応的としてはこれで問題ないのかとは思うが、認定事業所が大きな組織の場合、関係者間での情報共有が必ずしも十分でなく、事業所として上手く機能しなくなっているおそれもあるので、この点についても国、KHK の調査でしっかりと調査して欲しい。(自治体) ⇒保安検査周期の柔軟化については、今後のテクノロジーの進展を踏まえて検討していく予定であり、認定の手続きとは別に大臣が問題ないと認める場合に限り適用する予定としている。ご懸念の点も踏まえて検討したい。(METI)
・定期自主検査の廃止は、認定事業者としての義務として担保するものであり、制度的に手当てできているので廃止したという認識でよいか。(自治体) ⇒その理解で問題ない。(METI)
・資料 p25、新認定制度では変更の許可・届出の区分を従来の 2 区分（許可、事故届）から 3 区分（許可、事後届出、記録保存）に変更となるようであるが、軽微変更の考え方というのは認定事業所以外の事業所でも用いられている概念なので、届出書の名称等で混乱が起きないよう配慮願いたい。(自治体) ⇒新制度でのその他変更の事後届出書の名称については検討する。(METI) ・認定事業所であっても、非認定プラントの取扱いについては、従来どおりの取扱いとなるので、事業所に誤解させないよう配慮願いたい。(自治体)
・軽微変更の範囲拡大については、認定事業所のみ追加する事項という理解で良いか（自治体） ⇒基本的にはそのとおり。(KHK)
・設計条件を超える変更の事例の取扱いが一覧表に許可事項として記載されている。かなりレアケースではあるが、この場合は許可が必要となる事例との判断から一覧表に記載したとの説明があったが、工事を伴うものではなく、強度設計をやり直して肉厚に余裕がある設備の設計条件を変更したいというケースにおいて、県では、経年した設備の材質の保証が難しいこともあり、現状ではこのような事例は変更を認めておらず、設備の更新を指導している。これが出ると混乱を招く恐れがあるので、レアケースであれば一覧表に載せず、各自治体の判断に委ねて貰いたい。(自治体) ⇒この記載がないとこの強度計算をやり直す場合（再定格）が、事後届出と判断されるおそれがあることから記載したものだが、ご指摘の点も踏まえて表現方法については検討することとしたい。(KHK)
・記録保存については、行政側も確認できるとのことであるが、イメージが湧かない。例示とか示す予定はあるか。例えばいつでも行政側で見ることができるようになるのか。(自治体) ⇒記録保存すべき項目については、省令で示す予定である。クラウドへの保存は、事業者が自社のサーバーを用意すること難しい場合も考えられるため、外部のサーバーの利用を想定し、そのための要件を規定しようとするものであるが、行政側がいつでも自由にアクセスできることを想定したものではない。(METI)
・記録保存の様式を定めるのか？（自治体） ⇒いろいろな保存形式が考えられることもあり、記録保存の様式まで定めることは考えていない。ただし、技術基準で求められている事項等記録すべき事項を規定することは必要と考える。(KHK) ⇒記録を確認する側からすれば、様式が定めてあった方が便利ではある。(自治体)
・先ほどの、認定事業所と認定施設との関係について、認定施設かどうかで受けるインセンティブが違うことを明確に書き分けておく必要があるのではないか。(自治体) ⇒ご指摘は理解した。法律の中で認定の条件を規定する項目があるので、それを受けて定める省令の中で、認定施設に限定する縛りを掛けることになる

と考える。(METI)
・認定事業所は、危害予防規程の作成も任意となるのか？（自治体） ⇒危害予防規程の作成義務は残る。(METI)
・今回、重要な変更、その他の変更、軽微な変更の 3 区分に分かれることになるが、重要な変更と軽微な変更の事例を具体的列挙することで、それ以外のものはその他の変更になるという考え方でよいか？（自治体） ⇒そのとおりである。(METI)
6．新たな認定制度の審査体制
・P34 更新時に国によるしっかりした現地調査をするのか、簡素化かといった内容における労災の有無等について、事故の取り扱いについては事故対策要領を出していただいているところだが、事業所との認識に差があった場合、例えば C 級の事故を届けていなかったが、後々出てきたといった、遅れて出てきたことに関するペナルティはあるのか。（自治体） ⇒更新の申請のタイミングでは明らかになっていなかったが、直近 5 年間遡ることにより結果的に C1 が 1 年経過していないときに、C1 が発生したため B2 になるようなケースが事後にわかった場合の扱いについての質問だと理解した。どのタイミングで判明したか次第ではあるが、審査が滞りなく進むよう実務上の運用を工夫する必要がある。一つのやり方は、認定更新審査時にはその時点で明らかになっている情報に基づいて基準に該当するか否かを判断するが、事後的に B2 事故の発生が明らかになり、本来であれば現地調査、審査会をしなければならなかったことが判明すれば、その次の更新審査時に考慮することとする等、判断の基準日を設けていくことが考えられる。今の認定制度においても、更新後に違反が見つかったということもあるので、基本的にはこれまでの考え方と整合的に行っていく。事後的に判明した場合には次回以降の審査に反映させていく。(METI)
・次回以降ということで、C 級の後に C 級が起こっていたということに対するペナルティはないか。（自治体） ⇒ペナルティという観点から言えば、事故届漏れについては、法令違反に対する対応として自治体からの処分があるのではないかと思う。国は事実認定をしたうえで、認定基準を踏まえて、法令違反への対応をする。これは事故の話だけではなく、法令違反の有無という点にもかかわる。故意に隠していたといった悪質性がある場合は文書による厳重注意をするとか、何らかの処分につながるので、基本的にはペナルティは課されるし、審査のフローでも考慮される。法令違反が判明したタイミングでその時にとれる対応をしていく。隠していればより重いペナルティが課されていく。(METI) ⇒補足すると、認定要件の法適合確認能力に加えて、法令違反を覚知した場合は通報するようになるので、覚知した段階で通報しなかった場合は認定基準で定められている通報を怠ったことになり、認定基準に照らし合わせて事業所の対応としてどうかということになるし、重大な法令違反、組織的隠ぺいに該当する場合は取消に該当する形で通達に明記する方針が示されているので、隠すということに対するインセンティブが働かないような形の工夫がされていると考えている。(KHK)
・新たな現地調査の体制について聞きたい。資料では国と KHK が実施するとなっており、自治体の関与については読み取れなかったが、本日の説明の中で自治体の参加も求められていると理解した。現行制度では現地調査は KHK が主体となって実施しており、自治体は委員として参加し、国が参加する場合はオブザーバーという位置付けとの認識でいるが、新制度においては、国が主体となって現地調査を行うという理解で良いか。（自治体） ⇒現行制度及び新制度における現地調査の体制についてはご理解のとおりである。新制度においては、国による審査という全体スキームの中において、KHK 等への調査依頼制度を活用して審査を行うことを考えており、国から調査依頼を行うのは KHK 等となるので、国から直接自治体へ調査依頼を行う制度とはなっていない。しかし、自治体の関与を排除しようというものではなく、情報は全て共有させて頂くつもりであるし、現地調査及び審査会審査においてもオブザーバーという立場でご参加頂きたいと考えている。なお、ご指摘のとおり配布資料からは読み取りにくい部分があるので、今後資料を見直す際には修正したい。(METI)
・p34 更新時の現地調査の実施基準について、B2 事故が発生している場合には現地調査が必要となっている。厳しく臨むという制度設計なのかもしれないが、感覚的に少し厳しいのかなと感じる。ヒアリングでの更新となる場合は少ないのではないか。（自治体） ⇒厳しいのではという感覚は理解するが、B2 事故は、繰り返し事故が発生しているということであり、このような事業所は慎重に調査せざるをえないと考えている。B 2 事故があった場合に認定更新できないということではない。(METI)
・手数料の流れについて、現行制度において実態上は KHK への事前申請と国への本申請と 2 度手数料を納付する仕組みとなっているが、新制度においては、国に 1 度手数料を納付することになるのか。（自治体） ⇒そのとおり。事業者は国に納付すればよく、KHK へは国から必要費用を支払うとうい流れになる。(METI) ・現行制度で KHK の現地調査に県職員も同行させて頂いている。県が事業所へ立入検査をする際の参考となることも多いので、新制度においても可能であれば引き続き参加したいと考えているが、一方で人員減による職員の負担増を考えるとなかなか経験を積ませることも難しくなっている面もあって複雑である。(自治体)
・現地調査、審査会審査の体制について、現行制度では、学識経験者には審査会だけでなく、現地調査にも参加頂いている状況であるが、新制度においては、現地調査は国、KHK 等が主体で、学識経験者は審査会審査に第三者的立場の委員として参加するというスタイルになるということか。（自治体） ⇒ご理解のとおり。現地調査は国、KHK が主体となり、審査基準も審査の要領、視点を公開して実施することを考えている。よって、審査基準に合致しているかどうかを確認する作業が中心となり、現行の現地調査の 1 日目のようなプレゼンを実施することは考えていない。審査会審査の場で、KHK、国からの報告に対して、学識経験者からのアドバイス、コメントを頂くことになる。なお、審査会自体を公開する予定はないが、結果については企業の機微情報を除いた上で議事要旨を公開する予定である。(METI)
・資料①P31　下　労安法も含めて審査するが、実績は事業者からの申告か、行政間の情報共有によるか。（自治体） ⇒事業者の申告による情報で審査する。コンプライアンス体制の要件を強化したほか、虚偽報告に対する罰則措置も存在するため、虚偽申告は抑止できるものと考える。(METI)
・現地調査を行う指定機関は KHK 以外にあるか。（自治体） ⇒サイバー関係の審査機関が KHK の再委託先となる可能性がある。(METI)
・県の立場は調査委員会の委員であったものがオブザーバーとなるが、これまでは意見や採点に参加していたが、オブザーバー参加となると立場が下がるというか、意見を言えなくなるのか。（自治体） ⇒現行制度では、P30 のフロー図のとおり、KHK の事前調査の中で現地調査や調査委員会にご参加いただいていたと認識している。新制度では、法律上、国による責任の下、国から KHK 又は指定機関に調査を依頼するという仕組みになっており国から県に依頼する形にはなっていない運用の中で、自治体の参加を確保していくためには、資料に記載はないが、現地調査等に同席いただいて、場合によっては質疑していただいても差し支えないと考えて

いるが、基本は国から調査を依頼されているということではない。調査への関与がご負担となるのか、むしろ積極的にご参加されたいのか次第だが、、これまでボランタリーにご参加いただいていたように、今後もそのような機会、資料を共有させていただくということが一つの考え方ではないかと思う。それでは立場が弱いということであれば、そこはご意見としていただければありがたい。調査への関与を強く求められる自治体はこれまで（今回８カ所目）いなかったが、県に立地されている事業所という観点においては、もっと踏み込んだ立場で参加されたいということであれば、そうおっしゃっていただければと思う。(METI)
・オブザーバー参加は、参加しなくてもいいのか。（自治体） ⇒お名前を指定しての参加ではなく、県としてどなたか参加していただくという考え方かと思っている。そのうえで参加できないというのであれば、それも一つの判断と思っている。とはいっても議事録とかどういったやり取りがあったのかそういったところは共有させていただきたいと思っているし、資料自体も共有させていただく。(METI)
・今の審査会審査はオブザーバー参加の場合、WEB 参加可能か。（自治体） ⇒基本的に審査会審査は WEB 開催を考えている。場合によってはハイブリッドの可能性もある。オンラインで参加する方法は確保させていただきたい。（METI）
・現地調査について、現在３日間の予定で KHK がしているが、新制度のスケジュールはどうか。１日目の専門家の審査は続けるのか。（自治体） ⇒専門家へのプレゼンはやめる方向で考えている。基本的には審査プロセスの合理化というコンセプトがあり、認定要件に加えて、審査の基準を明確化していきたい。審査基準では、何を見るのかとどのような資料を確認するのか、ということを公表する。基準が陳腐化すれば必要に応じて随時見直しする。実際の審査では、提出いただいた認定要件に関する申請書を個々のエビデンスに沿って、認定基準を満たしているのかを確認していく。国、KHK 等で認定要件の適合性を確認する。現地調査では、提出された資料に沿ってポイントで紹介いただくことはあるかもしれないが、現行制度のような外部の専門家の方のためにプレゼンを実施し、翌日から認定要件の適合について確認していくという流れは考えていない。新認定制度の現地調査はおよそ２日と考えている。(METI)
・P34 の現地調査をする要件の案について、事故の B2 事故は仕方ないと思うが、労災の関係は事業所によっては、大きい事業所はそこそこ発生すると思うが、定量的に従業員何千人に何件といった方が良いかと思う。（自治体） ⇒この点は事業者の方からもご指摘をいただいており、休業４か以上の労災だと広すぎないか、高齢化が進む中においては怪我等も多発しており保安と直接的な関係のないものも労災としてカウントしてしまうというのは厳しすぎないか、といった意見もあった。この点については引き続き議論の余地があるが、国会から厳密に審査しなさいと指摘されていることや、この基準をクリアしなければ認定更新されないというものではないこと等を考慮すると、多少厳しめかもしれないというところがありつつも、その中で自主保安に取り組んでいただくという方が新しい制度の初回の運用の中においては望ましいのではないかと思う。また、ここは様々な御意見を頂いているところであるが、悩みながら議論させていただいている。(METI)
・１社１事業所といった小規模な事業所は全部ヒアリングになるのではないか。逆に２０施設あるようなところは毎回現地審査ありになると考えられる。（自治体） ⇒1 事業所個々に見ていくということなので、他に複数の事業所を持たなくても事業所単位の話となる。(METI) ・(「１社２０事業所」と発言したのは「１事業所２０製造施設」という趣旨であり）製造施設の数の話。1 事業所で 20 製造施設あるところと、1 事業所で 1 製造施設のところで違いが出てくる。(自治体) ⇒絶対数にすると、働く人間が多いところは労災の発生確率が上がるが、一方でたくさんの高圧ガス施設を持っているということは、多量の高圧ガスを扱っているということでもあるので、そこはしっかり見るということにつながるのではと思う。1 製造施設を子会社化して 1 事業所となっている場合のおいては、しっかり管理されているのであれば労災も事故も発生しないということなので、審査は簡略化でよいという考え方。大きければ労災が発生しても良いということではないと思うので、大きくてたくさん高圧ガスを持っているということは、もともと保有するリスクが高いということでもあるので､労災とはつながらないが結果としてそうなるのではと考えている｡もちろんその中でこれを達成するのは非常に優良な事業所といえると思う｡(KHK) ・そういう説明ならわかるが、この表現だと事故、労災の数だけで判断されると事業所が危機感を感じると思った。(自治体)
・認定更新が 3 日から 2 日となるが、見る件数は増える。書面審査とヒアリングとなった場合、現地調査ありと比較して、事業者が用意する書類の量・手数料の差は生まれるのか。（自治体） ⇒申請書類は大きく変わらない。手数料は少し考慮して価格差を設ける形になるのかなと思う。詳細は検討中。(METI)
・過去の先生（委員）の意見の中にペーパーワークに力をさくのではなく、現場の保安に力を入れてほしいということがあったが、書類の量は減る方向か。（自治体） ⇒今回の新しい制度では、それぞれの認定要件の審査基準が公表され、事業者は審査基準に沿って申請書類を作成することとなるため、ペーパーワークの数は減ると思う。(METI)
・2 年前に伺ったときは県が機動的な立入検査を行ってほしいという話があったが、そのあたりは省令で規定されるのか、又は今までどおりのスタンスなのか。（自治体） ⇒P36 のとおり。省令で県の取り組みについて規定することは予定しておらず今までの運用のとおりとしていただく。国はこれまでどおり中間立入を実施し、連携も取らせていただくということは従来と変更はない。また、個別事案の中で違反事例が起きれば、皆様方と協力させていただいて、県は自治事務として判断し、国も認定基準に従って何らかの措置が必要かどうかについて判断していく。機動的な立入検査については、適時適切な立入検査と記載している（P36）とおり。(METI)
・新制度での国の認定事業所への立検は行われるのか？その場合はどういうサイクルを考えているか。（自治体） ⇒現行と同様に中間立入検査を実施する予定で有り、そのサイクルとしては、認定期間中に 1 回程度立ち入ることを考えている。 ・行政のサイクルはどの程度か。(自治体) ⇒自治体によってまちまちではあるが、コンビ事業所にあっては、年に 1 回程度（自治体によっては、年 2 回）が一般的かと思う。(KHK)
・新規は審査会審査を行う一方で、更新時に一定の条件を満たすと審査会審査が行われないが、その場合の自治体の関与の仕方は？（自治体） ⇒資料①P34 のとおり書面審査とヒアリングにより更新可能となるが、この場合の基準はある程度厳しいものであろうと考えており、クリアできる事業所は一定程度のレベルが確保できるとも考えている。オンライン会議でヒアリングを行う場合は自治体も同席頂くことで関与して頂きたい。また、書面審査の内容についても共有したい。(METI)
・資料①P34　法令違反の①～④では、国による行政処分は想定されているが、自治体による行政処分は想定していないのか。（自治体）

⇒自治体による行政処分は国に共有され、その過程で認定基準に照らし合わせて、国からも行政処分を行うことになるものと想定している。(METI)

・資料①P34　法令違反の有無について、１００件を超える違反を伴うものの想定があるが、９０件の場合、現地調査、審査会審査を行わないで更新可能であることについて慎重に考えるべきではないか。(自治体)

⇒過去の法令違反の中には、定期修理中に死亡事故が起き同時に法令違反も発覚した事案があり、自治体から処分され、国からは処分を行わなかった。こうした事案は、「①死亡事故が発生したもの」として扱う。また別の事案では、軽微変更届出の対象工事に係る解釈に誤りがあり、結果として１００件を超える法令違反となったが、国からは処分を行わなかった。数だけに着目しているわけではないが、１００件とは象徴的な件数であるため基準とした。また、９０件であっても、その中に１件重大なものがあれば国から処分を行う可能性があるため、基準の③④に該当しうる。(METI)

⇒法適合性能力の担保は重要であり、取り消しにより職員が削減されると、体制が保てないため、本件の審査は慎重に行って頂きたい。(自治体)

・ｐ３３審査会は現行の KHK の認定委員会と同じ位置づけのものか？(自治体)

⇒制度上は新設制度となっているが、現行制度で KHK 内に設置されている認定委員会と同様の機能を持つものである。(METI)

・現行の KHK の委員会では県職員は委員という立場で現地調査にも立会しているが、新制度では、現地調査に立会することになるのか(自治体)

⇒国と KHK との関係では国から KHK に調査依頼をして現地調査を行うことになっているので、県についてはその場にオブザーバーという立場で立会していただくことになる。(METI)

・手数料はどうなるのか(自治体)

⇒詳細については現在検討中であるが、これまで KHK に支払う手数料と国に支払う手数料の２本立てとなっていたが、新制度では国で一本化して徴収する予定である。具体的な額も今後どのような費用が発生するか計算した上で算出することになるが、現行よりも上乗せするという想定はしていないので事業者の負担が増すということにはならないと思う。(METI)

⇒これから積算することになると思うが、要求事項との兼ね合いもあり、そこでどれ位の工数が発生するかを勘案して手数料を決定することになる。(KHK)

・審査会審査の開催基準に労災事故の件数を含めることになるのか。(自治体)

⇒事前のヒアリングの際にご指摘をいただいた事は承知しているが、ある程度客観的基準で運用したいという思いもある。ここの基準をクリアすれば現地調査も審査会審査を省略できるという制度であるが、一方、厳密な審査を行うという観点からは、基準はある程度厳格なものでも仕方がないと考えている。この点については業界側からも声が上がっているところではあるが、この基準に抵触したら更新できないものではないので、これくらい厳しい基準をクリアできる事業所になって貰いたいという思いもあり、保安力を高めるインセンティブとしてほしい。(METI)

・現在の制度では KHK の現地調査に県職員も参加しているが、新制度ではどうなるか？(自治体)

⇒新認定制度では、国が主体となって審査する制度に移行することになる。国と KHK との関係では、調査依頼制度を活用し、書類審査、現地調査を行って上で、審査会審査での報告等技術的項目のサポートをして貰うことになると考えている。その中で、県の皆様には現地調査については差し支えない範囲で参加いただきたいと考えており、また、国の審査会審査においてもオブザーバーとして参加いただきたいと考えている。(METI)

・現行制度では、ABC 評価が行われているが、新制度での審査会審査の評価結果はどのようになるのか？(自治体)

⇒新制度においては、認定基準に適合しているかどうかを判断し、合格、不合格のみを決定するため、ABC 評価を行うは考えていない。(METI)

⇒区分けの是非の議論はいろいろあったが、事業所側の負担になりかねないという意見もあり、新制度では○×評価ということになった。(KHK)

・審査会審査の開催要件にある法令違反の 2 回については、国に上がったものという考え方で良いか？(自治体)

⇒そのとおり。なお、一連のものを 1 回と見なす。(METI)

⇒今回認定基準に通報手順を課しているので、速やかに通報されなければ認定基準に違反していることになると思われる。(KHK)

７．新たな認定制度の認定の更新期間

・A 認定の更新期間が 7 年、B 認定の場合は 5 年となっているが、例えば B 認定であっても、長年事故を起こしていないような事業所については更新期間を延長するような考え方はないのか？(自治体)

⇒更新期間については A 認定が 7 年、B 認定が 5 年としているため、事故を起こしていない事業所に対する期間延長については考えていないが、認定審査の基準で考慮しており、更新時の審査会審査の開催要件に反映されていると考えている。(METI)

８．A 認定事業者向けの特例措置

９．その他

・保安検査、自主検査に関しては KHKS にのっとってやっているが、認定制度がかわったことで KHKS の改定は予定しているのか。(自治体)

⇒KHKS は第一種製造者全てを対象としている。通常認定に関しては告示で定める KHKS 以外の方法も大臣が認める方法としてできる、スーパー認定の方は保安の責任者が適合すると認めるものであればできるようになっている。新制度もその形を引き継ぐ。このため新制度において KHKS を見直すということはない。一方でテクノロジーの活用について、今は解釈でテクノロジーの活用ができることを書いているが、見直しのタイミングで基準に引き上げることは考えている。(KHK)

・認定取消事案が発生し、(他の認定事業所にも) 中間立入で聞いているとのことだが、事故届の定義について法第６３条によると災害が発生した場合に届出となっているが、この災害について定義があるのかという質問を受けたことがあり、KHKS1880-1（第１種製造者 特定の事業所用 危害予防規程の指針）に「災害」の定義がある。これによると「大きい事故又は自然災害により人身、設備等に損傷を及ぼし第三者に脅威を与え、あるいは外部に援助を要請する状態」を災害ということになっているが、事故届でいう災害と KHKS の災害と違うのか。(自治体)

⇒即答できないのでメールで回答する。(KHK)

・マニュアル、要領ができる前はこちらかと思い確認した次第。(自治体)

・今回の認定制度に関して事業所の方が軽微変更であれば記録保存となるが、認定事業所や都道府県をまとめた講習会等で認識を合わせるということは予定しているか。共通認識をもつためには同じ講習会を同時に受けるといったことがよいと思うが。(自治体)

⇒自治体向けの講習会の話か。(METI)

・自治体と認定事業所が講習を一緒に受けることにより法律の認識の差をなくすことになるかと思うが、自治体と事業者向けは分けてやっていくのか。(自治体)

⇒今後の説明会について検討中だが、制度が公布される前の５月、施行前の１０月ごろにそれぞれ説明会をしようと思っている。対象者は自治体、事業者を考えているが、開催の形態は検討していきたい。(METI)

・法律の解釈を一致させるということで、保安係員の法定講習はこれまでは都道府県の職員が法律の講師となっていたが、オンラインとなり機会がなくなった。保安係員の講習に自治体が参加することは可能か。（自治体）

⇒オンライン講習は講習の義務がある方や資格を取得する方を対象としており、自治体の職員が見ることは難しい。KHK は出張講習もしているので、そのようなご要望があれば出張講習、オンライン講習も可能。（KHK）

・講師の機会がなくなったので、講師をするための勉強と、どのように講習しているのか気になった。免許を取っていれば受講は可能か。事業所に所属しないと受講できないのか。（自治体）

⇒資格を取る動機なら受講できる。（KHK）

・認定の取消要件に、「重大・悪質な法令違反」とあるが、具体的に例示する予定はあるか。（自治体）

⇒先般の四国の事例のように、組織的に故意に隠蔽していたような場合が該当するものと思われるが、基本的には、重大・悪質の判断については、ケースバイケースに行うことになると思う。考え方として提示したものである。（METI）

・現在の自主保安高度化事業所はＢ認定となるのか、別の枠となるのか。（自治体）

⇒統合する議論も２年前にあったが、新制度の中ではＢ認定とは別の自主保安高度化については、Ｐ８のピラミッドの図のとおり、引き続きＢ認定とは関係なく、省令で措置する制度として維持していきたい。その上で見直しをして、よりインセンティブを持たせられる制度の見なおしも考えられないかという議論もあるので、引き続き存続するとともに制度の見直しということも考えている。バッジ処理の方に対するインセンティブ措置として、何らかの手当ができないかということで、引き続き存続させていきたいと考えている。（METI）

・P8 の中小企業向けのインセンティブ制度を設ける予定とあるが、具体的なものは。（自治体）

⇒高圧ガス保安室で検討している。法改正ではなく、人がいない、お金がないといった場合に、保安力をどうやって維持していくのかと考えたときに、第三者的な保安のアセスメントを導入することによって保安力を高めるとともに、そういった制度を使うとインセンティブも、例えば開放検査周期が伸びるといったこともできないかということを少し検討していたところではあるが、今この瞬間は近々こういった制度で始める予定ですといったところにはいきついていない。引き続き、全体的な引き上げも必要と考えている。自主保安高度化や別途の措置で手当していきたい。（METI）

・この制度の裾野を広げていくことも必要かと思う。例えば、認定制度取得のためのセミナーの開催や申請のお手伝い事業等はできないか？（自治体）

⇒今回の法令改正に対しての説明会は開催することを考えている。また、現在も認定事業所向けの保安セミナーは毎年開催しており、これらを通じて情報提供はするつもりだが、個々の事業所の申請のお手伝いをすることは依頼調査受ける立場上難しいと思う。（KHK）

・法令遵守等のコンプライアンスの体制については重要な事項と考えている。新制度における審査体制の変更は、従来の事前調査は KHK が行っていたが、新制度の調査は、国が主体的に行うようになったと認識している。調査依頼制度により KHK に依頼する場合には、主に技術的な事項として、法令遵守については、国がしっかりと確認をするということを示すのが、よいのではないか。審査体制について、法令遵守の確保が大切であり、国が直接見る制度として欲しい。（自治体）

・中間立入検査を行う場合、行政にスマート保安等の知識が必要である。以前、「国からも最大限の支援を行う」旨の発言があったが、国による研修等の計画はあるか。（自治体）

⇒毎年４月に研修を行っており、参加者以外にも研修内容が聴講できるよう、KHK とも相談しながらオンデマンドの環境を確保する。（METI）

・自治体が独自に事業所に立入検査を行うことも想定されるが、認定要件の不適合を覚知した場合の対応はどのようすべきか。（自治体）

⇒疑義がある場合は当該事業所に対して、経産省へ届け出るようにご指導頂きたい。場合によっては国と自治体が合同で立入検査を行い、不適合等を判断させて頂きたい。（METI）

１０．事後届の添付資料について（KHK より）

・事後届の位置づけ次第であるが、事後届の場合においても、技術基準に適合していることを確認されるのかお尋ねしたい。（KHK）

⇒軽微変更に関しても技術上の基準をすべて確認しており、強度計算も確認している。過去数件認定品の配管の厚みの記載が違っていたこともあり、許可になっても事後届になっても技術上の基準は全て確認してく方針と考えている。（自治体）

・事後届の場合においても、技術基準に適合していることを確認されるのかお尋ねしたい。（KHK）

⇒現在は、事後届出で問題ないことを確認するために必要な書類を求めているので、届出についても単なる供覧事項でなく、許可事案と同程度の書類をつけ、室長決裁事項としている。たしかにチェック不要とすれば、事務負担が減るとは思うが、現時点では今後どうするかという議論はしていないので現行と同様の運用になるのではないかと思う。（自治体）

・現状、軽微変更の取扱いが自治体によって一部異なっているので、運用統一をして欲しいという希望がある。そうなるとこれまでの自治体の運用方針を変更しなければならなくなることも出てくると思うが、それに対する懸念事項はあるか。（KHK）

⇒特に懸念事項はない。しかるべき所から統一見解が示されれば、自治体としてはそれに従うだけであり、むしろ自治体として判断しなければならない箇所がなくなることを期待する。（自治体）

・届け出に対する事前相談ばかりでは行政側の人員がそろえられないため、届け出の添付書類を簡略化すべきではないかと他の自治体から意見もあるがどうか。（KHK）

⇒届出の目的、何のために届出させるのか。課内で話をしていないが、個人の意見として、届出を受けるからには技術基準のチェックをしなければならないと思う。事後の届出を審査する中で技術基準に適合しないのではないかということがあれば困る。許可と届出で事務負担は変わらないと思う。（自治体）

・そうした中、他の自治体からの意見では、許可ではなく届出になると収入が減ることになるが、人員が減ってしまうかもしれないという懸念のもと、許可相当の審査を事後届にもするのかという意識を持たれている。（KHK）

⇒県で話があったのは、エビデンスは添付させないが技術基準に適合しているかの確認書類と申請書を提出するという話があった。全く見ないでよいというわけではないが、細かい資料を出していただく必要があるのかどうか、疑義があれば出していただくことになるが、許可と事後届の差が多少なりとも出てくるのかと思う。（METI）

・実情として軽微変更届について、許可と同様の資料を添付させて確認しているので、何とも言えないが。割と消防は、消防法の関係からも見るのではないかと思う。（自治体）

・事後届出の際の添付書類のどの程度のレベルの書類を求めるべきかについて考えがあればお聞きしたい。（KHK）

⇒難しい問題だと思うが、事後届出を受理した際に事後届出で問題がなかったことが確認できる程度の書類は必要に思う。（自治体）

・事後届出の際の添付書類のどの程度のレベルの書類を求めるべきかについて考えがあればお聞きしたい。(KHK)

⇒現状、軽微変更の届出の際の添付書類には、許可申請時に必要なレベルのものを求めている。個人的には、究極としてヒトが介入しなくても手続きが完了するようなシステムが構築できることが理想である。(自治体)

⇒その場合、様式の統一、添付書類の統一は必要である。どうしても念のためにいろいろな書類をつけておくという配慮から膨大な書類をつけたがる傾向があり、自治体としては添付された以上確認の義務が発生することになり、事務量の増加が懸念される。特に、電子申請が進むと簡単に書類添付できるので、ますますこの傾向が進みやすい。(自治体)

・事後届出の際の添付書類のどの程度のレベルの書類を求めるべきかについて考えがあればお聞きしたい。(KHK)

⇒現状、軽微変更の届出の際の添付書類には、許可申請時に必要なレベルのものを求めている。事業所側で技術基準等の遵守を確認しているということを示して貰うことは必要と考える。記録保存については、事業者の話を聞くと自治体に提出する必要があるので、チェックしているという面があるようで、単に記録保存に移行しても大丈夫かという心配もある。新認定制度ではこの点に問題がないかということをしっかり調査して貰いたい。(自治体)

・制度として事業所側にコンプライアンスは求めてはいるが、制度自体が複雑でわかりづらいものになると間違いが起きるリスクが高まるので、制度設計には気をつけたい。また、研修制度の充実、申請の電子化等についても検討し、より良い制度としたい。(METI)

・届出に係る事前相談ばかりでは、自治体の人員を確保できないことは理解している。事後届は詳細に基準適合に係るエビデンスを添付せず、工事の概要だけを受け取る受理は自治体としてあり得るか。(KHK)

⇒手続き（届出）に係る法的根拠は示す必要がある。また、エビデンスは不要であるが、技術基準に適合している旨の情報は必要。(自治体)

・届出の添付書類の考え方について、どの程度の詳細を求めるべきと考えるか (KHK)

⇒（後追いできるよう）ある程度の書類は必要と考える。軽微変更であることを確認する必要がある。どこまで省略できるかは議論の分かれるところかとは思うが、そうでなければ、受け付けができない。(自治体)

・変更工事については、都道府県によって若干その取扱いが異なっている場合もあると聞く。もしも、国によるガイドラインが制定された場合には、従来の県の指導方針と異なる場合は、新たにガイドラインに従うよう指導方針を変更することは可能か。(KHK)

⇒もともと、通達等で明確になっていない部分を県として指導してきているので、新たに国の方で判断基準が出されれば、それに従うことになる。

・事後届の場合においても、技術基準に適合していることを確認されるのかお尋ねしたい。(KHK)

⇒設備変更の特例措置の中で、事後届け出案件の取扱について、審査したいと考えている。現在の軽微変更届も間違えがないか審査しているので、同様に事後届についても審査するのであると考えている。

⇒次の事後届け出時の添付書類の取り扱いついて、審査ができないと困るので、簡素化しない方がいいかと考えているが、変更に関係ない部分であれば提出されなくても差し支えないかもしれない。変更許可申請なみのものがでてくれば審査に支障はないと思う。(自治体)

⇒この資料の趣旨は事後届の範囲が広がった場合、許可申請並みの確認をするとお互い非常に手間がかかると思うので、自治体さんによっては書類がたくさんついてくると見ざるを得ないことになり、簡素化するという考えもあるということで、本当に簡素化していいのかをお聞きしたかったという趣旨。県さんはきちんと審査するとおっしゃっていただいたと理解した。(KHK)

経済産業省

資料２

別添１２

高圧ガス保安法における
新たな認定制度の詳細設計について

2022年12月15日

高圧ガス保安室

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

1-1. 高圧ガス保安法等の一部を改正する法律（※）の概要

※高圧ガス保安法、ガス事業法、電気事業法、情報処理の促進に関する法律。令和４年６月22日に公布。

令和４年12月
経済産業省
産業保安グループ

背景

✓ 近年、産業保安分野において、**革新的なテクノロジーの進展**、**保安人材の不足**、**電力の供給構造の変化**、**災害の激甚化・頻発化**、**気候変動問題への対応の要請**など、様々な環境変化が生じており、これらを踏まえた**保安規制の見直し**が必要。

法律の概要

✓ （１）スマート保安※の促進、（２）新たな保安上のリスク分野への対応／災害対策・レジリエンスの強化、（３）カーボンニュートラル実現に向けた保安規制の整備の３つを柱に、**高圧ガス保安法**、**ガス事業法**、**電気事業法**等の改正を行う。

※ スマート保安：産業保安分野におけるIoT、ビッグデータ・ＡＩ、ドローン等の活用を通じた安全性と効率性の向上。「人の力・技術」との連携・融合。

（１）スマート保安の促進

✓ **「認定高度保安実施事業者制度」の創設**【高圧・ガス・電力】

「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」を**厳格に審査・認定**し、**安全の確保を前提に**、**その保安力に応じ**、**手続や検査の在り方を見直す**。

- 許可・事前届出を**事後届出・記録保存へ**
- **国等と事業者双方が行う検査を事業者による検査のみに**
- 常時監視・遠隔監視の普及を踏まえ、**検査時期や保安人員の配置を柔軟化**　等

⇨ **テクノロジーの活用促進により、保安レベルの向上と人材不足への対処**



ドローン・IoTによる点検



ビッグデータ・AIによる異常予兆検知・運転最適化

（２）新たな保安上のリスク分野への対応／災害対策・レジリエンスの強化

✓ **太陽光・風力発電設備の保安規制の見直し**【電力】

小規模な太陽光・風力発電設備※を、**「小規模事業用電気工作物」**と位置付け、**基礎情報の届出や使用前の自己確認等の対象とする**。

※出力が10kW以上50kW未満の太陽光・20kW未満の風力発電設備

- **設備の設置者の基礎情報の届出義務**（設備の種類、設置場所及び管理者等）
- **技術基準維持義務**、**使用前自己確認**（事業者が設備の安全性を事前に確認）等

＜太陽光パネルの崩落＞



＜風車の羽根の脱落＞



令和3年4月～12月未までに報告された小出力発電設備の事故件数は**158件**。

✓ **ガス事業者間の災害時の連携強化**【ガス】

災害時におけるガス事業者間の連携計画の事前策定を義務付け。

※電気事業法における災害時連携計画と同様の仕組みを導入。

（３）カーボンニュートラル実現に向けた保安規制の整備

✓ **燃料電池自動車の規制の一元化**【高圧】

高圧ガス保安法と道路運送車両法の両法が適用される**燃料電池自動車等**について規制を一元化（**高圧ガス保安法から適用除外**）。

✓ **「登録適合性確認機関」による確認制度の創設**【電力】

今後導入が進む**風力発電設備**について、安全かつ迅速な審査を行うため、工事計画届出の審査について、**専門機関**（「登録適合性確認機関」）**が技術基準の適合性を確認する仕組みとする**。



1-2. スマート保安を進めるための制度的環境整備のあり方 （“保安のテクノロジー化／デジタライゼーション”を進めるために）

出典:産構審保安・消費生活用製品安全分科会報告書（令和3年12月） の概要　P.4

テクノロジーの革新的進展
（IoT、BD・AI、ドローン等）

深刻な保安人材の枯渇
熟練の保安人材の不足
若年層の雇用困難化

保安体制の成熟化した産業分野・事業者

画一的・詳細な個別規制
膨大な届出・許可等の手続
高圧ガス：24万件／年
電力：22万件／年
都市ガス：1.4万件／年

保安レベルの持続的向上（保安イノベーション）と保安人材の枯渇の問題への対処のため、「スマート保安」を強力に推し進めるための制度的環境整備が必要である。

保安体制の成熟化した従来的な産業保安分野においては、自立的に高度な保安を確保できる事業者に対して、保安レベルに見合った合理的な規制のあり方を検討すべきである。

限りある行政リソースを新たなリスク分野に展開する必要

テクノロジーを前提に高度な保安を実現するためのメリハリある規制体系

保安レベルを下げることなく、むしろ、テクノロジーの活用により保安レベルを持続的に向上させるため、**「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」**については、行政の適切な監査・監督の下に、画一的な個別・事前規制によらず、**事業者の保安力に応じた規制体系へ移行**することとし、**手続・検査のあり方**をこれに見合った形に**見直す**措置を講じる（テクノロジーの活用を抜本的に促進しつつ、保安能力に見合う形で規制を適正化するスキーム（認定制度））。これにより、事業者の保安活動をテクノロジーを活用しつつ自己リスク管理がなされた高度な領域に強力に押し上げていくことが必要である。

電力　都市ガス　高圧ガス

前提１（安全の確保とメリハリある規制）

○テクノロジーを活用しつつ、「自立的に高度な保安を確保できる事業者」のみが対象

○行政が法令遵守状況等を立入検査により厳格にチェックすることや、重大事故や法令違反などが発生した場合には、その原因・内容・対応等を精査したうえで、機動的に認定の取消を実施することなど、安全確保のための行政による実効的な監督等を行う。

○高圧ガス保安法の現行「認定事業者制度」(高圧ガス保安法第3章の2)については、発展的に解消する。

前提２（事業者に対する環境整備）

テクノロジー化を目指す事業者が技術・人材面での支援を受けられるための環境整備

○産業横断的な技術支援／人材育成支援の取組推進
※関係機関との連携・取組強化　等

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

2-1. 主な審議事項と施行に向けたスケジュール

- **2023年12月頃の施行に向けて、新たな認定制度の詳細設計について、今回を含め三回にわたりご審議いただく**予定。

主な審議事項

制度総論	制度コンセプト・対応方針
	ターゲット
認定要件	要件の全体像
	要件１：経営トップのコミットメント
	要件２：高度なリスク管理体制
	要件３：テクノロジーの活用
	要件４：サイバーセキュリティなど関連リスクへの対応
認定特例	規制の特例措置
	A認定事業者向け特例措置
認定審査	審査体制
	認定更新期間

施行に向けたスケジュール（想定）

◇2022年
12月15日　高圧ガス小委員会①
主な審議事項：青枠の項目

◇2023年
２月頃　　高圧ガス小委員会②
主な審議項目：点線の項目
小委員会①の審議事項の深堀り

３月頃　　高圧ガス小委員会③
主な審議項目：とりまとめ※
※必要に応じて追加開催

◇2023年６月頃　　政令・省令等の公布

◇2023年12月頃　　施行

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

3-1. 新たな認定制度のコンセプト（目的）と具体的方針

- **新たな認定制度の導入に当たっては、国全体の高圧ガス分野の保安力向上を図ることを目的に、以下のような具体的方針の下、詳細設計を進めていく。**

新たな認定制度のコンセプト（目的）

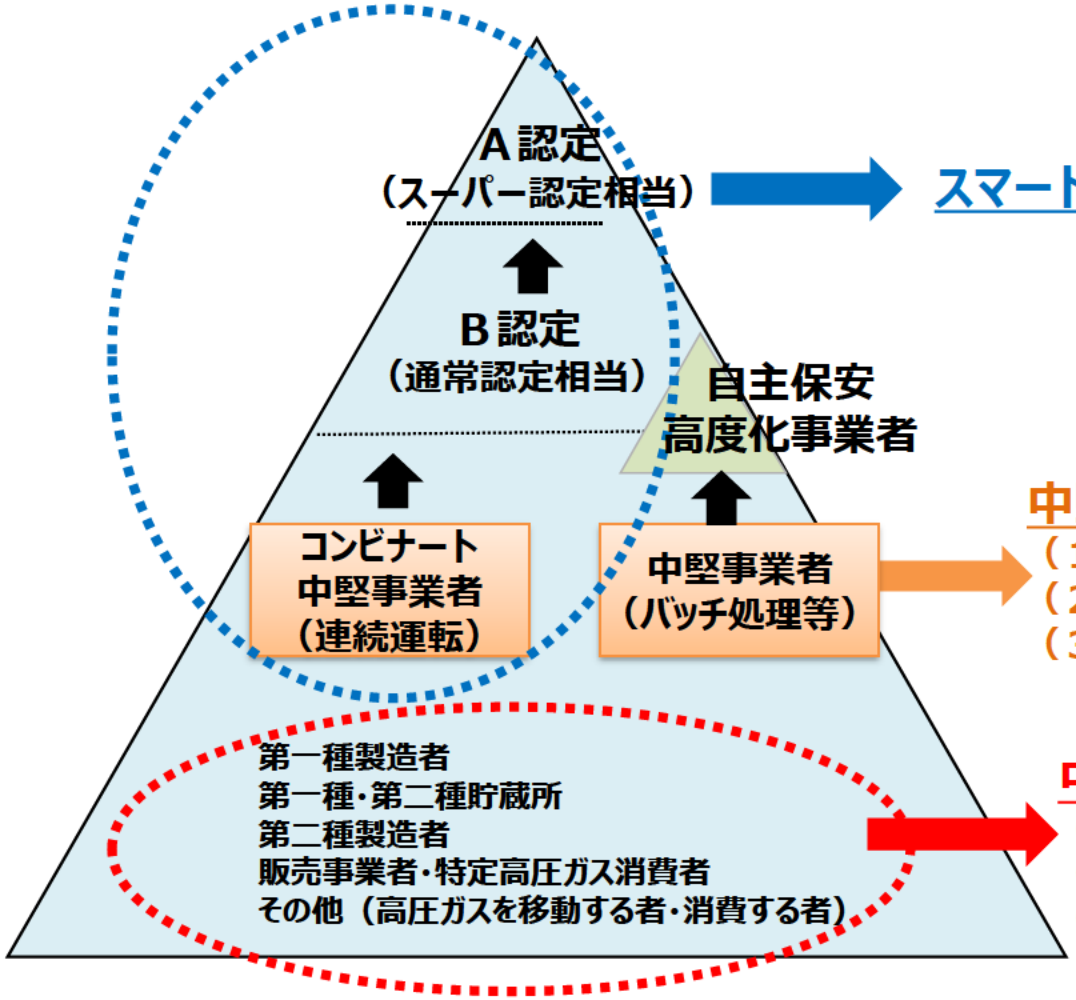
- 新認定制度の保安レベルの持続的向上や保安人材の枯渇問題の解消のため、**テクノロジーを活用したスマート保安を推進**する。
- 厳正な認定審査のもと、**テクノロジーを活用しつつ自立的に高度な保安を確保できると認められた事業者**については、**安全確保を大前提**に、**事業者の保安力に応じた規制体系へ移行**するとともに、**手続・検査の在り方をこれに見合った形に見直す。**これにより、**事業者・規制当局（国・自治体）のリソースを実質的な保安活動に配分することを可能**とする。
- 上記により、**国全体の高圧ガス分野の保安力向上（重大・悪質な法令違反、重大事故の削減）を目指す。**

具体的方針

1. 認定要件に**テクノロジー導入の要件を設け**、**保安分野へのテクノロジー導入を促進**する。
2. **合理的かつ迅速な認定審査へ移行**しつつ、**安全確保を大前提**に、**認定審査を厳正に行う**。
   併せて、**認定事業者に対する特例を拡充**する。
3. **テクノロジーを活用しつつ自立的に高度な保安を確保できる事業者（認定事業者）の増加**を目指す。

3-2. 新たな認定制度の対象事業者のイメージ

- **新たな認定制度の主な対象事業者は、現行認定制度の認定事業者の他、連続運転を行うコンビナートの中堅事業者**を想定。



スマート保安の促進を念頭に置いた新たな認定制度

中堅事業者における保安レベル向上のための対策
（１）スマート保安に向けた新技術導入支援
（２）スマート保安導入のための人材育成支援
（３）自主保安高度化事業者制度（非連続運転）

中小事業者における保安レベル向上のための対策
（１）“中小事業者向けインセンティブ制度”（省令事項）
（２）簡易アプリの開発・普及、許可・手続等のデジタル化
（３）中小事業者のデジタル化支援　等

（参考）現行高圧ガス保安法の認定制度の概要

高
保安力
低

スーパー認定

認定の要件

通常認定の要件に加えて、以下の取組が必要

① **高度なリスクアセスメント**の実施
② **IoT、ビッグデータ**等の**新技術の導入**
③ **高度な教育**の実施
④ **連続運転期間、検査手法の適切な評価体制の整備**
⑤ **第三者機関**によるアドバイスを実施

規制の合理化内容

①**連続運転期間・・・8年以下（事業者が自由に設定した期間）**
＜リスク・ベースドメンテナンス（リスクに応じた柔軟な保全）＞
②完成・保安検査・・・**事業者自らが検査**
③検査方法・・・**事業者が自由に設定した方法**
④設置・変更工事・・・許可不要な**軽微変更範囲の更なる拡大**
（熱交換器など、特定設備の取替え等）
⑤認定期間・・・**7年間**
⑥保安力の見える化・・・**スーパー認定マークを活用**

通常認定

認定の要件

① **リスクアセスメント**の実施。
② **PDCAサイクル**による保安体制の継続的改善
③ **教育訓練**の実施
④ **検査組織**の設置
⑤ **保安・運転・設備管理組織**の設置　等

規制の合理化内容

①**連続運転期間・・・4年間等（大臣に認められた期間）**
②完成・保安検査・・・**事業者自らが検査**
③検査方法・・・**大臣に認められた方法**
④設置・変更工事・・・許可不要な**軽微変更範囲の拡大**
（特定設備の管台の取替え等）
⑤認定期間・・・**5年間**
⑥保安力の見える化・・・**認定マークを活用**

自主保安高度化事業者

認定の要件

① **リスクアセスメント**の実施
② **PDCAサイクル**による保安体制の継続的改善

規制の合理化内容

①**連続運転期間・・・１年間（1年に1度運転を停止して検査）**
②完成・保安検査・・・**都道府県が検査（保安検査猶予期間（3カ月））**
③検査方法・・・**告示に定められた方法（KHKS）**
④設置・変更工事・・・許可不要な**軽微変更範囲の拡大**
⑤認定期間・・・**5年間**　⑥保安力の見える化・・・**認定マークを活用**

通常の事業所

①**連続運転期間・・・1年間（1年に1度運転を停止して検査）**
②完成・保安検査・・・**都道府県が検査**
③検査方法・・・**告示に定められた方法（KHKS）**
④設置・変更工事・・・**軽微な変更を除き、都道府県の許可**

高
事業者の自由度
低

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

4-1. 新たな認定制度の要件（総論）

- 新たな認定制度の要件（改正高圧法第39条の14第1項）は、スマート保安の促進の観点から、サイバー対策を含む**４つの要件で構成**する。**これまでの審議会での整理を基本とするものの、追加・拡充する要件については、審議を通じ具体化**していく必要。
- また、安全確保・事業者の保安能力の適正な判断を前提に、**認定基準の大括り化、簡素化、明確化**についても、併せて検討する。

出典:産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.８

（※）下記の表における赤字の下線部及び赤枠は、新たな制度的措置の認定基準において、現行の認定基準から拡充するものを示す。

	A 認 定	B 認 定
①経営トップのコミットメント	現行スーパー認定事業者制度の要件に加え、 コンプライアンス体制の整備（注1）、コーポレート・ガバナンスの確保	
②高度なリスク管理体制	現行スーパー認定事業者相当	現行通常認定事業者相当
③テクノロジーの活用	現行スーパー認定事業者制度における仕組み（注2）を基本とする ※認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用。	
④サイバーセキュリティなど関連リスクへの対応	各業界におけるサイバーセキュリティガイドライン（注3）に沿った内容とする	

（注1）高圧ガス保安法についての**法適合性確認能力**（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。
（注2）特定認定事業者及び自主保安高度化事業者の認定について（20201218保局第1号）における認定の基準「二 先進的な技術を適切に活用していること」の項目を参照。
（注3）「重要インフラにおける情報セキュリティ確保に係る安全基準等作成指針」（内閣官房内閣サイバーセキュリティセンター）を参考に業界団体が定める「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」、「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」。

4-2. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

論点

- ✓ 認定事業者による法令違反の発覚等を踏まえ、**会社全体の運営の健全性を確認することが必要**。
- ✓ **規制の特例の見直しにより**、事業者の自主保安に委ねられる領域が拡大※１することを踏まえ、事業者が**法適合性確認能力※２を有することを確認**することが必要。

※１　新たな認定制度の認定事業者においては、その保安確保能力を踏まえ、ガス種の変更又は製造能力が一定以上変更される場合など重要な変更については許可制を維持しながらも、軽微変更についてはその対象範囲を拡大した上で記録保存義務とされた。
※２　設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力。

産構審　分科会報告書における記載

現行のスーパー認定事業者制度の要件（経営トップによる保安の方針の明示等）に加え、**コンプライアンス体制の整備、コーポレート・ガバナンスの確保といった要件を拡充**し、特にコンプライアンス体制の整備については、**高圧ガス保安法についての法適合性確認能力（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していること等を確認**する。

※「コンプライアンス・ガバナンス」の観点からは、運営側の責任者の明確化、社内監視体制の整備とその責任者の明確化が重要である。その際、例えば、上場企業の場合には、上場審査基準の活用や、上場企業でない場合には、公益通報者保護法に基づく内部通報制度の整備と遵守といったようなところも考慮すべき」との意見があった。当該意見を踏まえつつ、「法適合性確認能力」の具体的審査項目については、金融関連法制やインフラ関係の業法等、高いコンプライアンスが求められる、他法の例も参考に策定（法令順守に関する組織や体制、第三者や相互の監視体制、内部通報制度の完備方針・マニュアルの整備、社内教育体制等）する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- **コンプライアンス体制の整備、コーポレート・ガバナンスの確保の要件は、**現行の認定制度の要件に経営トップによる保安の方針の明示等が含まれていることも踏まえ、**以下の四つの視点で検討する**。

1. **取締役等に保安についての責任とイニシアティブを持たせ、保安活動をトップダウンで推進できる体制の整備**が必要。
2. また、**取締役等が、保安に対する責務を適切に果たしていることを監督する体制の整備**が必要。
3. 行政手続漏れ等の法令違反を防止するためには、**事業所内で複層的なチェック体制を構築すること**が不可欠。
4. また、法令違反時の組織的隠蔽等を防止する観点から、**法令違反発生時の通報手順が明確に定められていること**が必要。

- 上記に加え、**認定取消の処分基準において、重大・悪質な法令違反が発覚した場合を明文化**することによって、法令遵守体制の整備を促す。

4-3. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

- 検討の視点を踏まえ、新たな認定制度における経営トップのコミットメントの要件は、現行の認定制度の要件※に下記の要素を追加することとしてはどうか。

※現行の認定制度の要件においては、法人の代表者が保安の基本方針を策定していること、法人の代表者が認定要件の適合性に対して責任を有していること等が規定されている。

検討の視点を踏まえた認定要件（案）

コーポレート・ガバナンスの要件

１　取締役等※を保安活動の責任者としていること

保安に係る意思決定を迅速に行い、トップダウンで社内横断的に適切な保安活動の実行を可能とする観点から、取締役等を保安活動の責任者としていること。　※代表取締役や他の職務との兼務も可能とする。指名委員会等設置会社における執行役も含むこととする。

２　監査役等※が保安体制の整備等について監査を行っていること

例えば、保安管理部門等から監査役等に保安活動の状況が定期的に報告されているほか、監査役等が事業所を定期的に訪問して改善意見を示しているなど、監査役等が保安活動に責任を有する取締役等の職務執行や事業所の保安活動全般に対して有効な監査を行っていること。　※指名委員会等設置会社・監査等委員会設置会社においては、監査（等）委員会等を想定。

コンプライアンスの要件

３　複層チェック体制の構築

設備の変更工事等の際に、行政手続の要否等を保安管理部門を含む複数の部門が確認する体制が構築されているなど、高圧法の法令事項を遵守するための複層的なチェック体制が構築されていること。

４　法令違反発生時の通報手順の策定

高圧法の法令違反が発覚した際の本社や関係行政庁への通報手順が適切に定められていること。

（参考）現行の認定制度における本社の体制の要件

（コンビナート等保安規則　別表第5（第41条第1項関係））

一　本社の体制について

イ　保安に係る基本姿勢

一　法人の代表者によつて、保安の確保に関する理念、基本方針等の諸施策が明確に定められ、かつ、文書化されていること。また、これらの諸施策が各事業所等の全ての就業者に理解され、実施され、かつ、維持されていること。

二　法人の代表者が、本社及び事業所をこの表に定める基準に適合させる責任を有することが明確に定められ、かつ、文書化されていること。

ロ　保安管理

一　役員を長とする保安対策本部等が設置されており、保安管理の基本方針の決定、各事業所ごとの保安管理実績の検討等の実施について明確に定められ、文書化され、かつ、適切に実施されていること。

二　保安管理部門が設置されており、生産計画、設備管理計画等に当該部門の意見が十分に反映されることが明確に定められ、文書化され、かつ、意見が十分反映されていること。

三　保安管理部門の長は、申請その他認定に関する業務を統括し、認定業務の責任者となることが明確に定められ、かつ、文書化されていること。

四　本社が、一年に一回以上事業所及び検査管理（認定完成検査の実施状況の不備及び検査結果がこの規則の基準に適合していない場合の改善勧告をいう。以下この表において同じ。）を行う組織に対し、この表に定める基準に適合しているかどうかについて監査を実施することが明確に定められ、文書化され、かつ、適切に実施されていること。

五　本社又は事業所における法令違反等に関する報告の受付等の業務を行う組織が、独立して設置されており、かつ、適切に運営されていること。

4-4. 新たな認定制度の要件（認定要件１：経営トップのコミットメント）

- **法令違反を防止するために企業がとりうる方策は多種多様**であるところ、自主保安を促進する観点からは、**事業者自身が最適だと考える方法によって、法令遵守体制の整備を進めることが重要**。
- そこで、事業者に法令遵守体制の整備を促す観点から、認定取消の処分基準において、**重大・悪質な法令違反**が発覚した場合を明文化することとしてはどうか。

現行の認定取消要件に関する記載

高圧ガス保安法

（認定の取消し等）

第三十九条の十二　経済産業大臣は、認定完成検査実施者又は認定保安検査実施者が次の各号のいずれかに該当するときは、第二十条第三項第二号又は第三十五条第一項第二号の認定を取り消すことができる。

一～五　（略）

六　**第三十九条の三第一項各号又は第三十九条の五第一項各号のいずれかに該当していないと認められるとき。**

七～十　（略）

通達（「認定完成検査実施者及び認定保安検査実施者の認定について」）

８．認定の取消

（１）法第３９条の１２第１項第１号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、認定を受けている製造事業所又は第一種貯蔵所において、次のいずれかの要件に該当する高圧ガスによる災害が発生した場合とする。

① 負傷の程度に応じて次の表 a から d までに定める被害以上の人的被害が発生したとき。

図（略）

② 直接損害額が２億円以上発生したとき。

③ 次のいずれかに該当し、かつ、社会的影響が大きいと認められたとき。

イ 多数又は長時間の避難者が発生する等住民の生活に多大な影響を及ぼしたとき。

ロ 認定を受けている製造事業所又は第一種貯蔵所外で人的被害が発生したとき。

ハ 認定を受けている製造事業所又は第一種貯蔵所外で物的被害が発生したとき。

ニ 著しい環境破壊を及ぼしたとき。

④⑤　（略）

（２）　（略）

（３）法第３９条の１２第１項第６号に該当するものとして、経済産業大臣が認定を取り消すことができるのは、次のいずれかに該当することとなった場合とする。

① 認定保安検査に係る検査脱漏、事業所の保安体制に不備が認められ、かつ、それが（１）の①から③まで（③イを除く。）に掲げるいずれかの災害を惹起するおそれが相当程度あったと認められたとき。ただし、本社による監査等により自ら確認し、速やかに報告があったものについては、この限りではない。

② **緊急時即時通報連絡が行われなかったとき等保安体制に重大な不備が認められたとき。**

（４）　（略）

4-5.新たな認定制度の要件（認定要件２：高度なリスク管理体制の要件）

論点

- ✓ 認定対象事業者の保安レベルを確保するべく、**認定の水準は、現行の認定制度より下げるべきではない**。また、**現行の認定制度の下における認定基準は、既に相当程度の保安レベルを確保できる水準であり、現行の認定基準をベースとすることが妥当。**
- ✓ **現行の通常認定制度**は、**認定要件にリスクに対する低減策の実施を求めていない**。

産構審　分科会報告書における記載

保安に関する専門部署の設置等、現行の認定事業者制度で要求されるリスク管理レベルは維持しつつ、事業者のリスク管理体制のレベルに応じ、**A認定については、現行のスーパー認定事業者相当のリスク管理体制**とし、**B認定については、現行通常認定事業者相当のリスク管理体制**を求める※。

※「設備が老朽化すると事故や支障も出やすいことから、高度なリスク管理体制の要件の中で、老朽化した施設についての管理のあり方についても考慮すべき」との意見があった。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- **A認定については、現行のスーパー認定事業者相当のリスク管理体制を、B認定については、現行通常認定事業者相当のリスク管理体制**を求める。
- 特定されたリスクに対する低減策の実施は、保安確保上不可欠であり、B認定に対しても求めることを検討する。

検討の視点を踏まえた認定要件（案）

- **A認定事業者**に対しては、**現行のスーパー認定事業者相当の要件**を課してはどうか。
- **B認定事業者**に対しては、**現行の通常認定事業者相当の要件に加え、特定したリスクに対する低減策を実施していること**を要件として課してはどうか。

4-6.新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

論点

- ✓ スマート保安の実現には、**テクノロジーの開発・導入に向けた経営トップのコミットメント**が必要。
- ✓ 導入の対象となりうるテクノロジーには、①**現場作業の効率化につながるもの**（例：ロボット・ドローン等を活用し点検作業を効率化）や、②**意思決定の高度化につながるもの**（例：運転時のプロセスデータから異常を早期に検知し、作業員の判断を補助・代替）等があり、その**目的やレベルは様々**である。
- ✓ テクノロジーの導入によって保安力を向上させるためには、**導入・効果検証・改善のサイクル**を繰り返すことが必要。
- ✓ A認定相当の事業者とB認定相当の事業者には**一定の保安レベルの差異が存在**する。

産構審　分科会報告書における記載

現行のスーパー認定事業者制度における仕組み※を基本とする。その際、認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用する（すなわち、保安に係るテクノロジーのイノベーションを阻害せず、むしろイノベーションを促進する観点から、一定の技術水準を確保しつつも、活用するテクノロジーの種類を明示的に限定することとはしない）。また、**テクノロジーの活用に向けた効果検証や改善等といったテクノロジー活用プロセスも重要**であることから、**現行のスーパー認定事業者制度の基準を踏まえて、これを要件とする**。

※現行のスーパー認定事業者制度においては、IoT等の先進的な技術の導入・効果検証・改善等を行っていること等を要件としており、具体的には、特定認定事業者及び自主保安高度化事業者の認定について(20201218保局第1号) における認定の基準の「二 先進的な技術を適切に活用していること」の項目を参照。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- 現行のスーパー認定事業者制度における仕組みを基本としつつも、これまでのスマート保安の実現に向けた取組等を踏まえ、以下の三つの視点でテクノロジーの活用の要件を検討する。

1. 事業者の保安レベルを考慮し、**導入を求めるテクノロジーのレベルは、A認定とB認定で差異を設ける**。
2. テクノロジー導入後、**導入・効果検証・改善のサイクルを構築**していること。
3. テクノロジー導入に向けた**経営トップの関与**が必要。具体的には、**テクノロジー導入に向けた計画が策定され、必要なリソース（予算・人材）が確保**されていること。

4-7. 新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

- 検討の視点を踏まえ、新たな認定制度におけるテクノロジーの活用の要件は、**現行のスーパー認定制度の認定要件を基本とし、以下のように見直してはどうか**。
- なお、**外部からのモニターの実施**（年１度の経済産業省への報告）については、別途報告を受けている※ことから、**廃止することとしてはどうか。**

※現在スーパー認定事業者に求めている外部モニターの実施（年１度の経済産業省への報告）については、スマート保安官民協議会等で代替できている。また、スーパー認定事業者に期待するトップランナーとしての役割は、良好事例の展開等の他の認定要件で代替可能。

検討の視点を踏まえた認定要件（案）

１　経営トップのコミットメント

保安の確保に資するテクノロジー導入に向けたビジョンが策定され、必要なリソース（予算・人材）が確保されていること。

２　保安の確保に資するテクノロジーを導入していること

A認定は①②のテクノロジーを導入していること、B 認定は①のテクノロジーを導入していること。

①現場作業の効率化につながるテクノロジー

例：異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等

②意思決定の高度化につながるテクノロジー

例：予測する技術、人の意思決定を補助又は代替する技術等

３　保安の確保に資するテクノロジー導入について継続的に改善する仕組みが構築されていること※

保安の確保に資するテクノロジーの導入に当たって、導入計画の策定やトライアル検証を行っていること。また、保安の確保に資するテクノロジーの導入後に効果検証・改善を行っていること。

※効果検証・改善が実施されるまでには一定の期間を要すると考えられるため、初回認定の認定審査時は、一部のテクノロジーについては導入計画の策定のみで足りるとすることなどが考えられる。

4-8. 新たな認定制度の要件（認定要件３：テクノロジーの活用の要件）

現行のスーパー認定制度の要件と新たな認定制度の要件との対応関係

スーパー認定制度の要件		新たな認定制度の要件	A認定	B認定
—	新設	①経営トップ※のコミットメント ※テクノロジーに関する投資計画・人材計画等に責任を持つ取締役等を想定。	✓ 保安の確保に資するテクノロジー導入に向けたビジョンの策定と必要なリソース（予算・人材）が確保されている	
① 先進的な技術の導入 ② 導入した①技術の効果検証・改善に向けた取組みの実施 ③ ビッグデータの収集・分析・未来予測・ヒトに気付きを与えミスを防ぐ観点からの技術の検証・導入・導入計画の策定 ④ ②技術について6カ月以上の検証	再編	②保安の確保に資するテクノロジーの導入	✓ 現場作業の効率化につながるテクノロジー（異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等） ✓ 意思決定の高度化につながるテクノロジー（予測する技術、人の意思決定を補助又は代替する技術等） を導入している	✓ 現場作業の効率化につながるテクノロジー（異常検知、モニタリング技術、人の作業を代替する技術、現場の状態を診断する技術等） を導入している
		③継続的に改善する仕組みの構築	✓ 導入計画の策定→トライアル検証→導入→効果検証→改善を行っている※ ※初回認定の認定審査時は、一部のテクノロジーについては導入計画の策定のみで足りるとすることなどが考えられる。	
⑤ 外部からのモニターの実施（年1度の経済産業省への報告）	廃止	–		

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

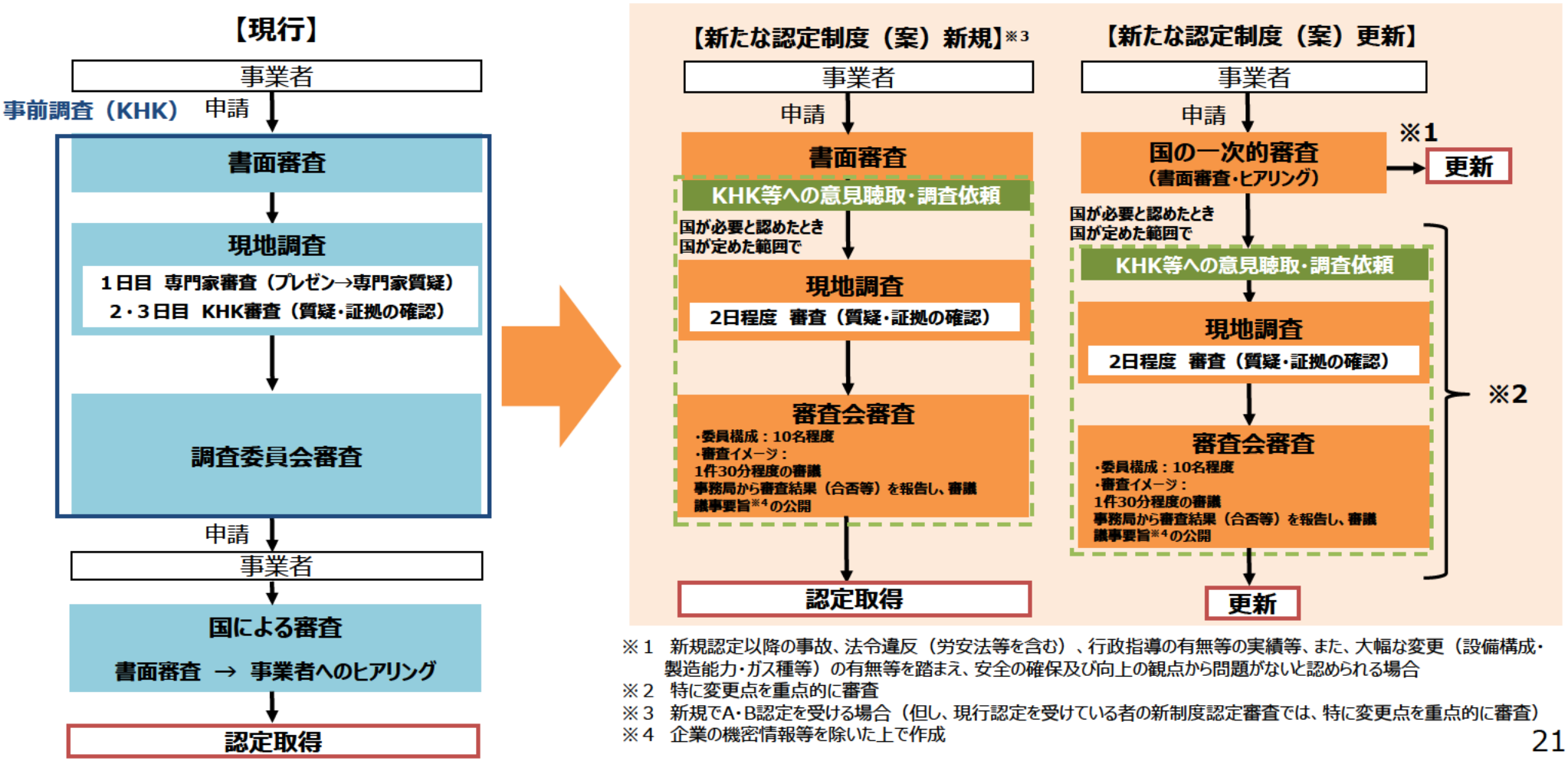
７．A認定事業者向けの特例措置

5-1. 新たな認定制度における認定審査のコンセプト

- 新たな認定制度では、**安全の確保及び向上を前提に、合理的かつ迅速な審査手続とする観点**から、**国が**（KHK等への意見聴取・調査依頼、外部有識者からなる審査会審査などを活用しつつ）**審査を行う**こととしており、以下のような見直しを行う方針。

  ① **審査プロセスの合理化（プロセスの合理化、申請書類・手数料の見直し、評価結果のランク付け廃止等）**

  ② **審査基準の透明化（審査基準・審査会審査の議事要旨※の公開）** ※企業の機密情報等を除いた上で作成。



※1 新規認定以降の事故、法令違反（労安法等を含む）、行政指導の有無等の実績等、また、大幅な変更（設備構成・製造能力・ガス種等）の有無等を踏まえ、安全の確保及び向上の観点から問題がないと認められる場合

※2 特に変更点を重点的に審査

※3 新規でA・B認定を受ける場合（但し、現行認定を受けている者の新制度認定審査では、特に変更点を重点的に審査）

※4 企業の機密情報等を除いた上で作成

5-2. 新たな認定制度における審査プロセスに関する今後の論点

- 残りの二回の審議において、下記の論点等を扱う予定。

論点①　調査依頼制度の詳細

- ✓ **対象とする範囲**
- ✓ **指定機関の要件**
- ✓ **初回申請時の扱い**

【産構審分科会報告書における記載】

国は、国の検査及び審査会審査を行う案件のうち、必要と認めたときは、その範囲を定めて、KHK又は指定機関に意見を聴取し、又は調査を依頼できるものとする。KHK等の調査が行われた場合、国の検査は、その範囲で省略され、重複の検査・調査は行わない。KHK等が一部の調査を行う場合、運用上は、国とKHK 等は一緒に（一回で）検査・調査を行う。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

論点②　審査会審査の詳細

- ✓ **審査方法**
- ✓ **委員構成**

【産構審分科会報告書における記載】

〇新規認定：全数を国の検査及び審査会審査（注）を行う。

○更新：国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況等を踏まえ安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査（注）を行う。

（注）審査会審査：外部有識者（KHK、高圧ガスやIoT等のテクノロジーに関する学識経験者等）からなる審査会で行う審査

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.24 図21）

論点③　更新時に現地調査・審査会審査を実施する場合の基準

- ✓ **認定更新時に、現地調査・審査会審査を実施する場合の基準**

【産構審分科会報告書における記載】

更新では、国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況や法令違反（労安法等含む）、行政指導等の有無、また、大幅な変更（設備構成・製造能力・ガス種等）の有無等を踏まえ、安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査を行うものとする。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

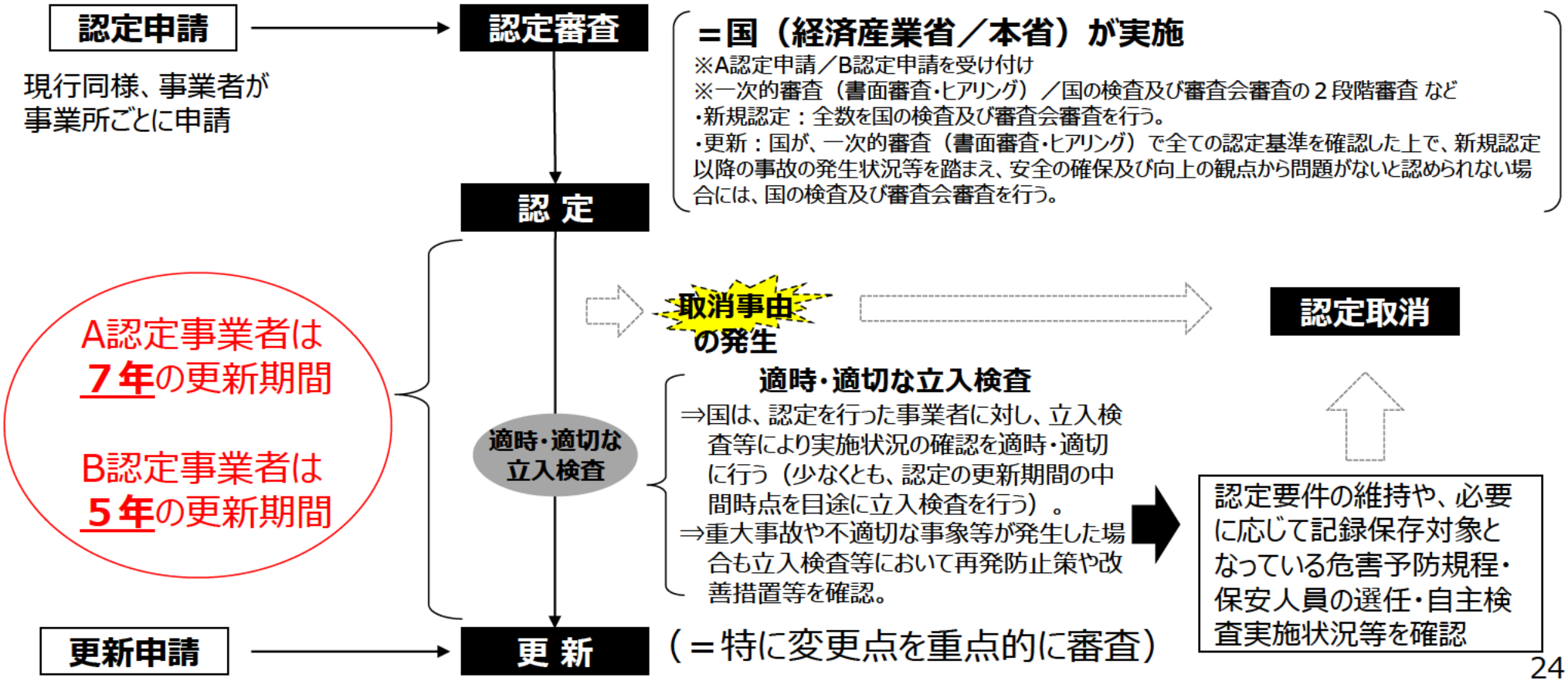
６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

6-1. 新たな認定制度の認定の更新期間について

- 新たな認定制度における認定の更新期間については、①新制度では一部の要件が拡充されるものの、要件の大部は現行制度と同等の保安レベルを求めるものであること、②特例の範囲が現行制度よりも拡充されること、③近年の認定事業所の重大事故・法令違反の状況を考慮する必要があることを踏まえ 、現行認定制度同様、**A認定（スーパー認定相当）7年、B認定（通常認定相当） 5年としてはどうか。**

＜認定から更新までのフロー図＞



１．高圧ガス保安法における新たな認定制度の概要

２．主な審議事項と施行に向けたスケジュール

３．新たな認定制度のコンセプト

４．新たな認定制度の要件

５．新たな認定制度の審査体制

６．新たな認定制度の認定の更新期間

７．A認定事業者向けの特例措置

7-1. A認定事業者に係る検査面での制度的措置（ふり返り）

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）**において、**A認定事業者には**、手続面での制度的措置に加え、**検査面での制度的措置を拡充し**、比例原則・リスクベースに基づき、**認定事業者間で制度的措置を差異化**することとされた。

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.11

①CBM（Condition Based Maintenance）の円滑化

●例えば、高圧ガス小委員会等で技術的検証を行い、以下について検討する。
- 現行の減肉判断：単純腐食に加え、クラック・クリープも対象
- CBMの考え方を用いた検査方法の拡大の検討：計測器類・遮断弁等

●KHKへの腐食環境や厚さ測定等のデータ提出義務を廃止

②検査等に係る基準・規格の柔軟化

－採用する基準・規格（海外規格等）の大臣認定制を導入する。
（採用する基準・規格の複線化・複相化の円滑化）

※具体的には、例えば、通達（補足1）において、肉厚測定検査及び開放検査を行う方法について「KHK/PAJ/JPCA S0851(2014)（補足2）又はこれと同等の基準」を用いることになっているが、「これと同等の基準」について、事業者自らの判断に加え、大臣が認定することにより、検査等に係る基準・規格を柔軟に選択できるようにすることが含まれる。また、肉厚測定の間隔（現行4年以内）及び検査時期設定係数（現行0.8）のあり方については、事業者において、その能力や設備管理の実態等に応じ、一定の範囲で決定できるなど仕組みの柔軟化を図る方向で検討する。その際、「一定の範囲」については、肉厚測定の間隔及び検査時期設定係数に関して事業者が選択しうる最大の値のあり方等について、B認定との差異化も考慮しつつ、技術的な検証を踏まえて検討する。

（補足1）「特定認定事業者及び自主保安高度化事業者の認定について」20201218保局第1号
（補足2）高圧ガス設備の供用適性評価に基づく耐圧性能及び強度に係る次回検査時期設定基準

（注１）A認定の認定時、採用する基準・規格のリストを添付し、同時に採用する基準・規格の認定を受けることも可能とする方向で検討する。

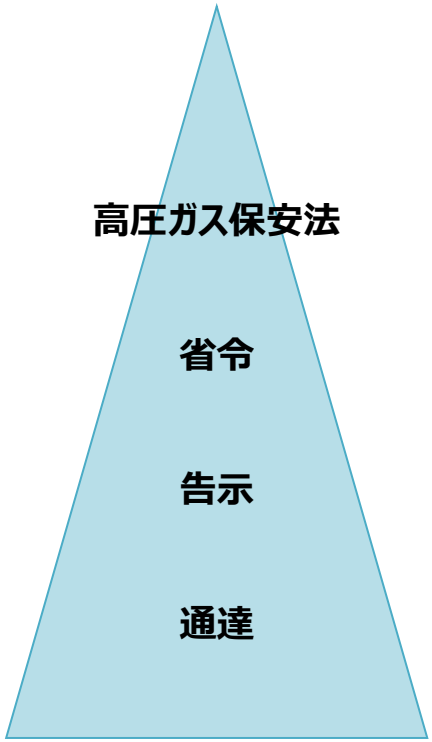
（注２）なお、B認定においては、引き続き、KHK/PAJ/JPCA S0851(2014)によることとするものの、技術的な検証を踏まえ、肉厚測定の間隔（現行最大2年⇒例えば4年）及び検査時期設定係数（現行0.5⇒例えば最大0.8）の柔軟化措置を講じる方向で検討する。

7-2. A認定事業者向けの特例措置（検査等に係る基準・規格の柔軟化のための新たな仕組みの導入）

- **現行のスーパー認定事業者（A認定相当）**には、**検査等に係る基準・規格の自由選択制が導入**されている。
- しかしながら、**事業者自らの判断により検査等に係る基準・規格を自由に導入することは積極的には活用されず**、**事業者は、実質的に法令で定められた基準・規格に従って保安業務を行っているのが実態**。
- このため、広く民間の先端の技術的知見を取り込み、一層民間規格の活用を促進する観点から、国・高圧ガス保安協会を中心とした従来の基準策定機能に加え、**A認定事業者による検査等に係る基準・規格の自由選択性が実質的に機能する仕組みを導入**することとしてはどうか。

【現行の高圧ガス保安法における検査方法】

- 現行のスーパー認定事業者は、**自由な検査方法を選択することができる**。



（法）高圧ガス保安法　第三十五条

4　第一項の都道府県知事、協会又は指定保安検査機関が行う**保安検査の方法は、経済産業省令で定める。**

（省令）コンビナート等保安規則

第三十七条　法第三十五条第四項の経済産業省令で定める**保安検査の方法は、開放検査、分解検査その他の各部の損傷、変形及び異常の発生状況を確認するために十分な方法並びに作動検査その他の機能及び作動の状況を確認するために十分な方法**でなければならない。

2　前項の**保安検査の方法は告示で定める。ただし、次の各号に掲げる場合はこの限りでない。**

一　（略）

二　**特定認定事業者が**、令第十条ただし書の認定に係る特定施設について行う保安検査の方法であつて、**次のいずれにも該当するものを用いる場合。**

イ　製造設備の寿命等を勘案して、適切な時期に、肉厚測定検査及び開放検査を行う方法

ロ　少なくとも八年に一回は運転を停止した検査を行う方法

ハ　保安検査に係る責任者が前項に定める方法に適合すると認めた方法

（告示）保安検査の方法を定める告示

保安検査の方法は、次の表の上欄に掲げる区分に応じ、それぞれ同表の下欄に掲げるものとする。

製造施設	保安検査の方法
四 コンビナート等保安規則の適用を受ける製造施設	四 高圧ガス保安協会規格ＫＨＫＳ ０８５０―３ （２０１７）保安検査基準

（通達）「特定認定事業者及び自主保安高度化事業者の認定について」

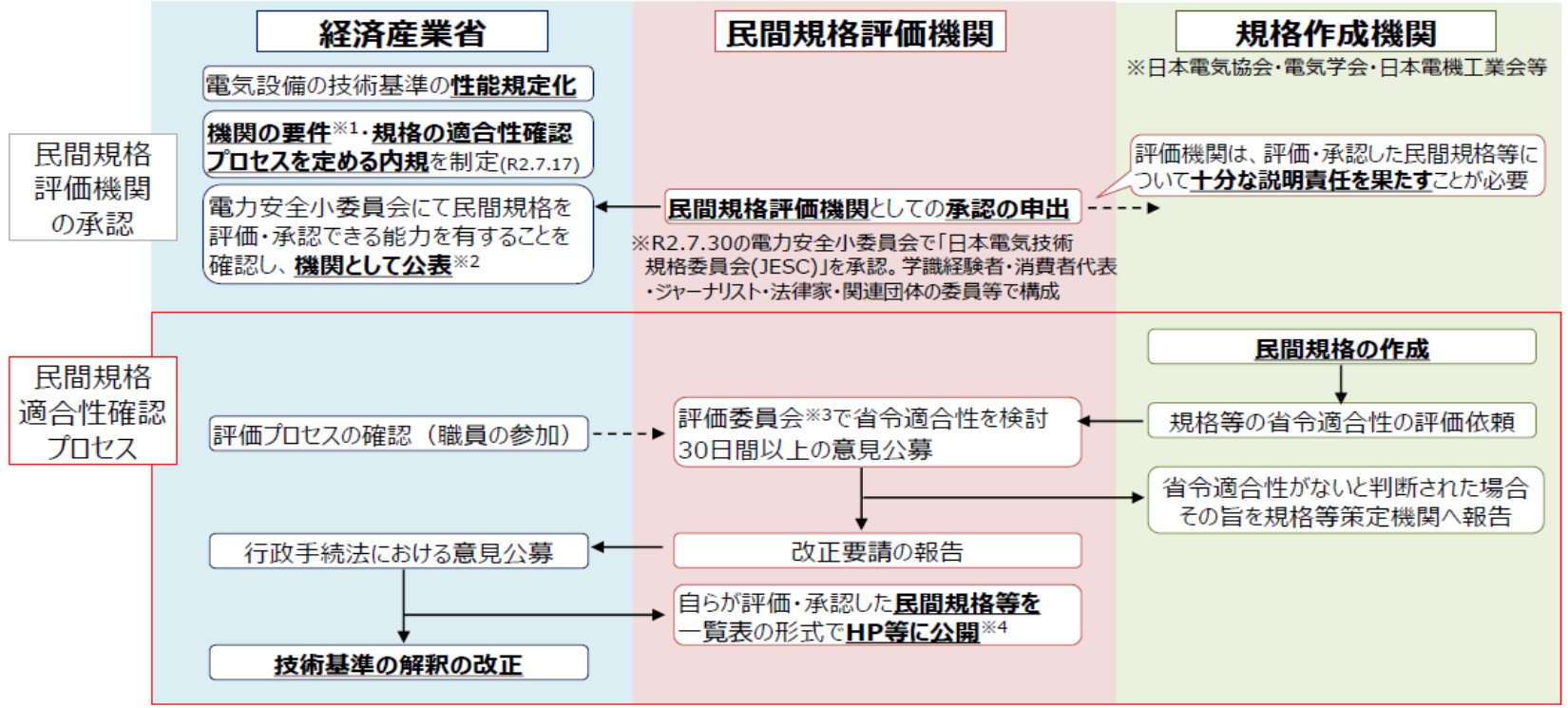
肉厚測定検査及び開放検査を行う方法について「KHK/PAJ/JPCA S0851(2022)又は**これと同等の基準**」を用いることになっている

7-3. A認定事業者向けの特例措置（電力分野を参考とした新たな仕組みの導入）

- **電気事業法における電気設備の技術基準への民間規格の取り込みを参考に、高圧ガス保安法上の検査等に係る基準・規格の自由な選択を促す仕組みを導入してはどうか。**
- 具体的には、**A認定事業者を対象に、国が定める要件を満たす民間規格評価機関が承認した検査等に係る基準・規格であれば、高圧ガス保安法上の適切な検査方法と認めることとする仕組みを導入してはどうか。**

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）P.65　図64

【電気事業法における電気設備の技術基準への民間規格の取り込み】



※1 技術評価委員会と民間規格評価委員会（規格の制改定プロセスの公正性等を含めた全体評価を行う）を設置する等。（以下の※2~4も要件に含む）
※2 適切な評価の実施は、国の職員による**評価委員会への立会い**、**１年ごとの定期報告**(評価の実施状況についての**有識者による外部評価**)等により確認
※3 民間規格等に係る**技術分野に加え**、**消費者問題、法律、ジャーナリズム等の幅広い分野の専門家から構成**
※4 規格として承認された日から**少なくとも五年に一回は、改正、廃止又は確認**が行われるよう適切に管理

（参考）電力分野における民間規格評価機関の詳細

出典：保安・消費生活用製品安全分科会
第22回電力安全小委員会　資料６－１　P.6

● 民間規格等の評価を行うに当たっては、**技術評価委員会**（技術的な側面の評価を行う）及び**民間規格評価委員会**（規格の制改定プロセスの公平性、客観性及び透明性等を含めた全体的な評価を行う）を設置する等、**評価が十分かつ確実に行われるような評価体制を求める**。

➢ 評価の方法

民間規格等の評価に当たっては、技術的な側面の評価を行う技術評価委員会と民間規格制改定プロセスの公平性、客観性及び透明性等を含めた全体評価を行う民間規格評価委員会を設置し、評価対象となる民間規格等に応じ適切な審議回数とするなどにより、十分な評価が行われるようにする。

また、評価対象となる民間規格等の作成に関与した専門家は評価に関与すべきではなく、これが確実に担保される措置を講じる。

➢ 技術評価委員会

民間規格等の評価の関係者の範囲として、評価対象となる民間規格等を使用するメーカー、施設者及び施工者のみならず、当該民間規格等が対象とする電気工作物のユーザーも加える等、評価対象となる民間規格等に関係する、できるだけ幅広い者を評価に加える。

➢ 民間規格評価委員会

民間規格等の評価に当たっては、規格内容に直接関係する専門分野に加え、消費者問題、法律及びジャーナリズムを含む幅広い観点から評価を行う専門家を必要とする。

（参考）電力分野における民間規格評価機関の詳細

出典：保安・消費生活用製品安全分科会
第22回電力安全小委員会　資料６－１　P.７

- 評価機関は、**民間規格等と技術基準との適合性について評価**を行い、承認した民間規格等を自らの承認リストに掲載し、**公開**。
- **年１回以上の外部評価**を受け、**評価プロセスが適切に運営されていることを自ら確認**し、必要に応じて改善策を講じる。

➢ 評価の観点

評価機関は、当該民間規格等が技術の動向や関連する最新の知見を適切に踏まえているか等を踏まえた評価を行い、結果を評価書にとりまとめる。

➢ 評価・承認した民間規格等の承認リストへの掲載

評価機関は、評価書をとりまとめ技術基準適合性を確認し、承認した民間規格等を、省令基準及び基準解釈との関係を明確にして、評価機関が公開する「評価機関が承認した民間規格等」のリストに当該民間規格等と技術基準の関係が明確になるように掲載する。

➢ 評価プロセスの外部評価

評価機関は、評価プロセスが適切に運営されていることを自ら確認するため（PDCAサイクルの構築）、外部評価を受け、その結果に基づく改善等を定期的に行う。

（参考）日本電気技術規格委員会の概要

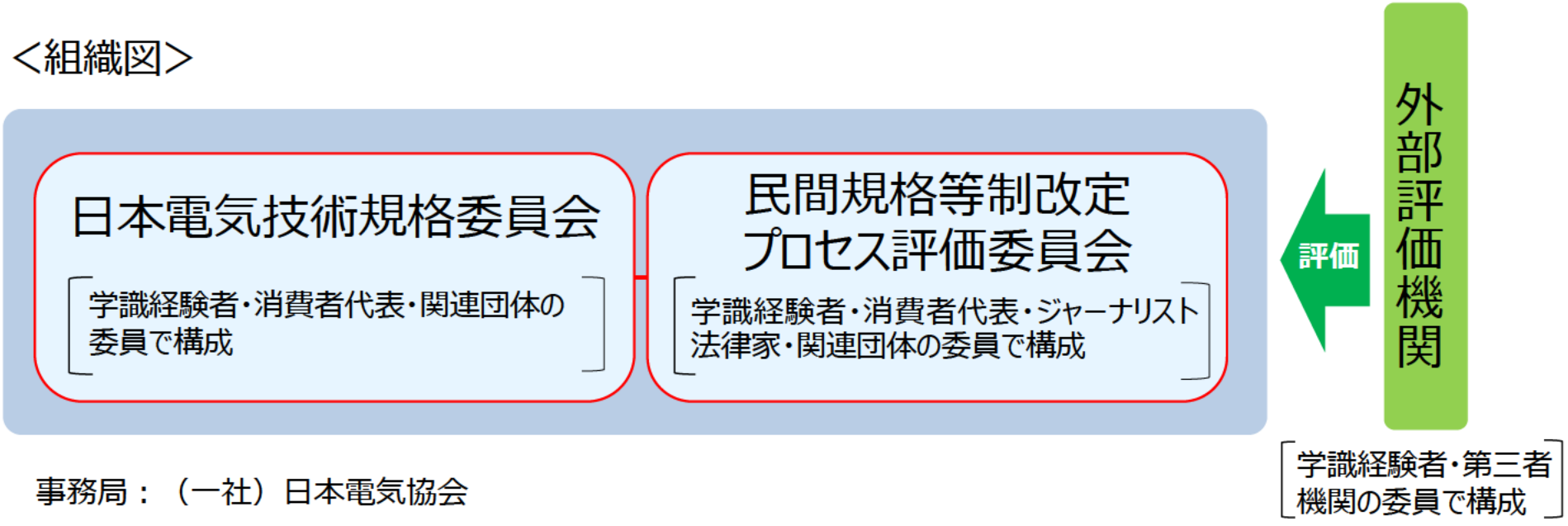
出典：保安・消費生活用製品安全分科会
第23回電力安全小委員会　資料１　P.8

- 日本電気技術規格委員会（JESC）は、**技術評価委員会として「日本電気技術規格委員会」及び民間規格評価委員会として「民間規格等制改定プロセス評価委員会」の２つの委員会を設置。**
- **外部評価機関**を設置し、民間規格等の制改定に係る評価プロセスが国の定める要件を満たし、委員会が**適切に運営・維持されているかを外部評価。**

日本電気技術規格委員会（JESC）

・設立：平成９年６月３０日
・公正・中立な立場で民間規格を策定・評価することにより、新たな知見や技術の規格への迅速な反映、公共の安全の確保を目指す委員会として設立
・電気工作物の保安に係る２４の関係団体の参加により運営
・事務局は（一社）日本電気協会が担当

＜組織図＞



事務局：（一社）日本電気協会

（参考）評価プロセスにおける国の関与

出典：保安・消費生活用製品安全分科会
第22回電力安全小委員会　資料６－１　P.８

- 国は、**候補となる機関が評価機関の要件を満たすことを確認**。また、評価機関における民間規格等の**評価プロセスが要件に従い運営されていることを確認**し、**必要があると認められる場合は改善指導等**を行う。
- これらの確認については、電力安全小委員会にて御審議・御確認いただく。

➢ 国による評価機関の確認

国は、候補となる機関が評価機関の要件を満たしているかどうかを確認する。
国の審議会の議事録や、評価機関について確認した内容をホームページ等で広く公開する。

➢ 評価プロセスにおける国の関与

国は、評価機関における民間規格等の評価プロセス全体について、評価委員会への立会い等により確認するとともに、評価機関から評価の実施状況について１年ごとの定期報告を求め、評価する。

上記ポイントに基づき、電力安全小委員会にて以下の項目を実施。

- ➢ 候補となる機関が評価機関の要件を満たしていることの確認が必要になった場合には、本委員会にて審議。
- ➢ 年１回、評価機関の活動について本委員会に報告し、当該評価機関が民間規格を適切に評価・承認できることの確認を実施。

7-4. その他検査面での制度的措置の見直し事項①

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の整理を踏まえ**、以下の検査面での制度的措置の見直しを行うこととしてはどうか。

① B認定を対象とした肉厚測定の間隔等の見直し

現行の規定

- 現行の通常認定では、次回検査時期の設定について、KHK/PAJ/JPCA S 0851(2022)（以下「KHKS」という。）によることができると規定されているが、現行の通達※において、以下①～③等の読み替えを行い、KHKSよりも厳格な運用を行っている。

  ① 肉厚測定の間隔（肉厚測定検査における次回検査時期までの間隔。KHKS上最大4年とされているところ、通達により最大2年に厳格化。）
  ② 検査時期設定係数（次回検査時期を算出する際に余寿命に乗じる数値。KHKS上最大0.8とされているところ、通達により0.5に厳格化。）
  ③ 肉厚測定回数（減肉速度の算定時に必要とされる肉厚測定の回数。KHKS上計3回分とされているところ、通達により計5回分に厳格化。）

※「認定完成検査実施者及び認定保安検査実施者の認定について」

見直し理由

- 通達においてKHKSを厳格に読み替える旨の運用を行った背景としては、本制度導入当時（2011年）、肉厚測定の間隔を１年以上に延長することが初めての試みであったことから、慎重を期す必要があるとの判断に基づくもの。
- **当該規定の制定から既に10年以上が経過し、この間、技術的不都合や安全性への懸念は生じていないことから、これを見直し、KHKSで定められている基準を適用する**ことが適切。

見直し後の措置

- B認定（通常認定相当）では、KHKSを現行の厳格に読み替える旨の運用は見直し、次回検査時期の設定について、KHKSによることができることとする。

7-5. その他検査面での制度的措置の見直し事項②

- **産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の整理を踏まえ**、以下の検査面での制度的措置の見直しを行うこととしてはどうか。

② KHKへの腐食環境や厚さ測定等のデータ提出義務の廃止

現行の規定

- 現行のスーパー認定事業者のうちCBM認定を受けている事業者に対しては、腐食環境や肉厚測定等のデータを定期的に高圧ガス保安協会に提出する義務が課せられている。

※「特定認定事業者及び自主保安高度化事業者の認定について」

見直し理由

- 腐食環境や肉厚測定等のデータ提出義務を課すこととした背景は、本制度導入当時（2019年）、開放検査の実施時期の設定についての柔軟化措置を講じることが初めての試みであったところ、制度導入初期は慎重な運用を期す必要があるとの判断に基づくもの。
- **当該規定の制定から一定期間が経過し、この間、技術的不都合や安全性への懸念は生じていないことから、これを廃止する**ことが適切。

見直し後の措置

- 高圧ガス保安協会への腐食環境や肉厚測定等のデータの提出義務は廃止する。

経済産業省

資料１

別添１３

高圧ガス保安法における
新たな認定制度の詳細設計について②

2023年２月24日

高圧ガス保安室

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の要件

３．新たな認定制度の特例

４．新たな認定制度の審査体制

５．A認定事業者向けの特例措置

1-1. 主な審議事項と施行に向けたスケジュール

- 今回は、主な審議事項のうち、青塗の項目を御審議いただく。

主な審議事項

制度総論	制度コンセプト・対応方針
	ターゲット
認定要件	要件の全体像
	要件１：経営トップのコミットメント
	要件２：高度なリスク管理体制
	要件３：テクノロジーの活用
	要件４：サイバーセキュリティなど関連リスクへの対応
認定特例	規制の特例措置
	A認定事業者向け特例措置
認定審査	審査体制
	認定更新期間

施行に向けたスケジュール（想定）

◇2022年
12月15日　高圧ガス小委員会①

◇2023年
２月24日　高圧ガス小委員会②
主な審議項目：青枠の項目
小委員会①の審議事項の深堀り

３月24日　高圧ガス小委員会③
主な審議項目：とりまとめ
※必要に応じて追加開催

◇2023年６月頃　政令・省令等の公布

◇2023年12月頃　施行

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の要件

３．新たな認定制度の特例

４．新たな認定制度の審査体制

５．A認定事業者向けの特例措置

2-1. 新たな認定制度の要件（総論）

- 新たな認定制度の要件（改正高圧法第39条の14第1項）は、スマート保安の促進の観点から、サイバー対策を含む**４つの要件で構成**する。
- 認定要件①～③については、前回の高圧ガス小委員会でご審議いただいたため、今回は「④サイバーセキュリティなど関連リスクへの対応」の要件を取り上げる。

出典:産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.８

（※）下記の表における赤字の下線部及び赤枠は、新たな制度的措置の認定基準において、現行の認定基準から拡充するものを示す。

	A 認 定	B 認 定
①経営トップのコミットメント	現行スーパー認定事業者制度の要件に加え、 コンプライアンス体制の整備（注1）、コーポレート・ガバナンスの確保	
②高度なリスク管理体制	現行スーパー認定事業者相当	現行通常認定事業者相当
③テクノロジーの活用	現行スーパー認定事業者制度における仕組み（注2）を基本とする ※認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用。	
④サイバーセキュリティなど関連リスクへの対応	各業界におけるサイバーセキュリティガイドライン（注3）に沿った内容とする	

（注1）高圧ガス保安法についての**法適合性確認能力**（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。
（注2）特定認定事業者及び自主保安高度化事業者の認定について (20201218保局第1号) における認定の基準 「二 先進的な技術を適切に活用していること」の項目を参照。
（注3）「重要インフラにおける情報セキュリティ確保に係る安全基準等作成指針」（内閣官房内閣サイバーセキュリティセンター）を参考に業界団体が定める「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」、「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」。

2-2. 新たな認定制度の要件（認定要件４：サイバーセキュリティなど関連リスクへの対応）

論点

- ✓**石油・化学等の重要インフラ事業者**※1**は、サイバーセキュリティの確保に努める**とされている（**努力義務**）※2。

※1　重要インフラ事業者には、情報通信、金融、航空、医療、水道、物流、石油、化学、電力、ガス等が指定されている(内閣サイバーセキュリティセンター「重要インフラのサイバーセキュリティに係る行動計画」別紙１より）。

※2　サイバーセキュリティ基本法(平成二十六年法律第百四号)
第六条　重要社会基盤事業者は、（中略）サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める（以下略）。

- ✓本要件は現行の認定制度にはない**新設の要件**。また、現在認定を取得している化学分野の事業者の中には、業界団体が作成した**サイバーセキュリティガイドラインが適用されない事業者も一定数存在**。

- ✓改正高圧法において、**認定要件は「保安の確保のための組織」に着目**することとしている。**内閣サイバーセキュリティセンターの安全指針**※**は、PDCAサイクルに沿った対策**を記載しており、これを踏まえることが必要。

※　内閣サイバーセキュリティセンター「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」

- ✓高圧ガス保安法の法目的を踏まえ、対象は**生産管理システム又はプラント制御システムのサイバーセキュリティ対策**とする必要。

産構審　分科会報告書における記載

サイバーセキュリティなど関連リスクへの対応「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（内閣官房内閣サイバーセキュリティセンター）において、石油・化学分野は重要インフラ分野とされており、この指針を参考に石油・化学分野の業界団体がサイバーセキュリティガイドラインを策定しているため、これに沿った内容とする。すなわち、**「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」**や**「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」に沿った内容**とする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.17）

検討の視点

- サイバーセキュリティなど関連リスクへの対応の要件は、**組織や体制に着目**した要件とする。具体的には、**PDCAサイクルが構築されていること**を要件とし、事業者が、**技術の進展等に応じて自主的に**、生産管理システム又はプラント制御システムに対する**サイバー攻撃等のリスクへ対応する体制を維持・改善する仕組みがあることを確認**する。

- 本要件は新設の要件であるため、**初回の認定審査時には一定の配慮**を行う（詳細は次ページ）。

2-3. 新たな認定制度の要件（認定要件４：サイバーセキュリティなど関連リスクへの対応）

- 検討の視点を踏まえ、サイバーセキュリティなど関連リスクへの対応の要件は、以下としてはどうか。また、今後、業界ガイドラインの改訂※等を踏まえて、**必要に応じて見直す**こととしてはどうか。

※ 2022年６月、サイバー基本法第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、「重要インフラのサイバーセキュリティに係る行動計画」（サイバーセキュリティ戦略本部）が策定された。今後、内閣サイバーセキュリティセンターにおいて「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」が策定され、業界別サイバーセキュリティガイドラインについても、業界団体において見直しすることが予定されている。

- また、初回の認定審査時においては、**審査方法等に一定の配慮を講じる**こととしてはどうか。

検討の視点を踏まえた認定要件（案）

１　生産管理システム又はプラント制御システム（以下「対象システム」という。）のサイバーセキュリティ対策に係る計画の策定及び体制の構築（Plan）

①対象システムを含むサイバーセキュリティ対策に係る基本方針が明確に定められ、かつ、文書化されていること。

②対象システムのサイバーセキュリティに関するリスクを特定していること。

２　対象システムのサイバーセキュリティ対策の実施（Do）

①対象システムのサイバーセキュリティに関して特定したリスクについて、必要に応じて、対策を講じていること。

３　継続的改善の実施（Check/Act）

①対象システムのサイバーセキュリティ対策を定期的に自己評価していること。

②自己評価の結果等を踏まえ、対象システムのサイバーセキュリティ対策の見直しを行っていること。

※初回の認定審査時における配慮事項

初回の認定審査時には、「１ 生産管理システム又はプラント制御システムのサイバーセキュリティ対策に係る計画の策定及び体制の構築（Plan）」のうち、「①対象システムを含むサイバーセキュリティ対策に係る基本方針が明確に定められ、かつ、文書化されていること」を確認し、その他の要件については、今後の対応予定時期計画を提出しその内容を確認することでも代替可能とする等の配慮を行う。

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の要件

３．新たな認定制度の特例

４．新たな認定制度の審査体制

５．A認定事業者向けの特例措置

3-1. 新たな認定制度の特例（総論）

- **新たな認定制度の認定事業者に対しては**、製造施設の位置・設備等の変更の手続や危害予防規程・保安人員に関する手続等について、**事業者の保安力に応じて、届出等の手続の不要化や事業者自身による検査等を柔軟に措置（記録保存義務は維持）**。

製造施設の位置・設備等の変更の許可・届出

- 現行法では、軽微変更を除き、製造施設の位置・設備等の変更（設備変更）には都道府県知事又は政令指定都市の長の許可が必要

- 新たな認定制度の認定事業者においては、その保安確保能力を踏まえ、**ガス種の変更又は製造能力が一定以上変更される場合など重要な変更**については、**許可制を維持**
- **軽微変更**については、その対象範囲を拡大した上で**記録保存義務**とする
- **それら以外の変更**は、事故時・法令違反時に行政が迅速に対応することを可能とするため、**行政による事業者情報の把握の観点から、事後届出**とする

完成検査・保安検査

- 現行の認定事業者制度と同様に**自主検査**を維持
- その際、新たな認定制度では、法適合性確認能力も含め、コンプライアンス体制の整備等の要件を拡充すること等も踏まえ、**事業者が自ら完成検査・保安検査の結果を適正に確認**するものとし、検査記録については都道府県知事への**届出を要しない**こととする
- ただし、行政が立入検査等により確認できるよう、**検査記録を保存**
- 保安検査については、**定期に行うことを基本としつつ**、**CBMや常時監視等**による場合には、**それ以外の時期によることも可能**とし得るよう措置

保安人員（保安係員等）の配置

- 現行法では、「製造のための施設の区分ごとに」保安人員を配置

- 新たな認定制度の認定事業者においては、これを基本としつつも、コンビナート連携の進展や、常時監視・遠隔監視システムの導入などを踏まえ、法律上は「製造のための施設の区分ごとに」とせず、**保安人員の柔軟な配置**を許容し、**必要人員の配置の適正化について検討**

危害予防規程の届出・保安人員（保安係員等）の選解任の届出

- 新たな認定制度における認定事業者は、危害予防規程の作成・変更や、保安人員の選解任については、自立的に管理するものとし、**記録保存**とする

定期自主検査

- 定期自主検査は、保安検査を補完する検査であり、その対象施設は保安検査の対象施設と同様にガス設備が基本／検査項目も重複的
- 自立的に高度な保安管理を行うことができるため、保安検査の実施を前提に、認定事業者には**定期自主検査の規定を適用しない**

出典：産構審保安・消費生活用製品安全分科会報告書（令和3年12月）の概要　P.９より抜粋

3-2. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

論点

- ✓ **ガス種の変更又は製造能力が一定以上変更される場合など、製造施設に与える影響が大きい工事や製造の方法の変更**については、安全性を確保する観点から、許可とすることが妥当。
- ✓ **軽微変更については記録保存とするものの、処理能力の変更を伴うものについては、事故時・法令違反時に行政が迅速に対応することを可能とする観点から、事後届出とすることが妥当。**
- ✓ 誤解を防止し、新制度の円滑な運用を確保する観点から、制度全体について**分かりやすさを確保**する必要。

産構審　分科会報告書における記載

現行法では、認定事業者・非認定事業者を問わず、軽微変更を除き、製造施設の位置・設備等の変更（設備変更）には都道府県知事又は政令指定都市の長の許可を受ける必要がある。**新たな認定制度の認定事業者においては**、その保安確保能力を踏まえ、**ガス種の変更又は製造能力が一定以上変更される場合など重要な変更については許可制を維持**しながらも、**軽微変更についてはその対象範囲を拡大した上で記録保存義務**とする。**それら以外の変更**については、事故時・法令違反時に行政が迅速に対応することを可能とするため、**行政による事業者情報の把握の観点から、事後届出（速やかに／変更後30日以内）**とすることとする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.18）

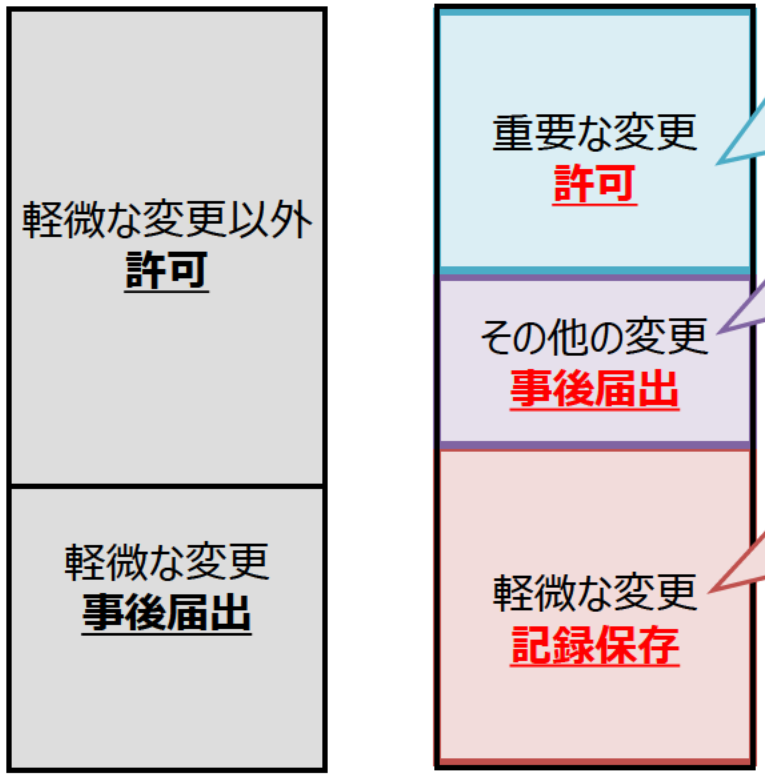
検討の視点

- 製造施設の位置・設備等の変更の許可・届出等の特例の検討に際しては、以下の三つの視点を考慮する。
  - ✓ **工事の規模や製造施設に与える影響の大小**
  - ✓ **行政が事業者情報を把握する必要性**
  - ✓ **制度運用上の分かりやすさ**

3-3. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- 新たな認定制度における製造施設の位置・設備等の変更の許可・届出等は、完成検査との関係（詳細は次ページ）を含め、**新制度の円滑な運用を確保する観点から、以下の分類**としてはどうか。
- その際、**「重要な変更」と「軽微な変更」の内容については、省令等において限定列挙**するとともに、**その他の変更を含め詳細な解釈についても通達等で可能な限り明らかにする**ことで、わかりやすい制度とする。

製造施設の位置・設備等の変更の許可・届出等の分類（案）



重要な変更

【変更の工事】
- ✓ 特定変更工事※に該当する変更の工事

※高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）

【製造の方法の変更・ガス種の変更※】
- ✓ 常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）
- ✓ ガス種の変更※

※ガス種の変更は、製造のための施設等の変更の特例の対象外（改正高圧ガス保安法39条の21第１項参照）。

その他の変更（重要な変更と軽微な変更以外のもの）

【変更の工事の例】
- ✓ 処理能力の変更が一定(20%) 範囲内の変更の工事

【製造の方法の変更の例】
- ✓ 常用圧力・常用温度の変更（設計条件内での変更を伴うもの） 等

軽微な変更

【変更の工事】
- ✓ 現行の軽微変更に該当する変更の工事※（ガス設備の変更の工事等）

※処理能力の変更を伴うものは除く

【製造の方法の変更】
- ✓ 常用圧力・常用温度の変更を伴わない製造の方法の変更

※軽微な変更の工事における通常認定とスーパー認定の差異（コンビ則第14条第１項第７号等）は、新たな認定制度においても踏襲することを予定 。

3-4. 新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- **製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係は、以下の整理**としてはどうか。
- なお、完成検査の検査記録は、現状届出義務となっているところ、**新たな認定制度においては記録保存義務**となるため、**完成検査終了後、速やかに運転を開始することができる**。

製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係

現行の認定制度

変更の工事			
軽微な変更以外の変更	特定変更工事※1	許可	完成検査必要（事後届出）
	特定変更工事以外の工事		完成検査不要
軽微な変更※2		事後届出	完成検査不要
製造の方法の変更・ガス種の変更			
軽微な変更以外の変更		許可	完成検査不要

新たな認定制度

変更の工事			
重要な変更	特定変更工事※1	許可	完成検査必要（記録保存）
その他の変更	特定変更工事以外の工事	事後届出	完成検査不要
軽微な変更※2		記録保存	完成検査不要
製造の方法の変更・ガス種の変更※3			
重要な変更	✓ガス種の変更※3 ✓常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）	許可	完成検査不要
その他の変更	✓常用圧力・常用温度の変更（設計条件内での変更を伴うもの）	事後届出	完成検査不要
軽微な変更	✓常用圧力・常用温度の変更を伴わない製造の方法の変更	記録保存	完成検査不要

※1　高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）
※2　軽微な変更の工事の範囲については、今後、必要に応じて見直すことを想定。
※3　ガス種の変更は製造のための施設等の変更の特例の対象外（改正高圧ガス保安法第39条の21第１項参照）。

3-5. 新たな認定制度の特例（保安検査時期の柔軟化、定期自主検査義務の廃止）

保安検査時期の柔軟化

産構審　分科会報告書における記載

「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」については、現行の認定事業者制度と同様に自主検査を維持する。ただし、その際、新たな認定制度では、法適合性確認能力も含め、コンプライアンス体制の整備等の要件を拡充すること等も踏まえ、事業者が自ら完成検査・保安検査の結果を適正に確認するものとし、検査記録については都道府県知事への届出を要しないものとする。ただし、行政が立入検査等により完成検査・保安検査の状況を確認することができるよう、事業者は検査記録を保存するものとする。また、**保安検査については、**現行法上「定期に」行うことと限定されている。現時点では定期に行うことを基本とするものの、今後、CBMや常時監視等の導入が本格化することも想定し、新たな認定制度の認定事業者については、当該「定期に」との法律上の文言を削除する。この場合、**検査の時期については、経済産業省令で定めるものとし、具体的には、現時点では、定期に行うことを基本としつつ、CBMや常時監視等による場合には、それ以外の時期によることも可能とし得るよう措置する。**

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 保安検査は、**定期に行う**こととする。
- ただし、CBMや常時監視等の高度な情報通信技術の活用状況等を踏まえ、**保安の確保上問題がないと経済産業大臣が認める時期に行うことも可能**としてはどうか。

定期自主検査義務の廃止

産構審　分科会報告書における記載

定期自主検査は、第一種製造者等が保有する設備が技術上の基準に適合しているかの確認について、保安検査を補完する観点から規定されている検査である。また、認定対象となる第一種製造者については、定期自主検査の対象施設は保安検査の対象施設と同様にガス設備※1を基本とし、検査項目も重複的なものである※2。これらを踏まえ、新たな認定制度の認定事業者は、自立的に高度な保安管理を行うことができるため、保安検査の実施を前提に、**認定事業者には定期自主検査の規定を適用しない**こととする※3。

※1　ガス設備：高圧ガス製造施設のうち、製造をする高圧ガスのガス（その原料となるガスを含む。）の通る部分。

※2　定期自主検査の対象施設は、ガス設備（コンビ則第38条第2項）とされている。保安検査の対象施設は、告示で定める製造施設以外の製造施設（コンビ則第34条第1項）とされており、「製造施設の位置、構造及び設備並びに製造の方法等に関する技術基準の細目を定める告示」には、保安検査を受ける必要のない製造施設として、①ガス設備以外の製造施設、②ガス設備のうち次に掲げるもの（可燃性ガス及び毒性ガス以外のガス設備等）等が規定されている。

※3　現在、**定期自主検査でのみ検査を行っている項目についても、継続的に検査を行っていくことを担保するため、例えば、更新認定に当たって、継続的な改善事項として考慮**する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.20）

方針（案）

- 定期自主検査でのみ検査を行っている項目について、継続的に検査を行っていることを、**認定審査において確認**※することとしてはどうか。

※「認定完成検査実施者及び認定保安検査実施者の認定に係る事業所の体制の基準を定める告示」第10条第２項第４号ロ(1)の要件充足性を審査する際に確認することを予定。

3-6. 新たな認定制度の特例
（危害予防規程の届出義務・保安人員の選解任の届出義務の廃止、保安人員の配置の柔軟化）

危害予防規程の届出義務・保安人員の選解任の届出義務の廃止

産構審　分科会報告書における記載

新たな認定制度における認定事業者は、**危害予防規程の作成・変更や、保安人員の選解任については、自立的に管理するものとし、都道府県知事等への個別の届出は要しないものとする**。ただし、行政が立入検査等によりその実施状況を確認できるよう、**記録保存義務を課す**ものとする。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 危害予防規程の作成・変更や、保安人員の選解任は記録保存とされた。記録保存は、文書による保存方法に加え、**電磁的方法**によることも可能とする。
- 電磁的方法による記録保存は、**クラウド保存による場合も想定して、関連規程※を見直す**こととしてはどうか。

※「電磁的方法による保存等をする場合に確保するよう努めなければならない基準」

保安人員の配置の柔軟化

産構審　分科会報告書における記載

現行法では、「製造のための施設の区分ごとに」保安係員及び保安主任者を配置することになっている。新たな認定制度の認定事業者においては、これを基本としつつも、**コンビナート連携の進展や、常時監視・遠隔監視システムの導入などを踏まえ、法律上は「製造のための施設の区分ごとに」とせず、保安人員を柔軟に配置することを許容**するとともに、**必要人員の配置の適正化について検討**する。

（出典：産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.19）

方針（案）

- 保安人員の配置の方法は、高度な情報通信技術の活用状況等を踏まえて、個別具体の事例ごとに判断することが適切。
- このため、高度な情報通信技術の活用により、適切な監視体制が確保され、また、緊急事態への対応も可能であるなど、**適切な保安管理が行えると経済産業大臣が認める場合**に、**保安人員の柔軟な配置を許容する**こととしてはどうか。

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の要件

３．新たな認定制度の特例

４．新たな認定制度の審査体制

５．A認定事業者向けの特例措置

4-1. 新たな認定制度における審査体制に関する論点

● 新たな認定制度における審査体制について、下記の論点を検討する。

論点①　調査依頼制度の詳細

出典:産構審保安・消費生活用製品安全分科会高圧ガス小委員会（令和4年12月）
資料２　P.22より抜粋

- ✓ **対象とする範囲**
- ✓ **指定機関の要件**
- ✓ **初回申請時の扱い**

【産構審分科会報告書における記載】

国は、国の検査及び審査会審査を行う案件のうち、必要と認めたときは、その範囲を定めて、KHK又は指定機関に意見を聴取し、又は調査を依頼できるものとする。KHK等の調査が行われた場合、国の検査は、その範囲で省略され、重複の検査・調査は行わない。KHK等が一部の調査を行う場合、運用上は、国とKHK等は一緒に（一回で）検査・調査を行う。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

論点②　審査会審査の詳細

- ✓ **審査方法**
- ✓ **委員構成**

【産構審分科会報告書における記載】

〇新規認定：全数を国の検査及び審査会審査（注）を行う。
〇更新：国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況等を踏まえ安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査（注）を行う。

（注）審査会審査：外部有識者（KHK、高圧ガスやIoT等のテクノロジーに関する学識経験者等）からなる審査会で行う審査

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.24 図21）

論点③　更新時に現地調査・審査会審査を実施する場合の基準

- ✓ **認定更新時に、現地調査・審査会審査を実施する場合の基準**

【産構審分科会報告書における記載】

更新では、国が、一次的審査（書面審査・ヒアリング）で全ての認定基準を確認した上で、新規認定以降の事故の発生状況や法令違反（労安法等含む）、行政指導等の有無、また、大幅な変更（設備構成・製造能力・ガス種等）の有無等を踏まえ、安全の確保及び向上の観点から問題がないと認められない場合には、国の検査及び審査会審査を行うものとする。

（出典：産業構造審議会　保安・消費生活用製品安全分科会　報告書（令和3年12月）P.25）

4-2. 論点① 調査依頼制度の詳細について

● **審査は国が行う**との方針を踏まえ、調査依頼制度の詳細は下記のとおりとしてはどうか。

✓ 調査依頼を行う場合

- **初回申請時**※及び**認定更新時に安全の確保及び向上の観点から問題がないと認められない場合**には、国は**調査依頼を行う**。
  ※現行の認定事業者が新たな認定制度を初めて申請する場合も含む。

✓ 調査依頼制度における調査の方針・対象とする範囲

- 経済産業大臣からKHK又は指定機関（以下「KHK等」という。）への調査依頼の対象は、書面審査及び現地調査とする。
- 書面審査及び現地調査では、事業所が認定要件を充足しているかについて確認・審査を行う。
- 調査依頼制度における確認・審査は、**国の責任の下、審査基準に示されている項目の範囲内で行うことを原則**とする。ただし、認定要件の範囲内であれば※、審査基準に示されていない視点であっても、確認・審査を行うことができる。
  ※安全の確保及び向上のための意見を述べることもできるが、要件充足性の判断に影響は及ぼさない。

✓ 現地調査への国（本省）の関与

- 国（本省）はKHK等が行う現地調査に参加し、審査をKHK等とともに行う。

✓ 指定機関の要件

- サイバーセキュリティの専門性の有無も考慮し、指定機関の要件を定める。

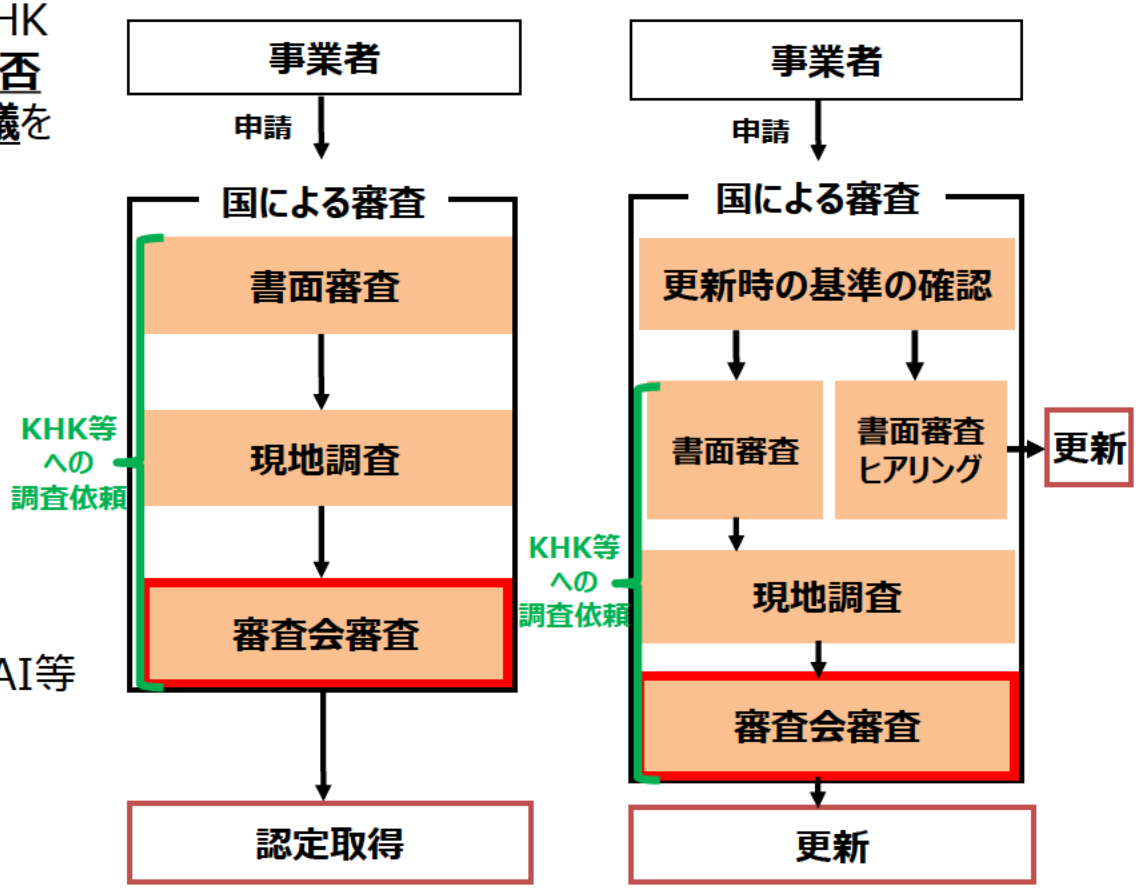
4-3. 論点② 審査会審査の詳細

● 審査会審査の審査方法及び委員構成は、下記のとおりとしてはどうか。

✓ 審査会審査の審査方法

- ４半期に一度開催する。
- 国及び調査依頼制度に参加する専門機関（KHK等）から**書面審査と現地調査の審査結果（合否等）を報告**する。その後、**審査結果について審議**を行う。
- 申請者（事業者）は不参加とする。
- **議事要旨は公開**※する。
  ※企業の機微情報を除いた上で作成。

【新規申請時の国の審査フロー】 【更新申請時の国の審査フロー】



✓ 審査会審査の委員構成

- **委員**

以下の分野の**外部有識者１０名程度で構成**する。
【外部有識者の主な分野】
✓ 学識経験者（高圧ガス、安全工学、IoT・BD/AI等のテクノロジー、サイバーセキュリティ）
✓ 企業法務（コンプライアンス）
✓ 企業ＯＢ等（実務経験者）
✓ 高圧ガス保安協会（ＫＨＫ） 等

- **オブザーバー**

✓ 申請事業所を管轄する地方自治体

4-4. 論点③ 更新時に現地調査・審査会審査を実施する場合の基準

- **新たな認定制度**においては、**国による書面審査・ヒアリングにより認定の更新を認める制度を新たに導入**する。
- その際、５年間（A認定の場合は７年間）の認定期間内に、**以下①～③の基準のいずれかに該当することとなった場合は、安全の確保及び向上の観点から問題がないと認められないと判断**し、現地調査及び審査会審査を行う。

更新時に現地調査・審査会審査を実施する場合の基準（案）

①事故や労働災害の有無

✓ **Ｂ２級※１以上の事故が発生**している事業所

✓ **死亡又は休業４日以上の労働災害※２が発生**している事業所

※１ 同一事業所において、Ａ級事故、Ｂ級事故又はＣ１級事故が発生した日から１年を経過しない間に発生したＣ１級事故（高圧ガスに係る事故に限る。）（「高圧ガス・石油コンビナート事故対応要領」３(2)）

※２ 従業員・協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

②法令違反の有無

✓ 高圧ガス保安法の法令違反が**２回※３以上**発生している事業所
（ただし以下の法令違反については**１回**）

① 死亡事故が発生したもの
② １００件を超えるような多数の法令違反を伴うもの
③ 国の行政処分が行われているもの
④ 国の行政文書による注意等が行われているもの

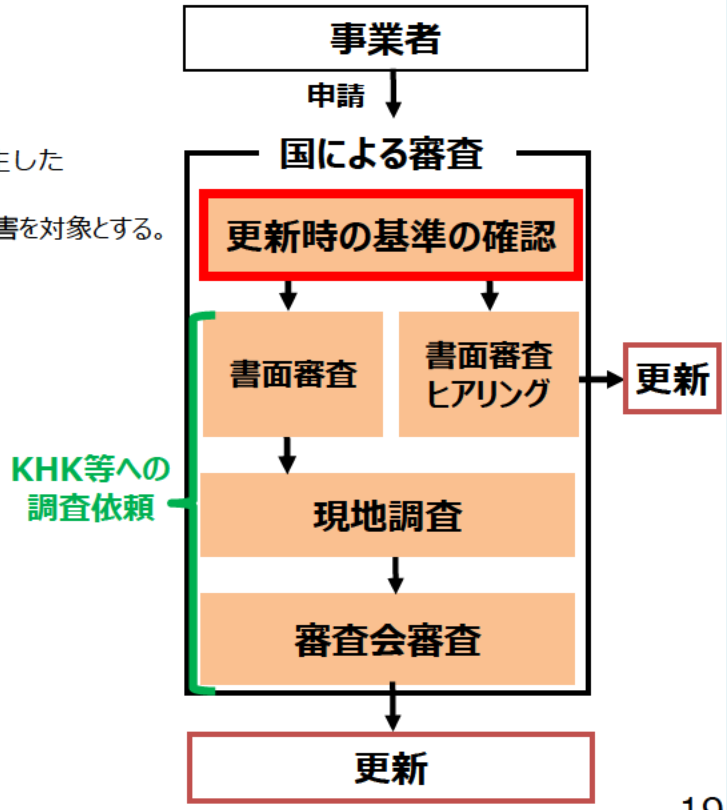
※３ 原則として、事業者からの報告数をカウントする。

③大幅な設備変更の有無

✓ **認定の対象に新たに高圧ガス製造施設を追加**する事業所※４

※４ 既存の認定施設において設備の変更工事が行われた場合、ガス種の変更等が行われた場合は含まない。

【更新申請時の国の審査フロー】



１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の要件

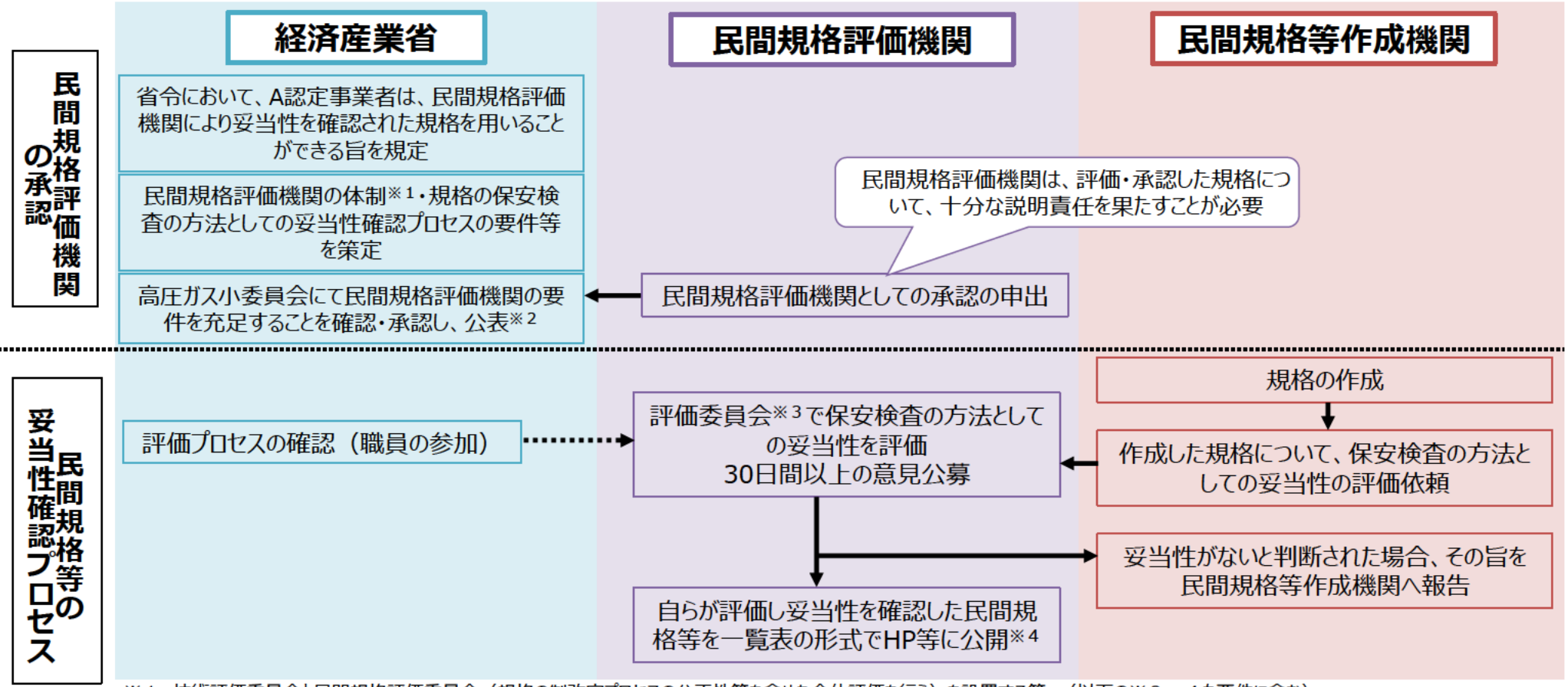
３．新たな認定制度の特例

４．新たな認定制度の審査体制

５．A認定事業者向けの特例措置

5-1. A認定事業者向けの特例措置（電力分野を参考とした新たな仕組みの導入）

- 第23回高圧ガス小委員会において、**A認定事業者を対象に、国が定める要件を満たす民間規格評価機関が承認した検査等に係る基準・規格であれば、高圧ガス保安法上の適切な検査方法と認めることとする仕組みを導入**する方針が了承された。
- 本仕組みを実現するため、**民間規格評価機関の要件を定める**ことが必要。



※1　技術評価委員会と民間規格評価委員会（規格の制改定プロセスの公正性等を含めた全体評価を行う）を設置する等。（以下の※２～４も要件に含む）
※2　国は、承認した民間規格評価機関の活動について、年に１回高圧ガス小委員会に報告し、当該民間規格評価機関が民間規格等を適切に評価・承認できることを確認。
※3　民間規格等に係る技術分野に加え、消費者問題、法律、ジャーナリズム等の幅広い分野の専門家から構成。
※4　規格として承認された日から少なくとも五年に一回は、改正、廃止又は確認が行われるよう適切に管理。

5-2. 民間規格評価機関の承認・要件適合性の確認

- 国は、**候補となる機関が民間規格評価機関の要件を満たすことを確認し、承認する**。
- 国は、承認した民間規格評価機関について、民間規格等の**妥当性確認プロセスが要件に従い運営されていることを確認**し、**必要があると認められる場合は改善指導等**を行う。
- 民間規格評価機関は、**年１回以上の外部評価**を受け、**妥当性確認プロセスが適切に運営されていることを自ら確認**し、必要に応じて改善策を講じる。

➢ 国による民間規格評価機関の承認

- 国は、高圧ガス小委員会において、候補となる機関が民間規格評価機関の要件を満たしているかどうかを確認し、承認する。
- 国は、国の審議会の議事録や、民間規格評価機関の要件等について確認した内容をホームページ等で広く公開する。

➢ 国による確認

- 国は、年に１回、民間規格評価機関の活動について高圧ガス小委員会に報告し、当該民間規格評価機関が民間規格等を適切に評価できることを確認する。

➢ 外部機関による評価

- 民間規格評価機関は、妥当性確認プロセスが適切に運営されていることを自ら確認するため（PDCAサイクルの構築）、外部評価を受け、その結果に基づく改善等を定期的に行う。

5-3. 民間規格評価機関における民間規格等の妥当性確認プロセス①

- 民間規格評価機関は、**技術評価委員会**（技術的な側面の評価を行う）及び**民間規格評価委員会**（規格の制改定プロセスの公平性、客観性及び透明性等を含めた全体的な評価を行う）を設置するなど、民間規格等の妥当性確認のための**十分かつ確実な評価体制を構築**する。

➢ 評価の方法

- 民間規格等の評価に当たっては、技術的な側面の評価を行う技術評価委員会と民間規格制改定プロセスの公平性、客観性及び透明性等を含めた全体評価を行う民間規格評価委員会を設置する。また、評価対象となる民間規格等に応じた適切な審議回数を確保することなどにより、十分な評価が行われるようにする。
- 評価対象となる民間規格等の作成に関与した専門家は評価に関与すべきではなく、これが確実に担保される措置を講じる。

➢ 技術評価委員会

- 民間規格等の技術的な側面の評価にあたっては、専門家、民間規格等を使用する事業者等（業界団体、エンジ会社、メーカー、検査会社等）も加える等、評価対象となる民間規格等に関係するできるだけ幅広い者の参加を必要とする。

➢ 民間規格評価委員会

- 民間規格等の評価にあたっては、規格内容の技術分野の専門家に加え、消費者問題、法律及びジャーナリズムを含む幅広い観点から評価を行う専門家の参加を必要とする。

5-4.民間規格評価機関における民間規格等の妥当性確認プロセス②

- 民間規格評価機関は、**民間規格等の保安検査の方法としての妥当性について評価**を行う。
- 民間規格評価機関は、妥当性を確認した民間規格等をリストに掲載し、**公開**する。
- **国は**、技術評価委員会と民間規格評価委員会への立合い等により、**民間規格評価機関における民間規格等の妥当性確認プロセス全体を確認する**。

➢ 評価の観点

- 民間規格評価機関は、当該民間規格等が技術の動向や関連する最新の知見を適切に踏まえているか等を踏まえた評価を行い、結果を評価書にとりまとめる。

➢ 妥当性を確認した民間規格等のリストへの掲載

- 民間規格評価機関は、評価書をとりまとめ、保安検査の方法としての妥当性を確認した民間規格等を、民間規格評価機関が公開する「民間規格評価機関が承認した民間規格等」のリストに掲載する。

➢ 妥当性確認プロセスにおける国の関与

- 国は、民間規格評価機関における民間規格等の妥当性確認プロセス全体について、技術評価委員会と民間規格評価委員会への立会い等により確認する。

経済産業省

資料３－１

別添１４

高圧ガス保安法における
新たな認定制度の詳細設計について③

2023年3月24日

高圧ガス保安室

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の特例

３．新たな認定制度の審査体制

４．A認定事業者向けの特例措置

1-1. 主な審議事項と施行に向けたスケジュール

- 今回は、これまで２回の高圧ガス小委員会における審議事項の深堀り等を行う。
- 今後、制度の円滑な施行に向けて、事業者・自治体向けの説明会を開催予定。

今回の主な審議事項

制度総論	制度コンセプト・対応方針
	ターゲット
認定要件	要件の全体像
	要件１：経営トップのコミットメント
	要件２：高度なリスク管理体制
	要件３：テクノロジーの活用
	要件４：サイバーセキュリティなど関連リスクへの対応
認定特例	規制の特例措置
	A認定事業者向け特例措置
認定審査	審査体制
	認定更新期間

施行に向けたスケジュール（想定）

◇2022年

12月15日　高圧ガス小委員会①

◇2023年

２月24日　高圧ガス小委員会②

３月24日　高圧ガス小委員会③
主な審議項目：小委員会②の審議事項の深堀り

５月頃　事業者・自治体向け説明会①
制度全体について

６月頃　政令・省令等の公布

10月頃　事業者・自治体向け説明会②
申請方法等について

◇2023年12月頃　施行

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の特例

３．新たな認定制度の審査体制

４．A認定事業者向けの特例措置

2-1. 新たな認定制度の特例（軽微な変更工事の範囲の拡大について）

- 産構審分科会報告書※において、「**軽微変更についてはその対象範囲を拡大**した上で記録保存義務とする」方針が示されている。

※産業構造審議会 保安・消費生活用製品安全分科会 報告書（令和3年12月）P.18

- 新たな認定制度における認定事業者が行う軽微な変更工事の範囲は、**事後届出の対象となる変更工事よりも危険性の低い工事**を対象とする。今般、具体的に軽微な変更工事の対象に追加する工事としては、現行制度において許可の対象となっている工事のうち、**現行の軽微な変更工事と同程度の危険性の部品の取替え工事**や、**高圧ガス設備の強度に影響のない変更工事**等を想定。

- なお、**新制度の円滑な運用を確保**する観点から、軽微な変更工事の範囲については、詳細な解釈を通達等において可能な限り明らかにすることを予定。

軽微な変更工事の対象に追加する工事

（現行認定事業者（通常・スーパー）・新認定事業者（A・B）共通）

①多管円筒形熱交換器以外（エアフィンクーラーを含む）の熱交換器のチューブの取替え

現行制度：特定設備に係る部品の取替えのうち、多管円筒形熱交換器のチューブの取替えが軽微な変更工事とされている

②フランジ継手以外の継手の変更

現行制度：認定事業者については、配管・バルブ・フランジ継手の単体又は組み合わせへの変更（処理能力及び設置位置の変更を伴わないもの）が、スーパー認定事業者については、これに加えて、附属機器類（特定設備を除く）も含んだ変更（処理能力の変更を伴わないもの）が、軽微な変更工事とされている（コンビ則14条１項７号二、８号ロ等）

③配管・バルブ・継手の変更に伴う配管の撤去工事

【参考】新たな認定制度の特例（製造施設の位置・設備等の変更の許可・届出等）

- **製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係は、以下の整理**としてはどうか。
- なお、完成検査の検査記録は、現状届出義務となっているところ、**新たな認定制度においては記録保存義務**となるため、**完成検査終了後、速やかに運転を開始することができる**。

製造施設の位置・設備等の変更の許可・届出等と完成検査の要否の関係

現行の認定制度

変更の工事			
軽微な変更以外の変更	特定変更工事※1	許可	完成検査必要（事後届出）
	特定変更工事以外の工事		完成検査不要
軽微な変更※2		事後届出	完成検査不要
製造の方法の変更・ガス種の変更			
軽微な変更以外の変更		許可	完成検査不要

新たな認定制度

変更の工事			
重要な変更	特定変更工事※1	許可	完成検査必要（記録保存）
その他の変更	特定変更工事以外の工事	事後届出	完成検査不要
軽微な変更※2		記録保存	完成検査不要
製造の方法の変更・ガス種の変更※3			
重要な変更	✓ガス種の変更※3 ✓常用圧力・常用温度の変更（設計条件を超える変更を伴うもの）	許可	完成検査不要
その他の変更	✓常用圧力・常用温度の変更（設計条件内での変更を伴うもの）	事後届出	完成検査不要
軽微な変更	✓常用圧力・常用温度の変更を伴わない製造の方法の変更	記録保存	完成検査不要

※1　高圧ガスの製造のための施設又は第一種貯蔵所の位置、構造若しくは設備の変更の工事（高圧ガス保安法第20条第３項）
※2　軽微な変更の工事の範囲については、今後、必要に応じて見直すことを想定。
※3　ガス種の変更は製造のための施設等の変更の特例の対象外（改正高圧ガス保安法第39条の21第１項参照）。

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の特例

３．新たな認定制度の審査体制

４．A認定事業者向けの特例措置

3-1.新たな認定制度の審査体制（高圧ガス小委員会での御指摘を踏まえた更新時の基準の変更点）

２月24日の事務局案における新たな認定制度の更新時に現地調査・審査会審査を実施する場合の基準の整理

- **新たな認定制度**においては、**国による書面審査・ヒアリングにより認定の更新を認める制度を新たに導入**する。
- ２月24日の事務局案では、労働災害は「**死亡又は休業４日以上の労働災害※が発生**している事業所」とすることを提示。

※ 従業員・協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

高圧ガス小委における御指摘事項

① 休業４日以上の労働災害には、**高齢者の腰痛、躓き、転倒等も含まれており、**こうした労災まで考慮すると、**高圧ガス製造施設の保安の維持・確保という制度趣旨から乖離**が生じる。

② **「休業４日以上の労働災害」の発生という基準は、範囲が広すぎる**。代替案として、重大労働災害の発生、としてはどうか。

③ 休業４日以上の労働災害は「プラント内（高圧ガス製造施設以外も含む）」で発生したものを対象としており、**高圧ガス製造設備以外の労働災害も考慮している点で厳しい**基準。重大事故を防止する観点から、災害等級・障害等級・強度率等の、より実態に即した基準の導入を検討いただきたい。

２月24日の事務局案の考え方

①新たな認定制度においては、合理的かつ迅速な認定審査へ移行しつつ、**安全確保を大前提に、認定審査を厳正に行う必要**がある。

②更新時の基準は、現地調査・審査会審査を省略する場合の基準であり、**認定更新が認められなくなるものではない**。

③分科会報告書において、認定更新時には、新規認定以降の事故の発生状況や法令違反（労安法等を含む）の有無等を踏まえることとしており、**労安法も考慮対象**の一つとしている。

御指摘を踏まえた修正案

- 労働安全衛生法において、**休業４日以上の労働災害**は、**遅滞ない報告が求められている**※1ほか、**ボイラー等の開放検査周期に係る認定制度の認定要件においても考慮**※2されている。また、更新時に現地調査・審査会審査が省略されるのは、特に優れた保安体制を備えた事業所のみを対象とすることが適切であるところ、**事業所全体の保安力を適切に評価する観点**からは、**高圧ガス製造施設以外で発生した労働災害も対象とすることが適切**。

- なお、高圧ガス小委員会での御指摘を踏まえて、交通事故や腰痛、躓き等の**事業所の安全管理と関係が希薄なものは除外することとしてはどうか。**

※１ 労働安全衛生法第100条第1項、労働安全衛生規則第97条第1項
※２ 「ボイラー等の開放検査周期に係る認定制度について」

【参考】論点③ 更新時に現地調査・審査会審査を実施する場合の基準

- **新たな認定制度**においては、**国による書面審査・ヒアリングにより認定の更新を認める制度を新たに導入**する。
- その際、５年間（A認定の場合は７年間）の認定期間内に、**以下①～③の基準のいずれかに該当することとなった場合は、安全の確保及び向上の観点から問題がないと認められないと判断**し、現地調査及び審査会審査を行う。

更新時に現地調査・審査会審査を実施する場合の基準（案）

①事故や労働災害の有無

✓ **Ｂ２級※１以上の事故が発生**している事業所

✓ **死亡又は休業４日以上の労働災害※２が発生**している事業所

※１ 同一事業所において、Ａ級事故、Ｂ級事故又はＣ１級事故が発生した日から１年を経過しない間に発生したＣ１級事故（高圧ガスに係る事故に限る。）（「高圧ガス・石油コンビナート事故対応要領」３(2)）

※２ 従業員・協力会社の社員について、認定事業所のプラント内（高圧ガス製造施設以外も含む）で発生した労働災害を対象とする。

②法令違反の有無

✓ 高圧ガス保安法の法令違反が**２回※３以上**発生している事業所
（ただし以下の法令違反については**１回**）

① 死亡事故が発生したもの
② １００件を超えるような多数の法令違反を伴うもの
③ 国の行政処分が行われているもの
④ 国の行政文書による注意等が行われているもの

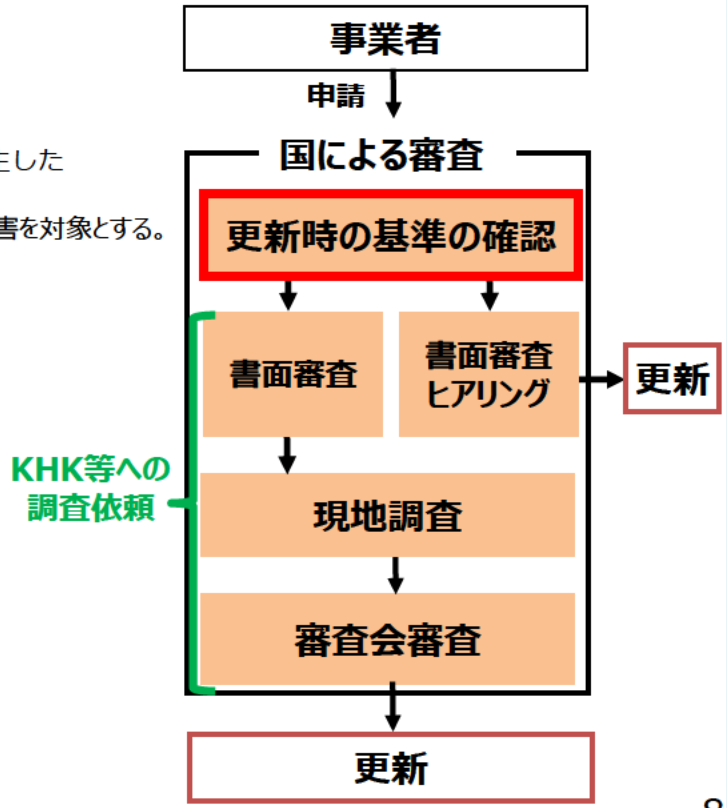
※３ 原則として、事業者からの報告数をカウントする。

③大幅な設備変更の有無

✓ **認定の対象に新たに高圧ガス製造施設を追加**する事業所※４

※４ 既存の認定施設において設備の変更工事が行われた場合、ガス種の変更等が行われた場合は含まない。

【更新申請時の国の審査フロー】



3-2. 新たな認定制度の審査体制（審査基準の作成･公開）

- 認定審査の透明性を確保する観点から、すべての認定要件について、認定審査時の**評価の視点**と**確認する書類の例**を明らかにした**審査基準を作成し公開**する。
- 審査基準は、今後、関係者の意見を参考に、国が作成する。

審査基準のイメージ

認定の基準	確認する書類	評価の視点
● 法人の代表者によって、保安の確保に関する理念、基本方針等の諸施策が明確に定められ、かつ、文書化されていること。また、これらの諸施策が各事業所等の全ての就業者に理解され、実施され、かつ、維持されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 経営理念が記載されたもの ✓ 基本方針が記載されたもの ✓ 社員へイントラネット、カード等により配信・配布している又は社内掲示しているもの ✓ 保安に係る諸施策についての、経営層と現場従業員との対話やアンケート等の実績	● 法人の代表者によって、経営理念、基本方針が系統立って作成されており、本社の姿勢、保安活動への経営者のコミットメントが示されている。 ● 全ての就業者が経営理念等を理解できるような取り組みを行っている。
● 役員を長とする保安対策本部等が設置されており、保安管理の基本方針の決定、各事業所ごとの保安管理実績の検討等の実施について明確に定められ、文書化され、かつ、適切に実施されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 本部等の設置規程等 ✓ 保安管理の基本方針の決定及び各事業所ごとの保安管理実績の検討等が分かるもの	● 保安対策本部等が設置されており、組織、メンバー構成、設置目的等を示す規程・基準類が整備されている。 ● 取締役（指名委員会等設置会社においては執行役）が長となっている。 ● 保安対策本部等において、保安活動を定期的に計画し、その実績を評価している。
● 保安管理部門が設置されており、生産計画、設備管理計画等に当該部門の意見が十分に反映されることが、明確に定められ、文書化され、かつ、意見が十分反映されていること。	● 要件を満足することを示した説明文書であって、例えば以下のもの。 ✓ 職務分掌規程等 ✓ 安全環境計画、生産計画及び設備管理計画等に保安管理部門の意見が反映されていることを示す会議議事録 ✓ 保安管理部門から社内外の保安関連情報（重大事故情報を含む）を展開し、それを踏まえて対応を行ったことを示すもの	● 保安管理部門が設置されている。 ● 安全環境計画、生産計画及び設備管理計画に保安管理部門の意見が反映されている。

3-3. 新たな認定制度の審査体制（新たな認定制度における審査期間の目安）

- 新たな認定制度における認定審査は**４半期単位で実施**することを予定。
- **申請が経済産業省に到達してから国が当該申請に対する処分をするまでに要する期間**は**４か月程度**（認定更新時に現地調査・審査会審査を行わない場合は**３カ月程度**）を想定※。

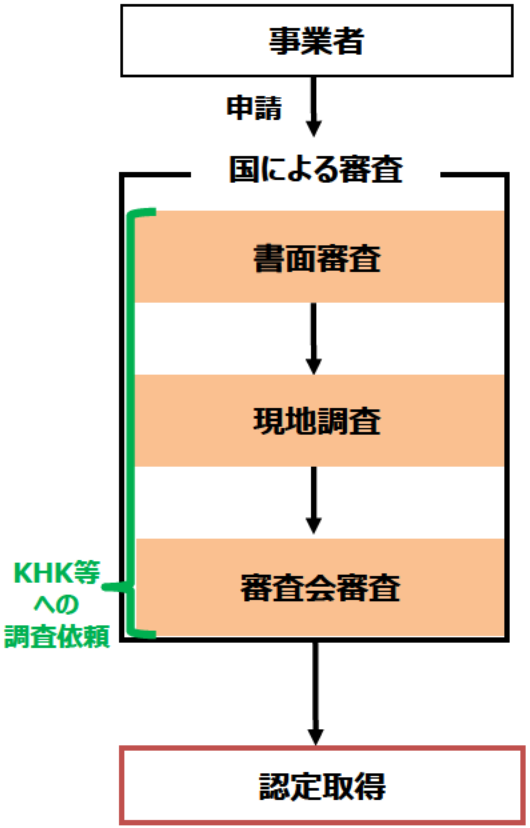
※申請者が国の審査に協力した場合の目安期間。なお、申請書類に重大な漏れがあった場合など、事業者側の要因により審査が長引く可能性あり。

新規※１の場合

スケジュールのイメージ

（８月頃～11月頃に認定更新期限を迎える事業者を想定）

４月中旬
申請書の提出
５月中旬～６月中旬
現地調査
７月中旬
審査会審査
８月上旬
大臣認定証の交付



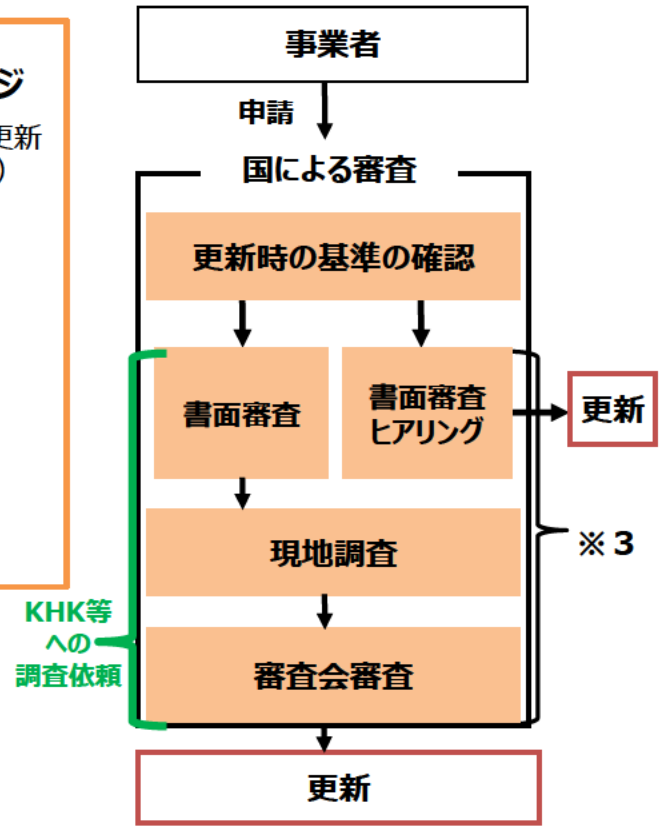
更新の場合※２

（現地調査・審査会審査が省略される場合）

スケジュールのイメージ

（７月頃～１０月頃に認定更新期限を迎える事業者を想定）

４月中旬
申請書の提出
５月中旬～６月中旬
国のヒアリング
７月上旬
大臣認定証の交付



※１　新規でA・B認定を受ける場合（ただし、現行認定を受けている者の新制度認定審査では、特に変更点を重点的に審査）
※２　更新時に現地調査・審査会審査を実施する場合は、新規の場合と同様のスケジュールを想定。
※３　特に変更点を重点的に審査

１．主な審議事項と施行に向けたスケジュール

２．新たな認定制度の特例

３．新たな認定制度の審査体制

４．A認定事業者向けの特例措置

4-1. A認定事業者向け特例措置（今後の進め方）

- これまで2回の高圧ガス小委員会の審議において、民間規格評価機関は**技術評価委員会**（技術的な側面の評価を行う）及び**民間規格評価委員会**（規格の制改定プロセスの公平性、客観性及び透明性等を含めた全体的な評価を行う）を設置するなど、民間規格等の妥当性確認のための十分かつ確実な評価体制を構築する方針が了承された。
- 上記内容を含む**民間規格評価機関の要件案（別紙）**について、御確認いただきたい。
- 今後、高圧ガス小委員会において、候補となる機関が評価機関の要件を満たしていることを確認した上で国が承認を行うほか、年に１度（３月頃）、民間規格評価機関の活動内容を確認する。
- なお、現行のスーパー認定事業者についても、民間規格評価機関が妥当性を確認した規格を活用することができる。

今後のスケジュールイメージ

