経済産業省 御中

令和２年度重要技術管理体制強化事業（産業競争力強化法に基づく技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業）報告書

2021 年 3 月 26 日

株式会社三菱総合研究所
デジタル・イノベーション本部

目 次

図 目 次

表 目 次

1. 背景・目的

1.1 背景

グローバルな競争が進む中で、技術等の情報の適切な管理は、事業者間での技術等の情報の共有の円滑化やイノベーションの促進の観点等から重要となっている。産業界におけるオープンイノベーション等の他者との連携を深める動きを促していくためには、適切な技術等の情報の管理に係る認証制度（産業競争力強化法に基づく技術情報管理認証制度。以下、「認証制度」という。）の普及を進めていくことが不可欠である。

1.2 目的

本事業では、中小企業等も含めた我が国産業界全体における技術等の情報の適切な管理を促進するため、認証制度を広めていくことを目的とする。

1.3 調査概要

適切な管理をすべき技術等の情報の漏えい防止措置（以下、「漏えい防止措置」という。）に係る具体的なアドバイスや漏えい防止措置の内部監査等を希望する事業者等（以下、「依頼者」という。）に対して、認証制度を広め、中小企業等における技術等の情報の適切な管理を促進するため、専門家を派遣した。また、本制度に関連した調査・広報活動を実施した。

具体的な実施事項は、以下の通りである。

1.3.1 専門家派遣の実施

専門家派遣については以下 3 つの具体的なニーズに、それぞれ対応して実施した。

① 適切な管理をすべき技術等の情報の特定やその漏えい防止措置に係るアドバイス

適切な管理をすべき技術等の情報の特定や、国が示す基準（「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」。以下、「認証基準」という。）に沿った具体的な漏えい防止措置の実施方法が課題となっている事業者に対して、具体的な対応方法や漏えい防止措置等について提案・アドバイス等を実施。

② 実施している漏えい防止措置に係る内部監査

事業者が実施している認証基準に沿った漏えい防止措置について、その漏えい防止措置が適切に行われているかについての認証手法（「技術等情報漏えい防止措置認証業務の実施の方法」）に沿った内部監査等を実施。

③ 業界等における漏えい防止措置のモデル構築支援に係るアドバイス

認証基準に沿った漏えい防止措置の標準的なモデルの構築を検討する団体に対して、その標準的なモデルの検討等において参考となる情報の提供や具体的な対策の提案・アドバイス等を実施。

今年度は、募集開始時点から申込窓口を認定技術等情報漏えい防止措置認証機関（以下、「認証機関」という。）及び委託機関（株式会社三菱総合研究所）として窓口を広くするとともに、セミナー講師としての派遣や、認証取得または認証機関認定に係る申請書作成等の支援依頼等への派遣に対応することで、認証制度の普及を目指した。さらに、認証取得を目指す事業者に対して複数回の派遣を可とする等、事業者に対して手厚い支援を行った。

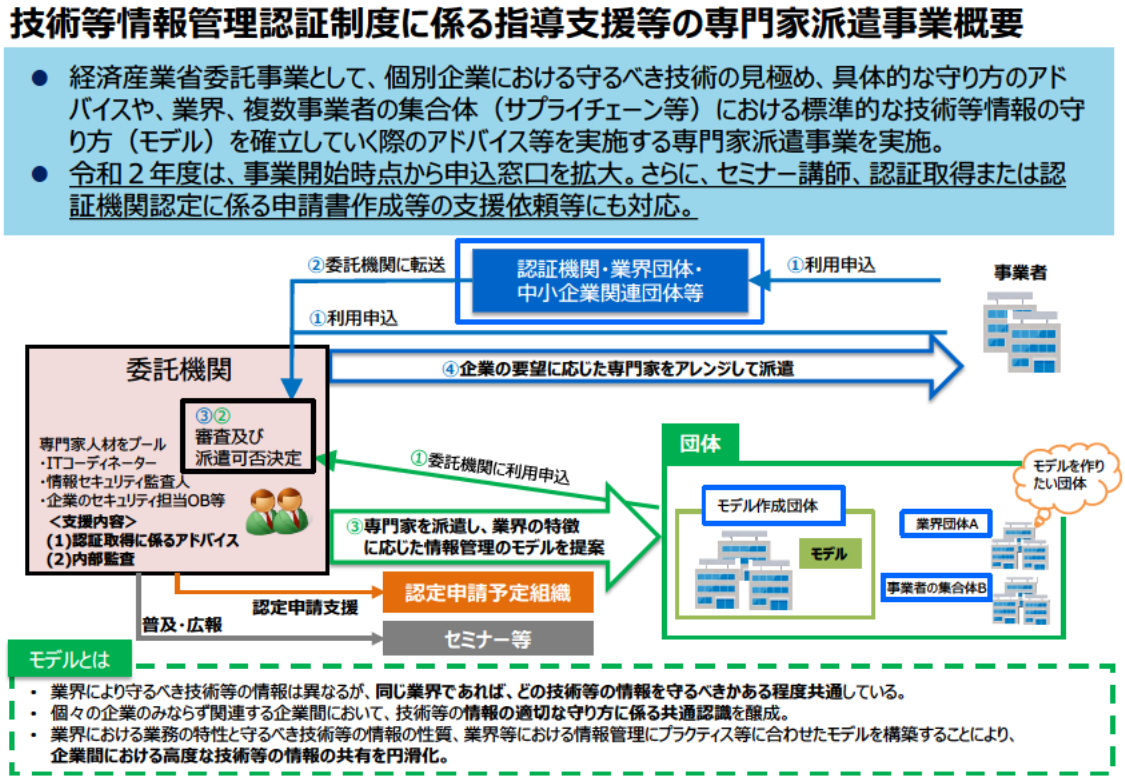


図 1-1　専門家派遣スキーム

1.3.2 専門家の派遣やその管理

派遣する専門家については、1.3.1 ①～③を実施できる人材として、情報セキュリティ・漏えい防止措置、及び情報セキュリティ監査についての知見をする者を、本事業を実施できる人数を確保した。

派遣する専門家に対しては、認証制度や基準、具体的な漏えい防止措置の実施方法の理解等のため、派遣前に研修受講の機会を設けた。

その後、研修を受講し派遣可能とした専門家のリストを作成した。その際、1.3.1 ①～③のどれを実施した人材かがわかるようにした。

1.3.3 専門家の派遣やその管理

依頼者からの申請については、委託機関（株式会社三菱総合研究所）への申請、及び 1.3.1 ①②に関しては、認証機関を通じた申請、1.3.1 ③を作成する予定の（又は作成した）団体

を通じた申請を受け付けた。

適切な管理をすべき技術等の情報の漏えい防止措置（以下「漏えい防止措置」という。）に係る具体的なアドバイスを求める事業者や漏えい防止措置の内部監査等を希望する事業者等（以下、「依頼者」という。）の依頼内容や意向を踏まえ、適切な専門家を派遣した。派遣した専門家には、実施した業務の報告書を作成いただき、依頼者には、派遣内容に関するアンケートを実施した。

1.4 海外動向等調査

認証制度に類似する諸外国における最新の政策動向等を文献及びヒアリングにて調査を実施し、認証制度との比較を行った。

1.5 普及のための広報活動等

認証制度の普及に向けた広報活動として、認証取得を目的とした事業者向けの研修素材やパンフレットを作成した。

また、既存の団体等が運用しているメールマガジンの配信及び説明会への講師派遣を実施した。

1.6 有識者会議等の運営

認証制度普及に向けた取り組みや、本事業の手法等について課題を洗い出し、改善の方向性について有識者会議及びワーキンググループを設置してとりまとめた。

1.6.1 有識者会議

(1) 設置目的

グローバルな競争が進む中で、技術等の情報の適切な管理は、事業者間での技術等の情報の共有の円滑化やイノベーションの促進の観点等から重要となっている。産業界におけるオープンイノベーション等の他者との連携を深める動きを促していくためには、適切な技術等の情報の管理に係る認証制度の普及を進めていくことが不可欠である。

この認証制度の普及を進めていくため、今後技術等の情報の適切な管理を取り組む中小企業等の事業者等への支援として、適切な管理をすべき技術等の情報の漏えい防止措置に係る具体的なアドバイスを求める事業者や漏えい防止措置の内部監査等を希望する事業者等に対して、専門家を派遣する事業を実施することとしているところ、本事業を適切に実施していくためには、産業界、有識者、関係機関からの意見を踏まえて進める必要がある。

そこで、技術情報管理認証制度の普及に向けた課題の洗い出しや改善の方向性について取りまとめるために、産業界、有識者、関係機関等を委員として意見を聴く場として「技術等情報管理認証制度に係る検討会」を設置する。

(2) 設置期間

2020 年 10 月 6 日～2021 年 3 月 26 日

(3) 委員

座長	田中 芳夫	一般社団法人ものこと双発推進　代表理事
委員	及川 勝	全国中小企業団体中央会 事務局長/総務企画部長/人材育成部長
	小川　隆一	独立行政法人情報処理推進機構　セキュリティセンター セキュリティ対策推進部　セキュリティ分析グループリーダー
	土井 和雄	全国商工会連合会　政策推進部　事業環境課　課長
	中島 康明	独立行政法人中小企業基盤整備機構　経営支援部　部長
	永宮 直史	特定非営利活動法人日本セキュリティ監査協会 エグゼクティブフェロー
	比留間 貴士	特定非営利活動法人 IT コーディネータ協会　常務理事
	山内 清行	日本商工会議所　産業政策第一部　部長

（2021/3/26 時点、委員五十音順、敬称略）

(4) 開催概要

1) 第 1 回

日時	2020 年 10 月 6 日（火）13:00 - 15:00
場所	株式会社三菱総合研究所 4 階大会議室 D オンライン開催（Skype for Business）
議題	(1) 開会 (2) 経済産業省 挨拶 (3) 検討会の趣旨について (4) 検討会の取り扱いについて (5) 座長の互選 (6) 座長の挨拶 (7) 産業競争力強化法に基づく技術等情報管理認証制度に係る指導支援等の専門家派遣事業について (8) 検討会の進め方について (9) 今後のスケジュールについて

2) 第 2 回

日時	2021 年 2 月 10 日（水）10:00 - 12:00
場所	オンライン開催（Skype for Business）
議題	(1) 開会 (2) 技術情報管理認証制度の普及促進に向けた今後の取組について (3) 認証制度に関連する国内外動向等調査結果について

	(4) 認証制度における監査について (5) パンフレットについて (6) 専門家派遣の状況 (7) 報告書骨子案 (8) 今後のスケジュールについて

3) 第 3 回

日時	2021 年 3 月 19 日（金）10:00 - 12:00
場所	オンライン開催（Skype for Business）
議題	(1) 開会 (2) 技術情報管理認証制度の普及促進に向けた今後の取組について (3) 報告書案について (4) 今後のスケジュールについて

1.6.2 運用ワーキンググループ

(1) 設置目的

グローバルな競争が進む中で、技術等の情報の適切な管理は、事業者間での技術等の情報の共有の円滑化やイノベーションの促進の観点等から重要となっている。産業界におけるオープンイノベーション等の他者との連携を深める動きを促していくためには、適切な技術等の情報の管理に係る認証制度の普及を進めていくことが不可欠である。

この普及を進めていくため、今後技術等の情報の適切な管理に取む中小企業等の事業者等に対して専門家を派遣する事業を実施することとしているところ、支援を受けた事業者等の認証取得を促すためには、認証制度の円滑な運用や認証機関の活動の充実が必要であり、関係機関からの意見を踏まえて進める必要がある。

技術情報管理認証制度の運用に向けた認証機関に関わる課題の洗い出しや改善の方向性について取りまとめるために、認証機関等を委員として意見を聴く場として「技術等情報管理認証制度に係る検討会運用ワーキンググループ」を設置する。

(2) 設置期間

2020 年 10 月 29 日～2021 年 3 月 26 日

(3) 委員

委員	金森 喜久男	一般社団法人情報セキュリティ関西研究所　代表理事
	小橋 弘政	日本検査キューエイ株式会社　取締役
	高村 博紀	一般財団法人日本品質保証機構　認証制度開発普及室　主幹
	中里 栄	一般社団法人日本金型工業会　専務理事
	羽田野 尚登	株式会社日本環境認証機構 IS ビジネスユニット審査グループ長
	六畑 方之	公益財団法人防衛基盤整備協会　情報セキュリティ部長

（2021/3/26 時点、委員五十音順、敬称略）

(4) 開催概要

1) 第 1 回

日時	2020 年 10 月 29 日（木）17:00 - 19:00
場所	オンライン開催（Skype for Business）
議題	(1) 開会 (2) 経済産業省 挨拶 (3) 運用ワーキンググループの趣旨について (4) 運用ワーキンググループの取り扱いについて (5) 産業競争力強化法に基づく技術等情報管理認証制度に係る指導支援等の専門家派遣事業について (6) 本事業の進め方について (7) 認証制度における監査の仕組みについて (8) 今後のスケジュールについて

2) 第 2 回

日時	2020 年 11 月 24 日（火）10:00 - 12:00
場所	オンライン開催（Skype for Business）
議題	(1) 開会 (2) 技術情報管理認証制度の普及促進に向けた今後の取組について (3) 認証制度における監査の仕組みについて (4) 今後のスケジュールについて

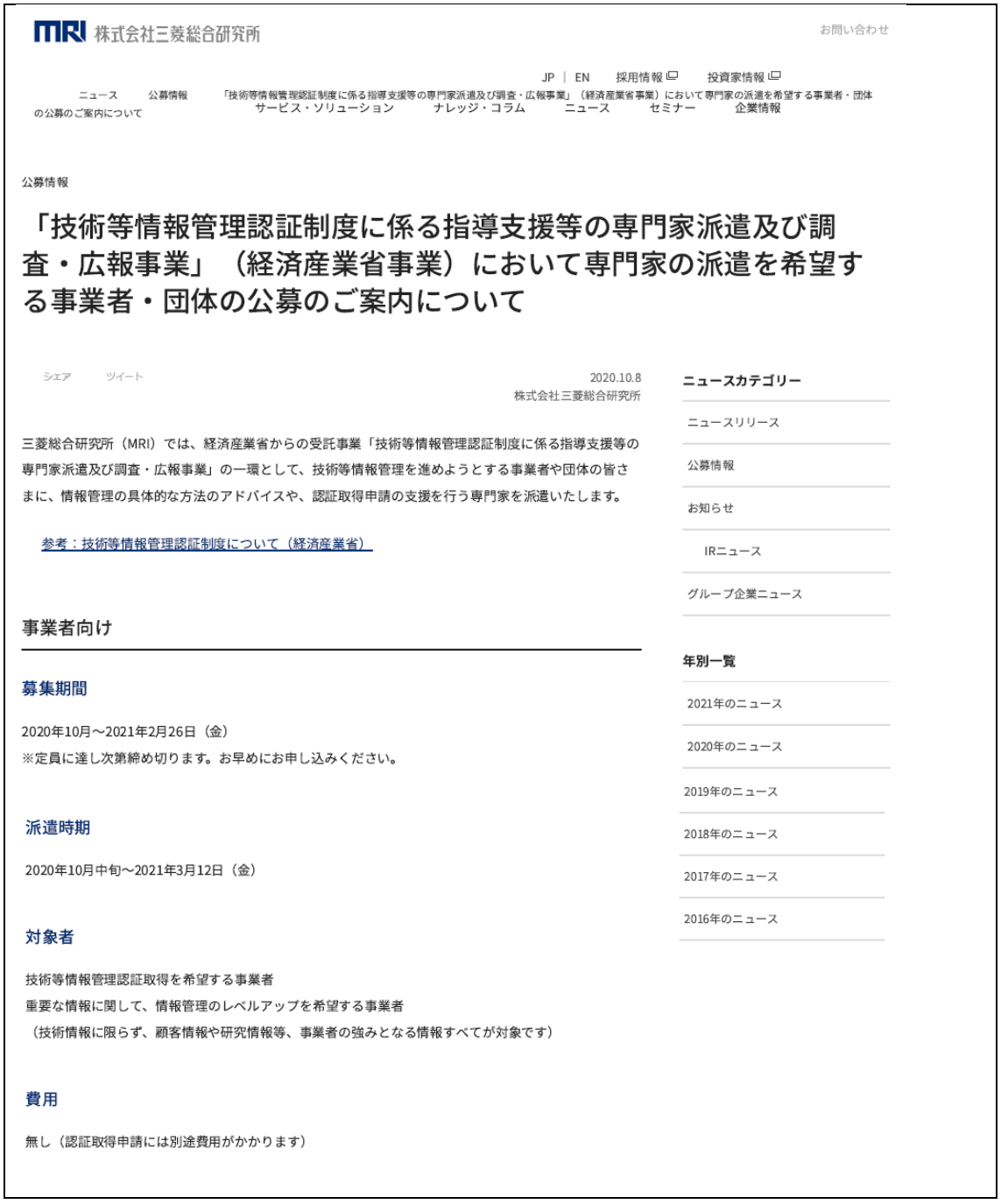
3) 第 3 回

日時	2020 年 12 月 21 日（月）13:00 - 15:00
場所	オンライン開催（Skype for Business）
議題	(1) 開会 (2) 技術情報管理認証制度の普及促進に向けた今後の取組について (3) 認証制度における監査の仕組みについて (4) 認証制度に関連する海外動向等調査結果について (5) パンフレットについて (6) 今後のスケジュールについて

2. 専門家派遣の実施結果

2.1 派遣募集

2020 年 10 月 8 日より、委託機関（株式会社三菱総合研究所）のホームページにおいて事業者向け・団体向けとも専門家派遣の募集を開始した。



MRI 株式会社三菱総合研究所

お問い合わせ

JP | EN　採用情報　投資家情報

ニュース　公募情報　「技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業」（経済産業省事業）において専門家の派遣を希望する事業者・団体の公募のご案内について

サービス・ソリューション　ナレッジ・コラム　ニュース　セミナー　企業情報

公募情報

「技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業」（経済産業省事業）において専門家の派遣を希望する事業者・団体の公募のご案内について

シェア　ツイート

2020.10.8
株式会社三菱総合研究所

三菱総合研究所（MRI）では、経済産業省からの受託事業「技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業」の一環として、技術等情報管理を進めようとする事業者や団体の皆さまに、情報管理の具体的な方法のアドバイスや、認証取得申請の支援を行う専門家を派遣いたします。

参考：技術等情報管理認証制度について（経済産業省）

事業者向け

募集期間

2020年10月～2021年2月26日（金）
※定員に達し次第締め切ります。お早めにお申し込みください。

派遣時期

2020年10月中旬～2021年3月12日（金）

対象者

技術等情報管理認証取得を希望する事業者
重要な情報に関して、情報管理のレベルアップを希望する事業者
（技術情報に限らず、顧客情報や研究情報等、事業者の強みとなる情報すべてが対象です）

費用

無し（認証取得申請には別途費用がかかります）

ニュースカテゴリー

ニュースリリース
公募情報
お知らせ
IRニュース
グループ企業ニュース

年別一覧

2021年のニュース
2020年のニュース
2019年のニュース
2018年のニュース
2017年のニュース
2016年のニュース

図 2-1　専門家派遣募集ホーム-ページ（1/2）

専門家実施内容、所要時間

(1) 情報管理方法のアドバイス：半日～最大5日程度
管理が必要な技術等の重要な情報の特定や、具体的な情報漏えい防止対策等について、それぞれの事業者の状況に合わせた提案・アドバイスを実施

(2) 認証取得のための内部監査：半日～最大3日程度
認証基準に沿った情報漏えい防止対策が行われているかを、第三者の立場で評価し、「自己宣言認証」（第一次審査のみによる認証）で利用できる監査記録を作成

※所要時間は認証対象とする情報の種類・量や拠点規模、対策数等によって異なります
※派遣は (1)のみ、(2)のみ、(1)(2)両方、のいずれも可

事業案内・申込用紙

事業案内 [610.2KB]
技術等情報管理認証制度に係る指導支援等の専門家派遣事業（事業者向け）申込書 [41.3KB]

団体向け

募集期間

2020年10月～2021年2月26日（金）

派遣時期

2020年10月中旬～2021年3月12日（金）

対象者

業界・団体等において情報管理の取り組みを促進するため、標準的な守り方（モデル）を構築しようとする団体等

費用

無し（認証取得申請には別途費用がかかります）

専門家実施内容

・モデル検討において参考となる情報の提供
　（例）一般的に求められる対策レベル、関連規格等における記載事項　等
・具体的な対策の提案、アドバイス

事業案内・申込用紙

事業案内 [525.4KB]
技術等情報管理認証制度に係る指導支援等の専門家派遣事業（団体向け）申込書 [33.6KB]

図 2-2　専門家派遣募集ホーム-ページ（2/2）

技術等情報管理認証制度

専門家派遣事業のご案内

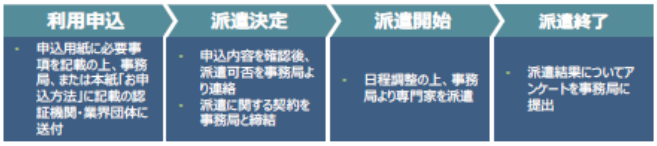
～ 技術など重要な情報・ノウハウの守り方を専門家がアドバイスします ～

平成 30 年 9 月 25 日、産業競争力強化法に基づき、技術等の情報の管理について、国の認定を受けた機関による認証を受けられる制度がスタートしました。
この認証取得を目指して、自社の技術等の情報管理を進めようとする事業者の皆様に、情報管理の具体的な方法のアドバイスや、認証取得申請の支援を行う専門家を派遣いたします。

派遣する専門家
（1） 情報管理方法のアドバイス（IT コーディネータ、中小企業診断士 等）
（2） 認証取得のための内部監査（情報セキュリティ監査人 等）

募集期間	2020 年 10 月～ 2021 年 2 月 26 日（金） ※ 定員に達し次第締め切ります。お早めにお申し込みください。
対象者	技術等情報管理認証取得を希望する事業者、技術等情報管理のレベルアップを希望する事業者
費用	無し （認証取得申請には別途費用がかかります）
専門家の実施内容、所要時間	（1） 情報管理方法のアドバイス ： 半日～最大 5 日程度 管理が必要な技術等の重要な情報の特定や、具体的な情報漏えい防止対策等について、それぞれの事業者の状況に合わせた提案・アドバイスを実施 （2） 認証取得のための内部監査 ： 半日～最大 3 日程度 認証基準に沿った情報漏えい防止対策が行われているかを、第三者の立場で評価し、「自己宣言認証」（第一次審査のみによる認証）で利用できる監査記録を作成 ※ 所要時間は認証対象とする情報の種類・量や拠点規模、対策数等によって異なります ※ 派遣は（1)のみ、(2)のみ、(1)(2)両方、のいずれも可
派遣時期	2020 年 10 月中旬 ～ 2021 年 3 月 12 日（金）

■ 専門家派遣の流れ



■ お申込方法

別紙「申込書」にご記入の上、**事務局、以下の認定技術等情報漏えい防止措置認証機関、またはご所属の業界団体**にお送りください。（申込先によって申込書の種類が異なりますのでご注意ください）

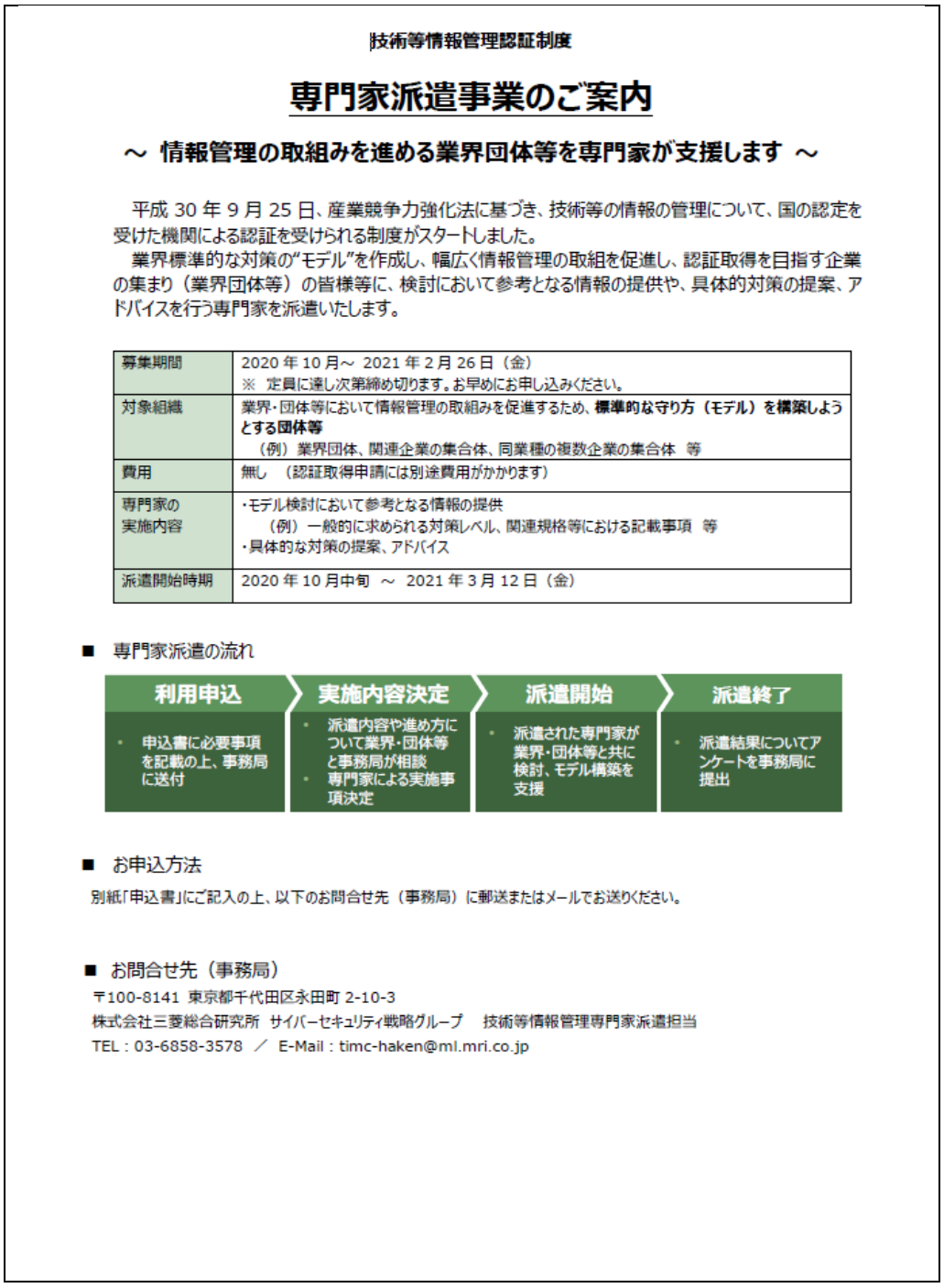
【認定技術等情報漏えい防止措置認証機関】
- 日本検査キューエイ株式会社（JICQA）
- 一般財団法人日本品質保証機構（JQA）
- 株式会社日本環境認証機構（JACO）
- 公益財団法人防衛基盤整備協会
- 一般社団法人情報セキュリティ関西研究所

■ お問合せ先（事務局）

株式会社三菱総合研究所 サイバーセキュリティ戦略グループ 技術等情報管理専門家派遣担当
TEL：03-6858-3578 ／ E-Mail：timc-haken@ml.mri.co.jp

2020/10/1 版

図 2-3 専門家派遣事業の案内（事業者向け）



技術等情報管理認証制度

専門家派遣事業のご案内

～ 情報管理の取組みを進める業界団体等を専門家が支援します ～

平成 30 年 9 月 25 日、産業競争力強化法に基づき、技術等の情報の管理について、国の認定を受けた機関による認証を受けられる制度がスタートしました。
業界標準的な対策の"モデル"を作成し、幅広く情報管理の取組を促進し、認証取得を目指す企業の集まり（業界団体等）の皆様等に、検討において参考となる情報の提供や、具体的対策の提案、アドバイスを行う専門家を派遣いたします。

募集期間	2020 年 10 月～ 2021 年 2 月 26 日（金） ※ 定員に達し次第締め切ります。お早めにお申し込みください。
対象組織	業界・団体等において情報管理の取組みを促進するため、**標準的な守り方（モデル）を構築しようとする団体等** （例）業界団体、関連企業の集合体、同業種の複数企業の集合体 等
費用	無し （認証取得申請には別途費用がかかります）
専門家の実施内容	・モデル検討において参考となる情報の提供 （例）一般的に求められる対策レベル、関連規格等における記載事項 等 ・具体的な対策の提案、アドバイス
派遣開始時期	2020 年 10 月中旬 ～ 2021 年 3 月 12 日（金）

■ 専門家派遣の流れ

利用申込	実施内容決定	派遣開始	派遣終了
・申込書に必要事項を記載の上、事務局に送付	・派遣内容や進め方について業界・団体等と事務局が相談 ・専門家による実施事項決定	・派遣された専門家が業界・団体等と共に検討、モデル構築を支援	・派遣結果についてアンケートを事務局に提出

■ お申込方法

別紙「申込書」にご記入の上、以下のお問合せ先（事務局）に郵送またはメールでお送りください。

■ お問合せ先（事務局）

〒100-8141 東京都千代田区永田町 2-10-3
株式会社三菱総合研究所 サイバーセキュリティ戦略グループ 技術等情報管理専門家派遣担当
TEL：03-6858-3578 ／ E-Mail：timc-haken@ml.mri.co.jp

図 2-4 専門家派遣事業の案内（団体向け）

専門家派遣にあたり、中小企業・製造業の情報管理や IT 活用に通じており、情報セキュリティ監査の知見を有する専門家を抱える特定非営利活動法人 IT コーディネータ協会及び一般社団法人情報セキュリティ関西研究所と連携し、円滑な派遣体制を構築した。

事業者向けの全ての派遣については、両組織を通じて行った。専門家の秘密保持については、連携した 2 組織と専門家の間の守秘義務、及び連携した 2 つの各組織と委託機関（株式会社三菱総合研究所）との守秘義務において確保した。

2.2 専門家向け研修会の実施

本事業において派遣する専門家として本認証制度及び情報管理について十分な知識を得ていただくために、専門家向けの研修会を実施した。派遣候補となる専門家は、各組織において相応の資格や実績のある方を選定いただいた。派遣候補となる専門家に対して、技術情報管理認証制度、及び今年度の専門家派遣事業に関する理解と、認証基準の考え方について学んでいただいた。なお、研修会については、特定非営利活動法人 IT コーディネータ協会の協力を得て実施した。

日時	2020 年 11 月 18 日（水）13:00 - 16:00
場所	オンライン会議（zoom） ※　配信場所：特定非営利活動法人 IT コーディネータ協会
議題	(1)　技術等情報管理認証制度、専門家派遣制度 （株式会社三菱総合研究所） (2)　技術等情報管理認証制度　基準等 （情報システム監査株式会社　監査・コンサルティング部 小河 裕一　氏） (3)　今後の手続等
参加者	28 名

2.3 派遣結果

2.3.1 派遣実績

専門家派遣事業の派遣実績は、一般事業者への派遣が 16 社延べ 26 日間（31 回）、日本金型工業会と連携して実施した会員企業への派遣が 22 社延べ 93 日間（120 回）でまた、認定を希望する機関への派遣が 1 機関延べ 25 日間であった。派遣形態は直接の訪問及びオンラインのいずれかとした。

一般事業者においては、関西地区が多く、製造業に限らず様々な業種から派遣希望があった。製造業においては技術情報が管理対象情報としていたが、その他の業種においては個人情報等においても管理対象情報としていた。

また、一般事業者への派遣においては、14 組織が助言、3 組織が監査（1 社は 1 回目が助言、2 回目が監査）であった。

今年度は、認証取得を希望する事業者に対する複数回の派遣を可能としたが、一般事業者においては 5 社が複数回の派遣、日本金型工業会への派遣は全て複数回の派遣を実施することができ、多くの企業に対して手厚い支援が可能であったと言える。派遣を行った 1 社については認証を取得（2021 年 3 月 22 日）、年度内にも複数社が認証取得予定である。

また、認定取得を希望する機関への派遣を通じて、1 機関が認定を受け（2020 年 11 月）認証業務を開始した。

専門家派遣実績の一覧は、表 2-1 及び表 2-2 の通り。

表 2-1　派遣実績（企業派遣：一般）

分類	No.	業種	従業員数	所在地	内容	派遣日	調整機関	日数 (回数)
事業者派遣 （一般）	1	製造業（い草製品）	31名	岡山県	助言	①12/16（水） ②12/25（金） ③1/15（金）、26（火） ④2/16（火）、22（月） ⑤3/5（金）	ITCA	26日間 (31回)
	2	防水工事	7名	福岡県	助言	1/20（水）	ITCA	
	3	輸送業	300名	愛知県	助言	12/10（木）	関西sec	
	4	製造業（金属加工機械）	175名	愛知県	①助言 ②監査	①1/25（月） ②3/19（金）	①ITCA ②関西sec	
	5	旅行業	4名	東京都	助言	①12/17（木） ②1/8（金） ③2/5（金） ④3/2（火）、10（水）	ITCA	
	6	設備メンテナンス	10名	大阪府	助言	12/2（水）	関西sec	
	7	その他サービス	5名	茨城県	助言	12/24（木）	ITCA	
	8	製造業（プラスチック製品）	250名	兵庫県	助言	①1/8（金） ②2/5（金） ③3/1（月）、10（水）	ITCA	
	9	教育	130名	大阪市	助言	11/12（木）	関西sec	
	10	製造業（化学）	128名	和歌山県	助言	11/20（金）	関西sec	
	11	製造業（機械器具）	150名	和歌山県	助言	11/25（水）	関西sec	
	12	旅行業	100名	大阪府	助言	12/8（火）	関西sec	
	13	保険業	52名	大阪市	助言	2/16（火）	関西sec	
	14	製造業（金属製品）	120名 (拠点28名)	大阪府	監査	3/2（火）	関西sec	
	15	製造業（金属製品）	120名 (拠点17名)	岡山県	監査	3/4（木）	関西sec	
	16	建設業	866名	東京都	助言	3/5（金）、10（水）	ITCA	

表 2-2　派遣実績（企業派遣：日本金型工業会、認定希望機関派遣）

分類	No.	業種	従業員数	エリア	内容	派遣日	調整機関	日数（回数）
事業者派遣（金型）	1	製造業（生産用機械器具）	50～99名	東海	助言	①1/18（月） ②2/1（月） ③2/26（金）	ITCA	93日間（120回）
	2	製造業（金型）	～49名	東海	助言	①1/22（金） ②1/24（日）、25（月）、26（火）、30（土）、2/4（木）、7（日）、12（金） ③2/18（木）	ITCA	
	3	製造業（金型）	～49名	関東	助言	①1/14（木） ②1/20（水） ③2/4（木） ④2/18（木）	ITCA	
	4	製造業（金型）	～49名	九州	助言	①2/5（金） ②2/12（金） ③2/18（木） ④2/25（木）	ITCA	
	5	製造業（金型）	50～99名	関東	助言	①1/18（月）　※2名 ②1/25（月）、2/8（月）　※2名	ITCA	
	6	製造業（生産用機械器具）	～49名	東海	助言	①1/19 ②2/2	ITCA	
	7	製造業（金型）	50～99名	中部	助言	①1/25、2/10 ②2/17、3/1	ITCA	
	8	製造業（金型）	～49名	関西	助言	①1/18（月） ②1/28（木） ③2/10（水） ④2/16（火）	ITCA	
	9	製造業（金型）	100名～299名	関東	助言	①1/13（水）　※2名 ②1/27（水）、2/10（水）　※2名 ③2/26（金）　※2名	ITCA	
	10	製造業（金型）	～49名	関西	助言	①2/4（木）、10（水） ②2/16（火）、3/1（月）	ITCA	
	11	製造業（金型）	300名～	中部	助言	①1/15（金）　※2名 ②2/3（水）、2/19（金）　※2名 ③3/2（火）　※2名	ITCA	
	12	製造業（金属加工機）	100名～299名	東海	助言	①1/13（水）　※2名 ②1/27（水）、2/10（水）　※2名 ③2/26（金）　※2名	ITCA	
	13	製造業（金型）	100名～299名	関東	助言	①1/22（金） ②2/10（水） ③2/22（月）	ITCA	
	14	製造業（金型）	50～99名	関東	助言	①1/28（木） ②2/10（水）、18（木） ③2/25（木）	ITCA	
	15	製造業（金型）	100名～299名	関東	助言	①1/15（金） ②1/22（金） ③2/2（火） ④2/19（金）	ITCA	
	16	製造業（金型）	～49名	九州 関西（工場）	助言	①1/25（月） ②2/5（金） ③2/8（月）、15（月）	ITCA	
	17	製造業（生産用機械器具）	～49名	関東	助言	①1/21（木）　※2名 ②2/12（金）　※2名 ③2/25（木）	ITCA	
	18	製造業（金型）	100名～299名	関東	助言	①1/19（火）、26（火） ②2/16（土）、26（火） ③3/4（木）、12（金）	ITCA	
	19	製造業（金型）	～49名	関西	助言	①1/26（火）　※2名 ②2/4（木）、12（金）　※2名 ③2/19（金）　※2名	ITCA	
	20	製造業（機械）	100名～299名	関東	助言	①1/27（水）　※2名 ②2/8（月）、15（月）　※2名 ③2/24（水）　※2名	ITCA	
	21	製造業（金属加工機械）	50～99名	東海	助言	①1/15（金）　※2名 ②1/29（金）　※2名 ③2/8（月）　※2名 ④2/19（金）　※2名	ITCA	
	22	製造業	100名～299名	東北	助言	①2/5（金）　※2名 ②2/24（水）　※2名 ③3/4（木）　※2名	ITCA	
認定希望機関派遣	1	–	–	東京都	–	10/20（火）～2/26（金）の間 延べ25日間	ITCA	25日間

(1) 事業者向け専門家派遣

事業者向け専門家派遣により、専門家から得られた主な意見として、事業者における成果と今後の技術等情報管理・認証取得に向けた見通し、困難だった点は以下の通り。

1) 支援による成果、事業者が得たメリット

●重要性の認識、課題の明確化

- 自社が優先すべき事業から着手し、管理すべき対象を拡大することが重要であることを認識頂いた。
- 重要な情報の特定及びリスク分析が重要であり、社内の人的資源を投入して実施することが必要であり時間がかかることを認識頂いた。
- なすべきことの明確化、重要情報の管理上の課題（重要情報の特定、具体的管理策等）が明確となった。
- 情報管理の取り組みの優先順位が明確になった。
- 今回の支援によって、情報管理の詳細内容、必要なプロセスが明確になると共に、現状のレベルで実施すべき内容が認識できた。
- 全社的情報管理体制の構築、情報管理規程の制定など重要情報の管理上の課題が明確となった。今後の情報管理強化の効果的な取り組みのポイントが明確になった。
- 営業部門における情報管理の課題が明確になった。
- 推進体制の構築や重要情報の特定、アクセス権の設定など、重要情報管理上の現状の問題点と課題が明確になった。
- 今後の情報管理強化の対策すべき内容が分かった。

●対策の推進

- 実際にリスク分析ができ、安全管理規程を定めることができた。
- 委託元からの「業務委託に関する情報セキュリティ調査シート」の内容理解と求められる態勢整備の必要性を理解し、求める情報セキュリティ管理レベルを担保するための情報セキュリティ管理規程の整備・運用の有効性を理解した。
  重要情報管理の体制と制度作り及びその浸透のグランドデザインの大枠と、社内での進め方の手順を整理できた。
- 重要情報の特定方法、必要な措置の決定方法を把握できた。

●認証制度

- 認証制度を前向きに検討することとなった。
- 認証審査における基準に対する自社の現状認識と、内部で必要な対応が分かった。

2) 事業者における今後の対策、認証取得の見通し

●事業者における今後の対策

- 企業側で、体制の構築、重要情報管理規程の制定等、情報管理の強化に向けた対策を実施する方向である。
- 「3 種の覚書作成（採用面接時、従業員、外注）」、「共有ドライブ設定、運用教育、運用（管理・許可人員携帯、モニタリング法教育）」、「書類の分類（社外秘、極秘分類）」、「保管棚の整理（施錠情報の洗い出しと実践）」を実施していく。

●認証取得の見通し

- 認証取得については、今後の検討課題とする。
- 内部監査による認証を検討されており、この認証を通して情報管理の体系を整備したいとの考えであった。
- 認証取得（自己宣言認証）については、今回の評価を踏まえて検討する。
- 2021 年 3 月を目標
- 2021 年 3 月末を目標
- まずは開発に係る技術情報を守る方法を学び、管理体制を構築してから製造部門、管理部門へと水平展開し、会社全体の体制が整った後で認証取得を目指す。
- P マーク等の認証取得をまず行い、次に全社の情報を対象として技術情報管理認証を進めていくことになった。
- 認証取得は、複数の手順を踏んだ後となるので、相当の期間を要する見通しである。

3) 支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報　等）

●事業者の対策状況

- 書庫やキャビネット等の施錠管理等、最低限実施されていると思われたリスク対策が全くされていなかった。
- 情報の取扱いについて担当従業者の個人管理に任せっぱなしであった。
- ほとんどの管理規程が存在していない為、会社が保有する機密情報（個人情報、営業機密情報）について、規程を全て新規に作成することが必要である。
- 個人情報の担当者が、その業務について全体を把握できていなかったことから、その業務のフロー及び取扱いにおけるリスク対策に対する認識レベルが低かった。
- 中小企業では個人のスキルに依存することが多く、担当の業務範囲が広く、他の担当者との重複業務も整理されていないことから、対象とする情報の特定には相当の時間がかかることを覚悟することが必要である。
- 状況によっては業務フローを一緒に作成し、整理することが必要である。（今回はある程度業務フローの作成方法を理解し、単独でも業務フローを作成できたため、リスク分析ができた。）

・　本社事務の女性の意識は高いが、社長自身の理解や危機感はあるものの現場優先。
・　情報管理の考え方に乏しく、アドバイスのみではなく、具体的な指導助言も必要。
・　要望事項の言葉の理解が企業側で困難な点があり、内部監査に時間がかかった。

●担当者の多忙
・　担当者が多岐にわたって業務をおこなっている為、メール等による事前の準備作業を頻繁に実施することができなかった。
・　支援企業にセルフチェックシートの対策状況記載を依頼したが、記載がなかったため、訪問当日のヒアリングとなった。
・　IPA「情報セキュリティ関連規程」雛形に基づき、自社「情報セキュリティ関連規程」原案の事前検討を依頼したが、準備不足であった。

●事業期間の短さ
・　リスク分析の結果、講じる必要があると判断したリスク対策が本支援期間内には、設備投資を一部でも完了させることができなかった。
・　助言での専門家派遣の後、監査時においては、事業期間内に特にＩＴについては、技術情報管理認証を取得する為にもセキュリティ対策のレベルを上げる必要があったが、着手もできなかった。

●その他
・　引き続き新型コロナ感染症の状況が思わしくないことから、現地を訪問しての指導など、難しい状況である。リモートでのコミュニケーションを密にしていきたい。

表 2-3　専門家派遣による成果と今後の見通し（1/5）

依頼事業者名	1 製造業（い草製品）	1 製造業（い草製品）	1 製造業（い草製品）	1 製造業（い草製品）	1 製造業（い草製品）
回数	1回目	2回目	3回目	4回目	5回目
支援による成果、企業が得たメリット	自社の人員体制及び情報の特定ができていないことから、まず自社が優先すべき事業であるネット通販事業から着手し、今後の展開の中で管理すべき対象を拡大することが重要であることを認識して頂いた。	「ネット通販事業に関わる顧客の個人情報及び自社の個人情報」においてJIS15001(プライバシーマーク)が要求している要求項目について理解して頂いた。 また、技術情報等管理も同じであるが、個人情報の特定及びリスク分析が重要であり、社内の人的資源を投入して実施することが必要であり時間がかかることを認識して頂いた。	今後自社が販売強化を予定している「ネット通販事業」に関わる顧客の個人情報の取扱業務の中で、既に事業化しており取得している個人情報が最も多いECモール（楽天市場、ヤフーショッピング）の業務における、個人情報の特定と個人情報の取扱い業務フロー（取得、利用、保管、廃棄）におけるリスク分析をおこなうことができた。	今後自社が販売強化を予定している「ネット通販事業」に関わる顧客の個人情報の取扱業務の中で、既に事業化しており取得している個人情報が最も多いECモール（楽天市場、ヤフーショッピング）の業務における、個人情報の特定と個人情報の取扱い業務フロー（取得、利用、保管、廃棄）におけるリスク分析をおこなうことができた。	①今後自社が販売強化を予定している「ネット通販事業」に関わる顧客の個人情報の及び、「採用業務、従業員管理業務、マイナンバー管理業務の3種類の総務経理に関わる個人情報」の個人情報の特定と個人情報の取扱い業務フロー（取得、利用、保管、廃棄）におけるリスク分析をおこなうことができた。 ②技術情報管理における安全管理に共通した対策としての検討を、①のリスク対策の検討の中で、実施でき安全管理規程として定めることができた。 ③技術情報管理の基本方針、基本規程、JIS15001規格に準拠した個人情報保護方針、個人情報保護基本規程の理解及び様式により管理記録の残し方について理解をして頂くことができた。 ④プライバシーマーク取得に向けた申請書類を整えることができ、個人情報保護方針、個人情報保護基本規程、様式の社内に認識させること（＝教育）、運用し様式に記録させること、監査及びマネジメントレビューを実施することで、プライバシーマークの申請ができる状態となった。
企業における今後の対策、認証取得の見通し	人員体制を踏まえて、自社の事業において今後強化する「ネット通販事業に関わる顧客の個人情報及び自社の個人情報」の情報管理におけるプライバシーマーク等の認証取得をまず行い、次に全社の情報を対象として技術等情報管理認証を進めていくことになった。	「ネット通販事業に関わる顧客の個人情報及び自社の個人情報」の情報管理におけるJIS15001(プライバシーマーク)の認証取得をまず行い、次に全社の情報を対象として技術等情報管理認証を進める方針を社長に理解して頂いた。 JIS15001(プライバシーマーク)の認証取得に必要な期間を認識して頂いたことから、ひな形を元に作成する規定や様式は後回しにして、まず個人情報の特定及びリスク分析を実施することとした。	①リスク対策において認識した、リスク対策を実施していない一部紙媒体の施錠保管、バックアップ媒体の施錠保管に対する措置を講じることが必要である。 ②この講じたリスク対策については安全管理規程に反映させるだけでなく、内部監査や運用点検による確認が必要となる。 ③業務を委託している事業者の選定・評価を実施し、機密保持契約の締結または利用約款による確認をすることが必要である。 ④今後、その他の個人情報の特定及びリスク分析を実施し、安全管理規程のひな形に反映させて自社の安全管理規程に反映させることになる。 その後、規格であるJIS15001に従った基本規程のひな形に基づいた自社の規程を作成し、教育、運用、監査を行って1回PDCAを回して認証取得申請となる。	①リスク対策において認識した、リスク対策を実施していない一部紙媒体の施錠保管、バックアップ媒体の施錠保管に対する措置を講じることを安全管理規程に反映させ、全従業者に教育することが必要となる。 ②業務を委託している事業者の選定・評価を実施し、機密保持契約の締結または利用約款による確認をすることが必要であることを認識して頂いているが、まだ未実施である。 ③全従業者に対する教育実施後、運用点検による確認及び内部監査の実施、マネジメントレビューの実施が必要となる。 ④安全管理措置だけでなく、JIS15001に従った基本規程のひな形に基づいた自社の規程を作成し個人情報保護方針及び規格要求事項の公表事項を自社のホームページにアップすること等をする必要がある。	①リスク対策において認識した、リスク対策を実施していない一部紙媒体の施錠保管、バックアップ媒体の施錠保管に対する措置を講じることを安全管理規程に反映させ、全従業者に教育することが必要となる。 （紙媒体の施錠保管については、キャビネットを施錠保管できるように改造作業を始めて頂いている。しかし、サーバについては、バックアップ媒体のワイヤーロックまでは計画して頂いているが、施錠できるサーバラックの設置までの検討は進んでいない。） ②業務を委託している事業者の選定・評価を実施し、機密保持契約の締結または利用約款による確認をすることが必要であることを認識して頂いているが、まだ未実施である。 ③全従業者に対する教育実施後、運用点検による確認及び内部監査の実施、マネジメントレビューの実施が必要となる。 ④安全管理措置だけでなく、JIS15001に従った基本規程のひな形に基づいた自社の規程を作成し個人情報保護方針及び規格要求事項の公表事項を自社のホームページにアップすること等をする必要がある。 ⑤①～④について実施し、定めた規定及び教育、運用、監査、マネジメントレビュー他の記録を揃えて、プライバシーマーク審査機関への申請、現地審査における指摘事項への対応をおこなって、プライバシーマークの取得が可能となる。 ⑥技術情報管理認証については、技術情報管理方針、技術情報管理規程の完成とその後の教育、運用、監査の実施はプライバシーマークに準じて進めることができると思われる。 しかし、情報の特定が最も時間がかかる為、継続的な専門家の派遣が必要となると思われる。
支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報等）	①事前チェックシートの通り、情報管理が全くされていなかった。 ②書庫やキャビネット等の施錠管理等、最低限実施されていると思われたリスク対策が全くされていなかった。	①技術情報等だけでなく個人情報の取扱いについて担当従業者の個人管理に任せっぱなしであり、中堅社員も定年による退職で人材不足になっている状態であった。 ②書庫やキャビネット等の施錠管理等、最低限実施されていると思われたリスク対策が全くされていない為、リスク対策に投入するべきハード設備投資が必要であった。 ③文書管理規程も制定されていない為、今後の文書や記録類の制定更新についても、今回制定する情報管理規程の中で規定し、全従業者に認識させることが必要であった。	①ISOの認証取得もされていない為、文書管理規程だけでなくほとんどの管理規程が存在していない為、会社が保有する機密情報（個人情報、営業機密情報）について、規程を全て新規に作成することが必要である。 ②機密情報（個人情報、営業機密情報）の特定及びリスク分析も皆無であった為、ネット通販事業で取得している個人情報を優先して進め、今後営業機密情報に対象を拡大していくことが必要である。	①今回の窓口担当者は「ネット通販事業」及びIT管理者及び仕入発注処理業務の多岐にわたって業務をおこなっている為、メール等による事前の準備作業を頻繁に実施することができなかった。 ②「採用業務、従業員管理業務、マイナンバー管理業務の3種類の総務経理に関わる個人情報」の担当者が、その業務について全体を把握できていなかったことから、その業務のフロー及び取扱いにおけるリスク対策に対する認識レベルが低かった。 この為、「採用業務、従業員管理業務、マイナンバー管理業務の3種類の総務経理に関わる個人情報」の特定表」、「業務フロー」、「リスク分析表」の作成にかなり時間を取られ、個人情報保護管理規程、安全管理規程の作成を着手することまでできなかった。	①技術情報管理の対象の特定が初回ヒアリング時点で非常に困難であることを、社長及び担当者が理解した。この為、従業者の理解もし易く特定し易いことと、今後の事業の主軸と期待しているネット通販事業から個人情報を対象とすることとした。 中小企業では個人のスキルに依存することが多く、担当の業務範囲が広く、他の担当者との重複業務も整理されていないことから、対象とする情報の特定には相当の時間がかかることを覚悟することが必要である。 状況によっては業務フローを一緒に作成し、整理することが必要である。（今回の事業者の担当者はある程度業務フローの作成方法を理解し、単独でもそこそこの業務フローを作成できた為、リスク分析ができた。） ②今回の事業者の担当者は「ネット通販事業」及びIT管理者及び仕入発注処理業務の多岐にわたって業務をおこなっている為、メール等による事前の準備作業を頻繁に実施することができなかった。 ③「採用業務、従業員管理業務、マイナンバー管理業務の3種類の総務経理に関わる個人情報」の担当者が、その業務については断片的な事務処理しか理解できていなかった。 この為、その業務のフロー及び取扱いにおけるリスク対策に対する認識レベルが低く、ブラッシュアップするのに時間がかかった。 ④リスク分析の結果、講じる必要があると判断したリスク対策が本支援期間内には、設備投資を一部でも完了させることができなかった。 特にＩＴについては、技術情報管理認証を取得する為にもセキュリテイ対策のレベルを上げる必要があったが、着手もできなかった。この為、残留リスクとして把握するのに留まっている。

表 2-4　専門家派遣による成果と今後の見通し（2/5）

依頼事業者名	**2 防水工事**	**3 輸送業**	**4 製造業（金属加工機械）**	**4 製造業（金属加工機械）**	**5 旅行業**	**5 旅行業**
回数			**1回目**	**2回目**	**1回目**	**2回目**
支援による成果、企業が得たメリット	なすべきことの明確化	・重要情報の管理上の課題（重要情報の特定、具体的管理策等）が明確となった ・情報管理の取り組みの優先順位が明確になった	今回の制度を利用し、当該社の情報管理を再度見直されてはとの提案に、認証制度を前向きに検討することとなった。	・認証審査に対する現状認識と内部での必要な対応が分かった	・当制度内容の理解 ・委託元が求める個人情報保護管理レベルの理解 ・自社の個人情報保護管理レベルの確認	・IPA「情報セキュリティ関連規程」（サンプル）に基づき、当社の個人情報管理実態のヒアリングし、当社の情報セキュリティ関連規程案を検討した。 ・情報セキュリティ管理レベル向上のため、IPA「SECURITY ACTION」認証取得の有効性を理解した。 ・委託元からの「業務委託に関する情報セキュリティ調査シート」の内容理解と求められる態勢整備の必要性を理解した。
企業における今後の対策、認証取得の見通し	3種の覚書作成 （採用面接時、従業員、外注） 共有ドライブ設定、運用教育、運用 （管理・許可人員携帯、モニタリング法教育） 書類の分類 （社外秘、極秘分類） 保管棚の整理 （施錠情報の洗い出しと実践）	・企業側で、体制の構築、重要情報管理規程の制定等、情報管理の強化に向けた対策を実施する方向 ・認証取得については、今後の検討課題とする	内部監査による認証を検討されており、この認証をとおして、情報管理の体系を整備したいとの考えであった。	・２０２１年４月を目標	・当社の委託元大手旅行社は、Pマーク及びISMS認証取得企業であるため、ISMS枠組みの個人情報保護管理の手順構築と運用支援が求められる	・技術等情報管理認証取得（セルフ認証）及びSECURITY ACTION（2つ星）の取得を目指す
支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報等）	工事現場で働く作業員の状況は未確認 現場作業員のIT成熟度は低いと推測される 本社事務の女性の意識は高いが、社長自身の理解や危機感はあるものの現場優先。	・企業には情報管理の考え方が弱かった（アドバイスのみではなく、具体的な指導助言も必要） ・特に困った点はなかった	当初、支援自体を否定的にとらえられていたため、認証を受けることの利点を中心に説明を行った。	・要望事項の言葉の理解が企業側で困難な点があり、内部監査に時間がかかった	・支援企業にセルフチェックシートの対策状況記載を依頼したが、記載がなかったため、訪問当日のヒアリングとなった。	・IPA「情報セキュリティ関連規程」雛形に基づき、自社「情報セキュリティ関連規程」原案の事前検討を依頼したが、準備不足であった。

表 2-5　専門家派遣による成果と今後の見通し（3/5）

依頼事業者名	**5 旅行業**	**5 旅行業**	**6 設備メンテナンス**	**7 その他サービス**	**8 製造業（プラスチック製品）**	**8 製造業（プラスチック製品）**
回数	**3回目**	**4回目**			**1回目**	**2回目**
支援による成果、企業が得たメリット	・IPA「情報セキュリティ関連規程」（サンプル）に基づき作成した当社情報セキュリティ関連規程案について、当社の実態との摺り合わせを行った。 ・情報セキュリティ管理レベル向上のため、IPA「SECURITY ACTION」認証2つ星取得の有効性を理解した。 ・委託元の「業務委託に関する情報セキュリティ調査シート」が求める情報セキュリティ管理レベルを担保するための情報セキュリティ管理規程の整備・運用の有効性を理解した。	IPA「情報セキュリティ関連規程」（サンプル）に基づき作成した当社「情報セキュリティ関連規程（案）」Ver 2.2を構築した。 ・情報セキュリティ管理レベル向上のため、IPA「SECURITY ACTION」認証1つ星宣言を取得し、2つ星宣言の取得準備を終了した。 ・委託元の「業務委託に関する情報セキュリティ調査シート」が求める情報セキュリティ管理レベルを担保するため、当社「情報セキュリティ関連規程」「IPA2021年版情報セキュリティ10大脅威」により、人材育成研修要点と資料収集方法を確認した。	・個人情報保護および管理の課題が明確となった ・Pマーク取得に向けた推進方法が分かった	事業者はプライバシーマークの認証を目指しており、その支援を望んでいた。今回の専門家派遣による支援では、様々な認証制度があることを伝え、それぞれに審査基準が違うため、認証制度に遭う対策を取る必要があることを理解してもらった。	今回の支援によって、情報管理の方向性、必要なプロセス、認証に向けた準備などが明確になると共に、現状のレベル（ある程度の対策は出来ているが、明確にするべき情報が多々ある）を認識できた。	今回の支援によって、情報管理の詳細内容、必要なプロセスが明確になると共に、現状のレベルで実施すべき内容が認識できた。
企業における今後の対策、認証取得の見通し	・情報セキュリティ管理規程の整備・運用及びSECURITY ACTION（2つ星）の取得を目指す ・このため、支援回数を2回程度延長し、情報セキュリティ管理規程による運用状況確認及びSECURITY ACTION（2つ星）取得支援を行いたい。	・当社は「情報セキュリティ関連規程」を3月1日に施行したことにより、今後は同規程によるPDCAサイクル管理に入る。 ・IPA「SECURITY ACTION」2つ星宣言を取得する。 ・当社は小規模企業のため、現時点での「技術等情報管理認証」取得は難しいが、今回の専門家派遣により当認証制度の理解は深まったため、今後、認証取得に向けた取り組みを期待したい。	・企業側で、体制の構築、個人情報管理規程の制定等、個人情報管理の強化に向けた対策を実施する方向 ・Pマーク取得に向けた取り組みを早期に実施予定	事業者はプライバシーマークの認証取得を目指しているため、今回の対象スキームによる認証は希望していない。プライバシーマークの認証を取得するためには、本事業のチェックシートに沿った取り組みだけでは足りず、個人情報についての理解、管理手法の確立も必要となる。	必要な対策は、ある程度の時間で準備できるものと思われる。認証取得については、ISOのMS活動の実績もあることから、可能性は高いものと考える。	必要な対策は、ある程度の時間で準備できるものと思われる。 認証取得については、まずは開発に係る技術情報を守る方法を学び、管理体制を構築してから製造部門、管理部門へと水平展開し、会社全体の体制が整った後で認証取得を目指す方向に転換された。
支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報等）	特になし	特になし	・Pマーク取得推進のため、今回の専門家派遣事業には、NHKの責任者も同席予定であった ・特に困った点はなかった	支援企業がプライバシーマークの認証を目指しており、技術情報の認証については対象としていなかった。セルフチェックシートによるチェックを事前に行っていたが、産業競争力強化法に基づいた認証に向けた審査基準と、Pマーク認証の審査基準が違うため、基本的なアドバイスが主となった。その上で、Pマーク認証の概要や位置づけ、本スキームとの違いを説明し、理解してもらうことに苦慮した。	現時点では、困難な状況と言える点はない。引き続き新型コロナ感染症の状況が思わしくないことから、現地を訪問しての指導など、難しい状況である。リモートでのコミュニケーションを密にしていきたい。	現時点では、困難な状況と言える点はないが、情報管理の内容、レベルを確実に上げていきたいとの思いが強く、慎重を期する考えをお持ちである。 また、引き続き新型コロナ感染症の状況が思わしくないことから、現地を訪問しての指導など、難しい状況である。リモートでのコミュニケーションを密にしていきたい。

表 2-6　専門家派遣による成果と今後の見通し（4/5）

依頼事業者名	8 製造業（プラスチック製品）	9 教育	10 製造業（化学）	11 製造業（機械器具）	12 旅行業	13 保険業
回数	3回目					
支援による成果、企業が得たメリット	今回の支援によって、情報管理の詳細内容、必要なプロセスが明確になると共に、現状のレベルで実施すべき内容が認識できた。	・個人情報以外の重要情報特定の必要性が明確となった ・Pマークの取組をベースにした情報管理強化の効率的かつ効果的な取り組みのポイントが明確になった	・全社的情報管理体制の構築、情報管理規程の制定など重要情報の管理上の課題が明確となった ・今後の情報管理強化の効果的な取り組みのポイントが明確になった	・推進体制の構築や重要情報の特定、アクセス権の設定など、重要情報管理上の現状の問題点と課題が明確になった ・今後の情報管理強化の対策すべき内容が分かった	・今回の専門家派遣事業で、個人情報以外の重要情報管理の必要性に気づいた ・今後の重要情報の管理強化に向けて、対策すべき内容が分かった	・営業部門における情報管理の課題が明確になった
企業における今後の対策、認証取得の見通し	必要な対策は、ある程度の時間で準備できるものと思われる。 認証取得については、まずは開発に係る技術情報を守る方法を学び、管理体制を構築してから製造部門、管理部門へと水平展開し、会社全体の体制が整った後で認証取得を目指す方向に転換された。	・企業側で、管理対象情報の基準、特定、管理責任者の選任等を含めた情報管理策を実施する方向 ・認証取得については、今後の検討課題とする	・企業側で、対策を推進中 ・認証取得（自己宣言認証）については、今回の評価を踏まえて検討する	・企業側で、体制の構築、重要情報の特定、重要情報管理規程の制定等、情報管理の強化に向けた対策を実施する方向 ・認証取得については、今後の検討課題とする （最終目標としては、認証取得を得たい旨の力強さを感じた）	・今後の主な対策は、企業側での重要情報の認識とその特定 ・認証に関しては、Ｐマーク更新を継続推進する	・認証取得の予定はない
支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報等）	現時点では、困難な状況と言える点はないが、情報管理の内容、レベルを確実に上げていきたいとの思いが強く、慎重を期する考えをお持ちである。 また、引き続き新型コロナ感染症の状況が思わしくないことから、現地を訪問しての指導など、難しい状況であった。	・事前調整・ヒアリング調査に積極的に協力いただき、教育サービス企業のリーディングカンパニーと感じた ・特に困った点はなかった	・全社的マネージメントシステム構築の一環として、協力的に取り組んでいただけた ・特に困った点はなかった	・オープニング・報告会では、社長も含め経営陣等１１名の参加をいただき、取組みの力強さを感じた ・特に困難な点はなかった	・困難だった点は、現状、情報管理は個人情報中心であり、その他の重要情報に触れなかった点 ・実施において、特に困難な点はなかった	・なし

表 2-7　専門家派遣による成果と今後の見通し（5/5）

依頼事業者名	**14 製造業（金属製品）**	**15 製造業（金属製品）**	**16 建設業**
回数			
支援による成果、企業が得たメリット	・認証審査に対する現状認識と内部での必要な対応が分かった	・認証審査に対する現状認識と内部での必要な対応が分かった	①重要情報管理の体制と制度作り及びその浸透のグランドデザインの大枠と、社内での進め方の手順を整理できた。 ②重要情報の特定方法、必要な措置の決定方法を把握できた。
企業における今後の対策、認証取得の見通し	・２０２１年３月末を目標	・２０２１年３月末を目標	重要情報の管理について、以下の手順で進めていくことになった。 ①重要情報の管理を進めていくことをグループ社長会でコンセンサスを得る ②重要情報を特定し、必要な措置を決定する ③措置を具体的な手順に落とし込み、文書化する ④規程、手順書を実行する体制を構築する ⑤グループ内全体へ周知し、実行する ⑥実施状況を定期的に確認し、徹底していく 認証取得は、以上の手順を踏んだのちになることから、相当の期間を要する見通しである。
支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報等）	・今回は、依頼事業者の必須・選択項目があまり多くなく、時間的な問題がなかった	・今回は、依頼事業者の必須・選択項目があまり多くなく、時間的な問題がなかった	特になし

派遣を受けた事業者から得られた主な意見は以下の通り。

＜良かった点＞

- 情報管理について何をすべきかわからなかったが、専門家の助言を受けて取り組みを進めることができた。
- 守るべき情報が特定でき、必要な対策を選択できたことが有益だった。
- 複数回の助言を受けることで、アドバイスを聞くだけではなく、実際の対策を進めることができた。
- 数年間、情報資産の洗い出しと重要度の評価ができていなかったため、本事業をきっかけに情報管理に関するグランドデザインを描くことができた。

＜改善点＞

- Pマーク取得を希望していたが、この認証は異なる制度であることがわかった。
- 派遣の募集から実際の派遣実施までの期間が空いた。

派遣を受けた事業者からのアンケート結果は以下の通り（一般6社、金型22社）。助言内容、わかりやすさとも、9割程度の方に満足いただけた。派遣時間については約8割、派遣時期については 9 割弱の方に満足と回答いただけたが、派遣時期については他の設問より「大変満足」割合がやや低かった。

認証取得時期は6割が2020年度～2021年度に取得との回答だった。

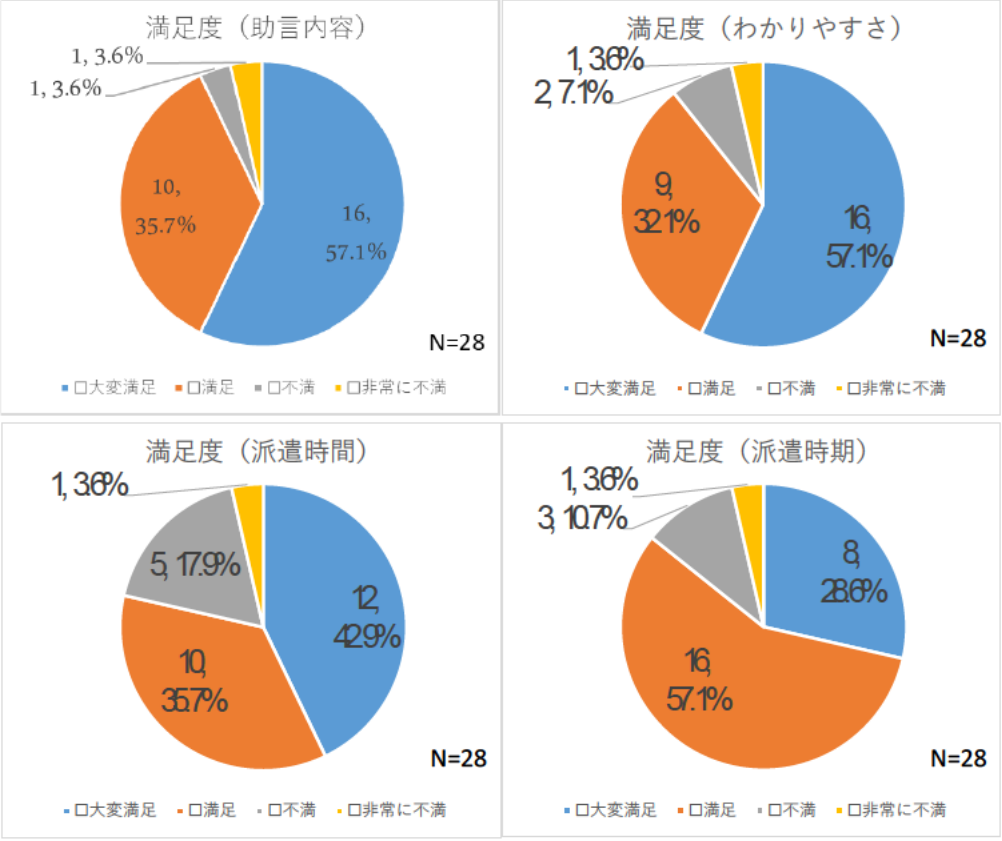


図 2-5　専門家派遣事業の満足度（アンケート）

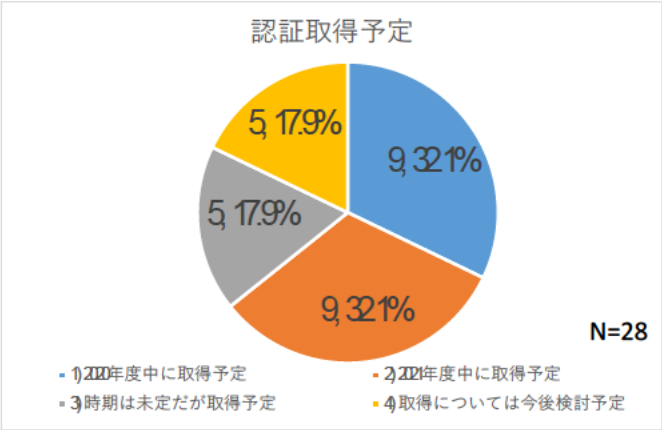


図 2-6　認証取得予定（アンケート）

1) 情報管理に関する効果

●意識の向上

- 現状の管理の甘さを認識させられ、情報管理に対する意識が高まった。実際に管理制度を整えるきっかけとなった。
- 社内の人間に情報管理のセミナーを行い、認識を高めるための良い機会となった。
- 組織として真面目に取り組む姿勢である、ということを認識する効果があった。
- 役職者の知識の向上及び全社員の意識レベルの向上に非常に役立った。
- 情報漏洩に対しての危機管理が高まった。今後社内に浸透させることが直近の課題。

●現状・課題の把握、実施事項の明確化

- 弊社で決めた行うべきことの管理方法など、指摘をいただけたことが参考になった。
- 課題を明確化でき、対応策に至るまでの指導を受け、今後のセキュリティ強化につながった。
- 指導前に弊社で運用中の管理方法、資料等の矛盾、整合性を指導していただき見直しと再整備、社員の情報の扱いに関する重要性を再認識させることができ良かった。
- 客観的視点からの指摘・アドバイス等により当社の現状を理解することができ、そのうえでの対策を検討・実施することができた。

●情報管理の取り組みのきっかけ

- 重要情報について認識はあったが、どの様に管理したら良いのか御指導頂くことにより活動をスタートする事ができた。
- 今まで情報管理について考えたことがなかったので、従業員が書類等を整理する意識を持つことの良い機会になった。

●対策の理解、推進

- 当社には情報管理に関する知見が少なかったが、個別に指導・助言してもらえたことで、当社の実態に即した仕組みの構築ができた。また、当面の情報管理に対する方向性が明確になり、改善に取り組みやすくなった。

・　従来の管理体制の不足や不備に対して対策を立てることができた。また、技術情報管理に対する認知（顧客及び自社の知的財産保護と対外的信用の向上と差別化）が図れた。
・　一つ一つの情報に関する内容を深める事ができ、今後何をすれば良いか方向性も確認することができた。実施が困難な項目も見方や考え方で対処しやすくなることも説明してくれたのでとても良かった。ぜひ継続して、専門家派遣をしてほしい。
・　規定はあるものの、実際に社内で効果的な規定かというとそうではないということで、見直し教育することを考えるための機会となり、どのような情報を守るべきか考えことができた。
・　今回の派遣で紙媒体から電子媒体への切り替え、保管も少しずつ動いている。

2) 専門家派遣事業に対するご意見、認証制度への改善要望等

●制度の難しさ
・　セルフチェックシートの必須以外の項目が多すぎで、指導助言者も内容を理解できていない。
・　指導助言者が理解できないものを、素人の我々が理解できる筈がなく、セルフになっていない。

●チェックシートの充実
・　レベル毎のチェックシートを作成し、具体例をもってチェックできるものにして欲しい。

●専門家派遣事業の有効性
・　０からスタートするのにあたりとても有益だった。派遣いただいた方から大変サポートテイブにアドバイスをいただき、助かった。
・　専門家派遣は、情報管理を広めるにはとても良い事業だと思う。認証制度は、実施要領・規程など開示されていない情報が多いので、徐々に開示されることを要望する。また、広く世の中に制度の認識を広め、第三者認証としての地位を確立して欲しい。
・　今後社内で恒久的に継続できる PDCA サイクルの維持のためにも、継続派遣等があれば中小の企業も認証制度の継続も高まると思われる。ぜひ検討いただきたい。

●専門家派遣事業の改善点
・　具体的な作業について、より細かく、詳細な指導があるとよい。
・　今回は認証取得に特化して必要最低限なことしか学べなかったので、継続的な運用・改善のサポートも必要と感じる。
・　期間が短く、今後の課題について相談する人がいないので、ある程度長い期間指導いただけると有難いと思う
・　具体的に例を挙げて、認証に問題が無いか確認しているが、全く回答を得られず役に立たなかった。意見がコロコロと変わりフラストレーションが溜まった。
・　内容からすれば、もう少し教育期間を設けて頂く必要があったように感じる。
・　今回はタイミング的に短期間での対応だったこともあり致し方ない面もあるが、も

う少し時間的余裕があったほうが取り組みやすいと感じた。
- 業界特有の運用方法や業務プロセスに合わせた管理要件を段階的に整備していくことが必要と感じた。
- 文言の表現が分かりにくく、同業他社がどの様対応しているかについてのアドバイスが欲しかった。
- 期間中、専門家の方にどこまでお願いしていいのか悩ましいことがあった。進め方のモデルスケジュールがあるとイメージしやすかった。

3) 望ましいサポート・資料・情報等

●望ましいサポート
- 次のステップへの改善事項
- ISO27001 取得を最終目標とするのであれば、それまでの道筋も参考に示して欲しい。
- 継続的な運用・改善を目的としたサポート（次回の継続認証審査までに少なくとも 1 回は合った方が良い）。
- 電子情報のアクセス制御について、技術的な支援をしてくれる会社等を紹介して欲しい。
- 半年後、1 年後のサポートがほしい。
- 年 1 回などフォローアップいただけると助かる。

●望ましい資料・情報等
- これから始めようとしている者にとって、導入しやすい・やさしい資料
- どのようなステップを踏んでいけば良いのか、具体例があると助かる。
- 今後も定期的な情報のアップデート、サポートをいただきたい。
- 情報管理の基本的な考えが分かる資料を紹介して欲しい。
- 会社規模毎でどの様な取組みをされているのか、他社の参考事例など資料があると助かる。
- 規格の趣旨、要点、内容についてより詳しい資料の配布があるとよい。
- 同じようなことが書かれている資料が多く、どこに記載されていたか探す事が困難であった。整理された資料が 1 つあれば良い。
- 動画マニュアルがあれば、空き時間で学べるので、ご検討願いたい。
- 規程の運用状況を定期的に確認する際のチェックリストの雛形があると助かる
- 法律条文の解説資料が欲しい（ISO9001 などの「要求事項の解説書」のイメージ）。
- 技術的（テクニカル的）に、どのような方策が好ましいのか具体的事例があると更によいと感じた（例：持出用 PC・USB・オンラインストレージ等活用したデータ保存方法の他社事例等）。
- 同業他社の対応についての資料
- 社内の教育で使えるようなヒヤリハット事例や、認証制度の ToDo リストなどがあればありがたい。
- 認証制度に対しての教本や社内教育資料をもう少し豊富にして頂きたい。

(2) 団体向け専門家派遣

団体向け専門家派遣は、団体向けの説明会が実施できなかったことから、実績は無しとなった。

(3) 認定を目指す組織向け専門家派遣

認定を目指す組織向け専門家派遣においては、主として、「産業競争力強化法に基づく認定技術等情報漏えい防止措置認証機関認定申請書等の注意事項」の 3.命令第 2 条第 2 号の書類は以下の書類は以下の書類を提出すること に基づく、「技術等情報漏えい防止措置認証業務の実施の方法」に関するもので、これら作成に関する支援を１団体(日本金型工業会)に対して実施した。

整備を支援した書類は以下の通り。

表 2-8　認定を目指す組織に向けて整備を支援した書類

NO.	書類名称	助言有無
・別紙１	認証業務規定	有
・別紙２	秘密保持契約書	特に無し
・別紙３	書類保存記録簿	特に無し
・別紙４	認証制度説明書（PR パンフレット、申請者用手引き）	有
・別紙５	認証業務実行マニュアル（関係者用手順書）	有
・別紙６	認証審査申込書（申請者用）	有
・別紙７	認証審査結果レビュー及び審査員評価シート	有
・別紙８	運営委員会規定	有
・別紙９	認証業務料金一覧表（料金体系表：含む指導助言料金）	有
・別紙１０	認証業務運営委員会委員名簿	有
・別紙１１	認証業務運営委員契約書	有
・別紙１２	マネジメントシステム運用マニュアル	有
・別紙１３	指導助言業務説明書（関係者用手順書）	有

・別紙１４	認証業務委託契約書（申込企業用）	有
・別紙１５	チェックシート（審査用、指導助言用、申込企業用）	有
・別紙１６	審査計画書	有
・別紙１７	審査報告書（1 次、2 次・現地審査、結果通知書等）	有
・別紙１８	認証契約書⇒別紙 14 と集約化	有
・別紙１９	自己適合宣言認証証明書（シルバー認証）	特に無し
・別紙２０	認証証明書（ゴールド認証）	有
・別紙２１	審査業務従事者の評価基準と評価記録	有
・別紙２２	審査業務従事者の業務遵守規定	特に無し
・別紙２３	認証審査業務委託契約書	有
・別紙２４	指導助言業務記録簿	有
・追加 1	指導助言用規程類等雛型一式	有
・追加 2	指導助言計画書・実施報告書	有
・追加３	審査員研修用教材	有
・追加 4	認証審査業務の内部監査報告書雛形（1 次審査のみの場合）	有

また、派遣された専門家から得られた成果と今後の認証業務実施に向けた見通し、困難だった点は以下の通り。

＜得られた成果＞

- 同工業会は 2020 年 11 月 20 日付けで本認証制度の認証機関に認定された。
- 審査等の実施に関しては、本支援で作成した書類を基に実施した、2010 年 12 月 14 日「認証審査員研修会」で専門家約 30 名を審査員及び指導助言専門家として育成し、審査を申し込まれた会員企業 22 社に対して、2021 年 1 月から審査を受ける準備のための「指導・助言専門家派遣（3 回程度）」を実施。

＜今後の見通し＞

- 3 月上旬以降、準備が完了した企業から随時審査を開始する予定としており、大半の企業が 3 月中に審査を完了できる見通しである。

＜困難だった点＞

- 同工業会は全く初めての認証業務遂行になるため、支援する専門家としては、同工業会の確認を受けながら「実施・運用の書類」を作成しながらも、実行の際には状況に合わせて柔軟に改善できることを念頭に置いた。
- 本制度自体が、まだ1社も認証事業者を輩出していないことから、実際に運用した際に発生する問題点や課題に対する事例がない“ファーストユーザー”の状況にある。実際、認証審査企業を募集し、企業の申込み・委託契約が完了した後も、委員会では、更新制度の改定やシルバー認証の廃止などの議論が行われ、制度の根幹が揺れ動く状況が続いている。
- 制度の運用に柔軟性は必要であるが、いったん認証を受けた企業にとっては、あまり過度の負担やマイナス面の変更が発生しないように望むとともに、認証を付与し、今後も直接担当する認証機関の責任として、最大限のフォローを行っていくことが必要。

2.4 派遣結果まとめ

専門家派遣を通じて得られた結果は以下の通り。

- 認証取得意向のある事業者への手厚い支援により、認証取得申請に効果
  今年度の専門家派遣事業は、認証取得の実績を得るところまで事業者に対して手厚い支援を実施することとして進めたが、情報管理に対して真剣に取り組み、専門家派遣事業を積極的に活用しようという事業者に対して複数回の派遣を行うことで、複数の事業者において認証取得申請まで繋げることが可能となったことは、今年度事業の大きな成果と言える。

- 管理対象となる情報の特定、及び対策の選択についてのサポートが必要
  専門家派遣の依頼者は、情報管理に関する意識は高いものの、管理対象とする情報の特定ができていない事業者がほとんどであった。また、守るべき情報が特定できたとしても、その情報を守るのに必要な対策については、その事業者の事業環境や情報の態様・使い方等を踏まえ、専門家による助言を得ながら適切なものを選定していく必要がある。守るべき情報の特定及び管理策の選択についての専門家のサポートは非常に有効と考えられる。

- 認定を目指す組織向け専門家派遣の成果は、広く展開することが有効
  今年度は、認定を目指す組織に向けた専門家派遣を実施し、認証機関として必要なドキュメント等の整備や体制構築等の支援を行うことで、円滑に認定を実現することができた。今後、この派遣の過程で得られた知見を活用し、認定を目指す組織に対してのガイドやひな形の整備等を進め公開することで、認証業務の知見や実績はないものの認定を目指す組織に対しての有効な支援となり、認証機関をさらに増やすことが可能と考えられる。もちろん、専門家派遣のような施策とのセットはより効果的である。

3. 国内外動向等の調査

3.1 海外動向の調査

情報管理や情報セキュリティ面で関連または類似する欧米の制度に関して、制度概要や審査内容等について文献調査及びヒアリング調査（コンサルティング企業、認証機関）を行った。

3.1.1 米国（CMMC/NIST SP800-171）

(1) NIST SP800-171

NIST[1] SP800-171 は、米国政府が提示する CUI（Controlled Unclassified Information）の守り方を示したものである。

ISMS（ISO/IEC27001）や政府関係組織に対する NIST SP800-53 のリストから、特に秘匿性（Confidentiality）にフォーカスしたものを選択したものであり、項目は 14 カテゴリ、110 項目に渡る。

NIST SP800-171 は管理策カタログではなくベースライン要件である。すなわち、政府の指定した CUI をいかに漏らさないかという観点で、守るべきミニマムルールを要件書として示したものである。NIST SP800-53 や ISO/IEC 27001 等の「セキュリティ全般に対する管理策の規格書」とは目的が異なる。

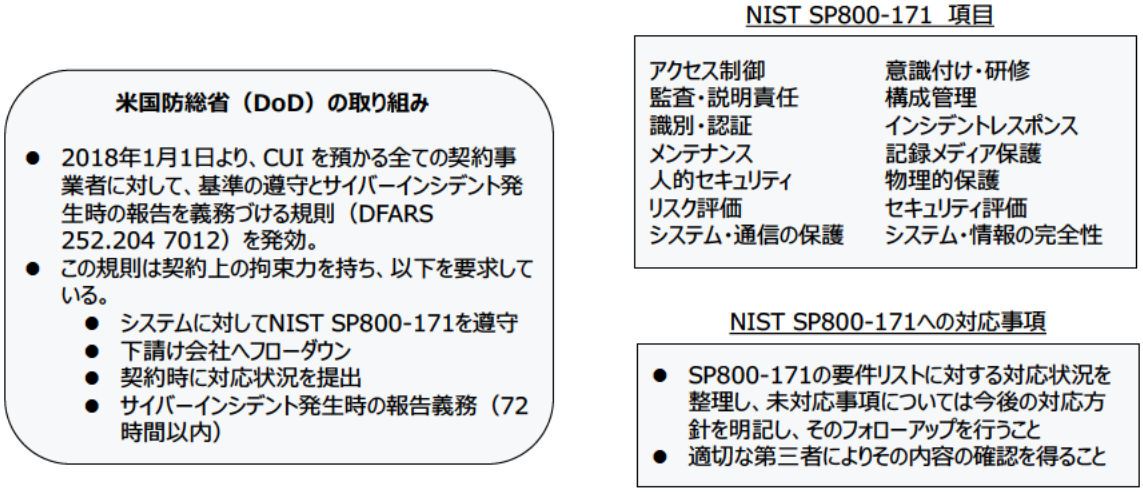


図 3-1　NIST SP800-171 の特徴

(2) CMMC

米国防総省は NIST SP800-171 の管理策に 「5 段階（レベル評価 ）」 を加えた新しい認証の仕組みとして CMMC[2] を適用することとした。

---

[1] NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

[2] CMMC：Cybersecurity Maturity Model Certification（サイバーセキュリティ成熟度モデル認証）

CMMC は成熟度モデルの構成を取っている。ソフトウェア開発等の成熟度モデルの「CMMI（Capability Maturity Model Integration：能力成熟度モデル統合）」と同様、定義された領域に対して、実施すべきプロセス、プラクティスが成熟度（レベル 1～5）にマップされる。特定のレベルを満たすためには、プロセスとプラクティスのいずれをも満たす必要がある。

プラクティスは、NIST SP 800-171 rev.1、 Draft NIST SP 800-171B、英国 Cyber Essentials、オーストラリア Essential Eight 等、複数のソースから組み込んでいる。ただし、多くは NIST SP800-171 の 110 項目をレベル 1 から 3 にマッピングしている。レベル 4 及び 5 は、さらに高度な対応を求められる企業に要求され、管理策も Draft NIST SP800-171B（SP800-172）のものが充てられている。

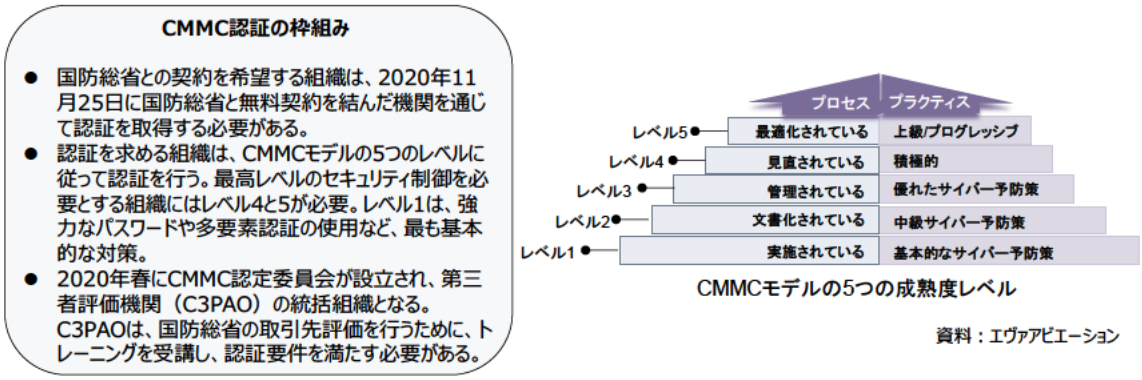


図 3-2　CMMC の特徴

国防総省は、国防総省と取引を行う事業者は 2025 年までに CMMC 認証を必要だとしている。CMMC の認証が必要な組織は、国防総省に製品やサービスを提供する全ての組織であり、30 万以上と見積もっている。C3PAO によるセキュリティ評価を 3 年毎に受け、特定の CMMC レベルに達していることの認証を受けなければならない。

CMMC 認定委員会（CMMC Accreditation Body：CMMC-AB）は認定第三者評価機関（C3PAO）の評価者を指導し、認定を行う。CMMC-AB は、国防総省の請負業者のために CMMC マーケットプレイスの立ち上げを計画している。

- C3PAO：職業行動規範に準拠し、ISO17021 認定を受け、100%米国市民の事業所有であるか、FOCI の身元調査を完了する必要がある。また、CMMC レベル 3 認定を取得する必要がある。初期費用 1,000 ドル、承認費用 2,000 ドル、継続費用 2,000 ドル/年。
- 認定 CMMC プロフェッショナル（Certified CMMC Professional：CCP）及び認定 CMMC アセッサ（Certified CMMC Assessor：CCA）：評価者。CCP は認定 CMP の監督下で評価チームメンバーになることが可能である。CCA はレベル 1・3・5 があり、各 CMMC ML-1・3・5 評価を実施することができる。
- 登録プロバイダ組織（Registered Provider Organization：RPO）及び登録実装者（Registered Practitioner）：認証を希望する企業に対して、アドバイス、コンサルティング、および推奨事項を提供できる。CMMC 評価は実施しない。
- ライセンスパートナーパブリッシャー（Licensed Partner Publisher：LPP）：大学、オンラインスクール、専門学校などの教育機関、あるいは消費者に対して、CMMC 関連のコンテンツ販売者、教育コースやコンテンツの発行者
- ライセンストレーニングプロバイダ（Licensed Training Provider：LTP）：CMMC 関連

の認定トレーニング提供者

認証取得までは 6 ヶ月以上が想定される。10 のステップは以下の通り。

1. CMMC の要求を理解する。
2. 企業、組織単位、プログラム単体等、スコープを特定する。
3. マチュリティレベルを決定する。
4. オプションとして、RPO または C3PAO による事前評価を行う。
5. 特定されたギャップを埋める。
6. CMMC-AB マーケットプレイスで C3PAO を探す。
7. C3PAO の認定された評価チームによる評価を受ける
8. 調査結果を解決するための最大 90 日の余裕がある。
9. CMMC-AB が評価結果をレビューする。
10. 評価結果が受け入れられると、3 年間有効の認証が取得できる。

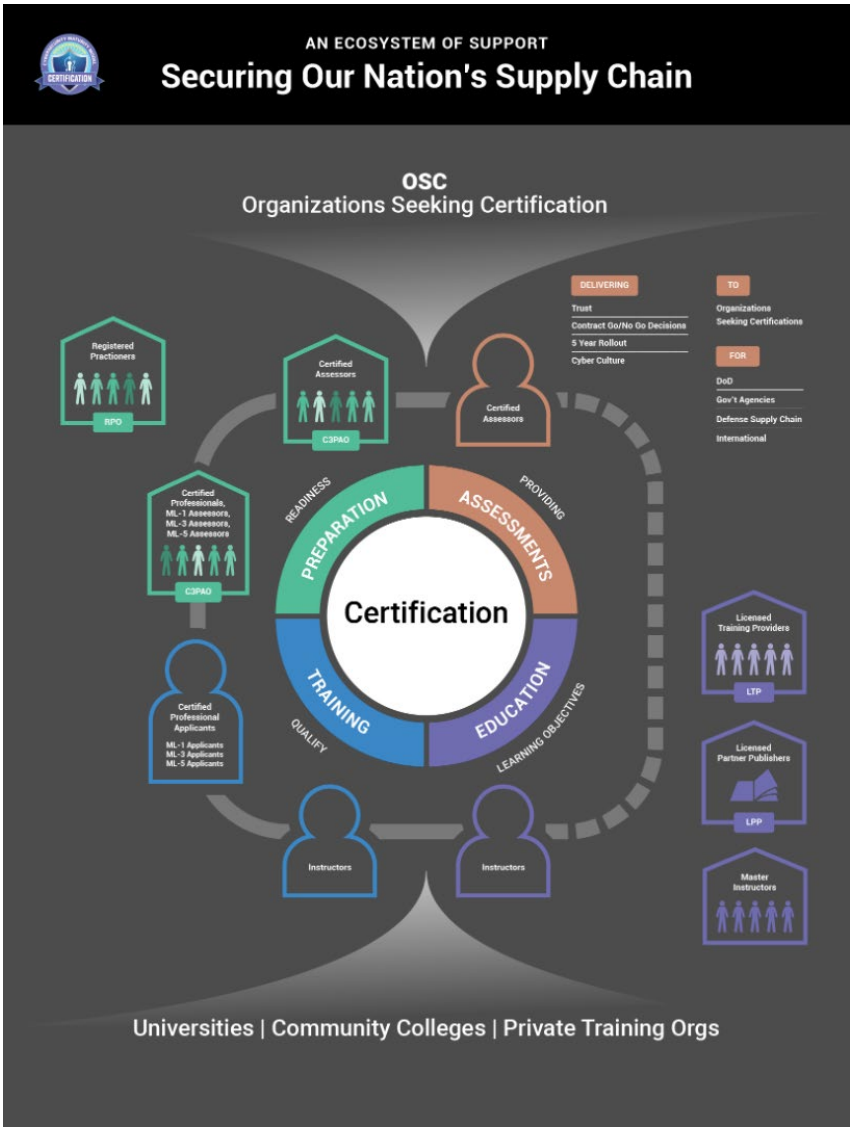


図 3-3　CMMC のエコシステム（https://cmmcab.org/）

図 3-4　CMMC エコシステムにおける評価スケジュール（https://cmmcab.org/）

3.1.2 欧州

(1) 輸出管理（EU ICP Guidance）

欧州の EU ICP[3] Guidance は、輸出業者がデュアルユースの貿易管理に関連するリスクを特定、管理、軽減し、関連する EU および国内の法律や規制を確実に遵守するためのフレームワークを提供することが目的である。

このガイダンスの中に、サイバーセキュリティの項目が含まれている。

ガイダンスは、企業が有効な認定経済事業者（Authorized Economic Operator）の認可を保持している場合、企業の税関活動の評価は、 ICP を開発またはレビューする目的の際に考

[3] ICP：Internal Compliance Programme

慮に入れることができる。なお、ガイダンスは明示的に拘束力がないため、ICP を実施する義務はない。

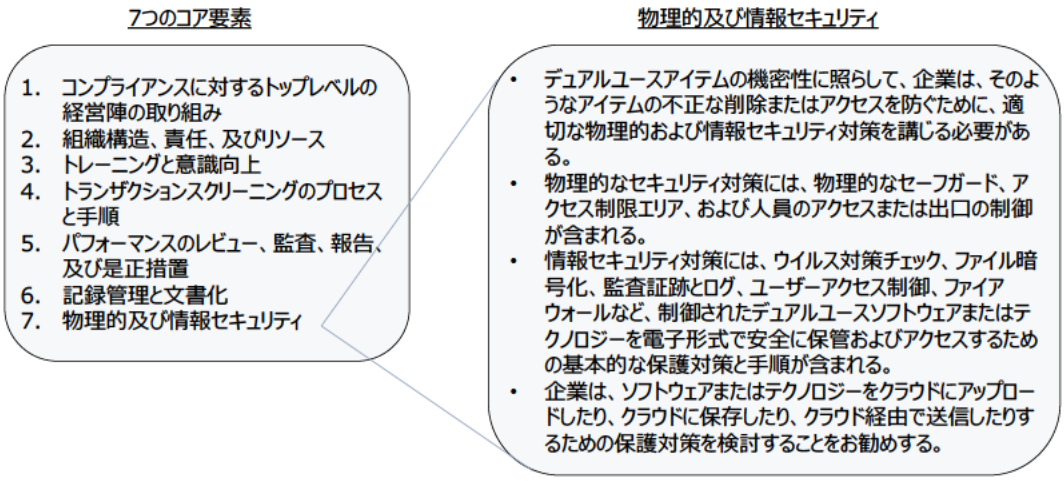


図 3-5　EU ICP Guidance

(2) GDPR

EU データ保護規則（GDPR）は、EU における個人データ保護に関する法律であり、1995 年に施行された「Data Protection Directive 95（EU データ保護指令）」に代わる法規制として 2016 年 4 月に制定され、2018 年 5 月 25 日に施行されている。

一般消費者、従業員、企業担当者等全ての個人について個人識別につながる情報が対象（オンライン識別子（例：IP アドレス）など、日本の個人情報保護法には含まれないデータも含まれる）となっている。

組織の情報管理としては、ISO/IEC 27001 の取組みに GDPR を取り込んで情報管理を進めるアプローチが見られる。

組織の情報管理とは異なるが、EU で従来からなされていた認証の取組みとして、EuroPriSe（欧州プライバシー・シール制度）は IT 産業に対するプライバシー・シール、EDAA（ヨーロッパの広告業界）や米国の TRUSTe（第三者が認証する個人情報・プライバシーに関する保護シールプログラム）等がプライバシー・シールの仕組みを運用しており、EU データ保護規則は、このような認証の取組みを明確にデータ保護の仕組みとして位置付けている。

図 3-6　GDPR データ保護認証の例（ビューロベリタス）

＜ウェブプライバシー認証＞

- TRUSTeマークがあるウェブサイトは、OECDプライバシーガイドラインに基づいたプライバシー保護の取り組みを実践し、その内容をプライバシーステートメントに記載している。
- プライバシーステートメントには、ウェブサイトを通じて収集した全ての個人情報の取扱いが完全公開される。
- TRUSTeは、プライバシーステートメント通りに個人情報が取り扱われているかどうかをチェックし、正しく運用されているウェブサイトに認証を与える。また、個人情報の取扱いに関するユーザーからの苦情を受付け、対応する。

図 3-7　TRUSTe

EuroPriSe
European Privacy Seal

＜IT 製品及び IT サービス認定＞

- プライバシー要件を満たす IT 製品および IT ベースのサービスのメーカーおよびベンダーに認定を提供。
- 法律および IT の専門家による製品またはサービスの評価と、独立した証明機関による評価レポートの検証で構成される。

＜ウェブサイトプライバシー認定＞

- EU のデータ保護法に準拠し、EuroPriSe のデータ保護要件を全て満たすサイトを認定。

図 3-8　EuroPriSe

3.2 国内動向の調査

情報管理や情報セキュリティ面で関連または類似する制度として、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）、プライバシーマーク（P マーク）、SECURITY ACTION を採り上げ、制度概要や審査内容等について調査を行った。

3.2.1 情報セキュリティマネジメントシステム（ISMS）

日本においては、情報処理サービス業のコンピュータシステムが十分な安全対策を実施しているかどうかを認定する制度として、昭和 56 年 7 月 20 日通商産業省告示 342 号による「情報システム安全対策実施事業所認定制度」（安対制度）があった。しかし、組織全体のマネジメントを確立する必要性が生まれ、この安対制度を廃止し、新たに情報セキュリティマネジメントシステム適合性評価制度を創設し、2002 年 4 月から本格運用を開始している。

表 3-1　情報セキュリティマネジメントシステム（ISMS）

項目	内容
名称	情報セキュリティマネジメントシステム適合性評価制度（Information Security Management System：ISMS）
概要	情報セキュリティの技術対策の他、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用する情報セキュリティマネジメントについて、国際基準への適合性を認証する制度
運営主体	情報マネジメントシステム認定センター（ISMS Accreditation Center：ISMS-AC） ※ 2018年、一般財団法人日本情報経済社会推進協会（JIPDEC）より独立し法人化
認証・審査機関等	日本品質保証機構、日本検査キューエイ、日本環境認証機構、防衛基盤整備協会システム審査センター、 日本規格協会ソリューションズ審査登録事業部、BSIグループジャパン 等27機関（2021年1月）
メリット	• 情報セキュリティを確保するための仕組みを持ち、その仕組みを維持し継続的に改善していることを顧客や取引先に対して客観的に示すことが可能 • 国際的な「適合性評価制度」に基づく制度であり、グローバルで調和の取れた取り組みが可能
関連・参照規格等	認証基準：JIS Q 27001（ISO/IEC 27001） ※ 認定機関（ISMS-AC）は、認証機関（ISO/IEC 27006）及び要員認証機関（ISO/IEC 17024）を認定
取得者数	6,327社（2021年1月）
対象となる情報	情報資産全般
取り組み対象	事業所・部門等
価格	取得 約90～100万円、更新 約70万円、維持審査　約50万円（従業員50名程度の場合、概算）
有効期間	3年（1年に1回維持審査）
他制度との関連	• 国際的なマネジメントシステム認証（ISO9001、ISO14001）との整合性あり • ISMSクラウドセキュリティ認証（ISO/IEC 27017：クラウド提供者/利用者がISMSにアドオンで取得可能な認証）
その他	• マネジメントシステムの認証であり、管理策については133項目のうち業務の実態に合わせて必要な項目を実施。

3.2.2 プライバシーマーク（P マーク）

1997 年、経済産業省が「個人情報保護に関するガイドライン」を改定し、日本企業が「EU データ保護指令」に自主的に適合できるよう個人情報保護の目安を提供した。この取組みを推進するため、その証をロゴによって示すことができる「プライバシーマーク制度」が創設され、1998 年 4 月、JIPDEC により運用開始された。2005 年、個人情報保護法の施行を機に知名度が高まり、認証取得事業者が増加している。

表 3-2　プライバシーマーク（P マーク）

項目	内容
名称	プライバシーマーク制度
概要	事業者が個人情報の取扱いを適切に行う体制等の整備を評価し、その証として「プライバシーマーク」の使用を認める制度
運営主体	日本情報経済社会推進協会（JIPDEC）　※付与機関
認証・審査機関等	一般社団法人情報サービス産業協会（JISA）、一般社団法人日本マーケティング・リサーチ協会（JMRA）、 一般財団法人医療情報システム開発センター（MEDIS-DC）、 一般社団法人日本情報システム・ユーザー協会（JUAS）等　19組織　※審査機関
メリット	• 「個人情報の保護に関する法律」（平成15年法律第57号）への適合性 • 自主的に高い保護レベルの個人情報保護マネジメントシステムを確立し、運用していることをアピールするツールとして活用
関連・参照規格等	JIS Q 15001個人情報保護マネジメントシステム－要求事項
取得者数	16,547社（2021年1月）
対象となる情報	個人情報
取り組み対象	企業全体
価格	取得 約62万円、更新 約46万円（従業員50名程度の場合、概算）
有効期間	2年間
他制度との関連	－
その他	• 要求項目全てを実施する必要あり。 • 審査員は登録制。付与機関から研修機関として指定を受けた団体が、審査員補を養成するための研修、並びに主任審査員、審査員及び審査員補が資格を維持するためのフォローアップ研修を実施する。 • 個人情報の取扱いにおける事故が発生した場合、報告書の提出が必要。提出された事故報告書については、「プライバシーマーク制度における欠格事項及び判断基準（PMK510）」に基づいて欠格レベルを判断し、外部有識者を交えた委員会の審議を踏まえて、最終的な措置が取られる。

3.2.3 SECURITY ACTION

2017 年 4 月、中小企業診断協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、IT コーディネータ協会、日本ネットワークセキュリティ協会、情報処理推進機構、中小企業基盤整備機構、日本商工会議所、日本税理士会連合会が、中小企業の情報セキュリティへの意識啓発及び自発的な対策の策定、実践の促進のため、連携して活動することを宣言。この核として SECURITY ACTION というセキュリティ活動の自己宣言の仕組みを創設した。

表 3-3　SECURITY ACTION

項目	内容
名称	SECURITY ACTION　（セキュリティアクション）
概要	中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
運営主体	独立行政法人情報処理推進機構（IPA）
認証・審査機関等	－　（取り組み実施を自己宣言する事業者が、IPAに対してロゴマークの使用を申込）
メリット	• ロゴをポスター、パンフレット、名刺、封筒、会社案内、ウェブサイト等に表示して、自らの取組みをアピールすることが可能 • 情報セキュリティへの取組みを宣言している中小企業等としてSECURITY ACTIONのウェブサイトに掲載
関連・参照規格等	★（一つ星）：中小企業の情報セキュリティ対策ガイドライン付録の「情報セキュリティ5か条」 ★★（二つ星）：中小企業の情報セキュリティ対策ガイドライン付録の「5分でできる！情報セキュリティ自社診断」を実施 情報セキュリティ基本方針を定め、外部に公開
取得者数	10万人以上（2020年7月）
対象となる情報	情報資産全般
取り組み対象	企業全体
価格	無料
有効期間	定め無し
他制度との関連	• IT導入補助金申請要件 • サイバーセキュリティ対策促進助成金（東京都）申請要件 • テレワーク導入支援補助金（堺市）申請要件
その他	• 2020年度、「中小企業の情報セキュリティマネジメント指導業務」によって、専門家派遣を受けることが可能。 （全国400社を対象に1社あたり4回専門家を派遣、指導は1回あたり2時間程度） • 2021年度以降、認定された中小企業向けセキュリティサービス（お助け隊サービス）を利用している「お助け隊マーク」と併用し、取引先に対して自社の信頼性をアピール可能となる見込み。

3.2.4 考察

(1) 各制度の特徴

情報管理や情報セキュリティ面で本認証制度に関連または類似する制度として調査した制度のうち、「情報セキュリティマネジメントシステム（ISMS）」「プライバシーマーク（Pマーク）」は認証の仕組みであり、「SECURITY ACTION」は自己宣言の仕組みである。

主な特徴は以下の通り。

- 情報セキュリティマネジメントシステム：対象は情報資産全般。国際標準（ISO）と共通のマネジメント規格構成となっており、品質、環境等複数のマネジメント活動を並行して行いやすい。マネジメント認証であるため、認証取得事業者であっても個々の対策レベルは事業者によって異なる。
- プライバシーマーク：対象は個人情報。「EU データ保護指令」に対して日本として自主的に適合できるよう成立した制度。認証対象は個人情報のみであり、コンプライアンス的な意味合いが強い。
- SECURITY ACTION：対象は情報資産全般。中小企業に特化したセキュリティ対策に関する自己宣言の仕組み。2020 年度、専門家派遣事業も合わせて提供され、中小企業のセキュリティ対策の普及・底上げにつなげている。

表 3-4　関連制度の違い

		ISMS	Pマーク	セキュリティアクション
制度概要	運営主体	情報マネジメントシステム認定センター（ISMS-AC）	一般財団法人日本情報経済社会推進協会（JIPDEC）	独立行政法人情報処理推進機構（IPA）
	対象となる情報	情報資産全般	個人情報	情報資産全般
	取り組み対象	事業所・部門等	企業全体	企業全体
	関連・参照規格等	JIS Q 27001（ISO/IEC 27001）	JIS Q 15001	中小企業の情報セキュリティ対策ガイドライン
	国内/海外	グローバル	国内	国内
審査内容	審査対象	マネジメントシステム（ISO/IEC 27001 付属書A 管理策133項目。ただし管理策は必要に応じて除外可能）	管理策（個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン）	管理策（中小企業の情報セキュリティ対策ガイドライン付録5項目または25項目）
	更新期間	3年（年1回維持審査：現地審査）	2年（年1回内部監査、更新時に内部監査結果提出）	定め無し（取り組んでいる限り宣言可能）
	内部監査	必要（外部委託可）	必要（外部委託可）	不要
	内部監査員の力量	定め無し（各種研修あり）	定め無し（各種研修あり）	－
	審査員の力量	「ISMS審査員の資格基準に関する指針」（JIPDEC）により、教育レベル、経験、研修、個人的資質の定め、「審査員補」「審査員」「主任審査員」の資格基準あり。	「プライバシーマーク審査員資格基準」（JIPDEC）により、就業経験、研修・試験合格の定め、「審査員補」「審査員」「主任審査員」の資格基準あり。	－
	特徴	国際標準（品質や環境）と共通の構成を持ち、複数のマネジメント活動を並行して行いやすい。対策レベルは企業の状況により異なる。	個人情報の保護に関する法律に基づく個人情報保護ルール及びマネジメントシステムを併せ持つ規格に準ずる。コンプライアンス準拠の性格が強い。	中小企業向けに特化した仕組みで、ファーストステップとして簡易な取り組みを示すもの。

(2) 本認証制度に関して検討が望ましい点

本認証制度は、保護すべきとして特定した情報を対象とした、情報管理に関わる第三者による認証の仕組みである。本認証制度の対象となる情報は、今回調査対象とした 3 制度いずれとも異なる。また、第三者による認証制度であるという点では ISMS、P マークと同様であるが、ISMS は国際標準（ISO）の規格や認証スキームに則っている点、P マークは国内標準規格（JIS）に則っている点で、本認証制度のスキームとは異なる。すなわち、本認証制度は、今回調査を行った関連制度とは対象となる情報や認証の枠組みは異なると言える。そのため、今後認証制度の普及を目指すためには、関連制度との違いを明確化し、ターゲットとなる事業者に普及啓発を促すことや、関連制度との連携を図り相乗効果を目指す等の方法が有効と考えられる。

また、普及方策については、ISMS、P マークとも、政府や民間企業における調達要件に含まれることで普及しており、SECURITY ACTION は、IT 導入補助金申請要件となり宣言件数が急増した。事業者にとって何らかのインセンティブが働くことで、認証取得件数あるいは自己宣言件数の増加につながることから、認証取得による事業者のインセンティブの創出は必須であると言える。

更新については、ISMS は 3 年更新（年 1 回維持審査）、P マークは 2 年更新（年 1 回内部監査）となっている。ISMS はマネジメントシステム認証であることから、更新自体は比較的長めの 3 年毎でよく、構築したマネジメント体制がきちんと運用されていることをサーベイランスで確認するという考え方である。P マークは、個人情報を有するやや小規模の

事業者も対象に含まれることから、過度な企業負担を避けることに配慮しつつ、事業環境やサイバーセキュリティ上の脅威の変化を踏まえ、2 年毎の更新となっている。更新とサーベイランスの考え方については、認証制度の目的・内容や、認証取得を想定する事業者が実施できるか等を踏まえて、異なるものとなる。

第三者による審査及び内部監査に関わる人員のスキル面では、ISMS 及び P マークとも、認証機関の審査員には資格要件があり、審査員に対する研修制度がある。また、いずれの制度も事業者側での内部監査が必要となっているが（外部委託も可能）、内部監査員への研修の仕組みがある。本認証制度では、審査員及び内部監査員のスキルが明確化されていないため、スキルの明確化及び育成の仕組みを検討することが有効と考えられる。

4. 普及のための広報活動等

本事業では、事業者における内部監査を支援するための各種ドキュメントの整備、事業者が情報管理の取り組みを進めるために参考とする研修素材、制度の普及啓発のためのパンフレットを作成した。

また、関連団体等におけるホームページやメールマガジン等を通じた、認証制度の広報活動を行った。

本認証制度における関連ドキュメントの位置付けを以下に示す。星印をつけたものが今年度作成したドキュメントである。

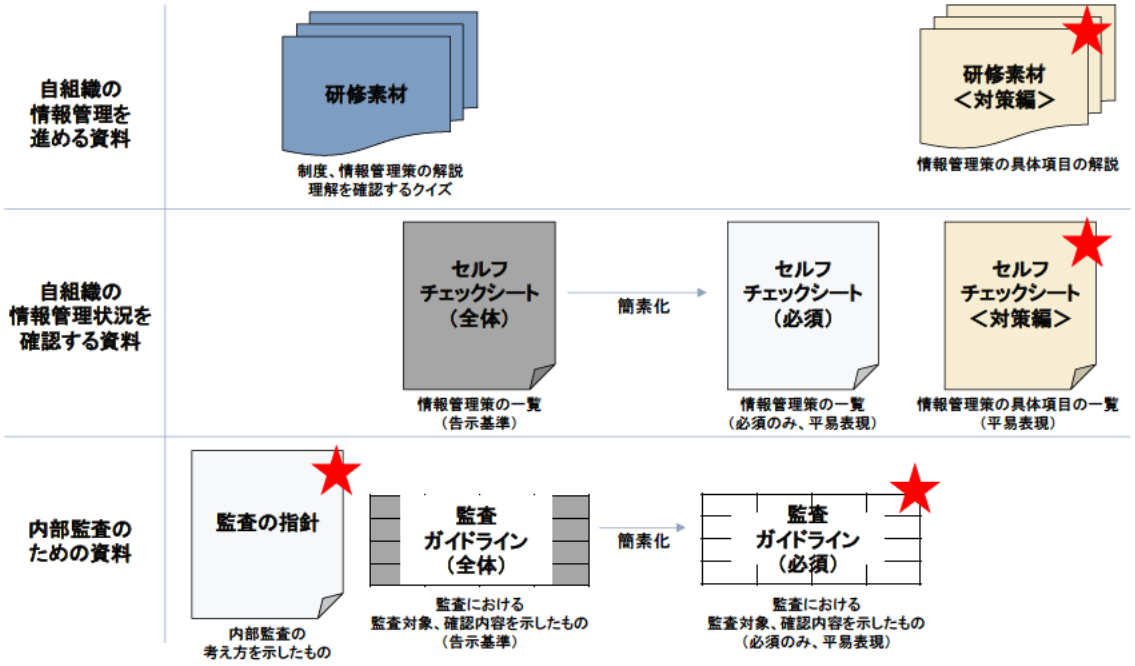


図 4-1　本認証制度における関連ドキュメント

4.1 内部監査関連資料の作成

内部監査を正しく実施し、必要な要件を満たす確認作業を容易に行うために、監査の際に参照可能なドキュメントやひな形等を提供する。2018 年度作成した「監査ガイドライン」及び「監査の指針」を更新した。

事業者が対策に取り組みやすくなるよう、具体的な実施事項に落とし込んだ「セルフチェックシート＜対策編＞」も策定した。

内部監査に求められる要件	（本事業で作成する）ドキュメント･ひな形
内部監査に用いる基準	
・監査人の行為規範	監査の指針（更新）
・評価の尺度（cf.チェックシートのチェック項目）	– 必須項目を対象 – セルフチェックシート＜対策編＞で目安を提示
内部監査人の要件 ・力量 （cf. 情報セキュリティ内部監査能力認定者）	– （=情報セキュリティ監査人資格等保有者）
内部監査人の独立性の要件 ・情報セキュリティ内部監査人の独立性に関するガイドラインに準拠	監査の指針（更新）
内部監査の監査手続 ・評価の根拠となる証拠及び評価の方法 （閲覧、質問、観察等）	チェックシートの必須項目について、各項目を 監査手続としてブレイクダウン（監査ガイドライン）
内部監査文書標準 ・監査計画書、監査報告書、監査調書など	監査計画書様式、監査報告書様式（済）
監査品質管理 ・ISO19011準拠等	–

4.1.1 監査の指針の更新、監査ガイドラインの策定方針

(1) 監査の指針

監査の指針については、以下の方針で更新を行った。

＜監査人の行為規範＞

- 公平性の観点や、理念等を守る点について、行為規範として追記。

＜内部監査人の独立性の要件＞

（掲載済）

- ＜内部監査文書標準＞

監査計画書ひな形を追加。（監査記録、監査報告書は掲載済）

＜監査品質管理＞

- 品質確保のためには客観性や公平性が必要となるため、ピアレビュー、独立した人のレビューを要求。
- 機密文書となるので、監査報告書等の管理が必要。

(2) 監査ガイドライン

監査ガイドラインについては、以下の方針で作成を行った。

- 告示の必須項目について、各項目を監査手続としてブレイクダウン。
- 各項目について、実施内容の定義がなされているか、実施されているか、責任者の承認・確認を得ているか、について確認する形で手続を具体化。

（注：2018 年度に作成した「監査ガイドライン」の内容は告示 1 項目毎に 1 監査手順で示しているが、今回の監査ガイドラインは告示 1 項目に対して複数の監査手続

きにブレイクダウンしており、2018 年度に作成した「監査ガイドライン」の表現は今回の監査ガイドラインの内容を包含していない部分がある）

- 事業者の方が利用するものとして、2018 年度に作成した「監査ガイドライン」の告示の表現にとらわれず、2019 年度に作成した「セルフチェックシート」の用語と整合性を取った、わかりやすい表現で作成。

(3) セルフチェックシート＜対策編＞

セルフチェックシートにおいて記載している告示の必須項目について、具体的に示す内容として参考となる項目を「セルフチェックシート＜対策編＞」として整理した。

記載項目は、他の関連基準やガイド等（ISMS、2018 年度業界モデル（金型）、セキュリティアクション等）で採り上げられている項目とした。さらに、対策の具体例としては「秘密情報の保護ハンドブック」等関連するドキュメントも参照した。

	必須項目	具体化項目（例）
1	重要情報の識別	（告示に記載された識別例）
2	（預けられた情報）	–
3	管理者の選任	–
4	（全従業員の認識）	–
5	管理の基本的な考え方	識別の手順確立、廃棄の手順確立、具体的な実現手法を記した文書（マニュアル）の作成
6	重要情報の管理をするためのトレーニング	（告示に記載されたトレーニング内容）
7	重要情報の漏えいの事故発生時の報告	報告手順の作成、事実関係の確認・必要な措置の手順・体制の確立
8	人的アクセスの制限	（告示に記載されたアクセス権設定時の考慮事項）、アクセス権者範囲の適切な時点での見直し、 アクセス権者の責任の明確化、必要がなくなった時点での速やかな失効、アクセス権者との秘密保持契約、 アクセス権者への教育、規則違反時の対応に関する社内規程
9	保管容器に保管できるものの物理的アクセスの制限	保管容器の施錠、保管容器に接近する者の監視（カメラやセンサーの設置）、 保管容器から持ち出す場合の手順
10	保管容器に保管が困難な場合等の物理的アクセスの制限	入退室管理、不審者の侵入に係る視認性向上、警備員等の駆け付け体制整備、常時監視 情報通信機器等の持込み禁止、運搬時の確認
11	（外部保管の場合）	–
12	電子情報の場合のアクセスの制限等	セキュリティに配慮した利用者の操作手順書の作成、ファイアウォールの導入、ログの取得・保存、 不正アクセス検知時の対応手順の策定、脆弱性情報管理、システム構成要素の管理簿の作成・管理、 ウィルス対策ソフトウェア等の導入・定期的な更新、ソフトウェアの導入管理、バックアップ、アクセス権管理（一意のID、適切な利用権限、パスワード管理）、クリアデスク、持ち出し手順の作成、外部委託管理

4.2 研修素材の作成

研修素材については、技術情報管理認証制度で定められる基準を元に、技術情報管理に関して、より具体的な管理方法の例や様式サンプルを示すために策定した。

以下の方々に対して活用いただくことを想定している。

- 情報管理を進める事業者、研究機関等の皆様
  - 情報管理を進める際の具体的な方法として参照していただく。
  - 内部監査を行う際に、管理方法についての妥当性を判断する参考にできます。
- 助言を行う組織や専門家の皆様
  - 事業者、研究機関等への助言の参考として活用いただく。

研修素材に記載した対策は「セルフチェックシート＜対策編＞」に一覧化しているため、対策の確認のために活用いただくことが可能である。

表 4-1　研修素材の項目

● 技術情報管理認証制度とは
● 技術情報管理認証制度における情報管理の進め方
● 各項目における具体的な対策

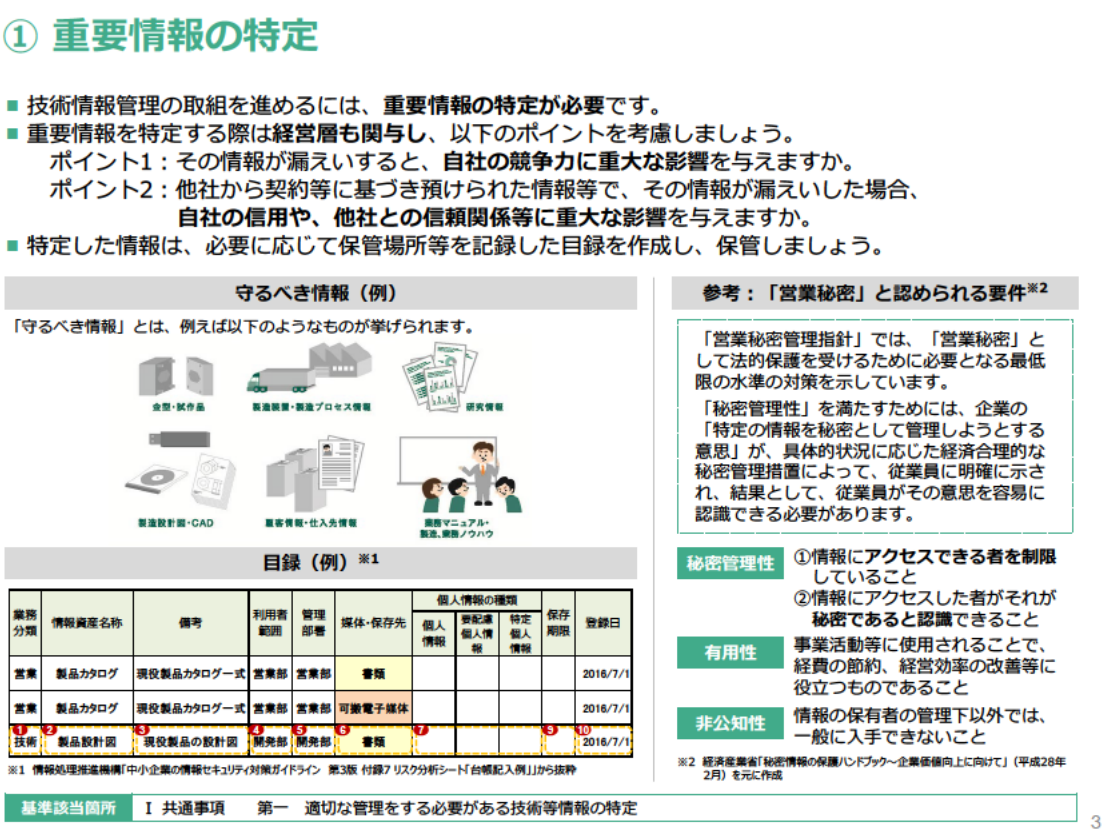


図 4-2　研修素材（イメージ）

4.3 パンフレットの作成

認証制度の認知度向上及び普及を目的として、パンフレットを策定した。2018 年度にもパンフレットを策定しているが、今年度は、適切な情報管理の重要性に加え、認証取得のメリットを訴求すること、及び実際の情報管理の取組みを促し、認証取得を視野に入れていただくことを目的として作成した。目的に照らして、中小企業の経営層（研究機関の責任者）から情報管理責任者など、認証取得を進める方を対象とした。

主な改訂ポイントは以下の通りである。

- 制度としての認知度向上（マーク・名称・略称の明示）
- 認証取得の情報充実（取得のための実施事項、認証取得によるビジネス上の効果、情

報管理の取組概要（チェックシート））

作成に当たってのポイント	●ターゲット： 中小企業の経営層（研究機関の責任者）～情報管理責任者を想定 ●目的と内容： 適切な情報管理の重要性に加え、認証取得のメリットを訴求 実際の情報管理の取組みを促し、認証取得を視野に入れていただく
	●サイズ： 一覧性の高いサイズ「出来上がりA4判2頁（両面） ※チェックシートは別紙、Webではセットで公開 ●カラー： 訴求力の高い「両面カラー印刷」 ●その他: マーク・略称による認知効果向上、国の制度であることの明示による信頼性向上 アピールポイントや訴えたい点に絞って提示、ストーリーをシンプル化してわかりやすさアップ 相談先としての認証機関連絡先はWebサイトへ誘導（QRコード）し情報量を絞る

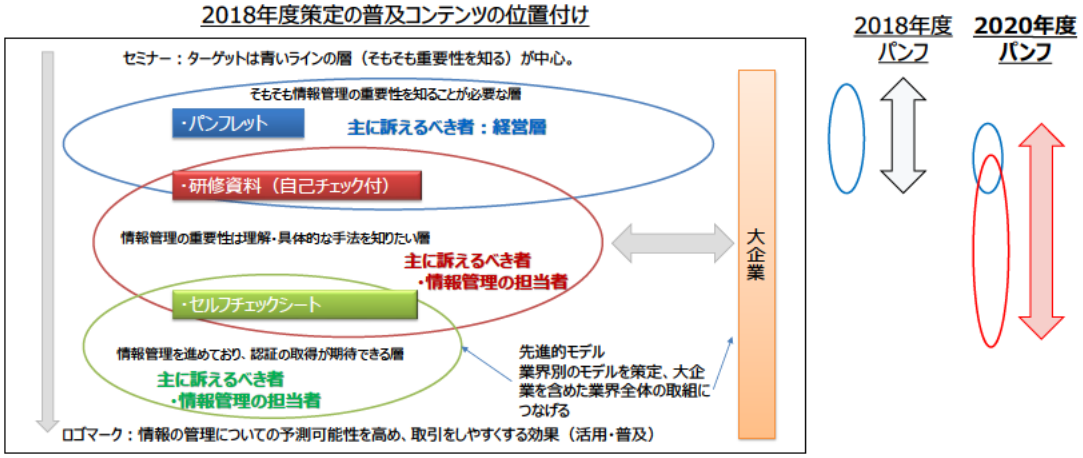


図 4-3　パンフレットの目的と概要

2018年度内容		改訂方針
表紙 (1)	・情報管理に関する疑問の投げかけ（内容への誘導）	削除
中左 (2)	・情報漏えい事例 ・情報漏えいによる企業経営への悪影響 ・情報管理の重要性	ボリューム減
中右 (3)	・認証制度の特徴	強化
	・サポートコンテンツ - セルフチェックシート 研修素材	削除 （Webへ誘動）
	・取組企業事例	更新
裏 (4)	・FAQ - 対象となる情報 - ISMSとの違い	削除
	・Webサイトへの誘導（METI名称含む）	維持

2020年度内容		備考
表	・認証制度概要（マーク・名称・略称・国の制度）	新規に策定したマーク・名称等のアピール
	・認証制度の特徴	
	・対象となる情報	
裏	・情報管理の重要性	データで提示
	・認証取得による効果	
	・認証取得のための実施事項（取組手順）	
	・認証取得事例	更新
	・Webサイトへの誘導（METI名称含む）	
別紙	・セルフチェックシート	具体的な取り組みイメージ
	・Webサイトへの誘導（METI名称含む）	

図 4-4　パンフレット内容構成

図 4-5　パンフレット（1/3）

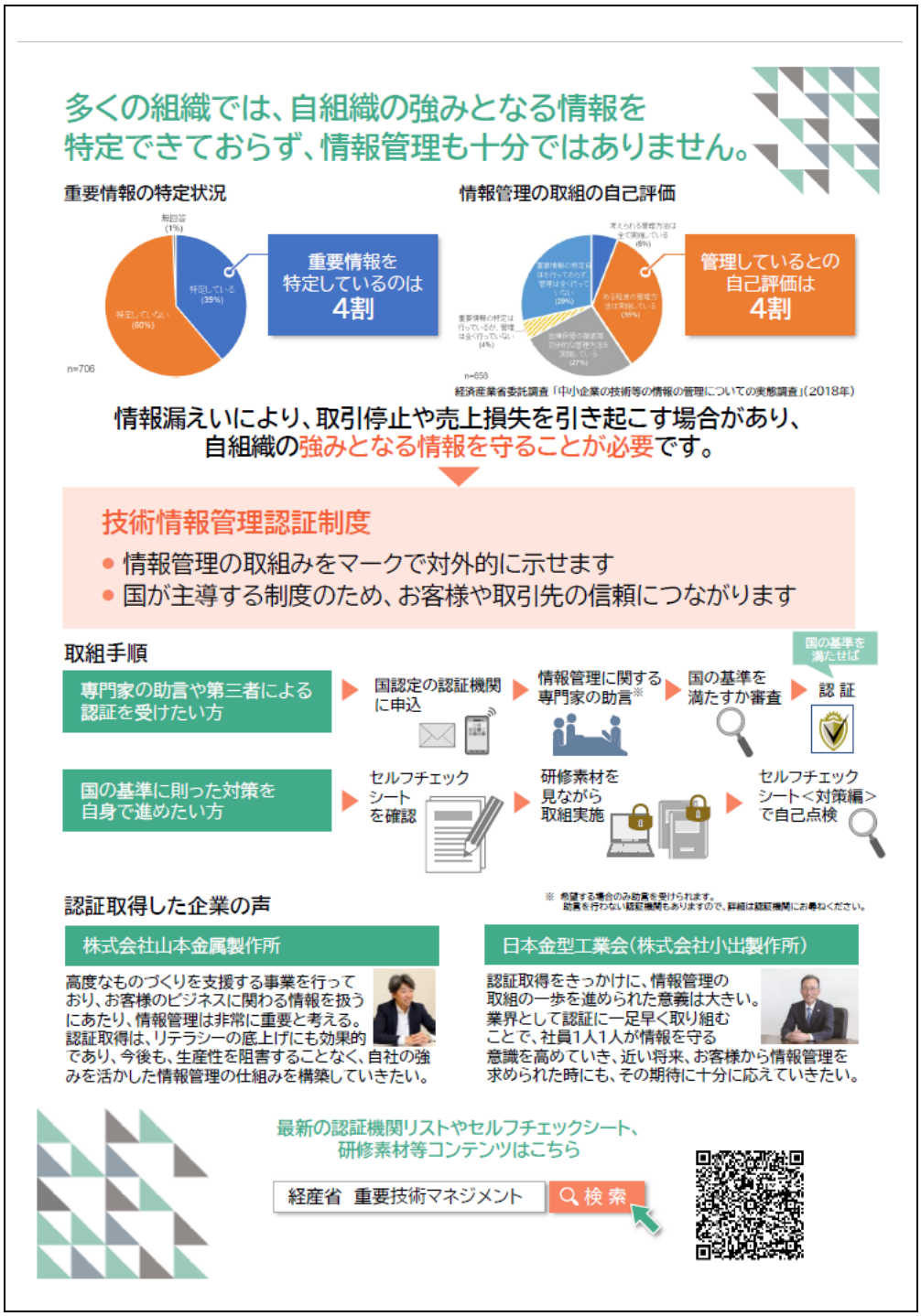


図 4-6　パンフレット（2/3）

別紙：情報管理の取組みをチェックしましょう！

重要な情報を守るために必要な取組みは以下の9項目です。

セルフチェックシート

	目 次	内 容	告示番号
共通事項			
1	重要情報の特定	情報が漏えいした場合に、自身の競争力に重大な影響を与えるような、特別な管理を必要とする重要情報を特定している。	Ⅰ 共通事項 第一 1
2	重要情報の識別	重要情報であることを明らかにするために、「関係者外秘」などの表示等を行っている。	Ⅰ 共通事項 第二 1
		重要情報の価値や形態（モノ／電子情報）に応じて、必要な管理方法を決定している。（他者から預けられた重要情報は、当該他者からの意見に基づく）	Ⅰ 共通事項 第二 2、3
3	管理者の選任	経営層は、以下の重要情報の管理に関わる責任者を定める。 （1）情報管理の手順を確立する。 （2）情報を取り扱う者の制限・管理、トレーニングを行う。 （3）情報漏洩防止対策を実施し、その実施状況を把握する。 （4）情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 （5）(2)-(4)の記録を取得し、保管する。	Ⅰ 第三1（1）
		従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識させるようにしている。	Ⅰ 第三1（2）
4	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	Ⅰ 第四 柱書き
5	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	Ⅰ 第五 柱書き
6	重要情報の漏えいの事故発生時の報告	情報漏えいの事故が発生した場合の報告先を定め、全従業員に対して周知している。	Ⅰ 第六 柱書き
7	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	Ⅱ 柱書き
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）			
8-1	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ 柱書き
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）			
8-2	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	Ⅳ 柱書き
		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	Ⅳ 柱書き
管理対象情報が電子情報の場合			
9	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	Ⅴ 柱書き

具体的な取組のための教材もWebサイトから！

詳細についてはウェブサイトへ

経産省　重要技術マネジメント　検索

図 4-7　パンフレット（3/3）

5. 今後の方向性

(1) 自己適合宣言に関する取扱いの検討

本認証制度の運用については、認証の有効期限やサーベイランス審査の規定、認証証明書や認証番号体系の定め、制度略称及び英語名称・マークの策定、「自己適合宣言確認型認証」と「現地審査を含む認証」の位置付けの明確化等、制度運用上定める必要がある事項について定めると共に、認証制度の関係者が運用に関する共通認識を持つための内容について明確化することができた。このように検討された事項については、今後、指針のように何らかの形でドキュメント化することを検討すると共に、将来的には、このような運用上明らかとなる課題に対して、認定スキームを維持・改善・推進していくための組織的取組みも検討していくことが有効と考えられる。

「自己適合宣言確認型認証」と「現地審査を含む認証」の整理においては、第三者による認証という仕組み上、自己適合宣言を認証するという仕組みは制度の信頼性担保の観点から困難であることを示したが、一方で中小企業が情報管理について取り組み、認証を取得しやすい仕組みについては引き続き検討する必要がある。

(2) 認証制度におけるコンサルティングの扱いの整理と指導・助言の活用方策の検討

本制度においては、中小企業において広く情報管理を進めていくことを目的として、認証取得の前段階において指導・助言がある点が特徴的である。一方、指導・助言が認証機関で禁止されているコンサルティングに該当するものとなると、認証制度自体の信頼性を損ねることになりかねない。

今年度は、制度上の指導・助言の範囲について明確化したが、今後、各認証機関においても、「指導・助言」と「コンサルティング」を区別し、制度に準じた形で適切に事業者に提供できるよう、認証機関及び審査員に対して適切に示していく必要がある。

また、指導・助言については、広く事業者における情報管理の取り組みを進めるうえでは非常に有効であると考えられる。事実、専門家派遣を実施した専門家からは、守るべき情報の特定と必要な対策の選定については、専門家の支援が得られないと事業者にとって推進が難しいという意見も得られた。指導・助言については、今後見直しを検討している「自己適合宣言」と合わせ、有効に活用することで、広く情報管理の取り組みを進めるとともに、一層の制度普及が期待できる。

(3) 業界団体等と連携した認証制度の普及

認証制度の普及という点では、業界団体等を連携する形で進めることが、事業者にとっての信頼感や活動しやすさの点で、情報管理を進めやすいと考えられる。

そこで、今年度は十分な活動ができなかった、団体モデルの策定に関する取り組みをより強化していくことに加え、業界団体が認証機関となるようなモデルについても、今後検討していくことが望ましい。認証業務に知見のない業界団体等において認証機関を目指してもらうには、今年度の専門家派遣の知見を生かし、認定を目指す機関に対するガイドやひな形

の整備等を進め公開することで、認証機関をさらに増やすことにつながると考えられる。もちろん、今年度のような専門家派遣を行うことはより有効である。

(4) 事業者における認証取得を促す環境整備

情報管理は重要と考える事業者も多いが、専門知識の不足や人材がいないことから、事業者が自主的に対策を進めることは難しい。特に中小企業においては、経営課題として情報管理の優先順位が上がらず、対策実施に繋がりにくいのが現状である。また、事業者が情報管理に取組む際に、認証取得を検討されることが望ましいが、認証制度自体の認知度はまだ低く、認証取得に対するインセンティブは働きづらいのが実態である。

そこで、認証制度に関するプロモーションを積極的に行い、特に認証制度がターゲットとする層に向けて認知度を高めると共に、事業者にとって認証取得が事業上のメリットとなるような方策について検討し、事業者の認証取得を促すような環境の整備を進めていくことが引き続き必要である。従来からの検討課題としても挙げられているが、例えば、事業者間の取引の際の情報管理に関する信頼性を確認するための活用、入札・調達時に加点要素とする等の優遇、融資における優遇、認証取得事業者における保険料の優遇等の方策が考えられる。また、重要な技術輸出について本制度の適用を検討していく、防衛産業等で参照されている米国の認証制度や国内の他の情報管理に関連した認証制度等、他制度と連携することも普及を促す点で有効と考えられる。

認証制度の認知度を高めるためには、中小企業等にもわかりやすいホームページ等の媒体を整備するとともに、認証取得件数を増やし、認証制度の活用事例を積極的に公表する場や認証取得企業の表彰等も効果的と考えられる。

専門家派遣事業については2年目であり、件数としてはまだ伸ばす余地はあるが、利用した事業者からは情報管理を進めるにあたって高評価を得られていることから、継続実施を検討することが望ましい。

(5) 制度改善に伴う事業者及び認証機関の支援コンテンツの拡充

運用ワーキンググループの検討結果を踏まえ、制度については今後告示改正も含めて見直しの方向となった。このような制度改善に伴い、認証に関する認知度の向上を図る普及啓発資料や、事業者及び認証機関に対して認証取得を容易とするような支援コンテンツについて引き続き拡充していくことが、認証取得を促す上で有効である。

(6) 認証制度における審査員・監査人のスキル明確化と育成・登録制度等の検討

国内の関連する認証制度調査の結果、審査員や内部監査を行う監査人のスキルが明確化されていない点が、本認証制度との違いとして明らかとなった。今後、審査員や監査人のスキルの明確化や、審査員や監査人を育成・登録する仕組み等についても整備を進めることで、認証制度を普及させると共に、認証の品質を維持することが可能となる。

別紙１　監査の指針

別紙２　監査ガイドライン

別紙３　セルフチェックシート

別紙４　パンフレット

別紙５　研修素材

「技術等情報管理認証制度に係る指導支援等の専門家派遣及び
調査・広報事業」報告書

2021 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL 03-6858-3578

技術情報管理認証制度

別紙１　監査の指針

目 次

1. 前文

本指針は、技術情報管理認証制度における事業者の内部監査で活用することを想定したものである。

技術情報管理認証制度における監査の目的は、技術等情報に関する管理が効果的に実施されるように、事業者が選択した基準において、適切な管理策の実施状況を、監査人が独立かつ専門的な立場から評価することにある。
技術情報管理は事業者の責任において行われるべきものであり、監査は事業者の技術等情報管理が有効に行われることを支援するものである。

技術情報管理認証制度における監査は、「情報セキュリティ監査基準」を元に実施することが求められるが、本指針は、特に監査において、監査人が遵守すべき事項等について示す。

なお、技術情報管理認証制度で作成する「監査ガイドライン」は、一義的には認証機関が審査を行う際に参照されるものであるが、監査においても活用可能である。

2. 監査の原則

監査において、適切かつ十分な結論を導き出すため、以下の原則を順守することが必要である。

(1) 高潔さ

監査人は、監査業務を倫理的に、正直に、かつ責任感を持って行うことが望ましい。また、全ての対応について公正さを持ち、偏りなく行われることが望ましい。

(2) 公正な報告

監査に関する報告は、ありのままに、かつ、正確に監査活動を反映することが望ましい。

(3) 専門家としての正当な注意

監査人は、監査業務の重要性、及び監査業務に関わる利害関係者が監査を行う者に対して抱いている信頼に見合う正当な注意を払うことが望ましい。監査において根拠ある判断を行う能力を持つことが重要である。

(4) 機密保持

監査人は、その任務において得た情報の利用及び保護について慎重であることが望ましい。

(5) 独立性

監査人は、可能な限り監査の対象となる活動から独立した立場にあり、全ての場合において偏り及び利害抵触がない形で行動することが望ましい。小規模の組織においては、内部監査を行う者が完全に独立していることは可能でない場合もあるが、偏りをなくし、客観性を保つあらゆる努力を行うことが望ましい。

(6) 証拠に基づくアプローチ

監査証拠は、検証可能なものであることが望ましい。監査証拠は、入手可能な情報からのサンプルに基づくことが望ましい。

3. 監査の独立性について

3.1 独立性

技術情報管理認証制度では、「情報セキュリティ監査基準」と同様、監査を客観的に実施するために、監査人に対して監査対象から独立していることを求める。監査を客観的に実施することの要件として、精神上の独立性だけでなく、外観上の独立性も監査人に求める。

3.2 精神上の独立性

監査人は、監査の実施にあたり、監査の専門家としての判断をゆがめるおそれのある諸要因から影響を受けない精神状態、及び客観性を確保し、専門家としての公正不偏な態度を堅持できる状態を保持していなければならない。

3.3 外観上の独立性

監査人は、監査を客観的に実施するために、監査対象から独立していなければならない。認証取得を目的とした監査の場合、被監査主体と身分上、密接な利害関係を有することがあってはならない。

「情報セキュリティ監査人の独立性のガイドライン」によると、外観上の独立性とは、第三者から見た際に、誠実性、客観性が阻害されていると推測される次のような事実や環境を避けることである。

１）禁止すべき利害関係（経済的利害関係）

２）避けるべき外観（不適正な外観）

3.3.1 内部部門による監査における独立性

技術情報管理認証制度における監査について、特定部門を被監査主体として内部部門が監査を実施する場合を想定すると、以下のような阻害要因を避ける必要がある。

内部部門による監査における外観上の独立性の阻害要因

阻害要因	阻害要件の事例
１）禁止すべき利害関係（経済的利害関係）	● 内部監査部門または内部監査人は、被監査主体と協力したビジネス活動に関与している ● 内部監査部門または内部監査人は、被監査主体の監査対象となる情報セキュリティの設計、構築、検査の業務に関わっている ● 内部監査部門または、被監査主体から便益や贈与を受けている ● 内部監査人は、自分自身に利害関係があり、または公正な判断に影響を及ぼすと合理的に推測される ● その他、内部監査部門に内部監査活動の目的および計画の達成を妨げるような制約がある
２）避けるべき外観（不適正な	● 内部監査部門または内部監査人は、被監査主体の配下の部署に所属しておらず、組織上独立していない

外観）	● 必要な情報及び資料の入手が困難である ● 内部監査部門または内部監査人は、助言勧告等がしにくい環境がある ● 監査人が前事業年度に在籍していた組織（部門や子会社等）が被監査主体である

資料）「情報セキュリティ監査人の独立性のガイドライン」
（特定非営利活動法人 日本セキュリティ監査協会 審査委員会、2011 年）

具体的には、以下のような方法で独立性を確保することが考えられる。

＜独立性を確保する体制（例）＞

- 事業者の内部監査部門が情報管理に関わる監査を実施する。
- 本制度における被監査部門とは独立した内部監査部門または内部監査人を経営者が設置または任命する。
- 内部監査部門に専門知識が不足する場合は、情報管理やＩＴの専門知識を持ち、可能な限り客観的な立場である者を臨時監査人として経営者が任命し、監査部門を構成する。

3.3.2 外部者による監査における独立性

技術情報管理認証制度における監査について、事業者全体あるいは一部の部門を被監査主体として外部の者が監査を実施する場合を想定すると、以下のような阻害要因を避ける必要がある。

外部者による監査における外観上の独立性の阻害要因

阻害要因	阻害要件の事例
１）禁止すべき利害関係（経済的利害関係）	● 外部監査組織または監査人が、被監査主体から社会慣行を超える接待もしくは贈答を受けること、または、被監査主体に対して社会慣行を超える接待もしくは贈答を行う ● 監査人及びその監査人の配偶者が、過去に被監査主体の役員、経営の意思決定に重要なかかわりをもつ使用人等であった ● 監査人と生計を一にする 2 親等以内の親族等が、被監査主体の株式を保有している ● 外部監査組織及び監査人が提供する設計、構築または検査の業務に従事して、当該業務の結果を監査対象とする ● 外部監査組織または監査人が被監査主体の経営者の意思決定に関与している
２）避けるべき外観（不適正な外観）	● 特定の被監査主体または被監査主体のグループ企業から継続的に受け取る報酬が、監査人の収入の大部分を占める ● 被監査主体のグループ企業が監査主体となり、グループ内の別の企業を被監査主体として監査を行う

	● 情報セキュリティ監査の言明書を監査人自らが作成したと受け取られる行為をする ● 特定の被監査主体と監査人との間に訴訟が起きていることまたは起きる可能性が高い関係にある

資料）「情報セキュリティ監査人の独立性のガイドライン」
（特定非営利活動法人 日本セキュリティ監査協会 審査委員会、2011 年）

4. 監査の実施について

4.1 監査証拠の入手と評価

監査人は、監査計画に基づいて、適切かつ慎重に監査手続を実施し、監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

4.2 監査調書の作成と保存

監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

5. 監査の報告について

5.1 監査報告書の提出と開示

監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

5.2 監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要について、監査人が必要と判断した事項を明瞭に記載しなければならない。

5.3 監査報告書のレビュー

監査報告書は、独立した立場の者によるレビューを受けること、もしくはピアレビュー（立場や職種の近い者が相互に評価・検証する形のレビュー）を行うこと等により、監査品質を確保することが望ましい。

付録：監査計画書ひな形

技術情報管理認証制度 監査計画書

日　付

1. 監査の目的

　○　の情報に関する技術情報管理認証取得に向けた内部監査のため

2. 監査対象・日程等

事業所・部門	日程	監査人 （所属・氏名）	備考

3. 監査項目

監査項目	備考

付録：監査報告書ひな形

技術情報管理認証制度 監査報告書

日　付

宛　名

監査人署名

われわれは、公認情報セキュリティ主任監査人 氏名、情報セキュリティ監査人補 氏名からなる監査チームを組織し、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に照らして、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間に係る XXX を対象として技術情報管理の状況について監査を実施した。われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある。

われわれの監査は、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に準拠して行われた。監査は、技術情報の管理が効果的に実施されるよう、適切な管理策が採用されているか否かについて検討し評価している。採用した監査手続は、われわれが必要と認めたものを適用しており、監査の結果として意見表明のための合理的な根拠を得たと確信している。

われわれの意見によれば、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間に係る XXX を対象とした技術情報管理の実施状況は、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に照らして適切であると認める。

付録：監査記録（例）

章	節	項	番		内容				確認内容
Ⅰ	第四	1	(1)		共通事項	管理対象情報の管理等	管理対象情報の管理簿の作成等	管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。	管理対象情報管理簿（XX年XX月XX日～XX月XX日記録）を閲覧し、管理対象情報の持ち出し、複製、廃棄等の記録が示されていることを確認した。
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。	管理対象情報の管理手法を示したマニュアル（XX年XX月XX日策定、第2版）を閲覧し、管理対象情報の適切な管理についての具体的な実現手法が記載されていることを確認した。
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。	管理対象情報の管理手法を示したマニュアルの周知記録（XX年度）を閲覧し、経営層がマニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認した。 管理対象情報を取り扱う製造部門の従業員へのインタビューにより、マニュアルを認識していることを確認した。
	第六	1				管理対象情報の漏えいの事故等の発生時等の報告		事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。	管理対象情報の漏えい事故を発見、または疑いがあると認めた場合、報告先として定められた技術等情報管理責任者に対して、報告をするように指示された文書（XX年XX月XX日）を確認した。 本文書が、翌週の各部門の朝礼で周知されたことを各部門からの週次報告で確認した。

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
I	第一	3			共通事項	適切な管理をする必要がある技術等情報の特定		事業者は、管理対象情報を特定した場合には、当該管理対象情報の態様が、紙情報（管理対象情報が記載された紙をいう。以下同じ。）、電子情報（管理対象情報が電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）又は試作品、製造装置等の物自体のいずれに当たるか識別し、必要に応じて保管場所等を記録した目録を作成し、合理的な期間保管する。		3	特定された管理対象情報一覧　（必要に応じて、管理対象情報目録）の現地調査を実施し、管理対象情報を特定した場合は、態様を識別し、必要に応じて保管場所等を記録した目録を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 特定された管理対象情報一覧　（必要に応じて、管理対象情報目録）	3.実施の結果である成果物を管理している
	第二	1				管理対象情報の識別と必要な措置の整理		事業者は、管理対象情報であることを明らかにするために、表示等の方法により他の技術等情報と区別して識別できるよう必要な措置を講ずるものとする。表示により識別できるようにする方法としては、例えば、紙情報の場合であればその情報が記載された紙に管理対象情報であること（社外秘等の表示）を記載し、電子情報の場合であればファイル名に管理対象情報であることを記録し、試作品、製造装置等の物の場合であれば当該物そのもの又はその保管容器に表示することが考えられ、その他の方法としては、例えば、第一の3の目録による管理や電子情報にアクセス可能な者を限定したフォルダにより管理する方法等が考えられる。		4	管理対象情報目録、識別された管理対象情報を閲覧し、管理対象情報を識別できることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報目録、識別された管理対象情報	1.実施している
		3						事業者は、当該管理対象情報が他者から預けられたものである場合は、当該他者からの意見を聞いてこの告示に掲げる措置のうち必要なものを決定し、当該他者からの求めがあったときは、その状況を記録し、合理的な期間保管し、報告する。		6	預託元の要求に沿った記録・保管・報告記録を閲覧し、預託情報の管理措置は、預託元の意見を聞いて決定し、要求に応じて記録・保管・報告を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 預託元の要求に沿った記録・保管・報告記録	1.実施している
	第三	1	(1)			管理者の選任	原則	事業者の取締役等の経営層は、管理対象情報に関し、以下に掲げる事項についての責任を有する者（以下「管理者」という。）を選任する。なお、その一部の実施を他の者に委任することを妨げない。		7	組織的対策に関する規程及び管理対象情報管理責任者選任記録、管理対象情報を取り扱う者の制限・管理記録、トレーニングの実施記録、管理対象情報の漏えいの防止措置の実施記録、管理対象情報の漏えいや兆候の把握と事象があった場合に必要な対応等の措置を定めた記録を閲覧し、経営層が管理対象情報についての責任者を定めていることを確認する。	【規定等】 組織的対策に関する規程 【記録やその他の確認対象】 管理対象情報管理責任者選任記録、管理対象情報を取り扱う者の制限・管理記録、トレーニングの実施記録、管理対象情報の漏えいの防止措置の実施記録、管理対象情報の漏えいや兆候の把握と事象があった場合に必要な対応等の措置を定めた記録	1.実施している
				一					管理対象情報について、第二の2により必要と決定した措置に係る必要な手順を確立させること。				
				二					管理対象情報を取り扱う者の制限及び管理を行い、当該管理対象情報を取り扱う者に対するトレーニングを行うこと。				
				三					保管容器又は立入制限区域の鍵の管理又は暗証番号の設定等の管理対象情報の漏えいの防止のために必要な措置を講じ、その状況を把握すること。				
				四					管理対象情報の漏えいの兆候や漏えいの事実の把握に努め、その事象があった場合に必要な対応等の措置を講ずること。				
				五					二から四までに掲げる事項について、記録を取得し、合理的な期間保管すること。				

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
			(2)					事業者は、当該事業者の従業員等（事業者との間で雇用関係等のある者をいう。以下同じ。）が多い場合、その管理対象情報が複数の事業部門にまたがるものである場合等には、社内規程に定めることや社内における掲示をすること等により、（1）の各事項の責任を誰が有しているかを当該事業者の従業員等の全ての者が認識できるように措置を講ずる。		8	管理者を記載した社内規程や社内掲示の現地調査を実施し、全ての従業員等が管理者を認識できるための措置を講じていることを確認する。（従業員へのインタビューにより、管理者を認識しているかどうかを確認する）	【規定等】 【記録やその他の確認対象】 管理者を記載した社内規程や社内掲示	1.実施している
		2					従業員等が少人数の場合等の措置 1にかかわらず、事業者の従業員等が少人数の場合等には、当該事業者の取締役等の経営層の判断により、経営層の者が管理者を兼務することができる。事業者の従業員等が少人数の場合等とは、例えば、取締役等の経営層が全ての従業員等を認識することが可能な程度の人数であり、当該取締役等の経営層が管理対象情報の取扱い状況をほぼ把握できるとともに、従業員等から当該取締役等の経営層に対して、管理対象情報に係る報告等が直接される取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態が確立している場合等が考えられる。		9	管理者を経営層が兼務することの記録（議事録等）、または管理者を経営者が兼務することの従業員の認識の現地調査を実施し、管理対象情報の管理者を経営層の者が兼務するにあたり、経営層が判断したことを確認する。	【規定等】 【記録やその他の確認対象】 管理者を経営層が兼務することの記録（議事録等）、または管理者を経営者が兼務することの従業員の認識	1.実施している
	第四				管理対象情報の管理等			事業者は、管理対象情報の作成から廃棄までのプロセスを通じて、管理対象情報を適切に管理（当該管理対象情報の正確さ及び完全さを保護すること並びに当該管理対象情報にアクセスすることを認められた者が要求したときにアクセス及び使用が可能であるようにすることを含む。以下同じ。）するための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態（管理対象情報が複製された場合の当該複製された情報（当該管理対象情報が電子情報である場合における当該管理対象情報がプリントアウトされたもの及び紙情報である場合におけるスキャナ等により電子化されたものを含む。以下この第四において同じ。）を適切に管理するための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を含む。）を確立させた上で、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、当該管理対象情報の適切な管理を行う。		10	管理対象情報の管理状況（あるいは、管理対象情報（複製含む）の管理記録）の現地調査を実施し、管理対象情報の作成から廃棄までのプロセスを通じて、管理対象情報を適切に管理するための取組が従業員等において実践されていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の管理状況（あるいは、管理対象情報（複製含む）の管理記録）	3.実施の結果である成果物を管理している
		1	(1)			管理対象情報の管理簿の作成等		管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。		11	管理対象情報管理簿を閲覧し、持ち出し、複製、廃棄等の管理対象情報の状況が記載されていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿	1.実施している
			(2)					管理者は、（1）の管理簿について、他者から預けられた管理対象情報についてのみの状況を管理するため、自らのものと別にして管理簿を作成する。		12	管理対象情報管理簿（預託管理対象情報）を閲覧し、預託された管理対象情報は自らのものと別に管理簿を作成していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿（預託管理対象情報）	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
			(3)		管理者は、(1) 又は(2) の管理簿について、保管期間を定めた上、施錠したロッカー等において保管し、又は暗号技術を用いてサーバ又はパーソナルコンピュータ(以下「サーバ等」という。)に記録する等適切に管理(当該ロッカー等の鍵の管理を含む。)する。				13	保管期間の定めがあるもの、ロッカーでの管理状況又はサーバでの管理状況を閲覧し、管理者が管理簿について保管期間を定めたうえ、施錠したロッカー等に保管もしくは暗号技術等によりサーバ等に記録する等、適切に管理(当該ロッカー等の鍵の管理を含む。)していることを確認する。	【規定等】 【記録やその他の確認対象】 保管期間の定めがあるもの、ロッカーでの管理状況又はサーバでの管理状況	1.実施している
			(4)		管理者は、(2) の管理簿について(3)の保管期間を定める場合は、当該管理簿に係る管理対象情報を預けた他者の確認をとる。				14	保管期間の定めがあるもの、保管期間を定めたときの預託元の承認を閲覧し、管理者が管理簿の保管期間を定めるにあたり、預託元の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 保管期間の定めがあるもの、保管期間を定めたときの預託元の承認	1.実施している
			(5)		管理者は、(1) 又は(2) の管理簿を定期的に点検する。				15	管理対象情報管理簿の点検記録を閲覧し、管理者が管理簿を定期的に点検していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿の点検記録	1.実施している
			(6)		管理者は、(1)の管理簿について廃棄をしようとする場合は事業者の取締役等の経営層に、(2)の管理簿について廃棄をしようとする場合は当該管理簿に係る管理対象情報を預けた他者に、それぞれ確認をとる。				16	管理対象情報管理簿の廃棄の確認状況(もしくは、確認記録)の現地調査を実施し、管理者が管理簿を廃棄する場合に、経営層または管理簿に係る預託元に確認を取っていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿の廃棄の確認状況(もしくは、確認記録)	1.実施している
			(7)		管理者は、他者から預けられた管理対象情報等他の技術等情報と明確に区別することが必要なものについて、当該管理対象情報の識別が容易になるよう体系的に管理するための手順を確立する。				17	(他の技術等情報とのく別が必要な管理対象情報を識別するための手順)の閲覧及び手順に沿った識別状況の現地調査を実施し、管理者が預託管理情報等他の技術等情報と明確に区別することが必要なものについて、識別が容易になるよう体系的に管理するための手順を定めていることを確認する。	【規定等】 (他の技術等情報とのく別が必要な管理対象情報を識別するための手順) 【記録やその他の確認対象】 手順に沿った識別状況	3.実施の結果である成果物を管理している
		2	(1)		管理者は、作成された技術等情報が管理対象情報である場合について、その識別をするための手順を確立する。		管理対象情報の作成時の識別		18	(管理対象情報を識別するための手順)を閲覧し、管理者が管理対象情報を識別をするための手順を定めていることを確認する。	【規定等】 (管理対象情報を識別するための手順) 【記録やその他の確認対象】	1.実施している
			(2)		管理者は、(1)の手順に従って措置が講じられていることを実地に確認すること等その措置が速やかに講じられることを確保するために必要な取組を行う。				19	管理対象情報の識別を確保する取組の実施状況に関する、管理者の上長または経営層による確認状況の現地調査を実施し、管理者が(1)の手順に従った措置が速やかに講じられることを確保するために必要な取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の識別を確保する取組の実施状況に関する、管理者の上長または経営層による確認状況	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
			(3)					管理者は、他者から預けられた管理対象情報が他の技術等情報と組み合わされている場合等において、当該他者から、当該管理対象情報が識別可能となるようにすることを求められたときは、当該他者の求めに応じ、下線を引く、枠囲いをする等管理対象情報が分かるよう適切な措置を講ずる。		20	管理対象情報の区別状況（自らのもの、預託管理対象情報）の現地調査を実施し、管理者は、預託管理対象情報を他の情報と組み合わせて利用する際に識別可能となるよう預託元から求められた場合に、当該管理対象情報が他の情報の中で区別できるよう適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の区別状況（自らのもの、預託管理対象情報）	1.実施している
		3	(1)				管理対象情報の内容の伝達	管理者は、原則として、この告示のⅡによりアクセス権を設定された者（以下「アクセス権者」という。）に限り、管理対象情報の内容の伝達（管理対象情報である紙情報や電子情報に記録された事項を当該紙情報や当該電子情報を用いずに口頭等により伝えること及び閲覧させることをいう。）がされるようにするための手順を確立する。		21	情報資産管理規程を閲覧し、管理者がアクセス権者に限り管理対象情報の内容の伝達されるための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
			(2)					管理者は、アクセス権者がそのアクセス権者の属する事業者の他の従業員等（管理対象情報の他のアクセス権者を除く。以下この第四において「他の従業員等」という。）に対して管理対象情報の内容の伝達をしようとする場合には、当該アクセス権者から、管理者に対して承認を得るための手順を確立する。		22	情報資産管理規程を閲覧し、管理者がアクセス権者が他の従業員等に対して管理対象情報の内容の伝達する際に管理者の承認を得るための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
			(3)					管理者は、アクセス権者から他の従業員等に対する管理対象情報の内容の伝達についての承認を求められた場合には、当該伝達が真に必要なものか否かの確認を行い、伝達の範囲を可能な限り限定した上で、これを認める。		23	管理対象情報の他の従業員等に対する内容伝達の承認要求時の手順（及び、管理対象情報管理簿）を閲覧し、管理者がアクセス権者から管理対象情報の内容の伝達についての承認を求められた場合には、伝達が真に必要なものか否かの確認を行い、伝達の範囲を可能な限り限定した上で、これを認めているか管理者の上長又は経営者が確認していることを確認する。	【規定等】 管理対象情報の他の従業員等に対する内容伝達の承認要求時の手順 【記録やその他の確認対象】 （及び、管理対象情報管理簿）	3.実施の結果である成果物を管理している
			(4)					管理者は、管理対象情報の内容の伝達について、1の（1）又は（2）の管理簿に記録する。		24	管理対象情報管理簿を閲覧し、管理者が管理対象情報の内容の伝達を管理簿に記録していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿	1.実施している
		4	(1)				管理対象情報の複製	管理者は、管理対象情報の複製をアクセス権者のみが行うことができるようにするための手順を確立する。		25	情報資産管理規程を閲覧し、管理者が管理対象情報の複製をアクセス権者のみに許可することを手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
			(2)					管理者は、アクセス権者が、管理対象情報の複製をしようとする場合には、当該アクセス権者から、管理者に対して承認を得るための手順を確立する。		26	情報資産管理規程を閲覧し、管理者が、管理対象情報の複製をする際にアクセス権者を承認するための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
			(3)					管理者は、アクセス権者から管理対象情報の複製についての承認を求められた場合には、当該複製が真に必要なものか否かの確認を行い、複製の範囲を可能な限り限定した上で、これを認める。		27	管理対象情報の複製の承認要求時の手順（及び、管理対象情報管理簿）を閲覧し、管理者がアクセス権者から管理対象情報の複製の承認を求められた場合に、必要性の確認、範囲の限定を指示のうえ、承認していることを管理者の上長又は経営者が確認していることを確認する。	【規定等】 管理対象情報の複製の承認要求時の手順 【記録やその他の確認対象】 （及び、管理対象情報管理簿）	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
			(4)					事業者は、電子情報である管理対象情報について、情報システム（ハードウェア、ソフトウェア（プログラムの集合体をいう。以下同じ。）、ネットワーク又は電子記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。）を構成する機器及び可搬式記録媒体（USB記録媒体、光ディスク、外付けハードディスク等パーソナルコンピュータ等に挿入し、又は接続することでパーソナルコンピュータ等に記録されている情報を記録することが可能な電子記録媒体をいう。以下同じ。）であって、個人が管理するものへの複製をするための手順を確立する。		28	情報資産管理規程を閲覧し、電子情報である管理対象情報について、個人が管理する情報システムを構成する機器及び可搬式記録媒体への複製の手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
			(5)					事業者は、管理対象情報を複製した場合において、当該複製された情報を管理対象情報として適切に管理する。		29	（管理対象情報管理簿、及び）複製した管理対象情報の管理状況の現地調査を実施し、管理対象情報の複製にあたり、複製した情報を管理対象情報と同等の方法で管理していることを確認する。	【規定等】 【記録やその他の確認対象】 （管理対象情報管理簿、及び）複製した管理対象情報の管理状況	1.実施している
			(6)					事業者は、管理対象情報の内容を他の記録媒体に記録する場合等において、当該記録媒体自体を管理対象情報として管理するための手順を確立する。		30	情報資産管理規程（及び、管理対象情報管理簿）を閲覧し、管理対象情報の内容を他の記録媒体に記録する場合、記録媒体自体を管理対象情報として管理する手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 （及び、管理対象情報管理簿）	1.実施している
		5	(1)				管理対象情報の廃棄等	事業者は、管理対象情報の廃棄については、当該廃棄に係る管理対象情報を探知することができないよう、紙情報の場合におけるシュレッダーでの細断、電子情報の場合における完全消去や難読化等その管理対象情報の態様に応じ、焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により廃棄をするための手順を確立する。		31	情報資産管理規程（及び、管理対象情報管理簿）を閲覧し、管理対象情報は、焼却、粉砕、細断、溶解、破壊等復元不可能な方法により廃棄するための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 （及び、管理対象情報管理簿）	3.実施の結果である成果物を管理している
			(2)					事業者は、紙情報である管理対象情報をシュレッダーにより細断をする場合には、以下に掲げるいずれかの性能を有するシュレッダーを用いる。		32	ーシュレッダーの現地調査を実施し、第四5(2)一二三の性能を有するシュレッダーを用いていることを確認する。（監査時には、シュレッダーの性能を記録する）	【規定等】 ー 【記録やその他の確認対象】 シュレッダー	1.実施している
				一					縦横細断方式のシュレッダーであって、一辺を3mm以内とし、細断された紙の面積が4.5 平方mm以内に細断をすることができるもの			
				二					縦横細断方式のシュレッダーであって、細断された紙の面積が10平方mm以内（一辺は1mm 以内とするものに限る。）に細断をすることができるもの			
				三					縦細断方式のシュレッダーであって、一辺を1mm以内に細断をすることができるもの			
			(3)					事業者は、他者から預けられた管理対象情報について、当該他者との間の取引等が終了した場合には、当該他者との取決め等に基づき、速やかに当該他者に返却をし、及び当該他者とともにその記録をし、又は（1）若しくは（2）の方法により廃棄する等の適切な管理をするための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		33	情報資産管理規程及び預託管理対象情報返却記録、預託管理対象情報の廃棄状況（あるいは、管理対象情報管理簿（預託管理対象情報））の現地調査を実施し、預託された管理対象情報について、取引等終了時には、預託元との取決め等に基づき、速やかに返却、記録をし、または廃棄する等が実施されていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 預託管理対象情報返却記録、預託管理対象情報の廃棄状況（あるいは、管理対象情報管理簿（預託管理対象情報））	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。		34	管理対象情報の管理手法を示したマニュアルを閲覧し、管理対象情報の適切な管理についての具体的な実現手法を記載したマニュアルを作成していることを確認する。	【規定等】 管理対象情報の管理手法を示したマニュアル 【記録やその他の確認対象】	4.標準的な事項を定義している
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。		35	管理対象情報の管理手法を示したマニュアルの周知状況の現地調査を実施し、経営層は、マニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認する。（管理対象情報を取り扱う可能性のある者へのインタビューにより、マニュアルを認識しているかどうかを確認する）	【規定等】 【記録やその他の確認対象】 管理対象情報の管理手法を示したマニュアルの周知状況	5.定義された事項を周知し、同一事項を実施している
			(3)					事業者は、管理対象情報が他者から預けられた情報である場合であって、当該管理対象情報についてのマニュアルを当該他者からの求めに応じて作成するときは、当該他者に当該マニュアルの内容についての確認をとる。これを変更するときも、確認をとる。		36	マニュアル作成、変更に関する預託元の確認記録を閲覧し、預託された管理対象情報についてのマニュアルを預託元からの求めに応じて作成、変更するときは、預託元に内容の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 マニュアル作成、変更に関する預託元の確認記録	3.実施の結果である成果物を管理している
			(4)					事業者の取締役等の経営層は、第二の2により必要と決定した措置の実施の状況を管理者に記録をさせ、当該記録の保管期間を定め、定期的に確認する。		37	管理措置の実施状況記録、及びその記録の経営者の確認状況の現地調査を実施し、経営層が管理措置の実施状況を管理者に記録をさせ、当該記録の保管期間を定め、定期的に確認していることを確認する。	【規定等】 【記録やその他の確認対象】 管理措置の実施状況記録、及びその記録の経営者の確認状況	1.実施している
	第五				管理対象情報の適切な管理をするためのトレーニング			事業者は、アクセス権者を含む全ての従業員等への管理対象情報を含む技術等情報の適切な管理に関する意識の啓発を図るためのトレーニング（会議、講義、e-learning等いずれの実施形態であるかを問わない。）を受講させる機会を設け、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、管理対象情報を含む技術等情報に係る認識向上による不正行為者の言い逃れの排除等に資するよう取組を行う。		38	技術等情報管理研修の実施状況（実績）の現地調査を実施し、全ての従業員等への技術等情報の適切な管理に関するトレーニングを受講させる機会を設け、必要と決定した措置を実施し、管理対象情報を含む技術等情報に係る認識向上の取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 技術等情報管理研修の実施状況（実績）	3.実施の結果である成果物を管理している
		1						事業者は、アクセス権者を含む全ての従業員等に対して、技術等情報の適切な管理に関する知識及び能力の向上を図るため、以下に掲げる事項のうち必要なものに係るトレーニングを受講させる機会を設ける。		39	技術等情報管理研修の実施状況（実績）、及び研修内容(研修資料等）の現地調査を実施し、全ての従業員等に、必要と事業者が考えるもの（選択した内容）を含むトレーニングを受講させる機会を設けている。（監査時には、トレーニングに含まれる内容を記録する）	【規定等】 【記録やその他の確認対象】 技術等情報管理研修の実施状況（実績）、及び研修内容（研修資料等）	1.実施している
				一					技術等情報と管理対象情報の違い				
				二					管理対象情報を適切に管理することの重要性、意識				
				三					管理対象情報を含む技術等情報の漏えいとその結果の事例				
				四					関係法令の内容				
				五					マニュアル、この告示のⅧの第四の方針又は対策等技術等情報の適切な管理に係る文書を作成している場合には、その内容				
				六					四及び五の関係法令等に違反した場合の処分等				

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
				七					管理対象情報の漏えいの事故等（管理対象情報の紛失の事故及び改ざん又は破壊がされた事実を含む。以下同じ。）が発生したことを発見した場合の報告手続				
				八					標的型メール等の警戒すべき手口並びに標的型メール等による情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染を防止するための対策及び感染した場合の対処の手順				
		2						事業者は、トレーニングを受講させる機会を定期的に設ける。		40	技術等情報管理研修計画及び技術等情報管理研修記録を閲覧し、トレーニングを受講させる機会を定期的に設けていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 技術等情報管理研修記録	1.実施している
		3						事業者は、従業員等における秘密の管理に係る意識の啓発を一層図るため、アクセス権者を含む全ての従業員等について、トレーニングに加えて、技術等情報の適切な管理に係る従業員相互間の確認を定期的に行わせるようにする。		41	技術等情報管理研修計画及び従業員相互間の定期的な確認記録を閲覧し、アクセス権者を含む全ての従業員等について、トレーニングに加えて、従業員相互間の確認を定期的に行わせていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 従業員相互間の定期的な確認記録	1.実施している
		4						事業者は、アクセス権者（アクセス権を設定することが見込まれる者を含む。）に対して、管理者又は当該管理者が指定する者により、例えば、Need to Knowの原則（情報は必要のある人のみ（情報へのアクセスは必要な人のみ）に伝え、知る必要のない人に伝えない（情報へのアクセスが必要ではない人にはアクセスを認めない。）という原則をいう。以下同じ。）を守ることの重要性（勤務において留意すべき事項を含む。）、管理対象情報の取扱手続の詳細や情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）を含むトレーニングを受講させる機会を設ける。		42	アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）の現地調査を実施し、アクセス権者に対して、管理者又は当該管理者が指定する者により、Need to Knowの原則を守ることの重要性（勤務において留意すべき事項を含む。）、管理対象情報の取扱手続の詳細や情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）を含むトレーニングを受講させる機会を設けていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）	2.実施計画があり、進捗管理している
		5						事業者は、アクセス権を設定することが見込まれる者については、原則として、管理対象情報にアクセスさせる前に4のトレーニングを受講させる。		43	研修の実施状況（及び、アクセス権者の設定の管理票）の現地調査を実施し、アクセス権を設定することが見込まれる者には、管理対象情報にアクセスさせる前に4のトレーニングを受講させていることを確認する。	【規定等】 【記録やその他の確認対象】 研修の実施状況（及び、アクセス権者の設定の管理票）	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		6						事業者は、アクセス権者に1（1の八の対処を実践させることを含む。）及び4のトレーニングを受講させる機会を1年に1度以上設ける。		44	技術等情報管理研修計画及びアクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容（研修資料等）の現地調査を実施し、アクセス権者への技術等情報の適切な管理に関するトレーニングを受講させる機会を1年に1度以上設けていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容（研修資料等）	2.実施計画があり、進捗管理している
		7						事業者は、アクセス権者のうちの4のトレーニングの未受講者に対して、アクセス権の失効等の適切な措置を講ずる。		45	アクセス権者のアクセス権の設定等の管理記録の現地調査を実施し、アクセス権者のうちのトレーニングの未受講者に対して、アクセス権の失効等の適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者のアクセス権の設定等の管理記録	2.実施計画があり、進捗管理している
	第六				管理対象情報の漏えいの事故等の発生時等の報告			事業者は、従業員等が管理対象情報の漏えいの事故等が発生したことを発見した場合、従業員等が管理対象情報を漏えいさせ、又は目的外に利用すること等事業者内部において情報の取扱いに係る不正を発見した場合等における報告先を、社内規程に定めること、社内における掲示をすること等事業者内部の従業員等の全てが認識できる方法により明らかにした上で、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、管理対象情報の漏えいの事故等が発生した場合の対応を迅速に講ずる。		46	管理対象情報漏えい事故発生時の報告先の設定状況、及び周知状況の現地調査を実施し、以下の2点について確認する。 ①従業員等が管理対象情報の漏えいの事故等の発生を発見した場合、事業者内部で情報の取扱いに係る不正を発見した場合等の報告先を、社内規程に定めていること ②報告先は、社内に掲示をする等従業員等が認識するようにしていること	【規定等】 【記録やその他の確認対象】 管理対象情報漏えい事故発生時の報告先の設定状況、及び周知状況	1.実施している
		1						事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		47	事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者を含む全ての従業員等に対して、管理対象情報の漏えい又はその疑いがある場合、直ちに、報告先に報告させるための手順を定めていることを確認する。	【規定等】 事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況	3.実施の結果である成果物を管理している
		2						事業者は、アクセス権者に対して、管理対象情報の紛失の事故及び改ざん若しくは破壊がされた事実、これらの事故若しくは事実につながる事象又はこれらのおそれのある場合等管理対象情報の適切な管理に支障が生じ、又は生じるおそれがあるとアクセス権者が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		48	アクセス権者における事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者に対して、管理対象情報の適切な管理に支障が生じるおそれがある場合に、直ちに、報告先として指定した者に報告をさせるための手順を定めていることを確認する。	【規定等】 アクセス権者における事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況	3.実施の結果である成果物を管理している
		3						事業者は、アクセス権者に対して、これまで接触がなかった者からのコンタクト（電話、メール、食事の誘い等）が著しく増加し、又は定期的に行われている場合や、保管容器等管理対象情報への物理的なアクセス制限措置（以下「物理的措置」という。）の不具合、第二の2により必要と決定した措置についてこの告示で求められる事項若しくは情報の取扱いに係る社内規程に照らした場合の不適合又はこれらの不具合若しくは不適合が発生するおそれがあることを発見した場合等管理対象情報の漏えいの兆候とアクセス権者が認める場合に、速やかに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		49	アクセス権者における事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者に対して、管理対象情報の漏えいの兆候とアクセス権者が認める場合に、速やかに、報告をさせるための手順を定めていることを確認する。	【規定等】 アクセス権者における事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況	3.実施の結果である成果物を管理している

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
		4						事業者は、アクセス権者を含む全ての従業員等に対して、以下に掲げる事項を含む管理対象情報の漏えいにつながると考えられる事象を発見した場合に、速やかに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		50	事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、全ての従業員等に対して、管理対象情報の漏えいにつながると考えられる事象を発見した場合に、速やかに、報告をさせるための手順を定めていることを確認する。	【規定等】 事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況	3.実施の結果である成果物を管理している
				一					管理対象情報への業務上必要のないアクセス行為を発見した場合				
				二					業務上必要がないにもかかわらず、個人が所有する可搬式記録媒体又は通信機器で管理対象情報を取り扱っている行為を発見した場合				
				三					特定の競合他社等外部の者とアクセス権者が頻繁に接触している事象を発見した場合				
				四					物理的措置についての破損等の不具合を発見した場合				
				五					電子情報である管理対象情報を記録しているサーバ等へのアクセス回数が大幅に増加していること、当該サーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等に感染していること又は当該サーバ等への不正アクセスがされていることを発見した場合				
				六					五のサーバ等に接続されている事業者内部の情報システムの他のサーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等に感染していることを発見した場合				
		5						事業者は、アクセス権者に対し、1から4までの報告の後で、アクセス権者が講じた措置を、管理者等当該事業者が報告先として指定した者に報告をさせる。		51	アクセス権者における事故報告後の措置に関する手順を閲覧し、アクセス権者に対し、1から4までの報告の後で、アクセス権者が講じた措置を報告させていることを確認する。（アクセス権者へのインタビューにより、事故報告後の措置に関する手順を認識しているかどうかを確認する）	【規定等】 アクセス権者における事故報告後の措置に関する手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		6						事業者は、アクセス権者に対して、1から5までの報告の義務を怠った場合のアクセス権の失効等の適切な措置を講ずるための手順を確立する。		52	アクセス権者の報告義務を怠った場合の失効に関する認識状況の現地調査を実施し、アクセス権者に対して、1から5までの報告の義務を怠った場合のアクセス権の失効等の適切な措置を講ずるための手順を定めていることを確認する。（アクセス権者へのインタビューにより、報告義務を怠った場合にアクセス権の失効することを認識しているかどうかを確認する）	【規定等】 【記録やその他の確認対象】 アクセス権者の報告義務を怠った場合の失効に関する認識状況	3.実施の結果である成果物を管理している
		7						事業者は、管理者等事業者が報告先として指定した者が1又は2の報告を受けた場合に、速やかにその事実を取締役等の経営層に報告をする取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		53	経営層への報告手順の認識状況の現地調査を実施し、報告先が、管理対象情報の事故等の報告を受けた場合、速やかに事実を経営層に報告をする取組が行われていることを確認する。	【規定等】 【記録やその他の確認対象】 経営層への報告手順の認識状況	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		8					事業者は、管理者等当該事業者が報告先として指定した者が1から4までの報告を受けた場合に、直ちに、証拠の収集により事実関係（漏えいの疑い等）を確認し、管理対象情報の適切な管理に関して必要な措置を講じ、又は講ずることをアクセス権者に指示するよう具体的な手順及び体制（確認をし、又は措置を講ずる責任体制を含む。）を確立する。		54	（管理対象情報漏えい事故対応に関する規程）及び報告先が報告を受けた場合、事実関係の確認や必要な措置を講ずる体制に組み込まれた人員における、手順の周知状況の現地調査を実施し、報告先が1から4までの報告を受けた場合、証拠の収集により事実関係を確認し、必要な措置を講じ、又は講ずることをアクセス権者に指示するよう具体的な手順及び体制（確認をし、又は措置を講ずる責任体制を含む。）を確立していることを確認する。	【規定等】 （管理対象情報漏えい事故対応に関する規程） 【記録やその他の確認対象】 報告先が報告を受けた場合、事実関係の確認や必要な措置を講ずる体制に組み込まれた人員における、手順の周知状況	3.実施の結果である成果物を管理している
		9					事業者は、管理対象情報が他者から預けられた情報である場合であって当該管理対象情報に係る5の報告がされたときに、管理者等当該事業者が報告先として指定した者により直ちに当該他者に同じ内容の報告をするための手順（報告をする責任者、連絡窓口、連絡系統図等を含み、常に最新の状態を維持するための手順を含む。）を確立する。この場合において、当該他者から、報告の詳細及び8の確認の結果（収集した証拠を含む。以下この9において同じ。）や措置の状況の報告を求められている場合には、当該報告の詳細及び8の確認の結果や措置の状況の報告の手順も確立する。		55	（管理対象情報漏えい事故対応に関する規程）及び報告先が報告を受けた場合、当該他者に同じ内容の報告をするための手順の認識状況の現地調査を実施し、預託された管理対象情報に係る5の報告がされたときに、報告先により直ちに当該他者に同じ内容の報告をするための手順（報告をする責任者、連絡窓口、連絡系統図等を含み、常に最新の状態を維持するための手順を含む。）を確立していることを確認する。預託元から求められている場合は、報告の詳細及び8の確認の結果や措置（収集した証拠を含む。）の状況の報告の手順も確立していることを確認する。	【規定等】 （管理対象情報漏えい事故対応に関する規程） 【記録やその他の確認対象】 報告先が報告を受けた場合、当該他者に同じ内容の報告をするための手順の認識状況	3.実施の結果である成果物を管理している
Ⅱ					管理対象情報への人的アクセスの制限			事業者は、原則として、アクセス権者のみが管理対象情報の取扱いを行い得ることとした上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への人的アクセスの制限を実施する。	56	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）の現地調査を実施し、アクセス権者のみが管理対象情報の取扱いを行い得ることとした上で、管理対象情報への人的アクセスの制限を実施していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	3.実施の結果である成果物を管理している
	第一	1				従業員等へのアクセス権の設定		事業者は、社内規程に定めること、社内における掲示をすること等事業者内部の従業員等の全てが認識できる方法により、アクセス権者のみが管理対象情報を取り扱い得ることを明らかにする。		57	アクセス権者のみが管理対象情報を取り扱い得ることを明らかにした社内掲示等の現地調査を実施し、従業員等の全てが認識できる方法により、アクセス権者のみが管理対象情報を取り扱い得ることを明らかにしていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者のみが管理対象情報を取り扱い得ることを明らかにした社内掲示等	1.実施している
		2					管理者は、管理対象情報へのアクセスができる者のアクセス権の設定を行う際は、以下の事項を考慮する。		58	アクセス権者管理簿を閲覧し、管理者がアクセス権の設定を行う際は、第一の2の事項を考慮していることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者管理簿	3.実施の結果である成果物を管理している
				一				Need to Knowの原則に照らし、グローバル競争が進む中での国外への技術等情報の流出リスク等を考慮しつつ、必要最小限の範囲となっているか否か。				
				二				事業者内部における情報の取扱いに係る社内規程への違反履歴				
				三				その従業員等の退職、研修員の派遣元への復帰等近い将来において管理対象情報を保有する事業者の直接の管理の対象から外れる可能性				
		3					管理者は、2に掲げる事項のほか、個人情報保護など関連する法令等に抵触しない範囲において、現に有する情報（法令の違反履歴、社内における飲酒トラブルの報告等をいう。この3において同じ。）又は入手することが可能な情報に基づき、その従業員等についてのレビューをした上で、管理対象情報へのアクセスができる者のアクセス権の設定を行う。		59	アクセス制御設定時のレビュー状況の現地調査を実施し、アクセス権の設定を行う際は、従業員等についてのレビューをした上で行っていることを確認する。（管理者へのインタビューにより、アクセス制御設定時のレビュー状況を確認する）	【規定等】 【記録やその他の確認対象】 アクセス制御設定時のレビュー状況	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		4						管理者は、アクセス権の設定について、統一的な判断基準（考え方）の下で行う。	60	（アクセス権設定に関する手順）及び（アクセス制御設定管理簿）の現地調査を実施し、管理者がアクセス権の設定について、統一的な判断基準の下で行っていることを確認する。	【規定等】 （アクセス権設定に関する手順） 【記録やその他の確認対象】 （アクセス制御設定管理簿）	3.実施の結果である成果物を管理している
		5						事業者は、全ての管理対象情報へのアクセス権の設定を一人の管理者が行っている場合には、当該アクセス権の設定に係る監査を当該管理者の上司等の他の者が行うことを確保するための仕組みを設ける。	61	アクセス権設定に係る監査の実施状況の現地調査を実施し、アクセス権の設定を一人の管理者が行っている場合には、アクセス権の設定に係る監査を他の者が行うことを確保するための仕組みを設けていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権設定に係る監査の実施状況	3.実施の結果である成果物を管理している
		6						事業者は、管理者以外の者がアクセス権の設定を行っているときは、当該管理者以外の者に対し、管理者にアクセス権の設定をされた者の氏名等必要な事項を連絡させる。	62	（管理者以外の者によるアクセス権の設定に関する手順）及び管理者以外でアクセス権の設定をされた者に関する事項の管理者への連絡状況の現地調査を実施し、管理者以外の者がアクセス権の設定を行っているときは、管理者以外の者に対し、管理者にアクセス権の設定をされた者の氏名等必要な事項を連絡させていることを確認する。	【規定等】 （管理者以外の者によるアクセス権の設定に関する手順） 【記録やその他の確認対象】 管理者以外でアクセス権の設定をされた者に関する事項の管理者への連絡状況	1.実施している
		7						事業者は、管理対象情報が他者から預けられた情報である場合には、当該他者からの要請に応じ、当該他者が、当該他者における当該管理対象情報の管理と同程度の管理を実現するために必要となるアクセス権の設定に係る調査をアクセス権の設定をすることが見込まれる者の同意の下で行う場合があることを、アクセス権の設定をすることが見込まれる者に対して説明をする。	63	預託元からの要請の有無、アクセス権の設定に係る調査時の説明記録の現地調査を実施し、預託元からアクセス権の設定に係る調査が行われる場合があることを、アクセス権の設定をすることが見込まれる者に対して説明していることを確認する。	【規定等】 【記録やその他の確認対象】 預託元からの要請の有無、アクセス権の設定に係る調査時の説明記録	1.実施している
	第二	1			アクセス権の管理			管理者は、アクセス権者の範囲を、定期的に、少なくとも個別のアクセス権の設定に係る業務の終了時点（例えば研究開発プロジェクトに係るアクセス権の設定であれば当該プロジェクトの終了時点）等の適切な時点で見直す。	64	（アクセス制御設定管理簿）の現地調査を実施し、管理者が、アクセス権者の範囲を定期的に、見直していることを確認する。	【規定等】 【記録やその他の確認対象】 （アクセス制御設定管理簿）	3.実施の結果である成果物を管理している
		2						管理者は、アクセス権者の従事する管理対象情報に係る業務の内容等に応じ、当該アクセス権者のアクセスの範囲を限定し、その責任を明確にする。	65	（アクセス権設定に関する手順）及び（アクセス制御設定管理簿）の現地調査を実施し、管理者が、アクセス権者の業務の内容等に応じ、アクセス範囲を限定し、その責任を明確にしていることを確認する。	【規定等】 （アクセス権設定に関する手順） 【記録やその他の確認対象】 （アクセス制御設定管理簿）	3.実施の結果である成果物を管理している
		3						管理者は、アクセス権者の従事する管理対象情報に係る業務の状況を確認すること等を通じて適切に状況を把握し、管理対象情報の適切な管理に関して必要な対応をアクセス権者に指示する。この場合において、管理者は、当該アクセス権者以外のアクセス権者に、手順を定めて、状況を把握させ、管理対象情報の適切な管理に関して必要な対応を指示させることができる。	66	管理者によるアクセス権者の業務の確認状況、管理者からアクセス権者への必要な対応の指示状況、当該アクセス権者以外のアクセス権者における対応手順の現地調査を実施し、管理者が、アクセス権者の管理対象情報の適切な管理に関して必要な対応をアクセス権者に指示していることを確認する。	【規定等】 【記録やその他の確認対象】 管理者によるアクセス権者の業務の確認状況、管理者からアクセス権者への必要な対応の指示状況、当該アクセス権者以外のアクセス権者における対応手順	1.実施している
		4						管理者は、退職等により必要のなくなった従業員等のアクセス権を直ちに失効をさせること等によりアクセス権を適切に管理する。	67	（アクセス制御設定管理簿）の現地調査を実施し、管理者が、必要のなくなったアクセス権を直ちに失効をさせること等によりアクセス権を適切に管理していることを確認する。	【規定等】 【記録やその他の確認対象】 （アクセス制御設定管理簿）	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		5						管理者は、アクセス権の管理を確実なものとするため、アクセス権者の氏名、役職、アクセス権の設定年月日、トレーニングの受講の状況等アクセス権者の範囲及びアクセス権者の状況を記録した管理簿を作成し、合理的な期間保管する。		68	アクセス制御設定管理簿の現地調査を実施し、管理者が、アクセス権者の情報を記録した管理簿を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス制御設定管理簿	1.実施している
	第三	1				アクセス権者に対する秘密保持等に関する担保		事業者は、アクセス権者としての責任を明確にするため、アクセス権者から、以下の事項のうち必要なもの（一以上に限る。）を確保する秘密保持の誓約書を得、又は秘密保持契約を締結する等文書（当該アクセス権者が、アクセス権を設定される前に当該事業者に提出した誓約書又は当該事業者と締結した秘密保持契約を含む。）により確認する（以下誓約書及び秘密保持契約を総称して「誓約書等」という。）。		69	秘密保持の誓約書等を閲覧し、アクセス権者から、秘密保持の誓約書等を得ていることを確認する。	【規定等】 【記録やその他の確認対象】 秘密保持の誓約書等	3.実施の結果である成果物を管理している
				一				第三者に対する守秘義務を厳守すること。					
				二				アクセス権の設定の解除の後（退職後も含む。）、も 当該アクセス権が設定されている間に知り得た管理対象情報について、公知になったものを除き、不正に開示し、又は使用しないこと。					
				三				マニュアルその他の事業者内部における情報の取扱いに係る社内規程を遵守すること。					
				四				管理対象情報の漏えいにつがなり得る事象等を発見した場合に管理者等事業者が指定した者に報告を行うとともに、管理対象情報の漏えいの事故等が発生した場合に必要な措置を講ずること。					
				五				管理対象情報へのアクセスのログ等をアクセス権の設定を行った者等から確認されること。					
				六				管理対象情報に接する必要がなくなった場合は、速やかに、返却すること等所要の対応が求められること。					
		2						事業者又は管理者は、誓約書等の記載事項の定期的な確認を実施するための手順を確立する。		70	誓約書等の定期的な確認手順を閲覧し、事業者又は管理者が、誓約書等の記載事項の定期的な確認を行う手順を定めていることを確認する。	【規定等】 誓約書等の定期的な確認手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		3						事業者又は管理者は、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等が発生した場合は、その都度、誓約書等の内容の見直しを実施し、必要に応じて、変更した誓約書等によりアクセス権者の責任を確認するための手順を確立する。		71	誓約書等の確認手順を閲覧し、事業者又は管理者が、状況の変化や事故等が発生した場合は、誓約書等の内容の見直しを実施し、必要に応じて、誓約書等によりアクセス権者の責任を確認するための手順を定めていることを確認する。	【規定等】 誓約書等の確認手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		4						事業者は、1に掲げる事項のうち誓約書等の記載事項として含まれていないものを定期的な上司からの説明等によりアクセス権者に理解させるための取組を行う。		72	誓約書等の記載事項として含まれていないものに関する説明記録を閲覧し、誓約書等の記載事項として含まれていないものをアクセス権者に理解させるための取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書等の記載事項として含まれていないものに関する説明記録	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		5						事業者は、トレーニングによる周知並びにその後の定期的な上司からの説明及び認識の確認等の方法により、アクセス権者としての責任を明確に認識させる。		73	アクセス権者に対する責任に関する周知、説明記録を閲覧し、トレーニングによる周知や定期的な上司からの説明・認識の確認等により、アクセス権者としての責任を明確に認識させていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者に対する責任に関する周知、説明記録	1.実施している
		6						事業者は、他者がアクセス権の設定に際し調査を行う場合には、アクセス権を設定することが見込まれる者に対し、当該調査の後で、1の誓約書等を当該他者に提出することが求められることがあることを説明する。		74	誓約書等の提出が求められることの説明記録を閲覧し、他者がアクセス権の設定に際し調査を行う場合、アクセス権を設定することが見込まれる者に対し、誓約書等の当該他者への提出が要求されることがあることを説明していることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書等の提出が求められることの説明記録	1.実施している
		7						事業者は、アクセス権者が確立された手順を守らない場合、マニュアル等の管理対象情報の取扱いに係る社内規程への違反等があった場合にアクセス権者のアクセス権の失効をさせる等の措置を講ずるための手順を確立する。		75	（アクセス権者の違反等の場合のアクセス権失効等のための手順）アクセス制御設定記録を閲覧し、アクセス権者が手順を守らない場合、社内規程への違反等があった場合にアクセス権の失効をさせる等の措置を講ずるための手順を定めていることを確認する。	【規定等】 （アクセス権者の違反等の場合のアクセス権失効等のための手順） 【記録やその他の確認対象】 アクセス制御設定記録	2.実施計画があり、進捗管理している
		8						事業者は、アクセス権者を含めた従業員等がマニュアルに違反し、管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合に関し、当該従業員等を解雇等の懲戒処分とすることについて就業規則等に定めるとともに、刑事告発や民事訴訟の法的手続に関する規程を社内規程に定める。		76	懲戒処分に関して記載された就業規則等、法的手続きに関する社内規程を閲覧し、従業員等が管理対象情報の漏えい等をした場合に関し、従業員等を懲戒処分とすることについて就業規則等に定めている。法的手続に関する規程を社内規程に定めていることを確認する。	【規定等】 懲戒処分に関して記載された就業規則等、法的手続きに関する社内規程 【記録やその他の確認対象】	1.実施している
		9						事業者は、アクセス権者を含めた従業員等が管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合には、当該不正の事例及びその処分の内容を全ての従業員等に周知する。		77	インシデント発生時の周知内容、周知時期の記録（実際に発生した場合。なお、発生がある場合、従業員へのインタビューにより、周知内容を認識しているか確認）を閲覧し、従業員等が管理対象情報を漏えい等をした場合には、不正事例及び処分内容を全ての従業員等に周知していることを確認する。	【規定等】 【記録やその他の確認対象】 インシデント発生時の周知内容、周知時期の記録（実際に発生した場合。なお、発生がある場合、従業員へのインタビューにより、周知内容を認識しているか確認）	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
	第四	1				その他の場合のアクセス権の設定		管理者は、管理対象情報を保有する事業者のアクセス権者以外の従業員等や、当該事業者の従業員等以外の者等（以下この第四において「訪問者」という。）による管理対象情報へのアクセス、例えば、立入制限区域にある管理対象情報である製造設備の見学のように一時的なアクセスについて、訪問者がNeed to Knowの原則を満たすものであるかを評価する。		78	アクセス制御及び認証や物理的対策に関する規程及びアクセス制御設定管理簿や施設の入退館記録を閲覧し、管理者が、アクセス権者以外の従業員等や訪問者による管理対象情報へのアクセスについて、例えばNeed to Knowの原則を満たすものであるかを評価していることを確認する。	【規定等】 アクセス制御及び認証や物理的対策に関する規程 【記録やその他の確認対象】 アクセス制御設定管理簿や施設の入退館記録	3.実施の結果である成果物を管理している
		2						事業者は、管理対象情報にアクセスする訪問者から、その訪問により得られた管理対象情報を第三者等に開示しないこと等を誓約する書面を得る。		79	誓約書、及び施設の入退館記録を閲覧し、訪問者から、管理対象情報を第三者等に開示しないこと等を誓約する書面を得ていることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書、及び施設の入退館記録	1.実施している
		3						管理者は、訪問者の管理対象情報へのアクセスについて、アクセス権者の立会い等管理対象情報を保護するために適切な措置を講ずる。		80	訪問者アクセスから管理対象情報を保護するための適切な措置、及びこれらの措置の管理者の上長または経営者による確認状況の現地調査を実施し、管理者が、訪問者の管理対象情報へのアクセスについて、アクセス権者の立会い等管理対象情報を保護するために適切な措置を講じていることを確認する。（管理者、及び管理者の上長または経営者へのインタビューにより、措置の状況や確認状況を確認する）	【規定等】 【記録やその他の確認対象】 訪問者アクセスから管理対象情報を保護するための適切な措置、及びこれらの措置の管理者の上長または経営者による確認状況	3.実施の結果である成果物を管理している
Ⅲ					管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等			事業者は、管理対象情報が、書類等の紙情報や試作品等の物であって、その管理対象情報が金庫等の保管容器に保管することができるものである場合には、当該管理対象情報を保管容器に施錠して保管するとともに、その保管容器から持ち出して当該管理対象情報の取扱いをする場合には、その取り扱う場所を限定する取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への物理的アクセスを制限する。		81	保管容器、保管容器の取扱場所、管理者による保管容器の管理状況の確認状況の現地調査を実施し、以下の点について確認する。 ①管理対象情報の保管には施錠することができる保管容器を用いること ②管理対象情報を保管容器から持ち出して利用する際、取り扱う場所を限定すること ③管理者が保管の状況や取り扱う場所の限定等の管理状況を確認していること	【規定等】 【記録やその他の確認対象】 保管容器、保管容器の取扱場所、管理者による保管容器の管理状況の確認状況	3.実施の結果である成果物を管理している
	第一	1				管理対象情報を保管するための保管容器		事業者は、管理対象情報を保管する保管容器について、施錠することができる保管容器を用いる。		82	物理的対策に関する規程及び管理対象情報の保管記録、保管容器を閲覧し、施錠された保管容器を用いていることを確認する。	【規定等】 物理的対策に関する規程 【記録やその他の確認対象】 管理対象情報の保管記録、保管容器	1.実施している
		2						管理者、又は管理者の委任を受けたアクセス権者は、保管容器の鍵について、差込み式の鍵である場合にあってはその鍵の貸出しを、文字盤鍵である場合にあってはその鍵番号の設定等を行うことにより、鍵等を管理する。この場合において、管理者又は管理者の委任を受けたアクセス権者が、鍵の貸出し又は鍵番号の共有等をするときは、共有をする相手方をアクセス権者に限るものとする。		83	鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順を閲覧し、アクセス権者は、保管容器の鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順を定めている。その手順に従って、管理者又は管理者の委託を受けたアクセス権者が管理している。	【規定等】 鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順 【記録やその他の確認対象】	2.実施計画があり、進捗管理している
		3						管理者は、アクセス権者が貸出しをされた鍵等の管理を適切に行うための手順を確立する。		84	アクセス権者に貸し出された鍵等の適切な管理手順を閲覧し、管理者が、アクセス権者に貸し出された鍵、共有された鍵番号の取扱いの手順を定めていることを確認する。	【規定等】 アクセス権者に貸し出された鍵等の適切な管理手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		4						管理者又は管理者の委任を受けたアクセス権者は、鍵の貸出し又は鍵番号の共有を管理するための管理簿を作成し、合理的な期間保管する。		85	鍵の貸出し又は鍵番号の共有を管理するための管理簿の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が管理簿を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 鍵の貸出し又は鍵番号の共有を管理するための管理簿	1.実施している
		5						管理者又は管理者の委任を受けたアクセス権者は、文字盤鍵で施錠することができる保管容器を管理対象情報の保管をするために用いている場合にあっては、当該保管容器の文字盤鍵の鍵番号を1年に1回以上変更する。		86	保管容器の文字鍵版の番号の変更記録の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が鍵番号を1年に1度以上変更していることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器の文字鍵版の番号の変更記録	3.実施の結果である成果物を管理している
		6						管理者又は管理者の委任を受けたアクセス権者は、文字盤鍵で施錠することができる保管容器を管理対象情報の保管をするために用いている場合にあっては、当該保管容器の文字盤鍵の鍵番号を、以下のような事象が生じた都度、変更する。		87	イベント毎の発生、鍵番号の変更実績の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が、イベント毎に鍵番号を変更していることを確認する。	【規定等】 【記録やその他の確認対象】 イベント毎の発生、鍵番号の変更実績	3.実施の結果である成果物を管理している
				一					保管容器の購入後、使用する場所に備え付け、又は使用する場所を変更した場合				
				二					管理者又は管理者の委任を受けたアクセス権者が替わった場合				
				三					鍵番号がアクセス権者以外の者に漏えいし、又はそのおそれがあると管理者又はアクセス権者が認めた場合				
		7						事業者は、管理対象情報を保管するための保管容器について以下に掲げる強度を有するものを用いる。		88	保管容器を閲覧し、管理対象情報を保管する保管容器について、7（1）～（4）に掲げる強度を有するものを用いていることを確認する。（監査時には、保管容器の仕様を記録する）	【規定等】 【記録やその他の確認対象】 保管容器	1.実施している
			(1)					材質について、JISG3141の冷間圧延鋼板及び鋼帯に定める標準厚さ1.2mmの鋼板（保管容器の内部に用いられる鋼板にあっては0.8mm以上の鋼板、裏板に用いられる鋼板にあっては1.0mm以上の鋼板）を使用した場合に得られる強度以上の強度を有する鋼板を用いている保管容器					
			(2)					材質及び構造について、JISS1037の耐火金庫と同等以上の性能を有する保管容器					
			(3)					扉について、丁番が破壊された場合であっても、その開放を防止することができる構造となっている保管容器					
			(4)	一				以下のいずれかの施錠装置を有する保管容器	三段式文字盤鍵で施錠することができる保管容器であって、三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるもの				
				二					三段式文字盤鍵及び差込み式の鍵の組合せにより二重以上の施錠方式で施錠することができる保管容器				

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
				三				三段式文字盤鍵及び差込み式の鍵の組合せにより二重以上の施錠方式で施錠することができる保管容器であって、その三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ 100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるもの				
				四				生体認証システム及び差込み式鍵の組合せ等により二重以上の施錠方式で施錠することができる保管容器					
		8					事業者は、保管容器を、セキュリティカメラが設置・運用され、又は人感センサーの設置等保管容器に近づく者を適切に確認するための措置（保管容器に近づく者をアクセス権者が視認できるよう視界を確保するためのレイアウト等を含む。）がとられた場所に設置する。		89	保管容器と設置状況の現地調査を実施し、保管容器に近づく者を適切に確認するための措置（保管容器に近づく者をアクセス権者が視認できるよう視界を確保するためのレイアウト等を含む。）がとられた場所に設置していることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器と設置状況	1.実施している
		9					事業者は、保管容器を、この告示のⅣの立入制限区域に設置する。		90	立入制限区域、保管容器の設置状況の現地調査を実施し、保管容器を立入制限区域に設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域、保管容器の設置状況	1.実施している
		10					事業者は、8又は9の場所に保管容器を設置した場合において、ワイヤで固定すること等により保管容器を物理的に持ち出せないよう適切な措置を講ずる。		91	保管容器の設置状況を閲覧し、保管容器をワイヤで固定すること等物理的に持ち出せないような措置が講じられていることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器の設置状況	1.実施している
	第二	1			管理対象情報の取扱いをする場所		管理者は、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所を限定するための手順を確立する。		92	アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順及び手順に沿っているかの管理者の確認状況の現地調査を実施し、アクセス権者が管理対象情報を保管容器から持ち出して、立ち入り制限区域でのみ取り扱うための手順を管理者が作成していることを確認する。	【規定等】 アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順 【記録やその他の確認対象】 手順に沿っているかの管理者の確認状況	2.実施計画があり、進捗管理している
		2					管理者は、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所をこの告示のⅣの立入制限区域に限定するための手順を確立する。この手順には、アクセス権者が管理対象情報の取扱いをする場所をこの告示のⅣの立入制限区域ではない場所で取り扱う（管理者が当該場所で管理対象情報を取り扱うことによる当該管理対象情報の漏えいの事故等が生じ、又はそのおそれがないと認める場合に限る。）ための承認の手順を含むことができる。		93	アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順を閲覧し、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所を立入制限区域に限定していることを確認する。アクセス権者が管理対象情報を保管容器から持ち出して、立入制限区域ではない場所で取り扱うための承認の手順を含むことができる。	【規定等】 アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順 【記録やその他の確認対象】	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容			ID	確認内容	確認対象	到達レベル
	第三	1			管理対象情報の運搬		管理者は、管理対象情報を保管容器から持ち出し、当該管理対象情報を取り扱うために当該管理対象情報を取り扱う場所に運搬すること、当該取り扱う場所から保管容器に運搬すること等を、アクセス権者又は管理者が指定した者に限り認めるための手順を確立する。		94	管理対象情報の運搬に関する手順及び（管理対象情報管理簿）を閲覧し、管理対象情報の運搬について、アクセス権者又は管理者が指定した者に限り、認めるための手順を管理者が定めていることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 （管理対象情報管理簿）	3.実施の結果である成果物を管理している
		2					管理者は、管理対象情報を管理者が指定した者が運搬する場合に、外部から当該管理対象情報を視認することができず、かつ、運搬中に不正があった場合に確認等ができるよう、当該管理対象情報を封筒に入れて封印する等の適切な措置を講ずるための手順を確立する。		95	管理対象情報の運搬に関する手順及び（管理対象情報管理簿）を閲覧し、管理対象情報を管理者が指定する者が運搬する場合に、外部から当該管理対象情報を視認することができないようにする等のため、封筒に入れて封印する等の適切な手順を管理者が定めていることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 （管理対象情報管理簿）	2.実施計画があり、進捗管理している
		3					管理者は、管理者が指定した者が、管理対象情報を運搬し、当該管理対象情報を取り扱うための場所等においてアクセス権者に引き渡したときに、当該アクセス権者から受領証を受け取り、管理者に提出するための手順を確立する。		96	管理対象情報の運搬に関する手順及びアクセス権者からの受領証の現地調査を実施し、管理対象情報の運搬について、管理者が指定した者が運搬する運搬し、アクセス権者に引き渡したときに、当該アクセス権者から受領証を受け取り、管理者に提出することを内容とする手順を管理者が定めており、その手順に従って管理者が指定した者から受領証が管理者に提出されている。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 アクセス権者からの受領証	2.実施計画があり、進捗管理している
		4					管理者は、管理対象情報を管理者が指定した者が運搬する場合に、当該管理対象情報を引き渡した者及び引き渡された者が相互に、その内容等についての確認を行うための手順を確立する。		97	管理対象情報の運搬に関する手順及び引き渡す側と引き渡された側の相互の確認結果の現地調査を実施し、管理対象情報の運搬について、管理者が指定した者が運搬する場合に、引き渡す側と引き渡された側で、相互に、その内容についての確認をするための手順を管理者が定めており、その手順に従って相互で確認している。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 引き渡す側と引き渡された側の相互の確認結果	2.実施計画があり、進捗管理している
		5					管理者は、管理対象情報が保管されている保管容器の設置された場所のある事業所以外の当該管理者の属する事業者の事業所等に運搬する必要がある場合又は当該管理者の属する事業者以外の者の事業所等に管理対象情報を運搬する必要がある場合に、その運搬を信頼できる輸送機関又は運搬事業者により行わせるための手順（その運搬中に管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果に基づき当該事故等への対応をするための手順を含む。）を確立する。		98	管理対象情報の運搬に関する手順及び輸送機関又は運搬事業者の確認結果を閲覧し、管理対象情報が保管されている保管容器の設置された場所のある事業所以外の事業所等に管理対象情報を運搬する場合に、その運搬を信頼できる輸送機関又は運搬事業者により行わせるための手順（その運搬中に管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果に基づき当該事故等への対応をするための手順を含む。）があり、その手順に従い信頼できる輸送機関又は運搬事業者に運搬を行わせている。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 輸送機関又は運搬事業者の確認結果	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		6						管理者は、当該管理者の属する事業者以外の者に管理対象情報を運搬する必要がある場合には、当該者の情報の管理について評価し、及び当該者と秘密保持契約を締結しているかを確認するための手順（当該者が管理対象情報を受領した場合に、受領した日付、受取者のサイン等を受領証に記載する手順を含む。）を確立する。当該事業者以外の者から当該事業者に運搬する場合も同様とする。		99	管理対象情報の運搬に関する手順及び秘密保持契約、及び受領証を閲覧し、管理者の属する事業者以外の者に管理対象情報を運搬する又は当該者から当該事業者に運搬する場合には、当該者の情報の管理について評価し、及び当該者と秘密保持契約を締結しているかを確認するための手順（当該者が管理対象情報を受領した場合に、受領した日付、受取者のサイン等を受領証に記載する手順を含む。）があることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 秘密保持契約、及び受領証	3.実施の結果である成果物を管理している
Ⅳ					管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等			事業者は、管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等には、当該管理対象情報が置かれ、又は置かれようとする場所を立入制限区域としてアクセス権者以外の者の立入りを制限する取組が習慣化し、文書等に定めがなくても当該事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への物理的アクセスの制限を実施する。		100-1	物理的対策に関する規程及びアクセス制御設定管理簿や立入制限の入退室記録を閲覧し、以下の点について確認する。 ①管理対象情報が製造装置である場合等に、保管容器に保管することが困難な場合、当該管理対象情報が置かれ、又は置かれようとする場所を立入制限区域としてアクセス権者以外の者の立入りを制限すること ②立入制限区域の状況、立入制限された場所の管理の状況を確認していること	【規定等】 物理的対策に関する規程 【記録やその他の確認対象】 アクセス制御設定管理簿や立入制限の入退室記録	3.実施の結果である成果物を管理している
								なお、事業者の管理対象情報を取り扱う事業所等が当該事業者以外の他者の所有に係る場合等には、当該他者（当該事業所等の管理をする者を含む。）、にⅥの秘密保持契約及び施錠、巡回監視等当該事業所等の適切な管理を依頼する契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第二の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。		100-2	委託管理に関する規程及び他者との秘密保持契約、警備委託契約を閲覧し、管理対象情報を取り扱う事業者の事業所等が当該事業者以外の他者の所有に係る場合等には、他者に秘密保持契約及び施錠、巡回監視等当該事業所等の適切な管理を依頼する契約を締結した上で、自社が定めた対策を実施していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 他者との秘密保持契約、警備委託契約	3.実施の結果である成果物を管理している
	第一	1				立入制限区域の構造と管理		事業者は、壁その他の物理的な境界で他の区域と区分することができる区域であってその区域が他の区域と接触する全ての入退室口を、差込み式の鍵、文字盤鍵、キーパッド式の鍵、認証システム（ICカード認証、生体認証、ワンタイムパスワード、PIN入力等）等により施錠することができる区域を立入制限区域として設定する。		101	物理的な境界、立入制限区域の施錠可能状況を閲覧し、物理的な境界で区分でき、全ての入退室口を施錠できる区域を立入制限区域として設定していることを確認する。	【規定等】 【記録やその他の確認対象】 物理的な境界、立入制限区域の施錠可能状況	1.実施している
		2						事業者は、立入制限区域に係る入退室口を、原則として業務時間中のみ開錠する。		102	立入制限区域の解錠・施錠記録を閲覧し、立入制限区域に係る入退室口を、原則として業務時間中のみ開錠していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の解錠・施錠記録	2.実施計画があり、進捗管理している
		3						事業者は、鍵の管理簿の作成、受付の設置による受付簿の管理、IDによる認証の導入、作業をしている者以外の者による同行と確認等により、立入制限区域へのアクセス権者を含む全ての者の立入りの状況（立入者の所属、氏名及び立入りの目的等を含む。）を記録し、合理的な期間保管することで事後的に確認可能とするための適切な措置を講ずる。		103	事後的に確認可能な措置の状況（鍵の管理簿、受付簿、認証状況、作業者以外の同行・確認状況等）を閲覧し、鍵の管理簿の作成、受付の設置による受付簿の管理、IDによる認証の導入、作業者以外の者による同行と確認等により、立入制限区域への全ての者の立入りの状況（立入者の所属、氏名及び立入りの目的等を含む。）を記録し、事後的に確認可能とするための適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 事後的に確認可能な措置の状況（鍵の管理簿、受付簿、認証状況、作業者以外の同行・確認状況等）	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		4						事業者は、立入制限区域の鍵を三段式文字盤鍵又は認証システム及び差込み式の鍵の組合せ等による二重以上の施錠方式のものとする。		104	立入制限区域の施錠状況の現地調査を実施し、立入制限区域の鍵を三段式文字盤鍵又は認証システム及び差込み式の鍵の組合せ等による二重以上の施錠方式のものとしていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の施錠状況	1.実施している
		5						事業者は、立入制限区域の鍵を三段式文字盤鍵とする場合は、その三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるものを用いる。		105	立入制限区域の施錠状況の現地調査を実施し、立入制限区域の鍵の三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、5に定められるものを用いていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の施錠状況	1.実施している
		6						事業者は、立入制限区域の内側に緊急時に開錠するための非常開閉装置を設ける。		106	立入制限区域の非常開閉装置の設置状況の現地調査を実施し、立入制限区域の内側に非常開閉装置を設けていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の非常開閉装置の設置状況	1.実施している
		7						事業者は、立入制限区域についての一定の強度を確保するため、当該立入制限区域を、以下に掲げる構造を有する施設にする。		107	立入制限区域の現地調査を実施し、立入制限区域を、第一の7の構造を有する施設にしていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
				一					その立入制限区域と他の区域とを区分する壁や天井、床について、鉄筋コンクリート又は不燃性の資材を用いた堅固な構造				
				二					その立入制限区域と他の区域とを区分する壁や天井、床について、厚さ10cm以上の鉄筋コンクリートを用いた堅固な構造又は以下に掲げるいずれかの方法による堅固な構造 イ 補強コンクリートブロックを用いる場合 中空部をコンクリートで充填した厚さ15cm以上のコンクリートブロックを用いた上で、直径9mm以上の鉄筋を縦40cm以下、横20cm以下の間隔で配筋する構造 ロ 鉄板を用いる場合 厚さ3.2mm以上の鉄板を用いて強化する構造（当該立入制限区域の内側と外側にそれぞれ鉄板を用いる場合には、それぞれの鉄板が1.6mm以上とすることを含む。） ハ 不燃性の資材を用いる場合 厚さ10cm以上の鉄筋コンクリートと同等以上の強度を有する不燃材を用いて強化する構造				

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
				三					その立入制限区域の天井の裏が、他の区域の天井の裏と接続している場合に、その境界部に金網を設置すること等により他の区域からの侵入を防止する構造				
				四					その立入制限区域の入退室口を一箇所とする構造（非常用の入退室口を別に設ける場合にあっては、立入制限区域の内側からのみ開けることができる扉とする構造）であって、当該入退室口の扉の上に常夜灯（停電時でも作動するものに限る。）を設けている構造				
				五					その立入制限区域の入退室口の扉として鋼鉄を用いている構造				
				六					その立入制限区域の入退室口の扉について、厚さ3.2mm以上の鋼鉄を用いたものであって、当該扉の丁番が当該立入制限区域の内側に埋め込まれたものを有する構造（当該丁番が切断された場合でも扉の開放を防止することができるものに限る。）				
				七					その立入制限区域の入退室口の扉に備え付けられるのぞき窓がドアスコープとなっている構造				
				八					その立入制限区域の入退室口の扉が両開きである場合には、その合わせ目に定規ぶちを取り付けている構造				
				九					その立入制限区域に窓がない構造又は窓がある場合には、必要最低限の数の不透明な窓となっており、かつ、当該窓に直径13mm以上の鉄棒で、その間隔が10cm以下となるよう鉄格子を堅固に取り付けた構造				
				十					その立入制限区域に備え付けられたダクト、通風調節装置、天窓、下水溝等の開口部が、大きさ、形状等から人の侵入、人による盗み見又は盗聴のおそれがあると認められるものである場合に、当該開口部に直径13mm以上の鉄棒で、その間隔が10cm以下となるよう鉄格子を堅固に取り付け、又は金網を取り付けた構造				
			8					事業者は、立入制限区域の扉を開けたときに、中が見えないようにカーテン又は衝立等を設置する。		108	立入制限区域の現地調査を実施し、立入制限区域の中が見えないようにカーテン又は衝立等を設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
			9					事業者は、ある施設の内部に間仕切りを用いて立入制限区域を設定する場合には、当該間仕切りは7の一又は二の資材を用いて天井まで届く高さの不透明な構造（特に高い天井の場合には、代用天井を用いて天井と代用天井の間を金網で補強する構造）とする。		109	立入制限区域の現地調査を実施し、立入制限区域の間仕切りは7の一又は二の資材を用いて天井まで届く高さの不透明な構造としていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		10						事業者は、赤外線警報装置、セキュリティカメラ等の警備システムの導入により、立入制限区域への不審者の侵入に係る視認性を高める。		110	立入制限区域に帯する警備システムの現地調査を実施し、立入制限区域への不審者の侵入に係る視認性を高めていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域に帯する警備システム	1.実施している
		11						事業者は、立入制限区域の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。		111	警備体制又は警備委託契約を閲覧し、立入制限区域の警備員等の駆けつけ体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備体制又は警備委託契約	1.実施している
		12						事業者は、警備員等がモニターにより立入制限区域及びその周辺を常時監視する体制を確保する。		112	常時監視体制又は警備委託契約を閲覧し、警備員等が立入制限区域及びその周辺を常時監視する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 常時監視体制又は警備委託契約	1.実施している
		13						事業者は、警備員等により立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保する。		113	巡回監視体制又は警備委託契約を閲覧し、立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 巡回監視体制又は警備委託契約	1.実施している
		14						管理者は、災害等緊急時の対応のため、立入制限区域の全ての鍵の解錠が可能なマスターキーの製作、共通パスワードの設定等がされている場合には、そのマスターキー等の管理の手順を確立する。		114	マスターキーや共通パスワード等の管理手順及びマスターキーや共通パスワード等の管理状況の現地調査を実施し、管理者が、立入制限区域のマスターキー、共通パスワード等の管理の手順を定めていることを確認する。	【規定等】 マスターキーや共通パスワード等の管理手順 【記録やその他の確認対象】 マスターキーや共通パスワード等の管理状況	3.実施の結果である成果物を管理している
		15						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とする。		115	立入制限区域の現地調査を実施し、立入制限区域を、他の区域と物理的に独立した施設としていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
		16						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、当該施設の周囲を1.8m以上の壁又はフェンス等で覆うこと等により不審者の容易な侵入を防ぐ措置を講ずる。		116	立入制限区域の現地調査を実施し、立入制限区域を他の区域と物理的に独立した施設とし、周囲を1.8m以上の壁等で覆うこと等により、不審者の容易な侵入を防ぐ措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している

別紙2　監査ガイドライン

章	節	項	番					内容		ID	確認内容	確認対象	到達レベル
		17						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、当該施設の基礎をコンクリートで固定する。		117	立入制限区域の現地調査を実施し、立入制限区域を他の区域と物理的に独立した施設とし、当該施設の基礎をコンクリートで固定していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
		18						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、かつ当該施設が複数ある場合に、その複数の施設を一つの区画に集め、当該区画の周囲を2m以上の壁、フェンス等で覆うことにより不審者の容易な侵入を防ぐ措置を講ずる。		118	立入制限区域の現地調査を実施し、立入制限区域を、他の区域と物理的に独立した施設としている。複数の施設を一つの区画に集め、当該区画の周囲を2m以上の壁、フェンス等で覆っていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
		19						管理者は、立入制限区域に管理対象情報が置かれていない状態であっても、アクセス権者以外の立入りを制限する。		119	立入制限区域の入退室記録の現地調査を実施し、管理者が、立入制限区域に管理対象情報が置かれていない状態でも、アクセス権者以外の立入りを制限していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の入退室記録	1.実施している
		20						事業者又は管理者は、立入制限区域の入退室口の施錠のための鍵又は鍵番号等の管理、警備の体制等立入制限区域を適切に管理するための手順及び体制を確立する。		120	立入制限区域を適切に管理するための手順及び体制の閲覧及び立入制限区域の入退室口の施錠や警備状況の現地調査を実施し、事業者又は管理者は、立入制限区域の入退室口の施錠のための鍵又は鍵番号等の管理、警備の体制等立入制限区域を適切に管理するための手順及び体制を定めていることを確認する。	【規定等】 立入制限区域を適切に管理するための手順及び体制 【記録やその他の確認対象】 立入制限区域の入退室口の施錠や警備状況	2.実施計画があり、進捗管理している
	第二	1			立入制限区域への立入者の視認性を高めるため等の措置			事業者は、立入制限区域への全ての立入者について、他の者から視認できるよう、当該立入制限区域に立ち入ることが許されていることがわかる標識の着用を求めるものとする。		121	立入制限区域を適切に管理するための手順の閲覧及び立入制限区域の立入者の標識着用状況の現地調査を実施し、立入制限区域への全ての立入者が視認できるよう、標識の着用を求めていることを確認する。	【規定等】 立入制限区域を適切に管理するための手順 【記録やその他の確認対象】 立入制限区域の立入者の標識着用状況	3.実施の結果である成果物を管理している
		2						管理者は、立入制限区域内へのカメラ、携帯型の情報通信機器等の持込みを原則として禁止し、持ち込む必要がある場合には、あらかじめ、管理者の承認を得ることを求めるための手順を確立する。この場合において、立入制限区域内におけるこれらの機器の利用について、管理者は、アクセス権者（当該アクセス権者が自ら使用する場合には別のアクセス権者）の視認できる範囲内においてのみ利用することができる旨を説明する。		122	立入制限区域を適切に管理するための手順の閲覧及び立入制限区域の現地調査を実施し、立入制限区域内へのカメラ、携帯型の情報通信機器等の持込みを原則として禁止し、必要な場合には管理者の承認を得ることを求める手順を定め、アクセス権者の視認できる範囲内においてのみ利用できる旨を説明していることを確認する。	【規定等】 立入制限区域を適切に管理するための手順 【記録やその他の確認対象】 立入制限区域	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		3						事業者は、立入制限区域内に、製造設備等の管理対象情報を設置する場合には、当該機器を物理的に持ち出せないようにワイヤ等で固定する。		123	立入制限区域の現地調査を実施し、立入制限区域内の製造設備等の管理対象情報は、物理的に持ち出せないようにワイヤ等で固定していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
		4						事業者は、立入者の立入制限区域からの退室に際し、当該立入者について、持ち物検査、体重検査等を実施する。		124	立入制限区域の現地調査を実施し、立入制限区域からの退室に際し、持ち物検査、体重検査等を実施していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域	1.実施している
		5						管理者は、アクセス権者以外の者（以下この5において「部外者」という。）の立入制限区域への立入りを認めるための手順（部外者の立入りによる当該立入制限区域に置かれている管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果を踏まえた対応をするための手順、Need to Knowの原則を満たすこと等の立入りの要件及び当該立入制限区域に係る管理対象情報が他者から預けられたものである場合に当該他者により立入りが認められた者に限り立入りを認めるときは、その手続を含む。）を確立する。		125	立入制限区域への立入りを認めるための手順及び立入制限区域への立入り記録を閲覧し、管理者が、アクセス権者以外の者の立入制限区域への立入りを認めるための手順（部外者の立入りによる当該立入制限区域に置かれている管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果を踏まえた対応をするための手順、Need to Knowの原則を満たすこと等の立入りの要件及び当該立入制限区域に係る管理対象情報が他者から預けられたものである場合に当該他者により立入りが認められた者に限り立入りを認めるときは、その手続を含む。）を定めていることを確認する	【規定等】 立入制限区域への立入りを認めるための手順 【記録やその他の確認対象】 立入制限区域への立入り記録	3.実施の結果である成果物を管理している
	第三					管理対象情報の運搬		管理者は、管理対象情報の運搬について、この告示のⅢの第三のうちⅠの第二の2により必要と決定した措置を実施する。		126	管理者が、告示Ⅲの第三のうちⅠの第二の2により管理対象情報の運搬について必要と決定した措置を実施していることを確認する。	【規定等】 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
Ⅴ					管理対象情報が電子情報である場合のアクセスの制限等			事業者は、管理対象情報が電子情報である場合には、可搬式記録媒体（パーソナルコンピュータを含む。以下このⅤにおいて同じ。）の持ち出しを管理し、当該電子情報が事業者の内部のサーバ等で記録されている場合には、ID認証、パスワード等により当該電子情報へのアクセスをアクセス権者に制限した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報へのアクセスの制限を実施する。なお、当該電子情報がクラウド等当該事業者以外の者のサーバ等で記録されている場合には、そのクラウド等を管理する者の信頼性を確認（例えば、ISO／IEC27017の認証の取得の状況、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるCSマークの取得の状況等を確認）、し 又は当該事業者以外の者であるデータセンターに自らのサーバ等を設置している場合は、当該データセンターの信頼性を確認（例えば、日本データセンター協会のデータセンターファシリティスタンダードのティア1からティア4を取得しているデータセンターのうち自らの管理対象情報の価値等に応じてデータセンターのサービスを適切に提供し得ること等を確認）、し 当該クラウド等を管理する者又はデータセンターとの間でⅥの秘密保持契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第二の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。		127	IT基盤運用管理に関する規程、クラウド等外部事業者の利用規程及び可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者との秘密保持契約、信頼性確認結果（認証取得状況の確認等）を閲覧し、以下の点について確認する。 ①可搬式記録媒体の持ち出しを管理している。 ②当該電子情報が事業者の内部のサーバ等で記録されている場合に、情報へのアクセスをアクセス権者に制限する等の必要な措置が実施されていることを確認する。 ③当該事業者以外の者のサーバ等で記録されている場合には、その管理者の信頼性を確認し、秘密保持契約を締結した上で、必要な措置を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程、クラウド等外部事業者の利用規程 【記録やその他の確認対象】 可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者との秘密保持契約、信頼性確認結果（認証取得状況の確認等）	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容			ID	確認内容	確認対象	到達レベル
	第一	1			情報システムの管理等		事業者（自らの情報システム（以下単に「情報システム」という。）の維持に責任を有する者を含む。以下2から10までにおいて同じ。）は、情報システムのセキュリティに配慮したログオン手順、電子メールで管理対象情報を送付する場合の手順等を含む操作手順書を作成し、常に利用者が利用可能な状態にする。		128	操作手順書を閲覧し、内容がセキュリティに配慮したログオン手順、管理対象情報を送付する場合の手順などが含まれているか、同操作手順書について常に利用可能な状態におかれているかを確認する。	【規定等】 操作手順書 【記録やその他の確認対象】	1.実施している
		2					事業者は、情報システムとインターネットの間にファイアウォールを導入する。		129	IT基盤運用管理に関する規程及びネットワーク図、セキュリティ対策機器の設定情報等を閲覧し、情報システムとインターネットの間にファイアウォールを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ネットワーク図、セキュリティ対策機器の設定情報等	2.実施計画があり、進捗管理している
		3					事業者は、情報システムへのアクセスログ等を取得する。		130	IT基盤運用管理に関する規程及びアクセスログを閲覧し、情報システムへのアクセスログ等を取得していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセスログ	1.実施している
		4					事業者は、3のアクセスログをその記録のあった日から合理的な期間以上保存し、情報システムの維持に責任を有する者（情報システムの管理を当該事業者以外の者に委託等をしている場合には、当該者を含む。以下この第一において同じ。）により定期的に点検させ、当該アクセスログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。		131	IT基盤運用管理に関する規程及びアクセスログ点検記録を閲覧し、アクセスログを合理的な期間以上保存し、情報システムの維持に責任を有する者によりアクセスログを定期的に点検させ、アクセスログを保護するために適切な措置を講じていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセスログ点検記録	3.実施の結果である成果物を管理している
		5					事業者は、IDS（Intrusion Detection System）等により、情報システムへの不正なアクセスを検知して、情報システムの維持に責任を有する者に通知するシステムを導入する。		132	IT基盤運用管理に関する規程やインシデント対応手順及びネットワーク図、もしくはシステム構成図を閲覧し、IDS等情報システムへの不正なアクセスを検知し、通知するシステムを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図	2.実施計画があり、進捗管理している
		6					事業者は、4の点検の結果により不正なアクセスが発見された場合、5の通知があった場合等に、情報システムの維持に責任を有する者が速やかに、適切な措置を講ずるための手順を確立する。		133	IT基盤運用管理に関する規程やインシデント対応手順を閲覧し、4の点検の結果により不正なアクセスが発見された場合、5の通知があった場合等に、情報システムの維持に責任を有する者が速やかに、対応するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		7					事業者は、IPS（Intrusion Prevention System）等により、情報システムへの不正なアクセスを検知し、防御するシステムを導入する。		134	IT基盤運用管理に関する規程やインシデント対応手順及びネットワーク図、もしくはシステム構成図を閲覧し、IPS等により、情報システムへの不正なアクセスを検知し、防御するシステムを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図	2.実施計画があり、進捗管理している
		8					事業者は、ネットワークに接続するサーバについて、不要なポートを閉鎖すること、匿名でのネットワークへの接続（Anonymous接続）を禁止すること等を実施する。		135	IT基盤運用管理に関する規程やインシデント対応手順を閲覧し、ネットワークに接続するサーバについて、不要なポートを閉鎖し、匿名でのネットワークへの接続を禁止すること等を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		9						事業者は、最新の脆弱性情報を常時入手し、当該脆弱性情報を、情報システムのセキュリティの向上をしていくために反映等をさせていく仕組みを確立する。		136	IT基盤運用管理に関する規程やインシデント対応手順脆弱性情報入手記録、入手した脆弱性情報の対応記録を閲覧し、最新の脆弱性情報を常時入手し、情報システムのセキュリティ向上のために反映等をさせていく仕組みを確立している。その仕組みに沿って、最新の脆弱性情報を常時入手し、情報システムへの影響を把握し、必要な措置を実施することで、情報セキュリティの向上を実現していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 脆弱性情報入手記録、入手した脆弱性情報の対応記録	7.成果達成のために予測し、運用している
		10						事業者は、情報システムを構成するハードウェア、ソフトウェア等について、サポート窓口が明確であり、当該サポート窓口に常時連絡がとれる事業者から導入する。		137	IT基盤運用管理に関する規程及びハードウェア・ソフトウェア管理簿やメーカサポート体制の一覧等を閲覧し、ハードウェア、ソフトウェア等について、サポート窓口が明確であり、サポート窓口に常時連絡がとれる事業者から導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ハードウェア・ソフトウェア管理簿やメーカサポート体制の一覧等	2.実施計画があり、進捗管理している
		11						情報システムの維持に責任を有する者は、情報システムを構成するハードウェア、ソフトウェア等の管理簿（保守（修理を含む。以下同じ。）及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応の記録を含む。）を作成し、合理的な期間保管する。		138	ネットワーク図、もしくはシステム構成図、ハードウェア・ソフトウェア管理簿を閲覧し、情報システムの維持に責任を有する者は、情報システムを構成するハードウェア、ソフトウェア等の管理簿（保守（修理を含む。以下同じ。）及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応の記録を含む。）を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図、ハードウェア・ソフトウェア管理簿	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		12						事業者（管理者等管理対象情報を取り扱う情報システム（以下このⅤにおいて「管理情報システム」という。）の維持に責任を有する者を含む。22から24までを除き、以下このⅤ及びⅦの第一の3において同じ。）、は 管理情報システムを最新の状態に更新されたウィルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行い、パッチの更新を行うこと等により、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護し、適切に機能を提供するための取組を実施する。		139	IT基盤運用管理に関する規程及びウイルス対策方法が記されたユーザマニュアル等を閲覧し、管理情報システムを最新のウィルス対策ソフトウェア等を用いて、少なくとも週１回以上フルスキャンを行い、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護し、適切に機能を提供するための取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等	1.実施している
		13						業者は、一定期間（例えば、1週間）電源の切られた状態にある管理情報システムを構成する機器については、再度の電源投入時に12の取組を実施する。		140	IT基盤運用管理に関する規程ウイルス対策方法が記されたユーザマニュアル等を閲覧し、一定期間電源の切られた状態にある管理情報システムを構成する機器については、再度の電源投入時に12の取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等	1.実施している
		14						事業者は、管理対象情報を記録するための可搬式記録媒体について、12又は13の取組を実施する。この場合において、13中「電源の切られた」とあるのは「使用されていない」、「電源投入時」とあるのは「使用の前」とする。		141	IT基盤運用管理に関する規程及びウイルス対策方法が記されたユーザマニュアル等を閲覧し、管理対象情報を記録するための可搬式記録媒体について、12又は13の取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等	1.実施している
		15						事業者は、管理情報システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限するための手順を確立する。		142	IT基盤運用管理に関する規程を閲覧し、管理情報システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		16						事業者は、管理情報システムにソフトウェアを導入する場合、管理者等管理情報システムの維持に責任を有する者によりソフトウェアの安全性が確認された場合を除き、認めないための手順を確立する。		143	IT基盤運用管理に関する規程を閲覧し、管理情報システムにソフトウェアを導入する場合、ソフトウェアの安全性が確認された場合を除き、認めないための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		17						事業者は、管理情報システムに対するペネトレーションテストを定期的に実施する。	144	IT基盤運用管理に関する規程ペネトレーションテスト報告書、ペネトレーションテスト後の対処状況を閲覧し、管理情報システムに対するペネトレーションテストを定期的に実施し、実施結果を踏まえて必要な対処が実施されているか確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ペネトレーションテスト報告書、ペネトレーションテスト後の対処状況	3.実施の結果である成果物を管理している
		18						事業者は、この告示のⅣの立入制限区域に管理情報システムを構成する機器のうちサーバ等一定のものを設置する。この場合において、管理者等管理情報システムの維持の責任を有する者は、当該一定のもの以外のサーバ等の持込みを禁止し、及びサーバ等を新設する場合の内蔵ソフトウェアの状況を確認した上で、当該サーバ等が従業員等の個人の所有にかからないものに限り認めるための手順を確立する。	145	IT基盤運用管理に関する規程を閲覧し、立入制限区域には管理情報システムを構成する機器のうちサーバ等一定のものを設置し、それ以外の持込みについて状況を判断のうえ、必要最小限認めるための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		19						事業者は、管理情報システムを構成する機器及び立入制限区域等の特定の場所でのみ使用する可搬式記録媒体について、施錠できるラック等への設置、セキュリティワイヤでの固定等不正な持ち出し、盗難等から保護するための措置（ラック等の鍵について、管理者等管理情報システムの維持に責任を有する者による管理を含む。）を講ずる。	146	物理的対策やIT機器利用、IT基盤運用管理に関する規程の閲覧及び管理情報システム構成機器の設置場所の現地調査を実施し、管理情報システムを構成する機器及び可搬式記録媒体について、施錠できるラック等への設置、セキュリティワイヤでの固定等不正な持ち出し、盗難等から保護するための措置（ラック等の鍵について、管理者等管理情報システムの維持に責任を有する者による管理を含む。）を講じていることを確認する。	【規定等】 物理的対策やIT機器利用、IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システム構成機器の設置場所	1.実施している
		20						事業者は、管理者等管理情報システムの維持に責任を有する者が、当該管理情報システムを構成する機器の持ち出しに伴うリスクを回避することができると判断し、その承認をした場合を除き、当該機器を持ち出させないための手順（持ち出しをする場合の記録を含む。）を確立する。	147	IT機器利用やIT基盤運用管理に関する規程及びシステム機器持ち出し管理簿を閲覧し、管理者等情報システムの維持に責任を有する者が、管理情報システムを構成する機器の持ち出しを承認した場合を除き、機器を持ち出させないための手順（持ち出しをする場合の記録を含む。）を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 システム機器持ち出し管理簿	3.実施の結果である成果物を管理している
		21						事業者は、管理情報システムを構成する機器について、不要なネットワークポート、USBポート、シリアルポートを物理的に閉塞すること等当該機器に可搬式記録媒体を接続することによる管理対象情報の流出を防止する措置を実施するための手順を確立する。	148	IT機器利用やIT基盤運用管理に関する規程及び管理情報システム構成機器のポートの状況の現地調査を実施し、管理情報システムを構成する機器について、不要なポートを物理的に閉塞すること等当該機器への可搬式記録媒体の接続を防止する措置を実施するための手順を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 管理情報システム構成機器のポートの状況	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		22						事業者は、管理者等管理情報システムの維持に責任を有する者の利用権限を必要最低限にとどめ、当該利用権限が最低限であることを定期的に監査するための手順を確立する。		149	IT基盤運用管理に関する規程及びアクセス権設定記録を閲覧し、管理者等情報システムの維持に責任を有する者の利用権限を必要最低限にとどめ、利用権限が最低限であることを定期的に監査するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセス権設定記録	3.実施の結果である成果物を管理している
		23						事業者は、管理者等管理情報システムの維持に責任を有する者について、その者による当該管理情報システムの設定変更や運用に関する作業ログを取得する。		150	IT基盤運用管理に関する規程及び機器のセキュリティログ情報等を閲覧し、管理者等情報システムの維持に責任を有する者による管理情報システムの設定変更や運用に関する作業ログを取得していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 機器のセキュリティログ情報等	3.実施の結果である成果物を管理している
		24						事業者は、23の作業ログについて、管理者等管理情報システムの維持に責任を有する者の上司等により、又はデータ解析ツール（データマイニングツール）を活用すること等により、定期的に点検させる。		151	IT基盤運用管理に関する規程及び機器のセキュリティログ情報等を閲覧し、23の作業ログについて、管理者等情報システムの維持に責任を有する者の上司等により、定期的に点検させていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 機器のセキュリティログ情報等	3.実施の結果である成果物を管理している
		25						事業者は、管理情報システムに係るサービス、システム、機器の保守及び点検をサプライヤー含む外部の第三者に行わせる場合であって、管理対象情報に関わるときは、管理者等管理情報システムの維持に責任を有する者の指示の下で、管理対象情報を他の記録媒体に移した上で、管理対象情報を復元できないように消去する等の措置を実施し、又は従業員等が保守及び点検業務に立ち会い、若しくは作業ログを取得し、若しくはカメラを設置すること等により、作業を監視することができる状況で行わせる手順を確立する。		152	IT基盤運用管理や委託管理に関する規程及び業務委託契約や委託先作業記録を閲覧し、管理情報システムに係る保守及び点検を外部の第三者に行わせ、管理対象情報に関わるときは、管理者等管理情報システムの維持に責任を有する者の指示の下で、管理対象情報を他の記録媒体に移した上で復元できないように消去する等の措置を行い、又は作業を監視することができる状況で行わせる手順を定めていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や委託先作業記録	3.実施の結果である成果物を管理している
		26						事業者は、管理情報システムに係るサービス、システム、機器の第三者による情報システムの保守及び点検に当たって、当該第三者の作業者にIDを付与することが必要な場合には、一時的なIDを付与することとし、作業終了後は、その権限を無効化するための手順を確立する。		153	IT基盤運用管理や委託管理に関する規程及び管理情報システムへのアクセス権設定記録を閲覧し、管理情報システムの第三者による保守及び点検に当たって、当該第三者の作業者には一時的なIDを付与し、作業終了後は、その権限を無効化するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 管理情報システムへのアクセス権設定記録	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		27			事業者は、管理情報システムを構成する機器をこの告示のⅣの立入制限区域に設置する場合であって、当該管理情報システムを構成する機器の保守及び点検をサプライヤーを含む第三者に行わせるときは、Ⅵの秘密保持契約を締結した上で行わせる。この場合において、管理者等管理情報システムの維持に責任を有する者は、当該第三者の作業者についてこの告示のⅣの第二の6の手順を確立しているときは当該手順に従い、若しくは当該手順を確立していないときは作業者を確認し、当該作業者の立入りを認め、並びに当該立入制限区域内の保守及び点検の対象となる機器以外の機器（当該立入制限区域内に保守及び点検の対象となる機器に記録された管理対象情報以外の管理対象情報が置かれている場合には当該管理対象情報を含む。）を撤去すること等により作業者が当該保守及び点検の対象となる機器以外の機器への接触を防止するための措置を講じた上で、作業者が作業を実施している間は管理者等管理情報システムの維持に責任を有する者が常時立ち会うようにし、又はその指定する者に立ち会わせ、当該指定する者からの作業の状況の報告を受けるものとする。		154	IT基盤運用管理や委託管理に関する規程及び業務委託契約や機密保持契約、委託先作業記録を閲覧し、立入制限区域に設置する管理情報システムを構成する機器の保守及び点検を第三者に行わせるときは、Ⅵの秘密保持契約を締結した上で行わせている。管理情報システムの維持に責任を有する者は、第三者の作業者について告示のⅣの第二の6の手順に従い、若しくは作業者を確認し、立入りを認め、並びに作業者が当該保守及び点検の対象となる機器以外の機器（当該立入制限区域内に保守及び点検の対象となる機器に記録された管理対象情報以外の管理対象情報が置かれている場合には当該管理対象情報を含む。）への接触を防止するための措置を講じた上で、作業間は常時立ち会う、又は指定する者に立ち会わせ作業状況の報告を受けることにより、作業の状況の報告を受けるものとしていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や機密保持契約、委託先作業記録	3.実施の結果である成果物を管理している
		28			事業者は、クラウド等を管理する者又はデータセンターのサーバ等で管理対象情報を管理している場合におけるその従業員等が、当該サーバ等の保守及び点検を行うときは、以下のいずれかの措置を実施する。				155	委託管理に関する規程や、クラウドやデータセンターにおける管理規程を閲覧し、クラウド等を管理する者又はデータセンターのサーバ等で管理対象情報を管理している場合、その従業員等が保守及び点検を行うときは、第一の28に定めるいずれかの措置を実施していることを確認する。	【規定等】 委託管理に関する規程や、クラウドやデータセンターにおける管理規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
				一		その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等である場合 当該保守及び点検を行う従業員等を確認する等の措置					
				二		その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等以外である場合 当該クラウド等を管理する者又はデータセンターにおいて25、26に掲げる措置等適切な措置を講ずることを確認する等の措置					
		29			事業者は、管理対象情報について、定期的な保存（バックアップ）を実施し、当該保存された情報を管理対象情報として適切に管理する。				156	IT基盤運用管理に関する規程及びデータバックアップ管理簿を閲覧し、管理対象情報について、定期的な保存（バックアップ）を実施し、バックアップを管理対象情報として適切に管理していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 データバックアップ管理簿	3.実施の結果である成果物を管理している
		30			事業者は、管理情報システムで取り扱われた管理対象情報の漏えいの事故等が発生した場合、その疑いがある場合及び管理対象情報が記録されたサーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染又は不正アクセスが認められた場合等に、その証拠を収集するための手順を確立する。				157	IT機器利用やIT基盤運用管理、インシデントの対応手順及びを閲覧し、管理情報システムで取り扱われた管理対象情報の漏えいの事故等が発生した場合等、その証拠を収集するための手順を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】	3.実施の結果である成果物を管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		31						事業者は、管理情報システムを構成する機器を再利用する場合は、管理対象情報が復元できない状態であることを点検した後で再利用する。		158	IT機器利用やIT基盤運用管理に関する規程及び管理情報システム構成機器のデータ消去記録を閲覧し、管理情報システムを構成する機器を再利用する場合は、管理対象情報が復元できない状態であることを点検した後で再利用していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 管理情報システム構成機器のデータ消去記録	3.実施の結果である成果物を管理している
		32						事業者は、管理情報システムの利用の状況、管理情報システムにおける管理対象情報へのアクセス（アクセス権者が利用した管理情報システムを構成する機器並びに当該機器へのログオン又はログオフの日時及びその成否並びに使用されたプログラムを含む。）及び例外処理を記録した監査ログを取得する。		159	IT機器利用やIT基盤運用管理、インシデントの対応手順及び機器のセキュリティログ情報等を閲覧し、管理情報システムの利用状況、管理対象情報へのアクセス（アクセス権者が利用した管理情報システムを構成する機器並びに当該機器へのログオン又はログオフの日時及びその成否並びに使用されたプログラムを含む。）及び例外処理を記録した監査ログを取得していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】 機器のセキュリティログ情報等	3.実施の結果である成果物を管理している
		33						事業者は、32の監査ログを記録のあった日から三月以上保存し、定期的に点検し、当該監査ログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。		160	IT機器利用やIT基盤運用管理、インシデントの対応手順及び機器のセキュリティログ情報等を閲覧し、32の監査ログを記録のあった日から三月以上保存し、定期的に点検し、当該監査ログを改ざん又は不正なアクセスから保護するために適切な措置を講じていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】 機器のセキュリティログ情報等	3.実施の結果である成果物を管理している
		34						事業者は、管理情報システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめる。		161	管理情報システムに対する監査ツールの利用状況の現地調査を実施し、管理情報システムの監査に用いるツールについて、必要最低限の使用にとどめていることを確認する。	【規定等】 【記録やその他の確認対象】 管理情報システムに対する監査ツールの利用状況	1.実施している
		35						事業者は、情報システムを構成するソフトウェアの利用状況を確認し、利用がされていない場合には、当該ソフトウェアを消去する。		162	IT機器利用やIT基盤運用管理に関する規程の閲覧及びソフトウェアの利用状況・削除の確認記録、ソフトウェアの利用状況の現地調査を実施し、情報システムを構成するソフトウェアの利用状況を確認し、利用がされていない場合には、当該ソフトウェアを消去していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 ソフトウェアの利用状況・削除の確認記録、ソフトウェアの利用状況	3.実施の結果である成果物を管理している
		36						事業者は、管理情報システム及びネットワークを通じて管理情報システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせる。		163	IT基盤運用管理に関する規程及びシステム構成図を閲覧し、管理情報システム及びネットワークを通じて管理情報システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 システム構成図	1.実施している
		37						事業者は、管理情報システムの共有ネットワーク（インターネット等）への接続については、その接続に伴うリスクから保護するため、アクセス権者の職務内容に応じて設定するアクセス制御の方針（定期的又は管理対象情報の漏えいの事故等があった場合に見直すことができるものに限る。）を定め、これに基づいて認めるための手順を確立する。		164	管理情報システムから共有ネットワークへのアクセス制御方針及び管理情報システムから共有ネットワークへのアクセス制御状況を閲覧し、管理情報システムの共有ネットワークへの接続についてのアクセス制御の方針を定め、これに基づいて認めるための手順を定めていることを確認する。	【規定等】 管理情報システムから共有ネットワークへのアクセス制御方針 【記録やその他の確認対象】 管理情報システムから共有ネットワークへのアクセス制御状況	5.定義された事項を周知し、同一事項を実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		38						事業者は、情報システムから外部への通信についてログの取得等により監視する。	165	IT基盤運用管理に関する規程及び情報システムから外部への通信ログを閲覧し、情報システムから外部への通信についてログの取得等により監視していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 情報システムから外部への通信ログ	3.実施の結果である成果物を管理している
		39						事業者は、管理情報システムを構成する機器について、無線でのネットワークへの接続をすることができるものを用いない。	166	IT基盤運用管理に関する規程及びシステム構成図等を閲覧し、管理情報システムを構成する機器について、無線ネットワークへの接続をすることができるものを用いていないことを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 システム構成図等	1.実施している
		40						事業者は、管理情報システムを構成する機器を廃棄する場合には、当該機器に記録された管理対象情報が復元できない状態であることを確認し、当該機器を物理的に破壊し、廃棄する。	167	IT機器利用やIT基盤運用管理に関する規程及びIT機器等の廃棄管理簿を閲覧し、管理情報システムを構成する機器を廃棄する場合には、管理対象情報が復元できない状態であることを確認し、物理的に破壊し、廃棄していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 IT機器等の廃棄管理簿	3.実施の結果である成果物を管理している
		41						事業者は、立入制限区域の内部のみで利用する管理情報システムを、有線により配線接続して構築し、当該立入制限区域の外部への通信を行わせないための手順を確立する。	168	IT基盤運用管理に関する規程の閲覧及び管理情報システムのネットワーク接続状況の現地調査を実施し、立入制限区域の内部のみで利用する管理情報システムを、有線接続して構築し、外部への通信を行わせないための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システムのネットワーク接続状況	3.実施の結果である成果物を管理している
		42						事業者又はアクセス権者は、管理情報システムが無人状態に置かれる場合、使用していない管理情報システムを構成する機器の電源を切り、又は機器の表示画面の表示停止と再表示時にパスワードが必要なよう設定すること等により、無人状態であっても管理対象情報が適切に保護されるよう必要な対応をする。	169	IT基盤運用管理に関する規程の閲覧及び管理情報システムの状況の現地調査を実施し、事業者又はアクセス権者は、管理情報システムが無人状態に置かれる場合、使用していない機器の電源を切り、又はの画面の表示停止とパスワード設定等により、無人状態であっても管理対象情報が適切に保護されるよう必要な対応をしていることを確認する。	【規定等】 IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システムの状況	2.実施計画があり、進捗管理している
	第二	1			電子情報である管理対象情報へのアクセスに関する対応			事業者は、管理情報システムの利用者の職務内容に応じて、利用できる機能を制限した上で、これを提供する。	170	管理情報システムのアクセス制御及び認証に関する方針及び管理情報システムの機能の利用設定を閲覧し、管理情報システムの利用者の職務内容に応じて、利用できる機能を制限した上で、提供していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 管理情報システムの機能の利用設定	1.実施している

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		2						事業者は、アクセス権者による管理情報システムへのアクセスを許可し、適切なアクセス権を付与するため、管理情報システムの利用者としての登録及び人事異動等に伴い速やかに登録の削除をするための手順（定期的な見直しを含む。）を確立する。		171	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、アクセス権者による管理情報システムへのアクセスを許可し、適切なアクセス権を付与するため、管理情報システムの利用者としての登録及び人事異動等に伴い速やかに登録の削除をするための手順（定期的な見直しを含む。）を定めていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況	7.成果達成のために予測し、運用している
		3						事業者は、管理情報システムの利用者に対して、初期又は仮のパスワードを発行する場合には、容易に推測されないパスワードを発行する等その適切な管理に配慮した方法で発行する。		172	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、管理情報システムの利用者に対して、容易に推測されない初期又は仮のパスワードを発行していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況	1.実施している
		4						事業者は、管理情報システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させる。		173	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、管理情報システムの利用者ごとに一意な識別子を保有させていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況	1.実施している
		5						事業者は、アクセス権設定等の特別な権限を持つ管理者等管理情報システムの維持に責任を有する者の管理情報システムへのログインに対して、二つの認証機能（パスワード、生体認証、電子証明書等）を組み合わせた二要素認証を導入する。		174	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムへのログイン環境の現地調査を実施し、特別な権限を持つ管理者等の管理情報システムへのログインには、二要素認証を導入していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムへのログイン環境	1.実施している
		6						事業者は、アクセス権者においてパスワードを自ら設定させ、パスワードを設定する場合には、当人の関連情報（例えば、名前、電話番号、誕生日等）に基づかないこと、辞書攻撃に脆弱でないこと（辞書に含まれる語からだけで成り立っていないこと）、同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではないことを求めること等アクセス権者以外の者から容易に類推されないような設定とするようアクセス権者に周知し、又は管理情報システムでパスワードを設定する者に対してその要求をするようにする。		175	管理情報システムのアクセス制御及び認証に関する方針の閲覧及びアクセス制御及び認証に関する方針の周知状況、又はパスワード設定状況の現地調査を実施し、アクセス権者においてパスワードを設定する場合には、アクセス権者以外の者から容易に類推されないような設定とするようアクセス権者に周知し、又は管理情報システムでパスワードを設定する者に対してその要求をしていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 アクセス制御及び認証に関する方針の周知状況、又はパスワード設定状況	2.実施計画があり、進捗管理している
		7						事業者は、管理情報システムそのものに、必要に応じてパスワードの変更を利用者に促す機能やパスワードの再利用を防止する機能等を持つようにする。		176	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムのパスワード設定に関する機能の実装状況の現地調査を実施し、管理情報システムそのものに、パスワードの変更を利用者に促す機能やパスワードの再利用を防止する機能等を持たせていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムのパスワード設定に関する機能の実装状況	1.実施している
		8						管理者等管理情報システムの維持に責任を有する者は、アクセス権者等に対して、管理情報システムにログオンするためのパスワードを記載した紙を目に見えるところに置かないこと等を周知する。		177	パスワード管理に関する周知状況の現地調査を実施し、管理者等は、アクセス権者等に対して、管理情報システムにログオンするためのパスワードを記載した紙を目に見えるところに置かないこと等を周知していることを確認する。	【規定等】 【記録やその他の確認対象】 パスワード管理に関する周知状況	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番							ID	確認内容	確認対象	到達レベル
								内容					
		9						事業者は、管理情報システムへのアクセスについては、複数者間で同じパスワード（共通パスワード）を使用しないための手順を確立する。		178	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムのパスワード設定に関する機能の実装状況、又はパスワード管理に関する周知状況の現地調査を実施し、管理情報システムへのアクセスについては、複数者間で同じパスワードを使用しないための手順を定めていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムのパスワード設定に関する機能の実装状況、又はパスワード管理に関する周知状況	3.実施の結果である成果物を管理している
		10						事業者は、アクセス権者によるテレワーク等外部からの管理情報システムの管理対象情報へのアクセスについて、利用者の認証を行うための手順（管理者等管理情報システムの維持に責任を有する者は、あらかじめ、認めた範囲でのみ認証をするためのものを含む。）を確立するとともに、可能な限り暗号化された通信路を用いさせる。		179	管理情報システムのアクセス制御及び認証に関する方針を閲覧し、アクセス権者による外部からの管理対象情報へのアクセスについて、利用者の認証を行うための手順（管理者等管理情報システムの維持に責任を有する者は、あらかじめ、認めた範囲でのみ認証をするためのものを含む。）を定めていることを確認する。可能な限り暗号化された通信路を用いさせていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】	2.実施計画があり、進捗管理している
		11						管理者等管理情報システムの維持に責任を有する者は、電子政府推奨暗号を用いて暗号化する等の措置を講じた上で管理情報システムにおいて管理対象情報を適切に管理するための手順を確立する。		180	IT基盤運用管理に関する規程を閲覧し、管理者等管理情報システムの維持に責任を有する者は、電子政府推奨暗号を用いて暗号化する等の措置を講じた上で管理情報システムにおいて管理対象情報を適切に管理するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】	2.実施計画があり、進捗管理している
	第三	1			管理対象情報の取扱い			事業者は、可搬式記録媒体に管理対象情報が記録されている場合には、当該可搬式記録媒体を管理対象情報そのものとして取り扱うための手順（可搬式記録媒体の使用を事業者が承認し、当該可搬式記録媒体を他の技術等情報が記録された可搬式記録媒体と容易に区別することができるよう措置するための手順を含む。）を確立する。		181	IT機器利用やIT基盤運用管理に関する規程を閲覧し、可搬式記録媒体に管理対象情報が記録されている場合には、可搬式記録媒体を管理対象情報そのものとして取り扱うための手順（可搬式記録媒体の使用を事業者が承認し、当該可搬式記録媒体を他の技術等情報が記録された可搬式記録媒体と容易に区別することができるよう措置するための手順を含む。）を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		2						管理者等管理情報システムの維持に責任を有する者は、管理対象情報を記録し、又は記録のために用いる可搬式記録媒体の管理簿（保守及び点検の記録、持ち出した場合の持ち出しの記録、データの消去の記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等の記録を含む。）を作成し、合理的な期間保管する。		182	IT機器利用やIT基盤運用管理に関する規程及び可搬式記録媒体管理簿、及び可搬式記録媒体の保存期間を閲覧し、管理者等は、可搬式記録媒体の管理簿（保守及び点検の記録、持ち出した場合の持ち出しの記録、データの消去の記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等の記録を含む。）を作成し、合理的な期間保管していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿、及び可搬式記録媒体の保存期間	2.実施計画があり、進捗管理している
		3						事業者は、電子情報である管理対象情報を可搬式記録媒体に記録する場合は、暗号技術を用いる。		183	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、管理対象情報を可搬式記録媒体に記録する場合は、暗号技術を用いていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿	1.実施している

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		4						事業者は、管理対象情報を記録した可搬式記録媒体を施錠することができるロッカー等に集中的に保管し、その鍵等を適切に管理する。		184	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、管理対象情報を記録した可搬式記録媒体を施錠することができるロッカー等に集中的に保管し、その鍵等を適切に管理していることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿	2.実施計画があり、進捗管理している
		5						事業者は、可搬式記録媒体に記録した管理対象情報を消去する場合には、復元できないように上書き消去（データの完全消去）を速やかに行うための手順を確立する。		185	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、可搬式記録媒体に記録した管理対象情報を消去する場合には、復元できないように上書き消去を速やかに行うための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿	3.実施の結果である成果物を管理している
		6						事業者は、5の手順に従い管理対象情報が消去された可搬式記録媒体に限り、その使用を認める。		186	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、5の手順に従い管理対象情報が消去された可搬式記録媒体に限り、その使用を認めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿	1.実施している
		7						事業者は、管理対象情報が記録されたサーバや可搬式記録媒体の廃棄を行う場合には、ハードディスクドライブ等全体に対して上書き消去（デー タの完全消去）を行い、その消去を確認した上で、物理的な破壊を行うための手順を確立する。		187	IT基盤運用管理に関する規程及び可搬式記録媒体管理簿、又はサーバ廃棄記録を閲覧し、管理対象情報が記録されたサーバや可搬式記録媒体の廃棄を行う場合には、ハードディスクドライブ等全体に対して上書き消去を行い、その消去を確認した上で、物理的な破壊を行うための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿、又はサーバ廃棄記録	3.実施の結果である成果物を管理している
		8						事業者は、管理情報システムを構成する機器の廃棄を行う場合には、データを消去すること等により読み取りができない状態にするための手順を確立する。		188	IT基盤運用管理に関する規程ハードウエア・ソフトウエアの管理簿、又は廃棄記録を閲覧し、管理情報システムを構成する機器の廃棄を行う場合には、データを消去すること等により読み取りができない状態にするための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ハードウエア・ソフトウエアの管理簿、又は廃棄記録	3.実施の結果である成果物を管理している
		9						事業者は、管理情報システムを構成する機器及び可搬式記録媒体であって、個人が所有するもので、管理対象情報を、取り扱わせないための手順を確立する。		189	IT機器利用に関する規程を閲覧し、管理情報システムを構成する機器及び可搬式記録媒体であって、個人が所有するもので、管理対象情報を、取り扱わせないための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		10						事業者は、管理対象情報を電子メールで送信する場合は、送信する管理対象情報又は電子メールそのものについて暗号化すること等の適切な措置を講ずるための手順を確立する。		190	電子メール利用に関する規定を閲覧し、電子メールで管理対象情報を送付する場合は、暗号化すること等の適切な措置を講ずるための手順を定めていることを確認する。	【規定等】 電子メール利用に関する規定 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		11						事業者は、管理対象情報を電子メールで送信する場合又は受信する場合に、その送受信のログを合理的な期間保存する。		191	IT基盤運用管理に関する規程及び電子メールの送受信ログ、及びログ保存期間を閲覧し、管理対象情報の電子メールでの送受信ログを合理的な期間保存していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 電子メールの送受信ログ、及びログ保存期間	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
		12						事業者は、管理対象情報を可搬式記録媒体に保存した上で管理情報システムからの消去を行うこと、他者から預けられた管理対象情報であって可搬式記録媒体に記録されたものを事業者の可搬式記録媒体にのみ保存し、利用すること等により、当該管理対象情報を、必要最小限の範囲で取り扱うための手順を確立する。		192	IT機器利用に関する規程可搬式記録媒体管理簿を閲覧し、管理対象情報を可搬式記録媒体に保存した上で管理情報システムからの消去を行うこと、他者から預けられた管理対象情報であって可搬式記録媒体に記録されたものを事業者の可搬式記録媒体にのみ保存し、利用すること等、管理対象情報を、必要最小限の範囲で取り扱うための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿	3.実施の結果である成果物を管理している
Ⅵ					管理対象情報をその管理対象情報を保有する事業者以外の者に渡す場合の措置			事業者は、管理対象情報を当該事業者の管理に属する従業員等以外の者（以下「外部委託先等」という。）に渡し、取り扱わせる場合には、当該管理対象情報の第三者への開示の禁止等を含む秘密保持契約を締結した後で引き渡す取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施することを通じて、外部委託先等における管理対象情報の適切な管理を確保する。		193	委託管理に関する規程及び秘密保持契約を閲覧し、管理対象情報を外部委託先等に渡し、取り扱わせる場合には、管理対象情報の第三者への開示の禁止等を含む秘密保持契約を締結した後で引き渡す取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約	3.実施の結果である成果物を管理している
	第一	1				外部委託先等に管理対象情報を取り扱わせる前の確認		事業者は、管理対象情報を外部委託先等に取り扱わせる場合には、当該外部委託先等からの情報の流出等のリスクを考慮し、真に必要な取引であるかを検討した上で行う。		194	委託管理に関する規程を閲覧し、管理対象情報を外部委託先等に取り扱わせる場合には、真に必要な取引であるかを検討した上で行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】	1.実施している
		2						事業者は、管理対象情報の取扱いを外部委託先等に行わせる場合には、当該外部委託先等が、管理対象情報を適切に管理し、かつ、当該事業者の要請に適切に対応できる能力を有するか否かについて事前に確認する。この確認は、基本的には、自らが講じている管理対象情報の適切な管理に係る取組と同等以上の取組が外部委託先等において行われているか否かを確認し、特に、外部委託先等が海外企業である場合等には、物理的に管理が行き届かないことや、法律や商慣行の違い等により漏えいリスクが高まる可能性も考えられるため、より確実に行う。		195	委託管理に関する規程及び業務委託契約を閲覧し、管理対象情報の取扱いの外部委託先等が、管理対象情報を適切に管理し、かつ、事業者の要請に適切に対応できる能力を有するか否かについて事前に確認していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 業務委託契約	1.実施している
		3						事業者は、管理対象情報を外部委託先等に渡す場合の当該外部委託先等の事前の確認及び評価のための手順を確立する。		196	委託管理に関する規程を閲覧し、管理対象情報を外部委託先等に渡す場合の当該外部委託先等の事前の確認及び評価のための手順を定めていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】	3.実施の結果である成果物を管理している
		4						事業者は、必要に応じて、外部委託先等に対して、作成したこの告示のⅧの第四の方針等を周知する。		197	委託管理に関する規程及び業務委託契約や委託先作業管理簿を閲覧し、外部委託先等に対して、作成した方針等を周知していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や委託先作業管理簿	1.実施している
	第二	1				秘密保持契約		事業者は、管理対象情報を外部委託先等に提供する前に、以下の事項のうち必要なものを含む秘密保持契約の締結又はこれに準ずる法的拘束力のある取決めを交わす取組が習慣化し、文書等の定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		198	委託管理に関する規程及び秘密保持契約を閲覧し、管理対象情報を外部委託先等に提供する前に、秘密保持契約の締結又はこれに準ずる法的拘束力のある取決めを交わす取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約	3.実施の結果である成果物を管理している
				ー					外部委託先等は、提供された管理対象情報の取扱者を限定すること。				

別紙2　監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象	到達レベル
				二					外部委託先等は、提供された管理対象情報の取扱者の氏名等を明らかにすること。				
				三					外部委託先等における提供された管理対象情報の取扱者の範囲がNeed to Knowの原則に照らして必要最小限であることを、当該管理対象情報を提供する者が確認すること。				
				四					外部委託先等は、外部委託先等における提供された管理対象情報の取扱者による管理対象情報へのアクセスを記録し、管理すること。				
				五					外部委託先等は、提供された管理対象情報の複製、廃棄等をした場合の管理簿を作成し、合理的な期間保管すること。				
				六					外部委託先等は、管理対象情報を提供する者から求められている場合には、当該管理対象情報を提供する者に対して、当該管理対象情報の複製、廃棄等をした旨の通知を行うこと。				
				七					外部委託先等は、提供された管理対象情報に係る契約の満了時又は解除時において、当該管理対象情報を速やかに廃棄又は返還等をすること。				
				八					外部委託先等は、管理対象情報を提供する者に対して、当該管理対象情報の状況について、定期的に報告をすること。				
				九					外部委託先等において、定期的又は不定期に管理対象情報を提供する者からの監査を受け入れること。				
				十					管理対象情報を提供する者及び外部委託先等の両者の責任の下で、管理対象情報が秘密保持契約等の対象である旨の表示を提供する管理対象情報に付し、提供された管理対象情報の目録を作成し、最新のものに更新し、維持すること。				
		2						事業者は、秘密保持契約又は取決めのひな形を定める。		199	委託管理に関する規程及び秘密保持契約のひな型を閲覧し、秘密保持契約又は取決めのひな形を定めていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約のひな型	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
Ⅶ	第一	1			その他の管理対象情報の管理を強化するための措置	管理対象情報の段階を分けた管理と対応		事業者は、管理対象情報をその価値等に応じて段階を設けて管理し、当該段階に応じてこの告示のⅠの第三の管理者を選任（複数の段階の管理対象情報に係る管理者を一の者とすることを含む。）し、価値の高いものであればよりアクセス権者を限定し、物理的措置を複数組み合わせて強化する等の措置を講ずる。		201	管理対象情報の段階分けルール及び価値の高い管理対象情報に対する対策強化の状況の現地調査を実施し、管理対象情報をその価値等に応じて段階を設けて管理し、段階に応じてⅠ第三の管理者を選任（複数の段階の管理対象情報に係る管理者を一の者とすることを含む。）し、価値の高いものは対策を強化する等の措置を講じていることを確認する。	【規定等】 管理対象情報の段階分けルール 【記録やその他の確認対象】 価値の高い管理対象情報に対する対策強化の状況	
		2						事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって、この告示のⅠの第四の1の（1）の管理簿を作成するときは、その段階に応じて、管理簿を分けて作成する。		202	管理対象情報管理簿（段階別）を閲覧し、管理対象情報を段階を設けて管理する場合、段階に応じて、管理簿を分けて作成していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿（段階別）	1.実施している
		3						事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって、当該管理対象情報が電子情報であるときの管理情報システムが提供する機能について、アクセス権者に対し、提供する機能を制限する。		203	管理情報システムの提供機能の現地調査を実施し、管理対象情報を段階を設けて管理する場合、管理情報システムが提供する機能について、アクセス権者に対し、提供する機能を制限していることを確認する。	【規定等】 【記録やその他の確認対象】 管理情報システムの提供機能	1.実施している
		4						事業者は、管理対象情報のうち特に価値の高いもの等を管理するために立入制限区域の内部で間仕切りする場合には、入退室口及び警報装置を間仕切りした区画ごとに独立して設置する。		204	立入制限区域内の間仕切り区画の現地調査を実施し、立入制限区域の内部を間仕切りする場合には、入退室口及び警報装置を間仕切りした区画ごとに独立して設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域内の間仕切り区画	1.実施している
	第二	1				管理対象情報のより強固な管理のための敷地全体の防護		事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を金網等で囲う。		205	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を金網等で囲っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		2						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を、高さ2m以上の金網等で囲う。		206	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を、高さ2m以上の金網等で囲っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周	1.実施している
		3						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を囲う金網等の上部に2本以上の有刺鉄線等で敷地の外側に向かって角度をつけた忍び返しを設け、全体の高さを2.4m以上の外柵とする。		207	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を囲う金網等の上部に2本以上の有刺鉄線等で敷地の外側に向かって角度をつけた忍び返しを設け、全体の高さを2.4m以上の外柵としていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周	1.実施している
		4						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周には、赤外線警報装置、セキュリティカメラ等警備システムの導入により不審者の侵入に係る視認性を高める措置の導入を行う。		208	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周には、不審者の侵入に係る視認性を高める措置の導入を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周	1.実施している
		5						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。		209	警備員等の駆けつけ体制の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周の警備システムが作動した場合の警備員等の駆けつけ体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備員等の駆けつけ体制	1.実施している
		6						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周及びその周辺をモニターにより警備員等が常時監視する体制を確保する。		210	警備員等の常時監視体制の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周及びその周辺を警備員等が常時監視する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備員等の常時監視体制	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		7						事業者は、警備員等により、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周及びその周辺を4時間に1回以上巡回監視を実施する体制を確保する。		211	巡回監視体制の現地調査を実施し、警備員等により、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周及びその周辺を4時間に1回以上巡回監視を実施する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 巡回監視体制	1.実施している
	第三	1				外部委託先等における管理対象情報をより的確に管理するために考えられる措置		事業者は、外部委託先等に管理対象情報を提供する場合には、可能な限り分割して引き渡すことにより、管理対象情報の全体が外部委託先等から見てわからないようにする取組を行う。		212	及び委託先への管理対象情報受け渡し状況の現地調査を実施し、外部委託先等に管理対象情報を提供する場合、可能な限り分割して引き渡すことにより、管理対象情報の全体が外部委託先等から見てわからないようにする取組を行っていることを確認する。（管理者へのインタビューにより、委託先への管理対象情報受け渡し状況を確認する）	【規定等】 【記録やその他の確認対象】 委託先への管理対象情報受け渡し状況	3.実施の結果である成果物を管理している
		2						事業者は、製造設備のリモートメンテナンス等、管理対象情報そのものを渡すことにはならない一方で、長期にわたり徐々に技術等情報がリモートメンテナンス等を行う事業者に蓄積され、管理対象情報を構成することができるような事例にも対応するため、この告示のⅥの措置を組み合わせて、外部委託先等が技術等情報を適切に管理し、かつ、自らの要請に適切に対応できる能力を有するか否かについて事前に確認をし、蓄積された管理対象情報の目的外利用の禁止（例えば、リモートメンテナンスであればリモートメンテナンス目的のみに利用することを規定する。）、第三者への開示の禁止を契約で明記し、条件違反等契約に違反した場合に損害賠償請求等の法的措置をとる旨の記載を行う等の取組を行う。		213	委託管理に関する規程及び契約書等を閲覧し、長期にわたり徐々に技術等情報がリモートメンテナンス等を行う事業者に蓄積され、管理対象情報を構成することができるような事例にも対応するため、外部委託先等が技術等情報を適切に管理し、かつ、自らの要請に適切に対応できる能力を有するか否かについて事前に確認をしている。蓄積された管理対象情報の目的外利用の禁止、第三者への開示の禁止を契約で明記し、条件違反等契約に違反した場合に損害賠償請求等の法的措置をとる旨の記載を行う等の取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 契約書等	3.実施の結果である成果物を管理している
		3						事業者は、管理対象情報を外部委託先等において取り扱わせる場合において、当該外部委託先等で管理対象情報に関連するもの（例えば、製造委託をした場合の製造設備）に係るメンテナンス等を第三者に行わせる場合については、当該メンテナンス等を通じて管理対象情報が漏えいしていくことも念頭におき、当該メンテナンス等を行う事業者について、当該管理対象情報を提供した者の承認を条件とすること等の適切な管理をする。		214	外部委託契約書の現地調査を実施し、外部委託先等において管理対象情報に関連するものを第三者に行わせる場合については、管理対象情報を提供した者の承認を条件とすること等の適切な管理を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 外部委託契約書	2.実施計画があり、進捗管理している
		4						事業者は、外部委託先等として、当該事業者と内外の他の事業者等とのジョイントベンチャー（以下「JV」という。）を組み、当該JVを構成する企業（以下「JV企業」という。）に管理対象情報を提供する場合については、JVの契約において、当該事業者からの取締役の派遣等コーポレートガバナンスを確実に効かせる措置を講ずる。		215	JVの役員構成等コーポレートガバナンスの状況の現地調査を実施し、外部委託先等として、JV企業に管理対象情報を提供する場合は、JVの契約において、コーポレートガバナンスを確実に効かせる措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 JVの役員構成等コーポレートガバナンスの状況	2.実施計画があり、進捗管理している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		5						事業者は、JV企業における管理対象情報の受入れに関しては、4の取締役の派遣とともに、管理対象情報の受入れについて当該JV企業の取締役会の全会一致の仕組みとすること等により、JV企業側において、組織機能的に、当該事業者からJV企業に管理対象情報が容易に引き渡されないような手順を確立する。		216	JV企業における管理対象情報の取り扱い手順を閲覧し、JV企業における管理対象情報の受入れに関しては、4の取締役の派遣とともに、JV企業側において、組織機能的に、管理対象情報が容易に引き渡されないような手順を定めていることを確認する。	【規定等】 JV企業における管理対象情報の取り扱い手順 【記録やその他の確認対象】	2.実施計画があり、進捗管理している
	第四	1				管理対象情報を継続的かつ適切に管理するための体制の構築等について		事業者は、管理対象情報ごとに、これを取り扱う関係部署の責任及び役割（複数の関係部署にまたがる場合には、これらの分担を含む。）を明確にする。		217	管理対象情報に関する関係部署の組織図、又は所掌が示された社内規程等を閲覧し、管理対象情報ごとに、関係部署の責任及び役割（複数の関係部署にまたがる場合には、これらの分担を含む。）を明確にしていることを確認する。	【規定等】 管理対象情報に関する関係部署の組織図、又は所掌が示された社内規程等 【記録やその他の確認対象】	1.実施している
		2						事業者は、管理対象情報の適切な管理に関する基本的な方針（以下この第四において「方針」という。）を作成する。		218	管理対象情報の管理方針を閲覧し、管理対象情報の適切な管理に関する基本的な方針を作成していることを確認する。	【規定等】 管理対象情報の管理方針 【記録やその他の確認対象】	4.標準的な事項を定義している
		3						事業者は、方針及びこの告示のⅠの第二の2により必要と決定した措置に沿って、管理対象情報の適切な管理に向けた対策（以下この第四において「対策」という。）を作成し、当該対策が確実に実施されていることについての記録をする。		219	管理対象情報の対策の作成状況、実施の記録状況の現地調査を実施し、管理対象情報の適切な管理に向けた対策を作成し、当該対策が確実に実施されていることについての記録をしていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の対策の作成状況、実施の記録状況	4.標準的な事項を定義している
		4						事業者は、管理対象情報が他者から預けられた情報である場合であって、当該管理対象情報に係る方針又は対策を定めたときは、当該他者に当該方針又は対策の内容についての確認をとる。		220	預託管理対象情報に係る方針又は対策を定めたときの預託元への確認状況の現地調査を実施し、預託元に、管理対象情報に係る方針又は対策の内容の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 預託管理対象情報に係る方針又は対策を定めたときの預託元への確認状況	1.実施している
		5						事業者は、方針又は対策について、管理対象情報を取り扱う可能性のある全ての者に周知し、方針に基づき、これらの者（誓約書等を提出していない者に限る。）から情報の取扱いに係る社内規程やマニュアルに従った手続の履行に関する誓約書を取得する。		221	方針又は対策の周知状況、手続の履行に関する誓約書の現地調査を実施し、方針又は対策について、管理対象情報を取り扱う可能性のある全ての者に周知し、方針に基づき、これらの者から情報の取扱いに係る社内規程やマニュアルに従った手続の履行に関する誓約書を取得することを確認する。	【規定等】 【記録やその他の確認対象】 方針又は対策の周知状況、手続の履行に関する誓約書	1.実施している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		6						事業者は、方針、対策又はマニュアルについて、定期的に見直しを実施し、当該方針、対策又はマニュアルを適切、有効かつ妥当なものに維持するための手順を確立する。		222	方針、対策又はマニュアルの見直し手順を閲覧し、方針、対策又はマニュアルについて、定期的に見直しを実施し、当該方針、対策又はマニュアルを適切、有効かつ妥当なものに維持するための手順を定めていることを確認する。	【規定等】 方針、対策又はマニュアルの見直し手順 【記録やその他の確認対象】	7.成果達成のために予測し、運用している
		7						事業者は、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等への対応、内部及び外部からの攻撃に関する監視、測定、評価の結果から教訓を導き出し、その都度管理対象情報を管理するプロセスを継続的に改善する体制を確立する（方針、対策又はマニュアルを作成している場合には、これらを必要に応じて変更することを含む。）。		223	組織的対策に関する規程及び管理対象情報リスク評価結果や経営者によるマネジメントレビューの結果を閲覧し、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等への対応、内部及び外部からの攻撃に関する監視、測定、評価の結果から教訓を導き出し、管理対象情報を管理するプロセスを継続的に改善する体制を確立（方針、対策又はマニュアルを作成している場合には、これらを必要に応じて変更することを含む。）していることを確認する。	【規定等】 組織的対策に関する規程 【記録やその他の確認対象】 管理対象情報リスク評価結果や経営者によるマネジメントレビューの結果	8.予測可能な実施事項を、変化に対応させ、継続的に改善している
		8						事業者の取締役等の経営層（管理対象情報が他者から預けられた情報である場合は、当該預けられた情報を活用し、事業を実施する部門の長を含む。）は、方針、対策又はマニュアルが作成（変更を含む。）された場合はその承認をすることや、管理対象情報の適切な管理の責任の明確化、自らの関与の明示等により、管理対象情報の適切な管理を確立するための取組を行う。		224	方針、対策又はマニュアルの作成・変更の際の経営層の承認状況、または管理責任の明確化や自らの関与の明示等の状況の現地調査を実施し、経営層は、方針、対策又はマニュアルが作成された場合、その承認や、管理対象情報の管理責任の明確化、自らの関与の明示等により、管理対象情報の適切な管理を確立するための取組を行っていることを確認する。 経営層は、方針、対策又はマニュアルが作成・変更された場合はその承認をすることや、管理対象情報の適切な管理の	【規定等】 【記録やその他の確認対象】 方針、対策又はマニュアルの作成・変更の際の経営層の承認状況、または管理責任の明確化や自らの関与の明示等の状況	2.実施計画があり、進捗管理している
		9						管理者は、方針、対策又はマニュアルについて、その責任の範囲において、これらの遵守状況（技術的な遵守状況も含む。）を確認する。		225	方針、対策又はマニュアルの遵守状況に関する管理者の確認状況の現地調査を実施し、管理者は、方針、対策又はマニュアルについて、その責任の範囲において、これらの遵守状況（技術的な遵守状況も含む。）を確認していることを確認する。	【規定等】 【記録やその他の確認対象】 方針、対策又はマニュアルの遵守状況に関する管理者の確認状況	6.実施事項を測定している

別紙2　監査ガイドライン

章	節	項	番		内容				ID	確認内容	確認対象	到達レベル
		10						管理者は、管理対象情報の適切な管理について、定期的に、又は情報の適切な管理に係る状況の重大な変化が生じた場合に監査を実施し、必要に応じた是正措置を講ずるための手順を確立する。この場合において、管理者は、監査の結果を、合理的な期間（管理対象情報が他者から預けられた情報である場合は当該他者が求める期間）、当該結果を施錠することができるロッカー等において、又は暗号技術を用いて電子化し、適切に管理（当該ロッカー等の鍵の管理を含む。）する。		226	監査及び是正措置を講ずるための手順及び監査結果の管理状況の現地調査を実施し、管理者は、管理対象情報の適切な管理について、定期的に、又は情報の適切な管理に係る状況の重大な変化が生じた場合に監査を実施し、必要に応じた是正措置を講ずるための手順を定めていることを確認する。管理者は、監査の結果を合理的な期間、施錠することができるロッカー等において、又は暗号技術を用いて電子化し、適切に管理（当該ロッカー等の鍵の管理を含む。）していることを確認する。	【規定等】 監査及び是正措置を講ずるための手順 【記録やその他の確認対象】 監査結果の管理状況	3.実施の結果である成果物を管理している
		11						事業者は、あらかじめ、自らの事業継続計画、コンティンジェンシープラン等に管理対象情報の漏えいの事故等を位置付け、当該漏えいの事故等が発生した場合の影響の最小化と事業継続のための措置を決定する。		227	事業継続計画を閲覧し、自らの事業継続計画、コンティンジェンシープラン等に管理対象情報の漏えいの事故等を位置付け、当該漏えいの事故等が発生した場合の影響の最小化と事業継続のための措置を決定していることを確認する。	【規定等】 事業継続計画 【記録やその他の確認対象】	2.実施計画があり、進捗管理している
		12						事業者は、管理対象情報の漏えい等の事故等に係る対応により得られた教訓を事業継続計画、コンティンジェンシープラン等に反映させ、継続的に見直していくための手順を確立する。		228	管理対象情報の漏えい等の事故等に係る対応により得られた教訓を事業継続計画、コンティンジェンシープラン等に反映させ、継続的に見直していくための手順を定めていることを確認する。	【規定等】 【記録やその他の確認対象】	7.成果達成のために予測し、運用している

監査ガイドライン－必須項目のみ具体化

共通事項				No.	主たる監査対象	監査技法	監査手続
1	重要情報の識別	重要情報であることを明らかにするために、「関係者外秘」などの表示等を行っている。	I　共通事項 第二　1	1-1	重要情報目録	閲覧（レビュー）	重要情報目録に、重要情報が記載されていることを確認する。
				1-2	重要情報	観察（視察）	重要情報を識別（明らかに）していることを確認する。 （例） ・紙情報の場合 ：その情報が記載された紙に重要情報であること（社外秘等の表示）の記載 ・電子情報の場合 ：ファイル名に重要情報であることの記録 ・試作品、製造装置等の物の場合 ：当該物そのもの又はその保管容器に表示 ・その他の方法 ：目録による管理、電子情報にアクセス可能な者を限定したフォルダにより管理
				1-3	重要情報目録	閲覧（レビュー）	重要情報を識別（明らかに）している記録を、責任者が確認していることを確認する。
2		他者から預けられた重要情報は、当該他者からの意見に基づき管理方法を決定している。	I　共通事項 第二　3	2-1	預託元の要求に沿った記録・保管・報告記録	閲覧（レビュー）	他者から預けられた重要情報の管理方法は、当該他者の意見を聞いて決定することが定められていることを確認する。
				2-2	預託元の要求に沿った記録・保管・報告記録	閲覧（レビュー）	当該他者の要求に応じて、預けられた重要情報の記録・保管・報告を行っていることを確認する。
				2-3	預託元の要求に沿った記録・保管・報告記録	閲覧（レビュー）	当該他者の要求に応じて、預けられた重要情報の記録・保管・報告を行っていることを、責任者が確認していることを確認する。

3	管理者の選任	経営層は、以下の重要情報の管理に関わる責任者を定める。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニングを行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。	Ⅰ　第三１（１）	3-1	組織的対策に関する規程	閲覧（レビュー）	経営層が重要情報について以下を実施する責任者を定めていることを確認する。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。
				3-2	管理対象情報管理責任者選任記録	閲覧（レビュー）	重要情報についての責任者が、(1)-(5)を実施している記録を確認する。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。
				3-3	管理対象情報管理責任者選任記録	閲覧（レビュー）	重要情報についての責任者が、(1)-(5)を実施している記録を経営者が確認していることを確認する。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。

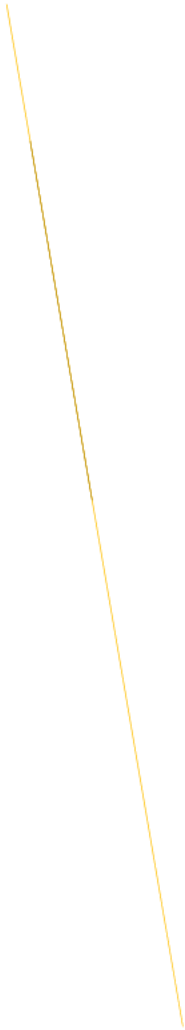
				3-4	管理対象情報管理責任者選任記録	閲覧（レビュー）	重要情報についての責任者が、(2)-(4)の記録の方法を定めていることを確認する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。
				3-5	管理対象情報管理責任者選任記録	閲覧（レビュー）	重要情報についての責任者が、(2)-(4)の記録・保管の方法・期間を定めていることを確認する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。
4		従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識させるようにしている。	Ⅰ　第三１（２）	4-1	社内規程、社内掲示	閲覧（レビュー）	全ての従業員が閲覧可能な状況で、責任者を認識できる方法を定めていることを確認する。
				4-2-1	社内規程、社内掲示	閲覧（レビュー） 観察（視察）	全ての従業員が閲覧可能な状況で、責任者を認識できる社内規程・社内掲示がなされているかを確認する。
				4-2-2	従業員	質問（ヒアリング）	責任者を認識しているかどうかを確認する。
				4-3	責任者を認識できる方法の実施記録	閲覧（レビュー）	全ての従業員が閲覧可能な状況で、責任者を認識できる方法についての実施状況を責任者が確認していることを確認する。
5	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	Ⅰ　第四　柱書き	5-1	管理状況（管理記録）	閲覧（レビュー）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が定められていることを確認する。

				5-2-1	管理状況（管理記録）	閲覧（レビュー） 観察（視察）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを確認する。
				5-2-2	従業員	質問（ヒアリング）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを確認する。
				5-4	管理状況（管理記録）	質問（ヒアリング）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを、責任者が確認していることを確認する。
6	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	Ⅰ　第五　柱書き	6-1	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させる機会について、その対象・内容・方法・期間等を設けていることを確認する。
				6-2	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させていることを確認する。
				6-3	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させていることを、責任者が確認していることを確認する。
7	管理対象情報の漏えいの事故等の発生時等の報告	情報漏えいの事故が発生した場合の報告先を定め、全従業員に対して周知している。	Ⅰ　第六　柱書き	7-1	管理対象情報漏えい事故発生時の報告先の設定状況	閲覧（レビュー）	従業員等が重要情報の漏えいの事故等の発生を発見した場合、事業者内部で情報の取扱いに係る不正を発見した場合等の報告先を、社内規程に定めていることを確認する。

				7-2	周知状況	閲覧（レビュー） 観察（視察）	報告先は、社内に掲示をする等従業員等が認識するようにしていることを確認する。
				7-3	周知状況	閲覧（レビュー）	報告先は、従業員等が認識するようにしていることを責任者が確認していることを確認する。
8	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	Ⅱ　柱書き	8-1	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を定めていることを確認する。
				8-2	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー） 観察（視察）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を実施していることを確認する。
				8-3	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を実施していることを責任者が確認していることを確認する。
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）							
9	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ　柱書き	9-1	保管容器の管理状況	閲覧（レビュー）	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定することを定めている。
				9-2	保管容器	観察（視察）	重要情報の保管には施錠することができる保管容器を用いていることを確認する。
				9-3	保管容器の取扱場所	観察（視察）	重要情報を保管容器から持ち出して利用する際、取り扱う場所を限定していることを確認する。
				9-4	保管容器の管理状況	閲覧（レビュー）	責任者が重要情報の保管の状況や取り扱う場所の限定等の管理状況を確認していることを確認する。
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）							

10	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	Ⅳ　柱書き	10-1	物理的対策に関する規程、又はアクセス制御設定管理簿	閲覧（レビュー）	重要情報が置かれる場所を立入制限区域としてアクセス権者以外の者の立入りを制限することを定めている。
				10-2	立入制限の入退室記録	観察（視察）	立入制限区域の状況、立入制限された場所にはアクセス権者以外の入室がないことを確認する。
				10-3	物理的対策に関する規程、又はアクセス制御設定管理簿	閲覧（レビュー）	立入制限区域の状況、立入制限された場所にはアクセス権者以外の入室がないこと責任者が確認していることを確認する。
11		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	Ⅳ　柱書き	10-1	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施することを定めている。
				10-2	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施していることを確認する。
				10-3	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施していることを責任者が確認していることを確認する。
管理対象情報が電子情報の場合							

12	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	V　柱書き	11-1	IT基盤運用管理に関する規程	閲覧（レビュー）	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を行うことを定めている。
				11-2	クラウド等外部事業者の利用規程	閲覧（レビュー）	重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結することを定めている。
				11-3	可搬式記録媒体の持ち出し管理簿	閲覧（レビュー）	可搬式記録媒体の持ち出しを管理していることを確認する。
				11-4	アクセス権設定状況	観察（視察）	重要情報が事業者の内部のサーバ等で記録されている場合に、情報へのアクセスをアクセス権者に制限する等の必要な措置が実施されていることを確認する。
				11-5	外部事業者の信頼性確認結果（認証取得状況の確認等）	閲覧（レビュー）	重要情報が外部データセンター等で管理する場合には、その管理者の信頼性を確認していることを確認する。
				11-6	外部事業者との秘密保持契約	閲覧（レビュー）	重要情報が外部データセンター等で管理する場合には、秘密保持契約を締結した上で、必要な措置を実施していることを確認する。
				11-7	可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者の信頼性確認結果（認証取得状況の確認等）、外部事業者との秘密保持契約	閲覧（レビュー）	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限の実施状況について責任者が確認していることを確認する。



セルフチェックシート（必須事項のみ）

プルダウンで「○」が選択できます。

	目次	内容	告示番号	チェック
共通事項				
1	重要情報の識別	重要情報であることを明らかにするために、「関係者外秘」などの表示等を行っている。	Ⅰ　共通事項 第二　1	
2		他者から預けられた重要情報は、当該他者からの意見に基づき管理方法を決定している。	Ⅰ　共通事項 第二　3	
3	管理者の選任	経営層は、以下の重要情報の管理に関わる責任者を定める。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニングを行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。	Ⅰ　第三１（１）	
4		従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識させるようにしている。	Ⅰ　第三１（２）	
5	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	Ⅰ　第四　柱書き	
6	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	Ⅰ　第五　柱書き	
7	重要情報の漏えいの事故発生時の報告	情報漏えいの事故が発生した場合の報告先を定め、全従業員に対して周知している。	Ⅰ　第六　柱書き	
8	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	Ⅱ　柱書き	
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）				
9	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ　柱書き	
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）				
10	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	Ⅳ　柱書き	

11		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	Ⅳ　柱書き	
管理対象情報が電子情報の場合				
12	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	Ⅴ　柱書き	

セルフチェックシート＜対策編＞

プルダウンで「○」が選択できます。

	目次	列1	内容	告示番号	チェック
共通事項					
1	重要情報の識別	(1-1)	重要情報であることを明らかにするために、書類やUSBメモリ、電子ファイルなどに対して、「関係者外秘」などの表示等を行っている。	Ⅰ　共通事項 第二　1	
		(1-2)	重要情報であることを明らかにするために、工場の生産ラインのレイアウトや金型等が保管されている場所に、「無断持出し禁止」、「写真撮影禁止」といった掲示を行っている。	Ⅰ　共通事項 第二　1	
2		(2-1)	他者から預けられた重要情報は、当該他者からの意見に基づき管理方法を決定している。	Ⅰ　共通事項 第二　3	
3	管理者の選任	(3-1)	経営層は、以下の重要情報の管理に関わる責任者を定める。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニングを行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。	Ⅰ　第三１（１）	
4		(4-1)	従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識できるようにするために、責任者を社内規程に定める、社内掲示をする等を行っている。	Ⅰ　第三１（２）	
5	管理の基本的な考え方	(5-1)	重要情報を保管するための手順や体制について、マニュアルを作成している。	Ⅰ　第四　柱書き	
		(5-2)	〈識別〉重要情報であることを明らかにするための手順を定めている。	Ⅰ　第四　柱書き	
		(5-3)	〈廃棄〉重要情報を廃棄するための手順を定めている。	Ⅰ　第四　柱書き	
6	重要情報の管理をするためのトレーニング	(6-1)	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るために、以下の内容を含むトレーニングを定期的に実施している。 (1)技術等情報と管理対象情報の違い (2)管理対象情報を適切に管理することの重要性、意識 (3)管理対象情報を含む技術等情報の漏えいとその結果の事例 (4)関係法令の内容 (5)マニュアル、重要情報の適切な管理に係る文書の内容 (6)関係法令等に違反した場合の処分等 (7)重要情報の漏えいの事故等発生時の報告手続 (8)標的型メール等の手口・ウィルス、感染防止の対策、感染した場合の対処の手順	Ⅰ　第五　柱書き	

		(6-2)	アクセス権の設定者に対して、Need to Knowの原則を守ることの重要性や、重要情報の取扱手続、情報の漏えい等の兆候事例等を含むトレーニングを受講させている。		
7	重要情報の漏えいの事故発生時の報告	(7-1)	情報漏えいの事故が発生した場合の報告先を社内規程に定め、全従業員に対して周知している。	Ⅰ　第六　柱書き	
		(7-2)	報告先が情報漏えいの事故報告を受けた場合、証拠の収集により事実関係を確認し、必要な対応についての具体的な手順及び体制を定める。		
8	人的アクセスの制限	(8-1)	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	Ⅱ　柱書き	
		(8-2)	アクセス権を有する者の範囲について、適切な時点で見直している。		
		(8-3)	アクセス権を有する者の責任を明確化している。		
		(8-4)	アクセス権を有する者のアクセス権については、必要がなくなった時点で速やかに失効手続を行っている。		
		(8-5)	アクセス権を有する者との秘密保持契約を交わしている。		
		(8-6)	アクセス権を有する者に対して、重要情報の管理に関する教育を定期的に行っている。		
		(8-7)	アクセス権を有する者が情報管理に関わる規則に違反した際の対応に関する社内規程を定めている。		
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）					
9	保管容器に保管できるものの物理的アクセスの制限	(9-1)	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ　柱書き	
		(9-2)	重要情報の保管容器については施錠管理を行っている。		

		(9-3)	重要情報の保管容器に接近する者の監視（カメラやセンサーの設置）を行っている。		
		(9-4)	重要情報の保管容器から重要情報を持ち出す場合の手順を定めている。		
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）					
10	保管容器に保管が困難な場合等の物理的アクセスの制限	(10-1)	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	Ⅳ 柱書き	
		(10-2)	重要情報が管理される立入制限区域における入退室管理を行っている。		
		(10-3)	重要情報が管理される立入制限区域に不正に侵入する者の監視（カメラやセンサーの設置）を行っている。		
		(10-4)	重要情報が管理される立入制限区域に不正に侵入する者が検知された場合の警備員等の駆け付け体制が整備されている。		
		(10-5)	重要情報が管理される立入制限区域の常時監視を行っている。		
		(10-6)	重要情報が管理される立入制限区域に、情報通信機器等の持込みを禁止している。		
		(10-7)	重要情報の運搬時に、正しく発出されているかどうか、発出した情報が正しく到着しているか確認する。		
11		(11-1)	重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	Ⅳ 柱書き	
管理対象情報が電子情報の場合					
12	電子情報の場合のアクセスの制限等	(12-1)	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	Ⅴ 柱書き	

別紙４　パンフレット

事業者・研究機関の皆様の情報を守る

技術情報管理認証制度

Technology Information Control System

国が策定した基準に基づき、国の認定を受けた機関による情報管理の認証制度です

特 徴

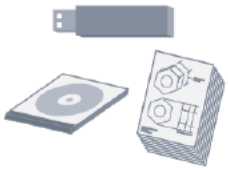
- 組織の「強み」となる情報に絞った管理を認証します
- 専門家の助言を得ながら情報管理を進められます
- 自社の状況や情報の重要性により、簡単な対策から始め、段階的にレベルアップできます

組織の「強み」となる情報の例


金型・試作品


製造装置・製造プロセス情報


研究情報

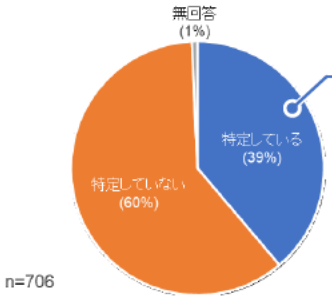

製造設計図・CAD


顧客情報・仕入先情報


業務マニュアル・製造/業務ノウハウ

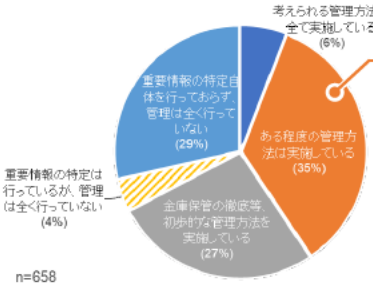
多くの組織では、自組織の強みとなる情報を特定できておらず、情報管理も十分ではありません。

重要情報の特定状況



重要情報を特定しているのは **4割**

情報管理の取組の自己評価



管理しているとの自己評価は **4割**

経済産業省委託調査「中小企業の技術等の情報の管理についての実態調査」（2018年）

情報漏えいにより、取引停止や売上損失を引き起こす場合があり、自組織の強みとなる情報を守ることが必要です。

技術情報管理認証制度

- 情報管理の取組みをマークで対外的に示せます
- 国が主導する制度のため、お客様や取引先の信頼につながります

取組手順

専門家の助言や第三者による認証を受けたい方

国認定の認証機関に申込 ▶ 情報管理に関する専門家の助言※ ▶ 国の基準を満たすか審査 ▶ 認証（国の基準を満たせば）

国の基準に則った対策を自身で進めたい方

セルフチェックシートを確認 ▶ 研修素材を見ながら取組実施 ▶ セルフチェックシート＜対策編＞で自己点検

※ 希望する場合のみ助言を受けられます。
助言を行わない認証機関もありますので、詳細は認証機関にお尋ねください。

認証取得した企業の声

株式会社山本金属製作所

高度なものづくりを支援する事業を行っており、お客様のビジネスに関わる情報を扱うにあたり、情報管理は非常に重要と考える。認証取得は、リテラシーの底上げにも効果的であり、今後も、生産性を阻害することなく、自社の強みを活かした情報管理の仕組みを構築していきたい。

日本金型工業会（株式会社小出製作所）

認証取得をきっかけに、情報管理の取組の一歩を進められた意義は大きい。業界として認証に一足早く取り組むことで、社員1人1人が情報を守る意識を高めていき、近い将来、お客様から情報管理を求められた時にも、その期待に十分に応えていきたい。

最新の認証機関リストやセルフチェックシート、研修素材等コンテンツはこちら

経産省　重要技術マネジメント　検索

別紙：情報管理の取組みをチェックしましょう！

重要な情報を守るために必要な取組みは以下の9項目です。

セルフチェックシート

	目 次	内 容	告示番号
共通事項			
1	重要情報の特定	情報が漏えいした場合に、自身の競争力に重大な影響を与えるような、特別な管理を必要とする重要情報を特定している。	Ⅰ 共通事項 第一 1
2	重要情報の識別	重要情報であることを明らかにするために、「関係者外秘」などの表示等を行っている。	Ⅰ 共通事項 第二 1
		重要情報の価値や形態（モノ／電子情報）に応じて、必要な管理方法を決定している。（他者から預けられた重要情報は、当該他者からの意見に基づく）	Ⅰ 共通事項 第二 2、3
3	管理者の選任	経営層は、以下の重要情報の管理に関わる責任者を定める。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニングを行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。	Ⅰ 第三１ （１）
		従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識させるようにしている。	Ⅰ 第三１ （２）
4	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	Ⅰ 第四 柱書き
5	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	Ⅰ 第五 柱書き
6	重要情報の漏えいの事故発生時の報告	情報漏えいの事故が発生した場合の報告先を定め、全従業員に対して周知している。	Ⅰ 第六 柱書き
7	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	Ⅱ 柱書き
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）			
8-1	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ 柱書き
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）			
8-2	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	Ⅳ 柱書き
		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	Ⅳ 柱書き
管理対象情報が電子情報の場合			
9	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	Ⅴ 柱書き

具体的な取組のための教材もWebサイトから！

詳細についてはウェブサイトへ

経産省　重要技術マネジメント　検索

別紙５　技術情報管理に関する研修素材

技術情報管理認証制度

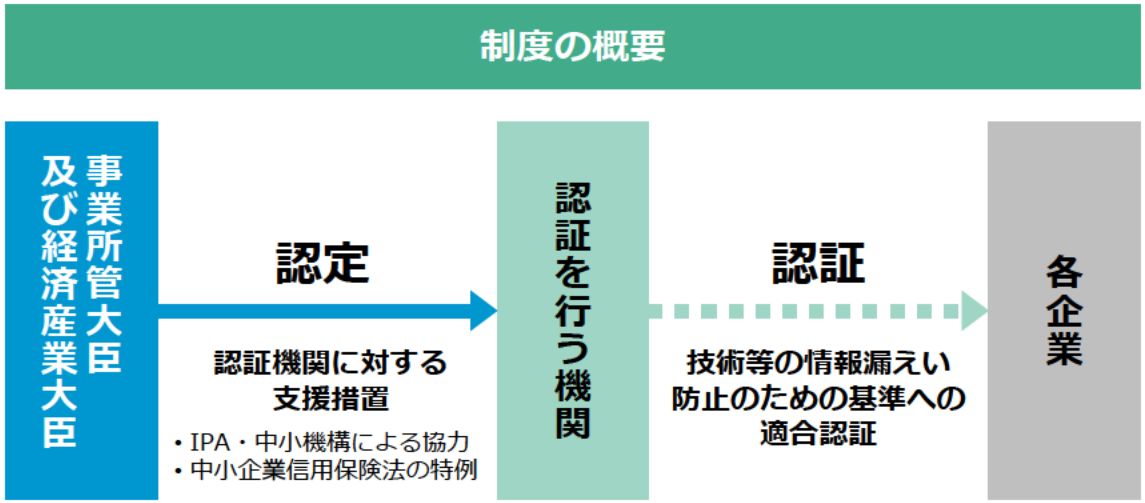
技術情報管理に関する研修素材

【本資料の使い方】

- 本資料は、「技術情報管理認証制度」で定められる基準を元に、技術情報管理に関して、より具体的な管理方法の例や様式サンプルを示したものです。
- 本資料は、以下の方々にご活用いただけます。
  - **情報管理を進める事業者、研究機関等の皆様**
    → 情報管理を進める際の具体的な方法として参照できます。
    → 内部監査を行う際に、管理方法についての妥当性を判断する参考にできます。
  - **助言を行う組織や専門家の皆様**
    → 事業者、研究機関等への助言の参考として活用できます。
- 本資料に記載した対策は「セルフチェックシート＜対策編＞」に一覧化しています。
  対策の確認のために、合わせてご活用ください。

技術情報管理認証制度とは

■ 産業競争力強化法に基づき、事業者（企業や研究機関等）の技術等の情報の管理について、国で示した「守り方」に即して守られているかどうかを、国の認定を受けた機関による認証を受けられる制度（平成30年9月25日開始）



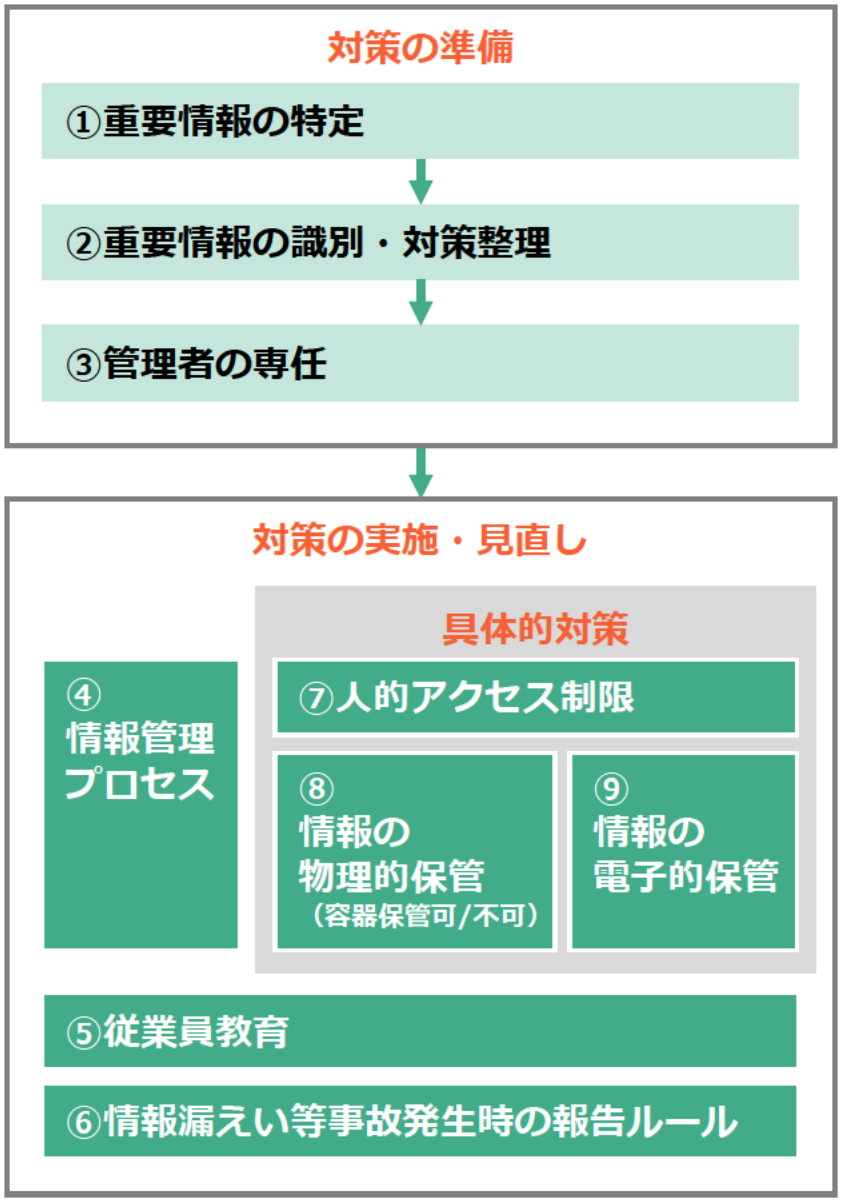
認証制度の特徴

1. 組織の**「強み」となる情報に絞った**管理状況が認証できます
2. **専門家の助言**を得ながら情報管理を進められます
3. 自組織の状況や情報の重要性により、**簡単な対策から**始め、**段階的にレベルアップ**できます

技術情報管理認証制度における情報管理の進め方

- 技術情報管理の取組を進めるには、**対策の準備**として以下を行います。
  - ① **重要情報の特定**
  - ② **重要情報の識別・対策整理**
  - ③ **管理者の責任**
- その後、実際の**対策の実施**として以下を行います。対策は、重要な情報の活用の仕方の変化や、従業員の管理状況などを踏まえて、必要に応じて**見直し**ます。
  - ④ **情報管理プロセス**の策定
  - ⑤ **従業員教育**
  - ⑥ **情報漏えい等事故発生時の報告ルール**の策定
- 情報管理における**具体的な対策**は、情報の態様（物理的な情報か電子情報か、保管容器に保管できるかできないか）を踏まえて以下の事項を実施します。
  - ⑦ **人的アクセス制限**
  - ⑧ **情報の物理的保管**
  - ⑨ **情報の電子的保管**
- 技術情報管理認証制度では、これらの①～⑨を必須の実施事項として定めています。これらを行うことにより、**重要情報の管理を包括的に進める**ことができます。

注）技術情報管理認証制度では、守るべき情報を「管理対象情報」としていますが、本資料ではわかりやすさのために「重要情報」と表現しています。



① 重要情報の特定

- 技術情報管理の取組を進めるには、**重要情報の特定が必要**です。
- 重要情報を特定する際は**経営層も関与し**、以下のポイントを考慮しましょう。
  ポイント1：その情報が漏えいすると、**自社の競争力に重大な影響**を与えますか。
  ポイント2：他社から契約等に基づき預けられた情報等で、その情報が漏えいした場合、**自社の信用や、他社との信頼関係等に重大な影響**を与えますか。
- 特定した情報は、必要に応じて保管場所等を記録した目録を作成し、保管しましょう。

守るべき情報（例）

「守るべき情報」とは、例えば以下のようなものが挙げられます。

目録（例）※1

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			保存期限	登録日
						個人情報	要配慮個人情報	特定個人情報		
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	書類					2016/7/1
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	可搬電子媒体					2016/7/1
❶技術	❷製品設計図	❸現役製品の設計図	❹開発部	❺開発部	❻書類	❼			❾	❿2016/7/1

※1 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン 第3版 付録7 リスク分析シート「台帳記入例」」から抜粋

参考：「営業秘密」と認められる要件※2

「営業秘密管理指針」では、「営業秘密」として法的保護を受けるために必要となる最低限の水準の対策を示しています。

「秘密管理性」を満たすためには、企業の「特定の情報を秘密として管理しようとする意思」が、具体的状況に応じた経済合理的な秘密管理措置によって、従業員に明確に示され、結果として、従業員がその意思を容易に認識できる必要があります。

秘密管理性
①情報に**アクセスできる者を制限**していること
②情報にアクセスした者がそれが**秘密であると認識**できること

有用性
事業活動等に使用されることで、経費の節約、経営効率の改善等に役立つものであること

非公知性
情報の保有者の管理下以外では、一般に入手できないこと

※2 経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）を元に作成

基準該当箇所 Ⅰ 共通事項　第一　適切な管理をする必要がある技術等情報の特定

② 重要情報の識別

- 重要情報は、**他の技術情報と区別して識別できるように表示**しましょう。
- 特定した重要情報については、情報の価値や種類等に応じて、必要な対策を決める必要があります。
- 他社から預けられた情報の場合は、契約内容等他社が求める対策を考慮して、必要な対策を検討する必要があります。

識別のための主な表示方法

紙の場合　　：紙そのものや、ファイル、書類棚等に「社外秘」等を表示し、守る情報であることを表示

電子情報の場合　　：ファイル名やフォルダ名に、守る情報であることを表示

試作品・製造装置の場合：保管容器にラベルを貼る、傍に看板を立てる等、守る情報であることを表示

紙の場合

電子情報の場合

【社外秘】設計図.doc

【関係者限り】試作品イメージ.ppt

モノの場合

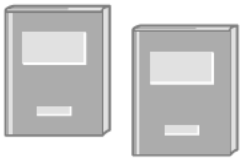
基準該当箇所	Ⅰ 共通事項　　第二　管理対象情報の識別と必要な措置の整理

③ 管理者の選任

- 経営層は、重要情報を守るための**対策推進に責任を持つ管理者を選任**する必要があります。
- 従業員数が多い場合や重要情報が複数の事業部門に関係する場合は、誰が管理者か従業員等が認識できるように、社内規程や社内掲示で周知しましょう。
- 従業員数が少人数の場合は、経営層が管理者を兼務する等、組織の規模に応じて適切な管理者を選任しましょう。

管理者の役割

（1）情報管理の**手順を確立**する。



（2）情報を取り扱う者の制限・管理、**従業員へのトレーニング**を行う。

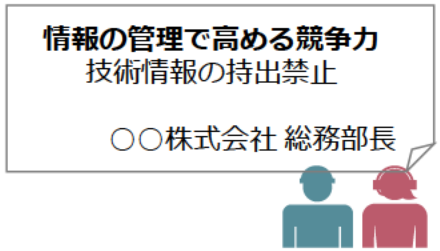
（3）情報漏えい防止**対策を実施**し、その実施状況を把握する。

（4）情報漏えいの兆候・事実の把握に努め、**事象発生時に必要な対応**を行う。

（5）（2）-（4）の**記録を取得し、保管**する。

周知の方法

- 「情報管理規程」にて、情報管理責任者を定め、社内研修にて周知する。
- 社内のポスター・標語で周知する。
- 朝礼等で適時に周知する。



Point
責任者を選任することで、対策を一元的に進めたり、組織としての意思決定を迅速に行うことができます。

基準該当箇所	Ⅰ 共通事項　　第三　管理者の選任

④ 情報管理プロセス（1/3）

- 重要情報を適切に管理するために、**重要情報の作成から廃棄までの情報管理プロセスを作成**する必要があります。
- 重要情報については、管理簿を作成し、情報の持出や複製・廃棄等の状況がわかるようにしましょう。
- さらに、情報管理プロセスは、従業員に周知し、情報管理の取組が習慣化するようにしましょう。

各プロセスの検討内容（例）

プロセス	検討内容例
作成	• 作成された情報が重要情報の場合、識別できるようにする手順を定める。
内容の伝達	• 情報へのアクセスが認められている従業員から、アクセスが認められていない従業員へ情報を伝える際の手順等を定める。
複製	• 重要情報の複製を認める際の基準や承認手順等を定める。
廃棄	• 重要情報を復元不可能な方法（細断や焼却等）で廃棄するための手順等を定める。

管理簿（例）

No.	対象情報	目的	媒体	取扱区分（収集・作成、保管、複製、利用、提供及び廃棄）	保管・持出場所	開始時			終了時			備考
						日付	担当者	承認者	日付	担当者	承認者	
1												
2												
3												
4												
5												
6												

基準該当箇所　Ⅰ 共通事項　　第四　管理対象情報の管理等

④ 情報管理プロセス（2/3）

情報管理規程の記載事項（例）

章	条	項目	内容
第1章 総則	第1条	目的	規程の目的
	第2条	適用範囲	規程の適用範囲
	第3条	定義	「秘密情報」等定義
	第4条	秘密情報の分類	「極秘」等分類
第2章 秘密情報の管理体制	第5条	管理責任者	管理責任者設置
	第6条	情報管理委員会	基準策定の委員会設置
	第7条	指定	秘密情報の指定、アクセス権者の範囲設定 等
	第8条	秘密情報の取扱い	規程及び基準の準拠
第3章 従業員等	第9条	申告	秘密情報取得時の申告
	第10条	秘密保持義務	秘密保持義務
	第11条	誓約書等	秘密保持誓約書の提出
	第12条	退職者	秘密保持契約の遵守 等
	第13条	教育	教育実施
	第14条	監査	監査実施・報告
第4章 社外対応	第15条	秘密情報の開示を伴う契約等	委託時の秘密保持義務
	第16条	第三者の情報の取扱い	秘密かどうかの確認、制約条件の明確化 等
	第17条	外来者・見学	運用手続の定め
第5章 雑則	第18条	罰則	違反時の罰則措置

情報管理基準の記載事項（例）

項目	小項目	内容
1.極秘情報の取扱い	(1)表示	「極秘」「○○限り」の表示
	(2)保管	区別した保管、暗号化・分離保管、施錠
	(3)複製	管理責任者のみ複製可、電子媒体やファイルの複製不可設定
	(4)閲覧	外部者への閲覧不可、要管理責任者許可、閲覧記録
	(5)配布	通し番号付与、会議後回収
	(6)社外への持出し	要管理責任者許可、暗号化・自らの携行・保管庫への保管
	(7)第三者への提供	要管理責任者許可・管理責任者下での開示・管理
	(8)廃棄	管理責任者管理下、読取不可形式での廃棄
2.対外秘情報の取扱い	(1)表示	「対外秘」の表示
	(2)保管	区別した保管、暗号化・分離保管
	(3)複製	複製の原則禁止、完了後の即座回収
	(4)閲覧	外部者への閲覧不可、画面表示注意
	(5)配布	「対外秘」表示、取扱方法説明　等
	(6)社外への持出し	暗号化・自らの携行・保管庫への保管
	(7)第三者への提供	要管理責任者許可・管理責任者下での開示・管理
	(8)廃棄	読取不可形式での廃棄

経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）を元に作成

基準該当箇所　Ⅰ 共通事項　　第四　管理対象情報の管理等

④ 情報管理プロセス（3/3）

情報セキュリティポリシーの記載事項（例）

章	項目
1 組織的対策	1.情報セキュリティのための組織
	2.情報セキュリティ取組みの**監査・点検/点検**
	3.情報セキュリティに関する情報共有
2 人的対策	1.雇用条件
	2.従業員の責務
	3.雇用の終了
	4.情報セキュリティ教育
	5.人材育成
3 情報資産管理	1.情報資産の管理
	2.情報資産の社外持ち出し
	3.媒体の処分
	4.バックアップ
4 アクセス制御及び認証	1.アクセス制御方針
	2.利用者の認証
	3.利用者アカウントの登録
	4.利用者アカウントの管理
	5.パスワードの設定
	6.従業員以外の者に対する利用者アカウントの発行
	7.機器の識別による認証
	8.端末のタイムアウト機能
	9.標準設定等

章	項目
5 物理的対策	1.セキュリティ領域の設定
	2.関連設備の管理
	3.セキュリティ領域内注意事項
	4.搬入物の受け渡し
6 IT機器利用	1.ソフトウェアの利用
	2.IT機器の利用
	3.クリアデスク・クリアスクリーン
	4.インターネットの利用
	5.私有IT機器・電子媒体の利用
	6.標準等
7 IT基盤運用管理	1.管理体制
	2.IT基盤の情報セキュリティ対策
	3.IT基盤の運用
	4.クラウドサービスの導入
	5.脅威や攻撃に関する情報の収集
	6.廃棄・返却・譲渡
	7.IT基盤標準
8 システム開発及び保守	1.新規システム開発・改修
	2.脆弱性への対処
	3.情報システムの開発環境
	4.情報システムの保守
	5.情報システムの変更

章	項目
9 委託管理	1.委託先評価基準
	2.委託先の選定
	3.委託契約の締結
	4.委託先の評価
	5.再委託
10 情報セキュリティインシデント対応ならびに事業継続管理	1.対応体制
	2.情報セキュリティインシデントの影響範囲と対応者
	3.インシデントの連絡及び報告
	4.対応手順
	5.情報セキュリティインシデントによる事業中断と事業継続管理
11 個人番号及び特定個人情報の取り扱い	（個人番号及び特定個人情報の適正な取り扱いに関する基本方針）
	（個人番号及び特定個人情報取扱規程）

情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン 第3版 付録5情報セキュリティ関連規程（サンプル）」を元に作成

基準該当箇所	Ⅰ 共通事項　　第四　管理対象情報の管理等

⑤ 従業員教育

- 重要情報の適切な管理の取組を進めるうえでは、**従業員等に対策を周知し情報管理に対する意識を高めるために、従業員教育を行うことが必要**です。
- 従業員教育の方法としては、社内会議での実施やe-learning等があります。
- 従業員教育は、1回実施するだけではなく、**定期的に実施**することが望ましいです。

全ての従業員等への教育内容（例）

以下のうち必要な項目について教育を実施します。

- 技術等情報（一般的な情報）と重要情報の違い
- 重要情報を適切に管理することの重要性、意識
- 重要情報を含む技術等情報の漏えいとその結果の事例
- 関係法令の内容
- マニュアル、技術等情報の適切な管理に係る文書の内容、関係法令等に違反した場合の処分等
- 重要情報の漏えいの事故等（重要情報の紛失の事故及び改ざん又は破壊がされた事実を含む）が発生したことを発見した場合の報告手続
- 標的型メール等の警戒すべき手口、標的型メール等による情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染を防止するための対策、感染した場合の対処手順

アクセス権を有する者への教育内容（例）

以下のうち必要な項目について教育を実施します。

- Need to Knowの原則（情報は必要のある人のみ（情報へのアクセスは必要な人のみ）に伝え、知る必要のない人に伝えない（情報へのアクセスが必要ではない人にはアクセスを認めない。）という原則）を守ることの重要性（勤務において留意すべき事項を含む。）
- 重要情報の取扱手続の詳細
- 情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）

Point
教育は1年に1回以上定期的に行うことが効果的です。入社時、昇格・昇進の機会の研修や、朝礼など、定期的な会議の時間を使って資料配布、周知・注意喚起を行うことで、従業員の意識を高めることもできます。

基準該当箇所 Ⅰ 共通事項　　第五　管理対象情報の適切な管理をするためのトレーニング

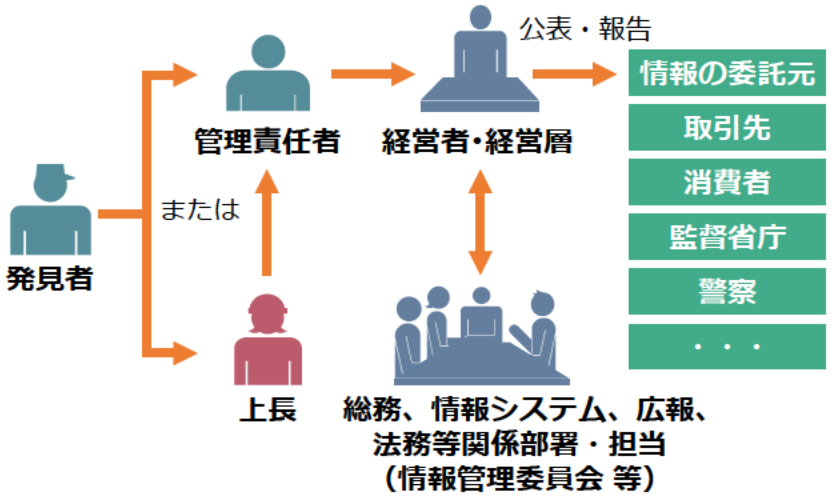
⑥ 情報漏えい等事故発生時の報告ルール（1/3）

- 重要情報の漏えいが疑われるような事故が発生した際に、被害の未然防止や拡大を防ぐために、**事故等発生時の報告ルールを策定し、従業員等に周知**する必要があります。
- 報告ルールには、どのような事象を発見したときに報告してほしいか、報告先は誰か等を整理しましょう。
  - 情報漏えいを完全に防ぐことは不可能です。
    万が一、情報漏えいが起こった場合に、迅速に対応できるように備えておくことが重要です。
  - 対応にあたっては、以下に留意することが必要です。
    - 漏えいの疑いを確実・迅速に把握すること
    - 情報漏えいの損失を最小限に抑えるとともに、原因究明や証拠保全の措置を迅速に実施すること
    - 損失の回復と将来的な再発防止のための責任追及を実施すること

情報漏えい等事故発生時の報告ルート・対応体制

- 兆候を発見した者は、上長または管理責任者に報告します。
- 管理責任者は、速やかに経営者・経営層に報告を行います。
- 対応を行う人員は、組織内での情報拡散を防止するために、必要最小限の人数で構成します。
- 取り扱う内容については秘密保持を徹底します。

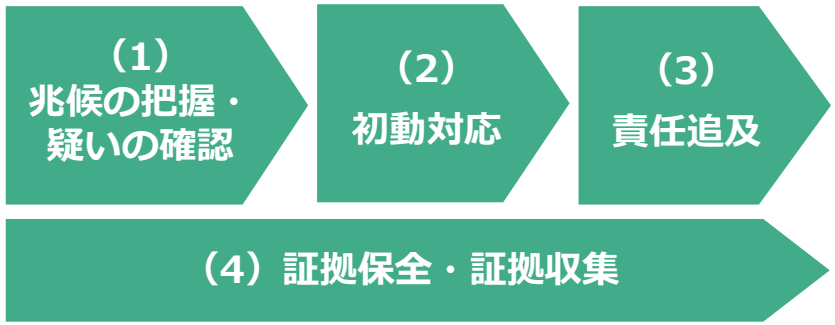
Point
発見者が日頃から上長や管理責任者に報告しやすいような風通しのよい風土を構築しておくことも有効です。



基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑥ 情報漏えい等事故発生時の報告ルール（2/3）

事故発生時の対応フロー



Point

「異変」や「異常」に気づくためには、
「通常」の状態を把握しておかなければなりません。

- 日頃の従業員の業務の様子
  （業務時間、PCや情報の利用状況、業務場所等）
- 取引先とのやり取り（情報照会等の要求 等）
- 物品（機器、メディア 等）の設置場所

従業員からの報告や面談等を通じて上長や管理責任者が認識しておくことが必要です。

（1）兆候の把握、疑いの確認

- 情報漏えいの兆候が報告された場合、その状況が正しいかどうかの確認を行います。

（2）初動対応

- 現状を正しく把握します。（時系列で、いつ、誰、何、どのようにを把握）
- 自社、取引先、情報が漏えいした顧客、一般消費者等の関係者に対して、どのような被害・影響があるかを検証します。
- 被害防止・最小化の観点で、更なる拡散の防止、法律に基づく監督省庁等への報告、対外公表等を行います。

（3）責任追及

- 情報漏えいの際には、不正競争防止法上の営業秘密侵害罪（同法第21条等）、不正アクセス行為の禁止等に関する法律違反の罪（同法第１１条等）、電子計算機使用詐欺罪（刑法第246条の2）、背任罪（同法第247条）、横領罪（同法第252条）等に該当する可能性があることから、都道府県警察への相談も検討します。

（4）証拠保全・証拠収集

- 各過程において、漏えいの事実を裏付ける証拠を収集します。

経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）を元に作成

基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑥ 情報漏えい等事故発生時の報告ルール（3/3）

報告を求める事象（例）

対象	兆候
従業員等の兆候	• （業務上の必要性の有無に関わらず）秘密情報を保管しているサーバーや記録媒体へのアクセス回数の大幅な増加 • 業務上必要性のないアクセス行為 • 業務量に比べて異様に長い残業時間や不必要な休日出勤 （残業中・休日中に情報漏えいの準備等を行う従業者が多いことから兆候となり得る） • 業務量としては余裕がある中での休暇取得の拒否 （休暇中のPCチェック等による発覚を恐れるため兆候となり得る） • 経済的、社会的に極めて不審な言動
退職者等の兆候	• 退職前の社内トラブルの存在 • 在職時の他社との関係 • 同僚内の会話やＯＢ会等で話題になっている、元従業員の不審な言動 • 退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった
取引先の兆候	• 取引先からの突然の取引の打切り • インターネット上での取引先に関する噂 • 取引先からの、取引内容との関係では必ずしも必要でないはずの業務資料のリクエストや通常の取引に比べて異様に詳細な情報照会 • 自社の秘密情報と関連する取引先企業の商品の品質の急激な向上 • 自社の秘密情報と関連する分野での取引先の顧客・シェアの急拡大
外部者の兆候	• 自社における事件の発生 自社会議室における偵察機器（盗聴器など）の発見 • 競合他社等での秘密情報漏えい、不法侵入等の事案発生（類似の技術を持つ自社の情報についても狙われやすいと考えられるため兆候となり得る） • ウィルス対策ソフト、セキュリティ対策機器による警報 • 自社の秘密情報それ自体ではないが、それと不可分一体のはずの情報が漏えいしていること • 電話、メール等を受信した関係者からの通報

経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）より抜粋

基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑦ 人的アクセス制限（1/4）

- 重要情報を適切に管理するために、必要な人のみが重要情報にアクセスできるように、**適切なアクセス権の設定**を行いましょう。
- **アクセス権の設定状況は、定期的に確認・見直し**を行う必要があります。特に、従業員の異動時や退職時等は気を付けましょう。
- また、従業員による情報漏えいを防ぐために、守秘義務の厳守や退職後に業務中に知り得た情報を不正に使用しないよう、秘密保持の誓約書を締結することも有効です。

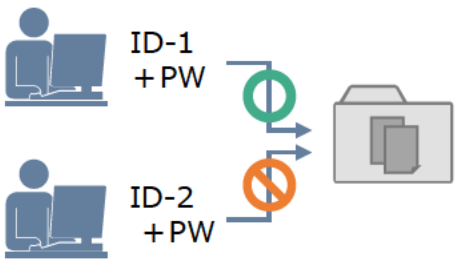
アクセス権の設定に関する考え方

- アクセス権を設定された者のみが重要情報を取り扱い得ることを明らかにします。
- アクセス権を設定する際には、以下を考慮します。
  - Need to Knowの原則に照らし、必要最小限の範囲となっているか否か
  - 情報の取扱いに係る社内規程への違反履歴
  - 退職、派遣元への復帰等、近い将来に自組織の直接の管理対象から外れる可能性
- アクセス権設定を一人の管理者が行っている場合には、アクセス権の設定に係る監査を他の者が行う仕組みを設けます。

Point
IDの登録作業は、複数の管理者が行うことで、適正な実施を確保できます。

アクセス権の管理方法

- アクセス権を設定された者の範囲は、定期的に、あるいはアクセス権の設定が必要となった業務の終了時点等の適切な時点で見直します。
- 退職等により必要のなくなった従業員等のアクセス権は、直ちに失効させます。
- アクセス権を設定された者の氏名、役職、アクセス権の設定年月日、トレーニングの受講の状況等、アクセス権を設定された者の状況を記録した管理簿を作成し、保管します。



従業員等に対して情報システム上のIDを付与し、そのIDを認証するパスワード（PW）等を設定します。

アクセス権を設定された者だけが、許可された電子データ等にアクセスできるように、IDを登録します。

⑦ 人的アクセス制限（2/4）

従業員の秘密保持について

- アクセス権を設定された者としての責任を明確にするため、アクセス権を設定された者から、以下のうち必要な事項を確保する秘密保持契約または誓約書を得ます。
  - 第三者に対する守秘義務を厳守すること。
  - アクセス権の設定の解除の後（退職後も含む） も アクセス権が設定されている間に知り得た重要情報について、公知になったものを除き、不正に開示したり、使用しないこと。
  - マニュアルその情報の取扱いに関する社内規程を遵守すること。
  - 重要情報の漏えいにつがなり得る事象等を発見した場合、指定された者に報告を行うとともに、重要情報の漏えいの事故等が発生した場合に必要な対応を行うこと。
  - 重要情報へのアクセスのログ等をアクセス権の設定を行った者等から確認されること。
  - 重要情報に接する必要がなくなった場合は、速やかに返却等の対応が求められること。

Point

従業員から秘密保持誓約書を得るタイミングは、入社・採用時、退職・契約終了時、在職中の取扱う情報が変更されるタイミング（昇進時等）が考えられますが、退職時にトラブル等が発生している場合は誓約書を得ることが難しいことがあります。
入社時に退職時も含めた誓約書を取得するとともに、在職中に研修と合わせる等して定期的に誓約を取得することで、適時な取得が可能になるとともに、従業員の意識を高める効果も期待できます。

⑦ 人的アクセス制限（3/4）

従業員の秘密保持契約・誓約書（例）　<入社時>

秘密保持誓約書

この度、私は、貴社に採用されるにあたり、下記事項を遵守することを誓約いたします。

記

第１条（在職時の秘密保持）
貴社就業規則及び貴社情報管理規程を遵守し、次に示される貴社の秘密情報について、貴社の許可なく、不正に開示又は不正に使用しないことを約束いたします。
①製品開発に関する技術資料、製造原価及び販売における価格決定等
の貴社製品に関する情報
②（以下略）

第２条（退職後の秘密保持）
前条各号の秘密情報については、貴社を退職した後においても、不正に開示又は不正に使用しないことを約束いたします。退職時に、貴社との間で秘密保持契約を締結することに同意いたします。

第３条（損害賠償）
前二条に違反して、第一条各号の秘密情報を不正に開示又は不正に使用した場合、法的な責任を負担するものであることを確認し、これにより貴社が被った一切の被害を賠償することを約束いたします。

第４条（第三者の秘密情報）
１．第三者の秘密情報を含んだ媒体を一切保有しておらず、また今後も保有しないことを約束いたします。
２．貴社の業務に従事するにあたり、第三者が保有するあらゆる秘密情報を、当該第三者の事前の書面による承諾なくして貴社に開示し、又は使用若しくは出願（以下「使用等」という。）させない、貴社が使用等するように仕向けない、又は貴社が使用等しているとみなされるような行為を貴社にとらせないことを約束いたします。

第５条（第三者に対する守秘義務等の遵守）
貴社に入社する前に第三者に対して守秘義務又は競業避止義務を負っている場合は、必要な都度その旨を上司に報告し、当該守秘義務及び競業避止義務を守ることを約束いたします。

以上

平成____年____月____日
株式会社_____
代表取締役社長_____ 殿

住 所_____
氏 名_____ 印

経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）より抜粋

基準該当箇所　Ⅱ　管理対象情報への人的アクセスの制限

⑦ 人的アクセス制限（4/4）

従業員以外（訪問者等）の秘密保持について

- アクセス権を設定された者以外の従業員等や、従業員等以外の者等（訪問者：（例）立入制限区域にある製造設備の見学者等）のように一時的なアクセスについて、以下の対応を行います。
  - 訪問者がNeed to Knowの原則を満たすものであるかを評価する。
  - 訪問者から、その訪問により得られた重要情報を第三者等に開示しないこと等を誓約する書面を得る。
  - アクセス権を設定された者の立会い等、重要情報を保護するために適切な措置を講ずる。

従業員以外（訪問者等）の秘密保持誓約書（例）<工場見学時>

秘密保持誓約書

____年____月____日

_____株式会社
_____殿

（所属/住所・名前）

この度、__年__月__日、貴社____工場を見学させていただくにあたり、私は、貴社が秘密である旨を明示し開示した一切の情報（以下「秘密情報」といいます。）について、厳に秘密を保持するものとし、第三者に秘密情報を開示しません。

以上

左：経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて」（平成28年2月）を元に作成

⑧ 情報の物理的保管（1/2）

- 重要情報が保管容器（金庫、キャビネット等）で保管できる（紙情報や試作品等）の場合、施錠して保管できる**保管容器を用いて保管し、物理的アクセスを制限**しましょう。
  - 鍵の適切な管理（鍵の貸出し管理簿作成、文字盤鍵の鍵番号の年1回以上変更　等）
- 保管容器から**情報を持ち出して取扱う場合や運搬する場合は、取扱のルール**を決めて、運用しましょう。
  - 運搬時の封筒の封印、受領証の受け取り、外部事業者との秘密保持契約締結　等

保管容器に求められる要件

- 施錠することができる保管容器を用いる。
- 保管容器の鍵の管理を行う。
  - 差込み式の鍵は、鍵の貸出し
  - 文字盤鍵の場合は、鍵番号の設定
- 鍵の管理手順を定める。
- 鍵の貸出し、鍵番号の共有を管理するための管理簿を作成し、保管する。
- 文字盤鍵の鍵番号は、年に1回以上変更する。
- 文字盤鍵の鍵番号は、以下のような事象が生じた都度、変更する。
  - 購入後の備え付け時、使用場所変更時
  - 管理者やアクセス権者が替わった場合
  - 鍵番号の漏えい（または恐れがある）時

保管容器の取り扱い場所

- 重要情報を保管容器から持ち出して、取扱いをする場所を限定するための手順を定める。

保管容器の運搬

- 重要情報を保管容器から持ち出し運搬することを、アクセス権を設定された者に限定するための手順を定める。
- 運搬時、重要情報を外部から見ることができず、運搬中の不正が確認できるようにするための手順を定める。（封筒に入れ封印する等）
- 重要情報の運搬後、受領証を受け取り、管理者に提出する手順を定める。
- 重要情報の運搬時、情報を引き渡した者と引き渡された者が相互に内容についての確認を行うための手順を定める。
- 運搬を信頼できる輸送機関又は運搬事業者に行わせる手順を定める。
- 運搬を行う外部事業者の情報管理について評価し、秘密保持契約を締結しているかを確認するための手順を定める。

基準該当箇所	
	Ⅲ　管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等 Ⅳ　管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等

⑧ 情報の物理的保管（2/2）

■ 製造装置等保管容器に保管できない場合は、**製造装置等を設置している場所の立ち入り制限区域にする等、物理的アクセスを制限**しましょう。
- 入退口の施錠管理、受付簿による立入状況の記録、立入者として視認可能な標識の着用　等

立ち入り制限区域について

- 壁等の物理的な境界で他の区域と区分することができる区域であり、全ての入退室口を施錠（差込み式の鍵、文字盤鍵、 キーパッド式の鍵、認証システム等）できる区域を立入制限区域として設定する。
- 立入制限区域の入退室口を、原則として業務時間中のみ開錠する。
- 立入制限区域への全ての者の立入りの状況を記録し、保管する。（鍵の管理簿の作成、受付簿の管理、IDによる認証の導入、作業者以外の者による同行・確認等）

<より高いレベルで管理を行う場合>

- 立入制限区域への不審者の侵入に関して、視認性を高める。（赤外線警報装置、セキュリティカメラ等の警備システムの導入等）
- 立入制限区域の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。
- 警備員等がモニターにより立入制限区域及びその周辺を常時監視する体制を確保する。
- 警備員等により立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保する。

立ち入り制限区域への立ち入りについて

- 全ての立入者について、他の者から視認できるよう、立ち入ることが許されていることがわかる標識の着用を求める。
- カメラ、携帯型の情報通信機器等の持込みを原則として禁止する。持ち込む場合には、予め管理者の承認を得る手順を定める。
- 立入制限区域内の製造設備等の重要情報は、持ち出せないようワイヤ等で固定する。

運搬について

- 重要情報の運搬時に、正しく発出されているかどうか、発出した情報が正しく到着しているか確認する。

基準該当箇所	
	Ⅲ　管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等
	Ⅳ　管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等

⑨ 情報の電子的保管

- 重要情報が電子情報の場合は、**パソコン等の可搬式記録媒体の持出を管理**しましょう。
- 電子情報を自社のサーバ等で保管する場合は、**IDやパスワード等による認証を行い、適切なアクセス制限を行い、必要な対策を実施**し、重要情報を適切に管理しましょう。
- 自社サーバではなくクラウドやデータセンターに保管している場合は、**委託先事業者と秘密保持契約を締結した上で、自社で行える対策を実施**し、重要情報を適切に管理しましょう。

電子情報の保管について

- 管理対象情報が電子情報である場合には、可搬式記録媒体（PC、USBメモリ等）の持ち出しを管理する。
- 内部サーバ等で記録している場合は、ID・パスワード等によりアクセス制限を行い、必要な対策を行う。

<外部環境を利用している場合>

- クラウド等外部サーバ等で記録している場合は、クラウド事業者の信頼性を確認する。
- データセンターに自らのサーバ等を設置している場合は、データセンターの信頼性を確認する。
- クラウド事業者やデータセンター事業者との間で秘密保持契約を締結する。
- クラウドやデータセンターの対策を踏まえ、自組織で必要な情報管理を実施する。

電子情報に対する主な対策について

- セキュリティに配慮した利用者の操作手順書の作成
- ファイアウォールの導入
- ログの取得・保存
- 不正アクセス検知時の対応手順の策定
- 脆弱性情報管理
- システム構成要素の管理簿の作成・管理
- ウィルス対策ソフトウェア等の導入・定期的な更新
- ソフトウェアの導入管理
- バックアップ
- アクセス権管理（一意のID、適切な利用権限、パスワード管理）
- クリアデスク
- 持ち出し手順の作成
- 外部委託管理

基準該当箇所	Ⅴ　管理対象情報が電子情報である場合のアクセスの制限等