製造産業における重要技術の情報の適切な管理に関する

基準となる考え方の指針（ガイドライン）

（初版）

平成２９年４月

経済産業省製造産業局

目次

はじめに　－本ガイドラインの目的と考え方について－

グローバルな競争が進む中で、我が国製造産業が保有する技術の適切なマネジメントは、我が国の産業競争力の維持・強化の観点から極めて重要であり、平成 29 年 3 月の産業構造審議会製造産業分科会においても、今後の製造産業政策の重要課題の一つとして、民間企業において保有する重要な技術の情報の管理を適切に実施していくための考え方が必要であるとの意見もなされた。

また、平成 29 年 1 月から 3 月にかけて開かれた民間企業の保有する技術の情報の守り方についての議論を行った外部有識者による委員会（「我が国の技術情報保全の在り方に関する検討委員会」）においては、民間企業における情報管理は、「活用管理」と「守秘管理」を含む考え方であることから、「守る」ことだけを考慮することなくその活用にも配慮すること、「守秘管理」を強化した場合の民間企業におけるコスト負担を考慮すること、等の意見も出された。

これらの外部有識者の意見等を踏まえ、経済産業省製造産業局として、民間企業におけるオープン＆クローズ戦略として想定されるビジネスの態様等を考慮しつつ、製造産業が保有する技術の情報のうち、クローズ領域においてノウハウ等として守るべきものについての一層適切な管理を図るべく、技術の情報の守り方の基準となる考え方を整理したものが、「製造産業における重要技術の情報の適切な管理に関する基準となる考え方の指針（ガイドライン）」である。

経済産業省製造産業局としては、本ガイドラインを、平成 29 年度の一部の研究開発事業における成果等の技術の情報について適切に管理を行うためのものとして、試行的に研究開発事業に援用すること等を通じて、その効果と妥当性等について検証を行いつつ、随時見直しを行う。

なお、本ガイドラインは、技術の情報の適切な管理において留意すべき最低限の事項を記載しているものであり、民間企業において、本ガイドラインに記載された事項を参照しつつ、情報の管理に関する追加的な措置の検討や実施など自主的な取組が行われることを期待するものである。

平成２９年４月　経済産業省製造産業局

１．適切な管理を行うべき技術の情報

本ガイドラインの対象として適切に管理を行うべき情報は、秘密情報の保護ハンドブック（以下「ハンドブック」という。）の秘密情報となる技術情報のうち、民間企業において、ノウハウ等として管理を的確に実施することが必要な情報とする。

（１）重要技術としての評価

民間企業においては、例えば、以下のメルクマールを参考として、個別に技術を評価・判断し、特に民間企業として、その情報の適切な管理を行うべき技術を特定する（以下特定された技術を「重要技術」という。）。

ⅰ）製品を分析するだけでは模倣が難しく、技術流出による影響が大きい重要技術に関する情報

ⅱ）その重要技術に関する情報を権利化した場合でも、権利侵害の探知や立証が難しいもの

この技術の評価・判断に当たっては、ハンドブックにおける保有する情報の把握と評価のプロセスを参照し、例えば研究開発の進展に応じて行うなど適切なタイミングで民間企業において行うことを推奨する。

（２）適切に管理を行う重要技術の情報について

１．（１）で特定された重要技術を構成する情報については、紙媒体若しくは電子媒体に記載若しくは記録され、試作品若しくは商品に化体し、又は製造工程そのものを構成する設備の組合せに化体したものなど様々な態様として考えられるが、本ガイドラインでは、例えば、紙媒体若しくは電子媒体に記載若しくは記録がされた情報、試作品に化体した情報又は製造工程（使用する装置や一連の製造プロセスにより構成されるもの及び製造ノウハウなど）の情報を対象とする。

上記の考え方に照らせば、例えば、外部に販売する製品等に化体した重要技術の情報については、本ガイドラインに則して適切な管理を行う対象とする情報には含まれないことになるが、これらの情報については、製造工程等の情報の適切な管理を行いつつ、リバースエンジニアリング対策やブラックボックス化を通じて、重要技術の情報が不用意に流出しないよう適切な措置を講じていくことを推奨する。

２．重要技術に係るリストの作成と重要技術の情報である旨の表示（マーキング）と管理

重要技術の情報を保有する民間企業の従業員等[1]において、その情報が適切な管理の対象となるものあると認識されないことにより情報が意図せぬ形で外部に流出してしまう事態を防ぐため、重要技術に係るリストの作成及び重要技術の情報そのものに表示（マーキング）を付すことで、当該情報を保有する民間企業の従業員等において、識別が可能なようにすることを通じて、管理を行うものとする。

（１）重要技術に係るリストの作成

民間企業においては、重要技術の目録（リスト）を作成し、民間企業において技術の情報の評価・整理がされる毎に、当該リストに、重要技術の名称、リストへの登載日等の記載（記録）を行うものとする。

重要技術の名称等についてのリストを、民間企業において別途作成している場合は、当該リストを活用・利用することができる。

なお、重要技術に係るリストは、重要技術の情報そのものとして本ガイドラインに則した管理を行うことが求められるものではないが、当該リストは、営業秘密の一部として確実に管理を行うものとする。

（２）重要技術の情報の表示（マーキング）と管理

重要技術の情報として適切な管理の対象であることを明らかにするために、民間企業では、重要技術の情報を作成した時点で当該重要技術の情報そのものに重要技術の情報である旨の表示をするものとする（例えば、紙であれば紙媒体に記載し、電子情報であればファイル名に記録する。また、製造工程であれば、その製造工程を構成する製造設備が設置された時点で、建屋の入口への表示を行う。）。

重要技術である旨の表示については、「部外秘」「社外秘」など民間企業の判断により様々な文言を用いることが考えられるが、重要技術の情報については、表示を見た者が、その情報が重要技術の情報であることを容易に識別できるよう、可能な限り統一的な表記を用いるものとする。

---

[1] 従業員等とは、典型的には役員や自社が雇用する従業員が該当するが、自社内の研修生や派遣労働者、委託先従業員であって自社内において勤務する者なども含む。

重要技術の情報を保有する民間企業においては、重要技術の情報の作成（評価・整理によるものを含む。以下「作成等」という。）、処理、保管（保存）、手交（送信）又は廃棄（削除）のプロセスを、このガイドラインに則して適切に管理をすることができるように手順を定めるものとする。

なお、重要技術の情報についてその活用と管理を適切に行うために、段階を分けて分類し、段階別に当該重要技術の情報にアクセスできる者を細かく管理することを推奨する。

３．重要技術の情報の管理の責任者

重要技術の情報を保有する民間企業は、このガイドラインに則して重要技術の情報の管理を的確に進めていくための責任者として重要技術情報管理責任者を置くものとし、当該重要技術情報管理責任者には、部門の長等を任命するものとする[2]。

また、重要技術の情報を保有する民間企業では、全ての従業員等が、それぞれの重要技術の情報毎に、誰が管理の責任を有しているかを認識できるように、社内規程等に重要技術情報管理責任者である者の役職等を定めるものとする。

重要情報技術管理責任者については、以下のことを確実に行うための権限と責任を有することを社内規程等に定めることを推奨する。

- 重要技術に係るリストを作成し、管理すること
- 重要技術の情報の作成等から廃棄まで適切に管理するための手順を確立させること
- 従業員等に対するアクセス権の管理を行うとともに、アクセス権の設定を行った従業員等に係る管理名簿を作成、管理すること
- 保管容器、立入制限区域の鍵、暗証番号の設定など重要技術の情報の管理に必要な措置を実施すること
- アクセス権の設定を行った者へのトレーニングを行うこと
- 重要技術の情報の管理に関する脅威又は重要技術の情報の漏洩等の兆候の把握に努めるとともに、脅威、漏洩等があった場合の必要な措置を講じること
- 上記の事項の実施に必要な手順・手続を定めること
- 上記の実施状況を含む重要技術の情報の管理に関する状況について、定期的（少なくとも１年に１度以上）に、社内の情報保護に関する総括的な責任者（又は重要技術情報管理責任者の上司たる取締役等）に対して報告を行うこと

[2] 重要技術情報管理責任者は、重要技術の情報の的確な管理が主要なミッションであるため、重要技術情報管理責任者以外にも、重要技術の情報以外の顧客情報等の管理を含めた各民間企業における情報保護に関する総括的な責任者を置くものとする。

４．重要技術の情報への接近防御

重要技術の情報を保有する民間企業は、重要技術の情報にアクセスできる人を制限するとともに、当該情報について、適切な保管容器等で保管・保存することや、原則として、重要技術の情報にアクセスできる人しか立ち入ることができない区域での取扱いをさせることを通じて、重要技術の情報の適切な管理を行うものとする。

（１）重要技術の情報への人的アクセスの制限

①　従業員等へのアクセス権の設定に当たっての考慮

重要技術の情報を保有する民間企業は、社内規程等により、当該重要技術の情報へのアクセスを認めた者に限り、当該重要技術の情報の取扱いを行い得ることを明らかにするものとする。

それぞれの民間企業において、当該民間企業において保有する重要技術の情報へのアクセスができる者の設定を行う際は、以下の点を考慮して設定するものとする（以下アクセス権を設定された者を「アクセス権者」という。）。

ⅰ）Need to Know 原則[3]に照らし、グローバル競争が進む中での国外へ技術の流出リスクなどを考慮しつつ、必要最小限の範囲となっているか否か

ⅱ）民間企業内における情報の取扱いの非違の履歴

また、民間企業において、アクセス権を設定する際は、従業員等の退職、研修員の派遣元への復帰など近い将来において重要技術の情報を保有する民間企業の直接の管理の対象から外れる可能性を確実に考慮するとともに、個人情報保護、個人識別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、飲酒トラブル、信用状態、犯罪記録等のレビューをすることを推奨する。

②　アクセス権の設定の権限

民間企業における従業員等に対するアクセス権の設定は、重要技術情報管理責任者若しくは民間企業内の情報保護に関する総括責任者など当該民間企業における秘密情報の取扱いについての責任を有する者又はこれらの者による委任を受けた者が行うものとする。

---

[3] 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。）、との考え方。

アクセス権の設定は、重要技術の情報を保有する民間企業において統一的な判断基準（考え方）の下で行うこととし、全ての重要技術の情報へのアクセス権の設定を一人で行っている場合については、当該アクセス権の設定に係る監査を、当該アクセス権の設定の権限を有する者の上司等が行うものとする。

なお、重要技術情報管理責任者以外の者がアクセス権の設定を行っている場合には、当該重要技術情報管理責任者以外の者は、そのアクセス権を設定した重要技術の情報の重要技術情報管理責任者に、アクセス権の設定をした者の氏名等必要な事項を連絡するものとする。

③　アクセス権の管理

重要技術情報管理責任者は、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）で見直すこととし、必要のなくなった従業員等のアクセス権の停止を適宜に行うなど、その適切な管理を行うものとする。

この管理を確実なものとするため、重要技術情報管理責任者は、アクセス権者の管理名簿（氏名、役職、アクセス権設定日時、アクセス権の範囲、４．（１）④に定める誓約書等の提出日、トレーニング受講歴がわかるもの。）を作成するものとする。ただし、既に、当該民間企業において、上記の管理名簿の記載事項を満たすリストを作成している場合には、当該リストをもって替えることができるものとする。

④　アクセス権者と民間企業との間の秘密保持等に関する担保

重要技術の情報を保有する民間企業は、４．（１）①のアクセス権の設定におけるプロセスを経て、従業員等にアクセス権を設定した際には、重要技術の情報の管理に係る従業員等としての責任を明確にするため、アクセス権者に対して秘密保持の誓約書の提出を求め、又は秘密保持契約を締結するものとする（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。）。

この誓約書等は、少なくとも以下の点の誓約・同意を求める内容を含めるものとする。

- 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重要技術の情報について、公知になったものを除き、不正に開示・使用しないこと
- 第三者に対する守秘義務を厳守すること

- 情報の漏洩につがなり得る事象等を発見した場合に適切に報告を行うとともに、情報の漏洩等の事故が発生した場合に適切な措置を講ずること
- 重要技術の情報へのアクセスのログ等をアクセス権の設定の行った者等から確認されること

⑤　その他の場合のアクセス権の設定

重要技術の情報を保有する民間企業のアクセス権者以外の従業員等や外部関係者等における重要技術の情報へのアクセス、例えば、見学のように一時的な訪問者によるアクセスついては、当該訪問者につき need to know 原則を満たすことを重要技術の情報を保有する民間企業の重要技術情報管理責任者で評価し、当該訪問者から重要技術の情報を第三者等に開示しないことを誓約する書面を得て、アクセス権者の立会いなど重要技術の情報の保護に関する適切な措置を講じた上で認めるものとする。

（２）重要技術の情報への物理的アクセスの制限

①　保管容器（金庫）

重要技術の情報を保管する保管容器については、三段式文字盤鍵のかかる金庫若しくは鋼鉄製の箱又はこれらに準じる強度を有するもの[4]とし、原則として、当該保管容器は、立入制限区域内に置くものとする。

三段式文字盤鍵の鍵番号は、重要技術情報管理責任者又はその委任を受けた者（アクセス権者に限る。以下この４．（２）①②において同じ。）が設定することとし、その鍵番号については、少なくとも１年に１度変更することを推奨する。
なお、鍵番号の共有は、アクセス権者に限るものとし、鍵番号を記したメモ等について、他の者の目につく場所には置かないことをアクセス権者に徹底するものとする[5]。

また、保管容器のある場所が立入制限区域の外の場合については、視認性を確保するため、セキュリティカメラの設置等を推奨する。

特に守秘性の高い重要技術の情報の保管容器からの持出しについては、重要

[4] 「これらに準じる強度を有する」ものか否かについては、重要技術情報管理責任者が判断するものとする。
[5] 「これらに準じる強度を有するもの」として物理的な鍵を用いる場合には、４．（２）②の立入制限区域の施錠に係る鍵の取扱いに準じて管理を行うものとする。

技術情報管理責任者が事後的に確認することが可能なように、持出しに係る事実関係（持ち出した者、持出し日時、返却日時等）の記録を作成するものとする。

② 立入制限区域

保管容器における保管が困難な場合等として、以下 ⅰ、ⅱに該当する場合は、原則として、アクセス権者のみの立入りが認められる区域（立入制限区域）において、当該重要技術の情報を保管し、又は取り扱うものとする。

ⅰ）重要技術の情報の化体したものの態様、サイズ等から保管容器での保管が困難な場合

ⅱ）ものの態様、サイズは保管容器で保管可能であるが、業務上、保管容器から出して使うことが必要な場合

立入制限区域への立入りについては、重要技術情報管理責任者が事後的に確認することが可能なように、立入制限区域への全ての立入者に係る事実関係（氏名、日時、入退室時間等）の記録を作成するものとする。

立入制限区域は、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として、その区域の外と接触する全ての入退室口を施錠可能とした上で、原則として業務時間のみ解錠するものとする。

立入制限区域への入退室口の施錠の方法は、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）など民間企業で適切と判断する方法を用いるものとする。

この方法については、重要技術情報管理責任者が立入制限区域へのアクセスそのものを管理でき、かつ、立入制限区域へのアクセスについての事実関係を、立入制限区域の入室管理の記録簿と照合することで事後的に確認することが可能なような方法を用いるものとして、例えば、鍵を用いる場合には、鍵の管理は、重要技術情報管理責任者又はその委任を受けた者が行うこととし、鍵の貸出しは、重要技術情報管理責任者又はその委任を受けた者の承認を得た上で、鍵の貸出日時、返却日時を記録することなどの措置をとるものとする。

また、鍵の管理に当たっては、当該鍵に対応する立入制限区域を含む構内（例えば工場敷地内）から持ち出さないことを徹底する[6]。

重要技術の情報を保有する民間企業では、立入制限区域の全ての鍵の解錠が

[6] キーパッド式の鍵の暗証番号等については、４.（２）①の保管容器の鍵番号に準じて取り扱うものとする。

可能なマスターキーの製作や共通パスワードの設定は行わないことを推奨する。災害等緊急時対応のため、マスターキーの製作等が必要な場合には、そのマスターキー等の管理は、重要技術情報管理責任者自らの管理とすることを推奨する。

加えて、立入禁止区域の窓は施錠可能なものとし、業務時間外は施錠するとともに、外部からの侵入を防止できる処置をとることを推奨する。

なお、立入制限区域には、セキュリティカメラの設置、警報装置など警備システムの導入、警備員の配置等により視認性を高める装置の導入等を推奨する。

③　立入制限区域へのアクセス制限の実効性を高めるための対応

立入制限区域については、２.（２）のとおり、その区域が立入制限区域であることを示す表示として、民間企業の判断により「立入禁止区域」や「アクセス権者以外立入禁止」などの表示を行うものとする。なお、この表示の表記については、重要技術の情報に係る立入制限区域につき、統一的な表記を行うものとする。

立入制限区域への全ての立入者については、他の者から視認できる形で、当該立入禁止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。

また、立入制限区域内には、カメラ、通信機器等携帯型情報通信・記録機器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、重要技術情報管理責任者の承認を得るものとする。

立入制限区域内における情報通信・記録機器の利用については、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ものとする。

立入制限区域内にパソコン等を設置する場合には、当該パソコン等を物理的に持ち出せないようにワイヤ等で固定するとともに、社内の一般システムや外部との接続のないスタンドアローンのものとすることを推奨する。

５．重要技術の情報の作成等、運搬、複製運搬、廃棄の取扱い

重要技術の情報については、作成等の時点において、重要技術である旨の表示（マーキング）を付し、立入制限区域からの持出しをさせないことが原則であるが、重要技術の情報の活用管理の観点から立入制限区域の外での取扱いが必要な場合や重要技術の情報を複製する必要がある場合又は重要技術の情報を廃棄する場合には、以下の基準に従って行うものとする。

重要技術情報管理責任者は、重要技術の情報の作成等、運搬、複製、廃棄の手順を定めるものとする。

（１）作成等

紙媒体、電子媒体等で重要技術の情報を作成し、又はある技術が重要技術であると評価された時において当該重要技術の情報がある場合には、当該重要技術の情報には、重要技術情報管理責任者が定める手順に従って、速やかに重要技術の情報である旨の表示（マーキング）を行うものとする。

（２）運搬

①　重要技術の情報の保管容器との立入制限区域との間の運搬

重要技術の情報について、立入制限区域の外に置かれている保管容器から立入制限区域で取り扱うために行う運搬（立入制限区域から他の立入制限区域や立入制限区域から立入制限区域の外に置かれている保管容器への運搬を含む。）は、アクセス権者又は重要技術情報管理責任者が重要技術の情報の運搬をすることを承認した者により行わせるものとする。

重要技術情報管理責任者により重要技術の情報の運搬の承認をされた者が、当該重要技術の情報のアクセス権者ではない場合には、外部から運搬する内容が視認できず、かつ、運搬中に不正があった場合に確認ができるよう重要技術の情報を封筒に入れる等の措置を、当該重要技術の情報のアクセス権者において講じるとともに、当該承認をされた者は、その重要技術の情報の受渡し時に、受領者によるサイン、日時の記載がされた受領証を受け取り、重要技術情報管理責任者に提出するものとする。

また、送付側と受取側は、アクセス権者以外に重要技術の情報を運搬させた場合は、相互に、内容、個数等の運搬した内容のチェックを行うものとする。

② 重要技術の情報の構外等への運搬

重要技術の情報を、当該重要技術の情報が現にある立入制限区域の以外の場所（同一構内、同一社内の立入制限区域を除く。）や構外に運搬する必要がある場合は、重要技術管理責任者は、当該運搬する先の者（場所）について、以下の点を確認するものとする。

- 当該運搬の先が社外の者である場合には、このガイドラインの６．に則して評価等がなされ、秘密保持契約の締結がされた後の者であるか否か
- 当該運搬の先が、同一構内、同一社内の他事業所などの民間企業の内部である場合には、当該他事業所で当該重要技術の情報を取り扱わせる必要性、当該他事業所における重要技術の情報の取扱いに関して重要技術の情報の管理を適切に行うための措置が講じられているか否か

重要技術の情報の構外への運搬に関しては、構内での運搬の方法に準じ、又は信頼できる輸送機関若しくは運搬事業者により行うものとする。

また、重要技術の情報の構外への運搬における運搬の先の受領者がこのガイドラインの６．に定める外部委託先等である場合には、その外部委託先等との秘密保持契約において限定された重要技術の情報の取扱いを行う者による受領の日時、サインを得ることとし、同一社内である場合には、当該重要技術の情報のアクセス権者である受領者による受領の日時、サインを得るものとする。

（３）重要技術の情報の複製

重要技術の情報の複製（重要技術の情報が保存されたサーバーからアクセス権者の個人のパソコンへのダウンロードやプリントアウトを含む。）は、重要技術情報管理責任者の承認を得て、アクセス権者のみが行うことができるものとし、複製された情報は、その元となる重要技術の情報と同じ取扱いを行うものとする。

重要技術情報管理責任者は、アクセス権者からの重要技術の情報の複製の承認の求めがあった場合には、当該複製が真に必要なものか否かの確認を行い、可能な限り限定された範囲での複製のみを認めるものとする。

（４）重要技術の情報の廃棄

重要技術の情報の廃棄については、紙媒体の場合にはシュレッダー（クロスカット方式のシュレッダーを推奨する。）による裁断をすることとし、他の物件については、重要技術の情報を探知することができないよう焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により廃棄するものとする。

６．重要技術の情報に係る外部委託先等のマネジメント

重要技術の情報については、一般的に社外の者に取り扱わせることは少ないと考えられるが、その活用管理の観点からは、共同研究の相手方と重要技術の情報を共有することが必要な場合等も想定されることも踏まえ、社外の者において重要技術を取り扱わせる場合の当該社外の者（以下「外部委託先等」という。）に係る事前の確認、契約における担保などを通じたマネジメントを確実に行うものとする。

（１）外部委託先等に重要技術の情報を取り扱わせる前の確認

重要技術の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ものとする。

重要技術の情報の取扱いを外部委託先等に行わせる場合については、当該外部委託先等が、重要技術の情報を適切に管理し、かつ、自社からの情報管理の要請に適切に対応できる能力を有するか否かを事前に調査・確認するものとする。その際、例えば、自社で講じている秘密の保護に係る取組と同等以上の取組が相手方において行われているか否かを調査・確認するものとし、当該調査・確認の評価の社内手続を定めることを推奨する。

特に、外部委託先等が海外企業である場合には、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洩リスクが高まる可能性も考えられるため、より確実に事前の調査・確認を行うものとする。

（２）秘密保持契約の締結

重要技術の情報を外部委託先等において取り扱わせる場合には、当該外部委託先等と必ず秘密保持契約を締結するものとし、その秘密保持契約には、第三者開示の禁止などの基本的事項に加えて、以下の事項を含むものとする。

- 外部委託先等における重要技術の情報の取扱者を限定するとともに、当該取扱者の氏名等を明らかにすること（Need to Know 原則に照らして必要最小限の範囲であることを、重要技術の情報を保有し、外部委託先等に提供する者（以下この６．（２）（３）において「委託元」という。）において確認する。）
- 限定された重要技術の情報の取扱者による重要技術の情報へのアクセス記録を外部委託先等において記録・管理すること
- 委託元から提供された重要技術の情報の複製、廃棄などが行われた場合の

記録簿の作成、適時の報告を委託元に対して行うこと

- 契約満了時又は契約解除時において、提供した重要技術の情報を廃棄（又は委託元へ返還）すること。廃棄する場合は、委託元への廃棄の手法と廃棄の結果の報告を求めること
- 重要技術の情報の管理状況について、外部委託先等から委託元に対して定期的に報告をすること、定期的又は不定期の委託元からの重要技術の情報の管理に係る監査を外部委託先等において受け入れること
- 実際の重要技術の情報の受渡しについては、両当事者で定めた表示を明示的に付して行うとともに、受渡しをした重要技術の情報のリストを作成し、両当事者協力の下で最新のものに更新を行うこと

（３）外部委託先等のマネジメントをより実効的にするための措置

重要技術の情報を外部委託先等において取り扱わせる場合には、可能な限り分割して情報を渡すなど、当該情報を含めて構成される重要技術の全体が外部委託先等から見てわからないような取組を行うことを推奨する。

民間企業では、製造設備のリモートメンテナンスなど、重要技術の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重要技術の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るようなケースにも留意する必要があると考えられる。

そのため、このようなケースについては、例えば、この６．（１）、（２）の考え方に従って、外部委託先等が秘密情報を適切に管理し、かつ、自社からの情報管理の要請に適切に対応できる能力を有するか否かを事前に調査・確認することとするとともに、蓄積された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、条件違反等違約の場合の損害賠償や法的措置を採る旨の記載を行うことを推奨する。

重要技術の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重要技術の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重要技術の情報が漏洩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も、委託元の承認を条件とするなど、委託元によるコントロールを効かせることを推奨する。

外部委託先等として、委託元と内外の他の企業とのジョイントベンチャー（JV）を組み、当該 JV 企業に重要技術の情報を扱わせる場合については、JV 契約において、委託元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

ための措置を講ずることを推奨する。
　また、当該 JV 企業における技術の受入れに関しては、委託元からの取締役の派遣とともに、技術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など、組織機能的かつ実体的に、委託元から JV 企業に重要技術の情報が容易に流れないような仕組みを講ずることを推奨する。

７．重要技術の情報の管理を確実に実行していくためのトレーニング

秘密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、重要技術の情報を保有する民間企業は、従業員等（アクセス権者のみならずその他の従業員等を含む。）への秘密の管理に関する意識の涵養を図るためのトレーニングを受講させるとともに、特に、アクセス権者については、重要技術の情報を的確に取り扱わせるための手順についてのトレーニングを受講させるものとする（トレーニングは会議、講義、e-learning 等いずれの実施形態であるかを問わない。）。

また、従業員等における秘密の管理に係る意識の涵養を一層図るため、全ての従業員等について、トレーニングに加えて、秘密情報保護に係るセルフチェックを定期的に行うようにするとともに、重要技術の情報を保有する複数の部署が存在する場合には、当該部署間での相互チェックを行うことを推奨する。

（１）全ての従業員等に対するトレーニング

重要技術の情報を保有する民間企業は、全ての従業員等に対して、定期的（一年に１回以上を推奨する。）に、秘密保全に関するトレーニングを受けさせる機会を設けるものとし、トレーニングの内容については、最低限、以下の事項を含めるものとする。

- 秘密の情報の管理の重要性、企業における秘密情報の分類と取扱い
- 秘密の情報の漏洩とその結果の事例
- 関係法令の内容
- 秘密の情報の漏洩等の兆候・端緒があった場合の報告手続
- 標的型メールなどの警戒すべき手口[7]
- 秘密の情報の管理に係るセルフチェックの実施とその方法

（２）アクセス権者に対するトレーニング

重要技術の情報を保有する民間企業は、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、重要技術情報管理責任者又は重要技術情報管理責任者が指定する者によるトレーニングを、少なくとも１年に１度受講させるものとする（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、重要技術の情報にアクセスさせる前にトレーニングを受講させる

[7] 標的型メールについての参考資料として、ＩＰＡテクニカルウォッチ『標的型メールの例と見分け方』 https://www.ipa.go.jp/files/000043331.pdf などを参照する。

とともに、トレーニングの未受講者に対して、アクセス権の失効などの適切な処置を講ずるものとする。）。

アクセス権者に対するトレーニングの内容は、７．（１）の全ての従業員等向けのトレーニングの内容に加えて、具体的な重要技術の情報の取扱手続、情報の漏洩等の兆候・端緒のケーススタディを含むものとする。

８．重要技術の情報に係る漏えいの兆候把握、事故発生時の報告等の対応

重要技術の情報を保有する民間企業においては、重要技術の情報に係る漏えい等のリスクを可能な限り速やかに探知するとともに、仮に漏えい等の事故が発生した場合の対応を迅速に講じていく観点から、従業員等が漏えい等のリスクを発見した場合等における報告の手順及び報告先等を確立するものとする。

（１）全ての従業員等が報告すべき事象

重要技術の情報を保有する民間企業は、全て従業員等に対して、少なくとも、以下の①②のような事象を発見した場合には、重要技術情報管理責任者又は当該重要技術の情報を保有する民間企業の情報の保護に関する総括的な責任者に報告を行わせるものとする。

重要技術の情報の漏洩等に係る報告が、情報の保護に関する総括的な責任者に行われた場合には、当該責任者は、重要技術情報管理責任者に当該報告を共有するものとする。

① 兆候等

- 秘密の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や業務上必要のないアクセス行為を発見した場合
- 特定の競合他社など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
- 保管容器など重要技術の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。）についての破損などの不具合を発見した場合

② 発生等

- 重要技術の情報に関する表示が付された書類、物件等へのアクセス権を有する者以外の者が、アクセス権者が近傍にいない状態で取り扱っていることを発見した場合

この報告の責務については、民間企業においては、少なくともトレーニングの機会を通じて全ての従業員等に対して周知を図ることとし、一般的な秘密保持契約や秘密保持に係る誓約書においても明記することを推奨する。

（２）アクセス権者が報告すべき事象

アクセス権者は、全ての従業員等が報告を行う必要のある事象に加えて、以下の８．（２）①②の事象を発見した場合には、重要技術情報管理責任者に対する報告を行う義務を負う。この義務については、重要技術の情報に係る誓約書

等において担保するものとする。
　また、アクセス権者が、重要技術の情報の漏えい等の事故の発生を発見した場合には、速やかに重要技術の情報の管理を適切に行うための措置をとるものとし、具体的な措置内容については、重要技術情報管理責任者において手順として定める。

① 兆候等
- 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）が著しく増加した場合
- 物理的措置についての不備など、このガイドライン及び社内の情報の保護に関するルールと照らして不具合と考えられるもの又は不具合が発生するおそれがあることを発見した場合

② 発生等
- 重要技術の情報の紛失、流出、漏えい等の事故の発生又は発生のおそれがある場合
- 重要技術の情報の漏えい等の事故の発生等があった場合に講じた措置

（３）報告があった場合の対応

　重要技術情報管理責任者は、重要技術の情報の漏えいの兆候等に関する報告・共有があった場合には、直ちに事実関係（漏えいの疑い等）を確認するとともに、重要技術の情報の管理に関して必要な措置を講じ、又は講じることをアクセス権者に指示するものとし、その手順の細則を定めるものとする。

　重要技術情報管理責任者が行った事実関係の確認の結果として、民間企業においてしかるべき対応をとる必要があると判断される場合には、ハンドブックの初動対応を参考として、適切な措置を講じるものとする。
　この措置を講ずる場合には、少なくとも役員を長とする民間企業内の組織又は役員が直接取り扱うものとし、重要技術情報管理責任者以外の者が長となり重要技術の情報の漏洩等に係る措置を講じる場合には、当該重要技術の情報に係る重要技術情報管理責任者からの意見を聴くことを推奨する。

９．情報セキュリティ（電子情報の保護等）について

重要技術の情報について、電子情報として保存がされている場合であっても、基本的には、他の媒体と同じように管理を行うものとするが、電子情報の特性等に応じて、以下の付加的な管理に係る措置を講じるものとする。

なお、これらの措置を重要技術の情報を保有する民間企業内部のリソースで講じることが難しい場合には、信頼のあるセキュリティの専門事業者などに協力を求めることを推奨する。

（１）電子情報である重要技術の情報の取扱いに係る管理

①　作成時の対応

作成された電子情報である重要技術の情報については、ファイル名に当該電子情報が重要技術の情報であることの表示を付すとともに、当該電子情報へのアクセスに、ID による認証又はパスワード設定による認証を求めるように設定するものとする。さらに、ID 又はパスワード設定による認証に加え、IC カード認証や生体認証等を組み合わせた多要素認証措置をとることを推奨する。

電子情報である重要技術の情報へのアクセスについて、パスワードを設定する場合には、以下の措置を講ずるものとする。

ⅰ）アクセス権者毎にパスワードを設定する場合

a) 当人の関連情報（例えば、名前、電話番号、誕生日）から他の者が容易に推測できる又は得られる事項に基づかないこと

b) 辞書攻撃に脆弱でない（辞書に含まれる語からだけで成り立っていないこと）

c) 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ものとし、パスワードの設定に係る要求事項を、プログラムやソフトウェア等の設定とすること

を推奨する。

また、情報システム（社内で接続された通信機器により構築された情報処理システム）そのものに、パスワードの定期的な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ことを推奨する。

ⅱ）重要技術の情報である電子情報そのものにパスワードを設定する場合

重要技術情報管理責任者又はその委任を受けた者（アクセス権者に限る。）がパスワードを設定するものとし、そのパスワードについては、少

なくとも１年に１度変更することを推奨する。
　パスワードの共有は、アクセス権者に限るものとし、アクセス権者に限定して伝達する方法により周知を行うこととし、パスワードを記したメモ等を目につく場所に置くことを禁止する。

電子情報である重要技術情報については、プログラムやソフトウェアの設定等により簡単に改ざんされないような措置を講じるものとする。

② 保存時の対応

電子情報である重要技術の保存に関して、暗号技術を利用する場合には、電子政府推奨暗号等を用いることを推奨する。

電子情報である重要技術の情報の保存は、サーバーに集中させるとともに、個人で使用するパソコンのシンクライアント化等を進めることを通じて、パソコン自体には重要技術の情報が保存できないような措置を講ずることを推奨する。また、電子情報である重要技術の情報を保存するサーバーは、通常の業務で用いるサーバーと別のサーバーの利用を推奨する。

電子情報である重要技術の情報が保存されるサーバーは、社内の他の情報システムとの間にファイアーウォールを設定することを推奨する。

電子情報である重要技術の情報であってサーバーで保存されているものについては、自由にダウンロードができないようなプログラム、ソフトウェア等の設定を行うものとする（サーバーからダウンロードされ、保存された記録媒体は、重要技術の情報そのものとする。）。

なお、電子情報である重要技術の情報の保存がされたサーバーについて、設置される場所が構内の場合における当該サーバーが設置される場所は、本ガイドラインの立入制限区域の考え方を参考に、重要技術情報管理責任者の指示の下、適切な物理的措置をとるものとする。

サーバーを除くパソコン、USB など可搬式記録媒体に電子情報である重要技術の情報が保存されている場合には、当該可搬式記録媒体を重要技術の情報そのものとして取り扱うこととし、当該電子情報については、文書作成ソフト等の利用により、複製（コピー）、印刷、他の記録媒体への記録ができないような設定をするものとする。
重要技術の情報が保存されたパソコンは、USB メモリの差込口がないものや差込口を無効化、物理的に塞ぐ部品を取り付けたパソコンとすることを推奨する。

重要技術を保有する民間企業は、重要技術の情報の取扱い等に外部のクラウド事業者のサーバーを利用する場合には、本ガイドライン６．の外部委託先等のマネジメントを参照し、当該クラウド事業者等と秘密保持契約を締結するとともに、クラウド事業者等に対して、メンテナンスなど重要技術の情報に関わる作業者を指定すること、操作ログを付け、操作ログの定期的な報告を行うことを求めるものとする。

なお、テレワーク等外部から電子情報である重要技術の情報へのアクセスは認めないように設定するものとする。

③　送信時の対応

電子情報である重要技術の情報を電子メールで送信する場合は、送信する情報そのものについて電子政府推奨暗号による暗号化をすることを推奨し、送信の際の送付先として、必ず重要技術情報管理責任者を Cc で入れるものとする。
パスワードを設定して重要技術の情報を電子メールで送信する場合は、パスワードは別メールで送信するものとする。

④　削除・廃棄時の対応

電子情報である重要技術の情報が不要となった場合には、重要技術情報管理責任者又はその指定する者（アクセス権者に限る。）は、速やかに、復元出来ないように上書き消去（データの完全消去）を行うものする。

重要技術の情報が記録されたサーバー、重要技術の情報であるパソコン、USB 等可搬式記録媒体について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、物理的な破壊を行うことを推奨する。

（２）電子情報である重要技術の情報へのアクセスに関する対応

電子情報である重要技術の情報を保有する民間企業では、誰が、どの通信機器から、いつ、どの重要技術の情報にアクセスしたか（アクセス履歴）のログを取得し、管理するものとする。なお、アクセス権者において、どのような操作をしているか（Web ページへのアクセス履歴や、メールの送受信履歴等）等のログを取得することを推奨する。

（３）情報システム全体における対策

電子情報である重要技術の情報を保有する民間企業が使用する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）を使用しないものする。

オペレーティングシステム（OS）及びソフトウェアによる制御を無効にできるシステムユーティリティソフトウエア（システム横断的に影響を与えるソフトウェア。）の使用については、情報システム及びそのセキュリティの維持・管理に必要なものを除き、可能な限り限定するものとする。

情報システムの OS、基本ソフトウェア、アプリケーションソフトなどは、可能な限り最新のものにアップデートするとともに、ウィルス対策ソフトウェアなどのセキュリティソフトを必ず導入し、当該セキュリティソフトは、可能な限り最新のものを利用するものとする。

情報システムは、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う等により、悪意あるコードから保護するものとし、情報システムを構成するサーバー、パソコン等の通信機器について、一週間以上電源の切られた状態にある場合には、再度の電源投入時に同じ措置をとることを推奨する。

情報システムには、原則として、業務に必要のないソフトウェアのインストールを禁止するものとする。

悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を防止又は検出するため、ブラックリスト化などの管理策を導入することを推奨する。

（４）情報システムの保守・点検

信頼できる第三者による情報システムの保守及び点検を行う場合であって、電子情報である重要技術の情報に関わる場合には、重要技術情報管理責任者の指示の下で、電子情報である重要技術の情報を他の記録媒体に移す等の処置を実施するか、又は重要技術の情報を保有する民間企業の従業員等が保守及び点検業務に立ち会って作業を監視することができる状況で行わせるものとする。

また、第三者による情報システムの保守及び点検に当たって、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ものとする。
　なお、民間企業内部の従業員等又は第三者による保守及び点検等の作業中は、パソコン等の作業画面を録画し、操作ログを取得することを推奨する。

（５）その他の推奨措置

　その他、電子情報である重要技術の情報の適切な管理を実施し、情報システムを健全に保つための措置として、以下の措置を講じることを推奨する。

- ファイアーウォールのログなどの外部からの通信に係るログ（ファイアーウォールの透過や拒否のログ等）、組織内から外部に向けた通信ログや、各パソコンのアクセス履歴に係るログ等を定期的に確認にし、又は閾値を設けて監視することにより、不正アクセスやウィルス感染による秘密情報の流出及びその兆候を監視する体制を構築すること
- アクセス権者に係るログについては、重要技術情報管理責任者又はその指定する者が少なくとも一月に１度チェックを行うこと
- 重要技術の情報を不正アクセス等から保護するため、不正侵入防御システム等を導入すること
- 情報システムの設定に際して、LAN を分割し、その分割された LAN 間においてファイアーウォールを設定すること
- SNS、アップローダー、Web メールサイト及び掲示板等へのアクセスを制限するコンテンツフィルタを導入すること
- 実際に社内システムを攻撃し、侵入できないという事実によってその安全性を確認するペネトレーションテストを実施すること
- 同業種間でサイバー攻撃やその兆候等に関する情報を共有するための枠組み[8]の立上げやその枠組みへの参加等によるサイバー攻撃等の情報の共有の取組を行うこと
- 重要技術の情報の盗難や紛失に備える観点から、以下のようなツールを利用すること
  - 遠隔操作によりパソコン内のデータを消去できるツール
  - 一定期間、管理サーバーとのやり取りがなされない状態が続いた場合に指定されたデータを自動的に消去できるツール
  - パスワードロックで、一定回数、認証に失敗すると重要情報を消去できるツール
  - 電子データそのものに遠隔操作による消去機能を備えさせるツール

以上

[8] 同業種間で情報を共有するための、既存の枠組みとして、例えば、ＩＳＡＣ（Information Sharing and Analysis Center。セキュリティ情報共有組織。）や独立行政法人情報処理推進機構が運用するサイバー情報共有イニシアティブ（Ｊ－ＣＳＩＰ）がある。