JAMA･JAPIA

自工会/部工会･サイバーセキュリティガイドライン V2.2 解説書

第2.2 版

2024 年 8 月 1 日

Japan Automobile Manufacturers Association, Inc.

一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

改訂履歴

版数	発行日	改訂内容
初版	2022 年 12 月 12 日	初版発行
第 2.1 版	2023 年 9 月 1 日	ガイドライン V2.1 発行に伴う文面/文言修正 版数をガイドラインに揃えて 2.1 版とした
第 2.1 版 Rev.1	2024 年 5 月 31 日	解説を拡充(解説対象を追加)
第 2.2 版	2024 年 8 月 1 日	ガイドライン V2.2 発行に伴う改定

目次

1. 本解説書の位置づけ

本解説書は、自工会/部工会・サイバーセキュリティガイドライン V2.1 の用語や要求事項、達成基準などに対し、解釈に迷う部分を抽出し解説を行ったものである。出来る限り全ての企業の観点で「解釈に迷う部分」を拾い上げ解説を加えているが、全ての項目に対してあらゆる視点での解説を行っている訳では無い事に留意頂きたい。

なお、本解説書の想定読者はセキュリティ部門に所属する方、及び関係部門の方を対象とする。

2. 解説対象

本解説書は、自工会/部工会・サイバーセキュリティガイドライン V2.1 における解釈に迷う項目を抽出し、解説を行う。

次頁へ続く

次頁へ続く

次頁へ続く

3. 解説書の見方

本解説書の見方を以下に示す。

ラベル	目的	要求事項	No	レベル	達成条件	達成基準
1 方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	(A) 自社の情報セキュリティ対応方針(ポリシー)を策定している	・自社の情報セキュリティ対応方針を策定し、文書化すること

【解説】

■ 達成条件

① "情報セキュリティ対応方針(ポリシー)"で策定すべき事項が満たされたサンプルはあるか？

そもそも情報セキュリティ対応方針(ポリシー)とは、企業として情報セキュリティを確保するための基本方針やそのための体制、対策基準を規定した文書である。具体的なサンプルとしては、JNSA（日本ネットワークセキュリティ協会）が公開している「情報セキュリティポリシーサンプル 1.0 版」(JNSA, 2016 年)(※1)がある。2002 年に作成されたサンプルを 2016 年 3 月 29 日に改定しており、スマートデバイスやクラウド、SNS といった新しい技術やサービスの登場にも対応している。2022 年現在も、企業規模を問わず、多くの企業が参考としているものであり、策定すべき事項の解説が参考となる。また、中小企業向けには「情報セキュリティ対応方針(サンプル)」(IPA, 2019 年)(※2)が参考となる。(B)

ただし、これらはあくまで参考情報であり、自社の組織や環境に応じて置き換えた上で策定することが重要である。

参考(※1)：https://www.jnsa.org/result/2016/policy/

参考(※2)：https://www.ipa.go.jp/files/000072146.docx

＜図：解説書のサンプル＞

解説書は、次のように構成されている。

A) 解説対象のガイドライン項目

ガイドライン原文の内容（ラベル、目的、要求事項、No、レベル、達成条件、達成基準）を記載している。

なお、後述の解説にて対象となるガイドラインの該当箇所はマーカーで明示している。

B) 解説

ガイドラインの内容で解釈に迷うと考えられる箇所に対し、解説を記載する。

その具体的な箇所は「■」と「“”」の記号を使い、次のように示す。

例：ガイドラインの達成条件における情報セキュリティ対応方針(ポリシー)に対し、解説を行う

【解説】

■ 達成条件

① "情報セキュリティ対応方針(ポリシー)"で・・・

4. 解説書

・ **共通事項**

① グループ企業の場合、チェックシートは個社ごとに回答するのか、グループでまとめて１つ回答するのか？

グループ企業様は、連結としての回答ではなく、単体（各社）毎に、ご回答をお願いします。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
1 方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	自社の情報セキュリティ対応方針(ポリシー)を策定している	・自社の情報セキュリティ対応方針を策定し、文書化すること

【解説】

- **達成条件**

① ″情報セキュリティ対応方針(ポリシー)″で策定すべき事項が満たされたサンプルはあるか？

具体的なサンプルとしては、JNSA（日本ネットワークセキュリティ協会）が公開している「情報セキュリティポリシーサンプル 1.0 版」(JNSA, 2016 年)(※1)がある。2002 年に作成されたサンプルを 2016 年 3 月 29 日に改定しており、スマートデバイスやクラウド、SNS といった新しい技術やサービスの登場にも対応している。2022 年現在も、企業規模を問わず、多くの企業が参考としているものであり、策定すべき事項の解説が参考となる。
また、中小企業向けには「情報セキュリティ対応方針(サンプル)」(IPA, 2019 年)(※2)が参考となる。
これらを見れば、企業として情報セキュリティを確保するための基本方針やそのための体制、対策基準をどのように規定すればよいか把握することができる。ただし、これらはあくまで参考情報であり、自社の組織や環境に応じて置き換えた上で策定することが重要である。
参考(※1)：https://www.jnsa.org/result/2016/policy/
参考(※2)：https://www.ipa.go.jp/files/000072146.docx

② ″自社″には海外拠点も含まれるか？

共通事項の解説①に記載の通り、個社単位となるため含まない。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
2 機密情報を扱うルール	機密情報を扱うルールを定め、 社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	4	Lv1	自社の守秘義務のルールを規定し、守らせている	【規則】 ・自社の守秘義務を策定し、文書化すること ・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること ・退職もしくは期間満了時に会社の機密情報を持ち出さないこと 【対象】 ・役員、従業員、社外要員（派遣社員等）

【解説】

- **達成基準**

① “自社の守秘義務のルールを規定”とあるが、守秘義務のルールは具体的にどのようなものを策定すればよいか？

自社の守秘義務をルール化するうえで、情報が漏洩したときに自社に与える影響や競合他社にとって有用であるか等の観点で、機密扱いとすべき情報を検討することになる。守秘義務の対象を明確にしたうえで、守秘義務のルールを規定することが望ましい。具体的なガイドラインとしては、「秘密情報の保護ハンドブック」（経済産業省）などが参考になる。例えば、ルールには下記のような内容を含める必要がある。（下記例示）

- 適用範囲　（役員、授業員、派遣社員、委託先従業員など）
- 機密情報の対象　（経営情報、個人情報、営業情報、知的財産等の技術情報など）
- 機密情報の分類　（役員外秘、部門外秘、社外秘）
- 機密情報の漏洩対策　（就業規則/誓約書等で自社の従業員に守秘義務を徹底させる、業務委託時に秘密保持契約を締結するなど）
- 機密情報漏洩時の罰則

＜自社の従業員に対する守秘義務の例＞

自社の従業員に対する守秘義務のルールの具体例としては、「秘密情報の保護ハンドブック」（経済産業省）の参考資料２「各種契約書等の参考例」に、従業員の就業規則や秘密情報管理規程の例があり参考になる。

＜社外要員に対する守秘義務の例＞
なお、社外に業務委託する場合は、社外要員は社内や業務に関する情報に少なからず触れることになり、委託先が機密情報や個人情報を漏洩した場合、自社も責任を問われることになるため、秘密保持契約を締結することや業務委託契約に秘密保持条項を記述することも検討する必要がある。秘密保持条項の具体例としては、「秘密情報の保護ハンドブック」（経済産業省）の参考資料２「各種契約書等の参考例」などを参考に、自社の法務担当者に相談のうえ検討することが望ましい。

※「秘密情報の保護ハンドブック」の“３－４ 具体的な情報漏えい対策例”には、企業の機密情報を守るための具体的な情報漏洩対策や具体例が記載されており参考になる。また、参考資料２「各種契約書等の参考例」の“第１”に従業員の就業規則の例、“第２”に秘密情報管理規程の例がある。
参考：秘密情報の保護ハンドブック（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

参考：参考資料２　各種契約書等の参考例（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

② **自社の守秘義務を“守らせている”とあるが、どうやって守秘義務を守らせるのか？**
①で解説のとおり、守秘義務の対象を明確にし、機密情報を含む情報や物にはラベル等で機密情報であることを明示することが重要となる。さらに、自社の従業員や社外要員に対しては、下記のような対策をすることが考えられる。（以下例示）

＜自社の従業員に対して守秘義務を守らせる＞
- 機密情報の管理方法に関する教育や研修を行い、ルールをしっかりと周知・認識させる
- 部門外秘等の機密情報が含まれる会話の場合は、議事録等で記録に残し、機密情報であることを認識させる
- 入社時や退職時に、誓約書を締結する
- 違反者に対する内部通報窓口を設ける

＜社外要員に対して守秘義務を守らせる＞
- 機密情報の管理方法に関する教育や研修を行い、ルールをしっかりと周知・認識させる
- 機密情報の開示/提供に関わる会話を議事録等で記録に残し、機密情報であることを認識させる

- 秘密保持契約等に、機密情報漏洩対策に関する監査や、機密情報へのアクセスログ提供に協力することを記載する
- 秘密保持契約等に、機密情報漏洩が発生した時に、調査協力や損害賠償・法的措置を取ることを記載する

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
2 機密情報を扱うルール	機密情報を扱うルールを定め、 社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	5	Lv2	自社の守秘義務のルールを規定し、守らせている	【規則】 ・守秘義務の誓約書を提出させること（社外要員除く）

【解説】

- **達成基準**

①　“守秘義務の誓約書”に関する具体的な記述は何を参考にすればよいか？

自社の守秘義務を規定しただけでは、従業員に守秘義務があることを認識してもらうことに対して不十分であるため、自社の従業員と守秘義務の誓約書を提出してもらうことが重要となる。また、従業員が退職した後も情報漏洩のリスクがあるため、守秘義務の誓約書の内容は、在籍中だけでなく退職後も守秘義務が有効となる内容とすることが求められる。守秘義務の誓約書のサンプルとしては、「秘密情報の保護ハンドブック」（経済産業省）の参考資料２「各種契約書等の参考例」に、秘密保持誓約書の例があり参考になる。

※「秘密情報の保護ハンドブック」の“３－４　具体的な情報漏えい対策例”には、従業員に対して誓約書を締結することの意義や留意点が記載されており参考になる。また、参考資料２の「各種契約書等の参考例」の“第３”に、秘密保持誓約書の例がある。

参考：秘密情報の保護ハンドブック（経済産業省）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

参考：参考資料２　各種契約書等の参考例（経済産業省）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
2 機密情報を扱うルール	機密情報を扱うルールを定め、 社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	6	Lv2	派遣社員、受入出向社員について、派遣元、出向元の会社と守秘義務を締結している	【規則】 ・守秘義務には、業務で知り得た情報を外部に漏えいさせない旨の記述があること 【時期】　※守秘義務の締結時期 ・業務開始前

【解説】

- **達成基準**

① **“守秘義務には、業務で知り得た情報を外部に漏えいさせない旨の記述”とあるが、守秘義務に関する具体的な記述は何を参考にすればよいか？**

派遣社員/出向社員が会社や業務に関わる機密情報や個人情報を漏洩させないため、自社の法務担当者と下記のような観点を相談したうえで、契約に反映することが望ましい。

- 派遣社員/出向社員が秘密保持すること
- 機密情報の漏洩防止に関する会社ルール等を、派遣社員/出向社員に業務指示することを認めること
- 機密情報の漏洩対策に関する監査に協力すること
- 機密情報漏洩の発生に備え、調査協力や損害賠償・法的措置を取ること
- 業務終了時には、機密情報や情報機器を返却すること　　（No.7 を参考のこと）

※厚生労働省や各県労働局が公開している労働者派遣契約書の雛形やサンプルがある。「労働者派遣基本契約書の雛形」（厚生労働省）の第 14 条、第 15 条に、秘密保持に関する記述があり参考になる。
参考：労働者派遣基本契約書の雛形（厚生労働省）

https://www.mlit.go.jp/common/001383155.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
2 機密情報を扱うルール	機密情報を扱うルールを定め、 社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	7	Lv2	退職や期間満了時には必要な機密情報、情報機器などを回収している	【基準】 ・回収物一覧のチェックシートまたは帳票を作成すること ・回収漏れが起こらない手順を整備、運用すること ・手順に従い回収しているかを確認し、必要に応じて手順の是正を行うこと [回収物] -情報(印刷物、記憶媒体) -情報機器(PC、スマートデバイス) -アクセス権（ID、鍵） ※上記の他に必要な回収物を各社で判断すること [回収状況の確認、手順の是正頻度] -1 回以上/年

【解説】

- **達成基準**

① 従業員が許可を得て自身の端末を業務利用している場合、その端末も回収すべき”情報機器”に含むか？

含まない。ただし、本項目の目的である「機密漏えいを防止」の観点からみると、情報機器回収の代替策を実施することが望ましい。(以下例示)

- 端末に業務データを保存できない仕組みとする(シンクライアントなど)
- 端末利用終了時に業務データを削除する運用ルールを定め、事前に従業員との間で誓約書を作成する

なお、こうした業務利用している従業員の個人端末のことを BYOD(Bring Your Own Device)端末といい、その運用により業務の効率化などメリットもあるが、適切に運用できないと情報漏えいなどのセキュリティリスク増加のデメリットも存在する。そのため、許可・不許可も含めて運用ルールを策定する必要があり、そちらについてはNo.8 が該当項目となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
2 機密情報を扱うルール	機密情報を扱うルールを定め、 社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	8	Lv1	業務で利用する情報機器の利用ルールを規定し、周知している (個人所有機器(BYOD)含む)	【規則】 ・情報機器（PC、サーバー、通信機器、記憶媒体、スマートデバイス等）の利用ルールを策定し、このルールには利用開始時、利用終了時の手続き、利用中の遵守・禁止事項、紛失時の手続きを含むこと ・情報機器の利用ルールを容易に確認できる状態にすること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定常的に、かつ、ルールの改正時に周知すること

【解説】

- **達成基準**

  ① 情報機器を利用する際の“利用中の遵守・禁止事項”にはどういった内容を含めればよいか？

  情報機器の利用中に従業員が守るべきセキュリティ対策については、「中小企業の情報セキュリティ対策ガイドライン」や付録 3「5 分でできる！情報セキュリティ自社診断」（IPA）などに対策例が書かれており、参考にすることが望ましい。
  情報機器の利用中のセキュリティ対策で特に押さえておくべきポイントや対策例としては下記が挙げられる。

  - 情報機器の OS やソフトウェアを常に最新に保つなど、情報セキュリティを確保すること
  - 情報機器の紛失や盗難防止のため、離席時や退社時には、情報機器を机上に放置しない、または安全に保管すること
  - 情報機器を社外に持ち出すときは、情報機器内のデータ暗号化等の対策がされていること
  - 個人所有機器の取り扱いとして、原則、個人所有機器の持込は認めないが、BYOD にて業務を行う必要がある場合は厳密な管理ルールに則り運用すること

  ※「中小企業の情報セキュリティ対策ガイドライン」の付録 3「5 分でできる！情報セキュリティ自社診断」には、情報セキュリティの診断項目および対策が記載されており参考にすることができる。

参考：中小企業の情報セキュリティ対策ガイドライン第 3.1 版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

参考：付録 3　5 分でできる！情報セキュリティ自社診断（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
3 法令順守	会社として、情報セキュリティに関する法令を順守する	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)	9	Lv1	情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している	【規則】 ・情報セキュリティに関連する法令を守るための社内ルールを策定すること ・策定した社内ルールを教育・周知すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 （教育） ・新規受け入れ時、かつ、１回／年 （周知） ・定常的に、かつ、ルールの改正時に周知すること

【解説】

- **達成条件**

①　ルール策定・教育実施・周知の 3 つの観点があるが、情報セキュリティに関する法令の教育にはどのような内容を盛り込むべきか？

法令そのものの詳細や解釈を教育するのではなく、法令を基に策定した社内ルールに対しての教育を行うことが重要である。社内ルールの遵守、理解度向上が目的となるため、遵守すべき事項、遵守できない場合の組織としてのリスクの説明が盛り込まれていればよい。

②　教育効果の確認まで実施するべきか？

当要求事項においては、教育効果の確認までは含まない。ただし、投資対効果の明確化や今後の改善のためには実施する方が望ましい。

③ ″情報セキュリティに関する法令″とは具体的に何を指すか？

事業内容によって遵守すべき法令は異なるため、関連法令の情報収集を行い社内ルール化していればよい。
参考として、代表的な国内の法令としては次のものがある。(以下例示)

- 不正競争防止法
- 電子署名認証法
- e-文書法
- 個人情報保護法
- 不正アクセス禁止法

なお、上記法律に関する事項は法務担当に確認することが望ましい。そういった部署がない場合は外部の専門家に相談し、関係する情報を明確にする必要がある。

- **達成基準**

④ ″定常的″な周知の具体的な頻度や方法は何か？

例えば、1回／年 の頻度で、メールやチャット・資料配布という方法がある。従業員が、法令違反しないための周知方法であれば、どのような方法でも良い。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
3 法令順守	会社として、情報セキュリティに関する法令を順守する	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)	10	Lv2	個人情報をお持ちの会社については、個人情報に特化した社内ルールの規定があること	【規則】 ・お客様個人情報の取り扱いにおける社内ルールを策定すること ［明確にする内容］ -個人情報の管理体制を確立 -取得時に利用目的を通知、明示 -本人の同意の範囲内で利用 -本人の同意なしに第三者提供しないこと -本人による開示・訂正・利用停止・消去などの要望に対応すること -個人情報の取扱いルールを定めること -個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集を行うこと -情報漏洩した時の対応手順 【対象】 ・個人情報を取扱う業務担当者

【解説】

■ **達成条件**

① **“個人情報”として取り扱うべき項目は何か？**

情報単体だけでなく、用途及び情報の組み合わせに応じて、項目は多岐に渡る。地域・国それぞれの法令によっても多少の項目の定義には差異があるものの、本国内の個人情報保護法を例にとると、次のような項目が個人情報として扱われる。(以下例示)

- 氏名
- 生年月日、連絡先（住所・居所・電話番号・メールアドレス）と本人の氏名を組み合わせた情報
- 防犯カメラに記録された情報等本人が判別できる映像情報
- 本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報

※「個人情報の保護に関する法律についてのガイドライン（通則編）」（個人情報保護委員会，2022 年）にて他の事例も記載されている。

参考：https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a2-1

② “個人情報に特化した社内ルール”を規定するための参考となる例はあるか？

国内の個人情報保護委員会が参考となるガイドラインを提示している（上記①の参考リンクを参照)。当ガイドラインには、各条項に対する解釈や例示等も説明されており、こうした内容を基に、社内ルールとして必要な部分を取捨選択することが望ましい。

■ 達成基準

③ “お客様個人情報”とあるが、自社の従業員の個人情報は含まなくてよいのか？

本来、個人情報はお客様のみならず、従業員、取引先、その他関係機関等、様々な主体に関するものも含むべきである。ただし、本項目の達成基準においては、情報が漏えいした際の被害の影響度を勘案し、対象をお客様にフォーカスしている。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
4 体制(平時)	情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	13	Lv1	情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している	【規則】 ・情報セキュリティを統括する役員（CISO 等)や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること

【解説】

■ **達成条件**

① “責任と役割を明確化”とはどのような文書へ規定することが望ましいか？

“責任と役割を明確化”のためには、社内の情報セキュリティに関わる文書に明記することが望ましい。ただし、その文書は要件の概要を規定した上位の規程類もあれば、手順を規定したより現場の業務目線での文書もあり、どの文書に記載すべきか判断に迷う点となる。しかし、“責任と役割”は、組織としての説明責任にも関係する重要な決定事項である。そのため、「情報セキュリティ方針」などの方針レベルの上位規程に記載することが一般的であり、関連する JIS 規格「JIS Q 27001」においても、当該文書に責任と役割を記載するよう規定している。

ただし、文書化することが最終的な目的ではなく手段であり、文書化した内容を周知し社内の認識を共通化することが重要である点に留意すること。

■ **達成基準**

② “連絡先リスト”を整備する際に必要な観点は何か？

連絡先リストを作成する上で重要な観点となるのは、必要な連絡先が網羅されていること、セキュリティ推進活動が実務として機能するか確認することの 2 点である。

＜必要な連絡先の網羅＞

平時の際に必要な連絡先を漏れなく連絡先リストに登録するために、以下のポイントを踏まえて確認するとよい。

- 社内からの情報セキュリティに関するルールなどについての問い合わせを受ける窓口が明確になっていること
- 情報セキュリティ担当部署からの社内向け周知事項、依頼事項を連絡する際のルートが目的・対象範囲別に確立されていること
- 情報セキュリティ責任者や、システム管理者の連絡先を明確化していること

また、メール・チャット・電話といった連絡手段は、連絡先ごとに想定しうる用途に応じて、適したものをそれぞれ確保しておくことが望ましい。

＜機能の確認＞

連絡先リストは作成するだけでなく、実際に機能することを確認し、その状態を保つことが重要である。

そのために、リストにある手段を用いて実際に連絡がとれるか確認を行う、連絡先リストの内容が古くならないよう定期的に最新化を行うといった運用ルールとするのが望ましい。このとき、各連絡先と連絡先リストについての共通認識を持つことで、連絡時の連携をより効率的にすることができる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
4 体制 (平時)	情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	14	Lv2	情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している	【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、組織的に経営判断できる体制を設置していること

【解説】

■ **達成基準**

① **“組織的に経営判断できる体制”を設置するためには、情報セキュリティの責任者または推進委員会に役員が就任することが必要か？**

必ずしも役員である必要はない。本質的に重要なことは、「どのような権限を持っているか」であり、その権限を有する方の就任が重要となる。多くの企業の傾向として、意思決定の権限は役員レベルとなることが多い。ただし、組織・事業の規模によっては部門長クラスの就任となるケースもある。上位の会議体（経営会議、取締役会等）への審議事項として申送りができる場合、特に、後者の傾向が強い（最終的な意思決定が上位の会議体で実施されるため）。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
4 体制 平時	情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	16	Lv1	サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している	【規則】 ・平時の体制に則り、情報セキュリティ事件・事故事例やその対応策を社内部署へ共有していること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・１回／年、もしくは、社内外で重大な情報セキュリティ事件・事故が発生した時

【解説】

■ **達成条件**

① “新たな手口”を知るための一般的な方法は何か？

攻撃の手口を知り、社内関係部署に共有し対策することは、情報セキュリティを高めるために重要となる。攻撃の手口を知るための具体的な方法は、「中小企業の情報セキュリティ対策ガイドライン」（IPA）などを参考にすることが望ましい。例として、「情報セキュリティ 10 大脅威」（IPA）、「早期警戒情報」（JPCERT/CC）がある。また、セキュリティベンダーが公開するレポート等の確認や、平素から付き合いのあるベンダーに相談することも有益である。

※「中小企業の情報セキュリティ対策ガイドライン」（IPA）の“5.より強固にするための方策”の“(1)情報集と共有”には、攻撃の手口を知るための情報収集先が参考情報として記載されている。

参考：中小企業の情報セキュリティ対策ガイドライン第 3.1 版（IPA）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

※「情報セキュリティ 10 大脅威」（IPA）は、社会的に影響が大きかった情報セキュリティ事案から抽出した 10 種類の脅威が毎年発信される。
https://www.ipa.go.jp/security/10threats/index.html

※「早期警戒情報」（JPCERT/CC）は、重要な情報インフラ等に重大な影響を及ぼす可能性がある脅威情報を提供している。
https://www.jpcert.or.jp/wwinfo/wwdata.html

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
4 体制(平時)	情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	17	Lv2	サイバー攻撃や予兆を監視・分析をする体制を整備している	【規則】 ・サイバー攻撃や脆弱性に関する公開情報、非公開情報を活用する体制を構築している ・相関分析によりサイバー攻撃や予兆の検知を可能とし、その分析結果から適切な対応が導きだせる体制を構築している ※相関分析： 複合的なログなどで分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法

【解説】

■ **達成条件**

① サイバー攻撃の“予兆”とは何か？

ここでの「予兆」とは、今後サイバー攻撃が発生するかもしれないということを想起させる事象を指す。例えば、SNS での不審な投稿や、普段アクセスがないような宛先からの疎通確認のための通信などが挙げられる。

② “サイバー攻撃や予兆を監視・分析をする体制”とはどのような組織を指すか？

一般的には、サイバー攻撃の検出や特定を行う SOC(Security Operation Center)や、インシデント対応を担う CSIRT(Computer Security Incident Response Team)と呼ばれるセキュリティ組織を指す。これらの組織は、自社で体制を整備する方法と、外部委託を活用する方法の 2 つがある。留意事項として、後者の場合は、専門的な体制や機能を提供する外部サービスの活用やその組み合わせなどを検討し、自社の状況を考慮して導入可能な体制を整備することが重要となる。

※本項目達成の一助になるサービスとして IPA のサイバーセキュリティお助け隊サービスなどがある。
参考：https://www.ipa.go.jp/security/otasuketai-pr/

■ **達成基準**

③ “複合的なログなどで分析”するとは具体的に何を指すか。

様々なネットワーク・セキュリティ機器のログを収集し、アクセス先 IP アドレスなどのキーや時刻情報などに基づいて横断的に分析することを指す。その分析結果により不審な振る舞いをリアルタイムで検知し、通知する製品・サービスとしては、SIEM(System Information and Event Management)が挙げられる。なお、SIEM の導入手段については№145 の解説に記載しているため参照することができる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
5 体制（事故時）	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生 時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること	18	Lv1	情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している	【規則】 ・情報セキュリティを統括する役員（CISO 等）や情報セキュリティ担当部署の役割・責任が明確化されていること ・情報セキュリティ事件・事故の基準や社内外組織との連絡先、ルートが明確化されていること

【解説】

■ **達成条件**

① 情報セキュリティ事件・事故発生時の対応手順を作成していれば、″責任と役割″の明確化ができているといえるか？

対応手順の作成だけでは十分と言えない。対応手順はどのような基準で、誰が、どのように対応するかが明文化されたような、現場の業務目線での文書である。しかし、″責任と役割″は、組織としての説明責任にも関係する重要な決定事項であるため、対応手順より上位の規程類である「情報セキュリティ方針」といった方針レベルの文書で規定することが望ましい。

■ **達成基準**

② “社内外組織との連絡先、ルート”を明確化するために重要な観点は何か？

有事の際に必要なタイミングで必要なメンバーに連絡が付くことが重要である。そのため、必要な連絡先が網羅されていること、機能するか確認することの 2 つの観点で確認するとよい。

＜必要な連絡先の網羅＞

有事の際に必要な連絡先を漏れなく連絡先として明確にするために、以下の 3 つのポイントを確認するとよい。

・　社内外からセキュリティ事故の発生報告を受ける窓口が明確になっていること
・　情報セキュリティ組織内での連絡ルートが確立されていること
・　情報セキュリティ事故発生時の外部組織の連絡先がリスト化されていること

なお、外部組織の連絡先としては、関連する取引先の連絡先を明確化することはもちろん、協力を仰ぐ外部の専門組織(JPCERRT/CC やセキュリティ企業など)が特に重要となる。加えて、セキュリティ事件・事故発生時の対応手順が明確化されている組織では、手順に記載のある連絡先が網羅されているかという観点でも確認するとよい。

また、メール・チャット・電話といった連絡手段は、連絡先ごとに想定しうる用途に応じて、適したものをそれぞれ確保しておくことが望ましい。

＜機能の確認＞

連絡先リストは作成するだけでなく、実際に機能することを確認し、その状態を保つことが重要である。

そのために、リストにある手段を用いて実際に連絡がとれるか確認を行う、連絡先リストの内容が古くならないよう定期的に最新化を行うといった運用ルールとするのが望ましい。このとき、各連絡先と連絡先リストについての共通認識を持つことで、連絡時の連携をより効率的にすることができる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること	21	Lv3	情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画を作成している	【基準】 ・セキュリティ事件・事故の対応履歴、リスク評価結果に基づき、対策計画を立案すること ・対策計画に沿って対策が実行されているか確認すること ［対策計画の内容］ -対策内容(何に対し、どのような対策を行うか) -スケジュール(開始、終了時期 および 対策の各プロセスに要する期間) ［対策の進捗状況の確認］ -1 回以上／年

【解説】

■ **達成条件**

① ″事業継続計画″と″緊急時対応計画″とはそれぞれ何が記載されたものを指すか？

事業継続計画とは、経営・ビジネス的な視点で事業を継続する、またはそのための復旧を図るための計画であり、より長期的な目線も含めた計画が記載されているものである。一般的には BCP(Business Continuity Plan)と呼ばれることが多く、緊急事態の際に企業が損害を最小限に抑えつつ、中核業務を継続あるいは早期復旧するための計画を指す。

1. 事業継続に影響を与える緊急事態の定義
2. 上記をリスクとして分析するためのアプローチ
3. 実際にリスクが顕在化した場合の体制／判断基準／手続きの概要
4. それら一連の対応を実施するためのスケジュール等

それに対し緊急時対応計画とは、システム／業務上の障害・問題から早期に復旧するための短期的な目線での活動に主眼を置いたものであり、上記の 1～4 が、よりシステム／業務に主眼を置いてまとめられたものである。一般的には EAP(Emergency Action Plan)と呼ばれることが多く、緊急事態またはシステム中断があった場合、暫定的に IT サービスを復旧させるため、迅速かつ最善の措置がとれるよう関係者の役割を調整するために文

書化した戦略的な計画である。暫定的措置には、IT システムおよび運用の別のサイトへの再配置、代替機器の利用による IT 機能の復旧、手動による IT 機能の実行などが含まれる。

■ **達成基準**

② 事業継続計画・緊急時対応計画策定時の″リスク評価″では情報セキュリティが最優先になっている必要があるか？

必ずしも情報セキュリティが最優先になっている必要はない。

自然災害や火災などと同様に情報セキュリティ関連のリスクを取り扱い、事業継続への影響度を評価して優先度付けがされていればよい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生 時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	23	Lv2	情報セキュリティ事件・事故として扱う対象範囲を明確にし、周知していること	【規則】 ・下記対象範囲が明確になっていること ［明確にする内容］ -事件・事故として扱う事象 -事件・事故のレベル 【対象】 ・役員、従業員、派遣社員、受入出向者への周知

【解説】

■ **達成条件**

① ”情報セキュリティ事件・事故として扱う対象範囲”はどのように明確化・周知されていればよいか？

初動対応手順を含むインシデント対応マニュアルのような規定に対象範囲が記載されていればよい。

なお、達成基準として周知を含むため、情報セキュリティ事件・事故の範囲を明確にしたものの資料配布や教育の実施が必要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生 時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること	24	Lv1	情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告

【解説】

■ **達成条件**

① “情報セキュリティ事件・事故時の対応手順”にはどのような内容が盛り込まれていればよいか？

情報セキュリティ事件・事故(マルウェア感染などのサイバー攻撃も含む)の発生時にとるべき対応として、次のような内容が必要に応じて盛り込まれていればよい。(以下例示)

- インシデント報告窓口が設けられて、周知されている
- 発生したインシデントの内容をどこまで情報共有すべきかの判断基準が決められている
- 過去に経験したインシデントを記録し、同じインシデントが発生した際に参照できるようになっている
- 誰に、どの範囲で、どういった手段で告知するか判断する手順が含まれている
- 抑制措置の手段と意思決定者が決められている
- 復旧後にモニタリングする手順が含まれている
- 再発防止策を講じる旨が記載されている

※「組織内 CSIRT 構築の参考資料 インシデント対応マニュアルの作成について」(JPCERT CC, 2015 年)が、盛り込むべき内容の参考となる。
参考：https://www.jpcert.or.jp/csirt_material/files/18_incident_response_manual_20151126.pdf

② ″情報セキュリティ事件・事故時の対応″の具体的な方法を知る参考となる資料はあるか？

情報セキュリティ事件発生時の対応手順ガイドラインである「コンピューターセキュリティインシデント対応ガイド」(IPA,2008 年)が参考となる。
参考：https://www.ipa.go.jp/files/000025341.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生 時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	26	Lv1	マルウェア感染時の対応手順を定めている	【規則】 ・マルウェア感染時用の対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告

【解説】

- **達成条件**

  ① ″マルウェア感染時の対応手順″の具体的な方法を知る参考となる資料はあるか？

  マルウェアの種類は日々、高度化・複雑化している。そのため、最新の手順を知るためには、各セキュリティベンダーが公開するレポートや記事を検索し、閲覧することが最も効果的である。ただし、マルウェアの定義や種類、オーソドックスな対応事項を知る限りにおいては、「マルウェアによるインシデントの防止と対応のためのガイド」(IPA,2008 年)が参考となる。

  参考：https://www.ipa.go.jp/files/000025349.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	28	Lv1	電子メールのマルウェア感染に関する社内への教育を行っている	【規則】 ・電子メールによるマルウェア感染の予防について、教育資料配布・掲示、e ラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における メール利用者 【頻度】 ・新規受け入れ時、かつ、１回／年以上

【解説】

- **達成条件**

① “教育”には何が盛り込まれていればよいか？

対象者・目的によって盛り込む事項は異なるが、対象者が電子メールを含むシステムの管理者(IT 要員)の場合と、電子メールを利用する一般従業員の場合とに分けて、それぞれ教育を行う必要がある。また、「理解向上」を目的とした教育を行う場合には、昨今の世の中の動向や、会社の規定を中心とした説明が望ましいが、「注意喚起」を目的とした教育を行う場合には、他社事例を織り交ぜた「注意しなくてはいけないこと」「してはいけないこと」などを具体的に紹介する事が望ましい。なお、本項目とNo.29 はどちらもマルウェア感染に関する教育を求める項目であるが、本項目では電子メールからのマルウェア感染を想定しているのに対し、No.29 では Web 閲覧による感染を想定しているという経路の違いがあり、それによって必要な予防策や説明すべき内容が異なる。そのため、それぞれの感染経路を想定した教育を実施することが望ましい。

② 教育効果の確認まで実施するべきか？

本項目では、そこまでの実施は求めていない。実施するまでが達成基準であり、参加者それぞれの視点にたっての効果確認までは含まない。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	29	Lv1	インターネットへの接続に関する社内への教育を行っている	【規則】 ・Web 閲覧によるマルウェア感染の予防について、教育資料配布・掲示、e ラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における インターネット利用者 【頻度】 ・新規受け入れ時、かつ、１回／年以上

【解説】

- **達成条件**

① “教育”には何が盛り込まれていればよいか？

対象者・目的によって盛り込む事項は異なるが、対象者が電子メールを含むシステムの管理者(IT 要員)の場合と、電子メールを利用する一般従業員の場合とに分けて、それぞれ教育を行う必要がある。また、「理解向上」を目的とした教育を行う場合には、昨今の世の中の動向や、会社の規定を中心とした説明が望ましいが、「注意喚起」を目的とした教育を行う場合には、他社事例を織り交ぜた「注意しなくてはいけないこと」「してはいけないこと」などを具体的に紹介する事が望ましい。なお、本項目とNo.28 はどちらもマルウェア感染に関する教育を求める項目であるが、本項目では Web 閲覧によるマルウェア感染を想定しているのに対し、No.28 では電子メールからの感染を想定しているという経路の違いがあり、それによって必要な予防策や説明すべき内容が異なる。そのため、それぞれの感染経路を想定した教育を実施することが望ましい。

② 教育効果の確認まで実施するべきか？

No.28 と同様に、本項目ではそこまでの実施は求めていない。実施するまでが達成基準であり、参加者それぞれの視点にたっての効果確認までは含まない。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	31	Lv2	標的型メール訓練を実施している	【規則】 ・標的型メール訓練を実施すること ・万が一開封した時の対応も訓練内容に含めること ・訓練内容や方法を振返り、次回の訓練を改善すること 【対象】 ・電子メールの利用者 【頻度】 ・１回以上／年

【解説】

- **達成基準**

① ″標的型メール訓練″として行うべき訓練内容は何か？

実践形式の訓練が求められる。具体的には、自社のビジネスを模倣したダミーのメールを従業員に対して一斉配信し、そのメール内のリンクをクリックしたかどうかを確認する形式が一般的には多く見られる。自組織の業務に関連がある件名や本文だとしても、不審なファイル・リンクが含まれたメールに対しては、不用意に反応しないことを啓発する上でこのような方法が効果的である。

※「メール訓練手引書」(日本 CSIRT, 2022 年)が標的型メール訓練の計画から改善までの手引きとして使用することができる。
参考：https://www.nca.gr.jp/activity/imgs/nca-mail-exercise-guidebook-v1.0.pdf

② 全社一斉に訓練を実施した場合、問い合わせにより、IT 部門がひっ迫する可能性があるが、訓練の実施方法に基準はあるか？

公的な基準は無い。組織に応じて、業務に支障がでない方法で実施することが重要となる。なお、一斉かどうかよりも、目的を明確にして(例：習熟レベルの向上、課題の明確化、動機付け、等)、それに合ったやり方を採用しているかどうかが重要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	情報セキュリティ事件・事故に迅速かつ適切に対応できるように事前に備え、事故発生時の被害拡大の防止・迅速な復旧を図る	自組織内あるいは組織を跨いで影響する情報セキュリティ事件・事故の発生と影響を抑制する教育・訓練を行っていること	38	Lv1	情報セキュリティ事件・事故発生時の対応について教育・訓練を実施している	【規則】 ・情報セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、e ラーニング、集合教育等による教育や訓練を実施すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・新規受け入れ時、かつ、１回／年以上

【解説】

- **達成基準**

  ① “教育や訓練”はどのように進めると効果的か？

  教育により社内で規定している対応手順への理解を深め、訓練により情報セキュリティ事件・事故への対応力を向上することで、情報セキュリティ事件・事故に迅速かつ適切に対応できるようになる。教育や訓練を行う際には、対象者によって役割や業務内容が異なることから、対象者ごとに教育や訓練の内容を変えることが効果的である。一般従業員向けには、情報や情報機器の取扱いに関する会社ルールを教育・訓練することが重要となる。さらに、情報セキュリティ担当者向けには、例えば No.24 で規定した対応手順に関する教育や訓練を行うことが考えられる。（以下例示）

  ＜一般従業員向け＞
  - 情報や情報機器の取扱いに関する会社ルールの教育　　（例：e ラーニングによる会社ルールの教育）
  - 情報や情報機器の取扱いに関する訓練　　（例：標的型メールを受信した際の報告訓練、マルウェア感染時の対応訓練）

＜情報セキュリティ担当者向け＞

- インシデント対応に関する教育　　（例：組織内 CSIRT 体制や対応手順に関する教育）
- インシデント対応に関する訓練　　（例：インシデント発生時の発見報告・初動・システム復旧等の対応訓練）

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	情報セキュリティ事件・事故に迅速かつ適切に対応できるように事前に備え、事故発生時の被害拡大の防止・迅速な復旧を図る	自組織内あるいは組織を跨いで影響する情報セキュリティ事件・事故の発生と影響を抑制する教育・訓練を行っていること	39	Lv3	組織を跨いだ情報セキュリティ事件・事故発生時の対応について教育・訓練を実施している	【規則】 ・組織を跨いだ情報セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、e ラーニング、集合教育等による教育や訓練を実施すること 【対象】 ・セキュリティ関連部門 【頻度】 ・１回／年以上

【解説】

- **達成条件**

① ″組織を跨いだセキュリティ事件・事故″とは具体的には何を指すか？

文字通り、複数の組織が関わることが前提となるが、そのパターンもいくつか想定され、次のようなケースが該当する。（以下例示）

＜外部組織で発生 ⇒ 自社に波及＞

- 取引先がサイバー攻撃を受け、マルウェアに感染。それを経由して、自社のネットワークへの不正侵入が発生。

＜自社で発生 ⇒ 外部組織に波及＞

- 自組織のサーバーが不正アクセスを受け、それを踏み台として取引先への攻撃が発生。

なお、本項目における”組織を跨ぐ”とは、上記のような会社間を跨ぐ場合と自社の部門間を跨ぐ場合のどちらも含む。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	41	Lv3	サプライヤーとモノ・データの流れを共有できている	【規則】 ・重要なサプライヤーを特定できていること ・モノ・データの流れを特定できていること ・取引の概要を図示して、サプライヤーと共有できていること 【対象】 ・取引のあるサプライヤー

【解説】

- **達成条件**

① ″モノ・データの流れ″とは具体的に何を指すか？

ここでのモノとは、製品及びその製造・生産につながる部品・材料等を意味する。データとは、設計図などの製品の製造・生産につながる情報や発注情報、顧客情報、またそれらに関連する電子情報を指す。ここでの流れとは、業務遂行のプロセスの順番を意味するが、重要なことは「サプライチェーン」目線である。つまり、自組織内の業務プロセスがどう進み、その中でモノ・データがどのように関係しているか、ではなく組織間における連携がどのように発生しているかという視点が重要となる。これらを踏まえて上での共有状況を確認することが求められる。

② ″モノ・データの流れ″を把握するために、データフロー図を作成する必要はあるか？

達成基準にあるようにモノ・データの流れが特定できていればよいため、データフロー図の作成は必須ではない。
ここでは、次の 3 点が把握できるようになっていればよい。
・自組織からの発注先、自組織、自組織への発注元という取引関係の概要
・自組織の全体における役割がわかる関係するサプライチェーンの概要
・事業への悪影響を及ぼすセキュリティインシデントが発生した際の、直接的な取引先及びサプライチェーン全体への影響

・ **達成基準**

③ ″重要なサプライヤー″はどのように判断すればよいか？

サプライヤーの数は多岐に渡るため、全てのサプライヤーを対象とすることは事実上困難である。現実的には、重みづけをした上で、より重要なサプライヤーに対して管理強度を高める必要がある。ここでの「重要」の尺度は個社によって異なるが、各社の経営事情を鑑みて、それぞれの事情に応じた「尺度」を明確にしておくことが求められる。（以下例示）

- 自社の高機密な技術情報を取り扱うサプライヤーかどうか。
- そのサプライヤーの業務に支障が出ることで、自社の開発・生産に致命的な遅延をもたらすかどうか。
- 直近、漏洩事件等を起こしているサプライヤーであり、再発リスクが懸念されるかどうか。

④ 対象となるサプライヤーは重要なサプライヤーのみでよいか？

達成基準の対象にあるように、取引のあるすべてのサプライヤーが対象となる。その上で重要なサプライヤーを特定する必要がある。大事なことは、全体像を把握した上で、その中でより、注力すべき箇所を特定できている状態にすることである。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	42	Lv3	重要な機密情報を取扱うパートナー企業のセキュリティ対策状況を把握している	【規則】 以下の例を参考にパートナー企業の対策状況を把握すること ・チェックシートを作成しパートナー企業から回答を受領する ・パートナー企業に訪問し点検を実施する 【対象会社】 ・自社の重要な機密情報を提供・共有する子会社、取引先など 例：″極秘″の機密情報を共有する会社 【頻度】 ・1 回以上/年

【解説】

- **達成条件**

  ① ″パートナー企業″とは具体的に何を指すか？

  達成基準にあるように自社の重要な機密情報を提供・共有する子会社、取引先等のことを指す。

  なお、パートナー企業から機密情報に該当するとして、セキュリティ実施状況の確認が難航するケースもある。

  そのような際は、秘密保持に係る契約の締結やそれが難しい場合は、双方の情報取り扱いに係る各種規定、取り扱うデータに求められる機微度・重要度、セキュリティ施策の深度等を考慮し、協議を行った上、提示可能な範囲の情報及びそれがセキュリティ対策状況の把握に資するかをすり合わせて進めることが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	43	Lv3	契約終了時に機密情報やアクセス権などを回収または破棄している	【規則】 ・回収すべき機密情報、アクセス権などのチェックシートを作成すること ・契約終了時にチェックシートを使用し機密情報、アクセス権などを回収すること ・回収、破棄が漏れなく行われていることを確認し、必要に応じて是正すること 【対象会社】 ・機密情報を提供・共有する子会社、取引先など 【頻度】 ・1 回以上/年

【解説】

- **達成基準**

  ① “チェックシートを作成”“チェックシートを使用”とあるが、どのようにチェックシートを作成・使用すると効果的か？

  機密情報やアクセス権などを提供・共有する際に、予め台帳で管理しておくことで、回収・破棄対象を漏らすことなくチェックシートを作成することができる。台帳で記載しておくべき情報としては下記が考えられる。(以下例示)

  - 機密情報やアクセス権の内容
  - 提供・共有した日時
  - 提供・共有した方法　(例：記憶媒体、メール)
  - 提供先　　(例：会社、部署、担当者)

  また、契約終了時にチェックシートを提示するのみでは、回収・破棄対象の認識が無く、回収・破棄が困難になることが想定される。そのため、予め、契約期間中に台帳やチェックシートなどを活用して、提供・共有先に認識させることが、契約終了時の確実な回収・破棄に有効である。
  なお、回収・破棄を委託先に実施してもらうためには、秘密保持契約等の取り交わしも必要になるため、No.44 も合わせて参照すること。

※「秘密情報の保護ハンドブック」の“３－４ 具体的な情報漏えい対策例の（３）取引先に向けた対策”には、取引先への機密情報を開示する際の留意点が記載されており参考になる。

参考：秘密情報の保護ハンドブック（経済産業省）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	44	Lv1	他社との間で、機密情報の取り扱い方法が明確になっている	【規則】 ・業務開始前に機密情報の取り扱いについての取り交わしを行うこと 【対象】 ・機密情報を共有する会社

【解説】

- **達成条件**

  ① “他社”とは、パートナー企業、取引先、サプライヤー等をすべて含むと考えるべきか？

  自社以外から機密情報が漏洩することを防ぐことが目的であるため、自社の機密情報を共有するすべての会社が対象である。

- **達成基準**

  ② “機密情報の取り扱いについての取り交わし”とあるが、どのような取り交わしを行えばよいのか？

  機密情報の取り扱いについての取り交わしとは、具体的には秘密保持契約等を取り交わすことである。秘密保持に係る条項の具体例としては、「秘密情報の保護ハンドブック」（経済産業省）の参考資料２「各種契約書等の参考例」などを参考に、自社の法務担当者に相談のうえ検討することが望ましい。秘密保持契約には、下記のような内容を含むことが考えられる。（以下例示）

  - 機密情報の内容
  - 機密情報の取扱い　　（例：情報取扱責任者を設定し厳重に保管・管理することや、目的外使用や第三者への提供を禁止すること。）
  - 機密情報の返還義務　　（例：回収または破棄の要否や、データ削除の場合は書面報告すること。）

※「秘密情報の保護ハンドブック」の“３－４ 具体的な情報漏えい対策例”の参考資料２「各種契約書等の参考例」の“第４”に、秘密保持契約書の例があり参考になる。
参考：秘密情報の保護ハンドブック（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

参考：参考資料２　各種契約書等の参考例（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	46	Lv1	情報セキュリティ事件・事故時の他社との役割と責任が明確になっている	【規則】 ・機密情報を共有する際、取り扱いとともに、情報セキュリティ事件・事故発生時の、会社ごとの役割と責任を文書化しておくこと

【解説】

- **達成基準**

  ① “情報セキュリティ事件・事故発生時の、会社ごとの役割と責任を文書化”とあるが、どのような内容を文書化するべきか？

  サプライチェーン上における情報セキュリティ事件・事故は、自社で発生する場合と委託先等の他社で発生する場合が考えられるが、いずれの場合も情報漏洩が発生した場合は、直ぐに情報漏洩が発生した会社が通知し、被害や影響範囲を最小限に抑えることが重要になる。そのため、自社と取引先等の会社との間で、情報漏洩が発生した際の連絡先を明確にしておく必要がある。連絡先の明確化における重要な観点については、No.18 の解説の②を参考にすること。

  また、委託契約等の契約書面においても、情報漏洩発生時の通知義務や、再発防止策を協議する際は自社の関与を認める旨を明記しておく必要がある。

  ※「秘密情報の保護ハンドブック」の“３－４ 具体的な情報漏えい対策例”の参考資料２「各種契約書等の参考例」の“第６”に、業務委託契約書の例として、事故発生時の役割や責任に関する記載例があり参考になる。

  参考：秘密情報の保護ハンドブック（経済産業省）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

参考：参考資料２　各種契約書等の参考例（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8 他社との情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること	48	Lv3	自社における他社の重要な機密情報の取扱い状況を把握している	【規則】 ・他社の重要な機密情報を自社で取扱った履歴を記録、保管すること ・適切に記録、保管されていることを確認し、必要に応じて是正すること 【記録、保管状況の確認、是正頻度】 ・1 回以上/年

【解説】

- **達成条件**

  ① “重要な機密情報”とは具体的にどのようなものが考えられるか？

  機密情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響の大きさから、重要度が決められるべきである。「秘密情報の保護ハンドブック」（経済産業省）の“（２）保有する情報の評価”に、情報の評価観点が記載されており、参考にすることができる。

- **達成基準**

  ② “他社の重要な機密情報を自社で取扱った履歴を記録、保管”とあるが、どのような方法が考えられるか？

  他社から受領する重要な機密情報は、秘密保持契約等の契約で取扱いに従うことが必須となる。具体的な記録方法は、受領した機密情報を台帳で管理することが求められる。台帳で記載しておくべき情報としては下記が考えられる。（以下例示）

  - 受領した機密情報
  - 受領した日時

・　受領した方法　（例：メール、郵送）
・　保管場所　（例：建屋、部屋、サーバー、キャビネット）
・　保管管理者　　（例：会社、部署、担当者）

保管方法については、例えば、一般従業員の誰でもアクセスできる場所に保管している場合、他社から機密情報の漏洩に関する訴訟を受けた際に、自社からは機密情報が漏洩していないことを立証することが困難になる。そのため、他社の訴訟に対する予防対策として、自社情報と分離して保管しておくことが望ましい。また、秘密保持契約等の契約において、機密情報は契約満了などで不要になった時点で回収・破棄することが求められることからも、自社情報とは分離して保管することが望ましい。具体的な保管方法としては、自社の情報とは分離した保管場所に保管し、施錠管理やアクセス管理を行うとともに、機密情報の持ち出しやデータ参照に対する貸出記録やアクセス記録を徹底する必要がある。

※「秘密情報の保護ハンドブック」の“（２）保有する情報の評価”には、自社の情報や他社の情報の重要度を評価する際の観点が記載されており参考になる。また、“３－４ 具体的な情報漏えい対策例”や“５－２ 他社の秘密情報の意図しない侵害の防止”には、他社の機密情報の取り扱う際の情報漏洩対策や留意点が記載されており参考になる。
参考：秘密情報の保護ハンドブック（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
9 アクセス権	アクセス権設定の不備に起因した、機密エリアやシステムへの不正アクセスを防止する	アクセス権入室権限やシステムのアクセス権 を適切に管理していること	49	Lv1	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている	【規則】 ・以下の内容等を含む管理ルールを定めること ・アクセス権の発行・変更・削除は申請・承認制であること ・与える入室許可・アクセス権の範囲は必要な範囲に限定すること ・入室権限やアクセス権の棚卸について定めていること ・与えた入室許可・アクセス権の申請書または台帳を管理していること 【対象】 ・業務で利用するシステムおよび PC ログオン時のユーザーID ・機密上の配慮が必要な場所や部屋

【解説】

- **達成基準**

  ① 人の異動に伴うアクセス権の“管理ルール”を定めるうえで特に気を付けることは何か？

  人の異動の中でも、特に退職者、派遣社員および委託業者は、業務終了後に入室またはシステムにアクセスできる状態が継続したために、機密情報が漏洩した事例があり、特に注意が必要である。そのため、業務が終了した退職者、派遣社員および委託業者については、アクセス権を即時削除する必要がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
9 アクセス権	アクセス権設定の不備に起因した、機密エリアやシステムへの不正アクセスを防止する	アクセス権(入室権限やシステムのアクセス権)を適切に管理していること	50	Lv2	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている	【規則】 ・重要情報を扱うシステムは、アクセス権を付与するための条件を明確にする ・アクセス権の設定は、システム管理者の要件および設定手順を明確にし、厳格な管理下で実施する。 ・重要情報を扱うシステムは、情報利用者とシステム管理者の権限を分離するなど、個人に権限が集中しない環境とする。 ・重要情報を扱うシステムは、その運用／利用状況を監視する。

【解説】

- **達成基準**

① “アクセス権を付与”してよいかどうかを判断する具体的な条件は何か？

その業務を遂行する権限を有しているかどうかが条件となる。その判断の観点としては、次のものがある。(以下例示)

- 所属部門
- 役職
- 部門内での役割（例：機密管理担当者）

② ″重要情報″とは具体的に何か？

組織によって異なる。一般的には機密管理に係る規程類において、明確に重要情報の定義がされているケースが多いため、こうした規定に準じることが重要となる。なお、一般的な傾向としては、次のような情報を「重要情報」として取り扱う傾向にある。(以下例示)

- 個人情報（顧客、従業員、取引先等）
- 経営情報（財務、戦略、人事等）
- 営業秘密情報（研究、設計、開発等）

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
9 アクセス権	アクセス権設定の不備に起因した、機密エリアやシステムへの不正アクセスを防止する	アクセス権(入室権限やシステムのアクセス権)を適切に管理していること	51	Lv1	管理ルールに沿ってアクセス権の発行、変更、無効化、削除を実施している	【規則】 ・No49 に定義した管理ルールの順守状況の点検を行っていること

【解説】

- **達成基準**

  ① “管理ルールの順守状況の点検”とは、具体的に何をするのか？

  管理ルールの順守状況の点検とは、管理ルールが適切に運用されていることを確認することである。定期的に点検することは、順守違反を発見して是正するだけでなく、管理ルールを順守する意識を向上する観点からも重要である。具体的な点検方法は、入室許可・アクセス権の申請書や台帳に記載されていないアクセス権の発行、変更、無効化、削除が無いかを確認することが考えられる。例えば、システム上のアクセス権の発行、変更、無効化、削除の履歴と、申請書や台帳の記録を比較・確認することなどが考えられる。すべての履歴の確認が難しい場合、サンプリングによる確認であっても、管理ルールの違反を抑制する効果があるため、実施することが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理機器	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	59	Lv1	重要度に応じた情報機器、OS 、ソフトウェアの管理ルールを定めている	【規則】 ・導入、設置、ネットワーク接続、セキュリティパッチ適用等のルールを含む管理ルールを定めていること

【解説】

- **達成条件**

  ① “重要度”はどのような考えで決めるのか？

  重要度は、その IT 資産が侵害された場合のビジネスへの影響度に応じて設定されるものである。例えば、その IT 資産が取り扱う情報の内容によって侵害された場合に、影響が自社に留まるのか、直接取引のあるお客様やサプライヤー等の取引先にまで影響を及ぼすのかといった観点がある。

- **達成基準**

  ② “管理ルール”は何に注意して定めるのか？

  管理ルールは、下記のポイントを踏まえて定めることが望ましい。

  - ハードウェア資産とソフトウェア資産の両方が含まれること。
  - IT 資産の情報を最新状態に保つ仕組みや手順が定められること　（例：サーバーや標準 OS のセキュリティパッチ適用のルール）

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理機器	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	60	Lv1	情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)について、一覧を作成している	【規則】 ・バージョン情報、管理者、管理部門、設置場所等の管理項目を含む情報機器、OS、ソフトウェアの一覧を作成すること

【解説】

- **達成基準**

  ① “一覧”で管理される項目には具体的にはどのようなものがあるか？

  一覧で管理する目的は、ソフトウェアのセキュリティパッチ適用など、IT 資産の情報セキュリティを最新にすることや、情報セキュリティ事件・事故が発生した場合に素早く対応を取れるようにすることである。その目的が満たせるように項目が管理されていればよい。一覧で管理される項目には具体例として下記が考えられる。

  - 機器名（ハードウェア機器、ホスト名）
  - ソフトウェア情報（ソフトウェア名称、バージョン情報）
  - ネットワーク情報（MAC アドレス、IP アドレス）
  - 設置場所（オフィス/データセンター/クラウド等）
  - 使用者（部署名、氏名、連絡先）
  - 管理者（部署名、氏名、連絡先）
  - サポート窓口の連絡先（社内または社外のサポート窓口担当者）

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理(機器)	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	61	Lv2	情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)の一覧を定期的、または必要に応じて、見直ししている	【頻度】 ・1 回/年 以上

【解説】

- **達成条件**

  ① ″見直し″とは棚卸が実施されていればよいか？

  本項目の目的は、サポート切れの古い OS や脆弱性のあるバージョンのソフトウェア等を使っていないか速やかに判断・対応できることであり、現状のバージョン情報や管理者等の情報が更新されていることが重要である。この点を踏まえ、次のポイントを押さえた棚卸作業が実施されていればよい。(以下例示)

  - 一覧の記載項目と実物が一致しているか
  - 破棄された等で一覧から削除すべき対象がないか
  - 正規購入された等で一覧に追加すべき対象がないか
  - 未承認の機器やソフトウェア等、システムから切り離すべき対象がないか

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理(機器)	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	63	Lv3	情報資産(機器)は重要度に応じた管理ルールに沿って管理している	【規則】 ・重要度に応じて、機器と搭載ソフトウェアが正規品である事をシリアル番号やハッシュ値を利用して定期的に確認すること 【頻度】 ・1 回/年 以上(資産棚卸時等)

【解説】

- **達成基準**

  ① ″機器と搭載ソフトウェア″が正規品であることを確認する手段は何か？

  IT 機器とソフトウェアとで、それぞれ次のような手段がある。(以下例示)

  ＜IT 機器＞

  - 資産検出ツールを用いて、ネットワークに接続されている機器が IT 資産管理台帳と一致しているか確認する。
  - 棚卸を行い、実物にあるシリアル番号と、管理している IT 資産管理台帳や購入時の納品書に記載されているシリアル番号を照合する。
  - 納品の際に、管理シールを貼り付けるなどの方法で識別を行い、管理シールの有無を確認する。

  ＜ソフトウェア＞

  - ツールを用いてソフトウェアのハッシュ値を定期的に正規品と確認する。
  - 棚卸又はツールを用いてインストールされているソフトウェアがライセンス契約内容と一致しているか確認する。
  - ライセンス契約に基づいた手順で配布されているか確認する。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理(機器)	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	64	Lv2	スマートデバイスへのアプリケーションの無断インストールを制限し、定期的にインストール状況を確認している	【規則】 ・インストール可能なアプリケーションを定義し、定期的にインストール状況を確認している。 【対象】 ・会社支給のスマートデバイス 【確認頻度】 ・1 回/年

【解説】

- **達成条件**

① ″スマートデバイス″とは何を指すか？

パソコン以外、かつ、持ち運びしやすい可搬性の高い媒体が該当する。通信機能を有していることが前提となり、具体的にはスマートフォン、タブレット端末、その他ネットワーク通信及び情報処理機能を有する小型端末が対象となる。

② “スマートデバイス”以外は本項目の規則を行わなくてもよいのか？

本項目では対象外。ただし、No.98 で PC 端末におけるソフトウェアインストール制限の実施が要求されており、それに準じた確認が必要となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
11 情報資産の管理(機器)	IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	65	Lv2	廃棄時(リース終了時含む)は、記憶媒体のデータを消去している	【規則】 ・情報資産(機器)の廃棄時(リース終了時含む)はデータを復元できないよう消去すること ・情報資産(機器)の記憶領域の消去を実施した記録または業者の廃棄証明書を保管すること ※ディスクのフォーマットは、データを復旧される可能性があるため不可 [対象] -サーバー、会社支給のクライアント PC、スマートデバイス、外部記憶媒体

【解説】

- **達成条件**

  ① “記憶媒体のデータを消去”するにはどのような方法があるか？

  記憶媒体を物理的に破壊する方法と、論理的にデータを消去する方法の 2 つがある。ここで重要となるのは、データを復元できない状態にすることである。どちらの方法であっても、不適切な手段や手順(例：ディスクフォーマットによるデータ消去、誤った手順による不完全な物理破壊、等)であれば、データが復元されてしまう可能性があるため、専用のデータ消去ツールの利用や、専門業者への委託など安全な手段をとることが望ましい。

  また、保存データの機密度が極めて高く、より確実にデータ消去を行いたい場合には、自社で論理的にデータを消去した上で専門の業者に委託し物理的破壊を行うなど、複数の方法・手段を組み合わせるとよい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
12 リスク対応	情報資産のセキュリティリスクを特定し、会社として組織的な対策を行うことにより、業務影響を極小化する	自組織内(自組織の業務：業務委託も含めて)の情報セキュリティリスクに対する対策を行っていること	66	Lv1	情報資産において 「機密性」「完全性」「可用性」の 3 要素が確保できなくなった場合のリスクを特定できている	【規則】 ・対象の情報資産に情報セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握すること 【対象】 ・No.56 で特定した情報資産 【観点】 ・外部の脅威 ・自社の脆弱性 ※必要に応じて、パートナー企業起因の脅威、脆弱性を考慮すること ・情報資産の価値 【方法】 ・対象の情報、情報システムを定めること ・各観点の評価規則、およびそれらを考慮したリスクレベルの規則を定めること ・各情報、情報システムについて、各観点の評価からリスクレベルを決定すること 【頻度】 ・重要な情報資産を見直した時、または、１回／年 以上

【解説】

- **達成基準**

① “情報セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握する”とは、何を実施すればよいか？

一般的に「リスクアセスメント」と呼ばれる、以下の 3 つのプロセスを実施していればよい。

1. リスク特定 … 保有している情報資産を洗い出し、それぞれにどのようなリスク(外部の脅威・自社の脆弱性)があるか特定する。
2. リスク分析 … 特定されたリスクごとに、その特性や発生頻度、影響度を調査・分析する。
3. リスク評価 … 対象となる情報資産の価値と、リスクの発生頻度、影響度から評価し、リスクの対応策や優先順位を検討する。

こうしたリスクアセスメントはセキュリティに関する JIS 規格である「JIS Q 27001」にも記載されており、その目的は、リスクに対して適切な対応策を選定することである。なお、そちらについてはNo.68 が該当項目となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
13 取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	取引先毎に、取引で取り交わされる情報資産と、取引に利用している手段を把握していること	70	Lv1	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している	【規則】 ・一覧表には取引に伴い授受／使用される情報資産とその取り扱いを記載し、取引先と相互に把握すること 【対象】 ・重要な情報資産（No.54 で定められた機密レベルが高い情報資産など）を共有する取引先 【頻度】 ・取引開始時／取り交わす情報・手段の変更時

【解説】

- **達成条件**

① すべての取引先に対して”取り交わす情報・手段”の一覧を作成する必要があるか？

必ずしもすべての取引先を対象とする必要はない。セキュリティ事故発生時に、BCP の観点から速やかに復旧を目指すことを目的とし、重要な情報資産を共有する取引先やその他、セキュリティリスクの危険性が高い条件下にある取引先を優先的な対象とし、作成することが望ましい。

② “取り交わす情報・手段”はどこまで一覧化していればよいか？

取り交わす情報については、自社の機密管理に係る規程類における管理区分（例：極秘、秘、社外秘、一般）に準じて重要な情報を明確とした上で、それを一覧化していればよい。例えば、設計図面データや受発注関連情報(買掛金、売掛金等)及び個人情報（顧客、従業員、取引先等）が一覧化の対象として考えられる。

また、取り交わす手段については、例えば、メール、クラウドストレージ、企業間電子データ交換、その他物理メディア(USB, CD, DVD 等)の受け渡しといった具体的手段を、取り交わすタイミングや頻度と併せて一覧化できていればよい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
13 取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	IT 機器調達における情報セキュリティリスクを管理すること	72	Lv3	IT 機器調達に対するセキュリティ要求事項が決められており、社内に周知されていること	【規則】 ・機器調達に対するセキュリティ要求事項を一覧化していること ・機器調達時に、セキュリティ要求事項を容易に確認できる状態にすること 【対象】 ［機器］ ・社内ネットワークに接続する IT 機器 ［周知］ ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定常的に、かつ、機器調達時のセキュリティ要求事項の改正時に周知すること

【解説】

- **達成条件**

① **“IT 機器調達に対するセキュリティ要求事項”とはどういう要件を提示すればよいか？**

調達先に提示しなければならないセキュリティ要求事項は、製品が扱う情報の重要度によって異なる。ただし、社内向けの管理ルールと同等程度を求める必要はなく、自社の環境を考慮して必要に応じたものを提示すればよい。例えば、クライアント PC 端末であれば次のものが挙げられる。(以下例示)

- 電源投入時パスワード認証機能、および管理者パスワード認証機能があること
- ハードディスクドライブロックの機能があること
- セキュリティロック用のケーブル及びキーが付帯していること
- 無線通信の傍受を防ぐ無線 LAN 規格に対応していること
- 夜間、無人によるセキュリティパッチ適用のため、リモート起動に対応していること

※「IT 製品の調達におけるセキュリティ要件リスト」(経産省, 2018 年)にセキュリティ上の脅威とその対抗策となる要求事項がリストアップされており、参考とすることができる。

参考：https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
13 取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	IT 機器調達における情報セキュリティリスクを管理すること	73	Lv3	IT 機器調達に対するセキュリティ要求事項を購入先と共有しており、購入時の評価結果を記録し保管している	【規則】 ・セキュリティ要求事項が購買契約等に明記されていること ・機器調達時に、セキュリティ要求事項の評価を実施し、結果が保管されていること ・定期的に確認結果が保管されていることを確認する 【対象】 社内ネットワークに接続する IT 機器 【保管状態の確認頻度】 1 回以上/年

【解説】

- **達成条件**

  ① ″IT 機器″とは、すべての IT 機器が対象か？

  全ての IT 機器となると膨大な種類・数となるため、本項目では達成基準にある通り「社内ネットワークに接続する IT 機器」を優先対象とする。ネットワークに接続している以上、マルウェア感染等の重大なリスクの危険性があるため、各機器のリスク強度に応じて濃淡をつけることを推奨する。

- **達成基準**

  ② ″セキュリティ要求事項の評価″とは具体的に何を実施していればよいか？

  セキュリティ要求事項が満たされているかどうかを、国際標準に基づく認証取得の確認や、検収時の受入テスト等が実施できていればよい。
  評価を実施する上で、セキュアな IT 機器調達のためのガイドラインとなる「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」(IPA, 2018 年) の、「2.(1).(b) セキュアな IT 製品を調達するためのフローについて.ガイド②における判断ポイント」に記載されているケース別の具体例が参考となる。
  参考：https://www.ipa.go.jp/files/000038924.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
14 外部への接続状況の把握	外部情報システム利用における安全性と信頼性の確保、および情報セキュリティ事件・事故発生時の迅速な対応を図る	関係組織（サプライヤー等含む）との関係において、自組織の通信ネットワーク構成を把握し、他組織との連携状態やデータの流れを監視すること	74	Lv2	ネットワーク図・データフロー図を作成し、関係組織（サプライヤー等含む）との通信を監視している	【基準】 ・ネットワーク図を作成すること ［対象範囲］ -自社の情報機器が存在するネットワーク ［見直し頻度］ -1 回/年以上 ＜追記＞ 【基準】 ・データフロー図を作成すること ［対象範囲］ -関係組織間のネットワークでやり取りされる自社内のデータ 【基準】 ・関係組織との通信を監視すること ［対象範囲］ -関係組織間のネットワークでやり取りされるデータ ［頻度］ -常時

【解説】

- **達成条件**

① “関係組織との通信を監視”するためには具体的に何を実施すればよいか？

通信を制御する機器(例: ファイアウォール、プロキシサーバー)や、攻撃を検知・防御する機器(例：IPS、IDS)が、自社と関係組織の通信が経由する場所に導入され、それらの機器の通信ログを監視できる体制が構築できていればよい。
体制の構築については、自社で監視体制を構築する方法と、外部のサービスを活用する方法がある。
後者の場合は、専門的な体制や機能を提供する外部サービスの活用やその組み合わせなどを検討し、自社の状況を考慮して導入可能な体制を整備することが重要となる。

- **達成基準**

② ″ネットワーク図を作成すること″、″データフロー図を作成すること″と記載されていることを踏まえると、両方作成しなければいけないのか？

両方必要となる。データの流れだけであれば、「データフロー図」だけでも問題ない。ただし、インターネット空間を通じた通信と閉域網を通じた通信ではリスクの度合いも変わるため、要求事項にある「他組織との連携状態」も含めた監視を行う上ではデータの流れだけでなく、ネットワーク上

どのように接続し、通信が発生しているか、という状況把握も重要となる。

※「制御システムのセキュリティリスク分析ガイド」(2017 年, IPA)の 3.2 及び 3.3 がネットワーク図・データフロー図の作成手順・例示となり、参考とすることができる。
参考：https://www.ipa.go.jp/files/000080712.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
14 外部への接続状況の把握	外部情報システム利用における安全性と信頼性の確保、および情報セキュリティ事件・事故発生時の迅速な対応を図る	外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること	76	Lv1	自組織の資産が接続している外部情報システムの利用ルールを定めている	【規則】 ・以下の内容を含む利用ルールを定めること ・外部情報システムの接続先と守秘義務契約を締結する ・外部の情報サービスを利用する際のセキュリティ要件を定めている ・外部の情報サービスの利用時にセキュリティ要件を満たしているか サービス内容を確認し、承認した証跡を保管している

【解説】

- **達成基準**

  ① “外部の情報サービスを利用する際のセキュリティ要件”は何を参考に定めるのか？

  クラウドサービスを始めとする外部の情報サービスを利用する際のセキュリティ要件は、システムの選択、運用、管理する観点から定めることが望ましい。(以下例示)

  ＜選択する観点＞
  - サービス提供事業者の情報セキュリティ方針と自社のセキュリティ方針の適合
  - サービスの稼働率や障害発生頻度等の信頼性

  ＜運用する観点＞
  - 適切な利用者のみが利用できる認証設定の可否
  - データのバックアップ取得可否

  ＜管理する観点＞
  - セキュリティ対策や機能の有無

・　データ保存先や保存期間の確認

※「中小企業の情報セキュリティ対策ガイドライン」の付録６「中小企業のためのクラウドサービス安全利用の手引き」には、クラウドサービスを安全に利用する為のポイントやチェックリストが解説されており参考になる。
参考：中小企業の情報セキュリティ対策ガイドライン第3.1版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

参考：付録６　中小企業のためのクラウドサービス安全利用の手引き（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
14 外部への接続状況の把握	外部情報システム利用における安全性と信頼性の確保、および情報セキュリティ事件・事故発生時の迅速な対応を図る	外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること	77	Lv1	利用している外部情報システムを一覧化している	【規則】 ・外部情報システムの一覧を作成していること

【解説】

- **達成条件**

  ① “外部情報システムを一覧化”するにあたり、管理すべき項目は何か？

  外部情報システムの一覧を作成することの目的は、組織の人員が利用している情報システムを把握することで、当該システムの利用にリスクが認められた場合に対策を講じることや、情報セキュリティ事件・事故が発生した場合に対応を図ることである。その目的が満たせるような項目が管理されていればよい。(以下例示)

  ＜利用者に関する管理項目＞
  - 利用者名、部署
  - 用途

  ＜外部情報システムに関する管理項目＞
  - システム概要、システム名
  - ベンダー名

  ＜契約に関する管理項目＞
  - 契約書名、契約先名
  - 契約日、契約満了日

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
14 外部への接続状況の把握	外部情報システム利用における安全性と信頼性の確保、および情報セキュリティ事件・事故発生時の迅速な対応を図る	外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること	78	Lv1	外部情報システムの一覧を定期的、または必要に応じて見直ししている	【規則】 ・定期的に棚卸を実施するとともに、新規あるいは利用中止するものを一覧に反映すること 【頻度】 ・1 回／年以上、かつ、新規開始あるいは利用中止時

【解説】

- **達成条件**

  ① “見直し”とは、何が実施されていればよいか？

  本項目の目的は、情報セキュリティ事件・事故発生時に迅速に対応するために、No.77 で作成した外部情報システムの一覧を最新化しておくことである。この目的を踏まえ、次のポイントを押さえて外部情報システムの一覧が棚卸されていればよい。(以下例示)

  - 利用中の外部情報システムの内容を最新に更新する
  - 利用しなくなった外部情報システムの状況を更新する
  - 新たに利用を始めた外部情報システムを追加する

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
15 社内接続ルール	社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する	社内ネットワークへの接続時には、情報システム・情報機器の不正利用を抑制する対策を行っていること	79	Lv1	業務で利用する情報機器の自社ネットワークへの接続ルールを定めている	○PC やサーバーなどの機器の接続ルール 【規則】 ・社内ネットワークへの接続に関するルールを定めること 【対象】 ・社内でネットワークに直接接続するすべての機器 ・会社標準機器、社外からの持ち込み機器含む ○社外から社内ネットワークへ接続するための追加ルール 【規則】 ・リモートアクセスを利用する場合のルールを定めること 【対象】 ・社外から公衆インターネット経由あるいは専用線経由で社内ネットワークに接続する全ての機器

【解説】

- **達成基準**

① “社内ネットワークへの接続に関するルール”を定める際のポイントや例は何か？

社内ネットワークへの接続機器のセキュリティ対策については、「中小企業の情報セキュリティ対策ガイドライン」の付録 3「5 分でできる！情報セキュリティ自社診断」（IPA）などに対策例が書かれており、参考にすることが望ましい。

社内ネットワークへの接続ルールで特に押さえておくべきポイントや対策例としては下記が挙げられる。

- 接続機器のセキュリティ対策の導入　（例：OS パッチやセキュリティ対策ソフトの導入）
- 社内ネットワークに接続できる機器の制限　（例：私有端末の扱い）

※「中小企業の情報セキュリティ対策ガイドライン」では、特に中小企業が情報セキュリティリスクに対して適切に対策を講じるための具体的な手引きを提供している。また、付録 3「5 分でできる！情報セキュリティ自社診断」には、情報セキュリティの診断項目および対策が記載されており参考にすることができる。

参考：中小企業の情報セキュリティ対策ガイドライン第 3.1 版（IPA）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

参考：付録３　５分でできる！情報セキュリティ自社診断（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

② “リモートアクセスを利用する場合のルール”を定める際のポイントや例は何か？

リモートアクセスは、出張先やリモートワークでの利用が考えられる。リモートアクセスは、出張先や自宅から社内ネットワークにアクセスでき、移動時間の削減効果や自宅に居ながらも業務を行う等の柔軟な働き方を実現できるメリットがある。一方で、従業員の自宅等、企業の管理下に無い環境で業務を行うことになり、例えばVPNの脆弱性を悪用したサイバー攻撃の事例が多くある。そのため、リモートアクセスのメリットだけでなく、セキュリティ確保を十分に検討したうえで、リモートアクセスを会社に導入することが求められる。「中小企業の情報セキュリティ対策ガイドライン」（IPA）や「テレワークセキュリティガイドライン」（総務省）などのガイドラインに従い、リモートアクセスを利用する場合のルールを策定することが望ましい。

リモートアクセスを利用する場合のルールで特に押さえておくべきポイントや例としては下記が挙げられる。

- 接続機器のセキュリティ対策の導入　（例：OSパッチやセキュリティ対策ソフトの導入）
- 社外ネットワークから接続できる機器の制限　（例：会社資産、私有物の扱い）
- 接続方法の限定　（例：VPN接続、VDI接続）
- 接続開始の申請・承認

※「中小企業の情報セキュリティ対策ガイドライン」の“より強固にするための方策の(4)テレワークの情報セキュリティ”には、リモートワークにおける情報セキュリティについても記載されており参考になる。
参考：中小企業の情報セキュリティ対策ガイドライン第3.1版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

※「テレワークセキュリティガイドライン」には、リモートワークのために、経営者・システム/セキュリティ管理者・リモートワーク勤務者が実施すべきセキュリティ対策について記載されており参考になる。
参考：テレワークセキュリティガイドライン第5版（総務省）
https://www.soumu.go.jp/main_content/000752925.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
15 社内接続ルール	社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する	社内ネットワークへの接続時には、情報システム・情報機器の不正利用を抑制する対策を行っていること	80	Lv3	許可された機器以外は社内ネットワークに接続できないよう、システムで制限している	【規則】 ・許可された機器以外の接続を検知・遮断する仕組みを導入すること 【対象】 ・社内ネットワークに接続する機器

【解説】

- **達成基準**

  ① “許可された機器以外の接続を検知・遮断する仕組み”の例にはどのようなものがあるか？

  許可された機器以外の接続を検知・遮断するために、接続を許可した機器のみ接続を許可する仕組みが求められる。その仕組みを実現する方法としては、下記が考えられる。

  - 機器認証した機器のみ許可する　　（例：クライアント証明書を用いて認証した機器のみ許可する）
  - 予め登録された MAC アドレスのみ許可する
  - 予め登録された IP アドレスのみ許可する

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
15 社内接続ルール	社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する	リモートワークの環境において、セキュリティ事故(主に情報漏えい、なりすまし)を抑制する対策を行っていること	82	Lv2	リモートワークで使用する情報機器や機密情報の条件についてのルールを定め、運用している	【規則】 ・リモートワークで使用する情報機器や機密情報の条件についてのルールを定め、周知すること ・ルールの遵守状況を確認し、必要に応じて是正すること [周知対象] -リモートワークを行う全ての従業員、派遣社員、受入出向者 [周知のタイミング] -リモートワークの開始前 [ルールの内容] -リモートワークで使用許可する情報機器 ※必要に応じて申請、承認の方法を含む -個人所有端末にダウンロード可能なファイルの機密区分や種類 [ルールの内容、遵守状況の確認頻度] -1 回以上/年

【解説】

- **達成基準**

  ① “リモートワークで使用する情報機器や機密情報”はどういうのがあるか？

  リモートワーク環境においては機密情報の漏洩のリスクが高く、リモートワークで使用する情報機器や取り扱える機密情報を制限することが重要である。そのため、情報機器や機密情報を予め把握する必要がある。

  リモートワーク環境で使用される情報機器には、下記のような例がある。
  - 会社貸与の PC/スマホ/タブレット
  - 私有の PC/スマホ/タブレット
  - 私有のプリンタ

  情報に関する分類は、「機密情報」「業務情報」「公開情報」等があり、「機密情報」には下記のような例がある。
  - 個人情報（顧客、従業員、取引先等）
  - 営業秘密（財務、戦略、人事等）

- 経営情報
- 顧客から預かった非公開情報

② リモートワークで使用する情報機器や機密情報についての“ルール”で定めておくべきポイントや例は何か？

No.79 の解説のとおり、「中小企業の情報セキュリティ対策ガイドライン」（IPA）や「テレワークセキュリティガイドライン」（総務省）などのガイドラインに従い、リモートアクセスを利用する場合のルールを策定することが効果的である。また、リモートワークは、自宅やカフェ等の飲食店での勤務など、場所を問わず働くことができるため、PC 等の情報機器の紛失等による情報漏洩のリスクが高まる。そのため、リモートワークで使用できる情報機器の制限に加え、リモートワークで取り扱う機密情報に関するルールも策定することが考えられる。特に顧客の個人情報等、機密レベルが高い情報については、機密情報漏洩時の影響度が大きいため、リモートワーク環境でアクセスしないようにすることが望ましい。

リモートワークで使用する情報機器についてのルールで定めておくべきポイントとして下記が挙げられる。
- リモートワークで使用できる機器の制限　　（例：会社資産、私有物の扱い）
- 接続機器のセキュリティ対策の導入　　（例：OS パッチやセキュリティ対策ソフトの導入）
- 接続方法の限定　　（例：VPN 接続、VDI 接続）
- 利用状況の把握方法　　（例：VPN ログ監視）

リモートワークで使用する機密情報についてのルールで定めておくべきポイントとして下記が挙げられる。
- リモートワークで取り扱う情報の制限　　（例：顧客の個人情報など機密レベルが高い情報の扱い）

※「中小企業の情報セキュリティ対策ガイドライン」の“5.より強固にするための方策”の“(4)テレワークの情報セキュリティ”には、リモートワークにおける情報セキュリティについても記載されており参考になる。
参考：中小企業の情報セキュリティ対策ガイドライン第 3.1 版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

※「テレワークセキュリティガイドライン」には、リモートワークのために、経営者やシステム・セキュリティ管理者・リモートワーク勤務者が実施すべきセキュリティ対策について記載されており参考になる。
参考：テレワークセキュリティガイドライン第 5 版（総務省）
https://www.soumu.go.jp/main_content/000752925.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
15 社内接続ルール	社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する	リモートワークの環境において、セキュリティ事故(主に情報漏えい、なりすまし)を抑制する対策を行っていること	83	Lv2	リモートワーク遂行上のルールを定め、運用している	【規則】 ・リモートワーク遂行上のルールを定め、周知すること ・ルールの内容や遵守状況を確認し、必要に応じて是正すること [周知対象] -リモートワークを行う全ての従業員、派遣社員、受入出向者 [周知のタイミング] -リモートワークの開始前 [ルールの内容や遵守状況の確認、是正頻度] -1 回以上/年

【解説】

- **達成基準**

① **“リモートワーク遂行上のルールで定めておくべきポイントは何か？**

リモートワークの情報セキュリティ確保のために、No.82 で定めたルールだけでなく、リモートワーク遂行上のルールを定める必要がある。
また、ルールを定めても、実際に人がルールを守らなければ、ルールの効果を発揮されることはない。そのため、リモートワーク勤務者に対する教育や啓発活動でルールの主旨を理解してもらい、ルールを順守することによるメリットを自覚してもらうことも重要となる。
具体的には、「中小企業の情報セキュリティ対策ガイドライン」（IPA）や「テレワークセキュリティガイドライン」（総務省）などのガイドラインを参考に、リモートワーク遂行上のルールを策定することが効果的である。

リモートワーク遂行上のルールで定めておくべきポイントとして下記が挙げられる。

- リモートワークの申請・承認
- リモートワークに関する教育受講
- リモートワークで使用する機器のソフトウェアのアップデートやパッチ適用　（例：OS パッチ）
- リモートワークで利用できるハードウェア/ソフトウェア/サービスの制限

- リムーバブルメディア利用の制限　（例：USB メモリ、CD/DVD）
- プリンタ接続の制限
- インストールするソフトウェア/アプリの制限
- クラウドサービス利用の制限

・　リモートワーク勤務中の行動　（例：機器の携行ルール、PC 画面フィルタ、離席時の PC 画面ロック）
・　情報機器の紛失や機密情報の漏洩が発生した場合の手続き

※「中小企業の情報セキュリティ対策ガイドライン」の“5.より強固にするための方策”の“(4)テレワークの情報セキュリティ”には、リモートワークにおける情報セキュリティについても記載されており参考になる。
参考：中小企業の情報セキュリティ対策ガイドライン第 3.1 版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

※「テレワークセキュリティガイドライン」には、リモートワークのために、経営者やシステム・セキュリティ管理者・リモートワーク勤務者が実施すべきセキュリティ対策について記載されており参考になる。
参考：テレワークセキュリティガイドライン第 5 版（総務省）
https://www.soumu.go.jp/main_content/000752925.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サーバー等の設置エリアには、物理的セキュリティ対策を行っていること	87	Lv2	サーバー等の設置エリアに不正侵入や不審行動を監視している	【規則】 ・入場時、退場時に持込み・持ち出し物を確認すること ・入場者の行動を監視すること

【解説】

- **達成条件**

  ① ″不正侵入や不審行動を監視″する方法は多数存在するが、何を観点に対策を選定するとよいか？

  対策は 3 つに大別される。施設や区画の特性、出入りに係る人流とその量も勘案した上で、最適な対策を選定することが望ましい。(以下例示)

  ＜人的対策＞

  - 持ち物検査
  - 定期的な入退室記録のレビュー

  ＜物理的対策＞

  - 施錠
  - ゲート設置

  ＜技術的対策＞

  - 防犯カメラ
  - 生体認証

② ″サーバー等の設置エリア″について、専用のサーバールーム以外に設置している場合（執務スペースの一角の個室等）、そのようなエリアも対象に含むか？

「サーバー」の定義が重要となる。組織として重要なデータやファイルが保存されており、それがネットワーク通信を介して利用される状況にある場合は、その端末はサーバーに含まれるべきである。例えば、ノート PC であっても、上記に該当する場合はサーバーの位置づけとなる。かつ、それが執務スペースの一角の個室だったとしても、そこは設置エリアとして認識するべきである。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	社内への入退場において、セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること	88	Lv2	入退場に関するルールを定め、周知、運用している	【規則】 ・自社の入退場ルールを定めること ・入退場ルールを周知すること ・入退場ルールの内容や遵守状況を確認し、必要に応じて改定や再周知を行うこと 【周知対象】 ・自社に出入りする全ての人員 【入退場ルールの内容】 ・入場制限エリアの定義 ・入退場時の申請、承認 ・入退場時の身分証明方法(社員証、入場許可証の着用など) ・入場許可証,通門証の発行規則 【入退場ルールの内容や遵守状況の確認、是正頻度】 ・1 回以上/年

【解説】

- **達成基準**

  ① “入場制限エリアの定義”とあるが、定義するための具体的な観点は何か？

  入場制限エリアは、自社の敷地・建物・部屋の単位で検討することが望ましい。例えば、建物の場合、それ自体が秘密情報に該当する製造機器が設置されている工場は不正侵入を抑制するために制限エリアとすることが考えられる。また、部屋の場合、サーバールーム以外にも、自社の情報資産や従業員の個人情報を取り扱う執務室などは制限エリアに含むべきである。また、原則として、外部者が不必要に制限エリアに接近しないルールを定めることが重要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	社内への入退場において、セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること	89	Lv2	重要なエリア、部屋への入場を制限し、入退場記録を保管している	【規則】 ・重要なエリア、部屋の入退場を制限すること ・重要なエリア、部屋への入退場記録を取得し、保管すること 【記録する項目】 ・入退場日時 ・入場者(氏名、所属、連絡先など) ・入場目的 ・承認者 【記録の保管期間】 ・6 ケ月以上

【解説】

- **達成基準**

  ① “入退場記録を取得し、保管する”とあるが、具体的な方法は何か？

  手書きの台帳で記録し保管する方法以外にも、入退室制限と記録の管理を同時に行うことのできるシステムを導入する方法が効率的である。ただし導入や運用には一定のコストがかかるため、自社への導入時には検討が必要である。

  ※「入退管理システムにおける情報セキュリティ対策要件チェックリスト」では、入退管理システムの情報セキュリティを向上させるための要件などが解説されているため、新たに入退管理システムを調達する際には参考となる。
  参考：入退管理システムにおける情報セキュリティ対策要件チェックリスト　第 1 版（IPA）
  https://www.ipa.go.jp/security/jisec/about/knowledge/cdk3vs00000024ph-att/checklist_ecs.pdf

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	社内への入退場において、セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること	90	Lv2	不正侵入や不審行動を監視している	【規則】 ・自社の重要な場所において、不正侵入や不審行動を監視すること ・監視が正常に機能していることを確認し、必要に応じて是正すること 【監視状況の確認、是正頻度】 ・1 回以上/6 か月

【解説】

- **達成条件**

  ① “不正侵入や不審行動を監視”するための対策は何か？

  No. 87 と同様の対策が求められる。(以下例示)

  ＜人的対策＞

  - 持ち物検査
  - 定期的な入退室記録のレビュー

  ＜物理的対策＞

  - 施錠
  - ゲート設置

  ＜技術的対策＞

  - 防犯カメラ
  - 生体認証

・ **達成基準**

② ″自社の重要な場所″とは具体的にどこを指すか？

研究・設計・開発エリアやサーバールーム等、機密情報を扱っているエリアを指す。多くの企業が機密管理に係る規定として、区画の定義を行っているため、そうしたルールに基づいた判断をすることが望ましい（ただし、こうした規定が存在しない場合は、社内の総務関連の組織も含めた確認および定義を行うべき）。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	脆弱性が発見された際の対策対象の把握や外部記憶媒体を用いた情報漏えい等を抑制する対策がおこなえていること	100	Lv2	マルウェアによる被害(データ暗号化等)を受けた場合に業務に支障をきたす重要データについては、PC 以外へ保管するようルールを定め、周知している	【規則】 ・重要データはクライアント PC 以外に保管すること ［周知対象］ -役員、従業員、派遣社員、受入出向者

【解説】

- **達成基準**

① ″重要データ″とあるが、重要かどうかの観点は何か？

達成条件にあるように、業務に支障をきたすか否かがポイントである。これは業種によって異なるが、製造業であれば、生産が止まること、出荷・販売できなくなることが短期的な支障として大きい。加えて、長期的な目線としては、機微な経営データや最新技術等の競争力の源泉につながるようなデータが漏洩した場合、同じく支障として大きい。こうした観点で重要かどうかを判断することが望ましい。

② “クライアント PC 以外”へ保管する理由は何か？

2 つの理由がある。1 つは、従業員が業務で使用する PC は、サーバーと比較して、マルウェア感染等の被害を受ける可能性が高い。そのため、日頃から社内ネットワーク上の安全な区域にあるファイルサーバー環境にデータを保存しておくことが求められる。2 つ目は、バックアップである。重要なサーバー環境は定期的なバックアップを取っており、サイバー攻撃等で被害を受けた場合、バックアップからのデータ復旧が可能となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	重要情報を格納・利用するシステムにおいて、人為的設定ミスによる被害を最小化する対策を実施していること	101	Lv2	サーバーの不要な機能を無効化している デフォルトユーザ ID の利用の停止をしている デフォルトパスワードの変更をしている	【規則】 ・不要サービス、デーモンを無効化すること ・デフォルトユーザ ID の利用を停止すること ・デフォルトパスワードの変更すること

【解説】

- **達成条件**

  ① “デフォルトユーザ ID の利用の停止”をすると、システムが停止するなど影響がある場合も停止すべきか？

  システムに影響が出ないよう回避策を検討した上で、原則停止すること。なぜならば、デフォルトユーザ ID は第三者が容易に知りうる情報であり、不正ログインなどのサイバー攻撃で狙われやすく、リスクが高いためである。

  しかし、回避策の実現可能性や、停止した場合の業務への影響度などを勘案し、どうしても利用を継続しなければならない場合に限り、該当サーバーへは特定の端末からの接続のみ許可するよう制限をかける、特定の他システムからのログインのみ許可するよう制限をかけるなどのリスク低減措置を講じることが必要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	103	Lv2	インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している	【規則】 ・社内と社外のネットワーク通信を制限する仕組みを導入すること [導入場所] -社内外ネットワークの境界 [制限する項目] -接続元および接続先の IP アドレス -通信ポート

【解説】

- **達成基準**

  ① “社内と社外のネットワーク通信を制限”とあるが、どのような観点で制限すればよいか？

  ファイアウォールは、ネットワーク通信を制限する機能であり、社内から社外への通信や社外から社内への通信を制限するものである。原則として、すべての通信を拒否し、必要な通信のみ許可するルールとする必要がある。業務上必要なサービスから必要な通信を検討し、ファイアウォールのルールを確実に設定することが必要になる。例えば、社内から社外への通信は、Web の http/https（ポート番号:80,443)のみに限定する等が考えられる。社外から社内への通信は、自社 Web サイト(ポート番号:443)、メールサーバ（ポート番号:587 等）やリモートアクセス（ポート番号:3389 等)のみに限定する等が考えられる。

  また、ファイアウォールの設置・設定には、情報セキュリティの専門知識が求められるため、セキュリティベンダーにネットワークの脆弱性診断等の相談をすることが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	104	Lv2	ファイアウォールのフィルタリング設定(通信の許可・遮断設定)を記録し、不要な設定がないか定期的に確認している	【規則】 ・社内外ネットワーク通信のフィルタリング設定を記録すること ・定期的に不要なフィルタリング設定がないか確認すること ・不要なフィルタリング設定を削除すること 【記録する項目】 ・申請者、接続元および接続先の IP アドレス、通信方向、プロトコル、ポート番号、利用用途、登録日、有効期限 【確認頻度】 ・1 回/年

【解説】

- **達成基準**

  ① “定期的に不要なフィルタリング設定がないか確認”とあるが、具体的な確認方法や留意点は何か？

  定期的に不要なフィルタリング設定を確認する必要があるのは、ファイアウォールのフィルタリング設定が意図どおりであることを確認するためである。フィルタリング設定の記録と実際のフィルタリング設定内容を比較して、不要な設定が無いか確認することになる。特に、一時的に許可したフィルタリング設定についても記録し管理することが必須である。一時的に許可したフィルタリング設定が放置されると、サイバー攻撃に対して脆弱となるため、不要になったタイミングでフィルタリング設定を即時元に戻すことが望ましい。例えば、外部のベンダーに一時的に許可した設定が、業務終了後にも元の設定に戻されないといったケースがあり、注意が必要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	105	Lv2	リモートアクセスの ID を管理し、不要な ID がないか定期的に確認している	【規則】 ・リモートアクセスの ID の発行・変更・削除は申請・承認制にすること ・定期的に不要な ID がないか確認すること ・不要な ID を削除すること 【確認頻度】 ・1 回/年

【解説】

- **達成条件**

① ″不要な ID″における、不要となる具体的な状況は何か？

社員の退職や休業、出向、異動、等が該当する。ただし、こうした人事的な変更を伴わなくても、組織内の役割変更等において、担当業務が変更になった場合、不要に該当するケースとなる。

② ″不要な ID が無いか定期的に確認″する理由は何か？

不要な ID は管理対象外となりやすく、それが盲点となりリスク発生につながる危険性があるためである。不要な ID を悪用して、内部者の犯行として重要情報の持ち出しにつながるリスクもあれば、外部ネットワークから侵入した攻撃者が不要な ID を乗っ取り、攻撃を仕掛けることもあるため、こうした ID が残留していないか、定期的に確認することが重要となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	106	Lv2	業務およびデータの重要性に応じてネットワークを分離している。	【規則】 ・業務内容やデータ重要性でシステムを分類し、専用のネットワーク毎に設置すること 【対象】 ・社外公開サーバー設置のネットワーク、 PC とサーバのネットワーク、工場ネットワーク／OA ネットワーク等

【解説】

- **達成条件**

① ″ネットワークを分離″とは、具体的にどう分離されていればよいか？

物理的な視点と論理的な視点の双方がある。前者は、文字通り、ネットワーク回線が分かれていることである。後者は、回線上は同一だったとしも、その中を流れるデータが仮想的に別区画として管理されている状態である。(以下例示)

＜物理的な分離＞

- 産業用制御システムが存在する場合、そのネットワークを、情報システムのネットワークと切り離して構成する。

＜論理的な分離＞

- 外部ネットワークに公開されるサーバーは DMZ と呼ばれる仮想的な別セグメントに配置する。
- 同一のハードディスクであっても、その中の区画を分けることで、仮想的な別空間の通信として管理する。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	108	Lv2	不正な Web サイトへのアクセスを制限している	【規則】 ・不正な Web サイトへのアクセスを制限すること 【対象】 -クライアント PC/Web ゲートウェイ

【解説】

- **達成条件**

① “不正な Web サイトへのアクセスを制限”するには、どういったフィルタリング方式を導入すればよいか？

次のような方式のものを導入していればよい。(以下例示)

- Web サイトの URL を予め登録することで制限する方式
- Web サイト内の各ページの内容（コンテンツ）で制限する方式

② “不正な Web サイトへのアクセスを制限”するには、どういった装置・サービスを導入していればよいか？

次のような Web フィルタリング機能を持つ装置・サービスを導入していればよい。(以下例示)

- PC にインストールしたソフトウェアによるフィルタリング
- ネットワーク上に設置されたセキュリティ機器によるフィルタリング（ファイアウォール等）
- クラウドサービスを利用したフィルタリング

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	109	Lv2	インターネットに公開している Web アプリケーションについて WAF(Web Application Firewall)を導入している	【規則】 ・WAF(Web Application Firewall)を導入すること 【対象】 ・重要な社外公開 Web アプリケーション

【解説】

- **達成基準**

  ① 対象となる"重要な社外公開 Web アプリケーション"にはクラウドサービスを利用しているケースを含むか？

  含む。ただし、汎用的なクラウドサービスを活用している場合、WAF の導入を依頼することはサービス利用契約上、困難なケースが多い。そのため、現実的には、契約時にサービス提供側に対して、WAF 導入有無を確認するに留まるケースや SLA（サービスレベルを規定した文書）の確認に留まるケースが多い。反面、自社インフラとしてクラウド環境を整備している場合は、自組織の判断で WAF の導入ができる可能性が高まる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	110	Lv2	インターネットに公開している Web サイト、システムについて、DDoS 攻撃を受けてもサービスを継続するための対策を実施している	【規則】 ・DDoS 攻撃を受けた際にサービスを継続する仕組みを導入すること 【対象】 ・重要な社外公開 Web サイト、DNS サーバー

【解説】

- **達成基準**

  ① 対象となる"重要な社外公開 Web サイト、DNS サーバー"にはクラウドサービスを利用しているケースを含むか？

  含む。ただし、汎用的なクラウドサービスを活用している場合、DDoS 対策の実施を依頼することはサービス利用契約上、困難なケースが多い。そのため、現実的には、契約時にサービス提供側に対して、DDoS 対策有無を確認するに留まるケースや SLA（サービスレベルを規定した文書）の確認に留まるケースが多い。反面、自社インフラとしてクラウド環境を整備している場合は、自組織の判断で DDoS 対策を実施できる可能性が高まる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	111	Lv2	インターネット経由の通信が盗聴、改ざんされないよう、通信を暗号化している	【規則】 ・社内外ネットワーク通信を暗号化すること 【対象】 ・社外から社内へのリモートアクセス通信 ・ユーザーと社外公開サーバーとの間で認証を伴う通信

【解説】

- **達成基準**

  ① 対象となる"社外から社内へのリモートアクセス通信"、"ユーザーと社外公開サーバーとの間で認証を伴う通信"にはクラウドサービスを利用しているケースを含むか？

  含む。汎用的なクラウドサービスを活用している場合、一般的にはサービス提供側で通信の暗号化は実施されている。しかし、使用する暗号技術やその強度の指定まではサービス利用契約上、困難なケースが多い。そのため、契約時にサービス提供側に対して、そうした「暗号化方式」「暗号強度」など詳細を確認の上、可能な限り自社要件に合わせた SLA(サービスレベルを規定した文書)を締結するなどの交渉を行うことが望ましい。
  一方、自社インフラとしてクラウド環境を整備している場合は、自組織で暗号化を実施する必要がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
17 通信制御	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	112	Lv2	端末と無線 LAN アクセスポイントの間の通信を暗号化している	【規則】 ・端末とアクセスポイントの間の通信を暗号化すること ・政府推奨暗号において危殆化している暗号技術は利用しないこと 【対象】 ・社内無線 LAN

【解説】

- **達成基準**

  ① “社内無線 LAN”の環境構築を外部委託するにあたり、その選定における留意点は何か？

  構築後のサポートや信頼関係といった観点も含めて選定することが重要となる。

  本項目に記載されている「端末とアクセスポイント間の通信の暗号化」の設定に関しては、構築時に安全な暗号化方式であっても、技術進歩や脆弱性の発見によって運用中に危険なものとなってしまい、設定変更しなければならないケースが想定される。したがって、そうした構築後の運用中のサポート面まで考慮して選定をする必要がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
18 認証・認可	情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏洩、改ざんを防ぐとともに、情報システムを安定稼働させる。さらに、情報漏えい、改ざんや情報システム停止の際の原因調査を可能にする	情報システム・情報機器への認証・認可の対策を行っていること	116	Lv2	外部情報システムのパスワード設定ルールを定め、周知している	【規則】 ・対象のパスワードを社外 Web サービスで設定しないこと ※同一の認証基盤(SSO 等)の場合は使いまわしに該当しない 【対象のパスワード】 ・PC ログオン時のパスワード ・メールシステムのパスワード(Microsoft 365 など) 【周知対象】 ・役員、従業員、派遣社員、受入出向者

【解説】

- **達成基準**

① “外部情報システムのパスワード設定ルール”はどのような考えで設定すればよいのか？

外部情報システムのパスワード設定ルールについても、No.115 で定めたパスワード設定のルールを適用してよい。なお、パスワード漏洩やセキュリティインシデントが発生した際の影響を最小限にするために、パスワードの使いまわしは確実に避けるようにパスワード設定ルールに反映する必要がある。(以下例示)

- 複数の外部情報システムで、同一のパスワードを使いまわしをしないこと
- 複数人で、同一のパスワードを使いまわしをしないこと

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
18 認証・認可	情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏洩、改ざんを防ぐとともに、情報システムを安定稼働させる。さらに、情報漏えい、改ざんや情報システム停止の際の原因調査を可能にする	情報システム・情報機器への認証・認可の対策を行っていること	120	Lv3	インターネットから利用できるシステムには多要素認証を実装している	【規則】 ・インターネットを経由した認証において、知識、所持、生体のいずれか 2 つ以上の認証を実装すること 【対象】 ・機密レベルが高い情報を取り扱うシステム ・特権アカウント ・リモートアクセス

【解説】

- **達成条件**

① ”インターネットから利用できるシステム”とは、VPN を経由して使用する様な社内システムを対象としているのか、ウェブアプリ等を含むインターネットからアクセス可能なシステム全てを含むのか？

インターネットからアクセス可能なシステム全てを含む。
そのため、社外からアクセスできる Web サイトや、VPN を用いての社内環境への接続も対象となる。
VPN 利用において特にリスクが高いのは社内環境への接続時の認証であるため、ここに多要素認証を実装することが必要となる。
対して、VPN 接続後にアクセスする社内システムへの認証における多要素認証は必須ではなく、システムの重要度に応じて認証の強度を調整することが望ましい。

② ″多要素認証″において、適切な要素の組み合わせはあるか？

要素としては知識、所持、生体の 3 つが考えられる。それら異なる要素の組み合わせによる認証となるように配慮すること。(以下例示)

＜知識認証＞

- ユーザーID とパスワード

＜所持認証＞

- デバイス、ワンタイムパスワード、SMS(ショートメッセージサービス)メール
- 接続制限（IP アドレス、セキュリティトークンなど）

＜生体認証＞

- 指紋、虹彩、静脈

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
18 認証・認可	情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏洩、改ざんを防ぐとともに、情報システムを安定稼働させる。さらに、情報漏えい、改ざんや情報システム停止の際の原因調査を可能にする	情報システム・情報機器への認証・認可の対策を行っていること	121	Lv2	重要システムではセッションタイムアウトを実装している	【規則】 ・重要システムではセッションタイムアウトを実装すること 【対象】 ・社外公開システム、重要な社内システム

【解説】

- **達成条件**

  ① ″セッションタイムアウトを実装″とは具体的に何を指すか。

  Web アプリケーションなどにログインしたあとに、一定時間操作しないままにすると強制的にログアウト状態になる機能を実装することを指す。
  強制ログアウトまでの時間が長いとサイバー攻撃によるリスクが高まるが、その時間が短すぎるとユーザーの利便性を損なう恐れがあるため、システムの重要度を考慮して設定することが望ましい。

- **達成基準**

  ② ″社外公開システム″とは、具体的にどのような状態のシステムを指すか？

  インターネットに公開されているシステムを指す。
  なお、達成基準の規則に記載されている″重要システム″とは上記のシステムと社内の重要システムの両方を含むこととしている。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
19 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	サポート期限が切れた機器、OS、ソフトウェアを利用しないようにしていること	123	Lv2	サポート期限が切れた OS、ソフトウェアを利用しないようにしている	【規則】 ・サポートのある OS、ソフトウェアを利用すること ・やむを得ずサポート切れの OS、ソフトウェアを利用する場合は、できる限り脆弱性悪用のリスクを低減すること 【対象】 ・会社支給のパソコンの OS、ブラウザ、Office ソフト ・サーバーの OS、ミドルウェア ・会社支給のスマートデバイスの OS、アプリ ・インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア

【解説】

- **達成基準**

  ① ″やむを得ずサポート切れの OS、ソフトウェア″の利用を継続しているが、“できる限りの脆弱性悪用のリスクを低減”する対策は何を観点に選定するとよいか？

  ＜点の対策＞

  サポート切れの OS、ソフトウェアの利用を継続している端末(以下、当該端末)そのものの保護を目的として、特定のアプリケーション以外起動できないように制限をかけるツール（例：ホワイトリスト）の導入や、過去事例に基づき、同様の特徴を持つプログラムを検知・防御するツール（例：ウイルス対策ソフト）を導入することが対策として挙げられる。また、必要な通信以外を遮断し保護することを目的に、当該端末の直前に専用のネットワーク機器(ファイアウォール機能)を設置する手段も有効である。

  ＜線の対策＞

  当該端末そのものの保護だけでなく、当該端末と繋がるあらゆる情報資産を横断的に保護することを目的として、ネットワークの分離や、通信を監視して不正な挙動を検知する機器(例：IDS/IPS)を導入することが対策として挙げられる。

  なお、達成条件においては、「サポート期限が切れた OS、ソフトウェアを利用しない」としているが、達成基準においては、そのような場合もリスクを低減することで基準を満たすと記載されている点に留意すること。

② ″やむを得ず″が示す状況は何か？

以下のようなシステムのリプレースができない状況を示す。（以下例示）

- 運用しているシステムの代替機器が無い
- 多大なコストがかかるため、リプレースを実行できていない

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
19 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	脆弱性を利用した不正アクセスを防止する施策を実施していること	124	Lv1	情報システム・情報機器、ソフトウェアへセキュリティパッチやアップデート適用を適切に行っている	【規則】 ・セキュリティパッチやアップデート適用を、規則と期限を定め実施すること ・やむを得ず適用できない場合は、適用対象外の理由を記録すること 【対象】 ・パソコン、スマホ、タブレット、サーバー、ネットワーク機器、ソフトウェア等 -会社支給のクライアント PC の OS、ブラウザ、Office ソフト -サーバーの OS、ミドルウェア -会社支給のスマートデバイスの OS、アプリ -インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア

【解説】

- **達成基準**

  ① “セキュリティパッチやアップデート適用を、規則と期限を定め実施”とあるが、どのように規則を定めればよいのか？

  セキュリティパッチやアップデートは、情報機器やソフトウェアの脆弱性を修正し、サイバーセキュリティの攻撃から保護するために行われる。そのため、サイバーセキュリティの観点では、情報機器やソフトウェアの状態は常に最新に保っておくことが望ましい。情報機器やソフトウェアのセキュリティパッチやアップデートの重要度や緊急性に応じた期限を設定する必要がある。

  規則と期限を定める際のポイントとして下記が挙げられる。

  - No.59 で定めた重要度の高い情報機器やソフトウェアについては、規則や期限が確実に定められているか
  - No.60 で作成した IT 資産一覧の情報機器やソフトウェアが対象として考慮できているか
  - セキュリティパッチやアップデートの重要度や緊急性に応じた規則や期限になっているか

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
19 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	脆弱性を利用した不正アクセスを防止する施策を実施していること	125	Lv2	脆弱性の管理体制、管理プロセスを定めている	【規則】 ・脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること ・脆弱性情報/脅威情報を収集する情報源、ツール、頻度を定めること ・収集した情報の対応要否判断基準・対応手順を定めること ・対応履歴を記録し、月次でチェックすること

【解説】

- **達成基準**

① “脆弱性情報の収集から対応まで担当部署の役割・責任”は、どのように決めればよいのか？

脆弱性情報は、主に No.124 のセキュリティパッチ適用対象の把握のために使用される。また、No.17 で言及している CSIRT 活動で使用されることもある。脆弱性情報を収集する担当部署については、基本的には IT 資産を管理する部署で脆弱性情報を収集することが検討の出発点となるが、会社の規模や事業のバリュエーションや数によっては、統括部門で一元的に脆弱性情報を収集する方が効率的な場合もある。

※「サイバーセキュリティ体制構築・人材確保の手引き」では、サイバーセキュリティに関する体制構築や人材確保に対して、適切な判断を行うためのポイントが解説されている。
参考：サイバーセキュリティ体制構築・人材確保の手引き　第 2.0 版（経済産業省，IPA）
http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

② “脆弱性情報/脅威情報を収集する情報源”とあるが、具体的には何があるか？

具体的には、「JVN iPedia」（IPA）や「重要なセキュリティ情報一覧」（IPA）がある。また、セキュリティベンダーが公開するレポート等で確認することや、平素から付き合いのあるベンダーに相談することも有益である。脆弱性情報の収集目的に応じて使い分けることが望ましい。（以下例示）

- IT 資産ごとに脆弱性情報を調査する場合：　「JVN iPedia」（IPA）
- 緊急性が高い脆弱性や脅威情報を調査したい場合：　「重要なセキュリティ情報一覧」（IPA）

※「JVN iPedia 脆弱性対策情報データベース」は、国内外問わず日々公開される脆弱性情報のデータベースで、IT 資産やその IT 資産を構成するハードウェア/ソフトウェアごとに脆弱性を調査することができる。
参考：JVN iPedia 脆弱性対策情報データベース（IPA）
https://jvndb.jvn.jp/index.html

※「重要なセキュリティ情報一覧」では、不正アクセスや情報漏洩等の危険性が高いセキュリティ情報が発信されている。緊急性が高い脆弱性をいち早く把握したい場合に適している。
参考：重要なセキュリティ情報一覧（IPA）
https://www.ipa.go.jp/security/security-alert/index.html

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
19 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	脆弱性を利用した不正アクセスを防止する施策を実施していること	126	Lv3	社外へ公開しているサーバーについて、本番稼働前および稼働後に脆弱性診断を実施し、判明した脆弱性に対して対策を行っている	【規則】 ・プラットフォームの脆弱性を診断すること ・脆弱性に対する対応の要否判断規則とリードタイムを決めること ・診断結果と対応結果を保管すること 【対象】 ・社外公開サーバーの OS、ミドルウェア 【診断頻度】 ・本番稼働前：1 回以上 ・本番稼働後：2 回/年およびシステムの大きな変更時 ・影響の大きな脆弱性が公開された時

【解説】

- **達成条件**

  ① ″脆弱性診断″とは何を行っていればよいか？

  まず、脆弱性診断とは自社のシステムに対して、設定ミスや不具合などによって不正アクセスや情報漏洩などの脅威が顕在化するリスクが存在しないか確認することを指す。

  その中でもプラットフォームの診断はサーバーの OS やミドルウェアを対象とし、システムに対する疑似攻撃や設定値のチェックによってリスクを洗い出すものである。加えて、洗い出されたリスクを分析し、その評価結果に応じて対応策をとることが重要である。

  また、診断対象の OS に Web アプリケーションを稼働させている場合は、併せてNo.128 のような診断を行うことが一般的である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
19 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	脆弱性を利用した不正アクセスを防止する施策を実施していること	128	Lv2	インターネットに公開している Web アプリケーションについて、アプリケーション脆弱性診断を実施している	【規則】 ・Web アプリケーションの脆弱性を診断すること ・脆弱性に対する対応の要否判断規則とリードタイムを決めること ・診断結果と対応結果を保管すること 【対象】 ・重要な社外公開 Web アプリケーション 【診断頻度】 ・本番稼働前：1 回以上 ・本番稼働後：アプリケーションの大きな変更時

【解説】

- **達成条件**

  ① ″アプリケーション脆弱性診断″とは何を行っていればよいか？

  まず、脆弱性診断とは、自社のシステムに対して、設定ミスや不具合などによって不正アクセスや情報漏洩などの脅威が顕在化するリスクが存在しないか確認することを指す。

  その中でもアプリケーション診断は Web アプリケーションを対象とし、システムに対する疑似攻撃や設定値チェック、プログラムの解析によってリスクを洗い出すものである。加えて、洗い出されたリスクを分析し、その評価結果に応じて対応策をとることが重要である。

  また、このアプリケーションが稼働しているプラットフォームについても併せて№126 のような診断を行うことが一般的である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
21 オフィスツール関連	不正アクセスやマルウェア感染のリスクを低減する	情報システム・情報機器のデータ保護を行っていること	131	Lv2	メール送信による情報漏えいを防止するための対策を実施している	【規則】 ・機密情報をメール送信する場合は、情報漏えい対策を実施すること

【解説】

- **達成条件**

  ① ″メール送信による情報漏えいを防止″する方法は様々なものが存在するが、何を観点に対策を選定するとよいか？

  次のような送信フェーズを観点に対策を選定するとよい。(以下例示)

  ＜送信前＞

  - 情報漏洩に関する教育

  ＜送信時＞

  - 誤送信を防止する仕組みの導入(宛先の複数回確認、遅延送信)
  - 添付ファイルの暗号化
  - メール本文暗号化

  ＜送信後＞

  - 通信の暗号化

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
21 オフィスツール関連	不正アクセスやマルウェア感染のリスクを低減する	情報システム・情報機器のデータ保護を行っていること	132	Lv2	メールの誤送信を防止する対策を実施している	【規則】 ・メールの誤送信を防止する対策を実施すること 【対象】 ・社外宛ての送信メール

【解説】

- **達成条件**

  ① ″メールの誤送信を防止する対策″とは、具体的に何を指すか？

  対策としては、教育による啓発とシステム機能の活用の 2 つが考えられる。ただし、本項目はラベル欄にある通り、「ツール関連」であるため、後者の対策が必要となる。具体的には、次のようなシステム機能を利活用することが望ましい。(以下例示)

  - 送信先に社外アドレスが含まれる場合は、最終確認のウインドウを表示し、間違いがないかどうかの確認を促す機能。
  - 添付ファイルが含まれる場合は、事前登録済みの上位者の承認後に、メールが社外に送信される機能。
  - 送信ボタンを押下後、一定時間が経過してからメールが外部に送信される機能（その間に送信の差戻しが可能)。

- **達成基準**

  ② 本項目は、重要情報を送付するメールのみを対象としてよいか？

そうした対応が可能であれば、問題ない。ただし、現実的には添付ファイルが重要情報であるかどうかを判定することは難しいため、機能によっては、特定の条件下での添付ファイルのみを対象とする、という濃淡をつけることは一案として考えられるものの、全ての添付ファイルが対象になるという仕様にならざるを得ない機能も出てくると考えられる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	136	Lv1	パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア(ウイルス対策ソフト)を導入している	【規則】 ・パソコン、サーバーごとにウイルス対策ソフトを導入すること ・機器に応じた適切なスキャン範囲と頻度を規定し、スキャンを実行すること 【対象】 ・ネットワークに接続している全てのパソコン、サーバー

【解説】

- **達成条件**

  ① “ウイルス対策ソフト”として EPP: Endpoint Protection Platform と EDR: Endpoint Detection and Response が存在するが、導入するのはどちらでも問題ないか？

  本項目の達成条件としては、EPP のみで十分である。EPP とはパターンマッチング技術により「既知」のマルウェアに対して感染する前に防御することを目的として製品である。一方、EDR とはサイバー攻撃者の動き(ふるまい)や、「既知」・「未知」に関わらずマルウェアによる攻撃の動き(ふるまい)を検知し、アラートを上げる仕組みである。

  ただし、昨今のサイバー攻撃においては、最低限の対策として EPP および EDR による多層防御の仕組みが必要であり、どちらかだけでは対策として不十分である。(EDR の導入については、No138 が該当項目となる。) 本項目の達成条件においてはマルウェア感染を検知・通報するソフトウェアを導入することと記載されているが、目的においてはマルウェア感染による情報漏洩、改ざん、システム停止を防ぐと記載されているため、目的の意図を鑑みて上記のように防御を意識することが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	137	Lv1	ウイルス対策ソフトのパターンファイルは常に最新化している	【対象】 ・No.136 の対象のとおり 【パターンファイルの更新頻度】 ・起動し利用する日ごとに１回 以上

【解説】

- **達成条件**

  ① 本項目は、EPP: Endpoint Protection Platform が導入されている場合のみ評価すればよいか？

  導入されている EPP の機能によって異なる。

  EPP には一般的にアンチウイルス、次世代形アンチウイルスの 2 種類が存在する。

  アンチウイルスと呼ばれるような、過去に発生した攻撃と同様の特徴を持つプログラムを検知・防御する製品は、マルウェアの検知率を上げるためにパターンファイルの最新化が重要であるため、本項目の対象となる。

  一方、次世代型アンチウイルスと呼ばれるような、人工知能を活用し、予測的に悪意のあるプログラムを検知・防御する製品は、パターンファイルそのものが存在しないため、本項目の対象外となる。

  なお、次世代型アンチウイルスは、搭載される人工知能の更新が必要とされる場合もあり、そうした場合は、ベンダーからの情報を基に更新の必要性を検討することが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	138	Lv3	エンドポイントでの詳細な履歴取得およびマルウェア感染後の遠隔対応が可能な行動追跡システムを導入している	【規則】 ・エンドポイント対策システムを導入すること 【対象】 ・会社支給のクライアント PC ・サーバー 【システム要件】 ・端末の操作履歴、プログラムの実行履歴、レジストリの変更履歴を取得できること ・遠隔から端末の調査ができること ・遠隔からネットワークからの切断ができること ・感染後の復旧対応ができること

【解説】

- **達成条件**

  ① ″詳細な履歴取得およびマルウェア感染後の遠隔対応が可能な行動追跡システム″として何を導入する必要があるか？

  達成基準にあるシステム要件を満たすような、各種ログ取得や端末の遠隔操作ができるツールを導入すればよい(EDR: Endpoint Detection and Response、等)。

  各種ログが取得できるだけではなく、遠隔からの端末調査やネットワーク切断ができることがマルウェア感染後の対応として重要なポイントであるため、ログ取得を行うだけのツールでは基準に満たないことには注意すること。

  ※本項目達成の一助になるサービスとして IPA のサイバーセキュリティお助け隊サービスなどがある。

  参考：https://www.ipa.go.jp/security/otasuketai-pr/

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	139	Lv2	メールによるマルウェア感染を防止するため、メールゲートウェイでのマルウェアチェックを実施している	【規則】 ・メールゲートウェイにマルウェアチェック機能を導入すること

【解説】

- **達成基準**

  ① “マルウェアチェック機能”には、一般的にどのような機能が含まれていればよいのか？

  メールゲートウェイのマルウェアチェック機能は、メールに仕掛けられたマルウェアへの感染を未然に防止することが目的であるが、メールを悪用したセキュリティリスクには、スパムメールやフィッシング攻撃もある。そのため、メールゲートウェイには、メールの包括的なセキュリティ機能が提供されていることが望ましい。以下のような機能があることが一般的である。(以下例示)

  - スパムメールのフィルタリング　(スパムメール対策)
  - メールの添付ファイルのスキャンや除去　(マルウェア感染対策)
  - メール内のリンクのスキャンや除去　(フィッシング攻撃対策)

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	140	Lv2	メールの添付ファイルによるマルウェア侵入を防止するため、システムで拡張子制限を実施している	【規則】 ・メールゲートウェイに特定の拡張子を制限する機能を導入すること

【解説】

- **達成基準**

  ① “拡張子を制限”とあるが、どのような拡張子を制限すればよいのか？

  ファイルを開くと実行される形式のファイル拡張子が、マルウェア感染に悪用されているケースが多く、メールゲートウェイのベンダーがマルウェア感染に悪用された実例があるファイル拡張子を調査したうえで制限リストに反映していることが多い。但し、個社の業務で普段利用しない拡張子が他にある場合は、制限リストに追加することが望ましい。

  例えば、下記のような拡張子が制限されるケースがある。(以下例示)

  「.exe, .pif, .scr, .bat, .com, .lnk, .cmd, .vbs, .cpl, .hta, .shs, .url, .desklink, .mapimail」

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	141	Lv2	不正な Web サイト閲覧によるマルウェア感染を防止するため、Web ゲートウェイでのマルウェアチェックを実施している	【規則】 ・Web ゲートウェイにマルウェアチェック機能を導入すること

【解説】

- **達成条件**

  ① “Web ゲートウェイ”とは何か？

  社内のネットワーク環境からインターネットの Web サイトにアクセスするための通信が経由し、その通信が正しいかどうかの監視、及び危険な通信であればそれを制限する役割を持った機器のことを指す。一般にインターネットとの出入口に設置され、本項目で求められるようなマルウェアチェック機能や、No.108 にある Web アクセス制限機能を導入するのに適している。

- **達成基準**

  ② ″Web ゲートウェイにマルウェアチェック機能を導入する″とあるが、マルウェアチェック機能とはどのような機能か？

  過去に発生した攻撃と同様の特徴を持つプログラムを検知・防御する機能のことである。

  さらに隔離された安全な環境で不審なプログラムを動作させ、その挙動を基に安全性を判断する機能や、PC 上でプログラムの挙動を監視し不審な挙動を検知するような機能を併せて導入することが、多層防御の観点で有効性が高い。このような機能はアンチウィルスゲートウェイと呼ばれ、専用の機器の設置やソフトウェアのインストール、クラウド型サービスなど様々な導入方法があるため、自社の状況とコスト、機能性などを考慮して選定することが望ましい。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
23 不正アクセスの検知	不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ	ネットワークへの不正アクセスを常時監視する体制を構築すること	142	Lv2	通信内容を常時監視し、不正アクセスや不正侵入をリアルタイムで検知/遮断および通知する仕組みを導入している	【規則】 ・不正アクセスをリアルタイム検知・遮断する仕組みを導入すること 【対象】 ・インターネットから社内への通信 ・社内から不正なサーバーへの通信 【導入場所】 ・社内外ネットワークの境界

【解説】

- **達成条件**

  ① ″通信内容を常時監視し、不正アクセスや不正侵入をリアルタイムで検知／遮断及び通知する仕組み″とは具体的に何を指すか？

  不正アクセスや不正侵入の際に発生するようなネットワーク上で発生する異常な通信やそのログを 24 時間監視する機器を導入することを指す。具体的には、不正アクセスや不正侵入を検知・遮断する機器(IPS、IDS)や、No.145 の解説に記載がある SIEM の導入が挙げられる。

  ただし、SIEM や IDS には自動で不正な通信を遮断する仕組みはないため、それらの通知を受けて、遮断要否を判断し対応する運用・体制が整っていることが必要である。

  なお、SIEM の導入方法についてはNo.145 の解説に記載があり、運用体制の整備方法についてはNo.17 の解説に記載がある。どちらについても、自社で実施する方法と外部サービスを活用する方法の 2 つがあり、自社の状況を考慮して実現可能な実施策をとることが重要となる。

- **達成基準**

  ② “社内外ネットワークの境界”とは具体的にどこを指すか？また、なぜそこが重要か？

インターネットと社内環境の間の出入口のことを指す。そこに設置されたファイアウォールやプロキシサーバー等の機器と①で解説した製品・サービスを連携させることが重要となる。なぜかというと、この”社内外ネットワークの境界”は社内環境とインターネットとの通信が経由する、リスクの高い場所であり、不正侵入の検知や遮断の仕組みを導入することで効果的にリスクを減らすことができるためである。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
23 不正アクセスの検知	不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ事件・事故が発生した場合に、侵入経路や漏えい経路の調査が行えるよう、ログが取得されていること	143	Lv2	インシデント発生時の調査のために必要なログを取得している	【規則】 ・下記ログを取得、保管している ［取得するログ(保管期間)］ -メールの送受信ログ(6 カ月) 取得項目：日時、宛先メールアドレス、送信元メールアドレス -ファイアウォールのログ(6 カ月) 取得項目；日時、送信元 IP アドレス、送信先 IP アドレス -プロキシサーバーのログ(6 カ月) 取得項目：日時、リクエスト元 IP アドレス、URL -リモートアクセスのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザーID -認証サーバーのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザーID、成功/失敗 -エンドポイント（パソコン、サーバー）の操作ログ（6 ヶ月） 取得項目：日時、ホスト名、ユーザーID、IP アドレス、操作内容 ※クラウドサービスの利用も対象に含む ※クラウドサービスを利用しており保管期間の規則を満たせない場合はリスクに応じて期間を各社で判断

【解説】

- **達成基準**

  ① “ログを取得、保管”する具体的な方法は？

  ログの保管については、ログが発生する機器で保管しておく方法や、ログ管理システムに集約して一元管理する方法がある。ログはインシデント発生時の調査のために用いられるため、ログの不正アクセス対策や改ざん対策をした状態で保管する必要がある。そのため、ログが発生する機器だけではなく、不正アクセス対策等のセキュリティ対策をしたログ管理システムにログを保管することが望ましい。

  ※ログの取得や保管の方法の一助として、下記サイトが参考になる。
  参考：情報管理担当者の情報セキュリティ対策＞ログの適切な取得と保管（総務省）
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_22.html

② “ログを取得、保管”することについて、保管時の留意点はあるか？

ログを保管する際の留意点として、解説の①で記載したログの不正アクセス対策や改ざん対策に加え、収集・保管するデータによっては、プライバシー性を考慮する必要がある。例えば、メール送受信やパソコン操作ログ等のデータもログとして保管する場合、データを収集・保管することに対する同意取得等のプライバシー対応が必要になることに注意が必要である。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
23 不正アクセスの検知	不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ事件・事故が発生した場合に、侵入経路や漏えい経路の調査が行えるよう、ログが取得されていること	144	Lv3	重要なシステムについて、アプリケーション操作ログを取得している	【規則】 ・ユーザー、管理者の操作ログを取得すること ［対象］ -重要なシステム　※対象はリスクに応じて各社判断 ［取得するログの項目］ -ユーザーID、タイムスタンプ、操作内容(ログイン、ログアウト、追加・削除などの操作) ［保管期間］ -6 カ月 ※クラウドサービスを利用しており保管期間の基準を満たせない場合はリスクに応じて期間を各社で判断

【解説】

- **達成条件**

  ①　“重要なシステム”とは何か？

  重要なシステムは、No.59 の解説のとおり、そのシステムが侵害された場合のビジネスへの影響度に応じて設定されるものであり、自社で選定するものである。また、No.143 や No.144 のログを保管するサーバーも、インシデント発生時の調査に用いられセキュリティ上重要なシステムであるため、重要なシステムと捉えるべきである。

- **達成基準**

  ②　“ユーザー、管理者の操作ログを取得”する理由は何か？

  インシデントの調査、セキュリティ監査等で、不正な操作が行われていないかを確認するために、ユーザー/管理者の操作ログを確認することがある。特に管理者は、変更や削除可能な権限を持っていることが多く、ログの調査や分析で有用となる。そのため、ユーザー/管理者の操作ログを取得・保管することが重要になる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
23 不正アクセスの検知	不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ	標的型攻撃など、サイバー攻撃による被害を抑制させるため、サイバー攻撃を速やかに検知、遮断する対策を行っていること	145	Lv2	ログを分析し、サイバー攻撃を検知する仕組みを導入している	【規則】 ・ログを常時分析し、異常発見時に通知する仕組みを導入すること [分析対象] -プロキシサーバー、IPS/IDS、ファイアウォール、エンドポイントのいずれか、または組み合わせ [監視時間] -24 時間/365 日 [機能要件] -インシデントアラートが即時発報されること -インシデントの速報レポートが作成され、通知されること

【解説】

- **達成条件**

  ① ″ログを分析し、サイバー攻撃を検知する仕組み″を導入するには、どのような手段があるか？

  様々なネットワーク・セキュリティ機器からあげられるログ情報の関連性を横断的に分析する SIEM(System Information and Event Management)と呼ばれる製品やサービスを導入することが一般的である。自社で体制を構築することも可能だが、監視・分析体制を提供しているベンダーのサービスを活用する方法がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
23 不正アクセスの検知	不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ	標的型攻撃など、サイバー攻撃による被害を抑制させるため、サイバー攻撃を速やかに検知、遮断する対策を行っていること	147	Lv3	インターネットに公開している Web サイトについて、サイトの改ざんを検知する仕組みを導入し、定期的に確認している	【規則】 ・Web サイトの改ざんを検知する仕組みを導入すること 【対象】 ・重要な社外公開 Web サイト

【解説】

- **達成条件**

  ① ″サイトの改ざんを検知する仕組み″とは具体的に何を指すか？

  Web サイト上のファイルが改ざんされた際に、改ざんが行われたことをツールや運用上の工夫等で検知することを指す。そのようなツールとしては、ファイルそのものの差分比較により検知するものや、過去の攻撃事例と比較し、同様である場合に検知するもの等、様々存在する。運用上の工夫としては、Web サイト上のファイルが更新された際に管理者に連絡する方法が上げられる。これらの仕組みの実現方法によっては、Web サイト管理者との連携の重要性が増し、負荷が高まる可能性もあるため、Web サイトの重要度や更新頻度等を鑑みた上で検討することが望ましい。また、様々なベンダーから Web 改ざん検知がサービスとして提供されているため、そのようなサービスの導入も一つの手段となる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
24 バックアップ・復元（リストア）	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	148	Lv1	適切なタイミングでバックアップを取得している	【規則】 ・取得対象、取得頻度を定めてバックアップを取得すること

【解説】

- **達成基準**

① “取得対象、取得頻度”はどのような考えで定めればよいか？

バックアップの取得対象や取得頻度を定めるうえで、システム停止やデータ消失時にビジネスに与える影響等の重要性や、データの更新頻度やバックアップのコストが考慮すべきポイントとなる。

- システム/データの重要性　（例：基幹システム、顧客情報、経営情報）
- システム/データの更新頻度　（例：更新頻度が高いソフトウェアやデータは取得頻度も高める）
- バックアップのコスト　（例：バックアップのデータ量や費用に応じて取得頻度を調整する）

② “取得対象、取得頻度”や“バックアップを取得”について、具体例はどのようなものがあるか？

取得対象、取得頻度やバックアップ方法については、下記のような例がある。

【取得対象、取得頻度の例】

・　ファイルサーバーに保存された文書や設定情報　（取得頻度：文書は日次、設定情報は月次）
・　メールサーバーに保存されたメールや設定情報　（取得頻度：メールは日次、設定情報は月次）

【バックアップ方法の例】
・　バックアップサーバーの活用
・　外部記録メディアに保管

※バックアップの考え方やバックアップ方法の一助として、下記サイトが参考になる。
参考：情報管理担当者の情報セキュリティ対策＞バックアップの推奨（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_10.html

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
24 バックアップ・復元（リストア）	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	149	Lv1	復元（リストア）手順を整備している	【規則】 ・バックアップ対象ごとにリストア手順書を整備すること

【解説】

- **達成条件**

  ① ″復元（リストア）手順″の整備には、クラウドサービスを利用しているケースを含むか？

  含む。汎用的なクラウドサービスを活用している場合、一般的にはサービス提供側で復元（リストア）の実施体制や、手順が確立されている。しかし、バックアップから復元するまでの目標時間や、どの時点までのデータを復元するかといった復旧レベルを指定することはサービス利用契約上、困難なケースが多い。そのため、契約時にサービス提供側に対して、そうした「目標復旧時間」「目標復旧レベル」など詳細を確認の上、可能な限り自社要件に合わせた SLA（サービスレベルを規定した文書）を締結するなどの交渉を行うことが望ましい。

  一方、自社インフラとしてクラウド環境を整備している等で、自組織が復元（リストア）を実施できる場合は、そのための手順の整備をする必要がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
24 バックアップ・復元（リストア）	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	150	Lv1	システムが停止した際も業務が遂行できる代替手段を用意している	【規則】 ・システム利用不可能時を想定した、実施可能な代替手法を整備すること ［対象］ -高い可用性が求められる（稼働停止許容時間が短い）システム ※対象はリスクに応じて各社判断 ［対策例］ -アナログツールの利用（FAX など） -クラウドサービスなどの外部情報システムの利用

【解説】

- **達成基準**

  ① “実施可能な代替手段”はどのような方法があるか？

  会社がサイバー攻撃を受けた場合は、社内ネットワーク内の情報システムが使えなくなることを想定しておく必要がある。代替手法は当該システムから物理的または論理的に分離された手法を選定することが望ましい。システムの停止時に備え、下記のような検討が求められる。

  - 人手による業務継続方法の検討　　（例：発注システム停止時に、電話や FAX で注文を受ける）
  - システム継続手法の検討　　（例：メインシステム停止時に、バックアップシステムに切り替える）
  - コミュニケーションに関わる代替手法の検討　　（例：予め複数の通話手段を確保しておく）

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
24 バックアップ・復元（リストア）	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	151	Lv2	重要なデータやシステムについてバックアップの復元(リストア)テストを実施している	【規則】 ・定めた復元手順により、復元ができることを確認すること 【対象】 ・重要なデータ・システム 【頻度】 ・システム構築時、変更時、定期的（リスク応じて判断）

【解説】

- **達成条件**

  ① ″重要なデータやシステムについてバックアップの復元(リストア)テスト″の実施には、クラウドサービスを利用しているケースを含むか？

  含む。汎用的なクラウドサービスを活用している場合、一般的にはサービス提供側で復元(リストア)の実施体制構築や、テスト実施が行われている。しかし、バックアップから復元するまでの目標時間や、どの時点までのデータを復元するかといった復旧レベルを指定し、それに応じたテストの実施を依頼することはサービス利用契約上、困難なケースが多い。そのため、契約時にサービス提供側に対して、そうしたテスト実施条件など詳細を確認の上、可能な限り自社要件に合わせた SLA(サービスレベルを規定した文書)を締結するなどの交渉を行うことが望ましい。
  一方、自社インフラとしてクラウド環境を整備している等で、自組織が復元(リストア)を実施できる場合は、既存サービスへの影響を考慮しつつ、テストを実施する必要がある。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
24 バックアップ・復元（リストア）	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	152	Lv2	サーバー等の設置エリアには、設備に災害対策、環境対策を実施している	【規則】 ・火災、水害、停電に対する対策を行うこと ・温湿度管理を行うこと

【解説】

- **達成条件**

① ″災害対策、環境対策″の実施には、クラウドサービスを利用しているケースを含むか？

含む。汎用的なクラウドサービスを活用している場合、一般的にはサービス提供側で災害対策や環境対策は実施されている。しかし、想定する災害の規模や、実施すべき具体的な対策内容などの詳細を指定することはサービス利用契約上、困難なケースが多い。そのため、契約時にサービス提供側に対して、そうした実施されている具体的な対策内容など詳細を確認の上、可能な限り自社要件に合わせた SLA(サービスレベルを規定した文書)を締結するなどの交渉を行うことが望ましい。

一方、自社インフラとしてクラウド環境を整備している場合は、自組織で災害・環境対策を実施する必要がある。

② ″サーバー等の設置エリア″とは、専用のサーバールーム以外に設置している場合（執務スペースの一角の個室等）、それらも対象に含むか？

「サーバー」の定義が重要となる。組織として重要なデータやファイルが保存されており、それがネットワーク通信を介して利用される状況にある場合は、その端末はサーバーに含まれるべきである。例えば、ノート PC であっても、上記に該当する場合はサーバーの位置づけとなる。かつ、それが執務スペースの一角の個室だったとしても、そこは設置エリアとして認識するべきである。

連絡先:一般社団法人　日本自動車工業会　安全・環境領域

〒105-0012　東京都港区芝大門一丁目 1 番 30 号　日本自動車会館
TEL:03-5405-6125　　FAX:03-5405-6136