

サプライチェーン強化に向けたセキュリティ対策
評価制度（SCS 評価制度）
★3・★4 自己評価等ガイド

2026 年 10 月 28 日

SCS 評価制度 制度運営機関

目次

第1章	はじめに	4
1.1	本ガイドの位置づけ	4
1.2	用語定義	4
第2章	取得単位及び適用範囲の決定	4
2.1	取得単位及び適用範囲の決定に係る実施プロセス	4
2.2	★3 確認責任者又は評価機関による妥当性の確認を要する事項	4
第3章	アセスメントシート等の取扱い	8
3.1	アセスメントシートの位置づけ及び見方	8
3.1.1	アセスメントシートの位置づけ	8
3.1.2	アセスメントシートの見方	9
3.2	アセスメントシートの使用方法	10
3.3	アセスメントシート記入後のエビデンス保持	12
第4章	★3 における確認の実施	14
4.1	★3 における確認の位置づけ及び実施内容	14
4.2	★3 確認責任者が自己評価結果の確認を行う場合の留意点	15
別紙	自己評価における適合基準等	16
1.	ガバナンスの整備	18
1-1	組織の状況	18
1-2	役割、責任、権限	20
1-3	ポリシー	25
1-4	監督	27
2.	取引先管理	29
2-1	サイバーセキュリティサプライチェーンリスクマネジメント	29
3.	リスクの特定	35
3-1	資産管理	35
3-2	リスクアセスメント	47
4.	攻撃等の防御	49
4-1	アイデンティティ管理、認証、アクセス制御	49
4-2	意識向上とトレーニング	72
4-3	データセキュリティ	77
4-4	プラットフォームセキュリティ	83
4-5	技術インフラのレジリエンス	96
5.	攻撃等の検知	100
5-1	継続的監視	100
5-2	有害事象の分析	104
6.	インシデントへの対応	106

6-1	インシデント管理.....	106
7.	インシデントからの復旧	109
7-1	インシデント復旧計画の実行	109

第1章 はじめに

1.1 本ガイドの位置づけ

本ガイドは、「サプライチェーン強化に向けたセキュリティ対策評価制度」（以下「SCS 評価制度」又は「本制度」という。）における★3 又は★4 の登録希望組織又は登録組織が行う取得単位及び適用範囲の決定、同組織が行う自己評価、並びに★3 確認責任者等が行う確認に関する手続きを示すものである。

1.2 用語定義

本ガイドで使用する用語は、特段の定めがない限り、「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）基本規程」（以下「基本規程」という。）において使用する用語による。

なお、本ガイドにおいて、「文書」「記録」「台帳」「一覧」「申請・承認」には、情報システム上の設定、登録情報、ワークフローの記録、ログ、管理ツール及びそれらの画面表示や出力（スクリーンショット、CSV 等）を含む。

第2章 取得単位及び適用範囲の決定

2.1 取得単位及び適用範囲の決定に係る実施プロセス

登録希望組織は、自己評価等に先立ち、取得単位及び適用範囲を自らの責任と判断においてあらかじめ定める必要がある。取得単位及び適用範囲の考え方、設定事例については、

「★3・★4 要求事項・評価基準 解説書」の第3章を参照されたい。

2.2 に示す通り、原則として、取得単位は法人又は個人事業主単位とする。事業部単位、企業グループ単位など取得単位を法人単位としない場合は、取得単位について、★3 確認責任者又は評価機関による妥当性の確認を受ける必要がある。また、登録希望組織は、取得単位に基づき設定した適用範囲について、★3 の登録に際しては★3 確認責任者、★4 の登録に際しては評価機関による妥当性の確認を受ける必要がある。

登録希望組織は、取得単位及び適用範囲について、★3 の登録に際しては★3 確認責任者、★4 の登録に際しては評価機関との間で合意した場合、文書確認等の後続の段階へ進むことができる。

2.2 ★3 確認責任者又は評価機関による妥当性の確認を要する事項

登録希望組織が定めた取得単位及び適用範囲の妥当性を確かめるために、★3 確認責任者又は評価機関は以下の事項について登録希望組織から適宜必要な情報の提供を受けつつ確認を行わなければならない。

(取得単位に関して確認を要する事項)

- 取得単位を法人又は個人事業主単位としていることを確認する。
- 事業部単位等、法人の一部を取得単位とする場合、以下を確認することで取得単位を事業部単位とすることに合理性があるかを確認する。
 - ・ 事業部、事業所や部署等の組織区分及び当該組織区分におけるサイバーセキュリティ対策の責任者が明確になっているか
登録希望組織は、アセスメントシート等の「適用範囲に係る質問事項」において、取得単位とする組織区分及び当該組織区分におけるサイバーセキュリティ対策の責任者の設置状況を回答する。
★3 確認責任者又は評価機関は、登録希望組織から提供を受けたアセスメントシート等の記入内容を確認し、サイバーセキュリティ対策の責任者が明記され、当該責任者が取得単位の組織区分に所属する者であることを確認する。
 - ・ 対象の事業部等は存立期間の定めのない（時限的なものではない）組織であるか
★3 確認責任者又は評価機関は、登録希望組織から提供を受けたアセスメントシート等の記入内容を確認し、登録希望組織が取得単位とする組織区分がプロジェクト等の時限的なものでないことを確認する。
- 企業グループ単位等、取得単位に複数の法人を含む場合、以下を確認することで取得単位を企業グループ単位とすることに合理性があるかを確認する。
 - ・ 取得単位に含まれる法人全てで共通の IT 基盤を利用しているか
登録希望組織は、アセスメントシート等の「適用範囲に係る質問事項」において、取得単位に含まれる法人全てにおいて共通の IT 基盤を利用しているかを回答する。その際、当該 IT 基盤に加え、法人ごとに独自のシステム等を使用することを妨げるものではない。
★3 確認責任者又は評価機関は、登録希望組織から提供を受けたアセスメントシート等の記入内容を確認し、取得単位に含まれる法人全てにおいて共通の IT 基盤を利用している点が記載され、「★3・★4 要求事項・評価基準 解説書」の 3.3 で例示するような取得単位、適用範囲及び適用範囲外との境界を示す概要図や組織体制図等に当該 IT 基盤が明記されていることを確認する。
 - ・ 共通のセキュリティ対応方針等が適用されているか
登録希望組織は、アセスメントシート等の「適用範囲に係る質問事項」において、取得単位に含まれる法人全てにおいて共通のセキュリティ対応方針が適用されているかを回答する。その際、当該方針に加え、法人ごとの事情に応じて独自の個別規程を定めることを妨げるものではない。
★3 確認責任者又は評価機関は、登録希望組織から提供を受けたアセスメントシート等の記入内容を確認し、共通のセキュリティ対応方針が適用されている点が記載されているかを確認する。

(適用範囲に関して確認を要する事項)

1. 取得単位を踏まえた適用範囲の確認

適用範囲が、取得単位となる組織が利用する IT 基盤を含み、かつ当該組織が管理する資産のうち適用範囲から除外されているものとの境界を明示しつつ記載されているかを確認する。適用範囲となる IT 基盤に含み得るもの及び含まないものの解説については、「★3・★4 要求事項・評価基準 解説書」の 3.2 を参照されたい。

なお、「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」(経済産業省・国家サイバー統括室、令和 8 年 3 月) 2.2.2 制度の対象範囲に記載の「特定の業務領域によらず全体の業務に共通する IT 基盤」とは、人事管理システムや営業管理システムといった特定の業務のためのシステムだけを適用範囲とすることはできないという意味である。

本確認の実施に際しては、登録希望組織から「★3・★4 要求事項・評価基準 解説書」の 3.3 で例示するような取得単位、適用範囲及び適用範囲外との境界を示す概要図や組織体制図等の提供を受け、登録希望組織が利用する IT 基盤が適用範囲に含まれていること、当該組織が利用する資産のうち適用範囲に含めないこととしたものとの境界が明確に記述されているかを確認することが考えられる。

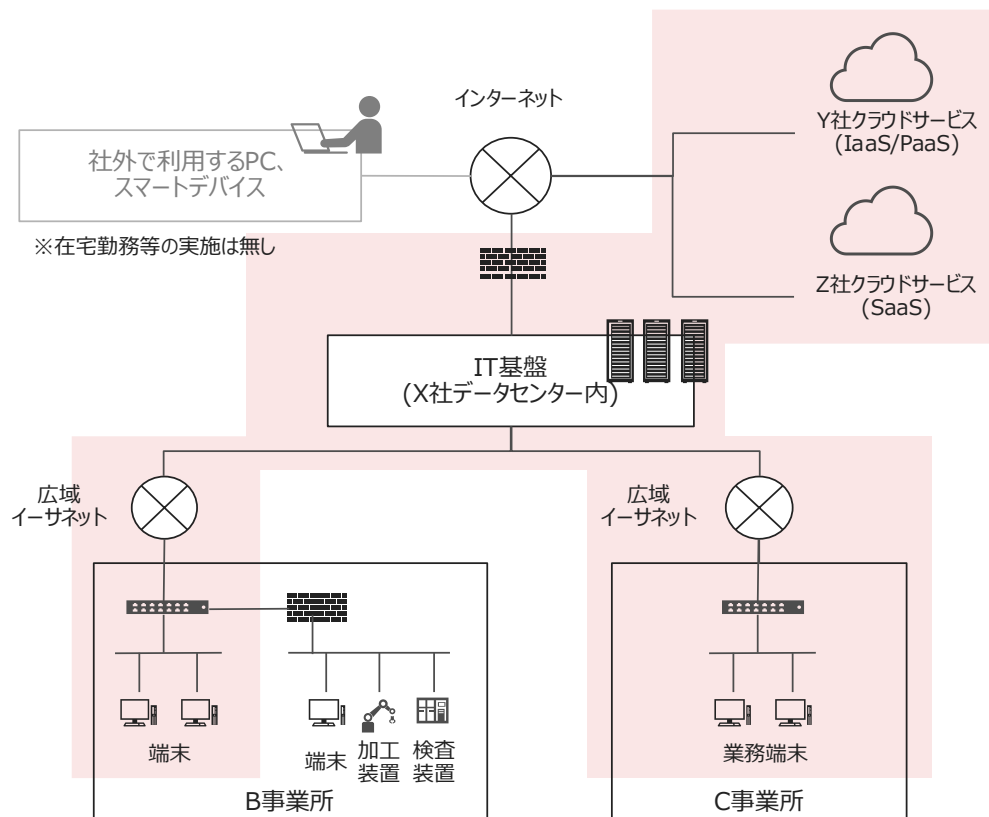


図1 取得単位及び適用範囲の概要図 (例)

2. インターネット公開サーバ（Web サーバ、メールサーバ等）の取扱いに関する確認
 取得単位の組織が管理するインターネット公開サーバが全て適用範囲に含まれているかという点について確認を行う。
 ★3 登録にあたっては、図 1 に示す概要図又はネットワーク図等においてインターネット公開サーバが全て適用範囲に含まれていることを確認するほか登録希望組織の担当者へ質問を行うこと等が考えられる。
 他方、★4 登録にあたっては、評価基準 No.3-1-2-3 で求められるネットワーク図においてインターネット公開サーバが全て適用範囲に含まれていることを確認しつつ、登録希望組織の担当者へ質問を行うこと等が考えられる。
3. 適用範囲の境界を構成する機器等における保護施策の実施状況の確認
 ネットワーク図等の閲覧又は登録希望組織の担当者への質問等により、適用範囲の境界を構成する機器等¹に対して、「★3・★4 要求事項・評価基準 解説書」3.3.3 に示す保護施策が講じられているかを確認する。
4. 適用範囲から除外したものの妥当性の確認
 登録希望組織が自組織の IT 基盤とみなし得るもののうち適用範囲から除外したものについて、「★3・★4 要求事項・評価基準 解説書」3.3.3 で示される考え方に基づき適用範囲との境界において保護施策が講じられているかを確認する。あわせて、除外した対象が具体的に記述されているかを確認する。

なお、適用範囲の確認について、第 3 章にて概要を示すアセスメントシートにおいて、「適用範囲に係る質問事項」を設定している。当該質問事項は上述の「適用範囲に関して確認を要する事項」に対応したものであり、登録希望組織は、自己評価の実施に際してそれらの質問事項についても回答を作成する必要がある。

★3 確認責任者又は評価機関による妥当性確認の結果、登録希望組織が設定した取得単位又は適用範囲に変更が必要と判断された場合、登録希望組織は必要な修正を行った上で改めて★3 確認責任者又は評価機関の確認を受ける。

¹ 「★3・★4 要求事項・評価基準 解説書」3.2 に示す通り、IT システム部門や子会社等が管理する IT 基盤を複数の事業部や子会社等が共同で利用する場合、登録希望組織が定める適用範囲と適用範囲外となる他の事業所等のネットワークとを分離等することが望ましいが、困難であることが想定される。取得単位を事業所単位とする場合や、取得単位をグループ単位としつつ IT 基盤を共同で利用する特定の事業所等を適用範囲から除く場合、適用範囲外とするネットワークとの境界でネットワークを分離等することまでは必ずしも求めない。ネットワーク分離等の対策を行わず適用範囲外の組織が IT 基盤を共同利用する場合は、適用範囲内への影響を考慮し、★3・★4 要求事項・評価基準と同等以上の対策が講じられていることを確認する必要がある。

第3章 アセスメントシート等の取扱い

3.1 アセスメントシートの位置づけ及び見方

3.1.1 アセスメントシートの位置づけ

登録希望組織は、要求事項・評価基準に対する遵守状況の自己評価を行い、★3の登録にあたっては★3 確認責任者による内容の確認を、★4の登録にあたっては評価機関による内容の確認を受ける必要がある。

自己評価の実施にあたって、登録希望組織は、本ガイド別紙「自己評価における適合基準等」に示す【自己評価方法】を参照し、要求事項・評価基準の遵守状況を確認する必要がある。アセスメントシートとは、当該自己評価等の実施において、登録希望組織が作成する自己評価結果を記入する様式である。自己評価等における本シートの利用は任意とするが、自己評価等の実施にあたって準備すべき証跡やその他必要な情報等を事前に網羅的に把握するため、利用を推奨するものとする²。登録希望組織は、IPAのSCS評価制度公式サイト

(<https://www.ipa.go.jp/security/scs/index.html>) より後述する事項があらかじめ記載されたアセスメントシートのテンプレートをダウンロードすることができる。

★3の取得にあたって、登録希望組織は、自組織内又は外部の★3 確認責任者に記入したアセスメントシート等³の確認を依頼する。依頼を受けた★3 確認責任者は受領したアセスメントシート等に必要事項がもれなく記載されているか及びその内容が妥当であるかを確認し、必要に応じて助言を行う。確認の結果、適用される全ての★3 要求事項・評価基準を満たしていると判断した場合は、★3 確認責任者は、受領したアセスメントシートに対して所定の確認を行った証として署名又は記名を行う。

★4の取得にあたっては、アセスメントシート等の確認を評価機関に依頼する必要がある。依頼を受けた評価機関は、アセスメントシート等に必要事項がもれなく記載され、かつ記載内容が妥当であるかを確認することにより、「文書確認」を行う。

なお、制度運営機関が提供するアセスメントシートを使用せず、独自の様式を用いて自己評価等を実施することも妨げないが、その際、当該様式は、アセスメントシートに含まれる各項目（以下に示すとおり）を含むものでなければならない。

- ① 要求事項・評価基準
- ② 各評価基準の内容が適用対象外となるかどうか及び適用対象外とする場合の理由を記入する欄
- ③ 各評価基準への自己評価結果（適合/不適合）を記入する欄
- ④ アセスメントシートに記載されたものと同じの質問事項（「適用範囲に係る質問事項」を含む。）及び質問事項への回答欄

² 自己評価等における本シートの利用はあくまで任意とするが、本シートそのものを利用しない場合であっても、登録希望組織は本シートに示された項目を最低限含むよう自己評価を記入しなければならない。

³ 本ガイドにおいて、登録希望組織が自己評価結果を記入するものについて、IPAが公開するテンプレート以外の様式があり得る点にも鑑み、「アセスメントシート等」と表記する。

アセスメントシート等として独自の様式を用いる場合、★3においては★3 確認責任者が確認の実施前に、★4においては評価機関が第三者評価の着手前に、当該様式が①から④を含むことを確認するものとする。含まない場合は、登録希望組織に修正を求める。

3.1.2 アセスメントシートの見方

本ガイドにおいて様式として定めるアセスメントシートは、登録を希望する段階ごとに★3用と★4用の2種類に分かれている。

アセスメントシートの構成は、★3・★4で同一であり、大きく分けて以下5つの部分に分かれる。

① 要求事項・評価基準

IPAのSCS評価制度公式サイトで公表される★3・★4 要求事項・評価基準⁴を示す。

② 評価基準に対する対象外

①における評価基準を対象外とする場合に、その旨及び対象外とした理由を記入する。各評価基準が対象外となるための条件は、本ガイド別紙を参照されたい。

③ 適合基準・自己評価方法

本ガイド別紙に記述する適合基準及び自己評価方法をそのまま記載している。

④ 自己評価結果

③における適合基準のそれぞれについて、適合しているかどうかを記入する欄である。

⑤ 質問事項・回答欄

確認（★3）又は第三者評価（★4）の実施に際して回答を準備すべき質問事項を示すものであり、当該質問事項に対して登録希望組織は、「質問事項に対する回答欄」へ記入するものとする。

⁴ IPA「要求事項・評価基準」（<https://www.ipa.go.jp/security/scs/requirements-criteria.html>）を参照

表1 アセスメントシートの構成

① 要求事項・評価基準		② 評価基準に対する 対象外		③ 適合基準・ 自己評価方法		④ 自己評価結果	⑤ 質問事項・回答欄					
要求事項 名	要求事項	★3/ ★4	評価 基準 No.	評価基準	NIST CSFC における 機能	対象外 ・評価基準に ついて全く該 当せず、回答 の必要がない 場合のみ「○」を選択	対象外とする 理由 ・対象外とした 理由を回答	適合基準	自己評価方法	自己評価 結果 [適合/不 適合]	質問事項	回答欄
社内ルール	セキュリティに関する 法令等に規定され た事項を考慮し、 社内ルールを策定 及び周知すること。	★4	1-1-1-1	・セキュリティに関連する以下 の事項を把握した上で、社内 ルールを定めること。 - 自社に関連する法令(事業法 、個人情報保護法等) - 所管省庁及び関係団体にお ける基準 - 取引先が提示する制限事項 及び要求事項	統治 (GV)			① 自社に関連する法令、所管 省庁・関係団体における基準、 取引先からの要求等を把握し ていること。	① 自社に関連する法令、所管 省庁・関係団体の基準、取引 先からの要求事項について、一 覧化した資料等を作成してい ることを確認する。		社内ルールを定めるに当 たりの把握している、自社に 関連する法令、所管省 庁・関係団体における基 準及び取引先からの要 求等の名称を回答してく ださい。	
						② 社内ルールを定める際に、① の事項を考慮していること。	② 社内ルールを定める場合や 見直しを行う際に、①で整理 した事項を考慮し、反映する要 否を検討した記録等を確認す る。					
			1-1-1-2	・No.1-1-1-1で定める事項 の改定及び変更の状況につ いて、年1回以上の頻度で確 認を行い、社内ルールの内 容を点検すること。			① No.1-1-1-1で定める自 社に関連する法令等の改定・ 変更の状況について、年1回 以上の頻度で確認を行って いること。	① No.1-1-1-1で定める自 社に関連する法令等の改定・ 変更の状況について、1年以 内に確認をしていること、ま た、自社に関連する法令等 を一覧化している資料等が更 新されていることを確認す る。	No.1-1-1-1で定める関 連する法令等の改定・変更 の状況の確認について、以 下の全ての項目について回 答してください。 - 実施頻度 - 直近の実施日			
						② ①で確認を行い把握した自 社に関連する法令等の改定・ 変更の状況について、社内 ルールに反映するかどうか 対応を検討していること。	② 改定・変更があった場合 に、社内ルールへ反映する 要否を検討した記録等を確認 する。					

また、アセスメントシートには、「適用範囲に係る質問事項」が含まれており、登録希望組織は、自己評価結果等とあわせてこれらに対する回答についても、★3 確認責任者又は評価機関による確認を受ける必要がある。

なお、★3 確認責任者や評価機関にあっては、各設問に対する適合・不適合等の判定結果などを記入すべく、適宜列を追加することも可能である。

3.2 アセスメントシートの使用方法

登録に際して、登録希望組織は、取得を目指す段階で求められる評価基準の全てについて、本ガイドの別紙で提示される自己評価方法を満たす記述がなされていることを確かめたうえで、★3 においては★3 確認責任者、★4 においては評価機関に記入済みのアセスメントシートについて文書確認を依頼する。アセスメントシートの質問事項への回答内容は、★3 確認責任者の確認、★4 における評価機関の第三者評価における基礎的な材料となる。

策定されている規程を尋ねる質問事項に対しては遵守を示す証拠に該当する具体的な規程の名称を記入する。

評価基準に対応する具体的な取り組みの回答を求める質問事項に対しては具体的な対策の取り組みを記入する。

以上により、★3 登録希望組織と★3 確認責任者、又は★4 登録希望組織と評価機関との間のコミュニケーションコストを低減することができる。また、要求事項・評価基準で求められる対策水準を自組織が満たしていることを首尾よく示すため、登録希望組織においては、自己評価実施の際、自組織における対策の状況について、「★3・★4 要求事項・評価基準解説書」及び本ガイド等を参照しておくことが望ましい。アセスメントシートにおける質問事項への回答の記入例を以下に示す。

表2 アセスメントシートの記入例

評価基準No.	評価基準	NIST CSF における機能	…	適合基準	自己評価方法	自己評価結果 [適合/不適合]	質問事項	回答欄
1-1-1-1	・セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。 - 自社に関連する法令事業法、個人情報保護法等 - 所管省庁及び関係団体における基準 - 取引先が提示する制限事項及び要求事項	統治(GV)		① 自社に関連する法令、所管省庁・関係団体における基準、取引先からの要求等を把握していること。	① 自社に関連する法令、所管省庁・関係団体の基準、取引先からの要求事項について、一覧化した資料等を作成しているかを確認する。	適合	社内ルールを定めるに当たり把握している、自社に関連する法令、所管省庁・関係団体における基準及び取引先からの要求等の名称を回答してください。	・個人情報保護法 ・XX業法 ・XXに関する基準
				② 社内ルールを定める際に、①の事項を考慮していること。	② 社内ルールを定める場合や見直しを行う際に、①で整理した事項を考慮し、反映する要否を検討した記録等を確認する。	適合		
1-1-1-2	・No.1-1-1-1で定める事項の改定及び変更の状況について、年1回以上の頻度で確認を行い、社内ルールの内容を点検すること。			① No.1-1-1-1で定める自社に関連する法令等の改定・変更の状況について、年1回以上の頻度で確認を行っていること。	① No.1-1-1-1で定める自社に関連する法令等の改定・変更の状況について、1年以内に確認をしていること、また、自社に関連する法令等を一覧化している資料等が更新されていることを確認する。	適合	No.1-1-1-1で定める関連する法令等の改定・変更の状況の確認について、以下の全ての項目について回答してください。 - 実施頻度 - 直近の実施日	・年に1回実施している。 ・直近では2026/XX/XXに実施した。
				② ①で確認を行い把握した自社に関連する法令等の改定・変更の状況について、社内ルールに反映するかどうか対応を検討していること。	② 改定・変更があった場合に、社内ルールへ反映する要否を検討した記録等を確認する。	適合		

3.3 アセスメントシート記入後のエビデンス保持

★3 又は★4 の登録の有効期間中は、制度運営機関による調査の際に登録申請時点のアセスメントシートがその後変更されていないことを確認できるよう、登録組織や評価機関は、当該アセスメントシート及びそのハッシュ値⁵を保管する必要がある。これは制度運営機関による調査の際に、登録申請時点のアセスメントシートのハッシュ値と、保管しているアセスメントシートのハッシュ値を照合することで、登録後にアセスメントシートの内容が改変されていないことを確認し、登録内容の信頼性及び公平性を確保するためである。ハッシュ値はアセスメントシートの内容を復元するものではないため、照合にはアセスメントシート本体とハッシュ値の双方が必要となる。

具体的には、★3 では、★3 確認責任者によって適合であると判断され、自己適合宣言に係る署名又は記名が行われたアセスメントシート全体を PDF 化し、当該 PDF ファイルについてハッシュ関数（SHA-256）によりハッシュ値を算出し⁶、当該 PDF ファイル及びハッシュ値を証跡として保管しなければならない。なお、アセスメントシート及びハッシュ値は、登録組織において適切に管理・保管するとともに、ハッシュ値については、制度運営機関へ提出する。

★4 では、評価機関によって適合であると判断され、自己適合宣言に係る署名又は記名が行われたアセスメントシート全体を PDF 化し、評価機関へ提出しなければならない。評価機関は、当該 PDF ファイルについてハッシュ関数（SHA-256）によりハッシュ値を算出し、登録希望組織及び制度運営機関へ提出するとともに、当該 PDF ファイル及びハッシュ値を証跡として保管する。PDF 化したアセスメントシート及びハッシュ値は、登録組織及び評価機関において適切に管理・保管する。また、登録組織は、アセスメントシートの内容に対して、1 年に 1 回以上の頻度で、内容を最新化する必要がある。更新を行ったアセスメントシートについては、自己適合宣言に係る署名又は記名が行われたアセスメントシート全体を PDF 化し、評価機関へ提出しなければならない。評価機関は、当該 PDF ファイルのハッシュ値を算出し、登録組織及び制度運営機関へ提出する。

「★3・★4 登録申請の手引」3.2.4 及び 4.2.5 に示す通り、登録組織は、登録期間中に、適用範囲の変更又は要求事項・評価基準の達成に顕著な影響を及ぼす変更があるかを把握する必要がある。該当する変更がある場合は、速やかに★3 確認責任者による再確認又は評価機関による再評価を受けなければならない。⁷

要求事項・評価基準の達成に顕著な影響を及ぼす変更の例を以下に掲げる。

⁵ 「ハッシュ値」とは、特定のアルゴリズム（ハッシュ関数）により算出される固定長の文字列のことで、データの指紋とも呼ばれる。

⁶ ハッシュ値の算出に使用するツールは問わない。また、ハッシュ値の算出は組織内部の担当者が実施することが望ましいが必要に応じ外部の者が実施することは構わない。

⁷ 規程・手順書等における誤字脱字・体裁の修正や、要求事項・評価基準の達成に顕著な影響のない軽微な設定・運用上の変更を除く。

- ・ 要求事項・評価基準に関連する社内規程・手順書等の大幅な変更
- ・ 要求事項・評価基準の達成方法や運用方法の大幅な変更（IT 基盤を構成する端末やサーバ等の大規模なリプレイス、クラウド基盤への大規模な移行、ネットワーク構成の顕著な変更等）

★3 の更新時に行う★3 確認責任者による確認又は★4 の有効期間中に毎年行う評価機関への自己評価結果の提出は、最新のアセスメントシート等に基づいて行う。確認又は評価の完了後、登録組織は、当該アセスメントシート等に対する★3 確認責任者又は評価機関の署名又は記名の確認をしなければならない⁸。

また、★4 の有効期間中に毎年行う評価機関への自己評価結果の提出が、登録日から 1 年を経過した日及び 2 年を経過した日を基準として、それぞれ少なくとも前後 3 か月以内の範囲内に行われない場合、登録が取り消される場合がある点に留意する必要がある。

なお、詳細は、「★3・★4 登録申請の手引」を参照のこと。

⁸ 登録取得後のエビデンスの保持等については、必要に応じて、「★3・★4 登録申請の手引」第 3 章及び第 4 章も参照されたい。

第4章 ★3 における確認の実施

4.1 ★3 における確認の位置づけ及び実施内容

★3 の登録取得にあたって、登録希望組織は、自組織内又は外部の★3 確認責任者に記入したアセスメントシート等の確認を依頼する。依頼を受けた★3 確認責任者は受領したアセスメントシート等に必要事項がもれなく記載されているかを確認し、必要に応じて助言を行う。★3 確認責任者は、最終的に★3 要求事項・評価基準を全て満たしていると判断した場合、アセスメントシートに含まれる★3 確認責任者署名・記名欄に署名又は記名を行う。他方、助言を行ってもなお妥当性を確認できない事項がある場合は、署名又は記名を行わない。登録希望組織は、前記の場合において、必要に応じて別の★3 確認責任者に確認を依頼することができる。

★3 確認責任者又は★3 確認従事者⁹による確認は、セキュリティ対策について一定の力量を有する者の見地からアセスメントシート等の記載内容の妥当性を確かめることにより、登録希望組織による本制度の趣旨に合った形での対策実施をより確からしいものとしつつ、結果としてサプライチェーン全体のセキュリティ水準の底上げに資することを目的とする。

その際、★3 確認責任者又は★3 確認従事者は、表 3 に例示する観点を踏まえつつ、登録希望組織から提供を受けたアセスメントシート等の回答内容に関して、確認を行うことが望ましい。

表 3 ★3 確認における観点

観点	実施する確認の例	登録希望組織に指摘すべき事項の例
網羅性	アセスメントシート等に質問への回答がもれなく記入されているか。	質問に対する回答の未記載
	取得単位、適用範囲に鑑み、対策の有効範囲が適切に示されているか。	規程等の有効範囲不足 (例：企業グループ単位での取得にもかかわらず、規程が特定個社のみ有効)
正確性	回答内容が設問の趣旨と整合しているか。記載内容に誤り・不自然な点はないか。	設問の趣旨と齟齬のある回答
適時性	回答が期間・時点に対して適切か。	回答内容における古い情報の残存 (例：年次的に実施する点検の最新実施日が確認時点から 1 年以上前)
一貫性	他の設問や回答内容と矛盾や食い違いがなく整合しているか。	アセスメントシート等の他の質問項目における回答との矛盾・不整合

「★4 第三者評価ガイド」別紙等で述べる★4 における「評価」とは異なり、★3 における

⁹ ★3 確認責任者による監督の下、確認の実務を担当する者。確認結果の最終判断及び品質責任については、★3 確認責任者が担う。

「確認」はアセスメントシート等に回答された対策等が実際に講じられているかを確認することまでを求めるものではなく、原則として、アセスメントシート等に記載された情報のみをもって要求事項・評価基準に対する妥当性を確認するものである¹⁰。アセスメントシート等に記載された情報の真実性については、登録希望組織が責任を負う。★3 確認責任者及び★3 確認従事者¹¹は、表 3 に例示する観点を踏まえて所定の確認を行ったこと及びその結果について責任を負うものであり、記載された情報が事実と異なっていたことをもって責任を負うものではない。

一般に、セキュリティ対策等について十分な知見・スキルを有さない法人等を中心として、自己評価結果としてアセスメントシート等に記入する事項に、アセスメントシート等の質問内容に鑑みて妥当性を十分に有しているとは言えない回答内容が含まれる場合も考えられる。★3 確認責任者又は★3 確認従事者は、確認の実施を通じて、登録希望組織による本制度の趣旨に合った形での対策実施をより確からしいものとしつつ、結果としてサプライチェーン全体のセキュリティ水準の底上げに資するよう業務に努めることが望ましい。

4.2 ★3 確認責任者が自己評価結果の確認を行う場合の留意点

★3 確認責任者及び★3 確認従事者は、「基本規程」6.1 に定められる通り、登録希望組織から受領したアセスメントシート等の秘密情報を本制度の目的の範囲内でのみ取り扱い、正当な権限を有しない者に開示し、又は漏えいしてはならない。また、秘密情報を本制度の目的外に使用し、複製し、又は不適切に保管してはならない。秘密保持義務は、当該者の本制度への関与が終了した後も継続する点にも留意する必要がある。

また、★3 においては登録希望組織に属する★3 確認責任者がアセスメントシート等の確認業務を行うことも想定される。登録希望組織は、確認の結果いかんにより、確認を実施した当人を人事等において不当な差別的取扱いの対象としてはならない。万が一不当な差別的取扱いとして遇され得る事象が生じた場合、確認を行った★3 確認責任者本人又はその状況を知り得た他の者が、制度運営機関が設ける窓口へ通報を行うこと等が望ましい。

¹⁰ 登録希望組織と★3 確認責任者等との間で適切な合意がなされているならば、登録取得に至る過程でアセスメントシート等に記載された対策等の実在性の確認等を行うことは何ら妨げられるものではない。

¹¹ ★3 確認責任者は★3 確認の最終判断及び品質に対して責任を有し、★3 確認従事者は★3 確認責任者の指導及び監督の下で確認の実務を担当する。いずれも表 3 に例示された観点を踏まえつつアセスメントシートの確認を実施し、記載内容の妥当性向上を支援することを担務とする。その際、アセスメントシートに記載された証跡の実在性確認を行う必要はないが、不自然な記載等があれば追加説明を求めることが望ましい。

別紙 自己評価における適合基準等

本ガイドの別紙では、要求事項・評価基準のそれぞれについて、登録希望組織が行う自己評価の方法及び適合基準等を示す。各項目の説明は、以下のとおりである。

【対象外となるための条件】

各評価基準を対象外とする条件を示す。登録希望組織は当該条件に合致し対象外となる旨を申告し、かつ、★3 確認責任者又は評価機関に当該申告は妥当であると認められた場合限り、評価の対象外とすることができる。「該当なし」の評価基準は、原則として対象外とすることができないが、★3 確認責任者又は評価機関に、登録希望組織の IT 基盤の状況等に鑑み、対象外とすることが妥当であると判断された場合は、その理由を記録した上で、対象外とすることが認められる。当該条件は、「★4 第三者評価ガイド」別紙で示される対象外となるための条件と同一である。

【適合基準】

対象の評価基準に関して、どのようなことがなされていれば適合と判断することができるかを示す。複数の基準が示されている場合は、原則として全ての基準を満たす必要がある

（「やむを得ず」に該当する場合は除く）。当該適合基準は、「★3・★4 自己評価等ガイド」附属のアセスメントシート（参考様式）及び「★4 第三者評価ガイド」別紙で示される適合基準と同一である。

【自己評価方法】

各適合基準への適合性を確認するために、どのような方法で自己評価を行えばよいかを示す。自己評価方法に示す方法はあくまで例示ではあるが、登録希望組織は自己評価方法を参考に自己評価を実施することが望ましい。当該自己評価方法は「★3・★4 自己評価等ガイド」附属のアセスメントシート（参考様式）で示される自己評価方法と同一である。

自己評価方法における「文書」「記録」「設定画面等」には、確認対象の設定又は状態に応じて、設定画面、管理ツール又は管理コンソールでの表示、システムが自動で生成する記録、ログその他の記録、製品・サービスの仕様書その他の技術資料、及び製品・サービスの導入・設定状況を確認できる資料等を含む。自己評価に当たっては、確認対象に応じて適切な確認手段・資料を選択すること。「文書の確認」や「記録等の確認」についても、紙文書による確認に限定するものではなく、ワークフローにおける文書一覧や設定画面のスクリーンショットによる確認を行うことができる。製品・サービスの仕様書その他の技術資料を確認する場合は、当該製品・サービスが実際に導入され、確認対象に適用されていることを、導入・設定状況を確認できる資料等により併せて確認すること。また、「周知」「教育・研修」については、社内掲示板や社内ポータルへの掲示、メールでの配信、eラーニング等、各組織の規模や環境に応じて関係者に確実に伝わる手段を選択して行うことを想定しており、必ずしも複数手段を組み合わせることを求めているわけではない点に留意されたい。なお、別紙で示す事項のほか、自己評価の実施に当たっては、「★3・★4 要求事項・評価

基準 解説書」において各要求事項・評価基準の内容で解釈に迷うと考えられる箇所に対し、解説を記載しているのでそちらも参照すること。

1. ガバナンスの整備

1-1 組織の状況

1-1-1 社内ルール

【要求事項】

セキュリティに関する法令等に規定された事項を考慮し、社内ルールを策定及び周知すること。

(1) No.1-1-1-1 ★4

【評価基準】

セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。

- 自社に関連する法令（事業法、個人情報保護法等）
- 所管省庁及び関係団体における基準
- 取引先が提示する制限事項及び要求事項

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社に関連する法令、所管省庁・関係団体における基準、取引先からの要求等を把握していること。
- ② 社内ルールを定める際に、①の事項を考慮していること。

【自己評価方法】

- ① 自社に関連する法令、所管省庁・関係団体の基準、取引先からの要求事項について、一覧化した資料等を作成しているかを確認する。
- ② 社内ルールを定める場合や見直しを行う際に、①で整理した事項を考慮し、反映する要否を検討した記録等を確認する。

(2) No.1-1-1-2 ★4

【評価基準】

No.1-1-1-1 で定める事項の改定及び変更の状況について、年1回以上の頻度で確認を行い、社内ルールの内容を点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.1-1-1-1 で定める自社に関連する法令等の改定・変更の状況について、年1回以上の頻度で確認を行っていること。
- ② ①で確認を行い把握した自社に関連する法令等の改定・変更の状況について、社内ルールに反映するかどうか対応を検討していること。

【自己評価方法】

- ① No.1-1-1-1 で定める自社に関連する法令等の改定・変更の状況について、1年以内に確認をしていること、また、自社に関連する法令等を一覧化している資料等が更新されていることを確認する。
- ② 改定・変更があった場合に、社内ルールへ反映する要否を検討した記録等を確認する。

(3) No.1-1-1-3 ★4

【評価基準】

策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 策定・見直した社内ルールについて、役員、従業員、派遣社員及び受入出向者を対象に何らかの手段・媒体で周知を行っていること。

【自己評価方法】

- ① 策定・見直した社内ルールについて、社内掲示板、社内ポータルサイト等、社内への周知を行う手段・媒体を確認し、役員、従業員、派遣社員及び受入出向者に周知されていることを確認する。

1-2 役割、責任、権限

1-2-1 セキュリティ推進活動部門

【要求事項】

セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。

(1) No.1-2-1-1 ★3

【評価基準】

セキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）及びセキュリティ担当部署の役割・責任を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティを統括する役員及びセキュリティ担当部署を決めていること。
- ② セキュリティを統括する役員及びセキュリティ担当部署の役割・責任を決めていること。

【自己評価方法】

- ① 社内規程や社内体制図、発令文書等を確認し、セキュリティを統括する役員及びセキュリティ担当部署を決めていることを確認するとともに、どのような文書に記載しているかを確認する。
- ② 社内規程や社内体制図等を確認し、セキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）及びセキュリティ担当部署の役割・責任を定めていることを確認するとともに、どのような文書に記載しているかを確認する。

(2) No.1-2-1-2 ★3

【評価基準】

平時のセキュリティ推進活動に必要な役員（例えば、CISOを設置する会社の場合は、当該CISO）及びセキュリティ担当部署の連絡先リストを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 平時のセキュリティ推進活動に必要な役員及びセキュリティ担当部署の連絡先リストを作成していること。

【自己評価方法】

- ① 社内体制図、連絡先一覧等を確認し、平時のセキュリティ推進活動に必要な役員及びセ

セキュリティ担当部署の連絡先リストを作成していることを確認するとともに、そのリストの文書名を確認する。

(3) No.1-2-1-3 ★3

【評価基準】

年1回以上の頻度で No.1-2-1-1 及び No.1-2-1-2 にて定めた平時の体制について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 年1回以上の頻度で No.1-2-1-1 及び No.1-2-1-2 にて定めた平時の体制について点検していること。

【自己評価方法】

- ① No.1-2-1-1 及び No.1-2-1-2 にて定めた平時の体制を点検した記録を確認し、年1回以上の頻度で点検を行っていることを確認する。

(4) No.1-2-1-4 ★4

【評価基準】

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前提として、その対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティリスクの対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置していること。

【自己評価方法】

- ① 社内体制図、社内規程等を確認し、セキュリティリスクの対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置していることを確認するとともに、当該情報セキュリティ委員会等の議事録等を確認し、設置している体制について活動実態があることを確認する。

1-2-2 サイバー攻撃の監視・分析体制**【要求事項】**

サイバー攻撃及び予兆を監視・分析をする体制を整備すること。

(1) No.1-2-2-1 ★4**【評価基準】**

サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を活用する体制を整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を収集していること。
- ② ①で収集した情報を活用するための体制（情報収集後の手順等）を整備していること。

【自己評価方法】

- ① サイバー攻撃及び脆弱性に関する情報を入手する情報源としてどのようなものを利用しているかを確認する。
- ② サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を収集した後のプロセス等を確認し、これらの情報を活用するための体制（情報収集後の手順等）を整備していることを確認する。

(2) No.1-2-2-2 ★4**【評価基準】**

入手した情報又はログの相関分析等により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 入手した情報又はログの相関分析等により、サイバー攻撃の予兆及びインシデントの発生を検知できるようになっていること。
- ② ①における検知の結果に基づき、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制（検知後の手順等）を整備していること。

【自己評価方法】

- ① サイバー攻撃の予兆及びインシデントの発生に関して収集している情報、ログ等を確認し、サイバー攻撃の予兆及びインシデントの発生の検知ができるようになっていることを確認する。
- ② 社内体制図、社内規程等を確認し、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制（検知後の手順等）が整備できていることを確認する。

1-2-3 守秘義務のルール**【要求事項】**

守秘義務のルールを策定し、遵守させること。

(1) No.1-2-3-1 ★3**【評価基準】**

役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 役員、従業員、派遣社員及び受入出向者を対象とした自社の守秘義務のルールを定めていること。

【自己評価方法】

- ① 就業規則、労働契約等を確認し、役員、従業員、派遣社員及び受入出向者を対象とした自社の守秘義務のルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(2) No.1-2-3-2 ★3**【評価基準】**

入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 入社時又は社外要員の受入れ時に No.1-2-3-1 で定めた守秘義務のルールを説明していること。

【自己評価方法】

- ① 入社時又は社外要員の受入れ時におけるオリエンテーション資料、受入手順等を確認し、守秘義務のルールを説明していることを確認する。

(3) No.1-2-3-3 ★4**【評価基準】**

自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。（社外要員を除く。）

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社の機密情報を取り扱う役員及び従業員が提出する守秘義務の誓約書の様式を定めていること。
- ② 自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させていること。

【自己評価方法】

- ① 情報取扱規程等の機密情報の取扱いに関するルールを確認し、自社の機密情報を取り扱う役員及び従業員が提出する守秘義務の誓約書の様式を定めていることを確認するとともに、その様式の文書名を確認する。
- ② ①の様式について、自社の機密情報を取り扱う役員及び従業員が実際に提出していることを確認する。

(4) No.1-2-3-4 ★4**【評価基準】**

派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。

【対象外となるための条件】

派遣社員及び受入出向者が存在しない場合

【適合基準】

- ① 派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結していること。

【自己評価方法】

- ① 派遣元及び出向元の会社との契約書、合意書その他の取り決めに係る文書を確認し、派遣社員及び受入出向者について守秘義務を締結していることを確認するとともに、その取り決めに係る文書の文書名を確認する。

1-3 ポリシー

1-3-1 セキュリティ対応方針の策定

【要求事項】

自社のセキュリティ対応方針を策定し、周知すること。

(1) No.1-3-1-1 ★3

【評価基準】

自社のセキュリティ対応方針を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社のセキュリティ対応方針を定めていること。

【自己評価方法】

- ① 自社のセキュリティ対応方針を策定していることを確認するとともに、そのセキュリティ対応方針の文書名を確認する。

(2) No.1-3-1-2 ★3

【評価基準】

定常的に役員、従業員、派遣社員及び受入出向者が最新のセキュリティ対応方針を参照できるようにすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 何らかの手段・媒体により、定常的に役員、従業員、派遣社員及び受入出向者が最新のセキュリティ対応方針を参照できるようになっていること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、役員、従業員、派遣社員及び受入出向者が No.1-3-1-1 で策定したセキュリティ対応方針を定常的に参照できる状態になっているかを確認する。

(3) No.1-3-1-3 ★3

【評価基準】

セキュリティ対応方針の改正時に、当該改正内容を役員、従業員、派遣社員及び受入出向者に周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティ対応方針の改正時に、当該改正内容を役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。

【自己評価方法】

- ① セキュリティ対応方針の改正履歴や社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、セキュリティ対応方針の改正時に、当該改正内容が役員、従業員、派遣社員及び受入出向者に周知されていることを確認する。

(4) No.1-3-1-4 ★4

【評価基準】

年1回以上の頻度でセキュリティ対応方針の内容を点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 年1回以上の頻度でセキュリティ対応方針の内容を点検していること。

【自己評価方法】

- ① セキュリティ対応方針の内容を点検した記録を確認し、年1回以上の頻度で点検を行っていることを確認する。

1-4 監督

1-4-1 セキュリティ対策推進計画

【要求事項】

セキュリティ対策推進計画を策定し、定期的に経営層へ対策実施状況に関する報告を行うとともに、報告結果を対策の推進に反映すること。

(1) No.1-4-1-1 ★4

【評価基準】

セキュリティ担当部署は、年1回以上、セキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）に対して、以下にて求める対策の点検の結果を踏まえたセキュリティ対策の実態及び当該実態を踏まえて策定した今後の対策推進計画を報告し承認を得た上で、当該報告結果を社内部署と共有すること。

[点検を求める対策（評価基準）]

No.1-1-1-2、1-2-1-3、1-3-1-4、2-1-1-2、3-1-1-4、3-1-1-7、3-1-2-4、3-1-4-2、3-1-4-4、3-1-4-6、3-1-5-3、3-2-1-5、4-1-7-2、4-1-9-3、4-2-1-5、4-2-2-3、5-1-2-2、6-1-1-4

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティ担当部署は、対策の点検の結果を踏まえたセキュリティ対策の実態を把握していること。
- ② セキュリティ担当部署は、①における実態を踏まえ、今後の対策推進計画を策定していること。
- ③ セキュリティ担当部署は、①における実態及び②における今後の対策推進計画を年1回以上の頻度でセキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）に対して報告し、承認を得ていること。
- ④ セキュリティ担当部署は、③における当該報告結果を社内部署と共有していること。

【自己評価方法】

- ① 少なくとも各対策の点検結果の確認を含め、セキュリティ対策の実態を把握していることを確認する。
- ② 対策推進計画を策定した文書を確認し、①における実態を踏まえたものとなっていることを確認するとともに、その文書名を確認する。
- ③ 役員への報告に係る議事録等を確認し、①における実態及び②における今後の対策推進計画を年1回以上の頻度でセキュリティを統括する役員に対して報告し、承認を得ていることを確認するとともに、報告及び承認に係る結果を記録した文書の文書名を確認する。
- ④ 社内担当部署への共有履歴を確認し、③における当該報告結果を社内部署と共有していることを確認する。

(2) No.1-4-1-2 ★4**【評価基準】**

No.1-4-1-1 における対策推進計画の報告に際し、役員からの改善に向けた指示があった場合、セキュリティ担当部署は、当該指示内容の記録、計画への反映及び不備の是正を実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.1-4-1-1 における対策推進計画の報告に際し、役員からの改善に向けた指示があった場合は、セキュリティ担当部署は、当該指示内容の記録を行っていること。
- ② ①における指示内容の記録に基づき、計画への反映を行っていること。
- ③ ①における指示内容の記録に基づき、対策の不備の是正を行っていること。

【自己評価方法】

- ① 役員報告に係る議事録等を確認し、No.1-4-1-1 における対策推進計画の報告に際し、役員からの改善に向けた指示があった場合は、セキュリティ担当部署は、当該指示内容の記録を行っていることを確認するとともに、その文書名を確認する。
- ② 対策推進計画の検討に係る記録等を確認し、①における指示内容の記録に基づき、計画への反映を行っていることを確認する。
- ③ 対策推進計画の検討に係る記録等を確認し、①における指示内容の記録に基づき、対策の不備の是正を行っていることを確認する。

2. 取引先管理

2-1 サイバーセキュリティサプライチェーンリスクマネジメント

2-1-1 取引先とのビジネス又はシステム上の関係

【要求事項】

取引先と自社とのビジネス又はシステム上の関係を把握すること

(1) No.2-1-1-1 ★3

【評価基準】

自社以外の組織（顧客・子会社・関係会社・クラウドサービス提供者を含む取引先）が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。

【対象外となるための条件】

自社以外の組織（顧客・子会社・関係会社・クラウドサービス提供者を含む取引先）が管理・提供し、自社の資産が接続しているシステムが存在し得ない場合

【適合基準】

- ① 自社以外の組織（顧客・子会社・関係会社・クラウドサービス提供者を含む取引先）が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備していること。
- ② ①の仕組みにより、自社以外の組織（顧客・子会社・関係会社・クラウドサービス提供者を含む取引先）が管理・提供し、自社の資産が接続しているシステム情報を把握していること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツール等を確認し、自社の資産が接続しているシステムを把握するための仕組みを整備していることを確認する。
- ② 実際に、自社の資産が接続しているシステムを把握していることを確認する。

(2) No.2-1-1-2 ★3

【評価基準】

年 1 回以上の頻度で No.2-1-1-1 において把握した情報の内容を点検すること。

【対象外となるための条件】

自社以外の組織（顧客・子会社・関係会社・クラウドサービス提供者を含む取引先）が管理・提供し、自社の資産が接続しているシステムが存在し得ない場合

【適合基準】

- ① No.2-1-1-1 で把握した情報の内容について、年 1 回以上の頻度で点検していること。

【自己評価方法】

- ① No.2-1-1-1 で把握した情報の内容を点検した記録を確認し、年 1 回以上の頻度で点検を行っていることを確認する。

(3) No.2-1-1-3 ★4**【評価基準】**

自社の機密情報を共有している子会社又は取引先について、以下の事項を把握するための仕組みを整備すること。

- 会社ごとに取り交わす手段（受発注の手段、情報のやり取り等）
- 取引に伴い授受・使用される情報資産及びその取扱い

【対象外となるための条件】

自社の機密情報を共有している子会社又は取引先が存在しない場合

【適合基準】

① 自社の機密情報を共有している子会社又は取引先について、以下の全ての事項を把握するための仕組みを整備していること。

- 会社ごとに取り交わす手段（受発注の手段、情報のやり取り等）
- 取引に伴い授受・使用する情報資産及びその取扱い

② ①の仕組みにより、上記に掲げる事項を把握していること。

【自己評価方法】

① 取引先との契約書、取引先管理台帳等を確認し、自社の機密情報を共有している子会社又は取引先について、以下の全ての事項を把握するための仕組みを整備していることを確認する。

- 会社ごとに取り交わす手段（受発注の手段、情報のやり取り等）
- 取引に伴い授受・使用する情報資産及びその取扱い

② 実際に、上記に掲げる事項を把握していることを確認する。

2-1-2 機密情報の取扱い**【要求事項】**

自社の機密情報の取扱い方法を、共有先との間で明確にすること

(1) No.2-1-2-1 ★3**【評価基準】**

自社の機密情報を共有する子会社又は取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項を取り決めること。

- 機密情報の定義
- 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否
- 機密情報の返還又は廃棄

【対象外となるための条件】

自社の機密情報を共有する子会社又は取引先が存在しない場合

【適合基準】

① 自社の機密情報を共有する子会社又は取引先との間で、以下の全ての事項を取り決めていること。

- 機密情報の定義
- 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否
- 機密情報の返還又は廃棄

【自己評価方法】

① 取引先との秘密保持契約書等を確認し、自社の機密情報を共有する子会社又は取引先との間で、以下の全ての事項を取り決めていることを確認するとともに、その取り決めの文書名を確認する。

- 機密情報の定義
- 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否
- 機密情報の返還又は廃棄

2-1-3 取引先のセキュリティ対策状況

【要求事項】

事業継続リスク及び情報管理リスクの観点から自社に影響を及ぼす可能性のある取引先のセキュリティ対策状況を把握すること。

(1) No.2-1-3-1 ★4

【評価基準】

以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握すること。

【対策状況把握の対象とする子会社又は取引先の条件】

- 自社の重要な機密情報を提供・共有する
- 自社の事業継続にとって重要な位置づけを持つ
- 当該取引先の環境から発注者の内部システムへのアクセスが可能

【対策状況の把握方法（例）】

- 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理する Web サイト等で確認する
- 取引先に訪問し点検を実施する
- セキュリティ対策チェックシートを作成して回答を受領する

【対象外となるための条件】

以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先が存在しない場合

【対策状況把握の対象とする子会社又は取引先の条件】

- 自社の重要な機密情報を提供・共有する
- 自社の事業継続にとって重要な位置づけを持つ
- 当該取引先の環境から発注者の内部システムへのアクセスが可能

【適合基準】

- ① 対策状況把握の対象とする子会社又は取引先を特定していること。
- ② ①で特定した子会社又は取引先について、年1回以上の頻度でセキュリティ対策状況を把握していること。

【自己評価方法】

- ① 取引先管理台帳、取引先管理システム等を確認し、対策状況把握の対象とする子会社又は取引先を特定していることを確認する。
- ② 子会社又は取引先におけるセキュリティ対策状況を確認した記録等を確認し、①で特定した子会社又は取引先について、年1回以上の頻度でセキュリティ対策状況を把握していることを確認するとともに、当該記録の文書名を確認する。

2-1-4 セキュリティインシデント発生時の役割・責任**【要求事項】**

セキュリティインシデント発生時の他社との役割及び責任を明確にすること。

(1) No.2-1-4-1 ★3**【評価基準】**

自社の機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任を定めること。

【対象外となるための条件】

自社の機密情報を共有する子会社又は取引先が存在しない場合

【適合基準】

- ① 自社の機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任を定めていること。

【自己評価方法】

- ① 契約書その他の取り決めを確認し、自社の機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任を定めていることを確認するとともに、その取り決めの文書名を確認する。

2-1-5 機密情報の回収・破棄

【要求事項】

取引先との契約終了時に自社の機密情報及び当該機密情報へのアクセス権を回収する又は破棄させること。

(1) No.2-1-5-1 ★4

【評価基準】

自社の機密情報を共有する子会社又は取引先から、契約終了時に機密情報及びアクセス権が回収又は破棄されていることについて確認する手順（例：回収物一覧のチェックシートの作成）を整備すること。

【対象外となるための条件】

自社の機密情報を共有する子会社又は取引先が存在しない場合

【適合基準】

- ① 自社の機密情報を共有する子会社又は取引先が、契約終了時に機密情報及びアクセス権を回収又は破棄していることを確認する手順を整備していること。

【自己評価方法】

- ① 自社の機密情報を共有する子会社又は取引先から、契約終了時に機密情報及びアクセス権を回収又は破棄していることについて確認する手順を整備していることを確認するとともに、どのような文書に記載しているかを確認する。

3. リスクの特定

3-1 資産管理

3-1-1 情報機器、OS 及びソフトウェアに関する情報の把握

【要求事項】

情報機器、OS 及びソフトウェアに関する情報を把握すること。

(1) No.3-1-1-1 ★3

【評価基準】

パソコン及びシンクライアントの製造元、OS 及び台数を把握するための仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン及びシンクライアントの製造元、OS 及び台数を把握する仕組みを整備していること。
- ② ①の仕組みにより、パソコン及びシンクライアントの製造元、OS 及び台数を把握していること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツール等、どのようにパソコン及びシンクライアントの製造元、OS 及び台数を把握する仕組みを整備しているかを確認する。
- ② 実際に、パソコン及びシンクライアントの製造元、OS 及び台数を把握していることを確認する。

(2) No.3-1-1-2 ★3

【評価基準】

サーバ、仮想サーバ及びハイパーバイザの製造元、OS 及び台数を把握するための仕組みを整備すること。

【対象外となるための条件】

自社オンプレミスサーバを開発、保有していない場合

【適合基準】

- ① サーバ、仮想サーバ及びハイパーバイザの製造元、OS 及び台数を把握する仕組みを整備していること。
- ② ①の仕組みにより、サーバ、仮想サーバ及びハイパーバイザの製造元、OS 及び台数を把握していること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツールなど、どのようにサーバ、仮想サーバ及びハイパ

ーバイザの製造元、OS 及び台数を把握する仕組みを整備しているかを確認する。

- ② 実際に、サーバ、仮想サーバ及びハイパーバイザの製造元、OS 及び台数を把握していることを確認する。

(3) No.3-1-1-3 ★3

【評価基準】

情報機器、OS 及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 情報機器、OS 及びソフトウェアについての管理ルールを定めていること。
- ② ①の管理ルールは、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含んでいること。

【自己評価方法】

- ① 情報機器、OS 及びソフトウェアについての管理ルールを定めていることを確認するとともに、その文書名を確認する。
- ② ①の管理ルールには、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含んでいることを確認する。

(4) No.3-1-1-4 ★3

【評価基準】

年 1 回以上の頻度で No.3-1-1-3 で定めた管理ルールの遵守状況について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-1-3 で定めた管理ルールの遵守状況について、年 1 回以上の頻度で点検していること。

【自己評価方法】

- ① 従業員へのチェックシートなど、No.3-1-1-3 で定めた管理ルールの遵守状況について点検した記録を確認し、No.3-1-1-3 で定めた管理ルールの遵守状況について、年 1 回以上の頻度で点検していることを確認する。

(5) No.3-1-1-5 ★4

【評価基準】

スマートデバイスの製造元、OS 及び台数を把握するための仕組みを整備すること。

【対象外となるための条件】

会社で管理するスマートデバイスが存在しない場合

【適合基準】

- ① スマートデバイスの製造元、OS 及び台数を把握する仕組みを整備していること。
- ② ①の仕組みにより、スマートデバイスの製造元、OS 及び台数を把握していること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツールなど、どのようにスマートデバイスの製造元、OS 及び台数を把握する仕組みを整備しているかを確認する。
- ② ①の仕組みにより、スマートデバイスの製造元、OS 及び台数を把握していることを確認する。

(6) No.3-1-1-6 ★4**【評価基準】**

重要なシステムを構成する情報機器について、設定情報を把握するための仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要なシステムを構成する情報機器の設定情報を把握する仕組みを整備していること。
- ② ①の仕組みにより、重要なシステムを構成する情報機器の設定情報を把握していること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツールなど、どのように重要なシステムを構成する情報機器の設定情報を把握する仕組みを整備しているかを確認する。
- ② ①の仕組みにより、重要なシステムを構成する情報機器の設定情報を把握していることを確認する。

(7) No.3-1-1-7 ★4**【評価基準】**

年1回以上の頻度で No.3-1-1-1、No.3-1-1-2、No.3-1-1-5 及び No.3-1-1-6 で把握した情報の内容について、点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-1-1、No.3-1-1-2、No.3-1-1-5 及び No.3-1-1-6 で把握した情報の内容について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① IT 資産の棚卸を実施した記録等を確認し、No.3-1-1-1、No.3-1-1-2、No.3-1-1-5 及び No.3-1-1-6 で把握した情報の内容について、年 1 回以上の頻度で点検していることを確認する。

3-1-2 ネットワークに関する情報の把握**【要求事項】**

ネットワークに関する情報を把握するための仕組みを整備すること。

(1) No.3-1-2-1 ★3**【評価基準】**

ネットワークを把握するための仕組みを整備すること。その際、把握すべき情報の中に各ネットワークの所在地及び用途に関する情報を含めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ネットワークを把握する仕組みを整備していること。
 ② ①で把握する情報に、各ネットワークの所在地及び用途を含めていること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツール、ネットワーク図など、どのようにネットワークを把握する仕組みを整備しているかを確認する。
 ② IT 資産管理台帳、IT 資産管理ツール、ネットワーク図等を確認し、①で把握する情報に、各ネットワークの所在地及び用途を含めていることを確認する。

(2) No.3-1-2-2 ★3**【評価基準】**

ネットワーク機器を把握するための仕組みを整備すること。その際、把握すべき情報の中に各機器の製造元、モデル及び保守事業者に関する情報を含めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ネットワーク機器を把握する仕組みを整備していること。
 ② ①で把握する情報に、各機器の製造元、モデル及び保守事業者を含めていること。

【自己評価方法】

- ① IT 資産管理台帳、IT 資産管理ツール、ネットワーク図など、どのようにネットワーク機器を把握する仕組みを整備しているかを確認する。
 ② IT 資産管理台帳、IT 資産管理ツール、ネットワーク図等を確認し、①で把握する情報

に、各機器の製造元、モデル及び保守事業者を含めていることを確認する。

(3) No.3-1-2-3 ★4

【評価基準】

ネットワークを対象として、ネットワーク図を作成すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ネットワークを対象としたネットワーク図を作成していること。

【自己評価方法】

- ① ネットワーク図等を確認し、ネットワークを対象としたネットワーク図を作成していることを確認するとともに、その文書名を確認する。

(4) No.3-1-2-4 ★4

【評価基準】

年1回以上の頻度で No.3-1-2-3 で作成したネットワーク図の記載内容について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-2-3 で作成したネットワーク図の記載内容について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① No.3-1-2-3 で作成したネットワーク図の記載内容を点検した記録を確認し、年1回以上の頻度で点検していることを確認する。

3-1-3 外部情報サービスの管理

【要求事項】

自社の機密情報を扱う外部情報サービスを管理すること。

(1) No.3-1-3-1 ★3

【評価基準】

外部情報サービスを利用する際のセキュリティ要件を定めたうえで、外部情報サービスの利用時に当該要件を満たしているかサービス内容を確認すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 外部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こと。
- ② 外部情報サービスの利用時に、当該サービスが①の要件を満たしているか確認していること。

【自己評価方法】

- ① 外部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ことを確認するとともに、その文書名を確認する。
- ② 外部情報サービス利用に係る社内ルール等を確認し、外部情報サービスの利用時に、当該サービスが①の要件を満たしているかを確認するルールとなっていることを確認する。

(2) No.3-1-3-2 ★3

【評価基準】

外部情報サービスの提供事業者と機密情報の取扱いについて合意を取り交わすこと。

【対象外となるための条件】

該当なし

【適合基準】

- ① 外部情報サービスの提供事業者と、機密情報の取扱いについて合意を取り交わしていること。契約等により合意を取り交わすことが困難な場合は、提供事業者が公開する情報又は説明書等により、機密情報の取扱いを確認していること。

【自己評価方法】

- ① 外部情報サービスの利用規約、契約書、合意書、提供事業者が公開する情報又は説明書等を確認し、外部情報サービスの提供事業者と、機密情報の取扱いについて合意を取り交わしていること、又は、契約等により合意を取り交わすことが困難な場合に、提供事業者が公開する情報又は説明書等により、機密情報の取扱いを確認していることを確認するとともに、その文書名を確認する。

3-1-4 機密区分に応じた情報の管理**【要求事項】**

機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。

(1) No.3-1-4-1 ★3**【評価基準】**

自社の保有する情報を対象に、以下の内容を含む管理ルールを定めること。

- 機密の特定
- 機密区分のレベル判定及び表示
- 区分に応じた取扱方法
- 取扱エリアの区分及び制限

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社の保有する情報の管理ルールを定めていること。
- ② ①の管理ルールには、以下の全ての内容を含んでいること。
 - 機密の特定
 - 機密区分のレベル判定及び表示
 - 区分に応じた取扱方法
 - 取扱エリアの区分及び制限

【自己評価方法】

- ① 情報管理規程等を確認し、自社の保有する情報の管理ルールを定めていることを確認するとともに、その文書名を確認する。
- ② 情報管理規程等を確認し、①の管理ルールには、以下の全ての内容を含んでいることを確認する。
 - 機密の特定
 - 機密区分のレベル判定及び表示
 - 区分に応じた取扱方法
 - 取扱エリアの区分及び制限

(2) No.3-1-4-2 ★3**【評価基準】**

年1回以上の頻度で No.3-1-4-1 で定めた管理ルールの内容について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-4-1 で定めた管理ルールの内容について、年1回以上の頻度で点検しているこ

と。

【自己評価方法】

- ① No.3-1-4-1 で定めた管理ルールの内容を点検した記録を確認し、年 1 回以上の頻度で点検を行っていることを確認する。

(3) No.3-1-4-3 ★3

【評価基準】

重要な機密情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備していること。

【自己評価方法】

- ① 情報資産管理台帳、情報資産管理ツールなど、どのように重要な機密情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備しているかを確認する。

(4) No.3-1-4-4 ★4

【評価基準】

年 1 回以上の頻度で No.3-1-4-3 で把握した項目の内容について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-4-3 で把握した項目の内容について、年 1 回以上の頻度で点検していること。

【自己評価方法】

- ① 情報資産管理台帳、情報資産管理ツール等の棚卸を実施した記録等を確認し、No.3-1-4-3 で把握した項目の内容について、年 1 回以上の頻度で点検していることを確認する。

(5) No.3-1-4-5 ★4

【評価基準】

退職時及び任期満了時には機密情報及び情報機器を回収すること。

- 回収物には、情報（印刷物及び記憶媒体）、パソコン、スマートデバイス及びアクセス権（ID 及び鍵）を含めること。
- 回収漏れが起こらない手順（例：回収物一覧のチェックシートの作成）を整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 退職時及び任期満了時に、機密情報及び情報機器を回収していること。
- ② ①の回収対象には、情報（印刷物及び記憶媒体）、パソコン、スマートデバイス並びにアクセス権（ID 及び鍵）を含めていること。
- ③ 回収漏れが起こらない手順を整備していること。

【自己評価方法】

- ① 退職・任期満了時の回収手順を確認し、退職時及び任期満了時に、機密情報及び情報機器を回収していることを確認する。
- ② ①の回収対象には、情報（印刷物及び記憶媒体）、パソコン、スマートデバイス並びにアクセス権（ID 及び鍵）を含めていることを確認する。
- ③ 退職・任期満了時の回収手順、回収物チェックリスト等を確認し、回収漏れが起こらない手順を整備していることを確認する。

(6) No.3-1-4-6 ★4

【評価基準】

年 1 回以上の頻度で No.3-1-4-5 で求める機密情報及び情報機器の回収の状況について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-4-5 で求める機密情報及び情報機器の回収状況について、年 1 回以上の頻度で点検していること。

【自己評価方法】

- ① No.3-1-4-5 で求める機密情報及び情報機器の回収状況を点検した記録を確認し、年 1 回以上の頻度で点検していることを確認する。

(7) No.3-1-4-7 ★4

【評価基準】

サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の廃棄時（リース終了時を含む。）はデータを復元できないよう抹消処理を行うこと。

※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十分

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の廃棄時（リース終了時を含む。）に、データを復元できない方法で抹消処理を行っていること。

【自己評価方法】

- ① 廃棄手順、データ消去証明書、廃棄作業記録等を確認し、サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の廃棄時（リース終了時を含む。）に、データを復元できない方法で抹消処理を行っていることを確認する。

(8) No.3-1-4-8 ★4**【評価基準】**

サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の記憶領域を抹消処理した記録を保管すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の記憶領域を抹消処理した記録を保管していること。

【自己評価方法】

- ① データ消去証明書、廃棄作業記録等を確認し、サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の記憶領域を抹消処理した記録を保管していることを確認するとともに、その文書名を確認する。

3-1-5 リモートワークにおけるルール**【要求事項】**

リモートワークで使用する情報機器及び機密情報の条件についてのルールを定めること。

(1) No.3-1-5-1 ★4**【評価基準】**

リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件について、以下の事項に関するルールを定めること。

- リモートワークで使用許可する情報機器及び当該許可の申請・承認の方法
- 個人所有機器にダウンロード可能なファイルの機密区分及び種類

【対象外となるための条件】

リモートワークを行う役員、従業員、派遣社員及び受入出向者が存在しない場合

【適合基準】

- ① リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件についてルールを定めていること。
- ② ①のルールは、以下の全ての事項を含んでいること。
 - リモートワークで使用を許可する情報機器及び当該許可の申請・承認の方法
 - 個人所有機器にダウンロード可能なファイルの機密区分及び種類

【自己評価方法】

- ① リモートワーク実施に係るルールを確認し、リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件についてルールを定めていることを確認するとともに、その文書名を確認する。
- ② リモートワーク規程、利用申請・承認記録、端末管理台帳及び点検記録等を確認し、①のルールには、以下の全ての事項を含んでいることを確認する。
 - リモートワークで使用許可する情報機器及び当該許可の申請・承認の方法
 - 個人所有機器にダウンロード可能なファイルの機密区分及び種類

(2) No.3-1-5-2 ★4**【評価基準】**

No.3-1-5-1 で定めたルールについて、リモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に対して周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-5-1 で定めたルールを、リモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、No.3-1-5-1で定めたルールが、リモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に周知されていることを確認する。

(3) No.3-1-5-3 ★4**【評価基準】**

年1回以上の頻度でNo.3-1-5-1で定めたルールの内容及び遵守状況について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.3-1-5-1で定めたルールの内容について、年1回以上の頻度で点検していること。
- ② No.3-1-5-1で定めたルールの遵守状況について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① リモートワーク規程、利用申請・承認記録、端末管理台帳及び点検記録等を確認し、No.3-1-5-1で定めたルールの内容について、年1回以上の頻度で点検していることを確認する。
- ② リモートワーク規程、利用申請・承認記録、端末管理台帳及び点検記録等を確認し、No.3-1-5-1で定めたルールの遵守状況について、年1回以上の頻度で点検していることを確認する。

3-2 リスクアセスメント

3-2-1 脆弱性の管理体制

【要求事項】

脆弱性の管理体制、管理プロセスを定め、それに基づく管理を行うこと。

(1) No.3-2-1-1 ★4

【評価基準】

脆弱性情報/脅威情報の収集から対応まで担当部署の役割・責任を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 脆弱性情報及び脅威情報の収集から対応までについて、担当部署の役割及び責任を定めていること。

【自己評価方法】

- ① 脆弱性管理規程等の脆弱性情報及び脅威情報の収集から対応までについて定めた文書を確認し、担当部署の役割及び責任を定めていることを確認するとともに、どのような文書に記載しているかを確認する。

(2) No.3-2-1-2 ★4

【評価基準】

脆弱性情報/脅威情報を収集する情報源、ツール及び頻度を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 脆弱性情報/脅威情報を収集する情報源、ツール及び頻度を定めていること。

【自己評価方法】

- ① 脆弱性情報/脅威情報を収集する情報源、ツール及び収集頻度を定めていることを確認するとともに、どのような文書に記載しているかを確認する。

(3) No.3-2-1-3 ★4

【評価基準】

収集した脆弱性情報/脅威情報の対応要否判断基準・対応手順を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 収集した脆弱性情報/脅威情報の対応要否判断基準及び対応手順を定めていること。

【自己評価方法】

- ① 脆弱性管理規程等を確認し、収集した脆弱性情報/脅威情報の対応要否判断基準及び対応手順を定めていることを確認するとともに、その基準及び手順の文書名を確認する。

(4) No.3-2-1-4 ★4**【評価基準】**

管理対象の情報機器における脆弱性の残存状況を把握するための仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 管理対象の情報機器における脆弱性の残存状況を把握する仕組みを整備していること。

【自己評価方法】

- ① 脆弱性管理台帳、脆弱性管理ツール等、どのように管理対象の情報機器における脆弱性の残存状況を把握する仕組みを整備しているかを確認する。

(5) No.3-2-1-5 ★4**【評価基準】**

収集した脆弱性情報/脅威情報に対する対応履歴を記録し、対応漏れがないかどうかについて月次で点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 収集した脆弱性情報及び脅威情報に対する対応履歴を記録していること。
- ② 対応漏れがないか、月 1 回以上の頻度で点検していること。

【自己評価方法】

- ① 脆弱性管理台帳、脆弱性管理ツール等を確認し、収集した脆弱性情報及び脅威情報に対する対応履歴を記録していることを確認する。
- ② 脆弱性管理台帳、脆弱性管理ツール等を確認し、対応漏れがないか、月 1 回以上の頻度で点検していることを確認する。

4. 攻撃等の防御

4-1 アイデンティティ管理、認証、アクセス制御

4-1-1 ユーザ ID の管理手続

【要求事項】

ユーザ ID の発行・変更・削除の手続を定めること。

(1) No.4-1-1-1 ★3

【評価基準】

自社の役員、従業員、派遣社員及び受入出向者に対するユーザ ID の付与・変更・削除は申請・承認制にすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社の役員、従業員、派遣社員及び受入出向者に対するユーザ ID の付与・変更・削除を申請・承認制としていること。

【自己評価方法】

- ① ID 管理規程等を確認し、自社の役員、従業員、派遣社員及び受入出向者に対するユーザ ID の付与・変更・削除を申請・承認制としていることを確認するとともに、その文書名を確認する。

(2) No.4-1-1-2 ★3

【評価基準】

ユーザ ID の共有について、以下のいずれかを適用すること。

- ユーザ ID を共有しない。
- やむを得ず共有 ID が必要な場合（例えば、システムの仕様により、使用人数分のユーザ ID を発行することができない場合）は、共有 ID を利用したユーザを特定できるようにする。

【対象外となるための条件】

該当なし

【適合基準】

- ① ユーザ ID の共有について、以下のいずれかの手続を適用していること。
- ユーザ ID を共有しない。
 - やむを得ず共有 ID が必要な場合（例えば、システムの仕様により、使用人数分のユーザ ID を発行することができない場合）は、共有 ID を利用したユーザを特定できるようにする。

【自己評価方法】

①ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、ユーザ ID の共有について、以下のいずれかの手続を適用していることを確認する。

- ユーザ ID を共有しない。
- やむを得ず共有 ID が必要な場合（例えば、システムの仕様により、使用人数分のユーザ ID を発行することができない場合）は、共有 ID を利用したユーザを特定できるようにする。

(3) No.4-1-1-3 ★3**【評価基準】**

ユーザ ID が不要になった場合（例えば、ユーザが組織を退職した場合又はユーザ ID が一定期間使用されなかった場合）、速やかにユーザ ID を削除又は無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ユーザ ID が不要になった場合、速やかに当該ユーザ ID を削除又は無効化する手続を定めていること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、ユーザ ID が不要になった場合、速やかに当該ユーザ ID を削除又は無効化する手続を定めていることを確認する。

(4) No.4-1-1-4 ★3**【評価基準】**

ユーザ ID に付与したアクセス権が不要になった場合（例えば、ユーザの業務上の役割が変わった場合）は、当該権限を速やかに削除又は無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ユーザ ID に付与したアクセス権が不要になった場合、速やかに当該権限を削除又は無効化する手続を定めていること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、ユーザ ID に付与したアクセス権が不要になった場合、速やかに当該権限を削除又は無効化する手続を定めていることを確認する。

4-1-2 管理者 ID の管理手続**【要求事項】**

管理者 ID の発行・変更・削除の手続を定めること。

(1) No.4-1-2-1 ★3**【評価基準】**

すべてのサーバ及びネットワーク機器について、システム管理者及び責任者を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① すべてのサーバ及びネットワーク機器について、システム管理者及び責任者を定めていること。

【自己評価方法】

- ① システム管理台帳等を確認し、全てのサーバ及びネットワーク機器について、システム管理者及び責任者を定めていることを確認するとともに、その文書名を確認する。

(2) No.4-1-2-2 ★3**【評価基準】**

管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者 ID について以下のいずれかを適用すること。

- 管理者 ID を共有しない。
- やむを得ず管理者 ID の共有が必要な場合（例えば、システムの仕様により、使用人数分の ID を発行することができない場合）は、共有の管理者 ID を利用したユーザを特定できるようにすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者 ID について以下のいずれかを適用していること。
- 管理者 ID を共有しない。
 - やむを得ず管理者 ID の共有が必要な場合（例えば、システムの仕様により、使用人数分の ID を発行することができない場合）は、共有の管理者 ID を利用したユーザを特定できるようにすること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者 ID について以下のい

いずれかを適用していることを確認する。

- 管理者 ID を共有しない。
- やむを得ず管理者 ID の共有が必要な場合（例えば、システムの仕様により、使用人数分の ID を発行することができない場合）は、共有の管理者 ID を利用したユーザを特定できるようにする。

(3) No.4-1-2-3 ★3

【評価基準】

各管理者 ID に対して当該 ID の用途に応じた必要最低限の権限のみを付与すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 各管理者 ID に、当該 ID の用途に応じた必要最低限の権限のみを付与していること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、各管理者 ID に、当該 ID の用途に応じた必要最低限の権限のみを付与していることを確認する。

(4) No.4-1-2-4 ★3

【評価基準】

開発環境を利用する役員、従業員、派遣社員及び受入出向者が本番環境において、開発環境における管理者権限で操作できないようにすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 開発環境を利用する役員、従業員、派遣社員及び受入出向者が、本番環境において開発環境の管理者権限で操作できないようにしていること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、開発環境を利用する役員、従業員、派遣社員及び受入出向者が、本番環境において開発環境の管理者権限で操作できないようにしていることを確認する。

(5) No.4-1-2-5 ★3

【評価基準】

組織内でどの役員、従業員、派遣社員及び受入出向者が管理者 ID を持っているかを把握するための仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 組織内の役員、従業員、派遣社員及び受入出向者のうち、誰が管理者 ID を持っているかを把握する仕組みを整備していること。

【自己評価方法】

- ① ID 管理台帳、ID 管理システムなど、どのように組織内の役員、従業員、派遣社員及び受入出向者のうち、誰が管理者 ID を持っているかを把握する仕組みを整備しているかを確認する。

(6) No.4-1-2-6 ★3**【評価基準】**

管理者 ID が不要になった場合（例えば、管理者が組織を退職した場合及び管理者 ID が一定期間使用されなかった場合）、速やかに管理者 ID を削除又は無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 管理者 ID が不要になった場合、速やかに当該管理者 ID を削除又は無効化していること。

【自己評価方法】

- ① ID 管理規程、ID 管理台帳、ID 管理システム等を確認し、管理者 ID が不要になった場合、速やかに当該管理者 ID を削除又は無効化していることを確認する。

(7) No.4-1-2-7 ★3**【評価基準】**

管理者 ID の付与・変更・削除は申請・承認制にすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 管理者 ID の付与・変更・削除を申請・承認制としていること。

【自己評価方法】

- ① ID 管理規程等を確認し、管理者 ID の付与・変更・削除を申請・承認制としていることを確認するとともに、その文書名を確認する。

(8) No.4-1-2-8 ★3**【評価基準】**

管理者 ID の付与・変更・削除並びにサーバ及びネットワーク機器の設定内容の変更を行う権限を業務上必要な役員、従業員、派遣社員及び受入出向者に限定すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 管理者 ID の付与・変更・削除を行う権限を、業務上必要な役員、従業員、派遣社員及び受入出向者に限定していること。
- ② サーバ及びネットワーク機器の設定内容を変更する権限を、業務上必要な者に限定していること。

【自己評価方法】

- ① ID 管理規程等を確認し、管理者 ID の付与・変更・削除を行う権限を、業務上必要な役員、従業員、派遣社員及び受入出向者に限定していることを確認する。
- ② サーバ及びネットワーク機器の設定変更手順等を確認し、サーバ及びネットワーク機器の設定内容を変更する権限を、業務上必要な者に限定していることを確認する。

4-1-3 認証の強度・実装方法の決定

【要求事項】

システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。

(1) No.4-1-3-1 ★3

【評価基準】

すべてのユーザ ID 及び管理者 ID について、システム及び情報機器へのアクセスを許可する前に、ユーザ ID ごとに設定されている認証情報（パスワード等）でユーザを認証すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全てのユーザ ID 及び管理者 ID について、システム及び情報機器へのアクセスを許可する前に、ID ごとに設定した認証情報（パスワード等）でユーザを認証していること。

【自己評価方法】

- ① システム仕様、認証システム等を確認し、全てのユーザ ID 及び管理者 ID について、システム及び情報機器へのアクセスを許可する前に、ID ごとに設定した認証情報（パスワード等）でユーザを認証していることを確認する。

(2) No.4-1-3-2 ★3

【評価基準】

重要な機密情報を取り扱うクラウドサービスにおいて、ユーザ及び管理者がサービスにアクセスする場合は、常に No.4-1-3-3 で示す認証要素を利用した多要素認証を使用すること。

【対象外となるための条件】

重要な機密情報をクラウドサービス上で取り扱っていない場合

【適合基準】

- ① 重要な機密情報を取り扱うクラウドサービスにユーザ又は管理者がアクセスする場合、常に No.4-1-3-3 で示す 2 種類以上の認証要素を利用した多要素認証を使用していること。

【自己評価方法】

- ① クラウドサービスで重要な機密情報を取り扱っているかを確認する。
- ② 取り扱っている場合、クラウドサービスの仕様等を確認し、ユーザ又は管理者がアクセスする場合に、No.4-1-3-3 で示す 2 種類以上の認証要素のどのような組み合わせで多要素認証を実現しているかを確認する。

(3) No.4-1-3-3 ★3**【評価基準】**

多要素認証の使用に当たっては、以下のいずれかの要素から 2 種類以上を選択し、利用すること。

- 知識情報（例：ID・パスワード）
- 所有情報（例：ワンタイムパスワード※又は証明書）
- 生体情報（例：指紋、顔、虹彩又は静脈）
- その他の情報（例：IP アドレス）

※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。

【対象外となるための条件】

該当なし

【適合基準】

- ① 多要素認証では、以下に示す知識情報、所有情報、生体情報又はその他の情報のうち、異なる 2 種類以上の認証要素を選択して利用していること。

- 知識情報（例：ID・パスワード）
- 所有情報（例：ワンタイムパスワード※又は証明書）
- 生体情報（例：指紋、顔、虹彩又は静脈）
- その他の情報（例：IP アドレス）（信頼できるネットワークからのアクセスにおける補助手段としての利用に限ることに注意）

※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。

【自己評価方法】

- ① 認証システム等を確認し、多要素認証では、以下に示す知識情報、所有情報、生体情報又はその他の情報のうち、異なる 2 種類以上の認証要素を選択して利用していることを確認する。

- 知識情報（例：ID・パスワード）
- 所有情報（例：ワンタイムパスワード※又は証明書）
- 生体情報（例：指紋、顔、虹彩又は静脈）
- その他の情報（例：IP アドレス）（信頼できるネットワークからのアクセスにおける補助手段としての利用に限ることに注意）

※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。

(4) No.4-1-3-4 ★3**【評価基準】**

多要素認証の知識情報として用いるパスワードは、8 文字以上とすること。

【対象外となるための条件】

多要素認証においてパスワードを利用していない場合は対象外

【適合基準】

- ① 多要素認証の知識情報として用いるパスワードを 8 文字以上としていること。

【自己評価方法】

- ① 認証システム等を確認し、多要素認証の知識情報として用いるパスワードを 8 文字以上としていることを確認する。

(5) No.4-1-3-5 ★4**【評価基準】**

重要な機密情報を取り扱うシステムにおいて、No.4-1-3-2 で対象としているクラウドサービスへのアクセスに加えて、以下に示す場合は、常に No.4-1-3-3 で示す認証要素を使用した多要素認証を使用すること。

- インターネットを経由して社内環境へ接続する場合
- 管理者がインターネット経由でシステムにアクセスする場合
- ユーザがインターネット経由で重要な機密情報を取り扱うシステムにアクセスする場合

【対象外となるための条件】

評価基準に定める場合に該当するアクセスを行っていない

【適合基準】

- ① インターネットを経由して社内環境へ接続する場合、No.4-1-3-3 で示す認証要素を使用した多要素認証を常に使用していること。
- ② 管理者がインターネット経由でシステムにアクセスする場合、当該多要素認証を常に使用していること。
- ③ ユーザがインターネット経由で重要な機密情報を取り扱うシステムにアクセスする場合、当該多要素認証を常に使用していること。

【自己評価方法】

- ① 認証システム等を確認し、インターネットを経由して社内環境へ接続する場合、No.4-1-3-3 で示す認証要素を使用した多要素認証を常に使用していることを確認する。
- ② 認証システム等を確認し、管理者がインターネット経由でシステムにアクセスする場合、当該多要素認証を常に使用していることを確認する。
- ③ 認証システム等を確認し、ユーザがインターネット経由で重要な機密情報を取り扱うシステムにアクセスする場合、当該多要素認証を常に使用していることを確認する。

4-1-4 アカウントロック制御

【要求事項】

パソコン及びスマートデバイスにはロック制御を行うこと。

(1) No.4-1-4-1 ★3

【評価基準】

パソコンへのログオン及びスマートデバイスのロック解除にあたって、以下のいずれかを適用すること。

- 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。
- 試行が少なくとも 10 回以上失敗すると端末をロックする。
- 上記で示す要件のいずれも設定することができない場合、No.4-1-5 で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコンへのログオン及びスマートデバイスのロック解除にあたって、以下のいずれかを適用していること。
 - 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。
 - 試行が少なくとも 10 回以上失敗すると端末をロックする。
 - 上記で示す要件のいずれも設定することができない場合、No.4-1-5 の要件よりも強度の高いパスワードを用いる等の代替策を用いること。

【自己評価方法】

- ① パソコンへのログオン及びスマートデバイスのロック解除に係る仕様等を確認し、パソコンへのログオン及びスマートデバイスのロック解除にあたって、以下のいずれかを適用していることを確認する。
 - 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。
 - 試行が少なくとも 10 回以上失敗すると端末をロックする。
 - 上記で示す要件のいずれも設定することができない場合、No.4-1-5 の要件よりも強度の高いパスワードを用いる等の代替策を用いること。

(2) No.4-1-4-2 ★3

【評価基準】

パソコンへのログオン及びスマートデバイスのロック解除を行う場合、最低でも 6 文字以上のパスワード又は PIN を利用すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコンへのログオン及びスマートデバイスのロック解除に、6 文字以上のパスワード又は PIN を利用していること。

【自己評価方法】

- ① パソコンへのログオン及びスマートデバイスのロック解除に係る仕様等を確認し、パソコンへのログオン及びスマートデバイスのロック解除に、6 文字以上のパスワード又は PIN を利用していることを確認する。

4-1-5 パスワード設定ルール

【要求事項】

パスワード設定に関するルールを定め、周知すること。

(1) No.4-1-5-1 ★3

【評価基準】

パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者は、それらにおけるデフォルトパスワードを変更するよう社内ルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者が、デフォルトパスワードを変更するよう社内ルールを定めていること。

【自己評価方法】

- ① 認証・パスワード管理規程等を確認し、パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者が、デフォルトパスワードを変更するよう社内ルールを定めていることを確認するとともに、その文書名を確認する。

(2) No.4-1-5-2 ★3

【評価基準】

ユーザ認証にパスワードを利用する場合、推測されやすい単語の設定を禁止するよう社内ルールを定めること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

- ① ユーザ認証にパスワードを利用する場合、推測しやすい単語の設定を禁止する社内ルールを定めていること。

【自己評価方法】

- ① 認証・パスワード管理規程等を確認し、ユーザ認証にパスワードを利用する場合、推測しやすい単語の設定を禁止する社内ルールを定めていることを確認するとともに、その文書名を確認する。

(3) No.4-1-5-3 ★3

【評価基準】

ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じるよう社内ルールを定めること。

- No.4-1-3-3 で示す認証要素を利用した多要素認証を使用するか、又は試行が少なくとも

10 回失敗した場合にアカウントロックするように制限したうえで、パスワードの長さを 8 文字以上とする。

・ 上記のとおり多要素認証又は試行回数の制限を実施できない場合、パスワードの長さは、英大文字小文字、数字を含めた 10 文字以上とする。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

① ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じるよう社内ルールを定めていること。

・ No.4-1-3-3 で示す認証要素を利用した多要素認証を使用するか、又は試行が少なくとも 10 回失敗した場合にアカウントロックするように制限したうえで、パスワードの長さを 8 文字以上とする。

・ 上記のとおり多要素認証又は試行回数の制限を実施できない場合、パスワードの長さは、英大文字小文字、数字を含めた 10 文字以上とする。

② ①で定めた社内ルールを、ユーザ認証において適用していること。

【自己評価方法】

① 認証・パスワード管理規程等を確認し、ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じるよう社内ルールを定めていることを確認するとともに、そのルールの文書名を確認する。

・ No.4-1-3-3 で示す認証要素を利用した多要素認証を使用するか、又は試行が少なくとも 10 回失敗した場合にアカウントロックするように制限したうえで、パスワードの長さを 8 文字以上とする。

・ 上記のとおり多要素認証又は試行回数の制限を実施できない場合、パスワードの長さは、英大文字小文字、数字を含めた 10 文字以上とする。

② 認証・パスワード管理規程、システム設定画面、認証ログ及び設定確認結果等を確認し、①で定めた社内ルールを、ユーザ認証において適用していることを確認する。

(4) No.4-1-5-4 ★3

【評価基準】

ユーザ認証にパスワードを利用する場合、情報機器及びサービス間でのパスワードを使い回さないよう社内ルールを定めること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

① ユーザ認証にパスワードを利用する場合、情報機器及びサービス間でパスワードを使い回さないよう社内ルールを定めていること。

【自己評価方法】

- ① 認証・パスワード管理規程等を確認し、ユーザ認証にパスワードを利用する場合、情報機器及びサービス間でパスワードを使い回さないよう社内ルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(5) No.4-1-5-5 ★3**【評価基準】**

No.4-1-5-1 から No.4-1-5-4 までで定めたパスワード設定に関するルールについて、役員、従業員、派遣社員及び受入出向者を対象に周知すること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

- ① No.4-1-5-1 から No.4-1-5-4 までで定めたパスワード設定ルールを、役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、No.4-1-5-1 から No.4-1-5-4 までで定めたパスワード設定ルールが役員、従業員、派遣社員及び受入出向者に周知されていることを確認する。

4-1-6 パスワード管理ルール

【要求事項】

パスワードの管理に関するルールを定め、周知すること。

(1) No.4-1-6-1 ★3

【評価基準】

紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管するよう社内ルールを定めること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

- ① 紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管するよう社内ルールを定めていること。

【自己評価方法】

- ① 認証・パスワード管理規程等を確認し、紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管するよう社内ルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(2) No.4-1-6-2 ★3

【評価基準】

パスワードの漏えいが判明した場合、又はその疑いがある場合に速やかにパスワードを変更するための手順を定めること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

- ① パスワードの漏えいが判明した場合又はその疑いがある場合に該当する状況（例：利用しているサービスの提供者からの通知、取引先からの連絡）を定めていること。
- ② ①の場合に、速やかにパスワードを変更する手順を定めていること。

【自己評価方法】

- ① 認証・パスワード管理規程等を確認し、パスワードの漏えいが判明した場合又はその疑いがある場合となる要件及び漏えい又は漏えいの疑いを検知する方法を定めていることを確認するとともに、そのルールの文書名を確認する。
- ② 認証・パスワード管理規程等を確認し、①の場合に、速やかにパスワードを変更する手順を定めていることを確認するとともに、そのルールの文書名を確認する。

(3) No.4-1-6-3 ★3**【評価基準】**

No.4-1-6-1 及び No.4-1-6-2 で定めたパスワードの管理に関するルールについて、役員、従業員、派遣社員及び受入出向者を対象に周知すること。

【対象外となるための条件】

ユーザ認証にパスワードを利用しない場合

【適合基準】

- ① No.4-1-6-1 及び No.4-1-6-2 で定めたパスワード管理ルールを、役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、No.4-1-6-1 及び No.4-1-6-2 で定めたパスワード管理ルールが役員、従業員、派遣社員及び受入出向者に周知されていることを確認する。

4-1-7 アクセス権の管理ルール

【要求事項】

アクセス権の管理ルールを定めること。

(1) No.4-1-7-1 ★3

【評価基準】

業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権並びに機密上の配慮が必要な場所及び部屋への入室について、以下の内容の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。
- 入室権限及び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又は台帳を管理していること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権並びに機密上の配慮が必要な場所及び部屋への入室について、管理ルールを定めていること。
- ② ①の管理ルールは、以下の全ての内容を含んでいること。
 - 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。
 - 入室権限及び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又は台帳を管理していること。

【自己評価方法】

- ① 業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権並びに機密上の配慮が必要な場所及び部屋への入室について、管理ルールを定めていることを確認するとともに、そのルールの文書名を確認する。
- ② アクセス権台帳、棚卸記録、利用ログ、監視記録及び是正記録等を確認し、①の管理ルールには、以下の全ての内容を含んでいることを確認する。
 - 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。
 - 入室権限及び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又は台帳を管理していること。

(2) No.4-1-7-2 ★4

【評価基準】

年1回以上の頻度で役員、従業員、派遣社員及び受入出向者に付与したアクセス権の棚卸を実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 役員、従業員、派遣社員及び受入出向者に付与したアクセス権について、年1回以上の頻度で棚卸を実施していること。

【自己評価方法】

- ① アクセス権管理台帳等を確認し、役員、従業員、派遣社員及び受入出向者に付与したアクセス権について、年1回以上の頻度で棚卸を実施していることを確認する。

(3) No.4-1-7-3 ★4**【評価基準】**

重要な機密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定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報を扱うシステムについて、アクセス権を付与するための条件を定めていること。

【自己評価方法】

- ① 重要な機密情報を扱うシステムについて、アクセス権を付与するための条件を定めていることを確認するとともに、その条件を定めた文書名を確認する。

(4) No.4-1-7-4 ★4**【評価基準】**

重要な機密情報を扱うシステムにおけるアクセス権の設定に当たっては、システム管理者の要件及び設定手順を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報を扱うシステムのアクセス権設定について、システム管理者の要件及びアクセス権の設定手順を定めていること。

【自己評価方法】

- ① 重要な機密情報を扱うシステムのアクセス権設定について、システム管理者の要件及びアクセス権の設定手順を定めていることを確認するとともに、その手順の文書名を確認する。

(5) No.4-1-7-5 ★4**【評価基準】**

重要な機密情報を扱うシステムは、ユーザ及び管理者ごとに必要最小限の権限を付与し、個人に権限が集中しない環境とすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報を扱うシステムについて、ユーザ及び管理者ごとに必要最小限の権限を付与し、個人に権限が集中しない環境としていること。

【自己評価方法】

- ① 重要な機密情報を扱うシステムのシステム仕様等を確認し、重要な機密情報を扱うシステムについて、ユーザ及び管理者ごとに必要最小限の権限を付与し、個人に権限が集中しない環境としていることを確認する。

(6) No.4-1-7-6 ★4**【評価基準】**

重要な機密情報を扱うシステムは、付与したアクセス権の運用/利用状況を監視する仕組みを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報を扱うシステムについて、付与したアクセス権の運用/利用状況を監視する仕組みを整備していること。

【自己評価方法】

- ① アクセスログの取得など、重要な機密情報を扱うシステムについて、どのように付与したアクセス権の運用/利用状況を監視する仕組みを整備しているかを確認する。

4-1-8 サーバ設置エリアへの入退室管理

【要求事項】

サーバの設置エリアへの入退室を管理し、記録すること。

(1) No.4-1-8-1 ★4

【評価基準】

サーバの設置エリアに入場可能な者を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバの設置エリアに入場可能な者を定めていること。

【自己評価方法】

- ① 入退場管理規程等を確認し、サーバの設置エリアに入場可能な者を定めていることを確認するとともに、そのルール of 文書名を確認する。

(2) No.4-1-8-2 ★4

【評価基準】

サーバの設置に当たって、以下のいずれかの安全確保策を適用すること。

- サーバの設置エリアを施錠すること。
- 施錠が出来ないエリアにサーバが設置されている場合、サーバを専用ラックに入れて施錠すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバの設置に当たって、以下のいずれかの安全確保策を適用していること。

- サーバの設置エリアを施錠すること。
- 施錠が出来ないエリアにサーバを設置している場合、サーバを専用ラックに入れて施錠すること。

【自己評価方法】

- ① サーバの設置方法等を確認し、サーバの設置に当たって、以下のいずれかの安全確保策を適用していることを確認する。
- サーバの設置エリアを施錠すること。
 - 施錠ができないエリアにサーバを設置している場合、サーバを専用ラックに入れて施錠すること。

(3) No.4-1-8-3 ★4**【評価基準】**

No.4-1-8-2 におけるサーバの設置エリア又は専用ラックの鍵等について、管理者を定めたいうえで安全に管理すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバの設置エリア又は専用ラックの鍵等について管理者を定めていること。
- ② ①の鍵等を安全に管理していること。

【自己評価方法】

- ① 入退場管理規程等を確認し、サーバの設置エリア又は専用ラックの鍵等について管理者を定めていることを確認するとともに、その文書名を確認する。
- ② 入場許可者一覧、鍵管理台帳、入退場記録、施錠状況の確認記録及び保管設定等を確認し、①の鍵等を安全に管理していることを確認する。

(4) No.4-1-8-4 ★4**【評価基準】**

入退場日時及び入場者氏名を含めて、サーバの設置エリアの入退場記録を取得し、少なくとも6ヶ月間保管すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバ設置エリアへの入退場について、入退場日時及び入場者氏名を含む記録を取得していること。
- ② ①の記録を少なくとも6か月間保管していること。

【自己評価方法】

- ① 入退場記録を確認し、サーバ設置エリアへの入退場について、入退場日時及び入場者氏名を含む記録を取得していることを確認するとともに、その記録の文書名を確認する。
- ② ①の記録について、少なくとも6か月間保管していることを確認する。

4-1-9 可搬媒体の制限**【要求事項】**

可搬媒体の持込み・持出しを制限すること。

(1) No.4-1-9-1 ★4**【評価基準】**

パソコン、スマートデバイス、カメラ及び外部記憶媒体（個人所有機器の業務利用（BYOD）を含む。）を対象とした社内への持込みルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン、スマートデバイス、カメラ及び外部記憶媒体（BYOD を含む。）を対象とした社内への持込みルールを定めていること。

【自己評価方法】

- ① パソコン、スマートデバイス、カメラ及び外部記憶媒体（BYOD を含む。）を対象とした社内への持込みルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(2) No.4-1-9-2 ★4**【評価基準】**

パソコン、スマートデバイス、カメラ、外部記憶媒体（個人所有機器の業務利用（BYOD）を含む。）及び印刷物（図面等の機密書類）に関する社外への持出しルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン、スマートデバイス、カメラ、外部記憶媒体（BYOD を含む。）及び印刷物（図面等の機密書類）を対象とした社外への持出しルールを定めていること。

【自己評価方法】

- ① パソコン、スマートデバイス、カメラ、外部記憶媒体（BYOD を含む。）及び印刷物（図面等の機密書類）を対象とした社外への持出しルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(3) No.4-1-9-3 ★4**【評価基準】**

年1回以上の頻度で No.4-1-9-1 及び No.4-1-9-2 で定めたパソコン、スマートデバイス、カメラ及び外部記憶媒体（個人所有機器（BYOD）を含む。）における持込みルール及び持出しルール内容及び遵守状況について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.4-1-9-1 及び No.4-1-9-2 で定めた持込み・持出しルールの内容について、年1回以上の頻度で点検していること。
- ② ①のルールの遵守状況について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① No.4-1-9-1 及び No.4-1-9-2 で定めた持込み・持出しルールの内容を点検した記録を確認し、年1回以上の頻度で点検していることを確認する。
- ② ①のルールの遵守状況を点検した記録を確認し、年1回以上の頻度で点検していることを確認する。

4-2 意識向上とトレーニング

4-2-1 セキュリティの意識向上のための教育・研修

【要求事項】

経営層を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること。

(1) No.4-2-1-1 ★4

【評価基準】

経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けていること。

【自己評価方法】

- ① セキュリティ教育・研修計画、セキュリティ教材、セキュリティ教育・研修の実施記録等を確認し、経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けていることを確認する。

(2) No.4-2-1-2 ★4

【評価基準】

セキュリティに関する職場特有のリスクの理解及びルールへの遵守が必要な場合、職場単位で重要なルール及びリスクについて、年1回以上の頻度で周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティに関する職場特有のリスクの理解及びルールへの遵守が必要な場合、職場単位で重要なルール及びリスクを年1回以上の頻度で何らかの手段・媒体により周知していること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、セキュリティに関する職場特有のリスクの理解及びルールへの遵守が必要な場合、職場単位で重要なルール及びリスクが年1回以上の頻度で周知されていることを確認する。

(3) No.4-2-1-3 ★4

【評価基準】

以下のトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ

時、かつ、年1回以上、教育資料配布・掲示、eラーニング、集合教育等による教育・研修を実施すること。

- 電子メールによるマルウェア感染の予防
- Web閲覧によるマルウェア感染の予防
- 機密区分の定義と取扱い

【対象外となるための条件】

該当なし

【適合基準】

- ① 以下の全てのトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、教育資料配布・掲示、eラーニング、集合教育等による教育・研修を実施していること。

- 電子メールによるマルウェア感染の予防
- Web閲覧によるマルウェア感染の予防
- 機密区分の定義と取扱い

- ② ①の教育・研修については、新規受入れ時、かつ、年1回以上実施していること。

【自己評価方法】

- ① セキュリティ教育・研修計画、セキュリティ教材、セキュリティ教育・研修の実施記録等を確認し、以下の全てのトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、教育資料配布・掲示、eラーニング、集合教育等による教育・研修を実施していることを確認する。

- 電子メールによるマルウェア感染の予防
- Web閲覧によるマルウェア感染の予防
- 機密区分の定義と取扱い

- ② 教育・訓練計画、教材、周知記録、実施記録及び受講記録等を確認し、①の教育・研修については、新規受入れ時、かつ、年1回以上実施していることを確認する。

(4) No.4-2-1-4 ★4

【評価基準】

No.4-2-1-3 で実施した教育・研修の実施状況を記録し、保管すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.4-2-1-3 で実施した教育・研修の実施状況を記録していること。
- ② ①の記録（以下同じ）を保管していること。

【自己評価方法】

- ① セキュリティ教育・研修の実施記録を確認し、No.4-2-1-3 で実施した教育・研修の実施状況を記録していることを確認するとともに、その記録の文書名を確認する。

- ② 教育・訓練計画、教材、周知記録、実施記録及び受講記録等を確認し、①の記録を保管していることを確認する。

(5) No.4-2-1-5 ★4

【評価基準】

年1回以上の頻度でセキュリティの意識向上のための教育・研修の実施内容について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティの意識向上のための教育・研修の実施内容について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① セキュリティ教育・研修計画の検討記録等を確認し、セキュリティの意識向上のための教育・研修の実施内容について、年1回以上の頻度で点検していることを確認する。

4-2-2 セキュリティインシデント発生時の教育・訓練**【要求事項】**

セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。

(1) No.4-2-2-1 ★3**【評価基準】**

役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年1回以上の頻度で、セキュリティインシデント発生時の対応について、教育資料の配布・掲示に加え、eラーニング又は集合教育による教育・訓練を実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時かつ年1回以上、セキュリティインシデント発生時の対応に関する教育資料を配布又は掲示していること。
- ② ①に加え、eラーニング又は集合教育による教育・訓練を実施していること。

【自己評価方法】

- ① セキュリティ教育・訓練計画、セキュリティ教材、セキュリティ教育・訓練の実施記録等を確認し、役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時かつ年1回以上、セキュリティインシデント発生時の対応に関する教育資料を配布又は掲示していることを確認するとともに、その文書名を確認する。
- ② セキュリティ教育・訓練計画、セキュリティ教材、セキュリティ教育・訓練の実施記録等を確認し、①に加え、eラーニング又は集合教育による教育・訓練を実施していることを確認する。

(2) No.4-2-2-2 ★3**【評価基準】**

No.4-2-2-1 で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録し、保管すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.4-2-2-1 で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録していること。
- ② ①の記録を保管していること。

【自己評価方法】

- ① セキュリティ教育・訓練の実施記録を確認し、No.4-2-2-1 で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録していることを確認するとともに、そ

の記録の文書名を確認する。

- ② セキュリティ教育・訓練の実施記録を確認し、①の記録を保管していることを確認する。

(3) No.4-2-2-3 ★3

【評価基準】

年1回以上の頻度でセキュリティインシデント発生時の対応に関する教育・訓練の実施内容について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティインシデント発生時の対応に関する教育・訓練の実施内容について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① セキュリティ教育・訓練計画の検討記録等を確認し、セキュリティインシデント発生時の対応に関する教育・訓練の実施内容について、年1回以上の頻度で点検していることを確認する。

4-3 データセキュリティ

4-3-1 データの暗号化

【要求事項】

情報機器及び情報システムの保管データを適切に暗号化するようルールを定め、周知すること。

(1) No.4-3-1-1 ★4

【評価基準】

社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化するルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。

【対象外となるための条件】

社外にパソコン及び記憶媒体を持ち出すことが一切ない場合。

【適合基準】

- ① 社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化するルールを定めていること。
- ② 当該ルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。
- ③ ①のルールに従って、社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化していること。

【自己評価方法】

- ① 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化するルールを定めていることを確認するとともに、その文書名を確認する。
- ② 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、当該ルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していることを確認する。
- ③ 暗号化の方式に応じて暗号化設定画面等を確認し、①のルールに従って、実際に社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化していることを確認する。

(2) No.4-3-1-2 ★4

【評価基準】

重要な機密情報を暗号化するルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報を暗号化するルールを定めていること。

- ② 当該ルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。
- ③ ①のルールに従って、重要な機密情報を暗号化していること。

【自己評価方法】

- ① 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、重要な機密情報を暗号化するルールを定めていることを確認するとともに、その文書名を確認する。
- ② 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、当該ルールを役員、従業員、派遣社員及び受入出向者に周知していることを確認する。
- ③ 暗号化の方式に応じて暗号化設定画面等を確認し、①のルールに従って、実際に重要な機密情報を暗号化していることを確認する。

4-3-2 データの保管ルール

【要求事項】

データを適切な場所に保管するようルールを定め、周知すること。

(1) No.4-3-2-1 ★4

【評価基準】

マルウェアによる被害を受けた場合に業務に支障をきたすデータはパソコン以外の社内ネットワーク（クラウドサービスを含む。）上の相対的に安全な区域にあるサーバに保管するようルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① マルウェア被害を受けた場合に業務に支障をきたすデータの要件及び当該データの保管場所を定めていること。
- ② ①で定めたデータを①で定めた場所へ保管するルールを定めていること。
- ③ ②のルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。
- ④ ①のルールに従って、データの保管を行っていること。

【自己評価方法】

- ① 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、マルウェア被害を受けた場合に業務に支障をきたすデータの要件及び当該データの保管場所を定めていることを確認する。
- ② 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、①の内容をルールとして定めていることを確認する。
- ③ 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、当該ルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していることを確認する。
- ④ ネットワーク図等を確認し、①のルールに従って、データの保管を行っていることを確認する。

4-3-3 取引先との情報共有ルール

【要求事項】

取引先との情報共有及び情報送信に関するルールを定め、周知すること。

(1) No.4-3-3-1 ★4

【評価基準】

取引先との情報共有及び情報送信に関して、以下をルールとして定め、役員、従業員、派遣社員及び受入出向者へ周知すること。

- 社外とファイル共有する場合は、信頼できる相手とのみ共有すること。
- 社外へファイル転送をする場合は、送信履歴を残すこと。

【対象外となるための条件】

該当なし

【適合基準】

- ① 取引先との情報共有及び情報送信に関するルールを定めていること。
- ② ①のルールは以下の全ての内容を含んでいること。
 - 社外とファイル共有する場合は、信頼できる相手とのみ共有すること。
 - 社外へファイル転送をする場合は、送信履歴を残すこと。
- ③ ①のルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していること。

【自己評価方法】

- ① 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、取引先との情報共有及び情報送信に関するルールを定めていることを確認するとともに、その文書名を確認する。
- ② ①のルールには以下の全ての内容を含んでいることを確認する。
 - 社外とファイル共有する場合は、信頼できる相手とのみ共有すること。
 - 社外へファイル転送をする場合は、送信履歴を残すこと。
- ③ 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、①のルールを役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していることを確認する。

4-3-4 適切なバックアップ**【要求事項】**

適切なバックアップを行うこと。

(1) No.4-3-4-1 ★3**【評価基準】**

取得対象、取得頻度及び保管期間を定めて自社で取り扱うデータのバックアップを取得すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社で取り扱うデータについて、バックアップの取得対象、取得頻度及び保管期間を定めていること。
- ② ①で定めた内容に従いバックアップを取得していること。

【自己評価方法】

- ① 情報取扱規程等のデータの取扱いに関して定めているルールを確認し、自社で取り扱うデータについて、バックアップの取得対象、取得頻度及び保管期間を定めていることを確認するとともに、その文書名を確認する。
- ② バックアップファイル等を確認し、①で定めた内容に従いバックアップを取得していることを確認する。

(2) No.4-3-4-2 ★3**【評価基準】**

重要な機密情報については、No.4-3-4-1におけるバックアップに加えて、遠隔地バックアップを実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 重要な機密情報について、No.4-3-4-1のバックアップに加えて遠隔地バックアップを実施していること。
※ネットワーク的に分離されたクラウドストレージ又は物理的に接続されていない媒体に保存する場合も、遠隔地バックアップに相当する対策として扱うことができる。

【自己評価方法】

- ① バックアップファイル等を確認し、重要な機密情報について、No.4-3-4-1のバックアップに加えて遠隔地バックアップを実施していることを確認する。
※ネットワーク的に分離されたクラウドストレージ又は物理的に接続されていない媒体に保存する場合も、保存先の構成又は接続状態を確認した上で、遠隔地バックアップに

相当する対策として扱うことができる。

(3) No.4-3-4-3 ★3

【評価基準】

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。

【対象外となるための条件】

該当なし

【適合基準】

① バックアップ対象ごとにリストア手順書を整備していること。

【自己評価方法】

① バックアップ対象ごとにリストア手順書を整備していることを確認するとともに、その手順の文書名を確認する。

4-4 プラットフォームセキュリティ

4-4-1 情報機器、OS 及びソフトウェアの安全な構成

【要求事項】

情報機器、OS 及びソフトウェアの安全な構成を確立し、維持すること。

(1) No.4-4-1-1 ★3

【評価基準】

パソコン、サーバ及びスマートデバイスで利用を許可していないソフトウェアを全て削除若しくは無効化するか、又は利用を許可するソフトウェア以外を自由にインストールできないようにすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン、サーバ及びスマートデバイスについて、利用を許可していないソフトウェアを全て削除又は無効化していること。又は、許可したソフトウェア以外を自由にインストールできないようにしていること。

【自己評価方法】

- ① IT 資産管理システム、グループポリシー等を確認し、パソコン、サーバ及びスマートデバイスについて、利用を許可していないソフトウェアを全て削除又は無効化していること、又は、許可したソフトウェア以外を自由にインストールできないようにしていることを確認する。

(2) No.4-4-1-2 ★3

【評価基準】

外部記憶媒体を使用する端末について自動実行（auto-run）又は自動再生（auto-play）を無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 外部記憶媒体を使用する端末について、自動実行（auto-run）又は自動再生（auto-play）を無効化していること。

【自己評価方法】

- ① 設定画面等を確認し、外部記憶媒体を使用する端末について、自動実行（auto-run）又は自動再生（auto-play）を無効化していることを確認する。

(3) No.4-4-1-3 ★3**【評価基準】**

サーバ及びネットワーク機器の設定変更を申請・承認制にすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① サーバ及びネットワーク機器の設定変更を申請・承認制としていること。

【自己評価方法】

- ① 設定変更手順等を確認し、サーバ及びネットワーク機器の設定変更を申請・承認制としていることを確認するとともに、その文書名を確認する。

(4) No.4-4-1-4 ★4**【評価基準】**

パソコン及びサーバ上で不要サービス及びプロトコルを無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン及びサーバ上の不要なサービス及びプロトコルを無効化していること。

【自己評価方法】

- ① 設定画面等を確認し、パソコン及びサーバ上の不要なサービス及びプロトコルを無効化していることを確認する。

(5) No.4-4-1-5 ★4**【評価基準】**

パソコン及びサーバ上で使用されているデフォルトユーザ ID の利用を停止するか、又はログインに当たって多要素認証等の強固な認証を用いること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン及びサーバ上のデフォルトユーザ ID の利用を停止するか、又は、当該 ID でのログインに多要素認証等の強固な認証を用いていること。

【自己評価方法】

- ① 設定画面等を確認し、パソコン及びサーバ上のデフォルトユーザ ID の利用を停止するか、又は、当該 ID でのログインに多要素認証等の強固な認証を用いていることを確認する。

(6) No.4-4-1-6 ★4

【評価基準】

利用する OS 及びソフトウェアについて、標準構成・設定ルールを定めること。

【対象外となるための条件】

該当なし

【適合基準】

① 利用する OS 及びソフトウェアについて、標準構成・設定ルールを定めていること。

【自己評価方法】

① 構成管理ツール等を確認し、利用する OS 及びソフトウェアについて、標準構成・設定ルールを定めていることを確認するとともに、そのルールの文書名を確認する。

4-4-2 サポート期限の切れた OS 及びソフトウェアへの対策

【要求事項】

サポート期限の切れた OS 及びソフトウェアの利用停止及び更改を実施すること。

(1) No.4-4-2-1 ★4

【評価基準】

利用する OS 及びソフトウェアについて、以下のいずれかを適用すること。

- 全ての OS 及びソフトウェアについてサポートのあるものを利用すること。
- やむを得ずサポート切れの OS 及びソフトウェアをそのまま利用する場合（例えば、代替システムを調達する必要がある、直ちに更改できない場合）は、更改計画を策定した上で、更改するまでの間、脆弱性悪用のリスクを低減する対策を実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全ての OS 及びソフトウェアについて、サポートの有無を把握していること。
- ② 全ての OS 及びソフトウェアについてサポートがあるものを利用していること。
- ③ やむを得ずサポート切れのものを利用する場合は更改計画を策定し、更改までの間、No.4-4-4-2 で求める脆弱性悪用リスクの低減策を実施していること。

【自己評価方法】

- ① IT 資産管理台帳、構成管理情報等を確認し、全ての OS 及びソフトウェアについて、サポートの有無を把握していることを確認する。
- ② IT 資産管理台帳、構成管理情報等を確認し、全ての OS 及びソフトウェアについてサポートのあるものを利用していることを確認する。
- ③ やむを得ずサポート切れのものを利用している場合は更改計画を策定し、更改までの間、No.4-4-4-2 で求める脆弱性悪用リスクの低減策を実施していることを確認する。

4-4-3 ログの取得

【要求事項】

システムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと。

(1) No.4-4-3-1 ★4

【評価基準】

インシデント発生時に調査を円滑に行うために必要なログとして、以下を取得及び保管すること。(※)

[取得するログ（保管期間）]

- ファイアウォールのログ（6 カ月） ※取引先と接続する閉域網の入口に設置されるものも含む。

取得項目：日時、送信元 IP アドレス及び送信先 IP アドレス

- プロキシサーバのログ（6 カ月）

取得項目：日時、リクエスト元 IP アドレス及び URL

- 認証サーバのログ（6 カ月）

取得項目：日時、接続元 IP アドレス、ユーザ ID 及び成功/失敗

※クラウドサービスの利用も対象に含む。

※利用するクラウドサービス又はシステム構成の仕様上、上記の要件を満たせない場合は、インシデント発生時の調査ができるよう、他の機器又は機能を利用して上記の要件に相当するログを取得及び保管すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① インシデント発生時に調査を円滑に行うために必要なログとして、以下の全てを取得していること。

[取得するログ]

- ファイアウォールのログ※取引先と接続する閉域網の入口に設置するものも含む。

取得項目：日時、送信元 IP アドレス及び送信先 IP アドレス

- プロキシサーバのログ

取得項目：日時、リクエスト元 IP アドレス及び URL

- 認証サーバのログ

取得項目：日時、接続元 IP アドレス、ユーザ ID 及び成功/失敗

- ② ①で取得したログについて、6 か月間保管していること。

※クラウドサービスの利用も対象に含む。

※利用するクラウドサービス又はシステム構成の仕様上、①の要件を満たせない場合は、インシデント発生時の調査ができるよう、他の機器又は機能を利用して①の要件に相当するログを取得し、②の期間保管していること。

【自己評価方法】

- ① ログファイル、ログ取得に係るルール等を確認し、インシデント発生時に調査を円滑に行うために必要なログとして、以下の全てを取得していることを確認するとともに、その文書名を確認する。

[取得するログ]

- ファイアウォールのログ※取引先と接続する閉域網の入口に設置するものも含む。

取得項目：日時、送信元 IP アドレス及び送信先 IP アドレス

- プロキシサーバのログ

取得項目：日時、リクエスト元 IP アドレス及び URL

- 認証サーバのログ

取得項目：日時、接続元 IP アドレス、ユーザ ID 及び成功/失敗

- ② ログ取得設定、保存先設定、保管記録、監視記録及びアラート調査記録等を確認し、①で取得したログについて、6 か月間保管していることを確認する。

(2) No.4-4-3-2 ★4**【評価基準】**

No.4-4-3-1 で取得及び保管を求めるログを脅威から保護するため、ログを保存する媒体及びシステムにインターネット経由でアクセスする場合は、常に No.4-1-3-3 で示す要素を利用した多要素認証を使用すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ログの保存媒体又はシステムへのアクセス方法を把握していること。
- ② ①において、No.4-4-3-1 で求めるログの保存媒体又はシステムにインターネット経由でアクセスする場合、常に No.4-1-3-3 で示す認証要素を利用した多要素認証を使用していること。

【自己評価方法】

- ① システムの仕様、ネットワーク図等を確認し、ログの保存媒体又はシステムへインターネット経由でアクセスするかどうかを確認する。
- ② ログの保存媒体又はシステムの認証に係る仕様等を確認し、No.4-4-3-1 で求めるログの保存媒体又はシステムにインターネット経由でアクセスする場合は、No.4-1-3-3 で示す認証要素を利用した多要素認証を常に使用していることを確認する。

(3) No.4-4-3-3 ★4**【評価基準】**

No.4-4-3-1 で取得及び保管を求めるログのうち、認証サーバのログについては、月 1 回以上の頻度でモニタリングを実施し、不審な認証試行を検知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 認証サーバのログについて、月 1 回以上の頻度でモニタリングしていること。
- ② ①のモニタリングにより不審な認証試行がないかどうか確認していること。

【自己評価方法】

- ① ログのモニタリング記録等を確認し、認証サーバのログについて、月 1 回以上の頻度でモニタリングしていることを確認する。
- ② ログのモニタリング記録等を確認し、①のモニタリングにより不審な認証試行がないかどうか確認していることを確認する。

4-4-4 セキュリティパッチ・アップデートの手続

【要求事項】

情報機器、OS 及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を定めること。

(1) No.4-4-4-1 ★3

【評価基準】

情報機器、OS 及びソフトウェアについて、以下の状態とすること。

- ライセンスが付与され、サポートされている。
- サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。
- やむを得ず、サポートが終了したものを利用する場合、脆弱性悪用のリスクを低減する対策を実施している。
- 可能であれば、自動アップデートが有効化されている。

【対象外となるための条件】

該当なし

【適合基準】

① システム、情報機器及びソフトウェアを以下に示す全ての状態としていること。

- ライセンスが付与され、サポートされている。
- サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。
- やむを得ず、サポートが終了したものを利用する場合、脆弱性悪用のリスクを低減する対策を実施している。
- 可能であれば、自動アップデートが有効化されている。

【自己評価方法】

① バージョン情報、更改計画等を確認し、システム、情報機器及びソフトウェアを以下に示す全ての状態としていることを確認する。

- ライセンスが付与され、サポートされている。
- サポートが終了した場合に削除するか、又はインターネットとの全てのトラフィックを遮断して適用範囲から削除する。
- やむを得ず、サポートが終了したものを利用する場合、脆弱性悪用のリスクを低減する対策を実施している。
- 可能であれば、自動アップデートを有効にしている。

(2) No.4-4-4-2 ★3

【評価基準】

利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから 14 日以内に、アップデートすること。

- 当該アップデートが、ベンダーにより「重大」(Critical) 又は「高リスク」(High Risk) と説明される脆弱性を修正するものである。
 - 当該アップデートが、CVSS の基本値が 7.0 以上の脆弱性を修正するものである。
 - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。
- やむを得ず上記のとおりアップデートができない場合（例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合）は、アップデート適用までの間、脆弱性悪用のリスクを低減する対策を実施すること。

【対象】

- 会社支給のパソコンの OS、ブラウザ及び Office ソフト
- サーバの OS 及びミドルウェア
- 会社支給のスマートデバイスの OS 及びアプリ
- 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 及びファームウェア

【対象外となるための条件】

該当なし

【適合基準】

- ① 対象機器・ソフトウェア及び利用している機能又は設定を把握していること。
- ② ①に関する脆弱性情報をベンダーや IPA、JPCERT/CC などの公的機関から収集し、把握していること。
- ③ ベンダーが「重大 (Critical)」又は「高リスク (High Risk)」と説明する脆弱性、CVSS の基本値が 7.0 以上の脆弱性、又はベンダーが詳細を提供していない脆弱性を修正するアップデートプログラムを、リリースから 14 日以内に適用していること。
- ④ やむを得ず 14 日以内にアップデートできない場合は、アップデート適用に係る対応計画を策定し、適用までの間、脆弱性悪用のリスクを低減する以下の対策のいずれかを実施していること。

<既に攻撃を観測している脆弱性の場合>

- 脆弱性悪用の対象となる機能を無効化すること。
- ベンダーが推奨する回避策を実施すること。
- 対象となる情報機器を適用範囲内のネットワークから分離すること。
- 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入している場合、監視や設定を一時的に強化すること。

<攻撃を観測していない脆弱性の場合>

- アップデート適用に係る対応計画を、完了するまで管理、記録すること。

【自己評価方法】

- ① IT 資産管理台帳、構成管理情報等を確認し、対象機器・ソフトウェア及び利用している機能又は設定を把握していることを確認する。
- ② ベンダーの脆弱性情報、アップデート情報、通知文書等を確認し、該当するアップデー

トプログラムを把握していることを確認する。

- ③ アップデートに係る適用記録、変更管理記録、更新ログ等を確認し、該当するアップデートプログラムをリリースから 14 日以内に適用していることを確認する。
- ④ 14 日以内にアップデートができていない場合、対応計画及び適合基準に記載した暫定対策の実施記録等を確認し、代替措置を講じていることを確認する。

(3) No.4-4-4-3 ★4

【評価基準】

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 及びファームウェアについては、CVSS 基本値 7.0 以上の脆弱性を有していないこと。

【対象外となるための条件】

該当なし

【適合基準】

- ① インターネットとの境界に設置したネットワーク機器の OS 及びファームウェアが、CVSS 基本値 7.0 以上の脆弱性を有していないこと。

【自己評価方法】

- ① 脆弱性管理台帳、脆弱性管理システム等を確認し、インターネットとの境界に設置したネットワーク機器の OS 及びファームウェアが、CVSS 基本値 7.0 以上の脆弱性を有していないことを確認する。

4-4-5 マルウェア感染からの保護

【要求事項】

システムをマルウェア感染から保護すること。

(1) No.4-4-5-1 ★3

【評価基準】

ネットワークに接続しているすべてのパソコン及びサーバに、マルウェア対策ソフトウェアを導入すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ネットワークに接続している全てのパソコン及びサーバに、マルウェア対策ソフトウェアを導入していること。

【自己評価方法】

- ① マルウェア対策ソフトウェアの管理画面、適用状況一覧等を確認し、ネットワークに接続している全てのパソコン及びサーバに、マルウェア対策ソフトウェアを導入していることを確認する。

(2) No.4-4-5-2 ★3

【評価基準】

パソコン及びサーバごとにマルウェア対策ソフトのスキャン範囲及び頻度を定め、スキャンを実行すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン及びサーバごとに、マルウェア対策ソフトウェアのスキャン範囲及び頻度を定めていること。
- ② ①で定めた内容に従いスキャンを実行していること。
※なお、次世代型アンチウイルス（NGAV）など定時スキャン機能を有しないソフトウェアを利用している場合は、リアルタイム保護（プロセス実行時・ファイルアクセス時の検査）及び振る舞い検知機能が有効であること。

【自己評価方法】

- ① パソコン及びサーバごとに、マルウェア対策ソフトウェアのスキャン範囲及び頻度を定めていることを確認するとともに、その文書名を確認する。
- ② マルウェア対策ソフトウェアの管理画面等を確認し、①で定めた内容に従いスキャンを実行していることを確認する。

(3) No.4-4-5-3 ★3**【評価基準】**

マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートすること。

【対象外となるための条件】

該当なし

【適合基準】

- ① マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートしていること。

【自己評価方法】

- ① マルウェア対策ソフトウェアのパターンファイルに係る設定等を確認し、マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートしていることを確認する。

(4) No.4-4-5-4 ★4**【評価基準】**

パソコン/Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① パソコン/Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限していること。

【自己評価方法】

- ① マルウェア対策ソフトウェア、Web ゲートウェイの管理画面等を確認し、パソコン /Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限していることを確認する。

(5) No.4-4-5-5 ★4**【評価基準】**

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、メールサーバ等でマルウェアチェックを実施すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 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又はメールサーバ等でマルウェアチェックを実施していること。

【自己評価方法】

- ① マルウェア対策ソフトウェアの管理画面、メールサービスの管理画面等を確認し、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又はメールサーバ等でマルウェアチェックを実施していることを確認する。

4-5 技術インフラのレジリエンス

4-5-1 ネットワーク境界防護

【要求事項】

ネットワークを適切に分離し、境界部分を防護すること。

(1) No.4-5-1-1 ★3

【評価基準】

全てのファイアウォール（又はファイアウォール機能を持つネットワーク機器）及びルータについて、デフォルトの管理パスワードを強固で一意のパスワードに変更する、又はリモートアクセスを完全に無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータについて、デフォルトの管理パスワードを強固かつ一意のパスワードへ変更している又は、リモートアクセスを完全に無効化していること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータについて、デフォルトの管理パスワードを強固かつ一意のパスワードへ変更している、又はリモートアクセスを完全に無効化していることを確認する。

(2) No.4-5-1-2 ★3

【評価基準】

ファイアウォール（又はファイアウォール機能を持つネットワーク機器）及びルータのパスワードを変更する手順を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータのパスワードを変更する手順を定めていること。

【自己評価方法】

- ① ファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータのパスワードを変更する手順を定めていることを確認するとともに、その手順の文書名を確認する。

(3) No.4-5-1-3 ★3**【評価基準】**

ファイアウォール（又はファイアウォール機能を持つネットワーク機器）及びルータに係る認証は、No.4-1-5 で定めるパスワード設定等に関する評価基準を満たすこと。

【対象外となるための条件】

該当なし

【適合基準】

- ① ファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータの認証が、No.4-1-5 で定めるパスワード設定等の評価基準を満たしていること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、ファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）及びルータの認証が、No.4-1-5 で定めるパスワード設定等の評価基準を満たしていることを確認する。

(4) No.4-5-1-4 ★3**【評価基準】**

全てのファイアウォール（又はファイアウォール機能を持つネットワーク機器）について、認証されていないインバウンド通信を遮断すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）で、認証を経していないインバウンド通信を遮断していること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）で、認証を経していないインバウンド通信を遮断していることを確認する。

(5) No.4-5-1-5 ★3**【評価基準】**

全てのファイアウォール（又はファイアウォール機能を持つネットワーク機器）について、インバウンド通信に関するファイアウォール・ルールが定められていること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）に

について、インバウンド通信に関するファイアウォール・ルールを定めていること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）について、インバウンド通信に関するファイアウォール・ルールを定めていることを確認するとともに、そのルールの文書名を確認する。

(6) No.4-5-1-6 ★3

【評価基準】

全てのファイアウォール（又はファイアウォール機能を持つネットワーク機器）について、不要になったファイアウォール・ルールを速やかに削除又は無効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）について、不要になったファイアウォール・ルールを速やかに削除又は無効化していること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、全てのファイアウォール（ファイアウォール機能を持つネットワーク機器を含む。）について、不要になったファイアウォール・ルールを速やかに削除又は無効化していることを確認する。

(7) No.4-5-1-7 ★3

【評価基準】

ファイアウォール・ルールの変更をインターネット経由で行う場合、No.4-1-3-3 で示す認証要素を利用した多要素認証を適用するか、又は信頼できる IP アドレスにアクセスを制限すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① ファイアウォール・ルールをインターネット経由で変更する場合、No.4-1-3-3 で示す認証要素を利用した多要素認証を適用しているか、又は、アクセス元を信頼できる IP アドレスに制限していること。

【自己評価方法】

- ① ファイアウォール・ルータの管理画面等を確認し、ファイアウォール・ルールをインターネット経由で変更する場合、No.4-1-3-3 で示す認証要素を利用した多要素認証を適

用しているか、又は、アクセス元を信頼できる IP アドレスに制限していることを確認する。

(8) No.4-5-1-8 ★4

【評価基準】

利用中の OS が対応していない場合を除いて、すべてのパソコン及びサーバにおいて、ソフトウェアファイアウォールを有効化すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 利用中の OS が対応していない場合を除き、全てのパソコン及びサーバでソフトウェアファイアウォールを有効化していること。

【自己評価方法】

- ① OS の設定画面等を確認し、利用中の OS が対応していない場合を除き、全てのパソコン及びサーバでソフトウェアファイアウォールを有効化していることを確認する。

(9) No.4-5-1-9 ★4

【評価基準】

社外公開サーバ及び重要な機密情報を扱うサーバについて、それぞれ専用のネットワークセグメントに設置し、セグメント内外のアクセスを必要最小限に限定すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 社外公開サーバ及び重要な機密情報を扱うサーバを専用のネットワークセグメントに設置していること。
- ② ①のセグメント内外のアクセスを必要最小限に限定していること。

【自己評価方法】

- ① ネットワーク図等を確認し、社外公開サーバ及び重要な機密情報を扱うサーバを専用のネットワークセグメントに設置していることを確認する。
- ② ネットワーク図等を確認し、①のセグメント内外のアクセスを必要最小限に限定していることを確認する。

5. 攻撃等の検知

5-1 継続的監視

5-1-1 ネットワーク接続・データの監視

【要求事項】

ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。

(1) No.5-1-1-1 ★3

【評価基準】

社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、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。

【対象外となるための条件】

該当なし

【適合基準】

- ① 社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、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していること。

【自己評価方法】

- ① IPS の設置、EDR の導入など、社内外ネットワークの境界又は端末において、どのようにインターネットから社内への通信及び社内から不正なサーバへの通信の双方について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しているかを確認する。

(2) No.5-1-1-2 ★3

【評価基準】

ネットワーク機器のログ及びアラートを分析し、セキュリティ担当部署の担当者又は管理者により不審な事象が発見された場合に、それがセキュリティインシデントに該当するかが判断されること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティ担当部署の担当者又は管理者が、ネットワーク機器のログ及びアラートを分析していること。
- ② セキュリティインシデントの判断基準を定めていること。
- ③ セキュリティ担当部署の担当者又は管理者が①の分析結果に基づき不審な事象を発見した場合、当該事象が②で定めたセキュリティインシデントに該当するか判断していること。

【自己評価方法】

- ① セキュリティ担当部署の担当者又は管理者において、ネットワーク機器のログ及びアラートを分析していることを確認する。
- ② インシデント対応手順等を確認し、セキュリティインシデントの判断基準を定めていることを確認するとともに、その基準を定めた文書名を質問する。(★4の場合は、No.5-2-1-1におけるセキュリティインシデントのレベル及びレベルごとの対象範囲をセキュリティインシデントの判断基準とすることができる。)
- ③ インシデント対応手順等を確認し、セキュリティ担当部署の担当者又は管理者が①の分析結果に基づき不審な事象を発見した場合、当該事象がセキュリティインシデントに該当するか判断していることを確認する。

(3) No.5-1-1-3 ★3**【評価基準】**

No.5-1-1-1 で設置したネットワーク機器又はサービスについて、以下の要件を満たす異常時に通知する仕組みを導入すること。

- アラートが速やかに発報されること。
- 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。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.5-1-1-1 で設置したネットワーク機器又はサービスについて、以下の全ての要件を満たす異常時に通知する仕組みを導入していること。
- アラートを速やかに発報すること。
 - インシデントの速報レポートを作成し、通知すること。

【自己評価方法】

- ① No.5-1-1-1 で設置したネットワーク機器又はサービスの仕様を確認し、以下の全ての要件を満たす異常時に通知する仕組みを導入していることを確認する。
- アラートを速やかに発報すること。
 - インシデントの速報レポートを作成し、通知すること。

5-1-2 情報機器及びソフトウェアの挙動監視

【要求事項】

情報機器及びソフトウェアの状態及び挙動を監視すること。

(1) No.5-1-2-1 ★4

【評価基準】

会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成していること。

【自己評価方法】

- ① 会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成していることを確認するとともに、その一覧の文書名を確認する。

(2) No.5-1-2-2 ★4

【評価基準】

年1回以上の頻度で会社支給のパソコンにおけるソフトウェアのインストール状況について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 会社支給のパソコンにおけるソフトウェアのインストール状況について、年1回以上の頻度で点検していること。

【自己評価方法】

- ① インストール状況の点検記録等を確認し、会社支給のパソコンにおけるソフトウェアのインストール状況について、年1回以上の頻度で点検していることを確認する。

(3) No.5-1-2-3 ★4

【評価基準】

外部から受け取ったファイルについて安全性を確認するため、マルウェア対策ソフトのリアルタイムスキャンを実行する、又は仮想環境上で安全性を確認する仕組みを整備する。

【対象外となるための条件】

該当なし

【適合基準】

- ① 外部から受け取ったファイルについて、マルウェア対策ソフトウェアのリアルタイムスキャンを実行しているか、又は、仮想環境上で安全性を確認する仕組みを整備していること。

【自己評価方法】

- ① 外部から受け取ったファイルに対して実施している処理方法を確認し、マルウェア対策ソフトウェアのリアルタイムスキャンを実行しているか、又は、仮想環境上で安全性を確認する仕組みを整備していることを確認する。

5-2 有害事象の分析

5-2-1 セキュリティインシデントのレベルごとの対象範囲

【要求事項】

セキュリティインシデントのレベル及びレベルごとの対象範囲を明確にすること。

(1) No.5-2-1-1 ★4

【評価基準】

自社におけるセキュリティインシデントのレベル及びレベルごとの対象範囲を定め、役員、従業員、派遣社員及び受入出向者に周知すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 自社におけるセキュリティインシデントのレベル及びレベルごとの対象範囲を定めていること。
- ② ①を役員、従業員、派遣社員及び受入出向者に周知していること。

【自己評価方法】

- ① インシデント対応手順等を確認し、自社におけるセキュリティインシデントのレベル及びレベルごとの対象範囲を定めていることを確認する。
- ② 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、①で定めた内容を役員、従業員、派遣社員及び受入出向者に何らかの手段・媒体により周知していることを確認する。

(2) No.5-2-1-2 ★4

【評価基準】

No.4-4-3-3 において不審な認証試行を検知した場合又は No.5-1-1-1 で導入されるネットワーク機器若しくはサービスからのアラートを受け取った場合は、No.5-2-1-1 で定めたレベル及び対象範囲に基づき、どのレベルのインシデントに該当するかを分析し、判断すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.4-4-3-3 において不審な認証試行を検知した場合又は No.5-1-1-1 で導入されるネットワーク機器若しくはサービスからのアラートを受け取った場合は、No.5-2-1-1 で定めたレベル及び対象範囲に基づき、どのレベルのインシデントに該当するかを分析し、判断していること。

【自己評価方法】

- ① インシデント対応手順等を確認し、No.4-4-3-3において不審な認証試行を検知した場合又は No.5-1-1-1 で導入されるネットワーク機器若しくはサービスからのアラートを受け取った場合は、No.5-2-1-1 で定めたレベル及び対象範囲に基づき、どのレベルのインシデントに該当するかを分析し、判断していることを確認するとともに、判断手順を定めた文書の文書名を確認する。

6. インシデントへの対応

6-1 インシデント管理

6-1-1 インシデント対応手順

【要求事項】

セキュリティインシデントへの対応手順、対応体制等を定めること。

(1) No.6-1-1-1 ★3

【評価基準】

以下の手順を含んだセキュリティインシデントへの対応手順を定めること。

①発見報告、②初動、③調査・対応、④復旧、⑤最終報告

【対象外となるための条件】

該当なし

【適合基準】

① セキュリティインシデント対応手順を定めていること。

② ①の手順に発見報告、初動、調査・対応、復旧及び最終報告の各プロセスを含めていること。

【自己評価方法】

① セキュリティインシデント対応手順を定めた文書を作成していること、及びその文書名を確認する。

② ①の手順の内容を確認し、発見報告、初動、調査・対応、復旧及び最終報告の各プロセスが含まれていることを確認する。

(2) No.6-1-1-2 ★3

【評価基準】

セキュリティインシデント発生時における社内外組織（関係当局及び所管省庁を含む。）の連絡先及び報告・情報共有ルートを定めること。

【対象外となるための条件】

該当なし

【適合基準】

① セキュリティインシデント発生時における社内外組織（関係当局及び所管省庁を含む。）の連絡先を定めていること。

② セキュリティインシデント発生時における報告・情報共有ルートを定めていること。

【自己評価方法】

① インシデント発生時の連絡先一覧等を確認し、セキュリティインシデント発生時における社内外組織（関係当局及び所管省庁を含む。）の連絡先を定めていることを確認するとともに、その連絡先の文書名を確認する。

- ② インシデント対応手順等を確認し、セキュリティインシデント発生時における報告・情報共有ルートを定めていることを確認する。

(3) No.6-1-1-3 ★3

【評価基準】

セキュリティインシデント発生時におけるセキュリティを統括する役員（例えば、CISO を設置する会社の場合は、当該 CISO）及びセキュリティ担当部署の役割・責任を定めること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティインシデント発生時におけるセキュリティを統括する役員及びセキュリティ担当部署の役割及び責任を定めていること。

【自己評価方法】

- ① インシデント発生時の体制図等を確認し、セキュリティインシデント発生時におけるセキュリティを統括する役員及びセキュリティ担当部署の役割及び責任を定めていることを確認するとともに、その文書名を確認する。

(4) No.6-1-1-4 ★3

【評価基準】

年 1 回以上の頻度で No.6-1-1-2 及び No.6-1-1-3 にて定めたセキュリティインシデント発生時の体制について点検すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① No.6-1-1-2 及び No.6-1-1-3 で定めたセキュリティインシデント発生時の体制について、年 1 回以上の頻度で点検していること。

【自己評価方法】

- ① No.6-1-1-2 及び No.6-1-1-3 で定めたセキュリティインシデント発生時の体制を点検した記録を確認し、年 1 回以上の頻度で点検していることを確認する。

(5) No.6-1-1-5 ★3

【評価基準】

セキュリティインシデントの報告フォーマットを整備すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① セキュリティインシデントの報告フォーマットを整備していること。

【自己評価方法】

- ① セキュリティインシデント対応手順等を確認し、セキュリティインシデントの報告フォーマットを整備していることを確認するとともに、その文書名を確認する。

(6) No.6-1-1-6 ★3**【評価基準】**

年1回以上及び社内外で重大なセキュリティインシデントが発生した際に、インシデント事例及びその対応策を社内部署へ共有していること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 年1回以上の頻度で、インシデント事例及びその対応策を社内部署へ何らかの手段・媒体により共有していること。
- ② 社内外で重大なセキュリティインシデントが発生した際にも、当該事例及び対応策を社内部署へ何らかの手段・媒体により共有していること。

【自己評価方法】

- ① 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、年1回以上の頻度で、インシデント事例及びその対応策を社内部署に何らかの手段・媒体により共有していることを確認する。
- ② 社内掲示板、社内ポータルサイト等の社内への周知を行う媒体を確認し、社内外で重大なセキュリティインシデントが発生した際にも、当該事例及び対応策を社内部署に何らかの手段・媒体により共有していることを確認する。

7. インシデントからの復旧

7-1 インシデント復旧計画の実行

7-1-1 事業継続要件に沿った復旧準備

【要求事項】

事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。

(1) No.7-1-1-1 ★3

【評価基準】

事業継続上重要なシステムについて、サイバー攻撃を念頭に、業務の目標復旧レベルを定め
たうえで、当該レベルまで業務を回復するために必要な対策を、以下の例を参考として整備
すること。

【復旧のための対策（例）】

- システムによる業務継続（例：予備機、クラウド環境等により待機系を整備する。）
- 人手による業務継続（例：電話、FAX 等による連絡又は業務の実施に備え、影響のある取引先の連絡先及び複数の連絡手段を整備する。）

【対象外となるための条件】

該当なし

【適合基準】

- ① 事業継続上重要なシステムについて、サイバー攻撃を想定した業務の目標復旧レベルを定めていること。
- ② ①のレベルまで業務を回復するために必要な対策を整備していること。

【自己評価方法】

- ① システム復旧手順書、事業継続計画等を確認し、事業継続上重要なシステムについて、サイバー攻撃を想定した業務の目標復旧レベルを定めていることを確認するとともに、その文書名を確認する。
- ② システム復旧手順書、事業継続計画等を確認し、①のレベルまで業務を回復するために必要な対策を整備していることを確認する。

(2) No.7-1-1-2 ★4

【評価基準】

事業継続上重要なシステムについて、サイバー攻撃を念頭に、以下の対策を講じること。

- 目標復旧時点への復旧ができるように No.4-3-4-1 及び No.4-3-4-2 で取得したバックアップを保管すること。
- No.4-3-4-3 で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップの復元ができることを確認すること。

【対象外となるための条件】

該当なし

【適合基準】

- ① 事業継続上重要なシステムについて、目標復旧時点まで復旧できるよう、No.4-3-4-1 及び No.4-3-4-2 で取得したバックアップを保管していること。
- ② No.4-3-4-3 で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップを復元できることを確認していること。

【自己評価方法】

- ① バックアップ記録等を確認し、事業継続上重要なシステムについて、目標復旧時点まで復旧できるよう、No.4-3-4-1 及び No.4-3-4-2 で取得したバックアップを保管していることを確認する。
- ② バックアップ記録及び復元テスト記録等を確認し、No.4-3-4-3 で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップ復元テストを行っていることを確認するとともに、当該記録の文書名を確認する。

改定履歴

日付	改定内容
2026 年 10 月 28 日	初版発行