

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）
★4 第三者評価ガイド

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
1.3 第三者評価の位置づけ.....	4
第2章 評価の実施方法.....	5
2.1 評価契約.....	5
2.2 申請資格.....	5
2.2.1 申請を受け付けてはならない条件	5
2.3 第三者評価に係る申請.....	5
2.3.1 第三者評価に係る申請書.....	5
2.3.2 申請関連書類	6
2.4 申請書等の確認	6
2.5 評価計画.....	6
2.6 第三者評価を実施する者の要件.....	6
2.6.1 第三者評価を行わせることができる要件.....	6
2.6.2 評価要員が評価を実施する際の基準.....	6
2.6.3 評価要員の誓約書	7
2.6.4 評価要員の記録.....	7
2.7 評価チームの構成及び評価チームへの指示・情報提供.....	7
2.7.1 評価チーム.....	7
2.7.2 手順の指示及び情報の提供.....	7
2.8 適用範囲の確認	7
2.9 文書確認	8
2.10 実地審査.....	9
2.10.1 審査事項	9
2.10.2 審査事項の通知.....	9
2.10.3 審査日及び審査場所.....	9
2.10.4 実地審査の参加者	10
2.11 不適合の指摘及び改善.....	10
2.11.1 不適合の指摘	10
2.11.2 改善報告の求め.....	10
2.11.3 改善報告の確認.....	10
2.12 技術検証	11
2.13 評価調書	11
2.14 評価報告書	11
2.14.1 合否の判定基準.....	11

2.14.2 評価報告書の作成	12
2.15 登録期間における対応	12
2.15.1 登録期間中の自己評価	12
2.15.2 登録期間中における再度の第三者評価	12
第3章 その他第三者評価に当たり遵守すべき事項	15
3.1 情報の管理	15
3.1.1 秘密保持	15
3.1.2 文書の保管	15
3.1.3 文書の保管方法	15
3.1.4 文書の破棄	16
別紙 ★4 第三者評価における適合基準等	17
1. ガバナンスの整備	19
1-1 組織の状況	19
1-2 役割、責任、権限	21
1-3 ポリシー	29
1-4 監督	31
2. 取引先管理	33
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	33
3. リスクの特定	40
3-1 資産管理	40
3-2 リスクアセスメント	55
4. 攻撃等の防御	58
4-1 アイデンティティ管理、認証、アクセス制御	58
4-2 意識向上とトレーニング	86
4-3 データセキュリティ	91
4-4 プラットフォームセキュリティ	97
4-5 技術インフラのレジリエンス	111
5. 攻撃等の検知	117
5-1 継続的監視	117
5-2 有害事象の分析	122
6. インシデントへの対応	124
6-1 インシデント管理	124
7. インシデントからの復旧	128
7-1 インシデント復旧計画の実行	128

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（SCS 評価制度）基本規程（以下、「基本規程」という。）★4における第三者評価について説明するものである。

評価機関は本ガイドの内容を踏まえて第三者評価を実施するものとする。

なお、第三者評価のうち、技術検証事業者が実施する技術検証については、「★4 技術検証ガイド」に従い実施するものとする。

1.2 用語定義

本ガイドで使用する用語は、本ガイドに別段の定めがある場合を除き、「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、管理ツールおよ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。

1.3 第三者評価の位置づけ

本ガイドで説明する第三者評価は、本ガイドに従って実施する文書確認、実地審査及び技術検証を通じて、評価時点における登録希望組織の要求事項・評価基準への適合性を評価するものである。したがって、第三者評価の結果については、次に掲げる点に留意されたい。

- ① 第三者評価は登録希望組織における本制度が定めた要求事項・評価基準への適合性を評価するものであり、登録組織においてインシデントが発生しないことを保証するものではない。
- ② 第三者評価は、一部の機器、端末、規程、手順等に対して実施するものであり、登録希望組織における全ての機器、端末、規程、手順等が要求事項・評価基準に適合していることを保証するものではない。
- ③ 第三者評価（特に実地審査）は、一部の要求事項・評価基準に対して実施するものであり、登録希望組織が全ての要求事項・評価基準に対してもれなく完全に適合していることを保証するものではない。
- ④ 第三者評価は、評価時点での要求事項・評価基準への適合性を評価するものであり、登録の有効期間にわたって要求事項・評価基準への適合性が有効であることを保証するものではない。

第2章 評価の実施方法

本章では、第三者評価の実施に当たって、評価機関が実施すべき事項について解説する。

なお、★4 登録の更新時における第三者評価についても本ガイドに従って実施するものとする。

また、本ガイドで定める第三者評価の流れの全体像については章末の図 1 を参照されたい。

2.1 評価契約

評価機関は、「評価機関指定基準」4.3 に従い、登録希望組織と、その第三者評価に関し、法的に拘束力のある合意を結んだ上で、第三者評価を行わなければならない。なお、この合意には技術検証に係る事項を含む。

2.2 申請資格

2.2.1 申請を受け付けてはならない条件

評価機関は、登録希望組織及び登録希望組織と同等とみなすことができる組織¹が次の表 1 に定める条件に該当する場合は、第三者評価の申請を受け付けてはならない。

表 1 申請を受け付けてはならない条件及び期間

条件	申請を受け付けてはならない期間
「★3・★4 登録申請の手引」に基づき★4 登録の取消を受けた場合	当該取消の日から 1 年
評価機関から第三者評価について不合格の旨の判定を受けた場合	当該判定が通知された日から 3 か月

2.3 第三者評価に係る申請

2.3.1 第三者評価に係る申請書

評価機関は、登録希望組織に対し、必要事項を全て記入した申請書を提出するよう要求しなければならない。申請書には次に掲げる全ての事項が含まれていなければならない。

- ① 第三者評価を申請する旨の明確な記述
- ② 登録希望組織に対する第三者評価を行うために必要な全ての情報を提供する旨の、登録希望組織の同意
- ③ 登録希望組織が 2.2.1 に規定する条件に該当しない旨の申告
- ④ 登録希望組織の正式名称・所在地等の基本情報
- ⑤ 取得単位及び適用範囲
- ⑥ 対象となる全ての拠点
- ⑦ 申請の種別（新規・更新）
- ⑧ 評価機関との連絡に係る担当者及びその連絡先

なお、申請書の様式、作成方法及び提出方法は、評価機関が定めるものとする。

¹ 当該登録希望組織と適用範囲が異なる同一組織及び当該登録希望組織が合併等により引き継がれた後の組織を指す。

2.3.2 申請関連書類

評価機関は、登録希望組織に、申請書に添えて、次に掲げる全ての書類を提出するよう要求しなければならない。

- ① 登録希望組織の自己評価結果を記入したアセスメントシート（「★3・★4 自己評価等ガイド」3.1.1に基づき評価機関等が独自で用意した自己評価等のための様式を含む。以下「アセスメントシート等」という。）
- ② その他評価機関が第三者評価の実施に必要と判断する書類

なお、申請関連書類の作成方法及び提出方法は、評価機関が定めるものとする。

2.4 申請書等の確認

評価機関は、登録希望組織から提出された申請書及び申請関連書類の確認をしなければならない。

評価機関は、申請書及び申請関連書類が、2.3.1及び2.3.2を満たしていることが確認できるまで、第三者評価に着手してはならない。なお、当該確認の結果として着手しない場合は、その理由を登録希望組織に通知し、補正の機会及び再提出期限を示さなければならない。

2.5 評価計画

評価機関は、申請書及び申請関連書類等の内容を確認した上で、登録希望組織に対する評価計画を定めなければならない。評価計画には、少なくとも次に掲げる全ての事項を含めるものとする。

- ① 第三者評価全体の実施スケジュール
- ② 第三者評価を担当するチーム（以下「評価チーム」という。）の構成員の氏名
- ③ 実地審査及び技術検証の実施日程及び実施場所（オンラインにより実施する場合はその旨を含む。）
- ④ 実地審査の実施方法及び実施対象
- ⑤ 技術検証の実施方法及び実施対象
- ⑥ 登録希望組織側で準備を求める資料

2.6 第三者評価を実施する者の要件

2.6.1 第三者評価を行わせることができる要件

評価機関は、「評価機関指定基準」で定める★4評価責任者及び★4評価従事者の要件を満たす者に、第三者評価を行わせなければならない。

評価機関は、★4評価責任者及び★4評価従事者以外の者に第三者評価を行わせてはならない。また、★4評価責任者は評価機関に雇用されている者でなければならない。

2.6.2 評価要員が評価を実施する際の基準

評価要員（「評価機関指定基準」3.2に規定する評価要員をいう。以下同じ。）は、第三者評価を行う際の適合基準として、「★3・★4 要求事項・評価基準」及び本ガイド別紙を参照するものとする。

2.6.3 評価要員の誓約書

評価機関は、評価要員に対し、当該評価機関が規定した内部規程及び文書（「評価機関指定基準」2.14 に規定する内部規程及び文書をいう。）に従うことを約束する誓約書に署名することを要求しなければならない。

なお、誓約書は文書又は電磁的記録により作成することとする。

2.6.4 評価要員の記録

評価機関は、評価要員に関して、次に掲げる全ての事項について記録し、かつ当該記録を最新の状態に維持しなければならない。

- ① SCS セキュリティ専門家の資格要件となっている資格の保有状況
- ② 本制度が指定する研修の受講履歴
- ③ 本制度における第三者評価の実施実績
- ④ 当該記録の最終更新年月日

2.7 評価チームの構成及び評価チームへの指示・情報提供

2.7.1 評価チーム

評価機関は、評価要員の中から評価チームを構成しなければならない。評価チームは、★4 評価責任者を含む 1 名以上により構成するものとする。評価機関が技術検証を自ら実施する場合は、「評価機関指定基準」4.5②に従い、評価の判断に直接関与する者と技術検証の実務を担う者とを分離する。

評価機関が評価チームを構成する際には、評価チームのメンバーが「評価機関指定基準」2.7 に規定する公平性の要件に適合していることを確認し、確認した結果を記録するものとする。

2.7.2 手順の指示及び情報の提供

評価機関は、第三者評価を行うために必要な情報として、少なくとも第三者評価の実施手順、評価調書及び評価報告書の作成の手順並びに登録希望組織から受領した申請書及び申請関連書類を評価チームに提供しなければならない。

評価機関は、評価チームに、評価機関が定めた手順に従った第三者評価を行わせなければならない。

2.8 適用範囲の確認

評価チームは、第三者評価を行うにあたっての前提として、登録希望組織が決定した適用範囲について次に掲げる手順により確認を行う²。当該確認を通じて観点に適合しない事項を発見した場合は、登録希望組織に照会の上、必要に応じて適用範囲の修正を求めるものとする。

- ① 事業部単位等、法人の一部を取得単位とする場合は、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。
 - a. 対象の事業部等において、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

² 本確認の詳細については、「★3・★4 自己評価等ガイド」2.2 を参照されたい。

- ティ対策の責任者が明確になっているか
 - b. 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
 - ② 企業グループ単位等、取得単位に複数の法人を含む場合は、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。
 - a. 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
 - b. 共通のセキュリティ対応方針が適用されているか
 - ③ 登録希望組織からアセスメントシート等やネットワーク構成図上における図示などの提供を受けることにより、評価の対象となる登録希望組織における取得単位及び適用範囲を確認する。併せて、以下の点についても確認を行う。
 - a. 登録希望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
 - b. 適用範囲の境界を構成する機器等に対して、「★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
 - c. 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
 - d. 除外した対象が具体的に記述されているか

2.9 文書確認

評価チームは、登録希望組織の提出したアセスメントシート等に対して文書確認を行うものとする。文書確認は、次の表 2 に定める観点でアセスメントシート等のみを対象として確認を行うものとし、文書確認の段階では、証拠の閲覧等は必ずしも実施する必要はない。（証拠の閲覧等は実地審査において行うことを想定している。）

文書確認を通じて観点に適合しない事項を発見した場合は、2.11.1 の不適合の指摘において当該事項の確認を行うものとする。

表 2 文書確認の観点

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漏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

2.10 実地審査

2.10.1 審査事項

評価チームは、登録希望組織の第三者評価を行うために、実地審査を実施しなければならない。実地審査は、登録希望組織における事業所の現地で実施するほか、情報の秘密保持、通信方法、オンラインでの審査可否及び審査範囲、評価チームの本人確認等について登録希望組織との間で合意が取れた場合は、オンライン方式により実施することも可能とする。

なお、実地審査を行う拠点は原則1拠点として、どの拠点を対象とするかは登録希望組織と協議のうえ、決定するものとする（必要に応じて複数拠点を対象とすることは妨げない）。

評価チームは、制度運営機関が別途公表する実地審査を必須とする要求事項を踏まえて、本ガイド別紙に規定する評価手法に基づき、適合・不適合を判定する。ただし、別紙に規定する評価手法は、最低限実施すべき評価手法であって、評価機関や評価者がこれに加えて証跡等の確認を行うことを妨げるものではない。

2.10.2 審査事項の通知

制度運営機関が年度ごとに指定する要求事項については、制度運営機関から評価機関に対して別途通知するものとする。

2.10.3 審査日及び審査場所

評価チームは、登録希望組織と審査日及び審査場所について合意した上で、実地審査を実施しなければならない。その際、評価チームは、少なくとも次に掲げる全ての事項を登録希望組織にあらかじめ通知しなければならない。なお、技術検証の実施に関する事項については、

「★4 技術検証ガイド」に従って行うものとする。

- ① 実地審査を実施する要求事項
- ② 審査対象となる規程、手順等の文書
- ③ 審査対象となる機器、端末等

2.10.4 実地審査の参加者

登録希望組織及び評価チーム以外で登録希望組織側又は評価機関側における実地審査への参加者がいる場合(例:登録希望組織の委託先企業や評価機関における評価チームの随行者等)には、当該者の参加についてあらかじめ評価機関と登録希望組織との間で合意し、記録するものとする。

2.11 不適合の指摘及び改善

2.11.1 不適合の指摘

評価チームは、文書確認及び実地審査において、評価基準に対する不適合を認識したときは、当該不適合の指摘を行うものとする。なお、不適合の指摘は、技術検証における是正対応の依頼³と必ずしも併せて行う必要はない。

評価チームが不適合の指摘を行う場合の手順は、少なくとも次に掲げる全ての事項を確実にするものでなければならない。また、評価基準への不適合箇所を特定した文書（以下「指摘文書」という。）においては、合否に影響する不適合のみを記載し、改善を強制しない事項や助言とは区別しなければならない。

- ① 評価チームは、登録希望組織に対して、評価基準に対する適合性に関して疑義がある場合には、不適合の指摘に先立って書面で質問の機会を与えること
- ② 評価チームは、指摘文書を登録希望組織に通知すること
- ③ 指摘文書には、少なくとも以下の事項を含むこと
 - a. 指摘文書発行の年月日
 - b. 文書確認及び実地審査を行った年月日
 - c. 評価責任者の氏名
 - d. 評価基準に対して不適合であることに関する指摘及びその根拠

2.11.2 改善報告の求め

評価チームは、不適合として指摘した事項を是正するために実施した処置についての報告(以下「改善報告」という。)を、登録希望組織が指摘文書を受領した日から遅くとも1か月以内に書面又は電磁的記録により、評価チームに提出するよう求めなければならない。

2.11.3 改善報告の確認

評価チームは、前項に基づき改善報告が提出された場合は、当該報告により指摘事項が修正され適合となっているかどうかを文書確認及び実地審査により確認したうえで、評価調書及

³ 「★4 技術検証ガイド」第4章に基づく是正対応の依頼を指す。なお、技術検証における是正対応については、「★4 技術検証ガイド」に基づき別途対応すること。

び評価報告書を作成するものとする。なお、前項に規定する期間内であれば、不適合の改善は複数回にわたって実施しても差し支えないものとする。

2.12 技術検証

技術検証事業者（技術検証事業者の指定を受けている評価機関を含む。）は、「★4 技術検証ガイド」に基づき、技術検証を別途実施するものとする。

評価チームは、技術検証事業者の指定を受けている評価機関又は評価機関から委託を受けた技術検証事業者が登録希望組織に対して実施した技術検証の結果を受領し、技術検証の可否を確認しなければならない。

2.13 評価調書

評価チームは、実施した文書確認及び実地審査の結果、評価に関連して入手した資料及び結果に至った経過を評価調書として作成しなければならない。評価調書の作成に当たっては、例えば表3のように、評価の結果に至った過程を追跡可能な形式で記録しなければならない。

表3 要求事項 No.1-2-1 における評価調書の作成例

要求事項	評価基準	適合基準	実施した評価手法	手続実施結果	評価結果	評価証跡
No.1-2-1 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。	No.1-2-1-1 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。	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。	質問：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 た文書の文書名を質問した。 閲覧：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 た文書を開覧した。	質問：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 た文書の文書名を特定した。 閲覧：社内体制図の開覧 により、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 た文書の実在を確認できた。	適合	XX社社内体制図
	No.1-2-1-2 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。	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。	質問：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 リストの文書名を質問した。 閲覧：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 リストを開覧した。	質問：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 リストの文書名を特定した。 閲覧：連絡先リストの開覧 により、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 リストの実在を確認できた。	適合	XX社連絡先リスト
	No.1-2-1-3 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。	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。	質問：No.1-2-1-1及び No.1-2-1-2で定める平時 の体制について、年1回以上 の頻度で点検を実施してい るか、また、直近の実施時期 について質問した。	質問：アセスメントシートに 記入された回答により、以下 のことが確認できた。 - 年1回以上の頻度で点 検を実施している。 - 直近の実施日が 2026/XX/XXであり、評 価実施日前1年以内に 点検を実施している。	適合	XX社アセスメントシート

2.14 評価報告書

2.14.1 合否の判定基準

文書確認及び実地審査において審査対象となっている評価基準の全てに適合が認められ、かつ、技術検証が合格となった場合（「★4 技術検証ガイド」第1部第5章に基づき脆弱性診断の実施が免除された場合を含む。）でなければ、★4 評価責任者は合格と判定してはならない。

2.14.2 評価報告書の作成

文書確認、実地審査及び技術検証の結果を踏まえ、★4 評価責任者が第三者評価についての可否の判定を行う。評価チームは、次に掲げる全ての事項を含む評価報告書を作成し、登録希望組織に報告しなければならない。

- ① 登録希望組織及び評価機関の名称
- ② 報告日
- ③ ★4 評価責任者の氏名
- ④ 文書確認、実地審査及び技術検証の実施日
- ⑤ 2.9 における文書確認の結果
- ⑥ 2.10 における実地審査の結果
- ⑦ 2.12 において受領した技術検証の結果
- ⑧ 第三者評価の最終的な可否結果

2.15 登録期間における対応

2.15.1 登録期間中の自己評価

評価機関は、合格と判定し、制度運営機関により登録された登録組織に対して、当該合格の判定に基づく登録の有効期間中において、アセスメントシート等に基づき実施した自己評価結果を、毎年提出するよう求めるものとする。

この場合において、当該自己評価結果の提出方法は評価機関ごとに定めるものとする。また、提出時期については、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おいて提出させるものとする。

（例：登録日が2027年4月1日である場合において、2028年4月1日の前後3か月以内及び2029年4月1日の前後3か月以内に自己評価結果の提出を求める。）

登録組織から期限を過ぎても提出がされなかった場合、評価機関は制度運営機関にその旨を書面にて報告する必要がある。

なお、評価機関は、提出を受けた自己評価結果について、「評価機関指定基準」4.9に基づきその内容を確認し、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の有無を確認したうえで、2.15.2の条件に該当しない場合、アセスメントシート等に署名または記名を行う。受領した自己評価結果については、3.1に従って文書の管理を行う必要がある。

2.15.2 登録期間中における再度の第三者評価

評価機関は、前項に基づき受領した自己評価結果について、登録組織における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った場合には、前項に規定する文書確認に加えて、再度実地審査及び技術検証を実施するものとする。

評価機関による再度の第三者評価の対象範囲は、当該変更に関係する箇所に限るものとし、以下のような場合を想定する。

- ① 登録組織における適用範囲の変更があった場合については、当該変更において追加された範囲に対してのみ、実地審査及び技術検証を行うものとする。
- ② 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が行われた場合は、当該社内規程・手順書等が評価対象となり、それ以外の文書やそれに紐づく要求事項・評価基準については、再度の実地審査及び技術検証は要しない。
- ③ IT 基盤における顕著な変更（PC、サーバ等の機器の大規模な入替、認証基盤の変更等）があった場合には、当該変更となった機器、基盤等に対してのみ実地審査を行うこととする。

また、ネットワーク基盤の大規模な更改等により、技術検証を実施した機器に更改があった場合には、「★4 技術検証ガイド」に従い、技術検証又は実施の免除を行うこととする。

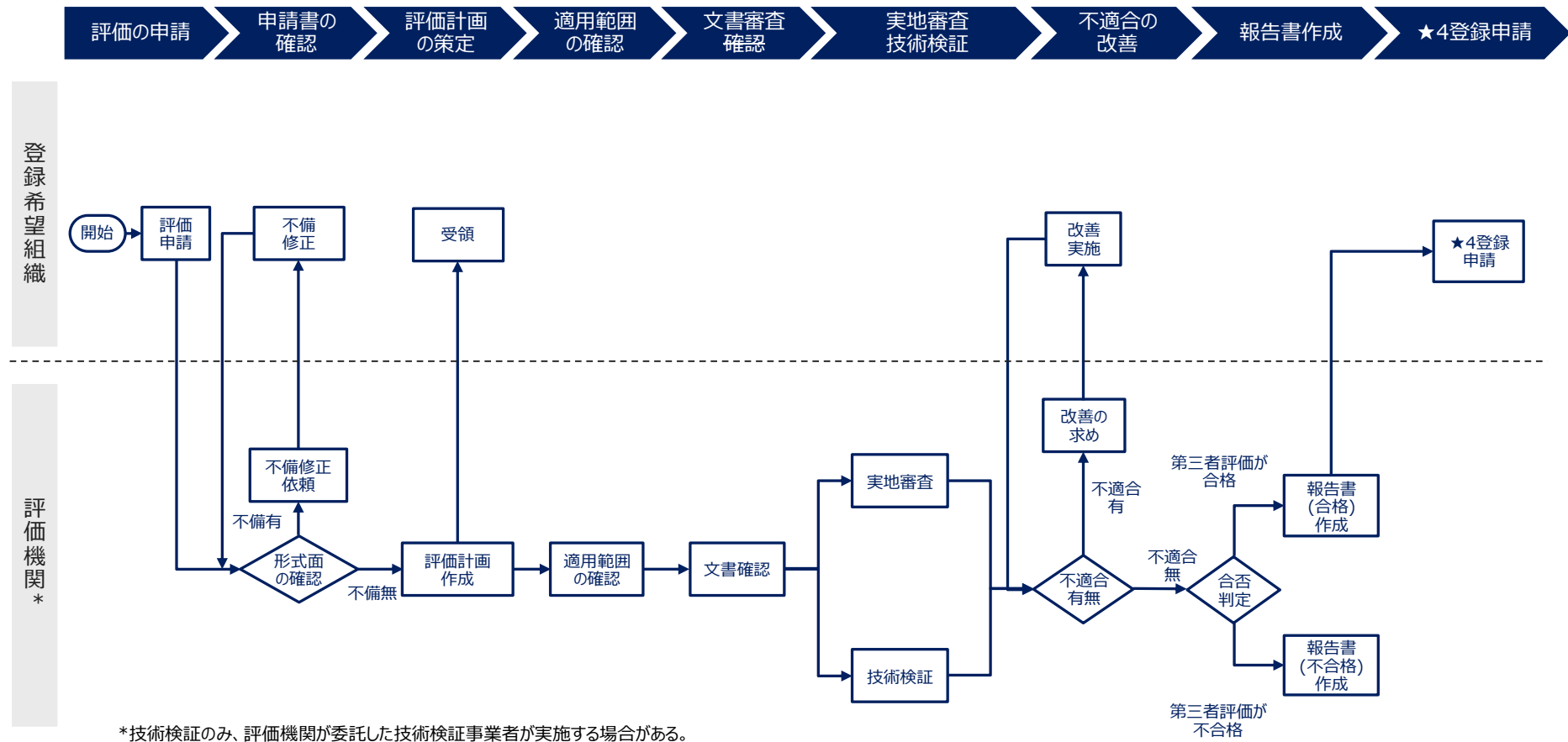


図1 ★4 第三者評価の流れ

第3章 その他第三者評価に当たり遵守すべき事項

3.1 情報の管理

3.1.1 秘密保持

評価機関は、第三者評価に係る業務を通じて得られた又は生じたすべての情報（対象システムの脆弱性に関する情報を含む。）を、当該情報に係る登録希望組織が公開している情報及び公開に同意している情報を除き、機密情報とし、その管理について責任を負わなければならない。

評価機関は、委託元評価機関に対する評価結果の提供その他業務上正当な理由がある場合又は当該登録希望組織の同意がある場合を除き、機密情報を開示してはならない。

評価機関は、登録希望組織以外（例：苦情申立者又は規制当局）から得られた当該登録希望組織に対する情報について、秘密として取り扱わなければならない。

3.1.2 文書の保管

評価機関は、評価結果に係る文書について、「評価機関指定基準」4.2に従って、保管しなければならない。

3.1.3 文書の保管方法

前項において評価結果に係る文書を安全に保管するために、評価機関は要求事項・評価基準において「重要な機密情報」に課せられる管理方法と同等の管理方法として、次に掲げる全ての項目を実施しなければならない。

- ① 文書を管理するに当たって、文書の管理者名、管理部署名、保管場所、保管期限、開示先及び管理者の連絡先を記録する。
- ② 文書を紙媒体で保管する場合には、施錠保管する。
- ③ 文書のファイルデータを保管する場合には、暗号化を実施する。
- ④ 文書をシステムに保管する場合には、当該システムのアクセス権を付与するための条件を定めるとともに、ユーザ及び管理者ごとに必要最小限の権限を付与する。
- ⑤ ④で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導入する。（例：アクセスログの収集・保管など）
- ⑥ 文書を社内ネットワーク上のシステムに保管する場合には、当該システムを分離された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。
- ⑦ 文書をクラウドサービスに保管する場合又はインターネット経由で文書にアクセスする際には多要素認証を実装する。

3.1.4 文書の破棄

評価機関は、3.1.2 で定める保管期間が終了したときは、評価結果に係る文書について復元できないよう抹消処理（例：データの場合は、記憶媒体の抹消処理、紙文書の場合は、文書裁断など）を行い廃棄すること。破棄した後、評価機関は、破棄した文書名、破棄した日付及び破棄した方法についての記録を登録希望組織に送付すること。

別紙 ★4 第三者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、評価機関が行う第三者評価の手續や適合基準を示す。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。登録希望組織から当該条件に合致する旨の申告があり、かつ、評価機関が当該申告は妥当であると認めた場合に限り、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、評価機関が、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する場合は、その理由を記録した上で、対象外とすることを認める。当該条件は、「★3・★4 自己評価等ガイド」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】

対象の評価基準において、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（「やむをえず」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」別紙及び「★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）で示される適合基準と同一である。

【評価手法】

対象の評価基準において、適合又は不適合の評価を行う際の評価手法を示す。評価手法は、質問、閲覧又は観察の中から、評価基準ごとに1つ又は複数の評価手法を指定する。本ガイドは、第三者評価において原則として確保すべき最低限の評価方法を示す。評価機関は、評価基準の趣旨及び確認事項を損なわない範囲で、評価対象の特性やリスク等に応じ、評価手法の追加、組合せ、確認対象の拡大等を行うことができる。評価手法を変更する場合は、必要な証拠を確保するとともに、変更の記録を行うこと。また、評価の客観性及び信頼性を損なってはならない。

- 質問：対策の整備状況又は運用状況に関して、関係者に対して口頭又は文書で問い合わせ、説明や回答を求めるもの。⁴
- 閲覧：対策の整備状況又は運用状況に関して、紙媒体、電子媒体又はその他の媒体による記録や文書を確認するもの。これには、管理ツール上の台帳等を含む。
- 観察：対策の整備状況又は運用状況に関して、評価チームがシステム上の設定画面等を目視によって確認するもの⁵。

⁴ なお、「★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）では、各評価基準に対する適合状況について確認するための質問事項を設けており、当該質問事項の回答をもって、評価手法の質問を代替することもできる。評価機関が必要と判断した場合は、回答内容に関する質問、関連記録の閲覧又は設定画面等の観察を追加することができる。

⁵ 設定画面等について観察を実施する場合は、本ガイド別紙の記述に従って、対象機器を抽出することとなるが、登録希望組織からの申告に基づき対象機器を決定することで差し支えない。評価機関は、登録希望組織と協議の上、対象機器を追加又は変更できる。

評価手法における「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。「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。

また、本ガイド 2.10.1 に記載したとおり、登録希望組織との合意の上で、オンラインによる評価を行うことを許容しており、その場合の閲覧、観察については、リモートカメラ等を活用する方法が考えられる。

なお、別紙で示す事項のほか、第三者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。

【評価手法】

▶質問

社内ルールを策定していることを確認した上で、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質問する。

（把握している法令等の妥当性まで確認することは求めない。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

策定・見直した社内ルールの周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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・責任を定めた文書の文書名を質問する。

▶閲覧

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・責任を定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の文書名を質問する。

▶閲覧

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が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

No.1-2-1-1 及び No.1-2-1-2 にて定めた平時の体制の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

- 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の情報収集源を質問する。
- ② 上記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）を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

- ① サイバー攻撃の予兆及びインシデントの発生を検知方法を質問する。
- ② 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）の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

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の文書名を質問する。

▶閲覧

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記載した文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

入社時又は社外要員の受入れ時における守秘義務のルールの説明方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の文書名を質問する。

▶閲覧

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が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

派遣社員及び受入出向者について守秘義務を締結した文書の文書名を質問する。

▶ 閲覧

派遣社員及び受入出向者について守秘義務を締結した文書が実在することを確認する。

▶ 観察

原則として実施しない。

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。

【評価手法】

▶質問

セキュリティ対応方針の文書名を質問する。

▶閲覧

自社のセキュリティ対応方針が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

セキュリティ対応方針の周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

セキュリティ対応方針を改正した際の周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

セキュリティ対応方針の内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

対策推進計画の文書名を質問する。

▶閲覧

対策推進計画が実在することを確認する。

対策推進計画の報告及び承認に係る結果を記録した文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

- ① 対策推進計画の報告に際して役員からの改善に向けた指示を記録した文書の文書名を質問する。
- ② 直近実施した対策の不備の是正の内容（是正の必要性がなく是正を実施していない場合も含む。）を質問する。

▶閲覧

対策推進計画の報告に際して役員からの改善に向けた指示を記録した文書が実在することを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

No.2-1-1-1 で把握した情報の内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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適合基準に列挙された事項を把握する仕組みの内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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

【評価手法】**▶質問**

秘密保持契約書等の取引先との機密情報に関する取り決めに係る文書の文書名を質問する。

▶閲覧

秘密保持契約書等の取引先との機密情報に関する取り決めに係る文書を閲覧し、以下の全ての事項が取り決められていることを確認する。

- 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

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

- ① 取引先のセキュリティ対策状況を把握する取組の内容を質問する。
- ② 上記の取組について、以下の全ての項目について質問する。
 - 実施頻度
 - 直近の実施日（1年以内に実施していることを確認する。）
- ③ 過去1年以内に取引先のセキュリティ対策状況を把握した記録の文書名を質問する。

▶閲覧

過去1年以内に取引先のセキュリティ対策状況を把握した記録を閲覧し、以下の全ての

項目を満たしていることを確認する。

- 対策状況把握の対象とする子会社又は取引先の条件を満たす子会社又は取引先に対して実施していること。
- 1年以内に実施していること。
- 評価基準に掲げる例示を満たすような取組を実施していること。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の文書名を質問する。

▶閲覧

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が実在することを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

IT 資産管理台帳、IT 資産管理ツールなど、登録希望組織が整備している仕組みを閲覧し、パソコン及びシンクライアントの製造元、OS 及び台数が把握されていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

IT 資産管理台帳、IT 資産管理ツールなど、登録希望組織が整備している仕組みを閲覧し、サーバ、仮想サーバ及びハイパーバイザの製造元、OS 及び台数が把握されていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

情報機器、OS 及びソフトウェアについての管理ルールの文書名を質問する。

▶閲覧

情報機器、OS 及びソフトウェアについての管理ルールを閲覧し、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。

▶観察

原則として実施しない。

(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 of 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。

【評価手法】**▶質問**

No.3-1-1-3 で定めた管理ルール of 遵守状況 of 点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の内容を質問する。

▶閲覧

IT 資産管理台帳、IT 資産管理ツールなど、登録希望組織が整備している仕組みを閲覧し、スマートデバイスの製造元、OS 及び台数が把握されていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

ネットワークを把握する仕組みの内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

ネットワーク機器を把握する仕組みの内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

ネットワーク図の文書名を質問する。

▶閲覧

ネットワーク図が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

No.3-1-2-3 で作成したネットワーク図の記載内容の点検について、以下の全ての項目について質問する。

- 実施頻度

- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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文書の文書名を質問する。

▶閲覧

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文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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定めた文書の文書名を質問する。

▶閲覧

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定めた文書が実在することを確認する。

▶観察

原則として実施しない。

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

【評価手法】

▶質問

自社の保有する情報の管理ルールの文書名を質問する。

▶閲覧

自社の保有する情報の管理ルールを閲覧し、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

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

No.3-1-4-1 で定めた管理ルールの内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

No.3-1-4-3 で把握した項目の内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

退職・任期満了時における機密情報及び情報機器の回収手順としてどのような事項を定めているかを質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

No.3-1-4-5 で求める機密情報及び情報機器の回収状況の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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。）に実施している抹消処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の文書名を質問する。

▶閲覧

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が実在することを確認する。

▶観察

原則として実施しない。

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

【評価手法】**▶質問**

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定めたルールの文書名を質問する。

▶閲覧

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閲覧し、以下の全ての内容を含んでいることを確認する。

リモートワークで使用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

▶観察

原則として実施しない。

(2) No.3-1-5-2 ★4**【評価基準】**

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対して周知すること。

【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 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。

【評価手法】**▶質問**

No.3-1-5-1 で定めたルールの周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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】

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 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。

【評価手法】**▶質問**

No.3-1-5-1 で定めたルールの内容及び遵守状況の点検について、以下の全ての項目について質問する。

- 実施頻度

- 直近の実施日（1 年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の文書名を質問する。

▶閲覧

脆弱性情報/脅威情報の収集から対応までについて定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを

確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

収集した脆弱性情報/脅威情報に対する対応履歴の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 か月以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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・承認制とすることを定めた文書の文書名を質問する。

▶閲覧

- ① ユーザ ID の付与・変更・削除を申請・承認制とすることを定めた文書が実在することを確認する。
- ② ユーザ ID の付与・変更・削除について申請・承認を行った記録を閲覧し、実際に申請・承認が行われていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

ユーザ ID の共有に係る手続について定めた文書の文書名を質問する。

▶閲覧

ユーザ ID の共有に係る手続について定めた文書を閲覧し、ユーザ ID の共有について、以下のいずれかの手続が適用され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。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

ユーザ ID の削除又は無効化に係る手続について定めた文書の文書名を質問する。

▶閲覧

ユーザ ID の削除又は無効化に係る手続について定めた文書を閲覧し、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が定められていることを確認する。

▶観察

原則として実施しない。

(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順を定めていること。

【評価手法】**▶質問**

ユーザ ID に付与したアクセス権の付与・削除に係る手順について定めた文書の文書名を質問する。

▶閲覧

ユーザ ID に付与したアクセス権の付与・削除に係る手順について定めた文書を閲覧し、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順が定められていることを確認する。

▶観察

原則として実施しない。

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】**

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。

【評価手法】**▶質問**

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

管理者 ID の共有に係る手続について定めた文書の文書名を質問する。

▶閲覧

管理者 ID の共有に係る手続について定めた文書を閲覧し、管理者 ID の共有について、以下のいずれかの手続が適用され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、使用人数分の管理者 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。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

管理者 ID の用途及び当該用途における管理者 ID に付与している権限の範囲を質問する（全ての管理者 ID に対して質問する必要はなく、例示でよい。）。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

本番環境における、開発環境の管理者権限の使用をどのように制限しているかを質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

管理者 ID が不要になった場合の処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

管理者 ID の付与・変更・削除を申請・承認制とすることを定めた文書の文書名を質問する。

▶閲覧

- ① 管理者 ID の付与・変更・削除を申請・承認制とすることを定めた文書が実在することを確認する。

- ② 管理者 ID の付与・変更・削除について申請・承認を行った記録を閲覧し、実際に申請・承認が行われていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

- ① 管理者 ID の付与・変更・削除を行う権限を付与している従業員等の範囲を質問する。
- 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付与している従業員等の範囲を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の認証方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

- 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、その重要な機密情報はどのようなものであるかを質問する。（重要な機密情報であるかの判断までは求めない。）
- ② 取り扱っている場合、重要な機密情報を取り扱っているクラウドサービスごとに 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質問する。

▶閲覧

原則として実施しない。

▶観察

重要な機密情報を取り扱うクラウドサービスのうち 1 つを抽出し、登録希望組織の従業員による重要な機密情報を取り扱うクラウドサービスへのログインを観察し、No.4-1-3-3 で示す認証要素を用いた多要素認証が使用されていることを確認する。

(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。

【評価手法】

▶質問

No.4-1-3-2 と併せて実施する。

▶閲覧

原則として実施しない。

▶観察

No.4-1-3-2 と併せて実施する。

(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。

【評価手法】

▶質問

多要素認証の知識情報として用いるパスワードの桁数を質問する。

▶閲覧

原則として実施しない。

▶観察

重要な機密情報を取り扱うクラウドサービスのうち 1 つを抽出し、認証の設定画面等を観察し、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場合

【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。

【評価手法】

▶質問

- ① インターネットを経由して社内環境等へ接続する場合があるかを質問する。
- ② 社内環境等へ接続する際の認証方法について質問する。

▶閲覧

原則として実施しない。

▶観察

登録希望組織の従業員によるインターネットを経由した社内環境へのアクセスを観察し、多要素認証が使用され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。

【評価手法】

▶質問

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おけるロック制御方法を質問する。

▶閲覧

原則として実施しない。

▶観察

パソコンへのログオン及びスマートデバイスを 1 台ずつ抽出し、ロック制御の設定画面等を観察し、評価基準におけるいずれかのロック制御が実施されていることを確認する。

(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。

【評価手法】

▶質問

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当たってのパスワード又は PIN の桁数を質問する。

▶閲覧

原則として実施しない。

▶観察

パソコンへのログオン及びスマートデバイスを 1 台ずつ抽出し、登録希望組織の従業員によるロック解除を観察し、6 文字以上のパスワード又は PIN が利用され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。

【評価手法】

▶質問

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定めた社内ルールの文書名を質問する。

▶閲覧

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定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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

ルの文書名を質問する。

▶**閲覧**

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文書が実在することを確認する。

▶**観察**

原則として実施しない。

(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。

【評価手法】

▶**質問**

ユーザ認証にパスワードを利用する場合の保護対策について定めた社内ルールの文書名を質問する。

▶**閲覧**

ユーザ認証にパスワードを利用する場合の保護対策について定めた社内ルールを閲覧し、評価基準に規定するいずれかの保護対策を講じる旨が定められていることを確認する。

▶**観察**

認証システムの管理画面等を観察し、評価基準に規定するいずれかの保護対策を講じる旨が定められ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。

【評価手法】**▶質問**

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定めた社内ルールの文書名を質問する。

▶閲覧

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定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

パスワード設定に関するルールの周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

パスワードの保管方法について定めた社内ルールの文書名を質問する。

▶閲覧

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など、何らかのパスワードの安全な保管方法を定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(2) No.4-1-6-2 ★3

【評価基準】

パスワードの漏洩が判明した場合、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 パスワードの漏洩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、報道等）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。

【評価手法】

▶質問

パスワードの漏洩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

更する手順の文書名を質問する。

▶閲覧

パスワードの漏洩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手順が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

パスワードの管理に関するルールの周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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係る管理ルールの文書名を質問する。

▶閲覧

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係る管理ルールを閲覧し、以下の全ての内容が含まれて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。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

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行った記録を閲覧し、1年以内に棚卸を実施していることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

重要な機密情報を扱うシステムにおけるユーザ及び管理者ごとに付与している権限の範

囲を質問する。(全ての ID に対して質問する必要はなく、例示でよい。)

▶ 閲覧

原則として実施しない。

▶ 観察

原則として実施しない。

(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。

【評価手法】

▶ 質問

重要な機密情報を扱うシステムにおける付与したアクセス権の運用・利用状況を監視する仕組みの内容を質問する。

▶ 閲覧

原則として実施しない。

▶ 観察

原則として実施しない。

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】

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 サーバの設置エリアに入場可能な者を定めていること。

【評価手法】

▶質問

サーバの設置エリアに入場可能な者を定めた文書の文書名を質問する。

▶閲覧

サーバの設置エリアに入場可能な者を定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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】

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。

【評価手法】

▶質問

サーバの設置に際して実施している安全確保策の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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
たうえで安全に管理すること。

【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。

【評価手法】

▶質問

- ① サーバの設置エリア又は専用ラックの鍵等の管理者を定めた文書の文書名を質問する。
- ② サーバの設置エリア又は専用ラックの鍵の管理方法を質問する。

▶閲覧

サーバの設置エリア又は専用ラックの鍵等の管理者を定めた文書が実在していることを
確認する。

▶観察

原則として実施しない。

(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 か月間保管すること。

【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。

【評価手法】

▶質問

- 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の文書名を質問する。
- ② 上記の記録の保管期間を質問する。

▶閲覧

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の文書が実在していることを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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の文書名を質問する。

▶閲覧

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の文書が実在していることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の文書名を質問する。

▶**閲覧**

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 of 文書が実在していることを確認する。

▶**観察**

原則として実施しない。

(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 of 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 of 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 of 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。

【評価手法】▶**質問**

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 of 内容及び遵守状況 of 点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶**閲覧**

原則として実施しない。

▶**観察**

原則として実施しない。

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】

経営層を含む全ての要員に対して、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。

【評価手法】

▶質問

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の内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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 of 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 of 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。

【評価手法】

▶質問

職場単位で重要なルール及びリスクの周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

- ① 以下の全てのトピックについて実施している教育の実施方法を質問する。
 - 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 上記の教育の実施について、以下の全ての項目について質問する。
 - 実施頻度
 - 直近の実施日

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

No.4-2-1-3 で実施した教育・研修の実施状況を記録した文書の文書名を質問する。

▶閲覧

No.4-2-1-3 で実施した教育・研修の実施状況を記録した文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

教育・研修の実施内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

- ① セキュリティインシデント発生時の対応について実施している教育・訓練の実施方法を質問する。
- ② 上記の教育・訓練の実施について、以下の全ての項目について質問する。
 - 実施頻度
 - 直近の実施日

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

教育・訓練の実施内容の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

- 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の文書名を質問する。
- ② 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の周知方法を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

社外に持ち出すパソコン及び記憶媒体を1点ずつ抽出し、暗号化の方式に応じて暗号化機能の設定画面等を観察し、当該パソコン及び記憶媒体の機密情報を、ルールに従って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。

【評価手法】**▶質問**

- ① 重要な機密情報を暗号化するルールの文書名を質問する。
- ② 重要な機密情報を暗号化するルールの周知方法を質問する。

▶閲覧

重要な機密情報を暗号化するルールを定めた文書が実在することを確認する。

▶観察

重要な機密情報を保管したパソコン、サーバ等の端末を1台抽出し、暗号化の方式に応じて暗号化機能の設定画面等を観察し、当該端末に保管された重要な機密情報を、ルールに従って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。

【評価手法】

▶質問

- ① 情報取扱規程等のデータの取扱に関して定められているルールの文書名を質問する。
- ② ①のルールを役員、従業員、派遣社員及び受入出向者に周知している手段について質問する。

▶閲覧

情報取扱規程等のデータの取扱に関するルールが定められている文書を閲覧し、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が定められていることを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

- ① 取引先との情報共有及び情報送信に関するルールの文書名を質問する。
- ② ①のルールを役員、従業員、派遣社員及び受入出向者に周知している手段について質問する。

▶閲覧

取引先との情報共有及び情報送信に関するルールが定められている文書を閲覧し、以下の全ての内容が含まれて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。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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た文書の文書名を質問する。

▶閲覧

- 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た文書が実在することを確認する。
- ② バックアップファイル等を確認し、①で定めた方法で実際にバックアップを取得していることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

重要な機密情報のバックアップ場所を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

バックアップ対象ごとにリストア手順書の文書名を質問する。

▶閲覧

バックアップ対象のうち1つを抽出し、それに対するリストア手順書が実在することを確認する。

▶観察

原則として実施しない。

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すべ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。

【評価手法】

▶質問

パソコン、サーバ及びスマートデバイスにおける、利用を許可していないソフトウェアの処理方法、又は、利用を許可するソフトウェア以外のインストール制限方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

外部記憶媒体を使用する端末における自動実行（auto-run）又は自動再生（auto-play）機能について、どのように設定しているかを質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

サーバ及びネットワーク機器の設定変更を申請・承認制とすることを定めた文書の文書名を質問する。

▶閲覧

- ① サーバ及びネットワーク機器の設定変更を申請・承認制とすることを定めた文書が実在することを確認する。
- ② サーバ及びネットワーク機器の設定変更について申請・承認を行った記録を閲覧し、実際に申請・承認が行われていることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

パソコン及びサーバ上のデフォルトユーザ ID の処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

利用する OS 及びソフトウェアについて、標準構成・設定ルールを定めた文書の文書名を質問する。

▶閲覧

利用する OS 及びソフトウェアについて、標準構成・設定ルールを定めた文書が実在することを確認する。

▶観察

原則として実施しない。

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、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.4-4-2 の適合基準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。

【評価手法】

▶質問

- ① OS 及びソフトウェアのライセンス・サポートの有効化有無、また、有効でない場合の対応方法について質問する。
- ② 自動アップデートの有効化有無を質問する。

▶閲覧

原則として実施しない。

▶観察

- ① OS 及びソフトウェアのうち 1 件を抽出し、バージョン情報等がわかる画面を観察し、サポートされていることを確認する。
- ② サポートされていない場合、脆弱性悪用のリスクを低減する対策が実施され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 カ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。

【評価手法】**▶質問**

ログの記録について定めた文書の文書名を質問する。

▶閲覧

ログの記録について定めた文書を閲覧し、評価基準で求める種類及び期間について保管していることを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の認証方法を質問する。

▶閲覧

原則として実施しない。

▶観察

登録希望組織の従業員によるインターネットを経由したログの保存媒体又はシステムへのアクセスを観察し、多要素認証が使用され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。

【評価手法】**▶質問**

認証サーバのログを取得していることを確認した上で、認証サーバのログのモニタリングについて、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1 か月以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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、No.4-4-4-2 の適合基準で求める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。

【評価手法】

▶質問

- ① システム、情報機器及びソフトウェアのライセンス・サポートの有効化有無、また、有効でない場合の対応方法について質問する。
- ② 自動アップデートの有効化有無を質問する。

▶閲覧

原則として実施しない。

▶観察

- ① システム、情報機器及びソフトウェアのうち 1 件を抽出し、バージョン情報等がわかる画面を観察し、サポートされていることを確認する。
- ② サポートされていない場合、No.4-4-4-2 の適合基準で求める脆弱性悪用のリスクを低減する対策が実施されていることを確認する。

(2) No.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。

【評価手法】

▶質問

- ① 対象機器・ソフトウェアの把握方法、脆弱性情報の把握方法、アップデート適用の判断方法について質問する。
- ② 14 日以内に適用できない場合があるか否か、また適用できない場合がある際の対応方法について質問する。

▶閲覧

- ① 脆弱性を 1 件抽出して該当するアップデートプログラムがリリースから 14 日以内に適用されていることを確認する。
- ② 14 日以内にアップデートができていない場合、その中から脆弱性を 1 件抽出して対応計画及び適合基準④に記載した暫定対策の実施記録等を確認し、代替措置が講じられていることを確認する。

▶観察

原則として実施しない。

(3) No.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。

【評価手法】

技術検証を実施

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。

【評価手法】

▶質問

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へのマルウェア対策ソフトウェアの導入状況を質問する。

▶閲覧

原則として実施しない。

▶観察

ネットワークに接続しているパソコン及びサーバを1台ずつ抽出し、マルウェア対策ソフトの管理画面等を観察し、ソフトウェアが有効になっ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）および振る舞い検知機能が有効であること。

【評価手法】**▶質問**

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た文書の文書名を質問する。

▶閲覧

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た文書の実在を確認する。

▶観察

ネットワークに接続しているパソコン及びサーバを1台ずつ抽出し、マルウェア対策ソフトの管理画面等を観察し、定められたスキャン範囲及び頻度どおりに設定されていることを確認する。

(No.4-4-5-1 と同時の実施で差し支えない。)

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) および振る舞い検知機能が有効であることを管理画面等で確認する。

(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。

【評価手法】**▶質問**

マルウェア対策ソフトウェアのパターンファイルのアップデート方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

パソコン及び Web ゲートウェイを対象に、不正な Web サイトへのアクセス制限方法を質問する。

▶閲覧

原則として実施しない。

▶観察

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観察し、不正な Web サイトへのアクセスが制限され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。

【評価手法】

▶質問

メールゲートウェイ又はメールサーバ等におけるマルウェアチェックの方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

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。）及びルータにおけるデフォルトの管理パスワードの変更有無、又は、リモートアクセスの無効化有無を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の文書名を質問する。

▶閲覧

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の存在を確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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。）及びルータの認証におけるパスワードの設定状況を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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。）における認証を経していないインバウンド通信の処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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・ルールを記録した文書の文書名を質問する。

▶閲覧

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・ルールを記録した文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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。）における、不要になったファイアウォール・ルールの処理方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

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の認証方法、又は、アクセス可能な IP アドレスの制限方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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、全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。

【評価手法】

▶質問

全てのパソコン及びサーバにおけるソフトウェアファイアウォールの有効化有無を質問する。

▶閲覧

原則として実施しない。

▶観察

パソコン及びサーバからそれぞれ 1 台ずつ抽出し、OS の設定画面等を観察し、利用中の OS が対応していない場合を除き、ソフトウェアファイアウォールが有効化され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。

【評価手法】

▶質問

- ① 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、ネットワーク上の設置場所を質問する。
- ② 併せて、セグメント内外のアクセス制御方法を質問する。

▶閲覧

ネットワーク図等を閲覧し、社外公開サーバ及び重要な機密情報を扱うサーバが専用のネットワークセグメントに設置されていることを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

社内外ネットワークの境界又は端末において不正アクセスをリアルタイム検知・遮断する仕組みの内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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

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。

【評価手法】

▶質問

- 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の分析を行っていることを確認の上、分析結果に基づき不審な事象を発見した場合の、判断プロセスを定めた文書の文書名を質問する。
- ② 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の分析結果に基づき不審な事象を発見した場合の、判断プロセスの内容を質問する。

▶閲覧

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の分析結果に基づき不審な事象を発見した場合の、判断プロセスを定めた文書が実在することを確認する。また、当該文書に従うことで、セキュリティインシデントに該当するかどうかを判断できる内容となっているかを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

不正アクセスをリアルタイム検知・遮断するネットワーク機器又はサービスについて、適合基準で列举する事項を実装する仕組みの内容を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

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。

【評価手法】**▶質問**

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一覧の文書名を質問する。

▶閲覧

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一覧の存在を確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶ 閲覧

原則として実施しない。

▶ 観察

原則として実施しない。

(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。

【評価手法】

▶ 質問

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質問する。

▶ 閲覧

原則として実施しない。

▶ 観察

端末を1台抽出し、外部からのファイルの受領を観察し、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が作動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。

【評価手法】

▶質問

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の周知方法を質問する。

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

- 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におけるインシデントレベルの判断手順を定めた文書の文書名を質問する。
- ② 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における、判断プロセスの内容を質問する。

▶閲覧

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におけるインシデントレベルを判断するための基準又は手順を定めた文書が実在することを確認する。また、当該基準又は手順に従うことで、セキュリティインシデントのレベルを判断できる内容になっているかを確認する。

▶観察

原則として実施しない。

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。

【評価手法】

▶質問

セキュリティインシデント対応手順の文書名を質問する。

▶閲覧

セキュリティインシデント対応手順を閲覧し、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。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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た文書の文書名を質問する。

▶閲覧

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た文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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統括役員及びセキュリティ担当部署の役割及び責任を定めた文書の文書名を質問する。

▶閲覧

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統括役員及びセキュリティ担当部署の役割及び責任を定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

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の点検について、以下の全ての項目について質問する。

- 実施頻度
- 直近の実施日（1年以内に実施していることを確認する。）

▶閲覧

原則として実施しない。

▶観察

原則として実施しない。

(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。

【評価手法】**▶質問**

セキュリティインシデントの報告フォーマットを定めた文書の文書名を質問する。

▶閲覧

セキュリティインシデントの報告フォーマットを定めた文書が実在することを確認する。

▶観察

原則として実施しない。

(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。

【評価手法】

▶質問

- ① インシデント事例及びその対応策の周知方法を質問する。
- ② 過去1年以内の社内外における重大なセキュリティインシデントの発生有無を質問する。

▶閲覧

過去1年以内に重大なセキュリティインシデントが発生していた場合に、事例やその対応策を社内部署へ共有した記録を確認する。

▶観察

原則として実施しない。

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、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】

事業継続上重要なシステムが存在しない場合

【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。

【評価手法】

▶質問

- 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た文書の文書名を質問する。
- ② 事業継続上重要なシステムについて目標復旧レベルまで業務を回復するために整備している必要な対策の内容を質問する。

▶閲覧

システム復旧手順書、事業継続計画等の事業継続上重要なシステムにおける目標復旧レベルを定めた文書を閲覧し、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が定められていることを確認する。

▶観察

原則として実施しない。

(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】

事業継続上重要なシステムが存在しない場合

【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。

【評価手法】

▶質問

事業継続上重要なシステムについてバックアップを取得していることを確認した上で、バックアップ復元テストの実施結果を記録した文書の文書名を質問する。

▶閲覧

事業継続上重要なシステムについてのバックアップ復元テストの実施結果のうち 1 件を抽出して閲覧し、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ていることを確認する。

▶観察

原則として実施しない。

改定履歴

日付	改定内容
2026 年 10 月 28 日	初版発行