

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 要求事項・評価基準 解説書

2026 年 10 月 28 日

SCS 評価制度 制度運営機関

目次

第1章 本解説書について	3
第2章 本制度における★3・★4の位置づけ等.....	4
2.1 ★3の位置づけ等	4
2.2 ★4の位置づけ等	5
2.3 他法制度との関係	6
第3章 取得単位及び適用範囲の考え方	7
3.1 取得単位の考え方	7
3.2 適用範囲の考え方	7
3.2.1 適用範囲に含むもの.....	9
3.2.2 適用範囲に含めないもの	10
3.2.3 端末の所有形態及び利用場所に応じた適用範囲の考え方	11
3.3 取得単位と適用範囲の設定事例等	12
3.3.1 事例①：少数の事業所からなる企業における設定事例.....	12
3.3.2 事例②：多数の子会社等からなる企業グループにおける設定事例	16
3.3.3 適用範囲の境界部分にて講じる必要のある保護施策の考え方	20
3.3.4 登録希望組織からクラウドサービス事業者等に確認すべき事項（例）	21
第4章 本制度（★3・★4）でカバーされるセキュリティのリスク・脅威	23
第5章 要求事項・評価基準の解説	25
5.1 要求事項・評価基準全体で共通する事項の解説	25
5.1.1 「★3・★4 要求事項・評価基準」の構成.....	25
5.1.2 「★3・★4 要求事項・評価基準」におけるシステム・情報の分類	25
別紙 要求事項・評価基準の個別解説	27
No.1 ガバナンスの整備	28
No.1-1 組織の状況.....	28
No.1-2 役割、責任、権限	30
No.1-3 ポリシー	37
No.1-4 監督	39
No.2 取引先管理	40
No.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	40
No.3 リスクの特定	46
No.3-1 資産管理	46
No.3-2 リスクアセスメント	57
No.4 攻撃等の防御	59
No.4-1 アイデンティティ管理、認証、アクセス制御.....	59
No.4-2 意識向上とトレーニング	78
No.4-3 データセキュリティ	81
No.4-4 プラットフォームセキュリティ	86
No.4-5 技術インフラのレジリエンス	97
No.5 攻撃等の検知	100
No.5-1 継続的監視.....	100
No.5-2 有害事象の分析	104
No.6 インシデントへの対応	105
No.6-1 インシデント管理	105
No.7 インシデントからの復旧	108
No.7-1 インシデント復旧計画の実行	108
付録1 用語集	110

第1章 本解説書について

「★3・★4 要求事項・評価基準 解説書」（以下「本解説書」という。）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「本制度」という。）において、登録希望組織が取得単位や適用範囲の設定、自己評価等を適切に実施できるよう、その考え方や留意点を解説するものである。

- ・ 第2章：本制度における★3・★4の位置づけ、評価スキームの概要
- ・ 第3章：取得単位及び適用範囲を設定する際の考え方
- ・ 第4章：「★3・★4 要求事項・評価基準」で対象とするセキュリティのリスク・脅威
- ・ 別紙：各要求事項・評価基準について対策の実施や解釈上留意が必要と考えられる箇所に対する解説

併せて、本解説書は「★3・★4 要求事項・評価基準」に基づくセキュリティ対策の実施に役立つ参考情報を提供するものである。

各評価基準への適合基準や具体的な評価方法については、「★3・★4 自己評価等ガイド」、「★4 第三者評価ガイド」を参照されたい。

第2章 本制度における★3・★4の位置づけ等

本制度は、★3、★4、★5という3つの段階を設けている¹。そのうち★5については今後更なる具体化が予定されている。

本解説書では、★3及び★4を対象として、要求事項・評価基準等を解説する。★3又は★4への取組を始めるに当たっては、独立行政法人情報処理推進機構（以下、「IPA」という。）が別途運営するSECURITY ACTION²についても参考にされたい。SECURITY ACTIONは、中小企業が情報セキュリティ対策への取組を自己宣言する制度であり、その一つ星・二つ星の取組は、本制度の基礎となるセキュリティ対策の実践につながるものである。

また、本制度では上位の段階には下位の段階で求められる事項がすべて含まれる。そのため、例えば、★3を取得していなくても、★4の登録申請を行うことができる。

★3又は★4の登録申請や登録後の維持に必要な手続の詳細については、「★3・★4 登録申請の手引」を参照されたい。

表1 本制度において設ける段階の概要

	★3	★4	★5[検討中]
想定される脅威	・ 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	・ 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 ・ 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	・ 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	すべてのサプライチェーン企業が最低限実装すべきセキュリティ対策	サプライチェーン企業等が標準的に目指すべきセキュリティ対策	サプライチェーン企業等がさらに目指すべき高度な対策
要求事項	26 件	43 件	(今後検討)
有効期間	1 年	3 年	(今後検討)
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

2.1 ★3の位置づけ等

★3では、一般的なサイバー攻撃から組織を守るために必要な基本的なセキュリティ対策を求めている。特に、攻撃者による初期侵入への防御や、侵害が発生した場合の被害拡大への防御を求めている。

（脅威に対する達成水準）

- ・ 組織内の役割と責任が明確に定められている。
- ・ 一般的なサイバー脅威への対処を想定し、自組織のIT基盤への初期侵入、侵害拡大等への対策を実施している。
- ・ インシデントが発生した場合に備え、取引先を含む組織内外の関係者への報告・情報共有に必要な最低限の手順を定め、実施している。

★3登録希望組織は、まず取得単位及び適用範囲を設定した上で、26件の要求事項に関して自己評価を行う。自己評価の結果は、★3確認責任者による確認を受ける必要がある（専門家確認付き自己評価）。その後、経営層が自己評価結果に基づいて要求事項への適合を宣言し、

¹ 「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） <https://www.meti.go.jp/policy/netsecurity/scs.html>

² 「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度である。（<https://www.ipa.go.jp/security/security-action/>）

制度運営機関に対して登録申請を行う。

★3 確認責任者による確認の位置づけや実施方法については、「★3・★4 自己評価等ガイド」第4章を参照されたい。

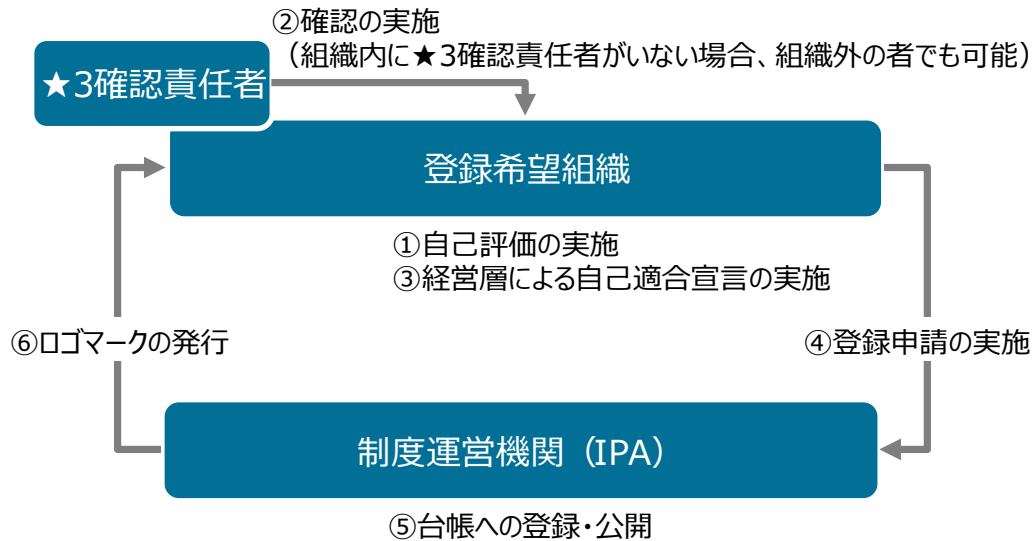


図1 ★3 評価スキームの概要

2.2 ★4 の位置づけ等

★4 は、★3 で求められる最低限の対策に加え、自組織の IT 基盤だけでなく、取引先等への被害拡大を防止し、事業停止や情報漏えい等の重大な被害につながるリスクを低減するための標準的なセキュリティ対策を求めている。

（脅威に対する達成水準）

- ・ 自組織及び取引先のシステムやデータへの被害拡大を防止するとともに、不正アクセス、情報窃取、システム停止等の被害に至ることを防ぐ対策を実施している。
- ・ 事業継続のための取組や取引先のセキュリティ対策状況の把握など、自組織の位置づけに応じたサプライチェーン強靱化策を行っている。

★4 の登録希望組織は、43 件の要求事項に関して自己評価を実施し、評価機関による第三者評価（技術検証事業者による技術検証の実施を含む）を受ける必要がある。評価機関から評価報告書の交付を受けた後、経営層が自己適合宣言を行い、制度運営機関に対して登録申請を行う。

★4 における第三者評価及び技術検証の詳細については、「★4 第三者評価ガイド」及び「★4 技術検証ガイド」を参照されたい。

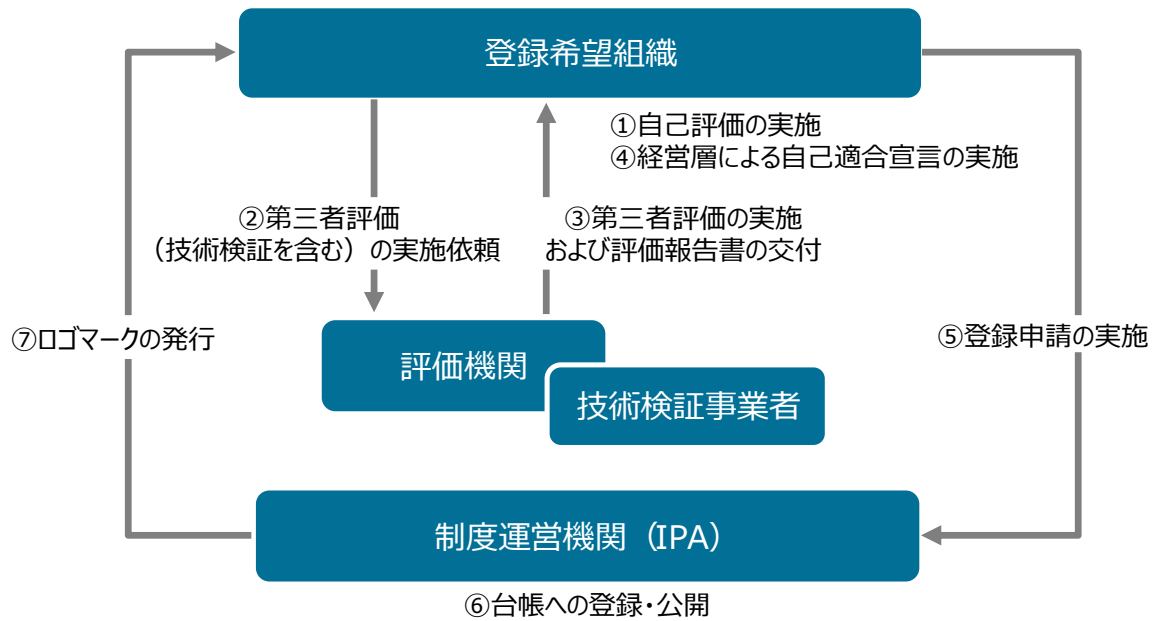


図2 ★4 評価スキームの概要

2.3 他法制度との関係

本制度による★3・★4の取得は、他法制度等（例えば、各重要インフラ分野における安全基準等）に優先・優越するものではなく、当該法制度等で求められるセキュリティ対策・要件・基準等を満たすことを必ずしも保証するものではない。

第3章 取得単位及び適用範囲の考え方

登録希望組織は、自己評価等を実施する前に、まず登録申請の対象となる組織（取得単位）を定める必要がある。その際、3.1 に示す考え方に従い、取得単位に含む事業部、法人等を整理する。次に、登録希望組織は、取得単位を踏まえ、要求事項・評価基準を適用する範囲（適用範囲）を定める。その際、3.2 に示す考え方に従い、適用範囲に含めるものと除外するものを明確に整理する必要がある。

なお、他組織が提供するクラウドサービスや企業グループ共通のネットワーク等を利用している場合、それらが適用範囲に含まれる場合がある。この場合、登録希望組織は、自ら実施すべき対策を行うとともに、それらのサービスの提供者との責任分界を踏まえた対応を行うことが求められる。

3.1 取得単位の考え方

取得単位は、原則として法人又は個人事業主とする。

ただし、法人においては、取得単位及び適用範囲について★3 確認責任者又は評価機関から妥当性の確認を受ける³ことを前提に、事業部、企業グループなどを取得単位とすることができる⁴。事業部、事業所、部署等、組織区分とサイバーセキュリティ対策の責任者が明確であれば、取得単位は規模の大小を問わない。また、取得単位には、登録希望組織の意向に応じて、国内の事業拠点に加えて、国外の事業拠点を含めることができる。

★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。

他の認証制度においては、プロジェクト単位等のあらかじめ存立期間の限られた主体を取得単位とした申請も行われている場合がある。一方で、本制度では、継続的なセキュリティ対策の実施・改善を求めていることから、プロジェクト組織のような期間限定の主体ではなく、法人、企業グループ、事業部等の恒常的な組織を取得単位とすることを求める。

（取得単位の例）

- ・ 個社：株式会社〇〇
- ・ 企業グループ：〇〇グループ⁵
- ・ 事業所：株式会社〇〇 ××事業所

3.2 適用範囲の考え方

適用範囲は、登録希望組織の IT 基盤（クラウド環境で運用するものも含む。）等を含める必要がある。IT 基盤としては、登録希望組織が設定する取得単位において利用されるサーバ、利用者が直接操作するパソコン、スマートフォンなどの端末、ネットワーク機器等のうち、以下のいずれかの条件を満たすものを含める必要がある⁶。適用範囲を設定する目的は、インターネットを経由した不正アクセスやマルウェア感染等の脅威から、登録希望組織の重要な資産を守ることである。そのため、まず保護すべきシステムや機器を明確にし、それらに対して要求事項・評価基準に基づくセキュリティ対策を実施する必要がある。

- ・ インターネットからの通信を受け付けるもの
- ・ インターネットを利用して外部のサービスやシステムと通信するもの

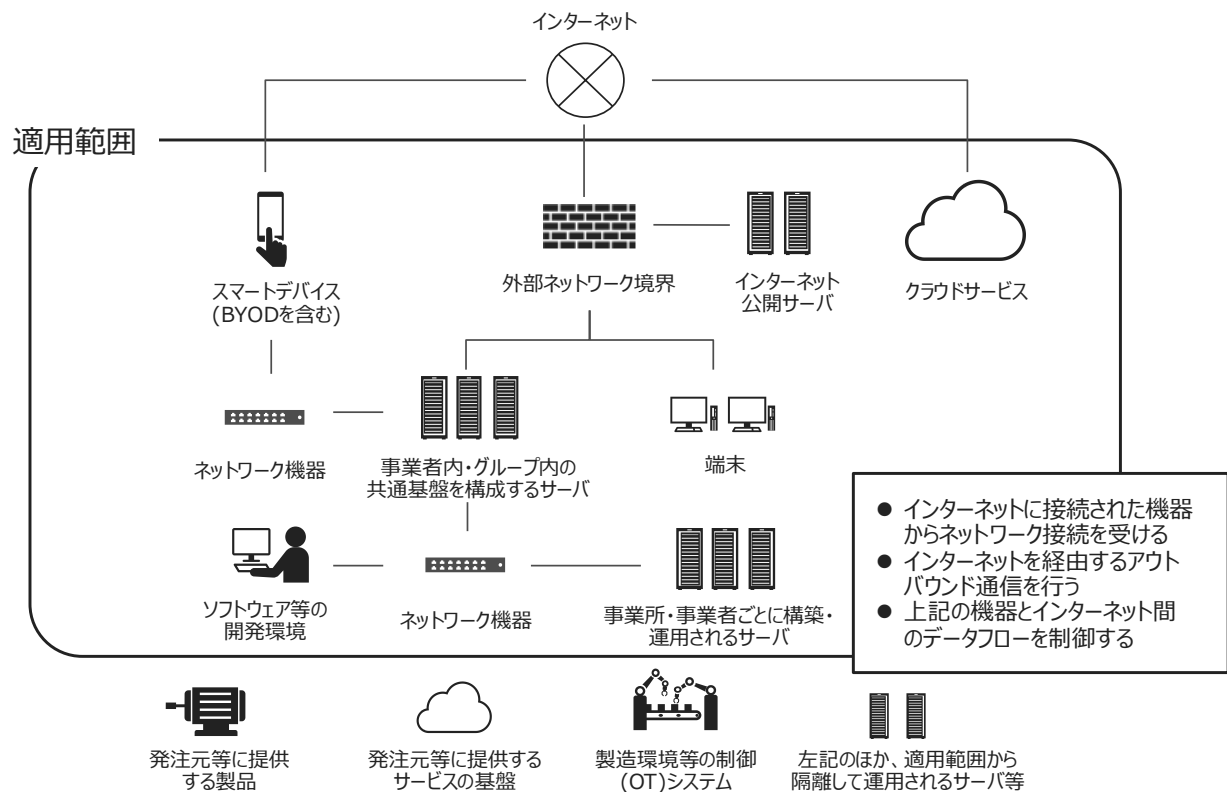
³ 具体的な確認項目については、「★3・★4 自己評価等ガイド」2.2 を参照されたい。

⁴ 事業部、事業所、部署等、当該区分及び責任者が明確であれば、規模の大小を問わない。

⁵ 複数法人を一括して申請する場合は、そこに含まれる法人をすべて列挙する必要がある。

⁶ 適用範囲には、サーバ、端末、ネットワーク機器等に係るハードウェア、OS、ミドルウェア及びアプリケーションのすべてを含む。

・ 上記の機器やシステムとインターネットとの間の通信を制御するもの
 上記を踏まえ、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を以下のように整理することができる。さらなる詳細については、本節 3.2.1 以降の記載のほか、3.3 に示す設定事例を参照されたい。



※1 図示されるもののうち、インターネット公開サーバは必ず適用範囲に含まなければならない。

※2 適用範囲の枠内に示されているか否かを問わず、図中に示すものについて適用範囲から除外する場合、3.3.3に示す考えに基づき適用範囲との境界部分にて保護措置を講じなければならない。

図3 適用範囲の構成例

登録希望組織は、適用範囲から除外する機器やシステムが有る場合、その除外対象及び除外理由を一覧等で整理し、以下に例示するように、その概要を適用範囲の説明に記載しなければならない。また、適用範囲と除外対象との境界にて、3.3.3で示す保護施策を実施する必要がある。

（アセスメントシート等における適用対象に係る記述方法の例）

- ・ 自社のすべての社内ネットワークを含む。ただし、ソフトウェアの開発環境は除く。
- ・ IT システム部門（取得単位）が管理するすべての社内ネットワークを含む。

適用範囲は、登録希望組織が定める取得単位と対応するよう定めなければならない。登録希望組織は、取得単位となる法人又は事業部等が利用するサーバ、端末、ネットワーク機器等のうち本節冒頭に示した条件に合致するものを適用範囲に含める必要がある。一方で、取得単位に含まれない事業部等や法人が独自に利用するサーバ、端末、ネットワーク機器等を適用範囲に含める必要はない。

一般に、企業グループにおいては、企業グループ内部のネットワークを複数の事業所又は法人等により共同で利用している。その際、登録希望組織が利用する適用範囲内のネットワークと、取得単位に含まれない組織が利用する適用範囲外のネットワークのセキュリティ対策が同一であるとみなせる場合、その境界部では、必ずしも 3.3 で示す保護施策の実施までは

求めない⁷。

ただし、境界部において適切な保護施策を実施しない場合、適用範囲外の端末やサーバ等の脆弱性が原因となり登録希望組織が内部ネットワーク経由で不正アクセス等を受けるリスクが残る。登録希望組織においては、取得単位及び適用範囲から除外した事業部等におけるセキュリティ対策状況を把握し、適用範囲の要求事項・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。

3.2.1 適用範囲に含むもの

適用範囲には以下を含む。取得単位に含まれる組織又は適用範囲に含む IT 基盤及び外部ネットワーク境界のうち、自ら管理可能である対象については、★3 又は★4 のうち該当するものの要求事項・評価基準に定められる事項をすべて満たさなければならない。

■ IT 基盤^{8,9}

- ・ IT 基盤を構成するサーバ群¹⁰
- ・ 端末（パソコン、スマートデバイス等、人が使用するインタフェースを持つもの）
- ・ 登録希望組織の IT 基盤を構成するが、他組織との間で対策に係る責任を共有するもの（例：クラウドサービス、親会社の提供する企業グループ共通のネットワーク等）

一般に、自社外の組織が提供するクラウドサービスや企業グループ共通のネットワーク等について、それらの利用者である登録希望組織から詳細なセキュリティ対策状況の確認や追加のセキュリティ対策実施の依頼を行うことは困難である。登録希望組織には、それら外部情報サービス等の利用に際して、以下の対策を行う必要がある。

- ・ 利用者の立場として行う必要のある対策の実施
利用するサービス等の類型により詳細は異なるが、登録を目指す段階（★3 又は★4）に応じて、利用者の立場として少なくとも以下の対策を含めて実施することが求められる。
 - 不正アクセスへの対策
例えば、ID 管理（要求事項 No.4-1-1,4-1-2）、ユーザ認証の実施（要求事項 No.4-1-3,4-1-4）、強固なパスワードの設定（要求事項 No.4-1-5）などが含まれる。
 - 不正アクセスの検知及び対応
例えば、保管データの保護とバックアップの取得（要求事項 No.4-3-1,4-3-4）、継続的な監視（要求事項 No.5-1-1,5-1-2）、インシデント対応手順の整備（要求事項 No.6-1-1）などが含まれる。

⁷ 例えば、同一の物理拠点で複数の事業部や法人等が IT 基盤を共同で利用する際、特定の事業部等が利用するネットワークと他の事業部等が利用するネットワークを分離することが現実的に困難である場合が考えられる。

⁸ IT 基盤には、サーバや端末等のハードウェア、OS・ミドルウェアに加えて、アプリケーションも含む。

⁹ 3.2 で示す条件に合致する場合、ソフトウェアの開発環境等が適用範囲に含まれる場合も想定されるところ、当該環境等において要求事項・評価基準の遵守が困難と考えられる場合は適用範囲内の IT 基盤との境界において、3.3.3 にて考え方を示すネットワーク境界防護要件を実装しなければならない。

¹⁰ 3.2.2 で定める「適用範囲に含めないもの」に該当するものを除く。インターネット公開サーバ（Web サーバ、メールサーバ等）は適用範囲に必ず含める。また、3.2 に示す条件に該当するサーバはその用途等を問わず適用範囲に含まれる。

■ 外部情報サービス等で実施される対策の確認

クラウドサービスに関しては、例えば、利用時のセキュリティ要件を定め、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等が必要である¹¹。別紙で述べるように、その確認は、認証取得状況の確認、SOC2（SOC for Service Organizations: Trust Services Criteria）報告書の確認又はサービス仕様の確認等により行うことが考えられる。

親会社の提供する企業グループ共通のネットワーク等についても同様の対応が求められる。例えば、共通ネットワークの提供者（例：親会社等）からアセスメントシート等を共有してもらう、又は★3 又は★4 のうちしかるべき段階の登録を有していることを確認する等により対策状況の確認を行うことも有効である。

■ 外部ネットワーク境界

- ・ 適用範囲の境界を定義するネットワーク機器（ファイアウォール、ルータ、VPN 機器等）¹²

なお、外部ネットワーク境界のうち、脆弱性を悪用された場合に登録希望組織の IT 基盤に対する攻撃の起点となり得る機器であり、外部から直接アクセス可能な VPN 機器、ルータ、ファイアウォールその他これらに類する通信制御機能を有する機器については、★4 第三者評価において技術検証の対象とする。

3.2.2 適用範囲に含めないもの

一般的に「IT 基盤」又は「外部ネットワーク境界」に含まれないと考えられる以下のシステム又は機器については、本制度の対象外とする。

- ・ 製造環境等の制御（OT）システム（例：一方向セキュリティゲートウェイで外部ネットワークと区切られた製造拠点の制御システム）
- ・ 上記のほか、事業上の必要性等により要求事項・評価基準の遵守が困難¹³であり、適用範囲から隔離して運用されるサーバ、端末
- ・ 発注元等に販売する製品等、登録希望組織が管理・運用を行わないもの、又は登録希望組織が管理・運用を行うが要求事項・評価基準の遵守にあたり登録希望組織以外の組織による対応が必要なもの（例：クラウドサービス等の登録希望組織が構築・運用し、社外組織向けに提供する IT サービスの提供基盤）

登録希望組織は、これらと適用範囲内の IT 基盤がネットワーク接続している場合、その境界において、3.3.3 で考え方を示すネットワーク境界防護要件を実装しなければならず、当該要件が具備されていない場合は制御（OT）システムに該当するものであっても適用範囲に含まねばならない。

製造環境等の制御（OT）システム、発注元等に提供する製品等については、対策実施の前提や求められる対応が基本的に異なる¹⁴ことから直接の対象とはしない。例えば以下に示すよ

¹¹ 例えば、評価基準 No.3-1-3-1 参照

¹² 他組織の内部システムへ接続する際の境界を構成する機器を含む。

¹³ 例えば、サービスの開発や研究等を推進するために、会社の許可リストにないソフトウェア又はサービスを利用している、又は古いソフトウェアをバージョンアップせずに利用している等が考えられる。

¹⁴ 例えば、工場等の製造環境においては、以下のような特徴があるため、こうした特徴に即した サイバーセキュリティ対策が必要となる。

- ・ IT セキュリティ分野で一般的なデータの保護だけでなく、機器稼働等の維持や安全の確保が求められる。

- ・ 古い設備が運用されている場合など、既存システムに対する段階的なセキュリティ対策の導入が必要になる。

うな他の制度・ガイドライン等に基づき対策を行うことを想定する。

- 制御（OT）システムを対象とする主な制度・ガイドライン等
 - ・ 経済産業省『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.1』
 - ・ 経済産業省『半導体デバイス工場における OT セキュリティガイドライン』
 - ・ 米国立標準技術研究所（NIST）『NIST SP 800-82 Rev. 3 Guide to Operational Technology（OT） Security』
 - ・ 国際電気標準会議（IEC）『IEC 62443 Industrial communication networks - Network and system security』
- IT 製品又は IoT 製品を対象とする主な制度・ガイドライン等
 - ・ IT セキュリティ評価及び認証制度（JISEC）
(<https://www.ipa.go.jp/security/jisec/index.html>)
 - ・ セキュリティ要件適合評価及びラベリング制度（JC-STAR）
(<https://www.ipa.go.jp/security/jc-star/index.html>)
 - ・ IPA『IT 製品の調達におけるセキュリティ要件リスト』
(<https://www.ipa.go.jp/security/it-product/index.html>)

3.2.3 端末の所有形態及び利用場所に応じた適用範囲の考え方

役員又は従業員が個人所有する端末を業務に利用する場合（BYOD：Bring Your Own Device）、それらの端末は適用範囲に含めること。ただし、業務上の通話、SMS（Short Message Service）及び多要素認証のためだけに利用する機器は、適用範囲から除くことができる。

役員又は従業員が在宅勤務等で利用する機器は、登録希望組織が支給したものであるかを問わず適用範囲に含める。登録希望組織が支給したルータは適用範囲に含めるが、それ以外のルータは適用範囲に含める必要はない。

この場合、当該ルータに接続する端末においてソフトウェアファイアウォール等の対策を講じることが望ましい。なお、VPN を経由して業務を行う場合、外部ネットワーク境界は当該 VPN の接続先に設置されたネットワーク機器とみなす。

委託先等が所有する端末を用いて自社のシステムに接続させる場合、当該端末は適用範囲には含めない。この場合においても、登録希望組織は、当該端末が自社の機密情報又は業務システムを取り扱う際の条件を定め、その遵守状況を確認する必要がある。

表 2 端末の所有形態及び利用場所に応じた適用範囲の考え方

機器所有形態	機器種別	適用範囲の設定における取扱い
登録希望組織所有	端末	適用範囲に含める。その際、利用場所（在宅勤務等）は問わない。
	ルータ	
個人所有	端末	業務に利用する場合、適用範囲に含める。 業務上の通話、SMS 及び多要素認証アプリの利用にのみ供する機器は、適用範囲から除くことができる。
	ルータ	適用範囲には含めない。
委託先所有	端末	適用範囲には含めない。
	ルータ	適用範囲には含めない。

・ 工場等の規模や性質によって行うべき対策が異なる。（経済産業省『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.1』
(https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.1.pdf))

3.3 取得単位と適用範囲の設定事例等

本節では、以下の取得単位と適用範囲の設定事例等について、解説する。

- 事例①：少数の事業所からなる企業における設定事例（3.3.1）
- 事例②：多数の子会社等からなる企業グループにおける設定事例（3.3.2）

各事例では、想定する組織及びネットワーク構成等を整理し、取得単位に応じて適用範囲に含めるべき構成要素を示す「適用範囲の構成例」、「適用範囲の定義にあたり講じる必要のある施策等」¹⁵を記載している。

その他、3.3.3 において適用範囲の境界部分にて講じる必要のある保護施策の考え方を示すとともに、3.3.4 において登録希望組織からクラウドサービス事業者等に確認すべき事項を例示する。3.3.3 及び 3.3.4 の内容は、3.3.1 と 3.3.2 に示す事例以外でも一般的に適用できるものである。

3.3.1 事例①：少数の事業所からなる企業における設定事例

(1) 想定する組織及びネットワーク構成等

以下では、少数の事業所からなる中小規模の企業を想定し、取得単位及び適用範囲の設定の考え方についてより具体的に解説するため、図 4 に示す企業について仮想的な設定事例を示す。

- ・ A 社は国内に B 事業所と C 事業所という 2 つの製造拠点を有する製造事業者（従業員規模としては 100～300 名程度を想定）である。
- ・ そのうち B 事業所は本社所在地でもあり、製造部門（製造 I 部）のほか、経営管理部及び営業部も所在している。情報システム及び IT セキュリティについては、経営管理部 総務課の情報システム係（2 名）が担当している。
- ・ C 事業所にも製造部門（製造 II 部）が置かれており、情報システム係が整備した情報端末等を利用している。
- ・ A 社で共通に利用されるシステムは、X 社が運用するデータセンター内に構築、運用されている。
- ・ A 社の Web サーバは、Y 社が提供する IaaS/PaaS 上に構築、運用されている。
- ・ 電子メール、社内で利用するファイルの保管等について、Z 社が提供する SaaS を利用している。

¹⁵ 「適用範囲の定義にあたり講じる必要のある施策等」は、例示のように適用範囲を設定しようとする際に登録希望組織が実施する必要のある施策等を示す。登録取得のためには、適用範囲に含まれる IT 基盤において別途要求事項・評価基準に基づく対策等の実装が必要である。

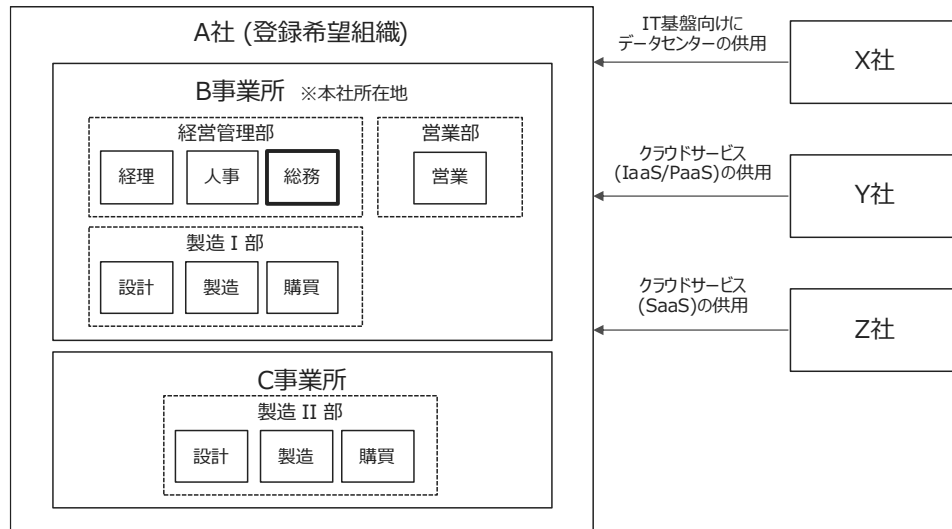


図4 想定する組織の概要図

A社は、図5に示すようなネットワーク構成を有する。

- ・ A社は、B事業所及びC事業所で共通に利用されるIT基盤をX社データセンター内に構築・運用している。
- ・ WebサーバをY社が提供するクラウドサービス（IaaS/PaaS）上に実装している。
- ・ 同様に、電子メール、勤怠管理等について、Z社が提供するクラウドサービス（SaaS）を利用している。
- ・ 各事業所は、広域イーサネットを通じてIT基盤を利用するほか、製造部門が主導して製造現場で稼動する加工装置、検査装置及び端末等を調達する場合がある。それら製造環境で稼動する機器は、ファイアウォールでIT基盤を利用する環境とは論理的に分離された環境に設置されている。

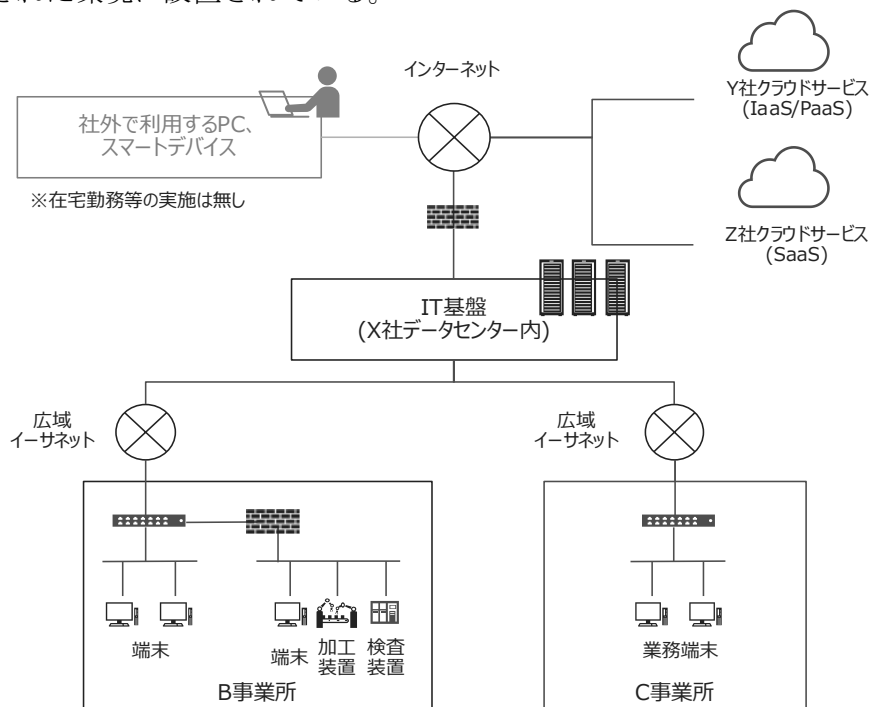


図5 想定するネットワーク構成の概要図

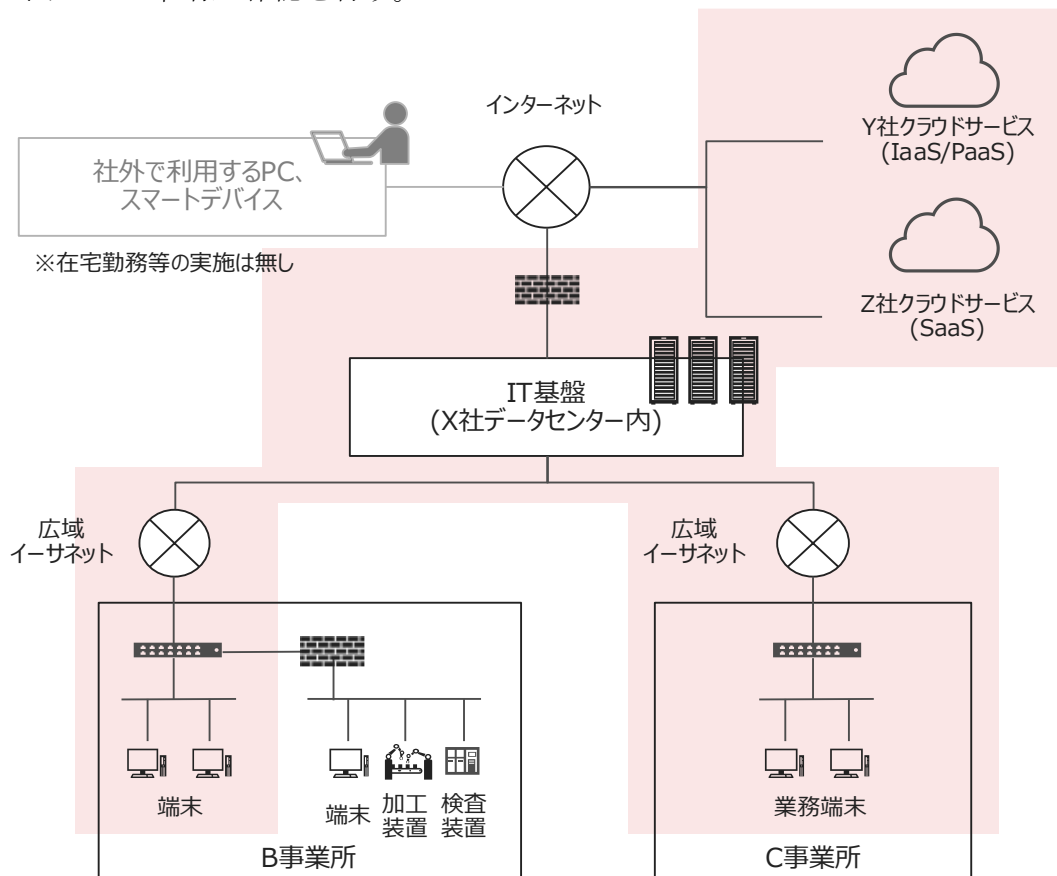
(2) B事業所とC事業所の両方を適用範囲に含める場合

■ 適用範囲の構成例

- ・ A社がB事業所とC事業所の双方を含めて登録を目指す場合、以下を適用範囲に含めることが考えられる。これらのうち、インターネット公開サーバ（Webサーバ、メールサーバ等）は必ず適用範囲に含まねばならない。
 - － IT基盤（X社データセンター内）
 - － Y社クラウドサービス（IaaS/PaaS）
 - － Z社クラウドサービス（SaaS）
 - － A社のB事業所及びC事業所で利用する端末

■ 適用範囲の定義にあたり講じる必要のある施策等

- ・ B事業所で利用される加工装置、検査装置及び端末等が所定のセキュリティ要件を遵守することが困難な場合、インターネットからの通信を受け付けないよう、ファイアウォール等により適用範囲内のネットワークと適切に分離する必要がある。
- ・ A社はX社、Y社及びZ社に対して、例えばサービス調達時にセキュリティ対策状況やサービス仕様の確認を行う。

図6 B事業所とC事業所の両方を適用範囲に含める場合の適用範囲（例）¹⁶

(3) B事業所のみを適用範囲に含める場合

■ 適用範囲の構成例

- ・ A社が適用範囲にB事業所を含め、C事業所を除いて登録を目指す場合、以下を適用範囲に含めることが考えられる。このような適用範囲設定を行う場合として、例えば、

¹⁶ 3.3.1 及び 3.3.2 で示す適用範囲の図において、網掛け部分が適用範囲を示す。また、登録希望組織の判断で図6でいう加工装置や検査装置を範囲に含めることも可能である。

C 事業所においてサポート切れの業務端末を利用しており、リプレースの計画も未定であり、要求事項 4-4-2 を満たせないために、適用範囲から除外せざるを得ないような場合が考えられる。

- IT 基盤 (X 社データセンター内)
- Y 社クラウドサービス (IaaS/PaaS)
- Z 社クラウドサービス (SaaS)
- A 社の B 事業所で利用する端末
- ・ 上記のうち、インターネット公開サーバ (Web サーバ、メールサーバ等) は必ず適用範囲に含まねばならない。

■ 適用範囲の定義にあたり講じる必要のある施策等

- ・ B 事業所で利用される加工装置、検査装置及び端末等が所定のセキュリティ要件を遵守することが困難な場合、インターネットからの通信を受け付けるものをファイアウォール等により適用範囲内のネットワークと適切に分離する必要がある。
- ・ C 事業所と IT 基盤との境界において、ファイアウォール等により適用範囲内のネットワークと C 事業所のネットワークを適切に分離することが望ましい。
- ・ A 社は X 社、Y 社及び Z 社に対して、例えばサービス調達時にセキュリティ対策状況やサービス仕様の確認を行う。

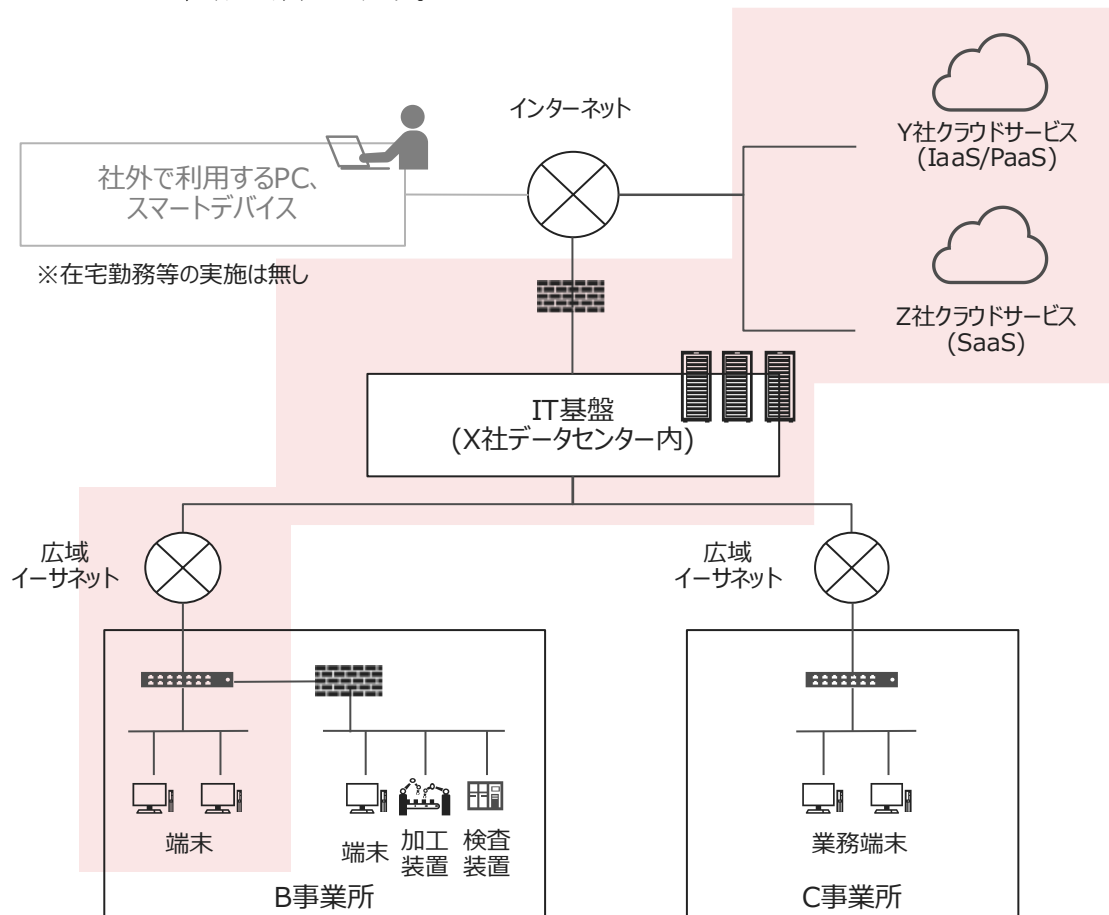


図 7 B 事業所のみを適用範囲に含める場合の適用範囲（例）

3.3.2 事例②：多数の子会社等からなる企業グループにおける設定事例

(1) 想定する組織及びネットワーク構成等

以下では、前項とは異なり、国内外に多数の子会社等を有する比較的大規模な企業における取得単位、適用範囲設定の考え方として、図 8 に示す企業群について仮想的な設定事例を示す。

- ・ A 社は多数の国内子会社（B 社を含む）、海外子会社を有する企業であり、子会社とあわせて A グループを構成している。
- ・ A 社 IT・セキュリティ部門は、自社に加えて国内子会社及び海外子会社が利用する共通の IT 基盤を X 社が提供するデータセンター内に構築・運用している。
- ・ A グループでは、同グループに含まれる法人すべてにおいて共通に適用される A グループ情報セキュリティ対応方針を策定している。その他、各法人において個別により具体的なセキュリティに係る規程等を策定している。
- ・ A 社では、事業所ごとにシステムを調達し、当該事業所の技術部が管理・運用している場合がある。
- ・ A 社は共通の IT 基盤の一部のサービスとして、Y 社が提供するクラウドサービス（IaaS/PaaS）を利用している。
- ・ A 社は一部のサービスについて、Z 社が提供するクラウドサービス（SaaS）を利用している。

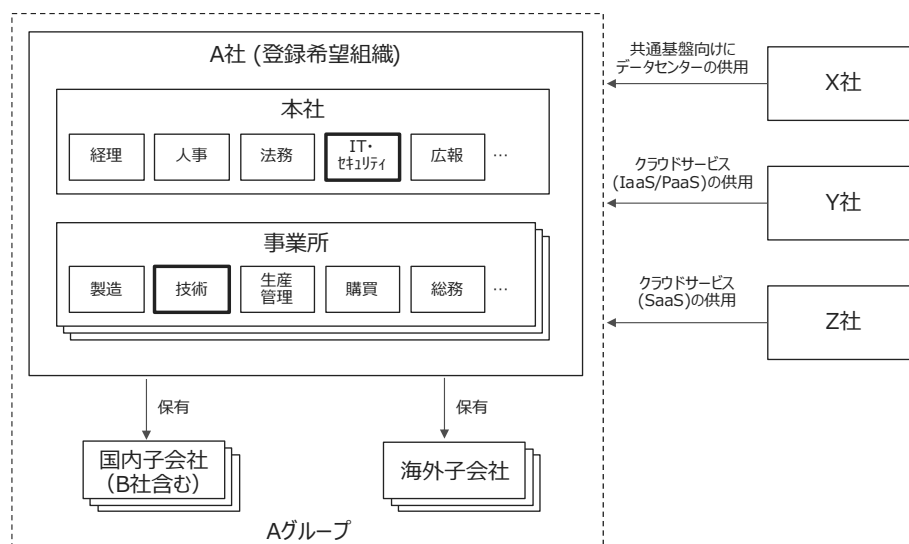


図 8 想定する組織の概要

A 社及びそのグループ会社は、図 9 に示すようなネットワーク構成を有する。

- ・ A 社は、自社に加えて国内子会社及び海外子会社が利用する共通の IT 基盤を X 社データセンター内に構築・運用している。
- ・ 共通の IT 基盤の一部のサービスを Y 社が提供するクラウドサービス（IaaS/PaaS）上に実装している。
- ・ 同様に、一部のサービスについて、Z 社が提供するクラウドサービス（SaaS）を利用している。
- ・ A 社内の各事業所、国内子会社、海外子会社は、拠点間 VPN 等を通じて共通の IT 基盤を利用するほか、各社個別にシステムを調達・構築・管理している。

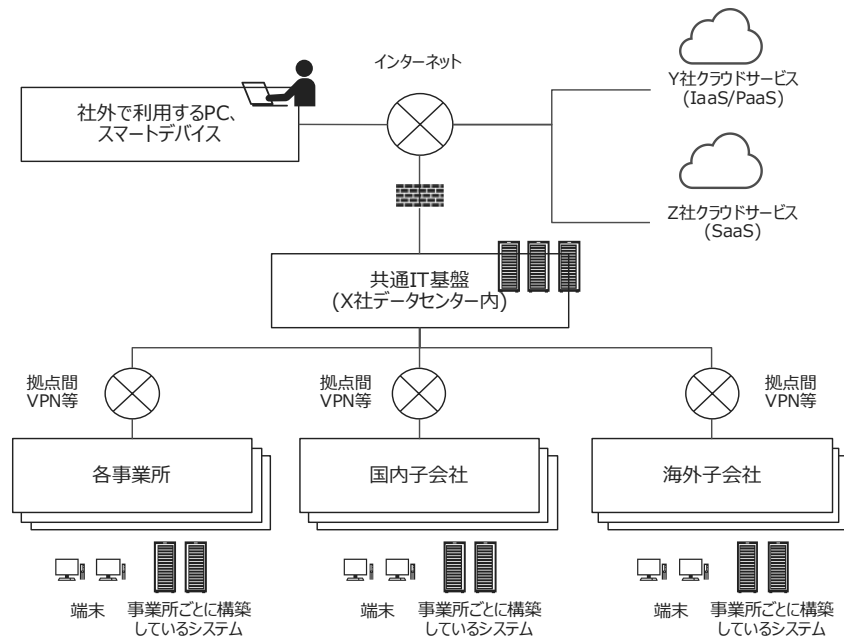


図9 想定するネットワーク構成の概要

(2)A 社（親会社、持株会社等）が単体で登録しようとする場合

適用範囲の構成例

A 社が単体で登録を目指す場合、以下を適用範囲に含めることが考えられる。これらのうち、インターネット公開サーバは（Web サーバ、メールサーバ等）必ず適用範囲に含まねばならない。

- ・ 共通の IT 基盤（X 社データセンター内）
- ・ 社外環境（パソコン、スマートデバイス等）
- ・ Y 社クラウドサービス（IaaS/PaaS）
- ・ Z 社クラウドサービス（SaaS）
- ・ A 社の各事業所で利用する端末、事業所ごとに構築しているシステム

■ 適用範囲の定義にあたり講じる必要のある施策等

- ・ 共通の IT 基盤等に接続する国内子会社、海外子会社を適用範囲から除外する場合、適用範囲の境界部分にてネットワーク機器等（例：VLAN、ファイアウォール）による保護施策を講じることが望ましい。なお、ネットワーク分離が困難である場合は、適用範囲外の組織に起因する事故等が適用範囲内に及ぼす影響を考慮し、アクセス管理、脆弱性管理、インシデント報告等について、「★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。
- ・ A 社は、共通の IT 基盤に加え、個々の管理部門へのアセスメントシート等の送付・回収等を通じて、事業所ごとに構築しているシステムが要求事項・評価基準に適合しているか確認する必要がある。
- ・ A 社は X 社、Y 社及び Z 社に対して、例えばサービス調達時にセキュリティ対策状況やサービス仕様の確認を行う。

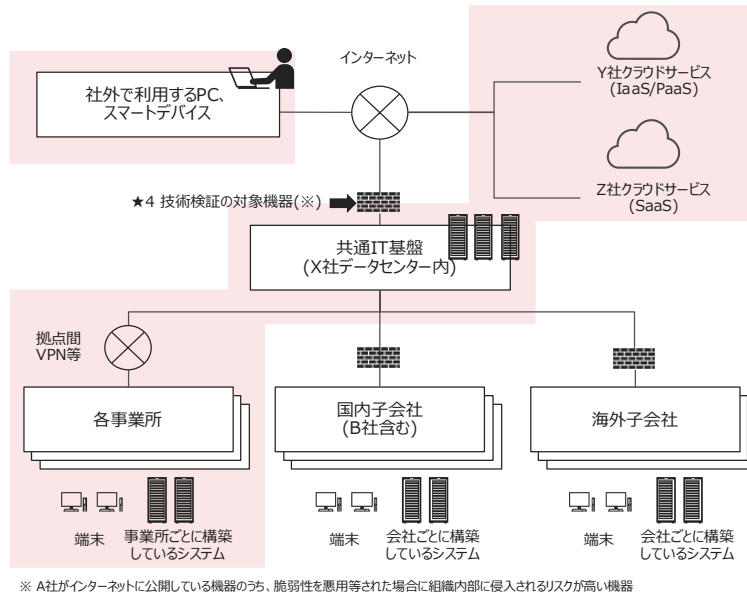


図 10 A 社（親会社、持株会社等）が単体で登録しようとする場合の適用範囲（例）

A 社が法人単位で登録しようとする場合のほか、A 社を構成する個別の事業所が登録しようとする場合も想定される。そのような場合においても図 10 に示す適用範囲を参考とすることができるが、以下について留意することが必要となる。

- ・ 取得単位となる事業所が自ら構築又は運用するシステムのほか、A 社内で共通に利用される IT 基盤のうち当該事業所で利用しているもの（クラウドサービスを利用しているものを含む）を適用範囲に含む必要がある。
- ・ 登録にむけて実施する自己評価に対する経営層の自己適合宣言について、取得単位を個別の事業所とする場合は、実施主体を A 社の経営層（例：取締役）とすることまでは要さず、当該事業所において経営に係る意思決定を行う者（例：事業所長）とすることである。

(3) 企業グループ単位（海外子会社を除く）で登録しようとする場合

■ 適用範囲の構成例

- ・ 企業グループ単位（海外子会社を除く）で登録を目指す場合、以下を適用範囲に含めることが考えられる。
 - － 共通の IT 基盤（X 社データセンター内）
 - － 社外環境（パソコン、スマートデバイス等）
 - － Y 社クラウドサービス（IaaS/PaaS）
 - － Z 社クラウドサービス（SaaS）
 - － A 社の各事業所で利用する端末、事業所ごとに構築しているシステム
 - － 国内子会社で利用する端末、事業所ごとに構築しているシステム

■ 適用範囲の定義にあたり講じる必要のある施策等

- ・ 共通の IT 基盤等に接続する海外子会社を適用範囲から除外する場合、適用範囲の境界部分にてネットワーク機器等（例：VLAN、ファイアウォール）による保護施策を講じることが望ましい。
- ・ A 社は、共通の IT 基盤に加え、個々の管理部門（B 社含む）へのアセスメントシート等の送付・回収等を通じて、事業所・国内子会社ごとに構築しているシステムが要求事項・評価基準に適合しているか確認する必要がある。
- ・ A 社は X 社、Y 社及び Z 社に対して、例えばサービス調達時にセキュリティ対策状況やサービス仕様の確認を行う。

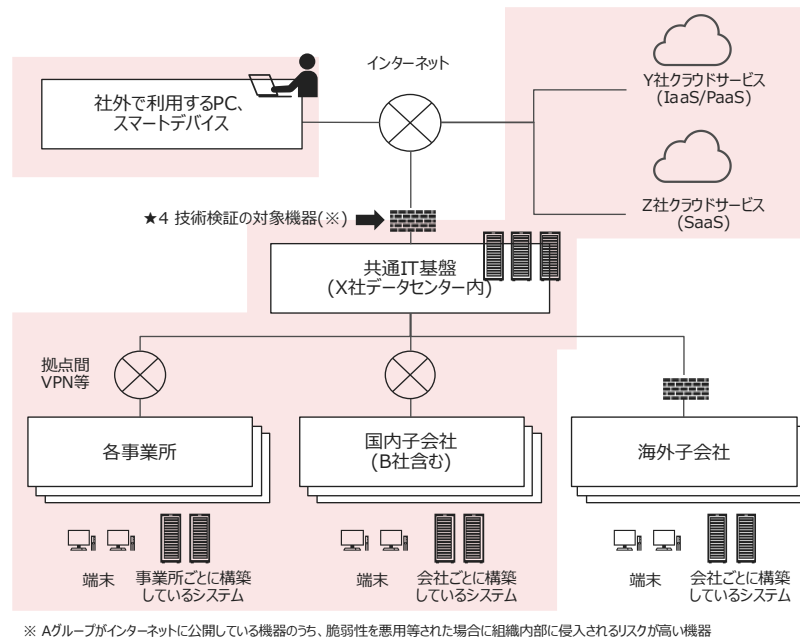


図 11 企業グループ単位（海外子会社を除く）で登録しようとする場合の適用範囲（例）

(4) B 社（グループ子会社）が単体で登録しようとする場合

■ 適用範囲の構成例

- ・ B 社が単体で登録を目指す場合、以下を適用範囲に含めることが考えられる。
 - － B 社で利用する端末、独自に構築しているシステム
 - － 社外環境（パソコン、スマートデバイス等）
 - － 共通の IT 基盤（X 社データセンター内）
 - － Y 社クラウドサービス（IaaS/PaaS）
 - － Z 社クラウドサービス（SaaS）

■ 適用範囲の定義にあたり講じる必要のある施策等

- ・ 共通の IT 基盤等に接続する他の組織（例：海外子会社）を適用範囲から除外する場合、除外対象とする組織との境界部分にてネットワーク機器等（例：VLAN、ファイアウォール）による保護施策を講じる、又は講じられていることを確認することが望ましい。
- ・ B 社は、自社で管理しているシステムに加え、親会社である A 社管理部門へのアセスメントシート等の送付・回収等を通じて、共通の IT 基盤等システムが要求事項・評価基準に適合しているか確認する必要がある。
- ・ B 社は A 社（A 社を通じて、X 社、Y 社、Z 社）に対して、例えばサービス調達時にセキュリティ対策状況やサービス仕様の確認を行う。

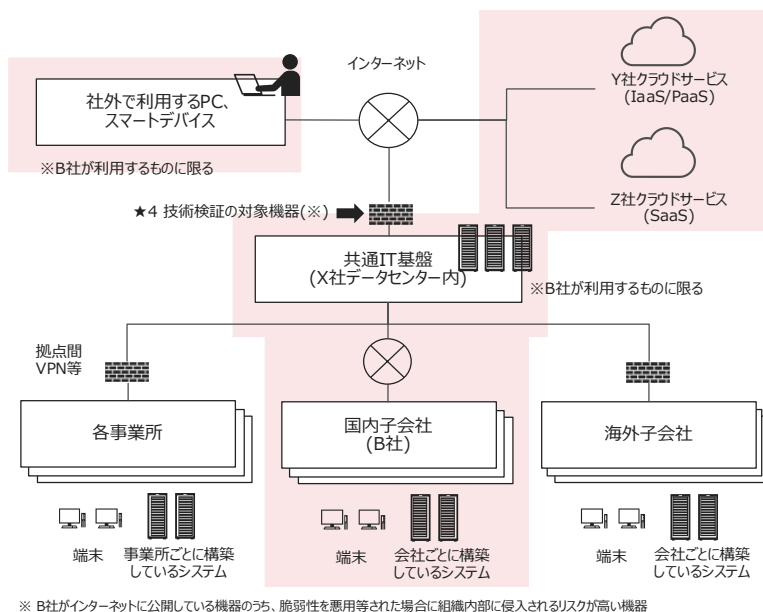


図 12 B 社（グループ子会社）が単体で登録しようとする場合の適用範囲（例）

3.3.3 適用範囲の境界部分にて講じる必要のある保護施策の考え方

適用範囲の境界部分では、図 13 に示す考え方に基づき適用範囲外で生じた侵害が適用範囲内へ容易に波及しないよう、環境に応じた対策を講じる必要がある。

- 適用範囲内と適用範囲外は、ファイアウォール、VLAN、クラウドサービスのネットワーク制御機能その他これらと同等の技術的手段により区分する。両者の間で通信を行う場合、評価基準 No.4-5-1-4 及び同 4-5-1-5 で定めるように、適用範囲外からの通信は適用範囲内のネットワークから見てインターネットからの通信と同様に扱うものと捉え、ファイアウォール、アクセス制御リスト等により、業務上必要な範囲に限定する。構成上可能な場合は、適用範囲外から適用範囲内への通信を原則として拒否し、必要な通信のみを許可することが望ましい。
- 適用範囲内と適用範囲外のネットワークは相互に通信が可能であっても、上記を満たす限りにおいて適用範囲の境界を構成するものとして有効である。その際、境界の保護は、ファイアウォール又は VLAN を使用して、OSI 参照モデルのデータリンク層、ネットワーク層又はそれらと同等の機能を提供する技術（例：クラウドサービスにおけるセキュリティグループ）¹⁷を用いて実施する必要がある。
- 上記の施策を行うことが困難な場合、ネットワークを共用する一方で取得単位と適用範囲に含まれていない事業部や法人等におけるセキュリティ対策状況を把握し、適用範囲の要求事項・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。

¹⁷ ここで「同等の機能を提供する技術」とは、ファイアウォール又は VLAN 等のネットワーク通信の制御によりアクセス制御等を行うものを想定するものであり、ID やパスワードの組合せ等によりアクセス制御を行うものは含まない。

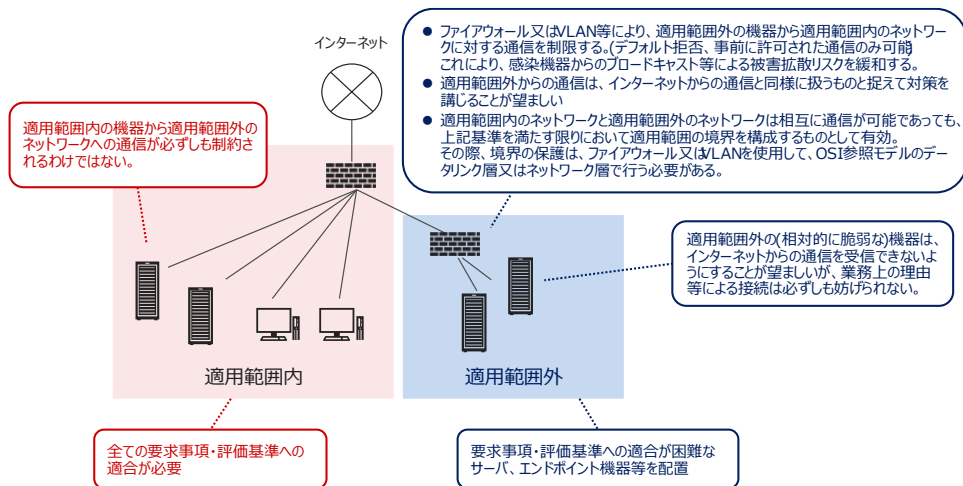


図13 適用範囲の境界部分にて講じる必要のある保護施策の考え方

3.3.4 登録希望組織からクラウドサービス事業者等に確認すべき事項（例）

一般に、クラウドサービスのセキュリティを高めるためには、クラウドサービス事業者とクラウドサービスの利用者が協力して、クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方（責任共有モデル）を多くのクラウドサービス事業者が採用している。

上記事例における登録希望組織のA社は、自社のIT基盤においてサービスを利用しているY社（IaaS/PaaS）又はZ社（SaaS）に対して、以下の要求事項（例）の遵守状況を確認することが考えられる¹⁸。当該確認は、サービス仕様やSOC2 Type 2 報告書¹⁹、クラウドサービス事業者等が開示する報告書等の確認によって行うほか、クラウドサービス事業者に対して個別に照会を行うことでも実施され得る。

■ 物理セキュリティの管理に係るもの

- ・ 要求事項 No. 4-1-8 サーバの設置エリアへの入退室を管理し、記録すること。
- ・ 要求事項 No. 4-1-9 可搬媒体の持込み・持出しを制限すること。

■ 仮想環境・OS・ミドルウェア²⁰等の管理に係るもの

- ・ クラウドサービスが提供する識別・認証・アクセス制御に係る機能
 - － 要求事項 No. 4-1-2 管理者 ID の発行・変更・削除の手続を定めること。
 - － 要求事項 No. 4-1-3 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。
- ・ クラウドサービスの提供に関連するソフトウェアの管理
 - － 要求事項 No. 3-2-1 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。
 - － 要求事項 No. 4-4-1 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。
 - － 要求事項 No. 4-4-2 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

¹⁸ これらの確認対象をどこまでとするかはサービスの類型等により異なる。

¹⁹ SOC2 は、米国公認会計士協会（AICPA）が定める、委託会社の内部統制やサイバーセキュリティについての内部統制の保証の報告書であり、中でも Type 2 は、サービス組織が一定の期間（通常は 6 ヶ月以上）にわたって、自社の情報セキュリティに対する管理策が持続的に適切に実装されていることを示す評価である。

²⁰ OS とアプリケーションソフトウェアの中間に位置し、様々なソフトウェアから共通して利用される機能を提供するもののこと。

- 改を実施すること。
- 要求事項 No.4-4-4 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。

第4章 本制度（★3・★4）でカバーされるセキュリティのリスク・脅威

★3・★4 が対象とするアタックサーフェス²¹として、「1. 運用中の IT 基盤に対する論理アクセス」、「2. 運用中の IT 基盤に対する物理アクセス」、「3. 廃棄時の IT 基盤構成要素（例：サーバ、端末）に対する物理アクセス」を想定し、開発・調達時の IT 基盤に係るサプライチェーンにおける接触は必ずしも対象としない。

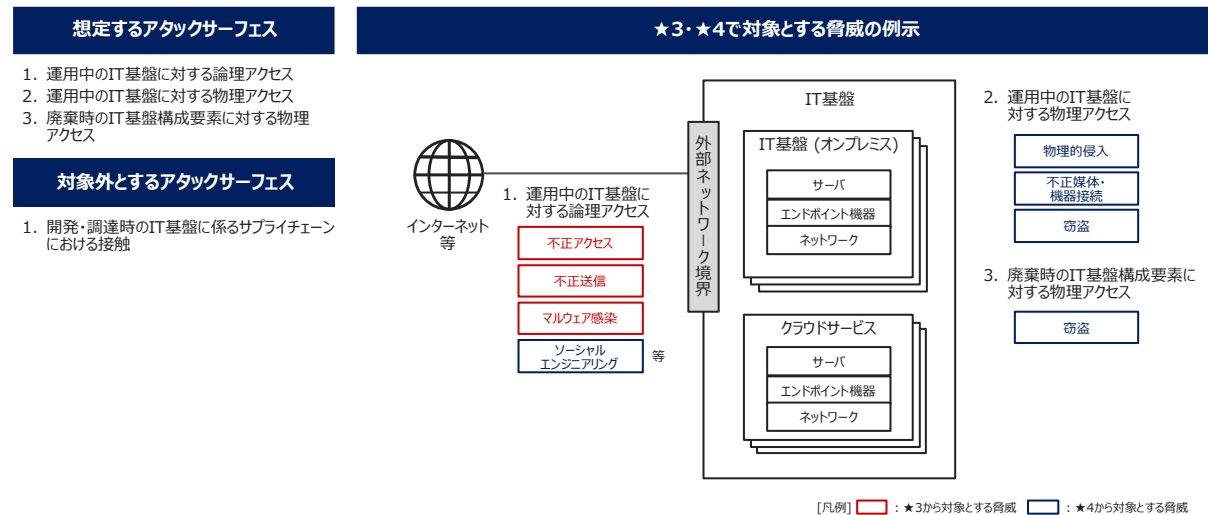


図 14 想定するアタックサーフェス及び脅威の例示

対象とするアタックサーフェスを踏まえ、★3・★4 で想定する脅威を以下のように整理している。

表 3 「★3・★4 要求事項・評価基準」でカバーされるセキュリティのリスク・脅威の分類

分類	脅威	概要	対応する要求事項等（例）	
論理	不正アクセス	正規の認証によりネットワーク経由で機器に侵入し、攻撃を実行する。	★3	4-1-3 認証の強度・実装方法の決定 4-1-5 パスワード設定ルール
		脆弱性の悪用によりネットワーク経由で機器に侵入し、攻撃を実行する。	★3	3-2-1 脆弱性の管理体制 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 4-4-4 セキュリティパッチ・アップデートの手続
	ソーシャルエンジニアリング（フィッシングを含む）	内部関係者（社員や協力者のうち、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	★4	4-2-1 セキュリティの意識向上のための教育・研修
	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	-	正規のプログラムやコマンド、サービス等の悪用は対応できない
	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正な	★3	4-1-2 管理者 ID の管理手続

²¹ アタックサーフェスとは、サイバー攻撃者が侵入する可能性のある、すべてのポイントや経路のこと

		データ（不正な値、不正な形式等）を送信する。		
	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	★3	4-4-5 マルウェア感染からの保護
	否認	攻撃者が操作ログを削除又は改ざん等することで、実行した操作を否定する。	★4	4-4-3 ログの取得
	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	★4	4-3-1 データの暗号化
		ネットワーク上を流れる情報を盗聴する。	★4	4-3-3 取引先との情報共有ルール
	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	★3	4-1-3 認証の強度・実装方法の決定 4-1-5 パスワード設定ルール
		ネットワーク上を流れる情報を改ざんする。	★4	4-3-3 取引先との情報共有ルール
	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。	★3	4-3-4 適切なバックアップ
			★4	7-1-1 事業継続要件に沿った復旧準備
	高負荷攻撃	DDoS 攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	-	DDoS 攻撃等に特有の対策事項は必ずしも求めている。
物理	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	★4	4-1-8 サーバ設置エリアへの入退室管理
	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVD や USB 機器等）を接続し、攻撃を実行する。	★4	4-1-9 可搬媒体の制限
	無線妨害	無線通信を妨害する。	-	無線通信の妨害に特有の対策事項は必ずしも求めている。
	窃盗	機器を窃盗する。	★4	2-1-5 機密情報の回収・破棄

★3 では、外部ネットワーク経由での論理的脅威を中心として、不正アクセス、不正送信、マルウェア感染、情報破壊に対して基礎的と考えられる対策を求めている。

他方、★4 においては、★3 で想定しているものに加え、ソーシャルエンジニアリング、否認、情報窃取、情報改ざん、情報破壊及び物理的侵入、不正媒体・機器接続等を含む物理的脅威に対する標準的と考えられる対策を求めている。

なお、表 3 で示した脅威のうち、★3・★4 のどちらにも対応する要求事項が存在しない脅威についても、自組織で扱う情報の重要性や自組織及び取引先等の業務の特性や業務への影響を考慮してその対応を検討することが推奨される。

第5章 要求事項・評価基準の解説

5.1 要求事項・評価基準全体で共通する事項の解説

5.1.1 「★3・★4 要求事項・評価基準」の構成

「★3・★4 要求事項・評価基準」は、以下に示す通り、7 の大分類の下、16 の中分類から構成され、★3 については計 26 件、★4 については計 43 件の要求事項からなる。

大分類及び中分類は、NIST Cybersecurity Framework (CSF) 2.0 における機能及びカテゴリに基づいたものとしているが、本制度が委託先等、サプライチェーン全体のセキュリティ対策の強化を目指すものである点を踏まえ、「取引先管理」を大分類として独立させた。別紙では、大分類、中分類に沿って、要求事項毎に解説を付す構成としている。

表 4 要求事項の構成

大分類	中分類	要求事項数	
		★3 計：26	★4 計：43
No.1 ガバナンスの整備	No.1-1 組織の状況	0	1
	No.1-2 役割、責任、権限	2	3
	No.1-3 ポリシー	1	1
	No.1-4 監督	0	1
No.2 取引先管理	No.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	3	5
No.3 リスクの特定	No.3-1 資産管理	4	5
	No.3-2 リスクアセスメント	0	1
No.4 攻撃等の防御	No.4-1 アイデンティティ管理、認証、アクセス制御	7	9
	No.4-2 意識向上とトレーニング	1	2
	No.4-3 データセキュリティ	1	4
	No.4-4 プラットフォームセキュリティ	3	5
	No.4-5 技術インフラのレジリエンス	1	1
No.5 攻撃等の検知	No.5-1 継続的監視	1	2
	No.5-2 有害事象の分析	0	1
No.6 インシデントへの対応	No.6-1 インシデント管理	1	1
No.7 インシデントからの復旧	No.7-1 インシデント復旧計画の実行	1	1

5.1.2 「★3・★4 要求事項・評価基準」におけるシステム・情報の分類

「★3・★4 要求事項・評価基準」では、適用範囲内のシステム及び登録希望組織が保有する情報について、いくつかの分類を設定し、追加の評価基準を課している場合がある。

登録希望組織は、自己評価等に先立って、自組織における「重要なシステム」や「事業継続上重要なシステム」、「重要な機密情報を取り扱うシステム」について、図 15 で示す分類を踏まえ自らが設定する基準に基づいて設定し、把握しておかねばならない。

図 15 中に示される「重要なシステム」等の定義は以下のとおりである。

- ・ 重要なシステム：侵害された場合のビジネスへの影響度が高いと登録希望組織が定め

たシステム²²

- ・ 事業継続上重要なシステム：高い可用性が求められる（稼働停止許容時間が短い）システムとして登録希望組織が定めたもの
- ・ 重要な機密情報を扱うシステム：「重要な機密情報」を取り扱うシステム
- ・ 機密情報：登録希望組織が保有している情報のうち、外部への開示が予定されない情報
- ・ 重要な機密情報：「機密情報」のうち、漏えいした場合における社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいと登録希望組織が定めたもの
- ・ 事業継続上重要な情報：登録希望組織が保有している情報のうち、利用不能や改ざんによる事業影響や重要業務の遂行への影響が大きいと登録希望組織が定めたもの

その際、システム・情報の分類基準を明確にするとともに、当該基準に基づいて分類した結果を確認できるよう整理しておくことが望ましい。

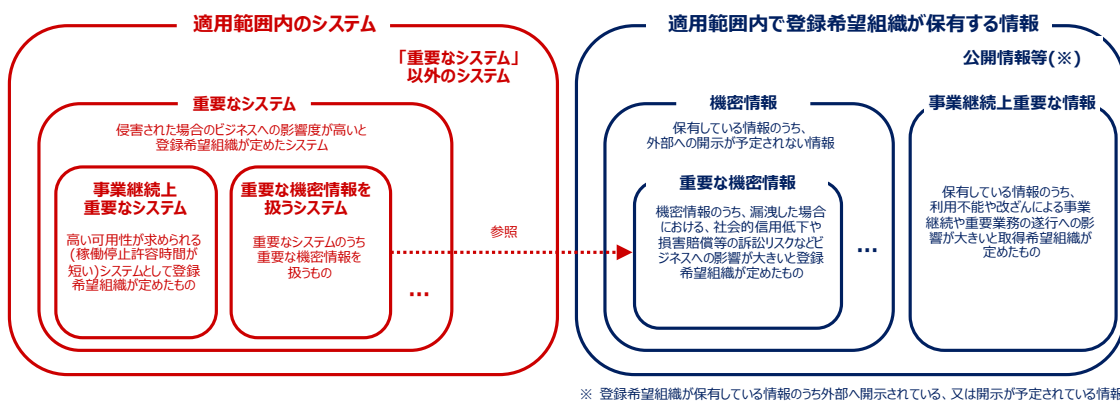


図 15 要求事項・評価基準におけるシステム・情報の分類

²² 「重要なシステム」には、「事業継続上重要なシステム」及び「重要な機密情報を扱うシステム」が含まれる。

別紙 要求事項・評価基準の個別解説

本別紙は、各要求事項・評価基準について対策の実施方法や解釈上留意が必要と考えられる箇所に対する解説を行うものであり、以下の内容から構成される。

【要求事項】

本制度において、登録希望組織が登録を受けるための条件として定めるセキュリティ要件を示す。「★3・★4 要求事項・評価基準」の要求事項の内容を転記している。

【評価基準】

本制度の要求事項について、自己評価又は第三者評価に際し、要求事項を満たしていると判断するための基準を示す。「★3・★4 要求事項・評価基準」の評価基準の内容を転記している。

【解説】

本別紙において新たに記述した項目であり、各要求事項・評価基準の内容の実施方法や解釈に迷うと考えられる箇所に対し、解説を記載する。

No.1 ガバナンスの整備

「ガバナンスの整備」は、組織のセキュリティ対応方針及びセキュリティ対策推進計画を確立、周知及びモニタリングすることを目的として実施するものであり、以下4つの中分類に分けられる。

別表1 「ガバナンスの整備」における中分類及びその目的

中分類	各分類の目的
組織の状況	組織のセキュリティに関連する法令、基準、制限事項及び要求事項を把握すること。
役割、責任、権限	セキュリティに関する役割、責任、権限を明確にし、組織的な対応体制を確立すること。
ポリシー	組織のセキュリティ対応方針を策定・周知し、実施すること。
監督	組織のセキュリティ対策の実施状況を把握し、対策の改善・推進につなげること。

No.1-1 組織の状況

(1)社内ルール[No.1-1-1]

【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。

【評価基準】

段階	No.	評価基準
★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
	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。
	1-1-1-3	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。

【解説】

評価基準 No. 1-1-1-1 関連

- 「自社に関連する法令」とは、どの範囲の法令を把握すればよい？
 - ・ 事業内容によって遵守すべき法令は異なるが、例えば代表的な国内の法令としては以下のものがある。
 - － 刑法、民法、会社法
 - － 不正競争防止法
 - － 個人情報保護法、マイナンバー法
 - － 不正アクセス禁止法
 - ・ 取得単位に海外子会社等を含む場合は、当該海外子会社等に適用される国・地域の法令についても把握し、これを踏まえて社内ルールを定めなければならない。
- 「社内ルール」(No.1-1-1-1)と「セキュリティ対応方針」(No.1-3-1-1)との関係は何か？
 - ・ 本評価基準でいう「社内ルール」とは、規程、指針、手順書その他これらに類する文書化されたルールの総称であり、「セキュリティ対応方針」もこれに含まれる。

- ・ その上で、No.1-1-1-1 及び No.1-3-1-1 の評価観点は異なり、No.1-1-1-1 は法令等を社内ルールへ反映するための取組を評価するものであるのに対し、No.1-3-1-1 は社内ルール的一种であるセキュリティ対応方針そのものの策定を評価するものである。

評価基準 No. 1-1-1-2 関連

■ 法令や基準等の改正状況を、どのように把握すればよいか？

- ・ 法令や基準等の改正状況については、各業界団体による情報発信やセミナーなどを利用することが考えられる。

評価基準 No. 1-1-1-3 関連

■ 「策定・見直した社内ルール」を、どのような方法で周知すればよいか？

- ・ 教育・周知の方法は、社内向けセミナー、社員等への注意喚起メール、社内 Web 掲示板への掲載などが考えられる。

No.1-2 役割、責任、権限

(1)セキュリティ推進活動部門[No.1-2-1]

【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。

【評価基準】

段階	No.	評価基準
★3	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。
	1-2-1-2	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。
	1-2-1-3	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。
★4	1-2-1-4	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。

【解説】

評価基準 No. 1-2-1-1 関連

■ 「セキュリティを統括する役員」とは、どのような者を指すか？

- 「セキュリティを統括する役員」とは、登録希望組織において、セキュリティ対応を統括する権限及び責任を有する者をいう。
- 例えば、適用範囲が法人全体である場合には取締役、執行役員又は CISO 等が、事業部門等である場合には事業部長等が該当することが考えられる。なお、会社法上の役員であることを必ずしも求めるものではない。
- サイバーセキュリティへの対応には、平時における人員・予算等の経営資源の配分や、有事におけるシステム又は事業の停止等の経営判断が伴うため、必要な権限及び責任を有する者が組織全体の取組を統括する必要がある。以下の資料が参考となる。
 - 経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0」
(https://www.meti.go.jp/policy/netsecurity/mng_guide.html)
 - 経済産業省「産業界へのメッセージ」
(<https://www.meti.go.jp/policy/netsecurity/message.html>)

■ 「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」として、どのような事項を規定することが考えられるか？

- 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・責任としては、組織構造等に応じて、例えば以下のような事項を規定することが考えられる。また、この中には、実質的な作業を外部委託するものの、その委託先管理を行うことを通じて役割を果たす場合も含む。
 - セキュリティを統括する役員の役割としては、例えば、セキュリティ対応方針の策定・見直しに関する指示、セキュリティ対応方針・予算・対策実施事項の承認等が考えられる。
 - セキュリティ担当部署の役割としては、例えば、セキュリティ教育・普及啓発、セキュリティリスクアセスメントの実施、セキュリティ対応方針及び関連するガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング等が考えられる。

- セキュリティを統括する役員、セキュリティ担当部署の役割を明確化するに当たっては、当該役割ごとに求められるタスク・スキル・知識を整理することが有効であり、その検討に当たっては、内閣官房国家サイバー統括室（NCO）「サイバーセキュリティ人材フレームワーク」及びフレームワークを実務で活用するための指針である各種手引き書（<https://www.cyber.go.jp/council/csjinzai/index.html>）を活用することが考えられる。

なお、各役割に対する責任の割当てについては、組織の指揮命令系統や意思決定権限等を踏まえ、自社の実態に応じて定めることが適当と考えられる。その際、中小企業等においては「小規模組織向け手引き書 2026」、大企業等においては「大規模組織向け手引き書 2026」を参考に取組を進めることが考えられる。

■ 「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・責任」を、どのような文書へ規定することが考えられるか？

- ・ 情報セキュリティ関連規程に記載することが考えられる。
- ・ 情報セキュリティ体制図を作成することも有効である。

評価基準 No. 1-2-1-2 関連

■ 「平時のセキュリティ推進活動に必要な役員」とは、どのような者を指すか？

- ・ 「平時のセキュリティ推進活動に必要な役員」とは、登録希望組織において、平時のセキュリティ推進活動を統括し、必要な意思決定を行う者をいう。
- ・ 例えば、適用範囲が法人全体である場合には取締役、執行役員又は CISO 等が、事業部門等である場合には事業部長等が該当することが考えられる。なお、会社法上の役員であることを必ずしも求めるものではない。

■ 「連絡先リスト」を整備する際に必要な観点は何か？

- ・ 連絡先リストを整備する上で必要な観点は、必要な連絡先が網羅されていること、連絡先リストが実際に機能することの 2 点である。

<必要な連絡先が網羅されていることの確認>

- 平時の際に必要な連絡先を漏れなく連絡先リストに登録するために、以下のポイントを踏まえて確認することが考えられる。
 - 社内からの情報セキュリティに関するルール等についての問い合わせを受ける窓口を明確にする
 - セキュリティ担当部署からの社内向け周知事項、依頼事項を連絡する際のルートを目的・対象範囲別に整理する
 - セキュリティ責任者や、システム管理者の連絡先を明確にする
- また、メール・チャット・電話といった連絡手段は、連絡先ごとに想定しうる用途に応じて確実に連絡できるよう、適した連絡手段をそれぞれ確保しておくことが望ましい。その際、メールやチャットといったネットワークサービスが使用できないことも想定しておくことは有効である。

<連絡先リストが実際に機能することの確認>

- 連絡先リストを基に、実際に連絡を取ることができる状態に保つことが重要である。そのため、定期的に連絡先の最新化を行い、実際に連絡可能であることを確認するといった運用ルールを設けることが望ましい。

評価基準 No. 1-2-1-4 関連

■ 経営層が関与する情報セキュリティの意思決定体制は、どのように構築すればよいか？

- ・ セキュリティ対策の推進においては、横断的な事項を審議する必要があるため、例えば、情報セキュリティを推進する CISO・セキュリティ担当部署及び各部門の代表者から構成される委員会を設置することが考えられる。
- ・ 当該委員会は、各部門間の意見調整を図りセキュリティ対策と組織の方針を整合的なものとする機能を持つことから、組織全体としての方向付けを要するセキュリティ対

応方針（1-3-1-1 参照）及び対策推進計画（1-4-1-1 参照）を審議事項としなければならない。

- ・ 情報セキュリティ委員会のような特別な体制でなくても、例えば経営会議の議題として取り上げることを定めて行うという方法も考えられる。
- ・ 小規模な組織においては、情報セキュリティに関する専用の委員会等を設置することまでは求められず、経営者等の経営判断を行う者が、既存の会議や定例的な打合せ等の場でセキュリティ対応方針や対策推進計画について審議・判断する体制とすることも考えられる。

(2)サイバー攻撃の監視・分析体制[No.1-2-2]

【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。

【評価基準】

段階	No.	評価基準
★4	1-2-2-1	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活用する体制を整備すること。
	1-2-2-2	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。

【解説】

評価基準 No. 1-2-2-1 関連

- 脆弱性情報やサイバー攻撃動向の把握にあたり、どのような公開情報の活用が考えられるか？
 - ・ 脆弱性情報やサイバー攻撃動向の把握に当たっては様々な情報源の活用が考えられるが、例えば、以下のような国内外の公的機関やセキュリティベンダー等が公開する情報を参照することが考えられる。
 - IPA：重要なセキュリティ情報
(<https://www.ipa.go.jp/security/security-alert/>)
 - IPA：サイバーセキュリティ注意喚起サービス「icat for JSON」
(<https://www.ipa.go.jp/security/vuln/icat.html>)
 - JVN：Japan Vulnerability Notes
(<https://jvn.jp/>)
 - JVN iPedia：脆弱性対策情報データベース
(<https://jvndb.jvn.jp/>)
 - JPCERT/CC：注意喚起
(<https://www.jpcert.or.jp/at/2026.html>)
 - CISA：KEV Catalog
(<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>)
 - NIST：NVD
(<https://nvd.nist.gov/>)
- 公開情報以外に、どのような手段でサイバー攻撃や脆弱性に関する情報を収集することが考えられるか？
 - ・ 公開情報以外では、例えば、利用している製品・サービスのベンダーから契約者・利用者等に限定して通知される脆弱性情報やサイバー攻撃に関する情報、業界団体等において会員等に限定して共有される情報、政府機関等から共有される情報を利用することが考えられる。
- 入手した情報を自組織で活用するために、どのような方法が考えられるか？
 - ・ 入手した脆弱性情報等が自社に影響するかどうかを判断するため、No.3-1-1 及び No.3-1-2 で把握した自社の情報機器、ソフトウェア、ネットワーク機器等の情報と照合し、影響の有無を確認することが考えられる。なお、インターネット上に公開されている自社の IT 資産を把握する方法については、No.3-1-2-2 関連の解説も参照されたい。
 - ・ 脆弱性対策情報共有フレームワーク（MyJVN）を活用し、脆弱性対策情報を効率的に収集することができる（脆弱性対策情報収集ツール（mjcheck）、MyJVN API）。
 - JVN iPedia：脆弱性対策情報共有フレームワーク（MyJVN）
(<https://jvndb.jvn.jp/apis/myjvn/>)

評価基準 No. 1-2-2-2 関連

■ 「サイバー攻撃の予兆検知及びインシデントの発生の検知を可能」とするための体制は、どのように整備すればよいか？

- ・ 体制を自組織で整備する方法と、外部委託を活用する方法が考えられる。
- ・ 自組織で整備する場合には、例えば、脆弱性情報やサイバー攻撃動向に関する情報を定期的に収集するとともに、社内外ネットワークの境界部分に設置された機器等のログを確認し、異常の有無を監視する担当者及び対応手順を定めることが考えられる。
- ・ 外部委託の場合、中小企業向けセキュリティ対策に不可欠なサービスをワンパッケージで提供している以下のようなサービスを活用することが考えられる。
 - － IPA：サイバーセキュリティお助け隊サービス
(<https://www.ipa.go.jp/security/otasuketai-pr/>)
 - ・ 入手した情報や社内外ネットワークの境界部分に設置された機器等のログについて、例えば UTM 等を活用して分析・監視を行う体制を整備することが考えられる。また、複数の機器等から取得したログを組み合わせて分析する場合には、SIEM (Security Information and Event Management) 等を活用して相関分析を行うことも有効である。
 - ・ 脆弱性対処やインシデント対応を円滑に実施するための方針・体制については以下の資料も参考になる。
 - － IPA：製品利用者ガイド
([https://www.ipa.go.jp/security/guide/vuln/rcu1hd000000a5en-att/guide for usr.pdf](https://www.ipa.go.jp/security/guide/vuln/rcu1hd000000a5en-att/guide%20for%20usr.pdf))

■ インシデントの予兆検知のために、どのような分析手法を用いることが考えられるか？

- ・ 分析手法の一つとして相関分析がある。これは、複合的なログなどを分析してセキュリティインシデントの予兆や痕跡を見つけ出す手法で、以下の資料が参考になる。
- － IPA「産業用制御システム向け侵入検知製品等の導入手引書」では、産業用制御システムを対象として、ログ分析や相関分析による侵入検知の考え方を解説している。本制度において制御システムは対象外であるが、相関分析の考え方を理解する上で参考になる。
(<https://www.ipa.go.jp/security/controlsystem/ps6vr7000001o2b1-att/icsidshandbook.pdf>)

(3)守秘義務のルール[No.1-2-3]**【要求事項】**

守秘義務のルールを策定し、遵守させること。

【評価基準】

段階	No.	評価基準
★3	1-2-3-1	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。
	1-2-3-2	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。
★4	1-2-3-3	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。）
	1-2-3-4	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。

【解説】評価基準 No. 1-2-3-1 関連

■ 守秘義務の対象者ごとに、どのようにルールを整理することが考えられるか？

- ・ 役員、従業員については、就業規則などに記載することが考えられる。また、退職時の規程として定めることや、機密情報の持ち出しがないことについて誓約書を提出してもらうなどの措置が考えられる。
- ・ 派遣社員及び受入出向者については、情報セキュリティ関連規程等の中に、派遣元又は出向元との契約に守秘義務を定める旨を規定することが考えられる。

■ 守秘義務のルールを定める際に、参考となる資料はあるか？

- ・ 守秘義務のルールを定める際には、例えば以下の資料が参考になる。
 - － 経済産業省「秘密情報の保護ハンドブック」の参考資料 2「各種契約書等の参考例」では、「第 1 秘密情報管理に関する就業規則（抄）の例」及び「第 2 情報管理規程の例」が紹介されており、役員及び従業員に対する守秘義務や情報管理に関するルールを定める際の参考となる。

(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf>)

評価基準 No. 1-2-3-2 関連

■ 入社時や社外要員の受入れ時において、守秘義務のルールはどのように説明すればよいのか？

- ・ 入社時や受け入れ時に対面で説明する、もしくは教育資料を作成して学習させるなどの方法が考えられる。

評価基準 No. 1-2-3-3 関連

■ 守秘義務の誓約書を作成する際に、参考となる資料はあるか？

- ・ 守秘義務の誓約書を作成する際には、例えば以下の資料が参考になる。
 - － 経済産業省「秘密情報の保護ハンドブック」の参考資料 2「各種契約書等の参考例」では、「第 3 秘密保持誓約書の例」として、従業員等の入社時、プロジェクト参加時及び退職時等に取得する誓約書の記載例が紹介されている。

(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf>)

■ 除外されている「社外要員」とは誰を指すか？

- ・ 評価基準 1-2-3-4 における「派遣社員及び受入出向者」を指す。

評価基準 No. 1-2-3-4 関連

- 派遣元又は出向元との守秘義務に関する契約を締結する際に、参考となる資料はあるか？
 - ・ 派遣元又は出向元との守秘義務に関する契約を締結する際には、例えば以下の資料が参考になる。
 - － 経済産業省「秘密情報の保護ハンドブック」の参考資料 2「各種契約書等の参考例」では、「第 4 業務提携の検討における秘密保持契約書の例」、「第 5 取引基本契約書（製造請負契約）（抄）の例」及び「第 6 業務委託契約書（抄）の例」が紹介されており、取引先等との契約において守秘義務を定める際の参考となる。
(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf>)

No.1-3 ポリシー

(1)セキュリティ対応方針の策定[No.1-3-1]

【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。

【評価基準】

段階	No.	評価基準
★3	1-3-1-1	自社のセキュリティ対応方針を定めること。
	1-3-1-2	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。
	1-3-1-3	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。
★4	1-3-1-4	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。

【解説】

評価基準 No. 1-3-1-1 関連

- 「セキュリティ対応方針」には、最低限どのような事項を規定する必要があるか？
 - ・ セキュリティ対応方針では、少なくとも以下の事項を規定することが考えられる。
 - ・ 経営者が自社のセキュリティに責任を負うこと
 - ・ 社内体制を整備すること
 - ・ 従業員のセキュリティ意識向上のための取組をすること
 - ・ 法令及び契約上の要求事項を遵守すること
 - ・ セキュリティ対策の継続的な改善を行うこと
 - ・ 違反及び事故への対応を定めること。
- 「セキュリティ対応方針」を策定する際に、参考となる資料はあるか？
 - ・ セキュリティ対応方針を策定する際は、以下の資料が参考になる。
 - － JNSA：情報セキュリティポリシーサンプル改版（1.0 版）
<https://www.jnsa.org/result/2016/policy/index.html>
 - － IPA：中小企業の情報セキュリティ対策ガイドライン第 4.0 版「情報セキュリティ基本方針（サンプル）」
<https://www.ipa.go.jp/security/guide/sme/about.html>

評価基準 No. 1-3-1-2 関連

- 「セキュリティ対応方針」を定常的に参照可能とするためには、どのような手段が考えられるか？
 - ・ 例えば、役員、従業員、社外要員（派遣社員等）が常時閲覧できる社内ポータルサイト上に開示することが考えられる。

評価基準 No. 1-3-1-3 関連

- 「セキュリティ対応方針」を改正した場合、どのように周知すればよいのか？
 - ・ 例えば、役員、従業員、社外要員（派遣社員等）が常時閲覧できる社内ポータルサイト上で告知する方法や社内メール等で一斉に告知する方法が考えられる。
 - ・ 加えて、セキュリティ対応方針の改正時に冊子又は電子ファイルの形式で改正版を配布し、内容を説明する会を設けることも考えられる。

評価基準 No. 1-3-1-4 関連

■ セキュリティ対応方針の内容は、どのように点検すればよいか？

- ・ セキュリティ対応方針について、組織やセキュリティを取り巻く状況の変化等を踏まえ、内容が引き続き適切であるかを年 1 回以上の頻度で点検し、必要に応じて見直すことが考えられる。
- ・ 点検を継続的かつ確実に実施するため、点検の実施方法、実施時期、担当者等を規程やルールとして定めておくことも有効である。

No.1-4 監督

(1)セキュリティ対策推進計画[No.1-4-1]

【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。

【評価基準】

段階	No.	評価基準
★4	1-4-1-1	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
	1-4-1-2	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。

【解説】

評価基準 No. 1-4-1-1 関連

- 「対策推進計画」とは、どのような目的で定められ、何を記載することが考えられるか？
 - ・ 対策推進計画は、セキュリティ対策に関する一連の取組を対象とした全体計画であり、セキュリティ対策を組織的・継続的に改善し、総合的に推進するために、セキュリティ対策に関する取組の全体方針のほか、対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を記載することが考えられる。
 - ・ セキュリティ対策推進計画の策定に当たっては、政府機関向けではあるが、以下の資料を参考にすることが考えられる。
 - － NCO：政府機関等の対策基準策定のためのガイドライン（令和7年度版）
【基本対策事項】2.1.3(4)-1,2
(<https://www.cyber.go.jp/policy/group/general/kijun.html>)
- 年1回以上の点検結果を踏まえた「セキュリティ対策の実態」及び「今後の対策推進計画」は、どのような場で報告・承認を得ればよい？
 - ・ セキュリティ対策の実態を報告する場としては、No.1-2-1-4に記載の情報セキュリティ委員会等が考えられる。

評価基準 No. 1-4-1-2 関連

- 「役員からの改善に向けた指示があった場合」の対応を実施するにあたり、どのような留意点が考えられるか？
 - ・ 計画の変更や不備の是正においては、セキュリティ担当部署のみならず複数の部門が影響を受ける場合が想定される。そのため、指示内容の文書化や関係部門への共有として、改善計画書の作成指示・共有といった方法が考えられる。

No.2 取引先管理

「取引先管理」は、組織が取引先に係るセキュリティリスク及び管理プロセスを識別、管理、モニタリング及び改善することを目的として実施するものであり、以下1つの中分類から構成される。

別表2 「取引先管理」における中分類及びその目的

中分類	各分類の目的
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	組織が取引先に係るセキュリティリスク及び管理プロセスを識別、管理、モニタリング及び改善すること。

No.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

(1)取引先とのビジネス又はシステム上の関係[No.2-1-1]

【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。

【評価基準】

段階	No.	評価基準
★3	2-1-1-1	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すること。
	2-1-1-2	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。
★4	2-1-1-3	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

【解説】

評価基準 No. 2-1-1-1 関連

- 「自社以外の組織が管理・提供し、自社資産が接続しているシステムを把握する」ために、どのような仕組みが考えられるか？
 - ・ 例えば、以下項目を含む一覧を整備することが考えられる。
 - <利用者に関する管理項目>
 - － 利用者名、部署
 - － 用途
 - <外部情報システムに関する管理項目>
 - － システム概要、システム名
 - － ベンダー名、クラウドサービス名
 - － API 等による外部情報サービスとの接続の有無
 - <契約に関する管理項目>
 - － 契約書名、契約先名
 - － 利用開始日、利用終了予定日
 - <連絡先に関する管理項目>
 - － インシデント発生時の連絡先
 - ・ 「自社資産が接続している外部システム」としては、組織の承認を得ずに従業員や利用部門が独自に導入・利用するシャドーITの把握も重要であるところ、組織の状況に応じて、プロキシ等の通信ログや、利用中のクラウドサービスを可視化し、アクセス

制御やデータ保護等を行う CASB (Cloud Access Security Broker) を活用することが考えられる。

- ・ 「自社資産が接続している外部システム」には、API 等を利用して自社のシステム、アプリケーション又はサービスから接続する外部情報サービスも含まれる。これらについては、接続先、利用目的、認証方式及び API キー等の認証情報の管理状況を把握することが望ましい。

評価基準 No. 2-1-1-3 関連

- 「機密情報を共有している子会社又は取引先」について、すべてを対象として把握する必要はあるか？
 - ・ 必ずしもすべての取引先を対象とする必要はなく、No.2-1-1-3 の対象となるのは、自社の機密情報を共有している子会社又は取引先である。
 - ・ 対象となる子会社又は取引先について把握・整理を進めるに当たっては、セキュリティ事故発生時に、事業継続 (BCP) の観点から速やかに復旧を目指すことを目的とし、重要な情報資産を共有する子会社又は取引先や、その他セキュリティリスクの危険性が高い子会社又は取引先を優先的に把握・整理することが望ましい。
- 「会社ごとに取り交わす手段 (受発注、情報のやり取り等)」として、どのようなものが考えられるか？
 - ・ 情報資産を取り交わす手段については、例えば、メール、クラウドストレージ、企業間電子データ交換、その他物理メディア (USB メモリ、CD、DVD 等) の受け渡しといった方法が考えられる。
- 「取引に伴い授受・使用される情報資産やその取扱い」を把握するために、どのような仕組みが考えられるか？
 - ・ 例えば、契約書や仕様書に盛り込む、覚書を締結するほか、取引先管理台帳、受発注システム、契約管理システム等に必要な情報を整理する方法が考えられる。

(2)機密情報の取扱い[No.2-1-2]**【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。

【評価基準】

段階	No.	評価基準
★3	2-1-2-1	自社の機密情報を共有する子会社又は取引先との間で、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

【解説】評価基準 No. 2-1-2-1 関連

- **機密情報の取扱いについて、どのような方法で取り決めることが考えられるか？**
 - ・ 業務開始前に機密情報の取扱いについて、以下の方法で取引先と取り交わしを行うことが考えられる。
 - 仕様書に明記する
 - 契約書に明記する
 - 取引先と、秘密保持契約（NDA）を締結する

- **「機密情報の返還又は廃棄」について、どのような事項を取り決めることが考えられるか？**
 - ・ 契約終了時その他機密情報を取り扱う必要がなくなった場合に備え、返還又は廃棄の対象、実施時期及び方法について、あらかじめ取り決めておくことが考えられる。
 - ・ 返還又は廃棄の対象については、例えば、提供した文書、電子データ、記憶媒体等を明確にしておくことが考えられる。
 - ・ 返還又は廃棄の対象外とする情報がある場合には、対象となる情報及びその取扱いについてあらかじめ合意しておくことが考えられる。

(3)取引先のセキュリティ対策状況[No.2-1-3]**【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。

【評価基準】

段階	No.	評価基準
★4	2-1-3-1	以下に示す条件のいずれか若しくは複数の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

【解説】**評価基準 No. 2-1-3-1 関連****■ 「内部システムへのアクセス」とは、どのような場合を指すか？**

- ・ 例えば、子会社又は取引先の環境から、VPN、専用線、リモートアクセス等を通じて、自社の社内ネットワーク又は一般に公開していない業務システムに接続できる場合が考えられる。

■ セキュリティ対策状況は、どのような方法で把握することが考えられるか？

- ・ セキュリティ対策状況の把握方法は、対象となる子会社又は取引先の特性や、自社に及ぼす影響の大きさ等を踏まえて選択することが考えられる。
- ・ 例えば、本制度における★の取得状況を確認する方法や、セキュリティ対策チェックシートを用いて必要な対策の実施状況を確認する方法が考えられる。
- ・ また、自社に及ぼす影響が大きい子会社又は取引先については、必要に応じて訪問し、対策状況を点検することも考えられる。
- ・ これらの方法は、確認する内容や対象先の状況に応じて、組み合わせて実施することも考えられる。

(4)セキュリティインシデント発生時の役割・責任[No.2-1-4]

【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。

【評価基準】

段階	No.	評価基準
★3	2-1-4-1	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ること。

【解説】

評価基準 No. 2-1-4-1 関連

- セキュリティインシデント発生時の「役割及び責任」として、どのような事項を定めることが考えられるか？
 - ・ 例えば、インシデント発生時の連絡、調査、封じ込め、復旧等について、自社と子会社又は取引先のどちらが主体となって対応するか、相手方がどのような報告・協力を行うか等を定めることが考えられる。
 - ・ これらの役割及び責任は、契約書その他の合意文書等で明確にすることが考えられる。

(5)機密情報の回収・破棄[No.2-1-5]**【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。

【評価基準】

段階	No.	評価基準
★4	2-1-5-1	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。

【解説】**評価基準 No. 2-1-5-1 関連**

- 機密情報やアクセス権の回収・破棄を確実に実施するためには、どのような手順を整備しておくことが考えられるか？
 - ・ 機密情報やアクセス権などを提供・共有する際に、あらかじめ台帳で管理しておくことが考えられる。これにより、回収・破棄対象を漏れなく把握しやすくなる。
 - ・ 回収又は破棄すべき機密情報、アクセス権等のチェックシート等を作成する際、回収又は破棄の手順も定めておくことが考えられる。
- 契約終了時に機密情報及びアクセス権の回収・破棄状況を確認するためのチェックシート等には、どのような項目を記載することが考えられるか？
 - ・ チェックシート等には、例えば以下の項目を記載することが考えられる。
 - － 基本的な情報（取引先・子会社名及び契約又は取引に関連する部署名、どの契約/プロジェクトに関する機密情報、アクセス権等か）
 - － 回収又は破棄すべき機密情報の一覧
 - 提供した文書、電子データ（メールを含む）、その他（試作品等）
 - 機密情報の保存場所
 - － 契約終了時に削除又は無効化すべきアクセス権の一覧
 - システムログイン ID 及びパスワード
 - ネットワークアクセス（VPN、イントラネットなど）
 - － 回収・破棄の実施日を記入するなど、回収・破棄済かを確認するためのチェック項目
 - － 必要に応じて証拠（例：証明書、ログファイル）の有無を記載する欄
- 契約終了時に、機密情報の返還又は廃棄を行わなくてもよい場合はあるか？
 - ・ No.2-1-2-1 に基づく取決めにおいて、返還又は廃棄の対象外とすることをあらかじめ合意している機密情報については、その限りではない。

No.3 リスクの特定

「リスクの特定」は、組織の現在のサイバーセキュリティリスクを理解することを目的として実施するものであり、以下 2 つの中分類に分けられる。

別表 3 「リスクの特定」における中分類及びその目的

中分類	各分類の目的
資産管理	組織の資産（データ、ハードウェア、ソフトウェア、システム、施設、サービス、人材を含む）を特定し、組織の目的及びリスク戦略に対する重要性に応じて管理すること。
リスクアセスメント	組織が、組織、資産、及び個人に対するセキュリティリスクを理解すること。

No.3-1 資産管理

(1)情報機器、OS 及びソフトウェアに関する情報の把握[No.3-1-1]

【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。

【評価基準】

段階	No.	評価基準
★3	3-1-1-1	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ための仕組みを整備すること。
	3-1-1-2	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。
	3-1-1-3	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。
	3-1-1-4	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。
★4	3-1-1-5	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。
	3-1-1-6	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。
	3-1-1-7	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。

【解説】

評価基準 No. 3-1-1-1、3-1-1-2、3-1-1-5 関連

■ 情報機器、OS 及びソフトウェアに関する情報を把握するために、どのような仕組みの整備が考えられるか？

- ・ IT 資産管理ツールの利用や情報システム台帳の整備等を実施することが考えられる。

■ どのような項目の管理が考えられるか？

- ・ 評価基準に定めのある項目以外にも含め、例として下記の事項を一覧で管理することが考えられる。
 - － 機器情報（ハードウェア機器・ホスト名、製造元）
 - － ソフトウェア情報（OS・ソフトウェア名称、バージョン情報）
 - － ネットワーク情報（MAC アドレス、IP アドレス）
 - － 設置場所（オフィス/データセンター/クラウド等）
 - － 使用者（部署名、氏名、連絡先）

- 管理者（部署名、氏名、連絡先）
- サポート窓口の連絡先（社内又は社外のサポート窓口担当者）

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
- 中小企業の情報セキュリティ対策ガイドライン第 4.0 版（IPA）
<https://www.ipa.go.jp/security/guide/sme/about.html>

評価基準 No. 3-1-1-3 関連

■ 「管理ルール」で考慮すべき事項としてどのようなものが考えられるか？

- ・ 情報機器、OS 及びソフトウェアの導入について、提供元の信頼性、サポート方針・期限などを考慮することが考えられる。
- ・ セキュリティパッチ適用のルールについて、要求事項 4-4-1、4-4-2 及び 4-4-4 を参照の上、策定することが考えられる。

評価基準 No. 3-1-1-6 関連

■ 重要なシステムを構成する情報機器について、どのような「設定情報」を把握することが考えられるか？

- ・ 例えば、サーバ機器については、以下のような設定情報が考えられる。
 - 認証設定（パスワードポリシー、多要素認証など）
 - ユーザ設定（管理者 ID のアカウント、ローカルアカウントなど）
 - アクセス制御設定（リモートアクセス（SSH、RDP など））
 - 監視設定（アラート条件、SNMP 設定）
- ・ 上記に加え、ネットワーク機器については、ルーティング設定、VLAN 設定、アドレス変換（NAT）設定などの通信制御設定の把握が考えられる。

■ 重要なシステムを構成する情報機器の「設定情報」を把握するために、どのような仕組みを整備することが考えられるか？

- ・ IT 資産管理ツールの利用や設定管理ツールの整備などを実施することが考えられる。

(2)ネットワークに関する情報の把握[No.3-1-2]**【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。

【評価基準】

段階	No.	評価基準
★3	3-1-2-1	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。
	3-1-2-2	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。
★4	3-1-2-3	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。
	3-1-2-4	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。

【解説】評価基準 No. 3-1-2-1 関連■ **どのような仕組みの整備が考えられるか？**

- ・ ネットワークの一覧にあたる文書を整備し、所在地及び用途が確認できるよう管理することが考えられる。

評価基準 No. 3-1-2-2 関連■ **どのような仕組みの整備が考えられるか？**

- ・ IT 資産管理ツールの利用や情報システム台帳の整備などを実施することが考えられる。機器の提供元から、サポート期間が明確に提示されていない場合は、最新のファームウェアのリリース日を記録しておくことも考えられる。このほか、自社で把握できていない IT 資産がインターネット上に公開されている可能性を考慮し、インターネット上に公開されている自社の IT 資産を発見・把握する ASM (Attack Surface Management) ツールにより、台帳に記載のない機器の有無を確認することも考えられる。

評価基準 No. 3-1-2-3 関連■ **どのような観点でネットワーク図を作成することが考えられるか？**

- ・ 例えば、以下の観点で作成することが考えられる
 - － 主要なネットワークセグメント間及び取引先や委託先との接続関係や、インターネットやクラウドとの境界点が把握できること。
 - － 脆弱性が発見された際に影響範囲を特定できること。
 - － 通信を制御する機器（例：ファイアウォール、プロキシサーバ）や、攻撃を検知・防御する機器（例：IPS、IDS）が、ネットワーク上どのように接続されているかが把握できること。
- ・ 本制度の対応に当たっては、適用範囲とそれ以外の境界及び当該境界におけるネットワーク保護施策が識別できるように図を作成することが望ましい。

■ **参考となる資料はあるか？**

- ・ 以下の資料が参考となる。
 - － 制御システムのセキュリティリスク分析ガイド 第2版（IPA）3.2 及び 3.3
<https://www.ipa.go.jp/security/controlsystem/ug65p900000019bkg-att/begoj90000000hpm8.pdf>
 ※同ガイドは制御システムを前提としているため、そのまま参考にできるものでは

ないが、ネットワークセグメント間の接続関係、外部との境界、通信を制御する機器や攻撃を検知・防御する機器の配置等を可視化する観点については、本評価基準におけるネットワーク図の作成に当たって参考とすることができる。

(3)外部情報サービスの管理[No.3-1-3]**【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。

【評価基準】

段階	No.	評価基準
★3	3-1-3-1	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、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。
	3-1-3-2	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。

【解説】**評価基準 No. 3-1-3-1 関連**■ **外部情報サービスとはどのようなものが対象か？**

- 外部情報サービスとは、自社の外部（社外）にあるインターネット経由のサービスやクラウド、Web サイトなどを通じて提供される情報サービスのことである。例えば、以下のサービスが考えられる。
 - － ホスティングサービス
 - － インターネット接続サービス
 - － クラウドサービス（IaaS、PaaS、SaaS、Web 会議サービス等）
 - － 生成 AI サービス
 - － 取引先等から提供される情報サービス

■ **どのような観点でセキュリティ要件を定めることが考えられるか？**

- 例えば、以下の観点から定めることが考えられる。
 - － サービス事業者の情報セキュリティ方針と自社のセキュリティ方針の適合
 - － サービスの稼働率や障害発生頻度等の信頼性
 - － セキュリティ対策水準や機能の有無
 - － データ保存先や保存期間の確認
- 「セキュリティ対策や機能の有無」の確認に当たっては、要求事項・評価基準のうち外部情報サービスが具備すべき事項への適合状況を確認することが考えられる。当該確認は、セキュリティ対策に係る認証の取得有無の確認、SOC2（SOC for Service Organizations: Trust Services Criteria）報告書の確認等により行うことも考えられる。

※SOC2 報告書とは、サービス事業者がデータ保護等の内部統制を適切に整備・運用しているかを外部監査人が評価し、発行する報告書である。

- なお、機密情報の取扱いに関する要件は、評価基準 2-1-2-1 において、情報共有先となるサービス事業者との間で明確化する。

■ **どのような方法で要件を満たしている旨の確認を行うことが考えられるか？**

- 外部情報サービス利用時の利用申請・承認手続を定めることが考えられる。申請に含める情報として、例えば以下の項目が考えられる。
 - － 外部情報サービス（クラウドサービスを含む）の名称
 - － 外部情報サービス（クラウドサービスを含む）の提供者の名称
 - － 利用目的（業務内容）
 - － 取り扱う情報の機密区分
 - － 利用期間
 - － 利用申請者（所属・氏名）、利用者の範囲（社員に限る、〇〇関係者に限るなど）
 - － 選定時のセキュリティ対策確認結果

- ・ 機密情報を扱うクラウドサービスを利用する際には、ISMAP 登録サービスを利用することも有効である

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － 中小企業の情報セキュリティ対策ガイドライン第 4.0 版 (IPA)
(https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf)
 - － 中小企業の情報セキュリティ対策ガイドライン第 4.0 版 付録 7 中小企業のためのクラウドサービス安全利用の手引き (IPA)
(https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_7.pdf)
 - － ISMAP－政府情報システムのためのセキュリティ評価制度
(https://www.ismap.go.jp/csm?id=csm_ismap_index)

評価基準 No. 3-1-3-2 関連

■ どのような合意を取り交わすことが考えられるか？

- ・ 取引開始時に、秘密保持の対象となる情報をできる限り明確化した秘密保持契約等を締結することが考えられる。
- ・ 対象となる情報について、双方協議の上、秘密保持の対象情報を別紙としてリスト化し、リストは常に最新の状態を保つよう更新することが考えられる。
- ・ なお、クラウドサービスの利用など、個々に提供元と合意文書の取り交わしができない場合は、合意の取り交わしではなく、外部情報サービス提供者の開示している要件・利用規約やサービス提供条件に沿ってリスクを確認することが考えられる

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － 秘密情報の保護ハンドブック (経済産業省)
第 3 章 3-4 (3) ④ a 「取引先に対する秘密保持義務条項」
(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>)

(4)機密区分に応じた情報の管理[No.3-1-4]**【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。

【評価基準】

段階	No.	評価基準
★3	3-1-4-1	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
	3-1-4-2	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。
	3-1-4-3	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。
★4	3-1-4-4	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。
	3-1-4-5	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。
	3-1-4-6	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。
	3-1-4-7	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
	3-1-4-8	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。

【解説】**評価基準 No. 3-1-4-1 関連****■ どのような文書に記載することが考えられるか？**

- ・ 情報資産管理規程・手順、情報取扱規程・手順、取扱エリアの対策基準・利用手順等に記載することが考えられる。

■ どのような機密区分を設定することが考えられるか？

- ・ 例えば、以下のように設定することが考えられる。
 - 極秘情報：インサイダー関連情報など極めて厳密な管理が必要で、漏えいすると企業の信頼が損なわれる情報
 - 機密情報：経営戦略、未公開の財務データ、顧客の個人情報、研究開発データなど社内であってもアクセス制限が必要な情報
 - 社外秘情報：社内での共有を前提とした情報で、外部への公開が制限される業務情報
 - 公開情報：Web サイトやパンフレットなど、一般に公開しても問題ない情報

■ 取扱エリアとはどのようなものか？

- ・ 設定した機密区分に応じて、建物や部屋などの物理的な場所に対して設定するものである。取扱エリアごとに立入制限、入退室管理方法、監視方法等の管理措置を定め、不正な立入りによる機密情報へのアクセスを防止する。例えば、以下のように設定することが考えられる。
 - － 機密エリア：極秘情報を扱うエリアとして、入場可能な者を特定の個人に限定する
 - － 業務エリア：社外秘情報を扱うエリアとして、入場可能な者を従業員に限定する
 - － 一般エリア：社外の来訪者や委託事業者を含め、入場可能なエリア

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － 中小企業の情報セキュリティ対策ガイドライン第 4.0 版（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf

評価基準 No. 3-1-4-3 関連

■ どのような仕組みの整備が考えられるか？

- ・ 情報資産台帳、情報資産一覧、資産目録等を作成するとともに、内容の更新に関するルールを定めて情報を最新化することが考えられる。

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － 中小企業の情報セキュリティ対策ガイドライン第 4.0 版 付録 6 資産管理台帳（サンプル）（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_6.xlsx

評価基準 No. 3-1-4-5 関連

■ どのような仕組みの整備が考えられるか？

- ・ 退職時の手引等の文書を作成し、記載に基づき役員、従業員の退職時、契約終了時その他情報を取り扱う必要がなくなった時に情報（印刷物、記憶媒体）、情報機器（パソコン、スマートデバイス）、アクセス権（ID、鍵）等を回収することが考えられる。
- ・ 回収漏れを起こさないために、回収物一覧のチェックシートには対象者のサインを求めることも有効である。

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

- ・ 含まない。ただし、本項目の目的である「機密漏えいを防止」の観点からみると、情報機器回収の代替策を実施することが望ましい。（以下例示）
- ・ 端末に業務データを保存できない仕組みとする（シンククライアントなど）
- ・ 端末利用終了時に業務データや業務アプリ・ツールを削除する運用ルールを定め、事前に従業員との間で誓約書を作成する

評価基準 No. 3-1-4-7、3-1-4-8 関連

■ どのような取組の実施が考えられるか？

- ・ 文書整備としては、情報取扱規程・手順等に抹消処理に関する事項を記載することが考えられる。
- ・ 具体的な抹消処理の実施方法としては、廃棄対象物により、記憶媒体を物理的に破壊する方法と、論理的にデータを消去する方法の 2 つがある。ここで重要となるのは、データを復元できない状態にすることである。どちらの方法であっても、不適切な手段や手順（例：ディスクフォーマットによるデータ消去、暗号化消去到に用いた鍵の不完全な廃棄、誤った手順による不完全な物理破壊）であれば、データが復元されてし

もう可能性があるため、一定の性能が保証された専用のデータ消去ツールの利用や、信頼できる専門業者への委託など安全な手段をとることが望ましい。

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

■ **どのような記録の保管が考えられるか？**

- ・ 委託先へ論理的な暗号化消去を依頼する場合には、消去証明書（第三者証明が望ましい）を、物理破壊などを行う場合には廃棄証明書を受領し、保管することが考えられる。
- ・ 社員自らによる媒体の物理破壊の場合、破壊前後の写真を撮るなど当該媒体を確実に破壊したことを証明できる証跡を保管するなどの方法が考えられる。

■ **参考となる資料はあるか？**

- ・ 以下の資料が参考となる。
 - － 総務省セキュリティポリシーガイドライン改定 「機器の廃棄・データ消去」における補足について（総務省）
(https://www.soumu.go.jp/main_content/001066789.pdf)
 - － データ適正消去実行証明協会
(<https://adec-cert.jp/>)

(5)リモートワークにおけるルール[No.3-1-5]**【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。

【評価基準】

段階	No.	評価基準
★4	3-1-5-1	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、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
	3-1-5-2	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。
	3-1-5-3	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。

【解説】**評価基準 No. 3-1-5-1 関連****■ 「リモートワークで使用する情報機器や機密情報」に含まれるものは何か？**

- ・ リモートワーク環境で使われる情報機器の例として、パソコン、スマホ、タブレット、ルータ又は外部記憶媒体がある。
- ・ 機密情報に関する分類は、「機密情報」「社外秘情報」「公開情報」等があり、「機密情報」には以下のような例がある。
 - － 個人情報（顧客、従業員、取引先等）
 - － 経営情報
 - － 顧客から預かった非公開情報

■ どのようなルールを整備することが考えられるか？

- ・ リモートワークで使用する情報機器についてのルールで定めておくべきポイントとして下記が挙げられる。
 - － リモートワークで利用できる機器の制限（例：会社資産、私有物の扱い）
 - － 接続機器のセキュリティ対策の導入（例：OS パッチやセキュリティ対策ソフトの導入）
 - － 接続方法の限定（例：VPN 接続、VDI 接続）
 - － 利用状況の把握方法（例：VPN ログ監視）
- ・ リモートワークで使用する機密情報の取扱いについてのルールで定めておくべきポイントとして下記が挙げられる。
 - － リモートワークで取り扱う情報の制限（例：顧客の個人情報など機密レベルが高い情報の扱い）
- ・ リモートワーク実施時のセキュリティ対策について、チェックリストを作成してリモートワーク実施者に確認させることも有効である。

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － 中小企業の情報セキュリティ対策ガイドライン第 4.0 版（IPA）
4 (4)「テレワークの情報セキュリティ」
(https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf)
 - － テレワークセキュリティガイドライン第 5 版（総務省）
(https://www.soumu.go.jp/main_content/000752925.pdf)

評価基準 No. 3-1-5-2 関連

- どのような方法で周知することが考えられるか？
- ・ 例として、下記の方法が考えられる。
 - ・ 社内ポータルへの掲載
 - ・ セキュリティ教育（e ラーニング等）への掲載
 - ・ 社内のメールマガジン等への掲載

No.3-2 リスクアセスメント

(1)脆弱性の管理体制[No.3-2-1]

【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。

【評価基準】

段階	No.	評価基準
★4	3-2-1-1	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。
	3-2-1-2	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。
	3-2-1-3	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。
	3-2-1-4	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。
	3-2-1-5	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。

【解説】

評価基準 No. 3-2-1-1 関連

■ どのような文書に記載することが考えられるか？

- 脆弱性情報対応マニュアル等に記載することが考えられる。

■ どのように「担当部署の役割・責任」を定めることが考えられるか？

- 脆弱性情報・脅威情報に係る対応が以下の流れで実施されることに鑑み、役割・責任を定めることが望ましい。
 - 情報の絞込み
多数の脆弱性関連情報から自組織に関連していると思われるソフトウェアの情報を収集する。
 - 脆弱性の危険度（深刻度）を確認
ベンダーや脆弱性関連情報データベースで公開している脆弱性関連情報に CVSS の基本値や攻撃状況に関する情報が含まれているかを確認する。
 - 自組織への影響を分析
1.及び2.で収集した情報を元に、該当の脆弱性が自組織のシステムにどの程度の被害を与える可能性があるかを分析する。
 - 対策の実施
3.の結果に基づき、パッチ適用の優先順位を定めた上で、対策を講じる。
- 役割・責任を定めるに当たり、評価基準 4-4-4-2 を満たすよう留意する必要がある。
- 脆弱性情報を収集する担当部署については、基本的には IT 資産を管理する部署で脆弱性情報を収集することが検討の出発点となるが、会社の規模や事業のバリエーションや数によっては、統括部門で一元的に脆弱性情報を収集の方が効率的な場合もある。

■ 参考となる資料はあるか？

- 以下の資料が参考となる。
 - サイバーセキュリティ体制構築・人材確保の手引き 第 2.0 版（経済産業省・IPA）
(<https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf>)
 - ISOG-J 脆弱性トリアージガイドライン作成の手引き
(<https://isog-j.org/output/2024/TriageGuidelines.html>)

評価基準 No. 3-2-1-2 関連

- どのような文書に記載することが考えられるか？
 - ・ 脆弱性情報対応マニュアル等に記載することが考えられる。
- どのような情報源が考えられるか？
 - ・ 以下の情報源が考えられる
 - － 「JVN iPedia」(IPA)
 - － 「重要なセキュリティ情報一覧」(IPA)
 - － 「注意喚起」(JPCERT/CC)
 - － 「MyJVN」(JPCERT/CC・IPA)
 - － 「KEV Catalog」(CISA)
 - － セキュリティベンダーが公開するレポート
 - － 平素から取引のあるベンダーへの相談
 - ・ なお、脆弱性情報の収集目的に応じ、以下のような使い分けが考えられる。
 - － IT 資産ごとに脆弱性情報を調査する場合：「JVN iPedia」(IPA)
 - － 緊急性が高い脆弱性や脅威情報を調査したい場合：「重要なセキュリティ情報一覧」(IPA)

評価基準 No. 3-2-1-3 関連

- どのような文書に記載することが考えられるか？
 - ・ 脆弱性情報対応マニュアル等に記載することが考えられる。
- どのような観点で「対応要否判断基準」を定めることが考えられるか？
 - ・ 対象となる情報資産の以下のような特性を考慮して判断することが考えられる。
 - － インターネット接続の有無
 - － 重要情報の取扱いの有無
 - － システム停止の許容範囲
- どのような観点で「対応手順」を定めることが考えられるか？
 - ・ 情報システムの変更管理プロセス及び手順を考慮して定義することが考えられる。
 - ・ 対応手順は、4-4-4-2 及び 4-4-4-3 も踏まえたものとしなければならない。
- 参考となる資料はあるか？
 - ・ 以下の資料が参考となる。
 - － 脆弱性対策の効果的な進め方（実践編）第2版（IPA）
<https://www.ipa.go.jp/security/reports/technicalwatch/hjuojm0000006nd2-att/000071660.pdf>

評価基準 No. 3-2-1-4、3-2-1-5 関連

- どのような仕組みの整備が考えられるか？
 - ・ 管理対象の情報機器一覧に、脆弱性に関する対応履歴を記録することが考えられる。
 - ・ システムの運用を委託している場合、月次報告などにより結果を確認することが考えられる。
 - ・ 管理対象機器が多い場合は、市販の脆弱性管理ツールを利用することも有効である。

No.4 攻撃等の防御

「攻撃等の防御」は、組織のサイバーセキュリティリスクを低減することを目的として実施するものであり、以下 5 つの中分類に分けられる。

別表 4 「攻撃等の防御」における中分類及びその目的

中分類	各分類の目的
アイデンティティ管理、認証、アクセス制御	資産への物理的又は論理的なアクセスを、許可された者、サービス、及びハードウェアに限定し、不正アクセスのリスクを評価した上で、そのリスクに応じた認証及びアクセス制御を行うこと。
意識向上とトレーニング	セキュリティ関連の職務を遂行できるよう、組織の人員に意識向上とトレーニングを提供すること。
データセキュリティ	情報の機密性、完全性、及び可用性を保護するために、データを管理すること。
プラットフォームセキュリティ	ハードウェア、ソフトウェア及びサービスを、機密性、完全性、及び可用性を保護するために管理すること。
技術インフラのレジリエンス	資産の機密性、完全性、可用性及び組織のレジリエンスを保護するために、セキュリティを保つための仕組みを管理すること。

No.4-1 アイデンティティ管理、認証、アクセス制御

(1)ユーザ ID の管理手続[No.4-1-1]

【要求事項】

ユーザ ID の発行・変更・削除の手続を定めること。

【評価基準】

段階	No.	評価基準
★3	4-1-1-1	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・削除は申請・承認制にすること。
	4-1-1-2	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。
	4-1-1-3	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。
	4-1-1-4	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。

【解説】

評価基準 No. 4-1-1-1 関連

■ どのような文書に規定することが考えられるか？

- ・ アカウント管理規程などに定めることが考えられる。

- 「ユーザ ID の付与・変更・削除」に係る申請・承認に際して、記録としてどのような事項を残すことが考えられるか？
 - ・ ユーザ ID が必要となった理由、承認者、承認日など必要な情報は記録として残し管理することが望ましい。
 - ・ ユーザ ID の申請が正しいものであるかを確認するため、本人以外の例えば上司などによる申請確認を行うことが望ましい。
- 「ユーザ ID の付与・変更・削除」に当たり、どのような点を考慮することが考えられるか？
 - ・ ユーザ ID には、利用者、所属、利用目的及び有効期限を紐付けて管理することが望ましい。具体的な管理項目の例として、以下が考えられる。
 - － 一意性：同じ組織内で同一のユーザ ID を重複発行しない
 - － 同一性：利用者の氏名、社員番号、所属部署を記録する
 - － 利用目的：通常利用、管理者業務、業務委託、緊急対応等を記録する
 - － 発行日：いつ発行したかを記録する
 - － 有効期限：派遣社員、委託先、期間限定業務には終了日を設定する
 - － 状態：有効、停止、削除、休職中、退職済み等を管理する
 - － 管理責任者：ID の利用を承認した責任者を記録する

評価基準 No. 4-1-1-2 関連

- ユーザ ID の共有について、原則としてどのような管理を行うことが考えられるか？
 - ・ ユーザ ID は基本的には個人に紐づいて作成・利用することが望ましい。
 - ・ 安易にユーザ ID を共有することを許容するのではなく、同一の権限を持つ複数ユーザを作成するなど操作するユーザが識別できるようにしておくことが望ましい。
- 「やむを得ず共有 ID が必要な場合」、ユーザを特定できるようにするために、どのような管理を行うことが考えられるか？
 - ・ 共有 ID は、その利用履歴だけでは利用者を特定できないため、不正な利用の検知が難しく、またセキュリティインシデントが発生した場合の真相究明の支障となる可能性がある。
 - ・ やむを得ずユーザ ID を共有する場合は、ユーザごとにアクセス管理簿を記録したり、作業日報でアクセス実績を記録するなどの運用を行うことが考えられる。
 - ・ やむを得ず複数のユーザで ID を共有する場合は代表者を選定し、定期的にパスワードを変更したり、共有が必要なユーザを見直すなどの運用を行うことが望ましい。

評価基準 No. 4-1-1-3 関連

- 「ユーザ ID が不要になった場合」に講じる措置として、例えばどのようなものが考えられるか？
 - ・ ユーザ ID が不要になった場合、以下を例とする措置を講じることが望ましい。
 - － 当該ユーザの ID を無効にすること。
 - － 当該ユーザに交付した ID カード等の認証情報を格納した装置を返還させること。
 - － 無効化した ID を他のユーザに新たに発行することを禁止すること。
- ユーザ ID が適切に「削除又は無効化」されていることを継続的に確認するための措置として、どのような対策が有効か？
 - ・ ユーザ ID の管理部署から利用部署に対してユーザ ID の棚卸しを依頼することも定期見直しの手段として有効と考えられる。
 - ・ ユーザ ID を共有している場合においては、共有しているユーザの見直し（代表者の見直し含む）も行うことが望ましい。

評価基準 No. 4-1-1-4 関連

- アクセス権が適切に「削除又は無効化」されていることを継続的に確認するための措置として、どのような対策が有効か？
- ・ 特に重要なデータや機器などは事前に抽出しておき、それらに対するアクセス権については、比較的高い頻度でアクセス権の見直しを行うことが望ましい。
 - ・ アクセス権の見直しについては、システム利用者側の自主的な見直しを期待するだけでなく、システム運用側からも積極的にシステム利用側に見直し依頼を要請することが望ましい。
 - ・ なお、No.4-1-1-2 においてユーザ ID を共有している場合、共有している者がひとりでもアクセス権が不要になった場合は、パスワードを変更するなどの措置を講じることが望ましい

(2)管理者 ID の管理手続[No.4-1-2]**【要求事項】**

管理者 ID の発行・変更・削除の手続を定めること。

【評価基準】

段階	No.	評価基準
★3	4-1-2-1	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ること。
	4-1-2-2	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。
	4-1-2-3	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。
	4-1-2-4	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。
	4-1-2-5	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。
	4-1-2-6	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。
	4-1-2-7	管理者 ID の付与・変更・削除は申請・承認制にすること。
	4-1-2-8	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。

【解説】**評価基準 No. 4-1-2-1 関連**

- 「システム管理者及び責任者」はどのような役割であり、別の者を割り当てる必要はあるか？
 - ・ 「システム責任者」とは、情報システム（クラウドサービスを含む。）ごとのセキュリティ対策及び運用の責任者を指す。一方、「システム管理者」とは、対象の情報システムの管理業務を行い、管理者権限を有する者を指す。
 - ・ 組織の規模等の個別の事情に鑑み、同一人物をシステム管理者及び責任者として定めることも差し支えない。ただし、その場合であっても、設定変更履歴や操作ログの確認、上長等による承認又は事後確認等により、権限の濫用や誤操作を防止するための牽制措置を講じることが望ましい。

評価基準 No. 4-1-2-2 関連

- 管理者 ID の共有について、原則としてどのような管理を行うことが望ましいか？
 - ・ 管理者 ID は基本的には個人に紐づいて作成・利用することが望ましい。
 - ・ 安易に管理者 ID を共有することを許容するのではなく、同一の権限を持つ複数アカウントを作成するなど操作する管理者が識別できるようにしておくことが望ましい。

- やむを得ず共有 ID が必要な場合、共有の管理者 ID を利用したユーザを特定するためにどのような管理を行うことが望ましいか？
 - ・ 万一共有せざるを得ない場合は、作業日報などで誰が管理者 ID を使用したかという実績を記録するなどの運用を行うことが考えられる。4-1-1-2【解説】も適宜参照されたい。

評価基準 No. 4-1-2-3 関連

- 「必要最低限の権限のみを付与」とは、どのような状態を指すか？
 - ・ 必要最小限の権限のみ付与とは、権限が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な権限を付与することにより、当該権限を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。
 - ・ 本対策の例として、システムを通常操作するユーザにおいては、あらかじめ実行できるプログラムやアクセス可能な領域を限定した権限を付与し、管理作業をするときに限定して管理者権限を利用することを可能とする方式（Unix 系システムにおける sudo 等）が考えられる。
 - ・ また、システム管理権限を持つ者が、システム内の機微な個人情報にアクセスする必要があるかについても検討し、システム管理権限とデータベースの管理権限を分離することも有効である。
 - ・ 管理者権限の悪用・乱用を防ぐためにも、全権限をもつ管理者権限という単一の権限を規定するのではなく、運用シナリオにそって管理者権限を複数に細分化し管理することが望ましい。
- API キーやサービスアカウント等はどのように管理すればよいか？
 - ・ システム間連携等に使用するサービスアカウント、API キー、アクセストークンその他の認証情報についても、不正利用された場合の影響を踏まえ、適切に管理することが望ましい。例えば、利用目的及び管理責任者を明確にし、必要最小限の権限とするとともに、不要となった場合には速やかに無効化又は削除することが考えられる。また、API キー等の認証情報については、ソースコード等への平文での埋込みを避け、安全に保管することが望ましい。

評価基準 No. 4-1-2-4 関連

- 開発環境を利用する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ためには、どのような管理を行うことが考えられるか？
 - ・ システム開発を実施する従業員・社外要員（派遣社員等）が自由に本番環境の管理者権限を使用することができないように制限することが重要であり、たとえば、開発環境の管理者権限と本番環境の管理者権限を分離すること、システム開発を実施する従業員・社外要員（派遣社員等）における作業を監視する仕組みを整備すること（例：操作ログの取得等）、本番環境への移行前に開発環境における管理者権限を削除すること、などが考えられる。

評価基準 No. 4-1-2-5 関連

- 「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」としてどのようなものが想定されるか？
 - ・ ID 管理台帳（ID インベントリ）の整備等を実施することや市販の ID 管理ツールを利用することなどが考えられる。

評価基準 No. 4-1-2-6 関連

- **管理者 ID が不要になった場合に講じる措置として、例えばどのようなものが考えられるか？**
 - ・ 管理者 ID が不要になった場合、以下を例とする措置を講じることが望ましい。
 - － 当該ユーザの ID を無効にすること。
 - － 当該ユーザに交付した ID カード等の認証情報を格納した装置を返還させること。
 - － 無効化した ID を他のユーザに新たに発行することを禁止すること。
- **管理者 ID が適切に削除又は無効化されていることを継続的に確認するための措置として、どのような対策が有効か？**
 - ・ 管理者 ID の管理部署から利用部署に対して管理者 ID の棚卸しを依頼することも定期見直しの手段として有効と考えられる。
 - ・ 管理者 ID を共有している場合においては、共有している管理者の見直し（代表者の見直し含む）も行うことが望ましい。

評価基準 No. 4-1-2-7 関連

- **どのような文書に規定することが考えられるか？**
 - ・ アカウント管理規程などに定めることが考えられる。
- **管理者 ID の付与・変更・削除に係る申請・承認に際して、記録としてどのような事項を残すことが考えられるか？**
 - ・ 管理者 ID が必要となった理由、承認者、承認日など必要な情報は記録として残し管理することが望ましい。
 - ・ 管理者 ID の申請が正しいものであるかを確認するため、本人以外の例えば上司などによる申請確認を行うことが望ましい。

(3)認証の強度・実装方法の決定[No.4-1-3]**【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。

【評価基準】

段階	No.	評価基準
★3	4-1-3-1	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。
	4-1-3-2	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。
	4-1-3-3	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。
	4-1-3-4	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。
★4	4-1-3-5	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

【解説】評価基準 No. 4-1-3-1 関連

- システム及び情報機器へのアクセスを許可する前に行う「認証」として、例えばどのようなものが有効か？
- ・ 有効なものとしては、以下を例とする認証方式が考えられる。
 - － 知識（パスワード等、利用者本人のみが知り得る情報）による認証
 - － 所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証
 - － 生体（指紋や静脈等、本人の生体的な特徴）による認証

評価基準 No. 4-1-3-2 関連

- 本評価基準の適用対象をどのように認識しておく必要があるか？
- ・ 評価基準 No.3-1-4-3 で把握する「重要な機密情報」を取り扱うクラウドサービスはすべて多要素認証適用の対象とする。
 - ・ 重要な情報を扱うと考えられるクラウドサービスであるか、重要な情報は扱わないクラウドサービスなのかを管理し、多要素認証の要否を管理することが望ましい。
 - ・ クラウドサービスの利用を検討する場合は多要素認証機能の有無をあらかじめ確認しておくことが望ましい。

評価基準 No. 4-1-3-3 関連

- 多要素認証を構成するものとして適当ではないものは、どのようなものが考えられるか？
 - ・ パスワードと PIN のように「知識情報」を 2 つ組み合わせても、本評価基準で求める多要素認証とならない点に注意が必要である。
- 「その他の情報」として、どのような情報を利用することが考えられるか？
 - ・ 「その他の情報」としては、送信元 IP アドレス等が考えられる。ただし、信用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が必要である。例えば、利用者が普段と異なる IP アドレスや国からログインしようとした場合のみ、追加の多要素認証を要求するなどセキュリティと業務効率のバランスに配慮できるというメリットがある。なお、利用する情報は利用者又は端末に固有に紐付くこと、容易に偽装又は共有されないこと、認証サーバ等により検証されること、ID・パスワード等の知識情報とは独立した要素であることを満たすことが望ましい。
- 使用するルータ等が多要素認証をサポートしていない場合にとり得る有効な施策はあるか？
 - ・ アクセス元が固定 IP の場合は、「その他の情報」に該当する送信元 IP アドレスを制限したうえで、ID・パスワードを用いた認証を行うことが考えられる。
 - ・ その他、ID 管理・認証サービス (IDaaS) と組み合わせて利用すること等が考えられる。
- 所有情報として用いる「証明書」には、どのような形態が含まれるか？
 - ・ IC カード等の外部媒体に格納された電子証明書のほか、端末（パソコン、スマートデバイス等）にインストールされた電子証明書（クライアント証明書）も含まれる。
 - ・ いずれの形態においても、利用者ごとに異なる証明書が発行されていることが必要である。また、秘密鍵が利用者以外に複製・持ち出しできないよう保護されていることが望ましい。
 - ・ なお、パスキー認証については、実装方式による差異はあるものの、利用者が所持する端末に格納された資格情報の利用に加え、生体認証又は端末のロック解除用パスワード等により利用者本人であることを確認する構成である場合は、所有情報と生体情報又は知識情報を組み合わせた認証として取り扱うことが考えられる。

評価基準 No. 4-1-3-4 関連

- パスワードをより強固なものとするために、どのような管理を行うことが考えられるか？
 - ・ 桁数を大きくすることに加え、単純な数値列や辞書に掲載されている英単語などをパスワードにさせないことが望ましい。

評価基準 No. 4-1-3-5 関連

- 「インターネット経由でシステムにアクセスする場合」とは、VPN を経由して使用する様な社内システムを対象としているのか、ウェブアプリ等を含むインターネットからアクセス可能なシステムすべてを含むのか？
 - ・ インターネットからアクセス可能なシステムすべてを含む。そのため、管理者については、社外からアクセスできる Web サイトや、VPN を用いての社内環境への接続も多要素認証の対象となる。
 - ・ 他方、インターネット経由で社内環境へ接続する場合は、ラテラルムーブメント²³対策の観点から特にリスクが高いため、管理者及びユーザの双方において多要素認証を実装することが必要となる。

²³ 外部の攻撃者やマルウェアが企業の内部ネットワークの侵入に成功した後、ネットワーク内を水平方向に移動し、侵害範囲を段階的に拡大していく攻撃手法。

- ・ 一方、社内環境への接続後にアクセスする社内システムについては、重要な機密情報を取り扱うシステムへアクセスする場合に、多要素認証を要求している。その他のシステムについても、システムの重要度に応じて認証の強度を調整することが望ましい。

(4)アカウントロック制御 [No.4-1-4]**【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。

【評価基準】

段階	No.	評価基準
★3	4-1-4-1	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。
	4-1-4-2	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。

【解説】**評価基準 No. 4-1-4-1 関連**

■ 要求されている端末のロック制御はどのように設定できるか？

- 例えば、Active Directory 環境においては、「グループポリシーの管理」から「アカウント ロックアウトのポリシー」を設定することが考えられる。
- [参考]

Cyber A2/AD「ランサムウェア防御チェックシート Level 1」では、ロック制御の詳細な設定方法を解説している。

(<https://www.softwareisac.jp/a2ad/level1-check-sheet/>)

- 要求されている端末のロック制御により、特定の ID を固定し、次々とパスワードを試す辞書攻撃や総当たり攻撃（ブルートフォース攻撃）のリスクを緩和できる。

■ 「No.4-1-5 で求められるよりも強度の高いパスワード」の設定として、どのようなものが考えられるか？

- 例えばログインパスワードについては、米国国立標準技術研究所（NIST）SP 800-63 に基づき、パスワード単独での認証の場合は、15 桁以上のパスフレーズを採用することが考えられる。
- 数字のみからなる PIN コードを用いる場合は、4-1-4-2 で要求するものよりも強度の高いものを利用することが考えられる。

評価基準 No. 4-1-4-2 関連

■ パスワード又は PIN で求められる強度に違いはあるか？

- ローカル認証で PIN コードを利用する場合、PIN という「知識」、PIN 情報が格納されている端末もしくは IC カードの「所有」が必要であり、オンライン認証でパスワードを用いる場合とは求められる強度が異なる。本評価基準における「最低でも 6 文字以上」という要求は、ローカル認証で PIN コードを利用する場合に適用されるものであり、オンライン認証でパスワードを用いる場合は、4-1-5 に定める要求を遵守する必要がある。

(5)パスワード設定ルール[No.4-1-5]**【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。

【評価基準】

段階	No.	評価基準
★3	4-1-5-1	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。
	4-1-5-2	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。
	4-1-5-3	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。
	4-1-5-4	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。
	4-1-5-5	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。

【解説】**評価基準 No. 4-1-5-2 関連**

■ 「推測されやすい単語の設定」として、例えばどのようなものが考えられるか？

- ・ ユーザ認証にパスワードを利用する場合、パスワードに利用者の名前や利用者個人に関連する情報から簡単に派生させたもの、キーボードの並び順(「qwertyuiop」等)等、容易に推測されるものを用いてはならない。
- ・ パスワードとして設定できる文字列の長さに制約がある場合は、辞書に載っている単語をそのまま使わず、英大文字・英小文字・数字・記号を組み合わせた推測されにくい文字列を設定することが望ましい。
- ・ 一方、十分に長いパスワードを設定できる場合は、複数の単語をランダムに組み合わせた長いパスフレーズを利用する方法も考えられる。この場合、必ずしも数字や記号を含める必要はない。

評価基準 No. 4-1-5-3 関連

■ パスワードをより強固なものとするために、どのような管理を行うことが望ましいか？

- ・ 強固なパスワードの要件を一律に定めることは困難であるが、4-1-5-2 で求める推測されやすい単語の設定を禁止することのほか、例えばパスフレーズを用いるなど、パスワードを設定する際に可能な限り桁数を増やして安全性を高めることが考えられる。
- ・ 例えば、NIST Special Publication 800-63 の最新版である Revision 4 では、単要素認証で利用するパスワードを 15 文字以上とすることが必須とされている。
- ・ 本評価基準に定めるパスワードの文字数や複雑性に係る要件は現時点における基準であり、国内外のガイドライン、サイバー攻撃の動向及びシステムの対応状況等を踏まえ、今後見直される可能性がある。このため、システム上の制約によって長いパスワードを設定できない場合は、将来の基準見直しにも対応できるよう、パスワードの文

字数上限の拡張、認証機能の改修、多要素認証に対応したシステムへの移行等について、早期に検討し、計画的に対応することを強く推奨する。

評価基準 No. 4-1-5-4 関連

- シングルサインオン（SSO）を利用している場合は、情報機器及びサービス間でのパスワードの使い回しに該当するか？
 - ・ 同一の認証基盤（SSO 等）を利用する場合は使いまわしに該当しない。

評価基準 No. 4-1-5-5 関連

- どのような方法で周知することが考えられるか？
 - ・ 例として、以下の方法が考えられる。
 - － 社内ポータルへの掲載
 - － セキュリティ教育（e ラーニング等）への掲載
 - － 社内のメールマガジン等への掲載

(6)パスワード管理ルール[No.4-1-6]**【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。

【評価基準】

段階	No.	評価基準
★3	4-1-6-1	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ること。
	4-1-6-2	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。
	4-1-6-3	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。

【解説】**評価基準 No. 4-1-6-1 関連****■ 「パスワードを安全に保管する」ための取組として、どのようなものが有効か？**

- ・ パスワードを安全に保管するための取組として、以下をすべて含む管理を行うことが考えられる。
 - 自己のパスワードを他者に知られないように管理すること。
 - 以下を例とする他者からのパスワード窃取行為に注意が必要である。
 - ・ パスワードを入力する際に他者が周囲から盗み見する。
 - ・ 他者が管理者を名乗ってパスワードを聞き出す。
 - 自己のパスワードを他者に教えないこと。
 - たとえ、他者に処理を代行させる目的であっても、従業員等は自己のパスワードを他者に教示してはならない。パスワードを他者に教示することによって、システムの ID と実際の操作者との関係が曖昧になり、アクセス制御、権限管理、ログ管理その他のセキュリティ対策が効果を失う可能性がある。また、教示された者にとっても、例えば、当該 ID によって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己のパスワードは他者に「教えない」ことを徹底すべきである。
 - 以下に挙げる行為は行うべきではない。
 - 自己のパスワードを、内容が分かる状態で付箋等に記入してモニタ、端末本体、及びその周辺に貼付する。
 - 自己のパスワードを、特段の保護をせずに平文のままテキスト形式で保存する。
- ・ パスワード管理アプリを利用してパスワードを暗号化して保管することも有効である。その際、パスワード管理アプリ自体に対して強固な認証を設定し、サービスごとに異なるパスワードを利用することが望ましい。

評価基準 No. 4-1-6-2 関連**■ 「パスワードの漏えい」をどのように検知することができるか？**

- ・ 本評価基準は、漏えいが判明した場合又はその疑いがある場合の手順を定めることを求めるものであり、漏えいを能動的に検知する仕組みを設けることまでを求めるものではない。漏えいは、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、報道等により判明する場合が多い。
- ・ そのうえで、より早期に把握するための方法としては、以下のような例が考えられる。
 - パスワード管理アプリの漏えいチェック機能を利用する
 - Have I been Pwned などのパスワード漏えいに係る検索サイトで使用しているパスワードが漏えいしていないかを定期的に確認する

評価基準 No. 4-1-6-3 関連

- どのような方法で周知することが考えられるか？
 - ・ 例として、以下の方法が考えられる。
 - － 社内ポータルへの掲載
 - － セキュリティ教育（e ラーニング等）への掲載
 - － 社内のメールマガジン等への掲載

(7)アクセス権の管理ルール[No.4-1-7]**【要求事項】**

アクセス権の管理ルールを定めること。

【評価基準】

段階	No.	評価基準
★3	4-1-7-1	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、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。
★4	4-1-7-2	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。
	4-1-7-3	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。
	4-1-7-4	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。
	4-1-7-5	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。
	4-1-7-6	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。

【解説】評価基準 No. 4-1-7-1 関連

- 「アクセス権の発行」や「与える入室許可・アクセス権の範囲」が妥当かどうかを判断する具体的な条件は何か？
- ・ その業務を遂行する権限を有しているかどうか条件となる。その判断の観点としては、次のものがある。
 (以下例示)
 - － 所属部門
 - － 役職
 - － 部門内での役割 (例：機密管理担当者)

評価基準 No. 4-1-7-2 関連

- 「アクセス権の棚卸」として何を実施することが有効と考えられるか？
- ・ アクセス権を定期的に棚卸することは、遵守違反を発見して是正するだけでなく、管理ルールを遵守する意識を向上する観点からも重要である。具体的な方法は、入室許可・アクセス権の申請書や台帳に記載されていないアクセス権の発行、変更、無効化、削除が無いことを確認することが考えられる。例えば、システム上のアクセス権の発行、変更、無効化、削除の履歴と、申請書や台帳の記録を比較・確認することなどが考えられる。すべての履歴の確認が難しい場合、サンプリングによる確認であっても、管理ルールの違反を抑制する効果があるため、実施することが望ましい。

評価基準 No. 4-1-7-3 関連

- 「重要な機密情報」とは何か？
- ・ 組織によって異なる。一般的には機密管理に係る規程類において、明確に重要情報の定義がされているケースが多いため、こうした規定に準拠することが重要となる。なお、

一般的な傾向としては、次のような情報を「重要な機密情報」として取り扱う傾向にある。

(以下例示)

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

評価基準 No. 4-1-7-4 関連

■ 重要な機密情報を扱うシステムにおける「システム管理者の要件」としてどのような事項を定めることが考えられるか？

- ・ 「システム管理者の要件」としては、例えば、情報システム部門に属し、部門長等から承認された者であること、システム管理者同士での作業の「相互牽制」及び「職務の分離」が有効に働くこと等が考えられる。

評価基準 No. 4-1-7-5 関連

■ 「必要最低限の権限のみを付与」とは、どのような状態を指すか？

- ・ 必要最小限の権限のみ付与とは、権限が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な権限を付与することにより、当該権限を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。
- ・ 本対策の例として、システムを通常操作するユーザにおいては、あらかじめ実行できるプログラムやアクセス可能な領域を限定した権限を付与し、管理作業をするときに限定して管理者権限を利用することを可能とする方式（Unix 系システムにおける sudo 等）が考えられる。※4-1-2-3【解説】も参照されたい。

評価基準 No. 4-1-7-6 関連

■ 「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」とは、どのようなものを指すか？

- ・ 付与したアクセス権の運用/利用状況をログとして記録しておき、定期的に確認することが有用である。
- ・ 重要な機密情報を扱うサーバや端末へのアクセスに関するログのほか、サーバが異常等を検出した際に出力するログ（エラーログ）を確認することも有効である。
- ・ アクセスログを確認する際は、運用管理作業の記録、管理者 ID によるアクセスを検知した場合の通知等の確認により、不正なアクセスが行われた可能性を確認することも考えられる。

(8)サーバ設置エリアへの入退室管理[No.4-1-8]**【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。

【評価基準】

段階	No.	評価基準
★4	4-1-8-1	サーバの設置エリアに入場可能な者を定めること。
	4-1-8-2	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。
	4-1-8-3	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。
	4-1-8-4	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。

【解説】評価基準 No. 4-1-8-1 関連

■ 「サーバの設置エリア」とは何か？

- ・ 各社で使用するサーバを設置する会社内外の場所（委託先やデータセンターを含む。）を指す。適切に管理する観点から、サーバを設置する単一又は複数の場所をあらかじめ設定し、サーバは当該エリア内において設置・管理を行う必要がある。また、設置エリアについては、施錠管理できる専用のサーバールーム等であることが望ましいが、施錠が出来ないエリアをサーバの設置エリアとすることも差し支えない（この場合は、No.4-1-8-2 に基づき、サーバを施錠可能な専用ラックに入れ、施錠管理を行う必要がある）。

■ 入場可能な者としてどのような者を定めればよいのか？

- ・ 不必要に誰でも入場可能な者としてよいというわけではなく、実際にサーバを操作する従業員や委託事業者の社員等に限定したうえで、入場可能な者を何らかの方法で一覧化しておく必要がある。

評価基準 No. 4-1-8-2 関連

■ 「施錠」の方法はどのようなものであればよいのか？

- ・ シリンダーキー、カードキー、暗証番号、指紋認証など、施錠可能であれば方法は問わない。

評価基準 No. 4-1-8-3 関連

■ 「安全に管理する」ために何を実施することが考えられるか？

- ・ シリンダーキーやカードキーなどの物理鍵の場合は、キーボックス、キーキャビネット等の一定の保管場所を設定し、当該保管場所において保管する必要がある。
- ・ 施錠方法が暗証番号の場合は、当該暗証番号を記載した紙媒体を施錠保管するなど、暗証番号の紛失、漏えい等を防止するような対策を講じる必要がある。
- ・ どのような施錠方式であっても、鍵等については管理者を定める必要がある。

評価基準 No. 4-1-8-4 関連

■ 「サーバの設置エリアの入退場記録」はどのように取得すればよいか？

- ・ サーバの設置エリアに対して入退場管理システムを導入している場合は、当該システムにより記録されたものを保管することが考えられる。このほか、入退場に係る台帳を設け、入退場者に入退場日時及び入場者氏名を記録させる方法も考えられる。

(9)可搬媒体の制限[No.4-1-9]**【要求事項】**

可搬媒体の持込み・持出しを制限すること。

【評価基準】

段階	No.	評価基準
★4	4-1-9-1	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。
	4-1-9-2	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。
	4-1-9-3	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の内容及び遵守状況について点検すること。

【解説】評価基準 No. 4-1-9-1 関連**■ 持込みルールとして具体的にはどのようなものを定めればよいか？**

- ・ ここでいう持込みルールとは、端末等を組織内に持ち込んでよいか、また、どのような条件で持ち込むことができるかを規定するルールのことを指す。（持ち込んだ端末等に対する管理・制御については、No.4-4-1-1 等で別途管理を行うことが考えられる。）
- ・ 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。）を社内に持ち込む場合は、情報漏えい、マルウェア侵入等のリスクが考えられることから、持込みについて一定の制限をかける必要がある。持込みのルールとしては、例えば、以下のような項目について定めることが望ましい。（以下例示）
 - － 持込み制限の対象とするエリア、物品
 - － 社内への持込み申請、承認方法
 - － 持込み記録の保管、管理方法
- ・ なお、サーバーームなどでは、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。）の持込みを全面的に禁止するというルールを定めることも有効である。

評価基準 No. 4-1-9-2 関連**■ 持出しルールとして具体的にはどのようなものを定めればよいか？**

- ・ 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）の社外への持出しは、機密情報流出防止の観点から一定の制限をかける必要がある。持出しのルールとしては、例えば、以下のような項目について定めることが望ましい。（以下例示）
 - － 社外への持出し申請、承認方法
 - － 持出し記録の保管、管理方法
 - － 社外へ持ち出した機器を社内ネットワークへ再接続する際の条件及び手順

No.4-2 意識向上とトレーニング

(1)セキュリティの意識向上のための教育・研修 [No.4-2-1]

【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。

【評価基準】

段階	No.	評価基準
★4	4-2-1-1	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ること。
	4-2-1-2	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。
	4-2-1-3	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
	4-2-1-4	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。
	4-2-1-5	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。

【解説】

評価基準 No. 4-2-1-1 関連

- 「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」とは具体的に何か？
- 例えば経営層の就任時において、各社で定めたサイバーセキュリティに関して経営層が果たすべき役割及び責任についてセキュリティ担当部署が説明を行う機会を設けることが考えられる。

評価基準 No. 4-2-1-2 関連

- 「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」とは何か？
- 各職場によってさまざまであるが、例えばパソコン等の可搬媒体を頻繁に社外に持ち運ぶ職場の場合は、当該媒体の紛失等のリスクが他の部署に比べて高い事や、メールを大量に発出する職場の場合は、メール誤送信のリスクが他の部署に比べて高い事などが考えられる。
 - なお、すべての部署ごとに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を設定する必要はないが、各社の活動単位（例：人事、営業、生産等）ごとに固有の重要なルール及びリスクを設定したうえで、啓発することが望ましい。

評価基準 No. 4-2-1-3 関連

- 教育・研修には何が盛り込まれていればよいのか？
- 対象者や目的によって盛り込む事項は様々であるが、「理解向上」を目的とした教育を行う場合には、昨今の世の中の動向や、会社の規定を中心とした説明が望ましく、また、「注意喚起」を目的とした教育を行う場合には、他社事例を織り交ぜた「注意しなくてはいけないこと」「してはいけないこと」などを具体的に紹介する事が望ましい。

- ・ 電子メールと Web 閲覧という経路の違いによって必要な予防策や説明すべき内容が異なるため、それぞれの感染経路を想定した教育を実施する必要がある。
- ・ また、機密区分の定義と情報の取扱いについては、各社の社内ルール等で定めた機密区分と、各機密区分の取扱いについて具体的に紹介する必要がある。

■ **教育・研修の効果の確認まで実施するべきか？**

- ・ 本項目ではそこまでの実施は求めているが、各組織の任意の取組として実施することは有効である。

評価基準 No. 4-2-1-4 関連

■ **記録はいつまで保管すればよいか？**

- ・ 特段の定めはないが、本制度の更新期間である 3 年間を目安とする。少なくとも No.4-2-1-5 における実施内容の点検や、各受講者における受講履歴の把握に支障のない期間保管する必要がある。

評価基準 No. 4-2-1-5 関連

■ **「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」とは、具体的に何を実施すればよいか？**

- ・ 最新のセキュリティ脅威に関する動向や国内外法規制との整合性を踏まえ、教育・研修の実施内容が最新となっているかどうかを確認することが考えられる。（評価基準 No.4-2-2-3 についても、同様の点検を行うことを想定している。）

(2)セキュリティインシデント発生時の教育・訓練[No.4-2-2]**【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。

【評価基準】

段階	No.	評価基準
★3	4-2-2-1	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。
	4-2-2-2	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。
	4-2-2-3	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。

【解説】**評価基準 No. 4-2-2-1 関連****■ 教育・訓練には何が盛り込まれていればよいのか？**

- ・ 教育や訓練を行う際には、対象者によって役割や業務内容が異なることを考慮し、例えば以下のように対象者ごとに教育や訓練の内容を変えることが効果的である。
(以下例示)
 <一般従業員向け>
 - セキュリティインシデント発生時における情報や情報機器の取扱いに関する会社ルールの教育（例：eラーニングによる会社ルールの教育）
 - セキュリティインシデント発生時における情報や情報機器の取扱いに関する訓練（例：標的型メールを受信した際の報告訓練、マルウェア感染時の対応訓練）
 <情報セキュリティ担当者向け>
 - インシデント対応に関する教育（例：組織内のインシデント対応に係る体制や対応手順に関する教育）
 - インシデント対応に関する訓練（例：インシデント発生時の発見報告・初動・システム復旧等の対応訓練）。
- ・ なお、最低限、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関して教育を実施する必要がある。

評価基準 No. 4-2-2-2 関連**■ 記録はいつまで保管すればよいのか？**

- ・ 特段の定めはないが、本制度の更新期間である3年間を目安とする。少なくとも No.4-2-2-3 における実施内容の点検や、各受講者における受講履歴の把握に支障のない期間保管する必要がある。

No.4-3 データセキュリティ

(1)データの暗号化 [No.4-3-1]

【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。

【評価基準】

段階	No.	評価基準
★4	4-3-1-1	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、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。
	4-3-1-2	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。

【解説】

評価基準 No. 4-3-1-1・4-3-1-2 関連

■ 具体的にどのような方法で暗号化すればよいのか？

- ・ パソコンの場合は、ドライブ全体を暗号化する場合と個々のファイル単位で暗号化する場合が考えられる。
 - － ドライブ全体を暗号化する場合は OS 標準のディスク暗号化機能（例えば、Windows の場合における BitLocker など）を使用することが考えられる。
 - － ファイル単位で暗号化する場合は、Office ソフトの暗号化機能や暗号化ツール・ソフトにより暗号化することが考えられる。
- ・ また、USB メモリ等の外部記憶媒体のうち外部に持ち出すものについては、パスワード等による暗号化機能を備えている製品を使用するほか、OS 標準の暗号化機能やファイル単位の暗号化により保護することも考えられる。
- ・ 端末に機密情報を保存しない方式（シンクライアント、セキュアブラウザ、セキュアコンテナ、VDI 等）の場合は、業務上利用するデータそのものを端末へ保存しないことを前提として、閲覧、編集又は印刷等の処理に伴い端末上に一時的に生成されるファイル（例：キャッシュファイル、テンポラリファイル、ブラウザの一時保存データ等）が暗号化されていれば差し支えない。

■ 具体的に何を周知すればよいのか？

- ・ 以下について暗号化することを定めた社内ルールの内容を周知する必要がある。なお、周知については、社内掲示板、社内ポータル等において当該社内ルールそのものや該当する規定の抜粋などを周知することが考えられる。
 - － 社外に持ち出すパソコン及び記憶媒体の機密情報
 - － 重要な機密情報

(2)データの保管ルール [No.4-3-2]**【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。

【評価基準】

段階	No.	評価基準
★4	4-3-2-1	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。

【解説】**評価基準 No. 4-3-2-1 関連****■ 相対的に安全な区域にあるサーバとは何か？**

- ・ クラウドサービスの場合は、No.4-1-3-2 に基づき、少なくともアクセスに当たって多要素認証を実装したものを指す。
- ・ それ以外の社内ネットワーク上のサーバの場合は、少なくともインターネットから直接アクセスできず、ファイアウォール等のネットワーク機器により内外の通信が制御されている領域を指す。
- ・ ランサムウェアによる被害では、利用者のパソコン上のデータだけでなく、当該パソコンからアクセス可能な共有フォルダやサーバ上のデータも暗号化される事例がある。このため、業務継続上重要なデータは、利用者端末とは分離された相対的に安全な区域に保管するとともに、必要最小限のアクセス権限のみを付与することが望ましい。
- ・ 日本国内で利用できるクラウドサービスを提供しているデータセンターは、必ずしも日本国内にあるわけではなく、データセンター内のデータ取扱いについて、国内法以外の法令及び規制が適用される場合がある。データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが法執行機関の命令により強制的に開示されることが考えられる。情報の開示が懸念される場合は、暗号鍵で暗号化するなどの措置の検討や、クラウドサービス提供者へデータ保護の措置等についての確認を行うようにすることが考えられる。
- ・ データ取扱いに関する準拠法については、以下の資料が参考となるので参照されたい。
 - IPA : ISMAP 管理基準（管理策基準 15.1.1.16B）
 (https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028)

(3)取引先との情報共有ルール [No.4-3-3]**【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。

【評価基準】

段階	No.	評価基準
★4	4-3-3-1	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。

【解説】**評価基準 No. 4-3-3-1 関連****■ ファイル共有/ファイル転送とは何か？**

- ・ ファイル共有とは、特定の場所にファイルをアップロードし、特定の相手にファイルのアクセスを許可することを指す。ファイル共有を実施する際には、アップロード場所の共有範囲やアクセス範囲に注意する必要がある。
- ・ ファイル転送とは、特定の相手にファイルを直接送信することを指す。少なくとも送信履歴として、メールの送信履歴やログ等により、送信先及び送信ファイルが特定できる必要がある。

■ “信頼できる相手”とは何か？

- ・ 業務上の必要に基づき情報共有を行う相手であって、所属組織及び本人確認ができている取引先、顧客、委託先等を指す。個人向けメールアドレスのみを用いる相手や、共有先が特定できない状態での公開リンク等は、「信頼できる相手」とはみなさないことが望ましい。

(4)適切なバックアップ[No.4-3-4]**【要求事項】**

適切なバックアップを行うこと。

【評価基準】

段階	No.	評価基準
★3	4-3-4-1	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。
	4-3-4-2	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。
	4-3-4-3	バックアップ対象ごとにリストア手順書を整備すること。

【解説】**評価基準 No. 4-3-4-1 関連****■ 取得対象、取得頻度はどのような考えで定めればよいか？**

- ・ バックアップの取得対象や取得頻度を定めるうえで、システム停止やデータ消失時にビジネスに与える影響等の重要性や、データの更新頻度やバックアップのコストが考慮すべきポイントとなる。
 - － システム/データの重要性（例：基幹システム、顧客情報、経営情報）
 - － システム/データの更新頻度（例：更新頻度が高いソフトウェアやデータは取得頻度も高める）
 - － バックアップのコスト（例：バックアップのデータ量や費用に応じて取得頻度を調整する）。

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

- ・ 取得対象、取得頻度及びバックアップ方法は、データの重要度、更新頻度及び障害発生時の業務影響等を踏まえて定めることが望ましい。

【取得対象、取得頻度の例】

- － ファイルサーバに保存された文書や設定情報（取得頻度：文書は日次、設定情報は月次）
- － メールサーバに保存されたメールや設定情報（取得頻度：メールは日次、設定情報は月次）
- － 業務システムで利用するデータベース（取得頻度：日次又は週次）
- － システム復旧時に必要となるサーバ及びネットワーク機器の設定情報（取得頻度：設定変更時又は月次）

【バックアップ方法の例】

- － バックアップサーバの活用
- － 外部記憶媒体への保管
- － クラウドストレージへの保管
- － 本番環境とは異なるネットワーク又は保管場所への保管

評価基準 No. 4-3-4-2 関連

■ 「遠隔地」とは、どのような条件を満たす場所を指すか？

- ・ 遠隔地について一概に定義することはできないが、遠隔地バックアップの目的は災害時に備えて主要なバックアップを実施している場所から離れたところにおいてもバックアップを行うことにあり、災害リスク等を考慮して、バックアップ場所を選定することが望ましい。
- ・ なお、遠隔地バックアップの実施先としてクラウドサービス上に対象データを保管することも差し支えない。

評価基準 No. 4-3-4-3 関連

■ 「リストア手順書」の整備には、クラウドサービスを利用しているケースを含むか？

- ・ 含む。汎用的なクラウドサービスを活用している場合、一般的にはすでにサービス提供側で復元（リストア）の実施体制や手順が確立されている場合が多い。
一方で、バックアップから復元するまでの目標時間や、どの時点までのデータを復元するかといった復旧レベルを指定することは、サービス利用契約上、困難なケースが多い。その場合は、サービス事業者との間でデータの保証や復元の責任範囲を確認したうえで、自社で実施する範囲において必要なリストア手順を整備することで代替可能である。
- ・ また、自社インフラとしてクラウド環境を整備している等で、自組織が復元（リストア）を実施できる場合は、そのための手順の整備をする必要がある。

No.4-4 プラットフォームセキュリティ

(1)情報機器、OS 及びソフトウェアの安全な構成[No.4-4-1]

【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。

【評価基準】

段階	No.	評価基準
★3	4-4-1-1	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。
	4-4-1-2	外部記録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。
	4-4-1-3	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。
★4	4-4-1-4	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。
	4-4-1-5	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。
	4-4-1-6	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。

【解説】

評価基準 No. 4-4-1-1 関連

- 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ための方法としてどのようなものがあるか？
 - ・ 例えば、以下の例が挙げられる。
 - － ユーザによるソフトウェアのインストールを制限するよう設定を行う。
 - － ユーザによるソフトウェアのインストールを監視し、利用を許可するソフトウェア以外のものがインストールされた場合は、当該ユーザに警告や削除依頼等を行う。
- BYOD 端末は対象となるか？
 - ・ BYOD 端末を業務利用する場合であっても、利用を許可していないソフトウェアを削除又は無効化することが望ましい。ただし、実施が困難である場合は、MDM（Mobile Device Management）又は MAM（Mobile Application Management）等を利用して業務利用アプリケーション及び業務データに対する適切な統制を実施することが考えられる。

評価基準 No. 4-4-1-2 関連

- 外部記録媒体を使用する端末とは何か？
 - ・ USB メモリ等の外部記録媒体（外部記憶媒体と同義）を接続する可能性のあるパソコン、サーバ等を指す。

- ・ 標的型攻撃に用いられる手段として、自動実行 (auto-run) 又は自動再生 (auto-play) 機能を悪用するものがあり、例えば、不正プログラムを格納した USB メモリを端末に接続させることにより、不正プログラムを実行させるという手法が想定される。外部記録媒体を接続する可能性のあるパソコン、サーバ等については、当該機能を無効にすることで、この機能を悪用する手段による被害に遭うリスクを低減する必要がある。
- ・ 一方で、そもそも外部記録媒体の接続を技術的に禁止しているなど、接続する可能性のない端末については、必ずしも当該機能の無効化を実施する必要はない。(任意の取組として無効化することを妨げるものではない。)

評価基準 No. 4-4-1-3 関連

■ あらゆる設定変更について申請・承認制とする必要があるか？

- ・ セキュリティ水準に影響を及ぼさない軽微な設定変更まで必ずしも申請・承認制とする必要はない(ただし、軽微な設定変更を含め、すべての設定変更を申請・承認制とすることを妨げるものではない。)。一方で、どの範囲の設定変更を申請・承認制とするかについては、あらかじめ定めておくことが望ましい。

評価基準 No. 4-4-1-4 関連

■ 不要なサービス及びプロトコルとは何か？

- ・ パソコンやサーバ上で稼働しているものの利用していないサービスやプロトコルのことを指す。このようなサービスやプロトコルは、思わぬ形で悪用され侵入経路となるリスクがあるため、無効化する必要がある。
- ・ サービス及びプロトコルを無効化するに当たっては、当該サービス及びプロトコルの機能や依存関係を確認したうえで、無効化してよいかどうかを判断することが望ましい。
- ・ 現在稼働しているサービスやプロトコルを定期的に棚卸し、不要なものが稼働した状態になっていないかどうかを点検することが望ましい。

評価基準 No. 4-4-1-5 関連

■ 「デフォルトユーザ ID の利用を停止」とはどこまで含まれるか？

- ・ 端末やサーバ装置、通信回線装置などで使用されている初期値として利用可能な ID (Administrator、root、admin 等) は、誰もが識別コードを知っているため不正アクセスの標的となる可能性が高い。そのため、アカウント無効化、ログイン禁止などにより、直接的な利用ができないような対策が講じられていれば差し支えない。

■ 「強固な認証」とは何か？

- ・ やむを得ずデフォルトユーザ ID をそのまま使用するに当たっては、ログイン時に多要素認証を実施することが望ましいが、そのほかに、できる限り長い桁数を備えた容易に推測できないパスワード (No.4-1-5-3 で定められた英大文字小文字、数字を含めた 10 文字以上等) をログイン時のパスワードとして設定することも考えられる。

評価基準 No. 4-4-1-6 関連

■ 標準構成・設定ルールとは何か？また、どのように定めればよいか？

- ・ 各端末で利用する OS 及びソフトウェアが統一されていないとセキュリティ水準にばらつきが出るため、標準構成・設定ルールを定める必要がある。
- ・ 標準構成とは、利用する OS 及びソフトウェアの名称とバージョンを指す。必ずしも全社で統一する必要はないが、少なくとも、社内で利用する OS、オフィスソフト、ブラウザ及びマルウェア対策ソフトについては、その名称とバージョンをあらかじめ定めておく必要がある。

- ・ 設定ルールとは、OS 及びソフトウェアにおいてどのような設定を実施している必要があるかというルールのことであり、OS 及びソフトウェアのベンダーが推奨する設定を参考にしつつ、定める必要がある。

(2)サポート期限の切れた OS 及びソフトウェアへの対策 [No.4-4-2]**【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。

【評価基準】

段階	No.	評価基準
★4	4-4-2-1	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。

【解説】**評価基準 No. 4-4-2-1 関連**

- 「サポート切れの OS 及びソフトウェア」とはどのようなものを指し、いかなる管理を行うことが望ましいか？
 - ・ ソフトウェアベンダー、他の事業者、OSS の開発コミュニティ、配布元等から、利用中のバージョンに対するセキュリティ修正等を一切受けられないものを指す。
 - ・ ソフトウェアベンダーから提供される製品の場合、製品ロードマップの見直し等により、サポートの終了が突然発表されることもあり得るため、利用するソフトウェアのサポート期間に関する情報を適時入手し、ソフトウェア更改やサポート事業者の切替え等の対策が適切に講じられるよう考慮することが望ましい。
 - ・ 適用範囲を構成する IT 基盤で使用しているソフトウェア等の IT 資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有する IT 資産管理ソフトウェアを導入することも有用である。
- 「脆弱性悪用のリスクを低減する対策等」として、どのようなものがあるか？
 - ・ 「脆弱性悪用のリスクを低減する対策」の具体的な内容については、評価基準 No.4-4-4-1 及び No.4-4-4-2【解説】を参照されたい。
- オープンソースソフトウェア（OSS）については、どのように考えればよいか？
 - ・ OSS については、商用ソフトウェアのように明確なサポート期限が設定されていない場合がある。この場合、開発コミュニティ、配布元、保守事業者等による更新状況、脆弱性情報及び修正プログラムの提供状況を確認し、実質的に保守が継続しているかを判断する。なお、OSS であることのみをもって、サポート切れとは判断しない。
 - ・ OSS の利用については、以下の資料が参考となるので参照されたい。
 - － IPA：ガイドブック その「思い込み」がリスクになる？OSS に対する誤解を解く 5 つの処方箋 (<https://www.ipa.go.jp/digital/kaihatsu/oss/learn/guidebook-biases-to-oss/index.html>)

(3)ログの取得 [No.4-4-3]**【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。

【評価基準】

段階	No.	評価基準
★4	4-4-3-1	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。
	4-4-3-2	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。
	4-4-3-3	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。

【解説】**評価基準 No. 4-4-3-1 関連**

■ 「ログを取得、保管」する具体的な方法としてどのようなものがあるか？

- ・ 本評価基準で対象としているログの取得目的は、インシデント発生時の調査のためであることに留意が必要である。
- ・ ログの保管については、ログが発生する機器で保管しておく方法や、ログ管理システムに集約して一元管理する方法がある。ログはインシデント発生時の調査のために用いられるため、No.4-4-3-2 に基づく不正アクセス対策に加え、改ざん対策を講じた状態で保管することが望ましい。そのため、ログが発生する機器だけではなく、不正アクセス対策等のセキュリティ対策をしたログ管理システムにログを保管することも考えられる。

■ 上記の要件に相当するログを取得及び保管とは何か？

- ・ 利用するクラウドサービス又はシステム構成の仕様によっては、ファイアウォール、プロキシサーバ又は認証サーバに相当する機器・サーバを設置しない場合も考えられる。そのような場合、当該機器に代わる機能又はサービスにおいて取得されるログの種類、取得項目及び保管期間を確認し、インシデント発生時の調査に必要な情報を追跡できるログを取得又は確認すること。なお、自組織で取得・保管できないログについては、クラウドサービス事業者から提供される仕様書、サービス仕様書、契約書そ

の他の資料により、当該ログが保管されていることを確認や、設定画面やサンプルログ等での確認により代替できる。

評価基準 No. 4-4-3-3 関連

■ 「不審な認証試行」としてどのようなものがあるか？

- ・ 以下のようなものが考えられる
 - － 短時間の大量失敗
 - － 通常と異なる国・地域からのログイン
 - － 管理者 ID による異常な時間帯のログイン
 - － 成功直後の権限変更
 - － 同一 ID による複数地域からの同時接続

■ 「モニタリング」はどのような頻度で実施すればよいか？

- ・ 評価基準 No.4-4-3-3 では、月 1 回以上のモニタリングで認証サーバのログに対するモニタリングを求めている。一方で、重要なシステム又はインターネット公開システムについては特に不正な認証を実行されるリスクが高いため、アラート機能、SIEM、IDaaS 等を活用し、異常な認証試行を可能な限りリアルタイム又は日次で検知することが望ましい。
- ・ なお、組織全体のセキュリティ対策としては、No.4-4-3-3 による不正アクセスの兆候の検知に加え、No.4-4-4-3 によるインターネットとの境界に設置されたネットワーク機器の重大な脆弱性への対応を組み合わせ、侵入リスクの低減及び早期発見を図ることが望ましい。

(4)セキュリティパッチ・アップデートの手続 [No.4-4-4]**【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。

【評価基準】

段階	No.	評価基準
★3	4-4-4-1	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。
	4-4-4-2	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
★4	4-4-4-3	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。

【解説】**評価基準 No. 4-4-4-1 関連****■ 「脆弱性悪用のリスクを低減する対策」として、どのようなものがあるか？**

- ・ 「脆弱性悪用のリスクを低減する対策」として、具体的には次のような対策等が講じられている必要がある。
 - － 脆弱性悪用の対象となる機能が無効化されている
 - － ベンダーが推奨する一時的な回避策(ワークアラウンド)が講じられている
 - － 対象となる情報機器が適用範囲内のネットワークから切り離されている

- 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(例：IPS)が導入されている

評価基準 No. 4-4-4-2 関連

■ 「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」のアップデート実施に際して、どのような方法が許容され得るのか？

- ・ 評価基準 No.4-4-4-2 では、CVSS の基本値が 7.0 以上等の脆弱性について、原則として 14 日以内にアップデートすることを求めている。一方で、近時公開されている脆弱性情報の量やそれらへの対応にあたりシステムの稼働に関して生じ得る影響等を踏まえると、該当するすべての脆弱性に対して期限内に対応することが現実的に難しいことも想定される。
- ・ 他方、CVSS の基本値で「重大」や「高リスク」と判定された脆弱性のうち、実際に悪用される脆弱性は非常に限られているという報告²⁴もある。そのような状況を踏まえると、CVSS の基本値等だけでなく脆弱性悪用状況等の情報も加味することで、本基準の対象となる脆弱性のうちより緊急度が高いものを特定し、優先的に期限内の対応を行う運用が、より効率的かつ効果的なアプローチとして許容され得るものと考えられる。
- ・ 本基準の対象となる脆弱性のうちより対応の緊急度が高いものの特定に当たっては、以下に例示する国内外の公的機関等が発出する情報源のいずれか又は複数を参照することが考えられる。
 - IPA「重要なセキュリティ情報」(<https://www.ipa.go.jp/security/security-alert/index.html>)
 - JPCERT/CC「注意喚起」(<https://www.jpcert.or.jp/at/2026.html>)
 - CISA「KEV Catalog」(<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>)
 - ENISA「European Union Vulnerability Database」(<https://euvd.enisa.europa.eu/>) 等
- ・ なお、CVSS の基本値が 7.0 以上でありかつ、情報公開時点で攻撃が観測されている又はその蓋然性が高いと考えられるために上記情報源に掲載された脆弱性については、対象機器のインターネットへの露出状況などに関わらず、14 日以内にアップデートプログラムを適用しなければならない。この場合、14 日に拘らず、さらに短い期間で対応することを検討することが推奨される。
- ・ 他方、CVSS の基本値が 7.0 未満だが、重大な事案において悪用が確認されている脆弱性も存在する。本評価基準においては CVSS の基本値が 7.0 以上という条件を対象の絞り込みに際して課しているが、これは CVSS の基本値が 7.0 未満であるものに対応する必要がないということを意味しない。特に、VPN 機器等の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等の OS 及びファームウェアについては、CVSS の基本値が 7.0 未満であったとしても、ベンダー・IPA・JPCERT/CC・CISA KEV 等で「攻撃可能性・悪用確認」とされた脆弱性を修正するアップデートを可及的速やかに行うことを強く推奨する。
- ・ 上述の情報源における脆弱性情報の公開が、アップデートプログラムのリリースから起算して 14 日よりも後になされる可能性もあるところ、当該脆弱性を 14 日以内のアップデート実施対象に含める必要は必ずしもないと考えられるが、後述する対応計画

²⁴ 例えば、以下では CVSS の基本値で「重大」や「高リスク」と判定された脆弱性のうち、実際に悪用される脆弱性は全体の 4%と報告されている。

(https://www.cisa.gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf)

における対応期限をより短く設定し直すなど、適切な対応を行うことが望ましい。

- また、優先度判定の結果として、対応期限を 15 日又はそれよりも長い期間で設定する場合、必然的に当該脆弱性を悪用したインシデント発生リスクも高まることから、要求事項 No.6-1-1 等で定めるインシデント対応体制の更なる強化（例：指示・連絡システムを強化する、モニタリング頻度を上げる等）を併せて進めることが望ましい。

■ 「脆弱性悪用のリスクを低減する対策等」として、どのようなものがあるか？

- 「脆弱性悪用のリスクを低減する対策等」として、具体的には次のような対策等が講じられている必要がある。
 - 脆弱性悪用の対象となる機能が無効化されている
 - ベンダーが推奨する一時的な回避策(ワークアラウンド)が講じられている
 - 対象となる情報機器が適用範囲内のネットワークから切り離されている
 - 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(例：IPS)が導入されている
- 上述の考え方に基づき対応期限を 15 日又はそれよりも長く設定する脆弱性については、「脆弱性悪用のリスクを低減する対策等」に列挙するもののほか、アップデートプログラムの適用に向けた対応計画を策定し、当該計画に沿ってアップデートを行う措置も有効なものとして許容され得る。対応計画を作成するに当たっては、攻撃の段階や対象機器のインターネットへの露出状況などの情報を踏まえて対応期限を決定し、かつ、脆弱性情報公開時点においてリスクを受容し、すぐに対応しないと判断したものも含めて漏れなく対応履歴を記録・追跡することが重要であり、例えば以下のように記録することが考えられる。この場合であっても、後日、攻撃が観測されることがあるため、その際に対応計画を見直すことができるよう備えることが重要である。

識別子	対象機器・ソフトウェア	CVSS 基本値	...	対応期限・時期	対応履歴
CVE-XXXX-XXXX	XXX	9.0	...	2026/XX/XX	2026/XX/XX 実施
CVE-XXXX-XXXX	XXX	7.5	...	次期更改時	

- そのほか、脆弱性の悪用によって最終的に生じる被害を最小限に抑える観点から、多層防御の考え方にに基づき、被害を早期に検知するための対策や、機密情報の流出や不正通信を防ぐための対策等を併せて講じることが望ましい。

評価基準 No. 4-4-4-3 関連

■ 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とは具体的に何を指すか？

- 登録希望組織が決定した適用範囲内において、脆弱性を悪用された場合に登録希望組織の IT 基盤に対する攻撃の起点となり得る機器であり、外部から直接アクセス可能な VPN 機器、ルータ、ファイアウォールその他これらに類する通信制御機能を有する機器が該当する。なお、No.4-4-4-3 については、第三者評価に当たり技術検証を実施する。詳細は「★4 技術検証ガイド」第 2 部 登録希望組織編を参照すること。

(5)マルウェア感染からの保護 [No.4-4-5]**【要求事項】**

システムをマルウェア感染から保護すること。

【評価基準】

段階	No.	評価基準
★3	4-4-5-1	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。
	4-4-5-2	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。
	4-4-5-3	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。
★4	4-4-5-4	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。
	4-4-5-5	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。

【解説】評価基準 No. 4-4-5-1 関連

■ マルウェア対策ソフトの導入対象としてどのような機器が考えられるか？

- ・ マルウェア対策ソフトウェアの導入対象としては、従業員等が利用するパソコンのほか、ファイルサーバ、メールサーバ及び業務システムを稼働させるサーバ（UNIX サーバを含む）等、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が考えられる。

評価基準 No. 4-4-5-2 関連

■ マルウェア対策ソフトのスキャン範囲及び頻度とは具体的には何か？

- ・ スキャン範囲とは、マルウェア対策ソフトにおいてどの範囲までスキャンを実施するかを指す。一般的なマルウェア対策ソフトでは、デバイスでよく使用される領域のみのスキャンを行うクイックスキャン（簡易スキャン）及びすべてのファイル等を対象にスキャンを行うフルスキャン（完全スキャン）の機能を備えていることが多い。
- ・ スキャン範囲によってはスキャンに時間がかかる場合も考えられるため、機器の性質やリスクを考慮したうえで、各社でスキャン範囲とその実行頻度を定め、マルウェア対策ソフトを設定しておく必要がある。
- ・ また、ファイルのダウンロード、作成、実行などの動作が発生したタイミングで都度スキャンを行うリアルタイムスキャン機能を有する場合は、当該機能の有効化も有効である。

評価基準 No. 4-4-5-3 関連

■ “ベンダーの推奨に従ってアップデートする”とは具体的に何を意味するか？

- ・ パターンファイルとは、既知のマルウェアのデータパターンが記録されたファイルのことを指す。パターンマッチング方式のマルウェア対策ソフトでは、対象ファイルとパターンファイルとの比較によりマルウェアを検出することが可能となるため、マルウェア感染防止の観点では、パターンファイルを最新化しておくことが重要である。
- ・ 一般的なマルウェア対策ソフトでは、推奨されるパターンファイルの更新頻度（多くは自動更新）が設定されており、当該推奨頻度に基づきパターンファイルを常に最新化しておく必要がある。

評価基準 No. 4-4-5-4 関連

- 「不正な Web サイトへのアクセスを制限」するには、こういったフィルタリング方式を導入すればよいか？
 - ・ 次のような方式のものを導入することが考えられる。
 - － Web サイトの URL をあらかじめ登録することで制限する方式
 - － Web サイト内の各ページの内容（コンテンツ）で制限する方式
- 「不正な Web サイトへのアクセスを制限」するには、こういった装置・サービスを導入していればよいか？
 - ・ 次のような Web フィルタリング機能を持つ装置・サービスを導入することが考えられる。
 - － パソコンにインストールしたソフトウェアによるフィルタリング
 - － ネットワーク上に設置されたセキュリティ機器によるフィルタリング（ファイアウォール等）
 - － クラウドサービスを利用したフィルタリング

評価基準 No. 4-4-5-5 関連

- 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として、具体的にはどのようなことを実施すればよいか？
 - ・ メールゲートウェイのマルウェアチェック機能としては、以下のような機能が挙げられる。
 - － スпамメールのフィルタリング（スパムメール対策）
 - － メール添付ファイルのスキャンや除去（マルウェア感染対策）
 - － メール内のリンクのスキャンや除去（フィッシング攻撃対策）
 - ・ 具体的な実装方法としては、上記のようなマルウェアチェック機能を有するメールゲートウェイを実装するほか、クラウドメールサービスにおいてはマルウェアチェック機能が標準で搭載されている場合が多く、当該機能の利用も有効である。

No.4-5 技術インフラのレジリエンス

(1)ネットワーク境界防護 [No.4-5-1]

【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。

【評価基準】

段階	No.	評価基準
★3	4-5-1-1	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。
	4-5-1-2	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。
	4-5-1-3	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。
	4-5-1-4	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。
	4-5-1-5	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。
	4-5-1-6	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。
	4-5-1-7	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。
★4	4-5-1-8	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。
	4-5-1-9	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。

【解説】

評価基準 No. 4-5-1-1 関連

■ 「デフォルトの管理パスワード」とは何か？

- 機器の出荷時に設定されている初期パスワードや、製品マニュアル等に記載されている標準の管理用パスワードを指す。このようなパスワードは、容易に推測されるおそれがあることから、No.4-5-1-3に基づき、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したパスワードに変更する必要がある。

- ・ リモートアクセスを完全に無効化している場合は、評価基準上はパスワードの変更は求められていないものの、パスワード漏えいのリスクを考慮し、デフォルトの管理パスワードについては変更することが望ましい。

評価基準 No. 4-5-1-2 関連

■ 手順は機器ごとに定める必要があるか？

- ・ 同一の管理方法や運用方法を採用している機器については、共通の手順として定めることも可能である。

評価基準 No. 4-5-1-3 関連

■ パスワード設定等に関する評価基準とは具体的に何か？

- ・ 主に、評価基準 No.4-1-5-3 に対応する必要がある。

評価基準 No. 4-5-1-4 関連

■ "認証されていないインバウンド通信"とは何か？

- ・ 社内ネットワークへ通常アクセスが想定されていない IP アドレスからのインバウンド通信を指す。そのような通信については原則としてすべて遮断する（Deny All）よう、ファイアウォール・ルールを設定する必要がある。

評価基準 No. 4-5-1-5 関連

■ どのようなファイアウォール・ルールを定めればよいのか？

- ・ ファイアウォール・ルールの定め方として、ブラックリスト方式（アクセスを拒否する送信元のリストを用意し、そのリストに含まれる送信元からのアクセスを拒否する方式）とホワイトリスト方式（許可する送信元のリストを用意し、そのリストに含まれる送信元からのアクセスのみを許可する方式）が考えられるが、少なくとも No.4-5-1-4 に基づき、認証されていないインバウンド通信は遮断する（Deny All）ようなファイアウォール・ルールを定めている必要がある。
- ・ ファイアウォール・ルールを定めるに当たっては、ベンダー推奨の設定等も参照することが考えられる。

評価基準 No. 4-5-1-6 関連

■ 不要になったファイアウォール・ルールとは何か？

- ・ 例えば、IP アドレスの変更により使用しなくなったファイアウォール・ルールが該当する。そのようなファイアウォール・ルールを放置すると侵入リスクとなり得ることから、速やかに削除又は無効化を行うことが望ましい。

評価基準 No. 4-5-1-7 関連

■ 信頼できる IP アドレスとは具体的に何か？

- ・ 自社又は運用・保守を担当する委託先で使用する IP アドレスを指す。また、組織で複数の IP アドレスを使用する場合は、それらのなかでもファイアウォール・ルールの変更を行う担当者が利用する IP アドレスを指す。

■ アクセスを制限するにはどのような方法があるか？

- ・ アクセス制限の方法として、ブラックリスト方式（禁止する IP アドレスのリストを用意し、そのリストに含まれる送信元からのアクセスを拒否する方式）とホワイトリスト方式（許可する IP アドレスのリストを用意し、そのリストに含まれる送信元からのアクセスのみを許可する方式）がある。
- ・ 動的 IP アドレスの場合は、IP アドレス変更の都度許可又は拒否リストを更新する方法のほかに、例えば、VPN 接続により IP アドレスを固定化する、DNS で割り当てたホスト名にて制限する、IP アドレスの変動範囲を範囲指定するなどの方法が考えられ

るが、例えば IP アドレスの変動範囲を範囲指定する方法の場合は範囲内の他の IP アドレスを許可してしまうなどのリスクがあり、そのようなリスクを考慮したうえで制限方法を検討する必要がある。

評価基準 No. 4-5-1-8 関連

- ソフトウェアファイアウォールとして、具体的にはどのようなものがあるか？
 - ・ 例えば、Windows における Windows ファイアウォールのようなパソコン及びサーバに OS 標準で搭載されているファイアウォール機能が該当する。
 - ・ なお、ソフトウェアファイアウォールの設定は OS ベンダーが推奨する設定を実施することが望ましいが、変更のリスクを考慮の上、システム、ソフトウェア等の都合上必要に応じて推奨設定から変更することが必要である。

評価基準 No. 4-5-1-9 関連

- 「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」とは、具体的にはどのような状態になっていればよいのか？
 - ・ サーバ内外のネットワークについて、物理的又は論理的な制御を行う必要がある。前者は、文字通り、ネットワーク回線が分かれていることである。後者は、回線上は同一だったとしても、その中を流れるデータが仮想的に別区画として管理されている状態である。
 - ・ いずれの方法をとった場合においても、ネットワーク図等においてどのような制御又は分離を行ったかを把握していることが望ましい。
- ＜物理的な制御の例＞
 - － 重要な機密情報を扱うサーバについて、通常のネットワークとは別の回線・機器により構成する。この場合において、通常のネットワークとの間で通信を行う必要があるときは、その境界にファイアウォール等を設置し、内外の通信を必要最小限に制御する。
- ＜論理的な制御の例＞
 - － 社外公開サーバは DMZ と呼ばれる別セグメントに配置する。
 - － 同一の物理回線上において、VLAN 等により通信を分離する。
 - － クラウドサービス (IaaS/PaaS) 上にサーバを設置する場合は、仮想ネットワーク (VPC 等) やサブネットの分割により専用のセグメントを構成し、セキュリティグループ、ネットワーク ACL、クラウド事業者が提供するファイアウォールサービス等により、セグメント内外のアクセスを必要最小限に制限する。
 - － サーバや仮想マシン (VM) などの単位で通信を制御し保護する (マイクロセグメンテーション)。

No.5 攻撃等の検知

「攻撃等の検知」は、セキュリティに係る攻撃及び侵害の可能性を発見し、分析することを目的として実施するものであり、以下2つの中分類に分けられる。

別表5 「攻撃等の検知」における中分類及びその目的

中分類	各分類の目的
継続的監視	異常、侵害の痕跡その他の潜在的な有害事象を発見するために、資産を監視すること。
有害事象の分析	異常、侵害の痕跡その他の潜在的な有害事象を、事象を特徴付け、セキュリティインシデントを検知するために分析すること。

No.5-1 継続的監視

(1)ネットワーク接続・データの監視 [No.5-1-1]

【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。

【評価基準】

段階	No.	評価基準
★3	5-1-1-1	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すること。
	5-1-1-2	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。
	5-1-1-3	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。

【解説】

評価基準 No. 5-1-1-1 関連

- 「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」とは何か？
 - ・ 社内外ネットワークの境界又は端末のいずれに設置するかによって異なる。
社内外ネットワークの境界に設置する場合は IPS 又は IPS 機能を有するネットワーク機器（UTM 等）を設置することとなる。端末に設置する場合は、EDR のような端末において不正アクセスを検知・遮断できるようなソフトウェアを導入することとなる。このうち社内から不正なサーバへの通信については、プロキシ、セキュアウェブゲートウェイ、DNS フィルタリング等による方法もある。これらをクラウドサービスとして利用する場合を含む。
- 評価基準 No.5-1-1-1 で端末に導入する方法を選択した場合、評価基準 No.5-1-1-2 及び評価基準 No.5-1-1-3 の対象は何か？
 - ・ 評価基準 No.5-1-1-2 の「ネットワーク機器のログ及びアラート」及び評価基準 No.5-1-1-3 の「ネットワーク機器又はサービス」には、評価基準 No.5-1-1-1 で導入した仕組みを含む。端末に導入した場合は、当該ソフトウェアが対象となる。

評価基準 No. 5-1-1-3 関連

■ 「インシデントの速報レポート」とは何か？

- ・ 一般的には、通信ログやセキュリティイベントを基に、不審な通信、異常な挙動、不正アクセスの試行、ブロックされた危険な通信等の情報を記録し、セキュリティインシデントへの該当性を分析・判断するために作成又は通知されるレポートをいう。
- ・ 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は、セキュリティインシデントへの該当性が未確定の事象を含め、通信やイベントの状況を記録するとともに、当該情報を分析・判断できるレポートを作成又は通知する機能を有している必要がある。

(2)情報機器及びソフトウェアの挙動監視 [No.5-1-2]**【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。

【評価基準】

段階	No.	評価基準
★4	5-1-2-1	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すること。
	5-1-2-2	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。
	5-1-2-3	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。

【解説】**評価基準 No. 5-1-2-1 関連****■ 社内で利用を許可するソフトウェアの一覧はどのように定めればよいのか？**

- ・ 社内で利用を許可するソフトウェアの一覧を定める際には、以下の事項を考慮して行うことが考えられる。
 - － ソフトウェアベンダーによるセキュリティパッチ等のサポートが提供されていることや、セキュリティベンダー等の第三者が提供するソフトウェアの脆弱性等に関する情報を確認する。
 - － 出所不明なソフトウェアは利用しないよう定める。
 - － 外部と通信を行う機能を有することが明確なものの又は外部との通信の有無について利用規約により確認できるものについては、当該機能によって使用するプロトコル（バージョンを含む。）、ポート、暗号化の有無を事前に確認する。プロトコルのバージョンについては、TLS などにおいて脆弱なバージョンを使用していないかなども確認する必要がある。
 - － インストール時に、他のソフトウェアのインストールの同意を求めるものについては、当該ソフトウェアの利用の可否についても併せて定める。
 - － ブラウザを含め個々のソフトウェアにおける機能拡張用のソフトウェア（いわゆる、プラグインやアドオン）の利用の可否についても併せて定める。
- ・ なお、利用を許可するソフトウェアの一覧の作成に際しては、ソフトウェアのバージョンを含めることが重要である。また、IT 資産管理ツールの利用も有効である。利用を許可するソフトウェアが膨大な場合、ソフトウェアを個別に列挙する方法に依らず、例えば「出所が明らかかつサポートが提供されている最新バージョンの表計算ソフトウェア」という具合に、ソフトウェアの種別毎に利用条件を定義する方法も考えられる。

評価基準 No. 5-1-2-2 関連**■ 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はどのように点検すればよいのか？**

- ・ 一般的には資産管理ツールを用いて、各パソコンにおけるソフトウェアにおいて利用を認めるソフトウェア以外のソフトウェアがインストールされていないかどうかを確認する方法が挙げられる。
- ・ その他、パソコンにおけるログを確認し、不明なソフトウェアをインストールするよ

うな不審な挙動がないかどうか確認することも考えられる。また、個々のパソコンについて、設定画面にてソフトウェアのインストール状況を個別に確認する方法でも差し支えない。

評価基準 No. 5-1-2-3 関連

■ 「仮想環境上で安全性を確認する仕組み」とは何か？

- ・ いわゆるサンドボックスのことを指す。サンドボックスとは、攻撃されても影響を与えない仮想環境を用意し、不審なファイル等を仮想環境にて動作させ異常がないかを分析するものである。当該仕組みを導入するためには、サンドボックス機能を備えたシステムやソフトウェアを導入することが必要となる。
- ・ なお、本評価基準はマルウェア対策ソフトのリアルタイムスキャンの実行によっても適合し得るものであり、サンドボックスの導入を必須とするものではない。

No.5-2 有害事象の分析

(1)セキュリティインシデントのレベルごとの対象範囲 [No.5-2-1]

【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。

【評価基準】

段階	No.	評価基準
★4	5-2-1-1	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、役員、従業員、派遣社員及び受入出向者に周知すること。
	5-2-1-2	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。

【解説】

評価基準 No. 5-2-1-1 関連

■ 「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」としてどのようなものを定めればよいのか？

- ・ セキュリティインシデントといっても、事業に及ぼす影響度合いは様々である。少なくとも、セキュリティインシデントに対する対応を円滑に実施するため、自社内でセキュリティインシデントをレベル分けし、それぞれのレベルの対象範囲（定義）を定めておく必要がある。

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
- ・ 中小企業の情報セキュリティ対策ガイドライン 付録 5 情報セキュリティ関連規程（サンプル）（IPA）
(<https://www.ipa.go.jp/security/guide/sme/about.html>)

No.6 インシデントへの対応

「インシデントへの対応」は、検知したセキュリティインシデントに関する措置を講じることを目的として実施するものであり、以下1つの中分類に分けられる。

別表6 「インシデントへの対応」における中分類及びその目的

中分類	各分類の目的
インシデント管理	検知したセキュリティインシデントへの対応を管理すること。

No.6-1 インシデント管理

(1)インシデント対応手順 [No.6-1-1]

【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。

【評価基準】

段階	No.	評価基準
★3	6-1-1-1	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
	6-1-1-2	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。
	6-1-1-3	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。
	6-1-1-4	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。
	6-1-1-5	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。
	6-1-1-6	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。

【解説】

評価基準 No. 6-1-1-1 関連

■ 「セキュリティインシデントへの対応手順」には具体的にはどのような内容が盛り込まれていればよいのか？

- ・ 評価基準 No.6-1-1-1 では、①発見報告、②初動、③調査・対応、④復旧、⑤最終報告の5項目を手順に含めるように求めているが、具体的には以下のような項目が盛り込まれていることが望ましい。

（以下例示）

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

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - 組織内 CSIRT 構築の参考資料 インシデント対応マニュアルの作成について (JPCERT/CC)
https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf
 - 中小企業のためのセキュリティインシデント対応の手引き (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_incidenttebiki.pdf

評価基準 No. 6-1-1-2 関連

■ 「社内外組織との連絡先、ルート」を明確化するために重要な観点は何か？

- ・ 有事の際に必要なタイミングで必要なメンバーに連絡がつくことが重要である。そのため、必要な連絡先が網羅されていること、機能するか確認することの2つの観点で確認することが望ましい。
 - <必要な連絡先の網羅>
 - 有事の際に必要な連絡先を漏れなく連絡先として明確にするために、以下の3つのポイントを確認することが望ましい。
 - 社内外からセキュリティ事故の発生報告を受ける窓口が明確になっていること
 - 情報セキュリティ組織内での連絡ルートが確立されていること
 - 情報セキュリティ事故発生時の外部組織の連絡先がリスト化されていること
 - ・ 外部組織の連絡先としては、関連する取引先の連絡先を明確化することはもちろん、協力を仰ぐ外部の専門組織 (JPCERT/CC やセキュリティ企業など) が特に重要となる。加えて、セキュリティ事件・事故発生時の対応手順が明確化されている組織では、手順に記載のある連絡先が網羅されているかという観点でも確認するとよい。
 - ・ また、セキュリティインシデントが不正アクセスによるものである場合には警察やIPAの届出窓口への報告や届出が必要となるほか、セキュリティインシデントにより個人情報の漏えい又はその疑いが発生した場合には、個人情報保護委員会への報告が必要となる。その他、所属する業種・業界を所管する省庁がある場合には、当該省庁への報告が必要となる場合がある。連絡先及び報告・情報共有ルートには、このような関係当局及び所管省庁への報告の観点も盛り込む必要がある。
 - ・ なお、メール・チャット・電話といった連絡手段は、連絡先ごとに想定しうる用途に応じて、適したものをそれぞれ確保しておくことが望ましい。

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - サイバーインシデント緊急対応企業一覧 (JNSA)
https://www.jnsa.org/emergency_response/

評価基準 No. 6-1-1-3 関連

■ 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・責任は、どのように定めればよいか？

- ・ セキュリティを統括する役員の役割・責任として、例えば、インシデント発生後の対応方針、対応計画の審議・承認、他の経営層やメディア等に対する対応状況の説明が考えられる。
- ・ セキュリティ担当部署の役割・責任としては、例えば、インシデントの連絡受付、重大度の判断 (トリアージ)、事象の原因分析等が挙げられる。

■ 参考となる資料はあるか？

- ・ 以下の資料が参考となる。
 - － インシデントハンドリングマニュアル (JPCERT/CC)
(https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf)
 - － セキュリティ対応組織の教科書 第3.2.2版 (2026年9月) (ISOG-J)
(https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html)

評価基準 No. 6-1-1-5 関連

■ どのような報告フォーマットを整備すればよいか？

- ・ 以下のような項目について報告できるようなフォーマットであることが望ましい。
 - － セキュリティインシデントの種別 (マルウェア、不正アクセス等)
 - － 被害を受けたシステム、機器等
 - － 被害状況
 - － 発見・対応の経緯
- ・ 上記に加え、インシデントの原因や再発防止策を記載する項目を設けることで、インシデント管理に活用することも考えられる。

評価基準 No. 6-1-1-6 関連

■ 「インシデント事例及びその対応策」はどのように入手すればよいか？

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

■ 「インシデント事例及びその対応策」はどのように共有すればよいか？

- ・ 必ずしも別途の共有の機会を設ける必要はなく、No.4-2-1で実施するセキュリティの意識向上のための教育・研修と併せて実施することも可能である。
- ・ その他、社内ポータルサイトや社内掲示板などを活用し、共有することも考えられる。
- ・ なお、インシデント事例に機微な情報が含まれる場合は、共有範囲等に留意する必要がある。

No.7 インシデントからの復旧

「インシデントからの復旧」は、セキュリティインシデントの影響を受けた資産及び業務を復旧させることを目的として実施するものであり、以下1つの中分類に分けられる。

別表7 「インシデントからの復旧」における中分類及びその目的

中分類	各分類の目的
インシデント復旧計画の実行	セキュリティインシデントの影響を受けたシステム及びサービスの運用可用性を確実にするための復旧活動を実施すること。

No.7-1 インシデント復旧計画の実行

(1)事業継続要件に沿った復旧準備 [No.7-1-1]

【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。

【評価基準】

段階	No.	評価基準
★3	7-1-1-1	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。）
★4	7-1-1-2	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。

【解説】

評価基準 No. 7-1-1-1 関連

■ どのような観点で目標復旧レベルを定めればよいか？

- ・ 目標復旧レベルは、少なくとも次の観点を含めることが考えられる。
 - 目標復旧時間（RTO）：業務を何時間以内に再開するか
 - 目標復旧時点（RPO）：どの時点のデータまで復元するか
 - 復旧対象業務：優先して復旧する業務
 - 復旧方法：待機系、人手による代替、バックアップからの復元

■ システムによる業務継続として、どのような対策を実施すればよいか？

- ・ ランサムウェアに代表されるように、昨今ではデータの暗号化等によりシステムを使用不可能にさせるようなサイバー攻撃が増加しており、このようなサイバー攻撃を想定したシステムの可用性を担保した対策を講じることが重要である。具体的には、例えば例示にあるとおり、メインで使用しているシステム（主系）に加えて、予備機、クラウド環境等により主系が使用できなかった場合に稼働させる予備のシステム（待機系）を整備することが考えられる。

■ 人手による業務継続として、どのような対策を実施すればよいのか？

- ・ 上記のとおりサイバー攻撃によりシステムが使用できなくなった場合は、復旧までの間人手による連絡又は業務の実施が必要となる場合も考えられる。そのような場合を想定し、あらかじめシステムを使用しない人手による手段を整備しておくことが重要である。具体的には、例えば例示にあるとおり、メールやチャットといったシステムを使用した手段ではなく、電話や FAX などのシステムによらない連絡手段を整備しておくことや、システムによる作業指示等を紙の帳票に切り替えて業務の運用を継続することなどが考えられる。

■ システムによる業務継続及び人手による業務継続のいずれの対策も整備しなければならないか？

- ・ システムや業務の性質により、システムによる業務継続又は人手による業務継続を整備することが困難な場合も想定されるため、必ずしもすべての対策を整備する必要はない。ただし、システムの事業継続上の重要度、代替手段の有無、目標復旧レベル等の観点を考慮したうえで、どのような対策を整備すべきかを検討する必要がある。

■ サイバー保険は、事業継続対策として活用できるか？

- ・ サイバー保険は、サイバー攻撃によるシステム停止や情報漏えい等が発生した場合に、事故対応費用、損害賠償費用、営業継続費用等を補償するほか、保険会社によっては事故発生時の専門事業者の紹介、脆弱性情報/脅威情報の提供、教育・訓練等の付帯サービスが提供される場合もある。これらは事業継続に向けた取組を支援する手段として有効であると考えられる。

－ [参考]

サイバー保険 | 企業のための保険ナビ | 日本損害保険協会
[\(https://www.sonpo.or.jp/sme_insurance/cyber-hoken/\)](https://www.sonpo.or.jp/sme_insurance/cyber-hoken/)

評価基準 No. 7-1-1-2 関連

■ バックアップの復元ができることの確認は、どのような頻度で実施すればよいのか？

- ・ 例えば以下のような時点において実施することが考えられる。(以下例示)
 - － システム構築時
 - － システム構成の変更時
 - － 定期的 (例えば年 1 回など、事業継続上の重要度に応じて周期を定める)

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

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

付録1 用語集

	用語	説明	該当箇所 (評価基準 No.)
あ	アクセス権	システムの利用者又は利用者のグループに対して設定される、そのシステムの利用権限のこと。アクセス制御に利用され、設定に応じてシステムの利用を許可したり拒否したりする。	2-1-5-1 3-1-4-5 4-1-1-4
	アップデートプログラム	OS やソフトウェアの一部又は全部のプログラムを更新するプログラムのこと。更新プログラムやパッチともいう。	4-4-4-2
	アラート	機器・サービスにおいて脅威を検出した際に発されるシグナルのこと。	5-1-1-2 5-1-1-3 5-2-1-2
	暗号化	特定のアルゴリズムを使用し、第三者が読み取ることができないように情報を変換すること。	4-3-1-1 4-3-1-2
	インバウンド通信	外部から社内ネットワーク等の内部ネットワークへ向かう通信のこと。	4-5-1-4 4-5-1-5
	遠隔地バックアップ	災害時に備えてバックアップデータを遠隔地に保管すること。	4-3-4-2
か	外部記憶媒体	コンピュータ本体の外部に接続し、プログラムやデータを長期保存・持ち運びするための記録メディアのことをいい、具体的には USB メモリ、メモ리카ード、CD・DVD 等を指す。要求事項・評価基準においては、「外部記録媒体」も同義として扱う。	3-1-4-7 3-1-4-8 4-1-9-1 4-1-9-2 4-1-9-3 4-4-1-2
	外部情報サービス	自社の外部（社外）にあるインターネット経由のサービスやクラウド、Web サイトなどを通じて提供される情報サービスのこと。取引先等から提供されるものを含む。	3-1-3-1 3-1-3-2
	仮想サーバ	1 台のコンピュータについて、中央演算装置（CPU）やメモリ、ディスクをまとめて仮想的に複数の領域として分割し、それぞれがあたかも 1 台のコンピュータのように複数台の仮想的なコンピュータとして、それぞれに異なる別の OS やソフトウェアを同時に実行させる技術を使用したサーバのこと。	3-1-1-2
	可搬媒体	運搬可能な情報機器のこと。具体的には、パソコン、スマートデバイス、カメラ及び外部記憶媒体を指す。	4-1-9-1 4-1-9-2 4-1-9-3

	用語	説明	該当箇所 (評価基準 No.)
か	機密情報	企業が保有している情報のうち外部への開示が予定されない情報のこと。開示されれば企業に損失が生じる恐れがある。	1-2-3-3 2-1-1-3 2-1-2-1 2-1-3-1 2-1-4-1 2-1-5-1 3-1-3-2 3-1-4-5 3-1-4-6 3-1-5-1 4-3-1-1 4-5-1-9
	脅威	システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。	3-2-1-1 3-2-1-2 3-2-1-3 3-2-1-5 4-4-3-2
	脅威情報	サイバー脅威への対応に役立つ可能性のある、攻撃者の傾向、攻撃技術及び攻撃手法・手順の分析結果等の情報のこと。	3-2-1-1 3-2-1-2 3-2-1-3 3-2-1-5
	クラウドサービス	自組織内で情報機器を保有しない形態の情報サービスであり、外部情報サービスに含まれる。主にインターネット上で提供される。	2-1-1-1 4-1-3-2 4-1-3-5 4-1-5-1 4-3-2-1 4-4-3-1

	用語	説明	該当箇所 (評価基準 No.)
さ	定める	ルール等を文書化し、当該ルール等に基づく運用を行うこと。	1-1-1-1 1-1-1-2 1-2-1-1 1-2-1-2 1-2-3-1 1-3-1-1 2-1-3-1 2-1-4-1 3-1-1-3 3-1-4-1 3-1-5-1 3-2-1-1 3-2-1-2 3-2-1-3 4-1-2-1 4-1-5-1 4-1-5-2 4-1-5-3 4-1-5-4 4-1-6-1 4-1-6-2 4-1-7-1 4-1-7-3 4-1-7-4 4-1-8-1 4-1-9-1 4-1-9-2 4-4-1-6 4-5-1-2 6-1-1-1 6-1-1-2 6-1-1-3
	事業法	業種ごとの基本的な事業要件を定める法律の総称のこと。例えば、電気通信事業法、銀行法、保険業法、建設業法などが挙げられる。	1-1-1-1
	システム管理者	管理者権限を有し、管理・運用、利用者へのサポート等を実施する、システムごとに定められた者。	4-1-2-1 4-1-7-4
	システム責任者	システムごとに定められた、システム管理・運用について責任を有する者のこと。例えば、システムを所管する部署の管理職などをシステム責任者として定めることが考えられる。	4-1-2-1
	自動実行(auto-run)/自動再生(auto-play)	端末に接続された外部記憶媒体に保存されたプログラムを自動的に実行させる機能のこと。	4-4-1-2

	用語	説明	該当箇所 (評価基準 No.)
さ	社内ルール	登録希望組織において定める、規程、指針、手順書などの文書化されたルールの総称。	1-1-1-1 1-1-1-2 1-1-1-3 4-1-5-2 4-1-5-3 4-1-5-4 4-1-6-1
	重要な機密情報	機密情報のうち、漏えいした場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいと登録希望組織が定めたもの。	2-1-3-1 3-1-4-3 4-1-3-2 4-1-3-5 4-1-7-3 4-1-7-4 4-1-7-5 4-1-7-6 4-3-1-2 4-3-4-2 4-5-1-9
	重要なシステム	侵害された場合のビジネスへの影響度が高いと登録希望組織が定めたシステムを指す。なお、少なくとも No.4-4-3-1 のログを保管するサーバは、インシデント発生時の調査に用いられセキュリティ上重要であるため、重要なシステムに含める必要がある。	3-1-1-6 7-1-1-1 7-1-1-2
	守秘義務	職務上知った秘密を他人に漏えいしてはいけないという義務のこと。	1-2-3-1 1-2-3-2 1-2-3-3 1-2-3-4
	遵守状況	社内ルールについて、どの程度守られているかを示す状況のこと。また、遵守状況の点検とは、従業員等において社内ルールがどの程度守られているかを確認することを指し、その方法としては、例えば対象となる社内ルールの遵守状況についてチェックリストやアンケートなどを従業員等に配布し、回答させることなどが挙げられる。	3-1-1-4 3-1-5-3 4-1-9-3

	用語	説明	該当箇所 (評価基準 No.)
さ	情報機器	情報の入出力や保存、処理、伝達などを主な機能や用途とする機器のことをいい、パソコン、サーバ、スマートデバイス及びネットワーク機器を含む。	3-1-1-3 3-1-1-6 3-1-4-5 3-1-4-6 3-1-5-1 3-2-1-4 4-1-3-1 4-1-5-4 4-4-4-1 4-4-4-2
	情報資産	組織が保有している守るべき情報(機密情報、個人情報等)並びに当該情報を取り扱う IT 資産 (情報機器、OS 及びソフトウェア、ネットワーク機器その他の IT に関する資産)。	2-1-1-3
	情報セキュリティ委員会	組織全体の情報セキュリティをマネジメントするために設置される全社横断的な組織のことをいい、各部門の責任者から構成されることが多い。一般的にはセキュリティ基本方針の策定・改定、セキュリティ基本方針の遵守状況の評価、セキュリティ監査結果の評価及びセキュリティ教育の計画・実施などの活動を担う。	1-2-1-4
	シンククライアント	情報システムで、従業員等が利用するコンピュータ(クライアント)に最低限の機能だけを持たせて、サーバ側でアプリケーションソフトやファイル等の管理を可能にするシステムの総称。また、そのようなシステムを実現するための、機能を絞ったクライアント用コンピュータのことをいう。	3-1-1-1
	スマートデバイス	パソコン以外であって、持ち運びしやすい可搬性の高い端末のこと。通信機能を有していることが前提となり、具体的にはスマートフォン、タブレット端末、その他ネットワーク通信及び情報処理機能を有する小型端末が対象となる。	3-1-1-5
	脆弱性	プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。	1-2-2-1 3-2-1-1 3-2-1-2 3-2-1-3 3-2-1-4 3-2-1-5 4-4-2-1 4-4-4-2 4-4-4-3

	用語	説明	該当箇所 (評価基準 No.)
さ	脆弱性情報	脆弱性の性質、特徴等に関する情報をいう。各製品ベンダーからの公表のほか、JVN 等の脆弱性情報データベースから、情報収集することができる。	3-2-1-1 3-2-1-2 3-2-1-3 3-2-1-5
	セキュリティインシデント	情報資産に内在した脆弱性が情報資産を取り巻く様々な脅威により突かれ、顕在化したもの。要求事項・評価基準においては、「インシデント」も同義として取り扱う。	2-1-4-1 4-2-2-1 4-2-2-3 5-1-1-2 5-2-1-1 6-1-1-1 6-1-1-2 6-1-1-3 6-1-1-4 6-1-1-5 6-1-1-6
	セキュリティ対応方針	組織が情報資産を保護し、情報セキュリティリスクに対処するための基本的な考え方や方向性を示す文書。	1-3-1-1 1-3-1-2 1-3-1-3 1-3-1-4
	相関分析	複合的なログなどを分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法のこと。	1-2-2-2
	ソフトウェア	情報システムを動かすために利用されるプログラムのこと。要求事項・評価基準においては、OS を含まない。特定の作業を行うために使用されるアプリケーションを指すことが多い。	3-1-1-3 4-4-1-1 4-4-1-6 4-4-2-1 4-4-4-1 4-4-4-2 4-4-5-1 5-1-2-1 5-1-2-2
	ソフトウェアファイアウォール	個々の端末にインストールされる、ファイアウォール機能を有するソフトウェアのこと。	4-5-1-8
た	待機系	システムの信頼性や耐障害性を高めるために同一のシステム構成を複数用意する場合において、メインで稼働しているシステムに障害が発生した際に、処理を引き継ぐシステムのこと。	7-1-1-1

	用語	説明	該当箇所 (評価基準 No.)
た	多要素認証	「知識情報」、「所有情報」、「生体情報」のうち、複数を組み合わせてユーザ認証を行う方式。MFA (Multi-Factor Authentication)。 要求事項・評価基準では、No.4-1-3-3において、多要素認証に用いる認証要素の例を以下のとおり示している。 - 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) ※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。	4-1-3-2 4-1-3-3 4-1-3-4 4-1-3-5 4-1-5-3 4-4-1-5 4-4-3-2 4-5-1-7
	デフォルトユーザ ID	パソコンやサーバにおいて初期値として利用可能な ID のこと。具体的には、Administrator、user、root などが該当する。	4-4-1-5
	点検する	要求事項・評価基準において把握することが求められる情報について、更新漏れ等の不備がないか確認を行い、必要に応じて当該情報の更新等を実施することをいう。例えば、情報資産管理台帳に記載されている又は情報資産管理ツールで管理している各情報資産について、その所在有無、所在場所、利用実態等について棚卸を行うことが該当する。	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 4-1-9-3 4-2-1-5 4-2-2-3 5-1-2-2 6-1-1-4
	トラフィック	通信回線やネットワーク上で送受信される信号やデータのこと。	4-4-4-1

	用語	説明	該当箇所 (評価基準 No.)
た	取引先	自組織が何らかの取引を行っている相手の組織の総称であり、顧客、取引先、関係会社、クラウドサービス提供者を含む。	1-1-1-1 2-1-1-1 2-1-1-3 2-1-2-1 2-1-3-1 2-1-4-1 2-1-5-1 4-3-3-1 4-4-3-1 7-1-1-1
な	認証サーバ	システムやネットワークへの接続を試みた人物が本人であるかどうかを確認する（認証を行う）サーバ。具体例として、Active Directory (Windows) などがある。	4-4-3-1 4-4-3-3
	ネットワーク機器	ルータ、スイッチ、ハブ等、情報通信ネットワークを構築する際に用いられる機器。	3-1-2-2 4-1-2-1 4-1-2-8 4-4-1-3 4-4-4-3 4-5-1-1 4-5-1-2 4-5-1-3 4-5-1-4 4-5-1-5 4-5-1-6 5-1-1-2 5-1-1-3 5-2-1-2
	ネットワーク図	通信に関わる機器や配線を図化した図面のこと。ネットワーク構成図ともいう。	3-1-2-3 3-1-2-4
は	ハイパーバイザ	サーバ仮想化などで利用される、コンピュータを仮想化するためのソフトウェアのこと。	3-1-1-2
	パスワード管理アプリ	ログインに必要な ID・パスワードを保存・管理するためのアプリのこと。	4-1-6-1

	用語	説明	該当箇所 (評価基準 No.)
は	パターンファイル	マルウェア対策ソフトがマルウェアを発見するために使用するデータのこと。マルウェアは日々新しいものが出現しているため、最新のマルウェアに対応するためには、パターンファイルを常に最新のものに更新しておく必要がある。パターンファイルは、マルウェア対策ソフトによっては「マルウェア（ウイルス）定義ファイル」や「マルウェア（ウイルス）検知用データ」、「シグネチャ」等と呼ばれ名が異なる。	4-4-5-3
	バックアップ	データを磁気テープなどの別の記憶媒体に保存して、大事なデータの複製を作っておくこと。又は、その複製データ。	4-3-4-1 4-3-4-2 4-3-4-3 7-1-1-2
	ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器。	4-4-3-1 4-5-1-1 4-5-1-2 4-5-1-3 4-5-1-4 4-5-1-5 4-5-1-6
	ファイアウォール・ルール	ファイアウォールにおいて設定する、通信の許可・遮断の判断基準のこと。	4-5-1-5 4-5-1-6 4-5-1-7
	不正アクセス	本来はアクセス権限を持たない者が、サーバやシステムなどの内部へ侵入する行為のこと。	5-1-1-1
	プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順等の規則のこと。通信プロトコル又は通信規約とも呼ばれる。	4-4-1-4
	閉域網	インターネットから切り離された独自のネットワークのことをいい、専用線、IP-VPN、広域イーサネットなどが含まれる。	4-4-3-1
	ベンダー	エンドユーザに IT 製品や IT サービスを販売する企業の総称。	4-4-4-2 4-4-5-3
ま	マルウェア	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスやワーム、スパイウェアなどが含まれる。	4-2-1-3 4-3-2-1 4-4-5-1 4-4-5-2 4-4-5-3 4-4-5-5 5-1-2-3

	用語	説明	該当箇所 (評価基準 No.)
ま	メールゲートウェイ	迷惑メール、マルウェア、フィッシング詐欺などの脅威から保護し、同時に誤送信や情報漏えいを防ぐ役割を持った機器等のことを指す。一般にメール送受信経路に設置され、本項目で求められるようなマルウェアチェック機能を導入するのに適している。	4-4-5-5
	メールサーバ	メールの送受信の役割を担うサーバのこと。	4-4-5-5
	目標復旧時間	システム障害や災害により業務が中断した際に、いつまでに業務を復旧するかという目標時間のこと。RTO (Recovery Time Objective) ともいう。	7-1-1-2
	目標復旧時点	システム障害や災害により業務が中断した際に、過去のどの時点まで遡ることを許容するかを定めた目標値のこと。これに基づいてバックアップの方法や機器、頻度が決定される。RPO (Recovery Point Objective) ともいう。	7-1-1-2
	目標復旧レベル	システム障害や災害により業務が中断した際に、どの程度の水準まで業務を復旧させるかを定めた目標値のこと。通常、平常時の業務水準を 100%とした時の業務遂行能力の割合で示す。RLO (Recovery Level Objective) ともいう。	7-1-1-1
や	ユーザ認証	システム、サービス等を利用しようとする者が、あらかじめ登録された本人であることを確認する行為のこと。	4-1-5-2 4-1-5-3 4-1-5-4
ら	リアルタイムスキャン	ファイルやプログラムの動作などを常時監視し脅威を検出する、マルウェア対策ソフトの機能のこと。	5-1-2-3
	リストア	障害発生時に、取得しておいたバックアップから、正常稼働状態にデータを戻すこと。	4-3-4-3 7-1-1-2
	リモートアクセス	遠隔地から公衆回線網やインターネット等を利用して社内の情報機器に接続すること。	4-5-1-1
	ルータ	ネットワーク上を流れるデータを他のネットワークに中継する機器。主に LAN と WAN の中継に用いられる。	4-5-1-1 4-5-1-2 4-5-1-3
	ログ	コンピュータが保有するユーザの接続時刻や処理内容などを記録したファイルのこと。	1-2-2-2 4-4-3-1 4-4-3-2 4-4-3-3 5-1-1-2

	用語	説明	該当箇所 (評価基準 No.)
ら	ログオン	ID、パスワードその他の認証情報を用いて、情報機器、システム又はサービスの利用を開始すること。本制度においては、「ログイン」も同義として取り扱う。	4-1-4-1 4-1-4-2
B	BYOD	従業員が個人保有の機器を使って、業務に使用すること。Bring Your Own Device の略。	4-1-9-1 4-1-9-2 4-1-9-3
C	CISO	組織内において実効力のあるセキュリティ施策を行うために設置される責任者のこと。サイバー攻撃やセキュリティインシデントの際の判断や対応を行う。Chief Information Security Officer の略称。	1-2-1-1 1-2-1-2 1-4-1-1 6-1-1-3
	CVSS	情報システムの脆弱性に対するオープンで汎用的な評価手法のことであり、ベンダーに依存しない共通の評価方法を提供している。 CVSS 基本値では、各脆弱性の深刻度を 0（低）～10.0（高）の数値で表し、数値が 9.0～10.0 であれば、「緊急（Critical）」に、7.0～8.9 であれば「重要（High）」、などのように分類される。Common Vulnerability Scoring System の略称。	4-4-4-2 4-4-4-3
I	IP アドレス	コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。現在主に使用されている IPv4 の場合は、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので表す。	4-1-3-3 4-4-3-1 4-5-1-7
O	OS	Operating System の略であり、コンピュータの土台を支えている基本ソフトウェアのこと。Windows、macOS、Linux などがある。	3-1-1-1 3-1-1-2 3-1-1-3 3-1-1-5 4-4-1-6 4-4-2-1 4-4-4-1 4-4-4-3 4-5-1-8
P	PIN	本人確認のために用いる本人のみが知り得る番号等のこと。Personal Identification Number（個人識別番号）の略。	4-1-4-2

	用語	説明	該当箇所 (評価基準 No.)
W	Web ゲートウェイ	社内のネットワーク環境からインターネットの Web サイトにアクセスするための通信が経由し、その通信が正しいかどうかの監視、及び危険な通信であればそれを制限する役割を持った機器等のことを指す。一般にインターネットとの出入口に設置され、No.4-4-5-4 にある Web アクセス制限機能を導入するのに適している。	4-4-5-4

改定履歴

日付	改定内容
2026 年 10 月 28 日	初版発行