S C S 評 価 制 度

★3 セルフチェックシート

SCS評価制度の★3は、自己評価にセキュリティ専門家の確認と署名を加えて申請します。本シートは、申請前に自社の対応状況を評価基準の単位で把握するためのチェック表です。★3の26要求事項・81評価基準を全て収録し、各項目に判定例と対策を添えているため、そのまま対策計画の下書きとしても使えます。

使い方

1. 各評価基準について、現在の状況に最も近い欄に印を付けてください。
2. 各項目に判定例と対策を、間違えやすい項目には注意点を添えています。
3. 最終ページの集計欄に記入すると、81項目に対する適合率が算出できます。
4. 適合率は「対応済み」のみを数えます。「一部対応」は不適合として扱ってください。

適合率の目安

85% 以上	★3の水準にほぼ到達。専門家確認に進める段階です。
60 - 84%	基礎は固まっています。準備期間は3〜4か月が目安です。
35 - 59%	対応項目が多く残ります。6か月程度を見込んでください。
35% 未満	個別の対策より先に、体制と方針の決定から着手してください。

※ 本シートは、経済産業省が2026年3月27日に公表した「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」の★3・★4要求事項・評価基準に基づいています。IPAおよび経済産業省による公式の評価ではなく、結果が★3の取得を保証するものではありません。なお本シートはAIを活用して作成しており、内容に誤りが含まれる可能性があります。正確な情報については当社までお問い合わせください。2026年7月時点の情報に基づきます。

対応済み　一部対応　未対応

1 ガバナンスの整備

要求事項3 / 評価基準8

1-2-1 セキュリティ推進活動部門

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

1-2-1-1 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。 ☐ ☐ ☐

対応済み　規程や職務分掌表に、統括役員と担当部署の役割・責任が明記されている
一部対応　担当者は決まっているが、役割・責任が文書化されていない
注意　CISOの設置は必須ではないが、統括する役員を特定できる必要がある

対策　情報セキュリティ管理規程に統括役員と担当部署の条項を設け、職務分掌表に役割・責任・権限を記載する。役員会での任命を議事録に残す。

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。 ☐ ☐ ☐

対応済み　統括役員と担当部署の連絡先リストが文書として存在し、最新である
一部対応　連絡先は把握しているが、リストとして整備されていない

対策　統括役員・担当部署・各拠点責任者の氏名／役職／連絡先を一覧化し、規程の別紙として管理する。人事異動のたびに更新する。

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。 ☐ ☐ ☐

対応済み　直近1年以内に体制と連絡先を点検し、記録が残っている
一部対応　見直してはいるが、頻度が不定期または記録がない
注意　点検した記録が残っていないと、実施していても対応済みと判断しにくい

対策　年間セキュリティ計画に体制点検を組み込み、期日を固定する。点検結果を所定様式に記録し、統括役員の承認を残す。

1-2-3 守秘義務のルール

守秘義務のルールを策定し、遵守させること。

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。 ☐ ☐ ☐

対応済み　就業規則や秘密情報管理規程に、派遣社員・受入出向者を含めた守秘義務を定めている
一部対応　正社員は対象だが、派遣社員・受入出向者が対象に含まれていない
注意　派遣社員・受入出向者が対象から漏れやすい。就業規則だけでは範囲が足りない場合がある

対策　就業規則の服務規律に守秘義務条項を置いたうえで、派遣社員・受入出向者を対象に含む秘密情報管理規程を整備する。派遣元との基本契約の守秘義務条項も確認する。

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。 ☐ ☐ ☐

対応済み　入社時・受入時に守秘義務を説明し、実施記録が残っている
一部対応　書類は渡しているが、説明の場や記録がない

対策　入社時オリエンテーションと社外要員の受入手続に、守秘義務の説明を組み込む。説明資料と受講者名簿（または誓約書の受領記録）を保管する。

対応済み　一部対応　未対応

1-3-1 セキュリティ対応方針の策定

自社のセキュリティ対応方針を策定し、周知すること。

1-3-1-1 自社のセキュリティ対応方針を定めること。 ☐ ☐ ☐

対応済み　情報セキュリティ基本方針を文書化し、経営層が承認している
一部対応　草案はあるが、経営層の承認を得ていない
注意　文書の名称は問われないが、経営層の承認を得ていることが要件

対策　情報セキュリティ基本方針を1〜2ページで作成し、経営会議または取締役会で承認する。承認日と決議内容を議事録に残す。

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。 ☐ ☐ ☐

対応済み　社内ポータル等に最新版を掲示し、派遣社員・受入出向者も参照できる
一部対応　一部の従業員しか参照できない、または最新版がどれか不明
注意　派遣社員・受入出向者も参照できる場所に置く必要がある

対策　社内ポータルや共有フォルダの誰でも見られる場所に最新版を掲示し、版数と改定日を明記する。派遣社員・出向者にも閲覧権限を付与する。

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。 ☐ ☐ ☐

対応済み　改正のたびに全対象者へ周知し、記録が残っている
一部対応　周知はしているが、対象範囲や記録が一部にとどまる

対策　改定時に全社メールや朝礼で周知し、配信ログまたは周知記録を保管する。周知対象に派遣社員・受入出向者を含める。

2 取引先管理

要求事項3 / 評価基準4

2-1-1 取引先とのビジネス又はシステム上の関係

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。

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。 ☐ ☐ ☐

対応済み　取引先・子会社・クラウド提供者が管理するシステムとの接続を、台帳等で把握する仕組みがある
一部対応　主要な取引先のみ把握し、クラウドサービスや子会社が漏れている
注意　クラウドサービス提供者も取引先に含まれる。SaaSの棚卸が漏れやすい

対策　取引先・子会社・クラウド提供者ごとに、接続しているシステム／接続方式／扱うデータを記載した接続台帳を作成する。新規契約時に台帳へ登録する手順を業務フローに組み込む。

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。 ☐ ☐ ☐

対応済み　直近1年以内に把握内容を点検し、記録が残っている
一部対応　随時更新はしているが、定期点検として実施していない

対策　年1回、台帳の全件を関係部署に照会して内容を確認する。確認日・確認者・変更点を台帳の履歴欄に残す。

		対応済み	一部対応	未対応

2-1-2 機密情報の取扱い

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。

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

☐ ☐ ☐

対応済み　業務開始前にNDA等で、定義・利用制限・保管方法・複製可否・第三者提供・返還廃棄まで取り決めている
一部対応　NDAはあるが、返還・廃棄や複製可否など一部の事項が定められていない
注意　一般的なNDAでは「返還又は廃棄」「複製可否」が抜けていることが多い

対策　NDAまたは業務委託契約に、機密情報の定義／利用制限／保管方法／複製可否／第三者提供の可否／返還・廃棄の6点を条項化する。既存契約は覚書で補う。

2-1-4 セキュリティインシデント発生時の役割・責任

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。

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。

☐ ☐ ☐

対応済み　契約書や覚書に、インシデント発生時の双方の役割と責任を明記している
一部対応　連絡はする取り決めだが、役割・責任の分担までは定めていない
注意　NDAとは別に、インシデント発生時の役割分担を明記する必要がある

対策　契約書または覚書に、インシデント発生時の通知期限・調査協力・費用負担・公表の可否など、双方の役割と責任を明記する。

3 リスクの特定

要求事項4 / 評価基準11

3-1-1 情報機器、OS及びソフトウェアに関する情報の把握

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。

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。

☐ ☐ ☐

対応済み　資産管理ツールや台帳で、PC・シンクライアントの製造元・OS・台数を把握できる
一部対応　台数は把握しているが、OSやバージョンまでは追えていない
注意　貸与済みの予備機や休眠端末が台帳から漏れやすい

対策　資産管理ツールまたはExcel台帳で、製造元／モデル／OSバージョン／台数／利用者を管理する。貸与・返却の手続と連動させ、休眠端末も登録する。

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。

☐ ☐ ☐

対応済み　物理・仮想サーバとハイパーバイザを含めて、製造元・OS・台数を把握できる
一部対応　物理サーバのみ把握し、仮想サーバやクラウド上のサーバが漏れている
注意　クラウド上の仮想サーバも対象。オンプレ分だけでは足りない

対策　物理サーバ・仮想サーバ・ハイパーバイザ・クラウド上のインスタンスを同一台帳で管理する。クラウドは管理コンソールの一覧を定期取得して突合する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　導入・設置・ネットワーク接続・パッチ適用を含む管理ルールを文書化している
一部対応　運用は定着しているが文書化していない、または一部の事項しか定めていない

対策　情報機器管理規程を作成し、導入・設置・ネットワーク接続・パッチ適用の各手順と承認者を定める。持出しと廃棄の手順も併せて規定する。

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。	☐	☐	☐

対応済み　直近1年以内にルールの遵守状況を点検し、記録が残っている
一部対応　気づいたときに確認しているが、定期点検の記録がない
注意　ルールを定めるだけでなく、遵守状況を点検した記録が必要

対策　年1回、台帳と現物の突合およびルール遵守状況を点検する。差異と是正内容を記録に残す。

3-1-2 ネットワークに関する情報の把握

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。

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。	☐	☐	☐

対応済み　ネットワーク構成図等で、各ネットワークの所在地と用途まで把握できる
一部対応　構成図はあるが更新されていない、または用途が記載されていない

対策　ネットワーク構成図に、拠点ごとの所在地・セグメント・用途（業務系／ゲスト／管理系など）を記載する。変更時に更新する手順を定める。

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。	☐	☐	☐

対応済み　台帳で、各機器の製造元・モデル・保守事業者まで把握できる
一部対応　機器の一覧はあるが、保守事業者や保守期限が不明
注意　保守事業者の情報まで求められる。保守切れ機器の把握にもつながる

対策　ネットワーク機器台帳に、製造元／モデル／設置場所／保守事業者／保守期限を記載する。保守切れ機器は更新計画に載せる。

3-1-3 外部情報サービスの管理

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。

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たうえで、外部情報サービスの利用時に当該要件を満たしているかサービス内容を確認すること。	☐	☐	☐

対応済み　利用前に確認するセキュリティ要件を定め、確認した記録が残っている
一部対応　都度判断しているが、確認すべき要件が文書化されていない
注意　無料のSaaSや、部門が独自に契約したサービスが対象から漏れやすい

対策　外部情報サービス利用基準を作成し、認証方式・暗号化・データ所在地・第三者監査報告書の有無などのチェック項目を定める。利用申請時にチェックシートで確認し記録を残す。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　利用規約やデータ保護に関する契約で、機密情報の取扱いについて合意している
一部対応　規約に同意しているが、機密情報の取扱条項を確認していない
注意　標準規約で足りるかは、機密情報の取扱いに関する条項の有無で判断する

対策　利用規約・データ保護契約・個別契約のいずれかで機密情報の取扱いを合意する。標準規約に不足がある場合は個別に覚書を締結する。

3-1-4 機密区分に応じた情報の管理

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。

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	☐	☐	☐

対応済み　機密の特定・区分の判定と表示・区分に応じた取扱方法・取扱エリアの制限まで定めている
一部対応　区分は定めているが、表示方法や取扱エリアの制限がない

対策　情報管理規程に、機密の特定方法／区分レベルと表示方法／区分ごとの取扱い（保存・持出・送信・廃棄）／取扱エリアの区分と入室制限を定める。

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。	☐	☐	☐

対応済み　直近1年以内に管理ルールの内容を点検し、記録が残っている
一部対応　改定はしているが、定期点検として実施していない

対策　年1回、規程の内容が実態と合っているかを点検し、記録を残す。

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。	☐	☐	☐

対応済み　台帳で、管理者名・部署名・保管場所・保管期限・開示先・連絡先まで管理している
一部対応　保管場所は把握しているが、保管期限や開示先が不明
注意　台帳に必要な項目が6つ指定されている。1つでも欠けると不足になりうる

対策　重要機密情報台帳を作成し、情報名／管理者名／部署名／保管場所／保管期限／開示先／管理者連絡先を記載する。

4 攻撃等の防御

要求事項13 / 評価基準48

4-1-1 ユーザIDの管理手続

ユーザIDの発行・変更・削除の手続を定めること。

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。	☐	☐	☐

対応済み　付与・変更・削除が申請と承認を経て行われ、記録が残っている
一部対応　申請はあるが承認者が不明、または削除だけ運用の外にある

対策　ID申請書またはワークフローを整備し、申請者・承認者・実施者を分ける。入社・異動・退職の人事イベントと連動させる。

対応済み　一部対応　未対応

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。

対応済み　共有IDが存在しない、または共有IDの利用者を特定できる仕組みがある
一部対応　共有IDが残っており、誰がいつ使ったか追えない場合がある
注意　共有IDを残す場合、誰が使ったか特定できる証跡の仕組みが必要

対策　共有IDを棚卸し、原則廃止する。廃止できない場合は利用者管理簿と操作ログで、いつ誰が使ったかを特定できる状態にする。

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。

対応済み　退職時および長期未使用のIDを、速やかに削除・無効化する運用が定着している
一部対応　退職時は削除しているが、長期間使われていないIDが放置されている
注意　一定期間使われていないIDも削除の対象。退職者対応だけでは足りない

対策　退職・異動時のID削除を人事手続のチェックリストに組み込む。あわせて90日などの期間を定め、未使用IDを定期的に抽出して無効化する。

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。

対応済み　異動時にアクセス権を見直し、不要になった権限を削除している
一部対応　権限を追加するだけで、異動前の権限が残ったままになっている
注意　異動時の権限剥奪が漏れやすい。棚卸の記録があると示しやすい

対策　異動時に旧部署の権限を削除する手順を定める。年1回以上のアクセス権棚卸を実施し、結果を記録する。

4-1-2　管理者IDの管理手続

管理者IDの発行・変更・削除の手続を定めること。

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。

対応済み　すべてのサーバ・ネットワーク機器に、システム管理者と責任者を定めている
一部対応　主要システムのみ定めており、一部の機器が未指定
注意　ルータやスイッチなどのネットワーク機器まで対象に含まれる

対策　サーバ・ネットワーク機器台帳に管理者と責任者の欄を設け、全機器に記入する。担当者の異動時に更新する。

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。

対応済み　管理者権限の付与対象を限定し、共有する場合も利用者を特定できる
一部対応　対象は限定しているが、共有の管理者IDの利用者を特定できない

対策　管理者権限の保有者を一覧化し、業務上の必要性を確認して削減する。共有が避けられない機器は、踏み台経由の操作や操作ログで利用者を特定できるようにする。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　管理者IDごとに、用途に応じた必要最小限の権限のみを付与している
一部対応　全管理者に同じ最上位権限を一律で付与している

対策　管理者IDごとに用途を定義し、必要な操作範囲に応じたロールを割り当てる。全権限の一律付与をやめる。

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。	☐	☐	☐

対応済み　開発環境の管理者権限では本番環境を操作できない設定になっている
一部対応　運用ルールで禁止しているが、技術的には操作できる状態
注意　技術的に操作できないことが問われる。運用ルールでの禁止だけでは足りない場合がある

対策　開発環境と本番環境で認証基盤またはアカウントを分離する。分離できない場合はロールを分け、本番への操作権限を付与しない。

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。	☐	☐	☐

対応済み　誰が管理者IDを保有しているかを、一覧で把握できる
一部対応　主要システムのみ把握しており、全体像がわからない

対策　管理者ID一覧を作成し、システム名／ID／保有者／付与日／用途を記載する。四半期または年1回で棚卸する。

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。	☐	☐	☐

対応済み　退職時および長期未使用の管理者IDを、速やかに削除・無効化している
一部対応　退職時は対応しているが、未使用IDの棚卸をしていない

対策　退職・異動時の管理者ID削除を手続に組み込む。未使用の管理者IDを定期的に抽出して無効化する。

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。	☐	☐	☐

対応済み　付与・変更・削除が申請と承認を経て行われ、記録が残っている
一部対応　口頭やチャットの依頼で対応しており、記録が残っていない

対策　管理者IDの申請・承認フローを整備し、口頭やチャットでの依頼を廃止する。申請記録を保管する。

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。	☐	☐	☐

対応済み　管理者IDの操作および機器の設定変更の権限を、業務上必要な者に限定している
一部対応　情報システム部門の全員が実施でき、必要性による限定がない
注意　限定していることの根拠（業務上の必要性）を示せるようにしておく

対策　管理者IDの操作および機器設定変更を行える担当者を指名し、規程に記載する。それ以外の要員からは権限を外す。

対応済み　一部対応　未対応

4-1-3 認証の強度・実装方法の決定

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。

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。 ☐ ☐ ☐

対応済み　すべてのユーザID・管理者IDについて、アクセス前に認証を行っている
一部対応　一部の社内システムに、認証なしでアクセスできる

対策　認証なしでアクセスできるシステムを洗い出し、認証を有効化する。改修できない場合はネットワーク制限などの代替策を講じる。

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。 ☐ ☐ ☐

対応済み　重要な機密情報を扱うクラウドで、利用者・管理者とも常時多要素認証を使用している
一部対応　管理者のみ多要素認証、または一部のサービスに適用できていない
注意　対象は重要な機密情報を扱うクラウド。まず該当サービスの特定が必要

対策　重要な機密情報を扱うクラウドを特定し、利用者・管理者の双方に多要素認証を必須化する。条件付きアクセス等で例外を作らない設定にする。

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。

対応済み　知識・所有・生体などから2種類以上の要素を組み合わせている
一部対応　パスワードと秘密の質問など、同じ要素の組み合わせにとどまる
注意　SMSやメールで送るワンタイムパスワードも、所有情報として認められる

対策　知識情報に加えて、認証アプリ・ワンタイムパスワード・証明書・生体のいずれかを組み合わせる。秘密の質問など同一要素の重複は避ける。

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。 ☐ ☐ ☐

対応済み　多要素認証で用いるパスワードを8文字以上に設定させている
一部対応　ルールはあるが、システム側で文字数を強制していない

対策　パスワードポリシーで最小8文字を設定し、システム側で強制する。ポリシーを設定できないサービスは利用の可否を見直す。

4-1-4 アカウントロック制御

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。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　10回以上の失敗で端末をロック、または試行間隔が延びる設定にしている
一部対応　設定できない端末があり、代替策も講じていない
注意　設定できない端末がある場合は、より強いパスワードなどの代替策が必須

対策　グループポリシーやMDMで、失敗10回でのロックまたは試行間隔の延長を設定する。設定不可の端末はパスワードを強化して代替とし、その旨を記録する。

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。	☐	☐	☐

対応済み　PC・スマートデバイスのパスワードまたはPINを6文字以上にしている
一部対応　一部の端末が4桁PINのままになっている

対策　MDMまたはグループポリシーで6文字以上のパスワード／PINを強制する。4桁PINの端末を洗い出して変更する。

4-1-5 パスワード設定ルール

パスワード設定に関するルールを定め、周知すること。

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。	☐	☐	☐

対応済み　デフォルトパスワードを変更することを、社内ルールとして定めている
一部対応　運用として変更しているが、ルールとして明文化していない

対策　パスワード管理規程に「初期パスワードは初回利用時に変更する」旨を定める。機器の導入手順書にも変更作業を組み込む。

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。	☐	☐	☐

対応済み　推測されやすい単語の使用禁止を、社内ルールとして定めている
一部対応　注意喚起はしているが、ルールとして定めていない

対策　規程に禁止例（社名・製品名・連続文字・辞書語など）を具体的に列挙する。可能なシステムでは辞書チェックを有効化する。

		対応済み	一部対応	未対応

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。

対応済み　多要素認証またはアカウントロックを前提に8文字以上、いずれもなければ10文字以上としている
一部対応　8文字以上だが、多要素認証もアカウントロックも設定していない
注意　多要素認証もアカウントロックもない場合は、10文字以上が必要になる

対策　多要素認証またはアカウントロックを導入したうえで8文字以上、いずれも導入できないシステムは英大文字・小文字・数字を含む10文字以上に設定する。

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。

対応済み　機器・サービス間でパスワードを使い回さないことを、社内ルールとして定めている
一部対応　推奨にとどまり、ルールとして定めていない

対策　規程に使い回し禁止を明記し、パスワード管理アプリの利用を推奨または全社配布する。

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。

対応済み　パスワード設定ルールを全対象者に周知し、記録が残っている
一部対応　一部の部署のみ周知、または周知した記録がない
注意　ルールを作るだけでなく、周知した記録が必要

対策　規程の周知を全社メール・研修・掲示のいずれかで行い、配信ログや受講記録を残す。派遣社員・受入出向者も対象に含める。

4-1-6 パスワード管理ルール

パスワードの管理に関するルールを定め、周知すること。

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。

対応済み　施錠保管やパスワード管理アプリの利用など、安全な保管方法をルール化している
一部対応　各自の判断に任せており、保管方法のルールがない
注意　紙に書いて施錠保管する方法も認められる。管理アプリの導入は必須ではない

対策　規程に保管方法（施錠保管、パスワード管理アプリの利用など）を定める。付箋やディスプレイ貼付、平文ファイルでの保管を明確に禁止する。

4-1-6-2 パスワードの漏洩が判明した場合、又はその疑いがある場合に速やかにパスワードを変更するための手順を定めること。

対応済み　漏洩またはその疑いが生じた場合の、変更手順を文書化している
一部対応　対応はできるが、手順として定めていない

対策　漏洩時のパスワード変更手順を、インシデント対応手順の一部として文書化する。連絡先と変更対象の特定方法を含める。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　パスワード管理ルールを全対象者に周知し、記録が残っている
一部対応　周知はしたが、対象範囲や記録が不明

対策　保管と変更のルールを周知し、周知記録を残す。

4-1-7 アクセス権の管理ルール

アクセス権の管理ルールを定めること。

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。	☐	☐	☐

対応済み　申請承認制・必要範囲への限定・棚卸の定め・台帳管理の4点すべてを定めている
一部対応　申請承認制はあるが、棚卸の定めや台帳の管理がない
注意　物理的な入室管理も同じ要求に含まれる。サーバ室の入退室記録が漏れやすい

対策　アクセス権管理規程に、申請承認制・必要最小限の付与・棚卸の頻度・台帳管理の4点を明記する。サーバ室等の入室許可も同じ規程で扱い、申請書と入退室記録を保管する。

4-2-2 セキュリティインシデント発生時の教育・訓練

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。

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。	☐	☐	☐

対応済み　新規受入時および年1回以上、eラーニングまたは集合教育を実施している
一部対応　教育資料の配布・掲示のみで、eラーニングや集合教育を行っていない
注意　資料の配布・掲示だけでは足りず、eラーニングか集合教育の実施が明示されている

対策　年間教育計画にインシデント対応の教育・訓練を組み込み、eラーニングまたは集合教育で実施する。新規受入時の実施も手続に組み込む。

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。	☐	☐	☐

対応済み　実施内容・実施方法・実施時期・受講状況を記録し、保管している
一部対応　実施はしているが、誰が受講したかを追跡していない
注意　受講状況の記録が必要。未受講者を追える状態にしておく

対策　実施内容・方法・時期・受講者名簿を記録し保管する。未受講者へ再通知する仕組みを設ける。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　直近1年以内に教育・訓練の実施内容を点検し、記録が残っている
一部対応　内容を毎年そのまま使い回しており、点検していない

対策　年1回、教育内容が最新の脅威や自社の状況に合っているかを点検し、記録を残す。

4-3-4 適切なバックアップ

適切なバックアップを行うこと。

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。	☐	☐	☐

対応済み　取得対象・取得頻度・保管期間を定めたうえで取得している
一部対応　取得はしているが、対象や保管期間が定められていない

対策　バックアップ方針書に、対象システム／対象データ／取得頻度／保管期間／保管先を定める。取得結果を監視し、失敗に気づける状態にする。

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。	☐	☐	☐

対応済み　重要な機密情報を、遠隔地またはクラウドにも保管している
一部対応　同一拠点内の別媒体にのみ保管している
注意　遠隔地の距離要件は示されていないが、同一拠点内の別媒体は該当しない

対策　重要な機密情報について、別拠点またはクラウドへの複製を確保する。ランサムウェア対策として、書換不可の保管やオフライン保管も検討する。

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。	☐	☐	☐

対応済み　バックアップ対象ごとにリストア手順書を整備している
一部対応　手順書はあるが対象の一部のみ、または復旧を試したことがない
注意　手順書の整備が要件。復旧試験までは求められていないが、実施が望ましい

対策　バックアップ対象ごとにリストア手順書を作成する。年1回の復旧試験を行い、所要時間と結果を記録すると精度が上がる。

4-4-1 情報機器、OS及びソフトウェアの安全な構成

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。

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。	☐	☐	☐

対応済み　許可していないソフトを削除・無効化、または自由にインストールできない設定にしている
一部対応　ルールで禁止しているが、技術的に制限していない
注意　技術的な制限が求められる。ルールでの禁止だけでは足りない場合がある

対策　資産管理ツールやアプリケーション制御で、許可外ソフトの導入を技術的に制限する。導入済みの不要ソフトは削除する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　外部記録媒体を使う端末で、自動実行・自動再生を無効化している
一部対応　一部の端末のみ設定、または設定状況を確認していない

対策　グループポリシーまたはMDMで自動実行・自動再生を無効化する。設定状況をレポートで確認する。

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。	☐	☐	☐

対応済み　サーバ・ネットワーク機器の設定変更を、申請承認制にしている
一部対応　重要な変更のみ承認を取り、軽微な変更は担当者の判断で行っている

対策　変更管理手順を定め、申請書またはチケットで承認を取る運用にする。緊急変更の事後承認ルールも定める。

4-4-4 セキュリティパッチ・アップデートの手続

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。

4-4-4-1	システム、情報機器及びソフトウェアは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。 - 可能であれば、自動アップデートが有効化されている。	☐	☐	☐

対応済み　すべてサポート対象で、終了したものは削除または通信を遮断。自動更新も有効化している
一部対応　サポートが終了した製品が残っており、遮断などの措置も取っていない
注意　サポート終了品は削除か通信遮断のいずれかが必要。そのままの稼働は認められない

対策　資産台帳にサポート期限を記載してEOL製品を抽出する。更新計画を立て、更新までの間はネットワーク分離や通信遮断で暫定対応する。自動更新は可能な範囲で有効化する。

		対応済み	一部対応	未対応
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、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - 脆弱性悪用の対象となる機能を無効化すること。 - ベンダーが推奨する回避策を実施すること。 - 対象となる情報機器を適用範囲内のネットワークから分離すること。 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。 [対象] -会社支給のパソコンの OS、ブラウザ及びOffice ソフト -サーバの OS及びミドルウェア -会社支給のスマートデバイスのOS及びアプリ -インターネットとの境界に設置されているネットワーク機器のOS及びファームウェア	☐	☐	☐

対応済み　重大・高リスクの更新を14日以内に適用し、困難な場合は緩和策を実施している
一部対応　適用はしているが期限が定まっておらず、遅延時の緩和策もない
注意　14日という期限が明示されている。間に合わない場合は緩和策の実施が条件

対策　脆弱性情報の収集経路を決め、重大・高リスクの更新を14日以内に適用する運用を定める。検証に時間を要する場合の緩和策（機能無効化・回避策・分離・監視）を手順書に明記する。

4-4-5 マルウェア感染からの保護

システムをマルウェア感染から保護すること。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　ネットワークに接続するすべてのPC・サーバに導入している
一部対応　PCには導入しているが、サーバの一部が未導入
注意　サーバへの導入漏れが多い。ネットワークに接続していれば対象になる

対策　全PC・サーバの導入状況を管理コンソールで確認し、未導入端末をゼロにする。サーバ用ライセンスの手当ても行う。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　PC・サーバごとにスキャン範囲と頻度を定め、実行している
一部対応　導入はしているが、スキャンが実行されているか確認していない

対策　対象ごとにスキャン範囲と頻度（フルスキャンは週1回など）を定め、実行結果を管理コンソールで確認する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　ベンダーの推奨に従ってパターンファイルを更新している
一部対応　自動更新に任せており、更新に失敗している端末を把握していない

対策　パターンファイルの自動更新を有効化し、更新に失敗している端末をコンソールで定期的に確認して是正する。

4-5-1 ネットワーク境界防護

ネットワークを適切に分離し、境界部分を防護すること。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　すべての機器で強固で一意のパスワードに変更、またはリモートアクセスを無効化している
一部対応　主要機器のみ変更し、拠点のルータが初期設定のまま残っている
注意　拠点や倉庫のルータが初期パスワードのまま残っていることが多い

対策　全拠点のファイアウォール・ルータを棚卸し、初期パスワードを機器ごとに異なる強固なものへ変更する。使わないリモート管理は無効化する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　パスワードを変更する手順を文書化している
一部対応　変更はできるが、手順として定めていない

対策　パスワード変更手順を機器管理手順書に定める。変更時期と実施者を記録する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　FW・ルータの認証が、4-1-5のパスワード設定基準を満たしている
一部対応　一部の機器が文字数などの基準を満たしていない
注意　ファイアウォールやルータの認証にも、4-1-5のパスワード基準がそのまま適用される

対策　機器の認証設定を4-1-5の基準（文字数・複雑さ・使い回し禁止）に合わせる。基準を満たせない機器は更新を検討する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　認証されていないインバウンド通信を遮断している
一部対応　遮断はしているが、許可している例外ルールを検証していない

対策　デフォルト拒否を方針とし、必要な通信のみ許可する設定にする。設定内容を定期的に確認する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　インバウンド通信のファイアウォール・ルールを、文書として定めている
一部対応　機器に設定はあるが、設定意図を記した文書がない

対策　ファイアウォール・ルールを一覧化し、各ルールの目的・申請者・有効期限を記載した管理表を作成する。

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。	☐	☐	☐

対応済み　不要になったルールを速やかに削除・無効化している
一部対応　削除しておらず、用途が不明なルールが残っている

対策　定期的にルールを棚卸し、用途不明・期限切れのルールを削除または無効化する。棚卸の記録を残す。

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。	☐	☐	☐

対応済み　多要素認証を適用、または信頼できるIPアドレスにアクセスを制限している
一部対応　パスワード認証のみで、インターネット経由で変更できる状態
注意　インターネット経由で変更する場合は、多要素認証かIP制限のいずれかが必須

対策　管理インターフェースへのアクセスを、多要素認証または送信元IPアドレスの制限で保護する。可能ならインターネットからの管理アクセス自体を遮断する。

5 攻撃等の検知

要求事項1 / 評価基準3

5-1-1 ネットワーク接続・データの監視

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。

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。	☐	☐	☐

対応済み　境界または端末で、外部から社内・社内から不正サーバの双方をリアルタイム検知・遮断できる
一部対応　外部からの通信のみ対策し、社内から外部への不正通信を見ていない
注意　外部から社内への通信だけでなく、社内から不正なサーバへの通信も対象

対策　境界にファイアウォールやIPS、端末にEDRなどを配置し、外向き通信も含めて検知・遮断できる構成にする。不審な宛先への通信を遮断対象に含める。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　ログとアラートを分析し、インシデントに該当するかを判断する運用がある
一部対応　アラートは届くが、確認されずに放置されることがある
注意　検知の仕組みだけでは足りず、人が該当性を判断する運用まで求められる

対策　アラートの確認担当と確認頻度を定め、インシデント該当性の判断基準（重大度の定義）を文書化する。確認結果を記録する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　速やかなアラート発報と、速報レポートの作成・通知の仕組みがある
一部対応　アラートは出るが、レポートの作成や通知の手順がない

対策　アラートの通知先と通知手段（メール・チャット・電話）を設定し、速報レポートの様式と作成期限を定める。

6 インシデントへの対応

要求事項1 / 評価基準6

6-1-1 インシデント対応手順

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。

		対応済み	一部対応	未対応
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	☐	☐	☐

対応済み　発見報告・初動・調査対応・復旧・最終報告の5段階を手順として定めている
一部対応　連絡先は決まっているが、初動以降の手順が定まっていない

対策　インシデント対応手順書を作成し、発見報告・初動・調査対応・復旧・最終報告の5段階ごとに、実施事項・判断基準・担当を記載する。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　関係当局・所管省庁を含む社内外の連絡先と、報告・情報共有ルートを定めている
一部対応　社内の連絡先のみで、外部への報告先が定まっていない
注意　関係当局・所管省庁への報告先が明示されている。社内連絡網だけでは足りない

対策　社内の報告ルートに加え、警察・個人情報保護委員会・所管省庁・取引先・保険会社などの外部連絡先を一覧化し、手順書の別紙とする。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　インシデント時の統括役員と担当部署の役割・責任を定めている
一部対応　担当者は決まっているが、権限と責任の範囲が不明確

対策　手順書に、統括役員と担当部署のインシデント時の役割・責任・意思決定権限を明記する。代理者も定める。

		対応済み	一部対応	未対応
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。	☐	☐	☐

対応済み　直近1年以内にインシデント時の体制を点検し、記録が残っている
一部対応　体制は定めているが、定期的な点検をしていない
注意　年1回以上の点検と、その記録が必要

対策　年1回、連絡先と体制を点検し記録を残す。机上演習と併せて実施すると効率がよい。

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。	☐	☐	☐

対応済み　インシデントの報告フォーマットを整備している
一部対応　都度自由記述で報告しており、決まった様式がない

対策　発生日時・事象・影響範囲・対応状況・報告先を含む報告フォーマットを作成し、手順書に添付する。

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。	☐	☐	☐

対応済み　年1回以上および重大インシデント発生時に、事例と対応策を社内部署へ共有している
一部対応　発生時のみ共有しており、平時の定期的な共有がない
注意　平時も年1回以上の共有が必要。インシデント発生時のみでは足りない

対策　年1回以上、社内外のインシデント事例と対応策を関係部署へ共有する。重大事例の発生時は速やかに共有し、実施記録を残す。

7 インシデントからの復旧

要求事項1 / 評価基準1

7-1-1 事業継続要件に沿った復旧準備

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。

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。)	☐	☐	☐

対応済み　重要システムの目標復旧レベルを定め、システムまたは人手による業務継続策を整備している
一部対応　目標復旧レベルは定めたが、待機系や代替連絡手段などが未整備
注意　システムによる継続と人手による継続のどちらでもよい。予備機の用意は必須ではない

対策　事業継続上重要なシステムを特定し、目標復旧時間と目標復旧レベルを定める。システム面（待機系・クラウド・予備機）と人手（電話・FAX・紙運用、取引先の複数連絡手段）の両面で継続策を整備し、手順書にまとめる。

集計欄

対応済み	一部対応	未対応	合計
適合	不適合	不適合	／81項目

適合率 ＝ 対応済みの項目数 ÷ 81 × 100 ＝ ＿＿＿＿＿＿ %

★3申請までの流れ

01	現状把握	本シートで不足項目を洗い出す
02	対策の実装	各項目の「対策」に沿って、技術的対策とルール整備を進める
03	文書の整備	規程・手順書・台帳を、確認を受けられる状態にそろえる
04	専門家の確認	登録されたセキュリティ専門家が自己評価の内容を確認し、署名する
05	申請・登録	経営層による自己適合宣誓を添えて事務局へ提出する

本制度は正式決定前です

SCS評価制度は制度構築方針に基づく設計段階にあり、2026年度末頃の運用開始に向けて詳細が具体化されている途中です。要求事項・評価基準・申請手続は今後変更される可能性があるため、最新の情報はIPAおよび経済産業省の公式サイトでご確認ください。

適合率の数え方について

制度上、評価基準は満たしているかどうかで判断され、部分点の考え方は示されていません。本シートでも「対応済み」のみを適合として数えます。「一部対応」は不適合ですが、あと一歩で満たせる項目です。着手の優先順位を決める材料としてください。

ステップ04について、および本シートの作成について

★3の申請には、事務局に登録されたセキュリティ専門家による確認と署名が必要です。社内に該当者がいない場合は、外部の専門家に依頼することになります。なお本シートはAIを活用して作成しており、内容に誤りが含まれる可能性があります。正確な情報については当社までお問い合わせください。