SCS★3 の評価基準81を、申請前に埋める準備表

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）の★3の評価基準81を1行ずつ読み、どの行にも「記載するために手元に出す物」「それを決める人」「今週できる最初の一手」を書いた1枚です。

81行すべてに書いてあります。

アセスメントシートに記載する前に、**何を用意すれば書けるか**が1行ずつ分かります。

用意する物は31個です。 81行を1行ずつ読む前に、**31個の物**か**5つの担当**で絞れます。

この表の読み方

1行が評価基準1つです。 左から、評価基準の番号・大分類と要求事項名・評価基準の冒頭の引用・手元に出す物・用意する物・決める人・最初の一手（今週）・参考。

列	何が書いてあるか
手元に出す物	その評価基準に記載するために用意する物。**文書・台帳・記録・設定・契約の5種**のどれかです
決める人	**経営／情シス／人事・総務／開発・運用／法務・調達の5つ**のどれかです。**当社が81行を読んで振り分けた分け方**です（原本にはありません）
用意する物	同じ物で埋まる行には**同じ名前**が入っています。ここで絞ると、**その1個で何行埋まるか**が見えます（全部で31個）
最初の一手（今週）	その行で今週できることを1文で。「規程を作る」ではなく「A4 1枚に責任者の名前を書く」の粒度です
参考	当社が公開している資料で、始めるときに使える所。**空いている行もあります**（当社の資料を使わなくても進められます）

Excel には「状態」の列があります（未着手／用意中／手元にある）。ここを埋めると、「進み具合」と「経営向け1枚」のシートが動きます。**PDF は読む物、Excel は埋める物**です。

手元に出す物は、評価基準の文の動詞で決まります。 「定めること」は文書、「仕組みを整備すること」は台帳か設定、「点検すること」は記録、「取り決めること」は契約です。

参考の列の読み方＝A-13 のような英字と数字は点検表61問の番号、問2 は取締役会で聞く問いの番号、台帳 工程0 は判定の台帳の工程、判断表 欄3 は判断表の欄です。

17の問いは通称で、実物は19行あります。 17は国の項目の数で、当社が2行足しました。**だから参考の列には問19まで出ます。**

評価基準の引用は、冒頭の 34 字までです。 全文は原本（下の出典）で確かめてください。

決める人ごとの件数

決める人	件数	主な中身
経営	**7**	体制・方針・目標復旧レベル
情シス	**64**	台帳・設定・バックアップ・検知
人事・総務	**14**	守秘義務・教育と訓練・周知・機密区分

決める人	件数	主な中身
開発・運用	**8**	本番の権限分離・境界機器・検知の仕組み
法務・調達	**4**	取引先との合意・事故時の役割
のべ	**97**	★1行に2人書いた行があるので、81より多くなります

決める人の列で絞れば、5つの担当にそのまま配れます。

この5つは、当社が81行を読んで振り分けた「決める人」です（原本にこの分け方はありません）。いちばん多いのは情シスで64行。**ほかの4つの担当が入る行は32行**あります（担当ごとに数えるとのべ33行＝人事・総務14行、開発・運用8行、経営7行、法務・調達4行）。

用意する物（同じ物で埋まる行をまとめた）

81行は、31個の物で埋まります。 同じ1枚の社内ルール、同じ1回の訓練の記録、同じ一覧に列を1本――そうやって複数の行が同時に埋まります。

用意する物	埋まる行
認証の設定	**7**
境界機器の設定と手順	**7**
年1回の点検の記録	**5**
事故対応の手順と連絡先	**5**
パスワードの社内ルール	**5**
機器とソフトの一覧	**4**
アカウントの申請承認と棚卸の記録	**4**
アカウントの一覧	**4**
セキュリティ対応方針	**3**
取引先と外部サービスの一覧	**3**
バックアップの設定と手順	**3**
マルウェア対策の設定	**3**
検知の設定と記録	**3**
取引先との契約	**2**
ネットワークの一覧	**2**

用意する物	埋まる行
本番と開発の権限の設定	**2**
変更と承認の記録	**2**
周知の記録	**2**
教育と訓練の記録	**2**
端末の設定	**2**
体制と役割の1枚	**1**
連絡先の一覧	**1**
守秘義務の規定	**1**
守秘義務を説明した記録	**1**
情報機器の管理ルール	**1**
機密区分の規程	**1**
重要情報の台帳	**1**
アクセス権の管理ルール	**1**
脆弱性対応の期限のルール	**1**
事例の共有の記録	**1**
目標復旧レベルと復旧手順	**1**
31個	**81行**

Excel では「用意する物」の列で絞ると、その1個で何行埋まるかが見えます。

手元に出す物の種類ごとの件数

種類	件数	何を指すか
文書	**24**	規程・方針・手順など、決めたことを書いた物
台帳	**16**	一覧。資産・取引先・アカウントなど
記録	**23**	実施・点検・受講・承認の記録
設定	**23**	画面で確かめられる設定

種類	件数	何を指すか
契約	**3**	取引先との合意
のべ	**89**	★1行に2種書いた行があるので、81より多くなります

準備表（81行）

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
1-2-1-1	ガバナンスの整備／セキュリティ推進活動部門	・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…	文書（体制図と役割1枚）	体制と役割の1枚	経営	統括する役員の名前と担当部署を A4 1枚に書く	問1
1-2-1-2	ガバナンスの整備／セキュリティ推進活動部門	・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…	台帳（平時の連絡先）	連絡先の一覧	情シス	役員・担当・外部窓口の連絡先を1枚にまとめる	C-9（事故時の連絡先を平時にも）
1-2-1-3	ガバナンスの整備／セキュリティ推進活動部門	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて…	記録（点検日と結果）	年1回の点検の記録	経営	年1回の点検日を予定表に置き、今年の1行を書く	
1-2-3-1	ガバナンスの整備／守秘義務のルール	・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…	文書（守秘義務の規定）	守秘義務の規定	人事・総務	就業規則と誓約書の該当条項を抜き出して1枚に書く	
1-2-3-2	ガバナンスの整備／守秘義務のルール	・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。	記録（説明した日）	守秘義務を説明した記録	人事・総務	入社・受入れの手続きに「守秘の説明」の行を足す	
1-3-1-1	ガバナンスの整備／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定めること。	文書（対応方針 A4 1枚）	セキュリティ対応方針	経営	目的・適用範囲・責任者の3つで方針を書く	問1
1-3-1-2	ガバナンスの整備／セキュリティ対応方針の策定	・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…	設定（置き場所）	セキュリティ対応方針	情シス	社内ポータルの固定の場所に方針を置く	
1-3-1-3	ガバナンスの整備／セキュリティ対応方針の策定	・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…	記録（改正日と周知日）	セキュリティ対応方針	人事・総務	方針の履歴表に改正日と周知日の列を作る	
2-1-1-1	取引先管理／取引先とのビジネス又はシステム上の関係	・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…	台帳（取引先とクラウドの一覧）	取引先と外部サービスの一覧	情シス	委託先・クラウド・外部 AI を1つの一覧にする	E-3・A-4・F-6／問4
2-1-1-2	取引先管理／取引先とのビジネス又はシステム上の関係	・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…	記録（最終確認日）	取引先と外部サービスの一覧	情シス	一覧に「最終確認日」の列を足して今日の日付を入れる	E-3／問4

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
2-1-2-1	取引先管理／機密情報の取扱い	・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…	契約（機密情報の取り決め）	取引先との契約	法務・調達	NDA に定義・利用制限・返還廃棄の3つがあるか見る	E-7
2-1-4-1	取引先管理／セキュリティインシデント発生時の役割・責任	・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…	契約と文書（事故時の役割）	事故対応の手順と連絡先	法務・調達／情シス	主要取引先と「誰が第1報を出すか」を1枚に書く	C-9・C-14／問4・問5／判断表 欄3
3-1-1-1	リスクの特定／情報機器、OS及びソフトウェアに関する情報の把握	・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…	台帳（PC の製造元・OS・台数）	機器とソフトの一覧	情シス	資産管理の画面か台帳から3列を出す	
3-1-1-2	リスクの特定／情報機器、OS及びソフトウェアに関する情報の把握	・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…	台帳（サーバ・仮想・ハイパーバイザ）	機器とソフトの一覧	情シス	社外に面した物の一覧に内部サーバを足す	A-13
3-1-1-3	リスクの特定／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ついて、導入、設置、ネットワーク接…	文書（導入・接続・パッチの管理ルール）	情報機器の管理ルール	情シス	導入申請・接続・期限の3項を1枚に書く	A-15／台帳
3-1-1-4	リスクの特定／情報機器、OS及びソフトウェアに関する情報の把握	・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…	記録（遵守の点検）	年1回の点検の記録	情シス	年1回の点検日を予定表に置く	
3-1-2-1	リスクの特定／ネットワークに関する情報の把握	・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…	台帳（ネットワークの所在地と用途）	ネットワークの一覧	情シス	拠点・セグメント・用途の一覧を作る	
3-1-2-2	リスクの特定／ネットワークに関する情報の把握	・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…	台帳（NW機器の製造元・モデル・保守）	ネットワークの一覧	情シス	境界機器の一覧に内部機器を足す	A-13
3-1-3-1	リスクの特定／外部情報サービスの管理	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…	文書と記録（外部サービスの要件と確認）	取引先と外部サービスの一覧	情シス	利用前チェック3項と確認の記録を作る	A-4・F-6・G-1／問19
3-1-3-2	リスクの特定／外部情報サービスの管理	・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…	契約（提供事業者との合意）	取引先との契約	法務・調達	利用規約・データ処理条項を一覧に添える	E-3
3-1-4-1	リスクの特定／機密区分に応じた情報の管理	・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…	文書（機密区分と取扱い）	機密区分の規程	経営／人事・総務	区分3段と取扱表を1枚に書く	

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
3-1-4-2	リスクの特定／機密区分に応じた情報の管理	・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…	記録（区分ルールの点検）	年1回の点検の記録	人事・総務	年1回の点検日を予定表に置く	
3-1-4-3	リスクの特定／機密区分に応じた情報の管理	・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…	台帳（重要情報の管理者・場所・期限）	重要情報の台帳	人事・総務／情シス	個人情報から重要情報台帳を始める	D-1・D-2／問13
4-1-1-1	攻撃等の防御／ユーザIDの管理手続	・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…	文書と記録（ユーザIDの申請承認）	アカウントの申請承認と棚卸の記録	情シス	申請フォームと承認の記録を1組にする	
4-1-1-2	攻撃等の防御／ユーザIDの管理手続	・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…	台帳（共有ID の一覧と利用者の特定方法）	アカウントの一覧	情シス	共有ID を数えて利用者の特定方法を書く	F-1
4-1-1-3	攻撃等の防御／ユーザIDの管理手続	・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…	記録（不要ID の削除）	アカウントの申請承認と棚卸の記録	情シス／人事・総務	退職者リストと削除日を突き合わせる	B-4・B-5／問3
4-1-1-4	攻撃等の防御／ユーザIDの管理手続	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…	記録（権限の見直し）	アカウントの申請承認と棚卸の記録	情シス	異動時に権限を見直す記録を1行書く	B-3・B-5
4-1-2-1	攻撃等の防御／管理者IDの管理手続	・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…	台帳（機器ごとの管理者と責任者）	機器とソフトの一覧	情シス	機器一覧に責任者の列を足す	
4-1-2-2	攻撃等の防御／管理者IDの管理手続	・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…	台帳（管理者ID の限定）	アカウントの一覧	情シス	管理者ID 全員の理由を1行ずつ書く	B-3／問3
4-1-2-3	攻撃等の防御／管理者IDの管理手続	・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…	台帳（管理者ID の用途と権限）	アカウントの一覧	情シス	用途ごとの権限を見直す	B-3・F-2
4-1-2-4	攻撃等の防御／管理者IDの管理手続	・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…	設定（開発と本番の権限分離）	本番と開発の権限の設定	開発・運用	本番の管理権限から開発アカウントを外す	
4-1-2-5	攻撃等の防御／管理者IDの管理手続	・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…	台帳（管理者ID 保有者）	アカウントの一覧	情シス	管理者ID の一覧を出す	B-3／問3
4-1-2-6	攻撃等の防御／管理者IDの管理手続	・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…	記録（不要な管理者IDの削除）	アカウントの申請承認と棚卸の記録	情シス	休眠の管理者ID を無効にして記録する	B-4・B-5／問3

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
4-1-2-7	攻撃等の防御／管理者IDの管理手続	・管理者IDの付与・変更・削除は申請・承認制にすること。	記録（管理者ID の申請承認）	変更と承認の記録	情シス	管理者ID の変更に承認の記録を付ける	C-2
4-1-2-8	攻撃等の防御／管理者IDの管理手続	・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…	設定と台帳（設定変更の権限者）	本番と開発の権限の設定	情シス	設定を変えられる人を数えて一覧にする	
4-1-3-1	攻撃等の防御／認証の強度・実装方法の決定	・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…	設定（全ID の認証）	認証の設定	情シス／開発・運用	認証なしで入れる経路が無いことを確かめる	A-6
4-1-3-2	攻撃等の防御／認証の強度・実装方法の決定	・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…	設定（クラウドの多要素認証）	認証の設定	情シス	重要クラウドの MFA を全員に有効にする	B-1・B-2／問7
4-1-3-3	攻撃等の防御／認証の強度・実装方法の決定	・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…	設定（認証要素の種類）	認証の設定	情シス	使っている要素を2種類以上にする	B-1／問7
4-1-3-4	攻撃等の防御／認証の強度・実装方法の決定	・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…	設定（パスワード8文字以上）	認証の設定	情シス	各システムのポリシー画面で文字数を確かめる	
4-1-4-1	攻撃等の防御／アカウントロック制御	・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…	設定（PC・スマホのロック）	認証の設定	情シス	MDM か GPO のロック設定を確かめる	
4-1-4-2	攻撃等の防御／アカウントロック制御	・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…	設定（PIN 6文字以上）	認証の設定	情シス	MDM か GPO のロック設定を確かめる	
4-1-5-1	攻撃等の防御／パスワード設定ルール	・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…	文書（初期パスワード変更のルール）	パスワードの社内ルール	情シス	社内ルールに1行足す	
4-1-5-2	攻撃等の防御／パスワード設定ルール	・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…	文書（推測されやすい語の禁止）	パスワードの社内ルール	情シス	社内ルールに1行足す	
4-1-5-3	攻撃等の防御／パスワード設定ルール	・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…	文書と設定（MFA か試行制限＋8文字）	認証の設定	情シス	どちらを使うか決めて1行書く	B-1・B-2
4-1-5-4	攻撃等の防御／パスワード設定ルール	・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…	文書（使い回し禁止）	パスワードの社内ルール	情シス	社内ルールに1行足す	

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
4-1-5-5	攻撃等の防御／パスワード設定ルール	No.4-1-5-1からNo.4-1-5-4までで定めたパスワード設…	記録（周知）	周知の記録	人事・総務	周知した日と方法を1行書く	
4-1-6-1	攻撃等の防御／パスワード管理ルール	・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…	文書（安全な保管）	パスワードの社内ルール	情シス	パスワード管理アプリの指定を書く	G-2
4-1-6-2	攻撃等の防御／パスワード管理ルール	・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…	文書（漏洩時の変更手順）	パスワードの社内ルール	情シス	社内と利用者の2通りの手順を1枚に書く	C-15／問11
4-1-6-3	攻撃等の防御／パスワード管理ルール	・No.4-1-6-1及びNo.4-1-6-2で定めたパスワードの管…	記録（周知）	周知の記録	人事・総務	周知した日と方法を1行書く	
4-1-7-1	攻撃等の防御／アクセス権の管理ルール	・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…	文書と台帳（アクセス権の管理ルール4点）	アクセス権の管理ルール	情シス／人事・総務	申請承認・最小・棚卸・台帳の4項を1枚に書く	B-3・B-4・B-5
4-2-2-1	攻撃等の防御／セキュリティインシデント発生時の教育・訓練	・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、…	記録（事故対応の教育・訓練）	教育と訓練の記録	人事・総務	年1回の訓練を予定表に置き、資料1枚を用意する	
4-2-2-2	攻撃等の防御／セキュリティインシデント発生時の教育・訓練	・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…	記録（受講記録）	教育と訓練の記録	人事・総務	受講者と日付の表を作る	
4-2-2-3	攻撃等の防御／セキュリティインシデント発生時の教育・訓練	・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…	記録（点検）	年1回の点検の記録	人事・総務	年1回の点検日を予定表に置く	
4-3-4-1	攻撃等の防御／適切なバックアップ	・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…	文書と設定（対象・頻度・保管期間）	バックアップの設定と手順	情シス	バックアップの3項を1枚に書く	C-12・C-13／問5
4-3-4-2	攻撃等の防御／適切なバックアップ	・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…	設定（遠隔地バックアップ）	バックアップの設定と手順	情シス	本番の管理者で消せない場所の複製を確かめる	C-13／問5
4-3-4-3	攻撃等の防御／適切なバックアップ	・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。	文書（リストア手順書）	バックアップの設定と手順	情シス	対象ごとの戻す手順を1枚に書く	C-12／問5
4-4-1-1	攻撃等の防御／情報機器、OS及びソフトウェアの安全な構成	・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…	設定（許可外ソフトの制限）	端末の設定	情シス	許可ソフトの一覧と制限の設定を確かめる	
4-4-1-2	攻撃等の防御／情報機器、OS及びソフトウェアの安全な構成	・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…	設定（自動実行の無効化）	端末の設定	情シス	端末の設定を確かめる	

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
4-4-1-3	攻撃等の防御／情報機器、OS及びソフトウェアの安全な構成	・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。	記録（設定変更の申請承認）	変更と承認の記録	情シス／開発・運用	変更の記録に承認の列を足す	C-1
4-4-4-1	攻撃等の防御／セキュリティパッチ・アップデートの手続	・情報機器、OS及びソフトウェアについて、以下の状態とすること。 -…	台帳（サポート・ライセンスの状態）	機器とソフトの一覧	情シス	機器・ソフト一覧にサポート期限の列を足す	A-13・A-14／問2／台帳 工程0・1
4-4-4-2	攻撃等の防御／セキュリティパッチ・アップデートの手続	・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…	文書と記録（14日以内のアップデート）	脆弱性対応の期限のルール	情シス	3条件の期限と、できないときの緩和策を1枚に書く	A-15・A-14／問2／台帳
4-4-5-1	攻撃等の防御／マルウェア感染からの保護	・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…	設定（マルウェア対策ソフト）	マルウェア対策の設定	情シス	全端末・全サーバの導入状況を一覧にする	
4-4-5-2	攻撃等の防御／マルウェア感染からの保護	・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…	設定（スキャン範囲と頻度）	マルウェア対策の設定	情シス	設定画面を確かめる	
4-4-5-3	攻撃等の防御／マルウェア感染からの保護	・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…	設定（パターン更新）	マルウェア対策の設定	情シス	設定画面を確かめる	
4-5-1-1	攻撃等の防御／ネットワーク境界防護	・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…	設定（FW・ルータの初期パスワード）	境界機器の設定と手順	情シス／開発・運用	初期パスワードの変更とリモート無効を確かめる	A-2
4-5-1-2	攻撃等の防御／ネットワーク境界防護	・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)…	文書（FW パスワード変更の手順）	境界機器の設定と手順	情シス	手順を1枚に書く	
4-5-1-3	攻撃等の防御／ネットワーク境界防護	・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)…	設定（FW の認証基準）	境界機器の設定と手順	情シス	パスワード設定が 4-1-5 を満たすか確かめる	
4-5-1-4	攻撃等の防御／ネットワーク境界防護	・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…	設定（未認証インバウンドの遮断）	境界機器の設定と手順	情シス／開発・運用	受け入れ規則を一覧にする	A-2・A-6
4-5-1-5	攻撃等の防御／ネットワーク境界防護	・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…	文書（インバウンド規則）	境界機器の設定と手順	情シス／開発・運用	規則の一覧に理由の列を足す	A-2
4-5-1-6	攻撃等の防御／ネットワーク境界防護	・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…	記録（不要規則の削除）	境界機器の設定と手順	情シス／開発・運用	使っていない規則を止めて記録する	A-2・B-7

評価基準No.	大分類／要求事項名	評価基準（冒頭の引用）	手元に出す物	用意する物	決める人	最初の一手（今週）	参考
4-5-1-7	攻撃等の防御／ネットワーク境界防護	・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…	設定（FW 変更時の MFA か IP 制限）	境界機器の設定と手順	情シス	管理画面の MFA と接続元制限を確かめる	B-1・B-6／問7
5-1-1-1	攻撃等の検知／ネットワーク接続・データの監視	・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…	設定（検知・遮断の仕組み）	検知の設定と記録	情シス／開発・運用	境界か端末のどちらで検知するかを決める	A-10・A-11・A-12・C-7
5-1-1-2	攻撃等の検知／ネットワーク接続・データの監視	・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…	記録（判断の記録）	検知の設定と記録	情シス	直近1か月の知らせを見て判断した記録を1行書く	C-7・C-8／問9
5-1-1-3	攻撃等の検知／ネットワーク接続・データの監視	・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…	設定（通知の宛先）	検知の設定と記録	情シス	異常時に誰に届くかを設定で確かめる	C-7／問9
6-1-1-1	インシデントへの対応／インシデント対応手順	・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…	文書（対応手順5段階）	事故対応の手順と連絡先	情シス／経営	発見報告・初動・調査・復旧・最終報告を1枚に書く	C-9／問5
6-1-1-2	インシデントへの対応／インシデント対応手順	・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…	台帳（社内外の連絡先と報告ルート）	事故対応の手順と連絡先	情シス／法務・調達	当局・所管省庁を含む連絡先を1枚にまとめる	C-9・C-10・C-11・E-6／問5・問16
6-1-1-3	インシデントへの対応／インシデント対応手順	・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(…	文書（事故時の役員と担当部署の役割）	事故対応の手順と連絡先	経営	対応手順に役割の表を足す	C-9／問5
6-1-1-4	インシデントへの対応／インシデント対応手順	・年1回以上の頻度でNo.6-1-1-2及びNo.6-1-1-3にて…	記録（体制の点検）	年1回の点検の記録	情シス	年1回の点検日を予定表に置く	C-9
6-1-1-5	インシデントへの対応／インシデント対応手順	・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。	文書（報告フォーマット）	事故対応の手順と連絡先	情シス	第1報の型を1枚で用意する	判断表（第1報の型）
6-1-1-6	インシデントへの対応／インシデント対応手順	・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…	記録（事例の共有）	事例の共有の記録	人事・総務／情シス	年1回、事例と対策を社内に共有した記録を残す	
7-1-1-1	インシデントからの復旧／事業継続要件に沿った復旧準備	・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…	文書（目標復旧レベルと復旧の手）	目標復旧レベルと復旧手順	経営／情シス	重要システムの目標復旧レベルを1行決める	C-12・C-9／問5／判断表 欄4

出典

文書	出したところ	日付	取得日	この表のどこに使ったか
要求事項・評価基準 Ver.1.1	独立行政法人情報処理推進機構	2026年10月28日（水）	2026年10月30日（金）	評価基準81の番号・大分類・要求事項名・文の引用
自己評価等ガイド	同	2026年10月28日（水）初版	2026年10月30日（金）	自己評価の形・自己適合宣言・★3確認責任者・証跡の実在は確かめないこと
★4 第三者評価ガイド	同	2026年10月28日（水）初版	2026年10月30日（金）	★4に指定評価機関の第三者評価が加わること
料金設定のお知らせ	同	2026年9月18日（金）	2026年10月30日（金）	登録申請の受付の時期
サイバーセキュリティ緊急対策パッケージ	サイバーセキュリティに関する関係閣僚会議	2026年11月6日（金）に策定	2026年11月6日（金）	SCS を名指しした3か所

この表は、申請の前に手元に出す物を決めるための1枚です。
