令和7年度セキュリティ人材活用促進実証に係る業務

ケース演習資料

セキュリティアセスメント編（グループワーク）

IPA Better Life with IT

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

ケース演習カリキュラム

	内容	担当	時間※1	
講演	ケース演習受講にあたっての説明（スケジュール、注意事項等）		10分	2時間
	マネジメント指導ツール（セキュリティアセスメント）の解説等		1時間30分	
	サプライチェーン対策評価制度動向の説明		20分	
グループワーク	1.ファシリテーターからの説明 ・アイスブレイク、「演習の流れ」「ケース事例について」「評価にあたっての留意事項」の説明 ・事例企業（A社）についての説明 ・ケース1を使用した評価に関する説明 ・「３」検討前に「タイムキーパー、発表者、記録係、司会」を決定 ・「４」の発表テーマは、発表前にファシリテーターがグループを指名して決定	ファシリテーター	30分	3時間
	2.参加者各自によるケース2～7の評価実施		20分	
	3.各グループによるケース2～7の評価実施		40分	
	～ 休憩 ～		10分	
	4.グループ順にロールプレイ実施 ・企業担当者役：ファシリテータ、企業社長役：事務局、専門家役：各グループ発表者を設定 ・専門家役から企業側に再確認の項目について質問 ・グループ内で適合・不適合の最終評価を実施 ・専門家役から企業側に評価結果を伝達（不適合の項目について理由と改善策を提案） ・企業側からの質問に専門家役が回答 ・ファシリテータが講評を行い、解答を提示		60分＋予備10分 （15分×４）	
	5.ファシリテーターからの全体講評、質疑応答		10分	

ケーステーマ

- グループワークのケーステーマは以下のとおり。

（SCS評価制度の要求事項より、評価基準中項目単位で様々なものを対象として選択）

- ケース1：1-2-3 守秘義務のルールを策定し、遵守させること。（ファシリテータの例示用）
- ケース2：2-1-1 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。
- ケース3：3-1-4 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。
- ケース4：4-1-1 ユーザID の発行・変更・削除の手続を定め、適切に運用すること。
- ケース5：4-3-4 適切なバックアップを行うこと。
- ケース6：4-4-1 ハードウェア・ソフトウェアの安全な構成を確立し、維持すること。
- ケース7：5-1-1 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。

SCS評価制度 要求事項No.

Ⅰ．グループワークの進め方

１．グループワークの流れ

２．ケース事例について

３．評価にあたっての留意事項

1．グループワークの流れ

1	13:00 ～ 13:30	ファシリテーターからの説明	ファシリテータが参加者全員に向け、演習の流れ、ケース事例、評価にあたっての留意事項、事例企業、評価についての説明等を行います。	30分
2	13:30 ～ 13:50	参加者各自の評価	参加者各自でテーマ２から７の評価を実施します。	20分
3	13:50 ～ 14:30	グループ毎の評価	グループ毎にテーマ２から７の評価を実施します。	40分
	14:30 ～ 14:40	（休憩）		10分
4	14:40 ～ 15:50	ロールプレイ	企業担当者役（ファシリテータ）、企業社長役（ファシリテータ補佐）、専門家役（各グループ発表者）として、ロールプレイ形式で評価を実施します。	70分
5	15:50 ～ 16:00	全体講評・質疑応答	ファシリテータから全体講評、及び質疑応答を行います。	10分

１ ファシリテーターからの説明

- アイスブレイク、＜演習の流れ＞についての説明
- 【ケース事例について】の説明
- 【評価にあたっての留意事項】の説明
- 事例企業（A社）についての説明
- テーマ１を使用した評価についての説明
- 「３」検討前 「タイムキーパー、発表者、記録係、司会」の決定
- 「４」発表テーマは、発表前にファシリテーターがグループを指名して決定

2 参加者各自の評価

- 参加者各自におけるテーマ２から７の評価

3 グループ毎の評価

- グループ毎のテーマ２から７の評価

4 ロールプレイ

- Aグループから順にロールプレイを実施（15分 x 4グループ） ※　発表者の入れ替わり（10分）
- 企業担当者役：ファシリテータ、企業社長役：ファシリテータ補佐、専門家役：各グループの発表者
- 専門家役から企業側に再確認の項目について質問
- グループ内で適合・不適合の最終評価を実施
- 専門家役から企業側に評価結果を伝達（不適合の項目について理由と改善策を提案）
- 企業側からの質問に専門家役が回答
- ファシリテータが講評を行い、模範回答を提示

5 全体講評・質疑応答

- ファシリテータからの全体講評、質疑応答

2．ケース事例について

- 要求基準・評価事項等はSCS評価制度に係る実証事業の際のものを使用してケースを作成しています。
  制度開始時には内容が変更となる可能性があります。
- 事例の企業は、実証に参加いただいた企業（複数社）を参考に作成した架空の企業です。

３．評価にあたっての留意事項

- 各評価基準について、「適合」又は「不適合」のいずれかを「評価結果」欄に記入してください。
- 「適合」と評価した場合には、補足すべき事項があれば「評価結果の補足」欄に記入してください。
- 「不適合」と評価した場合には、不適合の理由を「評価結果の補足」欄に記入してください。また、企業への評価結果のフィードバックの際に助言ができるように「適合」となるための改善案を検討してください。
- 情報不足のため「適合」・「不適合」の評価ができない場合には、一旦「再確認」として「評価結果の補足」欄に「再確認を要する事項」（追加質問）の内容を記載してください。また、どのような回答の場合に「適合」の評価になるかを検討してください。
- 「評価のためのガイダンス」に記載がある場合にはその内容を踏まえて評価を実施してください。

Ⅱ．ケース事例企業

事例企業（A社）

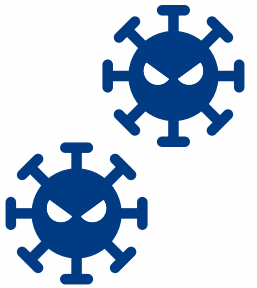
事例企業（A社）

- A社は、従業員30名の主に家電製品の部品を製造する企業である。精密加工技術に定評があり、他社では製造が難しい部品を製造している。愛知県に本社工場があり、東京都と大阪府に営業拠点を設けている。A社の売上のうち30%は大手家電製品製造企業であるB社への売上である。製造は主に本社工場で行っているが、一部の部品の製造は外部の協力会社C社に委託している。
- A社には、製造部、技術部、営業部、管理部がある。情報システムの専任担当はいないが、管理部に所属するベテラン社員Dと派遣社員Eが情報システムを担当している。A社社長が管理部長を兼務しており、情報システムに関する企画や運用はA社社長、社員D、派遣社員Eの３名体制で実施している。

事例企業（A社）

- ファイルサーバ等のオンプレミスサーバは本社工場のマシンルーム内に設置されている。本社工場、東京営業所、大阪営業所のネットワークはインターネットVPNで接続されており、東京営業所と大阪営業所でも本社工場と同じシステムを使用している。東京営業所と大阪営業所にはオンプレミスサーバは設置されていない。電子メールシステム等はA社が契約したクラウドサービスを利用している。また、営業拠点ではインターネット経由でB社等の取引先が運営するシステムも利用している。
- A社は5年前に情報セキュリティ体制整備のための専門家派遣制度を活用して情報処理安全確保支援士の支援を受けており、その際に情報セキュリティ基本方針および情報セキュリティ関連規程の整備を実施した。規程の整備後は管理部長であるA社社長の主導で情報セキュリティ関連規程に基づいたIT運用の文化が定着している。

事例企業（A社）



- 先月、B社の協力会社であるF社で二重脅迫型ランサムウェアの被害が発生しB社の秘密情報が流出するセキュリティ事故が発生した。A社にもB社の秘密情報が開示されているためA社社長は他人事ではないと考え情報セキュリティ管理体制の再確認を計画していたところ、B社からサプライチェーン対策評価制度に係る実証事業で参加企業を募集しているという話を聞き、実証に参加することとした。
- 実証に参加するにあたって、実証事業の事務局からサプライチェーン対策評価の適用範囲に関する質問があった。A社では、A社のデータやサービスにアクセスする全てのネットワーク、要員、IT機器をカバーする法人全体を適用範囲と定義した。（別紙１参照）ただし、製品製造上の環境については、インターネット及び社内LANから物理的に隔離しているため適用範囲外とした。
- その後、A社は実証事業の事務局から送付されたサプライチェーン対策評価のアセスメントシートについて質問事項に対する「回答」と「回答の補足」を記載して専門家Gに送付した。

事例企業（A社）

別紙1：適用範囲の内容

分類	項目	適用範囲
ネットワーク	社内	各拠点に１台ルータ（VPN・ファイアーウォール機能付き）を設置して下記のネットワークを構築 ・本社工場内ネットワーク ・東京営業所内ネットワーク ・大阪営業所内ネットワーク ・拠点間VPN接続 ・リモートアクセスVPN接続
	社外	インターネット経由で下記のクラウドサービスを利用 ・ホームページ ・電子メール ・クラウドストレージ ・グループウェア ・ワークフローシステム
要員	内部要員	役員：3名 従業員：30名
	外部要員	派遣社員：5名
IT機器	サーバ	基幹システム ファイルサーバ Active Directoryサーバ
	PC	Windows：30台 Mac：3台
	モバイル	会社では契約していないが、個人所有デバイスでメール送受信を行っている

Ⅲ. テーマ資料

- テーマ1：1-2-3 守秘義務のルールを策定し、遵守させること。【ファシリテーター説明用】
- テーマ2：2-1-1 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。
- テーマ3：3-1-4 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。
- テーマ4：4-1-1 ユーザID の発行・変更・削除の手続を定め、適切に運用すること。
- テーマ5：4-3-4 適切なバックアップを行うこと。
- テーマ6：4-4-1 ハードウェア・ソフトウェアの安全な構成を確立し、維持すること。
- テーマ7：5-1-1 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。

テーマ1

ファシリテーター説明用

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ1-1
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
1-2-3-1	**・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること**	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にしていますか。	Yes/No			・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。 ・社外要員については、情報セキュリティ関連規程の中に、契約書に守秘義務について盛り込むように規定することが考えられる。
1-2-3-2	**・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること**	・入社時あるいは社外要員の受け入れ時に守秘義務をどのように説明していますか。	記述式			・入社時や受け入れ時に対面で説明する、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。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ1-2
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
1-2-3-1	**・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること**	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にしていますか。	Yes/No	はい	「就業規則：2024/4/1改定」に記載している。	・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。 ・社外要員については、情報セキュリティ関連規程の中に、契約書に守秘義務について盛り込むように規定することが考えられる。
1-2-3-2	**・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること**	・入社時あるいは社外要員の受け入れ時に守秘義務をどのように説明していますか。	記述式	入社時に「情報システム使用に関する基本方針の承諾書」を締結している。		・入社時や受け入れ時に対面で説明する、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。

テーマ1-3

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
1-2-3-1	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること			・実際の規定まで確認する必要はない	
1-2-3-2	・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること			・説明の方法については、手段を問わないが、説明を受けていない従業員のチェックをどのようにしているかについては確認する必要がある	・役員、従業員については、守秘義務について解説している小冊子を作成し、小冊子を読んだことを報告してもらう形で説明している。 ・社外要員については、派遣元企業を通じて守秘義務について指導してもらっている。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ1-4
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
1-2-3-1	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること	再確認	[再確認を要する事項] 1.就業規則の対象に役員は含まれますか。 ＜適合の評価になる回答例＞ ・役員も就業規則の対象に含まれる ・役員は就業規則の対象に含まれないが、役員規則等の別の規則で役員の守秘義務のルールが策定されている 2.派遣社員等の社外要員を対象とする守秘義務のルールはありますか。 ＜適合の評価になる回答例＞ ・情報セキュリティ関連規程に業務委託契約の際に作成すべき守秘義務のルールを記載している	・実際の規定まで確認する必要はない	
1-2-3-2	・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること	再確認	[再確認を要する事項] 1.社外要員に対してどのように守秘義務を説明していますか。 ＜適合の評価になる回答例＞ ・社外要員に対しては派遣元企業から守秘義務を説明してもらっている 2.承諾書の締結が漏れている役員、従業員がいないかをどのようにチェックしていますか。 ＜適合の評価になる回答例＞ ・ワークフローシステムの設定で承諾書の締結を管理部長が確認しないと入社のワークフローが完了できないようになっている	・説明の方法については、手段を問わないが、説明を受けていない従業員のチェックをどのようにしているかについては確認する必要がある	・役員、従業員については、守秘義務について解説している小冊子を作成し、小冊子を読んだことを報告してもらう形で説明している。 ・社外要員については、派遣元企業を通じて守秘義務について指導してもらっている。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ1-5
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
1-2-3-1	**・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること**	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にしていますか。	Yes/No	はい	「就業規則：2024/4/1改定」に記載している。 [再確認に対する回答] 1.就業規則の対象に役員は含まれない。 2.情報セキュリティ関連規程に業務委託契約の際に作成すべき守秘義務のルールを記載している。	・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。 ・社外要員については、情報セキュリティ関連規程の中に、契約書に守秘義務について盛り込むように規定することが考えられる。
1-2-3-2	**・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること**	・入社時あるいは社外要員の受け入れ時に守秘義務をどのように説明していますか。	記述式	入社時に「情報システム使用に関する基本方針の承諾書」を締結している。 [再確認に対する回答] 1.社外要員に対しては派遣元企業から守秘義務を説明してもらっている。 2.承諾書の原本を保管しているが締結漏れについてはチェックしていない。		・入社時や受け入れ時に対面で説明する、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。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ1-6
1	ガバナンスの整備	1-2	役割・責任・権限	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。

評価基準No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
1-2-3-1	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務のルールを策定し、明確にすること	Yes/No	はい	「就業規則：2024/4/1改定」に記載している。 [再確認に対する回答] 1.就業規則の対象に役員は含まれない。 2.情報セキュリティ関連規程に業務委託契約の際に作成すべき守秘義務のルールを記載している。	不適合	[不適合の理由] 役員を対象とした守秘義務のルールを策定することが必要です。
1-2-3-2	・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること	記述式	入社時に「情報システム使用に関する基本方針の承諾書」を締結している。 [再確認に対する回答] 1.社外要員に対しては派遣元企業から守秘義務を説明してもらっている。 2.承諾書の原本を保管しているが締結漏れについてはチェックしていない。		不適合	[不適合の理由] 承諾書の締結が漏れている役員、従業員がいないかをチェックすることが必要です。

テーマ2

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】
2枚目：参加者が評価を記載するためのブランクシート　【事前配布】
3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート
4枚目：想定される再確認の内容に対する回答を記載したシート
5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ2-1
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	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No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること**	・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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していますか。	Yes/No	はい	全社に関わる外部情報システムは管理部で一覧表を作成している ＜一覧表の管理項目＞ -システム名 -提供事業者名 -用途 -接続先アドレス -利用開始日 -現契約の満了日 -契約の自動更新の有無	・一覧には、以下を例とする項目を含むことが考えられる。 ＜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 ＜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

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ2-2
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること			・一覧の整備がなされていれば、実際の一覧の内容の妥当性まで確認する必要はない。	

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ2-3
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること	再確認	[再確認を要する事項] 一部の部署のみで使用している外部情報システムはありますか。ある場合は一覧表を作成していますか。	・一覧の整備がなされていれば、実際の一覧の内容の妥当性まで確認する必要はない。	

テーマ2-4

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	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No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること**	・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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していますか。	Yes/No	はい	全社に関わる外部情報システムは管理部で一覧表を作成している ＜一覧表の管理項目＞ -システム名 -提供事業者名 -用途 -接続先アドレス -利用開始日 -現契約の満了日 -契約の自動更新の有無 [再確認に対する回答] 営業拠点の個別EDI等を使用しているが、管理部では管理・把握はしていない。情報セキュリティ関連規程（：2025/3/31更新）にて、全社に関わる外部システムは管理部で管理し、営業拠点で使用している外部システムは営業拠点で管理すると規定している。	・一覧には、以下を例とする項目を含むことが考えられる。 ＜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 ＜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

テーマ2-5

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	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No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
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等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること	Yes/No	はい	全社に関わる外部情報システムは管理部で一覧表を作成している ＜一覧表の管理項目＞ -システム名 -提供事業者名 -用途 -接続先アドレス -利用開始日 -現契約の満了日 -契約の自動更新の有無 [再確認に対する回答] 営業拠点の個別EDI等を使用しているが、管理部では管理・把握はしていない。情報セキュリティ関連規程にて、全社に関わる外部システムは管理部で管理し、営業拠点で使用している外部システムは営業拠点で管理すると規定している。	適合	[補足事項] 営業拠点の個別EDI等も一覧表に含めることが望ましいです。

テーマ3

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】

2枚目：参加者が評価を記載するためのブランクシート　【事前配布】

3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート

4枚目：想定される再確認の内容に対する回答を記載したシート

5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ3-1
3	リスクの特定	3-1	資産管理	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
3-1-4-1	**・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること** **- 機密の特定** **- 機密区分のレベル判定と表示** **- 区分に応じた取り扱い方法** **- 取り扱いエリアの区分及び制限**	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していますか。 - 機密の特定 - 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法 - 取り扱いエリアの区分及び制限	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にて定義	・情報の取扱いに関する運用規程や情報の取扱手順、情報資産管理手順書に記載することが考えられる。 ・要管理対策区域の対策の基準、管理区域の利用手順に記載することも考えられる。 ・管理ルールの策定には、以下の資料が参考になる。 IPA:情報漏えい対策のしおり https://www.ipa.go.jp/security/guide/shiori.html
3-1-4-3	**・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること**	・機密区分のうち、高い機密区分の情報資産(情報)について一覧を作成していますか。	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義	・情報資産台帳や情報資産一覧、資産目録等に記載することが考えられる。
	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含んでいますか。	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義	・一覧の更新に関するルールを定め、作成日、更新日を記録することが望ましい。

テーマ3-2

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
3	リスクの特定	3-1	資産管理	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。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
3-1-4-1	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること - 機密の特定 - 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法 - 取り扱いエリアの区分及び制限			・規程の整備が記載されていれば、具体的な内容まで確認する必要はない。	
3-1-4-3	・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること			・高い機密区分の情報資産(情報)のみで一覧を構成している必要はなく、情報資産台帳や情報資産一覧、資産目録等の中で機密区分が確認できるようになっていればよい。	
	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと			・一覧の整備がなされており、所定の項目の整備が記載されていれば、具体的な管理実態まで確認する必要はない。	

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
3	リスクの特定	3-1	資産管理	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。

テーマ3-3

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
3-1-4-1	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること - 機密の特定 - 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法 - 取り扱いエリアの区分及び制限			・規程の整備が記載されていれば、具体的な内容まで確認する必要はない。	
3-1-4-3	・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること	再確認	[再確認を要する事項] ・情報資産管理台帳では、高い機密区分の情報がどれかが分かるようになっていますか。	・高い機密区分の情報資産(情報)のみで一覧を構成している必要はなく、情報資産台帳や情報資産一覧、資産目録等の中で機密区分が確認できるようになっていればよい。	
	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと	再確認	[再確認を要する事項] 高い機密区分の情報資産(情報)一覧には、下記の全ての項目を記載していますか。 ・対象情報 ・管理者名 ・部署名 ・保管場所 ・保管期限 ・開示先 ・連絡先	・一覧の整備がなされており、所定の項目の整備が記載されていれば、具体的な管理実態まで確認する必要はない。	

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
3	リスクの特定	3-1	資産管理	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。

テーマ3-4

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
3-1-4-1	**・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること** **- 機密の特定** **- 機密区分のレベル判定と表示** **- 区分に応じた取り扱い方法** **- 取り扱いエリアの区分及び制限**	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していますか。 - 機密の特定 - 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法 - 取り扱いエリアの区分及び制限	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にて定義	・情報の取扱いに関する運用規程や情報の取扱手順、情報資産管理手順書に記載することが考えられる。 ・要管理対策区域の対策の基準、管理区域の利用手順に記載することも考えられる。 ・管理ルールの策定には、以下の資料が参考になる。 IPA:情報漏えい対策のしおり https://www.ipa.go.jp/security/guide/shiori.html
3-1-4-3	**・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること**	・機密区分のうち、高い機密区分の情報資産(情報)について一覧を作成していますか。	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義 [再確認に対する回答] 情報資産管理台帳の「機密区分」列で高い機密区分の情報がどれかが分かるようになっている。	・情報資産台帳や情報資産一覧、資産目録等に記載することが考えられる。
	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含んでいますか。	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義 [再確認に対する回答] 情報資産管理台帳の項目は以下の通り。 ＜記載項目＞ 対象情報、部署名、保管場所、保管期限、開示先	・一覧の更新に関するルールを定め、作成日、更新日を記録することが望ましい。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
3	リスクの特定	3-1	資産管理	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。

テーマ3-5

評価基準No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
3-1-4-1	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること - 機密の特定 - 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法 - 取り扱いエリアの区分及び制限	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にて定義	適合	
3-1-4-3	・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義 [再確認に対する回答] 情報資産管理台帳の「機密区分」列で高い機密区分の情報がどれかが分かるようになっている。	適合	
	・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと	Yes/No	はい	・情報資産管理台帳（：2025/3/31更新）にて定義 [再確認に対する回答] 情報資産管理台帳の項目は以下の通り。 ＜記載項目＞ 対象情報、部署名、保管場所、保管期限、開示先	不適合	[不適合の理由] 高い機密区分の情報資産(情報)一覧に、下記の項目を追加することが必要です。 ・管理者名 ・連絡先

テーマ4

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】

2枚目：参加者が評価を記載するためのブランクシート　【事前配布】

3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート

4枚目：想定される再確認の内容に対する回答を記載したシート

5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ4-1
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-1-1-1	**・自社又は必要に応じて社外要員(派遣社員等)に対して、ユーザIDの付与・変更・削除は申請・承認制にすること**	・ユーザIDの付与・変更・削除は申請・承認制にすることを定めていますか。 ・それは具体的にどのようなプロセスですか。	記述式	ワークフロー「システム利用申請書」にて、承認後にIDを付与している。		・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。
4-1-1-2	**・ユーザIDを共有しないこと**	・ユーザIDを共有しないというルールを定め、運用していますか。（ユーザIDを共有しないというルールを定めて運用している場合Yes）	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にてやむを得ない場合を除き共有IDの使用を禁止している	・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が必要な場合は、共有IDを利用したユーザを特定できるようにすること	・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにしていますか。 ・それはどのように実施していますか。	記述式	やむを得ず共有IDが必要な場合は、ユーザを特定できるようにワークフローの申請「共有ID 新規申請／利用者変更」を必須としている。		・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の見直しするなどの運用を行うことが望ましい。

テーマ4-2

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-1-1-1	・自社又は必要に応じて社外要員(派遣社員等)に対して、ユーザIDの付与・変更・削除は申請・承認制にすること			・以下を確認すること。 － 本項目に係る社内ルール(例：アカウント管理規程)が定められているか － ユーザIDの付与・変更・削除にあたって、情報セキュリティ責任者又はシステム管理者等の承認を得ることが規定されているか	当社ではアクセス制御及び認証に関する個別規定を設けており、その中で、以下を規定している。 － 利用者の認証に用いるアカウントは、情報セキュリティ責任者の承認に基づき登録する。 － アカウントが不要になる場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になった日の翌日までに実施する。 － 当社の従業員以外の者にアカウントを発行する場合は、情報セキュリティ責任者の承認を得たうえで、秘密保持契約を締結する。
4-1-1-2	・ユーザIDを共有しないこと			・規程はシステム管理規程やアカウント管理規程に示す等が考えられる。	
	・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにすること			・共有IDを利用したユーザを完全に特定するには困難も想定されることから、人事異動後の早期のパスワード変更などの不正アクセスリスクの軽減措置でも許容されるものとする。	・弊社では、システム用アカウント等において共有IDを利用する際、ネットワーク管理者に異動、退職などの人事が発生した場合は、パスワードを早期に変更している。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ4-3
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-1-1-1	・自社又は必要に応じて社外要員(派遣社員等)に対して、ユーザIDの付与・変更・削除は申請・承認制にすること	再確認	[再確認を要する事項] ・ワークフローで承認後にIDの付与・変更・削除を実施するというルールを規程等で定めていますか。 ・ワークフローの承認者は誰ですか。	・以下を確認すること。 － 本項目に係る社内ルール(例：アカウント管理規程)が定められているか － ユーザIDの付与・変更・削除にあたって、情報セキュリティ責任者又はシステム管理者等の承認を得ることが規定されているか	当社ではアクセス制御及び認証に関する個別規定を設けており、その中で、以下を規定している。 － 利用者の認証に用いるアカウントは、情報セキュリティ責任者の承認に基づき登録する。 － アカウントが不要になる場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になった日の翌日までに実施する。 － 当社の従業員以外の者にアカウントを発行する場合は、情報セキュリティ責任者の承認を得たうえで、秘密保持契約を締結する。
4-1-1-2	・ユーザIDを共有しないこと			・規程はシステム管理規程やアカウント管理規程に示す等が考えられる。	
	・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにすること			・共有IDを利用したユーザを完全に特定するには困難も想定されることから、人事異動後の早期のパスワード変更などの不正アクセスリスクの軽減措置でも許容されるものとする。	・弊社では、システム用アカウント等において共有IDを利用する際、ネットワーク管理者に異動、退職などの人事が発生した場合は、パスワードを早期に変更している。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ4-4
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-1-1-1	**・自社又は必要に応じて社外要員(派遣社員等)に対して、ユーザIDの付与・変更・削除は申請・承認制にすること**	・ユーザIDの付与・変更・削除は申請・承認制にすることを定めていますか。 ・それは具体的にどのようなプロセスですか。	記述式	ワークフロー「システム利用申請書」にて、承認後にIDを付与している。 [再確認に対する回答] 情報セキュリティ関連規程（：2025/3/31更新）にてワークフローで管理部長の承認後にIDの付与・変更・削除を行うというルールを定めている。		・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。
4-1-1-2	**・ユーザIDを共有しないこと**	・ユーザIDを共有しないというルールを定め、運用していますか。（ユーザIDを共有しないというルールを定めて運用している場合Yes）	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にてやむを得ない場合を除き共有IDの使用を禁止している	・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が必要な場合は、共有IDを利用したユーザを特定できるようにすること	・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにしていますか。 ・それはどのように実施していますか。	記述式	やむを得ず共有IDが必要な場合は、ユーザを特定できるようにワークフローの申請「共有ID 新規申請／利用者変更」を必須としている。		・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の見直しするなどの運用を行うことが望ましい。

テーマ4-5

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。

評価基準No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
4-1-1-1	・自社又は必要に応じて社外要員(派遣社員等)に対して、ユーザIDの付与・変更・削除は申請・承認制にすること	記述式	ワークフロー「システム利用申請書」にて、承認後にIDを付与している。 [再確認に対する回答] 情報セキュリティ関連規程（：2025/3/31更新）にてワークフローで承認後にIDの付与・変更・削除を行う際というルールを定めている。		適合	
4-1-1-2	・ユーザIDを共有しないこと	Yes/No	はい	・情報セキュリティ関連規程（：2025/3/31更新）にてやむを得ない場合を除き共有IDの使用を禁止している	適合	
	・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにすること	記述式	やむを得ず共有IDが必要な場合は、ユーザを特定できるようにワークフローの申請「共有ID 新規申請／利用者変更」を必須としている。		適合	

テーマ5

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】

2枚目：参加者が評価を記載するためのブランクシート　【事前配布】

3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート

4枚目：想定される再確認の内容に対する回答を記載したシート

5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ5-1
4	攻撃等の防御	4-3	データセキュリティ	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-3-4-1	**・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること**	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得していますか。 ・主な取得対象と取得頻度について説明してください。 ・主なバックアップ取得方法について説明してください。	記述式	一部行っている 頻度：毎日 方法：本社工場内の別筐体へ自動バックアップ		・バックアップの取得方法を検討する際には、以下の資料が参考となる。 IPA:セキュリティ対策の基本と共通対策 https://www.ipa.go.jp/security/10threats/nq6ept000000g23w-att/kihontokyoutsuu_2024.pdf
4-3-4-2	**・重要情報については、遠隔地を含めてバックアップを保管すること**	・重要情報については、遠隔地を含めてバックアップを保管していますか。 ・主な重要情報とそのバックアップ方法を説明してください。	記述式	基幹システムの売掛・買掛データについて定期バックアップを行っている		・遠隔地バックの対象となる重要情報は、主に可用性の観点から失われると事業継続上大きな問題となる情報やデータが考えられる。 ・遠隔地バックアップの方法としては、以下のような方法が考えられる。 -クラウドストレージを利用して、遠隔地のサーバーにデータを転送する -ネットワーク経由でバックアップデータを転送する -レプリケーション技術を用いて、メインのファイルサーバーと同じシステム環境を持つ「レプリカ」を遠隔地に用意する -テープやディスクなどの記憶媒体にバックアップしたデータを遠隔地に運んで保管する
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**	・バックアップ対象ごとにリストア手順書を整備していますか。	Yes/No	いいえ	手順書を作成していない	・バックアップのリストア手順書は、各ベンダーが作成している場合が多いので、それをベースとして作成することが考えられる

テーマ5-2

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-3	データセキュリティ	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。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 －[適合]の場合、補足があれば記載（任意） －[再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） －[不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-3-4-1	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること			・回答中に以下の点が明示されているかを確認する必要がある。 －取得対象(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(例：文書は日次、設定情報は月次) －バックアップ取得方法(例：バックアップサーバの活用、外部記録メディアに保管)	・基幹LAN上のNASの全データについて、外付けのHDDに日次で差分バックアップ、週次でフルバックアップを取得している。 ・各社員の端末に保管されているデータのうち、重要なデータは基幹LAN上のNASに日次でコピーするというルールにしている。
4-3-4-2	・重要情報については、遠隔地を含めてバックアップを保管すること			・回答中に以下の点が明示されているかを確認する必要がある。 －対象となる重要情報(例：顧客、従業員等の個人情報) －バックアップ方法(例えば、「対策実施のためのガイダンス」に記載の方法でバックアップがなされているか) ・回答に記載の重要情報の範囲、バックアップ方法が事業やシステムの観点から適切かどうかの詳細な検証を行う必要は必ずしもない。	・取引先から預かっている機密情報や取引先へ納品する機密情報を重要情報と定義し、取引先と合意の上、ISMAPに登録されているクラウドストレージにデータバックアップを取得している。
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			・回答の補足にて、規定又は手順書が示されていることを確認する。	

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ5-3
4	攻撃等の防御	4-3	データセキュリティ	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。

評価基準No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-3-4-1	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること	再確認	[再確認を要する事項] 基幹システム以外の主なバックアップの取得対象について説明をお願いします。	・回答中に以下の点が明示されているかを確認する必要がある。 － 取得対象(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(例：文書は日次、設定情報は月次) － バックアップ取得方法(例：バックアップサーバの活用、外部記録メディアに保管)	・基幹LAN上のNASの全データについて、外付けのHDDに日次で差分バックアップ、週次でフルバックアップを取得している。 ・各社員の端末に保管されているデータのうち、重要なデータは基幹LAN上のNASに日次でコピーするというルールにしている。
4-3-4-2	・重要情報については、遠隔地を含めてバックアップを保管すること	再確認	[再確認を要する事項] バックアップの方法とバックアップデータの保管場所（遠隔地）について説明をお願いします。	・回答中に以下の点が明示されているかを確認する必要がある。 － 対象となる重要情報(例：顧客、従業員等の個人情報) － バックアップ方法(例えば、「対策実施のためのガイダンス」に記載の方法でバックアップがなされているか) ・回答に記載の重要情報の範囲、バックアップ方法が事業やシステムの観点から適切かどうかの詳細な検証を行う必要は必ずしもない。	・取引先から預かっている機密情報や取引先へ納品する機密情報を重要情報と定義し、取引先と合意の上、ISMAPに登録されているクラウドストレージにデータバックアップを取得している。
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			・回答の補足にて、規定又は手順書が示されていることを確認する。	

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ5-4
4	攻撃等の防御	4-3	データセキュリティ	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。

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-3-4-1	**・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること**	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得していますか。 ・主な取得対象と取得頻度について説明してください。 ・主なバックアップ取得方法について説明してください。	記述式	一部行っている 頻度：毎日 方法：本社工場内の別筐体へ自動バックアップ [再確認に対する回答] 上記のバックアップの対象は基幹システムとファイルサーバ		・バックアップの取得方法を検討する際には、以下の資料が参考となる。 IPA:セキュリティ対策の基本と共通対策 https://www.ipa.go.jp/security/10threats/nq6ept000000g23w-att/kihontokyoutsuu_2024.pdf
4-3-4-2	**・重要情報については、遠隔地を含めてバックアップを保管すること**	・重要情報については、遠隔地を含めてバックアップを保管していますか。 ・主な重要情報とそのバックアップ方法を説明してください。	記述式	基幹システムの売掛・買掛データについて定期バックアップを行っている [再確認に対する回答] ネットワーク経由でクラウドストレージにバックアップを行っている		・遠隔地バックの対象となる重要情報は、主に可用性の観点から失われると事業継続上大きな問題となる情報やデータが考えられる。 ・遠隔地バックアップの方法としては、以下のような方法が考えられる。 -クラウドストレージを利用して、遠隔地のサーバーにデータを転送する -ネットワーク経由でバックアップデータを転送する -レプリケーション技術を用いて、メインのファイルサーバーと同じシステム環境を持つ「レプリカ」を遠隔地に用意する -テープやディスクなどの記憶媒体にバックアップしたデータを遠隔地に運んで保管する
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**	・バックアップ対象ごとにリストア手順書を整備していますか。	Yes/No	いいえ	手順書を作成していない	・バックアップのリストア手順書は、各ベンダーが作成している場合が多いので、それをベースとして作成することが考えられる

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ5-5
4	攻撃等の防御	4-3	データセキュリティ	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。

評価基準No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
4-3-4-1	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること	記述式	一部行っている 頻度：毎日 方法：本社工場内の別筐体へ自動バックアップ [再確認に対する回答] 上記のバックアップの対象は基幹システムとファイルサーバ		適合	[補足事項] ・Active Directoryサーバのバックアップ取得の要否について確認することが望ましいです。 ・各クラウドサービスに関してクラウド上のデータ保護の責任の所在について確認を行い、データのバックアップが利用者側の責任範囲となってクラウドサービスがある場合には、バックアップの取得対象を見直すことが望ましいです。
4-3-4-2	・重要情報については、遠隔地を含めてバックアップを保管すること	記述式	基幹システムの売掛・買掛データについて定期バックアップを行っている [再確認に対する回答] ネットワーク経由でクラウドにバックアップを行っている		適合	[補足事項] 情報資産管理台帳の棚卸などの際に基幹システムの売掛・買掛データ以外にも重要情報がないかを確認し、必要に応じて遠隔地保管するバックアップの対象の見直しを行うことが望ましいです。
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	Yes/No	いいえ	手順書を作成していない	不適合	[不適合の理由] 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が必要です。

テーマ6

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】

2枚目：参加者が評価を記載するためのブランクシート　【事前配布】

3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート

4枚目：想定される再確認の内容に対する回答を記載したシート

5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ6-1
4	攻撃等の防御	4-4	プラットフォームセキュリティ	4-4-1	ハードウェア・ソフトウェアの安全な構成	ハードウェア・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No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-4-1-1	・パソコン、サーバ、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又は無効化すること	・パソコン、サーバ、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又は無効化していますか。	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、端末へ導入するソフトウェアは「管理部が決めたもの」もしくは「新規のソフトウェアは管理部長の承認が必要」としている。	・情報システムの利用やパソコンや携帯電話の利用に関する規程、社員への教育資料に記載することが考えられる。 ・利用を認めるソフトウェアを定めることも有効である。
4-4-1-2	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にしていますか。	Yes/No	はい	Active Directoryのグループポリシーにて自動再生を無効化している。	・Windowsであればコントロールパネルの設定変更で自動実行や自動再生を無効化できる。
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	・サーバ及びネットワーク機器の設定変更を申請・承認制にしていますか。	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、サーバ及びネットワーク機器の設定変更は管理部の情報システム担当が実施することを定めている。	・情報システムセキュリティ関連規定に記載することが考えられる。 ・申請・承認の様式を整備することも有効である。

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ6-2
4	攻撃等の防御	4-4	プラットフォームセキュリティ	4-4-1	ハードウェア・ソフトウェアの安全な構成	ハードウェア・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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-4-1-1	・パソコン、サーバ、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又は無効化すること			・不要ソフトウェアの削除等を求める規定や手順書の記載有無又は対策の実施方法(例：標準ソフトウェア以外のインストール制限)を確認すること。 ・規定等の有無が確認できていれば対策の実施方法まで確認する必要はない。	
4-4-1-2	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること			・回答の補足にて、規定や手順書の記載有無又は対策の実施方法が示されているかを確認すること。	
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			・回答の補足にて、システム管理規程、手順書のような規程、又は申請・承認の様式が示されているかを確認する	

テーマ6-3

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-4	プラットフォームセキュリティ	4-4-1	ハードウェア・ソフトウェアの安全な構成	ハードウェア・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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 － [適合]の場合、補足があれば記載（任意） － [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） － [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
4-4-1-1	・パソコン、サーバ、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又は無効化すること			・不要ソフトウェアの削除等を求める規定や手順書の記載有無又は対策の実施方法(例：標準ソフトウェア以外のインストール制限)を確認すること。 ・規定等の有無が確認できていれば対策の実施方法まで確認する必要はない。	
4-4-1-2	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること			・回答の補足にて、規定や手順書の記載有無又は対策の実施方法が示されているかを確認すること。	
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	再確認	[再確認を要する事項] サーバ及びネットワーク機器の設定変更を実施する前に申請・承認を行っていますか。	・回答の補足にて、システム管理規程、手順書のような規程、又は申請・承認の様式が示されているかを確認する	

テーマ6-4

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-4	プラットフォームセキュリティ	4-4-1	ハードウェア・ソフトウェアの安全な構成	ハードウェア・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No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
4-4-1-1	・パソコン、サーバ、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又は無効化すること	・パソコン、サーバ、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又は無効化していますか。	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、端末へ導入するソフトウェアは「管理部が決めたもの」もしくは「新規のソフトウェアは管理部長の承認が必要」としている。	・情報システムの利用やパソコンや携帯電話の利用に関する規程、社員への教育資料に記載することが考えられる。 ・利用を認めるソフトウェアを定めることも有効である。
4-4-1-2	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にしていますか。	Yes/No	はい	Active Directoryのグループポリシーにて自動再生を無効化している。	・Windowsであればコントロールパネルの設定変更で自動実行や自動再生を無効化できる。
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	・サーバ及びネットワーク機器の設定変更を申請・承認制にしていますか。	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、サーバ及びネットワーク機器の設定変更は管理部の情報システム担当が実施することを定めている。 [再確認に対する回答] 設定作業実施時には申請・承認を行っていない。	・情報システムセキュリティ関連規定に記載することが考えられる。 ・申請・承認の様式を整備することも有効である。

テーマ6-5

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
4	攻撃等の防御	4-4	プラットフォームセキュリティ	4-4-1	ハードウェア・ソフトウェアの安全な構成	ハードウェア・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No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須 ・規程や手順書などの名称（：最新の更新日） ・記録の名称 ・その他	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
4-4-1-1	・パソコン、サーバ、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又は無効化すること	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、端末へ導入するソフトウェアは「管理部が決めたもの」もしくは「新規のソフトウェアは管理部長の承認が必要」としている。	適合	
4-4-1-2	・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること	Yes/No	はい	Active Directoryのグループポリシーにて自動再生を無効化している。	適合	
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	Yes/No	はい	情報セキュリティ関連規程（：2025/3/31更新）にて、サーバ及びネットワーク機器の設定変更は管理部の情報システム担当が実施することを定めている。 [再確認に対する回答] 設定作業実施時には申請・承認を行っていない。	不適合	[不適合の理由] 情報システム担当が実施する場合であっても、サーバ及びネットワーク機器の設定変更を実施する際には都度申請・承認が必要であることを規程等で定める必要があります。

テーマ7

スライド構成（テーマ２から７まで同様のスライド構成）

1枚目：企業からの回答を記載したシート　【事前配布】
2枚目：参加者が評価を記載するためのブランクシート　【事前配布】
3枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート
4枚目：想定される再確認の内容に対する回答を記載したシート
5枚目：企業の回答（初回・再確認）と最終評価の模範回答を記載したシート

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項 テーマ7-1
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	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No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
5-1-1-1	**・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入すること**	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入していますか。 ・具体的にはどのような仕組みですか。	記述式	・ファイアウォール機能の付いたルータを導入し社内外の通信を監視 ・社内からWebサイトも必要最低限のものしか閲覧できないようにフィルターをかけている		・ファイアウォールは、ネットワーク通信を制限する機能であり、社内から社外への通信や社外から社内への通信を制限するものである。原則として、すべての通信を拒否し、必要な通信のみ許可するルールとする必要がある。業務上必要なサービスから必要な通信を検討し、ファイアウォールのルールを確実に設定することが必要になる。
5-1-1-2	**・ネットワーク機器等のログやアラートを分析し、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。**	・ネットワーク機器のログやアラートを分析し、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、セキュリティ担当部署の担当者又は管理者により判断されますか。 ・判断基準はどのように定めていますか。	記述式	・ファイアウォールの警告レベルにて判断		・担当者によって違う判断にならないような判断基準を定め、複数の担当者間においても判断が同じになるような教育や訓練をしておくことが望ましい。 ・アラートの通知情報だけでなく運用上の影響の有無などの情報も判断基準として考慮することが望ましい。 ・セキュリティインシデントが発生した場合は、ある一定の短時間の間にアラートが複数の機器から複数通知されることが考えられる。そのような状況も想定しておくことが望ましい。

テーマ7-2

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
5-1-1-1	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入すること			・「社内外ネットワークの境界」とは、インターネットと社内環境の間の出入口のことを指す。 ・本項目では、不正アクセスや不正侵入を検知・遮断する機器IPS、IDS)の導入までは求めない。	弊社では、社内外ネットワーク境界にUTMを設置しており、インバウンド及びアウトバンドの不正通信検知や危険サイトのアクセス遮断、ウイルス遮断等を行っている。
5-1-1-2	・ネットワーク機器等のログやアラートを分析し、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。			・把握している事象がセキュリティインシデントにあたるかの判断を行う主体や判断のプロセス、判断基準が示されているかを確認すること。 ・セキュリティインシデントにあたるかの判断を行う主体は、セキュリティ担当部署の担当者・管理者等の個人、又は情報セキュリティ委員会等でもあり得る。 ・判断基準は、アラートの通知情報だけでなく運用上の影響の有無などの情報も加味して行われるもののほか、自社におけるセキュリティインシデントの定義等として示される場合もあり得る。	弊社では、セキュリティインシデント、又はそれが疑われる事象を検知した際、発見者(ログやアラートの分析を行う従業員又はセキュリティベンダーの作業従事者等)が情報セキュリティ委員会に遅滞なく報告するよう規定している。 情報セキュリティ委員会は、報告された事象がセキュリティインシデントに該当するかの判断を行う。 情報セキュリティ委員会では、以下に示す当社におけるセキュリティインシデントの分類に基づき、システム運用の委託先とも相談したうえで、報告事象がそれらに該当するかの判断を行う。 (1)セキュリティに対する侵害 例 不正アクセスによる情報漏えい、従業員による情報漏えい、ウイルス・マルウエア感染、DoS 攻撃、記録媒体等の紛失 等 (2)システム・ネットワークの故障・損壊 例 電源異常、熱暴走、天災による機器損壊 等 (3)情報資産への脅威

テーマ7-3

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	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No.	評価基準	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）	評価のためのガイダンス ・評価を実施するにあたってのポイントや注意事項	回答例 ・専門家/評価機関が評価を実施するにあたっての模範回答例（回答タイプ：記述式のもの）
5-1-1-1	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入すること			・「社内外ネットワークの境界」とは、インターネットと社内環境の間の出入口のことを指す。 ・本項目では、不正アクセスや不正侵入を検知・遮断する機器IPS、IDS)の導入までは求めない。	弊社では、社内外ネットワーク境界にUTMを設置しており、インバウンド及びアウトバンドの不正通信検知や危険サイトのアクセス遮断、ウイルス遮断等を行っている。
5-1-1-2	・ネットワーク機器等のログやアラートを分析し、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。	再確認	[再確認を要する事項] 1.不審な事象がセキュリティインシデントに該当するかどうかを判断するのは誰ですか。 2.不審な事象がセキュリティインシデントに該当するかどうかを判断する基準はどのように定めていますか。	・把握している事象がセキュリティインシデントにあたるかの判断を行う主体や判断のプロセス、判断基準が示されているかを確認すること。 ・セキュリティインシデントにあたるかの判断を行う主体は、セキュリティ担当部署の担当者・管理者等の個人、又は情報セキュリティ委員会等でもあり得る。 ・判断基準は、アラートの通知情報だけでなく運用上の影響の有無などの情報も加味して行われるもののほか、自社におけるセキュリティインシデントの定義等として示される場合もあり得る。	弊社では、セキュリティインシデント、又はそれが疑われる事象を検知した際、発見者(ログやアラートの分析を行う従業員又はセキュリティベンダーの作業従事者等)が情報セキュリティ委員会に遅滞なく報告するよう規定している。 情報セキュリティ委員会は、報告された事象がセキュリティインシデントに該当するかの判断を行う。 情報セキュリティ委員会では、以下に示す当社におけるセキュリティインシデントの分類に基づき、システム運用の委託先とも相談したうえで、報告事象がそれらに該当するかの判断を行う。 (1)セキュリティに対する侵害 例 不正アクセスによる情報漏えい、従業員による情報漏えい、ウイルス・マルウエア感染、DoS 攻撃、記録媒体等の紛失 等 (2)システム・ネットワークの故障・損壊 例 電源異常、熱暴走、天災による機器損壊 等 (3)情報資産への脅威

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	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。

テーマ7-4

評価基準No.	評価基準	質問事項 ・申請者が、各評価基準を満たしているかを社内関係部署や委託先に確認する事項について記載	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須	対策実施のためのガイダンス ・要求事項を達成するための対策例や参考情報を記載
5-1-1-1	**・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入すること**	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入していますか。 ・具体的にはどのような仕組みですか。	記述式	・ファイアウォール機能の付いたルータを導入し社内外の通信を監視 ・社内からWebサイトも必要最低限のものしか閲覧できないようにフィルターをかけている		・ファイアウォールは、ネットワーク通信を制限する機能であり、社内から社外への通信や社外から社内への通信を制限するものである。原則として、すべての通信を拒否し、必要な通信のみ許可するルールとする必要がある。業務上必要なサービスから必要な通信を検討し、ファイアウォールのルールを確実に設定することが必要になる。
5-1-1-2	**・ネットワーク機器等のログやアラートを分析し、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。**	・ネットワーク機器のログやアラートを分析し、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、セキュリティ担当部署の担当者又は管理者により判断されますか。 ・判断基準はどのように定めていますか。	記述式	・ファイアウォールの警告レベルにて判断 [再確認に対する回答] 1. 不審な事象がセキュリティインシデントに該当するかどうかの判断は情報システム担当から報告を受けた管理部長が行う 2.ファイアウォールからの警告レベルがあらかじめ定めた水準以上のものであればインシデントに該当と判断する		・担当者によって違う判断にならないような判断基準を定め、複数の担当者間においても判断が同じになるような教育や訓練をしておくことが望ましい。 ・アラートの通知情報だけでなく運用上の影響の有無などの情報も判断基準として考慮することが望ましい。 ・セキュリティインシデントが発生した場合は、ある一定の短時間の間にアラートが複数の機器から複数通知されることが考えられる。そのような状況も想定しておくことが望ましい。

テーマ7-5

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続･データの監視	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No.	評価基準	回答のタイプ	回答欄 - 回答のタイプが「Yes/No」の場合、「はい」か「いいえ」を記載	回答の補足 回答のタイプが「Yes/No」の場合、記載は必須	評価結果 -適合 -再確認 -不適合 から選択	評価結果の補足 ・評価結果の補足を記載 - [適合]の場合、補足があれば記載（任意） - [再確認]の場合、評価結果の補足欄に再確認を要する事項について記載（必須） - [不適合]の場合、評価結果の補足欄にその理由を記載（必須）
5-1-1-1	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、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)による監視、制御の仕組みを導入すること	記述式	・ファイアウォール機能の付いたルータを導入し社内外の通信を監視 ・社内からWebサイトも必要最低限のものしか閲覧できないようにフィルターをかけている		適合	
5-1-1-2	・ネットワーク機器等のログやアラートを分析し、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。	記述式	・ファイアウォールの警告レベルにて判断 [再確認に対する回答] 1．不審な事象がセキュリティインシデントに該当するかどうかの判断は情報システム担当から報告を受けた管理部長が行う 2.ファイアウォールからの警告レベルがあらかじめ定めた水準以上のものであればインシデントに該当と判断する		適合	


IPA