2026年3月最新版

CISA保有コンサルタント監修

経産省「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」

制度概要と対策の始め方

JIMUREQ Consulting

目次

※本資料は2025年12月26日に公表された制度構築方針をもとに作成しています。制度内容は今後変更される可能性があります。

なぜ今、サプライチェーン・セキュリティが経営課題なのか？

現在、サイバー攻撃の手口は、守りの固い大企業を直接狙うものから、
その取引先である中堅・中小企業を経由して侵入する「サプライチェーン攻撃」へと広がりつつあります。

そのため、「自社には盗まれるような情報がないから大丈夫」という考え方だけでは、十分とは言えなくなっています。
攻撃者にとって、セキュリティ対策が十分でない企業は、標的そのものではなく、大手企業へ侵入するための経路として利用される可能性があるためです。

もし自社が起点となるインシデントが発生した場合、調査・復旧対応に多くのコストが発生するだけでなく、
取引先へ影響が及ぶ可能性もあり、場合によっては取引関係の見直しにつながるケースもあります。

こうした背景を受け、経済産業省は「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」を策定しています。
2027年3月の制度開始以降、企業の対策状況は★1～★5の5段階で可視化される予定です。

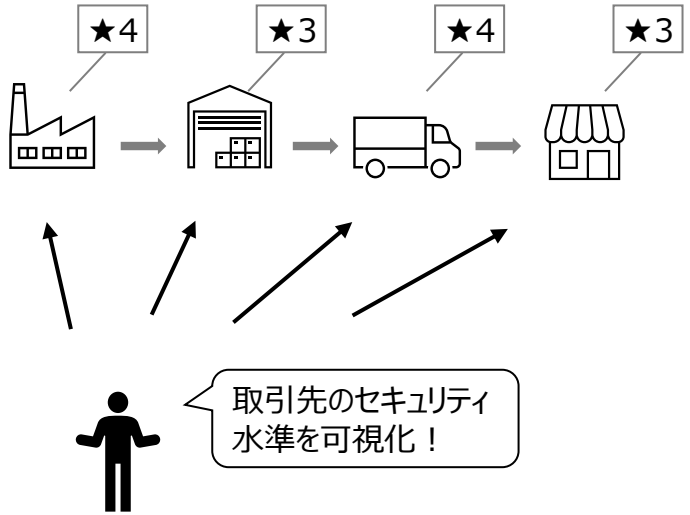
この制度は単なる形式的な評価ではなく、今後、多くの業界で取引先選定の参考指標として活用されていく可能性があります。

本書では、CISA（公認情報システム監査人）の知見をもとに、この制度のポイントと企業が取るべき実務対応をわかりやすく解説します。
限られたリソースの中でも現実的に進められる対策の考え方を整理し、企業としての信頼を維持していくための第一歩を紹介します。

経産省が定める新評価制度とは

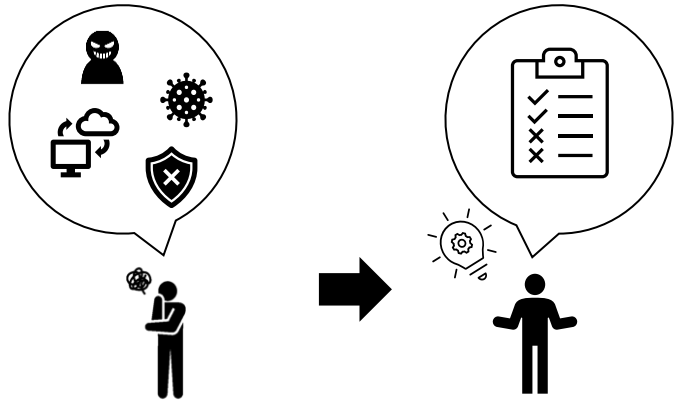
Point1：どんな仕組み？

「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」は、**企業のセキュリティ水準を★1~5の5段階で可視化し、取引先などが参考**にできる仕組み。



Point2：新制度の背景は？

サプライチェーンを通じたセキュリティインシデントが頻発しており、発注元・委託先の個社努力だけでは限界があるため、**対象とするリスク、必要な対策を提示し、リソースの限られる中小企業でも適切な対策が容易に取れる**ようにするため。

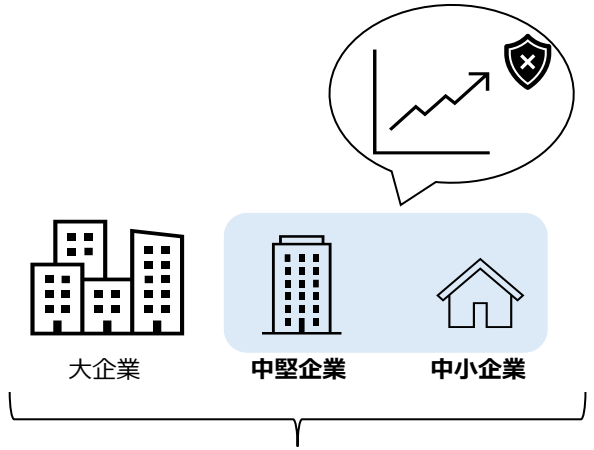


驚異の複雑化、高度化に
個別対応では限界・・・

リスクや対策が一覧化され
中小企業でも対応可能！

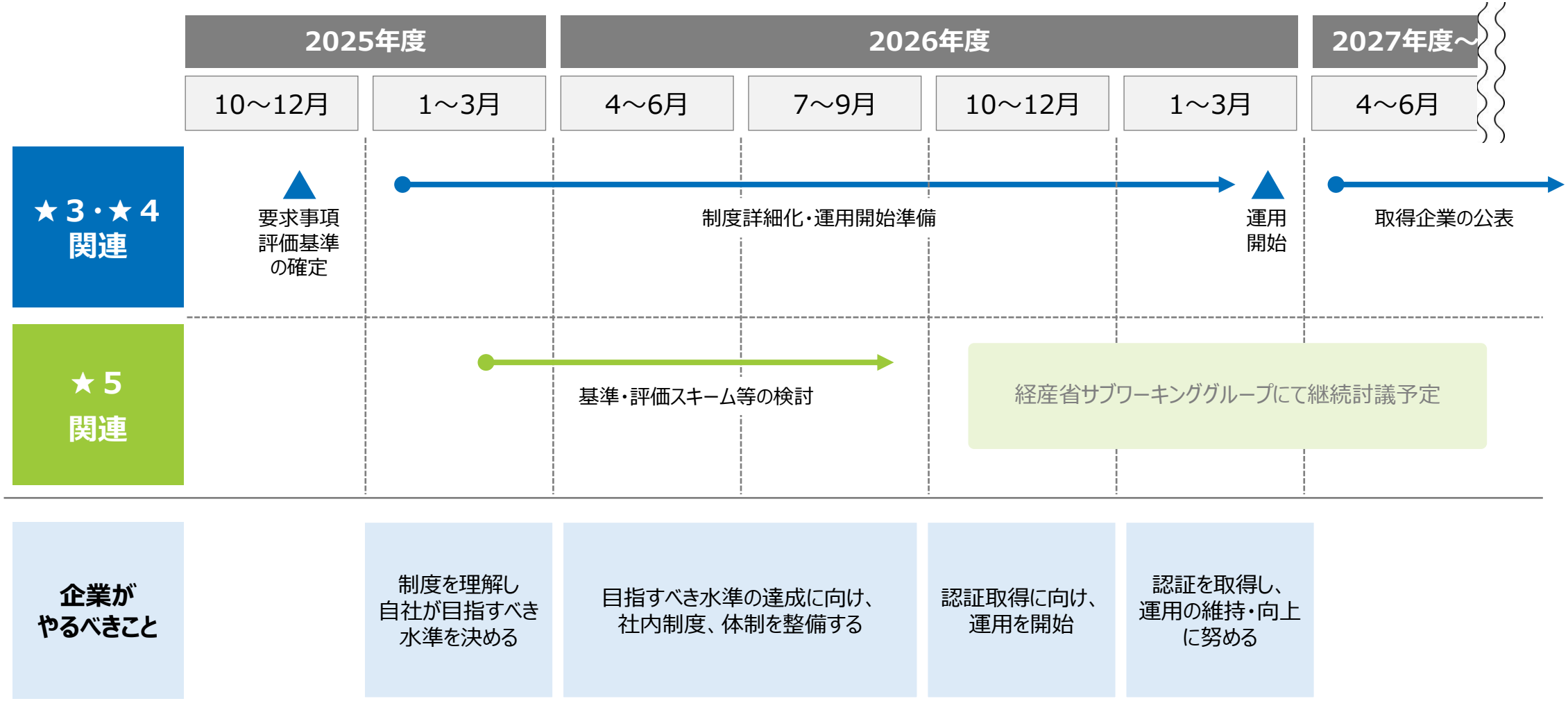
Point3：対象となる企業は？

業種・企業規模を問わず対象となり、特に、**中堅中小企業が川中、川下で対応を求められる場面を想定**して、企業に求められるセキュリティ水準が定められている。



サプライチェーン全体が対象となるが、
特に中堅中小企業による活用効果が大きい

2027年3月の運用開始を見据え、今から制度理解、現状分析を始めることが重要

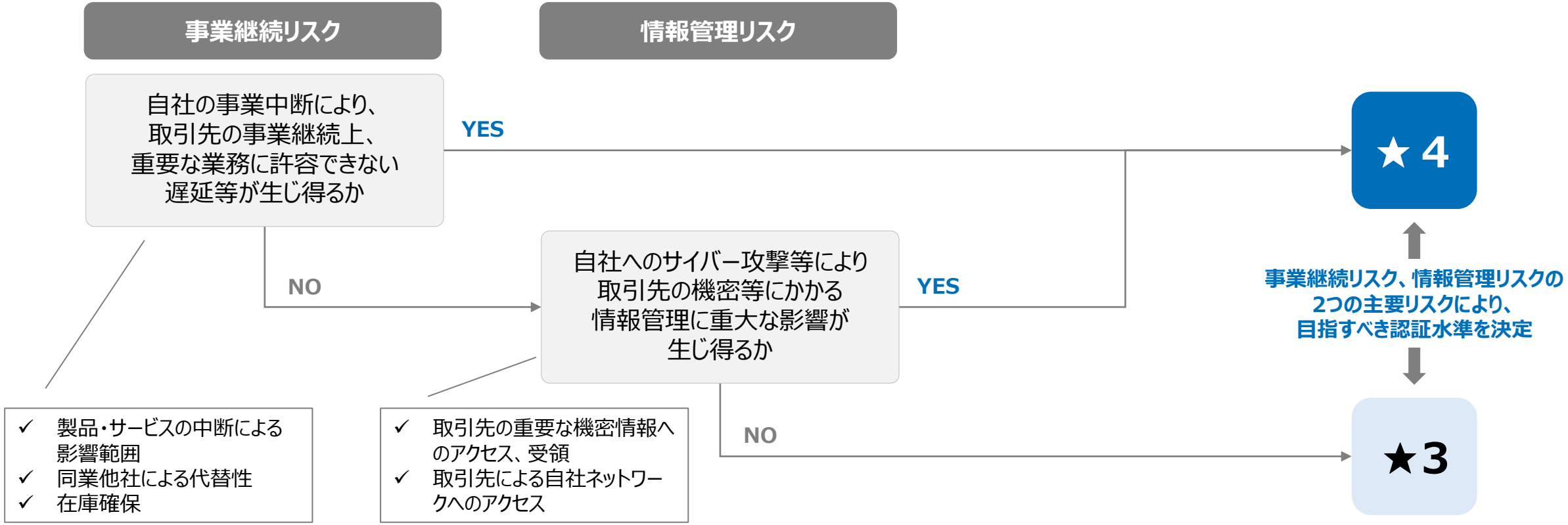


自社の置かれている状況を踏まえ、目指すべき水準(★3or★4)を定めるところからスタート

	★3	★4	★5
想定される脅威	広く認知された脆弱性を悪用する**一般的なサイバー攻撃**	**供給停止により、サプライチェーンに大きな影響**をもたらす企業、**機密情報等漏洩により大きな影響**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** ✓ **基本的な組織的対策とシステム防御**が中心	✓ サプライチェーン企業が**標準的に目指すべきセキュリティ水準** ✓ 組織ガバナンス、取引先、システム防御、インシデント対応等、**包括的な対策**	✓ サプライチェーン企業が**到達点として目指すべき対策** ✓ 国際規格等における、リスクベースの考え方に基づく、**現時点でのベストプラクティス**
評価項目数	✓ 要求事項：**26** 個 ✓ 評価基準：**83** 個	✓ 要求事項：**44** 個 ✓ 評価基準：**74** 個	★5の評価基準や評価スキームは2026年度に具体化される予定
評価スキーム	**自己評価** ＋ **セキュリティ専門家による文書確認および助言**	**認定第3者による評価** (文書に加え、実地審査、技術検証を実施)	
認証の有効期間	1年	3年 （1年ごとの自己点検が必要）	

サプライチェーンにおける立ち位置、取引先へ与える影響を考慮し、自社が取得すべき認証の水準を決める

目指すべき認証水準の判断フロー



※本来は、取引先の選定・評価を行う際に、自社に与える影響に鑑み、取引先に求めるセキュリティ水準を決めるための判断基準となるものだが、
自社が目指すべきセキュリティ水準の検討にあたっては、「自社が取引先の事業に与える影響の程度」を判断基準とする

2025年12月現在において、以下の7領域にて、計44個の要求事項、計156個の評価基準が提案されている

1.ガバナンスの整備

概要
経営層の関与を含め、組織としてセキュリティを統括・管理する体制が整備されているかを確認する領域。

主な観点例
・セキュリティ責任者（CISO等）の明確化
・セキュリティ方針・規程の策定
・経営層への定期的な報告・是正

2.取引先管理

概要
取引先・再委託先を含めたサプライチェーン全体のセキュリティ管理ができているかを確認する領域（本制度の特徴的要素）。

主な観点例
・機密情報を共有する取引先の把握
・重要取引先のセキュリティ対策状況の確認
・インシデント発生時の役割分担の明確化

3.リスクの特定

概要
自社IT基盤や情報資産、外部サービス等の把握を通じて、守るべき対象とリスクを特定できているかを確認する領域。

主な観点例
・情報資産・システム構成の把握
・クラウド等の外部情報サービスの管理
・脆弱性情報の把握体制

4.攻撃等への防御

概要
不正アクセスやマルウェア等の攻撃を防止・低減するための技術的対策が実装されているかを確認する領域。

主な観点例
・ID・アクセス権管理
・パスワード管理、多要素認証
・ネットワーク境界防御、パッチ適用、マルウェア対策

5.攻撃等の検知

概要
侵入や異常を早期に検知できる仕組みが整備されているかを確認する領域。

主な観点例
・ログの取得・保管
・ネットワークや端末の監視
・異常検知後の分析体制

6.インシデントへの対応

概要
セキュリティインシデント発生時に、被害拡大を防ぎ、適切に対処できる体制・手順があるかを確認する領域。

主な観点例
・インシデント対応手順書の整備
・社内外（取引先等）への報告・連携方法の定義

7.インシデントからの復旧

概要
インシデント後に、事業やシステムを適切に復旧・継続できる体制があるかを確認する領域。

主な観点例
・バックアップ、復旧手順の整備
・復旧目標（RTO/RPO）の設定
・事業継続を意識した復旧計画

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
1.ガバナンスの整備	1-1. 組織の状況	1-1-1. セキュリティに関する法令、契約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。	（該当項目なし）	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も含めた、関係者からの要求事項
				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。
	1-2. 役割、責任、権限	1-1-2. 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。	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理解し、その対応について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。
			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。	

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
1.ガバナンスの整備	1-2. 役割、責任、権限	1-2-2. 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。	（該当項目なし）	1-2-2-1. ・サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。 1-2-2-2. ・入手した情報及びログの相関分析により、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。
		1-2-3. 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。 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。	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。
	1-3. ポリシー	1-3-1. 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。 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。	1-3-1-4. ・年１回以上の頻度でセキュリティ対応方針及び社内で運用するその他のセキュリティ関連ルールの内容を点検すること。
	1-4. 監督	1-4-1. 各年度の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共に、報告結果を対策の推進に反映すること。	（該当項目なし）	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)及び関係部門に対して、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、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、1-3-1-3、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、3-1-5-2、3-2-1-5、4-1-7-2、4-1-9-3、4-2-1-6、4-2-2-3、5-1-2-3、6-1-1-5 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、関係部門への共有、計画への反映及び不備の是正を実施すること。

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準	
			★3	★4
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。	2-1-1-3. ・自社の機密情報を共有している取引先について、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情報・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
			2-1-1-2. ・年1回以上の頻度でNo.2-1-1-1において把握すべき情報の内容を点検すること。	
		2-1-2. 他社との間で、機密情報の取扱い方法を明確にすること。	2-1-1-2. ・自社の機密情報を共有する取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項の取り交わすこと。 - 機密情報の定義 - 機密情報の取扱い (表示、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	(該当項目なし)
		2-1-3. 重要な機密情報を取り扱う取引先のセキュリティ対策状況を把握すること。	(該当項目なし)	2-1-4-1. ・以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握すること。 [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準	
			★3	★4
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	2-1-4. 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 ・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について、以下の事項を定めること。 - セキュリティインシデント発生時の相手方への通知義務 - セキュリティインシデント発生時の連絡先 - 再発防止策の協議方法	（該当項目なし）
		2-1-5. 取引先との契約終了時に機密情報及びアクセス権を回収又は破棄すること。	（該当項目なし）	2-1-5-1 ・自社の機密情報を提供・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)を整備及び運用すること。

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
3.リスクの特定	3-1. 資産管理	3-1-1 ハードウェア、OS、及びソフトウェアの把握	3-1-1-1. ・適用範囲内の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。	3-1-1-5. ・適用範囲内の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。
			3-1-1-2. ・適用範囲内のサーバ、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。	3-1-1-6. ・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。
			3-1-1-3. ・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。	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で把握すべき情報の内容について、点検すること。
		3-1-2. ネットワークの一覧作成	3-1-2-1. ・適用範囲内の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目的に関する情報を含めること。	3-1-2-3. ・適用範囲内の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。
			3-1-2-2. ・適用範囲内の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。	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。
		3-1-3 外部情報サービスの管理	3-1-3-1. ・以下の内容を含む外部情報サービスの利用ルールを定めること。 - 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ること。 - 外部情報サービスの利用時にセキュリティ要件を満たしているかサービス内容を確認し、自社の役員又は従業員が承認すること。	（該当項目なし）
			3-1-3-2. ・外部情報サービスの接続先と機密情報の取扱いについて取り交わすこと。	

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
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	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	3-1-4-4. ・年1回以上の頻度でNo.3-1-4-3で把握すべき情報の内容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)を整備及び運用すること。
			3-1-4-3. ・機密区分のうち、高い機密区分の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。	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消去すること。 ※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
			3-1-4-2. ・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。	3-1-4-8. ・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消去した記録又は業者の廃棄証明書を保管すること。
		3-1-5. リモートワークにおけるルール	（該当項目なし）	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、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。 - 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 - 個人所有端末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. ・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。

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
3.リスクの特定	3-2. リスクアセスメント	3-2-1. 脆弱性の管理体制	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。 3-3-1-3. ・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。 3-4-1-4. ・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。 3-5-2-1. ・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。	（該当項目なし）

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	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 の発行・変更・削除の手続を定め、適切に運用すること。	4-1-1-1. ・自社の従業員、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における特別なアクセス権限が不要になった場合(例えば、スタッフ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。	（該当項目なし）
		4-1-2. 管理者IDの発行・変更・削除の手続を定め、適切に運用すること。	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。 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に対して役割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. ・システム開発を実施する役員、従業員、派遣社員及び受入出向者が本番環境において、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。 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。	（該当項目なし）

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-1. アイデンティティ管理、認証、アクセス制御	4-1-4. アカウントロック制御	4-1-4-2 ・業務で利用するシステムを構成する端末へのログオン(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、設定が可能な場合、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10回以上失敗するとアカウントをロックする。 4-1-4-2. ・No.4-1-4-1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。 4-1-4-3. ・パソコ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。	（該当項目なし）
		4-1-5. パスワード設定ルール	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こと。 - 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の使い回さないこと。	（該当項目なし）

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-1. アイデンティティ管理、認証、アクセス制御	4-1-3 認証の強度・実装方法の決定	4-1-3-1. ・すべてのユーザIDについて、アプリケーション及び情報機器へのアクセスを許可する前に、一意の認証情報(パスワード等)でユーザを認証すること。 4-1-3-2. ・重要な情報を取り扱うと考えられる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。	4-1-3-5. ・重要情報を取り扱うシステムにおいて、★3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、常に多要素認証を使用すること。 - 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機密区分が高い情報を取り扱うシステムにアクセスする場合
		4-1-4. アカウントロック制御	4-1-4-1. ・業務で利用するシステムを構成する端末へのログオン(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、設定が可能な場合、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10回以上失敗するとアカウントをロックする。 4-1-4-2. ・No.4-1-4-1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。 4-1-4-3. ・パソコ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。	（該当項目なし）

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-1. アイデンティティ管理、認証、アクセス制御	4-1-5. パスワード設定ルール	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こと。	（該当項目なし）
			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こと。 - 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の使い回さないこと。	
		4-1-6. パスワード管理ルール	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ことを定め、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。	（該当項目なし）
			4-1-6-2. ・設定可能な場合はパスワードの定期的な変更を強制しないこと。	
			4-1-6-3. ・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。	
		4-1-7. アクセス権の管理ルール	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。	4-1-7-2. ・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. ・重要情報を扱うシステムは、情報利用者及びシステム管理者の権限を分離し、個人に権限が集中しない環境とすること。
				4-1-7-6. ・重要情報を扱うシステムは、付与したアクセス権限の運用/利用状況を定期的に確認すること。

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-1. アイデンティティ管理、認証、アクセス制御	4-1-8. サーバ設置エリアへの入退室管理	（該当項目なし）	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. ・管理者を定めて、施錠管理を実施すること。 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。
		4-1-9. 可搬媒体の制限	（該当項目なし）	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(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(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。

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-2. 意識向上とトレーニング	4-2-1 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。	（該当項目なし）	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. ・役員、従業員、派遣社員及び受入出向者を対象に、年１回以上の頻度で、セキュリティの重要性を再認識する機会を設けること。 4-2-1-3. ・職場特有のリスクの理解及びルール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。 4-2-1-4 ユーザIDにおける特別なアクセス権限が不要になった場合(例えば、スタッフ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。・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 4-2-1-5. ・No.4-2-1-4で実施した教育の実施状況を記録し、保管すること。 4-2-1-6. ・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。
		4-2-2 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。 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。	（該当項目なし）

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-3. データセキュリティ	4-3-1. 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。	（該当項目なし）	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. ・No.3-1-4-3における高い機密区分の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。
		4-3-2. 重要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。	（該当項目なし）	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。
		4-3-3. 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。	（該当項目なし）	4-3-3-1. ・以下を明文化し、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。 -送信履歴が残らない方法で、社外へファイル転送することを禁止すること。
				4-3-3-2 ・No.4-3-3-1における取組の実施状況を記録し、記録として保管すること。
		4-3-4. 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組織で取り扱うデータのバックアップを取得すること。	（該当項目なし）
			4-3-4-2. ・重要情報については、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。	

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	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、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又は無効化すること。	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。
			4-4-1-2. ・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。	4-4-1-5. ・デフォルトユーザ ID の利用を停止すること。
			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。	4-4-1-6. ・利用するOS及びソフトウェアについて、ベンダーによる推奨セキュリティ設定を参考に、標準構成・設定ルールを定めること。
		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改を実施すること。	(該当項目なし)	4-4-2-1. ・利用するOS及びソフトウェアについて、以下のいずれかを適用すること。 - 全ての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利用する場合(例えば、代替システムを調達する必要があり、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、No.4-4-4-3で求める脆弱性悪用のリスクを低減する対策を実施すること。
		4-4-3. 情報機器及び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。	(該当項目なし) ー	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
				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。 ※クラウドサービスの利用も対象に含む。 ※クラウドサービスを利用する場合、利用するサービスによって取得できるログの種類、取得方法等が異なることが想定されるが、以下の保管期間の規則を満たせない場合は、クラウドサービス選定時に、それを許容できるかを判断すること。

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準	
			★3	★4
4.攻撃等への防御	4-4. プラットフォームセキュリティ	4-4-4. ハードウェア、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策定し、実行すること。	4-4-4-1. ・適用範囲内のシステム、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。	（該当項目なし）
			4-4-4-2. ・以下のいずれかに該当する場合、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 v3 の基本スコアが7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。 [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	
			4-4-4-3. ・やむを得ずNo.4-4-4-2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。 - ベンダーよりリリースされる仮想パッチを適用すること。 - 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境界部分に、通信を監視して不正な挙動を検知する機器を導入すること。	

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
4.攻撃等への防御	4-4. プラットフォームセキュリティ	4-4-5. システムをマルウェア感染から保護すること。	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。	4-4-5-4. ・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。
			4-4-5-2. ・情報機器に応じたスキャン範囲及び頻度を規定し、スキャンを実行すること。	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。
			4-4—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。	
	4-5. 技術インフラのレジリエンス	4-5-1. 内外のネットワークを適切に分離し、境界部分を防護すること。	4-5-1-1. ・すべ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、又はリモート管理アクセスを完全に無効化すること。	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。
			4-5-1-2. ・ファイアウォール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. ・ファイアウォール及びルータに係る認証は、No.4-1-3からNo.4-1-6までに定める認証、パスワード設定等に関する基準を満たすこと。	
			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デフォルトで遮断すること。	
			4-5-1-5. ・すべ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、担当者によって承認され、定められていること。	4-5-1-9. ・社外公開サーバ、重要情報を扱うサーバ及び工場ネットワーク/OA ネットワークについて、専用のネットワークセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定すること。
			4-5-1-6. ・すべ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、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。	
		4-5-2. 社内から社外への不正な通信を遮断する対策を実施すること。	（該当項目なし）	4-5-2-1. ・社内から不正なサーバへの通信を遮断する仕組みを導入すること。

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準 ★3	評価基準 ★4
5.攻撃等の検知	5-1. 継続的監視	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。	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。 -アラートが即時発報されること。 -関連したセキュリティ事象の速報レポートが作成され、通知されること。	（該当項目なし）
		5-1-2. ハードウェア及びソフトウェアの状態及び挙動を監視すること。	（該当項目なし）	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. ・利用を認めるもの以外のソフトウェアを役員、従業員、派遣社員及び受入出向者が自由にインストールできないよう社内ルールを定めること。 5-1-2-3. ・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。 5-1-2-4. ・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システムを導入すること。
	5-2. 有害事象の分析	5-2-1. セキュリティインシデントとして扱う対象範囲を明確にし、運用していること。		5-2-1-1. ・以下の対象範囲を定め、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。 -セキュリティインシデントとして扱う事象 -セキュリティインシデントのレベル 5-2-1-2 ・No.5-1-1で導入されるネットワーク機器又はサービスからのアラートを受け取った担当部署の責任者は、No.5-2-1-1で定めた対象範囲に基づき、以下を分析し、判断すること。 - 検知された事象がセキュリティインシデントに該当するか - (セキュリティインシデントに該当する場合)どのレベルのインシデントに該当するか

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準	
			★3	★4
6.インシデントへの対応	6-1 インシデント管理	6-1-1. 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。	6-1-1-1. ・セキュリティインシデントへの対応手順を定めること。	（該当項目なし）
			6-1-1-2. ・No.6-1-1-1で定めたセキュリティ対応手順には以下の手順を含んでいること。 ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告	
			6-1-1-3. ・セキュリティインシデントの基準並びに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への報告又は情報共有を含む。)との連絡先及びルートを定めること。	
			6-1-1-4. ・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。	
			6-1-1-5 ・年1回以上の頻度でNo.6-1-1-3及びNo.6-1-1-4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。	
			6-1-1-6. ・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。	
			6-1-1-7. ・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。	

要求事項・評価基準案(詳細)

大分類	中分類	要求事項	評価基準	
			★3	★4
7.インシデントからの復旧	7-1. インシデント復旧計画の実行	7-1-1. 事業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。)	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、以下の対策を構じること。 -求められる復旧ポイントへ復帰可能なバックアップ及びトランザクションデータログを保管すること。 -No.4-3-4-3で定めたバックアップのリストア手順書どおりに、かつ、求められる復旧時間で復元ができることを確認すること。

★3★4要求事項に基づく対策を行ったうえで認証評価に進む（具体的な評価手法などガイダンス資料は今後公開される見込み）

事前準備フェーズ

現状アセスメント/課題識別

★3★4の要求項目ごとに求められる水準と現状の対策状況を比較し、対応が不十分である項目で識別する。

計画策定

対応が不十分と診断された項目に対し、社内ルール整備、ツール導入などの対策の実行計画を立てる。

課題対応実施

策定した計画に基づきルール整備、ツール導入などを進めていく。

アウトプットイメージ

アセスメント結果

1-1-1 ○
十分なルールが定められている
1-1-2 ×
点検がな行われていない
1-1-3 ×
ルールの周知が行われていない
⋮

課題対応計画

課題1
ルールの最新化
課題2
定期点検の開始
課題3
社内研修の実施
⋮

課題対応

✓社内ルール整備
✓運用記録
✓セキュリティ構築
⋮

検証評価フェーズ

★3

- **自己評価**：所定の様式にて、認証取得希望組織自身が評価結果を取りまとめる
- **文書確認**：社内外のセキュリティ専門家が自己評価の結果をレビューし、十分な記載がされているか確認
- **是正・改善**：不適合が発見された場合、適切な是正対処を行い、専門家の了承を得る

→ ★3取得へ

★4

- **自己評価**：★3と同様
- **文書確認**：評価機関、技術検証事業者が文書確認を行う
- **実地審査**：社内ルール、管理プロセス、インシデント対応手順など重要な対策について証跡確認を含め評価
- **技術検証**：VPN・ルータなどインターネットに接続されている機器のうち、侵入リスクの高いものについて、脆弱性検査等を行う
- **是正・改善**：不適合事項の是正報告を一定期間内に提出し、評価化機関への了承を得る

→ ★4取得へ

評価ガイドラインは未整備ではあるものの、ほとんどの評価基準は既存の基準（ISO27001:2022など）を参照し作成されているため、ISO27001認証（ISMS）取得における水準を目指すことで、先行対応が可能

ISO27001:2022　附属書Aの管理策（例）

組織的管理策（37項目）

- ✓ 情報セキュリティ基本方針および関連規程が文書化され、定期的に見直されている
- ✓ 情報セキュリティに関する役割・責任（責任者、担当者等）が明確に定義されている

人的管理策（8項目）

- ✓ 従業員に対して情報セキュリティ教育・訓練が定期的に実施されている
- ✓ 入社・異動・退職時における権限管理や情報取扱いルールが定められている

物理的管理策（14項目）

- ✓ オフィスや重要エリアにおいて入退室管理が実施されている
- ✓ 情報資産（PC、記録媒体等）の盗難・紛失防止対策が講じられている

技術的管理策（34項目）

- ✓ システムや情報資産へのアクセス制御（権限設定・制限）が適切に行われている
- ✓ 利用者認証（ID・パスワード、多要素認証等）が実装されている

ISO27001（ISMS)取得にあたり目指す水準

① 社内ルール・セキュリティ製品の設定など、**必要な対策が定義・明文化されている**こと

② 上記が**定期的に見直され従業員に周知されている**こと

★3の要件

③ 自社が定めたルールに沿って**継続的な運用を行い、その実績が記録されている**こと

④ 定期的な活動を振り返り**十分な運用が継続されているか自己点検している**こと

★4の要件

サプライチェーンセキュリティ対応は、企業全体で取り組む経営課題に

本制度の導入により、企業のセキュリティ対策状況は★によって可視化され、
取引先などが参考にできる仕組みとして運用される予定です。

これにより、企業のセキュリティ対策は自社内部のIT課題にとどまらず、
取引関係やサプライチェーン全体の信頼性にも関わるテーマとして位置づけられるようになります。

また、本制度で求められる対応は、技術的なセキュリティ対策の導入だけではありません。
経営層の関与を含めたガバナンス体制の整備、社内ルールの明文化と継続的な運用、取引先を含めたリスク管理など、
組織全体で取り組むべき事項が幅広く含まれています。

そのため、制度への対応を検討する際には、まず自社が目指すべき認証水準を整理したうえで、
現在の対策状況とのギャップを把握し、優先度を踏まえた対応計画を策定していくことが重要になります。

こうした取り組みを段階的に進めていくことが、サプライチェーンの一員として求められるセキュリティ水準を満たし、
企業としての信頼を維持していくことにつながります。

JIMUREQ Consultingでは検討状況に応じて
壁打ち、クイックアセスメント、具体的な認証取得対策まで、幅広く対応可能です

支援プラン	想定ニーズ	事前準備フェーズ			検証評価フェーズ
		現状アセスメント/課題識別	課題対応/計画策定	課題対応実施	
壁打ちプラン クイックアセスメント	✓ 主要な対策は自社内で実施予定だが、外部専門家のアドバイスが欲しい	**1~2回/月程度での会議参加ベースのご支援を想定** 社内で進めている対策のレビュー、評価基準の個別解説、製品選定のアドバイス、他社事例調査など、必要最低限の工数でのアドバイザリー支援を実施			経産省より、具体的な評価プロセスのガイドラインが公表され次第、サービス提供について検討予定
診断プランA クイックアセスメント	✓ 現段階では情報収集が中心だが自社のセキュリティ対策状況を評価してもらいたい	**2週間~1か月でのご支援を想定** 各評価基準に対し、ヒアリング・調査票による対策状況の簡易評価レポートを作成し、★3/★4取得に向けた対応計画の素案を作成			
診断プランB ★３取得対策	✓ 現段階から★３認証取得に向けた具体的な対策を開始したい ✓ 取引先から、★3認証取得を求められる可能性がある	**2か月でのご支援を想定** 各評価基準に対し、ヒアリング・社内文書閲覧・現地視察を中心とした、対策状況の評価レポートを作成し、★3/★4取得に向けた社内ルール整備、ツール導入の実行計画案まで作成		社内ルール整備、ツール実装など課題対応の実行支援は別途ご提案	
診断プランC ★４取得対策	✓ 現段階から★４認証取得に向けた具体的な対策を開始したい ✓ 取引先から、★４認証取得を求められる可能性がある	**2か月でのご支援を想定** 各評価基準に対し、ヒアリング・社内文書閲覧・現地視察に加え、技術的なセキュリティ対策状況を検証のうえ評価レポートを作成。	**1か月でのご支援を想定** 評価結果をもとに、社内ルール整備、ツール選定および設定方針の初期案作成を行い、実行計画案の作成までを支援	社内ルール整備、ツール導入など課題対応の実行支援は別途ご提案	

※ 具体的な支援期間は、企業規模・スコープ等により変動

お問い合わせ

JIMUREQ Consulting株式会社

03-6161-2556

info@jimureq.com

https://jimureq.com

JIMUREQ Consulting