登録セキスペ活用
保有スキルの可視化 説明資料

2025年11月

独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

中小企業へのセキュリティ支援領域と必要スキル

IPA

- 令和6年度セキュリティ人材活用促進実証では、**中小企業へのセキュリティ支援領域**として、**６つの支援領域**を定め、**支援に必要とされる専門家スキル**の洗い出しを行い、項目ごとに専門家の実行レベルを問うアンケート項目を作成した。

《セキュリティ専門家スキル調査アンケート項目の設計》

NIST Cybersecurity Framework 2.0
1.統治（Govern）
2.特定（Identify）
3.防御（Protect）
4.検知（Detect）
5.対応（Respond）
6.復旧（Recover）

セキュリティ支援領域
1. セキュリティ対策の体制づくりと管理
2. セキュリティリスクの識別
3. セキュリティ対策の実践と運用の強化
4. サイバー攻撃の検知と監視、検知後の運用の策定
5. セキュリティインシデント発生時の対応
6. インシデントからの復旧とコミュニケーション

①中小企業へのセキュリティ支援領域として「NIST Cybersecurity Framework 2.0：Small Business Quick-Start Guide※（以下「NIST CSF2.0という」）」を参考に６つの支援領域を定めた。
※ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
②NIST CSF2.0ガイドに示された中小企業向け実行項目を基に、支援内容と支援に必要とされる専門家スキル（アセスメント基準）の洗い出しを行った。
③洗い出したスキルは6つの大分類（支援領域）と小項目（アセスメント基準）に整理し、項目ごとに専門家の実行レベルを問うアンケート項目を作成した。

支援領域と必要とされる専門家スキルの対応例（S1：セキュリティ対策の体制づくりと管理）

支援領域	スキルNo.	大分類（アセスメント基準）	No.	必要とされる専門家スキル	NIST CSF2.0 Small Business Quick-Start Guide 実行項目に対応する支援策
1．サイバーセキュリティ対策の方針策定と管理体制づくり	S1	a.経営戦略の理解、経営者とのコミュニケーション	1	経営戦略の理解：企業のビジョン、経営目標、マーケティング戦略を理解し、サイバーセキュリティインシデントがもたらすビジネスリスクを正しく評価できる	・サイバーセキュリティリスクがビジネスの使命達成をどのように妨げるかについて、企業が正しく理解するための支援を行う。(GV.OC-01)
			2	経営層への説得（サイバーセキュリティ対策）：サイバーセキュリティ対策の重要性を他のビジネスリスクと比較しながら経営者に説明できる	・企業が、サイバーセキュリティリスクを他のビジネスリスクと同様に適切に管理するための支援を行う。(GV.RM-03)
			3	経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる	・経営者がサイバーセキュリティを認識し、倫理的、継続的にリスク改善を行える文化を企業内に醸成することの重要性を理解するための支援を行う。(GV.RR-01)
			4	リスクの定量化：サイバー攻撃による潜在的な経営損失を具体的な数値で算出できる	・サイバーセキュリティリスクがビジネスに及ぼす全体的または部分的な潜在的損失を正しく計算・評価する。(GV.0C-04)
			5	サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる	・ビジネスリスクを踏まえ、サイバーセキュリティ対策保険加入の必要性ついて判断支援を行う。(GV.RM-04)
		b. サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の構築と運用	1	サイバーセキュリティ対策責任者の設定：サイバーセキュリティ対策の企画・実行における責任者を特定し、その役割・権限・責任範囲を明確にするための支援を実行できる	・企業におけるサイバーセキュリティ対策の開発と実行の責任者を明らかにするための支援を行う（GV.RR-02）
			2	サイバーセキュリティ対策の方針の策定と運用：サイバーセキュリティ対策の方針の策定から周知、運用、維持を行うための支援を実行できる	・サイバーセキュリティリスクに関する管理方針を周知・徹底し、確実に運用・維持するための支援を行う(GV.PO-01)
		c.外部リスク評価力、コンプライアンス対応	1	サプライチェーンリスクの評価：取引先やクラウドサービス提供者のセキュリティリスクを評価できる	・正式な関係を結ぶ前に、サプライヤーや取引先など第三者がもたらすサイバーセキュリティリスクを洗い出し、評価する支援を行う。(GV.SC-06)
			2	サイバーセキュリティに関する法令、規制、業界固有ガイドライン等の知識：サイバーセキュリティセキュリティに関する法律や、規程、取引要件となる業界のサイバーセキュリティガイドラインを理解し、適用のための支援を実行できる	・法的、規制上、契約上のサイバーセキュリティ要件や業界固有のガイドラインを理解するための支援を行う。(GV.OC-03)

セキュリティ専門家スキル調査項目の設定

- セキュリティ専門家スキル調査アンケート項目は、**6つの支援領域で34項目を設定**し、各項目の実行レベルは**習熟度を自己評価**してもらう方式とした。

スキルNo.	スキル名（支援領域）	実行可能な支援能力（質問項目数）
S1	サイバーセキュリティ対策の方針策定と管理体制づくり（9項目）	「a.経営戦略の理解、経営者とのコミュニケーション(5)」、「b.サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の構築と運用(2)」、「c.外部リスク評価力、コンプライアンス対応(2)」
S2	セキュリティリスクの識別（6項目）	「a.情報資産の洗い出しと情報資産管理台帳の運用設計、潜在リスクの特定と評価(2)」、「b.リスクに基づくサイバーセキュリティ対策の策定、現存対策の評価及び改善点の指摘(2)」、「c.社内外におけるサイバーセキュリティ対策の推進(2)」
S3	サイバーセキュリティ対策の実践と運用の強化（5項目）	「a.アカウント管理、アクセス管理(1)」、「b.データ管理、システムセキュリティ管理、コンテンツセキュリティ管理(3)」、「c.社内セキュリティ教育の策定と運用(1)」
S4	サイバー攻撃の検知と監視、検知後の運用策定（5項目）	「a.セキュリティインシデント対処教育の策定と実施(1)」、「b.ウイルス対策ソフトの運用、システム・ネットワークの監視、外部監視サービスの導入(3)」、「c.インシデント初動の運用設計と教育実施能力(1)」
S5	サイバー攻撃発生時の対応（4項目）	「a.セキュリティインシデント対応（セキュリティインシデント対応計画の策定、セキュリティインデント調査・対応、セキュリティインシデント報告・公表支援）(4)」
S6	セキュリティインシデントからの復旧とコミュニケーション（5項目）	「a.セキュリティインシデント復旧支援(5)」

セキュリティ専門家スキル調査アンケート項目例
（S1-a：経営戦略の理解、経営者とのコミュニケーション）

S1. サイバーセキュリティ対策の方針策定と管理体制づくり

a. 経営戦略の理解、経営者とのコミュニケーション

（0：知識・経験なし　1：基礎知識のみ　2：サポートがあれば実行可能　3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	経営戦略の理解：企業のビジョン、経営目標、マーケティング戦略を理解し、サイバーセキュリティインシデントがもたらすビジネスリスクを正しく評価できる	○	○	○	○
(2)	経営層への説得（サイバーセキュリティ対策）：サイバーセキュリティ対策の重要性を他のビジネスリスクと比較しながら経営者に説明できる	○	○	○	○
(3)	経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる	○	○	○	○
(4)	リスクの定量化：サイバー攻撃による潜在的な経営損失を具体的な数値で算出できる	○	○	○	○
(5)	サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる	○	○	○	○

※スキル調査アンケート項目の実行レベルは、各項目ごとに0～3の4段階で習熟度を自己評価してもらう方式とした。
- 0：知識・経験なし
- 1：基礎知識のみ
- 2：サポートがあれば実行可能
- 3：単独実行可能

登録セキスペの保有スキルの評価と可視化

- セキュリティ専門家スキル調査アンケートの各項目のスキル回答に対し、**保有スキルの評価**を行い、セキュリティ専門家リストの「保有スキル」欄に表記することで、**登録セキスペの保有スキルを可視化**し、**リスト利用者が直感的にセキュリティ専門家のスキルレベルを把握**できるようにした。

《セキュリティ専門家の保有スキル評価例》

例：支援領域S1の小項目(S1-a,S1-b,S1-c) のスキル回答に対する評価

【S1】 サイバーセキュリティ対策の方針策定と管理体制づくり	専門家A	専門家B	専門家C
S1-a 経営戦略の理解、経営者とのコミュニケーション（質問数5） [評点:13点]	3点×5 計15点:評点以上 **スキル有り**	3点×2、2点×3 計12点:評点以下	3点×3、2点×1、1点×1 計12点:評点以下
S1-b サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の策定と運用（質問数2） [評点:5点]	3点×2 計6点:評点以上 **スキル有り**	3点×1、2点×1 計5点:評点以上 **スキル有り**	3点×1、2点×1 計5点:評点以上 **スキル有り**
S1-c 外部リスク評価力、コンプライアンス対応（質問数2） [評点:5点]	3点×1、2点×1 計5点:評点以上 **スキル有り**	3点×2 計6点:評点以上 **スキル有り**	2点×1、1点×1 計3点:評点以下
総合評価	◎	○	

↑上記の例では、専門家AはS1スキル「◎」、専門家Bは「○」、専門家Cは「空白」と表記される。

【保有スキルの評価方法】

Step１：小項目(a,b,c)評点の設定

スキル調査では、支援領域（S1～S6）の下に複数の小項目（a, b, c）を設け、より詳細にスキルの保有状況を聞いている。これらの小項目には、含まれる質問項目数に応じた評点を設定した。

【評点】設定： 質問数が1項目: 評点3点、質問数が2項目: 評点5点、質問数が3項目: 評点7点、質問数が4項目: 評点10点、質問数が5項目: 評点13点

Step２：専門家回答データの小項目ごとの集計と評価

専門家が回答した内容は、小項目ごと単純合計し評点と比較する。評点より高い得点を有するものだけを「スキル有り」と判断。

質問回答：0～３

（0:知識・経験なし、1:基礎知識のみ、2:サポートがあれば実行可能、3:単独実行可能）

Step３：スキル（支援領域）毎の総合評価

全ての回答を小項目ごとに集計・評価後、支援領域ごとにスキルを有しているか、総合評価を行う。

【総合評価】：「◎」（二重丸）：当該スキル領域のすべての小項目が設定評点以上である場合
「○」（丸）：当該スキル領域において1つの小項目のみが設定評点に達していない場合
無表記: 当該スキル領域において2つ以上の小項目が設定評点に達していない場合

Step4:セキュリティ専門家リストへの反映

セキュリティ専門家リストの「保有スキル」欄へ可視化した各セキュリティ専門家のスキル状況を反映する。

【参考】セキュリティ専門家スキル調査項目

◇セキュリティ専門家スキル調査項目（S-1）

支援領域	スキル No.	大分類（アセスメント基準）	No.	必要とされる専門家スキル
１.サイバーセキュリティ対策の方針策定と管理体制づくり	S1	a.経営戦略の理解、経営者とのコミュニケーション	1	経営戦略の理解：企業のビジョン、経営目標、マーケティング戦略を理解し、サイバーセキュリティインシデントがもたらすビジネスリスクを正しく評価できる
			2	経営層への説得（サイバーセキュリティ対策）： サイバーセキュリティ対策の重要性を他のビジネスリスクと比較しながら経営者に説明できる
			3	経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる
			4	リスクの定量化：サイバー攻撃による潜在的な経営損失を具体的な数値で算出できる
			5	サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる
		b.サイバーセキュリティ対策体制の構築、 サイバーセキュリティ対策の基本方針の構築と運用	1	サイバーセキュリティ対策責任者の設定：サイバーセキュリティ対策の企画・実行における責任者を特定し、その役割・権限・責任範囲を明確にするための支援を実行できる
			2	サイバーセキュリティ対策の方針の策定と運用： サイバーセキュリティ対策の方針の策定から周知、運用、維持を行うための支援を実行できる
		c.外部リスク評価力、コンプライアンス対応	1	サプライチェーンリスクの評価：取引先やクラウドサービス提供者のセキュリティリスクを評価できる
			2	サイバーセキュリティに関する法令、規制、業界固有ガイドライン等の知識：サイバーセキュリティセキュリティに関する法律や、規程、取引要件となる業界のサイバーセキュリティガイドラインを理解し、適用のための支援を実行できる

【参考】セキュリティ専門家スキル調査項目

◇セキュリティ専門家スキル調査項目（S-2、３）

支援領域	スキル No.	大分類（アセスメント基準）	No.	必要とされる専門家スキル
２.セキュリティリスクの識別	S2	a.情報資産の洗い出しと情報資産管理台帳の運用設計、潜在リスクの特定と評価	1	情報資産の管理 ：情報資産管理台帳を作成し、継続的に更新・運用するプロセスを設計・実施できる
			2	情報資産リスクの評価： 情報資産持つリスクを体系的に分類、評価し、優先順位付けができる
		b.リスクに基づくサイバーセキュリティ対策の策定、現存対策の評価及び改善点の指摘	1	リスク対応策の策定と文書化：リスク管理表に基づき、各リスクへの対応策を具体化し、文書化する支援を実行できる
			2	サイバーセキュリティ対策の評価： 既存のサイバーセキュリティ対策の効果について評価し、改善点を指摘できる
		c.社内外における、サイバーセキュリティ対策の推進	1	サイバーセキュリティ対策の社内外への発信（コミュニケーション） ：サイバーセキュリティ対策やポリシーの内容、実施計画や運用について企業内外に発信する支援を実行できる
			2	セキュリティ文化の醸成 ：企業全体のセキュリティ意識向上のための具体的な施策を提案・実施ができる
３.サイバーセキュリティ対策の実践と運用の強化	S3	a.アカウント管理、アクセス管理	1	アカウント管理・アクセス管理：適切なアカウント＆アクセス管理ポリシーを設計し、アカウントの分類や権限管理を効果的に実施できる
		b.データ管理、システムセキュリティ管理、コンテンツセキュリティ管理	1	システム更新：ソフトウェア、OSの更新管理に関する支援を実施できる
			2	データバックアップ：適切な方式や頻度でのデータバックアップ実施と管理の支援を実施できる
			3	暗号化：暗号化を実施すべき情報機器を特定し、データ保護対策実施のための支援を実施できる
		c.社内セキュリティ教育の策定と運用	1	社内セキュリティ教育の策定：既存の社内セキュリティ教育を評価し、効果的な教育の策定と運用のための支援を実施できる

【参考】セキュリティ専門家スキル調査項目

◇セキュリティ専門家スキル調査項目（S-４、５）

支援領域	スキル No.	大分類（アセスメント基準）	No.	必要とされる専門家スキル
４.サイバー攻撃の検知と監視検知後の運用策定	S4	a.セキュリティインシデント対処教育の策定と実施	1	セキュリティインシデント対処の教育：セキュリティインシデントの一般的な兆候を識別する方法について、効果的な社員教育を実施できる
		b.ウイルス対策ソフトの運用、システム・ネットワークの監視、外部監視サービスの導入	1	ウイルス対策ソフトの運用： 適切なウイルス対策ソフトの選定、導入、運用設計を行い、効果的に実行する支援を実行できる
			2	システム・ネットワークの監視： システムおよびネットワークの監視に関する知識を持ち、必要な運用体制を設計・実装できる
			3	外部監視サービスの導入： 中小企業向けの外部監視サービスについて熟知し、適切なサービスの選定と導入のための支援を実行できる
		ｃ.インシデント初動の運用設計と教育実施能力	1	初動対応設計能力：セキュリティ事象の検知時の初動について、適切な運用を設計できる
5.セキュリティインシデント発生時の対応	S5	a.セキュリティインシデント対応（セキュリティインシデント対応計画の策定、セキュリティインデント調査・対応、セキュリティインシデント報告・公表支援）	1	セキュリティインシデント対応計画の策定： 情報セキュリティインシデント対応計画の策定と管理・運用体制を構築する支援を実行できる
			2	セキュリティインシデント分析： 発生した事象に基づき、セキュリティインシデントの原因、被害とその影響範囲を正確に分析できる
			3	封じ込め戦略立案： 発生した事象に基づき、適切なセキュリティインシデント封じ込め対策を設計できる
			4	セキュリティインシデントの報告と公表： セキュリティインシデント発生時における関係者への報告・公表プロセスを適切に実施および管理する支援を実行できる

【参考】セキュリティ専門家スキル調査項目

◇セキュリティ専門家スキル調査項目（S-６）

支援領域	スキル No.	大分類（アセスメント基準）	No.	必要とされる専門家スキル
6.セキュリティインシデントからの復旧とコミュニケーション	S6	a.セキュリティインシデント復旧支援	1	インシデント復旧支援： セキュリティインシデント発生時のビジネス復旧に関する責任の所在を正しく理解するための支援を実行できる
			2	インシデント事後報告書作成 ：インシデントの詳細、時系列、影響範囲から、実施された対応・教訓までを正確かつ簡潔に文書化する支援を実行できる
			3	データ復旧： セキュリティインシデントからの復旧時に、正しいバックアップデータを選定し、効果的な復旧を行うための支援を行える
			4	復旧行動の優先順位付け： セキュリティインシデント復旧対応について、適切に優先順位付けを行える
			5	ステークホルダーとのコミュニケーション： インシデント対応中の関係者、顧客等利害関係者への適切な頻度と内容での情報共有を管理できる


IPA