CISO 等セキュリティ推進者の
経営・事業に関する役割調査

－別冊－
CISO 等セキュリティ推進者の
経営・事業に関する役割プラクティス

2018年6月28日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目 次

1. はじめに

1.1 目的

経営層によるセキュリティ対策の主体的取組の推進には、経営層の示す経営方針に基づくセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、企業内の総合調整や実務者層をまとめリードできる人材が必要であるとされ、CISO 等（ CISO に加え CISO をサポートするメンバー（橋渡し人材等）を含む）が必要とされている。

このような状況を考慮すると、CISO 等には技術的な役割だけではなく、自社の経営方針・事業戦略とセキュリティ対策の整合等、経営・事業的貢献の観点からセキュリティ対策を推進する「経営・事業的役割」が今後求められると考えられる。

さらに、昨今、デジタルトランスフォーメーションと呼ばれるように、企業においても、社内システムのみならず、事業部門の情報システムや、工場等で利用される制御システムにおいても、デジタル技術活用を進めることで新たな事業価値を生み出すべく取組が進展しつつある。そのため、より広範囲な業種・業態において積極的なデジタル技術の活用が事業推進上必要不可欠な要素となりつつある。一方で、過剰なセキュリティ対策は、利便性や業務効率化を下げる場合もあり、スピードを持って事業を促進するためには、CISO 等が事業を深く理解しつつ、適切なリスク評価を行うことで事業とセキュリティのバランスを取り、セキュリティの面から事業推進を支援する役割の重要性が増している。

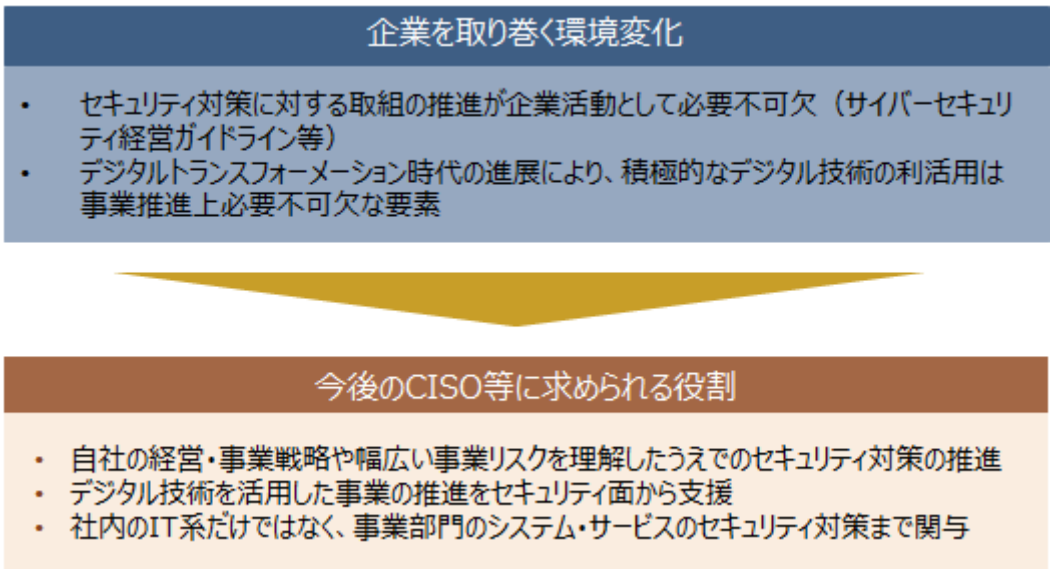

図 1-1　今後の CISO 等に求められる役割

本書は、「CISO 等セキュリティ推進者の経営・事業に関する役割調査－調査報告書－」の調査結果及び有識者へのヒアリング調査の結果を基に CISO 等に求められる経営・事業的役割について整理し、各役割の目的や役割を遂行する際のポイント等をまとめたものである。また二つの役割を例として取上げ、現実的な企業の状況の下で、当事者がどう経営・事業的な役割を果たすかを、ストーリー形式で説明したものを、付録として添付した。

企業によりデジタル化の進展度合いは異なり、例えば、IT サービス業や金融業等、従来から IT が事業の根幹であるような業種と、製造業や卸売業・小売業等、今後デジタル技術

の活用が本格化する業種とでは、CISO 等が担う経営・事業的役割も異なると想定される。本書は、現状、デジタル技術の活用が進むと想定される事業環境において、CISO 等が果たすべき役割を示したものであり、各企業の環境に応じ、必要に応じて読み替えて活用いただくことを想定している。

1.2 経営・事業的役割の全体像

調査結果を基に整理した、CISO 等の経営・事業的役割の全体像は図 1-2 の通りである。本書では、CISO 等の経営・事業的役割を企業としてのセキュリティ対策の「全体方針」を決めるレイヤーと、全体方針を基にした「具体的施策」を実施するレイヤーで整理した。なお、図 1-2 で示す役割は CISO 等の経営・事業的役割を網羅しているものではなく、企業規模や事業内容、事業環境の変化等により求められる経営・事業的役割は変化すると考えられる。

CISO 等の経営・事業的役割は、企業の経営・事業戦略と整合する形でセキュリティ対策が実施されるように、遂行することが望ましい。図 1-1 で示した通り、デジタル化の進展等企業を取り巻く環境の変化により、企業の経営・事業戦略を実行する上で、セキュリティは必要不可欠な要素となっている。今後の CISO 等には、自社の経営・事業戦略を理解した上で、事業推進・事業貢献の観点から、各経営・事業的役割を遂行することが求められる。さらに、CISO 等は自社の社内 IT システムだけではなく、事業部門が保有・提供している IT システム・IT サービスのセキュリティ対策にまで関与していくことが望ましい。

また、CISO は 3 つの防衛線（Three lines of defense）[1]のセカンドラインのトップであることに留意する必要もある。一般的にセカンドラインは、コントロール機能を担い、リスク管理の枠組み（リスクを発見、特定、追跡、報告、軽減、管理するために必要なツールや能力を含む）を策定し、事業部門に対するモニタリングを実施する。組織が許容できるリスクの範囲内で事業を遂行しているかについて、事業部門を監督する役割を担う。

[1] 業務執行部門が業務においてリスクの特定及び管理を行う第 1 の防衛線、業務執行部門のリスク管理の状況を業務執行部門から独立したリスク管理部門等がモニタリングする第 2 の防衛線、防衛線の有効性を合理的に保証する内部監査部門を第 3 の防衛線としたリスク管理の仕組みのこと。

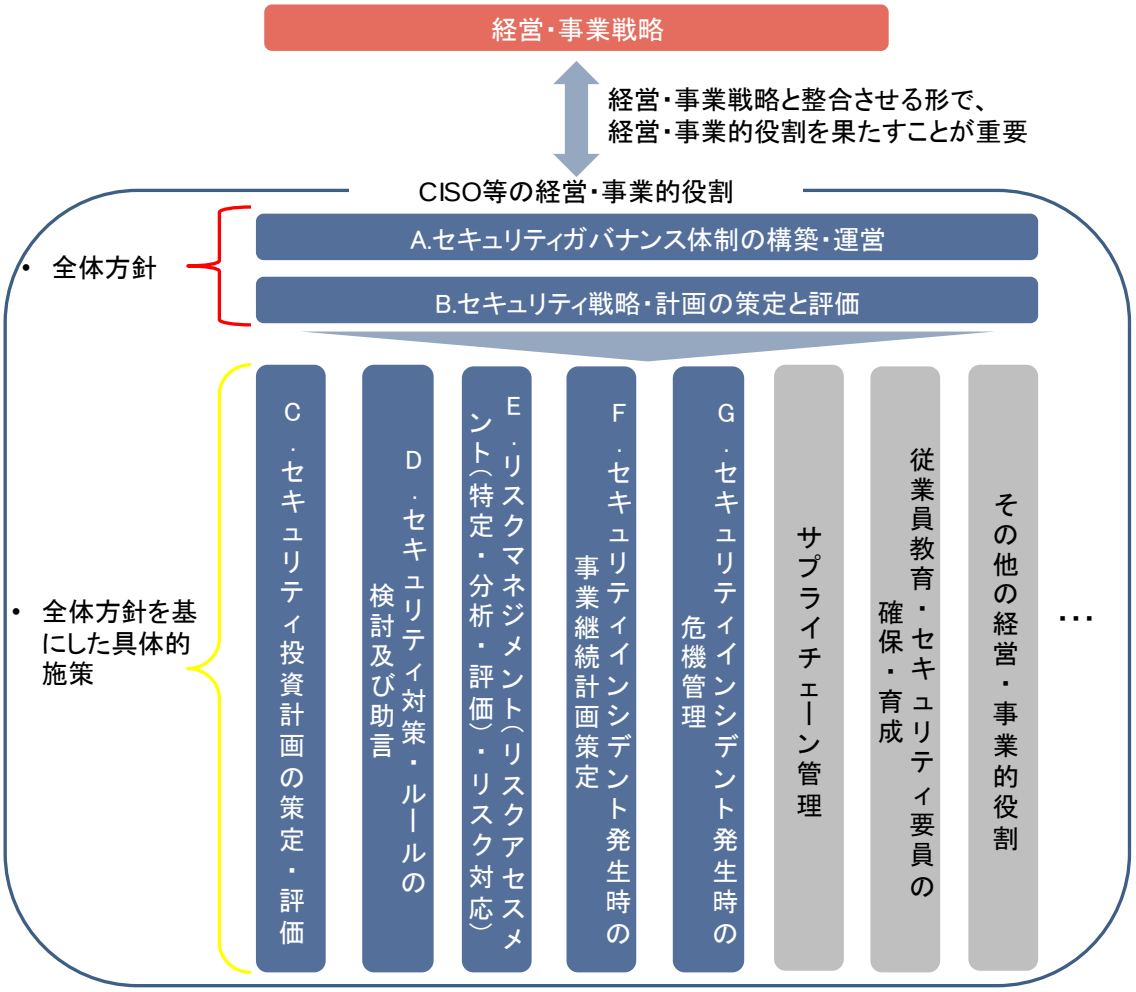

図 1-2　CISO 等の経営・事業的役割の全体像

本書では、CISO 等に求められる経営・事業的役割のうち、有識者ヒアリングの結果や事業推進や事業貢献の観点から、特に重要と考えられる役割として A~G の 7 つの役割を選定した。選定した役割の概要は表 1-1 の通りで、2 章～8 章では選定した役割について役割の目的や作業プロセス等の詳細を説明する。

表 1-1　本書で対象とする経営・事業的役割の概要

役割		概要
全体方針	A.セキュリティガバナンス体制の構築・運営	・　経営層がセキュリティリスクを認識し、組織として適切なリスク管理及びセキュリティ対策の実施、実施状況のモニタリング・評価できる体制を構築する ・　これを運用し、セキュリティに関する活動を自社の事業価値や事業推進につなげる
	B.セキュリティ戦略・計画の策定と評価	・　セキュリティ対策が自社事業に貢献するように、自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画（実施するセキュリティ対策、スケジュール、予算等のリソース配分等を含む）を策定する ・　セキュリティ戦略・計画の実施結果を自社事業への貢献度の観点から評価する
具体的施策	C.セキュリティ投資計画の策定・評価	・　自社の事業価値最大化の観点からセキュリティ投資計画を検討するために必要となる事業戦略等の社内外の情報を収集する ・　収集した情報を基にセキュリティ投資計画を策定し、経営層に説明し承認を得る ・　さらに、投資結果を自社の経営戦略・事業戦略との整合性の観点から評価する
	D.セキュリティ対策・ルールの検討及び助言	・　自社のIT・セキュリティニーズや法規制等の外部環境の変化に合わせて、事業部門やコーポレート部門に対してセキュリティ上の助言やルールの策定・改訂を実施する ・　セキュリティ上の助言やルールの策定・改訂は、セキュリティ対策が事業推進に影響を与えないように、事業負荷最小化の観点から実施する
	E.リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）	・　セキュリティリスクが事業に与える影響を低減するように、リスクアセスメント及びリスク対応を検討し、リスク対応を実施する
	F.セキュリティインシデント発生時の事業継続計画策定	・　自社の既存の BCP や IT-BCP と整合するように、セキュリティインシデント発生を想定した事業継続計画（IT-BCP）の基本方針や対象範囲、情報システムの復旧優先度等を検討し、策定する
	G.セキュリティインシデント発生時の危機管理	・　セキュリティインシデント発生時に企業価値を損なわないように、インシデントに関する情報収集・評価、対応計画の策定と指示・管理、社内外との調整等を行い、インシデントを収束させる

1.3 経営・事業的役割間の関係と本書の活用方法

本書で説明する 7 つの経営・事業的役割は、各役割が独立したものではなく、各役割の作業成果物（アウトプット）が他の役割を遂行する上でのインプットになる等相互に関連している。図 1-3 は役割間の関係を整理したものである（各役割の作業成果物については表 1-2 を参照）。図 1-3 において、各役割から伸びる矢印は、その役割の作業成果物（アウトプット）が、矢印の先の役割の作業を進めるためのインプットとなることを示している。例えば、役割 A から役割 B に伸びる矢印は、役割 A の作業成果物（アウトプット）が役割 B の作業を進めるためのインプットとなることを示している。

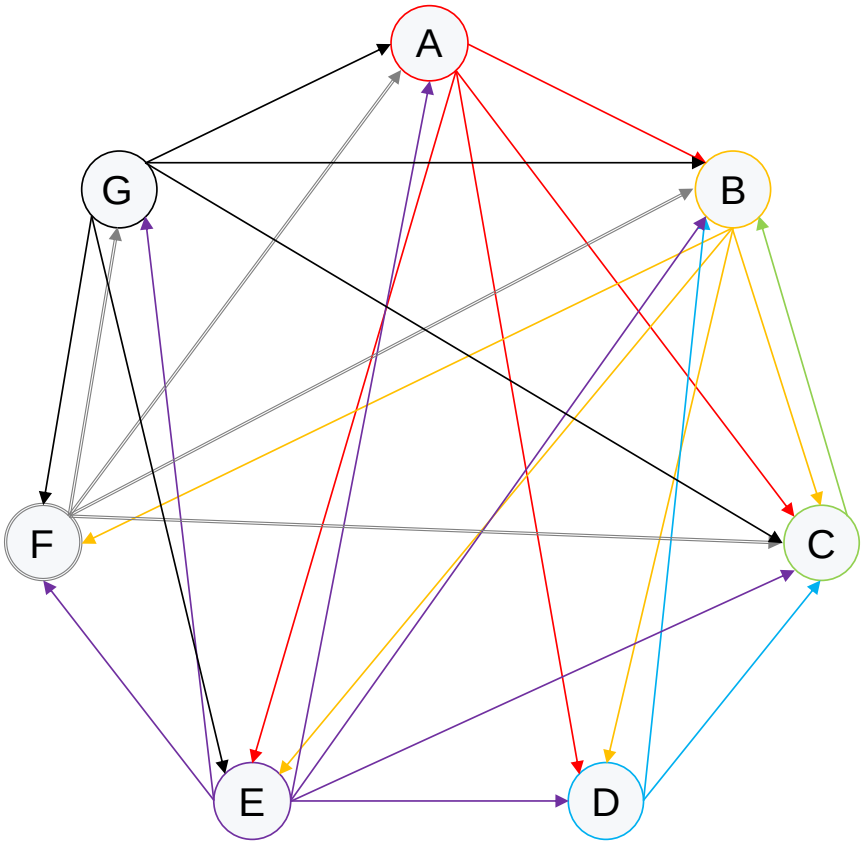

図 1-3　役割間のインプット・アウトプット関係

表 1-2　各役割の作業成果物

役割	作業成果物
A.セキュリティガバナンス体制の構築・運営	・　情報セキュリティ目的・目標 ・　情報セキュリティ目的・目標の達成度評価結果
B.セキュリティ戦略・計画の策定と評価	・　自社の事業戦略と整合させたセキュリティ戦略・計画 ・　セキュリティ戦略・計画の有効性検証結果
C.セキュリティ投資計画の策定・評価	・　セキュリティ投資計画 ・　自社の経営戦略・事業戦略との整合性の観点から評価したセキュリティ投資効果の評価結果
D.セキュリティ対策・ルールの検討及び助言	・　セキュリティ対策・ルール ・　事業部門やコーポレート部門に対するセキュリティ上の助言
E.リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）	・　リスクアセスメント結果 ・　リスク対応計画・結果
F.セキュリティインシデント発生時の事業継続計画策定	・　IT-BCP
G.セキュリティインシデント発生時の危機管理	・　インシデント対応結果報告書

図 1-3 に示す通り、7 つの役割は相互に関連しているため、本書を活用する上で、どの役割から取組を開始すればよいかの参考とするケースの例を表 1-3 に示す。

表 1-3　ケース別本書の活用方法

ケース	活用方法
役割 A～G の取組を既に実施している企業	・　全体方針（役割 A・B）・具体的施策（役割 C～G）の順に確認し、自社の取組で不足している点等を確認する。
役割 A～G の取組の一部を実施している企業	・　現在実施している役割について確認し、自社の取組で不足している点等を確認する。 ・　その後、全体方針・具体的施策の順で経営・事業的役割を確認し実施する。
役割 A～G の取組を全く実施していない企業	・　「E.リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）」から開始し、全体方針・具体的施策の順で実施する。 ・　社内に知見が蓄積されていないと考えられるため、必要に応じて同業他社等の情報を参考にする。
インシデント経験を受けて体制整備に着手する企業	・　「G.セキュリティインシデント発生時の危機管理」から実施し、セキュリティ体制の構築のために「A.セキュリティガバナンス体制の構築・運営」を実施する。 ・　その後役割 B～F を実施する。

2. セキュリティガバナンス体制の構築・運営（A）

2.1 目的・狙い

本役割は経営層がセキュリティリスクを認識し、組織として適切なリスク管理とセキュリティ対策が実施するための体制を構築・運用し、自社の事業価値や事業推進に貢献することを目的としている。

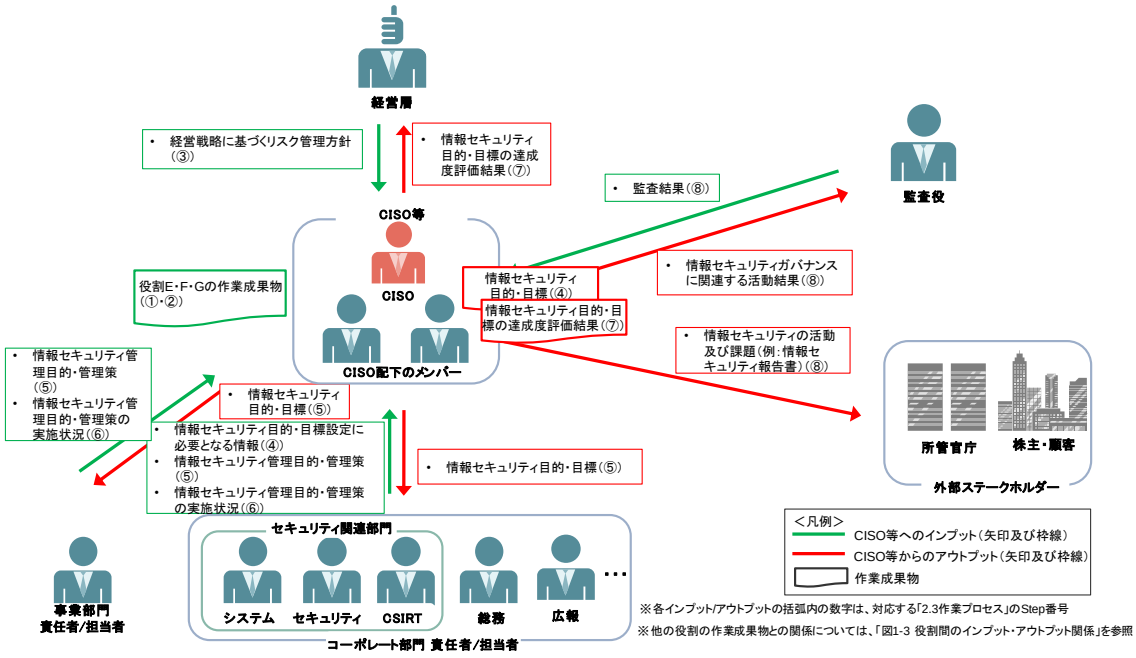

図 2-1 「セキュリティガバナンス体制の構築・運営」の全体像

2.2 役割の作業内容

本役割の作業内容は以下の通りである。

- 経営者による方針決定等の機能を有するセキュリティガバナンスのフレームワークの構築
- 経営層が示すリスク管理方針に基づいた情報セキュリティ目的・情報セキュリティ目標の設定
- 情報セキュリティ目的・情報セキュリティ目標の達成状況を評価し経営層に報告
- 外部監査や外部ステークホルダーへの報告実施

2.3 作業プロセス

本役割の作業プロセスは以下の通りである。

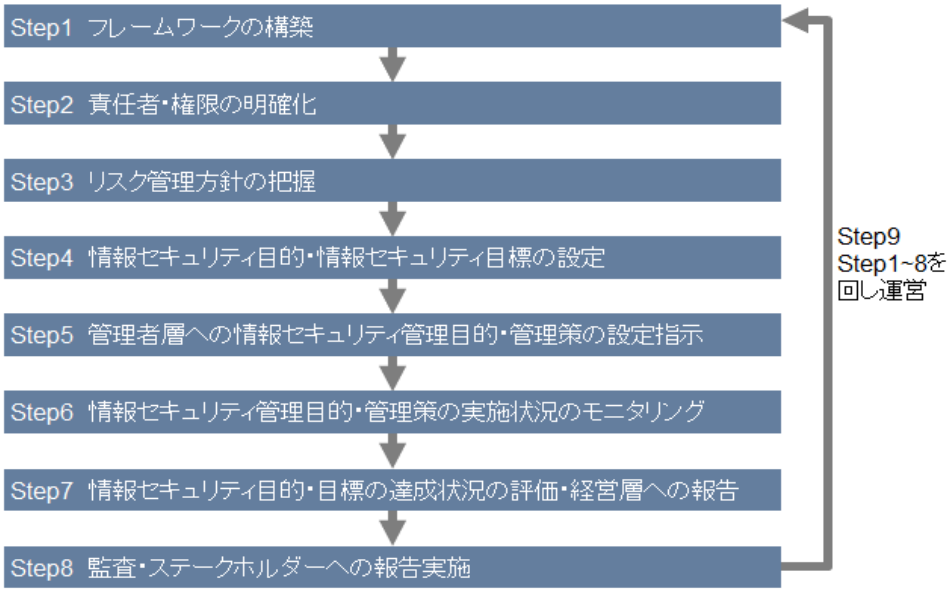

図 2-2 「セキュリティガバナンス体制の構築･運営」の作業プロセス

Step1 フレームワークの構築

以下の機能を有するフレームワークを構築する。

- 経営者による方針決定
- 組織内の状況をモニタリングする仕組み
- 利害関係者に対する開示
- 利害関係者による評価の仕組み

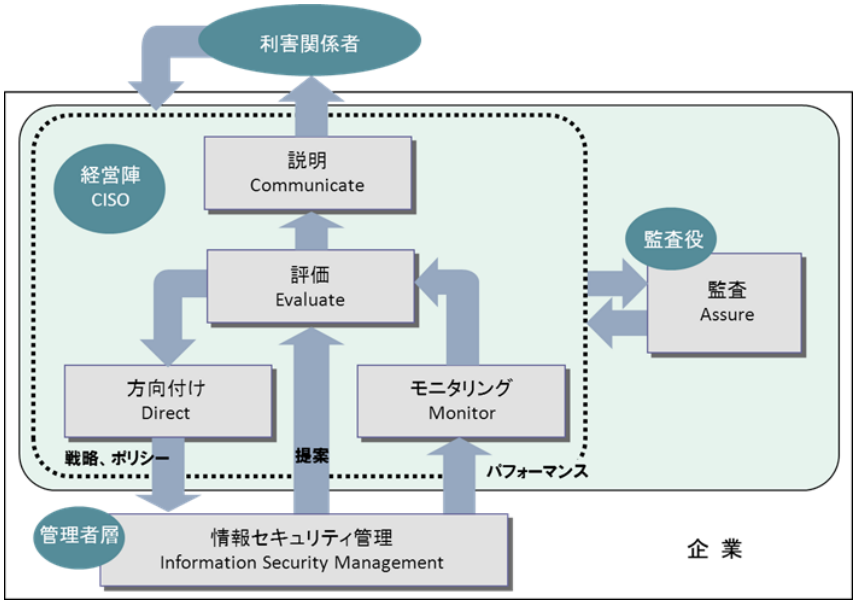

図 2-3 情報セキュリティガバナンスのフレームワーク

（出所）経済産業省「情報セキュリティガバナンス導入ガイダンス」を基に ISO/IEC 27014:2013 の内容を一部反映

Step2　責任者・権限の明確化

Step1 で構築したフレームワークを基に、責任者・権限を明確化する。

Step3　リスク管理方針の把握

経営層が示す、経営戦略や経営戦略に基づくリスク管理方針[2]を把握する。

Step4　情報セキュリティ目的・情報セキュリティ目標の設定

経営層が示したリスク管理方針を基に、情報セキュリティ目的[3]・情報セキュリティ目標[4]を設定する。

経営層が示すリスク管理方針を基にした、情報セキュリティ目的・情報セキュリティ目標の例は下表に示す通りである。

表 2-1　情報セキュリティ目的・情報セキュリティ目標の例

	内容
リスク管理方針	・　取引先からの信頼の維持・向上 ・　サプライチェーン間のネットワーク障害に対応する企業間連携体制の整備
情報セキュリティ目的	・　共有する技術情報の保護 ・　製造ラインの事業継続性の確保 ・　機密データの共用やリモートアクセスといった利便性はできる限り維持しつつ安全性を保つ ・　製造請負事業の積極展開に資する信頼性強化
情報セキュリティ目標	・　他社との共有資産である技術情報を含む重要情報が明確に区分され、会社の定める規程に則り適切に管理されること ・　情報管理規程が遵守されていること ・　情報システムの停止や処理能力の著しい低下が発生した場合にも、最低限の生産体制が維持できるよう、適切かつ合理的な方策が適用されていること ・　製造ラインの IT 汎用技術導入に応じて適切な情報セキュリティ管理策を適用すること

（出所）経済産業省「情報セキュリティガバナンス導入ガイダンス」を基に作成

Step5　管理者層への情報セキュリティ管理目的・管理策の設定指示

Step4 で設定した情報セキュリティ目的・目標を事業部門・コーポレート部門の管理者層に伝える。さらに、管理者層に対し情報セキュリティ目的・目標を実現するための情報セキュリティ管理目的・管理策の設定を指示する。

情報セキュリティ管理目的・管理策の設定にあたり、事業部門等セキュリティ人材等が不足していると考えられる組織に対しては、CISO 等が必要に応じて支援することが望ましい。

---

[2] 経営戦略に基づき設定されたリスク許容レベル。

[3] リスク管理方針の実現に向けて、情報セキュリティ分野で達成すべきゴール。

[4] 情報セキュリティ目的の達成度を評価できるように定める、情報セキュリティ目的の指標。

Step6　情報セキュリティ管理目的・管理策の実施状況のモニタリング

事業部門・コーポレート部門が設定した情報セキュリティ管理目的・管理策の実施状況をモニタリングする。

Step7　情報セキュリティ目的・目標の達成状況の評価・経営層への報告

Step6 のモニタリング結果を基に、情報セキュリティ目的・目標の達成状況を評価する。さらに、情報セキュリティ目的・目標の達成状況の評価結果を経営層に報告する。

Step8　監査・ステークホルダーへの報告実施

セキュリティガバナンスに関わる活動に関して監査を依頼し、監査結果を基に見直しを実施する。

また、外部ステークホルダーに対して、自社のセキュリティに対する取組について報告を実施する。

Step9　情報セキュリティガバナンス体制の運営

Step1～8 の取組を回し、情報セキュリティガバナンス体制を運営する。

2.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 2-2 「セキュリティガバナンス体制の構築・運営」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	・ 経営戦略に基づくリスク管理方針	・ 情報セキュリティ目的・目標の達成度評価結果
事業部門	・ 情報セキュリティ管理目的・管理策 ・ 情報セキュリティ管理目的・管理策の実施状況	・ 情報セキュリティ目的・目標
コーポレート部門	・ 情報セキュリティ目的・目標設定に必要となる情報（セキュリティ対策・業務委託・法規制等の情報） ・ 情報セキュリティ管理目的・管理策 ・ 情報セキュリティ管理目的・管理策の実施状況	・ 情報セキュリティ目的・目標
監査役	・ 監査結果	・ 情報セキュリティガバナンスに関連する活動結果
外部ステークホルダー	（特になし）	・ 情報セキュリティの活動及び課題（例：情報セキュリティ報告書）
ビジネスパートナー 外部委託先		
他の情報共有体制		
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ リスクアセスメント結果（E） ・ リスク対応計画・結果（E） ・ IT-BCP（F） ・ インシデント対応結果報告書（G）	（特になし）

2.5 作業の目標成果

本役割の成果は以下の通りである。

- 情報セキュリティ目的・目標
- 情報セキュリティ目的・目標の達成度評価結果

2.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、社内外の関係者との共同・連携が必要となる。

共同・連携する内容としては以下のようなものがある。

- 情報セキュリティ目的・情報セキュリティ目標達成のための、事業部門・コーポレート部門に対する連携・支援
- 外部ステークホルダーに対する自社のセキュリティ対策に関する情報開示

3. セキュリティ戦略・計画の策定と評価（B）

3.1 目的・狙い

本役割は、自社の経営戦略・事業戦略と整合したセキュリティ戦略・計画（実施するセキュリティ対策や実施スケジュール、予算等のリソース配分等）を策定し、自社の事業価値や事業推進につなげることを目的としている。

本役割で策定するセキュリティ戦略・計画は企業のセキュリティ対策に関する全体方針であり、このセキュリティ戦略・計画を基に、4 章以降の役割の具体的な施策が実施される。

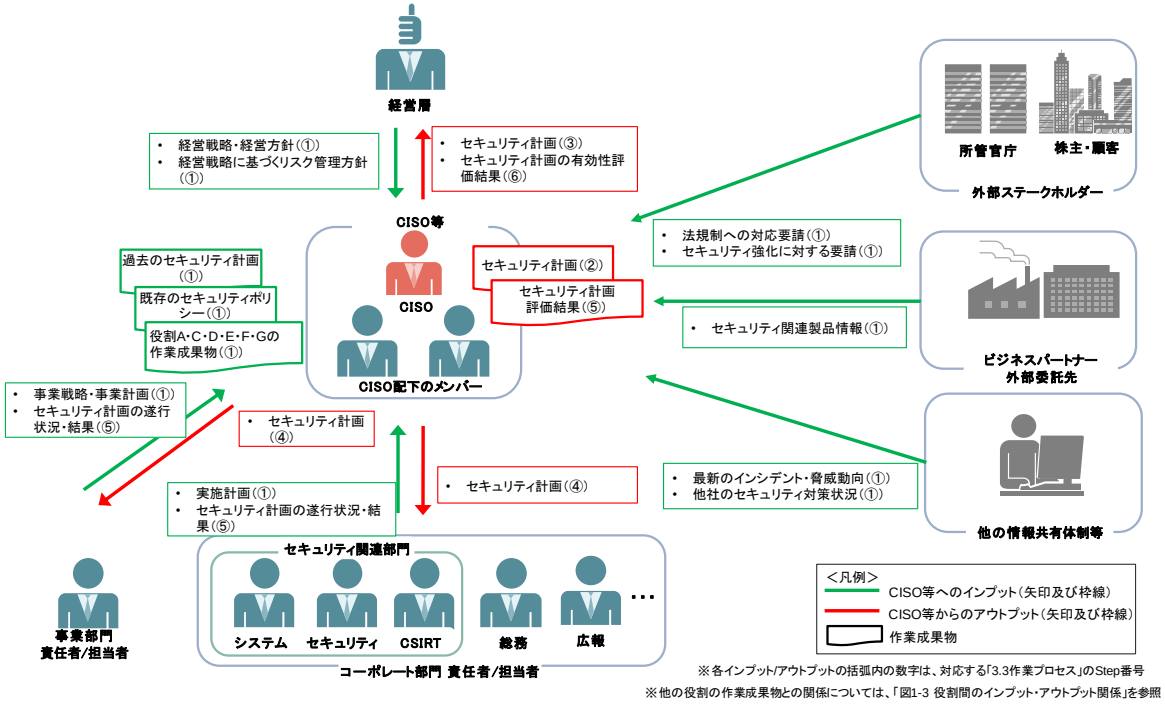

図 3-1　「セキュリティ戦略・計画の策定と評価」の全体像

3.2 役割の作業内容

本役割の作業内容は以下の通りである。

- 自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画の策定
- セキュリティ戦略・計画の実施結果の評価

3.3 作業プロセス

本役割の作業プロセスは以下の通りである。

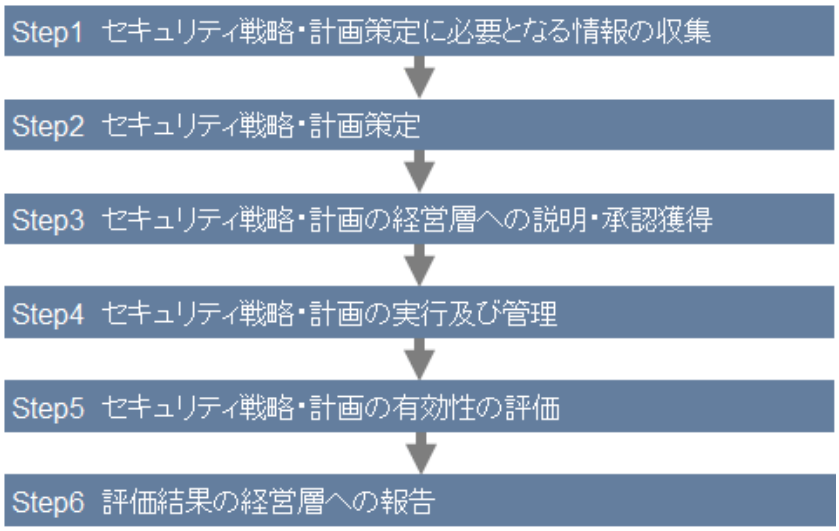

図 3-2 「セキュリティ戦略・計画の策定と評価」の作業プロセス

Step1 セキュリティ戦略・計画策定に必要となる情報の収集

セキュリティ戦略・計画の策定に必要となる情報として、以下の情報等を収集する。

- 経営戦略・経営方針
- 事業戦略・事業計画
- 自社に影響を与える法規制
- 最新のインシデント・脅威動向
- 情報セキュリティ目的・目標（A）
- セキュリティ投資計画（C）
- セキュリティ対策・ルール（D）
- リスクアセスメント結果（E）
- IT-BCP（F）
- インシデント対応結果報告書（G）

Step2 セキュリティ戦略・計画策定

Step1 で収集した情報を基に、セキュリティ戦略・計画を策定する。セキュリティ戦略・計画には、実施するセキュリティ対策や実施スケジュール、予算等のリソース配分等が含まれる。

Step3 セキュリティ戦略・計画の経営層への説明・承認獲得

Step2 で策定したセキュリティ戦略・計画を経営層に対して説明し、承認を得る。経営層から承認が得られなかった場合は、Step2 に戻り必要な修正を実施する。

Step4　セキュリティ戦略・計画の実行及び管理

Step3 で承認されたセキュリティ戦略・計画を実行する。事業部門・コーポレート部門が実行するセキュリティ戦略・計画に関しては、CISO 等が実行状況をモニタリングし管理するとともに、必要に応じて支援する。

Step5　セキュリティ戦略・計画の有効性の評価

事業部門・コーポレート部門のセキュリティ戦略・計画の実行状況・結果を把握し、セキュリティ戦略･計画の有効性を評価する。セキュリティ戦略･計画の有効性を評価する際は、自社の経営戦略・事業戦略との整合性や自社の事業価値への貢献等の観点から実施することが望ましい。

評価結果は次年度以降のセキュリティ戦略・計画を策定する際に活用する。

Step6　評価結果の経営層への報告

Step5 の評価結果を経営層へ報告する。

3.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 3-1 「セキュリティ戦略・計画の策定と評価」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	・ 経営戦略・経営方針 ・ 経営戦略に基づくリスク管理方針	・ セキュリティ戦略・計画 ・ セキュリティ戦略・計画の有効性評価結果
事業部門	・ 事業戦略・事業計画 ・ セキュリティ戦略・計画の遂行状況・結果	・ セキュリティ戦略・計画
コーポレート部門	・ 実施計画 ・ セキュリティ戦略・計画の遂行状況・結果	・ セキュリティ戦略・計画
外部ステークホルダー	・ 法規制への対応要請 ・ セキュリティ強化に対する要請	（特になし）
ビジネスパートナー 外部委託先	・ ベンダからのセキュリティ関連製品情報	（特になし）
他の情報共有体制	・ 最新のインシデント・脅威動向 ・ 他社のセキュリティ対策状況	（特になし）
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ 過去のセキュリティ戦略・計画や既存のセキュリティポリシー等 ・ 情報セキュリティ目的・目標（A） ・ 情報セキュリティ目的・目標の達成度評価結果（A） ・ セキュリティ投資計画（C） ・ セキュリティ投資効果の評価結果（C） ・ セキュリティ対策・ルール（D） ・ 事業部門やコーポレート部門に対するセキュリティ上の助言（D） ・ リスクアセスメント結果（E） ・ リスク対応計画・結果（E） ・ IT-BCP（F） ・ インシデント対応結果報告書（G）	（特になし）

3.5 作業の目標成果

本役割の成果は以下の通りである。

- 自社の事業戦略と整合させたセキュリティ戦略・計画
- セキュリティ戦略・計画の有効性検証結果

3.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、主に社内外の関係者との共同・連携が必要となる。
共同・連携する内容としては以下のようなものがある。

- 社内外の関係者からのセキュリティ戦略・計画策定に必要となる情報の収集
- 事業部門・コーポレート部門と連携したセキュリティ戦略・計画の実行

4. セキュリティ投資計画の策定・評価（C）

4.1 目的・狙い

本役割は、「セキュリティ戦略・計画の策定・評価」の役割で策定されたセキュリティ戦略・計画を基に、必要となるセキュリティ対策を検討し、対策実施に必要なセキュリティ投資計画を策定するものである。策定するセキュリティ投資計画には、新規の IT サービス・IT システムの導入だけではなく、既存の IT サービス・IT システムの継続利用等の判断も含まれる。

本役割の遂行にあたっては、セキュリティ投資が自社の企業価値の最大化につながるようにセキュリティ投資計画を策定し、自社の経営戦略・事業戦略との整合性の観点から投資の有効性を評価することが望ましい。

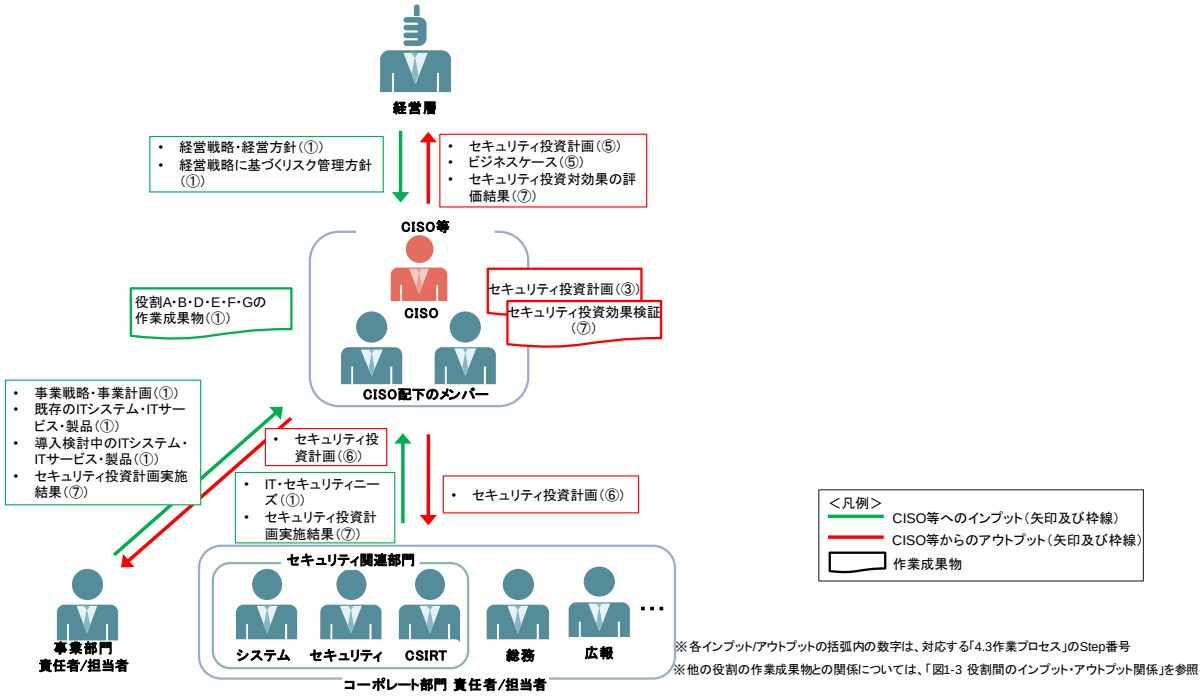

図 4-1 「セキュリティ投資計画の策定・評価」の全体像

4.2 役割の作業内容

本役割の作業内容は以下の通りである。

- 自社の企業価値最大化につながるセキュリティ投資計画の策定
- セキュリティ投資計画の有効性を示すビジネスケース[5]の策定
- セキュリティ投資計画・ビジネスケースの経営層への説明・承認獲得
- セキュリティ投資計画の実行及び投資効果の検証

[5] 経営層等が投資判断をする上で、投資計画の有効性を示すための資料。ビジネスケースには、投資実施の目的や必要性（IT・セキュリティニーズ）や必要なリソース、期間、投資効果（費用便益分析）等が含まれる。

4.3 作業プロセス

本役割の作業プロセスは以下の通りである。

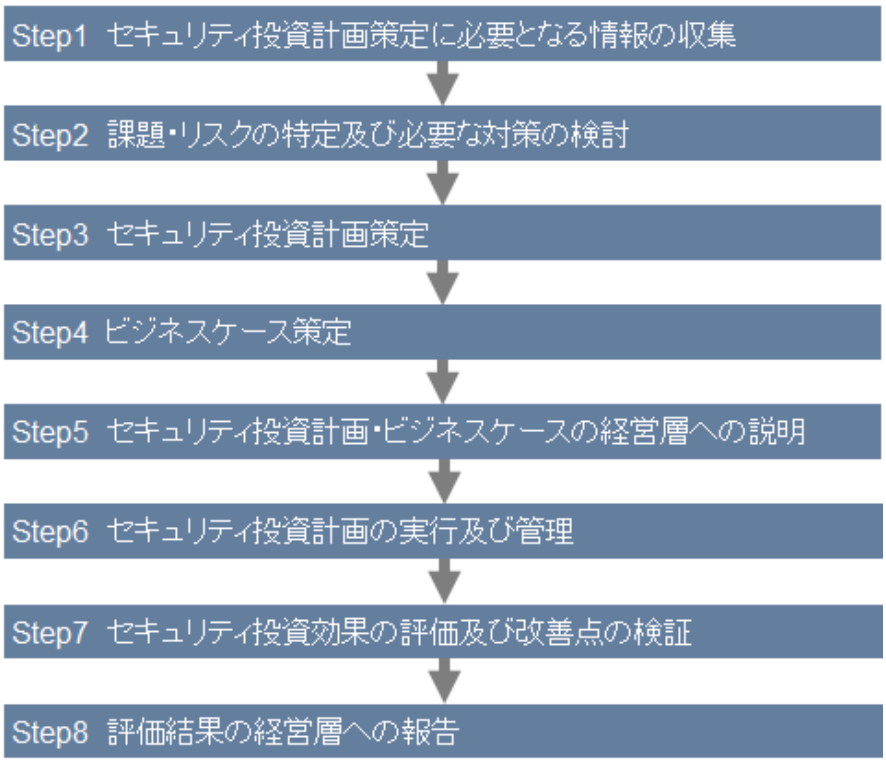

図 4-2 「セキュリティ投資計画の策定・評価」の作業プロセス

Step1 セキュリティ投資計画策定に必要となる情報の収集

事業部門やコーポレート部門、他の役割の成果物等からセキュリティ投資計画を策定する上で必要となる情報を収集する。

セキュリティ投資計画策定に必要となる情報としては以下のものがある。

- 経営戦略・経営方針
- 事業戦略・事業計画
- 既存または導入検討中の IT システム・IT サービス・製品
- 情報セキュリティ目的・目標（A）
- セキュリティ戦略・計画（B）
- セキュリティ対策・ルール（D）
- リスクアセスメント結果（E）
- IT-BCP（F）
- インシデント対応結果報告書（G） 等

Step2 課題・リスクの特定及び必要な対策の検討

Step1 で収集した情報を元に、自社のセキュリティ上の課題やリスクを特定し、必要な対策を検討する。

Step3　セキュリティ投資計画策定

Step2 で検討した対策を導入するために必要となるセキュリティ投資計画を策定する。

セキュリティ投資計画の策定にあたっては、自社の事業価値最大化につながるよう、経営戦略・事業戦略と整合させるように策定することが望ましい。

Step4　ビジネスケース策定

Step3 で策定したセキュリティ投資計画の有効性を経営層に示すために、ビジネスケースを策定する。

セキュリティ投資計画の有効性を示すビジネスケースには、以下の情報等が含まれる。

- セキュリティ投資の目的・必要性
- 必要なリソース
- 実施スケジュール
- 期待される投資効果　等

Step5　セキュリティ投資計画・ビジネスケースの経営層への説明

Step3・Step4 で策定したセキュリティ投資計画・ビジネスケースを経営層に説明し、承認を得る。経営層からの承認が得られなかった場合、Step3 に戻り必要な修正を行う。

Step6　セキュリティ投資計画の実行及び管理

経営層から承認を得たセキュリティ投資計画を実行する。事業部門やコーポレート部門が実行するセキュリティ投資計画については、その進捗状況等を CISO 等が管理する。

Step7　セキュリティ投資効果の評価及び改善点の検証

セキュリティ投資計画の実行結果を基に、セキュリティ投資の投資効果・改善点を検証する。

投資効果の検証の際には、自社の経営戦略・事業戦略との整合性や、自社事業推進にどの程度貢献したか等の観点から実施することが望ましい。

セキュリティ投資効果の検証結果に関しては、次年度以降のセキュリティ戦略・計画の策定やセキュリティ投資計画の策定に活用する。

Step8　評価結果の経営層への報告

Step7 で実施したセキュリティ投資効果の検証結果を経営層に報告する。

4.4 作業に必要な情報

作業に必要な情報には下表のものがある。

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	・ 経営戦略・経営方針 ・ 経営戦略に基づくリスク管理方針	・ セキュリティ投資計画 ・ セキュリティ投資計画の有効性を示すビジネスケース ・ セキュリティ投資対効果の評価結果
事業部門	・ 事業戦略・事業計画 ・ 既存の IT システム・IT サービス・製品 ・ 導入検討中の IT システム・IT サービス・製品 ・ セキュリティ投資計画実施結果	・ セキュリティ投資計画
コーポレート部門	・ IT・セキュリティニーズ ・ セキュリティ投資計画実施結果	・ セキュリティ投資計画
外部ステークホルダー		
ビジネスパートナー 外部委託先		
他の情報共有体制		
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ 情報セキュリティ目的・目標（A） ・ 自社の事業戦略と整合させたセキュリティ戦略・計画（B） ・ セキュリティ戦略・計画の有効性検証結果（B） ・ セキュリティ対策・ルール（D） ・ 事業部門やコーポレート部門に対するセキュリティ上の助言（D） ・ リスクアセスメント結果（E） ・ リスク対応計画・結果（E） ・ IT-BCP（F） ・ インシデント対応結果報告書（G）	（特になし）

4.5 作業の目標成果

本役割の作業成果は以下の通りである。

- セキュリティ投資計画（導入する製品・サービスや投資金額、実施時期、投資効果等を含む）
- 自社の経営戦略・事業戦略との整合性の観点から評価したセキュリティ投資効果の評価結果

4.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、主に社内の関係者（経営層・事業部門・コーポレート部門）との共同・連携が必要となる。

共同・連携する内容としては以下のようなものがある。

- 自社の経営戦略・事業戦略等の把握・セキュリティ上の課題の検討に必要となる情報の提供・意見交換
- 事業部門やコーポレート部門に対するセキュリティ投資計画の実行支援及び進捗状況の管理

5. セキュリティ対策・ルールの検討及び助言（D）

5.1 目的・狙い

事業部門やコーポレート部門の社内部門の新規の事業展開や新たな IT システム・IT サービスの利用等の内部環境の変化や、法規制や新規技術の登場等の外部環境の変化に合わせて、CISO 等にはセキュリティ上の助言や新たなルールの策定、既存ルールの改訂等の対応が求められる。

本役割では社内外の環境変化に合わせて、CISO 等がセキュリティ上の助言やルールの策定・改定を行うものである。本役割を遂行する際には、セキュリティ対策が事業推進に影響を与えないよう、事業負荷を最小にする観点から検討することが望ましい。また、CISO 等の役割が事業の推進を成功に導くようにセキュリティ対策・ルールを整備することであることに留意する必要がある。

本役割の全体像は以下の通りである。

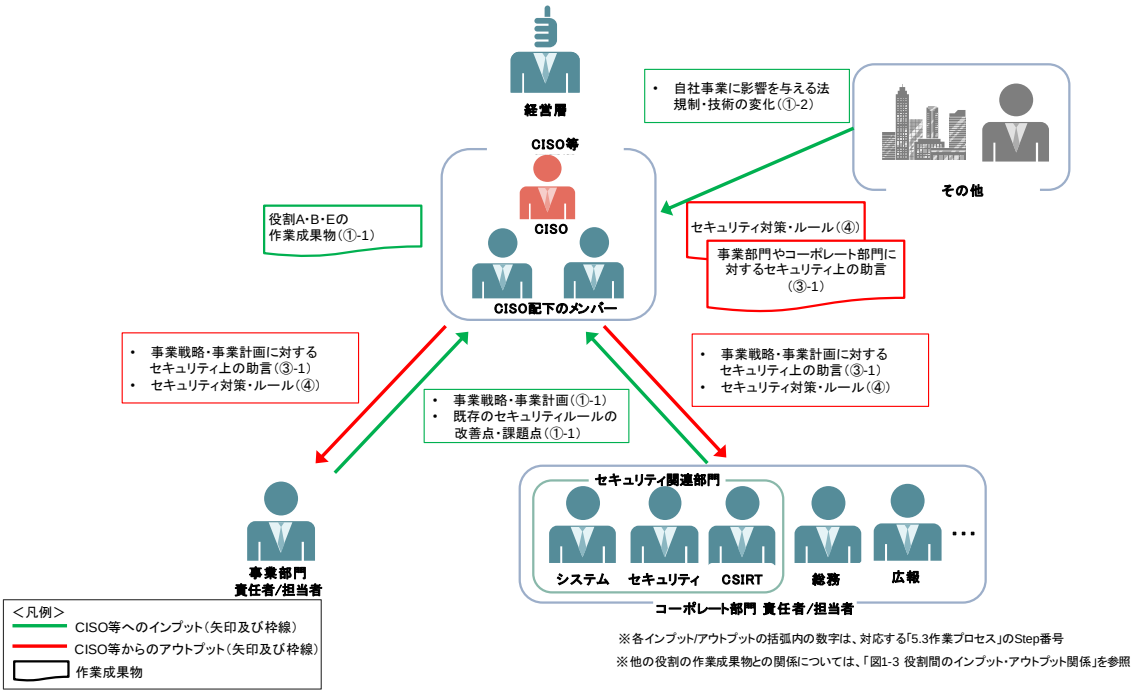

図 5-1　「セキュリティ対策・ルールの検討及び助言」の全体像

5.2 役割の作業内容

本役割の作業内容は以下の通りである。

- 事業部門・コーポレート部門等からの内部情報の収集及び法規制や技術動向等の外部情報の収集
- 収集した情報を基にした、自社の IT 利活用ニーズの把握及びセキュリティ上の課題の検討
- 検討した課題を基にした、事業部門・コーポレート部門に対するセキュリティ上の助言
- 検討した課題を基にした、既存のルールの改訂または新規ルールの策定及び見直し

本役割は、社内外の環境の変化に合わせて実施するため、定期的・不定期に遂行することが望ましい。実施するタイミングとしては以下のものが考えられる。

- 年度計画検討時
- 新規事業検討時
- 新規の IT サービス導入検討時
- 自社に影響を与える法規制や新規技術の登場時

5.3 作業プロセス

本役割の作業プロセスは以下の通りである。

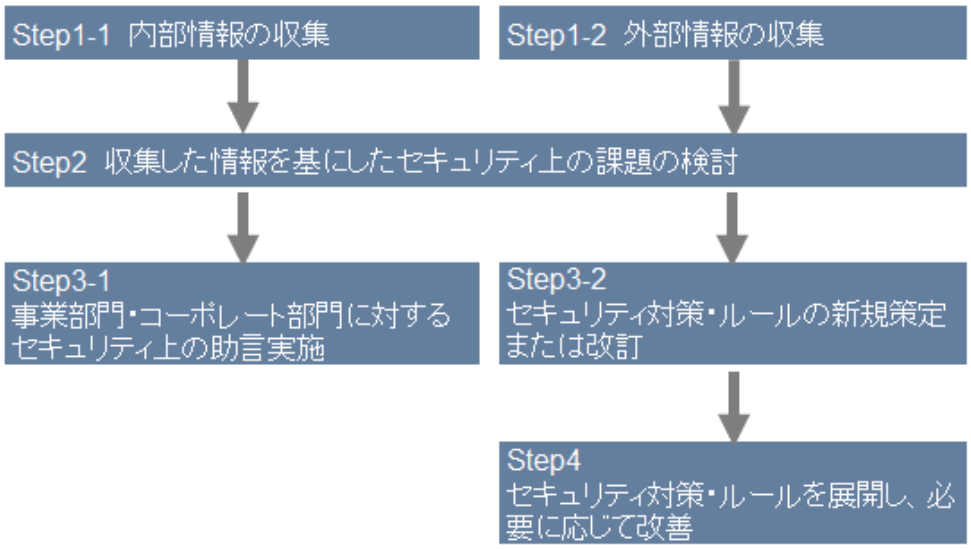

図 5-2 「セキュリティ対策・ルールの検討及び助言」の作業プロセス

Step1-1 内部情報の収集

事業部門及びコーポレート部門に対して、事業計画（IT システム・IT サービスを利用した新規事業や新規の IT システム・IT サービスの検討・導入等）や既存のセキュリティルール等に関する改善要望等の情報を収集する。

内部情報の収集にあたっては、他の役割の成果物である以下のものもインプットとなる。

- 情報セキュリティ目的・目標（A）
- 自社の事業戦略と整合させたセキュリティ戦略・計画（B）
- リスクアセスメント結果（E）
- リスク対応計画・結果（E）

Step1-2 外部情報の収集

自社事業に影響を与える法規制の変化や新規技術の動向等について、定期的に情報を収集する。

Step2　収集した情報を基にしたセキュリティ上の課題の検討

Step1-1 及び Step1-2 で収集した情報を基に自社の IT 利活用ニーズ等を把握し、セキュリティ上の課題がないか検討する。

Step3-1　事業部門・コーポレート部門に対するセキュリティ上の助言の実施

Step2 で検討した課題を基に、事業部門・コーポレート部門に対して、事業推進・業務運営に必要となるセキュリティ対策の実施等、セキュリティ上の助言を行う。

助言はセキュリティ対策が事業推進・業務運営の妨げにならないよう、事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

Step3-2　セキュリティ対策・ルールの新規策定または改訂

Step2 で検討した課題を基に、セキュリティに関するルールの新規策定または既存のルールの改訂を行う。

ルールの策定・改訂の際は、セキュリティに関するルールが事業推進・業務運営の妨げにならないよう、事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

Step4　セキュリティ対策・ルールを展開し、必要に応じて改善

策定・改訂したセキュリティに関するルールを社内に展開する。また、必要に応じて改善する。

5.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 5-1 「セキュリティ対策・ルールの検討及び助言」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層		
事業部門	・ 事業戦略・事業計画 ・ 既存のセキュリティルールの改善点・課題点	・ 事業戦略・事業計画に対するセキュリティ上の助言 ・ 新規または改訂された運用ルール
コーポレート部門	・ 事業戦略・事業計画 ・ 既存のセキュリティルールの改善点・課題点	・ 事業戦略・事業計画に対するセキュリティ上の助言 ・ 新規または改訂された運用ルール
外部ステークホルダー		
ビジネスパートナー 外部委託先		
他の情報共有体制		
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ 自社事業に影響を与える法規制・技術の変化 ・ 情報セキュリティ目的・目標（A） ・ 自社の事業戦略と整合させたセキュリティ戦略・計画（B） ・ リスクアセスメント結果（E） ・ リスク対応計画・結果（E）	（特になし）

5.5 作業の目標成果

本役割の成果は以下の通りである。

- 社内外の環境変化に対応した事業部門及びコーポレート部門に対するセキュリティ上の助言
- 社内外の環境変化に対応したセキュリティ対策・ルール

上記成果に関しては、セキュリティ対策が事業推進や業務運営に影響を与えないように、事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

5.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、主に社内の関係者（事業部門及びコーポレート部門）との共同・連携が必要となる。

共同・連携する内容としては以下のようなものがある。

- 自社の IT 利活用ニーズの把握・セキュリティ上の課題の検討に必要となる情報提供・意見交換
- 事業部門のセキュリティ対策の実施等に関して、コーポレート部門（主にセキュリティ関連部門）と連携した支援

6. リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応） (E)

6.1 目的・狙い

セキュリティ対策はセキュリティに関わるリスクに対応することである。しかし、対策にかけられる組織のリソースには限りがあることから、リスクを明確にし、対応の優先順位をつけ、最適な対策を選択する必要がある。また、組織が抱えるリスクは組織の状況により異なり、保有する情報資産や脅威の変化に伴い変化していくことから、セキュリティリスクに対しては、いったん評価・対応して終わりではなく、適切に管理していかなければならない。さらに、リスクの評価基準は企業としての判断であることから、経営・事業的な観点でリスクを評価し対応を検討していくことが必要である。

本役割は、自社のセキュリティ関連のリスクへの対応方針を定め、リスクが事業に与える影響を低減することを目的としている。

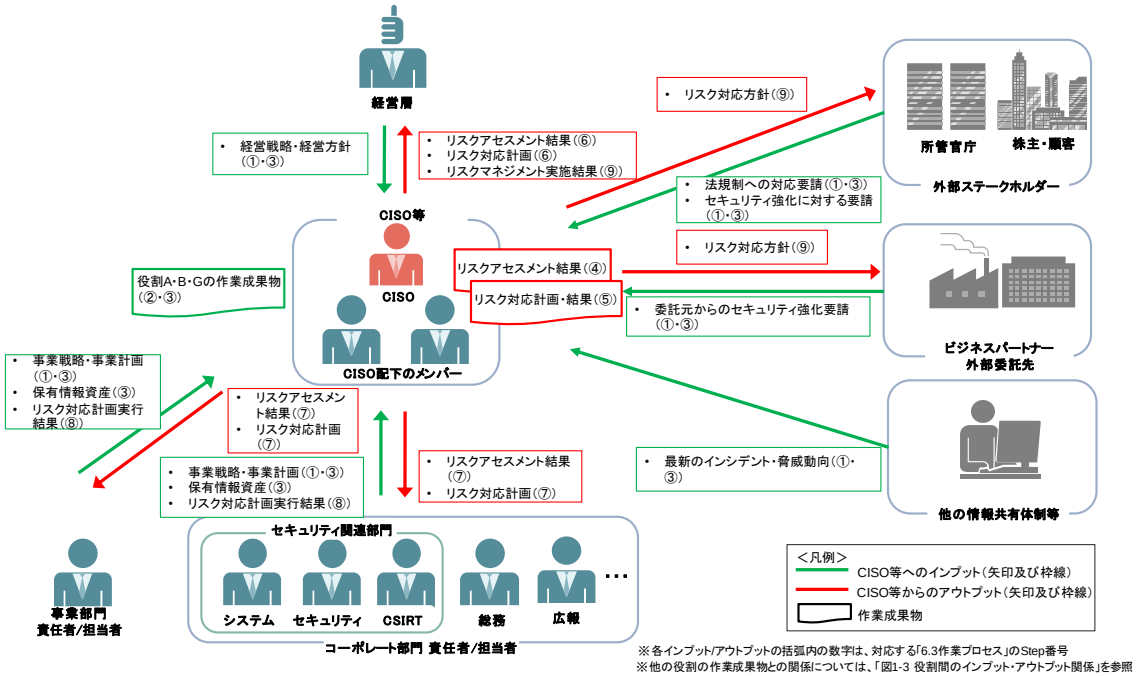

図 6-1 「リスクマネジメント」の全体像

6.2 役割の作業内容

本役割の作業内容は以下の通りである。

- セキュリティに関わるリスクアセスメント（特定・分析・評価）を行う。
- リスクアセスメント結果に基づき、リスク対応計画の策定を行う。
- リスク対応計画に基づいた、実行及び管理を行う。

6.3 作業プロセス

本役割の作業プロセスは以下の通りである。

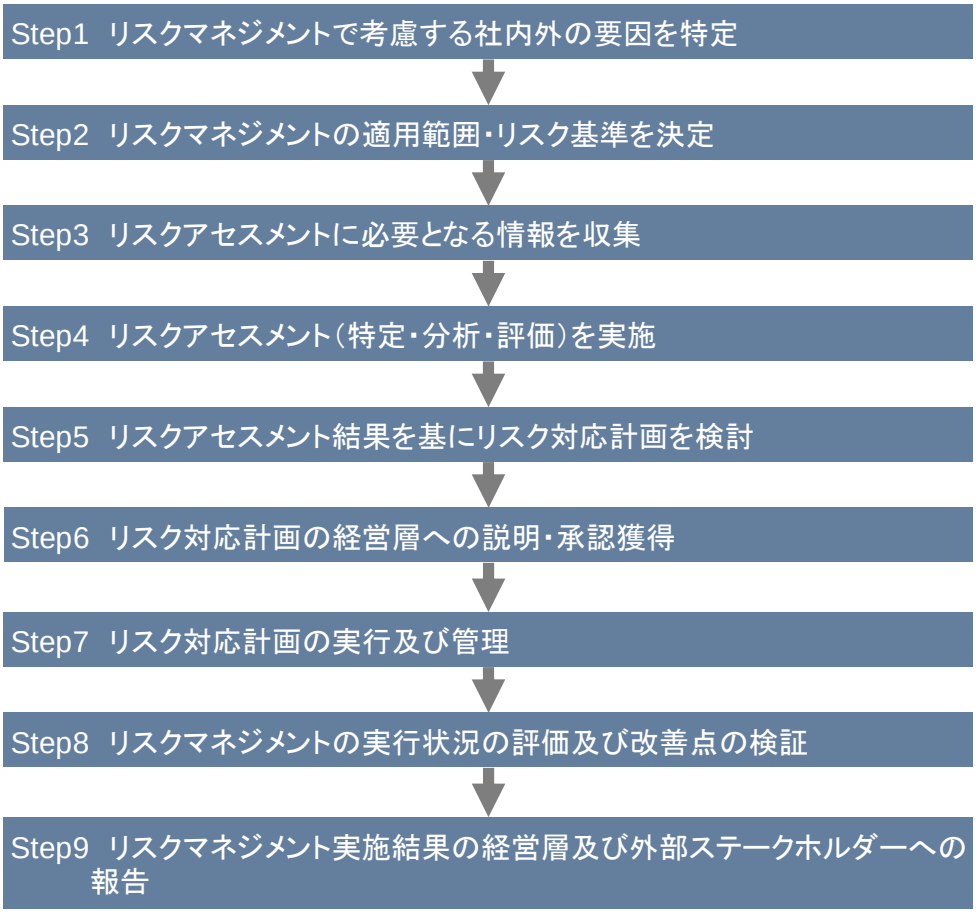

図 6-2 「リスクマネジメント」の作業プロセス

Step1 リスクマネジメントで考慮する社内外の要因を特定

組織の目的を明確にし、リスクマネジメントにおいて考慮するのが望ましい社内外の要因を特定する。外部環境とは、政治や経済、法規制、金融，技術等の社会動向全般、競争環境等市場の動向、ステークホルダーの状況等であり、内部環境とは、組織体制、方針･戦略、組織文化、情報システム、ステークホルダーの状況等である。

Step2 リスクマネジメントの適用範囲・リスク基準を決定

リスクマネジメントを適用する範囲と、リスクを評価するために使用する基準を定める。評価基準は、組織の目的やリソース等の状況、及び法律や規制の要求事項等によって検討される。

評価基準は、例えば事象の起こりやすさ、影響の種類や特徴、リスクレベル、複数のリスクの考慮等である。

Step3　リスクアセスメントに必要となる情報を収集

リスクアセスメント（特定・分析・評価）を行うために必要な情報を収集する。

Step4　リスクアセスメント（特定・分析・評価）を実施

リスク特定では、リスク源やその事象が発生しうる原因・結果を特定し、リスクの一覧を作成する。

リスク分析では，リスク評価や対応計画の策定に必要な情報を整理する。分析の際には、リスク源、原因と結果、起こりやすさ等を考慮する。

リスク評価では、リスク分析結果に基づき、対応が必要なリスクや実施の優先順位に関して意思決定を行う。

Step5　リスクアセスメント結果を基にリスク対応計画を検討

リスクアセスメントの結果、明確になったリスクに対して、対応方法及び実施時期を明確にし、リスク対応計画として定める。リスクの対応方針には「リスクの低減」「リスクの保有」「リスクの回避」「リスクの移転」の 4 つがある。

Step6　リスク対応計画の経営層への説明・承認獲得

Step5 で策定したリスク対応計画を経営層に対して説明し、承認を得る。経営層から承認が得られなかった場合は、Step5 に戻り必要な修正を実施する。

Step7　リスク対応計画の実行及び管理

経営層から承認を得たリスク対応計画を実行する。事業部門やコーポレート部門が実行するリスク対応計画については、その進捗状況等を CISO 等が管理する。

Step8　リスクマネジメントの実行状況の評価及び改善点の検証

リスク対応計画の実行結果を基に、リスク対応の効果・改善点を検証する。

リスク対応計画の改善点に関しては、次年度以降のリスク対応計画の策定に活用する。

Step9　リスクマネジメント実施結果の経営層及び外部ステークホルダーへの報告

Step8 で実施されたリスクマネジメントの実施結果を経営層に対して説明し、承認を得る。外部ステークホルダーに対する報告により、リスクマネジメントに関わる説明責任を果たす

6.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 6-1 「リスクマネジメント」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	・ 経営戦略・経営方針	・ リスクアセスメント結果 ・ リスク対応計画
事業部門	・ 事業戦略・事業計画 ・ 保有する情報資産 ・ リスク対応計画実施結果	・ リスクアセスメント結果 ・ リスク対応計画
コーポレート部門	・ 事業戦略・事業計画 ・ 保有する情報資産 ・ リスク対応計画実施結果	・ リスクアセスメント結果 ・ リスク対応計画
監査役		
外部ステークホルダー	・ 法規制への対応要請 ・ セキュリティ強化に対する要請	・ リスク対応方針
ビジネスパートナー 外部委託先	・ 委託元からのセキュリティ強化要請	・ リスク対応方針
他の情報共有体制	・ インシデントや脅威動向	（特になし）
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ 情報セキュリティ目的・目標（A） ・ 自社の事業戦略と整合させたセキュリティ戦略・計画（B） ・ インシデント対応結果報告書（G）	（特になし）

6.5 作業の目標成果

本役割の成果は以下の通りである。

- リスクアセスメント結果
- リスク対応計画・結果

6.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、社内外の関係者との共同・連携が必要となる。
共同・連携する内容としては以下のようなものがある。

・ 事業部門における事業リスクと、セキュリティ部門のセキュリティリスク、コーポレート部門における企業リスクを踏まえ、リスクアセスメントを実施する。
・ 事業部門、セキュリティ部門、コーポレート部門がそれぞれ実施可能なリスク対応計画を策定する。
・ リスクアセスメント結果を経営層に説明する。

7. セキュリティインシデント発生時の事業継続計画策定（F）

7.1 目的・狙い

セキュリティインシデントは、場合によってその企業の事業そのものの継続自体を脅かすこともある。しかし、地震等の自然災害と異なり、セキュリティインシデントは原因や影響がすぐに特定できないことから、IT サービスにインシデントが発生しても事業継続のために IT サービスを維持するのか、被害拡大防止や原因究明のために IT サービス停止するのかの意思決定を企業として行う必要がある。また、仮に IT サービスを停止したとしても、企業価値を損なわないために、事業継続できるよう行動計画を定めておくことが必要である。

本役割は、サイバー攻撃等のセキュリティインシデント発生を想定した IT-BCP を策定することを目的としている。

なお、本役割では、セキュリティインシデントを考慮した事業継続に関わる行動計画・ルール等を便宜的に「セキュリティインシデント発生時の IT-BCP」と呼ぶが、何らかの特定の計画をドキュメントとして策定することが目的ではなく、企業が既に有する BCP や IT-BCP と整合性の取れた形でセキュリティインシデント発生時に事業継続の観点を含んだ計画・ルール等を定めることを目的とするものである。

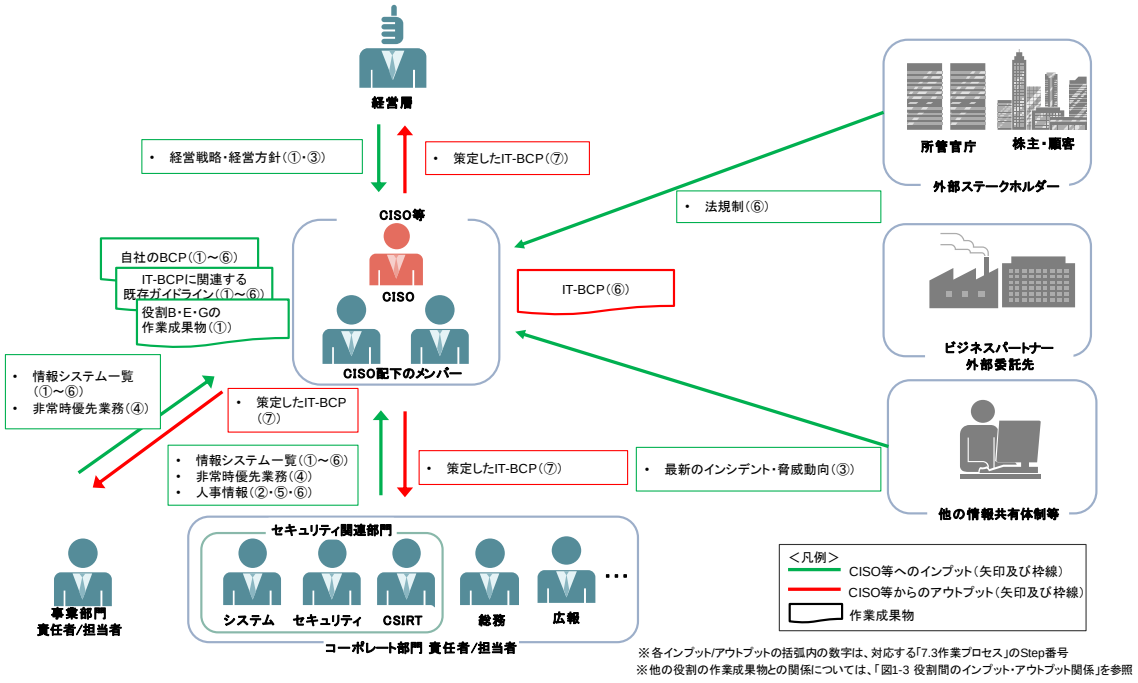

図 7-1 「セキュリティインシデント発生時の事業継続計画策定」の全体像

7.2 役割の作業内容

本役割の作業内容は以下の通りである。

- 事業継続との関係を考慮した上で、インシデントを想定した IT-BCP を策定する。
- インシデント発生時の対応を円滑に行うために、社内外に IT-BCP を説明し、承認を得る。

7.3 作業プロセス

本役割の作業プロセスは以下の通りである。

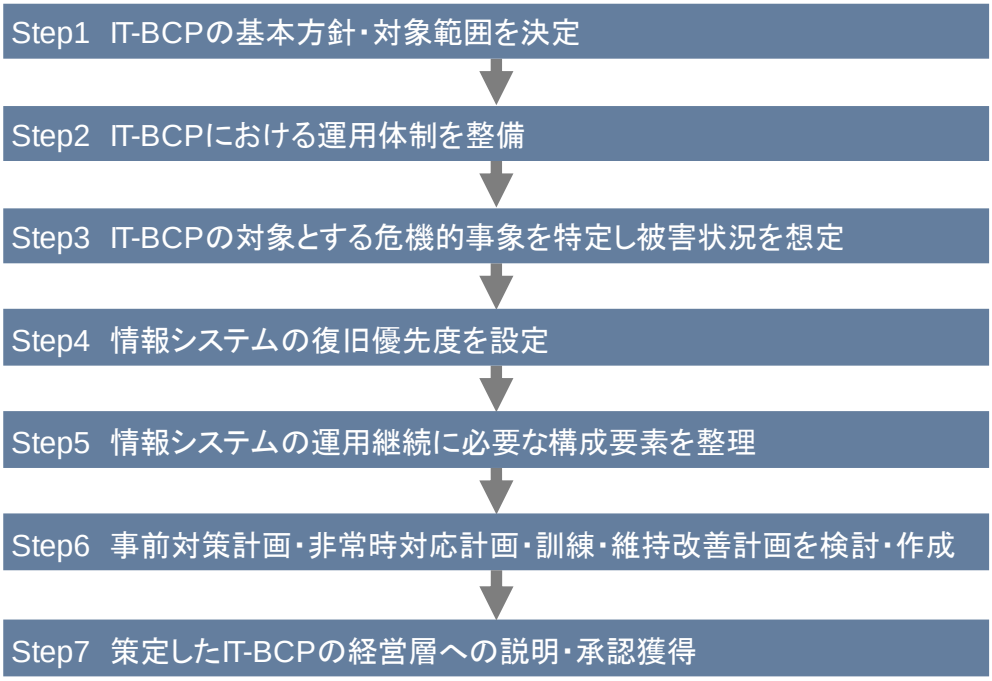

図 7-2 「セキュリティインシデント発生時の事業継続計画策定」の作業プロセス

Step1 IT-BCP の基本方針・対象範囲を決定

セキュリティインシデント発生時の事業継続計画策定にあたり、基本方針や対象範囲（対象となる事象、システムの範囲等）を定める。

Step2 IT-BCP における運用体制を整備

セキュリティインシデント発生時の事業継続計画策定の対象範囲を踏まえ、関係する組織（情報システム部、事業部門、コーポレート部門等）との間で検討・運用体制を整備する。

Step3 IT-BCP の対象とする危機的事象を特定し被害状況を想定

危機的事象における状況を明らかにし、対象とするシステムの早期復旧や稼働継続を阻害する要因である被害状況を想定する。

Step4 情報システムの復旧優先度を設定

被害発生時に優先して復旧する業務を設定し、目標とする復旧時間を確認した上で、復旧優先度を定める。

Step5　情報システムの運用継続に必要な構成要素を整理

業務の復旧に必要なシステムを洗い出し、そのシステムの復旧に必要な構成要素を分析する。さらに、システムの復旧優先度に従い、対策目標を設定する。

必要な情報の収集にあたっては、事業部門の協力を得る必要があり、対策目標を定める際も、事業部門の体制を考慮の上、実現可能な計画を立案する必要があることから、事業部門との良好なコミュニケーションを図ることが重要である。

Step6　事前対策計画・非常時対応計画・訓練・維持改善計画を検討・作成

危機的事象の発生時にシステムに生じる被害想定に対するシステムの脆弱性に関して、その脆弱性を解消する対策を検討し、事前対策計画として策定する。

システムの復旧活動に必要な対応体制を整備し、発生から復旧までの対応を示した対応フローや手順書を非常時対応計画として策定する。

担当者の理解力や対応力を高めるために、訓練計画を策定する。

事前対策計画、非常時対応計画、訓練計画をそれぞれ定期的に見直し、事業継続計画の実効性を継続的に維持するために、維持改善計画を策定する。

Step7　策定した IT-BCP の経営層への説明・承認獲得

Step6 で策定した IT-BCP を経営層に対して説明し、承認を得る。経営層から承認が得られなかった場合は、Step6 に戻り必要な修正を実施する。

7.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 7-1 「セキュリティインシデント発生時の事業継続計画策定」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	（特になし）	・ 策定した IT-BCP
事業部門	・ 情報システム一覧（構成要素、代替機器の有無、システム機能構成、設定情報、ベンダとの契約内容等） ・ 非常時優先業務	・ 策定した IT-BCP
コーポレート部門	・ 情報システム一覧（構成要素、代替機器の有無、システム機能構成、設定情報、ベンダとの契約内容等） ・ 非常時優先業務 ・ 人事情報（参集可能要員検討）	・ 策定した IT-BCP
監査役		
外部ステークホルダー	・ 法規制	（特になし）
ビジネスパートナー 外部委託先		
他の情報共有体制	・ 最新のインシデント・脅威動向	（特になし）
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ 既存ガイドライン、自社の BCP ・ 自社の事業戦略と整合させたセキュリティ戦略・計画（B） ・ リスクアセスメント結果（E） ・ リスク対応計画・結果（E） ・ インシデント対応結果報告書（G）	（特になし）

7.5 作業の目標成果

本役割の成果は以下の通りである。

・ IT-BCP

7.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、社内外の関係者との共同・連携が必要となる。

共同・連携する内容としては以下のようなものがある。

・ 事業部門における事業継続要求と、セキュリティ部門のセキュリティ対応可能な内容、コーポレート部門における広報等の必要な対応内容を踏まえ、実効的な IT-BCP を作成する。

・ 経営層、事業部門、コーポレート部門に対して、IT-BCP を説明し、承認を得る。

8. セキュリティインシデント発生時の危機管理（G）

8.1 目的・狙い

セキュリティインシデント[6]により、個人情報や機微情報が流出したり、インフラ供給や重要なサービスの停止により社会に影響を与えたりした場合、経営者は社会から経営責任が問われる可能性がある。しかし、サイバー攻撃は避けられないリスクである以上、非常時に迅速な対応が可能となるよう事前に対応計画や体制を整備すること、またインシデント発生後の通知先や開示が必要な項目に関して説明できるよう準備しておくこと、そして万が一インシデントによる被害が発生しても、対応計画に則り、適切に状況判断しながら、対処していくことが、企業価値を損なわないために必要である。

本役割は、経営層がセキュリティインシデントの発生時、企業価値を損なわないための機能を確実に維持することを目的としている。

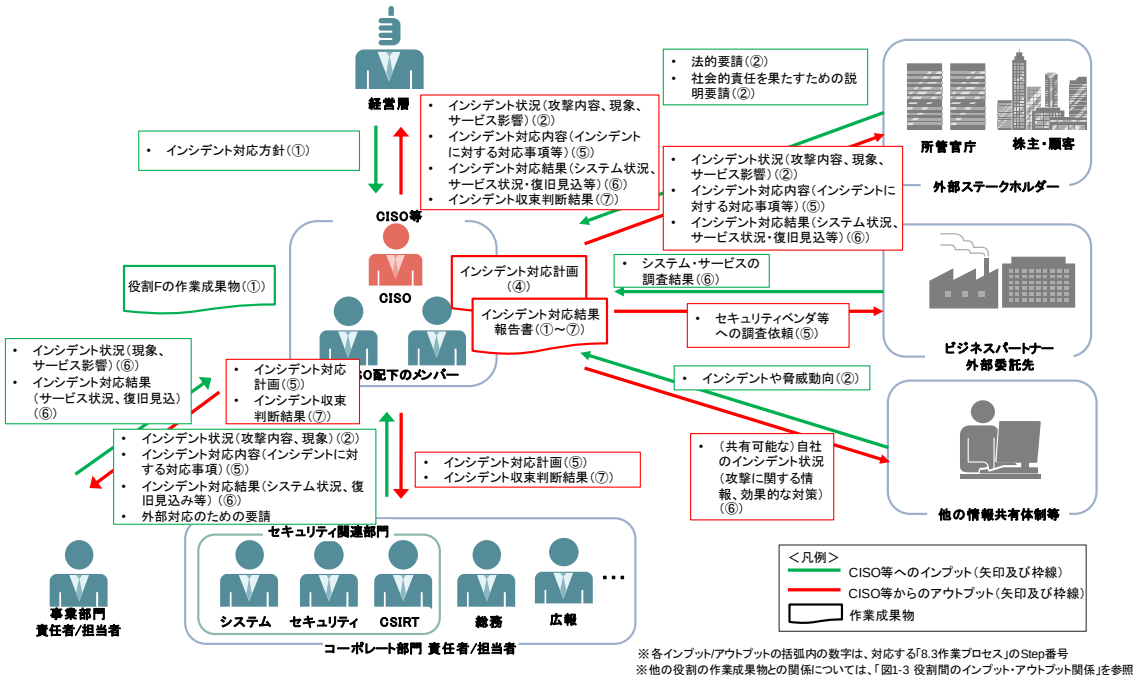

図 8-1 「セキュリティインシデント発生時の危機管理」の全体像

8.2 役割の作業内容

本役割の作業内容は以下の通りである。

- インシデントに関する情報収集・評価を行い、対応計画の策定と指示・管理を行う。
- 社内外との調整等を行い、インシデントを収束させる。

[6] インシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故を指す。

8.3 作業プロセス

本役割の作業プロセスは以下の通りである。

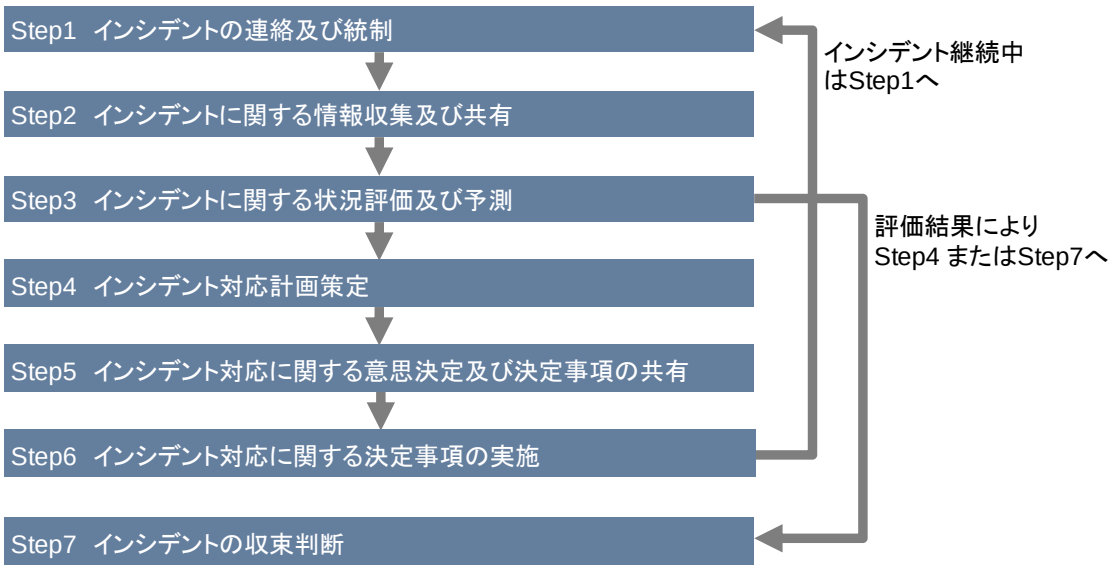

図 8-2 「セキュリティインシデント発生時の危機管理」の作業プロセス

Step1 インシデントの連絡及び統制

インシデントの状況を認識し、経営層からのインシデント対応方針に基づき、危機対応のための体制を構築する。

Step2 インシデントに関する情報収集及び共有

インシデントに関する情報を社内外から収集し、経営層及びインシデント対応を行う各部門に共有する。

Step3 インシデントに関する状況評価及び予測

収集されたインシデントに関する情報に基づき、インシデントや事業に関する状況を評価すると共に、今後のインシデントの変化や事業の状況、それに伴う事業に対する影響について予測を行う。

インシデントが収束したと判断した場合、Step7 に進む。

Step4 インシデント対応計画策定

Step3 におけるインシデントに関する状況評価及び予測に基づき、インシデント対応計画を策定する。

インシデント対応計画については、各事業部門の責任者も策定する。内容の整合性等については、危機時に全社的に組織される危機管理委員会等の統率組織等において調整を行う等が考えられる。

Step5　インシデント対応に関する意思決定及び決定事項の共有

Step4 で策定したインシデント対応計画に基づき、セキュリティ関連部門を含むコーポレート部門や事業部門に対して、各部門の所掌範囲に応じたインシデント対応計画についての指示を行う。

なお、事業部門に対する指示は、事業部門の責任者経由である場合と、事業部門に直接である場合がある。

Step6　インシデント対応に関する決定事項の実施

インシデント対応に関する対応事項を実施する。対応事項を指示した場合は、その対応状況について把握を行う。

対応状況については、（1）経営層／CISO 等の指示があった場合、（2）状況の変化があった場合、（3）（状況の変化がなくとも）一定時間が経過した場合、等、適時のタイミングで把握し、Step1 に進む。

Step7　インシデントの収束判断

Step3 のインシデントに関する状況評価結果により、インシデントが収束したと判断する。

なお収束判断としては、(1)インシデントに対する応急措置が終了した場合、(2)インシデントの原因調査・復旧対応が終了した場合、(3)正式な事故報告書の作成・影響を受けた顧客へのフォロー・再発防止策の検討等事後対応が終了した場合、等が想定される。

8.4 作業に必要な情報

作業に必要な情報には下表のものがある。

表 8-1　「セキュリティインシデント発生時の危機管理」に必要となる情報

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
経営層	・ インシデント対応方針	・ インシデント状況（攻撃内容、現象、サービス影響） ・ インシデント対応内容（インシデントに対する対応事項等） ・ インシデント対応結果（システム状況、サービス状況・復旧見込等） ・ インシデント収束判断結果
事業部門	・ インシデント状況（現象、サービス影響） ・ インシデント対応結果（サービス状況、復旧見込等）	・ インシデント対応計画 ・ インシデント収束判断結果
コーポレート部門	・ インシデント状況（攻撃内容、現象） ・ インシデント対応内容（インシデントに対する対応事項） ・ インシデント対応結果（システム	・ インシデント対応計画 ・ インシデント収束判断結果

関係者・組織	CISO 等へのインプット	CISO 等からのアウトプット
	状況、復旧見込等） ・ 外部対応のための要請（広報に必要な情報　等）	
監査役		
外部ステークホルダー	・ 法的要請 ・ 社会的責任を果たすための説明要請	・ インシデント状況（攻撃内容、現象、サービス影響） ・ インシデント対応内容（インシデントに対する対応事項等） ・ インシデント対応結果（システム状況、サービス状況・復旧見込等）
ビジネスパートナー 外部委託先	・ システム・サービスの調査結果	・ セキュリティベンダ等への調査依頼
他の情報共有体制	・ インシデントや脅威動向	・（共有可能な）自社のインシデント状況 （攻撃に関する情報、効果的な対策）
その他 （括弧内のアルファベットは関連する他の役割を示す。）	・ IT-BCP（F）	（特になし）

8.5 作業の目標成果

本役割の成果は以下の通りである。

- インシデント対応結果報告書（社内向け）

8.6 作業で協同・連携する社内外の関係者と協同・連携の内容

本役割を遂行するにあたっては、社内外の関係者との共同・連携が必要となる。
共同・連携する内容としては以下のようなものがある。

- 経営層に対して、インシデント状況やインシデント対応内容・結果、サービスの状況等についての適時の報告
- 企業価値を損なわないための、外部ステークホルダーに対する自社のインシデント状況、サービスへの影響等に関する情報開示
- 他の情報共有機関等とのインシデントや脅威動向に関する情報共有

9. 付録： CISO 等の経営・事業に関する役割のストーリー

現実的な企業の状況の下で、CISO 等の当事者がどう経営・事業に関する役割を果たすかイメージを掴んでもらうことを目的として、2 つの役割を取上げストーリー[7]を作成した。2 つの役割は、「全体方針」を決めるレイヤーの役割例として「A. セキュリティガバナンス体制の構築・運営」を、「具体的施策」を実施するレイヤーの役割例として「C. セキュリティ投資計画の策定・評価」を選んだ。

表 9-1　本ストーリーで取上げる役割と概要

役割		概要
全体方針	A.セキュリティガバナンス体制の構築・運営	・ 経営層がセキュリティリスクを認識し、組織として適切なリスク管理及びセキュリティ対策の実施、実施状況のモニタリング・評価できる体制を構築する
具体的施策	C.セキュリティ投資計画の策定・評価	・ 事業の価値最大化（セキュリティインシデントによる損失の最小化）の観点からセキュリティ投資計画を策定する ・ 収集した情報を基にセキュリティ投資計画を策定し、経営層に説明し承認を得る

このストーリーは、実在する企業の CISO 等の方から、経営・事業的役割に関する取組み内容をヒアリングして得られた知見に基づいて作成している。但し、ひとりの CISO 等の方から得た限られる経験談だけでは、現実感のあるストーリーを描くことは困難であることから、複数の CISO 等から伺った知見を組合せて描いている。その際、ストーリーの舞台となる企業は実在の企業とするのではなく、ストーリーに適した仮想企業を設定している。このストーリーを作成するにあたって、意図的に、ヒアリングにご協力いただいた実在の CISO 等の人物像や、実在の企業の特性に近い設定を避けた。万一、ストーリーに出てくる CISO 等や企業が特定の人物や企業に類似していた場合でも単なる偶然である。

ストーリー毎の記述の項目は、以下の通りである。

表 9-2　ストーリーの記述の項目

項目	内容
対象企業の状況	・ 仮想企業の事業内容や事業環境、CISO 等の設置状況等、仮想企業の組織構造について説明
解決すべきセキュリティ課題	・ 仮想企業が抱えているセキュリティ課題を説明
実施した活動	・「解決すべきセキュリティ課題」で設定した課題について、CISO 等がどのような取組を実施し、どのように課題を解決したか説明
活動結果及び評価	・ 一連の活動を通して、解決したセキュリティ課題、残課題について説明

本編のストーリーは、CISO 等の経営・事業に関する役割を検討する際の参考とすることを目的に作成したものであり、サイバーセキュリティ経営の適否の例示を目的としたものではない。また、記載された対策等を真似たことによって生じる結果について、なんら保証するものではない。

[7] 経営大学院で使われる教育方法ケースメソッドの教材である「ケース」を参考にした

このページは白紙です。

1. 準大手産業機器メーカーA 社：セキュリティガバナンス体制の構築・運営

登場人物

- CISO 室長　　このプラクティスの主人公。
  他社（流通業）の情報システム部門から昨年度途中に転職。
  前職での主な担当は社内システムの運用。
- CISO　　CIO を兼務する経営層の一人。
  昨年度期首に A 社情報システム部門長から昇格。

1.1. A 社の状況

（A 社と業界状況§§）

A 社は準大手産業機器メーカーで、国内に 10 社のグループ会社を有し、連結従業員数は昨年度末時点で 1 万人を超えた。グループ会社の半数は M&A を経て A 社グループ会社となっており、製造・販売拠点はグループ会社全部で 30 ヶ所にのぼる。A 社の事業は自社での機器製造、販売およびメンテナンスであり、ここ 10 年余りは製造した機器のリース事業も収益源になっている。

また現状では海外への製品展開は現地代理店に業務委託しているが、今後の事業拡大に伴い、現地法人を設立することも経営計画に挙げられている。

昨今の産業機械業界は、様々な業界で省力化投資への対応が重要視されていることや、IoT、ビッグデータおよび AI などの第四次産業革命を活用するための投資が、液晶・半導体、自動車やそれらの関連産業など幅広い業種で継続されていくものと見込まれ、受注規模は 5%程度の成長が期待されている。特に、第四次産業革命とものづくりを融合し、高付加価値を提供することが、今後の成長のカギになると想定されている。

（A 社での IT 活用）

A 社は、製品に各種センサと通信機能を組み込み、機器の異常や部品の消耗度合いをインターネット経由で確認できる基盤を有しており、販売およびリースした機器のメンテナンスに伴う利用者の操業停止時間短縮に貢献している。今後はセンサから収集した膨大な情報を分析し、部品や機器の設計および製造プロセスへフィードバックさせることで、高品質な機器の製造に役立てることも視野に入れている。このように、いわゆる IoT を活用したメンテナンスのサービス事業化により新たな収益源を確立するという CEO の経営方針の下、経営層に属する CIO がこれらの取り組みを主導的に進めている。

§§ 一般社団法人日本産業機械工業会：平成 30 年度 産業機械の受注見通し　http://www.jsim.or.jp/pdf/mitoushi-H30.pdf

（セキュリティ体制の概要）

A 社ではセキュリティガバナンスを所掌する CISO を経営層に設置しており、CIO が CISO を兼務している。A 社では、CISO の補佐とグループ全体での情報資産保護、セキュリティ対策統括を含むセキュリティマネジメントを担う組織として CISO 室を設置し、専任者 5 名および事業部との兼任者 10 名の総勢 15 名を配置している。また各グループ会社には会社としてのセキュリティマネジメントに責任を有するセキュリティ責任者とその実務を担うセキュリティ部門があり、セキュリティ全般に関して CISO 室との窓口となっている。

A 社では 5 年程前よりセキュリティに関する取組を進めており、前任 CISO 指示の下、グループ統一のセキュリティ対策基準（以降「基準」と略記する）の策定や、セキュリティ対策実施状況のモニタリングなどセキュリティガバナンス体制を構築し、3 年前に一応の完成をみた。

A 社では下記 3 つの活動をセキュリティマネジメントおよびセキュリティガバナンスの柱に据えている。

(1)　基準記載の推奨セキュリティアプライアンスおよびソフトウェア
　　（費用対効果を考慮して複数種類を記載）の適切な選択と導入および運用
(2)　運用状況の定期的な CISO 室への報告
(3)　CISO 室でのモニタリング（運用状況報告の精査と是正要請）

基準は CISO 室が 3 年前にグループ会社各社のセキュリティ対策状況をヒアリング等含め実態調査した上で、1 年かけてグループ会社全社で実現可能なセキュリティ対策を検討および策定したものであり、CISO 室がグループ会社各社のセキュリティ責任者へ集合会議形式および対面打合せで周知した。またモニタリングとしてセキュリティ責任者から対策実施状況を年 1 回（毎年 2 月、重大インシデント発生時にはその直後に適宜追加実施）報告する運用を定めた。

前任 CISO は基準策定とグループ会社全社への周知を見届けて退任となり、A 社情報システム部門長から昇格した現 CIO 兼 CISO がセキュリティガバナンス体制維持の任を引き継いでいる。

また CISO 室の責任者である室長は他社（流通業）の情報システム部門から昨年度途中に転職してきた。転職した前任者との引継ぎを経て、ようやく CISO 室の業務全体および対応窓口となるグループ会社各社のセキュリティ責任者の把握を完了し、今年度期首に室長へ昇格した。

最近同業他社でサイバー攻撃の被害が発生していること、各省庁からセキュリティに関する各種ガイドライン***が発行されたことから、経営層のセキュリティに対する関心がより一層高まっている。またメンテナンスのサービス事業化の推進に当たって、グループ全体としてのセキュリティ確保は事業が成立するための前提条件である、と A 社経営層は認識している。そのため、経営会議でもセキュリティが議題として取り上げられる機会が増えてきている。

（インシデントの発生）

セキュリティガバナンス体制構築開始から 5 年目となる今年度の初めに、グループ会社 X 社の営業

*** 例えば、下記のようなガイドラインが発行されている。
経済産業省：サイバーセキュリティ経営ガイドライン　http://www.meti.go.jp/policy/netsecurity/mng_guide.html
IoT 推進コンソーシアム、総務省、経済産業省：IoT セキュリティガイドラインを策定しました
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

拠点 Y で標的型攻撃メールによる従業員端末のウイルス感染が発生したことが、X 社のセキュリティ責任者から CISO 室へ報告された。拠点 Y のイントラネットとインターネットとの境界に設置されたファイアウォールが不正なアウトバウンド通信を検知して即座に遮断したことと、ウイルス感染が標的型攻撃メールを開封した従業員の端末のみで他端末へ感染が拡大しなかったことから、大きな被害にはいたらなかった。

本件の報告を受けながら、CISO 室長は違和感を覚えた。その標的型攻撃メールの文面に見覚えがあったからだ。CISO 室長自身も先月同じ文面のメールを受信していたのだ。しかし基準に従って導入している統合型セキュリティアプライアンスによって不審メールと判定されたため、添付ファイルを開かずメールごと削除した記憶があった。CISO 室長は本件について CISO へ速報するとともに、X 社における統合型セキュリティアプライアンス運用状況について追加調査を指示した。

1.2. 解決すべきセキュリティ課題

（インシデントの原因）

追加調査の結果、X 社は基準が推奨していない統合型セキュリティアプライアンスを導入していたことに加え、独自に製品選定や対策を実施していたことが判明した。Y 拠点に導入されていた統合型セキュリティアプライアンスでは、今回の標的型攻撃メールはインシデント発生時点では不審メールと判定されず、1 週間後のアップデートで対応がなされたことも判明した。今回のウイルス感染した端末についても、拠点 Y 独自のアンチウイルスソフトウェアが導入されていた。さらに前 CISO と対面打合せの結果、当面の間は従来の独自運用を基準相当の運用とみなし容認すること、及びリソース状況を見ながら順次基準を適用するとの合意がなされていたことが判明した。これは、セキュリティ対策に割り当てられる費用含めその他リソースが乏しい X 社の現状および Y 拠点がこれまで懇意にしていた OA 機器販売代理店と取引関係維持の必要性を訴えた当時の X 社セキュリティ責任者からの強い要望を受け入れた暫定措置であった。その合意は Y 拠点のセキュリティ担当者からヒアリングできたものの、記録が残っておらず、CISO 室では誰一人認識していなかった。また、基準適用への計画策定・実施は拠点の既存業務に埋もれてしまい、暫定運用のまま放置されていたことが判明した。

（グループ会社の現状把握）

追加調査の結果報告を受けた CISO は、当初から基準適用に例外を認めかつその状況を改善せず放置していたことが、グループ全体でのセキュリティガバナンス体制が形骸化している現状を招いたのではないかと懸念した。基準の形骸化は、企業として対外的な説明責任が果たせないだけでなく、自身が CIO として推進するサービス事業化の拡大に水を差しかねない危険性を抱えていると感じたからである。

CISO は経営会議で状況を共有して、是正に向けた適切な施策検討を開始したことを報告するとともに、CISO 室へ具体的な施策検討と実施を指示した。特に CISO 室が関係会社および拠点の対策実施状況を適切にモニタリングできていなかった事実を踏まえ、グループ会社全拠点の実態調査およびモニタリング体制不備の組織的な原因と適正化に向けた、実現性のある施策検討を実施するよう指示した。

CISO からの指示を受けた CISO 室長は、下記 3 フェーズで、課題の洗い出しと施策案の具体化を進めることにした。

(1) グループ会社各社での基準実施の実態調査
(2) CISO 室でのモニタリング業務の実態調査

(3)　モニタリング適正化に向けた施策検討

CISO 室長から報告を受けた CISO は上記方針を承認した。そして CISO 室全員でグループ会社の基準実施の実態調査から開始することになった。

（明らかになった現状）

2 ヶ月後、CISO 室はグループ会社全拠点の実態調査を完了した。並行して実施した CISO 室のモニタリング業務の調査も、同時期に完了した。その結果、CISO が懸念した「セキュリティガバナンスの形骸化」が現実であると分かった。CISO 室長は調査結果を見て驚いた。

（現場の現状）

昨年度末の調査報告に基づきグループ会社全拠点の実態を調査した結果、X 社 Y 拠点を含め 3 社 8 拠点で、基準と異なるセキュリティ対策および運用がなされていることが判明した。これは全 30 拠点の 1/4 強に相当する。当該 7 拠点についてさらに現状運用に至った要因を調査したところ、

a)基準を満たすシステムおよび機材調達費用の不足

b)基準を適切に運用するためのセキュリティスキルを備えた要員の不在

の 2 つが浮かび上がった。また W 事業部と CISO 室を兼務する w が、Z 社からの調査報告がないことに気が付いた。w は W 事業部門の部門長から、CISO 室兼務発令の際、事業部だけでなく所管グループ会社のセキュリティ施策についても留意するよう指示されていたため、調査開始時点で Z 社が報告対象に挙がっていないことにいち早く気が付いた。Z 社に確認したところ、一昨年度に M&A でグループ入りし、人事系および財務系システムの連携で手一杯だったこと、A 社情報システム部門からはセキュリティについて特段の指示がなく基準実施状況の調査や報告が必要であるとの認識がなかったことが明らかになった。ただし、Z 社では従来から独自のセキュリティ対策を実施しており、その内容も基準と類似する部分が多かったため、今回のインシデントも防止できていたことが分かった。

一方、現状は基準を満たす運用が実施されているグループ会社、拠点でも、

c)基準実施項目が多くかつ繁雑な書式での報告が負担になっている

とのコメントが寄せられた。特に自由記載での回答項目が 1/3 程度あり、基準運用や状況調査および CISO 室への報告に掛かる作業負荷の高さに不満を感じる担当者からは軽減を求める要望が出た。また

d)基準での対策が過剰と思われており、必要性の納得感が得られない

とのコメントが一部セキュリティ担当者や従業員から挙がり、基準対策実施のモチベーションが充分でないことも分かった。

（CISO 室の現状）

一方 CISO 室でのモニタリング業務の調査では、

e)CISO 室自体もリソース不足に陥っていた

という実態が判明した。グループ会社の全 30 拠点から年 1 回報告される基準実施状況の精査は、各所からの問合せ対応等通常業務をこなしながらの作業となるため 2 ヶ月弱の期間を要しており、精査ができていない調査項目があった。特に上記 c)については CISO 室でも記載の読み込みや結果整理が必要となり、モニタリング業務を繁雑なものにしていた。また精査作業の約半分は、各グループ会社セキュリティ責任者への個別問合せに割かれていた。すなわち、セキュリティ責任者は必ずしもセキュリ

ティスキルが充分でないためにCISO室との円滑なコミュニケーションが難しく、基準実施に当たってCISO室へのセキュリティ対策実施に関する確認や問合せが頻発していた。具体的な例では、基準記載のセキュリティ用語や略語についての問合せや、多層防御の意義等セキュリティに詳しいCISO室要員にとっては常識の事柄についても背景や思想から納得してもらうための説明など、個別対応に時間を割かれていた。また報告書の記載内容についてもセキュリティ責任者とCISO室との間に認識のズレがあり、

f)基準を満たさない運用でも報告書上は適切に実施されていると記載され、かつCISO室として現状確認がなされていない

ということも判明した。例えば離職者IDの削除について、基準では「適宜削除する」運用を求めているが、要員異動が少ない拠点ではこれを都合よく解釈して、年度途中の離職者のID作業は先送りして年度初めのみの一括作業としている拠点もあった。

CISO室長は判明した状況に驚きながらも、具体的な施策案検討に着手した。CISO室での議論の結果、優先して解決すべき課題を

(1)　モニタリングに要する過大なリソース負荷

(2)　スキル、モチベーションの不足によるモニタリングの精度の低さ

の2つに絞り、実態調査結果と併せCISOへ報告した。

1.3.　実施した活動

（施策案検討）

CISOは課題認識には同意した。特にセキュリティ対策についてのモチベーション不足は、CISO室とセキュリティ責任者のみならず全従業員についての課題であるとコメントした。しかしセキュリティ対策への早急かつ大幅な追加リソース投入は、予算や人事の制約から困難であるともコメントし、まずは現状実施可能な施策を検討し報告するよう指示した。

CISOのコメントと指示を受け、CISO室では施策検討を開始した。まずは全員で現状を共有し、ブレインストーミングで理想像を検討した。特に事業部との兼任者からは、事業部門の実情を共有してもらい、基準実施の阻害要因をコメントしてもらった。数回のブレインストーミングの結果、下記コメントがまとまった。

- 基準遵守徹底の指示だけでは、現場の状況や過去の経緯から早急な基準適合は難しいと思える。現場へのインセンティブの提示や、予算含めリソースの追加提供が必要かもしれない。
- 現状基準の実施内容は事業部門によっては過剰かもしれない。扱う情報の機密レベルに応じたセキュリティ対策にすべきではないか。
- セキュリティ責任者のスキルにばらつきがある。スキル不足な責任者がいる状況は致し方ないが、セキュリティの基本的な考えや基礎知識を備えてもらえれば、問合せ対応やモニタリングがより容易になると思われる。
- 現基準の記載にも改善の余地がある。例えば具体的な数値を記載すれば認識ズレを防げる。セキュリティ責任者にスキルが不足していても理解できるよう、対策の背景説明や図解があれば現場からの問合せを減らせるかもしれない。
- モニタリング結果の精査の時期だけリソース不足を補うため、CISO室を固定的に要員増強することは効率的ではない。とはいえ現状人事制度では一定時期だけ要員を増やすことは難しい。

CISO室ではこれらを踏まえて、実現可能な施策案として

(1)　基準項目の絞り込み
(2)　相互モニタリングによるスキル底上げ
の 2 つをまとめることにした。

（基準項目の絞り込み）

CISO 室は、グループ会社の事業内容や保有する秘密情報と、対応する基準項目についてサンプル調査を実施した。その結果、グループ会社間で差異はあるものの、基準での実施項目の 1～3 割は事業との関連が乏しいことが判明した。CISO 室では、これら事業と関連が乏しい基準項目を網羅するよりも、事業に直結する基準項目に絞って適切な実施を優先し、かつモニタリングの精度を上げることで、セキュリティ対策実施の負荷軽減とセキュリティ向上の両立、すなわちセキュリティの投資対効果向上を実現できるのではないか、との仮説を立てた。

そこでグループ会社で事業と関連が乏しい基準項目の和集合を任意項目とし、対策と報告の実施を必須とはしない方針を定めた。ただし任意項目の設定に当たっては、CISO 室と各グループ会社のセキュリティ責任者が協議し、各社の主要事業におけるセキュリティ確保に問題を生じないか、確認することにした。また文言解釈のズレをなくすため、目標数値を提示するなど具体性を持った記載に改めることにした。具体例としては顧客情報管理について、これまでの基準では適切に管理し不要時には廃棄することのみを記載していたが、今後は入手時の同意取得や半期に 1 度の棚卸実施（不要情報は 1 ヶ月以内に廃棄することを含む）と廃棄時の記録を保存するなどを基準に明記し、実施が困難な場合の代替策も、併せて記載した。

これらにより基準項目を
a)A 社含めグループ会社全体で必須実施
b)グループ会社個別に必須実施
c)実施を推奨するが必須ではない
の 3 種に分類する。実施必須となる基準項目は、各社平均 2 割程低減できると見込まれた。

（相互モニタリングによるスキル底上げ）

これまでのモニタリングは、各グループ会社からの状況調査結果を CISO 室が精査するという上意下達なものであった。CISO 室は「目付役」として煙たがられ、基準対策および状況調査実施の際、現場のモチベーション低下を招き、セキュリティ意識も向上しなかった。また精査する側の CISO 室も結果報告を読み込む負荷が高く、報告書だけで現場の状況を正しく把握することには限界があり、モニタリングの精度低下の一因にもなっていた。

そこで CISO 室では、モニタリングを CISO 室が実施するのではなく、グループ会社各社のセキュリティ実務担当者も参加したモニタリングチームを編成し、相互にモニタリングしあう方式を検討した。例えば実施状況調査の担当者として、CISO 室とモニタリング対象でないグループ会社のセキュリティ担当者の 2 者で構成するというものである。また結果報告書の精査だけでなく、グループ各社へ出向いた現状確認も含めることにした。

これには、運用当初はセキュリティスキルが充分でないグループ会社のセキュリティ担当者が含まれることによって、手戻りや知識共有のための作業負荷増が発生するというデメリットがあるものの、長期的にはモニタリングに掛かる CISO 室の作業量を現状の半分程度に軽減できるメリットが見込まれるだけでなく、セキュリティ担当者のスキル向上（底上げ）や、部外者から評価されることによ

るセキュリティ意識醸成につながると考えられる。検討の過程では、セキュリティのスキル向上や意識醸成の対策として研修実施も案に挙がった。しかし教材準備および研修実施にはグループ全体で時間と費用が捻出できない現状や、実務経験による OJT のほうがより効果的ではないかとの意見があり、CISO がモニタリングの一時的な進捗低下を承認することを前提に、セキュリティ担当者の現状確認参加を含めたモニタリングの実施を決定した。

グループ会社へ出向く現状確認の副次的な効果として、A 社グループ内でセキュリティに関わる人材の交流促進が見込める。これらにより CISO 室と各社セキュリティ担当者とのコミュニケーションが円滑になり、確認や問合せの効率化が期待できる。

（施策具体化に向けた検討）

さらに CISO 室では、これら 2 施策の優先度を議論し、「基準項目の絞り込み」を優先することにした。セキュリティ責任者との協議に際し推奨項目をあらかじめ提示できれば、負荷が軽減される現場としては受け入れやすいし、監査参加への心理的障壁も下がるのではないか、との思惑があった。

スケジュールについては、本施策についての CISO 承認後から「基準項目の絞り込み」を開始し、グループ会社各社のセキュリティ責任者との調整を含め 2 ヶ月で完了させる。その後 1 ヶ月かけてグループ会社責任者全員へ個別対面で基準説明と監査参加要請を実施し、下期からモニタリングを開始することにした。

施策案をまとめながら、CISO 室長は一抹の不安を感じていた。今回の施策検討は、軽微とはいえインシデント発生直後に CISO 指示で実施されたことを知っている従業員もおり、施策実施後に基準実施に不備があれば何らかのペナルティがあるのではないかと懸念する噂も耳にしていた。このような噂を払しょくし形骸化したセキュリティガバナンス体制を立て直すには、現場の協力が不可欠である。現場の CISO 室に対する認識を「目付役」から「相談相手」へと変えてもらうには、施策だけではない「何か」が必要であると悩み続けたものの、CISO への報告までに「何か」を見つけることはできなかった。

1.4. 活動結果及び評価

（CISO への施策案具申）

CISO 室長は、検討した 2 施策案の内容と実施スケジュール案を CISO へ報告した。また現場の協力を取り付ける「何か」が必要だと感じながらも、それを見つけられないことも率直に説明した。

CISO は施策案を概ね合意し、以下のコメントおよび追加指示を出した。

- これら 2 施策は「基準を実施できない悪者捜し」ではなく「セキュリティガバナンス体制の組織的な立て直し」が狙いであることに留意すること。必要であれば CISO 名義でこの狙いをグループ全体に周知する。
  - 当初はセキュリティガバナンス不備が頻繁に見つかるかもしれないが、立て直しのために必要な過程であり、それを責めることはない。セキュリティガバナンス不備が水面下で続く状態が続くことのほうがよくない。
- 基準の次回見直しはいつ実施予定か？事業環境が目まぐるしく変わる現状において、セキュリティ対策は適宜見直しされるべき。
- 「基準項目の絞り込み」および「相互モニタリング」については、a）A 社含めグループ会社全体で必須実施項目の案が完成次第、グループ会社各社のセキュリティ責任者と調整を開始するこ

と。

- セキュリティガバナンス体制の立て直しにはスピード重視で当たる必要がある。実施範囲を絞ったスモールスタートでよいが、記録保存を含め着実に実施すること。

- 「相互モニタリング」実施に当たっては対象グループ会社のセキュリティ実務者も加えた「3 者監査」とすること。
  - 本来の意味での「監査」ではなくなるが、この施策はセキュリティ教育の側面もあるため、少なくとも 3 年は「3 者監査」で実施すること。
  - 監査は、セキュリティ責任者ではなくグループ会社のセキュリティ実務担当者が実施すること。
  - b)当該グループ会社のみ実施必須の項目選定と併せて実施すること。グループ会社の特性や個別事情を把握している要員が参加することで、より適切な項目選定が可能になる。
  - 「3 者監査」では「不備の指摘」ではなく、「基準実施の阻害要因発見」に注力すること。監査対象が委縮し不備を隠蔽する状態に陥らないよう、監査側は言動に細心の注意を払うこと。
  - グループ会社からは監査要員リソース確保について、現場は事業優先のため非協力的な反応をするかもしれない。CEO とも相談し、一時的な兼務発令や当該事業への代替リソース投入等を当該グループ会社担当役員や人事担当役員とも掛け合う。

CISO 室長はこれらのコメントと指示を反映して施策を確定し、早速基準項目の絞り込みに取り掛かることにした。

（グループ会社への説明と反応）

1 ヶ月後、「基準項目の絞り込み」を終えた CISO 室は、グループ会社各社へ「絞り込んだ実施必須項目」と「グループ会社固有の適用基準」および「3 者監査への参加」について説明した。

グループ会社各社のセキュリティ責任者の反応は、およそ 3 つに分かれた。

1 つ目は今回の施策に概ね賛成する人々で、割合は 2/3 を占めた。絞り込みによる基準項目の低減は、調査コストの削減だけでなく、セキュリティ対策での注力ポイントの明確化にもなり、自社の経営層や事業部門にも受け入れられやすいとのことであった。

2 つ目は今回の施策を渋々受け入れることにした人々で、1/4 強の割合の 8 社が該当した。この中には今回インシデントが発生した X 社も含まれており、セキュリティ対策の更なる軽減を求めてきた。特に「3 者監査」については、要員確保の点から抗議もあった。そのような意見に対し CISO 室長は、セキュリティ人材育成の観点があることと、各社がセキュリティ対策を実施する上で他社での施策を参考にして気づきを得てほしいこと、を粘り強く説明し、各社のセキュリティ責任者も納得の度合いに差はあれ、全員から施策実施の合意を得た。

3 つ目の 2 社は、会社としてのセキュリティ対策実施自体に積極的ではなかった。この 2 社は以下の共通点があった。

- 汎用部品の生産を主とする二次部品メーカーであり、売上額の半分弱は A 社グループ外との取引による。すなわち A 社グループへの帰属意識が高くない。
- 経営層のセキュリティへの関心が低く、基準実施の必要性を納得していない。またこれまで（幸いにして）セキュリティインシデントに遭遇した経験がない。
- 売上原価率が 75%程度に高止まりしており、基準実施はおろか IT 関連の予算も充分に確保で

きていない。

- セキュリティに詳しい人材が社内にそれぞれ 1～2 名しかおらず、該当者は情報システム部門を兼務しているため極めて多忙である。

CISO 室長は、この 2 社のセキュリティ責任者へ言葉を尽くして説明したが、彼らは施策準拠のセキュリティ対策実施について明確な回答を避け、自社経営層と相談すると回答した。その後 2 週間、CISO 室長は 2 社のセキュリティ責任者へ相談状況を何度となく問い合わせた。しかし彼らから当初こそ「経営層との相談が長引いている」との返答があったが、やがて返答も立ち消えになった。CISO 室長は彼らの煮え切らない対応に痺れを切らし、事態打開のための策を練り始めた。

CISO 室長は 2 社のセキュリティ責任者の挙動から、このままでは 2 社のセキュリティ対策は、なし崩し的に現状が維持され、いつかは A 社グループ全体に波及する重大インシデントにつながるのではないかとの懸念を抱いた。海外では取引業者への標的型メールが発端になった大規模情報漏えいが発生した事例があったとも聞いている。A 社グループとしてのセキュリティガバナンス体制を立て直しには、所掌する CISO からも何らかのメッセージを発することが有効ではないかと考えた。

CISO 室長は、CISO へ現状を報告するとともに、CISO からグループ全社に向けたメッセージの発信について相談した。

（CISO からのメッセージ）

CISO はメッセージ発信を了承したが、条件を 2 つ付けた。1 つは、CISO はグループ会社各社のセキュリティ対策実施および基準準拠に向けた努力に感謝していることを伝える、ということである。もう 1 つは、今やセキュリティは A 社グループとしての事業継続に必要な要素となっていることを、特にグループ会社の経営層に向けてわかりやすく伝える、ということである。

また、CISO からは下記のコメントもあった。

- 基準実施に難色を示すグループ会社 2 社は、効果を明確に計測しづらい「セキュリティ対策」よりも、事業への投資を優先させたいと考えているのだろう。この考えはもっともである。セキュリティの重要性だけではなく、「別の方向性」から話をすることも必要ではないか。
- 「別の方向性」の材料として、世の中の動向や基準に関わるデータをいくつか算出しておくと役に立つかもしれない。また
  (1) A 社本社システムにおいて、基準実施により防御した昨年度の不正通信の件数及び全通信における不正通信の概算割合
  (2) A 社本体が基準準拠のために投じている、昨年度 1 年分の費用

CISO 室長は CISO との相談の中で、ジャストアイデアではあるが「費用対効果」の視点を踏まえてグループ会社 2 社へ改めて基準実施について打合せすることを提案し、その場で了承を得た。

CISO 室では、発信するメッセージの文言を検討するとともに、セキュリティ対策に関する最近の動向を大まかにではあるが調査することにした。すると米国の公的機関から発行した文書が最近改訂され、サプライチェーンでのサイバーリスクマネジメントについて追記があったことが分かった[†††]。

これらのコメントを受け、CISO 室では発信するメッセージの文言を検討するとともに、費用対効果およびサプライチェーンにおけるサイバーリスクの視点を踏まえて、グループ会社 2 社と改めて基準実施について打合せをすることにした。CISO 室長は作成したメッセージの内容について CISO の承認を

[†††] NIST：https://www.nist.gov/cyberframework/framework

得ると、グループ会社の経営層とセキュリティ責任者宛に、CISO 名でメッセージを発信した。

（施策実施と結果）

難色を示していた 2 社との再度の打合せで、CISO 室長は下記 3 点を説明した。

- A 社本社は絶えずある程度のサイバー攻撃を受けているが、そのほとんどは基準実施により実被害を未然に防いでいる。仮にこれらのサイバー攻撃が成功してしまった場合の被害額を算定してみると、基準実施費用の数倍になることが判明した。ブランド棄損や被害からの復旧過程での現業停滞も考慮すると、被害額はさらに膨れ上がるかもしれない。
- 基準実施のためのリソースを早急に追加投入することは難しい現状も承知しているし、これまでの取引先を無下にできないことも承知している。もし、基準実施以上の費用対効果が見込まれるセキュリティ対策があれば、A 社グループに展開したいので共有できないか。
- 米国ではサプライチェーンでのサイバーリスク管理について、公的機関から資料が出ている。今後 A 社グループが海外で事業を拡大していくにあたり、調達段階からのセキュリティ対策実施状況を問われる場面が出てくるのではないか。

説明を聞いた、2 社のセキュリティ責任者の顔色が変わった。彼らは自社で事業を牽引する立場でもあり、思うところがあったようだ。また現状の独自のセキュリティ対策が A 社グループ以外との取引における懸念材料となることにも思いが至ったのかもしれない。打合せの結果、CISO 室と 2 社は下記内容で合意することができた。

- 現状の独自対策を基準への移行措置として認めることを基準に明文化し、基準への移行について CISO 室が支援すること。
- 上記支援のため、CISO 室のメンバを 2 社へ兼務させること。

（今後の展望）

施策実施についてグループ会社全社の了解を取り付けた CISO 室は、早速 3 者監査でのチーム編成に取り掛かった。１つの監査チームに含まれるグループ会社および監査対象のグループ会社は、監査の公正・中立のため、できるだけ互いの事業関係が疎であるよう工夫した。3 者監査は今年度下期から実施するが、当初は様々な問題が発生することが想定される。発生した問題について 1 つ 1 つ原因を探り、考えられた改善策を来年度の 3 者監査へ適用することにした。

施策実施が一段落ついた後、CISO 室長はふと CISO からのコメントを思い出した。なぜあの時 CISO は「別の方向性」から話をすることに触れたのだろうか。「費用対効果」すなわち事業の視点や「世の中の動向」を踏まえないセキュリティ対策は、充分な効果を得ることが難しいことを、事業経験の乏しい自分に気付かせるため、あのような話し方をしたのではないか。CISO 室長は、技術やルール適用だけではないセキュリティ対策の難しさを実感するとともに、セキュリティと事業の関係性を気付かせてくれた CISO への感謝の想いを新たにした。

（以上）

2. 中堅アパレルメーカーX社： セキュリティ投資計画の策定

登場人物

- 菅 課長　　総務部システム管理課の課長（このプラクティスの主人公）
- 押尾 課長　　EC 事業推進室の課長
- 室井田 執行役　　執行役(営業担当) 兼 EC 事業推進室の室長

2.1. X 社の状況

（アパレル業界の EC 化と X 社）

X 社は、働く世代に人気がある、有名な中堅アパレルメーカーである。この社の主な顧客は、次のような特性を持つ。

- 30 代～40 代前半の働く世代
- 新しいものへの関心・適応性が高い
- 購買力があり、カード決裁の利用が多い

アパレル業界では、店舗販売の市場が伸び悩む中、ネット販売の成長性に期待が集まっている。業界新聞の調査によると、アパレルの EC[‡‡‡]での売上げはすでに国内で 1 兆 5 千億円超に達しており、売上全体に対する EC 化率は約 11%であるが成長率が前年比 10%増と他の販売チャネルに比べ存在感を増しつつある。米国ではすでに EC 化率が約 20%にまで成長しているが、むしろ日本でこそ、労働力不足を背景として、これを上回る割合になるとの読みもある。例えばアパレル全体を牽引している SPA[§§§]の業態の企業は当初から EC 化に積極的だった。最近では、メーカー、百貨店などあらゆる業態で、また企業の大小に関係なく EC 化を推進する傾向にある。X 社の競合他社の中には、前年度すでに EC 化率約 20%に到達したところもある。経済産業省の調査でも、アパレル業界は、特に EC 化の市場規模が大きな業界であることが分かっている（表 1）。

‡‡‡ Electronic Commerce。本稿ではインターネットを使った通販を指す。

§§§ Specialty Store retailer of Private label Apparel。製造小売などと呼ばれ、小売業が新たな製品のアイデア出しから生産・販売までまとめて管理する業態を指す。

しかしX社ではこれまで、自社の高級なブランドイメージを損ねる恐れがあると考え、EC化には積極的に取り組んでこなかった。また歴代の経営陣は、長いX社の歴史の中で培ってきた百貨店・専門店との関係を重視し、店舗販売以外の販売チャネルの急拡大に慎重だった。EC事業としては、他社が運営するオンラインモールに、小規模に出店しているだけである。

表1 物販系分野のB2C EC市場規模

分類	市場規模（億円）	EC化率（%）
衣類・服飾雑貨等	15,297	10.9
食品、飲料、酒類	14,503	2.3
家電、AV機器、PC等	14,278	29.9
雑貨、家具、インテリア	13,500	18.7
書籍、映像・音楽ソフト	10,690	24.5
化粧品、医薬品	5,268	5.0
自転車、自動二輪車等	2,041	2.8
事務用品、文房具	1,894	33.6

ところがマーケティング調査の結果、X社ブランドの商品に関心の高い潜在顧客の一定の割合が、ECサイトでの購買額の多い消費者であることが分かった。これをきっかけに、EC事業をもっと強化すべきだとの意見が社内に広まりつつある。

（X社 ECサイト構築の方針）

EC事業重視の先頭にいるのが、室井田執行役（営業担当）である。室井田は入社以来、ブランド開発・育成を手掛けてきた人物であり、この3年の間に、とあるキャリア女性向けブランドの事業部長として実績を積み、担当ブランドを旗艦ブランドに押し上げた。その功を買われ、半年前、執行役に就任し、既存ブランドの売上げ拡大と新規ブランド開発への貢献が期待されている。

室井田は、セカンドブランドやリテール・アウトレットのチャネルとしてオンラインモールを使うだけでなく、ネット販売の自社サイトを構築し潜在顧客を取り込むことで、売上げ拡大の手段として積極的に位置づける施策を打ち出した。室井田によれば、この施策を採る・採らないに選択の余地はなく、EC強化は必然だという。今年度、EC事業推進室（以下、EC推と略記）を新たに設立し、自ら室長に就任した。

EC推の第一の方針は、X社ブランドの高級感にふさわしいデザイン性・操作性に優れたECサイトにすることだ。従来出店してきたオンラインモールはサイトデザインの自由度が低く、旗艦ブランドをはじめとする主要ブランドの高級イメージに相応しいコンテンツは、実現できなかった。自社サイトにする目的の一つはこれである。

第二の方針は、X社ブランドの商品に関心の高い顧客のかなりの割合が、EC サイトでの購買額の多い消費者であるとの調査結果（前述）から、主要ブランドのほとんどをECサイトで購入できるようにして既存ブランドの売上げ拡大を狙うことである。

第三の方針は、X社ECサイトの訪問者の閲覧行動・購買行動から大量・緻密なデータを取得し、既存ブランドの販売キャンペーンや、新ブランド開発に役立つマーケティング分析の機能を実現することだ。このため、オンプレミスとして、高度で柔軟なデータ分析（データマイニング、ビッグデータ解析）機能、MA（マーケティングオートメーション）機能を実現する。オンラインモールは、こうしたオンプ

レミス上の機能と円滑な連携を組むことが難しく、これが、自社サイトにする目的の二つ目である。

この他、SEO[****]対策、コンバージョン率[††††]向上策等、通常の EC サイトのマーケティング施策はもとより、Web 限定商材の拡充や EC 専用ブランドの早期投入など、いくつもの施策を組合せる。EC 推はこれらを背景に、意欲的な事業計画を目論んでいる。EC 化率を 4.7%（来年）、6.5%（2 年目）、8.3%（3 年目）と向上させ、EC の売上高（営業利益）も 2 年目 44.5 億円（2.7 億円）、3 年目 57.8 億円（8.6 億円）と拡大する計画である。2 年目には単年度黒字化を達成する（図 1）。

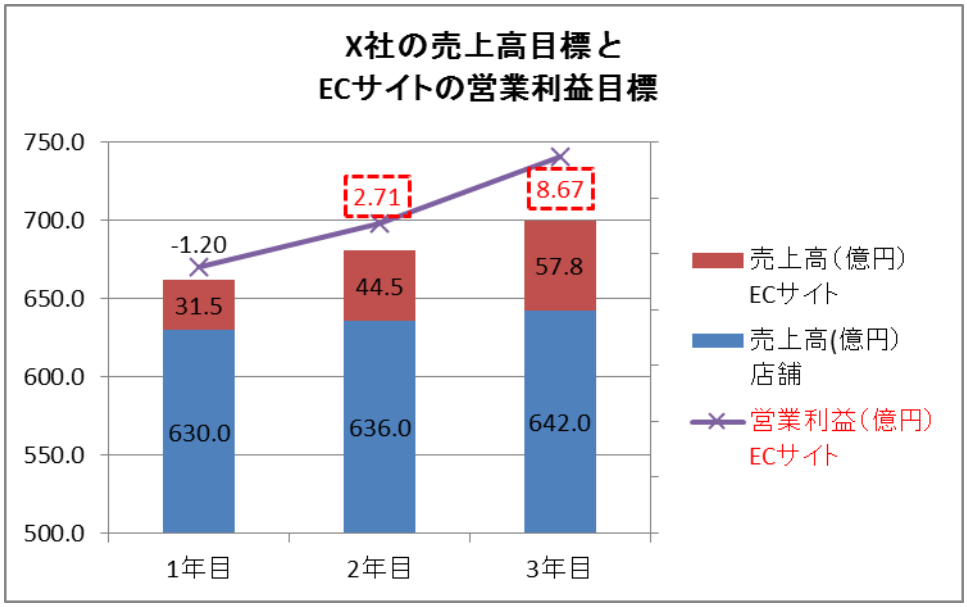

図 1　X 社の売上目標、EC サイトの営業利益目標[‡‡‡‡]

（EC 事業推進室）

これら方針の実現を任されたのは、EC 推の押尾課長である。押尾は、EC 推発足時に、小売業他社のネット通販部門から転職してきた人物である。IT 技術者ではないが、EC サイトの運用業務のリーダーを長年務めてきた人物で、EC 関係者の間では、とくに、MA や CRM（顧客管理）の専門家として名前が知られていた。

押尾チームの本来のミッションは X 社ブランドサイトの運用である。EC 推は、これまでオンラインモール関連の業務を担当していた社員の他、押尾と同様に他社からキャリア採用した、EC サイト運用の経験者で構成されている。しかし当面は、サイト構築が主な業務になっており、いち早くサイトを立ち上げることが求められている。X 社の中には Web サイトを開発する部署はないので、サイト構築とデータ分析機能の実装は、社外の Web サイト構築業者に発注することになる。

すでにブランドサイトの機能仕様は策定済みである。市販の EC サイト構築パッケージをベースに、X 社独自のカスタマイズを加えるのがその基本である。カスタマイズの主要項目はデータ分析機能等の

[****] Search Engine Optimization の略。検索エンジン最適化。

[††††] 本稿では、EC サイトの閲覧者数に対して商品購入に結びついた人数の割合を指す。

[‡‡‡‡] 複数のアパレル企業、EC 事業の公開されている事業計画を参考に、IPA で仮想的に作成。

実現である。

サイト構築のプロジェクトは開発予算・初年度の運営予算を計上し、先日、役員会の承認を得たばかりだ。次のステップとして、サイト構築のプロジェクトを予定通り進めながら、並行して各ブランドの営業部と共同し、コンテンツ準備を進めているところだ。それぞれの営業部も積極的にこの活動に取組んでいる。

2.2. X 社 EC サイトのセキュリティ投資の課題

ある日のこと、EC 推の定例会が終わり、押尾課長が会議室を出ようとしていると室井田室長に呼び止められた。セキュリティの仕様を一度、シス管に見せて意見を聴くように、と言うのだ。

総務部システム管理課（以下、シス管と略記）は、メールサーバーや社内のネットワークといった IT 基盤と、人事管理・経理・X 社のオフィシャルサイトなどの社内共通 IT（コーポレートの IT システム、以下 CIT[§§§§]と略記）を管理・運用している部署である。ネット通販サイトのような、事業部門による IT の事業活用（以下 BIT[*****]と略記）には関係していない。セキュリティ仕様について意見を聴きたいと持ちかけても、対応してもらえるのだろうか。室井田の話では、常務が業界団体のセミナーで情報セキュリティ対策のセッションを聴いてきたようで、EC サイトのセキュリティについてシス管の意見を聴いているのかと質問されたそうだ。シス管に相談にのってもらえるよう、私から総務部長に話しておくから…と、室井田は言った。

今回のブランドサイトの仕様は、押尾が前の会社で運営していた EC サイトのセキュリティ仕様をまねている。前のサイトは、3 年間の稼動中一度も情報セキュリティの問題はなかったうえに、さらに今回は新たに、クレジットカード情報を持たない仕様を採用した。すでに十分な対策のはずだが、シス管からお墨付きを貰えば常務への説明が容易になる。そう自分なりに考えた押尾は、自席に戻ると、シス管の菅課長にメールを書いた。「ブランドサイトのセキュリティ仕様を送るので、ご一読いただけないか。専門家のご意見を聴かせて欲しい。」

（総務部 システム管理課）

シス管は、菅課長以下 7 名の小さなチームである。1,000 名を越える従業員が使う CIT の安定稼動と、新規システムの立上げを同時に進めることは容易ではない。システム開発・改修などの業務は都度、外部のシステム構築業者に発注しているが、それでも内部の業務負荷は高い。いまも、営業職向けのモバイルタブレットの運用開始を間近に控え、繁忙感が強い。

業者との打合せから戻った菅課長は、EC 推 押尾課長の依頼メールに気づいた。EC 推とは所管の役員が違うこともあり、これまで業務上の繋がりはない。EC 推のブランドサイトは、シス管が管理運営している IT 基盤とは独立に、EC 推独自に外部で調達する IT 基盤上に構築されるらしい。X 社ではこれまで、IT は主に業務効率化のツールとして使われてきており、シス管はこうした位置づけの CIT を所管する部署だと認識されている。そのため、IT の事業活用が検討される場に、シス管が呼ばれることはないのだろう。

[§§§§] Corporate IT

[*****] Business IT

しかし菅課長は、シス管がもっと事業そのものに貢献できればと、以前から残念に思ってきた。いまはシス管全体が忙しく、この件を担当させられる課員はいない。しかしシス管が事業に貢献できるめったにない機会ではあるし、依頼内容も助言がほしいという程度だ。機会を逃すのは惜しい。そう考えた菅課長は、自分で対応することにした。

メールに添付されていた仕様書を開きセキュリティの箇所を斜め読みすると、そこには標準的な項目が一通り並んでいる。

(1) F/W、IPS の導入
(2) SQL インジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリ等への対策として、実装上の脆弱性対策
(3) 納品時のセキュリティ関連検査
(4) トークン方式によるクレジットカード情報の非保持化

(4)では、最近の EC サイトセキュリティのトピックスも押えているし、大きな違和感はない。一見した範囲でどう考慮されているのかはっきりしないのは、サイト運用開始後の脆弱性対策ぐらいである。

菅は返信に、できるだけ協力する、と書いた。また、運用開始後の脆弱性対策をどう考えるか、修正プログラム（パッチ）対応の資金的な準備や WAF 導入を検討しては、とのコメントを加えた。

（事業予算の制約）

3 日後、菅課長と押尾課長は初めて打合せを行った。押尾は事前に、修正プログラムの適用と WAF の導入について、Web サイト構築業者に相談したようだった。シス管 菅課長と EC 推 押尾課長の会話は、以下の通りである。

押尾「運用開始後に公表される新たな脆弱性への対策は盛込んでいなかった。サイト立上げ時点で既知の脆弱性は、Web サイト構築業者に対策をさせたうえで納品させるし、納品時の脆弱性検査も行う。万一、新たな脆弱性が公表された場合の対策までも、運用開始の時点で盛込んでおかなければならないものか。」

菅「現行の仕様に、既知の脆弱性を潰すことと脆弱性検査を盛込んでいるのはよいと思う。これで、運用開始の時点では脆弱性に関するリスクは抑制できている。しかし、新しい脆弱性がいつ公表され、修正プログラムが提供されるかは分からない。今回のブランドサイトが該当する脆弱性は、運用開始当日にも公表されるかもしれない。」

押尾「できれば対策を追加したいが、すでに役員会で決まった予算には盛り込んでなかったので、あまり余裕がない。業者に WAF について聞いてみたら、導入コストは 100 万程度とのことだから何とかなりそうだ。だが、うちのコンテンツに合せて初期設定を頼むには、別途業者からサービスを買わなければならないそうだ。もっと困るのは、WAF 運用の要員を内部で抱えなければならないことだ。EC 推には技術者はいないから、セキュリティ技術者を派遣してもらうか中途採用することになる。といっても、固定費が増えるので、それは簡単でない。

運用開始後すぐに新しい脆弱性が公表される可能性は、そんなに大きくないのではないのか。しかも、

その新しい脆弱性を突いて攻撃するときに、うちのような中堅アパレル企業のサイトを狙うだろうか、被害を受けるものなのだろうか、実感としてわからない。とりあえず今の対策でサイトを運用開始し、来年度以降、追加予算を考えるという方向で進めたいのだが。」

菅「脆弱性対策は Web セキュリティの基本。正確ではないかもしれないが、たとえば struts2 の脆弱性は 3、4 ヶ月の間に何件も発見されていたと思う。struts2 の件で、実際の被害がたくさん報告されている。」

押尾「私は前職でも EC サイトの運営に関わっていたが、担当していた間、一度も被害に合わなかった。struts のことはもちろん聞いているが....。もう一つの対策、修正プログラム適用のことだが...業者は、費用見積もりが難しいと言っている。適用後の回帰テストで問題が見つかるなどして、改修が必要になるかもしれないが、その費用は改修の内容で大きく変わる。予め見積もりはできない、と。
また、仮に費用を用意できたとしても、業者側は、サイトを再構築し開発要員をあてねばならないため、すぐに対応できるとは限らないそうだ。

いくら掛るか見積もれない上に発注も難しいとなると、ただでさえ予算が厳しいところを、無理して枠を押さえておくというのは、説明が難しい。
繰り返して申し訳ないが、これから公表されるかもしれない脆弱性まで、運用開始までに、完璧に対策しなければならないものか。」

菅「Web サイトの大きなインシデントをみると、せっかく修正プログラムが提供されていたのに適用しておらず、残念にも攻撃を受けて被害が甚大、というケースが多い。」

押尾「...可能性の話だけでは、上に対して説明が難しい。
教えてもらった二つの脆弱性対策が、EC 事業に対しどんな意味があるのかを、現実的・定量的に説明してもらえないだろうか。」

菅は、セキュリティリスクの怖さが、押尾には腹落ちしてないのではないかと感じた。脆弱性の放置が原因で受けるインパクトは、X 社が長年築き上げてきたブランド価値を、大きく損ねるかもしれない。セキュリティリスクが経営リスクであることを分かってもらわない限りは、何を言っても伝わらないだろう。菅は、押尾の言う現実的で定量的な説明ができないか、考えてみると答えて席を立った。
そうは言ったものの、ブランドサイトはシス管には関係がなく助言を求められただけだと思うと、菅は引っ掛かりを感じてもいた。リスクを正しく認識してもらう努力を、こちらがどこまでしなければならないのだろう。EC 推が IT を活用した事業をやるのだから、自分で、事業企画の一部としてセキュリティを考えるべきなのではないか。

2.3. 実施した活動

（定量的な説明、現実の例）

脆弱性対策が、EC 事業の運営上必要であることを、どう説明すればいいだろうか。菅は社外の情報セ

キュリティ教育で聞いた話を思い浮かべ、できるだけ定量化してみることにした。ブランドサイトで起きうる被害規模を想定すること。それと攻撃頻度の推定だ。昼間はシス管の業務で手一杯だった菅は、残業時間を費やして、何日か検討してみることにした。

（1）被害規模の想定

時間を掛けてデータを探したところ、EC サイトがサイバー攻撃を受けた場合、実害に繋がった割合は 7 割を超えるという調査を見つけた。また実害があった場合の 3 割が 1,000 万円以上の被害を被っている。さらに、調査対象が卸小売業の場合、従業員数が 1,000 名以上の規模の企業では被害総額が 1 億円～5 億円に上る割合が 6 割を超えていることも分かった。

被害は、実態把握のための調査や EC サイトの対策強化にかかる直接費用の他、顧客へのお詫びに要する費用や、原因特定・対策措置が終わるまでサイトを停止すること等による機会損失、さらに信用を失うことによる顧客離れと売上げダウンなど様々な項目に及ぶため、年々拡大する傾向にあるらしい。

（2）攻撃を受ける可能性

では、脆弱性を突く攻撃を受ける可能性は、どのくらいだろうか。さきほどの調査結果によると、OS やミドルウェア等の脆弱性を突く攻撃は、1 割～2 割程度の EC サイトで検出されているらしい。しかし菅はこの数字だけに頼るのではなく、自社の場合で、攻撃頻度を出せないか考えた。

シス管では、X 社のオフィシャルサイトを運営している。社外向け情報 PR のための Web サイトで機能は多くない。このサイトは既知の脆弱性を突く攻撃をどのくらい受けているのだろうか。オフィシャルサイトの管理を担当している課員に、ここ 2～3 年程度に見つかった著名な脆弱性に関して、その頻度を調べるように指示を出した。担当者の忙しさを考えると、あまり時間を掛けさせることはできない。「2～3 日くらいで、F/W や IPS などのログを分析してくれないか。できる範囲でよいから。」

4 日後、菅の手元に集計データが出てきた。ここ 2 年の間に公表された脆弱性 10 件のうち約半数に関して、攻撃が試みられた痕跡がログに残っていた。オフィシャルサイトは、修正プログラムの適用を含め、シス管自らセキュリティ対策を施している。オフィシャルサイトにはユーザー情報等の保護資産はなく、幸いこれらの攻撃で実害は起きていない。

ここまでのデータをまとめると次のようになる。

- X 社のサイトが、ひとつの脆弱性について攻撃を受ける確率　0.5
- 攻撃を受けた際、実害に繋がる確率 0.7
- 卸小売業の場合、実害が 1 億円～5 億円になる確率 0.6

これらから、脆弱性を放置していると、脆弱性 10 件につき 2 件の割合で、1 億円～5 億円の被害が出る可能性があると説明することにした。

（3）ワーストケース

これまでの検討で定量的なデータは揃えたが、セキュリティインシデントが経営リスクに繋がる説明としては、まだ説得力が弱いと考えた

そこで菅は、脆弱性を突く攻撃が、企業経営に大きな影響を与えた事例の紹介を、報告に添えたいと考

えた。ここ数年間の有名な事例をまとめて説明したいが今回は時間がない。ごく最近報道された海外の事例を説明することにした。

- 対象の企業：海外の消費者信用情報会社
- 被害：18 万人分の個人情報、21 万件のクレジットカード番号の漏洩
- 原因：struts2 のある脆弱性の放置（修正プログラムの非適用）等
- 経営へのインパクト
  - 株価が最大で約 4 割下落し、時価総額にして数十億ドルが消失
  - CIO に次いで CEO が辞任
  - 複数の集団訴訟に直面

経営リスクであることを説明するために、データ集めに思いのほか時間がかかってしまった。日常からこうしたデータを集めておけば、もっと慌てずに済んだかもしれない。菅はそう考えながら、押尾への報告をまとめることにした。

（経営層への説明、前編）

菅の資料を受け取った押尾から、返信が届いた。

- 定量的な説明は分かりやすかった。とくに事業計画に対する計数的な影響が分かったのがありがたかった。早速、室井田室長に送ったところ、説明して欲しいとのこと。ついては、セキュリティの詳細説明は、補助してもらえないか。
- とくに、脆弱性対策になぜ 2 つの対策（修正プログラム適用と WAF 導入）が必要か上手く説明できない。
- サイト構築を相談している業者に聞いて、大体の費用感覚は掴んだ。説明は用意しておく。

とのことだった。修正プログラムと WAF の両方の対策が必要となることを、押尾に説明させるのは難しいだろう。そう考えた菅は、室井田室長への説明に同席すると回答した。

2 日後、菅は押尾と一緒に、室井田室長の部屋にいた。菅が作った脆弱性対策の説明資料を使い、押尾は（1）被害規模の想定、（2）攻撃を受ける可能性、（3）他社で起きたワーストケースについて、一通り口頭で説明した。その間、室井田は黙って聴いていたが、説明が終わると押尾に向かって、質問を始めた。

室井田「その脆弱性？対策をやるとして、予算面はどうなるのか。」

押尾「WAF には、ソフトウェア購入の初期費用と運営を頼む派遣技術者の人件費が必要。また修正プログラムのための予算確保を合わせると、初年度は現行予算の二割増しになる。」

室井田「サイト構築と初年度の運営費の予算は、この間承認がとれたばかりだ。増額は申請できない。」

押尾「まず、EC サイトで扱うブランドは、主要ブランド 7 つすべてと考えているが、初年度はこれを 4 つに絞ればコンテンツ作成分の費用で賄える。
もしくは、サイトのバックヤードで動かすデータ分析機能と MA 機能に関して、初年度、業者から分析

支援のオプションサービスを買う予定にしていたが、これをやめれば賄える。」

室井田「扱うブランドを減らすことなどできるのか。外されるブランドの営業部は納得するのか。ブランド数を減らして、事業計画への影響はないのか。目標にしている２年目の単年度黒字化は達成できるのか。」

押尾「ブランド数が 4/7 になれば、営業利益に影響がでることは避けられない。次年度から当初計画通り７ブランドにするとしても、2 年目の単黒達成は難しい。」

室井田の表情が硬くなった。
「それでは計画承認の前提が崩れてしまう。話にならない。二つ目の案もそうだ。データ分析の機能だけ実現して、分析支援のサービスを買わないで、最初から EC 推だけでマーケティング分析できる自信はあるのか。…EC 推の方針はどうなる。」

　このやり取りを聴いて居心地の悪さを感じた菅は、こういう話は EC 推の中でやってくれればいいのに、EC 推の計数計画は私にはどうしようもない、と思った。

室井田「そもそも、その脆弱性対策が、当初予算案に盛込まれていないのはどういうことだ。」

　押尾が返答に窮していると、室井田は、今度は菅の方に向き直って尋ねた。

（経営層への説明、後編）
室井田「脆弱性対策をやらないと、2 割の確率で 1 億～5 億のロスとか、株価が下落するとか、実感が沸かない。尋ねておいて悪いが、話が大げさなんではないのか。アパレルの競合他社の EC サイトで、個人情報の漏えいなど聞いたこともない。ハッカーは中堅アパレルの EC サイトなんかに興味ないだろう。うちのようなファッションサイトが本当に狙われるのか。」

菅「確かに私も、アパレルの EC サイトがやられた事例は把握していない。しかし、大手の EC サイトはセキュリティ対策が充実してきたことから、攻撃者の狙いはむしろ、対策が手薄な中堅・中小に移ってきていると聞く。うちのオフィシャルサイトでも、実際に脆弱性を突く攻撃の痕跡が見つかった。…具体的な他社の事例は、今すぐ示すことはできないが、少し時間があれば事例をまとめられる。」

室井田「…押尾課長の当初の仕様にも、脆弱性対策というセキュリティの項目があった。さらに二つも脆弱性対策を加えなければいけないというのは、どういうことだ。」

菅は、ここで対策の違いをしっかり分かってもらわなければと思って、一気に説明を始めた。
菅「当初仕様には、既知の脆弱性に対する対策が盛込まれていたが、今後新たな脆弱性が公表される可能性への対策も必要だ。ベンダーがパッチを提供したらできるだけ早く当てるのが筋だが、すぐに当てられないことも多いので暫定対策として WAF が欲しい。一方、ではパッチは当てずに WAF だけがあればいいかというと、攻撃手法が公知になってないものには効果がないし、偽陽性とか偽陰性の問題もある。

恒久対策としてのパッチ当ては省けない。…本当は WAF だけじゃなく、仮想パッチ機能付きの IPS も…」

室井田「…ちょっと待て。キチ？パチ？コウチ？... 分からないよ。ギヨウセイとか IPS とか、それはなんだ。」

菅「... IPS は侵入防止システムのことだ。Web サイトのセキュリティ対策には何種類かあるが、それぞれ対処できることが違う。どう違うかというと…」。菅は、室井田にもわかるように説明しようと、ホワイトボードの上に F/W、IPS、WAF がそれぞれ対処できる攻撃等を図に描いた（図２）。「…このように、3 つの対策は役割が異なるわけで、確かに一部重複はしているが、基本的には全部あった方が...」

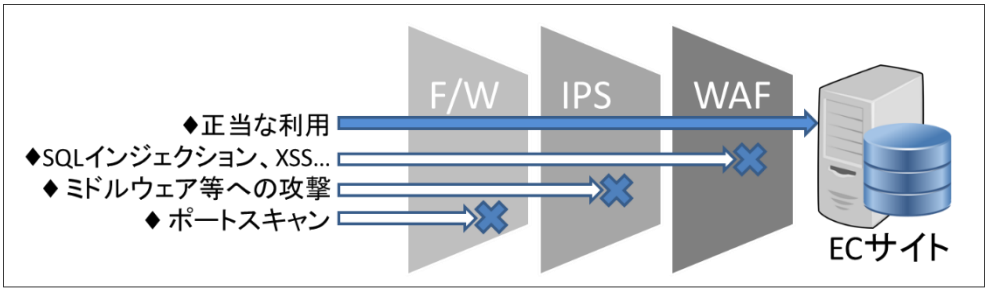

図２　Web サイトのセキュリティ対策の違い

室井田「…そういうことを聞いているんじゃない。セキュリティの細かい話はいいんだ。」むすっとした表情の室井田は、菅の話をさえぎった。「いまは事業の話をしているんだ。２年単黒をどう達成するか、コストが高すぎると言っているのだ。もっと安く対策できないのか。なんでも自動にするのではなく人が何かするとか。他にやりようはないのか。」

菅は、何をどう説明すればいいのか分からず、口を閉じた。

室井田「うちのようなアパレルだって狙われる対象となり危ない、というのはそうかもしれない。ハッカーの攻撃に対抗するため、あれがいる、これもいるというのは正しいのかもしれない。だが私は技術者じゃないんだ。そんな説明をされても分からない。
それに脆弱性の対策ばかりだが、ほかは大丈夫なのか？標的型メール攻撃とやらの対策はどうした。標的型攻撃の方は、よく新聞やテレビで聞く。ウイルスに感染しない入り口の対策は要らないのか。どうも今の話は、セキュリティの細かい話を聞かされている気がする。バランスが悪いんじゃないか。どうなんだ。」

何をどういえばよいか途方にくれて、菅が困っていると、押尾が後を引き取って言った。

押尾「話を整理して、出直したい。再度検討して、もう一度ご相談に上がる。」押尾はそう言って、室井田への説明を打ち切った。

二人が室井田の部屋を出たところで、押尾が言った。

「来てくれて助かった。だが申し訳ないが、室長に技術的なアプローチで説明してもだめだと思う。事業計画への影響に翻訳して説明する必要がある。
EC 推でその作業はやる。情報をもらえないか。中堅・中小が狙われた事例をまとめたものが欲しい。それと、一番大事なのは、もっと経済的な脆弱性対策はないのか、ということ。もうひとつ、標的型メールの話をどうするか、この 3 点の情報をもらえると助かる。
脆弱性対策を、どのくらいコストを掛けてやると、どこまでリスクが下がるのか、そのコストをひねり出すために EC 事業でなにをあきらめるのか、それによって計数計画がどう変わるのか。それを考えなければならない。予算が十分にあれば、脆弱性対策も当初事業計画の達成も両立できるのだろうが、今回は、室井田室長に、どうリスクと事業のバランスを判断してもらうかという話になりそうだ 2 年単黒をキープするための計数計画を EC 推で考える。」

（宿題）

自席に戻りながら菅は、室井田、押尾とのやり取りを思い返して、すっきりしない感覚を拭えなかった。そもそも、新たな脆弱性への対策に必要な予算を計上していなかった EC 推の問題が発端だ。菅は、セキュリティに必要な対策はハッキリしていると思った。それを説明して欲しいというなら、それはしよう。EC 推の計数計画への影響に、本来、BIT に無関係なシス管が、どこまで付き合わなければならないのだろうか。

席に着いた菅は、早く収束させたいと考え、下記の作業を課員に指示した。

(1) X 社と同様の小売業・同規模の企業のインシデント例の情報をまとめる。
(2) よりコストの低い脆弱性対策を検討。
(3) 標的型攻撃メール対策の説明を作成。

翌日、菅の下に検討結果が集まった。対応してくれた課員には負担をかけてしまったようだ。

(1) について

公開されている情報をもとに、ここ 2,3 年のインシデント 20 件のリストを作成した。

- 有名玩具メーカーのオンラインショップから、個人情報（氏名、郵便番号、電話番号など）が 10 万件余りが漏えい
- 有名食品メーカーの EC サイトが不正アクセスされ、個人情報（氏名、住所、電話番号、クレジットカード情報）が 5 万件余り漏えい
- 有名雑誌とコラボレートした通販サイトが不正アクセスを受け、個人情報（氏名、住所、電話番号）が 2 万人分漏えい

など。

セキュリティインシデントの情報を集めて分かったことだが、ほとんどの場合、根本原因の詳細や被害額などの情報は公表されていない。他社でのインシデントの事業への影響を、経営層に定量的に説明することは難しい。

(2) について

WAF の代わりに、最近ポピュラーになり始めているクラウド WAF を検討し、情報をまとめた。初期導入費用はオンプレミスの WAF 導入よりかなり手ごろ。また、ブラックリストの更新等の作業はクラウド側で行われるので自社に運用技術者をおく必要はない。年間使用料は、X 社ブランドサイ

トに必要なスペックで、運用技術者を雇う場合の 1/3～1/2 程。オンプレミスの WAF に比べてコスト面で有利である。

(3) について

標的型攻撃メール対策はブランドサイトの問題ではなく、全社で対応しなければならない問題である。すでにシス管では、模擬攻撃訓練を全社で行っており、十分とはいえないまでも、全く対策していないわけではない。室井田は、訓練が標的型攻撃メール対策であることを認識していないようにみえるため、説明する資料を作成した。また、懸案だった対策ソリューション導入の検討を急ぐことにした。

(1)～(3)の情報を資料にまとめ、押尾に送ることにした。

2.4. 活動の結果と振返り

（結果）

翌週、EC 推の押尾課長から連絡があった。先日菅が送った情報を元に、脆弱性対策への投資を計数計画に反映し、室井田室長の OK を得たとのこと。その概要は、

- クラウド WAF を採用。
- その費用は、初年度にブランドサイトに載せるブランドを 5 つに絞ることで捻出。
- 修正プログラム適用のための予算枠確保は、初年度は行わない。

外されることになったブランドの営業部との間で、調整は難航したとのこと。各ブランドで、コンテンツの検討・制作が進んでしまっていたこともあり、外れるブランドの営業部の説得は難しかったようだ。最後は、室井田室長がリスクと EC 事業とのバランスをとった判断だと言って、社内を調整したという。一方で、目標の 2 年目単黒達成の計数計画は変えなかったそうだ。

（振返り）

菅は、不十分ながらも、ブランドサイトに脆弱性対策が施されたことにホッとした。だが一方で、大きな課題が残ったと思った。

それは、まず直接的には、修正プログラム適用の予算が確保されていないことだ。他社で起きた脆弱性関連のインシデントは、修正プログラムが発行されているにも係らず、長期にわたって適用されずに放置されていたサイトで起きている。今回、ブランドサイトでも予算確保が見送られた。このまま議論が立ち消えになってしまうおそれもある。危険な脆弱性が見つかっても、すぐには費用が用意できないという理由で放置されたまま、半年くらい経ってしまわないだろうか。WAF がカバーできる脆弱性だけならばよいが、そこはリスクが残る。

二番目は、セキュリティ投資の事業的な意味合いの説明を、誰が検討するかと言う問題だ。BIT のセキュリティは担当事業部門で考えるべき事項のはずだ。シス管には、個別事業の内容は分からないから事業上の意味合いを考えることはできない。今回、不用意に EC 推の問題に絡んでしまったが、シス管にはシス管の計画業務があり、今後も常に支援できるとは限らない。

一方で、事業部門にはセキュリティに詳しい者はおろか IT 技術者もいない状況で、セキュリティ対策を考えろというのは土台無理な話だとも思う。こう考えると、BIT のセキュリティは誰が担当するのが適切かと言う問題は、簡単には解けそうもない。

…経営層に、セキュリティ投資の意味合いを説明するには、社外のデータを使ってでも客観的・定量的なロジックを組み立てることがいいらしいという事が分かったのは、今回巻き込まれたことの収穫だったが。

三番目は、事業に必要なセキュリティの検討は、事業企画に織り交ぜてやるべきだということ。今回のように、事業予算が固まってしまったあとで必要なセキュリティを考えるのでは、必要な費用の工面は難しい。事業企画の段階で、とくに予算検討の段階で自然にセキュリティを考えるようにするには、なにをどうすればいいのだろうか。規程にでも明記するのか。それは、誰にどう働きかければよいのか。

四番目は、世の中のセキュリティインシデントや対策の情報に関して、経営層に日ごろから慣れておいてもらわないと説明が大変だという事。当社のように、経営層に IT やセキュリティへの理解を期待できない業種の場合は、なおさらだ。当社が受けている攻撃の情報や、セキュリティ対策の状況に関する情報を、日ごろから経営層にインプットしておくことで、インシデント発生時の初動や、セキュリティ対策への投資の意思決定が容易になるのではないか。とはいえ、それはどうやればいいのだろうか。

シス管のミッションを大きく超えるこうした課題に、この後どう取組んでいけばいいのか、菅は途方にくれるような気分を覚えた。シス管を所管するのは総務担当の執行役だ。幸い、総務部はさまざまなリスク管理を担当している。まずは、総務部長への課題提起から、取組んでみようと菅は考えた。

（以上）

このページは白紙です。