

■ Sec03-02 経営者向けサイバーセキュリティ経営の体系的啓発資料

■ 【2018年7月6日】

日 サイバーセキュリティは経営問題

- 【サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】】
- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要
- セキュリティ投資は必要不可欠かつ経営者としての責務である。

☐ ☆ 経営者が認識すべき3原則

- 【サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】】

☐ (1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

- 【経営者自らがリーダーシップを発揮して適切な経営資源の配分を行う】
- □ ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを活用する機会は増加傾向にあり、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。
- □ また、サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
- □ このため、サイバーセキュリティリスクを多様な経営リスクの中での一つとして位置づけ、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）を任命するとともに、経営者自らがリーダーシップを発揮して適切な経営資源の配分を行うことが必要である。

☐ (2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

- 【自社のみならず、サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底する】
- □ サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じうる。
- □ このため、自社のみならず、サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底することが必要である。

☐ (3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

- 【平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行う】
- □ 万一サイバー攻撃による被害が発生した場合、関係者と、平時から適切なセキュリティリスクのコミュニケーションができていれば、関係者の不信感の高まりを抑えることができる。
- □ このため、平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である。

目次 ☆サイバーセキュリティ経営の重要10項目

- 【サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】】

- 経営者は、CISO等に対して、以下の10項目を指示し、着実に実施させるとともに、実施内容についてCISO等から定期的に報告を受けることが必要である。自組織での対応が困難な項目については、外部委託によって実施することも検討する。

目 3. 1. サイバーセキュリティリスクの管理体制構築

目 指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

- サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる。

☐ 対策を怠った場合のシナリオ

- ・経営者がサイバーセキュリティリスクへの対応を策定し、宣言していない場合、サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。
 - ・トップの宣言により、ステークホルダー（株主、顧客、取引先など）の信頼性を高め、ブランド価値向上につながるが、宣言がない場合は、企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。
- 指示2 サイバーセキュリティリスク管理体制の構築
- サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。
 - その際、組織内のその他のリスク管理体制とも整合を取らせる。
- 対策を怠った場合のシナリオ
- ・サイバーセキュリティリスクの管理体制を整備していない場合、組織としてサイバーセキュリティリスクの把握が出来ない。
 - ・組織内におけるその他のリスク管理体制との整合を取らないと、組織全体としてのリスク管理の方針と不整合が生じる恐れがある。
- 指示3 サイバーセキュリティ対策のための資源（予算、人材等）確保
- サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。
- 対策を怠った場合のシナリオ
- ・適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダへの委託が困難となる恐れがある。
 - ・適切な処遇の維持、改善ができないと、有能なサイバーセキュリティ人材を自社にとどめておくことができない。
- 3. 2. サイバーセキュリティリスクの特定と対策の実装
- 指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- 経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。
 - その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。
- 対策を怠った場合のシナリオ
- ・企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。
 - ・受容できないリスクが残る場合、想定外の損失を被る恐れがある
- 指示5 サイバーセキュリティリスクに対応するための仕組みの構築
- サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。
- 対策を怠った場合のシナリオ
- ・サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃が発生した場合の被害が拡大する可能性がある。
 - ・技術的な取組を行っていたとしても、攻撃の検知・分析とそれに基づく対応ができるよう、適切な運用が行われていない場合は、サイバー攻撃の状況を正確に把握することができず、攻撃者に組織内の重要情報を窃取されるなどの、致命的な被害に発展する恐れがある。
- 指示6 サイバーセキュリティ対策におけるPDCAサイクルの実施
- 計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる。
 - その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。
 - また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

□ 対策を怠った場合のシナリオ

- ・PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、立てた計画が確実に実行されない恐れがある。
- ・最新の脅威への対応ができていないかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、サイバーセキュリティを巡る環境変化に対応できず、新たに発生した脅威に対応できない恐れがある。
- ・適切な開示を行わなかった場合、社会的責任の観点から、事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、インシデント発生時に企業価値が大きく低下する恐れがある。

□ 3. 3. インシデント発生に備えた体制構築 3

□ 指示7 インシデント発生時の緊急対応体制の整備

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- また、インシデント発生時の対応について、適宜実践的な演習を実施させる。

□ 対策を怠った場合のシナリオ

- ・緊急時の対応体制を整備していないと、原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。
- ・速やかな情報開示が行われない場合、顧客や取引先等にも被害が及ぶ恐れがあり、損害賠償請求など責任を問われる場合がある。
- ・法的な取り決めがあり、所管官庁等への報告が義務づけられている場合、速やかな通知がないことにより、罰則等を受ける場合がある。
- ・演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない。

□ 指示8 インシデントによる被害に備えた復旧体制の整備


- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- BCPとの連携等、組織全体として整合のとれた復旧目標計画を定めさせる。
- また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

□ 対策を怠った場合のシナリオ

- ・重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。
- ・演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない。

□ 3. 4. サプライチェーンセキュリティ対策の推進

□ 指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

- 監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。
- システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。
- **中小企業自らがセキュリティ対策に取り組むことを宣言する制度** 

□ 対策を怠った場合のシナリオ

- ・系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されることもある。その結果、他社の2次被害を誘発し、加害者となる恐れもある。また、緊急時の原因特定などの際に、これらの企業からの協力を得られないことにより事業継続に支障が生ずる。

- ・システム管理などの委託業務において、自組織で対応する部分と委託する部分とが明確となり、対策漏れが生じる恐れがある。

[Expand](#) - [Collapse](#)

□ 3. 5. ステークホルダーを含めた関係者とのコミュニケーションの推進

□ 指示 10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び 提供

- 社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。
- また、入手した情報を有効活用するための環境整備をさせる。

□ 対策を怠った場合のシナリオ

- ・情報共有活動への参加により、解析した攻撃手法などの情報を用いて、他社における同様の被害を未然に防止することができるが、情報共有ができていないと、社会全体において常に新たな攻撃として対応することとなり、企業における対応コストが低減しない。

□ ★ CISO等セキュリティ推進者の経営・事業に関する7つの役割プラクティス

□ CISO等セキュリティ推進者の経営・事業に関する役割調査【2018年6月28日IPA】

- -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IPA】

□ 概要

- 「サイバーセキュリティ経営ガイドライン」（経済産業省とIPAが共同策定）(*1)には、経営者が認識すべき3原則が掲げられています。その中で、経営層はサイバーセキュリティリスクを認識し、リーダーシップをとって対策を進めることが必要とあります。
- 一方、「サイバーセキュリティ人材育成プログラム」（サイバーセキュリティ戦略本部）(*2)では、経営層自らがサイバーセキュリティ対策を企画・立案し、実務者層を動かすことは困難であるとしています。そのため同プログラムは、経営層を補佐し、経営戦略とサイバーセキュリティに関する業務課題を理解したうえで、様々な役割を持った実務者層を指揮する「橋渡し人材」が必要であるとしています。
- 「CISO等セキュリティ推進者の経営・事業に関する役割調査」では、CISO(*3)およびその補佐役となる橋渡し人材等のセキュリティ推進者が担う役割、とくにセキュリティへの取組みが経営と事業に貢献するようマネジメントする役割（以下、経営・事業に関する役割）について、その実態や期待されている内容を調査するため、文献調査・有識者へのインタビュー調査・アンケート調査を行っています。
- 調査結果に基づいて、CISO等セキュリティ推進者の経営・事業に関する役割7つについて整理し、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プラクティスを、調査報告書の別冊として作成しました。

□ 図 1-2 CISO等の経営・事業的役割の全体像

Expand - Collapse

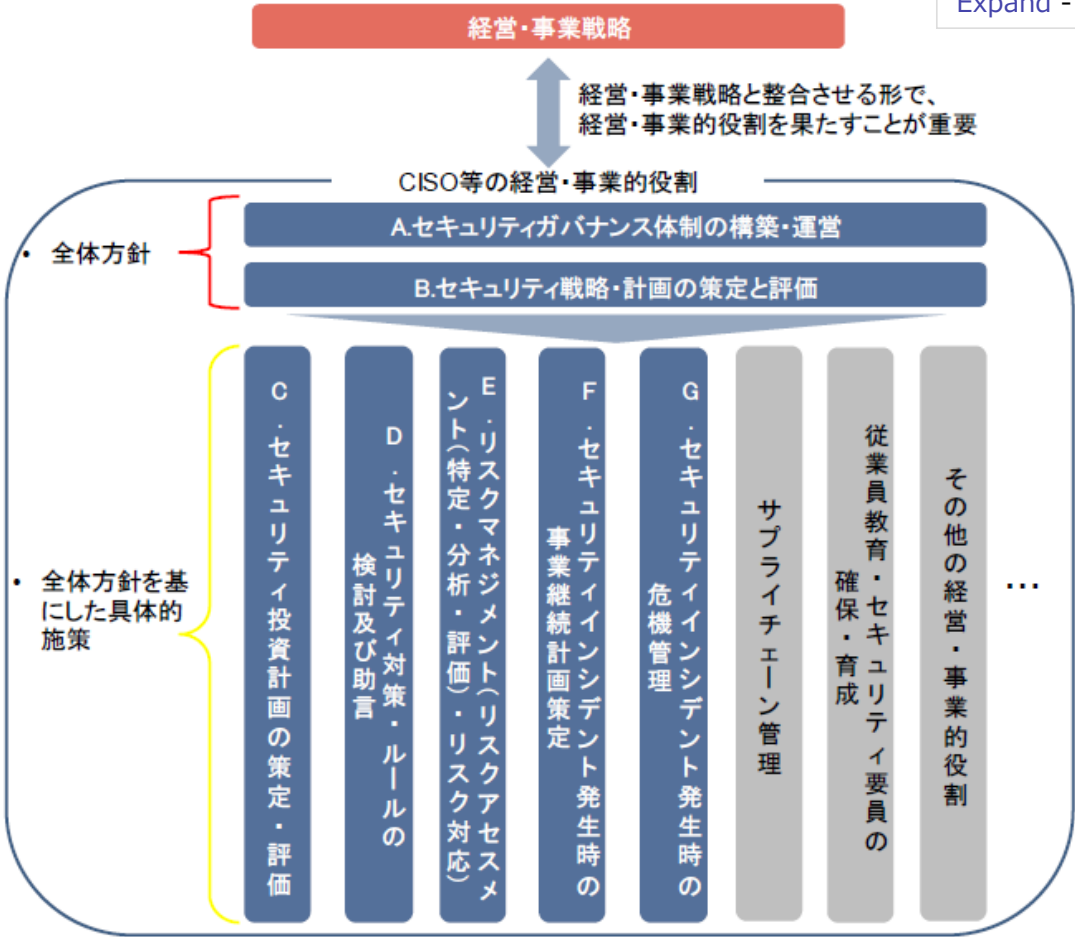


表 1-1 本書で対象とする経営・事業的役割の概要

Expand - Collapse

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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）	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

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を検討し、リスク対応を実施する

Expand - Collapse

- 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

図 1-3 役割間のインプット・アウトプット関係

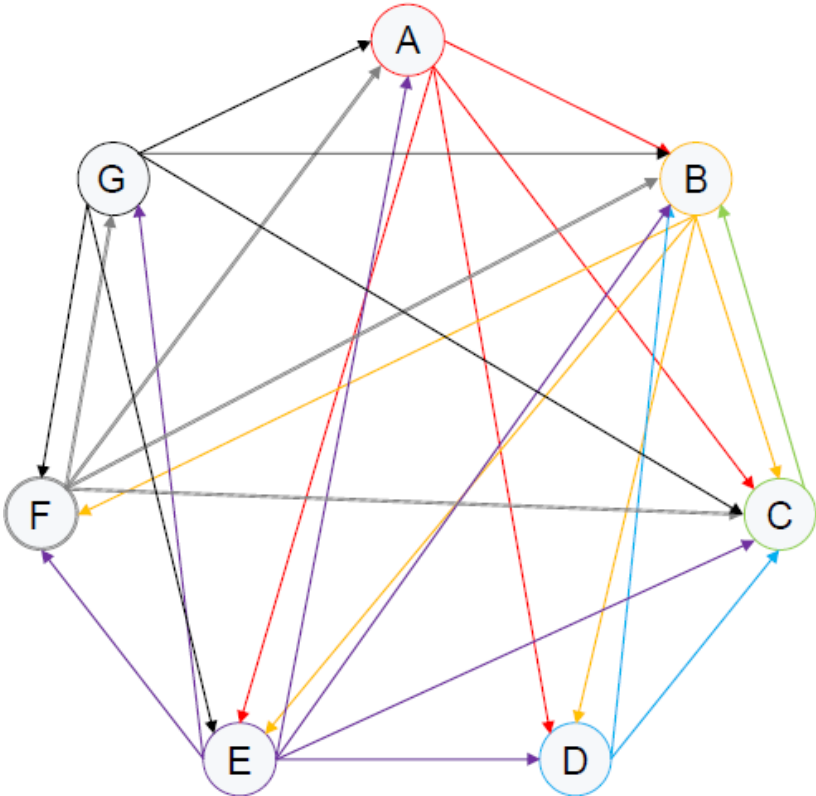


表 1-2 各役割の作業成果物

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

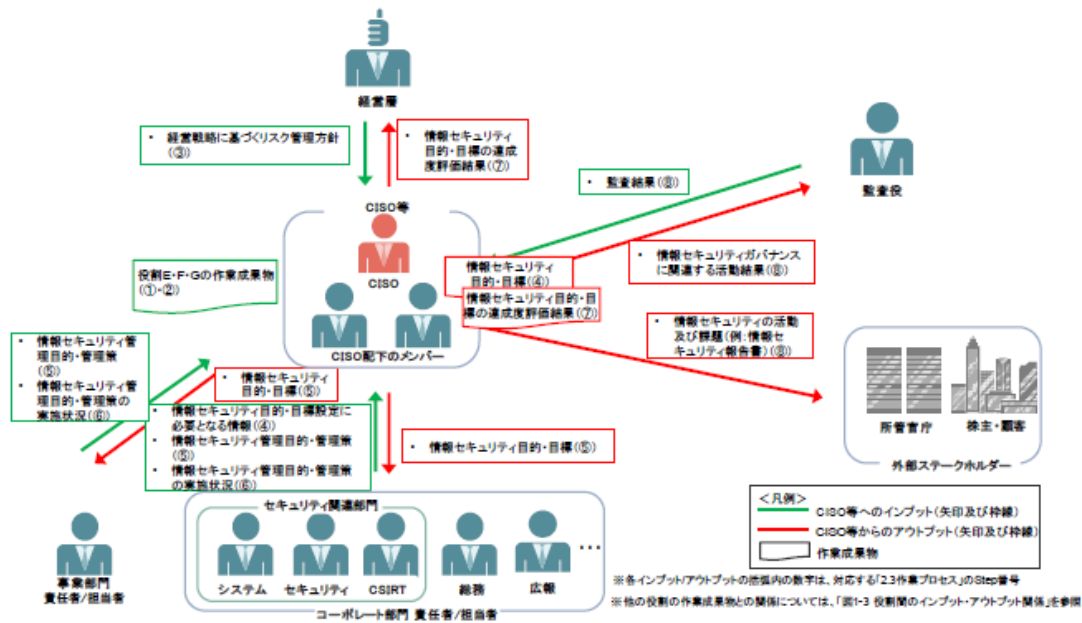
表 1-3 ケース別本書の活用方法

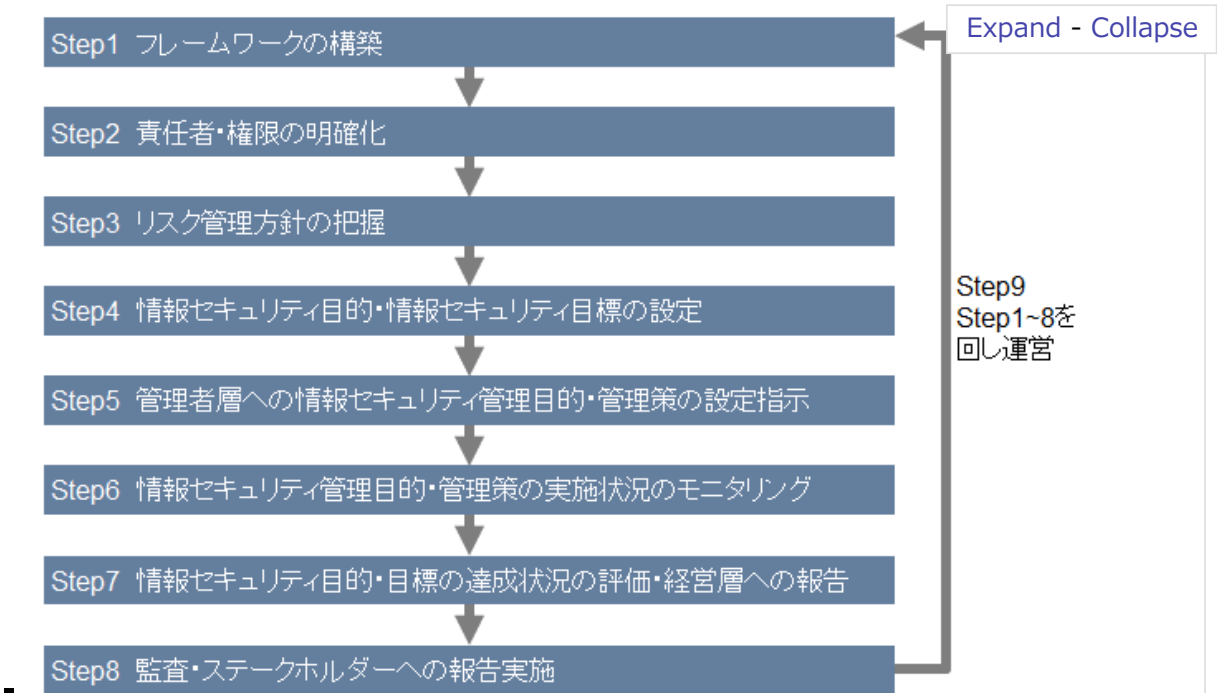
ケース	活用方法
役割 A～G の取組を既に実施している企業	・ 全体方針(役割 A・B)・具体的施策(役割 C～G)の順に確認し、自社の取組で不足している点等を確認する。
役割 A～G の取組の一部を実施している企業	・ 現在実施している役割について確認し、自社の取組で不足している点等を確認する。 ・ その後、全体方針・具体的施策の順で経営・事業的役割を確認し実施する。
役割 A～G の取組を全く実施していない企業	・ 「E.リスクマネジメント(リスクアセスメント(特定・分析・評価)・リスク対応)」から開始し、全体方針・具体的施策の順で実施する。 ・ 社内に知見が蓄積されていないと考えられるため、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。

- 経営・事業的役割の各項目の具体的な作業内容と手順
- 目的・狙い
 - 役割の作業内容
 - 作業プロセス
 - 作業に必要な情報
 - 作業の目標成果
 - 作業で協同・連携する社内外の関係者と」協同・連携の内容

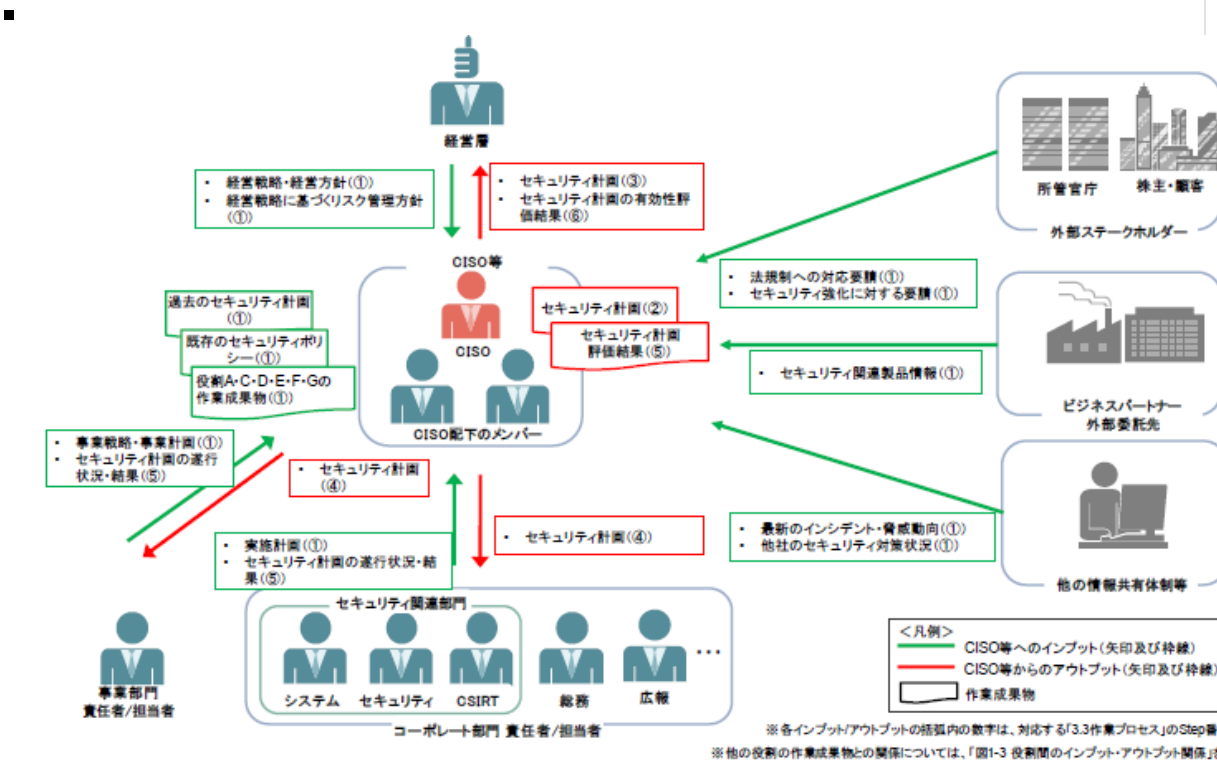
全体方針

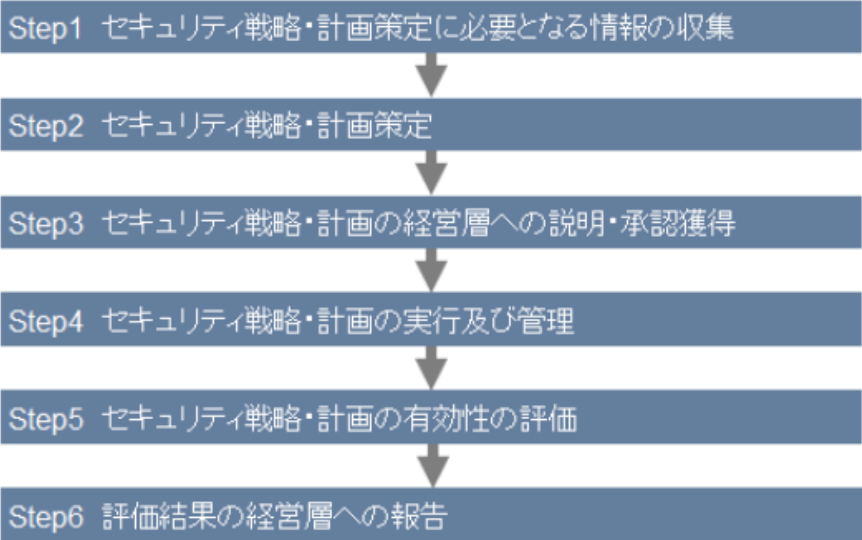
A.セキュリティガバナンス体制の構築・運営



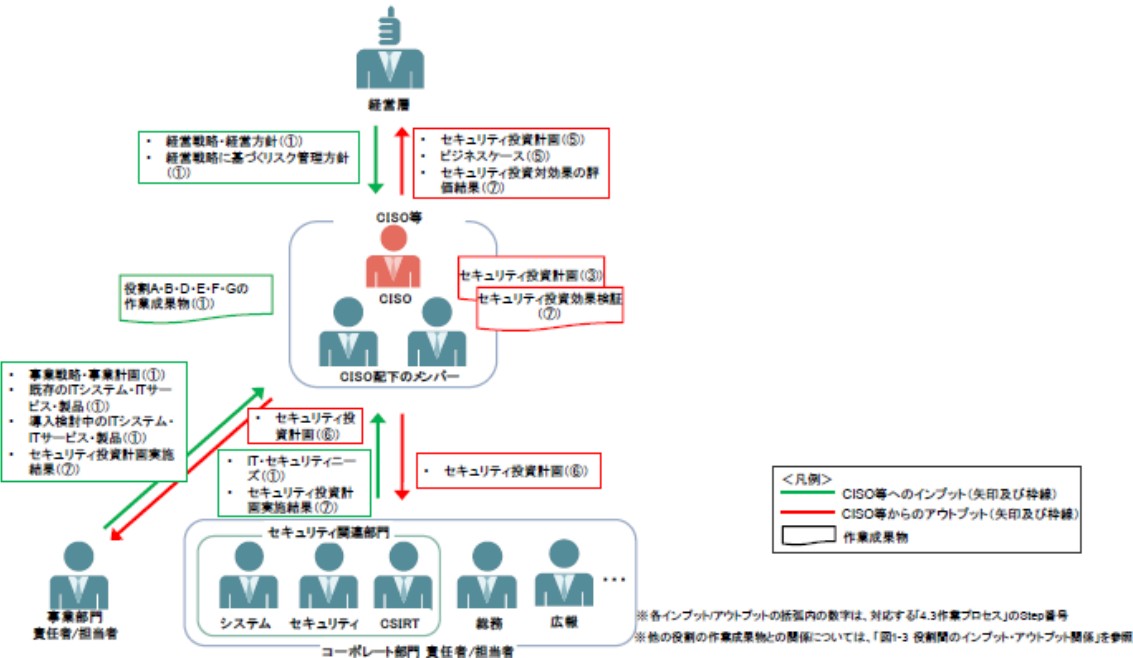


□ B.セキュリティ戦略・計画の策定と評価





- ▢ 具体的施策
- ▢ C.セキュリティ投資計画の策定・評価



Expand - Collapse

Step1 セキュリティ投資計画策定に必要な情報の収集

Step2 課題・リスクの特定及び必要な対策の検討

Step3 セキュリティ投資計画策定

Step4 ビジネスケース策定

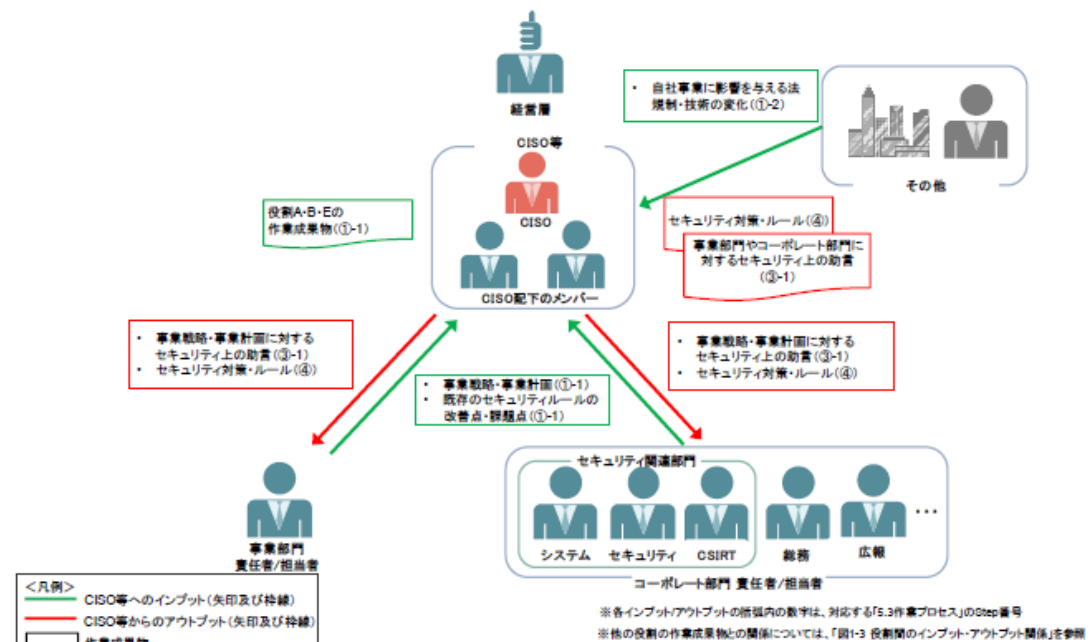
Step5 セキュリティ投資計画・ビジネスケースの経営層への説明

Step6 セキュリティ投資計画の実行及び管理

Step7 セキュリティ投資効果の評価及び改善点の検証

Step8 評価結果の経営層への報告

□ D.セキュリティ対策・ルールを検討及び助言



Step1-1 内部情報の収集

Step1-2 外部情報の収集

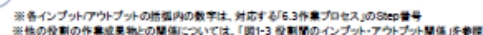
Step2 収集した情報を基にしたセキュリティ上の課題の検討

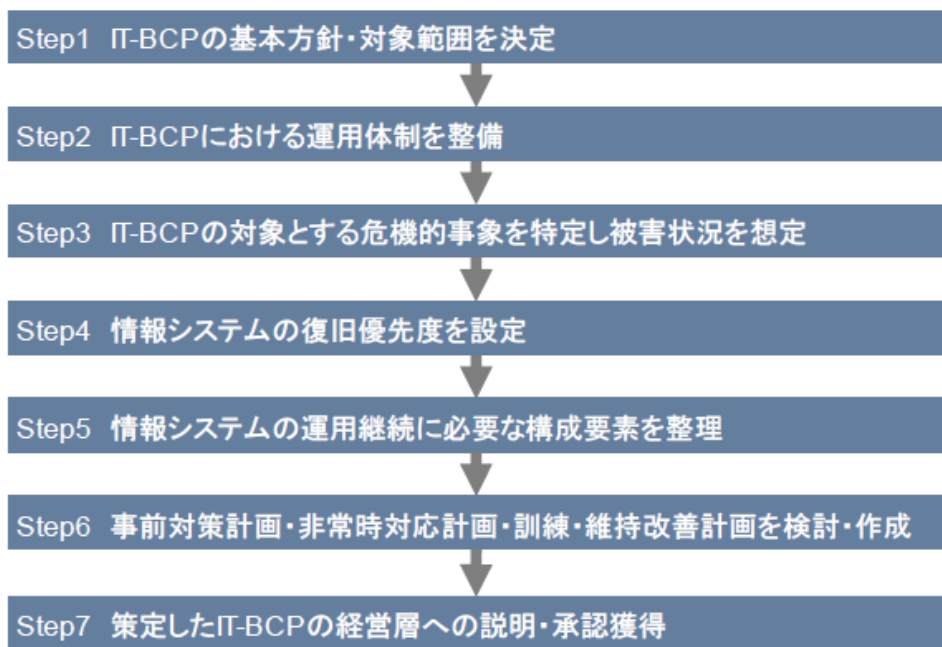
Step3-1 事業部門・コーポレート部門に対するセキュリティ上の助言実施

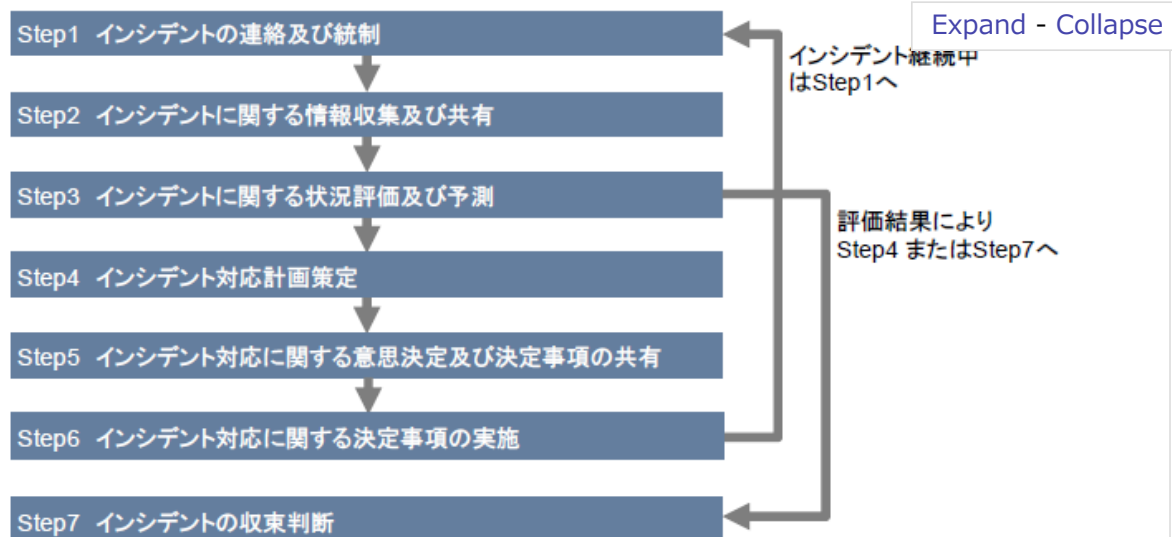
Step3-2 セキュリティ対策・ルールの新規策定または改訂

Step4 セキュリティ対策・ルールを展開し、必要に応じて改善

□ 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）



[illegible]



付録：CISO等の経営・事業に関する役割のストーリー

- 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(A)
- 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(C)