サイバーセキュリティ経営ガイドライン
解説書

Ver.1.0

2016年12月

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

目 次

0 はじめに

近年、組織を狙うサイバー攻撃が増加し、組織の重要な情報の漏えいや不正利用により、経営や事業に対して大きなダメージを与える事故や事件が発生しています。

このような組織を取り巻くサイバー攻撃の脅威は、経営課題として経営層が率先して取り組む必要があります。例えば会社法において取締役会の決議事項である「内部統制システム構築の基本方針」等に、サイバーセキュリティリスク管理が含まれています。また IT の発展によるビジネスの変革は、消費者向けのビジネスから企業間取引へと拡大し、IoT 技術の普及等によりサイバー空間と実空間の融合が進むなかでビジネスチャンスが一層増大しています。言うまでもなくこうしたビジネスはセキュリティが確保されて初めて成立するものであり、サイバーセキュリティは、やむを得ない「費用」ではなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待されています。[1]

このようにサイバーセキュリティの確保は、企業が IT を利活用し、ビジネスを発展させていく上で、経営者が果たすべき責任のひとつであり、経営者自らがリーダーシップをとってサイバーセキュリティ対策を講じる必要があります。このため 2015 年 12 月に経済産業省と独立行政法人情報処理推進機構（以下、IPA）は、サイバーセキュリティ経営ガイドライン（以下、本ガイドライン）を公表しました。ただし本ガイドラインは記述を簡潔にしたため、内容の実践に関する具体的な記述は含まれていませんでした。

こうした経緯から、IPA はサイバーセキュリティ経営ガイドライン解説書（以下、本解説書）を作成しました。本解説書は、本ガイドラインの中でも特に重要となる対策や考え方について具体的に説明しています。本解説書を利用することで、サイバーセキュリティの確保に向けて、経営者が正しく判断できるような組織内の体制や、社会的な信頼を維持向上するための組織外との連携体制が構築されることが期待されます。

0-1 本解説書の想定読者

本解説書は、下記のようなサイバーセキュリティ[2]対策を検討する必要のある大企業及び中小企業（但し小規模事業者を除く）の経営者と、経営者の指示を受けて対策を実施する責任者（CISO[3]等）や担当者を想定読者としています。

---

[1] 企業経営のためのサイバーセキュリティに関する基本的な考え方については、内閣官房 内閣サイバーセキュリティセンター（NISC）が策定した「企業経営のためのサイバーセキュリティの考え方」（2016 年 8 月 2 日）参照。

[2] サイバーセキュリティとは、コンピュータやネットワークに対してサイバー攻撃を受け、情報の窃取や破壊、または IT システムの機能の不備等の不具合が生じないよう対策を実施し、適切に維持管理することを言います。

[3] 最高情報セキュリティ責任者：Chief Information Security Officer

- IT に関する製品やシステム、サービス等を供給する企業
- 経営戦略上 IT の利活用が不可欠である企業

なお、本解説書では、経営者の指示を受けて対策を実施する責任者を以下 CISO 等と記述します。

0-2　本解説書の構成

本解説書は以下の構成となっています。０章はサイバーセキュリティ対策を検討している経営者、および対策の実施責任者となる CISO 等を想定読者として、経営者が認識する必要がある「３原則」を解説します。また、１章以降は、サイバーセキュリティ対策の実施責任者となる CISO 等を想定読者として、本ガイドラインに示される重要 10 項目について、記載されている順に解説します。なお本ガイドラインの重要 10 項目と本解説書での各章の略称の対応関係は下図に示します。

表　０－１　本解説書の構成と想定読者

本ガイドラインの重要 10 項目	本解説書における 10 項目の略称	想定読者	
		経営者	CISO 等
－	０．はじめに	○	○
１．サイバーセキュリティリスクの認識、組織全体での対応の策定	１．サイバーセキュリティ対応方針の策定		
２．サイバーセキュリティリスク管理体制の構築	２．リスク管理体制の構築		
３．サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	３．リスクの把握、目標と対応計画策定		
４．サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示	４．PDCA サイクルの実施と対策の開示		
５．系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握	５．系列企業・ビジネスパートナーの対策実施及び状況把握		
６．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	６．予算確保・人材配置及び育成		○
７．IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	７．IT システム管理の外部委託		
８．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のための環境整備	８．情報収集と情報共有		
９．緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施	９．緊急時対応体制の整備と演習の実施		
10．被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	10．被害発覚後の必要な情報の把握、開示体制の整備		

図 0-1 に「３原則」と「重要 10 項目」のポイントを示します（拡大版は付録 1 を参照）。

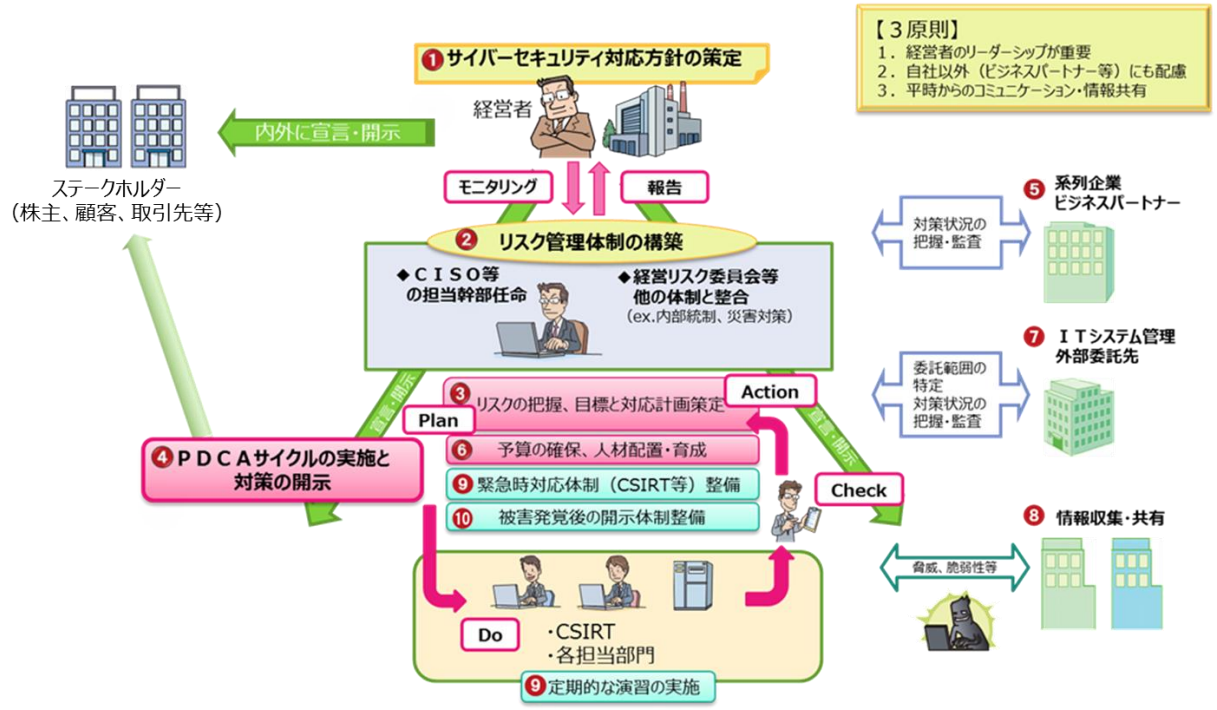


図　０－１　ガイドラインの３原則・重要１０項目

0-3　サイバーセキュリティ経営の原則

サイバーセキュリティリスクに対応するために経営者は、以下の３原則を認識し、組織の対策を進めることが重要です。

（１）　経営者は、IT 活用を推進する中で、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

サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、新しいリスクであるために、従来の企業におけるリスク対策の延長上では対策が進みにくいことから、サイバーセキュリティリスク対策を進める上で、経営者がリーダーシップを発揮することが必要不可欠です。

サイバーセキュリティ対策において、経営者によるリーダーシップが求められる具体的な事項として、例えば以下のものが考えられます。

１．サイバーセキュリティリスクを経営課題として位置づける。
２．CISO 等を任命し、役割と責任を明確にするとともに経営者が実施を支援する。
３．組織のサイバーセキュリティ対策の効果をチェックし、必要に応じて対策の見直しを行う。
４．自社のビジネスパートナー等とサイバーセキュリティ対策を共有し、連携して実施する。
５．これらを実施するために、サイバーセキュリティ対策に必要な情報を収集し、経営層に報告するための体制を構築する。

（２）　自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めたサイバーセキュリティ対策が必要

仮に子会社に委託した情報が漏えいした場合、「当社で生じた事故ではないので関係ありません」と言い訳することはできません。ビジネスパートナーや委託先における対策も、別段の特約等が無い限り、基本的には委託元が委託者としての責任を問われます。特に個人情報の処理を外部に委託する場合、法律で委託先の監督が義務づけられており、監督が不適切であったために漏えいが生じたと判断された場合は委託元が処罰されます。したがって、組織内の体制構築だけではなく、系列会社やビジネスパートナー等の外部組織を含めた情報共有体制や対策の連携が必要になります。詳細については、本ガイドラインの「５章 系列企業・ビジネスパートナーの対策実施及び状況把握」及び「７章 IT システム管理の外部委託」で解説します。

（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、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

サイバーセキュリティ対策状況を正しく把握するためには、適切なコミュニケーションが必要になります。組織内に対しては、軽微なインシデントや違反などの報告を参考に対策改善を行う必要があり、報告者を処罰するのではなく、奨励等も実施し、適切なコミュニケーションが行われる体制や組織風土、雰囲気を作る必要があります。

組織外に対しては、サイバーセキュリティリスク管理を経営上の重要課題として取り組んでいることや対策状況を正しく開示することで信頼を得ることができます。また、対策やサイバーセキュリティリスクの状況について、関係者と共有することも重要です。このとき、対策できているリスクと、対策できていないリスク（残留リスクとして受容しているリスク）を明らかにすることが必要です。これらの対策状況のすべてを関係者に一律に開示するのではなく、関係する企業や組織、ステークホルダー等に合わせて必要な情報を開示するべきです。例えば、緊急時に連携して対処する企業には、対処に必要な情報を提示し、被害が及びそうな関係者へは被害の状況や二次被害の有無などを開示する必要があります。

0-4　経営者が決定すべき事項

サイバーセキュリティリスク管理体制の構築と維持・効率化を行うために、経営者が決定、実践すべき事項は、大きく分けて下図の５種類があります。まず管理体制を構築するために、CISO 等の任命、CISO 等や CISO 等を補佐する担当者が策定したセキュリティポリシーの承認、及び実施計画の承認を行います。また、管理体制の維持・効率化のために、CISO 等から報告を受けて対策状況を把握し、CISO 等に対して対策・計画の改善を指示します。

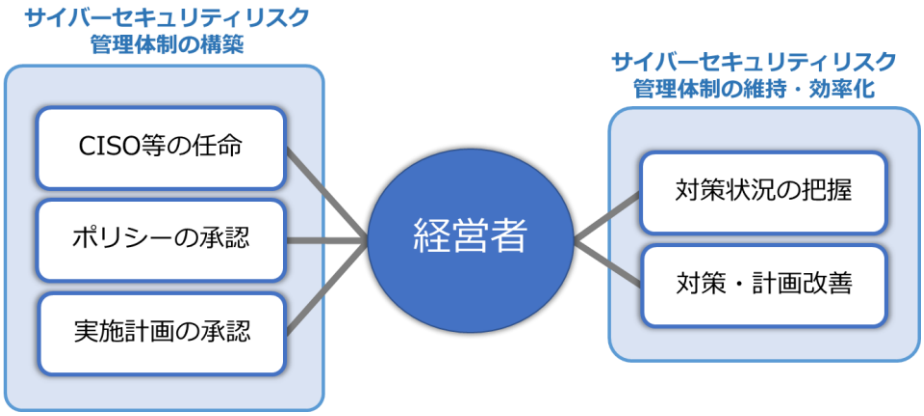


図　０－２　経営者が決定すべき事項

0-5　経営者が責務を果たしているかどうかの問い

事業継続と経営課題の解決に責任を負っている経営者は、サイバーセキュリティリスク管理に対して何をすべきでしょうか。例えば次の３つの質問を自分に問いかけることにより、サイバー攻撃に対して自社の事業を安全に継続できるようにするためにどうすべきか

を検討するきっかけにしてください。

問い① ネットワークが 1 週間遮断された場合のビジネスへの影響度がわかりますか？

問い② 自社への被害が想定されるサイバー攻撃について、社内に聞ける人がいますか？

問い③ 漏えい事故や事件発生後にどのように状況を報告し、信頼を維持・回復しますか？

問い①：事業で IT を利用している組織では、事業継続のために、IT が利用できなくなった場合の対処方法を検討する必要があります。普段、事業に利用しているネットワークもサイバー攻撃においては、侵入経路になります。仮に、サイバー攻撃を受けて情報漏えいなどの被害が生じた場合には、原因追及や被害調査のためにネットワークを遮断する必要が生じます。こうした状況において、サイバーセキュリティ対策を優先するか、それとも事業継続を優先するかの判断を迫られる場合があるため、トータルなビジネスリスクの中でサイバーセキュリティリスクを捉え、決断をくだす必要があります。

問い②：企業の顧客情報や機密情報を狙ったサイバー攻撃は日々発生しており、その攻撃手法も様々です。サイバー攻撃への対策を検討するためには、具体的な攻撃事例を知り、さらに自社にもその攻撃手法による被害が発生する可能性があるかどうかを知ることが必要です。自社の中でサイバー攻撃の事例や自社のリスクの大きさについて尋ね、回答を得ることができる人は、サイバーセキュリティリスク管理体制の CISO 等や、CISO 等を補佐する役割として適任者である可能性があります。サイバーセキュリティリスク管理責任者、あるいは責任者を支援しサイバー攻撃の情報を収集する人材等について、実態を把握しておく必要があります。

問い③：サイバー攻撃を受け、事業への何らかの影響が及ぶようなインシデント[4]が発生した場合の説明責任は経営者にあります。例えば、インシデントが顧客に影響する場合や取引先への二次被害が考えられる場合に、どの時点で、何を報告すべきでしょうか？メディアに対しては、いつ、何を発表すべきでしょうか？これらへの対処を予め検討しておく必要があります。自組織においては、いざという時にインシデント対応のために必要な情報が集約でき、しかるべき責任者が判断できる体制が、また組織外との関係においては、緊急事態だけではなく、常日頃からのコミュニケーションがそれぞれ必要になります。

[4] インシデントとは、サイバーセキュリティ分野において、サイバーセキュリティリスクが発現・現実化した事象のことを言います。

解説の記述方法

本ガイドラインの重要 10 項目の各対策は、下図の構成で記述しています。10 項目の方針を見出しとして、具体的に検討・実施すべき項目を枠で囲み示しています。実施する内容によっては、複数の項目を必要とするため、項目ごとに検討すべきポイントや考え方を示しています。

CISO 等や対策内容を検討する担当者は、検討・実施すべき項目の詳細を読み進めながら具体的な対策を検討してください。また、参考情報として、参考データ、コラム、仮想企業の検討の例示（各章末）を記載しています。

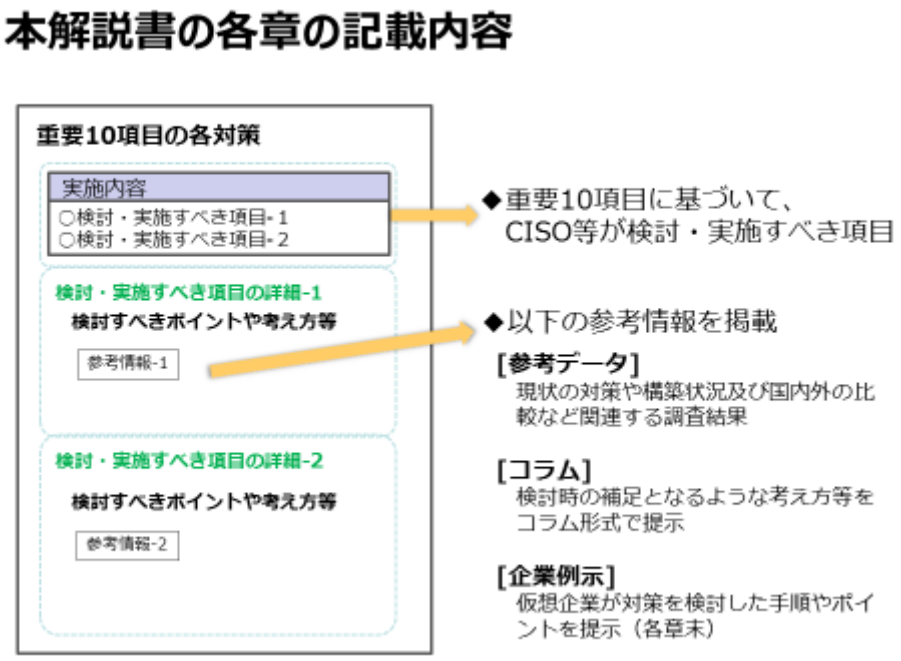


図 0－3　本解説書の各章の記載内容

なお、以下の付属資料等があります。必要に応じて内容を確認し、検討に役立ててください。付録２の「参照情報」については、本解説書で参考となる情報を章ごとに集めた情報です。また、付録３「サイバーセキュリティ経営チェックシートの実施の目安と確認事項」は、本ガイドライン 付録Ａ サイバーセキュリティ経営チェックシートの判断基準の参考資料です。

別添「サイバーセキュリティ対策に関連する被害事例」は、具体的なサイバー攻撃やリスク、脅威などを検討するために収集した被害事例です。

表 ０－２　本解説書の付録及び別添の構成

本解説書の付録及び別添の構成	本ガイドラインとの関係等
付録１：ガイドラインの３原則と重要 10 項目の概要図	本ガイドラインの３原則及び重要 10 項目の概要を１枚にまとめて示した図
付録２：参照情報	本ガイドラインの参照情報を拡充したもの
付録３：サイバーセキュリティ経営チェックシートの実施の目安と確認事項	本ガイドラインの付録Ａ「サイバーセキュリティ経営チェックシート」の判断基準を記載したもの
別添　：サイバーセキュリティ対策に関連する被害事例	本解説書で新たに追加 （サイバー攻撃の実例等を掲載）

なお、本解説書では、主として本ガイドラインの本文に記載されている項目について記載しているため、技術的な対策内容については、本ガイドラインの付録Ｂ 望ましい技術対策と参考文献、及び付録Ｂ－２ 技術対策の例を参照してください。

１ サイバーセキュリティ対応方針の策定

サイバーセキュリティリスク対策を実施するための対策方針、すなわちセキュリティポリシーを策定します。策定したセキュリティポリシーは、会社の行動等の規範にするものであるため、経営層の承認を得ることによって自組織内部に対して権威付ける必要があります。また、組織内に対しては周知徹底を図るために、また組織外に対してはセキュリティに関してその会社の姿勢を公に示すために、策定したセキュリティポリシーを内部に浸透させるための活動と、外部に発信するための活動とが必要となります。

実施内容１
１．セキュリティポリシーを策定し、経営者に承認を得る。 ２．策定したセキュリティポリシーを組織の内外に示す。

１-１ セキュリティポリシーの策定

CISO 等が推進役となり、セキュリティポリシーを策定します。セキュリティポリシーの策定方法については、すでに情報セキュリティマネジメントシステム（ISMS）[5]等について説明する資料[6]が数多くあるため、これらを参考にセキュリティポリシーを策定することができます。セキュリティポリシーには、表 １－１に示した項目を記載します。ここでは、①対応方針の策定、②リスク管理体制、③セキュリティポリシーを実践するための方法について概要を説明します。情報収集と情報共有、緊急時対応体制の整備と演習の実施については、８章、９章をそれぞれ参照してください。

セキュリティポリシーの主な検討項目

①対応方針の策定

一般的なセキュリティポリシーにおいて、対応方針として示されている内容は次の通りです。

- 経営リスクとしての位置付け：自社の経営において、サイバーセキュリティリスクは経営を左右するリスクとなる可能性があり、組織全体で取り組む必要があるということを経営者が認識していることを示します。その際、サイバー攻撃は、日々、新しい手法が生まれており、そのリスクをゼロにすることは出来ないため、守るべき情報資産に照らしてリスクを低減するといった考え方が重要です。
- 組織全体としてどのように対応するのか：セキュリティポリシーに記載した内容を

[5] 品質管理分野の ISO 9001、環境分野の ISO 14001 と同様、情報セキュリティ分野を対象とするマネジメントシステムの国際標準規格として、ISO/IEC 27001（日本工業規格 JIS Q 27001）が定められています。

[6] 例として、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）によるものを示します。
http://www.jnsa.org/result/2016/policy/

組織全体で遵守することを示します。

具体的な記載内容については、CISO 等が主体となって、各企業から公開されているセキュリティポリシー等を参考に自社の実態に合わせた目標を設定し、記載するようにします。さらに、策定したセキュリティポリシーについて経営層の承認を得る必要があります。経営層から承認を得るためには、その企業の文化によっても異なりますが、経営会議や役員会など経営層の意思決定の場において、以下の事項等を説明し、質疑応答を経て、納得してもらうというプロセスが必要になるでしょう。

- 策定したセキュリティポリシーは、その企業がさらされているセキュリティリスクへの対処に寄与するものであること
- 策定したセキュリティポリシーが、自社の経営戦略、事業目標と矛盾せず、むしろそれら戦略の遂行、目標の実現を支えるものであること
- 策定したセキュリティポリシーが、ヒト、モノ、カネ等のリソースにおける制約の範囲内で、現実的に対応可能な内容となっていること

②リスク管理体制

サイバーセキュリティリスク対策を維持し適切に改善していくためには、目標を設定し、目標を達成するための体制をセキュリティポリシーに明確に記載する必要があります。サイバー攻撃による組織全体の経営リスクへの対応を考え、サイバーセキュリティリスク管理体制は、組織全体の管理を対象とする体制であることが求められます。ISMS は、組織の一部や部門のみを対象として認証取得することも可能ですが、サイバーセキュリティリスク管理体制は、対策漏れを生じさせないためにも全組織で取り組むことが求められます。

③セキュリティポリシーを実践するための方法

方針と体制に続いて、どのような方法で対策に取り組むのかを示します。具体的には、対策を実践するために必要となる経営資源を確保した上で、PDCA マネジメントサイクルによるフレームワークのもとで、セキュリティポリシーで示した目標を達成するための対策を実践することを定めます。さらに、こうした取組の基盤として、従業員全体への教育を行うことも必要です。

表 1－1　セキュリティポリシーに記載すべき事項

セキュリティポリシーに掲載すべき事項	重要 10 項目との対応
対応方針の策定	
経営者がサイバーセキュリティリスクを経営リスクとして定める	(1)
経営者が組織全体でのサイバーセキュリティリスクの対応方針を定める	(1)
リスク管理体制	
CISO 等を責任者としたサイバーセキュリティリスク管理体制を定める	(2)
サイバーセキュリティリスク管理体制の関係者と責任を定める	(2)

セキュリティポリシーに掲載すべき事項	重要 10 項目との対応
守るべき資産とリスクの対策を定める	(3)
セキュリティポリシーを実践するための方法	
サイバーセキュリティ対策のための経営資源を確保する	(6)
PDCA マネジメントサイクルのもとでサイバーセキュリティ対策を実践する	(4)
従業員向けに定期的な研修等を実施することを定める	(6)
情報収集と情報共有	
関係者にサイバーセキュリティリスクや取組状況を共有することを定める	(4)
ビジネスパートナーや委託先にも自らの組織と同等なサイバーセキュリティ対策を要求し、その状況を確認することを定める	(5) , (7)
情報共有活動への参加を通じて得た攻撃情報を対策改善に活用することを定める	(8)
緊急時対応体制の整備と演習の実施	
サイバーインシデントへの対応体制を整備することを定める	(9)
緊急時対応の訓練や演習を定期的に実施することを定める	(9)

1-2 セキュリティポリシーの周知

CISO 等は、策定したセキュリティポリシーを組織の構成員や企業の従業員、ならびに取引先等の組織外の関係者に周知し、サイバーセキュリティに対する考え方を徹底する必要があります。従業員への周知は、すべての従業員が閲覧できる場所に掲載・保管する方法や新入社員への教育等を通じて実施します。掲載、保管及び教育については、CISO 等が実施するのではなく、各部の責任者や兼任の担当者を設置して行う場合もあります。

組織内への周知の重要性

同じ組織内でも部門によっては保護すべき資産や IT の利用度合いや利用形態は異なり、それによりサイバーセキュリティリスクも異なります（詳細は３章のリスクの把握、目標と対応計画策定を参照）。そのため、従業員はそれぞれの部門で異なった対策を実施することになりますが、それぞれの対策がセキュリティポリシーで示された目標を達成するためのものであることを理解することで、組織内でのサイバーセキュリティ対策に関する目的意識を共有することが可能となります。こうした目的意識を共有することは、ルールの遵守意欲を高め、新たな脅威への柔軟な対応を可能とする上で有用であり、従業員すべてが理解し、確実に実施する必要があります。

組織外への公開の重要性

取引先の重要情報を扱う場合、その取引先から重要情報の取扱に関する規定や管理体制及びセキュリティポリシーの提示を求められる場合もあります。この状況とは逆に、ビジネスパートナーや委託先に対し自組織の重要な情報を預ける場合には、自組織と同等なサイ

バーセキュリティ対策を要求する場合もあります。このような場合、預ける情報の自組織内での重要度と対策を開示することが必要になってくることも考えられます。

さらに、セキュリティポリシーを株主やビジネスパートナー等に広く宣言することで自組織のブランド価値向上に役立てることもできます。

セキュリティポリシー群の種類

一般的にセキュリティポリシー群は、組織のセキュリティの目標と目標を達成するために組織の構成員がとるべき行動等を宣言するポリシー（基本方針）、基本方針に従い何を実施しなければならないのかを規定するスタンダード（対策基準）、対策基準を詳細化し、手順を示すプロシージャー（実施手順）で構成されます。また、ポリシーは、各組織の状況や体制及び考え方に応じて策定するため、ポリシーにスタンダード（対策基準）を含んで策定する場合もあります。

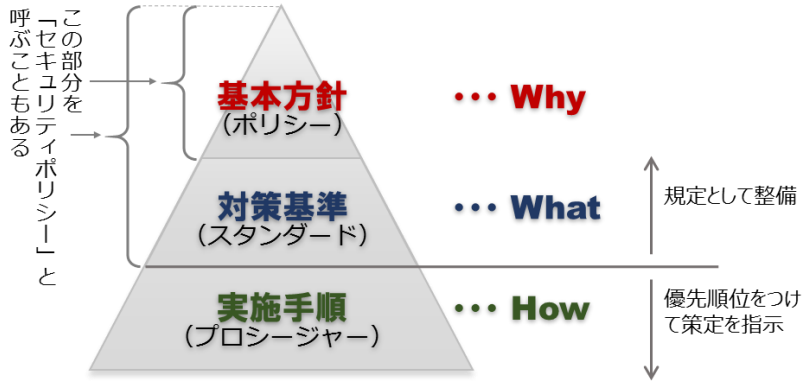


図　1－1　セキュリティポリシー群の概要

セキュリティポリシーの公開

組織内部では、これらのセキュリティポリシー群のすべてを周知し、徹底することが求められますが、組織外への公開（宣言）の内容は、公開する相手との関係性や関連法令により異なります。個人情報保護に関する日本工業標準（JIS Q 15001）で認証を取得する場合は、制度によって宣言書を公表することが求められますが、情報セキュリティでは広く開示することを求めていません。一方、企業の株主には、経営課題であるサイバーセキュリティ対策についてどのような目標を設定し、どのような体制で取り組むのかを示すことは信頼を得る上で重要です。また、企業の取引先には、対策基準を示して自社の重要情報について同等の対策を求める場合があります。このようにセキュリティポリシーとして組織外部に公開（宣言）する内容は、どのような関係者に何を公開し、宣言する必要があるのかによって異なります。

企業例示について

本解説書では、各実施内容の具体化のヒントになるように、規模・業種等の異なる２種類の仮想企業を題材に検討手順やポイントを示しました。仮想企業２社の特徴は下記のとおりであり、各章で示す実施内容に対して、それぞれ２社がどのような検討を行い、何を実施したか等について記載しているので適宜参考にしてください。

インターネットショッピングを行う企業（A社） EC サイト運営（中小企業）

A社は、EC サイトを独自で企画・運営し、インターネットを通じて商品を販売している中小企業です。EC サイトは、主に B2C の業務であるため、多くの顧客の個人情報を保有、管理しています。日常業務において社員全員が個人情報の漏えいには気を付けていますが、個人情報保護の専任担当者は設置しておらず、EC サイトの運営部門の少数のスタッフが兼任で対応していました。近年のマイナンバー対応やサイバー攻撃のニュースを受け、EC サイトの業務停止による事業継続性のリスクを考えるようになり、サイバーセキュリティ対策の検討を開始しました。

■業務内容：EC サイトの企画・運営・管理、アパレル製品の企画・販売
■資 本 金：３百万円
■従業員数：30 名
■売 上 高：1,200 百万円

電子機器の製造を行う企業（B社） 電子機器製造（大企業）

B社は、電子機器等の製造を行う一部上場企業（大企業）です。グループ企業や関連企業等と連携する業務が多く、受発注の一部や製造情報の一部を他企業の IT システムによって共有しています。 B社では、製品情報公開・ヘルプデスク web システム（以下ヘルプデスクシステム）を運営し、 B社製品の登録ユーザー向けに公開しているため、個人情報保護管理体制は構築済です。取引先との関係上、情報セキュリティ対策を実施しているものの、取引先ごとに個別に対応している状況です。

■業務内容：デジタル周辺機器製造・販売
■資 本 金：1,000 百万円
■従業員数：3,000 名
■売 上 高：45,000 百万円

企業例示「セキュリティポリシーの策定」

仮想企業Ａ社及びＢ社で、セキュリティポリシー策定を検討、実施した内容やポイントを示します。

企業Ａ社のセキュリティポリシー策定　**EC サイト運営（中小企業）**

対応方針の策定: 経営リスクとしての位置づけ、組織全体としての対応

これまで A 社には、セキュリティポリシーがありませんでした。今回初めて、A 社情報システム部門のセキュリティに詳しいメンバーをセキュリティポリシー担当者として任命し、策定に取り組む事になりました。セキュリティポリシーの担当者は、まずセキュリティのインシデントが発生すると A 社にとってどんな影響があるかを整理することから作業を始めました。下記が整理した結果です。

A 社の収益の柱は、EC サイトを運営するサービス事業です。もし、A 社のネット通販サイトで買い物をする会員の個人情報が漏えいすると、ネット通販業者としての信用を失い、大量の退会者がでるかもしれません。またセキュリティインシデントの発生により EC サイトを一時停止する事態になれば、テナントであるネット通販業者のお客様が商売できなくなる等、お客様に事業上の損害を与える恐れがあります。こうしたセキュリティリスクがおきると、規模が大きくない A 社は即座に多大な経済的打撃を被り、経営そのものが立ち行かなくなると考えました。

A 社は EC サイト会社であり、社長はもともと IT への見識が高い人物です。A 社にとって IT システムがもつビジネス上の重要性と、サイバーセキュリティの大切さ・怖さを漠然とは理解していました。しかし、セキュリティポリシー担当者が示した上記の整理を聞いて、改めて「サイバーセキュリティリスクは A 社の経営リスクだ」とはっきり認識するようになりました。また上記の整理から、サイバーセキュリティ上重要な保護すべき資産は、A 社自身の通販サイトの会員顧客の個人情報と、ネット通販業者がお客様である EC サイトのシステムそのものである、ということになりました。情報セキュリティの３要素に関しては、前者では機密性、後者では可用性の保護が大切です。

A 社では、全部門が受発注業務や顧客管理業務に関与し、顧客の個人情報に触れます。そこで社長を含む経営幹部全員が、個人情報の機密性の保護のためには、全部門でサイバーセキュリティ対策に取り組む必要があるという認識で一致しました。

ところで、EC サイト運営サービスための IT システムは、インターネットに接続した Web ベースのシステムです。セキュリティポリシー担当者が、同僚である EC 運営部門の運営担当者に話を聞いたところ、これまでにも度々、システムを構成している Web サーバ等にあらたな脆弱性が判明したり、未知のサイバー攻撃が出現していたことが分かりました。運営担当者によると、セキュリティリスク低減のためには、セキュリティ対策の定期的・継続的な見直しが不可欠だとのことでした。

セキュリティポリシー担当者は以上の検討結果をまとめて、セキュリティポリシーの冒頭に次の項目を盛り込むことにしました。

（A 社セキュリティポリシーの冒頭に盛り込む項目）

- A 社の社長自身、サイバーセキュリティリスクは A 社の経営リスクであると認識していること、
- A 社の重要な保護資産は、会員顧客の個人情報と EC サイトのシステムそのものであること、
- サイバーセキュリティ対策には A 社の全部門が取り組むこと、
- セキュリティ対策を定期的・継続的に見直し、セキュリティが保たれた状態を維持すること

セキュリティポリシーの担当者は、方針の策定とリスク管理体制のほか、セキュリティポリシーを実践する方法、情報収集と情報共有、緊急時体制の整備・演習の実施についての項目を検討し、サイバーセキュリティ委員会の審議を経て、A 社初のセキュリティポリシーとして取りまとめました。

・企業Ｂ社のセキュリティポリシー策定　　**電子機器製造（大企業）**

対応方針の策定: 経営リスクとしての位置づけ、組織全体としての対応

B 社は以前から、上場企業として株主や市場、社会に対する責任を果たすために、セキュリティの活動に取り組んできました。サイバーセキュリティリスクの対応は、様々な企業リスクをコントロールするため常設されている経営リスク管理委員会が所管します。この委員会は、リスクに関係する各部門（リスク管理部、法務部、製造部ほか）を所管する役員達と関係部門長とで構成され、リスク管理部が事務局になっています。このたび、経営リスク管理委員会の下で B 社セキュリティポリシーを整備することが決まり、その案をリスク管理部が策定することになりました。

リスク管理部の担当者はまず、他社事例の調査から着手しました。先進的な企業は、「CSR[7]報告書」や「情報セキュリティ報告書」を用いて、セキュリティの取組みを開示していることがあり、また、情報セキュリティリスクについて有価証券報告書の「事業等のリスク」で公表している場合もあることから、特に同じ業種で規模が同様な企業を対象に、これらの文書を収集し共通の特徴を分析しました。そのまとめは以下のとおりです：

- セキュリティポリシーを公開している大企業、特に ISMS の認証を取得している企業では、セキュリティポリシーの前文か最初の章・項目において、情報セキュリティの取組みを経営の重要課題と認識している事を記載している。

- そうした企業は、役員等の経営幹部を中心とした情報セキュリティ管理体制を構築し、全社的に情報セキュリティに取り組むことに言及している。

- 保護資産を守る上で必要なセキュリティ対策は、サイバーセキュリティの変化に適応させるために、継続的に見直すことにしている。

- 一定以上の規模を持ち複数の事業を行っている企業は、晒されるセキュリティリスクが多岐に亘り、また保護すべき資産も事業ごとにさまざまに異なる。こうした企業のセキュリティポリシーでは、リスクと保護資産を具体的・個別に列挙すること

[7] CSR: corporate social responsibility

はせず、包括的な表現で記載している。

これらの分析に基づき、担当者は、B 社セキュリティポリシーの中に次の項目を記載する事を決めました。

（B 社セキュリティポリシーに記載する項目（一部））

・B 社は、情報セキュリティの取組みを経営上の重要課題と位置づけ取り組んでおり、他の企業リスクも含めて一元管理する経営リスク管理委員会をトップとする管理体制を構築する。

・経営リスク管理委員会を中心に、サイバーセキュリティリスクの変化に合わせて、保護資産やセキュリティ対策を定期的、継続的に見直すサイクルをまわす。

・保護資産は「B 社の経営上及び事業上重要な資産」と表現する。またサイバーセキュリティリスクは、これら資産の機密性、可用性、完全性が損なわれる事により発生するあらゆるリスクと表現する。

2 リスク管理体制の構築

サイバーセキュリティ対策を実施するためには、サイバーセキュリティリスク管理体制を構築することが重要です。サイバーセキュリティリスク管理体制を構築する手順として、経営者は、セキュリティポリシーに基づき CISO 等を任命します。CISO 等が主体となって、経営リスクに対応するサイバーセキュリティリスク管理体制を構築し、各関係者の責任の明確化等を検討します。

実施内容２
１．セキュリティポリシーに基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築する。 ２．サイバーセキュリティリスク管理体制において CISO 等や各関係者の責任を明確にする。 ３．組織内のリスク管理体制が既に存在する場合、サイバーセキュリティリスク管理体制との関係を明確に規定する。

2-1　サイバーセキュリティリスク管理体制

サイバーセキュリティリスク管理体制の構築方法

サイバーセキュリティリスク管理体制を構築する際は、まず特定の事業部門等が個別に判断して対応するのではなく、全社横断的な意思統一が図られ、実践できる体制にすることを検討します。全社横断的な体制にするためには、CISO 等が経営者の意思を反映して構築を推進していることが、自社内で認識されていることが重要となります。

次に、担当者の役割や責任を検討します。具体的には、CISO 等が、事業部門ごとに責任者（以下、部門責任者）を任命し、その部門責任者にセキュリティポリシーの浸透や状況報告・意見集約など各部門を管理する役割を任命します。このとき管理する単位（課、室の組織等）と対象範囲について明確にしておきます。

さらに、CISO 等をはじめ各部門の責任者を集めた全社横断的な体制となる委員会を設置することを検討します。このような委員会が管理体制の中心となることで、部門間で異なる意見を調整しながら、全社的に意思統一を図り、トップダウンの運営が可能となります。

そのほか、策定したセキュリティポリシーや社内のルール等が、自社内で周知徹底されるように従業員向けた教育や演習等の実施を検討します。

このように構築されたサイバーセキュリティリスク管理体制に対して、経営者の承認を得るようにします。また監査役は、第三者的立場で体制が適切に運用されているかを監査します。

なお、一旦構築できたとしても、新規事業への参入や新たな脅威の出現等により、体制の見直しが必要になることが考えられます。よって、定期的に体制を評価し、見直すためのフレームワーク（PDCA）が重要となります。フレームワークについての詳細は４章で説明します。

サイバーセキュリティリスク管理体制の構築の必要性と経営者の責任

サイバーセキュリティリスク管理体制が整備されていない場合、全社横断的に対策状況やリスク等について把握ができません。経営者が適切に判断するための情報を集約し、万一インシデントが発生した際に全社的な組織対応ができるようにするために、管理体制を構築し、維持していく必要があります。

会社の経営者である取締役には、その執行するべき業務として（会社法第348条第３項第４号等）、また会社に対する善管注意義務（会社法第330条、民法第644条）により、会社における内部統制（会社が営む事業の規模、特性等に応じたリスク管理体制）に係る体制を構築することが義務付けられており、サイバーセキュリティに関するリスクが会社に重大な損失をもたらす危険のある場合には、これらの義務を履践していないとの評価がなされ、任務懈怠責任（会社法第423条第１項）を経営者個人に対して問われて、会社に対

する損害賠償責任を負う可能性があります[8]。

❑ **参考データ「経営者がセキュリティリスクを評価・審議する機会（国内外の比較）」**

「サイバーセキュリティリスク管理体制の構築方法」では、経営者の了承を得て体制を構築する必要性を示しました。一方、CISO の実態調査[1]の国内外比較では、「経営者が自社の情報セキュリティリスクを評価・審議する機会がない」企業の割合は、米国 2.8%、欧州 3.7%に比べ、日本は 13.6%と高く、経営者が自社の情報セキュリティリスクに関与していないケースが一定数存在しています。

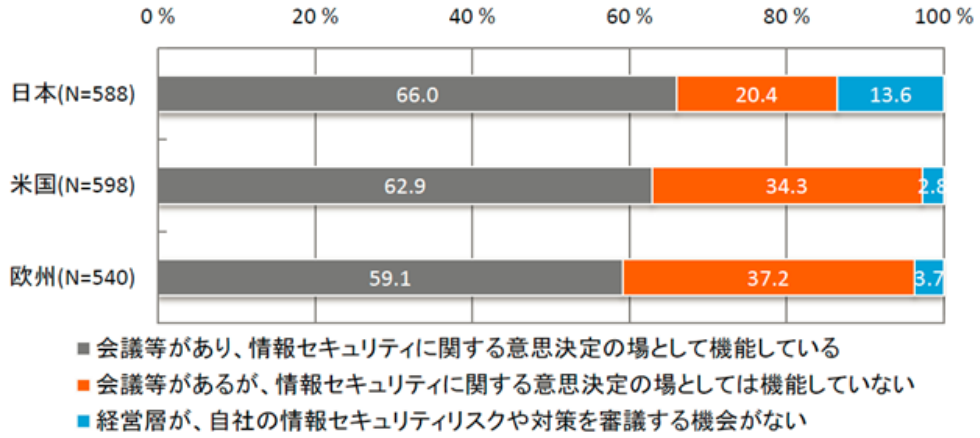


図 2－1 経営層の情報セキュリティに対する認識（国内外比較）

（引用）企業の CISO や CSIRT に関する実態調査 2016、独立行政法人情報処理推進機構

2-2 CISO 等に求められること

CISO 等は、サイバーセキュリティ対策を実施する現場と経営層を繋ぐ通訳となることが期待されます。例えば、経営層やステークホルダーに対して、自社のサイバーセキュリティリスクの状況や課題を、なるべく技術的な専門用語を使わずに説明し、合意を得る必要があります。またサイバーセキュリティ対策を推進していく上で、事業部門等の現場から手間が掛かる等の理由で反発を招かないように、現場の立場で支援するというスタンスが求められます。

[8] 詳細については、「情報セキュリティ関連法令の要求事項集（経済産業省作成）」参照。
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf

CISO 等の役割

組織の規模等に応じて、CISO 等が担う役割は様々ですが、役割の例として下記のようなものが考えられます。

・セキュリティポリシーを策定する。
・サイバーセキュリティリスク管理体制を構築する。
・自社のサイバーセキュリティリスクを把握し、リスク対応計画を策定する。
・対策実施に掛かる費用について経営層の承認を得る。
・構築した体制を維持、改善するための PDCA サイクルを統括、監督する。
・インシデント対応の陣頭指揮を執る。
・新規 IT 導入時等、事業部門に対するセキュリティの技術的観点からのアドバイスをする　等。

CISO 等が役割を果たすためには、自社の経営戦略や経営課題について認識し、理解していることが重要となります。例えばリスク対応計画の策定において、新規の事業計画を CISO 等が知る立場でない場合、その計画に内在するセキュリティリスクについて、対策を検討することは困難だからです。よって経営層は、CISO 等に、自社の経営戦略や経営課題が議論される取締役会等の場へ参加する権限を付与することを検討します。

なお、あらゆる役割を CISO 等が１人で担うことは難しい場合もあるため、CISO 室などの組織を設けて、CISO 等を支援するチームを構成し対応するケースもあります。また外部から CISO 等やその補佐となる人を招聘したり、CISO 等の役割の一部を外部の専門家に委託したりする場合もあります[9]。

[9] 近年 CISO をレンタルするサービスを提供する事業者も現れています。

❑ 参考データ「CISO 等の任命状況（国内外比較）」

「CISO 等に求められること」では、CISO 等に経営レベルの権限を付与することを検討する必要性について示しました。一方、CISO の実態調査[1]の国内外比較では、「CISO を任命していない」企業の割合は、米国 15.7%、欧州 11.3%に比べ、日本は 25.5%と高く、CISO 等の設置率が低い傾向にあります。

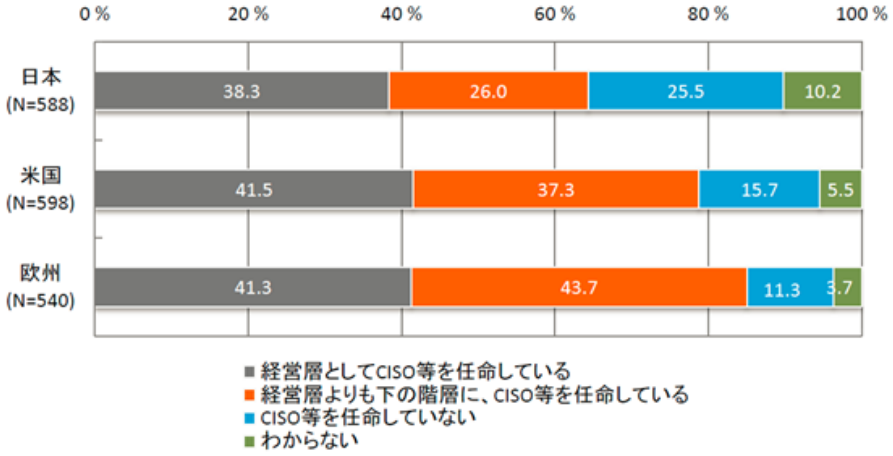


図 2－2 CISO 等の任命状況（国内外比較）

（引用）企業の CISO や CSIRT に関する実態調査 2016、独立行政法人情報処理推進機構

❑ 参考データ「リスク管理担当役員の任命状況（国内調査）」

国内企業のサイバーリスク管理の実態調査[2]では、「リスク管理の担当役員を任命している」という回答は、大企業（経営者）が 35.0%、中堅企業（経営者）が 19.2%、中小企業（経営者）が 9.9%であり、大企業に比べ中小企業はリスク管理の担当役員を任命している割合が低い傾向にあります。

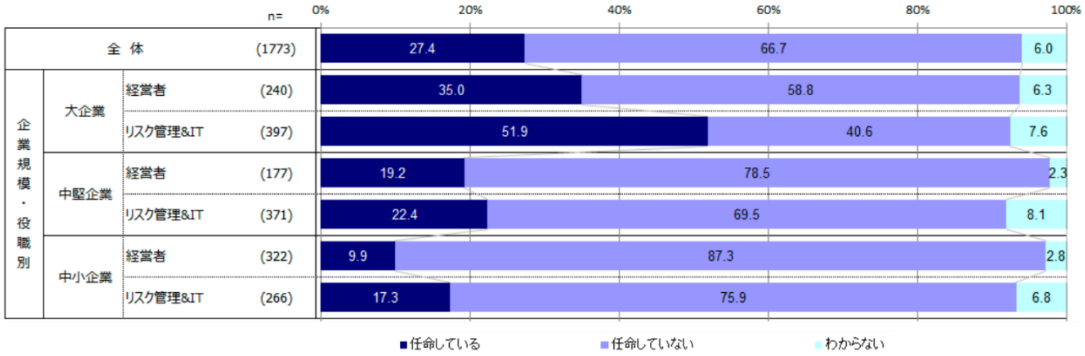


図 2－3 リスク管理担当役員の任命状況（国内調査）

(引用) 企業におけるサイバーリスク管理の実態調査 2015、独立行政法人情報処理推進機構

[コラム] 企業の形態に合わせた CISO の権限

CISO は、経営者の考える経営戦略を踏まえた効果的なリスクマネジメントを実践することが求められます。そのため、事業形態や企業文化等によって実態は様々ですが、CISO には部門横断的に情報を集約したり、緊急時に事業を停止する判断を行ったりといった経営者レベルの権限を付与することを検討する必要があります。

インシデントが発生した際に、緊急時の対応を検討する経営リスク委員会等において、CISO が一票を投じる程度の権限である場合や、被害の把握や拡大防止のために CISO 自身が特定のネットワークを分離、遮断できる権限を有する場合も考えられます。

サイバーセキュリティへの対策では、平時の対策だけではなく緊急時の対策を考慮した意思決定の体制や CISO の権限について検討する必要があります。インシデントの発覚から対処に至る過程には様々なケースがあり、そのすべてを想定し対策することは難しいため、各種のインシデント調査報告書などを参考に具体的な事象を想定した検討が重要です。

2-3 既存のリスク管理体制との関係

既に経営リスクに関する委員会等の管理体制が存在する場合には、サイバーセキュリティリスク管理体制との関係を整理し、各種取り組みや活動に重複等が生じないように配慮する必要があります。

既存の管理体制との整合

経営リスクに関する委員会、地震・水害等の自然災害における危機管理体制や防犯体制、事業継続計画（BCP）等、全社的なリスク管理体制が既に構築されている場合、その体制で想定すべきリスクの１つとしてサイバーセキュリティリスクを盛り込むことを検討します。

緊急時にどのような基準に基づいて、どのような手順で経営層に報告するかという、いわゆるエスカレーション[10]の仕組みを準用する等、サイバーセキュリティ管理体制と重複を避けて整合を取るようにします。

既存のリスク管理体制との関係性の明確化

情報セキュリティ管理体制や個人情報保護管理体制が存在する場合、サイバーセキュリティ管理体制で扱う資産との違い、各担当者や責任者及び管理体制の違いを明らかにしま

[10] 対応が困難な問題が発生した場合に、より上位の階層に報告し、対応を任せること

す。個人情報保護管理体制は、組織横断的な管理体制が構築されていますが、対象となる資産が個人情報に限定されています。サイバーセキュリティ管理体制の場合、求められる組織横断的な管理体制は同じであっても、対象となる情報資産は個人情報以外もあります。このような違いを明確にし、正しく周知しないと従業員の混乱を招くことになります。また、既存の情報セキュリティ管理体制と異なる場合にも、違いを明らかにし、従業員に周知する必要があります。これらの既にある情報セキュリティ関連の管理体制との違いを明確にするとともに、管理体制の統合の可能性についても検討します。

以下に、代表的な既存のリスク管理体制とサイバーセキュリティリスク管理体制の違いを説明します[11]。

① 情報セキュリティマネジメントシステムとの関係

情報セキュリティマネジメントシステム（ISMS）には、サイバーセキュリティ経営ガイドラインに記載しているサイバーセキュリティリスク管理体制と同等な体制が存在しています。例えば、CSIRT を整備していない場合でも情報セキュリティインシデントへの対応や情報セキュリティ事象に関する報告が定められており、サイバー攻撃を受け被害が発生した場合の対応や報告する役割が存在します。一方、昨今の標的型攻撃は巧妙化・高度化しているため、日々新たなリスクを発見し、速やかに対策することが求められる状況です。サイバーセキュリティの対策は、ISMS で想定している１年や半年の PDCA サイクルでは対応できないため、サイバー攻撃の情報収集や対策の改善などを短いサイクルで実施することが求められます。

② 個人情報保護管理体制との関係

個人情報の保護に関する法律（個人情報保護法）に対応した管理体制（以下、個人情報保護管理体制）が求められます。個人情報保護管理体制は、一般的に個人情報保護管理責任者が存在し、情報保護管理委員会や個人情報保護管理を監査する個人情報保護監査責任者も存在します。一方、管理対象となる情報資産は、個人情報に限定しているため、保護対象の情報資産を企業の重要な情報に拡大して検討する必要があります。さらに、ISMS と同様に、サイバーセキュリティへ対策するためには、一般的に個人情報保護管理体制が定める１年や半年の PDCA サイクルではなく、サイバー攻撃の情報収集や対策の改善などを短いサイクルで実施することが求められます。

[11] ここに掲載したフレームワーク以外に、米国国立標準技術研究所（NIST）が策定した「重要インフラのサイバーセキュリティを向上させるためのフレームワーク(CSF)」等があります。主に重要インフラ企業向けに書かれていますが、他の業種でも活用できる内容であり、海外で採用される事例が増えています。詳細については、https://www.ipa.go.jp/files/000038957.pdf 参照。

企業例示「管理体制の構築検討」

仮想企業Ａ社及びＢ社で、サイバーセキュリティリスク管理体制の構築を検討、実施した内容やポイントを示します。

企業Ａ社の管理体制構築　**EC サイト運営（中小企業）**

Ａ社では、情報セキュリティの管理体制や個人情報の保護管理体制が存在しないため、シンプルな管理体制の構築を検討しました。Ａ社の検討のポイントを示します。

- 経営者は、サイバーセキュリティリスク管理の責任者として、新たに取締役を CISO に任命した。

- CISO は、社内全体のサイバーセキュリティリスクを管理する責任を負い、各部門の責任者に対して各部門における具体的な検討や実施を指示する体制を構築した。この管理体制は、経営者―CISO―各部門責任者という３階層の構造である。

- CISO の指示及び各部門で実施しているサイバーセキュリティ対策の状態や有効性については、内部監査の責任者が監査することにした。

- 業務の中断が事業に与える影響が大きく、経営的なリスクになる EC サイトの運用については、EC 運営部門のみが対応するのではなく、情報システム部門の協力を得て、サイバーセキュリティリスクに対応する体制を構築した。

- 組織内で個人情報を保持し、管理している部門は、EC 運用部門、営業部門、総務部門があり、各部門の管理レベルを均一化するためにサイバーセキュリティ管理体制に主体的に関わる部門として各部門の責任者を管理体制に参加させた。

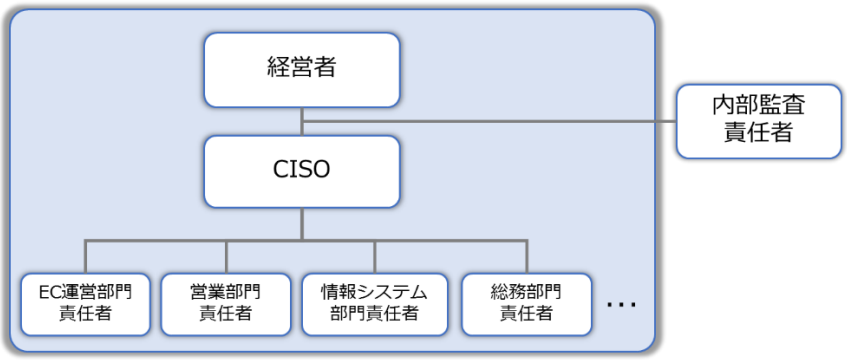


図　2－4　A社の管理体制の概要

企業Ｂ社の管理体制構築　　**電子機器製造（大企業）**

Ｂ社では、既存の管理体制として、個人情報の保護管理体制が存在していました。そのため、既存の個人情報保護管理体制にサイバーセキュリティリスク管理体制で不足している役割や機能を追加することによる構築を検討しました。Ｂ社の検討のポイントを示します。

・　経営者は、サイバーセキュリティリスク管理の責任者として、新たに情報セキュリティ部門責任者を CISO に任命した。

・　サイバーリスクの検討において、各部に偏在していた事業運営上のリスクを管理する担当者を新たに責任者として任命し、責任者を集めた経営リスク管理委員会を新たに設置した。経営リスク管理委員会の委員長を専務取締役とした。

・　CISO がサイバーセキュリティリスクの管理者となり、その状況や実施内容を報告し、経営的な判断を得ながら対策を進めることにした。この管理体制は、経営者―経営リスク管理委員会（CISO 含む）という２階層の構造である。

・　監査役は、経営に関するリスク全般について監査するが、この一部としてサイバーセキュリティ対策の実施状態や有効性についても監査する。

・　個人情報保護の管理体制では、保護対象が個人情報に限定されており、サイバーセキュリティリスクに関する観点等がないため、個人情報保護管理に関する経営層へのインプットは CISO が行うこととした。

・　新設した経営リスク管理委員会の運営、及び個人情報保護管理委員会が規定したリスクレベルや対策については、サイバーセキュリティリスク管理の検討もあるため、CISO が検討や見直しを行うこととした。

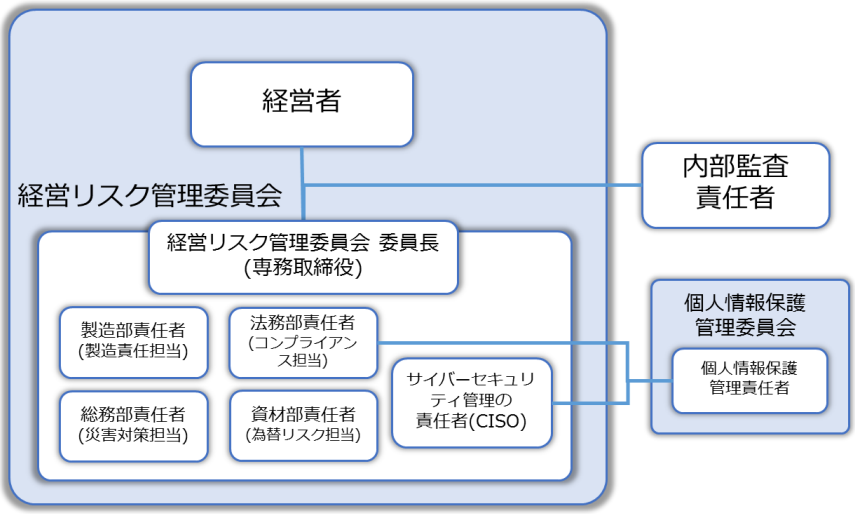


図　2－5　B社の管理体制の概要

３ リスクの把握、目標と対応計画策定

サイバーセキュリティリスクを把握し、リスクに応じた対策の目標と計画を策定します。

実施内容３
１．組織内に存在する資産の中で、守るべき資産を特定する。 ２．サイバー攻撃の脅威を識別する。 ３．サイバーセキュリティリスクが事業にいかなる影響があるかを推定し、リスクを把握する。 ４．サイバーセキュリティリスクの影響の度合いに応じた、リスクの低減、回避、移転等の目標や計画を策定する。また、サイバーセキュリティリスクの影響の度合いに従って対策しないと判断したものを残留リスクとする。

３-１　資産の特定

全社のサイバーセキュリティリスクを把握するためには、まずは事業を継続する上で重要な資産を特定することが求められます。また、法令及び業界内の安全基準等を遵守する観点からも組織として守るべき資産（例えば、個人情報やマイナンバーなど）を特定する必要があります。サイバー攻撃の対象となる資産は、個人情報だけではなく、組織の重要な営業秘密に関する情報や技術情報も含まれることに留意すべきです。

守るべき資産とは

企業の多くの部門には、サイバーセキュリティの脅威から守るべき様々な資産があります。部門が保有する業務情報の機密性や、部門で管理している社内向けあるいは社外向けシステムの可用性が損なわれると、その部門の業務だけでなく企業全体の事業継続に支障をきたす可能性があります。

守るべき資産は、例えば情報だけを取り上げてみても、クレジットカード番号、氏名、有効期限、セキュリティコードの情報のように、それ自体が経済価値を持つものに限りません。より広範囲の業務関連情報が、守るべき資産に該当します。守るべき資産の例として、企業の様々な部門で保有されている情報を以下に挙げます。

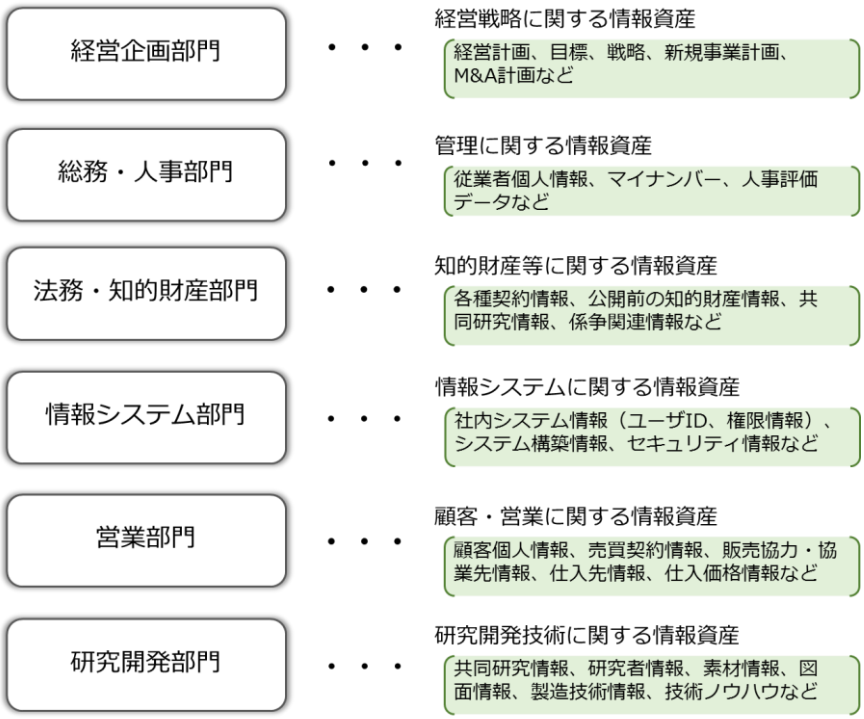


図 3－1　各部門で保有している資産の例示

守るべき資産の特定

重要情報は、組織の中の様々な部門に存在することが考えられるため、一般的には、CISO等が部門ごとに取りまとめを行う責任者（部門責任者）を設置し、この部門責任者が自らの部門に存在する資産を洗い出し、守るべき資産を特定します。他部門が所有する資産等、資産を洗い出す作業を行う担当者が直接利用しない資産については、その資産の価値がわからないケースがあるため、重要情報を作成した部門や担当者が、資産価値を判断することを検討します。ただし、情報の作成者は、自らが作成した情報の重要度を高く設定する傾向があるため、どのような資産がどの程度の重要度であり、どのように保護すべきかについて組織全体の考え方を統一したりサンプルを示したりするなど、情報の重要性についての認識を合わせる必要があります。

法令等による要求事項の明確化

守るべき資産の管理がずさんであった場合など、情報漏えい等の事故を起こしてしまうと法令違反[12]になることがあります。また、法令違反ではなくとも、サイバーセキュリティ上の脅威に起因する営業秘密の漏えいや、社外に供給しているITサービスの停止などのインシデントについて、法的責任を問われる可能性があります。営業秘密が漏えいしていなければ保持できた競争優位性を失い（あるいは、IT サービスが停止しなければ獲得できた営業機会を失い）、本来得られた筈の利益を逸失したのは経営者本人（あるいは担当取締役本

[12] 例えば、個人情報取扱事業者は、法の定める義務に違反し、主務大臣の命令にも違反した場合には、刑事罰として 6 ヶ月以下の懲役または 30 万円以下の罰金が課せられます。

人等）の責任であるとして、株主代表訴訟に発展するケース等がこれに該当します。守るべき資産に関して、法令違反のリスクや訴訟リスクを予め検討し、法的な要求事項を明確に把握しておくことが望ましいと考えられます。

なお、守るべき資産の管理以外にも、セキュリティポリシーの策定や従業員向けの研修等、実施した対策についてのエビデンスだけでなく、できる限りプロセスも含めて記録しておくことが重要です。万一インシデントによって訴訟になった場合に、証拠として残しておくことで企業や経営者等を守ることにつながるからです。また対策を実施していたとしても、記録が残っていない場合、適切な対策を取っていたことを証明できず、訴訟において不利になる可能性もあるため注意が必要です。

情報のライフサイクルに着目した資産のリスト化

守るべき資産は、組織内の各部門で存在し、日々作成、修正されます。また、作成時点から破棄に至るまで重要な情報である場合と、ある時点までは極秘扱いの情報が一定の期間の後に一般公開扱いとなる知的財産権のような情報等も存在します。そのため、各部門で取り扱っている情報の洗い出しをする際には、情報のライフサイクルに着目して、組織全体で守るべき資産を洗い出し、リスト化する必要があります。

ネットワーク上の守るべき資産の特定

守るべき資産が特定できたら、その資産がどこにあるかを把握する必要があります。サイバー攻撃は、インターネット等の外部のネットワークを通じて実施されることが多く、攻撃が成功した場合、組織内のネットワークへの侵入等を通じて情報が外部に漏えいするような被害に至ります。印刷された書類やUSBメモリといった物理的な資産は、どこにあるかを把握しやすいと考えられますが、電子化された情報はネットワーク上のどこに保管されているかを把握することが比較的難しく、その特定はサイバーセキュリティ対策を講じる上で重要です。把握しやすく、管理しやすい方法としては、ネットワーク内の特定の場所に一元管理し、その場所へのアクセスを制御するとともに、アクセスした記録（ログ）を保存し、アクセスした機器や人物を特定、追跡できるようにする方法があります。その他情報が複製できず、持ち出すことができないようなシステムを利用することなどの対策を検討します。

3-2 サイバー攻撃の脅威を識別

サイバー攻撃の具体的な事例や脅威及び脆弱性については、新聞の記事、過去のトラブルなどを収集し、必要に応じて、公的機関やセキュリティ関連事業者が公開している情報（脅威分析や脆弱性分析等）やホワイトペーパー等も収集します。サイバー攻撃の傾向は日々推移しており、できるだけ最新の情報を参考にすることが重要です。IPAでは毎年「情報セキュリティ10大脅威」として直近1年間に国内のIT利用者に影響を及ぼしている代表的な10種類の脅威を紹介しており、傾向を把握するのに役立ちます。このほか、特に被害の大きな脅威などが出現した場合は個別に特徴や対策などを説明しているので、付録２で紹介

している情報を参照してください。なお、サイバー攻撃による被害の事例については、本解説書別添の被害事例集を参照してください。

サイバー攻撃の事例に関する情報収集とは別に、自組織で利用している情報システムやソフトウェアの脆弱性に関する情報を収集することも重要です[13]。脆弱性情報については、その脆弱性を悪用する攻撃が行われた場合に想定される影響度が記載されている場合が多く、自らの組織に対する影響を知ることができます。

3-3 リスクの把握

守るべき資産とサイバー攻撃の脅威の識別結果を参考にして、自組織でも可能性のあるリスクを検討します。特に、事業継続に関わる重要なシナリオを明らかにし、そのシナリオに関する対策を検討する必要があります。サイバーセキュリティリスクは、経営リスクに直結する場合もあるため、そのリスクを把握・分析し、経営者とサイバーセキュリティリスクを共有しておく必要があります。経営者がリスクについて理解を深めるために、ビジネスへの影響度（主な業務の停止等によるビジネスインパクト）を分析する手法があります。

適切なリスク分析の重要性

リスクの把握は、サイバーセキュリティへの対応計画策定の大切な第一歩です。もしこの段階でリスクの把握に大きな漏れが生じたり、影響度合いの評価を大きく誤ったりすると、対応計画が不適切になり、業務や事業の継続が困難になる可能性もあり得ます。適切なリスク分析の重要性を、改めて認識することが重要です。

ともすれば、リスクの把握や分析に膨大な作業やコストが掛かることがあります。それを避けるあまり、例えば守るべき資産の一部しか分析の対象としなかったり、逆に守るべき資産の網羅性ばかりを重視し、個々の資産の分析に十分なコストを掛けず、表面的・形式的な分析で事足れりとしてしまえば、せっかくのセキュリティ投資も効果を発揮せず、無駄なものになってしまうおそれがあります。

また部門ごとに個別にセキュリティ投資を行っている場合、過不足や偏りが発生し、全体最適になっていない可能性があります。このため、全社的な観点から正確なリスクの把握や分析を実施することで、結果的には組織全体のセキュリティコストが下がることがあります。なお、正確なリスクの把握や分析を自らの組織だけで実施することが難しい場合は、外部の専門家に委託することも検討します。

リスク分析手法の種類について

ISMSにおいて参照されることが多いITセキュリティマネジメント[14]のガイドラインでは、

---

[13] 例えば、脆弱性情報については、IPAの重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html やJPCERT/CC 注意喚起 http://www.jpcert.or.jp/at/ 等で入手できます。

[14] 第3部：ITセキュリティマネジメントのための手法（JIS TR X 0036-3:2001）

ベースラインアプローチ[15]、非形式的アプローチ[16]、詳細リスク分析、及びこれらを組み合わせたアプローチがあることが述べられていますが、本解説書ではその概要を示すに留めます。リスク分析の手法については様々な参考書やガイドラインが出ていますので、自社の扱う情報資産の価値やセキュリティの成熟度に応じて、適宜リスク分析の手法を選択してください。

表 3－1　リスク分析手法の種類

名称	概要（長所／短所）
(1)ベースラインアプローチ	既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある。
(2)非形式的アプローチ	コンサルタント又は組織や担当者の経験、判断によりリスク分析を行う方法。短時間に実施することが可能であるが、属人的な判断に偏る恐れがある。
(3)詳細リスク分析	情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスクを評価していく。 厳密なリスク評価が行えるものの多大な工数や費用がかかる。
(4)組合せアプローチ	複数のアプローチの併用。よく用いられるのは、(1)ベースラインアプローチと(3)詳細リスク分析の組合せ。ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる。

事業継続を踏まえたビジネスインパクト分析

一般的にビジネスインパクト分析（BIA：Business Impact Analysis）[17]は、組織における重要な事業や業務及びプロセスと関連するリソースを特定し、事業継続のための脆弱性分析とリスク分析を行い、影響度に応じたリスクの低減策等を検討します。事業への影響度については、収益や試算に対する金銭的な影響だけでなく、顧客や取引先または株主などのステークホルダーに与える影響や、企業のブランドや社会的責任に及ぶ影響も含みます。ビジネスインパクト分析は、業務・プロセスと業務を遂行するために必要となるリソースをもとに、その業務が停止した場合等について事業上の影響を分析するため、顧客への影響や収益の影響など経営者に理解しやすい分析結果を提示できます。例えば、EC サイトに対する不

[15] ベースラインアプローチ、詳細リスク分析、組合せアプローチに関する詳しい解説は、「情報セキュリティ対策ベンチマーク活用集（付録）」、情報セキュリティ対策ベンチマーク普及検討会編を参照。

[16] 非形式的アプローチに関する詳しい解説は、「ISMS ユーザーズ・ガイド ―JIS Q 27001:2006（ISOS/IEC 27001:2005）対応－」、一般財団法人日本情報経済社会推進協会を参照。

[17] ビジネスインパクト分析に関する詳しい解説は、「事業継続管理（BCM）に関する利用ガイド」、一般財団法人日本情報経済社会推進協会を参照。

正アクセスがあり、約 10 日間の停止による損害（売上減、機会損失、その他の謝罪対応、調査費用等を含む）が 1 億円と想定される場合、どの程度の費用を掛けてサイバーセキュリティ対策を行うべきかについて検討する際の目安とすることができます。これらの情報や分析結果を経営者と共有、検討するだけではなく、事業部門とも共有、検討を行うことでサイバーセキュリティリスクが事業に与える影響度について共通認識を持つとともに、こうした関係者間でサイバー攻撃を受けた場合の対処方法を予め想定しておくことが可能となります。

❑ 参考データ「自社の経営リスク分析の実施状況・外部サービス利用状況（国内調査）」

「リスクの把握」では、リスクの分析や把握の重要性を示しました。一方、国内企業のサイバーリスク管理の実態調査[2]では、自社の経営リスク分析を行っているという回答は、大企業（経営者）が 49.2%、中堅企業（経営者）が 28.2%、中小企業（経営者）が 14.9%であり、大企業に比べ中小企業は自社の経営リスク分析を行っていない傾向にあります。

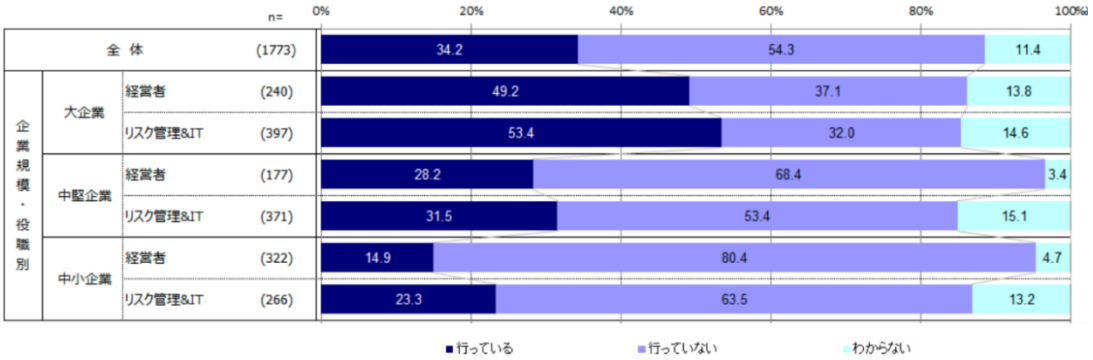


図 3－2 自社の経営リスク分析の実施状況（国内調査）

(引用) 企業におけるサイバーリスク管理の実態調査 2015、独立行政法人情報処理推進機構

[コラム] 企業が抱えるリスクとは？

企業が抱えるリスクには、様々なものがあり、自然災害や重要インフラの麻痺等によって事業活動が停止することも考えられます。事業継続や拡大がミッションである経営者は、このような事態を招くリスクに対応できないことによる事業活動の停滞や、経営が困難になるような事態を避ける必要があります。

米国では、このような企業の抱えるリスクを適切にコントロールするために、経営者の重要なミッションに企業のリスク（コーポレートリスク）への対応があると認識されています。最高リスク管理責任者や危機管理担当役員（CRO：Chief Risk Officer）を任命し、統合的リスクマネジメント（ERM：Enterprise Risk Management）の観点でリスクを捉えている企業もあります。

一方、日本でも有価証券報告書等において様々なリスクへの対応を株主やステークホルダーに開示するようになり、その一部として情報システムに関するリスクやサイバー攻撃のリスク等も記載されています。

今後、コーポレートリスクのひとつとしてサイバーセキュリティリスクが認識され、サイバーセキュリティリスクへの対策を強化していく企業が増えていくことが期待されます。

3-4 リスク対応計画の策定

識別したリスクに対して、サイバーセキュリティリスクが事業に与える影響を考慮した上で、リスクの対応方法を検討し、リスク対応計画を策定します。

リスク対応方法の検討

リスク対応には、大きく分けて①低減、②保有、③回避、④移転があり、事業に与える影響の度合いに従いこれらの対応方法を決定します。

① 低減（適切な管理策の採用）
脆弱性に対してサイバーセキュリティの様々な対策を講じることにより、脅威発生の可能性を下げることです。例えば、マルウェア対策ソフトを導入する、外部記憶媒体の接続を制限する等が該当します。

② 保有
リスクの持つ影響力が小さいため、特段リスク低減のための対策を講じず、許容範囲内として受容することです。この保有には、「許容できるリスクのレベル」を

超えるものの、現状において実施すべき対策が見当たらない場合や、資源（予算、人材等）に見合ったリスク対応の効果が得られない場合にリスクを受容することも含まれます。このようなリスク（対策を講じた後に残ったリスク、および対策されずに残ったリスク）は、残留リスクとも言われます。

③ 回避

脅威発生の要因を停止あるいは全く別の方法に変更することで、リスクが発生する可能性を取り去ることです。例えば、外部からの不正アクセスという脅威に対し、機密情報が保存されているサーバは外部接続を行わないこと等が該当します。

④ 移転

リスクを他者などに移すことであり、保険の活用や守るべき資産を外部の専門企業へ委託すること等が該当します。

なお、図３－３に示すとおり、一般的にリスク発生可能性が高いもの、あるいはリスクが発生した場合の損害が大きいものについては、低減、回避、移転などの対応を検討します。

一方、リスク発生可能性が低く、かつリスクが発生した場合の損害が小さいものについては、対策を取らず残留リスクとして保有（受容）します。また特に「許容できるリスクのレベル」を超えているが、対策をしないで保有する残留リスクは、経営的な判断が必要になる場合があるため、経営層がその残留リスクは受容できる範囲であることを承認する必要があります。

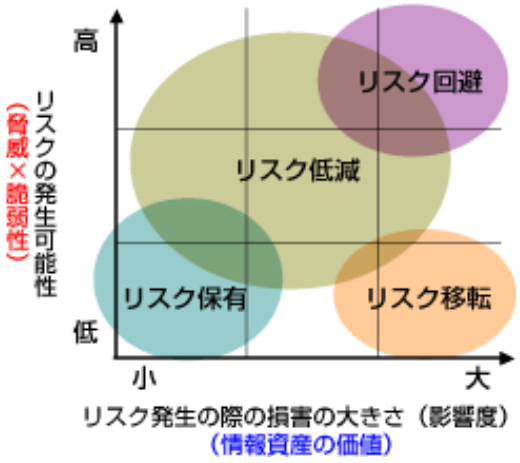


図 ３－３　　リスクへの対応

リスクに応じた対策の目標と対応計画の策定

セキュリティポリシーの対応方針やリスク分析の結果などを基に、CISO 等が主体となり対策の目標と対応計画を策定します。

策定時には、いかにサイバーセキュリティリスクを回避・低減できるか、という有効性の検証だけではなく、IT システムの利用制限によって業務の効率性を過度に損ねないこと（可用性）等についても十分考慮します。

また予算や人材等の資源には限りがあるため、あらゆる対策を一斉に講じることは現実的ではありません。目標と対応計画を策定する際は、対策に優先順位を付けて、誰がやるか、いつまでにやるか、どこまで達成すればよいか等の項目を検討します。

[コラム] サイバー保険とは

サイバー攻撃は、どれだけ対策を万全にしたとしても、完全に防ぐことはできない（リスクをゼロにできない）ため、リスクの一部を他者へ移転することも有効な対策となります。リスク移転の方法の１つとして「サイバー保険」があります。

自動車保険や火災保険と同様にサイバーリスクに対応するサイバー保険が、近年複数の損害保険会社から提供されるようになってきました。

現状におけるサイバー保険の一般的な補償内容は、

- 個人情報や営業秘密などの情報漏えいに関する損害賠償
- 不正アクセス等に関する原因調査費用や消失したデータの復旧費用
- ネットワーク中断に関わる利益損害　等

といった商品設計になっています。また調査・応急対応支援やコールセンター設置支援等、加入者のニーズに合った専門事業者を無料で紹介するサービスが付帯されている場合もあります。

なお、保険料（掛け金）は、補償内容や業種、売上高等に応じて異なりますが、保険会社によっては、加入者のセキュリティ対策状況に応じて（例.本ガイドラインのチェックシートの項目を満たしている、ISMS 認証を取得している等）保険料を割り引く制度があり、サイバー保険の加入者が適切なセキュリティ対策を講じる動機付けとなることが期待されています。

[コラム] 多層防御の実施

サイバー攻撃のすべてを未然に防止することは難しく、組織が考えるべき対策は、未然防止の対策だけではなく、サイバー攻撃を受けた事後の対策も必要になります。サイバー攻撃の発覚（感染など）が攻撃の終了ではなく、攻撃を発見し対応を始めた後も攻撃が継続している可能性もあります。感染後の被害回避や低減のために、予め侵入や被害拡大防止を考慮した複数の対策を多層に重ねる「多層防御措置」を検討する必要があります。

具体的には、業務で利用している端末において、OS やアプリケーションソフトウェアなどを常に最新の状態に保つことで業務利用端末等のマルウェア感染等のリスクを低減する（図①）、重要情報を保存しているサーバについてはネットワークを分離する（図②）、自組織内から外部へ出ていく通信ログを保存し確認するなど、侵入された場合を想定した出口対策を行うことにより被害を局所化する（図③）、標的型攻撃メールでよく用いられる実行形式ファイルが添付されたメールを受信拒否するなど、標的型攻撃に対してより強固な対策を検討する（図④）などといった複数の対策を組み合わせることが考えられます。

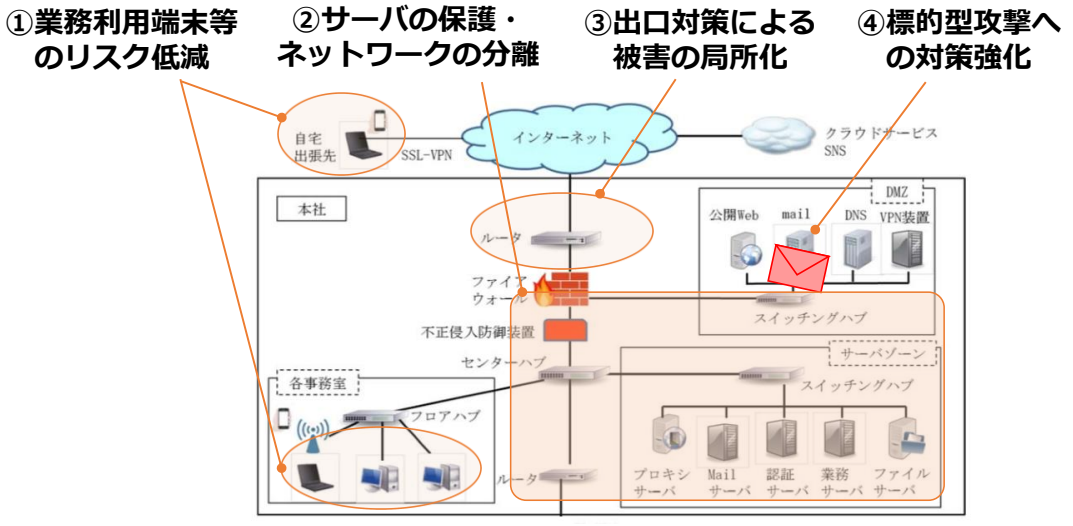


図 3－4 多層防御の概要図

企業例示「リスク対応の検討」

仮想企業Ａ社及びＢ社で、リスク対応について検討、実施した内容やポイント等を示します。

企業Ａ社のリスク対応の検討　　EC サイト運営（中小企業）

守るべき資産の特定

セキュリティポリシーの検討の過程で、A 社の重要保護資産は、A 社自身の通販サイトの会員顧客の個人情報と、ネット通販業者がお客様である EC サイトのシステムそのものであるとの認識ができました（１章企業例示参照）。

守るべき資産として特定すべきものは、この重要保護資産だけに限りません。この二つの資産を守るために、二次的に守るべき資産が存在します。それらをもれなく特定するため、EC 運営部門と情報システム部門から担当者を出し、共同で特定作業を行う事になりました。

さらに、上記の重要保護資産を守る上で二次的に守るべき保護資産とは別に、それ自身守らなければならない資産が他にある可能性を考え、ほかのすべての部門（総務部門、営業部門）でも担当者を置いて、特定作業を行う事にしました。

二次的な保護資産の特定

二次的な保護資産を特定した結果は、次のようになりました。

- A 社自身の通販サイトの会員顧客の関連情報

  顧客の氏名、生年月日、住所、電話番号、メールアドレス等のいわゆる「個人情報」の他、購買履歴の情報や、マーケティングに使う目的で記録している商品の閲覧記録も、広義の個人情報であるとみなす事にしました。

- A 社 EC サイトシステムの構成要素

  EC サイトシステムの可用性は構成要素（ショッピングカートサブシステム、商品管理サブシステム、問合せ管理サブシステム、顧客管理サブシステム、受注管理サブシステム、及びそれらに付随するデータベース）や、EC サイトシステムのプラットフォームとなっているサーバ、ネットワーク機器等の可用性に依存します。これらサ

ブシステム等も保護資産となります。守るべき資産の特定の後は、脅威の識別、リスクの把握と作業を進めますが、EC サイトシステムについては、これら構成要素等ごとに検討を進めることになります。

重要保護資産以外で、それ自身守るべき資産の特定結果

A 社のすべての部門で、重要保護資産以外の保護資産の特定を行う際、取り掛かりのヒントにしたのは法令等による要求事項でした。

A 社のすべての部門に関係する法律には、個人情報保護法があります。総務部門、営業部門の特定作業担当者は、各部門が保有している情報が個人情報に該当しないか再度洗い直しを行うことによって、改めて下記の保護資産等を見つけました。

- 総務部門
  社員の属性情報（住所、氏名、年齢、人事考課、給与額等）
  健康管理室利用履歴（誰が、いつ、どんな症状で利用したか、問診内容等）

- 営業部門
  EC サイトテナント見込み客への販促活動履歴（顧客候補の担当者の個人情報等）

企業 B 社のリスク対応の検討　**電子機器製造（大企業）**

守るべき資産の特定

多数の事業を行う企業の作業体制

B 社が製造する電子機器は、家庭用プリンターやパソコン外付けハードディスクドライブを例とする一般コンシューマ向けの製品から、業務用無線の基地局通信装置や各種生産ラインで使われる流量センサー等を例とする産業用機器に至るまで、非常に多岐にわたっています。お客様も、一般家庭、装置会社やサービス会社等様々で、製品の流通経路も異なります。こうした違いに対応するため、B 社は製品分野ごとに別々の事業部を設置し、その配下に製品ごとの担当部を作っています。

製品の違いを考慮に入れた上で、守るべき資産を特定し、脅威を洗い出し、経営・事業

へのリスクを把握するのは、その製品を担当している事業部・製品担当部自身が行わなければ、不正確になります。そこで、経営リスク管理委員会の事務局であるリスク管理部（１章企業例示を参照）は、リスクの把握と対応計画の策定の全社推進役を担い、事業部等の部門ごとの保護資産特定の作業は、部門自身が配下の組織の中に作業グループを編成し、実施するという分担にしています。

リスク管理部はまた、リスク把握・対応計画策定の年間予定を立案し、それに則って各部門の作業の進捗管理を行います。また、守るべき資産特定の結果をレビューして、内容が正確か、洗い出しに漏れがないか・ムラがないか等を検討し、その結果によっては、対象部門の作業指導を行います。

各部門での保護資産特定の事例

各部門の保護資産特定の作業グループは、各部の資産を調べて、

- 機密性・完全性を維持すべき個人情報に相当するデータ
- 機密性・完全性を維持すべき営業秘密
- 完全性を維持すべき、製品・半製品等
- 完全性・可用性を維持すべき、部ごとに管理している IT システム

等に該当しないか、検討を行います。

下記は、各部が特定した保護すべき資産の例です。リスク管理部の部員や、事業の実情を知らない他の部門の社員には、洗い出す事が難しいものが含まれていることに注目してください。

- （広報部：個人情報）B 社製品情報公開・ヘルプデスク Web システムの製品登録ユーザー情報（機密性・完全性）
  B 社製品登録ユーザーの氏名や連絡先等の個人情報であり、個人情報保護の観点から機密性を守る必要がある。

- （人事・総務部：個人情報）社員の個人情報、人事評価結果（機密性・完全性）
  社外関係者の情報に限らず、社員の情報も個人情報保護の観点から機密性を守る必要がある。

- （製造技術部：営業秘密）半導体製造装置の動作パラメータ及び歩留まりデータ（機密性）

  製造装置の動作パラメータ設定値のわずかな違いによって、製造する半導体の不良品発生量が大きく変わり、それが事業の利益率に大きな違いをもたらす。動作パラメータ設定値と歩留まりデータは、半導体事業の重要な営業秘密であり、機密性を守る必要がある。

- （アフターサービス部：製品）B 社 IT 製品のダウンロード用パッチ（完全性）

  製品のファームウェアなどをバージョンアップした際に、ユーザー自身に B 社 Web サイトからダウンロードさせ、交換させる為のパッチファイル。他社のセキュリティインシデントに、こうしたパッチが改ざんされ、ユーザーの重要情報を抜き取って収集する機能が製品に不正に混入された例があり、完全性を守る必要がある。

４ PDCA サイクルの実施と対策状況の開示

サイバーセキュリティ対策のフレームワーク（PDCA）を構築し、必要に応じて自らの組織の対策状況等を開示します。

実施内容４
１．組織内外の環境変化に応じた取組みを実施できるよう PDCA を構築する。 ２．組織内のサイバーセキュリティ対策の状況を把握し、CISO 等が経営者に対して定期的に報告する。また必要に応じて経営者が改善のための指示をする。 ３．ステークホルダーから信頼を得るために必要な情報を適切に開示する。

４-１　環境変化に応じたフレームワーク（PDCA）の構築

セキュリティポリシー（１章）や、サイバーセキュリティリスク管理体制（２章）、及びリスク対応計画策定（３章）などに基づく対策を PDCA として実施するフレームワークを構築し、環境の変化に応じて効率的に機能させる必要があります。

フレームワーク（PDCA）の構築

フレームワークを構築するための手法として PDCA があります。PDCA は、Plan（計画） ― Do（実行） ― Check（確認） ― Act（改善）の略です。PDCA は、品質改善や環境マネジメントでもよく知られた手法で、以下のステップを繰り返します。

1. Plan：問題を整理し、目標を立て、その目標を達成するための業務計画を立てます。
2. Do：目標と計画をもとに、対策を実行します。
3. Check：実行した対策が、計画通り行われて当初の目標を達成しているかを確認し、評価します。
4. Act：評価結果をもとに、業務の改善を行います。

例えば、サイバーセキュリティへの対策では、リスクの把握、目標と対応計画策定（３章）や予算確保・人材配置及び育成（６章）が、計画（Plan）にあたり、この計画に基づき対策を実行（Do）し、実行の結果を確認（Check）し、改善（Act）することで環境の変化に応じたフレームワークが構築できます。

一般的には、セキュリティ管理の主管部門やチームが PDCA のサイクルを設定し、そのサイクルにあわせて、各部門の責任者を通じて、各担当者に PDCA の実施を指示します。

サイバーセキュリティの対策は一度実施したら終わりということはなく、常に対策を改善し、効率化しないと、新たな脅威に対応できないという側面をもっているため、環境の変化に合わせて、絶えず見直しと改善が求められます。組織のサイバーセキュリティ対策における目標達成レベルを継続的に維持改善するために、PDCA サイクルを繰り返します。

フレームワーク（PDCA）のサイクル

情報セキュリティマネジメントシステム（ISMS）等では、PDCA のサイクルは、通常１年間とするケースが多く、この１年ごとのサイクルは、企業や組織における年度計画の見直しとタイミングが同じであるため、馴染み易いサイクルです。一方、昨今の環境変化は短期間に発生する場合もあり、未知のサイバー攻撃への対応などを考慮すると、さらに短いサイクルで見直しを実施することも検討します（次ページコラム参照）。

計画見直し方法の検討

多くの企業は、自社が抱えるリスクに関して何らかの取り組みを実施していると考えられます。これら既存の取り組みを最大限活用して、サイバーセキュリティリスクへの対応にも、効率的に効果を発揮させることが可能なケースも少なくありません。

例えば、新規の事業を実施するため取引先から重要な情報を預かる場合や、重要な情報を自組織の複数の部門で共有する場合の情報管理方法については、重要情報の入手や管理に関する手順書を参照して、既存の情報資産台帳の管理主体や資産利用の許容範囲等を確認したり、複数部門との情報共有の方法などを確認し、必要に応じて（実際の業務に照らし合わせて）見直しを行う、といったケースがそれにあたります。

また、PDCA を実施したことがない組織は、計画（Plan）から始めるのではなく、まずは現状のサイバーセキュリティの対策を確認（Check）することから始めることも検討します。

一般に、同じ企業においても、情報セキュリティを所管する部門（例えば情報システム管理部門等）では比較的 PDCA サイクルが機能している割合が高くなりますが、そうでない部門では PDCA サイクルが機能してないケースも見受けられます。セキュリティリスクが高い部門を優先して、PDCA サイクルの機能性を高める努力が必要になります。

さらに、CISO 等や CRO 等が定期的に異動するような組織の場合には、役職者や責任者の交代によって体制が大きく変わる、またはサイバーセキュリティリスクの取り組みへの注力度合いが大きく変わる可能性もあります。このような場合には、セキュリティへの取り組みを経営課題のひとつとして捉え、監査役の内部監査を受ける対象とすることで、PDCA サイクルの実効性を高める工夫もあります。その際には、監査役がサイバーセキュリティに対する社外の専門家の助言を受けるようにすると良いでしょう。

[コラム] PDCA と OODA

PDCA（Plan、Do、Check、Act）は、一般的に計画(Plan)から開始し、Do（実行）し、Check（評価）した後に Act（改善）するものだとされています。このため、計画から見直しが長期になり、改善が遅れることや計画されていない場合の対処の遅れが指摘されています。このような場合に、OODA ループを適用することにより、状況観察から判断や実行を早めることができます。OODA ループは、米国空軍が考案した意思決定の方法であり、観察（Observation）、情勢判断（Orientation）、意思決定（Decision）、実行（Action）の流れを繰り返すループです。

計画からスタートする PDCA に比べ、観察、情勢判断からスタートするため、状況に応じ、より柔軟性をもった判断を行うことが可能であり、意思決定から実行までのスピードも早くすることができます。この OODA ループは組織経営への適用も検討されていますが、サイバー攻撃への対処についても参考になります。

4-2 対策状況の把握

対策状況の把握には、平常時に行う全社に対する定期的な対策状況の把握と、インシデント発生時に行う関係部門に対する集中的な対策状況の把握の二通りがあります（後者については９章を参照してください）。

対策状況の把握方法

定期的な対策状況の把握では、３章で策定したリスク対応計画に基づき、各部門の責任者や従業員がセキュリティポリシーを正しく理解し、セキュリティポリシーに規定された対策を正しく実施しているかを確認します。セキュリティの所管部門が、確認項目のチェックシートを作成して、確認対象者に配布し自己点検させた結果を集約する方式や、チェックシートに基づいて所管部門の担当者が直接巡回して確認する方式などがあります。

経営者への報告内容

経営者への報告で最も重要なことは、経営者が自らの組織の対策状況を把握できるということです。したがって、報告に含まれる情報量が多く詳細であるからといって、経営者への報告が適切であるとはいえません。

経営者と CISO 等は予め、どのような情報をどのようなタイミングで報告すべきかを合意しておく必要があります。経営者が求める内容が、PDCA のサイクルにあわせた定期的な報告であれば、計画に照らし合わせた対策状況を報告します。

また報告内容には、２つの視点が考えられます。１つは、事業への影響度や情報の重要度に合わせて、どのようなリスクをどの程度低減できているかという視点です。もう１つは、環境変化や新たな脅威の発生と対応という視点です。

事業への影響度に合わせた報告では、事業への影響度が高い内容の報告（例えば、顧客情報管理リスクの状況等）に重きを置くことが必要です。一方で、環境変化や新たな脅威の発生と対応状況を把握する視点では、インシデントに至らなかったヒヤリハットなどの内容や件数を報告し、新たな脅威に対して未然に対策を打つための情報を提供することが必要です。

経営者が対策状況を正しく把握できるような報告をするためには、報告内容に応じた経営者へのエスカレーションを考える必要があります。このため、CISO 等が情報の集約を行った上で、経営者に報告します。必要に応じて事業目標や戦略への影響評価も添えて、経営者に報告することが、CISO 等に求められる役割です。

ヒヤリハットの報告は、自組織の対策状況を把握する上で重要ですが、報告者は自らの報告によって罰せられるのではないかと恐れて、報告しない傾向があります。そのため、報告者には軽微なインシデントを含めすべての報告を促し、報告を上げたことに対してまずは褒める等、報告を上げやすい環境を作ることが必要です。さらに、担当者がインシデントを報告しても、自部門に都合が悪いと判断する部門責任者が、情報を故意にエスカレーションしない場合を想定し、体制を整備するだけでなくエスカレーションすべき基準を明確にすることが重要です。

KPI の設定・モニタリング

経営者が、サイバーセキュリティ対策に関する全体状況を掴めるよう可視化する手法の１つとして、サイバーセキュリティ対策に関する KPI[18]の設定・モニタリングについて紹介します。

サイバーセキュリティ対策に関する全体状況には、いくつもの側面があります。たとえば、経営者によるガバナンスの徹底や、リスク管理プロセスの運用、社員のセキュリティ意識の高さなどがその例です。いくつもある個々の状況を、それぞれ言葉で詳細に説明していては、経営者はかえって全体像を見失ってしまいがちです。そこで、それぞれの状況を、簡潔かつ定量的な指標（すなわち KPI）で表現します。

経営者によるガバナンスの状況を表す KPI の例としては、IT 予算全体に対するサイバーセキュリティ対策予算の割合やリスクアセスメント[19]での指摘事項の数等が挙げられます。また、リスク管理の状況を表す KPI の例としては、セキュリティインシデントの発生数やリスクアセスメントの実施回数等があります。社員のセキュリティ意識の状況を表す KPI としては、セキュリティ教育の受講率や理解度テストの平均得点等が考えられます。KPI は、その企業のサイバーセキュリティに関する主な課題に合わせて、適切なものを設定する必要があります。

KPI の値を定期的に計測し経営者に提示することで、その企業のセキュリティに関する主な課題の現状を、全体的に把握してもらう事ができます。KPI の目標値との乖離や、KPI の増加・減少の傾向は、次の施策を検討する上で有益な情報になり、経営者の意思決定を助けます。

---

[18] Key Performance Indicator: 企業目標の達成度を評価するための主要業績評価指標

[19] リスク特定、リスク分析及びリスク評価のプロセス全体のこと

経営層による評価

経営層は、対策状況について報告を受けた際に、セキュリティリスクが期待通り低減できているか、残留リスクが許容したレベルを超えていないか等を評価します。セキュリティリスクが低減できていない、あるいは新たな脅威が顕在化した等の理由で許容レベルを超えた場合には、経営資源をどの程度投下し対策を強化するか、許容レベルを引き上げるか等を経営層が判断し、必要に応じて見直し・改善を指示します。

内部監査と外部監査

組織の形態に合わせて、サイバーセキュリティリスク管理体制を監査する必要があります。一般的な情報セキュリティ対策等では、組織内部の監査担当者が監査する内部監査と組織外に監査を依頼する外部監査があります。

外部監査は、監査主体が経営者や組織体から独立しているため、客観性と専門性が期待できます。そのため、監査結果の一部を組織の外部に公開する場合には、外部監査を検討します。さらに情報セキュリティ分野では、情報セキュリティ監査制度[20]もあり、監査するための管理基準や監査基準が策定されています。

内部監査には、外部監査のような独立性や客観性はありませんが、その一方で、自組織内の業務を理解した上で実施するため時間短縮が期待できます。そのため、組織内の監査部門など一定の独立性が担保される仕組みで、内部監査を実施する事例も多く存在します。内部監査は、外部監査主体に支払う監査費用が発生せず、内部監査の人員工数が明確でない場合は監査コストが見えにくく、一見コスト的なメリットがあると受け取られる場合もありますが、監査の品質を維持するための内部監査者の教育コストも考慮する必要があります。

また、サイバーセキュリティリスクを経営課題のひとつとして捉え、経営者が取り組むために、２章の企業例示で示した通り、監査役が実施する経営監査にサイバーセキュリティリスクへの対応を含めることを検討することも重要です。サイバーセキュリティリスクへの対応状況に監査役を含めることで経営者が継続的に経営課題として認識する体制を構築できます。

４-３　対策状況の開示

組織内で検討を重ねて作成したセキュリティポリシーを投資家や企業関係者等のステークホルダーに対して開示することによって、その企業がサイバーセキュリティを意識し、適切に対応していることをアピールすることができます。これによって、コーポレート・レピュテーション（企業の評判）の向上が期待できるという指摘があります。

具体的な開示の方法には、サイバーセキュリティの対策状況を各種報告書（CSR 報告書、有価証券報告書等）に記載する方法が一般的です。開示先や開示する内容等を下記に示します。

[20] 経済産業省　情報セキュリティ監査制度 http://www.meti.go.jp/policy/netsecurity/index.html

- **CSR 報告書、サステナビリティレポート**
  - **概要（開示目的）**：CSR 報告書は、企業の社会的責任（CSR：Corporate Social Responsibility）に関する報告書であり、サステナビリティレポートは持続可能性に関する報告書です。社会的責任及び持続可能性の観点から、社会や経済及び環境に関する事業活動、社会貢献について開示します。
  - **開示先**：株主や取引先だけではなく、顧客や社会一般、従業員とその家族等も対象としていますが、これらの対象者以外にも開示されています。
  - **開示内容**：マネジメント体制としてリスクマネジメントやコーポレートガバナンス及びサプライチェーンへの方針や対策状況を記載します。この一部にサイバーセキュリティリスクに関する認識や対応状況を記載する場合もあります。

- **有価証券報告書**
  - **概要（開示目的）**：金融商品取引法に基づいて上場会社が事業年度ごとに作成する会社内容の開示資料です。株式を上場している会社は、各事業年度終了後、3カ月以内に財務局長及び上場証券取引所への提出が義務付けられています。
  - **開示先**：株主、投資家、金融機関及び取引先等を対象としていますが、これらの対象者以外にも開示されています。
  - **開示内容**：企業や事業に関連する課題への取組状況を記載します。「事業等のリスク」の項目にサイバーセキュリティリスクに関する認識や対応状況を記載する場合もあります。

- **情報セキュリティ報告書**
  - **概要（開示目的）**：企業の情報セキュリティの取組の中で社会的関心の高い内容について開示するものであり、情報セキュリティ報告書として単体で公開する場合と CSR 報告書の一部として組み込む場合もあります。
  - **開示先**：顧客や投資家等を対象としていますが、これらの対象者以外にも開示されている場合もあります。
  - **開示内容**：情報セキュリティに関する考え方や、情報セキュリティガバナンス及び対策の計画や目標、実績や評価等を記載します。この一部にサイバーセキュリティリスクに関する認識や対応状況を記載する場合もあります。

例えば有価証券報告書では、情報漏えいのリスクについて、故意や過失だけではなく、サイバー攻撃も想定し、自組織やグループ企業の信頼性や企業イメージが低下すること、顧客の獲得・維持が困難になること、損害賠償やセキュリティシステムの改修に多額の費用負担が生じ、事業に影響を及ぼす可能性があることを記載する企業が多くなっています。

これらの情報を開示する理由や目的としては、経営者が企業や事業のリスクを認識し、対策していることを示すことで説明責任を果たすことが考えられます。これらの情報を開示しない場合には、経営者が企業や事業のリスクを認識していないことや説明責任を果たしていないことを問われる可能性もあります。一方、企業や事業に関する具体的なリスクや対策内容を開示することで攻撃者に有効なヒントを与えることから、リスクを高めてしまう可能性もあり、これらの情報を開示しないという選択も考えられます。また、第三者によっ

て開示する内容を確認しない場合（部分的には監査対象の内容も含みます）には、開示する内容は自己申告であるため、自社にとって不利な情報や関係者との調整が必要となる情報（例えば、事故報告等）を開示しないことも考えられます。このように開示する方法や内容については、開示に伴うリスクも考えられるため、開示する際には組織内の広報部門や顧問弁護士などと検討する必要があります。

企業例示「PDCA の検討」

仮想企業Ａ社及びＢ社で、PDCA を検討、実施した内容やポイントを示します。

企業Ａ社の PDCA　**EC サイト運営（中小企業）**

Ａ社では、PDCA を実施したことがなく、どの程度の間隔で、どのような内容を経営者に報告し、対策や計画の見直しを行うべきかを CISO が検討しました。特に、経営者からは、標的型攻撃メールやばらまき型攻撃メール等のサイバー攻撃が、どの程度、自組織に届いているか？というような、自組織で何が起こっているのかを含めて報告するように指示がありました。Ａ社の検討のポイントを示します。

新たなサイバー攻撃への対策を考慮すると 1 年ごとの PDCA のサイクルでは遅いと考え、経営者への報告は以下のように実施することとしました。

- 四半期ごとに自組織で何か起こっているのかを報告するために、従業員から報告された様々な内容について、事業への影響度で分類、集計し、件数をまとめた結果を CISO から経営者に報告する。
- 半期ごとに CISO から全体的な対策状況を報告する。この報告には、一般的なサイバーセキュリティ対策を含め、どの程度対策されているかを示すために、IPA の情報セキュリティ対策ベンチマークの簡易な成熟度モデルを適用した内容を利用することとした。上記同様に CISO から経営者に報告する。
- 期（1 年）ごとにサイバーセキュリティリスク管理体制の全体の実施内容を含めた状況報告として、リスク管理体制とは独立した内部監査責任者が実施する監査の結果を報告する。

企業Ｂ社の PDCA

電子機器製造（大企業）

Ｂ社では、サイバーセキュリティリスク管理の PDCA と既存の個人情報の保護管理体制の監査を合わせて実施することを検討しました。Ｂ社の検討のポイントを示します。

個人情報の保護管理体制の監査と同時にサイバーセキュリティ管理体制の監査を実施し、個人情報管理体制と合わせた報告会を実施することとした。監査人との打ち合わせの中で、個人情報を取り扱う担当者だけではなく、全従業員を対象とした場合には、メールの誤送信や情報管理不備等のヒヤリハット等の事例も含めた内容が適切に報告されるかという事に注力すべきであることが議論され、以下のように実施することとした。

- ヒヤリハット等の事例を集め、普段の作業で注意すべきポイントを参考にするために些細な内容でも積極的な報告を求めることを全従業員に周知した。また、ヒヤリハットを含んだ報告を受け、集計結果と普段の作業で注意すべきポイントを二ヶ月に１回、全社員に開示した。
- 経営者への報告には、監査結果に上記の情報の経年変化を含めることとした。

サイバーセキュリティの対策状況については、一部の取引先から定期的に開示するように依頼を受けていることもあり、事業部門からも広く一般的に開示することを強く求められた。検討した結果、取引先等の社外の関係者に向けて情報セキュリティ報告書を作成し、その一部を基にした内容を有価証券報告書に記載することを検討することとした。

上記のサイバーセキュリティ対策状況を有価証券報告書に盛り込む検討は、グループ企業の中でも新しい取り組みであり、注目される取り組みとなりました。特に、現状はグループ企業の各社が個別に対策している状況であるため、各社の取組状況や内容をまとめ、先行している対策内容をグループ内に展開することで効率的にグループ全体の底上げが可能であり、グループ横断でサイバーセキュリティリスク管理を検討することとなり、今後は、グループ全体の取組状況を開示することを検討することになりました。

５ 系列企業・ビジネスパートナーの対策実施及び状況把握

系列企業やサプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施状況を把握します。

実施内容５
１．系列企業やサプライチェーンなどのビジネスパートナーを含めたサイバーセキュリティ対策を実施する。 ２．系列企業やサプライチェーンなどのビジネスパートナーにおけるサイバーセキュリティ対策の状況を、監査の実施等を通じて把握する。

５-１ 系列企業・ビジネスパートナーを含めた対策の実施

サイバーセキュリティリスクへの対策は、自社だけではなく、関係する企業（系列企業やサプライチェーン）等のビジネスパートナーを含めて対策する必要があります。この場合のビジネスパートナーには、個人情報の処理を伴う業務の委託先や、営業秘密の提示を伴う物品の調達先などが含まれます。CISO 等は、部門責任者や関係企業と直接やり取りしている担当者に関係企業の対策を実施するよう指示します。

ビジネスパートナーに対してサイバーセキュリティリスクへの対策を求める場合には、依頼する業務の内容や実際に対策を依頼しているかどうかの確認を含め、現状の契約内容を整理する必要があります。一方、系列企業やグループ企業への対策は、サプライチェーン等の外部組織と比較すると取り組みやすいため、まずは系列企業やグループ企業の対策から着手することを検討します。

ビジネスパートナー等との対策実施・連携の検討

自社の重要情報をビジネスパートナーと共有している場合には、ビジネスパートナーから不正に持ち出されてしまうリスクもあります。特にサイバー攻撃では、特定の企業の重要情報を不正に入手するために、まずビジネスパートナーのシステムに侵入し、その後に特定の企業に侵入するといった手法もあり、自社だけではなくビジネスパートナーと共にサイバーセキュリティリスクへの対策を実施する必要があります。

ビジネスパートナーにおいてサイバーセキュリティリスクへの対策を確実に実施するためには、現実論として、サイバーセキュリティ対策の内容を委託契約書等に含め合意する必要があります。サイバーセキュリティリスクへの対策をどの程度求めるのかについては、委託する業務の内容や重要情報の有無等によって異なります。そのため、業務内容や取り扱う情報によって業務を依頼する担当者だけではなく、サイバーセキュリティリスク管理体制の部門責任者や法務部門など、複数の担当者が、ビジネスパートナーに求めるサイバーセキュリティ対策を検討する必要があります。

また、事業の実施については、事業主体者に主たる責任があり、サイバーセキュリティリスクへの対策が施されていない状態でサイバー攻撃を受け、重要情報が漏えいした場合や

業務が遂行できなくなった場合は、第一義的には事業主体である発注者や、事業形態等によっては親会社の責任が問われることになります。

なお委託契約書に記載する項目の例として、中小企業の情報セキュリティ対策ガイドライン 付録３＜ツールＢ＞情報セキュリティポリシーサンプルでは、下記のとおり記載されています。

【委託契約の締結】

1. 当社の社外秘又は極秘の情報資産及び個人情報の守秘義務
2. 再委託についての事項
3. 事故時の責任分担についての事項
4. 委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項
5. 情報セキュリティ対策の実施状況に関する監査の方法とその権限
6. 契約内容が遵守されない場合の措置
7. 事故発生時の報告方法

[コラム] サプライチェーンの上流が果たすべき役割

現在のビジネスは様々な関係者との繋がりの上に成り立っています。自社単独で実現できる事業は少なく、サプライチェーンなどの関係者との繋がりが無くなってしまうことは事業が継続できなくなることを意味します。このような関係のなかでは、事業において連携するだけではなく、サイバーセキュリティにおいても共に対策する必要があります。

サプライチェーンの上流は下流に対して、自らの重要情報を共有する場合には、どのような情報が重要であり、どのような保護・対策をすべきであるかを明確に示し、契約書に記載する必要があります。

また、サイバーセキュリティでは、サプライチェーンの下流から侵入し、上流の重要情報を入手するといったサイバー攻撃もあり、サプライチェーンの関係者全体にわたって外部からの侵入を防止する対策を実施することも重要になります。

その一方で、サプライチェーンの上流が求めるサイバーセキュリティの対策費用は、サプライチェーンの上流での調達費用に反映されるため、サプライチェーンの上流は、下流のサイバーセキュリティの対策費用を負担することも含めて、対策レベルの向上を検討する必要があります。

サプライチェーンの下流に対して、対策を一方的に押し付け、責任を転嫁するのではなく、対策費用の負担割合等も考慮しながら、サイバーセキュリティ対策を共に向上させるという考え方に転化することで、より詳細な対策を実施することができます。

例えば、自社が利用しているシステムを提供し、そのシステムで情報を共有することで自社と同じセキュリティ水準にするだけではなく、自らがアクセス制御の設定を行うことで、アクセス状況やアクセスログを確認することができます。このような形式により共同でサイバーセキュリティ対策を向上させる活動が増えつつあります。

5-2 ビジネスパートナーの対策状況の把握

系列企業やサプライチェーン等のビジネスパートナーに求めたサイバーセキュリティ対策が確実に実施されていることを確認します。

ビジネスパートナーの対策状況を把握する方法

対策状況を把握する方法は、大きく分けて次の３種類あります。

① **ビジネスパートナーから状況報告を受ける方法**

ビジネスパートナーによる自己点検がこれに該当します。対策として求める事項をチェックシートとして相手方に提示し、相手方はそのチェック項目をもとに自己点検を行い、結果を報告します。ビジネスパートナーが虚偽の報告を行い、その結果情報漏えい事故が発生した場合には、相手方の責任を問うことはできますが、対策が適切に実施されているかどうかの判断にはどうしても解釈に差が生じがちであり、あくまで相手方の主観的な判断に依存せざるを得ない点に留意する必要があります。そのため、重要情報を扱わないビジネスパートナーを対象として、サイバーセキュリティ対策状況を定期的に簡易な形で確認する場合に適しています。

② **自社がビジネスパートナーの対策状況を確認する方法**

自社の担当者が自らビジネスパートナーの事務所等を訪問し、対策状況に関する確認、監査を行う方法です。自社においてこうした対応に要する費用や人的リソースを確保しておくほか、訪問調査を実施することについて、契約段階で相手方の了解を得ておく必要があります。一方、この確認方法は、対策を求める側が自ら確認できることから、サイバーセキュリティ対策の状況について確実に把握することができます。

③ **第三者がビジネスパートナーの対策状況を確認する方法**

第三者（外部監査含む）が確認、監査する方法で、こうした外部への確認、監査に関する委託費用を確保する必要があります。第三者の客観的な視点が担保でき、情報セキュリティ監査事業者[21]に委託することで、専門的な観点から対策に関する助言を受けることができます。

上記に示した状況確認を行ったり、報告を受けたりして、求める対策状況に満たない場合、必要に応じて追加的な対策を講じることを求めます。なお、クラウドサービス事業者などの場合、予め定められた約款やサービスレベルで提供するだけで、こうした状況確認や監査を受け入れないことがあります。その場合は、情報セキュリティ対策に関する開示を行っていることが第三者によって認定されている次の各制度の適用対象事業者から、開示されている内容をもとに事業者を選定するとよいでしょう。クラウドサービスについては、７章で詳細について説明します。

- クラウド情報セキュリティ監査制度（クラウドセキュリティ・マーク）[22]

[21] 経済産業省ではこうした事業者を対象とした「情報セキュリティ監査企業台帳」を公開しています。
http://www.meti.go.jp/policy/netsecurity/is-kansa/

[22] 特定非営利活動法人 日本セキュリティ監査協会、クラウド情報セキュリティ監査制度、
http://jcispa.jasa.jp/cloud_security/

- ASP・SaaS/IaaS・PaaS/データセンターの安全性・信頼性に係る情報開示認定制度[23][24][25]

より効果的に対策状況を確認する方法

ビジネスパートナーの対策状況を確認するためには、次の３つの観点が重要になります。

① ビジネスパートナーによる自己確認以外の監査や確認を実施する
前述のとおり、ビジネスパートナーによる自己確認や自己点検では客観的な判断にならないことから、ビジネスパートナーによる委託元組織が自ら訪問調査で対策状況を確認することや、外部監査を行うことで、対策状況を正しく確認することができます。

② 対応の有無をチェックするだけでなく成熟度モデルを適用する
対応したかどうかをチェックするだけでは、実際に有効な対策ができているかどうかの確認ができません。そこで判断基準のひとつの目安として、成熟度モデルを利用することが考えられます。成熟度モデルを適用することで、PDCA を含めどの程度対策されているかを確認することができます（成熟度モデルを適用したチェック項目は、次の企業例示Ａ社の IPA のベンチマーク等を参照）。

③ 自らが情報をコントロールする環境を整える
例えば、自社が利用しているクラウドサービス等で利用できるアカウントをビジネスパートナーにも発行し、同様の対策を施したシステムを共同で利用することで、技術的対策を均一化し、自らがアクセス制御を行い、アクセス状況を確認するなどの方法が考えられます。

企業例示「関係者の対応状況把握」

仮想企業Ａ社及びＢ社で、関係者の対応状況把握について検討、実施した内容やポイントを示します。

企業Ａ社の関係者の対策状況把握　**EC サイト運営（中小企業）**

Ａ社は、ダイレクトメール事業者等のサプライチェーンに対して個人情報を含む重要情報のサイバーセキュリティ対策を徹底するよう依頼し、対策状況を把握する方法を検討

[23] 一般財団法人マルチメディア振興センター、ASP・SaaS の安全・信頼性に係る情報開示認定制度 https://www.fmmc.or.jp/asp-nintei/about.html
[24] 一般財団法人マルチメディア振興センター、IaaS・PaaS の安全・信頼性に係る情報開示認定制度 https://www.fmmc.or.jp/ip-nintei/about.html
[25] 一般財団法人マルチメディア振興センター、データセンターの安全・信頼性に係る情報開示認定制度 https://www.fmmc.or.jp/dc-nintei/about.html

しました。A社の検討のポイントを示します。

現状のサプライチェーンにおけるビジネスパートナーにおいてはコーポレート部門で全社の IT 利用実態を一括管理できておらず、個々の事業部門で IT の利用方針やサイバーセキュリティ対策を管理しているケースがありました。そこで、ビジネスパートナーと直接やり取りしている担当者から相手方のそれぞれに対して依頼している業務に関する IT の利用度を確認しました。

IT の利用度に応じて要求するサイバーセキュリティ対策を示し、対策の実施状況についての報告を受けることにしました。要求する対策は、自社で利用している IPA の「情報セキュリティ対策ベンチマーク」（表５－１に示す 27 問の情報セキュリティ対策状況に関するチェック項目で構成）を利用しました。

- IT の利用度が低い企業については、IT 関連のチェック項目（大項目 3 及び 4 の情報システム関連）を削除し、サイバーセキュリティ対策の状況を確認するように依頼した。
- IT の利用度が高い企業については、同ベンチマークで不足している対策（大項目 5 の事故対応状況）について、「連携体制の構築」及び「訓練の実施」に関するチェック項目を独自に追加し、確認するように依頼した。

さらに、新たな契約時や契約更新時に上記のサイバーセキュリティ対策のチェックについて定期的に報告すること（半年に一回程度）を盛り込むことにしました。

表 ５－１　IPA 情報セキュリティ対策ベンチマークにおけるチェック項目の構成[26]

大項目構成	対応するチェック項目	チェック項目の内容
大項目１	問 1(1)～(8)　８問	情報セキュリティに対する組織的な取組状況
大項目２	問 2(1)～(4)　４問	物理的（環境的）セキュリティ上の施策
大項目３	問 3(1)～(7)　７問	情報システム及び通信ネットワークの運用管理
大項目４	問 4(1)～(5)　５問	情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況
大項目５	問 5(1)～(3)　３問	情報セキュリティ上の事故対応状況

[26] 詳細は右記 URL 参照。http://www.ipa.go.jp/security/benchmark/

企業Ｂ社の関係者の対策状況把握　　**電子機器製造（大企業）**

Ｂ社は、グループ企業をはじめ数多くの関係者が存在するため、以下の共有状態に分けて依頼内容を整理することとしました。Ｂ社の検討のポイントを示します。

個人情報保護管理体制では、各部門の個人情報管理責任者が設置され、定期的に各部門の個人情報保有に関する状況調査を行い、各部門の個人情報管理責任者から管理本部への報告が徹底されています。この報告体制を利用し、個人情報以外の重要情報の有無と外部との共有状況を調査し、各部門の対策状況と外部へ依頼している対策を調査しました。

契約については、法務部門が最終確認するが、契約内容については、事業部門が責任を持ってプロジェクトごとに締結している状況であり、契約書にサイバーセキュリティ対策に関する内容がどの程度記載されているか一元管理されていない状況でした。そこで、上記の調査を通じて、情報共有している企業を特定した結果をもとに、法務部門で契約内容に情報管理やサイバーセキュリティ対策について記載されているかどうかを確認しました。特に、自組織の重要情報を共有している企業との契約内容、他社の重要情報を共有している場合の契約内容、および他社から預かった重要情報を共有している場合の契約内容を調査し、記述内容の統一について検討しました。

自社の特定の事業部門において、重要情報を扱うビジネスパートナーに対しては、自社が利用している外部の IT システムを利用できるように、以下の設定や確認を行うこととしました。

- 自社の管理者がアクセス権限を付与することで、自らアクセス制御を行う。
- これまでは部門単位でのアクセス権限を設定していたが、新たにプロジェクト単位でアクセス権限を設定することで、より詳細に状況を把握することとした。
- 定期的にアクセスログを確認し、万が一、漏えいした場合でも、時期などからある程度の絞り込みや特定ができるようにした。

６ 予算確保・人材配置及び育成

サイバーセキュリティ対策のために必要となる資源（予算、人材等）を確保します。

実施内容６
１．サイバーセキュリティ対策を実施するために必要な対策費用を確保する。 ２．サイバーセキュリティ対策を実施する上で必要となる人材の確保や人材育成の対策を講じる。

６-１ 必要な対策費用の確保

サイバーセキュリティリスク管理体制を構築、維持するためには、当然ながらその体制に要する費用を確保する必要があります。費用は大きく以下の３種類に分類されます。

- 事前対策費用（対策のための製品の調達費用、人材育成費用等）
- 対策運用費用（監視や予防の業務に要する費用、製品の保守費用等）
- 事後対策費用（インシデント対応費用、再発防止対策費用等）

どのようなサイバーセキュリティ対策を行うかを明確にすることで、それぞれの項目で必要となる費用も明らかになります。

対策費用の承認を得るためのポイント

サイバーセキュリティ対策に関する予算や人員計画は、経営会議など経営層の意思決定の場で承認されるべきことです。ビジネスへの影響を踏まえたサイバーセキュリティ対策の検討結果を CISO 等が経営会議などの場に提示し、実施する対策の内容、時期、費用等が適切かどうかといった項目を検討し、経営層の承認を得る必要があります。

経営層が対策費用（予算）を承認するためのポイントは、以下のように整理できます。

- 事業に対するリスク
  サイバーセキュリティの脅威やリスクが、主要な事業に対してどの程度の影響があり、どの程度の対策が必要なのかが明確であること
- 事業推進・品質向上
  サイバーセキュリティへの対応を行い、安心・安全な環境やネットワークを利用することで、自組織が活発に事業を推進でき、事業の品質も向上することが明確であること
- 社会的な責務
  サイバーセキュリティリスクへの対応が、顧客やステークホルダー等に対する責任を果たすことにつながることが明確であること

経営者が判断できる材料とは

経営者がサイバーセキュリティリスクへの対策費用の妥当性を判断する材料のひとつと

して、脅威への対策効果を示すことがあります。その事業のサイバーセキュリティリスクが高い場合、事業継続性の観点からサイバーセキュリティ対策を強化する必要があり、どの程度のリスクがあるかによって対策費用も対策に要する期間も異なります。想定するセキュリティリスクの大きさと対策のコストについて「見える化」を行い、経営者が判断できる材料を提示することが必要です。これは、重要な自組織の事業継続性を向上させるためだけではなく、重要な事業の品質や健全性をも向上させることにつながります。

経営者が必要な対策の妥当性を判断する材料は様々なものがありますが、例えば、４章で挙げた KPI や、以下のような分析結果を利用して想定するリスクと対策について「見える化」を行い、経営者の判断材料を提示することを考えます。

- **ビジネスインパクト分析**
  ３章で示したサイバーセキュリティリスクに関するビジネスインパクト分析を実施した結果を示します。事業とサイバーセキュリティリスクの全体像が把握でき、事業を踏まえたサイバーセキュリティ対策の優先度を検討することができます。

- **予測損失額の試算**
  サイバー攻撃を受け、被害が発生した場合を想定した予測損失額を試算し、ビジネスインパクト分析に加えて提示します。なお、インシデントに係る損失は様々なケースが想定され、予測損失額の試算の精度には幅があるため、予測損失額の詳細化や根拠が問題になる場合もあります。

❑ 参考データ「セキュリティ投資評価（国内外比較）」

「経営者が判断できる材料とは」では、サイバーセキュリティリスクへの対策費用の妥当性を判断することの重要性を示しました。一方、CISO・CSIRT の実態調査[1]の国内外比較では、自社が投資しているセキュリティ対策費用について、「評価を実施していない」企業の割合は、日本が 28.1%と米国 15.7%、欧州 9.3%に比べ高い傾向にあります。

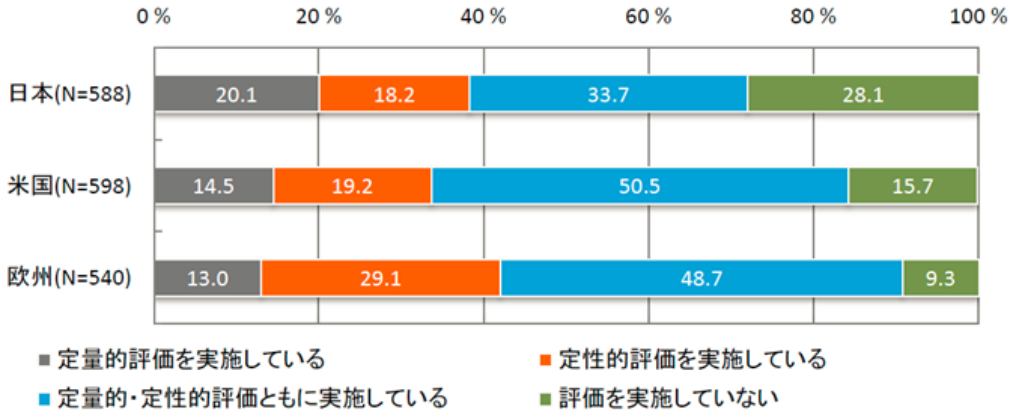


図 ６－１　セキュリティ投資評価（国内外比較）

（引用）企業の CISO や CSIRT に関する実態調査 2016、独立行政法人情報処理推進機構

6-2 必要な人材の確保・育成

サイバーセキュリティリスク管理体制を維持するためには、こうした体制を担う人材の確保や育成について考える必要があります。社内外の IT サービスに従事する人だけでなく、社内の IT ユーザー（いわゆる一般従業員）もサイバーセキュリティに関する知識を習得する必要があることから、人材育成は全従業員が対象となります。このうち一部の従業員は CISO 等や部門責任者のもとでサイバーセキュリティ対策を担う担当者として、サイバーセキュリティ対策に関するより高度な知識やスキルを習得する必要があります。こうした人材を自社で育成することが困難な場合などは、外部リソースの活用も検討します。

必要な人材と育成

セキュリティ担当者の育成と一般従業員の育成を分けて実施する必要があります。組織全体のセキュリティ意識を高めるためには、セキュリティ担当者以外も含めた従業員向け研修等のための予算を確保し、継続的にセキュリティ教育を実施することが求められ、状況に応じて教育内容や研修内容を見直す必要もあります。また、セキュリティ担当者を育成するためには、組織内人事部門において、IT の利活用に関する自社の戦略（情報システム部門における自社のシステム開発戦略、事業部門における IT を利活用した事業戦略を含む）を踏まえつつ、セキュリティ人材の育成計画を策定すること、さらにセキュリティ人材のキャリアパスを構築することが求められます[27]。組織内に適正なセキュリティ担当者がいない場合の育成については、社内で IT に詳しい人材を探して育成し担当者とする方法も考えられます。サイバーセキュリティ人材を外部から雇用（採用）することが困難な場合は、外部の専門ベンダに委託することも検討します。

また、大規模な組織等については、経営者の示す経営戦略を踏まえつつ、セキュリティ担当者との間でコミュニケーションを取りながら自社のサイバーセキュリティ対策を推進するいわゆる橋渡し人材（CISO 等を含む）や、自社のサイバーセキュリティ対策実施について、CISO 等を補佐するチームも必要になります。CISO 等を補佐するためには、CISO 等に求められる役割を担うことが要求され、こうした人材の確保も重要になります。例えば、（ISC）2[28]がセキュリティスペシャリストとして認定している CISSP では、CIO/CISO 補佐官の役割を担う人材に必要な知識を以下の８つのドメインで定義しています[29]。

1. セキュリティとリスクマネジメント
2. 資産のセキュリティ
3. セキュリティエンジニアリング
4. 通信とネットワークセキュリティ
5. アイデンティティとアクセス管理

---

[27] キャリアパスの検討には、情報セキュリティスペシャリストキャリアパス事例集が参考になります。
https://www.ipa.go.jp/files/000014185.pdf

[28] ISC スクエア＝International Internet Systems Security Certification Consortium の略称。1989 年に米国で設立された NPO（非営利団体）であり、情報セキュリティプロフェッショナルの認定・教育活動を展開している組織。

[29] このほか 2017 年度に創出される国家資格の「情報処理安全確保支援士」なども参考になります。
http://www.meti.go.jp/press/2016/10/20161021002/20161021002.html

6. セキュリティの評価とテスト
7. セキュリティの運用
8. ソフトウェア開発セキュリティ

セキュリティ担当者の育成

一般的にセキュリティ対策を推進、管理する担当者や部門は、セキュリティインシデントが発生しないことが当たり前として、様々な取り組みを実施していたとしても適切な評価をされにくい傾向があります。一方でインシデントが発生した際には、未知の攻撃を受けた場合でも対処がされていなかったということで評価が下がってしまう可能性もあります。

このようにセキュリティ担当者のモチベーションが低い場合、組織内部の犯人探しに終始してしまう等、リスクに関する正確な情報を共有し適切に対処するといったリスクコミュニケーションが、実施できない可能性があります。リスクコミュニケーションを適切に実施するためには、実施するセキュリティ担当者に関する業績評価の方法や指標を考慮する必要があります。

セキュリティ担当者の業績評価の指標は、軽微なインシデントやヒヤリハット等の報告から対策を改善した実績や、教育によってヒヤリハットを低減させた実績、または実施すべき対策に成熟度モデルを適用し、対策実施達成度等で評価することを検討する必要があります。

一般従業員の研修

サイバーセキュリティリスク管理体制では、セキュリティ担当者だけではなく、一般の従業員に対しても自組織のセキュリティポリシーの理解等を目的とする教育や研修が必要となります。一般の従業員に対して次のような教育を実施することで、従業員ひとりひとりのセキュリティ意識を高めることができ、組織全体のセキュリティ意識を底上げする効果も期待できます。

- 最新のサイバー攻撃の動向（どのような被害があり、どう対処すればよいのか等）
- 日常心がけるべき事項（セキュリティパッチ更新の励行、不審な電子メールの添付ファイルを開封しない等）
- サイバー攻撃の疑いがある現象を発見したときの連絡方法

また一度研修等を行えば終わりということではなく、新入社員や中途採用者等も含めて継続的に研修を行う必要があります。また、異動時や昇格時に対策が異なる場合には、その内容に応じた研修等も実施する必要があります。

さらに、サイバー攻撃の状況や予兆は、一般の従業員でもわかる場合があります。例えば、ネットワークが遅く感じる、特定のサイトや特定のファイルへのアクセスができない場合など、常日頃から、どのような現象が異常で、連絡や報告を必要とするのかを示しておくことで、サイバー攻撃に関する検知能力を高めることも期待できます。

積極的な外部リソースの活用

サイバーセキュリティ対策には、高度な技術力が求められる場面もあります。また、これ

らの高度な技術力の習得には時間を要するため、そのすべてを組織内の人員で実施できないことも考えられます。そのため、積極的な外部リソースの活用についても検討します。ただし、外部リソースの活用の実態が外部への丸投げであっては組織の安全は確保できません。専門的な対策を外部に委託するにしても、自組織内にそうした事業者と対話できるスキルを備えた担当者（CISO 等または部門責任者、こうした責任者から指示を受けた者など）を育成し、経営者の意図が適切に対策に反映されるようなコミュニケーションを実現できるようにする必要があります。

企業例示「資源の確保」

仮想企業Ａ社及びＢ社が経営資源の確保を検討、実施した内容やポイントを示します。

企業Ａ社の資源確保　　**EC サイト運営（中小企業）**

Ａ社の CISO は、事業への影響度が高い EC サイトを中心にサイバー攻撃対策の状況と望ましい対策とのギャップを示し、今後の計画を経営者に提示しました。Ａ社の検討のポイントを示します。

予算確保

- ビジネスインパクト分析の結果（EC サイトの停止による想定被害額等の算出等）をもとに、想定されるサイバー攻撃を受け被害が発生した場合の事業への影響度を検討し、サイバー攻撃対策の重要性を説明した。

- 現状の対策状況と、自社の EC サイトへのサイバー攻撃を想定した場合に望まれる対策とのギャップを示した。

- 自社の EC サイトへのサイバー攻撃を想定した場合に望まれる対策については、外部コンサルタントの意見や EC サイトの脆弱性診断サービスなどを活用した上で詳細を検討したいと考え、その費用の概算や期間等の計画を提示した。

- 特に EC サイトの対策費用の確保については、IT システム管理の外部委託の検討の結果を経営者に対して説明した。現在の EC サイトの対策状況、および EC サイトへのサイバー攻撃を想定した場合に望まれる対策を実施するためには、EC サイトをクラウドサービスへ移行した方がセキュリティの向上を期待できることを示し、クラウドサービスへの移行計画も提示した。

人材育成

- 今後の人材育成の一環として、サイバーセキュリティリスク管理体制の担当者に対しては、緊急時対応体制を強化するために、外部の演習を実習させる計画を提示した。

- 人材育成の状況については、IPA のベンチマークの簡易版を用いて、一般の従業員に求めるサイバーセキュリティ対策に対する理解度チェックの集計結果を報告した。

企業Ｂ社の資源確保　　**電子機器製造（大企業）**

Ｂ社の CISO は、経営者がすでにサイバーセキュリティリスク管理を理解していることもあり、サイバー攻撃の脅威などの説明は省略し、資源確保の計画を提示することを検討しました。Ｂ社の検討のポイントを示します。

■予算確保

- 経営者からは、現在のサイバーセキュリティリスク管理状況を把握したいとの要請があったこともあり、従業員の対策に対する理解度や、自社に想定されるサイバー攻撃への対応状況、IT 予算全体に対するサイバーセキュリティ対策予算の割合等を見える化し、その結果を提示した。

- 特に、従業員の対策に対する理解度については、簡単な対策についての教育とともに理解度チェックを実施し、その結果と求められる理解度とのギャップも報告した（ギャップを分析した結果、グループ横断の対応が浸透していないことがわかった）。

■人材育成

- セキュリティ人材の育成については、グループ企業が共通して取り組む必要があり、人員計画の一部としてセキュリティ人材についても検討をすすめることとし

た。また人事部門が主管となりセキュリティ人材に関する採用計画及び能力開発計画等を作成した。

・ 人材育成の一環として、緊急時対応に専門家の中途採用、及び CSIRT 運用に関するセミナーや研修等の費用を計上した。

7 IT システム管理の外部委託

IT システム管理の外部委託範囲を特定し、当該委託先のサイバーセキュリティを確保します。

実施内容 7
1．効率性などを考慮し IT システムの運用を外部に委託する部分を決定する。 2．外部へ委託した IT システムの運用についても自組織が求めるサイバーセキュリティが確保できるよう確認する。

7-1 自組織による対応と外部委託による対応

自組織における IT システム管理及びサイバーセキュリティ対策に関する技術力やその人的リソース確保の見通し等を踏まえて、３章で策定した対策項目のうち、自組織で対応するものと外部委託するものの切り分けを行います。求められるサイバーセキュリティ対策の内容と自組織で対応可能な内容及びコスト等を考慮して、自組織による対応と外部委託による対応を比較し、外部委託の有無を判断します。組織内部でのセキュリティパッチの適用状況確認のほか、セキュリティ専門企業による Web アプリケーションの脆弱性診断やプラットフォーム診断サービスを受けることを検討する必要があります。

外部委託する範囲を選択するポイント

IT システム管理において、自組織で対応できる内容と自組織で対応できない内容を整理する必要があります。例えば、ウイルス対策ソフトウェアでは検知できないようなマルウェアに感染した疑いのある端末の調査など、自組織では技術的に対応が困難なものについては、外部専門機関やセキュリティベンダに委託することを想定し、自組織で対応できることと外部に依頼が必要なことを予め切り分けておくことが重要です。また、外部に依頼するために必要となる予算を予め確保しておくだけではなく、調査依頼をするために必要となる情報や端末の状態などを確認しておく必要があります。

例えば、外部委託する範囲を選択する場合には以下のようなポイントがあります。

- 自社業務や自社システムの特性を把握する必要がある対策は、自前で行うことが望ましい（セキュリティパッチ更新の管理、アクセス権設定など）。
- 特に中小企業では、重要度の高い情報（大量の個人情報など）を管理する場合や、自組織で対策を行うリソースがない場合、クラウドを利用して、セキュリティも含めて業務を委託する選択肢がある。
- 専門性の高いサイバーセキュリティ対策として、運用監視（マネージドサービス）、情報セキュリティマネジメント監査、脆弱性検証（ペネトレーションテスト）、インシデント時のデジタルフォレンジックなどがある。これらは守るべきシステムの構成、資産の重要度、その業種で遵守すべき法制度にもよるが、専門性の高い業務を実施でき

る人材がいない場合には必要に応じて外部に委託することを検討する。

❑ **参考データ「自社 Web サイトの運用・管理の委託（国内調査）」**

「外部委託する範囲を選択するポイント」では、自組織で対策を行うリソースがない場合に、外部委託を選択することを示しました。一方、国内企業のサイバーリスク管理の実態調査[2]では、自社の Web サイトの情報システムの運用・管理を外部に委託している割合は、大企業が 39.1%、中堅企業が 33.5%、中小企業が 24.6%であり、規模が小さくなるにつれて外部委託する企業が少なくなる傾向にあります。

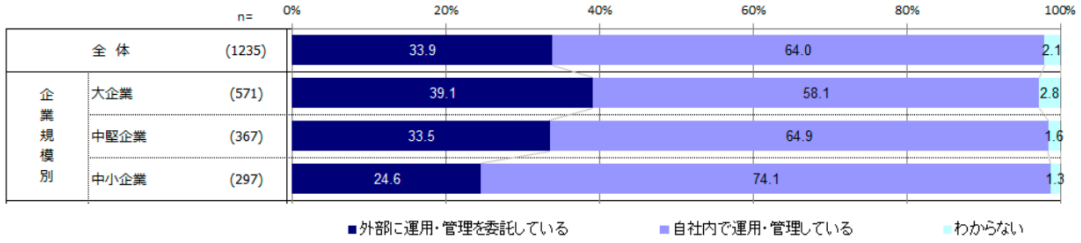


図 7－1 自社 Web サイトの運用・管理の委託（国内調査）

(引用) 企業におけるサイバーリスク管理の実態調査 2015、独立行政法人情報処理推進機構

7-2 委託先のサイバーセキュリティの確保

自組織のサイバーセキュリティ対策を外部委託する際には、委託先のサイバーセキュリティリスク対応を徹底するために、委託先のセキュリティレベルを契約書等で合意する必要があります。

委託先への依頼方法

受発注契約や基本契約にはセキュリティレベルを記載せず、別紙に取りまとめ、参照する形式で契約締結する場合が多く、社会環境や当事者の環境変化により、対策内容について見直すことを記載する必要があります。

また、委託元は委託先のサイバーセキュリティ対策を確保するだけではなく、再委託についても同様のサイバーセキュリティ対策を求めることを契約書等で合意しておくことが望ましいでしょう（委託先との契約内容については、5－1 系列企業・サプライチェーンを含む対策の実施を参照）。

なお一般論として、委託元が要求する対策に完全に対応できる能力を委託先が持っていない場合もあります。そうした場合は、委託先が提供する対策メニューなど、セキュリティ対策についてどんな情報開示をしているかを調べ、委託元が求める対策が実施できないか交渉し、実施できない場合にはその業者の選択が適切なのかどうか再検討する必要があります。

さらに、委託元はこれらの契約内容に基づいて対策状況を確認することが重要です。特

に自社システムを構築したベンダにサイバーセキュリティ対策を含めて運用を委託する場合は丸投げにせず、自社のセキュリティポリシーに基づいて運用されていることを確実にチェックする必要があります。自社のセキュリティポリシーに基づいて運用されているか等の対策状況を確認するには、委託元が委託先を監査する方法や、監査の代わりに委託先の監査レポート等（例えば、クラウドサービスにおける「Service Organization Control；SOC」レポートやその他のセキュリティや監査に関するレポート等）の報告を受ける方法があります。確認項目等の詳細については、５章の「ビジネスパートナー等の対策状況の把握」を参照してください。

連携体制の整備・構築

外部へ委託する処理やサービスについては、担保すべきセキュリティサービスやそのサービスのレベル、及び管理上の要求事項を明確に定める必要があります。また、もし委託先のセキュリティサービスやレベルが変更となるような場合についても、事前に確認できる状態にしておくことが重要です。さらに、サイバー攻撃を想定した場合、委託先や再委託先に自組織と同等のサイバーセキュリティ対策を求めるだけではなく、インシデント発生時の緊急体制や原因究明、必要と考えられる緊急対策等を事前に検討した連携体制を整備、構築する必要があります。このようにサイバーセキュリティ対策を含めて外部に委託する場合には、単に事業の一部分を切り出し、作業を委託するという考え方ではなく、緊急時の対策も含めた連携体制を構築するという考え方が重要になります。

外部委託先としてクラウドサービス事業者を選定する際のポイント

IT システム管理や運用における外部委託先の例として、近年クラウドサービスを利活用する事例が増えています。クラウドサービスの利用に当たっては、まずどのような情報やサービスを移行できるのかについて事前に情報を収集し、十分検討する必要があります。クラウドサービス安全利用のすすめ[30]において以下のような確認が重要とされています。

- **クラウドサービスの利用範囲についての確認**
  - **利用範囲の明確化**
    - ✧ クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールを設定する。
  - **扱う情報の重要度**
    - ✧ クラウドサービスで取扱う情報の管理レベルについて確認する。
  - **ポリシーやルールとの整合性**
    - ✧ 自社のセキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じないことを確認する。

- **クラウドサービスの提供条件についての確認**
  - **事業者の信頼性**
    - ✧ クラウドサービスを提供する事業者は信頼できる事業者であることを確認する。

[30] IPA クラウドサービス安全利用のすすめ
http://www.ipa.go.jp/security/keihatsu/pr2012/ent/02_cloud.html

- **サービスの信頼性**
  - ✧ サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルが示されていることを確認する。
- **セキュリティ対策**
  - ✧ クラウドサービスにおけるセキュリティ対策が具体的に公開されていることを確認する。
- **利用終了時のデータの確保**
  - ✧ サービスの利用が終了したときのデータの取扱い条件について確認する。

上記のとおり、利用範囲だけでなく、安心・安全にクラウドサービスを利活用していくために、委託先の信頼性や、適切にセキュリティ対策が実施されているかについても確認する必要があります。クラウドサービス事業者を選定する際の基準として、５章のビジネスパートナーの対策状況の把握で記載した第三者による監査制度に加えて、クラウドサービス事業者に関する国際規格（ISO/IEC 27017）[31]や認証制度（CSA STAR[32]など）等も参考にすることができます。

企業例示「IT システム管理の外部委託先への対応」

仮想企業Ａ社及びＢ社が委託先への対応について検討、実施した内容やポイントを示します。

企業Ａ社の外部委託先への対応　　**EC サイト運営（中小企業）**

A 社のサイバーセキュリティ委員会は、A 社 EC サイトそのものが、重要保護資産であると認識しています（１章企業例示を参照）。セキュリティ上の脅威によって EC サイトが停止を余儀なくされることは、受容できない経営上のリスクです。

クラウドへの移行（マイグレーション）

A 社は、EC サイトのセキュリティ向上を、外部のクラウドサービスへの移行によって実現すると計画しました（６章企業例示を参照）。クラウドサービスの多くは、セキュリティ管理サービスを付帯サービスとして提供しており、これを利用する事で可用性向上が期待できるからです。

ところで、A 社の EC サイトのシステムは、創業時にゼロから自社開発し、長年、機能

[31] ISO/IEC 27017：2015：
ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

[32] クラウドコンピューティングのセキュリティにおける成熟度を評価する認証制度
https://www.cloudsecurityalliance.jp/newsite/?page_id=429

向上を積み重ねてきたシステムです。EC サイトのシステムとプラットフォーム層との間のインタフェースを調査したところ、過去の経緯を引きずっているため、最近のインタフェースを使って実装できていない機能が多く見つかりました。EC 事業は競争相手が多く、顧客満足度向上に繋がるアプリケーションの機能追加に追われてきたので、現行のアーキテクチャにはできるだけ手を加えず、延命々々でしのいできた結果です。

EC サイトシステムをクラウドへ移行するには、最近のインタフェースに合わせアーキテクチャを見直し、改造を施さなければなりません。ざっと見積もったところ、改造に少なくとも 6 か月、その後の動作検証に 2 か月程度はかかると判明しました。移行自体にはそこから着手し、さらに何か月か掛かるでしょう。

EC サイトの状況

情報システム部門の部長は、可用性を阻害する脅威が世の中で頻繁に報告されている現状を念頭に、EC サイトの状況を次のように整理しました。

- 情報システム部門は多いときでも１０名弱の要員しかいないため、専任のセキュリティ担当をおいてこなかった。開発担当者の一人がセキュリティ担当を兼務しており、ニュースなどでセキュリティ事件の記事に気づく度、原因となった脆弱性の情報を集めている。開発業務の空き時間を利用して、EC サイトの構成要素（すなわち OS やデータベースなど）がそれらの脆弱性に該当していないか、攻撃対象になる可能性はないか判断し、必要な場合には、未適用のパッチを当てるなどの対応を取っている。

- この対応方法では、セキュリティインシデントに至らず大きく報道されていない脆弱性に対しては、十分対策できているか不明である。明日にでも、OS 等の脆弱性を突いた攻撃を受け、顧客の個人情報が漏えいしたり、EC サイトのコンテンツが改ざんされたりする可能性がある。

クラウドへの移行にはかなりの期間が必要ですが、元々の目的だったセキュリティ上の可用性向上は喫緊の課題です。そこで、クラウドへの移行には中期的なスパンで取り組むこととし、とりあえず緊急に可用性を向上するための策として、現行の EC サイトシステムに対してセキュリティ専門業者のサービスを受けることにしました。

可用性向上の代替策

代替策は以下の通りです。

- （既知の脆弱性への対応）現行の EC サイトシステム全体に対して、既知の脆弱性に関する包括的な診断サービスを受ける。
- （新たな脆弱性への対応）新たな脆弱性情報が出るたびに、現行の EC サイトシステムの構成要素に関係がないか一次的な判断を行い、影響が予想される場合に A 社へ警告を通知する脆弱性情報提供サービスに契約する。
- 現行の EC サイトシステムに対するセキュリティ監視サービス（SOC サービス）に契約する。

なお、脆弱性診断サービスや脆弱性情報提供サービスによって、緊急性の高い問題が見つかった場合には、早急に必要な対処（適切なパッチの適用、システムの改修等）を行う事にしました。

企業 B 社の外部委託先への対応　**電子機器製造（大企業）**

B 社でヘルプデスクシステムを運営しているシステム管理部は、他に多くの既存システムを運営しており、さらに新規のシステム開発を並行しているために、つねに高負荷が続いています。システム管理部については、既存システムの運営業務の負荷を下げ、新規システムの開発を加速する事が必要との議論が、経営幹部の間で話題になっています。

システム管理部では、社内のこうした意見に応えるために、情報公開系の Web システムを社外のクラウド上に移行（マイグレーション）し、運営業務の多くをクラウド事業者に外部委託する案を検討しています。まずは試行することになり、その対象としてヘルプデスクシステムが選ばれました。

【外部委託先としてクラウドサービス事業者を選定する際のポイント】

社内システムをクラウドへ移行するにあたっては、B 社のセキュリティ管理規程に合致したクラウド事業者を選ばなければなりません。ヘルプデスクシステムの移行では、システムが保持する製品登録ユーザーの個人情報の扱いに留意する必要があります。

個人情報は、万一漏えいした場合に、お客様に重大な影響をあたえるデータです。そうしたデータに対しては、下記の B 社セキュリティ管理規程が適用されます。

- **規定 a**：機密性 2（漏えいしたら取引先や顧客に重大な影響を与える）のデータを社外の IT システムで扱う際は、データベースやファイルの内容を暗号化する。

- **規定 b**：機密性 2 のデータに関する以下の項目を、システムログ又は利用実績として記録する。
  - アクセス者の個別のアイデンティティを識別できるアカウント情報
  - アクセス日時
  - アクセスしたデータ
  - アクセスしたデータに行った処理内容（例：閲覧、変更、削除、システム外への出力等)

デフォルトの暗号化機能

規定 a、b に適合するクラウド事業者を探すため、システム管理部は、いくつかのクラウド事業者のホームページから、セキュリティホワイトペーパーを入手し比較検討しました。その結果、X 社、Y 社のクラウドサービスには、基本料金の範囲で暗号化機能が提供されていると分かりました。これを利用すれば、規定 a の遵守のために、暗号化機能を自前で用意する必要がなく好都合です。

適切なロギング[33]機能

さらに、X 社のクラウドには、システムログ機能として、API[34]呼び出し元アカウントの ID、API 呼び出し元の IP アドレス、日時、データ、API 呼び出しパラメータ、API 処理の結果応答等を記録する機能が準備されています。これを使えば、規定 b に対応したロギングが容易に実現できそうです。

以上の検討から、ヘルプデスクシステムの移行先として、X 社のクラウドを選定しました。

[33] データ等の詳細をファイルに出力すること
[34] API：アプリケーションプログラムインタフェース

８ 情報収集と情報共有

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のための環境を整備します。さらに、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献します。

実施内容８
１．サイバー攻撃の手法や脅威などの情報を収集し、インシデントが発生した場合を踏まえて、自社で有効活用するための環境を整備する。 ２．攻撃情報を収集するだけではなく、情報共有活動に参加し、自社の情報を積極的に提供する。

８-１ 情報収集と自社での有効活用

サイバー攻撃への対策をより効率的に実施するためには、サイバー攻撃がもたらす脅威に関する具体的な内容や自社に影響しうる脆弱性について、常に最新の状況を理解しておく必要があります。そのためには意識的に情報収集に取り組むことが重要です。

情報収集の重要性

新たに発見された脆弱性を利用したサイバー攻撃に対応するためには、新たな脆弱性情報を収集し、早期に対策する（セキュリティパッチの適用等）必要があります。一方、サイバー攻撃には様々な手法があり、手法自体が改良される場合や複数の手法を組み合わせる場合などもあり、その手法を自社のみで把握することや分析することは困難です。そのため、サイバー攻撃の手法や脅威等を効率的に収集する情報源を特定し、常に情報収集すること、また必要に応じて IPA などの公的機関によるサイバー攻撃の分析結果を確認し、自社の対策に活用することが求められます。

具体的には、CISO 等は、IPA や JPCERT/CC[35]等による注意喚起情報[36]を確認し、自社のサイバーセキュリティ対策に活かします。また、日本シーサート協議会等のコミュニティ活動への参加によって得られた情報等を通じて、自社のサイバーセキュリティ対策に活かすことが望まれます。

---

[35] 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）https://www.jpcert.or.jp/

[36] IPA（重要なセキュリティ情報）http://www.ipa.go.jp/security/announce/alert.html
JPCERT/CC（注意喚起）https://www.jpcert.or.jp/at/

情報を常に最新の状態に保つ

サイバー攻撃には既知の脆弱性を利用した手法も多く、脆弱性に対応するためには、常に脆弱性情報を確認し、公開された脆弱性に対応する必要があります。公開された脆弱性情報は、攻撃者も入手しているため、その脆弱性を利用した攻撃が発生する可能性が否定できません。そのため、脆弱性が公開された時点から早急にセキュリティパッチを適用する等の対策が求められます。このように、パッチマネジメントを適切に実施し、最新の状態に保つだけでも多くのサイバー攻撃を防ぐ効果が期待できます。また、脆弱性情報だけではなく、サイバー攻撃に関する情報についても、同様に最新の状況を把握していることが望まれます。IPA や JPCERT/CC、警察庁、セキュリティ専門企業等などではサイバーセキュリティ関連で注目すべき攻撃が広まった場合にタイムリーに注意喚起や対策に関する情報の提供を行っていることから、こうした情報を速やかに入手できるように、メールニュース配信への登録や定期的な情報サイトのチェックを行うようにします。

収集した情報を活用するための環境整備

情報収集した脆弱性情報等については、必要な関係部門に展開し、速やかにパッチを適用する等の対処を実施します。そのためには、入手した情報については、どの部門や担当者に展開すべきか、またパッチ適用など、最終的に誰が対処するのかを決めておく必要があります。すべての脆弱性情報や攻撃に関する情報を咀嚼せずに、単純に関係者と思われる部門や担当者に連絡するだけでは活用されません。個々の脆弱性情報や攻撃に関する必要最小限の情報を必要な関係部門や担当者に届ける役割（ディスパッチャー）が必要です。

また、情報収集の担当者が、自組織にどのような製品、システム、サービスが存在しているのかを把握しておくためには、自社のサイトや製品を構成する IT 部品の構成管理情報のデータベース等の設置とメンテナンスが必要です。特に製造業においては、歴代の数多くの製品に関する構成管理情報のデータベース等を整備することは容易ではなく、構築に時間がかかる可能性があります。構成管理情報のデータベース等の整備は重要であるため、全社を管轄する品質保証部門の役目として規定することも検討します。

[コラム] 脆弱性情報の公開と対策

2014 年には、広く利用されるソフトウェアに脆弱性が見つかり、攻撃が発生しました。オープンソースの暗号ライブラリである OpenSSL で発見された「Heartbleed」、Linux 等で広く使用されるオープンソースのシェル bash で発見された「Shellshock」、Java のウェブアプリを作成するためのソフトウェアフレームワーク Apache Struts で発見された ClassLoader 脆弱性等は、中でも注目を集めました（下記、JVN iPedia の登録状況及び情報セキュリティ 10 大脅威 2015 を参照）。

一般的にソフトウェア開発者は、脆弱性対策情報の公表と同時に、修正プログラム（パッチ）を提供します。一方、多くの攻撃者もこのタイミングでソフトウェアの脆弱性を知ることとなり、パッチから脆弱性を解析し、脆弱性を悪用したサーバへの通信（攻撃パケットの送信）や、ウイルス感染させるファイルの作成と配布を行います。そのため、脆弱性対策情報が公表されたにも関わらず、対策の実施が遅れた場合や対策を実施しない場合には、被害を受ける可能性があります。下記の脆弱性対策情報等を参考に効果的な対策を検討してください。

- IPA 脆弱性対策情報データベース JVN iPedia の登録状況
  [2014 年第 2 四半期（4 月～6 月）]
  https://www.ipa.go.jp/security/vuln/report/JVNiPedia2014q2.html
- IPA 情報セキュリティ 10 大脅威 2015
  https://www.ipa.go.jp/security/vuln/10threats2015.html
- IPA テクニカルウォッチ 「脆弱性を悪用する攻撃への効果的な対策についてのレポート」の公開
  https://www.ipa.go.jp/about/technicalwatch/20130926.html
- IPA テクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」
  https://www.ipa.go.jp/security/technicalwatch/20150331.html

8-2 情報共有・情報提供

サイバー攻撃に関する外部の情報を収集するだけでなく、自社で発見した脆弱性情報や、自社に対する攻撃等に関する情報を関係機関に提供したり、関連会社等の企業内グループで共有したりすることで、社会全体でのサイバーセキュリティ対策の効果を高めることができます。

情報共有・提供の重要性

インターネットバンキングを対象としたマルウェア作成ツールが利用され、様々な亜種が、複数の銀行に対する攻撃に利用された事例があります。社会全体でサイバー攻撃の防御につなげることが求められており、自社で観測したサイバー攻撃に関する情報（システムにおける挙動の変化、被害の状況等）の提供等を通じた積極的な協力の実施が求められています。

情報を提供すべき相手先機関は、情報の種類によって異なります。ウイルス情報や不正アクセス情報等は、告示に基づく届出として IPA に情報提供します。ソフトウェア製品やウェブアプリケーションの脆弱性を発見した場合は、情報セキュリティ早期警戒パートナーシップ[37]に基づき IPA へ届け出ます。また、インシデント情報については、JPCERT/CC に情報提供を行い、必要に応じて調整を依頼します。さらに、重要インフラ事業者等の情報共有の場合には、J-CSIP[38]などの仕組みを利用します。詳細については、参照情報を確認してください。こうした公的機関は提供内容についての守秘義務を負っており、適切な提供方法を用いている限りにおいて、情報漏えいが生じるおそれはありません。サイバーセキュリティリスク管理体制では、このような情報提供や共有に関する機能を有していることが望まれます。

情報共有を行う場を提供する組織は、その情報の内容や分野などによって異なりますが、例えば、ISAC[39]は特定分野の情報を共有するために組織されています。一方、ICT-ISAC のように、通信事業者以外に IoT 機器の製造事業者やセキュリティベンダ等の複数の事業分野が参加し、特定分野に特化しない会員が情報共有を行う動きもあるため、様々な場や組織を利用して情報交換や情報共有することも可能です。

社会全体での対策向上

サイバーセキュリティ対策では、新たな脆弱性や脅威情報、新たなサイバー攻撃手法を分析し、改善することが重要です。これらの情報は、公的機関や専門家を通じて収集することも可能ですが、情報を収集しているだけは、情報が集まりにくいのも事実です。情報を発信

---

[37] IPA 情報セキュリティ早期警戒パートナーシップガイドライン、https://www.ipa.go.jp/security/ciadr/partnership_guide.html

[38] サイバー情報共有イニシアティブ、Initiative for Cyber Security Information Sharing Partnership of Japan。国内の重要産業・重要インフラ関連組織間において標的型攻撃などのサイバー攻撃の情報共有を相互に行い、即応的かつ高度な対策に繋げる IPA の取り組み

[39] Information Sharing and Analysis Center。脅威や脆弱性に関する情報や分析等を共有する任意団体やセンター

することで、同様の情報が得られたり、このような情報を知らないかといった問い合わせを受けたりすることにより、最新の情報が得られる機会が増えます。

外部に対して情報共有を行うためには、CISO 等やセキュリティ担当部門だけの判断ではなく、どのような情報を、どの範囲まで提供してよいか等に関して、経営層の意思決定が必要です。そのため、経営者には、社会全体がサイバー攻撃にさらされる現代においては、自社だけを守ることは不可能であり、コミュニティに参加する企業が、お互いを守りあうという考え方の理解を得る必要があります。

自社への攻撃があり被害が発生した場合、その攻撃情報を他社に情報共有することで、同様の被害が社会全体に広がることを未然に防止できます。例えば、各種公的機関が実施している啓発活動や業界団体等で実施している情報共有活動に参加することで、他社や他組織に対する脅威情報や分析情報を参考にすることができ、同じ攻撃が自組織に向けられていないかチェックすることや、今後同様の攻撃が自組織へ向けられる事態に備えた対策を検討できます。特に、犯罪に繋がるような事象が発生した場合には、警察へ情報提供することを検討する必要があります。普段から警察との連絡窓口を決めて交流しておくと、万が一事件が発生した際の対応もスムーズになることが考えられます。さらに、日頃からマルウェアや不審メール、インシデントに係る情報提供を各種届出窓口へ行うことで、情報共有活動を支える各組織を通じて社会貢献ができます。

脆弱性情報の扱いや対応については、社会貢献という側面だけではなく、社会的な責務という側面もあります。例えば、自社の脆弱性を対策せず放置することで、自社が踏み台になり、他組織の攻撃に利用される場合もあります。このように、自社の脆弱性を放置し、他組織に迷惑をかけることは、公害問題と同じだという考え方もあり、社会的な責務を果たしていないことから、（法的責任に加えて）経営責任を問われることも考えられます。

企業例示「情報収集及び情報共有の検討」

仮想企業Ａ社及びＢ社が情報収集と情報共有について検討、実施した内容やポイントを示します。

企業Ａ社の情報収集　**EC サイト運営（中小企業）**

Ａ社では、EC サイトへのサイバー攻撃の手法や脅威に関する情報収集について検討しました。Ａ社の検討のポイントを示します。

- EC サイトに関連する脆弱性情報提供サービスを購入することにしたが（7 章企業例示を参照）、将来的に自社で対応することも見据えて、IPA や JPCERT/CC 及び警察庁の@police 等の注意喚起情報を定期的に確認し、参考にすることとした。

・　不正アクセスが発生した場合を想定し、IPA への届出の方法や届出の際に必要となる内容を確認し、関係者間で共有した。

企業Ｂ社の情報共有　　**電子機器製造（大企業）**

Ｂ社では、サイバー攻撃に関する最新の情報の収集を行うとともに、より具体的な脅威情報や対策情報を収集するために、情報共有を積極的に行うことを検討しました。Ｂ社の検討のポイントを示します。

・　自組織と同じ業界や関連する企業について、どのようなサイバー攻撃が発生しているのか？また、どの程度の対策が考えられているのか？などの情報を収集するために日本シーサート協議会に参加することとした。また、社会貢献のために同協議会を通じて情報発信していくことも検討することとした。

・　日本シーサート協議会への参加については、自社グループでの参加とし、自社グループから数名を参加させることで、自社の担当者が参加できない場合でも情報共有できるようにし、自社の人的コストを抑えつつ、自社グループ内での情報交換も推進する体制を検討することとした。

・　業界団体の研究会活動として「サイバーセキュリティ研究会」を他の企業と一緒に立ち上げた。その場で 1～2 ヶ月に 1 回の会合を通じて各社の課題や取組についての情報交換を行ったり、セキュリティベンダを招いて製品動向の説明を受けたりすることを企画し、情報共有の機会を増やすようにした。

９ 緊急時対応体制の整備と演習の実施

緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）を整備するとともに、定期的かつ実践的な演習を実施します。

実施内容９
１．緊急時のための対応体制（CSIRT 等）を構築する。 ２．緊急連絡先や初動対応マニュアルを整備する。 ３．緊急時に適切に行動できるかどうかの確認を含めて、対応訓練や演習を実施する。

９-１ CSIRT の構築

CSIRT（Computer Security Incident Response Team）は、サイバーセキュリティに係るインシデント等に対処する組織であり、一般的には、サイバーセキュリティに関する窓口機能を有する場合が多くなっています（対外窓口には、自組織の Web サイトの脆弱性に関して外部からの通報を受ける窓口と、他の CSIRT と連携する窓口の双方が含まれます）。サイバーセキュリティに係るインシデントは、標的型攻撃や Web サーバの改ざんなど多様であり、連絡や連携を行う相手も多様であるため、こうした対処を行うチームや機能を被害が発生してから構築しようとしても不可能です。そのため、被害がないうちから構築しておき、いざというときに備えておくことが重要です。

CSIRT の構築方法

近年 CSIRT の重要性が強調されているのは、適切なサイバーセキュリティ対策を講じているような組織でも、サイバー攻撃の被害を完全に防ぐことは困難な状況であるという認識が、広まりつつあるためです。以下では、CSIRT 構築に向けて、組織内で検討、実施すべき事項の例を示します。

<組織内の状況把握>

CSIRT の体制をどのようにするかの検討に先立ち、関係者への聞き取り調査等により、次のような状況を把握しておく必要があります。

- 各部門の主要業務のフローとサイバー攻撃による影響の可能性
- 部門間での対策状況や脅威情報の共有及び連携の状況
- 各部門の責任者及びキーパーソン
- インシデント対応に関する規則類

<経営層への提案・承認の獲得>

CSIRT の構築・運用には、インシデントが発生した際に、原因追求や被害状況の調査のた

めに、部門横断的な調整が必要になる等の理由から、経営層の理解と協力が必要不可欠です。しかし、CSIRT の構築・運用には当然ながら費用がかかるため、「インシデントが起こらないようにすれば、そのような組織は不要ではないか」と考える経営層もいるかもしれません。サイバー攻撃で大きな被害が生じた経験がない組織であれば、経営層に CSIRT 設立に関する承認を得るのは容易でない場合があります。そこで、サイバー攻撃の被害を最小にするには、インシデント発生時に早急に対応できるようにすることが重要であり、その手段が CSIRT であるというロジック等を用いながら、経営層の理解と協力を得られるように提案するとよいでしょう。

経営層向けの説明資料を作るために、次のような作業を行うことが考えられます。

- 企業が CSIRT を持つべき必要性を訴求する材料集め（サイバー攻撃に関するニュースや、セキュリティベンダが作成した被害にあった企業の調査レポートなどを利用し、他社におけるインシデントの件数、インシデント発生による被害や財務への影響を示す統計データなどを提示）
- 企業が CSIRT を持つメリットを訴求する材料集め（CSIRT によってインシデント発生時の早期対応だけではなく、インシデント発生時のリスク低減が見込めることの説明、CSIRT によってインシデント収束までの期間短縮が想定でき、それにより財務への影響低減が見込めることの説明、インシデント対応の準備をしていることを対外的に訴求することによる企業イメージの向上の説明などを提示）

<CSIRT 構築作業チームの設置>

CSIRT の構築を担当するメンバーを集めます。前項の状況把握を通じてインシデント対応のスキルや能力を有する人材を発掘すると同時に、新たな組織を構築する際に調整が必要な部門へ働きかけを行うことも重要です。関係部門としては、情報セキュリティ部門のほか、情報システムの運用・保守部門、リスクマネジメント部門、広報部門などが関係します。こうした働きかけを行う際には、CISO 等が主導していることをアピールすることで、CSIRT の存在を周知できることから各部門の情報を得られやすく、スムーズに調整できる点でも有効です。

<CSIRT の設計>

組織にとって最適な CSIRT の形態は、組織の特徴によって様々です。そこで、CSIRT 構築作業チーム内での議論を通じて、構築する CSIRT における以下の内容を明らかにした上で、文書として取りまとめます。

- CSIRT の目的（組織における役割）
- 提供するサービス（インシデントマネジメント、連絡窓口、監視業務、等）
- サービスのレベル（24 時間体制、部門間の調整機能のみ、等）
- サービスの提供対象（活動範囲）
- サービスの提供主体（自社要員により対応、専属 or 兼務、外部サービス利用、等）
- 組織内での権限（外部ネットワークとの接続を切る権限を持つ、等）
- 新たに策定すべき規則等
- 運営上のポイント（特に重視する部門や事業など）

<予算・人員の確保>

CSIRT 運営に必要な要員と費用を明らかにします。このとき、平時とインシデント対応時の双方についての試算が必要です。インシデント対応についても、小規模なものと大規模なものとでは費用が変わってくるため、複数のシナリオで試算する必要があります。

- 人件費
- 外部委託費
- 監視や異常検知に必要な機器（IDS[40]、IPS[41]、SIEM[42]等）
- 会議や連絡のための設備や通信手段（TV 会議システム、携帯電話、等）

<その他>

上記のほか、事業活動に応じて以下について検討する必要があります。

- 遠隔地の工場や海外拠点の扱い
- 子会社・系列会社等の扱い（自社単独の CSIRT か、グループ全体の CSIRT か）
- 自社サービスを停止することで影響を受ける他社等のサービスとの調整

CSIRT の設計で検討すべき事項

検討すべき事項の例を以下に示します。

<CSIRT の役割・機能・権限>

CSIRT を構築する場合には、どのような役割や機能をどのようなチームで実施するのか等によって、様々な実現方法が存在します。例えば、JPCERT/CC では、代表的な CSIRT の構成例とその特徴について、表 9-1 のようにまとめています。組織内の情報システム部門が 24 時間の運用・監視・障害対応サービスを提供しているのであれば、CSIRT が新たに同様の機能を担う必要は無く、CSIRT が担うべき機能は外部との連絡窓口としての役割が主体になる可能性があります。一方、これまで IT を活用していなかった企業がクラウド化を機に活用するようになり、各部門に IT 関連のトラブル対応のスキルをもった要員がほとんどいないような場合は、CSIRT が障害対応機能を兼務することで、効率的な IT 活用ができる可能性があります。このように、CSIRT が担うべき役割や機能は組織の状況によって様々です。同様に権限についても、各部門の権限が大きい企業ではサイバー攻撃が行われた場合に、CSIRT が全社一律の外部とのネットワークの接続の遮断等を行うことに難色を示す部門が出てくる可能性がある一方、セキュリティ上の判断は自部門ではできないので CSIRT に任せたいという場合もあり得ます。いずれにせよ組織にあった運営方針を定めることが重要です。

---

[40] Intrusion Detection System：侵入検知システム。
[41] Intrusion Prevention System：侵入防止システム。
[42] Security Information and Event Management：ログデータを一元管理するセキュリティソフトウェアの一種。

表 9-1　代表的な CSIRT の構成例とその特徴

CSIRT 形態	説明
a)セキュリティチーム	既存の IT 部門やセキュリティ担当チームを要員も含めほぼ流用する形で、要員は通常の業務の一部として、インシデントハンドリングの活動を行う。実際には、インシデントが発生する都度、対応チームが結成されるケースが多いと考えられる。設置に掛かるコストや手間は最も少なく実施が容易である反面、既存業務との調整やなどが制約となる。
b)分散型 CSIRT	一部またはすべての下位組織の要員を仮想的に CSIRT の要員（専任／兼任）として指定し、全体の統括・調整を一人の責任者（マネージャ）が行う。要員は、それぞれの部門・部署をベースに活動し、インシデント発生時には CSIRT の要員として機能する。また、何人かは CSIRT の業務のみを専門とする。また、外部機関等とのやりとりは、全体の統括・調整を行う責任者が行う。
c)集中型 CSIRT	CSIRT が独立の正式な組織として設置され、専属の要員を中心に構成される。組織内で発生するすべてのインシデント対応への責任があり、責任者（マネージャ）や経営層（CIO など）に対する報告義務を伴う。
d)他組織との連携	自組織の CSIRT が CSIRT 間の連携体制における POC（Point of Contact）となることで、自らの経験だけでは解決困難な問題についても他組織の知見を活用することで対処が可能になる。また、CSIRT 同士の連携を通じて、適正なレベル感を相対的に把握することができる。
e)調整役 CSIRT	組織の内外に対するインシデントレスポンスの調整役を担うモデルで、例えば親会社の CSIRT が企業グループ全体を統括する立場から、個々のグループ企業の CSIRT を支援・牽引するような構造に適している。特に、情報の調整・流通を主な業務とし、インシデント対応の実務作業を行うことは少ない。

（引用）　経営リスクと情報セキュリティ ～ CSIRT：緊急対応体制が必要な理由 ～、一般社団法人 JPCERT コーディネーションセンター[43]

<CSIRT の組織上の位置付け>

CSIRT を実際の部門とするのではなく、各部門との兼務によるメンバーで構成される仮想組織として運営されている例もあります。実際の運用上の権限が部門にしかなく、CSIRT の機能として調整のみが期待されているような場合は、こうした仮想組織のほうが動きやすい可能性があります。このほか、既存の情報システム管理部門やリスク管理部門との関係についても色々なパターンがあり、こうした部門内の一部として CSIRT が運営されていることもあります。組織内での CSIRT に期待される役割に応じて、最適な位置付けについて検討することが望まれます。

[43] https://www.jpcert.or.jp/csirt_material/concept_phase.html　（図９－１、表９－２も同様）

<CSIRT 内のメンバー構成・役割>

CSIRT の役割・機能によってメンバー構成は変わってきます。CSIRT 業務に従事する人材に期待される役割の種類とそのために必要となるスキルについては、日本シーサート協議会が検討結果を公開していますので参考にしてください[44]。

<連絡窓口>

インシデント発生時に、CSIRT は組織内及び組織外との連絡窓口の機能を果たすことも求められます。ただし、利用者からの問合せなどの対応まで行うと、本来のインシデント対応業務への対応ができなくなることも懸念されます。インシデント発生時の窓口機能として、以下のような役割分担を行うことが考えられます。

- CSIRT：監督官庁等への報告、グループ企業や取引先等への連絡、経営層への報告、社内各部門へのアナウンス
- 広報部門：マスコミ取材対応
- サポートセンター：顧客からの取い合わせへの対応
- 社内ヘルプデスク：従業員からの問合せ対応

<CISO 等、幹部との連絡・報告体制>

CISO 等が CSIRT の指揮・命令系統のトップを兼ねることがあります。この場合は CISO 等へ通常のルートで報告することになりますが、CISO 等が直接 CSIRT の指揮・命令系統を有しない場合は CISO 等と緊密な情報共有ができる体制を構築しておくことが重要です。最高情報責任者（CIO）についても、社内システムや対外的な業務用サービスの提供に責任を負っていることもあり、緊密な関係を維持する必要があります。こうした責任者以外の役員については、CISO 等から連絡する体制や、CSIRT から直接連絡する体制等を、組織の事情に応じて構築します。

危機管理に求められる機能

緊急時に円滑に対応できるようにするためには、ただ単に CSIRT を構築すればよいというわけではなく、必要な機能を実装していることが重要です。JPCERT/CC では、危機管理体制と緊急対応に求められる機能を以下のように示しています。

企業経営や事業活動及び企業ブランドに重大な損失をもたらす事態、または社会一般に重大な影響を及ぼすと予想される事態を「危機」と考え、万一危機が発生した場合に損失を極小化するための活動が重要になります。このような活動を実施する体制を情報セキュリティ上の危機管理体制（インシデントマネジメント）といい、次のような機能の提供が必要になります。

[44] CSIRT 人材の定義と確保　http://www.nca.gr.jp/activity/training-hr.html

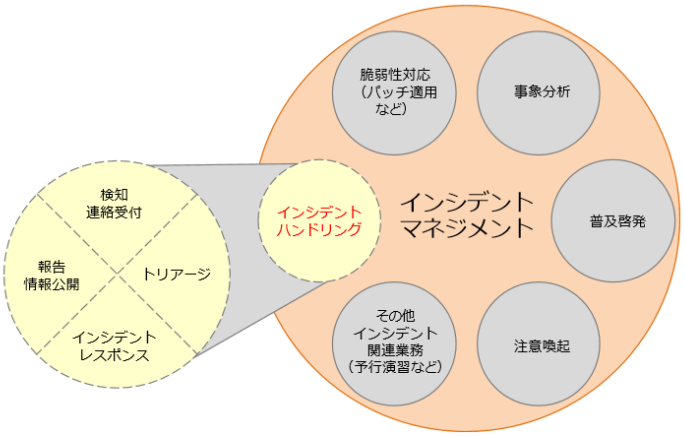


図 9－1　危機管理体制（インシデントマネジメント）の概要図

（引用）経営リスクと情報セキュリティ ～ CSIRT：緊急対応体制が必要な理由 ～ 、一般社団法人 JPCERT コーディネーションセンター

表 9－2危機管理体制（インシデントマネジメント）の概要

機能	内容
・脆弱性対応 （パッチ適用など）	脆弱性情報を収集し、自組織のシステムに対する脅威を分析して、必要に応じてパッチ（修正ソフト）の適用や設定変更を行います。
・緊急対応(インシデントハンドリング)	情報セキュリティインシデントが発生した際に、通報を受け、状況を踏まえ対処方針を決定し、問題解決を行い、インシデントを収束させる。緊急対応（インシデントハンドリング）は、主に以下の４つの機能で構成されます。 1.モニタリング（事象の検知、報告受付） 2.トリアージ（事実確認、対応の判断） 3.インシデントレスポンス（分析、対処、エスカレーション、連携） 4.リスクコミュニケーション（報告・情報公開）
・事象分析	発生した情報セキュリティインシデントに関するデータを分析し、原因や再発防止のための改善点を明らかにします。
・普及啓発	情報セキュリティインシデントの発生を低減するため、エンドユーザである従業員向けに教育・啓発活動を行います。
・注意喚起	情報セキュリティインシデントにつながるミスや情報セキュリティインシデントの発生時に、関係先に必要な注意喚起を行い、インシデントの被害拡大を防ぎます。
・その他のインシデント関連業務（予行演習など）	例えば、対処計画が適切に機能するか確認するため、模擬的に情報セキュリティインシデントの発生を設定し、関係者の行動を検証する演習を行うことが考えられます。

（引用）経営リスクと情報セキュリティ ～ CSIRT：緊急対応体制が必要な理由 ～ 、一般社団法人 JPCERT コーディネーションセンター

9-2　緊急連絡先・初動対応マニュアルの整備

緊急連絡先の整備では、組織内外の緊急連絡先をリストアップするだけではなく、併せて告知内容・方法・タイミング等も明確に定めておく必要があります。また、初動対応マニュアルは、初動対応のフローだけではなく、報告体制とエスカレーションの基準も含めて策定しておく必要があります。

緊急時の初動対応フローの整備（マニュアルの策定）

サイバー攻撃を受けた組織内部から報告を受ける場合と組織外から通報を受けた場合に、どのように被害状況を把握し、何をすべきかといった初動について予め確認しておき、フローをマニュアルとして取りまとめておく必要があります。

例えば、標的型メール攻撃を受けた疑いがあることに気が付いた従業員が、社内のインシデント対応窓口や CSIRT 担当者等のどこに報告すべきか、重大なインシデントかどうかの判断基準などの項目（検知、報告、初期対応等）について記載するようにします。

初動については、まさに緊急事態であるため、必要な情報を収集し冷静に判断するためには、情報の粒度や量などの適切性が求められます。事態を報告する際に、情報量が多すぎたり、技術的な専門用語を使用しすぎたりすると、事業部門のトップや経営者は正しく判断できない可能性もあります。インシデント発生時の被害原因の特定や解析を速やかに実施するために、組織内の連携体制や初動マニュアルを整備しておくことが重要です。

自組織で緊急時の対応ができない場合には、外部委託することも検討する必要があります。外部に委託する場合であっても、自組織内で緊急時の対応を判断することや自組織内外との調整を行う役割は委託できないため、判断及び調整機能は自組織内に存在することが必要です。また、外部に委託する場合には、緊急時対応の対象となるサービスを明確化し、緊急時対応に必要となる作業時間や予算なども予め想定、把握しておく必要があります。

報告体制・エスカレーション基準

インシデント発生時に必要な相手に迅速に報告を行うためには、予め連絡が必要な相手をリストアップし、緊急連絡先として取りまとめておきます。インシデントの兆候の中には、実際には誤検知に起因するものや、影響が軽微なため特段の対処を行う必要がないものが多数含まれます。こうした兆候のすべてについて報告を行うと、報告の受け手側の業務効率を低下させるだけでなく、重要なインシデントについての報告がそれらの本来報告不要な情報の中に埋没し、正しく相手に伝わらない結果を招く恐れもあります。したがって、どのような状況になったらどこまで情報を上げるべきか等、エスカレーションの基準を予め適切にまとめておくことが重要です。

社外を含めた緊急連絡先

緊急連絡先として考慮しておくべき相手の例を次表に示します。

表 9-3 インシデント発生時の CSIRT からの緊急連絡先の例

社内	・CISO 等 ・最高情報責任者（CIO） ・その他経営層（CISO からのエスカレーションが適切な場合もある） ・インターネット等を活用した事業を行っている部門の責任者
社外	・所管官庁（個人情報漏えいを伴うインシデント等の場合） ・所管警察署（サイバー犯罪に該当する可能性がある場合） ・マスメディア（プレスリリースが必要と判断される場合） ・ビジネスパートナー（事業部門からの連絡の方が適切な場合も多い） ・取引先（事業部門からの連絡の方が適切な場合も多い）

なお、組織の内外への開示内容等についての詳細は、10 章で説明します。

初動対応事項・復旧事項

サイバー攻撃を検知した場合、対外接続されているネットワークを遮断したり、攻撃対象となっているサービスを停止したりすることで、外部への情報流出や外部からの不正操作を停止させる効果が期待できますが、これらの操作によって社内の業務や社外とのコミュニケーションが不可能になってしまう弊害もあります。ログ等の分析で検知した場合は、検知の時点ですでに情報が流出してしまっている可能性も高く、遮断や停止を行うことによる効果は必ずしも期待できません。これらを踏まえて、どのような状態に至った場合に、サービスを停止するかといったことも事前に検討しておく必要があります。例えば、以下のような場合には、原因究明や被害拡大を避けるためにサービスを停止することが考えられます。

- マルウェア感染の疑いがあり検査をしないといけない場合
- 脆弱性があるシステムやサービスを停止し改修や設定変更する場合
- 不正に外部との通信を行っている場合
- 特定のファイルを変更または削除し続けている場合

サービス停止の検討を行う主体は、経営者や事業部門トップとの合議により判断される場合や、特定の事態において権限を移譲された CISO 等が判断する場合など、企業の形態により様々です。さらに、サービスの復旧についても検討すべき事項は多数あります。サービス妨害攻撃（DDoS 攻撃）の場合、サービスを復旧させた途端に攻撃が再開されることもあります。脆弱性を悪用した攻撃の場合は、脆弱性に対処した後であれば再開しても問題ないと考えられがちですが、すでに社内ネットワークに攻撃用のボット[45]が仕掛けられている可能性もあり、外部接続の再開とともに社外にある C&C サーバ（コマンド&コントロールサーバ：攻撃の指令を行う）との通信が復活することで、攻撃が再開されることもあります。これらを踏まえると、復旧等の判断を行う際には、サイバーセキュリティ関連サービスのベン

[45] コンピュータを外部から遠隔操作するための不正プログラム

ダやコンサルタントの支援を得るのが適切と言えます。しかしながら、初動の直後はこうした外部リソースをすぐに活用できるとは限らないため、ログから検知される内容や状況に応じて対処すべき内容をまとめた手順書等を整備することが望まれます[46]。

事後対応事項

インシデントが落ち着いたところで行うのが、原因究明と再発防止策の策定です。インシデントに至った原因を明らかにした上で、再発することがないようにサイバーセキュリティ対策や業務手順の見直しを図り、PDCA サイクルを通じて全社に反映させます。

9-3 定期的・実践的な演習の実施

以下では緊急時対応体制の不備な点を洗い出し、関係者の緊急時対応スキルの習熟を図るために行う訓練や演習に盛り込むべき観点を示します。また、対応担当者には実際にサイバー攻撃に対応するための訓練や演習を実施することで、インシデント発生時の対応能力を向上させます。

初動対応マニュアルの有効性の検証

日常の業務で用いるマニュアルは、日々使用している中で不備な点や改善したほうがよい事項などが洗い出され、改善される機会が比較的多くあります。一方でインシデントを対象にした初動対応マニュアルは、適切な対策を実施しながら業務を行っている場合、初動対応を行う機会がなかなか発生せず、改善の機会が少ないと考えられます。そこでこうした初動対応の機会を予め経験してもらう観点から、CSIRT 担当者を対象とする訓練や演習を行う際に、インシデント時に報告した内容が適切であったか、また、それらの報告をもとに判断した内容は適切であったか、他にどのような対処手段が考えられたのか等、訓練や演習参加者による振り返りを行うとととともに、初動対応マニュアルの有効性の検証を行うことが望まれます。例えば、インシデント内容に応じて、以下のような内容がチェック対象となります。

- 発生確認と報告にどの程度の時間がかかるか、どのようなルートで報告されるのか
- 告知や連絡する先や被害届の提出の判断等
- インシデント発生時にマニュアルや手順書のとおりに行動できるか
- 不足している内容はないか、等

マニュアルに記載されている内容が現実的でない、あるいは書いていない作業が重要であるなどのチェック結果をもとに、より有効な内容に修正します。例えば、マニュアルに記載されているとおりの連絡先に連絡した時に、相手先の業務用携帯電話の番号が変わっていることが演習でわかり、社内の電話番号簿を更新し、この電話番号簿との整合を確認させなければならないということが判明することもあります。なお、具体的なインシデント事例

[46] ログ分析方法を用いたサイバー攻撃の対処は、高度サイバー攻撃への対処におけるログの活用と分析方法 <https://www.jpcert.or.jp/research/apt-loganalysis.html>、情報システムのログ管理については、企業における情報システムのログ管理に関する実態調査報告書 <https://www.ipa.go.jp/security/fy28/reports/log_kanri/>が参考になります。

を想定したマニュアルの作成については、JPCERT/CC の「インシデント対応マニュアルの作成について」[47]が参考になります。

社内組織（部門）間のコミュニケーション、共同作業の有効性の検証

訓練や演習で特に重要なことは、技術的な対応だけではなく、経営者へのエスカレーション方法の確認やプレスリリースの発出方法及び所管官庁等への報告手順も含めて実施することで、訓練や演習の参加者のコミュニケーションの方法についても実際に体感し、今後の対応に活かせるものにすることです。エスカレーションのタイミングなどは、頭で考えている内容の通りにできるとは限らないため、望ましいタイミングで受け手に情報が届くようにするにはどのタイミングで情報を発信するのがよいのかを、訓練や演習を繰り返すことで確認します。

CSIRT 要員のスキル・量の十分性の確認

インシデント対応の訓練や演習を行う過程で、実際にどの程度の要員が必要となるかが明らかになります。要員が不足していることが理由で対応が遅れてしまった場合、増員することでより迅速な対応が可能となることが考えられます。なお、インシデント対応が長時間にわたる場合についての訓練や演習を行うのは簡単ではありませんが、実際に発生する可能性はあるため、交代要員による対応の継続について検討しておく必要があります。

一方、スキルの十分性については、スキルがあっても適切な判断ができるとは限らないため、簡単には確認できません。それでも、対応や判断のミスがスキル不足に起因すると考えられる場合は、想定される脅威についての知識や対応方法の習得を促すことで改善効果が期待できます。

セキュリティ技術対策の効率性・十分性の確認

技術的対策が有効かどうかの確認を行うには、インシデントに対応する要員向けとは異なる演習が必要となります。具体的には、サイバーセキュリティ対策に関する専門的な能力を有するベンダ等に依頼して、擬似的な攻撃（脆弱性診断等）を行うことで、対策が有効かどうかを検証します。

訓練・演習の考え方

サイバー攻撃を受けた場合の状況把握や、被害内容の確認、対策を行うのは緊急時であり、緊急時の判断は体験したことがない状況での判断を求められます。そのため、見聞きして理解している知識よりも演習を含んだ体験や経験が重要になります。例えば、サイバー攻撃の原因や被害の状況を経営者に報告する際に、技術的な専門用語や場合によっては法的な用語が含まれる可能性があるため、適切にコミュニケーションできる方法や適時判断を下すために必要な情報を関係者間でどのように共有するかといったことが、訓練や演習を通じ

[47] インシデント対応マニュアルの作成については、JPCERT/CC CSIRT マテリアルから入手できます。
https://www.jpcert.or.jp/csirt_material/build_phase.html

て体験できます。また、10 章に示す外部への開示や報告を想定した場合は、事業部門だけではなく、法務部門や広報部門や渉外担当部門など複数の部門が連携して状況把握や対策にあたる必要があります。組織外部への開示や報告を含んだ訓練や演習を実施することで、連携の不備がわかるほか、複数の事業部や組織が連携する場合に不足していることや気を付けるべきことも学ぶことができます。

定期的な訓練実施

サイバー攻撃は、様々な攻撃手法があり、日々、高度化する傾向があります。そのため、訓練や演習は、一度実施すればよいということはなく、様々なケースを想定して繰り返し実施する必要があります。実際のインシデント発生時には、どのような原因で、どの程度の被害が想定できるのかがわからない状態からはじまる場合が多く、同様のケースで訓練する場合でも初期の発覚や報告を変化させることで、より実践的な訓練を行うこともできます。このような訓練を定期的に繰り返し行うことで、対応手順が定着し、緊急時にも確実に対応できるようになると期待できます。

企業例示「緊急時の対策検討」

仮想企業Ａ社及びＢ社が緊急時の対策について検討、実施した内容やポイントを示します。

企業Ａ社の緊急時の対策検討　**EC サイト運営（中小企業）**

Ａ社では、サイバー攻撃を受けた場合に、最も影響のある EC サイトの緊急時対応体制を検討しました。Ａ社の検討のポイントを示します。

■緊急時対応体制

- 緊急時対応体制の設置や運用にかかる手間やコストを考慮し、サイバーセキュリティリスク管理体制をもとに緊急時対応に必要と思われる部門や担当者に限定し、構築することを検討した。

- CISO は、自らを緊急時対応体制の責任者として、EC サイトを運営する EC 運用部門と情報システム部門を中心に緊急体制を構築した。また関連する他の部門（総務部門、営業部門）の責任者を緊急時対応の担当者として任命し、体制を整備した。

■マニュアル類の作成

・　緊急時対応に必要となるマニュアル類は、JPCERT/CC など資料を参照し、EC 運用部門と情報システム部門が分担して作成することとした。

・　特に、EC サイトに対する不正アクセスや改ざんが発生した場合を想定して具体的な手順書を作成した。この手順書作成の作業の過程で不正アクセスや改ざんの検知が重要であると再認識し、検知を強化する計画を作成した。

■演習・訓練

・　上記で作成した手順書が実際に利用できるかを確認するために、検知から対処までの机上訓練を実施し、追加・修正を行った。

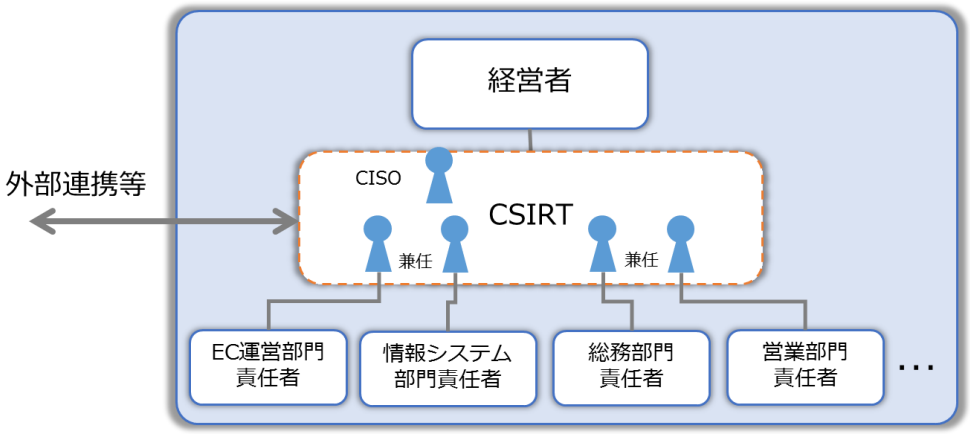


図　9－2　A社の緊急時対応体制

企業Ｂ社の緊急時の対策検討　　**電子機器製造（大企業）**

Ｂ社は、取引先等の関連する企業やグループ企業との情報共有に関する準備を行いました。Ｂ社の検討のポイントを示します。

■緊急時対応体制

・　緊急時対応体制の設置については、現在、グループ全体で検討しているため、これらの検討の中で自社の緊急時対応体制をどのように位置付けるかを検討した。

・　サイバーセキュリティリスク管理体制の CISO は、情報システム部門のトップを緊急時対応体制の責任者として任命し、関連する部門の責任者を兼任で緊急時対応体制に任命した。関連する主な部門は、事業部門、営業部門、及び広報部門とした。

・　各グループ企業は、各社で緊急時対応体制を構築し、各企業の緊急時対応体制の責任者を構成員としたグループ横断的な緊急時対応体制を構築することとした。以降、整備状況が整った際に、グループの CSIRT として立ち上げ、組織内外に存在を知ってもらい情報を集めやすくすることを検討した。

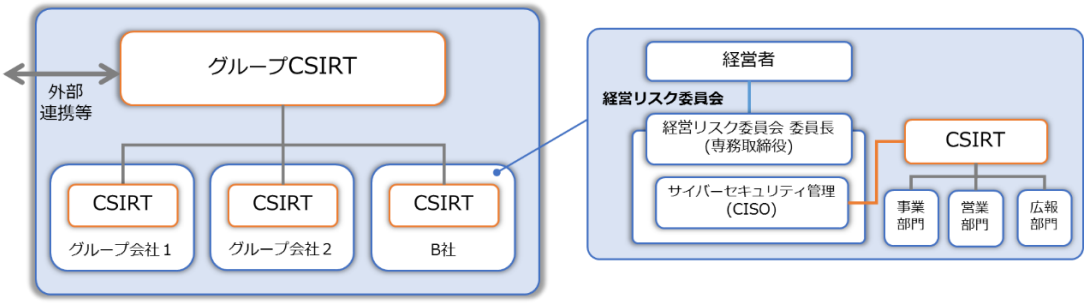


図　９－３　　Ｂ社及びＢ社グループの緊急時対応体制

■マニュアル類の作成

・　緊急時対応に必要となるマニュアル類は、JPCERT/CC などの資料を参照して作成することとした。

・　日本シーサート協議会に参加し、マニュアル作成において自社が工夫した点や、他社の工夫した点等について情報交換を行うことで、効率的にマニュアルを作成す

る等、情報を収集しつつ作成を進める方法について検討した。

・ 上記で作成したマニュアルや作成時に参考になる情報等をグループ内でも共有することとした。

■演習・訓練

・ 緊急時の演習は、 B社の重要情報が漏えいした場合を想定し、CSIRT 内での情報収集及び原因究明と対処を実施した。これらの演習によって、上記で作成したマニュアル類に不足している内容を議論、検討し、追加修正を行った。

・ 外部のサービスを利用し、標的型攻撃メールの訓練を実施した。この訓練の結果をもとに、どのようなメールに気を付けるべきか、添付ファイルを開いてしまった場合に、誰に何を報告するのかを再徹底した。

１０ 被害発覚後の必要な情報の把握、開示体制の整備

サイバー攻撃の被害が発生した際に円滑な状況把握ができるよう、収集すべき項目や情報を整理し、被害を受けたことを通知すべき相手方のリスト整備、経営者による説明の準備を予め進めておくことが大切です。

実施内容 10
１．サイバー攻撃の被害発覚時に備え、通知や開示が必要な項目や、関係者やステークホルダー等の通知先を整理しておく。 ２．予め経営者への報告方法を取り決め、経営者が組織の内外に報告、説明できるように準備する。

１０-１ 被害発覚後の情報収集体制および開示すべき項目の整備

サイバー攻撃を受け被害が発覚した場合に備えて、事前に被害発覚後の全社的な対応方針について検討し、体制を整備しておく必要があります。現状において適切と考えられるサイバー攻撃対策を講じていたとしても、そうした対策が今後生じる可能性のある新たなサイバー攻撃に対処できるとは限らないため、定期的に見直すことを踏まえておく必要があります。

開示・報告すべき情報の把握

被害発覚後の対応で重要なことは、関係者への通知に必要な情報を集約するとともに、被害の拡大防止や二次被害の回避など必要な対策を速やかに講じられるようにすることです。そのためには、インシデントに関する被害状況や他社への影響などに関する情報を速やかに収集できる体制が必要です。こうした情報を集約するための体制が構築できていない場合は、他の自然災害等における危機管理体制をベースに、適宜サイバーセキュリティリスクに関する項目等を追加し、極力既存の体制を活かして構築します。

通知先のリスト化と通知用のフォーマット作成

被害が発生した際にどこに通知すべきかを検討する際には、組織内で管理している情報（社外からの入手情報や共有情報等）や IT に関する製品、サービスごとに整理します。そのため、セキュリティ担当者だけでなく、事業部門や営業部門とも連携しながら通知先のリスト（一覧）を作成する必要があります。また、個人情報漏えいなど、インシデントの種類によっては、所管官庁やステークホルダーも報告先に含める必要があるため、予め情報開示の手段についても確認しておく必要があり、特に関連法令を確認して法的義務が遵守されるように具体的な手続きを確認しておくことが重要です。詳細は IPA から公表されている

「情報漏えい発生時の対応ポイント集」[48]や９章の表９－３に掲載した緊急連絡先の例等を参考に、通知先のリストや通知用のフォーマットを作成してください。

通知に必要な情報の整理と周知

通知先のリストや通知用のフォーマットを作成した後に、それらを被害発覚後の対応に従事する担当者と共有しておく必要があります。組織内への周知においては、インシデント内容や被害の状況により関連する部門や責任者を漏れなく抽出しておくことが重要です。

被害発覚後の対応で最低限必要な担当者は、緊急時に意思決定する責任者、インシデント対応や分析の担当者、及び外部との窓口担当者等になります。

組織の内外への開示・報告内容、タイミング

開示・報告すべき内容は、インシデントにより異なりますが、5W1H をもとに何が起こったのかが特定できるように把握します。具体的には、インシデントに関して「誰の」、「何に関する情報、システム、サービス等が」、「いつ頃」、「どの程度」、「どのような経由で」、「どのような状態か」を明確にして整理します。また、これらの事象の状況把握とともに、被害の状況や二次被害の可能性についても確認します。

開示・報告は、できるだけ早く行うことが望ましいですが、インシデントや被害の状況に応じて、初期発生時、被害状況把握時、インシデント収束時等の段階に応じて検討していきます。

被害の原因や規模、拡大する可能性等が不明な状況で開示しても、かえって関係者の不安をあおり、混乱をきたす場合があります。一方で開示に慎重を期すあまり対応が遅くなり、自社からの発表の前に第三者から情報漏えい等についての指摘がなされ、それが報道されると、マスメディアや社会から「事故隠し」と指摘されるおそれがあります。また所管官庁への報告がこうした報道の後になってしまうと、所管官庁からも報告が遅い旨の指導を受けることになります。

上記を踏まえ、インシデントや被害の状況に応じて、一部の情報が不明の状態であっても、ある程度被害状況が把握できた時点（例えば、被害の「封じ込め」ができた時点）等に、情報が完全に揃うまで待たずに速やかに開示することを検討します。

なお、インシデントが収束した時点でも改めて開示し、今後の被害の可能性、再発防止策、停止していたサービスの再開時期、事態が収束したこと等を開示・報告する必要があります。

開示・報告先について留意すべき点

開示・報告等に際しては、対象となる相手先によって、留意すべき点が異なります。詳細については、表 10-1 及び「情報漏えい発生時の対応ポイント集」（再掲）を参考にしてください。

[48] https://www.ipa.go.jp/security/awareness/johorouei/

表 １０－１　開示・報告先における留意点

開示･報告先	開示･報告時の留意点
所管官庁	･先方の窓口を事前に確認しておき、誰が報告するかも決めておく(日頃相談や報告、指導を受けている事業部門の担当者等と連携する等)。
サイバーセキュリティ関係機関(IPA, JPCERT/CC)	･サイバー攻撃の内容、実施していた対策、被害の概要等を報告する。 ･同種の攻撃手法等による二次被害を避けるため、至急報告する。
報道機関／マスメディア	･窓口を一本化し、対外的な情報に不整合が起こらないようにする。 ･レピュテーションの影響も踏まえて、法務部門、広報部門等と連携し、適切な公表時期を慎重に判断する。 ･SNS 等のソーシャルメディアにより、社会的に当該インシデントがどのように受け止められているか動向を確認する(次に何をすべきか等の参考にする)。 ･自社の HP 上で公表する等、謝罪する際には、他の企業の類似案件におけるお詫び文等を参考にする。 ･被害の状況に応じて、経営者が記者会見を行うことを想定し、公表する内容を検討する。
顧客	･被害者に至急その事実を通知しお詫びするとともに、個人情報(顧客情報)漏えいの場合は、詐欺や迷惑行為などの被害にあわないように注意喚起する。 ･被害者に連絡する方法(メーリングリストで一斉送信等)を確認･整備しておく。
ビジネスパートナー／同業者	･対処に必要な情報を速やかに関係者と共有する(外部委託先や、提携しているクレジットカード会社等)。 ･同業種を狙った一斉攻撃の可能性があるため、攻撃手法等を同業者間で共有する。

１０-２　組織内外へ経営者が説明できる体制の整備

被害が判明した後の組織内外への報告については、情報管理の責任者である経営者が感染被害の経緯や状況を公表し、ステークホルダー等の関係者に対する説明責任を果たす必要があります。経営者が説明できる体制を整備するために、報告ルートや報告する内容、タイミングに関するルール等を整備します。９章で示した CSIRT の体制整備の中で、こうした情報開示を担う体制を併せて整備しておくことも有効と考えられます。

経営者への報告ルートや報告ルールの整備

被害が判明した際に、経営者が組織の内外へ公表する場合に備えて、経営者や CISO 等への報告ルートを明確にしておきます。また経営者や CISO 等への報告ルールは、インシデントに関する被害状況や他社への影響などを中心に、必要な対策を講じるための判断材料を提示することを念頭におき、報告するべき内容や粒度等について検討します。

なおインシデントの全てを経営者に報告しても、正確な状況の把握や状況に応じた判断ができない可能性が高いため、９章で示したように、エスカレーションの基準を設定し、その基準に沿って CISO 等が情報の集約を行った上で、経営者に報告する体制を整備します。

実際に報告ルートやルール等を整備する際には、自組織で発生する可能性がある被害を想定したシナリオを検討し、そのシナリオに基づいて、具体的な役割も含めて検討するようにします。

企業例示「被害発覚時の準備」

仮想企業Ａ社及びＢ社が被害発覚時の準備について検討、実施した内容やポイントを示します。

企業Ａ社の被害発覚時の準備　**EC サイト運営（中小企業）**

個人情報漏えいの際の顧客への通知のタイミング

A 社が、被害発覚後の情報の把握と開示体制の整備に関して最初に取り組んだのは、社外の関係者に情報を開示するタイミングの検討でした。

A 社の事業は EC サイトの運営が主たる業務につき、EC サイトをご利用いただく個人のお客様からの信頼確保こそ最優先すべきだということが、A 社サイバーセキュリティ委員会（１章企業例示を参照）の結論になりました。もし、A 社自身の利益をお客様の利益に優先するならば、お客様の信頼を失うことに繋がりかねません。個人のお客様と距離の近い事業をしている以上、ひとたびお客様の信頼を失えばおそらく事業を継続する事はできない、と考えました。

そこで、お客様の個人情報が漏えいしたと判断した場合は、お客様が詐欺や迷惑行為などの被害にあわないよう注意喚起するため、遅滞なくその事実をお客様自身に連絡する、というルールを決めました。

実は委員会の議論では、A 社の収益の柱である EC サイトを止めないことが最優先との意見もでました。以前の委員会で、サイバーセキュリティ上重要な保護資産は、A 社自身の通販サイトの会員顧客の個人情報（の機密性）と、EC サイトのシステム（の可用性）であると決めています（１章企業例示を参照）。もしこの二つが相反する事態になった場

合、どちらを優先すべきか、という議論になりましたが、なかなか結論に至りませんでした。社会一般においても意見が分かれるかもしれませんが、あくまでもＡ社の判断として今回の結論となりました。

また、お客様の個人情報が漏えいした際のルール作りで検討すべき事は、お客様への連絡のタイミングだけではありません。所管官庁、サイバーセキュリティ関係機関、報道機関など他の関係者への通知のタイミングをどうするか、どんな内容を通知するかなど、多くの懸案事項があります。これらについても、社会一般に受け入れられる考え方が定まっていないとすると、セキュリティガバナンスの専門家や弁護士などと相談して、時間を掛けて検討する必要があるということになりました。

企業Ｂ社の被害発覚時の準備　**電子機器製造（大企業）**

Ｂ社は、取引先等のビジネスパートナーやグループ企業を踏まえて、被害発覚後の情報の把握と開示体制の準備について検討しました。Ｂ社の検討のポイントを示します。

- サイバー攻撃によって重要情報が持ち出された場合や喪失した場合を想定し、自社の重要情報や他社から預かる重要情報ごとに、取引先や関係者をリストアップした。具体的な重要情報と関係する企業やグループ企業の特定は、その情報を管理している担当者が記載し、最終的にリスク管理部門で取りまとめ、通知先リストを作成した。

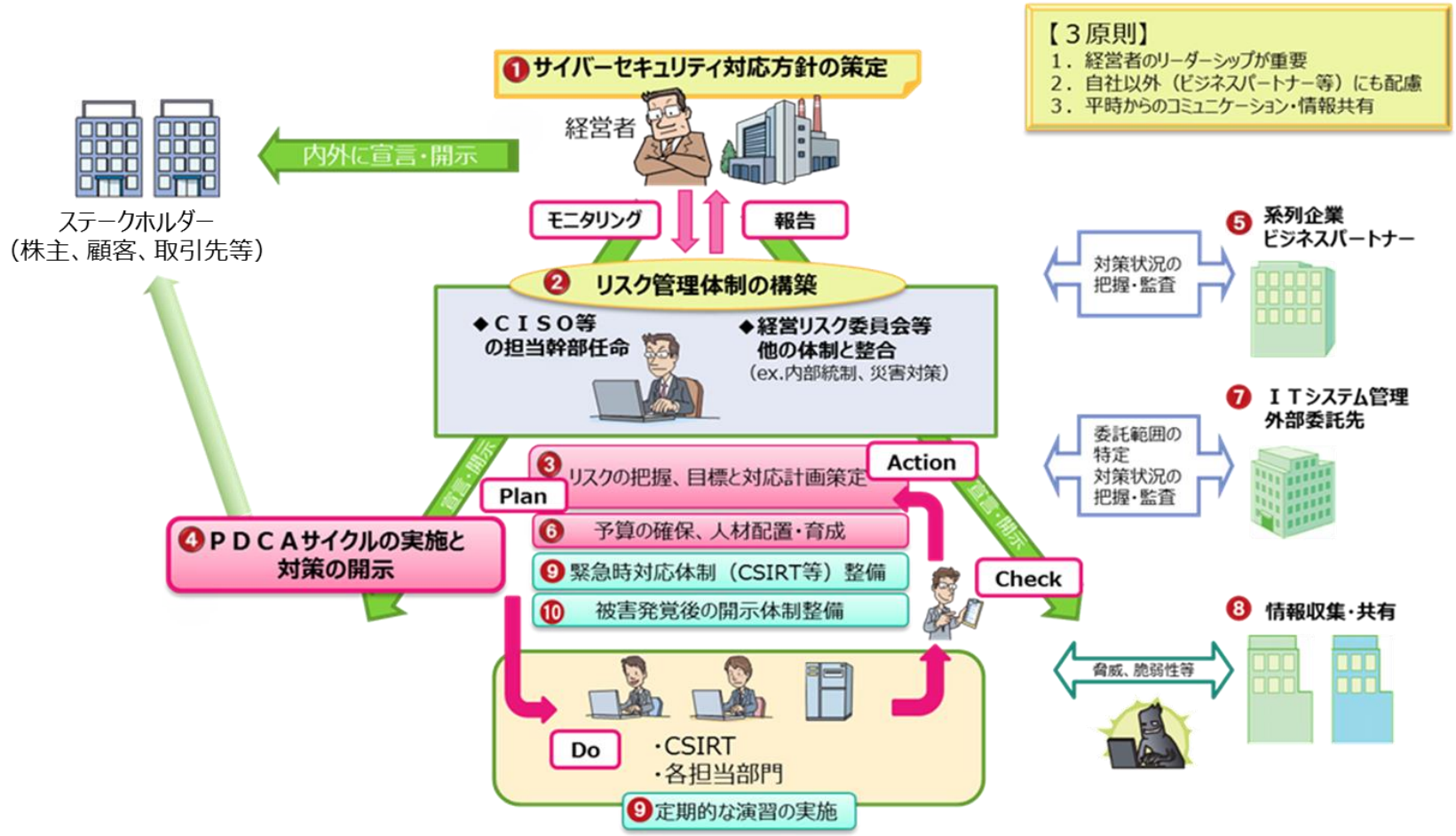
- 各重要情報の持ち出しや喪失の可能性があるとわかった場合に、どのような状況が確認された時点で情報を共有すべきか等について通知先リスト作成者及び法務部門で検討し、関係企業やグループ企業と議論した。

- 関係企業やグループ企業と議論した結果、以下の点についても詳細化する必要があり、引き続き検討を進めることとした。
  - サイバー攻撃は定時外にも発生する可能性があるため、緊急時に確実に連絡ができる緊急連絡先を作成し共有する。

- 業務提携している企業などのビジネスパートナーと共有している重要情報やIT システムについて、被害発覚後に外部へ情報開示する場合は、開示のタイミング等、業務提携先との調整も必要である。情報開示の方針について事前に共有しておく必要がある関係者は、グループ企業も含めてどこがあるかについて整備する。

付録 1 ガイドラインの 3 原則と重要 10 項目概要図

経営者が認識する必要がある「3 原則」に基づき、経営者が CISO 等に指示すべき「重要 10 項目」の概要を以下に示します。



付録 2 参照情報

各章で対策検討を行う上で参考となる情報を以下に示します。

0 はじめに

【ガイド】

- 内閣官房　内閣サイバーセキュリティセンター（NISC）　企業経営のためのセキュリティの考え方
  http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

1 サイバーセキュリティリスク対応方針の策定

【ガイド】

- IPA　中小企業の情報セキュリティ対策ガイドライン
  http://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
- IPA　組織における内部不正防止ガイドライン（付録Ⅴ：基本方針の記述例）
  https://www.ipa.go.jp/security/fy24/reports/insider/
- 総務省　地方団体における情報セキュリティポリシーに関するガイドライン 第２章
  http://www.soumu.go.jp/denshijiti/jyouhou_policy/

2 リスク管理体制の構築

【ガイド】

- 国立情報学研究所　高等教育機関の情報セキュリティ対策のためのサンプル規程集
  http://www.nii.ac.jp/csi/sp/
- JNSA　情報セキュリティポリシーサンプル
  http://www.jnsa.org/result/2016/policy/
- IPA　中小企業の情報セキュリティ対策ガイドライン
  http://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
- 総務省　地方団体における情報セキュリティポリシーに関するガイドライン
  3.2 節
  http://www.soumu.go.jp/denshijiti/jyouhou_policy/
- IPA　組織における内部不正防止ガイドライン（付録Ⅴ：基本方針の記述例）
  https://www.ipa.go.jp/security/fy24/reports/insider/

3 リスクの把握、目標と対応計画策定

【ガイド】

- IPA　中小企業の情報セキュリティ対策ガイドライン
  http://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
- IPA　「高度標的型攻撃」対策に向けたシステム設計ガイド
  https://www.ipa.go.jp/security/vuln/newattack.html
- IPA　2015 年 6 月 2 日【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を
  https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html
- IPA　情報セキュリティ 10 大脅威 2015（1 章対策の基本）
  https://www.ipa.go.jp/security/vuln/10threats2015.html
- IPA　組織における内部不正防止ガイドライン
  https://www.ipa.go.jp/security/fy24/reports/insider/
- JPCERT/CC　高度サイバー攻撃への対処におけるログの活用と分析方法
  https://www.jpcert.or.jp/research/apt-loganalysis.html

【ツール】

- IPA　iLogScanner
  https://www.ipa.go.jp/security/vuln/iLogScanner/

【参考】

- IPA　情報セキュリティ対策ベンチマーク普及検討会編　情報セキュリティ対策ベンチマーク活用集（付録）（PDF）
  https://www.ipa.go.jp/files/000011529.pdf
- 一般財団法人日本情報経済社会推進協会　ISMS ユーザーズ・ガイド ―JIS Q 27001:2006 (ISOS/IEC 27001:2005) 対応－（PDF）
  https://www.isms.jipdec.or.jp/doc/JIP-ISMS111-21_2.pdf
- 一般財団法人日本情報経済社会推進協会　事業継続管理（BCM）に関する利用ガイド（PDF）
  https://www.isms.jipdec.or.jp/doc/BCM1803.pdf

4 PDCA サイクルの実施と対策状況の開示

【制度】

- JIPDEC　情報セキュリティマネジメントシステム（ISMS）適合性評価制度
  https://www.isms.jipdec.or.jp/isms.html
- JIPDEC　サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度
  https://www.isms.jipdec.or.jp/csms.html
- 経済産業省　情報セキュリティ監査制度
  http://www.meti.go.jp/policy/netsecurity/index.html

【ツール】

- IPA　情報セキュリティ対策ベンチマーク
  http://www.ipa.go.jp/security/benchmark/
- IPA　 My JVN バージョンチェッカ
  http://jvndb.jvn.jp/apis/myjvn/vccheck.html

【文献】

- IPA　安全なウェブサイトの作り方（ほか『別冊：ウェブ健康診断』）
  https://www.ipa.go.jp/security/vuln/websecurity.html
- IPA　ウェブサイトにおける脆弱性検査手法の紹介(ウェブアプリケーション検査)
  https://www.ipa.go.jp/about/technicalwatch/20131212.html

【参考】

- JNSA　JNSA ソリューションガイド
  http://www.jnsa.org/JNSASolutionGuide/
- 経済産業省　情報セキュリティ報告書モデル
  http://www.meti.go.jp/policy/netsecurity/secgov-tools.html#report-model

5 系列企業・ビジネスパートナーの対策実施及び状況把握

【ガイド】

- 経済産業省　情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン（PDF）
  http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf

【参考】

・ 経済産業省　情報セキュリティ監査企業台帳
http://www.meti.go.jp/policy/netsecurity/is-kansa/

【制度】

・ 特定非営利活動法人日本セキュリティ監査協会　クラウド情報セキュリティ監査制度
http://jcispa.jasa.jp/cloud_security/
・ 一般財団法人マルチメディア振興センター　ASP・SaaS の安全・信頼性に係る情報開示認定制度
https://www.fmmc.or.jp/asp-nintei/about.html
・ 一般財団法人マルチメディア振興センター　IaaS・PaaS の安全・信頼性に係る情報開示認定制度
https://www.fmmc.or.jp/ip-nintei/about.html
・ 一般財団法人マルチメディア振興センター　データセンターの安全・信頼性に係る情報開示認定制度
https://www.fmmc.or.jp/dc-nintei/about.html

6 予算確保・人材配置及び育成

【ガイド】

・ IPA　情報セキュリティ強化対応スキル指標／職場の情報セキュリティ管理者の育成検討
https://www.ipa.go.jp/jinzai/hrd/security/
・ IPA　IT のスキル指標を活用した情報セキュリティ人材育成ガイド（PDF）
https://www.ipa.go.jp/files/000039528.pdf

【参考】

・ IPA　情報セキュリティスペシャリストキャリアパス事例集（PDF）
https://www.ipa.go.jp/files/000014185.pdf

7 IT システム管理の外部委託

【ガイド】

- 経済産業省　情報システムに係る政府調達への SLA 導入ガイドライン（PDF）
  http://www.meti.go.jp/policy/it_policy/tyoutatu/sla-guideline.pdf
- 経済産業省　SaaS 向け SLA ガイドライン（PDF）
  http://www.meti.go.jp/committee/materials/downloadfiles/g80207c05j.pdf
- 経済産業省　クラウドサービス利用のための情報セキュリティマネジメントガイドライン（PDF）
  http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf
- 経済産業省　クラウドセキュリティガイドライン活用ガイドブック（PDF）
  http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf
- 総務省　クラウドサービス提供における情報セキュリティ対策ガイドライン（PDF）
  http://www.soumu.go.jp/main_content/000283647.pdf
- 総務省　ASP・SaaS における情報セキュリティ対策ガイドライン（PDF）
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/pdf/asp_saas_zentai.pdf

【参考】

- IPA クラウドサービス安全利用のすすめ
  http://www.ipa.go.jp/security/keihatsu/pr2012/ent/02_cloud.html

8 情報収集と情報共有

【制度】

- IPA　コンピュータウイルス、不正アクセス、脆弱性関連情報に関する届出
  https://www.ipa.go.jp/security/outline/todoke-top-j.html
- IPA　標的型サイバー攻撃特別相談窓口
  https://www.ipa.go.jp/security/tokubetsu/index.html
- IPA 情報セキュリティ早期警戒パートナーシップガイドライン
  https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- IPA　サイバー情報共有イニシアティブ（J-CSIP）
  https://www.ipa.go.jp/security/J-CSIP/
- JPCERT/CC　インシデントの報告

https://form.jpcert.or.jp/

- JPCERT/CC　早期警戒情報の提供
  https://www.jpcert.or.jp/wwinfo/
- 日本シーサート協議会
  http://www.nca.gr.jp/

【情報収集】

- IPA 重要なセキュリティ情報一覧
  http://www.ipa.go.jp/security/announce/alert.html
- JPCERT/CC 注意喚起
  https://www.jpcert.or.jp/at/
- 警察庁セキュリティポータルサイト「@police」
  http://www.npa.go.jp/cyberpolice/
- NIST(訳：IPA)　コンピュータセキュリティログ管理ガイド(SP 800-92)（PDF）
  https://www.ipa.go.jp/files/000025363.pdf
- NIST(訳：IPA)　マルウェアによるインシデントの防止と対応のためのガイド(SP 800-83)（PDF）
  https://www.ipa.go.jp/files/000025349.pdf
- 経済産業省　コンピュータウイルス対策基準
  http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
- IPA　『高度標的型攻撃』対策に向けたシステム設計ガイド
  https://www.ipa.go.jp/security/vuln/newattack.html
- JPCERT/CC　高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
  https://www.jpcert.or.jp/research/apt-guide.html
- IPA　ウェブサイト構築事業者のための脆弱性対応ガイド
  http://www.ipa.go.jp/security/fy20/reports/vuln_handling/
- フィッシング対策協議会　フィッシング対策ガイドライン
  https://www.antiphishing.jp/report/guideline/

9 緊急時対応体制の整備と演習の実施

【体制整備】

- JPCERT/CC　CSIRT マテリアル
  https://www.jpcert.or.jp/csirt_material/
- IPA　企業における情報システムのログ管理に関する実態調査報告書
  https://www.ipa.go.jp/security/fy28/reports/log_kanri/
- 日本シーサート協議会　CSIRT スターターキット（PDF）
  http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf
- 日本シーサート協議会　CSIRT 人材の定義と確保
  http://www.nca.gr.jp/activity/training-hr.html
- ISOG-J 「やられたかな？その前に」ガイド
  http://isog-j.org/activities/result.html
- 中小企業庁　中小企業 BCP（事業継続計画）ガイド
  http://www.chusho.meti.go.jp/keiei/antei/2008/080418bcp_gude.html
- 内閣府　事業継続ガイドライン
  http://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk_04.html
- 経済産業省　事業継続計画策定ガイドライン（PDF）
  http://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyoKeizokuKeikakuSakuteiGuideline.pdf

【攻撃検知・被害特定】

- IPA　潜伏しているかもしれないウイルスの感染検査を今すぐ！
  https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html
- JPCERT/CC　Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起
  https://www.jpcert.or.jp/at/2014/at140054.html
- JPCERT/CC　高度サイバー攻撃への対処におけるログの活用と分析方法
  https://www.jpcert.or.jp/research/apt-loganalysis.html

10 被害発覚後の必要な情報の把握、開示体制の整備

【体制整備】

- IPA　情報漏えい発生時の対応ポイント集

https://www.ipa.go.jp/security/awareness/johorouei/

- JPCERT/CC　　CSIRT マテリアル
  https://www.jpcert.or.jp/csirt_material/
- 日本シーサート協議会　CSIRT スターターキット（PDF）
  http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf
- ISOG-J 「やられたかな？その前に」ガイド
  http://isog-j.org/activities/result.html
- 情報セキュリティ大学院大学　情報セキュリティ事故対応ガイドブック
  http://lab.iisec.ac.jp/~hiromatsu_lab/sub07.html

その他 データ

[1] 企業の CISO や CSIRT に関する実態調査 2016　IPA
https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/

[2] 企業におけるサイバーリスク管理の実態調査 2015　IPA
https://www.ipa.go.jp/security/fy27/reports/cyber-ins/

[3] セキュリティ関連コンテンツ一覧、経営者向けコンテンツ、運用者向けコンテンツ、開発者向けコンテンツ　経済産業省
http://www.meti.go.jp/policy/netsecurity/secdoc/secdoc_list.html

付録 3 サイバーセキュリティ経営チェックシートの実施の目安と確認事項

ここでは、本ガイドラインの「付録Ａ サイバーセキュリティ経営チェックシート」の項目について、判断基準の参考となる目安と確認事項を記載しています。同チェックシートを活用する際に、適宜利用してください。

なお、下記の事項については、CISO 等から実施確認の指示を受けた組織内部の担当者が、チェックシートに基づいて確認することを想定しています。

(1) サイバーセキュリティリスクの認識、組織全体での対応の策定

(1)-1 経営者がサイバーセキュリティリスクを経営リスクの１つとして認識している

【実施の目安】

- セキュリティポリシーに、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任について記載している。
- 経営会議や経営リスクに関する委員会等において、サイバーセキュリティリスクを検討している。

【実施の確認事項】

- サイバーセキュリティリスクに特化したセキュリティポリシーを新たに策定する場合には、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任に関する事項が記載されている。
- 既存の「情報セキュリティポリシー」や「情報セキュリティの取り組みについて」等にサイバーセキュリティへの対策を追記する場合には、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任に関する事項が追記されている。
- 経営会議や経営リスクに関する委員会等において、議事内容にサイバーセキュリティリスクや対応に関する事項があることを検証する。

(1)-2 経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言している

【実施の目安】

- サイバーセキュリティリスクに対する対応方針（セキュリティポリシー）を策定していること、及びサイバーセキュリティリスクに対しては組織全体で対策することを記載している。
- 策定したセキュリティポリシーを経営者が承認、周知している。
- 策定したセキュリティポリシーのうち、必要な部分については、組織外にも宣言して

いる。

【実施の確認事項】

- サイバーセキュリティリスクに対する対応方針（セキュリティポリシー）を策定し、サイバーセキュリティリスクに対しては組織全体を対象に対策することを記載していることを確認する。
- 策定したセキュリティポリシーが、経営者に承認されていることを確認する。
- 策定したセキュリティポリシーが、組織全体に周知されていることを確認する。
- 策定したセキュリティポリシーのうち、必要な部分について、組織外に宣言していることを確認する。
  例）組織外部への宣言については、自組織のホームページにセキュリティポリシーを掲載していることを確認する。

(2) サイバーセキュリティリスク管理体制の構築

(2)-1 組織の対応方針（セキュリティポリシー）に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築している

【実施の目安】

- セキュリティポリシーに記載しているサイバーセキュリティリスク管理体制を構築している。
- セキュリティポリシーにサイバーセキュリティリスク管理体制と CISO 等の役割について記載し、CISO 等を任命している。

【実施の確認事項】

- セキュリティポリシーに記載されているサイバーセキュリティリスク管理体制に基づいて、その体制を実際に構築し、運営している体制が組織のセキュリティリスク管理を遂行していくために必要なリソース条件を満足していることを確認する。
- セキュリティポリシー等に記載されているサイバーセキュリティリスク管理体制の管理責任を負う責任者（CISO 等）に対して、実際に定められた役割に従事していることを確認する。

(2)-2 サイバーセキュリティリスク管理体制において、各関係者の責任を明確にしている

【実施の目安】

・ セキュリティポリシー及び他の資料で、サイバーセキュリティリスク管理体制の関係者と責任を記載している。
・ サイバーセキュリティリスク管理体制に記載している関係者について、各々の責任と役割などについて役割分担表などで文書化している。

【実施の確認事項】

・ セキュリティポリシーや関連するスタンダード（対策基準）、プロシージャー（実施手順）、その他の内規等にサイバーセキュリティリスク管理体制の関係者（部門責任者や担当者、従業員など記載しているすべての役割）と責任（実施や管理及び確認など要求している内容）を記載していることを以下の要領で確認する。
  － セキュリティポリシーにおける記載事項の確認
  － 役割分担表で定められている役割と責任の網羅性に関する確認
  － 役割分担表における記載内容と現実との乖離がないことの確認

(2)-3 組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定している

【実施の目安】

・ サイバーセキュリティリスク管理に関連する情報セキュリティ管理や個人情報保護管理等の管理体制が存在する場合には、その関連する部分及び相違点等を明確に規定している。

【実施の確認事項】

・ 対象となる資産、管理体制（担当者や管理者の重複等）、経営者の関与等について、既存のリスク管理体制と比較し、その違いを経営者や従業員と共有していることを以下の要領で確認する。
  － サイバーセキュリティリスク管理に関する役割分担表等による相違点の確認
  － 経営者や従業員への聞き取り調査

(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

(3)-1 守るべき資産を特定している

【実施の目安】

・ 組織内すべての部門の保有する資産をリストアップし、守るべき資産を特定している。または、経営者や CISO 等との合意の上、優先的に守るべき資産を特定している。

【実施の確認事項】

・ 守るべき資産を特定するには、組織内で対象となる資産をリストアップし、そのリスト等の中から守るべき資産が特定されていることを確認する。
・ 優先度の検討において、経営者や CISO 等の意向や方針が反映されていることを作業過程の資料等を通じて確認する。

(3)-2 特定した守るべき資産に対するサイバー攻撃の脅威を識別し、経営戦略を踏まえたサイバーセキュリティリスクとして把握している

【実施の目安】

・ 情報収集したサイバー攻撃の中から、特定した守るべき資産に対して、具体的なサイバー攻撃を想定した上で、その脅威を識別している。または、経営者や CISO 等との合意の上、想定されるサイバー攻撃に関する脅威を識別している。（すべてのサイバー攻撃事例を網羅的に収集することは困難であるため、IPA が提供している脆弱性に関する情報源などを活用することで効率的に実施する。）
・ 識別した脅威は、経営戦略を踏まえたリスクとして把握している。

【実施の確認事項】

・ 守るべき資産とサイバー攻撃の対応については、CISO 等が脅威を踏まえた上で対応関係を把握していることを確認する。また、必要に応じて外部の専門家などへの相談などにより、守るべき資産に対するサイバー攻撃の可能性についての検討が実施されていることを確認する。
・ 特定のサイバー攻撃の脅威や、最低限対応すべきサイバー攻撃などを特定するなど、優先度を考慮してサイバー攻撃を識別する場合には、組織全体を見渡した優先度の割当が必要であるため、経営者や CISO 等との合意の上、優先的に対応すべきサイバー攻撃を識別する必要がある。この検討過程の記録等を確認する。
・ サイバー攻撃による脅威が経営戦略を踏まえたリスクとして把握されていることを確認するため、経営会議や経営リスクに関する委員会等の議事内容にサイバー攻撃の脅威に関する事項があることを確認する。

(3)-3 サイバーセキュリティリスクが事業にいかなる影響があるかを推定している

【実施の目安】

・ 前述の（３）－１及び（３）－２の検討結果としてサイバーセキュリティリスクが事業にいかなる影響があるかを推定している。

【実施の確認事項】

・ サイバーセキュリティリスクが及ぼす事業への影響については、CISO 等と経営者が推定結果に合意していることを確認する。
・ 経営会議や経営リスクに関する委員会等の議事内容にサイバーセキュリティリスクが招く事業への影響の推定に関する事項があることを確認する。

(3)-4　サイバーセキュリティリスクの影響の度合いに従って、低減、回避のための目標や計画を策定している

【実施の目安】

・ 前述の（３）－１から（３）－３の検討結果をもとに、低減と回避の可能性について検討する。
・ 脅威の影響を低減する目標を設定した上で、対策を講じて脅威発生の可能性を下げることで目標に到達するための計画を策定する。
・ 脅威の回避策として脅威発生の要因を除去することや全く別の方法に変更することを目標として設定し、目標に到達するための計画を策定する。

【実施の確認事項】

・ 脅威の影響に関する低減及び回避に関する目標と計画を策定し、CISO 等が認識していることを確認する。

(3)-5　低減策、回避策を取らないと判断したサイバーセキュリティリスクの移転策（サイバー保険の活用や守るべき資産について専門企業への委託等）を実施している

【実施の目安】

・ 前述の（３）－１から（３）－３の検討結果をもとに、残留リスクの移転策を検討している。
・ 残留リスクの移転に関する具体的な方法と移転先を以下の要領で実施している。
　－情報セキュリティに関連した保険商品（サイバー保険等）への加入
　－自社で実施すると情報漏えい等のリスクが高いと判断される作業の、外部の専門

企業への委託
－移転策について検討した結果、具体的な移転策は実施しないと判断した場合は、その検討過程等の記録を残す。

【実施の確認事項】

・ リスク移転の方法や移転先について、CISO 等が合意していることを確認する。

(3)-6 サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している

【実施の目安】

・ 前述の（３）－１から（３）－３の検討結果をもとに、サイバーセキュリティリスクのうち、対策をとらずに残留リスクとして受容するものを識別する。
・ 残留リスクのうち、リスク発生可能性が低く、かつリスクが発生した場合の損害が小さいものについては、対策を取らず保有（受容）していることが共有されている。
・ 残留リスクのうち、「許容できるリスクのレベル」を超えているが、対策が困難等の理由により、そのまま保有せざるを得ないものについては、経営層が承認している。

【実施の確認事項】

・ サイバーセキュリティリスクを残留リスクとして受容すると判断した根拠を含め、経営層や CISO 等が合意していることを確認する。

(4) サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

(4)-1　経営者が定期的に、サイバーセキュリティ対策状況の報告を受け、把握している

【実施の目安】

・ サイバーセキュリティ対策の計画に対する進捗状況については、年２回～４回を目安として経営者に報告する。
・ 新たなサイバー攻撃への対策状況や組織に発生している軽微なインシデントを含んだエスカレーションの確認など、個別のサイバーセキュリティ対策状況については、月に１回程度を目安として経営者に報告する。

【実施の確認事項】

・　サイバーセキュリティ対策の計画に対する進捗状況については、経営会議や経営リスクに関する委員会等の議事内容にサイバーセキュリティ対策の計画に対する進捗状況の報告事項があることを確認する。
・　個別のサイバーセキュリティ対策状況の報告については、内容に応じてメールや簡易レポート等で実施される場合もあるため、これらの内容を確認する。

(4)-2　サイバーセキュリティにかかる外部監査を実施している

【実施の目安】

・　サイバーセキュリティにかかる外部監査としては、実施している対策内容を第三者の視点で監査及び検査している。
・　第三者の視点での監査としては、例えば、情報セキュリティマネジメントシステム（ISMS）や個人情報保護に関する制度（PMS 等）を対象とした情報セキュリティ監査等を含み、これらの監査は、年に１回程度を目安とする。
・　第三者の視点での検査としては、例えば、脆弱性診断やペネトレーションテスト等の各種のセキュリティ診断を含み、これらの診断は、少なくとも年に１回以上を目安とする。
・　上記の外部監査の実施が困難である場合、サイバーセキュリティリスク管理体制の担当者以外の者による内部監査を実施している。
・　サイバーセキュリティリスクを経営課題のひとつとして捉え、監査役が統括する監査の対象にサイバーセキュリティリスク管理体制についての監査を含めている。

【実施の確認事項】

・　サイバーセキュリティにかかる監査及び検査に関する報告書を確認する。

(4)-3　サイバーセキュリティリスクや脅威を適時見直し、環境変化に応じた取組体制（PDCA）を整備・維持している

【実施の目安】

・　経営者に対する定期的な対策状況の報告（サイバーセキュリティ対策の計画に対する進捗状況や個別のサイバーセキュリティ対策状況報告）に基づき、必要に応じて、新たなリスクや脅威に対する見直しを実施する。見直しの基準については、（３）－１～（３）－６を検討する。

なお、新たなサイバーセキュリティリスクや脅威の情報収集については、「(8) 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のための環境整備」を参照。

【実施の確認事項】

- サイバーセキュリティ対策に関する計画（Plan)、実行（Do)、確認（Check)、見直し（Act）の PDCA のサイクルを経営者及び CISO 等が合意していることを確認する。
- 経営会議や経営リスクに関する委員会等の議事内容にサイバーセキュリティ対策の計画に関する事項があることを確認する。
- さらに、サイバーセキュリティリスクや脅威に関する情報収集から見直しに至る過程で経営者及び CISO 等が合意していることを確認する。

(4)-4　サイバーセキュリティリスクや取組状況を外部に公開している

【実施の目安】

- 以下のいずれかに、サイバーセキュリティリスクや取組状況に関して記載し、外部に公開する。
  - 情報セキュリティ報告書
  - CSR 報告書
  - サステナビリティレポート
  - 有価証券報告書
  - その他

【実施の確認事項】

- サイバーセキュリティリスクや取組状況に関し外部に公開している文書（情報セキュリティ報告書、CSR 報告書、サステナビリティレポート、有価証券報告書、その他）の記載内容を確認する。また、必要に応じてサイバーセキュリティ対策の計画との相違を確認する。

(5) 系列企業やサプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

(5)-1 系列企業や、サプライチェーンのビジネスパートナーのサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握している

【実施の目安】

- ビジネスパートナーに求めるサイバーセキュリティ対策に関する要求事項を作成し、ビジネスパートナーに提示している。
- サイバーセキュリティ対策を実施することについて契約書に記載している。
- ビジネスパートナーのサイバーセキュリティ対策の状況を報告もしくは確認（監査）する方法について、ビジネスパートナーと合意している。

【実施の確認事項】

- ビジネスパートナーに求めるサイバーセキュリティ対策に関する要求事項に関する資料を確認し、ビジネスパートナーに提示されていることを確認する。
- ビジネスパートナーとの契約書に必要なサイバーセキュリティ対策を実施することが記載されていることを確認する。
- ビジネスパートナーにおけるサイバーセキュリティ対策状況を把握するための方法が契約書に記載されていることを確認する。

(6) 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

(6)-1 必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している

【実施の目安】

- サイバーセキュリティ対策の費用を経営会議や経営に関する委員会等で検討し、サイバーセキュリティ対策の計画に則った適切な費用であることを、経営者または権限を委譲された CISO 等が承認している。

【実施の確認事項】

- サイバーセキュリティ対策の費用の妥当性を確認し、承認したことを確認するためには、経営会議や経営に関する委員会等の議事内容にサイバーセキュリティ対策の費用に関する事項があることを確認する。

(6)-2 サイバーセキュリティ対策を実施できる人材を確保している（組織の内外問わず）

【実施の目安】

- サイバーセキュリティ対策の計画に記載している低減策などを実施するために必要となる人材を確保する。
- サイバーセキュリティ対策の計画に記載している低減策などを自組織の人材で実施できない場合、もしくは自組織の人材で行うことが見合わない場合には、外部の専門家への依頼やサービスを利用している。

【実施の確認事項】

- 計画しているサイバーセキュリティ対策の実施について自組織内の人材による対応の可否について検討した結果を確認する。
- 上記の検討結果を CISO 等が承認していることを確認する。
- 組織内に人員計画がある場合には、その計画にサイバーセキュリティ対策に関する要員についての計画が含まれることを確認する。

(6)-3 組織内でサイバーセキュリティ人材を育成している

【実施の目安】

- 組織内にサイバーセキュリティ分野を対象とする研修制度または外部の研修やセミナー等の奨励制度がある。
- 組織内でサイバーセキュリティ対策に関連した研修計画、人材育成計画、人員計画、人事制度についての検討を実施している。

【実施の確認事項】

- 組織内のサイバーセキュリティ分野を対象とする研修制度、セミナー等の奨励制度を確認する。
- 組織内に研修計画、人材育成計画がある場合には、それらの計画にサイバーセキュリティ対策に関する内容が含まれることを確認する。

(6)-4 組織内のサイバーセキュリティ人材のキャリアパスを構築し、適正な処遇をしている

【実施の目安】

- 自組織に合わせたサイバーセキュリティ人材のキャリアパスを作成し、人事評価制度とリンクさせている。
- セキュリティ関連業務を対象とした業績評価基準が定められ、人事評価制度ともリンクしている。

【実施の確認事項】

- サイバーセキュリティ人材のキャリアパスを示した文書と人事評価制度との関連を確認する。
- セキュリティ関連業務の業績評価の基準を示した文書と人事評価制度との関連を確認する。

(6)-5 セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施している

【実施の目安】

- セキュリティ担当者と従業員に対するサイバーセキュリティに関する研修計画があり、研修計画のとおりに研修が実施されている。

【実施の確認事項】

- 以下の研修に関する成熟度に応じたいずれかの内容と記録を確認する。
  - 定期的にサイバーセキュリティに関する研修を実施することを規定している（セキュリティポリシーや実施計画等）。
  - サイバーセキュリティに関する研修を実施し、実施記録を保管している。
  - 定期的なサイバーセキュリティに関する研修を複数回実施し、研修内容の改良、見直しを行っている。
  - 自社に想定される事例があった場合には、その事例やサイバーセキュリティ対策などの研修に盛り込んでいる。
  - 従業員だけでなく役員、派遣社員等をサイバーセキュリティに関する研修の対象としている。

(7) IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

(7)-1 IT システムの管理等について、自組織で対応できる部分と外部に委託する部分で適切な切り分けをしている

【実施の目安】

- 自組織で対応できる部分と外部に委託する部分の切り分けを明文化している。
- 上記の明文化した内容をもとに外部委託の内容が定められている。

【実施の確認事項】

- サイバーセキュリティリスクへの対応、具体的な対策のレベル、緊急時対応の項目に関する明文化内容と外部委託の契約書等を確認する（契約書の確認については、契約書に直接記載する場合と契約の特記事項など契約書にリンクされている場合があることから、包括的な確認を行う）。
- 契約書以外の文書（例えば、仕様書や品質保証文書等）の確認については、その内容と明文化した内容に相違がないことを確認する。

(7)-2 委託先へのサイバー攻撃を想定し、委託先のサイバーセキュリティを確保している

【実施の目安】

- 委託先に求めるサイバー攻撃への対策内容を明文化し、契約書等の文書を通じて要求している。
- 外部に委託する部分に対する緊急時対応の項目を明文化している。
- 上記の明文化した内容が外部委託の契約書に盛り込まれている。

【実施の確認事項】

- 委託先に要求するサイバーセキュリティリスクへの対策、具体的な対策のレベル、緊急時対応の項目に関して契約書等で規定している内容を確認する。
- 契約書の確認については、契約書に直接記載する場合と契約の特記事項など契約書にリンクされている場合があることから包括的な確認を行う。

(8) 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のための環境整備

(8)-1 各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有を行い、自社の対策に活かしている

【実施の目安】

- サイバーセキュリティに関する注意喚起情報等の情報源として有用な各種団体をリスト化している。
- 注意喚起情報等を情報収集する担当者を定めている。
- 注意喚起情報等の情報収集結果の社内での報告先を定め、定期報告する頻度を定めている。
- 情報共有を行うコミュニティの参加先と担当者を定めている。
- コミュニティで情報共有等を行った結果の社内での報告先を定めている。

【実施の確認事項】

- 注意喚起情報等の情報源となる各種団体のリストを確認する。
- 情報収集する担当者、情報収集結果の報告先、定期報告する頻度に関する実績が定められた内容と乖離していないかを確認する。
- 情報共有を行うコミュニティの参加先、担当者、報告先として定められた内容と、実際のコミュニティでの活動状況を確認する。

(8)-2 マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPA への届出や一般社団法人 JPCERT コーディネーションセンターへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している

【実施の目安】

- マルウェア情報や不正アクセス情報を得たり、インシデントが発生したりした場合の報告先を整理した上で、それぞれの報告内容及びフォーマットへの対応について準備している。

【実施の確認事項】

- 報告先ごとの報告内容及びフォーマットへの対応についての準備状況や報告実績を確認する。

(9) 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

(9)-1 組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Web サイト保守・運用、契約しているセキュリティベンダの連絡先含む）

【実施の目安】

- 緊急事態の発生を想定し、組織の内外における緊急連絡先と伝達ルートを明文化している。
- 緊急連絡先と伝達ルートごとの連絡担当を定め、これらの担当者の割当てについて CISO 等及び緊急時対応体制の責任者が承認している。
- 緊急連絡先と伝達ルートを定期的に見直す頻度を定めている。

【実施の確認事項】

- 緊急連絡先と伝達ルート及びその担当者を確認する。
- 緊急連絡先と伝達ルート及びその担当者についての承認状況を確認する。
- 緊急連絡先と伝達ルートに関する定期的な見直しの実施結果を確認する。

(9)-2 他の災害と同様に、サイバー攻撃の初動対応マニュアルを整備している

【実施の目安】

- 他の自然災害の対策マニュアル等を参考に、サイバー攻撃の初動対応マニュアルを整備する。
- 自組織で発生する可能性のあるサイバー攻撃について、攻撃がインシデントに至るまでのシナリオを想定する。
- JPCERT/CC 等のインシデント対応マニュアルの作成に関する資料等を参考に、以下を定める。
  - インシデント対応する担当者や部門
  - インシデント発生前に準備しておく内容
  - インシデント対応フロー
- 初動対応マニュアルの内容を CISO 等及び緊急時対応体制の責任者が承認している。
- 初動対応マニュアルを定期的に見直す頻度を定めている。

【実施の確認事項】

・ サイバー攻撃の初動対応マニュアルを確認する。
・ 自組織で発生する可能性のあるサイバー攻撃を想定したシナリオの内容を確認し、そのシナリオがサイバー攻撃の初動対応マニュアルに盛り込まれていることを確認する。
・ 初動対応マニュアルに「インシデント対応する担当者や部門」、「インシデント発生前に準備する内容」、「インシデント対応フロー」が盛り込まれていることを確認する。
・ サイバー攻撃の初動対応マニュアルの内容についての承認状況を確認する。
・ サイバー攻撃の初動対応マニュアルを定期的に見直す頻度及び見直しの実績について確認する。

(9)-3 インシデント対応の専門チーム（CSIRT 等）を設置している

【実施の目安】

・ サイバーインシデントに対応する専門のチーム（CSIRT 等）を構築する。
・ CSIRT などサイバーインシデントに対応する専門のチームを構築することが困難な場合には、サイバーインシデントに対応するチーム（専門ではなく、他業務との兼任のチームやバーチャルなチーム）を構築し、サイバーインシデントに対応する機能を組織内に保持する。
・ JPCERT/CC 等のインシデント対応マニュアルの作成に関する資料等を参考に、サイバーインシデントに対応するチームについて以下を定める。
  ➢ サイバーインシデントに対応するチームの役割と範囲
  ➢ サイバーインシデントに対応するチームの形態
  ➢ サイバーインシデントに対応するチームの要員
  ➢ サイバーインシデントに対応するチームの活動内容
・ サイバーインシデントに対応するチームを組織内に周知し、必要に応じて組織外にも周知する。
・ サイバーインシデントに対応するチームの責任者を定め、サイバーインシデントに対応するチームの運営に関するルールやマニュアル等のドキュメントの内容を CISO 等が承認している。
・ サイバーインシデントに対応するチームに関するドキュメントを定期的に見直す期間を定めている。
・ 必要に応じて、被害の原因究明や被害状況の把握を行うための外部の専門家（コンピュータフォレンジックス等）へ依頼する体制となっている。

【実施の確認事項】

・ サイバーインシデントに対応するチームの運営に関するルールやマニュアル等のド

キュメントを確認する。
- サイバーインシデントに対応するチームに関するツールやマニュアル等に「チームの役割と範囲」、「チームの形態」、「チームの要員」、「チームの活動内容」が盛り込まれていることを確認する。
- サイバーインシデントに対応するチームの責任者及びサイバーインシデントに対応するチームに関するドキュメント内容の承認を確認する。
- サイバーインシデントに対応するチームに関するドキュメントを定期的に見直す期間及び見直した結果を確認する。
- 被害の原因究明や被害状況の把握を行うために外部の専門家に依頼する場合には、その依頼方法や依頼するために必要となる内容等を確認した結果を確認する。

(9)-4 インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている

【実施の目安】
- サイバーインシデントに関する対応訓練や演習を定期的に実施する。
- サイバーインシデントに関する対応訓練や演習を定期的に実施する期間を定めている。
- 自組織で発生する可能性のあるサイバーインシデントを想定したシナリオの内容を確認し、そのシナリオに対応した対応訓練や演習を実施する。
- サイバーインシデントに関する対応訓練や演習では、インシデント収束後の再発防止策の検討も行い、再発防止策の策定や見直しが行われている。

【実施の確認事項】
- サイバーインシデントに関する対応訓練や演習の実施を確認する。
- 自組織で発生する可能性のあるサイバーインシデントを想定したシナリオの内容を確認し、そのシナリオが対応訓練や演習に盛り込まれていることを確認する。
- サイバーインシデントに関する対応訓練や演習では、サイバーインシデントに対応するチーム内で実施するもの、自組織内の複数の部門で実施するもの、経営者も含めて実施するものいずれかを含む。
- サイバーインシデントに関する対応訓練や演習を定期的に実施する期間を確認する。
- サイバーインシデントに関する対応訓練や演習の結果をもとにインシデント収束後の再発防止策の検討を行ったこと、及び再発防止策の策定や見直した結果を確認する。

(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

(10)-1 組織外の報告先（ステークホルダーや所管官庁等を含む）をリスト化している

【実施の目安】

- 被害発覚後の対策を想定し、組織外の報告先をリスト化している。
- 組織外の報告先のリスト化は、自組織で発生する可能性のある被害発生を想定したシナリオの内容を検討し、そのシナリオに基づいた報告先が盛り込まれている。
- 組織外の報告先のリスト作成責任者を定め、リストの内容を緊急時対応体制の責任者が承認している。
- 組織外の報告先のリストを定期的に見直す期間を定めている。
- 犯罪に絡むインシデントに備え、管轄する警察署がリストに含まれている。

【実施の確認事項】

- 組織外の報告先のリストを確認する。
- 自組織で発生する可能性のある被害発生を想定したシナリオの内容を確認し、そのシナリオに基づいた報告先が盛り込まれていることを確認する。
- 組織外の報告先のリストの作成責任者及びリスト内容の承認を確認する。
- 組織外の報告先のリストを定期的に見直す期間及び見直した結果を確認する。

(10)-2 開示・報告すべき情報を把握・整備している

【実施の目安】

- 被害発覚後に開示・報告すべき情報については、報告フォーマットを定めている。
- 必要に応じて、被害の原因究明や被害状況の把握を行うために外部の専門家に依頼する場合には、依頼した結果、どのような内容が報告されるのかを確認する。
- 被害発覚後の検討には、自組織で発生する可能性のある被害発生を想定したシナリオの内容を検討し、そのシナリオに基づいて、報告フォーマットと報告・収集ルートが盛り込まれている。
- 報告フォーマットと報告・収集ルートの作成責任者を定め、その内容を緊急時対応体制の責任者が承認している。
- 報告フォーマットと報告・収集ルートを定期的に見直す期間を定めている。

【実施の確認事項】

- 報告フォーマットを確認する。

・　被害の原因究明や被害状況の把握を行うために外部の専門家に依頼する場合には、どのような内容が報告されるのかを確認した結果を確認する。
・　自組織で発生する可能性のある被害発生を想定したシナリオの内容を確認し、そのシナリオに基づいた報告内容が報告フォーマットに盛り込まれていることを確認する。
・　報告フォーマットの作成責任者及びその内容の承認を確認する。
・　報告フォーマットを定期的に見直す期間及び見直した結果を確認する。

(10)-3 経営者が、責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等について事前に検討している

【実施の目安】
・　被害発覚後に開示・報告すべき情報を把握するための自組織内の報告ルートや報告ルールを明文化する。
・　被害発覚後に経営者が、責任を持って組織の内外に説明、公表できる内容やタイミング等を検討する。
・　被害発覚後の検討には、自組織で発生する可能性のある被害発生を想定したシナリオの内容を検討し、そのシナリオに基づいて、公表できる内容やタイミングを明文化する。
・　報告ルートや報告ルールの作成責任者を定め、その内容を緊急時対応体制の責任者が承認している。
・　報告ルートや報告ルールを定期的に見直す期間を定めている。

【実施の確認事項】
・　報告ルートや報告ルールを明文化した内容を確認する。
・　経営者が、責任を持って組織の内外に説明、公表できる内容やタイミング等を検討した結果を確認する。
・　自組織で発生する可能性のある被害発生を想定したシナリオの内容を確認し、そのシナリオに基づいた報告ルートや報告ルールが盛り込まれていることを確認する。
・　報告ルートや報告ルールの作成責任者及びその内容の承認を確認する。
・　報告ルートや報告ルールを定期的に見直す期間及び見直した結果を確認する。