

サイバーセキュリティ経営ガイドラインVer 2.0  
実践のためのプラクティス集



独立行政法人 情報処理推進機構



経済産業省と独立行政法人情報処理推進機構(IPA)は、2017年11月にサイバーセキュリティ経営ガイドラインVer 2.0を発行しました。Ver 2.0では、米国のサイバーセキュリティフレームワークとの整合を意識し、攻撃検知対策やインシデント対応など、深刻化するサイバー攻撃への対応強化を狙った改訂が行われております。

本ガイドラインは企業の皆様に一定の認知をいただき、実践が進められてきましたが、上記の改訂にあわせ、サイバー攻撃への備えをさらに強化していただくため、国内で実際に行われている事例を基にしたプラクティス集を作成いたしました。

本プラクティス集は、「情報セキュリティの取組みはある程度進めてきたが、サイバー攻撃対策やインシデント対応は強化が必要。それに向けた体制づくりや対策は、何から始めるべきか」と考えている経営者、CISO等、セキュリティ担当者を想定読者とし、ガイドラインの重要10項目を実践する際に参考となる考え方やヒント、実施手順、実践事例が記載されております。経営者の方は第1章が、CISO等およびセキュリティ担当者の方は本プラクティス集全体が参考となるように構成いたしました。2章では重要10項目についてサイバーセキュリティ強化のために実践していただきたい事例、3章は実践の妨げとなる課題に対し、実際に試みられた工夫の事例を紹介しております。付録にはサイバーセキュリティに関する用語集や、対策の参考情報を記載しております。

本プラクティス集は小冊子であり、事例は必ずしも網羅的ではありません。読者の皆様のご意見をいただきながら、事例の拡充、改訂を進めていきたいと考えております。

目次		頁
はじめに	背景と目的	P.4
	想定読者と利用方法	P.5
	本プラクティス集の構成	P.6
	本プラクティス集のより良い実践のために	P.7
	本プラクティス集に関連する資料	P.8
第1章	経営とサイバーセキュリティ	
	1.サイバー攻撃による企業活動への影響	P.10
	2.なぜサイバーセキュリティ対策は経営課題か	P.11
	3.経営者が認識すべき3原則と指示すべき重要10項目	P.12
第2章	サイバーセキュリティ経営ガイドライン実践のプラクティス	
	指示1.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	P.14
	指示2.サイバーセキュリティリスク管理体制の構築	P.17
	指示3.サイバーセキュリティ対策のための資源（予算、人材等）確保	P.19
	指示4.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	P.22
	指示5.サイバーセキュリティリスクに対応するための仕組みの構築	P.23
	指示6.サイバーセキュリティ対策におけるPDCAサイクルの実施	P.28
	指示7.インシデント発生時の緊急対応体制の整備	P.29
	指示8.インシデントによる被害に備えた復旧体制の整備	P.33
	指示9.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	P.36
指示10.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	P.39	
第3章	セキュリティ担当者の悩みと取組みのプラクティス	
	1.インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	P.41
	2.インシデント対応の初動における情報共有に不安がある	P.43
	3.インシデントが起きた際のリスクヘッジが十分ではない	P.45
	4.IoT機器が「シャドーIT」化している	P.47
	5.自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる	P.59
	6.全国各地の拠点におけるセキュリティ管理状況に不安がある	P.51
	7.外部サービスの選定でIT部門だけでは対応が困難である	P.53
	8. IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている	P.55
	9.従業員に対してセキュリティ教育を実施しているが効果が感じられない	P.57
10.スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	P.59	
付録	サイバーセキュリティに関する用語集	P.62
	サイバーセキュリティ対策の参考情報	P.68

## はじめに 背景と目的

### 背景

経済産業省と独立行政法人情報処理推進機構（以下「IPA」という）は、2015年に共同でサイバーセキュリティ経営ガイドラインを発行し、2017年に改訂版（Ver 2.0）を発行した（以下「経営ガイドライン」という）。経営ガイドラインの認知度は向上しているものの、企業がこのガイドラインにある内容を実践する上では、**より具体的な手引き等を求める意見**が聞かれている。

また、経済産業省のコーポレート・ガバナンス・システム研究会は「グループ・ガバナンス・システムに関する実務指針」（仮）を作成している。当該指針のサイバーセキュリティ対策の在り方において、経営ガイドラインを参照する等、コーポレート・ガバナンス、またグループ・ガバナンスにおいて、**経営層によるサイバーセキュリティ対策の推進**が一層求められている。

### 目的

上述の背景をうけ、企業が経営ガイドラインの内容を実践する際の、**事例に基づく実施手順や取組みの例、取組む際の考え方、ヒントなどを提供することが、本プラクティス集の目的**である。

特に、本プラクティス集で紹介するプラクティスは、情報セキュリティの取組みはある程度進めてきたが、サイバーセキュリティ対策やインシデント対応について何から始めるべきかと考えている読者に向けて、ファーストステップとなり得る事項を提示するものである。

## はじめに 想定読者と利用方法

本プラクティス集は、サイバーセキュリティ対策を検討している企業の下記の方々を想定読者とする。

- サイバーセキュリティに向けてリスクマネジメントを強化したい経営者
- サイバーセキュリティ対策を実施する上での責任者となる担当幹部（以下、CISO等）
- サイバーセキュリティ対策の担当者、CSIRTのメンバー等（以下、セキュリティ担当者）
- 上記人材の育成や支援を担当する社内部門や社外の事業者  
（以下、人材育成・支援担当者）

また、以下のタイミングや場面において利用されることを想定する。

No	利用するタイミング	具体的な利用場面
1	新たにサイバーセキュリティ部門を設置・所管することになった場合や、CISO等に着任した場合など	どこからサイバーセキュリティの取組みに着手してよいかわからない際に、はじめの一步として実践事例や参考情報を活用する
2	経営環境の変化（デジタルトランスフォーメーションへの取組み着手など）により、サイバーセキュリティ対策の重要性が増し、対策を検討する場合など	経営ガイドラインに紐づく実践事例を参考に、サイバーセキュリティ対策の検討に役立てる
3	インシデントが発生し、サイバーセキュリティ対策を強化しなければならない場合など	取組みや工夫の例を参考にインシデントの再発防止に向けた対策の実施に役立てる
4	セキュリティ担当者へ教育を実施する場合や、外部の事業者としてサイバーセキュリティ対策を支援する場合など	人材育成の担当者が教材として活用する、また企業のサイバーセキュリティ対策支援に役立てる

## はじめに 本プラクティス集の構成

本プラクティス集は、紹介する取組み事例が様々な形態で利用されることを想定し、以下の観点で構成している。

第2章：ガイドラインの**指示項目毎**の企業の実践事例

第3章：セキュリティ担当者の**悩み毎**の企業の実践事例

各章の内容は以下の通りである。

### 第1章：経営とサイバーセキュリティ

経営者やCISO等に向けて、国内のサイバー攻撃の被害事例やサイバー攻撃の特徴を踏まえ、サイバーセキュリティが与える企業への影響や経営課題としての重要性をまとめる。

### 第2章：サイバーセキュリティ経営ガイドライン実践のプラクティス

サイバーセキュリティ対策を実施するCISO等やセキュリティ担当者、人材育成・支援担当者に向けて、事例に基づく重要10項目の実践手順、実践内容、取組む際の考え方、ヒントをプラクティスとして示す。

### 第3章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

サイバーセキュリティ対策を実施するセキュリティ担当者や人材育成・支援担当者が、対策を推進する上で経験した悩みとそれを解決するために取組んだ際の実践手順、内容、取組む際の考え方、得られた知見をプラクティスとして示す。

### 付録

サイバーセキュリティ対策を実践するCISO等やセキュリティ担当者、人材育成・支援担当者が実務で活用できるサイバーセキュリティに関する用語集、参考資料集を示す。

## はじめに 本プラクティス集のより良い実践のために

本プラクティス集では、企業へのアンケートおよびインタビューを通じて収集した、実際に行われている施策に基づいて、プラクティスを紹介する。その中心は、経営ガイドラインに記載の重要10項目のうち、改訂時の変更ポイントとなった項目である。プラクティスとして取り上げなかった項目についても、今後記載を拡充予定である。

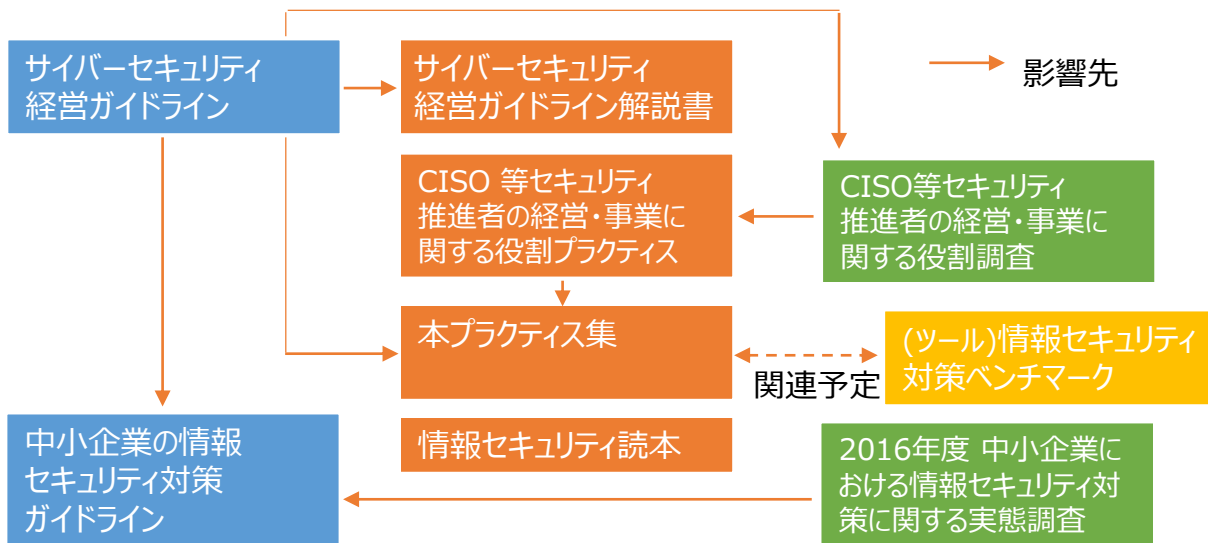
本プラクティス集で紹介する、プラクティスの基となった企業で実際に行われている施策は、それぞれの企業でのサイバーセキュリティに対する考え方や保有する人的および財務的リソース、企業風土や過去の経緯を踏まえて成立しているものである。

したがって、本プラクティス集で紹介するプラクティスを読者が自社において実践する際には、そのまま実践するだけでなく各社のこれまでの施策等を踏まえ、適用可否や実践手順を柔軟に検討いただければ幸いである。また自社の現状に応じて実践内容を適切に変更することで、より高い効果が上がることも期待できる。



# はじめに

## 本プラクティス集に関連する資料



資料名	発行年月日	対象読者	内容	URL
サイバーセキュリティ経営ガイドライン Ver 2.0	2017/11/16	経営者、CISO等、セキュリティ担当者	経営者のリーダーシップの下、サイバーセキュリティ対策を推進するためのガイドライン	<a href="http://www.meti.go.jp/policy/netsecurity/mn_g_guide.html">http://www.meti.go.jp/policy/netsecurity/mn_g_guide.html</a>
中小企業の情報セキュリティ対策ガイドライン第3版	2019/3/19	経営者、情報管理を統括する方	重要な情報を脅威から保護するための情報セキュリティ対策ガイドライン	<a href="https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html">https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html</a>
サイバーセキュリティ経営ガイドライン解説書	2016/12/8	経営者、CISO等、セキュリティ担当者	経営ガイドライン(※Ver1.1)の内容を補足し、実施方法を具体的に解説	<a href="https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html">https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html</a>
CISO等セキュリティ推進者の経営・事業に関する役割プラクティス	2018/6/28	CISO等、セキュリティ担当者	CISO等セキュリティ推進者の経営・事業に関する役割の目的・狙い、作業内容、作業プロセス、目標成果等	<a href="https://www.ipa.go.jp/files/000067656.pdf">https://www.ipa.go.jp/files/000067656.pdf</a>
情報セキュリティ読本 五訂版	2018/10/20	一般ユーザ、経営者、組織の運営に携わる方々	情報セキュリティの基本を分かりやすく説明	<a href="https://www.ipa.go.jp/security/publications/dokuhon/index.html">https://www.ipa.go.jp/security/publications/dokuhon/index.html</a>
2016年度中小企業における情報セキュリティ対策に関する実態調査	2017/3/30	セキュリティ担当者	情報セキュリティ被害やセキュリティ対策実践により経営に効果を発揮した事例等の実態調査	<a href="https://www.ipa.go.jp/security/fy28/reports/sme/">https://www.ipa.go.jp/security/fy28/reports/sme/</a>
CISO等セキュリティ推進者の経営・事業に関する役割調査	2018/3/28	CISO等、セキュリティ担当者	セキュリティへの取組みが経営と事業に貢献するようマネジメントする役割の実態調査	<a href="https://www.ipa.go.jp/security/fy29/reports/ciso/index.html">https://www.ipa.go.jp/security/fy29/reports/ciso/index.html</a>
(ツール)情報セキュリティ対策ベンチマーク4.7	2018/10/26	セキュリティ担当者	セキュリティ対策自己診断システム	<a href="https://www.ipa.go.jp/security/benchmark/">https://www.ipa.go.jp/security/benchmark/</a>

はじめに

第1章

第2章

第3章

付録



## 第1章 経営とサイバーセキュリティ

経営者やCISO等に向けて、サイバー攻撃の被害事例や特徴を踏まえて、経営課題としてのサイバーセキュリティ対策の重要性を示す。

# 1

## サイバー攻撃による企業活動への影響

### サイバー攻撃の傾向と企業への影響

サイバー攻撃は、金銭の詐取等の直接的な被害だけでなく、インシデントにより株価・純利益が下落・減少するといった間接的な被害も与えている。

サイバー攻撃による金銭の詐取等、直接的な被害を受けた件数が増加<sup>1</sup>

インシデントによる  
株価・純利益への影響<sup>2</sup>

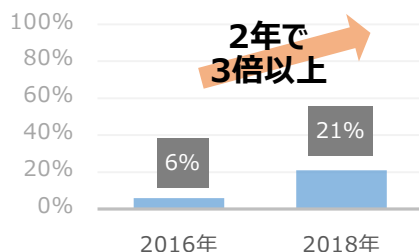


図1-1.1 日本企業が被害に遭った経済犯罪の内、サイバー攻撃の割合の推移

日本国内でインシデントに関する適時開示を行った企業では、

- **株価は平均10%下落**
- **純利益は平均21%減少**

### 多様化し破壊力を増すサイバー攻撃

サイバー攻撃の手法は多様化し、**情報漏えいだけでなく、業務停止**をも引き起こしている。

事例①：ランサムウェア感染による自動車工場の操業停止

大手自動車メーカーの工場設備に付帯するPCがランサムウェアに感染し、約1日操業を停止した。これにより、自動車約1000台の生産が停止した。

事例②：マルウェア感染によるポイントサービスの停止

小売チェーン店の委託先において、システムのサーバがマルウェアに感染し、約1週間に渡ってポイントサービスが利用できなくなった。

### サイバー攻撃の標的はサプライチェーン全体へ

企業を攻撃するための侵入口として、サイバーセキュリティ対策が進んでいない系列企業やビジネスパートナーを標的とするサイバー攻撃も見られる。サプライチェーン全体で脆弱点をなくすように、サイバーセキュリティ対策を推進する必要がある。

はじめに

経営とサイバーセキュリティ

第1章

第2章

第3章

付録

1 PwC「経済犯罪実態調査2018 日本分析版」

<https://www.pwc.com/jp/ja/knowledge/thoughtleadership/economic-crime-survey.html>

2 一般社団法人日本サイバーセキュリティ・イノベーション委員会 (JCIC) 「取締役会で議論するためのサイバーリスクの数値化モデル」  
[https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919\(JP\).pdf](https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf)

## 2

## なぜサイバーセキュリティ対策は経営課題か

昨今のサイバー攻撃の特徴として、下記5点が挙げられる。これらの特徴を考慮すると、サイバー攻撃による企業活動への影響を最小化するには、**IT部門だけでなく事業部門等も交え対策を推進することが必要となる**。そのため、**経営者のリーダーシップの下、サイバーセキュリティ対策を経営課題と位置づけて推進することが重要である**。

**①情報漏えいのみならず、業務停止を招くおそれがある**

- ・ 経営環境の変化(デジタルトランスフォーメーションへの取組み着手など)により、ITが事業基盤となっている企業においては、サイバー攻撃が大規模な業務停止を招くこともある。
- ・ サイバーセキュリティリスクは、『事業の停止』、『重要情報の改ざん』、『重要情報の漏えい』、『金銭の詐取』に及び、インシデント発生時の企業活動への影響が甚大である。

**②サイバー攻撃を完全に防ぐことは難しい**

- ・ 攻撃手法は複雑かつ常に変化し続けており、検知しにくい。
- ・ 巧妙な攻撃者は対象の情報を入手して優位な立場から攻撃をしかけるため、これを防ぐことは難しい。

**③どの企業もサイバー攻撃を受ける可能性がある**

- ・ インターネットへの接続がないとされていた工場等のシステムでも、間接的に又は意図せずにインターネットに接続されていた事例がある。
- ・ インターネットへの接続がない場合も、可搬記憶媒体等を介しマルウェアに感染する。
- ・ サプライチェーン上でセキュリティ対策が弱い系列企業やビジネスパートナーが攻撃されることがある。

**④被害の拡大範囲は自社にとどまらない**

- ・ マルウェア等に感染すると、ネットワークを介して被害が拡大する。
- ・ 業務停止等の被害の拡大は自社だけでなく、取引先や関係会社に及ぶ。

**⑤時間との戦いである**

- ・ 攻撃の兆候を察知してから対策を実施するまでに時間がかかると被害が拡大する。事業影響を極小化するために、経営者のリーダーシップの下、速やかな対応が求められる。

# 3

## 経営者が認識すべき3原則と 指示すべき重要10項目

経営ガイドラインでは、大企業及び中小企業(小規模事業者を除く)の経営者を対象として、サイバー攻撃から企業を守る観点で経営者が認識すべき「3原則」と、CISO等に対し指示すべきサイバーセキュリティ経営の「重要10項目」がまとめられている。

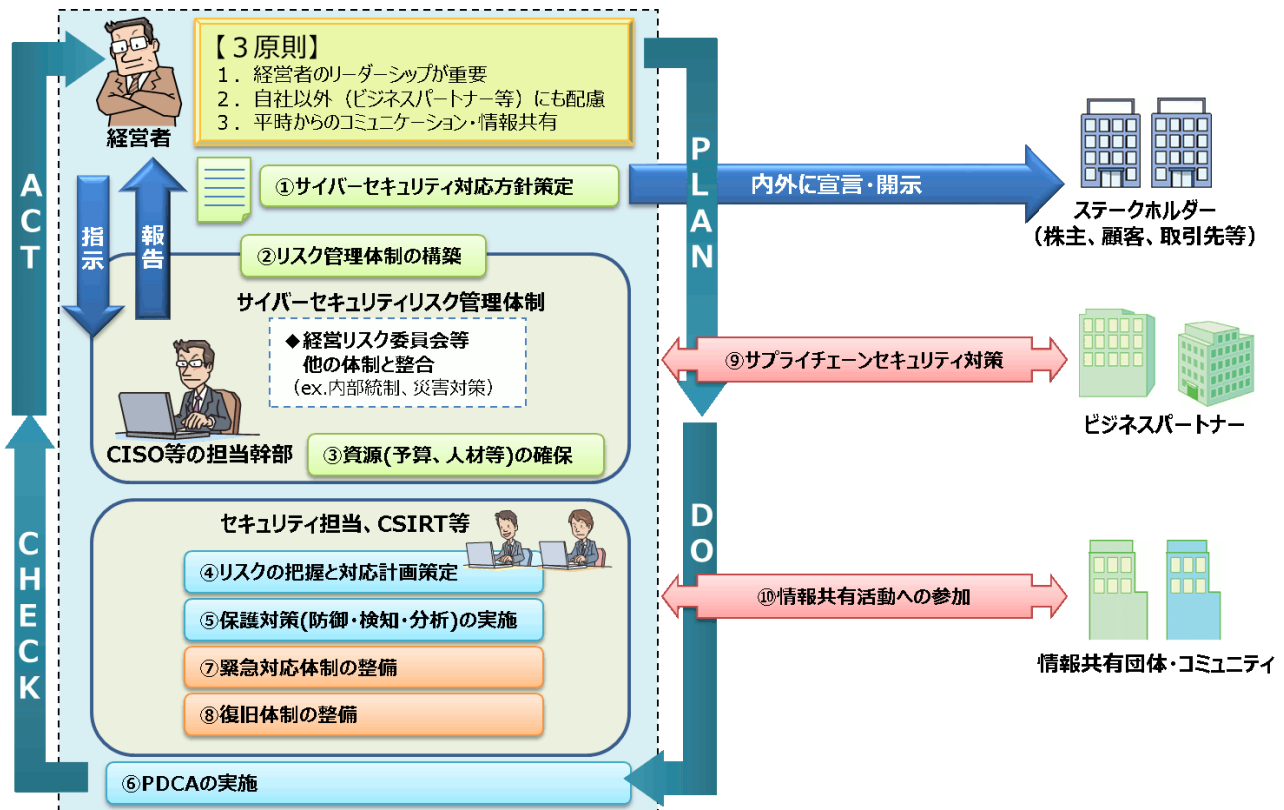


図1-3.1 経営者が認識する必要がある「3原則」および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」<sup>3</sup>

はじめに

経営とサイバーセキュリティ 第1章

第2章

第3章

付録

3 経済産業省「サイバーセキュリティ経営ガイドラインの概要」  
[http://www.meti.go.jp/policy/netsecurity/mng\\_guide.html](http://www.meti.go.jp/policy/netsecurity/mng_guide.html)

## 第2章 サイバーセキュリティ経営ガイドライン 実践のプラクティス

サイバーセキュリティ対策をこれから実践するCISO等やセキュリティ担当者に向けて、**企業での事例をベースとした重要10項目の実践手順、実践内容、取組む際の考え方、ヒント**を実践のプラクティスとして示す。

サイバーセキュリティ経営の重要10項目		実践のプラクティス
1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	1-1.経営者がサイバーセキュリティリスクを認識するための、他社被害事例の報告 1-2.セキュリティポリシーの改訂・共同管理
2	サイバーセキュリティリスク管理体制の構築	2-1.サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
3	サイバーセキュリティ対策のための資源（予算、人材等）確保	3-1.サイバーセキュリティ対策のための、予算の確保 3-2.サイバーセキュリティ対策のための、必要なサイバーセキュリティ人材の定義・育成
4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	(参考資料の提示)
5	サイバーセキュリティリスクに対応するための仕組み構築	5-1.多層防御の実施 5-2.アクセスログの取得
6	サイバーセキュリティ対策におけるPDCAサイクルの実施	(参考資料の提示)
7	インシデント発生時の緊急対応体制の整備	7-1.旗振り役としてのCSIRTの設置 7-2.従業員の初動対応の定義
8	インシデントによる被害に備えた復旧体制の整備	8-1.インシデント対応時の危機対策本部との連携 8-2.組織内外の連絡先の定期メンテナンス
9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	9-1.サイバーセキュリティリスクのある委託先の特定と対策状況の確認
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	(参考資料の提示)

## 指示 1

# サイバーセキュリティリスクの認識、 組織全体での対応方針の策定

### 指示内容

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

はじめに

第1章

ガイドライン実践のプラクティス  
第2章

第3章

付録

## 実践に向けたファーストステップ

経営リスクを認識して、組織全体としての対応方針を策定・宣言する主体は経営者である。そのため、実践する上でのファーストステップとして下記2点が考えられる。

- 経営層向けにサイバーセキュリティリスクに関する報告を増やす
- 既存のセキュリティポリシーの内容を確認し、サイバーセキュリティの観点から必要な改訂をする

## 想定される企業の状況

指示1の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- サイバーセキュリティリスクが自社にどのような影響を及ぼすか明らかになっていないため、経営者がサイバーセキュリティリスクを十分には認識していない
- 情報（顧客情報や営業秘密）保護の観点からセキュリティポリシーを定めている<sup>4</sup>が、サイバーセキュリティリスクは考慮されていない

4 情報セキュリティポリシーの策定方法は中小企業の情報セキュリティ対策ガイドライン(IPA)も参考にできる。  
<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

# プラクティス 1-1

## 経営者がサイバーセキュリティリスクを認識 するための、他社被害事例の報告

従業員数1,000名規模の小売業であるA社では、全社的なリスクや課題を報告する場である経営会議にセキュリティ施策を付議するも、一部の役員からはネガティブな反応があった。情報システム部の部長は経営層のサイバーセキュリティリスク、例えば『事業の停止』や『金銭の詐取』といったリスクの認識が十分でないと感じていた。

そのため、経営会議で、通常報告する「自社に対するサイバー攻撃の状況」や「対策の実施状況」に加え、「他社のサイバー被害事例」を報告することを考えた。また、トピック追加後も経営者への報告は同じフォーマットで続けることとした。

### A社の実践のステップ

情報システム部長が実践したステップは下記3点である。

- ① サイバー攻撃事例等を紹介するWebサイト<sup>5</sup>から他社の業務停止事例等を収集する
- ② 同様の被害が自社で発生する可能性を分析し、追加対策の要否を検討する
- ③ 上記の収集・分析・検討結果をCISO等が経営者の参加する経営委員会で定期報告する

### A社の実践内容

上記ステップに則り、情報システム部長が収集した事例と自社の追加対策要否をCISO等に説明し、CISOから経営会議に定期報告するプロセスとした。  
(関連するサイバーセキュリティ対策の予算確保については“プラクティス3-1”を参照)

経営会議 報告資料
<b>サイバーセキュリティリスクに関する報告</b>
1. 当社に対するサイバー攻撃の状況
2. サイバーセキュリティ対策の実施状況
<b>3. 他社のサイバー攻撃被害の発生状況</b>
4. その他 サイバー攻撃のトレンド

図2-1.1 経営委員会への報告内容の目次例

表2-1.1 他社のサイバー攻撃被害の発生状況の報告例

発生企業	国内小売業	国内製造業
被害内容	一時的に通販サイトが利用できない状態。翌日サービス再開。	製品生産を担う取引先が自己増殖型ランサムウェアに感染。供給が月単位で滞った。
原因	DDoS攻撃	取引先のランサムウェア感染
自社での発生可能性	発生確率：低	発生確率：高
必要な追加対策	追加対策不要。運営を委託する 自社WebサイトへのDDoS対策は実施済で、	ネットワーク分離が必要。OA環境と倉庫は同一ネットワーク上にあるため、感染時の被害拡大が懸念される。

<sup>5</sup> 他社のサイバー攻撃被害事例の収集元としては、下記のサイトが挙げられる  
サイバー情報共有イニシアティブ(J-CSIP) Webサイト <https://www.ipa.go.jp/security/J-CSIP/index.html>



# プラクティス 1-2 サイバーセキュリティリスクに対応するための、セキュリティポリシーの改訂・共同管理

従業員数600名規模の製造業であるB社では、総務部が情報保護の観点からセキュリティポリシーを定めているが、サイバーセキュリティ対策を推進する情報システム部の部長は既存のセキュリティポリシーがサイバーセキュリティリスクに対応しておらず、改訂の必要性を感じていた。

そのため、年に1回の全社的な規程類の改訂タイミングに合わせ、既存のセキュリティポリシーの改訂ポイントを洗い出し、所管する総務部と改訂に向けて連携するとともに、改訂後のセキュリティポリシーを総務部と情報システム部で共同管理することとした。

## B社の実践のステップ

情報システム部長が実践したステップは下記の2点である。

- ① 既存のセキュリティポリシーにサイバーセキュリティの観点で新規追加する内容を整理する
- ② 総務部と協力の上、既存のセキュリティポリシーを改訂する

## B社の実践内容

上記のステップに則り、情報システム部長は自社のセキュリティポリシーへサイバーセキュリティリスク対応を追加した。また、規程類の管理を共同で実施することを契機に、情報システム部と総務部が従業員向け教育へサイバーセキュリティの観点を追加するため、共同検討を始めた。

表2-1.2 B社における既存のセキュリティポリシーの主な改訂ポイント

改訂の観点	改訂(新規追加)した内容
想定する代表的なリスク	外部攻撃によるシステム停止や誤作動
リスク管理プロセス	(既存のリスク管理プロセスに則る)
リスク管理体制	平時、有事における体制と役割を定義
技術的な対策	重要なシステムに対する多層防御を定義
従業員への要求事項	標的型メール等への対応方法とインシデントや予兆の速やかな報告を規定

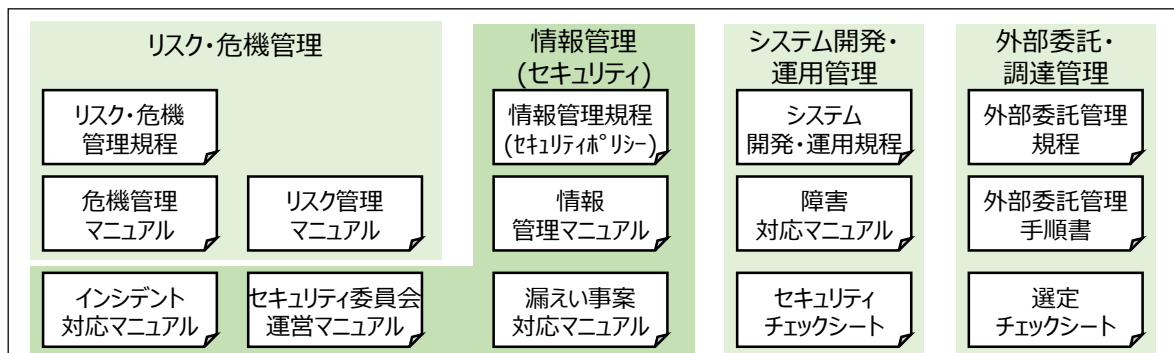


図2-1.2 B社の規程体系図の参考イメージ

## 指示 2

# サイバーセキュリティリスク管理体制の構築

### 指示内容

サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。

その際、組織内のその他のリスク管理体制とも整合を取らせる。

### 実践に向けたファーストステップ

サイバーセキュリティリスクが経営リスクであるとの認識の下、組織としてサイバーセキュリティリスクを把握し、対策を推進するための体制を構築することが望まれる。

実践する上でのファーストステップとしては、下記2点が考えられる。

- 組織内のリスク管理体制の役割、責任、範囲、人数規模など既存の状況を確認する
- サイバーセキュリティリスクの管理に足りてない役割を特定し、役割および責任の範囲を  
取り決める

### 想定される企業の状況

指示2の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- サイバーセキュリティ対策を計画・実施する情報システム部門の人材も不足しており、  
専任のセキュリティ部門を作ることができない

# プラクティス 2-1 サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築

従業員数1,200名規模の流通業であるC社では、情報保護の観点からコンプライアンス部がセキュリティリスクを管理しているが、情報システムに対する技術的な実装が多いサイバーセキュリティ対策は、暗黙のうちにIT統括部が担当している。

IT統括部のみでサイバーセキュリティ対策全般を推進することは困難であると考えたIT統括部長は、コンプライアンス部長、またコンプライアンス担当役員でもあるCISOと相談の上、サイバーセキュリティ対策を推進するための組織横断型の委員会を立ち上げた。また、委員会には自社業務の統括部門だけでなく、子会社のコンプライアンスを担当する執行役員を招集し、組織全体のサイバーセキュリティリスクを管理することとした。

## C社の実践のステップ

IT統括部長が実践したステップは下記3点である。

- ① グループ子会社含め、組織のサイバーセキュリティに関係する部門・担当者を選定する
- ② 委員会の役割や招集した部門・担当者の責任範囲を合意する
- ③ 委員会の運営を通じてサイバーセキュリティリスク管理、サイバーセキュリティ対策実施を推進する

## C社の実践内容

上記のステップに則り、C社はサイバーセキュリティ委員会を立ち上げ、公開資料<sup>6</sup>を参考に自社で具備すべき役割を定義した。(役割に応じた人材育成は“プラクティス3-2”参照)

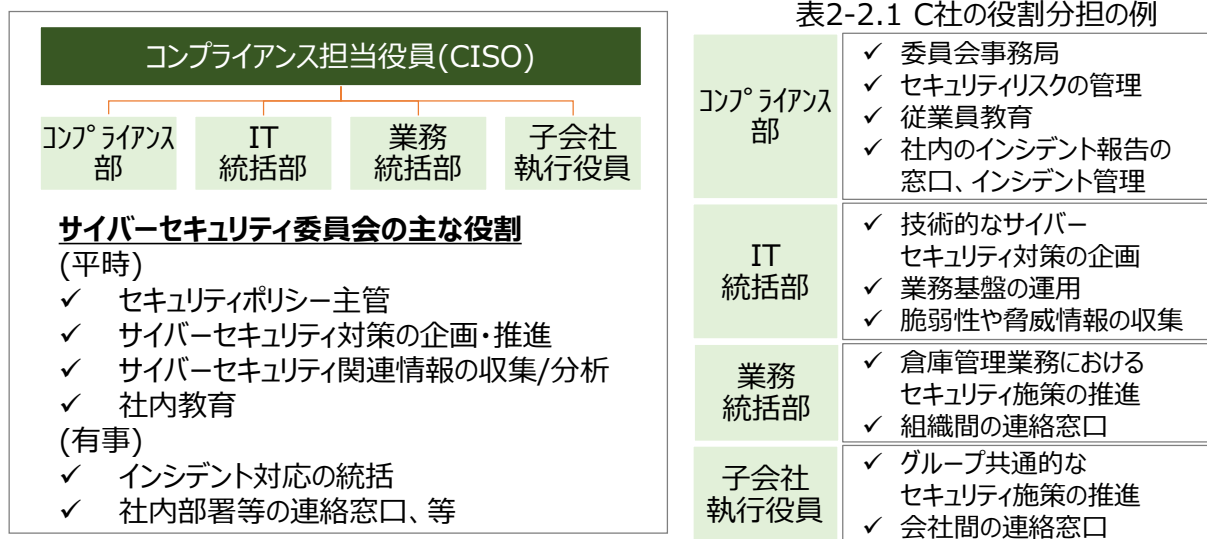


図2-2.1 C社のサイバーセキュリティ委員会イメージ

はじめに

第1章

ガイドライン実践のプラクティス 第2章

第3章

付録

6 サイバーセキュリティリスク管理体制の構築に向けては、セキュリティ対応組織(SOC/CSIRT)の教科書(日本セキュリティオペレーション事業者協議会 ISOG-J)も参考にできる。

[https://isog-j.org/output/2017/Textbook\\_soc-csirt\\_v2.html](https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html)

## 指示 3

# サイバーセキュリティ対策のための資源 (予算、人材等) 確保

### 指示内容

サイバーセキュリティリスクへの対策を実施するための予算確保と  
サイバーセキュリティ人材の育成を実施させる。

## 実践に向けたファーストステップ

予算確保の観点では、これまで重点化していなかったサイバーセキュリティ対策のための予算を確保することが望まれる。サイバーセキュリティにおいては、攻撃手法は常に変化し続けているため、継続的な予算の確保が必要である。

人材確保の観点では、自社でサイバーセキュリティ人材を雇用する場合は、役割に応じたセキュリティ教育を継続的に実施する等の育成活動を行うこと、自社でサイバーセキュリティ人材を雇用することが困難な場合は、外部の専門ベンダの活用を検討することが望まれる。

実践する上でのファーストステップとしては、予算確保とサイバーセキュリティ人材の確保それぞれの観点で、下記が考えられる。

- 予算の確保に向けては、必要なサイバーセキュリティ対策を明確にし、経営者に報告の上、対策実施の承認を得る
- 人材等の確保に向けては、専門ベンダの活用も考慮し、自社が最低限確保すべきサイバーセキュリティ人材を定義する

## 想定される企業の状況

指示3の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- サイバーセキュリティ対策の予算を確保したいが、セキュリティ対策は一般的に費用対効果(ROI)が不透明なため、経営者から理解が得られにくい
- システムの開発・運用は外部委託しており、サイバーセキュリティに求められる必要な知識や経験を有する人材を自社で確保する必要が分からない

# プラクティス 3-1

## サイバーセキュリティ対策のための、 予算の確保

プラクティス1-1に記載した従業員数1,000名規模の小売業であるA社では、経営会議での報告事項に「他社のサイバー被害事例」を追加し、自社での発生可能性と必要な追加対策を報告している。

情報システム部の部長は、必要な対策費用を継続的に確保するため、経営会議でサイバーセキュリティ対策の実施状況を報告すべきと考えた。具体的には、サイバーセキュリティ対策の現状と、未対応だが必要な対策について優先度、概算費用および対策を実施しなかった場合のインシデント発生可能性を合わせて報告することにした。

### A社の実践のステップ

情報システム部長が実践したステップは下記の2点である。

- ① 未対応の対策について、他社のサイバー被害事例を元に、自社でのインシデント発生可能性を見積もり、必要な追加対策とその費用概算を検討する
- ② 必要な追加対策、優先度と概算費用を経営会議へ報告し、対応時期を検討する

### A社の実践内容

情報システム部長はプラクティス1-1と合わせて、経営層に対しては必要な対策を継続的に説明することが重要と考えている。そのため、自社でもインシデントが発生する可能性はあるが予算確保が出来ていない対策についても、繰り返し対応優先度と概算費用を報告するプロセスとした。

表2-3.1 サイバーセキュリティ対策の実施状況報告の例

経営会議 報告資料
<b>サイバーセキュリティリスクに関する報告</b>
1. 当社に対するサイバー攻撃の状況
2. サイバーセキュリティ対策の実施状況
3. 他社のサイバー攻撃被害の発生状況
4. その他 サイバー攻撃のトレンド

図2-3.1 経営会議への  
報告内容の目次例

対策 (予算承認済)	対策の詳細	実施状況	
次世代 ファイアウォール 導入	サンドボックス(アプリケーションの振る舞い制御)機能による 入口対策強化。	済	
拠点間通信の VPN導入	本社-工場-データセンター間の 通信の暗号化による 仮想的な専用線の敷設。	済	
対策 (予算未承認)	対策の詳細	優先度	概算 費用
ネットワーク 分離	OA環境と倉庫のIPアドレスの 体系を分け、必要な通信のみ を通過させる施策を実施し、 倉庫への感染拡大を予防。	高	Xxx 万円
SIEMの導入	セキュリティ関連のログを分析・ 監視する専用のシステム。 攻撃の予兆を検知。	中	Xxx 万円

はじめに

第1章

ガイドライン実践のプラクティス

第2章

第3章

付録

## プラクティス 3-2

# サイバーセキュリティ対策のための、 必要なサイバーセキュリティ人材の定義・育成

プラクティス2-1に記載した従業員数1,200名規模の流通業であるC社では、サイバーセキュリティリスクを管理する横断的な組織としてサイバーセキュリティ委員会を立ち上げた。

C社はシステムの開発・運用を外部委託しているが、IT統括部の部長は経営リスクであるサイバーセキュリティについての対策をすべて外部に任せることはできないと考えた。そして自社に必要な知識・スキルを「専門ベンダとコミュニケーションできるレベルのセキュリティの基礎知識」、「自社にとって最適なサイバーセキュリティ対策を選択する能力」と定義し、IT統括部の担当者に専門ベンダの勉強会・セミナー、業界団体の勉強会に参加させることにした。

## C社の実践のステップ

IT統括部長が実践したステップは下記の3点である。

- ① 自組織に必要な役割のうち、専門ベンダを活用する領域、自社で対応が必要な領域を整理する
- ② ①の整理結果それぞれに対し、必要な能力・スキルをIT統括部内で協議、決定する  
その上で、担当者をアサインし、責任を与える
- ③ 担当者の育成に必要な教育や研修を洗い出し、受講させる

## C社の実践内容

IT統括部では、サイバーセキュリティにおいて外部委託する機能についても自社に必要な知識・スキルを定義した。これにより専門ベンダを活用する領域においても自社で最低限の情報収集が必要となることが明らかになり、ベンダ主催の勉強会やセミナーについても担当者をより適切なものに参加させることができるようになった。

表2-3.2 C社のIT統括部における必要な能力・スキルと情報収集元の例

IT統括部の主な役割	担当	自社に必要な能力・スキル	情報収集元
技術的なサイバーセキュリティ対策の企画	自社	<ul style="list-style-type: none"> <li>✓ 最新のサイバーセキュリティ対策を情報収集するスキル</li> <li>✓ 自社のシステム環境やリスクに応じてサイバーセキュリティ対策の優先度を設定するスキル</li> </ul>	<ul style="list-style-type: none"> <li>✓ 専門ベンダの勉強会・セミナー(有料・無料)</li> <li>✓ 業界団体の勉強会</li> </ul>
業務基盤の運用(インシデント対応を含む) 脆弱性や脅威情報の収集	外部委託	<ul style="list-style-type: none"> <li>✓ 外部委託先である専門ベンダとコミュニケーションするためのセキュリティに関する基礎知識</li> </ul>	<ul style="list-style-type: none"> <li>✓ 公開されている各種ガイドラインや研修資料</li> <li>✓ 専門ベンダのセキュリティに関するニュース記事</li> </ul>

7 組織におけるセキュリティ機能の配置、業務運用手順検討、必要なスキルの整理に向けては、下記の資料も参考にできる。  
ユーザ企業のためのセキュリティ統括室構築・運用キット(統括室キット)(産業横断サイバーセキュリティ人材育成検討会)

[https://cyber-risk.or.jp/cric-csf/report/Security-Supervisor\\_Toolkit\\_Part1\\_v1.0.pdf](https://cyber-risk.or.jp/cric-csf/report/Security-Supervisor_Toolkit_Part1_v1.0.pdf)

日本ネットワークセキュリティ協会 (JNSA)「セキュリティ知識分野 (Sec Bok) 人材スキルマップ2017年版」

<https://www.jnsa.org/result/2017/skillmap/>

# 指示 4

# サイバーセキュリティリスクの把握と リスク対応に関する計画の策定

## 指示内容

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。

その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

## 実践のステップ

サイバー攻撃は、情報の窃取だけでなく、システムの変更や停止など正常な運用を妨害するものもあるため、経営戦略の観点から守るべき情報やシステムを特定し、サイバーセキュリティリスクに対応することが望まれる。そのため、実践する上でのステップとしては下記2点が考えられる。

- 自社が保有する情報や利用するシステムを把握し、経営戦略の観点から守るべき情報とシステムを特定する
- サイバー攻撃の脅威や影響度から自社のサイバーセキュリティリスクを把握し、対応する

## 参考情報

情報資産に対するリスク分析については、中小企業の情報セキュリティ対策ガイドライン第3版、並びに付録7のリスク分析シート<sup>8</sup>が活用できる

情報資産管理台帳			評価値				現状から想定されるリスク（入力不要・自動表示）					
業務分類	情報資産名称	備考	機密性	完全性	可用性	重要度	脅威の発生頻度		脆弱性（「対策状況チェックシート」で設定）		被害発生可能性	リスク値
							脅威の状況「シート」で設定	脆弱性の状況「シート」で設定				
人事	社員名簿	社員基本	2	0	0		通常の状態で発生する（いつ発生してもおかしくない）	2.部分的に脆弱性未対策	2	可能性：中	4	リスク大
人事	社員名簿	社員基本	2	2	2		特定の状況で発生する（年に数回程度）	2.部分的に脆弱性未対策	1	可能性：低	2	リスク中
人事	健康診断の結果	雇入 定期健康	2	2	1		特定の状況で発生する（年に数回程度）	2.部分的に脆弱性未対策	1	可能性：低	2	リスク中

図2-4.1 中小企業の情報セキュリティ対策ガイドライン第3版 付録7 リスク分析シート

はじめに  
第1章  
第2章  
第3章  
付録

8 中小企業の情報セキュリティ対策ガイドライン(IPA)  
<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

## 指示 5

サイバーセキュリティリスクに対応するための  
仕組みの構築

## 指示内容

サイバーセキュリティリスクに対応するために保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

## 実践に向けたファーストステップ

情報システムのセキュリティ対策において、旧来は不正侵入を外部環境との接続点で防御しきることができるとの前提に立ち、接続点での不正侵入排除などの対策強化に重点を置いていた。その結果、内部環境には「許可された正常な通信のみ」が行われることが暗黙の想定となり、悪意を持った攻撃者が許可された通信を装って接続点での対策をすり抜け、防御・検知の仕組みが弱い内部環境で自由に活動できてしまうことがあった。

これらの状況を踏まえ、実践する上でのファーストステップは下記2点が考えられる。

- 接続点での対策に加え、内部環境についてもサイバーセキュリティ対策を実施する
- 検知・分析のためにサイバー攻撃の特性を考慮したログを取得する

## 想定される企業の状況

指示5の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- 運用を委託する情報システムに対して、ファイアウォールの設置などの入口対策は実施されているが、次の施策として何から手を付ければよいのかわからない。また、対策にあまりコストをかけられない
- システムの運用先にログ取得の要件を伝える必要があるが、サイバーセキュリティの観点でどのようなログを取得すべきかわからない



## 実践に向けた基礎情報～多層防御の必要性～

サイバーセキュリティ対策において多層防御の必要性が認識される背景として、サイバー攻撃がより高度化したことが挙げられる。「高度標的型攻撃」<sup>9</sup>等と総称されるこのような攻撃は、旧来の対策では侵入を検知することが困難な場合もあり、保存された機密情報の窃取や改ざん、システム停止等を引き起こす可能性がある。また執拗に再侵入を繰り返すことも特徴である。

サイバー攻撃を情報システムと外部環境との接続点で防御しきことは不可能であることを前提に、セキュリティ対策を組み合わせ、一つの対策が破られても次の対策で防御する、あるいは防御しきれなくてもインシデントを速やかに検知するといった、多層防御のアプローチが望まれる<sup>10</sup>。

なお、多層防御は、不正な通信が辿る経路から以下3つの観点で整理することができる。

表2-5.1 多層防御の観点整理の例

観点	対策の種類	説明
外部から侵入させない	ネットワーク(入口)	✓ 自社が管理するネットワーク、システムや端末等とインターネット等の外部環境との接続点で不正な通信が入り込むことを防ぐ対策
内部活動を拡大させない	ネットワーク(内部)	✓ 入口対策をすり抜けた不正な通信に対する、内部LANに保存・設置されている機密情報やシステム等に対する対策、攻撃の予兆等を検知する対策
価値ある情報を守る	ネットワーク(出口)	✓ 外部との不正な通信や外部への不正な情報持ち出しを防ぐ対策
	データ	✓ 持ち出された情報が実質的に利用されないようにする対策 ✓ 重要なデータが破壊・改ざんされても復旧できるよう、適切にバックアップする対策

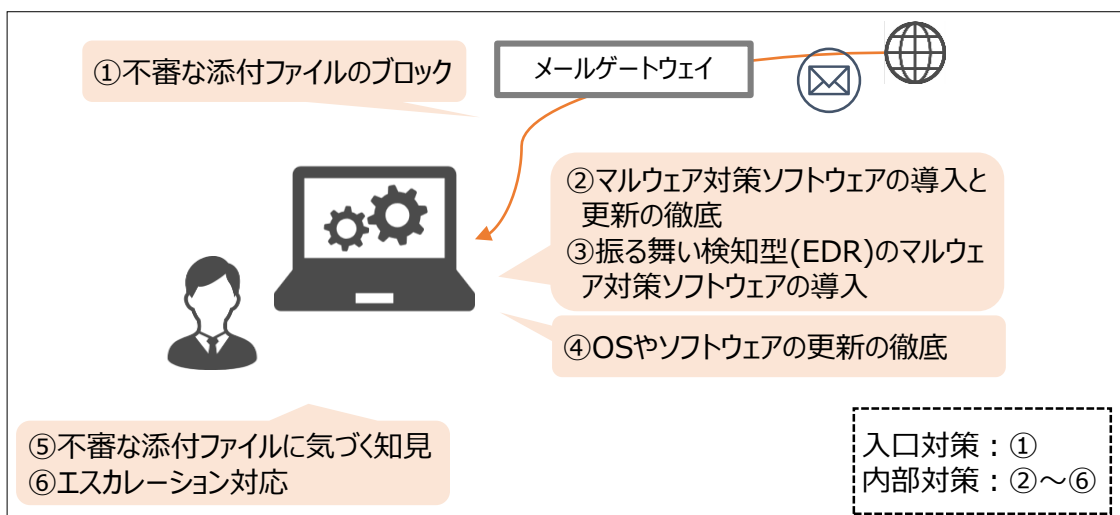


図2-5.1 多層防御の例(メールの添付ファイルによるマルウェア感染リスクの低減)

9 『高度標的型攻撃』対策に向けたシステム設計ガイド(IPA)

<https://www.ipa.go.jp/files/000046236.pdf>

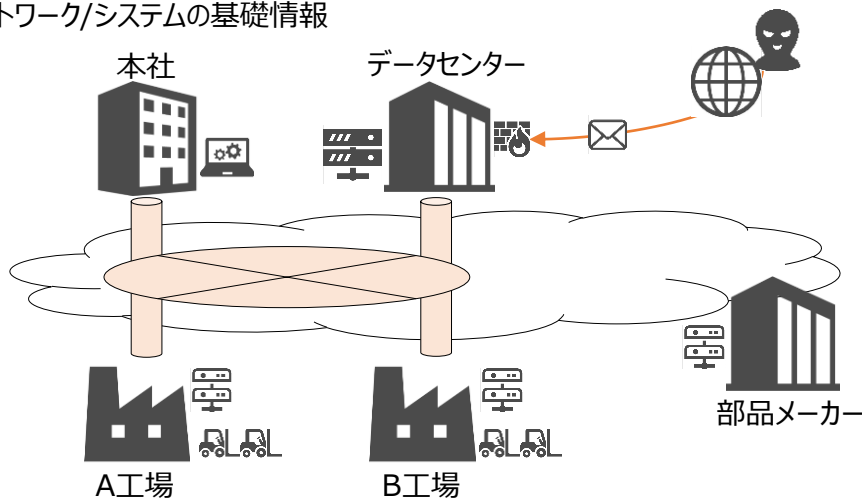
10 【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を(IPA)

<https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html>

## 前提となるD社のシステム環境

従業員数500名規模の製造業であるD社は、本社と2か所の工場をもち、情報システムの運用は全てアウトソーシングしている。各工場に設置されている生産管理を担う制御系システムを最重要のシステムと位置付けている。OA系システムや業務システムは全てデータセンターに設置されており、これまで特段大きなインシデントは発生していないと認識している。

D社ネットワーク/システムの基礎情報



設置場所	設置するシステム
本社	✓ OA系の端末(端末、複合機等)
データセンター	✓ OA系システム(ファイルサーバ、メールサーバ、認証システム等) ✓ 業務系システム(生産管理システム、会計システム、人事システム等)
A工場、B工場	✓ 制御系システム(監視システム、制御システム、コントローラー等)

- 本社、データセンター、各工場は、VPN技術を利用し相互に接続し、利便性を考慮し、構築当初より全て同一セグメントで利用している。
- インターネット利用は、データセンターから接続する設計としている。インターネットとの接続点にはファイアウォールとメールゲートウェイを設置し、委託先の会社で運用・監視している。
- 端末にはマルウェア対策製品が導入され、適宜修正プログラムが適用されている。
- 社外システムである部品メーカーの発注サイトを利用している。

図2-5.2 D社ネットワーク/システムの基礎情報

# プラクティス 5-1

## 多層防御の実施

### D社の実践のステップ

情報システム部の部長は、現状のセキュリティ対策で最重要システムがサイバー攻撃から適切に防御されるか、多層防御の観点を踏まえて確認する必要があると感じた。システム運用委託先と協力し、社内システム・ネットワークについて調査・整理した。

- ① 最重要システムについて、持ち込みPCや可搬記憶媒体の利用が常態化していないことを確認した
- ② 標的型攻撃を脅威シナリオとし、標的型攻撃のメールが社内のメールゲートウェイをすり抜けて端末へ到達し、C&Cサーバとの通信が確立したとの前提で、問題点を調査した
- ③ 業務システムやOSの権限設定等のアクセス制御に一部不備があること、そして最重要システムへ、ネットワーク上のどの端末からでも参照できる状態であることが判明した

### D社の実践内容

調査結果を受けた情報システム部長は、ガイドライン<sup>11,12</sup>を参考にコストとのバランスに配慮し、問題点と実践する対策を次表の通り選定した。各対策の内容は「A：攻撃に利用される端末への対策」、「B：最重要システムに到達させない対策」、「C：サーバへ侵入させない対策、検知のためのログ取得(“プラクティス5-2”参照)」、「D：破壊されても元に戻せる対策」である。

表2-5.2 多層防御の観点で発見された問題点と実践内容の例

	発見した問題点	実践内容
A: 端末への対応	➤ マルウェア対策ソフトウェア等の定義ファイルを更新していない端末があった	➤ 全端末の状態を常時監視し、定義ファイル等が古い場合は更新する運用とした
B: ネットワークの分離	➤ 最重要システムに無関係な端末が、最重要システムを参照できてしまった	➤ 場所毎にIPアドレス体系を分け、必要な通信のみが通過する設計とした ➤ 社外システムを利用する端末を限定し、社内ネットワークから切り離れた
C: サーバへの対応	➤ 社内を踏み台とした不正アクセスを想定した対応を検討していなかった	➤ サーバへのアクセス権限設定を見直した ➤ 検知のためのログ取得について検討した
D: バックアップ	➤ バックアップデータが同一システム内に保存される設計で、サイバー攻撃時に同時に破壊され、復旧できないリスクがあった	➤ バックアップデータを定期的に電子媒体にコピーし、システムとは別の場所で保管する運用とした

情報システム部の部長は次のステップとして、コストの問題で先送りした更なる投資(EDRの導入等)や、他の脅威シナリオをベースにした対策検討を予定している。

はじめに

第1章

ガイドライン実践のプラクティス

第2章

第3章

付録

11 日常における情報セキュリティ対策(IPA) <https://www.ipa.go.jp/security/measures/everyday.html>

12 『高度標的型攻撃』対策に向けたシステム設計ガイド(IPA) <https://www.ipa.go.jp/files/000046236.pdf>

# プラクティス 5-2 アクセスログの取得

前述のD社において、取り組むべきサイバーセキュリティ対策のもう一つの観点としてログの取得・分析が挙げられた。システムが出力するログは、不正アクセスの検知や被害状況の把握等の際に必要な重要な記録である。

また、予兆やインシデントの検知のためには、事前に、ログ取得の目的や取得する項目、また保管や確認方法等を整備しておく必要がある。

## D社の実践のステップ

情報システム部長は、「サーバへの対応」として挙げた、不正アクセスを検知するためのログ取得について調査した。

- ① ログを取得すべきサーバを、不正アクセスのターゲットとして懸念される「最重要システム（A工場とB工場の制御系システム）」と「ユーザ認証機能をもつシステム」と定めた
- ② 現在の設定では、社内を踏み台とした不正アクセス等が発生した際の調査を実施するためのログが不足しており、保管方法も再検討が必要であることが判明した

## D社の実践内容

アクセス失敗のログも取得できるように設定を変更する等、ログの収集設定と保管の運用を確立させたことで、インシデントが発生した「後」に調査可能な状態にした。

表2-5.3 ログ取得の観点で発見された問題点と実践内容の例

	発見した問題点	実践内容
アクセスログの取得	<ul style="list-style-type: none"> <li>➤ ログオン試行時のアクセス失敗のログを取得しておらず、悪意を持った第三者の振る舞いを検知できないリスクがある</li> </ul>	<ul style="list-style-type: none"> <li>➤ アクセス失敗のログも取得できるように設定を変更した</li> </ul>
アクセスログ等の保管	<ul style="list-style-type: none"> <li>➤ アクセスログやイベントログ等の検知に有益なログが同じシステム内に保存される設計であり、不正アクセス時に消去されるリスクがある</li> </ul>	<ul style="list-style-type: none"> <li>➤ 定期的に電子媒体にコピーし、システムとは別の場所で保管する運用とした</li> </ul>

情報システム部長は、不正アクセスの予兆やインシデントに気づくことを次のステップとして、情報システム部のメンバーによる日次での目視確認や専用システム<sup>13</sup>の導入等を検討し始めている。

13 セキュリティ関連のログを分析・監視することを目的とした専用のシステムとしてSIEM(Security Information and Event Management)システムがある。ログを一元管理し異常を自動検出するシステムである。ログの調査は対象システムだけではなく、OS等の関する知識も必要となるため、必要に応じて外部サービスを検討することも有用である。

# 指示 6

# サイバーセキュリティ対策におけるPDCAサイクルの実施

## 指示内容

計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる。  
 その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。  
 また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

はじめに  
第1章

## 実践のステップ

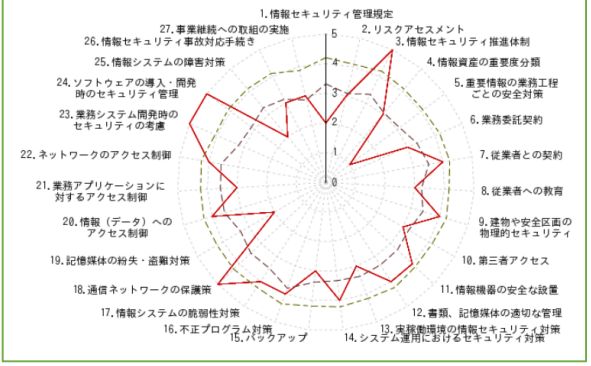
サイバーセキュリティ対策におけるPDCAサイクルの実施に向けては、新たな脅威の発生を含むサイバー攻撃のトレンドの変化や、セキュリティ製品等の対策の進化に対応し続けることが可能な体制とすることが望まれる。そのため、実践する上でのステップとしては下記の2点が考えられる。

- 自社のセキュリティ対策の状況や水準を評価する
- 評価結果については、問題点や改善策を含め経営者に報告する

## 参考情報

セキュリティ対策状況の評価については、情報セキュリティ対策ベンチマーク<sup>14</sup>が活用できる。Webページ上の質問に答えると、スコア（点数）、レーダーチャート、散布図などの診断結果が表示され、診断を行った他社の対策状況と比較できる。

第2章  
ガイドライン実践のプラクティス



主な診断項目は下記5点である。

- ① 組織的な取組み状況
- ② 物理・環境的セキュリティの施策
- ③ 情報システム及び通信ネットワークの運用管理状況
- ④ 情報システムのアクセス制御状況及び開発・保守におけるセキュリティ対策状況
- ⑤ 情報セキュリティ上の事故対応状況

第3章  
付録

図2-6.1 自己診断テスト結果イメージ

14 組織の情報セキュリティ対策自己診断テスト 情報セキュリティ対策ベンチマーク(IPA)  
<https://www.ipa.go.jp/security/benchmark/index.html>

## 指示 7

# インシデント発生時の緊急対応体制の整備

### 指示内容

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

また、インシデント発生時の対応について、適宜実践的な演習を実施させる。

### 実践に向けたファーストステップ

未対策の脆弱性を狙ったサイバー攻撃や、攻撃手法が解析されていない標的型攻撃等は、最先端のセキュリティ対策をしても完全には防げない。そのため、インシデント発生時には速やかに対応して被害を極小化する必要がある。平時からインシデント発生時の緊急対応体制を整備することが望まれる。実践する上でのファーストステップとしては下記の2点が考えられる。

- 自社にとって重要な影響を及ぼす可能性のあるインシデントに対して、対応部署や統括部署等の組織内の役割・体制を整備する
- 証拠保全や関係部門周知等、自社がなすべき初動対応を取り決める

### 想定される企業の状況

指示7の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- インシデントに対応するための組織内の対応体制(CSIRT等)が整備されていない
- 端末が攻撃された場合の証拠保全のルールを定めていない

## 実践に向けた基礎情報～緊急対応体制の必要性～

標的型攻撃等により、攻撃者が組織内部への侵入に成功すると、工場等の重要なシステムが長時間停止させられたり、重要な情報が長期間窃取され続けたり、他組織への攻撃の踏み台として利用される場合がある。

そのため、影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備することが重要となる。

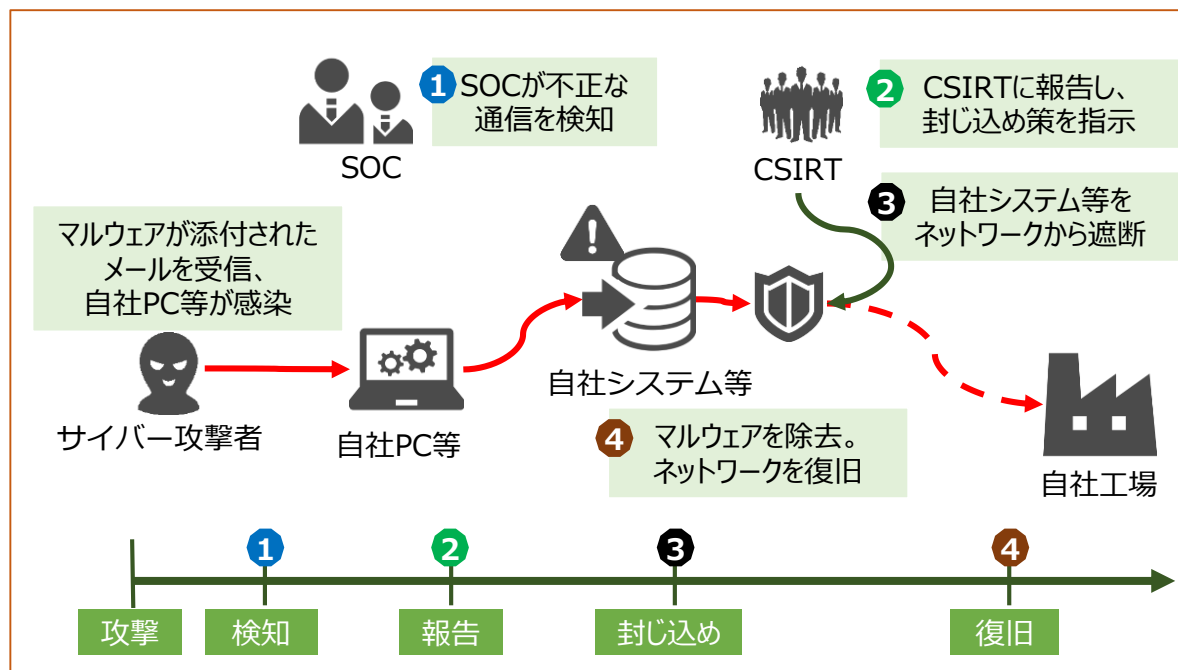


図2-7.1 サイバー攻撃に対するインシデントレスポンスの流れ(イメージ)

表2-7.1 インシデント対応の流れとCSIRTの主な活動の例<sup>15</sup>

インシデント対応の流れ	CSIRTの主な活動例
①検知	<ul style="list-style-type: none"> <li>Webサイトの改ざんやシステムの停止、また標的型メール等に関する外部組織や社内、顧客からの通報を受領</li> <li>ログ監視等からC&amp;Cサーバ等との不正な通信を発見</li> </ul>
②報告	<ul style="list-style-type: none"> <li>発生事象に応じた組織内外との連携（システム運用の委託先や専門ベンダを含む）</li> </ul>
③封じ込め	<ul style="list-style-type: none"> <li>インシデントの影響分析・対応優先度の判断</li> <li>被害極小化のための暫定対応の実施（システム停止・ネットワーク遮断など）</li> </ul>
④復旧	<ul style="list-style-type: none"> <li>恒久対応を実施し、サービスやシステムを復旧</li> </ul>

はじめに

第1章

ガイドライン実践のプラクティス 第2章

第3章

付録

15 脅威シナリオに応じたインシデント対応手順の策定に向けては、下記の資料も参考にできる。  
JPCERTコーディネーションセンター「インシデントハンドリングマニュアル」  
[https://www.jp-cert.or.jp/csirt\\_material/files/manual\\_ver1.0\\_20151126.pdf](https://www.jp-cert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf)

## プラクティス 7-1

# 旗振り役としてのCSIRTの設置

従業員数3,000名規模の小売業であるE社では、過去にビジネスメール詐欺の被害に遭った経験を持つ。その際に、インシデントによって対応部署が分かれていることもあり、従業員からのインシデント報告が速やかに行われず対応に時間を要した経緯がある。

そのため、総務部の部長と情報システム部の部長は、再発防止策としてインシデントが発生した際の対応を推進する旗振り部署となるCSIRT<sup>16,17</sup>を設置することとし、情報システム部の一部メンバが兼任することになった。

## E社の実践のステップ

総務部長と情報システム部長が実践したステップは下記の2点である。

- ① IPAが発表する「情報セキュリティ10大脅威<sup>18</sup>」のうち、自社でも起こりうる上位5件の脅威シナリオについて、インシデント発生時に対応を旗振りする部署と対応部署を決める
- ② 旗振り部署については、社内のポータルサイトに掲載する等、インシデント発生時の報告窓口として周知する

## E社の実践内容

上記のステップに則り、総務部の部長と情報システム部の部長は自社でも起こりうるセキュリティインシデントに対する認識を共有し、インシデント発生時の旗振り部署を定義し、周知した。

表2-7.2 E社におけるインシデント発生時の旗振り部署と対応部署の例

順位	組織に対する脅威	自社での発生可能性	旗振り部署	対応部署
1位	標的型攻撃による被害	○	情報システム部 (E社 CSIRT)	情報システム部
2位	ビジネスメール詐欺による被害	○		法務部
3位	ランサムウェアによる被害	○		情報システム部
4位	サプライチェーンの弱点を悪用した攻撃の高まり	○		総務部
5位	内部不正による情報漏えい	○	内部通報窓口	法務部 情報システム部

16 CSIRTに必要な人材については、下記の資料も参考にできる。

JPCERTコーディネーションセンター「組織内 CSIRT の役割とその範囲」

[https://www.jpcert.or.jp/csirt\\_material/files/02\\_role\\_of\\_csirt20151126.pdf](https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt20151126.pdf)

17 日本シーサート協議会「CSIRT人材の定義と確保(Ver.1.5)」

<http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf>

18 情報セキュリティ10大脅威 2019(IPA) <https://www.ipa.go.jp/security/vuln/10threats2019.html>



# プラクティス 7-2

## 従業員の初動対応の定義

前述のE社では再発防止策としてインシデントが発生した際の対応を推進する旗振り部署(CSIRT)を決め、社内にインシデント報告窓口として周知している。

上記の活動に加えて、E社ではインシデント発生時に従業員が速やかに適切な行動をとれるように、初動対応を定義し、CSIRTが周知している。

### E社の実践のステップ

総務部長と情報システム部長が実践したステップは下記の2点である。

- ① IPAが発表する「情報セキュリティ10大脅威」のうち、自社でも起こりうる上位5件の脅威シナリオについて、証拠保全<sup>19</sup>の観点からインシデント発生時における従業員の初動対応を定義する
- ② 社内のポータルサイトに掲載する等、CSIRTからインシデント発生時の初動対応を周知する

### E社の実践内容

上記のステップに則り、E社のCSIRTである情報システム部は自社でも起こりうるセキュリティインシデントとインシデント発生時に従業員が取るべき初動対応を定義し、周知した。

表2-7.3 E社におけるインシデント発生時の従業員の初動対応の例<sup>20</sup>

順位	組織に対する脅威	証拠保全	インシデント発生時の従業員の初動対応
1位	標的型攻撃による被害	要	<ul style="list-style-type: none"> <li>• PCをネットワークから切断する</li> <li>• メールやファイルを削除しない</li> <li>• PCの電源を切らない</li> </ul>
2位	ビジネスメール詐欺による被害	要	<ul style="list-style-type: none"> <li>• メールを削除しない</li> </ul>
3位	ランサムウェアによる被害	要	<ul style="list-style-type: none"> <li>• PCをネットワークから切断する</li> <li>• メールやファイルを削除しない</li> <li>• PCの電源を切らない</li> </ul>
4位	サプライチェーンの弱点を悪用した攻撃の高まり	要	<ul style="list-style-type: none"> <li>• 取引先周知</li> </ul>
5位	内部不正による情報漏えい	要	<ul style="list-style-type: none"> <li>• 関係部門周知</li> </ul>

はじめに

第1章

ガイドライン実践のプラクティス 第2章

第3章

付録

19 インシデント対応時の証拠保全については、下記の資料も参考にできる。  
デジタル・フォレンジック研究会「証拠保全ガイドライン第7版」  
<https://digitalforensic.jp/home-act-products-df-guideline-7th/>

20 サイバーインシデントに関する調査は、専門知識や十分な経験が無い状態で実施すると攻撃の痕跡を消してしまう可能性があるため、有事の際に相談できるセキュリティに関する外部専門組織を確保しておくことが有用。  
情報セキュリティサービス基準適合サービスリスト(IPA) [https://www.ipa.go.jp/security/it-service/service\\_list.html](https://www.ipa.go.jp/security/it-service/service_list.html)  
日本ネットワークセキュリティ協会(JNSA)サイバーインシデント緊急対応企業一覧  
[https://www.jnsa.org/emergency\\_response/](https://www.jnsa.org/emergency_response/)

## 指示 8

インシデントによる被害に備えた復旧体制  
の整備

## 指示内容

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。

BCPとの連携等、組織全体として整合のとれた復旧目標計画を定めさせる。

また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

## 実践に向けたファーストステップ

サイバー攻撃は情報漏えいだけでなく、重要なシステムの停止等による業務停止を引き起こすものがある。そのため、自然災害等を想定した既存のBCP<sup>21</sup>と連携する等、組織としてサイバー攻撃によるインシデントに対する復旧体制を整備することが望まれる。

実践する上でのファーストステップとしては下記の3点が考えられる。

- 自然災害等を想定したBCP策定の経験を有するチームとインシデント対応チームで情報を共有する
- インシデント影響度に応じた復旧対応の判断基準および判断フローを整備する
- システム障害の事業継続に与える影響が大きく優先度の高いシステムについて、復旧手順を検討し演習により確認する

## 想定される企業の状況

指示8の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取組みを実施した企業の事例をプラクティスとして紹介する。

- 自然災害を想定したIT-BCP<sup>22</sup>は策定しているが、どのような観点から既存のBCPと連携させるべきか分からない
- インシデントに対する訓練や演習を実施したいが、システム運用委託先に加え、セキュリティに関する専門ベンダとのコミュニケーションが必要となるため、実施のハードルが高いと考えている

21 BCPはBusiness Continuity Planの略で緊急事態の際の損害を最小限に抑え、事業の継続や復旧を図るための計画のこと  
22 IT-BCPの策定方法はIT-BCP策定モデル(NISC)も参考にできる。

<https://www.nisc.go.jp/active/general/itbcp-guideline.html>

# プラクティス

## 8-1

# インシデント対応時の 危機対策本部との連携

従業員数2,000名規模の流通業であるF社では、自然災害を想定したBCPを策定しており、重要システムのデータを遠隔地のデータセンターに保管する等、データセンターが被災した場合でも事業を継続できる体制を整備している。

情報システム部の部長はインシデント対応の特徴として、被害の拡大防止のために意図的にシステムを停止させたり、ネットワークから遮断させる場合がある点を考慮し、自社のBCPと整合したインシデント対応の判断フローを整備することとした。

## F社の実践のステップ

情報システム部長が実践したステップは下記の2点である。

- ① インシデント対応により意図的にシステム機能を制限したり、停止するケースを洗い出す
- ② 危機対策本部との連携を考慮したインシデント対応の判断フローを策定する

## F社の実践内容

既存のBCPと連携させるため、情報システム部長は危機対策本部との事前協議するインシデント対応として、取引影響がある重要システムに対するシステム停止等と全従業員に影響があるメール機能の制限を選定した。

表2-8.1 F社におけるシステム停止を伴うインシデント対応の判断者と役割の例

インシデント 対応	影響範囲	インシデント発生時の判断者と役割			
		システム部 担当者	システム部 部長	経営者	危機対策 本部
個別システムの 停止 (遮断を含む)	取引影響なし	最終判断	事前協議	事後報告	-
	取引影響あり (重要システム)	-	1次判断	最終判断	事前協議
メール機能の 制限	F社の全環境	1次判断	最終判断	事前協議	事前協議

はじめに

第1章

ガイドライン  
実践の  
プラクティス

第2章

第3章

付録

## プラクティス 8-2

# 組織内外の連絡先の定期メンテナンス

前述のF社では、自然災害を想定したBCPを策定しており、年に1回BCP訓練を実施しているが、サイバー攻撃を想定した訓練や疑似演習は実施していない。

情報システム部の部長は、サイバー攻撃によるインシデント発生時は通常のシステム障害と異なり、システム運用委託先に加えてセキュリティに関する専門ベンダとの連携が必要となると考え、BCP訓練のタイミングで組織内外の連絡先を全てメンテナンスすることとした。なお、災害発生時の連絡先はメーリングリストでまとめられているが、例年のBCP訓練では訓練シナリオに関係する連絡先のみをチェックしていた。また、連絡先にIT部門が含まれているかどうか確認したことがなかった。

### F社の実践のステップ

情報システム部長が実践したステップは下記の3点である。

- ① 必要なIT部門が災害時の連絡先に含まれているか確認し、抜け漏れがあれば追加する。
- ② BCP訓練対象でない連絡先について、訓練と同期して担当者の電話番号・メールアドレスに変更がないか、確認する
- ③ 災害発生時に利用する、BCP向けに存在している全ての連絡先にテストメールを発信する

### F社の実践内容

情報システム部長は、サイバー攻撃を想定した疑似演習において意図的に本番システムを攻撃させることは、実施のハードルが高いと考えた。そこで、自社だけで対応可能なインシデント発生時の連絡先の定期的なメンテナンスとメーリングリストへのテストメール発信を最低限実施するプロセスとした。

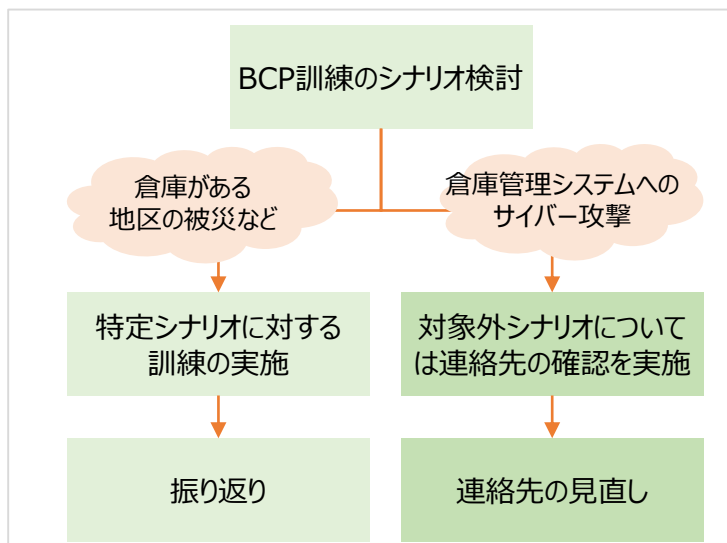


図2-8.1 F社のBCP訓練の流れ

## 指示 9

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

### 指示内容

監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。

システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

はじめに

第1章

### 実践に向けたファーストステップ

昨今、企業を取り巻くサプライチェーンは広がりを見せており、システム開発・運用等、様々な業務において系列企業だけでなく、多くのビジネスパートナーや委託先等が携わっている。

サイバー攻撃者は、大企業と比較してサイバーセキュリティ対策が進んでいない中小の委託先等を侵入口とし、そこからシステム・ネットワークを通じて繋がっている企業を攻撃することもあるため、ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握が望まれる。

実践する上でのファーストステップとしては下記の2点が考えられる。

- サイバーセキュリティリスクのある委託先の特定
- サイバーセキュリティリスクのある委託先に対するサイバーセキュリティ対策状況の把握

ガイドライン実践のプラクティス 第2章

第3章

付録

### 想定される企業の状況

指示9の実践に向けては下記のような状況や課題が想定されるため、本節ではそれらに対応するための取り組みを実施した企業の事例をプラクティスとして紹介する。

- 業務を主管する部署がそれぞれ業務委託しており、会社として委託先を把握していないため、サイバーセキュリティリスクがある委託先を網羅的に調査し、特定することができない
- サイバーセキュリティ対策の実施状況を、どのような観点で確認すべきか分からない

## プラクティス 9-1

# サイバーセキュリティリスクのある 委託先の特定と対策状況の確認

従業員数3,000名規模の製造業であるG社では、取引先がマルウェアに感染し、ある部品の供給が一時滞った経験を持つ。その際は、在庫で対応でき自社ビジネスに大きな影響はなかったものの、G社は自社のサイバーセキュリティを担当する情報システム部に相談の上、サイバーセキュリティリスクのある取引先/委託先に対して、サイバーセキュリティ対策状況を確認することとした。

## G社の実践のステップ

情報システム部長が実践したステップは下記の3点である。

- ① 委託元部署へのアンケートを通じて、取引先/委託先に対して業務におけるインターネットの利用等、サイバーセキュリティリスクの有無を調査する
- ② サイバーセキュリティリスクのある取引先/委託先に対して、サイバーセキュリティ対策状況に関するアンケート調査を実施する
- ③ 把握した課題やリスクは一覧化し、経営者に報告するとともに、組織として対応方針を検討する

## G社の実践内容

上記のステップに則り、まず情報システム部長は社内の調達に関連する情報が集まる法務部と相談の上、委託元部署へのアンケートを通じて、主要な取引先/委託先の洗い出しとサイバーセキュリティリスクの有無を調査した。

表2-9.1 委託元部署へのアンケート表の例

取引先/ 委託先名	取引/委託 元部署	取引/委託業務	インシデント発生時 に影響を受ける 自社の業務 (選択式)	委託先の 業務環境 (選択式)	委託業務に おける インターネット 利用
株式会社 123	倉庫管理部	商品Aの配送業務	商品Aの配送	他社と業務環境 を共有	無
<b>サイバーセキュリティリスク有と判断し、対策状況を確認</b>					
ABC 株式会社	総務部	コールセンター業務	直販商品Bの受注 カスタマーからの 苦情・相談受付	他社と業務環境 を共有	有
456 株式会社	製品部	原材料Aの製造	商品Aの製造停止	自社向けの 専用環境	有

次に、情報システム部長はサイバーセキュリティリスクがあると判断した取引先/委託先に対して、サイバーセキュリティ対策の実施状況を把握するため、アンケート表を送付した。なお、アンケート表作成においては、質問を依頼する委託元部署、並びに回答する取引先/委託先の負荷を考慮し、セキュリティに関するガイドライン<sup>23</sup>から主要なポイントを抽出し、必要最低限の質問事項とした。

表2-9.2 G社の取引先/委託先へのアンケート表の例

分類	質問事項	対策状況 (有/無)	具体的な対策の実施内容 (自由記入欄)
セキュリティ管理体制	セキュリティポリシーは策定していますか	有	<p><b>【受領した回答に対する対応】</b></p> <p>回答内容により、情報システム部より追加質問(対策状況を裏付ける証拠の依頼を含む)を実施し、対策状況の総合的な評価を実施</p>
	委託業務におけるセキュリティ管理体制はありますか		
	委託業務に従事する担当者に対してセキュリティ教育は実施していますか		
	(再委託がある場合のみ回答) 再委託先のセキュリティ対策状況は把握していますか		
外部攻撃に対する対策	通信経路は限定していますか		
	侵入防止機器は設置していますか		
	不正な通信を監視していますか		
	インシデント発生時の対応・復旧手順は整備していますか		
...	...		

はじめに

第1章

ガイドライン実践のプラクティス 第2章

上記のアンケート表にて、サイバーセキュリティ対策状況に懸念がある取引先/委託先については、現場判断で即時に取引先/委託先を変更する等の対応が困難な場合もあるため、調査結果を経営者へ報告するとともに、組織としてのリスク対応方針を検討することとした。

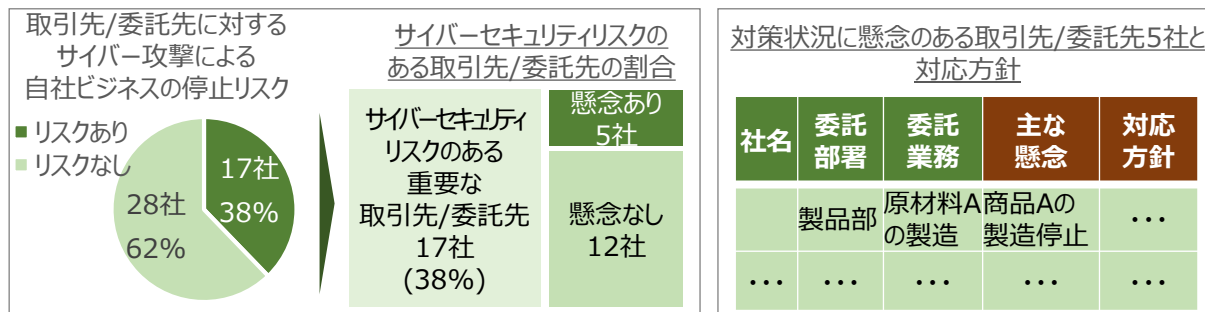


図2-9.1 調査結果の経営者報告資料のイメージ

第3章

付録

23 サイバーセキュリティ経営ガイドラインの他、情報セキュリティ管理基準(経済産業省)も参考にできる [https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS\\_Management\\_Standard\\_H28.pdf](https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf)

## 指示 10

情報共有活動への参加を通じた  
攻撃情報の入手とその有効活用及び提供

## 指示内容

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。

また、入手した情報を有効活用するための環境整備をさせる。

## 実践のステップ

情報共有活動への参加により、「他社での攻撃確認情報」や「脆弱性情報」などの情報を収集・活用し、他社と同様の被害を未然に防止することが望まれる。実践する上でのステップとしては下記2点が考えられる。

- サイバーセキュリティに関する情報共有活動に参加する
- 情報を提供・収集し、自社のサイバーセキュリティ対策に活用する

## 参考情報

IPAや一般社団法人JPCERTコーディネーションセンター等が公表する脆弱性情報などの注意喚起情報を確認する他、標的型サイバー攻撃を受けた際には情報提供を行い、必要に応じて調整を依頼することが可能である。

- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報(JPCERT/CC・IPA)  
<https://jvn.jp/report/index.html>
- コンピュータウイルス・不正アクセス・脆弱性情報に関する発見・被害の届出や情報提供(IPA)  
<https://www.ipa.go.jp/security/todoke/index.html>
- 標的型サイバー攻撃特別相談窓口(IPA)  
<https://www.ipa.go.jp/security/tokubetsu/index.html>
- @police(警察庁)  
<https://www.npa.go.jp/cyberpolice/>



## 第3章 セキュリティ担当者の悩みと取組みのプラクティス

サイバーセキュリティ対策をこれから実践するセキュリティ担当者が**対策を推進する上での悩み**を解決するために取組んだ際の**実践手順、内容、取組む際の考え方、得られた知見**をプラクティスとして示す。

セキュリティ担当者の悩み		取組みのプラクティス	関連する重要10項目
(1)	インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	社外専門家を活用しながら自社でサイバーセキュリティ人材を育成する	2
(2)	インシデント対応の初動における情報共有に不安がある	標的型メール訓練で開封したかではなく報告したかを意識させる	7
(3)	インシデントが起きた際の財務面でのリスクヘッジが十分ではない	初動対応のリスクを減らすサイバー保険の活用を検討する	4
(4)	IoT機器が「シャドーIT」化している	製造部門とIT部門が連携し、不正接続機器や不適切な設定を排除する	3
(5)	自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる	自社のセキュリティルールに整合する、適切なクラウドサービスを利用する	4
(6)	全国各地の拠点におけるセキュリティ管理状況に不安がある	拠点におけるセキュリティの取組みを把握し、対面に対話する	6
(7)	外部サービスの選定でIT部門だけでは対応が困難である	社内の関連部門と連携して外部サービスの選定を行う	2
(8)	IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている	外部講師による経営層向けの研修会を実施する	1
(9)	従業員に対してセキュリティ教育を実施しているが効果が感じられない	特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する	3
(10)	スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	セキュリティ対策の取組み、セキュリティ認証の取得状況を確認する	9

## 悩み (1)

# インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある

H社では、インシデント発生時に対応体制が明確でなく対応に時間を要した反省から、CSIRTを設置することとなった。しかし、自社にセキュリティ専門家が十分にいない状況であった。

### 基本情報

#### H社の状況

- ✓ 現在、セキュリティ委員会、CSIRTといったセキュリティ管理体制を構築している段階である。
- ✓ IT部門がセキュリティを主管しているが、セキュリティ専門家が十分にはいない。
- ✓ 外部ネットワークに接続していない制御システムを扱う製造部門では、セキュリティ意識が定着していないという課題がある。

#### H社のプロフィール

業種	製造業	
規模	500人	
管理体制	CISOの有無	有 (CROが兼任)
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

### セキュリティ担当者の問題・悩み



H社では、最近、ビジネスメール詐欺に遭った経験がある。

しかし、インシデント対応体制が整備されておらず、インシデント発生時の社内外への連絡体制が不十分であった。

そのため、社内の関連部署や外部機関と円滑に連携できず、対応完了までに約1ヶ月もの時間を要した。

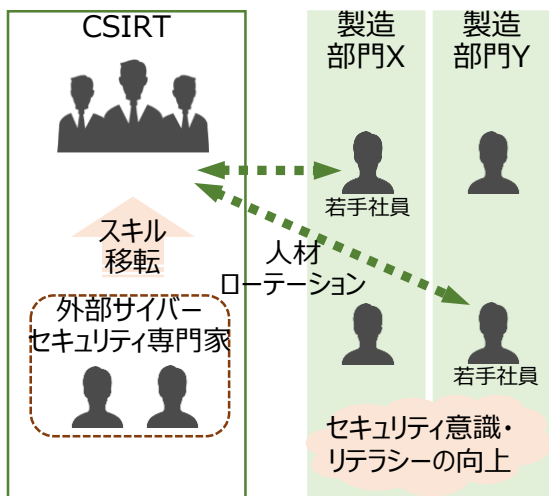
この件を受けて、IT部門長を筆頭に、**CSIRTを設置することになったが、社内**にセキュリティ専門家が十分にいないことが問題となっていた。

# 取組み (1) 社外専門家を活用しながら 自社でサイバーセキュリティ人材を育成する

## 解決に向けたアプローチ

### CSIRT (イメージ)

- 将来的に自社社員のみで運営可能なよう、**外部専門家からスキル移転**を行う
- 若手社員をCSIRTに配置し、**ローテーション**を行う



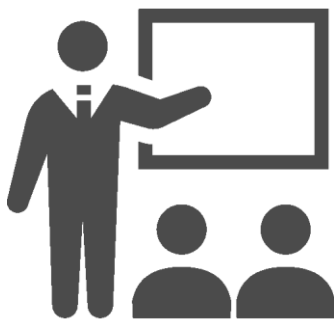
そこでH社は、**外部のサイバーセキュリティ専門家を活用しながら、自社でサイバーセキュリティ人材を育成**することを検討している。

- 体制構築～構築後序盤は**外部専門家**を関与させる。
- 社員のみでもCSIRTが運営できるよう、外部専門家から**スキル移転**を行う。
- ローテーションによる人的交流を活用し、CSIRTと各部署との連携のしやすさを促進させる。

人材ローテーションの副次効果として、以下も期待している。

- CSIRTを経て、**若手社員にセキュリティリテラシーを身に付けさせる**とともに、ローテーションで各部に再配置されることで、**各部門（特に製造部門）でのセキュリティ意識の向上**を図る。

## 得られた知見



IT部門長は、外部専門家に依存してしまうと、自社で適切な判断ができなくなってしまうおそれがあると考え、CSIRTが自社で運営可能な体制となるよう、**ローテーションを行う人材のキャリアパスを検討することが重要**と考えている。

また、これまで制御システムは外部ネットワークに接続していないケースが多く、サイバー攻撃等は受けにくいと考えられてきた。しかし、近年では製造ラインでIoT機器の利用も活発になってきており、サイバーセキュリティリスクが高まっている。

そのため、IT部門長は、**製造部門においてもセキュリティ意識を高めることが必要不可欠**であると考えている。

はじめに

第1章

第2章

第3章  
担当者の悩みと取組みのプラクティス

付録

## 悩み (2)

# インシデント対応の初動における 情報共有に不安がある

I社では、従業員が標的型攻撃メールに記載されたURLを参照してしまった、あるいはメールの添付ファイルを開けてしまった、といったインシデントに関する情報が報告されにくいという問題があった。

### 基本情報

#### I社の状況

- ✓ インシデント発生時にセキュリティ部門へ報告されにくいという問題がある。
- ✓ 以前、サイバー攻撃を受けた際には金銭が窃取される直前まで事態が深刻化し、関係者が厳しく叱責された、という事実とは異なる噂が社内に流れたことがあった。

#### I社のプロフィール

業種	製造業	
規模	1,000人	
管理体制	CISOの有無	有
	専任のセキュリティ部署	有
	サイバーセキュリティの 主管部署	セキュリティ部門

### セキュリティ担当者の問題・悩み



過去のインシデント対応において、従業員が標的型攻撃メールを開封してしまった際に、セキュリティ部門への連絡が速やかになされず、適切な初動対応が行えない事例があった。

従業員に対して、**インシデント発生時に報告しやすくする工夫が必要**ではないか、と考えていた。

## 取組み (2) 標的型メール訓練で開封したかではなく 報告したかを意識させる

### 解決に向けたアプローチ

そこでI社は、標的型攻撃メールの添付ファイルを開いてしまう等のインシデントが発生した際に、セキュリティ部門へ速やかに報告してもらうために、以下のような取組みを行った。

#### 報告率を向上させる工夫(例)

- ✓ 標的型攻撃メール訓練時には、メール記載のURLや、メールの添付ファイルの「開封率」だけでなく「報告率」も計測、分析。
- ✓ 報告率が低い、報告スピードが遅い傾向がある場合は、アンケートで原因分析を行った上で、初動対応方法の周知を行うなど個別にフォローアップを実施。
- ✓ 日頃から、不審なメールは「開封しない」ではなく「開封した場合は報告する」ことを周知。

#### 標的型攻撃メール訓練結果

	所属人数	開封者	開封率	開封報告	報告率
部署A	56人	32人	57%	30人	94%
部署B	72人	21人	29%	5人	24%
部署C	45人	12人	27%	10人	83%
⋮	⋮	⋮	⋮	⋮	⋮

部署Aは「開封率」は高いが、「報告率」が高い

部署Bは「開封率」が低い  
が、「報告率」が低い

部署Bに対しても「適時に報告すること」を、周知

### 得られた知見



セキュリティインシデントが起きないように最善を尽くすべきではあるが、どれだけ対策を講じても、インシデントをなくすことは難しい。そのためI社は、インシデント発生時には、速やかに対応し、被害を最小化することが重要であると考えている。

また、不審メールを開封したという、ネガティブに捉えられ、「報告・相談したくない」という意識が働いてしまいがちである。

しかし「報告してくれてありがとう」と伝えて、報告したことをポジティブに評価する風土を作りたいと考えている。

はじめに

第1章

第2章

担当者の悩みと取組みのプラクティス 第3章

付録

## 悩み (3)

# インシデントが起きた際の 財務面でのリスクヘッジが十分ではない

J社は顧客情報を活用する業態であり、個人情報漏えい保険に加入している。しかし、サイバー攻撃等については加入している個人情報漏えい保険では補償されないケースがあると聞き、インシデント発生時の特に財務面でのリスクヘッジについて検討していた。

### 基本情報

#### J社の状況

- ✓ 製造業であり、ECサイト経由で、消費者向けに製品の販売を行っている。
- ✓ 顧客情報を活用する業態である。
- ✓ 個人情報漏えい保険に加入している。

#### J社のプロフィール

業種	製造業	
規模	4,000人	
管理体制	CISOの有無	有 (CIOと兼任)
	専任のセキュリティ部署	有
	サイバーセキュリティの 主管部署	セキュリティ部門

### セキュリティ担当者の問題・悩み



J社のセキュリティ部門長は、既存の個人情報漏えい保険ではサイバー攻撃を受けた際に生じた被害の一部や調査費用は補償されなかった、という他社事例を聞いた。

そこで、現状の個人情報漏えい保険をそのまま契約し続けるべきか、インシデント発生時のリスク対策費用確保に係る経営リスクをよりヘッジする策は他にないか、を検討すべきと感じていた。

## 取組み (3) 初動対応のコストを減らす サイバー保険の活用を検討する

### 解決に向けたアプローチ

そこでセキュリティ部門長は、保険会社に問い合わせるなどして、J社が加入している保険では以下の問題点が解消されないことを認識し、対応策としてサイバー保険への加入提案を受けた。

#### 【問題点】

- ・ 情報漏えい保険では、情報漏えい以外の被害は補償されない場合がある。このためフォレンジック等の調査費用を工面するのに時間を要し、その間に被害が拡大する懸念がある。
- ・ サイバー攻撃によって事業が中断した場合の喪失利益については、情報漏えい保険では補償されない。

#### 【サイバー保険加入のメリット】

- ・ サイバー保険の多くは、情報漏えいに加えて、Web改ざんやDDoS攻撃などの各種**サイバー攻撃による被害やフォレンジック等の漏えい確定に必要となる調査費用も補償対象**としている。
- ・ 第三者への損害賠償や自社に発生した各種費用だけでなく、**サイバー攻撃による生産停止で事業が中断した場合の損害賠償等も補償される。**

セキュリティ部門長は上記を踏まえた上で、サイバー保険への加入を検討することとした。

### 得られた知見



セキュリティ部門長は「サイバー攻撃を受けてしまった場合は、速やかに被害を極小化することが大切。それは**時間との勝負**」と考えて検討を進めた。保険加入により調査費用工面の社内稟議が不要となり、スムーズな専門調査会社への発注で**調査着手までを迅速化**できることが最大のメリット、とも語った。

以下に参考までに日本でのサイバー保険の補償内容の主な例を示す。

#### 日本で取り扱われているサイバー保険の補償内容の主な例<sup>24,25</sup>

- ・ 損害賠償責任（損害賠償金、争訟費用等）
- ・ 危機管理対応（事故調査・被害拡大防止の費用、データ復元費用等）
- ・ 情報漏えい対応（見舞金・見舞品費用、社告のための費用、行政対応費用等）
- ・ 事業中断対応（事業中断に伴う喪失利益、営業継続費用等）

24 IPA「米国におけるサイバー保険の現状」p.10 図表 6：日本で取り扱われているサイバー保険の概要  
<https://www.ipa.go.jp/files/000062714.pdf>

25 一般社団法人日本損害保険協会「脅威を増すサイバー攻撃に備えるサイバー保険」  
<http://www.sonpo.or.jp/cyber-hoken/>

# 悩み (4)

## IoT機器が「シャドーIT」化している

K社では、既に製造部門がIoT機器を一部業務に活用しており、今後も積極的な活用を検討している。しかし、IoT機器導入に際しての明確なセキュリティ検討体制がない点が、内部監査で指摘された。

### 基本情報

#### K社の状況

- ✓ 製品製造ラインの一部にIoT機器を導入している。
- ✓ 通常、製造部門がシステムを導入する際には、情報システム部門が関与するルールである。
- ✓ 製造部門で製造に使用する制御システムは通常外部ネットワークに接続しない。

#### K社のプロフィール

業種	製造業	
規模	1000人	
管理体制	CISOの有無	有 (CIOが兼任)
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	情報システム部門

### セキュリティ担当者の問題・悩み



K社では、ITを業務に利活用し、より効率的に業務を図るべく、製造部門が主導となり、一部業務にIoT機器が導入されている。

しかし、内部監査において、**IoT機器の導入に際して、情報システム部門が十分に関与できていないことが問題として指摘された。**

製造部門が使用する制御システムは、外部ネットワークとは切り離されているため、IoT機器もこれまでの制御システムと同様に導入していた。そのため、**外部ネットワークとの接続を考慮したセキュリティ要件の検討が漏れている可能性があることが発覚した。**



## 取組み (4) 製造部門とIT部門が連携し、不正接続機器や不適切な設定を排除する

### 解決に向けたアプローチ

内部監査での指摘を踏まえ、K社は以下の対応を行った。

- IoT機器導入も、通常システム導入と同様に情報システム部門が関与するようルールを修正した。
- 製造部門と情報システム部門を巻き込んだIoTビジネス検討部会を設置した。



- IoT機器も含めて社内ネットワーク上に不正に機器が接続された場合に検知可能な製品を導入した。
- 既に導入したIoT機器について、利用者側で考慮すべきセキュリティ上の考慮漏れがないか、公知の情報<sup>26</sup>を参考に再度見直しを行った。
- なお、上記の見直しの結果、IoT機器の管理者用IDのパスワードが初期設定のままとなっている事が発覚したが、幸いにもサイバー攻撃の踏み台にされる等の事故は未然に防ぐことができた。

### 得られた知見



K社の情報システム部長は、IoT活用は自社が今後もビジネスで優位性を保つためには必須であると考えている。

一方で、IoT機器を導入することにより、これまでの“情報漏えいリスク”だけではなく、機器停止や誤作動等による“業務停止のリスク”や、最悪の場合には“人命に関わるリスク”を招きうる。

可用性や物理的な安全性も十分に考慮するためには、これまでと異なるアプローチや体制が必要だと考えている。

はじめに

第1章

第2章

第3章  
担当者の悩みと取組みのプラクティス

付録

26 例えば以下などが活用可能である

IoT推進コンソーシアム、総務省、経済産業省『IoTセキュリティガイドライン ver 1.0』

[http://www.soumu.go.jp/main\\_content/000428393.pdf](http://www.soumu.go.jp/main_content/000428393.pdf)

IPA『IoT開発におけるセキュリティ設計の手引き』<https://www.ipa.go.jp/files/000052459.pdf>

IPA『つながる世界の開発指針（第2版）』<https://www.ipa.go.jp/files/000060387.pdf>

## 悩み (5)

# 自前でのシステム運用の負担が大きく、 セキュリティ対策に不安を感じる

L社では、自社内で基幹システムを構築・運用しているが、システムの維持費用や、人的資源の不足に伴う、セキュリティ対策を始めとする運用・保守対応の負荷が高く、限界を感じていた。

### 基本情報

#### L社の状況

- ✓ 自社製品を、取引先に販売するシステム（基幹システム）を、オンプレミス形式で、自社内にて構築・運用している。
- ✓ IT部門に十分に担当者がおらず、特にセキュリティ担当者が十分にいない。

#### L社のプロフィール

業種	製造業	
規模	300人	
管理体制	CISOの有無	有 (CIOが兼任)
	専任のセキュリティ部署	無
	サイバーセキュリティの 主管部署	IT部門

### セキュリティ担当者の問題・悩み



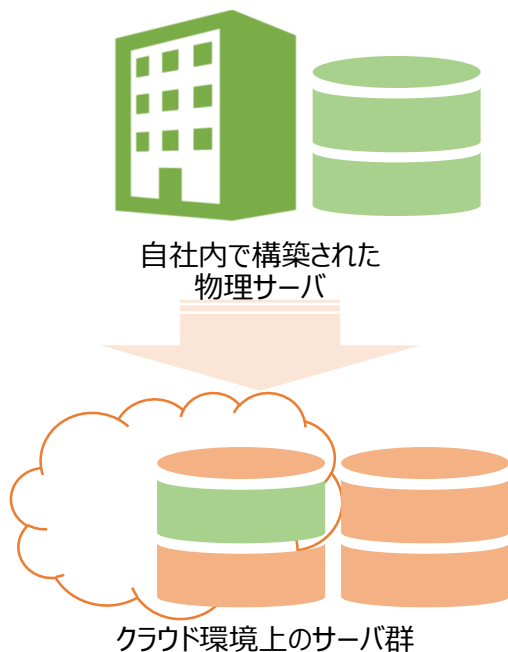
L社では自社で基幹システムを構築・運用している。しかし、日頃から**費用面の負担**だけではなく、IT部門の要員システムの調達、運用、保守にかけられる**人的資源が不足しており作業負担**が高くなっていった。

特に**セキュリティ対策**に関しては、サーバのマルウェア対策、OSのアップデート、セキュリティパッチの適用といった予防的な対策、またネットワークの監視、アクセスログのモニタリング等の発見的な対策など、種々の対策を講じているが、これらが**少ないセキュリティ担当者に対する大きな負荷**となっていた。

## 取組み (5) 自社のセキュリティルールに整合する、適切なクラウドサービスを利用する

### 解決に向けたアプローチ

#### オンプレミス環境からクラウド環境への移行 (イメージ)



そこでL社は、基幹システムのサーバが保守切れを迎えるタイミングで、従来のようにサーバを自社で保有してセキュリティ対策を実施するのではなく、一部のセキュリティ対策がサービスとして提供される**クラウドサービスに移行**することとした。

その際に、公知の情報<sup>27</sup>等を参考にしながら、例えば以下のようなポイントを検討した上で、自社で行うべき管理の内容を整理し、管理の簡素化や管理工数の削減を図った。

#### <移行時の考慮ポイントの例>

- クラウドで扱う情報と業務の重要性
- 自社・事業者間でのセキュリティルール・水準の整合性（データ暗号化やパスワード強度の警告など）
- セキュリティ対策の開示状況
- 直接監査の実施可能性、もしくは、代替可能なSOC報告書<sup>28</sup>の発行 等

### 得られた知見



L社のIT部門長は、システムの専門家であるクラウドベンダーが、セキュリティ対策も含めてサーバの維持を行ってくれるため負担は以前より軽減されたと感じる。

一方で、クラウド環境に移行した場合でも、全てベンダー任せにするのではなく、**自社で担保しなければならない部分**、例えば、ID管理やデータ暗号化やパスワード強度確認などのセキュリティ設定はしっかり対応し、**委託先の選定・モニタリングも重要**であると考えている。

はじめに

第1章

第2章

担当者の悩みと取組みのプラクティス 第3章

付録

27 例えば以下などが活用可能である

IPA「クラウドサービス安全利用のすすめ」 <https://www.ipa.go.jp/files/000011594.pdf>

28 クラウドサービスプロバイダが受託業務に係る内部統制の保証報告書（SOC報告書）を作成している場合がある。

## 悩み (6)

# 全国各地の拠点における セキュリティ管理状況に不安がある

M社では、全国各地の営業所のセキュリティ管理状況の把握、情報連携のため、全社的なセキュリティ委員会を設置しているが、各拠点のセキュリティ管理の実態については把握できていない状況であった。

### 基本情報

#### M社の状況

- ✓ 全国各地に営業所を構え、各拠点で機密性の高い情報を保有している。
- ✓ 全社セキュリティ委員会を設置し、各拠点のセキュリティ責任者・担当者と逐次情報連携を行っている。
- ✓ 本社にて各拠点でのサイバーセキュリティ管理状況の実態を正しく把握できているか自信がない。

#### M社のプロフィール

業種	製造業	
規模	2,000人	
管理体制	CISOの有無	有 (IT担当取締役が兼任)
	専任のセキュリティ部署	有
	サイバーセキュリティの主管部署	サイバーセキュリティ部門

### セキュリティ担当者の問題・悩み



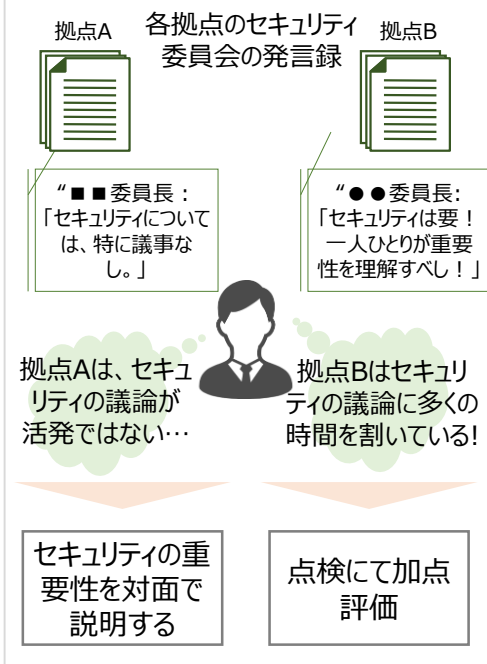
M社では、遠隔地拠点においても、適切にセキュリティ管理を行うため、各拠点にセキュリティ責任者・担当者を配置し、**全社的なセキュリティ委員会を設置の上、逐次情報連携**を行っている。

- **遠隔地等の目の届きづらい拠点のサイバーセキュリティ管理の状況が、本社からは把握しづらく、管理状況に不安を感じている。**
- 全社セキュリティ委員会にて**年次**で各拠点のセキュリティ対策状況の**点検**を実施しているが、**点検項目だけでは実態が掴みづらい。**

# 取組み (6) 拠点におけるセキュリティの取組みを把握し、対面で対話する

## 解決に向けたアプローチ

### 取組みのイメージ



そこでM社は、各拠点での**セキュリティに対する取組み状況や取組みの姿勢を把握**するため、全社的なセキュリティ委員会を構成するサイバーセキュリティ部門のメンバーが、以下のような取組みを行っている。

- 各拠点の**セキュリティ委員会の発言録**などから、拠点の責任者が「どの程度セキュリティに対して積極的に取り組んでいるか」「従業員に**セキュリティの重要性を説明しているか**」を読み解き、年次の点検の評価材料としている。
- セキュリティ委員会メンバーは、「セキュリティに対する理解度が不十分」と感じられる拠点の責任者には、**各拠点の責任者等と対面で対話**し、セキュリティの重要性を説明している。

## 得られた知見



M社のCISOは、従業員のセキュリティに対する意識を変化させることは一朝一夕には難しい点もあるが、CISO自身がセキュリティを推進するための**強いリーダーシップ**を発揮し、各部門のリーダーの協力のもと、**従業員一人ひとりにセキュリティを推進するためのメッセージを伝え続ける**ことが重要であると考えている。

そのためにも、**事業部門とも連携してセキュリティに関する体制を構築**することがポイントであると考えている。

はじめに

第1章

第2章

第3章  
担当者の悩みと取組みのプラクティス

付録

## 悩み (7)

# 外部サービスの選定でIT部門だけでは 対応が困難である

N社では、クラウド等の外部サービスを利用する際はチェックシートの運用を実施している。事業部門がチェックシートだけで利用可否を判断できず、システム部門への個別相談するケースが多くなり、システム部門は対応に苦慮していた。

### 基本情報

#### N社の状況

- ✓ 各事業部門から、外部のクラウドサービスを利用要請が増えたことを背景に、システム部門がクラウドサービス利用に際してのチェックシートを策定している。
- ✓ 外部のクラウド利用に際するチェックシートを設け、NG項目があれば非推奨としている。
- ✓ チェック項目はサービスやセキュリティの機能確認が主である。

#### N社のプロフィール

業種	製造業	
規模	4,000人	
管理体制	CISOの有無	有 (CIOと兼任)
	専任のセキュリティ部署	有
	サイバーセキュリティの 主管部署	システム部門

### セキュリティ担当者の問題・悩み



N社では、**要求を満たさないチェック項目があるサービスは、「非推奨」と位置づけ**、リスクをとってでも利用したい場合は、**事業部門長の承認を得させる仕組み**となっている。

しかしながら、**責任範囲や免責事項など利用規約に関するチェックはできておらず**、事業部門から個別に相談を受けた場合に**システム部門では規約の解釈や判断に苦慮することが増えてきた**。

## 取組み (7) 社内の関連部門と連携して 外部サービスの選定を行う

### 解決に向けたアプローチ

#### システム部門・法務部門の 早めの確認によるメリット



システム部門

- ✓ サービス事業者の信頼性・セキュリティ管理体制の確認
- ✓ サービス自体のセキュリティ対策の確認 等



法務部門

- ✓ 利用契約の精査
- ✓ サービス事業者との責任範囲の確認 等

外部サービス利用の検討段階から関与することで、ベンダー選定の判断がより適切になる

そこでN社のCISOは、外部サービス選定の判断に、**システム部門だけでなく法務部門にも参画してもらうことにした。**

当初はシステム部門で判断が難しい場合に適宜法務部門へ問い合わせていたが、問い合わせ件数の増加を踏まえ、定例会を開催することにした。

また、法務部門と協力しながら、チェックシートへ法務的な確認事項も追加し、事業部門で包括的な観点から確認ができるようにした。

### 得られた知見



N社のCISOは、クラウドサービス等の場合であっても、外部委託と同様、サービス選定に際しては、**サイバーセキュリティリスクの管理部門のみならず、法務部門等、複数の部門の関与が必要不可欠**であると考えている。

これまでは、システム部門・法務部門が定期的に連携することがなかったため、用語の使い方や認識の齟齬が発生することもあったが、次第に**互いに同じ方向で議論でき、建設的なコミュニケーション**ができるようになってきていると感じている。

はじめに

第1章

第2章

第3章  
担当者の悩みと取組みのプラクティス

付録

## 悩み (8) IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている

〇社は役員も対象に全従業員向けのセキュリティ教育を実施している。しかしながら、年1回の標的型メール訓練では経営層のメール開封率が他の従業員と比較して高い傾向にあった。

### 基本情報

#### 〇社の状況

- ✓ 役員を含めて、全社員向けのセキュリティ教育を設計、運営している。
- ✓ セキュリティ教育や訓練の結果を部署ごとに分析している。
- ✓ 経営層に対するセキュリティ教育はどのような内容を行えばよいかわからない。

#### 〇社のプロフィール

業種	製造業	
規模	6,000人	
管理体制	CISOの有無	有 (CIOと兼務)
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

### セキュリティ担当者の問題・悩み



〇社では、製造部門でIoTの利用が進んでいる等、経営としてセキュリティに取り組む必要性とともに以下のような悩みを持っていた。

- 経営層はセキュリティリスクを認識してはいるが、ITリテラシーが十分でない
- 経営層もサイバーセキュリティのトレンド等を理解していなければ、適切な経営判断が下せない

一方、部下の立場から経営層に研修を実施することに否定的な意見もあり、経営層のためのセキュリティ教育の実施について悩んでいた。



## 取組み (8) 外部講師による 経営層向けの研修会を実施する

### 解決に向けたアプローチ

#### 主な研修内容 (イメージ)

H社向け研修資料

①サイバー攻撃のトレンド

②ITのトレンド

③組織的なセキュリティ対策  
のポイント

④技術的なセキュリティ対策  
のポイント

そこでO社のCISOであるIT部門の部長は、セキュリティ研修を提供する外部機関に相談の上、研修の必要性や役員が受講したい内容を確認するために役員に対してアンケートを実施し、役員向け研修を企画・開催した。

#### 【役員向け研修の概要】

**対象：**ITやセキュリティ投資に係る役員

**時期：**年1回の定期開催（※但し、サイバー攻撃やITの  
トレンドが変化した場合は適宜開催）

**内容：**都度、検討するものの、初回は左記の内容とした

ビジネス誌等で見聞きする内容について外部講師に質問できたり、**事業部間でリスク認識を共有**できたり、と研修を受講した役員からの評判も上々であり、今後は年1回定期的に開催することが決まった。

部長は、外部講師の指摘に関連する社内の対策状況を定量的に報告するようにした。さらに、経営会議では経団連やNISCなど外部のセミナーや研修があれば紹介するようにした。

### 得られた知見



O社のCISOであるIT部門の部長は、経営層向けのセキュリティ研修実施の効果を「セキュリティに興味を持った結果として経営層が外部のセミナー等にも参加するようになった」ことにあると考えている。

まずは自社内の役員間においてリスク認識が共有されたことに加え、外部セミナー等に参加すると、他社の役員ともリスクや対策に関する情報共有が行われ、セキュリティ投資に関する理解が得られやすくなったと感じている。

はじめに

第1章

第2章

担当者の悩みと取組みのプラクティス 第3章

付録

## 悩み (9)

# 従業員に対してセキュリティ教育を実施しているが効果が感じられない

P社では全従業員を対象にセキュリティ意識を向上させるため、セキュリティ教育を定期的  
実施しているが、効果を感じられない状況であった。

### 基本情報

#### P社の状況

- ✓ 従業員向けに定期的なセキュリティ教育を行っている。
- ✓ PC紛失等のセキュリティインシデントの件数は減少していない。

#### P社のプロフィール

業種	流通業	
規模	5,000人	
管理体制	CISOの有無	有 (CIOと兼務)
	専任のセキュリティ部署	無
	サイバーセキュリティの 主管部署	IT部門

### セキュリティ担当者の問題・悩み



P社のCISOは全従業員を対象に下記のようなセキュリティ教育を実施している。

- E-learning(他社よりコンテンツ購入)
- 社内掲示板を通じた適宜の注意喚起  
(PC紛失やビジネスメール詐欺への注意等)
- 年2回の標的型攻撃メール訓練

教育の効果については、情報セキュリティを担当する  
コンプライアンス部門、サイバーセキュリティを担当するIT部門ともに  
一定程度認めているものの、PCの紛失等のセキュリティインシデント  
が無くなる状況に問題を感じていた。

## 取組み (9) 特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する

### 解決に向けたアプローチ

#### フォローアップの流れ

セキュリティテスト・  
メール訓練の実施



社内の弱点の  
分析



強化施策の検討



追加的な教育の  
実施

そこでP社のCISOは、実施したセキュリティ教育の結果を分析し、部署ごとの理解度や苦手分野を特定した。

その上で特定の部署や役職、年齢層に対して追加的な教育を実施するフォローアップの仕組みを企画した。

#### 【フォローアップの概要】

**対象：**特定の部署、役職、また年齢層

**内容：**独自作成(インターネットや書籍から関連するコンテンツを引用)

**試行：**セキュリティを担当するコンプライアンス部門、IT部門といった管理部門で試行し、内容の改善を図った後に全社展開

### 得られた知見



P社のCISOは、取組みのポイントとして、試行プロセスの重要性を挙げた。追加的なセキュリティ教育の実施は現場にとっては負荷となるため、**中途半端な施策では逆効果となるリスク**があると判断した。

また、フォローアップの効果として、SNSを通じた情報発信における注意事項の理解など、直接的に効果を感じられたものに加え、**試行した管理部門のセキュリティ意識の向上が見られた点**を効果として感じている。

はじめに

第1章

第2章

第3章  
担当者の悩みと取組みのプラクティス

付録

## 悩み (10)

# スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない

Q社では、自社のECサイトでの売上比率が高まっていることもあり、新技術を持つスタートアップ企業R社との取引に関する要望が拡大していた。しかし、セキュリティの観点からR社との取引に不安を感じていた。

### 基本情報

#### Q社の状況

- ✓ 事業部門からIT部門への開発要望をもとに、外部へ業務委託を行っている。
- ✓ AI(人口知能)やVR(仮想現実)を活用した新規ビジネスを検討している。
- ✓ サプライチェーンのビジネスパートナーには、定期的にサイバーセキュリティの取組み状況をチェックシートで確認している。

#### Q社のプロフィール

業種	小売業	
規模	3,000人	
管理体制	CISOの有無	無
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

### セキュリティ担当者の問題・悩み



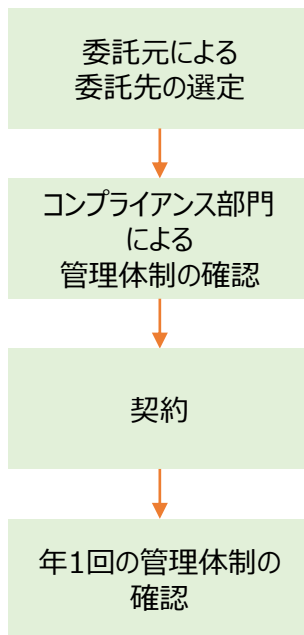
Q社のIT部門としては、新規ビジネスで活用する**顧客の身体的特徴**といった機微性の高い個人情報の取り扱いに際し、R社には**管理体制が未熟な点**があった。さらに、**チェックシートで確認した結果からも、R社との取引が推奨できない状況**であった。

また、R社は即座に管理体制を充実させることは現実的でなく、IT部門の頭を悩ませていた。

## 取組み(10) セキュリティ対策の取組み、 セキュリティ認証の取得状況を確認する

### 解決に向けたアプローチ

#### 委託先選定の流れ



事業部門からの強い要望もあり、Q社のIT部長は、管理体制に懸念のあるスタートアップ企業R社との取引を許容した。ただし、これまでサプライチェーンのビジネスパートナーにはチェックシートの状態を年1回確認していただけであったが、管理体制の整備状況など不明点があれば、R社の事務所等の現場へ直接出向いて確認したいという意向を伝えた。

さらに、R社の営業部長に対して、**セキュリティ管理体制の整備の取組み例として、契約後も継続的にプライバシーマーク等のセキュリティ認証を取得することを奨励した。**

はじめは、R社も認証取得はコストが掛かることを理由に消極的であった。しかし、IT部長はプライバシーマークの取得を通じた管理体制の整備がQ社との取引だけでなく、今後のビジネス拡大に必要なことを話し、R社はプライバシーマークの取得を検討し始めた。

### 得られた知見



Q社の取組みのポイントは、委託先のセキュリティ体制の担保を、短期的な視点と長期的な視点を並行して考慮したことである。短期的な視点ではチェックシートでの確認に加え、若干コストはかかるが**現地調査の実施を**、長期的な視点では第三者による認証を、**自社が求めるセキュリティ対策レベルの確認手段として活用した。**

委託元から管理体制の充実を依頼することは簡単であるが、委託先による不正もリスクとしてある中、健全な取引関係が最も望まれる。

はじめに


第1章

第2章

担当者の悩みと取組みのプラクティス

第3章

付録



## 付録 サイバーセキュリティに関する用語集 サイバーセキュリティ対策の参考情報

サイバーセキュリティ対策をこれから実践するCISO等、セキュリティ担当者や人材育成・支援担当者が実務で活用できるサイバーセキュリティに関する用語集、参考資料集を示す。

# 付録

## サイバーセキュリティに関する用語集(1/6)

### 【サイバーセキュリティ管理全般】

用語	意味
サイバーセキュリティ	サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすること。
サイバーセキュリティリスク	サイバーセキュリティに関連した不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと
サイバー攻撃	コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと
CISO	(Chief Information Security Officer) 経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のこと
CSIRT	(Computer Security Incident Response Team) インシデントの発生に対応するための体制のこと
SOC	(Security Operation Center) ネットワーク上の通信や特定の機器のログ等を監視し、予兆を含むサイバー攻撃の検知、また分析、対策のアドバイスをを行う組織のこと
セキュリティポリシー	企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したものの。セキュリティポリシーに沿って、組織内セキュリティ対策が規定される
多層防御	物理層、ネットワーク層からデータ層までの多層防御を導入することで、1つの機器やソフトウェアに依存する拠点防御対策や、単一の境界防御層（主としてネットワーク境界）に依存する対策の場合より、未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される
入口対策(例)	ネットワークへの不正侵入を防ぎ、マルウェア等に感染しないための対策
内部対策(例)	不正侵入があった場合にも重要な情報へのアクセスを防ぐための、侵入を前提として感染拡大を防止するための対策
出口対策(例)	マルウェアが外部へ通信しようとするのを遮断し、感染後の被害を最小限に食い止め、マルウェアに感染しても情報を盗まれないための対策

はじめに

第1章

第2章

第3章

付録

# 付録

## サイバーセキュリティに関する用語集(2/6)

### 【サイバーインシデント対応】

用語	意味
インシデント	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生した事象のこと ▶ サイバー攻撃による不正アクセスやマルウェアの侵入などセキュリティに影響を及ぼすあらゆる事故のことを指す
インシデントレスポンス	インシデントの発生に際して、それを検知し、関係組織と連絡をとり、被害の拡大を防ぐと共に、再発を防止するための原因究明と改善を行う、一連の組織的活動
トリアージ	インシデント対応の優先順位付け ▶ 判断基準に基づきCSIRTが対応すべきインシデントか否かを判断
ログ	コンピュータの利用状況やデータの通信記録。操作を行った者のIDや操作日付、操作内容などが記録される。セキュリティ上、インシデントの原因追究などに利用する
フォレンジック	不正アクセスや情報漏えいなどのトラブル発生時に、原因究明や捜査に必要なデータなどを収集・分析する方法、またはその技術のこと
コンティンジェンシープラン	災害等の緊急事態が発生することを想定し、その被害や損失を最小化するために、定めた対応策や行動計画

### 【開発・設計】

用語	意味
セキュリティバイデザイン	セキュリティを企画・設計段階から確保するための方策のこと
セキュアSDLC	(Secure System Development Life Cycle) 開発プロセス全体でセキュリティ対策を実施する考え方のこと



# 付録

## サイバーセキュリティに関する用語集(3/6)

### 【脆弱性対策】

用語	意味
脆弱性 / セキュリティホール	OSやソフトウェアに設計上のミスやプログラムの不具合がある場合に発生する欠陥のこと ▶ ソフトウェアの動作を妨げる欠陥のことをバグというが、脆弱性は開発者やユーザが意図しない動作をする欠陥のことを指す
CVE	(Common Vulnerabilities and Exposures) 複数の組織から発表される脆弱性情報に共通の識別番号を与えるプロジェクトのこと ▶ 米国の非営利団体MITREが採番しており、脆弱性の識別子として国際的に利用されている
CVE番号	個々の脆弱性に割り当てられる固有の識別番号： CVE-登録時の西暦-4桁以上の通番
CVSS / 共通脆弱性評価システム	(Common Vulnerability Scoring System) 情報システムの脆弱性の評価手法 ▶ 攻撃条件の複雑さや攻撃可能性などを総合的に判断し、脆弱性の特性を同一基準を用いて1～10で数値化する
JVN	(Japan Vulnerability Note) JPCERT/CCとIPAが共同で運営する脆弱性対策情報サイト
セキュリティパッチ	ソフトウェアの不具合が見つかった場合に配布される、不具合部分を修正するプログラム

はじめに

第1章

第2章

第3章

付録

# 付録

## サイバーセキュリティに関する用語集(4/6)

### 【サイバー攻撃手口】

用語	意味
標的型攻撃	特定の組織の重要情報の取得等を目的に行われるサイバー攻撃の手法。ばらまき型のメール攻撃と異なり、執拗に対象組織に対して攻撃を繰り返す特徴がある。
標的型メール	攻撃者が悪意のあるファイルを添付したり、悪意のあるサイトに誘導するためのURLリンクを貼り付けたメールを送信し、マルウェアに感染させようとする攻撃手法
水飲み場型攻撃	Webサイトにマルウェア等を仕込み、訪問者をマルウェアに感染させる攻撃手法
DDoS攻撃	(Distributed Denial of Service Attack) 攻撃対象としたネットワークやシステムに大量のデータを送り込む等の方法で対象のネットワークやシステムに負荷をかけ、サービスを提供できない状態にする攻撃手法
ゼロデイ攻撃	セキュリティホールが発見されてから実際にパッチ（セキュリティホールを塞ぐための修正プログラム）が提供されるまでの間の時間差を利用した攻撃手法
SQLインジェクション	Webアプリケーションと連携するデータベースに対する攻撃手法 <ul style="list-style-type: none"> <li>➤ ブラウザを介してWebアプリケーションに不正なSQL文を入力することで、動作不良を起こさせ、データベースを不正に操作したり個人情報などを詐取する</li> </ul>
クロスサイトスクリプティング	Webアプリケーションの脆弱性を狙った攻撃手法 <ul style="list-style-type: none"> <li>➤ 攻撃者が作成した悪意あるスクリプトを標的のWebサイトのWebアプリケーションに送り込み、意図しない処理を実行させる</li> </ul>

# 付録

## サイバーセキュリティに関する用語集(5/6)

### 【サイバー攻撃方法】

用語	意味
ポートスキャン	<p>ネット機器やシステムに信号を送り、接続可能なポートを探り当てる行為</p> <p>➤ 標的サイトの各サービス(ポート)の状況調査が攻撃・侵入の前段階に行われる</p>
ポート	システムや周辺機器が外部とデータを通信する際に利用する出入り口のこと
ポート番号	ネットワークのサービスごとに割り振った番号のことで、プロトコルにより使用するポート番号が決まっており、この番号をもとに通信元と通信先サービス送受信が行われる
バックドア	攻撃者がネットワークやサーバに侵入できるように作成される裏口のこと
マルウェア	セキュリティ上の被害を及ぼすウイルス、スパイウェア、ポットなどの悪意をもったプログラムを指す総称。これらのプログラムは、使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピュータに入り込み悪意ある行為を行う
C2サーバ / C&Cサーバ / 制御サーバ	<p>(Command &amp; Control)</p> <p>マルウェア等に感染したシステム等に対し、遠隔から不正なコマンドを送信するために利用されるサーバのこと</p>
ダークネット	PCやIoT機器などといったエンドポイントに割り当てられていない未使用のIPアドレス群

はじめに

第1章

第2章

第3章

付録

# 付録

## サイバーセキュリティに関する用語集(6/6)

### 【セキュリティ対策】

用語	意味
ファイアウォール	ネットワークの通信において、その通信がルールにマッチするか否かを判断し許可(通過)するか、または拒否する仕組み
WAF	(Web Application Firewall) 脆弱性を突いた攻撃から、Webアプリケーションを守るためのファイアウォール <ul style="list-style-type: none"> <li>・ブラックリスト方式：異常な通信パターン定義し、一致する通信をブロック</li> <li>・ホワイトリスト方式：正常な通信パターンを定義し、正常な通信以外は不正な通信としてブロック</li> </ul>
DMZ	(Demilitarized Zone) 外部ネットワークと社内ネットワークの間に作られるネットワーク <ul style="list-style-type: none"> <li>➢ DMZ内にサーバを設置するなどによってセキュリティ強化を図ることが可能</li> </ul>
VDI	(Virtual Desktop Infrastructure) 通常はパソコンで行っている処理をサーバ上の仮想化されたパソコンで実行する仕組み <ul style="list-style-type: none"> <li>➢ 利用者の手元の端末にはその画面だけを転送するため、マルウェア感染等のリスクが軽減される</li> </ul>
EDR	(Endpoint Detection and Response) 感染した端末の検知・調査・隔離する用途で導入されるマルウェア対策製品のこと
脆弱性診断 / セキュリティ診断	システムやネットワークを調査し、システム上の脆弱性などのセキュリティリスクを洗い出すこと
ペネトレーションテスト / 侵入テスト	ネットワークの外部もしくは内部からネットワークに侵入を試みるテスト <ul style="list-style-type: none"> <li>➢ 実際の侵入に使われる技術を利用し、疑似的なサイバー攻撃を行いシステムに脆弱性がないかどうかを調査する</li> </ul>

# 付録

## サイバーセキュリティ対策の参考情報(1/2)

資料名	対象読者	発行元	URL
<b>サイバーセキュリティ対策全般</b>			
サイバーセキュリティ経営ガイドライン Ver2.0	経営者、CISO等、セキュリティ担当者	経済産業省/IPA	<a href="http://www.meti.go.jp/policy/netsecurity/mng_guide.html">http://www.meti.go.jp/policy/netsecurity/mng_guide.html</a>
サイバーセキュリティ経営ガイドライン 解説書	経営者、CISO等、セキュリティ担当者	経済産業省/IPA	<a href="https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html">https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html</a>
情報セキュリティ10大脅威 2019	経営者、CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/vuln/10threats2019.html">https://www.ipa.go.jp/security/vuln/10threats2019.html</a>
<b>サイバーセキュリティリスクの管理体制構築(指示1、2、3)</b>			
中小企業の情報セキュリティ対策ガイドライン 第3版	経営者、CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html">https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html</a>
情報セキュリティ管理基準	CISO等、セキュリティ担当者	経済産業省	<a href="http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000008.html">http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000008.html</a>
別冊 CISO 等セキュリティ推進者の経営・事業に関する役割プラクティス	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000067656.pdf">https://www.ipa.go.jp/files/000067656.pdf</a>
セキュリティ対応組織(SOC/CSIRT)の教科書	CISO等、セキュリティ担当者	日本セキュリティオペレーション事業者協議会	<a href="https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html">https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html</a>
ユーザ企業のためのセキュリティ統括室構築・運用キット(統括室キット)	CISO等、セキュリティ担当者	産業横断サイバーセキュリティ人材育成検討会	<a href="https://cyber-risk.or.jp/cric-csf/report/Security-Supervisor_Toolkit_Part1_v1.0.pdf">https://cyber-risk.or.jp/cric-csf/report/Security-Supervisor_Toolkit_Part1_v1.0.pdf</a>
セキュリティ知識分野 (Sec Bok) 人材スキルマップ2017年版	CISO等、セキュリティ担当者	日本ネットワークセキュリティ協会	<a href="https://www.jnsa.org/result/2017/skillmap/">https://www.jnsa.org/result/2017/skillmap/</a>
<b>サイバーセキュリティリスクの特定と対策の実装(指示4、5、6)</b>			
サイバー・フィジカル・セキュリティ対策フレームワーク (案)	CISO等、セキュリティ担当者	経済産業省	<a href="http://www.meti.go.jp/press/2018/01/20190109001/20190109001-2.pdf">http://www.meti.go.jp/press/2018/01/20190109001/20190109001-2.pdf</a>
SP 800-30 [rev.1] リスクアセスメントの実施の手引き	CISO等、セキュリティ担当者	NIST	<a href="https://www.ipa.go.jp/files/000025325.pdf">https://www.ipa.go.jp/files/000025325.pdf</a>
『高度標的型攻撃』対策に向けたシステム設計ガイド	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000046236.pdf">https://www.ipa.go.jp/files/000046236.pdf</a>
【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	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html">https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html</a>
日常における情報セキュリティ対策	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/asures/ev eryday.html">https://www.ipa.go.jp/security/asures/ev eryday.html</a>
IoTセキュリティガイドライン ver 1.0	CISO等、セキュリティ担当者	IoT推進コンソーシアム、総務省、経済産業省	<a href="http://www.soumu.go.jp/main_content/000428393.pdf">http://www.soumu.go.jp/main_content/000428393.pdf</a>
IoT開発におけるセキュリティ設計の手引き	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000052459.pdf">https://www.ipa.go.jp/files/000052459.pdf</a>
つながる世界の開発指針(第2版)	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000060387.pdf">https://www.ipa.go.jp/files/000060387.pdf</a>
情報セキュリティ対策ベンチマーク	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/benchmark/index.html">https://www.ipa.go.jp/security/benchmark/index.html</a>

はじめに

第1章

第2章

第3章

付録

# 付録

## サイバーセキュリティ対策の参考情報(2/2)

資料名	対象読者	発行元	URL
<b>インシデント発生に備えた体制構築(指示7、8)</b>			
サイバーセキュリティ経営ガイドライン 付録C インシデント発生時に組織内で整理しておくべき事項	セキュリティ担当者	経済産業省/IPA	<a href="https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx">https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx</a>
組織内 CSIRT の役割とその範囲	CISO等、 セキュリティ担当者	JPCERT/CC	<a href="https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt20151126.pdf">https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt20151126.pdf</a>
CSIRT人材の定義と確保(Ver.1.5)	CISO等、 セキュリティ担当者	日本コンピュータ セキュリティインシデント 対応チーム協議会	<a href="http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf">http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf</a>
インシデントハンドリングマニュアル	CISO等、 セキュリティ担当者	JPCERT/CC	<a href="https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf">https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf</a>
証拠保全ガイドライン第7版	CISO等、 セキュリティ担当者	デジタルフォレンジック 研究会	<a href="https://digitalforensic.jp/home-act-products-df-guideline-7th/">https://digitalforensic.jp/home-act-products-df-guideline-7th/</a>
情報セキュリティサービス基準適合 サービスリスト	CISO等、 セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/it-service/service_list.html">https://www.ipa.go.jp/security/it-service/service_list.html</a>
サイバーインシデント緊急対応企業一覧	CISO等、 セキュリティ担当者	JNSA	<a href="https://www.jnsa.org/emergency_response/">https://www.jnsa.org/emergency_response/</a>
IT-BCP策定モデル	CISO等、 セキュリティ担当者	NISC	<a href="https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf">https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf</a>
<b>サプライチェーンセキュリティ対策の推進(指示9)</b>			
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	CISO等、 セキュリティ担当者	経済産業省	<a href="http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf">http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf</a>
クラウドサービス安全利用のすすめ	CISO等、 セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000011594.pdf">https://www.ipa.go.jp/files/000011594.pdf</a>
ITサプライチェーンの業務委託における セキュリティインシデント及びマネジメントに 関する調査報告書	CISO等、 セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/fy29/reports/scrm/index.html">https://www.ipa.go.jp/security/fy29/reports/scrm/index.html</a>
<b>ステークホルダーを含めた関係者とのコミュニケーションの推進(指示10)</b>			
日本で使用されているソフトウェアなどの 脆弱性関連情報とその対策情報	CISO等、 セキュリティ担当者	JPCERT/CC・IPA	<a href="https://jvn.jp/report/index.html">https://jvn.jp/report/index.html</a>

**サイバーセキュリティ経営プラクティス検討会 委員**  
**(五十音順、○は委員長)**

- |         |   |
|---------|---|
| 荒川 大    | 産業横断サイバーセキュリティ人材育成検討会 事務局長                |
| 上野 耕司   | 産業横断サイバーセキュリティ人材育成検討会 第二期 会長              |
| 落合 正人   | SOMPOリスクマネジメント株式会社<br>サイバーセキュリティ事業本部 特命部長 |
| 教学 大介   | 東京海上日動火災保険株式会社<br>企業商品業務部 担当課長            |
| 小松 靖直   | 日本商工会議所 情報化推進部 部長                         |
| ○ 橋本 正洋 | 東京工業大学 環境・社会理工学院 教授                       |
| 宮下 清    | 一般社団法人 日本情報システム・ユーザー協会 常務理事               |

(オブザーバ)

経済産業省 商務情報政策局 サイバーセキュリティ課

(事務局)

独立行政法人情報処理推進機構

セキュリティンター セキュリティ対策推進部 セキュリティ分析グループ

PwCあらた有限責任監査法人 システム・プロセス・アシュアランス部



独立行政法人 情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目28番8号

文京グリーンコートセンターオフィス

TEL:03-5978-7501 FAX:03-5978-7510

URL:<https://www.ipa.go.jp>