

# 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 第3版



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.5
	想定読者と利用方法	P.6
	本プラクティス集の構成	P.7
	本プラクティス集のより良い実践のために	P.8
	本プラクティス集に関連する資料	P.9
第1章	経営とサイバーセキュリティ	P.10
	1.サイバー攻撃による企業活動への影響	P.11
	2.なぜサイバーセキュリティ対策は経営課題か	P.12
	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.13
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	P.14
	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.15
	指示2. サイバーセキュリティリスク管理体制の構築	P.19
	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.21
	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.24
	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.28
	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.36
	指示7. インシデント発生時の緊急対応体制の整備	P.43
	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.50
	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.53
	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.56
第3章	セキュリティ担当者の悩みと取組のプラクティス	P.60
	1. 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.61
	2. 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.63
	3. 海外拠点のセキュリティ意識が低い	P.65
	4. 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を感じられない	P.67
	5. IoT機器が「シャドーIT」化している	P.69
	6. 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.71
	7. 内部不正で情報漏えいが生じた場合の自社事業への深刻な影響が心配	P.73
	8. 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.75
	9. 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.77
	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.79
	11. 経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない	P.81
	12. 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.83
	13. 効果的な演習をする方法がわからない	P.85
	14. サプライチェーンの委託先企業がセキュリティ対策に協力的でない	P.87
	15. 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	P.89
	16. ランサムウェア感染による事業停止を回避したい	P.91
	17. 工場のサイバーセキュリティ対策が急務となっている	P.93
	18. テレワーク導入等の急激な環境変化に対応したセキュリティ管理規程に見直したい	P.95

目次		頁
ミニプラ ティス	1：クラウドサービスを利用する際のセキュリティ対策を強化するにはどうすればよいのか？	P.35
	2：ペネトレーションテストの補完手段として、どのような対策があるのか？	P.35
	3：従業員向けのセキュリティ研修の受講モチベーションを高めるにはどうすればよいのか？	P.35
	4：経営層に自社のセキュリティ対策状況を客観的に説明するにはどうすればよいのか？	P.42
	5：セキュリティ対策に関する自己評価の客観性を高めるにはどうすればよいのか？	P.42
付録	サイバーセキュリティに関する用語集	P.98
	サイバーセキュリティ対策の参考情報	P.104

## 本書上部の見出し欄の各項目が示す内容

### 分類

指示の解説： 重要10項目でそれぞれ何をすべきなのかの説明に相当する内容  
 プラクティス： 企業における取組の事例  
 参考情報： 取組の参考となる情報源等

### 対象読者

経営者、CISO等、セキュリティ担当者のうち、当該ページで対象としている読者を黒文字で表記

### 業種

プラクティスとして紹介している取組を実施した企業の所属する業種

### レベル

レベル1：サイバーセキュリティ対策の「はじめの一步」に相当する取組  
 レベル2：一定の対策を実施済みの企業が、対策を一步先に進めるための取組  
 レベル3：高度な取組（本プラクティス集には該当なし）

### 悩みの 分類

企業でサイバーセキュリティ対策を進める上での悩みの特徴に基づく分類

### 対応する 指示項目

「悩みと取組」に記載されているプラクティスが、重要10項目におけるどの指示に対応するものかを示す

# 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、経済産業省がデジタル環境におけるコーポレート・ガバナンス、またグループ・ガバナンスにおける指針として公表している『グループ・ガバナンス・システムに関する実務指針』<sup>1</sup>及び『デジタルガバナンス・コード』<sup>2</sup>においても、そ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ことを求める等、**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の例、取り組む際の考え方、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。

1 経済産業省：グループ・ガバナンス・システムに関する実務指針（グループガイドライン）  
[https://www.meti.go.jp/policy/economy/keiei\\_innovation/keizaihousei/corporategovernance.html](https://www.meti.go.jp/policy/economy/keiei_innovation/keizaihousei/corporategovernance.html)  
2 経済産業省：デジタルガバナンス・コード  
[https://www.meti.go.jp/policy/it\\_policy/investment/dgc/dgc.html](https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html)

# 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**の企業の実取組事例

第3章：セキュリティ担当者の**悩み毎**の企業の実取組事例

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、取り組む際の考え方、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取組のプラクティス

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り組んだ際の実践手順、内容、取り組む際の考え方、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

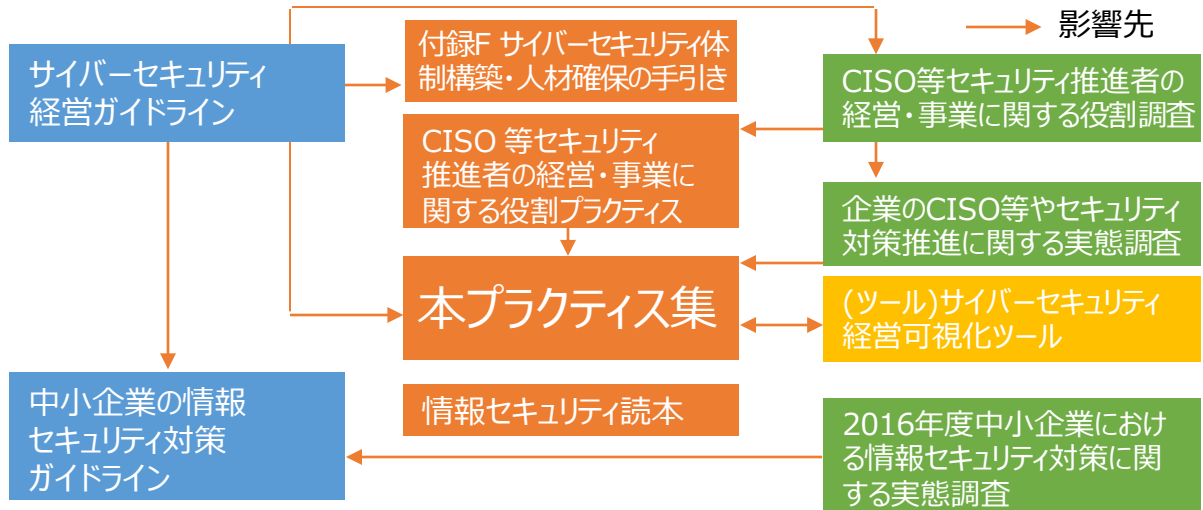
第1章

第2章

第3章

付録

# 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>
付録F サイバーセキュリティ体制構築・人材確保の手引き	2021/4/26	CISO等、セキュリティ担当者、人材育成担当者	サイバーセキュリティ対策を実施するための組織作りと従事する人材の育成のための手引き書	<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>
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>
企業のCISO等やセキュリティ対策推進に関する実態調査	2020/3/25	CISO等、セキュリティ担当者	CISO等の役割および企業のセキュリティ対策の取組状況を把握するための実態調査	<a href="https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html">https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html</a>
(ツール)サイバーセキュリティ経営可視化ツール	2021/8/17	経営者、CISO等、セキュリティ担当者	セキュリティ対策実践状況の把握や事業リスク評価等に活用するための自己診断ツール	<a href="https://www.ipa.go.jp/security/economics/hecktool/index.html">https://www.ipa.go.jp/security/economics/hecktool/index.html</a>



# 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>

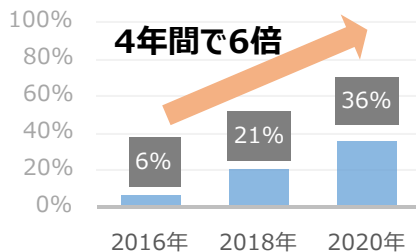


図1-1.1 日本企業が被害に遭った  
経済犯罪の内、サイバー攻撃の割合の推移

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：サイバー攻撃による決算発表の延期

大手食品メーカーでマルウェア感染によるシステム障害が発生した結果、四半期報告書の公表について2ヶ月以上の延期を余儀なくされた。

## 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。

1 PwC：経済犯罪実態調査2020 ―グローバル翻訳版・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（デジタル化の進展やニューノーマルへの対応、働き方改革の推進等）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。

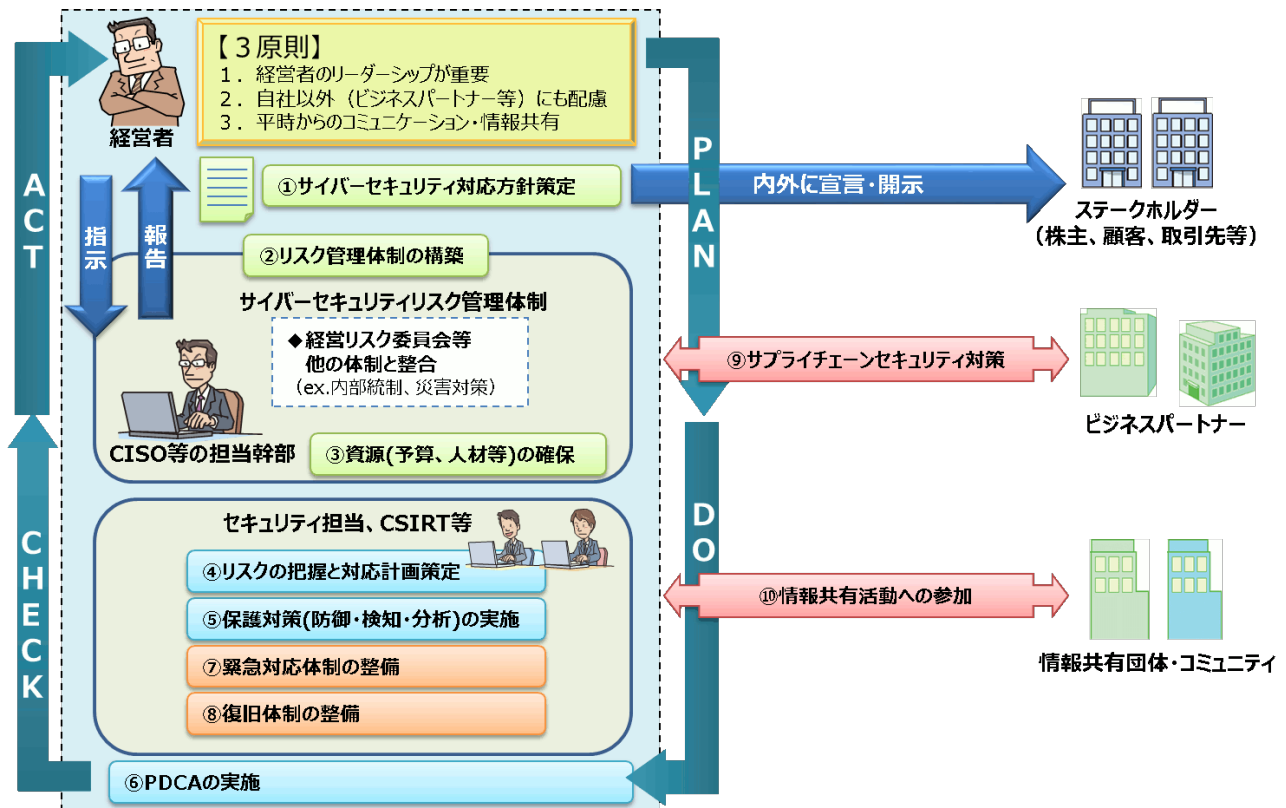


図1-3.1 経営者が認識する必要がある「3原則」および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」<sup>3</sup>

## 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、取り組む際の考え方、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.最新の脅威による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 1-3.海外拠点における情報保護に関するコンプライアンスを拠点別チェックリストで担保
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	4-1.経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応
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 5-3.セキュリティバイデザインを標準とする、クラウドベースの開発プロセスの励行
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	6-1.PDCAサイクルの検証と、演習・訓練を通じた評価・改善プロセスの強化 6-2.一律のルール適用が困難なビジネスにおけるセキュリティKPIを用いたリスク管理 6-3.ステークホルダーの信頼を高めるための、サイバーセキュリティ関連情報発信の工夫
7	インシデント発生時の緊急対応体制の整備	7-1.司令塔としてのCSIRTの設置 7-2.従業員の初動対応の規定 7-3.インシデント発生時の優先度に応じた顧客への通知・連絡・公表手順 7-4.想定されるインシデントについてのセキュリティ分析計画の事前策定
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	10-1.情報共有活動への参加による信頼獲得と、収集した知見の社内への還元 10-2.業界団体を活用した情報共有活動



## 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。

### 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
- 海外拠点における情報保護に関するコンプライアンス対応が適切に実施されているかどうかを把握できていない

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
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2-1.1 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、サーバダウンは受容する。懸念される。	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

5 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。

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/index.html>

## プラクティス 1-2

# 最新の脅威による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最新のサイバー攻撃等の脅威による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

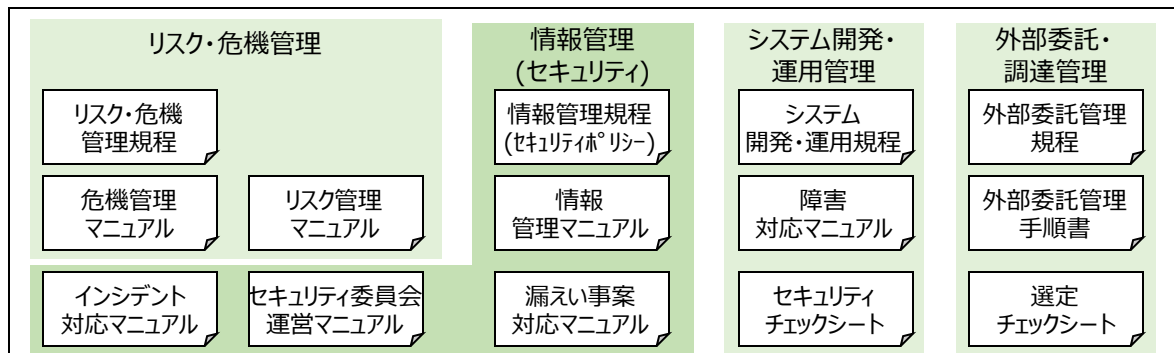


図2-1.2 B社の規程体系図の参考イメージ

## プラクティス 1-3

# 海外拠点における情報保護に関するコンプライアンスを拠点別チェックリストで担保

従業員数10,000名規模の精密機器メーカーであるC社は、北米、欧州、ASEAN地域の6カ国に12の製造拠点（現地法人）を有しているが、各国のコンプライアンス対応はこれまで各拠点任せになっており、現地での対応状況に差が生じていた。ある拠点で製品サポートを提供した顧客情報に管理不備が見つかり、意図しない漏えいの恐れがあるとのことで、現状の運用に問題があると考えた法務部門と海外事業部門からの指摘を踏まえ、危機感を抱いた経営層は本社CISOを中心に対応を指示した。

## C社の実践のステップ

CISOとサイバーセキュリティ推進部が各拠点の事情を踏まえ実践したステップは以下の3点である。

- ① 個人情報保護コンサルティング・監査サービスを提供する事業者の助言を受け、拠点立地国の個人情報やプライバシー情報の保護に関する要求事項（例：欧州GDPR）を整理した上で、現地对策を委ねることが困難な拠点を洗い出し、当該拠点毎のチェックリスト（例：個人情報を定められた場所に保存しているか、保管期限を経過した情報を削除しているか等）を作成
- ② ①のチェックリストを用いて、本社の支援のもと各拠点担当者が定期的な自己点検を実施
- ③ 情報セキュリティ対策に関する内部監査で②の遵守状況を確認し、必要に応じて是正を指示

## C社の実践内容

C社が実践した取組内容は次の通りである。

- 現地でのコンプライアンス対応に関しては、個人情報保護コンサルティング・監査サービス事業者の助言をもとに、現地法制度だけでなく、個人情報の格納場所（クラウドストレージ設置国の特定が求められる場合を含む）をチェックするなど、実務上の問題となり得ることを幅広く洗い出した。
- 拠点毎のチェックリストの作成に際しては、現地スタッフにとってわかりやすい内容となるよう、正確性を担保しつつ現地の商習慣、スタッフの役割等を考慮し各業務内容に沿った記載とした。
- 内部監査の実施に関しては、作成したチェックリストで拠点が自己点検を実施し、本社がその自己点検結果を監査することで監査要件を確保した。

表2-1.3 C社の海外拠点における情報管理上のコンプライアンス対応に関する役割分担

	対策策定フェーズ	運用フェーズ
海外拠点	● 本社がチェックリスト作成を支援（業務内容や扱う情報の説明等）	● 現地法規制等の遵守 ● チェックリストによる定期的自己点検
本社	● 外部事業者の助言を受け、拠点毎のチェックリストを作成	● 拠点での自己点検を支援 ● 内部監査を実施
外部事業者	● コンサルティングサービス提供（各国法制度に関する専門的な助言）	—

## 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D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にした。

## D社の実践のステップ

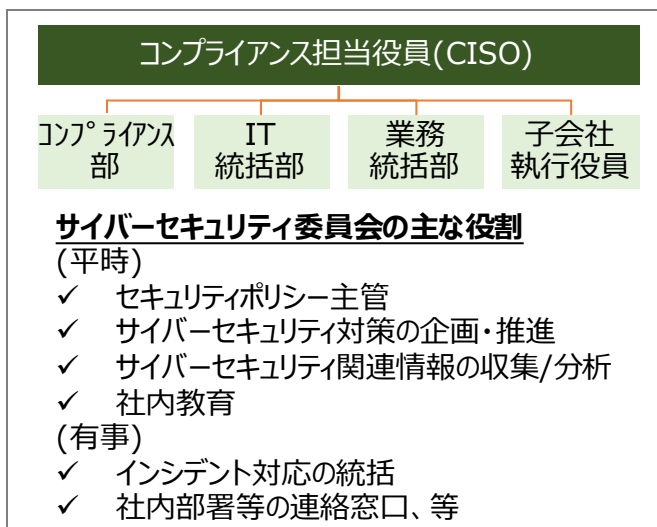
IT統括部長が実践したステップは下記3点である。

- 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

## D社の実践内容

上記のステップに則り、D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)

表2-2.1 D社の役割分担の例



コンプライアンス部	<ul style="list-style-type: none"> <li>✓ 委員会事務局</li> <li>✓ セキュリティリスクの管理</li> <li>✓ 従業員教育</li> <li>✓ 社内のインシデント報告の窓口、インシデント管理</li> </ul>
IT統括部	<ul style="list-style-type: none"> <li>✓ 技術的なサイバーセキュリティ対策の企画</li> <li>✓ 業務基盤の運用</li> <li>✓ 脆弱性や脅威情報の収集</li> </ul>
業務統括部	<ul style="list-style-type: none"> <li>✓ 倉庫管理業務におけるセキュリティ施策の推進</li> <li>✓ 組織間の連絡窓口</li> </ul>
子会社執行役員	<ul style="list-style-type: none"> <li>✓ グループ共通的なセキュリティ施策の推進</li> <li>✓ 会社間の連絡窓口</li> </ul>

図2-2.1 D社のサイバーセキュリティ委員会イメージ

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、以下の資料も参考にできる。  
 サイバーセキュリティ経営ガイドライン付録F『サイバーセキュリティ体制構築・人材確保の手引き』（本書P9で紹介）  
 日本セキュリティオペレーション事業者協議会（ISOG-J）：セキュリティ対応組織（SOC/CSIRT）の教科書  
[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

また、事業部門や管理部門等の担当者についても、業務遂行時の適切な対策実施や専門家との円滑なコミュニケーションに必要な能力を身につけるための「プラス・セキュリティ」<sup>7</sup>の取組も進める。

## 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あるが分からない

<sup>7</sup> プラス・セキュリティについては、『サイバーセキュリティ体制構築・人材確保の手引き』（本書P9で紹介）も参照。

## 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。

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

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

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

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D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設置した。

D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<sup>8</sup>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。

### D社の実践のステップ

IT統括部長が実践したステップ<sup>9</sup>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

### D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 D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)	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>
脆弱性や脅威情報の収集			

8 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。  
産業横断サイバーセキュリティ人材育成検討会：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)  
[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2021年版  
<https://www.jnsa.org/result/skillmap/>

9 サイバーセキュリティ経営ガイドライン付録F『サイバーセキュリティ体制構築・人材確保の手引き』（本書P9で紹介）では、本プラクティスをITSS+（セキュリティ領域）を用いて実践する場合の手順を紹介している。



## 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。

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

サイバー攻撃は、情報の窃取だけでなく、システムの改変や停止等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、実践する上でのファーストステップとしては、下記3点が考えられる。

- 経営層や事業部門との討議を通じ、自社の事業において重要な情報やシステムを特定する
- 特定したシステムに対して起こりうるサイバー攻撃を洗い出し、攻撃による被害発生の予想頻度（被害発生可能性）と、事故が生じた場合の影響の大きさ（重要度）を分析し、サイバーセキュリティリスクを把握する
- そのうえで、優先度を設けて対応を講じる

## 想定される企業の状況

指示4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した企業の事例をプラクティスとして紹介する。

- 最初から、自社が保有する情報やシステムを洗い出して可視化することは困難である
- 一方で、サイバー攻撃の脅威に早急に対応を講じる必要がある

## プラクティス 4-1

# 経営への重要度や脅威の可能性を踏まえた サイバーセキュリティリスクの把握と対応

従業員数800名規模の小売業であるE社の情報システム部長は、他社での情報流出の事案もあり、経営層から早急なシステムの点検を指示されていた。E社では、情報資産管理台帳の作成に着手したが、全ての情報資産を洗い出して評価することは困難であった。そこで情報システム部長は経営層との討議を通じて、被害発生時に経営への影響が大きいと見込まれる重要情報については、リスクが高い攻撃手法とシステムの組み合わせから、優先的に対策を講じることとした。

## E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以下の3点である。

- ① 経営層や事業部門等とのディスカッションを通じて、自社の経営戦略において重要な情報やシステムを特定する
- ② ①と並行し、システムベンダの協力も仰ぎながら、同業他社等で発生したサイバー攻撃の手口や利用された脆弱性等に関する情報を収集し、自社の情報やシステムへの影響度（被害発生可能性<sup>10</sup>）を特定する
- ③ 情報やシステムの重要度<sup>8</sup>と攻撃手法の影響度（被害発生可能性<sup>10</sup>）からリスク値を算定し、リスク値の高い攻撃手法とシステムの組み合わせから、優先的に対策を実施する

## E社の実践内容

情報システム部長は、経営戦略において重要な情報やシステムを特定するためには、経営を担う経営層、および業務の企画・執行を担う事業部門等のメンバーと討議を重ね、連携を深めた。また、最近のサイバー攻撃の手法や事例をリストアップする作業を並行して実施し、両者の情報を組み合わせることで、自社にとってリスクの高い攻撃手法とシステムの組み合わせを明らかにすることができた。これを基に、リスク値の高い攻撃手法やシステムの組み合わせから、優先的に経営層や事業部門等と相談を行い、対策を検討・実施することとした。さらにこの過程を通して、以下の対応が速やかに実施できた。

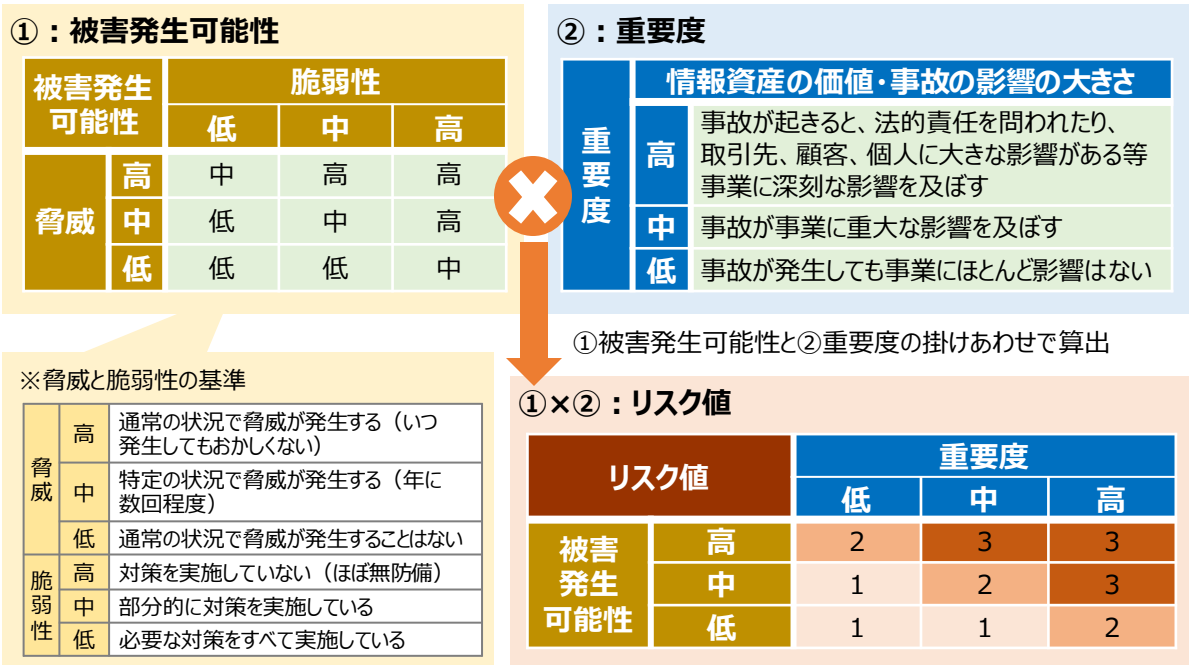
- 不正アクセスのリスクを検証したところ、サイバー攻撃の侵入経路を発見したため、急遽ファイアウォールを再設定した。
- 複数の業務用PCでOSのアップデート漏れが判明したため、情報システム部が管理する業務用PCについては、アップデートを自動化する仕組みを導入した。

10 リスク値の算定に係る「被害発生可能性」および「重要度」については、次項の図2-4.2 参照。

表2-4.1 E社で想定したサイバー攻撃の事例とリスク値の例

分類	攻撃手法	システム	重要 情報	被害発生 可能性	重要度	リスク値
WEBサ イト改ざ ん	攻撃者やマルウェア等により悪意のあるスクリプトやiframe等の埋め込み	情報提供サイト		低	低	1
		ECサイト	有	中	高	3
	ソフトウェアサプライチェーンを悪用したWebスキミング用の不正コードの埋め込み	情報提供サイト		低	低	1
		ECサイト	有	中	高	3
DoS/ DDoS 攻撃	大量のアクセスによるサーバプログラムの応答の低下、もしくは停止	ECサイト	有	中	高	3
	大量のメールを受信させることによるサービス妨害	メールサーバ	有	低	中	1
標的型 攻撃	悪意のある添付ファイルを開封させることによるマルウェアの埋め込み	業務用PC	有	高	高	3
		モバイル機器		高	中	3
	不正サイトへの誘導によるマルウェアの埋め込み	業務用PC	有	高	高	3
その他	クラウドサービスのセキュリティ対策の不備を突いたサーバへの不正侵入	給与システム	有	低	高	2
	従業員による無許可のクラウドサービスの利用（内部不正）	業務用PC	有	高	高	3
		社内サーバ	有	中	中	2
	脆弱性等を突いたシステムへの不正侵入	業務用PC	有	中	中	2
		社内サーバ	有	高	高	2
	ssh、ftp、telnet等に対するブルートフォース攻撃の成功による不正侵入	業務用PC	有	中	高	3

(リスク値) 3:深刻な事故が起きる可能性大、2:重大な事故の可能性有、1:事故が起きる可能性小、起きてても被害は受容範囲

図2-4.1 E社で利用した被害発生可能性と重要度からリスク値を判定する方法の例<sup>11</sup>

11 リスク値の算定方法の詳細については、中小企業の情報セキュリティ対策ガイドライン(IPA)を参照。

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

参考情報

情報資産に対するリスク分析を簡易的に実施するためには、中小企業の情報セキュリティガイドライン第3版、ならびに付録7のリスク分析シート<sup>12</sup>も活用できる。

図2-4.2 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

業務分類	情報資産名称	備考	評価値				現状から想定されるリスク（入力不要・自動表示）			
			機密性	完全性	可用性	重要度	脅威の発生頻度 （「脅威の状況」シートで設定）	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
人事	社員名簿	社員基本情報	2	0	0	2	3: 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	社員基本情報	2	2	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	雇入時・定期健康診断	2	2	1	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

また、制御システム等を対象としたリスク分析を実施するためには、制御システムのセキュリティリスク分析ガイド第2版、ならびに別冊の資産ベースのリスク分析シートおよび事業被害ベースのリスク分析シート<sup>13</sup>も活用できる。

図2-4.3 制御システムのセキュリティリスク分析ガイド第2版 別冊 事業被害ベースのリスク分析シート

表4-8 事業被害ベースのリスク分析シート（シナリオソフト版）

1. 広域での製品供給停止														
項目	攻撃シナリオ		評価指標				対策				対策レベル		攻撃ツリー番号	
							防御		検知／被害把握	事業継続	攻撃 ステップ	攻撃 ツリー	攻撃 ツリー 番号	構成 ステップ (項番)
							侵入／拡散段階	目的遂行段階						
	攻撃ツリー／攻撃ステップ		脅威 レベル	脆弱性 レベル	事業被害 レベル	リスク値								
	1-1	広域供給停止操作の実行により、広域で供給が停止する。												
1	侵入ロー情報HMI 悪意ある第三者が、情報NNWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。対策は「プロセス不正実行」のもの。						FW 通信相手の認証 パッチ適用 脆弱性回避 検察管理	○ ○ ○ ○ (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム 検察死活監視			2 ※1		
2	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。						通信相手の認証 パッチ適用 脆弱性回避 検察管理	○ ○ ○ ○ (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム 検察死活監視			2		
3	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	ソフトウェアのバージョンアップ データの署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#1-1 1.2.3	

12 IPA：中小企業の情報セキュリティ対策ガイドライン  
<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>  
 13 IPA：制御システムのセキュリティリスク分析ガイド  
<https://www.ipa.go.jp/security/controlsystem/riskanalysis.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。

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

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
- 企画・設計段階からセキュリティ機能を組み込むことができておらず、セキュリティ対策対応に係る担当者への負担増、手戻りによる開発遅延等が問題になっている

## 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>14</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>15</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

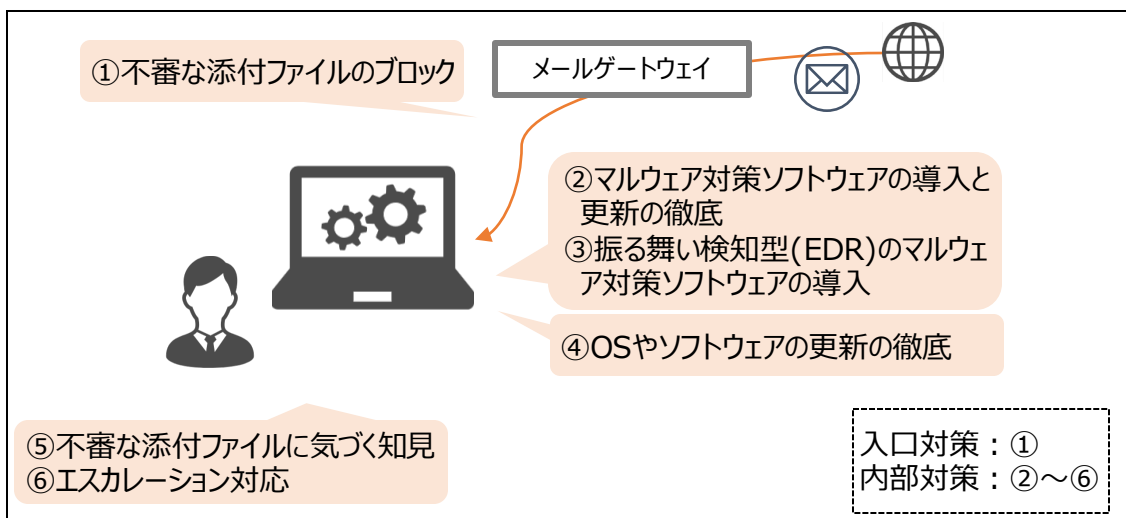


図2-5.1 多層防御の例(メールの添付ファイルによるマルウェア感染リスクの低減)

14 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/files/000046236.pdf>

15 IPA：【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

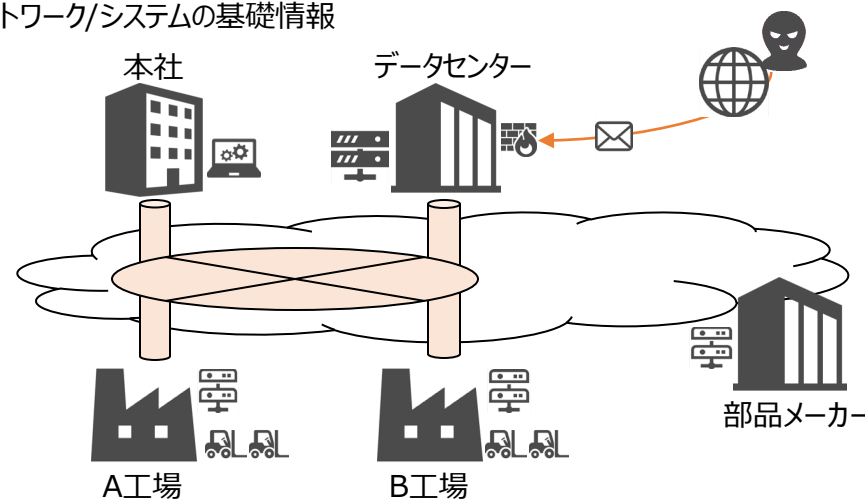
<https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html>



# 前提となるF社のシステム環境

従業員数500名規模の製造業であるF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。

F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 F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

## F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

## F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>16,17</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：攻撃に利用されうる端末への対策」、「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。

16 IPA：日常における情報セキュリティ対策 <https://www.ipa.go.jp/security/measures/everyday.html>  
17 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/files/000046236.pdf>



## プラクティス 5-2

# アクセスログの取得

プラクティス5-1に記載したF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。

## F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

## F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>18</sup>の導入等を検討し始めている。

18 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なく、OS等の関連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。

## プラクティス 5-3

# セキュリティバイデザインを標準とする、クラウドベースの開発プロセスの励行

従業員数500名規模の金融系IT子会社であるG社は、Fintechを含む金融系のサービスやプロダクトの開発・実証を行っている。現在、開発プロジェクトの対象はクラウドベンダーの提供するIaaS上で運用するものが主流となっている。同社は従来、開発工程で諸機能を実装するタイミングでセキュリティ機能も検討していたが、対応すべき脅威が多様化する中、開発部門の責任者は担当者への負担増や、手戻りによる開発スケジュール遅延等の発生等を課題と感じていた。全社のセキュリティ開発を統括するセキュリティチームとの相談の結果、いわゆる「セキュリティバイデザイン」として企画・設計段階からセキュリティ機能を組み込むことが適切と判断し、自社の標準的な開発プロセスとして規定することとした。

## G社の実践のステップ

セキュリティ機能は一般にソフトウェアの主たる目的には含まれないが、かといって後付けで実装しようとすると設計・開発段階まで手戻りが生じることにもなりかねない。近年、セキュリティバイデザインの重要性が認識されつつあるが、企画・設計段階でセキュリティ要件を明確化することは容易ではなく、同社も踏み込んだ検討には至っていなかった。G社のセキュリティチームのリーダーは、開発部門のニーズに合わせた脅威分析を支援することで、次のステップでセキュリティバイデザインの導入に取り組んだ。

- ① ソフトウェアの概念設計フェーズにおいて設計内容が固まった段階で、次ページ図の要領で開発と並行して脅威分析を行う手順を標準的な開発プロセスに追加した。なお、あくまで標準であって、プロジェクトの特徴に応じた個別対応を妨げるものとはしていない。
- ② 運用段階における対策については、インフラチームの協力を得ることで実装するクラウド環境における適切なセキュリティ設定の維持、仕様変更対応やインシデント対応体制等が担保されるようにした。
- ③ 現状では上記①②を通じてセキュリティバイデザインを概ね実践できているが、さらなる効率化を実現するため、ソフトウェアの用途や環境に応じた脅威分析の適切な粒度を見極めるための手法について検討している。

## G社の実践内容

G社が設計段階で実践しているセキュリティ対策は次の通りである。

- 脅威分析にはSTRIDE（次ページ参照）を利用。概念設計段階で作成するDFD（Data Flow Diagram）をもとに、各ポイントでどのようなセキュリティ脅威があるかの洗い出しを実施。洗い出しはセキュリティチームで行うが、ユースケースによって脅威が異なってくることもあることから、必要に応じて設計チームと脅威の想定についてのディスカッションを行っている。

- セキュリティ対策に関する要求仕様としては、公益財団法人金融情報システムセンターの『金融機関等コンピュータシステムの安全対策基準・解説書』に準拠しつつ、用途別にチェックリストを作成して対応。
- クラウド環境において実施する対策の選定にはCISベンチマーク（下欄）を使用。これは要求されている対策が具体的で顧客や開発ベンダ等とのコミュニケーションにも使いやすいとの判断による。
- クラウドが提供するアクセス制御機能やモニタリング機能等を活用。これらの可用性確保に関する保守をクラウドベンダに委ねることでセキュリティ機能の運用の効率化を実現。
- セキュリティ機能の実装には、対象のクラウドサービス用に業界で用いられているテンプレートを適用することで、利用可能なベンダーのセキュリティ機能を活用しながらセキュアな環境構築を行った。

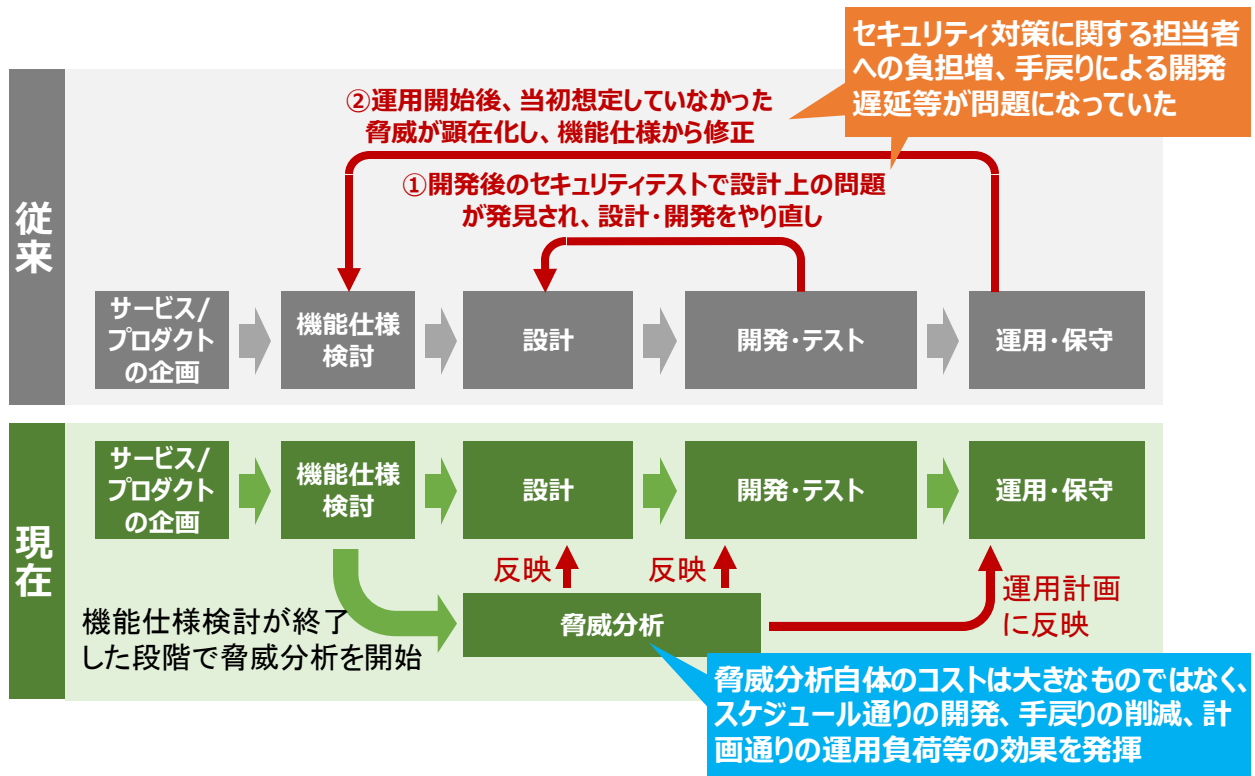


図2-5.3 G社のソフトウェアライフサイクルにおけるセキュリティバイデザイン導入の効果比較

## 参考情報

CISベンチマーク <https://www.cisecurity.org/cis-benchmarks/>

米国の非営利法人Center for Internet Securityが公表している、情報システムの構築・運用における構成要素別のセキュリティ対策のベストプラクティスを定めたガイドライン。

STRIDE <https://www.ipa.go.jp/files/000046476.pdf>

Microsoft が提唱する脅威の分類手法。「なりすまし」「改ざん」「否認」「情報漏えい」「サービス拒否」「特権の昇格」の6種類のカテゴリから脅威を洗い出す手法。

ミニ  
プラクティス

このプラクティス集を作成するために実施した企業インタビュー調査で得られた「指示 5」に関するプラクティスのうち、事例で紹介できなかったものを示します。

ミニプラクティス  
1

## クラウドサービスを利用する際のセキュリティ対策を強化するにはどうすればよいのか？

対応する  
チェック項目

5-3：システム設計時にリスク分析を行い、必要なセキュリティ機能を具体化し、開発時に実装している

企業による  
実践例 1

クラウドサービスの場合、オンプレミスのシステムと比較して現場のエンジニアが勝手に設定を変更してしまうようなことが生じやすい。そこで「これが守られていないとインシデントが生じかねない」というポイントを対象とする自動監査の仕組みを作り、定期的に監査している。（情報サービス業）

企業による  
実践例 2

クラウドサービス毎に、どのような設定にしておけば自社のセキュリティポリシーに従った運用ができるのかを整理したガイドラインを作って社内に配布している。ただしそれでも抜け漏れはあるので、実際に疑似攻撃することで問題を見つけることも併用して行っている。（情報サービス業）

ミニプラクティス  
2

## ペネトレーションテストの補完手段として、どのような対策があるのか？

対応する  
チェック項目

5-6：システム等に対する定期的な脆弱性診断や、継続的なパッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している

企業による  
実践例

チェックリストの励行のみで安心してしまうのは危険であって、攻撃が成功する恐れがないかを外部の目で確認する脅威ベースのペネトレーションテスト（TLPT）のような取組を行うことが望ましい。しかしながら小規模の変更等でTLPTを行うほどでもない場合、システムの対策状況を熟知している要員が攻撃側、防御側それぞれの役割を演じつつ、攻撃が成功するかどうかを検証する机上演習（テーブルトップエクササイズ）を実施するのみでも有益である。（金融業）

ミニプラクティス  
3

## 従業員向けのセキュリティ研修の受講モチベーションを高めるにはどうすればよいのか？

対応する  
チェック項目

5-10：従業員に対して、サイバーセキュリティの教育・演習を実施している

企業による  
実践例

サイバーセキュリティ研修の後で実施する確認テストの結果をもとに、それぞれの部門や個人がどのような傾向で間違えるか他部門との違いを示すことで、自分達のセキュリティに関する理解度がどうなのかを定量的に見せるようにしている。（教育業）

注）対応するチェック項目：サイバーセキュリティ経営ガイドライン経営可視化ツールの39問のチェック項目の番号に対応しています。（公開ページ）<https://www.ipa.go.jp/security/economics/checktool/index.html>

## 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

## 実践に向けたファーストステップ

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仕組み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。

- 自社のセキュリティ対策の状況や水準を評価し、改善に活かす仕組みを構築する
- 評価や改善の取組が形骸化しないよう、演習や訓練を通じて従業員の意識レベルを向上する

ガイドライン実践のプラクティス  
第2章

## 想定される企業の状況

指示6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した企業の事例をプラクティスとして紹介する。

- PDCAサイクルのうち、特にC（Check）やA（Act）をどのように実践すればよいかわからない
- セキュリティ対策状況の評価が形骸化している懸念がある
- 自社のセキュリティ対策状況を適切に可視化できていない
- 社外の投資家などに対して、自社で適切なセキュリティ対策をしていることの説明ができていない

第3章

付録



## プラクティス 6-1

# PDCAサイクルの検証と、演習・訓練を通じた 評価・改善プロセスの強化

従業員数1,500名規模の小売業であるH社では、サイバーセキュリティに関する目標と取組計画を策定している。情報システム部が主導する技術的な対策は計画通り進捗している一方で、従業員による不審メールの開封や無許可の業務用PCの持ち出し等が依然として頻発していた。各店舗におけるチェックシートを活用した点検に特段の課題は見られなかったため、情報システム部長は、店舗の業務とセキュリティの取組が切り離されており、取組計画の評価、改善が十分に機能していないと考えた。そこで、業務フローに踏み込んだ問題点の把握や対策の検討のため、セキュリティ評価の取組を見直すこととした。

## H社の実践のステップ

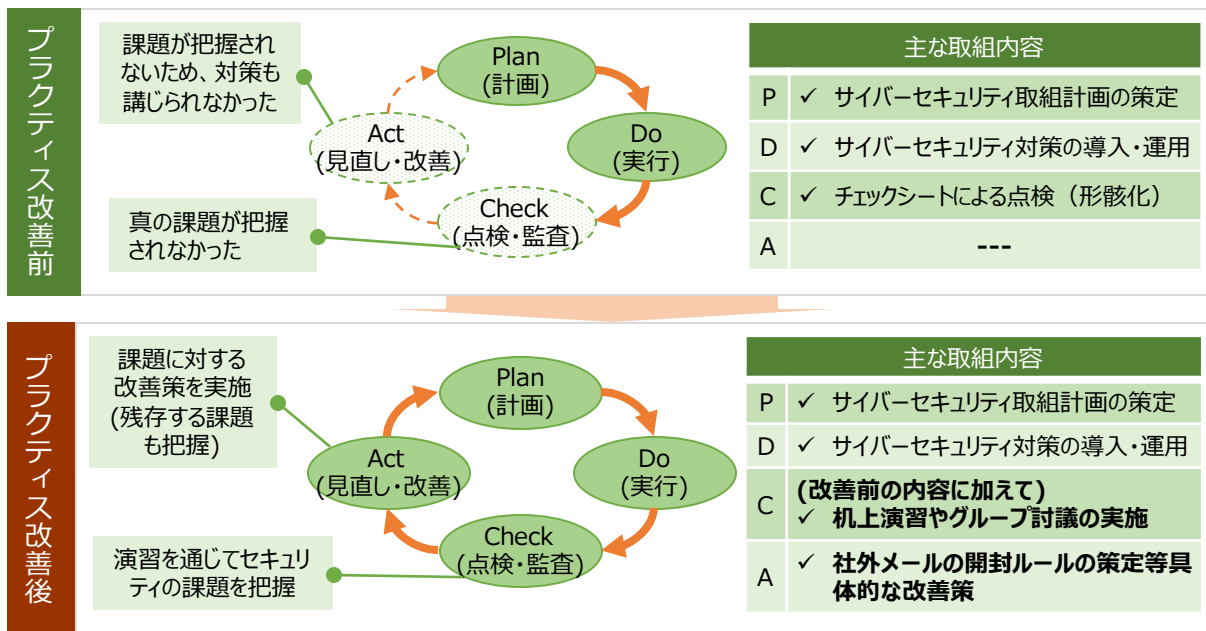
情報システム部長が実践したステップは以下の2点である。

- ① セキュリティの評価や改善に関する取組を検証し、課題点を把握する
- ② 課題点である従業員の意識付けの不足を解消するため、演習・訓練を実施する

## H社の実践内容

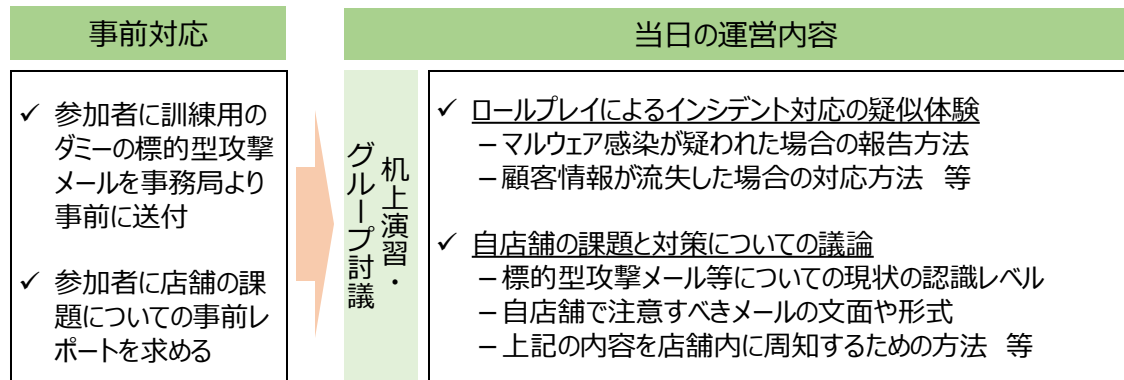
評価や改善についての現在の取組内容を検証したところ、現場でのチェックシートを活用した点検が形骸化しており、その結果、課題の発見に至らず有効な改善も実施されてこなかったことが把握できた。点検が形骸化した理由として、点検を実施する従業員への意識付けが不十分であると考えた情報システム部長は、新たに机上演習やグループ討議を実施することにした。

図2-6.1 H社で実践したPDCAサイクルの改善の例



情報システム部長は、机上演習やグループ討議の実施にあたり、参加者が実業務に関係する問題としてセキュリティを捉えられるよう、店舗の業務運営に関連するテーマを取り扱った。

図2-6.2 H社で実践した机上演習やグループ討議のイメージ例



また、参加者に対し、当日の気づきを踏まえて、後日自店舗のメンバーを集め、自店舗の課題や改善策の議論を行うよう徹底した。

H社では、こうした取組を毎年対象者を変えて実施している。その結果、各店舗において「多額の送金は、メールのみの依頼では対応せず、依頼先に電話確認するルールを策定した例」や、「朝礼で定期的に注意喚起を行うことにした例」等、具体的な改善が進んできている。

## 参考情報

PDCAサイクルを強化するための評価に関する取組として、情報システム部門等によるチェックリストを活用したセルフアセスメント（自己評価）や、独立した立場の専門家による第三者評価も有効である。<sup>19</sup>

表2-6.1 PDCAサイクルを強化するための評価に関する取組

評価に関する取組	内容
演習・訓練	<ul style="list-style-type: none"> <li>✓ インシデントを想定した疑似対応を行うことで、個々の管理策について評価</li> <li>✓ 手間や時間がかかる一方で、具体的な課題の抽出に繋がりがやすいとともに、従業員への意識付けも図られる</li> </ul>
セルフアセスメント（自己評価）	<ul style="list-style-type: none"> <li>✓ チェックリスト等を活用した個々の管理策の効果や達成度の評価</li> <li>✓ 手間、時間、費用が少なく済み、手軽に行うことが可能であるも、従業員の意識付けが不十分である場合、運用が形骸化することもある</li> </ul>
第三者評価	<ul style="list-style-type: none"> <li>✓ 対策の導入や運用に関与していない独立の立場の専門家による客観的評価</li> <li>✓ 独立の専門家に依頼するため、実施には時間と手間と費用がかかる</li> </ul>

<sup>19</sup> セルフアセスメント（自己評価）や第三者評価については、以下の資料も参考にできる。

IPA：情報セキュリティマネジメントとPDCAサイクル

<https://www.ipa.go.jp/security/manager/protect/pdca/evaluation.html>

IPA：サイバーセキュリティ経営可視化ツール

<https://www.ipa.go.jp/security/economics/checktool/index.html>

## プラクティス 6-2

# 一律のルール適用が困難なビジネスにおける セキュリティKPIを用いたリスク管理

従業員数1,800名のインターネットサービス事業者であるI社は、仮想現実（VR）を利用したゲームやSNS、非代替性トークン（NFT）応用など、最新技術を活用したサービスの提供に積極的であり、将来的にはメタバースでの事業展開も視野に入れて積極的な研究開発を行っている。

サービスの開発と運用はDevSecOpsモデルに基づいているが、新サービスについての脅威はサービス内容に応じて様々であるため画一的なセキュリティ対策を講じることができない。経営層がセキュリティ対策の財務面への影響が見えないことを懸念して定量的なKPIの検討をCISOへ指示したのを受け、同社のCISOはセキュリティ成熟度に基づいた定量化ができないか試行してみることにした。

## I社の実践のステップ

I社のCISOが実践した手順は次の通りである。

- ① サービス提供部門や研究開発部門との意見交換をもとに、サービス提供に伴うサイバーセキュリティリスクを許容できるレベルに抑制するための取組事例を収集した。
- ② ①の結果をもとに、バランストスコアカードによる有効性の可視化として、サイバーセキュリティリスクマネジメントにおける成熟度を、セキュリティ対策を講じる対象となる構成要素（アプリケーション等）毎に次ページ表のように策定した。
- ③ ②に基づいて新規サービス開始時の対策状況を定量評価できるようにした。

## I社の実践内容

セキュリティKPIの設定と運用の実践にあたって、I社のCISOが留意した点は次の通りである。

- 最新技術を用いたサービスの提供に伴うサイバーセキュリティ上の脅威の発生は避けられないことから、「リスクをなくすこと」ではなく、「リスクを把握し、管理すること」に重点を置いて指標の設定することとし、大きなリスクであってもその挙動が把握できていれば評価が高くなるようにした。
- 直接的に把握しにくいリスク（例：ルール更新の不備）や、顧客への効果が把握しにくい対策（例：要員のスキル向上）については、バランストスコアカードの活用により、直接的には効果がわかりにくくても、リスクマネジメントとしての有効性につながるものを可視化することに努めた。
- 一般にセキュリティKPIとして特定の対策の達成率（例：自己点検項目の達成率）が利用されがちであるが、達成率の改善が目的となって対策の本質が見失われる恐れがあると専門家による講演で学び、I社ではできるだけ対策の実践状況を表象しやすい指標（例：想定される被害額）を用いるようにした。



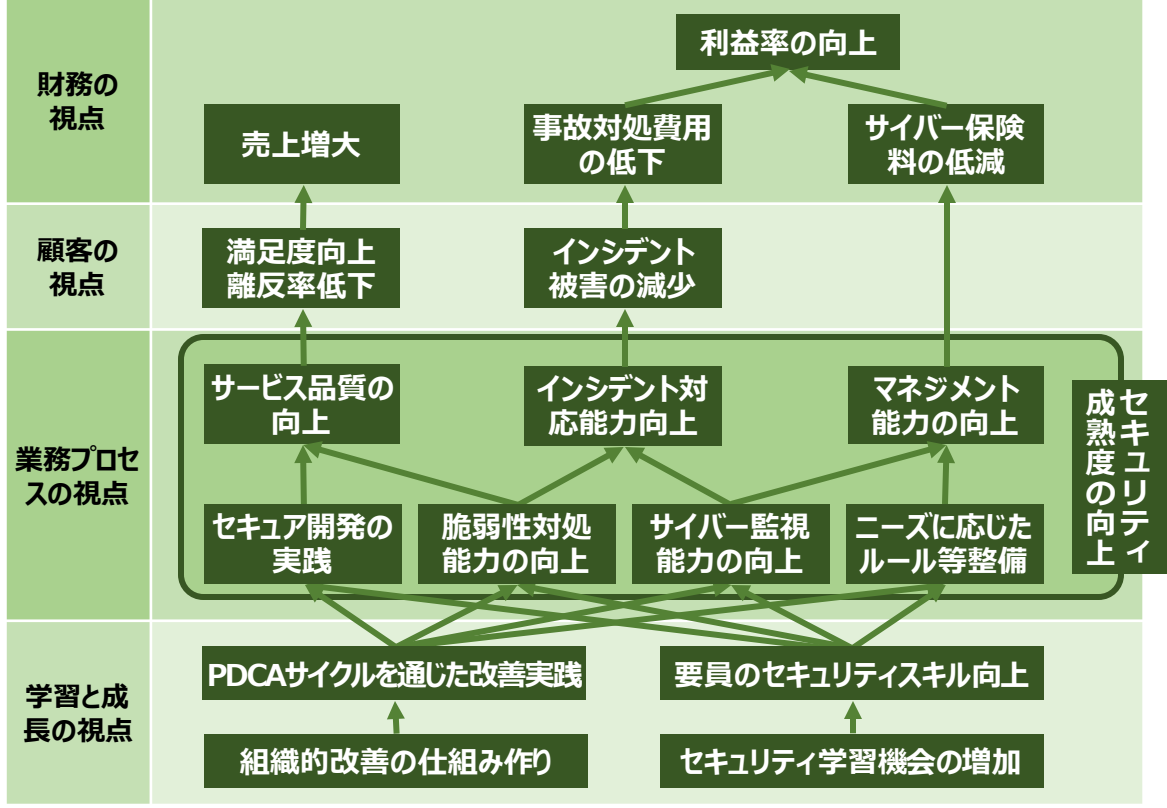


図2-6.3 I社のセキュリティ対策に関するバランストスコアカードの構成（抜粋）

表2-6.2 I社のセキュリティ対策に関するバランストスコアカードの対応項目

	定性的評価項目	定量的評価項目（KPI）
財務の視点	✓ リスクと対策費用のバランス ✓ 対策の見直し状況	✓ 対策しなかった場合の被害額（試算値）
顧客の視点	✓ セキュリティ関連の要望やクレームへの対処状況	✓ セキュリティ起因で顧客サービスが中断された時間
業務プロセスの視点	✓ 未対策となっているリスクがないか ✓ 環境変化への対応ができているか	✓ セキュリティ成熟度の平均値（表2-6.5による）
学習と成長の視点	✓ PDCAサイクルを通じた改善状況 ✓ 現場ニーズと要員スキルとの適合性	✓ スキルを備えた要員の充足率 ✓ 要員のセキュリティスキルのセルファセスメント結果の平均値

表2-6.3 I社が定めたセキュリティ成熟度の定義例（作業毎に定義）

成熟度	セキュリティ関連リスクの評価	リスク対応の実施
5	4に加えて、今後の継続的な変化にも対応	対策の有効性の評価を行いながら実施
4	3に加えてリスクの不確実性を考慮	PDCAマネジメントのもとで実施
3	全体的に実施している	ルールと実施体制を整備した上で実施
2	部分的に実施している	対策方法を定めた上で実施
1	形式的実施にとどまる	場当たり的な対応のみ

はじめに

第1章

第2章  
ガイドライン実践のプラクティス

第3章

付録

## プラクティス 6-3

# ステークホルダーの信頼を高めるための、サイバーセキュリティ関連情報発信の工夫

従業員数100名規模のバイオ系スタートアップ企業であるJ社は、ポストコロナ時代の成長期待企業として投資家からの注目が集まっている反面、同社の企業秘密を狙うサイバー攻撃による企業価値の毀損を恐れる投資家から、サイバーセキュリティ対策の強化を求められている。投資家が自社のどのような状況を不安に考えているかを認識し、その不安を解消するためにどのような情報提供をすべきなのか、J社のCISOは専門家のアドバイスを受けつつ、広報室のメンバーとともに検討することとした。

## J社の実践のステップ

J社のCISOが実践したステップは下記3点である。

- ① 投資家が懸念するリスクを洗い出し、伝えるべきリスクへの対策手段との組合せを整理した。
- ② 対外的に公表する自社のセキュリティ対応体制と、説明時に留意すべき内容のアピールポイントについて、経営層及び広報室と協議し、下表の内容について了解を得た。
- ③ ①と②の組合せをもとに、投資家向け資料におけるオペレーショナルリスクに相当する内容として、サイバーセキュリティリスクへの対応体制と対策方針に関する内容をとりまとめ、公表した。

## J社の実践内容

J社のCISOが情報発信において留意した内容は次の通りである。

- スタートアップである自社は若手研究者のイノベーションの尊重を謳っており、投資家からセキュリティ対策が甘くなりがちではと懸念されている。一方で対策を細かく公表すると、外部攻撃者に攻撃のヒントを与えることになりかねない。
- そこで投資家向け公表にあたっては、「研究者が意識せずに適切な情報管理を行える仕組みの整備（例：営業秘密へのアクセスに多要素認証を要求、サーバ上では自動的に暗号化された状態で管理等）」と「攻撃の予兆を素早く防御に反映できる」ことの2点をアピールすることで、投資家の信頼感醸成と攻撃への牽制の両面の効果を得ることに努めている。

表2-6.4 投資家が懸念するリスクとその対策方針例

主なリスク	左記リスクに対する対策方針
システム管理の不備による不正侵入	<ul style="list-style-type: none"> <li>✓ 多層防御により、1つの脆弱性で攻撃が成功しない環境を構築</li> <li>✓ 外部協業用環境を、内部の情報管理基盤と分離して運用</li> </ul>
研究者の操作ミスによる情報漏えい	<ul style="list-style-type: none"> <li>✓ 自社の営業秘密はすべて自動で暗号化される記録装置にて管理</li> <li>✓ 外部に情報を送る操作を行う際に、2段階確認プロセスを導入</li> </ul>
研究者の内部不正による不正持出	<ul style="list-style-type: none"> <li>✓ IRM（Information Rights Management）を用いた機密情報の個別トレースの実施</li> <li>✓ 重要情報へのアクセスを対象とするリアルタイム監視の実施</li> </ul>

ミニ  
プラクティス

このプラクティス集を作成するために実施した企業インタビュー調査で得られた「指示6」に関するプラクティスのうち、事例で紹介できなかったものを示します。

ミニプラクティス  
4

**経営層に自社のセキュリティ対策状況を客観的に説明するにはどうすればよいのか？**

対応する  
チェック項目

6-2：経営者が定期的に、サイバーセキュリティ運用に関する報告を受け、対策を指示している

企業による  
実践例1

自分達で構築し、提供しているサーバ類（サプライチェーンも含む）が外からどう見えるか、そのスコアが継続的に上がっているのかどうか、業界平均と比較してどうかのスコアを外部サービスを用いて常にとるようにしている。「自社が75～80点で、業界平均が73点」などと説明することで、経営陣にも納得してもらいやすい。（教育業）

企業による  
実践例2

経営層に自社グループ全体としてのセキュリティのマネジメントがどのようなレベルに位置付けられているかを報告している。その際に、類似の事業者はこのレベルにいて、世界的な大手先進事業者はこのレベルといった位置付けを表現し、「自社は5年後にはこの程度のレベルに到達することを目標とし、そのためにこのような施策に取り組む」という建て付けで、極力定量的な表現で報告するようにしている。（製造業）

企業による  
実践例3

重要なのは「重大インシデントが発生していないこと」であって、その実現のためにこのような取組を行い、そのスキルや実行力を維持しつつ、事業上の課題を解決しているという説明をしている。従って定量指標は作りにくいのだが、取組の過程で何件の脆弱性診断を実施し、何件の重大な脆弱性を発見して対応した、社内の相談に何件対応したといった実績を報告している。場合により、個人情報の保有件数に500円を乗じて脆弱性を検出する効果の試算を行うこともある。（情報サービス業）

ミニプラクティス  
5

**セキュリティ対策に関する自己評価の客観性を高めるにはどうすればよいのか？**

対応する  
チェック項目

6-3：サイバーセキュリティにかかる内部監査、監査役監査、外部監査を踏まえ、サイバーセキュリティ対策を適時見直している

企業による  
実践例1

外部評価に頼れない部分は自己評価するしかないが、その際にはできるだけ外部の評価基準（フレームワーク等）を使いながら、同じ基準でスコアが見えるように作っている。（教育業）

## 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り、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
- インシデント発生時の外部報告・公表のルールを定めていない
- 想定されるインシデントに応じた分析・対応手順を定めていない

## 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。

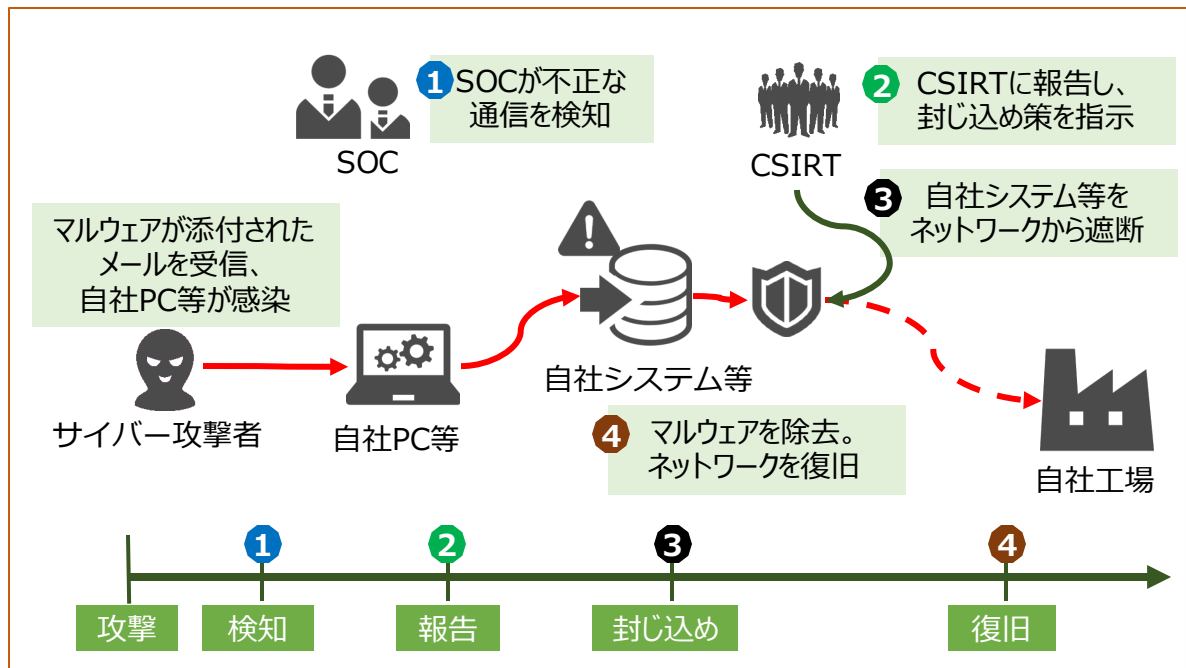


図2-7.1 サイバー攻撃に対するインシデントレスポンスの流れ(イメージ)

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>20</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>

<sup>20</sup> 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/CC：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

## 司令塔としてのCSIRTの設置

従業員数3,000名規模の小売業であるK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上での司令塔となるCSIRT<sup>21,22</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。

### K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>23</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の司令塔となる部署と対応部署を決める
- ② 司令塔となる部署については、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

### K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司令塔となる部署を規定し、周知した。

表2-7.2 K社におけるインシデント発生時の司令塔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	司令塔部署	対応部署
1位	ランサムウェアによる被害	○	情報システム部 (K社 CSIRT)	情報システム部
2位	標的型攻撃による機密情報の窃取	○		
3位	サプライチェーンの弱点を悪用した攻撃	○		総務部
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	○		情報システム部
5位	内部不正による情報漏えい	○		人事部

21 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/CC：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)

22 日本シーサート協議会：CSIRT人材の定義と確保(Ver.2.1)

<https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf>

23 IPA：情報セキュリティ10大脅威 2022 <https://www.ipa.go.jp/security/vuln/10threats2022.html>



# プラクティス 7-2

## 従業員の初動対応の規定

プラクティス7-1に記載したK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司令塔部署(CSIRT)を決め、社内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、K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、初動対応を規定し、CSIRTが周知している。

### K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>24</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

### K社の実践内容

上記のステップに則り、K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規定し、周知した。

表2-7.3 K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>25</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	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>
2位	標的型攻撃による機密情報の窃取	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>
3位	サプライチェーンの弱点を悪用した攻撃	要	<ul style="list-style-type: none"> <li>取引先周知</li> </ul>
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	要	<ul style="list-style-type: none"> <li>CSIRTに連絡（電話、メッセージング等）</li> <li>電話やメッセージングサービス等での状況確認</li> <li>メールやファイルを削除しない</li> </ul>
5位	内部不正による情報漏えい	要	（人事部と情報システム部で対応）

<sup>24</sup> 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8版  
<https://digitalforensic.jp/home-act-products-df-guideline-8th/>

<sup>25</sup> 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。  
IPA：情報セキュリティサービス基準適合サービスリスト [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/)



## プラクティス 7-3

# インシデント発生時の優先度に応じた 顧客への通知・連絡・公表手順

従業員数500名規模で10店舗で旅行代理店サービスを提供しているL社は、自社で過去に開発した業務システムで注文受付、海外事業者との決済、ホテルとの契約の交渉など様々な業務に利用している。従業員の端末がマルウェアに感染してしまったことが原因で、海外ツアー中の顧客へのサポートができなくなるインシデントが発生した。その際、正式な公表が遅れたことで取引先から苦情が寄せられるなど自社のレピュテーションへの悪影響が生じ、その反省を踏まえてインシデント発生時の外部報告・公表のルールを定めることになった。

## L社の実践のステップ

L社のCISOが実践したステップは下記3点である。

- ① インシデント発生時に連絡が必要な相手先のリストアップ
- ② 誰の責任で、誰に何を伝えるかのルール化
- ③ 重大なインシデントの場合の対外公表に関する社内判定会議の設定

## L社の実践内容

L社のCISOが実践した内容は次の通りである。インシデントが疑われる事象の場合、外部委託のセキュリティオペレーションセンター（SOC）からの通知や顧客からの連絡をもとに、自社でインシデントと判断したタイミングを起点として、次の要領でエスカレーションを行うこととした。

- SOCの助言により、エスカレーション担当を指名し、公開資料<sup>26</sup>を参考にその業務内容を規定。
- インシデント発生時のエスカレーション手順を、次の3種類の区分に基づいて設定：
  1. 業務システムの応答が悪いと真っ先に影響する予約・発券サイトの運営事業者との間では、「原因は不明だが、サーバの応答速度が低下している」といった段階から共有する
  2. それ以外の取引先については、一定の状況が把握できた段階で、予め定めた窓口宛に、相手先への影響見通しを含め、経営ガイドライン付録Cを参考に定めた様式<sup>27</sup>にて連絡を行う
  3. 重大と判断されたインシデントは社長承認のもと、広報室を通じて対外的に公表する
- 上記のルールが適切に機能することを、SOCベンダーと取引先の協力を得て訓練にて検証し、そこで得られた課題点をもとに様式の改良を行った。

26 一般社団法人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（日本CSIRT協議会）：CSIRT人材の定義と確保  
<https://www.nca.gr.jp/activity/training-hr.html>

27 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（Excel形式）  
[https://www.meti.go.jp/policy/netsecurity/mng\\_guide.html](https://www.meti.go.jp/policy/netsecurity/mng_guide.html)

## プラクティス 7-4

# 想定されるインシデントについての セキュリティ分析計画の事前策定

従業員数4,000名規模の中堅の機械部品メーカーであるM社は、サプライチェーンの中間で上流・下流双方に多数の取引先企業を抱えているほか、インターネットでの消費者向けの直販も行っている。

同社ではかつてマルウェアによるインシデント発生時のログ分析・調査の過程において、インシデント原因の究明をおろそかにしたことで、業務停止に至る被害が再発したことがあった。現場が早期の復旧を要望するのは当然ながら、安易に影響を過小評価することはかえって被害を大きくする恐れがあることから、M社のCISOは、一定規模以上のインシデントが発生した時に必ず実施すべきセキュリティ分析計画を定め、これを遵守させることとし、想定されるインシデントに応じた分析・対応手順の策定に取り組むこととなった。

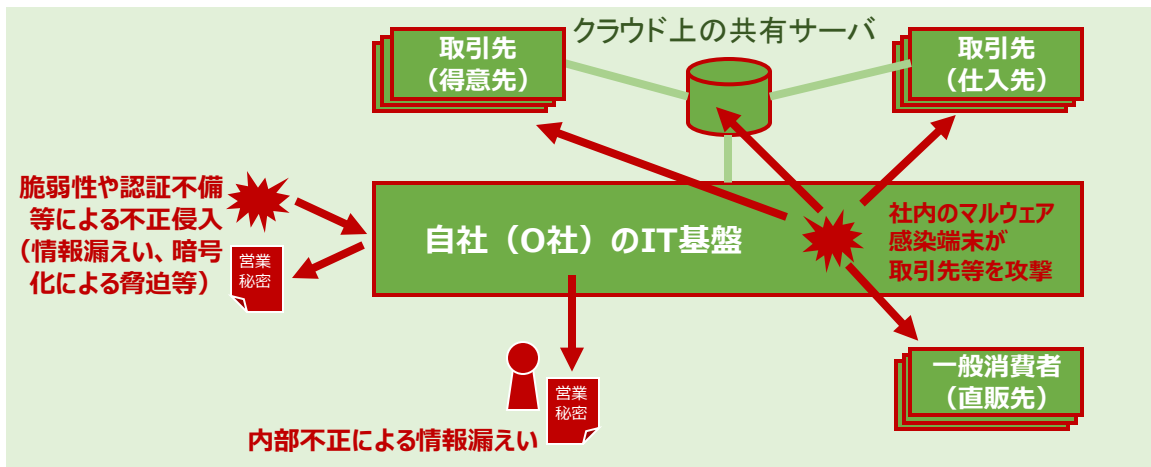


図2-7.2 M社でインシデントが発生した場合の影響範囲のイメージ（赤色部分）

## M社の実践のステップ

M社のCISOが実践したステップは下記4点である。

- ① 自社での発生が懸念されるインシデントを複数想定した上で、簡易なリスクアセスメントを実施
- ② ①の結果をもとに、次ページ表の要領でインシデント発生時に実施することが有用と考えられる分析作業の内容を洗い出し、インシデント対応と組み合わせた対応手順を検討
- ③ ②の結果をもとにM社におけるセキュリティ分析計画を作成し、インシデント発生時に社外ベンダーにスポット的に委託する必要がある作業の費用感を試算
- ④ ③の試算を経営層に示した結果、インシデント発生時に生じる臨時の支出を極力抑制したいとの方針のもと、リスクの移転手段としてセキュリティ分析費用の一部が支払われるサイバーセキュリティ保険に加入することとなった

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

表2-7.4 M社が想定する脅威と分析・調査との対応関係

リスクアセスメントで 洗い出された脅威	インシデントが疑われる場合に実施する分析・調査の例	
	自社で実施	ベンダーに委託
マルウェア感染	<ul style="list-style-type: none"> <li>✓ 異常発生状況の確認</li> <li>✓ 初動対応（感染が疑われる端末の隔離等）</li> <li>✓ エラーログ等の収集・保全</li> <li>✓ 感染端末とのやりとりのある取引先の把握</li> </ul>	<ul style="list-style-type: none"> <li>✓ 脅威インテリジェンス情報からの関連情報の収集</li> <li>✓ マルウェアの種類や挙動の特定</li> <li>✓ 感染経路の特定</li> <li>✓ 感染範囲の特定</li> <li>✓ 社外への流出情報の特定</li> </ul>
脆弱性や認証不備等による不正侵入	<ul style="list-style-type: none"> <li>✓ 不正侵入初動対応（侵入が疑われる端末の隔離等）</li> <li>✓ 最新の資産管理・構成管理情報の整理</li> <li>✓ 端末・サーバ毎の異常有無の確認</li> <li>✓ 重要情報の保管状況の整理</li> </ul>	<ul style="list-style-type: none"> <li>✓ 不正侵入の疑いがあるアクセスの行為者によるアクセス範囲の特定</li> <li>✓ 不正侵入に悪用された可能性のある脆弱性や認証不備等の特定</li> <li>✓ 社外への流出情報の特定</li> </ul>
内部不正	<ul style="list-style-type: none"> <li>✓ アクセスログの収集・保全</li> <li>✓ ログにおける業務上必要なアクセスとそれ以外のアクセスの分類</li> </ul>	<ul style="list-style-type: none"> <li>✓ 行為者による不正な活動に関する証拠の保全</li> <li>✓ 行為者が消去した証拠の復元</li> </ul>

## M社の実践内容

M社のCISOが実践した内容は次の通りである。

- リスクアセスメントの対象とする脅威は、JPCERT/CCの公開情報<sup>28</sup>等を参考に抽出し、マルウェア感染、脆弱性や認証不備等による不正侵入、内部不正等を想定することとした。
- サイバーセキュリティ保険の利用を前提に損害保険会社に相談。保険適用可能なサービスのうち、IPAが公表しているセキュリティサービスリスト<sup>29</sup>の「デジタルフォレンジックサービス」に掲載されているベンダーを選定し、保険適用可能な内容を踏まえつつ、自社で実施すべき内容とベンダーに委託する内容を切り分けた上で、想定する脅威毎のセキュリティ分析計画を作成した<sup>30</sup>。
- サイバー保険の保険料が妥当かどうかについて経営層への説明を行っていく中で、他社で生じているインシデントが自社で発生した場合に、原因分析や損害賠償等に要する費用、事業中断による損失等の推定被害額が可視化されることで、経営層による認識を高める効果が得られた。

28 JPCERT/CC：インシデント報告対応レポート <https://www.jpcert.or.jp/ir/report.html>

29 IPA：情報セキュリティサービス基準適合サービスリスト [https://www.ipa.go.jp/security/it-service/service\\_list.html](https://www.ipa.go.jp/security/it-service/service_list.html)

30 本プラクティスでは自社で定めた分析を行うことを前提にベンダーへの委託内容を個別に調整しているが、中小企業において想定されるサイバーセキュリティインシデントを対象に「見守り」「駆付け」「保険」の3種類をワンパッケージで提供する「サイバーセキュリティお助け隊サービス」が複数の民間事業者によって提供されている。 <https://www.ipa.go.jp/security/otasuketai-pr/>

## 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。

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

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>31</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>32</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

31 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。

32 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N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。

## N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、停止するケースを抽出する
- 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

## N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を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 N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	N社の全環境	1次判断	最終判断	事前協議	事前協議

## 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

プラクティス8-1に記載したN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。

## N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

## N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。

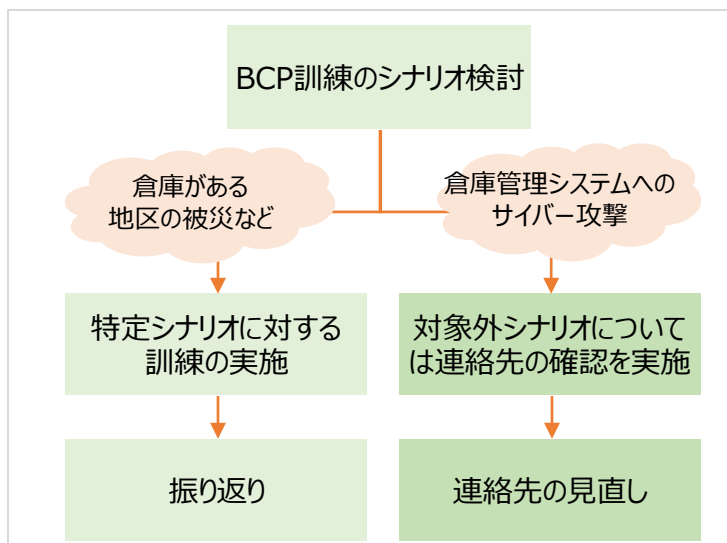


図2-8.1 N社のBCP訓練の流れ



## 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。

## 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

## 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O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、O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。

### O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

### O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
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					
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>33</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 O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	当社の情報管理規程により、組織的、物理的、人的、技術的な対策を定義
	委託業務におけるセキュリティ管理体制はありますか		<b>【受領した回答に対する対応】</b>  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 <b>総合的な評価</b> を実施
	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		
...	...		

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。

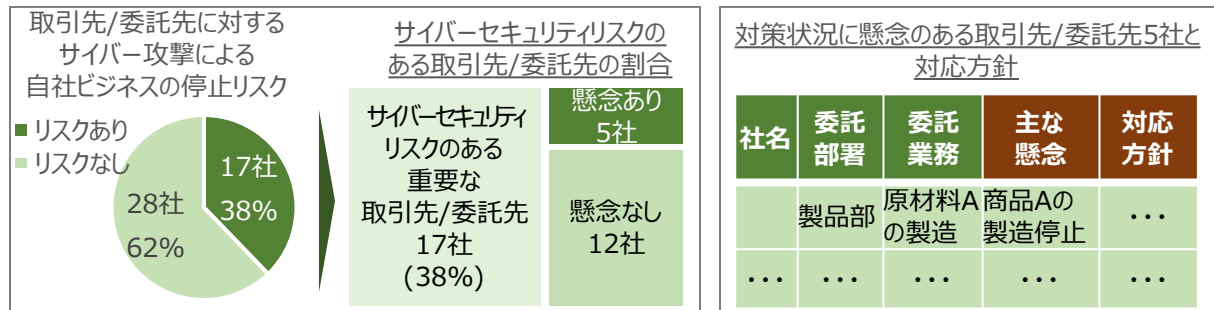


図2-9.1 調査結果の経営者報告資料のイメージ

33 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。

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

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」等の情報を収集・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。

実践する上でのファーストステップとしては、下記3点が考えられる。

- サイバーセキュリティに関するコミュニティ活動や講演会、セミナー等の情報共有活動に参加する
- 情報共有活動で得られた知見を踏まえ、自社システムの脆弱性の確認やその対応に役立てる
- 情報の収集・分析・対応に係る手順を整備する

## 想定される企業の状況

指示10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した企業の事例をプラクティスとして紹介する。

- 情報共有活動への参加の方法がわからない
- 入手した情報を有効活用するために、どのような対応が必要であるかがわからない

## プラクティス 10-1

# 情報共有活動への参加による信頼獲得と、 収集した知見の社内への還元

従業員数900名規模の流通業であるP社は、IPAやJPCERT/CC等が公表する注意喚起情報等の収集を行っていたが、サイバーセキュリティに関する高い専門性を有する人材がいなかったため、大量に提供される情報から自社にとって有用な最新のセキュリティの問題やインシデント等の情報を見極めることに苦戦していた。情報システム部長は、かねてから交流のあった同業他社に相談したところ、様々な企業が参加しているセキュリティ担当者向けの勉強会<sup>34</sup>を紹介された。

## P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以下の3点である。

- ① セキュリティに関係するできるだけ多くのメンバーに、業務として勉強会への参加を指示する
- ② 勉強会では、自社のかかえている課題等を他社へ積極的に情報提供することで、コミュニティにおける信頼を獲得させる
- ③ 参加メンバーに、勉強会を通じた得た情報や知見を社内で共有させる

## P社の実践内容

P社では、情報共有活動への参加に関して、以下の点を心掛けたことで、コミュニティの信頼を獲得し、円滑な情報共有が図られる関係性を構築できた。また、勉強会で得られた情報を社内に還元することで、他社の取組等セキュリティ対策の強化に繋がる知見に関し社内での共有が図られた。

表2-10.1 P社が情報共有活動への参加において心掛けた事項の例

分類	内容
① 継続的な参加	✓ 参加当初は議論についていくことで精一杯であり、また通常業務が逼迫する中で参加の時間を確保することに苦労しつつも、参加を継続する
② 多くのメンバーの参加	✓ 情報システム部長や課長の他、セキュリティに関係するできるだけ多くのメンバーが参加する
③ ルールの遵守	✓ コミュニティにおける情報共有のルールを遵守する
④ 情報提供	✓ 高度な内容ではなくても、自社から提供できる情報や自社の悩みを隠さずに共有する
⑤ 運営への協力	✓ 勉強会の準備や会場の手配等、事務局の運営を手伝う
⑥ 顔を突き合わせたコミュニケーション	✓ なるべく顔を突き合わせての参加を心がけ、親睦会等のオフタイムのコミュニケーションにも積極的に参加する
⑦ 社内への還元	✓ 勉強会で得らえた情報や知見を社内の他のメンバーに共有する

34 IPAやJPCERT/CC、JUAS、各業界ISAC等では、セキュリティに関する情報の提供や参加者同士の情報共有を目的として、各種セミナーやイベントを企画・運営しており、こうしたセミナーやイベントへの参加を通じて、人脈を形成することもできる。

また、情報システム部長は、勉強会での交流を通じて得られた情報の収集と分析に係る手法について、情報システム部の平常時の業務として定義した。さらに、手順書を整備し迅速な初動対応ができるようにした。

表2-10.2 P社が定めた情報収集手順の例

収集先	収集対象	手段	サイクル※	担当者
セキュリティに関するコミュニティ	✓ 同業他社のIT障害全般に関する情報 ✓ 脆弱性情報その他IT障害の未然防止、発生時の被害拡大防止等に資する情報	対面	隔月	課長
		メール	随時	担当
JPCERT/CC	✓ インシデント対応 ✓ 注意喚起情報 ✓ 脆弱性情報 ✓ 各種の重要なセキュリティ情報	WEB	日次	担当
IPA		WEB	日次	担当
警察		WEB	日次	担当

※インシデント発生時は、上記に関わらず随時情報を収集する

表2-10.3 P社が定めた情報分析手順の例

分析観点	分析方法
① どのようなインシデントか	✓ インシデントの対象（システム、情報資産等）及び、原因（攻撃手法、脆弱性等）は何か
② 自社システムに影響があるか	✓ 自社で保有・管理するシステムに関連のあるインシデントか
③ 自社システムで対策が図られているか	✓ ②該当の場合、①の原因について、自社では対策が図られているか
④ 速やかに対策が可能か	✓ ③で未対応であることが判明した場合、ウイルス対策ソフトウェアのアップデート等で速やかに解決を図ることができるか

表2-10.4 P社が定めた対応手順の例

対応分類	対応方法
① 速やかに対策が可能なもの	✓ セキュリティ対策ソフトのアップデート等を速やかに実施する ✓ 対策未実施期間中に不審な通信等を検知していないか、ベンダに確認する
② 速やかに対策ができないもの	✓ 関係部署と調整し、経営の承認を得た上で対策を実施する
③ 特に、社内への注意喚起・情報共有が必要なもの	✓ メール受信時やWebサイト閲覧時等に職員が被害を受ける恐れがある場合には、メールやWebサイトを開かないように注意喚起等を行う

情報システム部長は、経営層による問題点の認識・理解と、事業部門等他部門との連携が重要であると考えた。そこで、次のステップとして、こうした情報が事業リスクの評価やIT投資の検討等においても有効に活用できるよう、経営層や事業部門に対して、セキュリティへの認識や理解を得るための働きかけを行うことを予定している。

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

プラクティス  
10-2

# 業界団体を活用した情報共有活動

従業員数10,000名規模の製造業であるQ社は、自社並びにサプライチェーンを構成する関連会社における工場生産管理システムのセキュリティ対策に悩みを抱えていた。システムは様々な製造工程と連携しており、セキュリティパッチを適用する等の対策は業務への影響を考えると容易にできなかった。

そこでQ社は、ネットワーク監視を含むセキュリティ対策の導入を進めることにしたが、制御システム専用の通信プロトコル等Q社の要件を満たす製品が市場に存在していなかった。そのため情報システム部長は、同業他社が同様な課題を持っているか情報共有に向けた活動を行うことにした。

## Q社の実践のステップ

情報システム部が実践したステップは以下の3点である。

- ① 業界団体の勉強会等で機会を設け、制御システムのネットワーク監視に関する課題を説明する
- ② 勉強会で興味を持った有志でセキュリティ機能要求について検討する
- ③ 上記機能要求について、ベンダやメーカーに対し、開発可能性を相談する

## Q社の実践内容

同業他社も同様の悩みを抱えていることを認識し、その悩みを解決するためのセキュリティ機能要求について、業界団体の他社に呼び掛けて有志で検討してみた。検討においては、関連会社や同業他社のシステムでの導入を想定し、各社固有のカスタマイズを排除した。業界団体に参加しているベンダやメーカーに対し、検討したセキュリティ機能要求をできるだけ多くカバーする製品の開発可能性を相談した(後日、ベンダは業界でのニーズを把握できたので、製品開発を検討し始めた)。

セキュリティについて、他社との差別化を図るのではなく業界全体で取り組む課題と捉え、中長期的な目線での情報共有や対策検討をすることとした。

表2-10.5 業界団体の例<sup>35</sup>

業界団体	活動概要
業界ISAC	金融、電力、ICT、交通、医療、自動車、商社(日本貿易会)、ソフトウェア等各業界の民間事業者同士でセキュリティ情報の共有、分析、対策検討
セプターカウンシル	重要インフラの情報セキュリティ対策向上のため、分野横断的な連携推進
フィッシング対策協議会	フィッシング詐欺に関する事例情報、技術情報の収集及び提供
日本シーサート協議会	インシデント関連情報の収集、分析、対応方針や手順の策定
CSSC	重要インフラの制御システムセキュリティについて研究開発、人材育成、普及啓発等

35 URL等は、巻末の付録p.107参照  
サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集



# 第3章 セキュリティ担当者の悩みと取組のプラクティス

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り組んだ際の**実践手順、内容、取り組む際の方考え方、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		取組のプラクティス	関連する重要10項目
セキュリティ意識の向上	(1) 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
	(2) 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
	(3) 海外拠点のセキュリティ意識が低い	対面のコミュニケーションを通じ、セキュリティ意識を向上させる	2
	(4) 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を感じられない	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
	(5) 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
	(6) 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
	(7) 内部不正で情報漏えいが生じた場合の自社事業への深刻な影響が心配	内部不正を検知するための複数対策を組合せて導入し、周知により発生を抑制	5
	(8) 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を把握し、対面で対話する	6
	(9) 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
	(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、セキュリティ認証の取得状況を確認する	9
コミュニケーション	(11) 経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない	事業部門と協同し、事業戦略の一環としてセキュリティ対策の必要性を訴求する	1
	(12) 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
	(13) 効果的な演習をする方法がわからない	演習実施部門と演習対象部門が協同して、演習内容を企画する	7
	(14) サプライチェーンの委託先企業がセキュリティ対策に協力的でない	相手先が自分事として対策を進めてもらえるよう、工夫や配慮を実践	9
リスク対策費用の確保	(15) 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
マルウェア対策	(16) ランサムウェア感染による事業停止を回避したい	ランサムウェア感染の可能性をゼロにできないことを社内で共有し、被害軽減策を準備	5
制御システムの対策	(17) 工場のサイバーセキュリティ対策が急務となっている	工場システムのネットワークにおける役割分担を明確にする	5
新しい働き方の対策	(18) テレワーク導入等の急激な環境変化に対応したセキュリティ管理規程に見直したい	新しい働き方に相応しい情報管理ルールを整備し、安全性と利便性を両立させる	5



## 悩み (1)

# 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

a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

### a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。

### a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



a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(1)

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)

a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a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】

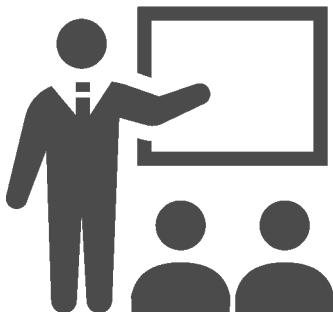
対象：ITやセキュリティ投資に係る役員

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



a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のプラクティス  
第3章

付録

## 悩み (2)

# 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

b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

### b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。

### b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



b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。

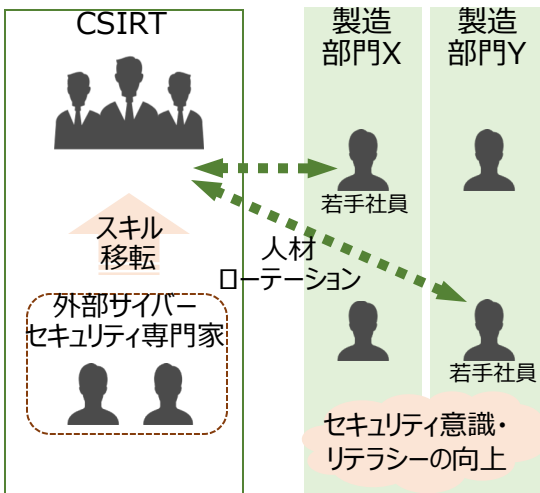
## 取組 (2)

# 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



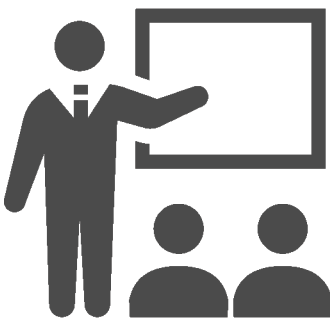
そこでb社は、**外部のサイバーセキュリティ専門家を活用しながら、自社でサイバーセキュリティ人材を育成**することを検討している。

- 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

担当者の悩みと取組のプラクティス 第3章

付録

## 悩み (3) 海外拠点のセキュリティ意識が低い

c社は近年、アジア各国を中心に生産拠点の海外展開を進めているが、国や地域により従業員のセキュリティ意識が低い拠点多く見られた。経営層は、海外拠点におけるセキュリティの確保に加え、対策が脆弱な海外拠点を踏み台にした本社への攻撃のリスクを低減するためにも、海外拠点のセキュリティ対策の強化が必要であると認識していた。

### 基本情報

#### c社の状況

- ✓ 現在、海外拠点には、グローバルポリシーで定めたベースライン（最低遵守事項）の遵守を求めている。
- ✓ なお、実施基準やセキュリティ製品の選定等は、法規制やビジネス習慣をふまえた各拠点の判断に委ねている。
- ✓ 本社より定期的にポリシーの遵守状況を確認し、遵守状況の良い拠点は表彰を行う運営としているが、依然として対応のレベルが低い拠点多くみられた。

#### c社のプロフィール

業種		製造業
規模		1,500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 主管部門	IT部門

### セキュリティ担当者の問題・悩み



経営層より、同業他社の海外拠点で発生したインシデントの事例を踏まえ、海外拠点のセキュリティ対策を強化するよう指示がなされた。

全ての海外拠点に、セキュリティの知見を有し、本社の指示のもとマネジメントを一任できるキーパーソンを配置することが理想であったが、海外拠点においてセキュリティの専門人材を確保し、定着させることは困難であった。

## 取組 (3)

# 対面のコミュニケーションを通じ、 セキュリティ意識を向上させる

## 解決に向けたアプローチ

c社の情報システム部は、海外拠点においてセキュリティ担当者を確保し、キーパーソンとして定着されるためには、本社と現地拠点との顔の見える関係作りや、セキュリティに対するモチベーションの向上が必要であると考えた。そこで、年に一度全拠点のセキュリティ責任者を本社等に招集し、取組状況を確認するセキュリティ連絡会を開催することにした。また、取組状況の悪い拠点（セキュリティに対する取組意識が低い拠点）については、拠点の担当者を日本に呼び寄せ、セキュリティやITに関するフォローアップを目的とした研修を受講させた。なお、セキュリティ担当者を配置できていない拠点等、直接的な支援が必要な拠点については、本社より担当者を派遣して直接支援を行った。また、互いの表情がわかるテレビ会議を活用し、定期的にコンタクトをとった。f社では、こうした対応について、グループ全社のガバナンスに必要な投資ととらえ、本社が負担して実施した。

### セキュリティ連絡会

- 各拠点の責任者を招集して実施
- 自拠点のグローバルポリシーの遵守状況を、責任者より発表
- 取組状況の良い拠点を表彰



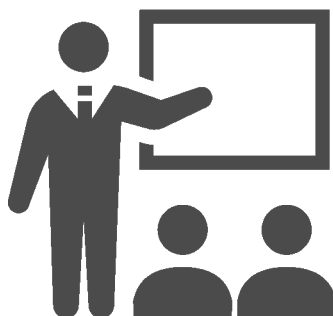
### 日本での研修受講

- 取組状況の悪い拠点のセキュリティ担当者を日本に招集
- 合同で、セキュリティやITに関する研修を受講させた



- ✓ セキュリティに対する意識やモチベーションの底上げ
- ✓ 海外拠点と本社のメンバー同士での、顔を突き合わせた交流による一体感の醸成

## 得られた知見



グローバル拠点におけるセキュリティ意識の向上においては、現地拠点のメンバーが、セキュリティに対してモチベーション高く取り組める仕組みを構築することが求められる。

また、セキュリティに関して共通の課題認識や目標感を共有するためには、顔を突き合わせたコミュニケーションや相互理解が重要となる。

はじめに

第1章

第2章

 担当者の悩みと取組のプラクティス  
第3章

付録



## 悩み (4)

# 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

d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

### d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。

### d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



d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

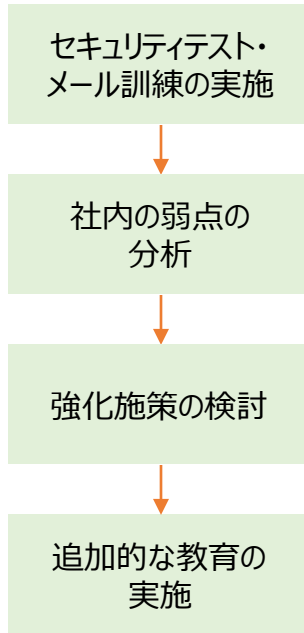
教育の効果については、情報セキュリティを担当する  
コンプライアンス部門、サイバーセキュリティを担当するIT部門ともに  
一定程度認めているものの、PCの紛失等のセキュリティインシデント  
が無くならない状況に問題を感じていた。

## 取組 (4)

# 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



そこでd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。

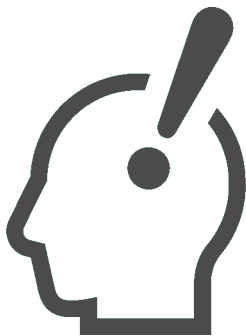
#### 【フォローアップの概要】

**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



d社のCISOは、取組のポイントとして、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

担当者の悩みと取組のプラクティス 第3章

付録

## 悩み (5) IoT機器が「シャドーIT」化している

e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

#### e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。

#### e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



e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 (5)

# 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

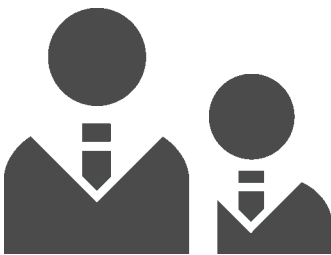
内部監査での指摘を踏まえ、e社は以下の対応を行った。

- IoT機器導入も、通常の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>36</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



e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のプラクティス

付録

<sup>36</sup> 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 (6)

# 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

f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

### f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。

### f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



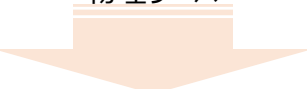
f社では自社で基幹システムを構築・運用している。しかし、日頃から**費用面の負担**だけではなく、IT部門の要員システムの調達、運用、保守にかけられる**人的資源が不足しており作業負担**が高くなっていた。

**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 (6)

## 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）自社内で構築された  
物理サーバ

クラウド環境上のサーバ群

そこでf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>37</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。

## &lt;移行時の考慮ポイントの例&gt;

- ・ 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>38</sup>の発行 等

## 得られた知見



f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のプラクティス 第3章

付録

37 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手引き <https://www.ipa.go.jp/files/000072150.pdf>

38 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 (7)

# 内部不正で情報漏えいが生じた場合の 自社事業への深刻な影響が心配

g社は自社が保有する製造技術やノウハウ等の営業秘密が企業価値の源泉となっており、その保護に多額の投資を行う一方、内部不正を通じた流出を懸念していた。

## 基本情報

### g社の状況

- ✓ 用途特化型の素材メーカー。競合他社にない製造技術が高く評価されており、グローバルでの市場シェアで業界有数。
- ✓ 製造技術やノウハウが海外の競合企業に漏えいした場合、利益減少や信用失墜による自社へのダメージのみならず、自社製品を利用して高品質の製品を製造している国内下流メーカーの競争力低下等、国内経済への影響も懸念される。

### g社のプロフィール

業種		製造業
規模		7,000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	情報セキュリティ 管理室

## セキュリティ担当者の問題・悩み



製造技術に関する営業秘密については、当該情報を管理している情報システムに対し、外部からのサイバー攻撃対策として、仮に従業員の端末やディレクトリサービスが乗っ取られても営業秘密に直ちにアクセス可能とならないよう、ネットワーク上で隔離管理を行っている。その一方で、悪意をもった従業員の内部不正による不正な取得・持ち出しについては、業務の実施過程において当該情報へのアクセスが必要な以上、完全に防ぐことは困難と考えている。

また、内部不正対策を厳しくし過ぎることで従業員が「自分が信用されていない」と感じ、かえってモチベーション低下を招いてしまうようなことも避けたい。

## 取組 (7)

# 内部不正を検知するための複数対策を組合せて導入し、周知により発生を抑制

### 解決に向けたアプローチ

g社のCISOは内部不正による営業秘密の流出防止対策<sup>39</sup>として次表の対策を定め、費用面の手当を含めて経営層の承認を得た。

#### g社が実施した内部不正対策に関する取組

目的	実施した事項
内部不正と思われるアクセスを早期に検知する	● 通常業務以外の異常なアクセスと疑われる操作をリアルタイムで検知できる仕組みを導入
不正なアクセスの証拠を保全する	● フォレンジックサービス事業者のアドバイスを受け、証拠保全性を考慮したログ管理を実践
自社から漏えいした情報であることがわかるようにする	● 営業秘密に関わる図面等への電子透かしの設定

対策の実施にあたってCISOが留意・工夫した点は次の通りである。

- 『サイバーセキュリティ関連法令Q&Aハンドブック』（NISC）<sup>40</sup>を参考に、営業秘密保護に関して留意すべき法令を抽出し、計画している対策が法令に抵触しないことを確認した。
- 従業員による営業秘密へのアクセスを対象とする常時（24時間365日）監視の導入にあたっては、会社や社員を守るための取組として導入することを社長から従業員等全社に伝えることとした。
- 他社における内部不正事例において、行為者が「気づかれずに持ち出せると思った」と考えて犯行に及ぶ例が多いことを踏まえ、複数の対策を組み合わせることで実施しているので、どこかで露見する可能性が高いことを、情報にアクセスできる全ての関係者にわかるように周知した。
- 社内コミュニケーションの問題が内部不正の原因となることも懸念されるため、上司や経営層が従業員の悩みや意見を聞く機会を積極的に創出することで、その解消に努めることとした。

### 得られた知見



内部不正による情報漏えいも近年のサイバー攻撃と同様、行為者が成功を期待して実施するものであり、その抑止には行為者に不正が必ず露見すると認識させることが重要である。これを踏まえると今後の技術の変化によってもその認識が維持されるよう、絶えず不正の可能性を想定していく必要があると考えている。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス 第3章

付録

<sup>39</sup> 内部不正による営業秘密の流出防止対策の検討にあたっては、以下の公表資料を参考にすることができる。

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/>

経済産業省：「秘密情報の保護ハンドブック」、「営業秘密管理指針」ほか営業秘密関連の基本資料

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

<sup>40</sup> NISC：サイバーセキュリティ関連法令Q&Aハンドブック [https://www.nisc.go.jp/security-site/law\\_handbook/](https://www.nisc.go.jp/security-site/law_handbook/)

## 悩み (8)

# 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

h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

#### h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。

#### h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



h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。

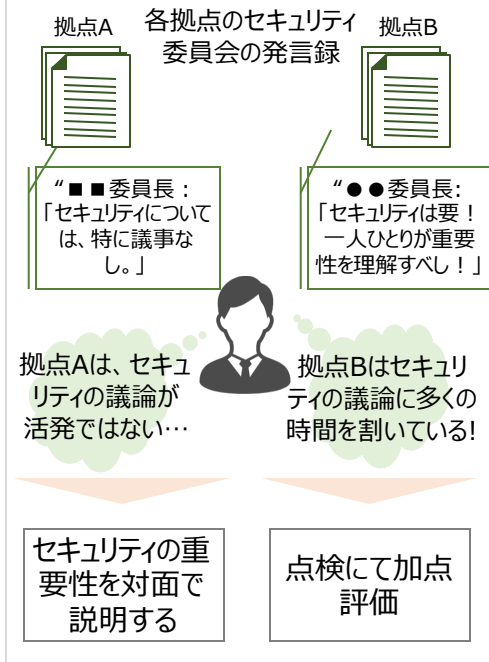
- ・ 遠隔地等の目の届きづらい拠点のサイバーセキュリティ管理の状況が、本社からは把握しづらく、管理状況に不安を感じている。
- ・ 全社セキュリティ委員会にて**年次**で各拠点のセキュリティ対策状況の**点検**を実施しているが、**点検項目だけでは実態が掴みづらい**。

## 取組 (8)

# 拠点におけるセキュリティの取組を把握し、対面で対話する

## 解決に向けたアプローチ

### 取組のイメージ



そこでh社は、各拠点での**セキュリティに対する取組状況や取組の姿勢を把握**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に対話し**、セキュリティの重要性を説明している。

## 得られた知見



h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のプラクティス

付録

## 悩み (9)

# 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 (9)

# 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

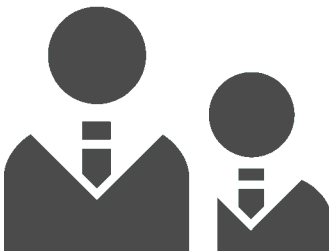
	所属人数	開封者	開封率	開封報告	報告率
部署A	56人	32人	57%	30人	94%
部署B	72人	21人	29%	5人	24%
部署C	45人	12人	27%	10人	83%
⋮	⋮	⋮	⋮	⋮	⋮

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のプラクティス 第3章

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

j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k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k社との取引に不安を感じていた。

### 基本情報

#### j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(人工知能)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状況をチェックシートで確認している。

#### j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



j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、k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、k社との取引が推奨できない状況であった。

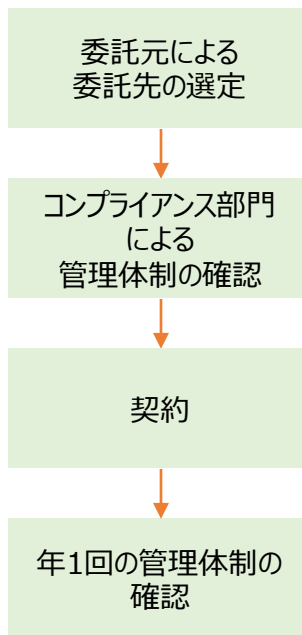
また、k社は即座に管理体制を充実させることは現実的でなく、IT部門の頭を悩ませていた。

## 取組 (10)

# セキュリティ対策の取組、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、j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k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、k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、k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、k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n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、k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



j社の取組のポイントは、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のプラクティス  
第3章

付録

## 悩み (11)

# 経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない

m社は、事業戦略としてEC事業への進出を企画しており、サイバーセキュリティの主管部門である情報システム部門は、セキュリティ強化の必要性を認識していた。しかし、EC事業を行う事業部門はECサイトを通じた売り上げ増加に注力しセキュリティ検討が後手になっており、情報システム部門は、経営層に対してその必要性を十分に伝えられていなかった。

### 基本情報

#### m社の状況

- ✓ 販売店による売り上げの減少を補うため、ECサイトを通じた直販を企画している。
- ✓ 同業他社でサイバー攻撃による情報流出が起き、事業部門もセキュリティ強化が必要と考えている。
- ✓ セキュリティ対策は自社の情報システム部門・担当者が全て行う事が当たり前となっており、経験や知見のある責任者がいない。
- ✓ 経営層は、セキュリティ対策によるサービスの開始遅延や追加コストを懸念している。

#### m社のプロフィール

業種		小売業
規模		300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門	情報システム部門

### セキュリティ担当者の問題・悩み



m社のサイバーセキュリティの主管部門である情報システム部門は、主に社内のIT機器の運用・サポートを担当しており、これまで、事業戦略の立案への関わりや、経営層へ報告を行う機会はほとんどなかった。

そのため、サイバーセキュリティ強化の必要性を、経営層に対してどのように伝えれば理解が得られるのかわからなかった。

## 取組 (11)

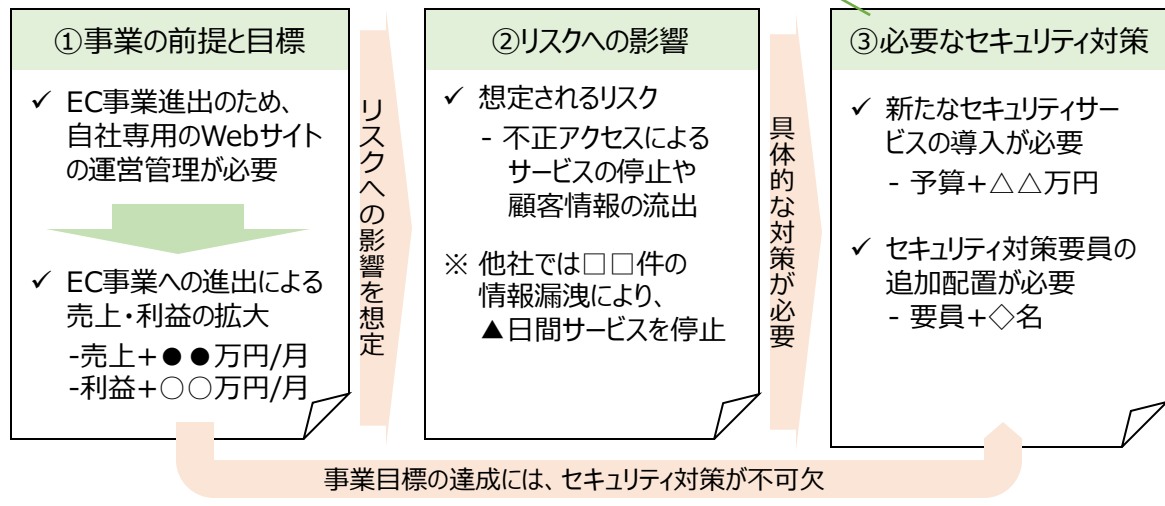
# 事業部門と協同し、事業戦略の一環としてセキュリティ対策の必要性を訴求する

### 解決に向けたアプローチ

そこでm社の情報システム部門は、EC事業を行う事業部門と協同し、経営層に対してサイバーセキュリティの必要性を訴求することにした。両部門の担当者が議論を重ねて、事業の目標や必要なセキュリティ対策を折り合わせ、事業の目標と整合したセキュリティ対策を取り纏めたうえ、事業戦略に関する報告の一環として、経営層に報告した。

#### 情報システム部門が事業部門と協同で行った経営層への報告例のイメージ

当初は③の内容のみを報告していたため、セキュリティ経費の納得感が得られなかった



こうした報告を継続して実施することで、経営層に対し、EC事業への進出（ビジネスモデルの変革）において、セキュリティ対策が不可欠であることを理解してもらった。なお、m社では、今回の対応を契機に、その後も、経営層に対して定期的にセキュリティに関する報告を継続している。

### 得られた知見



経営層に対し、サイバーセキュリティの必要性を理解してもらうためには、個々のセキュリティ対策のみを報告するのではなく、事業戦略の一環としてリスクと対策を整理し、報告することが重要である。

そのためには、サイバーセキュリティの主管部門と事業戦略を企画・立案する部門との密な連携が必要である。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス

第3章

付録

## 悩み (12)

# 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 (12)

# 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

担当者の悩みと取組のプラクティス  
第3章

付録



## 悩み (13) 効果的な演習をする方法がわからない

o社のシステム部門は、経営層より、セキュリティ対策の一環としてインシデントを想定した演習の実施を指示された。しかし、CSIRTを構築したばかりのo社ではこれまで演習を実施したことがなく、効果的な演習を行うために、どのように企画・運営を進めていけばよいかわからなかった。

### 基本情報

#### o社の状況

- ✓ 当初、システム部門単独にて、企画やシナリオの検討をおこなったが、演習に関する全般的なノウハウが不足していたことに加え、業務におけるシステムの利用実態や、セキュリティに関する課題についての理解も不足していた。
- ✓ 企画したシナリオを事前に事業部門等の他部門に報告したところ、「演習の趣旨や目的が不明瞭」「シナリオと業務との関連性が薄い」等否定的な反応をうけてしまった。

#### o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
	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門	システム部門

### セキュリティ担当者の問題・悩み



演習を形式的に実施しても効果は薄く、むしろシステム部門とその他の部門との溝を深めてしまうことになりかねない。

演習を通じて具体的な改善点が明らかとなり、全社を挙げて対策を推進していくためには、事業部門等の他部門も含む参加メンバーが現実的な危機感を共有し、効果を実感できるものとする必要がある。

## 取組 (13) 演習実施部門と演習対象部門が協同して、演習内容を企画する

### 解決に向けたアプローチ

そこで、システム部門は、演習の実施前（企画段階）において、専門のベンダのアドバイスを受けることにしたほか、参加メンバーと協同でシナリオを検討することにした。また、演習の実施時や実施後において、事務局と参加メンバー、または参加メンバー同士のコミュニケーションを深化する必要があると考えた。具体的には、経営層の協力も得ながら、以下の工夫を行った。

	工夫した内容	工夫による主な効果
実施前 （企画段階）	✓ 専門のベンダにアドバイスを依頼	✓ 効果的な演習シナリオの立案や、演習当日のファシリテーションの方法等について、実践的なノウハウが得られた
	✓ 他部門のメンバーと協同してシナリオの検討を実施	✓ 協同検討を通じ各部門の関心事項を把握し、シナリオに反映することができた。 事業部門：ECサイトへの攻撃による顧客情報の流出 法務部門：内部犯行による知的財産の流出 等
実施時	✓ 演習後に、参加メンバー間での振り返りを目的とした反省会を実施した	✓ 演習を通じて明らかとなった自身や組織の課題とその対応策について参加メンバーで意見交換を行うことで、メンバー同士での課題認識やノウハウの共有が図られたほか、一体感の醸成にもつながった。
実施後	✓ 改善策について、参加メンバーへフィードバックした	✓ 演習により明らかとなった課題について、その後実際に講じた対応策をフィードバックすることにより、参加メンバーが演習の効果を実感することができた。

こうした工夫を行ったことで、参加メンバーのモチベーションは向上し、演習に前向きに取り組む意識が醸成された。また、演習を通じて業務手順や体制の改善等に繋がる課題の抽出ができるようになった。

### 得られた知見



演習は、事務局による一方的な実施ではなく、他部門を含む参加メンバーと協同して企画・運営することが重要である。

参加メンバーと協同するためには、企画から振り返りまでの各プロセスにおいて、事務局と参加メンバー、または参加メンバー同士のコミュニケーションを活発化させる工夫が必要。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス 第3章

付録

## 悩み (14)

# サプライチェーンの委託先企業がセキュリティ対策に協力的でない

p社はサプライチェーン全体にわたるセキュリティ対策を推進する観点から、委託先企業に対して対策実施を要求しているが、重要な役割を担っている企業のうち、無視できない割合で消極的な企業が存在していることに悩んでいる。

### 基本情報

#### p社の状況

- ✓ 中堅の製造機器メーカー。最近はインターネット制御機器の展開も増やしている。
- ✓ 納入先は大手の電機メーカー、化学プラント等が中心。
- ✓ 素材加工や部品製造を委託している企業を100社以上抱えている。
- ✓ グローバルな業界再編等の動きを通じて、これまで取引のなかった企業との連携も発生している。

#### p社のプロフィール

業種		製造業
規模		3,000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	ITシステム部門 サイバーセキュリティ室

### セキュリティ担当者の問題・悩み



納入先企業からは、受注にあたりサプライチェーンを通じた再委託を行う場合には、再委託されることにより生じる脅威に対してセキュリティが十分に確保されることの担保を求められている。

一方で、委託先にセキュリティ対策を求めると、できない事情を挙げて拒否されたり、形だけの対策で済ませようとしたりなどで実効的な対策が進まない。

さらに、委託先にセキュリティ対策を要求する場合、その内容によっては下請法や独占禁止法に抵触する場合もあるとされていることも気になっている。

# 取組 (14) 相手先が自分事として対策を進めてもらえるよう、工夫や配慮を実践

## 解決に向けたアプローチ

p社のCISOは、経営者と相談の結果、委託先にそれぞれの事情があることを理解しつつ、各社が無理なく実施可能な形で必要な対策を実現するための方法として、次のような取組を行うことにした。

- 『サイバーセキュリティ関連法令Q&Aハンドブック』<sup>41</sup>『下請中小企業振興法第3条第1項の規定に基づく振興基準』<sup>42</sup>を参考に、委託先に対してサイバーセキュリティ対策を求めるにあたり、法令等に抵触する可能性のある行為を調査し、問題のない範囲を明確にした。
- サプライチェーン内の社長同士の会合において、s社の社長がIPAの公表資料等をもとに事業への具体的な負の影響を説明しながらセキュリティ対策の重要性を説き、賛同した社長の企業との間で共同でまず費用のかからない対策を導入することを決め、順次他の企業にも展開していくこととなった。
- 対策の実践を社外にアピールするとともに、社内への意識づけにも有効と期待されることから、IPAのSECURITY ACTION制度<sup>43</sup>での宣言実施を呼びかけた。
- 対策の普及にあたっては、次表のように「このような恐れがあるので、こうする必要がある」という具体例を示すことで、やってほしいことが明確にわかるように努めている。

### p社が作成したセキュリティチェックリストの抜粋

避けるべき問題	実施すべきことのチェックリスト
秘密情報が外部に漏えいする	✓ PCやモバイル機器の記録装置（SSD）が自動的に暗号化されるようにする
	✓ 関係者でのデータのやりとりはs社が提供するオンラインストレージを利用する
マルウェア感染して業務がマヒする	✓ 脆弱性対策をこまめに行う
	✓ 不審メールに関する情報を関係企業間で共有する
インシデントのとき連絡がとれずに被害が拡大する	✓ 日頃から顔の見える関係を築いておく
	✓ 定期的なインシデント対応訓練を共同で行う

## 得られた知見



お互いに余裕がない中ではあったが、必要なサイバーセキュリティ対策を講じておかないと、いざインシデントが発生したときに事業停止等で損害額が増大したり、自社の対策不備で他社に迷惑をかけたりする恐れがあることを根気よく説明した結果、相手先でも自分事としてとらえてもらえるようになり、着実に対策が進んでいることを実感している。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス 第3章

付録

41 NISC：サイバーセキュリティ関連法令Q&Aハンドブック [https://www.nisc.go.jp/security-site/law\\_handbook/](https://www.nisc.go.jp/security-site/law_handbook/)

42 中小企業庁：下請中小企業振興法第3条第1項の規定に基づく振興基準  
<https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm>

43 IPA：SECURITY ACTION制度 <https://www.ipa.go.jp/security/security-action/>

## 悩み (15)

# 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

q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

#### q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。

#### q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



q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こ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 (15) 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>44</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）

はじめに

第1章

第2章

 担当者の悩みと取組のプラクティス  
第3章

付録

<sup>44</sup> 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>

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 (16) ランサムウェア感染による事業停止を回避したい

r社は国内有名企業がランサムウェアに感染して事業に重大な支障が生じたとの報道に接し、自社でもいつ同様の状況になってもおかしくないと懸念していた。

### 基本情報

#### r社の状況

- ✓ 実店舗5店とオンラインショップを運営。
- ✓ 海外からの商品買い付けを電子メールを介して行うこともよくある。
- ✓ 売上データはPOSシステムベンダーの提供するSaaS型アプリで管理。
- ✓ 上記以外の仕入れや店舗間の情報共有のためのデータは、クラウドサービス上に構築した自社ファイルサーバ上に保存。
- ✓ ペーパーレス化した結果、クラウド上のデータが失われた場合の被害は深刻。

#### r社のプロフィール

業種		小売業
規模		1,000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システム部

### セキュリティ担当者の問題・悩み



海外の仕入れ先のうち、電子メールによるやり取りによらざるを得ないところも多く、その電子メール内には商品紹介ページへのリンクや、契約書の添付などもあり、サイバー攻撃目的の電子メールが紛れ込んでいても区別が困難な状況。海外の取引先が踏み台にされ、そこから詐欺メールが届いたこともあった。

そのような背景もあって、自社のデータがいつランサムウェア感染で暗号化されてしまっても不思議ではないと感じているが、社長に対策予算を要望しても、「ウイルス対策ソフトウェアを最新の状態にして、パッチも適用していればランサムウェアも防げるはず」と理解が得られていない。

# 取組 (16) ランサムウェア感染の可能性をゼロにできないことを社内で共有し、被害軽減策を準備

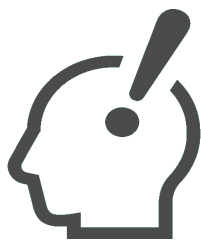
## 解決に向けたアプローチ

r社のCISOは、社長に対し、最新のマルウェア対策を実施していても、標的型攻撃等の手法により感染してしまうことが避けられず、ひとたび感染すると事業停止などの深刻な影響があることを他社事例を交えて説明し、次表の対策実施について、予算措置を含めて同意を得ることができた。

### r社が実施したランサムウェア対策に関する取組

	実施した対策	ランサムウェア対策としての有効性
運用系	通常のバックアップとは別に、週次で重要データを要員の手作業で保存し、通常時は電源を落としておくオンプレミスのストレージを確保	● 未知のランサムウェアに感染した場合でもバックアップの健全性を維持する
	ランサムウェア感染が疑われる挙動の検知の仕組みを導入するとともに、ファイルにアクセスできないなど、兆候と思われる挙動があればITシステム部に連絡して欲しい旨を従業員に通知	● ランサムウェアがすべてのデータを暗号化するまでに時間がかかるので、早い段階で認知することで被害を限定的なものにとどめる
教育系	海外との電子メールを扱う担当者（高リスク層）とそれ以外の従業員に分けて、それぞれの業務内容に応じて日頃意識すべき事項についての教育を実施	● 上記の対策を講じても、最終的に担当者による警戒に委ねざるを得ない部分も依然として存在するため、従来のマルウェア対策同様、継続的な意識向上を図る

## 得られた知見



ランサムウェアは以前から存在していたが、暗号資産（仮想通貨）の普及で身代金の回収が容易になったことと、犯行に見合うビジネス規模になったことから、ネットワークへの侵入を行う者、ランサムウェアを提供する者といった攻撃者における分業や組織化、攻撃の巧妙化により、最近の被害急増を招いている。また暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と二重に脅迫する攻撃もあって、機密性と完全性の両面にわたる脅威となっている<sup>45</sup>。

r社でもペーパーレス化が進み、電子データの消失や漏えいが生じた場合の事業への影響の大きさは従来とは比較にならない。r社のCISOはこうした事業を経営層に説明し、必要な予算の確保に理解を得ることができた。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス 第3章

付録

45 ランサムウェアに関する最新情報は以下のサイト等から入手できる。

NISC：ランサムウェア特設ページ <https://security-portal.nisc.go.jp/stopransomware/>

IPA：ランサムウェア対策特設ページ [https://www.ipa.go.jp/security/anshin/ransom\\_tokusetsu.html](https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html)

## 悩み (17)

# 工場のサイバーセキュリティ対策が急務となっている

s社では、これまで工場のサイバーセキュリティ対策はあまり意識してこなかった。しかし、DX<sup>46</sup>化推進の指示が工場にも及び、生産現場のセキュリティを含むIT化に悩みを抱えていた。

### 基本情報

#### s社の状況

- ✓ 工場で制御システムを運用している部門（以下、製造部門）は、IPプロトコルを利用する機器に対するリスクの評価を考える機会が不足している。
- ✓ 情報システム部門は制御システムを担当しておらず、工場内のIT資産の現状把握ができていない。
- ✓ s社経営層からDX化取組加速の通達が全社的に展開され、制御システムネットワーク見直しによる生産性向上が指示された。

#### s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
	専任のセキュリティ部署	有 (工場は未検討)
	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



これまでの事業に加え、DX化の取組として生産効率向上を進める際には工場内制御システムのIoT化促進のため、ネットワーク環境等を見直す必要がある。そのため、工場内のIT資産を早急に把握する必要があった。

しかしながら、DX化における工場のセキュリティについてはどの部門が対応するのか未検討の状態であった。

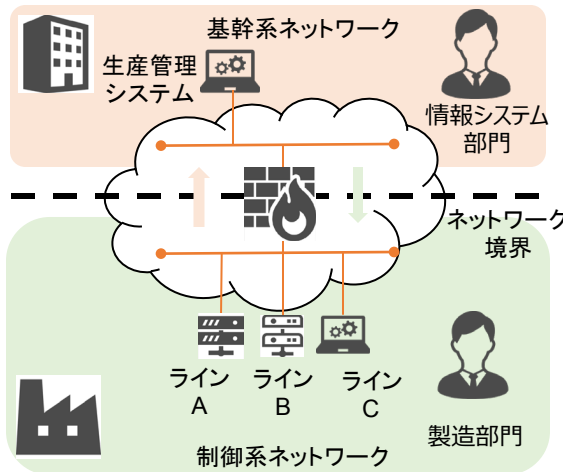
<sup>46</sup> デジタルトランスフォーメーション。企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること（経済産業省定義による）。  
<https://www.meti.go.jp/press/2018/12/2018121212004/2018121212004-1.pdf>

## 取組 (17)

# 工場システムのネットワークにおける 役割分担を明確にする

### 解決に向けたアプローチ

#### 工場における制御システムの ネットワーク境界（イメージ）



#### s社ネットワーク境界の役割分担例

- ・情シス部門：ファイアウォールのオーナー部門
- ・製造部門：ファイアウォールのセキュリティ設定※の実施部門  
(※IPアドレス、ポート番号、プロトコル、方向)

そこで、工場のDX化推進を任せられたp社工場の製造部門は、経営幹部にDX化に伴うセキュリティリスクを認識してもらった上で情報システム部門に働きかけを行い、DX化に向けた**工場側制御系ネットワークの把握**について協力を要請した。

両部門の課題認識は一致しているため、互いに協力して進めることになった。

最初の実践として、ベンダ協力のもと、情報システム部門の担当者が工場の生産現場担当者からヒアリングを行い、現状の**制御系ネットワークの構成図を作成**することから開始した。

これにより、脅威の起点となりやすい**ネットワーク境界を特定**し、境界の役割部門を明確化した。（境界には管理部門が不明な無線機器や事前申請不明なクラウド接続等があった。）

### 得られた知見



情報システム部門と製造部門との**連携が強化**したことで**コミュニケーションが活性化**し、セキュリティ対策の実施が可能となった。

工場内ITシステムの現状が把握でき、今後のDX化に向けて**検討のベースの整備**ができた。

今後は**ネットワーク境界以外の部分**に関しても**継続して検討**を進めたいと考えている。

はじめに

第1章

第2章

担当者の悩みと取組のプラクティス

第3章

付録

## 悩み (18)

# テレワーク導入等の急激な環境変化に対応したセキュリティ管理規程に見直したい

t社はテレワーク等で柔軟な働き方を推進する一方で、オフィス内での勤務を前提に設計した情報管理ルールが形骸化しているのではないかと危惧していた。

### 基本情報

#### t社の状況

- ✓ ある県庁所在都市を拠点とした物件を扱う県内大手の不動産事業者。
- ✓ 書面で扱うことが必要又は適切な場合を除き、業務文書のペーパーレス化を推進中。
- ✓ コロナ禍による緊急事態宣言発令前は顧客情報を扱う観点からテレワークを認めていなかったが、現在はVPNの利用を前提に在宅勤務を併用。
- ✓ 在宅から秘密情報の参照・編集を行うことも容認している。

#### t社のプロフィール

業種	不動産業
規模	800人
CISOの有無	有 (CIOと兼任)
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

### セキュリティ担当者の問題・悩み



テレワークの導入を機に在宅勤務だけでなく、不動産物件への往訪の多い営業担当者が外出先から会社支給のモバイルPC端末を用いてVPN経由で社内サーバ上の文書にアクセスできるようにした。

担当者からは好評ではあるが、個人情報等の秘密情報の管理に関して、自社の情報管理ルールでは社内の施錠可能なキャビネ又は社内ファイルサーバーに保管することを前提に、業務上必要最小限の範囲で持出しを許可するとしていたところ、テレワーク環境ではその前提が崩れてしまっている。一方で、テレワークの実践を通じて、電子データとして管理している秘密情報は、適切に管理すれば印刷物よりも保護しやすい面もあると感じている。

## 取組 (18)

# 新しい働き方に相応しい情報管理ルールを整備し、安全性と利便性を両立させる

## 解決に向けたアプローチ

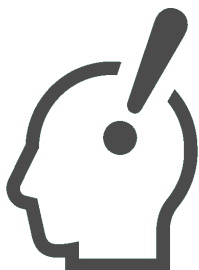
t社のCIOは、自社内での新しい働き方を踏まえたアプローチとして、試行を通じて事業への影響がないことを確認した上で、次のようなサイバーセキュリティ対策を講じることに関する経営者の承認を得た。

- 保護すべき秘密情報について、クラウド上に構築した自社ファイルサーバーに暗号化されて保管されている状態を標準とし、各文書の所有者（オーナー）、アクセス権限の付与手順、開示範囲等のルールを明確化。
- テレワーク環境等から文書アプリケーションを通じて直接その読み書きを行う場合、持出等の手続は不要とした。自宅での秘密情報の印刷は特別に許可された場合を除き禁止とした。
- リモートアクセスにおいて2要素認証（電子証明書、ワンタイムパスワード）を必須とするとともに、認証ログにおいて通常と異なる挙動（異常な時刻やアクセス先URL等）を不審なものとみなして自動的に検知し、警告が通知されるようにした。
- 公開資料<sup>47</sup>を参考に、VPNを経由せずテレワーク端末から直接クラウドサーバを利用するルールを整備し、安全性と利便性の双方を担保した。

### テレワークによる情報管理上のリスクとt社が実施した対策

主なリスク	左記リスクに対する対策方針
文書管理サーバに対する不正アクセス	<ul style="list-style-type: none"> <li>✓ 2要素認証を必須とすることによる認証の強化</li> <li>✓ 文書アプリケーションの暗号化機能を用いて権限外からの参照を防止</li> </ul>
従業員が利用するPCからの漏えい	<ul style="list-style-type: none"> <li>✓ EDR（Endpoint Detection and Response）を導入してデバイス（接続）制御、ログ監視、送信先チェックを実施</li> <li>✓ 端末の記録装置を暗号化し、盗難・紛失時の漏えいを防止</li> </ul>
通信ネットワーク経由の漏えい	<ul style="list-style-type: none"> <li>✓ クラウド型の文書管理アプリケーションが提供する暗号化機能により通信ネットワークからの情報漏えいを防止</li> </ul>

## 得られた知見



情報管理はあくまでセキュリティを確保するための手段であり、働き方が変化した以上はそれに見合った方法に見直す必要がある。

管理する側の都合を押しつけるのではなく、従業員が快適に利用できる環境の整備や使い勝手に配慮することで、情報管理に積極的に協力してもらえるような関係構築ができた。

はじめに

第1章

第2章


 担当者の悩みと取組のプラクティス  
第3章

付録

47 総務省：テレワークセキュリティガイドライン

[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)





## 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。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 ➤ 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
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 ➤ 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

## 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	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 ➤ 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
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、ボ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 (Command & Control)	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
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 ・ 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 ・ 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
DMZ (Demilitarized Zone)	外部ネットワークと社内ネットワークの中間に作られるネットワーク ➢ 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
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 ➢ 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
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 ➢ 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

# 付録

## サイバーセキュリティ対策の参考情報(1/5)

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>
情報セキュリティ10大脅威 2022	経営者、CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/vuln/10threats2022.html">https://www.ipa.go.jp/security/vuln/10threats2022.html</a>
サイバーセキュリティ関連法令Q&Aハンドブック	CISO等、セキュリティ担当者	内閣サイバーセキュリティセンター (NISC)	<a href="https://www.nisc.go.jp/security-site/law_handbook/">https://www.nisc.go.jp/security-site/law_handbook/</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="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</a>
付録F サイバーセキュリティ体制構築・人材確保の手引き	CISO等、セキュリティ担当者、人事担当者	経済産業省	<a href="http://www.meti.go.jp/policy/netsecurity/mng_guide.html">http://www.meti.go.jp/policy/netsecurity/mng_guide.html</a>
ITSS+ (セキュリティ領域)	CISO等、セキュリティ担当者、人事担当者	IPA	<a href="https://www.ipa.go.jp/jinzai/itss/itssplus.html">https://www.ipa.go.jp/jinzai/itss/itssplus.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2021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 (JNSA)	<a href="https://www.jnsa.org/result/skillmap/">https://www.jnsa.org/result/skillmap/</a>
CSIRT人材の定義と確保(Ver.2.1)	CISO等、セキュリティ担当者	日本シーサート協議会 (NCA)	<a href="https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf">https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf</a>
セキュリティ業務を担う人材のスキル可視化施策の考察～プラス・セキュリティ人材の可視化に向けて～	CISO等、セキュリティ担当者	情報セキュリティ教育事業者連絡会(ISEPA) JTAG認定WG	<a href="https://www.jnsa.org/isepa/images/outputs/JTAGreport2019.pdf">https://www.jnsa.org/isepa/images/outputs/JTAGreport2019.pdf</a>
攻めのプラス・セキュリティ人材でDX with Securityの実現を	CISO等、セキュリティ担当者	日本サイバーセキュリティ・イノベーション委員会 (JCIC)	<a href="https://www.j-cic.com/pdf/report/Proactive-Plus-Security-Human-Resources.pdf">https://www.j-cic.com/pdf/report/Proactive-Plus-Security-Human-Resources.pdf</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(2/5)

資料名	対象読者	発行元	URL
<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 (Ver1.0)	CISO等、セキュリティ担当者	経済産業省	<a href="https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html">https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html</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>
CISベンチマーク	CISO等、セキュリティ担当者	Center for Internet Security	<a href="https://www.cisecurity.org/cis-benchmarks/">https://www.cisecurity.org/cis-benchmarks/</a>
脅威分析法	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000046476.pdf">https://www.ipa.go.jp/files/000046476.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/vu/20150602-secop.html">https://www.ipa.go.jp/security/ciadr/vu/20150602-secop.html</a>
ランサムウェア特設ページ	CISO等、セキュリティ担当者	内閣サイバーセキュリティセンター (NISC)	<a href="https://security-portal.nisc.go.jp/stopransomware/">https://security-portal.nisc.go.jp/stopransomware/</a>
ランサムウェア対策特設ページ	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html">https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html</a>
侵入型ランサムウェア攻撃を受けたら読むFAQ	CISO等、セキュリティ担当者	JPCERT/CC	<a href="https://www.jpcert.or.jp/magazine/security/ransom-faq.html">https://www.jpcert.or.jp/magazine/security/ransom-faq.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/measures/everyday.html">https://www.ipa.go.jp/security/measures/everyday.html</a>
テレワークセキュリティガイドライン	CISO等、セキュリティ担当者	総務省	<a href="https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/">https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/</a>
テレワークを行う際のセキュリティ上の注意事項	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/announc/telework.html">https://www.ipa.go.jp/security/announc/telework.html</a>
Web会議サービスを使用する際のセキュリティ上の注意事項	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/announc/webmeeting.html">https://www.ipa.go.jp/security/announc/webmeeting.html</a>
営業秘密 ～営業秘密を守り活用する～	CISO等、セキュリティ担当者	経済産業省	<a href="https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html">https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html</a>
組織における内部不正防止ガイドライン	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/fy24/reports/insider/">https://www.ipa.go.jp/security/fy24/reports/insider/</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>
サイバーセキュリティ経営可視化ツール	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/economics/checktool/index.html">https://www.ipa.go.jp/security/economics/checktool/index.html</a>
SECURITY ACTION制度	CISO等、セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/security-action/">https://www.ipa.go.jp/security/security-action/</a>
サイバーインデックス企業調査2021	CISO等、セキュリティ担当者	日本IT団体連盟 サイバーセキュリティ委員会	<a href="https://www.itrenmei.jp/topics/2021/3700/">https://www.itrenmei.jp/topics/2021/3700/</a>

# 付録

## サイバーセキュリティ対策の参考情報(3/5)

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.2.1)	CISO等、 セキュリティ担当者	日本シーサート協議会 (NCA)	<a href="https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf">https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.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8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/home-act-products-df-guideline-8th/">https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/</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>
サイバーセキュリティお助け隊サービス	CISO等、 セキュリティ担当者	IPA サービス提供事業者	<a href="https://www.ipa.go.jp/security/otasuke/etai-pr/">https://www.ipa.go.jp/security/otasuke/etai-pr/</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>
下請中小企業振興法第3条第1項の規定に基づく振興基準	CISO等、 セキュリティ担当者	中小企業庁	<a href="https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm">https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm</a>
クラウドサービス安全利用の手引き	CISO等、 セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/files/000072150.pdf">https://www.ipa.go.jp/files/000072150.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>
米国情報共有分析機関(ISAO)関連文書の翻訳(情報共有入門、分析入門等)	CISO等、 セキュリティ担当者	IPA	<a href="https://www.ipa.go.jp/security/publications/isao/index.html">https://www.ipa.go.jp/security/publications/isao/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(4/5)

### 【情報共有コミュニティ】

情報共有 コミュニティ	対象者	活動概要	設立 (年/月)	URL
業界ISAC (Information Sharing and Analysis Center)	各業界関連事業者	各業界の民間事業者同士でセキュリティ情報の共有、分析対策検討。 金融ISAC <a href="http://www.f-isac.jp/">http://www.f-isac.jp/</a> 電力ISAC <a href="https://www.je-isac.jp/">https://www.je-isac.jp/</a> ICT-ISAC <a href="https://www.ict-isac.jp/">https://www.ict-isac.jp/</a> 交通ISAC <a href="https://t-isac.or.jp/">https://t-isac.or.jp/</a> 医療ISAC <a href="https://www.m-isac.jp/">https://www.m-isac.jp/</a> J-Auto-ISAC (自動車) <a href="https://j-auto-isac.or.jp/">https://j-auto-isac.or.jp/</a> 日本貿易会ISAC (商社) <a href="https://www.jftc.or.jp/shosha/isac/">https://www.jftc.or.jp/shosha/isac/</a> ソフトウェアISAC <a href="https://www.sai.or.jp/activity/project/softwareisac/">https://www.sai.or.jp/activity/project/softwareisac/</a>	(業界により異なる)	(左記に記載)
J-CSIP (サイバー情報共有イニシアティブ)	重要インフラ機器製造業者	サイバー攻撃等の情報を集約、分析、匿名化し情報共有。IPAが事務局。	2011/10	<a href="https://www.ipa.go.jp/security/J-CSIP/">https://www.ipa.go.jp/security/J-CSIP/</a>
セプターカウンシル	重要インフラ事業者	情報セキュリティ対策向上のため、分野横断的な連携推進。各重要インフラ14分野の業界団体等が事務局。	2009/2	<a href="https://www.nisc.go.jp/active/infra/shisaku2.html">https://www.nisc.go.jp/active/infra/shisaku2.html</a>
サイバーセキュリティ協議会	行政機関、重要インフラ事業者、サイバー関連事業者、大学等	官民の多様な主体の連携による、迅速な脅威情報等の共有・分析、対策情報等の作出・共有。NISCおよびJPCERT/CCが事務局。	2019/4	<a href="https://www.nisc.go.jp/conference/cs/kyogikai/index.html">https://www.nisc.go.jp/conference/cs/kyogikai/index.html</a>
サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3)	コンソーシアムの目的及び事業に賛同する法人その他の団体等	中小企業を含めた日本の産業サプライチェーン全体でのサイバーセキュリティ対策を促進することを目的とした、情報共有・報告・公表等の促進、関連する取組の検討・推進、情報の収集・発信、普及・啓発等を実施。IPAが事務局。	2020/11	<a href="https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html">https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html</a>
CSSC (技術研究組合制御システムセキュリティセンター)	制御システムセキュリティに関連する企業・大学等	重要インフラ制御システムセキュリティについて研究開発、人材育成、普及啓発。国際規格の整備・提案、国際規格準拠認証、インシデント対策サポート。	2012/3	<a href="http://www.css-center.or.jp/index.html">http://www.css-center.or.jp/index.html</a>
日本シーサート協議会	組織のCSIRT	インシデント関連情報の収集、分析、対応方針や手順の策定。組織内CSIRT設立支援、インシデント対応共同演習、各種ワークショップの開催。	2007/3	<a href="https://www.ncagr.jp/">https://www.ncagr.jp/</a>

## 【情報共有コミュニティ】

情報共有 コミュニティ	対象者	活動概要	設立 (年/月)	URL
JNSA（日本 ネットワーク セキュリティ協会）	JNSAの目的に 賛同する組織、 個人	ネットワークセキュリティに関する啓発、教育、調査研究及び 情報提供。各部会・WGに分かれ活動。	2001/5	<a href="https://www.jnsa.org/">https://www.jnsa.org/</a>
フィッシング 対策協議会	フィッシング攻撃 対象・防御手段 を提供し得る 組織、個人	フィッシングに関する情報収集・提供、動向分析、技術・ 制度的対応の検討。対策ガイドラインや動向レポートの 作成。JPCERT/CCが事務局。	2005/4	<a href="https://www.antiphishing.jp/">https://www.antiphishing.jp/</a>
CSAジャパン（日本 クラウドセキュリティ アライアンス）	CSAジャパンの 目的に賛同する 組織、個人	クラウドのセキュリティに関する情報発信、調査研究と提言、 教育活動。米国Cloud Security Alliance（CSA）の 公認日本支部。	2010/6	<a href="https://www.cloudsecurityalliance.jp/">https://www.cloudsecurityalliance.jp/</a>
FIRST (Forum of Incident Response and Security Teams)	組織のCSIRT、 FISRTに関心を 持つ個人	国際的な CSIRT 相互の情報交換やインシデント対応に 関する協力関係を構築。事例ごとのベストプラクティスや CSIRT・PSIRTのサービスフレームワークも提供。	1990	<a href="https://www.first.org/">https://www.first.org/</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)

氏名（敬称略）	所属・役職（いずれも就任時）
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 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 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  
セキュリティセンター 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(第1版)  
株式会社NTTデータ経営研究所 金融政策コンサルティングユニット(第2版)  
みずほリサーチ&テクノロジーズ株式会社 経営・ITコンサルティング部 (第3版)





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:03-5978-7530 FAX:03-5978-7513

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