TANIUM

TANIUM

# IT担当者のための「サイバー防災」ハンドブック

楢原 盛史　坂本 祐一
高崎 直人　三浦 貴将 監修

# はじめに

タニウムは、2023年に「Taniumで始めるサイバーセキュリティ サイバーハイジーン徹底解説」（タニウム合同会社 著）、2024年には「経営者のためのサイバーセキュリティ講義　サステナブルサイバーセキュリティ」（楢原 盛史 著）を出版し、企業のセキュリティ対策とそれにおけるサイバーハイジーンの重要性を、技術的な観点や経営層の視点から解説してきました。

本冊子では、これらの書籍をもとに、現場でIT運用やセキュリティ運用に関わっている方々に向けてサイバーハイジーンの定義と要点についてご紹介しています。サイバーセキュリティの取り組みを日本人に馴染みの深い「防災」と「減災」に例え、サイバーハイジーンという言葉を初めて聞く方にもより分かりやすい表現になるよう努めました。

2024年に発表された「金融分野におけるサイバーセキュリティに関するガイドライン」でもサイバーセキュリティに関する基本的な対応事項のひとつとして紹介されるなど、サイバーハイジーンは現代のサイバーセキュリティを考える上で重要なキーワードです。本冊子が、読者の皆様の組織におけるサイバーセキュリティ強化へのヒントをもたらすことができれば幸いです。

タニウム合同会社
**楢原 盛史　　坂本 祐一　　高崎 直人　　三浦 貴将**

# 1 サイバーセキュリティで注目が高まる「防災」

## サイバーセキュリティの世界における**「防災」とは何か？**

「ボヤの火種を作らない」のが防災、「ボヤを早く消火する」のが減災

▶ **自然災害と同様に、サイバー災害に対しても「攻撃の標的となり得る前提」で備える**

全ての攻撃を防ぐことは不可能。詐欺メールは「必ず誰かがクリックする」

▶ **だからこそ、攻撃を受けても被害を発生させないために「日常から備え」を**

サイバー防災の手法は「IT 資産管理」「構成管理」「脆弱性管理」

▶ **３つを徹底することを「サイバーハイジーン」と呼ぶ**

## 「攻撃の標的となり得る前提前提」で考えるサイバー防災

かつて「防災」といえば、地震や台風、火災といった自然災害に備えることを意味していました。日本は災害大国であり、個人も企業も「攻撃の標的となり得る前提」で災害に備える文化を育んできました。しかし近年、もう一つの災害が静かに、そして確実に私たちの社会と経済に深刻な影響を与えつつあります。それが、IT領域におけるサイバー災害です。サイバー攻撃による情報漏えいやシステム停止、業務停止、ブランド毀損――これらはもはや情報システムの問題にとどまらず、「経営のリスク」であり、社会インフラそのものを脅かす存在です。こうした状況下で、IT担当者や経営層に求められるのが、「サイバー防災」という新しい視点です。

## 防災と減災 ――その本質的な違い

自然災害対策では、「防災」と「減災」は明確に使い分けられています。前者は「被害を未然に防ぐ」こと、後者は「発生した後の被害を最小限にとどめる」ことを意味します。例えば、建物の耐震化や避難訓練は「防災」であり、地震後のライフライン復旧や避難所運営は「減災」に該当します。個人の対応に例えると、グラグラした家具を倒れないように金具で固定をしたり、ハザードマップを準備し、倒壊の危険性がある建物を把握して避難経路を確保したりするのが「防災」です。ライフラインが止まった場合に、常備したモバイルバッテリーやガスコンロを利用したり、予め常備している食料を食べたりすることで、日常生活におけるインパクトを最小化する考え方が「減災」です。

サイバーセキュリティの世界でも同様です。これまでの多くの企業では、サイバー災害が発生した後の対応(減災)に重点が置かれてきました。たとえば、インシデント対応フローの整備やログの保存、フォレンジック調査の準備などは、「火事が起きた後、いかにインパクトを最小化するか」を考えるアプローチです。

しかし本来、最優先されるべきは「そもそも火事を起こさない」ための対策、すなわち「ボヤの火種を作らない」こと、つまり「防災」です。自然災害と同様に、サイバー災害も「攻撃の標的となり得る前提」で備えることが求められます。そのためには、リスクの芽を摘み取り、日々の運用の中でサイバー上の火種を一つでも多く消しておく必要があります。

## 「サイバー防災」は日常の運用に組み込まれていることが重要

サイバー災害に対する「防災」は、一度限りの計画や単発の対策ではなく、企画設計フェーズからセキュリティ対策を組み込んでおくセキュア・バイ・デザインの考えと等しく、日々の運用の中に組み込まれる必要があります。そこで重要になるのが、「IT資産管理」「構成管理」「脆弱性管理」の3つの領域です。

これらを徹底することで、企業全体のIT環境を常時健全に保つことが可能になります。サイバー空間を人間社会に例えると、常にモニターで空気中に含まれる病原体をチェックし、空気清浄機で空気中の衛生管理を行い、うがい手洗い、マスク、アルコール消毒などを定期的に実施することで病気などにかかりにくい状態を維持すること、であると言えます。このような状態をサイバーハイジーン(Cyber Hygiene)が徹底されている、と表現します。サイバー空間における防災では最も基本の考え方です。

### 1. IT資産管理

「見えないものは守れない」という言葉がある通り、まずは「何が存在しているのか」を常時正確に把握することが出発点です。管理されていない端末やソフトウェアは、攻撃者にとって格好の標的となります。こうした「見えない資産」を可視化し、常時監視下に置くことが、火種を作らないための基本です。

### 2. 構成管理

次に、「どのような構成なのか」を常時把握し、設定が適切かを継続的に管理する必要があります。脆弱なOSバージョンやセキュリティ機能オフなどの不適切な設定などは、攻撃者が最初に狙うポイントです。継続的な構成管理の徹底により、脆弱な状態を未然に是正できます。

### 3. 脆弱性管理

最後に、判明している脆弱性に対する迅速な対応が不可欠です。脆弱性を日々可視化して速やかに是正する仕組み(脆弱性管理ライフサイクル)を整備します。可視化された脆弱性に対してパッチ適用や設定変更、バージョンアップ等で是正するというサイクルを継

続することで、脆弱性の「放置」を最小限に抑えることができます。

この3つを徹底すれば、攻撃を受けたり侵害されたりしてしまう可能性を格段に下げることが可能になります。すなわち、「サイバー防災」の要諦は、「備えを積み重ねる日常そのもの」にあるのです。結果として経営目線で考えると、単発で終わらせない継続可能（サステナブル）なサイバーセキュリティの実現は、情報システム部門が各ビジネス部門や経営陣を巻き込んで進めていくものであるといえます。

# 「サイバー防災」と「サイバー減災」

## サイバー防災

サイバー攻撃の標的となり得る前提で、**被害の「発生そのものを防ぐ」ことを目的とした取り組み**です。

## サイバー減災

万が一サイバー攻撃が成功した場合でも、その**被害を「最小限にとどめる」ことを目的とした対策**です。

### 自然災害に置き換えると？

たとえば地震を例に考えてみましょう。

【防災】
家具の転倒防止、
ハザードマップの準備

【減災】
実際に地震が起きた後の避難行動、
応急手当、火災消火

### 言い換えると？

**サイバー防災 ≒ サイバーハイジーン**

IT 資産管理、構成管理、
脆弱性管理などを通じた
「平時の備え」

**サイバー減災 ≒ サイバーレジリエンス**

インシデント対応力の強化や
業務継続（BCP）に向けた
「有事の対応力」

### 具体的にはどんな対策？

| 区分 | 主な対策内容 |
|---|---|
| **サイバーハイジーン（防災）** | 全IT資産の可視化と管理、脆弱性の是正、パッチ適用、非管理端末の撲滅、設定ポリシーの徹底 |
| **サイバーレジリエンス（減災）** | 各種セキュリティツールによる検知と隔離、インシデント対応、復旧および復旧体制の整備 |

# サイバーセキュリティの原理・原則


※ 組織が予め定義した端末／ソフトウェア／設定状態／脆弱性／管理者権限の実態

# 2 なぜ「サイバー防災」が今、重要視されているのか？

**なぜ「サイバー防災」が今、重要視されているのか？**

後追いでは限界がある。「ボヤの火種を作らない」ことが重要

▶**「減災」中心の考えから脱却し、「防災」にも力を入れるべきと考える**

真っ先に「シャドーIT」と脆弱なパスワードが狙われる
防災の弱さにより減災にかかる時間とコストが増えてしまう

▶**見えないものは守れない。IT資産の可視化を徹底する**

減災対策は一巡
侵害や攻撃の検知から始まる対策では防ぎきれないセキュリティの限界が明らかに

▶**グローバル基準における防災の中核は「シフトレフト」「セキュア・バイ・デザイン」へ**

## 後追いでは限界がある。「ボヤの火種を作らない」ことが重要

サイバー攻撃は、地震や台風のように自然発生的に起こるものではなく、攻撃者が意図的・計画的に引き起こす人為的災害です。攻撃者は脆弱なポイントを探し、わずかな隙をついて組織内に侵入してきます。そして一度侵入が成功すれば、そこから被害が急速に拡大するという特徴を持っています。

このような攻撃に対して、侵害や攻撃の検知から始まる減災型のアプローチには限界があります。インシデント対応のマニュアルを整備し、ログを記録し、迅速に報告体制を整えたとしても、すでに機密情報が漏えいしていたり、システムが停止していたりすれば、その損失は取り返しがつきません。現実に、多くの企業が「気づいたときには手遅れ」という状況に直面しています。

だからこそ、今求められているのは「防災」の視点です。火が燃え広がった後の消火活動（減災）ではなく、そもそもボヤの火種を作らないという「未然の備え」が、最も重要なセキュリティ施策として位置づけられ始めました。

たとえば、継続的なIT資産の棚卸や、セキュリティパッチの適用、不要なアカウントや権限の削除といった取り組みは、目立たず地味ではあるものの、攻撃の火種

を取り除く確実な手段です。防災とは、こうした日々の運用の徹底であることは、前述のとおりです。

## シャドーITの脆弱性が狙われている。防災の弱さが減災を無効化する

現在、多くの企業において、IT担当者が把握していない資産、すなわち「シャドーIT」の存在が深刻な問題となっています。従業員が個人の判断で導入したアプリケーションやデバイス、管理対象外のまま放置された旧システムなどは、脆弱性の温床となりやすく、サイバー攻撃者にとっては格好の侵入口です。

たとえば、クラウドサービスの利用が増える中で、正式な手続きを経ずに導入されたSaaSツールや、パッチのあたっていないテスト用サーバなどが社内ネットワークに存在していた場合、それが「裏口」として攻撃者に悪用される可能性があります。しかもこれらは、通常の管理体制の目が届かないため、攻撃を受けてもすぐには気づけません。

このような「見えない脆弱性」が存在する状態では、たとえ高度な検知ツールや迅速な通報体制を整えていても、攻撃を完全に防ぐことはできません。防災の甘さが、減災対策そのものを無効化してしまう――これが、現代のセキュリティにおける最も厄介な課題の一つです。

だからこそ、サイバー防災の第一歩は、「見えないものをなくす」こと。つまり、IT資産の可視化を徹底することです。全社の端末やソフトウェア、アカウント、ネットワーク機器を一元的に管理し、リアルタイムで監視する体制を築くことが、あらゆるサイバー防災の出発点となります。

## 減災対策は一巡。「シフトレフト」「セキュア・バイ・デザイン」へ

近年、世界的なセキュリティの潮流として注目されているのが「シフトレフト（Shift Left）」と「セキュア・バイ・デザイン（Secure by Design）」という考え方です。

NIST（National Institute of Standards and Technology：米国立標準技術研究所）のサイバーセキュリティフレームワークによると、セキュリティ運用のフローは以下の5手順に分別されます。

**特定：** IT資産の把握、脆弱なポイントの把握、脅威情報を利用可能にしておく

**防御：** 脆弱なポイントを是正しておく

**検知：** アノーマリや不審な兆候、あるいは侵害・攻撃そのものを検知する

**対応：** 攻撃、インシデント発生の影響に対応し、影響を極小化する

**復旧：** 環境を攻撃、インシデント発生以前の状態に戻す

これを左から順番に以下のように定義しています。

**特定 → 防御 → 検知 → 対応 → 復旧**

既存の考え方では、検知、対応(右側)に重きが置かれていましたが、特定、防御(左側)に重きが置かれ始めている、というのが現在のトレンドです。これを左側にシフトする、を意味する「シフトレフト(Shift Left)」と呼びます。

シフトレフトはインシデント発生前に対処を行うことから、事後対応を減らすことが可能なため、低コストでリスクを低減することができ、注目が集まっています。

現在のサイバー攻撃は、極めて短時間で侵入・拡散・情報奪取が行われます。「気づいた時にはもう遅い」という事態を防ぐためには、侵害や攻撃の検知や対処(=右側)に偏った対策では間に合いません。これを「攻撃の標的となり得る前提で、攻撃が成立しないよう備える」という考え方が必要です。また、セキュリティ対策は、早い段階で行えば行うほどコストが安く、効果も高いという特徴があり、低コストで高リスクを防ぐという観点でも「シフトレフト」の考え方に注目が集まっています。

一方のセキュア・バイ・デザインは、製品やサービス、システムを企画・設計する段階からセキュリティ要件を組み込むというアプローチです。「完成後、利用段階でのみ守る」のではなく、「設計段階から攻撃が成立しないように備える」という思想は、そもそも災害(インシデントや攻撃被害)の発生を防ぐ、という防災の本質そのものであり、企業のあらゆるデジタル施策に組み込まれるべきだ、という考え方がソフトウェア開発部門で始まり、現在は利用者であるユーザー部門まで広まっています。

この2つのキーワードは、「火がついてから消す」のではなく、「そもそも火種をつくならい設計をする」というサイバー防災の本質を表すものといえます。

こうした考え方は、すでに欧米を中心とした企業や政府機関で導入が進んでおり、「減災」偏重から「防災」重視へのシフトが明確に起きています。つまり、サイバーセキュリティはもはや「運用部門だけの課題」ではなく、企画・設計・経営判断にまで組み込まれるべきものだという認識が広がっているのです。

## サイバー防災は「経営戦略」である

サイバー攻撃によって被る影響は、情報漏えいや業務停止にとどまりません。近年では、ブランド毀損や株価下落、訴訟リスク、さらにはESG評価の低下といった「非財務リスク」が、企業の価値に直接影響を与えることが明らかになっています。ESGとは、Environment、Social、Governanceを指します。この中で特にサイバー防災と関係が深いのがG(Governance)です。企業のサイバーセキュリティ対策は、情報資産

の保護やリスク管理体制の一部として評価される項目であり、近年ではESG投資家や格付け機関がその取り組みの有無を評価対象としています。なお、前述のNISTのサイバーセキュリティフレームワークにおいて、2024年11月に改訂されたバージョン2.0では新たにGovernance がプロセス全体を包含する観点として追加されています。グローバル標準の考え方としてGovernanceは改めて重要度が増しています。

こうしたリスクに対し、防災的な取り組みは企業の持続可能性を支える柱となります。実際に欧州をはじめとしたグローバル市場では、サイバーセキュリティへの取り組みが投資判断の材料とされることも珍しくありません。

このように、サイバーセキュリティにおける防災は単なるIT施策ではなく、経営そのものを守る戦略的な取り組みとして位置づける企業が増えています。そのためにも、経営層と現場が一体となって、システム設計・業務設計・リスク管理のあらゆる場面で、防災視点を持ち込むことが求められます。

# 3 サイバー災害の実態を知る

## サイバー攻撃は**いつどうやって**起こるのか

ステップ型の攻撃プロセスが存在する
=「脆弱性の探索→マルウェア感染→アクセス権限の窃取→管理者権限の乗っ取り→情報の公開・金銭要求」

▶ **各段階に対する技術的・組織的対策を考える**

フィッシングメールで人の心理に働きかけ、シャドーITを突いて侵入

▶ **人とシステム両方の脆弱性が狙われる**
**従業員教育と、IT資産の脆弱性管理の両軸で備える**

攻撃スピードは極めて速く「気づいてからでは遅い」

▶ **常時監視と、即時検知・初動対応体制が重要**

## 攻撃は「ある日突然」ではない

多くのIT担当者が日々直面するセキュリティの脅威。その中でも「サイバー攻撃」は、自然災害のように「ある日突然」やってくる――そう思われがちです。しかし、実際には攻撃者たちは周到な準備と明確なプロセスをもって侵入・拡散・乗っ取り・脅迫を行っています。サイバー攻撃は突発的なイベントではなく、明確な「段階(ステップ)」を持って進行していく「人災」です。本章では、サイバー攻撃がどのようなプロセスをたどって組織を侵害していくのかを説明します。

## サイバー攻撃は5つのステップで進む

サイバー攻撃のプロセスは、以下の5つの段階に分けることができます。

ステップ1：脆弱性の探索
▼
ステップ2：マルウェア感染（ウイルスなどの仕込み）
▼
ステップ3：アクセス権限の窃取
▼
ステップ4：管理者権限の乗っ取り
▼
ステップ5：機密情報の公開・金銭要求

これらはまるで犯罪の設計図のように整っており、攻撃者が順を追って確実に支配領域を広げていく過程です。

このステップ型プロセスに対しては、それぞれの段階ごとに技術的・組織的な対策を講じることが極めて重要です。たとえば、入口の探索に対してはIT資産の可視化と構成管理、感染段階ではEPP（Endpoint Protection Platform）/EDR（Endpoint Detection and Response）による端末監視、権限の窃取には多要素認証やパスワードポリシーの強化などが求められます。また、情報公開を防ぐためには、インシデント対応フローやバックアップ体制の事前整備が必要です。

**ステップ1：脆弱性の探索**

すべてのサイバー攻撃は「入口」を探すところから始まります。攻撃者はターゲット企業のネットワーク上に存在するスキを見つけようと、日々インターネット越しにスキャンを繰り返しています。

たとえば、以下のような「脆弱な資産」がターゲットになりやすいものとして挙げられます。

- Windows Server 2012など、既にサポート切れとなったOS
- VPNやNAS、業務ごとに導入したSaaSなど、IT部門が管理していないシャドーIT
- 長期間パッチ未適用のWebアプリケーション

特にシャドーITは、可視化されていないためにIT部門が対応しきれず、常に高リスクな状態にあります。システムとしての脆弱性だけでなく、「気づかれていない」という事実そのものが最大の穴となります。

**ステップ2：マルウェア感染（ウイルス等の仕込み）**

侵入経路が特定されると、次に行われるのは「仕掛け」です。攻撃者はマルウェアをターゲット端末に送り込み、足がかりを作ります。

この段階では、システム面の脆弱性と同じくらい、「人の脆弱性」も狙われます。特にフィッシングメールや悪意ある添付ファイルなどは、日常の業務に巧妙に溶け込んでおり、心理的なスキを突いてきます。たとえば以下のようなものが対象となります。

- 「上司からの急ぎの依頼」メールに添付された見積書ファイル
- 「税務署からのお知らせ」メールのリンク先が偽装サイト

こうした攻撃は、技術的なガードだけでは防ぎきれず、従業員一人ひとりのセキュリティリテラシーが試されます。従業員教育とフィッシング訓練の定期的な実施が欠かせません。また、近年ではフィッシングメールの完成度も高くなっており、完全に防ぐことはますます困難となっています。

### ステップ3：アクセス権限の窃取

マルウェアの感染が完了すると、次に攻撃者は「認証情報の収集」に移行します。ここで狙われるのは、ログインID・パスワード・トークン・クッキーなどの「アクセスの鍵」です。

特に脆弱なパスワードは狙われやすく、単純なパスワードや、使い回しのパスワードは格好の標的です。「社内のWi-Fiに“12345678”で接続できる」「社員共通の管理パスワードがある」といった運用実態は危険信号です。

攻撃者はこうした情報をもとに、次々と社内システムにアクセスし、横移動を繰り返しながら権限をエスカレーションさせてより強い影響力を得ていきます。

### ステップ4：管理者権限の乗っ取り

ステップ4はゴール目前のステップです。ここまで来ると、攻撃者は組織のITシステムを自由に操作できる「管理者（ドメインアドミン）」の資格情報を狙います。一度管理者アカウントが奪われると、以下のことが可能になります。

- セキュリティソフト（EPP、EDR等）の無効化
- バックアップデータの消去
- 社内サーバやファイル共有への完全アクセス
- 監視ログの消去

つまり、組織の脳が乗っ取られた状態です。この段階に至るまでの時間は、従来であれば数週間を要しましたが、近年では数時間以内、最悪1時間未満でActive Directoryの乗っ取りが完了するケースもあります。

### ステップ5：機密情報の公開・金銭要求

最後のステップでは、攻撃者が「手に入れた情報」と「掌握したシステム」を使って脅迫を開始します。いわゆるランサムウェア型の攻撃です。例えば以下のような脅迫が企業に届きます。

**「情報を公開されたくなければ、**
**3日以内に◯億円支払え」**

**「バックアップを復旧したいなら、**
**暗号解除キーを購入しろ」**

最近では、単にデータを暗号化して身代金を要求するだけでなく、同時に盗んだ機密情報を暴露サイトに段階的に掲載していく「ダブルエクストーション（二重脅迫）」や、取引先やメディアに通報する「三重脅迫」も確認されています。

## なぜサイバー攻撃が日常化するようになったのか

一昔前のサイバー攻撃は、「人力」が必要なものでした。ところが現在では、マルウェアの構築から侵入、感染、窃取、拡散、管理者権限の奪取、脅迫文の送付に至るまで、その大半が自動化ツールで行われます。ダークウェブで「攻撃一式セット」が売られていたり、ChatGPTのような生成AIを使った詐欺メールの文章や攻撃スクリプトが作成されていたりしており、特定のスキルがなくても犯罪行為ができるような環境が整ってきています。攻撃者の製品開発力はすでに一部のベンダーに匹敵する水準にあり、しかもコストが低くなっているのです。サイバー攻撃が日常化する理由がここにあります。

攻撃者のスピードは極めて速く、人的対応だけでは到底間に合わなくなりました。「気づいたらやられていた」では遅すぎるからこそ、常時監視と、即時検知・初動対応体制が求められます。また、サイバー攻撃は「システム」と「人」の両方の脆弱性を突いてくることから、技術対策と従業員教育を両輪で進める必要もあります。

攻撃者がどのような順番で組織に侵入し、何を足がかりにするのかを理解しておくことで、初動対応のスピードを生み出し、リスクを最小化する助けとなります。自動化が進んだサイバー攻撃は「いきなり起こった天災」というよりも「存在する行程の中で発生した人災」なのです。

# 4 サイバー攻撃のもたらすビジネスへの影響

## サイバー攻撃のもたらす**ビジネスへの影響**

サイバー攻撃がビジネスにもたらす影響は「情報漏えい」と「事業停止」

▶ **被害を「自社に起こるもの」として捉え、業務フローと密接に結びついたリスク分析を実施する**

株価下落・ブランド毀損・賠償金といった間接被害が甚大

▶ **経営層に向けて、セキュリティ投資の必要性を「財務インパクト」として可視化する**

ESG 投資における非財務指標（株価への影響）としても重視される

▶ **セキュリティ体制を「経営戦略」として捉えられるように経営層に働きかける**

### 「情報漏えい」と「事業停止」——二大直接被害

サイバー攻撃がIT部門だけの問題でないことは、近年の事例にみられる被害内容を見れば明らかです。直接的な被害として、「情報漏えい」と「事業停止」が発生し、サイバー攻撃は、組織の中核事業そのものを揺るがす「経営課題」となりました。

**【情報漏えい】**

サイバー攻撃による被害の代表格としてまず挙げられるのが情報漏えいです。これは単に個人情報が流出するというだけではありません。漏えいする情報の種類によって、企業に与える影響は多岐にわたります。

たとえば、顧客の氏名や住所、連絡先といった個人情報の流出は、プライバシー侵害や損害賠償請求につながりやすく、迅速な公表や本人通知といった対応が法的に求められます。また、従業員の人事情報や給与データ、健康情報などが漏えいすれば、内部からの信頼が失墜し、組織文化にも深刻なダメージを与えるでしょう。

さらに、企業が保有する製品設計書や研究開発データ、知的財産が流出すれば、技術的な優位性を失い、競合他社との競争力が損なわれます。営業戦略やマーケティング計画、価格表といった営業秘密の漏えいも、ビジネスの根幹を揺るがすリスク要因です。

近年では、取引先や委託先の情報、つまりサプライチェーン情報の漏えいも深刻な影響をもたらします。サプライヤーやパートナー企業の信用に関わるだけでなく、全体の連携・調達体制が崩れる可能性も否定できません。

このように、「情報漏えい」は、単なるデータの流出という枠にとどまらず、顧客信頼の喪失、法的責任の発生、競争力の低下、ひいては株価の下落や企業ブランドの毀損にまで発展する、極めて多面的なリスクを内包しています。

**【事業停止】**

事業停止は、サイバー攻撃が企業活動の根幹を物理的に止めてしまう深刻なインパクトをもたらします。ITシステムの可用性がゼロになり、業務が完全に麻痺することで、企業は直接的な損失を被るだけでなく、信頼の回復にも長い時間を要します。

たとえば、基幹システムのダウンによって受発注業務が停止すれば、製品の出荷ができず、売上計上そのものが不可能になります。生産管理システムの停止による製造ラインの稼働停止は、1日ごとの損害が億単位に達することも珍しくありません。POSやECサイトのダウンは、小売・流通業においては即座に売上停止を意味し、消費者からの信頼喪失にも直結します。

さらに、病院や空港、港湾などの社会インフラを担う業界では、サイバー攻撃によるシステム停止が人命や安全にも関わる重大事案に発展します。実際に国内外では、医療機関の電子カルテや検査機器が利用できず、緊急手術が延期されるといった被害も報告されています。

一部のケースでは、社内ネットワーク全体の遮断を余儀なくされ、メールすら使えない「完全な通信不全」に陥ることもあります。こうなると、災害対策本部を立ち上げるような緊急体制が必要となり、復旧対応にかかる人的・時間的・金銭的リソースは莫大になります。

また、復旧作業には専門的なデジタルフォレンジック調査や再構築のための作業も伴い、最悪の場合、数週間から数か月単位で業務停止が続くリスクもあります。さらに、復旧の見通しが立たない状況自体が、株価の暴落や取引先の離反といった二次被害を引き起こす可能性もあるのです。

いずれの被害も、単なるITのトラブルではなく、業務フローに直結した「ビジネスの中断」であり、BCP（事業継続計画）にも深く関わるものです。リスク分析は「万が一」ではなく、「起きた場合、どの業務が、いつ、どのように止まるのか？」を具体的に可視化する必要があります。

## 間接被害の深刻さ<br>――財務インパクトを「見える化」する

直接的な情報漏えいや業務停止に加え、近年問題視されているのが「間接的なビジネスダメージ」です。具体的には以下のような影響が挙げられます。

**【株価下落】**
特に上場企業においては、セキュリティ事故が公表された直後に株価が大きく下落する傾向があります。ある大手IT企業では、サイバー攻撃の被害公表後、一日で10%以上下落し、時価総額にして数千億円規模の損失となりました。投資家はセキュリティ体制の甘さを企業統治の不備と捉え、即座に反応します。

**【ブランド毀損】**
顧客情報を漏えいした場合、その企業への信頼は一瞬で失われます。特に、BtoC企業では風評被害が拡散しやすく、メディア報道やSNSでの炎上が長期的にブランド価値を毀損します。一度傷ついたブランドは、数年かけても回復できないケースもあります。

**【賠償金と調査コスト】**
インシデント対応に伴い発生するフォレンジック調査費用、コールセンター設置費用、法律事務所への相談費用などは膨大です。さらに、被害者への損害賠償が発生すれば、直接的な金銭支出が経営を圧迫します。

これらの影響を経営層に訴えるには、単なる「起こりうる可能性」ではなく、「起こった場合の損失額」を具体的に試算することが重要です。たとえば、業務停止1日あたりの損失、平均賠償金額、復旧費用を積み上げることで、数十億円の潜在リスクを明確に可視化できます。

## ESGと非財務指標<br>——注目高まる「ガバナンス」

近年、ESG(環境・社会・ガバナンス)投資の拡大に伴い、サイバーセキュリティは単なるIT課題ではなく、「企業統治に関する非財務リスク」として評価対象になっています。グローバルの投資家の間では、ESG(環境・社会・ガバナンス)の観点から、サイバーセキュリティは、非財務指標として重要な投資指標と位置付けられるようになりました。これにともなって海外では、上場企業に対して「サイバー攻撃に対する説明責任」を求めるガイドラインが整備され、SEC(米国証券取引委員会)などが情報開示義務を課しています。

国内でも、金融庁が「サイバーガバナンス・コード」を策定し、取締役会レベルでのリスク認識と対策を求める動きが加速しています。すなわち、セキュリティ体制は「あるかないか」ではなく、「どのレベルまで整備されているか」で評価され、資本市場での信用度に影響を及ぼす時代に入りました。

セキュリティ投資は「費用」ではなく、「経営戦略の一環」と位置づけ、IT部門としては、経営層に対して「これは守りの投資ではなく、持続可能な企業価値を支える投資である」と明確に訴求する必要があります。経営層がセキュリティを戦略として理解し、投資判断を下せるよう、IT部門としてはわかりやすい情報提供と対話が求められます。

# 5 サイバー災害の収束に時間とコストがかかる理由

**サイバー災害の収束に時間とコストがかかる理由**

防御の「無力化」と「痕跡消去」により被害把握が困難

▶ **監視ログの長期保存と分散管理、検知手段の多層化を**

フォレンジック調査・復旧・顧客対応に莫大なリソースが必要となる

▶ **有事を想定したシナリオ訓練や、復旧手順の事前整備をする**

情報開示・報告義務にも時間制限がある

▶ **インシデント報告フローの整備と、法令対応担当者との連携体制を日頃から確認しておく**

## 初めから困難を極める対応

サイバー攻撃の被害は、発生の瞬間だけではありません。その収束までに必要とされる対応こそが、組織にとって最大の負担となることが少なくありません。攻撃によって防御が無力化され、痕跡が消されることで特定が難しく、初動からいきなり高い壁に当たります。さらに調査そのものや復旧、顧客対応の負担、そして情報開示や報告義務への対応と、時間とコストが多くかかります。

## 防御システムが「無力化」され、痕跡も消される

サイバー攻撃が進行すると、攻撃者は単に情報を盗むだけではなく、検知・追跡・復旧を困難にするため、企業の防御機能を徹底的に無力化します。犯罪者はサイバー攻撃に目障りな「減災」システムを無力化したいという動機があり、「防災」の弱さを突いて「減災」を無力化します。具体的な無力化の方法としては以下のようなものがあります。

- EPP や EDR のアンインストール、サービスの停止
- Windows イベントログや監視ログの削除、改ざん

- **セキュリティアラートの設定変更（アラートをオフにする）**
- **管理者権限でのログ無効化や監視除外設定の操作**

このような無力化により、「どの端末が」「いつ」「どのように感染したか」といった攻撃の全容が、後から追えなくなります。たとえば、EDRで異常通信が検知されていたはずなのに、後で確認すると該当ログが消えていたといった事態が実際に起こっています。攻撃者は自身の痕跡を消すだけでなく、インシデント対応そのものを妨害します。

このような事態に備えるためには、ログの長期保存と、複数拠点への分散保管が不可欠です。ゲートウェイやクラウド、エンドポイント、Active Directory、バックアップシステムが出力するログを多面的に監視し、CSIRT/SOCや外部SOCと連携して一元的に対応するモデル（統合SOC）が必要です。これを多面防御（マルチレイヤセキュリティ）と呼んでいます。

## フォレンジック調査・復旧・顧客対応の負担

インシデントが起きた後、情報システム部門やCSIRTには多岐にわたるタスクが一気に押し寄せます。中でも、フォレンジック調査・システム復旧・顧客対応は特に大きな負担になります。

**【フォレンジック調査】**

まず必要なのは、攻撃の詳細を証拠として明らかにすることです。第三者機関と連携して、ネットワーク通信の履歴や端末内の痕跡を徹底的に調査し、法的証拠を見つけに行きます。フォレンジック調査では以下のような調査が行われます。

- **感染端末のメモリダンプやレジストリの分析**
- **C2通信（攻撃者からの遠隔操作通信）の痕跡追跡**
- **ファイル操作や権限昇格のタイムスタンプ比較**
- **削除されたファイルや破損したファイルの復元**

フォレンジック調査には1～2週間以上かかることが多く、調査中のシステム隔離や関係者のヒアリングも並行して進みます。費用は数百万円から数千万円にのぼることもあり、時間的にも金銭的にも負担の重いものになります。

**【システム復旧】**

次に待っているのが、破壊または暗号化されたサーバ群の復旧作業です。最新のバックアップが正しく機能すれば短時間で復旧できますが、「バックアップまで暗号化されていた」「バックアップポリシーが実行されていなかった」「本番とテスト環境で復旧手順が異なっていた」など、想定外のトラブルが発生し、数日～数週間単位のシステムダウンに陥るケースも少なくありません。

**【顧客・取引先対応】**

情報が漏えいした場合、企業は単なる社内対応にとどまらず、次のような外部対応も迫られます。

- **被害に遭った顧客への個別通知や謝罪文の発送**
- **問い合わせ窓口（コールセンター）の設置**
- **SNSや報道対応、風評拡大の防止策**
- **契約先への影響報告と信頼回復措置**

顧客や取引先への対応には、「いま言えること、言えないこと」「はっきりしていないこと」についてどう納得してもらうかなど、相手の顔が見えるだけに非常に神経がすり減るものです。ビジネス部門からの厳しい声にさらされることにもあるでしょう。さらにこれらは一時的な業務ではなく、1年以上続く対応活動に発展することもあります。そうならないためには、平時からの訓練や、復旧・通知までの一連フローの整備が重要になります。

## 情報開示・報告義務への対応と時間的プレッシャー

サイバー災害は、企業内部だけで収められる問題ではありません。インシデントの種類や影響範囲によっては、法令や業界団体から報告義務が課せられ、非常に短期間での情報提出が求められます。しかも、これらの義務の中にはすでに罰則が規定されていたり、情報開示の不備に対する民事訴訟の可能性があったりと、企業は無視できるものではありません。特に欧米における違反のペナルティは厳しく、企業の存続すら危ぶまれる可能性もあります。以下、例として3つの義務を提示します。

- SEC（米国証券取引委員会）：
  重大インシデントの開示を4営業日以内に義務付け
- EU NIS2指令：
  重要事業者は発生から24時間以内に初報告
- 日本の個人情報保護法：
  個人情報漏えい時には速やかな委員会報告と本人通知が必要

報告には「原因・経緯・影響範囲・再発防止策」などを含めなければならず、組織内の法務部門・経営層・広報部門との迅速かつ正確な連携が必要です。

実際、報告の遅れや曖昧な説明は「情報隠蔽」と捉えられ、ブランドイメージの悪化や行政処分にもつながりかねません。これを防ぐための手段の一つとして、報告テンプレートの整備や通信経路の確認（誰が、どこに、何を届けるか）、担当者と決裁者の関係整理などは、日常業務の一環として組み込んでおく方法があります。

## グループやサプライチェーン経由による攻撃に注意

日本国内の例を見ると、ある重要インフラ業者がランサムウェア感染により3日間の事業停止になりました。大手エンターテインメント企業でも同様にサーバをターゲットにしたランサムウェア感染によって1か月以上の事業停止が発生しています。同様の事例は枚挙にいとまがありません。これらの多くでは、グループやサプライチェーン経由による攻撃であることも多いのが現状です。自社だけ対策してればよいとは言えなくなってきているのが、より問題を複雑化させています。

# 6 まだ間に合う！「サイバー防災」のすゝめ

## 「サイバー災害」に備えるために

サイバー災害は「攻撃の標的となり得る前提」で、脆弱性は「発見される前提」で

▶ **脆弱性を可視化して速やかに是正する仕組み（脆弱性管理ライフサイクル）を整備する**

「人の脆弱性」もサイバーリスクの一部

▶ **ソーシャルエンジニアリングや誤操作が発生・存在する前提で従業員教育と訓練を継続的に実施する**

初動対応こそが被害拡大を防ぐ鍵

▶ **インシデント対応マニュアルや通報フローを現場レベルまで浸透させておく**

前章までで、サイバーセキュリティにおける「防災」の重要性、そしてその具体的な手法である「サイバーハイジーン」の概念について解説してきました。本章では、依然として多くの企業が抱える課題を踏まえ、「まだ間に合う！」をキーワードに、より実践的なサイバー防災への取り組みを解説します。

## サイバー災害は「攻撃の標的となり得る前提」で、脆弱性は「悪用される前提」で

自然災害と同様に、サイバー攻撃もまた「しかけられる前提」で備えるべき時代です。もはや「うちの会社は大丈夫だろう」という楽観的な考えは通用しません。サイバー攻撃者は常に新たな脆弱性を探し、わずかな隙をついて組織内に侵入してきます。「完全な防御は不可能」であり、標的型攻撃においては、「詐欺メールは『必ず誰かがクリックする』」という前提に立つ必要があります。OSやアプリケーションの脆弱性もまた、常に存在し、「悪用される前提」で対策を講じることが重要です。

この「しかけられる前提」という考え方に基づけば、セキュリティ対策の重点は、侵入や攻撃を成立させる可能性を下げること、すなわち構造的な備えに置かれるべきです。そのためには、システムに潜在する脆弱性は常に「悪用される前提」で対策を講じる必要があります。

具体的には、脆弱性を可視化して速やかに是正する

仕組み（脆弱性管理のライフサイクル）を整備することになります。これは、単に脆弱性のリストを把握するだけでなく、発見された脆弱性に対して、パッチ適用、設定変更、バージョンアップ などの対策を迅速に実施し、その効果を検証する継続的なプロセスです。このサイクルを回し続けることで、脆弱性の「放置」を最小限に抑え、攻撃者に悪用されるリスクを低減することができます。

## 「人の脆弱性」も サイバーリスクの一部

システムやソフトウェアにおける脆弱性対策と並んで重要なのが、「人の脆弱性」への対策です。高度化するサイバー攻撃は、システムだけでなく、脆弱なパスワード、ソーシャルエンジニアリングや従業員による誤操作といった人間の弱点も巧みに突いてきます。特に、フィッシングメールや悪意のある添付ファイルは、日常業務に巧妙に紛れ込み、従業員の心理的な隙を狙います。

このような「人の脆弱性」に起因するリスクを軽減するためには、従業員教育と訓練を継続的に実施することが不可欠です。サイバー攻撃の手口や最新の脅威動向に関する知識を定期的にアップデートし、フィッシング訓練 などを通じて、従業員一人ひとりのセキュリティリテラシーを高める必要があります。また、人の脆弱性を悪用された後の感染拡大防止策、例えばEDRやゼロトラストの導入といった多層防御の仕組みも、日常的な防災の一環として重要になります。「人のミスは避けられない前提」で、システムと人の両面から対策を講じることが、組織全体のサイバーリスク低減に繋がります。

## 初動対応こそが被害拡大を防ぐ鍵

サイバー攻撃は、攻撃スピードが極めて速いという特徴があります。「気づいてからでは遅い」レベルで被害が拡大する可能性も十分にあり得ます。そのため、サイバー攻撃を受けてしまった場合には、初動対応こそが、被害を最小限に食い止めるための最も重要な鍵となります。

そのためには、インシデント発生時の対応マニュアルや通報フローを事前に整備し、現場レベルまで浸透させておくことが不可欠です。誰が、いつ、何を確認し、誰に報告するのかといった一連の流れを明確化し、定期的な訓練を通じて、従業員一人ひとりが適切な行動を取れるようにしておく必要があります。また、常時監視体制 や即時検知・初動対応体制の構築も重要であり、早期に異常を検知し、迅速に対応することで、被害の拡大を防ぐことができます。インシデント発生後のログの記録や報告体制の整備も重要ですが、それ以上に、「起こった後」に対応する従来の減災型のアプローチ に限界があることを認識し、「起こる前」の備え（防災）を徹底することが、結果的に被害を最小化することに繋がります。

## サイバー防御プロセス 5つのステップ

STEP 1
**全IT資産の可視化で「見えないものは守れない」をなくす**
動的なIT資産管理／構成管理の仕組化、全IT資産の棚卸、脆弱性の常時可視化・優先度付けをおこなう

STEP 2
**高リスク脆弱性の可視化と是正で脅威を排除する**
動的な脆弱性管理。パッチ適用や設定変更、バージョンアップ等で是正。このサイクルを繰り返す

STEP 3
**ツールを活用し防御力を最適化する**
EPP、EDRの導入。IT資産の適切な管理でツールのROIを最大化させることもできる

STEP 4
**サイバーハイジーンによる包括的な防御体制の構築**
動的なエンドポイント管理により、サイバーハイジーンを徹底し、「健全」な」状態を維持し続ける

STEP 5
**セキュリティ検証と継続的改善**
演習・アセスメント・DevSecOpsを通じて、日々の防御プロセスの有効性を評価・改善し続ける体制を構築する

効果的なサイバー防災を実現するためには、体系的なプロセスに基づいた取り組みが欠かせません。企業個別の状況を踏まえながらも、先人たちが試行錯誤しながら作り上げたプロセスをしっかりと踏んでいくことが、効率的かつ効果的なサイバー防災につながります。

### STEP 1
## 全IT資産の可視化で「見えないものは守れない」をなくす

サイバー事故を経験した組織の共通キーワードが「見えないものは守れない」であれば、「見えるものは守れる」状態にするのがまず行うべき施策になるでしょう。サイバー防災の最初のステップは、組織内に存在する全IT資産を正確に把握する（可視化する）ことです。管理されていないシャドーIT（企業が正式に承認していないアプリケーションやデバイス、管理対象外の旧システムなど）は、脆弱性の温床となりやすく、攻撃者にとって格好の侵入口となります。

全IT資産の可視化のためには、連続的に非管理端末をあぶり出し、端末を見つけ次第資産管理台帳を更新し、非管理端末を徹底的に排除し続けるプロセスが欠かせません。このプロセスを「動的なIT資産管理」と呼び、全IT資産を把握すると、その資産の構成情報が可視化できます。ハードウェア、ソフトウェアはもちろんのこと、クラウドサービスやネットワーク機器など、組織が利用する全てのIT資産を漏れなく

把握し、常に最新の状態に保つことが、サイバー防災の基盤となります。管理されていない端末やソフトウェアは、攻撃者にとって格好の標的となることを肝に銘じましょう。

シャドーITを可視化するもう一つの理由は「ガバナンス全範囲の網羅性」にこれが含まれるということです。取締役の責務としてのコーポレートガバナンスに非管理端末の可視化が含まれることを、IT担当者としても理解しておく必要があります。グローバル企業では、この全範囲は本社および本社管轄の国内拠点、海外拠点、資本関係のある国内グループ、海外グループ、さらにサプライチェーンにまで広がります。この範囲で業務に携わる従業員は、オフィスや工場、店舗、在宅、営業車などのオンプレミス、リモートすべての環境まで対象となります。「見えないものをなくす」上では、ガバナンスの物理的な全範囲を網羅しつつ、ハイブリッド環境も同時に網羅する必要があります。資本関係のある海外グループ拠点の営業担当が、営業車からノートパソコンで仕事をしている環境もガバナンスの責任範囲になります。

別の視点から見ると、IT資産や構成管理の重要性は、経済安全保障の観点からも注目されています。たとえばその一例として、「セキュリティ・クリアランス制度」が挙げられます。同制度は、サイバー攻撃から情報を守るために、機密情報に触れるエンジニアや担当者に対して、事前に「信頼できる人物か」を審査・認証する仕組みです。これは、各国において国家の安全保障を担当する機関が定めており、日本でも政府が策定を主導しています。防衛産業だけでなく、電力、通信、金融など重要インフラ事業者のセキュリティ担当者は、クリアランス保持を求められていく可能性があります。要件を満たすには、以下のステップが必要になります。

**① 守るべき機密情報（当該情報）を定義（識別と格付け）する**

**② 定義された当該情報が保存されているIT資産（デバイス）を定義（識別と格付け）する**

**③ ①×②にアクセスする権限を紐付ける**

## STEP 2
## 脆弱性を可視化と是正で排除する

全IT資産の可視化に続く第二のステップは、IT資産に存在する脆弱性を常時可視化し、組織が定めた脆弱性管理基準に基づいて是正する脆弱性管理です。脆弱性の中でも特に深刻なのが非管理端末の存在です。次に、組織が利用しているOSやアプリケーションに含まれる既知の脆弱性が挙げられます。

さらに、ITの内製化が進む中で開発されたソフトウェアに含まれるオープンソースやサードパーティ製コンポーネントの脆弱性も重要なリスク要因です。ソフトウェアコンポーネントのリスクを適切に把握・管理するために、SBOM（Software Bill of Materials：

ソフトウェア部品表）の活用が有効です。SBOMを用いることで、ソフトウェアに含まれるすべてのコンポーネントを可視化し、既知の脆弱性（CVE：Common Vulnerabilities and Exposures など）との照合を通じて、迅速な対応が可能になります。

現代のサイバー攻撃は、脆弱性の悪用から管理者権限が奪われるまで、わずか１時間足らずで完了するケースも存在します。このような状況下では、脆弱性可視化に数週間もかけていては、対策が後手に回ってしまいます。ここでもまた「動的な」脆弱性管理が重要です。脆弱性を特定・識別する可視化を行うだけでなく、パッチ適用や設定変更、バージョンアップ等で是正するまでを含みます。この可視化と是正のサイクルを継続的に繰り返すことで、脆弱性の「放置」を防ぎ、攻撃者に悪用されるリスクを最小限に抑えることができます。

動的なIT資産管理と動的な脆弱性管理はサイバーハイジーンを構成するための必須要素です。サイバーハイジーンができていないと、ウイルス対策製品（EPP：Endpoint Protection Platform）が導入されているにもかかわらず、それが動作していない端末が放置されたままといった状況が発生します。導入したセキュリティツールが働いていないということほど、恐ろしいことはありません。サイバーハイジーンのための調査をしようとすると、「臭い物の蓋が開く」、「パンドラの箱が開く」「そして責められる」といったIT担当者の嘆きをよく聞きます。これはIT部門の問題ではなく、時代の変遷とともにサイバーセキュリティの要求レベルが高まっているためであり、IT担当者は経営問題にもなりかねないこのリスクを、恐れることなく可視化し、対応していくことが事業運営に寄与すると考えましょう。

### STEP 3
## ツールを活用し防御力を最適化する

脆弱性を排除することで、セキュリティ事故の発生を未然に防御することができますが、100％の防御は不可能であることも事実です。CIS（Center for Internet Security：米国のセキュリティ標準化を推進する政府、企業、学術機関による団体）のデータでは、サイバーハイジーンの防御は85％以上防げるとあります。別の調査機関のデータでは、サイバーハイジーンでは防げないゼロデイと呼ばれる未知の脆弱性は0.4%、つまり未然に防御可能な攻撃は99.6% とあります。このように100％とはいえないのです。

そこで第三のステップとして、セキュリティツールを効果的に活用し、防御力を最適化することになります。威力を発揮するのが、EPP（Endpoint Protection Platform）や EDR（Endpoint Detection and Response）、そして近年注目されているXDR（Extended Detection and Response）といったソリューションです。

EPPやEDRは、エンドポイントにおけるマルウェアの検知・防御や、侵害の兆候をリアルタイムで監視・

対応する機能を提供します。XDRはこれらをさらに発展させたもので、エンドポイントだけでなく、ネットワーク、クラウド、メールなど複数のセキュリティデータを統合的に分析し、より高度な脅威の検知と迅速な対応を可能にします。

これらのツールは、サイバーハイジーン(基本的なセキュリティ対策)では防ぎきれないゼロデイ攻撃や高度な標的型攻撃に対しても有効であり、いくつかの製品ではAI技術を活用することで、検知精度や対応スピードが飛躍的に向上しています。

ウイルス対策製品は正しいバージョンを全端末にインストールし、正常性を確認し続けることが重要です。STEP2でサイバーハイジーンを実現していれば、インストールされていない端末は発生しないはずです。サイバーハイジーンの実現によって、導入ツールの投資対効果を最大化させることができています。

## STEP 4
## サイバーハイジーンによる包括的な防御体制の構築

ここまでのステップを踏まえ、第四のステップでは、サイバーハイジーンを徹底し、動的なエンドポイント管理と連携して侵入や攻撃を成立させる可能性の最小化を目指します。そのために「包括的な」防御態勢に目を向けてみます。

企業・組織の内部ではネットワークセキュリティツール群(ファイアウォール、IPS、各種コンテンツフィルタなど)やクラウド基盤上のセキュリティツールのSASE (Secure Access Service Edge)、SSE (Security Service Edge)など、またID管理基盤としてAD(Active Directory)や、認証・認可の基盤(IdP/MFA)等々、ハイブリッド環境を網羅するさまざまなセキュリティツールが実装されています。IT部門のCSIRT(Computer Security Incident Response Team) や SOC (Security Operation Center)チームは、セキュリティツールからのアラートや生ログをベースにサイバー攻撃を分析し、対処します。

一方、経営陣は、実際に検知された攻撃がグローバルITガバナンスの責任範囲において、どういう影響があったのか把握する必要があります。リスク影響度分析で、リスクがあっても隔離し、是正して、問題ないことが確認できれば、経営陣は安全宣言を発出できますが、多くの企業・組織は、安全宣言の発出が困難な実態に苦しんでいます。リスク影響度分析で、リスクがあっても隔離し、是正して、問題ないことが確認できれば、経営陣は安全宣言を発出できますが、多くの企業・組織は、安全宣言の発出が困難な実態に苦しんでいます。

STEP1での「動的なIT資産管理」ができていれば、IT資産の一部であるエンドポイントも動的に管理されていることになります。この動的なエンドポイント管理と連携することで、組織内の全てのエンド

ポイントの状態は常に把握され、脆弱性の早期発見と迅速な是正を可能にします。これにより、侵害や攻撃が成立する可能性を最小化します。サイバーハイジーンの徹底こそが、包括的な防御体制構築の要であることはここでも明らかです。

なお、サイバーハイジーンは、サイバー攻撃に対する自己免疫力を高めるための基盤となる取り組みであり、「ボヤの火種を作らない」防災に相当します。STEP3とSTEP4は「サイバーレジリエンス」（サイバー攻撃に対して求められる耐性力、回復力）の位置づけであり、「ボヤが発生したら大火にならないよう一秒でも早く消化する」減災に相当します。サイバー防御プロセスはこのサイバーハイジーンとサイバーレジリエンスが動的かつ緊密に連携することにより、最大のパフォーマンスを発揮することができ、そのために重要なのが、動的なエンドポイント管理です。

## STEP 5
## セキュリティ検証と継続的改善

サイバー防御プロセスの最後のステップは、これまでの対策が有効に機能しているかを定期的に検証し、継続的に改善していく体制を構築することです。具体的には以下のような対策やフレームワークがあります。

**アセスメント（NIST CSF成熟度アセスメントなど）**

NIST（National Institute of Standards and Technology：米国立標準技術研究所）のCSF（Cybersecurity Framework：サイバーセキュリティ向上のためのフレームワーク）は年次で実施が求められる成熟度アセスメントの一例です。また、自動車業界であれば自工会／部工会のサイバーセキュリティガイドラインなど、各業種、業態によって対応が求められるアセスメントが存在します。このようなセキュリティフレームワークを活用し、自社のセキュリティ対策の成熟度を評価し、課題や改善点を明確にすることができます。なお、欧米のように、政府に関連する組織に対し強制的な対応と対応不備の罰則がセットになっている厳しいものもあります。

**演習（サイバー攻撃演習、フィッシング訓練など）**

アセスメントと同じ目的を持ち、犯罪者視点から擬似的にサイバー攻撃を仕掛けるという演習があります。フィッシングメールを従業員に送付し、その開封率を測る訓練もあります。演習は実際の攻撃を想定した訓練を実施することで、従業員の対応能力やインシデント対応プロセスの有効性を評価します。中でもTLPT（Threat-Led Penetration Testing：脅威ベースのペネトレーションテスト）は、対象組織に実害は与えないものの、その直前まで犯罪者と同じロジックでサイバー攻撃を仕掛け、サイバー防御レベルを測定します。経営陣が意思決定して実施し、IT部門もその実施を知らされません。途中まで本当のサイバー攻撃と認識しての対処が求められ、より実践的な防御レベルの測定に有効です。

**DevSecOps**

企業が利用するソフトウェアは世の中に流通する商用ソフトウェアに限りません。自社で開発した内製化ソフトウェアも存在します。この内製化ソフトウェアの脆弱性を悪用した攻撃が拡大しています。そこで、ソフトウェア開発のライフサイクル全体にセキュリティ対策を組み込んだものがDevSecOpsとして注目を集めています。開発フェーズからセキュリティ対策を実施して、開発完了時のセキュリティチェックによる手戻りをなくし、リリースタイミングの遅延を防ぎ、リリース後の脆弱性対応の負荷も最小化させます。

サイバーハイジーンによる予防施策を徹底しても、すべてのリスクを防ぐことはできません。サイバーハイジーンを突破した攻撃は、オンプレミスならゲートウェイ、クラウドならクラウドサービス側のツールで防御します。例えばBEC（ビジネスメール詐欺）のような攻撃は、ゲートウェイやクラウドで一次防御し、すり抜けたメールがエンドポイントに到達します。しかし、エンドポイントで適切な対策が講じられていれば、マルウェア感染を防ぐことが可能です。

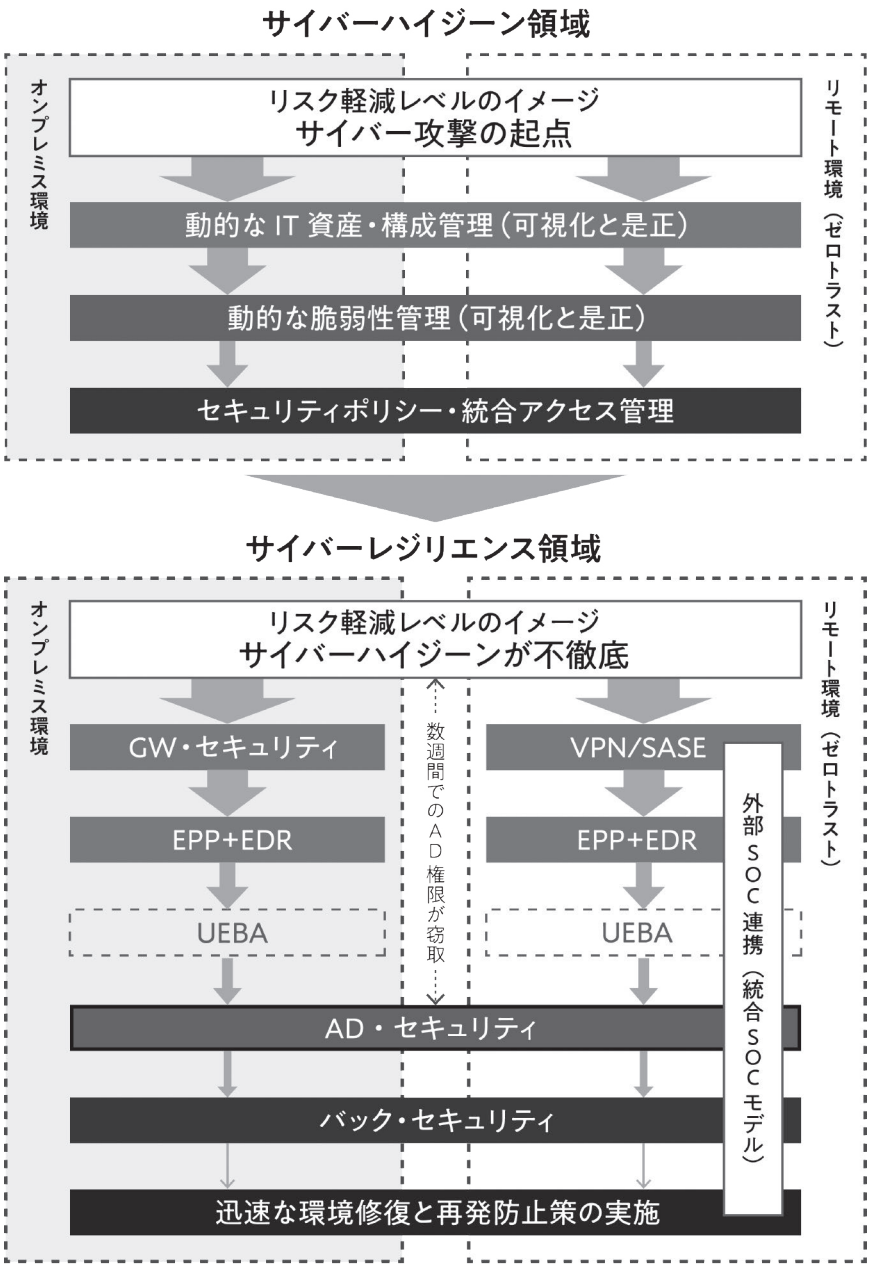
それでも、防げない未知の脆弱性（ゼロデイ）やネットワーク機器の脆弱性が悪用された場合、エンドポイントを経由せずにAD（Active Directory）サーバが直接攻撃されるケースもあります。ADが乗っ取られると、組織の全ITシステムが犯罪者の手中に落ちるため、AD専用のセキュリティ監視が不可欠です。この領域は、一般的なツールでは防御が難しく、専門家による24時間365日の監視が推奨されています。

さらに、ADが陥落すると、犯罪者はバックアップデータの暗号化を試みます。これに備えるには、バックアップ自体を安全に守る「バックアップセキュリティ」が必要です。たとえドメインアドミンが奪われても、バックアップデータが暗号化できない仕組みを整えることで、最後の砦を守ることができます。

これら全体を監視・連携するためには、ゲートウェイ、クラウド、エンドポイント、AD、バックアップシステムを統合的に監視する「統合SOCモデル」が求められます。

こうした多層的な防御体制は、近年「多面防御（マルチレイヤセキュリティ）」と呼ばれ、必須の考え方になっています。

サイバー防御ではこれらの活動を通じて、日々の防御プロセスの有効性を評価・改善し続けるPDCAサイクルを回していきます。サイバー攻撃の手法は常に進化しているため、一度対策を講じただけで安心するのではなく、常に最新の脅威動向を把握し、対策をアップデートしていく姿勢が求められます。動的な運用によるコスト効果とリスク抑制を意識し、運用や技術の固定化を避ける柔軟性を仕組みで保つことが、長期的なサイバーセキュリティ対策を有意義なものにします。




サイバー防御プロセスの全体像

# 7 グローバルの潮流から学ぶ「防災」

## グローバルの潮流から学ぶ「防災」

「報告期限と罰則規定」がキーワード。セキュリティはIT部門だけの話ではない

- **経営層や業務部門を巻き込み、横断的なタスクフォースの設置を提案・主導することで、自部門だけに負担が集中しない体制を築く**

NIST CSF等のグローバル基準をベースにしたセキュリティ実態分析

- **世界標準フレームワークを取り入れた管理体制を目指す。自社独自ルールに閉じない。運用に落とし込む**

「可視化と統合」による一元的サイバー対応が進んでいる

- **エンドポイントをリアルタイムに可視化・制御できる統合プラットフォームの導入を検討する**

これまで、サイバー防災に必要なサイバーハイジーンや、動的なIT資産・脆弱性管理を中心とした包括的な取り組みを紹介してきました。本章では、グローバル組織の取り組みの潮流に焦点を当てます。先進企業はどのように「防災」を日常運用へと組み込み、組織全体の耐性強化を図っているのでしょうか。

## 「報告期限と罰則規定」がキーワード。セキュリティはIT部門だけの話ではない

グローバルでのサイバーセキュリティ対策は、2022年から2023年を振り返ると、「報告期限と罰則規定」をキーワードに、法令遵守の厳格化が進んでいます。例えば、米国やEUなどでは、サイバーインシデント発生時の報告義務が明確に定められ、違反した場合の罰則規定も存在します。罰則の中には、全世界売上高の数%にあたる巨額ペナルティが科される可能性があります。これは、サイバー攻撃による事案の深刻度が増していることの表れであり、政府機関が攻撃に対する耐性を強化し、被害を早期に最小化することを重視していることを示唆しています。

例えば、米国の場合、重要インフラ事業者に対する「サイバーインシデント報告法」では、インシデントが発生したら24時間以内に当局へ報告することを求めています。EUのNIS2指令ではインシデント発生から72時間以内にインシデントを報告することを求めています。オーストラリアでも、重要インフラ事業者でインシデントが発生した場合、12時間以内

の報告義務があります。今後は法令や指令に対して報告期限が設けられることが当たり前になり、その報告期限が守られない場合はペナルティを課すというパターンが一般化していくことが予想されます。報告期限や罰則（およびインシデントによる影響）を考えると、セキュリティはもはやIT部門だけでのものではないといえます。

## NIST CSF等のグローバル基準をベースにしたセキュリティ実態分析

多くのグローバル組織は、サイバーセキュリティ対策の基盤として、NIST CSFやCIS Controlsといった世界標準のフレームワークを採用しています。これらのフレームワークは、長年の経験と知見に基づいて体系的に整理されており、ベストプラクティスを取り入れた管理体制を構築する上で非常に有効です。

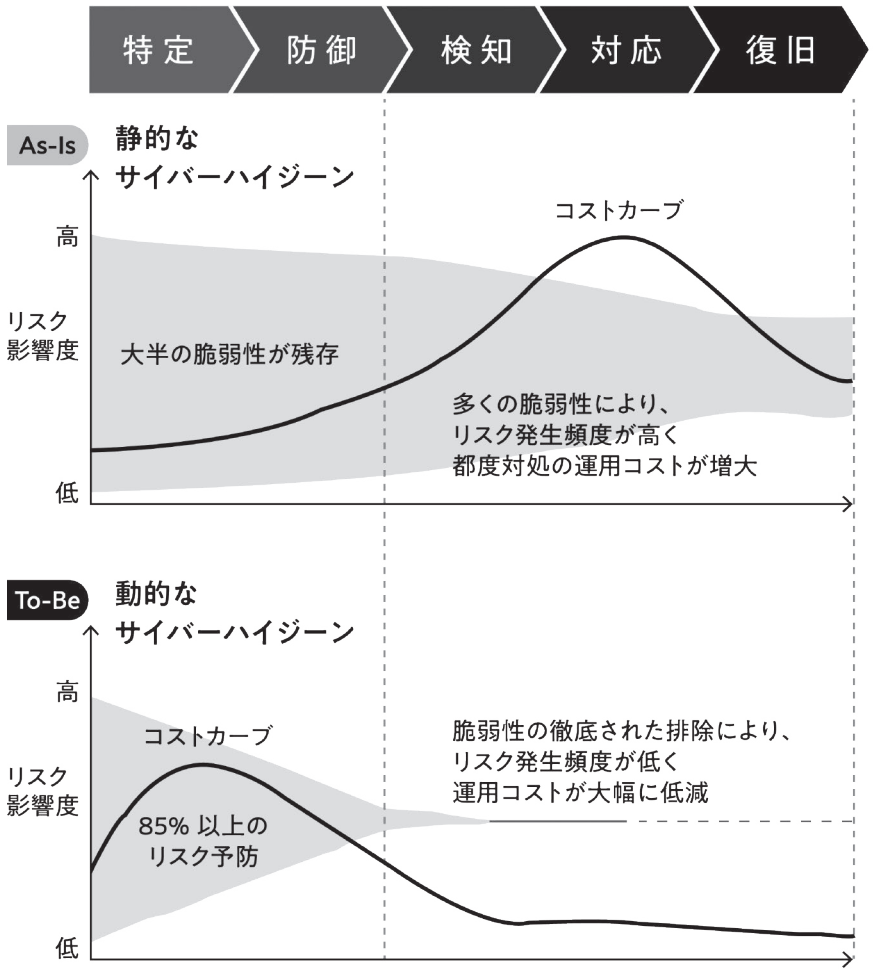
特に「サイバーセキュリティの教科書」としてトップに位置付けられるNIST CSFは、国内の大規模組織におけるセキュリティ施策の実態評価に役立ちます。

NIST CSFのコア（Core：サイバーセキュリティ対策の一覧）は「統治・特定・防御・検知・対応・復旧」の６つの機能で定義され、「統治＝ガバナンス」という機能が「特定」の前に設定されています。これらの機能を、エンドポイント（PCやサーバ）に絞って評価できます。NIST CSFは全IT資産の特定・識別を徹底的に実施し、非管理端末を撲滅し、資産管理台帳を随時、最新化するよう示唆しています。これは「特定」と「防御」の施策を最優先に設定するシフトレフトの考え方にも通じます。

サイバーセキュリティ対策で最もコストがかかるのは「検知・対応・復旧（サイバーレジリエンス）」です。たとえば、端末台数の把握が年に1～2回、棚卸しのタイミングのみなどのケースでは、非管理端末の把握も困難です。その結果、リスク発生要因の脆弱性に対処することができず、セキュリティ防御プロセスが、後段の検知・対応・復旧に委ねられます。脆弱性が対処されていないので、常にサイバー攻撃を検知、防御、分析し続けなければならず、業務負荷が向上し、コスト増加につながります。

一方、動的な運用の場合は、組織が保有する端末台数を常に把握でき、リアルタイムで正確な台数を把握できます。その上で、NIST CSFのフレームワークに沿ってシフトレフトが実現されると、リスク発生頻度が低く運用コストが大幅に低減するという理想の状態が出来上がります。

このように、自社独自のルールに閉じこもるのではなく、これらのグローバル基準に準拠した管理体制を目指すことは、グローバルサプライチェーンにおける信頼性の向上や、海外の規制当局や取引先との円滑なコミュニケーションにも繋がります。ただし、単純にフレームワークを導入するだけでなく、自社のIT環境やビジネス特性に合わせてカスタマイズし、




NIST CSFとサイバーハイジーンのコスト分析

日々の運用に落とし込むことも必要です。単に「導入した」という事実だけでなく、実効性のある運用が求められます。

## 「可視化と統合」による一元的サイバー対応が進んでいる

グローバル組織のサイバーセキュリティ対策の最新トレンドとして、「可視化と統合」による一元的なサイバー対応が進んでいます。これは、組織内に散在するIT資産に関する情報を一元的に集約し、リアルタイムに可視化することで、脅威の早期発見、迅速な分析、そして効果的な対応を実現するものです。

特に、エンドポイント（PC、サーバなど）をリアルタイムに可視化・制御できる統合プラットフォームの導入を検討することは、シャドーITの排除、脆弱性管理の徹底、そしてインシデント発生時の迅速な初動対応に繋がる有効な手段となります。このような統合プラットフォームは、IT資産管理、構成管理、脆弱性管理、インシデントレスポンスなどの機能を統合的に提供し、サイバーハイジーンの徹底と、セキュリティインシデント発生時の被害最小化を両立させることを可能にします。

グローバル化が進んだいま、日本に本社を置く企業でも無関係ではありません。日本が本社でも、EUやアメリカに拠点を持つ企業は、その国の法令対象になります。例えば自社のCSIRTチームが、EUの拠点でサイバー事案の発生を把握し、場合によっては外部機関からも同様の報告を受けた場合、IT部門はそのサイバー攻撃による影響や深刻度を迅速かつ正確に経営陣に伝えられるでしょうか？どのような経路（原因）でサイバー攻撃を受けたのか、どのような影響が出ているのか、当局への報告に必要なデータを経営陣に説明できるレベルで整理されているでしょうか？「海外子会社で起きたインシデントでも本社が責任を負う」と認識しておきましょう。

このような状況下では、サイバーセキュリティ対策はIT部門だけの問題ではなく、経営層を含む組織全体の課題として捉える必要があります。IT部門は経営層や業務部門を巻き込み、横断的なタスクフォースの設置を提案・主導することが求められます。コミュニケーションにおいては、なるべく専門用語を避け、経営層のプロトコルを意識することも必要です。

# 8 シフトレフトと定量評価による防災レベルの向上

## シフトレフトと定量評価による防災レベルの向上

起こってから動く「減災」に偏りすぎると疲弊する

▶ **起こさない工夫（防災）を強化し、対処型セキュリティからの脱却を図る**

今あるルールに固執しない。常に改善を

▶ **セキュリティ施策の PDCA を回し、運用や技術の固定化を避ける柔軟性を仕組みで保つ**

やっている、だけではなく KPI（評価指標）を設定する

▶ **数値目標を設定することで、セキュリティ対策の実態を定量的に評価する仕組みを持つ**

サイバーセキュリティ対策は、あたかも終わりのない災害対策のようです。常に新たな脅威が出現し、対策の範囲も拡大し続けます。このような状況において、IT担当者は何に、どこまで取り組むべきなのでしょうか。

## 起こってから動く「減災」に偏りすぎると疲弊する

サイバー攻撃が発生した後に対処する「減災」の対策は重要ですが、それに偏りすぎると、常に後手に回り、IT担当者や組織が疲弊してしまいます。「ボヤが発生したら大火にならないよう一秒でも早く消化する」ことも重要ですが、それ以上に「ボヤの火種を作らない」防災を強化し、対処型セキュリティからの脱却を図る考え方が求められます。

サイバーハイジーンの徹底は、まさに「起こさない工夫（防災）」であり、組織の自己免疫力を高めることに繋がります。脆弱性の放置をなくし、攻撃者の侵入経路を塞ぐことで、インシデントの発生頻度を大幅に減らすことが可能となり、結果的に減災にかかる労力やコストを削減することができます。

## 今あるルールに固執しない。常に改善を

サイバー攻撃の手法は常に進化しており、過去の成功体験や今あるルールに固執していては、新たな脅威に対応できません。セキュリティ対策においては、

PDCAサイクルを回し、運用や技術の固定化を避け、常に改善を続けていく柔軟性を仕組みで保つことが重要です。

定期的なセキュリティ実態分析を実施し、現状の対策の有効性を評価するとともに、最新の脅威動向や技術革新を取り入れ、対策をアップデートしていく必要があります。「科学と理論」に基づく教科書であるNIST CSFなどを参考に、常に最新の知識やベストプラクティスを学び続ける姿勢が求められます。

## やっている、だけではなく KPI（評価指標）を設定する

サイバーセキュリティ対策では、防災レベルを定量的に評価する仕組みを持つことが重要です。

非管理端末の検出の網羅性や、パッチ適用率、脆弱性該当状況の特定にかかる時間など、サイバーハイジーンの各運用項目についてKPIを設定し、目標の達成度を定量的に評価し続けることが、組織全体のサイバー防災レベルの向上に繋がります。

# 今こそサイバー防災に取り組もう

サイバー防災の仕組み構築はまだ間に合います。「攻撃の標的となり得る前提」での備え、サイバーハイジーンの徹底、継続的な改善そして定量的な評価の重要性を再認識し、組織全体を巻き込んだ対策を推進することで、強靭なサイバーセキュリティ体制を構築し、持続可能な企業活動 を実現していくことができるでしょう。今こそ、従来の「減災」中心の対策から脱却し、「防災」を主軸とした戦略へとシフトチェンジする時です。

---

**タニウム リソースセンターのご案内**

お客様事例や調査レポート、ホワイトペーパー、ウェビナー動画など、
コンテンツが満載のリソースセンターが開設しました。ぜひお役立てください。

**https://explore.tanium.com/japan-resource-center/**