NEWS RELEASE

2025 年 10 月 15 日
タニウム合同会社

タニウム、『IT 担当者のための「サイバー防災」ハンドブック』を公開

～継続的なサイバーセキュリティの実現に必要な「サイバーハイジーン」を徹底解説～

AI を活用した自律型エンドポイント管理（AEM）プラットフォームで業界をリードするタニウム合同会社（本社：東京都千代田区、代表執行役社長：原田英典、以下タニウム）は、IT・セキュリティ運用の実務担当者に向けて、サイバーハイジーンの定義と要点について解説する『IT 担当者のための「サイバー防災」ハンドブック』をオンライン公開しました。

近年、生産システムを停止に追い込むようなサイバー攻撃が増加の一途をたどっています。攻撃者から「システムを復活したければ金を払え」という脅迫を受けるケースも頻繁に発生し、深刻度が増大しています。また情報漏えいを受けて、多額の賠償金を顧客に支払ったという事例もこの 10 年でも多数発生しています。

これらを背景に、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取り組みである「サイバーハイジーン」の重要性が一層高まっています。「サイバーハイジーン」は、2024 年に金融庁が公表した「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」でも基本対応事項のひとつに位置づけられるなど、現代における重要なキーワードになっています。

タニウムでは、2023 年以降に関連書籍（※）を出版し、技術面・経営面両方の観点からこの概念を解説してきました。今回公開した『IT 担当者のための「サイバー防災」ハンドブック』では、これら過去の出版物を基に、IT・セキュリティ運用の実務担当者に向けて、サイバーハイジーンの定義と要点を 35 ページにわたって解説しています。
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。

（※）「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）
「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）

ダウンロードはこちら：
https://explore.tanium.com/japan-resource-center/col/917f8044-77a2-4f28-ae8a-a1a5b56ef1d5/eb-cyber-disaster-prevention-jp

■『IT 担当者のための「サイバー防災」ハンドブック』概要

①サイバーセキュリティで注目が高まる「防災」

・「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
・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」
・サイバー防災の手法は「IT 資産管理」「構成管理」「脆弱性管理」

②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
・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
・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

③サイバー災害の実態を知る

・ステップ型の攻撃プロセスが存在する
・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
・攻撃スピードは極めて速く「気づいてからでは遅い」

④サイバー攻撃のもたらすビジネスへの影響

・サイバー攻撃がビジネスにもたらす影響は「情報漏えい」と「事業停止」
・株価下落・ブランド毀損・賠償金といった間接被害が甚大
・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

⑤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
・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
・情報開示・報告義務にも時間制限がある

⑥まだ間に合う！「サイバー防災」のすゝめ

・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
・「人の脆弱性」もサイバーリスクの一部
・初動対応こそが被害拡大を防ぐ鍵

⑦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
・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
・「可視化と統合」による一元的サイバー対応が進んでいる

⑧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
・今あるルールに固執しない。常に改善を

・やっている、だけではなく KPI（評価指標）を設定する

■タニウムについて

Tanium Autonomous Endpoint Management (AEM) は、業種を問わずエンドポイントをインテリジェントに管理するための最も包括的なソリューションを提供し、IT 資産の発見とインベントリ、脆弱性管理、エンドポイント管理、インシデント対応、リスクとコンプライアンス、デジタル従業員体験の機能を提供します。タニウムのプラットフォームは、 Fortune 100 企業の 40%に導入され、世界中で 3,500 万のエンドポイント管理をサポートしています。より効率的な運用とより強化なセキュリティ体制を、規模に関わらず高い信頼性をもってリアルタイムで提供します。The Power of Certainty™の詳細については、**https://www.tanium.jp/** をご覧いただき、**Facebook** と **X** でフォローしてください。

日本法人名：タニウム合同会社
グローバル代表 CEO：ダン・ストリートマン
日本代表執行役社長：原田英典
設立年：2007 年
設立年（日本）：2015 年
所在地（日本オフィス）：〒100-0004 東京都千代田区大手町 2 丁目 6-4 常盤橋タワー25F
事業内容：自律型エンドポイント管理のプラットフォーム提供
URL：https://www.tanium.jp/

■免責事項

ここに記載されている情報は一般的な情報提供のみを目的としています。本情報は、当社が将来の製品、特徴、または機能を提供することについて確約、保証、申し出、および約束を行うものでも、法的義務を負うものでもありません。また、いかなる契約にも組み込まれることを意図しておらず、そのように見なされるものでもありません。最終的に提供される製品、特徴、または機能の実際の時期は記載されているものと異なる可能性があります。