

サイバー攻撃——疑いを認知したら、1時間以内に止めて報告する

Published: 2025-10-22 / Updated: 2026-08-26

Summary

本稿は、サイバー攻撃の疑いを認知した後の初動を、遮断、第一報、証跡保全、並行調査、段階復旧の順で整理します。関連する「セキュリティは本当に『攻撃を防いだ価値』なのか」では正常時のSecurity KPIをBlock MoreからWork Safelyへ転換する考え方を扱い、本稿では異常時にWork Safelyを取り戻すためのContainmentとRecoveryを具体化します。

Key Points

- セキュリティの目的は、攻撃を何件止めたかではなく、安全に業務を完遂できる状態を維持することです。正常時には必要な情報へ安全に到達できる構造を保ち、異常を認知したら対象を遮断し、第一報と証跡保全を開始し、安全を確認した機能から段階的に復旧します。つまり、止め過ぎない設計と、止めるべき時に止めて戻せる運用は、同じ「Work Safely」を支える二つの側面です。
- 業務影響が顕在化する前の疑い段階を含め、情報セキュリティインシデントへ組織的に対応する必要性
- Security KPIをBlock MoreからWork Safelyへ転換し、安全性・可用性・生産性を通信構造全体で評価する考え方
- 認証、DNS、ネットワーク、通信機器、物理電源まで含む共通依存関係とSPOFの切り分け
- 可用性要求を情報システム、通信、物理電源、監査証跡、調達仕様へGroundingする整理

Sources / References

Public-primary

内閣官房 国家サイバー統括室「政府機関等の対策基準策定のためのガイドライン（令和7年度版）」

URL: https://www.cyber.go.jp/pdf/policy/general/guider8_6_01.pdf

First-party-analysis

セキュリティは本当に「攻撃を防いだ価値」なのか | 企業ネットワークを通信構造から問い直す

URL: <https://www.ieee802.co.jp/articles/article-213-security-productivity.php>

First-party-technical

情報システムの可用性は電源で止まる | ISMS・SPOF対策になぜ無瞬断の可搬型UPSが必要なのか

URL: <https://www.ieee802.co.jp/articles/article-099-isms-spod.php>

First-party-policy-analysis

自治体の「機密性・完全性・可用性」を支える電源設計とは | 可用性2・復旧要件・監査対応から見るUPSの役割

URL: <https://www.ieee802.co.jp/articles/article-071-isms.php>

Source Article

<https://www.ieee802.co.jp/articles/article-004-antiransom.php>

© Kei Communication Technology Inc.

This document is a summary of the source article. For the latest information, refer to the source URL.