中部管区警察局出前授業

4I24 中川寛之

サイバー攻撃のニュースを1件調査し報告せよ。

サイバー攻撃の調査報告：KADOKAWAの事例

---

1. 概要

- **発生時期**：2024年6月8日未明の発覚
- **対象組織**：株式会社KADOKAWA及び同社グループ（株式会社ドワンゴなど）
- **事象**：グループのデータセンターに対する大規模なサイバー攻撃の発生

2. 攻撃手法

- **種類**：ランサムウェア（身代金要求型ウイルス）による攻撃
- **侵入経路**：従業員アカウント情報のフィッシング攻撃による窃取（推定）
- **攻撃者**：ランサムウェアグループ「BlackSuit」の関与の可能性（報道による）

3. 主な被害

- **サービス停止**：
  - 「ニコニコ動画」をはじめとするニコニコファミリー全サービスの長期停止
  - KADOKAWAオフィシャルサイト、ECサイト「ebten」などの複数のWebサイトの停止
- **業務停止**：
  - 社内業務システム（経理・編集・物流）の機能停止
  - 出版物の製造・物流、経理業務への甚大な影響
- **情報漏洩**：
  - 約25万件にのぼる個人情報の流出（取引先クリエイター、従業員、N高等学校の生徒情報など）
  - 契約書や社内文書など、機密情報の窃取

4. 組織の対応

- **初動**：攻撃検知後、被害拡大防止のためのサーバーの物理的なシャットダウン
- **公表**：サイバー攻撃の事実の公表と、警察・個人情報保護委員会への即時報告
- **復旧**：
  - 外部専門家の支援によるフォレンジック調査の実施
  - 身代金要求の拒否（公式発表）
  - 安全な環境下での全面的なシステム再構築の決断
  - 「ニコニコ動画」は新バージョンとして約2ヶ月後の段階的再開

5. 影響

- **業績**：復旧費用、補償、売上機会損失による数十億円規模の業績悪化の見込み
- **信頼**：サービス利用者および取引先からの信頼への大きな打撃

参考資料

- トレンドマイクロ (JP) Wikipedia
- piyolog
- KADOKAWAのお詫び
- KADOKAWAのプレスリリース

次の語句について調査し説明せよ。

デジタル・フォレンジック

->「デジタル・フォレンジック」とは、コンピュータやスマートフォン、ネットワーク機器などの電子機器に残されたデータを収集・分析し、法的な証拠（犯罪や不正行為の証拠）を見つけ出すための一連の科学的調査技術や手法のこと。

警察の「鑑識」が現実世界の指紋や足跡を調べるように、デジタル・フォレンジックは デジタル世界の「足跡」（アクセスログ、削除されたファイル、通信履歴など）を調査します。

主な目的

- **サイバー攻撃の調査:** 不正アクセス、マルウェア感染、DDoS攻撃などの被害状況の特定と原因究明。
- **不正行為の調査:** 企業内での情報漏洩、データ改ざん、横領などの証拠特定。
- **法的証拠の確保:** 刑事事件や民事訴訟において、裁判所に提出できる電子的証拠を確保すること。

調査の過程では、元のデータを改ざんしないこと（証拠保全性）が非常に重要であり、特別な手順とツールを用いてデータの複製（保全）を行ってから分析します。

参考資料

- 警察庁
- GMO

CSIRT

->「CSIRT（シーサート）」とは、"Computer Security Incident Response Team" の略。

企業や政府機関などの組織内に設置され、セキュリティ上の問題（インシデント）が発生した際に、専門的に対応するチームのことを指します。

組織にとっての「セキュリティ専門の消防隊」や「救急対応チーム」のような存在で、問題発生時に迅速に駆けつけ、被害を最小限に食い止める役割を担います。

主な役割

- CSIRTの役割は、インシデント発生後の対応（リアクティブ活動）だけでなく、発生を防ぐ活動（プロアクティブ活動）も含まれます。

- **インシデント対応**:
    - セキュリティ侵害（ウイルス感染、不正アクセスなど）の通報受付窓口。
    - 被害状況の把握、原因分析、被害拡大の防止措置（例：ネットワークからの隔離）。
    - システムの復旧支援、関係各所への報告。
- **事前準備・予防**:
    - 最新のセキュリティ情報（脆弱性や攻撃手法）の収集と組織内への注意喚起。
    - セキュリティ対策の訓練や、従業員への啓発活動。
    - インシデント対応マニュアルの整備。

参考資料

- docomoビジネス
- 三井住友海上

出前授業を通して学んだこと、感想などを述べよ。

今回の中部管区警察局による出前授業では、実際の捜査現場で使用されているデータ復元やログ解析といったデジタル・フォレンジック技術をツールを用いて体験することができ、特にJPGファイルを偽装して実行ファイル（exe）に変換する手法は非常に興味深いと感じた一方で、見た目では判断できない悪意あるプログラムの危険性を実感し、ファイルの拡張子だけで安全性を判断せず、信頼できない送信元からのファイルは安易に開かないという基本的なセキュリティ意識の重要性を改めて認識した。KADOKAWAの事例で調査したように、実際のサイバー攻撃は組織に甚大な被害をもたらすため、今回学んだ知識を活かし、将来エンジニアとして働く際にはセキュリティを常に意識した安全なシステム構築に貢献したいと考える。