SEAJテキストで解説するセキュリティ知識は実社会でどう役立つのか？～最近のランサムウェア動向について学ぶ～

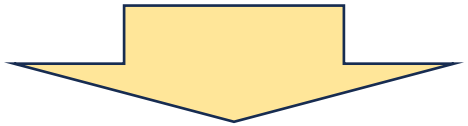
2025 年 8 月 20日

日本ネットワークセキュリティ協会（JNSA）
教育部会 教育実証WG
玉川 宏志

はじめに

○ ITは日進月歩。
情報セキュリティも同じ。ITの進化、攻撃者の動向などあり常に変化し続ける領域
○ ITのない日常生活が考えられないほど、日常生活に定着。
攻撃者にとって、サイバー攻撃で得られる利得が増大。

■セキュリティの学習
（テキスト等による）基本の学習に加えて、最新動向を知ることは非常に重要



マルウェアの中で最もホットで動きのあるランサムウェアについての動向を紹介

基礎編テキストの改訂　～マルウェア関連～

○ 11章から9章に移動
○ 章の名称を変更：不正プログラム　→　マルウェア
○ 旧11章の構成・内容をベースに最新の動向、情報にアップデート

1章 情報セキュリティマネジメント
2章 セキュリティ運用
3章 インフラセキュリティ
4章 不正アクセス
5章 ファイアウォール
6章 侵入検知
7章 アプリケーションセキュリティ
8章 OSセキュリティ
9章 認証
10章 プログラミング
11章 不正プログラム
12章 暗号
13章 電子署名
14章 PKI
15章 セキュリティプロコトル
16章 法令・規格

1章 情報セキュリティマネジメント
2章 物理的セキュリティ
3章 人的セキュリティ
4章 ネットワークのアクセスコントロール
5章 ネットワークセキュリティ
6章 認証
7章アクセスコントロール
8章　ソフトウェアの脆弱性
9章 マルウェア
10章 暗号
11章 電子署名
12章 PKI
13章 法令・規格

基礎編テキストの改訂　～マルウェア関連～

○ 主な改訂ポイント

・マルウェアについての説明を追加

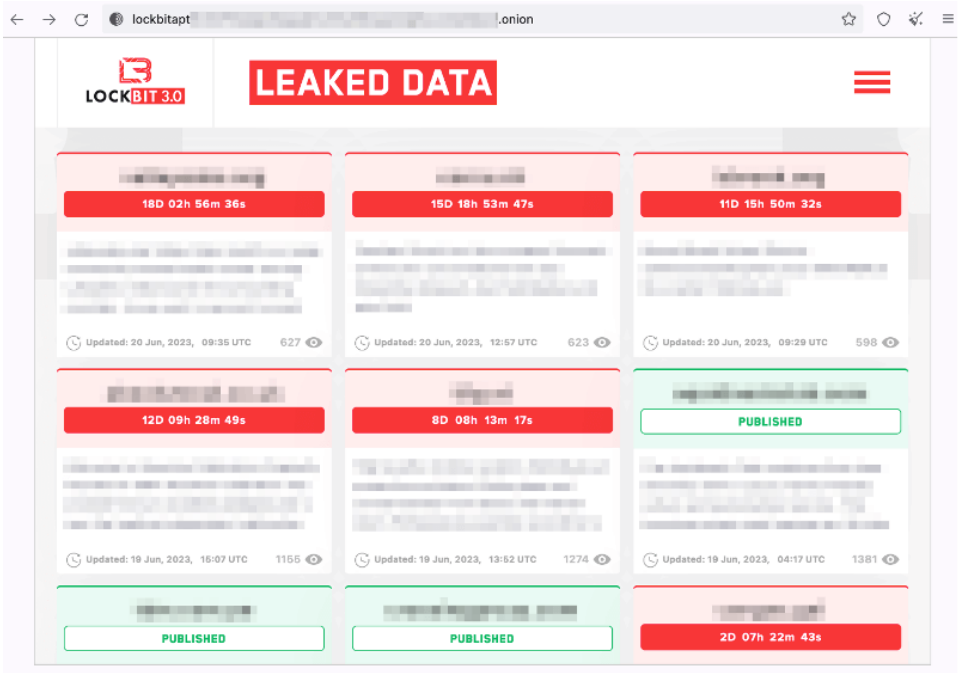
・マルウェアの種類について追加、説明を更新
（ファイルレスマルウェア、ダウンローダ、ルートキット、ランサムウェア、ボットなど）

・感染経路に関する説明を更新（脆弱性の悪用、フィッシングなど）

ランサムウェアとは・・・

- ランサムウェアは、被害者に対して身代金（ransom）を支払うよう要求するマルウェア
- 脅迫の手段には、暗号化、スマートフォンなどのロックなどがある
- 暗号化、情報の公開（暴露）、DDoS攻撃などから複数を組み合わせて脅迫するケースもある（多重脅迫ランサムウェア）

感染した場合に表示される画面の一例



暴露サイトの例
https://www.fortinet.com/jp/blog/threat-research/lockbit-most-prevalent-ransomware

情報セキュリティ10大脅威2025 組織編

○ ランサムウェアは1位。10年連続ランクイン。
○「XX年連続」ランクインが8件を占める。ずっと脅威は変わっていないのか？

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

ランサム事例①（多重脅迫ランサムウェア）

KADOKAWAのシステム障害、原因はランサムウェアを含む大規模攻撃と発表

ZDNET Japan Staff　2024-06-14 18:23

KADOKAWAは6月14日、同社グループで8日未明から発生しているシステム障害について、原因はランサムウェアを含む大規模サイバー攻撃によるものだと発表した。復旧では経営および出版事業の機能を最優先し、動画配信サービスの「ニコニコ」の復旧には1カ月以上を要する見込みだという。

同社によると、システム障害は8日午前3時30分頃に発生した。グループ内の複数のサーバーにアクセスできない状況となり、すぐに社内で分析調査をした結果、「ニコニコ」を中心とするサービス群を標的にしたランサムウェアを含む大規模サイバー攻撃がグループデータセンター内のサーバーへ行われていることが確認されたという。

同社では8日中に対策本部を立ち上げ、被害の拡大阻止とデータ保全のために直ちにデータセンター内のサーバーをシャットダウンするなどの緊急措置を講じたとし、現在まで被害状況の全容把握と復旧に向けた調査対応を進めているという。

○2024年6月のKADOKAWAへのランサムウェア

○侵入原因は、フィッシング等によるアカウント窃取と推測

○被害
- システムの障害によるサービスの停止
- 25.4万件の個人情報を含む情報の漏えい

○ 攻撃者が公開したとされる情報が、SNS等を通じて拡散される2次被害。投稿削除対応なども発生

ランサム事例②（ノーウェアランサム）

○ マルウェア（ランサムウェア）が存在しない脅迫の事例

国際塩基配列データベース「DDBJ」に対するサイバー脅迫に関するご報告

2024/10/22 お知らせ AGD BioProject BioSample DDBJ DRA GEA JGA MetaboBank TogoVar DDBJ Center

ホーム > ニュース > 国際塩基配列データベース「DDBJ」に対するサイバー脅迫に関するご報告

大学共同利用機関法人 情報・システム研究機構 Research Organization of Information and Systems

2024年10月22日
大学共同利用機関法人情報・システム研究機構

情報・システム研究機構 国立遺伝学研究所 生命情報・DDBJセンター（センター長：有田正規）は、国際ハッカー集団から、DDBJ（国際塩基配列データベース連携）の公開データを窃取したと2024年10月8日深夜にX（旧Twitter）上で脅迫を受けました。徹底した調査を実施いたしましたが、現在のところ、システムへの不正侵入、システム内部の改ざん、データ消失等は検出されていません。

【詳細】

- DDBJは国際塩基配列データベース連携（INSDC：インスディーシー）と呼ばれる事業を、米国及び欧州とともに1987年より30年以上実施し、全世界の誰でも、自由に学術情報を利用できるオープンサイエンスの基盤を築いてきました。この世界的なオープンサイエンスの取組に対して、10月8日深夜、サイバー脅迫を受けました。
- 犯行声明を発表したのはCyberVolk（サイバーフォルク）と名乗る国際ハッカー集団です。DDBJのデータ5%を公開し、1万ドルを支払わなければ残りの95%も公開すると、X（旧Twitter）上で脅迫しています。
- 知識とデータの無償公開を推進する大学共同利用機関配下のDDBJに、このような犯行声明が出されたことは大変遺憾です。犯行グループが窃取したと主張し公開したデータは、BioSampleと呼ばれるデータベースの情報であり、もともと誰でも無料でダウンロードでき、脅迫は無意味です。
- DDBJではシステムへの不正侵入等が無いか、徹底した内部調査を実施いたしました。現在のところ、システムへの不正侵入、システム内部の改ざん、データ消失等は検出されていません。
- 研究者の方々へのサービスは通常通り継続していますが、DDBJに新規登録されたデータは10月10日以降、米国及び欧州に反映されていません。登録された研究者の方々には多大なご迷惑をおかけしており、大変申し訳ありません。10月22日より通常のデータ交換を再開させていただく予定です。
- 誰でもダウンロードできるデータであったとしても、サイバー脅迫は、科学と社会をつなぐ公共事業に対する脅威であり、この行為に対し、DDBJは断固として反対いたします。オープンサイエンスを掲げる学術機関に対する攻撃は、世界に対する攻撃でもあります。今後こうした行為を断固として許さない社会の構築にも尽力したいと考えています。

https://www.ddbj.nig.ac.jp/news/ja/2024-10-22

ランサムウェアの進化

○ ランサムウェアは登場から約35年経過するが、最近約15年で大きく変化
○ 当初は個人向けの脅迫が主だったが、組織・企業を脅迫する脅威に進化（変化）

時期	概要
1989	ランサムウェア登場（AIDSトロイの木馬）
:	
2010～	ビットコインなど仮想通貨登場　ランサムウェアが増加（ばらまき型　拡散なし、端末の暗号化などで脅迫）
2013	「CryptLocker」ランサムウェアの登場
2016	10大脅威2016に初ラインクイン（個人2位、組織7位） 日本語表示ランサムウェア増加、スマートフォン向けランサムウェア（端末ロック型）登場
2017	ワーム機能をもつランサムウェアWannaCry登場。10大脅威2017（個人、組織2位） MS17-010 smb脆弱性を悪用して、組織内で感染拡大する機能を保持
2018	人手によるランサムウェア登場
2019	二重脅迫ランサムウェア登場　（暗号化＋情報の暴露で脅迫を実施） RDPなど公開サーバから侵入するケースを確認
2020	個人向け10大脅威からランサムウェアが外れる
2020～	三重脅迫、四重脅迫ランサムウェア登場（＋関係者への連絡、DDoS攻撃） ノーウェアランサム登場

多重脅迫ランサムウェア

以下で脅迫して、金銭の支払いを要求する。

- ファイルの暗号化
- 窃取した（機密）情報の暴露
- ランサムウェア被害について関係者への連絡
- DDoS攻撃

二重脅迫ランサムウェア：ファイルの暗号化＋窃取した（機密）情報の暴露
三重脅迫ランサムウェア：二重脅迫の手口＋関係者への連絡 or DDoS攻撃
四重脅迫ランサムウェア：4つすべてを組み合わる攻撃

ノーウェアランサム

- ファイルの暗号化を行わず、窃取した情報で脅迫を行う手口
- DDoSで脅迫するランサムDDoS攻撃
- 企業によるバックアップ取得など対策が進んだことで
  暗号化による脅迫効果が低下した可能性
  （とはいえ、バックアップの対策は不要というわけではない。）

ランサムウェアに気づくきっかけ

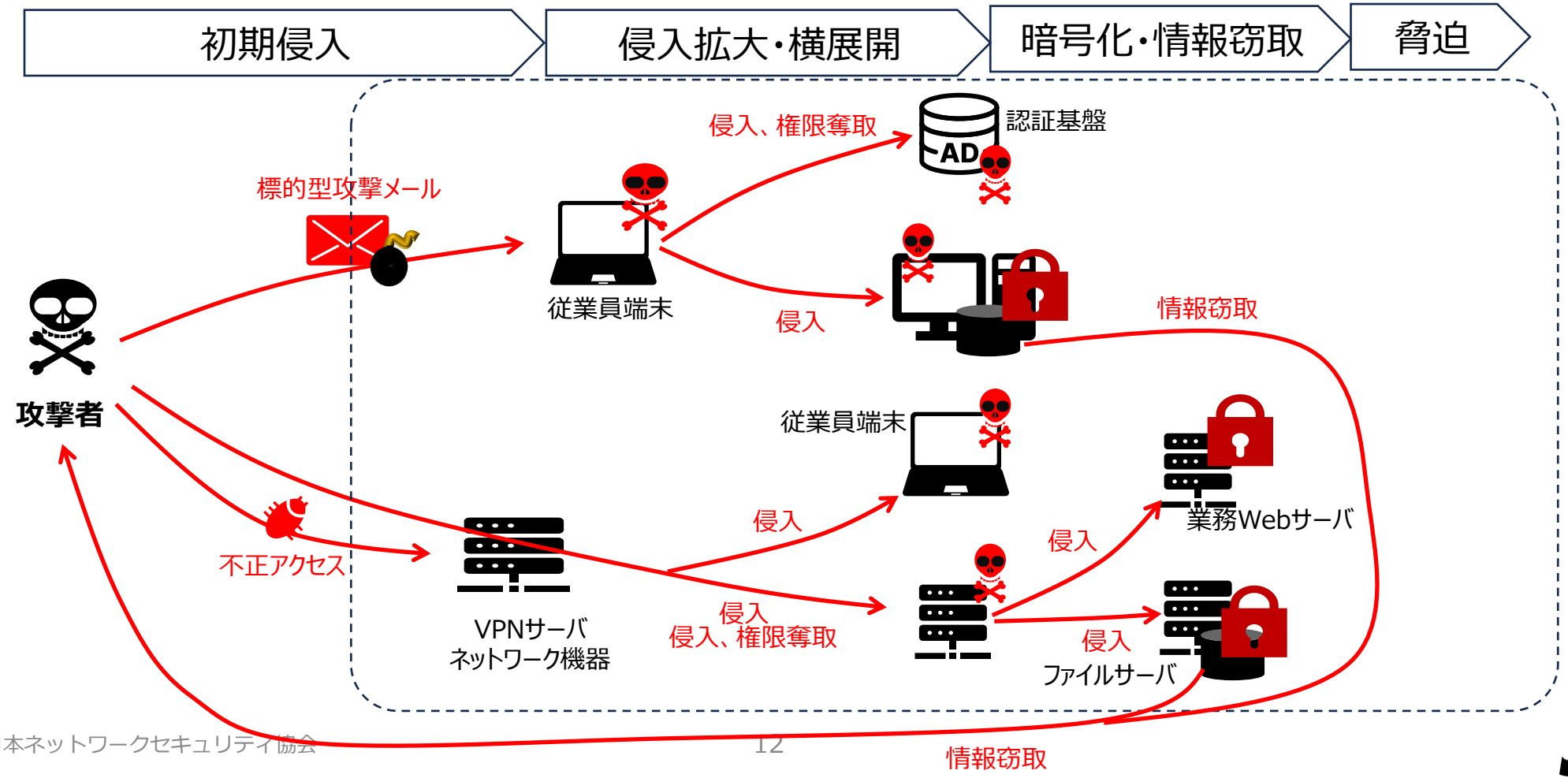
○ システム障害　（が起きて、調査したらサイバー攻撃だった）

○ 脅迫文の発見

○ 外部からの連絡（暴露サイトへの掲載など）　など

ランサムウェア攻撃の流れ

従来の攻撃は拡散しながらランサムウェアに感染した端末を攻撃（暗号化等）していたのに対して、
最近の攻撃では価値のある情報を狙って組織内に広く侵入を図り、暗号化や情報窃取を行う。



ランサムウェアの主な侵入手口

■ インターネット公開機器に対する不正アクセス

１）脆弱性を悪用する

在宅業務で必要なSSL-VPNサーバなど

２）外部公開されたリモートデスクトップなどから侵入

不用意な行為、設定ミス、簡単なパスワード など

■ Web、メールなどから

１）フィッシングによるアカウント情報窃取

２）Webサイト、メールの添付ファイルにマルウェアを仕込む

システムの脆弱性を突いた攻撃

○ ランサムウェアの侵入手口で頻出

○ 攻撃対象が変化

2010年代：Windows、MS-Office、Flash Playerなど

2020年代：VPN機器やCMSなどインターネット公開機器

○ 公開前（直後）の脆弱性を悪用するケース

4月 IIJセキュアMXサービスにおけるお客様情報の漏えいインシデント

事案発生時では未発見の脆弱性Active! mailの脆弱性を悪用

ランサムウェアに対する対策（予防策）

○ 予防のための対策

攻撃は、初期侵入～横展開～ランサムウェア展開、情報窃取等
多岐にわたるので、広範な対策が必要

- 公開サーバ（、VPN機器）への不正アクセス対策
- 標的型攻撃、フィッシングメール対策（教育含め）
- PC、サーバへのセキュリティ対策（監視、設定含む）
  OS、ソフトウェアの最新のセキュリティパッチを適用
  監視システムの導入
    ウイルス対策、EDR、NDR、DLP、AD認証監視、IDS/IPS、WAF等

ランサムウェアに対する対策（発生後）

○ インシデント発生後の準備

- 適切なバックアップの運用の実施

  バックアップデータが暗号化されないように保管

  復旧手順の準備、訓練

- インシデント発生時の対応体制を整備

  インシデント対応フロー、手順を用意する

  インシデント対応時の緊急体制を用意する

  調査を依頼するサービス、業者を選定しておく

脅威は変わっているのかどうか

○「XX年連続」とはなっているが、見出しレベルでも少し変わっている。
○ 解説内容を見ると、比較的変化があるものと無いものに分かれる。

順位	10大脅威2024	10大脅威2025
1	ランサムウェアによる被害	ランサム攻撃による被害
2	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃
3	内部不正による情報漏えい等の被害	システムの脆弱性を突いた攻撃
4	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	機密情報等を狙った標的型攻撃
6	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組みを狙った攻撃
7	脆弱性対策情報の公開に伴う悪用増加	地政学的リスクに起因するサイバー攻撃
8	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）
9	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺
10	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等

10大脅威2024から10大脅威2025の変化

変化した点を把握し、自組織の対策が十分かレビュー（見直し）することが重要

2024「ランサムウェアによる被害」 → 2025「ランサム攻撃による被害」

○ 対策の実施に対抗する攻撃手法の変化
- ランサム攻撃 ＝ ランサムウェアを用いた攻撃
- ランサムウェアを用いない（暗号化による脅迫をしない）攻撃事例の出現（ノーウェアランサム）

2024「テレワーク等のニューノーマルな働き方を狙った攻撃」
→ 2025「リモートワーク等の環境や仕組みを狙った攻撃」

○ テレワーク、リモートワークは定着したが、関連システムの脆弱性や攻撃リスクは継続。
- 2020年～ 当初はパンデミックによる急激なテレワークの導入による脆弱な体制（私有環境、SNS等）
- リモートワークのために必要な環境は、引き続き攻撃者の格好のターゲット
  VPN製品（サーバ）・・・脆弱性、設定ミス
  アカウント利用情報による不正アクセス（VPN接続、RDP、クラウドサービス）
  リモートワーク用の端末

まとめ

○ セキュリティについては、日進月歩。日々状況が進化しています。

○ 基本的な知識はベースとして重要ですが、加えて最新の動向を
　把握することも重要となります。

○ SEA/Jのテキストで基本的な内容は理解可能と思います。
　加えて実務面を考えると様々な情報収集や経験が重要になります。