ランサムウェアと生成AIが変える サイバー攻撃の最前線

～2024年サイバーセキュリティレポート～

Cyber Security Laboratory © Canon IT Solutions Inc.

2024年サイバーセキュリティレポート

掲載テーマ一覧

- **1章** | 2024年のサイバーセキュリティ脅威について
- **2章** | 移り変わるランサムウェア攻撃
- **3章** | スレットハンティングで検出した2024年のサポート詐欺サイトについて
- **4章** | 生成AIの関わる脅威・リスク～業務活用を行っていくために～
- **5章** | サイバー攻撃被害情報の共有と公表のあり方について

サイバーセキュリティ情報局にて公開中

Cyber Security Laboratory © Canon IT Solutions Inc.

1章 2024年のサイバーセキュリティ脅威について

概要

2024年にESET製品で検出されたマルウェアの統計を解説
日本国内におけるセキュリティトピックを紹介し、今後推奨されるセキュリティ対策を考察

2024年マルウェア検出数TOP10

1位	JS/Adware.TerraClicks	悪意のある広告を表示させるアドウェアの検出名 アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります	前年4位 ↗
2位	JS/Adware.Agent	悪意のある広告を表示させるアドウェアの汎用検出名 Webサイト閲覧時に検出されます	前年1位 ↘
3位	HTML/Phishing.Agent	フィッシング詐欺を目的としたHTMLファイルの検出名 メールの添付ファイルやWebサイトアクセス時に検出される	前年3位 →
4位	DOC/Fraud	詐欺を目的としたDOCファイルの検出名	前年2位 ↘
5位	JS/Agent	不正なJavaScriptの汎用検出名	前年6位 ↗
6位	JS/Adware.Sculinst	ユーザーを騙して拡張機能やそのほかアドウェアコンテンツをインストールさせようとするGoogle Chromeの偽の通知の検出名	前年5位 ↘
7位	HTML/Fraud	詐欺を目的としたHTMLファイルの検出名	前年8位 ↗
8位	HTML/Phishing	フィッシング詐欺を目的としたHTMLファイルの検出名	前年10位 ↗
9位	Win64/Riskware.PEMalform	64bit環境で動作するブラウザハイジャッカーの検出名	前年圏外 ↗
10位	MSIL/TrojanDownloader.Agent	MSILで作成されたダウンローダーの検出名 過去に、「AgentTesla」「Smoke Loader」のダウンロードを確認	前年圏外 ↗

アドウェア　詐欺を目的としたマルウェア　ダウンローダー　その他

2024年のセキュリティトピック

- ランサムウェア感染被害と流出情報の拡散
- 代行会社によってハードルが下がったDDoS攻撃
- 不正アクセス・Webページ改ざん起因の情報流出

対策ポイント	セキュリティ対策
脆弱性	• ハードウェア・ソフトウェア管理 • セキュリティパッチ適用
DDoS攻撃	• IPアドレス、ポートの制限 • BOT化の検知施策
ランサムウェア	• 機器の脆弱性、認証管理 • オフラインバックアップ

統計やトピックを踏まえたセキュリティ対策を実施しよう

Cyber Security Laboratory © Canon IT Solutions Inc.

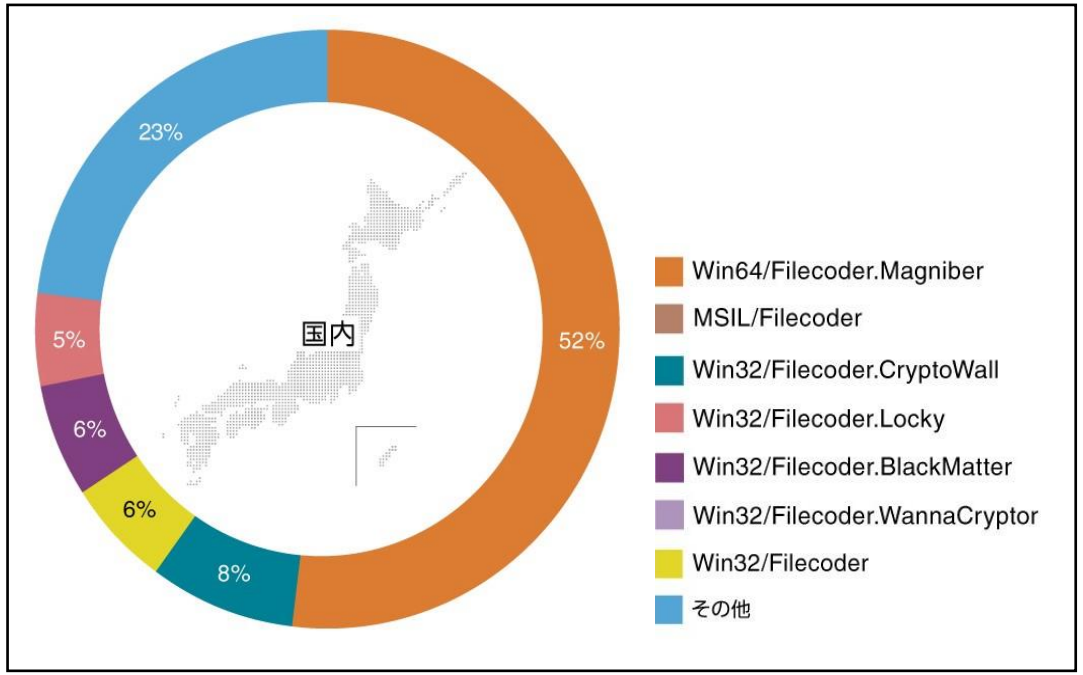
2章 移り変わるランサムウェア攻撃

～フィジカル空間の犯罪スキームを取り入れて進化する攻撃体制の考察～

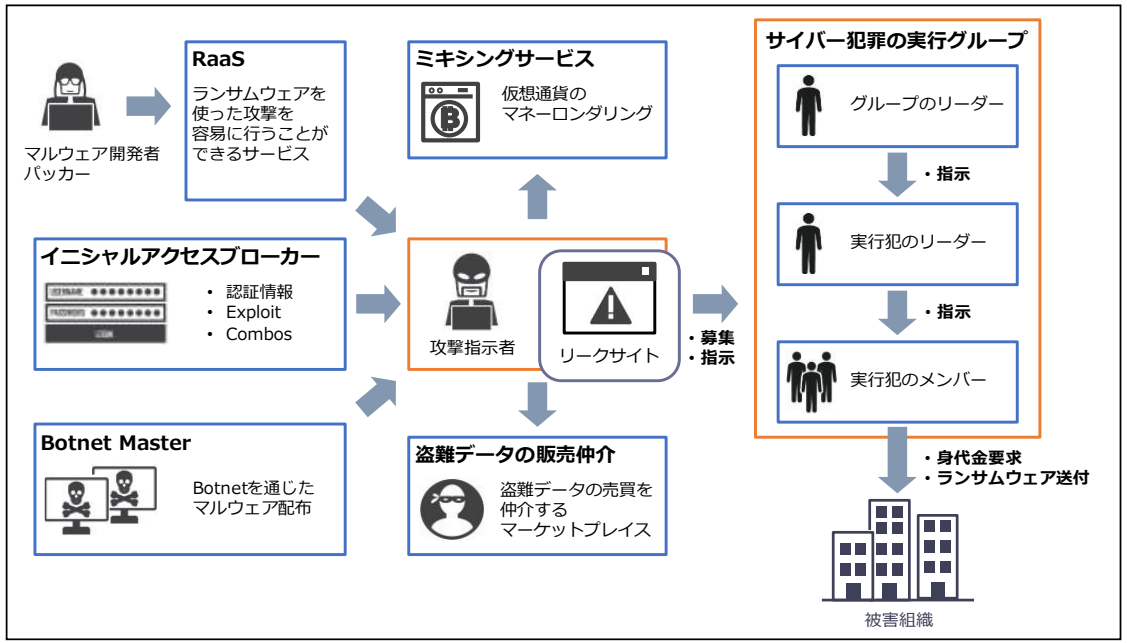
概要

2024年におけるランサムウェア攻撃の動向や最新の攻撃手法について紹介
匿名・流動型犯罪グループによる事件を引き合いに、**将来起こりうるランサムウェア攻撃**について考察

2024年に検出されたランサムウェアファミリー



将来起こりうるランサムウェア攻撃（イメージ）



一般人がサイバー攻撃の実行者となってしまうことを防ぐ注意喚起の取り組みを整備しよう

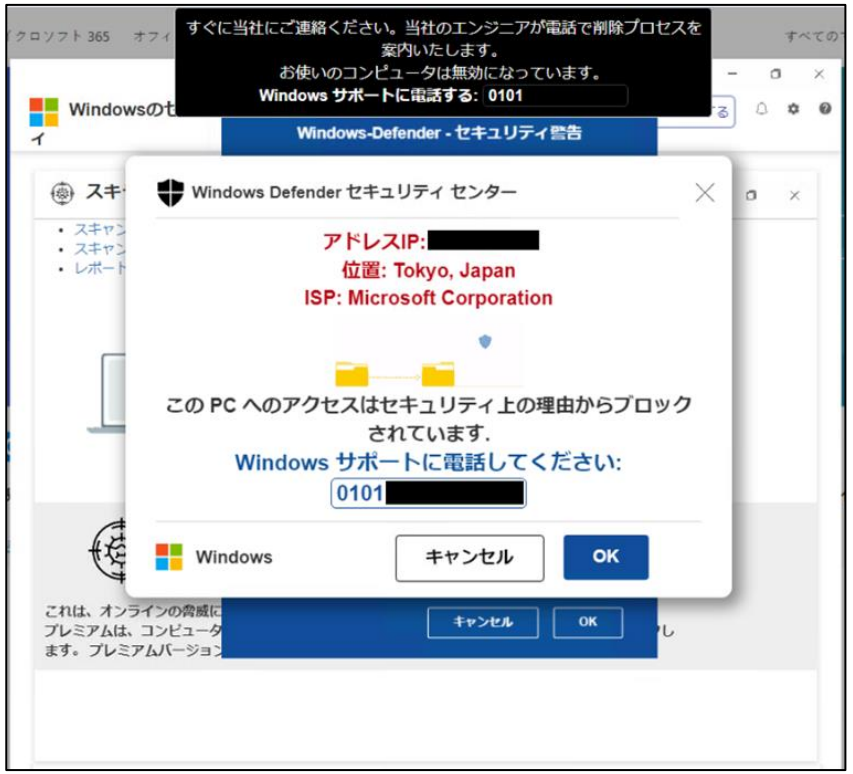
Cyber Security Laboratory © Canon IT Solutions Inc.

3章 スレットハンティングで検出した 2024年のサポート詐欺サイトについて

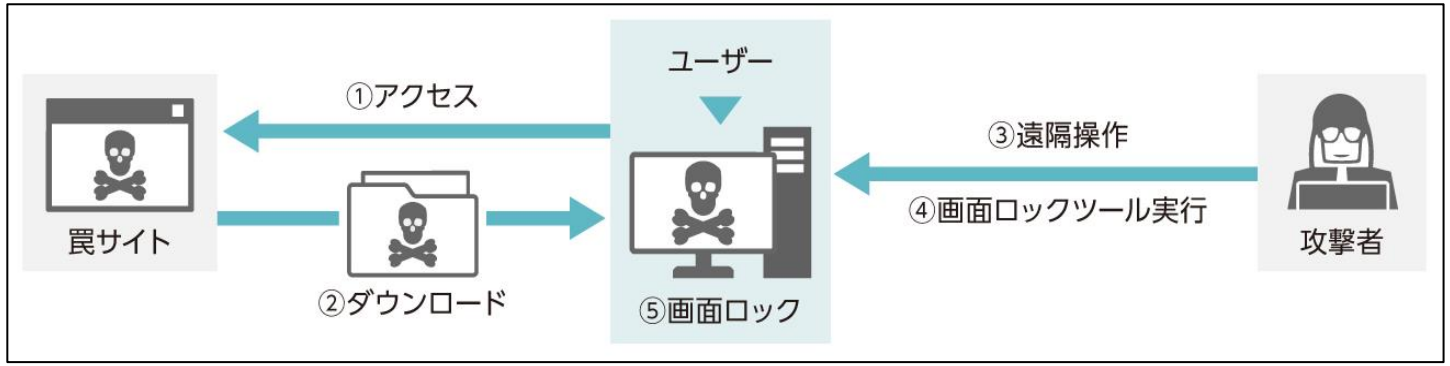
概要

近年のサポート詐欺サイトの概要を説明
2024年から報告されるようになった**画面ロックツールを用いた新しい攻撃手法**について紹介

サポート詐欺サイトの一例



画面ロックツールを用いた新しい攻撃手法



サポート詐欺は誰もが遭遇する可能性のある脅威
一人一人が対策を学べるように、組織教育の見直しを

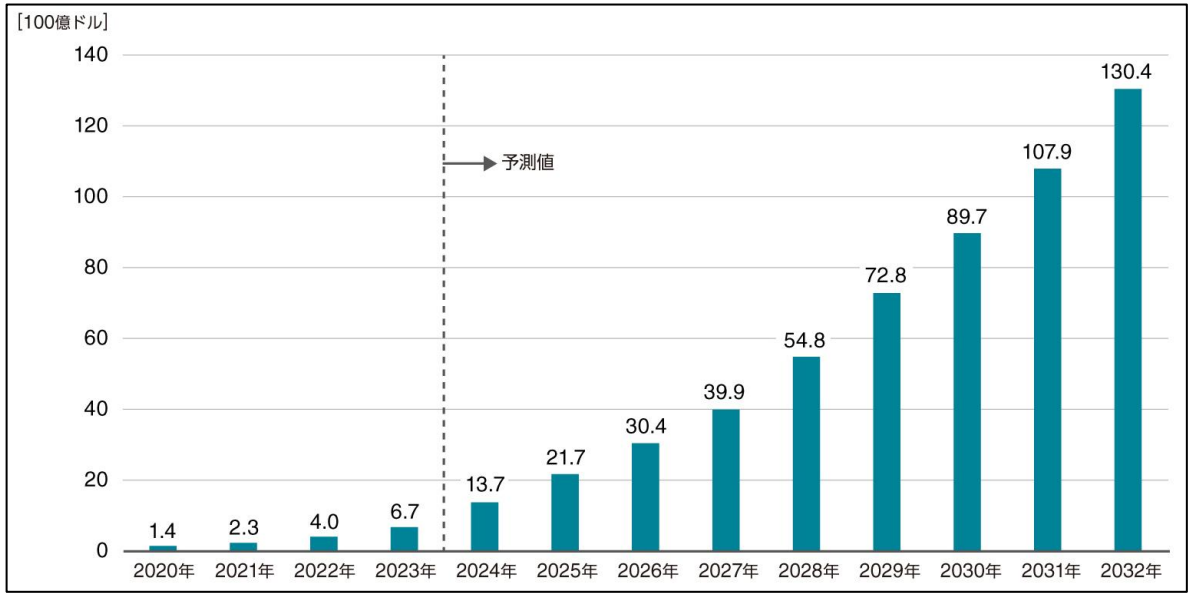
Cyber Security Laboratory © Canon IT Solutions Inc.

4章 生成AIの関わる脅威・リスク～業務活用を行っていくために～

概要

生成AIの業務活用例と一般ユーザーが遭遇する可能性が高いリスクについて解説
リスクに対して、どのような対策を講じればよいかを紹介

生成AIの利用拡大と今後の予測



＊ Generative artificial intelligence (AI) revenue worldwide from 2020 with forecast until 2032を参考に作成
(https://www.statista.com/statistics/1417151/generative-ai-revenue-worldwide/)

一般ユーザーが遭遇しうるリスク

- ビジネス利用によるリスク
  - ✓ プロンプト・インジェクション
  - ✓ 機密情報漏洩
  - ✓ ハルシネーション
- 悪意ある攻撃者によるリスク
  - ✓ フェイクコンテンツ
  - ✓ サイバー攻撃悪用

→ OWASP大規模言語モデル
・アプリケーションリスクトップ10

日常的に情報収集を行うことで生成AIを悪用した攻撃の被害に遭うリスクを低減しよう

Cyber Security Laboratory © Canon IT Solutions Inc.

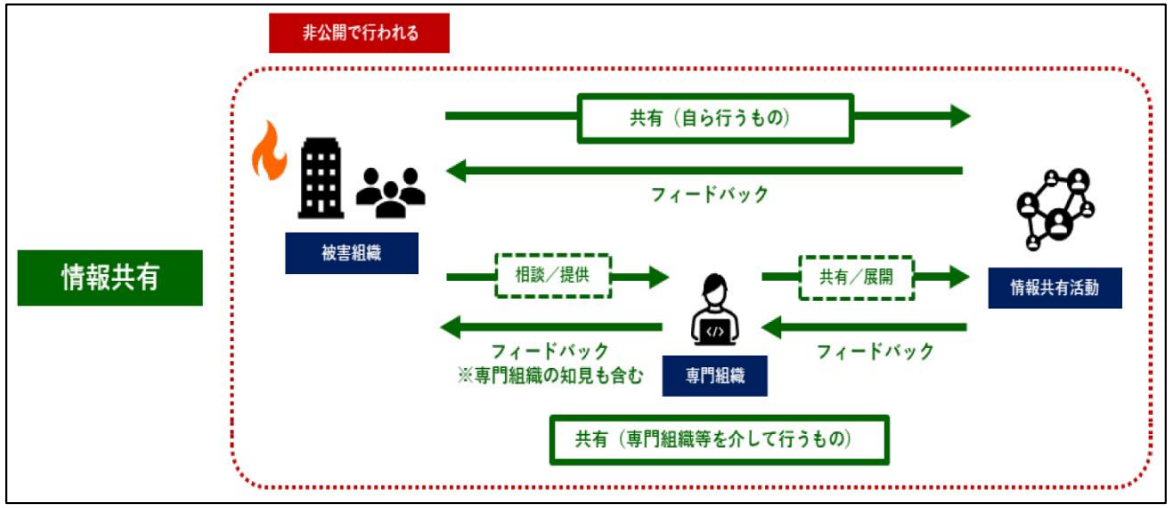
5章 サイバー攻撃被害情報の共有と公表のあり方について

概要

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」について概要を紹介
実際のインシデントでの情報共有について、ケーススタディとして考察

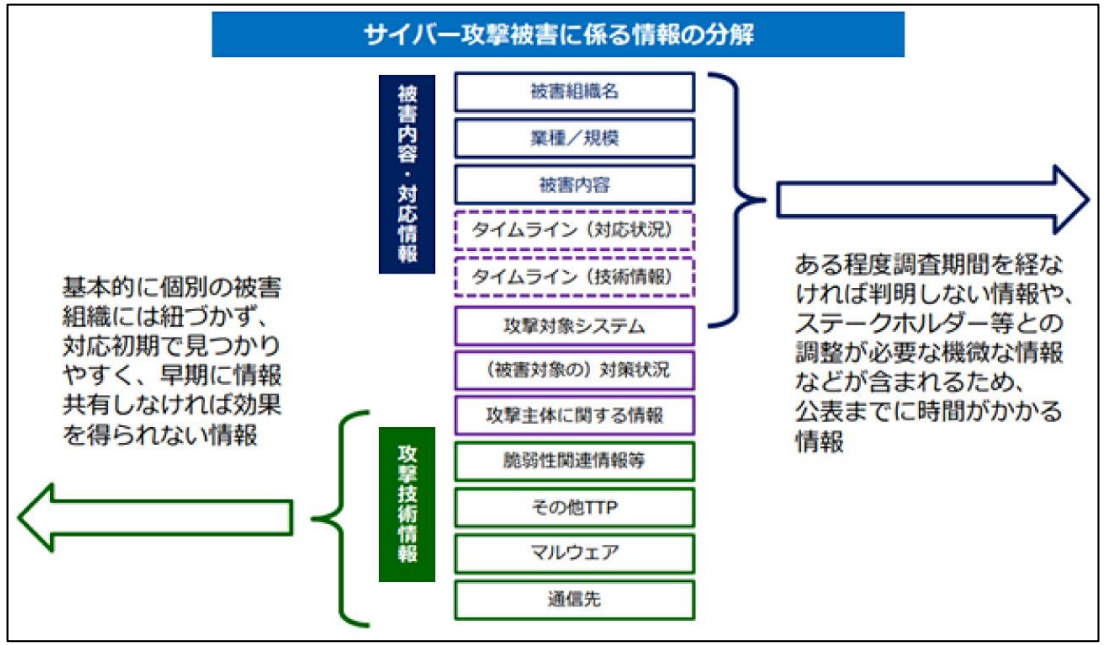
「サイバー攻撃被害に係る情報の共有・公表ガイダンス」

サイバー攻撃被害組織における情報共有/公開の指針



＊「サイバー攻撃被害に係る情報の共有・公表ガイダンス」
（https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html）

サイバー攻撃被害に係る情報の分解



「情報共有」と「被害公表」を想定した、リスクを極小化するための見直しが求められている

Cyber Security Laboratory © Canon IT Solutions Inc.

サイバーセキュリティ情報局のご紹介

キヤノンマーケティングジャパンが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか

サイバーセキュリティラボがまとめた

日本におけるマルウェア動向を

詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局　検索

Cyber Security Laboratory © Canon IT Solutions Inc.

ご視聴ありがとうございました。