

2022年のセキュリティ脅威動向と 2023年に求められる対策

キヤノンITソリューションズ株式会社
サイバーセキュリティラボ
セキュリティエバンジェリスト

西浦 真一, CISSP

自己紹介



□ 保有資格

CISSP

情報処理安全確保支援士 ほか



第009576号



Certified Information
Systems Security Professional

西浦 真一

セキュリティエバンジェリスト

キヤノンITソリューションズ株式会社
サイバーセキュリティラボ

- 2006年より、ネットワークを中心としたセキュリティリスク対策の提案や海外セキュリティ製品のローカライズに従事
- レポートの執筆やセミナー・カンファレンス等でセキュリティに関する情報を発信

□ 社外活動

JNSA (NPO 日本ネットワークセキュリティ協会)

- セキュリティ理解度チェックWG リーダー
- インシデント被害調査WG サブリーダー

キャノンITソリューションズ サイバーセキュリティラボ

1

調査・研究

- サイバー攻撃の調査
- 大学との共同研究
- セキュリティ技術の開発

2

サービス

- マルウェア解析
- スレットハンティング
- セキュリティアドバイザリ

3

情報発信

- 技術レポートの公開
- 脅威情報の発信
- 産学連携

サイバーセキュリティ情報局



半期ごとのサイバーセキュリティレポート、
マルウェアレポートのほか、
セキュリティに関する情報を提供



サイバーセキュリティ情報局

Search

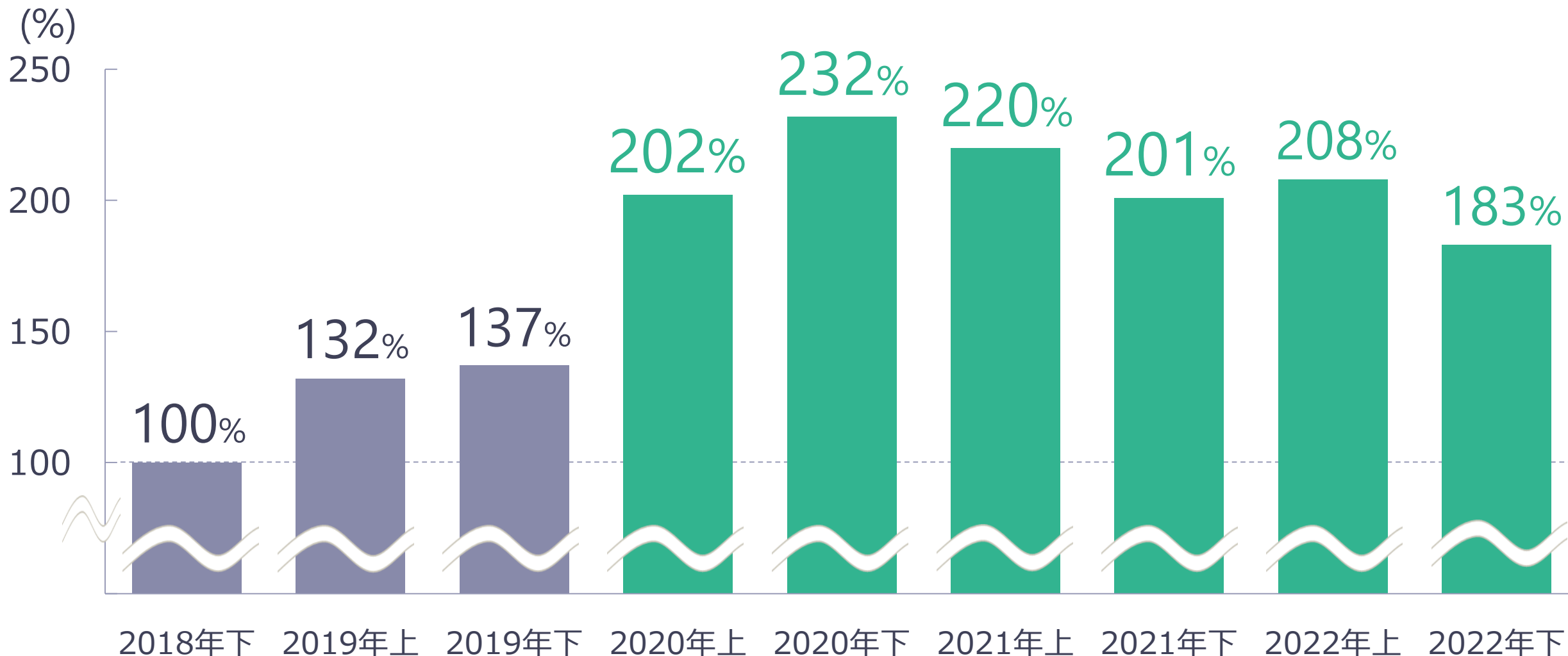
本日はお話しすること

1. 2022年の
セキュリティ脅威動向
2. 対策のポイント

本日はお話しすること

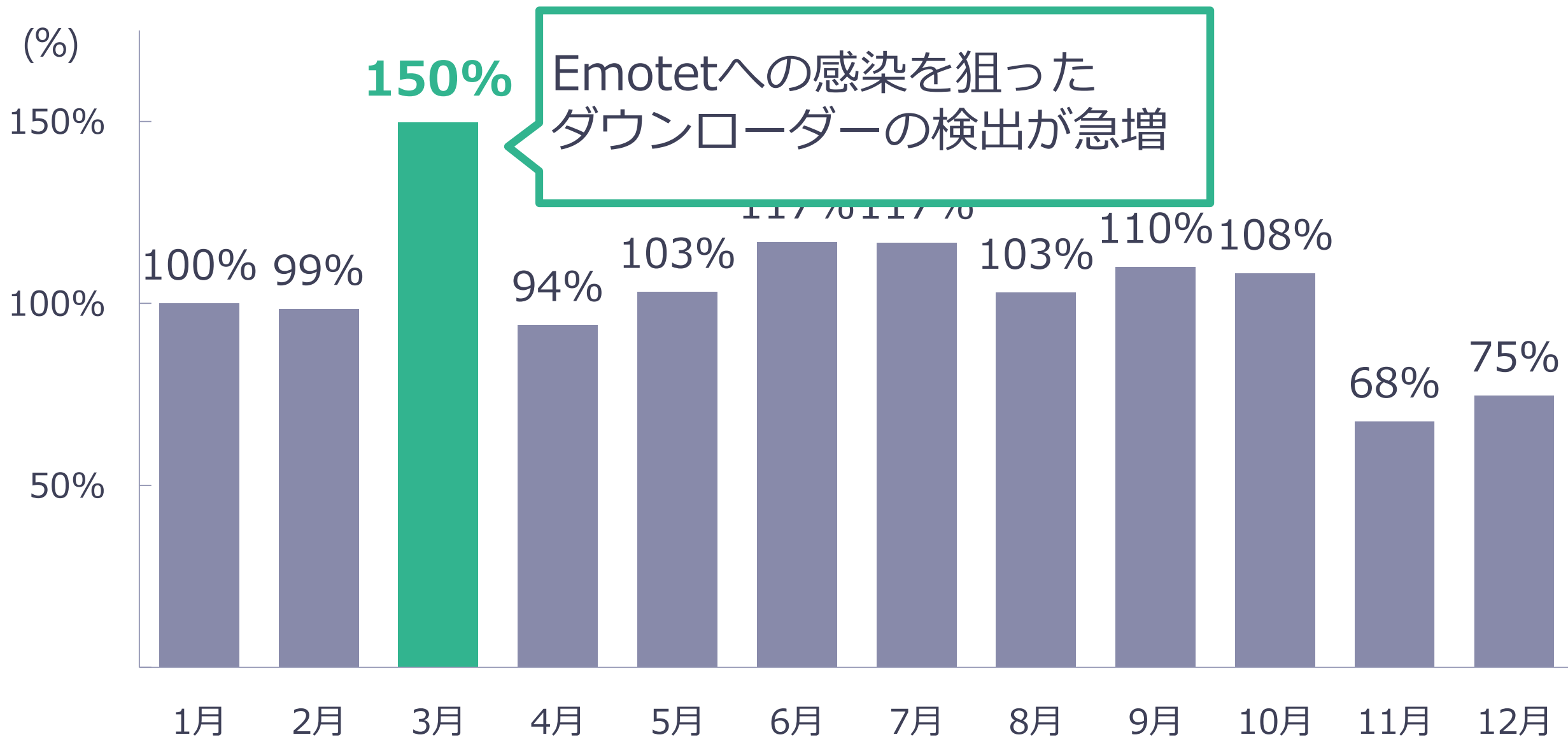
1. 2022年の
セキュリティ脅威動向
2. 対策のポイント

国内のマルウェア検出総数の推移



(※)ESETの国内検出データより作成

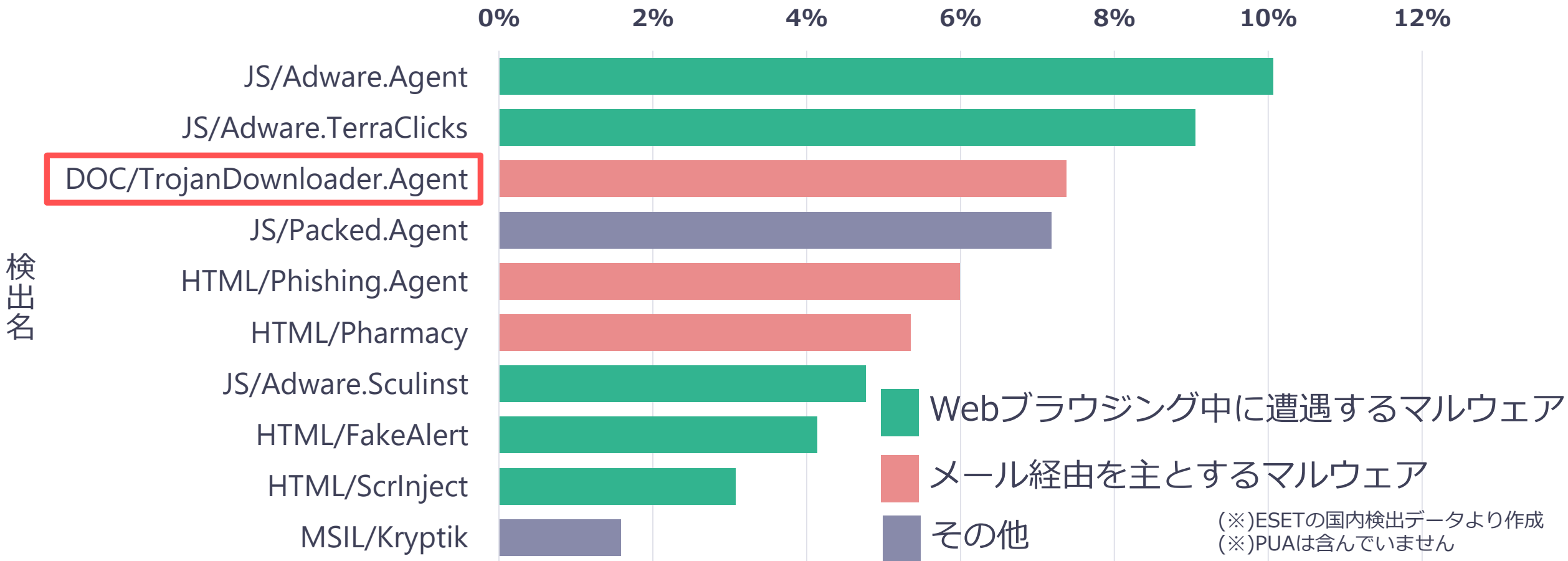
2022年の国内マルウェア検出数推移



(※)ESETの国内検出データより作成

国内で検出されたマルウェアの内訳（2022年）

検出数の上位10種



Emotetへの感染を狙う大規模な攻撃キャンペーンをはじめ、メール経由を主とするマルウェアの検出が増加

注目すべき2つの脅威



**Emotet &
Downloader**



Ransomware

Emotet & Downloader

マルウェアによるダウンローダーの利用

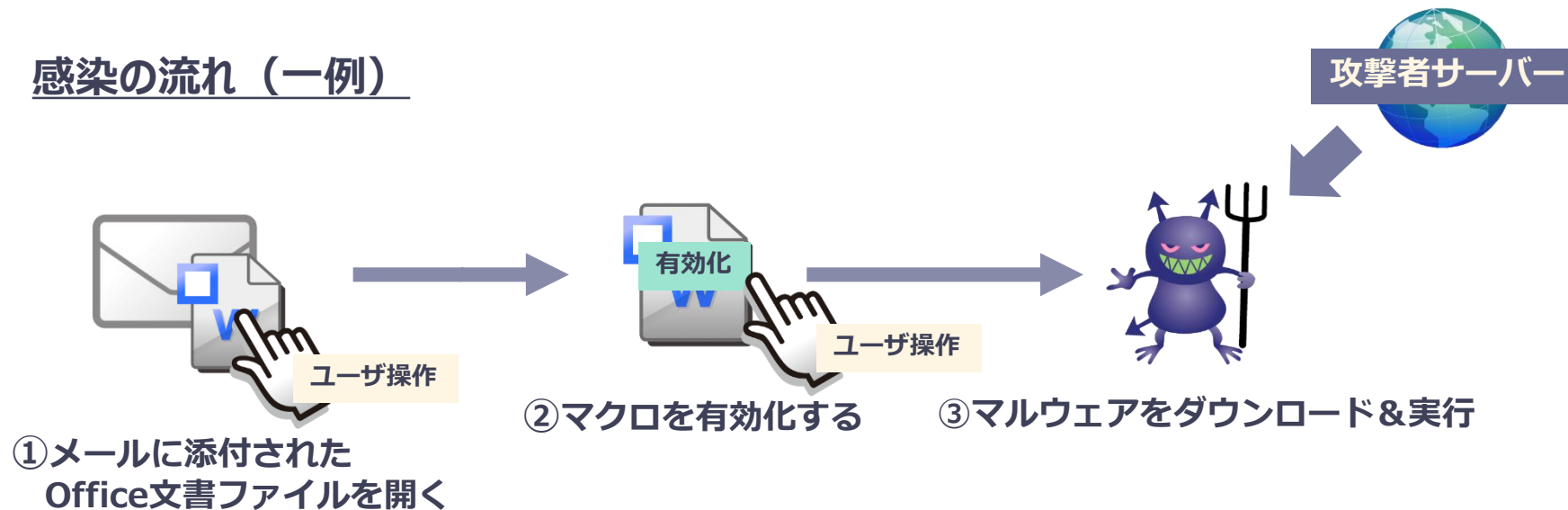
ダウンローダーとは

マルウェアをダウンロードするプログラム

攻撃者がダウンローダーを使用するメリット

1. 変更が容易でセキュリティ製品による**検出を逃れやすい**
2. 感染させるマルウェアを**自在に変更**（アップデート）できる

感染の流れ（一例）



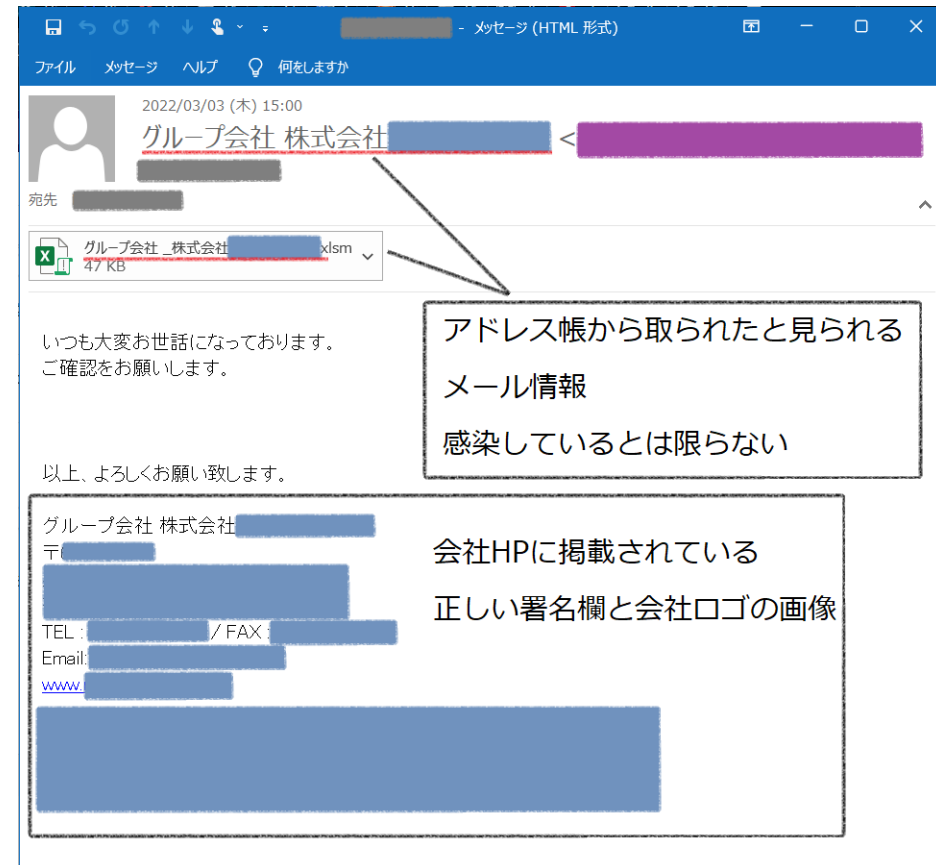
Emotet

2014年頃にバンキングマルウェアの1つとして確認

2017年頃から様々なマルウェアをダウンロードし感染させる媒介機能を持ち全世界で多くの被害が発生

Emotetがもたらす主な被害

- 情報漏えい
- ランサムウェアなど
他のマルウェアへの感染
- 社内端末への感染拡大
- Emotet感染を狙った
ばらまきメール送信の踏み台



実際する組織を騙るなりすましメール

出典: JPCERT/CC | マルウェアEmotetの感染再拡大に関する注意喚起
<https://www.jpccert.or.jp/at/2022/at220006.html>

Emotet感染被害を公表した国内組織

2022年上半期に**269件**

分類別

学校法人・研究機関 10件 3%

病院 11件 4%

団体等

40件

15%

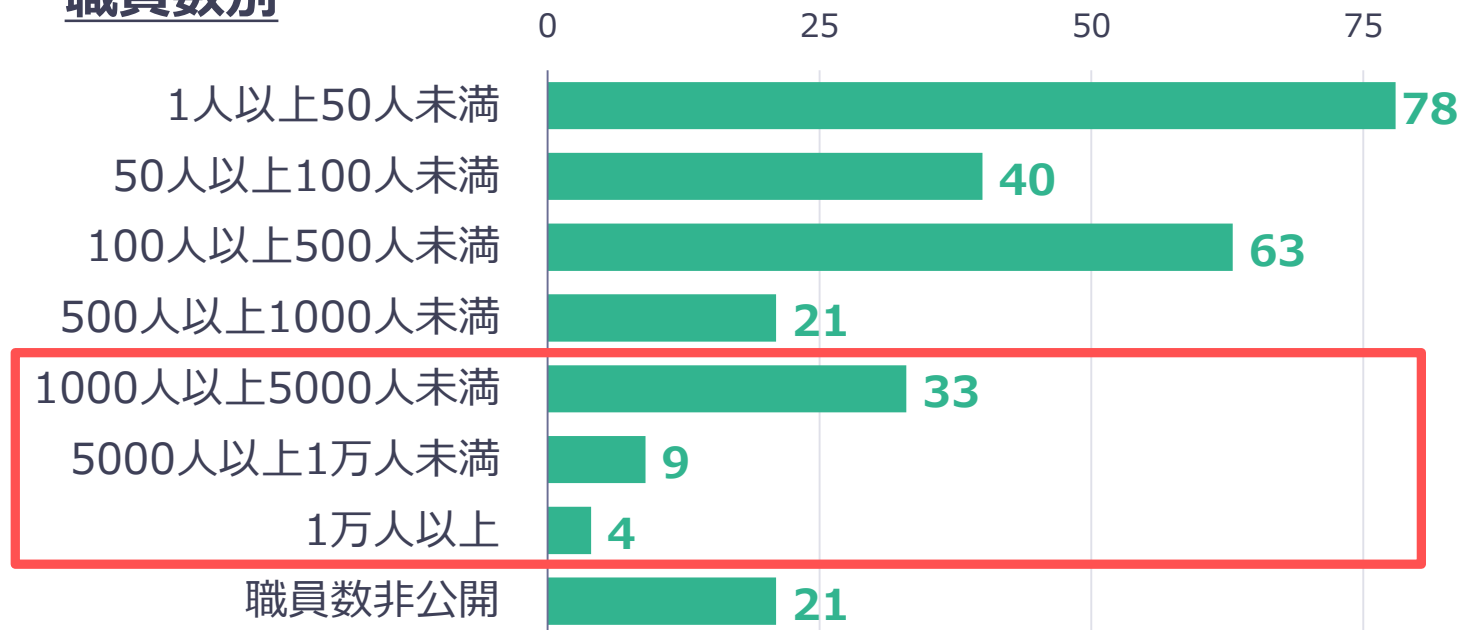
国内のEmotet
被害報告件数
269件

企業

210件

78%

職員数別



セキュリティ対策が進んでいると考えられる
大規模な組織でも多くの感染被害

システムへの対策だけでなく

セキュリティ教育や組織内の情報共有が重要

2022年におけるEmotetの変化

2022年4月

ダウンローダーの感染手法の変化
LNK形式のダウンローダーを利用し始める

2022年3月

ばらまきメールを多数検出
感染報告が多数公表される

Microsoft社がOffice製品で
VBAマクロ実行を
ブロックするよう変更

ショートカットファイルの悪用（2022/4/25～）

パターン①

メールに添付されたショートカットファイルを開く



パターン②

メールに添付された暗号化Zipファイルを展開し、ショートカットファイルを開く



ユーザ操作

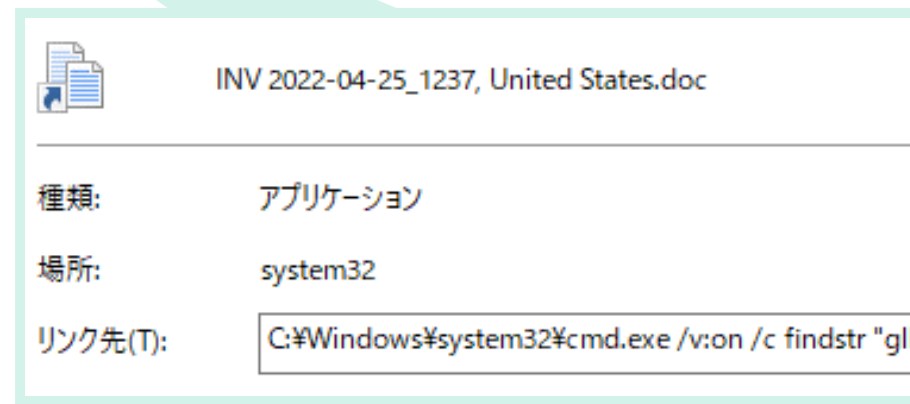
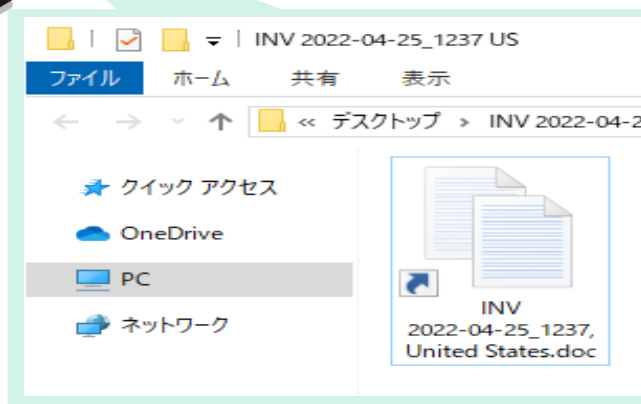
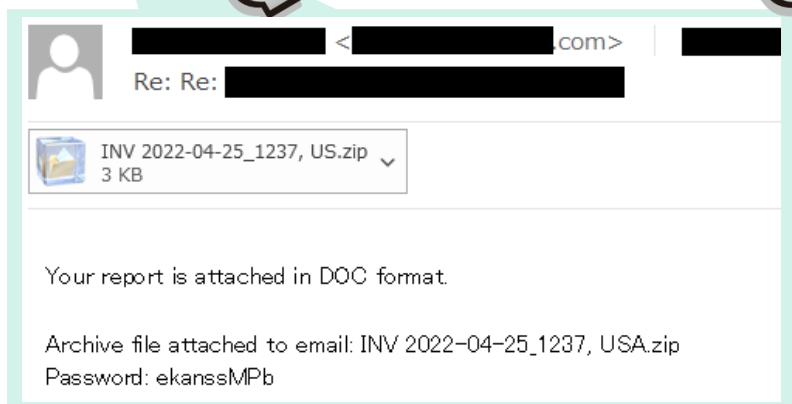
Webサーバー

• PowerShell
• cmd & wscript

スクリプトが実行され、Emotetがダウンロード・実行される



Emotetに感染



2022年におけるEmotetの変化

2022年4月

ダウンローダーの感染手法の変化
LNK形式のダウンローダーを利用し始める

2022年10月

情報窃取モジュールの変化
窃取する感染端末の設定情報が変化

2022年3月

ばらまきメールを多数検出
感染報告が多数公表される

2022年6月

情報窃取モジュールの変化
Webブラウザ（Google Chrome）に保存された
クレジットカードの認証情報も窃取対象に

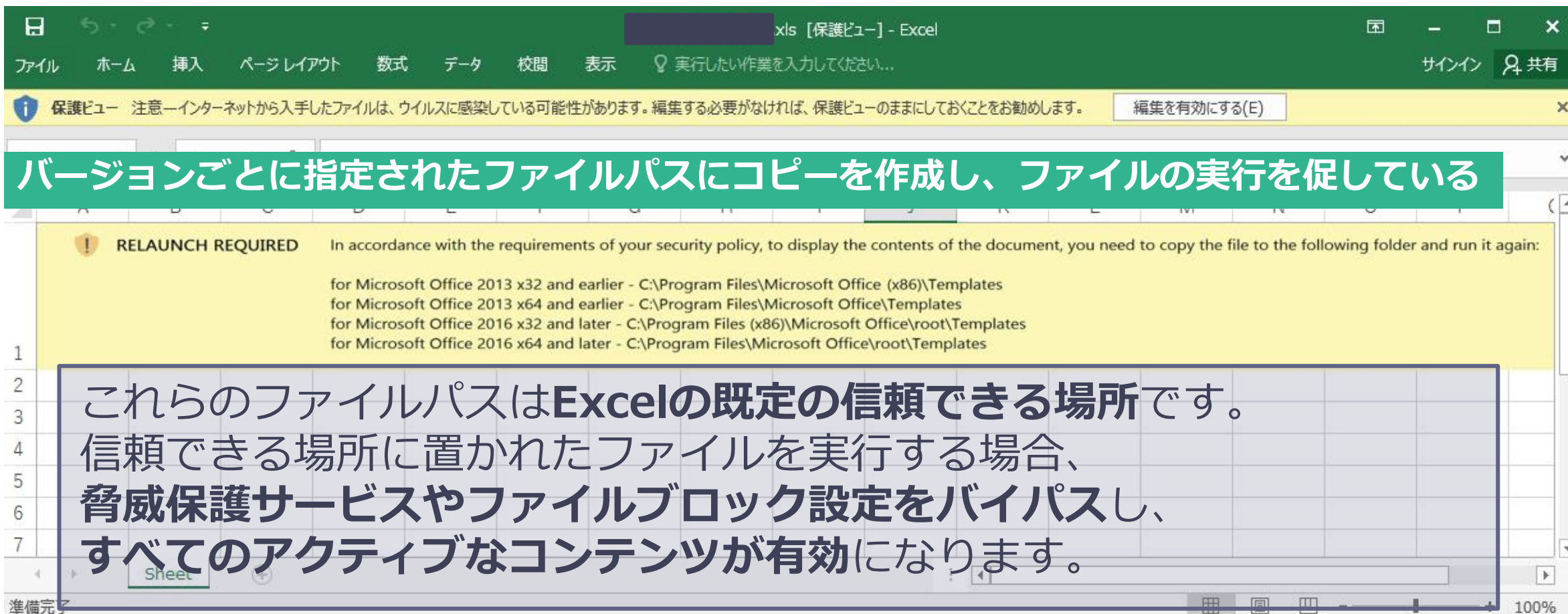
Microsoft社がOffice製品で
VBAマクロ実行を
ブロックするよう変更

2022年11月

ダウンローダーのExcelファイルの変化
添付ファイルを開いた際の表示画面が変化

2022年11月のメール送信再開後のEmotet

添付ファイルのExcelファイルが変化



The screenshot shows the Microsoft Excel interface with a security warning. The warning message reads: "RELAUNCH REQUIRED In accordance with the requirements of your security policy, to display the contents of the document, you need to copy the file to the following folder and run it again: for Microsoft Office 2013 x32 and earlier - C:\Program Files\Microsoft Office (x86)\Templates for Microsoft Office 2013 x64 and earlier - C:\Program Files\Microsoft Office\Templates for Microsoft Office 2016 x32 and later - C:\Program Files (x86)\Microsoft Office\root\Templates for Microsoft Office 2016 x64 and later - C:\Program Files\Microsoft Office\root\Templates". A green text box is overlaid on the warning, stating: "バージョンごとに指定されたファイルパスにコピーを作成し、ファイルの実行を促している". Below the warning, a blue text box contains the following text: "これらのファイルパスはExcelの既定の信頼できる場所です。信頼できる場所に置かれたファイルを実行する場合、脅威保護サービスやファイルブロック設定をバイパスし、すべてのアクティブなコンテンツが有効になります。". The Excel window title is "xls [保護ビュー] - Excel". The status bar at the bottom left says "準備完了" and the zoom level is 100%.

バージョンごとに指定されたファイルパスにコピーを作成し、ファイルの実行を促している

RELAUNCH REQUIRED In accordance with the requirements of your security policy, to display the contents of the document, you need to copy the file to the following folder and run it again:

- for Microsoft Office 2013 x32 and earlier - C:\Program Files\Microsoft Office (x86)\Templates
- for Microsoft Office 2013 x64 and earlier - C:\Program Files\Microsoft Office\Templates
- for Microsoft Office 2016 x32 and later - C:\Program Files (x86)\Microsoft Office\root\Templates
- for Microsoft Office 2016 x64 and later - C:\Program Files\Microsoft Office\root\Templates

これらのファイルパスはExcelの既定の信頼できる場所です。
信頼できる場所に置かれたファイルを実行する場合、
脅威保護サービスやファイルブロック設定をバイパスし、
すべてのアクティブなコンテンツが有効になります。

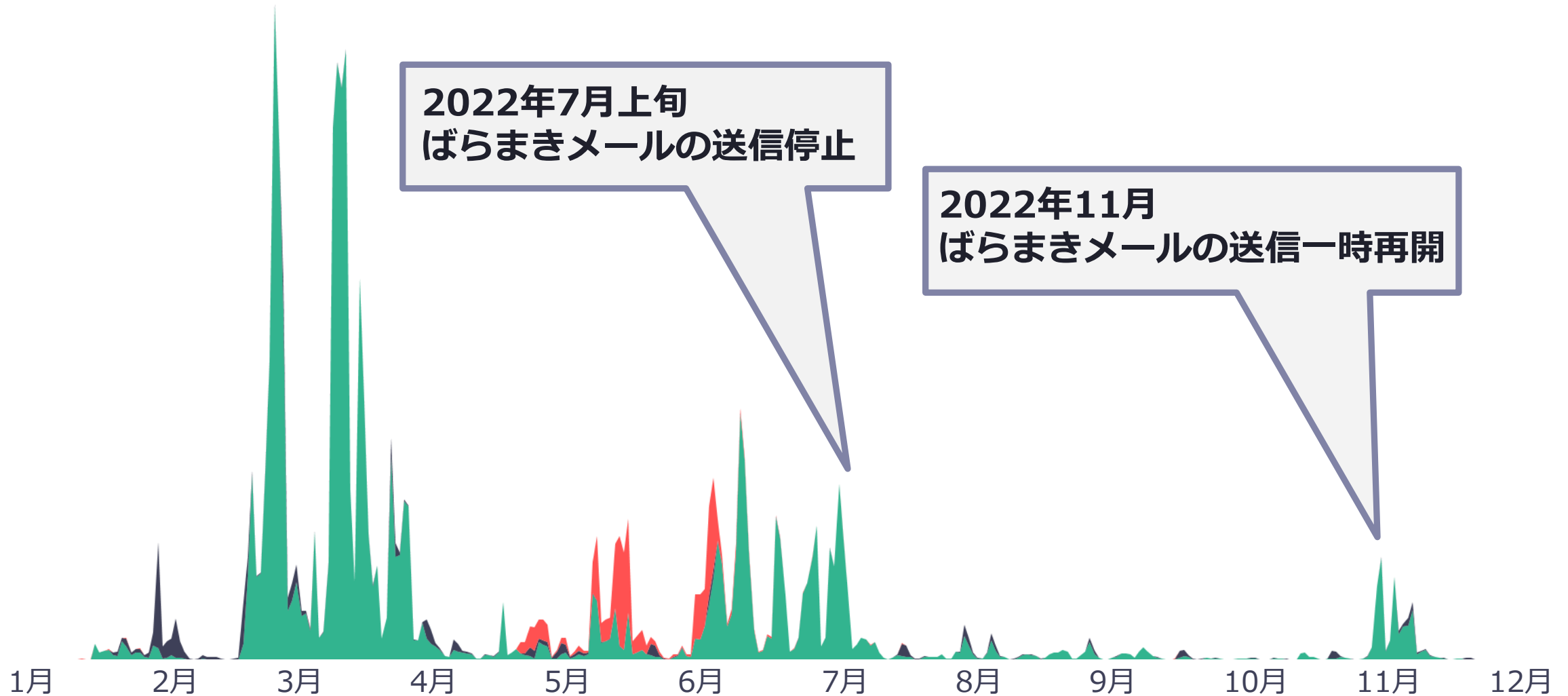
Emotetダウンローダー検出推移（2022年・国内）



■ DOC/TrojanDownloader.Agent

■ VBA/TrojanDownloader.Agent

■ LNK/TrojanDownloader.Agent



Emotetダウンロード検出推移（2022年・国内）



■ DOC/TrojanDownloader.Agent

■ VBA/TrojanDownloader.Agent

■ LNK/TrojanDownloader.Agent

2022年4月

ダウンロードの感染手法の変化

2022年10月

情報窃取モジュールの変化

2022年3月

ばらまきメールを多数検出

2022年6月

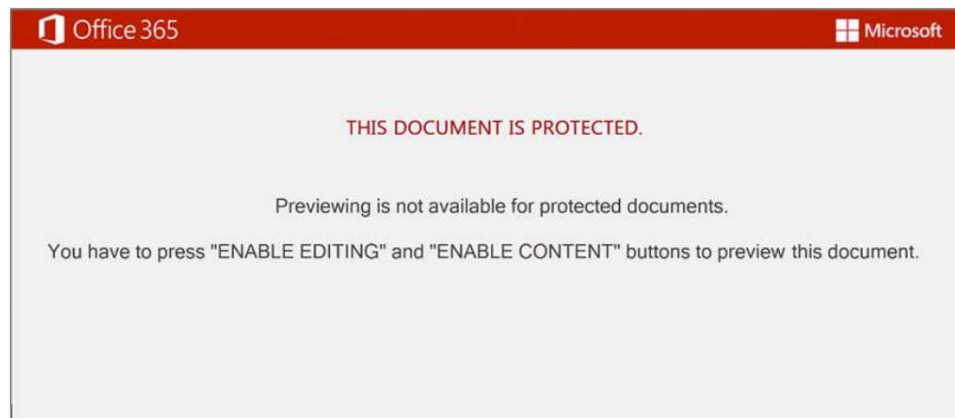
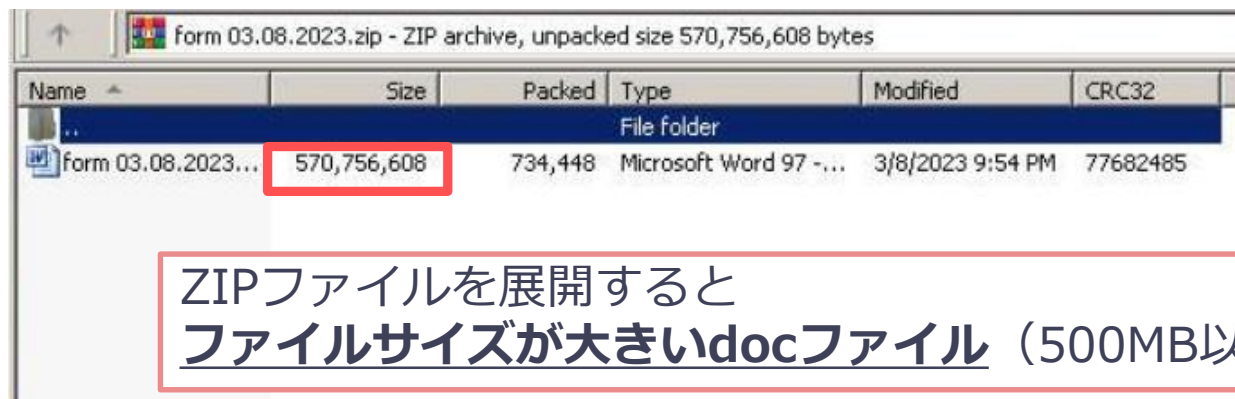
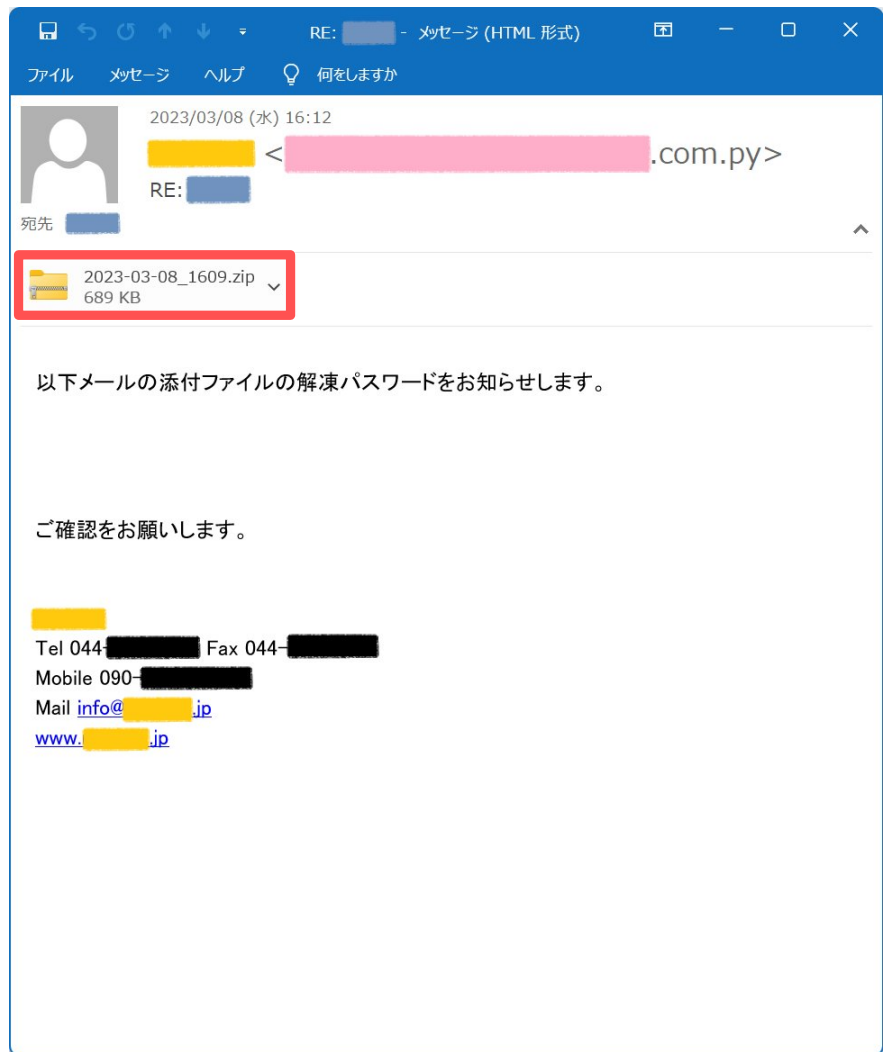
情報窃取モジュールの変化

2022年11月

ダウンロードのExcelファイルの変化

1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月

2023年3月7日、ばらまきメール送信が再開

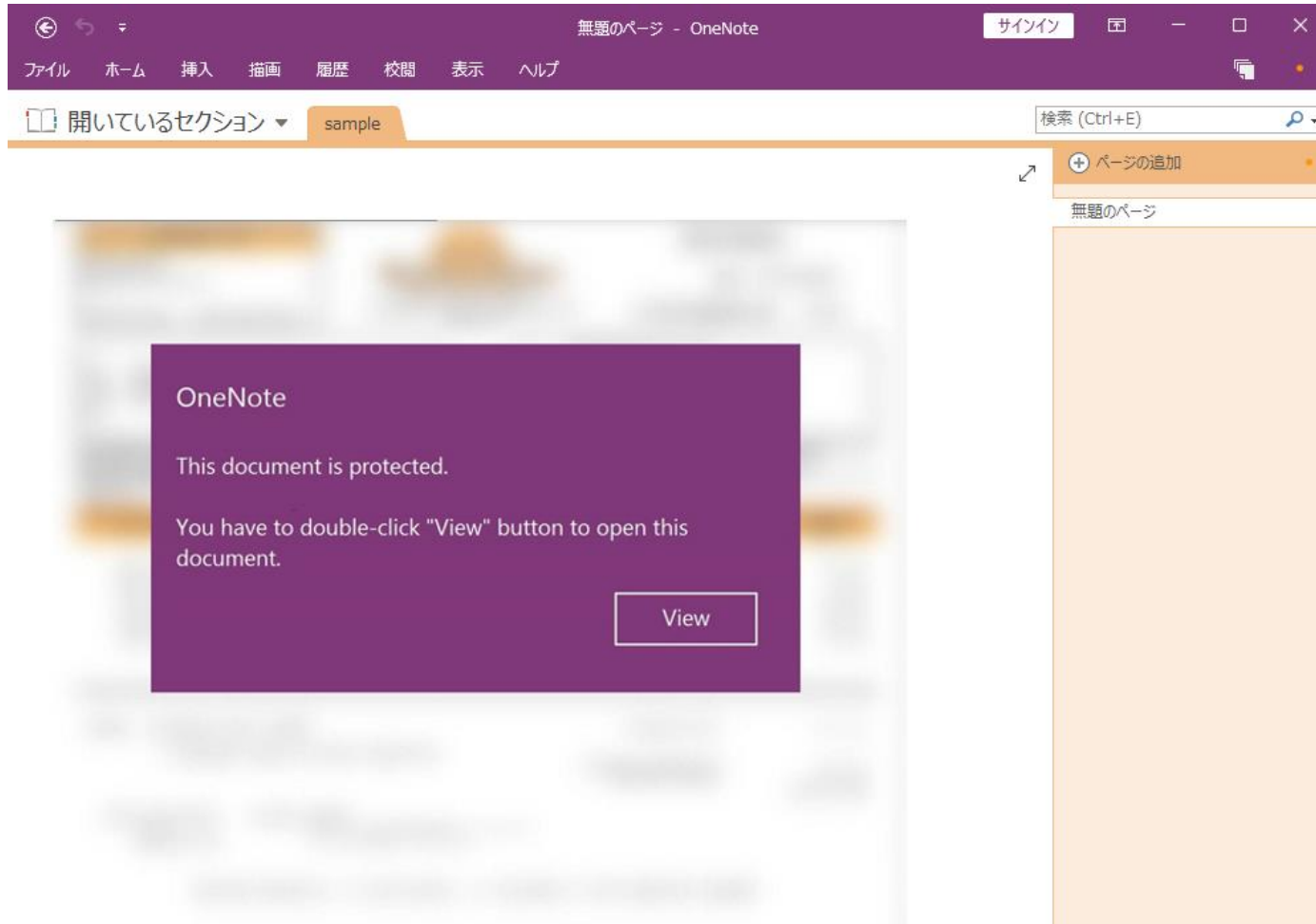


DOCファイル内の表示例

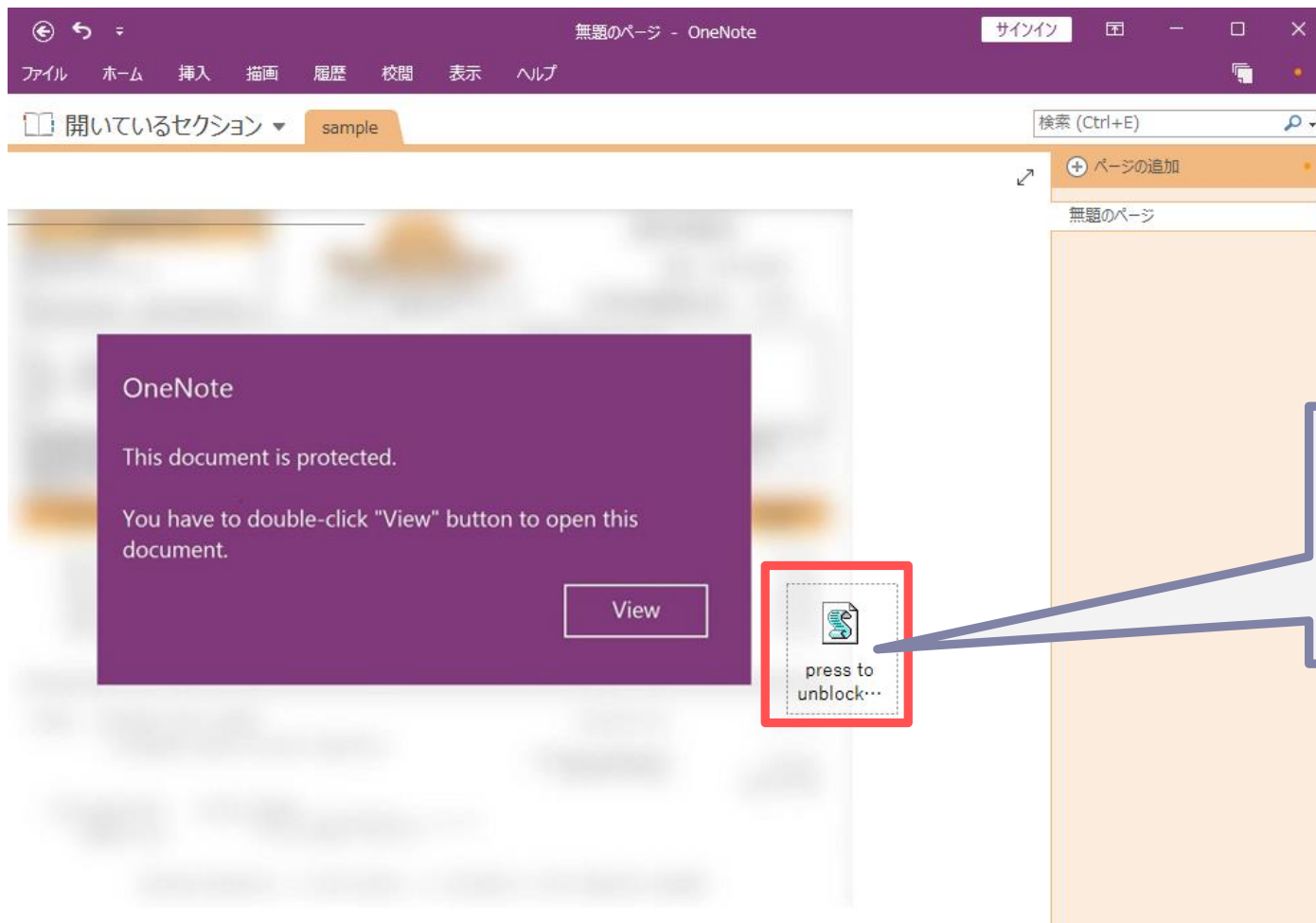
ファイルサイズを大きくすることで
セキュリティ製品による検査を回避する狙い
があると考えられる

出典:twitter @bomccss
<https://twitter.com/bomccss/status/1633375248635789312>
※一部の画像はtweet内のanyrun実行結果から作成

OneNoteファイルの悪用（2023/3/16～）

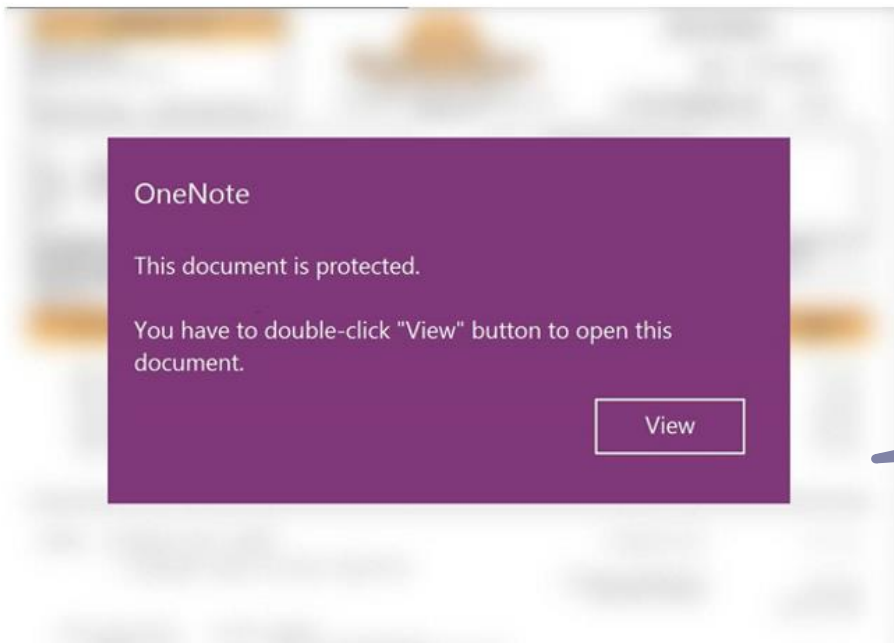


OneNoteファイルの悪用（2023/3/16～）



Viewボタンの裏に
悪意のあるスクリプトファイル

OneNoteファイルの悪用（2023/3/16～）



Viewボタンの裏に
悪意のあるスクリプトファイル

画面上のボタン（を模した画像）をダブルクリックすると、
ボタンの裏に隠れているスクリプトファイルが実行。
Emotetに感染する仕組み

Ransomware

A person's hands are shown typing on a laptop keyboard in a dimly lit office. The background features a computer monitor displaying code, a pen holder, and a coffee cup. The word "Ransomware" is overlaid in large, bold, green and dark blue text.

社会に大きな影響を与えたサイバー攻撃

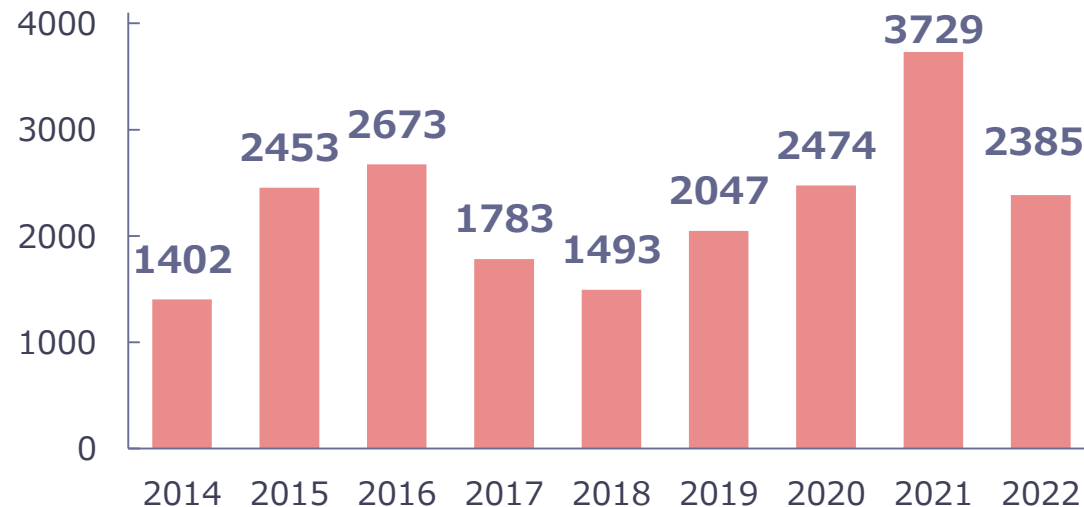
ランサムウェア

ファイルを暗号化するなどの障害を意図的に発生させ、その解決のための身代金（Ransom）を要求するマルウェア

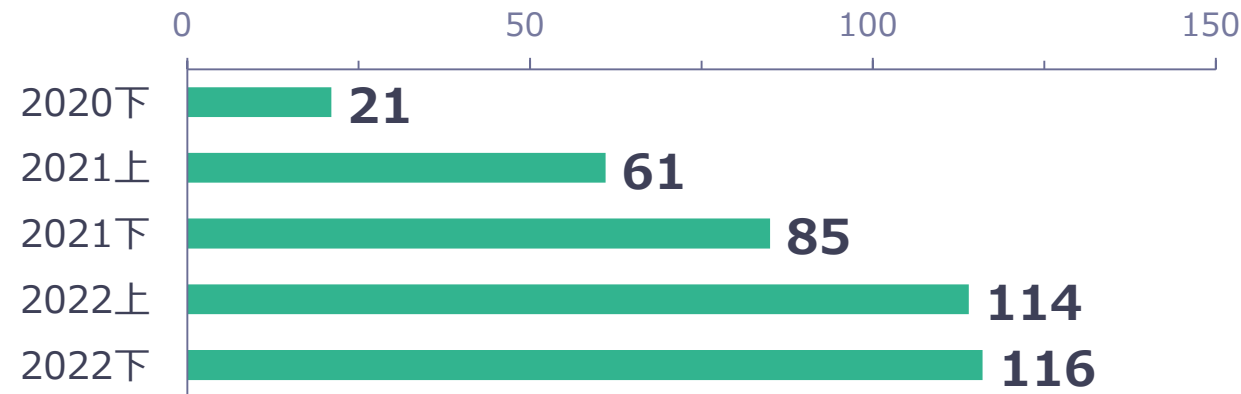
全世界で被害が続いており、

IPA 情報セキュリティ10大脅威でも3年連続1位（組織の部）

ランサムウェアによる被害の統計（米国）（IC3の資料をもとに作成）



企業・団体等におけるランサムウェア被害の報告件数（国内）



（警察庁の資料をもとに作成）

参考：IPA | 情報セキュリティ10大脅威2023
<https://www.ipa.go.jp/security/10threats/10threats2023.html>

出典：IC3 <https://www.ic3.gov/>

出典：警察庁 | サイバー空間をめぐる脅威の情勢等
<https://www.npa.go.jp/publications/statistics/cybersecurity>

国内組織の主なランサムウェア被害事例（2022年）

国内

自動車部品メーカーでサーバーやPCの一部のデータが暗号化被害

自動車内装材メーカーで一部の商品の製造停止に追い込まれる

公立病院（大阪府）で電子カルテに障害
診療業務の縮小を余儀なくされる

衣料品チェーンで社内システムに障害発生

民間病院（徳島県）で電子カルテ、院内LANシステムに障害。新規患者の診療を制限

1 2 3 4 5 6 7 8 9 10 11 12

国外の関連組織

自動車部品メーカーのドイツ子会社が情報公開脅迫に遭う

タイヤメーカーのアメリカ子会社で生産、販売活動に一部障害が発生

国内新聞社のシンガポール法人でサーバーの一部データが暗号化被害

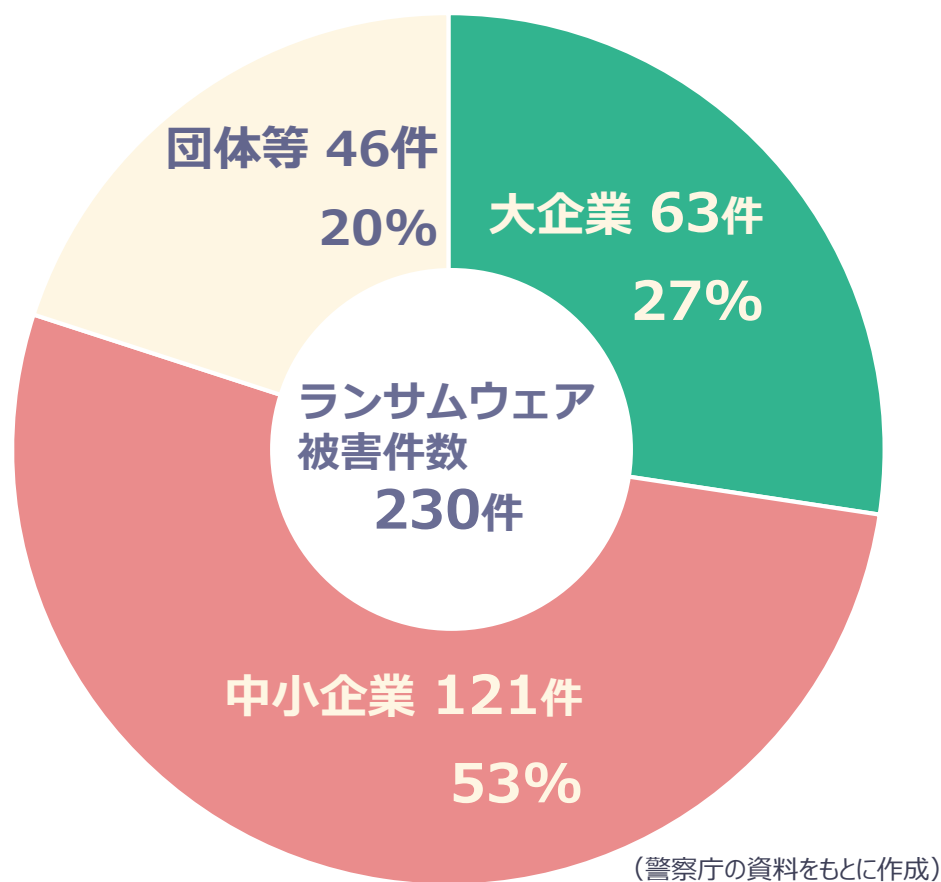
電機メーカーのカナダ子会社がリークサイトで情報公開被害

国内保険会社傘下の台湾保険仲介会社でサーバーのデータが暗号化被害

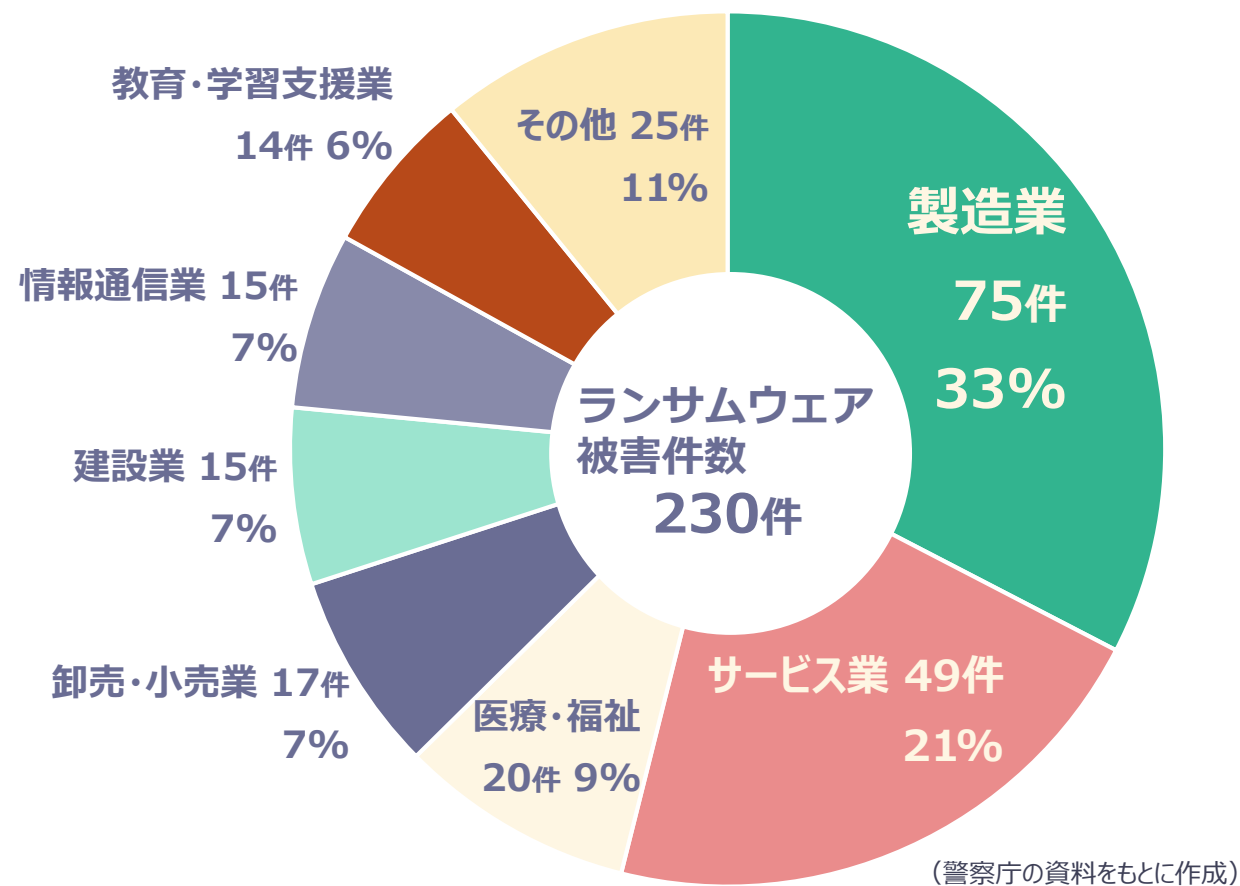
ランサムウェアのターゲット

企業・団体等の規模や業種を問わず狙われている

被害組織の規模別報告件数（2022年）



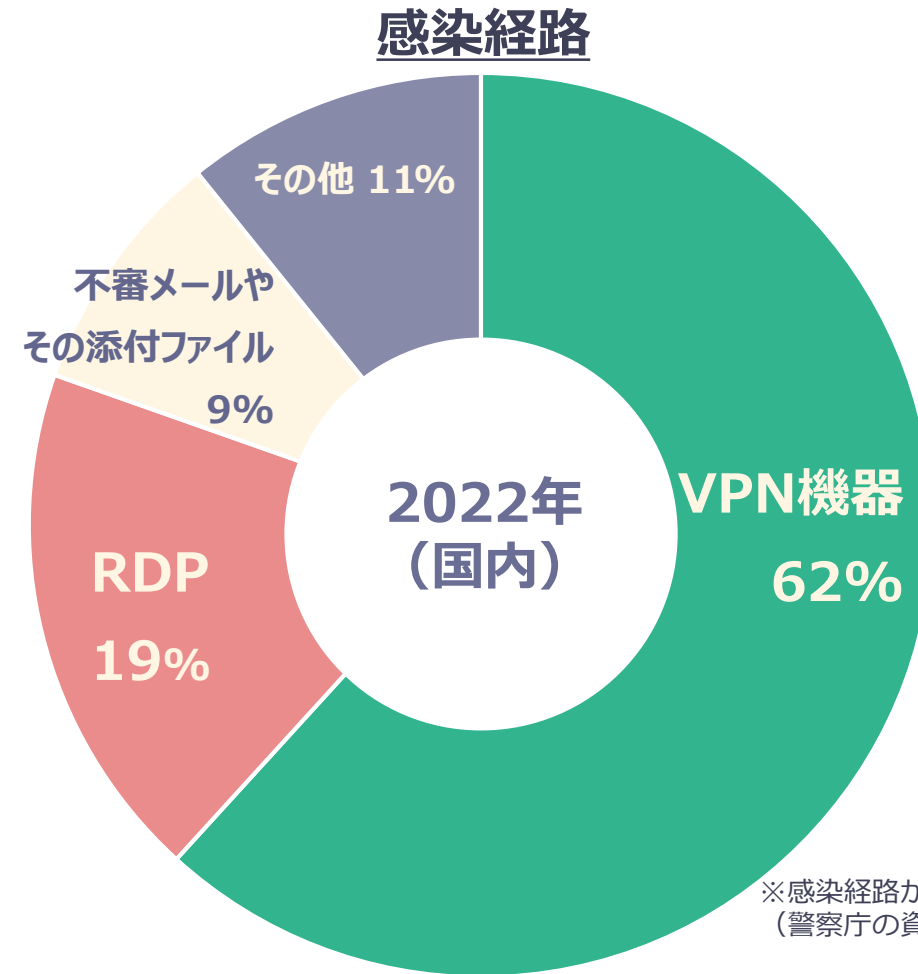
被害組織の業種別報告件数（2022年）



ランサムウェアの初期感染経路

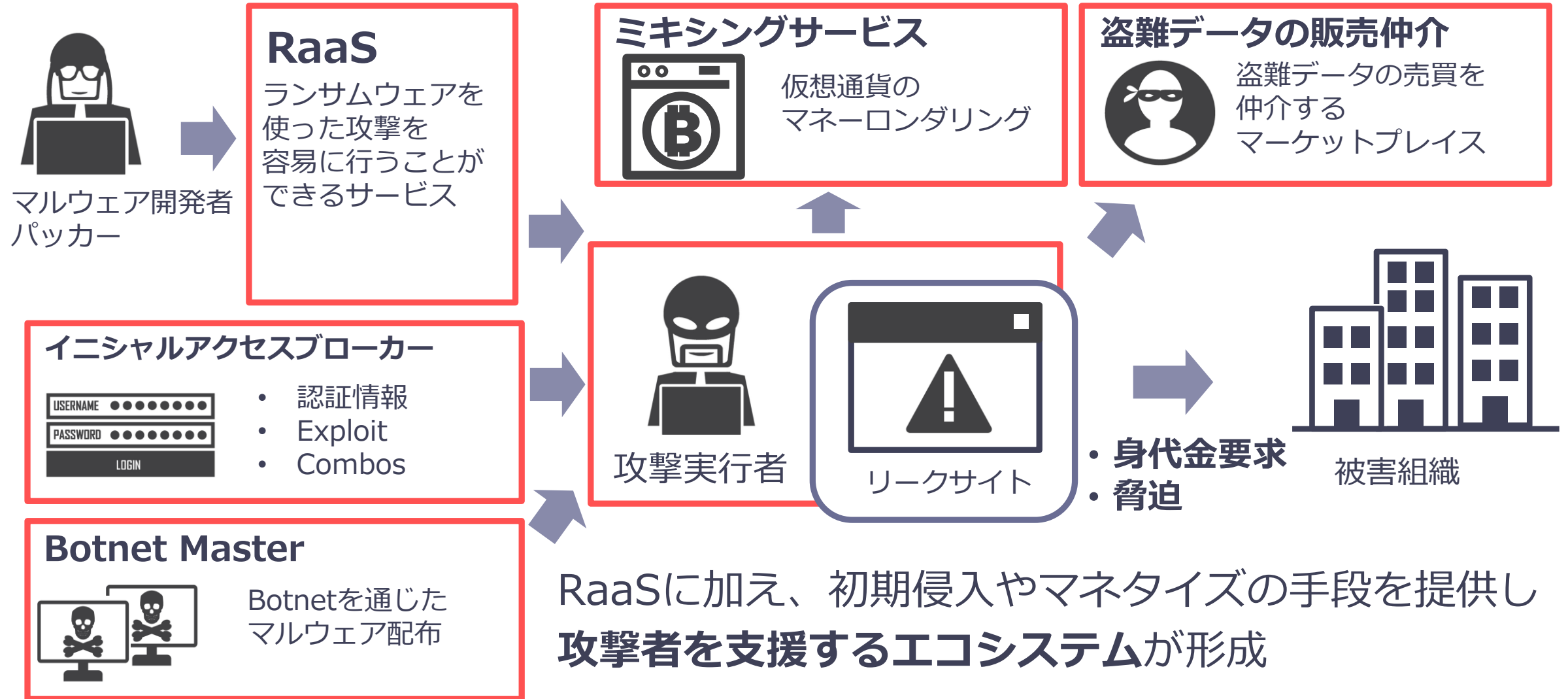
2022年に国内で確認された
ランサムウェアの感染経路は
VPN機器からの侵入が62%
RDPからの侵入が19%を占める

投影のみ



全世界ではRDPからの侵入は減少傾向

攻撃を後押しするエコシステム



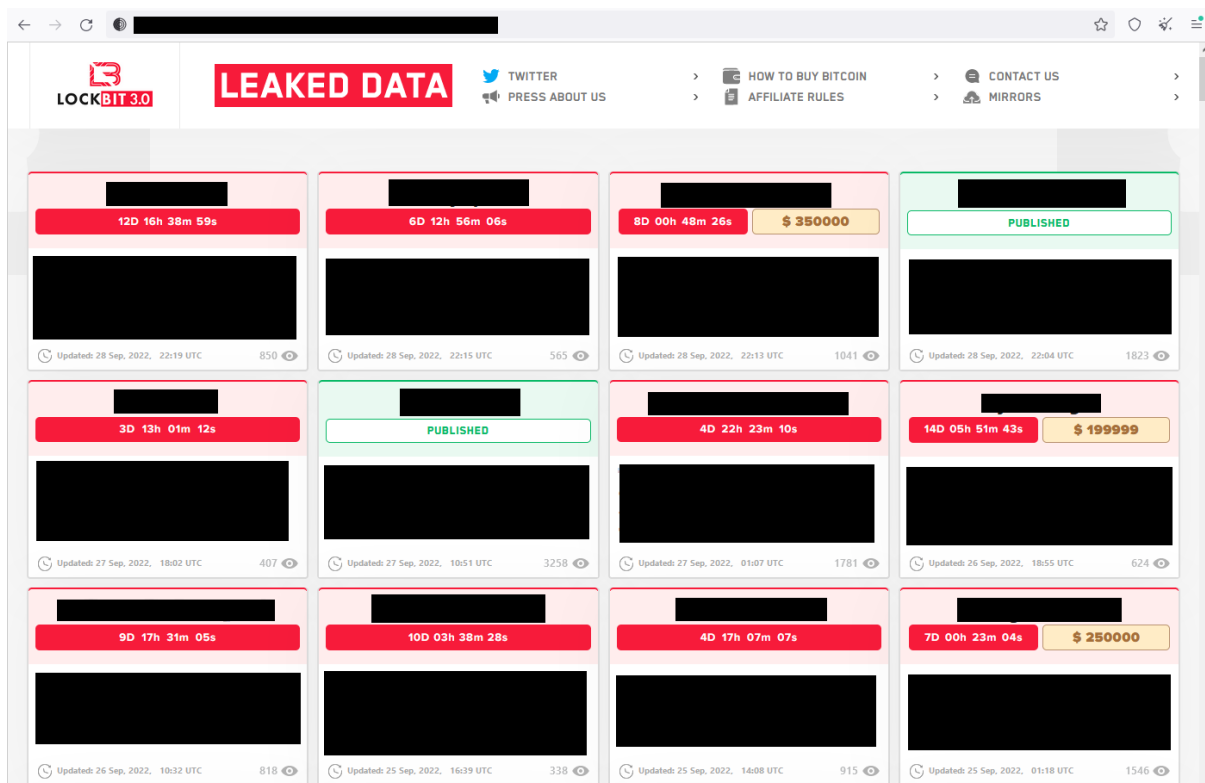
RaaSに加え、初期侵入やマネタイズの手段を提供し
攻撃者を支援するエコシステムが形成

攻撃者の分業化により、**攻撃のサイクルが加速**

多様化するランサムウェア攻撃者のマネタイズ方法

脅迫される身代金

ランサムウェアの被害金額が増加
2022年Q4の身代金平均額は
\$408,644 (約5,300万円) (Coveware社)



ランサムウェアによる身代金の平均値と中央値



LockBit3.0のリークサイト

特定のターゲットに対しては要求に応じない場合
データの公開を行うと脅迫

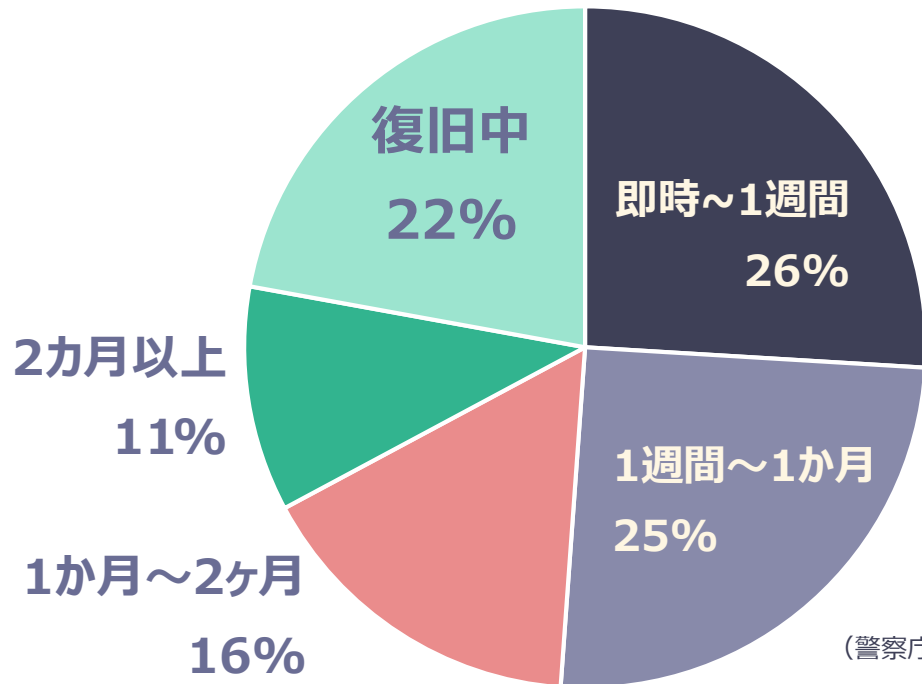
ランサムウェアからの復旧

経営に大きな影響を与える調査・復旧コスト

被害組織の**46%**が**1,000万円以上**と回答

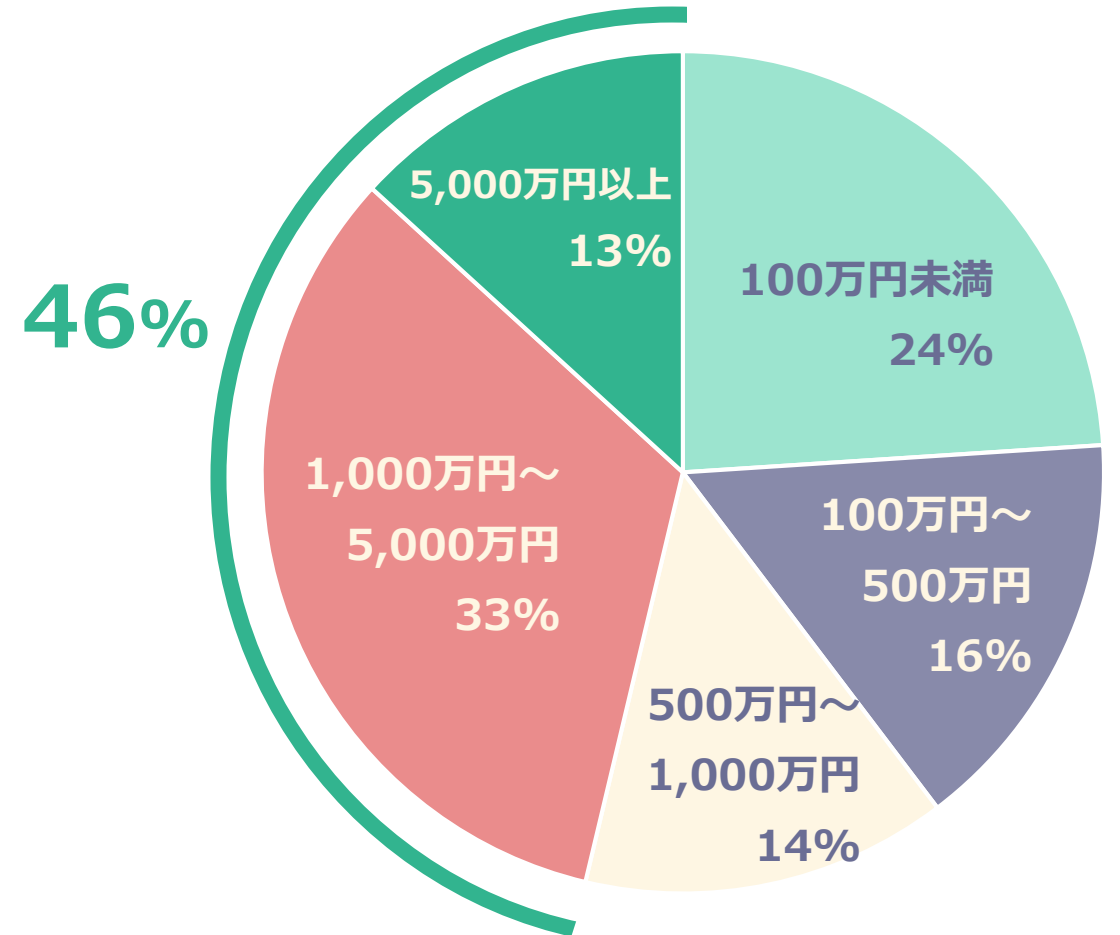
復旧が長期間に及ぶケースも確認

被害から復旧に要した期間（2022年）



(警察庁の資料をもとに作成)

調査・復旧費用（2022年）



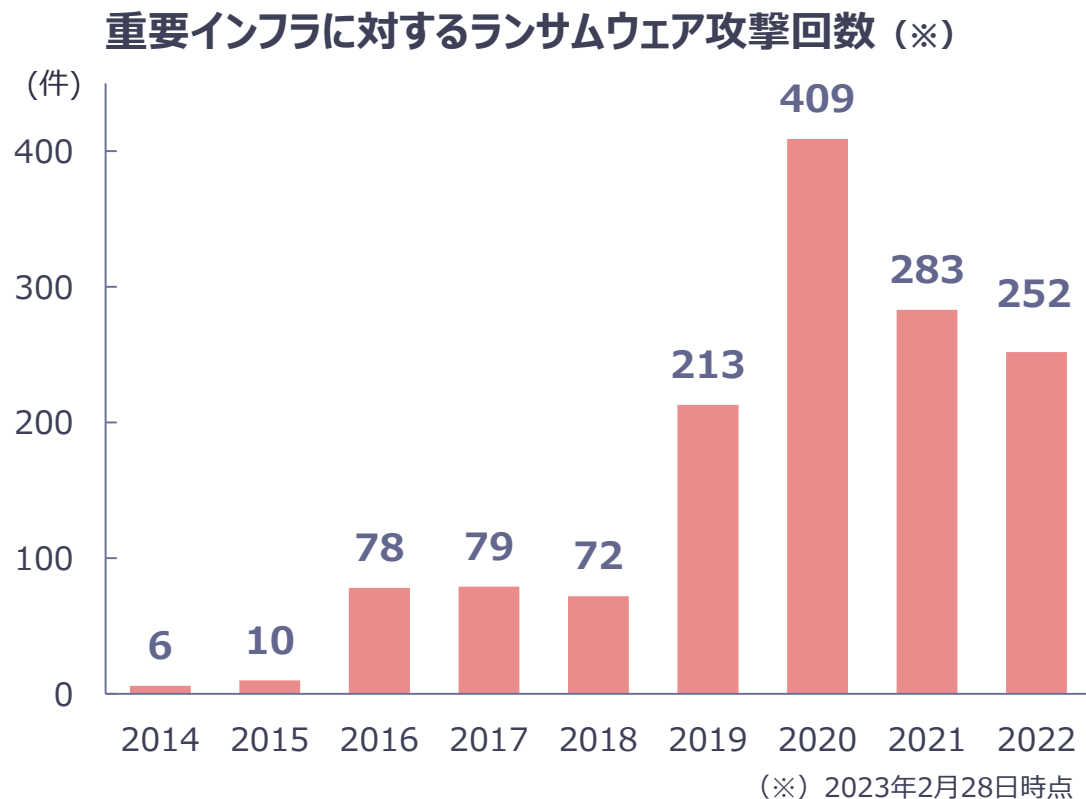
(警察庁の資料をもとに作成)

出典：警察庁 |サイバー空間をめぐる脅威の情勢等
<https://www.npa.go.jp/publications/statistics/cybersecurity/>

サイバー空間からフィジカル空間へ

サイバー脅威の影響範囲拡大

政府機関や重要インフラに対するサイバー攻撃が増加



出典 : Temple University | Critical Infrastructure Ransomware Attacks (CIRA)
<https://sites.temple.edu/care/cira/>

□ Stuxnetによるイランの核施設攻撃 (2010年)

遠心分離機を制御するマシンに侵入、
遠心分離機の回転速度を無理やり変更し
負荷を与え、最終的に遠心分離機が物理的に破壊

□ 石油パイプラインへの攻撃 (2021年)

ランサムウェアDarkSideを使用する
攻撃者グループが米国の石油パイプラインを攻撃。
同パイプラインは5日間の操業停止に追い込まれる

□ KILLNETによる攻撃 (2022年)

ロシアを支持するサイバー犯罪集団「KILLNET」の
DDoS攻撃により、政府機関や企業のサービスで
通信障害が発生

サイバー攻撃はサイバー空間だけでなく
フィジカル空間にも大きな影響

本日はお話しすること

1. 2021年の
サイバーセキュリティ脅威動向
2. 対策のポイント

対策のポイント



脆弱性への対応

- セキュリティパッチの適用
- 脆弱性診断の活用



製品の適切な利用

- 適切な設定で使用する
- 最新の状態を保つ
- 複数の層で守る



被害を受けた場合を 想定した対策

- 情報資産の適切な管理
- ログモニタリング
- インシデント発生時の対応を明確化



情報収集と セキュリティ教育

- 脅威情報の収集
- 脅威を知ってもらう
- ガイドラインの参照・適応

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

Search

