2021年を振り返り備える！

サイバーセキュリティ脅威動向と2022年の対策ポイント

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
セキュリティエバンジェリスト
西浦 真一, CISSP

自己紹介

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への対策の提案や
  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

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

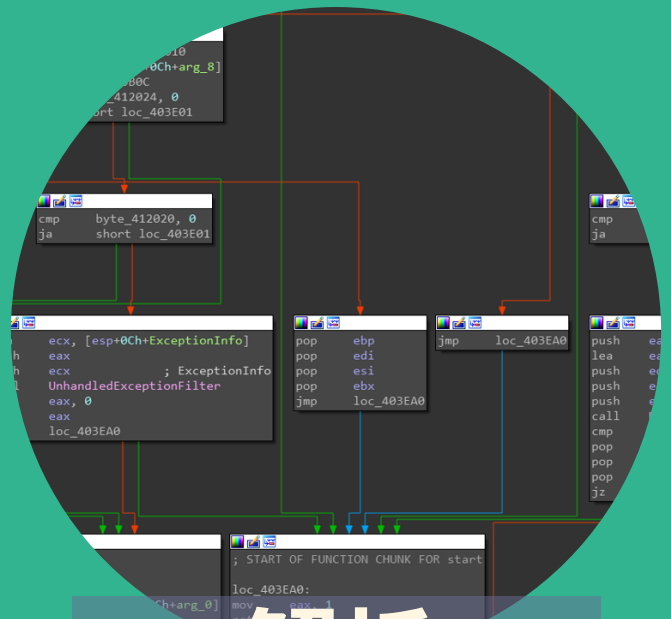
社外活動

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

キヤノンITソリューションズ
サイバーセキュリティラボ

研究



解析

発信

サイバーセキュリティ情報局

2021年 サイバーセキュリティレポートを
3月16日にリリース

サイバーセキュリティ情報局 Search

＃本日お話しすること

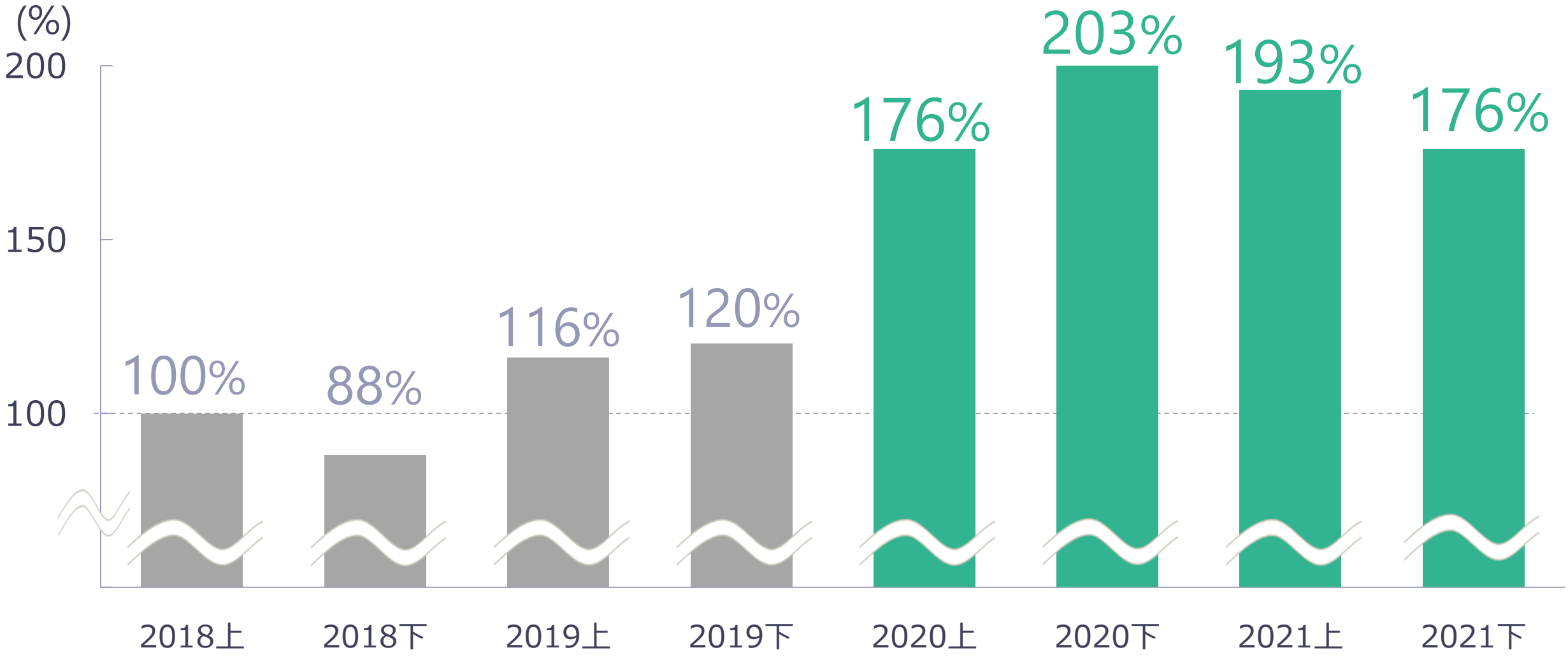
1. 2021年の
   サイバーセキュリティ脅威動向
2. 対策のポイント

＃本日お話しすること

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

国内のマルウェア動向

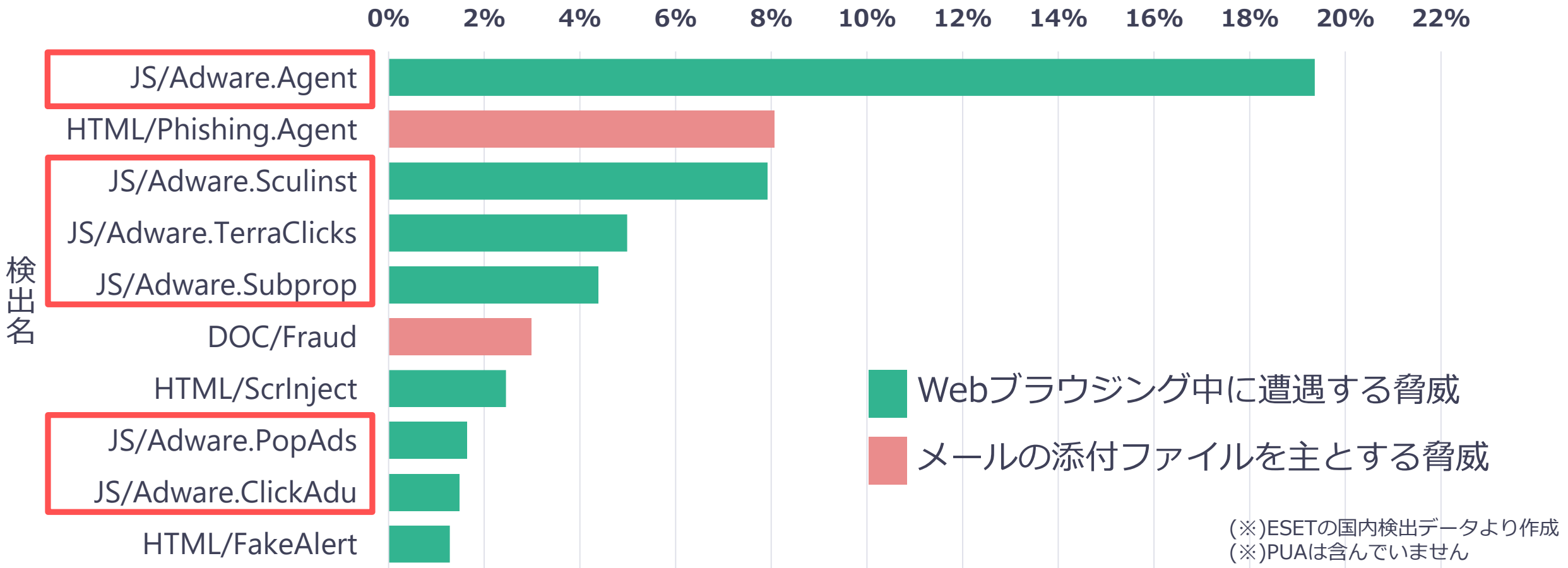
国内のマルウェア検出総数の推移



(※)ESETの国内検出データより作成

国内で検出されたマルウェアの内訳（2021年）

検出数の上位10種



(※)ESETの国内検出データより作成
(※)PUAは含んでいません

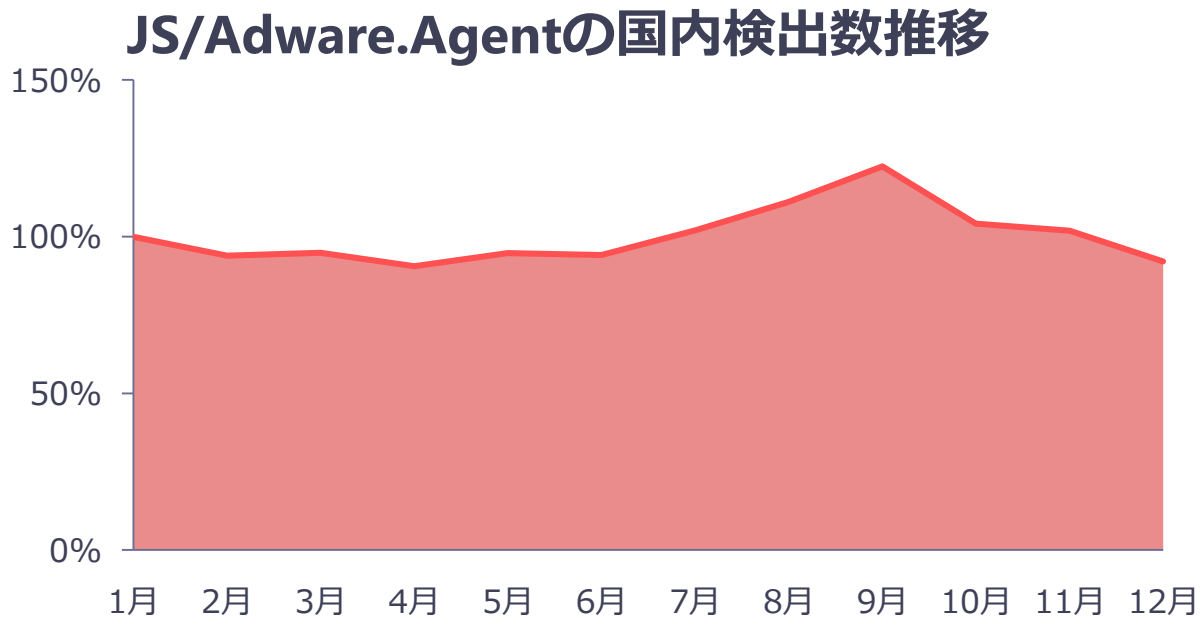
- ✓検出の大多数をWebブラウジング中に遭遇する脅威が占める
- ✓電子メールの添付ファイルによる脅威も引き続き検出

Webブラウジング中に遭遇する脅威が増加

アドウェア

Webブラウザー上などで実行され、
不正な広告を表示するマルウェアの一種

国内マルウェア検出数上位にも複数ある
JS/Adware だけで、2021年に日本で
検出されたマルウェアの**39.8%**を占める



(※)ESETの国内検出データより作成

アドウェアの中には不正な広告を表示させるだけではなく、
Webブラウザーのアクセス履歴を外部へ送信するものもあるので注意が必要

Webサイトアクセス時に不用意に許可やインストールを行わないことが重要

RansomWare

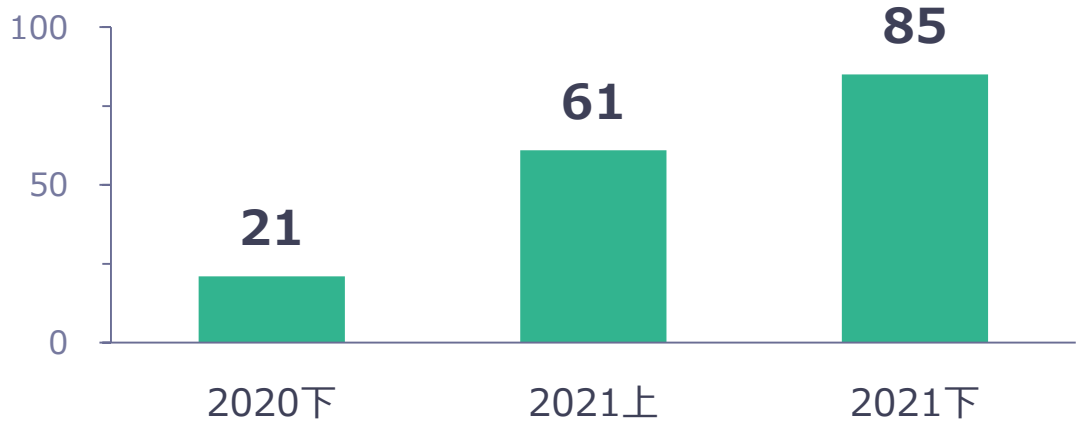
社会に大きな影響を与えたサイバー攻撃

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
2年連続1位（組織の部）

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）

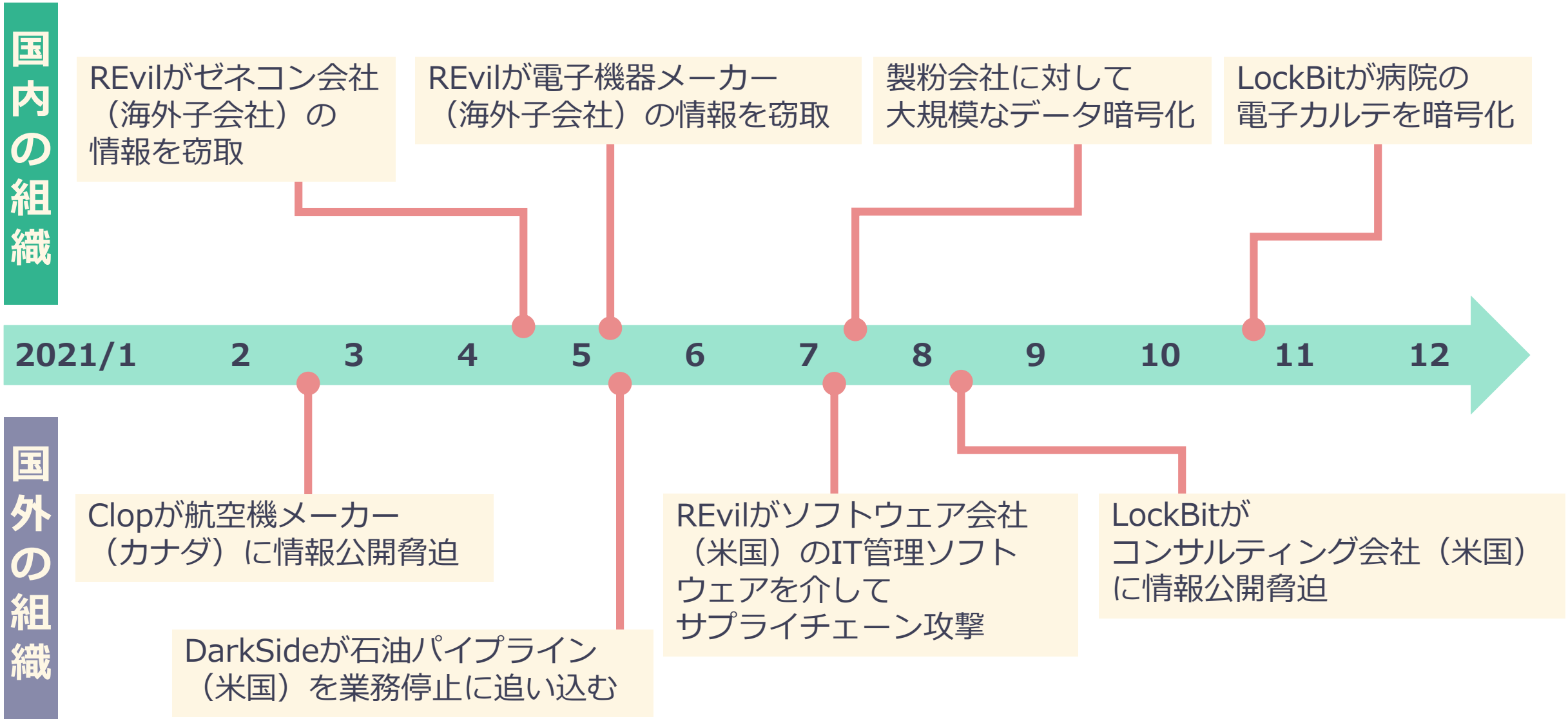


2021年のランサムウェアの検出傾向（日本）

投影のみ

出典：警察庁 |令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

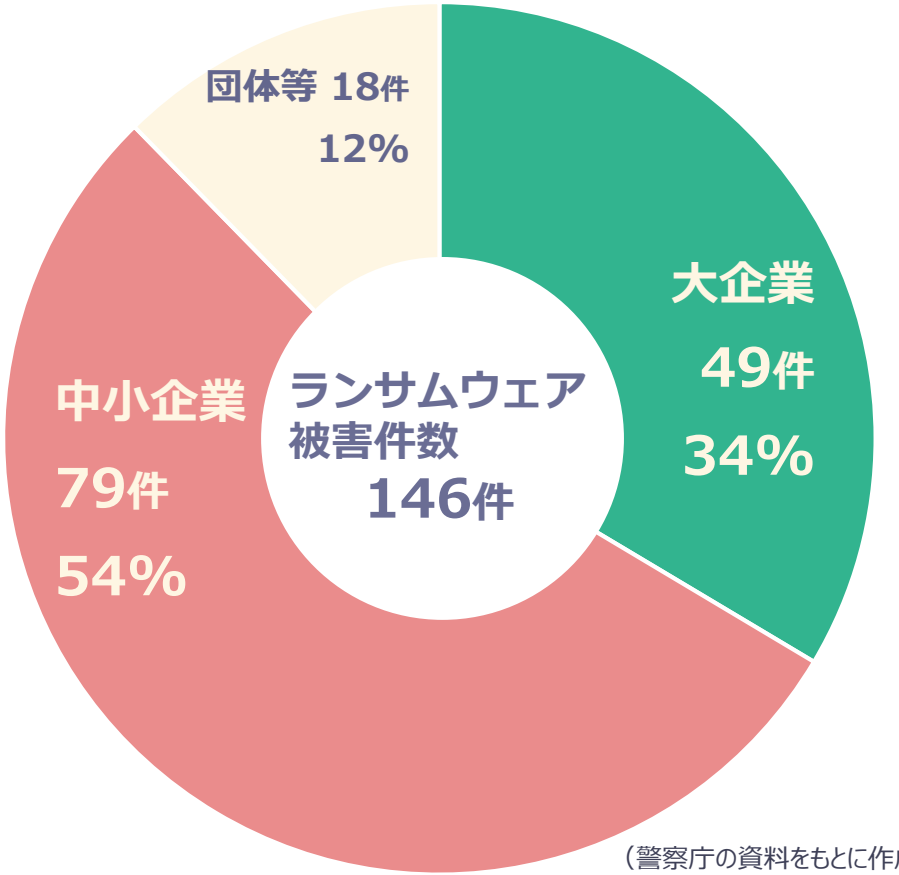
国内外の主なランサムウェア被害事例



ランサムウェアのターゲット

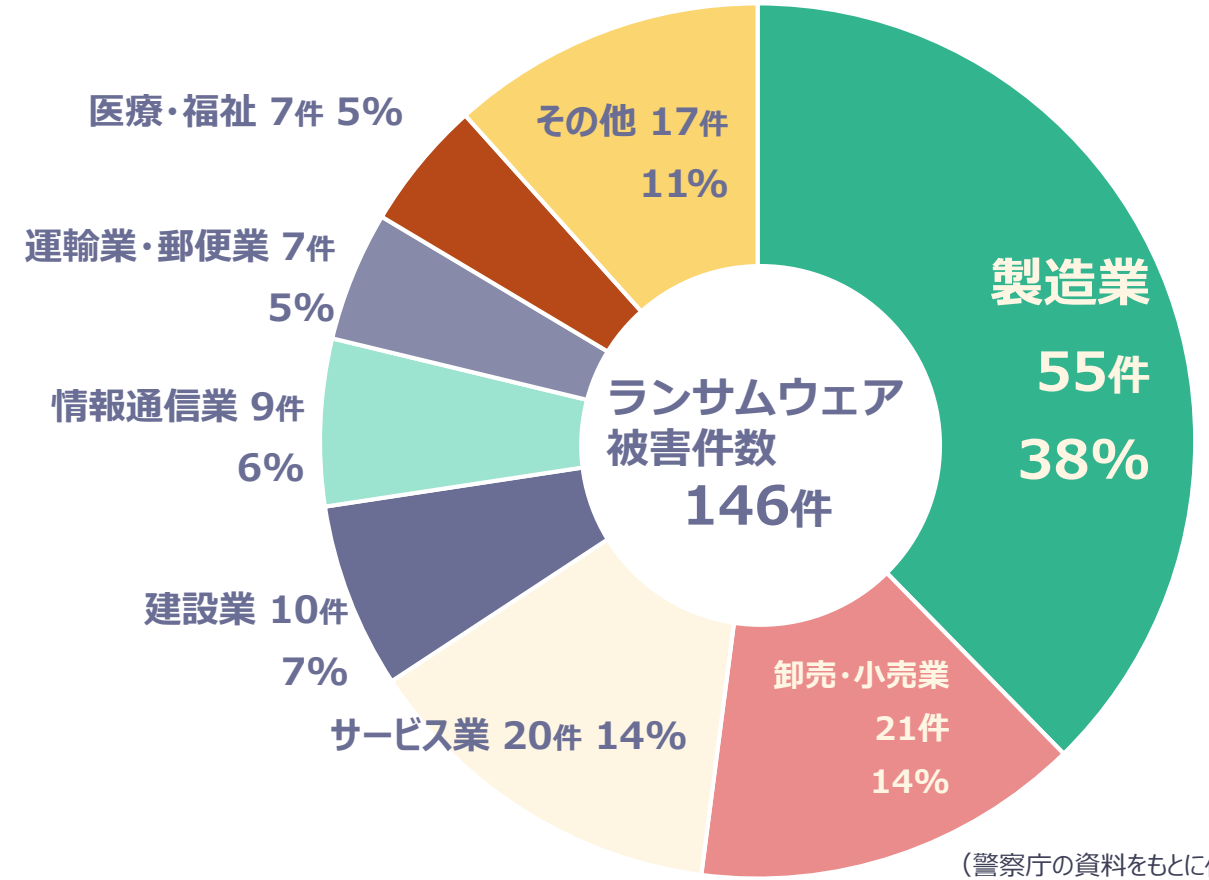
企業・団体等の規模や業種を問わず狙われている

被害組織の規模別報告件数（2021年）



（警察庁の資料をもとに作成）

被害組織の業種別報告件数（2021年）



（警察庁の資料をもとに作成）

出典：警察庁 |令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

身代金要求の手口

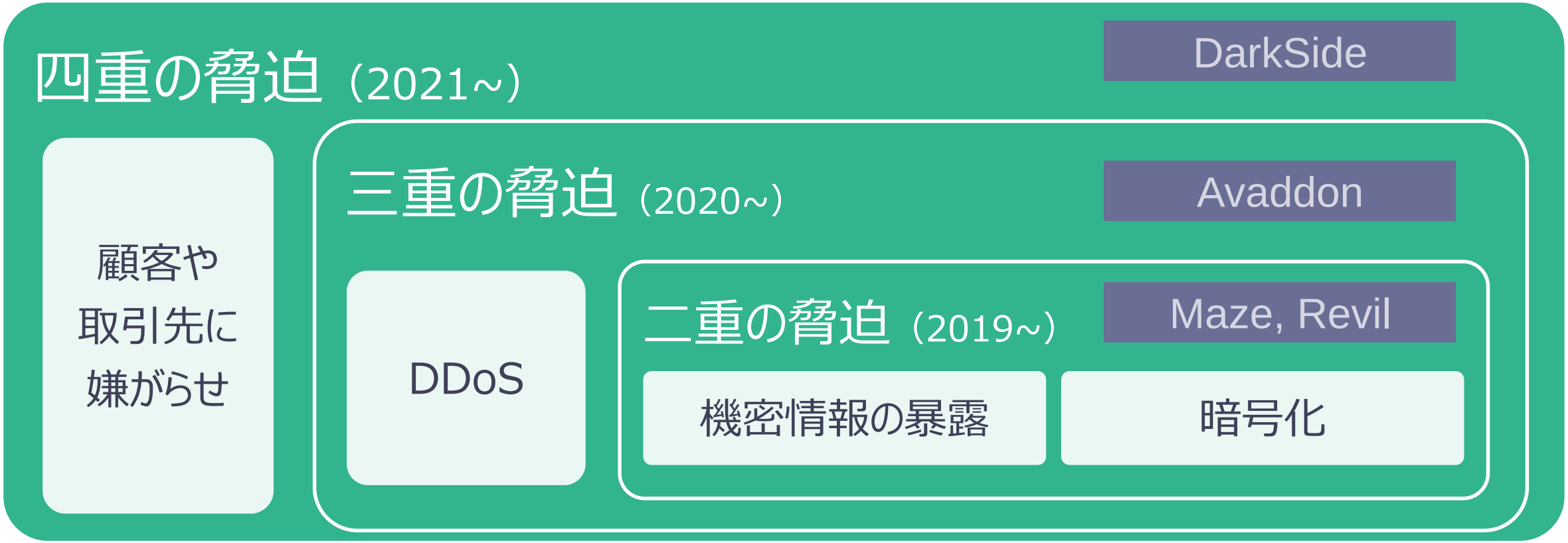
四重の脅迫

ランサムウェアによる暗号化だけではなく、様々な脅迫（攻撃）手法を**併用**

Coveware社の調査では、2021年第4四半期に確認された

ランサムウェア被害の**84%**でデータ流出を確認

参考：Coveware | Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021 https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021



ランサムウェアにより組織が受けるダメージ

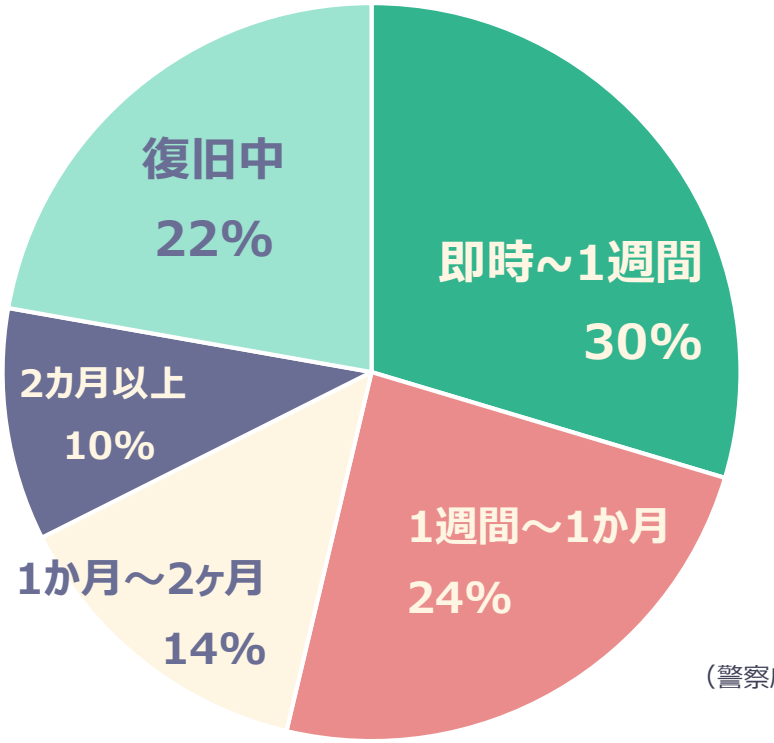
莫大な身代金と復旧コスト

ランサムウェアの被害金額が増加

2021年4Qの身代金平均額は

$322,168（約3,750万円）（ Coveware社）

被害から復旧に要した期間



（警察庁の資料をもとに作成）

ランサムウェアによる身代金の平均値と中央値

投影のみ

身代金の支払いを拒否できた場合でも

復旧が長期間に及ぶケースがあり、**経営に大きな影響**

出典：Coveware
https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

出典：警察庁 |令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

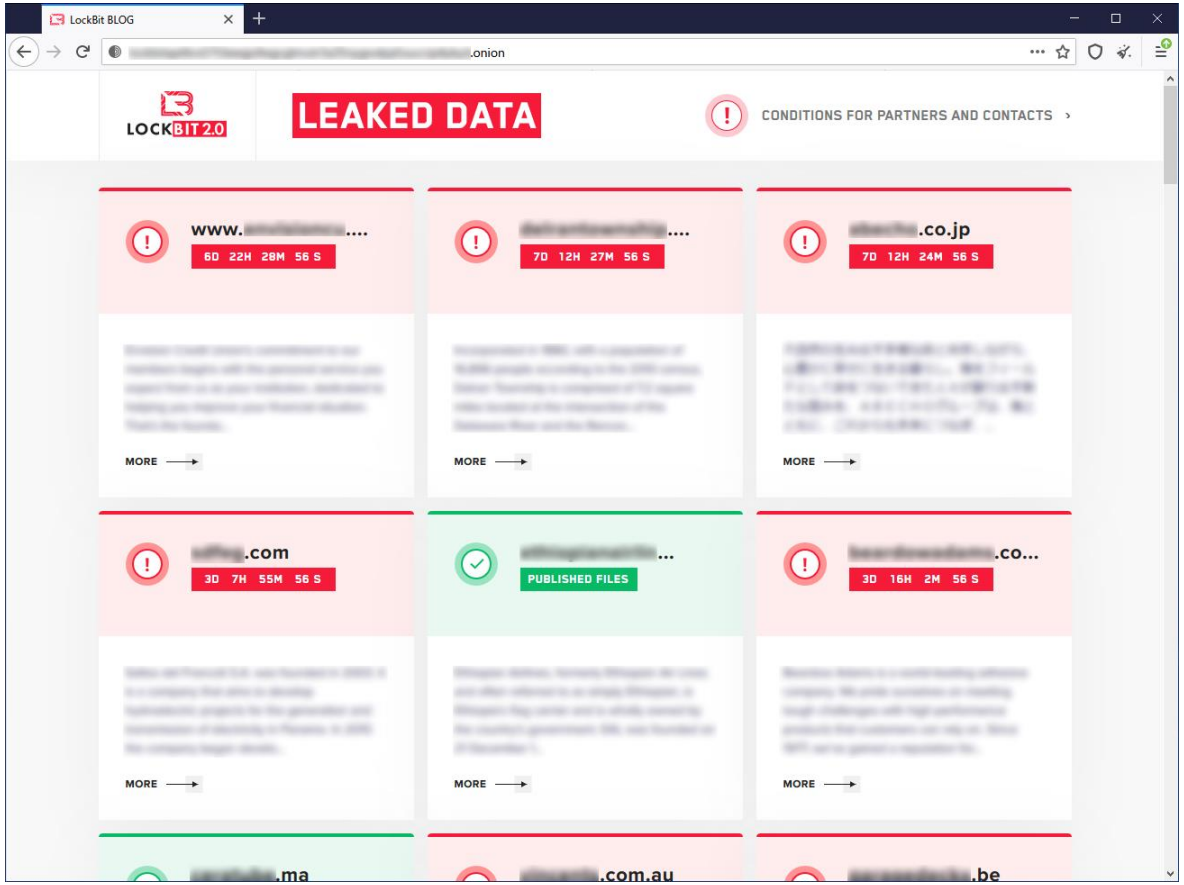
2021年に大きな被害を生んだランサムウェア例

LockBit2.0

2021年6月頃に確認されたランサムウェア

LockBit2.0の代表的な機能

- 言語環境の検出
  （特定の言語環境では暗号化を行わない）
- ローカルディスクおよび
  同一ネットワーク内の共有フォルダーの暗号化
- 暗号化を妨げるプロセスやサービスの終了
- シャドウコピーの削除
- イベントログの削除
- Wake On LAN（WOL）による
  シャットダウン状態のPC起動
- プリンターを使用した脅迫文書の印刷

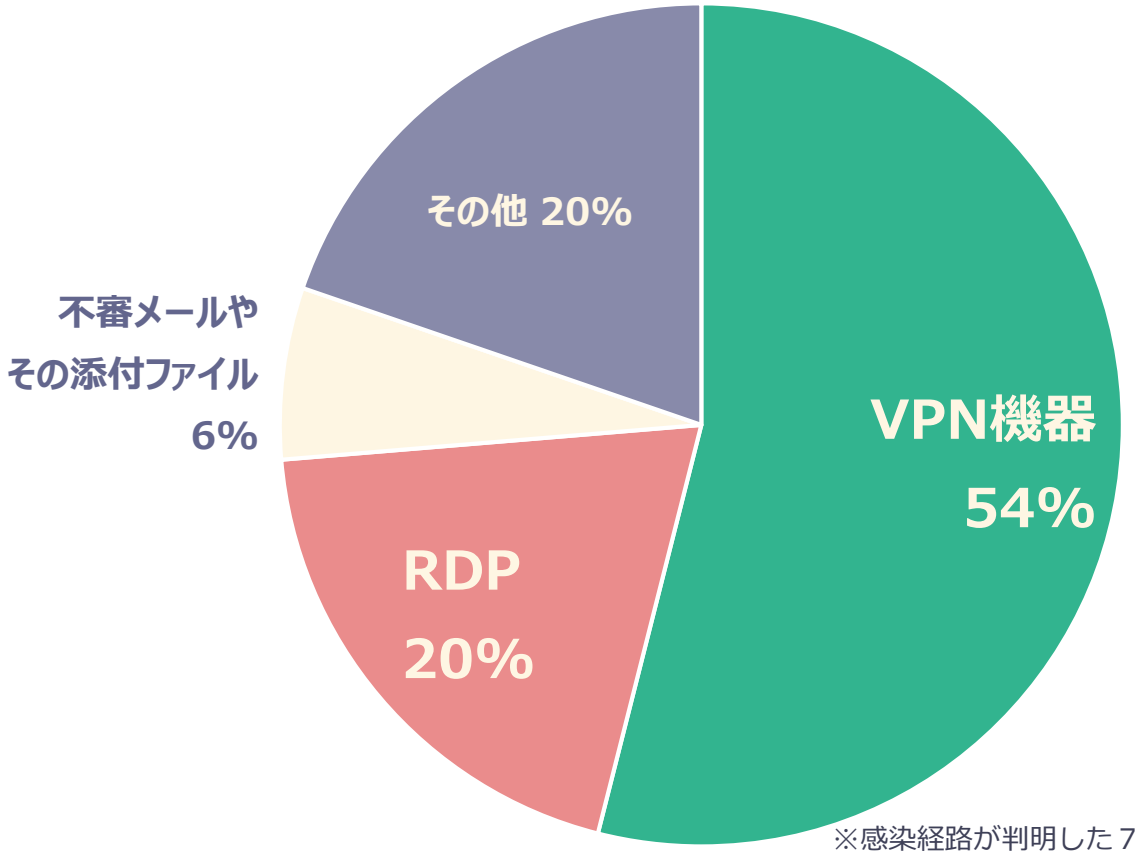


LockBit2.0のリークサイト
特定のターゲットに対しては要求に応じない場合
DDoS攻撃を行うと脅迫

ランサムウェアの初期感染経路

従来のばらまき型メールや
スピアフィッシングメールから変化

2021年に確認されたランサムウェアの感染経路



※感染経路が判明した７6件の内訳
（警察庁の資料をもとに作成）

ランサムウェアの感染経路は
VPN機器からの侵入が54%
RDPからの侵入が20%を占める

出典：警察庁 |令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

VPN機器からの侵入：脆弱性の悪用

脆弱性を悪用するためのコードの公開も確認

脆弱性対策が不十分なまま利用を続けてしまうと、攻撃者に脆弱性を悪用され、
認証情報や組織の機密情報が外部に流出する等の被害に遭うおそれ

Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	**国内外900社（国内は38社）の認証情報が公開**

Fortinet製FortiOSのSSL VPN機能の脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	**脆弱性の影響を受ける約5万台の機器情報が公開** **（IPアドレス、ユーザーアカウント名、平文パスワード等）**
2021年9月	**脆弱性の影響を受ける約8万7千台** **（国内は1000社）の認証情報が公開**

セキュリティパッチが
公開されている場合は
速やかに適用をご検討ください

攻撃が確認されている期間に
古いファームウェアのまま
使用されていた方は
侵害有無の確認、
認証情報の変更を推奨します

参考：JPCERT/CC |
Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について
https://www.jpcert.or.jp/newsflash/2020112701.html
複数の SSL VPN 製品の脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190033.html

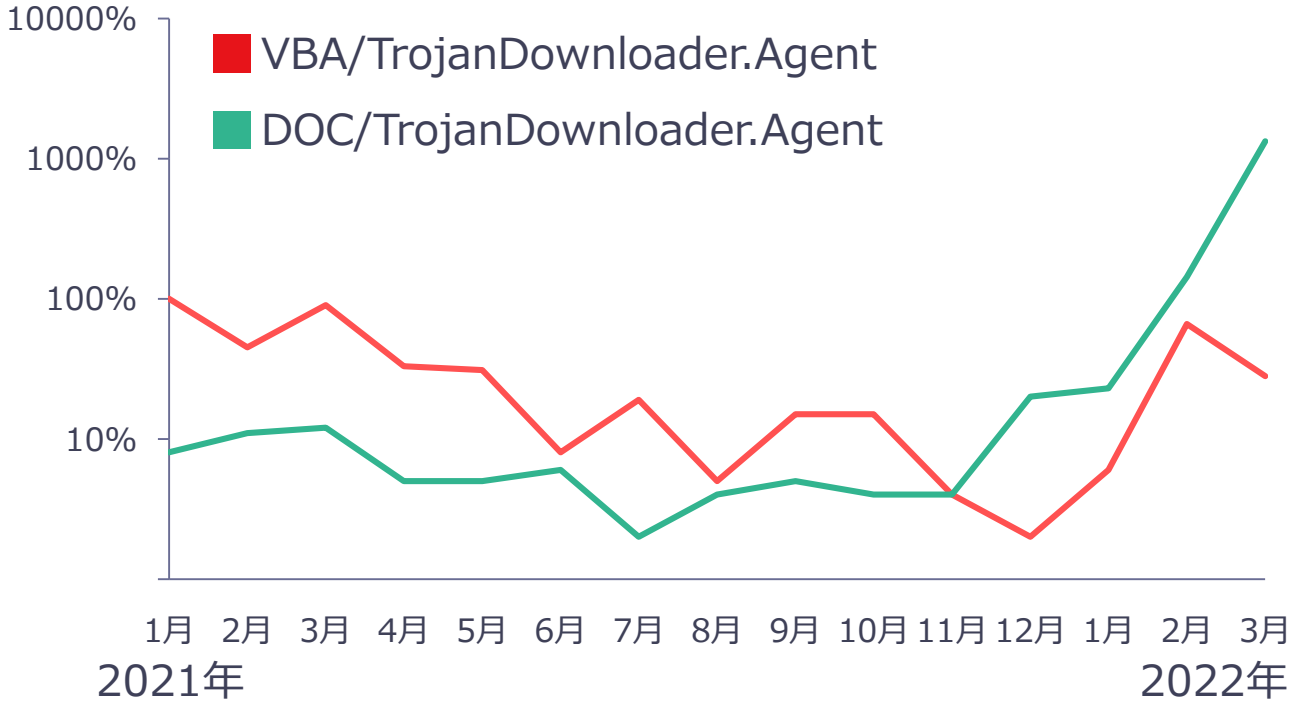
参考：Fortinet |悪意のあるアクターがFortiGate SSL-VPNの認証情報を公開
https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

Emotet

Emotetの活動再開

2019年10月から2020年にかけて多くの被害をもたらしたマルウェア
2021年1月末のテイクダウン以降、休止状態だったが
2021年11月14日ごろから再稼働

Emotetの主なダウンローダーの国内検出数推移



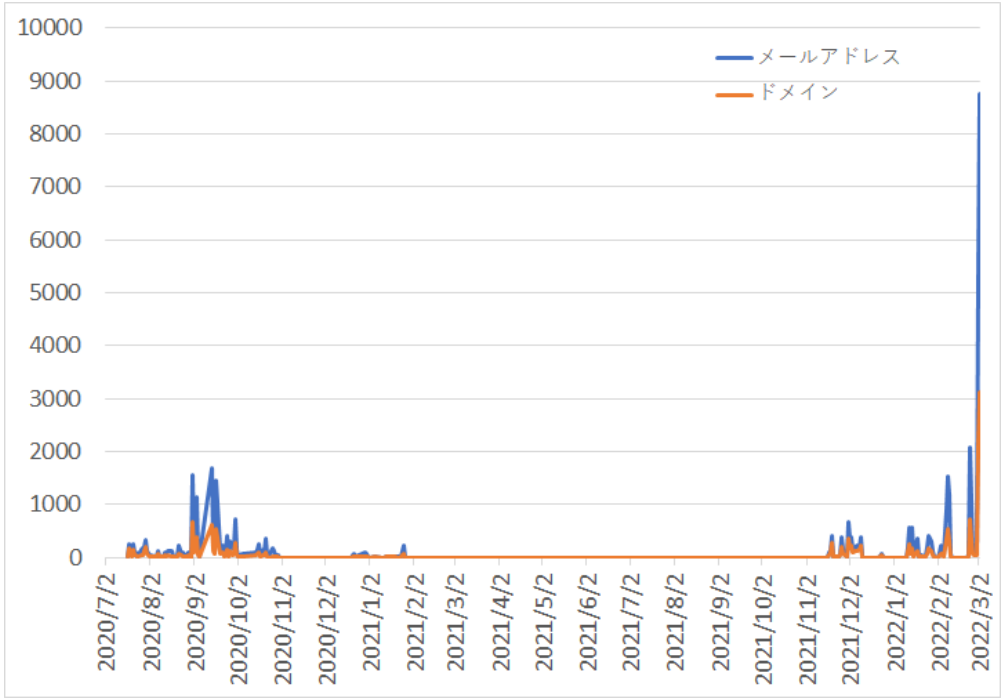
(※)ESETの国内検出データより作成
2021年1月のVBA/TrojanDownloader.Agentの国内検出数を100%とした場合の検出数推移

メールの添付ファイルを
初期潜入経路するランサムウェアが
再び増加する可能性

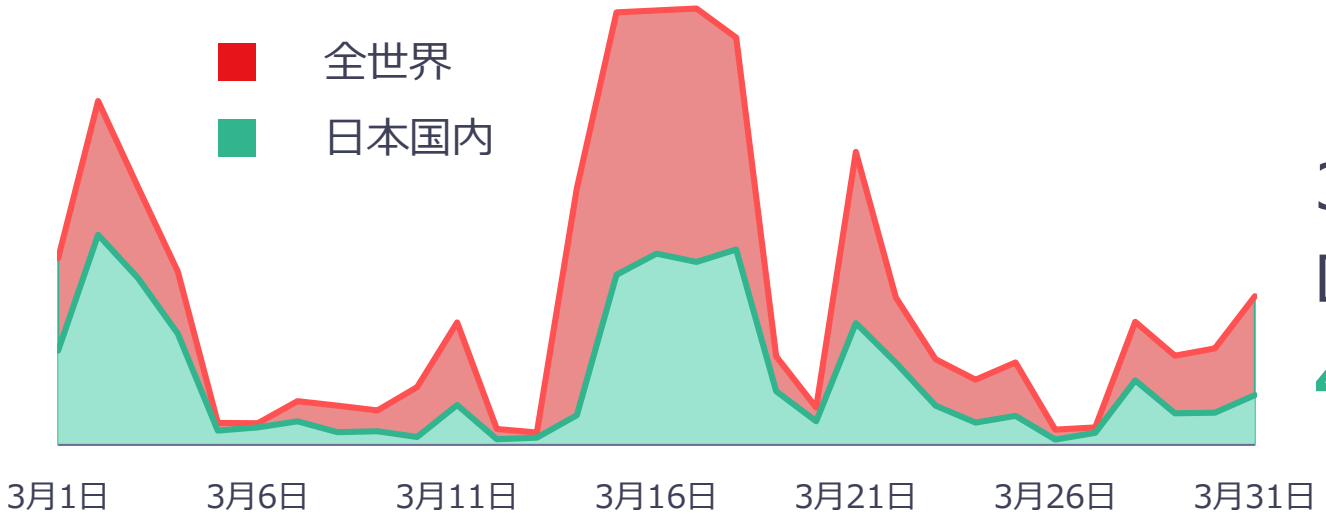
国内での感染拡大

2022年3月、Emotetに感染し
メール送信に悪用される可能性のある
.jpメールアドレス数が
2020年の感染ピーク時の**約5倍以上に急増**

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.jpcert.or.jp/at/2022/at220006.html

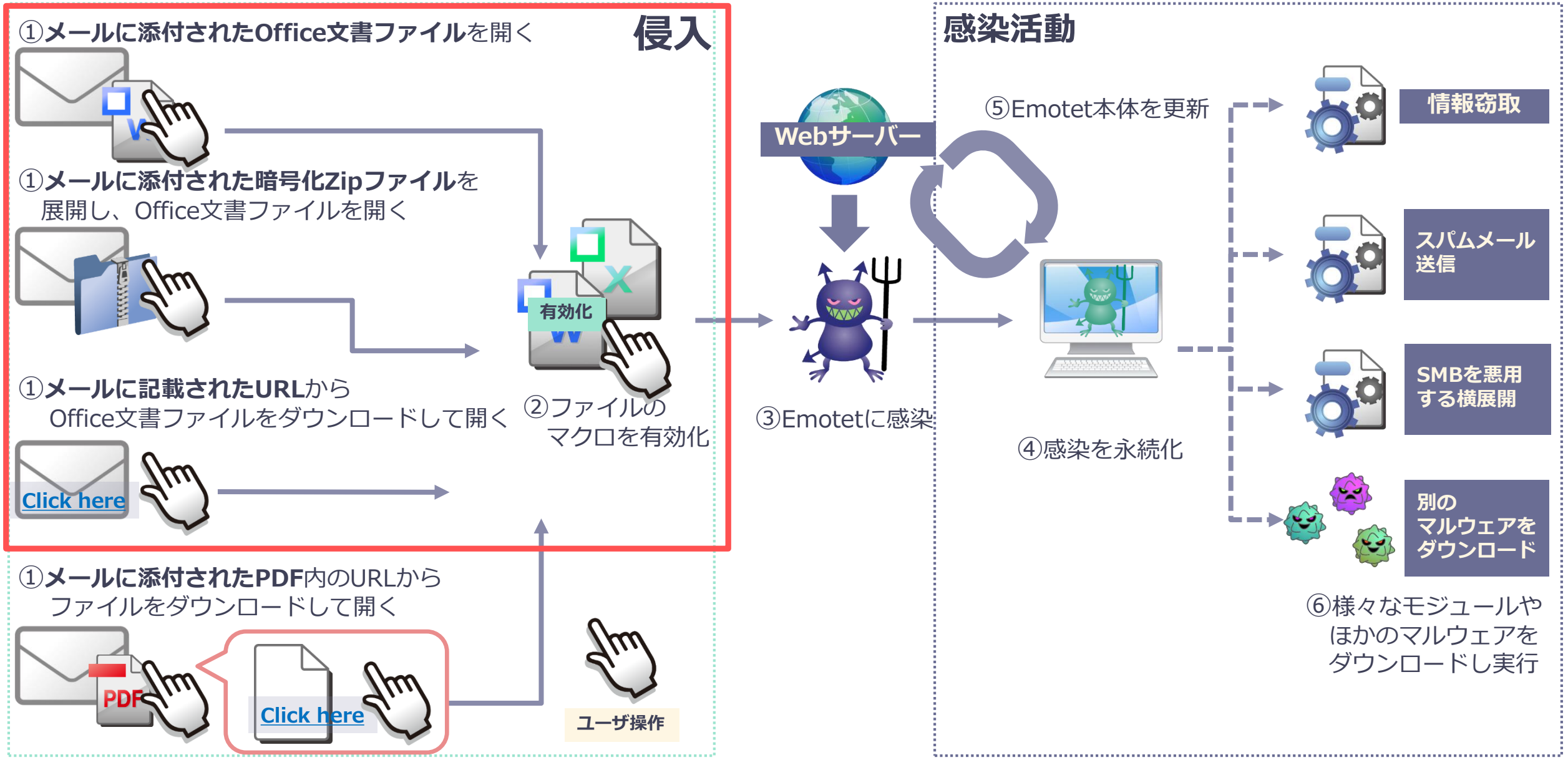


DOC/TorojanDownloader.Agentの検出数推移（2022年3月）



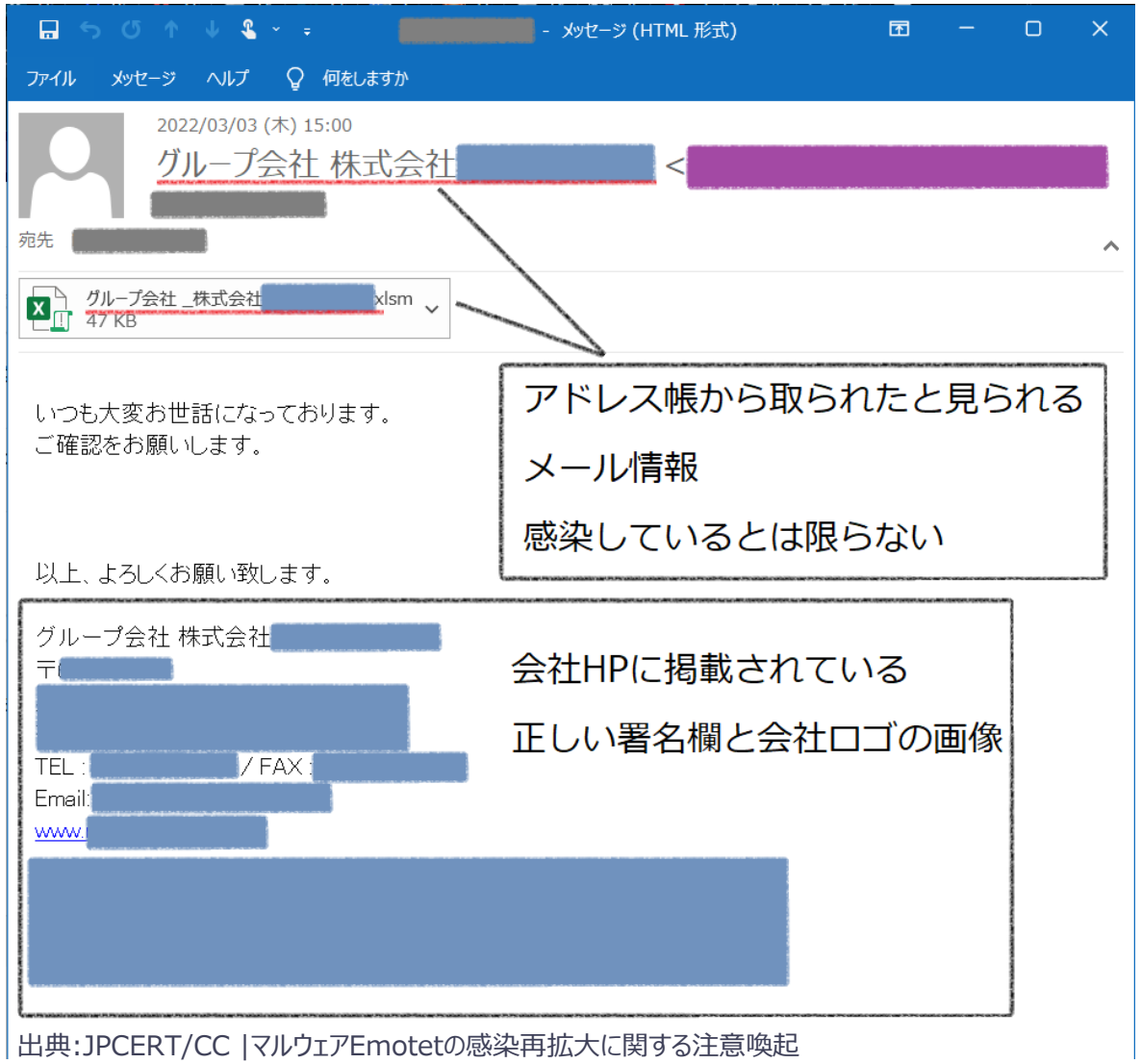
3月に全世界で観測された
DOC/TrojanDownloader.Agentのうち、
46.1%を日本が占める

Emotet感染の流れ



日々巧妙化する侵入手口

実在する組織を騙る、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.jpcert.or.jp/at/2022/at220006.html

メールの添付ファイル名や本文中に、
なりすまし元の組織名や署名などが
掲載されるケースを確認

Emotetが感染端末内のメーラーから
窃取した情報とみられる

インシデント被害発生時の損害額

インシデント損害額調査レポート

インシデント発生時に必要となる各種対応、
その対応によって生じるコスト（損害額・損失額）
を取りまとめ

出典：JNSA | インシデント損害額調査レポート 2021年版
https://www.jnsa.org/result/incidentdamage/2021.html

インシデント被害発生時の損害額

モデルケース：軽微なマルウェア感染

従業員がメールに添付されていたファイルを開いたところ、マルウェアに感染

調査結果

- メールを介して感染が
  拡大するマルウェアであり、
  従業員端末3台とサーバー1台の感染が判明
- 個人情報の漏えいなど、顧客影響等はなし

損害額：600万円

内訳

- 事故原因・被害範囲調査：500万円
- 再発防止策：100万

ランサムウェアに感染した場合、
事故原因・被害範囲調査がより困難となり
復旧費用も必要となるため、さらに大きな損害となる

出典：JNSA | インシデント損害額調査レポート 2021年版
https://www.jnsa.org/result/incidentdamage/2021.html

2021年のサイバーセキュリティ脅威動向

まとめ

- ✓ コロナ禍以降、**マルウェアの検出数は高い水準が継続**
- ✓ **ランサムウェアの初期侵入経路**は、
  VPN機器の脆弱性悪用や**RDP**が許可された端末が増加
- ✓ データの暗号化だけではなく**機密情報の暴露**など、脅迫の手口が凶悪化
  身代金の支払いを拒否した場合も**復旧に長期間が必要**となり**経営に大きな影響**
- ✓ 2021年11月、**Emotetが復活**
  感染拡大の手口がより巧妙になり、**メールにも引き続き注意が必要**

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

日々高度化、巧妙化するサイバーセキュリティ脅威に対する備えが必要

＃本日お話しすること

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と
ESET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