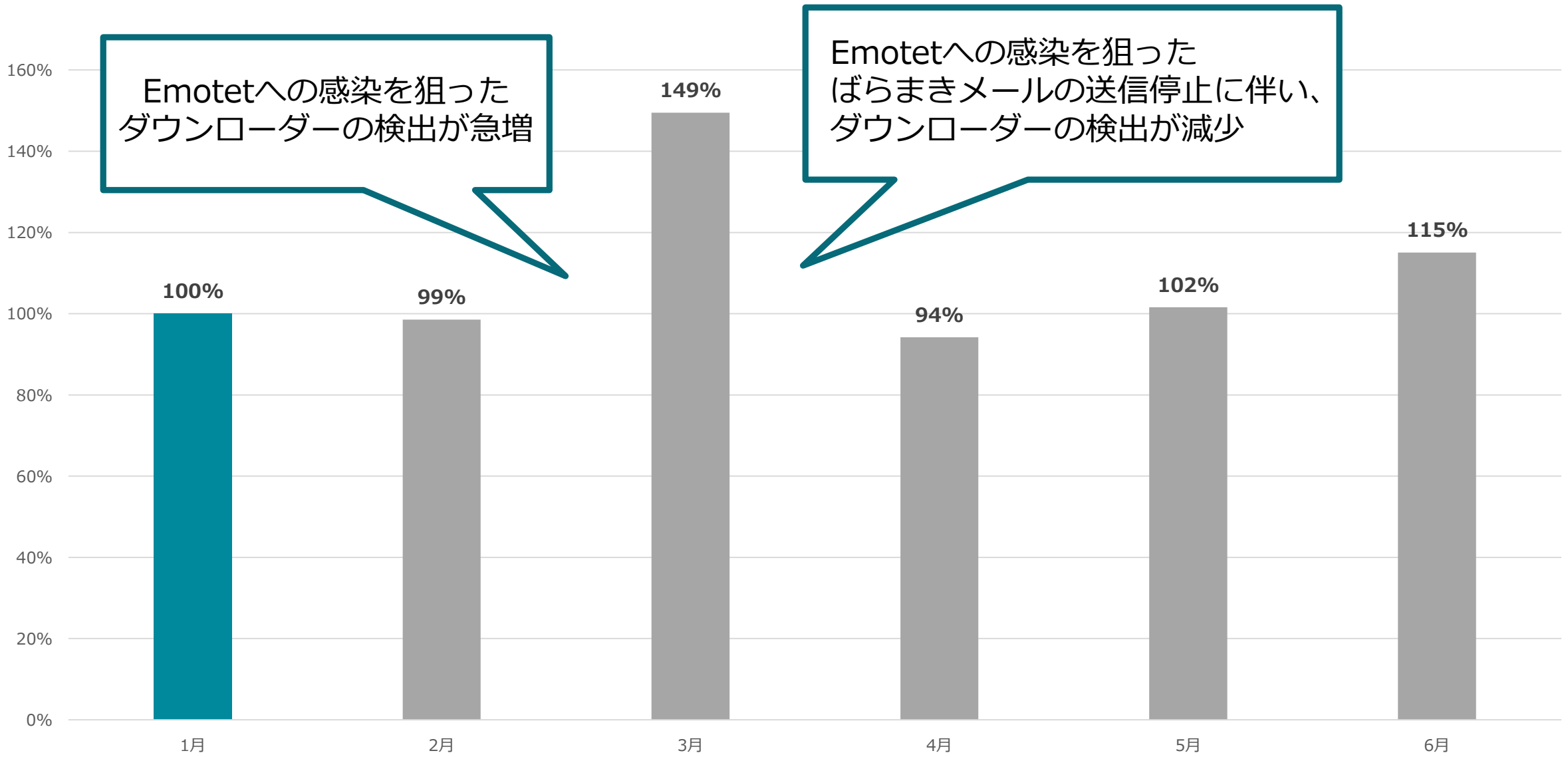
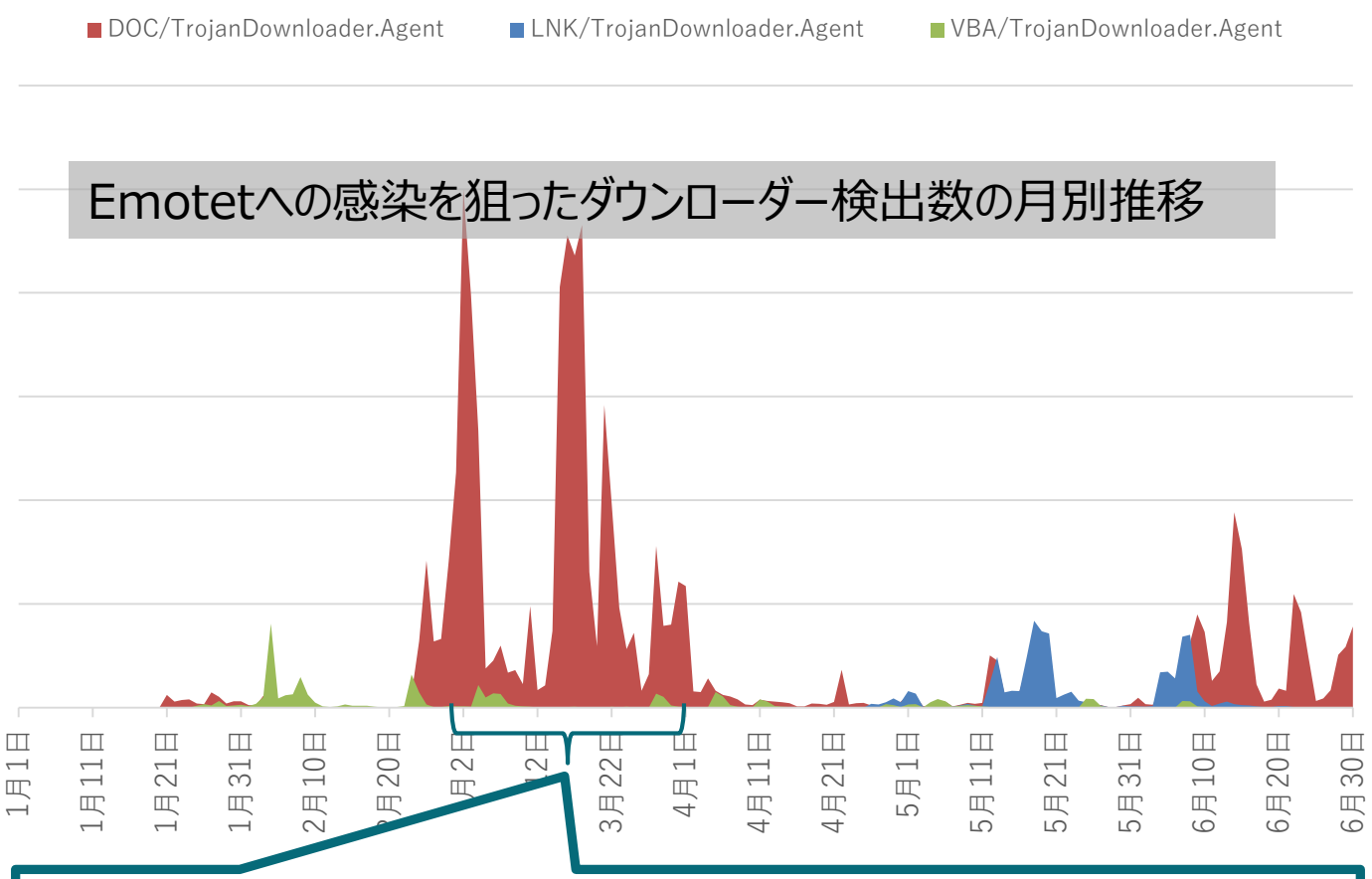
2022年上半期
サイバーセキュリティレポート
紹介動画

ご紹介内容

2022年上半期統計　～国内検出数月別推移～



2022年上半期のEmotetの活動状況

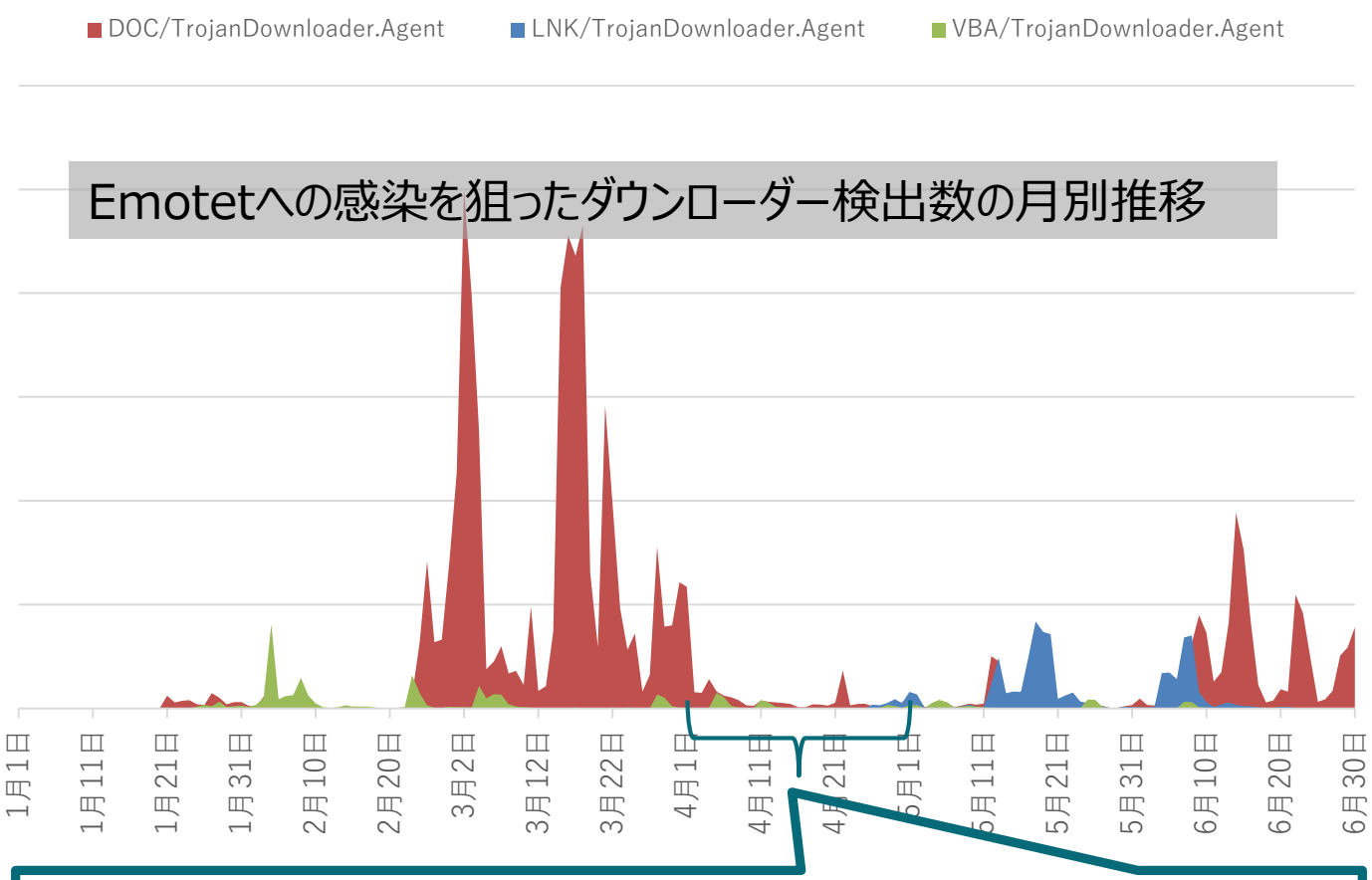


2022年3月

Emotetへの感染を狙ったばらまきメールを多数検出

Emotetへの感染報告を公表する企業も増加

2022年上半期のEmotetの活動状況



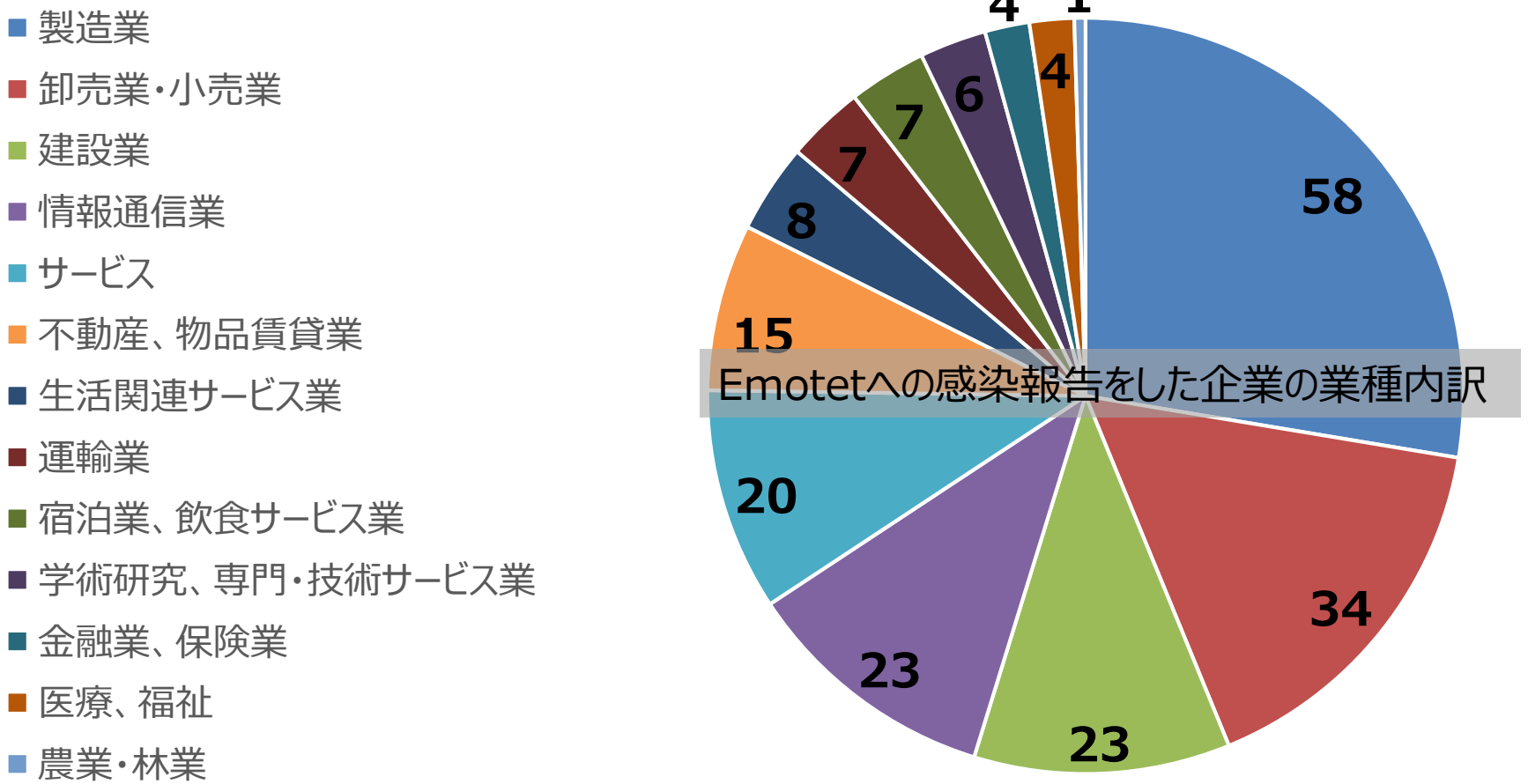
2022年4月

Emotetへの感染を狙ったばらまきメールの送信が一時停止

ばらまきメール送信再開後に、LNK形式のダウンローダーを確認

2022年上半期のEmotetの活動状況

製造業や小売業などで多数の報告が公表
特定の業種ではなく、様々な業種で感染している



Emotetへの感染報告をした企業の業種内訳

Internet Explorerのサポート終了に伴う今後の展望

Microsoft社のWebブラウザであるIE

- 2022年6月にサポート終了を発表
- 2000年代はWebブラウザの世界シェア1位
- 様々な要因によって、徐々にシェアが低下

多くの脆弱性が発見された

- サイバー攻撃に悪用される機会が多かった

Web標準への準拠度合いが低かった

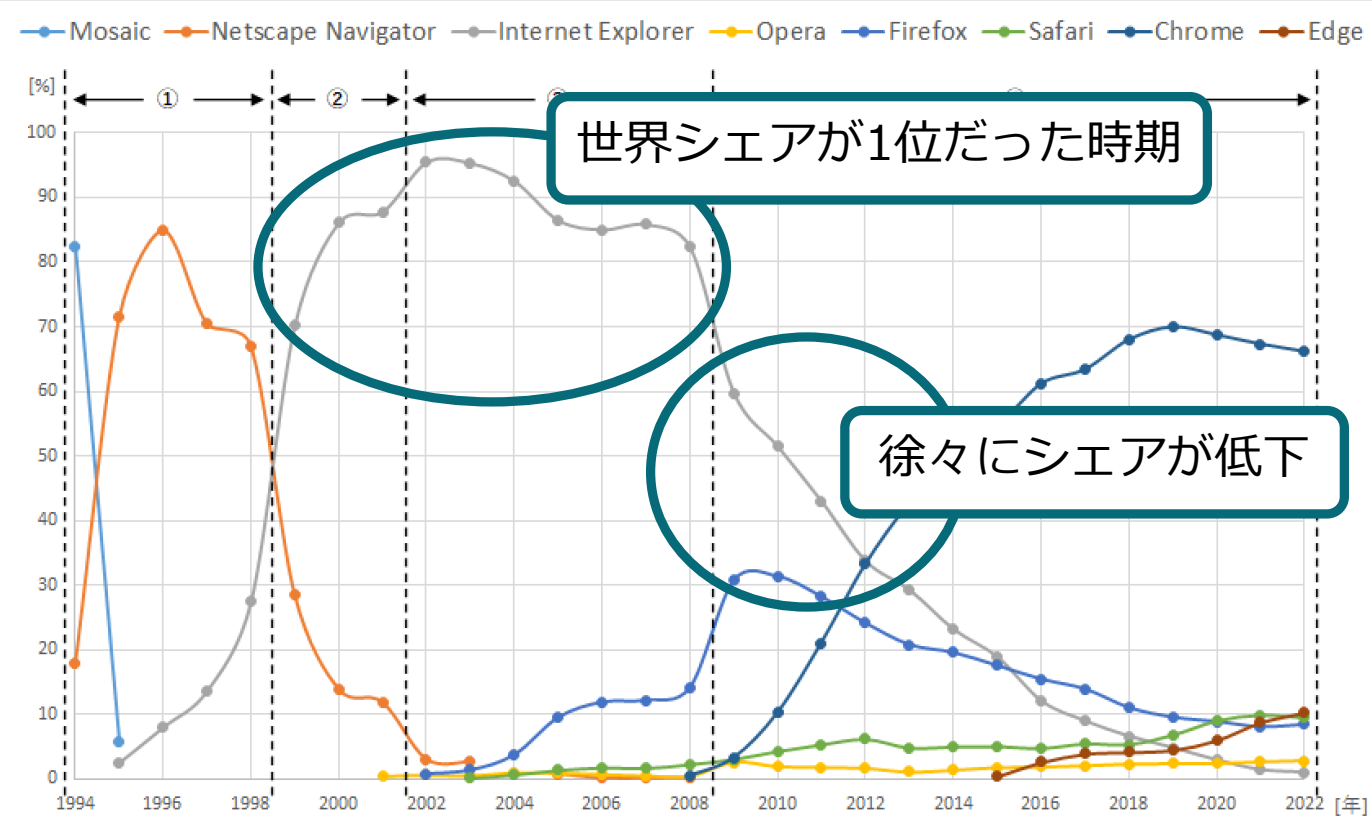
- Webページが正しく表示されないケースが見られた

Windows OSに標準搭載した

- 独占禁止法に抵触するとして対応を迫られ、イメージ悪化に繋がった

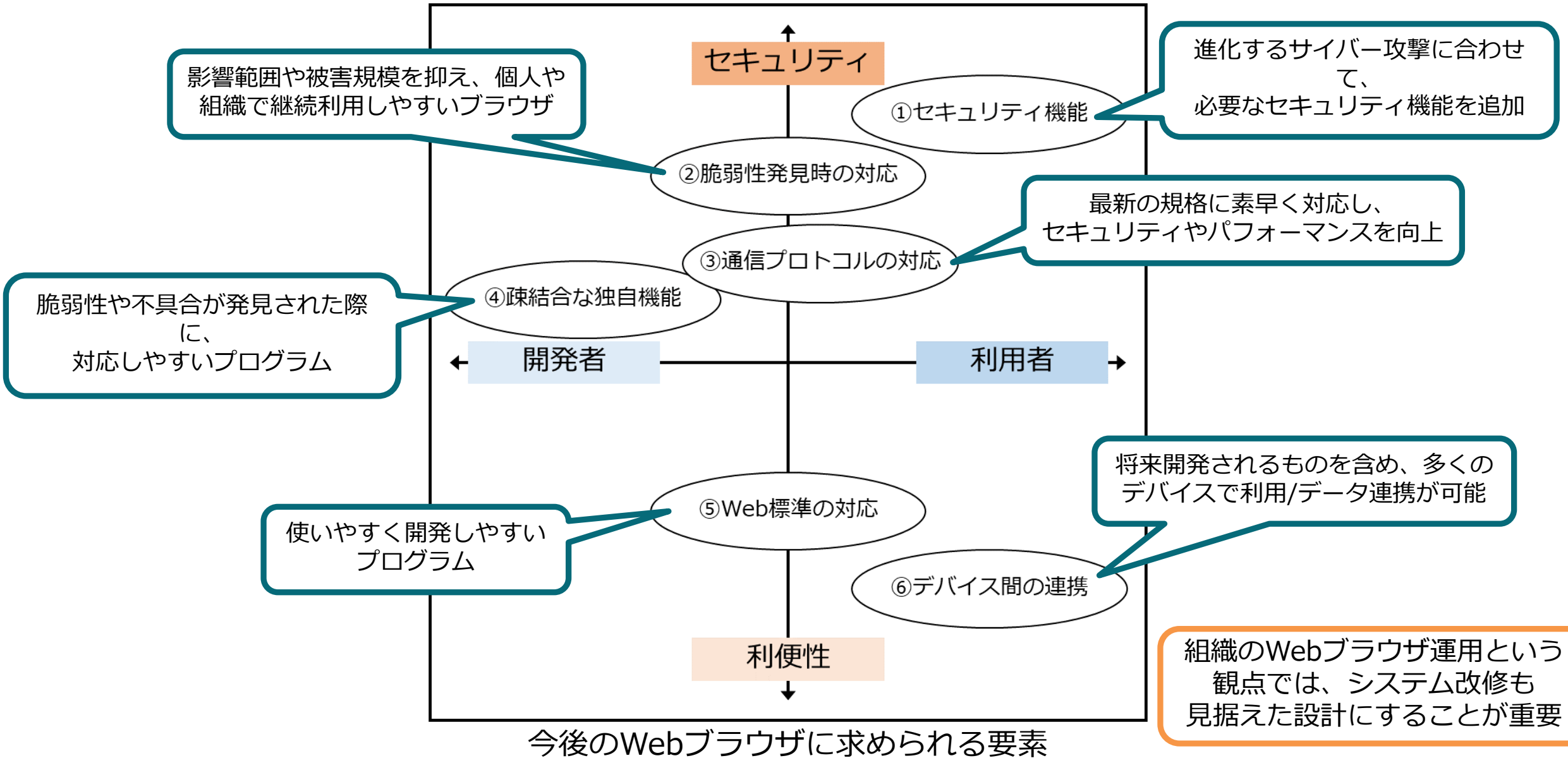
新興のWebブラウザが台頭した

- 使用者と開発者の双方が扱いやすいブラウザが次々と開発された



主要なWebブラウザの世界シェア推移

Internet Explorerのサポート終了に伴う今後の展望

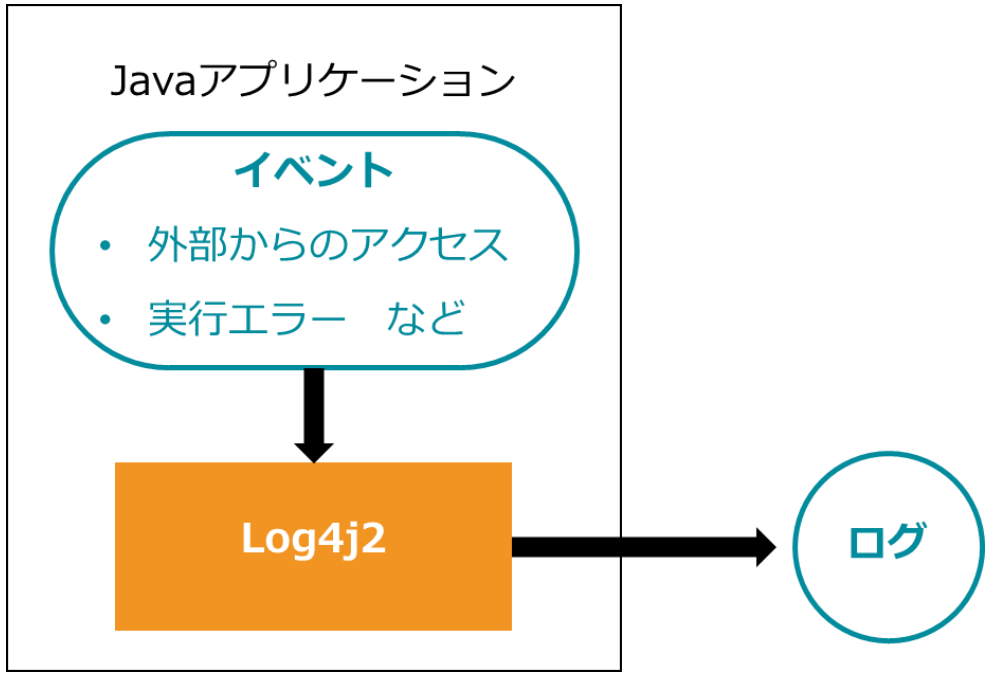


今後のWebブラウザに求められる要素

Log4Shellの検出状況と解説

Log4Shellとは:

- ロギングライブラリのApache Log4j
  バージョン2.x系（Log4j2）で発見された脆弱性

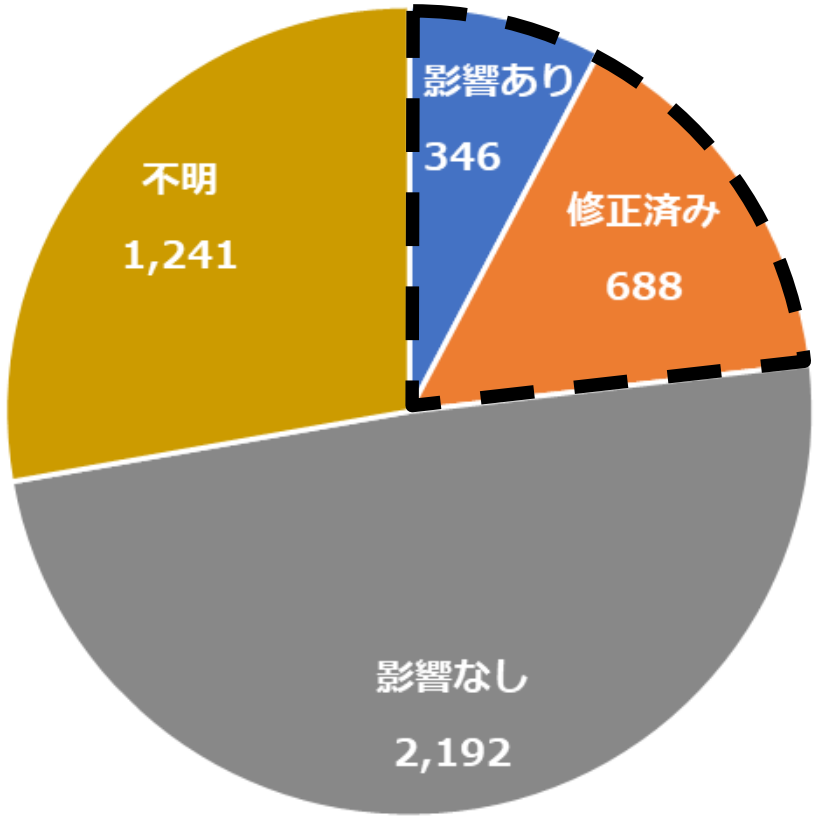


Log4j2の概要

- 悪用された場合、
  リモートの攻撃者による任意のコード実行が可能

Log4Shellの影響を受ける製品は

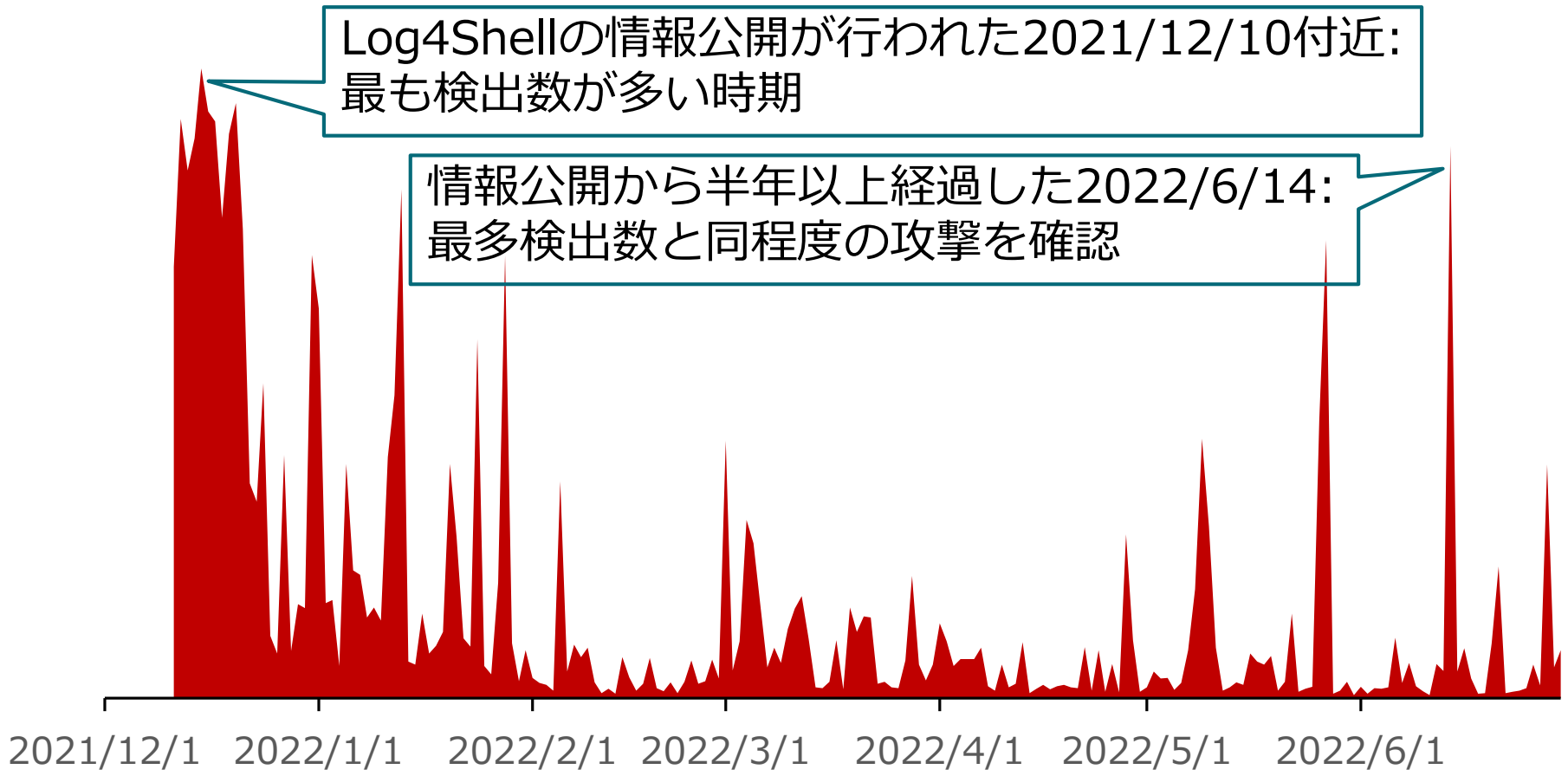
少なくとも1,000以上



CISAによるLog4Shellの影響有無に関する調査結果
（N=4,467）[2022/8/2時点]
https://github.com/cisagov/log4j-affected-db/blob/develop/software_lists/README.md

Log4Shellの検出状況と解説

Log4Shellを悪用する攻撃を**JAVA/Exploit.CVE-2021-44228**として検知し、ブロックします



JAVA/Exploit.CVE-2021-44228の日別検出数推移
（2021年12月～2022年6月・日本）

- Log4Shellを悪用する攻撃は継続中
- 脆弱なLog4j2を未だに使用していないか、組織内での再度確認を推奨

本章終盤では、
Log4Shellが発生する
原因を解説【技術者向け】

国家によるセキュリティ製品の調達制限

ネットワーク機器やセキュリティ製品の
調達を国家が制限するケースが増加

近年の調達制限例

ロシアのセキュリティ企業

- FCC(米連邦通信委員会)
  「安全保障上の脅威がある企業」に追加
- ドイツ連邦情報セキュリティ庁（BSI）
  注意喚起を発表

中国企業5社からの通信機器

- 米国内での製品販売に必要な
  メーカーの認証を禁じる法案調達が成立

調達制限の背景

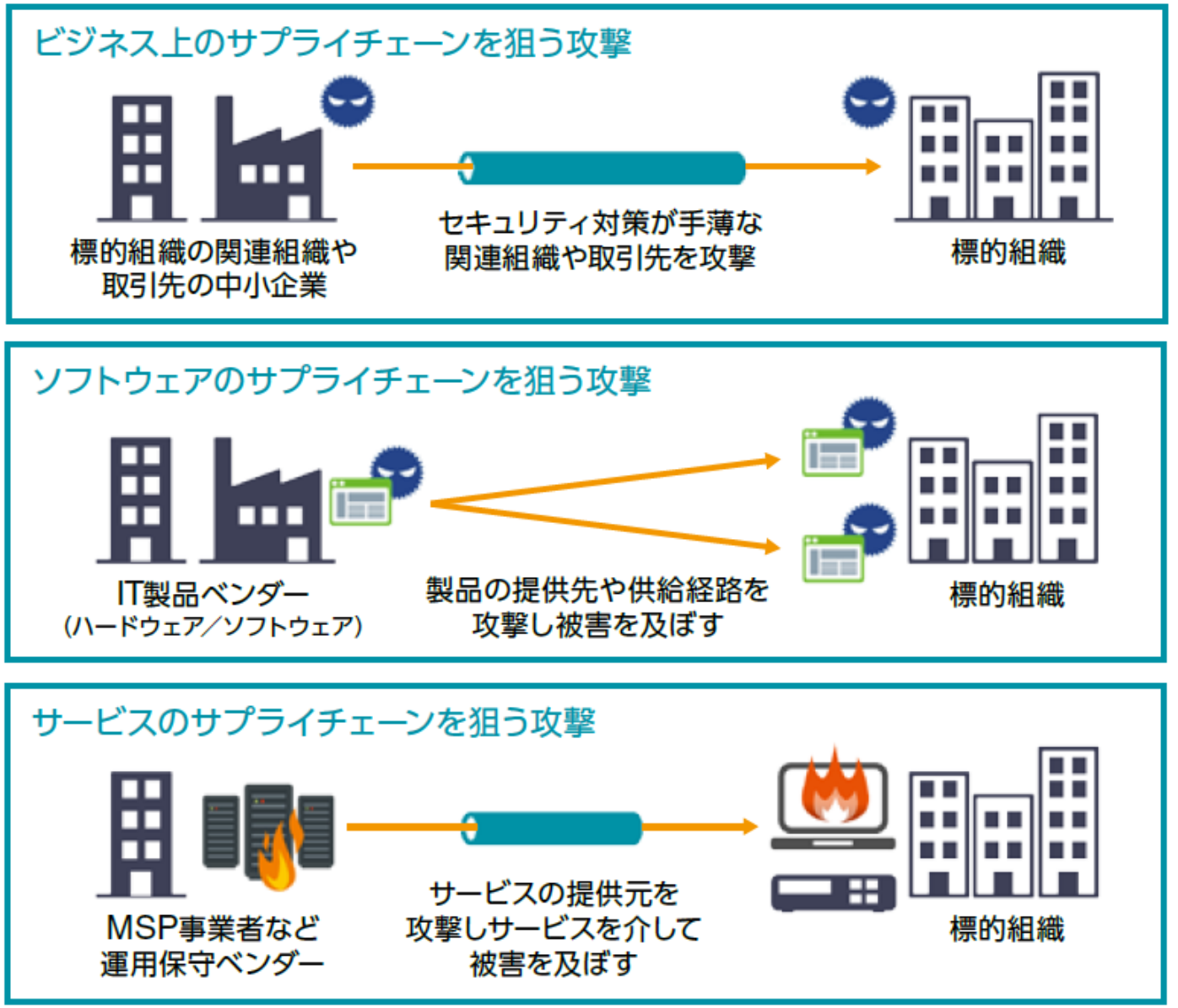
ネットワーク機器やセキュリティ製品の**特性**

その特性が悪用され場合のリスクとして、類似の特性も持つ製品が
悪用された例を挙げ、サプライチェーンリスクを紹介

サプライチェーン攻撃とは

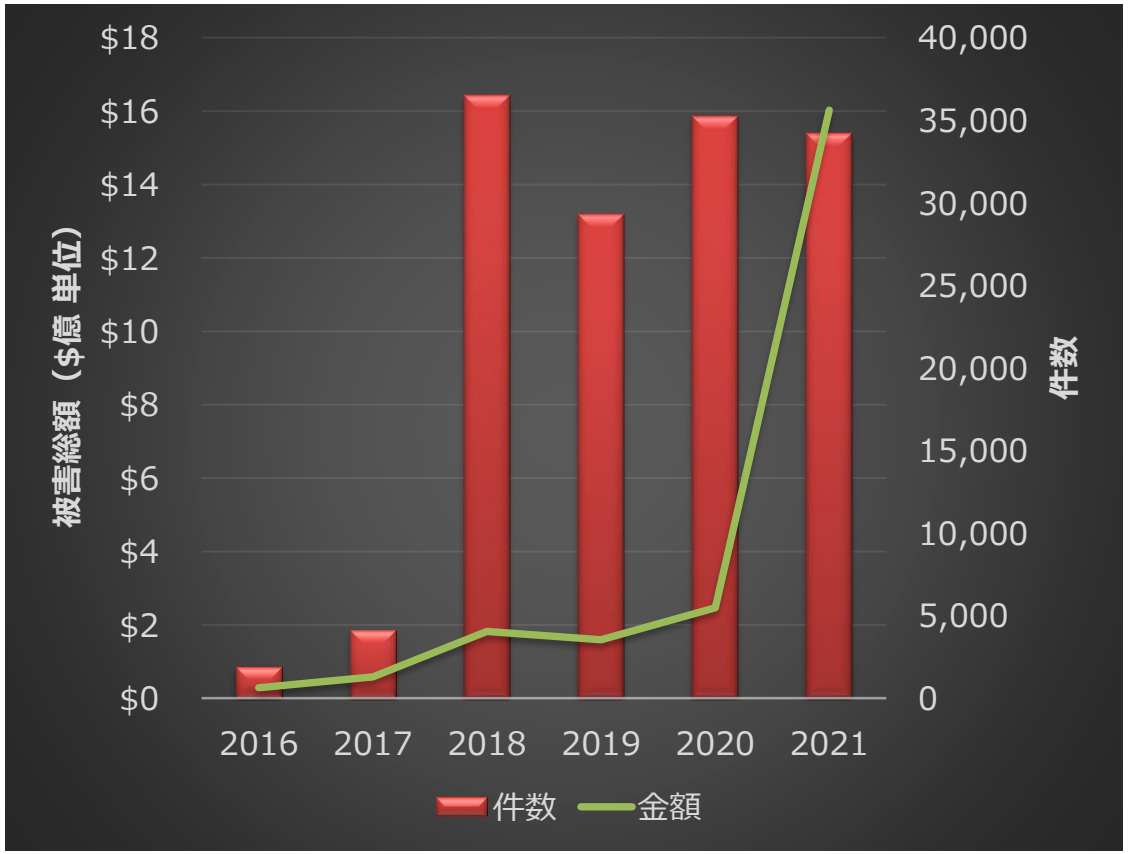
サプライチェーンにおける
関係性を悪用する攻撃

強いシステム権限を持つ製品は、
ソフトウェアのサプライチェーン、
サービスのサプライチェーンを
狙う攻撃に悪用されると
大きな被害につながるリスクがある



暗号通貨とサイバー犯罪との関わり

IC3 Internet Crime Report によると、
2021年は暗号通貨（暗号資産）に関するサイバー犯罪の被害額が、前年の7倍に達しました。

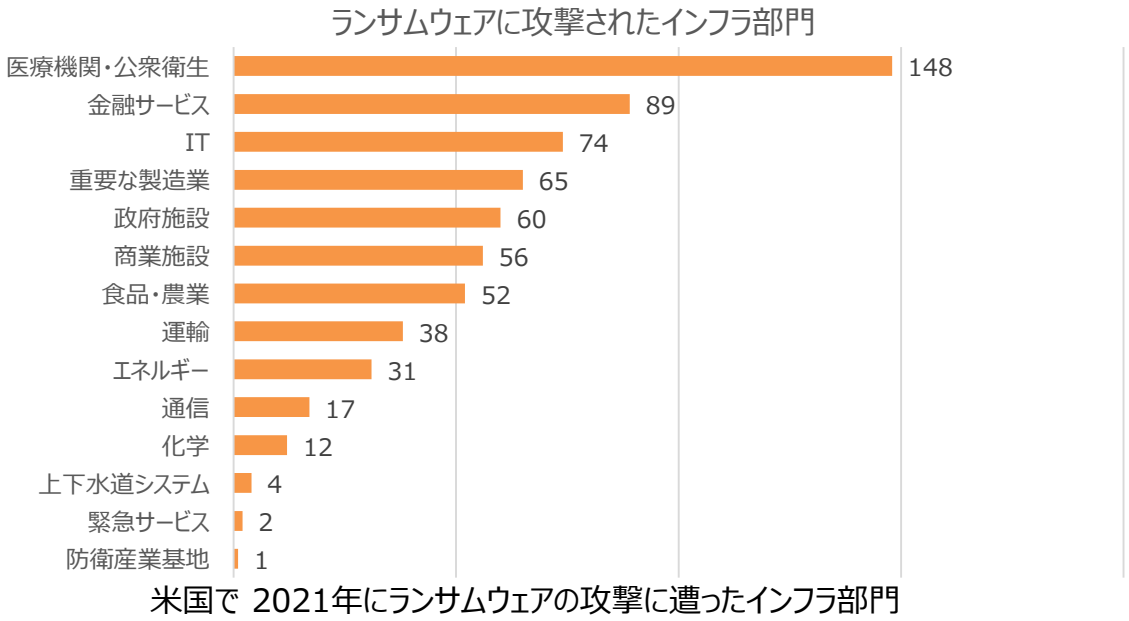


米国での、暗号通貨が関わっているサイバー犯罪の件数と被害総額の推移

被害額が大きくなる要因

暗号通貨取引所に対する攻撃

このような攻撃は、**高度な手法**が使われているため、**国家支援ハッキンググループの関与**が取り沙汰されています。



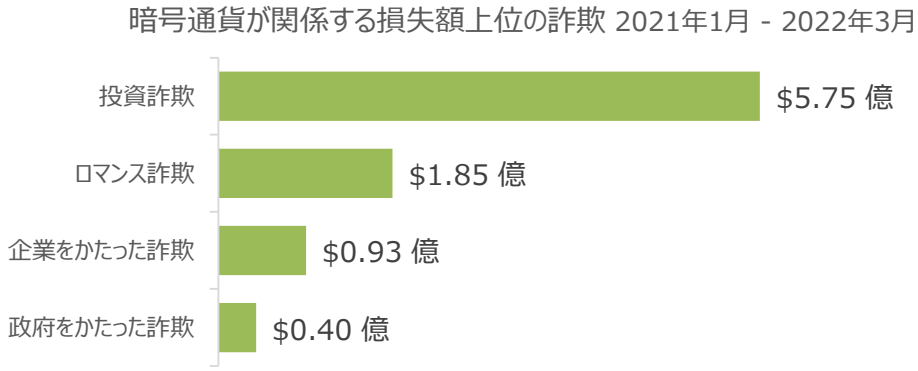
米国で 2021年にランサムウェアの攻撃に遭ったインフラ部門

ランサムウェアの身代金支払いへの悪用

身代金支払いは、暗号通貨が主流となってきています。
近年では、重要インフラや医療機関を狙った多額の身代金を要求する攻撃も増えており、一件当たりの被害額も増加しています。

暗号通貨を悪用した詐欺

FTC（米国連邦取引委員会）の資料によると、
暗号通貨が関係する詐欺で、2021年には **6.8億ドル** の被害が発生しています。
その中で最も被害が多いのが**投資詐欺**です。
国内においても、**暗号通貨を使用した投資詐欺の被害が増加**しています



米国での暗号通貨が関連する詐欺被害額（損失額上位）

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

ご視聴ありがとうございました。