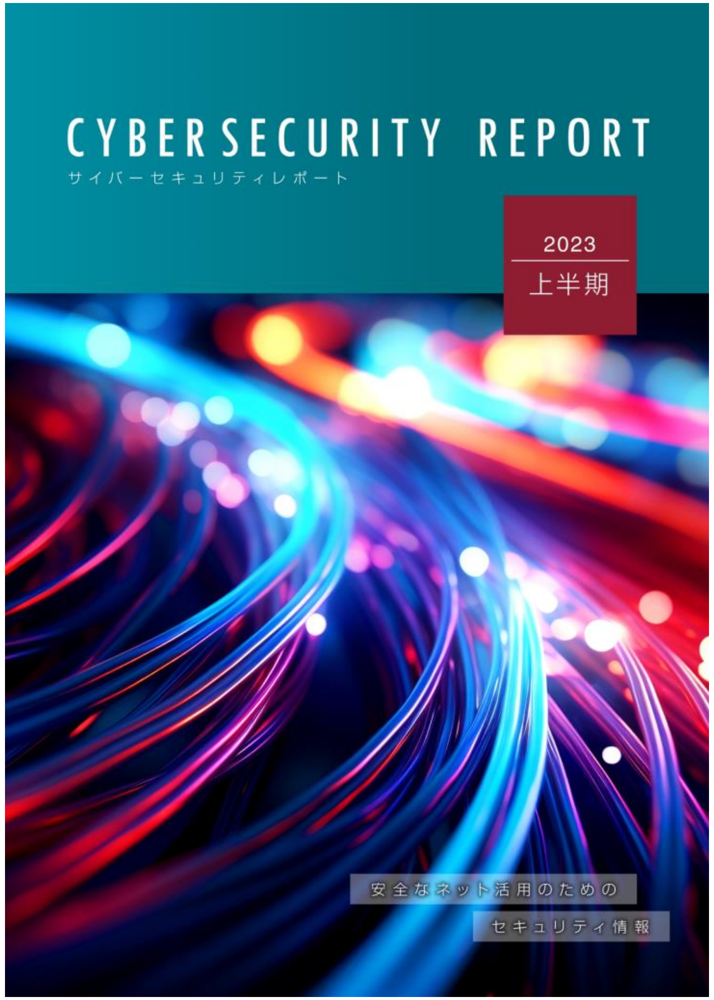
2023年上半期サイバーセキュリティレポート 紹介動画

2023年上半期サイバーセキュリティレポート



1章　2023年上半期マルウェア検出統計

2章　Emotetも悪用?OneNote形式のダウンローダーについて

3章　次世代Web3.0技術のセキュリティ
IPFSを悪用したフィッシング詐欺について

4章　ChatGPTをはじめとする生成AIの悪用シナリオと、
安全に使うために気を付けるべきこと

5章　医療機器の脆弱性～その攻撃可能性と対策

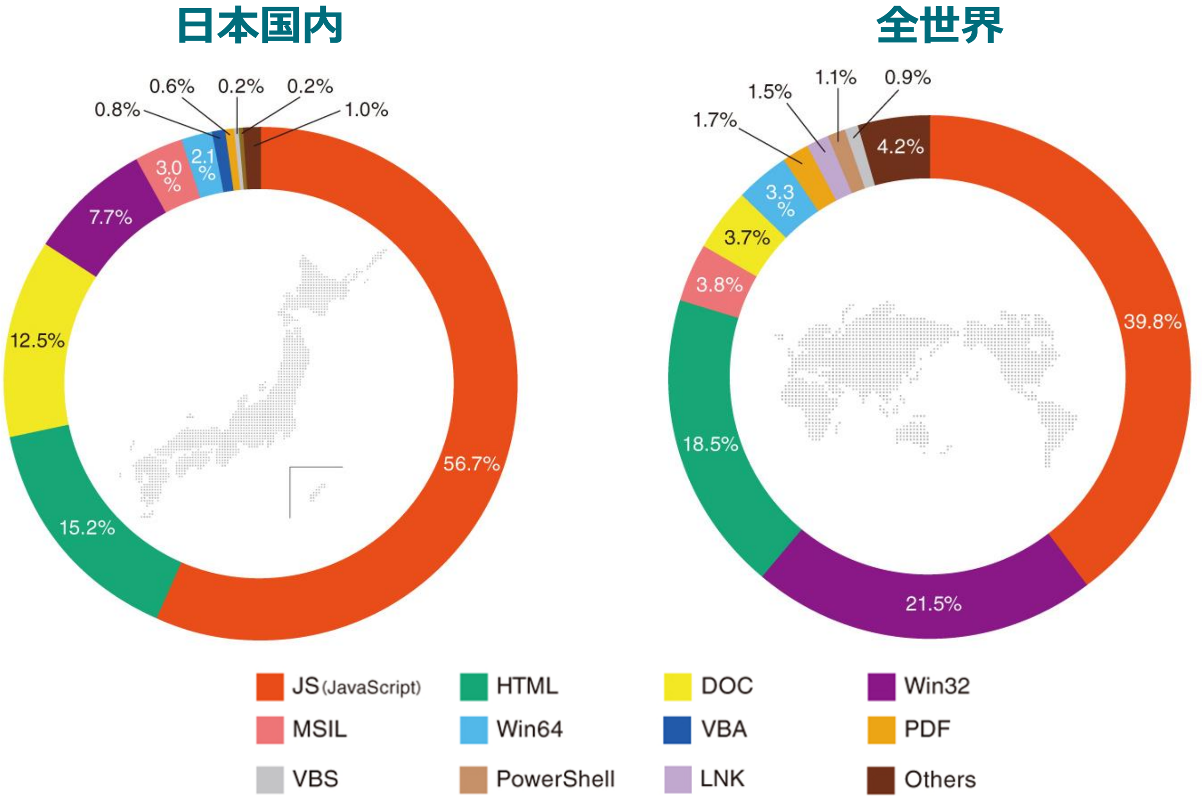
6章　実践！シフトレフト～今から始めるソフトウェア開発者の
セキュリティ対策

サイバーセキュリティ情報局Webページで公開中

1章 2023年上半期マルウェア検出統計

概要

2023年上半期にESET製品で検出されたマルウェアの統計を解説
検出数TOP10やファイル形式別統計も説明しています



2023年上半期における
マルウェア検出数のファイル形式別の割合
国内と全世界での傾向の違い

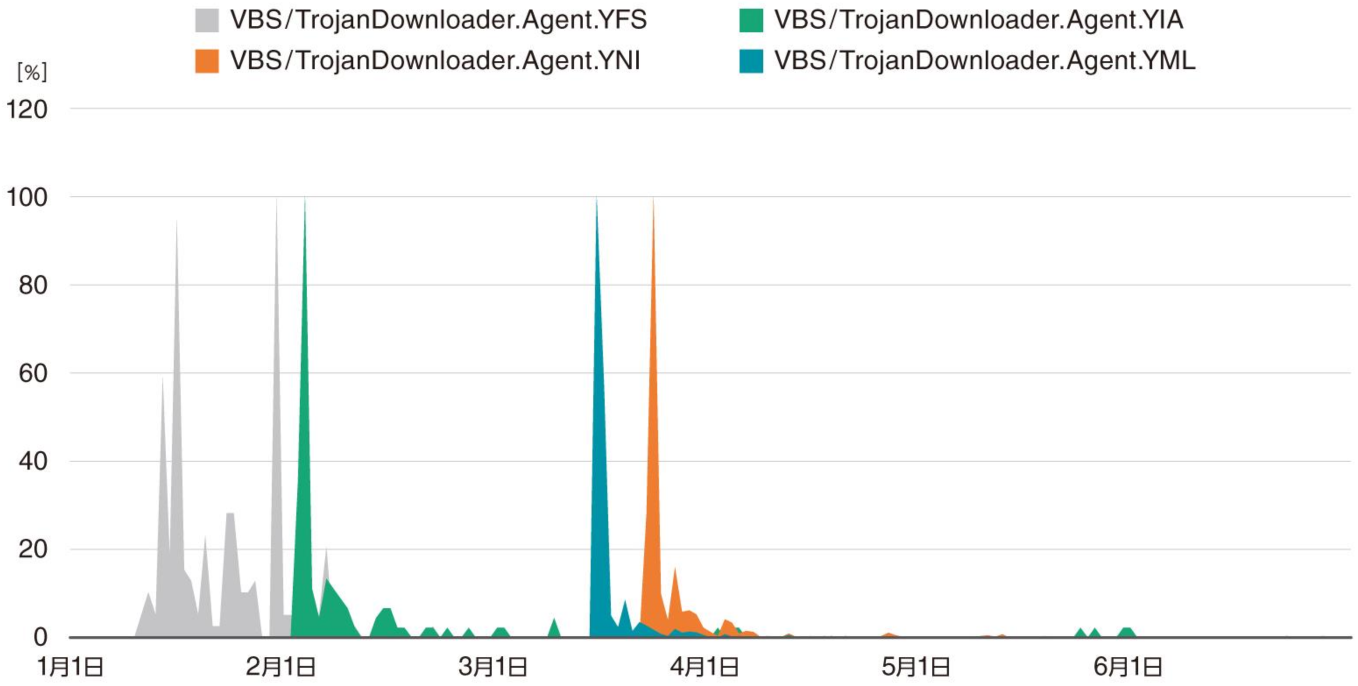
国内
■ **DOC形式**の占める割合が**全世界より高い**
DOC/Fraud の検出数が大きく影響

全世界
■ **LNK形式**の占める割合が**国内より高い**
LNK/Agentの検出数が大きく影響

2章 Emotetも悪用?OneNote形式のダウンローダー

概要

Emotetも悪用したOneNote 形式のダウンローダーを解説
OneNote 形式のダウンローダーへの対策も説明しています



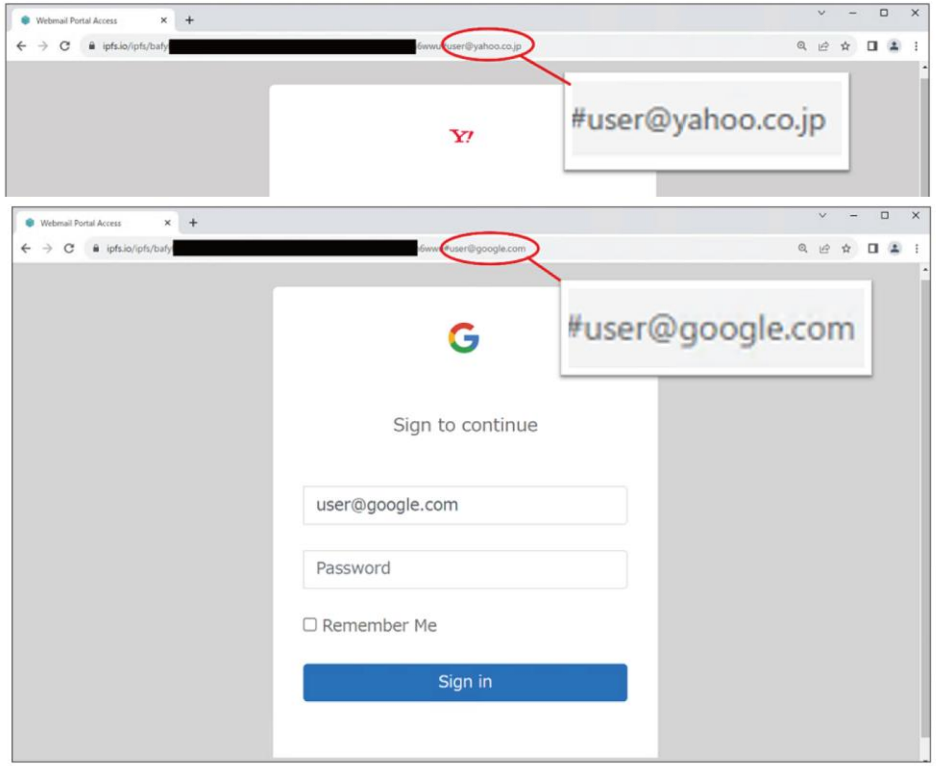
- 検出時期は主に**1月～4月**
- ダウンロードされる**マルウェアが異なる**

検出名	ダウンロードされるマルウェア
VBS/TrojanDownloader.Agent.YML	Emotet
VBS/TrojanDownloader.Agent.YNI	
VBS/TrojanDownloader.Agent.YIA	Qakbot
VBS/TrojanDownloader.Agent.YFS	AsyncRAT

3章 次世代Web3.0技術のセキュリティ IPFSを悪用したフィッシング詐欺について

概要

近年利用が進んでいるIPFSの仕組みやHTTPとの違いを解説
IPFSを悪用したフィッシング詐欺の事例も説明しています



サイバーセキュリティラボで確認したフィッシング事例

- URIに含まれるメールアドレスが変更されると、**メールアドレスに合わせてIPFSでホストされたフィッシングページが変更**される

結果として

1つのURIが異なるユーザーを対象としたフィッシングキャンペーンで使用されることがある
場合によっては、**数十のキャンペーンで使用**されることも

4章 ChatGPTをはじめとする生成AIの悪用シナリオと、安全に使うために気を付けるべきこと

概要

利用が進むChatGPTに関する悪用シナリオと対策を解説
生成AIの利用に関する公的機関のガイドラインも説明しています

悪用シナリオ	悪用例
攻撃者によるChatGPTの悪用	ChatGPTを騙る攻撃
	詐欺を目的とした文章を作成する（フィッシングやBECの増加）
	マルウェアの生成
ChatGPTを使用するシステムへの攻撃	プロンプト・インジェクション

ChatGPTを悪用する手法

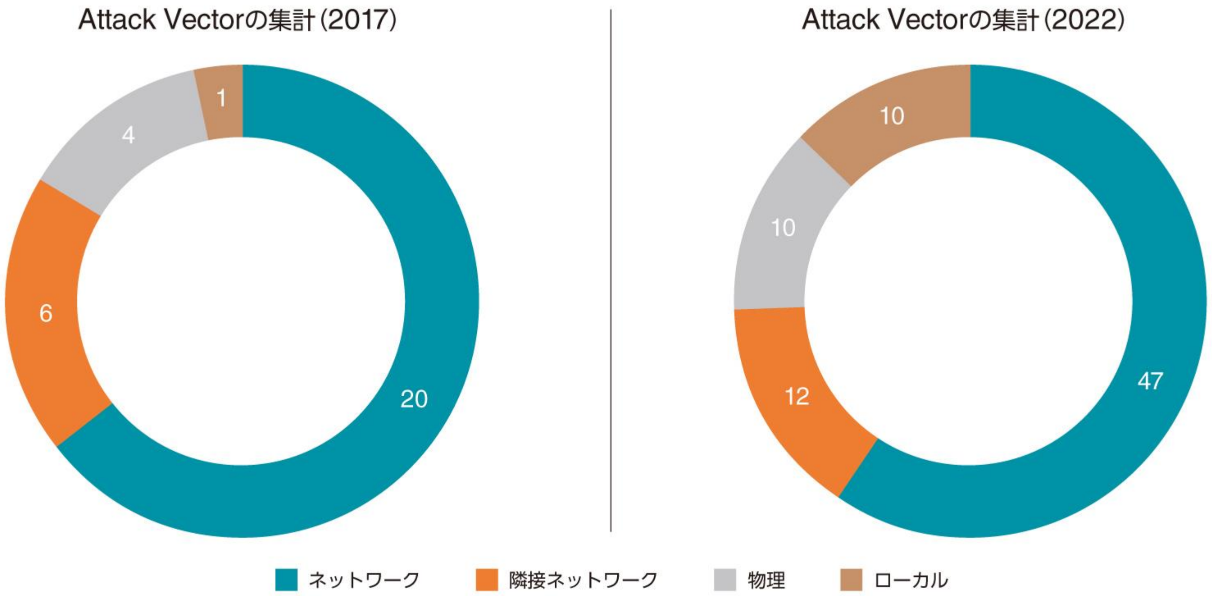
■ 悪意のない要求
依頼に対して状況の説明など条件を追加することで
悪意のない要求に見せかけ、
要求を実行させる手法

■ ChatGPT Jailbreak
ChatGPTに施された**予防措置をバイパス**する手法

5章 医療機器の脆弱性～その攻撃可能性と対策

概要

医療機器の脆弱性の特徴や事例、攻撃可能性を解説
国内外の公的機関から公開されたガイドラインについても説明しています



2017年と2022年のICSMAをAttack Vectorで集計した結果
（Cybersecurity Alerts & Advisories | CISAのデータより作成）

- **ネットワーク経由の攻撃**が**7割**を占める

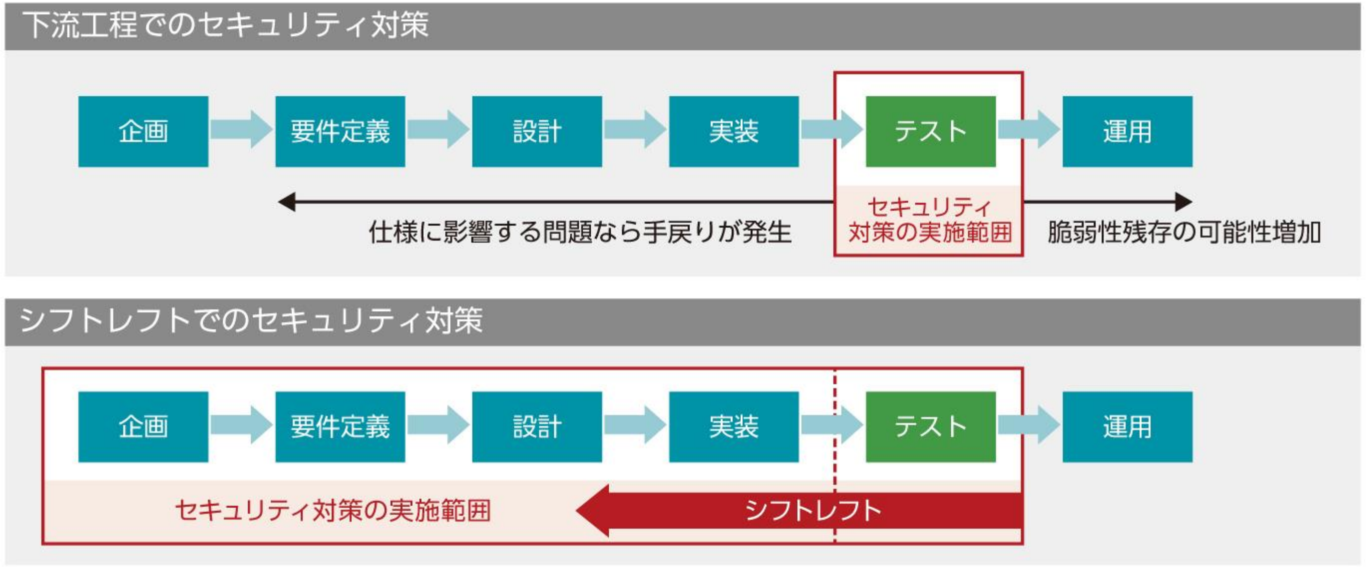
背景には
さまざまな要因

- 複数の医療機器を**ネットワークで接続**し、中央のサーバーで監視やデータ保存を行う医療機器が増えた
- 1つの製品で、ネットワークに関する**脆弱性が複数発見**されることが多い

6章 実践！シフトレフト ～今から始めるソフトウェア開発者のセキュリティ対策

概要

ソフトウェア開発現場におけるセキュリティ対策として「シフトレフト」を解説
具体的な事例を元にシフトレフトのポイントも説明しています



ソフトウェア開発において、
下流工程でのみセキュリティ対策を実施すると

- 仕様に影響する問題が発生した場合、**手戻りによるコスト**発生
- セキュリティ要件や仕様の抜け漏れにより、**運用後に脆弱性が残る可能性**が上昇

セキュリティ向上させるために

下流工程ではなく**上流工程などの早い段階**でセキュリティ対策を講じる
シフトレフトが効果的

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**

ご視聴ありがとうございました。