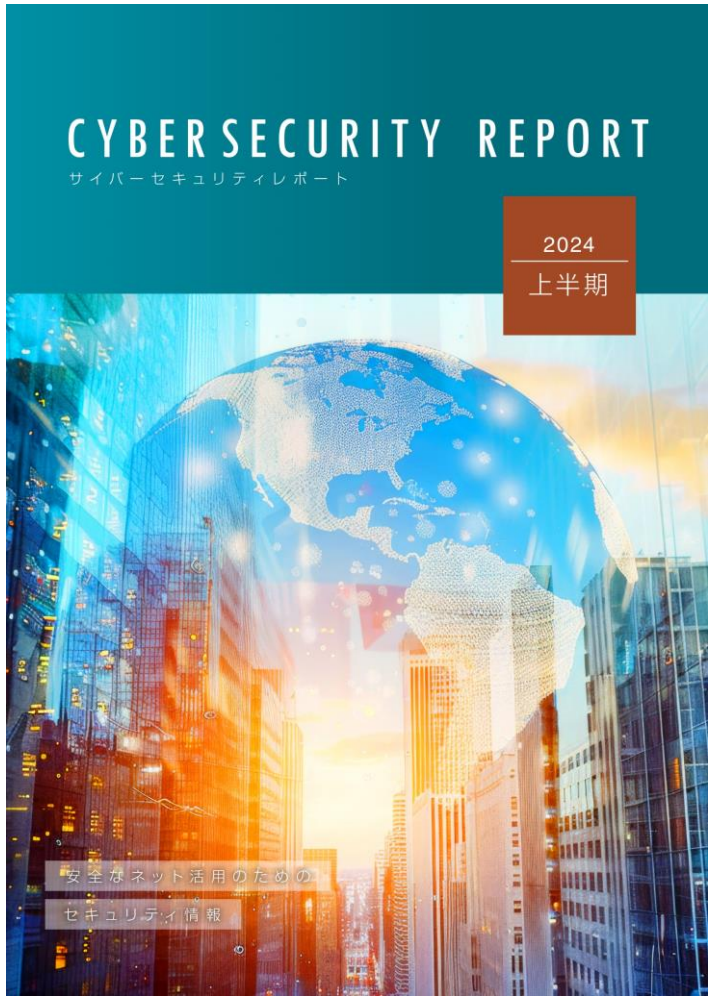
2024年上半期サイバーセキュリティレポート

～脆弱性を悪用したカスタムツールGooseEggやWordPressを狙った攻撃事例を解説～

2024年上半期サイバーセキュリティレポート



掲載テーマ一覧

- 1章 | 2024年上半期マルウェア検出統計
- 2章 | 脆弱性を悪用して権限昇格を行うカスタムツールGooseEgg
- 3章 | 仕組まれた分散型ブルートフォース攻撃と狙われたWordPress
- 4章 | パスワード単独認証の限界とその対策

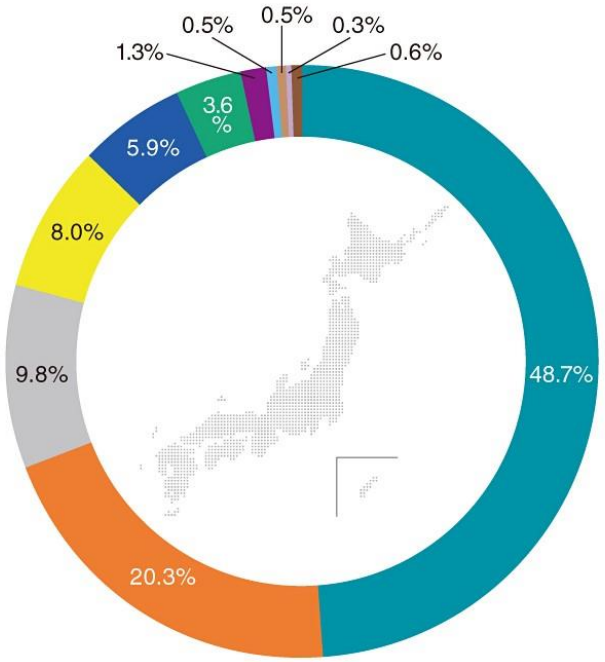
サイバーセキュリティ情報局にて公開中

1章 2024年上半期マルウェア検出統計

概要

2024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
通信プロトコルや脆弱性悪用についても統計を紹介

形式別マルウェア検出数の割合（2024年上半期・国内）



マルウェア以外の脅威の検出数TOP10

マルウェア以外の脅威検出数*TOP10

国内

1位 RDP/Attack.Bruteforce	6位 SMB/Exploit.DoublePulsar
2位 SMB/Attack.Bruteforce	7位 SMB/Exploit.EternalBlue
3位 JAVA/Exploit.CVE-2021-44228	8位 SMB/Exploit.MS17-10
4位 HTTP/Exploit.CVE-2021-41773	9位 PHP_CVE-2024-4577
5位 CVE-2017-5638.Struts2	10位 CVE-2015-1635

通信プロトコルを狙った攻撃　脆弱性を悪用した攻撃

*本図にはPUAを含めていません。

組織内で使用しているソフトウェアの洗い出しや認証情報の棚卸を検討してください

2章 脆弱性を悪用して権限昇格を行うカスタムツールGooseEgg

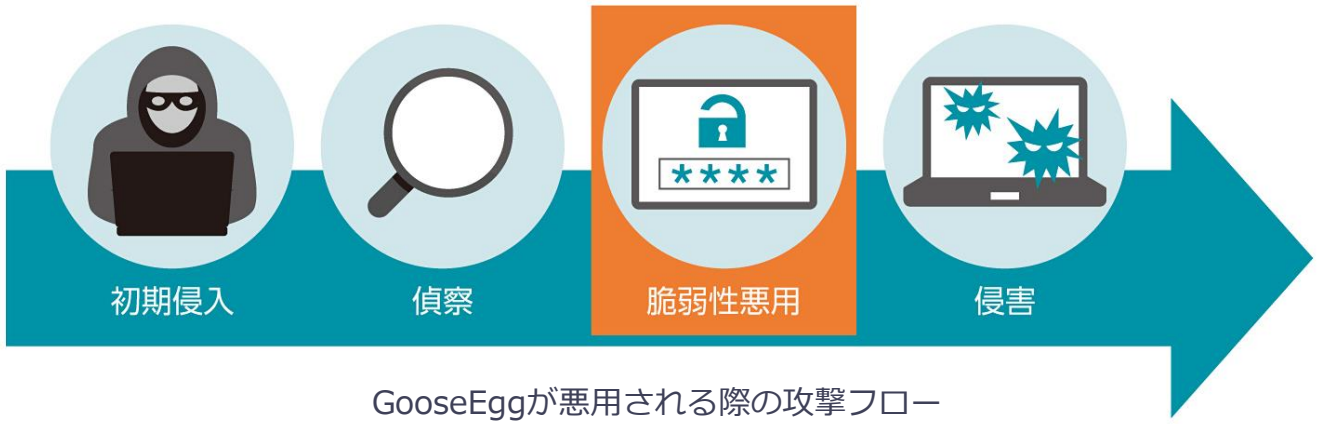
概要

2024年4月にMicrosoftより悪用が報告されたカスタムツールGooseEggについて紹介
日本国内を標的とした攻撃でGooseEggが悪用される可能性について警告

GooseEggとは

- 攻撃者グループForest Blizzardが作成した権限昇格を行うカスタムツール
- CVE-2022-38028を悪用して権限昇格を行う

GooseEggは主に標的型攻撃で使用される



GooseEggが悪用される際の攻撃フロー

侵入後の攻撃者の活動

侵入した環境に存在する
脆弱性を調査

↓

発見した脆弱性を悪用

↓

管理者権限を用いて
更なる侵害行為を実行

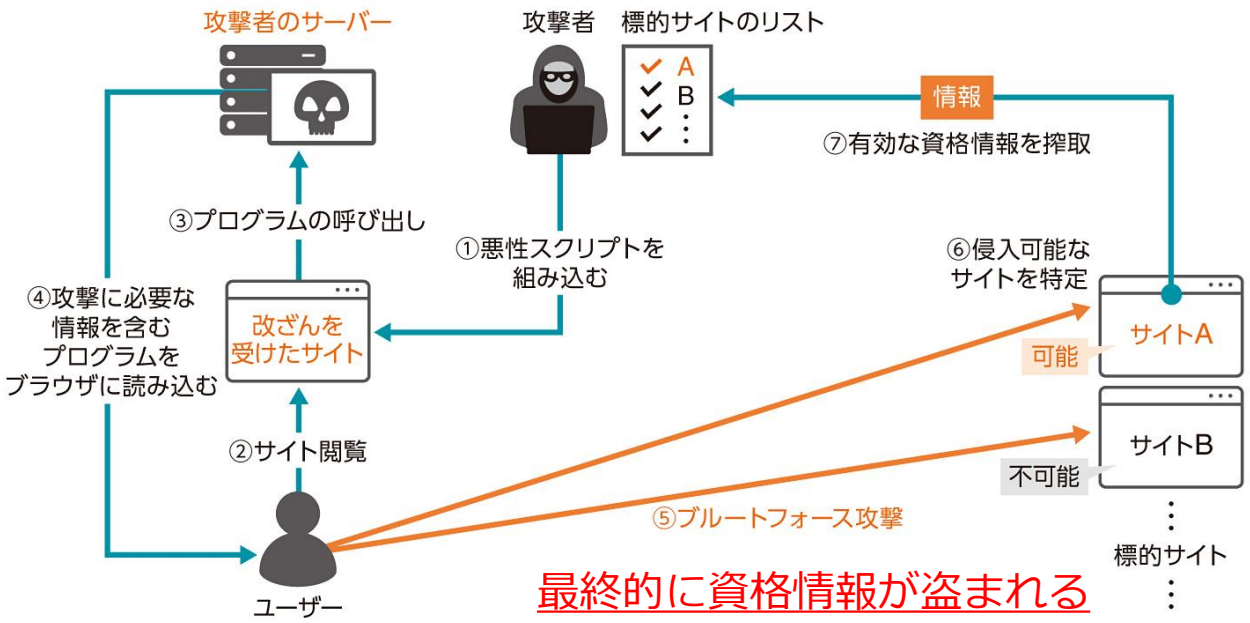
権限昇格が行われると深刻な被害が想定されるため、適切な対策を行う必要がある

3章 仕組まれた分散型ブルートフォース攻撃と狙われたWordPress

概要

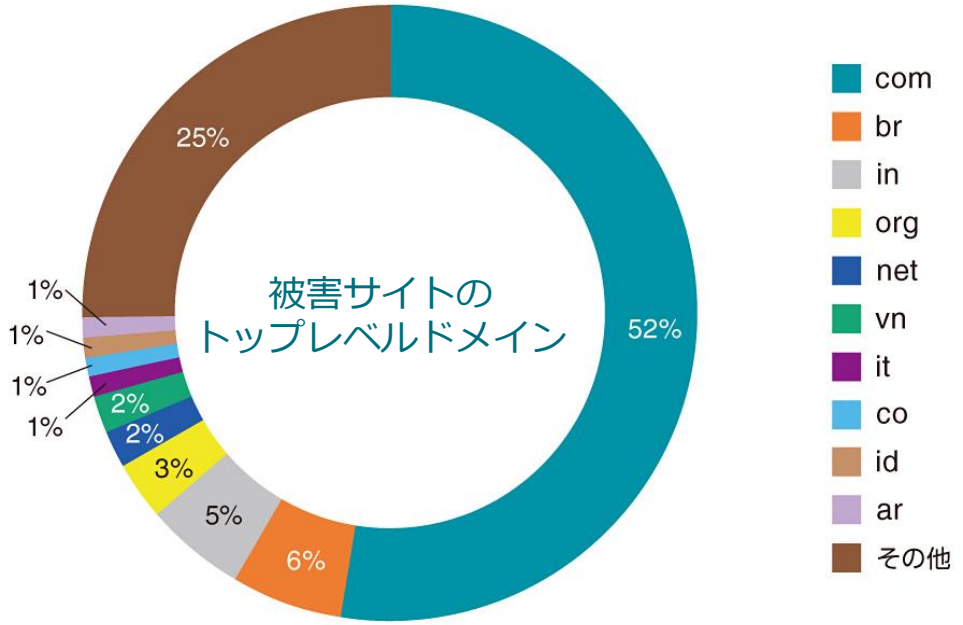
WordPressで構築されたWebサイトに対する改ざんを検出、海外で観測された手口と同一であると確認
攻撃手法について解説し、改ざん被害を受けたWebサイトの傾向について調査結果を紹介

分散型ブルートフォース攻撃の流れ



最終的に資格情報が盗まれる

改ざん被害を受けたWebサイトの傾向について調査



企業内エンドポイントと公開Webサイト双方を守れる体制づくりが重要です

4章 パスワード単独認証の限界とその対策

概要

更新された「サイバーセキュリティ初心者のための三原則」を取り上げて考察
パスワードに対する攻撃手法を紹介し、それに対抗できる「強固なパスワード」について解説

サイバーセキュリティ初心者のための三原則

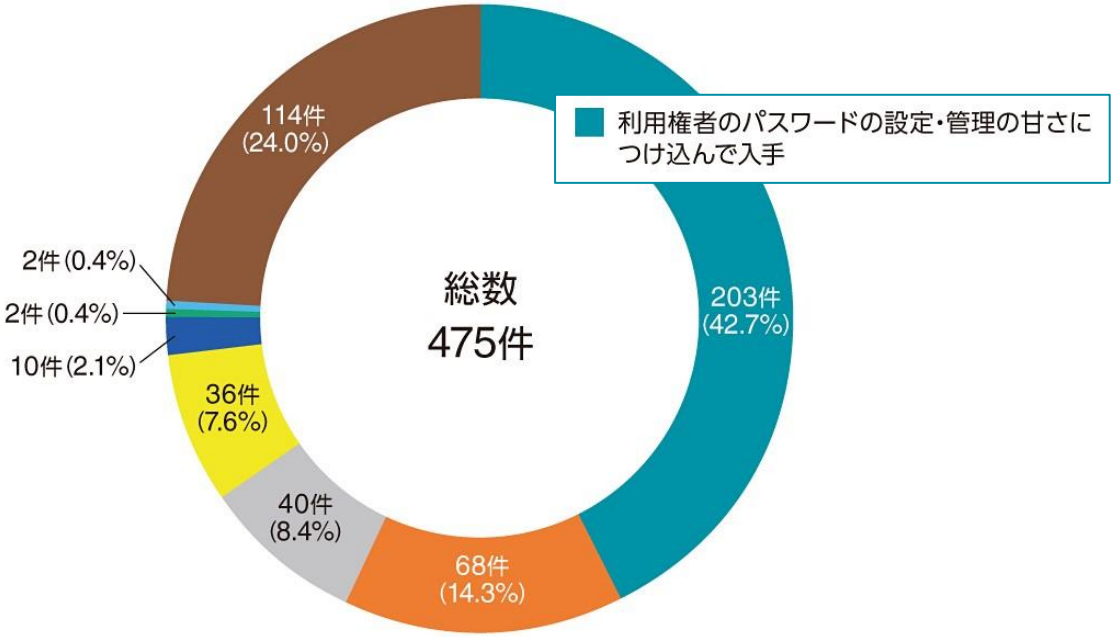
- ソフトウェアを最新に保とう
- 強固なパスワードの設定と多要素認証を活用しよう
- 不用意に開かない・インストールしない

➡ 未知のマルウェアやフィッシングを想定

強固なパスワードとは……

- パスワードの文字数、文字の種類
- パスワードの使いまわしを行わない
- 多要素認証

不正アクセスは「パスワードを不正に入手」が最多



サービスを安全に使用するために、強固なパスワードと多要素認証を設定しよう

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。