おまかせサイバーみまもり

2025年11月　セキュリティ対応状況と検知状況

2025年12月
NTT東日本株式会社

セキュリティ対応状況

2025年11月6日（現地時間）、PushSecurityより、ソーシャルエンジニアリングの一種である「ClickFix」の攻撃手法が進化し、複数OSへの対応やマルウェアに感染させる操作手順の巧妙化について報告されております。最新のClickFix攻撃は、利用中のデバイスに合わせて適応し、OSごとに異なる手順を表示するようになっております。また、「クリックで問題解決」と表示するCloudflare認証画面を装うなど、他のメーカーの正規ウィンドウを装い、より説得力を持たせるように工夫されております。

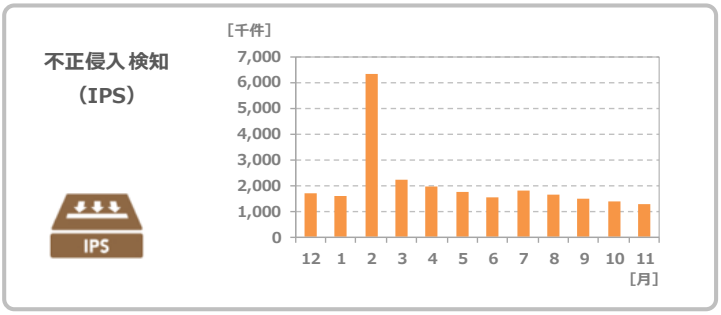
エンドユーザ視点の対策としては、不審なウィンドウに表示された手順を安易に実行せず、正規のサイトであるかを確認すること、動画サイトやSNSで紹介されるツールの正当性を必ず公式サイトで確認することが重要となります。

■参考PushSecurity
https://pushsecurity.com/blog/the-most-advanced-clickfix-yet/

セキュリティ検知状況

- おまかせサイバーみまもり専用BOXで検知したアラート数をNTT東日本が集計
- 集計期間：2024年12月～2025年11月

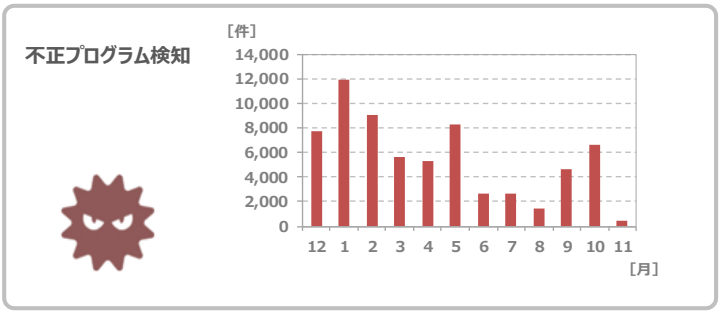
不正侵入検知



直近12カ月平均：2,066,316件
2025年11月：1,297,985件

直近12カ月の月平均に比べ低い検知状況が継続しています。
引き続きサーバ等を公開する際には十分にセキュリティ対策を実施してください。

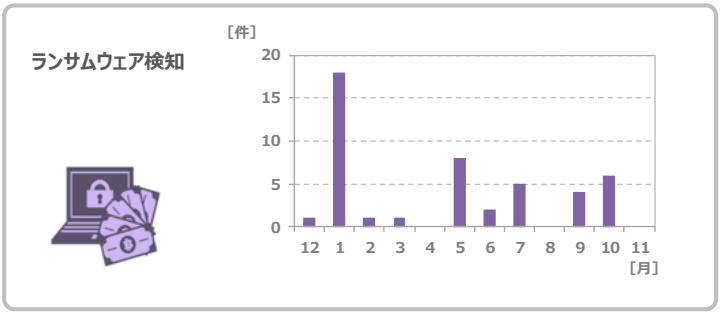
不正プログラム検知



直近12カ月平均：5,544件
2025年11月：392件

直近12カ月の月平均に比べ低い検知状況となっています。
インフォスティーラー(Infostealer)※1などの不正プログラムについては、引き続き十分に注意してください。

ランサムウェア検知



直近12カ月平均：4件
2025年11月：0件

11月は検知数が0件となり、直近12カ月の月平均に比べ低い検知状況となっています。
ランサムウェアには、引き続き十分に注意してください。

※1：感染した端末から機密情報を密かに盗み出すことを目的としたマルウェア(不正プログラム)の一種。
パスワード、クレジットカード情報、内部ファイルなど、あらゆる情報を盗み取るために設計されたマルウェアのこと。