おまかせサイバーみまもり

2026年1月　セキュリティ対応状況と検知状況

2026年2月
NTT東日本株式会社

セキュリティ対応状況

Varonis Threat Labsより、Microsoft Copilot Personal(個人向け) における新しい攻撃手法「Reprompt」に関する報告がされています。Repromptは、利用者が正規のMicrosoft Copilotのリンクをクリックするだけで、攻撃者が利用者のセッションを乗っ取り、機密データを外部へ送信させる攻撃手法です。Microsoftは既にこの問題を修正しております。また、この攻撃手法は個人向けのMicrosoft Copilot Personalにて発見された手法であり、企業向けのMicrosoft 365 Copilotを利用している場合には影響がないとのことです。

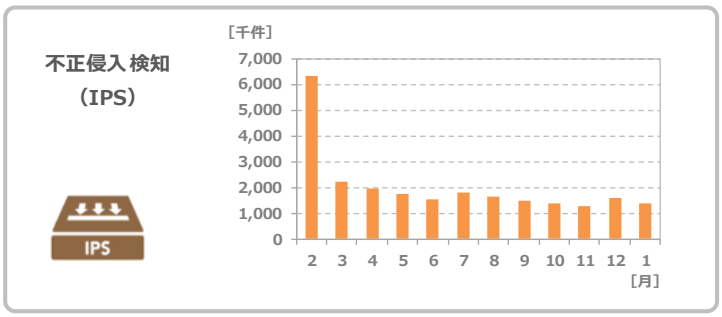
エンドユーザ視点の対策としては、AIツール利用時であっても信頼できる情報源以外のリンクをクリックしないこと、入力されているプロンプトを必ず確認すること、AIツールが個人情報や業務情報を求めたり意図しない動作を示した場合はその時点で利用を中断することが重要です。

■参考Varonis Threat Labs
https://www.varonis.com/blog/reprompt

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：2025年2月～2026年1月

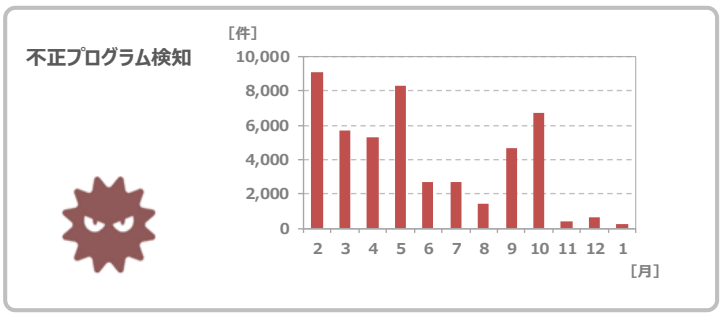
不正侵入検知



直近12カ月平均：2,039,378件
2026年1月：1,386,396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。

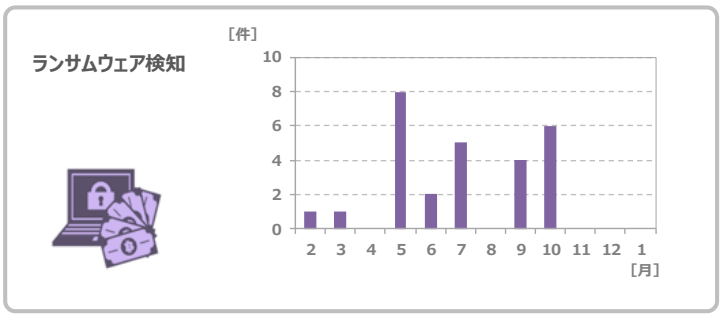
不正プログラム検知



直近12カ月平均：3,973件
2026年1月：　229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：2件
2026年1月：0件

1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。