



# 2023年6月 セキュリティ対応状況と検知状況

2023年7月  
東日本電信電話株式会社

## セキュリティ対応状況

2023年6月12日（現地時間）に、Fortinet社から「FortiOSおよびFortiProxyのSSL VPNにおけるヒープベースのバッファオーバーフローの脆弱性（CVE-2023-27997）」が公表されております。Fortinet社は本脆弱性の重要度を「クリティカル」と位置付けており、既に悪用の事実も確認されていることから当該製品を利用中でSSL-VPN機能を有効化している場合には脆弱性に対処したバージョンへのアップグレードが推奨されています。

本脆弱性が悪用された場合、認証されていない遠隔の第三者が細工したリクエストを送信し、任意のコードやコマンドを実行する可能性があります。

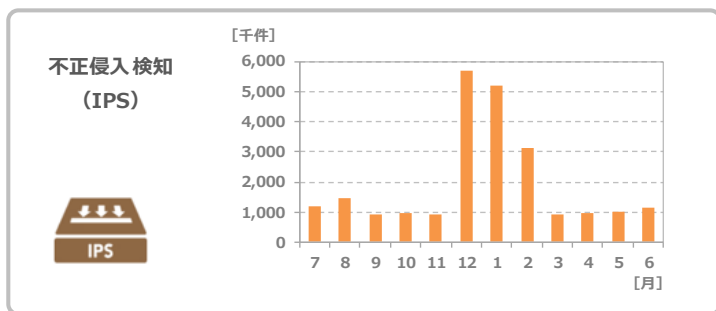
### ■参考

<https://www.fortiguard.com/psirt/FG-IR-23-097>

## 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：2022年7月～2023年6月

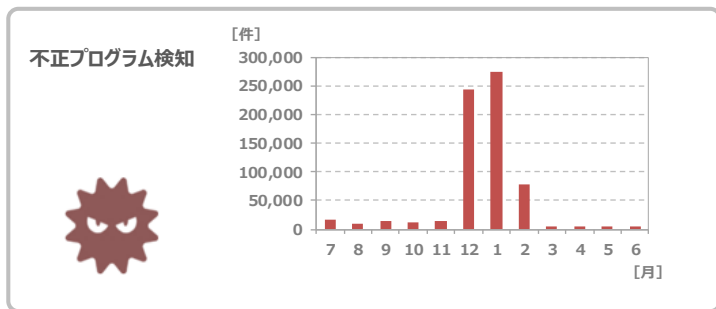
### 不正侵入検知



直近12カ月平均：1,956,230件  
2023年6月：1,128,509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。

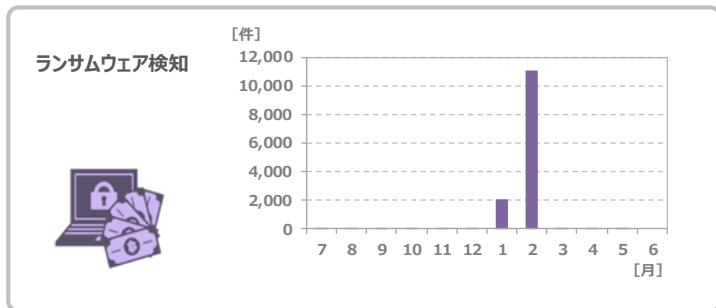
### 不正プログラム検知



直近12カ月平均：56,524件  
2023年6月：5,449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Emotet等の不正プログラムには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：1,105件  
2023年6月：0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。引き続きランサムウェアには十分に注意してください。