

サイバーセキュリティ岐阜

令和7年 6月発行
第103号

岐阜県警察本部
サイバー犯罪対策課
058-271-2424

Fortinet社製通信機器を狙った攻撃が発生しています！

脆弱性情報が発表されています！

- Fortinet社製の一部通信機器で脆弱性情報が発表されています。
- 通信機器への認証を通り越し、外部からネットワークに侵入される恐れがあります。
- この問題の深刻度は、「緊急」です。

- CVE-2024-55591

- CVE-2025-24472

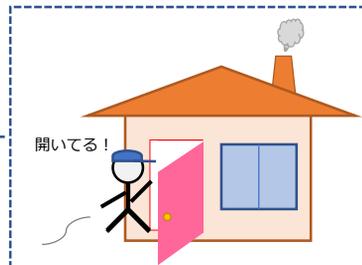
- CVE-2025-22252

※詳細は以下ページをご覧ください。

<https://fortiguard.com/psirt/FG-IR-24-535>

<https://fortiguard.com/psirt/FG-IR-24-472>

- ⇒ 対象のFortinet社製通信機器を利用されている場合、**FortiOSのバージョンアップを実施してください！！**



※イメージ

Windowsサーバを対象とした攻撃に注意

- 通信機器の認証を通り越してネットワークに侵入された後、WMIC※と呼ばれるWindowsの付属ツールを悪用し、ネットワーク内にWindowsサーバがないかどうかを探されます。
- ※ Windows Management Instrumentation Command line utility
- サーバ内のファイルを抜かれた後、「SuperBlack」と呼ばれるランサムウェアを組み込まれます。
- 「SuperBlack」は、サーバ内のデータを窃取し、暗号化の上、金銭の支払いを要求します。
- 対策として、EDR製品（セキュリティソフト）の導入もご検討ください。
- ⇒ コンピュータの異常な挙動を検知し、被害を抑えられる可能性があります。

転ばぬ先の杖、改めて基本的な対策を！

いつ、誰が、サイバー攻撃の被害に遭うかわかりません。

そのため日頃から…

- Windows等、OSのアップデートを定期的に行う
- ランサムウェア感染に備え、ファイルのバックアップを定期的に行う
- 不審なメールを開いたり、ファイルを開かない（実行しない）
- 通信機器やサーバの、ログ設定を適切に行う（保存期間、ログへの記載内容）



⇒Fortinet社製の通信機器を使っていなくても同様です！！

御面倒でも、転ばぬ先の杖と思い、不断の対策をお願いいたします。

明日は我が身

大丈夫かな？と思ったら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口



<https://www.npa.go.jp/bureau/cyber/soudan.html>



- X (旧Twitter) -
『岐阜県警察サイバー
セキュリティ情報』



- Instagram -
『岐阜県警察サイバー
セキュリティ情報』



岐阜県警察