

- 06月15日：「FortiOS」に判明したゼロデイ脆弱性で米政府が注意喚起
- 06月15日：「Chrome」にセキュリティアップデート - 深刻な脆弱性へ対処
- 06月14日：総務省かたるフィッシング - 固定資産税の納付通知を偽装
- 06月13日：Fortinetの「SSL VPN」に深刻な脆弱性 - アップデートの実施を
- 06月12日：自動車保険料の請求に見せかけたフィッシング
- 06月12日：情報サービス業グループ子会社でランサム被害 - サービスは再開へ
- 06月12日：「水道料金滞納」「給水停止」と不安煽る水道局装うSMS
- 06月09日：会計システムなど複数システムでランサム被害 - その他製造業（文房具・オフィス家具）
- 06月09日：杉並区の学童クラブ委託先でランサム被害 - バックアップも
- 06月09日：ランサムウェア「CI0p」、「MOVEit Transfer」にゼロデイ攻撃を展開
- 06月08日：シスコのビデオ会議サーバに脆弱性 - 重要度「クリティカル」も
- 06月06日：複数サーバがランサム被害、影響など調査中 - 医薬品業
- 06月05日：「じゃらん」を装うフィッシング - 「旅行支援金」口実に誘導
- 06月02日：WP向け人気プラグイン「Jetpack」に深刻な脆弱性 - 早急に更新を
- 06月01日：重要インフラ狙う中国関与の「Volt Typhoon」攻撃 - 中小企業も攻撃の踏み台

被害報告相次ぐ！



ランサムウェアの

フィッシング報告件数

1月	38,269件
2月	59,044件
3月	77,056件
4月	92,932件
5月	113,789件

今年1月から

3倍

## フィッシング詐欺の報告件数増加

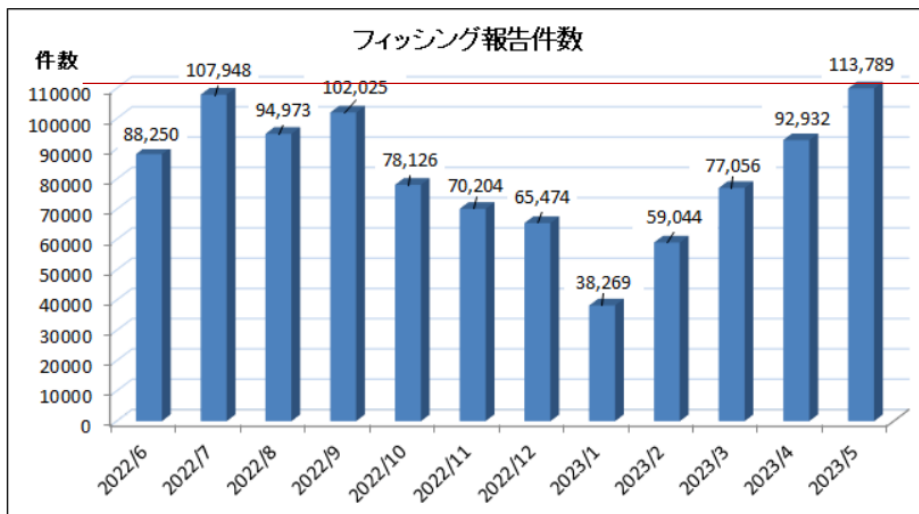
PICKUP!

※出典：2023年6月6日フィッシング対策協議会 Council of Anti-Phishing Japan | 報告書類 | 月次報告書 | 2023/05 フィッシング報告状況 <https://www.antiphishing.jp/report/monthly/202305.html>  
 出展：2023年6月12日 マイナビニュース <https://news.mynavi.jp/techplus/article/20230612-2699058/>



## 5月のフィッシング、報告件数が過去最高記録 ファミペイの悪用が最多【フィッシング対策調べ】

2023年5月のフィッシングの報告件数は11万3,789件で、2023年4月と比較して2万857件増加している。



過去最多

- 出典：2023年6月7日 中国支援のAPTグループによるインフラへのサイバー攻撃、今後も継続見込み チェックポイントが発表  
<https://enterprisezine.jp/news/detail/17861>
- 出展：2023年6月7日 PRTIMES <https://prtimes.jp/main/html/rd/p/000000213.000021207.html>



## 中国支援のハッカー集団によるインフラへのサイバー攻撃 同種の攻撃が今後も継続すると警告

2023年6月7日、チェック・ポイントの脅威インテリジェンス部門であるチェック・ポイント・リサーチ（以下、CPR）は、Microsoftが今年5月に発表した、中国が支援するハッカー集団が世界各国でサイバーインフラを侵害しているとの警告を受けて、同種の攻撃が今後も継続されるとの予測を発表した。

### 攻撃の手法

Volt Typhoonが、ルーターなどのネットワーク機器の脆弱性を悪用する手法があります。

### エッジデバイスが攻撃対象となる理由

ルーターは、ネットワークトラフィックを**正当なものから悪意のあるものまで**管理する役割を担っています。

これらのデバイスを侵害することで、攻撃者は自分たちのトラフィックを正規の通信に紛れ込ませることができ、検出は著しく困難になります。また、これらのデバイスを再設定または侵害することにより、攻撃者はネットワークを通じて通信のトンネル化が可能になり、トラフィックの効果的な匿名化と、従来の検出方法による回避が可能になります。



スパイ攻撃の対象は  
米国だけではない!

## ネットワークを保護するために



基本が大切です!

- ソフトウェアのアップデート
- 最新パッチの適用
- デフォルトの認証情報を変更する
- 防止優先のセキュリティを用いる

### チェックポイント社の防止優先のネットワーク・セキュリティ・ソリューション

チェック・ポイントのネットワーク・セキュリティ・ソリューションは、Camaro Dragon※ APTグループが使用する攻撃手法に対して、高度な脅威防御とリアルタイムのネットワーク保護機能を提供します。