LATEST & PICKUP! SECURITY NEWS

Fuva Brain
Vol.58

最新個人情報漏えい事件・関連ニュース LATEST

DATE：2023.09.26

サイバーセキュリティ.com　SecurityNEXT、jiji.com、Yahoo!NEWS

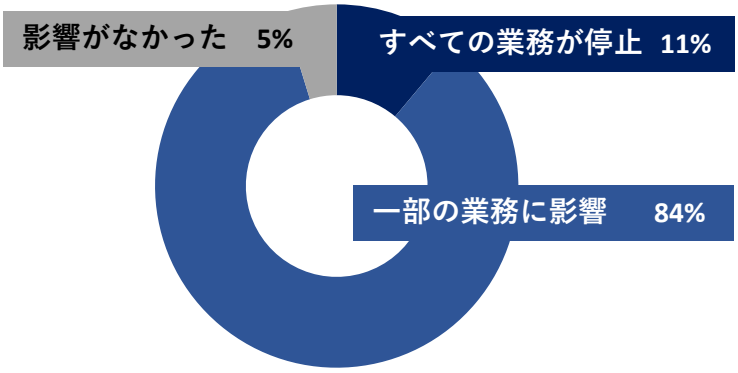
- 9月22日:　**「iPhone」や「iPad」に3件のゼロデイ脆弱性 - アップデートを公開**
- 9月20日:　**米当局、脆弱性の悪用について警戒呼びかけ - 1週間で13件**
- 9月19日:　**トレンドの法人向けセキュリティ製品に脆弱性 - すでに悪用済み**
- 9月19日:　**QNAP製NASに複数の脆弱性 - 修正版以降へ更新を**
- 9月19日:　**サーバに不正アクセス、個人情報10万件超が流出の可能性 - マツダ**
- 9月15日:　**北米法人で情報流出を確認、ランサム影響か - アルプスアルパイン**
- 9月15日:　**Palo Alto Networksの「PAN-OS」や「Cortex XDR」に脆弱性**
- 9月15日:　「Splunk Enterprise」に複数の脆弱性 - アップデートで修正
- 9月14日:　Array Networks製VPN機器、標的型攻撃の対象に - 侵害状況の確認を
- 9月14日:　**Fortinet、「FortiOS」など複数製品の脆弱性を修正**
- 9月14日:　**ビデオ会議サービス「Zoom」のクライアントなどに脆弱性**
- 9月13日:　一部サーバにランサム攻撃、生産や出荷に影響 - アルプスアルパイン
- 9月13日:　**Ciscoセキュリティ製品のVPN機能にゼロデイ脆弱性 - ランサムの標的に**
- 9月13日:　「Adobe Acrobat/Reader」にゼロデイ脆弱性 - 早急にアップデートを
- 9月13日:　MS、9月の月例パッチを公開 - ゼロデイ脆弱性にも対応
- 9月12日:　**「iOS 15」や旧世代macOSにアップデート - ゼロデイ脆弱性対応で**
- 9月07日:　「Citrix ADC」への攻撃、 米当局があらたな手口を公開
- 9月07日:　**「Apache RocketMQ」**に対する攻撃が発生 - 米当局が注意喚起
- 9月06日:　「Chrome」にセキュリティアップデート - 脆弱性4件を修正

サイバー攻撃「ランサムウェア」被害企業の9割 “業務に影響”　警察庁調べ PICKUP!

※出典：警察庁サイバー空間をめぐる脅威の情勢等
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

企業・団体等におけるランサムウェア被害及びその実態

ランサムウェア被害が業務に与えた影響



被害企業の95%は業務に影響…
ランサムウェアに新たな手口を確認

9月21日、警察庁は、「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」を発表しました。

データを勝手に暗号化して、身代金を要求する「ランサムウェア」と呼ばれるサイバー攻撃の被害が、ことしも全国で相次いでいて、**被害に遭った企業などのうち9割以上で業務への影響が出ていた**ことが警察庁の調べで分かりました。**新たな手口も確認されていて、警察庁は、セキュリティの強化を呼びかけ**ています。

PICKUP!

暗号化しないまま金銭要求、新たなランサム「ノーウェアランサム」の脅威

※出典：警察庁サイバー空間をめぐる脅威の情勢等
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

暗号化しないまま情報を盗み出し、金銭要求！
新たなランサム「ノーウェアランサム」の脅威

警察庁が新たに「ノーウェアランサム」と名付けた攻撃は、**暗号化をしないまま情報を盗み出し、金銭を要求する手口とのこと**です。システムに侵入してデータを盗み、「公開する」と脅して金品を要求する新型のサイバー攻撃が今年上半期（１～６月）に国内で６件確認されました。身代金要求型ウイルス「ランサムウェア」と異なり、**データを暗号化しないのが特徴で、警察庁が警戒を強めて**います。

ランサムウェア「ノーウェアランサム」とは

攻撃者にとって効率的な攻撃

図：ノーウェアランサム

ノーウェアランサム攻撃は、暗号化が生じず通常より脅威度の低い攻撃に見えます。しかし、攻撃者の視点では余分な処理が生じず手軽であるうえ、情報を人質にした脅迫は可能であり、個人情報や機密情報を人質にした要求行為は可能です。

【図表２：攻撃の流れ（左：ランサムウェア攻撃、右：ノーウェアランサム攻撃）】

出典：警察庁資料　警察庁サイバー空間をめぐる脅威の情勢等　トピック3「ノーウェアランサム」引用

ランサムウェアの主な感染経路は、
VPNや**リモートデスクトップ**であり、
改めてセキュリティの見直しを！