ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●大物ランサムウェア「Lockbit」摘発、警察庁は暗号化データの復号ツールリリース…一週間で活動再開か

https://www.itmedia.co.jp/news/articles/2402/21/news125.html
https://www.jiji.com/jc/article?k=2024022001027
https://www.tokyo-np.co.jp/article/311753

### このニュースをザックリ言うと･･･

- 2月21日(日本時間)、警察庁(関東管区警察局サイバー特別捜査隊)より、欧州Europol・米FBI・英NCAといった各国警察機構との連携により、ランサムウェア「LockBit」のテイクダウンを行ったと発表されました。

- LockBitを利用していた犯罪者グループのメンバー2名を逮捕、ダークウェブ上のリークサイト(LockBitに感染した被害者や奪取した機密情報を掲載するWebサイト)を閉鎖したとしています。

- 併せて同庁からは、LockBitで暗号化されたデータを復号するツールを開発し、12月にEuropolに提供していたことが発表されており、国内の被害企業等に対し最寄りの警察署へ相談するよう呼び掛けるとともに、求めに応じツールを用いた被害回復作業を行うとしています。

### AUS便りからの所感等

- 復号ツールは9割以上のデータの復元に成功する等一定の効果を見せているとされ、過去にLockBitに感染した各組織においては安易に身代金を支払わずツールの提供を受けるべきでしょう。

- 一方で、テイクダウンから一週間後の2月27日にはLockBit側がリークサイトを復活させ、早くも活動を再開させているとみられ、今後の新たな被害発生の可能性についてはまだ安心はできない状況です。

- 相手が開発するであろう新たなLockBitはこれまでと異なるデータ暗号化機構を持つ可能性が高く、その場合には復号ツールの対応にもある程度のタイムラグが発生するとみられ、各組織では今後のランサムウェア攻撃について引き続き注意を払い、各種データバックアップ(およびバックアップデータ自体の保全と復元復旧体制の確立)の実施を心掛けてください。

ITmedia NEWS

**名古屋港攻撃のランサムウェア集団「LockBit」、主要インフラ無力化　ユーロポールが主導　警察庁も復号ツール開発などで協力**

2024年02月21日 14時47分 公開　[ITmedia]

欧州刑事警察機構（ユーロポール）は2月20日（現地時間）、名古屋港への攻撃などで知られるランサムウェア集団「LockBit」のインフラを無効化し、関係者2人を逮捕したと発表した。

LockBitは世界各国で企業や病院などを恐喝して身代金を脅し取っているランサムウェア集団。日本では、2023年に名古屋港で貨物や設備の管理に使う基盤システムが被害に遭い、話題になった。ユーロポールによれば、世界での被害額は数十億ユーロに上るという。

捜査はユーロポールが主導し、フランス、ドイツ、日本、カナダ、米国、英国など10カ国の警察組織などが協力した。すでに「LockBitの主要なプラットフォームや犯罪につながるインフラを停止した」（ユーロポール）といい、オランダやドイツ、スイス、米国にあった34のサーバを停止したとしている。

## ●病院に不正アクセス、ランサムウェア感染…認証無しでリモートデスクトップ接続が可能

https://373news.com/_news/storyid/191272/
https://kokubu-seikyo.jp/category/pickup/

### このニュースをザックリ言うと・・・

- 3月4日(日本時間)、鹿児島県霧島市の国分生協病院より、同病院のシステムがランサムウェアに感染したと発表されました。
- 2月27日に深夜に電子カルテシステムの画像管理サーバーに感染、PDFデータの一部が暗号化されたことが確認されたとしています。
- 電子カルテ・会計システムは発表時点で復旧しているものの、救急・一般外来の受入について制限を行っているとしています。

### AUS便りからの所感

- 発表では、ランサムウェアに侵入された原因として、保守のためのネットワーク機器に、外部から認証なしで病院内のコンピュータにリモートデスクトップ接続が可能な設定があったこと、画像管理サーバーにアンチウイルスソフトが導入されていなかったことが挙げられています。
- システムへのリモートアクセスとそれを経由してのリモートデスクトップへのアクセスで二度認証の手間がかかるとしても、片方を認証なしにするのは、社内LANや、ふとしたタイミングで外部からの攻撃に無防備となる恐れがあります。
- 各ポイントでの認証設定は確実に行い、公開鍵認証等強固な認証を用いる、パスワードの場合は決して推測可能なものは使わない、そしてくれぐれもリモートデスクトップサービス(WindowsであればTCP/UDPポート3389番)は外部から直接アクセス可能な状態としない(可能であれば社内LANからもアクセス元を制限する)ことが重要です。


南日本新聞

国分生協病院が「ランサムウエア」サイバー攻撃受ける　一部診療を制限

2024/03/04 20:55

鹿児島県霧島市の国分生協病院は４日、身代金要求型コンピューターウイルス「ランサムウエア」によるサイバー攻撃を受けたと発表した。現在、救急や一般外来の受け入れを制限している。

厚生労働省によると、県内医療機関へのランサムウエア攻撃は、確認できた２０２１年度以降初めて。

同院によると、画像管理サーバーの一部データが暗号化された。個人情報の流出は、現時点で確認されていない。紙カルテを運用し、予約外来や入院患者は対応している。



拡大

## ●2月はWordPressの29のプラグインに脆弱性…Sucuri社発表

https://news.mynavi.jp/techplus/article/20240305-2896341/
https://blog.sucuri.net/2024/02/wordpress-vulnerability-patch-roundup-february-2024.html

### このニュースをザックリ言うと・・・

- 2月29日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、2月に報告された27のWordPressプラグインに存在する29件の脆弱性のまとめ記事が発表されました。
- 今回発表分で最も危険度が高い「High」は6件で、クロスサイトスクリプティング(XSS)が3件の他、トラバーサル系2件、サービス拒否1件となっています。
- また、XSSの脆弱性については29件のうち実に25件を占めています。

### AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、1月分で28件、2023年12月分で23件と、多数の報告がまとめられています(ただし別の情報源ではここでまとめられていない脆弱性も報告されており、調査の際は複数の情報源をあたることが重要です)。
- WordPress本体においても1月にセキュリティアップデート6.4.3がリリースされるなど、不定期に更新されることがあり、本体・プラグインともインストールした状態のままで放置するようなことは決してせず最新に保つよう努めること、加えてセキュリティを強化する何らかのプラグインを導入し、さらに並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入についても検討するのが良いでしょう。


TECHブログ Powered by ワイヤレスニュース

2月のWordPressプラグイン脆弱性まとめ、確認と対応を

掲載日 2024/03/05 07:31　　著者：後藤大地

Sucuriは2月29日(米国時間)、「WordPress Vulnerability & Patch Roundup February 2024」において、2024年2月に明らかになったWordPressの脆弱性およびセキュリティパッチの情報について伝えた。SucuriはWebサイト所有者に対して新たな脅威を把握して対処してもらえるよう、1カ月間のWordPressエコシステムの重要なセキュリティアップデートと脆弱性パッチの一覧をまとめて公表している。