

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。

●新聞社サーバーがランサムウェア感染…紙面ページ数縮小の事態

<https://xtech.nikkei.com/atcl/nxt/news/18/16480/>
<http://www.nagano-np.co.jp/articles/119535>



このニュースをザックリ言うと…

- 12月21日(現地時間)、長野県の地方新聞「長野日報」を発行する長野日报社より、同社の社内サーバーがランサムウェアに感染したと発表されました。
- 同19日23時過ぎにサーバーと組版用端末において感染が確認され、製作に影響が出たとしており、発表が掲載された21日発行分の紙面は通常の16ページから8ページに縮小した特別紙面となっています。
- 被害を受けたサーバーは公開を前提として紙面に使用する記事と写真データが蓄積されていたもので、個人情報の流出はなく、ホームページやメールシステムは通常通り稼働しているとのこと。

AUS便りからの所感等

- 22日には同社ホームページにもお詫びが掲載され、同日発行分も引き続き特別紙面になるとしており、またこの時点では被害の長期化も予想されるとしています。
- 警察庁の発表では2022年に過去最大の230件のランサムウェア被害、また2023年も上半期に103件の被害が報告されており、7月には名古屋港のコンテナターミナル管理システムが「LockBit」に感染して搬出入作業に影響が出る(AUS便り 2023/07/11号参照)等、依然猛威を奮っています。
- ランサムウェアへの対策において重要なのは、クライアント・サーバー共に感染しないこと以上に、感染が発生した場合のシステム・データの保護、およびバックアップから確実に復旧できる体制を整えることであり、バックアップデータをも暗号化されて復旧に使用できなくなる事態とならないよう、「複数コピーをとる」「オンラインから隔離された場所あるいは書き換え不可能なストレージ(サービス)に保管する」「バックアップとリストアが確実に実行できるようテスト」ことが推奨されています(同2021/09/14号参照)。

日経 XTECH

長野日报社がランサムウェア被害、ページ数半減など新聞製作に影響

永田 雄大 日経クロステック/日経コンピュータ

2023.12.21

長野日报社は2023年12月21日、ランサムウェアに感染したと発表した。被害を受けたのは新聞製作のためのメインサーバー。この影響により、同社は同日付の朝刊を通常の16ページから8ページに半減する特別紙面を発行した。

社会

おわび (サーバーダウンによる特別紙面)

社会 © 2023年12月21日 08時00分

いいね! 文庫ポスト Pocket

弊社のサーバーが悪意のあるコンピューターウイルス(ランサムウェア)に感染し、新聞製作に影響を及ぼしています。このため、21日付本紙は特別紙面体制として発行します。

12月19日深夜に、弊社サーバーが身代金要求型ウイルス(ランサムウェア)による被害が発生していることを確認しました。今回の被害に対応するため、ネットワークからサーバーを切り離しています。当社のホームページやメールシステムは通常通り稼働しています。

現在、外部専門家や警察と連携の上、システムの保護と復旧に向けて作業を進めています。長期化も予想されます。読者や広告クライアントの皆様等関係者には多大なるご迷惑をおかけすることをおわび申し上げます。

長野日报社

長野日报社はランサムウェア感染の影響で、2023年12月21日付の朝刊が特別紙面になったことをおわびした

(出所:長野日报社のホームページを日経クロステックがキャプチャー)

[画像のクリックで拡大表示]

同社が被害を確認したのは2023年12月19日午後11時過ぎのこと。被害の規模は調査中だ。長野日报社の宮坂康弘専務取締役編集局長によれば、「新聞製作のメインサーバーと紙面を作るための組み版端末がランサムウェアに感染した」。現在は緊急用の端末で対応している。



● SSHプロトコルに脆弱性、サーバー側およびクライアント側のアップデートを

<https://gigazine.net/news/20231220-terrapin-attack/>
<https://terrapin-attack.com/>

このニュースをザックリ言うと…

- 12月18日(現地時間)、ドイツの大学のセキュリティ研究者より、**SSH(セキュアシェル)プロトコルに存在する脆弱性(CVE-2023-48795他)を突く攻撃「Terrapin Attack」**が発表されました。
- SSH通信時に**特定の暗号化形式**もしくは**特定のMAC(メッセージ認証符号)**を使用している場合、いわゆる「**中間者攻撃**」により、**攻撃者が安全な通信を妨害することが可能**としています。
- SSHの最もメジャーな実装である**OpenSSH**には**9.5までのバージョンに脆弱性が存在**するとし、対策等を行った**最新バージョン9.6をリリース**している他、PuTTYやTeraTerm等**SSHに対応した各種ターミナルソフト**でも**対策が進んでいます**。

AUS便りからの所感



- 攻撃はSSHポートが開いているサーバーに対し**直接実行できる類のものではなく**、**SSH通信を途中のルーター等で傍受できる場合に可能**となるものです。
- 脆弱性が発生する条件は、暗号化形式として**ChaCha20-Poly1305**、あるいはMACとして**Encrypt-then-mac(eth)**に対応するものを利用していること、とされていますが、**OpenSSHのデフォルトの設定**(サーバー・クライアント共)ではこれら(MACについては「eth@openssh.com」という文字列を含むもの)を**優先して使用**するため、**影響範囲は比較的広い**とみられます。
- **Terrapin Attackに関する公式サイト**では、SSHサーバーやクライアントに**脆弱性が存在するか検証可能なツール**も提供されています。
- ともあれ、Linuxサーバー等への**安全な接続・ログインに欠かせないSSHに****影響する脆弱性**であり、**サーバー側はもちろんクライアント側でもセキュリティアップデートを確実に適用**することが重要です。

2023年12月20日 13時00分 セキュリティ

SSH接続後の中間者攻撃を可能にするエクスプロイト「Terrapin Attack」が発見される

セキュリティで保護されていないネットワークを通じてコンピューターに安全にコマンドを送信する「Secure Shell(SSH)」プロトコルにおいてハンドシェイクプロセス中にシーケンス番号を操作してSSHプロトコルの整合性を破る「Terrapin Attack」という攻撃が発見されました。この操作で、攻撃者は通信チャネルを通じて交換されるメッセージを削除あるいは変更できるように、さまざまな攻撃が可能になります。

● 年末年始における情報セキュリティの注意喚起、IPAより発表

<https://www.ipa.go.jp/security/anshin/heads-up/alert20231221.html>



このニュースをザックリ言うと…

- 12月21日(日本時間)、**IPAより、年末年始を迎えるにあたっての、情報セキュリティに関する注意喚起**が発表されました。
- 多くの企業・組織において、この時期に従業員等が**長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得る**ことを鑑み、「**組織のシステム管理者**」「**組織の利用者**」「**家庭の利用者**」それぞれを対象に、「**休暇前**」「**休暇中**」「**休暇明け**」に行うべき基本的な対策と心得が「**長期休暇における情報セキュリティ対策**」においてまとめられています。
- IPAは毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っています(<https://www.ipa.go.jp/security/measures/vacation.html>)。

AUS便りからの所感



- 注意喚起の内容は、システム管理者が**長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気づきにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性**まで、多様なものとなっています。
- 挙げられているセキュリティ対策の内容は**毎回大きく異なるようなものではなく**、この他にも**長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策**(<https://www.ipa.go.jp/security/measures/everyday.html>)」として別途まとめており、**平日頃において準備・点検を行うよう意識**していくことが肝要です。

2023年度 年末年始における情報セキュリティに関する注意喚起

公開日：2023年12月21日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人が年末年始の長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応が遅れたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生したり、長期休暇後の業務継続に影響が及ぶ可能性があります。

このような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、のそれぞれを対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

[長期休暇における情報セキュリティ対策](#)
[日常における情報セキュリティ対策](#)

※上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。

- (1)個人の利用者：個人向けの対策 (3.)
- (2)企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策 (2-2./3.)
- (3)企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策 (2-1./2-2./3.)

被害に遭わないためにもこれらの対策の実施をお願いします。

被害に遭わないためにもこれらの対策の実施をお願いします。