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。

●宇陀市立病院がランサムウエア被害、1,133人分のデータが暗号化

https://www.nikkei.com/article/DGXMZO36900170V21C18A0000000/
http://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/press-release.html

このニュースをザックリ言うと･･･

- 10月23日（日本時間）、奈良県宇陀市(うだし)より、同市立病院の電子カルテシステムがランサムウェア「GandCrab(ガンクラブ)」に感染したと発表されました。
- 国内の病院がランサムウェアの被害を受けたと公表されたのは、今回が初めての事例とされています。
- 電子カルテシステムは10月1日に導入されたばかりで、同15日までに来院した3,835人の診療記録のうち、1,133人分のデータがランサムウェアに暗号化されたとのことです。
- 発表の時点で暗号化されたデータは復元できておらず、セキュリティ企業に復元を依頼しているとのことです。

AUS便りからの所感等

- GandCrabは2018年に入ってから活動が確認されているランサムウェアで、当初はFlash Playerの古いバージョンに存在する脆弱性を突いて感染するとされていました（「AUS便り2018/06/04号」参照）が、その後様々な感染手段を持つようになった模様です。
- 感染が発覚したのは同16日の早朝で、感染したサーバを物理的にネットワークから切り離した（コンピュータのLANケーブルを抜く）ことにより、一部を除くクライアントPCへの大規模な感染は防がれたとみられます。
- 一方で、データの定期的なバックアップのための磁気テープがセットされていなかったためにバックアップができていなかったとのことです。
- ランサムウェアは今年も依然として脅威であり、OSやアプリケーションを最新に保つこと、アンチウイルスやUTMによる防御を行うことに加え、万が一の感染時に備え、確実なデータバックアップ（およびバックアップからの復元）ができる態勢を整えておくことが重要です。

日本経済新聞

宇陀市立病院がランサムウエア被害、身代金は支払わず

科学&新技術 BP速報

2018/10/25 15:00

保存 共有 印刷 その他

日経XTECH 日経クロステック

奈良県の宇陀市立病院は2018年10月23日、10月1日に導入した電子カルテシステムがランサムウエアに感染したと発表した。セキュリティーリサーチャーのpiyokango氏によれば、国内の病院では
う。

ランサムウエアに感染
パソコン。サーバーに
れ、ランサムウエアに
「感染に気付いたのが
る」という。またクラ
ため、感染を免れたと

電子カルテシステムに
ていたが、システム会
クアップが取られてい
は現状復元できていな
金銭を支払わずに、感
タの復元を依頼してい

■ランサムウエアはGandCrab

ランサムウエアの感染は、職員が10月16日午前5時40分ごろに電子カルテシステムを使用できなかったことで発覚。システム会社がサーバーを確認し、ランサムウエア感染を示す画面が表示されていたため、サーバーを物理的にネットワークから切り離し、システムを停止させたという。

感染したランサムウエアは、「GandCrab（ガンクラブ）」。piyokango氏は、「GandCrabは2018年に入って存在が確認されたランサムウエア。たびたび機能が拡張され、様々なバージョンがある。WindowsやAdobe Flash Playerの脆弱性を利用するタイプから、メールで配布するタイプ、ウェブサイトを改ざんしてシステムツールに偽装するタイプなど、複数の手口がこれまで報告されている」という。なお、同病院での感染経路は特定できていない。

同病院では、感染したサーバーとパソコンのランサムウエアを削除し、再セットアップ。ウイルス対策ソフトを最新の状態にして、電子カルテシステムを10月18日までに復旧させたという。復旧までの間は、9月30日まで使っていた紙のカルテを使って診療を続けたとしている。感染原因の一つとして、ウイルス対策ソフトが最新ではなかった点を挙げている。

宇陀市立病院 UDA CITY HOSPITAL

報道発表資料

平成 30 年 10 月 23 日　16 時
宇陀市長　高見　省次

電子カルテシステムの障害発生について

2018 年 10 月 16 日（火）午前 5 時 40 分頃、ウイルス感染により電子カルテシステムが使用できない状況となりました。10 月 18
者情報が参照できない状況にあります。患
とを深くお詫び申し上げます。
なお、現時点では、患者様の個人情報の
これまでの状況については、下記のとお

1）発生状況
10 月 1 日に導入した電子カルテシ
10 月 16 日（火）午前 5 時 40 分頃、
気付き、すぐにシステム会社に連絡。
システム会社の担当者が、サーバー画
事を確認したため、システム全面停止
タの LAN ケーブルを抜く）を行う。

2）直後の対応
・システム会社には、早期データの復旧
での究明を指示するとともに、専門機
・システム会社による対応として、サー
去し、再セットアップの完了。各部門
イルスの除去作業を完了し、安全確認
ス対策ソフトをインストールした。
運用が確認できたことから１８日（
関した。

5）経緯
2018 年 10 月 16 日（火）
午前 5 時 40 分頃　職員が電子カルテシステムを使用出来ない状況であったので、システム会社に連絡。
午前 8 時頃　システム会社の担当者が、サーバー画面にウイルス感染を示すメッセージが表示されたため、システム全面停止、ネットワークからの物理的遮断（コンピュータの LAN ケーブルを抜く）を行う。復旧作業に時間を要するため、紙カルテ及び臨業運用による診療を決定する。
午後 5 時　復旧見込みが約 2 日間を要し、また復旧に必要なバックアップデータが、システム会社の不備により、存在しないことが判明
2018 年 10 月 17 日（水）
院内は紙カルテ及び臨業運用による診療を継続する。
システム会社に対し、ウイルス感染についての専門機関への調査依頼を指示した。同日、専門機関が作業を開始し、「調査には 1 週間のシステム監視が必要である」との事。
2018 年 10 月 18 日（木）
午前 7 時　サーバ、クライアントパソコンを個別にウイルス除去し、再セットアップの完了。各部門システムのウイルス感染状況調査と感染したウイルスの除去作業を完了させ、安全確認を行うとともに再発防止のために最新のウイルス対策ソフトをインストールする。また、データバックアップ機能の強化により安全運用が確認できたことから電子カルテシステムの運用を再開した。
2018 年 10 月 23 日（火）
午後 2 時　専門機関からの中間報告によりますと、監視センサーにより通信を監視しているＬＡＮにおいては、情報漏洩及び感染拡大は発生していない。しかし、ウイルスにより暗号化されたデータの解読は、継続解析中。

●発信元はWindows Server 2003か…TCPポート445番へのアクセス急増

https://news.mynavi.jp/article/20181020-709589/

このニュースをザックリ言うと・・・

- 10月18日（日本時間）、JPCERT/CCより、2018年7～9月のインターネット定点観測レポートが発表されました。

- 国内で観測されたパケットの宛先ポートで最も多かったのはTCPポート23番(Telnet)、次いで445番(Windows関連サービス)と、前四半期(4～6月)と同様ですが、445番ポート宛パケットが8月12日以降急増していたとのことです。

- 445番ポート宛パケットの発信元ホストについて調査したところ、8割がWindows Server 2003が稼働していたとのことで、JPCERT/CCでは該当する発信元IPアドレスの管理者に連絡をとったところ、一部の管理者からアンチウイルスソフトでマルウェアが検出されたとの回答を得たとしています。

AUS便りからの所感等

- Windows Server 2003の一般的なサポートは2015年7月に終了しており、それ以降に確認された脆弱性を突いて445番ポートから感染したマルウェアがさらに感染を拡大しようと外部にパケットを送信していたと考えられます。

- JPCERT/CCも推奨していますが、脆弱性への対応が行われているOSへの移行をまず検討すべきであり、やむを得ない事情がある場合は、外部や他のクライアントPCがあるネットワークへの不正なパケットの送信を遮断するようUTM等により隔離することが重要です。

- 頻繁に狙われているポートとしては、前述したものの他に、8080番(管理用等のWebサービス)や22番(SSH)も挙げられ、これらのポートが不特定多数からアクセスされることを想定していないのであれば、ファイアウォール等によって特定IPアドレス以外からのアクセスを遮断する設定を行い、また不審なログイン等の活動についても可能な限り検知・遮断できる状態にしておくべきでしょう。


マイナビニュース

2018/10/20 18:26:27

8月12日からTCP 445番ポートへのアクセス増加 - JPCERT/CC

[表1：宛先ポート番号トップ5]

順位	宛先ポート番号	前四半期の順位
1	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	2
3	80/TCP(http)	3
4	8080/TCP	6
5	22/TCP (ssh)	4

※ ポート番号とサービスの対応の詳細は、IANAの文書[*1]を参照してください。なお、サービス名はIANAの情報をもとに記載していますが、必ずしも各サービスプロトコルに則ったパケットが観測されているとは限りません。

インターネット定点観測レポート(2018年 7～9月) 宛先ポート番号トップ5 - 資料: JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center、JPCERT/CC）提供

●件名「Amzon」など、Amazonを装うフィッシングメールが拡散中

https://internet.watch.impress.co.jp/docs/news/1149176.html

このニュースをザックリ言うと・・・

- 10月19日（日本時間）、フィッシング対策協議会より、Amazonをかたる複数のフィッシングメールが出回っているとして注意喚起が出されています。

- フィッシングメールは、件名が「お使いのAmazon IDがロックされます！」で始まるものや「Amzon - 親愛なるお客様，セキュリティリスクのため、お客様のアカウントは停止されています。」等で、リンク先は「amazno」「amazen」「amazom」「amzeon」といった文字列を含む、または「amazon-●●●●.cc」「amazon-japan-●●●●.com」といったドメインの偽サイトとなっています。

- 同協議会では、このようなフィッシングサイトにて、ログイン情報・クレジットカード情報あるいは個人情報を絶対に入力しないよう警告しています。

AUS便りからの所感等

- Amazonをかたるフィッシングは毎月のように確認され、そのたびにフィッシング対策協議会から注意喚起が出されています。

- 微妙にサービス名のつづりが異なったり、メールやサイトの文言・デザインがおかしかったりと、フィッシングと見分けられる要素はいくつもありますが、それでもいつ本物と見間違えるほどのフィッシングが現れても引っかからないよう、感覚を麻痺させることなく注意を払い対応することが重要です。

- メーラー・ブラウザ・セキュリティソフトおよびUTMのアンチスパム機能・アンチフィッシング機能を必ず有効にした上で、普段利用しているサービスへはメールのリンクからではなくブラウザに登録したブックマークからアクセスすることを推奨致します。


INTERNET Watch

件名「Amzon」など、Amazonを装うフィッシングメールが拡散中

誘導先のサイトのドメインは「amazno」「amazen」「amazom」「amzeon」など

磯谷 智仁　2018年10月22日 15:00

ツイート リスト いいね！309 シェア B! 22 Pocket 49

Amazonの偽サイトへ誘導してログイン情報などを詐取する、Amazonを装うフィッシングメールが拡散されているとして、フィッシング対策協議会が注意を促している。

フィッシングメール本文は、ユーザーのAmazonアカウントにセキュリティ上の問題があるとして利用を一時的に停止し、再開にはアカウント情報の確認が必要だと不安を煽る内容になっている。フィッシングメールはHTML形式で書かれており、表示されたURLと実際にアクセスするURLが異なるように偽装されているものも確認された。

誘導先の偽サイトのドメインは「amazno-●●●●.com」「amazon-●●●●.cc」「amazen-●●●●.bz」「amazom●●●●.jp」「amzeon-●●●●.com」「amazon-japan-●●●●.com」などがあった。