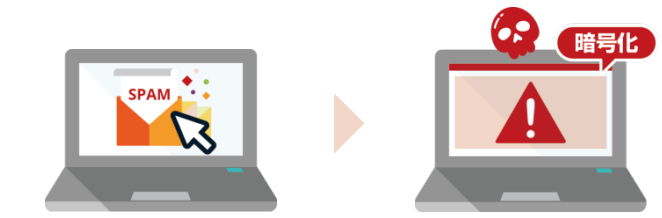
進化する明日へ Continue thinking
I-O DATA
2016年4月発行 vol.1

緊急！

身代金要求型不正プログラム ランサムウェア の問い合わせ急増中！

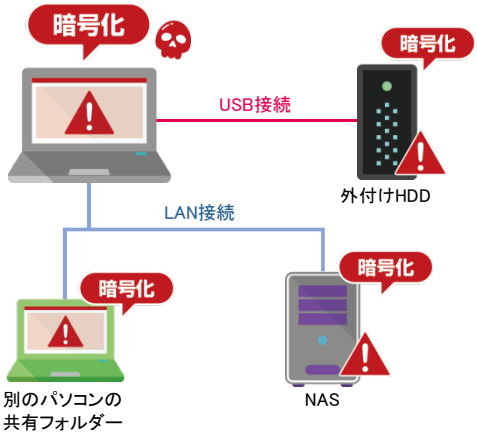
ランサムウェアはマルウェアの一種で、感染したパソコンやそのパソコンに接続したUSBハードディスク、同一ネットワーク上の共有フォルダー（NASやファイルサーバー）内のデータを暗号化など様々な方法で使用不能にし、その復帰と引き換えに「身代金（ramsom：ランサム）」を要求する不正プログラムです。感染経路はメール添付やウェブ閲覧など多岐に渡り、現在新種や亜種が数多く出回っているためウイルス対策ソフトでも完全に防ぐことはできません。Windowsの履歴管理機能であるボリュームシャドウコピーを破壊する（過去履歴に戻れなくする）などの活動を行う高度なタイプも確認されています。

ランサムウェア感染イメージ



メール添付のファイルやウイルスが仕込まれたサイトへのアクセス

パソコンがランサムウェアに感染し、オフィスファイル等が**暗号化される**



パソコンにUSB接続した外付けHDDや、同一ネットワーク上の**共有フォルダー内のデータを暗号化**

感染したパソコンからアクセス可能な全てのファイルサーバーが対象となります。
※ 直接NASがランサムウェアに感染するのではないため、当社「HDL2-H/TMシリーズ」などに使用されているNASのウイルス対策機能では防ぐことができません。
（NASに保存されたファイルにランサムウェアが含まれていた場合は検出可能です。）

請求料金を支払っても暗号化が解除される保証はありません。
請求に応じることのないようご注意ください。

ランサムウェアへの対策

パソコンを感染させない

■ **不審なメールの添付ファイルやリンクを開かない。**

一見正常なメールに見えても心当たりのない添付ファイルは開かない、あるいは送信者に確認する。

参照：IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/topics/alert280413.html

■ **パソコンへのウイルス対策ソフト導入や最新パターンファイルの適用。**

※ただし、パターンファイルに登録されていない新種のウイルスは妨げない場合があります。

■ **Windows UpdateなどOSを最新状態に保つ。**

■ **WEBブラウザ、JavaやFlash等のブラウザプラグインを更新し最新状態に保つ。**

ランサムウェアによるデータの暗号化に備える

■ **パソコンはこまめにバックアップを取り、そのバックアップファイルにパソコンが直接アクセスできないようにする。**

ランサムウェアの被害は、ファイルが暗号化され開けなくなってしまうことです。暗号化されてしまったファイルの復元は困難なことから、重要なファイルについてはいつでも復元できるよう、定期的なバックアップを行うことが対策となります。

参照：
IPA 独立行政法人情報処理推進機構
2016年1月5日第16-01-345号 今月の呼びかけ

「ランサムウェア」に備えるバックアップの詳細は裏面へ

「ランサムウェア」対策に有効なNASのバックアップ方法

ランサムウェアは、感染したパソコンから読み書きできるドライブ（内蔵HDD、パソコンに接続した外付けHDD、共有されたNAS）などのファイルの暗号化処理を試みます。

しかし、バックアップ先のドライブを読み書きできないようにしておくことで、バックアップデータをランサムウェアによる被害から守ることが可能です。
そのためファイル共有用途のNASやファイルサーバーのデータを、パソコンから読み書きできないドライブにバックアップしていただくことで、ランサムウェアの被害を最小限に抑えることができます。

NASに接続したバックアップ先の外付けHDDのネットワーク共有を「無効」にしてください。

ネットワーク共有を「無効」にし、共有できない状態になっていることを確認してください。これにより、感染パソコンからのアクセスは不可となるため、ランサムウェアからバックアップ先の外付けHDD内のファイルを守ることが可能です。

※NASでバックアップ設定を行うと、バックアップ先共有フォルダーは読み込み専用となりますが、管理者権限のあるパソコンからは読み書き可能となるため、必要な時以外、共有設定を無効にすることで確実に保護します。

世代管理のできるバックアップ方法で外付けHDDにデータをバックアップしてください。

当社では、ランサムウェアに備えたNASのデータのバックアップ方法として、外付けHDDへの変更した部分の履歴を残すことができる「履歴差分バックアップ」を推奨しております。バックアップに履歴を残しておくことで、暗号化されてしまったファイルのひとつ前の世代（暗号化される前のファイル）を取り出すことが可能です。

※ バックアップは複数世代を残す設定を推奨いたします。また、履歴保存世代数にも上限がありますので、気付いたらすぐにバックアップからデータを取り出すようにしてください。

アイ・オーNAS商品における推奨バックアップ方法

Windows Storage Server搭載モデル

利用するバックアップ方法 ： **Windows Server バックアップ**
ネットワーク共有サービスの出荷時設定 ： **無効**
➡ 外付けHDDがエクスプローラから見えないことを確認してください。

■ LAN DISK Z シリーズ

Linuxベースオリジナル OS搭載モデル

利用するバックアップ方法 ： **履歴差分バックアップ**（LAN DISK Aシリーズはバックアップ履歴モード）
ネットワーク共有サービスの出荷時設定 ： **有効** ➡ 設定を変更してください。

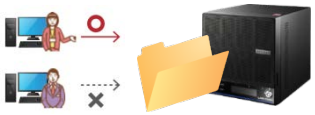
■ LAN DISK H シリーズ　■ LAN DISK XR、XV シリーズ　■ LAN DISK A シリーズ

※ 各商品のバックアップの設定についてはマニュアルをご確認ください。

■ その他推奨設定

アクセス権は適切に設定しましょう

「LAN DISKシリーズ」は、共有フォルダーごとにアクセス権を設定することが可能です。アクセス権を適切に設定することにより、暗号化のリスクを減らすことが可能です。



アクセスログを保存しましょう

「LAN DISK Hシリーズ」であれば、アクセスログの長期保存が可能です。万が一の際、どのPCにより暗号化されたのか確認することができます。

※ LAN DISK Hの「ログ拡張」機能で実現

推奨バックアップHDDラインアップ

3つの安心に対応！ 法人向け利用に最適なバックアップHDDをご紹介いたします。

※履歴差分バックアップでは複数世代を残すため、十分なドライブ容量の外付けHDDをお選びください。（目安：NASの容量の2倍程度）

ミラーリング対策2ドライブモデル
ZHD2-UTX シリーズ
2TB　4TB　6TB　8TB　12TB

1ドライブモデル
ZHD-UTX シリーズ
1TB　2TB　3TB　4TB　6TB

■ ランサムウェア対策の最新情報は当社HPにて　http://www.iodata.jp/biz/ransomware/index.htm

進化する明日へ Continue thinking
株式会社 アイ・オー・データ機器　www.iodata.jp
商品選びで悩んだら！ インフォメーション デスク
TEL. 0120-777-618
月曜日～金曜日（祝・祭日を除く）10:00～17:00