

自宅や外出先には、まさかの落とし穴が!!

CrossLinks データプロテクション

オンライン会議/テレワーク時代、危険だらけのリモート環境

発生頻度 ↑

① 起こす操作ミス
32% データを消失した原因で操作ミス(上書き等)の割合

RAID構成でビルド中、別HDDで障害が発生するとデータを消失

① 誤操作対策

- Windowsバージョン管理利用
- ファイルを読み取り専用にする
- バックアップをこまめにとる

② サイバーセキュリティ
54% フィッシングサイトのURLでHTTPS使用の割合

高リスクURL中フィッシング用は81%
ランサムウェア身代金平均は\$15万

② 入口対策

- アクセス権限管理と認証・記録
- ガイドライン作成と周知徹底
- ウイルス検知ソフトを検討

③ 壊れるハードウェア
80% 大手クラウドプロバイダのサーバHDD4年後の生存率

ハードドライブの年間交換率(ARR)は3%でメーカー試算よりずっと高い

③ 災害対策

- HDDは3年が交換の目安
- 冗長化/多重化で稼働率向上
- バックアップをこまめにとる

④ パソコンの紛失/盗難
3.7% パソコン紛失(未遂を含む)、盗難にあつた社員の割合

会社貸与PC100台中4台が紛失
パスワード解析ツールでハッキング

④ 盗難対策

- 勤務先への接続はVPNで
- Wi-Fiスポットは業務で使わない
- 遠隔操作で情報漏洩を防止

被害規模 →

テレワーク時代のエンドポイントプロテクション、あなたの会社は??

- ❑ バックアップはハイブリッド(分散型)で、その1つはクラウドである?
- ❑ バックアップはこまめにとっている(1日複数回)?
- ❑ マルウェア対策ソフトは常に最新状態になっている?
- ❑ PCを紛失/盗難した場合、遠隔操作で漏洩防止ができる?
- ❑ 操作ミスで上書きしたファイルを元に戻す仕組みがある?

上記の3項目以上に該当しないなら、**今のエンドポイント環境を見直すべきです**

<参考文献>

1. ウェブroot脅威レポート2021(2021.6.16) <https://mypage.webroot.com/2021-threat-report.html?country=japanese>
2. 独立行政法人情報処理推進機構(IPA)「組織における内部不正とその対策」(2017.5) <https://www.ipa.go.jp/files/000059582.pdf>
3. JNSAI「情報セキュリティシニアに関する報告書～発生確率編～」(2011.4.1) <https://www.infosec.co.jp/column/89.html>
4. ハードドライブの平均寿命は? 使わなければいつまでも壊れない? (2015.5.30) https://www.lifehacker.jp/2015/05/150530_hddlimit.html
5. ハードディスクドライブの故障率に関する事実(2016.3.23) <https://tech.nikkeibp.co.jp/it/article/COLUMN/20070529/272852/>
6. どうしてデータ消失が起こるか 消失事故の4パターンから導くバックアップ対策(2014.2.27) <https://www.sbbt.jp/article/cont1/27612>

これで絶対安心! あなたのこれからのテレワーク!!

CrossLinks データプロテクションの特徴

誤操作対策

① 超高速バックアップ(キャッシュ&圧縮)

CARBONITE

重複排除/可逆圧縮/ブロック分割

バックアップ

ローカルキャッシュ

Carbonite Endpoint Cloud (Azure)

リストア

解凍/ブロック組立/復元

→ ケタ違いのバックアップスピード(1GBが約1分半)

入口対策

② 超高速・軽量フルクラウドセキュリティ

WEBROOT

新規ファイル

収集

リアルタイム参照

Webroot Bright Cloud

分析公開

新規URL

グローバル脅威データベース

→ 定義ファイル不要のフルクラウド型で超高速・軽量を実現

災害対策

③ ハイブリッドバックアップ

CARBONITE

Microsoft 365

ローカル

Carbonite M365 Cloud (Azure)

Carbonite Endpoint Cloud (Azure)

海外クラウドデータセンター

国内クラウドデータセンター

→ MS365バックアップは容量契約/アカウント数契約を選択可能

盗難対策

④ 遠隔デバイス管理 エンドユーザー-設定変更不可

ファイル選択管理

エンドユーザーによる自己管理

管理者が一元管理

管理者

遠隔データロック

遠隔データ削除

パソコンの位置情報

→ 遠隔データ削除(リモートワイプ)後は直近バックアップからリストア

更に...

⑤ 監視サービスを提供

→ ストレージ使用状況や検出脅威情報などをレポート



CrossLinks データプロテクション 製品ラインアップ				
製品名	クラウドバックアップ		エンドポイントセキュリティ	
	デバイスデータバックアップ	クラウドデータバックアップ	盗難データ保全(遠隔データロック/削除)	マルウェア検知/駆除URL脅威検知
データプロテクションスイート	○	○	○	○
データプロテクション	○		○	
MS365バックアップ		○		

<システム要件>
対応OS PC : Windows 8.1/10/11, macOS Sierra(10.12) 以降、サーバー : Windows Server 2012/2012 R2/2016/2019

販売代理店 : 販売元 : 株式会社クロスリンクス

スイート製品のうちバックアップ製品は米国Carbonite社の"Carbonite Endpoint"です。Carbonite社は2006年に創業し、2020年6月現在世界で2万4千社のパートナー企業を含む45万人の顧客に利用され、7000億のファイル(250ペタバイト)を管理しています。またセキュリティ製品は米国Webroot社の"Webroot® Business Endpoint Protection"です。Webroot社は1997年に創業し、2020年6月現在1万5千社のパートナーを含む20万社の法人に利用され、3,000万以上の契約数を持っています。

ランサムウェア、もはや100%の防御は不可能です!!

従来のサイバーセキュリティ産業の限界

🕒 回顧的	📦 サイロ型	🕒 遅れ
従来型ツールは、これまでに見られたことのあるテクニックを検知し、攻撃に反応することしかできない	Eメール/クラウド/ネットワーク/エンドポイント/OTに対するセキュリティソリューションは別々に進化してきた	これまでマシンスピードの脅威に対処するためにも人間に頼ってきた

💡 サイバー犯罪者はEメールゲートウェイ、アンチウイルスツール、エンドポイントソリューションが使用する回顧的な拒否リストを回避できることを知った

🦠 攻撃インフラを更に獰猛なものに更新し進化させた

🦠 新型コロナのように変異し巧妙化

📊 攻撃の範囲を拡大し、Eメールや SaaS 環境からクラウドインフラ、IoT、産業用制御装置 (ICS) まで、デジタルエンタープライズ内のさまざまなエリアを標的とするようになった

脅威の新時代 (5つのトレンド)

- 1. ランサムウェアの台頭** 産業用ICSを標的としたランサムウェアは増えつつあり、2018年以降500%増加している
- 2. ステルス&先行性APT*** 大手の多国籍企業や政府機関だけでなく、より広範囲な企業が標的
- 3. クラウドベースの攻撃** デバイスではなくIDを狙う: SaaSアカウントの乗っ取り (Zoom/Teams/Microsoft365等)
- 4. ゼロデイ攻撃** マイクロソフト Exchange サーバーのゼロデイを悪用した攻撃が発生中であることを発表
- 5. 攻撃型AIの出現** AIはサイバー犯罪者の攻撃力を増し、よりステルスの、より高速な、より効果的な攻撃を可能にする

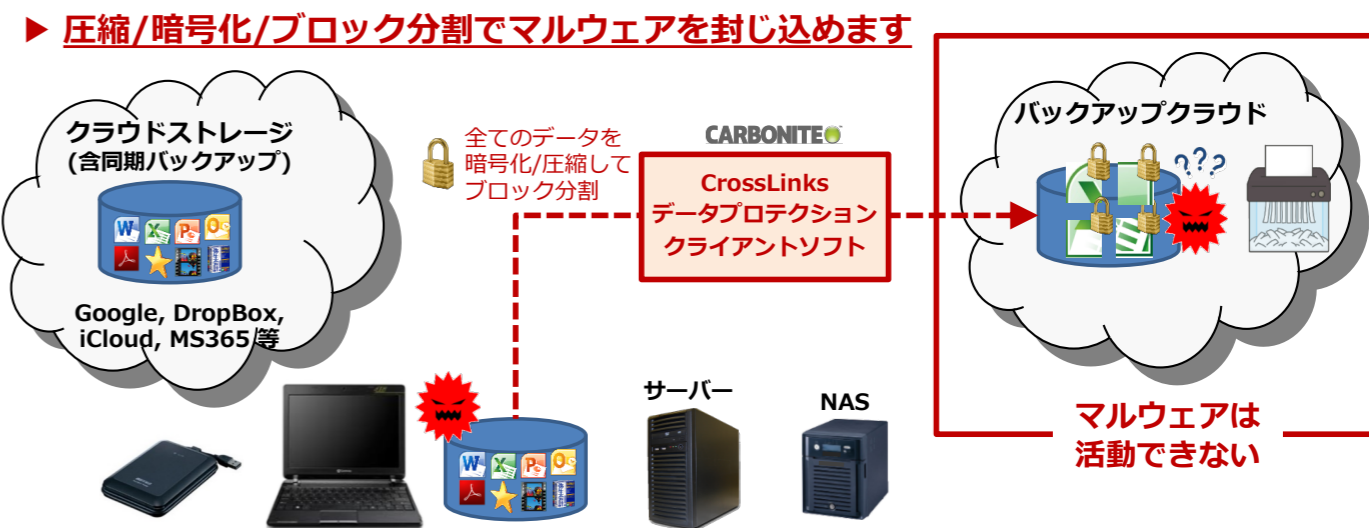
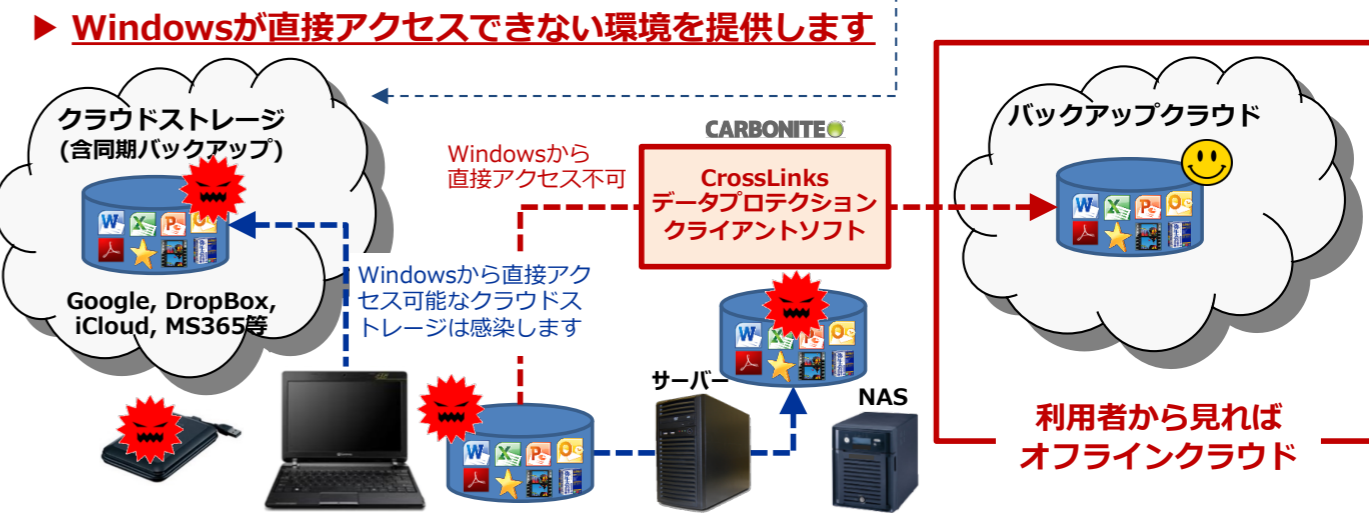
*APT(Advanced Persistent Threat): 脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃のこと (IPA) 出典:ダークトレース社ホワイトペーパー

確実な復旧こそ最終対策、安全安心のバックアップは最後の砦!!

データプロテクションで新しい脅威の対策を

攻撃を受けたデータの格納場所の6割がパブリッククラウド*という事実に対し

*出典: IT Leaders 2020.5.28



CrossLinks データプロテクション 製品ラインアップ					
製品名	機能	クラウドバックアップ		エンドポイントセキュリティ	
		デバイスデータバックアップ	クラウドデータバックアップ	盗難データ保全 (遠隔データロック/削除)	マルウェア検知/駆除 URL脅威検知
データプロテクションスイート		○	○	○	○
データプロテクション		○		○	
MS365バックアップ			○		

<システム要件>
 対応OS PC: Windows 8.1/10/11, macOS Sierra(10.12) 以降、サーバー: Windows Server 2012/2012 R2/2016/2019

販売代理店: 販売元: 株式会社クロスリンクス

スイート製品のうちバックアップ製品は米国Carbonite社の"Carbonite Endpoint"です。Carbonite社は2006年に創業し、2020年6月現在世界で2万4千社のパートナー企業を含む45万人の顧客に利用され、7000億のファイル(250ペタバイト)を管理しています。またセキュリティ製品は米国Webroot社の"Webroot® Business Endpoint Protection"です。Webroot社は1997年に創業し、2020年6月現在1万5千社のパートナーを含む20万社の法人に利用され、3,000万以上の契約数を持っています。