わかる!
マルウェア・ランサムウェアへの防御と対策

守るべきものを守り、ビジネスを止めない

マルウェア・ランサムウェアの被害が拡大

ランサムウェアなど、マルウェアによる攻撃は増加の一途をたどり、コロナ禍でのテレワークにともなって急増しています。被害の実態が広く認識されるようになり、IPA(独立行政法人情報処理推進機構)「情報セキュリティ10大脅威 2022」でも、ランサムウェアによる被害が昨年に続き2年連続1位になるなど、影響の大きさが際立っています。

また、ランサムウェア対策は企業規模の大小を問わず、仕組みの検討と導入コスト、万が一の際の身代金や社会的な影響など多岐にわたり、現実的に効果のある対策を各社で模索しています。

一般的なランサムウェア対策とそこに潜む問題

そもそもランサムウェアにかからないことが一番なため、予防策が最も重要です。多くの企業では、外部から狙われる隙をつくらないように、デバイス・サーバー・ネットワーク・運用管理・人的体制にいたるまで、多層防御を施していますが被害は後を絶ちません。

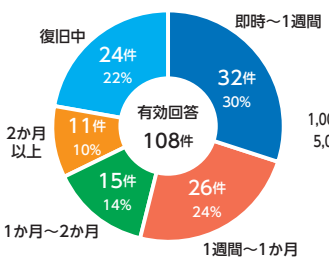
具体的には、外部からの侵入を防ぎ異常を検知する監視、バックアップをとり事後に復元することが一般的に行われている対策です。これらには、以下の盲点があります。

- アンチウィルス・監視・バックアップなどのポイントソリューションでは、重要なコンテンツを守る対策がない(侵入されてしまえばお手上げ)
- 複数の対策ツールを用いるため複雑な運用となり、不備が発生しやすくコスト高になる(不備の隙やリアルタイムではない隙を突かれる)

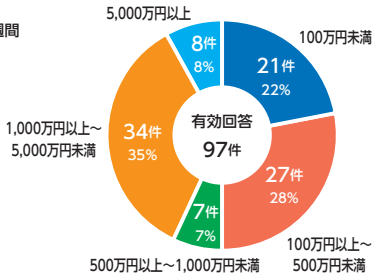
順位	「組織」向け脅威	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

【出典】IPA「情報セキュリティ 10 大脅威 2022」

【被害からの復旧に要した期間】



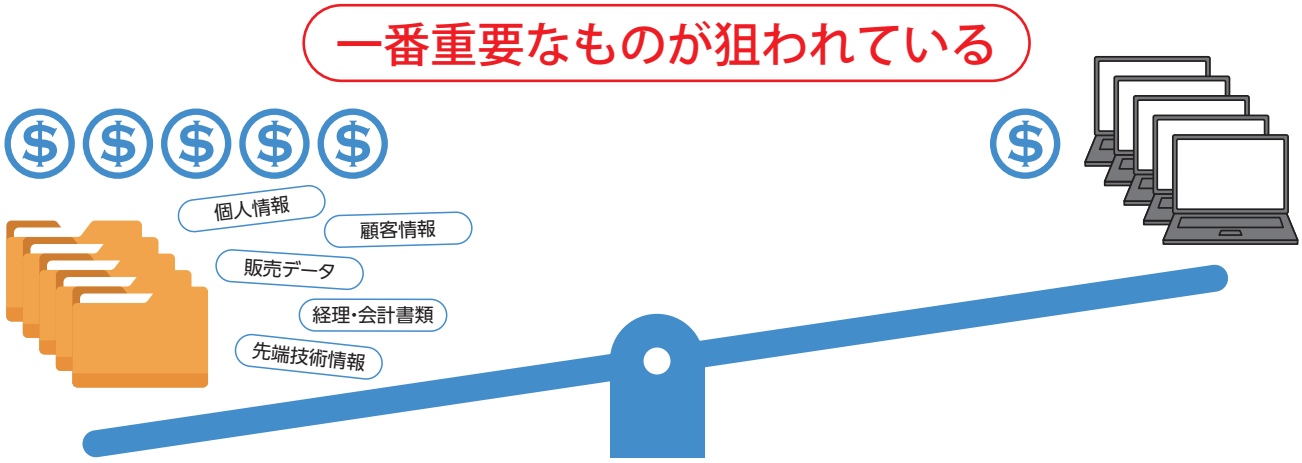
【被害の調査・復旧に要した総額】



【出典】警察庁「令和３年におけるサイバー空間をめぐる脅威等の情勢について(速報版)」

何を守るべきか?

ランサムウェアはシステムではなく情報そのもの、つまりファイルやコンテンツを人質にします。対策としては、情報資産を強固に守り、万が一被害を受けた際にも影響を最小限に抑え、ビジネスを継続できるようにすることが必要です。現在の情報セキュリティにおいては、業務に欠かせない情報資産(＝ コンテンツ)を守ることが、最も重要なことなのです。



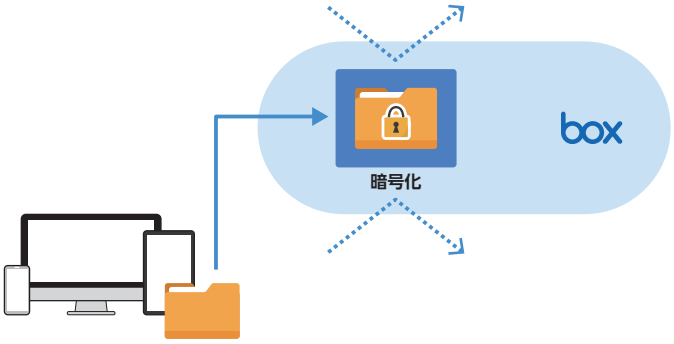
ランサムウェアに強いBox！

Boxの基本サービスに組み込まれているデフォルト機能で、ランサムウェアの予防と対策ができます。予防や対策に専用のソリューションを追加導入する必要はなく、Boxを使うだけで、シンプルにランサムウェア対策ができます。

予防策

Boxにアップロードされたコンテンツは、自動で暗号化されます。それはラッピングされたような状態で、外からの影響を受けません。例えば、もしランサムウェアに感染したファイルがあっても、ランサムウェアに操作されたり実行されたりすることはなく、感染が拡散することはありません。意図的に暗号化を行うといった、特別なオペレーションも不要です。あくまでも、コンテンツをBoxにアップロードするだけです。

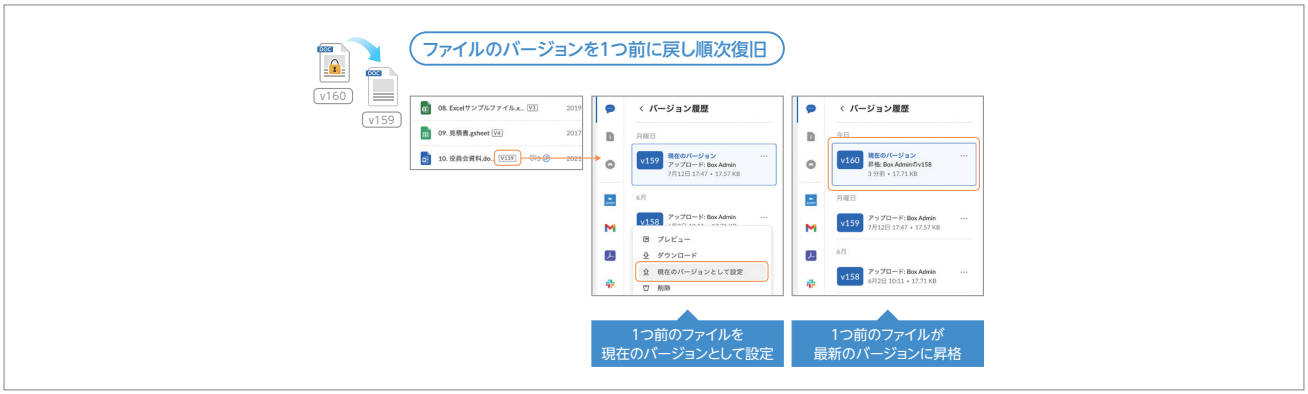
つまり、Boxはそもそもランサムウェアに強く、Boxを使うことがランサムウェアの予防になるのです。

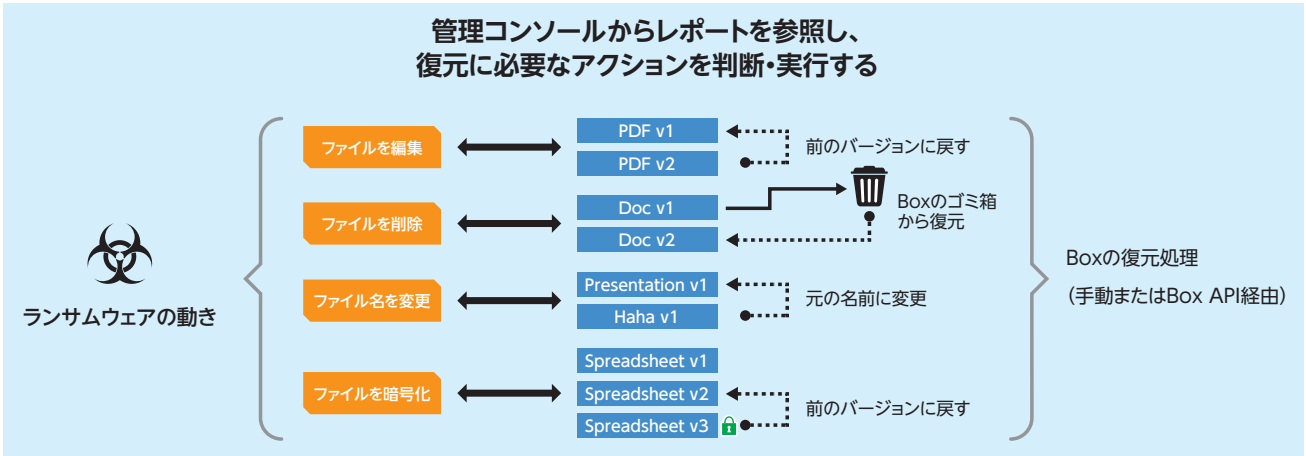


万が一の感染後の対策

万が一感染した場合でも、Box上のコンテンツは自動バージョニング(版管理)されているため、ファイルは感染した時点でバージョンが上がり、バージョン履歴から感染前のバージョンに戻すことでコンテンツを元に戻し、即座に業務を継続することができます。

また、管理コンソールからレポートを参照し、何が行われたのか(ファイルを編集、ファイルを削除、ファイル名を変更、ファイルを暗号化)を確認して、それが行われた時刻、誰と共有しているかを把握し、影響を受ける範囲を特定します。そして、復元に必要なアクションを判断し、実行します。



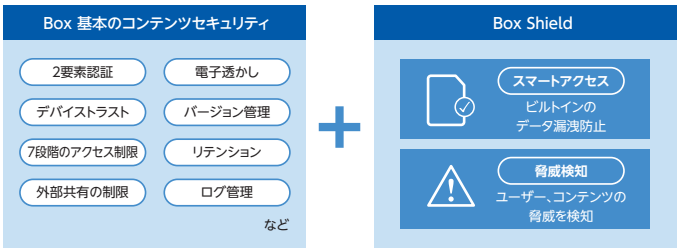


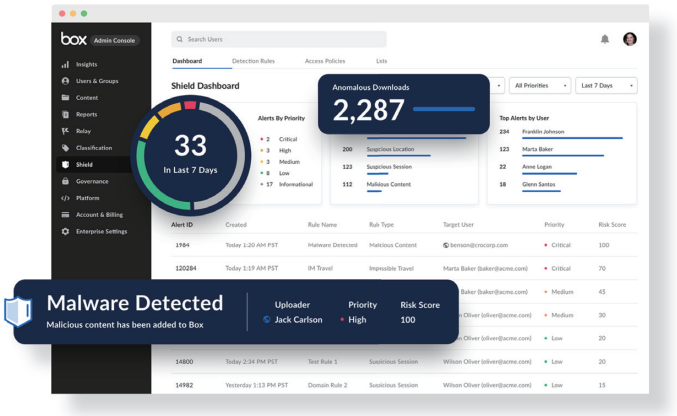
脅威へのさらなる対策

Boxには、ランサムウェアやマルウェアの脅威へのオプション機能もあります。

Box Shieldにはマルウェアの脅威検知機能があり、アップロード・ダウンロード・プレビュー・共有・コピーといった、アクションごとにファイルをスキャンし、悪意あるコンテンツをほぼリアルタイムに検知します。ハッシュ関数ベースのスキャンだけではなく、機械学習ベースのスキャンを実行することで、悪意や疑わしい脅威の検知を強化しています。

万が一Box Shieldが悪意あるコンテンツを検知したら、ローカルへのダウンロードや、他のアプリケーションとの接続をブロックして拡散を防ぎます。コンテンツへのアクセスにも制限をかける一方で、コンテンツは前述のとおり暗号化された状態で安全なため、プレビューやオンラインエディタで編集したり、共同作業を継続することができるため、業務を継続できるのです。





まとめ

ビジネスの中心には常にコンテンツがあり、ランサムウェアもそこを狙います。ゼロトラストへの移行だけでは守りきれない企業資産に、コンテンツを強固に守るセキュリティ＝コンテンツセキュリティを施すことが、いま最も重要なセキュリティ要件です。コンテンツセキュリティの対策下に、ランサムウェアのターゲットとなっている企業のコンテンツを置けばリスクは最小化し、万が一の影響も最小限かつ早急な回復を図れます。企業が求める、何があってもビジネスを継続できる環境をBoxが提供します。

Boxとクラウドコンテンツ管理の情報サイト

Box Square

企業・組織のコンテンツやコラボレーションに関わる課題を解決する総合ポータルサイトです。働き方改革、生産性向上、DX、デジタルワークプレイス、セキュリティなどをテーマに、ブログ、お客様事例やインタビュー、各種レポートなど最新情報をお届けします。

https://www.boxsquare.jp/

株式会社 Box Japan

〒100-0005
東京都千代田区丸の内1-8-2 鉄鋼ビルディング15階
www.box.com/ja-jp/home

Box導入に関するお問い合わせ
www.boxsquare.jp/inquiry

Box製品ご購入後のサポートに関するお問い合わせには返信できませんので、予めご了承ください。

販売代理店