セキュリティ特集

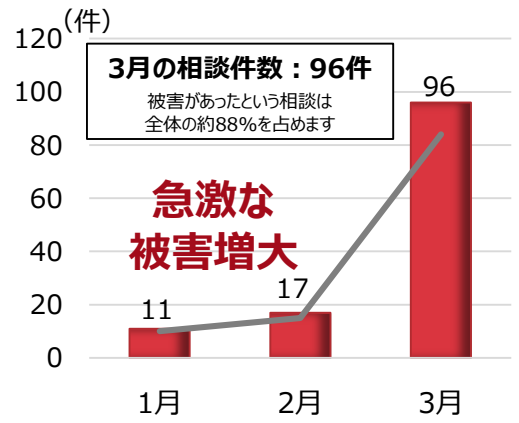
ランサムウェア対策

感染したパソコンをロックして操作不能にしたり、重要なファイルを暗号化したりする「ランサムウェア」による被害が、2016年に入り日本国内でも急増しています。ロック解除や暗号化されたファイルを復元することと引き換えに「身代金」を要求します。感染すると業務継続できないため、ビジネス活動に大きな影響を及ぼします。パソコンに限らず、病院や教育機関などの業務システムでの感染例も報告されています。
ランサムウェアの対策について富士通のソリューションをご紹介します。

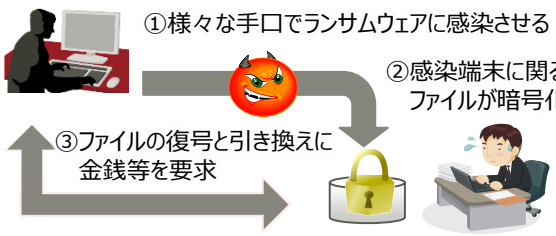
感染被害が急増しているランサムウェア

システムやデータを使用不能にして金銭を要求するランサムウェア攻撃の感染被害が今年に入り急増しています。主な感染経路は偽装メールの添付ファイルや改ざんされたWebサイト閲覧などになります。標的型攻撃に比べ短時間で目的を達成できることもあり、新たな脅威として注目されています。

IPAへの相談数が過去最悪



企業において業務が停止する恐れ



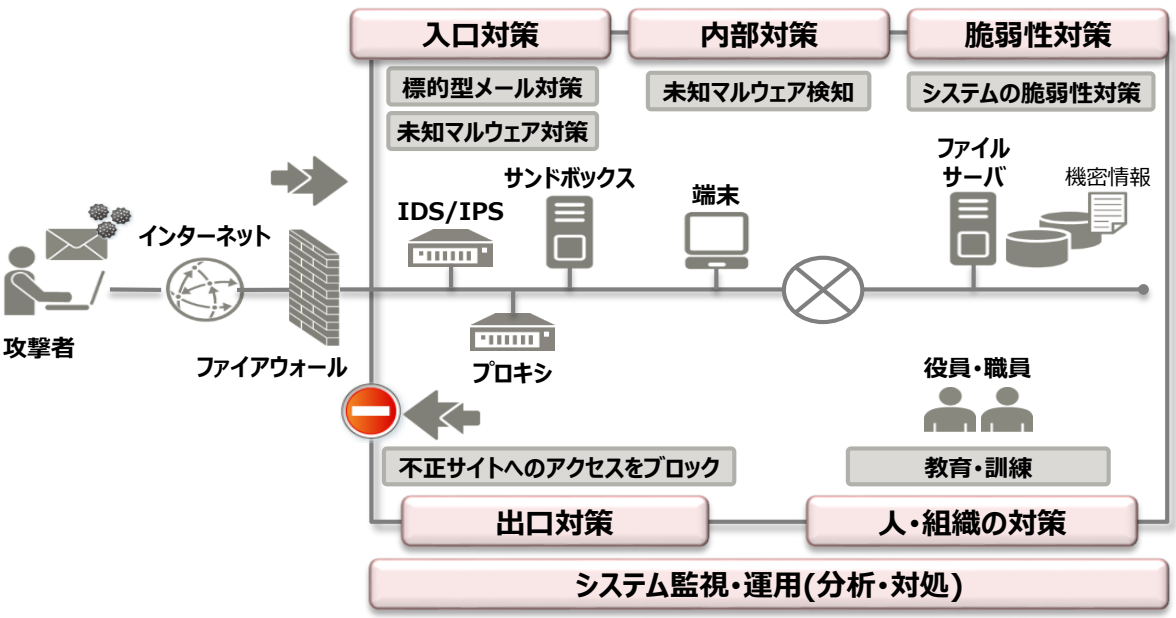
ランサムウェアは2種に大別される

- 端末ロック型ランサムウェア [端末を人質]
  画面ロックやアプリの強制終了などの手口で感染端末を操作不能にするタイプ
- 暗号化型ランサムウェア [データを人質]
  感染端末内のデータやネットワーク上のデータを暗号化し使用不能にするタイプ

出典：IPA【注意喚起】ランサムウェア感染を狙った攻撃に注意　https://www.ipa.go.jp/security/topics/alert280413.html

ランサムウェア対策の考え方

ランサムウェアもマルウェアの一種で感染経路も同じため、対策も他の不正プログラムと同様に標的型攻撃対策が有効です。攻撃の全体像を把握した上で、多層防御によりランサムウェアの侵入や感染を防ぎます。



ランサムウェアによる被害を最小限に抑える対策

サイバー攻撃の手法は年々巧妙になっており、ランサムウェアの確実なブロックは保証できません。ランサムウェア感染を前提に、業務への影響を最小限に抑えることがセキュリティマネジメントには必要です。最も効果的な方法は「バックアップ」です。復旧できる唯一の手段となりますので、バックアップ先が被害に遭わないようにすること、感染済のデータでバックアップを上書きしないよう、世代管理運用が重要となります。

ランサムウェア対策に有効なバックアップの考え方

復旧対策

① 業務影響を最小限に抑える

- クライアントPC全台数分のバックアップは有効ですが、大容量の確保やネットワーク負荷、管理面において多額のコストが掛かることを考慮する必要があります。
- PC内も含め社内に散在するデータを棚卸し、データの重要度/機密性に応じてデータを仕分ける。業務への影響がある重要なデータは、必ずPC以外に保存する運用を徹底し、バックアップ容量も削減する。

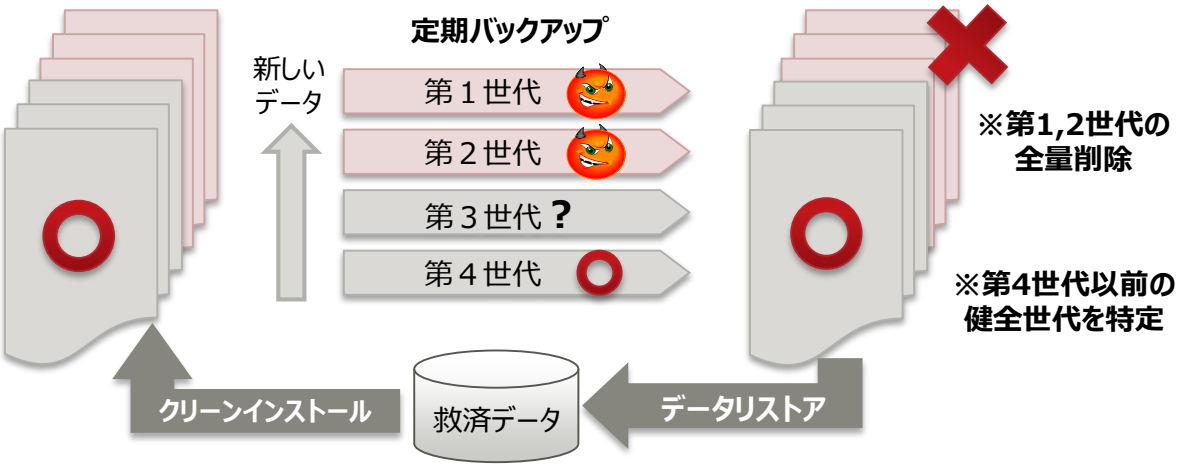
② ランサムウェアがアクセスできない場所に保存する

- ランサムウェアは、感染したPCだけでなく組織のネットワーク共有上のデータも暗号化する動作をします。仕分けした重要データの保存先も暗号化されるリスクがある為、バックアップソフト等を使用し、感染PCからアクセスできない場所（ネットワークから隔離されている）へのバックアップが求められます。
- ディザスタリカバリー観点のデータロスト防止策として、遠隔地（物理的に別の場所）へのバックアップも考慮します。

③ バックアップの世代管理でリスクを下げる

- ランサムウェア感染の発見が遅く、暗号化されてしまったデータをバックアップしてしまうリスクがあります。
  また、バックアップデータの中に、ランサムウェア自体が含まれていることも考えられます。
- 最新のデータだけでなく複数世代管理のバックアップを実施することで、感染の発見が遅れても希望するデータを復旧できる可能性が高くなります。
- より安全にリストアするべく、バックアップデータにマルウェアが含まれていないか確認します。
  ＊マルウェアには多くの亜種が存在するため、全てのマルウェアの検出は保証されません。

複数世代管理バックアップ

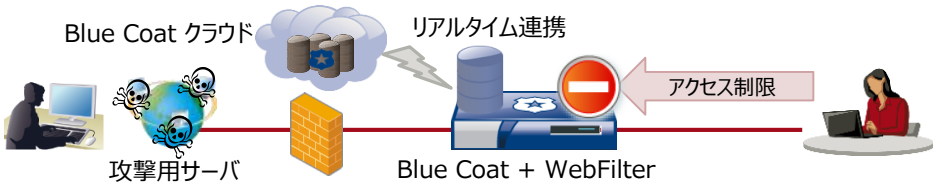


ランサムウェア対策ソリューションの提供

入口対策 **出口対策** **不正サイトのアクセスをブロック** ➢ 危険なWebサイトへの**アクセスを遮断**

例：Blue Coat ProxySG +WebFilter

■脅威が含まれているサイトやC&Cサーバ等、外部への不正なアクセスをリアルタイムでブロック
■C&Cホスト、1日限定ホストに関する世界中の共有情報を利用し、攻撃用サーバとの不正通信をブロック



入口対策 **出口対策** **標的型メール対策** **未知マルウェア対策** ➢ 未知マルウェアによる**侵入を検知**

例：Palo Alto Networks PAシリーズ

■仮想実行(sandbox)環境でプログラムを実行することで振る舞いベースでマルウェアを検知
迅速にシグネチャを生成し標的型攻撃への対応を強化

既知のファイルと比較 **シグネチャ自動生成**
サンドボックス環境で実行 **管理用Webポータル**

・PAシリーズがファイルをWildFireクラウドに送信
・新しいシグネチャをPAシリーズに配信、マルウェアフォレンジックを表示

内部対策 **未知マルウェア検知** ➢ 標的型攻撃で利用される**未知の脆弱性やマルウェアを検知・防御**

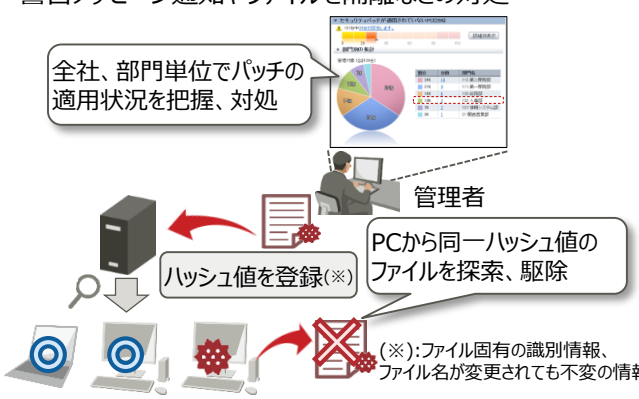
例：FFR yarai

■ウイルスパターンファイルに依存しないヒューリスティック・エンジンを活用し、未知のウイルスを検知して動作を阻止
■外部媒体(USBメモリ等)からの侵入も防御

脆弱性対策 **システムの脆弱性対策** ➢ ランサムウェアに利用される**脆弱性の管理**

<オンプレミス版>
例：Systemwalker Desktop Patrol

■Windowsのセキュリティパッチ、ウイルス定義ファイルが最新にアップデートされているか管理
■マルウェアのファイルと同一ファイルの所持状況を把握、警告メッセージ通知やファイルを隔離などの対処



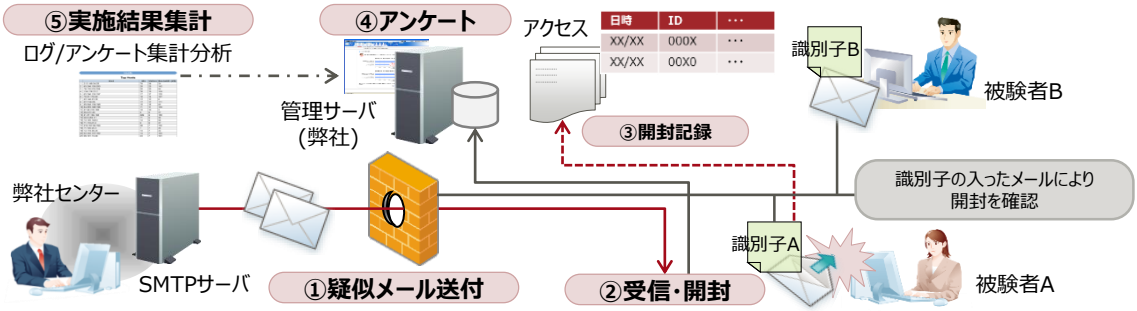
<クラウドサービス版>
例：ProIT Policy N@vi

■WindowsUpdateやAdobeFlash、ウイルス定義ファイルが最新にアップデートされているか管理

人・組織の対策　教育・訓練 ➢ 不審なメールに対する**職員のリテラシーを向上**

例：標的型メール攻撃訓練サービス

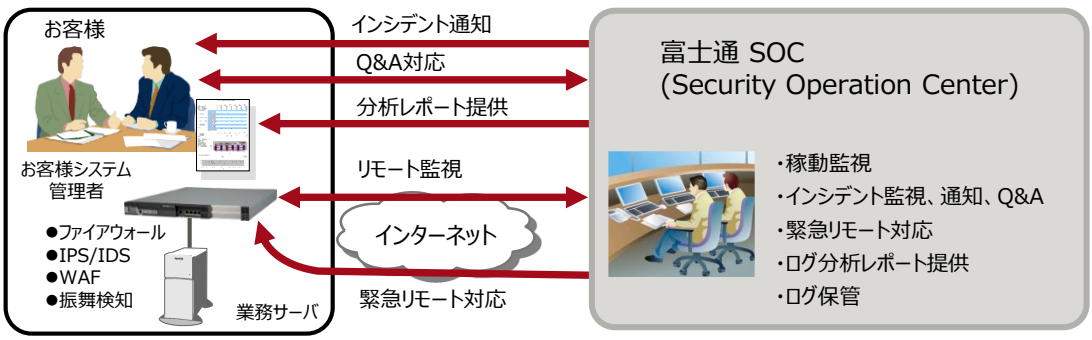
■訓練用に作成した疑似攻撃メールを対象者に送信し、添付ファイルの開封やURLのクリック状況を集計
■標的型メール攻撃を体験することで、的確な知識と判断能力を身につける体験型教育プログラム



監視・運用　システム監視 ➢ **24時間365日**お客様のシステムに対する**不正アクセスを監視**

例：セキュリティ最適化サービス 不正アクセス監視モデル

■24時間365日、外部からの不正アクセス監視だけでなく、内部侵入したマルウェアの振る舞い監視にも対応



復旧対策　データバックアップ ➢ PC、ファイルサーバのシステム、**データの復旧**

例：Acronis Backup Advanced

■PCのシステム、データを、定期的にテープへ世代管理バックアップ
■万が一 ランサムウェアに感染して重要なデータが暗号化されてしまった場合、システムごと重要なデータをテープから復旧