arcserve

ランサムウェア対策は、バックアップが最後の砦

Arcserveで行うランサムウェア対策

人物紹介

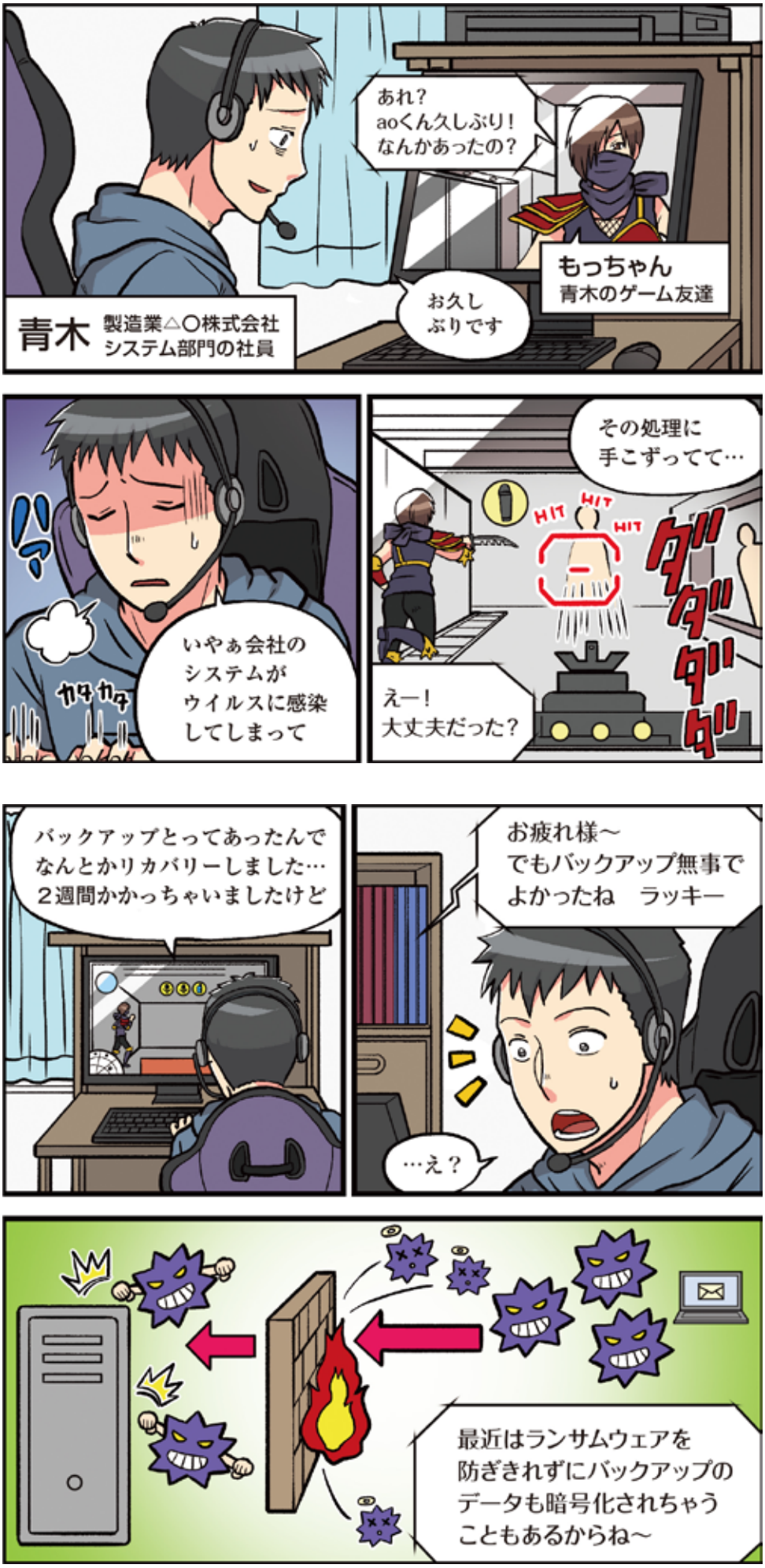
青木

製造業△〇株式会社のシステム担当者。システム部に配属されたのは最近で、知識はある程度あるが経験は浅い。趣味はゲームで、帰宅後ほぼ毎日 PC ゲームに勤しんでいる。
ゲーム内の名前は「ao」。

もっちゃん

青木のゲーム友達の女性。青木と直接会ったことは無いが、ほぼ毎日一緒にゲームをしている。なぜかセキュリティに関する知識が豊富。
ゲーム以外での素性は謎に包まれている。

INDEX


あれ？
aoくん久しぶり！
なんかあったの？
もっちゃん
青木のゲーム友達
お久し
ぶりです
青木
製造業△〇株式会社
システム部門の社員
ハァ
カタカタ
いやぁ会社の
システムが
ウイルスに感染
してしまって
その処理に
手こずってて…
HIT
HIT
HIT
ダダダダ
え一！
大丈夫だった？
バックアップとってあったんで
なんとかリカバリーしました…
２週間かかっちゃいましたけど
お疲れ様～
でもバックアップ無事で
よかったね　ラッキー
…え？
最近はランサムウェアを
防ぎきれずにバックアップの
データも暗号化されちゃう
こともあるからね～


バックアップまで…!?
そんなことになったら
復旧まで何か月かかるか…
ズーン
Arcserve
UDP
まぁまぁ落ち着いて
感染予防対策と合わせて
データ復旧対策をすれば
大丈夫だから
データ復旧対策？
そう！ 万一感染してしまっても
バックアップが残っていれば
復旧できるでしょ？


バックアップデータ
感染
5日前
4日前
3日前
2日前
1日前
時間
月次
週次
Arcserve UDPなら
バックアップ専用
サーバーがあるから
安全性が高いし
データの多世代管理を
してくれるから
それができるのよ
…ってあれ
もう倒しちゃった
んですか!?
へー！ これは
うちの会社に
すぐ入れないと！

もっちゃんって
何者!?
あたりまえ
でしょ～！

拡大するランサムウェア被害

ランサムウェアとは、ファイルを暗号化し、元の状態に戻すために「身代金」（ランサム）を要求する攻撃。

アメリカで石油パイプライン大手の企業がランサムウェア攻撃により数日間の操業停止を余儀なくされた上に、4億 8000 万円の身代金を仮想通貨で支払ったり、国内の大手製造業がランサムウェア攻撃を受け、基幹システムを始めとする社内システムが全面的に使用不能となるなど、国内外、企業の大小を問わず今も感染は拡大傾向です。

ランサムウェア対策は、バックアップが最後の砦

ランサムウェア対策としてネットワークやシステムのセキュリティ対策は重要ですが、攻撃者は常に新しい攻撃手法を作り出しており、ランサムウェアによる侵入や感染を 100% 防ぐことはほぼ不可能です。

感染した場合を想定した対策も準備しておくことが重要です。災害などからの被災に対していかに速く業務環境を復旧させるための BCP（事業継続計画）に、ランサムウェア感染も含めた対策を準備しておくべきでしょう。

感染前の状態に戻すために絶対欠かせないのがバックアップです。仮にランサムウェアによってファイルが暗号化されても、感染前にバックアップしたファイルを復元（リストア）できれば、攻撃の被害を最小にしつつ、その時点からの業務を再開させることができます。

つまり、ランサムウェア対策はセキュリティ対策とバックアップの両輪で準備しておくことが大切なのです。

迅速な業務復旧には、システム全体のバックアップが重要

多くの企業では、データのバックアップはしっかりやっているものの、業務の再開を踏まえたシステムのバックアップ戦略まで構築できている組織は少ないようです。「いざとなれば再構築すれば大丈夫」と捉えがちで、システム全体のバックアップまではしていなかったり、やっていても頻度が低いということが多いのではないでしょうか。

スムーズな業務復旧を考えれば望ましい状態ではありません。OS やアプリケーションのアップデートが頻繁になされる今日、数ヶ月前のシステムですら、そのままでは使うことができない可能性もあり、直近への復旧までに手間も時間もかかってしまいます。

データと同様にシステムも高い頻度でバックアップしておく必要があります。

感染してしまっても、業務再開へ向けた迅速な復旧を目指すためには、以下の３つのポイントを踏まえたバックアップを行うことをお勧めします。

ポイント１：「複数世代の保持」
長期間、かつできるだけ多くの世代のバックアップを保持することで、感染前の状態に復元できる可能性が高まります。多くの世代、長期間のバックアップを保持するということは、同時に、バックアップデータの増大も意味しますので、何らかの対応策が必要です。

ポイント２：「安全な場所に保管」
ユーザがバックアップデータに直接アクセスできないように専用の格納先を確保することで、感染リスクを最小限にします。冒頭で紹介した大手製造業では、バックアップサーバー内のデータも暗号化されてしまったため、一部のデータしかリストアできず、復旧までに長期間かかったと言われています。

ポイント３：「オフラインで保管」
物理的に隔離された環境にバックアップデータを保管することで感染リスクを低減できます。例えば、取り外し可能な媒体やテープメディア、クラウドや外部のデータセンタなど、社内ネットワークとは切り離された（切り離しできる）環境にバックアップデータを置くことで、感染リスクを低減できます。

バックアップ運用でさまざまな策を講じることで、ランサムウェアによる被害を最小限にすることができますが、その分、手間や工数がかかるので対応が難しいと考えられる方も少なくないでしょう。導入の容易さ、簡単操作で運用のしやすさ、といった特徴を備えた統合イメージバックアップ ソフトウェアがArcserve® Unified Data Protection (Arcserve UDP) です。

Arcserve UDP ならバックアップの３つのポイントを押さえた運用がシンプルに実現でき、巧妙化するランサムウェアに備えることができます。

ディスクのイメージを丸ごとバックアップ、初回以降は増分バックアップのみで運用できる「イメージバックアップ」により、データのみならず OS やアプリケーションを含むシステム全体をまとめてバックアップし、簡単に復旧が可能です。また、バックアップ元とは異なるサーバーや仮想マシンへの復旧も標準でサポートしています。いざというとき、より短時間でのシステム復旧がシンプルに実現できます。また、感染状況に応じて、丸ごと復旧だけでなく、ファイル単位の復旧も可能です。

さらに、設定や運用は、直感的で使い易い Web ベースの管理コンソールで、簡単に行うことができるので安心です。

冒頭で紹介した国内大手製造業では、オンラインで接続されていたバックアップサーバーにも被害が及び、システムの復旧を困難にしたと言われています。このような事態を防ぐためにも、前述したランサムウェア対策に欠かせないバックアップの３つのポイント
「複数世代保持」
「安全な場所に保管」
「オフラインで保管」
を押さえた運用を実践しましょう。

Arcserve UDP は、３つのポイント押さえた運用を簡単に実現できるだけでなく、さまざまな機能強化を行うことで、巧妙化するランサムウェアへの対応を行っています。

■ バックアップデータを「複数世代保持」

「永久増分バックアップ」および「重複排除」機能で、バックアップデータ容量を圧縮することができ、多世代、長期間のバックアップデータ保持を限られたストレージ容量でも実現します。

■ バックアップデータを「安全な場所に保管」

権限のあるユーザのみが操作できるバックアップデータの格納庫「復旧ポイントサーバー（RPS）」を導入しバックアップデータを作成・保存することで、データへの感染を防止します。

■ バックアップデータを「オフラインで保管」

組織の状況に合わせ、様々なメディアへ保存できます。
「テープメディアへのバックアップ」機能を利用すると、復旧ポイントサーバー (RPS) に保存されたバックアップデータの二次バックアップ先として、テープと連携ができます。

クラウド ストレージへの対応 ※
クラウドストレージ サービスが提供する上書きができない不変ストレージに対応した「オブジェクトロック機能対応」など、ランサムウェア対策に有効な機能を標準で装備し、最大限バックアップデータを保護する環境を提供します。

※ イミュータブル ストレージへの対応
Arcserve では、オンプレミスで導入・利用できるイミュータブル ストレージを近日リリース予定です。ご期待ください。

■ 健全な時点を調査し、「確実に復元」

いつのバックアップデータなら健全なのかを調査する必要があります。Arcserve UDP は、保存したバックアップデータを迅速、確実に復旧するための仕組みを提供、事業継続を強力に支援します。

「インスタント VM（IVM）」機能：ウィザードを実行するだけで、バックアップデータを直接参照できる仮想マシン（VM）を数分で起動できます。過去のバックアップに遡って仮想マシンを起動し、感染の有無を確認し健全な時点を見つけだし、利用できます。

「仮想スタンバイ（VSB）」機能：バックアップの一連の流れで、バックアップデータから仮想マシンを作成します。ローカル、または遠隔地の仮想環境やクラウド上に代替機を自動的に構築します。いざというときには待機状態の仮想マシンを起動するだけで、利用できます。

■「セキュリティ」をさらに強化

「多要素認証」対応：バックアップ管理者の不正や乗っ取りを防ぐために、Arcserve UDP の管理コンソールのログオン時の多要素認証に対応しています。

「専用回線」対応：業務 LAN とは別のバックアップ専用 LAN に対応することで、セキュリティリスクを低減できます。

■ 業務のレジリエンスを強化

「もしも」ランサムウェアに感染したとしても、迅速にシステムやデータを復旧し、事業継続を高めるバックアップシステムを構築できます。

Arcserve UDP で落ち着いて対応ができる仕組みの導入を検討してみてはいかがでしょうか。

後日談：△〇株式会社オフィスにてオンライン会議をする青木――

青木：こんにちは！青木です。よろしくお願いします。

？：こんにちは！ SIer の橋本です！本日は UDP の導入をご検討されているとのことで…

青木：よろしくお願いします！

青木：（あれ…？この声どこかで聞いたことあるな…）

青木：橋本…はしもっちゃん…　もしかしてもっちゃん!?

橋本：…え!?　もしかして ao くん!?

詳細は、Arcserve Unified Data Protection カタログをご参照ください。

arcserve

お問い合わせ

〒 101-0051　東京都千代田区神田神保町 1-105　神保町三井ビルディング

お問い合わせ窓口：Arcserve ジャパン ダイレクト（0120-410-116）

：JapanDirect@arcserve.com

WEB サイト　：www.arcserve.com/jp

※記載事項は変更になる場合がございます。