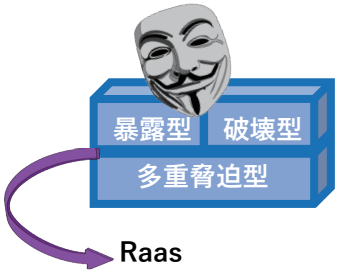
# ランサムウェアの被害軽減を想定したバックアップ運用

## ・ランサムウェアとは？

ランサムウェアは、昔からあるコンピューターウィルスの部類ですが、感染させて終了ではなく、システム / データのロック / データの流出などを盾に脅迫を行い、身代金を要求する行為全般に該当します。
現在では、昔のウィルスのようにパソコン１台を感染させるのではなく、ターゲットは企業のシステムに向けられており、サーバーテロ / 身代金ビジネス / 愉快犯などの目的で、世界中で被害が発生しています。
主に攻撃タイプとしては、右図のようなタイプがあります。
（暴露型） 盗んだ企業情報を公開
（破壊型） ファイル／システムにダメージ
（多重脅迫型） 上記２種類の融合型です。




またランサムウェアは専門知識がなくても、RaaS（Ransomware-as-a-Service）といったサービスもあり、利用されるケースもあるようです。また標的型として特定企業を標的とする場合と、サプライチェーン攻撃として、ターゲットに直接攻撃せずに子会社 / 関連会社を攻撃する場合、そしてランダムに攻撃する場合があるため、インターネットに接続している世界中のコンピューターがオンプレミス / クラウド含めてターゲットとなります。

## ・主なランサムウェア

| | |
|---|---|
| CryptoLocker | コンピューター内のファイル暗号化 / アクセスをブロック。 |
| Petya | ファイル / システム自体を暗号化して起動不能になる。 |
| WannaCry | ビットコインで身代金請求することで有名になった。被害が 40 億ドル以上発生した。 |
| LockBit | 主に企業 / 政府機関を中心に発見。自動拡散機能を持っている。 |
| Conti | Windows OS を攻撃対象。ファイル暗号化 / サイトで一部のファイルを公開される。 |
| Qlocker | QNAP 製 NAS の脆弱性を攻撃する特化型。 |
| Ryuk | ファイル暗号化 /Windows システム復元も無効化する。 |
| GoldenEye | ディスク単位で暗号化を行う。 |
| Bad Rabbit | Adobe Flash のインストーラーの偽装タイプ。 |

※その他多数あります。

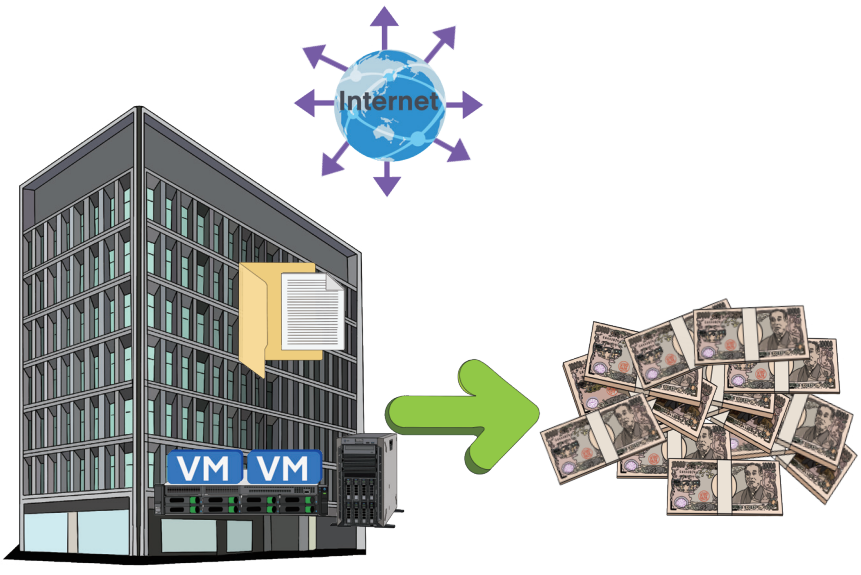
## ・ランサムウェアの感染経路と感染範囲

以前から存在する偽装メールなどからの感染もありますが、最近ではテレワークの影響もあり、VPN などの外部に公開されているシステムの脆弱性 / 不正入手の認証情報を使用して侵入するランサムウェアもあります。
感染はファイルのみでなく、仮想基盤の仮想ディスクなども対象となるため、システムの起動が困難となるケースもあるようです。またクラウドサービス上のコンピューターも同様で、バックアップなどもクラウドサービス内で運用している場合、復旧不可という最悪のシナリオが現実になる可能性もあります。

## ・ランサムウェアに感染した場合の被害

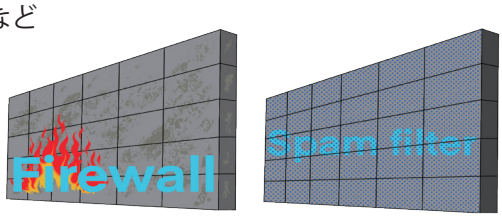
・機密情報の流出
・業務の停止
・システムの停止
・各種ファイルの損失

結果事業継続が不可能になる場合もあり、莫大な損失を招く自体になります。



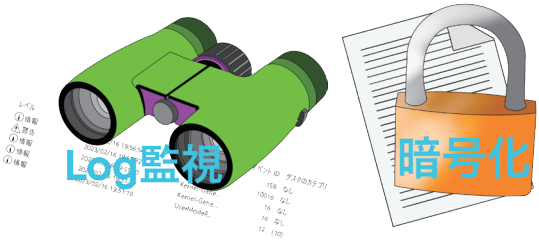
・ランサムウェア対策とは？

ランサムウェア対策として 1 番始めに考えられるのは入口対策となります。
（入口対策）
ファイアウォール、スパムフィルター、IDS/IPS（不正侵入検知、防衛システム）、ウィルス対策ソフト、
OS の最新アップデート、ウェブサイトへのアクセス制限、不審メールのフィルタ　など
Firewall は不正アクセス防止
Spam Filter はスパムメールのブロック
IPS は不正侵入させないようにブロック
IDS は不正侵入発生時に通達
End Point　攻撃の防止他




IPS Intrusion Prevention System( 侵入防止システム )
IDS Intrusion Detection System( 侵入検知システム )

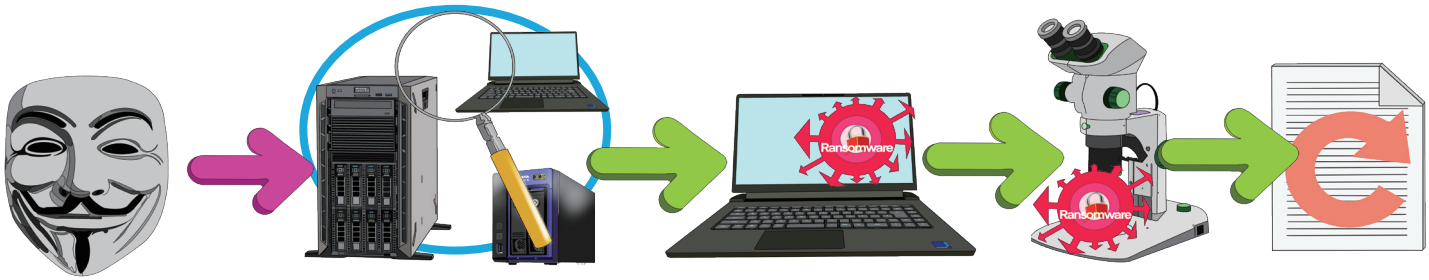

（内部対策）
ログ監視、バックアップ、ファイル暗号化　など
ログ監視は不正なアクセス、ユーザー有無の確認
バックアップは最終手段といえるシステム復旧
ファイル暗号化は流出した際のデータ漏洩防止




（出口対策）
標的攻撃対策
サンドボックス、WAF など
サンドボックス型は基本的に社内のシステムから隔離された環境下で、リンクなどを踏んだ実行結果に基づいてランサムウェアなどの脅威を確認
WAF は WEB アプリケーションの脆弱性対策（データ持ち出しの監視）


EDR 対策

**EDR (Endpoint Detection and Response)**




マルウェアなどの侵入検出　感染端末/サーバーなどの隔離　収集情報から調査/分析　原因ファイルの駆除/復旧

**EPP(Endpoint Protection Platform)**

EDR は EPP と異なり、ランサムウェアのふるまい検知を行い、ランサムウェアと認識された場合に、隔離 / 調査 / 復旧を行います。最近では AI を活用して様々なふるまいのパターンをデータ化して検知を行います。


従来の侵入防御

100% 保護出来る製品はありません。

結論としてバックアップ＋セキュリティの組み合わせでの運用が必要です。

・ランサムウェアに対しての注意喚起

現在経済産業省でも注意喚起されていますが、警視庁サイバー犯罪対策プロジェクトのランサムウェア被害防止対策では下記のように記載されています。

未然対策

・電子メール等への警告　　添付ファイル /URL のクリック。
・VPN 機器等のぜい弱性対策　インターネット上で公開されている機器のぜい弱性を OS 更新 / パッチ適用などでなくす。
・ウイルス対策ソフト等の導入　他のマルウェアやハッキングツール対策。
・認証情報の適切な管理　　利用しているリモートデスクトップサービスなどの認証パスワード管理など。

しかしやはり感染を 100% 防ぐことは難しいため、現実的には「感染に備えた被害軽減対策」が重要となります。

・データのバックアップ等の取得

バックアップデータも暗号化されるケースがあるため、取り外しデバイスへの保管と、日頃からシステム復旧手順の確認を推奨。

・アクセス権等の権限の最小化

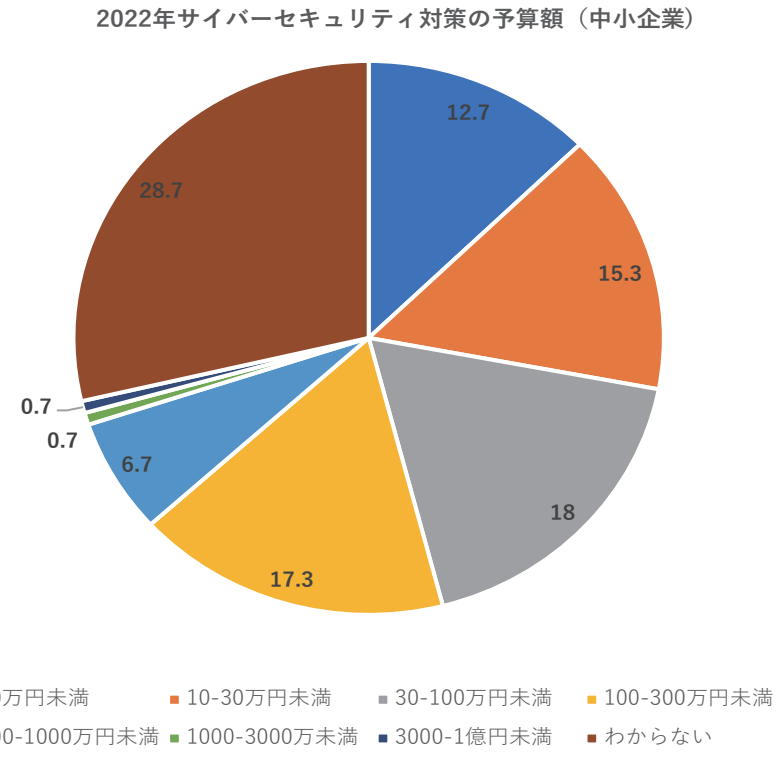
侵入された場合に被害範囲の拡大を防ぐためにユーザーアカウントの権限の範囲を狭くする。

・ネットワークの監視

外部との不審な通信の監視。EDR などを使用して不審なふるまい検知を行い早期発見する。

## ・中小企業のサイバーセキュリティ対策予算額

ランサムウェア被害の多い中小企業でのサイバーセキュリティ対策の予算は、10 万円 ~300 万円未満が主流となります。




日経 BP コンサルティング
「勤務先のサイバーセキュリティ調査」(2022 年 4 月実施 ) より

## ・サイバーセキュリティ対策費用概算

IDS/IPS

50,000 円 ~/ 月単位

LOG 管理ツール

836,000 円 ~　300,000 円 / 年

WAF

初期費用 98,000 円　29,800 円 (0.5Mbs)/ 月単位

サンドボックス

3,000,000 円 / ユーザー　最低利用 5 年

Endpoint

6-25　5,360 円 /1 ユーザー / 年額

EDR

クラウド型 1 万円 ~100 万円
オンプレ　100 万円 ~1,000 万円
種類によっては 1 ユーザー 500 円 / 月などもある

※上記各種ソリューションはあくまで目安となります。価格は各メーカー毎に異なります

## バックアップ

ActiveImage Protector
物理サーバー　145,100 円／ 1 台　永続ライセンス
仮想　217,800 円 / 1 ホスト　ゲスト無制限　永続ライセンス

・ランサムウェアに感染した場合の対処

身代金要求されているメールアドレス /Web サイトのアドレス、オニオンアドレス (.onion で終わるもの)、ビットコインアドレス

↓ ランサムウェアの種類の特定

NO MORE RANSOM （官民連携プロジェクト）

↓ 適合した複合ツールがあれば、除去の可能性がある。

複合ツールの入手 ( 現在約 170 種類掲載 )

※サイトにも記載がありますが、復旧を保証することはありません。

ランサムウェアに感染して身代金を支払って複合ツールを入手した場合でも、上記のサイトで特定した複合ツールを入手した場合でも、一部のデータは戻るかもしれませんが、綺麗に元の通りになることは基本的にないと考えた方がよいと思われます。このような状況を踏まえて、バックアップ運用するだけでなく、使用方法を工夫して復旧する必要があります。

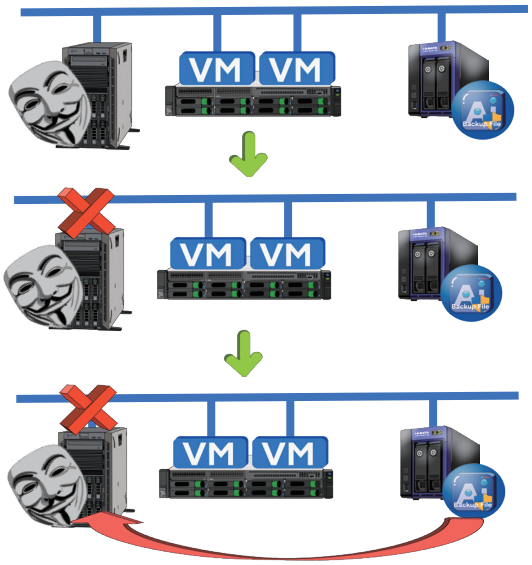
・間違ったバックアップからの復旧方法

例えば、物理サーバーと仮想サーバーのバックアップを、ローカルエリアネットワーク上の NAS を保存先として運用していた場合。

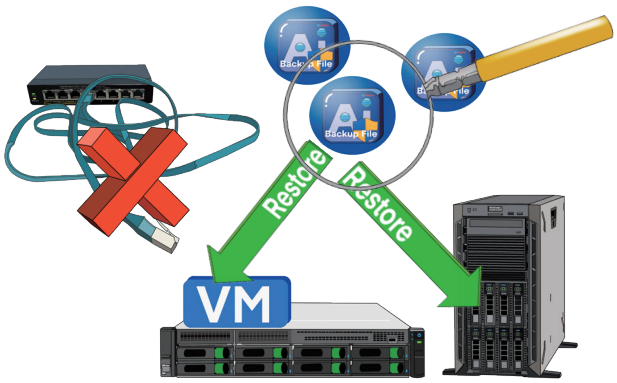
ランサムウェアに物理サーバーが感染しました。

感染したマシンを隔離します。

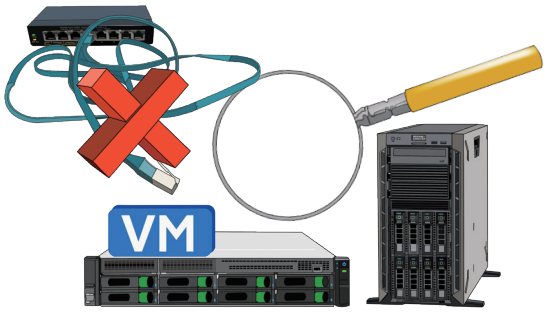
直ぐにバックアップから復元します。




ハードウェア / ソフトウェア障害などによる、システム復旧の場合であれば、上記のように直ぐにバックアップファイルから復旧を行い、RTO を短縮して、業務に影響がでないように最短で復旧すれば良いですが、ランサムウェアに感染した場合、感染範囲の特定を行う、またはある一定のセグメントで切り離しを行い、感染状況を確認する必要があると思われます。また、ランサムウェアに感染した場合の復旧に使用するバックアップファイルの中に感染がないか、可能な範囲で確認を必ず行うことが重要となります。また、リカバリーを行うマシンは、物理 / 仮想問わずに社内のネットワークに接続していない状態でのリカバリー処理を行います。リカバリー処理完了後に起動を行い、不審なユーザーアカウントの有無など、最終確認を行った上で、社内ネットワークへの接続を行う必要があります。



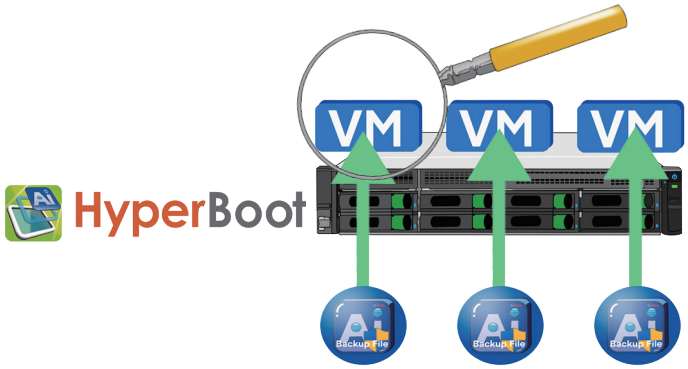

リカバリーするバックアップファイルの選定




リカバリー後に起動して再度確認

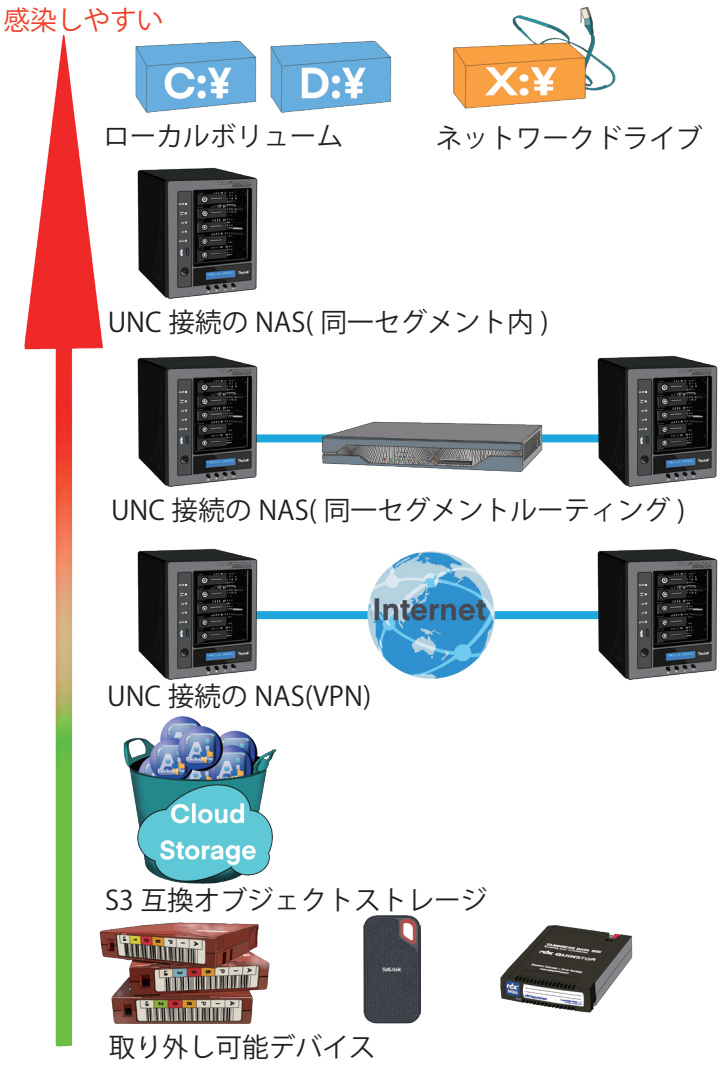
## ・バックアップファイルの選定方法

リカバリーで使用するバックアップファイルの選定方法について、ActiveImage Protector ではバックアップファイルをマウントすることでフォルダ / ファイル単位での確認を行えます。
しかしこれでは、システム上の不正なアカウントの有無を確認することができません。ActiveImage Protector では、バックアップファイルを直接起動させることが可能な、HyperBoot を無料提供しています。システムに予めセキュリティソフトウェアを実装している場合には、HyperBoot で起動させた環境上で動作を行うことも可能です。




※動作状況は各製品により異なります。( 別途検証が必要 )

## ・ランサムウェア対策として考えるバックアップファイルの保存先 ( 感染拡大の速度について )




感染したファイルの同じボリュームから、そのボリュームにマウントされている各ボリュームには短時間で感染しているようです。ネットワーク上の共有ボリュームをドライブレターを割当している場合も同様となります。

ネットワーク上の共有ボリュームを UNC パスを設定して使用している場合は、ドライブレターを割当されている場合よりは多少感染タイミングが遅い傾向があります。

感染したマシンの接続されているネットワークと別のセグメントのルーティングされている環境の場合も多少感染タイミングが遅くなる傾向です。

VPN 接続による遠隔地への感染は、ローカルエリアネットワーク内のマシンと比較して感染速度が遅い傾向があります。

S3 互換のオブジェクトストレージについては、まだ情報が少ない状況ですが、VPN 接続先の共有フォルダよりは、アクセスが難しいため、感染の確率は現在はまだ低いと思われます。またオブジェクトストレージの機能の、オブジェクトロックなどを使用することにより、書き込まれたファイルの変更が一切できない状態にできるため、ランサムウェア対策としては有効です。

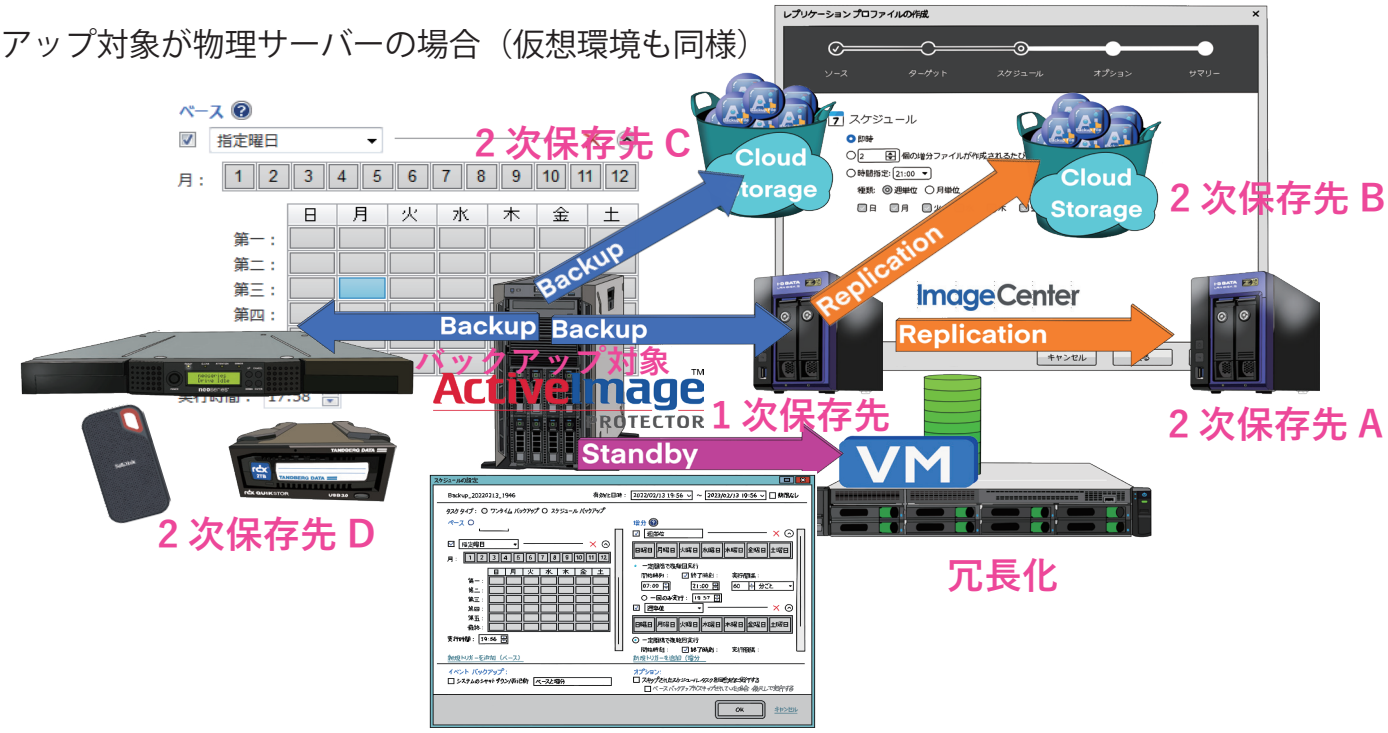
LTO/RDX/USB 機器などの取り外し可能デバイスについては、普段は取り外して保管することと複数のデバイスでローテーションすることにより、もっともランサムウェア対策に有効と思われます。しかしハードウェアであるため、故障 / 破損についての対策も必要となります。

※上図は今後の新しいランサムウェア及びサイバー攻撃によって変化する可能性があります。あくまでも感染リスクを考えた場合のリスク軽減の目安として参照してください。

バックアップ保存先は通常のシステム障害だけを考慮した場合、1 箇所の保存先で十分運用ができましたが、現在では 2 箇所以上の保存先を設定するケースが増えています。また、取り外し可能デバイス / 遠隔地 ( オブジェクトストレージ他含む) を 2 次保存先とした場合、普段のオペレーションミス / ハードウェア故障などのリカバリー時には、ローカルエリア内の NAS からリカバリー処理を行うことにより、通常復旧の利便性の向上ができ、2 次保存先についてはランサムウェア / 災害発生時に非常に有効な BCP/DR 対策として活用することができます。

・バックアップ分散化構成とスケジュール

バックアップ対象が物理サーバーの場合（仮想環境も同様）




ActiveImage Protector では、マルチスケジュールに対応しているため、複数のスケジュールを作成して、スケジュール毎に保存先を別々に設定することができます。また一般的なベースバックアップ＋増分バックアップの組み合わせと、ベースバックアップのみのタスク分けも可能です。

・バックアップ対象に ActiveImage Protector をインストールしています。

・たとえば、スケジュールタスク ( 毎週土曜日にベースバックアップ＋月曜～金曜日まで毎日 1 回増分バックアップ）を作成して、1 次保存先にバックアップを行います。( 世代管理で 2 世代保持 )

・1 次保存先に付属の ImageCenter をインストールすることにより、1 次保存先に保存されたバックアップファイルを参照して即時または、別のスケジュール設定で各 2 次保存先へバックアップファイルをレプリケーションします。また 1 次保存先と同様に、世代管理にも対応しています。

・ActiveImage Protector の 1 次保存先のスケジュールタスクに追加で、タスク ( 毎月第何週目の何曜日にフルバックアップ等) を作成して、遠隔地の 2 次保存先 (A/C/D) 上図参照にバックアップを直接書き込むことができます。

・各種取り外しデバイスは複数用意してローテーションを行い、バックアップファイルを管理します。

・またバックアップファイルベース / バックアップファイルレスで、上図冗長化のようにコールドスタンバイの仮想マシンを作成することも可能です。

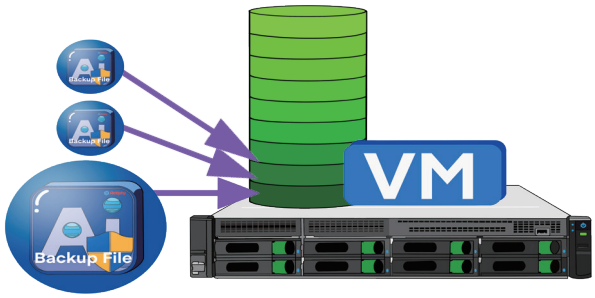
このように最低でも 2 次保存先または、3 次保存先を用意することで、バックアップファイルの分散保管が可能です。実際にリカバリーする際のバックアップファイルの選定対象も増えるため、被害が広範囲の場合でも、リカバリー成功率の大幅な向上が期待できます。

・スタンバイの動作について

ActiveImage Protector のスタンバイ機能は、バックアップファイルを作成しないで、ダイレクトにスタンバイマシンを作成する vStandby とバックアップファイルを監視して、即時 / スケジュールで作成する HyperStandby の 2 通りより実行することができます。

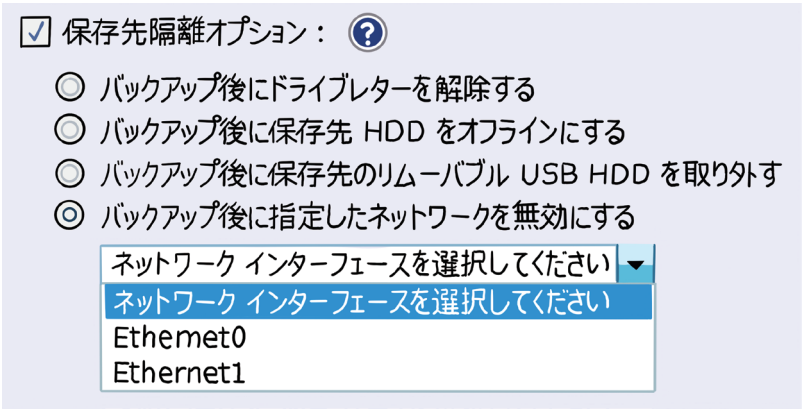
動作は永久増分方式で、初回にベースの仮想ディスク作成後、増分バックアップが動作すると、スタンバイ仮想マシンのブートポイントとして、最大 30 個までを保有することができます。軽度な感染で、ダウンタイムを短時間にしたい場合などには、少し前のブートポイントに移動して起動することにより、復旧することが可能です。

スタンバイマシンのブートポイント作成のタイミングをスケジュール設定することにより、通常の HA/FT のような同時感染から回避することが可能です。



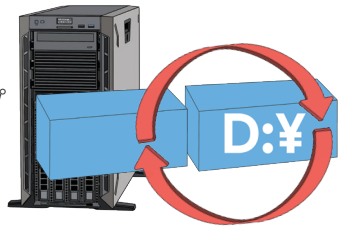
・隔離プションの使用用途

ActiveImage Protector の隔離オプションはバックアップ保存先を、バックアップ実行時以外にアクセスできない状態とします。下図のように 4 項目から選択することができます。



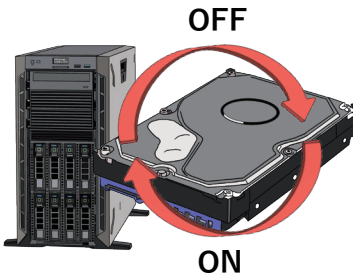

○ バックアップ後にドライブレターを解除する

バックアップ対象に接続した保存先ディスク内のボリュームについて、バックアップ終了後に自動的にドライブレターを解除します。次のバックアップ開始時に自動的にドライブレターの割当を行い、バックアップ終了後に再度解除します。



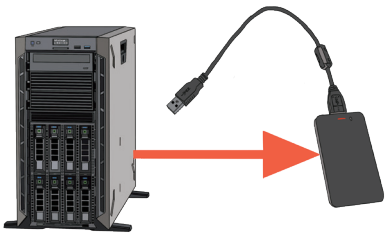

○ バックアップ後に保存先 HDD をオフラインにする

バックアップ対象に接続した保存先ディスク自体を、バックアップ終了後に自動的にオフライン状態にします。次のバックアップ開始時に自動的にオンライン化を行い、バックアップ終了後に再度オフライン化を行います。




○ バックアップ後に保存先のリムーバブル USB HDD を取り外す

バックアップ対象に接続した USB HDD/SSD をバックアップ終了後に自動的に取り外した状態とします。但し、USB 機器のため、次回バックアップ時には、USB HDD/SSD を手動で抜き差しを行い再度認識させる必要があります。

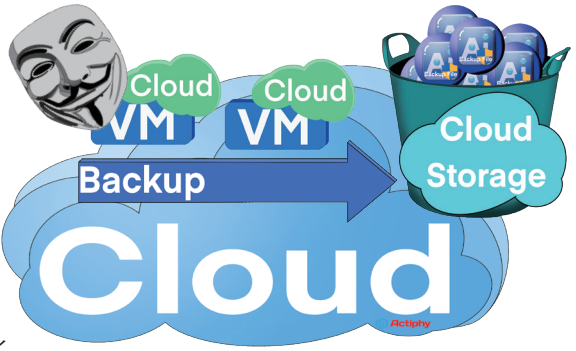


○ バックアップ後に指定したネットワークを無効にする

バックアップ対象から、ネットワーク上の共有フォルダーに接続しているネットワークカードを指定し、バックアップ終了後に自動的に無効化します。次のバックアップ開始時に自動的に有効化を行い、バックアップ終了後に再度無効化を行います。この機能では、複数のネットワークカードを装着した環境下でも、ネットワーク自体の指定を行うことが可能です。またこの機能を使用するに辺り、下図のようなネットワーク構成を推奨しています。


バックアップ対象マシンのネットワークカードの片方をバックアップ専用のセグメントに接続を行い、NAS と専用のネットワークで接続することにより、バックアップ実行時以外は NAS へのアクセスを制限できるため、通常の社内ネットワーク使用と比較して、バックアップ保存先の NAS の感染確率が下がります。

## ・クラウドサービス上の仮想マシンの保護




クラウドサービス上で稼働している仮想マシンは、ランサムウェアの感染とは無縁と考えている方もいますが、実際は感染した場合、クラウドサービス内で構成しているネットワーク環境内で感染が広がる可能性があります。
セキュリティサービスでの保護は、オンプレミス同様に最大 99.999% となるため、バックアップを行うことをお勧め致します。各種クラウドサービスには様々なセキュリティオプションもありますが、基本はスナップショットベースで、保存先は同一ネットワーク内の仮想マシン上の共有フォルダ /S3 互換などのクラウドストレージとなります。クラウドサービスで用意されているセキュリティサービスだけで、100% 防御できるのであれば良いのですが、オンプレミス環境との最大の違いは、今現在 1 番安心感のある取り外し可能デバイスでの運用が出来ません。またクラウドサービスにもよりますが、例えば S3 互換のストレージにバックアップを行った場合と、そのバックアップファイルをオンプレミスに定期的にダウンロードする際に発生するパケット費用などが、変動的に発生するため、システム運用コストの面でも導入の弊害になっているケースもあるようです。

## ・取り外し可能デバイスによるクラウドサービス上の仮想マシンの保護

クラウドサービス上の仮想マシンをオンプレミス環境に保管するメリットはあります。同一クラウドサービスの S3 互換などのクラウドストレージからダウンロードも可能ですが、S3 互換のクラウドストレージサービスの Wasabi などでは、リーズナブルな価格でパケット費用も掛からないため、経済的に下図のような構成を構築することが可能です。よりスピードを求める場合にはダイレクトコネクトで接続することにより、オンプレミス環境同等以上の速度でバックアップファイルのダウンロードを実現できます。またダウンロードしたバックアップファイルはオンプレミスの各種デバイスなどに保存も可能ですが、ActiveImage Protector を使用することにより、オンプレミス上での C2V も実現可能です。クラウドサービスとオンプレミスを組み合わせてハイブリッド型にすることにより、運用面とセキュリティ面の強化を実現することができます。

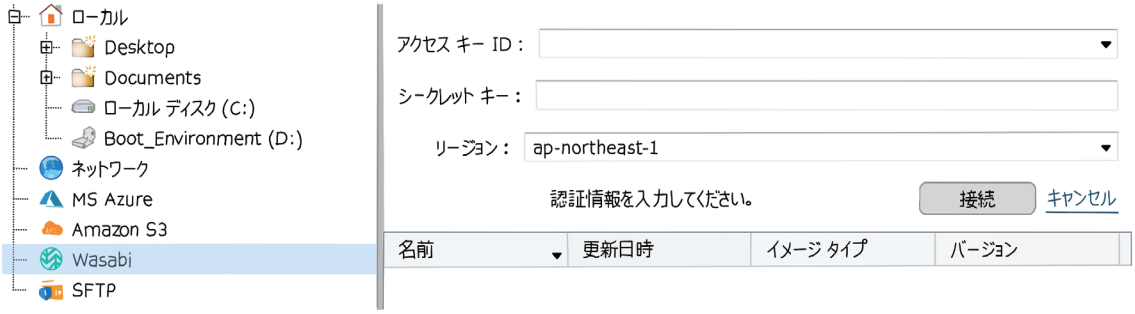

## ・Wasabi について

Wasabi は S3 互換のクラウドストレージです。

特長

・高速での読み書き / 安価な価格設定 / パケット費用不要

また ActiveImage Protector では下図のように Wasabi を使用する際の専用ボタンも用意しています。設定は「アクセスキー」と「シークレットキー」を入力してリージョンを選択するだけで、バックアップの保存先として利用可能です。




また ActiveImage Protector ではバックアップ対象から直接バックアップに加えて、1 次保存先からのレプリケーションにも対応しています。直接バックアップを行う場合についても、ベースバックアップ + 増分バックアップタスクを、ローカルエリア内の NAS の共有フォルダを保存先として利用する場合、同様に使用することができます。またセキュリティレベルを上げる、Wasabi 側のオブジェクトロック / バージョニングを有効にした場合でも、特に ActiveImage Protector 側の動作制限はありません。また Wasabi 上のバケットから、ファイル単位 / システム全体のリカバリーに対応しています。

※ActiveImage Protector のファイルリカバリーは Wasabi Japan 及びグローバルの Wasabi のみ対応しています。

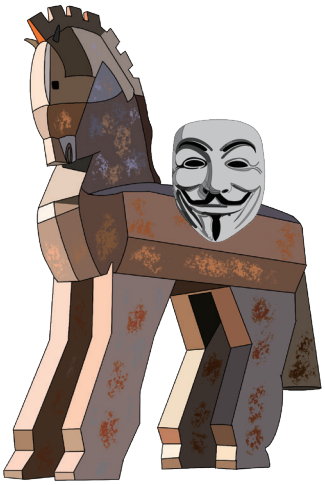
## ・ランサムウェア及びサイバーテロの被害にあった場合の復旧策

デジタル化が進んだ現代では、サーバー & クライアントシステムは企業に必要なシステムで、電子データの保管など社会的責任も高くなっています。従来のハードウェア障害 / 人的操作ミス / 災害対策に加えてランサムウェアを含むサイバー攻撃からシステムを守ることが、事業継続計画 (BCP 対策）となります。
安価なデバイスの組み合わせでも、システムの規模によっては、緊急時には非常に効果がある場合もあります。
またシステムのリカバリー方法なども事前にある程度把握することにより、システムのダウンタイムを防ぎ事業継続が容易になるため、事前の作業確認をお勧めしております。
弊社の ActiveImage Protector はお客様からのサポートを電話 / メール / チャットにて、弊社のエンジニアが直接行っております。ActiveImage Protector であれば、導入後につきましても、安心して運用して頂けます。この資料が限られた予算で効果的で現実的な対策を見直すきっかけとなれば幸いです。

ActiveImage™ PROTECTOR
**サポート**

## ・これからのランサムウェアの脅威について

ActiveImage Protector のバックアップソリューションと何のセキュリティソリューションを組み合わせるかは非常に難しい課題となります。過去のランサムウェアの場合であれば、入口対策の IPS/IDS で検知して感染を防ぐことも出来ると思われます。しかし新たなランサムウェアの場合、EDR のようなふるまいを基準とした検知が必要となりますが、全てのランサムウェアのふるまいが検知できるかについては分かっておりません。また最近ではトロイの木馬型のランサムウェアも存在し、感染から直ぐにふるまい ( 動作 ) を行わないため、検知が難しくなります。例えば、半年後に動作するようなランサムウェアの場合、バックアップファイルを取り外し可能デバイスに保管した場合でも、過去半年間の保有の場合、トロイの木馬型のランサムウェアがすでに含まれた状態になっていることも考えられます。このような事を考慮した場合、月次 & 年次といった対策も必要になるのかもしれません。お客様のシステム規模に応じたバックアップポリシーで是非ご検討頂ければ幸いです。



## ・ActiveImage Protector 2022 について

ActiveImage Protector 2022 シリーズは株式会社 アクティファイの開発製品となります。

各種製品の情報は下記よりご確認頂けます。
https://www.actiphy.com

ご評価版などにつきましては下記よりお申込みください。
https://www.actiphy.com/ja-jp/form/trial-activeimage-protector/

各種ご相談などは下記にご連絡頂ければ幸いです。
TEL: 03-5256-0877
Mail: sales@actiphy.com