Synology

ランサムウェアから組織を保護する

ランサムウェア攻撃による組織の損失は、2023年だけでも総額で8兆米ドルに及ぶと想定されています。[1] ランサムウェアやその他の形のサイバー犯罪による影響を減少させるには、素早い復元オプションを備えたデータ保護プランが不可欠です。

Date 2023年10月13日

バックアップ：災害時の最後の砦

悪意のある削除や変更によりデータが失われた場合、バックアップでミッションクリティカルなデータを復元することで、コストのかかるダウンタイムを回避できます。Synologyのデータ保護ソリューションを活用して、ITインフラ全体のバックアップ戦略を計画してください。

完璧な保護

主要なバックアップだけでなく、エンドポイントも保護することで、何層ものデータのセーフティネットを構築できます。

高速復元

即時復元オプションにより、災害発生時のダウンタイムを最小限に抑えます。

イミュータブル ストレージ

データとスナップショットに対する不正な変更を防止します。

ライセンスフリーのバックアップ

ストレージが許す限り、制限や隠れた費用無しでデータをバックアップできます。

ランサムウェアに対する一元的な保護

ワークステーション、サーバー、仮想マシン、クラウドアプリケーションなどのバックアップを一元化します。データ重複排除技術と増分バックアップ技術により、ストレージの消費量を最適化し、帯域幅のボトルネックを回避します。
https://www.synology.com/dsm/solution/infrastructure

物理的なワークロード

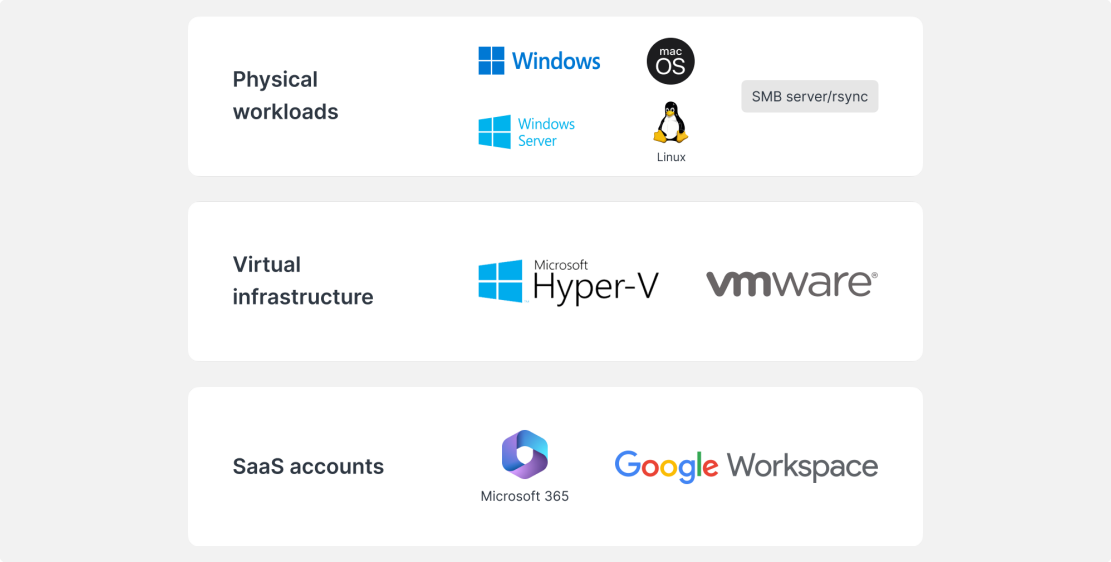
包括的なベアメタルバックアップと柔軟なファイルレベルの復元で、悪意のある攻撃からエンドポイントを保護します。

仮想インフラ

強力なデータ削減技術により、VMware® vSphere™、Microsoft® Hyper-V® VM、LUNをバックアップします。

SaaSアカウント

新しく追加されたアカウントを自動で認識し、クラウド上のデータを継続的に保護します。



効率的な復元

ローカルまたはオフサイトのSynologyシステムからバックアップを迅速に復元することで、重要な生産システムのダウンタイムを最小限に抑えます。

ゼロに等しいRTO

できるだけ早く業務を再開すべく、VMware®、Hyper-V®、Synology Virtual Machine Managerにバックアップイメージをマウントします。サービスの中断を避けるため、VMを別のハイパーバイザーに復元します。

最小のRPO

ニーズに合わせてバックアップの頻度を設定することで、攻撃を受けた際に影響が出るデータ量を最小限に抑えます。また、増分バックアップと重複排除技術により、システムを迅速に保護します。

直感的な操作

電子メール、連絡先、ファイルを復元する前に便利なポータルサイトから閲覧、プレビューすることができ、より使いやすいユーザー体験とITチームの負担の軽減を実現します。

追加の保護レイヤ

3-2-1バックアップ戦略に従って3つ目のデータをオフサイトまたはクラウドに保存することで、火災、自然災害、盗難からデータを保護します。

オフサイトのサーバーへ

バックアップを別の場所にあるSynologyサーバーに保存することで物理的な災害から保護したり、イミュータブルスナップショットを複製することでランサムウェアに対する保護を追加できます。

クラウドへ

クライアントサイドのAES-256暗号化により、不正なアクセスからデータを保護しながら、主要なクラウドストレージプロバイダーにバックアップします。

https://c2.synology.com/storage/nas

多種多様な業界からの信頼

「Synology [...] のおかげで、サーバーハードウェアのための支出が減り、 [...] インフラやワークステーションのバックアップ、システムログ、ファイル管理が非常に簡単になりました」
https://www.synology.com/company/case_study/Investortools

「Active Backup for Businessのおかげですべてのバックアップが一元化され、24時間365日利用できるようになったので、ダウンタイムを最小限に抑えて、FERPAの規制を遵守することができます」
https://www.synology.com/company/case_study/University_of_Washington

「[...] Active Backup for Businessのバックアップ速度は驚異的で、また素晴らしいデータの重複排除技術により、サーバー上の合計58TB分のデータがわずか28TBになりました[...]」
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

「[...] Active Backup for Business [...] によって、すべてのバックアップ作業を1つのコンソールで一元管理できるようになりました。また、高速で信頼性の高い復元により、ビジネスの継続性も確保されています」
https://www.synology.com/company/case_study/UNESCO

よく聞かれる質問

ランサムウェアとは？

ランサムウェアはファイルを暗号化するマルウェアの一種です。攻撃者はデータへのアクセスを回復させる代わりに身代金を要求し、支払われない場合にはデータを永久に破壊すると脅迫することがよくあります。ランサムウェアの攻撃は非常に深刻で、個人や組織に多大な経済的損失をもたらします。そのため、ソフトウェアを最新の状態に保ち、定期的にファイルをバックアップするなど、ランサムウェアから自分自身とデバイスを保護することが重要です。

今のランサムウェアにはどんな種類がありますか？

ランサムウェアには非常に多くの種類が存在し、常に新しい種類が生み出されています。ランサムウェアの代表的な種類として、以下が挙げられます。

- **暗号化ランサムウェア** — もっとも一般的なランサムウェアで、被害者のファイルを復号鍵がなければアクセスできないよう暗号化します。次に攻撃者は、鍵と引き換えに身代金を支払うよう要求します。
- **ロッカーランサムウェア** — ログイン資格情報を変えたり、メッセージを表示して被害者が自分のシステムにアクセスできないようし、コンピューターを操作不能にするランサムウェアです。次に攻撃者は、コンピュータのロック解除と引き換えに身代金を要求します。
- **Ransomware-as-a-Service (RaaS)** — 攻撃者が、攻撃を実施しようとする他の個人またはグループにランサムウェアを提供するビジネスモデルです。通常、前者がランサムウェアを提供して支払いのやりとりをし、後者は支払われた身代金の一定割合を受け取ります。
- **スケアウェア (Scareware)** — 被害者を怖がらせて身代金を払わせるために作られたランサムウェアです。これは通常、被害者のコンピューターがウィルスに感染していると主張する見せかけのセキュリティ警告やメッセージを表示します。その後攻撃者は、その感染を除去するための身代金を要求します。

ランサムウェアの被害はどのように広がりますか？

通常、ランサムウェアはフィッシングメールやコンピューターシステムの脆弱性を突いて拡散します。フィッシング攻撃では、まず攻撃者が銀行や有名企業など正規の送信元と思われるようなメールを送信しますが、そのメールに含まれているリンクをクリックすると、コンピューターにランサムウェアがインストールされてしまいます。システムの脆弱性を悪用する場合も同様に、攻撃者はシステムのセキュリティ上の欠陥を利用して、被害者が知らないうちにランサムウェアをインストールしてしまうよう仕向けます。いずれの場合も、ランサムウェアがインストールされると、同じネットワーク内にある他のコンピューターにまで瞬く間に広がります。

一般的なランサムウェアの攻撃手順はどのようなものですか？

通常、ランサムウェアの攻撃は以下の手順で行われます。

1. 攻撃者は、フィッシングメールを送信するか、またはシステムの脆弱性を悪用して被害者のコンピューターにアクセスします。
2. 攻撃者は被害者のコンピューターにアクセスできると、システムにランサムウェアをインストールします。
3. そしてランサムウェアが被害者のファイルを暗号化し、アクセスできないようにします。
4. 攻撃者は暗号化されたファイルを復号するための復号鍵と引き換えに、ビットコインのようなデジタル通貨の形で、被害者に身代金を要求します。
5. 被害者が身代金を支払えば、攻撃者は復号鍵を提供し、被害者は再びファイルにアクセスできるようになります。しかし、攻撃者が実際に鍵を渡す保証はなく、仮に渡してくれたとしても、被害者のファイルは暗号化処理の影響を受けて損傷したり、破壊されている可能性があります。

この手順には多くの種類が存在し、すべてのランサムウェア攻撃が同一の手順に従うわけではないことに注意してください。例えば、ファイルの暗号化を全く行わない攻撃もあれば、恐喝行為やブラックメールのような方法をとるものもあります。

どのようにしてランサムウェアに感染するのですか？

ランサムウェアに感染する方法はいくつかあります。最も一般的な方法は、フィッシングメール内の悪意あるリンクや添付ファイルをクリックしてしまうことです。この手のメールのメールアドレスは正式なものに見えるよう作られており、有名な企業や組織から送信されていると思わせます。メールに記載されているリンクや、添付ファイルをクリックすると、コンピュータにランサムウェアがインストールされます。 ランサムウェアに感染するもう1つの方法は、乗っ取られたウェブサイトにアクセスすることです。これらのウェブサイトは攻撃者によってハッキングされているため、サイトにアクセスした人のコンピュータに自動的にランサムウェアをインストールするコードが埋め込まれています。 また、ランサムウェアに感染したファイルをインターネットからダウンロードすることで自身も感染してしまうケースもあります。これは、怪しいウェブサイトからファイルをダウンロードした場合や、知らない人から共有されたファイルをダウンロードした場合などで起こります。 つまり、インターネットを閲覧する際には細心の注意が必要で、見慣れないリンクをクリックしたり、ファイルをダウンロードしたりしないことが重要です。これにより、ランサムウェアやその他の種類のマルウェアに感染するのを防ぐことができます。

ランサムウェアのターゲットは誰ですか？

インターネットに接続されたコンピュータやその他の機器を使用している人なら、誰でもランサムウェア攻撃の標的になる可能性があります。しかし、その中でも特に標的になりやすいユーザー層として、企業や組織が挙げられます。これは、企業がより価値のあるデータを保有しており、身代金を支払ってでもデータを取り戻そうとする可能性が高いためです。また、病院や教育機関など重要なサービスを提供している組織も、ランサムウェアによって業務が中断されると人々の生命が危険にさらされる可能性があるため、頻繁に狙われるターゲットとなります。 個人もランサムウェア攻撃のターゲットになります。その場合、攻撃者は身代金が支払われない限り、個人ファイルを削除したり、機密情報を公表すると脅迫したりして、被害者から金銭を脅し取ろうとすることがあります。 ランサムウェアの攻撃対象は、データの価値と、データを取り戻すために身代金を支払う意思があるかどうかを基準に選ばれることが一般的です。

ランサムウェアに支払いをするリスクはありますか？

ランサムウェアの攻撃者に身代金を支払うことは、ファイルを取り戻すもっとも簡単な手段に思えるかもしれませんが、実は非常に危険な判断です。身代金を支払うことで、以下のようなリスクが生じます。

- 攻撃者が実際に復号鍵を提供する保証はありません。多くの場合、身代金を支払っても鍵を受け取ることはできず、被害者はファイルにアクセスできないままです。
- 身代金を支払うことで、攻撃者は更に要求してくる場合があります。攻撃者は被害者に身代金を支払う意思があることがわかると、今後さらなる攻撃を仕掛けてくる可能性が高まります。
- 身代金を支払うことは、今後もターゲットとして狙われることに繋がります。身代金を支払う意思が攻撃者に伝われば、将来的に標的となる可能性が高まります。
- 身代金を支払うことが違法となる場合もあります。場合によっては、犯罪集団に身代金を支払うことで、テロやその他の違法行為に資金提供をしているとみなされることがあります。

身代金を支払うことは、ファイルを取り戻すためのもっとも簡単な方法のように思えるかもしれませんが、実際には非常に危険な決断となる可能性があります。リスクをよく検討した上で決断することが大切です。

ランサムウェア被害における被害額はいくらですか？

ランサムウェア攻撃の被害額は、使用されたランサムウェアの種類、暗号化されたファイルの数、攻撃の有効性など、さまざまな要因によって大きく異なります。場合によっては、ランサムウェア攻撃による身代金がほんの数百ドル程など、被害が小さなものもあります。一方、被害者のファイルアクセスを妨げるために、攻撃者が数千ドル、あるいはそれ以上の金額を要求するケースもあり、被害額が非常に高額となることもあります。 身代金の支払いに伴う直接的なコストに加え、ランサムウェア攻撃は間接的にも大きな被害をもたらします。例えば、ランサムウェアの攻撃によりシステムにダウンタイムが発生し、生産性が低下することで、収入や所得が失われる可能性があります。また、企業の評判や顧客の信頼が損なわれ、ビジネスに長期的な悪影響が及ぶ可能性もあります。こうした間接的なコストは、身代金そのものよりもはるかに高額になることが多いのです。

ランサムウェア攻撃による症状はどのようなものですか？

ランサムウェアの攻撃による症状は、使用されるランサムウェアの種類によって異なります。しかし、一般的な症状には以下のようなものがあります。

- 自分のファイルが暗号化され、アクセスできない
- 攻撃者から、復号鍵と引き換えに身代金の支払いを要求するメッセージを受け取った
- 自分のコンピュータで見知らぬプログラムやプロセスが実行されている
- コンピュータの動作が遅い、または応答しない
- コンピュータに見慣れないエラーメッセージやポップアップウィンドウが表示されている

自分のコンピューターがランサムウェアに感染したと疑われる場合、迅速な行動が重要です。インターネットからコンピューターを切断し、ランサムウェアの広がりを防いでください。

ランサムウェア攻撃を防止する方法は？

ランサムウェア攻撃から身を守るために、以下のような対策があります。

- 信頼できるアンチウイルスやセキュリティソフトウェアを使用し、常に最新の状態を保持してください。これにより、コンピューターがランサムウェアやその他のマルウェアに感染することから防ぎます。
- メールの添付ファイルやリンクを開く際には注意が必要です。ランサムウェアは、フィッシングメールによって拡散されることが多いため、クリックをする内容に十分注意することが重要です。
- お使いのオペレーティングシステムやその他のソフトウェアは、常に最新の状態を保持してください。ソフトウェアアップデートには、ランサムウェアやその他の脅威からコンピューターを守るセキュリティパッチが含まれている場合があります。
- ファイルを定期にバックアップしてください。これにより、万が一コンピューターがランサムウェアに感染しても、データを保護できます。3-2-1バックアップ戦略など、推奨されるバックアップ戦略を実行してください
- ランサムウェアのリスクに留意し、その脅威についての情報を組織の人々と共有してください。これにより、ランサムウェア攻撃の被害を防ぎ、被害発生時にも素早く検出、対応できます。

ランサムウェアの攻撃を防ぐ最善の方法は、常に警戒を怠らず、コンピュータとデータを保護するための措置を講じることです。これにより、ランサムウェア攻撃のリスクを軽減し、万が一攻撃が発生した場合でも簡単に復旧できます。

Synology はどのようにしてランサムウェアからデータを保護するのですか？

ランサムウェアの被害に遭わないようにするには、予防措置が不可欠です。お使いのアンチウイルス ソフトウェアに加えて、これらの Synology ソリューションを使用してください。

- **アクセスの防止** — ファイルやアプリケーション、アクセスに対する権限を設定し、Secure SignInおよびC2 Passwordを用いて安全なログイン資格情報を設定することでランサムウェアの広がりを減らします。
- **デバイスの保護** — 古いシステムには大きなリスクがあります。使用しているすべてのNASを、Synology Central Management System (CMS)でアップデートし、Synology Directory ServerおよびC2 Identityでのグループポリシーを用いてその他のデバイスを保護します。
- **疑わしいファイルは開かない** — 疑わしいファイルを含むスパムメールやフィッシングメールは、ランサムウェアの拡大のための常套手段です。Synology MailPlusは、強力なアンチ マルウェア保護とスパム防止機能をもっています。
- **脆弱性のチェック** — Synology Security Advisor を用い、マルウェアや脆弱性、異常なログイン行動を定期的にスキャンします。推奨される変更を導入することで、NAS のセキュリティを高めます。 https://www.synology.com/dsm/overview/security

データを保護する数々の手段

本体の管理

データへのアクセス権限、ソフトウェアの状態、システムの健全性などを一元管理する豊富な機能を活用できます。
https://www.synology.com/dsm/overview/administration

すべてのシステムの監視

デバイスがどこにあっても、不審なログイン操作の特定、アップデート管理、デバイスの健康状態を監視します。
https://www.synology.com/dsm/feature/active-insight

データの安全な保護

3-2-1バックアップ ルールに従い、偶発的および、悪意のある変更や削除に対抗してデータを保護します。
https://www.synology.com/dsm/solution/data_backup

始めましょう

お問い合わせ先

詳細は各地域の営業部門にお問い合わせください
https://www.synology.com/form/inquiry/sales

取り扱い販売店

お近くのSynologyパートナーをお探しください
https://www.synology.com/wheretobuy

注意事項：

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

ランサムウェアから組織を保護する

https://www.synology.com/ja-jp/dsm/solution/ransomware

Synology ウェブサイト

https://www.synology.com/

お問い合わせ先

https://www.synology.com/company/contact_us