FUJIFILM
Value from Innovation

HORISON
Information Strategies

Fred Moore, President
Horison.com

ハイパースケールストレージシリーズ

テープ エアギャップ

サイバー攻撃からデータを守る

データ保護の目的は、システム障害や人的ミスからのリカバリを目的としたデータバックアップから、急増するサイバー攻撃への対策へと、状況が進化しています。長年にわたって、ハードウエアとソフトウエアの信頼性レベルと耐性レベルは大幅に改善されてきましたが、セキュリティは人間の問題であり、サイバー攻撃を起こすのは人間です。今や、データ保護において、サイバー攻撃は最大の脅威となっています。匿名の個人が他人の価値あるデジタルデータから利益を得ようとしており、リスクは大きくなる一方です。サイバー攻撃がなくなる可能性は極めて低く、データ保護とサイバーセキュリティの統合は、急速に進み、高い代償を払わねばならなくなるランサムウェアをはじめとしたサイバー攻撃の急増に対抗しようとしています。

サイバー攻撃の増加によって、エアギャップストレージソリューションは、デジタルデータ保護の重要な構成要素に位置付けられるようになりました。データに「テープエアギャップ」を適用するとデータをハッキングできなくなり、ストレージ環境が大きいほど、その効果が高まります。

ハイパースケールデータセンター(HSDC)とは、大規模データセンターのことであり、その多くはクラウドサービスプロバイダー(CSP)です。数百もの顧客の重要なデータ資産について、セキュリティの全責任をHSDCが負うことはできません。大容量の重要データを含むクラウドストレージ環境を狙うサイバー脅威が急速に増えている今、このことが大きく懸念されているのです。

2020年のサイバー攻撃のシナリオ

デスクトップからクラウド、HSDCに至るまで、サイバー攻撃の影響を受けないコンピューターシステムはありません。マルチクラウド環境は、さまざまなCSPから希望のサービスを選択できるため、多くの組織で好まれていますが、拡大し続けるこのマルチクラウド環境が原因となり、新しいリスクが生じています。

サイバー攻撃の60%以上はEメールによってもたらされ、そこからコンピューターのHDDやSSDへ感染します(しかしエアギャップのあるテープには決して感染しません)。サイバーセキュリティの脆弱性はセキュリティ企業、政府機関、ソフトウエアベンダー、ハードウエアベンダー、エンドユーザーに見抜けていない場合があります。エンドポイントセキュリティ、ファイアウォール、VPN、および認証システムは、ほぼすべてのシステムに備わっていますが、これらのセキュリティレイヤーで、組織に必要な持続可能かつ十分な防御を備えた対サイバーセキュリティを、本当に実現できるでしょうか。残念ながら、ハッカーはこうしたセキュリティレイヤーすべてに対して、組織にそのまま侵入できるバックドアを作成してしまいます。また、毎年1,110億を超えるソフトウエアコード行が新たに作成されており、話題のIoT(モノのインターネット化)により2025年までにエンドポイント数が4,000万を超えると推定されています。これにより、数えきれないほどの脆弱性が新たに生まれ、悪用される可能性があります。まさにサイバー攻撃の嵐というわけです。

Key Point

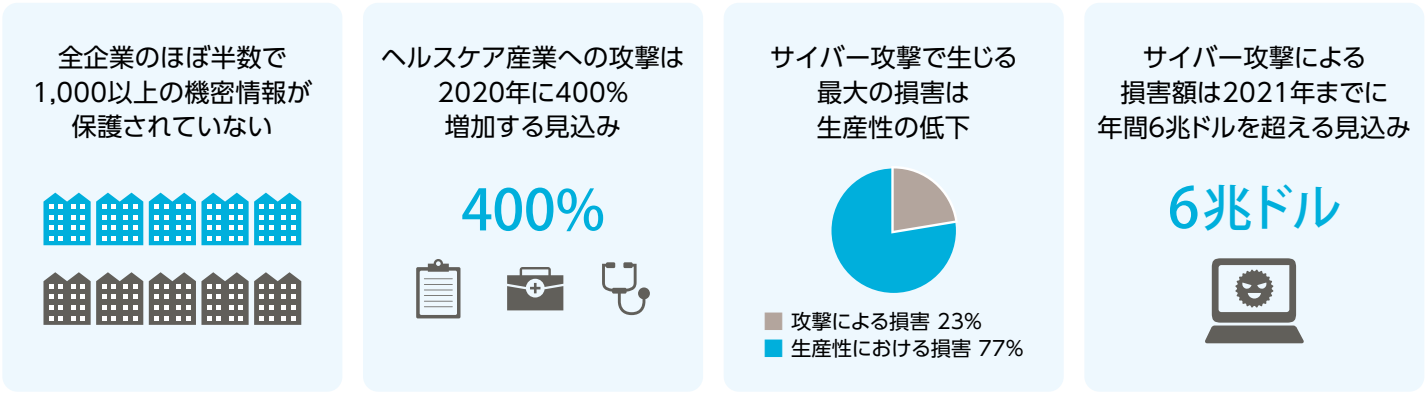
HSDCにとって、クラウドセキュリティは、適切なレベルのデータセキュリティ制御を顧客が実装できるかどうかに大きく依存します。特に、マルチクラウドストレージソリューションの場合は、これが当てはまります。

サイバーセキュリティに関する高まる課題

サイバー攻撃による被害を過小評価してはならないのは下記の統計から明らかです。

- 全世界のサイバーセキュリティ関連コストは、2022年までに1,330億ドルに達すると予測されている。(出典:Varonis)
- 電子メールに組み込まれたURLは依然としてコンピューターがウイルスに感染する最大の要因。(出典:Safety Detectives)
- ハッカーによる攻撃頻度は39秒に1回、つまり1日に2,244回に達する。(出典:Varonis)
- 2020年までに、ユーザーおよび機械が生成するパスワードの数は全世界で3,000億個にまで増加する見込み。(出典:Cybersecurity Media)
- 2019年、ランサムウェア攻撃で生じた平均損害額は14万1,000ドル、損害額合計は115億ドル。
- 金融サービス業界は、1企業あたり平均1,830万ドルの損害額を被っており、サイバー犯罪による損害額が最も高くなっている。(出典:Accenture)
- サイバーセキュリティ関連の人員は2021年までに全世界で350万人不足する見込み。(出典:Cybersecurity Ventures)
- サイバー犯罪による侵害の件数は2024年までにおよそ70%増加する見込み。(出典:Security Boulevard)
- サイバー犯罪による損害額は2021年までに年間6兆ドルに達する見込み。(出典:Cybersecurity Ventures)

■サーバーセキュリティに関する統計(2019年)



サイバー犯罪者は、新型コロナウイルスの世界的流行により始まった「新しい生活」に潜むさまざまなリスクに入り込もうとしています。多くの会社員が在宅勤務をしており、従来のオフィスネットワークの境界外で、ハイブリッドのWFH(Work-From-Home)ネットワークを使用しています。この新たに拡大した混在の仕事環境で、企業ネットワークやWiFiネットワークを共有すると、家族や学校に通う子どもがウイルスベクターとなって感染が他の機器に容易に広がることになり、ネットワーク全体に簡単に広がってしまう可能性もあります。新型コロナウイルスの世界的流行は、サイバー犯罪者にとって望ましい状況になっているのです。サイバー犯罪者は、新型コロナウイルスに対する人々の恐怖心を利用して、エンドポイントにまで広がっているセキュリティ脆弱性を悪用しています。ハイブリッドのWFHネットワークがクラウドにバックアップされている場合は、セキュリティがさらに複雑になります。

ハイブリッド環境はニューノーマルとなりつつあるのでしょうか。こうしたハイブリッド環境では、全体でセキュリティが確保できる、統合型のサイバーインフラを構築することが重要になります。従来は信頼できるデバイスや信頼できるIPアドレスに重点が置かれていましたが、この点は変えなければならなくなるでしょう。ニューノーマルでは、ストレージ企業はセキュリティを後付けやアドオン機能として扱うのではなく、セキュリティを考慮しながらシステムを設計することになります。デバイスセキュリティの重要性は、エッジコンピューティングなど従来型のユーザーではない環境、特にIoTで最も高まります。

Key Point

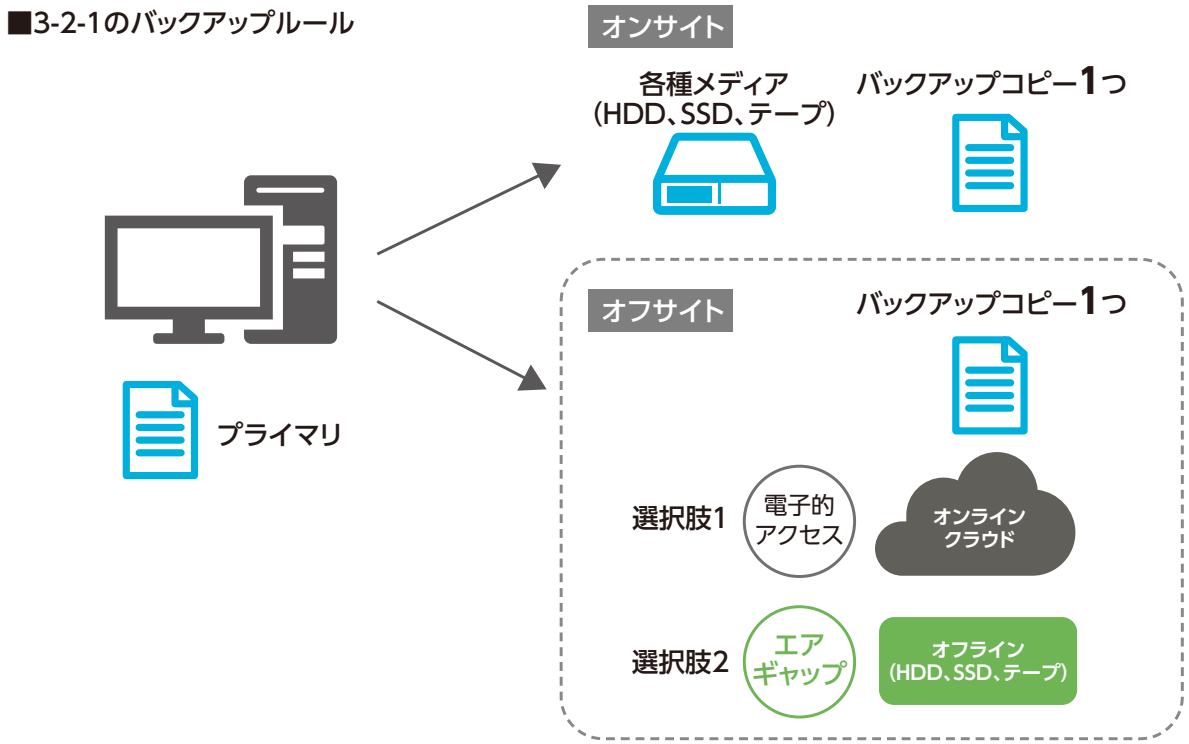
サイバー攻撃の課題は高まり続けており、データ資産が最大の脅威にさらされています。HSDCでは、さまざまな企業にストレージサービスを提供しており、セキュリティが極めて高いストレージインフラを提供することが必要となっています。

最適なバックアップ戦略

サイバー攻撃が世界的に拡大する中で、ITの基本概念において、データバックアップの役割が大きくなっています。バックアップは重要ですが、1つのバックアップコピーだけでは十分でない場合があります。最適なバックアップ戦略では、3-2-1のバックアップルールが黄金律として導入されています。

このルールでは、企業は3つのバックアップコピーを2つの異なるメディアタイプに配置し、そのうち1つをオフサイトに保存する必要があるとしています。オフサイトにデータコピーを保存するには、オンラインコピー（電子的アクセス）とオフラインコピー（エアギャップまたは手動アクセス）の2つの方法があります。バックアップコピーをローカルとオフサイト（物理的）またはクラウドの両方に保存することにより、予期しないイベントや災害が発生した場合に備えてデータを二重で保護できます。

これらのどちらの手法でも、データボルトおよびCSPを使用できます。また、どちらの手法でも、一般的なデータセンターと同様に、バックアップストレージに同じSSD、HDD、そしてエアギャップ環境となるテープを使用できます。



「テープエアギャップ」によるサイバー攻撃からの保護

通常、従来のバックアップデータとアーカイブデータは、ローカルに保存されるか、クラウド環境に保存されます。それに対して、サイバーレジリエンスを備えたデータコピーは、さらに厳しい追加の要件を満たしていなければなりません。これは、「エアギャップ」とテープ技術が躍進を遂げ貢献している領域です。サイバー攻撃の増加によって、テープに保存されたデータのオフラインコピーやクラウドコピーの保護がより重要になっており、これがいわゆる「テープエアギャップ」です。「テープエアギャップ」は、ロボティクスライブラリーまたはテープラック内で電子的に切断または分離されているデータコピーのことであり、バックアップ、アーカイブ、その他のデータコピーに対するサイバー犯罪者の攻撃を防ぎます。ネットワークに接続されていない通常の状態では、テープに保存されているデータをハッキングすることはできません。また一般に、テープであればWORM（Write Once Read Many）機能でアーカイブデータを保存するので、一回書き込めば変更することはできません。この書き込み保護により、データは変更不可能であること、および、いったんデバイスに書き込まれたデータは変更できないことが保証されます。

テープメディアは、テープドライブにマウントされている場合にのみオンラインになります。ドライブにマウントされていない場合は

すべてのシステムから電子的に切断され、エアギャップによって保護されます。一方、HDDとSSDは常にオンラインになっており、ハッカーがアクセスできるため、サイバー犯罪による感染の最初の侵入地点になります。CSPとHSDCでは、バックアップデータとアーカイブデータにテープシステムを実装すれば、即座に保護が実現します。CSPの顧客は、CSPにエアギャップ保護を求めることで、最高レベルの保護サービスを確実に受けることができます。

Key Point

増え続けているHSDCにとって、ランサムウェア攻撃に対抗できる確率を上げるには、プロアクティブな災害復旧計画を策定するしかありません。テープエアギャップのストレージシステム実装が、サイバー攻撃に対するセキュリティを最も簡単に強化する方法となります。

攻撃ループがサイバー攻撃やランサムウェアからの保護をより困難に

デジタル脅迫は新しいものではありませんが、2019年に行われた調査ではサイバーセキュリティの専門家582人のうち50%が、所属組織ではランサムウェア攻撃を防御する準備ができていないと回答しています（出典:Pwnie Express）。
ランサムウェアは、クリプトウイルスを使用した一般的なデジタル脅迫の手法であり、ファイアウォールとマルウェア対策ツールの裏をかき、特定のユーザーのファイルを暗号化することによりシステムの画面をロックします。通常、ランサムウェア攻撃は、エンドユーザーがWebサイトリンクをクリックするか、フィッシング（ランダム型）やスピアフィッシング（標的型）など悪質な電子メールに添付されたファイルを開くことで実行されます。
これらの攻撃では、このような遅延型の検知されないマルウェアがオンラインのファイルに埋め込まれ、マルウェアは潜伏状態になり、ものによっては再びアクティブになるまで数カ月潜伏します。その間、マルウェアは気づかれることなくバックアップデバイス（通常はテープ、HDD、クラウド）にバックアップされてしまいます。そして、遅延型のオンラインマルウェアのアクティブ化によってファイルが無効化された後で、攻撃前のバージョンのバックアップがリストアされると、HDDまたはテープに保存されていたリカバリデータによってランサムウェアがシステムに再び入り込んで、全体のデータが再び無効化されて、終わりのない攻撃ループが生じます。このように、データがリカバリされるとランサムウェアが再び注入されるため、バックアップファイルのリストアが無意味になります。一般に、攻撃のループは解読キーと交換にランサムウェアの身代金が支払われるまで続き、通常は匿名の仮想通貨口座が振込先に使用されます。
幸いなことに、攻撃ループ防御ソフトウエアの提供が開始されています。これらのソフトウエアは、バックアップリポジトリーへの侵入時に悪意のあるコードを識別して隔離し、オンライン環境へのリカバリの前にも、悪意のあるコードを無効化します。高度な攻撃ループ防御ソフトウエアでは、自動化された自己学習型のAI戦略やML戦略を取り入れ始め、検出機能が向上しています。「テープエアギャップ」と併用することで攻撃ループを防ぐベストオプションを提供しています。今後数年にわたってこのソフトウエア技術の大幅な進歩が期待され、ランサムウェアを防ぐために、こうした技術の発展がサイバーセキュリティソフトウエアに密接に統合されると期待されています。
HSDCやCSPのクラウドストレージインフラは、本質的にランサムウェアの影響を受けずにはいられません。ランサムウェア攻撃が増加するにつれて、顧客は、企業を保護するためにできることは何か、と考えています。これに対する自然な対応として、クラウドストレージベンダーとバックアップベンダーは、攻撃ループ防御ソフトウエアとハードウエアの「テープエアギャップ」技術をランサムウェアの脅威に対抗するためのソリューションとして位置付けています。

Key Point

ランサムウェア攻撃は、過去2年間で97%以上増加しています（出典:Phishme）。「テープエアギャップ」と攻撃ループ防御ソフトウエアを利用することで、サイバー犯罪に対する防御を強化できます。

まとめ

今日の世界は、日を追うごとに世界中とオンラインでつながれるようになっています。しかし、そのメリットと引き換えに、盗難、詐欺、悪用のリスクも大幅に増大しています。サイバー攻撃に対処するためには、HSDC、CSP、およびすべての組織が各自のデータ保護戦略を評価し直さなければなりません。エアギャップソリューションを、データ保護戦略に不可欠な構成要素とするのが理想的です。こうした堅牢なセキュリティ計画を策定していないHSDCやCSPは、いつでも身代金を支払えるように仮想通貨口座を作っておかないと大変なことになります。

「テープエアギャップ」は、データ保護の最終的な防御策として活用できます。犯罪者は、ネットワーク経由、あるいは他の電子的リンク経由でアクセスできないものを削除したり暗号化したりすることはできないからです。暗号化、WORM、そして「テープエアギャップ」を併用することで、テープによる最高レベルのハードウエアデータ保護が得られます。セキュリティ上の新たな課題が日々生じる中で、増大する脅威に対抗するため、データ保護とサイバーセキュリティの統合が日々進められています。サイバーセキュリティ戦略を効果的かつ継続的に進化させることで、企業は脅威を軽減することができるのです。

FUJIFILM
富士フイルム株式会社　記録メディア事業部　〒107-0052 東京都港区赤坂9-7-3　TEL.03-6271-2084　FAX.03-6271-2185

「データアーカイブソリューション dternity」の情報はこちら