Acronis

21世紀のヘルスケア業界の課題に対応するサイバープロテクションソリューション

ヘルスケア技術専門家はサイバー脅威の新時代にいかに機密データを保護できるのか

ヘルスケア業界では、大規模なデジタルトランスフォーメーション進んでおり、患者情報を旧式の方法で保存することから、新しいデータ集中型の診断・治療アプリケーションへの移行が進んでいます。同時に、ヘルスケア機関は利益を増加させ、プライバシー規制を遵守し、患者ケアを最適化し、支払人、サプライヤー、サービス提供パートナー、学術機関及び患者との相互運用性を改善するという膨大な圧力にさらされています。

大量のヘルスケアデータが物理的な場所、コンピューティングデバイスおよびネットワーク（プライベートとパブリックのクラウドを含む）を通じて増化・拡散しています。遠隔医療や遠隔患者監視、仮想・拡張現実ベースのトレーニングなどの新しい重要なヘルスケアアプリケーションは、さらに大量のデータを生み出してしています。人工知能（AI）、モノのインターネット（IoT）、ブロックチェーンのような新しい技術も状況を多様化させており、多くのユーザーがデータにアクセスしています。

一方、業界はプライバシー侵害、ランサムウェア攻撃、クリプトジャッキングキャンペーンのような多数のサイバー脅威に悩まされています。ヘルスケアデータの可用性、アクセシビリティ、プライバシーを維持するのがこれまでになく複雑になっています。

サイバー犯罪者や敵対的国家は、ヘルスケア業界を攻撃目標に定めており、ランサムウェアのようなマルウェア攻撃が機密データへのアクセスが生死を分ける問題に直結するという恐怖を悪用します。

ランサムウェア攻撃を受けた医療機関には英国の NHS や Hancock Health、Adams Memorial Hospital、MedStar Health、Erie County Medical などが含まれます。医療セクターのデータ漏洩は、頻繁に聞かれるニュースとなっており、多数の機密患者記録と支払記録が毎年盗まれています。

また、米国医療保険の携行性と責任に関する法律 (HIPAA)、欧州連合の一般データ保護規則（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）などの州レベルのプライバシー規制を含むプライバシー規制に注力するコンプライアンス当局の注目も集めています。業界当事者もクレジットカードデータ保護基準（PCI DSS）のようなクレジットカード規制基準に違反するリスクがあります。

患者に関する電子データへの依存が高まるにつれて、無停止可用性の重要性が増しています。ダウンタイムによって引き起こされる、患者の安全性に対する明らかな脅威に加えて、医療機関の存続が脅かされるほどのコストがかかる可能性もあります。Gartner の 2014 年 2 月 28 日付けの「データセンターの災害復旧計画のダウンタイムコストカルキュレータ」によるとダウンタイムの平均コストはあらゆる種類の企業で分当たり $5,600 で時間当たりに直すと約 $300,000 です。

こうした課題に直面しつつ生き残るには、下記に示すサイバープロテクションの 5 つのベクトルの上に構築されたデータを守るための新しいアプローチが必要です。

SAFETY（セーフティ）

信頼できるデータのコピーが常に利用できることを保証

ACCESSIBILITY（アクセシビリティ）

いつでもどこでも簡単にデータを利用できるようにする

PRIVACY（プライバシー）

データに対する可視性とアクセスを管理

AUTHENTICITY（真正性）

コピーが、元のデータとまったく同じであることのゆるぎない証明を作成

SECURITY（セキュリティ）

データ、アプリケーション、システムを悪意ある脅威から保護

Information Technology Intelligence Consulting は、**98% の企業に 1 時間のダウンタイムで $100,000 以上のコストが生じ、大企業の多くでは $100 万～ $500 万となっています。**

一方、医療機関の IT 部門は増大するインフラの複雑さ、能力のあるスタッフの採用と継続的雇用の難しさ、実行中のアプリケーションのプライベート、パブリッククラウドへの移行、スマートフォンやタブレットなどのモバイルデバイスの増加、IoT センサー、アセットトラッカー、ウェブカメラの出現、新規データのリアルタイム分析の必要性などといった、すべての業界と共通する課題にも悩まされています。

本文書では、以下に示すヘルスケア業界の 7 つの主要な観点からこうした基本的サイバープロテクションの原則を精査します：

1. **データ漏洩**対策
2. **ランサムウェアやクリプトジャッキングのような**マルウェア脅威に対する保護
3. コンプライアンス要件に**準拠**
4. パブリックおよびプライベートクラウドへの**移行**
5. データ可用性を常に**提供**
6. モバイルデバイスの**使用**
7. インフラをシンプルに保ちデータ保護を**強化**

ヘルスケア IT の状況

データ保護とセキュリティは依然として今日のヘルスケア組織の最優先事項です。データ漏洩の調査において、サイバーセキュリティ企業の Protenus はヘルスケア業界の攻撃ペースが2017年には1日当たり1件以上だったと伝えています。

同じ年に、560 万件の患者記録が漏洩し、組織が漏洩の発生に気づくまでに平均 308 日を要しています。

ヘルスケア業界でのデータ漏洩件数を削減するには、物理システム、仮想マシン（VM）、クラウドデバイスおよびモバイルデバイスを取り巻く IT インフラのセキュリティを階層化する必要があります。基本的な対策には、エンドポイントでのマルウェア対策、ファイアウォールによる外部ネットワークの脅威に対する防御、社内ネットワークへの攻撃拡散を制限する vLAN やソフトウェア定義ネットワークによるネットワークのセグメント化などが含まれます。バックアップやディザスタリカバリによるデータ保護は、機密データが攻撃によって損害を受けたり、破壊されたり、アクセスを拒否された場合に不可欠なものになります。これを実現するには、オンプレミスとクラウドの両方でセキュアで完全に暗号化されたバックアップとストレージを用意する必要があります。

マルウェア脅威

大半のセキュリティ研究者によると、ヘルスケア業界に影響を及ぼし、最近の数年間で最も蔓延しているマルウェアはランサムウェアとクリプトジャッキングの 2 つです。

ランサムウェアはヘルスケアのサーバー、デスクトップ、モバイルデバイスを感染させ（通常、ユーザーが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することで感染）、あらゆるファイルを手当たり次第に暗号化し、被害者のファイルの復号化に必要な解読キーの代償にオンラインでの金銭の支払いを要求します。ランサムウェア攻撃を検出して阻止する対策がない場合や、最新のバックアップから復元できない場合、多くのヘルスケア組織は患者の生命を脅かし、生産性低下や修復コストが何百万ドルもかかるダウンタイムに苦しむことになります。

クリプトジャッキングはそれほど知られていませんが、増加中のサイバー攻撃で、感染したヘルスケアマシンがボットネット内でゾンビになり、サイバー犯罪者向けに暗号通貨をマイニングします。マルウェアは被害者からコンピューティングサイクル、メモリ、電力、冷却能力などのリソースを盗むだけですが、エネルギーコストやシステムの摩耗が増加します。さらに、クリプトマイニングマルウェアはランサムウェアのようなその他の脅威を感染先のシステムに注入することがよくあります。

コンプライアンス要件

ヘルスケア業界の規制当局の調査は、ランサムウェアのようなマルウェアを使用するサイバー犯罪者の格好の標的になるのを助長しています。機密の患者データがランサムウェア攻撃によってロックされることで引き起こされるコンプライアンス違反のリスクによって、被害者がデータへのアクセスを取り戻すために支払いを強要される可能性が高まります。

2 年連続でランサムウェア攻撃は**ヘルスケアセクターにおけるすべてのマルウェアインシデントの 70% 以上を占めています**（「2019 年 Verizon 漏洩調査レポート」による）。

アプリケーションおよびストレージのクラウドへの移行

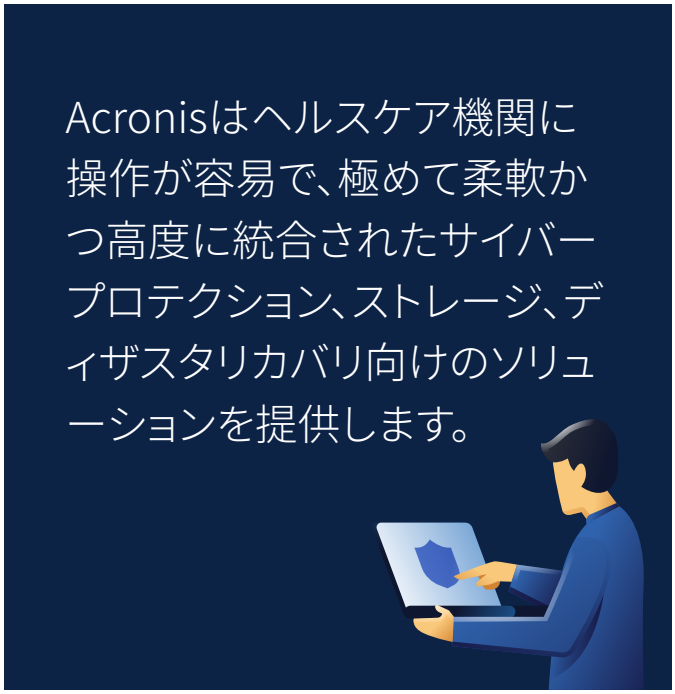
ほとんどの業界と同様にヘルスケア業界は中核となるアプリケーションやデータをパブリックやプライベートのクラウドインフラに移行している最中です。その目的は、コストや商用減価償却資本資産を予測可能なサービスコストに低減し、データのアクセシビリティを改善して任意のロケーションとデバイスで共有できるようにすることです。
しかし、多くの機関ではデータプライバシーと規制に対するコンプライアンスを維持しながらストレージとデータ保護リソースをクラウドに安全に移行する上で、問題が発生しています。

2 年連続でランサムウェア攻撃はヘルスケアセクターにおけるすべてのマルウェアインシデントの 70% 以上を占めています（「2019 年 Verizon 漏洩調査レポート」による）。

データ可用性

ヘルスケア業界は高度なデータ可用性を継続することを重視しており、患者の健康と生存はデータ可用性にかかっていると言っても過言ではありません。

バックアップとリカバリの点から見ると、これを実現するには、ヘルスケア IT 専門家が目標復旧時点（RPO）と目標復旧時間（RTO）という 2 つの指標に十分注意する必要があります。RPO はある特定時点でどれほどの情報を失う余裕があるかを意味します。実際には、重要なデータのバックアップ頻度を定義します。RTO はデータ障害イベントとリカバリ正常終了までの時間、つまり、機関が耐えられるダウンタイムの長さを意味します。ほとんどの機関は、より厳しい RPO と RTO が必要なアプリケーションはどれか、そして、より大きなデータ損失や長時間のリカバリタイムに耐えられるものはどれかを容易に識別できます。



BYOD のリスク

ヘルスケアでのユビキタスな従業員所有デバイスの登場は業界に、スタッフの生産性やコラボレーションの向上といった飛躍的なメリットをもたらしています。しかし同時に、容易に侵入されたり、紛失したり、盗難されたりする個人のデバイスに機密データが保存される可能性が高いため、データ保護の問題になってもいます。

サイバープロテクションの簡略化

多くの業界と同じようにヘルスケア業界の IT マネージャーは優れたオペレーションスタッフを集めるのに苦労しているため、オペレーションを簡略化するのが最優先事項になっています。これはデータ保護のような日常的なオペレーションで特に重要です。複数のシステムをデプロイしてさまざまな IT 環境を管理し、その運用に高度なスキルを有するエンジニアを採用することが最適であるとは言えません。

ACRONIS はヘルスケア業界向けにサイバープロテクションソリューションをいかに提供するか

Acronis は複数の方法でデータ漏洩に対する保護を提供します。Acronis Cyber Backup は転送中および保存時に機密データの暗号化を行い、データ漏洩が成功した場合でもサイバー犯罪者が漏洩データを使用できないようにします。

また、Acronis Cyber Backup では、サイバー攻撃によって改ざんされたり、破壊されたり、ロックされたりしたデータを完全に復元することもできます。

Acronis Cyber Cloud Storage はデータとバックアップ（転送中と保存時の両方）の強力な暗号化や認証済みのセキュアなクラウドデータセンターなどを含むさまざまなサイバー防御を使ってデータとバックアップの漏洩を防ぎます。

ランサムウェアやクリプトジャッキングのようなマルウェア脅威に対する保護

Acronis Active Protection を搭載する Acronis Cyber Backup は AI と ML を使用してデータやバックアップファイル、バックアップエージェントへの変更を検出・阻止・復旧します（キャッシュを使ってファイルの変更を取り消し）。また、クリプトジャッキング攻撃も検出・阻止します。

このようにしてヘルスケア業界でもっとも蔓延している脅威のうちの 2 つに対する防御を提供し、さらにシグネチャベースやアンチウイルスソフトウェアのような従来の対策を補完するゼロデイ脅威の防御も提供します。

また、Acronis Cyber Backup はバックアップエージェントとアーカイブをマルウェア攻撃に対しても強化し、機関が漏洩後に迅速に復旧し、通常の業務を再開できるようにします。

コンプライアンス要件への対応

Acronis Active Protection と Acronis Cyber Cloud Storage を搭載する Acronis Cyber Backup の暗号化機能もヘルスケアの機密情報のプライバシーを保護することで（漏洩に成功した場合でも情報がサイバー犯罪者に使えないようにすることで）、コンプライアンス目標をサポートします。Acronis 製品にはその他多数の機能があり、適切に構成および使用すれば HIPAA 並びに経済的および臨床的健全性のための医療情報技術（HITECH）の遵守をサポートします。HIPAA に対する公式で法的に認められた証明プロセスや認定はありませんが、**Acronis は顧客の HIPAA および HITECH 遵守に関する懸案事項を最小化するために作成されたセキュリティおよび遵守プログラムを維持しています。**詳細については、Acronis リソースセンターをご覧ください。

重要なアプリケーションとストレージをパブリックとプライベートクラウドに移行

Acronis Cyber Backup は、広範なクラウドサービス、オペレーティングシステム (物理および仮想)、アプリケーションワークロード（プレミス & クラウドベース)、およびエンドポイントをサポートすることで、ヘルスケアアプリケーションをクラウドに移行するプロセスを簡略化します。Acronis Cyber Backup にはさまざまなデータ管理ツールがそろっており、ワークロードを物理、仮想、クラウド環境間で簡単かつ安全に移動でき、プライベートクラウドや Acronis Cyber Cloud Storage、そして Amazon、Google、Microsoft などのパブリッククラウドサービスを含む新しいプラットフォームに高速かつリスクなしで移行できます。

常にデータ可用性を提供

Acronis Cyber Backup は次の環境を含むアプリケーション環境にわたって RTO を効率的に管理し、ヘルスケア機関を支援する便利な機能を提供します：

1. Acronis Instant Restore は、ほとんどの重要アプリケーションでほぼゼロの RTO と RPO を提供します。
2. Acronis Universal Restore は、システムを新しいベアメタルハードウェアや異なるプラットフォーム（例えば、必要に応じて物理マシンから仮想マシンに）に柔軟に復元する機能を提供します。
3. ビルトインの Acronis Active Protection はランサムウェアやクリプトジャッキング攻撃に関連するダウンタイムや性能劣化を排除します。

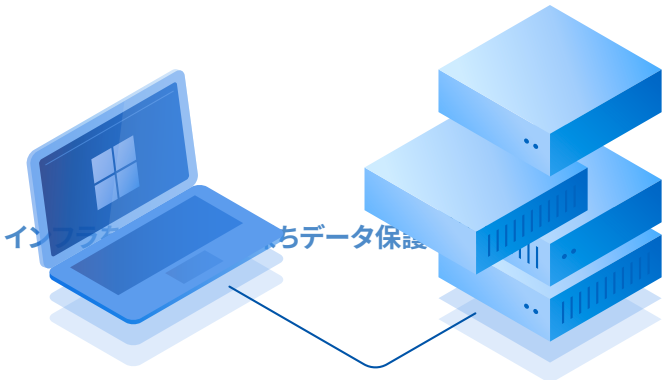
あらゆるデバイス間で機密データを保護

Acronis Files Advanced は患者ケアを強化し、運用効率を改善するのに役立ちます。また、米国における医療保険の相互運用性と説明責任に関する法令（HIPAA）などのセキュリティとコンプライアンスに関する厳しい基準の遵守も保証します。Acronis Files Advanced を使えば、ヘルスケアの従業員、パートナー、請負業者が機密文書を共有したり、協働したりできます。その一方で機関はデータロケーションや管理、プライバシーなどに対して完全なコントロールを保持します。

Acronis Files Advanced ポリシーエンジンは詳細な管理機能を提供し、コンテンツやユーザー、デバイスに対するコントロールとコンプライアンスを保証します。また、このソリューションは保存時や転送中のデータに対してセキュアなエンドツーエンド暗号化を行うことで、完全なデータ保護と機密性を保証します。さらに、Acronis Files Advanced によって、ポリシーの集中管理を通じて IT が情報漏洩やデータ共有違反、セキュリティ侵害を防ぐことができるようになります。

ヘルスケアプロバイダー、開業医、患者は Acronis Files Advanced を使用して、任意のデバイス（デスクトップ、ノートパソコン、タブレット、スマートフォンなど）を通じてヘルスケアデータに対するアクセス、編集、作成、共有を行います。さらに、開業医はソリューションを活用して以下を行います：

- **機密な患者データと管理文書**（例えば、機密情報および研究、学術、企業の契約）の保護
- **医者、研究者、医療管理者にヘルスケアデータへのアクセスを付与**し、任意のデバイスからの容易な共有を実現
- **保存時および転送中の患者記録を**保護
- **内部的（ヘルスケア組織内）と外部的（パートナーと）に患者ケアで迅速かつ効率的に**協働
- **ヘルスケアファイルへのアクセスと共有を**追跡
- **HIPAA を含む厳しいセキュリティとコンプライアンスの基準に**対応



Acronis Cyber Backup は組織のワークロードのすべてを保護できる単一のプラットフォームを提供することで、ヘルスケアのサイバープロテクションオペレーションコストを簡略化し、削減します。

また、クラウド、仮想、物理、モバイルのプラットフォームだけでなく、Microsoft、Oracle、Google などの人気のあるワークロードを含めて全面的にストレージ、保持、バックアップ、復元操作を管理できます。さらに、強力で直観的なインターフェースと監視ツールによって、比較的経験の少ないスタッフでも十分容易に運用できるため、より経験の豊富なスタッフは戦略的なプロジェクトに集中することができるようになります。

最後に、Acronis Disaster Recovery アドオンはシンプルで操作が容易な Acronis Cyber Backup の拡張機能で、ヘルスケア機関は、セキュアな Acronis Cloud を実行している仮想マシンで実行されるバックアップに自動的に切り替えることで重要な IT システム、アプリケーション、データの障害から習慣的に復元できます。また、Windows Server、Linux、VMware、Hyper-V、KVM、XenServer、RedHat Vertualization などの仮想化プラットフォーム、Exchange、SQL Server、SharePoint、Active Directory などの Microsoft アプリケーションを含む人気のあるさまざまなコンピューティングプラットフォームとアプリケーション向けのフェールオーバーを提供します。

アクロニス独自のクラウドアーキテクチャによって、データをコントロール可能に

まとめ

現代は急速なデジタルトランスフォーメーション、データ量の爆発、相互運用性ニーズの増加、および株主や規制当局の調査などが絡み合って、ヘルスケア業界にとって困難な時代になっています。データセーフティ、アクセシビリティ、プライバシー、真正性、セキュリティのバランスを同時に満たすのはデリケートな問題です。特に、貴重なヘルスケアデータを盗んで身代金を狙っているサイバー犯罪者への対策は急務です。ヘルスケア機関には、複雑な新規アプリケーションの実現、コストの削減、患者の転帰（治療成績）の改善などが期待される一方では、スタッフ保持、クラウドへの移行、モバイルや IoT デバイスの増加など、さまざまな IT 課題の克服も求められます。

Acronis は実績のあるサイバープロテクション、ストレージ、セキュアなファイル同期・共有およびヘルスケア業界向けに最適化されたディザスタリカバリソリューションにより支援することができます。

Acronis のサイバープロテクションソリューションが米国の病院に恩恵をもたらしているかは、こちら . をご覧ください。

ヘルスケア業界向け製品の **30 日間無償トライアル**については以下から入手できます：

- Acronis Active Protection 搭載の Acronis Cyber Backup 30日間無償試用版をご利用ください
- Acronis Cyber Backup 用の Acronis Disaster Recovery アドオン 30日間無償試用版をご利用ください
- Acronis Files Advanced 30日間無償試用版をご利用ください

Acronis

詳細は**www.acronis.com**をご覧ください。