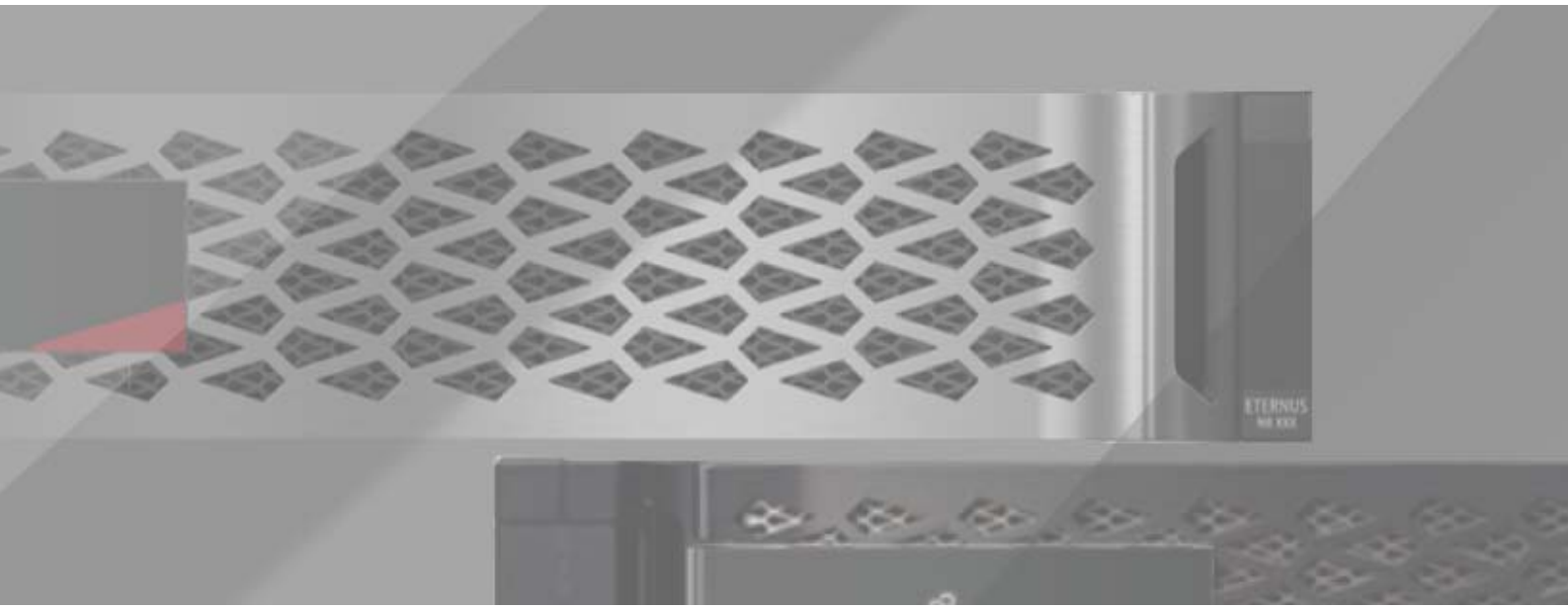
P3AG-6542-01Z0

FUJITSU Storage
ETERNUS AX series オールフラッシュアレイ ,
ETERNUS HX series ハイブリッドアレイ

ランサムウェアソリューション



FUJITSU

目次

図目次

はじめに

本書では、ランサムウェアについて説明します。どのように進化してきたか、また、ランサムウェア対策ソリューションを使用して、可能な限り迅速に特定、早期検出、拡散防止、復旧する方法についても説明します。本書に記載されているガイダンスとソリューションは、情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を満たしながら、組織がサイバー攻撃に強いソリューションを利用できるようにすることを目的としています。

初版
2022 年 3 月

登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/

本書では、本文中の ™、® などの記号は省略しています。

本書の読み方

対象読者

本書は、ETERNUS AX/HX の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

関連マニュアル

ETERNUS AX/HX に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

本書の表記について

■ 本文中の記号

本文中では、以下の記号を使用しています。

注 意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備 考	本文を補足する内容や、参考情報を記述しています。

第 1 章
ランサムウェアの概要

ランサムウェア攻撃が、組織が直面する可能性のある最大のサイバーセキュリティ脅威の 1 つであることは誰もが知っています。潜在的な損害は、直接的な関連復旧コスト (Sophos によると、2019 年から 2020 年の間に 241% 増加) だけではありません。企業の評判とブランドにも影響を与えます。

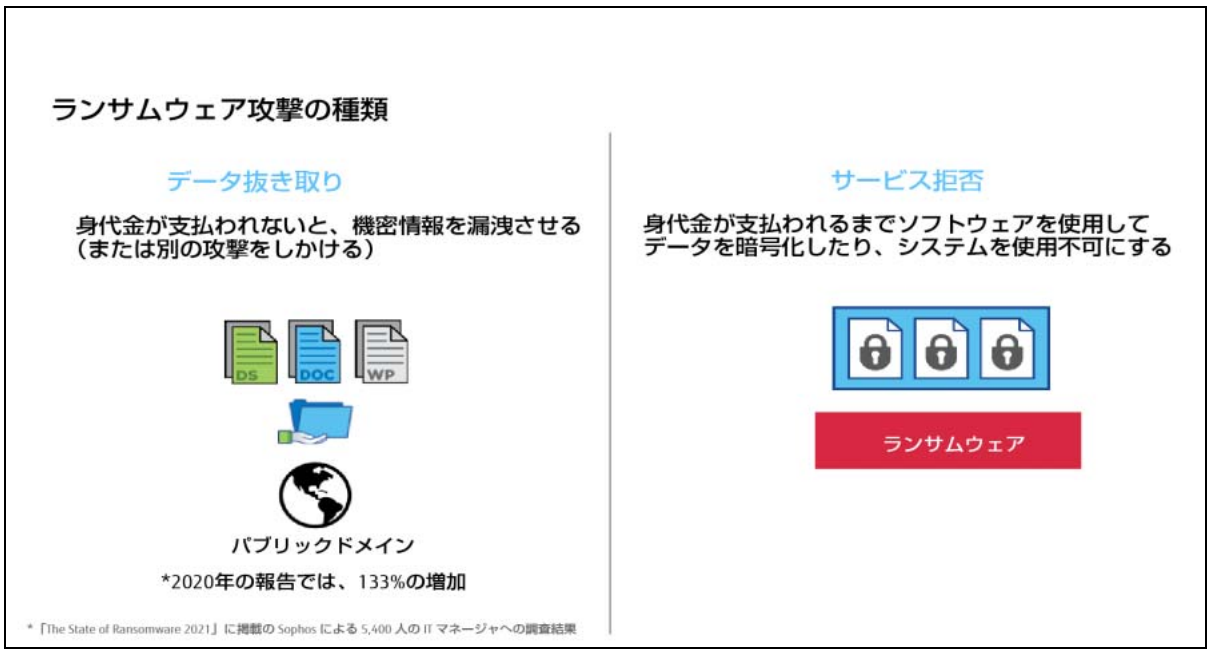
1.1 ランサムウェアとは？

攻撃者がランサムウェアを利用する目的は、できるだけ手軽に金儲けすることにあります。長年にわたって、攻撃者が使用する戦略は進化してきました。これまで攻撃者は、顧客が商品を購入するために利用する企業のウェブサイトにアクセスできなくする分散型サービス拒否攻撃を利用していました。サービス拒否は身代金が支払われるまで続きました。この戦略は今日ではあまり使われていません。もう 1 つの方法は、データ抜き取りと呼ばれます。この戦略では、攻撃者は企業の IT システムにアクセスし、機密データを社外の未知の場所に移動して、身代金が支払われない場合はそのデータを公開すると脅します。Sophos によると、データ抜き取りは再び増加しており、この分野の攻撃は前年比で 133% 増加したということです。

最も一般的なランサムウェアは、「Denial of Service (DoS：サービス拒否) ランサムウェア」と呼ばれています。このランサムウェア戦略では、攻撃者はユーザーが誤って暗号化プログラム (マルウェア) をダウンロードするように仕向けます。インストール後、マルウェアはすべてのローカルクライアントファイルと、企業ネットワーク上の NFS または SMB 共有上で可能なすべてのファイルを暗号化します。ファイルが暗号化されると、元のファイルは削除され、ファイル内のデータにアクセスする方法はなくなります。ファイルはまだネットワーク上にあることが分かりますが、攻撃者が暗号化しているためアクセスできません。

これまでの方法とは対照的に、企業の Web サイトをオフラインにするために大量のボットを呼び出す必要がなく、データを別の場所にコピーする必要もないため、攻撃者にとって DoS 攻撃のオーバーヘッドは非常に低くなります。攻撃者は、データへのアクセスを回復できるように、復号化キーを取得するために身代金を支払うよう要求します。身代金の額は通常、攻撃者が相当な額の金銭を得るのに十分な大きさですが、組織にとっては支払うのが非現実的なほど大きくはありません。

図 1.1　現在組織に対して使用されている 2 つの主要なランサムウェア

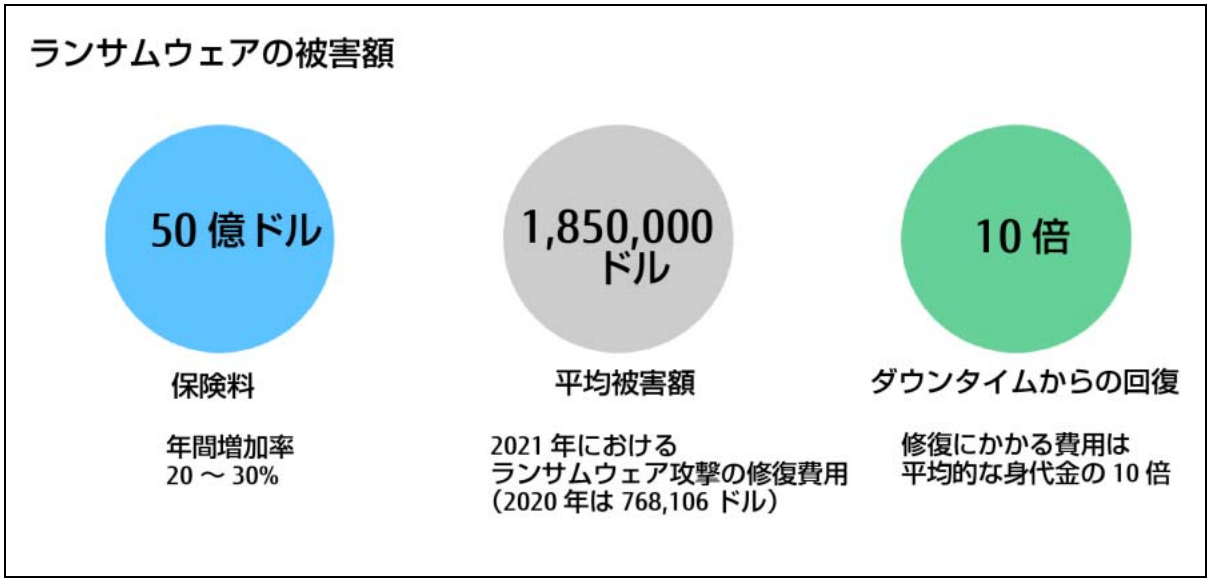


1.2　ランサムウェアの実際の損失

身代金の支払い自体が、ビジネスに対する最大の金銭的影響だと考えるかもしれません。しかし、支払いはささいなものではない（平均的な被害額は 1 件あたり 154,108 ドルにもなると考えられている）ものの、ランサムウェア攻撃後のダウンタイムによる実際の損失と比べると見劣りします。

企業がビジネスに不可欠なデータにアクセスできない場合、生産性に深刻な影響が及びます。Coveware が 2020 年 1 月に発表した分析結果によると、ランサムウェアによる平均的なダウンタイムは 17 日以上であり、ダウンタイムによる損失は通常、実際の身代金の 10 倍だといいます。アメリカでの復旧にかかる平均費用は 180 万ドルです。ダウンタイムの影響とその結果生じるコストは、ビジネスのタイプによって組織ごとに異なります。IT の可用性に大きく依存している組織（電子商取り引き、株式取引、医療など）は、10 倍の金銭的被害を受けます。つまり、実際にダウンタイムが発生した場合、組織は 1,154,108 ドル程度またはそれ以上の損失を被る可能性があります。これは 1 件あたりの金額なので、複数件発生すると、損失が増加する可能性があります。また、被保険企業に対するランサムウェア攻撃の可能性が非常に高いことから、サイバー保険のコストも増加し続けています。

図 1.2　ランサムウェアによる主な損失は、リカバリ中に組織が直面するダウンタイムに発生



第 2 章
ランサムウェアソリューション

2.1 階層型防御アプローチ

ランサムウェアの拡散を防ぎ、甚大な損害を与えるダウンタイムを回避するには、ランサムウェアの検出をできるだけ早く行うことが重要です。ただし、効果的なランサムウェア検出戦略には、複数の保護レイヤーを含める必要があります。車両の衝突安全機能で例えてみることができます。事故から身を守るために、シートベルトのような 1 つの機能だけに頼りたくはありません。エアバッグ、アンチロックブレーキ、そして前方衝突警報さえも、より良い結果をもたらす追加の安全機能です。ランサムウェア対策も同じように考えるべきです。

ユーザーアカウントを 1 つ乗っ取るのは、ランサムウェア攻撃を仕掛ける際にハッカーが取るかもしれない手段の 1 つにすぎず、悪意のある攻撃者は、攻撃手法を絶えず進化させています。

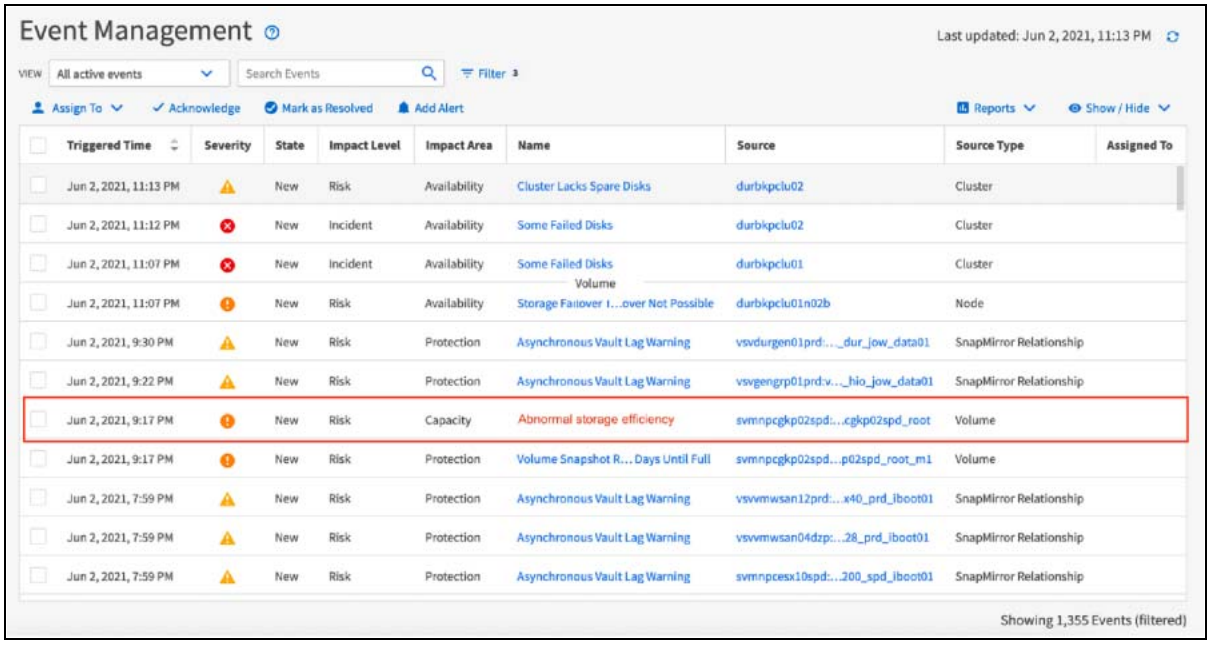
Active IQ Unified Manager は、ランサムウェアを検知するためのさらなる層を提供します。Active IQ Unified Manager はまた、Snapshot コピーの異常な増加やストレージ効率の低下を示すアラートを生成します。これは、ランサムウェア攻撃の可能性を示します。

そこで登場するのが、ONTAP 9.10.1 以降のランサムウェア対策機能です。これは、ボリュームのワークロードアクティビティとデータエントロピーを参照する組み込みのオンボックス機械学習(ML)を利用して、ランサムウェアを自動的に検出します。UBA とは異なるアクティビティを監視するため、UBA では検出できない攻撃を検出できます。

2.2　ネイティブ検出ツール

ETERNUS AX/HX には、ランサムウェアを早期に検出するためのツールがネイティブまたは組み込みで用意されています。ONTAP の場合、これらのツールには、異常な Snapshot コピーとボリューム増加率、およびストレージ効率の低下に関する Active IQ Unified Manager のアラートが含まれます。

図 2.1　Active IQ Unified Manager によるストレージ効率の異常に関するアラート



また、ONTAP System Manager を使用して、Snapshot の割合の変更やストレージ容量の節約をリアルタイムで確認することもできます。

2.3　ネイティブ FPolicy

FPolicy (File Policy という名前を発展させたもの) は、NFS または SMB/CIFS プロトコル経由のファイルアクセスを監視および管理するために使用するファイルアクセス通知フレームワークです。ONTAP には 10 年以上前から組み込まれており、ランサムウェアの検出に非常に役立ちます。このゼロトラストエンジンは、Access Control List (ACL：アクセスコントロールリスト) でのアクセス許可以外にも追加のセキュリティ対策を提供するため、重要です。

ゼロトラストの背後にある概念は、決して信頼せず、常に検証することです。ただし、重要な点は、ユーザー (または管理者) にファイルやフォルダへのアクセス許可があるからといって、そのコンテンツを変更できるとは限らないということです。

FPolicy は当初、不要なファイルがエンタープライズグレードのストレージアプライアンスに保存されないようにすることを目的としていました。(たとえば、Spotify などの音楽ストリーミングサービスが普及する以前は、多くのユーザーは .mp3 ファイルをホームフォルダに保存していたため、自分のデバイスから音楽をストリーミングできました。) しかし、FPolicy は既知のランサムウェアファイル拡張子をブロックする方法も提供します。ユーザーにはホームフォルダへの完全なアクセス許可がありますが、FPolicy では、管理者がブロックするとマークしたファイル (.mp3 ファイルまたは既知のランサムウェアファイルの拡張子) を保存することはできません。

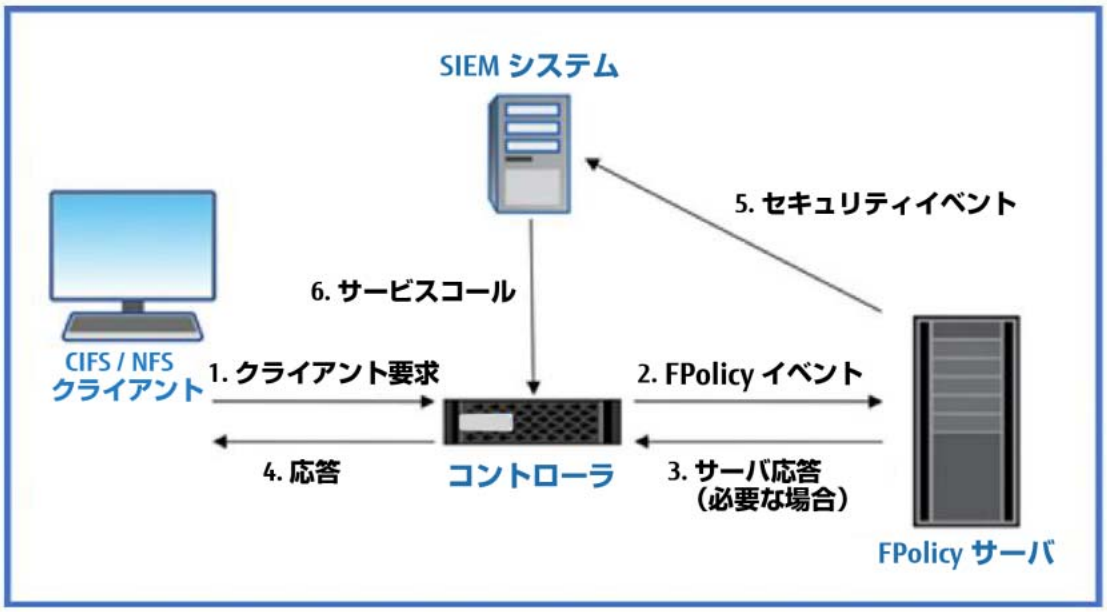
2.4　外部 FPolicy

ONTAP の FPolicy 外部モードは、UBA (UEBA：User and Entity Behavior Analytics とも呼ばれる) をキーとして、ゼロデイランサムウェア攻撃を阻止します。その方法を理解するには、UBA を十分に理解する必要があります。

人間は習慣の生き物です。私たちの習慣は、データへのアクセス方法や作業方法など、多くのことに当てはまります。多くの場合、ユーザーとグループは特定のデータセットにアクセスしてジョブを実行します。UBA はこれらの動作を追跡し、ユーザーの一般的なアクセスパターンを識別し、そのユーザーの動作がパターンと異なる場合にレポートできます。さらに、ユーザーが通常のパターン以外のことをしている場合、UBA はファイルデータへのアクセスを拒否することもできます。FPolicy 外部モードは、UBA を使用する外部サーバと統合され、ユーザが通常は実行しない操作をいつ実行しているかを判断します。

次のセキュリティ情報およびイベント管理 (SIEM) システムの例では、すべての CIFS または NFS クライアント要求が FPolicy サーバに送信され、FPolicy サーバはアクセスを許可するかどうかを判断します。

図 2.2　外部モードの FPolicy は、FPolicy 固有の API を使用して外部サーバと統合



この追加レベルの分析は、操作しようとしているファイルデータに対してユーザーがアクセス許可を持っている場合でも実施されます。権限を常に正しく取得するのは難しいため、ユーザーが不正行為をしようとしていないかを判断する上で、FPolicy を使用した UBA は、はるかに優れた判定基準を提供します。

UBA は非常に効果的ですが、ゼロデイランサムウェア攻撃に対抗するための最終手段ではありません。富士通のパートナーやベンダーの多くは、外部の FPolicy サーバに人工知能 (AI) と ML を組み込み始めています。各ベンダーの製品は、ONTAP に組み込まれている FPolicy 機能にプラグインしているため、これらの AI/ML 拡張機能をすぐに利用できます。

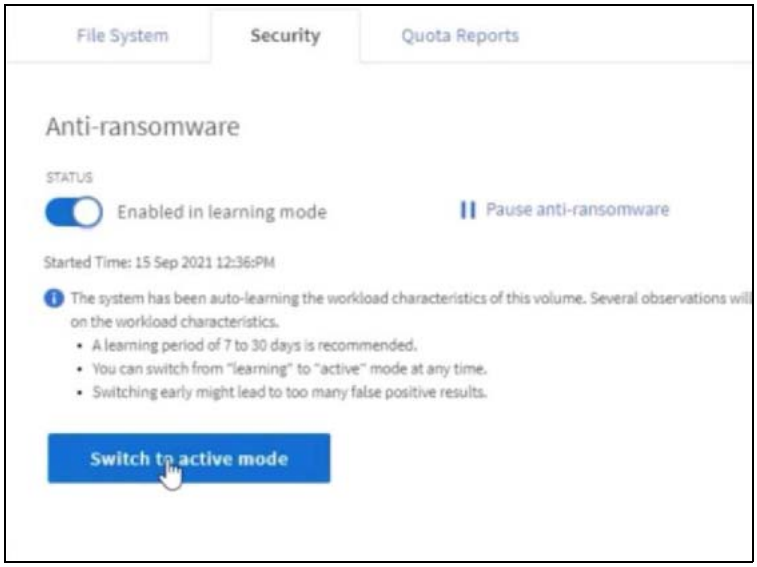
2.5　オンボックスアンチランサムウェア

ONTAP 9.10.1 以降では、ランサムウェア対策機能として、まったく新しいランサムウェアの検出と防止方法が導入されています。これは、ボリュームのワークロードアクティビティとデータエントロピーを参照する組み込みのオンボックス機械学習 (ML) を利用して、ランサムウェアを自動的に検出します。また、UBA とは異なるアクティビティを監視して、UBA では検出できない攻撃を検出できるようにします。

ONTAP のランサムウェア対策は、「Security and Compliance」ソフトウェアバンドルの一部として提供されています。このバンドルをすでにお持ちのお客様は、最新バージョンの ONTAP (ONTAP 9.10.1) にアップグレードするだけでこの機能を利用できます。ONTAP の組み込み管理インターフェースである System Manager を使用して構成可能であり、ボリューム単位で有効化されます。

ランサムウェア対策機能は学習モードで起動します。ML が NAS ボリュームの一般的なワークロードを理解できるように、最低 30 日間を推奨しています。アンチランサムウェアがアクティブモードになると、ランサムウェアの可能性がある異常なボリュームアクティビティの検出が開始されます。

図 2.3　アクティブモードを設定する前に学習モードでアンチランサムウェアを有効化 (推奨 30 日間)



異常なアクティビティが検出されると、自動的に Snapshot コピーが作成され、感染する直前のポイントが提供されます。同時に、管理者が異常なファイルアクティビティを確認できるようにする自動アラートが生成されます。これにより、アクティビティが本当に悪質であるかどうかを判断し、適切なアクションを実行できます。アクティビティが想定内のワークロードであった場合は、そのアクティビティをフォールスポジティブとして容易にマークできます。アンチランサムウェアの ML は、ワークロードの変化を検知しますが、攻撃の可能性の警告を通知しなくなります。また、この機能によって I/O が中断されることはありません。その代わり、管理者にネイティブの分析、インサイト、データリカバリ機能を提供し、前例のないオンボックスランサムウェア検出を可能にします。ランサムウェア対策機能により、NAS ワークロードの自動ランサムウェア検出を ONTAP でこれまで以上に容易に実行できるようになります。

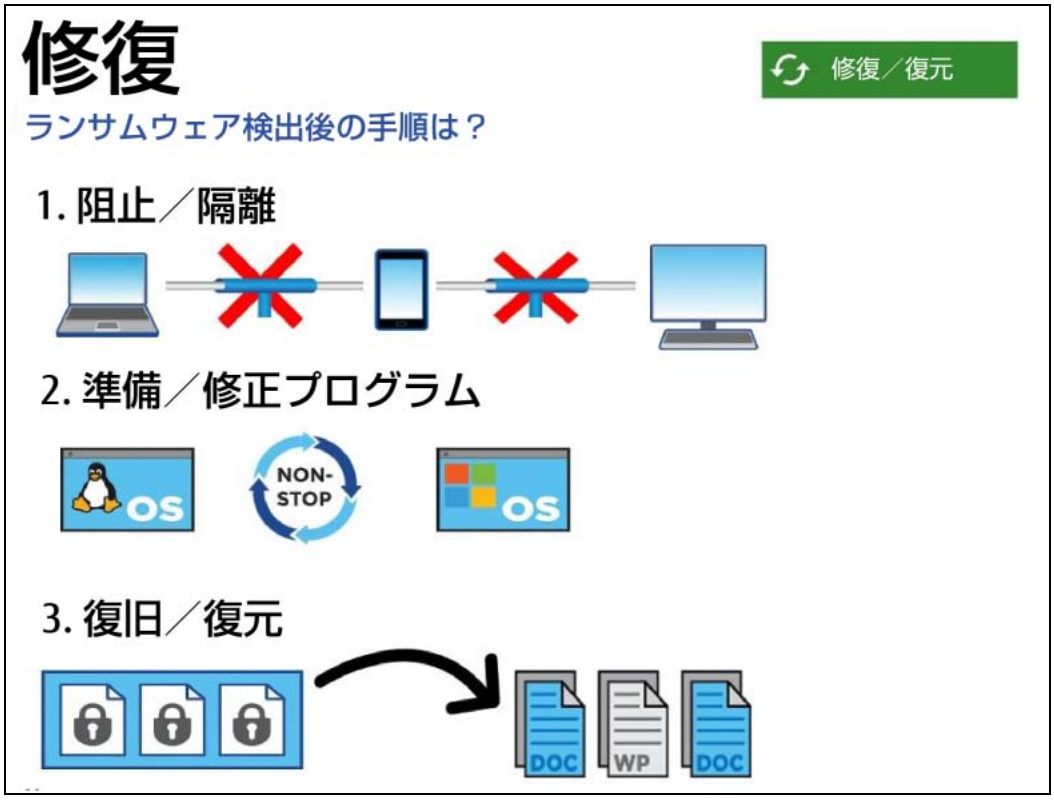
ランサムウェア対策機能の詳細については、アンチランサムウェア ETERNUS AX/HX のドキュメントを参照してください。

2.6　ランサムウェア攻撃からの復旧に関する推奨事項

ランサムウェア攻撃を受けた後の最初の行動は、データを即座に復旧させることかもしれません。これはもちろん可能ですが、ランサムウェアが戻ってこないようにするために他の手段を講じないと、再感染してしまい、貴重な時間を無駄にしてしまいます。

ランサムウェア感染から環境を適切かつ総合的に修復するには、3 つの重要なステップがあります。これらのステップは以下の図に示されており、記載された順序 (ただし、必須ではない) で完了させます。

図 2.4　攻撃から復旧するための推奨手順



この方法は、データを復元するときに再感染を回避する最も効果的な方法です。

2.7　ONTAP リカバリ機能

ランサムウェア攻撃からリカバリする最も迅速な方法は、バックアップからのリストアであることは誰もが知っています。簡単に聞こえるかもしれませんが、実際の復元プロセスは複雑で、時間もかかります。

- バックアップデータも暗号化されていますか？
- 必要なバックアップは残っていますか？
- 暗号化されたデータのリストアにはどのくらいの時間がかかりますか？
- データのリストアは本番ワークロードに影響しますか？

リストア中の長時間のダウンタイム（ランサムウェアの実際の損失）を回避するために、これらすべてに対策をすることが重要です。

ONTAP Snapshot テクノロジーは、これらの項目を満たし、高速リストア（数秒で数テラバイト）を実現し、バックアップをランサムウェア暗号化から保護し、貴重なバックアップデータの削除を防止するための鍵となります。災害復旧、データアーカイブ、データ階層化などのために、ビジネス生態系全体にわたって Snapshot コピーの機能を活用できます。

2.8　SnapLock – 論理的なエアギャップ

攻撃者がバックアップコピーを破壊し、場合によっては暗号化する傾向が高まっています。サイバーセキュリティ業界の多くが、全体的なサイバーレジリエンス戦略の一環として、エアギャップバックアップの使用を推奨しているのはそのためです。

問題は、従来のエアギャップによってリストア時間が大幅に増加し、ダウンタイムとそれに伴う全体的なコストが増加する可能性があることです。また、一般に複雑さも増します。論理的なエアギャップは、従来のエアギャップに代わる優れたソリューションであり、オンラインのバックアップを維持しながら同じセキュリティ保護の原則を備えています。富士通システムを使用すると、テープやディスクのエアギャップの複雑さを論理的なエアギャップで解決できます。これは、変更不可の Snapshot コピーと SnapLock Compliance によって実現できます。

10年以上前にSnapLock機能をリリースし、HIPAA (Health Insurance Portability and Accountability Act: 医療保険の相互運用性と説明責任に関する法律)、サーベンス・オクスリー法 (米企業改革法)、その他の規制データ規則など、データコンプライアンスの要件に対応しています。また、プライマリ Snapshot コピーを SnapLock ボリュームにヴォールトして、コピーを WORM にコミットし、削除できないようにすることもできます。SnapLock ライセンスには 2 つのバージョンがあります。SnapLock Compliance と SnapLock Enterprise です。ランサムウェアから保護するため、Snapshot コピーをロックして、ONTAP管理者や富士通サポートでも削除できない特定の保存期間を設定できるSnapLock Compliance を推奨しています。

第 3 章
まとめ

他多数のマルウェアの脅威と同様に、ランサムウェアも進化し続けていることは明らかです。防御方法が改善されるのと同じように、攻撃方法とベクターも改善されています。1 つのソリューションですべての攻撃を阻止することはできませんが、パートナーシップやサードパーティを含むソリューションのポートフォリオを使用すると、階層型の防御が可能になります。

ETERNUS AX/HX は、ランサムウェアの早期発見、感染拡大の防止、必要に応じた迅速な復旧を支援し、甚大な損害を与えるダウンタイムを回避するための、可視性、検出、修復のためのさまざまな効果的なツールを提供します。従来の階層型の防御ソリューションは依然として普及しており、可視性と検出のためのサードパーティやパートナーのソリューションも同様です。効果的な修復は、あらゆる脅威への対応において重要な部分であり続けます。変更不可の Snapshot コピーテクノロジーと SnapLock の論理的なエアギャップソリューションを活用した独自の業界アプローチは、他とは一線を画すランサムウェア対策のベストプラクティスです。

FUJITSU Storage
ETERNUS AX series オールフラッシュアレイ ,
ETERNUS HX series ハイブリッドアレイ
ランサムウェアソリューション

P3AG-6542-01Z0

発行年月　2022 年 3 月
発行責任　富士通株式会社


FUJITSU