



ランサムウェア向けNetAppソリューション ONTAP Technical Reports

NetApp
February 23, 2026

目次

ランサムウェア向けNetAppソリューション	1
ランサムウェアとNetAppの保護ポートフォリオ	1
データが主なターゲット	1
ランサムウェアの真のコスト	1
データレイヤでのランサムウェア対策	2
NetAppのランサムウェア対策ポートフォリオ	2
ランサムウェアからのリカバリ保証	3
SnapLockと改ざん防止スナップショットでランサムウェアを保護	3
SnapLock Compliance	3
スナップショットの改ざん防止	4
FPolicyファイルブロッキング	4
FPolicyネイティブモードで悪意のあるファイルをブロック	4
FPolicy外部モードを使用したユーザとエンティティの動作分析（UEBA）の有効化	4
Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ	5
NetApp ONTAPに搭載されたAIベースの検出と応答機能	6
自律型ランサムウェア防御（ARP）	6
自律型ランサムウェア対策 / AI（ARP / AI）	6
ONTAPでのサイバーウォールティングによるエアギャップによるWORM保護	7
SnapLock Complianceと論理的なエアギャップによるサイバーウォールティング	7
スナップショットの改ざん防止	7
Digital Advisorによるランサムウェア対策	8
NetAppランサムウェア保護による包括的な回復力	8
NetAppランサムウェア保護	9

ランサムウェア向けNetAppソリューション

ランサムウェアとNetAppの保護ポートフォリオ

ランサムウェアは、2024年に組織のビジネス中断を引き起こす最も重大な脅威の1つです。の "[Sophosランサムウェアの現状2024](#)"調査によると、ランサムウェア攻撃は調査対象者の72%に影響を及ぼしています。ランサムウェア攻撃はより高度で標的型に進化しており、脅威アクターは人工知能などの高度な手法を採用して影響と利益を最大化しています。

組織は、境界、ネットワーク、ID、アプリケーション、データの保存場所など、セキュリティ体制全体をストレージレベルで把握し、これらのレイヤを保護する必要があります。今日の脅威の状況では、ストレージレイヤでサイバー保護にデータ主体のアプローチを採用することが不可欠です。単一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などのソリューションポートフォリオを使用することで、多層的な防御を実現できます。

には[NetApp製品ポートフォリオ](#)、可視化、検出、修復のためのさまざまな効果的なツールが用意されており、ランサムウェアの早期発見、拡散の防止、必要に応じた迅速なリカバリを支援して、コストのかかるダウンタイムを回避できます。可視化と検出のためのサードパーティやパートナーソリューションと同様に、従来の階層型防御ソリューションは依然として普及しています。効果的な修復は、あらゆる脅威への対応において依然として重要な部分を占めています。書き換え不能なNetApp SnapshotテクノロジーとSnapLockの論理的エアギャップソリューションを活用する業界独自のアプローチは、ランサムウェア対策機能における業界の差別化要因であり、業界のベストプラクティスでもあります。



2024年7月以降、以前PDFとして公開されていたテクニカルレポート『TR-4572：NetApp Ransomware Protection』のコンテンツがdocs.netapp.comで公開されました。

データが主なターゲット

サイバー犯罪者は、データの価値を認識し、データを直接ターゲットにすることが増えています。境界、ネットワーク、およびアプリケーションのセキュリティは重要ですが、バイパスすることができます。ソースであるストレージレイヤでのデータ保護に重点を置き、重要な最終防衛線を提供します。ランサムウェア攻撃の目的は、本番環境のデータにアクセスして暗号化したりアクセス不能にしたりすることです。そのためには、攻撃者は境界からアプリケーションのセキュリティまで、今日組織によって導入されている既存の防御をすでに貫通している必要があります。

[境界からデータセキュリティまでのセキュリティレイヤ]

残念ながら、多くの組織はデータレイヤのセキュリティ機能を利用していません。そこで登場するのが、NetAppランサムウェア対策ポートフォリオであり、最前線でお客様を保護します。

ランサムウェアの真のコスト

身代金の支払い自体は、ビジネスへの最大の金銭的影響ではありません。支払い額はわずかではありませんが、ランサムウェアインシデントの被害によるダウンタイムコストと比べると、わずかです。

身代金の支払いは、ランサムウェア攻撃に対処する際のリカバリコストの要素の1つにすぎません。支払われた身代金を除くと、2024年の組織の報告によると、ランサムウェア攻撃からの復旧に要する平均コストは2730万ドルであり、2023年に報告された1820万ドルから100万ドル近く増加して "[2024 Sophosランサムウ](#)

エアの現状があります。Eコマース、株式取引、医療など、ITの可用性に大きく依存している組織の場合、コストは10倍以上になる可能性があります。

また、被保険企業がランサムウェア攻撃を受ける可能性が非常に高いことから、サイバー保険のコストも上昇し続けています。

データレイヤでのランサムウェア対策

NetAppは、境界からストレージレイヤでのデータの配置場所まで、組織全体にわたってセキュリティ体制が広く深く浸透していることを認識しています。セキュリティスタックは複雑であり、テクノロジスタックのあらゆるレベルでセキュリティを提供する必要があります。

データレイヤでのリアルタイムの保護は、さらに重要であり、独自の要件があります。効果的に機能するには、この層のソリューションが次の重要な属性を提供する必要があります。

- *設計によるセキュリティ*により、攻撃が成功する可能性を最小限に抑える
- *リアルタイムの検出と対応*により、攻撃が成功した場合の影響を最小限に抑えます。
- *エアギャップによるWORM保護*重要なデータのバックアップを分離
- *単一のコントロールプレーン*による包括的なランサムウェア防御

NetAppはこれらすべてを実現し、さらに多くの機能を提供します。

[NetAppランサムウェア対策ポートフォリオ（説明されている重要な属性を含む）]

NetAppのランサムウェア対策ポートフォリオ

NetAppは、**"組み込みのランサムウェア対策"**重要なデータに対してリアルタイムで堅牢かつ多面的な防御を提供します。その中核である、AIを活用した高度な検出アルゴリズムは、データパターンを継続的に監視し、99%の精度で潜在的なランサムウェアの脅威を迅速に特定します。攻撃に迅速に対応することで、ネットアップのストレージはデータのスナップショットを迅速に作成し、コピーを保護して迅速なリカバリを実現します。

データをさらに強化するために、NetAppの**"サイバーフォールティンク"**機能は論理的なエアギャップでデータを分離します。重要なデータを保護することで、迅速なビジネス継続性を確保します。

NetApp**"NetAppランサムウェア保護"**単一のコントロールプレーンで運用上の負担を軽減し、エンドツーエンドのワークロード中心のランサムウェア防御をインテリジェントに調整および実行します。これにより、リスクのある重要なワークロードデータを1回のクリックで識別して保護し、潜在的な攻撃の影響を制限するために正確かつ自動的に検出して対応し、数日ではなく数分以内にワークロードを回復して、貴重なワークロードデータを保護し、コストのかかる中断を最小限に抑えることができます。

データへの不正アクセスを保護するためのネイティブの組み込みONTAPソリューションとして、**"マルチ管理者認証 (MAV)"** ボリュームの削除、管理ユーザの追加作成、Snapshotの削除などの処理を、2人目の指定管理者から承認を得た場合のみ実行できる堅牢な機能セットを備えています。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。スナップショットを削除する前に、指定された管理者承認者を必要な数だけ設定できます。



NetApp ONTAPは、Webベースの **"多要素認証 (MFA)"** System ManagerおよびSSH CLI認証の要件に対応しています。

NetAppのランサムウェア対策は、進化し続ける脅威の状況にも安心して対応します。その包括的なアプローチは、現在のランサムウェア攻撃から防御するだけでなく、新たな脅威にも適応し、データインフラに長期的なセキュリティを提供します。

その他の保護オプションについて

- ["Digital Advisorによるランサムウェア対策"](#)
- ["Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ"](#)
- ["FPolicy"](#)
- ["SnapLockと改ざん防止スナップショット"](#)

ランサムウェアからのリカバリ保証

NetAppは、ランサムウェア攻撃が発生した場合にSnapshotデータをリストアすることを保証します。当社の保証：スナップショットデータのリストアをサポートできない場合は、適切に対応します。この保証は、AFF Aシリーズ、AFF Cシリーズ、ASA、FASシステムの新規購入時に利用できます。

詳細

- ["リカバリ保証サービスの説明"](#)
- ["ランサムウェア対策保証ブログ"](#)です。

関連情報

- ["NetAppサポートサイトのリソースページ"](#)
- ["NetApp製品のセキュリティ"](#)

SnapLockと改ざん防止スナップショットでランサムウェアを保護

NetAppのスナップ兵器の重要な武器は、ランサムウェアの脅威からの保護に非常に効果的であることが証明されているSnapLockです。不正なデータ削除を防止することで、SnapLockは追加のセキュリティレイヤを提供し、悪意のある攻撃が発生した場合でも重要なデータに影響を与えずにアクセスできるようにします。

SnapLock Compliance

SnapLock Compliance (SLC) は、データを消去できない方法で保護します。SLCでは、管理者がアレイを再初期化しようとした場合でも、データの削除が禁止されています。他の競合製品とは異なり、SnapLock Complianceはそれらの製品のサポートチームを通じてソーシャルエンジニアリングのハッキングに対して脆弱ではありません。SnapLock Complianceボリュームで保護されているデータは、そのデータが有効期限に達するまでリカバリできます。

SnapLockを有効にするには["ONTAP One"](#)、ライセンスが必要です。

詳細

- ["SnapLockのドキュメント"](#)

スナップショットの改ざん防止

改ざん防止Snapshot (TPS) コピーを使用すると、悪意のある行為からデータを簡単かつ迅速に保護できます。SnapLock Complianceとは異なり、TPSは通常、ユーザが決められた時間データを保護し、高速リカバリのためにローカルに残しておくことができるプライマリシステムや、プライマリシステムからデータをレプリケートする必要がないプライマリシステムで使用されます。TPSはSnapLockテクノロジーを使用して、同じSnapLock保持期限を使用しているONTAP管理者でもプライマリSnapshotが削除されないようにします。SnapLockが有効になっていなくても、Snapshotは削除できません。ただしSnapshotには、SnapLock Complianceと同じ消去不能な性質はありません。

スナップショットの改ざんを防止するには、["ONTAP One"ライセンス](#)が必要です。

詳細

- ["Snapshotをロックしてランサムウェア攻撃から保護"](#)です。

FPolicyファイルブロッキング

FPolicyは、エンタープライズクラスのストレージプライアンスへの不要なファイルの保存をブロックします。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。ユーザには引き続きホームフォルダに対するフルアクセス権限がありますが、FPolicyでは管理者がブロック済みとしてマークしたファイルを格納することはできません。これらのファイルがMP3ファイルであるか、既知のランサムウェアファイル拡張子であるかは関係ありません。

FPolicyネイティブモードで悪意のあるファイルをブロック

NetApp FPolicyのネイティブモード（ファイルポリシーという名前を発展させたもの）は、不要なファイル拡張子が環境に侵入するのをブロックできるファイル拡張子ブロックフレームワークです。10年以上にわたってONTAPの一部として提供されており、ランサムウェアからの保護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) 権限以外にもセキュリティ対策を追加できるため、価値があります。

ONTAP System Manager およびNetApp Consoleでは、3000 を超えるファイル拡張子のリストを参照できます。



一部の拡張機能はご使用の環境では正当なものであり、ブロックすると予期しない問題が発生する可能性があります。ネイティブFPolicyを設定する前に、環境に適した独自のリストを作成してください。

ONTAPのネイティブモードはすべてのライセンスに含まれています。

詳細

- ["ブログ：ランサムウェアとの戦い：パート3—ONTAP FPolicy、もう1つの強力なネイティブ（別名フリー）ツール"](#)

FPolicy外部モードを使用したユーザとエンティティの動作分析（UEBA）の有効化

FPolicy外部モードは、ファイルアクティビティとユーザアクティビティを可視化するための、ファイルアクティビティの通知および制御フレームワークです。これらの通知は、外部ソリューションでAIベースの分析を

実行して悪意のある動作を検出するために使用できます。

FPolicy外部モードは、特定のアクティビティを許可する前にFPolicyサーバからの承認を待機するように設定することもできます。このような複数のポリシーを1つのクラスターに設定できるため、柔軟性に優れています。



承認を提供するように設定されている場合、FPolicyサーバはFPolicy要求に応答する必要があります。そうしないと、ストレージシステムのパフォーマンスが低下する可能性があります。

FPolicy外部モードには含まれてい"スヘテノONTAPライセンス"ます。

詳細

- ["ブログ : Fighting Ransomware: Part Four—UBA and ONTAP with FPolicy external mode"](#)

Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ

ストレージワークロードセキュリティ (SWS) は、ONTAP環境のセキュリティ体制、回復性、アカウントビリティを大幅に強化するNetApp Data Infrastructure Insightsの機能です。SWSはユーザ中心のアプローチを採用し、環境内のすべての認証済みユーザからのすべてのファイルアクティビティを追跡します。高度な分析を使用して、すべてのユーザの通常のアクセスパターンと季節的なアクセスパターンを確立します。これらのパターンは、ランサムウェアシグネチャを使用せずに疑わしい動作を迅速に特定するために使用されます。

SWSは、潜在的なランサムウェアやデータ削除を検出すると、次のような自動アクションを実行できます。

- 該当するボリュームのSnapshotを作成します。
- 悪意のあるアクティビティの疑いがあるユーザアカウントとIPアドレスをブロックします。
- 管理者にアラートを送信します。

SWSは、内部の脅威を迅速に阻止し、すべてのファイルアクティビティを追跡する自動化されたアクションを実行できるため、ランサムウェアイベントからのリカバリをはるかに簡単かつ迅速に実行できます。高度な監査ツールとフォレンジックツールが組み込まれているため、攻撃の影響を受けたボリュームやファイル、攻撃元のユーザアカウント、実行された悪意のあるアクションをすぐに確認できます。Snapshotの自動作成により、被害を軽減し、ファイルのリストアを高速化します。

[Data Infrastructure Insightsサイトストレージワークロードセキュリティ攻撃結果]

ONTAPのAutonomous Ransomware Protection (ARP;自律型ランサムウェア対策) によるアラートもSWSに表示されるため、ARPとSWSの両方を使用してランサムウェア攻撃から保護する単一のインターフェイスが提供されます。

詳細

- ["NetAppData Infrastructure Insights"](#)

NetApp ONTAPに搭載されたAIベースの検出と応答機能

ランサムウェアの脅威がますます巧妙になるにつれ、防御メカニズムも進化していきます。NetAppの自律型ランサムウェア対策（ARP）は、ONTAPに組み込まれたインテリジェントな異常検出機能を備えたAIを基盤としています。オンにすると、サイバーレジリエンスに新たな防御レイヤを追加できます。

ARPとARP / AIは、ONTAPの組み込みの管理インターフェイスとSystem Managerを使用して設定でき、ボリューム単位で有効にできます。

自律型ランサムウェア防御（ARP）

ONTAP 9.10.1以降のもう1つのネイティブ組み込みONTAPソリューションである自律型ランサムウェア対策（ARP）では、NASストレージボリュームのワークロードのファイルアクティビティとデータエントロピーを調べて、潜在的なランサムウェアを自動的に検出します。ARPは、管理者にリアルタイムの検出、分析情報、データリカバリポイントを提供し、これまでにないオンボックスの潜在的なランサムウェア検出を可能にします。

ARPをサポートするONTAP 9.15.1以前のバージョンでは、ARPは学習モードで開始され、一般的なワークロードのデータアクティビティを学習します。ほとんどの環境では、この処理に7日かかることがあります。ラーニングモードが完了すると、ARPは自動的にアクティブモードに切り替わり、ランサムウェアの可能性のある異常なワークロードアクティビティを探し始めます。

異常なアクティビティが検出された場合は、即座にSnapshotが自動作成され、感染データを最小限に抑えながら、可能な限り攻撃時点に近いリストア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自動アラート（設定可能）が生成され、アクティビティが実際に悪意のあるものかどうかを判断して適切なアクションを実行できるようになります。

アクティビティが想定されるワークロードである場合、管理者は簡単に誤検出としてマークできます。ARPはこの変更を通常のワークロードアクティビティとして学習し、今後の潜在的な攻撃としてフラグを立てなくなります。

ARPをイネーブルにするには"ONTAP One"、ライセンスが必要です。

詳細

- ["自律型ランサムウェア対策"](#)

自律型ランサムウェア対策 / AI（ARP / AI）

ONTAP 9.15.1で技術プレビューとして導入されたARP / AIを使用することで、NASストレージシステムの組み込みのリアルタイム検出は次のレベルに引き上げられます。AIを活用した新しい検出テクノロジーは、100万件を超えるファイルやさまざまな既知のランサムウェア攻撃についてトレーニングされています。ARPで使用する信号に加えて、ARP/AIはヘッダー暗号化も検出します。AIパワーと追加信号により、ARP/AIは99%以上の検出精度を実現します。これは、ARP/AIに最高のAAA評価を与えた独立したテストラボであるSE Labsによって検証されています。

モデルのトレーニングはクラウドで継続的に行われるため、ARP / AIはラーニングモードを必要としません。オンになった瞬間にアクティブになります。継続的なトレーニングとは、ARP / AIが発生したときに常に新しいタイプのランサムウェア攻撃に対して検証されることも意味します。ARP/AIには、自動更新機能も搭載されており、ランサムウェアの検出を最新の状態に保つために、すべてのお客様に新しいパラメータを提供します。ARPの他のすべての検出、インサイト、およびデータ復旧ポイント機能は、ARP/AI用に維持されます。

ARP/AIを有効にするには"ONTAP One"、ライセンスが必要です。

詳細

- ["ブログ：NetAppのAI-based real-time ransomware detection solution achieves AAA rating"](#)

ONTAPでのサイバーウォールティングによるエアギャップによるWORM保護

NetAppのサイバーボルトへのアプローチは、論理的にエアギャップを埋めるサイバーボルトのために構築されたリファレンスアーキテクチャです。このアプローチでは、SnapLockなどのセキュリティ強化テクノロジーやコンプライアンステクノロジーを活用して、変更や消去が不可能なSnapshotを作成できます。

SnapLock Complianceと論理的なエアギャップによるサイバーウォールティング

攻撃者がバックアップコピーを破棄し、場合によっては暗号化する傾向が高まっています。そのため、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を使用することを推奨しています。

問題は、従来のエアギャップ（テープとオフラインメディア）によってリストア時間が大幅に増加し、ダウンタイムと全体的な関連コストが増加することです。エアギャップソリューションに対するより現代的なアプローチでさえ、問題が発生する可能性があります。たとえば、新しいバックアップコピーを受信するためにバックアップウォールトを一時的に開いてから、プライマリデータへのネットワーク接続を切断して閉じ、再び「エアギャップ」状態にすると、攻撃者はこの一時的なオープンを利用する可能性があります。接続がオンラインになっている間に、攻撃者がデータを侵害または破壊する可能性があります。このタイプの設定は、一般に不要な複雑さを追加します。論理的なエアギャップは、バックアップをオンラインに維持しながらセキュリティ保護の原則が同じであるため、従来のエアギャップや最新のエアギャップの代替として最適です。NetAppでは、変更不可のスナップショットとNetApp SnapLock Complianceを使用して、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。

[NetApp Cyber Vaultとの論理的なエアギャップ]

NetAppは、医療保険の携行性と責任に関する法律（HIPAA）、サーベンスオクスリー法、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するために、10年以上前にSnapLock機能をリリースしました。また、プライマリSnapshotをSnapLockボリュームにバックアップしてコピーをWORM状態にコミットし、削除を回避することもできます。SnapLockライセンスには、SnapLock ComplianceとSnapLock Enterpriseの2つのバージョンがあります。NetAppでは、ランサムウェア対策のためにSnapLock Complianceを推奨しています。ONTAP管理者やNetAppサポートがSnapshotをロックして削除できない特定の保持期間を設定できるためです。

詳細

- ["ブログ：ONTAP cyber vault overview"](#)

スナップショットの改ざん防止

SnapLock Complianceを論理的なエアギャップとして活用することで、攻撃者によるバックアップコピーの削除を防止できますが、SnapVaultを使用してSnapshotをセカンダリSnapLock対応ボリュームに移動する必要があります。そのため、多くのお客様がネットワーク経由でセカンダリストレージにこの構成を導入しています。これにより、プライマリストレージにプライマリボリュームのSnapshotをリストアするよりもリストア時間が長くなる可能性があります。

ONTAP 9.12.1以降では、改ざん防止スナップショットを使用して、プライマリストレージとプライマリボリュームのスナップショットをほぼSnapLock Complianceレベルで保護できます。SnapVaultを使用してSnapLockedのセカンダリボリュームにSnapshotをバックアップする必要はありません。改ざんを防止するSnapshotには、SnapLockテクノロジーを使用して、ONTAPのフル管理者が同じSnapLock保持期限を使用している場合、プライマリSnapshotが削除されないようにします。これにより、リストア時間が短縮され、改ざん防止されたSnapshotを使用してFlexCloneボリュームをバックアップできるようになります。これは、従来のSnapLock Complianceで保存されたSnapshotではできません。

SnapLock Compliance SnapLock Complianceスナップショットと改ざん防止スナップショットの主な違いは、保存されたスナップショットがまだ有効期限に達していない場合、SnapLock ComplianceではONTAPアレイの初期化と消去を実行できない点です。スナップショットの改ざんを防止するには、SnapLock Complianceライセンスが必要です。

詳細

- ["Snapshotをロックしてランサムウェア攻撃から保護"](#)

Digital Advisorによるランサムウェア対策

Active IQを基盤とするDigital Advisorは、NetAppストレージのプロアクティブなケアと最適化を、実用的なインテリジェンスによって簡素化し、最適なデータ管理を実現します。多様なインストールベースから得られるテレメトリデータを活用し、高度なAIとML技術を駆使して、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を発見します。

だけで ["NetAppデジタルアドバイザー" "セキュリティの脆弱性を排除"](#)なく、ランサムウェアからの保護に特化した分析情報やガイダンスも提供します。専用の健全性カードに必要な対処方法と対処されたリスクが表示されるため、システムがこれらのベストプラクティスの推奨事項を満たしていることを確認できます。

[NetAppデジタルアドバイザーダッシュボードの健全性監視]

[Ransomware Defense Wellness]ページで追跡されるリスクとアクションには、次のものが含まれます（その他多数）。

- ボリュームのSnapshot数が少ないため、ランサムウェアによる保護の可能性が低下しています。
- NASプロトコル用に設定されたすべてのStorage Virtual Machine (SVM) でFPolicyが有効になっているわけではありません。

ランサムウェア対策の実際の動作については、を参照してください["Digital Advisor"](#)。

NetAppランサムウェア保護による包括的な回復力

ランサムウェアの検出は、拡散を防ぎ、コストのかかるダウンタイムを回避できるように、できるだけ早く実施することが重要です。しかし、ランサムウェアを効果的に検出するには、複数の保護レイヤが必要です。NetAppのランサムウェア保護は、NetApp Consoleを使用したデータ サービスにまで拡張されるリアルタイムのオンボックス機能と、サイバー ボールディング用の分離された階層化ソリューションを含む包括的なアプローチを採用しています。

NetAppランサムウェア保護

NetApp Consoleは、包括的かつワークロード中心のランサムウェア防御をインテリジェントにオーケストレーションする単一のコントロールプレーンです。NetAppランサムウェア保護は、ARP、FPolicy、改ざん防止スナップショットなどのONTAPの強力なサイバーレジリエンス機能と、NetApp Backup and RecoveryなどのNetAppデータサービスを組み合わせています。自動化されたワークフローによる推奨事項やガイダンスも追加されており、単一のUIでエンドツーエンドの防御を実現します。ワークロードレベルで動作し、業務を支えるアプリケーションを保護して、攻撃が発生した場合に可能な限り迅速にリカバリを行えるようにします。

[NetApp Ransomware Protection は、ワークロードデータの損失を最小限に抑え、迅速に回復するために必要なAIベースのインテリジェンスと支援です。この画像はNetApp ConsoleUIを示しています。]

お客様にもたらされるメリット：

- ランサムウェアへの備えを支援することで、運用上のオーバーヘッドを軽減し、効果を向上
- AI / MLを活用した異常検出により、高い精度と迅速な対応でリスクを抑制
- アプリケーションと整合性のあるガイド付きリストアにより、ワークロードを数分で簡単にリカバリできます。

"NetAppランサムウェア保護"これらのNIST機能をより簡単に実現できます。

- アプリケーションベースの最上位のワークロードに重点を置いて、NetAppストレージ*内のデータを自動的に*検出*し、優先順位を付けます*。
- トップワークロードのデータバックアップ、不変で安全な構成、悪意のあるファイルブロッキング、さまざまなセキュリティドメインのワンクリック保護。
- 次世代のAIベースの異常検出*を使用して、*ランサムウェアを*可能な限り*迅速に*正確に検出*します。
- 自動化された応答とワークフロー、およびトップ* SIEMおよびXDRソリューションとの統合*。
- シンプルな*オーケストレーションされたリカバリ*を使用してデータを迅速にリストアし、アプリケーションのアップタイムを短縮します。
- ランサムウェア対策*戦略と*ポリシー*を導入し、*成果を監視*します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。