

# ONTAPのセキュリティ機能



## 社会に欠かせないリソース、データを安全に保護

NetApp® ONTAP®データ管理ソフトウェアは、ソリューションにセキュリティ機能を組み込んだ、進化し続ける製品です。ONTAPの最新リリースには多数のセキュリティ機能が新しく追加され、ハイブリッド クラウド全体でのデータ保護や、ランサムウェア攻撃の阻止、業界のベストプラクティスへの準拠を目指す組織にとって、計り知れない価値をもたらします。これらの新機能は、組織のゼロトラスト モデルへの移行も支援します。

ONTAPソリューション強化の詳細については、『[TR-4569: Security Hardening Guide for NetApp ONTAP](#)』を参照してください。

課題

今日の企業はデジタル変革の実現を迫られています。企業のハイブリッド クラウド全体のデータはますます分散化が進み、動的で多様になっているため、管理を効率化する必要があります。ITをとりまく脅威は日増しに拡大、複雑化し、危険性が高まっていることから、ITチームは、データや情報の管理者兼運用者として、データのライフサイクルを通じて安全にデータを管理し、維持することが期待されています。

ソリューション

NetApp ONTAPソフトウェアは、データを保護し、コンプライアンス要件を満たすための中心的存在です。このデータシートおよび『TR-4569: Security Hardening Guide for NetApp ONTAP』は、業界で実証されたセキュリティ体制を作り、最も重要なリソースであるデータを守るために欠かせないものです。

主なメリット

データの機密性、整合性、可用性を向上

ONTAPのハイブリッド クラウド セキュリティ テクノロジにより、企業の最も重要なリソースであるデータを保護

セキュリティ体制の強化

セキュアなインフラを構築するための可視性とセキュリティ機能を活用して、企業のハイブリッド クラウド全体でセキュアな基盤を確立

ネットアップと業界のベストプラクティスをセキュリティとランサムウェア対策に適用

ネットアップの専門知識と業界のノウハウを活かした、検証済みのセキュリティ基盤を構築

ガバナンスとコンプライアンスの要件に対応

セキュリティに関して、確立されたベストプラクティスを使用して業界の規制に準拠し、セキュリティのコンプライアンスを実現

ONTAPのセキュリティ機能

ソフトウェア / 機能名	機能	影響
自律型ランサムウェア対策	機械学習によって攻撃を予防的に検知する自律型ランサムウェア対策機能が標準搭載されています。	異常が検出されると、ONTAPは自動的にSnapshotコピーを作成し、管理者にアラートを送ります。
NetApp Snapshot™コピー	ONTAP Snapshotは、効率に優れたポイントインタイムの読み取り専用のデータ コピーです。Snapshotは、数時間前、数日前、数週間前、数カ月前、数年前など、Snapshotが取得された時点でのデータの状態を表すものです。	Snapshotコピーは読み取り専用なので、ランサムウェアに感染することはありません。ランサムウェア攻撃から復旧するには、攻撃を受ける前に取得したSnapshotからリストアするだけです。
NetApp SnapLock®テクノロジー	NetApp SnapLockは、論理的なエアギャップによる隔離でデータ消去を完璧に防止するバックアップを実現し、NetApp SnapVault®を使用したSnapshotコピーを保護します。	SnapLockを利用することで、管理者の人為的なミスや、不満を抱いている従業員、盗んだクレデンシャルを悪用しようとする人物によってSnapshotコピーが削除されるリスクがなくなります。
Snapshotコピーロック	Snapshotコピーロックは、SnapLockテクノロジーを使用して、指定した期間手動または自動でSnapshotを消去できないようにします。	Snapshotは、管理者の人為的なミス、不満のある従業員や盗難されたクレデンシャルを悪用した第三者によって削除されかねません。
NetApp FPolicyテクノロジー	FPolicyはONTAPのインフラ コンポーネントで、パートナーアプリケーションを使用してファイルのアクセス権限を監視および設定できます。ファイル ポリシーはファイル タイプに基づきます。FPolicyは、ストレージ システムが個々のクライアントシステムから受信する作成、表示、名前の変更、削除などの操作の要求を処理する方法を指定します。  注意：ONTAPでは、FPolicyのファイル アクセス通知フレームワークが強化され、フィルタリング制御と短時間のネットワーク遮断への耐障害性が追加されます。	アクセス制御はセキュリティ構造の要です。したがって、ファイル アクセスやファイル操作を可視化し、応答できるようにすることは、セキュリティ体制の維持に欠かせません。可視性とファイル アクセス制御を提供するため、ONTAPソリューションではFPolicy機能を使用しています。NetApp Cloud Insights / Cloud Secureなど外部のFPolicyサーバでは、ユーザ行動分析を利用してマルウェアやランサムウェアを特定し、広い意味でのデータ侵害の影響を軽減します。
NetApp Volume Encryption (NVE)	NVEはソフトウェアベースの暗号化技術で、ボリュームごとに一意のキーを使用して、あらゆるタイプのディスクのデータを暗号化できます。	保存データの暗号化は、今でも業界の注目を集めています。NVEは、この期待に応えるとともに、他のセキュリティ関連機能を通じて、強力なセキュリティ体制をハイブリッド クラウド全体で維持します。
NVEでのセキュアな削除	この機能では、コマンドを使用して無害なファイルを移動し、感染ファイルの暗号化に使用したキーを削除することで、NVEボリューム上で削除したファイルを暗号化によって破棄できます。	システムの使用中であっても、データ流出をオンラインで修復できます。また、この機能は、GDPR（一般データ保護規則）の最新の「データ削除権」にも対応します。
NetApp Aggregate Encryption (NAE)	NAEはソフトウェアベースの暗号化技術で、暗号化ボリューム全体で共有されるアグリゲートごとに一意のキーを使用して、あらゆるタイプのディスクのデータを暗号化できます。	NVEと同様に、NAEでは保存データを暗号化できます。NAEではアグリゲート重複排除が利用可能で、ボリュームがアグリゲート間でキーを共有するため、ストレージ効率が大幅に高まります。

## ONTAPのセキュリティ機能

ソフトウェア / 機能名	機能	影響
デフォルトのDAR（保存データ）暗号化	外部のキー管理ツールまたはオンボード キー マネージャ ツールのいずれかが定義されている場合、デフォルトでDAR暗号化が有効になります。NVEまたはNAEのどちらかのソフトウェアベースの暗号化機能が使用されます。クラスタ構成の一部にNSEドライブが含まれる場合、DAR暗号化が適用され、デフォルトではソフトウェアベースの暗号化は使用されません。	デフォルトでDAR暗号化を使用することで、ハイブリッド クラウド全体で、強力なセキュリティ体制を容易に維持できます。
NetApp Storage Encryption (NSE)	NSEは、FIPS-140-2レベル2の自己暗号化ドライブを使用することで、ネットアップにFull Disk Encryption (FDE; フルディスク暗号化) を実装するものです。さらにNSEでは、ネットアップのストレージ効率化テクノロジーを全面的にサポートするシステム停止ゼロの暗号化が提供されます。	保存データの暗号化は、今でも業界の注目を集めています。NSEでは、この期待に応えるFDEを提供します。ネットアップ データ ファブリックは、エンドツーエンドの強力なセキュリティ体制を維持します。
Intel AES New Instructions (AES-NI) 高速化を使用するSMB暗号化	Intel AES-NIではAESアルゴリズムが向上していて、サポートされるプロセッサ ファミリーでデータ暗号化を高速化します。	セキュリティ機能を高速化することで効率性を高めます。リソースの効率的な使用は、セキュリティ ソリューションの成功に欠かせません。
NetApp暗号化セキュリティ モジュール	このモジュールでは、選択したSecure Sockets Layer (SSL) ベースの管理サービスに対して、FIPS 140-2認証の暗号化機能を使用できます。ONTAP 9.11.1からTLS 1.3がサポートされたことで、FIPS 140-2認証への準備が可能になりました。	専用セキュリティ モジュールにより、リソース効率が向上します。さらに、FIPS 140は、暗号化製品や暗号化ソリューションの業界標準として認められています。
NetApp CryptoMod	このモジュールにより、NVE、NAE、およびOKM（オンボード キー マネージャ機能）でFIPS 140-2認証の暗号化機能を使用できます。	FIPS 140-2は、暗号化製品や暗号化ソリューションの業界標準として認められています。
SHA-2 (SHA-512) のサポート	パスワードのセキュリティを強化するため、ONTAPではSHA-2パスワード ハッシュ機能をサポートし、デフォルトでSHA-512を使用して、新規作成または変更されたパスワードのハッシュ化を行います。	SHA-2は、侵入を受けることが多いSHA-1基準に比べてセキュリティ体制が大幅に向上しているため、ハッシュ機能の業界標準となっています。
セキュアなログ転送 (Transport Layer Security [TLS] によるsyslog転送)	ログの転送元と転送先を指定して、転送先でsyslogや監査情報を受信できるようにする機能です。syslogや監査情報は安全管理が必要なため、ONTAPではこの情報を、TCP暗号化パラメータを使用することで、TLS経由でセキュアに送信できます。	ログや監査情報は、サポートやシステム可用性の観点から組織に欠かせません。また、ログ (syslog) や監査レポート、出力結果には、通常、取り扱いに注意を要する情報が含まれています。セキュリティの仕組みが崩れないよう常にコントロールするには、ログと監査データをセキュアな方法で管理することが必要です。
TLS 1.1およびTLS 1.2	ONTAPでは、セキュアな通信と管理機能にTLS 1.1とTLS 1.2を使用します。	TLS 1.0はきわめて脆弱で、PCI-DSSなどのコンプライアンス標準を満たせないことから、ネットアップは使用を推奨していません。ネットアップが推奨するのは、強力で信頼性に優れたTLS 1.1とTLS 1.2です。
Online Certificate Status Protocol (OCSP)	OCSPが有効な場合、TLS通信 (LDAP、TLSなど) を使用するONTAPアプリケーションは、デジタル証明書の失効状態を確認できます。アプリケーションは受信した署名付き応答から、要求した証明書の状態が有効 (good)、失効 (revoke)、不明 (unknown) のいずれであるかを知ることができます。	OCSPを使用することで、Certificate Revocation List (CRL; 証明書失効リスト) を要求しなくてもデジタル証明書の現在の状態を判断できます。
オンボード キー マネージャ (OKM)	ONTAPのOKMは、保存データ向けの自己完結型暗号化ソリューションを提供します。OKMはNVEと連携し、データの暗号化とあらゆるタイプのディスク使用を可能にするソフトウェアベースの暗号化メカニズムを提供します。また、NSEとの連携を通じて、自己暗号化ドライブを使用することでFDEに対応します。	OKMはNSEとNVE向けのキー管理機能を提供します。さらに、ONTAPでこの暗号化テクノロジーを使用することで、保存データを保護でき、重要なセキュリティ ソリューションを提供します。
OKMセキュア ブート	このオプションにより、ノードの再起動後、ドライブのロック解除とボリュームの復号化の際にパスフレーズを要求できます。	NSEとNVEでOKMを使用すると、セキュア ブート機能により、ドライブだけでなくストレージ アレイ全体が盗難から保護されます。また、クラスタ全体の物理的移動と機器の返却も保護できます。



## ONTAPのセキュリティ機能

ソフトウェア / 機能名	機能	影響
外部キー管理	外部キー管理は、ストレージ環境のサードパーティ製システムを使用して実施されます。このサードパーティ製システムは、NSE、NVE、NAEなどのストレージ システムの暗号化機能で使用する認証キーや暗号化キーを安全に管理します。ストレージ システムはSSL経由で外部のキー管理サーバに接続し、Key Management Interoperability Protocol (KMIP) を使用して認証キーやボリューム データの暗号化キーを読み出し、保管します。	外部キー管理を使用することで、組織のキー管理機能を一元化しながら、資産の付近でキーが保管されるのを避けることができます。これにより、データが危険にさらされる可能性が減少します。
セキュア マルチテナンシー	セキュア マルチテナンシーとは、複数の異なるテナント間で物理環境を共有する目的で、共有の物理ストレージ環境に設けられたセキュアな仮想パーティションを使用することで、ONTAPでは、このパーティションをStorage Virtual Machine (SVM) と呼びます。	セキュア マルチテナンシーにより、SVMでプラットフォーム内のすべてのテナントをセキュアに隔離することで、ONTAPは共有プラットフォームの機能を果たします。
マルチテナント外部キー管理	マルチテナント外部キー管理では、個々のテナントやストレージ仮想マシン (SVM) で、NVE向けKMIPを使用して独自のキーを保持できます。	マルチテナント外部キー管理を使用することで、組織のキー管理機能を部門やテナント別に一元化しながら、資産の付近でキーが保管されるのを避けることができます。これにより、データが危険にさらされる可能性が減少します。
クラスタ型外部キー管理機能	外部キー管理サーバ (KMIP) の冗長性は、ネットアップのKMIPキー サーバ パートナーが提供するクラスタリング機能によってサポートされています。ONTAP 9.11.1以前では、最大4つの外部KMIPサーバを定義でき、ONTAPは各サーバにキーを書き込んで冗長性を提供できました。	ONTAPのお客様には、クラスタ型外部キー管理機能の採用が広がっています。ONTAPでこの機能がサポートされたため、お客様はこの機能を完璧な状態で利用できます。
ファイルシステム監査の強化	ONTAPでは、ソリューション全体でレポートされる監査のイベントや詳細の数が増加しています。イベントが作成されると、キーに関する以下の詳細情報が記録されます。 ファイル フォルダ 共有アクセス 作成、変更、または削除されたファイル ファイル読み取りアクセスの成功 フィールドの読み取りまたはファイルの書き込みの失敗 フォルダ アクセス権の変更	NASファイルシステムは、今日の脅威の状況の中でシェアを高めてきました。そのため、監査機能によって可視性を確保することは依然として非常に重要です。ネットアップはONTAPの監査機能を増強することで、これまで以上に詳細なCIFSの監査を可能にしています。
CIFS SMBの署名と封印	SMBの署名は、ストレージ システムとクライアントの間のトラフィックを保護することで、反射攻撃や中間者攻撃からデータ ファブリックのセキュリティを保護するために役立ちます。また、SMBメッセージの署名の有効性も確認します。さらに、ONTAPでは、SMB暗号化による封印もサポートします。	一般的に、ファイルシステムやアーキテクチャに対する脅威ベクトルはSMBプロトコル内に潜んでいます。署名と封印により、共有ベースのセキュアなデータ転送に加えて、トラフィックの完全な検証が可能となります。
Kerberos 5とkrb5pのサポート	ONTAPは128-bitおよび256-bitのKerberos向けAES暗号化をサポートします。プライバシー サービスには、受信データの整合性の確認、ユーザ認証、転送前のデータ暗号化の各機能が含まれます。	krb5p認証は、チェックサムを使用してクライアントとサーバの間のすべてのトラフィックを暗号化することで、データの改ざんとスヌープから保護します。
Lightweight Directory Access Protocol (LDAP) SMBの署名と封印	ONTAPは、LDAPサーバへのクエリの際にセッションのセキュリティを保護するための署名と封印をサポートします。	署名機能では、秘密キーのテクノロジーを使用してLDAPペイロード データの整合性を確認します。署名によりLDAPペイロード データを暗号化し、平文での機密情報の送信を防ぎます。
Secure Shell (SSH) のEd25519およびNIST曲線 (最新アルゴリズムとハッシュベース方式の認証コード[ HMAC])	ONTAPは、AES、3DES、SHA-256、SHA-512など、最新のSSH暗号とキー交換機能を提供します。	脅威の状況がますます深刻になり、プロトコルと製品機能の整合性を保つうえで、強力なプロトコル アルゴリズム、暗号、キー交換の重要度が非常に高まっています。

## ONTAPのセキュリティ機能

ソフトウェア / 機能名	機能	影響
<b>SSHログイン試行失敗の最大回数の設定機能</b>	ONTAPでは、security ssh modifyコマンドにparameter-max-authentication-retry-countが追加され、ログイン試行の最大回数を設定できるようになりました。1回のSSH接続で可能なデフォルトの最大回数は6回ですが、ネットアップでは、セキュリティのベストプラクティスとして3回を推奨しています。	この機能は、ブルートフォース攻撃からの保護に役立ちます。
<b>多要素認証 (MFA)</b>	NetApp ONTAP System ManagerとNetApp Active IQ® Unified Managerでは、Security Assertion Markup Language (SAML) と外部IDプロバイダによる管理者WebアクセスでMFAを使用できます。ONTAPへのコマンドラインを通じた管理者アクセスは、ユーザIDとパスワードおよびパブリック キーを使用するローカル2段階認証方式によって実行できます。SSHコマンドライン管理者アクセスのための2段階認証の1要素として、パブリック キーを含むnsswitchを使用できます。FIDO2は、Yubikeyハードウェア認証機器または他のFIDO2と互換性のある機器を使用して、SSH認証にも使用可能です。	システム侵害の原因のほとんどは、管理者アクセスの脆弱な資格情報です。MFAを使用することで、単純なパスワードベースのアカウントで管理者としてアクセスすることはできなくなります。
<b>NetApp SnapLockテクノロジーとNSEおよびNVE</b>	ONTAPは、NSEおよびNVEでSnapLock機能をサポートしています。この機能により、Write Once, Read Many (WORM) データを管理し、保存できます。	SnapLockテクノロジーにより、消去不可、再書き込み不可の状態ではファイルを保存できる特殊用途のボリュームが作成されます。SnapLockは、NSEおよびNVEソリューションのセキュアな体制 (暗号化) を維持しながら、この状態を無期限または指定した保持期間、保持することができます。
<b>アップグレード イメージの検証</b>	ONTAPのアップグレードでは、イメージが本物のONTAPであることをアップグレード時に検証します。	この検証により、アップグレード プロセスでの破損イメージや偽造イメージの使用が検出されます。
<b>Unified Extensible Firmware Interface (UEFI) セキュア ブート</b>	システムを起動するたびにイメージの検証が行われます。	署名済みのONTAPイメージがブート ロードで検証されるので、起動のたびに偽造イメージの使用が防止されます。
<b>クラスタ ピア暗号化</b>	クラスタ ピア暗号化では、TLS 1.2を使用して、データの複製にクラスタ ピアリングを使用する基盤のONTAP機能 (NetApp SnapMirror®, SnapVault®, FlexCache®) とクラスタ ピアとの間で、ネットワークを介して送信されるすべてのデータを暗号化します。	データを複製するONTAP機能では、転送時の暗号化を使用できます。さらに、保存データの暗号化 (NVE / NSE) では、クラスタ ピア暗号化を使用するONTAPクラスタ間でエンドツーエンドの暗号化を実行できます。
<b>IPSec暗号化</b>	IPSecは、NFS、iSCSI、SMB / CIFSなどのプロトコルによるすべてのIPトラフィックに対して、転送中のデータ暗号化を提供します。	IPSecは、転送中のデータを継続的に安全に暗号化します。クライアントとONTAPの間のネットワーク トラフィックは、反射攻撃や中間者 (MITM) 攻撃に対抗するための予防策によって保護されます。
<b>ロールベース アクセス制御 (RBAC)</b>	ONTAPのRBACでは、定義されたロールに許可されるレベルにユーザの管理アクセスを制限できます。この機能を使用して、管理者は割り当てたロール別にユーザを管理できます。	アクセス制御は、セキュリティ システムを構成する基本要素です。RBACなどの機能を利用すると、組織は、誰がどの範囲のデータにアクセスできるかを定義し、データ漏洩や権限のエスカレーションなど、セキュリティの脆弱性を狙った行為や権限の乱用に歯止めをかけることができます。
<b>マルチ管理者認証 (MAV)</b>	MAVIは、1人以上の管理者の承認がなければ、単独のクラスタ管理者が「ボリューム スナップショットの削除」や「ボリューム削除」など慎重な扱いを要するコマンドを実行できないようにします。	MAVを導入することで、悪意のある管理者や乗っ取られた管理者アカウントが貴重なデータを破壊できないようになります。ONTAPのデータ主体のゼロトラスト環境を強化するためには、この機能が不可欠です。
<b>ウイルス対策コネクタ (ウイルススキャン)</b>	ウイルス対策コネクタとウイルス対策ソフトウェアを実行するVscanサーバでは、ウイルススキャンが行われます。通常、ONTAPを実行するシステムでは、クライアントがファイルの変更またはアクセスを行うと、ファイルがスキャンされるように設定されています。	脅威や攻撃の手段は進化し続けています。したがって、アクセスまたは変更が行われたファイルをオンラインでウイルススキャンすることで、組織のファイルの整合性を守るために役立ちます。

## ONTAPのセキュリティ機能

ソフトウェア / 機能名	機能	影響
ログイン バナーとMessage-Of-The-Day (MOTD) バナー	ログイン バナーは認証プロセスの前に表示されるバナーです。組織や管理者は、ログイン バナーやMOTDバナーを使用してシステム ユーザにメッセージを伝えることができます。	ログイン バナーを使用すると、オペレータ、管理者、さらには不正なユーザにも、システムで認められる使用条件について知らせることができます。また、システムへのアクセスを許可されているユーザについても表示されます。
ディスク完全消去	ディスク完全消去は、ディスクまたはディスク セットのデータを消去して、そのデータを復元できないようにします。	セキュリティ プロトコルでは、ディスクでデータを復元できないようにすることを求められる場合がありますが、このディスク完全消去機能を使用して、それを実現できます。