データシート

ONTAP 9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

主なメリット

データの機密性、整合性、可用性を向上
ONTAPデータ ファブリックのセキュリティ構造を使用して、組織で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
組織のデータ ファブリックにセキュアな基盤を構築し、セキュアなインフラを実現する可視性とセキュリティを提供

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

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 9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と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 9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 9』を参照してください。

主なビジネス課題

今日の企業はデジタル変革の実現を迫られています。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、ストレージ エンジニアは、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 9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 9』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。

NetApp®

ONTAP 9のセキュリティ機能

表1は、ONTAP 9のセキュリティ機能について解説しています。

ソフトウェア / 機能名	特長	影響
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。
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のいずれ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はAESアルゴリズムを向上させたものであり、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。	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 140-2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。
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 9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や監査情報は安全な管理が必要なため、ONTAP 9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することができます。	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 9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 9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 9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と連係し、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との連係を通じて、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 9でこの暗号化テクノロジを使用することで、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。

表1）セキュリティ機能

ソフトウェア / 機能名	特長	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され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。
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。
ファイル システム監査の強化	ONTAP 9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 9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 9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 9では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 9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 9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。
SSHログイン試行失敗の最大回数の設定機能	ONTAP 9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。
多要素認証（MFA）	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。	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。

ソフトウェア / 機能名	特長	影響
NetApp SnapLock®テクノロジとNSEおよびNVE	ONTAP 9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テクノロジにより、消去不可、再書き込み不可の状態で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。
アップグレード イメージの検証	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。
Unified Extensible Firmware Interface（UEFI）セキュア ブート	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 ローダで検証されるので、起動のたびに偽造イメージの使用が防止されます。
クラスタ ピア暗号化	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。
ロールベース アクセス制御（RBAC）	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。
ウィルス対策コネクタ（ウィルススキャン）	ウィルス対策コネクタとウィルス対策ソフトウェアを実行するVscanサーバでは、ウィ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インラインでウィ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。
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多くありますが、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。
NetApp FPolicy™テクノロジ	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 9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。

表1）セキュリティ機能

ネットアップについて

ネットアップは、ハイブリッド クラウド環境におけるデータ管理のオーソリティです。クラウド環境からオンプレミス環境にわたるアプリケーションとデータの管理を簡易化し、デジタル変革を加速する包括的なハイブリッド クラウド データ サービスを提供しています。グローバル企業がデータのポテンシャルを最大限に引き出し、お客様とのコンタクトの強化、イノベーションの促進、業務の最適化を図れるよう、パートナー様とともに取り組んでいます。詳細については、www.netapp.com/jpをご覧ください。#DataDriven

ネットアップ合同会社
TEL:03-6870-7600 Email:ng-sales-inquiry@netapp.com

DS-3846-1019-jaJP