データシート

EシリーズSANtricity OSのセキュリティ機能

社会に欠かせないリソース、情報を安全に保護

主なメリット

データの機密性、整合性、可用性を向上
NetApp EシリーズSANtricityのセキュリティ機能と組み込みの管理機能を活用して、組織の最も重要なリソースであるデータの機密性、整合性、可用性を強化

お客様の環境のセキュリティ システムを確立
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活用
ネットアップの専門知識、業界のノウハウ、一般的な手法を活かした、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活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® SANtricity®ストレージ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。EシリーズSANtricityの数々のセキュリティ機能は、セキュリティ システムを維持し、業界のベストプラクティスへの準拠を目指す組織に計り知れない価値をもたらします。SANtricityの新しい機能があれば、データの機密性、整合性、可用性に最優先で取り組めます。

EシリーズSANtricity OS 11.50は、ネットワーク デバイスのコラボラティブ プロテクション プロファイル（NDcPP）向け情報セキュリティ国際評価基準の認定を受けています。詳しくはこちらをご覧ください。

ネットアップが推進するセキュリティ ソリューションとセキュリティ管理ソリューションについては、TR-4474『NetApp SANtricity Drive Security』とTR-4712『NetApp SANtricity Management Security』をご覧ください。

主なビジネス課題

ITをとりまく脅威が日増しに拡大、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、データや情報資産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することが期待されています。

ソリューション

このデータシートでは、SANtricity 11.50以降のセキュリティ機能について、標準搭載の機能と新たに加わった機能の概要を紹介します。重要なリソースであるデータを保護するには、実績のあるセキュリティ システムが必要です。その構築に欠かせない要素がわかります。

証明書の失効状態を確認するセキュリティ機能

ソフトウェア / 機能名	特長	影響
Online Certificate Status Protocol（OCSP）による証明書の失効状態の確認	TLS通信（LDAP、TLSなど）を使用するEシリーズのアプリケーションは、OCSPを使用して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。 情報セキュリティ国際評価基準では、OCSPを有効にする設定が推奨されています。	OCSPを有効にすると、証明書の失効状態を確認するための検証が実行されます。

暗号化によるセキュリティ機能

ソフトウェア / 機能名	特長	影響
Transport Layer Securityプロトコルで管理インターフェイスに対応	Eシリーズは、管理GUI、セキュアなCLI、REST APIにTLS v1.2を活用して、セキュアな通信と管理機能を実現します。	TLS v1.0とTLS v1.1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、ネットアップはこの2つのバージョンの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 v1.2です。
FIPS準拠の暗号化	Eシリーズは、FIPS 140-2レベル1準拠の暗号化APIコレクション、Bouncy Castleですべてのデータを暗号化します。	FIPS 140-2レベル1は、暗号化製品や暗号化ソリューションの業界標準です。

データ セキュリティ機能

ソフトウェア / 機能名	特長	影響
Full Disk Encryption（FDE）	FDEは、自己暗号化ドライブのデータを暗号化するハードウェアベースの暗号化技術です。FIPS140-2認定取得のFDE対応ドライブにより、FIPS140-2準拠の暗号化アルゴリズムを使用してディスクのデータを暗号化します。	保存データの暗号化が業界の注目を集めているのは、今も変わりません。FDE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の仕組みをサブシステム レベルで維持します。
FDE内部キー管理	FDE内部キー管理機能は、保存データ向けの自己完結型暗号化ソリューションです。内部キー管理に、自己暗号化ドライブを使ってフルディスク暗号化を実行するFDEを使用します。	FDE内部キー管理は自己完結型ソリューションです。外部キー管理サーバへの投資を避けて、TCOを削減したい組織に適しています。保存データの保護にも役立つ、重要なデータ セキュリティ ソリューションです。
FDE外部キー管理	FDE外部キー管理は、ストレージ環境に配置されたサードパーティのシステムを使用して、ストレージ システムの暗号化機能（FDEなど）が使用する認証キーをセキュアに管理するソリューションです。ストレージ システムはSSL経由で外部のキー管理サーバ（Gemalto SafeNet KeySecureなど）に接続し、業界標準のKey Management Interoperability Protocol（KMIP）を使用して認証キーを読み出し、保管します。	FDE外部キー管理は、組織のキー管理機能を一元化し、キーが資産の近くに保管されないように図ることで、データが危険にさらされる可能性を抑えます。
FDE対応ドライブ向けのSecure Erase	Secure Erase機能を使用すると、FDE対応ディスクのデータを削除して、ディスクの完全消去を実現できます。複数のディスクのデータをまとめて削除することも可能で、一度削除したデータは決してリカバリできません。	ドライブを廃棄したり転用したりする際には、セキュリティ上、データをリカバリ不能にすることが必要です。

メッセージ ロギングに関するセキュリティ機能

ソフトウェア / 機能名	特長	影響
ログインバナーと本日のメッセージ(MOTD)バナー（SANtricity OS 11.40.1以降）	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 バナーを使うと、システムの運用者や管理者、場合によっては不正なユーザにも、システムを正しく使用するための条件やアクセスが許可されるユーザの種別を表示できます。
セキュアなログ転送（Transport Layer Security [TLS]によるsyslog転送）（SANtricity OS 11.40.1以降）	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ですが、Eシリーズでは、TCP暗号化パラメータを使用し、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。
Simple Network Management Protocol（SNMP v2c）	SNMPは、ネットワークに接続されたデバイス（Eシリーズ アレイ）の状態監視に使用する標準的なプロトコルです。EシリーズがサポートするSNMP v2cは、セキュリティの仕組みが強化されています（コミュニティベースの認証）。 情報セキュリティ国際評価基準では、SNMPを無効にする設定が推奨されています。	SNMPを使用すると、SNMP管理アプリケーション経由でNetApp Eシリーズ ストレージ アレイの機能を簡単に監視できます。

OS認証機能

ソフトウェア / 機能名	特長	影響
デジタル署名されたSANtricity OSファームウェア（SANtricity OS 11.40.2以降）	バージョン8.42以降にはデジタル署名されたコントローラ ファームウェアが必要です。署名のないファームウェアはダウンロードが拒否されます。 またアレイの運用開始時には、ファームウェアに変更が加えられていないかどうかを確認するための自己診断が実行されます。	不正なユーザや悪意のあるユーザが、ネットアップ以外のコード バンドルや改ざんされたコード バンドルをダウンロードしないように防止します。

ユーザ アクセスを制御するセキュリティ機能

ソフトウェア / 機能名	特長	影響
ロールベース アクセス制御（RBAC）	Eシリーズの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。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。
Lightweight Directory Access Protocol（LDAP）	企業のIT環境にストレージを導入するには、基本として、ディレクトリのユーザを認証する機能が必要です。	Eシリーズ ストレージ アレイの管理業務を実行するためのユーザをLDAPで設定し、割り当てることができます。
Secure Lightweight Directory Access Protocol（LDAPS）によるディレクトリ サービスへのアクセス	Eシリーズでは、LDAPサーバへのアクセスにセキュアな通信チャネル（LDAPS）が使用されます。	LDAPSを使用すると、機密情報がクリアテキストで伝送されるのを防止できます。
SAML 2.0テクノロジを使用した多要素認証（MFA）	Eシリーズに組み込まれたSANtricity System ManagerのGUIはSAMLに対応しています。SAMLを使用すると、アイデンティティ プロバイダ（IdP）を通じて認証を管理できます。SAMLでは、管理者がIdPシステムとストレージ アレイ間で通信を確立してから、ストレージ アレイに埋め込まれたローカルのユーザ ロールにIdPユーザをマッピングします。	SAML規格に対応することで、多要素認証ソリューションを実装して、連邦政府のID管理ガイドラインに準拠できます。
パスワード ポリシー	パスワード ポリシーは、SANtricity System Managerにログインを試みる回数をコントローラごとに設定し、回数を超えた場合に一定時間ログインをロックする機能です。 管理者は、IPアドレス ベースのロックアウト（デフォルト）と、ユーザ アカウント ベースのロックアウトの2つのモードから選んで設定できます。情報セキュリティ国際評価基準では、ユーザベースのロックアウトが推奨されています。 Eシリーズでは、パスワードに必要な文字数を最小15文字に設定できます。最大文字数は30文字です。	攻撃者がストレージ アレイに何度もアクセスを試みることができなくなり、サービス拒否攻撃を受ける可能性を抑えられます。 パスワードに必要な最小文字数を増やすと侵入が難しくなり、連邦政府の要件も満たせます。

ユーザ インターフェイスのセキュリティ機能

ソフトウェア / 機能名	特長	影響
SSHによるコンソール アクセス	Eシリーズでは、アレイのコンソールへの接続にSSHを使用できます。 情報セキュリティ国際評価基準では、SSHアクセスを無効にする設定が推奨されています。	一般にストレージ アレイでは、問題のトラブルシューティング時にSSHでコンソールにアクセスします。この作業は通常、ネットアップのカスタマー サポート チームが提供するガイダンスに沿って行われます。
プロトコルとポートを保護する、セキュアなHTTPSプロトコルによるREST APIアクセス	EシリーズはREST APIに対応しており、これによって、ストレージ アレイと管理クライアント間に、セキュアなHTTPSプロトコルを介したセキュアな通信インターフェイスを提供します。 情報セキュリティ国際評価基準では、SYMbol（独自の通信インターフェイス）を無効にする設定が推奨されています。	REST API暗号化管理インターフェイスを使用すると、ストレージ アレイと管理クライアント間の通信を機密扱いにすることができます。
コマンドラインへのセキュアなアクセス	Eシリーズには、ストレージ アレイに通信するためのSMcliが実装されています。セキュアなCLIが提供するセキュアな通信チャネルは、クライアントとサーバ間のTLSプロトコルによるCLI通信に使用されます。	ソリューションの安全性を守るには、システムとの間にセキュアなアクセスを確立することが重要です。

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、顧客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