テクニカル レポート

PCI DSS 4.0

ONTAP 9

NetApp
Matt Trudewind
2022年9月| TR-4401

概要

本テクニカルレポートは、認定セキュリティ評価者およびストレージ管理者を対象としており、PCI DSS 4.0標準に照らしたシステムの検証に重点を置いています。本ドキュメントでは、NetApp® ONTAP® 9ストレージシステムに適用するコントロールの要件を満たすためのガイダンスを提供します。

目次

表一覧

PCI DSSの概要

このテクニカルレポートでは、NetApp® ONTAP® 9システムを実行するストレージシステムにPayment Card Industry（PCI）データセキュリティ基準（DSS）要件を適用する際に、監査担当者およびシステムオペレータが役立つガイダンスと情報を提供します。

ONTAP 9は、コントロールプレーン機能と管理プレーン機能（管理に使用）を、データユーザがアクセスするデータプレーンから分離します。このテクニカルレポートでは、コントロールプレーンでのシステム構成の管理に焦点を当てて説明します。NetAppでは、ユーザデータの要件が、ストレージシステムではなくデータに対してガバナンスを適用するアプリケーションによって満たされていると想定しています。

本レポートでは、特に2022年3月にリリースされたPCI DSS 4.0標準のガイダンスを提供することに焦点を当てています。PCI DSS 4.0は、2024年3月31日に廃止されるまで有効なPCI DSS v3.2.1に代わるものです。この日付以降のすべてのPCI DSS検証は、PCI DSS 4.0を使用して検証する必要があります。

安全なネットワークとシステムの構築と維持

要件1：ネットワークセキュリティ制御のインストールと保守

ファイアウォールやその他のネットワークセキュリティテクノロジーなどのネットワークセキュリティ制御（NSC）は、通常、定義済みのポリシーまたはルールに基づいて、2つ以上の論理または物理ネットワークセグメント（またはサブネット）間のネットワークトラフィックを制御するネットワークポリシー適用ポイントです。

NSCは、セグメントに出入りするすべてのネットワークトラフィックを調べ、定義されたポリシーに基づいて、ネットワークトラフィックが通過できるか、拒否されるかを決定します。通常、NSCは、セキュリティニーズや信頼レベルが異なる環境間に配置されます。ただし、一部の環境では、NSCは信頼境界に関係なく、個々のデバイスへのトラフィックを制御します。ポリシーの適用は一般にOSIモデルのレイヤ3で行われますが、上位レイヤに存在するデータはポリシーの決定にも頻繁に使用されます。

従来、この機能は物理ファイアウォールによって提供されていましたが、現在では、仮想デバイス、クラウドアクセス制御、仮想化またはコンテナシステム、およびその他のSoftware-Defined Networkingテクノロジによって提供されています。

NSCは、機密性の高いエリアと機密性の低いエリアの間など、エンティティ自身のネットワーク内のトラフィックを制御し、エンティティのリソースを信頼できないネットワークにさらされないように保護するために使用されます。カード所有者データ環境(CDE)は、エンティティのネットワーク内のより機密性の高い領域の例です。
多くの場合、信頼されていないネットワークとの間のパスは、機密性の高いシステムへの保護されていないパスを提供する可能性があります。NSCは、あらゆるコンピュータネットワークに重要な保護メカニズムを提供します。

信頼されないネットワークの一般的な例としては、インターネット、B2B通信チャネルなどの専用接続、ワイヤレスネットワーク、キャリアネットワーク（携帯電話など）、サードパーティネットワーク、および企業が制御できないその他のソースがあります。信頼されていないネットワークには、PCI DSSの範囲外と見なされる企業ネットワークも含まれます。企業ネットワークは評価されず、セキュリティ制御の存在が検証されないため、信頼されていないネットワークとして扱われる必要があります。企業は、インフラストラクチャの観点から内部ネットワークを信頼されていると見なすことができますが、ネットワークがPCI DSSの範囲外である場合、そのネットワークはPCI DSSでは信頼されていないと見なす必要があります。

ONTAPストレージ・システムは、PCI DSSの原則に準拠するように、外部ファイアウォールやその他のソフトウェア・デファインド・ネットワーク・テクノロジーなどの適切なNSCの背後に設置し、保護する必要があります。さらに、ONTAPは、サービスへの管理アクセスを制御するための基本的なNSCおよびファイアウォール機能を提供します。各ノードでデフォルトで有効になっており、クラスタ全体を保護します。ONTAPのバージョンに応じて、ONTAPで使用できるNSCには、サービスポリシーと組み込みのファイアウォールが含まれています。これらは、専用ファイアウォールなどの適切なNSCを置き換えるように設計されていませんが、必要に応じてプロトコルを許可またはブロックすることで、内部保護の追加層を提供します。

ONTAPのバージョンに応じて、各Storage Virtual Machine（SVM、旧Vserver）管理LIFには、ファイアウォールポリシー、サービスポリシー、またはその両方を関連付けることができます。ONTAP 9.10.1以降では、ファイアウォールサービスポリシーが廃止され、LIFのサービスポリシーに置き換えられました。以前のリリースでは、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。この機能は、ONTAP 9.10.1以降ではLIFサービスポリシーを使用して実現されます。

サービス ポリシーは、LIFでサポートされる一連のネットワーク サービスを定義します。ONTAPには、LIFに関連付けることができる一連の組み込みのサービスポリシーが用意されています。組み込みのサービスポリシーには、HTTPS、Secure Shell（SSH）、DNS、Lightweight Directory Access Protocol（LDAP）などの管理サービスが含まれます。

ファイアウォールポリシーエントリは、プロトコルタイプ、ファイアウォールアクション、およびアクションが適用されるサブネットまたは特定のIPアドレスで構成されます。各LIFにファイアウォールポリシーを適用して、そのインターフェイスを経由するすべてのトラフィックを処理できます。また、ファイアウォールポリシーはSVMごとに異なる場合があります。

NetAppでは、支払いデータを格納するSVMには、SVMの管理に必要なプロトコルと特定のサブネットまたはIPアドレスだけを許可するという、可能な限り厳密な設定を行うことを推奨しています。サービスポリシーとファイアウォールポリシーの詳細については、『ONTAP 9ネットワーク管理ガイド』を参照してください。

以前のPCI DSS 3.2.1標準からの要件の進化

- 「ネットワークセキュリティ制御」に重点を置いて、主要要件のタイトルを更新します。「ファイアウォール」および「ルータ」という用語を「ネットワークセキュリティ制御」に置き換えて、従来ファイアウォールで満たされていたセキュリティ目標を満たすために使用される幅広いテクノロジーをサポートします。
- 「概要of groups, roles and responsibilities for management of network components」の要件を、要件1の役割と責任に関する一般的な要件に置き換えます。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- ネットワークセキュリティ制御ルールセット（1.2.1）の設定標準の定義、実装、および保守について、以前のヌル要件（すべてのコンテンツが他の要件を指していた）に焦点を当て直します。
- 要件6.5.1(1.2.2)で定義された変更管理プロセスに従って変更が管理されることを明確にする。
- 少なくとも6か月に1回、ネットワークセキュリティ制御の構成をレビューする意図の明確化（1.2.7）。
- 元のヌル要件のリフォーカス（すべてのコンテンツは他の要件を指しています）。この目的は、信頼できるネットワークと信頼できないネットワーク間の制御を実装することであることを明確にします（1.4.1）。

データストレージへの影響

ベスト プラクティス

ONTAPでファイアウォールポリシーとサービスポリシーを有効にして、外部ファイアウォールやその他のソフトウェア定義ネットワークテクノロジなどのNSCを強化します。

クラスタSVMで管理トラフィックを有効にするサービスポリシーは、次のコマンドを使用して定義します。

```
 network interface service-policy create -vserver <svm_name> -policy <service_policy_name> -
services <service_name> -allowed-addresses <IP_address/mask,...>
```

表1）LIFサービス

サービス	フェイルオーバーの制限事項	説明
intercluster-core	ホームノードのみ	中核となるクラスタ間サービス

サービス	フェイルオーバーの制限事項	説明
management-core	ホームノードのみ	中核となる管理サービス
management-ssh	ホームノードのみ	SSH管理アクセス用のサービス
management-http	ホームノードのみ	HTTP管理アクセス用のサービス
management-https	ホームノードのみ	HTTPS管理アクセス用のサービス
management-autosupport	ホームノードのみ	AutoSupportペイロードの投稿に関連するサービス
management-bgp	ホームポートのみ	BGPピアのやり取りに関連するサービス
backup-ndmp-control	ホームポートのみ	NDMPバックアップ制御のサービス
management-ems	ホームポートのみ	管理メッセージングアクセスのためのサービス
management-ntp-client	ホームポートのみ	ONTAP 9.10.1で導入されました。NTPクライアントアクセス用のサービス
management-ntp-server	ホームポートのみ	ONTAP 9.11.1で導入されました。NTPサーバ管理アクセス用のサービス
management-portmap	ホームポートのみ	portmap管理用のサービス
management-rsh-server	ホームポートのみ	rshサーバ管理のためのサービス
management-snmpserver	ホームポートのみ	SNMPサーバ管理のためのサービス
management-telnetserver	ホームポートのみ	Telnetサーバ管理のためのサービス

表1のリストに、ONTAP 9.11.1以降のシステムSVMでLIFが使用できるサービスを示します。カスタムサービスポリシーにサービスを追加して、どのNSCをシステムSVMに適用する必要があるかを定義できます。詳細については、「ネットワーク管理 ONTAP」を参照してください。サービスポリシー管理の例として、次のコマンドを使用して、という名前の新しいカスタムサービスポリシーを作成し secure_management、HTTPSサービスを指定できます。このコマンドでは、カスタムポリシーを使用して適用する各サービスを指定できます。

例：サービスポリシー「secure_management」を作成する

```
Cluster1::> network interface service-policy create -vserver cluster1 -policy secure-management -
services management-https -allowed-addresses 10.2.0.0/16
```

完了したら、次のコマンドを使用して新しいポリシーをLIFに割り当てる必要があります。

```
Cluster1::> network interface modify -vserver cluster1 -lif lif1 -service-policy secure-
management
```

注： LIFの作成時にサービスポリシーを指定することもできます。

ONTAP 9.10.1以降の変更点は次のとおりです。

- ファイアウォール サービス ポリシーは廃止され、LIFサービス ポリシーに置き換えられました。以前のリリースでは、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。ONTAP 9.10.1では、オンボードファイアウォールはLIFサービスポリシーを使用して管理されます。
- ファイアウォール ポリシーはすべて空であり、基盤となるファイアウォールでいずれのポートも開きません。代わりに、LIFサービスポリシーを使用してすべてのポートを開く必要があります。
- ONTAP 9.10.1以降にアップグレードしたあとも、ファイアウォールサービスポリシーからLIFのサービスポリシーに移行する必要はありません。以前のONTAPリリースで使用していたファイアウォールサービスポリシーと整合性のあるLIFのサービスポリシーが自動的に作成されます。カスタム ファイアウォール ポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、代わりにカスタム サービス ポリシーを作成するようにスクリプトのアップグレードが必要になることがあります。

詳細については、「ネットワーク管理ONTAP 9」を参照してください。ONTAP 9.10.1以前では、よく使用される管理サービスにもサービスポリシーを使用できますが、ファイアウォールポリシーは引き続き必要です。次のコマンドを使用して、管理インターフェイスにセキュアなファイアウォールポリシーを定義できます。

```
system services firewall policy create -vserver <SVM name> -policy <policy-name> -service
<protocol_name> -allow-list <ip_address/mask>
```

注： 新しいポリシーへの最初のコマンド参照でポリシーが作成されます。以降の参照では、そのポリシーにエントリが追加されます。

表2）セキュリティで保護された管理ファイアウォールポリシーエントリの設定

プロトコル	-allow-list	正味効果
dns	許可されたDNSサーバのIPアドレスリスト	リストへのDNSアクセスを許可する
http	127.0.0.1/32、::1/128	すべて拒否
https	許可されているHTTPS管理者のIPアドレスリスト	リストへのHTTPSアクセスを許可
ndmp	127.0.0.1/32、::1/128	すべて拒否
ntp	許可されているNTPサーバのIPアドレスリスト	リストへのNTPアクセスを許可
rsh	127.0.0.1/32、::1/128	すべて拒否
snmp	許可されているSNMP管理ステーションのIPアドレスリスト	リストへのSNMPアクセスを許可
ssh	許可されているSSHクライアントのIPアドレスリスト	リストからのSSHアクセスを許可する
telnet	127.0.0.1/32、::1/128	すべて拒否

表2 に、最も一般的なインターフェイスとプロトコルを示します。ONTAPのバージョンによっては、一部のプロトコルがサービスポリシーに置き換えられた場合に使用できないことがあります。詳細については、「ネットワーク管理 ONTAP 9」を参照してください。ファイアウォールポリシー管理の例として、次のコマンドを使用してというポリシーを作成します secure_mgmt。このコマンドは、表1の各エントリに対して適切な変更を加えた状態で繰り返されます。

例：ファイアウォールポリシー「secure_mgmt」を作成する

```
Cluster1::> system services firewall policy create -vserver cDOT-1 -policy secure_mgmt -service
dns -allow-list 10.63.165.0/24, ::1/128
```

完了したら、次のコマンドを使用してポリシーアクションエントリを確認できます。

```
Cluster1::> system services firewall policy show -policy secure_mgmt
```

次の手順では、前のコマンドで作成したファイアウォールポリシーを、クラスタおよびノード管理インターフェイス（e0M）上のインターフェイスに適用します。この手順は、クラスタSVMと各クラスタノードSVMに対して実行します。

クラスタSVM全体に対して、次のコマンドを例として使用します。

```
Cluster1::> network interface modify -vserver cDOT-1 -lif cluster_mgmt -firewall-policy
secure_mgmt
```

ユーザデータストレージSVMの場合は、次のコマンドを例として使用します。

```
Cluster1::> network interface modify -vserver cDOT-1-01 -lif mgmt1 -firewall-policy secure_mgmt
Cluster1::> network interface modify -vserver cDOT-1-02 -lif mgmt1 -firewall-policy secure_mgmt
```

詳細については、「ネットワーク管理 ONTAP 9」を参照してください。前述したサービスポリシーとファイアウォールポリシーに加えて、次の推奨事項によってセキュリティが強化されます。

- クラスタ内のトラフィックに使用されるポートは、クラスタ内の分離されたプライベートネットワーク上に配置する必要があります。クラスタへのアクセスに使用するIPサブネットがパブリックインターネットで認識されないようにする必要があります。セキュアな信頼ネットワークの外部からアクセスできないプライベートIPサブネット（10.10.x.xなど）を使用します。これにより、ネットワーク外での露出を最小限に抑えることができます。また、ONTAPはコントロールプレーンとユーザデータプレーンを分離するため、制御および管理トラフィックとは別のVLANにデータトラフィックを配置することで、セキュリティをさらに強化できます。必要に応じて、この分離をSVM単位で実行することもできます。
- ONTAPは、ネットワークタイムプロトコル（NTP）、DNSなどのネットワークサービスを使用します。NetAppでは、インターネットなどの信頼できないネットワークにシステムを公開するのではなく、これらのサービスを内部ネットワークソースまたは信頼できるネットワーク上のプロキシによって提供することを推奨しています。また、これらのサービスは、データトラフィックとは別に管理IPサブネット（VLAN）でも提供する必要があります。
- サービスプロセッサ（SP）またはベースボード管理コントローラ（BMC）が管理プレーンのVLANに配置されている必要があります。SPを使用すると、ストレージシステムにリモートからアクセスして管理し、エラー状態を診断できます。これは、システムへの追加の侵入ポイントを提供するため、保護する必要がある攻撃対象領域の一部です。前述したサービスポリシーとファイアウォールタイプの機能に加えて、SP内のIPアドレスにはホワイトリスト方式があります。

  また、SPへのアクセスを許可するIPアドレスの範囲を制限することもできます。`system service-processor ssh add-allowed-addresses -allowed-addresses` コマンドは、IPアドレスによるSPへのSSHアクセスを許可します。

  SPとその機能の詳細については、『ONTAP 9のクラスタ管理』の「SPにアクセスできるIPアドレスの管理」を参照してください。

要件2：すべてのシステムコンポーネントにセキュアな構成を適用する

悪意のある個人（エンティティの外部と内部の両方）は、多くの場合、デフォルトのパスワードと他のベンダーのデフォルト設定を使用してシステムを侵害します。これらのパスワードと設定はよく知られており、公開情報を使用することで簡単に取得できます。

システムコンポーネントにセキュアな構成を適用すると、攻撃者がシステムを侵害する手段が減ります。デフォルトのパスワードの変更、不要なソフトウェア、機能、およびアカウントの削除、不要なサービスの無効化または削除はすべて、潜在的な攻撃対象を減らすのに役立ちます。

クラスタ管理者はクラスタ全体を管理し、SVMを作成できます。クラスタ管理者は、作成したSVMにリソース（アグリゲートとボリューム）を割り当てることができます。各SVMで、SVM管理者がそのSVMのデータストレージを管理します。SVMは独立したストレージマシンであるため、各SVMを別々のネットワークおよびセキュリティドメインにセットアップし、SVM管理者が管理できます。SVMへのアクセスは、クラスタ管理者によってSVMに割り当てられたLIFインターフェイスを介して（コントロールプレーンとデータプレーンの両方）行われます。

ONTAPは強化されたアプライアンス（NetApp Cloud Volumes ONTAPやONTAP Selectなどの仮想アプライアンス、またはNetApp AFFやFASなどの物理アプライアンス）であり、デフォルトで不要なサービスが実行されることはありません。ONTAPシステム上のすべてのサービスは、データストレージを目的としています。ONTAPはデフォルトでセキュアなポスチャを使用します。

新しいシステムをインストールした場合、クラスタ管理者の工場出荷時のデフォルトのパスワードはありま

せん。初期セットアップ時に、シリアルポートを使用してこれらのアカウントのパスワードを設定するように求められます。ブルートフォース推測攻撃を避けるために、十分な長さ（10文字以上）と複雑さ（大文字/小文字、特殊文字）のパスワードを使用してください。

クラスタ管理者は、SVMを作成する際にSVM管理者のパスワードを作成できます。SVM管理者にパスワードの即時変更を要求するために、クラスタ管理者は、パスワードの有効期限をSVM管理者ロールに適用できます。

アクティブアカウントのリストを表示するには、次のコマンドを使用します。

```
security login show
```

初期インストールでは、通常、次のアカウントをデフォルトとして使用できます。

- 次のものにアクセスできる1つのクラスタ管理者アカウント

  `console`、`ontapi`（NetApp Manageability SDK）、`http`、 `service-processor`、および `ssh`
- `vserver` 次の項目にアクセスできる管理者アカウントが少なくとも1つ必要です。

  `ontapi`、`ssh`

パスワードをリセットするには、次のコマンドを使用します。

```
cluster1::> security login password -username admin -vserver vs
```

クラスタレベルには、adminとdiagの2つのデフォルトの管理者アカウントがあります。diagアカウントは下位レベルのシステムアクセスを提供するため、通常は必要ありません。デフォルトでは無効になっており、NetAppのサポート担当者から指示があった場合を除き、絶対に使用しないでください。管理者アカウントには、システムの管理に必要なすべてのコマンドにアクセスできるロールが設定されています（ロールベースアクセス制御（RBAC）を使用）。ロックして、該当するコマンドへのアクセスを適切なロールを持つアカウントに制限する必要があります。保護を強化するために重複するアカウントを作成し、管理者アカウントをシステムから削除することもできます。これを行うには `security login role create` 、コマンドを使用してカスタムロールを作成します。

セキュリティをさらに強化するために、ロールに `max-failed-attempts` 属性を設定することで、無効なログインに対して自動ロックアウトを適用できます。

ONTAPシステムでは、SNMPを監視と管理に使用できます。セキュリティを強化するために、ONTAPはSNMPv3をサポートしています。これには、SNMPメッセージの認証と暗号化が含まれます。NetAppでは、`security login create` コマンドを使用して認証とプライバシー（暗号化）のパラメータを指定してSNMPユーザを作成し、認証と暗号化の両方を設定することを推奨しています。SNMPの設定と使用の詳細については、TR-4220：『SNMP Support in Data ONTAP』を参照してください。

以前のPCI DSS 3.2.1標準からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価に対して即座に有効です。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- 主要要件のタイトルが更新され、ベンダーが提供するデフォルト設定だけでなく、一般的なセキュアな構成に重点が置かれていることが反映されました。
- 異なるセキュリティレベルを必要とする主な機能を管理するための要件の意図の明確化。
- 要件の目的は、安全でないサービス、プロトコル、またはデーモンが存在するかどうかであることを明確にします。
- データストレージへの影響：

これらのガイドラインに従ってONTAPを設定できます。

ベストプラクティス：
最小権限の原則を使用して、ONTAPのロールとアカウントを設定します。ONTAPオペレーティングシステムはすでに強化されたアプライアンスであり、デフォルトで不要なサービスが実行されることはありません。

管理者ユーザアカウントを管理するには、2つの手順があります。まず、ユーザの機能を許可するロールが確立されます。次に、ユーザアカウントが作成され、そのロールに割り当てられます。表3に示すように、ONTAPには クラスタ管理者アカウント用の事前定義されたロールが用意されています。

表3）クラスタ管理者のロール

ロール	デフォルトの機能
admin	• すべてのコマンドディレクトリへのすべての（読み取り、書き込み）アクセス
AutoSupport	• すべてのアクセス権を設定 • システムモードAutoSupport • 他のコマンドディレクトリはありません
バックアップ	• SVMサービスNDMPへのすべてのアクセス • ボリュームへの読み取り専用アクセス • 他のコマンドディレクトリにアクセスできない
読み取り専用	• セキュリティログインパスワードへのすべてのアクセス • すべてのアクセス権を設定 • その他のすべてのコマンドディレクトリへの読み取り専用アクセス
なし	• どのコマンドディレクトリにもアクセスできない

表3 に示すように、管理者アカウントはすべて強力です。他のアカウントでは機能が制限されており、 `none` 機能のないアカウントもあります。これらのロールは、コマンドディレクトリを追加または削除してカスタムロールを作成するための出発点となります。より強力なカスタムユーザロールの場合は、adminロールから開始し、不要なコマンドディレクトリを減算できます。逆に、非常に限定されたカスタムロールを作成する場合は、noneロールから開始して必要なコマンドディレクトリを追加する方が簡単です。AutoSupport、Backup、Readonlyの各ロールは、特殊なユースケースに対応しています。

クラスタ管理者のロールと同様に、SVM管理者には表4に示す4つのデフォルトロールがあります。

表4）SVM管理者のロール

ロール	デフォルトの機能
Vsadmin	• 自身の管理者アカウント、ローカルパスワード、および公開鍵の管理 • ボリューム、クォータ、qtree、NetApp Snapshot™コピー、NetApp FlexCache® ファイル、ファイルの管理 • LUNを管理します。 • プロトコルの設定 • サービスの設定 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
Vsadmin-volume	• ボリューム、クォータ、qtree、FlexCacheファイル、およびファイルの管理 • LUNを管理します。 • プロトコルの設定 • サービスの設定 • ネットワーク インターフェイスの監視 • SVMの健全性の監視

ロール	デフォルトの機能
Vsadmin-protocol	• プロトコルの設定 • サービスの設定 • LUNを管理します。 • ネットワーク インターフェイスの監視 • SVMの健全性の監視
Vsadmin -読み取り専用	• SVMの健全性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

SVM管理者用のデフォルトのロールリストでは、業務が分離されています。たとえば、データプロトコルサービスの管理と設定は、ストレージ自体の管理から分離されます。このアプローチは、一般的なセキュリティベストプラクティスの最小権限の原則に準拠しています。

これらのロールは、PCI DSS 4.0で新しいロールを変更または作成するのに十分です。『ONTAP 9セキュリティおよびデータ暗号化ガイド』を参照してください。適切なロールを設定したら、ユーザアカウントを作成してロールを割り当てることができます。`security login create` アカウントを作成してロールを割り当てるには、を使用します。たとえば、次のコマンドでは、ユーザ名 `monitor`、アプリケーション、`ssh`認証方式、 `password`アクセス制御ロールの `guest` SVMへのログインを作成します `vs`。

```
cluster1::> security login create -username monitor -application ssh -authmethod password -role
guest -vserver vs
```

クラスタ管理者とSVM管理者のデフォルトアカウントには、ほとんどのお客様がデフォルトで使用する一般的なロールが割り当てられます。ただし、オプションとして、これらのアカウントをロックし、最小権限のセキュリティ哲学に従って、より制限されたロールを持つ新しいアカウントを作成することもできます。

クラスタ管理者とONTAPシステム上の他のすべてのユーザアカウントのセキュリティをさらに強化するために使用できるもう1つのオプションは、ONTAP 9.11.1以降に組み込まれているマルチ管理者検証（MAV）と呼ばれるセキュリティ機能を使用することです。MAVを使用すると、ボリュームやSnapshotコピーの削除などの特定の処理が、指定した管理者の承認後にのみ実行されるようにすることができます。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が望ましくない変更やデータの削除を行えないようにすることができます。MAVの詳細については、『ONTAP 9セキュリティおよびデータ暗号化ガイド』を参照してください。

また、ONTAPシステムは、ユーザやアプリケーションにシステムへのWebサービスアクセスを提供します。NetAppでは、HTTPSのみを使用するように設定し、HTTPを無効にすることを推奨しています。ONTAP 9.11.1以降では、TLS 1.3と1.2が有効になり、TLS 1.1、1.0、およびSSLv3はデフォルトで無効になります。NetAppではTLS 1.3を推奨していますが、下位互換性を確保するためにTLS 1.2、1.1、1.0、およびSSLv3が提供されています。

アカウントデータの保護

要件3：保存されているアカウントデータを保護する

暗号化、切り捨て、マスキング、ハッシュなどの保護方法は、アカウントデータ保護の重要なコンポーネントです。侵入者が他のセキュリティ制御を迂回し、暗号化されたアカウントデータにアクセスすると、適切な暗号キーがなければデータを読み取ることができず、その侵入者はデータを使用できません。保存されたデータを保護するその他の効果的な方法も、潜在的なリスク軽減の機会と考える必要があります。たとえば、リスクを最小限に抑える方法には、必要でない限りアカウントデータを保存しない、完全なプライマリアカウント番号(PAN)が不要な場合にカード所有者データを切り捨て、電子メールやインスタントメッセージなどのエンドユーザーメッセージングテクノロジーを使用して保護されていないパンを送信しないなどがあります。

アカウントデータが非永続的メモリ（RAM、揮発性メモリなど）にある場合、アカウントデータの暗号化は

必要ありません。ただし、メモリが非永続的な状態を維持するように、適切な制御を行う必要があります。ビジネス目的（関連するトランザクションなど）が完了したら、揮発性メモリからデータを削除する必要があります。データストレージが永続的になると、保存データの暗号化など、該当するすべてのPCI DSS要件が適用されます。

要件3個々の要件に特に明記されていない限り、保存されたアカウントデータの環境保護。

以前のPCI DSS 3.2.1標準からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価に対してただちに有効です。
- データ保持および廃棄ポリシー、手順、およびプロセスの実装を通じて、承認が完了する前に保存されたアカウントデータに対処するための新しい要件項目。この箇条書きは、2025年3月31日（3.2.1）までのベストプラクティスです。
- 承認が完了する前に電子的に保存される、保存されたアカウントデータを暗号化するための新しい要件。この要件は、2025年3月31日（3.3.2）までのベストプラクティスです。
- パンが表示されているときにパンがマスクされていることを明確にします。これにより、業務上必要な人だけがパンのビン/最後の4桁（3.4.1）よりも多くを見ることができます。
- リモートアクセステクノロジを使用する場合、PANのコピーと再配置を防止するための技術的制御の新しい要件。以前の要件12.3.10から拡張されました。この要件は、2025年3月31日（3.4.2）までのベストプラクティスです。
- パンを読めないようにレンダリングするための「インデックストークンとパッド」の箇条書きからパッドを削除します（3.5.1）。
- PANを読み取り不能にするためにハッシュを使用する場合のキー付き暗号化ハッシュの新しい要件。この要件は、2025年3月31日（3.5.1.1）までのベストプラクティスです。
- ディスクレベルまたはパーティションレベルの暗号化は、リムーバブル電子メディアでPANを読み取り不能にするためにのみ使用される、またはリムーバブルでない電子メディアで使用される場合、PANは要件3.5.1を満たすメカニズムによって読み取り不能になるという新しい要件。この要件は、2025年3月31日（3.5.1.2）までのベストプラクティスです。
- サービスプロバイダーは、本番環境およびテスト環境で同じ暗号キーを使用できないようにするために、暗号アーキテクチャの文書化された概要にのみ含める必要があります。この箇条書きは、2025年3月31日（3.6.1.1）までのベストプラクティスです。
- 以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化
- 発行者による保存されたアカウントデータの保存は、正当な発行のビジネスニーズに必要なものに制限され、保護されているという以前のテスト手順に対処するための要件の追加(3.3.3)。

データストレージへの影響

PCI DSS 4.0では、パーティションレベルの暗号化またはディスクレベルの暗号化のいずれかの方法で暗号化を実行でき、適切なキー管理が必要であると規定されています。PCI DSS 4.0の要件を満たすディスク暗号化を使用できます。

NetAppストレージ暗号化（NSE）は、業界をリードするベンダーが提供するFIPS-140-2レベル2の認定済み自己暗号化ドライブ（SED）を使用して、NetAppにFull Disk Encryption（FDE）を実装したものです。NetApp Volume Encryption（NVE）は、ボリュームレベルで暗号化するため、SSD、NetApp AFF、さらにはNSEドライブなどの物理メディアとは関係なく暗号化機能を利用できます。NetAppアグリゲート暗号化（NAE）はアグリゲートレベルで暗号化を行うため、アグリゲート内のすべてのボリュームで暗号化を共有し、重複排除や圧縮などのONTAP Storage Efficiencyを最大限に活用できます。

NSEは、使いやすい包括的で対費用効果の高いハードウェアベースのセキュリティを提供する暗号化実装です。この単一ソース ソリューションを使用すると、ストレージ効率を損なうことなく、業界や政府の規制に対する全体的なコンプライアンスを強化できます。

NSEには次の機能があります。

- 重複排除、圧縮、アレイベースのウィルス対策スキャンなど、NetAppが提供する一連のStorage Efficiencyテクノロジをすべてサポートします。
- タレス、Entrust、IBMなどのNetAppパートナーが提供するサードパーティの外部キー管理サーバをサポートします。すべてのリストについては、NetApp Interoperability Matrix Toolを参照してください。
- お客様がFISMA、HIPAA、PCI、Basel II、SB 1386、 および、FIPS 140-2認定ハードウェアを使用したEUデータ保護指令95/46/ECおよびEU一般データ保護規則。
- OASIS KMIP標準に準拠しており、他のキー管理ツールや暗号化デバイスとの互換性を提供しています。
- ハイパースケーラのキー管理ソリューション（KMS）をサポート

NVEとNAEは、ONTAP管理ソフトウェアで使用できる、ソフトウェアベースの保存データ暗号化ソリューションです。NAEとNVEはどちらもFIPS 140-2に準拠しています。ONTAPでNVEを使用すると、（AES 256ビット暗号化を使用して）ボリューム単位でデータを暗号化できます。NAEは、アグリゲート内のすべてのボリュームでAES-256ビット暗号化キーを共有します。NAEアグリゲートとNVEボリューム暗号化キーは、外部キー管理ツールに格納できます。外部キー管理ツールにアクセスせずにコントローラとディスクを移動した場合、NAEアグリゲートとNVEボリュームにアクセスできず、復号化できません。

NVEには次の機能があります。

- 重複排除、圧縮、アレイベースのウィルス対策スキャンなど、NetAppが提供する一連のStorage Efficiencyテクノロジをすべてサポートします（NVEアグリゲートのインライン重複排除ボリュームはこの効率化から除外されます）。
- タレス、Entrust、IBMなどのNetAppパートナーが提供するサードパーティの外部キー管理サーバをサポートします。すべてのリストについては、NetApp Interoperability Matrix Toolを参照してください。
- お客様がFISMA、HIPAA、PCI、Basel II、SB 1386、および、FIPS 140-2認定暗号モジュールソフトウェアを使用したEUデータ保護指令95/46/ECおよびEU一般データ保護規則。OASIS KMIP標準に準拠しており、他のキー管理ツールや暗号化デバイスとの互換性を提供しています。
- ハイパースケーラのキー管理ソリューション（KMS）をサ

ポートNAEには次の機能があります。

- アグリゲートインライン重複排除、重複排除、圧縮、アレイベースのウィルス対策スキャンなど、NetAppが提供する一連のStorage Efficiencyテクノロジをすべてサポートします。
- タレス、Entrust、IBMなどのNetAppパートナーが提供するサードパーティ製の外部キー管理サーバをサポートします。すべてのリストについては、NetApp Interoperability Matrix Toolを参照してください。
- お客様がFISMA、HIPAA、PCI、Basel II、SB 1386、および、FIPS 140-2認定暗号モジュールソフトウェアを使用したEUデータ保護指令95/46/ECおよびEU一般データ保護規則。
- OASIS KMIP標準に準拠しており、他のキー管理ツールや暗号化デバイスとの互換性を提供しています。
- ハイパースケーラのキー管理ソリューション（KMS）をサポート

ベスト プラクティス

支払いデータを保存するには、NetAppストレージ暗号化、NetAppアグリゲート暗号化、NetAppボリューム暗号化、またはその両方を使用します。

要件4：オープンなパブリックネットワークを介した転送中に強力な暗号化を使用してカード会員データを保護する

強力な暗号化を使用することで、データの機密性、整合性、否認防止をより確実に保護できます。

セキュリティ侵害から保護するには、信頼されていないネットワークやパブリックネットワークなど、悪意のあるユーザが簡単にアクセスできるネットワークを介した送信中にPANを暗号化する必要があります。ワイヤレスネットワークの設定ミスや、従来の暗号化および認証プロトコルの脆弱性は、これらの脆弱性を悪用してCDEへの特権アクセスを取得することを目的とした悪意のある個人によって引き続き標的にされています。カード所有者データを企業の内部ネットワークまたはネットワーク経由で送信すると、そのネットワークはカード所有者データを保存、処理、または送信するため、PCI DSSの対象となります。そのようなネットワークは、該当するPCI DSS要件に照らして評価および評価する必要があります。

要件4個 々 の要件で特に言及されていない限り、PANの環境送信。

PAN送信を保護するには、データが送信される前にデータを暗号化するか、データが送信されるセッションを暗号化するか、またはその両方を実行します。データレベルとセッションレベルの両方で強力な暗号化を適用する必要はありませんが、推奨されます。

以前のPCI DSS 3.2.1標準からの要件の進化

- 役割と責任に関する新たな要件この要件は、すべてのv4.0評価（4.1.2）でただちに有効になります。
- オープンなパブリックネットワークを介したPAN送信に使用される証明書を確認するための新しい要件は有効であり、期限切れまたは取り消されていません。この要件は、2025年3月31日（4.2.1）までのベストプラクティスです。
- 信頼されたキーと証明書のインベントリを維持するための新しい要件。この要件は、2025年3月31日までのベストプラクティスです。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- カード所有者データの送信を保護するための強力な暗号化に焦点を当てた主な要件タイトルの更新。

データストレージへの影響

データ暗号化の要件はさまざまであるため、NetAppでは、カード所有者データと管理データの両方をパブリックネットワーク経由で送信する場合に、外部VPN暗号化を使用することを推奨しています。

ベスト プラクティス

カード所有者データを送信するには、外部VPNデータ暗号化を使用します。NASプロトコルの場合は、NFSおよびSMB暗号化にKerberos 5認証とプライバシサービス（krb5p）を使用します。Internet Protocol security（IPsec;インターネットプロトコルセキュリティ）は、すべてのIPデータトラフィックで使用できます。krg5p、SMB暗号化、およびIPSecの詳細については、『Security Hardening Guide for NetApp ONTAP 9』を参照してください。

脆弱性管理プログラムの保守

要件5：悪意のあるソフトウェアからすべてのシステムとネットワークを保護する

悪意のあるソフトウェア（マルウェア）とは、所有者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、または可用性を侵害する目的で、所有者の知識または同意なしにコンピュータシステムに侵入または損傷を与えるように設計されたソフトウェアまたはファームウェアです。

たとえば、ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェア、 キーロガー、ルートキット、悪意のあるコード、スクリプト、およびリンク。

マルウェアは、従業員の電子メール(フィッシングなど)やインターネット、モバイルコンピュータ、ストレージデバイスの使用など、ビジネスで承認された多くの活動中にネットワークに侵入する可能性があり、その結果、システムの脆弱性が悪用されます。

あらゆる種類のマルウェアに対応するマルウェア対策ソリューションを使用すると、現在および進化しているマルウェアの脅威からシステムを保護できます。

以前のPCI DSS 3.2.1標準からの要件の進化

- 「アンチウイルス」という用語を「アンチマルウェア」に置き換えて、従来のアンチウイルスソフトウェアで満たされていたセキュリティ目標を満たすために使用される幅広いテクノロジーをサポートします。
- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（5.1.2）でただちに有効になります。
- 企業のターゲットリスク分析において、マルウェアのリスクにさらされていないシステムコンポーネントを定期的に評価する頻度を定義する新しい要件。この要件は、2025年3月31日（5.2.3.1）までのベストプラクティスです。
- 企業のターゲットリスク分析における定期的なマルウェアスキャンの頻度を定義するための新しい要件。この要件は、2025年3月31日（5.3.2.1）までのベストプラクティスです。
- リムーバブル電子メディア用マルウェア解決策の新しい要件。この要件は、2025年3月31日（5.3.3）までのベストプラクティスです。
- フィッシング攻撃から人員を検出して保護するための新しい要件。この要件は、2025年3月31日（5.4.1）までのベストプラクティスです。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- 悪意のあるソフトウェアからすべてのシステムとネットワークを保護することに重点を置いて、主要要件のタイトルを更新します。
- 対象を「マルウェアの危険性のないシステムコンポーネント」に変更することによる要件の明確化(5.2.3)。
- 1つの要件を3つに分割して、各要件を1つの領域に絞り込みます。
  - 自動更新(5.3.1)を使用して、マルウェアの解決策を最新の状態に保ちます。
  - 定期的なスキャンとアクティブまたはリアルタイムのスキャン（連続的な行動分析のための新しいオプションを使用）を実行します（5.3.2）。
  - マルウェア解決策（5.3.4）を使用して監査ログを生成します。

データストレージへの影響

NetAppでは、カード決済サービスを提供するコンピュータ上でマルウェア対策ソフトウェアを実行することを推奨しています。

ONTAPシステムでは、セキュリティ保護を強化するために、NAS（NFSおよびSMB）に接続された共有上のマルウェア（ランサムウェアなど）からの保護もサポートできます。たとえば、NetApp FPolicy™ とNetApp Cloud Insights、または当社のパートナーが提供する同様の機能を組み合わせることで、ユーザー行動分析（UBA）を通じてマルウェアを検出することができます。個々のユーザーの行動の側面から潜在的なマルウェア攻撃を探します。1つのユーザーアカウントをハイジャックすることは、ハッカーがマルウェア攻撃を開始する際に取る可能性のある1つの手段にすぎません。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。

NetApp Active IQ® とNetApp Active IQ Unified Managerには、ランサムウェアの検出機能も追加されています。Active IQは、ONTAPシステムがNetApp設定のベストプラクティス（FPolicyの有効化など）に準拠しているかどうかをチェックします。Active IQ Unified Managerは、Snapshotコピーの異常な増加やStorage Efficiencyの損失に関する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ている可能性があります。ONTAP 9.10.1以降では、組み込みの機械学習（ML）機能を活用して、ボリュームワークロードのアクティビティとデータエントロピーを使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し、UBAでは検出できない攻撃を検出できるようにします。

ベスト プラクティス

マルウェアに対する階層型防御アプローチを導入し、FPolicy、Cloud Insights、オンボックスランサムウェア対策などのNetAppテクノロジを使用して支払いカードサービスを保護します。詳細については、TR-4572『The NetApp 解決策for ransomware』を参照してください。

要件6：セキュアなシステムとソフトウェアの開発と保守

悪意のある攻撃者は、セキュリティの脆弱性を利用して、システムへの特権アクセスを取得する可能性があります。これらの脆弱性の多くは、ベンダーが提供するセキュリティパッチによって修正されています。このパッチは、システムを管理するエンティティによってインストールする必要があります。すべてのシステムコンポーネントには、悪意のある個人や悪意のあるソフトウェアによるアカウントデータの悪用や侵害から保護するために、適切なソフトウェアパッチがすべて適用されている必要があります。

適切なソフトウェアパッチは、既存のセキュリティ設定と競合しないことを確認するために評価およびテストされたパッチです。カスタムソフトウェアの場合、ソフトウェアライフサイクル(SLC)プロセスと安全なコーディング手法を適用することで、多数の脆弱性を回避できます。

アプリケーションコード、システム構成、またはアカウントデータまたはCDEのセキュリティに影響を与える可能性のあるその他の構成データを格納するコードリポジトリは、PCI DSS評価の対象となります。

PCI SSC検証済みのソフトウェアおよびソフトウェアベンダーの使用、およびPCI SSCのソフトウェア標準の使用が要件6の制御を満たす上でどのように役立つかについては、「PCI DSSとPCI SSCソフトウェア標準の関係」の7ページを参照してください。

注: 要件6環境ソフトウェアを安全に開発するためのセクション6.2を除くすべてのシステムコンポーネント。これは、CDEに含まれる、またはCDEに接続されているシステムコンポーネントで使用されるカスタムソフトウェアにのみ適用されます。

以前のPCI DSS 3.2.1標準からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（6.1.2）でただちに有効になります。
- カスタムソフトウェアとカスタムソフトウェアの在庫を維持するための新しい要件。この要件は、2025年3月31日（6.3.2）までのベストプラクティスです。
- Webベースの攻撃を継続的に検出して防止する、公開されているWebアプリケーション用に自動化されたテクニカル解決策を導入するという新たな要件が追加されました。この新しい要件により、要件6.4.1では、手動または自動のアプリケーション脆弱性評価ツールまたは方法を使用してWebアプリケーションをレビューするオプションが削除されます。この要件は、2025年3月31日（6.4.2）までのベストプラクティスです。
- 消費者のブラウザにロードされて実行されるすべての支払いページスクリプトの管理に関する新しい要件。この要件は、2025年3月31日（6.4.3）までのベストプラクティスです。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- 主要要件タイトルの更新に「アプリケーション」ではなく「ソフトウェア」が含まれるようになりました。要件6環境要件6.2を除くすべてのシステムコンポーネントが、特注およびカスタムソフトウェアにのみ適用されることを明確にします。
- 「内部および外部」という用語が「カスタムメイドのカスタムソフトウェア」に置き換えられました。この要件環境ソフトウェアは、企業自身の使用のために、または企業によって開発されたものであり、サードパーティのソフトウェアには適用されないことを明確にします(6.2.1)。
- 要件6.2の下ですべてのソフトウェア開発コンテンツを調整するために、ソフトウェア開発者をトレーニングするための要件6.5の要素の移動。ソフトウェア開発担当者のトレーニング要件の明確化(6.2.2)。
- 要件6.2の下ですべてのソフトウェア開発コンテンツを調整するために、リリース前にカスタムソフトウェアをレビューするための要件の移動。一般的なコードレビュープラクティスを、手動でのコードレビューが実行された場合に必要なものと分離するための要件の分割(6.2.3、6.2.3.1)。

- 要件6.2の下ですべてのソフトウェア開発コンテンツを調整するために、一般的なコーディングの脆弱性に対処するための要件の移動。一般的なソフトウェア攻撃を防止または軽減する方法を1つの要件にまとめ、各攻撃タイプを記述する言語を一般化します(6.2.4)。
- 特注ソフトウェアおよびカスタムソフトウェアおよびサードパーティソフトウェアの脆弱性への適用性を明確にするための箇条書きが追加されました（6.3.1）。
- 特定の文書化された手順の要件を削除し、関連する各要件に対するポリシーと手順を検証するためのテスト手順を追加しました。
- 「開発/テストおよび本番環境」という用語を、「本番環境および前本番環境」という用語に置き換えます（6.5.3）。
- 「開発/テストおよび本番環境」という用語を、「本番環境および前本番環境」という用語に置き換えます。「職務の分離」という用語を置き換え、承認された変更のみが展開されるように、本番環境とテスト運用環境の役割と機能を分離することが説明責任を果たすことを目的としていることを明確にしました（6.5.4）。
- 「テストまたは開発」という用語は、「テスト環境」から「テスト運用環境」に置き換えられます。
- 該当するすべてのPCI DSS要件が適用されている場合を除き、ライブパンはテスト運用環境では使用されません（6.5.5）。

データストレージへの影響

NetAppは、自社の製品開発ライフサイクル全体にわたってセキュアな開発原則に従っています。NetAppは、安全な開発プログラムを継続的に拡張し、改善しています。NetAppの標準手順の一部として、安全な設計原則、開発者トレーニング、および広範なテストプログラムを実装しています。

NetAppは、脆弱性への対応とお客様への通知の際に複数の手順を踏んでいます。

- **脆弱性に関する報告の受領：**NetAppでは、PGPで暗号化された電子メールを使用して機密情報をVulnerability Response Team（PSIRT）に送信することをお客様や研究者に推奨しています。NetAppは、弊社製品の脆弱性の疑いを調査し、7営業日以内に脆弱性レポートの受領を確認します。
- **検証：**ファインダーが潜在的な脆弱性に関するNetAppとの連絡を開始した後、NetApp PSIRTエンジニアは脆弱性を検証し、Common Vulnerability Scoring System (CVSS)フレームワーク内で評価を行います。
- **解決策の構築：**NetAppは、厳格な品質管理基準で認められているように、重要な修正と緩和策を顧客ベースに迅速に提供するよう努めています。テストと検証は、多くの場合、時間のかかるプロセスです。
- **通知：**NetAppは、お客様が環境における脆弱性の影響を評価するために必要な最小限の情報と、脅威を軽減するために必要な手順を開示します。悪意のある人物によるエクスプロイトの開発を防止するために、詳細情報は提供しません。
- **功績の評価：**NetAppは、外部の脆弱性発見者が特定されることに明示的に同意し、NetAppが脆弱性を公開する前に修正して顧客ベースに通知する機会を提供した場合、アドバイザリで外部の脆弱性発見者を信用しています。

公開されている各脆弱性の概要を標準化するために、NetAppセキュリティアドバイザリはCommon Vulnerabilities and Exposures（CVE）IDを参照しています。NetAppはバージョン3.0のCVSSを使用して、脆弱性の優先順位と通知戦略を決定します。

NetAppセキュリティアドバイザリおよび通知には、NetAppが決定した基本脆弱性スコアが含まれています。脆弱性の分類と管理にCVSSを使用しているお客様には、独自の時間スコアと環境スコアを計算して、CVSSメトリックを最大限に活用することをお勧めします。

NetAppセキュリティ情報の標準的な配信方法は次のとおりです。

- **セキュリティアドバイザリ。**NetApp製品に直接影響し、アップグレード、パッチ適用、またはお客様への直接の対処が必要な、重大なセキュリティ脆弱性。

  NetApp Active IQは、セキュリティアドバイザリに記載されている潜在的なセキュリティリスクに関する情報を提供します。これらのリスクは、NetApp PSIRTが投稿するCVE IDに対応しています。Active IQランディングページおよびDigital Advisorのセキュリティカードの「セキュリティの脆弱性」の「健全性の概要」セクションを参照してください。詳細については、Active IQを参照してください。
- **セキュリティ情報。**NetApp製品に影響する、重大度の低い、または中程度のセキュリティ問題。
- **セキュリティ通知：**NetApp製品の脆弱性について第三者が未確認の公開声明を出した場合、またはNetApp製品がセキュリティインシデントに非公式に関与しているとみなされた場合に使用できます。
- **セキュリティバグレポート。**重大度が低いセキュリティの脆弱性に関する情報は、Bugs Onlineで確認できます（ログインが必要です）。

詳細については、「NetApp製品セキュリティ」を参照してください。

ベスト プラクティス

NetApp通知にサブスクライブするか、NetApp Active IQを使用して、セキュリティパッチと更新プログラムが利用可能になったら実装します。登録するには、NetAppセキュリティアドバイザリにアクセスしてください。Active IQの詳細については、Active IQのランディングページを参照してください。

強力なアクセス制御手段の実装

要件7：ビジネスニーズに応じてシステムコンポーネントとカード所有者データへのアクセスを制限する

アクセス制御のルールや定義が無効なため、権限のない個人が重要なデータやシステムにアクセスできる可能性があります。権限のある担当者のみが重要なデータにアクセスできるようにするには、必要に応じて職務に応じてアクセスを制限するシステムとプロセスを導入する必要があります。

アクセス権またはアクセス権は、システム、アプリケーション、およびデータへのアクセスをユーザーに提供するルールによって作成されます。一方、権限を使用すると、ユーザーはそのシステム、アプリケーション、またはデータに関連して特定のアクションまたは機能を実行できます。たとえば、あるユーザが特定のデータへのアクセス権を持っていても、そのデータの読み取りのみが可能か、データの変更や削除も可能かどうかは、そのユーザに割り当てられている権限によって決まります。

「知る必要がある」とは、ジョブの実行に必要な最小限のデータのみにアクセスできるようにすることを意味します。「最小権限」とは、ジョブの実行に必要な最小限の権限のみを提供することを意味します。

これらの要件は、従業員、請負業者、コンサルタント、社内外のベンダー、およびその他のサードパーティ(サポートやメンテナンスサービスの提供など)のユーザーアカウントとアクセスに適用されます。エンティティによって使用されるアプリケーションアカウントとシステムアカウント（サービスアカウントとも呼ばれる）には、一定の要件が適用されます。

注意： これらの要件は、消費者(カード所有者)には適用されません。

以前のPCI DSS 3.2.1標準からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（7.1.2）でただちに有効になります。
- すべてのユーザアカウントと関連するアクセス権限を確認するための新しい要件。この要件は、2025年3月31日（7.2.4）までのベストプラクティスです。
- すべてのアプリケーションアカウントとシステムアカウント、および関連するアクセス権限の割り当てと管理に関する新しい要件。この要件は、2025年3月31日（7.2.5）までのベストプラクティスです。

- アプリケーションおよびシステムアカウントごとのすべてのアクセス権および関連するアクセス権を確認するための新しい要件。この要件は、2025年3月31日（7.2.5.1）までのベストプラクティスです。

以前のPCI DSS 3.2.1標準からの追加のガイダンスと明確化

- システムコンポーネントとカード所有者データを含めるための主要要件タイトルの更新。
- 特定の文書化された手順の要件を削除し、関連する各要件に対するポリシーと手順を検証するためのテスト手順を追加しました（7.2.1、7.2.2、7.2.3）。
- 要件がアクセス制御モデルの定義に関するものであることを明確にしました（7.2.1）。
- 要件は、権限を持つ担当者による必要な権限の承認に関するものであることを明確にします（7.2.3）。

データストレージへの影響

デフォルトのクラスタ管理者ロールは、「admin」ロールの機能へのフルアクセスを提供します。また、一部の管理者の権限を読み取り専用ユーザまたはAutoSupportユーザに制限するために、クラスタコンテキスト用にいくつかの事前定義された管理ロールが用意されています。これらのデフォルトのクラスタ管理者ロールには、概要レベルの管理者ロールに加え、読み取り専用アクセスに対してより制限されたロールが含まれています。

通常は、クラスタ管理者とSVM管理者用に事前定義されたロールで十分なセキュリティを確保できます。データプレーンと管理プレーンが分離されているため、通常、管理者はユーザデータに直接アクセスできません。（主な例外は、管理者がユーザデータにアクセスするために追加のユーザアカウントを作成した場合に発生します）。 お客様のデータアクセスは、ローカルまたはLDAPまたはActive Directoryを介した許可されたアカウントに制限されます。それがユーザにID管理を提供しますこれにより、データユーザを特定のボリュームに制限できます。

SMBオヨヒNFSヲシヨウシタNASアクセスニカンスルエイキョウ

NFSおよびSMBのファイルアクセスを制御するには、NTFS Access Control List（ACL；アクセス制御リスト）やUNIXモードビットなど、標準のNASプロトコル権限が使用されます。NASアクセスには、アクセスに関する主な考慮事項が4つあります。

- **エクスポートポリシールール**ユーザ認証を実行する前に、NASアクセス用のエクスポートポリシールールを評価する必要があります。SMB共有ではエクスポートポリシールールを利用できますが、ONTAP 9ではこれらのルールがデフォルトで無効になっています。NFSエクスポートでは、エクスポートポリシールールと共有レベルのアクセスに基づいて、ホスト名/クライアントIP、許可されたセキュリティタイプ（SYSやKRBなど）、アクセスを試みるユーザのタイプなどの一連の要素が常に適用されます。
- **認証：**ユーザーは、自分が自分であることを証明する必要があります。この認証は、ファイルシステムのセキュリティ形式に基づくネームマッピングによって行われます。アクセスを要求しているユーザが有効なユーザにマッピングされていない場合、アクセスは拒否されます。Kerberosなどの他の認証機能も、システム構成に応じて有効になる場合があります。
- **共有権限。**SMB共有では、ACLベースの共有権限を使用して、認証されたユーザが共有にアクセスできるかどうかを制御します。認証するユーザがACLに登録されていない場合、共有へのアクセスは拒否されます。共有レベルの権限はファイルレベルの権限とは異なり、Microsoftのドキュメントで説明されています。
- **許可：**ユーザが認証されて共有へのアクセスが許可されたら、そのユーザがファイルレベルまたはフォルダレベルで実行できる処理を、データオブジェクトのACLで確認する必要があります。ACL権限は、ユーザが認証されたユーザおよびファイルシステムのセキュリティ形式に基づいて決まります。

NASファイルシステムのローカルアカウント（SMBワークグループ）

ONTAP 9以降では、ローカルで定義されたユーザとグループを使用してサーバに認証するSMBクライアントを含むワークグループにSMBサーバを設定できます。ワークグループクライアント認証は、従来のドメイン認証と整合性のある追加のセキュリティレイヤを提供します。

注： ワークグループモードのSMBサーバでは、Windows NT LAN Manager（NTLM）認証のみがサポートされ、Kerberos認証はサポートされません。

NetAppでは、組織のセキュリティ体制を維持するために、SMBワークグループでNTLM認証機能を使用することを推奨しています。NetAppでは `vserver cifs session show`、SMBセキュリティポスチャを検証するために、コマンドを使用して、IP情報、認証メカニズム、プロトコルバージョン、認証タイプなどのポスチャ関連の詳細を表示することを推奨しています。

Active Directory、LDAP、NISなどの外部ネームサービスサーバを使用して、ユーザとグループを照会して認証と許可を行うことができます。NASアクセスの詳細については、次のテクニカルレポートを参照してください。

- TR-4067：『NFS in NetApp ONTAP−Best Practice and Implementation Guide』
  https://www.netapp.com/us/media/tr-4067.pdf
- TR-4073：『Secure Unified Authentication』
  https://www.netapp.com/us/media/tr-4073.pdf
- TR-4543：『SMB Protocol Best Practices』
  https://www.netapp.com/us/media/tr-4543.pdf
- 『Best Practices Guide for Clustered Data Windows File Services』
  https://www.netapp.com/us/media/tr-4191.pdf
- NetApp ONTAP 9セキュリティ強化ガイド
  https://www.netapp.com/us/media/tr-4569.pdf

ベストプラクティス

デフォルトの管理ロールを使用して、各管理者アカウントの許可を管理します。

アクセス権を持つ各ユーザに一意のIDとパスワードを割り当てます（ロギング目的）。割り当てられたタスクに対して最低限の権限を持つ各ユーザアカウントにロールを割り当てます（最小権限の原則）。

LDAP、Active Directory、またはNetwork Information Service（NIS）を使用して、データユーザに特定のボリュームへの認証アクセスを提供します。

要件8：ユーザの識別とシステムコンポーネントへのアクセスの認証

ユーザの識別と認証には、次の2つの基本原則があります。

- コンピュータシステム上の個人またはプロセスのIDを確立します。
- IDに関連付けられているユーザが、そのユーザがそのユーザであると主張しているユーザであることを証明または検証します。

コンピュータシステム上の個人またはプロセスの識別は、ユーザー、システム、またはアプリケーションIDなどの識別子を介して個人またはプロセスにIDを関連付けることによって行われます。これらのID (アカウントとも呼ばれます)は、個人またはプロセスごとに一意のIDを割り当てることで、基本的に個人またはプロセスのIDを確立します。各ユーザーまたはプロセスが一意に識別されると、そのIDによって実行されるアクションに対するアカウンタビリティが確保されます。アカウンタビリティが設定されている場合、実行されるアクションは、既知の許可されたユーザーとプロセスに追跡できます。

IDの証明または検証に使用される要素は、認証要素と呼ばれます。認証要素は次のとおりです。

- パスワードやパスフレーズなど、知っている情報。
- トークンデバイスやスマートカードなど、お持ちのもの。
- バイオメトリック要素など、あなたがいるもの。

IDと認証要素の組み合わせは認証クレデンシャルと見なされ、ユーザ、アプリケーション、システム、またはサービスアカウントに関連付けられた権限と権限にアクセスするために使用されます。

IDと認証に関するこれらの要件は、支払いエコシステムをサポートするための業界で受け入れられているセキュリティ原則とベストプラクティスに基づいています。NIST Special Publication 800-63, Digital Identity Guidelinesは、デジタルアイデンティティと認証要素のための許容可能なフレームワークについて追加情報を提供している。NISTデジタルアイデンティティガイドラインは、米国連邦政府機関を対象としており、その全体を見る必要があることに注意することが重要です。これらのガイドラインで定義されている概念とアプローチの多くは、スタンドアロンパラメータとしてではなく、相互に連携することが期待されています。

注： 要件に特に記載がないかぎり、これらの要件は、以下を含むがこれらに限定されない、すべてのシステムコンポーネントのすべてのアカウントに適用されます。

- 販売時アカウント
- 管理機能を持つアカウント
- システムアカウントとアプリケーションアカウント
- カード所有者データを表示またはアクセスするため、またはカード所有者データを使用してシステムにアクセスするために使用されるすべてのアカウント。

注: これには、従業員、請負業者、コンサルタント、社内外のベンダー、およびその他のサードパーティ(サポートやメンテナンスサービスの提供など)が使用するアカウントが含まれます。

特定の要件は、一度に1つのカード番号にしかアクセスできないユーザーアカウント（POS端末でレジ係が使用するIDなど）には適用されません。アイテムが適用されない場合は、特定の要件内に直接記載されます。

注意：これらの要件は、消費者(カード所有者)が使用するアカウントには適用されません。

以前のPCI DSS 3.2.1からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（8.1.2）でただちに有効になります。
- 共有認証クレデンシャルの使用を許可するという要件の焦点が変更されましたが、例外的な場合に限ります（8.2.2）。
- ユーザIDをロックアウトするまでの無効な認証の試行回数が6回から10回（8.3.4）に増加しました。
- パスワードの長さを7文字以上から12文字に増やす必要が新たに追加されました（システムで12文字がサポートされていない場合は8文字以上）。この要件は、2025年3月31日までのベストプラクティスです。2025年3月31日までは、v3.2.1要件8.2.3に従い、パスワードは7文字以上にする必要があることを明確にしました。この要件は、要件8.3.1を満たすための認証要素としてパスワードまたはパスフレーズが使用されている場合にのみ適用されます。この要件は、単一のトランザクションを容易にするために一度に1つのカード番号にしかアクセスできないPOS端末のユーザーアカウントに適用されることを意図したものではありません(8.3.6)。
- パスワードやパスフレーズを90日に1回以上変更するのではなく、アカウントのセキュリティ体制を動的に分析してリソースへのアクセスを自動的に決定するオプションが追加されました（8.3.9）。
- サービスプロバイダーのみの新しい要件–パスワードまたはパスフレーズが顧客ユーザーアクセスの唯一の認証要素である場合、パスワードまたはパスフレーズは少なくとも90日に1回変更されるか、アカウントのセキュリティ体制を動的に分析してリソースへのアクセスが自動的に決定されます。この要件は、2025年3月31日までのベストプラクティスです。この要件は、支払いカード情報にアクセスする消費者ユーザーのアカウントには適用されません。この要件は、要件8.3.10が有効になった時点で要件8.3.10よりも優先され、その日までにサービスプロバイダーは要件8.3.10または8.3.10.1（8.3.10.1）のいずれかを満たすことができます。
- CDEへのすべてのアクセスに多要素認証（MFA）を実装するための新しい要件。この要件は、2025年3月31日までのベストプラクティスです。要件8.4.2および8.4.3で指定された両方のタイプのアクセスにMFAが必要であること、およびあるタイプのアクセスにMFAを適用しても、他のタイプのアクセスにMFAの別のインスタンスを適用する必要がなくなるわけではないことを明確にする注記を追加しました（8.4.2）。

- MFAシステムをセキュアに実装するための新しい要件。この要件は、2025年3月31日（8.5.1）までのベストプラクティスです。
- 対話型ログインに使用できるシステムアカウントまたはアプリケーションアカウントの管理に関する新しい要件。この要件は、2025年3月31日（8.6.1）までのベストプラクティスです。
- 対話型ログインに使用できるすべてのアプリケーションおよびシステムアカウント用に、パスワードやパスフレーズをファイルやスクリプトにハードコーディングしないという新たな要件が追加されました。この要件は、2025年3月31日（8.6.2）までのベストプラクティスです。
- アプリケーションおよびシステムアカウントのパスワードまたはパスフレーズを不正使用から保護するための新しい要件。この要件は、2025年3月31日（8.6.3）までのベストプラクティスです。

以前のPCI DSS 3.2.1からの追加のガイダンスと明確化

- 「認証要素」および「認証クレデンシャル」という用語の標準化。「非消費者ユーザー」という用語の削除および概要の明確化d消費者(カード所有者)が使用するアカウントには要件が適用されないこと。
- この要件は、単一のトランザクションを容易にするために一度に1つのカード番号にしかアクセスできないPOS端末のユーザーアカウントには適用されません(8.2.1)。
- この要件は、単一の取引を容易にするために一度に1つのカード番号にしかアクセスできないPOS端末のユーザーアカウントには適用されません(8.2.2)。
- この要件は、要件8.3.1（8.3.5）を満たすための認証要素としてパスワードまたはパスフレーズが使用されている場合にのみ適用されることを明確にします。
- この要件は、要件8.3.1を満たすための認証要素としてパスワードまたはパスフレーズが使用されている場合にのみ適用されることを明確にします。この要件は、単一の取引を容易にするために一度に1つのカード番号にしかアクセスできないPOS端末のユーザーアカウントには適用されません。この要件は、サービスプロバイダーの顧客アカウントには適用されませんが、サービスプロバイダーの担当者のアカウントには適用されます（8.3.9）。

データストレージへの影響

有効期限、特殊文字の数などに関するパスワードポリシーを設定する必要があります。ロールごとに次のパラメータを設定できます。

- ユーザ名の必須最小長
- ユーザ名に英文字と数字を混在させる必要があるかどうか
- パスワードの必須最小長
- パスワードに英文字と数字を混在させる必要があるかどうか
- パスワードで要求される特殊文字の最小数
- ユーザが自分のアカウントに最初にログインする場合にパスワードを変更する必要があるか
- 再利用できない以前のパスワードの数（最大4つ）
- 次回のパスワード変更までに経過する必要がある最小日数（最大90日）
- パスワードが期限切れになるまでの日数
- アカウントの自動ロックをトリガーする無効なログイン試行の回数
- 無効なログイン試行の最大回数に達してからアカウントがロックされる日数

多要素管理アクセス

ONTAP 9.3以降では、この要件に対応したのが、NetApp ONTAP System ManagerおよびActive IQ Unified Managerでの管理用Web認証と、NetApp ONTAPでのSSH管理用CLI認証です。

詳細については、「ONTAP 9.3における多要素認証」を参照してください。

ベストプラクティス

ONTAPシステムへのSSH管理アクセスには、プライマリおよびセカンダリのチェーン認証方式を使用するローカルで管理される管理者アカウント `password` と `publickey nsswitch`、およびのチェーン認証方式を使用するNIS/LDAPアカウントを使用し `publickey`ます。

ONTAP System Manager Web UIまたはActive IQ Unified Manager Web UIには、Security Assertion Markup Language（SAML）2.0を使用します。ONTAP OCSMまたはOCUMはサービスプロバイダのロールで、Microsoft Active Directoryフェデレーションサービス（ADFS）またはシボレスはアイデンティティプロバイダ（IdP）のロールです。認証要素はIdPで設定します。

ONTAPのパスワードのデフォルトのルールは次のとおりです。

- パスワードにユーザ名を含めることはできません。
- パスワードは8文字以上にする必要があります。
- 英文字と数字がそれぞれ1文字以上含まれている必要があります。
- 直近の6つのパスワードと同じパスワードは使用できません。

ユーザアカウントのセキュリティを強化するには、`security login role config modify` コマンドのパラメータを使用してアクセス制御ロールの設定を変更します。

- ユーザ名のルール設定は次のとおりです。
  - ユーザ名の必須最小長(`-username-minlength`)
  - ユーザー名に英文字と数字を混在させる必要があるかどうか(`-username- alphanum`)
- パスワードのルール設定は次のとおりです。
  - パスワードの必須最小長（`-passwd-minlength`）。（PCI-DSS 4.0では、最小文字数は12文字です）。
  - パスワードに英文字と数字を混在させる必要があるかどうか`-passwd- alphanum`()
  - パスワードに必要な特殊文字の数()`-passwd-min-special-chars`
  - ユーザが初めてアカウントにログインするときにパスワードを変更する必要があるかどうか（`-require-initial-passwd-update`）
  - 再利用できない以前のパスワードの数()`-disallowed-reuse`
  - 次回のパスワード変更までに経過する必要がある最小日数（`-change-delay`）
  - パスワードが期限切れになるまでの日数()`-passwd-expiry-time`
- 初期ログイン試行についてのルール設定は次のとおりです。
  - アカウントが自動的にロックされる無効なログイン試行の回数（`-max- failed-login-attempts`）。ユーザーの無効なログイン試行回数がこのパラメータで指定された値（PCI-DSS 4.0あたりの最大値は10）に達すると、ユーザーアカウントは自動的にロックされます。`security login unlock` コマンドは、ユーザアカウントのロックを解除します。
  - 無効なログイン試行が許可された最大回数に達した場合にアカウントがロックされる日数（`-lockout-duration`）

ルールの現在の設定を表示するには、`security login role config show` コマンドを使用します。`security login role config` コマンドとデフォルト設定については、ONTAP 9ドキュメントセンターのマニュアルページまたは失敗したログインの管理を参照してください。便宜上、サービスプロバイダーで使用されるログインアカウントは、一般的な管理アクセスに使用されるONTAPの一般的なアカウントと一致させることができます。

前述のパスワード保護に加えて、サービスプロバイダーファームウェア1.2以降では、IPアドレスからの失敗したSSHログイン試行が追跡されます。10分以内にIPアドレスから繰り返しログインエラーが5回以上検出された場合、サービスプロバイダーは次の15分間、そのIPアドレスとのすべての通信を停止します。通常の通信は15分後に再開されますが、ログインエラーが繰り返し検出されると、次の15分間は通信が再び中断されます。

要件9：カード所有者データへの物理的なアクセスを制限する

カード所有者データを保存、処理、または送信するカード所有者データまたはシステムへの物理的なアクセスは、個人がカード所有者データを含むシステムまたはハードコピーにアクセスして削除する機会を提供します。個人がカード所有者データにアクセスできないように、物理的なアクセスを適切に制限する必要があります。

要件9に記載されている3つの領域があります。

- 特に機密領域を参照する要件は、それらの領域にのみ適用されます。
- CDEを特に参照する要件は、CDE内に存在する機密領域を含め、CDE全体に適用されます。
- 施設を具体的に参照する要件は、CDEと機密領域が存在する事業構内（建物など）の物理的な境界でより広範に管理される可能性のある制御のタイプを参照しています。これらのコントロールは、訪問者を識別し、バッジを付け、ログを記録するガードデスクなど、CDEや機密領域の外に存在することがよくあります。「ファシリティ」という用語は、これらの制御が施設内のさまざまな場所に存在する可能性があることを認識するために使用されます。たとえば、建物の入り口、データセンターやオフィススペースの内部入り口などです。

以前のPCI DSS 3.2.1からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（9.1.2）に対してただちに有効です。
- 企業のターゲットリスク分析に基づいて、定期的なPOIデバイス検査の頻度を定義するための新しい要件。この要件は、2025年3月31日（9.5.1.2.1）までのベストプラクティスです。

以前のPCI DSS 3.2.1からの追加のガイダンスと明確化

- 概要では、要件9に記載されている3つの異なる領域（機密領域、CDE、および施設）を明確にしています。各要件環境CDE、機密領域、または施設が全体的に明確にされているかどうか。
- 使用していないときにコンソールをロックすることで、機密性の高い領域のコンソールへのアクセスを制限する、以前のテスト手順Bulletに対処するための要件が追加されました(9.2.4)。
- メディアを物理的に保護する手順(9.5)の要件を削除し、関連する要件に手順をマージしました。メディアバックアップを安全な場所に保存するための要件と、オフラインバックアップの場所のセキュリティを少なくとも12カ月ごとに2つの要件（9.4.1、9.4.1.1、9.4.1.2）に分ける必要があります。
- メディアの内外への配布手順の要件を撤廃(9.6)し、関連要件(9.4.2,9.4.3、9.4.4)に統合しました。
- メディアの保管とアクセシビリティを厳密に制御するための手順の要件を削除し(9.7)、関連する要件に手順をマージしました。メディアインベントリログの維持とメディアインベントリの年間実施に関する要件を、2つの要件（9.4.5、9.4.5.1）に分割します。
- メディアが不要になったときのメディア破壊手順の要件の削除(9.8)、関連する要件に手順をマージしました。不要になったメディアを破棄するオプションには、電子メディアを破棄するか、カード所有者データを回復不能にすることが含まれます（9.4.6、9.4.7）。
- 要件の焦点は、「支払いカードフォームファクタとの直接的な物理的インタラクションを使用して支払いカードデータをキャプチャするPOI（Point-of-Interaction）デバイス」であることを明確にします。

要件環境がカード存在トランザクション（9.5.1）で使用されるPOIデバイスを導入したことを明確にしました。

データストレージへの影響

ONTAPシステムは、ロックされた部屋に設置し、できればロックされたラックに設置する必要があります。NetAppでは、PCI DSS 4.0の要件を満たすかそれ以上の保護を実現するために、NSE、NVE、NAEを推奨しています。NSEは、業界をリードするベンダーが提供するFIPS-140-2レベル2の検証済みSEDを使用して、NetAppがFull Disk Encryption（FDE）を実装したものです。NVEとNAEは、NetAppソフトウェアベースの保存データ暗号化解決策で、あらゆるドライブタイプで使用できます。NAEとNVEはどちらもFIPS 140-2に準拠しています。ONTAPでNVEを使用すると、（AES 256ビット暗号化を使用して）ボリューム単位でデータを暗号化できます。NAEは、アグリゲート内のすべてのボリュームでAES-256ビット暗号化キーを共有します。NAEアグリゲートとNVEボリューム暗号化キーは、外部キー管理ツールに格納できます。NSE、NVE、NAEを2つの暗号化レイヤとして組み合わせることができます。物理的なセキュリティが侵害され、ディスクがシステムから物理的に取り外された場合、ディスクの暗号化によってデータが保護されます。

NSE、NAE、NVEの詳細については、NetApp暗号化パワーガイドを参照してください。

ベスト プラクティス
物理的な部屋へのアクセスを制御し、ロック付きの密閉ラックを使用して、ONTAPシステムを物理的に保護します。NSEとNVEを使用して保護を強化

ネットワークの定期的な監視とテスト

要件10：システムコンポーネントとカード所有者データへのすべてのアクセスをログに記録して監視する

ロギングメカニズムとユーザアクティビティを追跡する機能は、データ侵害の影響を防止、検出、または最小限に抑えるために重要です。すべてのシステムコンポーネントとCDEにログが存在することで、問題が発生した場合の追跡、警告、および分析を徹底的に行うことができます。侵害の原因を特定することは、システムアクティビティログなしでは不可能ではないにしても困難です。

この要件には、従業員、請負業者、コンサルタント、社内外のベンダー、およびその他のサードパーティ（サポートまたはメンテナンスサービスを提供するベンダーなど）による環境ユーザアクティビティが含まれます。

これらの要件は、消費者(カード所有者)のユーザー活動には適用されません。

以前のPCI DSS 3.2.1からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（10.1.2）でただちに有効になります。
- 自動化されたメカニズムを使用して監査ログのレビューを実行するための新しい要件。この要件は、2025年3月31日（10.4.1.1）までのベストプラクティスです。
- 他のすべてのシステムコンポーネントの定期的なログレビューの頻度を定義するターゲットリスク分析の新しい要件（要件10.4.1では定義されていません）。この要件は、2025年3月31日（10.4.2.1）までのベストプラクティスです。
- すべての企業が、重要なセキュリティ制御システムの障害を検出、警告し、迅速に対処するための新しい要件。この要件は、2025年3月31日までのベストプラクティスです。この新しい要件環境All entities - この要件には 、サービスプロバイダー（10.7.2）の要件10.7.1に含まれていない2つの重要なセキュリティ制御が追加されています。
- 重要なセキュリティ制御の障害に迅速に対応するための新しい要件。サービスプロバイダの場合：これは現在のPCI DSS v3.2.1の要件です。その他すべての（サービスプロバイダー以外の）エンティティの場合：これは新しい要件です。この要件は、2025年3月31日（10.7.3）までのベストプラクティス（非サービスプロバイダ向け）です。

以前のPCI DSS 3.2.1からの追加のガイダンスと明確化

- 監査ログ、システムコンポーネント、カード所有者データに重点を置くように、主要要件タイトルを更新します。これらの要件は、消費者(カード所有者)のユーザー活動には適用されないことを明確にします。全体を通して「監査証跡」という用語が「監査ログ」に置き換えられました。

データストレージへの影響

NetApp ONTAPシステムには、広範な監査ログと監視制御機能があります。ログは重大度の高いイベントトリガー型メッセージで、ONTAPシステムによって生成され、クラスタ上のフラットテキストファイルに記録されます。ログは、管理者、NetAppサポートおよびNetApp Active IQ（AutoSupport）が、さまざまな問題の根本原因を特定して切り分けるための主要なリソースです。同様に、ログはPCI DSS 4.0のロギング要件も満たしています。

ONTAPは、いくつかのタイプのログを提供します。主なタイプには、Event Management System（EMS；イベント管理システム）、監査ログ、およびActive IQログがあります。

EMSは、syslog標準に基づいて構築されたONTAPメッセージング機能です。EMSを使用すると、クラスタ全体のイベントの管理と、管理者による通知方法の選択が簡易化されます。EMSはカタログ化されたロギングメカニズムを提供し、すべてのイベントに正式な定義があります。このメカニズムにより、EMSは自動スパム管理（メッセージ抑制など）、設定可能な通知、低レベルデータをわかりやすいテキストに変換する支援、NVMEMによるメッセージのバックアップ、メッセージの自動タグ付けなどのサービスを提供できます。

EMSではイベントがキャプチャされますが、アクションのキャプチャには監査ログが使用されます。監査ログには、クラスタに送信されたコマンド、送信元のユーザ、およびコマンドの成功または失敗が記録されます。この情報には環境、CLI、REST API呼び出し（NetApp管理ツールや自動化からのコマンドなど）、およびHTTPS要求が含まれます。

最後に、Active IQログには、EMSイベント、監査ログエントリ、およびシステムの状態情報の組み合わせが記録されます。この情報は、NetAppサポート担当者がシステムの健全性を診断する際に役立ちます。

3種類のログ（EMS、監査、Active IQ）を組み合わせることで、セキュリティ上の理由から、システムの記録が明確かつ永続的に記録されます。

デフォルトでは、set要求は `command-history.log` およびに記録されます `mgwd.log`が、get要求は記録されません。この設定を表示または変更するには `security audit`、CLI操作を実行します。security auditコマンドの設定に関係なく、set要求は常に `command- history.log` ファイルに記録されます。

ログファイルにアクセスするには、Service Processor Infrastructure（spi）Webサービスを使用します。spi Webサービスはデフォルトで有効になっており、手動で無効にすることができます（`vserver services web modify - vserver * -name spi -enabled false`）。spi Webサービスでは、ログファイルをダウンロードできますが、システムでは変更できません。また、十分に高い権限を持つ管理ユーザがファイルを削除することもできます。

ロギングの詳細については、TR-4303：『Logging in Clustered Data ONTAP』を参照してください。また、ONTAPがONTAP 9ドキュメントセンターで監査ログを実装する方法でも説明します。

adminロールにはspi Webサービスへのアクセスがデフォルトで許可されており、アクセスを手動で無効にすることができます（`services web access delete -vserver cluster_name -name spi -role admin`）。

1. Webブラウザでspi WebサービスのURLを次のいずれかの形式で指定します。

   `https://cluster-mgmt-LIF/spi/cluster-mgmt-LIF` は、クラスタ管理LIFの名前またはIPアドレスです。

2. ブラウザにユーザ アカウントとパスワードの入力画面が表示されたら、これらの情報を入力します。アカウントが認証されると、`/mroot/etc/log//mroot/etc/crash//mroot/etc/mib/` クラスタ内の各ノードの、およびディレクトリへのリンクがブラウザに表示されます。

すべてのロギング情報は、PCI DSS準拠のセキュリティポリシーの一部として管理する必要があります。EMSログには、システムに影響を与えたイベントの概要が表示され、外部攻撃（DDoS攻撃など）の検出に役立ちます。同様に、監査ログは、システムに入力された悪意のあるコマンドを検出するのに役立ちます。

また、すべてのシステムのログを一元的に確認できるように、リモートsyslogサーバなどの一元的な場所にログを送信することも推奨されます。ONTAPは、クラスタログ転送機能でこの機能をサポートしています。詳細については、TR-4569：『Security Hardening Guide for NetApp ONTAP 9』の「Sending out syslog」の質問を参照してください。

ベスト プラクティス

管理操作を監視するには、ONTAPの監査ログ機能を使用します。ログを定期的に確認するための組織ポリシーを確立します。ログをONTAPから外部syslogサーバにエクスポートして、ロギングと監視を一元化します。

要件11：システムとネットワークのセキュリティを定期的にテストする

脆弱性は、悪意のある個人や研究者によって継続的に検出され、新しいソフトウェアによって導入されます。システムコンポーネント、プロセス、カスタムソフトウェアを頻繁にテストして、セキュリティ制御が変化する環境を継続的に反映していることを確認する必要があります。

以前のPCI DSS 3.2.1からの要件の進化

- 役割と責任に関する新しい要件。この要件は、すべてのv4.0評価（11.1.2）でただちに有効になります。
- 内部の脆弱性スキャン中に検出されたその他のすべての該当する脆弱性(高リスクまたはクリティカルではない脆弱性)を管理するための新しい要件。この要件は、2025年3月31日（11.3.1.1）までのベストプラクティスです。
- 認証済みスキャンを使用して内部脆弱性スキャンを実行するための新しい要件。この要件は、2025年3月31日（11.3.1.2）までのベストプラクティスです。
- マルチテナントサービスプロバイダは、顧客の外部侵入テストをサポートするという新たな要件を満たしています。この要件は、2025年3月31日（11.4.7）までのベストプラクティスです。
- サービスプロバイダーは、侵入検知および侵入防止技術を使用して、マルウェアの隠れた通信チャネルの検出、アラートオン/防止、および対処を行う必要があります。この要件は、2025年3月31日（11.5.1.1）までのベストプラクティスです。
- コンシューマブラウザが受信するHTTPヘッダーと支払いページの内容に対する不正な変更を警告するための変更および改ざん検出メカニズムを導入するための新しい要件。この要件は、2025年3月31日（11.6.1）までのベストプラクティスです。

以前のPCI DSS 3.2.1からの追加のガイダンスと明確化

- 主要要件タイトルのマイナー更新。
- 要件の目的は、許可されたワイヤレスアクセスポイントと許可されていないワイヤレスアクセスポイントの両方を管理することであることを明確にします。Aこの要件は、ワイヤレステクノロジの使用を禁止するポリシーが存在する場合でも適用されます（11.2.1）。
- 次の点の明確化：（11.4.1）：
  - この方法論は、エンティティによって定義、文書化、実装されます。
  - ペネトレーションテストの結果は、少なくとも12か月間保持されます。
  - この方法論には、侵入テスト中に発見された悪用可能な脆弱性とセキュリティの弱点によって引き起こされるリスクを評価し、対処するための文書化されたアプローチが含まれています。

  - ネットワーク内部からのテスト（内部ペネトレーションテスト）とネットワーク外部からのテスト（外部ペネトレーションテスト）の意味。
- 侵入テストの結果は、セキュリティ問題(11.4.4)によってもたらされるリスクの企業の評価に従って修正されることの明確化。

データストレージへの影響

日常的なセキュリティ検証は、包括的なセキュリティポリシーの一部である必要がある継続的で動的なプロセスです。多くの組織では、よく知られた業界ツールを使用して、定期的に（四半期ごとまたはそれ以上の頻度で）セキュリティスキャンを実施しています。これらのツールはさまざまな方法で動作し、さまざまなタイプの結果を生成するため、組み合わせて使用することがよくあります。

サービスプロバイダーには、隠れたマルウェアの通信チャネルを検出、警告、防止、対処するための追加の対応力があります。NetApp ONTAPシステムは、NAS（NFSおよびSMB）に接続された共有上のマルウェア（ランサムウェアなど）からの保護もサポートします。たとえば、FPolicyは、NetApp Cloud Insightsまたは当社のパートナーが提供する同様の機能と組み合わせて、ユーザー行動分析（UBA）を通じてマルウェアを検出する優れた機能を提供します。個々のユーザーの行動の側面から潜在的なマルウェア攻撃を探します。1つのユーザーアカウントをハイジャックすることは、ハッカーがマルウェア攻撃を開始する際に取る可能性のある1つの手段にすぎません。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とActive IQ Unified Managerには、ランサムウェアの検出機能も追加されています。Active IQは、ONTAPシステムがNetApp設定のベストプラクティス（FPolicyの有効化など）に準拠しているかどうかをチェックします。Active IQ Unified Managerは、Snapshotコピーの異常な増加やStorage Efficiencyの損失に関する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ている可能性があります。ONTAP 9.10.1のランサムウェア対策機能は、組み込みのMLを活用して、ボリュームワークロードアクティビティとデータエントロピーを使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し、UBAでは検出できない攻撃を検出できるようにします。

ONTAPでの脆弱性スキャン

セキュリティスキャナの結果を理解するには、それらがどのように動作するかについていくつかの側面を理解することが重要です。セキュリティの脆弱性について、スキャナがデバイスの実際のテストを実行することはほとんどありません。一部のセキュリティスキャナは、デバイスで検出されたリリースバージョン識別子に対するスキャンされたデバイスの機能に関する前提条件を基にしています。これらの識別子とデバイスで実行されているソフトウェアによって、修正された脆弱性が特定され、「誤検出」レポートが生成される可能性があります。

たとえば、ONTAPやその他のNetApp製品は、新機能が導入されたり、セキュリティの脆弱性の疑いがあるものが特定されて修正されたりすると、時間の経過とともに変更されます。NetApp製品のオープンソースコンポーネントに適用されるライセンスでは、多くの場合、コード内で元のリリースバージョン識別子を使用する必要があります。そのため、NetAppは既知の脆弱性に対する修正を継続的に適用しますが、必ずしも脆弱性スキャナによって検出されるバージョンの更新をトリガーするわけではありません。

認証されたユーザーとして脆弱性スキャンを実行すると、これらの誤検出を減らすことができます。PCI DSS 4.0では、認証済みスキャンを使用して内部脆弱性スキャンを実行することを推奨しています。

詳細については、NetAppナレッジベースの記事「Vulnerability Scanner Indicates ONTAP asan unsupported Unix version」を参照してください。

ポートスキャナまたはその他の方法で、疑わしい脆弱性を発見した場合は、「NetAppサポートページにセキュリティの問題を報告する方法」の手順を参照してください。このページでセキュリティアドバイザリを購読することもできます。

ベスト プラクティス

データセンター内のすべてのシステムに対して脆弱性スキャナを定期的に実行するポリシーを確立します。

情報セキュリティポリシーの維持

要件12:組織のポリシーとプログラムで情報セキュリティをサポートする

組織の全体的な情報セキュリティポリシーは、組織全体のトーンを設定し、従業員に期待される内容を通知します。すべての従業員は、カード所有者データの機密性と、それを保護する責任を認識する必要があります。

要件12の目的上、「人員」とは、アカウントデータを保護するためのセキュリティ責任を負う、またはアカウントデータのセキュリティに影響を与える可能性のあるフルタイムおよびパートタイムの従業員、派遣社員、請負業者、およびコンサルタントを指します。

以前のPCI DSS 3.2.1からの要件の進化

- 組織全体のリスク評価および特定のターゲットリスク分析による置き換えの正式な要件の削除(12.3.1および12.3.2)。
- 担当者の責任に関する正式な承認の追加(12.1.3)。
- リモートアクセス技術を使用する場合、PANのコピーおよび移動を防止するための技術的な制御のための要件の削除および新しい要件3.4.2の追加(3.4.2)。
- PCI DSS要件のターゲットリスク分析を実行する新しい要件で、実行頻度に柔軟性があります。この要件は、2025年3月31日（12.3.1）までのベストプラクティスです。
- カスタマイズされたアプローチを使用して、エンティティがカスタマイズされたアプローチで満たす各PCI DSS要件のターゲットリスク分析を実行するエンティティの新しい要件。この要件は、v4.0評価を受け、カスタマイズされたアプローチ(12.3.2)を使用しているすべての企業に対して直ちに有効です。
- 少なくとも12か月に1回、使用されている暗号スイートとプロトコルを文書化してレビューするための新しい要件。この要件は、2025年3月31日（12.3.3）までのベストプラクティスです。
- 使用中のハードウェアおよびソフトウェアテクノロジを12カ月に1回以上レビューするという新しい要件が追加されました。この要件は、2025年3月31日（12.3.4）までのベストプラクティスです。
- PCI DSSの範囲を少なくとも12カ月ごとに文書化して確認する新しい要件。範囲内の環境に大幅な変更があった場合。この要件は、すべてのv4.0評価（12.5.2）に対してただちに有効です。
- サービスプロバイダは、PCI DSSの範囲を少なくとも6か月に1回、および範囲内の環境に大きな変更がある場合に文書化して確認する必要があります。この要件は、2025年3月31日（12.5.2.1）までのベストプラクティスです。
- 組織構造に重大な変更がある場合に、PCI DSSの範囲と統制の適用可能性への影響を文書化してレビューするためのサービスプロバイダーの新しい要件。この要件は、2025年3月31日（12.5.3）までのベストプラクティスです。
- セキュリティ意識向上プログラムのレビューと更新（必要に応じて）の新しい要件は、少なくとも12か月に1回です。この要件は、2025年3月31日（12.6.2）までのベストプラクティスです。
- CDEのセキュリティに影響を与える可能性のある脅威や脆弱性を認識するためのセキュリティ認識トレーニングの新しい要件。この要件は、2025年3月31日（12.6.3.1）までのベストプラクティスです。
- 要件12.2.1に準拠したエンドユーザテクノロジーの受け入れ可能な使用についての認識を含めるためのセキュリティ認識トレーニングの新しい要件。この要件は、2025年3月31日（12.6.3.2）までのベストプラクティスです。
- サービスプロバイダーが要件12.8.4および12.8.5を満たすために顧客の情報要求をサポートするための新しい要件。この要件は、すべてのv4.0評価（12.9.2）に対してただちに有効です。

- インシデント対応担当者の定期的なトレーニングの頻度を定義するために、ターゲットリスク分析を実行するための新しい要件。この要件は、2025年3月31日（12.10.4.1）までのベストプラクティスです。
- インシデント対応計画の一環として、監視および対応するセキュリティ監視システムの要件と更新を統合し、次のものを含めました（12.10.5）。
  - 不正なワイヤレスアクセスポイントの検出（旧11.1.2）、
  - 重要なファイルの変更検出メカニズム（旧11.5.1）、
  - 支払いページの変更および改ざん検出メカニズムを使用するための新しい要件箇条書き（新しい要件11.6.1に関連）。

注： この箇条書きは2025年3月31日までのベストプラクティスです。

- インシデント対応手順が導入され、予期しない場所に保存されたパンが検出されたときに開始されるという新しい要件。この要件は、2025年3月31日（12.10.7）までのベストプラクティスです。

以前のPCI DSS 3.2.1からの追加のガイダンスと明確化

- 情報セキュリティをサポートする組織のポリシーとプログラムに重点が置かれていることを反映するための主要要件タイトルの更新。
- 責任は、最高情報セキュリティ責任者またはその他の知識豊富な経営陣のメンバーに正式に割り当てられていることを明確にします。情報セキュリティの責任を正式に割り当てるためのマージされた要件(12.1.4)。
- 要件の目的がエンドユーザテクノロジーの利用ポリシーであることを明確にします。経営陣の明示的な承認、テクノロジーの受け入れ可能な使用、および従業員の使用のために会社が承認したハードウェアおよびソフトウェア製品のリストに焦点を当てるために、要件を統合および削除しました（12.2.1）
- 目的は、すべての従業員が企業の情報セキュリティポリシーとカード所有者データの保護における彼らの役割を認識していることであることを明確にする(12.6.1)
- 「サービスプロバイダ」という用語を「サードパーティサービスプロバイダ（TPSP）」に置き換える。PCI DSSに準拠したTPSPを使用しても、PCI DSSに準拠したエンティティにはならず、独自のPCI DSS準拠に対するエンティティの責任を排除するものではないことを明確にします(12.8.1-12.8.5)。
- 「サービスプロバイダ」という用語の「サードパーティサービスプロバイダ（TPSP）」への置き換え（12.8.2）。
- 「サービスプロバイダ」という用語の「サードパーティサービスプロバイダ（TPSP）」への置き換え（12.8.3）。
- 「サービスプロバイダ」という用語を「サードパーティサービスプロバイダ（TPSP）」に置き換える。企業が企業に代わってPCI DSS要件を満たすためにTPSPと合意している場合、企業はTPSPと協力して、該当するPCI DSS要件が満たされていることを確認する必要があることを明確にします。TPSPが該当するPCI DSS要件を満たしていない場合、それらの要件はエンティティにも適用されません(12.8.4)。
- 「サービスプロバイダ」という用語を「サードパーティサービスプロバイダ（TPSP）」に置き換える。TPSPおよびエンティティによって管理されるPCI DSS要件に関する情報には、TPSPとエンティティ間で共有されているものを含める必要があることを明確にします(12.8.5)。
- 「システム違反」および「侵害」という用語を「疑わしいセキュリティインシデントまたは確認済みセキュリティインシデント（12.10.1）」に置き換える。
- 「alerts」という用語を「suspected or confirmed security incidents（12.10.3）」に置き換える。
- 「システム違反」という用語を「疑わしいまたは確認済みのセキュリティインシデント（12.10.4）」に置き換える。

データストレージへの影響

組織の情報セキュリティポリシーに準拠し、サポートするようにONTAPを設定できます。これには、RBAC、ネットワークサービス（NTPなど）、パスワードポリシー、管理アクセス用のMFA、データ保持、バックアップポリシー、MAVが含まれ、データの削除などの潜在的に有害な操作が複数の管理者の承認を得られるようにします。

ベストプラクティス：

各ユーザの責任に一致するロールを使用して、セキュリティポリシーに準拠するようにONTAPを設定します。MFAを使用して盗まれた認証情報から保護し、MAVを使用して潜在的に有害なアクションが複数の管理者の承認を得ていることを確認します。

詳細情報の入手方法

- ネットワーク管理ガイドONTAP 9
  https://docs.netapp.com/us-en/ontap/pdfs/sidebar/Network_management.pdf
- クラスタアドミニストレーションガイドONTAP 9
  https://docs.netapp.com/us-en/ontap/pdfs/sidebar/Cluster_administration.pdf
- Data ONTAPでのSNMPサポート（NetAppログインが必要）
  https://fieldportal.netapp.com/content/250723
- セキュリティONTAP 9
  https://docs.netapp.com/us-en/ontap/pdfs/sidebar/Security.pdf
- FIPS 140-2準拠の暗号化モジュールソフトウェア
  https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144
- NetApp製品のセキュリティ
  https://security.netapp.com/
- NetAppセキュリティアドバイザリ
  https://security.netapp.com/advisory/
- TR-4067：『NFS in NetApp ONTAP Best Practice and Implementation Guide』
  https://www.netapp.com/us/media/tr-4067.pdf
- TR-4073：『Secure Unified Authentication』
  https://www.netapp.com/us/media/tr-4073.pdf
- TR-4543：『SMB Protocol Best Practices』
  https://www.netapp.com/us/media/tr-4543.pdf
- TR-4303：『Logging in Clustered Data ONTAP』
  https://www.netapp.com/us/media/tr-4303.pdf
- How to Report Security Issues to NetApp
  https://security.netapp.com/contact/
- TR-4569：『Security Hardening Guide for NetApp ONTAP 9』
  https://www.netapp.com/us/media/tr-4569.pdf
- TR-4191：『Best Practices Guide for Clustered Data ONTAP Windows File Services』
  https://www.netapp.com/us/media/tr-4191.pdf
- TR-4647：『Multifactor Authentication in ONTAP 9.3』
  https://www.netapp.com/us/media/tr-4647.pdf
- セキュリティとデータ暗号化ONTAP 9
  https://docs.netapp.com/us-en/ontap/pdfs/sidebar/Security_and_data_encryption.pdf
- 脆弱性スキャナがONTAPをサポートされていないUNIXバージョンとして示している
  https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Vulnerability_Scanner_indicates_ONTAP_as_an_unsupported_Unix_version
- PCI-DSS規格
  https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss#agree メント

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。

doccomments@netapp.comまでお問い合わせください。

件名に「TECHNICAL REPORT 4401」と添えてください

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン2.0	2022年9月	Matt Trudewind：PCI DSS 4.0の要件に合わせて更新。
バージョン1.3	2018年11月	Dan Tulledge：NSEドライブの説明。
バージョン1.2	2018年10月	Dan Tulledge：セクション2.1「firewall policy-allow-list」を更新。
バージョン1.1	2018年3月	Dan Tulledge: PCI DSSバージョン3.2を更新。
バージョン1.0	2015年5月	初版リリース

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4401-0922-JP

NetApp