



## **TR-4645 : 『Security features』**

StorageGRID solutions and resources

NetApp  
December 12, 2025

# 目次

TR-4645 : 『Security features』	1
オブジェクトストア内のStorageGRIDデータとメタデータを保護	1
追加情報の参照先	1
用語と略語	2
データアクセスセキュリティ機能	2
オブジェクトとメタデータのセキュリティ	11
管理セキュリティ機能	13
プラットフォームのセキュリティ機能	17
クラウドとの統合	19

# TR-4645：『Security features』

## オブジェクトストア内のStorageGRIDデータとメタデータを保護

StorageGRIDオブジェクトストレージソリューションに組み込まれているセキュリティ機能をご確認ください。

これは、データアクセス、オブジェクトとメタデータ、管理アクセス、プラットフォームセキュリティを網羅した、NetApp® StorageGRID® のさまざまなセキュリティ機能の概要です。StorageGRID 12.0 でリリースされた最新の機能が含まれるように更新されました。

セキュリティは、NetApp StorageGRIDオブジェクトストレージソリューションに不可欠な要素です。オブジェクトストレージに適した多くのタイプのリッチコンテンツデータも機密性が高く、規制やコンプライアンスの対象となるため、セキュリティは特に重要です。StorageGRIDの機能が進化し続ける中で、このソフトウェアは、組織のセキュリティ体制を保護し、業界のベストプラクティスに準拠するのに役立つ多くのセキュリティ機能を利用できるようにします。

このホワイトペーパーでは、StorageGRID 12.0 のさまざまなセキュリティ機能の概要を 5 つのカテゴリに分けて説明します。

- ・データアクセスセキュリティ機能
- ・オブジェクトとメタデータのセキュリティ機能
- ・管理セキュリティ機能
- ・プラットフォームのセキュリティ機能
- ・クラウドとの統合

このホワイトペーパーはセキュリティデータシートとして作成されており、デフォルトでは構成されていない、本書に記載されているセキュリティ機能をサポートするようにシステムを構成する方法については詳しく説明していません。その "StorageGRIDセキュリティガイド"公式ウェブサイトで入手可能 "StorageGRID のドキュメント"ページ。

このレポートで説明する機能に加えて、StorageGRIDはにも準拠して "NetApp製品セキュリティ脆弱性対応および通知ポリシー" います。報告された脆弱性は、製品のセキュリティインシデント対応プロセスに従って検証され、対応されます。

NetApp StorageGRIDは、要件の厳しいエンタープライズオブジェクトストレージのユースケースに対応する高度なセキュリティ機能を提供します。

## 追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- ・NetApp StorageGRID : SEC 17a-4 (f) 、FINRA 4511 (c) 、CFTC 1.31 (c) - (d) コンプライアンス評価 <https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf>
- ・NetApp StorageGRID NIST FIPS 140-3 カーネル暗号化認定 <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097>

- NetApp StorageGRID NIST SP 800-90B エントロピー認定 <https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223>
- NetApp StorageGRIDカナダサイバーセキュリティセンター コモンクライテリア認定 <https://www.commoncriteriaproduct.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf>
- StorageGRIDドキュメントページ [https://docs.netapp.com/us-en/storagegrid/\[\]](https://docs.netapp.com/us-en/storagegrid/)
- NetApp製品ドキュメント <https://www.netapp.com/support-and-training/documentation/>

## 用語と略語

このセクションでは、ドキュメントで使用される用語の定義について説明します。

用語または頭字語	定義
S3	Simple Storage Serviceの略。
クライアント	データアクセス用にS3プロトコルを使用するか、管理用にHTTPプロトコルを使用してStorageGRIDと連携できるアプリケーション。
テナント管理者	StorageGRIDテナントアカウントの管理者
テナントユーザ	StorageGRIDテナントアカウント内のユーザ
TLS	トランSPORT層セキュリティ
ILM	情報ライフサイクル管理
LAN	ローカルエリアネットワーク
グリッド管理者	StorageGRIDシステムの管理者
グリッド	StorageGRIDシステム
バケット	S3に格納されたオブジェクトのコンテナ
LDAP	Lightweight Directory Access Protocolの略
秒	証券取引委員会（取引所メンバー、ブローカー、ディーラーを規制）
フィンラ	金融業界規制当局（SEC Rule 17a-4 (f) のフォーマットおよびメディア要件を延期）
CFTC	商品先物取引委員会、商品先物取引の規制
NIST	米国標準技術研究所

## データアクセスセキュリティ機能

StorageGRIDのデータアクセスセキュリティ機能について説明します。



機能	機能	影響	コンプライアンス
設定可能なTransport Layer Security (TLS)	<p>TLSは、クライアントとStorageGRIDゲートウェイノード、ストレージノード、またはロードバランサエンドポイント間の通信用にハンドシェイクプロトコルを確立します。</p> <p>StorageGRIDでは、TLSで次の暗号スイートがサポートされています。</p> <ul style="list-style-type: none"> <li>• TLS_AES_256_GCM_SHA384</li> <li>• TLS_AES_128_GCM_SHA256</li> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• ECDHE-ECDSA-AES128-GCM-SHA256</li> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• TLS_AES_256_GCM_SHA384</li> <li>• DHE-RSA-AES128-GCM-SHA256</li> <li>• DHE-RSA-AES256-GCM-SHA384</li> <li>• AES256-GCM-SHA384</li> <li>• AES128-GCM-SHA256</li> <li>• TLS_CHACHA20_POLY1305_SHA256</li> <li>• ECDHE-ECDSA-CHACHA20-POLY1305</li> <li>• ECDHE-RSA-CHACHA20-POLY1305</li> </ul> <p>TLS v1.2および1.3をサポート。</p> <p>SSLv3、TLS v1.1以前はサポートされていません。</p>	<p>クライアントとStorageGRIDがお互いを識別して認証し、機密性とデータ整合性を維持して通信できるようにします。最新のTLSバージョンを確実に使用します。[設定/セキュリティ]設定で暗号を設定できるようになりました。</p>	—

機能	機能	影響	コンプライアンス
設定可能なサーバ証明書（ロードバランサエンドポイント）	グリッド管理者は、サーバ証明書を生成または使用するようにロードバランサエンドポイントを設定できます。	標準の信頼された認証局（CA）によって署名されたデジタル証明書を使用して、ロードバランサエンドポイントごとにグリッドとクライアント間のオブジェクトAPI処理を認証できるようになります。	—
設定可能なサーバ証明書（APIエンドポイント）	グリッド管理者は、組織の信頼されたCAによって署名されたサーバ証明書を使用するように、すべてのStorageGRID APIエンドポイントを一元的に設定できます。	標準の信頼されたCAによって署名されたデジタル証明書を使用して、クライアントとグリッドの間のオブジェクトAPI処理を認証できます。	—

機能	機能	影響	コンプライアンス
マルチテナント	StorageGRIDでは、グリッドごとに複数のテナントがサポートされ、各テナントに独自のネームスペースがあります。テナントはS3プロトコルを提供します。デフォルトでは、バケット/コンテナおよびオブジェクトへのアクセスはアカウント内のユーザに制限されます。テナントには、1人のユーザ（各ユーザが独自のアカウントを持つエンタープライズ環境など）または複数のユーザ（サービスプロバイダ環境など、各アカウントがサービスプロバイダの企業および顧客であるサービスプロバイダ環境など）を設定できます。ユーザはローカルまたはフェデレーテッドにすることができます。フェデレーテッドユーザは、Active DirectoryまたはLightweight Directory Access Protocol (LDAP) によって定義されます。StorageGRIDには、ユーザがローカルまたはフェデレーテッドアカウントのクレデンシャルを使用してログインするテナントごとのダッシュボードが用意されています。ユーザは、バケットに格納されているデータ内の使用状況やオブジェクトの使用状況など、グリッド管理者によって割り当てられたクォータに対するテナント使用状況に関する可視化されたレポートにアクセスできます。管理権限を持つユーザは、ユーザ、グループ、アクセスキーの管理など、テナントレベルのシステム管理タスクを実行できます。	StorageGRID管理者は、テナントアクセスを分離しながら複数のテナントのデータをホストできます。また、Active DirectoryやLDAPなどの外部のアイデンティティプロバイダとユーザをフェデレーションすることでユーザIDを確立できます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
アクセスクレデンシャルの否認防止	すべてのS3処理は、一意のテナントアカウント、ユーザ、およびアクセスキーで識別され、ログに記録されます。	Grid管理者は、どのAPIアクションをどのユーザが実行するかを設定できます。	—

機能	機能	影響	コンプライアンス
匿名アクセスの無効化	デフォルトでは、S3アカウントに対して匿名アクセスは無効になっています。テナントアカウント内のバケット、コンテナ、またはオブジェクトにアクセスするには、要求者がテナントアカウント内の有効なユーザの有効なアクセスクレデンシャルを持っている必要があります。明示的なIAMポリシーを使用して、S3バケットまたはオブジェクトへの匿名アクセスを有効にできます。	グリッド管理者がバケット/コンテナおよびオブジェクトへの匿名アクセスを無効化または制御できるようにします。	—
コンプライアンスWORM	SEC Rule 17a-4 (f) の要件を満たすように設計され、Cohassetによって検証されています。バケットレベルでの準拠を有効にできます。保持期間は延長できますが、短縮することはできません。情報ライフサイクル管理 (ILM) ルールでは、最小限のデータ保護レベルが適用されます。	規制上のデータ保持要件があるテナントで、格納オブジェクトとオブジェクトメタデータのWORM保護を実現できます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
WORM	グリッド管理者は、[Disable Client Modify]オプションを有効にすることで、グリッド全体のWORMを有効にできます。これにより、クライアントがすべてのテナントアカウントのオブジェクトまたはオブジェクトメタデータを上書きまたは削除できなくなります。  S3テナント管理者は、IAMポリシーを指定して、テナント、バケット、またはオブジェクトブレフィックスでWORMを有効にすることもできます。このポリシーには、オブジェクトおよびメタデータの上書きに関するカスタムのS3 :PutOverwriteObject権限が含まれています。	グリッド管理者とテナント管理者は、格納オブジェクトとオブジェクトメタデータに対するWORM保護を制御できます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)

機能	機能	影響	コンプライアンス
KMSホストサーバ暗号化キー管理	グリッド管理者は、Grid Managerで1つ以上の外部キー管理サーバ（KMS）を設定して、StorageGRIDサービスとストレージアプライアンスに暗号化キーを提供できます。各KMSホストサーバまたはKMSホストサーバクラスタは、Key Management Interoperability Protocol（KMIP）を使用して、関連付けられたStorageGRIDサイトのアプライアンスノードに暗号化キーを提供します。	保存データの暗号化が実現されます。アプライアンスボリュームが暗号化されると、ノードがKMSホストサーバと通信できる場合を除き、アプライアンス上のデータにアクセスすることはできません。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
自動フェイルオーバー	StorageGRIDは、あらかじめ組み込まれた冗長性と自動フェイルオーバー機能を提供します。ディスクまたはノードからサイト全体に至るまで、複数の障害が発生しても、テナントアカウント、バケット、オブジェクトへのアクセスを継続できます。StorageGRIDはリソースを認識し、使用可能なノードとデータの場所に要求を自動的にリダイレクトします。StorageGRIDサイトは、孤立モードでも動作できます。WANが停止してサイトがシステムの残りの部分から切断された場合、ローカルリソースで読み取りと書き込みを続行でき、WANがリストアされるとレプリケーションが自動的に再開されます。	グリッド管理者は、アップタイムやSLAなどの契約上の義務に対処し、ビジネス継続性計画を実装できます。	—
• S3固有のデータアクセスセキュリティ機能*	AWS署名バージョン2およびバージョン4	API要求の署名は、S3 API処理の認証を提供します。AmazonはSignature Version 2とVersion 4の2つのバージョンをサポートしている。署名プロセスは、要求者の身元を確認し、転送中のデータを保護し、潜在的なリブレイ攻撃から保護します。	シグネチャバージョン4に関するAWSの推奨事項に準拠し、シグネチャバージョン2を使用する古いアプリケーションとの下位互換性を有効にします。

機能	機能	影響	コンプライアンス
—	S3 オブジェクトのロック	StorageGRIDのS3オブジェクトロック機能は、Amazon S3 のS3オブジェクトロックに相当するオブジェクト保護ソリューションです。	テナントは、特定のオブジェクトを一定期間または無期限に保持することを求める規制に準拠するために、S3オブジェクトロックを有効にしたバケットを作成できます。
SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ル ール4511 (c)	S3クレデンシャルのセキュアなストレージ	S3アクセスキーは、パスワードハッシュ関数 (SHA-2) で保護された形式で格納されます。	キーの長さ ( $10^{31}$ ランダムに生成された数字) とパスワードハッシュアルゴリズムを組み合わせて、アクセスキーのセキュアな格納をインペーブルにします。
—	タイムバウンドのS3アクセスキー	ユーザのS3アクセスキーを作成するときに、アクセスキーに有効期限の日時を設定できます。	グリッド管理者は、一時的なS3アクセスキーをプロビジョニングできます。
—	ユーザアカウントごとに複数のアクセスキー	StorageGRIDを使用すると、1つのユーザアカウントに対して複数のアクセスキーを作成し、同時にアクティブにすることができます。各APIアクションはテナントユーザアカウントとアクセスキーを使用してログに記録されるため、複数のキーがアクティブであっても拒否されません。	クライアントがアクセスキーを無停止でローテーションできるようにします。また、各クライアントに独自のキーを割り当てるため、クライアント間でのキー共有が不要になります。
—	S3 IAMアクセスポリシー	StorageGRIDはS3 IAMポリシーをサポートしているため、グリッド管理者はテナント、バケット、またはオブジェクトプレフィックスごとに詳細なアクセス制御を指定できます。StorageGRIDでは、IAMポリシーの条件と変数もサポートしているため、より動的なアクセス制御ポリシーを使用できます。	グリッド管理者がテナント全体に対してユーザグループ別にアクセス制御を指定できるようにします。また、テナントユーザが自身のバケットとオブジェクトに対してアクセス制御を指定できるようにします。

機能	機能	影響	コンプライアンス
—	S3 セキュリティトークンサービス API AssumeRole	StorageGRID は、S3 STS API AssumeRole をサポートし、権限の範囲が狭められ、有効期間が制限された一時的なセキュリティ認証情報 (アクセスキー ID、シークレットアクセスキー、セッショントークン) を提供します。セッション中に権限をさらに制限するINLINE セッションポリシーは、AssumeRole API の一部としてサポートされています。	テナント管理者がオブジェクトデータへの安全な一時アクセスを提供できるようにします。
—	シンプルな通知サービス	<p>StorageGRID は、オブジェクトアクセスに関する通知の送信をサポートしています。次のイベントタイプがサポートされています。</p> <ul style="list-style-type: none"> <li>• s3:オブジェクトが作成されました:</li> <li>• s3:オブジェクト作成:配置</li> <li>• s3:オブジェクト作成:投稿</li> <li>• s3:オブジェクト作成:コピー</li> <li>• s3:ObjectCreated:Complete MultipartUpload</li> <li>• s3:オブジェクトが削除されました:</li> <li>• s3:オブジェクトが削除されました:削除</li> <li>• s3:オブジェクトが削除されました:削除マーカーが作成されました</li> <li>• s3:オブジェクトの復元:投稿</li> </ul>	テナント管理者がオブジェクトへのアクセスを監視できるようにする
—	StorageGRIDで管理されるキー (SSE) によるサーバ側の暗号化	StorageGRIDはSSEをサポートしているため、StorageGRIDで管理される暗号化キーを使用して保管データをマルチテナントで保護できます。	テナントでオブジェクトを暗号化できます。これらのオブジェクトの書き込みと読み出しには暗号化キーが必要です。

機能	機能	影響	コンプライアンス
SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ル ール4511 (c)	ユーザ指定の暗号化キーによる サーバ側の暗号化 (SSE-C)	StorageGRIDはSSE-Cをサポー トしており、クライアントが管 理する暗号化キーを使用して保 管データをマルチテナントで保 護できます。  StorageGRIDはすべてのオブジ ェクトの暗号化および復号化処 理を管理しますが、SSE-Cを使 用する場合、クライアントは暗 号化キーを自身で管理する必 要があります。	クライアントが制御 するキーを使用して オブジェクトを暗号 化できます。これら のオブジェクトの書 き込みと読み出しに は暗号化キーが必 要です。

## オブジェクトとメタデータのセキュリティ

StorageGRIDのオブジェクトとメタデータのセキュリティ機能を確認します。

機能	機能	影響	コンプライアンス
Advanced Encryption Standard (AES) サーバ側オ ブジェクト暗号化	StorageGRIDは、AES 128お よびAES 256ベースのサーバ側オ ブジェクト暗号化を提供しま す。グリッド管理者は、暗号化 をグローバルなデフォルト設定 として有効にすることができます。 StorageGRIDはS3のx- amz-server-side-encryptionヘッ ダーもサポートしており、オブ ジェクト単位で暗号化を有効ま たは無効にできます。有効にす ると、グリッドノード間で格納 または転送中のオブジェクトが 暗号化されます。	基盤となるストレージハードウ エアに依存せずに、ストレージ やオブジェクトの転送を保護し ます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ル ール4511 (c)
組み込みのキー管理 機能	暗号化を有効にすると、各オブ ジェクトがランダムに生成され た一意の対称キーで暗号化さ れ、外部アクセスなし でStorageGRID内に格納されま す。	外部キー管理を必要とせずにオ ブジェクトを暗号化できます。	

機能	機能	影響	コンプライアンス
Federal Information Processing Standard (FIPS) 140-2準拠の暗号化ディスク	SG5812、SG5860、SG6160、およびSGF6024 StorageGRIDアプライアンスには、FIPS 140-2準拠の暗号化ディスクをオプションで選択できます。必要に応じて、外部KMIPサーバでディスクの暗号化キーを管理できます。	システムデータ、メタデータ、オブジェクトのセキュアなストレージを実現します。また、StorageGRIDソフトウェアベースのオブジェクト暗号化を提供し、オブジェクトのストレージと転送を保護します。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
ノード向け連邦情報処理規格 (FIPS) 140-3準拠の暗号化	SG5812、SG5860、SG6160、SGF6112、SG1100、およびSG110 StorageGRIDアプライアンスは、FIPS 140-3 準拠のノード暗号化オプションを提供します。ノードの暗号化キーは外部の KMIP サーバーによって管理されます。	システムデータ、メタデータ、オブジェクトのセキュアなストレージを実現します。また、StorageGRIDソフトウェアベースのオブジェクト暗号化を提供し、オブジェクトのストレージと転送を保護します。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
バックグラウンド整合性スキャンと自己回復	StorageGRIDでは、オブジェクトレベルとサブオブジェクトレベルでハッシュ、チェックサム、巡回冗長検査 (CRC) のインターロックメカニズムを使用して、オブジェクトが格納中と転送中の両方でデータの不整合、改ざん、変更から保護します。StorageGRIDは、破損したオブジェクトや改ざんされたオブジェクトを自動的に検出して置換し、変更されたデータを隔離して管理者に警告します。	グリッド管理者は、SLA、規制、データ保持に関するその他の義務を満たすことができます。データの暗号化、改ざん、変更を試みるランサムウェアやウイルスの検出を支援します。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
ポリシーベースのオブジェクトの配置と保持	StorageGRIDを使用すると、グリッド管理者はILMルールを設定して、オブジェクトの保持、配置、保護、移行、有効期限を指定できます。グリッド管理者はStorageGRID、メタデータでオブジェクトをフィルタリングし、グリッド全体、テナント、バケット、キープレフィックス、およびユーザ定義のメタデータのキーと値のペア。StorageGRIDを使用すると、クライアントによって明示的に削除されないかぎり、ライフサイクル全体を通じてオブジェクトがILMルールに従って格納されるようになります。	データの配置、保護、保持を徹底データ保持性、可用性、パフォーマンスに関するSLAの達成を支援	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)

機能	機能	影響	コンプライアンス
バックグラウンドメタデータスキヤン	StorageGRIDは、オブジェクトメタデータをバックグラウンドで定期的にスキヤンし、オブジェクトデータの配置または保護の変更をILMの指定に従って適用します。	破損したオブジェクトの検出に役立ちます。	
調整可能な整合性	テナントはバケットレベルで整合性レベルを選択して、マルチサイト接続などのリソースを利用できるようにすることができます。	必要な数のサイトまたはリソースが使用可能な場合にのみ、グリッドへの書き込みをコミットするオプションを提供します。	

## 管理セキュリティ機能

StorageGRIDの管理セキュリティ機能を確認します。

機能	機能	影響	コンプライアンス
サーバ証明書 (Grid管理インターフェイス)	グリッド管理者は、組織の信頼されたCAによって署名されたサーバ証明書を使用するようにグリッド管理インターフェイスを設定できます。	標準の信頼されたCAによって署名されたデジタル証明書を使用して、管理クライアントとグリッドの間の管理UIおよびAPIアクセスを認証できます。	—
管理ユーザ認証	管理ユーザは、ユーザ名とパスワードを使用して認証されます。管理ユーザと管理グループは、ローカルまたはフェデレーテッド、お客様のActive DirectoryまたはLDAPからインポートできます。ローカルアカウントパスワードはbcryptで保護された形式で保存され、コマンドラインパスワードはSHA-2で保護された形式で保存されます。	管理UIおよびAPIへの管理アクセスを認証します。	—

機能	機能	影響	コンプライアンス
SAMLノサホオト	StorageGRIDは、Security Assertion Markup Language 2.0 (SAML 2.0) 標準を使用したシングルサインオン (SSO) をサポートしています。SSO が有効な場合は、Grid Manager、Tenant Manager、Grid 管理 API、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。ローカルユーザは StorageGRID にサインインできません。	グリッド管理者やテナント管理者向けに、SSOや多要素認証 (MFA) などのセキュリティレベルを強化できます。	NIST SP800-63
権限のきめ細かな制御	グリッド管理者は、ロールに権限を割り当てたり、管理ユーザグループにロールを割り当てたりできます。これにより、管理クライアントが管理UIとAPIの両方を使用して実行できるタスクを適用できます。	Grid管理者が管理者ユーザと管理者グループのアクセス制御を管理できるようにします。	—

機能	機能	影響	コンプライアンス
分散監査ログ	<p>StorageGRIDは、組み込みの分散監査ログインフラを提供し、最大16のサイトにまたがる数百のノードに拡張できます。StorageGRIDソフトウェアノードは監査メッセージを生成します。このメッセージは冗長な監査リレーシステムを介して送信され、最終的に1つ以上の監査ログリポジトリにキャプチャされます。監査メッセージには、クライアントが開始したS3 API処理、ILM別のオブジェクトライフサイクルイベント、バックグラウンドのオブジェクト健全性チェック、管理UIまたはAPIからの設定変更など、オブジェクトレベルのきめ細かなイベントが記録されます。</p> <p>監査ログは syslog によってエクスポートできるため、Splunk や ELK などのツールで監査メッセージをマイニングできます。監査メッセージには次の 4 つの種類があります。</p> <ul style="list-style-type: none"> <li>・システム監査メッセージ</li> <li>・オブジェクトストレージ監査メッセージ</li> <li>・HTTPプロトコル監査メッセージ</li> <li>・管理監査メッセージ</li> </ul> <p>監査ログは、長期保存とアプリケーションアクセスのために S3 バケットに保存できます。</p>	<p>Grid管理者は、実績と拡張性に優れた監査サービスを利用して、さまざまな目的の監査データをマイニングできます。その目的には、トラブルシューティング、SLAパフォーマンスの監査、クライアントデータアクセスAPI処理、管理設定の変更などがあります。</p>	—
システム監査	システム監査メッセージには、グリッドノードの状態、破損オブジェクトの検出、ILMルールで指定されたすべての場所でコミットされたオブジェクト、システム全体のメンテナンススク (グリッドタスク) の進捗状況など、システム関連のイベントが記録されます。	システムの問題のトラブルシューティングを支援し、オブジェクトがSLAに従って格納されていることを証明します。SLAはStorageGRIDのILMルールによって実装され、整合性が保護されます。	—

機能	機能	影響	コンプライアンス
オブジェクトストレージの監査	オブジェクトストレージ監査メッセージには、オブジェクトAPIトランザクションとライフサイクル関連のイベントがキャプチャされます。これらのイベントには、オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。	システム内のデータの進捗状況と、StorageGRID ILMとして指定されたSLAが提供されているかどうかをお客様が監査できるようにします。	—
HTTPプロトコルの監査	HTTPプロトコル監査メッセージには、クライアントアプリケーションとStorageGRIDノードに関するHTTPプロトコルのやり取りがキャプチャされます。さらに、特定のHTTP要求ヘッダー（X-Forwarded-Forやユーザメタデータ[x-amz-meta-*]など）を監査に取り込むこともできます。	クライアントとStorageGRIDの間のデータアクセスAPI処理を監査し、個々のユーザーアカウントとアクセスキーまでのアクションをトレースできるようにします。ユーザメタデータを監査に記録し、SplunkやELKなどのログマイニングツールを使用してオブジェクトメタデータで検索することもできます。	—
管理監査	管理監査メッセージには、管理UI（Grid管理インターフェイス）またはAPIへの管理ユーザ要求が記録されます。APIに対するGETまたはHEAD以外のすべての要求は、応答に加えて要求のユーザ名、IP、およびタイプをログに記録します。	グリッド管理者は、どのユーザがどのソースIPから、どのデスティネーションIPから何時に行ったシステム設定変更の記録を作成できるようになります。	—
管理UIおよびAPIアクセスでのTLS 1.3のサポート	TLSは、管理クライアントとStorageGRID管理ノードの間の通信用にハンドシェイクプロトコルを確立します。	管理クライアントとStorageGRIDが相互に識別および認証し、機密性とデータ整合性を維持して通信できるようにします。	—

機能	機能	影響	コンプライアンス
SNMPv3によるStorageGRID監視	<p>SNMPv3は、プライバシーのために強力な認証とデータ暗号化の両方を提供することでセキュリティを提供します。v3では、プロトコルデータユニットは暗号化プロトコルにCBC-DESを使用して暗号化されます。</p> <p>プロトコルデータユニットを送信したユーザ認証は、HMAC-SHAまたはHMAC-MD5認証プロトコルによって提供されます。</p> <p>SNMPv2とv1は引き続きサポートされます。</p>	管理ノードでSNMPエージェントを有効にすることで、グリッド管理者がStorageGRIDシステムを監視できるようにします。	—
Prometheus指標エクスポート用のクライアント証明書	グリッド管理者は、クライアント証明書をアップロードまたは生成して、StorageGRID Prometheusデータベースへのセキュアな認証されたアクセスを提供できます。	グリッド管理者は、クライアント証明書を使用して、Grafanaなどのアプリケーションを使用してStorageGRIDを外部から監視できます。	—

## プラットフォームのセキュリティ機能

StorageGRIDのプラットフォームセキュリティ機能について説明します。

機能	機能	影響	コンプライアンス
内部公開鍵インフラ (PKI) 、ノード証明書、TLS	StorageGRIDは、内部PKIおよびノード証明書を使用して、ノード間通信を認証および暗号化します。ノード間通信はTLSで保護されます。	特にマルチサイト展開では、LANまたはWAN経由のシステムトラフィックの保護に役立ちます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
ノードのファイアウォール	StorageGRIDは、IPテーブルとファイアウォールルールを自動的に設定して、送受信ネットワークトラフィックを制御し、未使用のポートを閉じます。	StorageGRIDシステム、データ、メタデータを未承諾のネットワークトラフィックから保護します。	—
OSのセキュリティ強化	StorageGRID物理アプライアンスと仮想ノードのベースオペレーティングシステムが強化され、関連のないソフトウェアパッケージが削除されます。	潜在的な攻撃対象領域を最小限に抑えます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)

機能	機能	影響	コンプライアンス
プラットフォームとソフトウェアの定期的な更新	StorageGRIDでは、オペレーティングシステム、アプリケーションバイナリ、ソフトウェアアップデートなどのソフトウェアリリースを定期的に提供しています。	StorageGRIDシステムを最新のソフトウェアとアプリケーションバイナリで更新するのに役立ちます。	—
Secure Shell (SSH) を使用したルートログインの無効化	SSH経由のrootログインは、すべてのStorageGRIDノードで無効になっています。SSHアクセスでは証明書認証が使用されます。	rootログインの潜在的なリモートパスワードクラックからお客様を保護するのに役立ちます。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
自動時刻同期	StorageGRIDは、各ノードのシステムクロックを複数の外部タイムネットワークタイムプロトコル (NTP) サーバと自動的に同期します。Stratum 3以降のNTPサーバが少なくとも4台必要です。	すべてのノードで時刻参照が同じになるようにします。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
クライアント、管理者、内部のグリッドトラフィック用に別々のネットワークを使用	StorageGRIDソフトウェアノードとハードウェアアプライアンスは、複数の仮想ネットワークインターフェイスと物理ネットワークインターフェイスをサポートしているため、クライアントトラフィック、管理トラフィック、内部グリッドトラフィックを別々のネットワーク経由で分離できます。	グリッド管理者は、内部と外部のネットワークトラフィックを分離して、SLAの異なるネットワーク経由でトラフィックを配信できます。	—
複数の仮想LAN (VLAN) インターフェイス	StorageGRIDでは、StorageGRIDクライアントネットワークおよびグリッドネットワークにVLANインターフェイスを設定できます。	グリッド管理者はアプリケーショントラフィックをパーティショニングして分離し、セキュリティ、柔軟性、パフォーマンスを確保できます。	—
Untrusted Client Networkの略	信頼されていないクライアントネットワークインターフェイスは、ロードバランサエンドポイントとして明示的に設定されたポートでのみインバウンド接続を受け入れます。	信頼されていないネットワークに公開されているインターフェイスのセキュリティが確保されます。	—

機能	機能	影響	コンプライアンス
設定可能なファイアウォール	管理、グリッド、クライアントの各ネットワークの開いているポートと閉じているポートを管理します。	グリッド管理者がポートでのアクセスを制御し、ポートへの承認済みデバイスアクセスを管理できるようにします。	
SSH動作の強化	インストール前にデフォルトで SSH を無効にします。デフォルト状態では、SSH アクセスはリンクローカル管理ポート アドレスでのみ有効になります。管理者およびルート ユーザーのパスワードは、アプライアンスのコンピューティング コントローラーのシリアル番号に設定されます。ログインはシリアル コンソールとグラフィカル コンソール (BMC KVM) でのみ許可されます。すべてのネットワーク ポート上の SSH が無効になっています。	ネットワーク アクセス保護を強化します。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)
ノード暗号化	新しいKMSホストサーバ暗号化機能の一部として、StorageGRIDアプライアンスインストーラに新しいノード暗号化設定が追加されます。	この設定は、アプライアンスの設置のハードウェア構成段階で有効にする必要があります。	SECルール17a-4 (f) CTFC 1.31 (c) - (d) (FINRA) ルール4511 (c)

## クラウドとの統合

StorageGRIDとクラウドサービスの統合方法をご紹介します。

機能	機能	影響
通知ベースのウィルススキャン	StorageGRIDプラットフォームサービスでは、イベント通知がサポートされます。外部のクラウドコンピューティングサービスでイベント通知を使用すると、データに対してウィルススキャンワークフローをトリガーできます。	テナント管理者は、外部のクラウドコンピューティングサービスを使用してデータのウィルススキャンをトリガーできます。

## 著作権に関する情報

Copyright © 2025 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隨時、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 5225.227-19（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権を有し、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権については、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。