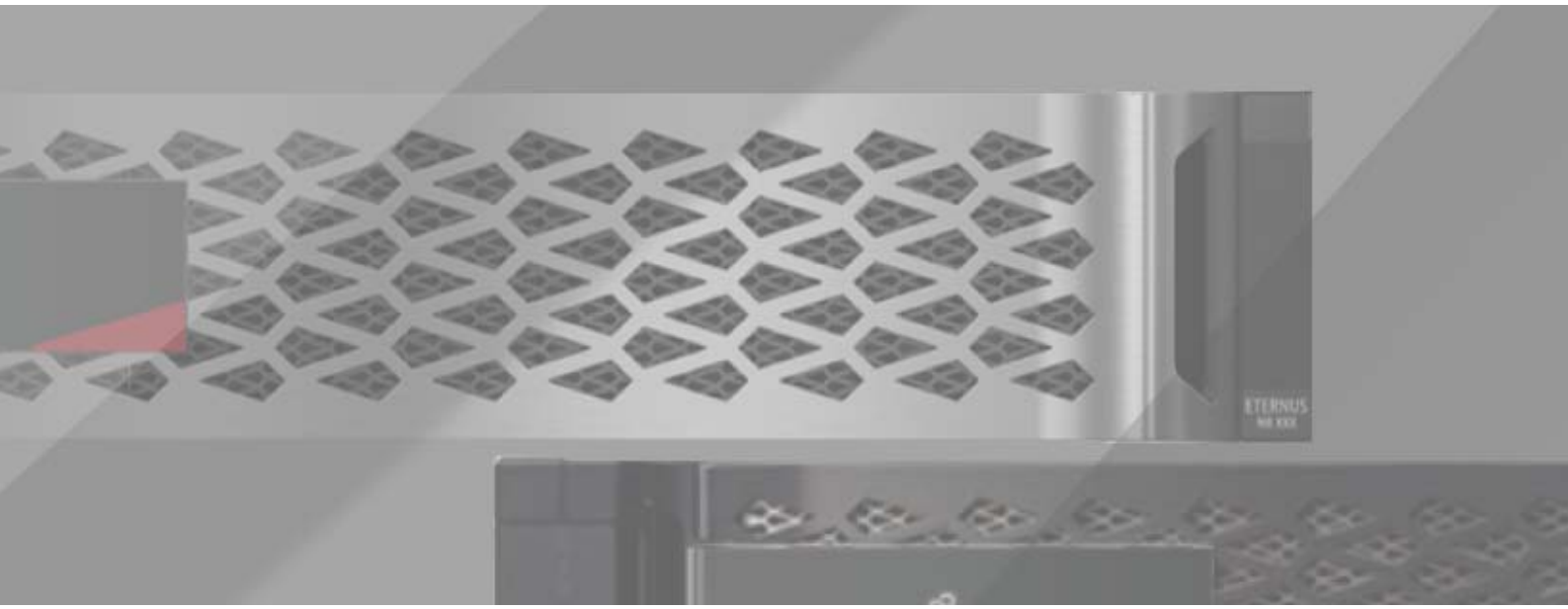
P3AG-5762-02Z0

Fujitsu Storage
ETERNUS AB series オールフラッシュアレイ，
ETERNUS HB series ハイブリッドアレイ

SANtricity ドライブのセキュリティ
SANtricity 11.70 を使用した機能の詳細



FUJITSU

目次

図目次

表目次

はじめに

フルディスク暗号化機能により、ETERNUS AB/HB series の保存データの暗号化を提供します。本書では、FIPS 140-2 有効化ドライブのサポート、内部および外部の鍵管理サポートを含む、ETERNUS AB/HB series システム向けの SANtricity のフルディスク暗号化機能に関する詳細情報を提供します。

第 2 版
2022 年 12 月

登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/

本書では、本文中の ™、® などの記号は省略しています。

本書の読み方

対象読者

本書は、ETERNUS AB/HB の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

関連マニュアル

ETERNUS AB/HB に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

本書の表記について

■ 本文中の記号

本文中では、以下の記号を使用しています。

注 意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備 考	本文を補足する内容や、参考情報を記述しています。

第 1 章
ソリューションの概要

企業のデータは、おそらく最も貴重な資産です。データセキュリティ攻撃の増加に伴い、組織のデータを紛失や盗難から保護することがますます重要になっています。SANtricity フルディスク暗号化技術は、システムのパフォーマンスや使いやすさを損なうことなく、保存されているデータの包括的なセキュリティとともに、内部および外部鍵管理機能を提供します。本書に記載しているセキュリティ機能は、ETERNUS AB2100/AB3100/AB5100/AB6100 および ETERNUS HB2000/HB5100/HB5200 でサポートしています。

1.1 SANtricity フルディスク暗号化の使用例

SANtricity フルディスク暗号化は、主に物理的セキュリティ違反が発生した場合にデータを保護します。

ストレージアレイ全体を入手した人物によるデータへの不正アクセスを防止するために、別のレベルの保護を追加して輸送中のストレージアレイへの脅威に対応しています。本機能は、サードパーティ製の鍵管理ソリューションを導入し、外部鍵管理機能を一元化することで実現しています。ただし、データセンターそのものへの不正侵入があった場合は、不正アクセスからデータを守ることができません。

SANtricity フルディスク暗号化は、2 つの主な使用例に対応します。

- システム全体が不正アクセスされた同じストレージアレイが使われた場合、認証済みのドライブがウイルスに汚染された別のストレージアレイが使われた場合、あるいはスタンドアロンツールが使われた場合でも、正式なセキュリティ認証情報がないデータへの不正アクセスを防止します。
- データのセキュリティを維持しながら、コントローラーをアップグレードしたり、ストレージアレイ間で一連のドライブを適正に移動したりできます。

このレポートの情報を使用して、富士通のサポートとパートナーは、ETERNUS AB/HB ソリューションがお客様のセキュリティ要件を満たしていることを確認できます。これらの要件は、以下の機関を含む市場によって異なる場合があります。

- 米国および日本の公的機関
- 金融
- 医療
- 小売業

ETERNUS AB3100/AB6100 は、NVMe 自己暗号化ドライブおよび FIPS ドライブをサポートしています。これらのドライブは、SAS 自己暗号化ドライブまたは FIPS ドライブで使用されている TCG Enterprise 規格のかわりに、TCG Opal 規格に準拠しています。セキュリティ機能に関しては、ドライブの規格が異なっていても、SANtricity OS は使用の差異を感じさせることなく実行します。

1.2　SANtricity ドライブセキュリティ

ETERNUS AB/HB series は、自己暗号化ドライブを使用して、保存データを暗号化します。これらのドライブは、フルディスク暗号化機能が有効かどうかに関係なく、書き込み操作ではデータを暗号化し、読み取り操作ではデータを復号化します。SANtricity 機能が有効になっていない場合、データはメディア上で暗号化されますが、読み取り要求時には自動的に復号化されます。

ストレージアレイでドライブセキュリティ機能が有効になっている場合、ストレージアレイが正しいセキュリティキーまたは認証キーを提供しない限り、ドライブは読み取りまたは書き込み操作からドライブをロックすることによって、保存されているデータを保護します。この処理によって、あらかじめドライブのロックを解除する正規のセキュリティキーファイルをインポートしていない別のストレージアレイがデータにアクセスするのを防ぎます。同時に、サードパーティ製のツールが各ドライブのデータにアクセスすることも防止します。

このような内部鍵管理機能に加えて、SANtricity 11.60 以降ではさらにドライブセキュリティの拡張機能を提供します。これらの追加拡張機能によって、Key Management Interoperability Protocol (KMIP) に準拠した Fujitsu Security Key Lifecycle Manager 4.1 以降または IBM Storage ETERNUS SF KM 4.1 などの外部鍵管理機能を一元化するシステムを使用した、完全なディスク暗号化セキュリティ鍵を管理できるようになります。基本要件は KMIP 1.0 への準拠です。

ドライブ内のハードウェアによって実行される暗号化および復号化操作は、ユーザーには見えず、パフォーマンスやユーザーのワークフローには影響しません。各ドライブには固有の暗号化キーがあり、ドライブからの転送、コピー、または読み取りはできません。暗号化キーは、National Institute of Standards and Technology (NIST) AES で指定されている 256 ビットキーです。ドライブの一部だけでなく、ドライブ全体が暗号化されます。

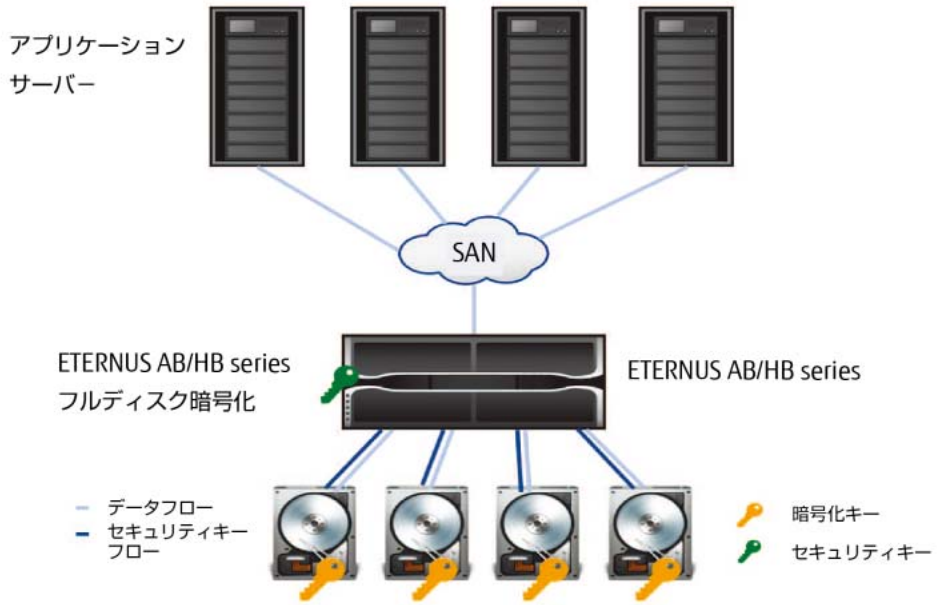
「Volume Group」メニューまたは「Disk Pool」メニューで「Secure Drives」オプションを選択することにより、セキュリティをいつでも有効にできます。このオプションは、ボリュームグループまたはプールの作成時、または作成後に設定できます。「Secure Drives」を選択しても、ドライブの既存データには影響ありません。

注 意

このオプションを無効にするには、影響を受けるボリュームグループまたはプールのすべてのデータを消去する必要があります。

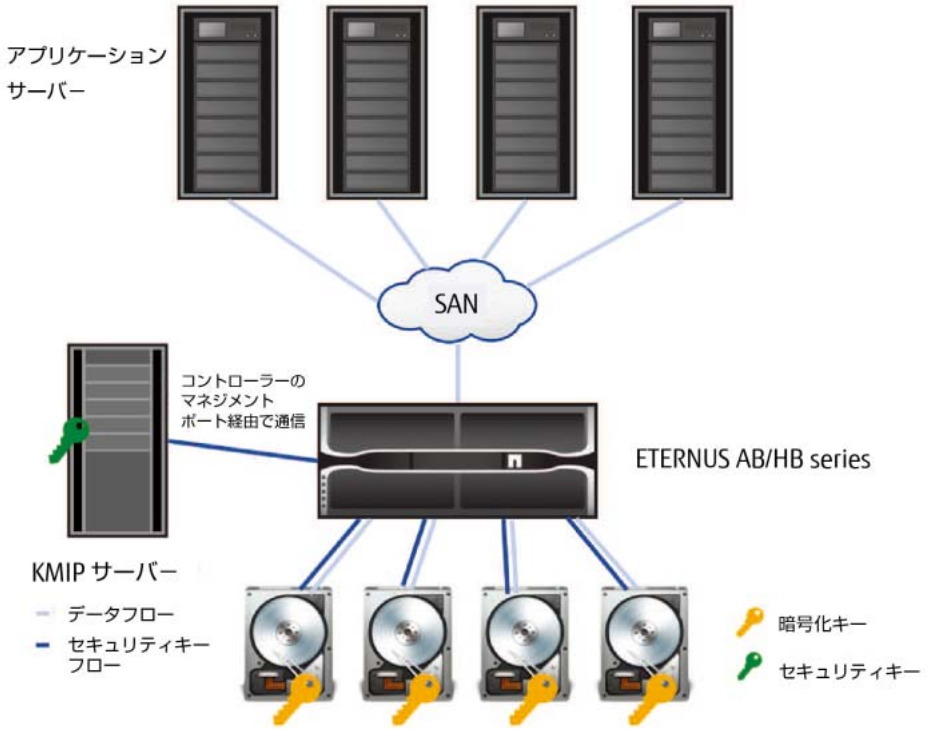
ETERNUS AB/HB のフルディスク暗号化機能の技術コンポーネントと、内部で管理されるセキュリティキーを図 1.1 に示します。

図 1.1　内部で管理されているセキュリティキーを使用した ETERNUS AB/HB フルディスク暗号化



ETERNUS AB/HB のフルディスク暗号化機能と外部で管理されるセキュリティキーの技術コンポーネントを図 1.2 に示します。

図 1.2　外部で管理されているセキュリティキーを使用した ETERNUS AB/HB フルディスク暗号化



第 2 章
セキュリティキー認証

ETERNUS AB/HB series のフルディスク暗号化機能が有効な場合は、ストレージアレイのセキュリティキーを作成する必要があります。ストレージアレイごとに 1 つのセキュリティキーがあり、保護が有効なすべてのボリュームグループまたはプールを保護するために使用されます。このセキュリティキーは、保護が有効なドライブのロックを解除して読み書き操作ができるようにします。

ボリュームグループまたはプール内フルディスク暗号化セキュリティを部分的に使用することはありません。セキュリティ機能を使用するには、ボリュームグループまたはプール内のすべてのドライブがセキュリティに対応している必要があります。保護が有効に設定されたボリュームグループまたはプールから構成されたすべてのボリュームが保護されます。

ETERNUS AB/HB series は、内部鍵管理または外部鍵管理を使用してセキュリティキーを管理します。内部鍵管理では、ストレージアレイ上でセキュリティキーが維持されます。外部鍵管理では、セキュリティキーは外部 KMIP サーバーで管理されます。どちらの方法でも、セキュリティキーをバックアップする必要があります。バックアップキーは、ユーザーが指定したパスフレーズでラップされ、AES-128 を使用して暗号化されます。バックアップファイルの保存場所を指定できます。バックアップファイルには、暗号化されたセキュリティキーのコピーが 2 つ含まれています。バックアップセキュリティキーは、SANtricity System Manager ソフトウェアまたは CLI で検証できます。この検証プロセスでは、バックアップキーがアンラップ可能であり、ストレージアレイまたは KMIP サーバーに格納されているセキュリティキーと一致することを確認します。検証プロセスでは、バックアップセキュリティキーファイルの作成に使用したものと同じパスフレーズを入力する必要があります。

セキュリティキーに加えて、セキュリティキー識別子が作成され、セキュリティキーが変更されるたびに変更されます。セキュリティキー識別子を使うと、実際のセキュリティキーを知らないユーザーでも特定のストレージアレイのセキュリティキーを識別できます。識別子は最大 255 バイトの文字列で、内部鍵管理用にユーザー定義値に設定されるか、外部鍵管理用にコントローラーによって自動的に生成されます。セキュリティキーとは異なり、セキュリティキー識別子は人間が読み取るように設計されています。セキュリティキー識別子は、コントローラーおよびそのセキュリティキーに関連付けられたすべてのドライブに格納され、セキュリティキーとともにバックアップされます。

別の ETERNUS AB/HB series にドライブをインポートすると、関連付けられたセキュリティキーがインポートされるまでは新しいストレージアレイで書き込みまたは読み取り操作が許可されません。セキュリティキーのインポート時は、新しいストレージアレイがインポートされたセキュリティキーのセキュリティキー ID とインポートされたドライブのセキュリティキーのセキュリティキー ID を比較します。両方のストレージアレイが一元的な外部鍵管理システム（同じ KMIP サーバーなど）を使用している場合は、セキュリティキーを手動でインポートする必要はありません。新しいストレージアレイは、インポートされたドライブのロックを解除するためのキーを KMIP サーバーから自動的に取得します。インポートされたドライブのロックが解除されると、新しいストレージアレイのセキュリティキーにキーが再設定されます。

ストレージアレイのセキュリティキーは、基礎となるユーザーデータに影響を与えることなく、いつでも変更できます。内部鍵管理を使用したキー更新操作中の中断を防止するため、新しいキーが生成されてすべての保護されたドライブに適用されるまで、古いキーはストレージアレイから削除されません。外部鍵管理システムを使用する場合、新旧のキーは常に KMIP サーバーで管理され、ストレージアレイに永続的に保存されることはありません。

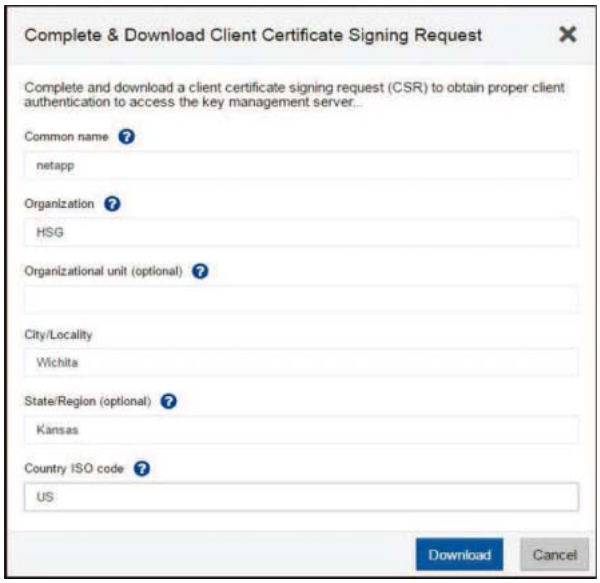
第 3 章
外部 KMIP サーバー認証

外部鍵管理システムは、データが存在するストレージアレイからセキュリティキーを切り離すことによって、セキュリティ層を強化します。しかし、セキュリティ層を追加するためには、暗号管理ハードウェアまたは暗号管理ソフトウェアを購入するため追加コストが発生します。また、ストレージアレイと KMIP サーバーの両方を適切な証明書のセットで構成し、KMIP サーバーが要求を認証して受け入れるようにする手順も必要です。

リクエストを認証するようにストレージアレイと KMIP サーバーを設定するには、以下の手順を実施します。

手順 ▶▶▶

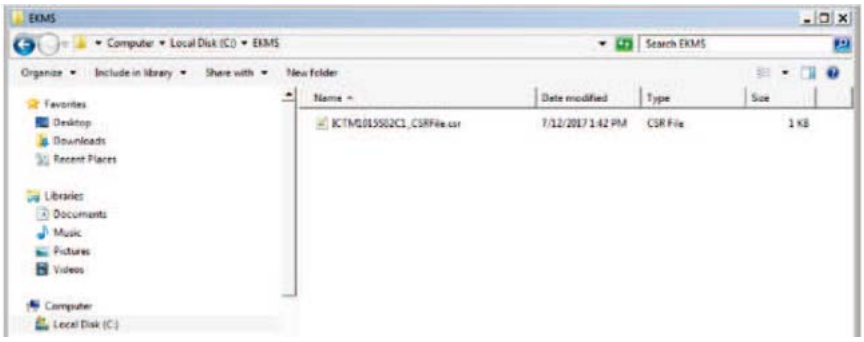
1. CLI または SANtricity System Manager から証明書署名要求 (CSR) を開き、適切な Secure Sockets Layer(SSL) 識別名 (DN)、ビジネス名、およびロケーション情報を入力します。

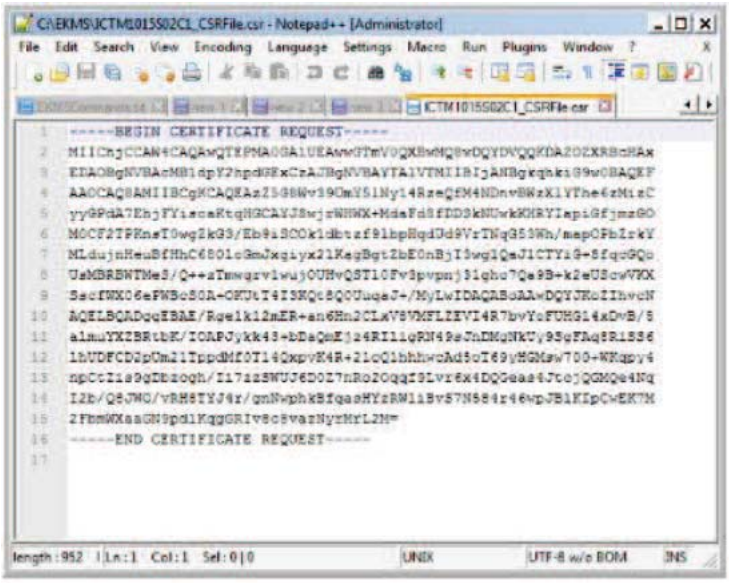


注 意

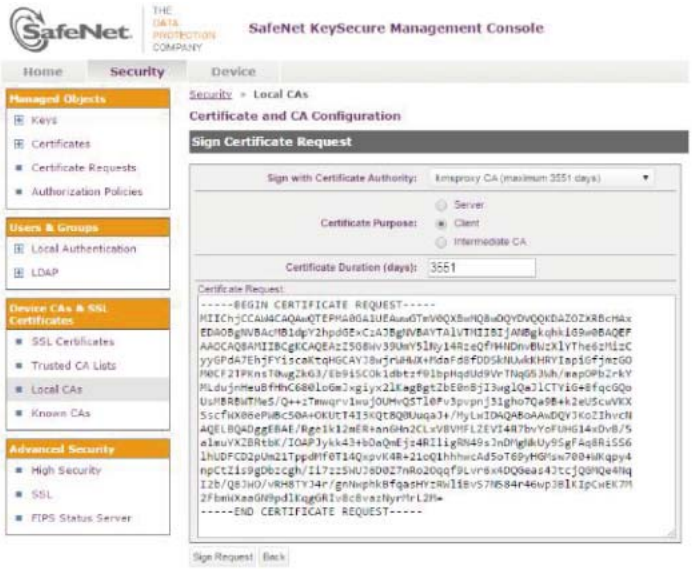
証明書署名要求 (CSR) を作成するためには、CSR 上のコモンネームを、鍵管理サーバー上に作成したユーザー名の一つと一致させる必要があります。

ETERNUS AB/HB series 上の OpenSSL ライブラリは、秘密鍵と公開鍵を生成します。CSR は、生成された公開鍵とユーザー提供の DN を使用して作成されます。



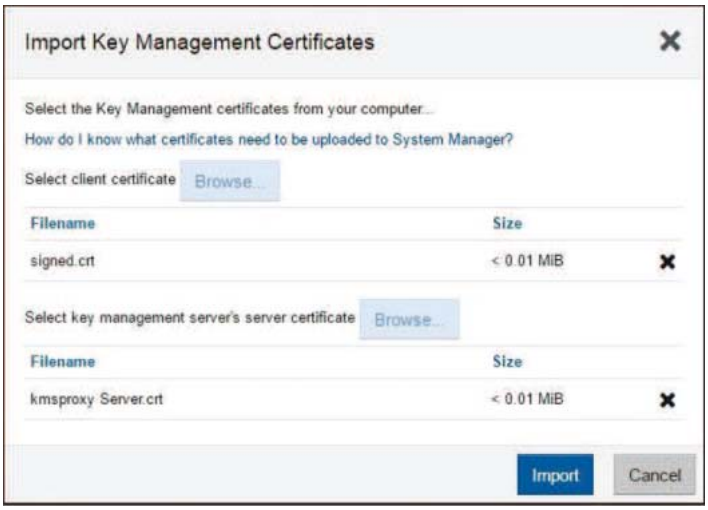


2　`.csr` ファイルの内容をコピーして (上図参照) 認証局 (CA) のユーティリティにペーストし、CSR を CA に提出して、CA の署名済みクライアント証明書ファイルを生成します (下図参照)。



署名済みのクライアント証明書ファイルが生成されます。

3 署名済みのクライアント証明書ファイルと鍵管理サーバーのサーバー証明書をインストールします。



使用可能な KMPI サーバーの署名済みサーバー証明書がない場合は、次の手順を実行します。

a　KMIP サーバーに CSR の作成と署名済みサーバー証明書ファイルの生成を要求します。

b　ETERNUS AB/HB series 上の KMIP サーバーから、署名済みサーバー証明書ファイルをダウンロードしてインストールします。

4 すべての証明書をインストールしたら、ETERNUS AB/HB series がセキュリティ有効なドライブの新しいセキュリティキーを要求する際に使用する外部鍵管理を有効にします。

第 4 章
FIPS 140-2 Level 2 に準拠

第三機関の認証が政府機関や企業のお客様の基本的なビジネス要件となっている中、フルディスク暗号化機能に米国標準技術局 (NIST) が開発した FIPS 140-2 基準に準拠したドライブを使用して、より高いレベルの保証を提供します。ドライブは FIPS 140-2 Level 2 に準拠しており、改ざん防止ドライブやそのほかの承認済みプロトコルを使用した追加のセキュリティ保護層を備えています。FIPS 140-2 ドライブを使用する場合でも、セキュリティキーの作成と認証のプロセスは変わりません。セキュリティが確保されたドライブは、FIPS 140-2 Level 2 暗号化ドライブまたはフルディスク暗号化ドライブ (FDE) として認識されます。使用する暗号化モジュールに違いはないものの、FDE に指定されたドライブは NIST で認証されていません。FIPS 140-2 Level 2 を完全にサポートするためには、FIPS 140-2 検証済みの暗号化モジュールを搭載した、外部鍵管理サーバーが必要です。これにより、SANtricity OS 11.60 以降が動作する ETERNUS AB/HB series (ETERNUS AB2100/AB3100/AB5100/AB6100 および ETERNUS HB2000/HB5100/HB5200 など) で、FIPS 140-2 検証済みのセキュアドライブの安全な外部鍵管理が可能になります。

4.1 FIPS 140-2 Level 2 準拠モードでの動作

FIPS 140-2 検証済みドライブが ETERNUS AB/HB series にインストールされると、特定のドライブモデルの FIPS 140-2 セキュリティポリシーに従って初期化プロセスが実行されます。初期化プロセスの後、SANtricity UI は FIPS 準拠として FIPS ドライブを識別します。ストレージアレイがハードウェアの最新バージョンにアップグレードされ、ボリュームグループまたはプールが FIPS 140-2 検証済みドライブのみで構成されている場合、ドライブは FIPS 140-2 準拠モードになるように初期化されます。

第 5 章
安全なドライブ操作

標準ボリュームグループ (RAID) またはプールは、暗号化機能などの特定のサービス品質 (QoS) 規則に従う必要があるドライブをグループ化したものです。安全性が確保されていないボリュームグループまたはディスクプールはセキュリティ対応ドライブとセキュリティ非対応ドライブを混在して作成できますが、安全性が確保されたボリュームグループまたはディスクプールはセキュリティ対応ドライブだけで構成する必要があります。セキュリティ対応のボリュームグループまたはプールでセキュリティを有効にすると、そのドライブグループはセキュリティ有効になります。これらのセキュリティが有効なボリュームグループまたはディスクプールに作成されたボリュームはいずれもセキュアになります。ETERNUS AB/HB series は、セキュリティ有効、セキュリティ対応、セキュリティ非対応のボリュームグループまたはプールの混在を許容します。

ストレージアレイ間でデータを保持したまま、セキュリティが有効なボリュームグループを移動するには、次の手順に従います。

(1)ソースシステムからボリュームグループをエクスポートします。

(2)ボリュームグループを対象のストレージアレイにインポートします。

(3)内部鍵管理の場合、または対象のストレージアレイの KMIP サーバーにセキュリティキーがない場合は、バックアップ済みのセキュリティキーのコピーを適用して、インポートしたドライブのロックを解除します。

両方のストレージアレイが一元的な外部鍵管理システム (同じ KMIP サーバーなど) を使用している場合は、バックアップ済みのセキュリティキーを手動でインポートする必要はありません。新しいストレージアレイは、インポートされたドライブのロックを解除するために、KMIP サーバーから自動的にセキュリティキーを取得します。

注 意

ETERNUS AB/HB series では、ストレージアレイ間でのプールに関連づけられたドライブの移動はサポートされていません。

ストレージアレイは、さまざまな機能での使用方法を含め、安全なドライブと FIPS ドライブの使用に関する構成ルールを適用します。たとえば、ドライブは再プロビジョニングすることで安全に消去できます。この機能は、個々のドライブの暗号化キーのキー更新のトリガーとなり、以前のデータをすべて読み取り不能にします。各トピックに関連付けられているルールの詳細については、次のセクションを参照してください。

5.1　ボリュームグループとディスクプールの構成

ボリュームグループまたはプールは、セキュリティに対応しているとみなされるフルディスク暗号化および FIPS 140-2 準拠ドライブ上のセキュリティ非対応ドライブと、セキュリティ対応ドライブを混在して構成できます。ボリュームグループまたはディスクプールのセキュリティを確保したい場合は、ボリュームグループまたはディスクプールを構成するドライブをセキュリティ対応ドライブ（フルディスク暗号化または FIPS 140-2 準拠のドライブ）にする必要があります。FIPS 140-2 準拠のボリュームグループまたはプールが必要な場合は、すべての構成ドライブが FIPS 140-2 準拠である必要があります。グローバルホットスペアを使用する場合は、少なくともボリュームグループと同じ安全性が必要です。表 5.1 に、構成ルールを示します。

表 5.1　ボリュームグループとディスクプールの構成ルール

ドライブタイプ	FIPSセキュリティ有効またはFIPSセキュリティ対応のボリュームグループまたはディスクプール	フルディスク暗号化セキュリティ有効のボリュームグループまたはディスクプール	フルディスク暗号化セキュリティ対応のボリュームグループまたはディスクプール	セキュリティ非対応のボリュームグループまたはディスクプール
FIPS	はい (*1)	はい (*2)	はい	はい
フルディスク暗号化	いいえ	はい	はい	はい
セキュリティ非対応	いいえ	いいえ	はい (*3)	はい

*1: ボリュームグループまたはディスクプールは、すべてのドライブが FIPS に準拠している場合にのみ、FIPS 有効または FIPS 対応にすることができます。

*2: 個別の FIPS ドライブがフルディスク暗号化セキュリティが有効なボリュームグループまたはディスクプールで使用されている場合、そのドライブは FIPS 準拠モードになりますが、ボリュームグループまたはプールは FIPS 準拠とは見なされません。

*3: ボリュームグループまたはプールが、セキュリティ対応ドライブとセキュリティ非対応ドライブの混在で構成されている場合、セキュリティ非対応ドライブをセキュリティ対応ドライブに交換するまで、セキュリティを有効にすることはできません。

5.2　グローバルホットスペアの互換性

表 5.2 に、標準の RAID 構成でグローバルホットスペアドライブを使用するための要件を示します。

注 意

- セキュリティ対応ドライブだけでボリュームグループを作成した場合、ボリュームグループのセキュリティが有効になっていない場合でも、スペアまたは交換ドライブはセキュリティに対応している必要があります。
- プールはスペアドライブを使用しませんが、表 5.2 に記載したルールが故障ドライブの交換時に適用されます。

表 5.2　グローバルホットスペアの互換性ルール

ドライブタイプ	FIPSセキュリティ有効またはFIPSセキュリティ対応のボリュームグループ	フルディスク暗号化セキュリティが有効なボリュームグループ	フルディスク暗号化セキュリティ対応のボリュームグループ	セキュリティ非対応のボリュームグループ
FIPS	はい	はい (*1)	はい (*1)	はい (*1)
フルディスク暗号化	いいえ	はい	はい	はい (*2)
セキュリティ非対応	いいえ	いいえ	はい (*3)	はい

*1:　FIPS 140-2 準拠のドライブは、ほかのオプションがない場合にのみ使用されます。

*2:　セキュリティ対応ドライブとセキュリティ非対応ドライブの両方が使用可能な場合は、セキュリティ非対応ドライブが選択されます。

*3:　セキュリティ対応ドライブとセキュリティ非対応ドライブの両方が使用可能な場合は、セキュリティ対応ドライブが選択されます。セキュリティ非対応ドライブが使用されている場合、そのボリュームグループは、セキュリティ対応ドライブと交換するまで安全性が確保されないことがあります。これにより、ボリュームグループが同種のセキュリティ対応状態にリストアされます。

5.3　安全な消去とディスク消去

前述のように、ドライブの安全な消去 (再プロビジョニング) は、安全なドライブと FIPS 準拠のドライブの両方で実行できます。SANtricity OS 11.70.1 以降、セキュリティ非対応ドライブでもデータ消去オプションが使用可能です。SANtricity System Manager の「Hardware」と「Drives」で選択された全ての消去オプションが確認できます。

構成済みのボリュームグループまたはプールに組み込まれたドライブは消去できません。SANtricity System Manager では、「Storage and Pools & Volume Groups」を選択することでボリュームグループとプールの消去オプションを確認できます。

セキュリティ対応ドライブの消去により、個々のドライブの暗号化キーのキー更新が行われ、以前のすべてのデータが読み取り不能になります。SAS ドライブの場合、安全なドライブと FIPS ドライブの両方が同じプロセスを使用して再プロビジョニングされます。ただし、ドライブのセキュリティキーが FIPS ドライブで使用できない場合、関連する FIPS ドライブを安全に消去するためには CLI コマンドを実行する物理的なセキュア ID (PSID) が必要です。PSID はドライブのラベルに記載された判読可能な文字列であり、SANtricity 管理ソフトウェアまたは SANtricity CLI に手動で入力する必要があります。

ETERNUS AB3100/AB6100 の基本コントローラーエンクロージャには、NVMe ドライブが使用されています。セキュリティ対応のドライブと FIPS NVMe ドライブでドライブのセキュリティキーが使用できない場合、ドライブの再プロビジョニングにはPSIDの入力が必要です。CLIコマンドまたはSANtricity System Manager GUI のいずれかを使用してこの操作を実行できます。

ドライブの消去後、ストレージアレイで再利用する際は事前にドライブの初期化が必要です。SANtricity System Manager で初期化を実行する場合は、ドライブのコンテキストメニューで「Initialize」を選択してください。

図 5.1　SANtricity System Manager GUI でのドライブのリセット / プロビジョニング手順

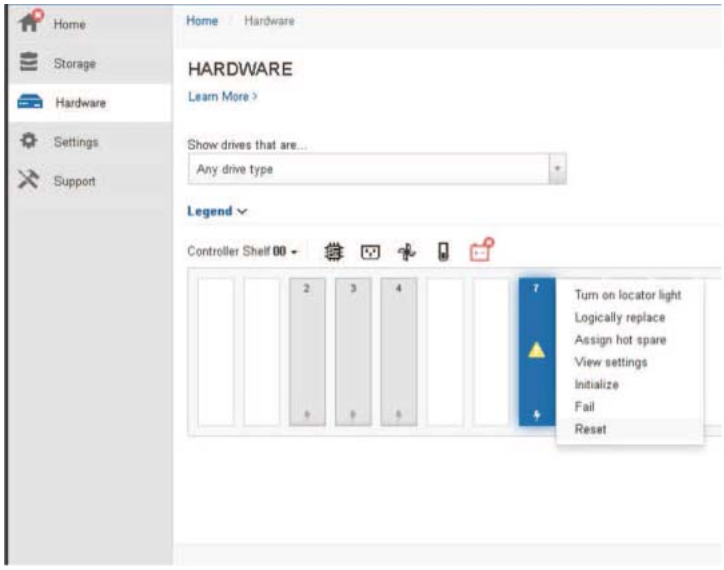
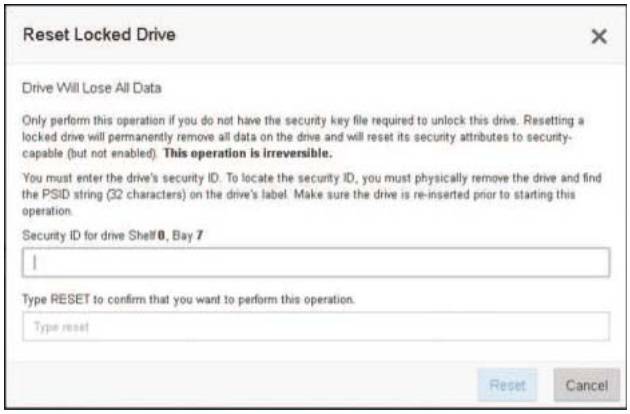


図 5.2　SANtricity System Manager GUI の「Reset Locked Drive」ダイアログボックス



第 6 章
機能の相互作用

このセクションでは、一覧表示された機能に関連する、ドライブセキュリティに関連する規則について説明します。

6.1 ボリュームコピー

ボリュームコピー機能に制限はありません。コピー操作のソースとターゲットのセキュリティ機能を任意に組み合わせて選択できます。ただし、高いセキュリティボリュームから低いセキュリティボリュームにコピーすると、SANtricity System Manager は警告を生成します。

6.2 Snapshot イメージ

リザーブした Snapshot コピーリポジトリは、Snapshot コピーの作成元のボリュームと同じ安全性が必要です。

6.3 同期ミラーリング

同期ミラーリング機能に制限はありません。プライマリボリュームとセカンダリボリュームのセキュリティ機能を任意に組み合わせて選択できます。ベストプラクティスとしてセキュリティ機能が一致したボリュームを選択することを推奨しています。

注 意

同期ミラーリングは、ETERNUS AB3100/AB6100 ではサポートされていません。

6.4　非同期ミラーリング

ミラーリポジトリは、ミラー化されるボリュームと同じセキュリティである必要があります。表 6.1 に、プライマリボリュームとセカンダリボリュームの QoS の制限を示します。

表 6.1　非同期ミラーリングの構成ルール

プライマリミラーのセキュリティ状態	セカンダリミラーのセキュリティ状態
セキュリティ非対応	セキュリティ非対応 (*1)
フルディスク暗号化セキュリティ対応 (*4)	フルディスク暗号化または FIPS セキュリティ対応 (*2)、 フルディスク暗号化または FIPS セキュリティ有効
フルディスク暗号化セキュリティ有効	フルディスク暗号化または FIPS セキュリティ有効
FIPS セキュリティ対応 (*4)	フルディスク暗号化または FIPS セキュリティ対応、 フルディスク暗号化または FIPS セキュリティ有効
FIPS セキュリティ有効	フルディスク暗号化または FIPS セキュリティ有効 (*3)

*1:　役割の反転の結果、互換性のない修正不可能な構成になるため、セカンダリボリュームはセキュリティに対応しません (新しいセカンダリボリュームを保護できません)。

*2:　役割が反転すると、構成に互換性がなくなります。これを修正するには、新しいセカンダリボリュームでセキュリティを有効にします。この状態になるとシステムが警告を出します。

*3:　役割を反転させると、プライマリボリュームのセキュリティレベル（フルディスク暗号化による保護が有効）がセカンダリボリュームのセキュリティレベル（FIPS セキュリティ有効）より低くなります。これに対するユーザーの対処は不要であり、システムも警告を出しません。ベストプラクティスは、FIPS セキュリティ対応ドライブからプライマリボリュームとセカンダリボリュームの両方を作成することです。

*4:　プライマリのセキュリティを有効にすると、構成に互換性がなくなります。これを修正するには、セカンダリボリュームのセキュリティを有効にします。この状態になるとシステムが警告を出します。

注 意

非同期ミラーリングは、ETERNUS AB3100/AB6100 ではサポートされていません。

6.5　SSD リードキャッシュ

SSD リードキャッシュは、作成時にのみセキュリティを有効にできます。内蔵 HDD ボリュームは、SSD リードキャッシュがすでに有効になっている場合に限り、いつでもセキュリティを有効にすることができます。表 6.2 に、構成ルールを示します。

表 6.2　SSD リードキャッシュの構成ルール

SSDリードキャッシュ	セキュリティ非対応のHDDボリューム	フルディスク暗号化セキュリティに対応したHDDボリューム	フルディスク暗号化セキュリティが有効なHDDボリューム	FIPSセキュリティに対応したHDDボリューム	FIPSセキュリティが有効なHDDボリューム
セキュリティ非対応のSSDキャッシュ	はい	いいえ	いいえ	いいえ	いいえ
フルディスク暗号化セキュリティに対応したSSDキャッシュ	はい	はい	いいえ	はい (*1)	いいえ
フルディスク暗号化セキュリティが有効なSSDキャッシュ	はい	はい	はい	はい	はい (*2)
FIPSセキュリティに対応したSSDキャッシュ	はい	はい	いいえ	はい	いいえ
FIPSセキュリティが有効なSSDキャッシュ	はい	はい	はい	はい	はい

*1:　SSD リードキャッシュの潜在的なセキュリティが HDD ボリュームよりも低いというメッセージが表示されます。
*2:　SSD リードキャッシュの有効セキュリティが HDD ボリュームよりも低いというメッセージが表示されます。

注 意

SSD キャッシュは、ETERNUS AB3100/AB6100 ではサポートされていません。

第 7 章
よくある質問

次に、SANtricity ドライブのセキュリティ機能のルールと機能に関する一般的な質問を示します。

■ ストレージアレイと外部鍵管理サーバーの認証方法を教えてください。

回答：
外部鍵管理機能を有効にする場合、ストレージアレイに一連の証明書をインストールする必要があります。これらの証明書は、ストレージアレイと鍵管理サーバー間の安全な接続を確立するために使用されます。SANtricity System Manager は、管理者が証明書署名要求 (CSR) を生成し、署名済みのクライアント証明書および KMIP サーバー Secure Sockets Layer (SSL) 証明書をインストールするプロセスを実行するためのインターフェースを提供します。このプロセスは CLI から実行できます。

■ バックアップセキュリティキーファイルとパスフレーズはいつ必要ですか。

回答：
バックアップセキュリティキーファイルは、ユーザーが指定したパスフレーズを使用して作成され、安全にラップされます。バックアップセキュリティキーファイルは、新しいロックキーが作成されるたびに作成されます。以下の状況では、ロックされたドライブのロックを解除するために、バックアップセキュリティキーファイルとパスフレーズが必要です。

- ストレージアレイの電源が再投入され、キーの KMIP サーバーにアクセスできない場合。
- 保護されたドライブからボリュームグループをインポートする場合。
- ストレージアレイ内のすべてのドライブが保護されているデュアルコントローラーを交換する場合。

■ IPv6 アドレス指定は、ストレージアレイと KMIP サーバー間の通信でサポートされていますか。

回答：
はい。外部鍵管理サーバーがサポートしていれば IPv6 アドレス指定がサポートされます。

■ 1 つのストレージアレイに、保護されたドライブと保護されていないドライブを混在させることはできますか。

回答：
はい。 1 つのストレージアレイに、保護されたボリュームグループまたはプールと保護されていないボリュームグループまたはプールを混在させて構成できます。前述したように、ボリュームグループまたはプールにセキュリティ対応ドライブとセキュリティ非対応ドライブが混在している場合、ボリュームグループまたはプールのセキュリティを有効にすることはできません。

■ 1 つのボリュームグループまたはダイナミックディスクプールに、保護されたボリュームと保護されていないボリュームの両方を含めることはできますか。

回答：
いいえ。ボリュームグループまたはプール全体が、保護されているか、保護されていないかのいずれかである必要があります。

■ 暗号化をサポートするドライブのタイプを教えてください。

回答：
現在出荷されている HDD と SSD は、一部の容量とモデルで暗号化をサポートしています。
FIPS または FDE と表記される場合があります。

■ FIPS 準拠のドライブのタイプはどれですか？

回答：
現在出荷されている HDD および SSD は、一部の容量およびモデルで FIPS に準拠しています。

■ このソリューションでは、どのレベルの暗号化が使用されていますか。

回答：
ドライブは AES-256 暗号化を使用しています。キーの作成時、キーの更新時、またはバックアップ要求時にキーファイルに返されるバックアップ済みのセキュリティキーは、AES-128 暗号化を使用してラップされます。

■ ドライブのセキュリティはいつでも有効または無効にできますか。

回答：
データを配置した状態でいつでもセキュリティを有効にできます。唯一の例外は SSD のリードキャッシュ機能です。SSD リードキャッシュのセキュリティは、キャッシュの作成時にのみ有効にできます。再プロビジョニングにより、ドライブのセキュリティを無効にできます。再プロビジョニングを行うには、ドライブがユーザーデータに組み込まれていない必要があります。ドライブの再プロビジョニング処理は、ドライブ上の暗号化キーが変更され、元に戻すことができないため、安全な消去操作です。

■ フルディスク暗号化機能 FIPS 140-2 は有効ですか？

回答：
はい。使用中のドライブは FIPS 140-2 と表記されます。FIPS 140-2 Level 2 で認証された全てのドライブは、NIST 規格に準拠した厳しい品質試験と検証を受けています。ドライブの暗号化モジュール（ハードウェアまたはソフトウェア）は、NIST と連携したドライブ製造元によって検証されています。ETERNUS AB/HB series では、NIST のガイドラインに従って適切な認証を行い、すでに認証されている FIPS ドライブの所有権を得ています。このプロセスは、通常の安全なドライブの認証や所有権とは異なります。

■ フルディスク暗号化を使用している間にコントローラーを交換できますか。

回答：
はい。デュアルコントローラーシステムでシングルコントローラーを交換すると、セキュリティキーとそのほかの設定パラメーターが自動的に同期されます。シンプレックスコントローラーシステムでコントローラーを交換する場合またはデュアルコントローラーシステムで両方のコントローラーを交換する場合は、元のコントローラーからバックアップ済みのセキュリティキーを提供する必要があります。セキュリティキーのバックアップが利用できない場合は、ドライブ上のデータにアクセスできません。

Fujitsu Storage
ETERNUS AB series オールフラッシュアレイ，
ETERNUS HB series ハイブリッドアレイ
SANtricity ドライブのセキュリティ
SANtricity 11.70 を使用した機能の詳細

P3AG-5762-02Z0

発行年月　2022 年 12 月
発行責任　富士通株式会社

FUJITSU