



# セキュリティキーの設定

## SANtricity 11.8

NetApp  
December 16, 2024

# 目次

セキュリティキーの設定 .....	1
内部セキュリティキーの作成 .....	1
外部セキュリティキーの作成 .....	2

# セキュリティキーの設定

## 内部セキュリティキーの作成

ドライブセキュリティ機能を使用するには、ストレージレイのコントローラとセキュリティ対応ドライブで共有される内部セキュリティキーを作成します。内部キーは、コントローラの永続的メモリに保持されます。

開始する前に

- ストレージレイにセキュリティ対応ドライブが搭載されている必要があります。対応するドライブには、Full Disk Encryption (FDE) ドライブと連邦情報処理標準 (FIPS) ドライブがあります。
- ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーにお問い合わせください。



ストレージレイにFDEドライブとFIPSドライブの両方が搭載されている場合は、すべてのドライブで同じセキュリティキーが共有されます。

タスクの内容

このタスクでは、内部セキュリティキーに関連付ける識別子とパスフレーズを定義します。



ドライブセキュリティのパスフレーズは、ストレージレイの管理者パスワードとは別のものです。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理\*で、\*内部キーの作成\*を選択します。

まだセキュリティキーを生成していない場合は、セキュリティキーの作成ダイアログボックスが開きます。

3. 次のフィールドに情報を入力します。

- セキュリティキー識別子を定義--デフォルト値(コントローラファームウェアによって生成されたストレージレイ名とタイムスタンプ)をそのまま使用するか独自の値を入力することができます入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読点、記号は使用できません。



入力した文字列の前後に追加の文字が自動的に生成されて付加されます。文字が追加されることで識別子が一意であることが保証されます。

- パスフレーズを定義/パスフレーズを再入力--パスフレーズを入力して確認します値は8~32文字で、次の文字をそれぞれ含める必要があります。
  - 大文字のアルファベット (1文字以上)。パスフレーズでは大文字と小文字が区別されることに注意してください。
  - 数字 (1文字以上)。

- ・ !、\*、@などの英数字以外の文字（1文字以上）。



後で使用するために、必ず入力を記録しておいてください。セキュリティ有効ドライブをストレージレイから移動する必要がある場合は、ドライブデータのロックを解除するために識別子とパスフレーズが必要です。

#### 4. [作成 (Create)] をクリックします。

セキュリティキーは、コントローラのアクセスできない場所に格納されています。実際のキーと一緒に、ブラウザからダウンロードされる暗号化されたキーファイルがあります。



ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

#### 5. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、\*閉じる\*をクリックします。

#### 結果

これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループおよびプールでセキュリティを有効にしたりできます。



ドライブの電源をオフにして再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

#### 終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

## 外部セキュリティキーの作成

キー管理サーバでドライブセキュリティ機能を使用するには、キー管理サーバとストレージレイのセキュリティ対応ドライブで共有される外部キーを作成する必要があります。

#### 開始する前に

- ・ アレイにセキュリティ対応ドライブが搭載されている必要があります。対応するドライブには、Full Disk Encryption (FDE) ドライブと連邦情報処理標準 (FIPS) ドライブがあります。



ストレージレイにFDEドライブとFIPSドライブの両方が搭載されている場合は、すべてのドライブで同じセキュリティキーが共有されます。

- ・ ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーにお問い合わせください。
- ・ ストレージレイのコントローラ用の署名済みクライアント証明書ファイルがあり、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol (KMIP) 要求を

信頼できるようにします。

- キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。キー管理サーバ証明書は、ストレージレイがサーバのIPアドレスを信頼できるように、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。



サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

## タスクの内容

このタスクでは、キー管理サーバのIPアドレスと使用するポート番号を定義し、外部キー管理に使用する証明書をロードします。

## 手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理\*で、\*外部キーの作成\*を選択します。



現在内部キー管理が設定されている場合は、外部キー管理に切り替えるかどうかを確認するダイアログボックスが開きます。

[外部セキュリティキーの作成]ダイアログボックスが開きます。

3. [キーサーバへの接続]で、次のフィールドに情報を入力します。
  - キー管理サーバのアドレス-キー管理に使用するサーバの完全修飾ドメイン名またはIPアドレス（IPv4またはIPv6）を入力します。
  - キー管理ポート番号-- KMIP通信に使用するポート番号を入力します。キー管理サーバの通信に使用される最も一般的なポート番号は5696です。

\*オプション：\*バックアップ・キー・サーバを構成する場合は、\*キー・サーバの追加\*をクリックし、そのサーバの情報を入力します。プライマリキーサーバに到達できない場合は、2番目のキーサーバが使用されます。各キーサーバが同じキーデータベースにアクセスできることを確認します。アクセスできないと、アレイはエラーを投稿し、バックアップサーバを使用できません。



一度に使用されるキーサーバは1つだけです。ストレージレイがプライマリキーサーバに到達できない場合、アレイはバックアップキーサーバに接続します。両方のサーバ間でパリティを維持する必要があることに注意してください。そうしないと、エラーが発生する可能性があります。

- クライアント証明書の選択--最初の\*参照\*ボタンをクリックして、ストレージレイのコントローラの証明書ファイルを選択します。
  - キー管理サーバのサーバ証明書を選択-- 2番目の\*参照\*ボタンをクリックして、キー管理サーバの証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。
4. 「\*次へ\*」をクリックします。
  5. 「キーの作成/バックアップ」では、セキュリティ上の理由からバックアップ・キーを作成できます。
    - (推奨) バックアップキーを作成する場合は、チェックボックスを選択したまま、パスフレーズを入

力して確認します。値は8~32文字で、次の文字をそれぞれ含める必要があります。

- 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
- 数字（1文字以上）。
- !、\*、@などの英数字以外の文字（1文字以上）。



後で使用するために、必ず入力を記録しておいてください。セキュリティ有効ドライブをストレージレイから移動する必要がある場合は、ドライブデータのロックを解除するためにパスフレーズが必要です。

+

- バックアップキーを作成しない場合は、チェックボックスを選択解除します。



外部キーサーバへのアクセスが失われ、バックアップキーがないと、ドライブを別のストレージレイに移行するとドライブ上のデータにアクセスできなくなることに注意してください。このオプションは、System Managerでバックアップキーを作成する唯一の方法です。

## 6. [完了]をクリックします。

入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。その後、セキュリティキーのコピーがローカルシステムに格納されます。



ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

## 7. パスフレーズとダウンロードしたキーファイルの場所を記録し、\*閉じる\*をクリックします。

ページには、次のメッセージと外部キー管理用のリンクが表示されます。

Current key management method: External

## 8. 「\* Test Communication \*」を選択して、ストレージレイとキー管理サーバの間の接続をテストします。

テスト結果がダイアログボックスに表示されます。

### 結果

外部キー管理を有効にすると、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループおよびプールでセキュリティを有効にしたりできます。



ドライブの電源をオフにして再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

## 著作権に関する情報

Copyright © 2024 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随時、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 5252.227-19（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权を有し、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权については、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。