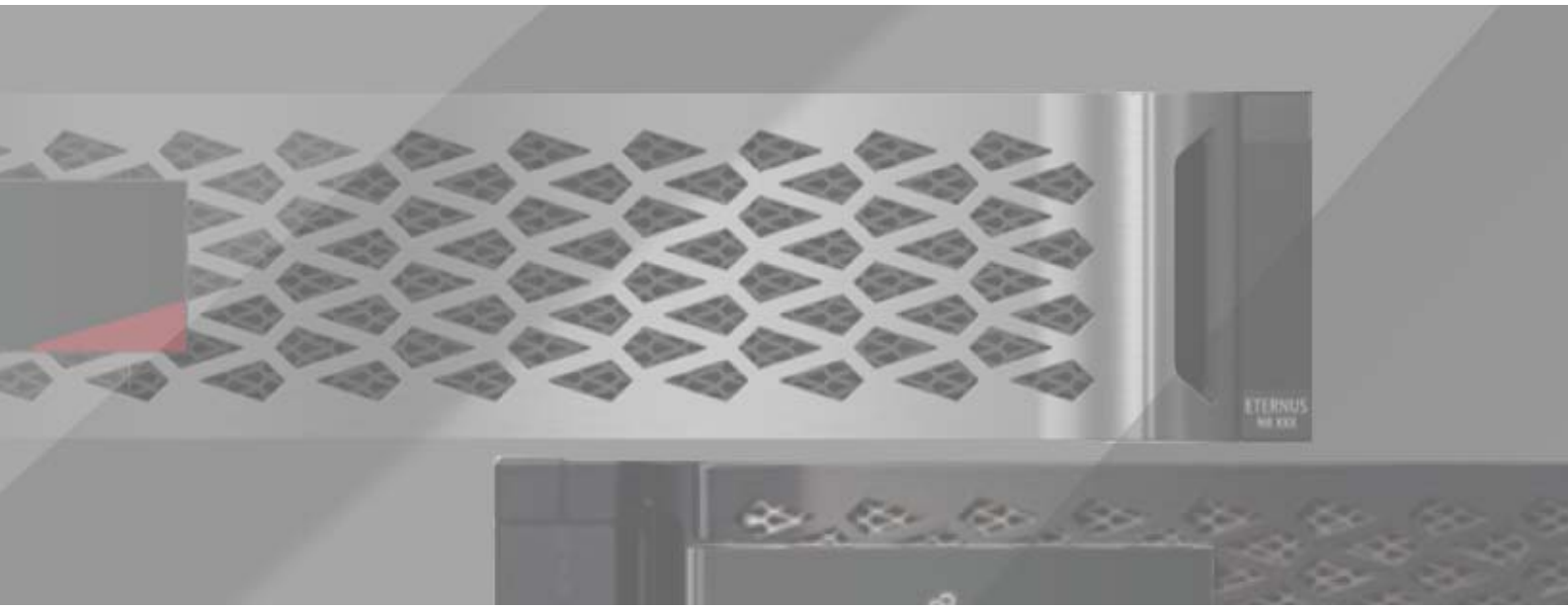
P3AG-6412-01Z0

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

ETERNUS AB/HB series ストレージシステムの証明書管理



FUJITSU

目次

図目次

表目次

はじめに

本書では、最新のETERNUS AB/HBシリーズのコントローラおよびアプリケーションを使用してセキュリティ証明書を管理する方法について説明します。

初版
2021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。

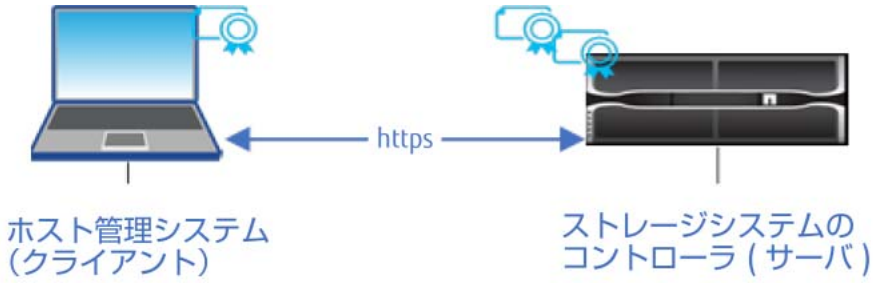
注 意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備 考	本文を補足する内容や、参考情報を記述しています。

第 1 章
証明書管理の概要

証明書は、インターネット上の安全な通信のために、Web サイトやサーバなどのオンラインエンティティを識別するデジタルファイルです。証明書によって、Web 通信は、暗号化された形式でプライベートに、変更されずに指定されたサーバとクライアントの間でのみ送信されます。

ETERNUS AB/HB series ストレージシステムを使用したネットワークでは、ホスト管理システム (クライアントとして動作) 上のブラウザとストレージシステム内のコントローラ (サーバとしての機能) の間で証明書を管理できます。

図 1.1　クライアントとサーバで使用される証明書



1.1　文書範囲

本書では、次の SANtricity バージョンおよびコントローラモデルを使用して証明書を管理する方法について説明します。

- **SANtricity アプリケーション**
  - OS バージョン 11.60 以降の System Manager
  - バージョン 4.0 以降の Web Services Proxy と Unified Manager
- **コントローラモデル**
  - ETERNUS AB2100 および ETERNUS HB2000/HB1000 ストレージシステム
  - ETERNUS AB5100 および ETERNUS HB5000 ストレージシステム
  - ETERNUS AB3100 および ETERNUS AB6100 ストレージシステム

備 考

本書では、古い SANtricity バージョン、古いコントローラモデル、CLI や API などのその他のタイプの SANtricity 管理アプリケーションについては説明しません。また、ミラーリング操作による証明書の構成についても説明しません。これらの製品および方法による証明書管理の詳細については、富士通マニュアルサイトに掲載の「ETERNUS AB/HB series SANtricity 管理セキュリティ」を参照してください。

1.2　証明書の基本

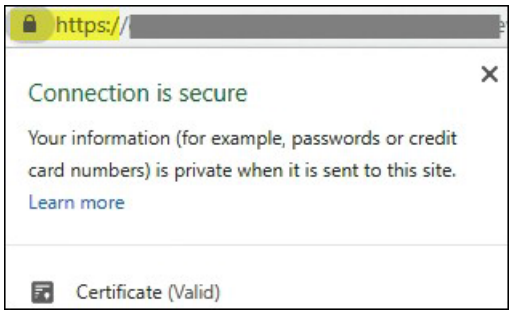
証明書には、信頼できる機関によって署名されているものと、自己署名されているものがあります。署名するということは、誰かが所有者の ID を確認し、そのデバイスが信頼できるものであると判定したということです。

1.2.1　署名付き証明書とは？

署名付き証明書は、信頼できる第三者機関である認証局 (CA) によって検証されます。署名付き証明書には、エンティティ (通常はサーバまたは Web サイト) の所有者に関する詳細、証明書の発行日と有効期限、エンティティの有効なドメイン、および文字と数字で構成されるデジタル署名が含まれます。基本的に、署名付き証明書は ID カードのように機能し、所有者が本人であることを確認します。

ブラウザを開いて Web アドレスを入力すると、システムはバックグラウンドで証明書チェックプロセスを実行し、有効な CA 署名証明書を含む Web サイトに接続しているかどうかを判断します。一般に、署名付き証明書でセキュリティ保護されたサイトでは、次の例のように、アドレスに南京錠のアイコンと https の指定が含まれます。

図 1.2　署名付き証明書を持つ Web サイトの例



CA 署名証明書が含まれていない Web サイトに接続しようとすると、ブラウザにサイトが安全ではないという警告が表示されます。

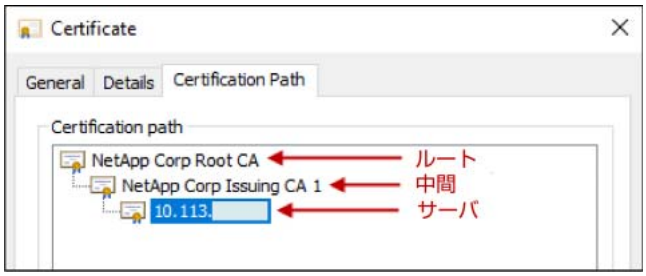
1.2.2　認証局とは？

認証局 (CA) とは、Verisign や DigiCert などの信頼された第三者機関であり、Web サイトやその他のデバイスにデジタル証明書を発行します。CA を発行機関にするには、主要なブラウザ、オペレーティングシステム、およびモバイルデバイスから信頼されるための厳しい基準を満たす必要があります。認可された CA のリストは、民間企業から政府機関まで、インターネット上で見つけることができます。

デジタル証明書を申請すると、CA はユーザーの身元を確認する手順を実行します。このプロセスで、CA は登録されている企業に電子メールを送信して業務アドレスを確認し、HTTP または DNS の確認を実行します。有効な ID を発行する組織 (自動車管理局など) と同様に、CA はインターネット上で動作するエンティティの ID を検証します。
アプリケーションプロセスが完了すると、CA からデジタルファイルが送信され、ホスト管理システムにロードされます。通常、これらのファイルには、次のようなトラストチェーンが含まれます。

- **ルート**
  階層の最上位にはルート証明書があり、他の証明書に署名するために使用される秘密鍵が含まれています。ルートは、特定の CA 組織を識別します。すべてのネットワークデバイスに同じ CA を使用する場合、必要なルート証明書は 1 つだけです。
- **中間**
  ルート証明書から分岐しているのが、中間証明書です。CA は、保護されたルート証明書とサーバ証明書の間の仲介者として機能する 1 つ以上の中間証明書を発行します。
- **サーバ**
  チェーンの一番下には、Web サイトやその他のデバイスなど、特定のエンティティを識別するサーバ証明書があります。ETERNUS AB/HB series ストレージシステムの各コントローラには、個別のサーバ証明書が必要です。

図 1.3　証明書チェーンの例

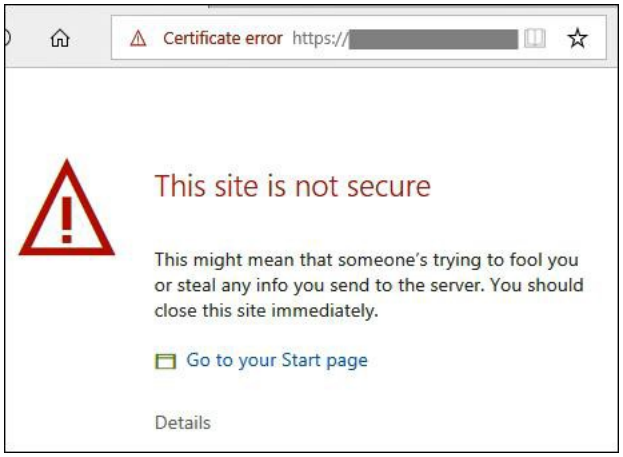


証明書チェーンは、セキュリティイベントが発生した場合の被害を最小限に抑えるのに役立ちます。CA は、関連するすべての署名付き証明書も失効されるように、中間ファイルを失効させることができます。チェーンが信頼できなくなったため、このアクションが必要です。

1.2.3　自己署名証明書とは？

自己署名証明書は CA 署名証明書に似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA 署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、データが暗号化され、サーバとクライアント間の HTTPS 接続を介して送信されます。ただし、自己署名証明書は、CA 署名証明書と同じトラストチェーンを使用しません。
自己署名証明書はブラウザから「信用」されません。自己署名証明書のみを含む Web サイトに接続しようとするたびに、ブラウザに警告メッセージが表示されます。次の例では、[Details] をクリックして、Web サイトに進むためのリンクにアクセスする必要があります。この操作によって、原則的にその自己署名証明書を受け入れることになります。

図 1.4　署名付き証明書のない Web サイトの例



1.2.4　署名証明書または自己署名証明書のどちらを使用するべきか？

環境に最適な証明書の種類は、セキュリティ要件と予算によって異なります。

CA 署名証明書は、より優れたセキュリティ保護 (例えば中間者攻撃の防止) を提供しますが、大規模なネットワークを使用している場合は、高額な料金が必要になることがあります。これとは対照的に、自己署名証明書はセキュリティが劣りますが、無料です。したがって、自己署名証明書は、ほとんどの場合、運用環境ではなく、内部テスト環境で使用されます。

表 1.1　証明書タイプによる違い

種類	長所と短所
CA 署名	• 信頼できる第三機関によって検証される • より強固なセキュリティを提供 • 高額になる可能性がある • 本番環境に最適
自己署名	• お客様の組織によって検証される • 制限されたセキュリティを提供 • 無料 • テスト環境での使用に最適

1.3　証明書の用語

表 1.2 は、このドキュメントで使用される用語を定義します。

表 1.2　証明書の用語

用語	定義
証明書	セキュリティ目的で Web サイトまたはネットワークデバイスの所有者を識別するデジタルファイル。
認証局 (CA)	デジタル証明書を管理および発行する、Verisign や DigiCert などの信頼された第三者機関。
証明書チェーン (ルート、中間、サーバ)	証明書のセキュリティを強化するファイルの階層。通常、チェーンには、階層の最上位に 1 つのルート証明書、1 つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれます。
証明書署名要求 (CSR)	デバイスの証明書を要求するために CA に送信するデータファイル。CSR には、組織の詳細が含まれます。また、デバイスの IP または DNS 名も表示されます。 SANtricity アプリケーションから CSR を作成すると、自己署名証明書が生成され、署名付き証明書が CA から戻されるまで使用されます。さらに、秘密鍵が生成され、データの暗号化に使用されます。証明書自体には、デバイスまたはエンティティを識別するサブジェクト ID (識別名とも呼ばれる) があります。
キーストア、トラストストア	キーストアは、対応する公開鍵と証明書とともに秘密鍵を含むホスト管理システム上のリポジトリです。これらのキーと証明書は、ETERNUS AB/HB series のコントローラなどの独自のエンティティを識別します。 トラストストアは、CA などの信頼できる第三機関からの証明書を含むリポジトリです。 基本的に、キーストアは独自の資格情報 (サーバまたはクライアント) を格納するために使用され、トラストストアは他の信頼できるソースからの資格情報を格納するために使用されます。
プレインストールされた証明書	SANtricity アプリケーションで使用される用語で、コントローラとともに出荷される自己署名証明書を指します。
自己署名証明書	エンティティの所有者によって検証される証明書。このデータファイルには秘密鍵が含まれており、HTTPS 接続を介してサーバとクライアントの間でデータが暗号化形式で送信されます。また、文字と数字で構成されるデジタル署名も含まれます。自己署名証明書は、CA 署名証明書と同じトラストチェーンを使用しないため、テスト環境で最もよく使用されます。
署名付き証明書	CA によって検証される証明書。このデータファイルには秘密鍵が含まれており、HTTPS 接続を介してサーバとクライアントの間でデータが暗号化形式で送信されます。さらに、署名付き証明書には、エンティティ (通常はサーバまたは Web サイト) の所有者に関する詳細と、文字と数字で構成されたデジタル署名が含まれます。署名付き証明書はトラストチェーンを使用するため、ほとんどの場合、運用環境で使用されます。
ユーザーがインストールした証明書	SANtricity アプリケーションで使用される用語で、コントローラに保管されている CA 署名証明書、またはトラストストアにインポートした証明書を指します。

1.4　ETERNUS AB/HB series システムでの証明書の動作

ETERNUS AB/HB series ストレージシステムの最新モデルには、各コントローラに自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、コントローラとホストシステム間のより安全な接続のために CA 署名証明書を取得することもできます。

証明書を管理するには、次の SANtricity アプリケーションを使用します。

- **シングルコントローラ用の System Manager**
  System Manager は、コントローラのオペレーティングシステムに含まれるストレージ・プロビジョニング・アプリケーションです。System Manager を使用するには、コントローラの管理ポートに接続されているホストからブラウザを開き、コントローラの IP アドレスまたはドメイン名を入力します。Web インタフェースから、ストレージ・システム内の 2 つのコントローラのうちの 1 つを管理し、CSR を生成し、コントローラの CA 署名証明書をインポートできます。
- **複数のコントローラに対応する Unified Manager**
  Unified Manager は、ネットワーク上の Windows または Linux ホストに個別にインストールされる Web サービスプロキシの一部です。Unified Manager を使用するには、ホストからブラウザを開き、Unified Manager の URL を入力します。Web インタフェースから、ネットワーク内で検出されたすべてのアレイを管理できます。ただし、個々のコントローラの CA 署名証明書をインポートするには、System Manager を使用する必要があります。

備 考

CLI コマンドや API コマンドなど、他の方法でコントローラと証明書を管理する場合は、富士通マニュアルサイトに掲載の「ETERNUS AB/HB series SANtricity 管理セキュリティ」を参照してください。

図 1.5　System Manager アプリケーションインタフェース

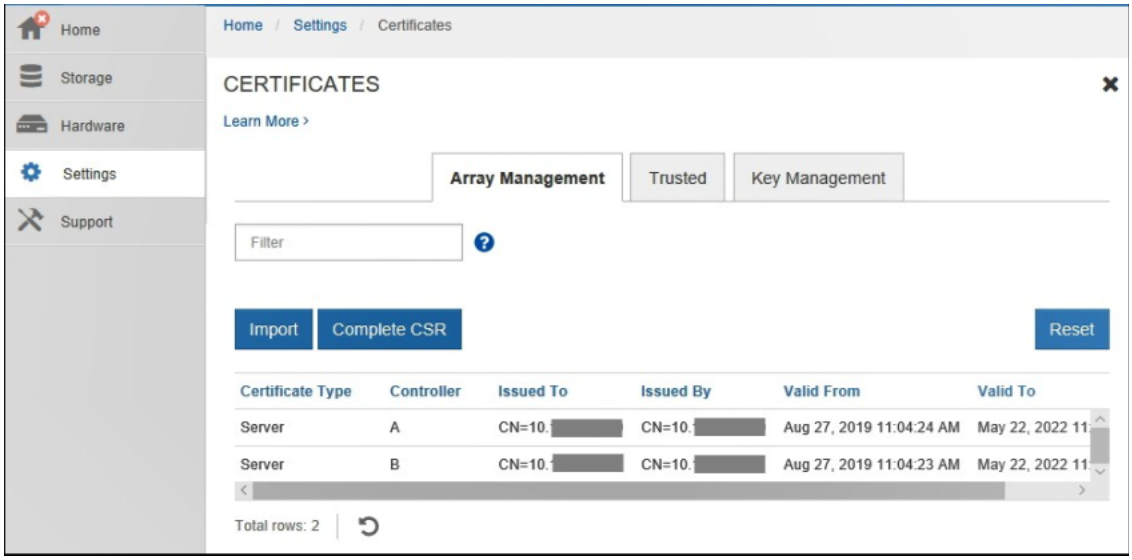
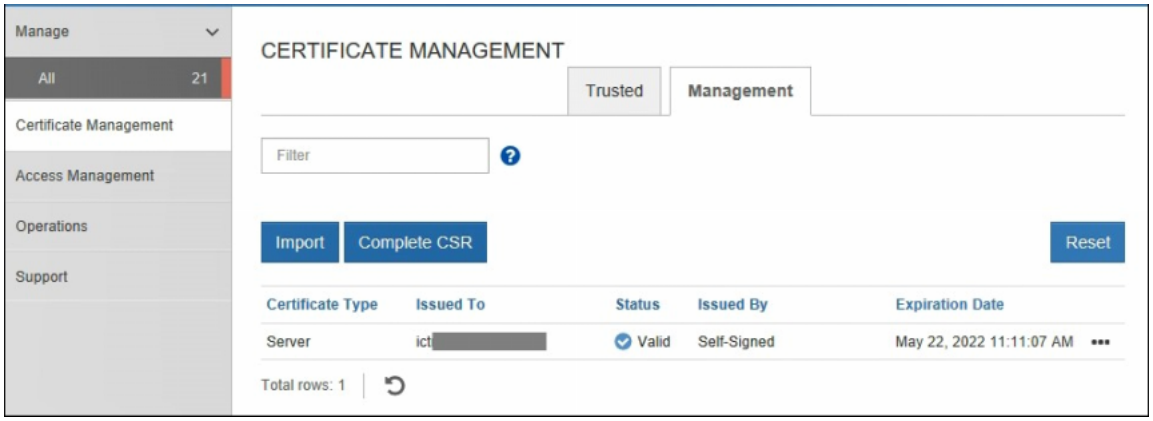


図 1.6　Unified Manager アプリケーションインタフェース



1.5　証明書の基準と要件

表 1.3 では、ETERNUS AB/HB series システムで使用される証明書に関する重要な情報について説明します。

表 1.3　証明書の基準と要件

項目	定義
フォーマット基準	証明書の形式は、国際電気通信連合・電気通信標準化部門 (ITU-T) の X.509 国際標準によって指定されています。
エンコード形式	ETERNUS AB/HB series システムでは、以下の証明書ファイルタイプを含む PEM (Base64 ASCII エンコード) 形式が必要です。 .pem、.crt、.cer、または .key。

第 2 章
System Manager を使用した証明書の管理

System Manager は、コントローラのオペレーティングシステムに含まれるストレージ・プロビジョニング・アプリケーションです。System Manager では、コントローラとホスト管理システムの間で証明書を管理する方法が 2 つあります。

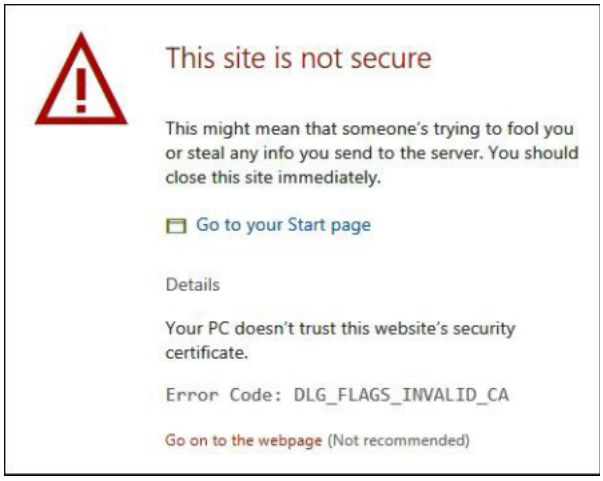
- コントローラの自己署名証明書を引き続き受け入れます。
- コントローラの CA 署名証明書を取得します。

2.1 System Manager での自己署名証明書の使用

ETERNUS AB/HB series コントローラには自己署名証明書が含まれており、System Manager へのアクセスに使用されるブラウザはコントローラを信頼しないため、接続が安全でないことを示す警告メッセージが表示されます。

2.1.1 ログイン時のコントローラ接続の信頼

System Manager にアクセスするには、コントローラの管理ポートに接続されているホストからブラウザを開き、コントローラのIPアドレスまたはドメイン名を入力します。ブラウザは、System Manager のログイン画面を表示する前に、コントローラが信頼できるソースであるかどうかを確認します。ブラウザがコントローラの CA 署名証明書を見つけられない場合は、以下のような警告メッセージが表示されます。そこから Web サイトに進むことができます。続行すると、そのセッションに対するコントローラの自己署名証明書を受け入れることになります。



2.2　コントローラに対する CA 署名証明書の使用

コントローラ (サーバとして機能) と System Manager で使用するブラウザ (クライアントとして動作) との間の安全な通信のために CA 署名証明書を取得するには、次のワークフローに従います。

手順 ▶▶▶

1. **CSR ファイルを生成する**
   System Manager を使用して、ストレージシステムのコントローラごとに証明書署名要求 (CSR) を作成します。
2. **CSR ファイルを CA に送信する**
   CSR ファイルをダウンロードして CA に送信し、証明書が返されるのを待ちます。
3. (必要に応じて) **証明書チェーンを展開する**
   場合によって、CA が証明書を配布するときに、チェーンをルート証明書、中間証明書、およびサーバ証明書の 3 つ以上の個別のファイルに展開する必要があります。
4. **CA 署名証明書をインポートする**
   System Manager を使用して、CA から証明書ファイルをインポートします。

◀◀◀

2.2.1　ステップ 1: CSR の生成

CSR は、組織に関する情報、コントローラの IP アドレスまたは DNS 名、およびコントローラ内の Web サーバを識別するキーペアを提供します。

備 考

CA への送信後に新しい CSR を生成しないでください。
CSR を生成すると、秘密鍵と公開鍵のペアが作成されます。公開鍵は CSR の一部であり、秘密鍵はキーストアに保持されます。署名付き証明書を受け取ってキーストアにインポートすると、システムは秘密鍵と公開鍵の両方が元のペアであることを確認します。
そのため、CA に提出した後に新しい CSR を生成しないでください。これを行うと、コントローラによって新しい鍵が生成され、CA から受け取る証明書は機能しなくなります。

ここでは、System Manager から CSR ファイルを生成する方法を説明します。または、OpenSSL などのツールを使用して CSR ファイルを生成し、ステップ 2 に進むこともできます。

System Manager を使用して一方または両方のコントローラの CSR ファイルを作成するには、次の手順に従います。

手順 ▶▶▶

1. System Manager にログインします。ブラウザを開き、コントローラの IP アドレス、またはコントローラのドメイン名とポート番号 (デフォルトは 8443) のいずれかを入力します。例) https://< ドメイン名 >:8443

2 ユーザー名とパスワードを入力します。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。

3 [Settings]-[Certificates] を選択します。

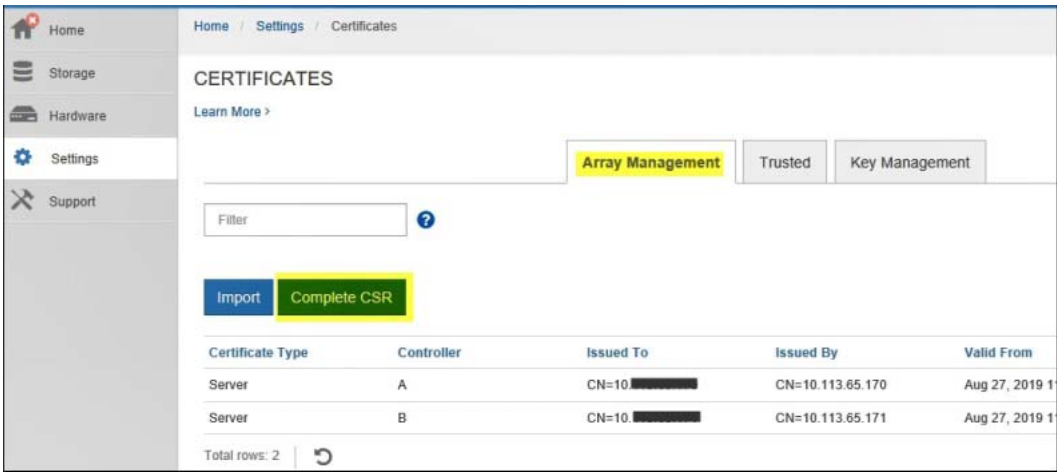
4 2 番目のコントローラの自己署名証明書を受け入れるように求めるダイアログボックスが表示されたら、[Accept Self-Signed Certificate] をクリックして次に進みます。

5 [Array Management] タブが選択されていることを確認します。

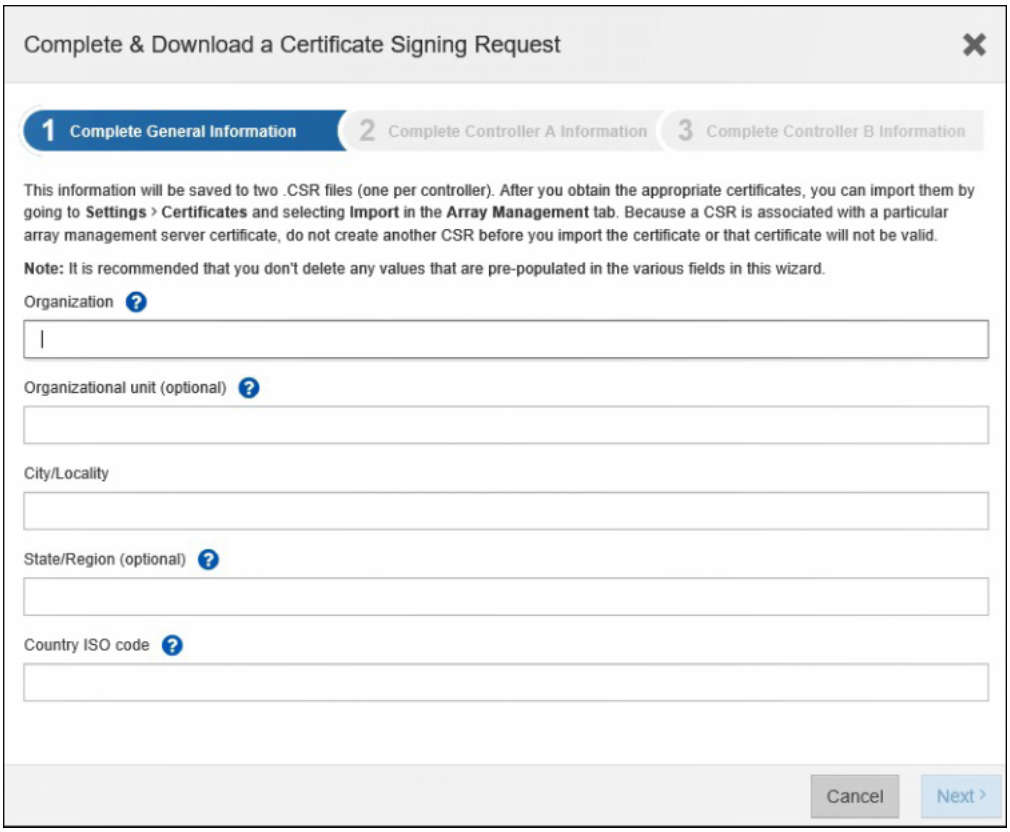
備 考

(オプション) ストレージ・システムをインストールして構成した後、[Reset] を選択すると、コントローラの自己署名証明書を再生成できます。このコマンドは、ストレージシステムのインストール後、プロセスをクリーンな状態で再開します。

6 [Complete CSR] をクリックします。



7 最初のダイアログボックスで、組織の情報と所在地を入力します。



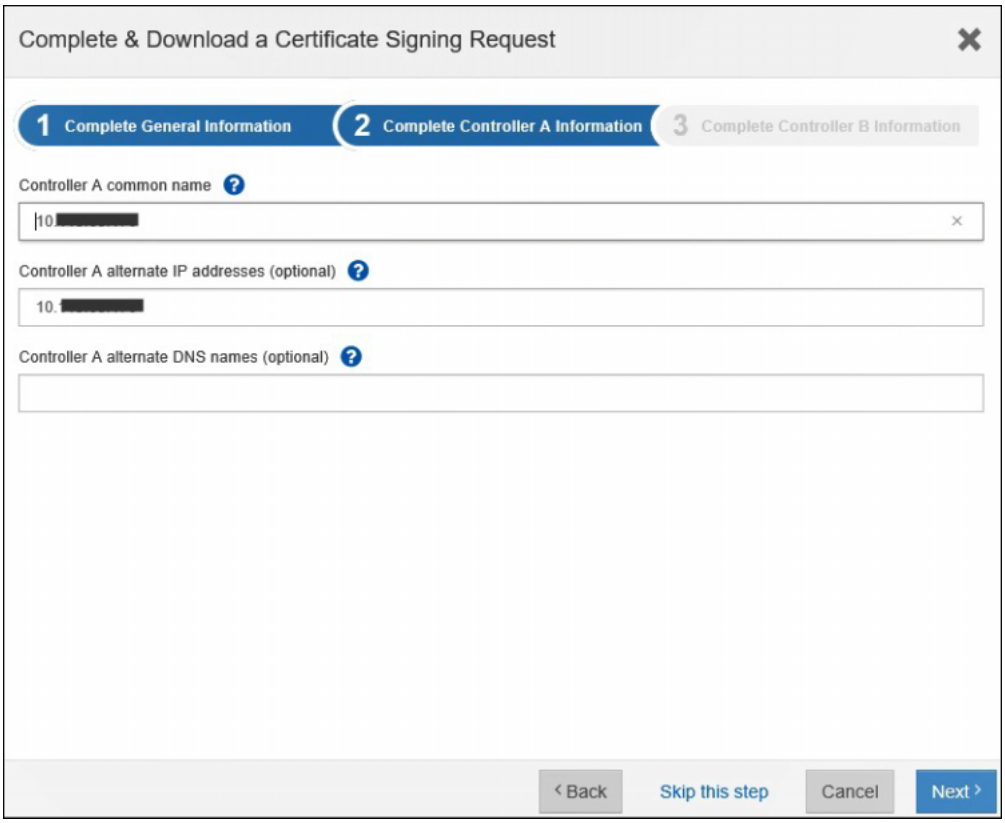
8 [Next] をクリックして、最初のコントローラ (コントローラ A) のダイアログボックスを表示します。

表示される値が正しくない場合を除き、事前設定された値を変更しないでください。DNS サーバを使用している場合は、次の例に示すように、アレイの管理ネットワークにあるサーバコマンドプロンプトから nslookup コマンドを実行してアドレスを確認できます。

```
C:\Users\admin>nslookup 192.13.85.213
Server:  DNS1.location.group.company.com
Address: 192.11.102.130

Name:    ICTM0904C1-A.group.company.com
Address: 192.13.85.213

C:\Users\admin>nslookup 192.13.85.214
Server:  DNS1.location.group.company.com
Address: 192.11.102.130

Name:    ICTM0904C1-B.group.company.com
Address: 192.13.85.214
```

9 コントローラ A については、設定済みの値が正しいことを確認するか、正しい情報を入力します。

- **コントローラ A の共通名**
  デフォルトでは、コントローラ A の IP アドレスまたは DNS 名が表示されます。完全修飾ドメイン名 (FQDN) を入力することを推奨します。例) `name.domain.com` このアドレスが正しいことを確認してください。ブラウザで System Manager にアクセスするために入力した内容と正確に一致する必要があります。http:// または https:// を含めないでください。DNS 名は 63 文字に制限されており、英字または数字で開始および終了する必要があります。英字、数字、およびハイフンのみを使用できます。DNS 名の先頭にワイルドカードを使用することはできません。
- **コントローラ A の代替 IP アドレス**
  (オプション) コントローラ A の代替 IP アドレスまたはエイリアスを一覧表示できます。エントリが複数ある場合は、カンマ区切り形式を使用します。
- **コントローラ A の代替 DNS 名**
  最初のフィールドに FQDN を入力した場合は、その名前をここにコピーします。さらに、コントローラの代替 FQDN を一覧表示できます。複数のエントリの場合は、カンマ区切り形式を使用します。DNS 名の先頭にワイルドカードを使用することはできません。



10 コントローラの情報を再確認して、アドレスが正しいことを確認します。アドレスが正しくない場合は、CA から返された証明書をインポートしようとすると失敗します。

ストレージシステムにコントローラが 1 つしかない場合は、[Finish] ボタンを使用できます。ストレージシステムにコントローラが 2 つある場合は、[Next] ボタンを使用できます。

備 考

最初に CSR リクエストを作成するときは、「Skip This Step」リンクをクリックしないでください。このリンクは、エラーを回復する際に表示されます。まれに、一方のコントローラでは CSR 要求が失敗し、もう一方のコントローラでは失敗しないことがあります。このリンクを使用すると、コントローラ A に CSR 要求が定義されている場合は、その要求を作成する手順を省略して、コントローラ B に CSR 要求を再作成する次の手順に進むことができます。

11 コントローラが 1 つしかない場合は、[Finish] をクリックします。コントローラが 2 つある場合は、[Next] をクリックして、(前のダイアログボックスと同じく) コントローラ B の情報を入力し、[Finish] をクリックします。

◀◀◀

2.2.2　ステップ 2: CSR ファイルの送信

CSR ファイルを CA に送信するには、次の手順に従います。

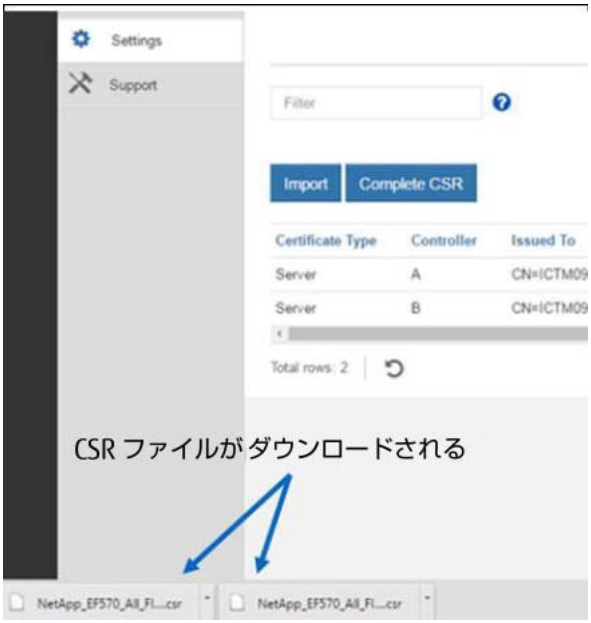
手順 ▶▶▶

1 ダウンロードした CSR ファイルを探します。

コントローラが 1 つの場合、1 つの CSR ファイルがローカルシステムにダウンロードされます。デュアルコントローラの場合、2 つの CSR ファイルがダウンロードされます。フォルダの場所は、ブラウザによって異なります。

2 CSR ファイルを CA(たとえば、Verisign や DigiCert) に送信し、PEM 形式の署名付き証明書を要求します。

3 CA が証明書を返すのを待ちます。



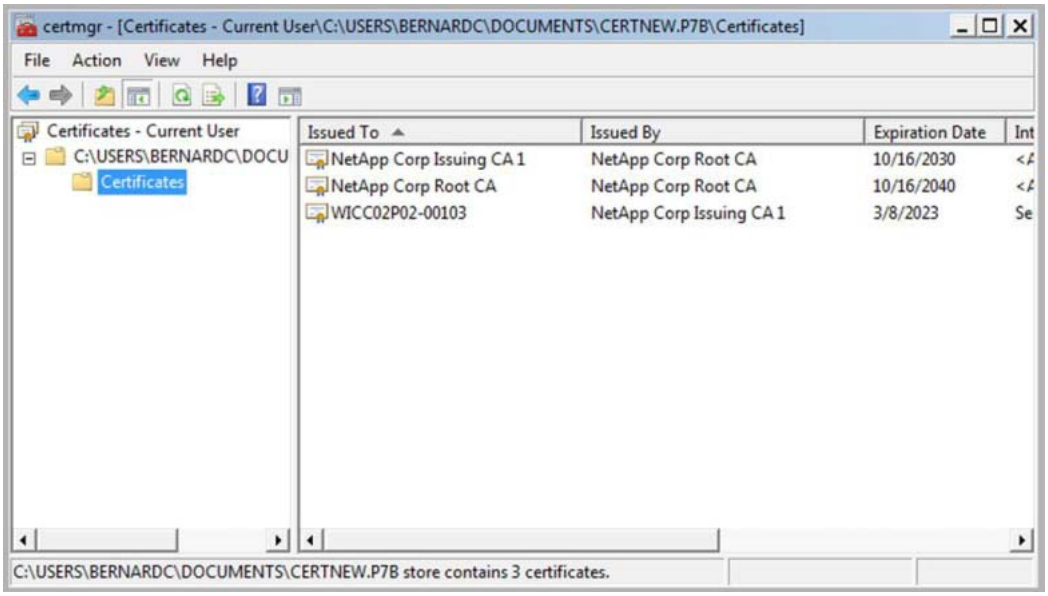
◀◀◀

2.2.3　ステップ 3: 証明書チェーンの展開

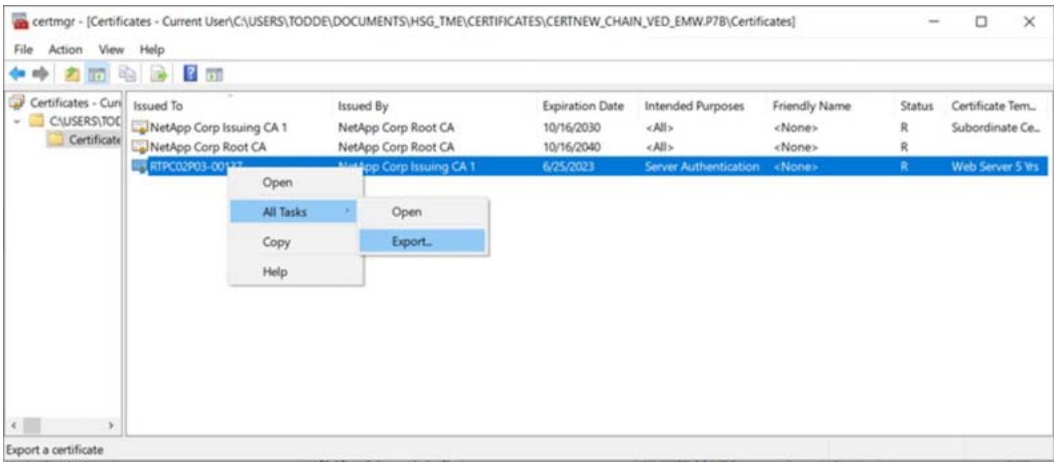
CA が個々の証明書ではなくチェーン証明書を提供する場合は、次の手順に従って証明書チェーンを分割します。

手順 ▶▶▶

1. Windows の certmgr ユーティリティを使用して、[.p7b-PKCS#7] 証明書ファイルをダブルクリックします (ファイルの種類が認識されます)。
2. Windows の Cert Manager で、証明書ツリーを展開し、右側のウィンドウに証明書を表示します。



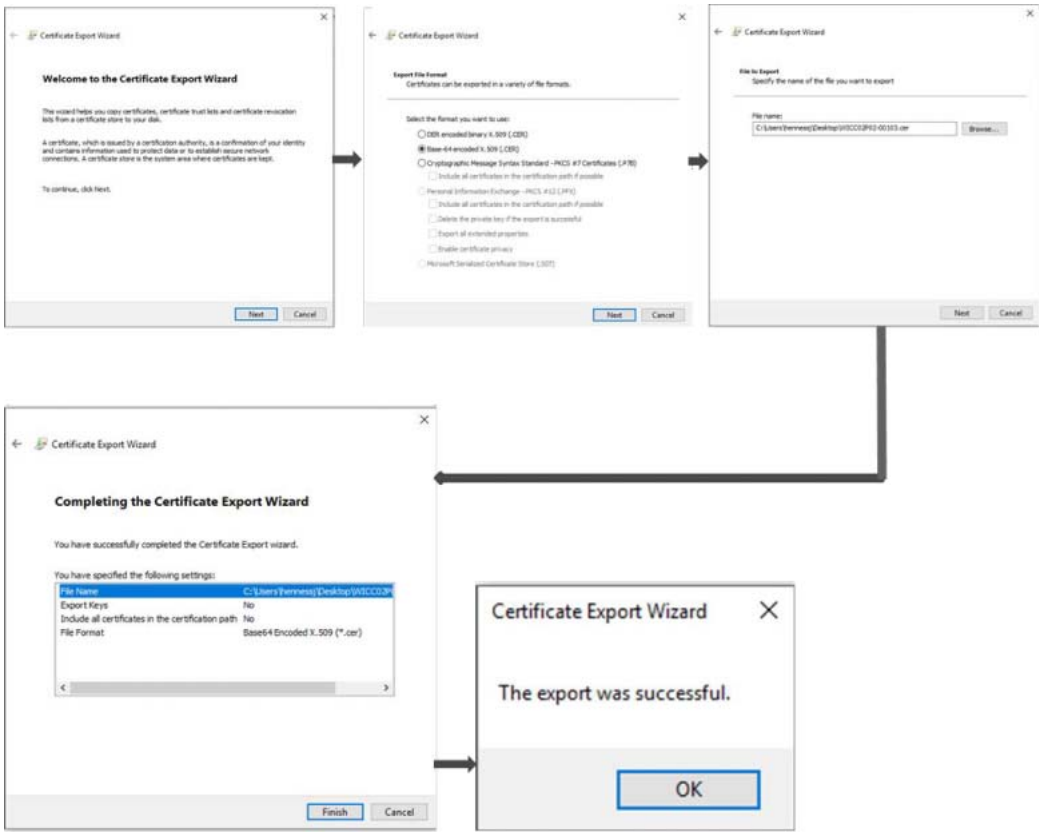
3. 各証明書を右クリックし、[すべてのタスク]-[エクスポート] を選択します。



4 ウィザードに従って、チェーン内の各証明書を、CSR を生成したホスト上のローカルディレクトリにエクスポートします。

備 考

必要な証明書ファイルタイプを選択してください。富士通では、Base-64 エンコード形式を推奨しています。Base-64 エンコード形式を使用すると、共通のデコーダ・ソフトウェアを使用してキーを容易に検証できます。



エクスポートが完了すると、チェーン内の証明書ファイルごとに CER ファイルが表示されます。

2.2.4　ステップ 4: コントローラの CA 署名証明書のインポート

証明書をインポートするには、次の手順に従います。

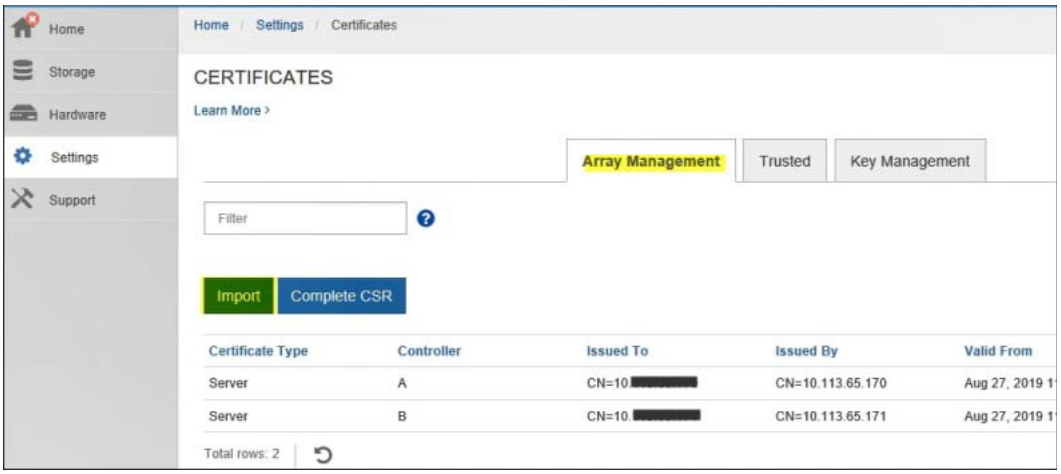
手順

1 コントローラに接続されているホストシステムに証明書ファイルをロードします。

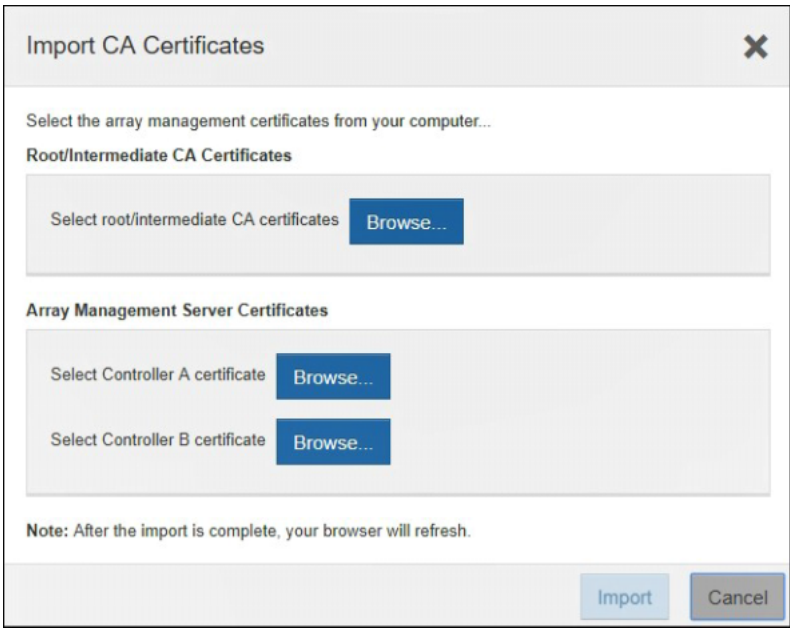
2 System Manager にログインします。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。

3 [Settings]-[Certificates] を選択します。

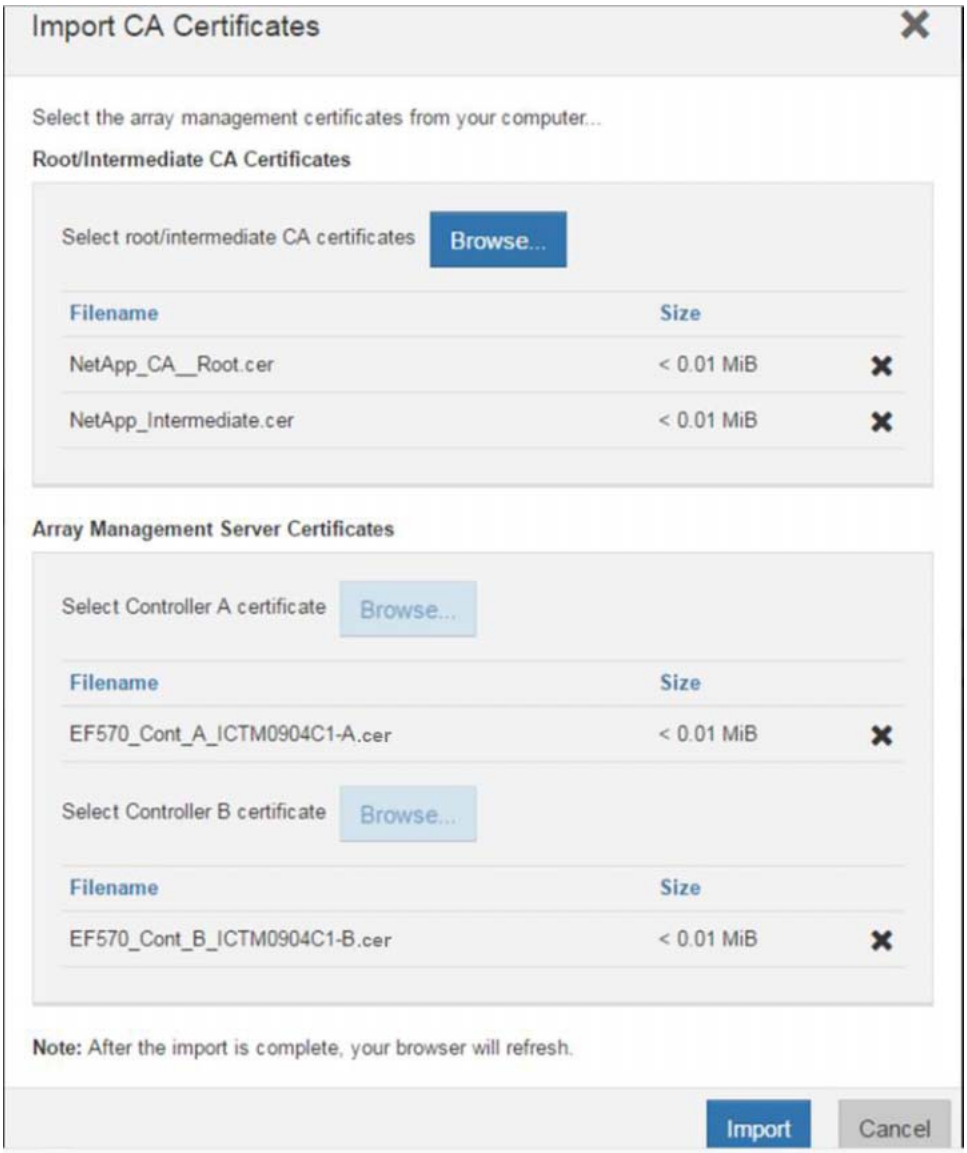
4 [Array Management] タブで、[Import] をクリックします。



5 [Import CA Certificates] ダイアログボックスで、[Browse] ボタンをクリックして最初にルートファイルと中間ファイルを選択し、次にコントローラの各サーバ証明書を選択します。ルートファイルと中間ファイルは、両方のコントローラで同じです。サーバ証明書だけが各コントローラで一意です。外部ツールから CSR を生成した場合は、CSR とともに作成された秘密鍵ファイルもインポートする必要があります。



6 各ファイルを選択したら、[Import] をクリックします。



7 プロンプトが表示されたら、管理者資格情報を入力します。

8 プロンプトが表示されたら、ブラウザセッションを更新します。

ブラウザセッションを閉じて新しいSystem Managerセッションを開始すると、新しいセッションはセキュリティで保護されたブラウザ接続を示します。

第 3 章
Unified Manager を使用した証明書の管理

Unified Manager は Web Services Proxy (WSP) に含まれるアプリケーションで、Linux ホストまたは Windows ホストにインストールされ、ネットワーク内の複数のコントローラを管理します。Unified Manager には、コントローラと WSP サーバ間の証明書を管理するために、次のオプションが用意されています。

- 引き続き、WSP サーバとストレージシステム・コントローラの自己署名証明書を受け入れます。
- WSP サーバの CA 署名証明書を取得します。
- コントローラの署名付き証明書をインポートします。

3.1 Unified Manager での自己署名証明書の使用

自己署名証明書を引き続き使用する場合は、Unified Manager へのアクセスに使用するブラウザに、セキュリティで保護されていない接続に関する警告メッセージが表示されることに注意してください。

3.1.1 ログイン時の WSP サーバ接続の信頼

Unified Manager にアクセスするには、WSP のホストからブラウザを開き、URL とログイン認証情報を入力します。ブラウザは、Unified Manager のログイン画面を表示する前に、WSP の Web サーバが信頼できるソースであるかどうかを確認します。ブラウザがサーバの CA 署名証明書を見つけられない場合は、以下のような警告メッセージが表示されます。そこから Web サイトに進むことができます。続行して、そのセッションの自己署名証明書を受け入れます。

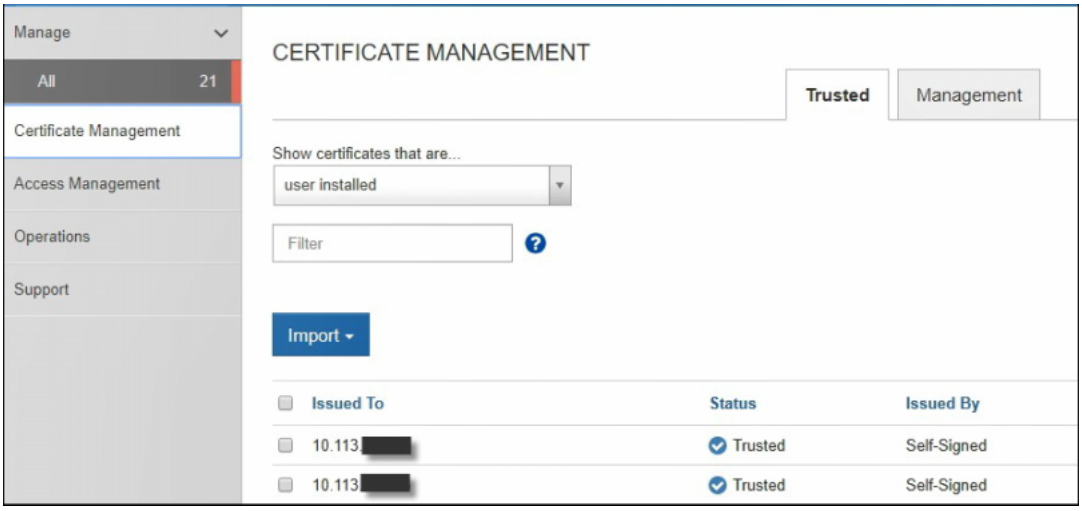
3.1.2　セッション中のコントローラ接続の信頼

Unified Manager セッション中に、CA 署名証明書を持たないコントローラにアクセスしようとすると、追加のセキュリティメッセージが表示される場合があります。この場合、自己署名証明書を永続的に信頼できます。選択内容は、ユーザーが管理するトラストストアに書き込まれ、Unified Manager セッション全体に保持されます。

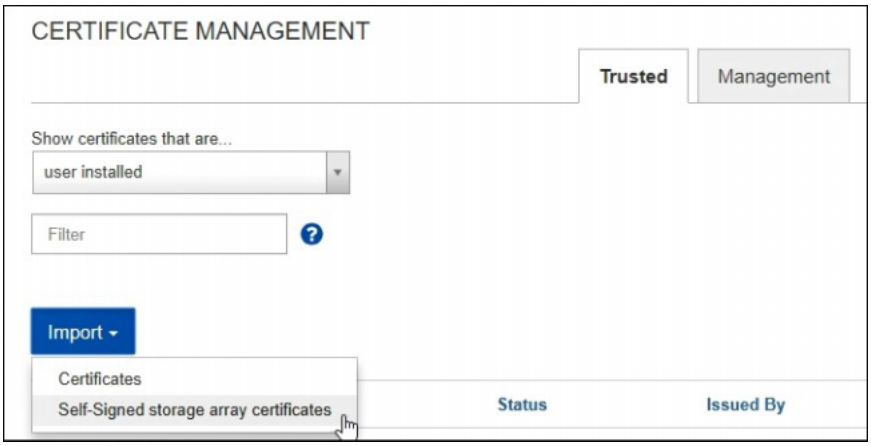
コントローラの接続を信頼するには、次の手順に従います。

手順 ▶▶▶

1. Unified Manager に移動します。ブラウザを開き、次のように入力します。
   https://<WSP サーバの FQDN>:<port>/um
2. ユーザー名とパスワードを入力してログインします。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。
3. [Certificate Management]-[Trusted] タブを選択します。
   [Trusted] ページには、ストレージシステムについて報告されたすべての証明書 (自己署名証明書と CA 署名証明書の両方) が表示されます。



4 [Import]-[Self-Signed Storage Array Certificates] を選択します。



5 ダイアログボックスで証明書を選択し、[Import] をクリックします。証明書がアップロードされ、検証されます。

3.2　WSP サーバに対する CA 署名証明書の使用

コントローラと Web サービスプロキシ (WSP) サーバ間の安全な通信のために CA 署名証明書を取得するには、次のワークフローに従います。

手順 ▶▶▶

1 **CSR ファイルを生成する**
証明書署名要求 (CSR) を作成するには、Unified Manager を使用します。

2 **CSR ファイルを CA に送信する**
CSR ファイルをダウンロードして CA に送信し、証明書が返されるのを待ちます。

3 (必要に応じて) **証明書チェーンを展開する**
場合によって、CA が証明書を配布するときに、チェーンをルート証明書、中間証明書、およびサーバ証明書の 3 つ以上の個別のファイルに展開する必要があります。

4 **CA 署名証明書をインポートする**
Unified Manager を使用して、CA から証明書ファイルをインポートします。

3.2.1　ステップ 1: WSP サーバの CSR ファイルの生成

CSR は組織に関する情報を提供し、Web サーバを識別する公開鍵を含みます。

備 考

CA への送信後に新しい CSR を生成しないでください。
CSR を生成すると、秘密鍵と公開鍵のペアが作成されます。公開鍵は CSR の一部であり、秘密鍵はキーストアに保持されます。署名付き証明書を受け取ってキーストアにインポートすると、システムは秘密鍵と公開鍵の両方が元のペアであることを確認します。
そのため、CA に提出した後に新しい CSR を生成しないでください。これを行うと、サーバによって新しい秘密鍵が生成され、CA から受け取る証明書は機能しなくなります。

ここでは、Unified Manager から CSR ファイルを生成する方法を説明します。または、OpenSSL などのツールを使用して CSR ファイルを生成し、ステップ 2 に進むこともできます。

Unified Manager を使用して CSR ファイルを生成するには、以下の手順に従ってください。

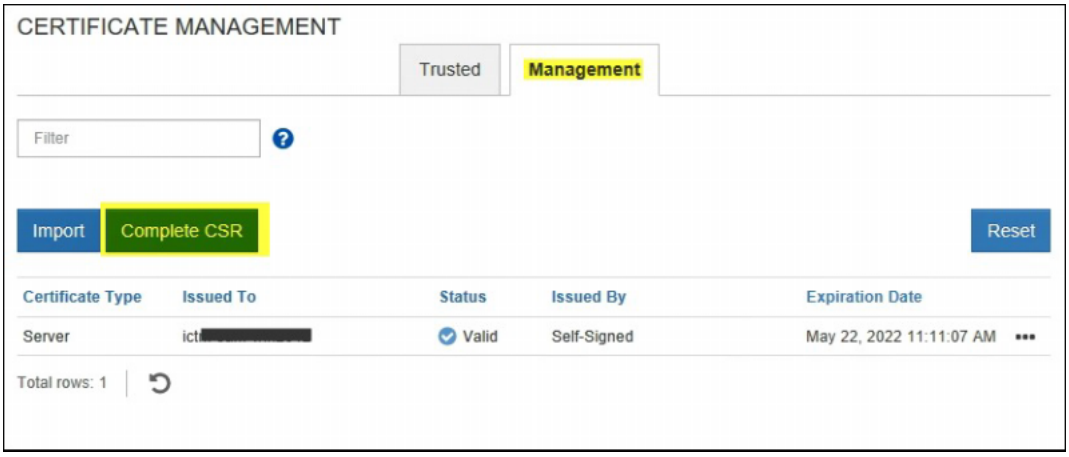
手順 ▶▶▶

1. Unified Manager に移動します。ブラウザを開き、次のように入力します。
   https://<WSP サーバの FQDN>:<port>/um
2. ユーザー名とパスワードを入力します。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。
3. [Certificate Management]-[Management] タブをクリックします。

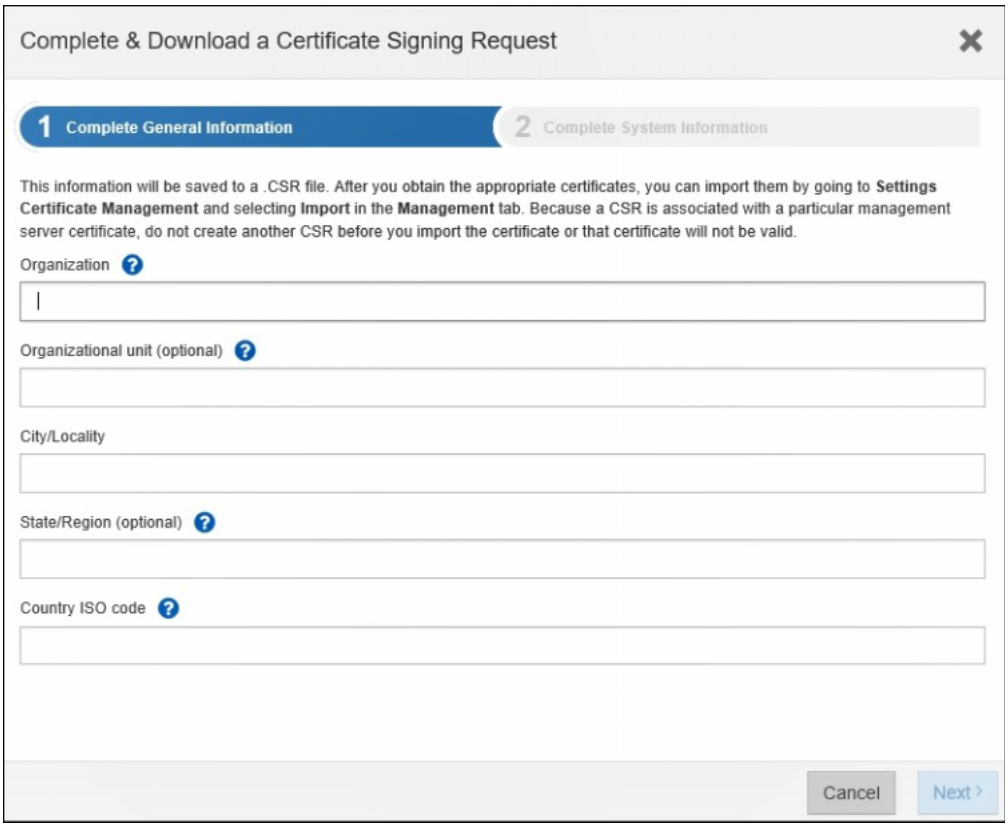
   備 考

   (オプション) ストレージ・システムをインストールして構成した後、[Reset] を選択すると、コントローラの自己署名証明書を再生成できます。このコマンドは、ストレージシステムのインストール後、プロセスをクリーンな状態で再開します。

4. [Complete CSR] を選択します。



5 最初のダイアログボックスで、組織の情報と所在地を入力します。[Next] をクリックします。



6 2 番目のダイアログボックスで、次の情報を入力します。

- **共通名**
  Web サービスプロキシがインストールされているホストシステムの IP アドレス、または DNS 名。完全修飾ドメイン名 (FQDN) を入力することを推奨します。
  例) `name.domain.com`
  このアドレスが正しいことを確認してください。ブラウザで Unified Manager にアクセスするために入力した内容と正確に一致する必要があります。http:// または https:// を含めないでください。DNS 名は 63 文字に制限されており、英字または数字で開始および終了する必要があります。英字、数字、およびハイフンのみを使用できます。DNS 名の先頭にワイルドカードを使用することはできません。
- **代替 IP アドレス**
  (オプション)。ホストシステムの任意の代替 IP アドレスまたはエイリアスを一覧表示できます。複数のエントリの場合は、カンマ区切り形式を使用します。
- **代替 DNS 名**
  最初のフィールドに FQDN を入力した場合は、その名前をここにコピーします。さらに、ホストシステムの任意の代替 FQDN を一覧表示できます。複数のエントリの場合は、カンマ区切り形式を使用します。DNS 名の先頭にワイルドカードを使用することはできません。

7 ホスト情報が正しいことを再確認します。ホスト情報が正しくない場合は、CA から返された証明書をインポートしようとすると失敗します。

8 [Finish] をクリックします。

3.2.2　ステップ 2: CSR ファイルの送信

CSR ファイルを CA に送信するには、次の手順に従います。

手順 ▶▶▶

1. ダウンロードした CSR ファイルを探します。
   ダウンロードするフォルダの場所は、ブラウザによって異なります。
2. CSR ファイルを CA(たとえば、Verisign や DigiCert) に送信し、PEM 形式の署名付き証明書を要求します。
3. CA が証明書を返すのを待ちます。

◀◀◀

3.2.3　ステップ 3: 証明書チェーンの展開

CA が個々の証明書ではなくチェーン証明書を提供する場合は、Windows 証明書マネージャーツールを使用してチェーンを分割します。富士通では、証明書チェーンを分割するときに base-64 エンコーディングを使用することをお勧めします。手順については、「2.2.3 ステップ 3: 証明書チェーンの展開」(P.21) を参照してください。

備 考

この CA に証明書を既に要求している場合は、以前に取得したものと同じルートファイルと中間ファイルを使用できます。WSP サーバ証明書のみが一意になります。

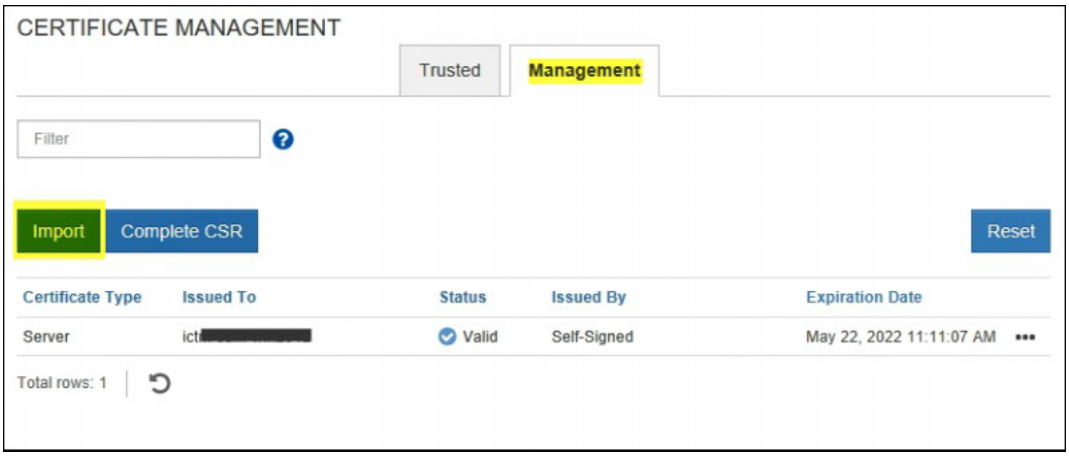
3.2.4　ステップ 4: WSP サーバの CA 署名証明書のインポート

証明書をインポートするには、次の手順に従います。

手順 ▶▶▶

1. WSP サーバがインストールされているホストシステムに証明書ファイルをロードします。
2. Unified Manager に移動します。ブラウザを開き、次のように入力します。
   https://<WSP サーバの FQDN>:<port>/um
3. ユーザー名とパスワードを入力してログインします。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。
4. [Certificate Management]-[Management] タブをクリックします。

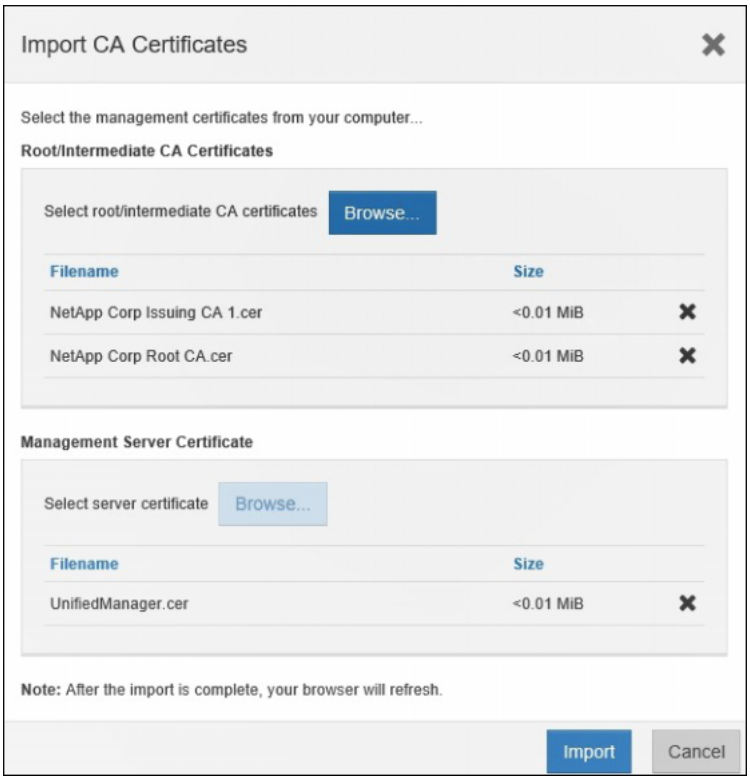
5 [Import] をクリックします。



6 [Import] ダイアログボックスで、[Browse] ボタンをクリックして最初にルートファイルと中間ファイルを選択し、次にサーバ証明書を選択します。外部ツールから CSR を生成した場合は、CSR とともに作成された秘密鍵ファイルもインポートする必要があります。

ファイル名がダイアログボックスに表示されます。

7 [Import] をクリックします。



Web サーバが再起動し、ブラウザが更新されます。ブラウザを閉じて、セキュリティで保護された新しいブラウズセッションを開始できます。

3.3　コントローラの CA 署名証明書のインポート

以前にコントローラ用に CA 署名証明書を取得している場合は、これらのファイルを Unified Manager にインポートすると、Web Services Proxy (WSP) サーバがこれらのコントローラからのクライアント要求を認証できます。独自の CA を持っている場合や、あまり知られていない CA を使用する場合にも、コントローラの証明書のインポートが必要になることがあります。

備 考

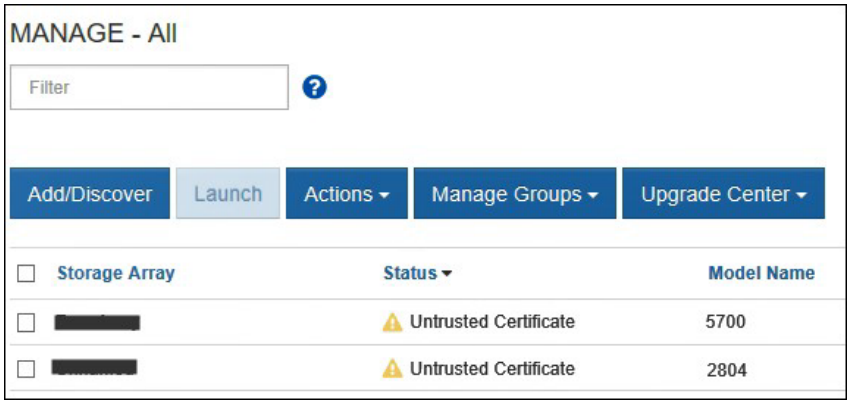
コントローラの CA 署名証明書がない場合は、System Manager を使用して CSR を作成し、CA から証明書ファイルを受信したときに証明書ファイルをインポートする必要があります。手順については、「2.2 コントローラに対する CA 署名証明書の使用」(P.16) を参照してください。

Unified Manager でコントローラの署名付き証明書をインポートするには、以下の手順に従ってください。

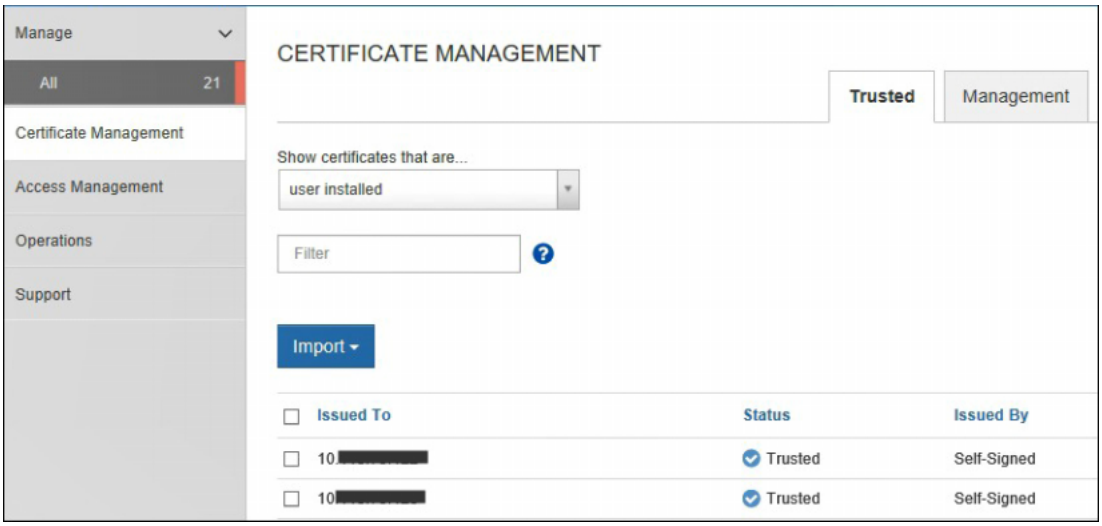
手順 ▶▶▶

1. Unified Manager に移動します。ブラウザを開き、次のように入力します。
   https://<WSP サーバの FQDN>:<port>/um

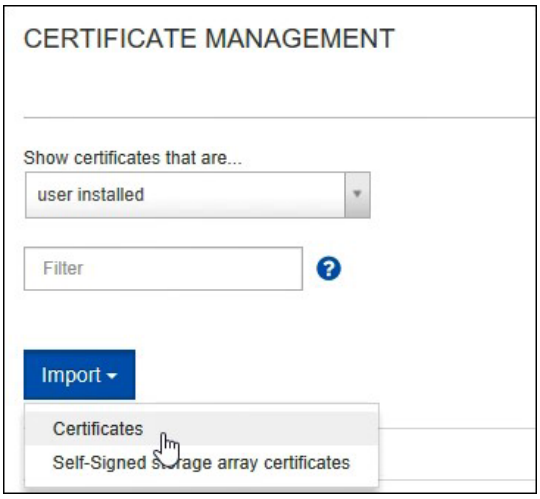
2. ユーザー名とパスワードを入力してログインします。セキュリティ管理者権限を含むユーザープロファイルを使用してログインする必要があります。それ以外の場合、証明書の機能は表示されません。
   検出されたストレージシステムは、そのステータスとともに [Manage] ページに表示されます。



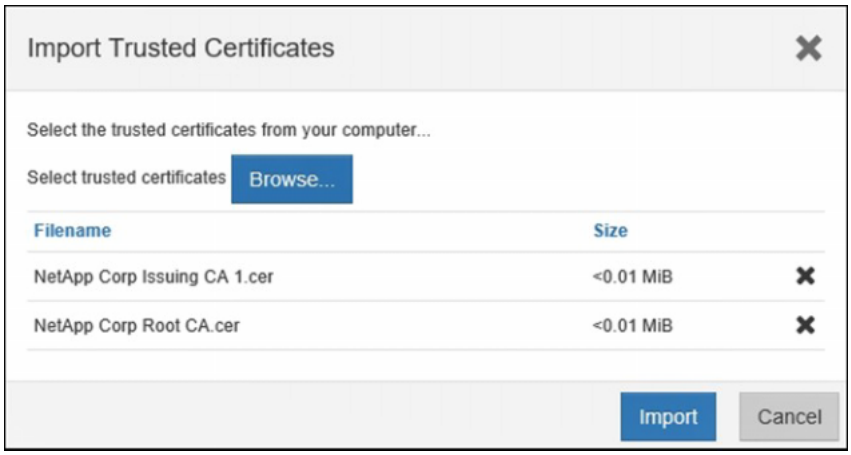
3 [Certificate Management]-[Trusted] タブを選択します。



4 [Import]-[Certificates] を選択し、CA 署名証明書をインポートします。



5 ダイアログボックスで、ルート証明書ファイルと中間証明書ファイルを選択し、[Import] をクリックします。



選択したルートおよび中間ファイルに関連付けられた署名付き証明書を含む証明書ファイルがアップロードおよび検証されます。これらのステータスは、[Certificate Management] ページに表示されます。

第 4 章
追加の証明書管理タスク

本章では、証明書に関連する 2 つの追加タスクについて説明します。

- コントローラ用の信頼できる証明書のインポート
- 失効設定の構成

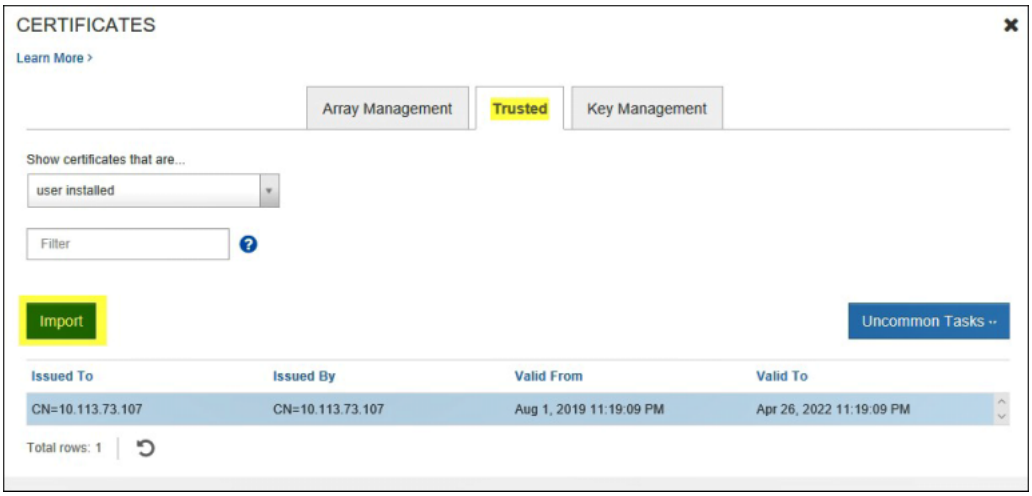
4.1 クライアントとして動作するコントローラの信頼できる証明書のインポート

独自の CA を持っている場合や、あまり知られていない CA を使用していて、TLS を使用する syslog サーバを設定しようとしている場合は、コントローラの証明書のインポートが必要になることがあります。この場合、コントローラはサーバではなくクライアントとして動作します。

コントローラがサーバのトラストチェーンを検証できないために接続を拒否する場合は、次の手順に従います。

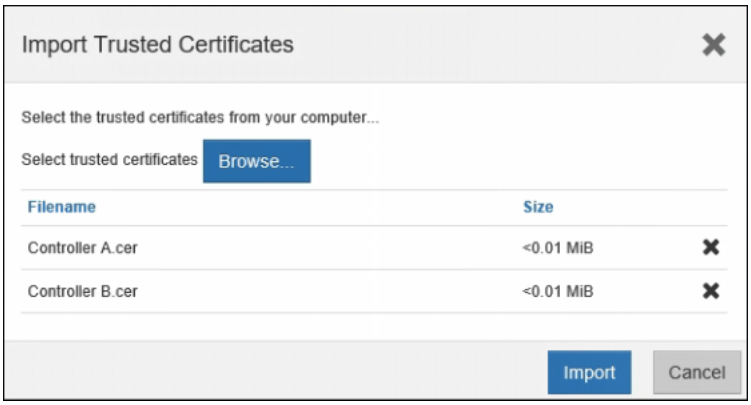
手順 ▶▶▶

1. [Settings]-[Certificates] を選択します。
2. [Trusted] タブを選択し、[Import] をクリックします。



ダイアログボックスが開き、信頼できる証明書ファイルをインポートできます。

3 [Browse] をクリックして、コントローラの証明書ファイルを選択します。
ダイアログボックスにファイル名が表示されます。



4 [Import] をクリックします。

4.2　CA 証明書の失効設定の構成

自動失効確認は、CA が証明書を不適切に発行した場合や、秘密鍵の情報が漏洩した場合に役立ちます。ストレージシステムが、失効した証明書を持つサーバに接続しようとすると、接続が拒否され、イベントがログに記録されます。

失効確認を有効にすると、System Manager は証明書ファイルからオンライン証明書状態プロトコル (OCSP) サーバの URL を検索します。この OCSP サーバを引き続き使用することも、独自の OCSP を構成することもできます。

備 考

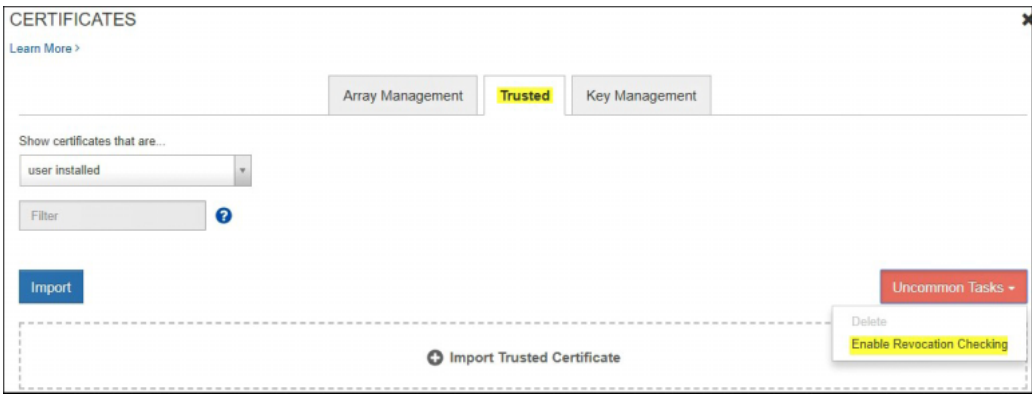
失効確認が有効になっている場合、OCSP サーバの FQDN の使用を有効にするには、両方のコントローラで DNS サーバを構成する必要があります。DNS 構成は、System Manager の「Hardware」ページから利用できます。
失効設定を構成する手順は以下の通りです。

手順

1 System Manager で、[Settings]-[Certificates] を選択します。

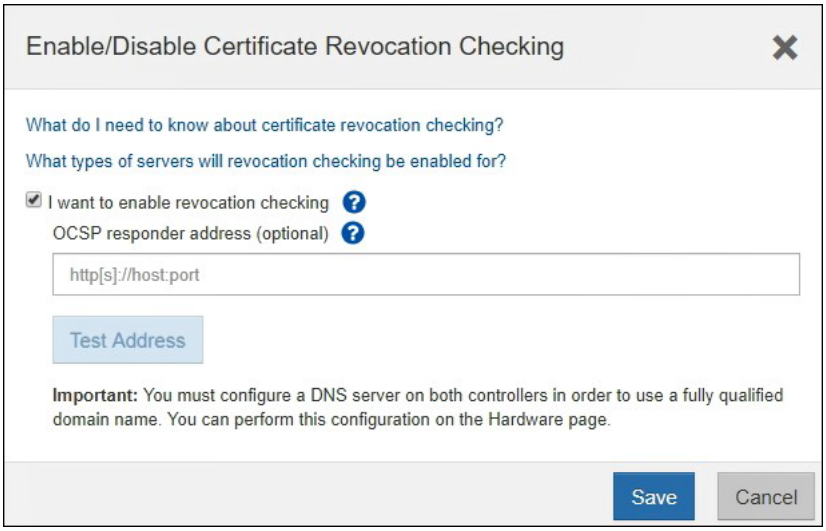
2 [Trusted] タブを選択します。

3 [Uncommon Tasks] をクリックし、ドロップダウンメニューから [Enable Revocation Checking] を選択します。



4 [I Want to Enable Revocation Checking] を選択します。

チェックボックスにチェックマークが付き、ダイアログボックスに追加フィールドが表示されます。



5 デフォルトでは、System Manager は証明書ファイルに指定されている OCSP サーバの URL を使用します。独自のサーバを使用する場合は、[OCSP Responder Address] フィールドに URL を入力します。

備 考

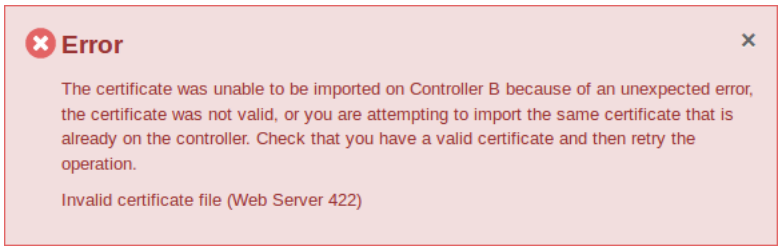
System Manager で OCSP 応答アドレスを指定すると、証明書ファイルにある OCSP アドレスが上書きされます。

6 [Test Address] をクリックして、指定した URL への接続をシステムが開くことができることを確認します。

7 [Save] をクリックします。

第 5 章
無効な証明書エラーのトラブルシューティング

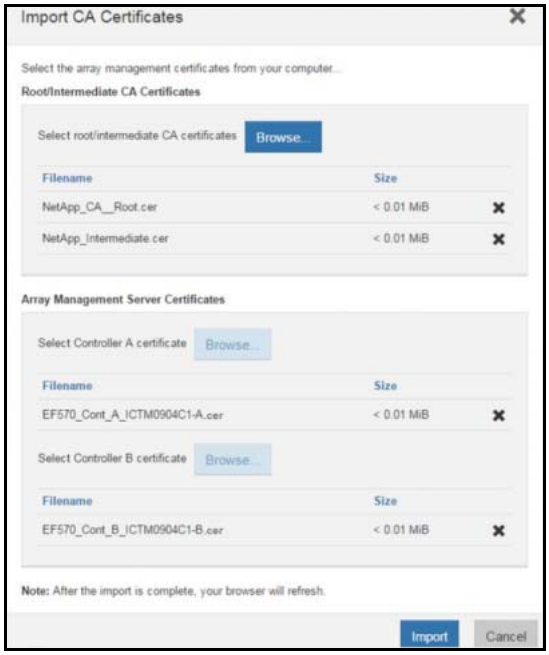
CA が署名した証明書をインポートするとき、この例のような「無効な証明書ファイル (Web サーバ 422)」エラーが表示されることがあります。



この Invalid Certificate File (Web Server 422) エラーメッセージが表示された場合は、表 5.1 のチェックリストに従って問題のトラブルシューティングを行います。

表 5.1　証明書が有効かどうかを確認するチェックリスト

チェックリストの質問	解説と解決策
1. 元の CSR を CA に送信した後、別の CSR ファイルを生成しましたか？	**解説** 証明書署名要求 (CSR) を生成するたびに、システムは新しい公開鍵 / 秘密鍵のキーペアを作成します。元の CSR を CA に送信した後で別の CSR を生成すると、キーペアが上書きされ、新しいペアが生成されます。その結果、古い秘密鍵のキーペアに基づく CA 署名証明書をインポートしようとすると、インポートは失敗します。 **解決策** 最新の CSR ファイルを CA に再送信し、新しい証明書を要求します。
2. CSR に正しいコントローラアドレスを入力しましたか？	**解説** CSR フォームに入力するときは、コントローラのサブジェクト代替名 (または IP アドレス) が正確である必要があります。それ以外の場合、インポートは失敗します。 **解決策** CSR ファイルを確認し、コントローラの共通名とサブジェクト代替名が正しいことを確認します。CSR ファイルを読み込むには、インターネット上にある無料の CSR デコーダを使用します。 例) https://www.sslshopper.com/csr-decoder.html コントローラのアドレスが正確でない場合は、CSR を再生成し、新しい証明書を取得するために CA に送信する必要があります。
3. CA は、サポートされている形式の証明書ファイルを返しましたか？	**解説** 証明書ファイルは、次のいずれかのファイル拡張子を持つ PEM (Base64 ASCII エンコード) でフォーマットする必要があります。 .pem, .crt, .cer, または .key **解決策** CA に連絡して、PEM 形式の証明書ファイルを要求します。または、ファイル形式を PEM に変換できる Web サイトを見つけます。

チェックリストの質問	解説と解決策
4. ワイルドカード証明書をインポートしようとしましたか？	**解説** ワイルドカード証明書は現在サポートされていません。 **解決策** CA に連絡して、PEM 形式の証明書を要求します。
5. 証明書チェーンを個々のファイルに分割しましたか？	**解説** 通常、CA は単一の証明書チェーンファイル (p7b ファイルなど) を送信します。このファイルはインポートできません。代わりに、Windows 証明書マネージャーなどのユーティリティを使用して、チェーンをルート、中間、およびサーバファイルに分割する必要があります。その後、個別にインポートすることができます。 **解決策** 「2.2.3 ステップ 3: 証明書チェーンの展開」(P.21) の指示に従います。証明書チェーンを展開します。ルート証明書は正常にインポートされたが、他の証明書はインポートされなかった場合、テクニカルサポートにお問い合わせください。
6. コントローラの証明書ファイルの名前は一意ですか。	**解説** 各コントローラには、一意の名前を持つ証明書ファイルが必要です。名前が同じ場合、インポートは失敗します。 **解決策** コントローラ A とコントローラ B のサーバ証明書ファイルの名前を変更します (ContrACert、ContrBCert など)。
7. インポート時にすべての証明書 (ルート、中間、およびサーバ) を含めましたか？	**解説** 証明書をインポートするときは、ルート、中間、およびサーバの各ファイルをチェーンに含める必要があります。これらのファイルのいずれかがない場合、チェーンは検証されず、インポートは失敗します。 **解決策** ダイアログボックスの上部にルート証明書と中間証明書の両方が含まれ、下部にサーバ証明書が含まれていることを確認します。 

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
ETERNUS AB/HB series ストレージシステムの証明書管理

P3AG-6412-01Z0

発行年月　2021 年 12 月
発行責任　富士通株式会社

FUJITSU