# 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

© 2021-2025 Fsas Technologies Inc.

1.	証明書管理の概要	6
1.1	文書範囲	6
1.2	証明書の基本	7
1.2.1	署名付き証明書とは?	7
1.2.2	認証局とは?	7
1.2.3	自己署名証明書とは?	
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?	9
1.3	証明書の用語	9
1.4	ETERNUS AB/HB series システムでの証明書の動作	
1.5	証明書の基準と要件	
2.	System Manager を使用した証明書の管理	12
2.1	System Manager での自己署名証明書の使用	
2.1.1		
2.2	コントローラに対する CA 署名証明書の使用	
2.2.1	ステップ 1: CSR の生成	
2.2.2	ステップ 2: CSR ファイルの送信	
2.2.3	ステップ 3: 証明書チェーンの展開	
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	19
3.	Unified Manager を使用した証明書の管理	22
3.1	Unified Manager での自己署名証明書の使用	
3.1.1	ログイン時の WSP サーバ接続の信頼	
3.1.2	セッション中のコントローラ接続の信頼	
3.2	WSP サーバに対する CA 署名証明書の使用	
3.2.1	ステップ 1: WSP サーバの CSR ファイルの生成	
3.2.2	ステップ 2: CSR ファイルの送信	
3.2.3	ステップ 3: 証明書チェーンの展開	26
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	
3.3	コントローラの CA 署名証明書のインポート	
4.	追加の証明書管理タスク	30
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 30
4.2	CA 証明書の失効設定の構成	
5.	無効な証明書エラーのトラブルシューティング	33

図目次

図 1.1	クライアントとサーバで使用される証明書	
図 1.2	署名付き証明書を持つ Web サイトの例	
図 1.3	証明書チェーンの例	
図 1.4	署名付き証明書のない Web サイトの例	
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	

# 表目次

表 1.1	証明書タイプによる違い	9
表 1.2	証明書の用語	9
表 1.3	証明書の基準と要件	11
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	33

# 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。

第2版 2025年3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™、<sup>®</sup>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



# 1. 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、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

### 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

https://	P
Connection is secure	×
Your information (for example, passwords or credit	
card numbers) is private when it is sent to this site. Learn more	
Certificate (Valid)	

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。

#### 1.2 証明書の基本

#### 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

General Details Certification Path Certification path Image NetApp Corp Root CA	X
Certification path	
III NetApp Corp Root CA チャー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
	1
Interaction in the image of	

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

## **1.3 証明書の用語**

<u>表 1.2</u> 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。

1. 証明書管理の概要

1.4 ETERNUS AB/HB series システムでの証明書の動作

用語	定義
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

#### 備考

使用する必要があります。

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、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。

1.5 証明書の基準と要件

図 1.5 System Manager アプリケーションインタフェース

f	Home	Home / Settings /	Certificates	S			
	Storage	CERTIFICATES	6				×
	Hardware	Learn More >					
٥	Settings			Array Management	Trusted	Key Management	
*	Support	Filter Import Comp	Diete CSR	er Issued To	Issued By	Valid From	Reset
		Server	A	CN=10.	CN=10.1	Aug 27, 2019 11:04:24 AM	May 22, 2022 11.
		Server < Total rows: 2	в )	CN=10.	CN=10.	Aug 27, 2019 11:04:23 AM	May 22, 2022 11

図 1.6 Unified Manager アプリケーションインタフェース

Manage 🗸 🗸	CERTIFICATE MANAGEMEN	т	
All 21		Trusted Management	
Certificate Management			
Access Management	Filter		
Operations	Import Complete CSR		Reset
Support			
	Certificate Type Issued To	Status Issued By	Expiration Date
	Server ict	Valid Self-Signed	May 22, 2022 11:11:07 AM
	Ct 1 Store		

# **1.5** 証明書の基準と要件

<u>表 1.3</u> 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。

# 2. 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。

Λ	This site is not secure
7:7	This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.
	Go to your Start page
	Details
	Your PC doesn't trust this website's security certificate.
	Error Code: DLG_FLAGS_INVALID_CA
	Go on to the webpage (Not recommended)

2.2 コントローラに対する CA 署名証明書の使用

## 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。

#### 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。

- 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。

A Home	Pome Settings			
🛢 Storage	ALERTS	SYSTEM	ACCESS MANAGEMENT	CERTIFICATES
A Hardware	0		000	
Ø Settings		342.57		· · · · · · · · · · · · · · · · · · ·
X Support				-0
	<ul> <li>Alerts have not been configured</li> </ul>	Automatic Load Balancing Enabled	Directory Services have been configured	
				1
			[CERTIFIC	CATES] を選択

- **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	春年生成できます。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れ	意で再開します。

**6** [Complete CSR] をクリックします。

Home	Home / Settings / Cer	tificales			
Storage	CERTIFICATES				
Hardware	Learn More >				
Settings			Array Management	Trusted Key Mana	agement
X Support	Filter Import Complete	O			
	Certificate Type	Controller	Issued To	Issued By	Valid From
	Server	A	CN=10.	CN=10.113.65.170	Aug 27, 2019 1
	Server	В	CN=10.	CN=10.113.65.171	Aug 27, 2019 1
	Total rows: 2 3				

#### 2.2 コントローラに対する CA 署名証明書の使用

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。

Complete & Download a Ce	ertificate Signi	ng Request			×
1 Complete General Information	2 Comple	ete Controller A Inform	nation 3 Comp	lete Controller B Info	rmation
This information will be saved to two .CS going to <b>Settings</b> > Certificates and sel array management server certificate, do	SR files (one per cor ecting Import in the not create another	ntroller). After you obtai Array Management t CSR before you import	in the appropriate cert ab. Because a CSR is the certificate or that	ificates, you can impo associated with a par certificate will not be v	rt them by ticular valid.
Note: It is recommended that you don't	delete any values th	at are pre-populated in	the various fields in t	his wizard.	
Organization 🕜					
Organizational unit (optional) 💡					
City/Locality					
State/Region (optional) 💡					
Country ISO code 💡					
				_	
				Cancel	Next

**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。

Complete & Download a Certifi	icate Signing Request		×
1 Complete General Information	2 Complete Controller A Information	3 Complete Controller B Inform	
controller A common name 🕜			
10.			×
controller A alternate IP addresses (optional)	0		
10.1			
ontroller A alternate DNS names (optional)	0		
	( Back	Skin this step Cancel	Mont

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。

- 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。
- 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。

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)。

#### 2.2 コントローラに対する CA 署名証明書の使用

**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。

• 🔿 🙎 🛅 🙆 🛸 🚺				
Certificates - Current User	Issued To 🔺	Issued By	Expiration Date	Ir
C:\USERS\BERNARDC\DOCU	NetApp Corp Issuing CA 1	NetApp Corp Root CA	10/16/2030	<
Certificates	NetApp Corp Root CA	NetApp Corp Root CA	10/16/2040	<
	WICC02P02-00103	NetApp Corp Issuing CA1	3/8/2023	S

**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。

• • 2 10 4									
Certificates - Curi	Issued To		Issued By		Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem
	NetApp Corp Issuing CA 1		NetApp Corp Root CA		10/16/2030	<all></all>	«None»	R	Subordinate Ce_
Certificate	NetApp Corp Root	t CA	NetA	pp Corp Root CA	10/16/2040	<ali></ali>	<none></none>	R	
	RTPC02P03-00127	Open		pp Corp Issuing CA 1	6/25/2023	Server Authentication	<none></none>	R	Web Server 51
		All Tasks		Open					
		Сору		Export_					
		Help							

**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		
 必亜か証明書ファイⅡ.タイ <sup>−</sup>	プを選択してください Base-(	34 エンコード形式が堆将されています
Base-64 エンコート形式を19	き用すると、共通のテコータ・	ソノトワェアを使用してキーを谷易に検証
できます。		
+ 🖉 Certificate Export Witzert	←	4 🕞 Canticute Equat Wand
Welcome to the Certificate Export Wizard	Export file Format Certificates can be exported in a variety of file formats.	Note in Separt Specify the name of the file you want to export
This wated helps you copy certificates, certificate trust lists and certificate revocation lass from a certificate store to your disk.	Select the format you want to use:	File name:
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network.	O DBR. encoded (binary X. 509 (-CBR)     @ Base-64 encoded (X. 509 (-CBR)	Contraction and Referably Second as an University
	Cryptographic Hessage Syntax Standard - PKCS #7 Certificates (#76)     Drdude al cartificates in the certification path if possible	
Te contrue, doi hest	Personal Information Exchange - PKCS #12 (JPK)     Produce all certification in the certification path if possible	
	Delete the private lay if the export is successful     Export all extended properties	
	Installe certificate privacy     (507)     Horseoft Serialized Certificate Inste (507)	
Next Cancel	Net Cancel	Nest Cancel
	×	
← 😺 Certificate Export Wizard		
	<b>4</b>	
Completing the Certificate Export Wizard		
You have successfully completed the Certificate Export wizard.		
You have specified the following settings:		
File Name Ccl/Users/henness/Desktop/ Export Keys No	Certificate Export Wizard	X
Include all certificates in the certification path No File Format Base64 Encoded X.509 (*.cr		
¢	The export was success	ful.
	OK	
Finish	Cancel	

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。

- 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。

Home	Home / Settings / Cer	tificates				
Storage	CERTIFICATES					
Hardware	Learn More >					
Settings			Array Management	Trusted	Key Managem	ent
X Support	Filter Import Complete	O				
	Certificate Type	Controller	Issued To	Issued By	У	Valid From
	Server	A	CN=10.00000000000000000000000000000000000	CN=10.11	13.65.170	Aug 27, 2019 1
	Server	в	CN=10.	CN=10.11	13.65.171	Aug 27, 2019 1
	Total rows: 2 5					

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。

Import CA Certificates	×
Select the array management certificates from your computer Root/Intermediate CA Certificates	
Select root/intermediate CA certificates Browse	
Array Management Server Certificates	
Select Controller A certificate Browse	
Select Controller B certificate Browse	
Note: After the import is complete, your browser will refresh.	
In	Cancel

6 各ファイルを選択したら、[Import] をクリックします。

Import CA Certificates		×
Select the array management certificates from your computer Root/Intermediate CA Certificates		
Select root/intermediate CA certificates Browse		
Filename	Size	
NetApp_CARoot.cer	< 0.01 MiB	×
NetApp_Intermediate.cer	< 0.01 MiB	×
Array Management Server Certificates Select Controller A certificate Browse		
Filename	Size	
EF570_Cont_A_ICTM0904C1-A.cer	< 0.01 MiB	×
Select Controller B certificate Browse		
Filename	Size	
EF570_Cont_B_ICTM0904C1-B.cer	< 0.01 MiB	×
Note: After the import is complete, your browser will refresh.		
	Import	Cancel

- 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。

# 3. 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。

Δ	This site is not secure
7:7	This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.
	Go to your Start page
	Details
	Your PC doesn't trust this website's security certificate.
	Error Code: DLG_FLAGS_INVALID_CA
	Go on to the webpage (Not recommended)

# 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。

 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

#### 3.1 Unified Manager での自己署名証明書の使用

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。

Manage 🗸 🗸	CERTIFICATE MANAGEMENT		
All 21		Trusted	Management
Certificate Management	Show certificates that are		
Access Management	user installed		
Operations	Filter		
Support			
	Import -		
	Ssued To	Status	Issued By
	0.113	Trusted	Self-Signed
	10.113	Trusted	Self-Signed

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

CERTIFICATE MANAGEMENT			
		Trusted	Management
Show certificates that are			
user installed *			
Filter			
Import -			
Certificates			
Self-Signed storage array certificates	Status		Issued By

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。

- 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。

- **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。

CERTIFICATE MANAGEMENT			
	Trusted	Management	
Filter 🕜			
Import Complete CSR			Reset
Certificate Type Issued To	Status	Issued By	Expiration Date
Server ict	📀 Valid	Self-Signed	May 22, 2022 11:11:07 AM
Total rows: 1 3			

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。

Complete & Download a Certificate Signing Request	×
1 Complete General Information         2 Complete System Information	
This information will be saved to a .CSR file. After you obtain the appropriate certificates, you can import them by going to Settings Certificate Management and selecting Import in the Management tab. Because a CSR is associated with a particular managemen server certificate, do not create another CSR before you import the certificate or that certificate will not be valid.	t
Organization 🕜	
1	
Organizational unit (optional) 💡	_
City/Locality	
State/Region (optional) 👔	
Country ISO code 😧	
Cancel	ext >

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。

- 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。
- 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。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推奨します。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.17) 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。

- 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。

Trusted	Management	
		Reset
Status	Issued By	Expiration Date
🕑 Valid	Self-Signed	May 22, 2022 11:11:07 AM •••
Valid	Self-Signed	May 22, 2022 11:11:07 AM
	Trusted Status Valid	Trusted     Management       Status     Issued By       Valid     Self-Signed

- 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。

port CA Certificates				
lect the management certificates from your computer.				
ot/Intermediate CA Certificates				
Select root/intermediate CA certificates Browse				
Filename	Size			
NetApp Corp Issuing CA 1.cer	<0.01 MiB	×		
NetApp Corp Root CA.cer	<0.01 MiB	×		
nagement Server Certificate				
Select server certificate Browse				
Filename	Size			
UnifiedManager.cer	<0.01 MiB	×		
te: After the import is complete, your browser will refr	esh.			

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. Unified Manager を使用した証明書の管理

3.3 コントローラの CA 署名証明書のインポート

## 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、「<u>2.2 コント</u> ローラに対する CA 署名証明書の使用」(P.13) 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。

- **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。

MANAGE - All		
Filter	0	
Add/Discover Launch	Actions - Manage Group	ps - Upgrade Center -
Storage Array	Status -	Model Name
	🛕 Untrusted Certificat	te 5700
	🛕 Untrusted Certificat	ie 2804

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。

Manage 🗸 🗸	CERTIFICATE MANAGEMENT			
All 21			Trusted	Management
Certificate Management	Show certificates that are			
Access Management	user installed			
Operations	Filter			
Support				
	Import -			
	Issued To	Status		Issued By
	□ 10	Trusted		Self-Signed
		🕑 Trusted		Self-Signed

#### 3.3 コントローラの CA 署名証明書のインポート

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

ow certificates that are	
iser installed	*
Filter	0
Import -	
Import -	
ficates	
self-Signed Sarage a	rray certificates

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。

Import Trusted Certificates		×
Select the trusted certificates from your computer Select trusted certificates Browse		
Filename	Size	
NetApp Corp Issuing CA 1.cer	<0.01 MiB	×
NetApp Corp Root CA.cer	<0.01 MiB	×
	Import	Cancel

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。

# 4. 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。

- **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。

ERTIFICATES						
arn More >						
		Array Management	Trusted	Key Management		
Show certificates that are						
user installed	*					
Filter	0					
Filter	Ø				Uncommor	1 Tasks •
Filter Import Issued To	Issued	l By	Valid Fr	om	Uncommon	1 Tasks •

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。

Import Trusted Certificates		×
Select the trusted certificates from your computer Select trusted certificates Browse		
Filename	Size	
Controller A.cer	<0.01 MiB	×
Controller B.cer	<0.01 MiB	×
	Import	Cancel

4. 追加の証明書管理タスク

4.2 CA 証明書の失効設定の構成

**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。

- 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。

ay Management Trusted	Key Management	
ay Management Trusted	Key Management	
		Uncommon Tasks +
		Delete
Import Trusted 0	Certificate	Enable Revocation Checking
	Import Trusted (	Import Trusted Certificate

- 4.2 CA 証明書の失効設定の構成
  - 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。

Enable/Disable Certificate Revocation Checking	×
What do I need to know about certificate revocation checking? What types of servers will revocation checking be enabled for?	
I want to enable revocation checking      OCSP responder address (optional)     http[s]://host:port	
Test Address Important: You must configure a DNS server on both controllers in order to use a domain name. You can perform this configuration on the Hardware page.	fully qualified
Save	Cancel

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

きされます。 [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

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

- 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を確認します。
- **7** [Save] をクリックします。

# 5. 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。

Error	×
The certificate was unable to be imported on Controller B because of an unexpected the certificate was not valid, or you are attempting to import the same certificate tha already on the controller. Check that you have a valid certificate and then retry the operation.	error, t is
Invalid certificate file (Web Server 422)	

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、<u>表 5.1</u>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?	<ul> <li>解説</li> <li>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。</li> <li>解決策</li> <li>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。</li> </ul>	
2. CSR に正しいコントローラアドレス を入力しましたか?	<ul> <li>解説</li> <li>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。</li> <li>解決策</li> <li>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。</li> <li>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。</li> </ul>	
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?	<ul> <li>解説</li> <li>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。</li> <li>.pem, .crt, .cer, または .key</li> <li>解決策</li> <li>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。</li> </ul>	
4. ワイルドカード証明書をインボート しようとしましたか?	<b>解説</b>     ワイルドカード証明書は現在サポートされていません。   <b>解決策</b>   CA に連絡して、PEM 形式の証明書を要求します。	

チェックリストの質問		解説と解決策	
5. 証明書チェーンを個々のファイルに 分割しましたか?	<ul> <li>解説</li> <li>通常、CA は単一の証明書チェー す。このファイルはインポートで ネージャーなどのユーティリティ びサーバファイルに分割する必要 ことができます。</li> <li>解決策</li> <li>「2.2.3 ステップ 3: 証明書チェー チェーンを展開します。ルート語 書はインポートされなかった場合 い。</li> </ul>	-ンファイル (p7b ファイルなど ) を送信しま できません。代わりに、Windows 証明書マ ィを使用して、チェーンをルート、中間、およ 要があります。その後、個別にインポートする <u>ンの展開」(P.17)</u> の指示に従います。証明書 証明書は正常にインポートされたが、他の証明 合、テクニカルサポートにお問い合わせくだこ	よる 明さ
6. コントローラの証明書ファイルの名 前は一意ですか。	<b>解説</b> 各コントローラには、一意の名前 じ場合、インポートは失敗します <b>解決策</b> コントローラ A とコントローラ す (ContrACert、ContrBCert な	前を持つ証明書ファイルが必要です。名前が同 す。 B のサーバ証明書ファイルの名前を変更しま ・ど )。	司
7. インボ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 ?	<b>解説</b> 証明書をインポートするときは、 チェーンに含める必要があります チェーンは検証されず、インポー <b>解決策</b> ダイアログボックスの上部にルー にサーバ証明書が含まれているこ Import CA Certificates Select the array management certificates from your computer. RootIntermediate CA Certificates	、ルート、中間、およびサーバの各ファイルを す。これらのファイルのいずれかがない場合、 ートは失敗します。 ート証明書と中間証明書の両方が含まれ、下音 ことを確認します。	を · · ·
	Select root/intermediate CA certificates Browse Filename NetApp_CA_Root.cer NetApp_Intermediate.cer	Size < 0.01 MiB X < 0.01 MiB X	
	Array Management Server Certificates Select Controller A certificate EF570_Cont_A_ICTM0904C1-A.cer Select Controller B certificate Browse	Size < 0.01 MiB	
	Filename EF570_Cont_B_ICTM0904C1-B.cer Note: After the import is complete, your browser will refresh.	Size < 0.01 Mi8 X Import Cancel	

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-6412-02Z0

発行年月 2025 年 3 月 発行責任 エフサステクノロジーズ株式会社

- 本書の内容は、改善のため事前連絡なしに変更することがあります。
- 本書の内容は、細心の注意を払って制作致しましたが、本書中の誤字、情報の抜け、本書情報の使用に起因す る運用結果に関しましては、責任を負いかねますので予めご了承願います。
- 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその 責を負いません。
- 無断転載を禁じます。

**F**sas Technologies