



セキュリティ認定準拠

次のトピックでは、セキュリティ認定規格に準拠するようにシステムを設定する方法について説明します。

- [セキュリティ認定準拠のモード \(1 ページ\)](#)
- [セキュリティ認定準拠特性 \(2 ページ\)](#)
- [セキュリティ認定準拠の推奨事項 \(3 ページ\)](#)
- [セキュリティ認定コンプライアンスの有効化 \(4 ページ\)](#)

セキュリティ認定準拠のモード

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower システムでは、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- **コモンクライテリア (CC)** : 国際コモンクライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- **Unified Capabilities Approved Products List (UCAPL)** : 米国防情報システム局 (DISA) によって確立された、セキュリティ要件を満たす製品のリスト



(注) 米国政府は、Unified Capabilities Approved Products List (UCAPL) の名称を Defense Information Network Approved Products List (DODIN APL) に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- **連邦情報処理標準 (FIPS) 140** : 暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順につ

いての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。



注意 この設定を有効にした場合、無効にすることはできません。設定を無効にする必要がある場合は、サポートに連絡して支援を求めてください。

セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。（ログインアカウントの制約は、Web インターフェイスアクセスではなくコマンドラインまたはシェルアクセスを指します。）

システムの変更	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	○	○
バックアップまたはレポートについては、リモートストレージは利用できません。	○	○
追加のシステム監査デーモンが開始されます。	なし	○
システムブートローダは固定されています。	なし	○
追加のセキュリティがログインアカウントに適用されます。	なし	○
ログインアカウントセッションの自動ログアウトを実行します。	なし	○
再起動キー シーケンスの Ctrl-Alt-Del を無効にします。	なし	○
最大 10 の同時ログインセッションを実行します。	なし	○
システムは eStreamer を使用したイベントデータのエクスポートをサポートしていません。	○	○

システムの変更	CC モード	UCAPL モード
ログインアカウントの厳密なセーフガードを適用します。 <ul style="list-style-type: none"> パスワードは、大文字および小文字を組み合わせ最大 15 の英数字として、1 つ以上の数字を含む必要があります。 パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。 3 回連続ログインに失敗した場合、そのユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。 パスワード履歴を保存しています。 ログインが成功した場合は、失敗したログインの履歴を表示します。 	なし	○

セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。



注意 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベントデータを受信しません。

- 次の機能を使用するようにシステムを設定できません。
 - 電子メールレポート、アラート、データのプルーニング通知。
 - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
 - バックアップまたはレポート用のリモートストレージ。
 - サードパーティクライアントのシステムデータベースへのアクセス。
 - 電子メール (SMTP)、SNMP トラップ、syslog から送信される外部通知、アラート。
 - アプライアンスとサーバの間のチャネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログメッセージ。
 - eStreamer を使用したイベントデータの外部クライアントへのエクスポート。

- CC モードを使用して展開中に SSO を有効にできません。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。



(注) Firepower システムは、以下に関する CC および UCAPL モードをサポートしていません。

- ハイ アベイラビリティ ペアの Firepower Management Center
- スタックまたはハイ アベイラビリティ ペアの従来型デバイス

セキュリティ認定コンプライアンスの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来型の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは、構成が有効になりません。



注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、Cisco TAC にご連絡ください。

始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Firepower Management Center に登録することをお勧めします。

手順

ステップ 1 設定するアプライアンスの種類に応じて、次のようにします。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 従来型管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス (UCAPL/CC Compliance)] をクリックします。

(注) UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2つの選択肢があります。

- [コモンクライテリア (Common Criteria)] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [CC] を選択します。
- [Unified 機能承認製品リスト (Unified Capabilities Approved Products List)] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [UCAPL] を選択します。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型アプライアンスに適用します。
- 認証エンティティによって提供されるこの製品のガイドラインの説明に従い、追加の設定変更を行います。
- 設定変更を展開します。[設定変更の導入](#)を参照してください。

