



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 \(4 ページ\)](#)
- [セキュリティ認定コンプライアンスの有効化 \(7 ページ\)](#)

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。Cisco Secure Firewall は、以下のセキュリティ認定標準規格への準拠をサポートします。

- 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 Secure Firewall 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後は、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

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アクセスを指します）

システムの変更	Secure Firewall Management Center		従来型管理対象デバイス		Secure Firewall Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	はい	はい	はい	はい	はい	はい
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。	はい	はい	—	—	—	—
追加のシステム監査デーモンが開始されます。	非対応	はい	非対応	はい	非対応	非対応
システム ブートローダは固定されています。	非対応	はい	非対応	はい	非対応	非対応
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。	非対応	はい	非対応	はい	非対応	非対応
再起動のキー シーケンス Ctrl+Alt+Del を無効にします。	非対応	はい	非対応	はい	非対応	非対応
最大10の同時ログインセッションを実行します。	非対応	はい	非対応	はい	非対応	非対応
パスワード長は少なくとも15文字で、大文字/小文字の英数字を組み合わせて1つ以上の数字を含む必要があります。	非対応	はい	非対応	はい	非対応	非対応
ローカル admin ユーザに必要な最小パスワード長を設定するには、ローカル デバイス CLI を使用できます。	いいえ	非対応	非対応	非対応	はい	はい

システムの変更	Secure Firewall Management Center		従来型管理対象デバイス		Secure Firewall Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
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。	非対応	はい	非対応	はい	非対応	非対応
3 回連続してログインに失敗した場合、admin 以外のユーザー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。	非対応	はい	非対応	はい	非対応	非対応
デフォルトでは、システムはパスワード履歴を保存します。	非対応	はい	非対応	はい	非対応	非対応
admin ユーザーは、Web インターフェイスで設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	はい	はい	はい	はい	—	—
admin ユーザーは、ローカルアプライアンス CLI で設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	いいえ	非対応	はい（セキュリティ認定準拠の有効/無効にかかわらず）。	はい（セキュリティ認定準拠の有効/無効にかかわらず）。	はい	はい
次の場合、システムは、アプライアンスとの SSH セッションで自動的にキーを再生成します： <ul style="list-style-type: none"> セッションアクティビティでキーが 1 時間使用された後 キーを使用して接続で 1 GB のデータが伝送された後 	はい	はい	はい	はい	はい	はい
システムは、ブート時にファイルシステム整合性チェック（FSIC）を実行します。FSIC が失敗した場合、Cisco Secure Firewall ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカル コンソールを介してのみアプライアンスにアクセスできます。これが発生した場合は Cisco TAC に連絡してください。	はい	はい	はい	はい	はい	はい

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 **Secure Firewall 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、**Secure Firewall 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。

- すべてのユーザーに対して、パスワードの強度確認を有効にし、パスワードの最小長を認証機関で求められる値に設定します。
- 高可用性設定で **Secure Firewall Management Center** を使用するには、高可用性ペアを形成する前に、同じセキュリティ認定準拠モードを使用するように双方を構成します。
- **Firepower 4100/9300** で、**CC** または **UCAPL** モードで動作するように **Secure Firewall Threat Defense** を設定した場合は、**Firepower 4100/9300** も **CC** モードで動作するように設定する必要があります。詳細については、*Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager* コンフィギュレーション ガイドを参照してください。
- 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ン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。
- **CC** モードを使用して展開する場合は、**LDAP** または **RADIUS** を使用して外部認証を有効にしないでください。
- **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、**Cisco Secure Firewall REST API** 経由での **Secure Firewall 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。
- **CC** モードを使用して展開中に **SSO** を設定できません。



- (注) 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。
- クラスタ内の Secure Firewall Threat Defense デバイス
 - Secure Firewall Threat Defense のコンテナ インスタンス Firepower 4100/9300
 - 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。

アプライアンスの強化

システムの強化に使用可能な機能の詳細については、最新バージョンの *Cisco Cisco Secure Firewall Mangement Center Hardening Guide* と *Cisco Secure Firewall Threat Defense Guide*、および本書の以降のトピックを参照してください。

- [ライセンス](#)
- [Firewall Management Center ユーザー](#)
- [Management Center へのログイン](#)
- [監査ログ](#)
- [監査ログ証明書](#)
- [時刻の同期](#)
- [Cisco Secure Firewall Management Center デバイス構成ガイドの「Configure NTP Time Synchronization for Threat Defense」](#)
- [電子メール アラート応答の作成](#)
- [侵入イベントに対する電子メール アラートの設定](#)
- [Cisco Secure Firewall Management Center デバイス構成ガイドの「Configure SMTP」](#)
- [Cisco Secure Firewall Management Center デバイス構成ガイドの「About SNMP for the Firepower 1000」](#)
- [Cisco Secure Firewall Management Center デバイス構成ガイドの「Configure SNMP」](#)
- [SNMP アラート応答の作成](#)
- [Cisco Secure Firewall Management Center デバイス構成ガイドの「Configure Dynamic DNS」](#)
- [DNS キャッシュ](#)
- [監査と Syslog](#)
- [アクセス リスト](#)
- [セキュリティ認定準拠 \(1 ページ\)](#)

- リモートストレージ用の SSH の設定
- 監査ログ証明書
- HTTPS 証明書
- Web インターフェイス用のユーザー ロールのカスタマイズ
- 内部ユーザーの追加または編集
- セッションタイムアウト
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」
- Firewall Management Center のバックアップのスケジュール
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Site-to-Site VPNs for Firewall Threat Defense*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Remote Access VPN*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*FlexConfig Policies*」

ネットワークの保護

ネットワークを保護するために設定できる機能については、次のトピックを参照してください。

- アクセス制御ポリシー
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Security Intelligence*」
- Cisco Secure Firewall Management Center デバイス構成ガイドの *Snort 3* 侵入ポリシーの開始
- Cisco Secure Firewall Management Center デバイス構成ガイドのルールを使用した侵入ポリシーのチューニング
- Cisco Secure Firewall Management Center デバイス構成ガイドの *Snort 3* のカスタムルール
- 侵入ルールの更新
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Application Layer Preprocessors*」
- 監査と Syslog
- 侵入イベント
- イベント検索
- ワークフロー
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Device Management*」
- ログイン バナー

- 更新

セキュリティ認定コンプライアンスの有効化

この設定は、Secure Firewall Management Center または管理対象デバイスに適用されます。

- Secure Firewall Management Center では、この設定はシステム設定の一部になります。
- 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firewall Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。



注意 この設定を有効にした後に無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

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 Firewall Management Center に登録することをお勧めします。
- Secure Firewall Threat Defense デバイスは評価ライセンスを使用できません。輸出管理機能を有効にするには、Smart Software Manager アカウントを有効にする必要があります。
- Secure Firewall Threat Defense デバイスはルーテッドモードで展開する必要があります。
- このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 Firewall Management Center を設定するか管理対象デバイスを設定するかに応じて、次の操作を実行します。

- Firewall Management Center : [システム (System)] > [構成 (Configuration)] を選択します。
- Firewall Threat Defense 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、Secure Firewall Threat Defense 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。Firewall 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

- 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。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。