SonicOS 7
デバイスの設定

管理ガイド

SONICWALL®

内容

1

機器の設定について

ウェブ ベースの SonicOS 管理インターフェースを使用すると、SonicWall ネットワーク セキュリティ装置（ファイアウォール）を設定することができます。

このドキュメントでは、以下に関する情報が提供されます。

- SonicWall ライセンスの管理
- システム管理
- 時間の設定
- 証明書の管理
- SNMP の管理
- ファームウェア設定
- システムの再起動

2

SonicWall ライセンスの管 理

ⓘ **重要:** 仕様では、SonicWall ライセンス マネージャは、サードパーティ プロキシ サーバを使用するように設定できません。すべての HTTP および HTTPS トラフィックをサードパーティ プロキシ サーバに送るネットワークでは、ライセンス マネージャの問題が発生することがあります。

トピック:

- ライセンス
- セキュリティ サービスの管理
- SonicWall 装置の登録
- ゲートウェイ アンチウイルス、アンチスパイウェア、および IPS サービスのライセンスの有効化
- 無料トライアルの有効化

ライセンス

SonicOS 管理インターフェースの「**デバイス | 設定 > ライセンス**」ページには、SonicWall セキュリティ サービスのライセンスを有効化、アップグレード、または更新するためのリンクがあります。このページから、SonicWall セキュリティ装置のすべてのライセンスを管理できます。「**サービス**」テーブルに表示される情報は、mysonicwall.com アカウントの情報をもとに更新されます。また、「**ライセンス**」ページには、SonicWall セキュリティ サービスの無料トライアルへのリンクもあります。

セキュリティ サービスの管 理

インターネット接続を確立したら、お使いの SonicWall セキュリティ装置を登録することをお勧めします。登録すると、次のメリットが得られます。

- SonicWallゲートウェイ アンチウイルス、アンチスパイウェア、および 侵入防御、コンテンツ フィルタ サービス、クライアント アンチウイルスの 30 日間の無料トライアルを試用できる
- SonicWall アンチスパムを有効にできる
- SonicWall セキュリティ サービスおよびアップグレードを有効にできる
- SonicOS ファームウェア更新にアクセスできる
- SonicWall テクニカル サポートが得られる

トピック:

- サービス サマリ
- セキュリティ サービスのオンライン管理

サービス サマリ

「**デバイス | 設定 > ライセンス**」ページには、SonicWall セキュリティ装置で使用可能なサービスと有効化されているサービスがすべて表示されます。セキュリティ装置のわかりやすい名前が「**サービス**」テーブルの上に表示されます。

「**ビュー**」ドロップダウン ボックスで適切なオプションを選択し、有効化状況に基づいてサービスを表示します。利用可能なオプションは:

- **購読済と未購読**
- **購読済**
- **未購読**

このテーブルには、以下の情報が表示されます。

- **サービス** – SonicWall セキュリティ装置で利用できるすべての SonicWall セキュリティ サービスおよびアップグレードが表示されます。
- **状況** – セキュリティ サービスが有効になっているか (購読済)、有効にできるか (未購読)、または有効でないか (失効) が表示されます。
- **動作** – ライセンス状況に応じて、サービスをアップグレード、更新、試用、有効化するためのオプションが表示されます。

- **個数** – 装置に現在接続しているノード/ユーザの数が表示されます。セキュリティ装置のライセンスがノード数無制限の場合、ノード数は「無制限」と表示されます。
- **最大 数** – ライセンスで許可されるノード/ユーザの最大数が表示されます。
- **失効期日** – 購読済みセキュリティ サービスの失効期日が表示されます。

「**サービス**」テーブルの情報は、次回 SonicWall セキュリティ装置が自動的に(1 日に 1 回) MySonicWall アカウントと同期したとき、またはユーザがテーブルを更新するためにこのページの「**同期**」ボタンを選択したときに、mysonicwall.com アカウントの情報で更新されます。

SonicWall セキュリティ サービスの詳細については、https://www.sonicwall.com/ja-jp/support/technical-documentation/ で提供されている『*SonicOS 7.0 セキュリティ サービス*』マニュアルを参照してください。

セキュリティ サービスのオンライン管 理

次の方法のいずれかを使用して、サービスを有効化、アップグレード、または更新することができます。

- MySonicWall でサービス ライセンスの更新を実行し、変更を SonicOS 管理インターフェースで同期する。
    1. 「**デバイス | 設定 > ライセンス**」ページに移動します。
    2. 「**サービス**」テーブルの上の「**MysonicWall**」を選択します。
    3. MySonicWall アカウントにログインし、ライセンスをアップグレードします。MSW のオンライン ヘルプを参照してください。
    4. 変更を同期します。次を参照してください。変更の同期。
- SonicOS 管理インターフェースからサービス ライセンスの更新を実行する。次を参照してください。SonicOS 管理インターフェースからのサービスの管理。

トピック:

- SonicOS 管理インターフェースからのサービスの管理
- 変更の同期

SonicOS 管 理 インターフェースからのサービスの管 理

「**デバイス | 設定 > ライセンス**」ページで、セキュリティ サービスのライセンスを有効化、アップグレード、更新することができます。

サービスを有効化、アップグレード、または更新するには、以下の手順に従います。

1. **「デバイス | 設定 > ライセンス」に移動します。**
2. 「**サービス**」テーブルの上の「**ビュー**」ドロップダウン ボックスで適切なオプションを選択しします。
3. 有効化/更新/アップグレードするサービスを見つけます。
4. サービスに対して実行する必要がある動作に基づいて「**動作**」列に表示されるオプションを選択します。

    サービスに関して「**動作**」列に表示されるオプションは、サービスの状況によって異なります。

    - 無料トライアル版を有効にする場合は、「**試用**」をクリックします。
    - セキュリティ サービスを有効にする場合は、「**有効化**」リンクを選択します。
    - セキュリティ サービスを更新する場合は、「**更新**」リンクを選択します。
    - セキュリティ サービスをアップグレードする場合は、「**アップグレード**」を選択します。

5. 表示される指示に従ってサービスのライセンスを有効化/更新/アップグレードします。処理が完了すると、「**ライセンス**」ページに戻ります。

変更の同期

MySonicWall のセキュリティ サービスに対して行った変更を、自動的に同期されるのを待たないで明示的に同期させることができます。

MySonicWall アカウントを SonicOS 管理インターフェースの「サービス」テーブルと同期させるには、以下の手順に従います。

1. 「**デバイス | 設定 > ライセンス**」に移動します。
2. 「**サービス**」テーブルの上の「**同期**」オプションを選択します。

閉じた環境での手動アップグレード

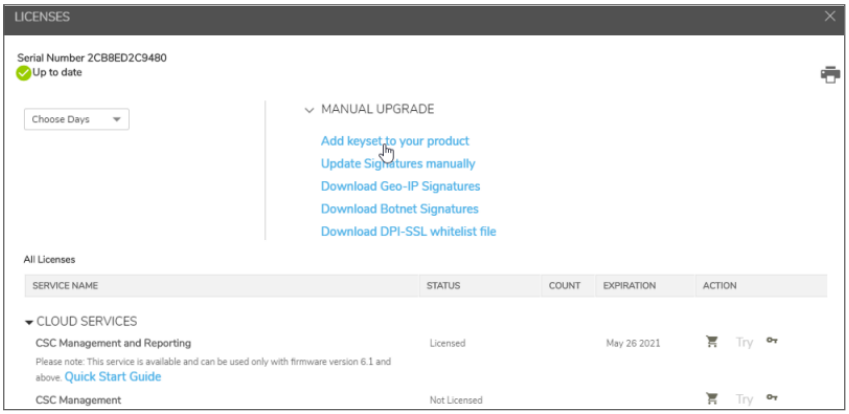
SonicWall セキュリティ装置から直接インターネットに接続することを許可していないセキュリティの高い環境に SonicWall セキュリティ装置を配備している場合は、から暗号化されたライセンス キー情報を入手し、https://mysonicwall.com SonicOS 管理インターフェースの「**デバイス | 設定 > ライセンス**」ページで、手動で入力することができます。

ⓘ **補足:** 暗号化されたライセンス キーセットの手動アップグレードは、閉じた環境専用の機能です。ファイアウォールをインターネットに接続している場合は、装置の自動登録機能およびセキュリティ サービス アップグレード機能を使用することをお勧めします。

インターネットに接続しているコンピュータでステップ 1 ～ 4 を実行してから、インターネット接続していないセキュリティ装置の SonicOS 管理インターフェースで手順を続行する必要があります。

1. 先に進む前に、にアカウントがあることと、https://mysonicwall.com SonicWall セキュリティ装置がそのアカウントに登録されていることを確認してください。
2. MySonicWall にログインした後、「**製品管理 > 製品管理**」に表示されている登録済みの SonicWall セキュリティ装置のシリアル番号を選択します。

3. 「**手動でアップグレード**」を選択し、「**製品にキーセットを追加**」を選択します。暗号化された文字列が表示されます。これは、選択した SonicWall セキュリティ装置と有効化されているセキュリティ サービスについてのライセンス キーセットです。



4. 「**コードをコピー**」を選択して、「**設定 | ライセンス**」ページに貼り付けるキーセットの文字列をコピーします。
5. SonicWall 装置で SonicOS の最新バージョンを実行していることを確認します。
6. 「**デバイス | 設定 > ライセンス**」に移動します。
7. ページの右上にある「**手動ライセンス**」を選択します。
8. 「**手動ライセンス アップグレード**」ダイアログの「キーセットの入力」フィールドにキーセット（手順 3 で作成したもの）を貼り付けます（または入力します）。

9. SonicWall セキュリティ装置を更新するには、「**適用**」を選択します。ページの最下部にある「状況」フィールドには、設定が更新されたことが表示されます。
10. 「**デバイス | 診断 > テクニカル サポート レポート**」からレポートを生成して、アップグレードの詳細を確認できます。

ⓘ **補足:** 手動でアップグレードした後、「**設定 | ライセンス**」ページに登録およびアップグレードの情報は表示されません。

SonicWall 装置の登録

プライマリ装置への初回ログイン時、ソフトウェア取引契約書（STA）が表示されます。これに同意すると先に進むことができます。CLI を使用している場合は、先に進む前に「**Yes**」（はい）を入力（または選択）してください。STA に同意すると、その後、ファームウェアまたはソフトウェアのアップグレードでこれが表示されることはありません。

ⓘ **補足:** MySonicWall の登録情報は、売却されたり、他社と共有されることはありません。

ライセンスの手動適用、ライセンスの手動同期、およびファームウェアのアップグレードの詳細については、お使いのセキュリティ装置の『*クイック スタート ガイド*』を参照してください。

ゲートウェイ アンチウイルス、アンチスパイウェア、および IPS サービスのライセンスの有効化

これらのセキュリティ サービスを利用するには、MySonicWall に装置を登録する必要があります。次を参照してください。「SonicWall 装置の登録」またはお使いのセキュリティ装置の『*クイック スタート ガイド*』を参照してください。

SonicWall アンチスパイウェア は SonicWall ゲートウェイ アンチウイルス、アンチスパイウェア、および 侵入防御 の一部なので、受け取った有効化鍵は SonicWall セキュリティ装置上で 3 つのサービスのいずれにも使用できます。

SonicWall ゲートウェイ アンチウイルス、アンチスパイウェア、および 侵入防御 のライセンスが SonicWall セキュリティ装置で有効化されていない場合は、SonicWall 再販業者または MySonicWall アカウント（米国およびカナダのお客様のみ）からライセンスを購入する必要があります。

無料トライアルの有効化

SonicWallゲートウェイ アンチウイルス、アンチスパイウェア、および 侵入防御の無料トライアル版を試用できます。無料トライアル版のセキュリティ サービス（一部またはすべて）を有効化する方法については、お使いのセキュリティ装置の『*クイック スタート ガイド*』または次を参照してください。「セキュリティ サービスのオンライン管理」。

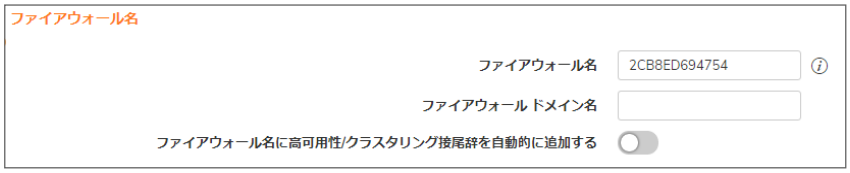
3

システム管理

ファイアウォール名の設定

ファイアウォール名を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**ファイアウォール管理者**」を選択します。



3. 「ファイアウォール名」フィールドに、ファイアウォールの 16 進数のシリアル番号を入力します。この番号は SonicWall セキュリティ装置を一意に識別します。既定の番号はファイアウォールのシリアル番号です。シリアル番号は SonicWall セキュリティ装置の MAC アドレスでもあります。ファイアウォール名を変更するには、「ファイアウォール名」フィールドに英数字で一意の名前を入力します。名前は 8 文字以上の長さにする必要があり、最大 63 文字まで使用できます。
4. 「ファイアウォール ドメイン名」フィールドにわかりやすい名前を入力します。この名前には、プライベートな名前（内部ユーザ向け）を指定することも、外部登録されたドメイン名を指定することもできます。このドメイン名は、ユーザ ウェブ ログイン設定とともに使用されます。
5. イベント ログでプライマリ/セカンダリ ファイアウォールを簡単に確認できるようにするには、「**ファイアウォール名に高可用性/クラスタリング接尾辞を自動的に追加する**」をオンにします。このオプションをオンにすると、「**監視 | ログ > システム ログ**」ページでファイアウォール名の後に適切な接尾辞が自動的に追加されます。

   このオプションは、既定では選択されていません。イベント ログの詳細については、『*SonicOS 7.0 ログ（監視）*』マニュアルを参照してください。

無線 LAN とIPv6 の有効化

無線 LAN や IPv6 の可視性を有効にするには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理 > ファイアウォール管理者**」に移動します。
2. 「**無線 LAN を有効にする**」および/または「**IPv6 を有効にする**」を選択します。これらのオプションは、既定ではオンになっています。確認メッセージが表示されます。

   ⓘ | **重要:** 無線 LAN 機能を有効または無効にするには、ファイアウォールを再起動する必要があります。

   WLAN が無効である場合:

   - アクセス ポイントおよび無線に関連する管理インターフェースのすべてのページは表示されません。
   - WLAN はゾーン種別として表示されません。
   - 既存の WLAN ゾーンまたはオブジェクトは編集できなくなります。

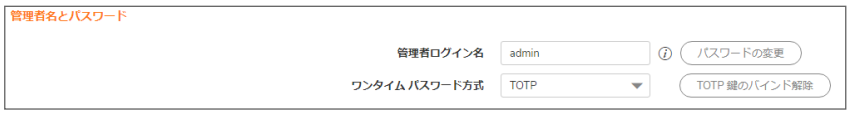
   IPv6 が無効である場合は、すべての IPv6 パケットがファイアウォールによって破棄され、「**監視 | ツールと監視 > パケット監視**」ページにログ メッセージが表示されます。
3. 「**OK**」を選択します。

管理者名とパスワードの変更

各 SonicWall セキュリティ装置には、初期段階で既定の管理者名 admin とパスワード password が設定されています。

管理者の名前やパスワードを変更するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**ファイアウォール管理者**」を選択します。

3. 「管理者ログイン名」フィールドに新しい名前を入力します。
   管理者名は、既定で「admin」に設定されますが、32 文字までの英数字を使用して変更できます。
4. 以下のステップを実行してパスワードを変更するか、ステップ 4 に進みます。
   a. 「**パスワードの変更**」を選択します。
   b. 「古いパスワード」フィールドに古いパスワードを入力します。

c. 「新しいパスワード」フィールドに新しいパスワードを入力します。新しいパスワードは最大 32 文字の英数字および特殊文字にします。

d. 既定のパスワード (password) は、独自の個別パスワードに変更することを推奨します。他人が簡単に推測できない強力なパスワードを入力してください。強力なパスワードは、英字の大文字、小文字、数字、特殊文字をそれぞれ少なくとも 1 文字含めて作成してください。例えば、MyP@ssw0rd と入力します。

e. 「パスワードの確認」フィールドにもう一度新しいパスワードを入力します。

f. 「**適用**」を選択します。

5. 二段階認証を強制するには、「**TOTP**」を「ワンタイム パスワード方式」ドロップダウンから選択します。これで次回ログイン時にモバイル認証アプリケーションとユーザ アカウントをバインドすることができます。

6. 「**適用**」を選択します。

ログイン セキュリティの設定

内部 SonicOS ウェブサーバでは、HTTPS 管理セッションとネゴシエートする場合に、TLS 1.1 以降を強力な暗号 (128 ビット以上) と組み合わせて使うことができます。SSL の実装はサポートされていません。この強化された HTTPS セキュリティにより、潜在的な SSLv2 ロールバックの脆弱性を防御し、PCI (Payment Card Industry) をはじめとするセキュリティおよびリスク管理の標準規格に確実に準拠します。

ヒント: SonicOS は、最新のブラウザがサポートする HTML5 などの先端のブラウザ技術を利用しています。SonicWall では、SonicOS の管理に最新バージョンの Chrome、Firefox、Internet Explorer、または Safari (Windows プラットフォームは対象外) ブラウザを使用することを推奨しています。SonicWall システムの管理には、モバイル デバイスのブラウザは推奨されません。

SonicOS パスワードの制約の強制により、管理者およびユーザが必ず安全性の高いパスワードを使用するように設定できます。このパスワードの制約の強制により、現在の情報セキュリティ管理システムで定義されている機密保持の要件、および情報セキュリティ国際評価基準や PCI (Payment Card Industry) などの標準に準拠するための要件を満たすことができます。

トピック:

- パスワードの準拠の設定
- ログイン制約の設定

パスワードの準拠の設定

パスワードの準拠を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**ログイン / 複数の管理者**」をクリックします。
   「**ログイン セキュリティ**」セクションで、以下のように設定します。
3. 指定した日数が経過するたびにパスワードの変更をユーザに要求するには:
   a. 「**パスワードの強制変更間隔（日数）**」を選択します。フィールドが有効になります。このオプションは、既定では選択されていません。
   b. フィールドに日数を入力します。既定の日数は 90、最小値は 1 日、最大値は 9999 です。

   有効期限の切れたパスワードでログインしようとすると、新しいパスワードの入力を求めるポップアップ ウィンドウが表示されます。「 ユーザ ログイン状況 」ウィンドウには、ユーザがいつでもパスワードを変更できるように「パスワードの変更」ボタンが用意されています。
4. パスワードを変更してから次に変更するまでの最短の期間を時間単位で指定するには:
   a. 「**次の時間を経過後にパスワードを変更する（時間）**」を選択します。フィールドが有効になります。
   b. 時間数を入力します。最小値（既定値）は 1 時間、最大値は 9999 時間です。
5. 指定したパスワード変更回数の範囲で重複しないパスワードを使用することをユーザに要求するには:
   a. 「**同じパスワードの繰り返し使用を禁止する回数**」を選択します。フィールドが有効になります。
   b. 変更回数を入力します。既定値は 4 回、最小値は 1 回、最大値は 32 回です。
6. 新しいパスワードを作成するときに、古いパスワードで使用していたアルファベット、数字、記号の 8 文字以上を変えることをユーザに要求するには、「**Apply password constrains（パスワードの制約を適用する）**」を選択します。使用できる文字を指定する方法については、ステップ 7 を参照してください。
7. パスワードに使用できる最小の長さを指定するには、「最小パスワード長」フィールドに最小文字数を指定します。既定値は **8**、最小値は 1、最大値は 99 です。
8. ユーザのパスワードに要求される複雑さの度合いを「 パスワードの複雑さを強制する 」ドロップダウン メニューで選択します。
   - **なし**（既定）
   - **英数字** – アルファベットと数字を必ず併用
   - **英数字と記号** – アルファベット、数字、記号を必ず併用。記号は !、@、#、$、%、^、&、*、(、および) のみ使用可能であり、それ以外は使用できません
9. 複雑なパスワードの強制オプションとして「なし」以外を選択すると、「 複雑なパスワードの要件 」の下のオプションが選択可能になります。ユーザのパスワードで使用する必要があるアルファベット、数字、記号の最小文字数を入力します。既定の文字数はそれぞれ 0 です。すべてのオプションの文字数の合計は 99 文字以内にする必要があります。
   - 英大文字
   - 英小文字
   - 数字
   - 記号

ⓘ | **補足:**「記号」フィールドは、「**英数字と記号**」を選択した場合のみ有効になります。

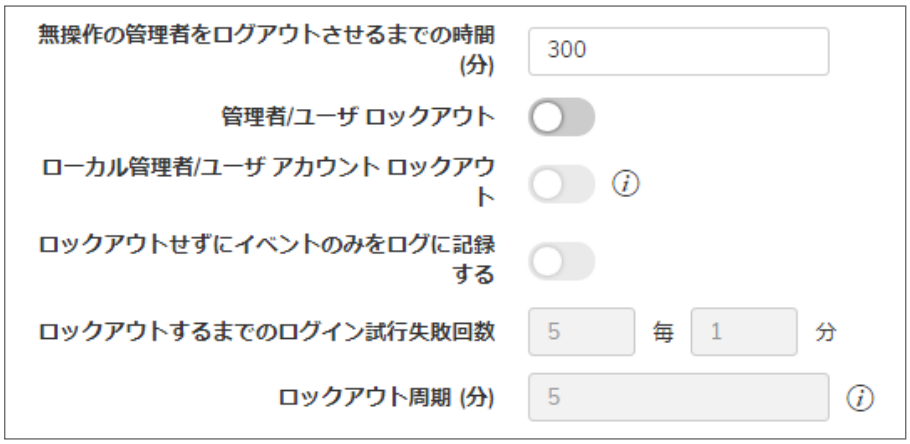
10. パスワード制約を適用するユーザのクラスを「 上記のパスワード制約を以下のユーザに対して適用する:」で選択します。既定では、すべてのオプションが選択されています。
    - **管理** – admin というユーザ名の既定の管理者です。
    - **その他の完全管理者**
    - **制限された管理者**
    - **ゲスト管理者**
    - **その他のローカル ユーザ**

ログイン制約の設定

ログイン制約を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**ログイン / 複数の管理者**」をクリックします。

「**ログイン セキュリティ**」セクションで、以下のように設定します。



1. 無操作時に管理者が管理インターフェースから自動的にログアウトさせられるまでの時間を指定するには、「無操作の管理者をログアウトさせるまでの時間 （分）」フィールドに分単位で時間を入力します。既定では、無動作時間が 5 分経過すると管理者はログアウトさせられます。タイムアウトは 1～9999 分の範囲で指定できます。

   ⓘ | **ヒント:**「無操作の管理者をログアウトさせるまでの時間 (分)」に 5 分を超える時間を設定した場合、ファイアウォールの管理インターフェースへの不正アクセスを防ぐため、各管理セッションを終了するときに必ずビューの右上の「ログアウト」をクリックしてください。

2. ログイン資格情報が正しくない場合に管理者またはユーザをロックアウトするよう SonicWall セキュリティ装置を設定するには、「**管理者/ユーザ ロックアウト**」を有効にします。指定した回数の不正なログイン試行が行われた場合、管理者とユーザの両方がロックアウトされ、ファイアウォールにアクセスできなくなります。このオプションは、既定では無効になっています。このオプションを有効にすると、以下のフィールドが有効になります。

△ **注意: 管理者とユーザが同じ送信元 IP アドレスを使用してファイアウォールにログインしようとすると、管理者もファイアウォールからロックアウトされます。ロックアウトは、ユーザまたは管理者の送信元 IP アドレスに基づいています。**

a. 「**ローカル管理者/ユーザ アカウントのロックアウトを有効にする**（ログイン IP アドレスでロックアウトするには、無効にします）」を選択します。このオプションは、所定の回数を超える不正なログイン試行を受けた場合に、ユーザ アカウントと IP アドレスをロックアウトします。このオプションは、「**管理者/ユーザ ロックアウト**」が有効な場合にのみ使用できます。

b. SonicOS の「**ロックアウトせずにイベントのみをログに記録する**」を選択します。この場合、失敗したユーザ ログイン試行で一定のしきい値に達したものが記録されますが、ユーザまたは IP アドレスはロックアウトされません。このオプションは、「**管理者/ユーザ ロックアウト**」が有効な場合にのみ使用できます。

ユーザまたは IP アドレスがロックアウトされると、"ユーザ ログインが拒否されました – ユーザはロックアウトされています" というメッセージがログイン画面に表示され、ログインが拒否されます。

ⓘ **補足:「ローカル管理者/ユーザ アカウント ロックアウト」が有効になっているときは、「使用中のユーザ」ページで、ロックアウトされたすべてのユーザ アカウントを確認し、編集することができます。**

c. 「1 分間のログイン失敗回数が次の回数になったらロックアウト」フィールドに、ユーザをロックアウトするまでの指定時間内のログイン失敗回数を入力します。既定値は 5、最小値は 1、最大値は 99 です。失敗が許される最大時間を入力します。既定値は 5 分、最小値は 1 分、最大値は 240 分（4 時間）です。

d. 「ロックアウト周期 （分）」フィールドに、ロックアウトされたユーザがファイアウォールに再度ログインできるようになるまでの時間を入力します。既定値は 5 分、最小値は 0 分（無期限のロックアウト）、最大値は 60 分です。

3. 「CLI による最大ログイン試行回数」フィールドに、コマンド ライン インターフェース（CLI）からのログインが何回失敗したらロックアウトするかを指定します。既定値は 5、最小値は 3、最大値は 15 です。
4. 「**適用**」をクリックします。

複数管理者サポート

SonicOS は、完全な管理者権限、読み取り専用権限、制限付きの権限を持つ複数の管理者による同時アクセスをサポートします。これまでのバージョンの SonicOS は、完全な管理者権限でファイアウォールにログオンできる管理者は 1 人だけでした。他のユーザに "制限付き管理者" のアクセス権を付与することはできますが、SonicOS GUI のあらゆる領域を変更できる完全なアクセス権を複数の管理者が同時に持つことはできません。

SonicOS では、複数管理者の同時アクセスがサポートされています。この機能により、複数のユーザが完全な管理者権限でログインできるようになりました。既定の admin ユーザ名に加え、他の管理者ユーザ名を作成できます。複数の管理者が同時に設定を変更することによって競合が生じる可能性もあるため、設定の変更は 1人の管理者にのみ許可されています。その他の管理者には GUI に対する完全なアクセス権が付与されますが、設定を変更することはできません。

複数管理者サポートには、次のようなメリットがあります。

- **生産性の向上**: ファイアウォールに対して複数の管理者が同時にアクセスできるため、装置に対して 2 人の管理者が同時にアクセスした場合に一方の管理者が自動的にシステムからログアウトされる "自動ログアウト" が不要になります。

- **設定リスクの軽減**: 新たに読み取り専用モードが追加されたため、意図しない設定変更を誤って実行してしまうリスクなしに、ファイアウォールの現在の設定と状況を確認することができます。

複数管理者サポートの動作

トピック:

- 構成モード
- ユーザ グループ
- 管理者の先制時に適用される優先順位
- GMS と複数管理者サポート

構成モード

複数の管理者による同時アクセスを許可しつつ、複数の管理者が同時に設定を変更することによって競合が生じることがないように、次の構成モードが定義されています。

構成モード	管理者に設定を編集するための完全な権限が割り当てられます。装置にログインしている管理者がいない場合、完全な管理者権限および制限付き管理者権限を持った（読み取り専用管理者以外の）管理者には自動的に構成モードが適用されます。 ⓘ **補足:** 完全な設定権限を持つ管理者は、コマンド ライン インターフェース（CLI、『*SonicOS 7.0 CLI リファレンス ガイド*』を参照）を使ってログインすることもできます。
読み取り専用モード	管理者は設定に変更を加えることは一切できませんが、管理 UI 全体を表示することや、監視操作を実行することはできます。 SonicWall 読み取り専用管理者ユーザ グループに属する管理者には読み取り専用アクセス権が付与され、他の構成モードにはアクセスできません。
非構成モード	管理者は、読み取り専用グループと同じ情報を閲覧できるほか、設定の競合を引き起こすおそれのない管理操作を実行できます。 非構成モードにアクセスできるのは、SonicWall 管理者ユーザ グループに属する管理者だけです。既に構成モードを利用している管理者が存在するとき、新しい管理者が既存の管理者を先制しなかった場合は、このモードになります。既定では、構成モードを先制された管理者は、非構成モードに切り替わります。「**デバイス	設定 > 管理**」ページでこの動作を変更して、元の管理者がログアウトされるようにすることもできます。

「**各種構成モードにおいて利用可能なアクセス権**」の表は、各構成モードで利用できるアクセス権をまとめたものです。なお、この表には制限付き管理者のアクセス権も記載されていますが、制限付き管理者が利用できる機能の一部が含まれていません。

各種構成モードにおいて利用可能なアクセス権

機能	構成モードでの完全な管理者権限	非構成モードでの完全な管理者権限	読み取り専用管理者	制限付き管理者
証明書のインポート	X			
証明書署名リクエストの生成	X			
証明書のエクスポート	X			
装置の設定のエクスポート	X	X	X	
TSR のダウンロード	X	X	X	
その他の診断の使用	X	X		X
ネットワーク設定	X			X
ARP キャッシュの消去	X	X		X
DHCP サーバの設定	X			
VPN トンネルの再ネゴシエート	X	X		
ユーザのログオフ	X	X		ゲスト ユーザのみ
ロックアウトされたユーザのロック解除	X	X		
ログの消去	X	X		X
ログのフィルタ	X	X	X	X
ログのエクスポート	X	X	X	X
ログの電子メール送信	X	X		X
ログ種別の設定	X	X		X
ログ設定	X			X
ログ レポートの生成	X	X		X
完全な UI の参照	X	X	X	
ログ レポートの生成	X	X		X

ユーザ グループ

複数管理者サポート機能では、次の 2 つの既定ユーザ グループをサポートしています。

- SonicWall 管理者: このグループのメンバーには、設定を編集するための完全な管理者アクセス権が付与されます。
- SonicWall 読み取り専用管理者: このグループのメンバーには、完全な管理インターフェースを閲覧できる読み取り専用アクセス権が付与されます。設定を編集したり、完全な構成モードに切り替えたりすることはできません。

これらの複数のユーザ グループにユーザを追加することはお勧めできません。ただし、そのようにした場合は、次の動作が適用されます。

所属ユーザ グループ	付与される権限
SonicWALL 管理者	制限付き管理者ユーザ グループまたは SonicWall 読み取り専用管理者ユーザ グループにも追加した場合、メンバーには完全な管理者権限が付与されます。
制限付き管理者	SonicWall 読み取り専用管理者ユーザ グループに追加した場合、メンバーには制限付き管理者権限が付与されます。
読み取り専用管理者	その後、別の管理グループに所属させた場合、SonicWall 読み取り専用管理者グループ設定の「この読み取り専用管理者が他の管理グループと共に使用された場合」のオプション次第で、メンバーのアクセスが前と同じく読み取り専用に制限されるか、もう一方のグループで設定された完全な管理者権限が付与されます。

管理者の先制時に適用される優先順位

既に装置にログインしている管理者を先制する場合、各種の管理者区分には、次の規則に従って優先順位が適用されます。

1. **admin** ユーザおよび SonicWall Global Management System (GMS) には、どちらも最も高い優先順位が適用され、すべてのユーザを先制できます。
2. **SonicWall 管理者**ユーザ グループに所属するユーザは、**admin**、SonicWall GMS を除くすべてのユーザを先制できます。
3. **制限付き管理者**ユーザ グループに所属するユーザは、**制限付き管理者**グループの他のメンバーのみを先制できます。

GMS と複数管理者サポート

SonicWall GMS を使用してファイアウォールを管理している場合、GMS は各種のアクティビティ (GMS 管理の IPSec トンネルが正しく作成されたかどうかを確認するなど) を行う関係上、装置にログインする機会が多くなります。GMS はローカル管理者を先制できるため、このような GMS ログインが頻繁に生じることで、装置のローカル管理が困難になる場合があります。

複数管理者アクセスの設定

複数管理者アクセスを設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
   「**ログイン / 複数の管理者**」をクリックします。

2. ある管理者が別の管理者が優先される場合の動作を設定するには、他の管理者が優先される場合の動作 のオプションから、先制された管理者を非構成モードに変換するか、またはログアウトさせるかを選択します。

   - **非構成モードに降格**: 他の管理者によるアクセスを遮断することなく、複数の管理者が非構成モードで装置にアクセスできるようにします。このオプションは、既定では選択されていません。
   - **ログアウト**: 新しい管理者が他のセッションを先制します。

   ⓘ **補足:** 「ログアウト」を選択すると「非構成」モードは無効になり、「非構成モード」に手動で入ることはできなくなります。

3. 指定した時間の経過後に、優先順位の低い管理者が現在の管理者を先制できるようにするには、「無操作の状態が次の時間を経過した場合、低い優先順位の管理者に対して先制を許可する （分）」フィールドに時間を分単位で入力します。既定値は 10 分、最小値は 1 分、最大値は 9999 分です。
4. SonicOS 管理インターフェースは、管理者が管理インターフェースを通じて、同じ装置にログインしている他の管理者にテキスト メッセージを送信できるようにします。メッセージはブラウザのステータス バーに表示されます。このオプションを有効にするには、以下の手順に従います。

   a. 「**管理者間メッセージ**」を選択します。「メッセージング ポーリング間隔（秒）」フィールドが有効になります。

   b. 「メッセージング ポーリング間隔 （秒）」フィールドに、管理者間で送られるメッセージをブラウザがチェックする頻度を指定します。この間隔を適度に短く設定してメッセージの受け渡しがタイミングよく行われるようにしてください。特に、多数の管理者が装置にアクセスする必要があると考えられる場合は、この設定に注意してください。既定値は **10 秒**、最小値は **1 秒**、最大値は **99 秒**です。

5. システム管理者、暗号化管理者、監査管理者によるアクセスを有効にするには、「**複数の管理者の役割**」を選択します。このオプションが無効なとき、これらの管理者はシステムおよび関連するどのユーザ グループにもアクセスできず、それらに関する情報が非表示となります。このオプションは、既定では選択されていません。

拡張監査ログのサポートの有効化

拡張ログ エントリには、「**監視 | ログ > システム イベント**」ページの変更されたパラメータとユーザ名が含まれます。

「監視 | ログ > システム ログ」ページのすべての設定変更がログに記録されるようにするには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**監査 / SonicOS API**」を選択します。
3. 「**拡張監査ログのサポート**」セクションで、「**拡張監査ログ**」を有効にします。

4. 「**適用**」を選択します。

無線 LAN コントローラの設定

無線コントローラ モードを有効にするには、以下の手順に従います。

ⓘ | **重要**: 無線コントローラのモードを変更した後、ファイアウォールを再起動する必要があります。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**監査 / SonicOS API**」を選択します。
3. 「**無線 LAN コントローラ**」セクションで、「**無線コントローラ モード**」ドロップダウン メニューから以下のオプションのいずれか 1 つを選択します。
   - **無線コントローラ専用** (既定)
     無線コントローラ モードを有効にします。
   - **無線なし**
     無線なしコントローラ モードを有効にします。
   - **全機能ゲートウェイ**
     通常のファイアウォール モードを有効にします。

4. 適切な無線コントローラ モードを選択した後で、表示されている警告メッセージ内の「**OK**」を選択します。
5. 「**適用**」を選択します。

SonicOS API の有効化と認証方式の設定

選択した機能を設定する SonicOS コマンド ライン インターフェース (CLI) の代わりに SonicOS API を使用することができます。これを行うには、最初に SonicOS API を有効にする必要があります。SonicOS API の詳細について

は、https://www.sonicwall.com/ja-jp/support/technical-documentation/ で提供されている『*SonicOS 7.0 API* マニュアル』を参照してください。

SonicOS API を有効化してクライアント認証を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**監査 / SonicOS API**」を選択します。
3. 「**SONICOS API**」セクションで、「**SonicOS API**」を有効にします。
4. 初期クライアント認証として以下の認証方式のいずれかを選択します。
    - **RFC-7616 HTTP ダイジェスト アクセス認証**
        - 適切なダイジェスト アルゴリズムを選択します。**SHA256**（既定）、MD5
        - 統合防御: **無効**（既定）、許可、強制
        - セッション別形（パスワードの代わりにパスワード ハッシュ): **無効**、**許可**（既定）、**強制**
    - **CHAP 認証**
    - **RFC-2617 HTTP 基本アクセス認証**
    - **公開鍵認証**
        - **RSA モジュール（鍵/暗号のビット サイズ)**: **2014** が既定の設定です。
        - **RSA パディング種別**: PKCS#1 v1.5 または PKCS#1 v2.0 OAEP
            - OAEP ハッシュ方式: SHA-1、SHA-256、その他
            - OAEP マスク（MGF1）方式: SHA1、SHA-256、その他
        - **RFC-7616 ダイジェスト アクセス認証を使用したセッション保護**
            - クライアントから受け取ったユーザ パスワードを保持できる
            - 最大ノンス使用数: 既定で 10
        - **二段階認証およびベアラトークン認証**
5. 「**適用**」を選択します。

GMS 管理を有効にする

補足: SonicWall グローバル管理システムの詳細については、にある『*SonicWall GMS*』および『*SonicWall 管理サービス*』の管理マニュアルを参照してください。https://www.sonicwall.com/ja-jp/support/technical-documentation.

GMS で管理できるようにセキュリティ装置を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**監査 / SonicOS API**」を選択します。
3. スクロールして、「**より高度な管理**」セクションを見つけます。

4. 「**GMS を使用する管理**」を有効にします。「**設定**」ボタンが使用可能になります。
5. 「**設定**」を選択します。「**GMS 設定**」画面が表示されます。

6. 「GMS ホスト名または IP アドレス」フィールドに GMS コンソールのホスト名または IP アドレスを入力します。
7. 「GMS Syslog サーバ ポート」フィールドにポートを入力します。既定値は **514** です。
8. ログ メッセージの代わりにハートビート状況のみを送信するには、「**ハートビート状況メッセージのみ送信する**」を選択します。

9. ネットワークで NAT を実行しているデバイスの背後に GMS コンソールが配置されている場合、「**NAT デバイス背後の GMS**」を選択します。「**NAT デバイス背後の GMS**」を選択すると、「NAT デバイス IP アドレス」フィールドが有効になります。
10. 「NAT デバイス IP アドレス」フィールドに NAT デバイスの IP アドレスを入力します。
11. 「**管理モード**」ドロップダウン メニューから以下の GMS モードのいずれか 1 つを選択します。
    - **管理用 IPSEC トンネル** – IPsec VPN トンネルを越えた先の GMS 管理コンソールからファイアウォールを管理できます。このオプションを選択した場合は、ステップ 11 に進みます。
    - **既存のトンネル** – GMS 管理サーバとファイアウォールの接続に既存の VPN トンネルを使用します。このオプションを選択した場合は、ステップ 13 に進みます。
    - **HTTPS** – 2 つの IP アドレス（GMS プライマリ エージェントとスタンバイ エージェントの IP アドレス）から HTTPS 管理が可能になります。また、SonicWall ファイアウォールは、3DES とファイアウォール管理者のパスワードを使用して暗号化された Syslog パケットと SNMP トラップも送信します。GMS レポーティング サーバを設定するオプションが表示されます。このオプションを選択した場合は、ステップ 12 に進みます。
12. SonicOS によって値が入力済みの既定の IPsec VPN 設定が表示されます。設定内容を確認します。

    a. 「**暗号化アルゴリズム**」から、適切なアルゴリズムを選択します。
    b. （オプション）「暗号化鍵」フィールドに新しい暗号化鍵を入力します。

方式	鍵
DES	16 進数 16 文字
3DES	16 進数 48 文字

    c. （オプション）「認証鍵」フィールドに新しい認証鍵を入力します。

方式	鍵
MD5	16 進数 32 文字
SHA1	16 進数 40 文字

    d. ステップ 13 に進みます。
13. SonicOS は GMS レポーティング サーバを認識する必要があります。

a. 「**Syslog メッセージを分散 GMS レポーティング サーバに送信する**」を選択します。「GMS レポーティング サーバ IP アドレス」オプションと「GMS レポーティング サーバ ポート」オプションが使用可能になります。

b. 「GMS レポーティング サーバ IP アドレス」フィールドに、GMS サーバの IP アドレスを入力します。

c. 「GMS レポーティング サーバ ポート」フィールドに、GMS サーバのポートを入力します。既定のポートは **514** です。

14. 「**OK**」を選択します。
15. 「**適用**」を選択します。

管理インターフェースの設定

このセクションでは、以下を設定します。

- 管理インターフェースのテーブルを表示する方法。
- 証明書の使用方法。
- 構成モードと非構成モードのどちらで操作するか。
- その他の管理オプション。

トピック:

- HTTP/HTTPS を介した管理
- セキュリティ証明書の選択
- 管理インターフェースのテーブルの制御
- TLS のバージョンの強制
- 構成モードの切り替え
- ブラウザ Cookie の削除
- SSH 管理の設定

HTTP/HTTPS を介した管理

SonicWall セキュリティ装置は HTTP または HTTPS とウェブ ブラウザを使用して管理できます。既定では、HTTPのウェブ ベースの管理は無効です。工場出荷時の設定の SonicOS 管理インターフェースへのログインには HTTPS を使います。

HTTP または HTTPS を介して管理するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. HTTP を介した管理をグローバルに有効化するには、「**ウェブ管理設定**」セクションで「**HTTP を介しての管理を許可する**」を選択します。このオプションは、既定では選択されていません。
4. HTTP の既定ポートはポート **80** ですが、他のポートからアクセスするように設定することもできます。「HTTP ポート」フィールドに、使用するポート番号を入力します。

   ⓘ **重要:** HTTP 管理用に 80 番以外のポートを設定した場合、IP アドレスを使用して SonicWall セキュリティ装置にログインするときにポート番号も入力する必要があります。例えば、ポートを 76 番に設定した場合は、ウェブ ブラウザに "LAN IP アドレス:76" (`http://192.18.16.1:76` など) と入力しなければなりません。

5. HTTPS 管理の既定ポートは **443** です。この既定ポートを変更することによって、SonicWall セキュリティ装置へのログインにセキュリティ層をもう 1 つ追加するには、「HTTPS ポート」フィールドに別のポート番号を入力します。

   ⓘ **重要:** ただし、HTTPS 管理ポートとして別のポートを設定した場合は、IP アドレスを使用して SonicWall セキュリティ装置にログインするときにポート番号も入力する必要があります。例えば、このポートに 700 番を使用する場合、`https://192.18.16.1:700` のようにポート番号と IP アドレスを使用して SonicWall にログインする必要があります。

セキュリティ証明書の選択

セキュリティ証明書は、データ暗号化とセキュア ウェブ サイトを提供します。

セキュリティ証明書の種別を指定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**証明書の選択**」ドロップダウン ボックスから、ウェブサイトで使用する証明書の種別を選択します。

   - 「**自己署名証明書を使用**」を選択した場合、SonicWall セキュリティ装置にログインするごとに新しい証明書をダウンロードすることなく、1 つの証明書を続けて使用できます。このオプションは、既定では選択されています。ステップ 3 に進みます。
   - 「**証明書のインポート**」を選択した場合は、管理インターフェースに対する認証のために「**デバイス | 設定 > 証明書**」ページからインポートした証明書を選択します。確認メッセージが表示されます。
     a. 「OK」を選択します。「**デバイス | 設定 > 証明書**」ページが表示されます。
     b. 次を参照してください。証明書の管理 セクションに移動してください。
4. 「証明書コモン ネーム」フィールドに、ファイアウォールの IP アドレスまたはコモン ネームを入力します。「自己署名証明書を使用」を選択した場合、SonicOS によってファイアウォールの IP アドレスがフィールドに入力されます。
5. 「**適用**」を選択します。

自己署名証明書を再生成するには、以下の手順に従います。

1. 「**デバイス | システム > 管理 > 管理**」に移動します。
2. 「**ウェブ管理設定**」セクションで、「**証明書の再生成**」を選択します。
3. 表示される確認メッセージで、「OK」を選択します。

管理インターフェースのテーブルの制御

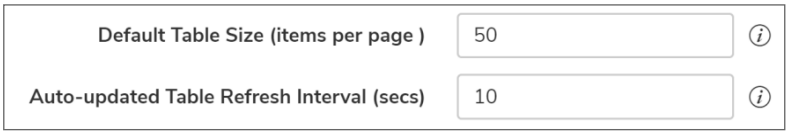
SonicWall 管理インターフェースでは、管理インターフェースのすべてのテーブルにわたるような大きなテーブル情報の表示を次の点で制御できます。

- 1 ページに表示するテーブル エントリの数。
- テーブルをバックグラウンドで自動更新する頻度。

一部のテーブルでは、1 ページあたりの項目数をテーブルごとに個別に設定できます。その個別の設定はログイン時に初期化されて、ここで設定した値になります。これらのページの表示後に項目数を変更しても個別の設定はその場では変化しません。ここで行った変更は次回のログイン時にページの表示に初めて反映されます。

テーブルの表示と更新頻度を変更するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**ウェブ管理設定**」セクションで、
   a. 「既定のテーブル サイズ （1 ページあたりの項目数）」フィールドに、1 ページに表示させる項目数を入力します。最小値は 1、最大値は 5000、既定値は **50** です。
   b. 「自動更新テーブルの再表示間隔 （秒）」フィールドに、再表示させる間隔を秒数で入力します。最小値は 1 秒、最大値は 300 秒、既定値は 10 秒です。



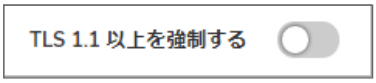
4. 「**適用**」を選択します。

TLS のバージョンの強制

SonicOS は、バージョン 1.0、1.1、および 1.2 の Transport Layer Security（TLS）プロトコルをサポートしています。安全性の高いバージョン 1.1 以上が確実に使用されるようにすることができます。

TLS バージョン 1.1 以上の使用を強制するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**ウェブ管理設定**」セクションで、「**TLS 1.1 以上を強制する**」を有効にします。



4. 「**適用**」を選択します。

構成モードの切り替え

各装置には、管理インターフェースの構成モードを切り替える「モード」オプションがあります。現在は構成モードの場合、いつでも非構成モードに切り替えることができます。現在は非構成モードの場合、構成モードに切り替えることができます。

ヒント:この方法以外に、各ビューの「モード」設定からもモードを切り替えることができます。モードの詳細については、『*SonicOS 7 SonicOS について*』マニュアルを参照してください。

モードを切り替えるには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**ウェブ管理設定**」セクションで、

- 現在は構成モードの場合、「**構成モードの終了**」を選択し、「**OK**」を選択します。
  ページの右上にある「モード」インジケータに「**非構成**」と表示されます。
- 現在は非構成モードの場合、「**構成モード**」を選択します。
  ページの右上にある「モード」インジケータに「**構成**」と表示されます。

ブラウザ Cookie の削除

ⓘ | **重要:** Cookie を削除すると、管理インターフェースで行った未保存のすべての変更が失われます。

セキュリティ装置で保存されたすべてのブラウザ Cookie を削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**Cookie の削除**」を選択します。
4. 「**OK**」を選択します。

SSH 管理の設定

SSH を使用してファイアウォールを管理する場合、セキュリティを強化するために SSH ポートを変更できます。

SSH ポートを変更するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**管理**」を選択します。
3. 「**SSH 管理設定**」までスクロールします。

4. 「SSH ポート」フィールドにポートを入力します。既定の SSH ポートは**22**です。
5. 「**適用**」を選択します。

クライアント証明書の確認

コモン アクセス カード (CAC) を使う場合と使わない場合について、証明書の確認を設定できます。

ⓘ | **補足:** 既定では、どのオプションも選択されていません。

トピック:

- コモン アクセス カードについて
- クライアント証明書の確認の設定
- 「クライアント証明書の確認」の使用
- ユーザ ロックアウトの解決

コモン アクセス カードについて

コモン アクセス カード (CAC) は、米国国防総省 (DoD) のスマート カードです。インターネット上でセキュリティ性の高いアクセスを必要とする軍人その他の政府、非政府機関の職員が使用します。CAC では PKI 認証および暗号化を使用します。

ⓘ | **補足:** CAC を使うには、外付けのカード リーダーを USB ポートに接続する必要があります。

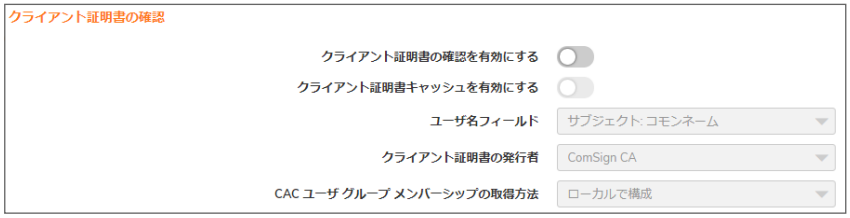
「クライアント証明書の確認」は、一応 CAC を使うことを想定していますが、HTTPS/SSL 接続でクライアント証明書を必要とするどのようなシナリオにも対応しています。クライアント証明書に対する CAC サポートは HTTPS 接続でのみ有効です。

ⓘ | **補足:** CAC は、Microsoft Internet Explorer 以外のブラウザでは機能しない可能性があります。

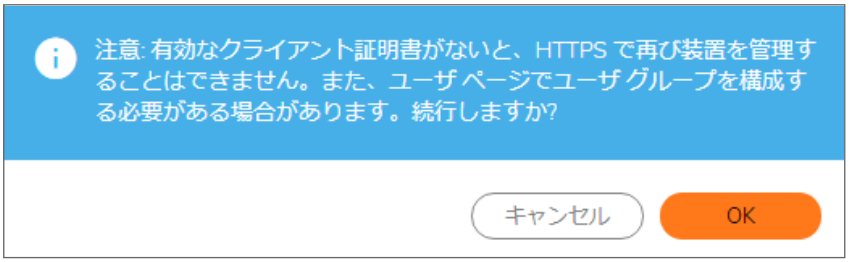
クライアント証明書の確認の設定

クライアント証明書の確認を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**証明書確認**」を選択します。



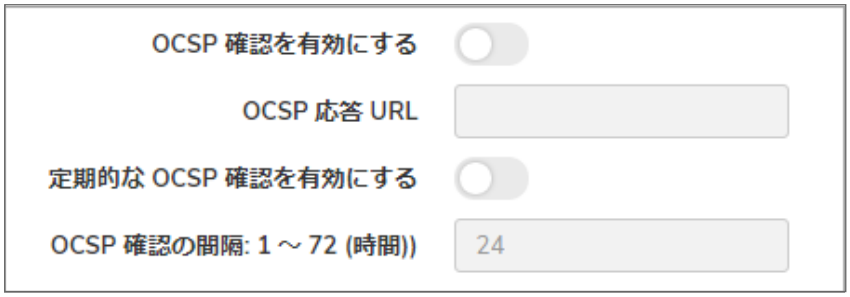
3. SonicWall セキュリティ装置でのクライアント証明書の確認と CAC サポートを有効にするには、「**クライアント証明書の確認を有効にする**」を選択します。このオプションを有効にすると、他のオプションが使用できるようになります。次のような確認の警告メッセージが表示されます。



4. 「**OK**」を選択します。
5. クライアント証明書キャッシュを有効にするには、「**クライアント証明書キャッシュを有効にする**」を選択します。

   ⓘ **補足:** キャッシュの有効期限は有効化後 24 時間です。
6. 証明書のどのフィールドからユーザ名を取得するかを指定するには、「ユーザ名フィールド」からオプションを選択します。ユーザ名フィールド:
   - **件名 :コモンネーム**(既定)
   - **サブジェクト代替名: 電子メール**
   - **サブジェクト代替名: Microsoft ユニバーサル プリンシパル名**
7. 証明機関 (CA) 証明書の発行者を選択するには、「**クライアント証明書の発行者**」ドロップダウン メニューから 1 つを選択します。既定値は「**thawte Primary Root CA – G3**」です。

   ⓘ **補足:** この一覧に目的とする CA がなければ、その CA を SonicWall セキュリティ装置にインポートする必要があります。次を参照してください。証明書の管理 セクションに移動してください。
8. CAC ユーザ グループのメンバーシップを取得する方法を選択するには、「CAC ユーザ グループ メンバーシップの取得方法」ドロップダウン メニューで選択します。これで適切なユーザ権限が決まります。
   - **ローカルで構成** (既定) – これを選択した場合は、適切なメンバーシップを持つローカル ユーザ グループを作成してください。
   - **LDAP から** – これを選択した場合は、LDAP サーバを設定する必要があります (https://www.sonicwall.com/ja-jp/support/technical-documentation/ で提供されている『*SonicOS 7.0 ユーザ*』マニュアルの「*LDAP 用の SonicWALL の設定*」セクションを参照してください)。
9. クライアント証明書がまだ有効で失効していないことを確認するための OCSP (Online Certificate Status Protocol) 確認を有効にするには、「**OCSP 確認を有効にする**」を選択します。このオプションを有効にすると、「 OCSP 応答 URL 」フィールドが表示され、「定期的な OCSP 確認を有効にする」オプションが表示されます。



「OSCP 確認用 URL」フィールドに、クライアント証明書の状況を確認する OCSP サーバの URL を入力します。

OCSP 確認用 URL は、通常はクライアント証明書内に埋め込まれているため、入力する必要はありません。クライアント証明書に OCSP リンクが含まれていない場合は、URL リンクを入力できます。このリンクは、OCSP による確認を行うサーバ側の CGI (Common Gateway Interface) を参照している必要があります。例えば、*http://10.103.63.251/ocsp* です。

10. クライアント証明書がまだ有効で失効していないことを確認するための定期的な OCSP 確認を有効にするには、以下の手順に従います。
    a. 「**定期的な OCSP 確認を有効にする**」を選択します。「**OCSP 確認間隔**」フィールドが使用可能になります。
    b. 「OCSP 確認の間隔: 1 ～ 72 (時間)」フィールドに、OCSP による確認の間隔 (時間) を入力します。最小の間隔は 1 時間、最大の間隔は 72 時間、既定値は **24** 時間です。
11. 「**適用**」を選択します。

「クライアント証明書の確認」の使用

クライアント証明書の確認で CAC を使用しない場合は、ブラウザにクライアント証明書を手動でインポートする必要があります。

クライアント証明書の確認で CAC を使用する場合は、クライアント証明書はミドルウェアによってブラウザに自動的にインストールされます。HTTPS を介して管理セッションを開始すると、証明書の確認を求める証明書選択ウィンドウが表示されます。

ドロップダウン メニューからクライアント証明書を選択した後で、HTTPS/SSL 接続が再開され、SonicWall セキュリティ装置はクライアント証明書が CA によって署名されているかを確認するためにクライアント証明書の発行者を検証します。一致が検出されると、管理者ログイン ページが表示されます。一致が検出されない場合は、ブラウザの接続が失敗したことを示す次のようなメッセージが表示されます。

ウェブ ページを表示できません。

OCSP が有効な場合、管理者ログイン ページが表示される前に、ブラウザによって OCSP 確認が行われ、確認中、次のメッセージが表示されます。

クライアント証明書 OCSP の確認中 . . .

一致が確認されると、管理者ログイン ページが表示され、管理者の資格情報を使って SonicWall セキュリティ装置の管理を開始できます。

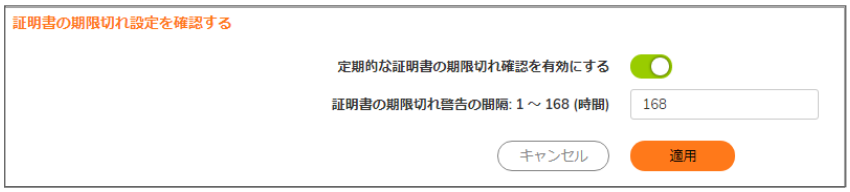
一致が検出されない場合は、ブラウザに次のメッセージが表示されます。

OCSP 確認が失敗しました。システム管理者に問い合わせてください。

証明書の期限切れの確認

証明書の期限切れの定期的な確認を有効にするには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理 > 証明書確認**」に移動します。
2. 「**証明書の期限切れ設定を確認する**」セクションで、「**定期的な証明書の期限切れ確認を有効にする**」を選択します。このオプションは、既定では選択されています。これを有効にすると、「証明書の期限切れ警告の間隔」フィールドが使用可能になります。



3. 証明書を確認する間隔（時間）を設定するには、「証明書の期限切れ警告の間隔： 1 ～ 168 （時間）」フィールドに間隔を入力します。最小の間隔は 1 時間、最大の間隔は 168 時間、既定値は **168** 時間です。
4. 「**適用**」を選択します。

ユーザ ロックアウトの解決

クライアント証明書機能を使う場合、以下の状況で SonicWall セキュリティ装置からユーザがロックアウトされる可能性があります。

- 「**クライアント証明書の確認を有効にする**」が選択されているが、ブラウザにクライアント証明書がインストールされていない。
- 「**クライアント証明書の確認を有効にする**」が選択され、ブラウザにクライアント証明書がインストールされているが、「**クライアント証明書の発行者**」が選択されていない、または誤った**クライアント証明書の発行者**が選択されている。
- 「**OCSP 確認を有効にする**」が有効だが、OCSP サーバが利用できないか、ネットワークの問題で SonicWall セキュリティ装置が OCSP サーバにアクセスできない。

ロックアウトされたユーザへのアクセスを回復するために、次の CLI コマンドが用意されています。

- `web-management client-cert disable`
- `web-management ocsp disable`

言語の選択

ファームウェアに英語以外の言語が含まれている場合は、「言語選択」から言語を選択できます。

ⓘ **補足:** SonicOS 管理インターフェースの言語を変更するには、SonicWall セキュリティ装置を再起動する必要があります。

管理インターフェースの言語を選択するには、以下の手順に従います。

1. 「**デバイス | 設定 > 管理**」に移動します。
2. 「**言語**」を選択します。

3. 「**言語**」セクションの「**言語選択**」ドロップダウン ボックスから適切な言語を選択します。
4. 「**適用**」を選択します。

4

時間の設定

「**デバイス | 設定 > 時間**」ページでは、ログ イベントのタイム スタンプ、SonicWall セキュリティ サービスの自動更新、およびその他の内部の目的に使用する時刻と日付の設定を定義します。

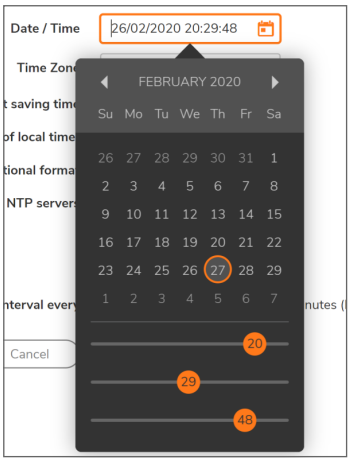
既定では、SonicWall セキュリティ装置は公開 NTP サーバの内部リストを使用して時刻を自動的に更新します。ネットワーク タイム プロトコル (NPT) は、コンピュータのネットワーク内でコンピュータの時刻を同期するために使用されるプロトコルです。NTP は協定世界時 (UTC) を使用してコンピュータの時計をミリ秒の分解能 (場合によってはさらに小さな単位) で同期します。

システム時間の設定

システム時間は、「**デバイス | 設定 > 時間**」ページの「**設定**」画面で設定します。

システム時間を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 時間**」に移動します。
2. 「**設定**」画面で、「**タイム ゾーン**」ドロップダウン リストからタイム ゾーンを選択します。
3. 時刻を自動的に設定するには、内部リストの NTP（ネットワーク タイム プロトコル）サーバを使用することを設定する「**NTP を使用して自動的に時刻を調整する**」をオンにします。このオプションは、既定では選択されています。
4. 時刻を手動で設定するには、以下の手順に従います。
    a. 「**NTP を使用して自動的に時刻を調整する**」をオフにします。「**日付/時刻**」オプションが使用可能になります。
    b. 「**日付/時刻**」フィールド内のカレンダー アイコンをクリックし、カレンダーを表示します。
    c. カレンダーで日付、時、分、秒を選択します。
    d. カレンダーから離れた場所をクリックして、設定を適用します。



5. サマータイムの自動調整を有効にするには、「**自動的にサマータイムを調整する**」を選択します。サマータイムを使用する地域では、このオプションは既定で選択されています。
6. ログ イベントにローカル タイムではなく、協定世界時 (UTC) を使用するには、「**ログに UTC (協定世界時) を使用する**」を選択します。このオプションは、既定では選択されていません。
7. 日が月より前に示される国際形式で日付を表示するには、「**国際形式で時刻を表示する**」を選択します。
8. 内部リストの NTP サーバではなく、手動で入力されたリストの NTP サーバを使用してファイアウォールの時計を設定するには、「**個別 NTP サーバのみ使用する**」を選択します。

   ⓘ **重要:** 1 つ以上の NTP サーバを設定済みである場合に限り、このオプションを選択してください。NTP サーバの詳細については、次を参照してください。NTP の設定。
9. 「**適用**」を選択します。

NTP の設定

ネットワーク タイム プロトコル (NPT) は、コンピュータのネットワーク内でコンピュータの時刻を同期するために使用されるプロトコルです。NTP は協定世界時 (UTC) を使用してコンピュータの時計をミリ秒の分解能 (場合によってはさらに小さな単位) で同期します。

ⓘ **ヒント:** SonicWall セキュリティ装置は NTP サーバの内部リストを使用します。このため、手動による NTP サーバの入力はオプションです。

ユーザ定義 NTP サーバを使用したファイアウォールの時計の更新

ローカル サーバを使用してファイアウォールの時計を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > 時間**」に移動します。
2. 次の説明に従って 1 つ以上の NTP サーバを追加します。NTP サーバの追加。
3. 「**ユーザ定義 NTP サーバのみ使用する**」を選択します（「システム時間の設定」を参照）。このオプションは、既定では選択されていません。
4. NTP サーバがファイアウォールを更新する頻度を設定するには、「**再表示間隔（分）**」に時間間隔を入力します。既定値は **60** 分です。範囲は 5 ～ 99,999 分です。
5. 「**適用**」を選択します。

NTP サーバの追加

ファイアウォールの設定に NTP サーバを追加するには、次の手順に従います。

1. 「**デバイス | 設定 > 時間**」ページの「**NTP サーバ**」タブを選択します。
2. 「**+ 追加**」ボタンを選択します。

   「**NTP サーバの追加**」ダイアログが表示されます。
3. 「**NTP サーバ**」フィールドに、リモート NTP サーバの IP アドレスを入力します。

4. 「**NTP 認証種別**」ドロップダウン リストで、認証種別を選択します。
    a. **認証なし** – 認証は不要であり、以下の 3 つのオプションが淡色表示になります。ステップ 8 に進みます。
    b. **MD5** – 認証は必須であり、以下の 3 つのオプションはアクティブになります。
5. 「信頼鍵番号」フィールドに信頼鍵番号を入力します。最小値は 1 で、最大値は 65535 です。
6. 「鍵番号」フィールドに鍵番号を入力します。最小値は 1 で、最大値は 65535 です。
7. 「パスワード」フィールドにパスワードを入力します。
8. 「**追加**」を選択します。成功メッセージが表示されます。
9. 「**閉じる**」を選択して、「**NTP サーバ**」画面に戻ります。「**NTP サーバ**」テーブルに追加したサーバが表示されます。

NTP サーバ エントリの編集

NTP サーバ エントリを編集するには、以下の手順に従います。

1. 「**デバイス | 設定 > 時間**」ページで「**NTP サーバ**」画面に移動します。
2. 「**NTP サーバ**」テーブルで、その NTP サーバがある行の上にマウス ポインタを置いて、**編集**アイコンを選択します。「**NTP サーバの追加**」ダイアログが開き、サーバの現在の設定が表示されます。
3. 変更を加えます。詳細については、以下を参照してください。NTP サーバの追加。
4. 「**編集**」を選択します。

NTP サーバ エントリの削除

NTP サーバ エントリを削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > 時間**」で「**NTP サーバ**」画面に移動します。
2. 「**NTP サーバ**」テーブルで、その NTP サーバがある行の上にマウス ポインタを置いて、**削除**アイコンを選択します。
3. 「**OK**」を選択します。

複数の NTP サーバを削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > 時間**」で「**NTP サーバ**」画面に移動します。
2. 削除する NTP サーバの横にあるチェックボックスをオンにします。

ⓘ **補足:** すべての NTP サーバを削除するには、「**NTP サーバ**」テーブルのタイトルの横にあるチェックボックスをオンにします。

3. テーブルの右上にある「**削除**」ボタンを選択します。

4. 「**OK**」を選択します。

5

証明書の管理

VPN ポリシーでの証明書の使用を実装するには、有効な CA 証明書をサードパーティの CA サービスから取得する必要があります。有効な CA 証明書を取得したら、ローカル証明書を有効にするために CA 証明書をファイアウォールにインポートします。有効な CA 証明書をファイアウォールにインポートするには、「**デバイス | 設定 > 証明書**」ページを使用します。有効な CA 証明書をインポートしたら、それを使用してローカル証明書を有効にします。

SonicOS は、SonicWall セキュリティ装置に多数の証明書を提供します。これらはビルトイン証明書であり、削除したり設定したりできません。

SonicOS は、ローカルの証明書失効リスト (CRL) をサポートします。これは、発行元の認証局 (CA) によって、有効期限が切れる前に失効され、信頼されなくなったデジタル証明書のリストです。ローカル CRL の詳細については、テクニカル サポートにお問い合わせください。

デジタル証明書について

デジタル証明書は、認証局 (CA) として知られる信頼されるサードパーティによって身元を確認するための電子的な手段です。X.509 v3 証明書規格は暗号化証明書で使用される仕様で、証明書に含める拡張領域を定義できます。SonicWall では、サードパーティ証明書のサポートの一環としてこの規格を実装しています。

サードパーティの CA によって署名され確認された証明書は、IKE (インターネット鍵交換) VPN ポリシーで使用できます。IKE は IPsec VPN ソリューションの重要な部分であり、SA (Security Association) を設定する前にデジタル証明書を使用して相手の機器を認証できます。デジタル証明書を使用しない場合、VPN ユーザは共有鍵または対称鍵を手動で交換して認証する必要があります。デジタル署名を使用する機器またはクライアントは、新しい機器またはクライアントがネットワークに追加されるたびに設定を変更する必要はありません。

一般的な証明書は、データ セクションと署名セクションの 2 つのセクションで構成されます。データ セクションには通常、証明書がサポートする X.509 のバージョン、証明書のシリアル番号、ユーザの公開鍵に関する情報、識別名 (DN)、証明書の有効期間、証明書の利用目的のようなオプション情報などの情報が含まれます。署名セクションには、発行元 CA が使用した暗号化アルゴリズムおよび CA のデジタル署名が含まれます。

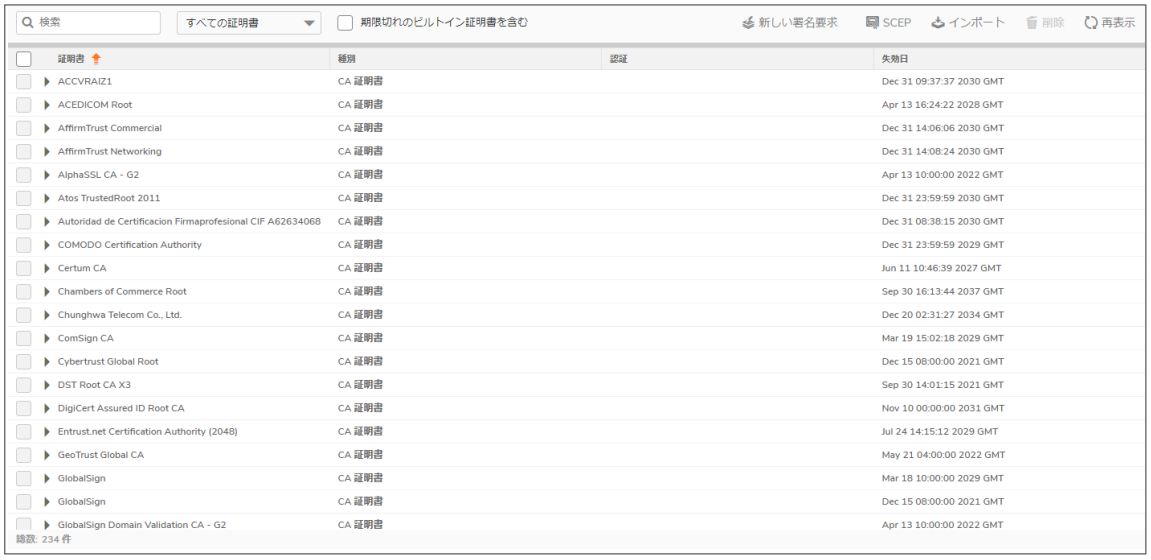
SonicWall セキュリティ装置は、X.509 v3 準拠のすべての証明書発行者と相互運用性があります。SonicWall セキュリティ装置は、以下の CA 証明書ベンダーについてテスト済みです。

- Entrust
- Microsoft
- OpenCA
- OpenSSL と TLS
- VeriSign

トピック:

- 「証明書」テーブルについて
- 証明書のインポート
- 証明書の削除
- 証明書署名リクエストの生成
- 単純証明書登録プロトコルの設定

「証明書」テーブルについて



以下を除く「証明書」ページは、CA 証明書とローカル証明書を管理するためのすべての設定を提供します。

「証明書」ページのテーブルには、証明書に関する次の情報が表示されます。

列	表示される情報
証明書	証明書の名前。
種別	証明書の種別: • CA 証明書 • ローカル証明書 • 要求の保留中
認証	認証情報: • 空白 • 自己署名 • 失効まであと n 日 • 失効
失効日	証明書の期限が切れる日時。

証明書の詳細について

テーブル内の証明書の行を選択すると、その証明書に関する情報が表示されます。証明書の種別によって異なりますが、以下の情報が含まれます。

- **署名アルゴリズム**
- **証明書発行者**
- **サブジェクト識別名**
- **公開鍵アルゴリズム**
- **証明書シリアル番号**
- **有効期間の開始**
- **失効日**
- **CRL 状況（未処理リクエストまたはローカル証明書の場合）**

証明書の種別によって異なる詳細情報「**証明書発行者**」、「**証明書シリアル番号**」、「**有効期間の開始**」、および「**有効期間の終了**」は、証明書の発行者によって生成される情報であるため、未処理リクエストの場合には表示されません。

証明書のインポート

CA サービスによって未処理リクエストの証明書が発行されるか、またはローカル証明書が提供されたら、それをインポートして VPN またはウェブ管理認証で使用できます。CA 証明書をインポートして、IKE ネゴシエーションで使用されるローカル証明書および相手の証明書を確認することもできます。

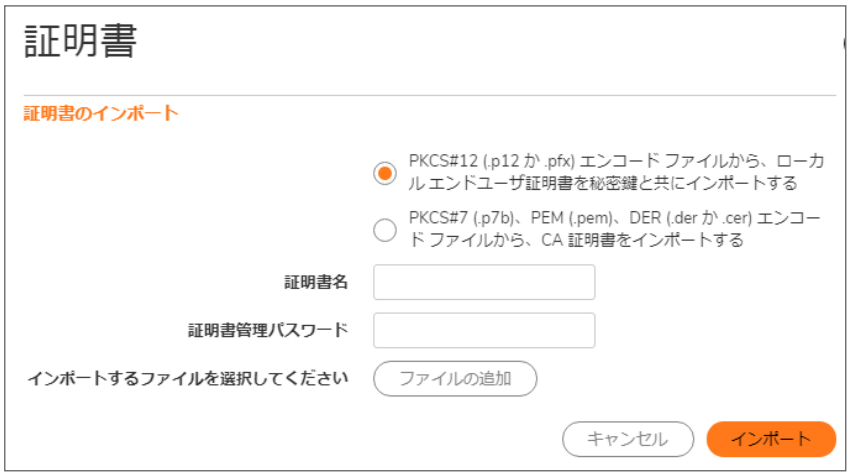
トピック:

- 認証局の証明書のインポート
- ローカル証明書のインポート
- PKCS-12 形式の証明書ファイルの作成（Linux システムのみ）

ローカル証明書のインポート

認証局の証明書をインポートするには、以下の手順に従います。

1. 「**デバイス | 設定 > 証明書**」に移動します。
2. 「**インポート**」を選択します。
   「**証明書のインポート**」ダイアログが表示されます。

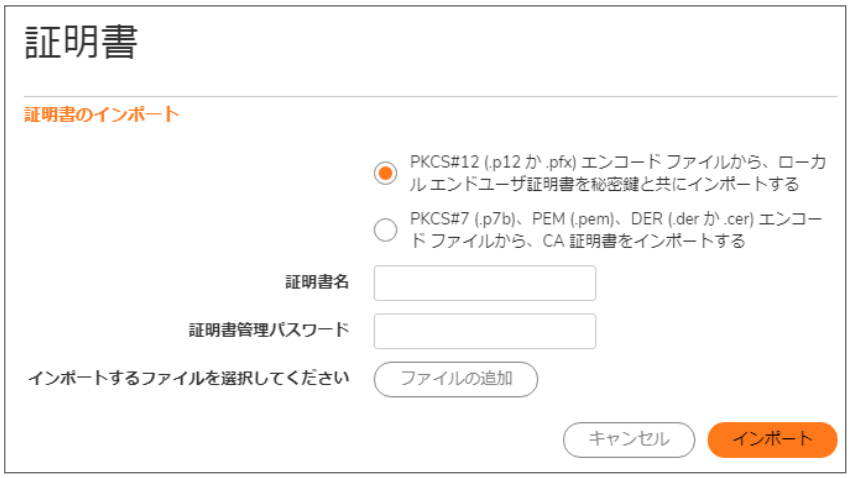


3. 「証明書名」フィールドに証明書の名前を入力します。
4. 「証明書管理パスワード」フィールドに、認証局が PKCS#12 ファイルの暗号化に使用したパスワードを入力します。
5. 「**ファイルの追加**」を選択して証明書ファイルを見つけます。
6. 証明書を選択し、「**開く**」を選択します。
7. 「**インポート**」を選択してファイアウォールに証明書をインポートします。インポートが完了すると、「証明書」テーブルに証明書のエントリが表示されます。
8. 「**証明書**」ページに表示されている証明書を選択し、状況や他の詳細情報を確認します。

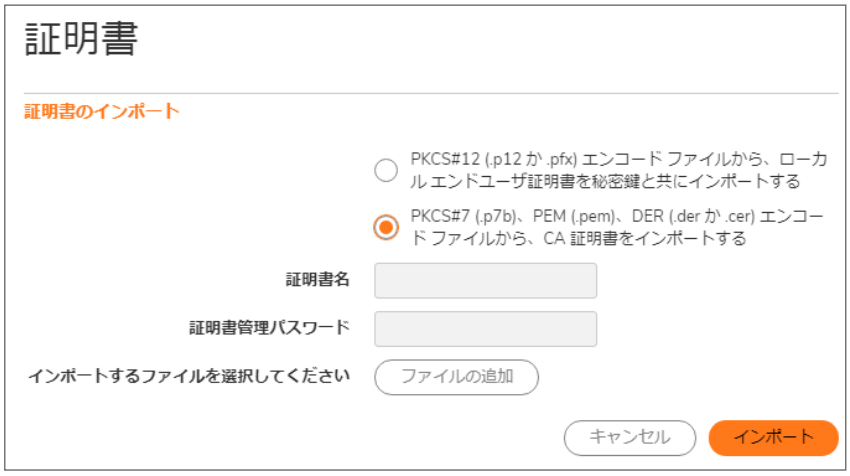
認証局の証明書のインポート

ローカル証明書をインポートするには、以下の手順に従います。

1. 「**デバイス | 設定 > 証明書**」に移動します。
2. 「**インポート**」を選択します。
   「**証明書のインポート**」ダイアログが表示されます。



3. 「**PKCS#7 (.p7b)、PEM (.pem)、DER (.der か .cer) エンコード ファイルから、CA 証明書をインポートする**」を選択します。「証明書のインポート」ダイアログの設定が変わります。



4. 「**ファイルの追加**」を選択して証明書ファイルを見つけます。
5. 「**開く**」を選択します。
6. 「**インポート**」を選択してファイアウォールに証明書をインポートします。インポートが完了すると、「**証明書**」テーブルに証明書のエントリが表示されます。
7. 「**証明書**」ページに表示されている証明書を選択し、状況や他の詳細情報を確認します。

PKCS-12 形式の証明書ファイルの作成 (Linux システムのみ)

PKCS-12 形式の証明書ファイルは Linux システムで OpenSSL により作成できます。PKCS-12 形式の証明書ファイルを作成するには、証明書の次の 2 つの構成要素が必要です。

- 秘密鍵 (通常、拡張子 .key を持つファイル、またはファイル名に単語 "key" を含むファイル)
- 公開鍵を含む証明書 (通常、拡張子 .crt を持つファイル、またはファイル名に単語 "cert" を含むファイル)

例えば、Linux 上の HTTP サーバ Apache では、秘密鍵と証明書は次の場所にあります。

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

これら 2 つのファイルがある状態で、次のコマンドを実行します。

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

この例では、**out.p12** が PKCS-12 形式の証明書ファイルになり、**server.key** と **server.crt** が PEM 形式の秘密鍵および証明書ファイルです。

openssl コマンドを実行した後で、ファイルを保護/暗号化するためのパスワードの入力を求められます。パスワードを選択すると、PKCS-12 形式の証明書ファイルの作成が完了し、装置にインポートできるようになります。

証明書の削除

ⓘ | **補足:** ビルトイン証明書は削除できません。

インポートした証明書は、証明書の期限が切れた場合、または VPN 認証にサードパーティの証明書を使用しない場合に削除できます。作成した証明書はいつでも削除できます。

証明書を削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > 証明書**」に移動します。
2. 証明書の上にマウス ポインタを置き、**削除**アイコンを選択します。

複数のエントリを削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > 証明書**」に移動します。
2. 削除する証明書の横にあるチェックボックスをオンにして、証明書を選択します。

   ⓘ | **ヒント:** すべての証明書を選択するには、見出し行の「**証明書**」列の横にあるチェックボックスをオンにします。
3. テーブルの上部にある**削除**アイコンを選択します。

証明書署名リクエストの生成

ローカル証明書とともに使用する証明書ポリシーを作成する必要があります。証明書ポリシーは、証明書を検証するために必要な認証要件および認証制限を定めます。

証明書署名リクエストを生成するには、以下の手順に従います。

1. 「**デバイス | 設定 > 証明書**」に移動します。
2. 「**新しい署名リクエスト**」を選択します。「**証明書**」ダイアログが表示されます。

3. 「証明書名」フィールドに証明書のエイリアス名を入力します。
4. 以下の表に示すドロップダウン メニューを使用して識別名 (DN) を作成し、関連フィールドに証明書の情報を入力します。

   ⓘ **補足:** DN ごとに、関連ドロップダウン メニューから国を選択できます。他のすべての構成要素については、関連フィールドに情報を入力します。

ドロップダウン メニュー	適切な情報を選択
国	国名（既定） 都道府県 住所 会社名または組織
都道府県	国 都道府県（既定） 住所 会社名または組織 部署
住所	住所（既定） 会社名または組織 部署 グループ チーム
会社名または組織	会社名または組織（既定） 部署 グループ チーム コモン ネーム シリアル番号 電子メール アドレス
部署	部署（既定） グループ チーム コモン ネーム シリアル番号 電子メール アドレス
グループ	グループ（既定） チーム コモン ネーム シリアル番号 電子メール アドレス
チーム	チーム（既定） コモン ネーム シリアル番号 電子メール アドレス
コモン ネーム	コモンネーム（既定） シリアル番号 電子メール アドレス

構成要素の情報を入力すると、「**サブジェクト識別名**」フィールドに識別名 (DN) が生成されます。

5. 必要に応じて、ドロップダウン メニューから種別を選択した後で、証明書に以下のサブジェクト代替名を付けることもできます。
   - **ドメイン名**
   - **電子メール アドレス**
   - **IPv4 アドレス**
6. 「 署名アルゴリズム 」ドロップダウン メニューから署名アルゴリズムを選択します。
   - **SHA1** (既定)
   - **MD5**
   - **SHA256**
   - **SHA384**
   - **SHA512**
7. 「 サブジェクト鍵種別 」ドロップダウン メニューからサブジェクト鍵を選択します。

RSA (既定)	データを暗号化するために使用される公開鍵暗号化アルゴリズム。
ECDSA	高強度鍵ビット単位セキュリティを確保する Elliptic Curve Digital Signature Algorithm (楕円曲線デジタル署名アルゴリズム) を使用してデータを暗号化します。

8. 「**サブジェクト鍵サイズ/曲線**」ドロップダウン メニューで、サブジェクト鍵サイズまたは曲線を選択します。

ⓘ **補足:** 認証局はすべての鍵サイズまたは曲線をサポートするわけではないので、認証局がサポートする鍵サイズや曲線を確認する必要があります。

選択した鍵種別が

RSA の場合は鍵サイズを選択	ECDSA の場合は曲線を選択
1024 ビット（既定）	prime256vi: 256 ビット素体を超える X9.62/SECG 曲線（既定）
1536 ビット	secp384r1: 384 ビット素体を超える NIST/SECG 曲線
2048 ビット	secp521r1: 521 ビット素体を超える NIST/SECG 曲線
4096 ビット	

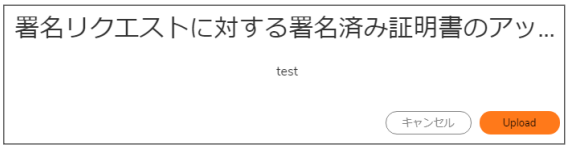
9. 「**生成**」を選択して証明書署名リクエスト ファイルを生成します。

   証明書署名リクエストが生成されると、結果を示すメッセージが表示され、新しいエントリが「証明書」テーブルに「**未処理の要求**」という種別で表示されます。

10. **エクスポート** アイコンを選択します。「**証明書署名リクエストのエクスポート**」ダイアログが表示されます。

11. **エクスポート** アイコンを選択して、コンピュータにファイルをダウンロードします。「**<certificate> を開く**」ダイアログが表示されます。
12. 「**OK**」を選択して、コンピュータ上のディレクトリにファイルを保存します。

    これで、検証のために認証局に送信できる「**証明書署名リクエスト**」が生成されました。
13. 署名リクエストに対する署名済み証明書をアップロードするために、**アップロード** アイコンを選択します。「**証明書のアップロード**」ダイアログが表示されます。



14. 「**ファイルの選択**」をクリックして、ファイルを選択します。
15. ファイルを選択し、「**開く**」を選択します。
16. 「**アップロード**」を選択します。

単純証明書登録プロトコルの設定

単純証明書登録プロトコル（SCEP）は、拡張性に優れた手法でネットワーク機器への証明書の保護された発行をサポートするように設計されています。SCEP に対して、2 つの登録シナリオがあります。

- SCEP サーバ CA が自動的に証明書を発行する。
- SCEP 要求が PENDING に設定されて、CA 管理者が手動で証明書を発行する

SCEP の詳細については、http://tools.ietf.org/html/draft-nourse-scep-18 (Cisco Systems の単純証明書登録プロトコル draft-nourse-scep-18) を参照してください。

証明書の発行に SCEP を使うには、以下の手順に従います。

1. 次の説明に従って、署名リクエストを生成します。証明書署名リクエストの生成。
2. 「**証明書**」ページで、「**SCEP**」を選択します。
   「**SCEP 構成**」ダイアログが表示されます。

3. 「**CSR リスト**」では、既定の CSR リストが SonicOS によって自動的に選択されます。複数の CSR リストが設定されている場合は、これを変更できます。
4. 「CA URL」フィールドに、認証局の URL を入力します。
5. 「チャレンジ パスワード (オプション)」フィールドに、要求されている場合は CA のパスワードを入力します。
6. 「要求回数」フィールドに、リクエストの回数を入力します。既定値は **256** です。
7. 「ポーリング間隔 (秒)」フィールドで、ポーリング メッセージの送信間隔の既定値 (秒単位) を変更できます。既定値は 30 秒です。
8. 「最大ポーリング時間 (秒)」フィールドで、ファイアウォールがポーリング メッセージへの応答をタイムアウトまで待つ間隔の秒数を既定値から変更できます。既定値は 28800 秒 (8 時間) です。
9. 「**SCEP**」を選択して、SCEP 登録を提出します。
   ファイアウォールは証明書をリクエストするために CA に接触します。これにかかる時間は、CA が証明書を自動または手動のどちらで発行するかに依存します。発行された証明書は、「**デバイス | 設定 > 証明書**」ページの「インポートした証明書とリクエスト」または「すべての証明書」種別の利用可能な証明書リスト内に表示されます。

6

SNMP の管理

SonicWall セキュリティ装置を、SNMP または SonicWall グローバル管理システム (GMS) を用いて管理することができます。このセクションでは、SNMP を使って SonicWall を管理するように設定する方法を説明します。GMS を用いた SonicWall 装置の管理の詳細については、https://www.sonicwall.com/ja-jp/support/technical-documentation/ にある *SonicWall GMS および SonicWall 管理サービス*の管理マニュアルを参照してください。

トピック:

SNMP について

SNMP (Simple Network Management Protocol) は UDP (User Datagram Protocol) 上で使用されるネットワーク プロトコルです。ネットワーク管理者は SNMP を利用して SonicWall セキュリティ装置の状態を監視したり、ネットワーク上で重大なイベントが発生した際に通知を受信したりできます。SonicWall セキュリティ装置は、SNMP v1/v2c/v3 および関連するすべての Management Information Base II (MIB-II) グループ (**egp**、**at** 以外) をサポートしています。

SNMPv3 は、以前のバージョンの SNMP を拡張で、パケットの認証と暗号化の組み合わせによってネットワーク機器への保護されたアクセスを提供します。

パケット セキュリティは以下で提供されます。

- **メッセージの完全性** – 通信中にパケットが改ざんされていないことを保証します。
- **認証** – メッセージが正しい送信元からのものであることを確認します。
- **暗号化** – パケットの内容を難読化して、権限の無い送信元によって参照されることを防ぎます。

SNMPv3 はセキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルはユーザとユーザが所属するグループ間で設定される認証方式です。セキュリティ レベルは与えられたセキュリティ モデルで許可されるセキュリティのレベルです。セキュリティ モデルとそれに関連したセキュリティ レベルによって、SNMP パケットの処理方法が決定されます。SNMPv3 は追加レベルの認証と秘匿に加え、追加の承認とアクセス制御を提供します。

SNMP のバージョンに基づくセキュリティ レベル、認証、および暗号化 – 異なるバージョンの SNMP によってどのようにセキュリティ レベル、認証、および暗号化が処理されるかを示しています。

SNMP のバージョンに基づくセキュリティ レベル、認証、および暗号化

バージョン	レベル	認証種別	暗号化	認証方式
v1	noAuthNoPriv	コミュニティ文字列	無	コミュニティ文字列照合
v2c	noAuthNoPriv	コミュニティ文字列	無	コミュニティ文字列照合
	noAuthNoPriv	ユーザ名	無	ユーザ名照合
	authNoPriv	MD5 または SHA	無	HMAC-MD5 または HMSC-SRA アルゴリズムに基づいた認証。
v3	authPriv	MD5 または SHA	DES または AES	HMAC-MD5 または HMSC-SRA アルゴリズムに基づいた認証。CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化、および AES 128 ビット暗号化も提供。

SonicWall セキュリティ装置は任意のインターフェースを使って MIB-II 用の SNMP `Get` コマンドに応答し、トラップ メッセージ生成のための個別 SonicWall MIB をサポートします。個別 SonicWall MIB は SonicWall のウェブ サイトからダウンロードでき、HP Openview、Tivoli、SNMPC などのサードパーティ製 SNMP 管理ソフトウェアにロードできます。

管理者は SNMP の設定を表示および設定できます。ユーザは設定の参照や編集ができません。SNMPv3 はユーザまたはグループ レベルで編集可能です。アクセス ビューは読取り、書込み、またその両方にすることが可能で、ユーザやグループに割り当て可能です。単一のビューがそれに関連する複数のオブジェクト ID (OID) を持つことが可能です。

SNMPv3 エンジン ID に対する SNMPv3 設定は、「**SNMP ビュー構成**」ダイアログの「**一般**」メニュー内で設定できます。この**エンジン ID** は、受信した SNMP パケットの承認に使われます。一致したパケット エンジン ID だけが処理されます。

SNMP アクセスの設定

SNMP の設定は以下の作業で構成されます。

- SNMP アクセスの有効化と設定
- SNMPv3 グループとアクセスの設定

SNMP アクセスの有効化と設定

SNMPv1/v2 両方の基本的な機能を使うことも、より高機能な SNMPv3 オプションを使うように SonicWall セキュリティ装置を設定することも可能です。

SNMP を使用するには、まず SNMP を有効にします。

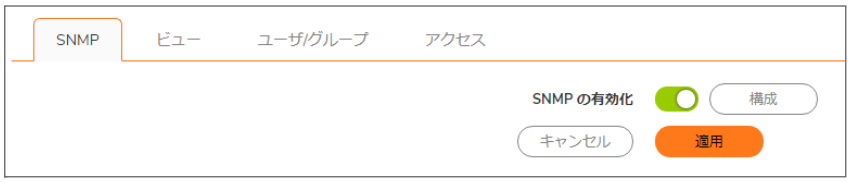
トピック:

- 基本的な機能の設定
- SNMPv3 エンジン ID の設定
- SNMPv3 ビューに対するオブジェクト ID の設定
- グループの作成とユーザおよびアクセスの追加
- アクセスの追加

基本的な機能の設定

SNMP を有効にするには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**SNMP の有効化**」を選択します。既定では、SNMP は無効になっています。



3. 「**適用**」を選択します。SNMP 情報が SNMP ページに設定され、「設定」が使用可能になります。
4. SNMP インターフェースを設定するには、「**設定**」を選択します。「**SNMP ビュー構成**」ダイアログが表示されます。

5. 「**一般**」ページで、「システム名」フィールドに セキュリティ装置のホスト名を入力します。
6. (オプション)「システムの連絡先」フィールドにネットワーク管理者の名前を入力します。

7. (オプション)「システムの場所」フィールドに電子メール アドレス、電話番号、またはポケットベル番号を入力します。
8. SNMPv3 設定オプションを使用する場合は、「資産番号」フィールドに資産番号を入力します。それ以外の場合、このフィールドはオプションです。
9. 「Get コミュニティ名」フィールドに SNMP データを参照できる管理者のグループまたはコミュニティの名前を入力します。
10. (オプション)「Trap コミュニティ名」フィールドに SNMP トラップを参照できる管理者のグループまたはコミュニティの名前を入力します。
11. 「ホスト 1」から「ホスト n」のフィールドに SNMP トラップを受信する SNMP 管理システムの IP アドレスまたはホスト名を入力します。少なくとも 1 つの IP アドレスまたはホスト名を設定する必要があります。ただし、設定できる数は、システムでのアドレス数またはホスト名の最大数が上限になります。
12. 次のようにします。
    - SNMPV3 を設定するには、「」に進みます。SNMPv3 エンジン ID の設定 。
    - 現時点での SNMP の設定が完了した場合は、「**追加**」を選択します。

SNMPv3 エンジン ID の設定

SNMPv3 を使用する場合は、SNMPv3 エンジン ID と SNMP 優先順位を設定できます。SNMPv3 エンジン ID を設定すると、SNMP 管理のセキュリティが最大限に強化されます。

SNMPv3 エンジン ID を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. システムの SNMP をまだ設定していない場合は、「基本機能の設定」のステップ 1 ～ ステップ 11 に従います。
3. 「**詳細**」を選択します。

4. 「**SNMPv3 を必須にする**」を選択します。これによって SNMPv1/v2 が無効になり、SNMPv3 アクセスのみが可能になるため、SNMP 管理のセキュリティが最大限に強化されます。

   ⓘ **重要:** このオプションを選択する場合、「**OK**」を選択する前に、「**一般**」ページでアセット番号を指定する必要があります。
5. 「エンジン ID」フィールドに 16 進のエンジン ID 番号を入力します。

このフィールドは SonicOS によって自動で入力されますが、変更できます。この番号は受信した SNMP パケットと照合されて、パケット処理の承認に使われます。エンジン ID がこの番号と一致したパケットのみが処理されます。

6. 必要に応じて、「**SNMP サブシステムの優先順位を上げる**」を有効にします。
   システムの処理を効率化するために、特定の処理が SNMP クエリへの応答よりも優先されることがあります。このオプションを有効にすると、SNMP サブシステムの応答と処理が常に高いシステム優先順位で行われるようになります。
   ⓘ | **重要**:このオプションを有効にすると、システム全体のパフォーマンスに影響が生じることがあります。
7. 「**OK**」を選択します。パケット処理で SNMPv3 セキュリティ オプションが使用されるようになります。

SNMPv3 ビューに対するオブジェクト ID の設定

SNMPv3 ビューはユーザまたはグループに対するアクセス設定を示します。ユーザとグループの設定は管理者が作成します。これらのセキュリティ設定はユーザには変更できません。SNMPv3 ビューはオブジェクト ID (OID) とオブジェクト ID グループを定義し、SNMPv3 アクセス オブジェクトと呼ばれることもあります。

この SNMP ビューは、OID と OID グループの集合を定義します。最初の既定ビューのセットは、変更または削除できません。既定ビューはルート ビュー、システム ビュー、IP、インターフェース、その他最もよく使われるビューを提供します。これらのビューの OID は事前割当済みです。

さらに、特定のユーザやグループに対して個別のビューを作成できます。

管理者は自分が作成したビューを変更できます。システムが作成したビューは変更できません。

SNMPv3 ビューの OID を設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**ビュー**」を選択します。

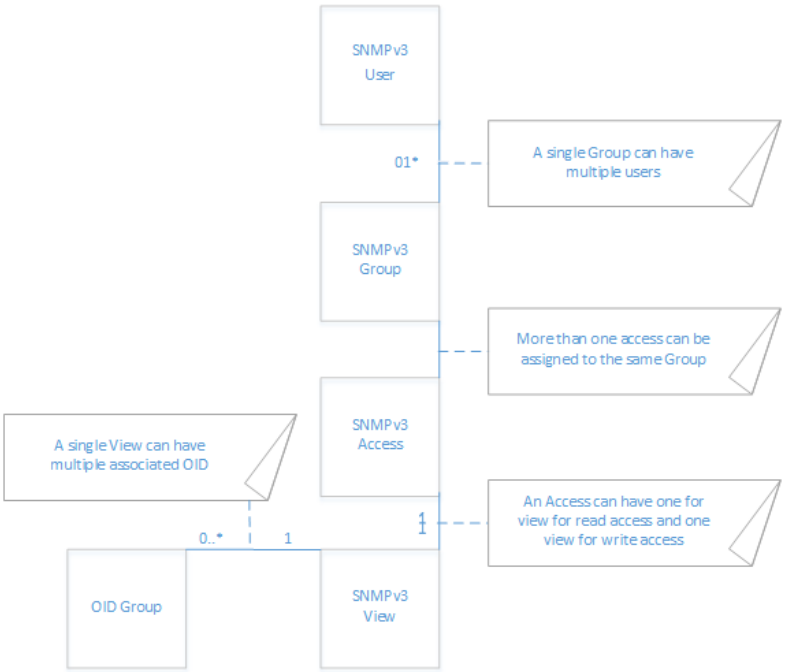
3. 「ビュー」ページで、「**+ 追加**」を選択します。「**ビュー名**」ダイアログ ボックスが表示されます。

4. 「ビュー名」フィールドにわかりやすい名前を入力します。

5. 「**OID の追加**」を選択して、作成されたビューに OID を追加します。「**SNMP OID の追加**」ダイアログが表示されます。
6. 「OID 名」フィールドに名前を入力し、「**OK**」を選択します。
   ビュー名に関連付けられた OID が「OID」テーブルに表示されます。「OID 一覧」から OID を削除するには、OID の上にマウス ポインタを置いて「削除」を選択します。
7. さらに OID を追加してビューに関連付けます。
8. 「**OK**」を選択します。「ビュー」ページに新しいビューが表示されます。

SNMPv3 グループとアクセスの設定

SNMPv3 では、グループとアクセスを設定し、異なるレベルのセキュリティを割り当てることが可能です。オブジェクト ID を種々の許可レベルに関連付け、単一のビューを複数のオブジェクトに割り当てることが可能です。「SNMPv3 グループとユーザ アクセス」は、グループとユーザのアクセスが、これらのさまざまな許可レベルにどのように関連付けられるかを示しています。



グループの作成とユーザおよびアクセスの追加

トピック:

- グループの作成
- ユーザの追加
- アクセスの追加

グループの作 成

グループを作成するには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**ユーザ/グループ**」を選択します。
3. 「**グループの追加**」をクリックします。

4. 「**SNMP グループの追加**」ダイアログで、「グループ名 」フィールドに名前を入力します。
   グループ名は英数字 32 文字までで指定します。
5. 「**OK**」を選択します。
   「**ユーザ/グループ**」ページのテーブルが更新され、新規追加したグループが表示されます。

アクセスの追 加

SNMPv3 アクセスは以下のようなオブジェクトです。

- SNMPv3 ビューの読み/書きアクセス権を定義します。
- SNMPv3 グループに割り当てることができます。

複数のグループを同一のアクセス オブジェクトに割り当てることが可能です。アクセス オブジェクトはまた、割り当てられた複数のビューを持つことが可能です。

アクセス オブジェクトを作成するには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**アクセス**」を選択します。
3. 「**+ 追加**」を選択します。
   「**アクセス名**」ダイアログが表示されます。

4. 「アクセス名」フィールドにわかりやすい名前を入力します。
5. 「**読込ビュー**」で、利用可能なビューのリストからビューを選択します。
6. 「**マスター SNMPv3 グループ**」で、利用可能なグループのリストからグループを選択します。

   ⓘ **補足:** アクセスは、1 つの SNMPv3 グループにのみ割り当てることができます。ただし、グループを複数のアクセス オブジェクトに関連付けることはできます。
7. アクセス セキュリティ強度セキュリティ レベルを選択します。
   - **なし**
   - **認証のみ**
   - **認証とプライバシー**
8. 「**OK**」を選択します。「アクセス」ページのテーブルにアクセス オブジェクトが追加されます。」ページでアクセスできます。

ユーザの追 加

ユーザを追加するには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**ユーザ/グループ**」を選択します。
3. 「**名前の追加**」を選択します。

4. 「**ユーザ名**」フィールドにユーザ名を入力します。
5. 「セキュリティレベル」から次のいずれかのセキュリティレベルを選択します。
    - **なし**（既定）
    - **認証のみ** – 次の 2 つの新しいオプションが表示されます。
        - **認証方式** – 認証方式として「MD5」または「SHA1」を選択します。
        - **認証鍵** – フィールドに認証鍵を入力します。この鍵には、印字可能な 8 ～ 32 文字の任意の文字列を指定できます。
    - **認証とプライバシー** – 次のようにさらに多くのオプションが表示されます。
        - 「 暗号化方式 」ドロップダウン メニューから暗号化方式 「AES」または「DES」を選択します。
        - 「暗号鍵」フィールドに暗号化鍵を入力します。この鍵には、印字可能な 8 ～ 32 文字の任意の文字列を指定できます。
6. 「**グループ**」ドロップダウン ボックスからグループを選択します。
7. 「**OK**」を選択します。ユーザが「ユーザ/グループ」テーブルに追加され、適切なグループに追加されます。

SNMP のサービスとしての設定およびルールの追加

既定で、SNMP は SonicWall セキュリティ装置上で無効になっています。SNMP を有効にするには、最初に「**デバイス | 設定 > SNMP**」ページで SNMP を有効にし、次に個々のインターフェースに対して有効にします。これを実行するには、「**ネットワーク | システム > インターフェース**」ページに移動して、SNMP を有効化するようにインターフェースを編集します。SNMP のサービスとしての設定およびルールの追加の詳細については、『*SonicOS 7.0 システム*』マニュアルの「*インターフェースの構成*」セクションを参照してください。

SNMP 管理システムが自動検出をサポートしている場合は、SonicWall セキュリティ装置エージェントがネットワーク上の SonicWall セキュリティ装置を自動検出します。サポートしていない場合、SNMP 管理システム上の SNMP 管理機器のリストに SonicWall セキュリティ装置を追加する必要があります。

7

ファームウェア設 定

トピック:

- ファームウェアの管理とバックアップ
- バックアップ ファームウェア イメージの作成
- ファームウェアの更新
- 設定のインポートとエクスポート
- ファームウェアとバックアップの設定

ファームウェアの管 理とバックアップ

「**デバイス | 設定 > ファームウェアと設定**」ページは、ファームウェアの簡単なアップグレードおよび設定管理を可能にする設定を提供します。

「ファームウェアの管理とバックアップ」ページでは、以下の操作が可能です。

- バックアップの作成とスケジュール（次を参照）。バックアップ ファームウェア イメージの作成。
- ローカル バックアップやクラウド バックアップの表示（次を参照）。バックアップ ファームウェア イメージの作成
- 一覧中のバックアップの検索（次を参照）。テーブルの検索。
- 構成のインポートとエクスポート（次を参照）。設定のインポート と 設定のエクスポート。
- ファームウェア イメージおよびシステム設定のアップロード（次を参照）。ファームウェアの更新。
- 各設定の構成（次を参照）ファームウェアとバックアップの設定。
- 選択したファームウェアおよびシステム設定での起動（次を参照）ファームウェアの更新。

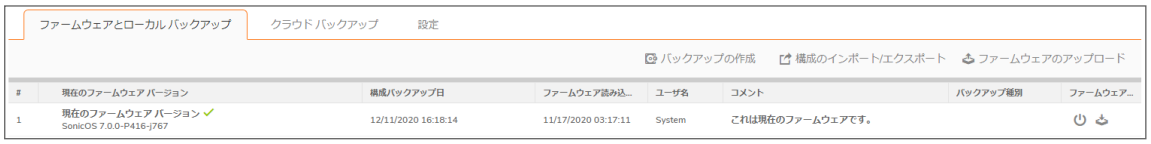
「ファームウェアの管 理とバックアップ」テーブル

トピック:

- 「ローカル」テーブル
- 「クラウド」テーブル
- 「設定ファイルの表示」テーブル

「ローカル」テーブル

「ファームウェアの管理とバックアップ」テーブルの「ローカル」セクションには、次の情報が表示されます。



- **ファームウェア バージョン** – ファイアウォールに現在ロードされているファームウェア。
- **ファームウェア読み込み日** – ファームウェアが装置にインストールされた日時。
- **ファームウェア ビルド日** – ファームウェアが作成された日時。
- **構成日** – 装置の構成が最後に更新された日時。
- **ユーザ名** – ファームウェアをインストールまたは更新したユーザ。
- **コメント** – マウス ポインタを合わせるとファームウェアまたはバックアップ ファイルの情報を表示する情報アイコン。バックアップの作成時にコメントを指定しなかった場合は、次の既定のコメントが表示されます。
  - これは現在のファームウェアです
  - これはローカル バックアップです
  - ユーザ定義コメント
- **起動** – 起動アイコンを選択すると、ファイアウォールの再起動時に現在の設定と工場出荷時の既定の設定のどちらが使われるかが表示されます。

△ **注意: ファームウェア イメージの隣にある「起動」を選択すると、現在のファームウェア イメージが上書きされて、上書き後のイメージが「現在のファームウェア」イメージになります。**

△ **注意: ファイアウォールにファームウェアをアップロードするときには、ウェブ ブラウザを閉じたり、リンクを選択したり、新しいページをロードしたりして、ウェブ ブラウザを中断しないでください。ウェブ ブラウザを中断すると、ファームウェアが破損することがあります。**

- **ファームウェアの動作** – ダウンロード アイコンが表示されます。このアイコンを選択すると、お使いのコンピュータまたはネットワーク上の新しい場所にファームウェアが保存されます。別の場所に保存できるのは、アップロードしたファームウェアのみです。

「クラウド」テーブル

「**ファームウェアと設定**」ページの「**クラウド**」テーブルには、次の情報が表示されます。

- **ファームウェア バージョン** – クラウドにバックアップされたファームウェア。ファームウェアごとに最高 3 バージョンまでリストされます。
- **ファームウェア読み込み日** – ファームウェアが装置にインストールされた日時。
- **ファームウェア ビルド日** – ファームウェアが作成された日時。
- **ユーザ名** – ファームウェアをインストールまたは更新したユーザ。
- **コメント** – ファームウェアまたはバックアップ ファイルに関する情報が表示されます。バックアップの作成時にコメントを指定しなかった場合は、次の既定のコメントが表示されます。
  - 自動バックアップ
  - これはクラウド バックアップ ファームウェアです
  - ユーザ定義コメント

「設定ファイルの表示」テーブル

ファームウェア バージョンの横の矢印を選択すると、クラウド上にあるそのファームウェア バージョンのバックアップ ファイルに関する情報が表示されます。

構成バージョン	バックアップ ファイルのバージョン番号。
構成日	バックアップ ファイルが作成された日付。
バックアップ種別	バックアップの種別（**自動**または**手動**）と次のアイコン。 • 設定ファイルを保持 – このアイコンを選択すると、自動または手動バックアップ時にバックアップ ファイルが上書きされないようになります。 • ゴールド マスター – このアイコンを選択すると、現在のバックアップ ファイルが「ゴールド マスター」とされます。すなわち、現在の設定ファイルの組み合わせとファームウェア イメージの組み合わせが最も安定した設定であると指定できます。ゴールド マスターと宣言したエントリは、ゴールドでない標準ファイルであると宣言するまで削除することもピン留めを外すこともできません。これで最も安定したバージョンが保護されます。複数のバックアップをゴールドと宣言することはできません。

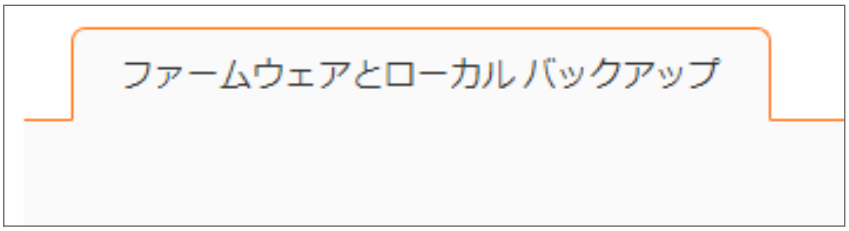
コメント	ファームウェアまたはバックアップ ファイルに関する情報が表示されます。バックアップの作成時にコメントを指定しなかった場合は、次の既定のコメントが表示されます。 • 自動バックアップ • これはクラウド バックアップ ファームウェアです • ユーザ定義コメント
ユーザ名	ファームウェアをインストールまたは更新したユーザ。
起動	起動アイコンを選択すると、ファイアウォールの再起動時に現在の設定と工場出荷時の既定の設定のどちらが使われるかが表示されます。 △ **注意: ファームウェア イメージの隣にある「起動」を選択すると、現在のファームウェア イメージが上書きされて、上書き後のイメージが「現在のファームウェア」イメージになります。** △ **注意: ファイアウォールにファームウェアをアップロードするときには、ウェブ ブラウザを閉じたり、リンクを選択したり、新しいページをロードしたりして、ウェブ ブラウザを中断しないでください。ウェブ ブラウザを中断すると、ファームウェアが破損することがあります。**
設定動作	次のアイコンが表示されます。 • **ダウンロード** – お使いのコンピュータまたはネットワーク上の新しい場所にファームウェアが保存されます。別の場所に保存できるのは、アップロードしたファームウェアのみです。 • **コメントの編集** – 既定のコメントまたはユーザ定義コメントを編集できます。 • **削除** – バックアップ ファイルを削除します。

テーブルの検索

検索機能を使用してバックアップ テーブルを検索できます。検索機能はすべてのテーブルに適用されますが、結果は実際に目に見えるテーブルについてだけ表示されます。例えば、種類の異なる「設定ファイルの表示」テーブルについての結果を確認するには、テーブルを 1 つずつ表示する必要があります。

テーブルを検索するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「検索」フィールドに検索条件を入力します。



テーブル内で結果が強調表示されます。

バックアップ ファームウェア イメージの作成

「**バックアップの作成**」を選択すると、SonicWall セキュリティ装置は現在のシステム状態、ファームウェア、および構成の設定情報についてスナップショットをとり、そのスナップショットを新しいシステム バックアップ ファームウェア イメージとします。バックアップは、ローカルまたはクラウドに保存できます。バックアップが自動的に実行されるようにスケジュールすることもできます。

ⓘ **重要:** バックアップを作成すると、既存のバックアップ ファームウェア イメージは必要に応じて上書きされます。

バックアップ ファイルを使って正常な設定を保存しておき、将来のアップグレードや設定でシステムが不安定になったり大きな問題が発生した場合は、そのファイルを起動します。設定ファイルは扱いやすいようにオンボードに保存されます。ファイルの作成日時と、その時点で使用中のファームウェアのバージョンが、「 ファームウェアの管理とバックアップ 」テーブルに表示されます。「ファームウェアの管理とバックアップ」テーブルに表示される各項目の日付は、ファームウェア イメージ自体のビルド日付です。

装置の現在の構成設定のバックアップを作成し、現在のファームウェア バージョンまたは新しくアップロードされたファームウェア バージョンで使用できます。

トピック:

- ローカル バックアップ ファームウェア イメージの作成
- セカンダリ ストレージ バックアップ ファームウェア イメージの作成
- クラウド バックアップ ファームウェア イメージの作成
- ファームウェア イメージ バックアップのスケジュール

ローカル バックアップ ファームウェア イメージの作成

ローカル バックアップ ファイルを作成するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**バックアップの作成 > ローカル バックアップ**」を選択します。

3. 「**ローカル バックアップ**」ダイアログで、以下を実行してバックアップを作成します。

a. ローカル バックアップを保持するには、「**ローカル バックアップを保持する**」を有効にします。

b. 「コメント」フィールドにコメントを入力します。

c. 「OK」を選択します。

ローカル ストレージに作成されたバックアップ イメージが「ローカル」セクションに表示されます。」セクションに移動してください。

セカンダリ ストレージ バックアップ ファームウェア イメージの作成

ⓘ **補足:** セカンダリ ストレージの使用の詳細については、『ログとレポート』を参照してください。このマニュアルにアクセスするには、https://www.sonicwall.com/ja-jp/support/technical-documentation/ に移動して、ご使用の製品モデル シリーズを選択します。次に、「管理」から『ログとレポート』を探します。

セカンダリ ストレージ バックアップ ファイルを作成するには、以下の手順に従います。

1. 「**バックアップの作成**」を選択します。
2. 「**セカンダリ ストレージ バックアップ**」を選択します。警告メッセージが表示されます。
3. 「**確認**」を選択します。

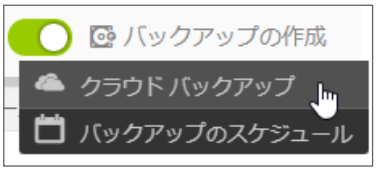
   バックアップ ファイルの作成には数分かかることがあります。

ⓘ **補足:** バックアップ ファイルは現在のファームウェアまたはアップロードされたファームウェアで起動できる小さな設定ファイルです。これにはファームウェア イメージは入っていません。

クラウド バックアップ ファームウェア イメージの作成

クラウド バックアップ ファイルを作成するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. クラウド バックアップが有効になっていない場合は、「**クラウド バックアップ設定**」セクションで「**クラウド バックアップ**」を有効にします。
3. 「**バックアップの作成 > クラウド バックアップ**」を選択します。



4. このバックアップ設定ファイルを保存し、追加のバックアップ設定ファイルをクラウド上に作成したときに上書きしないようにするには、「**クラウド バックアップを保持**」を選択します。

5. 必要に応じて「コメント」フィールドを使用して、後で識別しやすいように、バックアップ設定ファイルに関連するコメントを作成することができます。
6. 「OK」を選択します。バックアップ ファイルの作成には数分かかることがあります。

ファームウェア イメージ バックアップのスケジュール

ⓘ **補足:** ファームウェア設定ファイルのバックアップをスケジュールするには、「クラウド バックアップ」を有効にしておく必要があります。この機能は、ローカル バックアップに対してはサポートされていません。

バックアップをスケジュールするには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**バックアップの作成 > バックアップのスケジュール**」を選択します。

「**バックアップのスケジュール**」ダイアログが表示されます。

3. 作成するバックアップに対するオプションを設定します。
    - 1 回のみのバックアップをスケジュールするには、1 回のみのバックアップのスケジュール
    - 繰り返しバックアップをスケジュールするには、繰り返しバックアップのスケジュール
    - 混在バックアップをスケジュールするには、「**混在**」を選択して、「1 回のみのバックアップのスケジュール と 繰り返しバックアップのスケジュール」で説明した手順に基づいて設定を構成します。このスケジュールは、開始と終了の日時を設定し、時刻と曜日も設定して、その期間に同じタイミングで繰り返し発生します。

1 回のみのバックアップのスケジュール

1 回のみのバックアップをスケジュールするには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**バックアップの作成 > バックアップのスケジュール**」を選択します。
3. 「**バックアップのスケジュール**」ページで、以下を実行します。
    a. 「**スケジュール種別**」で、「**1 回**」を選択します。
    b. 「**1 回**」セクションの「**範囲の選択**」フィールド内でカレンダー アイコンを選択し、スケジュールを設定します。
    c. 「**1 回**」セクションで、バックアップを作成する期間を設定します。ドロップダウン メニューから年、月、日、時、分を選択し、バックアップの開始期間と終了期間を設定します。

d. 「**保存**」を選択します。

繰り返しバックアップのスケジュール

繰り返しバックアップをスケジュールするには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**バックアップの作成 > バックアップのスケジュール**」を選択します。
   「**バックアップのスケジュール**」ダイアログが表示されます。
3. 「**スケジュール種別**」で、「**繰り返し**」を選択します。
4. 「**繰り返し**」セクションで、以下の操作を行います。

a. バックアップを作成する曜日を選択します。すべての曜日を一度に選択するには「**すべて**」を選択します。

b. レポートの開始時刻と終了時刻を 24 時間形式（午前 2 時は 02:00、午後 2 時は 14:00 など）で入力します。

c. 「**追加**」を選択して、レポートを「**スケジュール リスト**」に追加します。

d. スケジュールするバックアップごとにこれらの手順を繰り返します。

5. 「**保存**」を選択します。

スケジュール済みバックアップの削除

特定のスケジュール済みバックアップを削除するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**バックアップの作成 > バックアップのスケジュール**」を選択します。
   以下を除くバックアップのスケジュール 」ダイアログが表示されます。
3. 「スケジュール リスト」セクションに表示されている、スケジュール済みバックアップの**削除**アイコンを選択します。
4. すべてのスケジュールを一度に削除するには、見出し行の**削除**アイコンを選択します。

ファームウェアの更新

ファームウェアを手動で更新するか、ファームウェア自動アップデート機能を使うことができます。

△ **注意: 新しいファームウェアをアップロードすると、既にアップロードされていたファームウェア イメージは上書きされます。**

ⓘ **補足:** 新しいファームウェアをアップロードする前に、現在の設定をバックアップすることを推奨します。次を参照してください。「バックアップ ファームウェア イメージの作成」現在の構成設定のバックアップを作成する方法の詳細が記載されています。

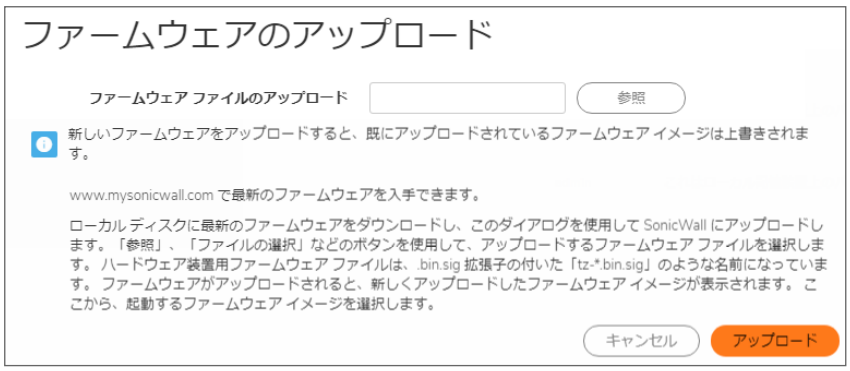
トピック:

- ファームウェアを手動で更新
- ファームウェア自動アップデート
- セーフモードを使用したファームウェアのアップグレード

ファームウェアを手動で更新

ファームウェアを手動で更新するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**ファームウェアのアップロード**」を選択します。
3. 新しいファームウェアをアップロードする前に、「OK」を選択して現在の設定のバックアップを作成します。
   「**ファームウェアのアップロード**」ダイアログが表示されます。



4. 「**参照**」を選択します。「ファイルのアップロード」ダイアログが表示されます。
5. ローカル ドライブにあるファームウェア ファイルを見つけます。
6. 「**開く**」を選択します。
7. 「**アップロード**」を選択して、新しいファームウェアを SonicWall セキュリティ装置にアップロードします。成功したことを示すメッセージがステータス バーに表示され、「ファームウェアの管理」テーブルに新しいファームウェアが表示されます。
8. 今ダウンロードしたファームウェアの「**起動**」アイコンを選択します。
9. 新しいファームウェアを、現在の設定でインストールするか、既定の設定でインストールするかを選択します。
10. 「OK」を選択します。ファームウェアを起動する時間についてのメッセージが表示されます。
11. 「OK」を選択します。起動状況を示すメッセージがステータス バーに表示されます。
12. 再起動後に再度ログインすると、「**デバイス | 設定 > ファームウェアと設定**」ページにファームウェアの更新が反映されています。

ファームウェア自 動 アップデート

SonicOS は、ファームウェア自動アップデート機能をサポートしています。この機能により、SonicWall セキュリティ装置のファームウェアを常に最新のリリースに保つことができます。

ファームウェア自動アップデートのオプションを設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。以下を除く設定 」ポップアップ ダイアログが表示されます。
3. 「 ファームウェア自動アップデート 」セクションに移動してください。
4. 次のどちらかを選択します。
   - **ファームウェア自動アップデートを有効にする** — 新しいファームウェアがリリースされると、**警告**アイコンが表示されます。このオプションは、既定では選択されています。
   - **利用可能な時に、新しいファームウェアを自動でダウンロードする** – 新しいファームウェアがリリースされたら、SonicWall セキュリティ装置にダウンロードします。このオプションは、既定では選択されていません。
5. 「OK」を選択します。

セーフモードを使用したファームウェアのアップグレード

SonicOS 管理インターフェースに接続できない場合は、セーフモードでセキュリティ装置を再起動できます。セーフモード機能を使用すると、簡素化された管理インターフェースを使って、不確実な設定状態から素早く回復できます。

セーフモードを使用してファームウェアをアップグレードするには、以下の手順に従います。

1. コンピュータを装置の X0 ポートに接続して、コンピュータの IP アドレスを 192.168.168.0/24 サブネット上のアドレス（192.168.168.20 など）に設定します。
2. 装置をセーフモードにするために、伸ばしたクリップや楊枝のような細くてまっすぐなものを使用して、SonicWall 装置の前面にある「**リセット**」ボタンを、**Test** ライトが点滅を開始するまで 20 秒以上押したままにします。
3. SonicWall セキュリティ装置がセーフモードで再起動されると、**Test** ライトが点滅を開始します。
4. コンピュータのウェブ ブラウザに「192.168.1.254」と入力して、セーフモードの管理インターフェースにアクセスします。
5. 「**ファームウェアのアップロード**」をクリックします。
6. SonicOS ファームウェア イメージ ファイルを保存した場所を参照します。
7. ファイルを選択し、「**アップロード**」を選択します。
8. 以下のいずれかの行にある起動アイコンを選択します:
   - **アップロードされたファームウェア – 更新!** – 現在の設定で装置を再起動するには、このオプションを使用します。
   - **アップロードされたファームウェア（工場出荷時の設定）– 更新!** – 既定の設定で装置を再起動するには、このオプションを使用します。
9. 確認のダイアログで「**OK**」を選択して次に進みます。
10. ファイアウォールの LAN または WAN インターフェースから SonicOS に接続するには、以下の手順に従います。
    a. コンピュータを MGMT ポートから切断します。
    b. 次のどちらかを行います。
       - IP アドレスと DNS サーバ アドレスを自動的に取得するようにコンピュータを再設定します。
       - コンピュータをリセットして通常の静的な値に戻します。
11. コンピュータをローカル ネットワークに接続します。
12. ブラウザで SonicWall 装置の LAN または WAN IP アドレスを指定します。
13. ファームウェアが正しく起動されると、ログイン画面が表示されます。工場出荷時の設定で再起動した場合は、既定のユーザ名とパスワード（**admin/password**）を入力して SonicOS 管理インターフェースにアクセスします。

設定のインポートとエクスポート

ファームウェア管理構成設定をインポートおよびエクスポートできます。

トピック:

- 設定のインポート
- 設定のエクスポート

設定のインポート

ⓘ **補足:** 新しい構成をインポートする前に、現在の構成をエクスポートするか、複製をクラウドにアップロードすることを推奨します。

以前に保存した設定ファイルをファイアウォールにインポートするには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**構成のインポート/エクスポート > 構成のインポート**」を選択します。

ⓘ **重要:** 先に進む前に、バックアップをローカルまたはクラウドに作成することを推奨します。次を参照してください。ローカル バックアップ ファームウェア イメージの作成 または クラウド バックアップ ファームウェア イメージの作成 ファームウェア構成バックアップの作成手順についての詳細が記載されています。

3. 「 構成のインポート 」ダイアログで「**参照**」を選択して、ファイアウォールにインポートする構成設定を以前に保存した設定ファイルを選択します。

   ⓘ **補足:** ファイル名拡張子 .exp を持つファイルを選択してください。

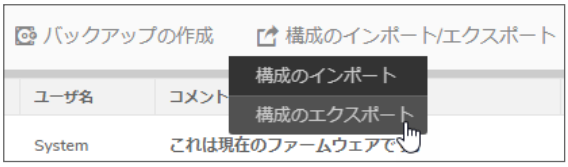
4. 「**インポート**」を選択します。
   新しい設定ファイルをインポートすると、現在の設定が上書きされます。インポートが完了すると、SonicWall 装置が自動的に再起動します。

設定のエクスポート

ファームウェアのリセットが必要になった場合には、エクスポートしたこのプリファレンス ファイルを セキュリティ装置にインポートできます。

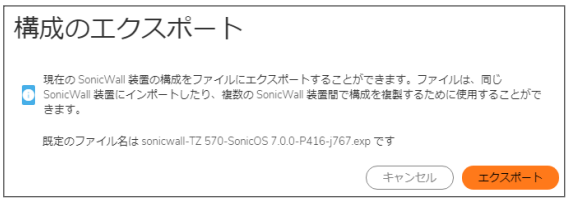
ファイアウォールから構成の設定をエクスポートするには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**構成のインポート/エクスポート > 構成のエクスポート**」を選択します。



3. 「 構成のエクスポート 」ウィンドウで、「**エクスポート**」を選択します。

   ⓘ **重要:** SonicWall 装置の現在の構成が .exp ファイルにエクスポートされ、ローカル システムで使用できるようになります。このファイルは、同じ SonicWall によってインポートしたり、複数の SonicWall システム間での構成の複製に使用したりできます。



4. 「**閉じる**」を選択します。

ファームウェアとバックアップの設 定

セカンダリ ストレージ デバイスを持つすべてのセキュリティ装置について、SonicOS は、システムの制限が許す限りファームウェアとプリファレンス ファイルのバックアップ (ファームウェア スナップショット) を作成する機能をサポートしました。

ファームウェアとバックアップを設定するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。
   「**設定**」ダイアログ ボックスが表示されます。

トピック:

- 設定またはレポートの FTP による送信
- テクニカル サポートへの診断レポートの送信
- ファームウェア自動アップデート
- ワンタッチ構成切替
- FIPS モードの有効化
- NDPP モードの有効化

設定またはレポートの FTP による送信

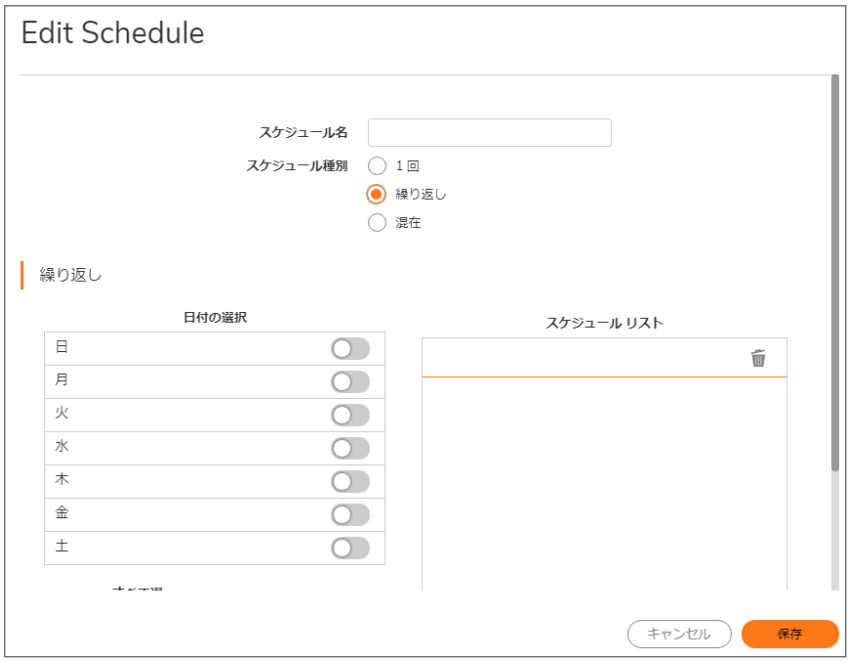
構成設定やテクニカル サポート レポート (TSR、つまりセキュリティ装置の設定および状況に関する詳細レポート) を、特定の FTP サーバに一度だけ、または定期的に送信することができます。FTP サーバへのこうしたレポートの送信スケジュールを設定することで、スケジュール オブジェクトと実行スケジュール時刻の作成と管理が可能になります。

診断レポートをテクニカル サポートに送信するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. **設定**アイコンを選択します。

3. FTP で TSR を送信するには、「**テクニカル サポート レポートを FTP で送信**」を選択します。このオプションは、既定では選択されていません。
4. FTP で構成設定を送信するには、「**設定を FTP で送信する**」を選択します。このオプションは、既定では選択されていません。
5. どちらかまたは両方の「動作」設定が選択されている場合、サーバ フィールドが使用可能になります。必要に応じて変更を行います。
    a. 「FTP サーバ」フィールドにサーバの IP アドレスを入力します。既定値は「0.0.0.0」です。
    b. 「 ユーザ名 」フィールドに、サーバと関連付けられているユーザ名を入力します。
    c. 「パスワード」フィールドに、ユーザ名と関連付けられているパスワードを入力します。
    d. 「ディレクトリ」フィールドに、送信するレポートがあるディレクトリを入力します。

6. 「**スケジュールの設定**」を選択します。「**設定**」ダイアログが表示されます。



「スケジュール名」は「TSR 報告時間」になっていて、変更できません。

7. スケジュールを設定します。スケジュールの設定方法については、次を参照してください。「ファームウェア イメージ バックアップのスケジュール 」セクションに移動してください。
8. 「**保存**」を選択します。

テクニカル サポートへの診断レポートの送信

システムの問題を解決する目的で、システム診断を SonicWall テクニカル サポートへ送信することができます。

診断レポートをテクニカル サポートに送信するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。
3. 「 診断 」セクションに移動してください。
4. 「 診断 」セクションで、「**診断レポートをサポートに送信**」を選択します。この処理には、最大で 1 分ほどかかることがあります。レポートの送信中は、画面の一番下のステータス バーに次のように表示されます。

5. 「**OK**」を選択します。

起動設定

診断を有効にして SonicWall ネットワーク セキュリティ装置を起動するには、以下の手順に従います。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。以下を除く設定 」ダイアログが表示されます。
3. 「**ファームウェア診断を有効にして起動する（可能な場合）**」を選択します。このオプションは、既定では選択されていません。
4. 「**適用**」を選択します。

ワンタッチ構成切替

ⓘ **補足:** 現在の構成を復元できるよう、構成切替を実行する前に必ず SonicWall セキュリティ装置の構成をエクスポートしてください。次を参照してください。「設定のエクスポート」。

△ **注意: ワンタッチ構成切替は、SonicWall セキュリティ装置の振舞いを変更することを意識してください。ワンタッチ構成切替を適用する前に、構成の一覧を確認してください。特に、以下の構成はユーザ エクスペリエンスに影響する可能性があります。**

- **「デバイス | 設定」ページの管理者パスワード要件**
- **HTTPS 管理の要求**
- **HTTP から HTTPS へのリダイレクトの無効化**
- **Ping 管理の無効化**

ワンタッチ構成切替機能の設定は、設定 ダイアログ（「**デバイス | 設定 > ファームウェアと設定**」ページから使用可能）で行います。この機能は、SonicWall ネットワーク セキュリティ装置のセキュリティ設定をすばやく調整するための機能と見なすことができます。ワンタッチ構成切替では、シングルクリックで、60 個を超える構成設定値を適用して、SonicWall の推奨ベスト プラクティスを実装できます。これらの設定は、装置が確実に SonicWall のセキュリティ機能を利用するようにします。

ワンタッチ構成設定を切り替えるには、以下の手順に従います。

ⓘ **補足:** 更新を完全に反映させるには、システムを再起動する必要があります。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。「 設定 」ダイアログが表示されます。
3. 「 ワンタッチ構成切替 」セクションに移動してください。

- **DPI およびステートフル ファイアウォール セキュリティ** – ゲートウェイ アンチウイルス、侵入防御、アンチ スパイウェア、アプリケーション ルールなど、精密パケット検査（DPI）セキュリティ サービスを有効にしているネットワーク環境用です。

- **ステートフル ファイアウォール セキュリティ** – 有効にしている DPI セキュリティ サービスがないが、SonicWall のステートフル ファイアウォール セキュリティのベスト プラクティスを利用したいネットワーク環境用です。

この両方のワンタッチ構成切替配備では、次の設定を実装します。

- 管理者セキュリティのベスト プラクティスを設定する
- HTTPS ログインを強制し、Ping を無効にする
- DNS 再割り当てを設定する
- アクセス ルールのベスト プラクティスを設定する
- ファイアウォール設定のベスト プラクティスを設定する
- ファイアウォール フラッド防御のベスト プラクティスを設定する
- VPN 詳細設定のベスト プラクティスを設定する
- ログ レベルを設定する
- フロー報告と可視化を有効にする

また、DPI およびステートフル ファイアウォール セキュリティ配備では、次の DPI 関連の設定も構成します。

- 適用可能なすべてのゾーンで DPI サービスを有効にする
- アプリケーション ルールを有効にする
- ゲートウェイ アンチウイルスのベスト プラクティスを設定する
- 侵入防御のベスト プラクティスを設定する
- アンチスパイウェアのベスト プラクティスを設定する

どの設定が再構成されるかを正確に確認するには、各ボタンの横の「プレビュー」リンクを選択してください。各設定と、設定される値の一覧を示すページが表示されます。

FIPS モードの有効化

FIPS (連邦情報処理規格) モードで操作する場合、SonicWall セキュリティ装置は FIPS 140-2 に準拠したセキュリティをサポートします。SonicOS の FIPS 準拠の機能には、PRNG-based on SHA-1 と、FIPS でのみ承認されたアルゴリズム (DES、3DES、および AES with SHA-1) のサポートが含まれます。

FIPS を有効にし、現在の設定のうち使用できない設定または存在しない設定の一覧を表示するには、以下の手順に従います。

ⓘ **補足:** 「FIPS モードを有効にする」オプションは、同じく「 ファームウェアとバックアップ > 設定 」ダイアログにある「NDPP モードを有効にする」オプションと同時に有効にすることはできません。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。
   以下を除く設定 」ダイアログが表示されます。
3. 「 FIPS 」セクションに移動してください。
4. 「**FIPS モードを有効にする**」オプションを有効にします。

5. 「**OK**」を選択します。

「**FIPS モード設定準拠チェックリスト**」ダイアログに、必要な設定と使用できない設定の一覧が表示されます。

6. SonicWall 装置が
   - チェックリストの要件を満たしている場合は、**ステップ 7** に進みます。
   - チェックリストの要件を満たしていない場合は、FIPS モード設定準拠チェックリストを満たすように設定を手動で変更するか、無効にします。

     ⓘ **ヒント:** 設定を変更している間、チェックリスト ダイアログは開いたままにしておいてください。必要なすべての変更が終わる前に「**OK**」を選択すると、確認ダイアログを閉じると同時に「**FIPS モードを有効にする**」チェックボックスが自動的にオフになります。このチェックボックスを再びオンにして、FIPS に準拠するために変更しなければならない設定が他にもないか確認してください。
7. 「**OK**」を選択するとセキュリティ装置が FIPS モードで再起動します。2 番目の警告が表示されます。
8. 起動を続行するには「**はい**」を選択してください。通常の動作に戻すには、「**FIPS モードを有効にする**」チェックボックスをオフにし、ファイアウォールを非 FIPS モードで再起動します。

   △ **注意: SonicWall セキュリティ装置で FIPS に準拠した処理を実行する場合、SonicWall セキュリティ装置に貼ってある不正開封防止ステッカーはそのままにしておき、触れないでください。**

NDPP モードの有効化

SonicWall ネットワーク セキュリティ装置は、Network Device Protection Profile (NDPP) に準拠するように有効にできますが、その場合は一部のセキュリティ装置設定が使用できなくなるか、特定のファイアウォール設定が必要となります。

ⓘ **補足:** NDPP はコモン クライテリア (CC) 認証の一部です。ただし、SonicOS の NDPP は、現在、認証を取得していません。

Protection Profile への準拠を要求するデバイスのセキュリティ上の目的は、以下のように定義されます。

準拠 TOE (評価対象) は、TOE への脅威に対処するセキュリティ機能を提供し、法律や規制によって課せられるポリシーを実装します。提供されるセキュリティ機能には、TOE との通信および TOE 要素間の通信の保護、TOE

およびその設定機能への管理アクセス、セキュリティ関連イベントの検出を目的としたシステム監視、リソース利用の制御、および TOE に対する更新のソース確認機能などがあります。

NDPP を有効にすると、ポップアップ メッセージで NDPP モード設定準拠チェックリストが示されます。このチェックリストに現在の SonicOS 設定のうち NDPP に準拠しないものがすべて表示されるので、該当する設定を変更できます。これらの変更を行うには、SonicOS 管理インターフェースに移動する必要があります。工場出荷時の設定の装置用のチェックリストを以下の手順に示します。

NDPP を有効にし、現在の設定のうち使用できない設定または存在しない設定の一覧を表示するには、以下の手順に従います。

ⓘ **補足:** 「NDPP モードを有効にする」オプションは、同じく「ファームウェアとバックアップ > 設定」ダイアログにある「FIPS モードを有効にする」オプションと同時に有効にすることはできません。

1. 「**デバイス | 設定 > ファームウェアと設定**」に移動します。
2. 「**設定**」を選択します。「**設定**」ダイアログが表示されます。
3. 「**NDPP**」セクションまでスクロールします。
4. 「**NDPP モードを有効にする**」を選択します。

「**NDPP モード設定準拠チェックリスト**」で、必要な設定と使用できない設定の一覧が示されます。

5. SonicWall 装置が
   - チェックリストの要件を満たしている場合は、**ステップ 6** に進みます。
   - チェックリストの要件を満たしていない場合は、NDPP モードの要件を満たすように設定を手動で変更するか、無効にします。

     ⓘ **ヒント:** 設定を変更している間、チェックリスト ダイアログは開いたままにしておいてください。必要なすべての変更が終わる前に「**OK**」を選択した場合、チェックリスト ダイアログを閉じると同時に「**NDPP モードを有効にする**」オプションは自動的にオフになります。このオプションを再びオンにして、NDPP に準拠するために変更しなければならない設定が他にもないか確認してください。
6. 「**OK**」を選択します。

8

システムの再起動

ファイアウォールを再起動するには、以下の手順に従います。

注意: 再起動の処理には数分程度かかります。再起動中は、すべてのユーザが切断されます。設定を変更した場合は、再起動する前にそれを適用してください。

1. 「**デバイス | 設定 > 再起動**」に移動します。
2. 「**SonicOS の再起動**ボタンを選択します。

9

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます https://www.sonicwall.com/ja-jp/support。

サポート ポータルでは、次のことができます。

- ナレッジベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする https://community.sonicwall.com/technology-and-support。
- ビデオ チュートリアルを視聴する。
- 次のサイトにアクセスする https://mysonicwall.com。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートに連絡するには、次の URL にアクセスします https://www.sonicwall.com/ja-jp/support/contact-support。

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS デバイスの設定 管理ガイド
更新日 – 2021 年 1 月
ソフトウェア バージョン – 7
232-005449-00 Rev A

エンド ユーザ製品契約

SonicWall エンド ユーザ製品契約を参照する場合は、以下に移動してください https://www.sonicwall.com/ja-jp/legal。

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、"SonicWall Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035