

## SonicWall Secure Mobile Access 10.2.0 リリースノート

このリリースノートでは、SonicWall Secure Mobile Access (SMA) 10.2.0 日本語版リリースについて説明します。

バージョン:

- [バージョン 10.2.0.10](#)
- [バージョン 10.2.0.9](#)
- [バージョン 10.2.0.8](#)

### バージョン 10.2.0.10

2022 年 4 月

### SonicWall SMA 10.2.0.10 について

SonicWall SMA 10.2.0.10 には、以前のリリースで見つかったさまざまな既知の問題に対する修正が含まれています。詳細については、「[修正された問題点](#)」セクションを参照してください。このリリースは、これまでの SMA 10.2 リリースのすべての機能と修正された問題点をサポートします。

### アップグレードに関するナレッジ ベース記事

① | **重要:** SMA 装置をアップグレードする前に、次のナレッジ ベース記事を参照してください。

- [SMA 100 シリーズ装置でファームウェアをアップグレードする方法 \(英語\)](#)
- [追加で必要な SMA 100 シリーズ 10.X および 9.X ファームウェア更新 \(英語\)](#)
- [SMB SSL-VPN: SMA 500v 仮想装置のファームウェア アップグレード \(英語\)](#)

# 互換性とインストールの注意事項

SonicWall SMA 10.2.0.10 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v (ESXi 用 SonicWall SMA 500v は、VMware ESXi 5.0 以降への展開がサポートされています)
- Hyper-V 用 SMA 500v (Hyper-V 用 SonicWall SMA 500v は、Hyper-V Server バージョン 2016 と 2019 以降への展開がサポートされています)
- AWS 用 SMA 500v
- Azure 用 SMA 500v

SMA 10.2.0.10 は、キャプチャセキュリティセンター (CSC) と互換性があります。CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

- CSC にログインするには、[cloud.sonicwall.com](https://cloud.sonicwall.com) で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

詳細については、次を参照してください: [プラットフォーム別の機能サポート](#)。

## プラットフォーム別の機能サポート

すべての SonicWall SMA 装置が主要な Secure Mobile Access 機能をサポートしていますが、すべての SonicWall SMA 装置上ですべての機能がサポートされるわけではありません。SonicWall SMA 装置は、以下を含むほとんどの主要な Secure Mobile Access 機能を共有します。

- 仮想オフィス
- NetExtender
- アプリケーション オフロードと負荷分散
- ウェブ アプリケーション ファイアウォール
- 地域 IP とボット ネット フィルタ
- エンド ポイント 制御
- キャプチャ ATP
- CSC 管理とレポート

## 新機能

- 「修正された問題点」に一覧されている問題のメンテナンス修正。

## 修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3141	AJAX 呼び出しで 403 エラーが発生します。
SMA-3240	10.2.0.8 ファームウェアにアップグレードした後、Windows と Mac OS 上で HTTP リソースが停止します。
SMA-3361	ユーザ裁量オプションを有効にすると、パスワード変更オプションが動作しません。
SMA-3390	SMA 500v 装置の状況ページで、地域の位置が「不明」と表示されます。
SMA-3568	SonicWall SSL-VPN NetExtender Windows クライアント v10.2.322 にバッファオーバーフローの脆弱性があります。
SMA-3606	SMA100 OpenSSL CVE-2022-0778 DoS の脆弱性
SMA-3610	NetExtender OpenSSL CVE-2022-0778 DoS の脆弱性

## 確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3652	ライセンスのアップグレードが VM 装置でサポートされません。ライセンス テキスト ボックスの手動アップグレードが Hyper-V、Azure と AWS で利用できます。

# バージョン 10.2.0.9

2021 年 11 月

## SonicWall SMA 10.2.0.9 について

SonicWall SMA 10.2.0.9 には、以前のリリースで見つかったさまざまな既知の問題に対する修正が含まれています。詳細については、「[修正された問題点](#)」セクションを参照してください。このリリースは、これまでの SMA 10.2 リリースのすべての機能と修正された問題点をサポートします。

## アップグレードに関するナレッジ ベース記事

① | **重要:** SMA 装置をアップグレードする前に、次のナレッジ ベース記事を参照してください。

- [SMA 100 シリーズ装置でファームウェアをアップグレードする方法 \(英語\)](#)
- [追加で必要な SMA 100 シリーズ 10.X および 9.X ファームウェア更新 \(英語\)](#)
- [SMB SSL-VPN: SMA 500v 仮想装置のファームウェア アップグレード \(英語\)](#)

# 互換性とインストールの注意事項

SonicWall SMA 10.2.0.9 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v (ESXi 用 SonicWall SMA 500v は、VMware ESXi 5.0 以降への展開がサポートされています)
- Hyper-V 用 SMA 500v (Hyper-V 用 SonicWall SMA 500v は、Hyper-V Server バージョン 2016 と 2019 以降への展開がサポートされています)
- AWS 用 SMA 500v
- Azure 用 SMA 500v

SMA 10.2.0.9 は、キャプチャセキュリティセンター (CSC) と互換性があります。CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

- CSC にログインするには、[cloud.sonicwall.com](https://cloud.sonicwall.com) で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

詳細については、次を参照してください: [プラットフォーム別の機能サポート](#) および [バージョン 10.2.0.9](#).

## プラットフォーム別の機能サポート

すべての SonicWall SMA 装置が主要な Secure Mobile Access 機能をサポートしていますが、すべての SonicWall SMA 装置上ですべての機能がサポートされるわけではありません。SonicWall SMA 装置は、以下を含むほとんどの主要な Secure Mobile Access 機能を共有します。

- 仮想オフィス
- NetExtender
- アプリケーション オフロードと負荷分散
- ウェブ アプリケーション ファイアウォール
- 地域 IP とボット ネット フィルタ
- エンド ポイント 制御
- キャプチャ ATP
- CSC 管理とレポート

## 新機能

- 「修正された問題点」に一覧されている問題のメンテナンス修正

## 修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3235	脆弱性: SMA100 で、複数の認証されないファイルエクスプローラヒープベースとスタックベースのバッファオーバーフロー。
SMA-3233	脆弱性: SMA100 で、POST 認証 RCE。
SMA-3231	脆弱性: SMA100 で、getBookmarks ヒープベースのバッファオーバーフロー。
SMA-3229	新モードで、パスワード変更ダイアログが表示されません。旧モードでは表示されます。
SMA-3213	「Let's Encrypt」証明書が動作しません。
SMA-3208	脆弱性: SMA100 で、認証されない「混乱した代理」。
SMA-3207	脆弱性: SMA100 で、認証されない CPU 枯渇の脆弱性。
SMA-3206	脆弱性: SMA100 で、認証されないファイルアップロードパス横断の脆弱性。
SMA-3204	脆弱性: SMA100 で、root として認証されたコマンドインジェクションの脆弱性。
SMA-3199	ユーザログインの顧客ロゴをクリックすると、管理コンソールにリダイレクトされます。
SMA-3155	10.2.0.8 ファームウェアの新モードで DUO の 2 段階認証を使用すると、VPN ログインが動作しません。
SMA-3148	新モードで装置に接続できません。サーバがダウンしており、到達不能のエラーが発生します。
SMA-3127	脆弱性: SMA100 で、ログインしなくても複数の管理 API にアクセスできます。
SMA-3122	新モードの「クライアント > 設定」で設定を変更すると、「クライアント > ルート」の「強制トンネル」設定が無効になります。
SMA-3111	脆弱性: HTTP ホストヘッド値の反映。
SMA-3001	装置を 9.0.0.10-28sv から 10.2.1.1-19sv にアップグレードした後に、証明書ドメインを使用してログインできません。
SMA-2927	SMA ソフトウェアを 10.2.0.7 にアップグレードすると、RDP ブックマークのパスワードを問い合わせします。
SMA-2925	10.2.1.0 にアップグレードすると、装置の「再起動スケジュール」が動作しません。
SMA-2702	ファームウェアを 10.2.0.7 にアップグレードすると、「ウェブアプリケーションファイアウォール」の「コンテンツセキュリティポリシー」に問題が発生します。
SMA-2683	オフロードアプリケーションに WebSocket の問題があります。
SMA-2662	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。

問題番号	問題の詳細
SMA-2661	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。
SMA-2927	SMA ソフトウェアを 10.2.0.7 にアップグレードすると、RDP ブックマークのパスワードを問い合わせします。
SMA-2925	10.2.1.0 にアップグレードすると、装置の「再起動スケジュール」が動作しません。
SMA-2702	ファームウェアを 10.2.0.7 にアップグレードすると、「ウェブ アプリケーション ファイアウォール」の「コンテンツセキュリティポリシー」に問題が発生します。
SMA-2683	オフロード アプリケーションに WebSocket の問題があります。
SMA-2662	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。
SMA-2661	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。
SMA-2927	SMA ソフトウェアを 10.2.0.7 にアップグレードすると、RDP ブックマークのパスワードを問い合わせします。
SMA-2925	10.2.1.0 にアップグレードすると、装置の「再起動スケジュール」が動作しません。
SMA-2702	ファームウェアを 10.2.0.7 にアップグレードすると、「ウェブ アプリケーション ファイアウォール」の「コンテンツセキュリティポリシー」に問題が発生します。
SMA-2683	オフロード アプリケーションに WebSocket の問題があります。
SMA-2662	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。
SMA-2661	電子メールアドレスに「-」が含まれていると、電子メールによる設定バックアップの送信に失敗します。

## 確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3262	診断設定ページの「定期的再起動」の時刻に誤りがあります。
SMA-3249	Linux の NetExtender で、複雑なパスワードに対するローカルパスワード更新のエラーメッセージに誤りがあります。
SMA-3248	SSL VPN サービスを再起動した際に、AOV NetExtender セッションが自動再接続しません。
SMA-2893	ワンタイムパスワードが入力されていない状態でも、「安全なネットワークの検出 (SND)」が検知されます。

# バージョン 10.2.0.8

2021 年 9 月

## SonicWall SMA 10.2.0.8 について

SonicWall SMA 10.2.0.8 には、以前のリリースで見つかったさまざまな既知の問題に対する修正が含まれています。詳細については、「[修正された問題点](#)」セクションを参照してください。このリリースは、これまでの SMA 10.2 リリースのすべての機能と修正された問題点をサポートします。

## アップグレードに関するナレッジ ベース記事

① | **重要:** SMA 装置をアップグレードする前に、次のナレッジ ベース記事を参照してください。

- [SMA 100 シリーズ装置でファームウェアをアップグレードする方法 \(英語\)](#)
- [追加で必要な SMA 100 シリーズ 10.X および 9.X ファームウェア更新 \(英語\)](#)
- [SMB SSL-VPN: SMA 500v 仮想装置のファームウェア アップグレード \(英語\)](#)



## 互換性とインストールの注意事項

① | **メモ:** SMA 10.2.0.8 は、キャプチャセキュリティセンター (CSC) と互換性があります。

SonicWall SMA 10.2.0.8 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v (ESXi 用 SonicWall SMA 500v は、VMware ESXi 5.0 以降への展開がサポートされています)
- Hyper-V 用 SMA 500v (Hyper-V 用 SonicWall SMA 500v は、Hyper-V Server バージョン 2016 と 2019 以降への展開がサポートされています)
- AWS 用 SMA 500v
- Azure 用 SMA 500v

SMA 10.2.0.8 は、キャプチャセキュリティセンター (CSC) と互換性があります。CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

- CSC にログインするには、[cloud.sonicwall.com](https://cloud.sonicwall.com) で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

詳細については、「[プラットフォーム別の機能サポート](#)」および「[10.2.0.8 でリリースされたクライアントのバージョン](#)」を参照してください。

## プラットフォーム別の機能サポート

すべての SonicWall SMA 装置が主要な Secure Mobile Access 機能をサポートしていますが、すべての SonicWall SMA 装置上ですべての機能がサポートされるわけではありません。SonicWall SMA 装置は、以下を含むほとんどの主要な Secure Mobile Access 機能を共有します。

- 仮想オフィス
- NetExtender
- アプリケーションオフロードと負荷分散
- ウェブ アプリケーション ファイアウォール
- 地域 IP とボット ネット フィルタ
- エンド ポイント 制御
- キャプチャ ATP
- CSC 管理とレポート

## SonicWall SMA 200/210 でサポートされない機能

以下の機能は SonicWall SMA 400/410 でサポートされていますが、SonicWall SMA 200/210 ではサポートされません。

- アプリケーション プロファイリング
- 高可用性

## AWS と Azure 用 SonicWall SMA 500v でサポートされない機能

- 高可用性

## 10.2.0.8 でリリースされたクライアントのバージョン

トピック:

- [NetExtender クライアントのバージョン](#)
- [SMA Connect Agent のバージョン](#)

### NetExtender クライアントのバージョン

以下に、本リリースで導入されている NetExtender クライアント バージョンのリストを示します。

説明	バージョン
NetExtender Linux RPM 32 ビット	NetExtender.Linux-10.2.827-1.i686.rpm
NetExtender Linux RPM 64 ビット	NetExtender.Linux-10.2.827-1.x86_64.rpm
NetExtender Linux TGZ 32 ビット	NetExtender.Linux-10.2.827.x86.tgz
NetExtender Linux TGZ 64 ビット	NetExtender.Linux-10.2.827.x86_64.tgz
NetExtender Windows	NetExtender.Linux-10.2.314

### SMA Connect Agent のバージョン

以下に、本リリースでサポートされている SMA Connect Agent のバージョンのリストを示します。

説明	バージョン
SMA Connect Agent Windows	1.1.37
SMA Connect Agent macOS	1.1.30

# 製品ライセンス

SonicWall Secure Mobile Access 10.2.0.8 ファームウェアは、SonicWall SMA 装置上でユーザーベースのライセンスを提供します。ライセンスは SonicWall ライセンス マネージャ サービスによって制御されており、MySonicWall アカウントを通してライセンスを追加できます。未登録の装置は、そのモデルに対する既定のライセンス割り当てをサポートしますが、MySonicWall からの追加のライセンスを有効化するには装置を登録する必要があります。

ライセンス状況は Secure Mobile Access 管理インターフェース内にある「システム > 状況」ページの「ライセンスと登録」セクションに表示されます。「システム > 診断」ページ上で生成されるテクニカルサポート レポートには、装置で現在利用可能な総ライセンス数およびアクティブ ユーザーライセンス数が表示されます。

ユーザーが仮想オフィス ポータルへのログインを試みて、利用可能なユーザーライセンスがなかった場合は、ログイン ページに「No more User Licenses available. Please contact your administrator. (ユーザーライセンスが不足しています。管理者にお問い合わせください。)」というエラー メッセージが表示されます。すべてのユーザーライセンスが使用中の状態で、ユーザーが NetExtender クライアントを起動した場合も同様のエラーが表示されます。これらのログイン試行は同様のメッセージとともにログ エントリに記録され、「ログ > 表示」ページに表示されます。

**装置のライセンスを有効化するには、以下の手順に従います:**

1. 管理者としてログインし、「システム > ライセンス」ページに移動します。
2. 「サービスの購読、アップグレード、及び更新」リンクをクリックします。  
「MySonicWall ログイン」ページが表示されます。
3. MySonicWall アカウントの資格情報をフィールドに入力して、MySonicWall にログインします。これは、装置を登録した、またはこれから登録するアカウントである必要があります。MySonicWall ウェブ インターフェースで装置のシリアル番号が既に登録されている場合も、装置自体のライセンス情報を更新するためにログインする必要があります。  
MySonicWall によってシリアル番号と認証コードが自動的に取得されます。
4. 装置を説明する名前を「ニックネーム」フィールドに入力し、「適用」をクリックします。
5. 登録の確認が表示された後で、「次へ」を選択します。
6. 必要に応じて、その他のサービスのライセンスのアップグレードや有効化を行います。
7. 有効化の後、装置で「システム > ライセンス」ページを参照すると、アクティブなライセンスのキャッシュされたバージョンが表示されます。

## アップグレード情報

アップグレードの情報については、次のナレッジ ベース記事を参照してください: [アップグレードに関するナレッジ ベース記事](#)

- ① **メモ:** SMA のアップグレードは、順番に行うことを推奨します。例えば、SMA 8.6 を実行している SMA 装置の場合、まず 9.0.0.10 にアップグレードしてから、10.2.0.8 にアップグレードします。

最新ファームウェアの取得方法、SonicWall 装置のファームウェア イメージのアップグレード方法、および他の装置から構成設定をインポートする方法については、サポート ポータル (<https://www.sonicwall.com/ja-jp/support/technical-documentation>) から入手できる『SonicWall SMA アップグレード ガイド』を参照してください。

## 高可用性ペアのアップグレード

SMA 高可用性ペアでファームウェアをアップグレードするには、次の手順に従います:

1. アクティブ装置 (ノード 1) に新しい SMA ファームウェアをアップロードします。
2. アクティブ装置 (ノード 1) で新しいファームウェアを起動します。
3. ノード 1 が起動している間、アイドル装置がアクティブになります (ノード 2)。
4. アクティブ装置 (ノード 2) に新しいファームウェアをアップロードします。
5. アクティブ装置 (ノード 2) で新しいファームウェアを起動します。

2 台の装置が再起動した後、高可用性ペアは新しいファームウェアで完全に更新されます。

## クライアントのアップグレードについて

ファームウェアに新しいクライアント バージョンが含まれる場合、クライアントは通常自動的にアップグレードされます。

- ① **メモ:** NetExtender クライアントが Windows MSI インストーラでインストールされている場合は、自動的にアップグレードされません。

## 修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-2144	フェイルオーバーが不規則に発生することによって、高可用性 (HA) が安定しません。
SMA-2184	Duo の PUSH プロキシ スクリプトが意図したとおりに動作しません。
SMA-2243	10.2.0.5-29 バージョンにアップグレードした後に、EPC の更新が失敗します。
SMA-2344	SAML ユーザが SMA 500v 装置にログインできません。
SMA-2345	10.2.0.6 にアップグレードした後に、アプリケーション オフロード ポータルが読み込まれません。
SMA-2432	NetExtender RPM パッケージに "libNetExtenderEpc" ファイルが含まれていません。
SMA-2435	CIFS/SMB ブックマークのファイル名に 14 文字以上の日本語が含まれる場合、ファイルのダウンロードに失敗します。
SMA-2436	バージョン 10.2.0.6-32 にアップグレードした後に、Azure 用 SMA 500v の CPU 使用率が 100% と高く表示されます。
SMA-2437	SRA Cookie の「HTTP のみ」が有効化されている場合、エラー「Insecure configuration of Cookie attributes (安全でない Cookie 属性の構成)」が表示されて、PCI スキャンが失敗します。
SMA-2438	HTTP ブックマークに、誤ったスペイン語の文字が表示されます。

問題番号	問題の詳細
SMA-2439	デバイスリスト ページでデバイス情報を検索した際に、デバイス情報の編集と削除ができません。
SMA-2445	最新のファームウェア バージョンにアップグレードした後に、旧モードと新モードの両方でエラー「有効な Cookie ドメイン名ではありません」が表示されます。
SMA-2446	新モードで DUO 認証をした後に、仮想オフィス ブックマークがパスワードを転送しません。
SMA-2448	バージョン 10.2.0.6 にアップグレードした後に、FTP バックアップが意図したとおりに動作しません。
SMA-2449	構成した日次バックアップ スケジュールが意図したとおりに動作しません。
SMA-2458	Azure AD LDAP にリンクされたローカルLDAP の RDP ブックマーク SSO が失敗します。
SMA-2462	Citrix ブックマークの SSO 認証が意図したとおりに動作しません。
SMA-2530	X1 インターフェースで HTTP と HTTPS を無効にしているにもかかわらず、ユーザが X1 インターフェースを介して管理にアクセスできます。
SMA-2533	電子メールでログを送信できません。
SMA-2535	Kaspersky EPC が、すべての属性のバージョンしか確認しません。
SMA-2548	NetExtender で接続すると、DNS タブにすべての DNS 接尾辞が表示されません。
SMA-2563	フォルダ内のファイル名に ASCII 以外の文字が含まれている場合、フォルダのダウンロードに失敗します。
SMA-2620	バックアップ システムがプライマリの役割に切り替わらず、IP の所有権を得ることができません。
SMA-2636	「VPN 常時有効」で、ワンタイムパスワードのパスワード タイムアウトが意図したとおりに動作しません。
SMA-2642	周辺機器 ID の EPC 確認が失敗します。ユーザ PC のシリアル番号には PC のシリアル番号ではなく、「System Serial number (システムシリアル番号)」が表示されます。
SMA-2647	設定のインポートができず、SMA 装置へのログ記録に失敗します。
SMA-2664	HTTP DoS 設定により、オフロード ポータルが破棄されます。
SMA-2690	SAML 認証で、SMA Connect が NetExtender を起動しません。
SMA-2707	"X-Frame-Options" に "sameorigin" が設定されている場合、フレームが表示されません。
SMA-2717	バージョン 10.2.0.6 にアップグレードした後に、Mac のウェブ ユーザが RDP ネイティブ クライアント ブックマークを開けません。
SMA-2720	新 UI モードで SMS ワンタイムパスワード オプションに切り替えると、常にワンタイムパスワードが起動されます。
SMA-2727	ワンタイムパスワードのユーザ裁量が有効の場合、ユーザ ポータルに設定オプションが表示されません。
SMA-2736	バージョン 10.2.0.6 のファームウェアで、ブックマークに登録されているウェブ サイトの日本語が文字化けします。

問題番号	問題の詳細
SMA-2741	エラーメッセージ「Update Signature failed, error code 500 (シグネチャの更新に失敗しました。エラーコード 500)」により、シグネチャの更新が頻繁に失敗します。
SMA-2759	Azure AD SSO で正常に認証した後に、タブのリソースが利用できません。
SMA-2766	新モードで、ユーザが作成したブックマークを編集できません。
SMA-2807	ユーザが期限切れパスワードを使用してログインしようとした際に、RADIUS 認証で問題が発生します。
SMA-2818	新モードで、RADIUS のチャレンジ/レスポンス認証が意図したとおりに動作しません。
SMA-2819	HTTP ブックマークに、誤ったフランス語の文字が表示されます。
SMA-1583	いくつかのウェブブラウザで、アプリケーション オフロード ポータルの機能にアクセスできません。
SMA-2822	SMA 装置で電源障害が発生した際に、保存されたデバイス ID が消去されます。
SMA-2823	バージョン 10.2.0.6 にアップグレードした後に、アプリケーション オフロード ポータルに変換の問題があります。
SMA-2825	NetExtender (MSI) による初めてのログインで、判読できないルートが表示されます。
SMA-2876	ネットワークの変更を検知した際に、「VPN 常時有効」を有効にした NetExtender が自動的に再接続しません。
SMA-2934	SMA100 で、認証されない任意のファイルを削除する脆弱性。
SMA-2957	SMA100 で、認証された任意のコマンド インジェクションの脆弱性。
SMA-2973	公開しているポータルに、プライベート IP が表示されます。
SMA-3002	Net-SNMP パッケージに、NULL ポインタの確認が不十分である脆弱性があります (SNMP DoS)。
SMA-3015	高可用性でのコマンド インジェクションによるローカル権限昇格。

## 確認されている問題点

問題番号	問題の詳細
SMA-2276	「強制方式」が「既存のセッションからログアウトしたことを確認する」に設定されている場合でも、最初のユーザセッションが自動的にログアウトされます。
SMA-2662	電子メールアドレスに "-" 記号が含まれていると、電子メールでの設定のバックアップに失敗します。
SMA-2765	ウェブ アプリケーション ファイアウォールが有効か無効にかかわらず、Teams のカレンダーの同期に失敗します。
SMA-2893	ワンタイムパスワードが入力されていない状態でも、「安全なネットワークの検出 (SND)」が検知されます。

# 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。
- <https://mysonicwall.com> にアクセスする。
- 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 を開きます: <https://www.sonicwall.com/ja-jp/support/contact-support>

## このドキュメントについて

- ① | **メモ:** メモアイコンは、補足情報があることを示しています。
- ① | **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。
- ① | **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。

Secure Mobile Access リリースノート  
更新日 - 2022年4月  
ソフトウェアバージョン - 10.2.0.10  
232-005756-00 Rev D

Copyright © 2022 SonicWall Inc. All rights reserved.

本文書の情報はSonicWallおよびその関連会社の製品に関して提供されています。明示的または暗示的、禁反言にかかわらず、知的財産権に対するいかなるライセンスも、本文書または製品の販売に関して付与されないとします。本製品のライセンス契約で定義される契約条件で明示的に規定される場合を除き、SONICWALL および/またはその関連会社は一切の責任を負わず、商品性、特定目的への適合性、あるいは権利を侵害しないことの暗示的な保証を含む(ただしこれに限定されない)、製品に関する明示的、暗示的、または法定的な責任を放棄します。いかなる場合においても、SONICWALL および/またはその関連会社が事前にこのような損害の可能性を認識していた場合でも、SONICWALL および/またはその関連会社は、本文書の使用または使用できないことから生じる、直接的、間接的、結果的、懲罰的、特殊的、または付随的な損害(利益の損失、事業の中断、または情報の損失を含むが、これに限定されない)について一切の責任を負わないものとします。SonicWall および/またはその関連会社は、本書の内容に関する正確性または完全性についていかなる表明または保証も行いません。また、事前の通知なく、いつでも仕様および製品説明を変更する権利を留保し、本書に記載されている情報を更新する義務を負わないものとします。

詳細については、次のサイトを参照してください: <https://www.sonicwall.com/ja-jp/legal>

## 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/end-user-product-agreements/>

## 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