SonicWall™ グローバル VPN クライアント 4.10

管理ガイド

SONICWALL™

凡例

警告: 物的損害、けが、または死亡に至る可能性があることを示しています。

注意: 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。

重要、メモ、ヒント、モバイル、またはビデオ: 補足情報があることを示す表示です。

グローバル VPN クライアント 管理ガイド
更新日 - 2017 年 5 月
ソフトウェア バージョン - 4.10
232-003872-00 Rev A

目次

1

グローバル VPN クライアントの概要

グローバル VPN クライアントの概要

SonicWall™ グローバル VPN クライアントは、プライベート データの機密性を維持するために、コンピュータと企業ネットワーク間に仮想プライベート ネットワーク (VPN) 接続を作成します。グローバル VPN クライアントは、インターネットを通じてリモート ユーザに安全な暗号化されたアクセスのための使いやすいソリューションを提供します。

SonicWall が個別開発したグローバル VPN クライアントは、SonicWall インターネット セキュリティ装置上の GroupVPN と連携して、VPN の配備と管理を劇的に能率化します。SonicWall の Client Policy Provisioning 技術を使用して、SonicOS 管理者はグローバル VPN クライアント用の VPN コネクション ポリシーを確立します。VPN 設定データは SonicWall VPN ゲートウェイ (SonicWall インターネット セキュリティ装置) からグローバル VPN クライアントに透過的にダウンロードされるため、ユーザは VPN コネクションをプロビジョニングする負担から解放されます。

SonicWall セキュリティ装置を設定して SonicOS GroupVPN でグローバル VPN クライアントをサポートする場合は、SonicWall セキュリティ装置 (ご利用の VPN ゲートウェイ装置) で実行中のファームウェア バージョンに対応する『SonicOS 管理ガイド』を参照してください。

トピック:

グローバル VPN クライアントの機能

SonicWall グローバル VPN クライアントは、強力な IPsec VPN ソリューションを提供します。その特長は以下のとおりです。

- **容易な設定と操作** - 素早く簡単にインストールが可能なインストール ウィザードと、選択してクリックするだけで VPN コネクションをアクティブにできるわかりやすい設定ウィザードに加え、サポートの負担を最小限に抑える洗練された管理ツールが提供されています。

- **多言語対応** - グローバル VPN クライアントのユーザ インターフェースは、英語、中国語 (簡体字)、日本語、韓国語、ポルトガル語 (ブラジル) に対応しています。UI は、自動的に Windows の表示言語で表示されます。
- **Client PolicyProvisioning** - SonicWall VPN ゲートウェイの IP アドレスまたは完全修飾ドメイン名 (FQDN) のみを使用して、VPN の設定データが安全な IPsec トンネルを介して SonicWall VPN ゲートウェイから自動的にダウンロードされるため、VPN コネクションをプロビジョニングする負担からリモートユーザを解放します。
- **RADIUS による XAUTH 認証** - グローバル VPN クライアントでは、VPN コネクション確立のための認証に外部 RADIUS サーバを使用して、セキュリティを強化することができます。
- **フェイルセーフによる高可用性を実現するコネクション** - SonicWall VPN ゲートウェイに障害が発生した場合は、自動的にリダイレクトさせることができます。SonicWall VPN ゲートウェイがダウンしている場合、グローバル VPN クライアントは別の SonicWall VPN ゲートウェイを使用することにより VPN トンネルの切断を回避できます。
- **複数のサブネットに対応** - グローバル VPN クライアントは複数のサブネットに接続可能で、企業ネットワークに柔軟に対応します。
- **サードパーティの証明書に対応** - VeriSign、Entrust、Microsoft、Netscape の各認証局 (CA) をサポートし、高性能なユーザ認証を実現しています。
- **VPN トラフィックの制御** - VPN トンネル向けでないすべてのトラフィックを遮断できます。これにより、インターネットからの攻撃が VPN コネクションを通じて企業ネットワーク内に侵入することを防止します。
- **DHCP リレーのサポート** - ISP (インターネット サービス プロバイダ) から取得した IP アドレスを使用した VPN コネクションが可能です。また、VPN トンネルを通じて企業内の DHCP サーバから IP アドレス等の設定を取得することも可能です。
- **安全な VPN 設定** - グローバル VPN クライアントの重要な設定情報はロックされ、ユーザがみだりに変更できないようになっています。
- **AES と 3DES 暗号化** - 168ビットの鍵を使用する 3DES (Data Encryption Standard) と、 AES (Advanced Encryption Standard) をサポートし、セキュリティを向上させます。SonicWall VPN ゲートウェイ装置での AES の使用には SonicOS 2.0 以上が必要です。
- **GMS による管理** - グローバル VPN クライアントのコネクションは、多くの VPN トンネルに対する統合的な管理運用を実現する SonicWall のグローバル管理システム (GMS) で管理できます。
- **複数プラットフォームのクライアントのサポート** - 以下の Windows の 32 ビット版と 64 ビット版をサポートしています。Windows 10、Windows 8、Windows 8.1、Windows 7
- **NAT トラバーサル** - グローバル VPN クライアントは、NAT (ネットワーク アドレス変換) を使用したネットワーク内から外部の SonicWall VPN ゲートウェイに対してVPN 接続することが可能です。SonicWall グローバル VPN クライアントは IPsec VPN トラフィックをカプセル化して、NAT デバイスを通過させます。NAT デバイスは、ローカル ネットワーク全体で 1 つの外部 IP アドレスを使用できるように広く導入されています。
- **障害発生時の自動再接続** - 対岸のゲートウェイとの接続に問題が発生した場合に、グローバル VPN クライアントは再接続を試み続けます。この機能により、グローバル VPN クライアントは一時的に接続できなくなった SonicWall VPN ゲートウェイとの接続をユーザの介入なしに自動的に再開できます。
- **大規模展開のための複製インストール** - グローバル VPN クライアントをインストールして複製イメージを作成した後に仮想アダプタがデフォルト アドレスを取得することが可能です。

- **NT ドメイン ログオン スクリプトのサポート** - グローバル VPN クライアントが IPsec トンネルを確立した後に Windows NT ドメインの認証を受けることができます。SonicWall VPN ゲートウェイはログオン スクリプトをグローバル VPN クライアントの設定の一部として渡します。この機能により、VPN ユーザはマッピングしたネットワーク ドライブやその他のネットワーク サービスにアクセスできます。
- **デュアル プロセッサのサポート** - デュアル プロセッサのコンピュータでグローバル VPN クライアントを使用できます。
- **アドレスオブジェクト単位でのアクセス制限** - グローバル VPN クライアントからのアクセスはカスタマイズ可能で、指定したアドレス オブジェクトへのアクセスを制限できます (SonicOS Enhanced が必要です)。
- **ハブ スポーク型 VPN アクセス** - LAN サブネット以外のすべてのリモート グローバル VPN クライアント用に異なるサブネットを設定するために、SonicWall VPN ゲートウェイの DHCP サーバからグローバル VPN クライアントへの IP アドレスの付与が可能です。これはハブ - スポーク型の VPN アクセスをより簡単にします。グローバル VPN クライアントはセントラル サイトでの認証に成功した場合、仮想の IP アドレスを受け取ります。このアドレスで他の信頼された VPN サイトへのアクセスも可能です。
- **デフォルト VPN コネクション ファイル** - SonicOS 管理者は、VPN クライアントの展開を簡素化するために、グローバル VPN クライアント ソフトウェアに企業用 VPN コネクションを設定して配布可能です。
- **ローミングのための複数 SonicWall セキュア ワイヤレス装置とのシングル VPN コネクション** - 1 つの VPN コネクションで、複数の SonicWall セキュア ワイヤレス装置のネットワークに アクセスできます。
- **DNS を使用した多重化ゲートウェイの自動設定** - IPsec ゲートウェイのドメイン名から複数の IP アドレスが解決される場合、グローバル VPN クライアント はリスト内の IP アドレスをフェイルオーバー ゲートウェイとして扱います。
- **トンネル状態表示機能の拡張** - グローバル VPN クライアントは、VPN トンネルの状態に関する情報を示します。「有効」、「無効」、「接続」の他に「認証中」、「準備中」、「接続中」が、トンネルの状態としてグローバル VPN クライアントに表示されます。
- **ポップアップ ウィンドウによるトンネルの状況表示** - グローバル VPN クライアントは、トンネルが接続または切断されたとき、小さなポップアップ ウィンドウでそのことをユーザに通知します。
- **スマートカードおよび USB トークン認証** - グローバル VPN クライアントは Microsoft Cryptographic アプリケーション プログラム (MS CryptoAPI または MSCAPI) と統合しており、スマートカードや USB トークンにデジタル証明書を使用するユーザ認証をサポートします。
- **NAT-T RFC 3947 に対応** - IKE フェーズ 1 において、2 つの IKE ピア間のパスで NAT を自動的に検出できます。ピア間に NAT が検出されると、パケットはポート 4500 を使用して UDP カプセル化されます。
- **DNS リダイレクト** - 仮想アダプタに関連する DNS 接尾辞 への DNS クエリは、物理アダプタ上では送信されません。
- **VPN トラフィックの制御の拡張** - クリアなトラフィックを、Route All ポリシーで設定されて直接接続されているネットワーク インターフェースにルーティングすることができます。通常、これは WLAN ゾーンで使用されます。
- **VPN コネクションのプログラム自動スタート** - 「**コネクション プロパティ**」ダイアログで指定されているとおりに VPN コネクションが正常に確立した場合、オプションの引数とともにプログラムが自動的に実行されます。

グローバル VPN クライアントエンタープライズ

グローバル VPN クライアントエンタープライズには、グローバル VPN クライアントと同じ機能に加え、ライセンス共有機能が追加されています。

このガイドについて

『*SonicWall グローバル VPN クライアント管理ガイド*』では、SonicWall グローバル VPN クライアントのインストール、設定、取り扱い方法について説明します。また、SonicWall グローバル VPN クライアント エンタープライズについても説明します。

SonicWall セキュリティ装置を設定して SonicOS GroupVPN でグローバル VPN クライアントをサポートする場合は、SonicWall セキュリティ装置 (ご利用の VPN ゲートウェイ装置) で実行中のファームウェア バージョンに対応する『SonicOS 管理ガイド』を参照してください。

トピック:

テキスト表記規則

表記	説明
太字	グローバル VPN クライアント インターフェース、または SonicOS 管理インターフェースで選択できる項目を表します。
メニュー項目 > メニュー項目	続けて複数のメニューを選択することを意味します。例えば、「「**ファイル > 開く**」を選択」は、「**ファイル**」メニューを選択した後に「**開く**」を「**ファイル**」メニューから選択することを意味します。
画面上の文字	コンピュータ画面に表示される文字、またはコマンド ラインから入力する文字を表します。例: `myDevice> show alerts`

メッセージ アイコン

注意を喚起するために以下の記号を使用しています。

警告：物的損害、けが、または死亡に至る可能性について警告する重要な情報です。

注意: ファイアウォールのパフォーマンスやセキュリティ機能に影響を及ぼすか、SonicWall 装置に問題を引き起こす可能性のある機能について注意を促す重要な情報です。

ヒント: SonicWall 装置のセキュリティ機能および設定に関する便利な情報です。

重要: 特に注意が必要な機能に関する重要な情報です。

補足: 機能に関する補足情報です。

モバイル： SonicWall 装置のモバイル アプリに関する有益な情報です。

ビデオ： SonicWall 装置の機能に関する詳細情報を紹介するビデオへのリンクです。

2

グローバル VPN クライアント導入ガイド

このセクションでは、SonicWall グローバル VPN クライアントのインストール、アップグレード、起動について説明します。

グローバル VPN クライアントのインストール

SonicWall グローバル VPN クライアントは、操作の簡単なウィザードを使用してインストール処理を行います。

補足: グローバル VPN クライアントのインストールには管理者権限が必要です。

SonicWall グローバル VPN クライアントは、32 ビットまたは 64 ビット版の Windows 10、Windows 8.1、Windows 8、Windows 7 のクライアント オペレーティング システム上で動作します。

グローバル VPN クライアントは、Gen5 (5.0 以降) および Gen6 (6.1 以降) の SonicOS ファームウェア バージョンを実行するすべての SonicWall セキュリティ装置でサポートされています。

補足: ご使用の SonicWall 装置でサポートされる SonicWall グローバル VPN クライアント接続数や、ご使用の装置に対するグローバル VPN クライアントのライセンスについては、グローバル VPN クライアントのライセンス (52 ページ)を参照してください。

セットアップ ウィザードの使用

このセクションでは、**セットアップ ウィザード**を使用して SonicWall グローバル VPN クライアントプログラムをインストールする方法について説明します。

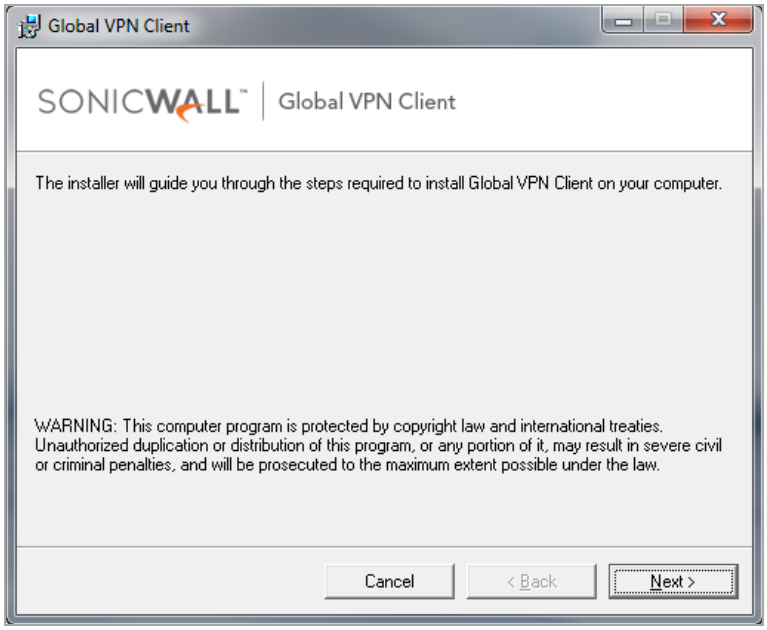
重要: 最新の SonicWall グローバル VPN クライアントをインストールする前に、サードパーティの VPN クライアント プログラムをすべて削除してください。

SonicWall グローバル VPN クライアントがインストールされている場合は、それをアンインストールしてから バージョン 4.10.x をインストールします。

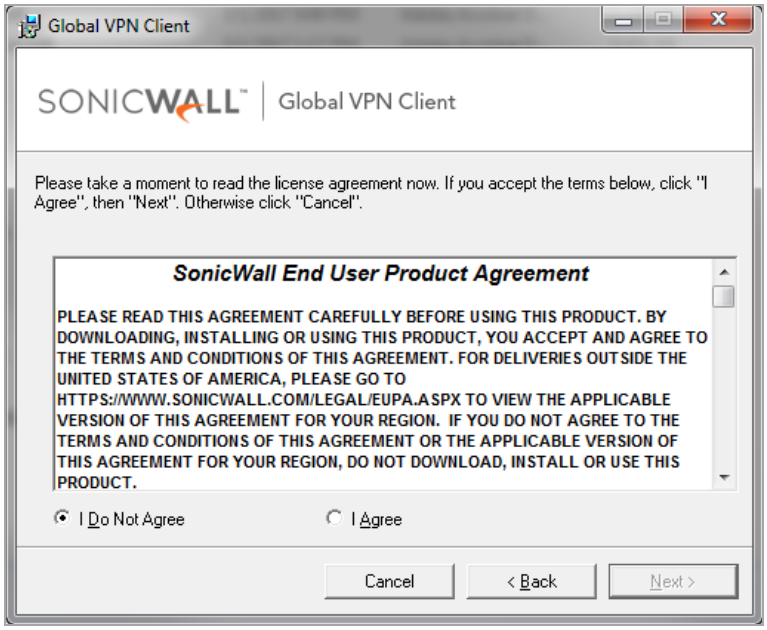
セットアップ ウィザードを使用するには:

1 MySonicWall から自己解凍型のインストーラ **GVCSetupXX.exe** (**XX** は、32 ビット Windows プラットフォームの場合は **32**、64 ビット Windows プラットフォームの場合は **64**) をダウンロードします。

2 **GVCSetupXX.exe** をダブルクリックします。**セットアップ ウィザード**が起動します。

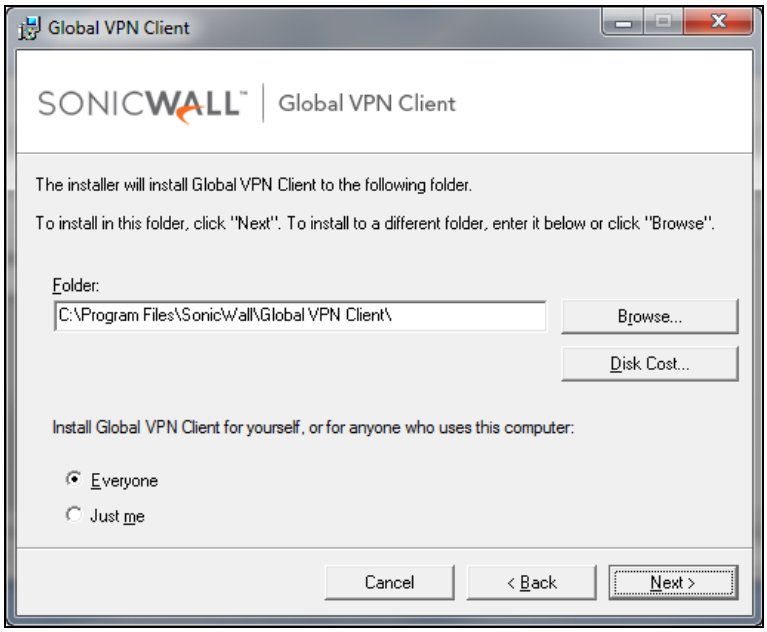


3 「**次へ**」をクリックして VPN クライアントのインストールを続行します。「**ライセンス規約**」ページが表示されます。



4 「**同意する**」ラジオ ボタンを選択します。

5 「**次へ**」を選択します。「**インストール フォルダの選択**」ページが表示されます。

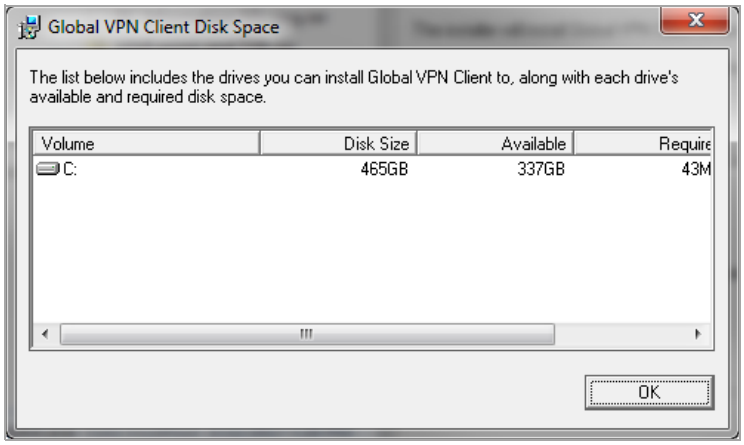


6 別のインストール先を指定する場合は、「**参照**」をクリックします。

a 場所を選択します。

b 「**OK**」を選択します。

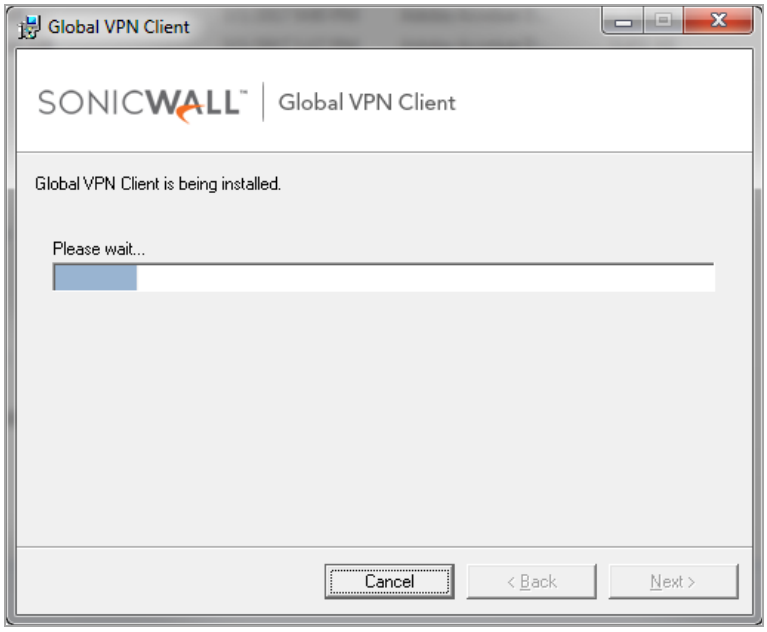
7 必要に応じて、「**ディスク領域**」ボタンをクリックして、必要なディスク容量を確認します。



8 「**SonicWall グローバル VPN クライアントを現在のユーザ用か、またはすべてのユーザ用にインストールします**」の下で、「**すべてのユーザ**」または「**このユーザのみ**」のいずれかを選択します。

9 「**次へ**」を選択します。すると、インストールの準備が整ったことを示すページが表示されます。

10 「**次へ**」を選択します。「**グローバル VPN クライアントをインストール中**」というページが表示され、インストールの進行状況が示されます。



11 SonicWall グローバル VPN クライアントのファイルがコンピュータにインストールされるまで待ちます。インストールが完了したら、「**グローバル VPN クライアントは正しくインストールされました**」というページが表示されます。

12 「**閉じる**」を選択してウィザードを閉じます。インストールが完了した後の動作は、保存済みの接続があるかどうかによって異なります。

- SonicWall グローバル VPN クライアントの前のバージョンの接続設定を保存していた場合、グローバル VPN クライアントが起動すると、デフォルトの接続によってログイン資格情報の入力を求められます。
- 以前の接続設定がない場合は、「**コネクションの作成ウィザード**」が自動的に起動します。これは、グローバル VPN クライアントの初回起動時のみ行われます。詳細について

は、コネクションの作成ウィザードを使用した VPN コネクションの作成 (20 ページ)を参照してください。

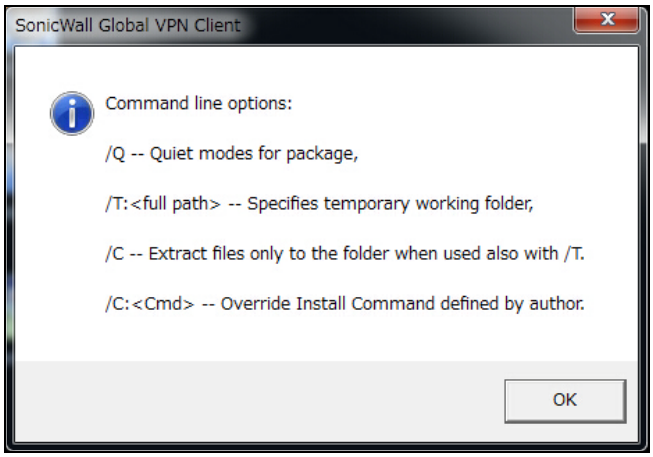
ヒント: 「**表示 > オプション**」ページの「**一般**」タブで、コンピュータにログオンするたびにグローバル VPN クライアントが毎回自動時に起動するように設定できます。詳細については、グローバル VPN クライアントの起動オプションの指定 (17 ページ)を参照してください。

グローバル VPN クライアントを前のバージョンからアップグレードする

前のバージョンからのアップグレードはサポートされていません。バージョン 4.9.22 以前の SonicWall グローバル VPN クライアントがインストールされている場合は、そのバージョンをアンインストールして PC を再起動してから バージョン 4.10.x をインストールしてください。4.10.x のインストーラでは、以前のバージョンからのアップグレードはできません。

インストール用のコマンドライン オプション

複数のコマンドライン オプションが、SonicWall グローバル VPN クライアントのインストールに使用できます。



オプションはすべて大文字・小文字を区別せず、フォワード スラッシュ (/) を前に置く必要があります。

- **/Q** – クワイエット モード。SonicWall グローバル VPN クライアントの通常 (サイレントでない) インストールでは、ユーザは必要な情報をダイアログのフォームに対して入力する必要があります。しかし、サイレント インストールでは、入力が求められることはなく、代わりに全オプションに対してデフォルトが使用されます。以下の **XX** の個所は、32 ビット Windows プラットフォームの場合は **32**、64 ビット Windows プラットフォームの場合は **64** と入力します。

  ```
  GVCSetupXX.exe /q
  ```

- **/T** – インストール プロセス中に生成される一時ファイルを置いておく一時作業フォルダを指定します。T オプションでは、その後ろにコロン (:) と使用するフォルダに対するフルパスを記述する必要があります。例えば、次のように入力します。

  ```
  GVCSetupXX.exe /t:C:\TemporaryFiles
  ```

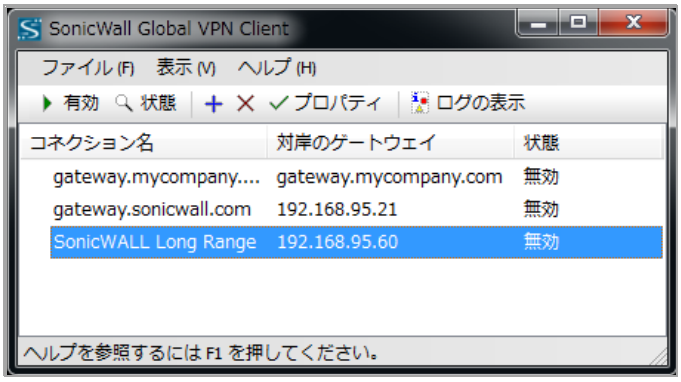
- **/C** – インストール パッケージから抽出された全ファイル (MSI インストーラ ファイル) を T オプションで指定されるフォルダ内に配置します。C オプションは、T オプションと一緒に使用された場合にのみ有効です。例えば、次のいずれかのように入力します。

  ```
  GVCSetupXX.exe /c /t:C:\TemporaryFiles
  GVCSetupXX.exe /T:C:\TemporaryFiles /c
  ```

グローバル VPN クライアントの起動

SonicWall グローバル VPN クライアントを起動するには:

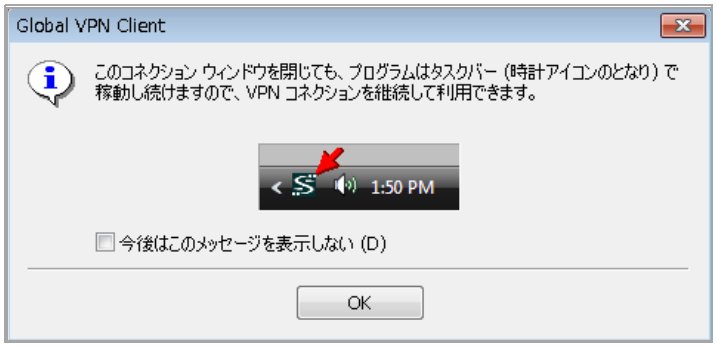
1 「**スタート > すべてのプログラム > グローバル VPN クライアント**」を選択します。



2 次の操作を実行できます。

- 確立した VPN コネクションをアクティブにしたままでグローバル VPN クライアントのダイアログを閉じるには、「**X**」をクリックするか、**Alt+F4** を押すか、または「**ファイル > 閉じる**」を選択します。

  ダイアログを閉じても、グローバル VPN クライアントプログラムと、有効化されているすべての VPN コネクションは継続して利用できることを通知するメッセージが表示されます。



  グローバル VPN クライアントのダイアログを閉じるたびにこの通知メッセージを表示したくない場合は、次の操作を行います。

  a) 「**今後はこのメッセージを表示しない**」チェックボックスをオンにします。

  b) 「**OK**」を選択します。

- グローバル VPN クライアントのダイアログを表示するには:
  - システム トレーのグローバル VPN クライアントアイコンをダブルクリックします。

- アイコンを右クリックし、「**グローバル VPN クライアントを開く**」を選択します。

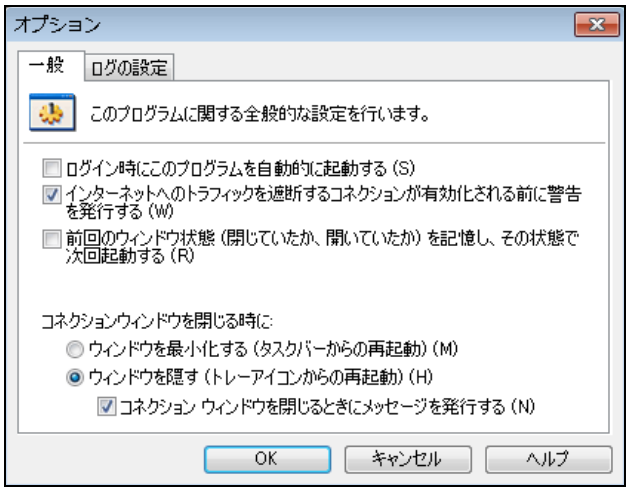
注意: SonicWall グローバル VPN クライアントをシステム トレーのアイコン メニューから終了すると、有効な VPN コネクションがすべて無効になります。

ヒント: 次の操作が可能です。

- SonicWall グローバル VPN クライアントのデフォルトの起動設定を変更できます。詳細については、グローバル VPN クライアントの起動オプションの指定 (17 ページ)を参照してください。
- デスクトップ、タスクバー、**スタート** メニューからグローバル VPN クライアントダイアログを自動的に開いて VPN コネクションを有効化するためのショートカットを作成できます。詳細については、グローバル VPN クライアントのライセンス (52 ページ)を参照してください。
- グローバル VPN クライアントをコマンドラインから起動できます。詳細については、グローバル VPN クライアント CLI の使用 (63 ページ)を参照してください。

グローバル VPN クライアントの起動オプションの指定

「**オプション**」ダイアログの「**一般**」タブの制御設定により、SonicWall グローバル VPN クライアントの起動方法と、通知ウィンドウの表示内容を指定できます。「**表示 > オプション**」を選択して「**オプション**」ダイアログを表示します。



「**一般**」タブには、グローバル VPN クライアントの起動を制御する以下の設定があります。

- **ログイン時にこのプログラムを自動的に起動する** - コンピュータにログインすると、SonicWall グローバル VPN クライアントが起動します。
- **インターネット へのトラフィックを遮断するコネクションが有効化される前に警告を発行する** - 「**コネクションに関する警告**」メッセージをアクティブ化し、VPN コネクションによってローカル インターネットとネットワーク トラフィックがブロックされることを通知するようにします。
- **前回のウィンドウ状態 (閉じていたか、開いていたか) を記憶し、その状態で次回起動する** - 次回プログラムを開始する時に、グローバル VPN クライアントが最後のウィンドウ状態 (閉じていたか、開いていたか) を記憶できるようにします。例えば、ユーザはデスクトップ上のウィンドウを開けずに、システム トレーからグローバル VPN クライアントを起動できます。

- **コネクション ウィンドウを閉じる時に** - ウィンドウを閉じる場合のグローバル VPN クライアントの動作を指定します。
  - **ウィンドウを最小化する (タスクバーからの再起動)** - グローバル VPN クライアント ウィンドウを最小化してタスクバーに入れ、ウィンドウを開く場合はタスクバーから元に戻します。
  - **ウィンドウを隠す (トレーアイコンからの再起動)** - グローバル VPN クライアントウィンドウを閉じる際に非表示にするデフォルト設定です。グローバル VPN クライアントは、システム トレーのプログラム アイコンから起動できます。この設定を有効にすると、「**コネクションウィンドウを閉じるときにメッセージを発行する**」チェックボックスも表示されます。
    - **コネクションウィンドウを閉じるときにメッセージを発行する** - このチェックボックスをオンにすると、プログラムの実行中に**グローバル VPN クライアント**ウィンドウを閉じたときに必ず、「**SonicWall グローバル VPN クライアント非表示通知**」ウィンドウが表示されます。このウィンドウには、ウィンドウを閉じて (非表示にして) も、グローバル VPN クライアントプログラムが実行し続けることを通知するメッセージが表示されます。

グローバル VPN クライアントのシステム トレー アイコンの管理

グローバル VPN クライアントウィンドウを起動すると、プログラム アイコンがタスクバーのシステムトレーに表示されます。

このアイコンは、プログラムと VPN コネクションの状況インジケータや、SonicWall グローバル VPN クライアントの共通コマンドのメニューとなります。システム トレーの**グローバル VPN クライアント**アイコンを右クリックすると、プログラム管理オプションのメニューが表示されます。

- **グローバル VPN クライアントを開く** - プログラム ウィンドウを表示します。
- **有効化** - 有効化できる VPN コネクションのメニューを表示します。
- **無効化** - 無効化できる VPN コネクションのメニューを表示します。
- **ログ ビューアを開く** - ログ ビューアを開いて情報やエラー メッセージを表示します。ログ ビューアの詳細については、グローバル VPN クライアントのログについて (44 ページ)を参照してください。
- **証明書マネージャを開く** - 証明書マネージャを開きます。証明書マネージャの詳細については、証明書の管理 (42 ページ)を参照してください。
- **終了** - **グローバル VPN クライアント**ウィンドウを終了し、すべてのアクティブ状態の VPN コネクションを無効にします。

システム トレーのグローバル VPN クライアントアイコンにマウスを重ねると、有効化されている VPN コネクション数が表示されます。

システム トレーの**グローバル VPN クライアント**アイコンは、グローバル VPN クライアントと SonicWall ゲートウェイの間を通過するデータに関する視覚的なインジケータとしても機能します。

3

VPN コネクションの追加

VPN コネクションについて

グローバル VPN クライアントでは、複数のコネクションを同時に設定することができます。それらのコネクションが複数のゲートウェイからプロビジョニングされているか、1 つまたは複数のファイルからインポートされているかは問いません。コネクションは複数のゲートウェイから設定できるため、コネクションポリシーが競合している場合には、各コネクションが許可された動作を明示的に指定します。管理者は、複数のコネクション設定情報がある場合に許可される動作を明示的に指定します。

VPN コネクションポリシーには、ゲートウェイへの安全な IPsec トンネルを確立するのに必要なパラメータがすべて含まれます。以下に示すように、コネクション ポリシーにはフェーズ 1 とフェーズ 2 のセキュリティ アソシエーション (SA) パラメータが含まれます。

- 暗号化と認証のプロポーザル
- フェーズ1 の ID ペイロード タイプ
- フェーズ2 のプロキシ ID (トラフィック セレクタ)
- クライアントのフェーズ1 クレデンシャル
- 他のアクティブな VPN コネクションがある場合に許可される接続動作
- クライアントのキャッシュ動作

新しい VPN コネクションの追加は簡単です。SonicWall の Client Policy Provisioning では、必要な設定情報はすべて自動的に提供され、ローカル ネットワークまたはリモート ネットワークと安全に接続されます。グローバル VPN クライアントのユーザは、VPN コネクション パラメータを設定する負担から解放されます。VPN コネクションは以下の 3 つの方法で作成できます。

- 「**コネクションの作成ウィザード**」を使用して SonicWall VPN ゲートウェイからグローバル VPN クライアントに VPN ポリシーをダウンロードします。このウィザードは、設定情報の配布元を特定する過程を通じて、安全な IPsec VPN トンネル上で VPN コネクション設定情報を自動的にダウンロードします。
- SonicWall グローバル VPN クライアントに VPN ポリシー ファイルをインポートします。VPN ポリシーは .rcf ファイルとして送られます。これは**コネクションのインポート** ダイアログを使用してインストールされます。
- グローバル VPN クライアントソフトウェアの一部として `default.rcf` ファイルをインストールするか、グローバル VPN クライアントをインストールした後に default.rcf ファイルを追加しま

す。SonicWall VPN ゲートウェイの管理者が default.rcf ファイルをグローバル VPN クライアントソフトウェアの一部として含めた場合、事前設定されている 1 つ以上の VPN コネクションがプログラムのインストール時に自動的に作成されます。

補足: default.rcf ファイルを作成してグローバル VPN クライアント ソフトウェアとともに配布すると、SonicWall VPN ゲートウェイの管理者は VPN クライアントを効率的に展開できるようになり、ユーザは素早く VPN コネクションを確立できるようになります。default.rcf ファイルがダウンロードしたグローバル VPN クライアント ソフトウェアに含まれている場合、SonicWall VPN ゲートウェイの管理者が設定した VPN ポリシーが使用され、クライアントソフトウェアのインストール時にコネクションが自動的に作成されます。default.rcf ファイルの作成についての詳細は、default.rcf ファイルの使用 (54 ページ)を参照してください。

補足: グローバル VPN クライアントの自動プロビジョニングをスムーズにするには、SonicWall 装置の設定に GroupVPN を使用します。GroupVPN での装置の設定については、『SonicOS 管理ガイド』を参照してください。

補足: グローバル VPN クライアントに証明書をインポートする手順については、証明書の使用 (42 ページ)を参照してください。

コネクションの作成ウィザードを使用した VPN コネクションの作成

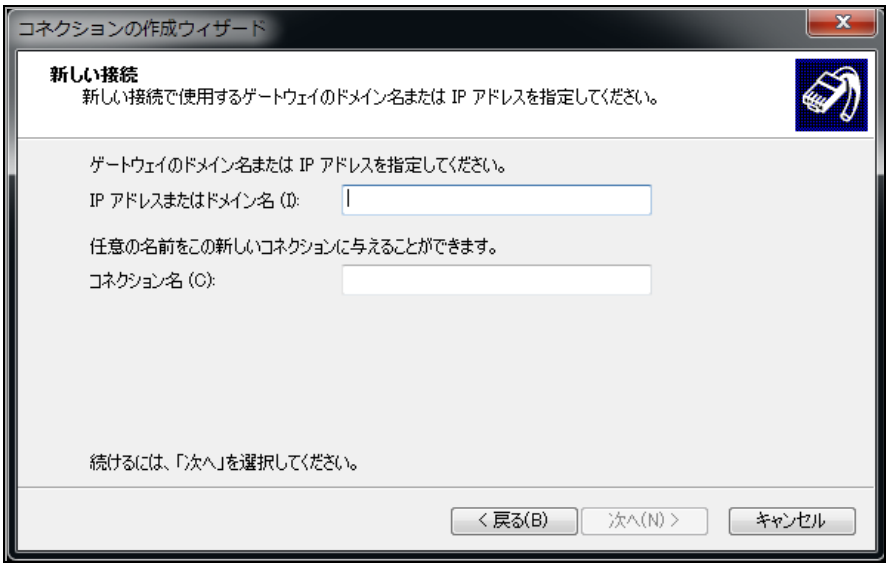
「**コネクションの作成ウィザード**」を使用してローカルまたはリモートの SonicWall VPN ゲートウェイからグローバル VPN クライアントの VPN コネクション ポリシーを自動的にダウンロードする手順を以下に説明します。

「コネクションの作成ウィザード」を使用するには:

1 「**スタート > すべてのプログラム > グローバル VPN クライアント**」を選択します。SonicWall グローバル VPN クライアントを最初に起動した時には、自動的に「**コネクションの作成ウィザード**」が起動します。

2 「**コネクションの作成ウィザード**」が表示されない場合は、「 **コネクションの作成** 」ボタン をクリックして起動します。

3 「**次へ**」を選択します。「**コネクションの作成**」ページが表示されます。



4 ゲートウェイの IP アドレスまたは FQDN を「**IP アドレスまたはドメイン名**」フィールドに入力します。「**IP アドレスまたはドメイン名**」フィールドに入力した値は「**コネクション名**」フィールドにも入力されます。

5 コネクション名を変更したい場合は、「**コネクション名**」フィールドに新しい名前を入力してください。

6 「**次へ**」を選択します。「**コネクションの作成ウィザードの終了**」ページが表示されます。

7 必要に応じて、以下を行います。

- この VPN コネクション用のショートカット アイコンをデスクトップ上に作成する場合は、「**作成したコネクションのショートカットをデスクトップに作成する**」を選択します。
- SonicWall グローバル VPN クライアントの起動時に、VPN コネクションを自動的に確立する場合は、「**プログラム起動時にこのコネクションを有効にする**」を選択します。

8 「**完了**」を選択します。作成した VPN コネクションが、**グローバル VPN クライアント** ウィンドウに表示されます。

VPN 設定ファイルのインポート

VPN コネクションは、SonicWall VPN ゲートウェイの管理者がファイルとして作成してユーザに送付できます。この VPN 設定ファイルは、ファイル名に .rcf という拡張子が付けられます。管理者から VPN コネクション ファイルを受け取ったら、「**コネクションのインポート**」ダイアログを使用してそれをインストールすることができます。

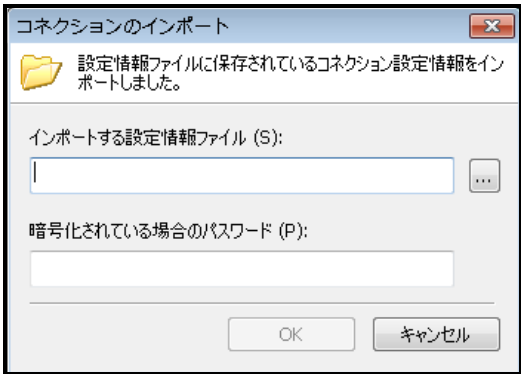
VPN ポリシー ファイルは XML 形式になっており、ポリシー情報が効率よくエンコードされるようになっています。ファイルは暗号化できるため、事前共有鍵もファイルに入れてエクスポートできます。暗号化方式は RSA Laboratories の PKCS#5 Password-Based Cryptography Standard (パスワード ベースの暗号化標準) に準拠しており、3DES 暗号化と SHA-1 メッセージ ダイジェスト アルゴリズムを使用します。

補足: SonicWall 装置からエクスポートされる .rcf ファイルが暗号化されている場合は、グローバル VPN クライアントにインポートする際にパスワードが必要です。

ゲートウェイ管理者から提供されたコネクション ファイルをインポートして VPN コネクションを追加するには:

1 「**スタート** > **すべてのプログラム** > グローバル VPN クライアント」を選択します。

2 「**ファイル** > **インポート**」を選択します。「**コネクションのインポート**」ダイアログが表示されます。



3 次のどちらかを行います。

- 「インポートする設定情報ファイル」フィールドにファイルのパスを入力します。
- 「**参照**」ボタン … をクリックして、ファイルを指定します。

4 ファイルが暗号化されている場合は、「**暗号化されている場合のパスワード**」フィールドにパスワードを入力します。

5 「**OK**」を選択します。

別のワークステーションのグローバル VPN クライアントの使用

SonicWall グローバル VPN クライアントを使用して Microsoft Network に接続する場合には、一部制限があります。通常、Microsoft Network に属しているコンピュータは、ユーザの資格情報を確認するドメイン コントローラに永続的にネットワーク接続します。ユーザの資格情報がドメイン コントローラで確認されると、ローカルにキャッシュされたプロファイルが作成され、ドメイン コントローラ

が利用できない際に使用されます。しかし SonicWall グローバル VPN クライアントは、ドメイン コントローラを含む Microsoft Network に対してインターネットを介したアドホックで安全なネットワーク接続を提供するため、コネクションは永続的にはなりません。リモート コンピュータは、SonicWall グローバル VPN クライアントによって接続が行われるまでドメイン コントローラに接続してログオン資格情報を確認することができないため、ローカルにキャッシュされたプロファイルを利用できない場合はログオンに失敗します。

ありがちな問題を以下に示します。

1 Microsoft ドメイン コントローラに対してリモートから通信するには、グローバル VPN クライアントのセッションを確立する必要があります。

2 グローバル VPN クライアントは、ワークステーションにログオンした後にしか起動できません。ログオンする前にグローバル VPN クライアントを接続する手段はないため、最初のログオン時にはそれをドメイン ログオンに使用することはできません。

3 以前にワークステーションにログオンしている場合には、ログオンに使用されるローカルにキャッシュされたプロファイルが存在します。

   a それによってグローバル VPN クライアントが起動でき、ドメインへの接続が確立します。

   b ドメインへの接続後は、ログオン スクリプトの実行、パスワードの変更、ドメイン リソースへのアクセスなどが可能になります。

   c ログオフすると、グローバル VPN クライアントは終了し、ドメイン通信ができなくなります。

4 以前にワークステーションにログオンしていない場合には、ログオンに使用されるローカルにキャッシュされたプロファイルが存在しないため、ログオンすることはできません。

ログオフ (手順 c) すると SonicWall グローバル VPN クライアントが終了するため、別のユーザはログオンすることも、ローカルにキャッシュされた新規のプロファイルを作成することもできません。これには、既存の (ローカルにキャッシュされた) プロファイルを持つユーザ以外はグローバル VPN クライアントを通してログオンできないという望ましくない影響があります。

これに対する標準的な対策は、まずドメイン コントローラにローカルに接続してから、SonicWall グローバル VPN クライアントを使用する予定の各アカウントでログオンすることです。これによって、ローカルにキャッシュされたプロファイルが各アカウントに対して作成され、ドメイン コントローラに接続しなくてもクライアントのログオンが有効になります。

この対策において残念なのは、コンピュータ上にキャッシュされたプロファイルがないユーザはドメイン コントローラを持つネットワークを利用しなければログオンできないことです。これは、遠く離れたオフィスからメイン オフィスに戻るなどの特定の状況においては、非常に扱いにくくなります。

対策 - ローカルにキャッシュされた新規プロファイルの強制的な作成

上記の問題を回避するには、ローカル プロファイルを強制的に作成してから、SonicWall グローバル VPN クライアントを使用して Microsoft ドメインにログオンします。

ローカル プロファイルを強制的に作成するには:

1 ローカルにキャッシュされたプロファイル (たとえば `mydomain\user1` または ローカル マシン アカウント) でワークステーションにログオンします。ローカルにキャッシュされたプロファイルは通常、`C:\Documents and Settings` ディレクトリに保存されています。このパスに `user1` というフォルダがあり、その中に user1 のプロファイルがあります。

2 SonicWall グローバル VPN クライアントを起動します。

3 SonicWall グローバル VPN クライアントがコネクションを確立し、ワークステーションがドメイン コントローラと通信できるようになったら、ローカルにキャッシュされた別のプロファイルの作成が可能になります。user1 から提供されるグローバル VPN クライアントのコネクションを使用しながら、runas コマンドを使用して新しいユーザ (たとえば mydomain\user2) 向けのローカルにキャッシュされたプロファイルを作成することができます。

4 コマンド プロンプトで、「runas /user:mydomain\user2 explorer.exe」と入力します (mydomain の部分には実際のドメインを、user2 の部分には実際のユーザ名を入力します)。好みに応じて、explorer.exe の代わりに notepad.exe を使うこともできます。

5 プロンプトに対して、user2 のドメイン パスワードを入力します。

6 user2 のローカル プロファイルの作成と explorer.exe プログラムの起動には、数秒から数分かかります。起動後は、explorer.exe プログラムを終了できます。

7 この時点で、C:\Documents and Settings ディレクトリには user2 のフォルダが含まれています。

8 グローバル VPN クライアントを閉じます。

9 user1 としてワークステーションからログオフします。お馴染みの「**Windows にログオンします**」というダイアログが表示されます。

10 新たに作成されたローカルにキャッシュされたプロファイルで、user2 としてワークステーションにログオンします。

11 SonicWall グローバル VPN クライアントを起動します。この時点で、user2 プロファイルによって、すべてのドメイン アクセス (実行中のログオン スクリプトも含む) の資格情報が提供されます。

12 この手順は、追加のプロファイルの作成が必要になる度に何度でも繰り返すことができます。

また、グローバル VPN クライアントからドメイン コントローラに接続できる別のアカウントを持っている場合は、期限切れのユーザ パスワードをこの手順で変更することもできます。パスワードは、Windows セキュリティ ダイアログから簡単に変更できます。ダイアログを表示するには、

1 **Ctrl+Alt Delete** を押します。

2 「**パスワードの変更**」を選択します。

3 古いパスワードを入力します。

4 新しいパスワードを入力します。

5 新しいパスワードを再度入力します。

6 **矢印**ボタンをクリックします。

4

VPN コネクションの確立

概要

設定情報が SonicWall VPN ゲートウェイで管理されているため、グローバル VPN クライアントからの VPN コネクションの確立は簡単です。SonicOS (VPN ゲートウェイ) 管理者は VPN コネクションに許可する内容と許可しない内容のパラメータを設定します。例えば、セキュリティ上の理由から複数の VPN コネクションを許可しない、VPN コネクション中はインターネットやローカル ネットワークへのアクセスを制限するといった設定が可能です。

グローバル VPN クライアントは次の 2 つの IPsec 認証モードに対応しています。

- IKE (事前共有鍵を使用)
- IKE (サード パーティ証明書を使用)

事前共有鍵は、IPSec 認証モードの最も一般的な形式です。VPN コネクション ポリシーがサードパーティ証明書を使用している場合は、証明書マネージャを使用して、グローバル VPN クライアントがデジタル証明書を使うように設定します。

事前共有鍵 (単に共有鍵ともいう) は VPN トンネルの 2 つのエンドポイントで IKE (Internet Key Exchange) セキュリティ アソシエーションを設定するために事前に定義されたパスワードです。このフィールドは、4 から 128 文字までのアルファベットと数字の組み合わせで構成できます。事前共有鍵は通常、グローバル VPN クライアントのプロビジョニングの一部として設定されます。そうでない場合は、リモート ネットワークにログインする際に事前共有鍵の入力を求められます。

多重化ゲートウェイへのアクセス

グローバル VPN クライアントは、VPN コネクションの「プロパティ」ウィンドウの「対岸候補」タブで対岸のゲートウェイを手動で追加することによる、VPN ゲートウェイの多重化をサポートします。IPsec ゲートウェイのドメイン名から複数の IP アドレスが解決される場合、グローバル VPN クライアントは多重化ゲートウェイを自動的にサポートします。例えば、`gateway.yourcompany.com` から `67.115.118.7` と `67.115.118.8` と `67.115.118.9` が解決される場合、グローバル VPN クライアントは解決されたこれらの IP アドレスに対し、応答するゲートウェイを見つけるまで順に接続を試行します。つまり、複数の IP アドレスをフェイルオーバー ゲートウェイとして使用することができます。解決されたどの IP アドレスからも応答がなく、別の対岸のゲートウェイが「**プロパティ**」ダイアログの「**対岸候補**」タブで設定されている場合、グローバル VPN クライアントは次の対岸のゲートウェイに接続を切り替えます。詳細については、コネクション プロパティの対岸候補の設定 (34 ページ)を参照してください。

補足: VPN 多重化ゲートウェイを設定する際、グループ VPN ポリシーの属性 (事前共有鍵や「**対岸候補の情報**」ページ上の属性など) は、ゲートウェイの FQDN が複数の IP アドレスに解決される場合には、すべてのゲートウェイに共通のものである必要があります。ただし、「**対岸候補**」タブで複数の対岸候補をセットアップする場合は、各対岸候補のゲートウェイは独自の設定を持つことができます。

VPN コネクションの確立

SonicWall グローバル VPN クライアントによる VPN コネクションの確立は、2 フェーズからなる透過的なプロセスです。フェーズ 1 でコネクションが有効になり、ISAKMP (Internet Security Association and Key Management Protocol) ネゴシエーションが完了します。フェーズ2 はIKE（Internet Key Exchange）ネゴシエーションで、これでデータ送受信のためのVPN トンネルが確立されます。

VPN コネクションを有効にすると、グローバル VPN クライアント ウィンドウの「**状況**」列に以下の情報が表示されます。

- 「***無効***」が「***接続中***」に変わります。
- 「**ユーザ名 / パスワードを入力してください**」というダイアログが表示されると、「***接続中***」が「***認証中***」に変わります。
- ユーザ名およびパスワードを入力すると、「***認証中***」が「***接続中***」に変わります。
- 「***接続中***」が「***認証中***」に変わります。
- VPN コネクションが完全に確立されると、「***準備中***」が「***接続済み***」に変わります。VPN コネクション アイコンに緑のチェックマークが表示されます。

VPN コネクションが確立されると、グローバル VPN クライアントのシステム トレイ アイコンのポップアップ通知に、「**コネクション名、IP アドレスに接続済み、仮想 IP アドレス**」が表示されます。

VPN 接続中にエラーが発生すると、「**状況**」列に「**エラー**」が表示され、「VPN コネクション」アイコンにエラー マーク (赤の X) が表示されます。VPN コネクションがすべてのフェーズ 2 のコネクションを正常に完了できない場合は、「**コネクション**」アイコンに黄色の警告マークが表示されます。

補足: グローバル VPN クライアントで VPN コネクションが確立されない場合は、「ログ ビューア」を使用してエラーメッセージを表示し、問題をトラブルシューティングすることができます。詳細については、グローバル VPN クライアントのログについて (44 ページ)を参照してください。

グローバル VPN クライアントを使用して VPN コネクションを確立するには:

1 次のいずれかの方法で VPN コネクションを有効にします。

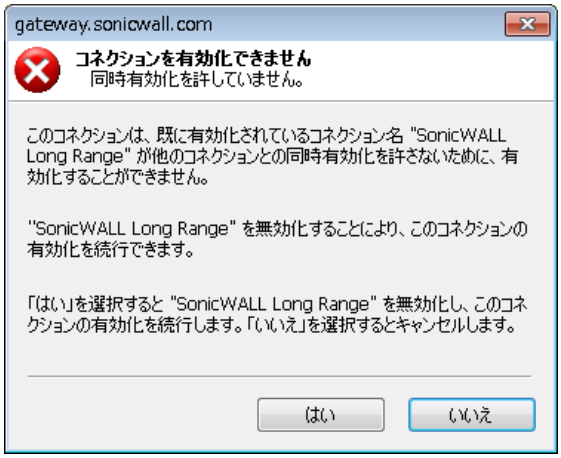
- 「**コネクションの作成ウィザード**」で「**プログラムの起動時にこのコネクションを有効にする**」を選択した場合は、SonicWall グローバル VPN クライアントの起動時に自動的に VPN コネクションが確立されます。
- グローバル VPN クライアントの起動時に VPN コネクションが自動的に確立されない場合は、次のいずれかの方法を選択して VPN コネクションを有効化します。
  - VPN コネクションをダブルクリックします。
  - コネクション名アイコンを右クリックして、メニューから「**有効化**」を選択します。
  - コネクション名を選択して、**Ctrl+B** を押します。
  - コネクション名を選択して、ツールバーの「**有効化**」ボタンをクリックします。
  - コネクション名を選択して、「**ファイル > 有効化**」を選択します。
- **グローバル VPN クライアント**アイコンがシステム トレーに表示されている場合は、そのアイコンを右クリックし、「**有効化** > コネクション名」を選択します。グローバル VPN クライアントは、**グローバル VPN クライアント**ウィンドウを開くことなく VPN コネクションを有効化します。

2 VPN コネクションの設定に応じて、以下のダイアログが表示される場合があります。

- **コネクションを有効化できません** – 複数のコネクションの確立 (27 ページ)を参照
- **事前共有鍵を入力してください** – 事前共有鍵の入力 (28 ページ)を参照
- **ユーザ名およびパスワードを入力してください** – ユーザ名とパスワードの認証 (29 ページ)を参照
- **コネクションに関する警告** – コネクションに関する警告 (30 ページ)を参照

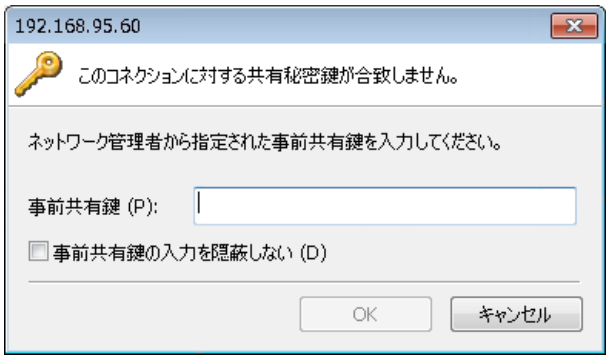
複数のコネクションの確立

1 回の操作で複数のコネクションを有効化できますが、それは VPN ゲートウェイで確立されるコネクションパラメータに依存しています。ゲートウェイが、複数のコネクションを許可しない状態で、グローバル VPN クライアントが追加コネクションを有効にしようとすると、現在有効になっている VPN ポリシーが複数の有効な VPN コネクションを許可しないため、VPN コネクションを確立できないことを知らせる「**コネクションを有効化できません**」というメッセージが表示されます。追加のコネクションを有効にするには、現在有効になっているコネクションを無効にする必要があります。



事前共有鍵の入力

VPN コネクションの属性によっては、デフォルトの事前共有鍵を使用しない場合、VPN コネクションを確立するために事前共有鍵をゲートウェイ管理者から取得する必要があります。ダウンロードまたはファイルとしてインポートされたデフォルト事前共有鍵がコネクション ポリシーの一部として含まれていない場合、VPN コネクションの確立前に「**事前共有鍵を入力してください**」というダイアログが表示されます。



事前共有鍵を入力するには:

1 「事前共有鍵」フィールドに事前共有鍵を入力します。セキュリティ保護のために、デフォルトでは事前共有鍵は表示されません。

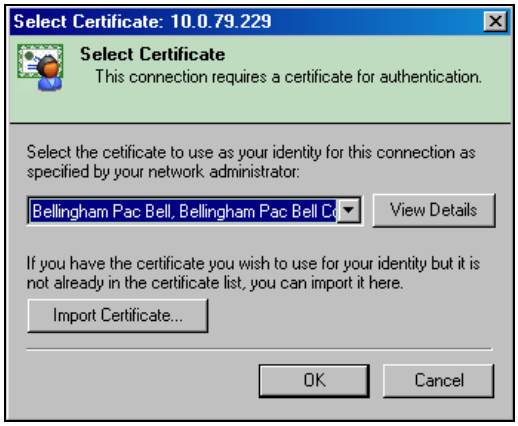
2 正しい事前共有鍵が入力できているかどうか確認する場合は、「事前共有鍵の入力を隠蔽しない」を選択します。入力した事前共有鍵がそのまま「事前共有鍵」フィールドに表示されます。

> **ヒント:** このオプションを有効にした場合は、事前共有鍵を確認した後で必ず解除してください。

3 「OK」を選択します。

証明書の選択

SonicWall VPN ゲートウェイが、VPN コネクション用の ID を確立するためにデジタル証明書を要求する場合は、「**Select Certificate (証明書の選択)**」ダイアログが表示されます。このダイアログには、グローバル VPN クライアントにインストールされた利用可能な証明書がすべて表示されます。



> **補足:** 「証明書マネージャ」の使い方の詳細については、証明書の管理 (42 ページ)を参照してください。

証明書を選択するには:

1 以下のいずれかを実行します。

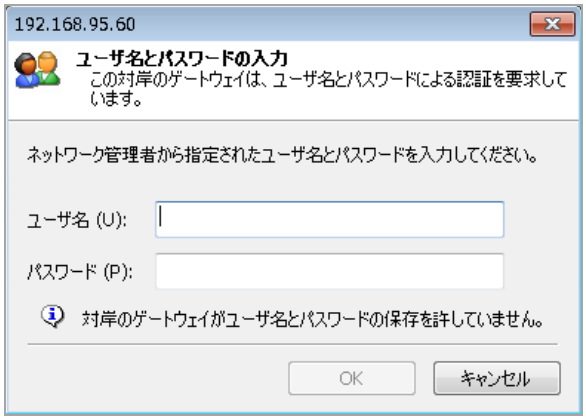
- メニューから証明書を選択します。
- 保有している証明書が「**証明書マネージャ**」を使用してグローバル VPN クライアントにインポートされていない場合は、「**証明書のインポート**」をクリックします。

2 「**OK**」を選択します。

ユーザ名とパスワードの認証

ゲートウェイ管理者によりリモート ネットワークに入るためのユーザ名とパスワードを求めるように設定されている場合は、ユーザ名とパスワードの入力ダイアログが表示されます。ユーザ名とパスワードを入力します。

ユーザ名とパスワードを入力してリモート ネットワークに入るよう SonicWall VPN を設定すると、「**ユーザ名とパスワードを入力してください**」というダイアログが表示されます。



ユーザ名とパスワードを入力するには:

1 ユーザ名とパスワードを入力します。

2 ゲートウェイで許可されている場合は、「**ユーザ名とパスワードを記憶する**」を選択してユーザ名とパスワードを記憶すれば、後日 VPN コネクションに自動的にログインできます。

3 「OK」ボタンをクリックして VPN コネクション確立手順を続行します。

VPN コネクションへのショートカットの作成

ヒント: SonicWall グローバル VPN クライアントプログラムへのデスクトップ ショートカットを作成すると、すべてのコネクションに簡単にアクセスできるようになります。

VPN コネクションの有効化を簡単にするため、VPN コネクションのショートカットをデスクトップ、タスクバー、スタート メニューに置くことができます。また、ショートカットはシステム上の任意の場所に置くことができます。

ショートカットを作成するには:

1 グローバル VPN クライアントウィンドウにショートカットを作成する、コネクション名を選択します。

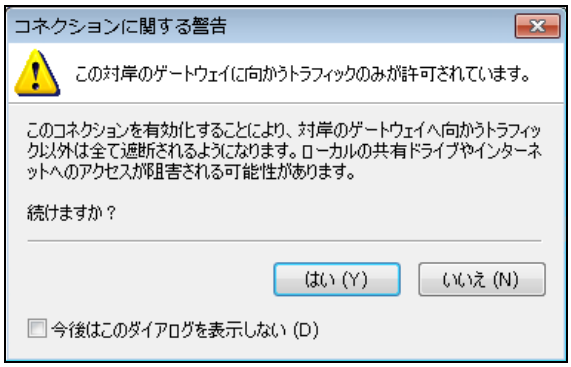
2 「**ファイル > ショートカット**」を選択します。

3 目的のショートカットのオプションを選択します。「**デスクトップ上**」、「**タスクバー上**」、「**スタート メニュー内**」、「**場所を選択**」から選択できます。

VPN コネクション名を右クリックし、「**ショートカットの作成 > *ショートカット オプション***」を選択するという方法もあります。

コネクションに関する警告

VPN コネクション ポリシーによってゲートウェイへのトラフィックのみが許可されている場合、「コネクションに関する警告」メッセージが表示され、VPN トンネルの対岸にあるリモート ネットワークに向けられたネットワーク トラフィックだけが許可されるという警告が表示されます。ローカルのネットワーク インターフェースおよびインターネットへのトラフィックはすべて遮断されます。



「**今後はこのダイアログを表示しない**」を選択すると、VPN コネクションを有効にするたびに「**コネクションに関する警告**」ダイアログが表示されることはなくなります。

「**はい**」ボタンをクリックして VPN コネクション確立手順を続行します。

5

VPN コネクション プロパティの設定

コネクション プロパティ ダイアログの表示

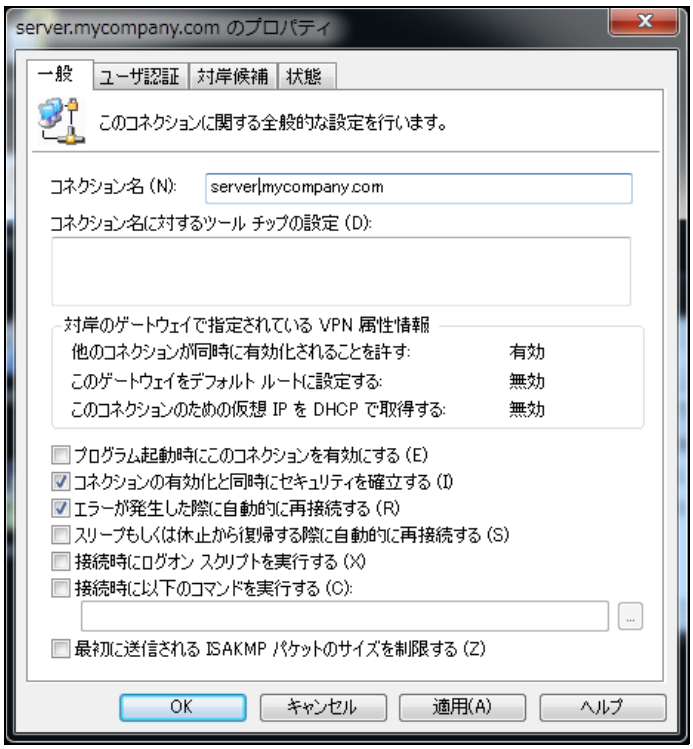
「**コネクション プロパティ**」ダイアログでは、個別の VPN コネクションを設定できます。「**コネクション プロパティ**」ダイアログを開くには、以下のいずれかの方法を選択します。

- コネクション名を選択して、「**ファイル > プロパティ**」を選択する。
- コネクション名を右クリックし、「**プロパティ**」を選択する。
- コネクション名を選択し、グローバル VPN クライアントウィンドウのツールバーにある「**プロパティ**」ボタンをクリックする。

「**コネクション プロパティ**」ダイアログには、「**一般**」タブ、「**ユーザ認証**」タブ、「**対岸候補**」タブ、「**状態**」タブがあります。

コネクション プロパティの一般設定

「**コネクション プロパティ**」ダイアログの「**一般**」タブには以下の設定があります。



- **コネクション名** - VPN コネクション名が表示されます。
- **コネクション名に対するツール チップの設定** - コネクションに関するポップアップ テキストが表示されます。テキストは、マウスでコネクション名をポイントすると表示されます。
- **対岸のゲートウェイで指定されているVPN属性情報** - VPN トラフィックの制御状態を表示します。これらの設定は SonicWall VPN ゲートウェイで管理されます。
    - **他のコネクションが同時に有効化されることを許す** - これが有効になっている場合、VPN コネクション有効時にコンピュータはローカルのネットワークまたはインターネットの接続にアクセスできます。
    - **このゲートウェイをデフォルトルートに設定する** - これが有効になっている場合、SonicWall VPN ゲートウェイを通過するようになっていないトラフィックがすべてブロックされます。この設定が有効な状態で VPN コネクションを有効にすると、「**コネクションに関する警告**」メッセージが表示されます。
    - **このコネクションのための仮想 IP を DHCP で取得する** - VPN クライアントがゲートウェイから VPN トンネルを通じて DHCP によって IP アドレスを取得できるようにします。
- **プログラム起動時にこのコネクションを有効にする** - SonicWall グローバル VPN クライアント起動時に、この VPN コネクションをデフォルトとして確立します。
- **コネクションの有効化と同時にセキュリティを確立する** - IKE のフェーズ 1 のネゴシエーションを、ネットワークトラフィックの伝送開始を待たずに、コネクションが有効になるとすぐに開始します。この設定はデフォルトで有効になっています。
- **エラーが発生した際に自動的に再接続する** - この機能を有効にすると、対岸のゲートウェイとの接続に問題が発生した場合にグローバル VPN クライアントは再接続を試み続けます。この機能により、グローバル VPN クライアントは一時的に使用できなくなった VPN コネクションをユーザの介入なしに再開できます。

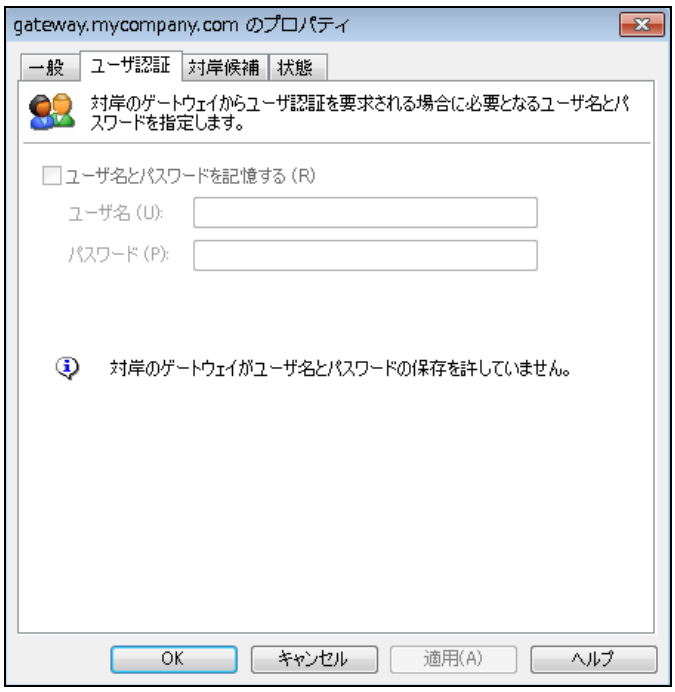
接続のエラーが間違った設定 (DNS や対岸のゲートウェイの IP アドレスの設定など) によるものの場合は、手動で修正する必要があります。ログビューアを確認して問題を特定してから、コネクションを編集してください。

このオプションは既定で有効です。このオプションが無効の場合、接続の試行時にエラーが発生すると、グローバル VPN クライアントはエラーをログに記録して、エラーメッセージのダイアログを表示し、接続の試行を中止します。

- **スリープもしくは休止から復帰する際に自動的に再接続する** - コンピュータがスリープ状態やハイバネーション状態から復帰すると自動的に VPN コネクションが有効になります。この設定はデフォルトで無効になっています。
- **接続時にログオン スクリプトを実行する** - SonicWall VPN ゲートウェイにログインして安全なトンネルを確立したら、ログオン スクリプト内に設定されたアクションを実行します。
- **接続時に以下のコマンドを実行する** - VPN コネクションが正常に確立されると、プログラムはオプションの引数とともに自動で実行できるようになります。
- **最初に送信される ISAKMP パケットのサイズを制限する** - このオプションは、グローバル VPN クライアントが接続試行時に「The peer is not responding to phase 1 ISAKMP requests」などのエラーを受信する場合に使用できます。このエラーは、ISAKMP パケットがサイズを理由に断片化されているが、ネットワーク機器 (ルータ) は VPN コネクションの確率時に断片化されたパケットを許可しない場合に生じる可能性があります。

コネクション プロパティのユーザ認証の設定

「**ユーザ認証**」タブでは、ゲートウェイによってユーザ認証が求められた場合に必要となるユーザ名とパスワードを指定します。SonicWall VPN ゲートウェイがユーザ名とパスワードの保存 (キャッシュ) をサポートしていない場合は、このタブの設定は無効になっており、ページ下部に「**対岸のゲートウェイがユーザ名とパスワードの保存を許していません**」というメッセージが表示されます。

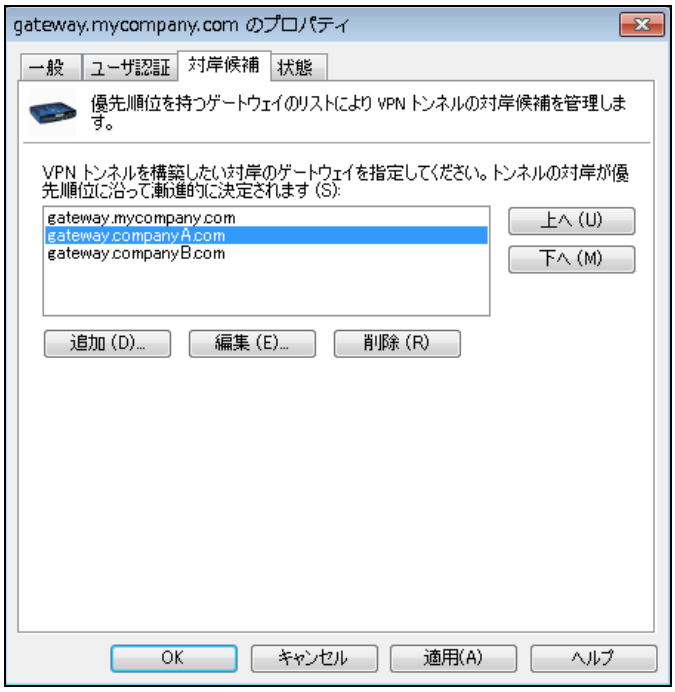


- **ユーザ名とパスワードを記憶する** - SonicWall VPN ゲートウェイに接続するためのユーザ名とパスワードの保存を有効にします。

- **ユーザ名** - ゲートウェイ管理者から指定されたユーザ名を入力します。
- **パスワード** - ゲートウェイ管理者から指定されたパスワードを入力します。

コネクション プロパティの対岸候補の設定

「**対岸候補**」タブでは、コネクションが VPN トンネル構築の相手として使用できる VPN ゲートウェイを指定できます (エントリが複数ある場合は、複数の VPN ゲートウェイを通じて VPN コネクションが確立できます)。対岸のゲートウェイ群に対する VPN トンネル構築の試行は、リストに表示された順に行われます。



対岸候補を追加するには:

1 「**追加**」を選択します。

2 「**対岸候補の属性**」ダイアログの「IP **アドレスまたは DNS 名**」フィールドに **IP アドレス**または DNS 名を入力します。

3 「**OK**」を選択します。

対岸候補のエントリを編集するには:

1 対岸候補名を選択します。

2 「**編集**」を選択します。

3 「**対岸候補の属性**」ダイアログで必要に応じて修正を加えます。「対岸候補の属性」ダイアログ (35 ページ)を参照してください。

4 「**OK**」を選択します。

対岸候補のリストの順番を変更するには:

1 対岸候補名を選択します。

2 「**上へ**」または「**下へ**」をクリックします。

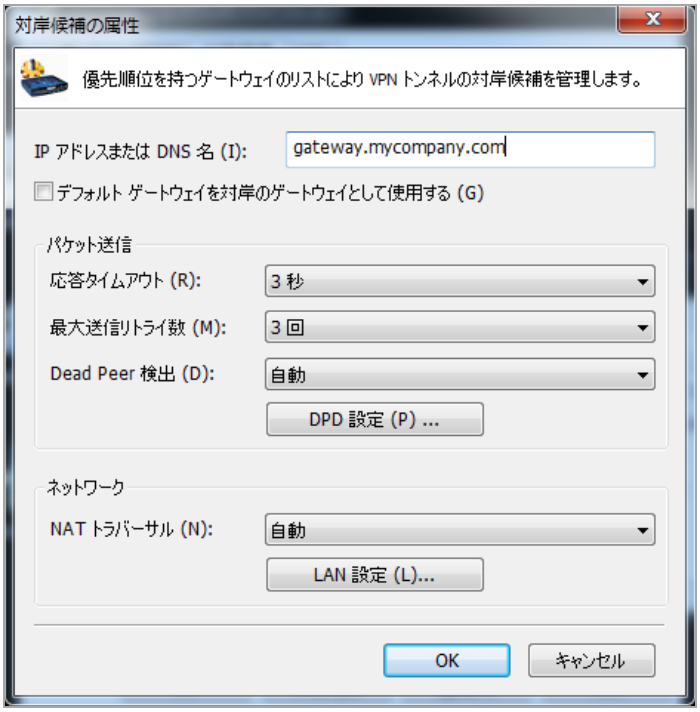
対岸候補のエントリを削除するには:

1 対岸候補のエントリを選択します。

2 「**削除**」を選択します。

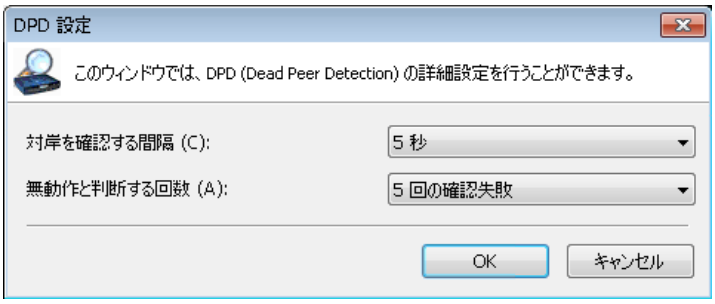
「対岸候補の属性」ダイアログ

「**対岸候補の属性**」ダイアログでは、対岸のゲートウェイ情報の追加や編集ができます。

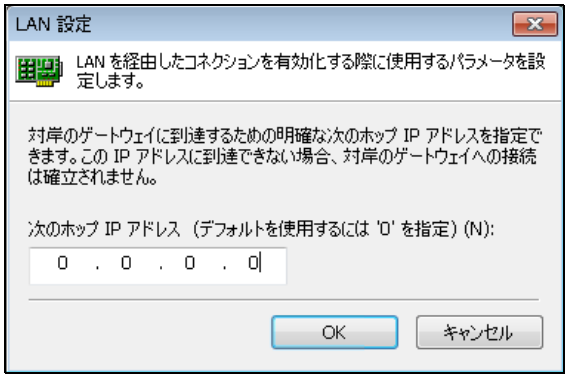


- **IP アドレスまたは DNS 名** - 対岸のVPNゲートウェイの IP アドレスまたは DNS 名を指定します。
- **デフォルト ゲートウェイを対岸のゲートウェイとして使用する** - デフォルト ゲートウェイを対岸のゲートウェイとして使用します。この機能を有効にすると、IP アドレスまたは DNS 名フィールドは入力できなくなります。グローバル VPN クライアントは、ルーティング テーブルからデフォルトのゲートウェイを取得します。
- **応答タイムアウト** - 送信したパケットへのレスポンスの最大待ち時間を指定します。この待ち時間が経過すると、送信したパケットは消失したと見なされ、同じパケットが再送信されます。有効範囲は 1 秒から 10 秒までです。

- **最大送信リトライ数** - 対岸候補が応答していないことを確認する前に、同じパケットを最大何回送信するかを指定します。有効範囲は 1 回から 10 回までです。
- **Dead Peer 検出** (DPD) - 以下のいずれかを選択します。
  - **自動** - トラフィックをベースとした DPD です。グローバル VPN クライアントがレスポンス データを受信しない場合 (一方通行)、グローバル VPN クライアントはハートビート パケットを交換して対岸のゲートウェイが作動しているか検出します。**DPD 設定** で指定した回数のチェックに失敗したことを知らせるハートビート パケットのレスポンスがない場合、グローバル VPN クライアントは IKE ネゴシエーションの再実行を試みます。この設定はデフォルトで有効になっています。
  - **強制使用** - DPD を定期的に実行します。グローバル VPN クライアントは、対岸のゲートウェイが作動しているかどうか検出するために ハートビート パケットを交換します。**DPD 設定** で指定した回数のチェックに失敗したことを知らせるハートビート パケットのレスポンスがない場合、グローバル VPN クライアントは IKE ネゴシエーションの再実行を試みます。
  - **無効** - DPD が無効化されます。ハートビート パケットは交換されません。これにより、グローバル VPN クライアントはゲートウェイが使用できない場合の検出を行わなくなります。
- **DPD 設定** - **DPD** 設定ダイアログを表示します。



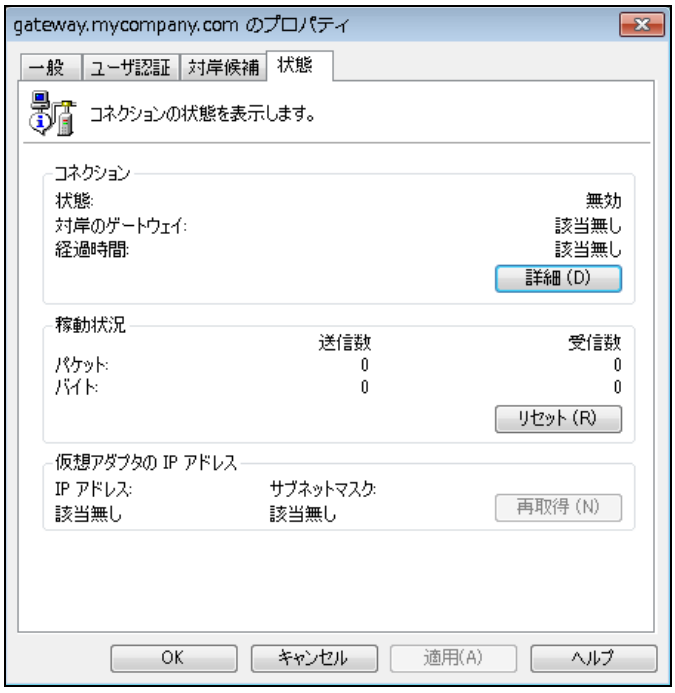
  - **対岸を確認する間隔** - 3、5、10、15、20、25、30 秒 から選択します。
  - **無動作と判断する回数** - 失敗を確認する回数を 3、4、5 回 から選択します。
- **NAT トラバーサル** - 下記の 3 つから選択します。
  - **自動** - 対岸候補間で IPsec パケットの UDP カプセル化を使用するかどうかを自動的に決定します。
  - **強制使用** - NAPT/NAT 装置が対岸との間に存在するかどうかにかかわらず、IPsec パケットの UDP カプセル化を有効にします。
  - **無効** - 対岸との間の IPsec パケットの UDP カプセル化を無効にします。
- **LAN 設定** - LAN を経由したコネクションを有効化する際に使用するパラメータを設定するための、**LAN 設定**ダイアログを表示します。



「**次のホップ IP アドレス**」フィールドに、デフォルト ルートの代わりに使用する次のホップ IP アドレスを入力します。0 のままにすると、グローバル VPN クライアントはデフォルト ルートを使用します。

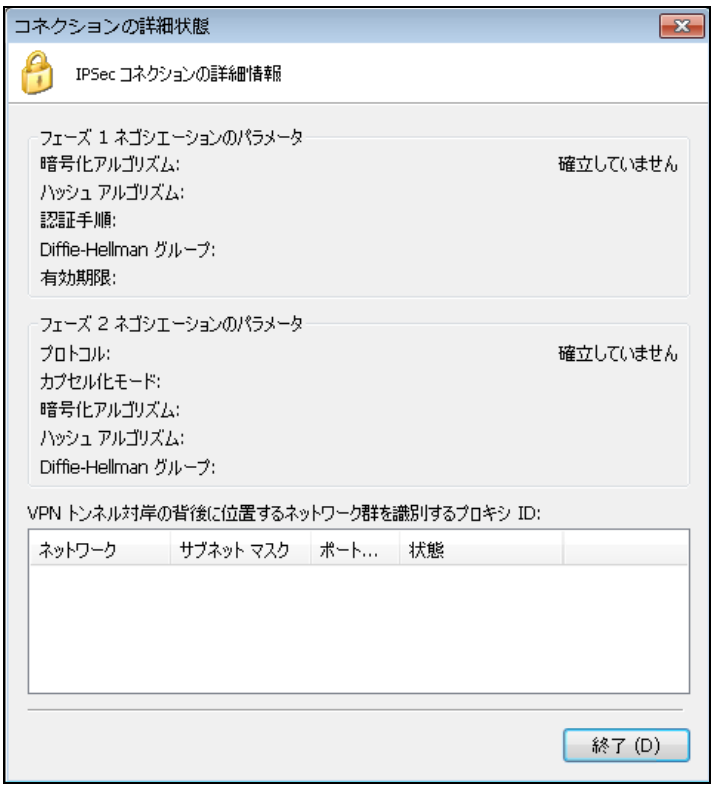
コネクション プロパティの状態の設定

「**状態**」タブには、コネクションの現在の状態が表示されます。



- **コネクション**:
  - **状態** - VPN コネクションが有効であるか無効であるかが示されます。
  - **対岸のゲートウェイ** - 対岸のゲートウェイの IP アドレスが表示されます。
  - **経過時間** - 接続時間が表示されます。

- **詳細** - **コネクションの詳細状態**ダイアログが表示され、ネゴシエートされたフェーズ 1 とフェーズ 2 のパラメータおよびフェーズ 2 のセキュリティ アソシエーション (SA) の状態が示されます。



- **稼動状況**:
  - **パケット** - VPN トンネルを通じて送受信されたパケット数が表示されます。
  - **バイト** - VPN トンネルを通じて送受信されたバイト数が表示されます。
  - **リセット** - パケットおよびバイトの値をゼロにリセットします。これらのカウントはただちに再開されます。
- **仮想アダプタの IP アドレス**:
  - **IPアドレス** - VPN ゲートウェイから VPN トンネルを通じて DHCP によって割り当てられた IP アドレスです。
  - **サブネット マスク** - 仮想 IP アドレスのサブネット マスクです。
  - **再取得** - DHCP リースを更新します。

6

VPN コネクションの管理

VPN コネクションについて

SonicWall グローバル VPN クライアントでは、VPN コネクションを必要なだけ設定することができます。このセクションでは、グローバル VPN クライアントが提供するコネクション管理に役立つツールについて説明します。

コネクションの並べ替え

グローバル VPN クライアントウィンドウ内のコネクションの数が増えてくると、コネクション名を並べ替えた方がアクセスしやすくなります。**グローバル VPN クライアント**ウィンドウ内のコネクション名は、「**表示 > ソート**」を選択すると並べ替えられます。

- **名前** - コネクション名の順にコネクションをソートします。
- **対岸のゲートウェイ** - 対岸候補名の順にコネクションをソートします。
- **状態** - 状態別にコネクションをソートします。
- **昇順** - 有効化されている場合は A-Z のように昇順で、無効化されている場合は Z-A のように降順でコネクションをソートします。デフォルトでは、「**名前**」の「**昇順**」でソートします。

コネクション名の変更

コネクション名を変更するには、コネクション名を選択して「**ファイル > 名前の変更**」を選び、新しい名前を入力します。コネクション名を右クリックして、表示されるメニューから「名前の変更」を選択することによって名前を変更することもできます。

コネクションの削除

重要: 有効になっているコネクションを削除することはできません。コネクションを先ず無効にしてから削除します。

コネクションを削除するには、次のいずれかの操作を行います。

- コネクション名を選択して、**Delete** キーを押します。
- 「**ファイル > 削除**」を選択します。
- コネクション名を右クリックして、「**削除**」を選択します。

すべてのコネクションの選択

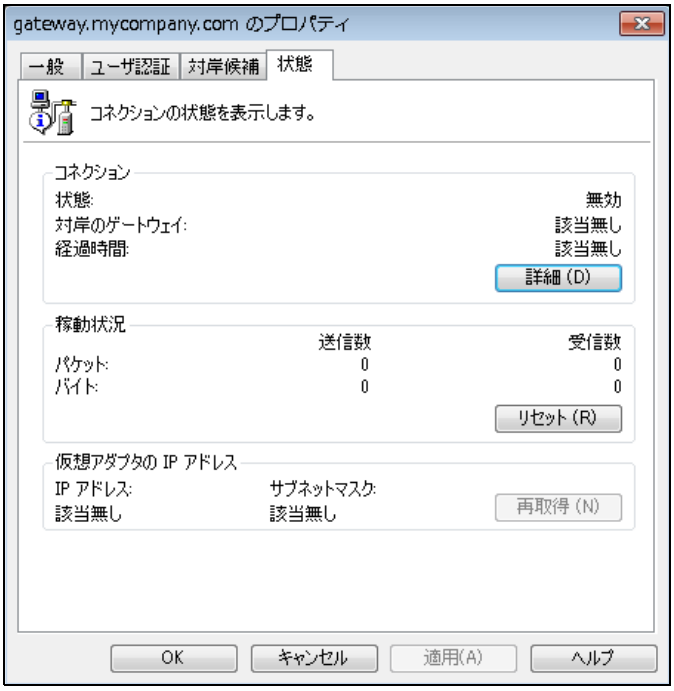
グローバル VPN クライアントウィンドウのすべてのコネクションを選択するには、「**表示 > すべてを選択**」を選択するか、**Ctrl+A** を押します。

VPN コネクションの状態のチェック

SonicWall グローバル VPN クライアントには、VPN コネクションの状態を示すさまざまなインジケータが含まれています。メインの**グローバル VPN クライアント**ウィンドウには、VPN コネクションと、それらの各状態が**無効**、**有効**、**接続**、**エラー**のいずれかで示されます。

- 接続されているコネクションは、**ポリシー** アイコンに緑のチェックマークが付きます。
- フェーズ 2 の SA (セキュリティ アソシエーション) のいずれかが失敗したコネクションは、**ポリシー** アイコンに黄色の警告マークが付きます。
- 正常に接続できない VPN ポリシーに対しては、**ポリシー** アイコンにエラー マーク (赤い X) が付きます。
- システム トレーの**グローバル VPN クライアント**アイコンは、グローバル VPN クライアントとゲートウェイの間を通過するデータに関する視覚的なインジケータを表示します。
- 「**プロパティ**」ダイアログの「**状態**」タブには、有効な VPN コネクションの状態に関する詳細情報が表示されます。特定の VPN コネクションの「**状態**」タブを表示するには以下のいずれかの方法があります。
    - 有効になっている VPN コネクション名をダブルクリックする。
    - コネクション名を選択して、**Ctrl+T** を押す。
    - コネクション名を選択して、ツールバーの「**状態**」ボタンをクリックする。

- **グローバル VPN クライアント**ウィンドウのコネクション名を右クリックして、「**状態**」を選択する。



ヒント:「状態」タブの詳細については、コネクション プロパティの状態の設定 (37 ページ)を参照してください。

VPN コネクションの無効化

VPN コネクションを無効にすると、VPN トンネルが終了します。VPN コネクションを無効にするには以下のいずれかの方法があります。

- **グローバル VPN クライアント**ウィンドウのコネクション名を右クリックして、「**無効化**」を選択する。
- システム トレーの**グローバル VPN クライアント**アイコンを右クリックし、「**無効化 > *コネクション名***」を選択する。
- コネクション名を選択して、**Ctrl+B** を押す。
- コネクション名を選択して、**グローバル VPN クライアント**ウィンドウのツールバーにある「**無効化**」ボタンをクリックする。

7

証明書の使用

証明書の情報の取得

VPN コネクションポリシーの一部として デジタル証明書が必要な場合は、証明書のインポートに必要な情報をゲートウェイ管理者から取得する必要があります。次に、証明書マネージャを使用してグローバル VPN クライアントに証明書をインポートしなければなりません。

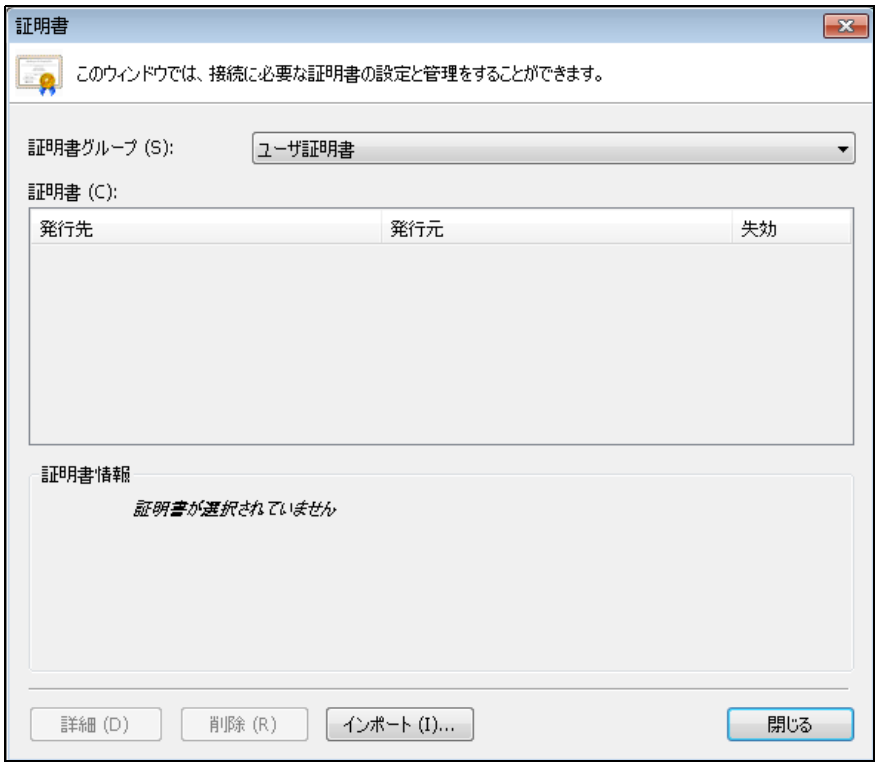
注意: VPN コネクションポリシーの一部としてデジタル証明書が必要な場合は、証明書をゲートウェイ管理者から取得する必要があります。

証明書の管理

証明書マネージャにより、SonicWall グローバル VPN クライアントが VPN コネクションで使用するデジタル証明書を管理できます。VPN ゲートウェイがデジタル証明書を使用している場合には、「**証明書マネージャ**」を使用して CA とローカル証明書をインポートする必要があります。

証明書を管理するために証明書マネージャを開くには:

1 「**表示**」メニューをクリックします。



2 **グローバル VPN クライアント**ウィンドウの「**証明書**」を選択します。

3 「**証明書グループ**」ドロップダウン メニューで証明書の種類を選択します。以下の種類があります。

- **ユーザ** – VPN SA を確立するために使用されるローカル デジタル証明書です。
- **CA** – ユーザ証明書を確認するためのデジタル証明書です。
- **信頼されるルート CA** – CA 証明書を確認するために使用されます。

4 リストから証明書を選択したら、次のいずれかの操作を行います。

- 「**証明書**」ウィンドウの「**インポート**」ボタンをクリックして「**証明書のインポート**」ウィンドウを表示し、証明書ファイルをインポートします。
- 「**削除**」ボタンをクリックして、選択した証明書を削除します。
- 「**詳細**」ボタンをクリックして、選択した証明書の詳細を表示します。

ヒント: SonicWall 装置での VPN の証明書の使用に関する詳細は、『SonicOS 管理ガイド』を参照してください。

8

グローバル VPN クライアントのトラブルシューティング

トラブルシューティングの手段

SonicWall グローバル VPN クライアントには、VPN コネクションのトラブルシューティングを行うための手段があります。

- ログ ビューア – グローバル VPN クライアントのログについて (44 ページ)
- ヘルプ レポート – ログの設定 (47 ページ)
- SonicWall のサポート サイト – SonicWall グローバル VPN クライアントテクニカル サポートへのアクセス (50 ページ)
- SonicWall グローバル VPN クライアントのヘルプ システム – SonicWall グローバル VPN クライアントテクニカル サポートへのアクセス (50 ページ)
- グローバル VPN クライアントのアンインストール – グローバル VPN クライアントのアンインストール (50 ページ)

グローバル VPN クライアントのログについて

グローバル VPN クライアントウィンドウには、グローバル VPN クライアントのアクティビティに関するメッセージが表示されます。メッセージの保存と管理が可能です。

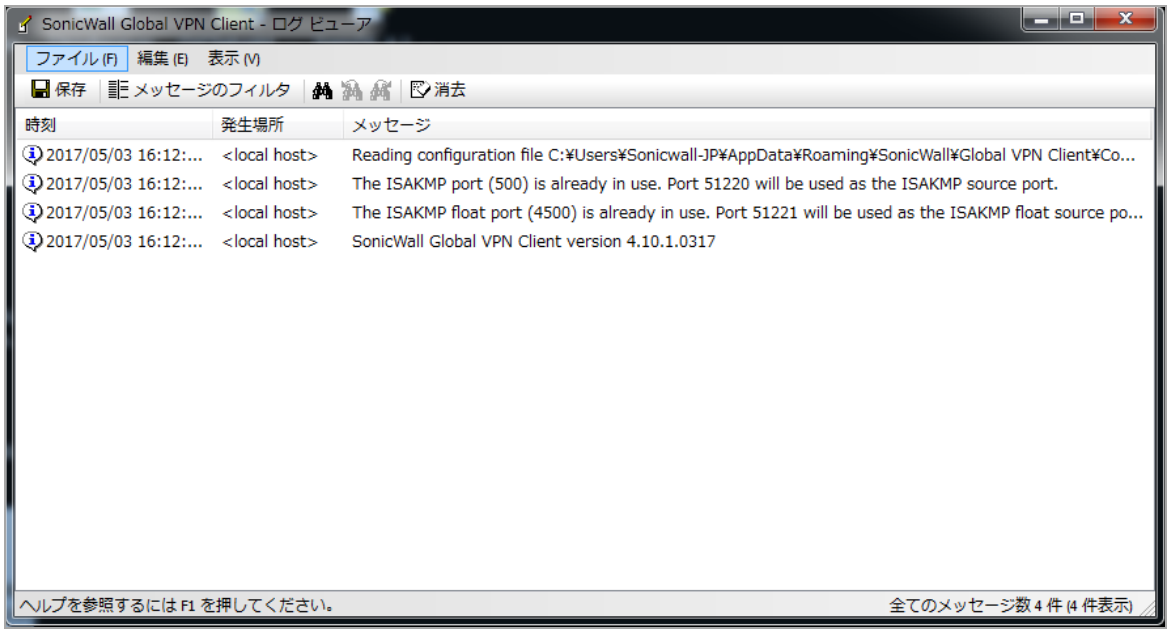
トピック:

ログ ビューア ウィンドウの表示

ログ ビューア ウィンドウを表示するには:

1 以下のいずれかを実行します。

- **グローバル VPN クライアント**ウィンドウのツールバーにある「**ログの表示**」ボタンをクリックします。
- 「**表示 > ログ ビューア**」を選択します。
- **Ctrl+L** を押します。



ログ ビューア ウィンドウに以下の情報が表示されます。

- **種別** - メッセージの種類を示すアイコンです。
  - **情報** -
  - **警告** -
  - **エラー** -
- **時刻** - メッセージが生成された日付および時刻。
- **発生場所** - 対岸候補の IP アドレスまたは FQDN。
- **メッセージ** - イベントを説明するメッセージのテキスト。

現在のログの保存

「**保存**」ボタンをクリックして、現在のログを .txt ファイルに保存します。現在のログをファイルに保存する際に、グローバル VPN クライアントは、**ヘルプ レポート**を自動的に付け加えます。これには、SonicWall グローバル VPN クライアントの状態やそれを実行しているシステムに関する、トラブルシューティングに有益な情報が含まれています。**ヘルプ レポート**の情報は、ログ ファイルの初めに挿入されます。詳細については、ヘルプ レポートの作成 (48 ページ)を参照してください。

ヒント: ログ ビューア メッセージの詳細なリストは、「ログ ビューア メッセージ (65 ページ)」を参照してください。

ログ メッセージの管理

ログビューアは、ログ メッセージを管理するために次の機能を提供します。

- 現在のログを .txt ファイルとして保存するには、ツールバーの「保存」ボタンをクリックするか、**Ctrl+S** を押すか、「**ファイル > 保存**」を選択します。現在のログをファイルに保存する際に、グローバル VPN クライアントは、ヘルプ レポートを自動的に付け加えます。これには、SonicWall グローバル VPN クライアントの状態やそれを実行しているシステムに関する有益な情報が含まれています。
- すべてのメッセージを選択するには、**Ctrl+A** を押すか、「**編集 > すべて選択**」を選択します。
- ログの内容をコピーして他のアプリケーションにペーストするには、コピーするメッセージを選択し、**Ctrl+C** を押すか、「**編集 > コピー**」を選択します。
- あまり詳細でない情報をログ ビューアに表示するには、ツールバーの「メッセージのフィルタ」ボタンをクリックして「**表示 > メッセージのフィルタ**」を選択します。
- ログ メッセージから文字列を検索するには、次のいずれかの操作を行います。
  - ツールバーの「**検索**」アイコン をクリックします。
  - 「**編集 > 検索**」を選択し、「**検索**」ダイアログに文字列を入力します。

    ダイアログ内では、「**単語全体にのみマッチ**」、「**大文字と小文字を区別してマッチ**」、「**アップ**」、「**ダウン**」を検索方法として選択できます。
  - 「次を検索」アイコンをクリックして検索します。「**検索**」ダイアログに文字列を入力した後で、X をクリックしてダイアログを閉じても、ツールバーの「**次を検索**」アイコンと「**前を検索**」アイコンを使用できます。
- 現在のログ情報をクリアするには、次のいずれかの操作を行います。
  - ツールバーの「クリア」をクリックします。
  - Crtl+X を押します。
  - 「編集 > クリア」を選択します。
- ログ ビューア ウィンドウのツールバーを表示または非表示するには、「表示 > ツールバー」を選択してツールバーのオンとオフを切り替えます。
- ログ ビューア ウィンドウのステータスバーを表示または非表示するには、「表示 > ステータスバー」を選択してステータスバーのオンとオフを切り替えます。

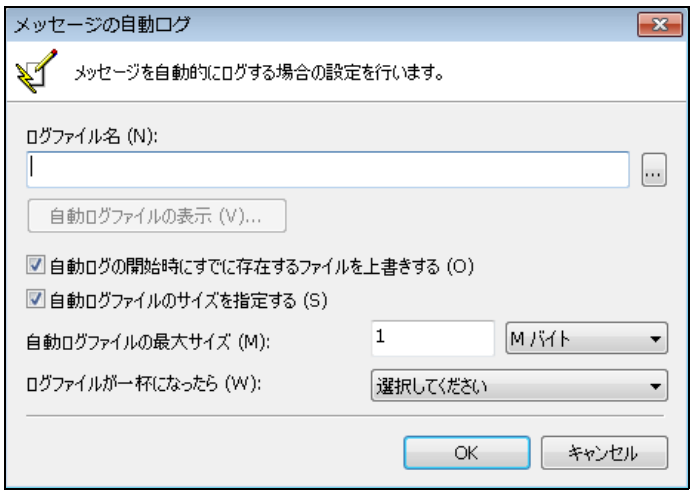
ログの設定

「**表示 > オプション**」ダイアログの「**ログ**」タブでは、グローバル VPN クライアントのログの動作を設定します。

- **保有するログ メッセージの最大数** - ログ ファイルに保存されているログ メッセージの最大数を指定します。
- **ISAKMP ヘッダー情報をログする** - ISAKMP ベッダ情報のログ機能を有効にします。
- **DPD パケットをログする** - DPD パケットのログ機能を有効にします。
- **NAT keep-aliveパケットをログする** - NAT キープアライブ パケットのログ機能を有効にします。
- **自動ログを有効にする** -「**自動ログ**」ウィンドウで指定されるとおりに、ファイルへのメッセージの自動ログを有効化します。
- **設定** -「**自動ログ**」ダイアログを表示します。詳細については、「自動ログの設定 (47 ページ)」を参照してください。

自動ログの設定

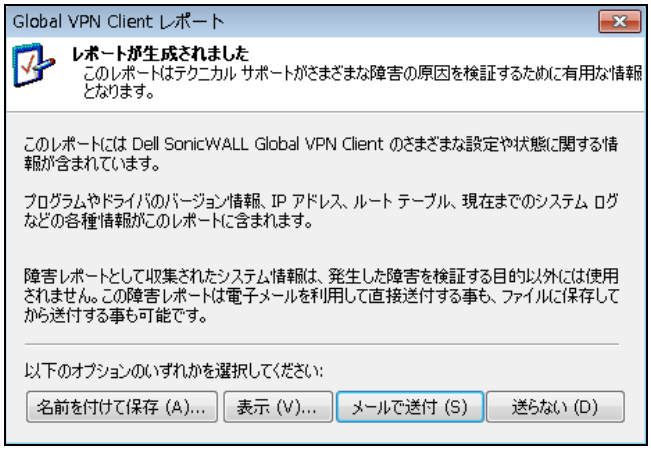
「**設定**」をクリックすると、「**自動ログ**」ダイアログが表示され、メッセージをファイルに記録する自動ログの設定を行うことができます。ログ ファイルは、テキスト ファイル (`.txt`) として保存されます。



- **ログ ファイル名** - ログ メッセージを保存するファイルを指定します。「参照」ボタンをクリックすると、自動ログ ファイルの場所を指定できます。ファイル名のみを指定する (ファイル名にパスを指定しない) 場合、ログ ファイルは TEMP ディレクトリに作成されます。
- **自動ログ ファイルの表示** - ログ ファイルを最大 71,000行まで参照できます。
- **自動ログの開始時にすでに存在するファイルを上書きする** - 自動ログの開始時に既存の自動ログ ファイルファイルを上書きします。
- **自動ログ ファイルのサイズを指定する** - ログ ファイルの最大サイズを制限します。
- **自動ログ ファイルの最大サイズ** - 最大ファイル サイズを KB または MB で指定します。
- **ログファイルが一杯になったら** - 自動ログ ファイルが最大サイズに達したときの動作を指定します。
    - **ユーザに確認する** - 最大ファイル サイズに達した時点で、「**自動ログを停止する**」「**自動ログ ファイルを上書きする**」のどちらにするかをユーザに確認します。
    - **自動ログを停止する** - 最大ファイル サイズに達すると、自動ログが停止します。
    - **ログ データを上書きする** - 最大ファイル サイズに達すると、自動ログ ファイルが上書きされます。

ヘルプ レポートの作成

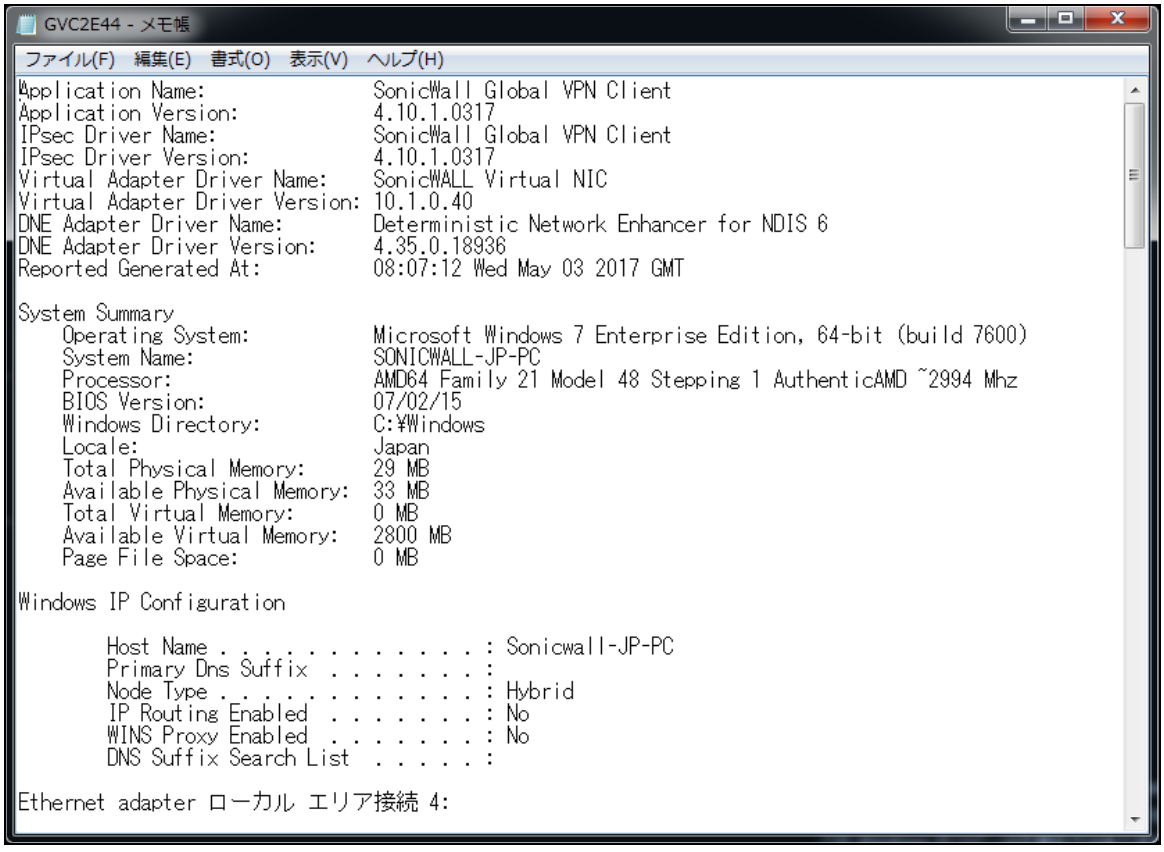
グローバル VPN クライアントウィンドウの「**ヘルプ > レポートの作成**」を選択すると、「**グローバル VPN クライアントレポート**」ダイアログが表示されます。



「**レポートの作成**」により、グローバル VPN クライアントの使用中に問題が発生した場合の対応に役立つ情報を準備することができます。レポートには、SonicWall グローバル VPN クライアントの状態やそれを実行しているシステムに関する情報も含まれます。

- バージョン情報
- ドライバ
- システム情報
- IP アドレス
- ルート テーブル
- 現在のログ メッセージ

デフォルトのテキスト エディタ ウィンドウでレポートを参照するには、「**表示**」をクリックします。



- レポートをテキスト ファイルとして保存するには、「名前を付けて保存」をクリックします。
- レポートを電子メールで送信するには、「メールで送付」をクリックします。
- 何も操作を実行せずにダイアログを閉じるには、「送らない」をクリックします。

SonicWall グローバル VPN クライアントテクニカル サポートへのアクセス

SonicWall は、包括的なサポート サービスでネットワーク セキュリティ製品を保護し、柔軟なサポートを提供します。SonicWall グローバル VPN クライアントのサポートは、SonicWall ネットワーク セキュリティ装置のサポート プログラムの一部として含まれています。

- 「**ヘルプ > テクニカル サポート**」を選択すると、SonicWall サポート サイトにアクセスできます。

  https://support.sonicwall.com/ja-jp/

- SonicWall サポート サイトでは、広範にわたるオンライン リソースや SonicWall の強化サポート プログラムなど、さまざまなサポート サービスに関する情報を提供しています。SonicWall サポート サービスは、ご利用の MySonicWall アカウントから以下のサイトにて購入 / アクティブ化できます。

  http://www.mysonicwall.com

ヘルプ トピックの表示

「**ヘルプ > ヘルプ トピック**」を選択すると、SonicWall グローバル VPN クライアントのヘルプ ウィンドウが表示されます。以下のオプションを利用することで、ヘルプ トピックを検索することができます。

- **目次** - 目次ビューの表を用いてヘルプを表示します。
- **インデックス** - トピックをアルファベット順に並べてヘルプを表示します。
- **検索** - キーワードを用いて検索することができます。

グローバル VPN クライアントのアンインストール

SonicWall グローバル VPN クライアントのアンインストールは簡単です。 既存の VPN コネクションを保存するか、アンインストールと同時に削除するかを選択できます。

補足: プログラムをアンインストールする前に SonicWall グローバル VPN クライアントを終了する必要があります。

SonicWall グローバル VPN クライアントをアンインストールするには:

1 Windows コントロールパネルを開きます。

2 「**プログラムと機能**」をダブルクリックします。

3 「グローバル VPN クライアント」 を選択します。

4 「**削除**」を選択します。

5 「**ファイル削除の確認**」ダイアログで、「**はい**」または「**OK**」をクリックし、SonicWall グローバル VPN クライアントの削除を確認します。

6 必要に応じて、次の操作を行います。

- 既存の VPN コネクションをすべて削除するには、「**すべての個人ユーザ設定情報を削除する**」を選択します。これを選択しない場合、VPN コネクションは保存され、後に SonicWall グローバル VPN クライアントをインストールした時に再度表示されます。
- 次回グローバル VPN クライアントをインストールした時に現在の SonicWall VPN アダプタの MAC アドレスを使用する場合は、「**MAC アドレスを保存**」を選択します。

7 「**次へ**」を選択します。

8 グローバル VPN クライアントを削除した後、再起動を求める表示に従ってコンピュータを再起動します。

9

グローバル VPN クライアントに対する SonicWall 装置の設定

GroupVPN ポリシーについて

SonicOS GroupVPN ポリシーを使えば、SonicWall セキュリティ装置からSonicWall グローバル VPN クライアントを自動的にプロビジョニングすることができます。GroupVPN ポリシーは、SonicWall グローバル VPN クライアントでのみ利用可能です。SonicOS GroupVPN では、次の 2 つの IPsec キーイングモードがサポートされています。

- **IKE (共有鍵を使用)**
- **IKE (サード パーティ証明書を使用)**

GroupVPN ポリシーを作成すると、ポリシーをダウンロードして SonicWall グローバル VPN クライアントを自動的にプロビジョニングするように設定するか、手動インストール用にポリシー ファイルを SonicWall グローバル VPN クライアントにエクスポートすることができます。

補足: SonicWall グローバル VPN クライアントをサポートするための SonicWall 上の GroupVPN の設定については、『SonicOS 管理ガイド』を参照してください。SonicWall 製品のドキュメントはすべて以下のサイトの「サポート」のページで提供されています。

https://support.sonicwall.com/ja-jp/

グローバル VPN クライアントのライセンス

グローバル VPN クライアントのライセンスは、SonicWall 装置に対するグローバル VPN クライアントの同時接続数に基づきます。グローバル VPN クライアントの同時接続数の上限に達した場合、SonicOS は、グローバル VPN クライアントの接続をそれ以上追加することを拒否します。グローバル VPN クライアントの同時接続数が上限を下回った時点で、新規のグローバル VPN クライアント接続を確立できます。

各プラットフォームでサポートされるグループ VPN 接続数

SonicWall の各装置モデルで、サポートされるグローバル VPN クライアントのライセンス数は異なります。グローバル VPN クライアント ソフトウェアおよびグローバル VPN クライアントライセンスは、再販業者から購入するか、または mysonicwall.com においてオンラインで購入することができます。

グローバル VPN クライアントの有効化

SonicWall グローバル VPN クライアントソフトウェアを有効化してダウンロードするためには、有効な MySonicWall アカウントを所有していることと、SonicWall 装置をアカウントに登録しておくことが必要です。MySonicWall のアカウントがない、もしくは、装置をアカウントに登録していない場合には、次のサイトでアカウントを作成して登録してください。http://www.mysonicwall.com

グローバル VPN クライアントのライセンスを有効化するには:

1 MySonicWall アカウントにログインします。

2 登録されている SonicWall ネットワーク セキュリティ装置を選択します。

3 「**使用可能なサービス**」メニューから「**グローバル VPN クライアント**」を選択します。

4 「**有効化**」を選択します。

5 「**アクティベーション キー**」フィールドにアクティベーション キーを入力します。

6 「**適用**」を選択します。

正常に起動すると、確認メッセージが表示されます。

ヒント: 後日参照できるよう、SonicWall 装置のシリアル ナンバーを記録しておきます。ライセンスのアクティベーションは、これで完了です。

グローバル VPN クライアントのソフトウェアおよびドキュメントのダウンロード

1 ウェブ ブラウザで、MySonicWall アカウントにログインします。

2 「製品管理」ページで、グローバル VPN クライアントのライセンスを有効化した SonicWall 装置の名前を選択します。

3 「**ソフトウェア ダウンロード**」を選択します。このサービスが有効化されていない場合には、「**同意する**」を選択して有効化します。

4 SonicWall グローバル VPN クライアントのソフトウェアおよびドキュメントをダウンロードします。

A

default.rcf ファイルの使用

default.rcf ファイルについて

default.rcf ファイルでは、SonicWall グローバル VPN クライアント用に事前設定した VPN コネクションを作成して配布できます。グローバル VPN クライアントソフトウェアとともに **default.rcf** ファイルを配布することにより、事前設定済みの VPN コネクションを自動的に作成して、展開を簡素化することができます。

default.rcf ファイルから作成された VPN コネクションは、グローバル VPN クライアントウィンドウに表示されます。グローバル VPN クライアントユーザは、単に VPN コネクションを有効化するだけで、ユーザ名とパスワードによる XAUTH 認証後、ポリシーのダウンロードが自動的に完了します。

default.rcf ファイル使用時のグローバル VPN クライアントの動作

グローバル VPN クライアントは起動時に、`C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\` ディレクトリで設定ファイル **Connections.rcf** を必ず検索します。このファイルが存在しない場合は、グローバル VPN クライアントのインストール ディレクトリである `C:\Program Files\SonicWall\グローバル VPN クライアント\` で **default.rcf** ファイルを検索します。

グローバル VPN クライアントは、**default.rcf** ファイルが存在する場合はこれを読み込み、設定ファイル **Connections.rcf** を `C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\` ディレクトリに作成します。**Connections.rcf** ファイルには、暗号化された機密データ (ユーザ名およびパスワード) とともに、SonicWall グローバル VPN クライアントの VPN コネクション設定情報がすべて含まれています。

default.rcf ファイルの展開

default.rcf ファイルを SonicWall グローバル VPN クライアントにインストールするには、以下の 3 つの方法があります。

- インストーラを実行する前に、**default.rcf** ファイルをインストーラ ソフトウェア **GVCInstall*XX*.MSI** に追加します。***XX*** の部分は、32 ビット Windows プラットフォームの場合は **32**、64 ビット Windows プラットフォームの場合は **64** です。default.rcf ファイルを MSI インストーラに追加する (55 ページ)を参照してください。
- SonicWall グローバル VPN クライアントアプリケーションを初めて開く前に、**default.rcf** ファイルをプログラム インストール ディレクトリに追加します。default.rcf ファイルを インストール ディレクトリに追加する (56 ページ)を参照してください。
- **Connections.rcf** 設定ファイルがユーザの設定ファイル フォルダ内に存在している場合には、プログラム インストール ディレクトリにある **default.rcf** の設定を使用して Connections.rcf 設定ファイルを置き換えます。既存の .rcf ファイル を default.rcf ファイルで置き換える (56 ページ)を参照してください。

default.rcf ファイルを MSI インストーラに追加する

default.rcf ファイルを作成したら、インストーラを実行する前に、MSI インストーラと同じフォルダに追加します (この MSI インストーラは **GVCInstall*XX*.MSI** です。***XX*** の個所は、32 ビット Windows プラットフォームの場合は **32**、64 ビット Windows プラットフォームの場合は **64** です)。 これで、インストール プロセスにおいて **default.rcf** がプログラム インストール ディレクトリにコピーされます。このインストールの後、グローバル VPN クライアントプログラムを起動すると、**default.rcf** で定義されるコネクションを使用して、設定ファイル **Connections.rcf** が`C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\` ディレクトリに作成されます。これが、グローバル VPN クライアントを使用するユーザにとって最も簡単な方法です。

インストール中に同じプロファイルを (default.rcf から) すべてのユーザに対して取得するには:

1. 複数のコネクションを確立する場合は、SonicWall ネットワーク セキュリティ装置 (VPN ゲートウェイ) から WAN groupVPN 設定をエクスポートするか、**default.rcf** を作成します。
2. **default.rcf** にエクスポートされる設定ファイルの名前を変更します。
3. 次のようにコマンド行を入力して、**GVCSetup*XX*.exe** から **GVCInstall*XX*.MSI** を抽出します (***XX*** の個所は、32 ビット Windows プラットフォームの場合は **32**、64 ビット Windows プラットフォームの場合は **64** です)。

   ```
   GVCSetupXX.exe /T:<MSI が抽出されるパス> /C
   ```

4. **GVCInstall*XX*.MSI** (インストーラ ファイル) が置かれているディレクトリに **default.rcf** ファイルをコピーします。
5. インストーラ (**GVCInstallXX.MSI**) を起動します。インストール プロセスにおいて **default.rcf** が GVC インストール ディレクトリにコピーされます。
6. インストールが完了してグローバル VPN クライアントを起動すると、**default.rcf** が読み込まれ、そこから定義済みのコネクションが作成されます。

△ **注意:** プログラムが default.rcf ファイル内で定義された設定を基に **Connections.rcf** ファイルを書き込むためには、**default.rcf** ファイルがグローバル VPN クライアントのインストール ディレクトリである `C:\Program Files\SonicWall\グローバル VPN クライアント\` に配置されている必要があります。

default.rcf ファイルを インストール ディレクトリに追加する

グローバル VPN クライアントソフトウェアをインストールした後、プログラムを実行する前に、**default.rcf** ファイルをグローバル VPN クライアントのインストール ディレクトリである C:\Program Files\SonicWall\グローバル VPN クライアント\ に追加することができます。

グローバル VPN クライアントプログラムを起動すると、**default.rcf** ファイルの設定を基に、設定ファイル **Global VPN Client.rcf** が C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\ ディレクトリに作成されます。

既存の .rcf ファイル を default.rcf ファイルで置き換える

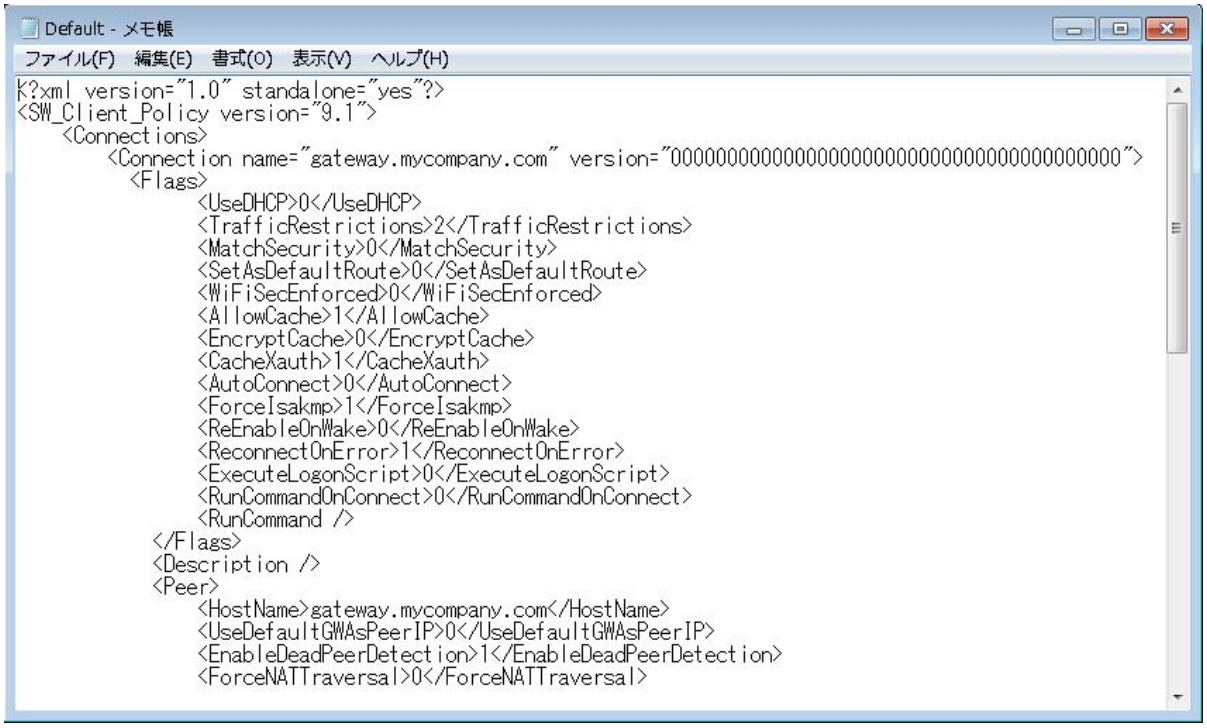
設定ファイル **Connections.rcf** が C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\ ディレクトリに既に存在している場合に、このファイルを削除して、**default.rcf** ファイルをグローバル VPN クライアントのインストール ディレクトリ C:\Program Files\SonicWall\グローバル VPN クライアント\ に追加することができます。ユーザが次にグローバル VPN クライアントを起動すると、**default.rcf** ファイルの設定を基に、**Connections.rcf** ファイルが C:\Users\<user>\AppData\Roaming\SonicWall\グローバル VPN クライアント\ ディレクトリに作成されます。

注意: Connections.rcf ファイルはユーザ固有となっており、ほとんどの場合、同じマシン上であっても、SonicWall グローバル VPN クライアントを実行する別のユーザに対しては機能しません。

注意: 既存の Connections.rcf ファイルを削除すると、グローバル VPN クライアント内で作成した VPN コネクションも削除されます。これらの VPN コネクションは、グローバル VPN クライアントから新規に作成された Connections.rcf ファイル内に、再度追加することができます。

default.rcf ファイルの作成

Windows のメモ帳などのテキストエディタで、**default.rcf** ファイルを作成できます。



default.rcf ファイルに使用するタグの説明

default.rcf で明示しなかったタグは、デフォルトに設定されます (これは、グローバル VPN クライアント内で新規の VPN コネクションを手動設定する時と同じ動作です)。各タグのデフォルト設定は、**[default]** のように括弧付きの太字で示されています。

<SW_Client_Policy version =”9.0”>

<Connections> – default.rcf ファイル内のコネクション定義です。コネクション数にハード上の制限はありません。

<Connection name = コネクション名**>** – グローバル VPN クライアントウィンドウに表示されるコネクション名です。

<Description> *説明テキスト* **</Description>** – グローバル VPN クライアントウィンドウで VPN ポリシーにマウスを合わせた時に表示される、各コネクション プロファイルの説明です。<Description> タグに設定する説明文は最大 1023 文字までです。

<Flags>

<AutoConnect>[Off=0]/On=1**</AutoConnect>** – プログラム開始時にこのコネクションを有効化します。

<ForceIsakmp>Off=0/[On=1]**</ForceIsakmp>** – コネクションを有効にした際、ネットワークトラフィックを待たずに IKE ネゴシエーションを開始します。無効にした場合、接続先ネットワークへのトラフィックが発生した時に IKE ネゴシエーションを開始します。

<ReEnableOnWake>[Off=0]/On=1**</ReEnableOnWake>** – コンピュータがスリープ状態やハイバネーション状態から復帰すると自動的に VPN コネクションが有効になります。

<ReconnectOnError>Off=0/**[On=1]</ReconnectOnError>** – エラー発生時にコネクションの有効化を自動的に試行し続けます。

<ExecuteLogonScript>[Disable=0]/Enable=1**</ExecuteLogonScript>** – ログイン スクリプトを強制的に起動します。

</Flags>

<Peer> – VPN コネクションの対岸のゲートウェイを定義します。1 つの VPN コネクションで 5 つまで対岸のゲートウェイをサポートします。

<HostName>*IP アドレス/ドメイン名***</HostName>** – SonicWall ゲートウェイの IP アドレスもしくは ドメイン名です。

<EnableDeadPeerDetection>Off=0/On=1**</EnableDeadPeerDetection>** – 対岸の動作停止を検出させます。この機能が有効な場合、対岸の無動作を検出するハートビート トラフィックを有効にするために、IKE ネゴシエーション中にベンダー ID が SonicWall 装置に送信されます。

補足: NAT トラバーサル - 以下の 3 つの項目を含むドロップダウン選択リストがあります。

- **自動** - NAT トラバーサルがオンであるかオフであるかを検出します。
- **強制使用** - NAT トラバーサルを強制的にオンにします。
- **無効** - NAT トラバーサルを強制的にオフにします。

個別の **default.rcf** ファイル内で 「自動」を指定するには、ForceNATTraversal および DisableNATTraversal を 0 に設定するか、これらのタグを一切示さないようにします。

<ForceNATTraversal>[Off=0]/On=1**</ForceNATTraversal>** – NAPT・NAT装置が対岸との間に存在するかどうかにかかわらず、NAT トラバーサルを有効にします。通常、NAT 装置が対岸との間に存在するかを自動的に検出して、IKE ネゴシエーション完了後に IPSec パケットの UDP カプセル化の有効化を開始します。

<DisableNATTraversal>[Off=0]/On=1**</DisableNATTraversal>** – 間に NAT デバイスがない場合でも、NAT トラバーサルを無効にします。通常、NAT 装置が対岸との間に存在するかを自動的に検出して、IKE ネゴシエーション完了後に IPSec パケットの UDP カプセル化の有効化を開始します。

<NextHop>IP アドレス**</NextHop>** – このコネクションの次のホップ IP アドレスです。

重要: <NextHop> の設定は、次のホップがデフォルトゲートウェイと異なる場合のみ必要です。

<Timeout>[3]<Timeout> – パケット伝送のタイムアウトを秒で定義します。<Timeout> の最小値は 1 秒、最大値は 10 秒です。

<Retries>[3]<Retries> – コネクションが切断されたとみなされるまでのパケットの再送回数です。<Retries> の最小値は 1、最大値は 10 です。

<UseDefaultGWAsPeerIP>[Off=0]/On=1**</UseDefaultGWAsPeerIP>** – PC のデフォルト ゲートウェイ IP アドレスが対岸候補の IP アドレスとして使用されるよう指定します。

<WaitForSourceIP>Off=0/**[On=1]</WaitForSourceIP>** – ローカル ソースの IP アドレスが利用できる場合にパケットが送信されるよう指定します。

<D**PDInterval>[[3]**-30]**</DPDInterval>** – 対岸候補が機能していないことを宣言するまでの待ち時間 (秒単位) を指定します。インターバル時間の許容値は、**3** 秒、5 秒、10 秒、15 秒、20 秒、25 秒、30 秒です。

<DPDAttempts>[3-**[5]]</DPDAttempts>** – 対岸候補との交信の試行に何回失敗したら対岸候補が機能していないことを宣言するかを指定します。許容値は、3 回、4 回、**5** 回です。

<DPDAlwaysSend>[*Off=0]*/*On=1*</DPDAlwaysSend> – 対岸から受信したネットワーク トラフィックに基づいて DPD パケットを送信するようにグローバル VPN クライアントに指示します。

</Peer> – このコネクションに対する対岸のゲートウェイの数だけ、<Peer> タグ配下のタグを繰り返します。各コネクションには最大 5 つまで対岸のゲートウェイを設定できます。

</Connection> – 設定ファイル内の各コネクション設定の終了を意味します。

</Connections> – **Default.rcf** ファイル内のすべてのコネクション設定の終了を意味します。

</SW_Client_Policy>

default.rcf ファイルのサンプル

以下は **default.rcf** ファイルの例です。このファイルには、2 つの VPN コネクションが含まれています。Corporate Firewall および Overseas Office。Corporate Firewall コネクションには、VPN 接続の多重化のために 2 つの対岸のゲートウェイ設定があります。

注意: このサンプル ファイルを ASCII テキスト エディタに直接コピーする場合には、各行の終わりにある段落記号をすべて削除してから保存する必要があります。配信前に、このファイルをグローバル VPN クライアント アプリケーションにインポートできるか検証してください。

```
<?xml version="1.0" standalone="yes"?>
<SW_Client_Policy version="9.0">
    <Connections>
        <Connection name="Corporate Firewall">
            <Description>これは企業向けファイアウォールです。接続の問題については、1-800-fix-today にお問い合わせください。</Description>
            <Flags>
                <AutoConnect>0</AutoConnect>
                <ForceIsakmp>1</ForceIsakmp>
                <ReEnableOnWake>0</ReEnableOnWake>
                <ReconnectOnError>1</ReconnectOnError>
                <ExecuteLogonScript>0</ExecuteLogonScript>
            </Flags>
            <Peer>
```

```
            <HostName>CorporateFW</HostName>
            <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
            <ForceNATTraversal>0</ForceNATTraversal>
            <DisableNATTraversal>0</DisableNATTraversal>
            <NextHop>0.0.0.0</NextHop>
            <Timeout>3</Timeout>
            <Retries>3</Retries>
            <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
            <InterfaceSelection>0</InterfaceSelection>
            <WaitForSourceIP>0</WaitForSourceIP>
            <DPDInterval>3</DPDInterval>
            <DPDAttempts>3</DPDAttempts>
            <DPDAlwaysSend>0</DPDAlwaysSend>
        </Peer>
        <Peer>
            <HostName>1.2.3.4</HostName>
            <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
            <ForceNATTraversal>0</ForceNATTraversal>
            <DisableNATTraversal>0</DisableNATTraversal>
            <NextHop>0.0.0.0</NextHop>
            <Timeout>3</Timeout>
            <Retries>3</Retries>
            <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
            <InterfaceSelection>0</InterfaceSelection>
            <WaitForSourceIP>0</WaitForSourceIP>
            <DPDInterval>3</DPDInterval>
            <DPDAttempts>3</DPDAttempts>
            <DPDAlwaysSend>0</DPDAlwaysSend>
        </Peer>
    </Connection>
    <Connection name="Overseas Gateway">
        <Description>これは海外旅行時に接続するファイアウォールです。</Description>
        <Flags>
            <AutoConnect>0</AutoConnect>
            <ForceIsakmp>1</ForceIsakmp>
            <ReEnableOnWake>0</ReEnableOnWake>
            <ReconnectOnError>1</ReconnectOnError>
```

```
                <ExecuteLogonScript>0</ExecuteLogonScript>
            </Flags>
            <Peer>
                <HostName>&lt;Default Gateway&gt;</HostName>
                <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
                <ForceNATTraversal>0</ForceNATTraversal>
                <DisableNATTraversal>0</DisableNATTraversal>
                <NextHop>0.0.0.0</NextHop>
                <Timeout>3</Timeout>
                <Retries>3</Retries>
                <UseDefaultGWAsPeerIP>1</UseDefaultGWAsPeerIP>
                <InterfaceSelection>0</InterfaceSelection>
                <WaitForSourceIP>0</WaitForSourceIP>
                <DPDInterval>3</DPDInterval>
                <DPDAttempts>3</DPDAttempts>
                <DPDAlwaysSend>0</DPDAlwaysSend>
            </Peer>
        </Connection>
    </Connections>
</SW_Client_Policy>
```

default.rcf ファイルのトラブルシューティング

問題点	解決法
default.rcf ファイルに不正確な項目または入力誤りが存在する場合、**default.rcf** ファイルの設定はグローバル VPN クライアントに反映されず、コネクション プロファイルがグローバル VPN クライアントウィンドウに一切表示されません。次のいずれかのエラー メッセージが表示されます。 • 「***Failed to parse configuration <ファイル>***」というメッセージが、グローバル VPN クライアントのログ ビューアに表示されます。 • **「指定された設定ファイルをインポートできませんでした。このファイルは破損しています」**というメッセージが、ファイルをインポートしようとしたときに表示されます。	ファイルに ASCII 文字以外の文字が含まれていないことを確認します。**default.rcf** ファイルで作成された **Connections.rcf** ファイルは、\ ディレクトリおよびエラー修正編集された **default.rcf** ファイルから削除してください。
default.rcf ファイルが「読み取り専用」の属性を持つことができません。	**default.rcf** ファイルで作成された **Connections.rcf** ファイルは、\ ディレクトリおよび「読み取り専用」の属性が削除されてエラー修正された **default.rcf** ファイルから削除してください。
接続試行時、対岸候補名 <Default Gateway> に次のエラーメッセージが表示されます。「**対岸候補名 <Default Gateway> の IP アドレスへの変換に失敗しました**」。	対岸候補名を <Default Gateway> の特例に設定する際に、**<UseDefaultGWAsPeerIP>** のタグを **1** に設定します。**default.rcf** ファイルによって作成された Connections.rcf ファイルは、\ ディレクトリから削除します。

B

グローバル VPN クライアント CLI の使用

グローバル VPN クライアント CLI について

SonicWall グローバル VPN クライアントは、CLI (コマンドライン インターフェース) から実行することができます。このインターフェースを使えば、グローバル VPN クライアントアプリケーションを直接操作しなくても、グローバル VPN クライアントの特定の機能を、プログラムまたはスクリプト ベースで実行できます。グローバル VPN クライアント CLI により、特定のアプリケーションまたはコネクション方式を開始する場合に必ず安全なトンネルを自動的に確立するスクリプトをセットアップすることができます。

CLI コマンドでは、グローバル VPN クライアントアプリケーションの完全なパス名の後に、ユーザ名やパスワードなどの各種のフラグや変数の情報を指定することが求められます。

注意: ユーザのパスワードをスクリプトに直接組み込むのは、セキュリティ上のリスクとなります。スクリプトにアクセスできれば、誰でもセキュリティを回避するパスワードを読むことができます。コネクションの起動前にスクリプトまたはプログラムのダッシュボードでパスワードを求めてから変数をクリアするようにしてください。

コマンドライン オプション

以下のオプションを使用して、コマンドラインからグローバル VPN クライアントのさまざまなアクションを実行できます。

- **/E "*コネクション名*"** – 特定のコネクションを有効化します。
- **/D "*コネクション名*"** – 特定のコネクションを無効化します。
- **/Q** –プログラムを終了します。プログラムが起動されていない場合には無視されます。
- **/A [*ファイル名*]** –プログラムを起動し、すべてのメッセージを指定したログファイルに記録します。ログファイルを指定しない場合には、デフォルトファイル名の **gvcauto.log** が使用されます。既にプログラムが起動されている場合には、このオプションは無視されます。
- **/U "*Username*"** - XAUTH で使用するユーザ名を指定します。このオプションは、**/E** とともに使用します。
- **/P "*Password*"** - XAUTH で使用するパスワードを指定します。このオプションは、**/E** とともに使用します。

コマンド ラインの例

- **<*path*>\swgvpnclient** - アプリケーションの実行や起動を行います。アプリケーションが既に実行されている場合は、別のインスタンスは作成されません。
- **<*path*>\swgvpnclient /E <*connection name*> /U <*username*> and /P <*password*>** - アプリケーションの実行や起動を行い、指定のコネクションを有効にし、<username> と <password> をユーザ認証に使用します。ユーザ名やパスワードを指定しない場合、グローバル VPN クライアントは処理の続行に必要な情報を求めるダイアログを表示します。
- **<*path*>\swgvpnclient /A <*path\filename*>** - アプリケーションの実行や起動を行い、ログ ファイルに対する全イベントの自動ログを有効にします。ファイル名を指定しない場合、<gvcauto.log> のデフォルト名でログ ファイルが作成されます。グローバル VPN クライアントの各セッションの自動ログを保存する場合は、ファイル名オプションを使用して、アプリケーションを起動するたびに別のファイル名を指定します。パスを指定しない場合、このファイルはグローバル VPN クライアント アプリケーションが起動するのと同じディレクトリに作成されます。

C

ログ ビューア メッセージ

このセクションでは、SonicWall グローバル VPN クライアントのログ メッセージについて説明します。グローバル VPN クライアントのログ ビューアに表示される**エラー**、**情報**、**警告** の各メッセージを、以下の表に示します。

エラー メッセージ

種別	メッセージ
ERROR 【エラー】	"Invalid DOI in notify message,"
ERROR 【エラー】	: called with invalid parameters.
ERROR 【エラー】	A phase 2 IV has already been created.
ERROR 【エラー】	An error occurred.
ERROR 【エラー】	Attributes were specified but not offered.
ERROR 【エラー】	Authentication algorithm is not supported.
ERROR 【エラー】	CA certificate not found in list.
ERROR 【エラー】	Calculated policy configuration attributes length does not match length of attributes set into policy configuration payload.
ERROR 【エラー】	Calculated XAuth attributes length does not match length of attributes set into XAuth payload.
ERROR 【エラー】	Can not change the Diffie-Hellman group for PFS.
ERROR 【エラー】	Can not process packet that does not have at least one payload.
ERROR 【エラー】	Can not process unsupported mode config type.
ERROR 【エラー】	Can not process unsupported XAuth type.

種別	メッセージ
ERROR 【エラー】	Can not set IPSEC proposals into empty SA list.
ERROR 【エラー】	Cannot do quick mode: no SA's to negotiate.
ERROR 【エラー】	Certificate error.
ERROR 【エラー】	Certificate ID not specified.
ERROR 【エラー】	Deallocation of event publisher context failed.
ERROR 【エラー】	Diffie-Hellman group generator length has not been set.
ERROR 【エラー】	Diffie-Hellman group prime length has not been set.
ERROR 【エラー】	DSS signature processing failed - signature is not valid.
ERROR 【エラー】	Encryption algorithm is not supported.
ERROR 【エラー】	ESP transform algorithm is not supported.
ERROR 【エラー】	Failed to add a new AH entry to the phase 2 SA list.
ERROR 【エラー】	Failed to add a new ESP entry to the phase 2 SA list.
ERROR 【エラー】	Failed to add IPSEC encapsulation mode into the payload.
ERROR 【エラー】	Failed to add IPSEC group description into the payload.
ERROR 【エラー】	Failed to add IPSEC HMAC algorithm into the payload.
ERROR 【エラー】	Failed to add IPSEC life duration into the payload.
ERROR 【エラー】	Failed to add IPSEC life type into the payload.
ERROR 【エラー】	Failed to add OAKLEY authentication algorithm into the payload.
ERROR 【エラー】	Failed to add OAKLEY encryption algorithm into the payload.
ERROR 【エラー】	Failed to add OAKLEY generator G1 into the payload.
ERROR 【エラー】	Failed to add OAKLEY group description into the payload.
ERROR 【エラー】	Failed to add OAKLEY group type into the payload.
ERROR 【エラー】	Failed to add OAKLEY hash algorithm into the payload.

種別	メッセージ
ERROR 【エラー】	Failed to add OAKLEY life duration into the payload.
ERROR 【エラー】	Failed to add OAKLEY life type into the payload.
ERROR 【エラー】	Failed to add OAKLEY prime P into the payload.
ERROR 【エラー】	Failed to add policy configuration INI format into the payload.
ERROR 【エラー】	Failed to add policy configuration version into the payload.
ERROR 【エラー】	Failed to add XAuth password '' into the payload.
ERROR 【エラー】	Failed to add XAuth status into the payload.
ERROR 【エラー】	Failed to add XAuth type into the payload.
ERROR 【エラー】	Failed to add XAuth username '' into the payload.
ERROR 【エラー】	Failed to allocate bytes.
ERROR 【エラー】	Failed to allocate memory.
ERROR 【エラー】	Failed to begin phase 1 exchange.
ERROR 【エラー】	Failed to begin quick mode exchange.
ERROR 【エラー】	Failed to build a DSS object.
ERROR 【エラー】	Failed to build dead peer detection packet.
ERROR 【エラー】	Failed to build dead peer detection reply message.
ERROR 【エラー】	Failed to build dead peer detection request message.
ERROR 【エラー】	Failed to build phase 1 delete message.
ERROR 【エラー】	Failed to calculate DES mode from ESP transfer.
ERROR 【エラー】	Failed to calculate policy configuration attributes length.
ERROR 【エラー】	Failed to calculate XAuth attributes length.
ERROR 【エラー】	Failed to compute IV for connection entry.
ERROR 【エラー】	Failed to construct certificate payload.

種別	メッセージ
ERROR 【エラー】	Failed to construct certificate request payload.
ERROR 【エラー】	Failed to construct certificate.
ERROR 【エラー】	Failed to construct destination proxy ID payload.
ERROR 【エラー】	Failed to construct DSS signature.
ERROR 【エラー】	Failed to construct hash payload.
ERROR 【エラー】	Failed to construct IPSEC nonce payload.
ERROR 【エラー】	Failed to construct IPSEC SA payload.
ERROR 【エラー】	Failed to construct ISAKMP blank hash payload.
ERROR 【エラー】	Failed to construct ISAKMP delete hash payload.
ERROR 【エラー】	Failed to construct ISAKMP DPD notify payload.
ERROR 【エラー】	Failed to construct ISAKMP ID payload.
ERROR 【エラー】	Failed to construct ISAKMP info hash payload.
ERROR 【エラー】	Failed to construct ISAKMP key exchange payload.
ERROR 【エラー】	Failed to construct ISAKMP nonce payload.
ERROR 【エラー】	Failed to construct ISAKMP notify payload.
ERROR 【エラー】	Failed to construct ISAKMP packet header.
ERROR 【エラー】	Failed to construct ISAKMP phase 1 delete payload.
ERROR 【エラー】	Failed to construct ISAKMP SA payload.
ERROR 【エラー】	Failed to construct ISAKMP vendor ID payload (ID =).
ERROR 【エラー】	Failed to construct mode config hash payload.
ERROR 【エラー】	Failed to construct NAT discovery payload.
ERROR 【エラー】	Failed to construct PFS key exchange payload.
ERROR 【エラー】	Failed to construct policy provisioning payload.

種別	メッセージ
ERROR 【エラー】	Failed to construct quick mode hash payload.
ERROR 【エラー】	Failed to construct quick mode packet.
ERROR 【エラー】	Failed to construct responder lifetime payload.
ERROR 【エラー】	Failed to construct RSA signature.
ERROR 【エラー】	Failed to construct signature payload.
ERROR 【エラー】	Failed to construct source proxy ID payload.
ERROR 【エラー】	Failed to construct XAuth payload.
ERROR 【エラー】	Failed to convert the peer name to an IP address.
ERROR 【エラー】	Failed to create a new connection entry: an entry already exists with ID.
ERROR 【エラー】	Failed to create connection entry with message ID.
ERROR 【エラー】	Failed to decrypt buffer.
ERROR 【エラー】	Failed to decrypt mode config payload.
ERROR 【エラー】	Failed to decrypt notify payload.
ERROR 【エラー】	Failed to decrypt packet.
ERROR 【エラー】	Failed to decrypt quick mode payload.
ERROR 【エラー】	Failed to encrypt mode config payload.
ERROR 【エラー】	Failed to encrypt notify payload.
ERROR 【エラー】	Failed to encrypt packet.
ERROR 【エラー】	Failed to encrypt quick mode payload.
ERROR 【エラー】	Failed to expand packet to size bytes.
ERROR 【エラー】	Failed to find an SA list for PROTO_IPSEC_AH.
ERROR 【エラー】	Failed to find an SA list for PROTO_IPSEC_ESP.
ERROR 【エラー】	Failed to find an SA list given the protocol.

種別	メッセージ
ERROR 【エラー】	Failed to find certificate with ID.
ERROR 【エラー】	Failed to find connection entry for message ID.
ERROR 【エラー】	Failed to find exit interface to reach.
ERROR 【エラー】	Failed to find MAC address in the system interfaces table.
ERROR 【エラー】	Failed to find matching SA list.
ERROR 【エラー】	Failed to find message ID and matching cookies in the connection entry list.
ERROR 【エラー】	Failed to find message ID in the connection entry list.
ERROR 【エラー】	Failed to find message ID in the SA list.
ERROR 【エラー】	Failed to find OAKLEY group specified in the SA payload.
ERROR 【エラー】	Failed to find private key for certificate with ID.
ERROR 【エラー】	Failed to find protocol ID in the SA list.
ERROR 【エラー】	Failed to find route to reach.
ERROR 【エラー】	Failed to find sequence number.
ERROR 【エラー】	Failed to find source IP address to reach.
ERROR 【エラー】	Failed to flush the system ARP cache.
ERROR 【エラー】	Failed to generate Diffie-Hellman parameters.
ERROR 【エラー】	Failed to generate quick mode initiator key.
ERROR 【エラー】	Failed to generate quick mode responder key.
ERROR 【エラー】	Failed to generate SKEYID.
ERROR 【エラー】	Failed to get the size of the system interfaces table.
ERROR 【エラー】	Failed to get the size of the system IP address table.
ERROR 【エラー】	Failed to get the system interface table.
ERROR 【エラー】	Failed to get the system IP address table.

種別	メッセージ
ERROR 【エラー】	Failed to get transforms from SA list.
ERROR 【エラー】	Failed to match initiator cookie.
ERROR 【エラー】	Failed to match responder cookie.
ERROR 【エラー】	Failed to parse certificate data.
ERROR 【エラー】	Failed to parse configuration file.
ERROR 【エラー】	Failed to read the size of an incoming ISAKMP packet.
ERROR 【エラー】	Failed to re-allocate bytes.
ERROR 【エラー】	Failed to receive an incoming ISAKMP packet.
ERROR 【エラー】	Failed to receive an incoming ISAKMP packet.The length is incorrect.
ERROR 【エラー】	Failed to send an outgoing ISAKMP packet.
ERROR 【エラー】	Failed to set policy configuration attributes into payload.
ERROR 【エラー】	Failed to set proposals into phase 1 SA payload.
ERROR 【エラー】	Failed to set proposals into phase 2 SA payload.
ERROR 【エラー】	Failed to set responder lifetype attributes.
ERROR 【エラー】	Failed to set the ESP attributes from the SA payload into the SA.
ERROR 【エラー】	Failed to set the IPSEC AH attributes into the phase 2 SA.
ERROR 【エラー】	Failed to set the IPSEC ESP attributes into the phase 2 SA.
ERROR 【エラー】	Failed to set the OAKLEY attributes into the phase 1 SA.
ERROR 【エラー】	Failed to set vendor ID into packet payload.
ERROR 【エラー】	Failed to set XAuth attributes into payload.
ERROR 【エラー】	Failed to sign hash.
ERROR 【エラー】	Failed to verify certificate signature.
ERROR 【エラー】	Failed to verify informational message hash payload.

種別	メッセージ
ERROR 【エラー】	Failed to verify mode config message hash payload.
ERROR 【エラー】	Hash algorithm is not supported.
ERROR 【エラー】	Hash Payload does not match.
ERROR 【エラー】	Hash size invalid:
ERROR 【エラー】	Header invalid (verified)!
ERROR 【エラー】	Invalid certificate:ASN sequence is not correct.
ERROR 【エラー】	Invalid certificate: payload length is too small.
ERROR 【エラー】	Invalid hash payload.
ERROR 【エラー】	Invalid payload.Possible overrun attack!
ERROR 【エラー】	Invalid SA state:
ERROR 【エラー】	Invalid signature payload.
ERROR 【エラー】	Invalid SPI size.
ERROR 【エラー】	is not a supported Diffie-Hellman group type.
ERROR 【エラー】	is not a supported DOI.
ERROR 【エラー】	is not a supported exchange type.
ERROR 【エラー】	is not a supported ID payload type.
ERROR 【エラー】	is not a supported IPSEC protocol.
ERROR 【エラー】	is not a supported notify message type.
ERROR 【エラー】	is not a supported payload type.
ERROR 【エラー】	is not a supported policy configuration attribute type.
ERROR 【エラー】	is not a supported policy configuration message type.
ERROR 【エラー】	is not a supported proxy ID payload type.
ERROR 【エラー】	is not a supported XAuth attribute type.

種別	メッセージ
ERROR 【エラー】	is not a valid quick mode state.
ERROR 【エラー】	is not a valid XAuth message type.
ERROR 【エラー】	is not a valid XAuth status.
ERROR 【エラー】	ISAKMP SA delete msg for a different SA!
ERROR 【エラー】	No certificate for CERT authentication.
ERROR 【エラー】	No entry in the system IP address table was found with index.
ERROR 【エラー】	No KE payload while PFS configured mess_id.
ERROR 【エラー】	Out of memory.
ERROR 【エラー】	Phase 1 authentication algorithm is not supported.
ERROR 【エラー】	Phase 1 encryption algorithm is not supported.
ERROR 【エラー】	Protocol ID has already been added to the SA list.
ERROR 【エラー】	Protocol mismatch: expected PROTO_IPSEC_AH but got.
ERROR 【エラー】	Protocol mismatch: expected PROTO_IPSEC_ESP but got.
ERROR 【エラー】	Publisher deregistration failed.
ERROR 【エラー】	Responder cookie is not zero.
ERROR 【エラー】	RSA signature processing failed - signature is not valid.
ERROR 【エラー】	SA hash function has not been set in.
ERROR 【エラー】	Signature Algorithm mismatch is X.509 certificate.
ERROR 【エラー】	Signature verification failed!
ERROR 【エラー】	The certificate is not valid at this time.
ERROR 【エラー】	The current state is not valid for processing mode config payload.
ERROR 【エラー】	The current state is not valid for processing signature payload.
ERROR 【エラー】	The first payload is not a hash payload.

種別	メッセージ
ERROR【エラー】	The following error occurred while trying to open the configuration file:
ERROR【エラー】	The peer is not responding to phase 1 ISAKMP requests.
ERROR【エラー】	The peer is not responding to phase 1 ISAKMP requests.
ERROR【エラー】	The state flag indicates that the IPSEC SA payload has not been processed.
ERROR【エラー】	The system interface table is empty.
ERROR【エラー】	The system IP address table is empty.
ERROR【エラー】	Unable to compute hash!
ERROR【エラー】	Unable to compute shared secret for PFS in phase 2!
ERROR【エラー】	Unable to read configuration file.
ERROR【エラー】	User did not enter XAuth next pin.
ERROR【エラー】	XAuth CHAP requests are not supported at this time.
ERROR【エラー】	XAuth failed.
ERROR【エラー】	XAuth has requested a password but one has not yet been specified.

情報メッセージ

種別	メッセージ
INFO【情報】	"The connection """" has been disabled."
INFO【情報】	A certificate is needed to complete phase 1.
INFO【情報】	A phase 2 SA can not be established with until a phase 1 SA is established.
INFO【情報】	A pre-shared key is needed to complete phase 1.
INFO【情報】	AG failed.SA state unknown.Peer:
INFO【情報】	An incoming ISAKMP packet from was ignored.
INFO【情報】	DSS g value:
INFO【情報】	DSS p value:
INFO【情報】	DSS q value:
INFO【情報】	Event publisher deregistered.
INFO【情報】	Event publisher registered for.
INFO【情報】	Failed to negotiate configuration information with.

種別	メッセージ
INFO【情報】	Found CA certificate in CA certificate list.
INFO【情報】	Ignoring unsupported payload.
INFO【情報】	Ignoring unsupported vendor ID.
INFO【情報】	ISAKMP phase 1 proposal is not acceptable.
INFO【情報】	ISAKMP phase 2 proposal is not acceptable.
INFO【情報】	MM failed.Payload processing failed.OAK_MM_KEY_EXCH.Peer:
INFO【情報】	MM failed.Payload processing failed:OAK_MM_NO_STATE.Peer:
INFO【情報】	MM failed.Payload processing failed:OAK_MM_SA_SETUP.Peer:
INFO【情報】	MM failed.SA state not matching mask process auth.Peer:
INFO【情報】	MM failed.SA state not matching mask process key.Peer:
INFO【情報】	MM failed.SA state not matching mask process sa.Peer:
INFO【情報】	MM failed.SA state unknown.Peer:
INFO【情報】	NAT Detected:Local host is behind a NAT device.
INFO【情報】	NAT Detected:Peer is behind a NAT device.
INFO【情報】	peer certificate missing key value.
INFO【情報】	Phase 1 has completed.
INFO【情報】	Phase 1 SA lifetime set to.
INFO【情報】	Phase 2 negotiation has failed.
INFO【情報】	Phase 2 SA lifetime set to.
INFO【情報】	Phase 2 with has completed.
INFO【情報】	Proposal not acceptable: not authentication algorithm specified.
INFO【情報】	Proposal not acceptable: not Diffie-Hellman group specified.
INFO【情報】	Proposal not acceptable: not encryption algorithm specified.
INFO【情報】	Proposal not acceptable: not hash algorithm specified.
INFO【情報】	Proposal not acceptable: proposal not found in list.
INFO【情報】	QM failed.Load SA failed.Peer:
INFO【情報】	Reading configuration file.
INFO【情報】	Ready to negotiate phase 2 with.
INFO【情報】	Received address notification notify.
INFO【情報】	Received attributes not supported notify.
INFO【情報】	Received authentication failed notify.
INFO【情報】	Received bad syntax notify.
INFO【情報】	Received certificate unavailable notify.
INFO【情報】	Received dead peer detection acknowledgement.
INFO【情報】	Received dead peer detection request.
INFO【情報】	Received initial contact notify.
INFO【情報】	Received invalid certificate authentication notify.
INFO【情報】	Received invalid certificate encoding notify.

種別	メッセージ
INFO【情報】	Received invalid certificate notify.
INFO【情報】	Received invalid certificate request syntax notify.
INFO【情報】	Received invalid cookie notify.
INFO【情報】	Received invalid exchange type notify.
INFO【情報】	Received invalid flags notify.
INFO【情報】	Received invalid ID information notify.
INFO【情報】	Received invalid key info notify.
INFO【情報】	Received invalid major version notify.
INFO【情報】	Received invalid message ID notify.
INFO【情報】	Received invalid minor version notify.
INFO【情報】	Received invalid payload notify.
INFO【情報】	Received invalid protocol ID notify.
INFO【情報】	Received invalid signature notify.
INFO【情報】	Received invalid SPI notify.
INFO【情報】	Received invalid transform ID notify.
INFO【情報】	Received malformed payload notify.
INFO【情報】	Received no proposal chosen notify.
INFO【情報】	Received notify SA lifetime notify.
INFO【情報】	Received phase 1 delete message.
INFO【情報】	Received phase 2 delete message for SPI.
INFO【情報】	Received policy provisioning acknowledgement.
INFO【情報】	Received policy provisioning OK.
INFO【情報】	Received policy provisioning update.
INFO【情報】	Received policy provisioning version reply.
INFO【情報】	Received policy provisioning version request.
INFO【情報】	Received responder lifetime notify.
INFO【情報】	Received situation not supported notify.
INFO【情報】	Received unequal payload length notify.
INFO【情報】	Received unknown notify.
INFO【情報】	Received unsupported DOI notify.
INFO【情報】	Received unsupported exchange type notify.
INFO【情報】	Received XAuth request.
INFO【情報】	Received XAuth status.
INFO【情報】	Re-evaluating ID info after INVALID_ID_INFO message.
INFO【情報】	Releasing IP address for the virtual interface ().
INFO【情報】	Renewing IP address for the virtual interface ().
INFO【情報】	Saving configuration file.
INFO【情報】	Sending dead peer detection acknowledgement.

種別	メッセージ
INFO【情報】	Sending dead peer detection request.
INFO【情報】	Sending phase 1 delete.
INFO【情報】	Sending phase 2 delete for.
INFO【情報】	Sending policy provisioning acknowledgement.
INFO【情報】	Sending policy provisioning version reply.
INFO【情報】	Sending XAuth acknowledgement.
INFO【情報】	Sending XAuth reply.
INFO【情報】	Signature Verified!
INFO【情報】	SonicWall グローバル VPN クライアント version.
INFO【情報】	SonicWall VPN Client.
INFO【情報】	Starting aggressive mode phase 1 exchange.
INFO【情報】	Starting authentication negotiation.
INFO【情報】	Starting configuration negotiation.
INFO【情報】	Starting ISAKMP phase 1 negotiation.
INFO【情報】	Starting ISAKMP phase 2 negotiation with.
INFO【情報】	Starting main mode phase 1 exchange.
INFO【情報】	Starting quick mode phase 2 exchange.
INFO【情報】	The configuration for the connection has been updated.
INFO【情報】	The configuration for the connection is up to date.
INFO【情報】	The configuration has been updated and must be reloaded.
INFO【情報】	The connection has entered an unknown state.
INFO【情報】	The connection is idle.
INFO【情報】	The hard lifetime has expired for phase 1.
INFO【情報】	The hard lifetime has expired for phase 2 with.
INFO【情報】	The IP address for the virtual interface has been released.
INFO【情報】	The IP address for the virtual interface has changed to.
INFO【情報】	The ISAKMP port (500) is already in use.Port will be used as the ISAKMP source port.
INFO【情報】	The peer is not responding to phase 2 ISAKMP requests to.
INFO【情報】	The phase 1 SA has been deleted.
INFO【情報】	The phase 1 SA has died.
INFO【情報】	The phase 2 SA has been deleted.
INFO【情報】	The phase 2 SA has died.
INFO【情報】	The SA lifetime for phase 1 is seconds.
INFO【情報】	The SA lifetime for phase 2 is seconds.
INFO【情報】	The soft lifetime has expired for phase 1.
INFO【情報】	The soft lifetime has expired for phase 2 with.
INFO【情報】	The system ARP cache has been flushed.
INFO【情報】	Unable to encrypt payload!

種別	メッセージ
INFO【情報】	User authentication has failed.
INFO【情報】	User authentication has succeeded.
INFO【情報】	User authentication information is needed to complete the connection.
INFO【情報】	XAuth has requested a username but one has not yet been specified.

警告メッセージ

種別	メッセージ
WARNING【警告】	A password must be entered.
WARNING【警告】	AG failed.SA state not matching mask process auth.Peer:
WARNING【警告】	AG failed.SA state not matching mask process key.Peer:
WARNING【警告】	AG failed.State OAK_AG_INIT_EXCH is invalid when responder.Peer:
WARNING【警告】	AG failed.State OAK_AG_NO_STATE is invalid when initiator.Peer:
WARNING【警告】	Failed to process aggressive mode packet.
WARNING【警告】	Failed to process final quick mode packet.
WARNING【警告】	Failed to process informational exchange packet.
WARNING【警告】	Failed to process main mode packet.
WARNING【警告】	Failed to process mode configuration packet.
WARNING【警告】	Failed to process packet payloads.
WARNING【警告】	Failed to process payload.
WARNING【警告】	Failed to process quick mode packet.
WARNING【警告】	Ignoring AUTH message when aggressive mode already complete.Peer:
WARNING【警告】	Invalid DOI in delete message:
WARNING【警告】	Invalid IPSEC SA delete message.
WARNING【警告】	Invalid ISAKMP SA delete message.
WARNING【警告】	is not a supported OAKLEY attribute class.

種別	メッセージ
WARNING 【警告】	Protocol ID is not supported in SA payloads.
WARNING 【警告】	Received an encrypted packet when not crypto active!
WARNING 【警告】	Received an unencrypted packet when crypto active!
WARNING 【警告】	Responder lifetime protocol is not supported.
WARNING 【警告】	The password is incorrect.Please re-enter the password.
WARNING 【警告】	The pre-shared key dialog was cancelled by the user.The connection will be disabled.
WARNING 【警告】	The select certificate dialog was cancelled by the user.The connection will be disabled.
WARNING 【警告】	The username/password dialog was cancelled by the user.The connection will be disabled.
WARNING 【警告】	Unable to decrypt payload!

アジア太平洋地域対象 SonicWall エンド ユーザ製品利用規約

改訂：2017 年 2 月 10 日

本製品をご利用になる前に本契約を熟読して下さい。本製品をダウンロード、インストール、又は利用することにより、貴方 (貴社) は本契約の条件を承諾しこれに同意します。本契約の条件に同意しない場合は、本製品のダウンロード、インストール、又は利用はお控え下さい。

このアジア太平洋地域対象 SonicWall エンド ユーザ製品利用規約 (以下「本契約」といいます) はカスタマーである貴方 (貴社) (以下「カスタマー」又は「貴方」といいます) とプロバイダ (以下に定義します) との間で締結されました。

1.定義。本文中に定義されていない以下の用語は、以下のとおりの意味を有します。

(a) 「関連会社」とは、本契約の当事者を支配し、これに支配され、又はこれと同一の支配下にある法人をいいます。但し当該支配関係が存続している場合に限ります。

(b) 「アプライアンス」とは、ソフトウェアが事前に搭載された状態で引き渡されるコンピュータハードウェア製品をいいます。

(c) 「ドキュメント」とは、プロバイダが本製品に対して提供するユーザ マニュアル及びその他の文書並びにこれらの写しをいいます。

(d) 「メンテナンス サービス」とは、プロバイダによる本製品のメンテナンス及びサポートの提供をいい、下記の「メンテナンス サービス」のセクションに記載されます。

(e) 「パートナー」とは、プロバイダ又は他のパートナーと契約を締結しており、当該契約に基づいて本製品又はメンテナンス サービスを再販売する権限を有する再販売業者又は販売業者をいいます。

(f) 「***プロバイダ***」とは、(i) 台湾においては 5455 Great America Parkway, Santa Clara, CA 95054 USA に主たる営業所を有する SonicWall Inc.、(ii) (台湾以外の) アジアにおいては SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland をいいます。

(g) 「本製品」とは、本契約に基づいてカスタマーに提供されるソフトウェア及びアプライアンスをいいます。

(h) 「ソフトウェア」とは、アプライアンス上で提供されるソフトウェアのオブジェクト コード バージョン、後からカスタマーに提供されるその他任意のソフトウェア、本契約に従いカスタマーに利用可能とされる当該ソフトウェアのすべての新規バージョン及びリリース、並びにこれらのコピーをいいます。

2.ソフトウェアのライセンス。

(a) **一般条項。**本契約の条件に従い、プロバイダはカスタマーに対し、プロバイダ又はパートナーから購入したソフトウェアの各品目を、以下に記載されたライセンス タイプ (以下「**ライセンス タイプ**」といいます) の範囲内で購入した数量までアクセス及び利用する、非独占的、譲渡不能 (本契約に別途定められている場合を除きます)、且つサブライセンス不能のライセンスを付与します (以下「ライセンス」といいます) 。MSP ライセンス (以下に定義します) を除いて、カスタマーは、自社及び世界各地に所在するその関連会社の内部業務の運営の補助のみを目的としてかかるソフトウェアを使用します。

(b) **ライセンス タイプ**。アプライアンス上に最初に提供されるソフトウェアのライセンス タイプは、「**アプライアンス単位**」です。アプライアンス単位でライセンス供与されるソフトウェアは、それが提供されているアプライアンス上でしか使用できませんが、その他の量的制限はありません。サブスクリプションに基づいて購入されるソフトウェア、又は定期的に購入されるソフトウェアは、ユーザ又は管理ノードごとにライセンス供与されます。「**ユーザ**」とは、ソフトウェアに個別の ID でログインする各個人を指します。「**管理ノード**」とは、ソフトウェアによって管理される任意のオブジェクトを指します。これには、プロバイダによって販売されるファイアウォールや機器などの品目が含まれますが、これらに限定されません。

(c) **Software as a Service 。**カスタマーが、プロバイダ又はそのサプライヤが運用する設備上のソフトウェア (以下「SaaS ソフトウェア」といいます) にアクセスして使用する権利を購入する場合、(i) かかる SaaS ソフトウェアのライセンスは、オーダーに記載された期間中 (以下「SaaS 期間」といいます) 付与されるものとし (かかる SaaS 期間は、自動的又は合意による更新によって延長となることがあります)、(ii) 本契約の「SaaS 条件」のセクションに記載する条件は、かかるソフトウェアのすべてのアクセス及び使用に適用されるものとします。カスタマーの設備にインストールされるソフトウェアの品目が、SaaS ソフトウェアとの関連において提供される場合、かかるソフトウェアのライセンス期間は、該当する Saas 期間についてとし、又カスタマーは、プロバイダが提供するかかるソフトウェアのすべてのアップデートを速やかにインストールするものとします。

(d) **MSP ライセンス。**

「マネジメント サービス」には、カスタマーが自身の顧客 (以下、それぞれを「クライアント」といいます) の設備にソフトウェアのコピーをインストールする、又は本製品に対するアクセスをクライアントに提供する場合に、クライアントに対してカスタマーが提供するアプリケーション、オペレーティング システム及びデータベースの実行、パフォーマンス チューニング、並びにメンテナンス サービスが含まれますが、これらに限定されません。カスタマーは、マネジメント サービスを提供するためにソフトウェア及びこれに付随するドキュメントを使用するライセンス (以下「MSP ライセンス」といいます) を付与されます。各 MSP ライセンスには、本契約の条件及び当事者間の合意に基づくその他の条件が適用されます。

カスタマーがマネージド サービス プロバイダとして本製品を使用する場合、カスタマーは、(i) 本製品に関して本契約に含まれる SonicWall の表明又は保証を超える表明又は保証を行わないこと、(ii) 各クライアントが、カスタマーから提供されたマネジメント サービスの一環としてのみ、本製品及びドキュメントを使用すること、(iii) 当該使用が、本契約 (本契約の「輸出」のセクションを含むがそれに限定されません) の制約及び制限を受けること、且つ (iv) 各クライアントが、プロバイダ又はプロバイダが指定する代理人によって実施される遵守状況検査に際して、プロ

バイダに協力することを、確保しなければなりません。カスタマーは、クライアントとの間のマネジメント サービスの終了の際、自身のクライアントの電子機材にインストールされている全てのアプライアンス及びソフトウェアを速やかに取り除くか、又は、クライアントに対して当該対応を取ることを要求しなければなりません。カスタマーは、プロバイダに対して、ソフトウェア及びドキュメントの使用に関するクライアントの作為・不作為についてクライアントと連帯して責任を負い、かつ、自身の費用において、カスタマーのマネジメント サービスに関連してクライアントがプロバイダに対して提起した訴訟又は請求についてプロバイダを防御するとともに、当該訴訟又は請求に関連してだされた最終判断又は和解並びにプロバイダが支払った費用を支払うものとします。

(e) **評価/ベータ版ライセンス。**評価を目的にプロバイダからソフトウェアを取得する場合、又はベータ版のソフトウェアを取得する場合、カスタマーは製造を目的としない自社内部での評価のみを目的として当該ソフトウェア及び付随するドキュメントを使用するライセンス (以下「***評価ライセンス***」といいます) を付与されます。各評価ライセンスは、(i) アプライアンスの出荷日の 5 日後、若しくは (ii) ベータ版ソフトウェア又は SaaS ソフトウェアへのアクセスが付与された日から最長 30 日間の評価期間に加えて、プロバイダが書面により付与する延長期間 (以下「評価期間」といいます) の間、付与されます。評価期間中の評価ライセンスについては使用料が発生しませんが、カスタマーは、発送料又は税金、及び本契約において許可される範囲を超える使用についての使用料を負担します。本契約に基づきライセンス供与されるベータ版ソフトウェアには、SonicWall が一般提供するソフトウェアの商用版では提供されていない、リリース前の機能が含まれている場合があります。SonicWall は、評価ライセンスの期間中に SonicWall ベータ版ソフトウェアを変更、改訂、又はカスタマーの施設内から削除する権利を保有します。カスタマーは、ベータ版ソフトウェアに対するすべての修正、二次的著作物、変更、拡張、又は改良、並びにベータ版ソフトウェアの使用に関連して全部若しくは一部が行われた、すべてのレポート、テスト データ又は結果、フィードバック、ベンチマークなどの解析結果が SonicWall に帰属することに同意します。本契約における矛盾する規定の有無にかかわらず、評価ソフトウェア及びベータ版ソフトウェアがすべての不具合を含めて「現状のまま」提供され、SonicWALL が評価又はベータ版ライセンスについて保証又は保守サービスを提供せず、SonicWALL が評価期間中及び評価期間終了後における評価ソフトウェア又はベータ版ソフトウェアの使用 (あるいは使用の試み) に起因するいかなる直接的、間接的、偶発的、懲罰的、特別又は結果的な損害に対しても一切責任を負わず、かかるソフトウェアについてカスタマーにサポートを提供する義務を負わないことを、カスタマーは理解して同意します。ベータ版ソフトウェアには欠陥が含まれている場合があり、ベータ版ソフトウェアをライセンス供与する主たる目的は、ベータ版ソフトウェアの性能に関するフィードバックを得ることと、欠陥を検出することにあります。カスタマーは、重要なデータを保護し、ベータ版ソフトウェア及び付随する資料を注意して使用し、正しい機能と性能を一切期待しないことが推奨されます。

(f) **第三者による使用。**カスタマーは、自身のサービス ベンダー及び請負業者 (以下、それぞれを「第三者ユーザ」といいます) に対し、カスタマーにサービスを提供するためにのみ、本契約においてカスタマーに提供された本製品及びドキュメントのアクセス及び使用を許可することができます。但し、(i) 第三者ユーザによる本製品及びドキュメントのアクセス又は使用が、本契約 (本契約の「輸出」のセクションを含むがそれに限定されません) の制約及び制限を受けること、(ii) 第三者ユーザが、プロバイダ又はプロバイダが指定する代理人によって実施される遵守状況検査に際して、プロバイダに協力すること、且つ (iii) 第三者ユーザが、本セクションに基づいて許可された本製品のアクセス又は使用の必要性が終了した際に自身の電子機材にインストールされたすべてのソフトウェアを速やかに取り除くことを、カスタマーが確保することを条件とします。カスタマーは、自身の第三者ユーザによる当該作為又は不作為が本契約の違反となる場合、それがカスタマーによるものか否かにかかわらず、プロバイダに対して責任を負うことに同意します。

3.制限事項。カスタマーは、ソフトウェア又はその一部をリバース・エンジニアリング、デコンパイル、逆アセンブルしたり、その基本となるソース コードをいかなる方法によっても解析し若しくは変更しようと試みたりしてはなりません。但し、(a) かかる制約が適用法令によって禁止されており、且つ (b) カスタマーが相互運用性情報を書面でプロバイダに要求済みであるにもかかわらず、プロバイダが適時に当該情報を提供していない場合はその限りではありません。更にカスタマーは、(i) 本製品、ドキュメント又はその一部を変更、翻訳、ローカライズ、適合、賃貸、リース、貸与し、二次著作物を製作若しくは作成し、又はこれに基づく特許を作成すること、(ii) 本製品若しくはドキュメントを再販売、サブライセンス供与、又は流通させること、(iii) 本製品の全部若しくは一部を提供し、利用可能にし、又は使用を許可すること (本契約に明示的に記載する場合を除きます)、(iv) 安値での提供を定め若しくは促進し又はその他プロバイダと競業する目的で本製品又はドキュメントを使用すること、(v) プロバイダの書面による承諾なく、提供されたアプライアンスに搭載されているソフトウェアを当該アプライアンスから取り除き、当該ソフトウェアを他のアプライアンスに搭載すること、又は (vi) その他の作為又は不作為により、本製品又はドキュメントについてプロバイダが有する知的財産権の不正利用又は侵害を引き起こすことを行ってはなりません。カスタマーが本契約に基づき作成するソフトウェア及びドキュメントのコピーにはすべて、そのオリジナル版と同様の所有権、商標、著作権及び権利の制限に関する表示を付すものとします。カスタマーは、本製品が第三者の製品とともに作動することがあることを理解し、カスタマーが当該第三者の製品を使用するライセンスを適切に取得する責任を負うことに同意します。本契約の別段の定めに拘わらず、本契約の条件及び制限は、カスタマーが、本製品に含まれ又は本製品とともに提供されるオープン ソース ソフトウェアについての追加の又は異なる権利を、本製品に付属していたか、若しくは要請に応じてカスタマーに提供された当該オープン ソース ソフトウェアのライセンス条件に従って行使することを、阻止または制限するものではありません。カスタマーは、プロバイダが提供していないライセンス キー又はその他のライセンス アクセス デバイス (「海賊版キー」を含みますが、これに限定されません) を使用してソフトウェアをインストール又はアクセスしてはいけません。

4.所有権。カスタマーは、(i) 本製品が著作権その他の知的財産権に関する法令及び条約により保護されており、(ii) プロバイダ、その関連会社又はそのライセンサーが本製品の著作権及びその他の知的財産権を保有しており、(iii) ソフトウェアがライセンスされているものであり、販売されたものではなく、(iv) 本契約がプロバイダの商標又はサービス マークに関する如何なる権利もカスタマーに付与するものではなく、且つ、(v) プロバイダが黙示的かその他によるかを問わず、本契約において明示的にカスタマーに付与されていないあらゆる権利を留保することを、了解し、これに同意します。

5.権限。プロバイダ、その関連会社又はそのライセンサーは、すべてのソフトウェアの権限を所有します。

6.支払。カスタマーは、プロバイダ (又は、場合により、パートナー) に対し、各オーダー記載の料金 (発送料が発生する場合は、記載された発送料を含みます) を支払うことに合意します。カスタマーは、本製品の納入後速やかに又は更新メンテナンス期間の開始前に支払の請求を受けます。カスタマーは、各請求書の日付から 30 日以内、又はオーダーに記載されたその他の期日 (もしあれば) にプロバイダに対する支払額を全額支払います。プロバイダは、カスタマーがプロバイダに支払うべき金額のうち、誠実な議論の対象とはならず支払期日経過後も未払いである額には、かかる額が支払われるまでの間について月 1.5% の割合 (又は法令により認められる最高利率、いずれか低い方) による遅延利息を課すことができます。

7.租税。プロバイダ又はパートナーからのオーダーに記載される料金には税金が含まれていない場合があります。プロバイダが、本契約に基づき提供する本製品若しくはメンテナンス サービス、又はカスタマーによる本製品若しくはメンテナンス サービスの使用に関連し、売上税、使用税、財産税、付加価値税又はその他の税金を支払う義務を負う場合、かかる税金は、カスタマーに請求され、カスタマーが支払います。本セクションは、プロバイダ又はパートナーの所得に基づく税金には適用されません。

8.終了。

(a) 本契約又は本契約に基づき付与されたライセンスは、(i) プロバイダとカスタマーの相互の書面の合意により、又は (ii) いずれかの当事者 (若しくは第三者ユーザ) が、本契約に違反し、当該違反当事者が、違反の通知を受けた後 30 日以内に、違反をしていない当事者が合理的に満足のいく程度にかかる違反を是正しなかった場合、当該違反をしていない当事者により、終了します。上記の定めに拘わらず、MSP ライセンスについては、カスタマー又はそのクライアントが連続する 12 カ月間で本契約に 2 度違反した場合、違反当事者にかかる違反に対する是正期間は与えられず、プロバイダは違反当事者に対する書面による通知をもって直ちに本契約を終了できます。

(b) 理由の如何に関わらず本契約の終了又はライセンスの満了若しくは終了により、該当するソフトウェアについてカスタマーに付与されたあらゆる権利は直ちに消滅し、カスタマーは直ちに、(i) 該当するソフトウェア及びドキュメントの使用を停止し、(ii) 該当するソフトウェアのコピー、インストール及びインスタンスを、該当するソフトウェアがインストールされたアプライアンス、カスタマーのコンピュータ、及びその

他すべてのデバイスから削除し、該当する全第三者ユーザ及びクライアントにも当該削除を確実に実行させ、(iii) 該当するソフトウェアをドキュメントその他ソフトウェアに付随する書類並びにこれらの複製のすべてと共にプロバイダに返却し、又はこれらを破棄し、(iv) 該当するソフトウェアに関連するメンテナンス サービスの利用を停止し、(v) プロバイダ又は該当するパートナーに対して終了日までに支払うべき金額をすべて支払い、且つ (vi) カスタマー、第三者ユーザ、及びクライアント (適宜該当する場合) が、10 日以内に、本項規定の義務を全て遵守した旨の書面による証明をプロバイダに提出します。

(c) (i) 本契約の終了後、(ii) ライセンスの終了若しくは期間満了後、または、(iii) SaaS 期間の満了後に、実行することを要し、又はその実行が予定される本契約の規定は (本契約の「制限事項」、「支払」、「租税」、「終了」、「存続」、「保証についての免責事項」、「権利の侵害 補償」、「責任の限定」、「秘密情報」、「遵守状況確認」及び「一般条項」の各セクションを含みますが、これらに限定されません) 、そのような終了又は期間満了に拘わらず、他方当事者並びにその承継人及び譲受人に対して執行することが可能です。本契約又はライセンスの終了は、本契約に定められた制限及び除外規定に服することを条件として、終了当事者又はパートナーが法令に基づいて有するその他の救済手段の行使を妨げないものとします。

9.輸出。カスタマーは、本製品及びメンテナンス サービスがアメリカ合衆国及びその他の関連国の政府機関の輸出規制に関する法令、規則、規制及び国家安全保障管理 (以下「輸出規制」といいます) による制限を受けることを確認するものとし、且つ輸出規制を順守することに同意します。カスタマーはここに、輸出規制に従って本製品及びメンテナンス サービスを使用することに同意し、また輸出規制に違反して本製品、そのコピー、その一部、又はこれらの直接生産品を輸出若しくは再輸出、販売、リース若しくはその他移転しないものとします。カスタマーは、輸出、再輸出、販売、リース又は移転に関連して必要な許認可の一切を取得すること、及びかかる許認可要件を確実に順守することについて単独で責任を負います。カスタマーは、(i) カスタマー、及びカスタマーが本契約に定められた MSP ライセンスの下でサービスを提供する場合はその各クライアントが、輸出規制により本製品の発送若しくはメンテナンス サービスの提供が禁止されている法人又は個人ではないことを表明し、且つ (ii)(a) アメリカ合衆国の禁輸措置の対象国、(b) アメリカ合衆国の禁輸措置の対象国の国民若しくは居住者、(c) 輸出規制により本製品の発送が禁じられている個人若しくは組織、又は (d) 核物質、核施設、核兵器、ミサイル、化学兵器若しくは生物兵器の設計、開発、生産又は使用に関連する活動に携わる者に対して、本製品を輸出し、再輸出し、その他本製品を譲り渡さないことに同意します。カスタマーは、その経費負担で、プロバイダ及びその関連会社を、カスタマーが輸出許可の存在に関して行った不正確な表明、輸出許可の取得のためのカスタマーによるプロバイダへの情報の不提供、又はカスタマーによる輸出規制の侵害若しくは侵害疑惑を理由としたプロバイダに対する主張 (以下「輸出関連請求」といいます) に起因して生じた第三者の請求若しくは法的行為より防御します。またカスタマーは、輸出関連請求に関連して達した判決若しくは和解の金額及び輸出関連請求に関するプロバイダの費用を支払うものとします。

10.メンテナンス サービス。

(a) **説明。**メンテナンス期間中に、プロバイダは以下のことを行うものとします。

(i) ソフトウェアの新バージョン及び新リリースをメンテナンス サービスの一環として追加料金なく一般に提供する場合、これらをカスタマーに対して提供します。

(ii) これまでカスタマーがプロバイダに報告したことのないソフトウェアの誤作動を報告するカスタマーからの連絡に対応します。前述の規定は、ソフトウェアの誤作動に関するカスタマーからの連絡のフォローアップを限定又は制限すると解釈されないものとします。

(iii) ソフトウェアの誤作動に関するものではないソフトウェアの操作及び技術面についてのカスタマーの技術担当者からの協力要請に応じます。プロバイダは、誤作動に関するものではないかかる協力要請について、その要請内容が極端であり性質上過度に繰り返されるものであるとプロバイダが合理的に判断した場合には、対応を制限することができます。

(iv) https://support.sonicwall.com/ja-jp/ のプロバイダのソフトウェア サポート ウェブサイト (以下「サポートサイト」といいます) にアクセスできるようにします。

(v) 当該ライセンスの購入時から継続してメンテナンス サービスを購入しているカスタマーに対し、ソフトウェアが提供されているアプライアンスのサポートサイトに記載されている修理及び返品プログラムを提供します。

メンテナンス サービスは、サポートサイトに記載された地域的な営業サポート対応時間 (以下「営業時間」といいます) に提供されます。但し、カスタマーが 24x7 サポートを購入している場合は、その限りではありません。24x7 サポートが提供可能又は必要なソフトウェアは、サポートサイト上のグローバル サポート ガイドに列挙のとおりとします。

プロバイダが買収又は合併により取得したソフトウェアのメンテナンス サービスについては、当該買収又は合併の効力発生日から一定期間、本セクションに定める条件とは異なる条件が適用される場合があります。異なる条件は (もしあれば)、サポートサイトに掲示されます。

(b) **メンテナンス期間。**カスタマーがメンテナンス サービスを受けることのできる最初の期間は、プロバイダの登録ポータルに本製品を登録した日 (以下「**登録**」といいます) より開始し、その 12 カ月後に終了します (以下「***初年度メンテナンス期間***」といいます)。初年度メンテナンス期間の後、本製品のメンテナンス サービスをさらに 12 カ月以上の期間更新することができます (以下、それぞれを「更新メンテナンス期間」といいます) 。本契約において、初年度メンテナンス期間及び各更新メンテナンス期間は、「メンテナンス期間」とみなされます。疑義を避けるために付言すると、本契約は各更新メンテナンス期間に適用されるものとします。メンテナンス サービスをキャンセルしても、カスタマーが本製品をその他の方法で継続使用する権利は終了しません。メンテナンス料は、各更新メンテナンス期間の事前に支払い義務が発生し、本契約に定められた支払条件により支払われるものとします。本製品のメンテナンス サービスが終了した後にこれを復活させる手続きは https://support.sonicwall.com/ja-jp/essentials/support-guide に記載のとおりとします。メンテナンス サービスはオプションであり、別途購入された場合に限り提供されます。

SaaS ソフトウェアの場合、メンテナンス期間は、該当する SaaS 期間に相当する期間とします。非永続的なライセンス、又は非永続的な MSP ライセンスの場合、メンテナンス期間は、ライセンスの期間に相当する期間とします。

11.保証及び救済。

(a) ソフトウェアの保証。プロバイダは、適用される保証期間 (下記サブセクション (c) 項に定義します) 中、以下を保証します。

(i) プロバイダが提供したソフトウェアが、そのドキュメントに実質的に従って動作すること (以下「動作保証」といいます)。

(ii) プロバイダが提供したソフトウェアに、ウィルス、ワーム、トロイの木馬、その他プロバイダが設計した不当若しくは破壊的コードで、ソフトウェアへの侵入、停止若しくは消去を可能にするものが含まれないこと。但し、ソフトウェアには、付与されたライセンスの範囲にその使用を制限するキーが含まれている場合があり、また、プロバイダが暫定的使用のために発行したライセンス キーは、時間的制約があります (以下「ウィルス保証」といいます)。

(iii) 商業的に合理的な努力をもって、SaaS ソフトウェアを年中無休で提供すること。ただし、メンテナンス、アップデートのインストール、プロバイダの合理的な制御を超えた要素、プロバイダがカスタマーに伝えた最小システム要件のカスタマーによる不履行、及び SaaS ソフトウェアの利用可能性に影響を及ぼすようなカスタマーによる本契約の違反の場合を除きます (以下「SaaS 利用可能性保証」といいます)。

(b) **アプライアンス保証。**プロバイダは適用される保証期間中、SNWL ソフトウェアをそれぞれドキュメントと実質的に適合して使用できる形でアプライアンスが動作することを保証します (（以下「 アプライアンス保証」といいます)。

(c) **保証期間**。上記の各保証の「***保証期間***」 (ソフトウェア保証を含まない E-class アプライアンスを除きます) は、以下のとおりです。(i) ソフトウェア及びウィルス保証に適用される動作保証については、ソフトウェアの初期登録から 90 日間、(ii) SaaS ソフトウェアに適用される動作保証及び SaaS 利用可能性保証については、SaaS 期間中、並びに (iv) アプライアンス保証については、アプライアンスがプロバイダに登録された日から 1 年間とします。

(d) **救済。**前述の保証に違反があった場合、カスタマーは、該当する保証期間中にプロバイダに報告しなければなりません。かかる違反に関するカスタマーの唯一且つ独占的な救済措置及びプロバイダの唯一の義務は以下のとおりとします。

(i) ソフトウェアの使用に影響を及ぼす動作保証の違反については、プロバイダは、違反を生じさせたソフトウェアの再現可能な誤作動を、当該誤作動の重症度及びそのカスタマーへの影響を考慮した合理的期間内に修正し若しくはその回避方法を提供し、又はプロバイダの選択により、適合しないソフトウェアをカスタマーがプロバイダに返却し、本契約に基づくこれにかかるライセンスの終了の後に、当該不適合ソフトウェアについて支払われたライセンス料を返還します。

(ii) SaaS ソフトウェアの使用に影響を及ぼす動作保証の違反については、プロバイダは、違反を生じさせたソフトウェアの再現可能な誤作動を修正し、又はソフトウェアが該当するドキュメントに実質的に適合して動作しなかった期間に該当する料金を振込み若しくは返還します。

(iii) ウィルス保証の違反については、プロバイダは、ソフトウェアを、ウィルス保証に準拠したコピーと交換します。

(iv) SaaS 利用可能性保証の違反については、プロバイダは、SaaS ソフトウェアが利用できなかった期間について該当する料金を振込み又は返還します。

(e) **保証に関する例外事項。**本セクションに記載する保証は、(i) プロバイダが商業的に合理的な努力をした後にも再現できない不適合、(ii) 該当する本製品の誤用又は本契約若しくはドキュメントに沿わない方法での本製品の使用により生じた不適合、又は (iii) プロバイダ以外の者による本製品の変更により生じた不適合には適用されません。

(f) **第三者製品。**特定のソフトウェアには、第三者製品と相互動作するよう設計された機能が含まれる場合があります。かかる第三者製品が該当する供給元より提供されなくなった場合、プロバイダは、関連する製品機能の製造を中止することがあります。プロバイダは製造中止をカスタマーに通知しますが、カスタマーには、製造中止に伴う返金、払い戻し、又はその他の補償を求める権利はありません。

(g) **保証についての免責事項。**プロバイダが本契約に基づき提供する保証及び救済措置は、本セクションに明示的に定められたものに限られます。適用法令により許容される限りにおいて、その他のあらゆる保証又は救済措置 (明示的か黙示的か、あるいは口頭によるか書面によるかを問いません。商品性、特定目的への適合性、非侵害性若しくは品質についての黙示の保証、その他売買又は取引若しくは履行の過程で生じる保証を含みます) は、適用されません。プロバイダは、本製品が中断なく又は誤作動なく作動することを保証しません。

(h) 高リスクに関する責任の否認。カスタマーは、本製品が耐障害性ではないこと、また高リスク若しくは危険な環境 (核施設の運転、航空機の航行、航空管制、生命維持装置、武器システム、又はその他製品の故障若しくは異常があった場合には死亡、人身傷害、深刻な物的損害若しくは深刻な環境害につながることが合理的に予見されるその他のアプリケーションを含みますが、これらに限定されません) (以下「高リスク環境」といいます) での使用のために設計若しくは意図されたものではないことについて、理解し、同意します。したがって、(I) カスタマーは、高リスク環境において本製品を使用すべきではなく、(II) 高リスク環境においてカスタマーが本製品を使用する場合は、カスタマー自身の危険負担によるものとし、(III) プロバイダ、その関連会社及びサプライヤは、ハイリスク環境での本製品の使用について、カスタマーに対し一切責任を負わないものとし、また、(IV) プロバイダは、高リスク環境での本製品の使用に関して明示若しくは黙示の保証又は確証を行うものではありません。

12.権利の侵害 補償。プロバイダがカスタマーにソフトウェアの使用を許諾した国 (ソフトウェアがカスタマーに納入された国を含みますがこれに限定されません) において有効な特許、著作権、商標、その他の知的財産権をソフトウェアが直接侵害する、又は当該国の営業秘密を不正に使用しているとの申立に基づいて、第三者がカスタマーに対して提起した請求、訴訟又は法的手続き (以下「請求等」といいます) について、プロバイダはカスタマーに補償するものとします。請求等に対する補償は以下を含みます。プロバイダは、(a) 請求等について自己の費用で防御しまたは和解します、(b) 請求等に基づきカスタマーに支払を命じる確定判決又は請求等の和解によりカスタマーが支払義務を負う金額を支払います、(c) 請求等の対応のためにカスタマーが必要的に負担した合理的な手続費用 (合理的な弁護士費用を含みますがこれに限定されません) を返金します。本「権利の侵害 補償」セクションに基づくプロバイダの義務は、カスタマーが (i) 請求等についてプロバイダに速やかに書面により通知し、(ii) 請求等についての調査、防御又は和解についてプロバイダに単独の支配権を認め、且つ (iii) 請求等に関連してプロバイダが合理的に要求するところに従い、プロバイダに協力し、支援することを条件とします。プロバイダは、(a) 本契約において認められていないソフトウェアの使用に起因する請求等、(b) プロバイダ以外の者によるソフトウェアの変更に起因する請求等、(c) 侵害の可能性若しくは実際に侵害があったことを理由としてプロバイダが使用の停止を推奨し、侵害しないバージョンを無償で提供した後にカスタマーがソフトウェアのいずれかのリリースを使用したことに基づく請求等、又は (d) プロバイダが提供していない他の製品、サービス、若しくはデータと併せてソフトウェアを利用したことに起因又は関連する請求等で、かかる利用がなければ侵害を回避できたものについては、カスタマーを防御する本契約上の義務を負いません。請求等又は差止命令の結果、カスタマーがソフトウェアの使用を中止しなければならない場合 (以下「侵害ソフトウェア」といいます)、プロバイダは、その費用及び選択により、(1) 侵害ソフトウェアの利用を継続する権利をカスタマーのために取得すること、(2) 当該侵害ソフトウェアを同一の機能を有する、権利を侵害しないソフトウェアと交換すること、(3) 権利の侵害とならないよう侵害ソフトウェアを変更すること、又は (4) 侵害ソフトウェアのライセンスを終了し、また、(A) SaaS ソフトウェア以外については、侵害ソフトウェアの返品を受け入れ、当該侵害ソフトウェアについて支払われたライセンス料を、かかるソフトウェアの最初の納入日から 60 カ月の期間で案分した額を返還すること、

若しくは (B) SaaS ソフトウェアについては、カスタマーが侵害ソフトウェアにアクセス及びこれを使用する権利を中止し、当該侵害ソフトウェアについてカスタマーが事前に支払ったライセンス料の未使用分を案分した額を返還することの、いずれかを行います。本セクションは、請求等及び侵害ソフトウェアについてのプロバイダの全責任及びその唯一かつ排他的な補償責任を規定するものです。

13.責任の限定。(A) 本契約の「制限事項」若しくは「秘密情報」のセクションの違反、(B) 本契約の「権利の侵害 補償」のセクションに基づきプロバイダ又はカスタマーが第三者に支払うべき判決若しくは和解金、並びに、本契約の「行動」、「輸出」、「MSP ライセンス」及び「第三者による使用」の各セクションに基づきカスタマーがプロバイダに代わってまたはプロバイダに対して支払うべき判決若しくは和解金、又は (C) 適用法令上排除若しくは制限が認められない責任を除いて、カスタマー若しくはその関連会社、又は、プロバイダ、その関連会社若しくはサプライヤは、如何なる場合も (X) 間接損害、付随的損害、特別損害又は派生的損害の一切について、あるいは (Y) 売上損失、現実若しくは予想された利益の喪失、事業の喪失、契約の損失、信用若しくは評判の損失、貯蓄機会の損失、データの損失若しくは破損について、その発生態様に拘わらず、また、かかる損害が予見可能であったか意図されていたかを問わず、また契約違反、不法行為 (過失を含みます)、法律上の義務違反又はその他に基づく責任であるかを問わず、一切責任を負いません。

(A) 本契約の「ソフトウェアのライセンス」、「制限事項」若しくは「 秘密情報」の条項の違反、他方当事者の知的財産権の侵害、(B) 本契約の「権利の侵害 補償」のセクションに基づくプロバイダの明示的な義務並びに本契約の「行動」、「輸出」、「MSP ライセンス」及び「第三者による使用」の各セクションに基づくカスタマーの明示的な義務、(C) プロバイダの滞納金回収のための費用 (誠実な議論の対象となっている滞納金は除きます)、(D) 本契約の「訴訟費用」のセクションに基づく勝訴当事者の訴訟費用、又は (E) 適用法令上排除若しくは制限が許されない責任を除いて、カスタマー及びその関連会社、プロバイダ、その関連会社及びそのサプライヤの本契約に基づく損害に対する責任の総額 (累積的限度額) は、それが契約違反、不法行為 (過失を含みます)、法律上の義務違反又はその他により生じたかに関わらず、(Y) 違反にかかる本製品についてカスタマー若しくはその関連会社が支払った若しくは支払うべき (適宜該当するもの) 金額又は 500 米ドルのいずれか高額な方と同額とします。但し、(Z) 料金の支払が複数回発生するメンテナンス サービス又は製品については、責任の総額 (累積的限度額) は、違反の前 12 カ月間に当

該メンテナンス サービス又は製品について支払われた若しくは支払うべき (適宜該当するもの) 金額又は 500 米ドルのいずれか高額な方とします。両当事者は、上記の責任の限定が、プロバイダのカスタマーに対する本製品及びサービスの提供に関する対価の一部を構成するリスク分配の合意であること、及び上記の責任限定が、限られた救済措置の本質的目的を達成することができない場合でも、また、一当事者が当該責任の発生又は誤作動の可能性について知らされていたとしても、適用されるものであることに合意します。

プロバイダの関連会社及びサプライヤ並びにカスタマーの関連会社は、本「責任の限定」セクションについて、利益を受ける者であり、カスタマーのクライアント及び第三者ユーザは、本契約の「MSP ライセンス」及び「第三者による使用」のセクションに基づき付与される権利を享受するものとし、これら以外で本契約において利益を受ける第三者は存在しません。プロバイダは、カスタマーの第三者ユーザ、クライアント、その他の第三者に対するあらゆる責任を明示的に否定します。

14.秘密情報。

(a) **定義。**「秘密情報」とは、一方当事者 (以下「開示当事者」といいます) が他方当事者 (以下「受領当事者」といいます) に開示する情報又は資料であって、公知のものではなく、またそれらの性質を理由として同様の状況下において合理的な判断をする者が秘密として扱うものをいいます。これには、財務、販売、及び価格に関する情報、営業秘密、ノウハウ、独自開発のツール、知識及び手順、ソフトウェア (ソース コード及びオブジェクト コード形式)、ソフトウェアの機能及び性能に関する情報又は基準試験結果、カスタマーに提供されるソフトウェアのライセンス キー、並びに本契約の条項が含まれますがこれらに限定されません。

秘密情報には、(i) 公知の情報若しくは資料 (但し、カスタマーが本契約を承諾した日 (以下「契約発効日」といいます) 以降の受領当事者による無許可の開示の結果によるものを除きます)、(ii) 受領当事者が開示当事者から受領する前に秘密保持義務を負うことなく取得していた情報若しくは資料、(iii) 受領当事者が、第三者から適法に、当該第三者が合意若しくは誠実義務に違反することなく、取得した情報若しくは資料、(iv) 下記の「保護データ」のセクションに基づいてプロバイダによって保護されている情報、又は (v) 受領当事者が開示当事者の秘密情報を利用若しくは使用することなく独自に開発した情報若しくは資料は含まれないものとします。

(b) **義務。**受領当事者は、(i) 下記のサブセクション (c) 項で認められる場合を除き、開示当事者の秘密情報を第三者に開示せず、且つ (ii) 開示当事者の秘密情報を、自己の類似の情報を保護するのと同程度以上の注意をもって (但し、いかなる場合であっても合理的な注意の程度を下回ってはなりません)、不正使用又は不正開示から保護するものとします。受領当事者は、開示当事者の秘密情報の不正使用又は不正開示を知った場合はその旨速やかに開示当事者に通知し、開示当事者が自己の専有的権利を保護するために第三者に対して提起するあらゆる訴訟において開示当事者に協力します。疑義を避けるために付言すると、本セクションは、契約発効日現在の両当事者の秘密情報の一切の開示に適用され、本契約に基づく各当事者の履行に起因しているか否かを問いません。

(c) 許可された開示。上記の定めに拘わらず、受領当事者は、開示当事者の秘密情報を、開示当事者の事前の書面による同意なく、自身の関連会社、取締役、役員、従業員、コンサルタント、請負業者又は代理人 (以下、総称して「代理人等」といいます) に対し開示することができます。但し、その場合であっても、(i) 本契約の目的遂行、又は本契約に関連する専門的アドバイスの提供のために「知る必要」があり、(ii) 受領当事者に対して、秘密情報のような情報を本契約に定める条件と同程度以上に制限的な条件に従い保護する法的義務を負い、且つ (iii) 受領当事者より、秘密情報の機密性及び本セクションに定める開示と利用に関する制限について通知を受けている代理人等に限ります。受領当事者は、開示当事者に対し、受領当事者が秘密情報を開示した代理人等の作為又は不作為について、当該作為又は不作為が受領当事者自身による場合には本契約の違反となる場合、責任を負うものとします。

更に、受領当事者が、法の適用又は法的手続きの要請に従い、開示当事者の秘密情報を開示する場合、本セクションの違反とはなりません。但し、管轄権を有する裁判所、仲裁廷、その他の法的機関が明示的に禁止する場合を除き、受領当事者が、当該開示について事前に開示当事者に通知することを条件とします。

15.保護データ。本セクションにおいて、「保護データ」とは、本契約中にカスタマーからプロバイダに対して提供された情報のうち、単独またはその他のあらゆる情報と合わさることによって、プライバシー法の下において定義される個人情報に該当すると考えられる、特定の又は特定できる個人に関する情報をいい、「プライバシー法」とは、プライバシー、データ保護、情報保護義務及び保護データの処理に関して適用される法律、法令又は規制をいいます。

本契約で許可されているか、又はプライバシー保護法若しくは法的手続きにおいて必要とされる範囲を除き、プロバイダは、保護データの許容していない第三者に対する開示又は第三者によるアクセスを防止するために合理的な技術的及び組織的な方法を採用することとし、本契約に基づく義務の履行に必要な場合にのみ保護データの保存及び処理を行うこととします。保護データに関するカスタマーによる書面での指示にプロバイダが従う場合、指示に従った結果として生じた本セクションの違反について、プロバイダはカスタマーに対していかなる責任も負わないものとします。プロバイダは、本セクションに違反する第三者への保護データの開示又は第三者による保護データへのアクセスがあった場合は、速やかにカスタマーに通知するものとし、当該開示又はアクセスの影響を合理的に回復するためにカスタマーに協力することとします。プロバイダはカスタマーに対し、欧州連合 (以下「***EU***」といいます) から EU 域外の国への保護データの移転について、EU 標準の契約規定を含む適切な契約を締結していることを確認します。

カスタマーは、(i) プロバイダに対して保護データを提供する権利があることを表明し、(ii) プロバイダが本契約に基づく義務を履行するためだけに世界中で保護データを保存及び使用することを承諾し、(iii) プロバイダの通常営業活動をサポートするために必要な場合において、プロバイダ及びその代理人等が保護データにアクセスし使用することに同意し、また、(iv) メンテナンス サービスの一環として提供されたカスタマーの連絡先情報 (メール アドレス、氏名など) で構成される保護データがプロバイダのサービス向上過程においてプロバイダの外部サービス プロバイダに対して提供される可能性があることに同意します。

16.遵守状況確認。カスタマーは、ソフトウェアのインストール、取得及び使用方法を正確に追跡し、書面化し、且つ報告するためのシステム及び手続きを維持し使用することに同意します。当該システム及び手続きは、カスタマーによるソフトウェアのデプロイメント、又は該当する場合は SaaS ソフトウェアの使用が、当該カスタマーに許可された数量、条件、及びメンテナンス リリースの範囲内であるかを判断できるものでなければなりません。プロバイダ又はその指定された監査代理人は、カスタマーによるソフトウェアのデプロイメント、又は該当する場合は SaaS ソフトウェアの使用が、本契約の条件に従っていることを監査する権利を有するものとします。かかる監査は、その 10 日前までに予定され、カスタマーの施設においてその通常営業時間内に実施されるものとします。カスタマーは、当該監査に対し、全面的な協力及び支援を行い、該当する記録及びコンピュータへのアクセスを提供するものとします。上記の一般性を制限することなく、当該監査の一部として、プロバイダはカスタマーに対し、その時点におけるカスタマーによるソフトウェアのデプロイメント、並びに SaaS ソフトウェアにアクセスして使用した個人の数を示した書面による報告で、権限のある代表者が署名したものの提出を要請することができるものとし、カスタマーは当該報告を提出することに同意します。カスタマーが購入したソフトウェアの権利を超えてかかるソフトウェアをデプロイメントし、又は該当する場合は SaaS ソフトウェアを使用していた場合、カスタマーは、超過するデプロイメントの数量について、当該時点で有効なプロバイダの価格表に基づく代金に、該当するメンテナンス サービス料金及び超過デプロイメント料を追加した金額を請求されます。当該金額は、全額、本契約に従い支払われるものとします。更に、当該未払い額が当該ソフトウェアについて支払われた料金の 5% を超える場合、カスタマーは、プロバイダによる当該監査の実施にかかった合理的費用を負担します。本セクションの要件は、

本契約の適用を受ける最後のライセンスの終了後 2 年間存続するものとします。

17. SaaS 条件。

(a) **データ。**カスタマーは、カスタマーによる SaaS ソフトウェアの使用に関連してアクセスの提供を受けるシステム上にデータを保存することができます (以下「SaaS 環境」といいます)。プロバイダは、定期的にカスタマー データのバックアップ コピーを作成することができますが、かかるバックアップは、カスタマーが定期的にデータ バックアップ又は冗長データのアーカイブを維持する義務に代わることを意図したものでは

ありません。カスタマーは、SaaS 環境に保存されるすべてのカスタマーデータの収集、入力及びアップデートについて、また当該データが (i) 第三者の著作権、営業秘密、商標その他の知的財産権の実際の侵害若しくは悪用又はその可能性のあるものであることを知りながら作成し保存されておらず、 又は (ii) 合理的に考えて反道徳的、抽象的、嫌がらせ的、攻撃的若しくは悪意的であると見られる目的で SaaS 環境を使用しないことについて、単独で責任を負います。プロバイダは、本契約又は本契約に基づき付与された SaaS ソフトウェアのライセンスの終了から 30 日後に、SaaS ソフトウェアの使用に関連して保存されたすべてのカスタマー データを削除する権利を有します。カスタマーは、すべてのカスタマー又は第三者のデータをカスタマー若しくは該当するカスタマー関連会社が所在する国の内外において使用及び移転するために必要なすべての権利、許可及び同意を取得していること (適切な開示内容の提供及びカスタマーの従業員、顧客、代理人及び請負業者からの法的十分な同意の取得を含みます) を表明し、保証します。カスタマーが、SaaS ソフトウェアにリンクされている又はアクセス可能とされている第三者ウェブサイト又はその他のプロバイダにデータを送信する場合、カスタマーは、かかる送信を行うことを可能とする同意をプロバイダに与えているとみなされ、またプロバイダは、かかる送信に関連する第三者の請求についてカスタマーに対する責任を負わないものとします。

(b) **行動。**SaaS ソフトウェアの使用に関連して、カスタマーは、 (i) プロバイダ若しくは第三者のネットワーク若しくは設備への無許可でのアクセスを使用又は獲得の試み、(ii) 他の個人若しくは法人への SaaS ソフトウェアのコピーの許可、(iii) SaaS ソフトウェア若しくは関連するアクセス認証情報への無許可アクセス若しくは使用の提供、(iv) プロバイダ又はプロバイダの顧客若しくはサプライヤの SaaS 環境、システム、アカウント若しくはネットワークの脆弱性の調査、スキャン若しくはテストの試み、(v) ユーザ、ホスト若しくはネットワークへのサービスの妨害又は妨害の試み、(vi) あらゆる性質の詐欺的、攻撃的若しくは違法な活動への関与又は個人若しくは第三者の知的財産権若しくはプライバシー権を侵害する活動への意図的な関与、(vii) 未承諾若しくは商業メッセージの送信、(viii) ワーム、トロイの木馬、ウィルス、破損ファイル若しくは類似のアイテムの意図的な配布、(ix) 意図、目的若しくは知識にかかわらず、他の者が SaaS ソフトウェア (安全性及びセキュリティの機能を備えたツールを除きます) を使用若しくは享受する能力の制限、禁止その他妨害、又は、(x) SaaS 環境を提供するために使用されるプロバイダ (若しくはプロバイダのサプライヤ) の施設にパフォーマンスの制約、禁止、妨害その他阻害若しくは悪化を生じさせることを行ってはいけません。カスタマーは、SaaS 環境の機能停止、安全上の問題及び本セクションの違反のおそれについてのプロバイダによる合理的な調査に協力するものとし、また、その経費負担で、プロバイダ及びその関連会社を、カスタマーによる本セクションの規定の違反により第三者に害が生じていると主張する、当該第三者による請求、訴訟若しくは法的行為 (以下「第三者請求」といいます) より防御するものとします。加えて、カスタマーは、第三者請求に関連して達した判決若しくは和解の金額及びかかる第三者請求に応じるためのプロバイダの費用を支払うものとします。

(c) **使用停止。**プロバイダは、(a) 法執行若しくは法的手続きによりそのように要求された場合、(b) プロバイダ若しくはその顧客に差し迫った安全上のリスクが生じた場合、又は、(c) 継続使用によってプロバイダに重大な責任が生じる場合、カスタマーによる SaaS ソフトウェアの使用を停止することができます。プロバイダは、このような状況においては、商業的に合理的な努力を用いて、かかる使用停止についてカスタマーに事前の通知を行うものとします。

18.一般条項。

(a) **準拠法及び裁判地。**本契約は、抵触法の原則に関わらず、シンガポールの法律に準拠し、これに従って解釈されるものとします。両当事者は、本契約がウィーン売買条約 (国際物品売買契約に関する国際連合条約) の適用を受けないことに合意します。本契約若しくは本契約の規定又は救済処置の執行を求める手続きは、本契約に適用される法律の州及び国の裁判所のみに提起するものとします。本契約の各当事者は、かかる裁判所の管轄権に服することに同意します。

(b) **第三者の権利。**本契約の当事者でない者は、契約 (第三者の権利) 法 (シンガポール共和国法第53B 章) に基づき本契約の規定を執行する権利を有しないものとし、本契約の当事者は、本契約が、第三者の権利を発生させるものではなく、第三者に対し黙示的にも明示的にも権利を付与することを意図していないことを認めます。 本セクションは、セクション 18(a) に従い本契約がシンガポールの法律に準拠する場合にのみ適用されます。

(c) 譲渡。本契約において別途定める場合を除き、カスタマーは、本契約の一部、又は本契約に基づき付与されるライセンス又はその他の権利、利益若しくは義務について、任意、契約、法の運用又は合併 (かかる当事者が存続主体であるか消滅主体であるかを問いません)、株式若しくは資産の売却、整理、解散、政府の行為若しくは命令又はその他によるものであれ、その全部又は一部を、プロバイダの事前の書面による同意なく、譲渡又は移転してはなりません。本契約で許可されていないカスタマーによる譲渡又は移転の試みは、全て無効とします。

(d) **契約の可分性。**本契約のいずれかの規定について、管轄権を有する裁判所が法令に反すると判断した場合、当該規定は法令に反しない限りにおいて執行されるものとし、本契約のその他の規定は依然有効に存続するものとします。上記の定めに拘わらず、保証、救済手段又は損害を制限、放棄又は排除する本契約の規定について、当事者は、これらを独立した規定として意図しており、合意した救済手段が執行不能であっても、これら規定は依然有効とします。当事者は、本契約を締結するにあたって本契約に定められた制限及び排除に依拠しました。

(e) 通知。本契約に基づく全ての通知は書面によるものとし、プロバイダの場合は legal@sonicwall.com 、カスタマーの場合は、プロバイダがカスタマーについて記録するメール アドレス宛てに、電子メールで送付できるものとします。全ての通知、要請、請求又は通信は、本項に従って配送された時点で有効とみなされます。

(f) **カスタマーの開示。**プロバイダは、その顧客リストにカスタマーを加えることができ、またカスタマーからの書面による合意を得た上で、プロバイダのマーケティング活動において、カスタマーがプロバイダを選択した事実を公表することができます。

(g) 権利放棄。 本契約に基づく義務の履行は、他方当事者の権限のある代表者が署名した権利放棄書によってのみ免除され、この権利放棄は、権利放棄書に記載された特定の義務に関してのみ有効とします。本契約のある条項の免除又は不執行があった場合でも、これをもってその他の条項の免除又は別の機会における当該条項の権利放棄をしたものとはみなされません。

(h) **差止による救済。**各当事者は、本契約の重大な違反があった場合 (本契約の「ソフトウェアのライセンス」、「制限事項」又は「秘密情報」の各セクションの違反を含みますが、これらに限定されません)、違反のない当事者が、当該当事者のその他の権利及び救済手段を制限することなく、直ちに差止命令による救済を求めることができることを確認し、これに同意します。

(i) 不可抗力。各当事者は、自己の合理的支配を超える事由 (天災、ストライキ、ロックアウト、暴動、戦争行為、疫病、通信手段の故障、停電を含みますがこれらに限定されません) の結果、自己の責任又は過失によらずに、義務又はサービスの履行を妨げられた期間中、妨げられた範囲において、その履行を免除されます。疑義を避けるために付言すると、不可抗力事由の継続中における本契約に基づく料金の支払債務の猶予は、本契約に基づくカスタマー又はその関連会社の当該料金を支払う契約上の義務を免除するものではありません。

(j) 見出し。本契約の見出しは、便宜上のものであり、本契約の意味又は解釈に影響を与えません。本契約は、当事者の一方に有利にも不利にも解釈されるものではなく、それが公正に意味するところに従い解釈されます。本契約における「含みます」という用語は、「含みますが、これらに限定されません」という趣旨に解釈されます。

(k) 訴訟費用。本契約に基づく権利又は義務を執行するために法的手続きが執られた場合、勝訴当事者は、認められた他の救済措置に加え、その合理的な弁護士費用、裁判費用及びその他の回収費用の補償を受けることができます。

(l) 完全なる合意。本契約は、本契約の対象に関する当事者らの終局的な合意として当事者らにより意図されており、当事者間の従前又は同時期の合意が当事者らによって署名されていない限り、かかる合意の存在により否定されません。かかる合意がない場合、本契約は諸条件を完全に記載した唯一の書面となり、本契約にかかる手続きにおいては本契約に関してこれ以外のいかなる証拠も提出されないものとします。各当事者は、本契約を締結するにあたり、本契約に明示的に定められた以外の記述、表明、確証又は保証 (過失又は無知によるかを問いません) に依拠したことがなく、またこれらに関して何らの権利又は救済も有していないことを認めます。本契約などの契約書の原本 (ファックス、電子コピー、写しでないもの) 又は契約書上の手書きの署名 (電子署名でないもの) が法律又は規制によって要求される管轄地において、かかる法律又

は規制にかかわらず、両当事者はここに、本契約書のファックス、電子コピー、又は写し、及び本契約書上の認定電子署名が、執行可能且つ有効な契約の作成のために十分であることに合意します。本契約は、各当事者の適法な権限のある代表者が署名した書面によってのみ、修正又は変更できます。その他いかなる行為、文書、利用、又は慣習も、本契約を修正又は変更するものとはみなされません。

(m) **各国特有の条件**。本セクションに記載する条件 (以下「**現地国特約**」といいます) は、本製品が最初に納入され、カスタマーによって購入された国に適用されます。現地国特約は、本契約の条件を修正又は補足することができ、当該国で購入された本製品に関連する適用条件において不可欠な部分を形成します。現地国特約が、本契約の他の規定と矛盾する場合は、現地国特約が、本契約に含まれる矛盾する又は異なるいかなる条件にも優先します。

オーストラリア:

1 「**租税**」のセクション – 以下の段落をこのセクションに追加します。「本契約に基づいてプロバイダが製作した課税対象品について、物品サービス税 (以下「GST」といいます) が課される場合、これにかかる GST 税額が対価に追加してプロバイダに支払われます。本セクションにおいて、本契約の他の箇所で定義されていない大文字表記の語句は、1999 年新税制 (物品サービス税) 法 [A New Tax System (Goods and Services Tax) Act 1999 (Cth)] における意味を有します。」

2 「責任の限定」のセクション – 以下の段落をこのセクションに追加します。「本契約の条項は、2010 年競争・消費者法 (Competition and Consumer Act 2010)、又はこれと同等の法令 (以下「本件法」といいます) のいかなる規定も除外、制限、又は変更するものではありません。いずれかの本件法により、ある条件又は保証が黙示的に本契約条件に規定されているとみなされ、且つ当該条件又は保証の適用、行使又はこれに基づく責任を排除又は変更する契約の条項を、本件法が無効とし又は禁止している場合、当該条件又は保証は、本契約条件に含まれるとみなされます。但し、法令により認められる限りにおいて、プロバイダ、その関連会社又はライセンサーの当該条件又は保証の違反に関する責任は、(a) 物品に関する違反である場合は、プロバイダの選択により (i) 物品の交換若しくは同等品の提供、(ii) 物品の修繕、(iii) 物品の交換若しくは同等品の取得にかかる費用の補償、又は (iv) 物品の修繕にかかった費用の補償、又は、(b) サービスに関する違反である場合は、プロバイダの選択により (i) サービスの再提供、若しくは (ii) サービスの再提供を受ける費用の補償に限られます。」

3 「**準拠法及び裁判地**」のセクション -「シンガポールの法律」という文言を「オーストラリア連邦ビクトリア州の法律」に置き換えます。

中国の香港特別行政区とマカオ特別行政区:

1 「**準拠法及び裁判地**」のセクション -「シンガポールの法律」という文言を「中国の香港特別行政区の法律」に置き換えます。

インド

1 「**準拠法及び裁判地**」のセクション -「本契約に適用される法律の州及び国の裁判所のみ」という文言を「シンガポールの高等法院のみ」に置き換えます。

日本

1 「**租税**」のセクション – 2 つめの文を以下のように修正します。「プロバイダが、本契約に基づき提供する本製品若しくはメンテナンス サービス、又はカスタマーによる本製品若しくはメンテナンス サービスの使用に関連し、売上税、使用税、財産税、付加価値税、消費税又はその他の税金を支払う義務を負う場合、かかる税金は、カスタマーに請求され、カスタマーが支払います。」

2 「**メンテナンス サービス**」のセクションを以下のように修正します。

「(a) **説明。**メンテナンス期間中に、プロバイダは、自ら又はパートナーを通して以下のことを行うものとします。

(i) ソフトウェアの新バージョン及び新リリースをメンテナンス サービスの一環として追加料金なく一般に提供する場合、これらをカスタマーに対して提供します。

(ii) これまでカスタマーがプロバイダまたはパートナーに報告したことのないソフトウェアの誤作動を報告するカスタマーからの連絡に対応します。前述の規定は、ソフトウェアの誤作動に関するカスタマーからの連絡のフォローアップを限定又は制限すると解釈されないものとします。

(iii) ソフトウェアの誤作動に関するものではないソフトウェアの操作及び技術面についてのカスタマーの技術担当者からの協力要請に応じます。プロバイダは、誤作動に関するものではないかかる協力要請について、その要請内容が極端であり性質上過度に繰り返されるものであるとプロバイダが合理的に判断した場合には、対応を制限することができます。

(iv) https://support.sonicwall.com/ja-jp/ のプロバイダのソフトウェア サポート ウェブサイト (以下「**サポートサイト**」といいます) にアクセスできるようにします。

(v) 当該ライセンスの購入時から継続してメンテナンス サービスを購入しているカスタマーに対し、ソフトウェアが提供されているアプライアンスのサポートサイトに記載されている修理及び返品プログラムを提供します。

メンテナンス サービスは、サポートサイトに記載された地域的な営業サポート対応時間 (以下「**営業時間**」といいます) に提供されます。但し、カスタマーが 24x7 サポートを購入している場合は、その限りではありません。24x7 サポートが提供可能又は必要なソフトウェアは、サポートサイト上のグローバル サポート ガイドに列挙のとおりとします。

プロバイダが買収又は合併により取得したソフトウェアのメンテナンス サービスについては、当該買収又は合併の効力発生日から一定期間、本セクションに定める条件とは異なる条件が適用される場合があります。異なる条件は (もしあれば)、サポートサイトに掲示されます。

(b) **メンテナンス期間。**カスタマーがメンテナンス サービスを受けることのできる最初の期間は、プロバイダの登録ポータルに本製品を登録した日 (以下「**登録**」といいます) より開始し、その 12 カ月後に終了します (以下「***初年度メンテナンス期間***」といいます)。初年度メンテナンス期間の後、本製品のメンテナンス サービスをさらに 12 カ月以上の期間更新することができます (以下、それぞれを「**更新メンテナンス期間**」といいます)。本契約において、初年度メンテナンス期間及び各更新メンテナンス期間は、「**メンテナンス期間**」とみなされます。疑義を避けるために付言すると、本契約は各更新メンテナンス期間に適用されるものとします。メンテナンス サービスをキャンセルしても、カスタマーが本製品をその他の方法で継続使用する権利は終了しません。メンテナンス料は、各更新メンテナンス期間の事前に支払い義務が発生し、本契約に定められた支払条件により支払われるものとします。本製品のメンテナンス サービスが終了した後にこれを復活させる手続きは https://support.sonicwall.com/ja-jp/essentials/support-guide に記載のとおりとします。メンテナンス サービスはオプションであり、別途購入された場合に限り提供されます。

SaaS ソフトウェアの場合、メンテナンス期間は、該当する SaaS 期間に相当する期間とします。非永続的なライセンス、又は非永続的な MSP ライセンスの場合、メンテナンス期間は、ライセンスの期間に相当する期間とします。

3 「**準拠法及び裁判地**」のセクション - 「シンガポールの法律」という文言を「日本の法律」に置き換え、「本契約に適用される法律の州及び国の裁判所のみ」という文言を「東京地方裁判所のみ」に置き換えます。

4 「**一般条項**」のセクション – 以下のサブセクションを追加します。

言語。本契約は、日本語と英語の双方により作成され、締結されるものとします。英語版と日本語版で解釈に齟齬又は不一致がある場合は、英語版が優先します。

韓国

1 「**準拠法及び裁判地**」のセクション -「シンガポールの法律」という文言を「韓国の法律」に置き換え、「本契約に適用される法律の州及び国の裁判所のみ」という文言を「韓国ソウルにあるソウル中央地方裁判所のみ」に置き換えます。

2 「**一般条項**」のセクション – 以下のサブセクションを追加します。

言語。本契約は、韓国語と英語の双方により作成され、締結されるものとします。英語版と韓国語版で解釈に齟齬又は不一致がある場合は、英語版が優先します。

ニュージーランド:

1 「**保証及び救済**」のセクション – 以下の段落をこのセクションに追加します。「1993 年消費者保証法 (Consumer Guarantee Act 1993) により、ある条件又は保証が黙示的に本契約に規定されているとみなされ、且つ当該条件又は保証の適用、行使又はこれに基づく責任を排除又は変更する契約の条項が無効とされ又は禁止されている場合、当該条件又は保証は、本契約に含まれるとみなされます。」

2 「**責任の限定**」のセクション – 以下の段落をこのセクションに追加します。「カスタマーが 1993 年消費者保証法 (Consumer Guarantee Act 1993) に定義されるところの「消費者」として本契約に基づく物品及びサービスを取得した場合、本セクションにおける制限は 1993 年消費者保証法における制限に服します。」

3 3.「**準拠法及び裁判地**」のセクション -「シンガポールの法律」という文言を「ニュージーランドの法律」に置き換えます。

中華人民共和国 (香港特別行政区、マカオ特別行政区、及び台湾を除く):

1 「**租税**」のセクションを以下で置き換えます。「各当事者は本契約に基づく本製品及びメンテナンス サービスに関連して支払うべき税金を中華人民共和国の該当する租税法に従って負担します。」

2 「**準拠法及び裁判地**」のセクションを以下で置き換えます。

「本契約は、抵触法の原則に関わらず、中華人民共和国の法律に準拠し、これに従って解釈されるものとします。両当事者は、本契約がウィーン売買条約 (国際物品売買契約に関する国際連合条約) 及び UCITA (統一コンピュータ情報取引法) のいずれの適用も受けないことに合意します。本契約により生じ又は本契約に関連するあらゆる紛争は中国国際経済貿易仲裁委員会 (以下「CIETAC」といいます) による仲裁に付され、当該仲裁は仲裁時に有効な CIETAC の仲裁規則に従って実施されます。仲裁は 3 人の仲裁人により構成され、当該 3 人のうち 2 名は各当事者がこれを選任しますが、いずれかの当事者が CIETAC の仲裁規則に定められた期間内に仲裁人を選任できない場合には CIETAC の委員長がこれを選任します。第 3 の仲裁人は両当事者の合意により選任されるものとしますが、両当事者が CIETAC の仲裁規則に定められた期間内に仲裁人を選任できない場合には CIETAC の委員長がこれを選任します。仲裁手続きは北京において、中国語で実施されます。仲裁決定は終局的なものであり、両当事者を拘束します。仲裁費用は、これと異なる旨仲裁において決せられた場合を除いて、敗訴当事者がこれを負担します。

E

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や、トライアル バージョンをお持ちのお客様は、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、https://support.sonicwall.com/ja-jp/ に移動します。

サポート ポータルでは、次のことを実行できます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- ソフトウェアをダウンロードする。
- ビデオ チュートリアルを視聴する。
- ユーザ フォーラムで他のユーザや専門家と交流する。
- ライセンス アシスタンスを受ける。
- MySonicWall 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。
- トレーニングや認定プログラムに登録する。

SonicWall サポートへの連絡方法は、https://support.sonicwall.com/ja-jp/contact-support をご覧ください。

SonicWall エンド ユーザ製品利用規約 (EUPA) については、https://www.sonicwall.com/jp-ja/legal/eupa.aspx を参照してください。お客様の地域に適用される EUPA を表示するには、地理的位置に応じて言語を選択してください。

索引