# YAMAHA VPN クライアント
# YMS-VPN1
# ユーザ マニュアル

2006 年 6 月

本マニュアルでは、YAHAMA VPN クライアント YMS-VPN1 について説明します。YMS-VPN1 は、ヤマハ RT シリーズと Windows PC を、IPsec VPN 通信できるようにするためのユーティリティソフトウェアです。

ヤマハ株式会社
http://netvolante.jp

# 目　　次



# 第 1 章　はじめに

## 1.1. YMS-VPN1 について

YMS-VPN1 は、Windows ワークステーションのネットワーク通信を保護するソフトウェア製品です。IP ( Internet Protocol: インターネット プロトコル ) のトラフィックは、IETF ( Internet Engineering Task Force: インターネット技術標準化委員会 ) の規格に基づく IPsec ( Internet Protocol Security: インターネット プロトコル セキュリティ ) プロトコルを使用して保護されます。

YMS-VPN1 は、単一のユーザワークステーションを対象としたクライアントタイプの IPsec アプリケーションです。企業内ネットワークへのリモート アクセス、リモート管理、ファイル転送、電子メールの送受信 ( SMTP、POP ) 、IP テレフォニなどの重要なネットワーク接続を効果的に保護できます。YMS-VPN1 は、ダイヤルアップを含むすべてのネットワーク接続タイプをサポートしています。

YMS-VPN1 は、単一のワークステーション用に設計されたエンドユーザソフトウェアですが、企業での使用にも容易に対応できます。
YMS-VPN1 が現在対応している Microsoft Windows オペレーティング システムは、Windows 2000、Windows XP、および　Windows Server 2003 です。

YMS-VPN1 はエンドユーザ向けに設計されているために、使い方も簡単です。主な特徴として、直感的なインストールと構成が挙げられます。。YMS-VPN1 は、セキュアで堅牢な製品であり、既存のネットワーク環境に速やかに適応します。

YMS-VPN1 は、多数のカスタマおよびエンドユーザの要求に応じて、商用プラットフォーム向けの本格的な IPsec ソリューションを提供し、強力な認証でネットワークでの全面的な暗号化を可能にします。

## 1.2. 本マニュアルについて

本マニュアルでは、YMS-VPN1 のインストール手順と使用方法について説明します。個人のワークステーションを管理するエンドユーザおよびシステム管理者を対象としています。

本マニュアルの構成は、次のとおりです。

- YMS-VPN1 のインストール
- かんたんポリシーエディタの使い方
- 保守管理

本マニュアルの内容は、使用しているオペレーティング システム ( Windows ) とネットワーク通信の基礎を理解していることを前提にしています。

本マニュアルに含まれない最新の情報については、YMS-VPN1 のリリースノートを参照してください。

## 1.3. IP (**インターネット プロトコル**)

IP は、そのオープン アーキテクチャにより、ローカルおよびグローバル通信にとってパフォーマンス効率、費用効率、および柔軟性に優れたプロトコルです。グローバルインターネットに限らず、大企業の社内ネットワークでも広く採用されています。

IP は、ランダムなネットワークエラーに対して信頼性の高いプロトコルとして設計されています。ただし、悪意ある攻撃に対してはセキュアではありません。実際、いくつかの代表的な攻撃に対しては脆弱であることが知られています。この脆弱性のために、機密性を要求される商用のデータ伝送などには全面的に使用されていません。代表的な攻撃には、次のようなものがあります。

- 盗聴。パスワード、クレジットカード番号、企業秘密などの傍受です。
- 通信の乗っ取りまたはハイジャック。通信当事者間で伝送されているデータを攻撃者が盗み見て改ざんするという方法です。
- ネットワーク アドレスのなりすまし。IP スプーフィングとも呼ばれます。ネットワークアドレスに基づくアクセス制御機構を混乱させるか、接続を偽のサーバにリダイレクトします。

## 1.4. IPsec (Internet Protocol Security: **インターネット プロトコル セキュリティ**)

IETF ( インターネット技術標準化委員会 ) は、IP に対する誤用と攻撃を防止するために IPsec プロトコルスイートを開発しました。IETF は、インターネット関連技術を開発する数百の代表的な企業、大学、および個人の代表から構成される国際規格団体です。IETF の

実績には、IP 自体のほかに、インターネットのバックボーンを形成する他のプロトコルおよび技術の大半が含まれます。

IPsec プロトコルスイートは、基本の IP バージョン 4 プロトコルにセキュリティを追加するものであり、インターネット製品関連のすべての代表的なベンダによりサポートされています。IPsec は、次世代の IP プロトコルである IP バージョン 6 の必須部分です。IPsec プロトコルは、ネットワークレベルで動作します。IPsec プロトコルは、転送される各データパケットに認証と暗号化を追加します。パケットを盗聴と改ざんから保護し、パケットの正しい送信元の認証を行います。

IPsec は、アプリケーション プロトコルとは独立して動作します。したがって、IP プロトコルを使用してデータを転送するすべてのアプリケーションは、平等に、透過的に保護されます。IPsec は、インターネットを通じて機密データを安全に伝送できるようにします。IPsec の採用により、インターネットのビジネス利用を停滞させていた最大の障害が取り除かれます。

ただし、IPsec のみでは、オペレーティングシステムとネットワーク アプリケーションに関連するセキュリティ上の問題を解決できません。IPsec はセキュリティ上の問題に対する一定の保護対策を提供し、より容易に侵入を追跡できるようにします。しかし、オペレーティングシステムとアプリケーションのセキュリティを完全に保護するものではないことを理解しておく必要があります。さらに、IPsec が円滑に動作するには、公開鍵インフラストラクチャが必要です。公開鍵インフラストラクチャは未熟な段階にあり、インターネットでの鍵インフラストラクチャの本格的な使用は始まったばかりです。結論として、セキュリティ ポリシーとアクセス ポリシーの管理は実に複雑な分野であり、手っ取り早い解決策はありません。

ただし、IPsec はインターネットのセキュリティに関して、いくつかの最も重要な問題を確実に解決します。IPsec は、代表的な攻撃の大半を完全に無力化します。そのために、トラフィックの機密性、整合性、および認証という手段を提供します。

# 第 2 章　YMS-VPN1 のインストールと削除

## 2.1. 要件

YMS-VPN1 は、一般的な Microsoft Windows プラットフォームで使用できます。サポートされているプラットフォームは、次の表に示すとおりです。

| プラットフォーム | バージョン | 注記 |
|---|---|---|
| Windows 2000 | SP4 以降 | - |
| Windows XP | SP1 以降 | - |
| Windows Server 2003 | | - |

使用しているコンピュータの Windows バージョンを ( Windows 2000 から XP などに ) 更新する場合は、オペレーティングシステムの更新の前に、YMS-VPN1 を削除し、オペレーティングシステムを更新した後で再インストールしてください。

YMS-VPN1 は、IPsec のクライアントタイプの実装です。一部の Windows プラットフォームはルータとして機能できますが、YMS-VPN1 は IPsec ゲートウェイ ソフトウェアではありません。

YMS-VPN1 のインストールを開始する前に、他の IPsec 実装、ネットワーク スニッファ、NAT アプリケーション、ファイアウォール、またはサードパーティの中間ネットワーク ドライバがインストールされていないことを確認します。YMS-VPN1 は、他のソフトウェアの機能に影響する場合があります。

YMS-VPN1 を実行するために推奨されるパーソナルコンピュータの最小構成は次のとおりです。

| | |
|---|---|
| プロセッサ | Pentium Ⅲ 500 MHz |
| メモリ (RAM) | 256 MB |
| ハードディスク容量 | 30 MB の空きディスク容量 |
| ネットワーク接続 | TCP/IP ネットワーク プロトコル |

YMS-VPN1 をインストールするには、コンピュータのシステムファイルに対する完全なアクセス権が必要です。Windows 2000/XP/Server 2003 では、管理者の権限でログインする

必要があります。

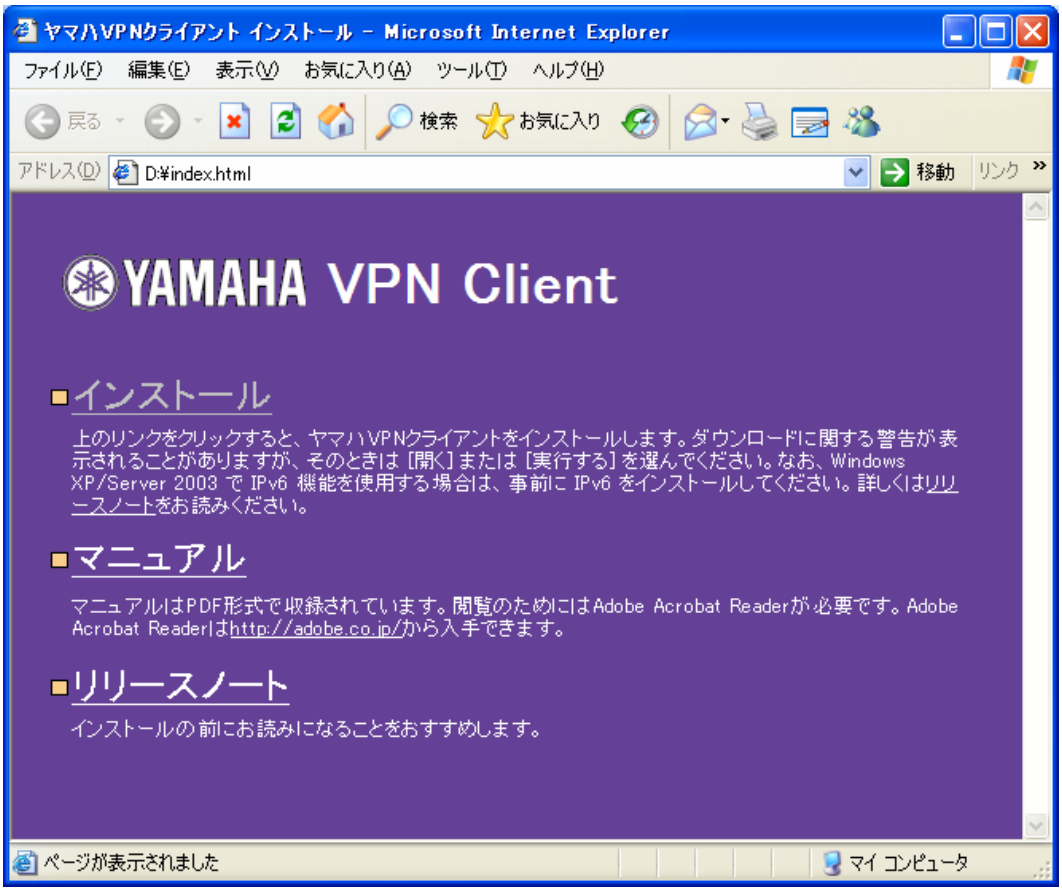
インストールは、ローカル コンピュータでのみ実行できます。YMS-VPN1 のリモートインストールは不可です。インストール プログラムによってネットワークとリモート アクセスに関するカーネル モードのコンポーネントが更新されるためです。

## 2.2. YMS-VPN1 のインストール

YMS-VPN1 をインストールします。以下の手順は Administrator 権限のあるユーザで実行してください。インストールの前にリリースノートをお読みすることをおすすめいたします。

### 2.2.1. インストールの開始

インストールを開始するには、CD を挿入して、以下のウィンドウの「インストール」をクリックするか、



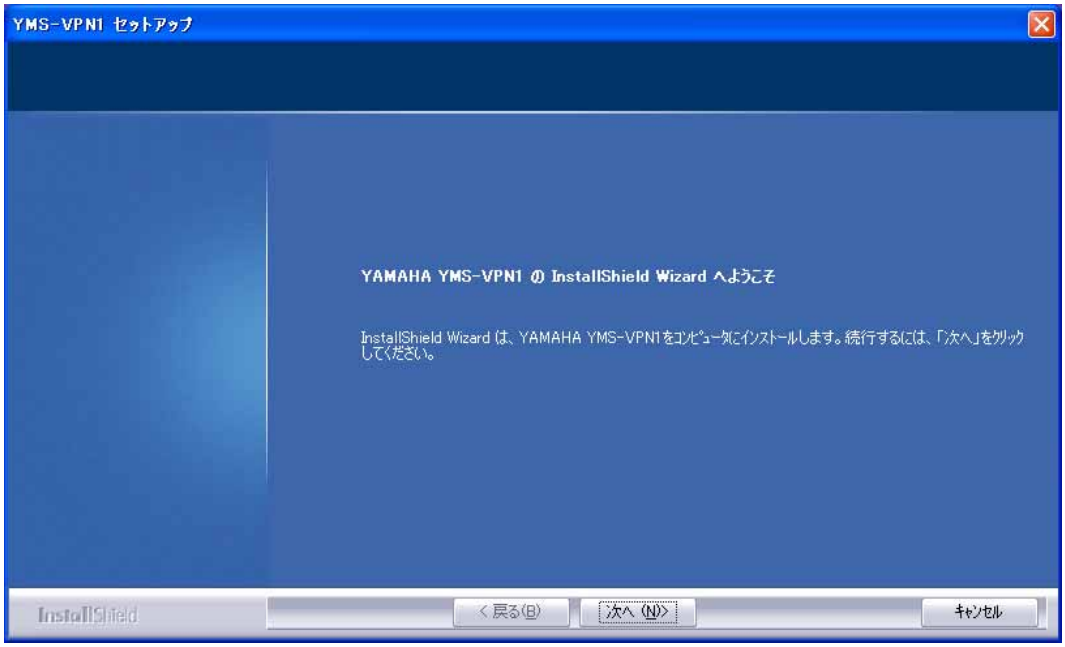
YMS-VPN1 インストールパッケージアイコン(YMS-VPN1.exe) をダブルクリックします。パッケージは、YMS-VPN1 CD または YMS-VPN1 をダウンロードしたディレクトリにあります。


**図 2-1　YMS-VPN1 インストール パッケージ アイコン**

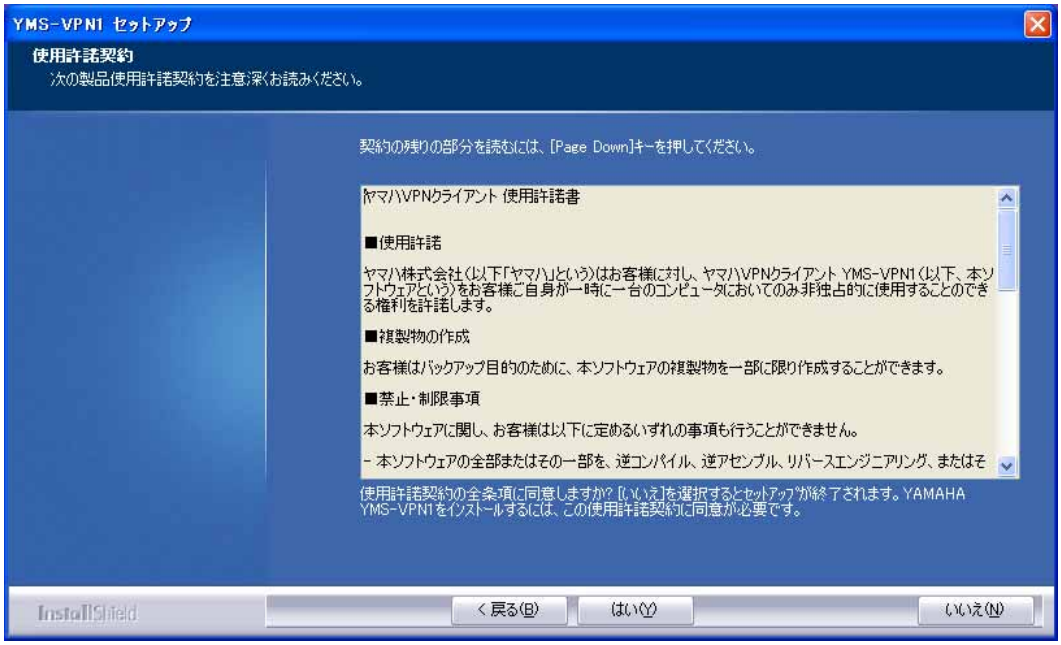
インストーラによってインストール ウィザードが起動し、手順に従ってインストールを進めることができます。

**注記:** コンピュータに以前のバージョンの YMS-VPN1 ソフトウェアがインストールされている場合は、新しいバージョンをインストールしようとすると、ウィザードによってソフトウェアが更新され、ここで説明する手順はスキップされます。「2.3 YMS-VPN1 の更新」の項を参照してください。

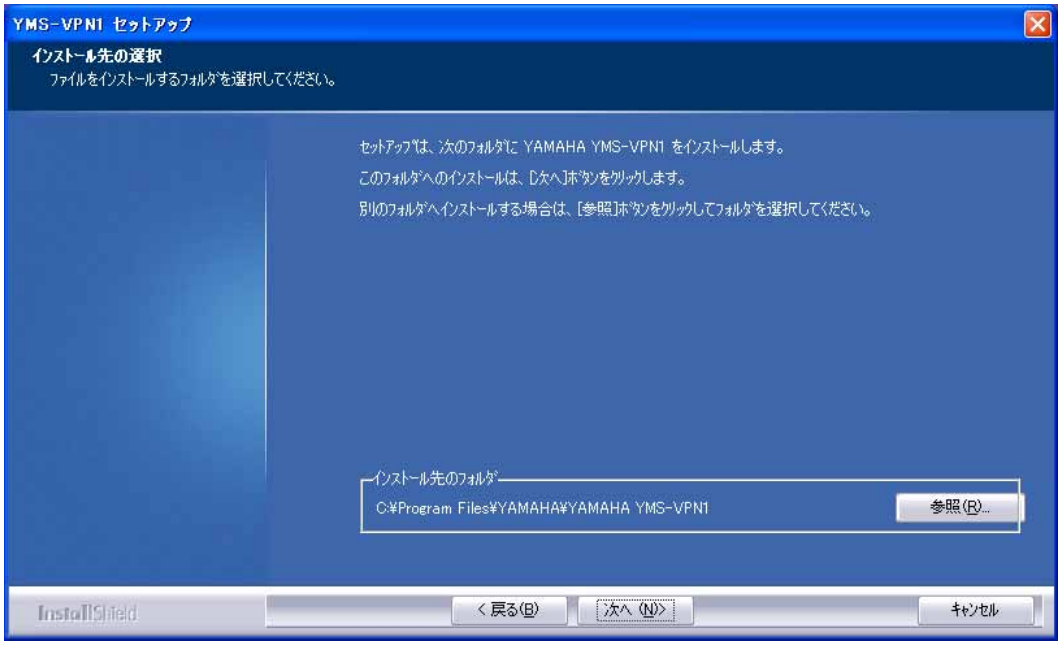
インストール ウィザードを起動すると、セットアップウィンドウが表示されます。



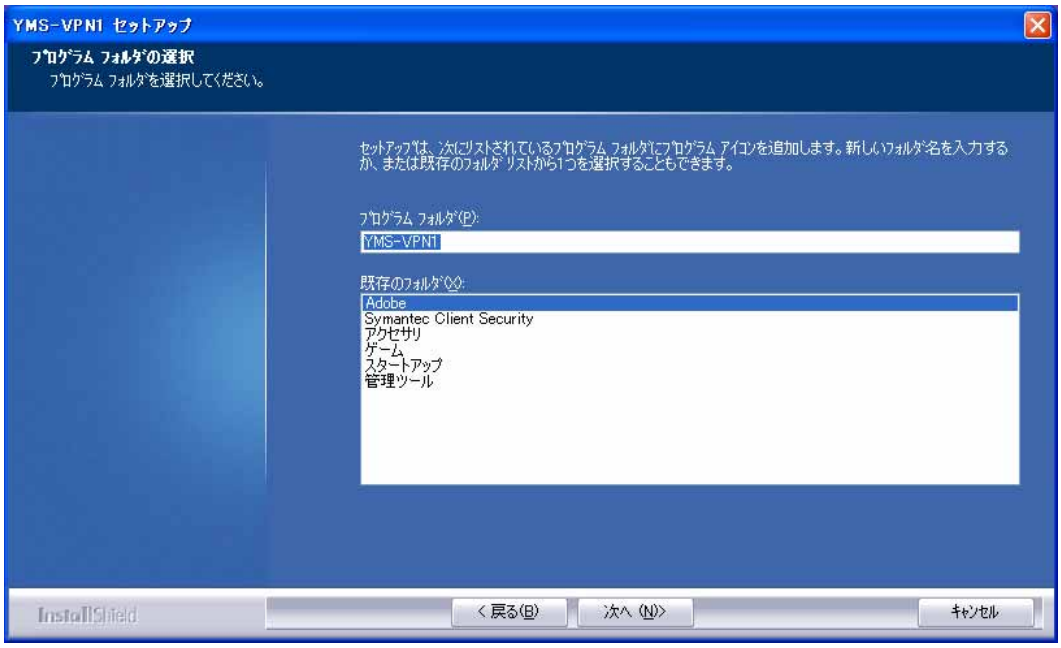

「次へ」をクリックすると、使用許諾契約ウィンドウが表示されます。



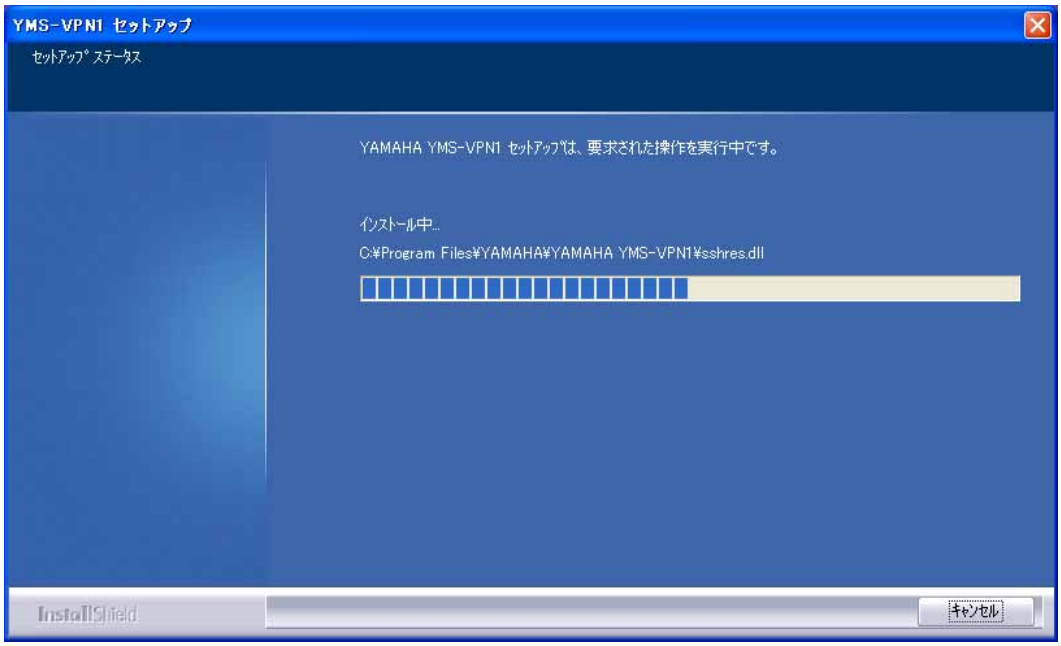

使用許諾契約書に同意しない場合は、インストールが直ちに中止されます。使用許諾契約書を最後まで注意してお読みください。同意される場合、「はい」をクリックすると、インストール先の選択ウィンドウが表示されます。インストール先を変更する場合は、「参照」ボタンをクリックして変更してください。通常は、変更する必要はありません。




「次へ」をクリックするとプログラム フォルダの選択ウィンドウが表示されます。




通常は変更する必要はありませんので、「次へ」ボタンをクリックすると、ファイルのコピーが開始されます。

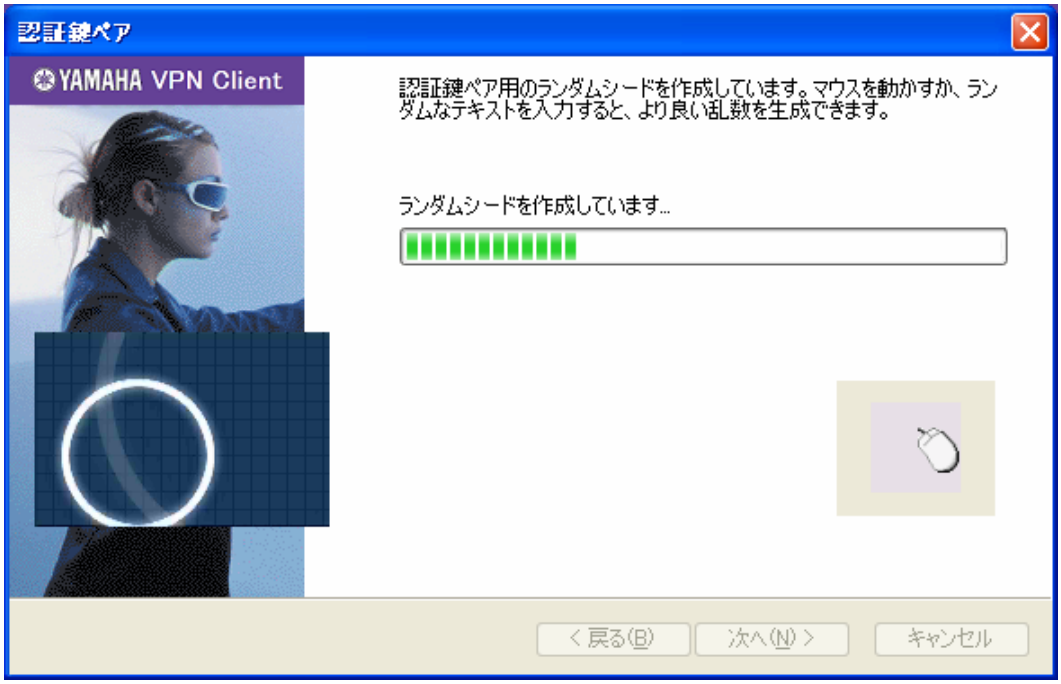


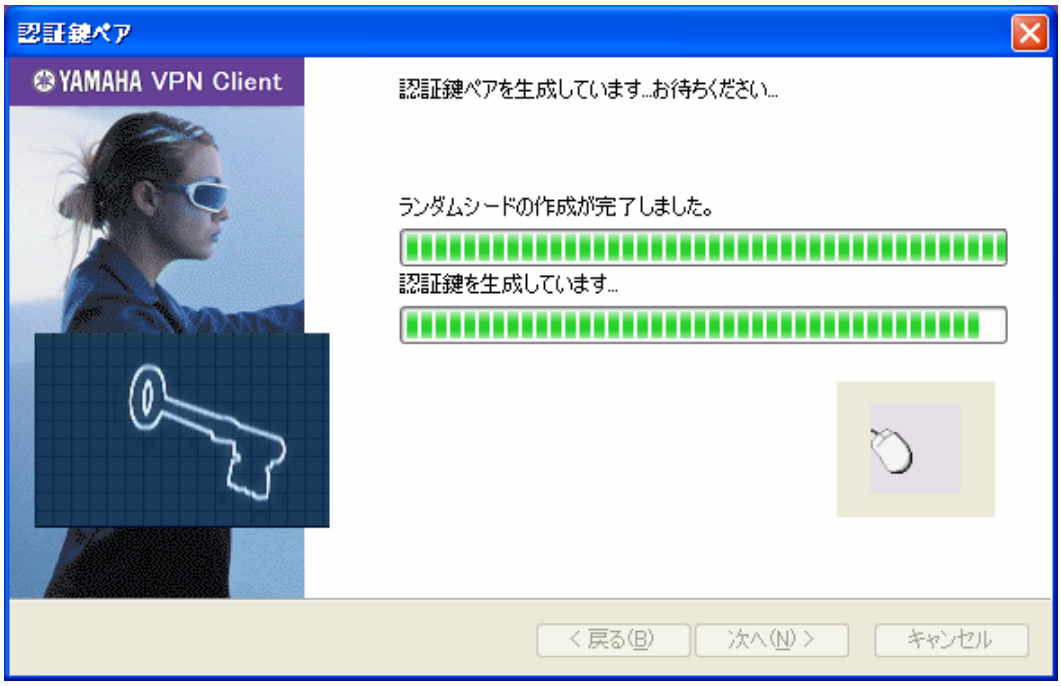
### 2.2.2. 認証鍵ペアの生成

YMS-VPN1 インストールウィザードは、認証に使用するプライマリ認証鍵を最初に生成します。プライマリ認証鍵は 1024 ビットの RSA 鍵ペアであり、デジタル署名と強力な認証に使用します。1024 ビットの RSA 認証鍵が提供する一般的なセキュリティ レベルは、軍事レベルに匹敵する強力さです。

認証鍵の生成は、ランダム シードの生成から開始されます。ユーザによるマウスの移動またはランダムなテキストの入力に基づいて、データのランダムなプールが収集されます。（何も操作しない場合には、インストーラが自動で生成します。）次に、データがシードとして使用され、すべての認証鍵が一意になるように作成されます。この方法では、2 つの同じ認証鍵が生成される確率は極めて低くなります。




鍵ペアの生成には約 30 秒かかります。その間、コンピュータの CPU のリソースを一時的にほぼ占有する場合もあります。




### 2.2.3. 識別情報

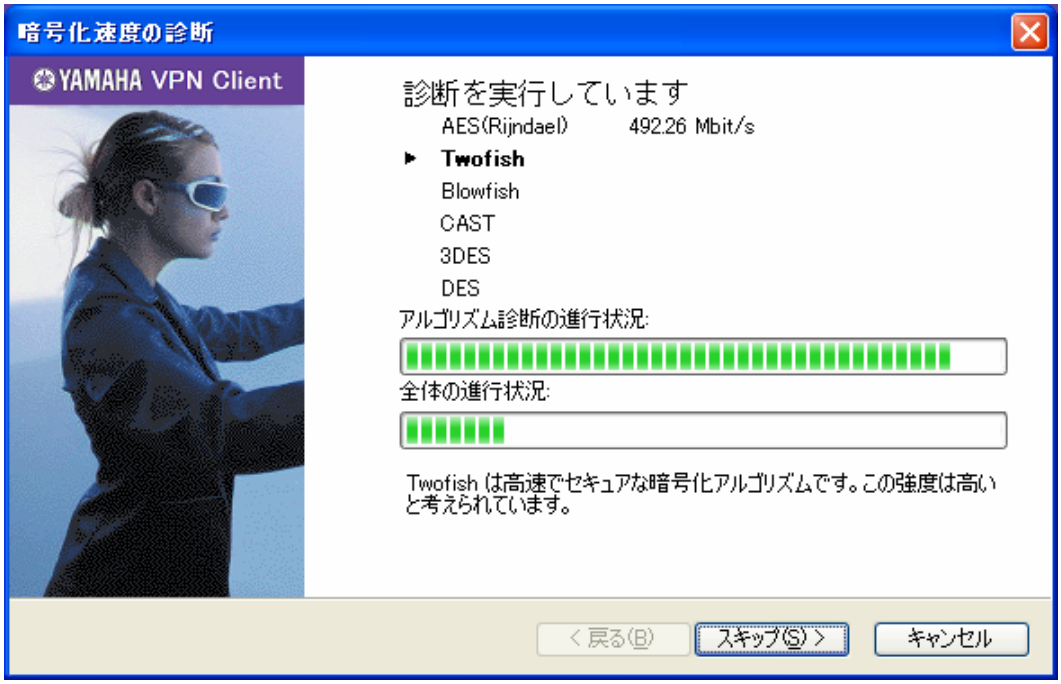
YMS-VPN1 では、証明書とデジタル署名をプライマリ認証方法として使用します。YMS-VPN1 は、IETF の公開鍵インフラストラクチャ X.509v3 の規格に従って証明書を処理し、公開鍵インフラストラクチャ ( PKI ) を利用できるようにします。ただし、スタンドアロンの製品として、YMS-VPN1 を公開鍵インフラストラクチャとは独立して実行することもできます。

認証鍵ペアには ID を関連付ける必要があります。ホストに静的なドメイン名があり、ネーム サービスを確実に使用できると判断できる場合は、ホストのドメイン名を ID として使用します。ドメイン名は FQDN (Fully Qualified Domain Name: 完全修飾ドメイン名) とも呼ばれます。ドメイン名を使用できない場合は、ホストの静的 IP アドレスを ID として使用します。ドメイン名も IP アドレスも使用できない場合は、電子メール アドレスを使用できます。ただし、通常、IPsec 規則は静的なドメイン名または IP アドレスに結び付けられるため、リモートホストとの IPsec で保護された接続を確立する際に障害が発生する可能性があります。

本バージョンでは、この処理は、インストーラによって自動的に処理されます。この処理のために、インストーラはいくつかのウィンドウを表示します。

### 2.2.4. 暗号化速度の診断

YMS-VPN1 は、インストールの最後の手順として暗号化アルゴリズムの診断を実行します。本バージョンでは、すべての診断を実行し、自動で次のステップに進みます。この手順を省略するには、ダイアログ ボックスの [ スキップ ] ボタンをクリックしてください。（省略しても、インストーラの動作には影響ありません。）




診断では、各暗号化アルゴリズムの速度の比較結果が表示されます。YMS-VPN1 は、暗号化アルゴリズムとして AES 、Twofish 、Blowfish 、CAST 、3DES 、および DES をサポートしています。DES 以外のすべてが商用としてセキュアなアルゴリズムであると考えられています。DES 暗号化アルゴリズムは、相互運用性の理由からフォールバック オプションとしてサポートされています。AES は、一般に高速、セキュア、および高信頼性のアルゴリズムと考えられており、YMS-VPN1 のデフォルトの暗号化アルゴリズムになっています。

診断では、アルゴリズムを実行するコンピュータの相対速度も表示されます。暗号化速度に関しては矛盾する情報が少なくありません。診断結果は、ユーザ独自の判断に従って利用できます。

診断では、コンピュータのメモリ内での暗号化速度が測定されます。データパケットはネ

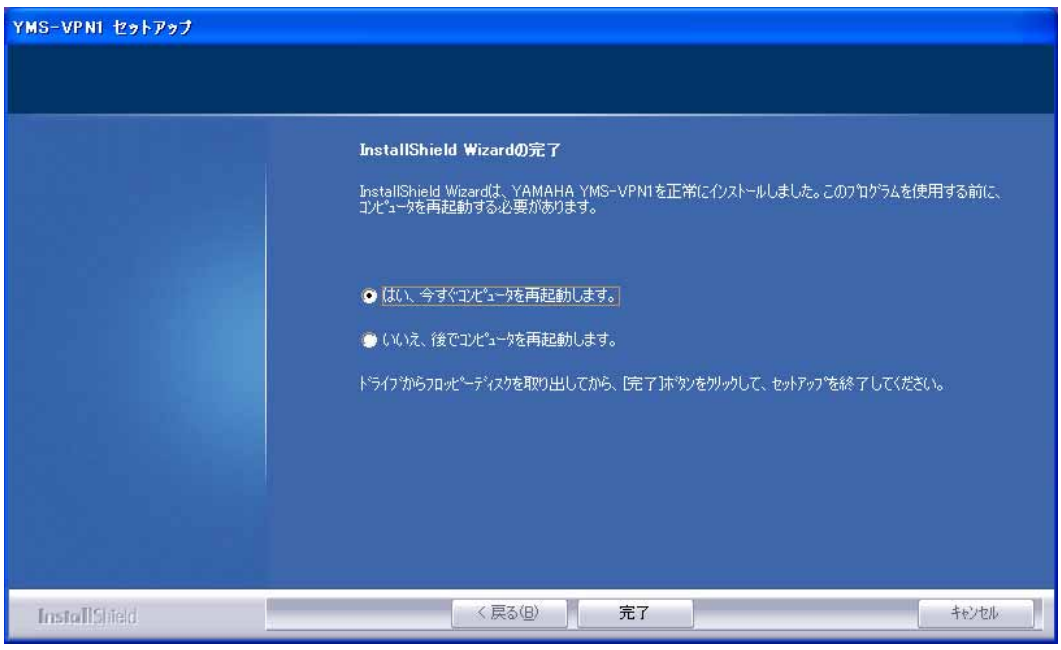
ットワークに転送されません。これは暗号化ハードウェアのベンダ間で一般に使用されているパフォーマンスの測定方法です。この方法では、速度を単純な数値として取得できます。最終結果にはさまざまな要素が影響を及ぼすため、ネットワーク全体のスループットを測定するための、信頼性の高い標準環境を定義することはきわめて困難です。それ以前の問題として、インストール後に再起動するまではカーネル モードの IPsec エンジンを使用できないため、インストール中に実際のネットワークのスループットを測定することができません。

通常、800 MHz のインテル Pentium Ⅲ プロセッサを搭載したパーソナルコンピュータを使用すると、最適な暗号化アルゴリズムで 40 Mbit/s 以上の最大 IPsec スループットを得られます。ただし、オペレーティングシステム、ネットワーク帯域幅、CPU 負荷などの他の可変要素により、スループットは制限されます。

診断が終わると、インストーラは自動で次のステップに進みます。

### 2.2.5. インストールの完了

YMS-VPN1 ソフトウェアをインストールすると、カーネル モードのコンポーネントがオペレーティングシステムのネットワーク管理に追加されるため、YMS-VPN1 を使用する前にコンピュータを再起動する必要があります。



「はい、今すぐコンピュータを再起動します。」を選択して「完了」ボタンをクリックしてください。コンピュータが再起動されます。

## 2.3. YMS-VPN1 の更新

コンピュータに以前のバージョンの YMS-VPN1 ソフトウェアがある場合、インストールパッケージを起動すると、YMS-VPN1 は自動的に更新されます。ポリシー、規則、認証鍵などのコンテンツは保持されます。ソフトウェアのバージョンのみが更新されます。

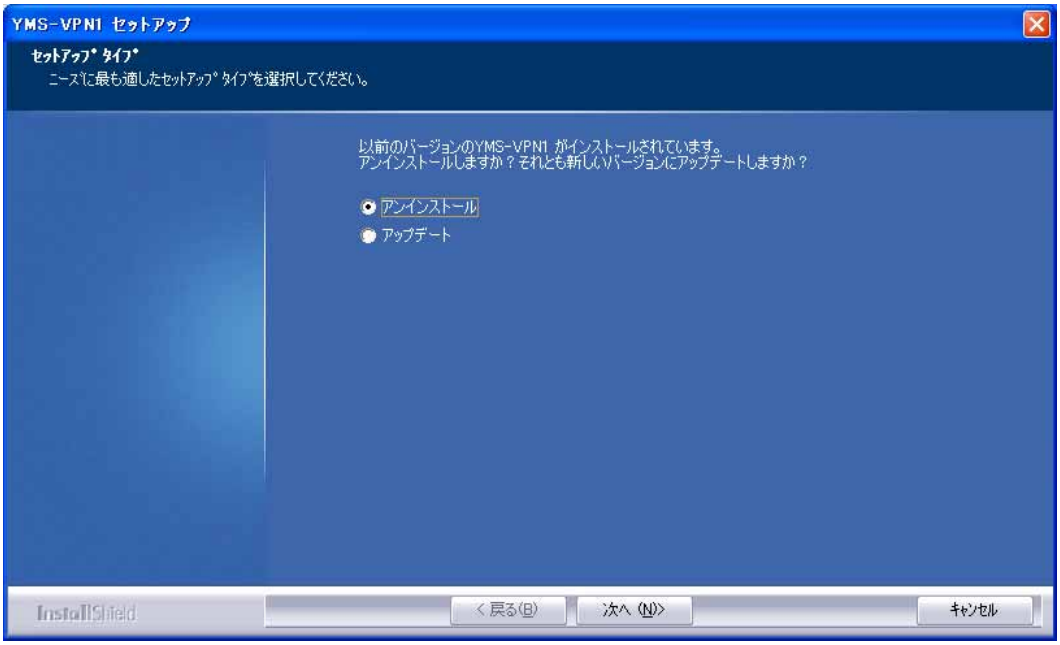
## 2.4. YMS-VPN1 の削除

YMS-VPN1 を削除する前に、次の操作を実行します。

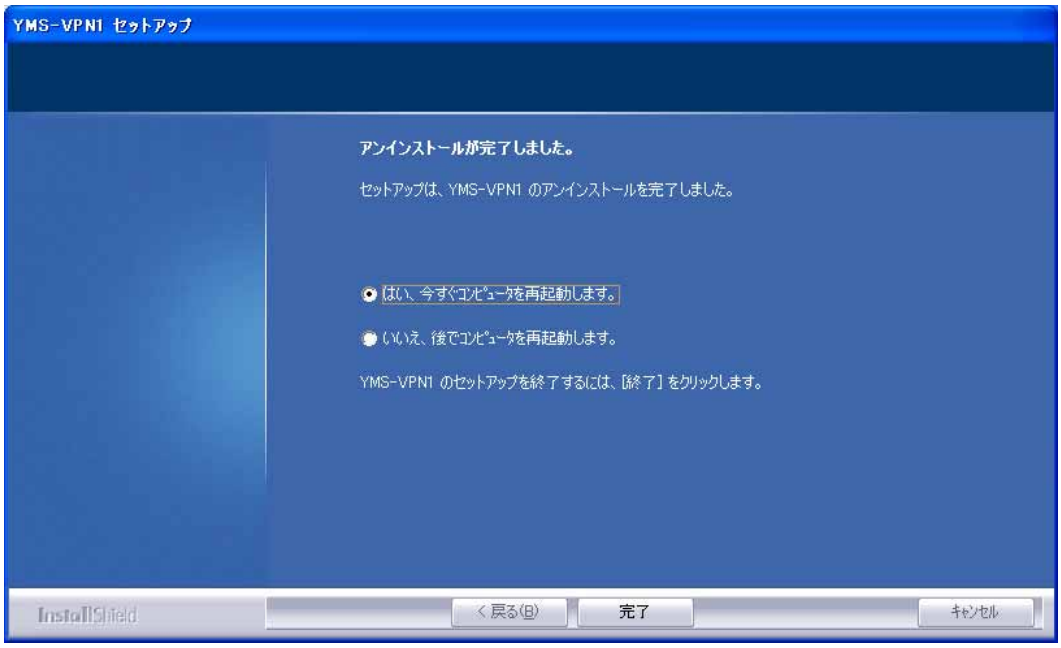
1. YMS-VPN1 の必要なデータをエクスポートして保存します。たとえば、信頼されたルート証明書を将来使用する場合は、これを保存します。YMS-VPN1 を削除すると、関連するすべてのファイルが削除されるので、データは別のフォルダに保存します。保存したデータは、再インストール後に YMS-VPN1 にインポートできます。
2. 安全策として、他のアプリケーションの保存されていないデータもすべて保存し、すべての開いているアプリケーションを終了します。

YMS-VPN1 を削除するには、Windows の標準の削除手順に従います。[ スタート ] メニューの[ 設定 ] をポイントし、[ コントロールパネル ] の [ アプリケーションの追加と削除 ] を開きます。リストから[ ヤマハ VPN クライアント YMS-VPN1 ] を選択します。


「変更と削除」ボタンをクリックします。




「アンインストール」を選択し、「次へ」ボタンをクリックします。ファイル削除の確認ウィンドウが表示されるので、「OK」をクリックして削除を行います。アンインストールが完了すると以下のウィンドウが表示されます。




削除を完了するためにコンピュータを再起動します。

オペレーティングシステムを更新する場合には、更新を行う前に必ず YMS-VPN1 を削除してください。オペレーティング システムの更新後に YMS-VPN1 を再インストールしてください。

## 2.5. シリアルキー

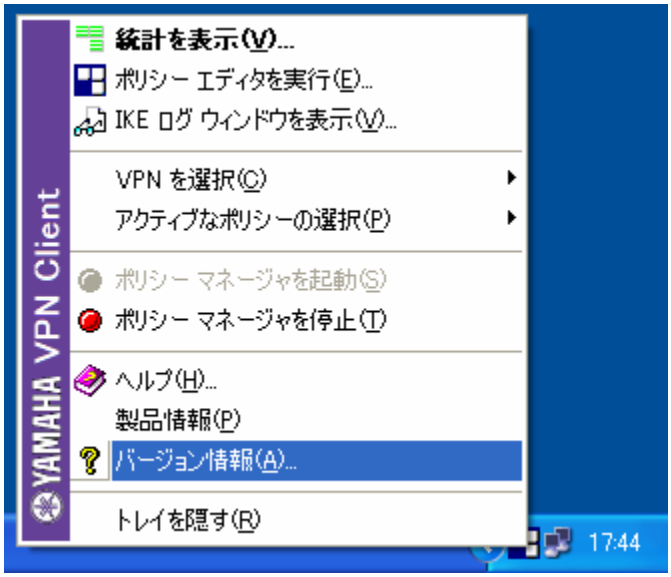
### 2.5.1. シリアルキーの購入

YMS-VPN1 は、シリアルキーをご購入いただかないと、30 日しか使用することができません。シリアルキーは、ヤマハ RT シリーズを購入した代理店からご購入ください。

### 2.5.2. シリアルキーの入力

購入したシリアルキーは、以下の手順で登録します。

タスクトレイの YMS-VPN1 アイコンの上でマウスの右ボタンをクリックし、メニューの「バージョン情報」を選択します。

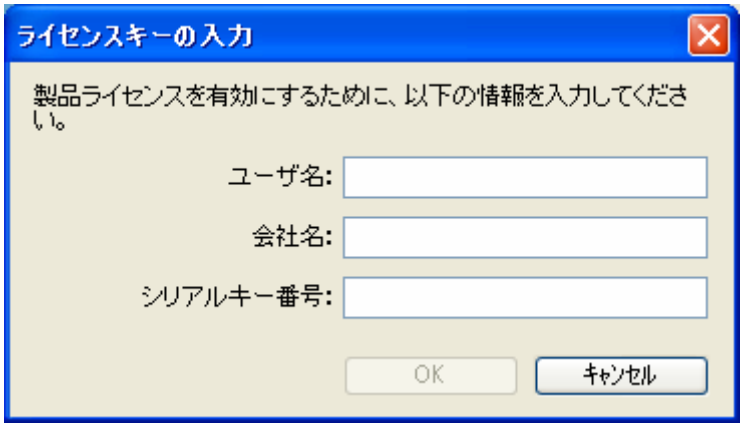



バージョン情報のウィンドウが表示されるので、「ライセンスキーの入力」をクリックします。


ライセンスキーの入力画面が表示されるので、

- ユーザ名
- 会社名
- 購入したシリアルキー

を入力してください。




「OK」ボタンをクリックして終了してください。

# 第 3 章　ポリシー エディタ

## 3.1. YMS-VPN1 ソフトウェアのコンポーネント

YMS-VPN1 ソフトウェアは、主に*ポリシー エディタ*、*ポリシー マネージャ*、および *IPsec エンジン*の 3 つで構成されます。

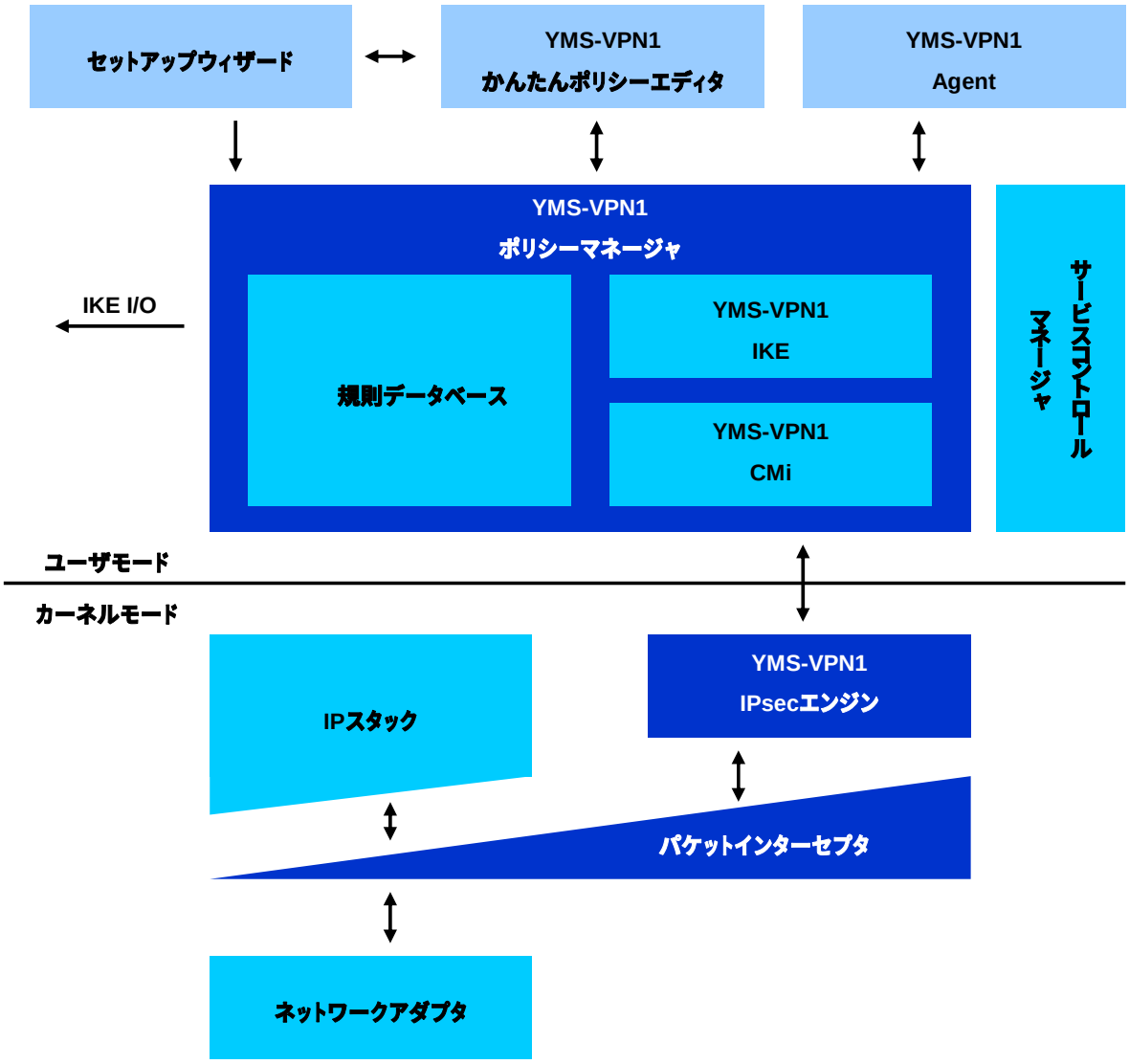



**図 3-1　ソフトウェアの詳細なアーキテクチャ**

セキュリティ ポリシーは、ネットワークからの悪意ある攻撃からホストを保護します。信頼ポリシーは、信頼する相手を規定します。YMS-VPN1 では、セキュリティポリシーは規則群で構成されます。規則に基づいて、送受信される各データパケットへのアクションが

決定されます。セキュリティ ポリシーを構成する規則を設定するには、ポリシー エディタをユーザ インターフェイスとして使用します。また、信頼ポリシーと認証鍵もポリシーエディタを使用して管理します。

規則は、ポリシー マネージャの一部である規則データベースに保存されます。規則を追加、削除、または変更するたびに、規則データベースが更新されます。

データ パケットに対するアクションを実際に決定するのは IPsec エンジンです。エンジンはデータトラフィックを監視し、そのインターセプタによって適切なパケットをトラップしてセキュリティポリシーを適用します。エンジンは、規則データベースのアクティブなポリシーの規則からポリシーマネージャによって作成されたセキュリティポリシーの内部表現を保持します。規則セットを更新するたびに、ポリシー マネージャによって IPsec エンジンの内部表現が再作成されます。

## 3.2. YMS-VPN1 Agent

ポリシーマネージャの実行中は、Windows タスクバーの右側のシステムトレイに YMS-VPN1 アイコンが表示されます。ポリシー マネージャが何らかの理由で無効になっていると、ポリシー規則はネットワークのデータトラフィックに適用されず、アイコンは淡色表示になります。マウスの右ボタンをクリックすると、フローティング メニューが開いて次の項目が表示されます。

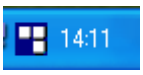



**図 3-2 YMS-VPN1 システムのトレイ アイコン**

**統計を表示**

YMS-VPN1 の統計を表示します。トレイ アイコンをダブルクリックして、この画面を表示することもできます。「4.2 統計」の項を参照してください。

**ポリシー エディタを実行**

かんたんポリシー エディタを開きます。

**IKE ログウィンドウを表示**

IKE ログウィンドウを開きます。トラフィックを監視し、トラブルシューティングを実行できます。詳細については、「4.1 IKE ログ」の項を参照してください。

**アクティブなポリシーの選択**

ホストで使用可能なポリシーのリストから適用するポリシーを選択します。

**VPN 接続の選択**

リストの該当する接続を選択して VPN 接続を開きます。

**ポリシー マネージャを起動**

ポリシー マネージャを有効にします。アクティブなポリシーが適用されます。

**ポリシー マネージャを停止**

ポリシー マネージャを無効にします。ポリシーは適用されません。

**ヘルプ**

YMS-VPN1 のオンライン ヘルプを開きます。

**製品情報**

YMS-VPN1 のサポート Web ページを開きます。

**バージョン情報**

YMS-VPN1 ソフトウェアに関する一般的な情報を表示します。別途購入したシリアルキーの入力を行います。

**トレイを隠す**

トレイアイコンを隠します。トレイアイコンを再表示するには、YMS-VPN1 Agent を

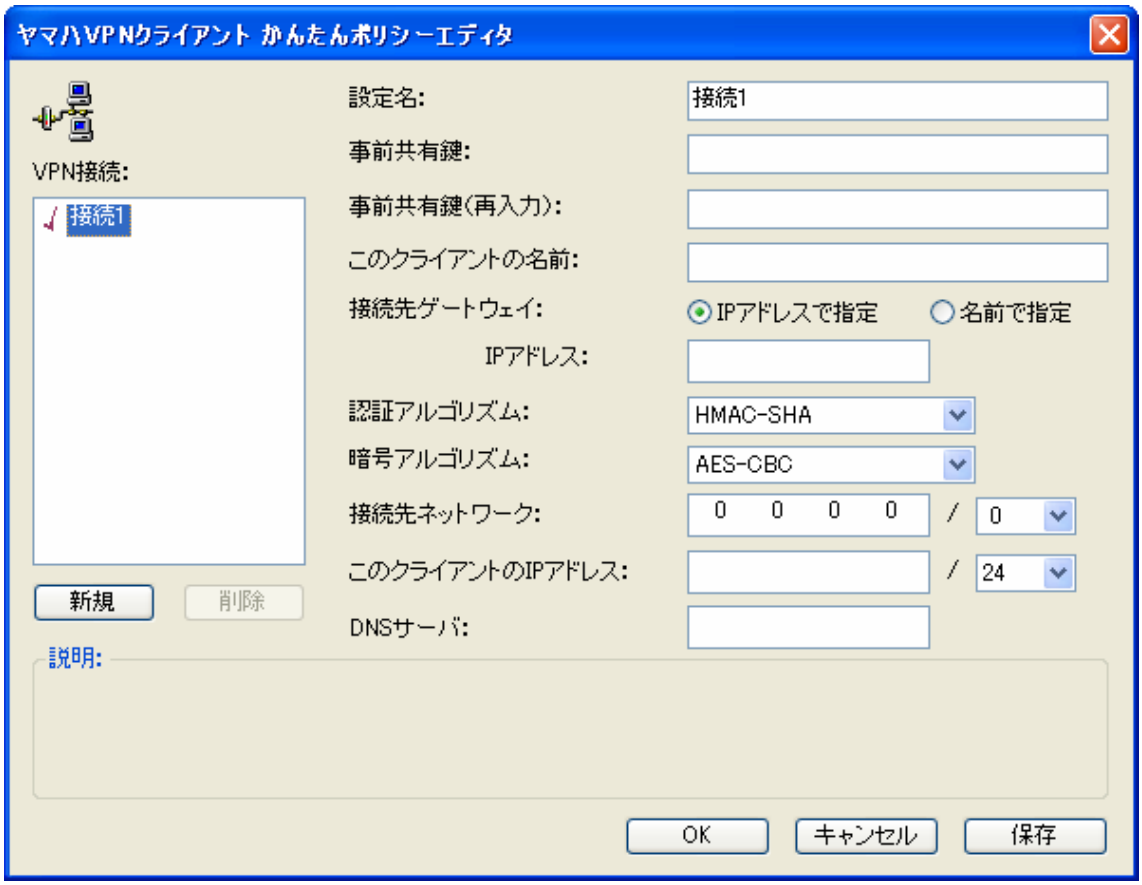
 

YMS-VPN1 フォルダから起動します。アイコンが隠されている場合でも、コンピュータの再起動後に画面に再表示されます。トレイ アイコンを表示しないようにするには、Windows の [ スタート ] メニューの[ スタートアップ ] フォルダから [ YMS-VPN1 Agent ] を削除します。ただし、YMS-VPN1 のメイン フォルダからは YMS-VPN1 Agent を削除しないように注意してください。[ スタートアップ ] フォルダの正確な場所は、Windows のバージョンによって異なります。

## 3.3. かんたんポリシー エディタを開く

かんたんポリシー エディタを開くには、次のいずれかの操作を行います。

- YMS-VPN1 のメイン メニューで[ ポリシー エディタを実行 ] を選択します。
- Windows の [ コントロール パネル ] を開きます。[ YMS-VPN1 ] アイコンをダブルクリックします。または、アイコンをマウスで右クリックし、表示されるメニューで [ 開く ] を選択します。
- Windows の [ スタート ] メニューで [ プログラム ] を開きます。[ YMS-VPN1 ] の [YMS-VPN1 かんたんポリシーエディタ ] を選択します。




## 3.4.　かんたんポリシーエディタの使い方

かんたんポリシーエディタでは、ヤマハ RT シリーズと接続するために必要な項目を設定します。すべての項目を必ず設定してください。設定が終了したら、必ず保存ボタンをクリックして設定を保存してください。

- 設定名
  この設定を認識するための文字列です。最大 32 文字まで入力できます。

- 事前共有鍵
  鍵交換を始める前にお互いを認証するための鍵文字列です。最大 32 文字まで入 力できます。接続先のヤマハルータの"ipsec ike pre-shared-key"コマンドの 設定と一致させてください。
  事前共有鍵は、入力文字が「＊」で表示されるので、事前共有鍵（再入力）のボックスにも同じ文字列を必ず入力してください。

- このクライアントの名前
  このクライアントを特定するための名前をあらわす文字列です。最大 32 文字ま で入力できます。接続先のヤマハルータの"ipsec ike remote name"コマンドの 設定と一致させてください。

- 接続先ゲートウェイ
  「IP アドレスで指定」または「名前で指定」のどちらかを選択します。
  「IP アドレスで指定」を指定した場合には、接続先のヤマハルータの IP アドレスを指定してください
  「名前で指定」を指定した場合には、接続先のヤマハルータの FQDN を指定してください。

- 認証アルゴリズム
  IPsec/ESP で用いる認証アルゴリズムです。接続先のヤマハルータの"ipsec sa policy" コマンドの設定と一致させてください。

- 暗号アルゴリズム
  IPsec/ESP で用いる暗号アルゴリズムです。接続先のヤマハルータの"ipsec sa policy" コマンドの設定と一致させてください。

- 接続先ネットワーク
  接続先ネットワークの IP アドレスとサブネットマスクを指定します。

- このクライアントの IP アドレス
  このクライアントが使用する仮想アダプタの IP アドレスとサブネットマスクを指定します。

- DNS サーバ
  VPN 接続中に利用する DNS サーバを設定します。DNS サーバを使用しない場合は、空欄、または 0.0.0.0 を指定します。

VPN 接続には、保存された設定の一覧が表示されます。編集中の設定には、左側に赤のチェックマークが表示されます。

「保存」ボタンをクリックすると、編集中の設定を保存することができます。設定を修正した場合には、必ず保存ボタンをクリックして設定を保存してください。

「新規」ボタンをクリックすると、新しい設定を作成することができます。作成後は、必ず「保存」ボタンをクリックして設定を保存してください。

保存された設定を選択すると編集することができます。設定を修正した場合には、必ず保存ボタンをクリックして設定を保存してください。

VPN 接続を選択し、「削除」ボタンをクリックすると、選択した設定が削除されます。

# 第 4 章　保守管理

YMS-VPN1 には、インターネット鍵交換 ( IKE ) のネゴシエーションやネットワーク トラフィック全体の統計に関する情報を確認するツールがあります。

## 4.1. IKE ログ

リモート ホストへの接続を確立する際の問題を検出して調査するには、[ YMS-VPN1 IKE ログ ] を使用してインターネット鍵交換 ( IKE ) のネゴシエーションに関する情報を確認します。この情報はファイルに書き込むこともできます。YMS-VPN1 のメイン メニューから [ IKE ログウィンドウを表示 ] を選択します。

表示される情報の量は、選択するログレベルに応じて異なります。

- *[ Off ]* に設定すると、情報はログに記録されません。
- *[ Low ]* レベルでは、ネゴシエーションの成否に関する情報が示されます。ネゴシエーションが成功すると、確立されたパラメータが表示されます。ネゴシエーションが失敗すると、大まかな原因が示されます。
- *[ Moderate ]* レベルでは、ネゴシエーションのより詳細な情報が示されます。通常、このレベルは失敗したネゴシエーションの原因を調べるのに適しています。
- *[ Detailed ]* レベルでは、すべての情報が表示されます。詳細レベルは大量のメッセージを伴うために、通常は使用しません。また、詳細レベルを使用すると、ネゴシエーションが遅くなります。

メッセージをファイルに書き込むには、[ ログファイルに保存 ] オプションを選択し、メッセージを書き込むファイルを選択します。ログファイルに保存中にログ ウィンドウを閉じると、ファイルへのメッセージの書き込みを続行するかどうかを確認するメッセージが表示されます。ログの続行を選択すると、ログをオフに切り替えない限り、ログが継続されます。

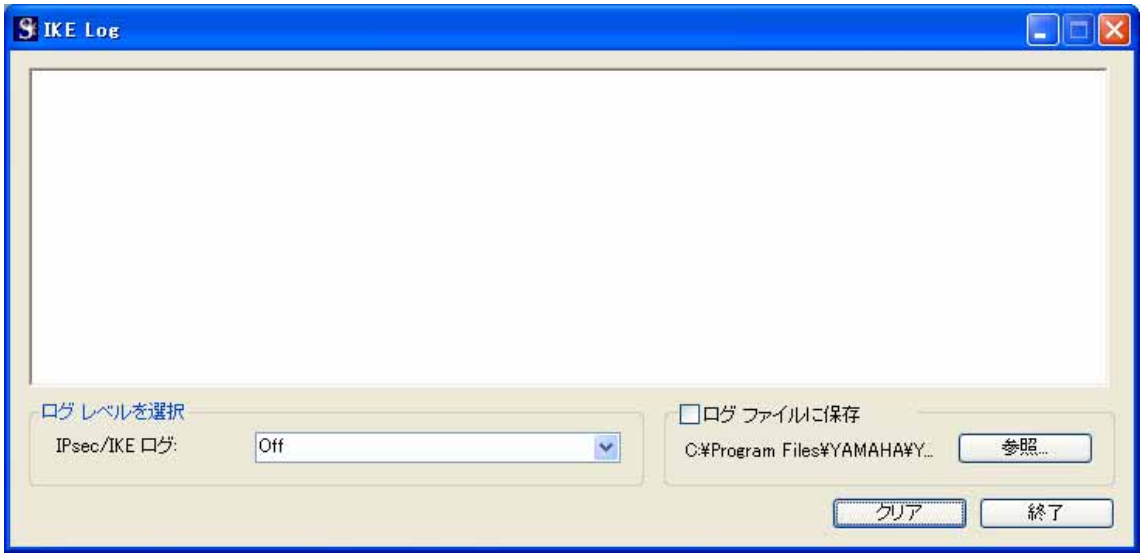



図 4-1 IKE ログウィンドウ

## 4.2. 統計

YMS-VPN1 統計は、ローカル ホストとやり取りされるデータ トラフィックに関する情報を表示します。確立されたセキュリティの関連付け、転送されたデータ パケット、データ トラフィックで検出されたエラーなどを参照できます。

YMS-VPN1 統計を開くには、メイン メニューの [ 統計を表示 ] を選択します。表示されるダイアログ ボックスには、[ セキュリティの関連付け ] と [ IPsec 統計 ] の 2 つのページがあります。

### 4.2.1. セキュリティの関連付け

[ セキュリティの関連付け ] ページには、確立された現在のセキュリティの関連付けが表示されます。

**リモート**

リモート ホストの IP アドレスまたは DNS 名。

**種類**

セキュリティの関連付けの種類として ESP または ESP+IPComp 。

**Kbytes in**

ローカル ホストで受信されたデータの量。

**Kbytes out**

ローカル ホストから送信されたデータの量。

セキュリティの関連付けを解除するには、関連付けを選択して [ 終了 ] ボタンをクリックします。

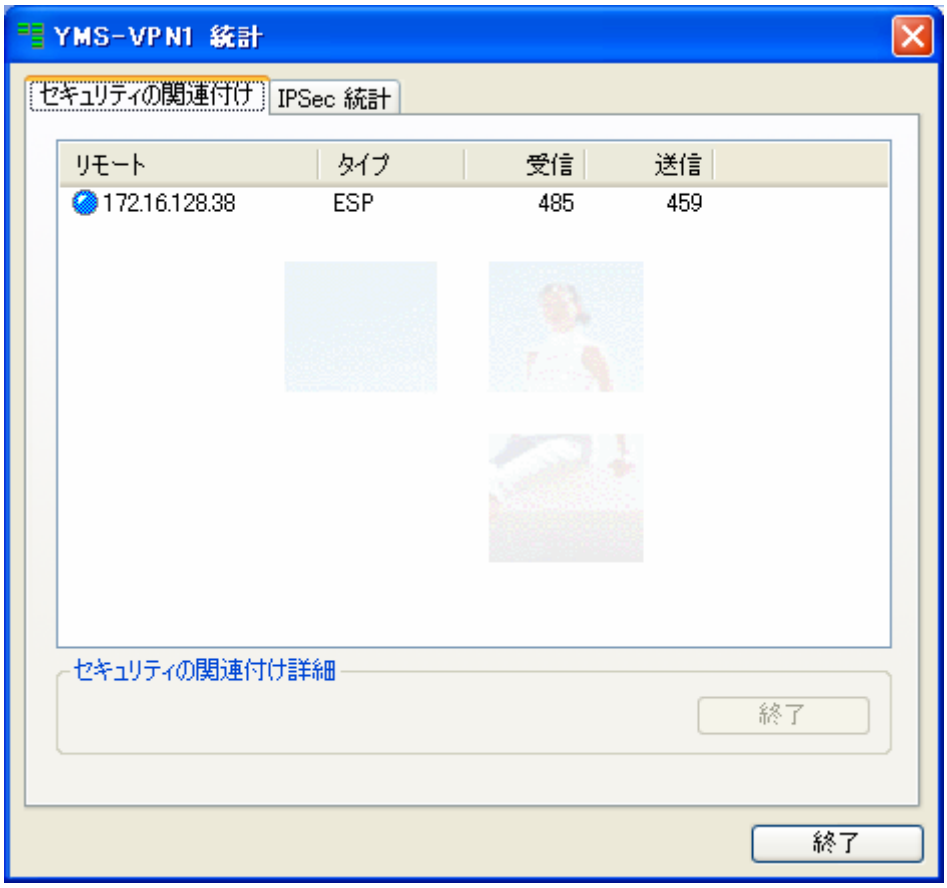



**図 4-2　確立されたセキュリティの関連付け**

確立されたセキュリティの関連付けは、[ 統計 ] ダイアログ ボックスに表示されます。

### 4.2.2. IPsec 統計

[ IPsec 統計 ] ページでは、ローカル ホストのデータ トラフィック全体を監視できます。

**暗号化**

データのスループットが ＫＢ 単位で図示されます。

**ネットワークの使用履歴**

データ トラフィックの履歴が図示されます。プレーン テキスト パケット、暗号化されたパケット、およびドロップされたパケットが区別されます。

**IKE のネゴシエーション**

**IKE Phase-1 の合計**

開始された IKE Phase-1 のネゴシエーションの総数。

**IKE Phase-1 の失敗**

IKE Phase-1 のネゴシエーションの失敗数。

**IKE クイックモードの合計**

クイック モードで開始された IKE のネゴシエーションの総数。

**IKE クイックモードの失敗**

クイック モードで失敗した IKE Phase-1 のネゴシエーションの数。

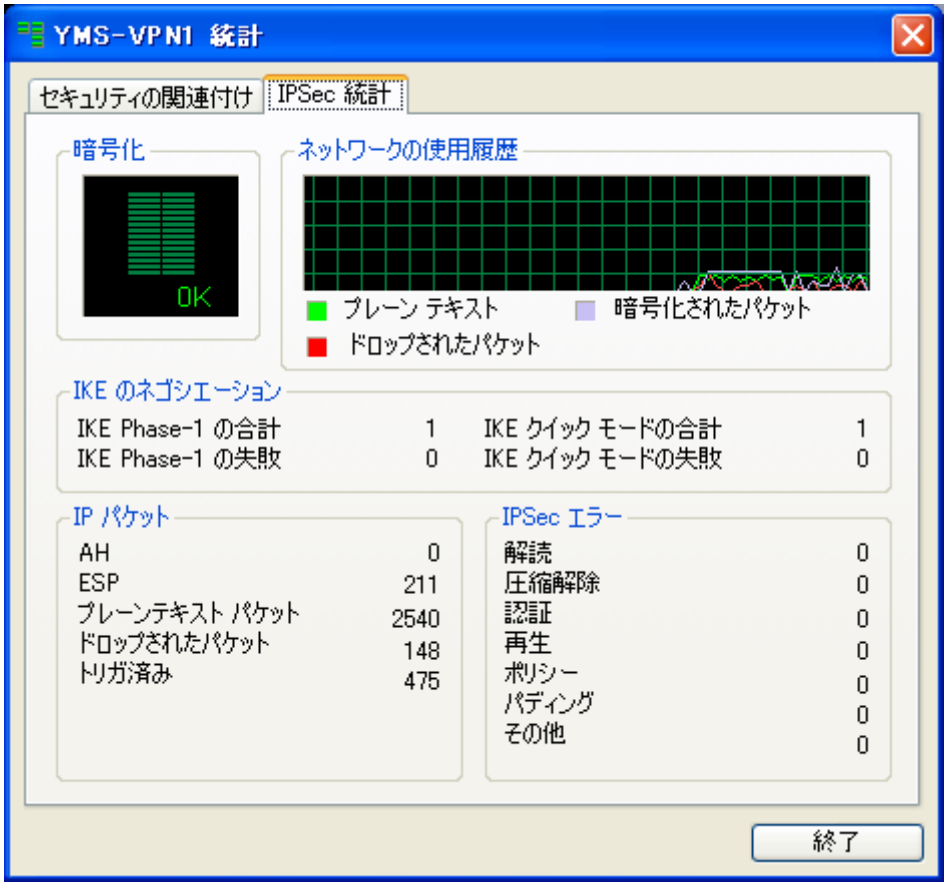



図 4-3　IPsec 統計

### IP パケット

IP パケットの転送数が表示されます。AH、ESP、およびプレーン テキストごとにパケット数が表示されます。フィルタ規則によってドロップされたパケット数と、IPsec エンジンによってトリガされたパケット数も表示されます。

### IPsec エラー

このボックスに表示される情報を使用して、受信データ パケットのエラーを追跡できます。データ パケットの解読、圧縮解除、認証、およびパディング別のエラー数が表示されます。データ再生の疑いがある状況についても表示されます。これらのカテゴリに該当しないエラーについては、[ その他 ] のエラーに分類されます。

[ 解読 ] エラーと [ 圧縮解除 ] エラーは、単にデータ パケットの解読時または圧縮解除時にそれぞれ発生するエラーです。[ 認証 ] エラーは、データ パケットの送信元が認証さ

れない場合、つまり、通信相手の証明書を信頼しない場合などに発生します。[ 再送 ] エラーは、インターネットの代表的な攻撃タイプに関連します。この攻撃では、悪意ある攻撃者が同じデータパケットを繰り返し送信します。データ パケットの長さが足りない場合に挿入するパディングに問題があると、[ パディング ] エラーが発生します。

# 第 5 章　用語集

この用語集では、本ユーザマニュアルで使用される特殊な用語と略語の定義を示します。インターネット セキュリティに関する用語の詳細については、RFC 2828 を参照してください。

**AES ( Advanced Encryption Standard )**　AES は、対称暗号化アルゴリズムの新しい米国政府標準です。AES は、Rijndael ブロック暗号を使用します。NIST ( National Institute of Standards and Technology : 米国商務省国立標準化技術研究所 ) によって FIPS 197 に定義されています。

**AH ( Authentication Header: 認証ヘッダー )**　IP パケット内で IP ヘッダーとペイロードの間に位置する上位レベルのヘッダー。通常、AH には IP パケットの転送に依存しない内容の ICV ( integrity check value: 整合性チェック値 ) が含まれています。チェックサムの正確な内容は、使用する変換に応じて異なります。AH は、ペイロードと IP ヘッダーの両方を含む IP パケット全体の整合性を確認するために使用します。データの機密性は提供されません。AH 変換は、RFC 2402 に定義されています。

**Blowfish**　Bruce Schneier によって設計された対称ブロック暗号。Blowfish では、ブロック サイズとして 64 ビット、鍵長として 32 ～ 448 ビットを使用します。

**CAST-128**　ブロック サイズとして 64 ビット、鍵長として最大 128 ビットを使用する対称ブロック暗号。CAST-128 は非常に強力であるとされています。詳細については、『RFC 2144』を参照してください。

**DES ( Data Encryption Standard: データ暗号化規格 )**　DES は、DEA ( Data Encryption Algorithm: データ暗号化アルゴリズム ) を定義する米国の FIPS ( Federal Information Processing Standard: 連邦情報処理規格 ) です。DES はデータ暗号化アルゴリズム自体を指す用語としてもよく使用されます。

このアルゴリズム自体は、ブロック サイズを 64 ビット、鍵長を 64 ビット( その内の 8 はパリティビット ) とする対称ブロック暗号です。このアルゴリズムは、1970 年代に米国の NSA (National Security Agency: 国家安全保障局) の支援の下に IBM によって作成されました。Horst Feistel のアイデアに基づいて IBM の科学者チームが考案した暗号が暗号研究に影響を与えました。

DES の鍵長と設計上の問題を廻る議論が発展し、元のアルゴリズムから多くのバリエーションが誕生しています。3DES ( トリプル DES または TDEA とも呼ばれる ) が最も広く使用されています。ブロック暗号に関して解明された大半の知識は、DES の解析に負っています。DEA および TDEA は、FIPS 46-3 に定義されています。

**ESP ( Encapsulating Security Payload: カプセル化セキュリティ ペイロード )** ペイロードの内容が暗号化されている ( および別の方法でも保護されている場合がある ) ことを示す上位レベルの IP ヘッダー。ESP は、IP ヘッダーの後、ESP ヘッダーの後、または理論的には IP パケット内の任意の位置に挿入できます。ESP はペイロードの内容のみを保護します。関連するヘッダーは保護されません。したがって、たとえば ESP を含む IP パケットのヘッダーで任意のフィールドを変更しても、セキュリティ違反が生じません。ESP ヘッダーの内容は、保護されたデータを復元するために必要な変換と SA の情報を持たない部外者にはわかりません。ESP には整合性の保護が含まれる場合もあります。ESP プロトコルは、RFC2406 に定義されています。

**HMAC ( Hash Message Authentication Code: ハッシュ メッセージ認証コード )** 秘密鍵認証アルゴリズム。HMAC が提供するデータ整合性とデータ送信元認証は、秘密鍵の配布範囲によって異なります。送信元と送信先のみが HMAC 鍵を知っている場合は、当事者間で送信されるパケットのデータ送信元認証とデータ整合性の両方が提供されます。HMAC が正しい場合は、それが送信元によって追加されたものであることが証明されます。

**ICV ( Integrity Check Value: 整合性チェック値 )** 通常は MD5 または SHA-1 のハッシュ関数を使用する HMAC アルゴリズムです。ただし、DES-MAC アルゴリズムまたは HMAC-RIPEMD アルゴリズムの場合もあります。整合性も参照してください。

**IETF ( インターネット技術標準化委員会 )** インターネットで使用されている IP プロトコルおよび他の大半のプロトコルを規格化した国際規格団体。IETF の Web ページは、http:// www.ietf.org/ で参照できます。

**IKE ( Internet Key Exchange: インターネット鍵交換 )** IPsec で使用される鍵設定プロトコル。IKE は、以前は ISAKMP/Oakley 鍵交換と呼ばれていました。IKE プロトコルは、RFC2409、RFC 2408、および RFC 2407 に定義されています。

**IP ( インターネット プロトコル )** STD 5 に定義されている、TCP/IP プロトコルスイートのネットワーク層。IP はコネクションレス型、ベストエフォート型のパケット交換

プロトコルです。データ リンク層を介してパケットのルーティング、分割、および再組み立てを行います。

**IPsec ( インターネット プロトコル セキュリティ )**　IETF によって定義された、パケットレベルで IP トラフィックを保護するためのプロトコル スイート。IPsec を使用して、IP に基づく任意のサービスまたはアプリケーションからの転送データを保護できます。IPsec プロトコルは、RFC 2401 に定義されています。IPsec を理解するには、最初に RFC 2411 を参照することをお勧めします。

**IP アドレス**　IPv4 で、IP プロトコルを使用するデバイスを識別する 32 ビットの数値です。IP アドレスは、ユニキャスト、ブロードキャスト、またはマルチキャストの場合があります。詳細については、『 STD 5 』を参照してください。

**IP パケット**　転送元と転送先のコンピュータ間で以前に行われたデータ交換や転送ネットワークに依存せずに転送元から転送先のコンピュータにルーティングされるために必要な情報を含む独立したデータのエンティティ。IP ( インターネット プロトコル ) は STD 5 に定義されています。

**IP ヘッダー**　IP パケットの、パケット ルーティングに使用されるデータを含む部分。このヘッダーのサイズは 20 バイトですが、通常はこのヘッダーに続く IP のオプションもヘッダーとして計算されます。ヘッダーの最大長は 60 バイトです。ヘッダーのフォーマットは、STD 5 ( および RFC 791 ) に定義されています。

**IP ペイロード**　上位レベルのアプリケーションデータを含む、IP パケットの部分。

**ISAKMP ( Internet Security Association and Key Management Protocol: インターネット セキュリティアソシエーションおよび鍵管理プロトコル )**　SA の設定、ネゴシエーション、変更、および削除を行うプロトコル。ISAKMP は、認証および鍵交換のためのフレームワークを提供しますが、両者を定義することはしません。ISAKMP は、特定の鍵交換に依存しないように設計されています。つまり、多くの異なる鍵交換をサポートするように設計されています。ISAKMP/Oakley は、ISAKMP と Oakley 鍵交換を統合します。Oakley は、モードと呼ばれる鍵交換群と、鍵交換別のサービスの詳細を記述します。たとえば、鍵の PFS (perfect forward secrecy)、ID の保護、認証などを記述します。ISAKMP は、IKE プロトコルの一部です。

**MD5**　RSA Security の Ron Rivest によって開発されたメッセージダイジェストアルゴ

リズム。ドキュメントに対してセキュアで、非可逆の、暗号として強力な 128 ビットのハッシュ値を計算します。このアルゴリズムは、RFC 1321 に定義されています。SHA-1 などのより新しい 160 ビットのアルゴリズムは、MD5 以上にセキュアであると考えられています。

**PKI ( Public-Key Infrastructure: 公開鍵インフラストラクチャ )** PKI は、鍵のペアを持つエンドエンティティ、認証局、証明書リポジトリ ( ディレクトリ ) 、公開鍵暗号の使用時に必要な他のすべてのソフトウェア、コンポーネント、およびエンティティで構成されます。

**RFC ( Request For Comments )** Internet Society の規格化に関するドキュメント。RFC は http:/ /www.ietf.org/rfc.html で参照できます。

**Rijndael** Joan Daemen と Vincent Rijmen によって設計された対称ブロック暗号で、可変ブロックサイズを 128、192、256 ビット、および可変鍵長を 128、192、256 ビットとします。Rijndael は、米国 AES ( Advanced Encryption Standard ) で採用されているアルゴリズムです。

**RSA** Ron Rivest 、Adi Shamir 、および Leonard Adleman によって考案された公開鍵暗号化およびデジタル署名のアルゴリズム。詳細については、Bruce Schneier 著『Applied Cryptography 』を参照してください。RSA アルゴリズムは、RSA Security により特許として登録されましたが、特許は 2000 年 9 月で期限が切れています。

**SA ( Security Association: セキュリティの関連付け )** セキュリティ目的で作成された単方向の接続。SA に関与するすべてのトラフィックに同じセキュリティ処理が適用されます。IPsec のコンテキストでは、SA は AH または ESP の使用を介して実装されるインターネット層の抽象です。変換を IP パケットに適用する方法を制御するデータが含まれています。データは、特別に定義された SA 管理機構を使用して決定されます。データは、SA および鍵ネゴシエーションを自動化して生成するか、手動で定義します。この用語は、RFC 24 01 に定義されています。

**SGW ( Security Gateway: セキュリティ ゲートウェイ )** 2 つのネットワーク間で通信インターフェイスとして機能する中間システム。セキュリティ ゲートウェイの内側にあるサブネットワークおよびホストは、共通のローカル セキュリティ管理により信頼できるものと見なされます。信頼されるサブネットワークも参照してください。

セキュリティ ゲートウェイの外側のホストおよびネットワークのセットは、信頼できない、または信頼性がより低いと見なされます。IPsec のコンテキストでは、セキュリティ ゲートウェイは、内部ホストのセットとして機能する AH または ESP が実装される場所です。セキュリティゲートウェイは、これらのホストが、同じように IPsec を使用する( 直接または別のセキュリティゲートウェイを介して ) 外部ホストと通信する際に、セキュリティサービスを提供します。この用語は、RFC 2401 に定義されています。

**SHA (Secure Hash Algorithm )**　暗号として強力なハッシュ アルゴリズムに関する米国規格。このアルゴリズムは、NSA ( National Security Agency: 国家安全保障局 ) によって設計され、NIST ( National Institute of Standards and Technology: 米国商務省国立標準化技術研究所 ) によって定義されたものです。MD5 も参照してください。

**SHA-1**　元の SHA ( Secure Hash Algorithm ) を改良したバージョン。このアルゴリズムは、160 ビットのメッセージダイジェストを生成する、優れたアルゴリズムであると考えられています。このアルゴリズムは米国 DSS　Digital Signature Standard ) の一部であり、FIPS 180-1 に定義されています。

**STD ( Standard )**　インターネット規格を指定する RFC ( Request For Comments ) のサブシリーズ。STD シリーズの規格は、RFC 番号も保持しています。

**TCP ( Transmission Control Protocol )**　広く使用されているコネクション型で信頼性の高い ( ただし、セキュアでない ) 通信プロトコル。インターネットで使用されている標準の転送プロトコルです。TCP は、STD 7 (および RFC 793) に定義されています。

**Twofish**　Bruce Schneier によって考案された強力で高速なブロック暗号。Twofish は、米国政府の新しい暗号規格である AES(Advanced Encryption Standard) の 5 つの最終候補の 1 つです。Twofish はブロック サイズとして 128 ビットおよび鍵長として最大 256 ビットを使用します。

**UDP ( User Datagram Protocol: ユーザ データグラム プロトコル )**　インターネットで広く使用されている、データグラム指向の、信頼性が低い通信プロトコル。IP プロトコルの上位の層です。UDP は、STD 6 (および RFC 768) に定義されています。

**VPN ( バーチャル プライベート ネットワーク )**　VPN は、下位のプロトコル層で暗号化を使用し、通常はセキュアでないネットワーク ( インターネットなど ) においてセキュアな接続を提供します。暗号化は、ファイアウォール ソフトウェア、ルータ、専用の VPN

セキュリティ ゲートウェイなどを使用して実行できます。

**X.509** ITU-T X.509 勧告は、X.509 証明書および X.509 CRL のフォーマットを定義しています。X.509 のアプリケーション別の定義は、IETF の PKIX 作業部会で行われています。たとえば、X.509 バージョン 3 の公開鍵証明書や X.509 バージョン 2 の CRL が定義されています。

**アクセス制御** リソースの不正使用を防止するためのセキュリティ対策。IPsec のコンテキストでは、ホストのコンピューティング サイクル、ホストの保存データ、セキュリティ ゲートウェイの内側のネットワーク、そのネットワーク上の帯域幅などのリソースがアクセス制御の対象になります。

**暗号化** データを可読形式 ( プレーンテキスト ) から不可読形式 ( 暗号テキスト ) に変換して機密性を確保するためのセキュリティ機構。逆の変換プロセスは解読と呼ばれます。

**機密性** データの漏洩を防ぐためのセキュリティ サービス。通常は、アプリケーション レベルのデータの漏洩が問題ですが、通信の外部特性の漏洩が問題になる場合もあります。トラフィック フローの機密性サービスは、この後者の問題に対処するために、送信元と宛先のアドレス、メッセージ長、または通信頻度を隠します。IPsec のコンテキストでは、トンネル モードの ESP を特にセキュリティ ゲートウェイで使用することにより、トラフィック フローの一定の機密性を確保できます。トラフィック解析も参照してください。

**共有シークレット** 認証で共有シークレット (既知共有鍵) を使用することは、通信当事者間に事前に生成された共有パスワードまたは鍵があることを意味します。

共有シークレットは、IKE で使用できます。この場合、2 つのピアはエンド ポイントを認証するための共有パスワードを暗号化の方法で設定しています。A が暗号化したパケットを B が解読できるということは、A と B が同じシークレットを共有していることを B が知っていることになります。その逆も同じです。この認証方法は、適用範囲が限られるため、制限された数のホストに使用します。大規模なホストのグループに対しては、証明書ベースの認証を使用します。

**公開鍵** 公開鍵暗号では、公開鍵は証明書に含まれ、署名の確認とメッセージの暗号化に使用されます。

**公開鍵暗号**　暗号鍵が 1 つのみの対称 ( 秘密鍵 ) 暗号とは異なり、公開鍵暗号では各ユーザまたは各ホストが 2 つの鍵を持ちます。1 つは秘密鍵であり、送信メッセージの署名と受信メッセージの解読に使用します。もう 1 つは公開鍵 であり、送信元からの署名されたメッセージの認証と送信先へのメッセージの暗号化に使用します。秘密鍵はその所有者以外には使用できないようにする必要があります。公開鍵は信頼されたチャネルを介して一般に公開されます。

**証明書**　証明書は、通信当事者の本人性を確認するために使用されるデジタル文書です。本マニュアルでは、主に X.509 公開鍵証明書を意味します。公開鍵証明書は、エンティティの識別情報とエンティティの公開鍵を一定の有効期限の間結び付けます。

**整合性**　データの変更の検出を保証するセキュリティ サービス。整合性サービスは、アプリケーションの要件に対応している必要があります。認証サービスと整合性サービスは個別に扱われますが、実際には両者は密接に結び付いており、通常は両方がセットとして提供されます。

**セキュリティ ポリシー**　セキュリティポリシーの目的は、組織の自衛手段を決定することです。通常、ポリシーは一般ポリシーと特別規則 ( システム別ポリシー ) の 2 つの部分で構成されます。一般ポリシーは、セキュリティへの全般的なアプローチを設定します。規則は、許可事項と不許可事項を定義します。本マニュアルでは、通常、セキュリティ ポリシーを後者の意味で使用しています。セキュリティ ポリシーは、データの保護方法、トラフィックの許可 / 拒否、および誰がネットワーク リソースを使用できるかを定義します。

**デジタル署名**　メッセージのダイジェストを秘密鍵で暗号化すると、暗号化されたダイジェストに公開鍵を適用 ( デジタル署名 ) し、その結果をメッセージのダイジェストと比較することにより、後で認証を実行できます。

**トラフィック解析**　攻撃者が攻撃に役立つ情報を推測する目的でネットワーク トラフィック フローを解析すること。たとえば、通信の頻度、通信当事者の識別情報、IP パケットのサイズ、フロー識別子などが解析されます。

**ドメイン名**　ドメイン名は、インターネットホストのテキスト名 ( www.dit.co.jp など ) です。ドメイン名を IP アドレスに変換するには、DNS ( Domain Name System: ドメイン名システム ) インフラストラクチャを使用します。詳細については、『STD 13』を参照してください。

**認証** ユーザまたはプロセスの本人性を確認すること。通信システムでは、認証によってメッセージの送信元が正しいことを確認します。

**認証局（CA）** デジタル証明書 ( 特に X .509 公開鍵証明書 ) を発行し、証明書内のデータ アイテム間の有効な結び付きを保証する PKI のエンティティ。

証明書のユーザ ( エンド エンティティ ) は、証明書が提供する情報の有効性に依存します。したがって、CA はエンドエンティティから信頼されることが必要であり、通常は政府や企業などの組織によって創設され権限を付与された公的な機関が担当します。

**ハッシュ関数** 長いメッセージの短いダイジェストを計算するアルゴリズム。通常、ダイジェストは固定サイズです。MD5 と SHA-1 も参照してください。

**秘密鍵** 公開鍵暗号では、秘密鍵はその保持者のみが知っています。秘密鍵を使用してメッセージの署名および解読ができます。

**プレーン テキスト** 暗号化されていないテキスト。暗号テキストの逆です。

**ブロック暗号** 固定長のプレーン テキスト ブロック(64 ビットなど) ごとに暗号化する、代表的な対称( 秘密鍵) 暗号化アルゴリズム。ブロック暗号では、同じ鍵を使用すると、同じプレーンテキストブロックが常に同じ暗号テキスト ブロックに変換されます。

**変換** IP パケットに適用される特定のタイプの変更。たとえば、ESP 暗号化、AH 整合性サービス、ペイロード圧縮などの変換タイプがあります。SA は、鍵およびその他の関連に固有なデータを変換に提供します。IPSEC の変換は、RFC 2401、RFC 240 2、RFC 2403、RFC 2404、RFC 2406、および RFC 2405 に定義されています。

**ホスト** 自分宛でないパケットを転送しないノード。通常、この用語は IP ベースのネットワークに接続されたコンピュータまたはコンピューティング デバイスを意味します。

**ルータ** 自分宛でないパケットを転送するノード。ルータの要件は、RFC 1812 に定義されています。

YAMAHA VPN クライアント
YMS-VPN1
ユーザ マニュアル

2006 年 6 月

---

ヤマハ株式会社