NET-G Secure VPN Client
ユーザー マニュアル

2010 年 3 月

本マニュアルでは、NET-G Secure VPN Client ソフトウェアについて説明します。NET-G Secure VPN Client は、TCP/IP 接続を通じてセキュアな通信を提供する SSH コミュニケーションズ・セキュリティ社（現在は SafeNet 社）の IPSec クライアント製品をベースに、株式会社ディアイティが IPv6 および Windows Vista /7 に対応したものです。

株式会社ディアイティ
〒135-0016 東京都江東区東陽 3-23-21 プレミア東陽町ビル
http://www.dit.co.jp/
info@dit.co.jp（営業的なお問い合わせ）
support@dit.co.jp（技術的なお問い合わせ）

目　　次

第 1 章　はじめに

1.1. NET-G Secure VPN Client について

NET-G Secure VPN Client 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。

NET-G Secure VPN Client は、単一のユーザー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。NET-G Secure VPN Client 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。

NET-G Secure VPN Client 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ー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。NET-G Secure VPN Client は、PKI (Public Key Infrastructure: 公開鍵インフラストラクチャ) で効果的に機能し、ポリシーの集中管理をサポートします。
NET-G Secure VPN Client 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 XP、Windows Vista、Windows 7 です。

NET-G Secure VPN Client はエンドユーザー向けに設計されているために、使い方も簡単です。主な特徴としては、直感的なインストールと構成、簡単な方法での証明書の認証が挙げられます。NET-G Secure VPN Client 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。

NET-G Secure VPN Client は、多数のカスタマおよびエンドユーザーの要求に応じて、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、NET-G Secure VPN Client 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ーおよびシステム管理者を対象としています。わかりやすいステップ別の手順に加えて、セキュリティ上の問題に対する背景の説明と、設問形式での解説も含まれています。

本マニュアルの構成は、次のとおりです。

- セキュリティ ポリシーの概要
- NET-G Secure VPN Client のインストール
- フィルタ規則と接続規則の設定
- 認証鍵の管理
- 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、NET-G Secure VPN Client のリリースノートを参照してください。

1.3. IP (Internet Protocol: 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（Internet Engineering Task Force: 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　NET-G Secure VPN Client のインストールと削除

2.1. 要件

NET-G Secure VPN Client は、一般的な Microsoft Windows プラットフォームで使用できます。対応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	NET-G Secure VPN Client			注記
		ver.2.2.x 以前	ver.2.3.x 以降	ver.2.4.x 以降	
Windows 98	SE	○			※1
Windows NT 4.0	SP4 以降	○			※1, 2
Windows Me		○			※1
Windows 2000	SP4 以降	○	○		※1
Windows XP	SP1 以降	○	○		※1
Windows XP	SP3		○	○	
Windows Server 2003		○	○		※1
Windows Vista			○		
Windows Vista	SP2 以降		○	○	
Windows Vista (64bit Edition)	SP2 以降			○	
Windows 7				○	
Windows 7 (64bit Edition)				○	

注記：　※1　「NET-G Secure VPN Client ver 2.2.x 以前」は終息商品

※2　Internet Explorer 5.01 以降が必要

使用しているコンピュータの Windows バージョンを（ Windows XP から Windows Vista などに ）更新する前に、NET-G Secure VPN Client 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ます。

NET-G Secure VPN Client 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、NET-G Secure VPN Client は IPsec ゲートウェイ ソフトウェアではありません。

NET-G Secure VPN Client 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。NET-G Secure VPN Client は、他のソフトウェアの機能に影響する場合があります。

NET-G Secure VPN Client 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。

Windows XP

プロセッサ	Intel Pentium Ⅲ 500 MHz
メモリ（RAM）	256 MB
ハードディスク容量	100 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

Windows Vista

プロセッサ	1GHz 以上のプロセッサ
メモリ（RAM）	512MB
ハードディスク容量	100 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

Windows 7

プロセッサ	1GHz 以上のプロセッサ
メモリ（RAM）	1GB
ハードディスク容量	100 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

NET-G Secure VPN Client 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。

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。NET-G Secure VPN Client 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.　NET-G Secure VPN Client のインストール

ホストで通常のインストールを実行する場合は、次のことが実行されます。

- 認証鍵ペアが作成されます。
- 鍵ペアに関連する自己署名証明書が作成されます。これはローカル ID 証明書になります。
- （ オプション ）認証局への証明書要求が作成されます。
- 初期の規則セットおよび信頼ポリシーが設定されます。

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、NET-G Secure VPN Client インストールパッケージアイコン(setup.exe ）をダブルクリックします。パッケージは、NET-G Secure VPN Client CD または NET-G Secure VPN Client をダウンロードしたフォルダにあります。

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 NET-G Secure VPN Client 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 NET-G Secure VPN Client 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、最初に基本的なインストール ダイアログがいくつか表示されます。使用許諾契約書を参照し、インストールフォルダを選択できます。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。

図 2-1　NET-G Secure VPN Client インストール パッケージ アイコン

2.2.2.　IPsec エンジンのインストール

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。
ここで、IPsec エンジンをインストールします。インストール中に何度か、以下の画面が表示されます。必ずインストールを続行する方のオプションを選択してください。

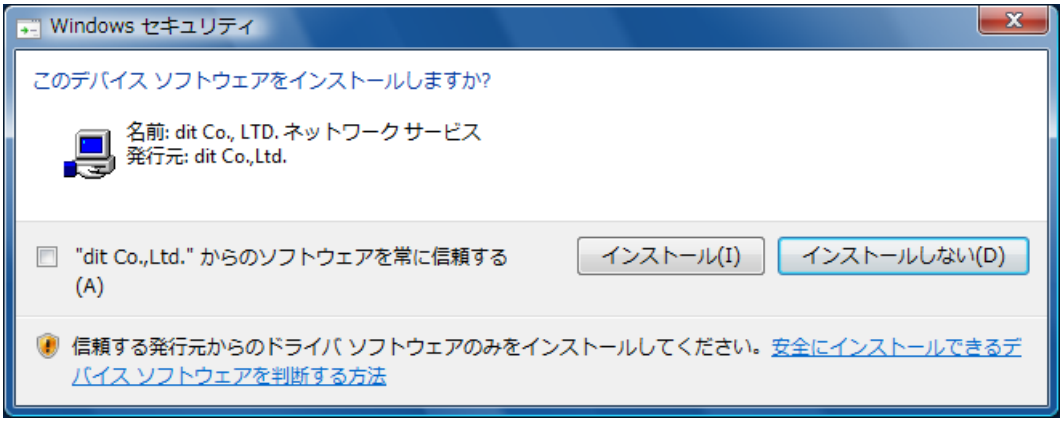

図 2-2 IPsec エンジンのインストール中に表示される画面（Windows Vista）

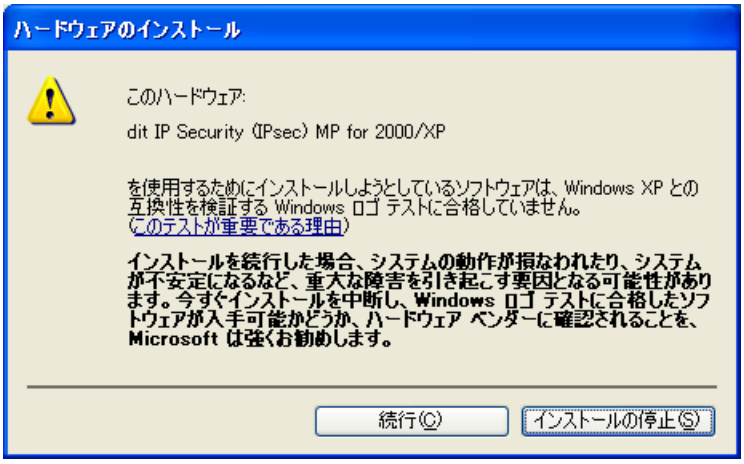

図 2-3 IPsec エンジンのインストール中に表示される画面（Windows XP）

2.2.3. 仮想アダプタのインストール

バーチャル プライベートネットワーク接続を行い、リモート プライベート ネットワークとのシームレスな仮想の統合を達成するために、そのネットワークのアドレス空間から未使用の IP アドレスを取得して使用します。この高度な統合を実現するために、NET-G Secure VPN Client はリモート ネットワークに直接接続しているように見える別のネットワーク インターフェイスを作成します。アダプタはリモート ネットワークに物理的には接続されていませんが、接続されているように見えるネットワーク インターフェイスをローカル コンピュータに提供します。この種のネットワーク アダプタは仮想アダプタと

呼ばれます。
ここで、仮想アダプタをインストールします。インストール中に何度か、以下の画面が表示されます。必ずインストールを続行する方のオプションを選択してください。

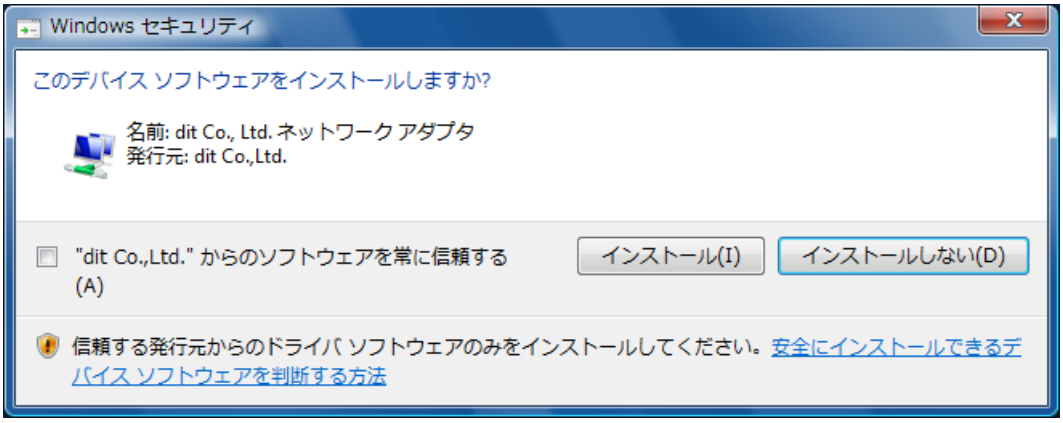

図 2-4　IPsec エンジンのインストール中に表示される画面（Windows Vista）

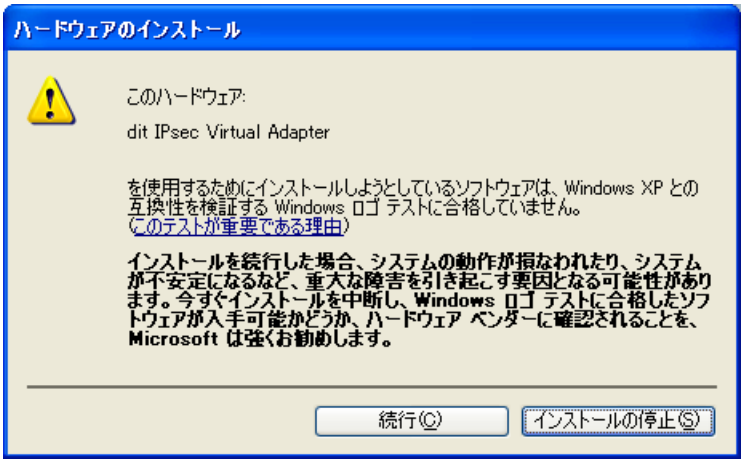

図 2-5　IPsec エンジンのインストール中に表示される画面（Windows XP）

2.2.4.　認証鍵ペアの生成

NET-G Secure VPN Client 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。ユーザー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。

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。認証鍵の生成が完了した後で、[次へ] ボタンをクリックして続行します。

2.2.5. 識別情報

NET-G Secure VPN Client 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。NET-G Secure VPN Client 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、NET-G Secure VPN Client 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。

リストからプライマリ ID を選択します。実際の ID であるホストのドメイン名、ホストの IP アドレス、または管理者の電子メール アドレスを、該当するフィールドに入力します。[次へ] をクリックして続行します。

2.2.6. 登録プロトコルの選択

インストール中には自己署名証明書が自動的に作成されますが、それに加えて認証局への証明書要求も作成できます。証明書要求は、オンラインで登録することも、ファイルに保存して、後で認証局に送付することもできます。オンラインで登録すると、証明書要求は作成した直後に送付されます。利用できる認証局が存在しないか、何らかの理由で証明書要求の作成を延期する場合は、自己署名証明書のみを作成します。

[証明書の登録] ダイアログボックスで、次のいずれかの登録方法を選択します。

- 自己署名証明書のみを作成する場合は、[自己署名証明書を作成します。] を選択します。[次へ] をクリックして暗号化速度の診断に進みます。
- 証明書要求を作成してオンラインで登録するには、[証明書要求を作成し、すぐにオンラインで証明書を登録します。] を選択します。自己署名証明書も作成されます。[次へ] をクリックして続行します。
- 証明書要求を作成してファイルに保存する場合は、[証明書要求を作成し、後で登録するようにファイルに保存します。] を選択します。自己署名証明書も作成されます。[次へ] をクリックして続行します。

オンライン登録情報

オンライン登録を選択すると、次に [認証局] ダイアログ ボックスが表示されます。認証局と登録に関する情報を入力します。

登録プロトコル

ドロップダウン リストから登録プロトコルを選択します。認証局でサポートされているプロトコルを選択する必要があります。使用できるプロトコルは、SCEP (Simple Certificate Enrollment Protocol) と CMP(Certificate Management Protocol) です。

CA サーバアドレス

認証局サーバのアドレス（URL）を指定します。

CA 証明書

認証局の証明書は、認証局に送る証明書要求を暗号化するのに必要です。認証局の証明書は、通常、認証局の Web サイトから取り出すことができます。

Web サイトから証明書を取り出すには、このフィールドにアドレス (URL) を入力します。別の方法として、証明書名を指定し、前のフィールドに指定したアドレスから証明書を取り出すことができます。証明書を事前に取り出してファイルに保存するか、クリップボードにコピーすることもできます。証明書をファイルからインポートするには、[参照] ボタンをクリックしてファイルを探します。クリップボードから貼り

付けるには、リストから [クリップボードからの貼り付け] を選択します。

証明書を Web サイトから取り出すか、クリップボードから貼り付ける場合、証明書は PEM でエンコードされたフォーマットであることが必要です。ファイルからインポートする証明書には、バイナリ (X.509) および PEM のフォーマットを使用できます。

プロキシ サーバを使用する

ローカル ホストはファイアウォールで保護されるため、プロキシの設定が必要です。[設定] ボタンをクリックして値を指定します。この場合、ローカル ホストでサーバアドレスを解決できることが必要です。

参照番号

CMP(CertificateManagementProtocol) でのみ使用します。証明書を要求しているユーザーを識別するには、鍵と共に鍵 ID を使用します。

鍵

証明書要求で使用する、認証局から付与された共有シークレット。証明書を要求しているユーザーを確認するために使用します。

オフライン証明書要求

オフライン証明書要求は単なるファイルです。このファイルに証明書要求を保存して、後で使用します。証明書要求は PKCS#10 のフォーマットであり、PEM (Privacy Enhanced Mail) でエンコードされて保存されます。ファイルの場所は [証明書要求] ダイアログボックスで指定します。ファイルシステムを参照するには、[参照] ボタンをクリックします。[次へ] をクリックして暗号化速度の診断に進みます。

登録を完了するには、証明書要求を認証局に送付します。証明書要求を認証局に送付するには、要求を保存したフロッピー ディスクを郵送するか、要求を電子メールで送信するか、または Web での登録サービスも使用できます。

2.2.7. 暗号化速度の診断

NET-G Secure VPN Client 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。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。

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。NET-G Secure VPN Client 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、NET-G Secure VPN Client 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、ユーザー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 Intel 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。診断の完了後に [次へ] をクリックして続行します。

2.2.8. ライセンスキーの入力

ユーザ名、会社名、および NET-G Secure VPN Client のライセンスキーを入力します。

ライセンスキーを入力しない場合、NET-G Secure VPN Client は評価版として動作します。評価版は、インストール後 30 日間すべての機能をお試しいただけます。
ライセンスキーは、後で設定することも可能です。

2.2.9. インストールの完了

NET-G Secure VPN Client 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、NET-G Secure VPN Client 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。
インストールの結果として、次のことが実行されます。

- 初期のフィルタ規則セットが作成されます。
- 認証鍵ペアと自己署名証明書が作成されます。オプションとして、認証局への証明書要求が作成されます。
- 自己署名証明書がデフォルト応答規則に挿入されます。
- 自己署名証明書が信頼された認証局に挿入されます。

2.3. NET-G Secure VPN Client の更新

コンピュータに以前のバージョンの NET-G Secure VPN Client 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、NET-G Secure VPN Client 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。
ただし、Windows バージョンを（Windows XP から Windows Vista などに）更新した場合は、NET-G Secure VPN Client は更新できません。以前のバージョンの NET-G Secure VPN Client を削除した後に、新しいバージョンのインストールを行ってください。

2.4. NET-G Secure VPN Client の削除

NET-G Secure VPN Client を削除する前に、次の操作を実行します。

1. NET-G Secure VPN Client 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。NET-G Secure VPN Client 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 NET-G Secure VPN Client 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。

NET-G Secure VPN Client 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［NET-G Secure VPN Client］を選択します。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前に、NET-G Secure VPN Client を削除します。オペレーティング システムの更新後に NET-G Secure VPN Client を再インストールします。

第 3 章　ポリシー エディタ

3.1.　NET-G Secure VPN Client ソフトウェアのコンポーネント

NET-G Secure VPN Client 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。

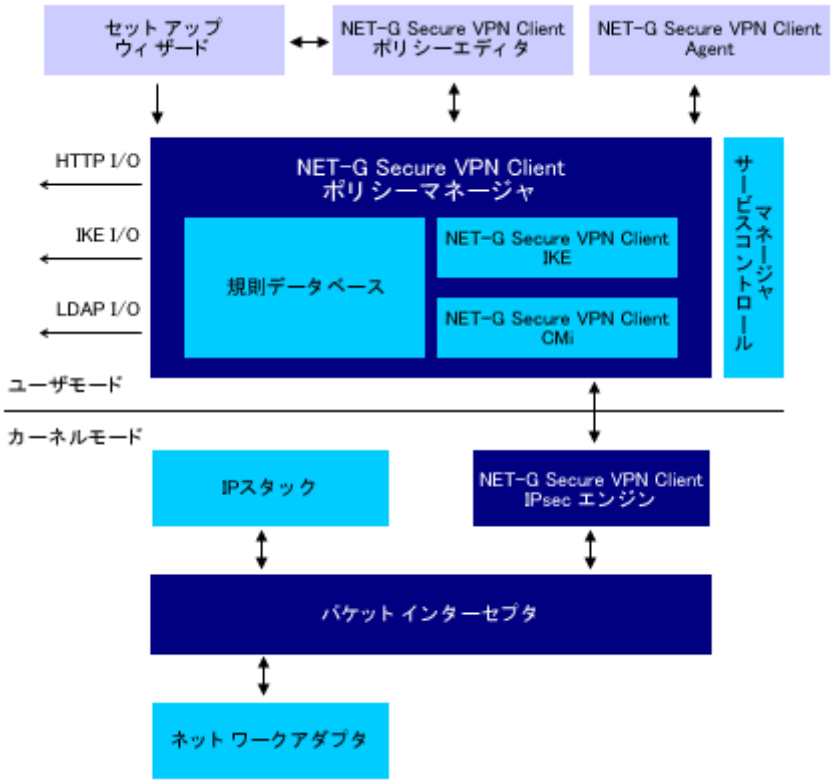

図 3-1　ソフトウェアの詳細なアーキテクチャ

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。NET-G Secure VPN Client 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 エディタをユーザー 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. NET-G Secure VPN Client 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 NET-G Secure VPN Client 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、メイン メニューが開いて次の項目が表示されます。

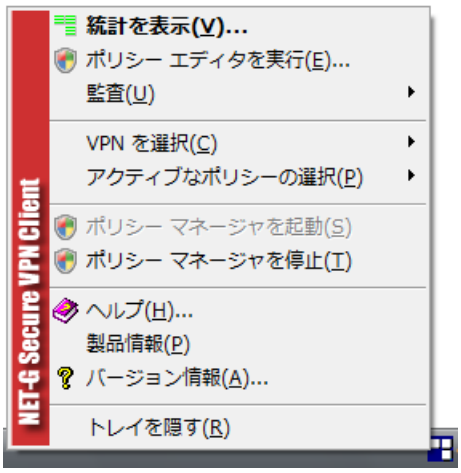

図 3-2 NET-G Secure VPN Client のメイン メニュー

統計を表示

NET-G Secure VPN Client 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。「14.4 統計」の項を参照してください。

ポリシー エディタを実行

ポリシー エディタを開きます。

監査

監査ログを表示

参照する監査ログを開きます。監査ログと監査の詳細については、「14.1 監査」の項を参照してください。

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、「14.2 IKE ログ」の項を参照してください。

監査の設定

[監査の設定] ダイアログボックスを開きます。設定を表示および変更できます。詳細については、「14.1 監査」の項を参照してください。

VPN 接続の選択

VPN 接続を開きます。スタートアップ時に自動的に開く VPN 接続は、リストの上部に淡色表示されます。他の接続を開くには、リストの該当する接続を選択します。仮想アダプタを使用する 1 つの接続のみを一度に開くことができます。詳細については、「7.3.5 仮想 IP アドレス」の項を参照してください。起動時に VPN 接続を自動的に開く方法については、「7.2.9 VPN 接続を開いて終了する」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。

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

NET-G Secure VPN Client のオンライン ヘルプを開きます。

製品情報

株式会社ディアイティの Web ページを開きます。

バージョン情報

NET-G Secure VPN Client ソフトウェアに関する一般的な情報を表示します。

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、Windows の［ スタート ］メニューで［ すべてのプログラム ］の［ NET-G Secure VPN Client ］フォルダから［ NET-G Secure VPN Client Agent ］を選択します。
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［ すべてのプログラム ］の［ スタートアップ ］フォルダから［ NET-G Secure VPN Client Agent ］を削除します。ただし、NET-G Secure VPN Client のメイン フォルダからは NET-G Secure VPN Client 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. ポリシー エディタを開く

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。

- NET-G Secure VPN Client 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。［ NET-G Secure VPN Client ］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［ すべてのプログラム ］を開きます。[NET-G Secure VPN Client ］の[NET-G Secure VPN Client ポリシーエディタ ］を選択します。

3.4.　ポリシー エディタの使い方

ポリシー エディタでは、ポリシー規則と認証鍵を表示して管理できます。規則と鍵を管理するページとして、それぞれ［ セキュリティ ポリシー ］と［ 鍵管理 ］があります。

3.4.1.　セキュリティ ポリシー

セキュリティ ポリシーは、ポリシー エディタの［ セキュリティ ポリシー ］ページで管理します。

図 3-3　セキュリティ ポリシー ページ

セキュリティ ポリシーは、次の項目で構成されます。

- 2 つの独立したトラフィック フィルタ
- IPsec トラフィック規則

- 受信 IPsec トラフィックおよび保護されていない IP トラフィックの両方を処理するデフォルト応答規則

3.4.2. 鍵管理

[鍵管理] ページでは、認証鍵を管理します。

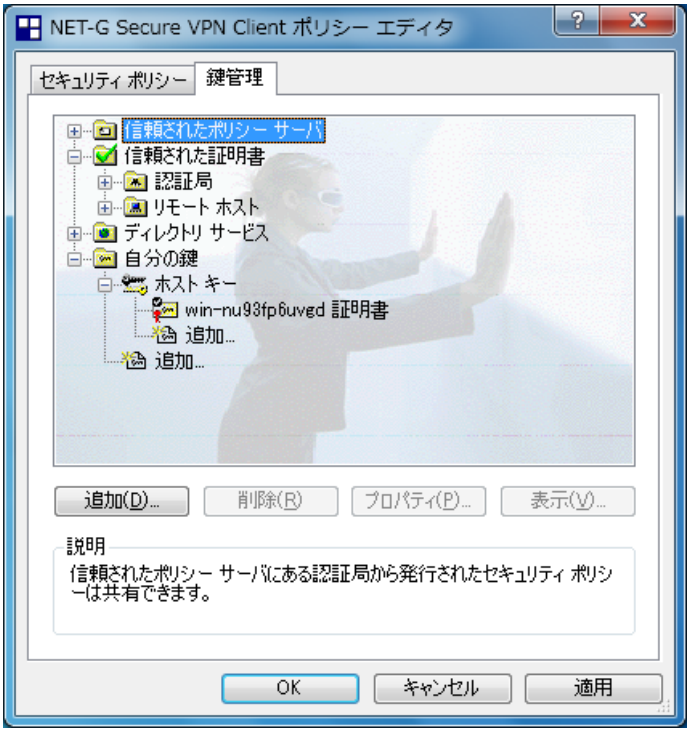

図 3-4 鍵管理 ページ

認証鍵は、次のカテゴリに分類されます。

- 信頼されたポリシー サーバのセキュリティ ポリシーは共有できます。この種の証明書は、システムのすべてのポリシーに共通です。
- 認証局は、下位レベルの認証局とエンド エンティティ (ホスト) に証明書を発行します。リモートホストの証明書は、信頼する認証局から発行されている場合は、自動的に信頼されます。
- 認証局と公開鍵インフラストラクチャを利用できない場合は、リモートホストの自己署名証明書を認証に使用します。
- ローカル ホストの認証鍵は、[自分の鍵] ブランチに一覧表示されます。この種の鍵には、既知共有鍵、自己署名証明書、および認証局から発行された証明書が含まれます。

[鍵管理] ページでは、ディレクトリサービスも管理します。ディレクトリサービスは、公開鍵インフラストラクチャを使用する場合と、リモートサーバのポリシーを探す場合に必要です。

第 4 章　複数のポリシー

4.1. 複数のポリシーとは

NET-G Secure VPN Client ソフトウェアは、マルチレイヤのポリシー構造をサポートしており、ホストが保持できるセキュリティ ポリシー レイヤの数には制限がありません。単一のポリシー レイヤには、完全なセキュリティ ポリシーおよび信頼ポリシーが含まれています。すべてのポリシーに共通するのは、ローカルホストの認証鍵と信頼されたポリシー サーバの証明書です。後者は、集中管理ポリシーをダウンロードするのに必要です。同時に適用できるポリシー レイヤ（ アクティブなポリシー レイヤ ）は 1 つのみです。

ポリシー レイヤは、ローカルで管理されるか、集中管理されます。ローカル ポリシーは自由に更新できますが、集中管理ポリシーは集中管理による変更でのみ更新されます。更新内容は、定期的にポリシー サーバから取り出されます。

4.2. ポリシーの管理

4.2.1. ポリシーの追加

新しいポリシーは次のいずれかの方法で追加します。

- ローカル ポリシーを最初から作成する。
- ファイルからポリシーをインポートする。
- 集中管理ポリシーを共有する。

ファイルからインポートしたポリシーは、自由に更新できるローカル ポリシーになります。

ポリシーを追加するには、次の手順に従います。

1. 既存のポリシーのヘッダーをクリックしてポリシーを選択し、[追加] ボタンをクリックします。
2. [ポリシーの追加] ダイアログ ボックスが開きます。必要な値を指定します。
   - ポリシーにわかりやすい名前を付けます。この名前は単なる参照用です。
   - ポリシーのソースを選択します。最初からローカルポリシーを作成することも、ファイル、ポリシーサーバ、HTTP サーバ、または LDAP サーバからポリシーをイ

ンポートすることもできます。

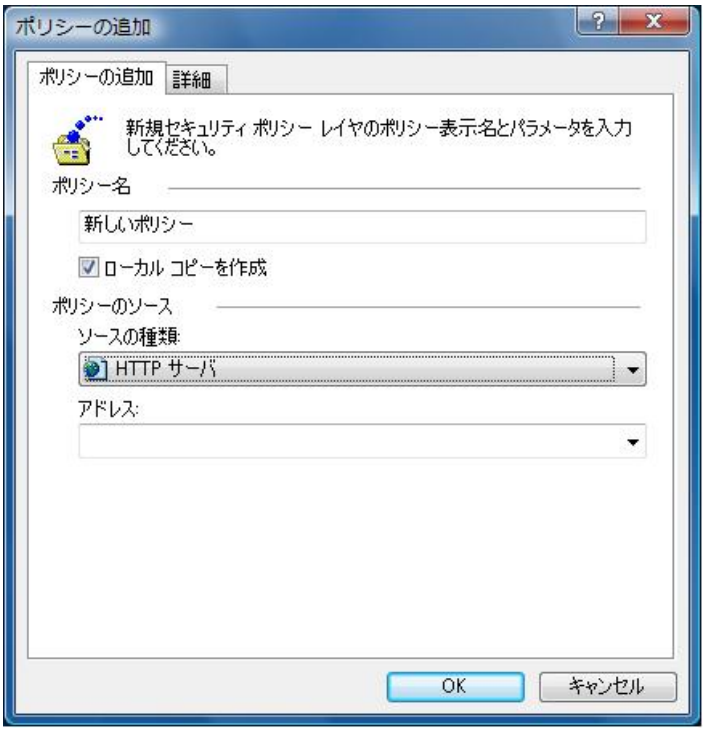

図 4-1 新しいポリシーを追加するためのダイアログ ボックス

- ポリシーをインポートする場合は、フィールドにファイル名とアドレス、またはサーバアドレスを指定します。また、LDAP サーバからポリシーをインポートする場合は、他の 2 つのフィールドにポリシー名(省略可) と基本オブジェクト識別名（DN）（必須）を指定します。条件が不完全な場合は、条件に一致するすべてのポリシーが返され、表示されるリストから目的のポリシーを選択できます。
- 集中管理ポリシーのローカル コピーを作成する場合は、[ローカルコピーを作成] オプションを選択します。集中管理によってポリシーが更新されても、ローカル コピーには反映されません。この操作は元に戻せません。

3. 準備ができたら、[OK] をクリックします。キャンセルするには、[キャンセル] をクリックします。
4. 集中管理ポリシーを取り出している場合は、ポリシー サーバに接続され、ポリシーがダウンロードされます。サーバに接続するために socks とプロキシの設定が必要な場合は、それを求めるメッセージが表示されます。これらの設定は、後で使用できるように自動的に保存されます。これらの設定は、ダイアログボックスの [詳細] ページで前もって指定しておくこともできます。
5. 集中管理ポリシーを共有する認証局の証明書が使用できない場合は、その証明書を受

け入れるように求めるメッセージが表示されます。受け入れると、証明書は［ 信頼されたポリシーサーバ ］の下の鍵管理ツリーに追加されます。前もって証明書を取り出しておくこともできます。証明書のインポート方法の詳細については、「10.2.2 証明書と鍵ペアのインポート」の項を参照してください。

6. ポリシー エディタに戻った後で、［ 適用 ］または［ OK ］をクリックすると、新しいポリシーが有効になります。変更を破棄するには、［ キャンセル ］をクリックします。注記: 新しいポリシーを適用するには、そのポリシーをアクティブに設定します。詳細については、「4.2.6 ポリシーのアクティブ化」の項を参照してください。

別の方法として、ポリシー ファイルのアイコンをダブルクリックしてポリシーをインポートすることもできます。NET-G Secure VPN Client は、拡張子.spsl を持つポリシー ファイルを認識します。ファイル名拡張子への関連付けは、Web ブラウザからも有効です。ポリシーのインポートは、ダブルクリックによるポリシーの更新と同じロジックに従います。詳細については、「4.2.8 集中管理ポリシーの更新」の項を参照してください。

4.2.2. ポリシーの名前の変更

ポリシーの名前を変更するには、ポリシーを右クリックし、表示されるメニューで［ 名前の変更 ］を選択します。新しい名前を入力します。アクティブなポリシーの名前は変更できません。

4.2.3. ポリシーの削除

ポリシーを削除するには:

1. ポリシー エディタでポリシーを選択します。
2. ［ 削除 ］ボタンをクリックします。
3. 削除を確定するには、［ 適用 ］をクリックします。

アクティブなポリシーは削除できません。

4.2.4. ポリシーのエクスポート

署名付きまたは署名なしで、ポリシーをエクスポートしてファイルに保存することができます。署名に使用できるのは、ローカル ID 証明書だけです。ローカル ID 証明書が使用できない場合、エクスポート時にポリシーに署名することはできません。ローカル ID 証明書の詳細については、「9.1.3 自己署名証明書」の項を参照してください。

ポリシーをエクスポートするには:

1. ポリシーをマウスの右ボタンで選択して、表示されるメニューで [名前を付けて保存] を選択するか、または [ポリシーのプロパティ] ダイアログ ボックスの [エクスポート] ボタンをクリックします。
2. ファイルを保存するための標準のダイアログボックスが開きます。フォルダを選択し、フィールドにポリシーの名前を指定します。ファイルの種類で、[SPSL ポリシー ファイル] を選択します。
3. ポリシーに署名する場合は、[ローカル ID 証明書を使ってポリシーに署名します。] オプションを選択します。
4. [保存] をクリックして、ポリシーをエクスポートします。

4.2.5. ポリシーのローカル コピーの作成

集中管理ポリシーのローカル コピーを作成すれば、ポリシーは通常のローカル ポリシーになり、更新することができます。この操作は元に戻せません。

集中管理ポリシーのローカル コピーを作成するには、次のいずれかの操作を行います。

- ポリシーを右クリックし、表示されるメニューで [ローカル コピーを作成する] を選択します。
- [ポリシーのプロパティ] ダイアログボックスの [ローカル コピー] オプションを選択します。

4.2.6. ポリシーのアクティブ化

一度に 1 つのポリシーのみをアクティブにして適用できます。ポリシーをアクティブに設定するには、次のいずれかの操作を行います。

- ポリシー エディタを使用する場合は、アクティブにするポリシーをマウスの右ボタンで選択します。表示されるメニューで [アクティブに設定] を選択します。アクティブなポリシーでは、このメニュー項目は選択できなくなります。
- NET-G Secure VPN Client のトレイ アイコンを使用する場合は、トレイ アイコンをマウスで右クリックしてメニューを開きます。[アクティブなポリシーの選択] をマウスの左ボタンでクリックします。表示されるリストから目的のポリシーを選択します。

4.2.7. ポリシーの表示と編集

ポリシーレイヤのプロパティは、[ポリシーのプロパティ] ダイアログ ボックスで表示および編集できます。

1. 表示するポリシーを選択し、[プロパティ] ボタンをクリックしてダイアログボックスを開きます。
2. 必要な値を表示して編集します。ただし、集中管理ポリシーのコピーを更新することはできません。
3. 変更を保存するには、[OK] をクリックします。変更を破棄するには、[キャンセル] をクリックします。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシーエディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

4.2.8. 集中管理ポリシーの更新

この項では、外部ソースからポリシーを更新する方法を説明します。

集中管理ポリシーの取得

集中管理では、ポリシーを再取得して更新する間隔を指定します。標準の間隔は 4 時間です。さらに、ポリシー マネージャを再起動するたびに更新が自動的に再取得されます。[更新] ボタンをクリックして手動で更新を取得することもできます。

ダブルクリックによるポリシーの更新

ポリシー ファイルのアイコンをダブルクリックしてポリシーを更新できます。NET-G Secure VPN Client は、拡張子「spsl」「spl」を持つポリシー ファイルを認識します。ファイル名拡張子への関連付けは、Web ブラウザからも有効です。

ポリシーはサーバから再取得されます。つまり、ポリシーがインポートされ、古いポリシ

ーが新しいポリシーに置き換えられます。既存のポリシーを同じ名前の新しいポリシーに置き換えようとすると、操作を確認するメッセージが表示されます。

証明書が鍵管理にない認証局がポリシー ファイルに署名している場合は、その証明書をインポートする許可を求めるメッセージが表示されます。これを拒否すると、証明書もポリシーもインポートされません。ポリシーをインポートできる信頼されたポリシーサーバの詳細については、「4.4 信頼されたポリシー サーバ」の項を参照してください。

ポリシーに認証局の署名がない場合は、署名のないポリシーをインポートする許可を求めるメッセージが表示されます。

4.3. ポリシーのプロパティ

ポリシーのプロパティは、[ポリシーのプロパティ] ダイアログボックスの [全般] 、[詳細]、および [共有] ページに表示されます。

4.3.1. 全般プロパティ

ポリシーの種類

NET-G Secure VPN Client には、ローカルポリシーと集中管理ポリシーの 2 種類があります。

ローカル ポリシーは、ローカルで保存および保守管理するセキュリティ ポリシーです。ローカル ポリシーは、最初から新規作成することも、ファイルからインポートすることもできます。

集中管理ポリシーは、リモートで作成および保存するセキュリティ ポリシーです。ローカルホストに取り出した集中管理ポリシーは、キャッシュ コピーとしてローカルホストに表示されます。集中管理によるポリシーへのすべての変更は、ローカルホストに自動的にダウンロードされます。ローカル ホストでポリシーを更新することはできません。ポリシーは信頼されたポリシー サーバからのみ取り出すことができます。詳細については、「4.4 信頼されたポリシー サーバ」の項を参照してください。

ポリシーのソース

ポリシー サーバおよびポリシー名。

説明

ポリシーに関する短い自由形式の説明。

作成日時

ポリシーの作成日時。

変更日時

ポリシーの最終更新日時。

属性

アクティブなポリシー

これが適用されたポリシーである場合は、このボックスにチェック マークが表示されます。システムに複数のポリシーがある場合は、一度に 1 つのポリシーのみをアクティブにして適用できます。アクティブなポリシーは、ポリシー エディタで太字で表示されます。アクティブなポリシーは削除できず、名前も変更できません。

ローカル コピー

集中管理ポリシーのローカルコピーを作成するときに選択します。こうすると、ポリシーは更新可能な通常のローカルポリシーになります。この操作は元に戻せません。

読み取り専用

ポリシーが更新されないように保護するときに選択します。当然、読み取り専用のポリシーは変更できません。

4.3.2. 詳細プロパティ

プロキシと socks の設定は、サーバがファイアウォールで保護されている場合に、そのファイアウォールを通過するために使用します。これらの設定を使用するには、[設定の使用] オプションを選択します。HTTP および socks のプロキシ設定は、手動で指定できます。[自動検出] ボタンをクリックして自動的に設定を検出することもできます。

最初に集中管理ポリシーを取り出すときに、設定を指定することができます。その設定は後で使用できるように保存され、このページに表示されます。

4.3.3. プロパティの共有

ローカル ポリシーが対象の場合にのみ使用できます。

非共有

これを選択すると、他のユーザーがポリシーを共有できなくなります。

共有

これを選択すると、他のユーザーがポリシーを共有できます。リモート ホストでローカルホストのポリシーを取り出すには、リモートホストで SPRP (Simple Policy Retrieval Protocol) をサポートしている必要があります。リモート ホストでは、ローカルホストのポリシーが集中管理ポリシーとして表示されます。このポリシーをリモート ホストで変更することはできません。ローカル ホストでのポリシーへの変更はリモートホストに自動的に反映されます。

リモート LDAP サーバへ発行

これを選択すると、ポリシーがリモート LDAP サーバでダウンロードできるようになります。必要な情報を指定するには、[LDAP 設定] ボタンをクリックします。

- サーバ アドレス (ldap.mycompany.com など) を入力します。
- 基本オブジェクト識別名(DN) (“cn=Policy Server, o=dit, c=FI” など) を入力します。文字列に特殊文字が含まれる場合は、引用符で囲む必要があります。
- 必要な場合は [アクセス時のログイン情報を登録する] を選択し、ユーザー名とパスワードを入力します。

ポリシーをローカルホストで共有したり、リモート サーバに発行したりする場合は、次のようなオプションも使用できます。

説明

ポリシーに関する自由形式の説明。わかりやすい名前を付けることをお勧めします。

署名

ローカル ホストの自己署名証明書でポリシーに署名します。ローカルホストのポリシーを共有するリモート ホストでは、ローカル ホストを信頼されたポリシー サーバと見なします。

期限時間

この値は、ローカルホストのポリシーを共有するリモートホストがローカルホストから更新を取り出す間隔を示します。期限時間は、2 つの連続した更新間の最大間隔です。デフォルトでは、この値は 4 時間に設定されます。

4.4. 信頼されたポリシー サーバ

4.4.1. 信頼されたポリシー サーバとは

リモート サーバから集中管理ポリシーのコピーを取り出すには、そのリモート サーバが信頼されたポリシー サーバであることが必要です。サーバは、ポリシーをデジタル署名します。ポリシーを取り出すには、リモート サーバの証明書がローカル ホストの信頼ポリシーに必要です。

信頼されたポリシー サーバの証明書は、鍵管理ツリーの [信頼されたポリシー サーバ] ブランチに保存されます。ポリシーを取り出す場合は、このブランチの証明書のみを信頼します。したがって、IPsec で保護された接続をサーバと確立する際には、証明書を認証に使用できません。一般信頼ポリシーに証明書を追加するには、証明書を信頼された認証局またはホストに追加する必要があります。

4.4.2. 信頼されたポリシー サーバの管理

信頼されたポリシー サーバの証明書は、ポリシー エディタの [鍵管理] ページの [信頼されたポリシー サーバ] の下に表示されます。これらの証明書の管理は、他の証明書の管理とほぼ同じです。詳細については、「第 10 章 証明書」を参照してください。

第 5 章　ポリシー規則の設定

5.1. セキュリティ ポリシーの規則

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ローカルホストを保護します。NET-G Secure VPN Client 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。規則では、データ パケットを通過または停止するか、暗号化するか、認証を要求するかを決定します。認証鍵を制御する信頼ポリシーは、セキュリティ ポリシーにリンクされます。

ポリシー エディタの [セキュリティ ポリシー] ページでは、セキュリティ ポリシーの規則を表示および変更できます。サーバから共有している集中管理ポリシーは変更できません。

セキュリティ ポリシーは、次の項目で構成されます。

- 2 つの独立したトラフィック フィルタ
- IPsec トラフィック規則
- 受信 IPsec トラフィックおよび保護されていない IP トラフィックの両方を処理するデフォルト応答規則

5.1.1. トラフィック フィルタ

トラフィック フィルタ規則は、データ パケットを単に通過または停止させます。規則が影響するデータ パケットは、次のセレクタによって特徴付けられます。

- トラフィック プロトコル
- リモート ホスト (またはネットワーク) の IP アドレスとポート
- ローカル ホストのポート
- トラフィック方向: 受信、送信、または両方

規則は、次のアクションを実行します。

- データ パケットをバイパスします。バイパスされたデータ パケットは暗号化されず、規則セットの他の規則には影響されません。

- データ パケットをドロップします。データ パケットは破棄されます。
- データ パケットを拒否します。パケットは破棄され、パケットが拒否されたことを知らせるメッセージが送信元に送られます。

トラフィック フィルタでは、IPsec カプセル化を使用するデータ パケットをトラップできません。すべての状況で IPsec の転送にフィルタを適用するために、2 つの独立したフィルタを使用できます。

- IPsec 前フィルタ。IPsec 変換を実行する前に適用されます。
- IPsec 後フィルタ。IPsec 変換後に適用されます。

2 つの独立したフィルタは、混乱を生じる場合があります。この混乱を避けるために、フィルタ規則は慎重に設定する必要があります。通常、送信トラフィックには IPsec 前フィルタを適用し、受信トラフィックには IPsec 後フィルタを適用します。ただし、両方のフィルタはすべてのトラフィックに適用されます。

5.1.2. IPsec 規則

IPsec 規則には、バーチャル プライベート ネットワーク、セキュアな接続、およびセキュアなネットワークに関する規則があります。リモート ホストに対する IPsec 規則がある場合、ローカル ホストはリモート ホストとの間で送受信される IPsec で保護されたトラフィックのみを受け入れます。リモート ホストに送信されるデータ パケットは、IPsec カプセル化を含むように変換されます。リモート ホストからローカルホストに保護されていない IP パケットが送られると、IPsec ネゴシエーションが開始されます。

5.1.3. デフォルト応答規則

デフォルト応答規則は、評価できる規則が指定されていない場合に、受信データ パケットに適用されます。IPsec トラフィックと保護されていない IP トラフィックへのアクションは別個に設定されます。デフォルトの IPsec 規則には、使用する認証鍵が含まれています。保護されていない IP トラフィックへのデフォルト応答では、トラフィックがドロップまたは許可されます。トラフィックの拒否は、データ パケットの破棄を意味します。データ パケットの許可は、データ パケットがデフォルト規則をパスするが、残りの処理を拒否しないことを意味します。つまり、パケットは次に IPsec 後フィルタに転送されます。

5.2. 接続の確立

ポリシー エディタで設定した規則は、規則データベースに保存されます。これらの規則に基づいて、ポリシー マネージャはエンジンが認識するコードを作成します。エンジンは、データ パケットを検出し、データ パケットにセキュリティ ポリシーを適用します。インターネットの任意のホストに対してデータ トラフィックへのセキュアな接続規則を作成するとします。ポリシー エディタで規則を追加すると、規則は規則データベースに保存され、セキュリティ ポリシーを適用するためにエンジンで使用されるコードがポリシー マネージャによって再作成されます。

次に、エンジンのインターセプタがホストに転送されるデータ パケットをトラップするとします。規則セットから導出されたコードに基づいて、エンジンによりデータ パケットを IPsec でカプセル化する必要があることが認識されますが､その認識方法は特定されません。たとえば、エンジンでは使用する暗号化アルゴリズムは認識されず、データを暗号化する必要があるということのみが認識されます。IPsec 変換の詳細は、セキュリティの関連付け (SA) という形式でエンジンに提供されます。セキュリティの関連付けが存在しない場合、エンジンはそれを作成することをポリシー マネージャに指示します。

5.3. インターネット鍵交換

必要なセキュリティの関連付けを作成するために、ポリシー マネージャはリモート ホストとの間でインターネット鍵交換（IKE）を開始します。IKE では、通信するエンティティは開始側と応答側と呼ばれます。前者がプロセスを開始した側です。

プロセスの最初のフェーズ（IKE フェーズ 1）では、インターネット鍵交換のセキュリティの関連付け（ 略して IKE SA）が作成されます。IKE のセキュリティの関連付けが提供する保護の下で、IPsec のセキュリティの関連付けが次のステップ（IKE フェーズ 2）で確立されます。

5.4. セキュリティの関連付け

IPsec のセキュリティの関連付けは、セキュアな通信に関して、2 つの通信するエンティティ(ローカル ホストとリモート ホスト) 間で交わされる契約です。この契約では、特に使用する暗号化アルゴリズムと認証鍵について規定します。セキュリティの関連付けは常に単一方向です。したがって、通常は 2 つのセキュリティの関連付けが必要です。1 つはローカル ホストからリモートホストへの関連付けであり、もう 1 つはリモート ホストか

らローカル ホストへの関連付けです。セキュリティの関連付けをネゴシエートする場合、通信するエンティティは関連付けの有効期間も決定します。有効期間が切れると、関連付けは有効でなくなります。2 つのホスト間で通信が進行中である場合は、新しい関連付けが設定されます。

例に戻ると、セキュリティの関連付けが設定されると、ローカル ホストからリモート ホストに転送されるデータ パケットは IPsec のセキュリティの関連付けに従って IPsec でカプセル化され、リモート ホストに送信されます。

5.5. 規則の評価

規則は、ユーザーインターフェイスに表示される順に評価されます。

1. IPsec 前フィルタ
2. IPsec 規則
   a. バーチャル プライベート ネットワークの規則
   b. セキュアな接続の規則
   c. セキュアなネットワークの規則
3. デフォルト応答規則
4. IPsec 後フィルタ

5.5.1. 送信データ パケットの管理

IPsec 前フィルタ

IPsec 前フィルタは、最初に送信データ パケットに適用されます。適用結果は、次のいずれかになります。

- バイパス規則がデータ パケットに一致すると、データ パケットは他のすべての規則をパスします。
- ドロップまたは拒否規則がデータ パケットに一致すると、データ パケットは破棄されます。
- いずれの規則もデータ パケットに一致しないと、パケットは IPsec 規則に転送されます。

IPsec 規則

IPsec 規則がデータパケットに一致すると、以前に成功したネゴシエーションの結果としてセキュリティの関連付けが残っていない限り、リモート側との接続ネゴシエーションが開始されます。ネゴシエーションが成功すると、セキュリティの関連付けが確立され、データ パケットが IPsec 変換に転送されます。変換後のデータ パケットは、ESP（encapsulated security payload: カプセル化セキュリティペイロード）プロトコルとして、IPsec 後フィルタに転送されます。ネゴシエーションが失敗すると、データ パケットはドロップされます。

IPsec 規則のいずれとも一致しない場合、データ パケットはそのまま IPsec 後フィルタに転送されます。

IPsec 後フィルタ

IPsec 後フィルタは、以前の規則によってドロップまたはバイパスされなかったすべてのトラフィックに適用されます。適用結果は、IPsec 前フィルタと同じように、次のいずれかになります。

- バイパス規則がデータ パケットに一致すると、データ パケットはネットワークに渡されます。
- ドロップまたは拒否規則がデータ パケットに一致すると、データ パケットは破棄されます。
- いずれの規則もデータ パケットに一致しないと、パケットはネットワークに転送されます。

注意事項

あいまいなフィルタ規則を作成するのを避けるために、通常は IPsec 前フィルタは主に送信データ トラフィックに適用し、IPsec 後フィルタは受信データ トラフィックに適用します。

すべてのプロトコルのトラフィックをドロップすると、ESP（IPsec で保護された）パケットを含むすべてのパケットが文字どおりドロップされます。通常は、「すべてをドロップ」するような規則は作成しないようにします。

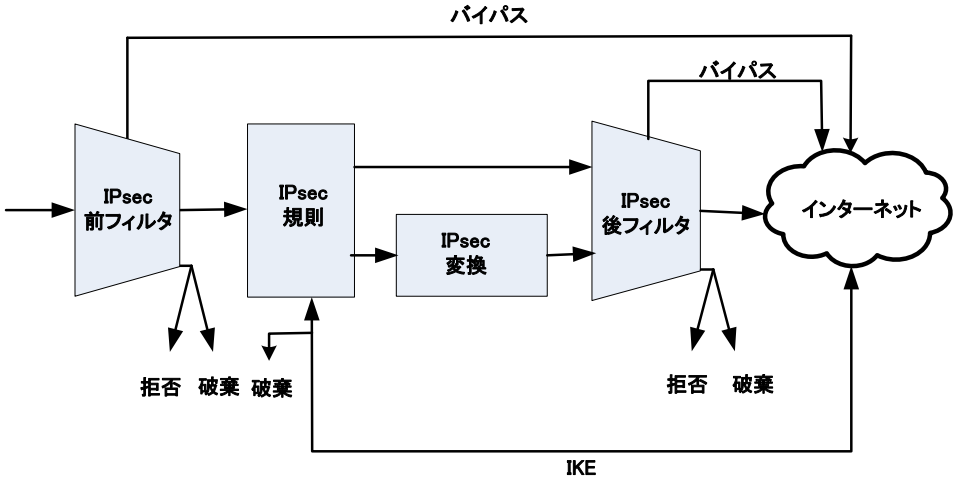

図 5-1 送信データ パケットの管理

IPsec 前フィルタですべてのプロトコルをホストにバイパスすると、パケットは IPsec 規則のテストを受けません。したがって、ホストへのセキュアな接続規則がある場合でも、トラフィックは IPsec によって保護されません。

ネゴシエーションの失敗によってパケットがドロップしても、それは送信元に報告されません。したがって、IPsec 規則の作成時点で接続の診断を実行することをお勧めします。診断では接続を確立し、その際に問題が検出されると報告されます。

IPsec の接続を確立するには、IKE ネゴシエーションの失敗は許されません。したがって、IPsec 前フィルタでは IKE トラフィック（ サービス ）をバイパスします。この規則は、ソフトウェアのインストール時に自動的に作成されます。DHCP および SPRP のパケットをバイパスする規則も、ソフトウェアのインストール時に作成されます。

5.5.2. 受信データ パケットの管理

IPsec 前フィルタ

IPsec 前フィルタは、最初に受信データ パケットに適用されます。適用結果は、次のいずれかになります。

- バイパス規則がデータ パケットに一致すると、データ パケットは他のすべての規則をパスして、TCP/IP スタックに転送されます。

- ドロップまたは拒否規則がデータ パケットに一致すると、データ パケットは破棄されます。
- いずれの規則もデータ パケットに一致しないと、パケットは IPsec 規則に転送されます。

IPsec 規則とデフォルト応答

次に、受信データ パケットは IPsec 規則のチェックを受けます。最初に、受信データ パケットが ESP プロトコルである場合について検討します。この場合、特定の規則またはデフォルト応答規則に基づく IPsec 接続がリモート ホストとの間に既に確立されています。したがって、対応するセキュリティの関連付けが存在することになり、パケットは次に IPsec のカプセル化解除と IPsec 後フィルタに転送されます。対応するセキュリティの関連付けが存在しない場合は、IPsec ネゴシエーションが開始されてセキュリティの関連付けが確立されます。ネゴシエーションが成功すると、パケットは IPsec のカプセル化を解除された後に IPsec 後フィルタに転送されます。ただし、ネゴシエーションが失敗すると、データパケットは破棄されます。

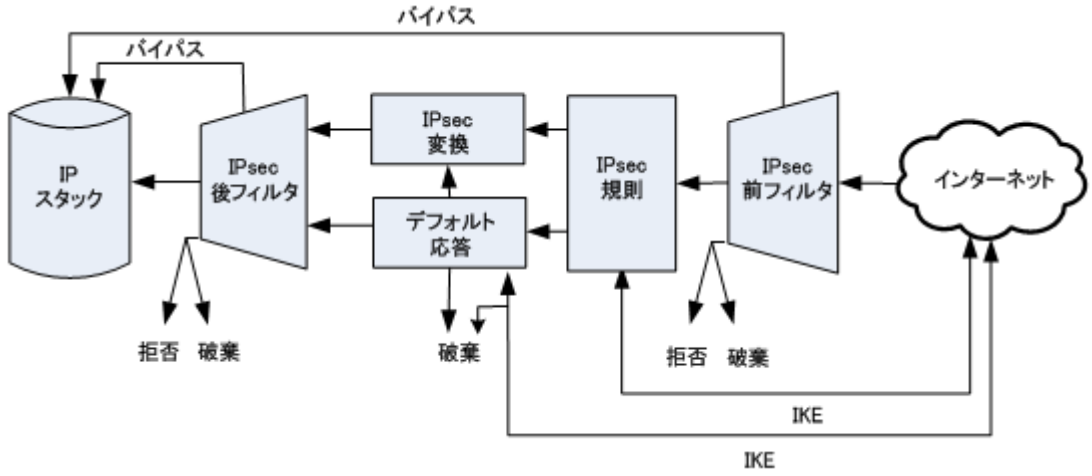

図 5-2　受信データ パケットの管理

いずれの IPsec 規則も IPsec で保護された受信データ パケットに一致しない場合は、デフォルト応答規則が評価されます。定義されたパラメータに基づいて、システムは IPsec 接続をネゴシエートします。ネゴシエーションが成功すると、パケットは IPsec のカプセル化を解除された後に IPsec 後フィルタに転送されます。ただし、ネゴシエーションが失敗すると、データ パケットは破棄されます。

IPsec 規則はあるが、保護されていない IP パケットがリモート ホストから送られると、

システムはリモート ホストとの IPsec 接続をネゴシエートします。ネゴシエーションが成功すると、セキュリティの関連付けが設定され、リモート ホストはデータ パケットを IPsec でカプセル化して再送信します。以後、パケットは通常どおりに処理され、IPsec のカプセル化を解除された後に IPsec 後フィルタに転送されます。
最後に、保護されていない IP パケットがいずれの IPsec 規則にも一致しない場合は、デフォルト応答が適用されます。デフォルト応答のアクションは、次のとおりです。

- データ パケットを拒否（ 破棄 ）します。
- データ パケットを許可（IPsec 後フィルタに転送 ）します。

IPsec 後フィルタ

カプセル化を解除した IPsec トラフィックは標準の IP パケットになるため、IPsec 後フィルタを適用できます。以前の規則でバイパスまたはドロップされなかった、保護されていないトラフィックにもフィルタが適用されます。適用結果は、IPsec 前フィルタと同じように、次のいずれかになります。

- バイパス規則がデータ パケットに一致すると、データ パケットは TCP/IP スタックに渡されます。
- ドロップまたは拒否規則がデータ パケットに一致すると、データ パケットは破棄されます。
- いずれの規則もデータ パケットに一致しないと、パケットは TCP/IP スタックに転送されます。

注意事項

ESP パケットはフィルタ規則でトラップされないため、受信 IPsec トラフィックには IPsec 後フィルタを適用する必要があります。IPsec 後フィルタは、データパケットに IPsec 変換が実行された後で評価されます。

ただし、すべてのトラフィック プロトコルに影響する規則は、ESP パケットにも影響します。したがって、IPsec 前フィルタですべてのプロトコルをドロップすると、受信 IPsec トラフィックもドロップされます。IPsec 前フィルタですべてのプロトコルを渡すと、受信 ESP パケットもそのまま TCP/IP スタックに渡されます。TCP/IP スタックでは、ESP スタックの処理方法が認識されないために、パケットはドロップされます。通常は、「すべてを渡したりドロップ」したりするような規則は作成しないようにします。

IPsec の接続を確立するには、IKE ネゴシエーションの失敗は許されません。したがって、IPsec 前フィルタでは IKE トラフィックをバイパスします。この規則は、ソフトウェアのインストール時に自動的に作成されます。DHCP および SPRP のパケットをバイパスする規則も、ソフトウェアのインストール時に作成されます。

第 6 章　トラフィック フィルタ

6.1. トラフィック フィルタとは

フィルタ規則は、IPsec が提供するパケット保護機能を補完します。IP パケットにフィルタを適用することにより、危険性が高いホストとの接続を破棄し、不要なトラフィックを排除できます。システム管理者は、トラフィックのフィルタ規則を使用してサービスへのアクセスを制限できます。

NET-G Secure VPN Client ソフトウェアのトラフィック フィルタは、伝送データ パケットに IPsec 変換を実行する前のフィルタと後のフィルタに分かれます。受信トラフィックについては、IPsec カプセル化の解除前に IPsec 前フィルタが適用され、その解除後に IPsec 後フィルタが適用されます。同じように、送信トラフィックについては、IPsec カプセル化の前に IPsec 前フィルタが適用され、カプセル化の後に IPsec 後フィルタが適用されます。
この種の設定は、IPsec で暗号化されたトラフィックにフィルタを適用するために必要です。IPsec で暗号化されたトラフィックは ESP プロトコルであるため、TCP および UDP のトラフィックを処理するフィルタ規則の影響は受けません。結果として、通常、送信トラフィックの汎用フィルタには IPsec 前フィルタが使用され、受信トラフィックには IPsec 後フィルタが使用されます。ただし、IPsec で暗号化されたトラフィックであるかどうかに関係なく、すべてのトラフィックに両方のフィルタが適用されます。どちらのフィルタでもユーザー インターフェイスと管理方法は同じです。ここでの説明は両方のフィルタに該当します。例と図には IPsec 前フィルタを使用しています。

6.2. フィルタ規則の管理

6.2.1. 規則の追加

新しいフィルタ規則を追加するには、次の手順に従います。

1. ポリシー ツリーの [IPsec 前フィルタ] ブランチを選択し、[追加] ボタンをクリックします。
2. 必要な値を入力します。詳細については、「6.3 フィルタ規則のプロパティ」の項を参照してください。
3. 変更を確定するには［OK］をクリックします。規則の追加を中止する場合は、[キャ

ンセル] をクリックすると、変更が破棄されます。

4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

6.2.2. 規則の削除

規則を削除するには:

1. ポリシー エディタで、[IPsec 前フィルタ] ブランチを展開して規則を選択します。
2. [削除] ボタンをクリックします。
3. 削除を確定するには、[OK] または [適用] をクリックします。[OK]をクリックした場合は、ポリシー エディタが閉じます。いくつかの削除をした後でも、[OK] または [適用] で変更を確定する前であれば、[キャンセル] をクリックして規則セットを復元できます。

6.2.3. 規則の表示と編集

作成したフィルタ規則のプロパティは、いつでも表示して変更できます。ただし、集中管理ポリシーの規則を更新することはできません。規則の基本リストを表示するには、[IPsec 前フィルタ] ブランチを展開します。詳細なリストを表示するには、[IPsec 前フィルタ] をダブルクリックします。

図 6-1　IPsec 前フィルタ規則の基本リスト

規則の詳細を表示して値を編集するには、次の手順に従います。

1. 規則を選択して［ プロパティ ］ボタンをクリックし、［ フィルタ規則のプロパティ ］ダイアログボックスを開きます。
2. 必要な値を表示して編集します。詳細については、「6.3 フィルタ規則のプロパティ」の項を参照してください。
3. 編集後に変更を確定するには、［ OK ］ をクリックします。変更を破棄するには、［ キャンセル ］をクリックします。いずれのボタンをクリックした場合でも、ポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、［ 適用 ］または［OK］をクリックすると、変更が有効になります。［OK］をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、［ キャンセル ］をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、［ 適用 ］または［OK］をクリックすると、これまでのすべての変更が適用され、［ キャンセル ］をクリックすると、これまでのすべての変更が破棄されます。

6.2.4. 評価順序の変更

フィルタ規則は評価順（ 上から下 ）に一覧表示されます。接続に一致する最初の規則が適用され、他の規則は評価されません。したがって、FTP 接続を全体としては拒否するが、特別なホスト host-1 の FTP 接続のみは受け入れる場合、2 つの規則を作成します。1 つの規則では host-1 からの FTP をバイパスし、もう 1 つの規則ではすべてのホストからの FTP を拒否します。全体的な拒否規則の前に、特殊なバイパス規則を評価する必要があります。

評価順序を変更するには、次の手順に従います。

1. 順序を変更する規則を選択します。ポリシーツリーの下に 2 つの矢印ボタンが表示されます。
2. 矢印ボタンを使用して規則を上下に移動します。メニュー コマンドの [上へ] と [下へ] を使用することもできます。
3. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

6.2.5. 規則の有効化と無効化

規則は無効 / 有効にすることができます。無効 / 有効にするには:

1. 規則を右クリックし、表示されるメニューで [規則が有効] を選択します。規則が有効になると、このメニュー項目の横にチェックマークが表示されます。規則を無効にすると、規則アイコンの上に × マークが表示され、チェック マークがメニューから消えます。
2. 変更を有効にするには、[適用] ボタンをクリックします。

6.2.6. 規則の監査

規則を監査するには、次のいずれかの操作を行います。

- 規則をマウスの右ボタンで選択します。表示されるメニューで [規則の監査] をクリックします。規則が監査されることを示すチェック マークが表示されます。また、規

則のアイコン上に小さい感嘆符 (!) が表示されます。または

- 規則を選択して [プロパティ] ボタンをクリックし、[規則のプロパティ] ダイアログ ボックスを開きます。[詳細] タブをクリックして、監査オプションを表示します。[この規則を監査する] オプションを選択します。[OK] をクリックして戻ります。

変更を有効にするには、[適用] ボタンをクリックします。

規則の監査を中止するには、逆の操作を行います。

- 規則をマウスの右ボタンで選択し、[規則の監査] を再び選択します。メニューからチェックマークが消え、規則のアイコン上の感嘆符も消えます。または
- [規則のプロパティ] ダイアログ ボックスの [詳細] ページで、[この規則を監査する] チェックボックスをオフにします。

変更を有効にするには、[適用] ボタンをクリックします。監査の詳細については、「14.1 監査」の項を参照してください。

6.3. フィルタ規則のプロパティ

規則のプロパティは、[フィルタ規則のプロパティ] ダイアログ ボックスの [全般] ページと [詳細] ページに表示されます。ポリシー エディタで規則を選択して [プロパティ] ボタンをクリックし、ダイアログボックスを開きます。

6.3.1. 全般プロパティ

フィルタの種類

フィルタ アクション

データ パケットに対するアクションは、バイパス、ドロップ、または拒否です。バイパスされたデータ パケットは、変更なしで TCP/IP スタック (受信パケット) またはネットワーク(送信パケット) に転送されます。トラフィックをドロップすると、データ パケットは破棄されます。トラフィックを拒否した場合もデータ パケットは破棄されます。ただし、転送が拒否されたことが送信元に知らされます。

方向

規則が影響する方向として、受信トラフィックのみ（ リモート ホストから送信されてローカル ホストで受信されるデータパケット）、または送信トラフィックのみ（ ローカル ホストから送信されてリモート ホストで受信されるデータ パケット ）を指定できます。両方向（ 受信と送信 ）を指定することもできます。

プロトコル

上位レベル（ トランスポート層 ）のプロトコル。ドロップダウンリストには、使用可能なオプションとして、udp、tcp、icmp、tcp および udp、any が表示されます。[any] を選択すると、規則は ESP（IPsec トラフィック ）を含むすべてのプロトコルのトラフィックと一致します。

ローカル エンドポイント

ポート / サービス

ローカル ホストで使用しているポートまたはサービス名。サービス（ アプリケーション）別に関連するポートは異なるため、ポートを指定することによって特定のサービスを拒否し、残りのサービスを許可できます。ポート番号（ 「10」など ）またはポート番号の範囲（ 「10-20」など ）を入力するか、サービスを選択してドロップダウン リストからポートを選択します。

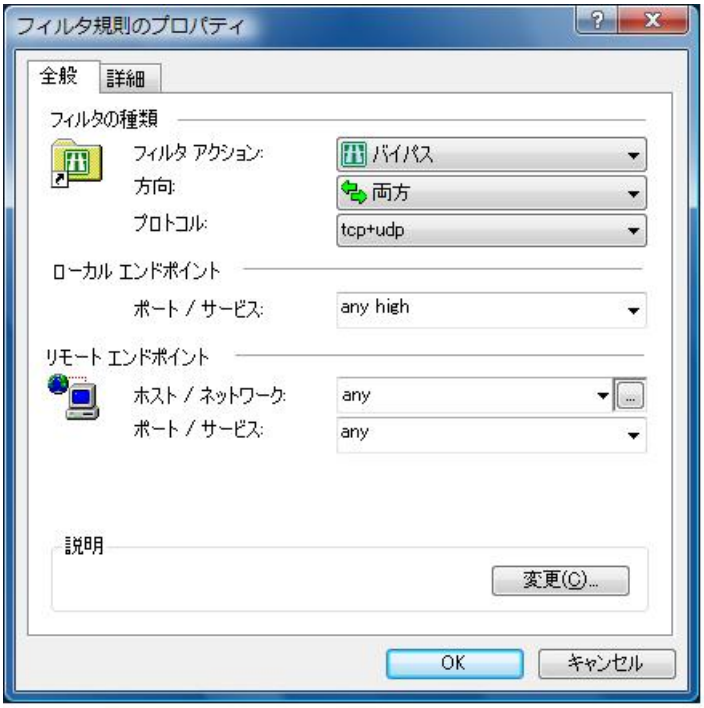

図 6-2　フィルタ規則のプロパティ

リモート エンドポイント

ホスト / ネットワーク

使用可能なネットワーク定義のリストからリモート ネットワーク（ ホスト ）を選択するか、[...] ボタンをクリックして新しいネットワークを定義します。詳細については、「6.3.3 ネットワーク エディタ」の項を参照してください。

ポート / サービス

リモート ホストで使用しているポートまたはサービス名。サービス（ アプリケーション ）別に関連するポートは異なるため、ポートを指定することによって特定のサービスを拒否し、残りのサービスを許可できます。ポート番号（ 「10」など）またはポート番号の範囲（「10-20」など ）を入力するか、サービスを選択してドロップダウン リストからポートを選択します。

説明

規則を選択したときにポリシー エディタの最下部に表示される自由形式テキスト。こ

のテキストを編集するには、[変更] ボタンをクリックし、表示されるテキスト フィールドに新しい説明を入力します。

6.3.2. 詳細プロパティ

監査オプションは、[フィルタ規則のプロパティ] ダイアログボックスの [詳細] ページに表示されます

この規則を監査する

規則を監査するには、このチェックボックスを選択します。監査の詳細については、「14.1 監査」の項を参照してください。

6.3.3. ネットワーク エディタ

内部アプリケーション用にネットワークを定義し、名前を付けるには、[ネットワーク エディタ] ダイアログ ボックスを使用します。

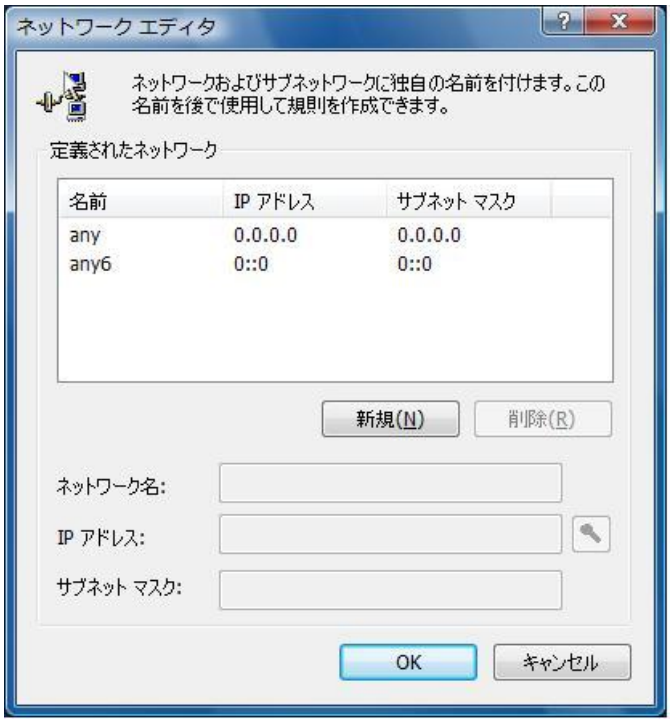

図 6-3 ネットワークエディタ

1. エディタを開くには、[フィルタ規則のプロパティ] ダイアログ ボックスの [全般]

ページで、[ホスト / ネットワーク] フィールドの右にある [...] ボタンをクリックします。

2. 定義されているネットワークが [定義されたネットワーク] ボックスに表示されます。新しいネットワークを定義するには、[新規] ボタンをクリックします。ボタンの下のテキスト フィールドがアクティブになります。
3. 必要な値を入力します。
   - ネットワーク名は、自分のみが参照するものです。わかりやすい名前を付けることをお勧めします。
   - ネットワークの IP アドレス。
   - ネットワークのサブネット マスク。
4. [OK] をクリックして新しいネットワークを追加します。変更を破棄するには、[キャンセル] をクリックします。いずれのボタンをクリックした場合でも、[フィルタ規則のプロパティ] ダイアログ ボックスに戻ります。

定義したネットワークは、設定した任意の規則で使用できます。ネットワークを削除するには、[削除] をクリックします。

第 7 章　IPsec で保護された接続

7.1.　IPsec で保護された接続とは

7.1.1.　VPN (バーチャル プライベート ネットワーク) の接続

バーチャル プライベート ネットワークとは、権限を持つユーザーが遠隔地から接続してプライベート ネットワークにアクセスするための設定を指します。プライベート ネットワークは、セキュリティ ゲートウェイで保護されます。プライベート ネットワークとやり取りされるすべてのトラフィックはセキュリティ ゲートウェイを通ります。セキュリティ ゲートウェイとユーザーのホストの間では、パブリック ネットワークを通じて接続を確立します。通常は、バーチャル プライベート ネットワークの接続を使用して、ホーム オフィスなどの遠隔地から企業内ネットワークへのアクセス、地理的に分散したオフィスの接続、ネットワークへのリモート アクセスやリモート ワーキングを実現します。

ホストとセキュリティ ゲートウェイの間には、IPsec で保護されたトンネルが作成されます。伝送データは暗号化され、通信当事者は認証されます。セキュリティの関連付けがセキュリティ ゲートウェイに結び付けられます。

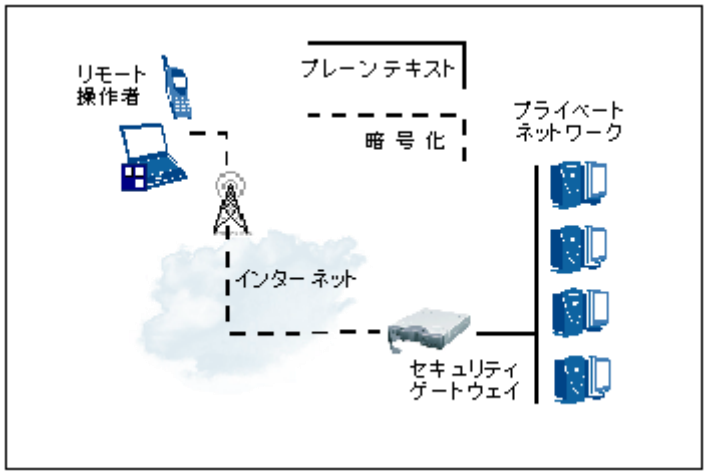

図 7-1　代表的なバーチャル プライベート ネットワークのレイアウト

7.1.2.　セキュアな接続

セキュアな接続とは、単純なピアツーピアの、IPsec で保護された接続です。通常、コンピュータのリモート管理、ファイルの転送またはダウンロード、電子メールの送受信、Web の

ブラウズ、IP テレフォニなどの重要な IP 接続は IPsec で保護されます。

リモート ホストとのセキュアな接続を確立すると、伝送データは暗号化されます。また、接続の両側が認証されます。

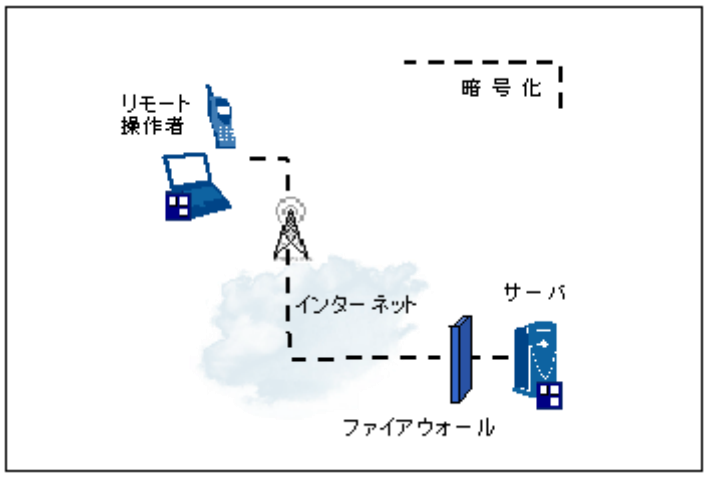

図 7-2 ピアツーピア接続のレイアウト

7.1.3. セキュアなネットワーク

セキュアなネットワークは、セキュアな接続の概念を拡張したものです。1 つのポリシー規則が、ネットワーク セグメント全体のデータ トラフィックに影響します。すべてのトラフィックは暗号化され、ホストは認証されます。セキュアなネットワークは、悪質な攻撃、認証されていないネットワーク アクセス、ネットワーク スニッフィング、およびデータの改ざんから保護します。オープンであるがために攻撃に対して脆弱な WLAN（ ワイヤレス LAN）も効果的に保護されます。

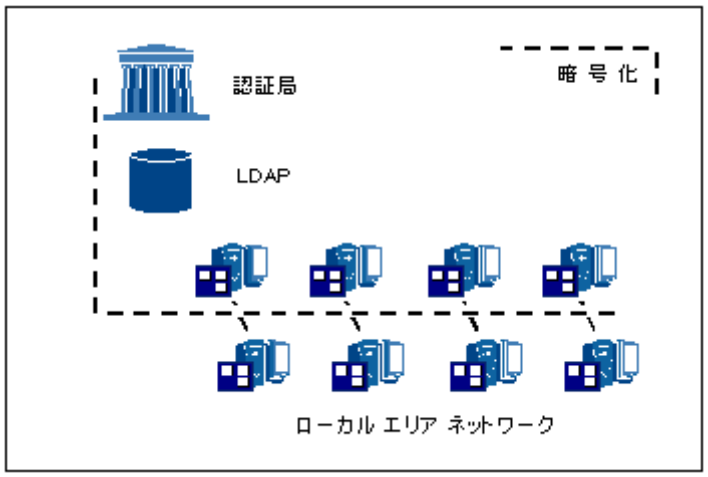

図 7-3　セキュアなネットワークのレイアウト

セキュアなネットワーク規則を適用する場合は、WINS サーバを使用して不必要なブロードキャスト トラフィックを排除することをお勧めします。Microsoft NetBIOS プロトコルは、通常、TCP ヘッダーと UDP ヘッダーにカプセル化され、IPsec 規則が適用されます。このプロトコルはトラフィックが多いため、ホスト間に IPsec/IKE ネゴシエーションの「ストーム」が発生する可能性があります。

セキュアなネットワーク規則がネットワーク セグメント全体を対象とする場合でも、接続の確立とセキュリティの関連付けのペアは個別のホストが対象です。結果として、1 つのセキュアなネットワーク規則に基づく複数の接続とセキュリティの関連付けのペアが同時に存在する場合があります。

7.2.　接続規則の管理

7.2.1.　VPN 接続規則の追加

バーチャル プライベート ネットワークの新しい接続規則を追加するには、次の手順に従います。

1. ポリシー ツリーで［VPN 接続 ］を選択し、［ 追加 ］ボタンをクリックします。
2. ［VPN 接続を追加 ］ダイアログボックスが開きます。必要な値を入力します。
   - リモート セキュリティ ゲートウェイのドメイン名または IP アドレス。右のボタンを使用してホスト名と IP アドレスを切り替えることができます。
   - 定義されたネットワークのリストからリモート ネットワークを選択します。ネットワークが定義されていない場合は、［ ... ］ボタンをクリックしてネットワークに

名前を付けます。詳細については、「7.3.7 ネットワーク エディタ」の項を参照してください。

- ホストを認証するための認証鍵を選択します。

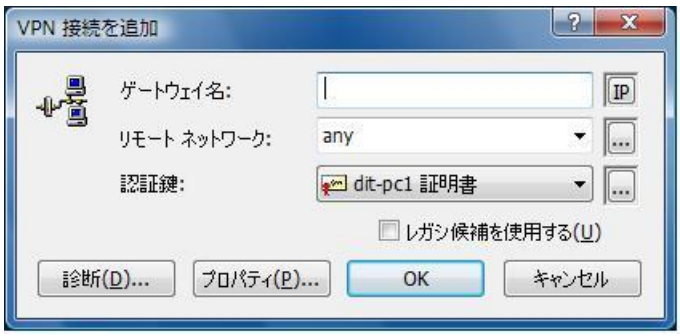

図 7-4 バーチャル プライベートネットワーク接続への規則の追加

3. 候補の短い形式を使用する場合は、[レガシ候補を使用する] オプションを選択します。規則のプロパティをより詳細に指定するには、[プロパティ] ボタンをクリックします。詳細については、「7.3 規則のプロパティ」の項を参照してください。接続をテストする場合は、[診断] をクリックします。この段階では常に接続を診断することをお勧めします。詳細については、「7.2.6 接続のテスト」の項を参照してください。[OK] をクリックして続行します。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

7.2.2. セキュアな接続規則の追加

セキュアな接続規則を新しく追加するには、次の手順に従います。

1. ポリシー ツリーで [セキュアな接続] を選択し、[追加] ボタンをクリックします。
2. [セキュアな接続を追加] ダイアログ ボックスが開きます。必要な値を入力します。
   - リモート ホストのドメイン名または IP アドレス。右のボタンを使用してホスト名と IP アドレスを切り替えることができます。
   - ホストを認証するための認証鍵。

図 7-5　新しいピアツーピアのセキュアな接続の追加

3. 規則のプロパティを詳細に指定するには、[プロパティ] ボタンをクリックします。詳細については、「7.3 規則のプロパティ」の項を参照してください。[診断] ボタンをクリックして接続をテストします。この段階で接続を診断することをお勧めします。詳細については、「7.2.6 接続のテスト」の項を参照してください。[OK] をクリックして続行します。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

7.2.3. セキュアなネットワーク規則の追加

セキュアなネットワーク規則を新しく追加するには、次の手順に従います。

1. ポリシー ツリーで [セキュアなネットワーク] を選択し、[追加] ボタンをクリックします。
2. [セキュアなネットワークを追加] ダイアログ ボックスが開きます。必要な値を入力します。
   - 定義されたネットワークのリストからネットワークを選択します。新しいネットワークを定義するには、[...] ボタンをクリックします。詳細については、「7.3.7 ネットワークエディタ」の項を参照してください。
   - ホストを認証するための認証鍵。

図 7-6 セキュアなネットワーク規則の追加

3. 規則のプロパティをより詳細に指定するには、[プロパティ] ボタンをクリックします。詳細については、「7.3 規則のプロパティ」の項を参照してください。[OK] をクリックして続行します。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシーエディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

7.2.4. 規則の削除

規則を削除するには:

1. ポリシー エディタで、対応するブランチ ([VPN 接続]、[セキュアな接続]、または [セキュアなネットワーク]) を展開し、規則を選択します。
2. [削除] ボタンをクリックします。
3. 削除を確定するには、[OK] または [適用] をクリックします。[OK]をクリックした場合は、ポリシー エディタが閉じます。いくつかの削除をした後でも、[OK] または [適用] で変更を確定する前であれば、[キャンセル] をクリックして規則セットを復元できます。

7.2.5. 規則の表示と編集

作成した接続規則のプロパティは、いつでも表示および変更できます。ただし、集中管理ポリシーの規則を更新することはできません。規則の基本リストを表示するには、対応するブランチ ([VPN 接続]、[セキュアな接続]、または [セキュアなネットワーク]) を展開します。より詳細なリストを表示するには、ブランチをダブルクリックします。規則

の詳細を表示して値を編集するには、次の手順に従います。

図 7-7　セキュアな接続規則の基本リスト

1. 規則を選択して［ プロパティ ］ボタンをクリックし、［ 規則のプロパティ ］ダイアログ ボックスを開きます。
2. 必要な値を表示して編集します。詳細については、「7.3 規則のプロパティ」の項を参照してください。［ 全般 ］タブと［ 詳細 ］タブをクリックして 2 つのページを切り替えることができます。
3. 編集後に変更を確定するには、［ OK ］をクリックします。変更を破棄するには、［ キャンセル ］をクリックします。いずれのボタンをクリックした場合でも、ポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、［ 適用 ］または［OK］をクリックすると、変更が有効になります。［OK］をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、［ キャンセル ］をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、［ 適用 ］または［OK］をクリックすると、これまでのすべての変更が適用され、［ キャンセル ］をクリックすると、これまでのすべての変更が破棄されます。

規則を更新した場合は、対応するセキュリティの関連付けに変更を反映する必要があります。その場合、［ 適用 ］または［OK］をクリックして規則の変更を確定すると、以前の対

応するセキュリティの関連付けは破棄されます。

7.2.6. 接続のテスト

バーチャル プライベートネットワークまたはセキュアな接続をテストするには、診断を実行します。

1. ポリシー エディタで規則を選択します。
2. [診断] ボタンをクリックします。
3. 完了すると、診断の結果が表示されます。診断が成功すると、確立された接続のパラメータが表示されます。診断が失敗すると、失敗の原因が表示されます。

接続の診断は規則の作成時に実行することをお勧めします。接続を実際に確立するときにネゴシエーションの失敗によってパケットがドロップしても、その事実はユーザーに通知されません。

診断では、通常の接続ネゴシエーションが実行されます。ただし、そのネゴシエーションの結果として作成されるセキュリティの関連付けは、直ちに破棄されます。また、診断の実行時にセキュリティの関連付けが存在すると、その関連付けは破棄されます。

7.2.7. 規則の有効化と無効化

規則は無効 / 有効にすることができます。無効 / 有効にするには:

1. 規則を右クリックし、表示されるメニューで [規則が有効] を選択します。規則が有効になると、このメニュー項目の横にチェックマークが表示されます。規則を無効にすると、規則アイコンの上に × マークが表示され、チェック マークがメニューから消えます。
2. 変更を有効にするには、[適用] ボタンをクリックします。

7.2.8. 規則の監査

規則を監査するには、次のいずれかの操作を行います。

- 規則をマウスの右ボタンで選択します。表示されるメニューで [規則の監査] をクリックします。規則が監査されることを示すチェック マークが表示されます。また、規

則のアイコン上に小さい感嘆符 (!) が表示されます。または

- 規則を選択して [プロパティ] ボタンをクリックし、[規則のプロパティ] ダイアログ ボックスを開きます。[詳細] タブをクリックして、監査オプションを表示します。[この規則を監査する] オプションを選択します。[OK] をクリックして戻ります。

変更を有効にするには、[適用] ボタンをクリックします。

規則の監査を中止するには、逆の操作を行います。

- 規則をマウスの右ボタンで選択し、[規則の監査] を再び選択します。メニューからチェックマークが消え、規則のアイコン上の感嘆符も消えます。または
- [規則のプロパティ] ダイアログ ボックスの [詳細] ページで、[この規則を監査する] チェックボックスをオフにします。

変更を有効にするには、[適用] ボタンをクリックします。監査の詳細については、「14.1 監査」の項を参照してください。

7.2.9. VPN 接続を開いて終了する

NET-G Secure VPN Client のトレイ メニューから VPN 接続を開くことができます。

1. Windows タスク バーのアプリケーション アイコンをマウスの右ボタンでクリックし、NET-G Secure VPN Client のトレイ メニューを開きます。
2. [VPN 接続の選択] を選択し、さらに開く VPN 接続を選択します。これで接続が開きます。接続が開かない場合は、エラー メッセージが表示されます。

ポリシー マネージャの起動時に自動的に VPN 接続を開くように設定するには、[規則のプロパティ] ダイアログ ボックスの [詳細] ページで [起動時に開く] オプションを選択します。同時に開くことができるのは、仮想アダプタを使用する 1 つの VPN 接続のみです。複数を開こうとすると、ソフトウェアは予測しない動作をする場合があります。仮想 IP アドレスと仮想アダプタの詳細については、「7.3.5 仮想 IP アドレス」の項を参照してください。

ポリシー マネージャがシャットダウンされると、VPN 接続は自動的に閉じます。

7.3. 規則のプロパティ

規則のプロパティは、[規則のプロパティ] ダイアログ ボックスの [全般] ページと [詳細] ページに表示されます。ポリシー エディタで規則を選択して [プロパティ] ボタンをクリックし、ダイアログ ボックスを開きます。

7.3.1. 全般プロパティ

図 7-8 VPN (バーチャルプライベート ネットワーク) 接続の全般プロパティ

リモート エンドポイント

ゲートウェイ

VPN 接続のみ。セキュリティ ゲートウェイのドメイン名または IP アドレス。テキスト ボックスの右のボタンを使用してドメイン名と IP アドレスを切り替えることができます。

リモート ネットワーク

VPN 接続のみ。リモートネットワークの名前。ネットワークに名前を付けて定義する

場合は、[...] ボタンをクリックしてエディタを開きます。詳細については、「7.3.7 ネットワーク エディタ」の項を参照してください。

ホスト

セキュアな接続のみ。リモート ホストのドメイン名または IP アドレス。テキストボックスの右のボタンを使用してドメイン名と IP アドレスを切り替えることができます。

ネットワーク

セキュアなネットワークのみ。リモート ネットワークの名前。ネットワークに名前を付けて定義する場合は、[...] ボタンをクリックしてエディタを開きます。詳細については、「7.3.7 ネットワーク エディタ」の項を参照してください。

IPsec / IKE 候補

認証鍵

ホストを認証するための認証鍵を、使用可能な鍵のリストから選択します。使用可能な鍵には、証明書と既知共有鍵の両方が含まれています。認証鍵に関する詳細については、「第 9 章 認証鍵の管理」を参照してください。

候補テンプレート

通常は、標準候補［normal］を使用します。標準候補には、NET-G Secure VPN Client によってサポートされている各パラメータのすべての値が含まれています。長い候補を処理できない一部の IPsec ソフトウェア製品のために、NET-G Secure VPN Client は短い形式の候補もサポートしています。レガシ候補［ legacy ］には、各パラメータの別の値がごくわずか含まれています。パラメータ候補を表示するには、[設定] ボタンをクリックします。詳細については、「7.3.3 パラメータ候補」の項を参照してください。

仮想 IP アドレスの取得

VPN 接続のみ。接続先のプライベートネットワークから仮想 IP アドレスを取得し、

そのネットワークとのシームレスな統合を実現するときに選択します。設定を指定するには、[設定] ボタンをクリックします。詳細については、「7.3.5 仮想 IP アドレス」の項を参照してください。

拡張認証を要求する

VPN 接続のみ。セキュリティ ゲートウェイがログインを要求するかどうかを選択します。ログイン情報を指定するには、[設定] ボタンをクリックします。詳細については、「7.3.6 拡張認証」の項を参照してください。

説明

規則を選択したときにポリシー エディタの最下部に表示される自由形式テキスト。このテキストを編集するには、[変更] ボタンをクリックし、表示されるテキスト フィールドに新しい説明を入力します。

7.3.2. 詳細プロパティ

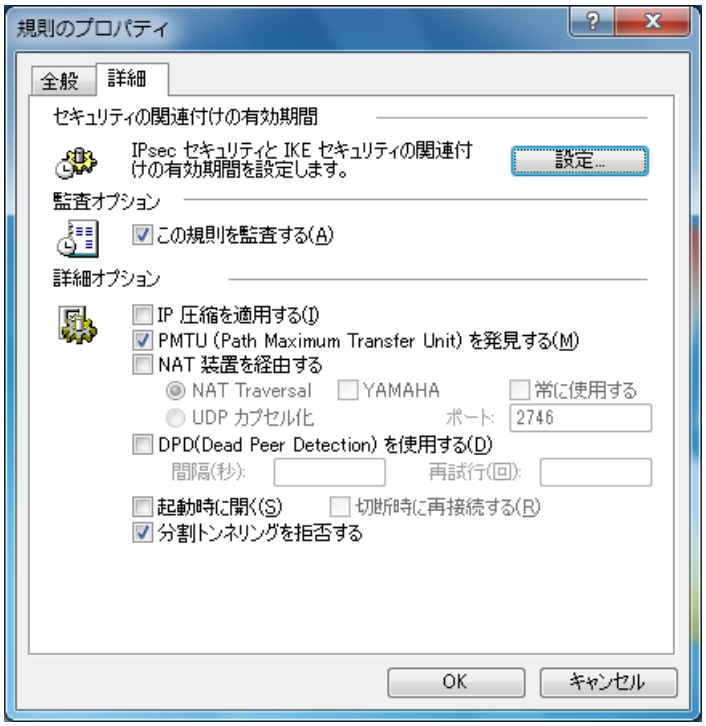

図 7-9 VPN (バーチャルプライベート ネットワーク) 接続の詳細プロパティ

セキュリティの関連付けの有効期間

IKE および IPsec に関するセキュリティの関連付けの有効期間を制御するには、[設定] ボタンをクリックします。詳細については、「7.3.4 セキュリティの関連付けの有効期間」の項を参照してください。

監査オプション

規則を監査するには、[この規則を監査する] チェック ボックスをオンにします。監査の詳細については、「14.1 監査」の項を参照してください。

詳細オプション

IP 圧縮を適用する

このオプションを選択すると、各データ パケットが圧縮されて転送されます。その結果、転送が高速化されます。転送先も圧縮をサポートしている場合にのみ圧縮が実行されます。NET-G Secure VPN Client は、IP の deflate 圧縮をサポートしています。

PMTU (Path Maximum Transfer Unit) を発見する

データの断片化を避けるために、転送単位の最大サイズを確認します。接続を通じて転送できるデータ パケットのサイズがシステムによって確認されます。次に、データ パケットが最大サイズで送信されます。データは最少数のパケットで配布されるため、転送が高速化され、エラーの発生率も低下します。

NAT 装置を経由する

NAT (Network Address Translation: ネットワーク アドレス変換) とは、IP アドレスを特定のネットワークから別のネットワークの形式に変換する方法です。プライベート アドレスを使用するプライベート ネットワークからインターネットに接続するときなどに、この変換が必要になります。ただし、従来のプライベート ネットワークのソリューションは、セキュリティ上の問題があるために、ネットワーク アドレス変換に対応できません。

NAT-Traversal (Network Address Transformation Traversal)

NAT-T プロトコルを適用している NAT デバイスをバイパスします。この機能の実装は RFC3947 および RFC3948 に基づいています。

YAMAHA

YAMAHA ルータの RFC3947 の実装と、NET-G Secure VPN Client のバージョン 2.3.x における RFC3947 の実装には同じ誤りが存在しました。NET-G バージョン 2.4.x では、この実装の誤りを修正したため、これらの機器との接続性に問題が発生することとなりました。このオプションを使用すると、これらの機器と接続するために古い実装を使用します。

常に使用する

このオプションを選択すると、NAT 装置を経由していないと判断できる場合にも、NAT 装置を経由している場合と同様にカプセル化を行います。これにより ESP パケットを通過しない経路を使用していても IPsec 通信が可能となります。ただし、対向の機器によっては動作しないこともあります。

UDP カプセル化

送信したデータパケットを UDP ヘッダーでカプセル化して、NAT デバイスをバイパスします。フィールドにポートを指定します。この実装は、IETF ドラフト「IPsec ESP Encapsulation in UDP for NAT Traversal (draft-huttunen-ipsec-esp-in-udp-00)」に基づいています。
このオプションを使用するためには、相手側も同じ機能を有し、それを使用することが必要です。

起動時に開く

VPN 接続のみ。このオプションを選択すると、ポリシー マネージャの起動時にバーチャル プライベート ネットワーク接続を自動的に開くことができます。仮想アダプタを使用する 1 つの VPN 接続のみを一度に開くことができます。VPN 接続はトレイ メニューから開いて閉じることができます。仮想 IP アドレスと仮想アダプタの詳細については、「7.3.5 仮想 IP アドレス」の項を参照してください。

切断時に再接続する

VPN 接続のみ。このオプションを選択すると、何らかの問題でバーチャル プライベート ネットワーク接続が切断された場合に自動的に再接続を行います。

DPD (Dead Peer Detection) を使用する

VPN 接続のみ。対向機器が DPD をサポートしているとき、このオプションを使用すると、「間隔（秒)」で指定された時間の間対向機器からのデータ受信がなかったときに、対向機器に対して問い合わせを送信します。問い合わせは「間隔（秒)」ごとに「回数(回)」だけ再送され、対抗機器からの応答がないときは接続を切断します。この機能を使用すると、対向機器が RFC3706 DPD に対応しているときに対抗機器との間の通信障害を検出することが可能となります。

分割トンネルを拒否する

VPN 接続のみ。このオプションを選択すると、保護されていないすべてのトラフィックは拒否されます。実際には、デフォルト応答規則の後に、追加のドロップ規則をトラフィック フィルタに挿入します。このドロップ規則により、保護されていないすべての送受信パケットは拒否されます。

7.3.3. パラメータ候補

IKE および IPsec のパラメータ候補を制御するには:

1. ポリシー エディタで規則を選択し、[プロパティ] ボタンをクリックします。[全般] ページで、[IKE / IPsec 候補] というタイトルの下の [設定] ボタンをクリックし、[パラメータ候補] ダイアログ ボックスを開きます。
2. 必要な値を設定します。各パラメータの代替値の数は、選択する候補テンプレートに応じて異なります。標準候補にはすべての値が含まれ、レガシ候補には制限された数の値のみが含まれています。テンプレートを選択するには、[規則のプロパティ] ダイアログボックスの [全般] ページを使用します。
3. 選択した値のみに候補のサイズを制限し、ダイアログ ボックスに表示するには、[選択した値のみ候補に加える] オプションを選択します。このオプションを選択しないと、すべての値が候補に含まれ、選択する内容は最初に優先される値として扱われます。

4. 変更を確定して戻るには［OK］をクリックします。[キャンセル] をクリックすると、変更は破棄されます。

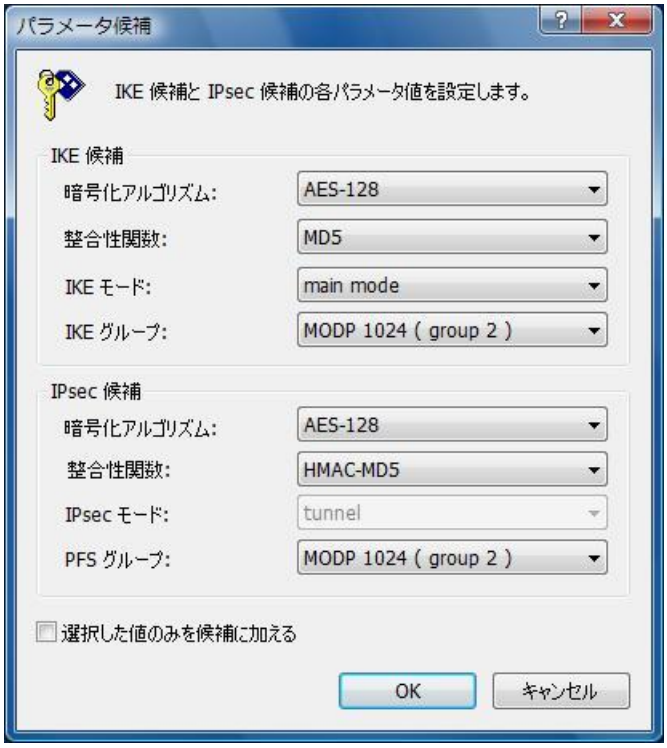

図 7-10 パラメータ候補

IKE 候補

パラメータ候補	標準候補	レガシ候補
暗号化アルゴリズム	AES,Twofish,Blowfish, CAST,3DES,DES	3DES, DES
整合性関数	MD5,SHA-1	MD5,SHA-1
IKE モード	main, aggressive	main, aggressive
IKE グループ	MODP 768(group 1) MODP 1024(group 2) MODP 1536(group 5)	MODP 768(group 1) MODP 1024(group 2) MODP 1536(group 5)

暗号化アルゴリズム

メッセージを暗号化するためのアルゴリズム。アルゴリズムごとに強さが異なります。通常、AES が最も強力で DES が最も弱いと考えられています。

整合性関数

整合性を確保するために、ハッシュ関数を使用してチェックサムを計算し、データパケットが伝送中に変更されているかどうかを確認します。

IKE モード

IKE（ Internet Key Exchange: インターネット鍵交換 ）には、main mode と aggressive mode の 2 つのモードがあります。aggressive mode は高速であり、main mode は柔軟性と成功率に優れています。

IKE グループ

接続をネゴシエートする際に、通信当事者はデータを暗号化するための実際の鍵も決定します。鍵は、各当事者の秘密鍵とランダムなデータに基づきます。ランダムなデータの生成は、プール ビットに基づきます。IKE グループは、基本的にプール ビット数を示します。プールビット数が多いほど、数値が大きくなります。数値が大きいほど、解読が困難になります。結果として、プール ビット数が多いほど、よりセキュアになります。

IPsec 候補

パラメータ候補	標準候補	レガシ候補
暗号化アルゴリズム	AES,Twofish,Blowfish, CAST,3DES,DES	3DE,DES
整合性関数	HMAC-MD5, HMAC-SHA-1	HMAC-MD5,HMAC-SHA-1
IPsec モード	transport, tunnel	transport, tunnel
PFS グループ	none	none
	MODP 768(group 1)	MODP 768(group 1)
	MODP 1024(group 2)	MODP 1024(group 2)
	MODP 1536(group 5)	MODP 1536(group 5)

暗号化アルゴリズム

メッセージを暗号化するためのアルゴリズム。アルゴリズムごとに強さが異なります。通常、AES が最も強力で DES が最も弱いと考えられています。

整合性関数

整合性を確保するために、ハッシュ関数を使用してチェックサムを計算し、データパケットが伝送中に変更されているかどうかを確認します。

IPsec モード

transport mode と tunnel mode の 2 つがあります。バーチャル プライベート ネットワーク接続では、tunnel mode のみを使用できます。

PFS グループ

PFS (Perfect Forward Secrecy) グループは、Diffie-Hellman 鍵交換のプール ビット数を示します。プール ビット数が多いほど動作は遅くなりますが、よりセキュアになります。

[選択した値のみを候補に加える] オプションを選択すると、このダイアログボックスに表示された値 (パラメータにつき 1 つの値) のみが候補に含まれます。この候補は、非常に短くなります。

候補とは

接続パラメータについて合意するには、インターネット鍵交換 (IKE) を実行します。ネゴシエーションの結果として、IKE および IPsec のセキュリティの関連付け (SA) が確立されます。候補とは、ネゴシエーションの土台となる提案です。候補には、ローカル ホストがパラメータ別にサポートしているすべての値が含まれます。たとえば、NET-G Secure VPN Client は複数の暗号化アルゴリズムをサポートしています。NET-G Secure VPN Client には、候補のすべてのアルゴリズムが含まれており、リモート ホストが特定のアルゴリズムを選択するまで各アルゴリズムを順に提案します。

7.3.4. セキュリティの関連付けの有効期間

確立された IKE および IPsec のセキュリティの関連付けを制御するには:

1. ポリシー エディタで規則を選択し、[プロパティ] ボタンをクリックします。[詳細]

ページで、[セキュリティの関連付けの有効期間] というタイトルの下の [設定] ボタンをクリックし、[セキュリティの関連付けの有効期間] ダイアログ ボックスを開きます。

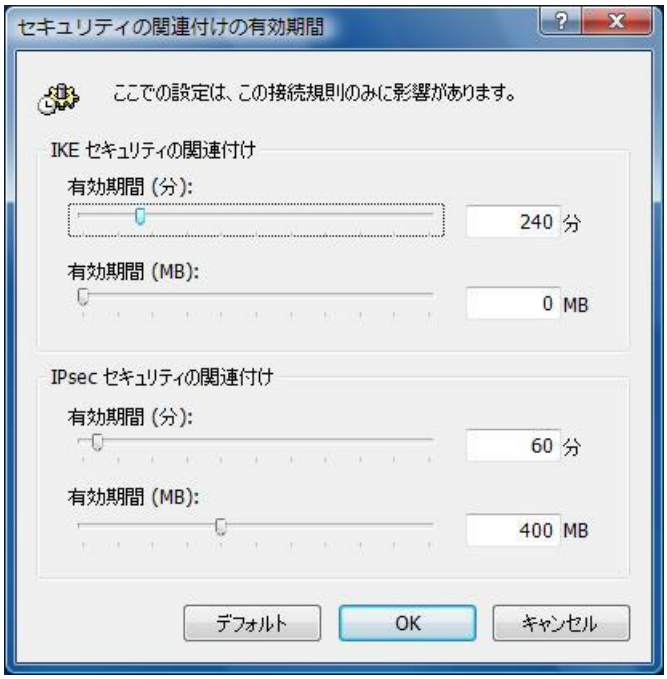

図 7-11　セキュリティの関連付けの有効期間

2. 値を設定するには、スライダを使用するか、対応するフィールドに数値を入力します。IKE と IPsec には、セキュリティの関連付けに関する独立したコントロールがあります。ただし、両者のコントロールは似ています。有効期間は、経過時間 (分) または転送データのサイズ (MB) で制御します。いずれかの限度に達すると、既存のセキュリティの関連付けが破棄され、その結果新しい関連付けが確立されます。デフォルト値に戻すには、[デフォルト] ボタンをクリックします。設定は、該当する接続規則とその対応するセキュリティの関連付けにのみ影響します。
3. 変更を確定して戻るには［OK］をクリックします。[キャンセル] をクリックすると、変更は破棄されます。

セキュリティの関連付けとは

セキュリティの関連付け (SA) は、インターネット鍵交換 (IKE) の結果として確立されます。プロセスの最初のフェーズ（IKE フェーズ 1）では、インターネット鍵交換のセキュリティの関連付け (略して IKE SA）が作成されます。IKE のセキュリティの関連付けが提供する保護の下で、IPsec のセキュリティの関連付けが次のステップ（IKE フェーズ 2）

で確立されます。

IPsec のセキュリティの関連付けは、セキュアな通信に関して、通信するエンティティ（ ローカル ホストとリモート ホスト ）間で交わされる契約です。この契約では、特に使用する暗号化アルゴリズムと認証鍵について規定します。

セキュリティの関連付けは常に単一方向です。したがって、通常は双方向のセキュリティの関連付けが必要です。1 つはローカル ホストからリモート ホストへの関連付けであり、もう 1 つはリモート ホストからローカル ホストへの関連付けです。セキュリティの関連付けをネゴシエートする場合、通信エンティティは関連付けの有効期間も決定します。有効期間が切れると、関連付けは有効でなくなります。2 つのホスト間で通信が進行中である場合は、新しい関連付けが設定されます。

ポリシー マネージャがシャットダウンすると、セキュリティの関連付けは終了し、アクティブなピアが通知されます。

7.3.5. 仮想 IP アドレス

バーチャル プライベートネットワークの接続規則にのみ適用可能。

プライベート ネットワークから仮想 IP アドレスを取得するには:

1. ポリシー エディタで規則を選択し、[プロパティ] ボタンをクリックします。[全般] ページの [仮想 IP アドレスを取得する] オプションを選択します。
2. [設定] ボタンをクリックし、[仮想 IP アドレス] ダイアログ ボックスを開いて必要な値を指定します。
3. IP アドレスを動的に割り当てるには、[IKE 設定モード] を選択します。IKE 設定モードがセキュリティ ゲートウェイでサポートされていない場合は、手動でアドレスを指定します。
4. [OK] をクリックして戻ります。

仮想 IP アドレスとは

リモート プライベート ネットワークとのシームレスな仮想の統合を達成するには、そのネットワークのアドレス空間から未使用の IP アドレスを取得して使用します。この高度な統合を実現するために、NET-G Secure VPN Client はリモート ネットワークに直接接

続しているように見える別のネットワーク インターフェイスを作成します。アダプタはリモート ネットワークに物理的には接続されていませんが、接続されているように見えるネットワーク インターフェイスをローカル コンピュータに提供します。この種のネットワーク アダプタは仮想アダプタと呼ばれます。アダプタの設定は、[コントロール パネル] の [ネットワーク接続] をダブルクリックして確認できます。ただし、その設定内容は変更しないでください。

NET-G Secure VPN Client は、仮想 IP アドレスをホストに動的に割り当てるために、IKE 設定モードをサポートしています。さらに、フォールバック オプションとして、仮想 IP アドレスを手動で指定することもできます。

NET-G Secure VPN Client の現在のバージョンでは、仮想アダプタの数は 1 つに制限されています。実際には、この制限により仮想アダプタを使用して一度に開くことができるバーチャルプライベートネットワークの接続は 1 つのみです。ただし、通常は 1 つの接続で十分です。

IKE 設定モード

通常、IKE 設定モードは Cisco や Nortel などのさまざまなベンダのデバイスと通信するときに仮想 IP アドレスを取得するために使用します。このプロトコルは IKE フェーズ 1.5 とも呼ばれ、さまざまな接続パラメータを設定したり、仮想 IP アドレスを VPN クライアントに割り当てるために使用できます。プライベート ネットワークと通信する場合、VPN クライアントはネイティブの IPsec トンネル モードを使用します。

このプロトコルの普及は鈍化しています。ベンダが実装している標準のドラフト バージョンが古くて統一もされていないために相互運用性の問題が発生することが原因です。NET-G Secure VPN Client は、最新のバージョンをサポートしており、Cisco のデバイスの実装を基準としてテストしています。

手動での指定

上に示したいずれのプロトコルもセキュリティ ゲートウェイでサポートされていない場合は、仮想 IP アドレスを手動で指定します。アドレスを手動で指定する場合に、セキュリティ ゲートウェイの一部の機能を必要とします。これらの機能は、一部の静的なルート エントリを追加するためと、プロキシ ARP を行うために使用します。

図 7-12 仮想 IP アドレスを割り当てるためのプロトコルの選択

7.3.6. 拡張認証

バーチャルプライベートネットワークの接続規則にのみ適用可能。拡張認証のログイン情報を指定するには:

1. ポリシー エディタで規則を選択し、[プロパティ] ボタンをクリックします。[全般] ページの [拡張認証] オプションを選択します。
2. [設定] ボタンをクリックし、[拡張認証] ダイアログ ボックスを開いてログイン情報を指定します。
3. オプションの選択
   - 必要に応じてログインを確認するメッセージを表示する場合は、[ログインの確認] オプションを選択します。
   - ログイン情報を自動的に送信する場合は、
   - [ログイン情報を自動的に送信する] オプションを選択します。目的のフィールドにログイン名とパスワードを指定します。
4. VPN ゲートウェイがこの機能をサポートしている場合は、[認証方法の種類を使用する] チェック ボックスをオンにします。クライアントとゲートウェイは、拡張認証を適用するかどうかと、適用する場合の実行方法についてネゴシエートします。

5. 必要に応じて、[２要素（SecurID）認証を使用する] を選択します。
6. [OK] をクリックして戻ります。

[ログインの確認] オプションを選択すると、セキュリティ ゲートウェイで拡張認証が必要になったときに、ダイアログ ボックスが表示されます。このダイアログ ボックスに、ユーザー名とパスワードを入力します。このダイアログ ボックスでは、[このユーザー名とパスワードを保存する] オプションを選択できます。入力するユーザー名とパスワードは、後でこの VPN 接続の拡張認証で自動的に使用されます。ユーザー名とパスワードが有効でない場合のみ、ログインを確認するメッセージが表示されます。

拡張認証とは

一部のセキュリティ ゲートウェイは、リソースにアクセスするためにログインを要求します。NET-G Secure VPN Client では、ログイン情報を自動的に送信するか、ログインを確認するメッセージを表示することができます。

7.3.7. ネットワーク エディタ

バーチャルプライベートネットワークの接続規則とセキュアなネットワーク規則にのみ適用可能。内部アプリケーション用にネットワークを定義し、名前を付けるには、[ネットワーク エディタ] ダイアログ ボックスを使用します。

1. ポリシー エディタで規則を選択し、[プロパティ] ボタンをクリックします。[全般] ページで、[ネットワーク] フィールドの右にある [...] ボタンをクリックします。
2. 定義されているネットワークが [定義されたネットワーク] ボックスに表示されます。新しいネットワークを定義するには、[新規] ボタンをクリックします。ボタンの下のテキスト フィールドがアクティブになります。
3. 必要な値を入力します。
   - ネットワーク名は、自分のみが参照するものです。わかりやすい名前を付けることをお勧めします。
   - ネットワークの IP アドレス。
   - ネットワークのサブネット マスク。
4. [OK] をクリックして新しいネットワークを追加します。変更を破棄するには、[キャンセル] をクリックします。いずれのボタンをクリックした場合でも、[規則のプロパティ] ダイアログボックスに戻ります。

定義したネットワークは、設定した任意の規則で使用できます。ネットワークを削除するには、[削除] をクリックします。

第 8 章　デフォルト応答規則

8.1. デフォルト応答規則とは

デフォルト応答規則は、評価できる規則が指定されていない場合に、送信および受信データパケットに適用されます。IPsec と保護されていない IP トラフィックへの応答は別個に設定します。

送信パケットの場合、デフォルト応答規則は IP トラフィック処理（「8.4 IP トラフィック処理」の項を参照 ）を評価しますが、IPsec のカプセル化は行いません。受信 ESP パケットはカプセル化が解除されます。受信プレーン テキストトラフィックの場合、IP トラフィック処理によってパケットを許可するか拒否するかが決められます。

8.2. デフォルト応答規則の管理

8.2.1. デフォルト応答規則の表示と編集

デフォルト応答規則を表示および変更するには、次の手順に従います。

1. ポリシー ツリーの [デフォルト応答] ブランチを展開し、表示されるプロパティのいずれかを選択して、[プロパティ] ボタンをクリックします。
2. [デフォルト応答規則] ダイアログ ボックスが開きます。このダイアログ ボックスには、[IPsec 応答] と [IP トラフィック処理] の 2 つのページがあります。必要な値を表示して編集します。詳細については、「8.3 IPsec 応答」および「8.4 IP トラフィック処理」の項を参照してください。
3. 変更を確定する場合は、[OK] ボタンをクリックします。[キャンセル] をクリックすると、変更は破棄されます。いずれのボタンをクリックした場合でも、ダイアログ ボックスが閉じてポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

8.2.2. デフォルト応答規則の監査

デフォルト応答規則を監査するには:

1. [デフォルト応答規則] ダイアログ ボックスを開いて、[IPsec 応答] タブをクリックし、対応するページを開きます。
2. ダイアログ ボックスの下部の [この規則を監査する] オプションを選択します。ポリシー エディタで変更を有効にすると、IPsec と保護されていない IP トラフィックの両方に対するデフォルト応答が監査されます。
3. ネットワークのさまざまなサーバからの一般的なブロードキャスト メッセージに対する応答も取り込むと、監査ログ内のイベント数が増大します。そのため、既定ではブロードキャスト メッセージは監査に含まれません。ただし、ブロードキャスト トラフィックへのデフォルト応答も監査する場合は、[ブロードキャスト トラフィックを監査する] オプションを選択します。
4. 変更を確定する場合は、[OK] ボタンをクリックします。[キャンセル] をクリックすると、変更は破棄されます。いずれのボタンをクリックした場合でも、ダイアログ ボックスが閉じてポリシー エディタに戻ります。
5. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシーエディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

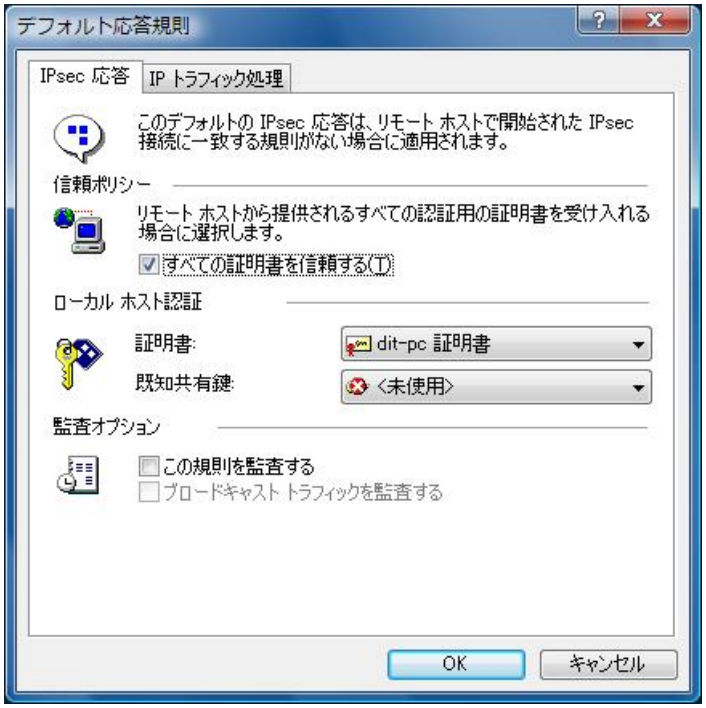

図 8-1　IPsec で保護された受信トラフィックへのデフォルト応答

8.3.　IPsec 応答

信頼ポリシー

[すべての証明書を信頼する] オプションを選択すると、リモート ホストから受信されたすべての証明書は、追加の確認なしでローカル ホストによって信頼されます。このオプションを選択しない場合、信頼できない証明書がローカル ホストで受信されると、トラフィックはドロップされます。後者の場合、鍵管理の信頼されたホストの証明書に該当する証明書、または信頼する認証局から発行された証明書は信頼できます。

証明書への信頼は、現在の接続にのみ適用されます。つまり、その証明書は鍵管理の一般信頼ポリシーには含まれません。さらに、この設定はデフォルトの IPsec トラフィック処理にのみ影響します。一般信頼ポリシーは、[鍵管理] ページの設定に基づいて決定されます。

ローカル ホスト認証

デフォルト応答 ID は、ローカル ホストがそれ自体を認証する方法を定義します。証明書と既知共有鍵の 2 つの認証方法があります。いずれかまたは両方の認証方法を指

定できます。リモート ホストは、接続のネゴシエーションを開始する場合に、ローカル ホストから送信する認証鍵を指定します。

証明書は、最初にインストール プロセスの一部として設定されます。インストール中に自己署名証明書のみを作成した場合は、その証明書がここに表示されます。ただし、認証局の証明書に対する登録に成功し、同時にその証明書を受け取った場合は、その証明書がここに表示されます。

証明書または既知共有鍵を対応するリストから選択することにより、両方の設定を変更できます。証明書または既知共有鍵を［<未使用>］に設定した場合は、認証鍵を使用できません。

8.3.1. 監査オプション

この規則を監査する

デフォルト応答規則を監査するには、このオプションを選択します。

ブロードキャスト トラフィックを監査する

ネットワークのさまざまなサーバからの一般的なブロードキャスト メッセージに対する応答を監査ログに取り込む場合は、このオプションを選択します。このオプションを選択すると、ログ内のイベント数が増大する場合があります。

8.4. IP トラフィック処理

次の 2 つのオプションから選択できます。

保護されていない IP トラフィックを許可

特定の規則のいずれにも一致しない、すべての保護されていない IP トラフィックを許可することを選択できます。つまり、フィルタ規則によって破棄されない、すべての保護されていないトラフィックを許可します。デフォルト規則で許可された場合でも、データ パケットは次に IPsec 後フィルタに転送され、そこで一部のパケットが破棄されることもあります。

保護されていない IP トラフィックを拒否

別のオプションとして、保護されていないトラフィックをデフォルトで拒否することを選択できます。つまり、IPsec 前フィルタの規則でバイパスされなかったすべてのトラフィックを破棄します。

第 9 章　認証鍵の管理

9.1. 認証とは

整合性および機密性に加えて、認証はセキュアな通信の重要な一部を構成します。認証は IKE (Internet Key Exchange: インターネット鍵交換) の一部です。

9.1.1. 認証鍵

認証鍵は、ID とその証拠を結び付けます。ネットワークでは、ID には慣習的に (静的な) IP アドレスまたはドメイン名が使用されています。したがって、認証されるのはホストのコンピュータであり、それを使用するユーザーではありません。
NET-G Secure VPN Client には、既知共有鍵と証明書の 2 種類の認証鍵があります。

既知共有鍵

既知共有鍵は、通信を開始する前に通信当事者間で共有するシークレットです。互いにシークレットを知っていることを確認した上で、通信を開始します。共有シークレットのセキュリティは、パスワードの「性能」によります。たとえば、パスワードに日常語を使用すると、辞書攻撃などの格好の標的になります。認証方法としては、事前共有シークレットを使用せずにできるだけ証明書を使用することをお勧めします。既知共有鍵を使用する場合は、シークレットを注意して選択する必要があります。ネットワーク管理者が規定したガイドラインに従ってください。

証明書と鍵ペア

証明書は、より洗練された認証方法であり、認証鍵ペアを使用します。鍵ペアは、公開鍵と秘密鍵で構成され、暗号化に使用できます。その名前が示すように、公開鍵はネットワーク全体に公開されており、秘密鍵は証明書を保有するエンティティのみが知っています。両方の鍵は数学的には依存関係にありますが、秘密鍵を公開鍵から導き出すことはできません。さらに、両者は独特な関係にあり、一方の鍵で暗号化した内容は他方の鍵でのみ解読できます。

証明書は、ID (ホストの IP アドレスなど) および証拠としての鍵ペアの公開鍵で構成されます。しかし、ID と証拠を結び付けるものが必要です。証拠が示すとおりにホストが本

人であることを確認する必要があります。

9.1.2. 認証局

公開鍵と ID の結び付きは認証局（CA）が提供します。認証局は、結び付きが有効であり、証明書が認証に使用できることを保証します。

エンティティ（ ホスト ）は、その ID（ 静的な IP アドレスなど ）と公開鍵を送信することで、証明書を登録できます。認証局は、登録に問題がなければ証明書を発行します。認証局は、発行する証明書をそのデジタル署名で署名します。

公開鍵インフラストラクチャ

公開鍵インフラストラクチャは、認証局と証明書の登録の概念を洗練させたものです。この環境では、証明書を発行する認証局と証明書を登録するエンド エンティティ（ ホスト ）があります。さらに、認証局は複数のレベルで構成される場合があります。エンド エンティティが下位レベルの認証局から受け取った証明書は、より上位レベルの認証局から発行されている場合があります。公開鍵インフラストラクチャでは、論理的なパターンに従って推論します。認証局を信頼するならば、その認証局が発行するすべての証明書も信頼することになります。したがって、発行元の認証局を信頼できる場合にのみ、そこから発行された証明書を信頼します。認証局の証明書がさらに別の上位レベルの認証局から発行されているなど、証明書チェーンは非常に長くなることがあります。信頼できることを確認するために、場合によっては証明書チェーンをルートの認証局までさかのぼることが必要になります。

証明書失効リスト

認証局は、何らかの理由で信頼性が失われた証明書を、失効リスト（certificate revocationlist: CRL）として発行します。証明書を信頼する前に、CRL を確認する必要があります。証明書チェーンに複数の認証局が関与している場合は、各認証局から発行された失効リストを確認します。

ディレクトリ サービス

認証局がリモートサーバに配置した失効リストを見つけるには、ディレクトリ サービスを定義します。ディレクトリ サービスは、リモート サーバの集中管理ポリシーとそのポリ

シーに関連付けられた証明書を探す場合にも役立ちます。

9.1.3. 自己署名証明書

公開鍵インフラストラクチャはテクノロジとして未成熟な段階であるため、インフラストラクチャを利用できない状況も発生する場合があります。NET-G Secure VPN Client は、公開鍵インフラストラクチャを利用できない場合でも、証明書ベースの認証を可能にするために、自己署名証明書の使用をサポートしています。

認証局から発行される証明書は、認証局のデジタル署名によって保護されます。自己署名証明書では、認証局の署名の代わりにホスト自体のデジタル署名を使用します。したがって、リモート ホストの自己署名証明書を受け入れる場合は、慎重に検討する必要があります。リモート ホストが本人であることを示すものはリモート ホスト自体の言葉のみです。ただし、通信相手を知っていて、電話などで証明書のフィンガープリントを確認できる場合、通信はセキュアであると妥当に判断できます。

ローカル ID 証明書

NET-G Secure VPN Client の通常のインストール時には、ローカル ホストの自己署名証明書が作成されます。この自己署名証明書は、[自分の鍵] リストと信頼された認証局のリストに含まれています。インストールの一環として作成される自己署名証明書は、ローカル ID と見なされます。

リモート ホストの自己署名証明書を受け入れると、その証明書は信頼されたリモート ホストのブランチに挿入されて、ローカル ホストの自己署名証明書でデジタル署名されます。ローカル ホストの自己署名証明書は認証局と見なされるため、証明書チェーンは完結します。

ローカル ID 証明書を削除すると、デフォルト ID 証明書として使用する、新しい自己署名証明書の作成がすぐに強制されます。新しい証明書が正常に作成された場合のみ、古い証明書が削除されます。「10.2.5 証明書の削除」および「10.2.1 証明書の作成」の項を参照してください。

9.1.4. 認証鍵の交換

ネゴシエーションの最初のフェーズ（ IKE フェーズ 1 ）の IKE（ インターネット鍵交

換 ）のセキュリティの関連付けを確立する際に、認証鍵が交換されます。ホスト間で互いの認証を受け入れると、他の問題が発生しない限り、ネゴシエーションは成功します。いずれかのホストが認証を受け入れない場合は、ネゴシエーションが失敗します。

リモート ホストの証明書を受け入れるには、ローカル ホストがその証明書を信頼する必要があります。ルート認証局の証明書または、自己署名証明書の場合はリモート ホストの証明書がシステムに必要です。

証明書が見つからないという理由のみでネゴシエーションが失敗する場合があるために、IPsec 規則の作成時に常に診断を実行することをお勧めします。診断を実行すると、証明書が見つからない場合にそれを知らせるメッセージが表示されます。一方、ネゴシエーションが失敗した場合は、データ パケットが単にドロップされます。

9.2. 鍵管理

認証鍵は、ポリシー エディタの [鍵管理] ページに表示されます。

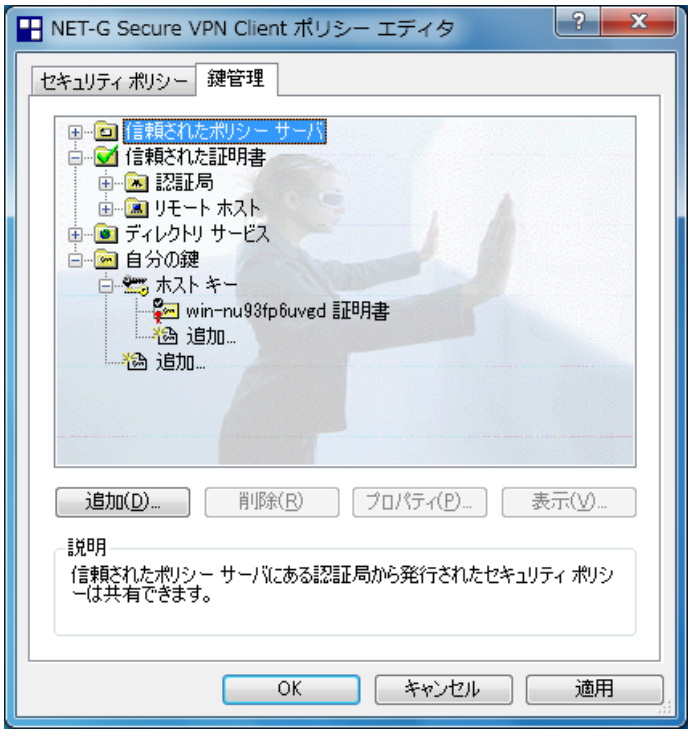

図 9-1 ポリシー エディタの [鍵管理] ページ

信頼されたポリシー サーバ

ここに表示されるサーバのポリシーは共有できます。これらの証明書の管理は、公開鍵インフラストラクチャのロジックに従います（「4.4 信頼されたポリシーサーバ」の項を参照 ）。この種の証明書はすべてのポリシーに共通です。

信頼された認証局

信頼する認証局の証明書です。この種の証明書はポリシー別に異なります。

信頼されたリモート ホスト

ネットワーク内の信頼するホストの自己署名証明書です。自己署名証明書の扱いについては慎重になりすぎることはありません。信頼できるという十分な根拠がある自己署名証明書のみを信頼してください。この種の証明書は、ポリシー別に定義します。

ディレクトリ サービス

ディレクトリサービスは、認証失効リストを探す場合などに必要です。ディレクトリサービスはポリシー別に定義します。

自分の鍵

ローカル ホストの認証鍵です。既知共有鍵と証明書の両方が含まれます。さらに、ここには自己署名証明書と認証局から発行された証明書の両方が表示されます。ローカル ホストの認証鍵はすべてのポリシーに共通です。

Accession 鍵

SSH Accession がインストールされた環境では、スマートカードで検出された証明書は[Accession 鍵] ブランチの下に表示されます。スマートカードは、SSH Accession で管理します。スマート カードをリーダに挿入すると、その証明書が NET-G Secure VPN Client に表示されます。ただし、ローカル ホストの証明書を発行した認証局の証明書をインポートする必要があります。インポート方法の詳細については、「10.2.2 証明書と鍵ペアのインポート」の項を参照してください。スマートカードと認証鍵の管理は、SSH Accession で実行します。詳細については、SSH Accession のマニュア

ルを参照してください。

第 10 章 証明書

10.1. 証明書とは

鍵管理の証明書は、次のカテゴリに分類されます。

- ローカル ホストの証明書（ 自分の鍵 ）
- 信頼された認証局 (CA) の証明書
- 信頼されたリモート ホストの証明書
- 信頼されたポリシー サーバの証明書

カテゴリは証明書の用途を示します。ただし、証明書の一般的な管理は、すべてのカテゴリにほぼ共通です。証明書の管理に関する以下の説明は、特に断らない限り、すべての証明書に該当します。

10.2. 証明書の管理

10.2.1. 証明書の作成

[自分の鍵] にのみ適用可能。

ローカル ホストの新しい自己署名証明書と、認証局への証明書要求を作成できます。ウィザードが手順を示します。

1. ウィザードを起動します。作成する内容に応じて、次のいずれかの操作を行います。
   - 既存の鍵ペアに基づいて新しい証明書を作成する場合は、鍵ペアを選択して [追加] ボタンをクリックします。
   - 新しい鍵ペアとそれに基づく証明書を作成する場合は、[自分の鍵] ブランチを選択して [追加] ボタンをクリックします。
2. 表示される [新しい認証鍵] ダイアログ ボックスで認証鍵の種類を選択します。次の登録方法から選択できます。
   - 新しい鍵ペアと証明書を作成するには、[認証鍵ペアと証明書を作成する] オプションを選択します。
   - 選択した鍵ペアを証明書要求に含めて、新しい証明書を登録するには、[証明書を登録する] オプションを選択します。

- 新しい既知共有鍵を作成するには、[既知共有鍵を作成する] オプションを選択します。詳細については、「11.2.1 既知共有鍵の作成」の項を参照してください。

[次へ] をクリックして続行します。

3. 認証鍵ペアを作成しない場合は、このステップを省略します。このステップでは、認証鍵ペアを作成します。最初に、鍵生成用のランダムシードを収集します。マウスを移動するか、テキストを入力してシードを生成します。ユーザーのランダムな入力を利用して一意な鍵を生成します。2 つの入力が類似し、生成される鍵も類似するという確率は極小です。シード用のデータが十分に収集されると、ソフトウェアによって実際の鍵ペアが計算されます。この計算が完了するまでには約 20 秒かかります。生成の完了後に [次へ] をクリックして続行します。
4. [証明書情報] ダイアログ ボックスで、証明書の ID に関する情報を指定します。各フィールドに必要な値を入力します。

プライマリ ID

ホストを識別するためのプライマリ情報。IP アドレス、ドメイン名、および電子メールアドレスのいずれかを選択できます。IP アドレスまたはドメイン名を選択することをお勧めします。静的なドメイン名および IP アドレスのみを使用します。ローカルホストに静的な IP アドレスも静的なドメイン名もない場合は、電子メールアドレスを代わりに選択します。ただし、IPsec 規則は通常ドメイン名または IP アドレスに結び付けられるため、他のソフトウェア製品と相互運用性の問題を生じる可能性があります。

選択するプライマリ ID の種類に応じて次のフィールドの名前が変わります。実際の ID として、ローカルホストの IP アドレス、ドメイン名、または電子メール アドレスを入力します。

詳細

[詳細] ボタンをクリックすると、[詳細情報] ダイアログボックスが開きます。所属部署、組織、および国を指定できます。

[次へ] をクリックして続行します。

5. 次に、[証明書の登録] ダイアログ ボックスで証明書の登録方法を指定します。次の方法を指定できます。
   - 自己署名証明書を作成します。

- 証明書要求を作成して、すぐにオンラインで証明書を登録します。
- 証明書要求を作成し、後で登録するようにファイルに保存します。

[次へ] をクリックして続行します。

6. 次の手順は、前の手順で選択した内容に応じて異なります。
   - 自己署名証明書を選択した場合: NET-G Secure VPN Client によって自己署名証明書が作成されます。
   - オンライン登録を選択した場合: [認証局] ダイアログ ボックスが表示されます。必要な値を入力します。

登録プロトコル

オンライン登録プロトコルとして、SCEP（ Simple Certificate Enrollment Protocol ）と CMP (Certificate Management Protocol ）です。

CA サーバ アドレス

サーバのアドレス（URL）。

CA 証明書

認証局の証明書。この証明書は、認証局に送る証明書要求を暗号化するのに必要です。

このフィールドに証明書名を入力した場合は、その名前を使用して前のフィールドのアドレス(URL)から証明書が取り出されます。別の方法として、証明書があるアドレス(URL)を入力するか、[参照] ボタンをクリックして証明書があるファイルを探すこともできます。証明書をクリップボードにコピーした場合は、メニュー項目の [クリップボードからの貼り付け] を使用することもできます。

プロキシ サーバを使用する

必要に応じて選択します。[設定] ボタンをクリックして値を指定します。この場合、ローカルホストで認証局のサーバ アドレス（URL）を解決できることが必要です。

参照番号

登録で CMP プロトコルを使用する場合に必要です。証明書を要求しているユーザーを識別するのに、参照番号と鍵（ 下を参照 ）が使用されます。

鍵

認証局から付与される共有シークレットです。鍵は、証明書を要求しているユーザーを識別します。

[次へ] をクリックして登録します。

- オフライン要求を選択した場合:[証明書要求] ダイアログ ボックスで、要求を保存するファイルを選択します。ファイルを探すには、[参照] ボタンをクリックします。

7. [終了] をクリックすると、新しい証明書の作成が完了します。

要求をファイルに保存した場合は、自分で認証局に要求を送る必要があります。

10.2.2. 証明書と鍵ペアのインポート

次のような場合は証明書を手動でインポートします。

- 登録した認証局から証明書がファイルで返された場合。
- リモート ホストまたは認証局が証明書をファイルで提供する場合。

信頼できる証明書のみをインポートするよう注意してください。

[自分の鍵] ブランチにインポートするときは、次のいずれかを選択できます。

- 証明書のみをインポートします。
- 証明書および対応する鍵ペアをインポートします。
- 証明書、対応する鍵ペア、および認証局の証明書をインポートします。
- 鍵ペアのみをインポートします。

NET-G Secure VPN Client では、有用な証明書のみをインポートするために、次のような初歩的なチェックが実行されます。

1. 全体的な有用性。証明書の暗号化が正しく、システムにとって読むことができる形式

であること。
2. 有効期限が過ぎていないこと。
3. NET-G Secure VPN Client の要件として、デジタル署名の拡張が選択されていること。
4. 認証局を追加する場合は、対応するフラグ フィールドがあること。

リモート ホストの自己署名証明書をインポートすると、その証明書はローカル ホストの自己署名証明書で署名されます。リストに表示されるローカル ホストの自己署名証明書は信頼される認証局と見なされるので、証明書チェーンは完結します。

ファイルからの証明書のインポート

PEM（Privacy Enhanced Mail）、バイナリ、または RSA PKCS #12 フォーマットの証明書ファイルをインポートするには、次の手順に従います。[自分の鍵] ブランチにインポートすると、PKCS #12 ファイルには、エンド エンティティ（ ローカル ホスト ）の証明書以外に、認証鍵ペアまたは CA 証明書、あるいは両方が含まれていることがあります。

1. インポートするものに応じて、次のように操作します。
   - リモート ホストの証明書をインポートする場合は、[鍵管理] ツリーから目的のブランチ（[信頼されたポリシー サーバ]、[認証局]、[リモート ホスト]）を選択します。
   - 鍵ペアは含まれず、おそらく CA 証明書は含まれているローカルホストの証明書をインポートする場合は、[自分の鍵] ブランチの下の対応する認証鍵ペアを選択します。
   - 鍵ペアが含まれ、おそらく CA 証明書も含まれているローカルホストの証明書をインポートする場合は、[自分の鍵] ブランチを選択します。
2. マウスの右クリックで表示されるメニューで、[インポート] を選択します。
3. [開く] ダイアログボックスで、ファイル システム内のファイルを参照します。ファイルを見つけて、[開く] をクリックします。表示するファイル数を制限するには、[ファイルの種類] フィールドで必要な選択を行います。
4. インポートする各証明書のフィンガープリントなどの基本的な情報が表示され、インポートするかどうかを確認するメッセージが表示されます。信頼できる証明書のみをインポートするよう注意してください。必要に応じて、証明書のフィンガープリントを確認します。
5. CA 証明書付きのローカル ホスト証明書をインポートするときは、次のことに注意してください。CA 証明書は、現在アクティブなポリシーにのみインポートされます。ただし、ローカル ホストの証明書はすべてのポリシーに共通であるため、インポートし

た証明書はすべてのポリシーで使用できます。アクティブなポリシーを変更すると、証明書は新しいアクティブなポリシーでは信頼されていないものとして表示されます。他のポリシーでも証明書を信頼するには、他のポリシーそれぞれに CA 証明書をインポートする必要があります。証明書は、PKCS#12 ファイルからインポートするか、クリップボードにコピーしてクリップボードから貼り付けることができます。

6. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

次のように操作すると、証明書をすばやくインポートできます。

- ドラッグ アンド ドロップ: PEM でエンコードされた証明書ファイルをポリシー エディタにドラッグし、適切なブランチにドロップします。
- ダブルクリック: 証明書ファイルをダブルクリックします。NET-G Secure VPN Client は、拡張子.psk を持つ証明書ファイルを認識します。ファイル名拡張子への関連付けは、Web ブラウザからも有効です。

認証局、信頼されたポリシー サーバ、またはリモートホストの証明書をインポートする場合は、[追加] ボタンがメニュー項目の [インポート] と同じ役割を果たします。ただし、ローカル ホストの証明書の場合は、[追加] ボタンをクリックすると、新しい認証鍵を作成するためのウィザードが起動します。「10.2.1 証明書の作成」の項を参照してください。

ファイルからの鍵ペアのインポート

RSA PKCS #1、PKCS #12、または SSH X.509 フォーマットの鍵ペア ファイルをインポートするには、次のように操作します。

- 鍵管理ツリーの [自分の鍵] ブランチをマウスで右クリックし、表示されるメニューで [インポート] を選択します。
- ファイルを見つけ、ファイル名を入力し、ファイル フォーマットを選択します。[開く] をクリックしてファイルをインポートし、ポリシー エディタに戻ります。
- ポリシー エディタで、[適用] または [OK] をクリックして変更を保存します。これで、鍵管理ツリーに鍵ペアが表示され、証明書の登録などに使用することができます。

クリップボードからの証明書の貼り付け

クリップボードに証明書をコピーして、後で貼り付けることもできます。

1. 鍵管理ツリーの目的のブランチ（ ローカル ホストの証明書を貼り付ける場合は鍵ペア ）をマウスで右クリックします。
2. 表示されるメニューで［ 貼り付け ］を選択します。Shift + Insert および Ctrl + V キーの組み合わせを使用することもできます。
3. ［ 適用 ］または［OK］をクリックすると、変更が有効になります。［OK］をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、［ キャンセル ］をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、［ 適用 ］または［OK］をクリックすると、これまでのすべての変更が適用され、［ キャンセル ］をクリックすると、これまでのすべての変更が破棄されます。

リストからの証明書の選択

認証局の証明書をリストから選択してインポートできます。このリストには、スマートカードで検出された認証局の証明書が表示されます。SSH Accession がインストールされた環境ではスマート カードの証明書を認証に使用する前に、対応する認証局の証明書をインポートする必要があります。

1. 鍵管理ツリーで［ 認証局 ］の下の［ リストから選択 ］ブランチをダブルクリックします。
2. 証明書のリストを示すダイアログ ボックスが開きます。SSH Accession がインストールされた環境では、スマート カードで検出された証明書が［ SSH Accession ］ページに表示されます。追加する証明書の左のボックスにチェック マークを付けます。証明書を表示するには、それを選択して［ 表示 ］ボタンをクリックします。
3. 証明書を選択した後で、［ OK ］ボタンをクリックすると、証明書がインポートされます。証明書をインポートしない場合は、［ キャンセル ］をクリックします。いずれのボタンをクリックした場合でも、ポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、［ 適用 ］または［OK］をクリックすると、変更が有効になります。［ OK ］をクリックした場合は、ポリシーエディタが閉じます。変更を破棄するには、［ キャンセル ］をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、［ 適用 ］または［OK］を

クリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

10.2.3. 証明書のエクスポート

証明書をエクスポートする（ ファイルに保存する）には、次の手順に従います。

1. エクスポートする証明書を選択して、[表示] ボタンをクリックし、[証明書情報] ダイアログボックスを開きます。
2. [エクスポート] ボタンをクリックします。ファイルを保存するための標準のダイアログ ボックスが開きます。
3. ファイルの保存先を選択し、ファイル フォーマットを選択します。証明書は DEM/PEM フォーマットおよびバイナリ フォーマットで保存できます。
4. 証明書を保存すると、[証明書情報] ダイアログ ボックスに戻ります。[終了] をクリックすると、ポリシー エディタに戻ります。

クリップボードへの証明書のコピー

クリップボードに証明書をコピーし、各種のアプリケーションに貼り付けることができます。

1. コピーする証明書を選択します。
2. マウスを右クリックしてメニューを開き、[コピー] を選択します。証明書がクリップボードにコピーされます。

10.2.4. 証明書の名前の変更

証明書の名前を変更するには:

1. 証明書を選択します。
2. マウスを右クリックしてメニューを開き、[名前の変更] を選択します。
3. 新しい名前を入力します。この名前は単なる参照用です。
4. [適用] または［OK］をクリックして、変更を確認します。［OK］をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または［OK］をクリックすると、これまでのすべての変

更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

10.2.5. 証明書の削除

証明書を削除するには:

1. ポリシー エディタで証明書を選択します。
2. [削除] ボタンをクリックします。
3. 削除を確定するには、[OK] または [適用] をクリックします。[OK] をクリックした場合は、ポリシー エディタが閉じます。いくつかの削除をした後でも、[OK] または [適用] で変更を確定する前であれば、[キャンセル] をクリックして鍵管理ツリーを復元できます。

規則で使用されている証明書は削除できません。削除しようとすると、最初に依存関係を削除してから証明書を削除することを指示するメッセージが表示されます。

デフォルト ID 証明書を削除しようとすると、デフォルトのローカル ID 証明書として使用する新しい自己署名証明書を作成することを強制されます。新しいデフォルト ID が正常に作成された場合にのみ、古いデフォルト ID が削除されます。ローカル ID 証明書の詳細については、「9.1.3 自己署名証明書」の項を参照してください。

10.2.6. 証明書要求の取得

[自分の鍵] ブランチの保留状態の証明書に対してのみ適用できます。

認証局に証明書要求を送ると、証明書のステータスは保留状態になります。証明書要求のステータスを取得するには、次の手順に従います。

1. 保留状態のステータスの証明書を選択します。表示される [取得] ボタンをクリックします。
2. 証明書のステータスが返されます。認証局からローカル ホストに証明書が既に発行されている場合は、その証明書が返されます。要求が保留状態である場合、そのステータスは更新されません。

システムは、要求のステータスを定期的に取得します。認証局から証明書が発行されると

同時に、ステータスが更新されます。

10.2.7. 証明書情報の表示

証明書を表示するには、[証明書情報] ダイアログ ボックスを開きます。

1. 表示する証明書を選択し、[表示] ボタンをクリックします。
2. 情報が表示されます。[全般] タブと [詳細] タブをクリックして 2 つのページを切り替えることができます。
3. 情報を確認した後で、ダイアログ ボックスを閉じるには [終了] をクリックします。

[エクスポート] ボタンは、証明書のエクスポートに使用します（ 「10.2.3 証明書のエクスポート」の項を参照 ）。

10.2.8. 証明書のプロパティの表示と編集

証明書のプロパティを表示および変更するには:

1. プロパティを表示または編集する証明書を選択し、[プロパティ] ボタンをクリックします。
2. [証明書のプロパティ] ダイアログボックスでプロパティを表示し、編集します。
3. 編集後に［ OK ］をクリックして変更を確定し、ポリシー エディタに戻ります。変更を破棄するには、[キャンセル] をクリックします。
4. ポリシー エディタに戻った後で、[適用] または［OK］をクリックすると、変更が有効になります。［OK］をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または［OK］をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

10.3. 証明書情報

証明書情報は、[証明書情報] ダイアログ ボックスに表示されます。[全般] ページには代表的な値が表示され、[詳細] ページにはすべての値が表示されます。

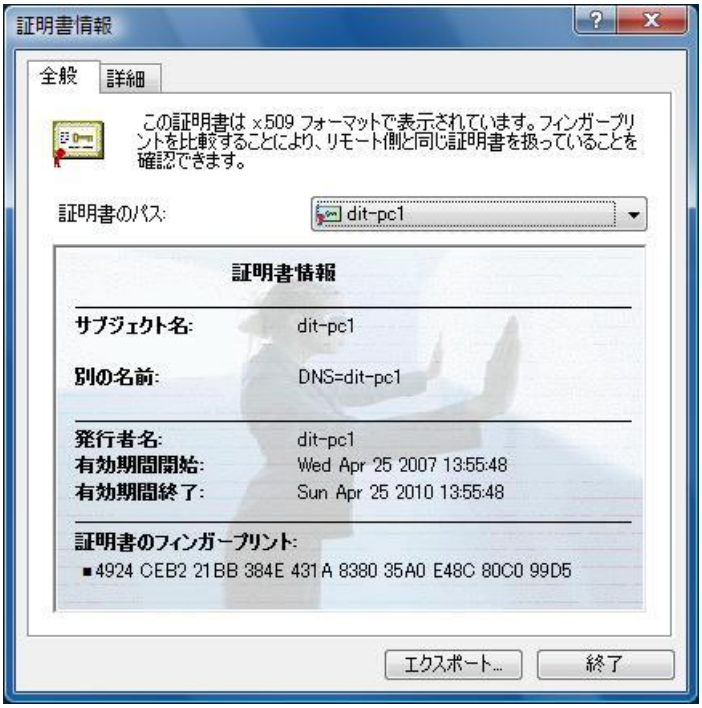

図 10-1　証明書情報

証明書のパス

証明書のパスは、証明書に継承された信頼の経路を示します。証明書が認証局 A1 から発行されたとします。この場合、A1 がリストに表示されます。さらに、A1 はその証明書を上位レベルの認証局 B2 から受け取ったとします。この場合は、B2 と A1 の両方がリストに表示されます。B2 を信頼する場合は、それが A1 に発行した証明書も信頼できます。したがって、A1 とそれが発行する証明書も信頼できます。証明書がルート証明書である場合は、それのみがリストに表示されます。証明書の有効期限が切れていると、[信頼されていません] というテキストが表示されます。

サブジェクト名

証明書の保有者の通称。たとえば、ホストのドメイン名などを指します。

別の名前

ホストの別名。通常は、IP アドレス、ドメイン名、または電子メール アドレスです。

発行者名

証明書の発行者、認証局。

有効開始日

有効期限の開始日時。有効期限外の証明書は信頼されていないものとして分類されます。

有効終了日

有効期限の終了日時。有効期限外の証明書は信頼されていないものとして分類されます。

証明書のフィンガープリント

システムによって計算される証明書のチェックサム。フィンガープリントを使用すると、当事者間で同じ証明書を扱っていることを簡単に確認できます。当事者間では、使用しているアルゴリズムとフィンガープリント自体が同じであることを確認するだけで済みます。

フィンガープリントのアルゴリズム

証明書のフィンガープリントとして証明書のチェックサムを計算するためのアルゴリズム。

バージョン

X.509 証明書のバージョン。

シリアル番号

発行局から付与される、証明書のシリアル番号。認証局はそれが発行する各証明書に続き番号を付けます。

発行者の別名

認証局の別名。通常は、IP アドレス、ドメイン名、または電子メール アドレスです。

使用

証明書の用途の説明。代表的な用途は、認証と他の証明書の証明です。

CRL 配布ポイント

証明書失効リスト（ CRL ）の検索方法に関する情報。失効リストは認証局から発行され、その認証局から発行された証明書の中で何らかの理由で信頼性が失われたすべての証明書を表示します。このフィールドの値は単なる検索キーです。失効リストを実際に検索する場合は、ディレクトリ サービスを利用します。ディレクトリ サービスの詳細については、「第 12 章 ディレクトリ サービス」を参照してください。

署名のアルゴリズム

証明書に関連する鍵を作成するために適用されるアルゴリズム。

公開鍵

証明書に関連付けられた公開鍵。このデータ フィールドには、アルゴリズムと鍵長が表示されます。鍵自体はウィンドウの下部に表示されます。

[エクスポート] ボタンの説明については、「10.2.3 証明書のエクスポート」の項を参照してください。

10.4. 証明書のプロパティ

証明書のプロパティは、[プロパティ] ダイアログ ボックスに表示されます。このダイアログ ボックスを開くには、証明書を選択し、[プロパティ] ボタンをクリックします。

CRL（ 証明書失効リスト）を発行する

このオプションを選択すると、認証局から発行される CRL (証明書失効リスト) を確認してから証明書を信頼するかどうかを最終的に決断できます。

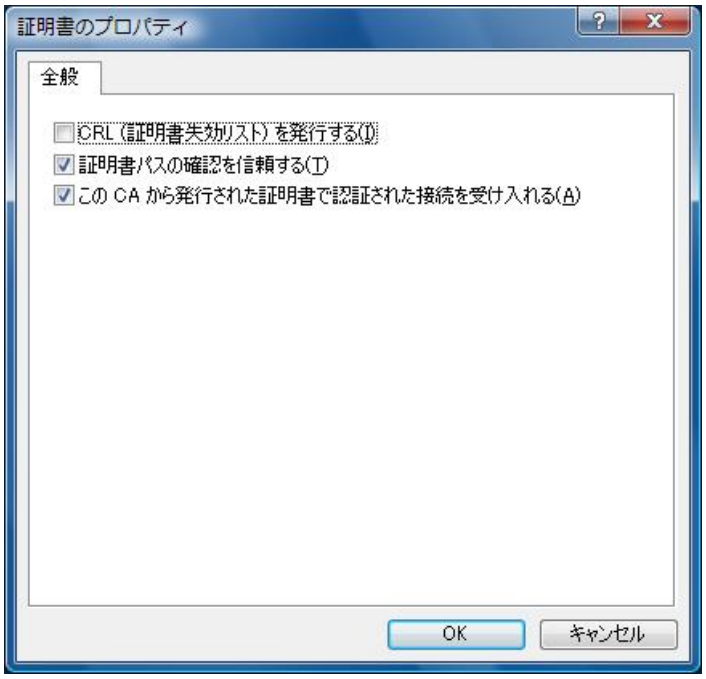

図 10-2 証明書のプロパティ

証明書パスの確認を信頼する

通常は、このオプションを選択し、認証局を信頼します。ただし、信頼しない証明書でもシステムに保存したい場合があります。信頼しない認証局からローカルホストに発行された証明書については、[信頼されていません] というラベル付きで表示されます。この認証局から発行されたリモート ホストの証明書についても認証として受け入れません。詳細については、次の説明を参照してください。

この CA から発行された証明書で認証された接続を受け入れる

このオプションは、上のオプションを選択した場合にのみ有効です。上のオプションを選択して、このオプションも選択した場合は、認証局から発行された証明書で認証されたリモート ホストとの接続を受け入れます。このオプションを選択しない場合は、この認証局から発行された証明書を実際には信頼するときでも、その証明書で認証されたリモート ホストからの接続を受け入れません。ただし、この認証局から発行されたローカル ホストの証明書は認証として受け入れます。

第 11 章 既知共有鍵

11.1. 既知共有鍵とは

既知共有鍵は、通信を開始する前に通信当事者間で共有するシークレットです。互いにシークレットを知っていることを確認した上で、通信を開始します。共有シークレットのセキュリティは、パスワードの「性能」によります。たとえば、パスワードに日常語を使用すると、辞書攻撃などの格好の標的になります。認証方法としては、事前共有シークレットを使用せずにできるだけ証明書を使用することをお勧めします。既知共有鍵を使用する場合は、シークレットを注意して選択する必要があります。ネットワーク管理者が規定したガイドラインに従ってください。

11.2. 既知共有鍵の管理

11.2.1. 既知共有鍵の作成

ウィザードの指示に従って、新しい既知共有鍵を作成できます。

1. [自分の鍵] ブランチまたはその下にある任意の項目を選択し、[追加] ボタンをクリックします。
2. [新しい認証鍵] ダイアログボックスで、[既知共有鍵を作成する] オプションを選択します。[次へ] をクリックして続行します。
3. [既知共有鍵] ダイアログ ボックスが開きます。必要な値を入力します。[次へ] をクリックして続行します。

名前

既知共有鍵に任意の名前を付けます。わかりやすい名前を付けることをお勧めします。

共有シークレット

非可読形式のシークレット。既知共有シークレットのセキュリティは、パスワードとしてのシークレットの「性能」に依存します。たとえば、パスワードに日常語を使用すると、辞書攻撃などの格好の標的になります。したがって、認証方法としては、既知共有鍵を使用せずにできるだけ証明書を使用する必要があります。既知共有鍵を使

用する場合は、シークレットを注意して選択する必要があります。ネットワーク管理者が規定したガイドラインに従ってください。

共有シークレットの確認

入力ミスを防ぐために文字列を再入力します。

フィンガープリント (SHA-1)

SHA-1 MAC アルゴリズムを使用して、共有シークレットのチェックサムが自動的に計算されます。フィンガープリントは一意であり、計算を逆にたどることは非常に難しいため、アルゴリズムとフィンガープリントがわかっている場合でも、共有シークレットを解読することは実質的に不可能です。電話などでフィンガープリントを交換することにより、通信相手と同じシークレットを使用していることを確認できます。したがって、実際のシークレットを明かす必要はありません。この場合、通信当事者間で類似のフィンガープリントを使用するには、同じアルゴリズムを適用する必要があります。

4. [ID の設定] ダイアログ ボックスが開きます。既知共有鍵に関連付ける ID を設定する場合は、必要な値を入力します。[次へ] をクリックして続行します。

ローカル: プライマリ ID

ローカル ホストを識別する情報です。ホストの IP アドレス、ホストのドメイン名、管理者の電子メール アドレス、またはベンダ固有の文字列を指定する場合に選択します。[ID なし] に設定することもできます。静的な IP アドレスまたはドメイン名を使用することをお勧めします。ベンダ固有の文字列は、CISCO VPN Client 用に設定された CISCO 社 VPN サーバ機器に接続する場合に設定します。下のフィールドに実際の ID を指定します。

リモート: プライマリ ID

リモート ホストを識別する情報です。ホストの IP アドレス、ホストのドメイン名、管理者の電子メール アドレス、またはベンダ固有の文字列を指定する場合に選択します。[ID なし] に設定することもできます。静的な IP アドレスまたはドメイン名を使用することをお勧めします。ベンダ固有の文字列は、CISCO VPN Client 用に設定

された CISCO 社 VPN サーバ機器に接続する場合に設定します。下のフィールドに実際の ID を指定します。

5. [終了] をクリックすると、既知共有鍵の作成が完了します。

既知共有鍵の識別情報およびその他のプロパティは、[既知共有鍵] ダイアログ ボックスで更新できます。詳細については、「11.3 既知共有鍵のプロパティ」の項を参照してください。

11.2.2. 既知共有鍵の表示と編集

既知共有鍵は、鍵管理ツリーの [自分の鍵] ブランチに表示されます。既知共有鍵は、[既知共有鍵] ダイアログ ボックスで表示および編集できます。

1. 既知共有鍵を選択し、[プロパティ] ボタンをクリックします。
2. [既知共有鍵] ダイアログ ボックスが開きます。必要な値を表示して編集します。[プロパティ] タブと [ID] タブをクリックして 2 つのページを切り替えることができます。
3. 編集後に [OK] をクリックして変更を確定し、ポリシー エディタに戻ります。変更を破棄するには、[キャンセル] をクリックします。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

11.2.3. 既知共有鍵の削除

既知共有鍵を削除するには:

1. ポリシー エディタで鍵を選択します。
2. [削除] ボタンをクリックします。
3. 削除を確定するには、[OK] または [適用] をクリックします。[OK] をクリックした場合は、ポリシー エディタが閉じます。いくつかの削除をした後でも、[OK] または [適用] で変更を確定する前であれば、[キャンセル] をクリックして鍵管理ツ

リーを復元できます。

IPsec 規則で参照される鍵は削除できません。参照を置換してから鍵を削除してください。

11.3. 既知共有鍵のプロパティ

既知共有鍵のプロパティは、[既知共有鍵] ダイアログ ボックスの [プロパティ] ページと [ID] ページに表示されます。

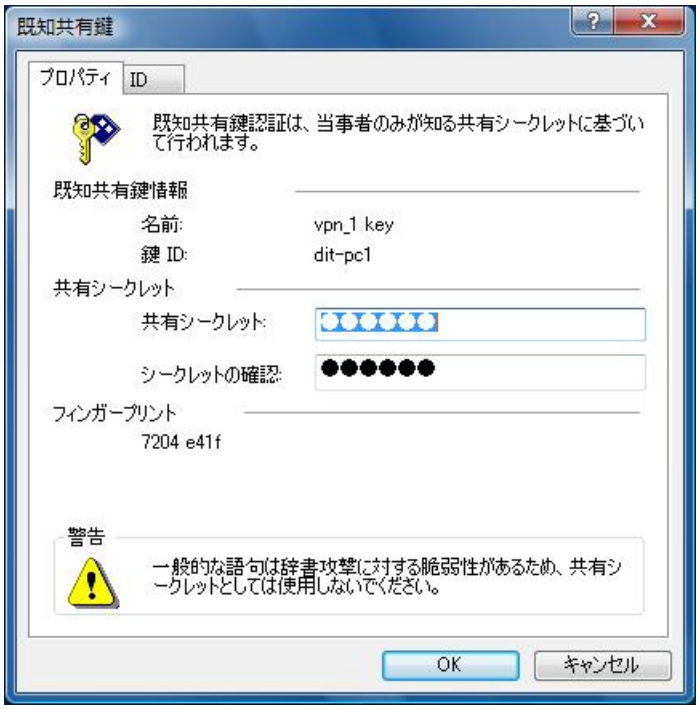

図 11-1 既知共有鍵のプロパティ

11.3.1. プロパティ

名前

既知共有鍵の名前。この名前は、既知共有鍵の作成時にユーザーが指定します。更新不可です。

鍵 ID

ローカル ホストの ID 。ID は、[ID] ページで変更できます。

共有シークレット

非可読形式のシークレット。事前共有シークレットのセキュリティは、パスワードとしてのシークレットの「性能」に依存します。たとえば、パスワードに日常語を使用すると、辞書攻撃などの格好の標的になります。したがって、認証方法としては、既知共有鍵を使用せずにできるだけ証明書を使用する必要があります。既知共有鍵を使用する場合は、シークレットを注意して選択する必要があります。ネットワーク管理者が規定したガイドラインに従ってください。

シークレットの確認

入力ミスを防ぐための確認フィールド。

既知共有鍵のフィンガープリント (SHA-1)

SHA-1 MAC アルゴリズムを使用してシステムによって計算される共有シークレットのチェックサム。フィンガープリントは一意であり、計算を逆にたどることは非常に難しいため、アルゴリズムとフィンガープリントがわかっている場合でも、共有シークレットを解読することは実質的に不可能です。電話などでフィンガープリントを交換することにより、通信相手と同じシークレットを使用していることを確認できます。したがって、実際のシークレットを明かす必要はありません。この場合、通信当事者間で類似のフィンガープリントを使用するには、同じアルゴリズムを適用する必要があります。

11.3.2. ID

既知共有鍵に関連付けられる ID は、[ID] ページに表示されます。ローカル ホストとリモートホストの両方の ID を指定できます。デフォルトでは、両方の ID は [ID なし] に設定されます。

ローカル: プライマリ ID

ローカル ホストを識別する情報です。ホストの IP アドレス、ホストのドメイン名、管理者の電子メール アドレス、またはベンダ固有の文字列を指定する場合に選択します。[ID なし] に設定することもできます。静的な IP アドレスまたはドメイン名を

使用することをお勧めします。[ベンダ固有]の文字列は、CISCO VPN Client 用に設定された CISCO 社 VPN サーバ機器に接続する場合に設定します。下のフィールドに実際の ID を指定します。

リモート: プライマリ ID

リモート ホストを識別する情報です。ホストの IP アドレス、ホストのドメイン名、管理者の電子メール アドレス、またはベンダ固有の文字列を指定する場合に選択します。[ID なし] に設定することもできます。静的な IP アドレスまたはドメイン名を使用することをお勧めします。[ベンダ固有]の文字列は、CISCO VPN Client 用に設定された CISCO 社 VPN サーバ機器に接続する場合に設定します。下のフィールドに実際の ID を指定します。

第 12 章 ディレクトリ サービス

12.1. ディレクトリ サービスとは

認証局は、何らかの理由で信頼性が失われた証明書に関する証明書失効リスト（CRL）を発行します。接続を確立する前に、失効リストをチェックし、リモート エンドの証明書が発行元の認証局からまだ信頼されていることを確認する必要があります。

認証局がリモート サーバに配布した失効リストを見つけるには、ディレクトリ サービスを定義する必要があります。ディレクトリ サービスは、リモート サーバの集中管理ポリシーとそのポリシーに関連付けられた証明書を探す場合にも役立ちます。

12.2. ディレクトリ サービスの管理

12.2.1. ディレクトリ サービスの追加

ディレクトリ サービスを追加するには、次の手順に従います。

1. ポリシー エディタで [ディレクトリ サービス] ブランチを選択し、[追加] ボタンをクリックして [ディレクトリ サービス] ダイアログ ボックスを開きます。
2. 必要な値を入力します。
   - わかりやすいサービス名を指定します。
   - サーバ名とポートを指定します (ポートは [詳細] ページで指定します)。詳細については、「12.3 ディレクトリ サービスのプロパティ」の項を参照してください。
3. 次に、[OK] をクリックしてサービスを追加します。変更を破棄するには、[キャンセル] をクリックします。いずれのボタンをクリックした場合でも、ポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

12.2.2. ディレクトリ サービスの表示と編集

[ディレクトリ サービス] ブランチを展開すると、既存のディレクトリ サービスのリストが表示されます。サービスの詳細は [ディレクトリ サービス] ダイアログ ボックスに表示されます。値を表示および変更するには、次の手順に従います。

1. [鍵管理] ページで、表示するディレクトリ サービスを選択し、[プロパティ] ボタンをクリックします。
2. [ディレクトリ サービス] ダイアログ ボックスが開きます。このダイアログ ボックスには、[全般] ページと [詳細] ページの 2 つがあります。必要な値を参照して更新します。
3. 次に、[OK] をクリックして変更を確定します。[キャンセル] をクリックすると、このダイアログ ボックスで行った変更が破棄されます。いずれのボタンをクリックした場合でも、[ディレクトリ サービス] ダイアログ ボックスが閉じてポリシー エディタに戻ります。
4. ポリシー エディタに戻った後で、[適用] または [OK] をクリックすると、変更が有効になります。[OK] をクリックした場合は、ポリシー エディタが閉じます。変更を破棄するには、[キャンセル] をクリックします。注記: これらの操作は、規則セットおよび鍵管理のすべての変更に影響します。したがって、[適用] または [OK] をクリックすると、これまでのすべての変更が適用され、[キャンセル] をクリックすると、これまでのすべての変更が破棄されます。

12.2.3. ディレクトリ サービスの削除

ディレクトリ サービスを削除するには:

1. ポリシー エディタでディレクトリ サービスを選択します。
2. [削除] ボタンをクリックします。
3. 削除を確定するには、[OK] または [適用] をクリックします。[OK] をクリックした場合は、ポリシー エディタが閉じます。いくつかの削除をした後でも、[OK] または [適用] で変更を確定する前であれば、[キャンセル] をクリックして鍵管理ツリーを復元できます。

12.3. ディレクトリ サービスのプロパティ

12.3.1. 全般プロパティ

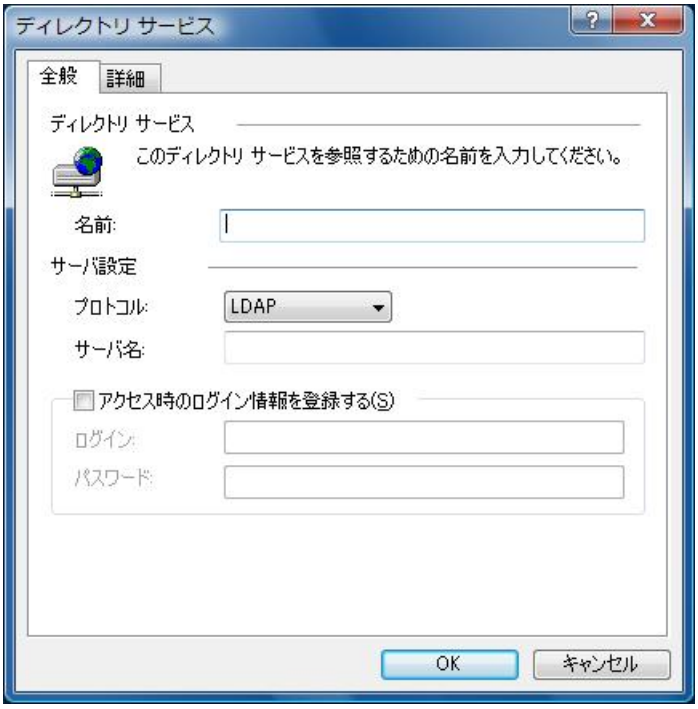

図 12-1　ディレクトリサービスの全般プロパティ

名前

ディレクトリサービスに付けたわかりやすい名前。この名前は、鍵管理の［ ディレクトリ サービス ］ブランチに表示されます。

プロトコル

サービスにアクセスするためのプロトコル。現時点では、LDAP（ Lightweight Directory Access Protocol）のみがサポートされています。

サーバ名

ディレクトリサービスを提供するサーバ。

アクセス時のログイン情報を登録する

サーバがログインを要求し、そのログイン情報を自動的に送信する場合に選択します。

目的のフィールドにログイン名とパスワードを指定します。

12.3.2. 詳細プロパティ

サーバのポート

使用しているサーバのポート番号。

プロキシの設定

プロキシと socks の設定は、サーバがファイアウォールで保護されている場合に、そのファイアウォールを通過するために使用します。必要に応じて、[socks サーバを使用する] オプションを選択します。これらの設定はポリシー レイヤに共通で、[ポリシーのプロパティ] ダイアログ ボックスで指定します。詳細については、「4.3 ポリシーのプロパティ」の項を参照してください。

第 13 章 外部アプリケーション インターフェイス

NET-G Secure VPN Client の基本的な管理のために、機能が限定されたコマンドラインツールが提供されます。各コマンドは、常に sshcpa.exe に続けて指定します。

次の全般オプションを使用できます。

オプション	説明
-h, -help	ヘルプメッセージを表示します。
-V, -version	バージョンを表示します。
-F, -force	変更を強制します。はい / いいえの質問には [はい] を選択します。
-apply	ユーザー インターフェイスを表示せずに変更を適用します。
-silent	ユーザーにメッセージを表示しません。

使用できるコマンドは、次のとおりです。

コマンド	説明
policy-add [<name>] [<URL>]	新しいポリシーを追加します。
set-active <name>	指定したポリシーレイヤをアクティブにします。
start-vpn <session id|rule name>	指定した VPN 接続を開きます。
close-vpn <session id|rule name>	指定した VPN 接続を閉じます。

既知共有鍵を管理するためには、次のオプションを使用できます。

オプション	説明
-A, --psk-add=<name>[:<passphrase>] <URL> [LOCAL=ipv4|fqdn|usr@fqdn(<identity >)] [REMOTE=ipv4|fqdn|usr@fqdn(<identity >)]	新しい既知共有鍵を追加します。特定の URL で見つかったもの

証明書を管理するためには、次のオプションを使用できます。

オプション	説明
-a, --cert-add=[<name>] <URL> [<URL>]	特定の URL で見つかった証明書を追加します。
-t, --cert-add-ca=[<name>] <URL>	特定の URL で見つかった CA 証明

	書を追加します。
-crl	証明書失効リスト(CRL) を発行します。
--no-trust	証明書パスの確認を信頼しません。
--no-accept	この CA が発行した証明書で認証された接続を受け入れません。

ポリシー管理コマンドの例:

policy-add:
New Policy という名前のデフォルト ポリシーを作成します。
```
sshcpa policy-add
```

ファイルからポリシーを取得します。'test' ファイルの後に名前が付けられます。
```
sshcpa policy-add file:///a:¥test.spl
```

http サーバからポリシーを取得します。
```
sshcpa policy-add test-policy http://10.2.1.28/policies/test.spl
```

sprp サーバから test-policy という名前のポリシーを取得し、ローカル ポリシーとして追加します。
```
sshcpa policy-add test-policy sprp://10.2.1.28 --localcopy
```

ldap サーバからポリシーを取得します。
```
sshcpa policy-add test-policy ldap://10.2.1.28 "CN=Policyt,O=dit,C=FI"
```

set-active:
```
sshcpa set-active test-policy
```

規則の管理コマンドの例:

start-vpn:
```
sshcpa start-vpn "172.16.12.253 (10)" --silent
```

close-vpn:
```
sshcpa close-vpn 172.16 --silent
```

既知共有鍵の管理オプション:

psk-add:
PSK を作成します（name=test, secret=test）。
```
sshcpa -A test:test
```

ファイルから PSK を取得します。
```
sshcpa --psk-add file:///a:¥test.psk
```

ID のあるテスト PSK を作成します。
```
sshcpa -A test:test LOCAL=ipv4(10.2.1.1) REMOTE=usr@fqdn
(vpnuser@dit.co.jp)
```

証明書の管理オプション:

cert-add:
ファイルから証明書と秘密鍵を追加します。
```
sshcpa -a file:///a:¥test.crt file:///a:¥test.prv
```

pkcs12 ファイルから証明書と秘密鍵を追加します（ パスワード=qwerty)。
```
sshcpa --cert-add file://:qwerty@/a:¥openssl.p12
```

cert-add-ca:
```
sshcpa -t file:///a:¥test_ca.cer --crl
```


第 14 章 保守管理

NET-G Secure VPN Client には、ネットワークトラフィックを監視する複数のツールがあります。接続の診断(単純な IKE の調査による接続別のチェック) ツールから、ネットワーク トラフィック全体の統計や監査規則に関するものまで各種のツールがあります。

14.1. 監査

セキュリティ ポリシーの各規則を監査するように設定できます。監査を有効にすると、規則を適用するたびに、監査ログにイベントとして記録されます。監査ログは Web インターフェイスを通じて表示できます。

14.1.1. 規則の監査

任意の規則 (フィルタ規則、IPsec 規則、およびデフォルト応答規則) を監査するように設定できます。同時に監査できる規則の数には制限がありません。
規則を監査するには、次のいずれかの操作を行います。

- 規則をマウスの右ボタンで選択します。表示されるメニューで [規則の監査] をクリックします。規則が監査されることを示すチェック マークが表示されます。また、規則のアイコン上に小さい感嘆符 (!) が表示されます。または
- 規則を選択して [プロパティ] ボタンをクリックし、[規則のプロパティ] ダイアログ ボックスを開きます。[詳細] タブをクリックして、監査オプションを表示します。[この規則を監査する] オプションを選択します。[OK] をクリックして戻ります。

変更を有効にするには、[適用] ボタンをクリックします。

規則の監査を中止するには、逆の操作を行います。

- 規則をマウスの右ボタンで選択し、[規則の監査] を再び選択します。メニューからチェック マークが消え、規則のアイコン上の感嘆符も消えます。または
- [規則のプロパティ] ダイアログ ボックスの [詳細] ページで、[この規則を監査する] チェック ボックスをオフにします。

変更を有効にするには、[適用] ボタンをクリックします。デフォルト応答規則の監査方法の詳細については、「8.2.2 デフォルト応答規則の監査」の項を参照してください。

14.1.2. 監査の設定

監査ログは [監査の設定] ダイアログ ボックスで管理します。このダイアログ ボックスを開くには:

1. NET-G Secure VPN Client のメイン メニューで [監査] を選択します。
2. 表示されるサブメニューで [監査の設定] をクリックします。

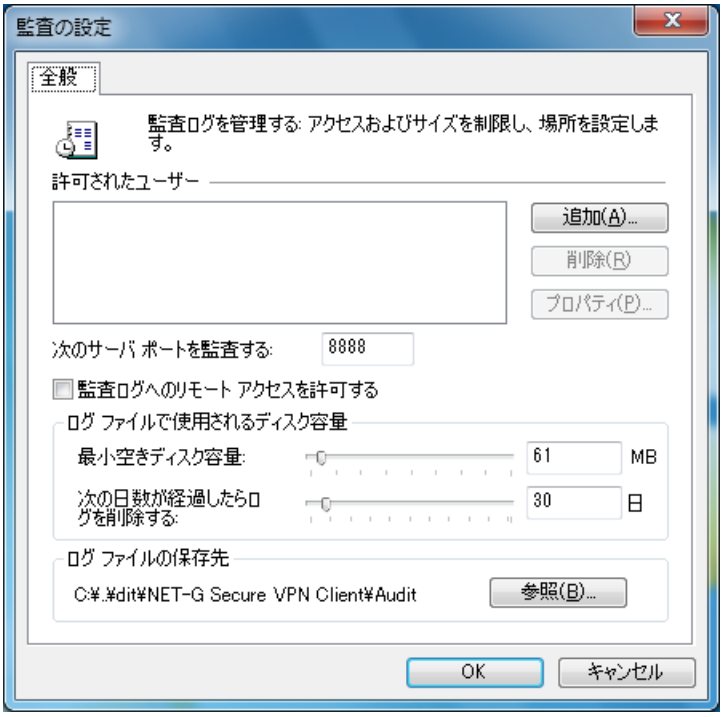

図 14-1 監査の設定

許可されたユーザー

[許可されたユーザー] ボックスには、監査ログへのアクセスを許可されたすべてのユーザーが表示されます。Web インターフェイスを開いてログを表示するときに、ユーザー名とパスワードを要求されます。

ユーザーを追加するには、[追加] ボタンをクリックし、該当するテキスト フィールドにユーザー名とパスワード (確認のために 2 回) を入力します。ユーザーを削除

するには [削除] ボタンをクリックし、パスワードを変更するには [プロパティ] ボタンをクリックします。

次のサーバ ポートを監査する

監査ログへのインターフェイスを使用して監査サーバにアクセスするためのポート。

監査ログへのリモート アクセスを許可する

このオプションを選択すると、監査サーバへのリモート アクセスが許可されます。このオプションを選択しない場合は、ローカル ホストからのみ監査サーバにアクセスできます。

ログファイルで使用されるディスク容量

ログファイルはサイズが大きくなりがちです。特に、規則数が多いと、ホストへのネットワーク アクションが増え、サイズが増大します。ログファイルのサイズを制限し、古いファイルを定期的に削除することが重要です。これらのコントロールを使用して、自動的なクリーンアップを実行し、ディスク使用率を制限してください。

最小空きディスク容量

この設定は、監査ログの保存後にハード ディスク上に必要な空き容量を指定することにより、監査ログのサイズを制限します。空き容量がない場合は、ログが書き込まれず、イベントは記録されません。

変更するには、スライダを移動するか、該当するフィールドに値を入力します。値の範囲は 0 ～ 1,024 MB です。

削除の間隔

この値はクリーンアップの間隔を示します。この制限値より古いログはすべてハードディスクから自動的に削除されます。

値を変更するには、スライダを移動するか、テキスト フィールドに値を入力します。値の範囲は 0 ～ 365 日です。

ログファイルの保存先

このパスは、監査ログの保存先を示します。[参照] ボタンをクリックして保存先を指定できます。

14.1.3. 監査ログの表示

監査ログは Web ブラウザのインターフェイスで表示します。リソースにアクセスするには、プロキシサーバを使用しているホストからローカルホスト（127.0.0.1）を除外します。ログを表示するには、NET-G Secure VPN Client のメイン メニューで [監査] の下の [監査ログを表示] を選択します。

インターフェイスでは、[監査の設定] ダイアログ ボックスで設定したユーザー名とパスワードを確認する画面が最初に表示されます。ユーザー名とパスワードを正しく入力すると、メインページが開きます。この最初のページで、目的のホストを IP アドレスと DNS 名で識別します。[監査ログを表示] リンクをクリックしてログを一覧表示し、表示するログを選択します。

監査ログは毎日作成されます。ログに入るイベントがない場合でも空のログが作成されます。監査対象の規則が適用されるたびに新しいイベントがログに書き込まれます。適用されたポリシーを変更しても監査ログ ファイルは変更されません。

表示されるイベント数を減らすには、時間およびリモート ホストでイベントをフィルタリングします。リストには、イベントごとに次の情報が表示されます。

時間

ログ時間。

イベント

イベントの種類。IPsec 規則によってトリガされたイベントの種類は [トリガ] です。インターネット鍵交換（IKE）によるイベントの種類は、[Phase 1 の成功] 、[Phase 1 の失敗] 、[Phase 2 の成功]、および [Phase 2 の失敗] です。フィルタ規則によってトリガされたイベントは、アクションに応じて、[バイパス]、[ドロップ] 、

または [拒否] です。デフォルト応答規則によってトラフィックが許可された場合のイベントは [許可] です。IKE エンジンに基づく各種のイベントもあります。たとえば、問題について報告する [ペイロード削除の受信] や [不正なペイロード長] などのイベントがあります。

規則 / ソース

適用した規則によってイベントが発生した場合は、このフィールドに規則のグループ（IPsec 前フィルタ、セキュアな接続など ）が表示されます。クリックすると、規則の詳細が表示されます。規則を削除または変更した場合は、規則を表示できません。IKE エンジンによってイベントがトリガされる場合もあります。その場合は、このフィールドに［IKE］と表示されます。

ローカル

ローカル ホストの IP アドレス。クリックすると、詳細が表示されます。

方向

矢印は、ネットワーク トラフィックの方向を示します。

リモート

リモート ホストの IP アドレス。クリックすると、詳細が表示されます。

プロトコル

トラフィック プロトコル。

カウント

イベントは、5 秒ごとにログに書き込まれます。5 秒の間に同じイベントが複数回検出された場合は、イベントが複数回書き込まれずに、このカウントが増えます。

14.2. 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、[NET-G Secure VPN Client 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。NET-G Secure VPN Client のメイン メニューから［IKE ログ ］を開きます。[監査] と［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。

- ［None ］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。

ログをファイルに保存するには、[選択] ボタンをクリックして、ログを保存するファイルを選択し、[ファイルに保存] の左にあるチェック ボックスをオンにします。ウィンドウを閉じても、ログをオフに切り替えない限りログは継続して保存されます。

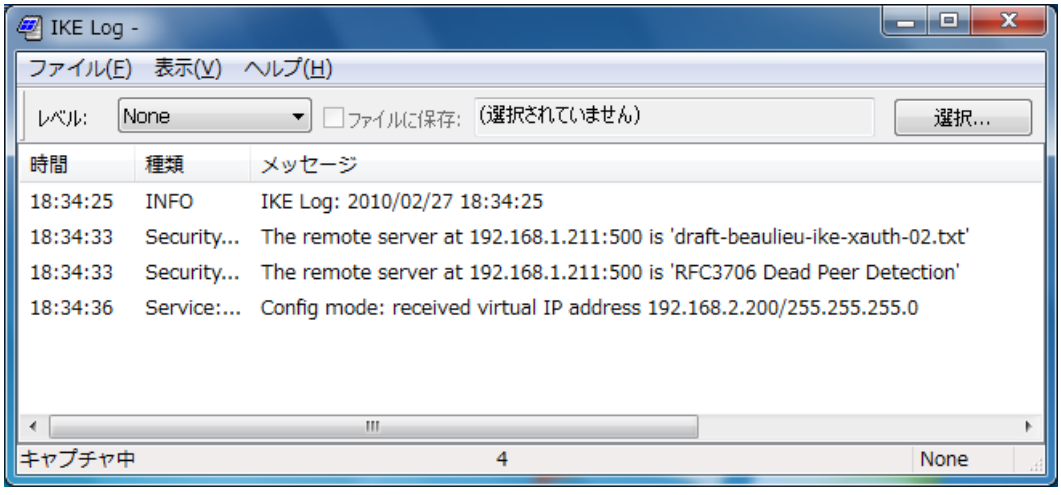

図 14-2 IKE ログウィンドウ

14.3. 接続の診断

セキュアな接続またはバーチャル プライベート ネットワークの接続は、診断を実行してテストできます。診断を実行するには、規則を選択して［ 診断 ］ボタンをクリックします。接続の診断は規則の作成時に実行することをお勧めします。接続を実際に確立するときにネゴシエーションの失敗によってパケットがドロップしても、その事実はユーザーに通知されません。

診断では、通常の接続ネゴシエーションが実行されます。ただし、そのネゴシエーションの結果として作成されるセキュリティの関連付けは、直ちに破棄されます。また、診断の実行時にセキュリティの関連付けが存在すると、その関連付けは破棄されます。

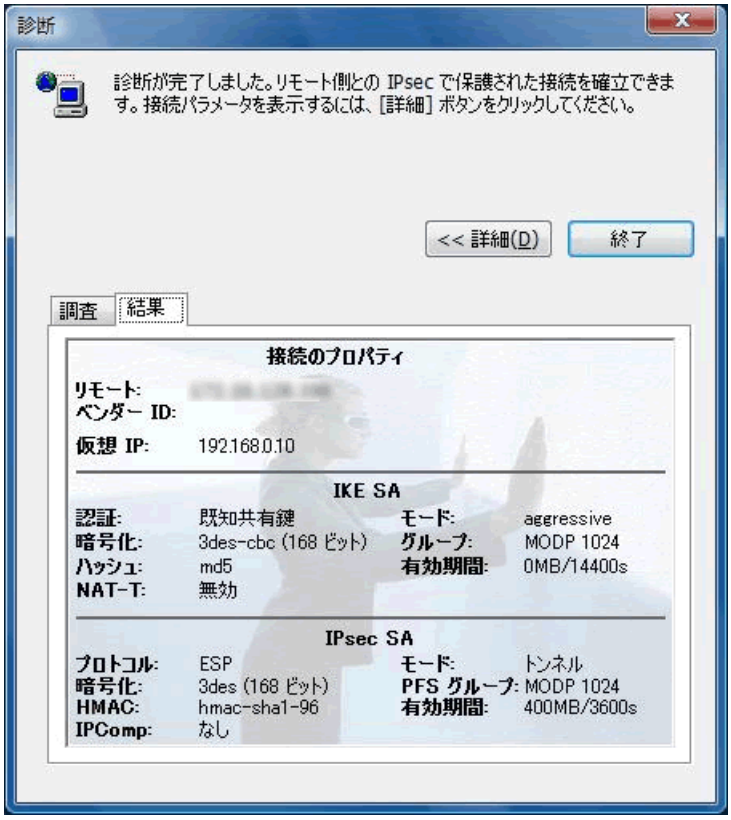

図 14-3　接続の診断の結果

14.4. 統計

NET-G Secure VPN Client 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。

NET-G Secure VPN Client 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。

14.4.1. 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。

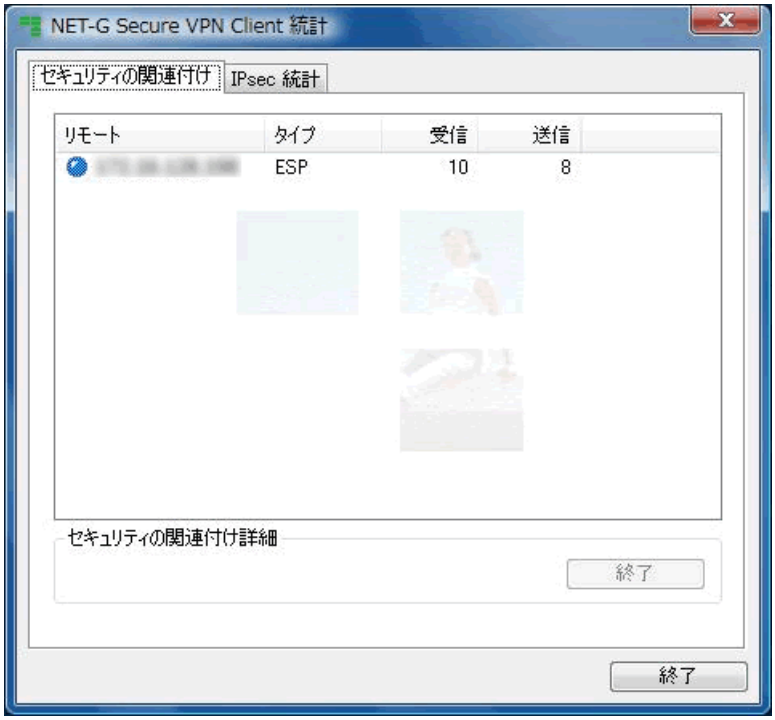

図 14-4 確立されたセキュリティの関連付け

リモート

リモート ホストの IP アドレスまたは DNS 名。

タイプ

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

受信

ローカル ホストで受信されたデータの量。

送信

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。
確立されたセキュリティの関連付けは、［ セキュリティの関連付け詳細 ］に表示されます。

14.4.2. 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。

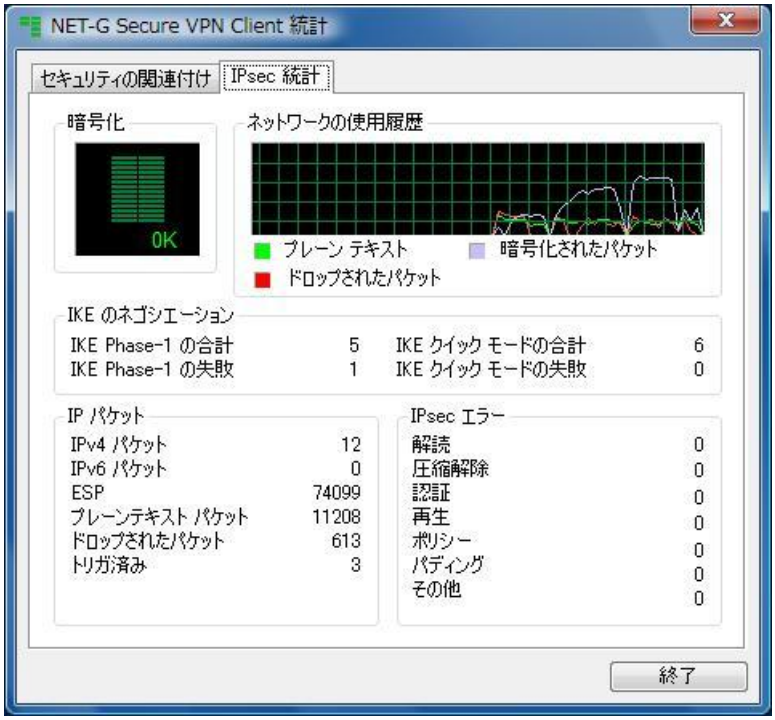

図 14-5　IPsec 統計

暗号化

データのスループットがキロバイト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 Phase-2 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-2 のネゴシエーションの数。

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。[再生] 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 15 章 用語集

この用語集では、本ユーザー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。

ARP（ Address Resolution Protocol: アドレス解決プロトコル ）　ARP プロトコルは、ネットワーク上にある別のホストの物理リンク層アドレス（ イーサネット アドレス ）を調べるために、イーサネット ネットワークで使用されます。このプロトコルは、STD 37（ および RFC 826）に定義されています。

Base 64　64 個の ASCII 文字を使用してバイナリ データの 6 ビット文字列（ 値 0 ～ 63）を表す方法。Base 64 エンコード方式は、当初 PEM（Privacy Enhanced Mail）で使用されていたために、PEM エンコード方式とも呼ばれます。

BGP（ Border Gateway Protocol ）　独立したインターネットサービスプロバイダ間で通常使用されるルーティング プロトコル。このプロトコルは、RFC 1771 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。

CMP（Certificate Management Protocol） CMP は、PKI でのエンド エンティティ、登録機関、および認証局の間におけるオンラインのやり取りを定義します。CMP は、IETF の PKIX 作業部会によって開発されたプロトコルであり、RFC 2510 に定義されています。CMP の拡張バージョンである CMPv2 は、現在インターネット ドラフトの段階です。

CRL（Certificate Revocation List: **証明書失効リスト**） 有効期限が切れる前に証明書の発行元 (CA) により失効または保留された証明書のシリアル番号を示す署名されたリスト。通常、CA は新しい CRL を頻繁に発行します。現在の PKIX に実装されている CRL は、X.509 バージョン 2 の CRL です。詳細については、『RFC 2459』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。

DHCP（Dynamic Host Configuration Protocol） LAN（ローカルエリアネットワーク）上のコンピュータに IP アドレスを動的に割り当てるためのプロトコル。システム管理者は一定範囲の IP アドレスを DHCP に割り当てます。LAN 上の各クライアント コンピュータでは TCP/IP ソフトウェアを設定し、その DHCP サーバに IP アドレスを要求するようにします。IP アドレスの要求および許可は、制御可能な期限付きのリースという考え方に基づいて行われます。DHCP は RFC 2131 に定義されています。

Diffie-Hellman 鍵交換　通信当事者間の鍵交換の方法。この方法を使用して、セキュアでない媒体上で中立的な秘密鍵を生成できます。この方法には多くのバリエーションがあります。man-in-the-middle（ 中間一致 ）攻撃と呼ばれる有名な攻撃は、デジタル署名などの認証方法を Diffie-Hellman プロトコルで使用することを強制するものです。

DoS （Denial of Service: サービス妨害 ）　それ自体ではセキュリティ違反を起こさないが、サービスのアベイラビリティを損なうような攻撃を意味します。たとえば、攻撃者から大量の偽造パケットが IPsec VPN ホストに送られると、ホストのパフォーマンスが低下する場合があります。NET-G Secure VPN Client IPSEC アーキテクチャの設計目標の 1 つは、DoS 攻撃の影響を最小限に抑えることです。

DSA（ Digital Signature Algorithm: デジタル署名アルゴリズム ）　DSA は、デジタル署名の公開鍵アルゴリズムです。DSA アルゴリズムは、米国の NSA（National Security Agency: 国家安全保障局 ）によって考案され、NIST によって FIPS 186-2 に定義されています。詳細については、Bruce Schneiner 著『Applied Cryptograp hy』を参照してください。DSS も参照してください。

DSS（Digital Signature Standard: デジタル署名規格 ）　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米国デジタル署名規格。DSA 公開鍵アルゴリズムと SHA-1 ハッシュ アルゴリズムを使用するデジタル署名に関する規格です。

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。

GPRS（ General Packet Radio Service: 汎用パケット無線サービス ）　GSM に基づく新しいデータ伝送方法であり、データを送受信するためにポータブル端末から継続的なチャネルを設定せずに、パケットでデータを送受信します。GPRS では、56 ～ 114 kbit/s の

速度でデータを転送できます。GPRS を使用すると、VPN (Virtual Private Network: バーチャル プライベート ネットワーク) のモバイルユーザーはダイヤルアップ接続を介さずにプライベート ネットワークに継続的にアクセスできるようになります。

GSM (Global System for Mobile Communications: グローバル移動体通信システム) GSM は、国際ローミング機能を持つデジタル移動体通信用の規格です。GSM は、ヨーロッパとアジアでは 900 MHz と 1,800 MHz の周波数帯域で、アメリカでは 800 MHz と 1,900 MHz の周波数帯域で運用されています。従来の GSM 携帯電話では、最大 14.4 kbit/s の速度でデータを転送できます。GSM のデータ機能を向上するために HSCSD と GPRS が開発されています。

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。

HSCSD (High Speed Circuit Sw itched Data: 高速回線交換データ) GSM リンク上で最大 57.6 kbit/s の速度で回線交換データの伝送を可能にする GSM の拡張。

HTTP (Hypertext Transfer Protocol: ハイパーテキスト転送プロトコル) HTTP は、Web ページを WWW サーバからブラウザに転送するためのプロトコルです。HTTP クライアントはサーバに要求を送り、その応答として特定のデータを受け取ります。HTTP は、サーバ上のオブジェクトを識別するのに URI または URL を使用します。詳細については、RFC 2068 を参照してください。

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。

IPv4（ IP バージョン 4 ）　これは現行バージョンの IP（Internet Protocol: インターネットプロトコル ）です。

IPv6（ IP バージョン 6 ）　これは新しいバージョンの IP（Internet Protocol: インターネットプロトコル ）です。「次世代」IP とも呼ばれます。多くの面で向上されていますが、特にアドレス空間が拡張され、セキュリティが改善されています。このバージョンは、RFC 2460 に定義されています。バージョン 5 はありません。

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。

L2TP （Layer Two Tunneling Protocol ） L2TP は、エンド ユーザーとアプリケーションの両方に対してできるだけ透過的な方法で、中間のネットワークをトンネルして PPP パケットを転送します。L2TP は、RFC 2661 に定義されています。

LAN（ Local Area Network: ローカル エリア ネットワーク ） ローカルエリア(通常は単一の建物内 ）で運用されるネットワーク。LAN を構築するための代表的なテクノロジは、イーサネットです。

LDAP（ Lightweight Directory Access Protocol ） LDAP は、X.500 DAP（Directory Access Protocol）のリソース要件を伴わずに、X.500 Directory モデルをサポートするディレクトリにアクセスするためのディレクトリ アクセス プロトコルです。RFC 2251 と RFC1777 に定義されています。このプロトコルは、ディレクトリに対する読み込み / 書き込みの相互アクセスを提供する管理アプリケーションおよびブラウザ アプリケーションを特に対象としています。このプロトコルは、X.500 DAP のセッション / プレゼンテーション オーバーヘッドの大半をバイパスして、TCP または他のトランスポート上を直接伝送されます。

MARS ブロック サイズを 128 ビット、鍵長を 128 ～ 448 ビットの可変長とする対称ブロック暗号。MARS は、IBM によって設計され、米国 AES（ Advanced Encryption Standard）の 5 つの最終候補に選ばれた中の 1 つです。

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。

MTU（ Maximum Transfer Unit: 最大転送単位 ）　TCP パケットの不必要な断片化を避けるための制御値。TCP MSS（Maximum Segment Size）検出では、この目的を達成するために、対応するネットワークの MTU に一致するように TCP パケットのサイズを制限します。パケットをトンネルしたときにパケットサイズが増える場合は特に注意が必要です。その場合は、断片化を避けるために、トンネル ノードでパス MTU 検出を実行する必要があります。

NAT（ Network Address Translation: ネットワーク アドレス変換 ）　2 つのネットワーク間に接続されるデバイスであり、それを介して送られるパケットの IP アドレスを変換します。通常、2 つのネットワークのいずれかがグローバル アドレスを使用し、他方のネットワークがローカル アドレスを使用します。インターネット上での NAT の使用が増えています。使用可能な IP アドレス空間が減少しているために、大企業ではインターネット サービス プロバイダを変更する場合などにコンピュータの番号の付け替えを避けるために NAT を使用しています。

従来の NAT には 2 つのバリエーションがあります。1 つは IP Network Address Translation（ Basic NAT とも呼ばれる ）です。もう 1 つは NAPT Network Address Port Translation）で、複数の（ ローカル ）IP アドレスを単一の（ グローバル ）IP アドレスに変換します。ただし、ローカル IP アドレス別に異なるポート番号が割り当てられます。NAPT では TCP プロトコルと UDP プロトコルのみを使用できます。従来の NAT の詳細については、『RFC 3022』を参照してください。従来の NAT に加えて、IPv4 と IPv6 の間でアドレスを変換するための NAT-PT（ Network Address Translation -Protocol Translation）と呼ばれる方式があります。NAT-PT は、RFC 2766 に記述されています。

NAT-T（NAT-Traversal）　IPsec と NAT は、通常、共用されません。IPsec では、NAT のパケット処理が通信整合性の違反と見なされるためです。IPsec の NAT-Traversal ソリューションは、この非互換性の問題を解決するためにＳＳＨ コミュニケーションズ・セキュリティによって開発されました。NAT-Traversal では、IPsec パケットを UDP のエンベロープにカプセル化します。エンベロープには、IPsec パケットを再生するための情報が含まれています。UDP のトラフィックは、IKE のネゴシエーションと同じルートをたどります。NAT-Traversal は RFC3947 に定義されています。

NFS（ Network File System: ネットワーク ファイル システム ）　異機種混合システムでファイルを共有するためのクライアント/ サーバアーキテクチャを実装する規格です。

NTP（ Network Time Protocol ） インターネット上の分散したタイム サーバおよびクライアントの間でタイムキーピングを同期化するためのプロトコル。このプロトコルでは、長期にわたってミリ秒以内の正確性を確保できます。このプロトコルは、STD 12（ RFC 1119）に定義されています。

OCSP（ Online Certificate Status Protocol ） 金融や電子商取引などのアプリケーションでは、CRL よりもタイムリーに証明書失効ステータスを取得する必要があります。OCSP を使用すると、定期的に発行される CRL の代わりまたは補完としてデジタル証明書の現在の失効ステータスを確認できます。OCSP は、RFC 2560 に記述されています。

PEM（ Privacy Enhanced Mail ） 暗号化、認証、メッセージの整合性、および鍵管理に関するプロトコルのスイート。詳細については、RFC 1421 を参照してください。通常、PEM は、証明書などのバイナリ オブジェクトをアルファベットの 64 文字のサブセットを使用する印刷可能なフォーマットに変換するエンコード方式 (Base 64 エンコード方式とも呼ばれる) を指します。

PFS（ Perfect Forward Secrecy ） ある鍵が解読されても、それが他の鍵の解読につながらない性質を指します。PFS を有効にするには、データの転送を保護する鍵から別の鍵を派生しないことが重要です。データの転送を保護する鍵が別の鍵材料から派生されている場合は、その材料から他の鍵を派生しないようにします。PFS（ Public-key Forward Secrecy: 公開鍵転送秘密 ）とも呼ばれます。

PKCS（Public-Key Cryptography Standards: 公開鍵暗号化標準規格 ） PKCS 規格は、RSA Laboratories の文書群です。PKCS 規格の中で重要なものは、RSA 暗号化および署名フォーマットを規定する PKCS＃1、暗号メッセージのカプセル化を規定する PKCS#7、証明書要求を規定する PKCS#10 、スマートカードでよく使用される暗号トークンインターフェイスを規定する PKCS#11 などです。

PKCS #1 この規格は、RSA アルゴリズムによる暗号化とデジタル署名の方法を定義しています。鍵のエンコードとアルゴリズム入力のフォーマットに関する明確な提案が含まれています。

PKCS #7 この規格は、暗号が適用されるデータに関する一般的な構文を定義します。このデータには、暗号オブジェクトのデジタル署名とデジタル エンベロープの再帰的なエンコードが含まれます。

PKCS #8　この規格は、秘密鍵と属性セットを含む秘密鍵情報に関する構文を定義しています。この規格は、暗号化された秘密鍵に関する構文も定義しています。

PKCS #10　この規格は、証明書要求のフォーマットを定義しています。

PKCS #11　この規格は、暗号デバイス（ スマート カードや暗号アクセラレータなど ）のインターフェイスである CryptoKi を定義しています。

PKCS #12　この規格は、ユーザーの秘密鍵、証明書、およびその他のシークレットを保存または転送するためのポータブル フォーマットを定義しています。PKCS #12 は、ユーザーの秘密鍵のインポートおよびエクスポート用として通常の Web ブラウザでサポートされています。

PKCS #15　この規格は、鍵、証明書、およびアプリケーション固有のデータを ISO/IEC 7816 準拠のスマート カードに保存する方法を定義しています。

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。

PKIX　Public-Key Infrastructure（X.509）の略。IETF の同名の作業部会によって策定された X.509 に基づくアーキテクチャとプロトコル群の総称。

PPP（ Point-to-Point Protocol ）　PPP は、ポイントツーポイントリンク上でマルチプロトコルデータグラムを転送するための標準的な方法を提供します。PPP は、STD 51（ および RFC 1661）に定義されています。

RA（ Registration Authority: **登録機関** ）　PKI のオプションのエンティティ。CA とは独立しています。RA が実行する機能は状況に応じて異なりますが、通常は識別情報の認証と名前の割り当て、鍵の生成、トークンの配布、および失効のレポート作成が含まれます。

RC5　1994 年に RSA Security の Ronald Rivest によって考案された対称ブロック暗号。RC5 はブロック サイズとして 32 ～ 128 ビット、鍵長として 0 ～ 2,040 ビットを使用

します。暗号化のラウンド数は 0 ～ 255 です。

RC6 RSA Security の Rivest 、Sidney 、および Yin によって考案された、RC5 に基づく対称ブロック暗号。ブロック サイズ、鍵のサイズ、およびラウンド数は可変です。鍵のサイズの上限は 2,040 ビットです。R C6 は、米国 AES（ Advanced Encryption Standard）の 5 つの最終候補に選ばれた中の 1 つです。

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。

SCEP（ Simple Certificate Enrollment Protocol ） SCEP は Cisco Systems および VeriSign により開発されました。Cisco のルータがサポートする登録プロトコルです。

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。

SNMP (Simple Network Management Protocol: 簡易ネットワーク管理プロトコル)　一般に、ルータなどのネットワーク要素のステータスを監視するために使用されるプロトコル。このプロトコルは、STD 15 (および RFC 1157) に定義されています。

SOCKS　SOCKS は、アプリケーションのゲートウェイ ファイアウォールを通過するためのプロトコルです。ファイアウォール内のアプリケーションは、グローバルインターネット上のリソースにアクセスできます。このプロトコルは、RFC 1928 に定義されています。

SPI (Ssecurity Parameters Index: セキュリティ パラメータ インデックス)　SA を一意に識別するために宛先アドレスおよびセキュリティ プロトコルと併用される任意の値。SPI は、AH プロトコルおよび ESP プロトコルで伝送され、受信した IP パケットをどの SA で処理するかを受信側のシステムで選択できるようにします。SPI は、SA の作成者 (通常は SPI を運ぶ IP パケットの受信者) によって定義されるために、その影響はローカルな範囲に限られます。したがって、一般的に SPI は不透明なビットの文字列と見なされます。ただし、SA の作成者は SPI 内のビットを解釈してローカル処理を行うことを選択できます。この用語は、RFC 2401 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。

TLS（ Transport Layer Security ） TLS は、ストリームに類似する接続に対して機密性、認証、および整合性を提供します。通常、HTTP の接続を保護するために使用します。このプロトコルは、IETF の作業部会によって規格化されています。

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: ユーザー 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。

URI（ Uniform Resource Identifier: 統一リソース識別子 ） URI は、世界またはインターネット上のリソースまたはオブジェクトを識別することを想定しています。URI は、RFC 2396 に定義されています。最もよく使用されているタイプの URI は URL です。

URL（ Uniform Resource Locator: 統一リソース ロケータ ） URL は、Web ページの場所を記述するために使用します。他の多くのコンテキストでも使用できます。URL の例は http://www.dit.co.jp/index.html などです。URL は RFC 1738 および RFC 1808 に定義されています。URL は、URI の特殊なケースです。

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。

WLAN（ Wireless Local Area Network: ワイヤレス ローカル エリアネットワーク ） ワイヤレス LAN。通常、この用語は IEEE 802.11 規格に基づくワイヤレス イーサネット ネットワークを指します。

X.500　X.500 Directory を定義する ITU-T/ISO 共同規格のファミリ。このディレクトリは、証明書や人に関する情報を保存するなどの目的で、多くのアプリケーションに使用できます。X.500 Directory にアクセスするには、通常、LDAP を使用します。

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。

アベイラビリティ　ネットワークへの攻撃によるサービスの拒否または低下を避けるために、セキュリティ上の問題に対処するセキュリティ サービス。たとえば、IPsec では、AH と ESP で再送防止機構を使用することによりアベイラビリティをサポートしています。

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。

暗号学　暗号化方法の数学的基礎を研究する数学の分野。

暗号テキスト　暗号化システムによって暗号化されたテキスト。プレーンテキストの逆です。

イーサネット　イーサネットは、社内ネットワークで最も広く使用されているタイプの LAN（ ローカル エリア ネットワーク ）です。イーサネットでは、ワークステーションごとにネットワークアダプタの製造元から割り当てられた一意の 48 ビット アドレスがあります。イーサネット アドレスと IP アドレスの相互変換には、ARP プロトコルが使用されます。イーサネット上での IP パケットの伝送方法は、STD 41（ および RFC 894 ）に定義されています。

エンド エンティティ 証明書の発行先の人またはアプリケーション。エンドエンティティは、証明書の公開鍵に対応する秘密鍵も所持します。

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ーまたは各ホストが 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。

証明書の登録 証明書の登録とは、認証局 (CA) から公開鍵を証明してもらうことです。この場合、クライアントは CA に公開鍵とその他のデータを証明書要求として提供します。

CA は、この鍵とその他の情報を CA 独自の秘密鍵で署名し、署名した証明書をクライアントに返します。

証明書要求　証明書要求は、要求を行うエンティティの公開鍵およびその他の識別情報を含み、そのエンティティの秘密鍵で署名されます。証明書要求は、エンドエンティティまたは RA によって作成され、CA 宛に送信されます。CA の証明書ポリシーで許可された場合は、その要求に応じた証明書が発行されます。

信頼されるサブネットワーク　直接的または間接的な攻撃に関与しないことを相互に信頼できるホストとルータのサブネットワーク。LAN や CAN などの通信チャネル自体は他のいかなる手段でも攻撃されていないものと仮定されます。

ストリーム暗号　一度に 1 つのビットを暗号化する代表的な対称（ 秘密鍵 ）暗号化アルゴリズム。ストリーム暗号を使用すると、同じプレーン テキストのビットまたはバイトは、暗号化されるたびに異なるビットまたはバイトに変換されます。

スマート カード　スマート カードまたは IC カードは、情報システムのユーザーのセキュアな識別を行うためのデバイスです。通常、スマート カードには、カード上の秘密鍵を使用して秘密鍵操作を実行するプロセッサと、証明書、公開鍵、およびカード使用に関するその他のデータを保持するファイル システムが含まれています。

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 ユーザー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。

証明書のユーザー（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。

ノード 本マニュアルでは、ノードは TCP/IP プロトコルスイートを実装するシステムを意味します。

パケット フィルタリング IP パケットの受け渡しの処理方法を決定する方法。パケット フィルタリングは、IPsec エンジンを通過するすべての IP パケットに適用されます。パケット フィルタリングでは、IP パケットを変更するか、変更なしで渡すか、または破棄することもあります。

パス MTU パス最大転送単位。パス MTU はネットワークの転送元と転送先のアドレスにバインドされます。この点で MTU とは異なります。パス MTU 検出については、RFC 1191 に記述されています。

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。

ファイアウォール　管理ドメインの境界でドメインのセキュリティ ポリシーを実装するノード。ファイアウォールは、通常、アドレスおよびポートベースのパケット フィルタリングを実行します。また、電子メールなどのサービス用にプロキシサーバを用意するのが一般的です。

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。

プロキシ　プロキシは、ファイアウォールとして機能するキャッシュサーバであり、ローカルネットワークを保護します。プロキシ内のアプリケーションは、グローバル インターネット上のリソースにアクセスできます。

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。

有効期間　IKE では、セキュリティの関連付け(SA) の有効期間を意味します。SA を使用できる最大秒数または SA を使用して転送できる最大キロバイト数として指定できます。

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。

NET-G Secure VPN Client
ユーザー マニュアル

2010年3月

株式会社ディアイティ

〒135-0016
東京都江東区東陽 3-23-21
プレミア東陽町ビル
電話　03-5634-7651
ＦＡＸ　03-3699-7048

