NET-G Secure VPN Client ver.2.6.4 Release Note

2021 年 4 月 19 日

株式会社ディアイティ

目　　次

1. はじめに

NET-G Secure VPN Client は、当時の SSH Sentinel 日本語版（現在は Inside Secure 社が継承）をベースに、株式会社ディアイティが IPv6 対応、各 Windows 環境への対応をはじめとする各種の機能を追加した IPsec セキュリティクライアントソフトウェアです。

NET-G Secure VPN Client の最新版である ver. 2.6 シリーズでは、弊社従来製品 NET-G Secure VPN Client ver. 2.5 シリーズをベースに、Windows 10 に対応しました。

本書には、NET-G Secure VPN Client 付属のマニュアルおよびヘルプに記載された情報を補足または更新する情報が記載されています。かならずお読みください。

2. 動作環境

本バージョンの NET-G Secure VPN Client は、以下の Windows 環境で動作します。

- Windows 10（32 ビットまたは 64 ビット）(*1)(*2)(*7)
- Windows 8.1（32 ビットまたは 64 ビット）(*3)(*4)(*5)
- Windows 7 Service Pack 1 (SP1)（32 ビットまたは 64 ビット） (*6)

(*1) Anniversary Update 以降のアップデート版を含みます。
(*2) Windows 10 Mobile は含みません。
(*3) Windows 8 はサポート対象外です。Windows 8.1 をご使用ください。
(*4) Windows 8.1 Update(KB2919355) を適用していない Windows 8.1 はサポート対象外です。
(*5) Windows RT は含みません。
(*6) 更新プログラム KB3033929 を適用する必要があります。詳しくは本書の章「注意事項」の項目「コード・サイニング証明書の SHA-2 対応」をご参照ください。
(*7) Windows 10 November Update (1511) はサポート対象外です。Windows 10 Anniversary Update (1607) 以降をご使用ください。

(**) Windows Vista はサポート対象外です。
(***) Windows XP はサポート対象外です。ただし、Windows XP SP3 で従来の NET-G Secure VPN Client を使用している既存のユーザーは、本バージョンアップへのアップデートを含むサポートを継続して受けることができます。詳しくはお問い合わせください。

上記の Windows 環境であっても以下の Windows では動作しません。

- 日本語版以外の Windows
- IA64 版 Windows

- ARM 版 Windows
- Windows Phone
- Windows Server（サーバー版 Windows）

以下は、NET-G Secure VPN Client のバージョン毎の対応プラットフォームの一覧です。

プラットフォーム	バージョン	NET-G Secure VPN Client のバージョン							注
		2.3 以前	2.3.x	2.4.x	2.5.x	2.6.0	2.6.0.1	2.6.1 以降	
Windows 98	SE	2.0.0-							※1
Windows NT 4.0	SP4 以降	2.0.0-							※1 ※2
Windows Me		2.0.0-							※1
Windows 2000	SP4 以降	2.0.0-	○						※1
Windows XP (32bit のみ)	SP2	○	○						※1
	SP3			○	○	△	△	S	※3 ※4
Windows Server 2003		2.0.0-							※1
	SP1 以降	2.1.4-	○	○					※1
Windows Vista			○						※1
	SP2			○	○	○	○		

注記：　※1　このバージョンのプラットフォームにおける NET-G Secure VPN Client のサポートは終息

※2　Internet Explorer 5.01 以降が必要

※3　△ は非推奨環境

※4　S　は保守契約を締結した既存ユーザーへのみ提供

NET-G Secure VPN Client のバージョン毎の対応プラットフォームの一覧（つづき）

プラットフォーム	バージョン	NET-G Secure VPN Client のバージョン								注
		2.4.x	2.5.x	2.6.0	2.6.0.1	2.6.1	2.6.2	2.6.3	2.6.4	
Windows 7		○								※1
	SP1	2.4.1.2 以降	○	○						※1
	SP1 +KB3033929				○	○	○	○	○	※8
Windows 8			○	○	△					※1 ※3
Windows 8.1			○	○	○					※1
	Update (+KB2919355)			○	○	○	○	○	○	
Windows 10	1507 (RTM)			○	○	○	○	○	○	※5
	1511 November Update				○	○				
	1607 Anniversary Update				○	○	○	○	○	※6
	1703 Creators Update					○	○	○	○	
	1709 Fall Creators Update						○	○	○	
	1803 April 2018 Update						○	○	○	※7
	1809 October 2018 Update							○	○	
	1904							○	○	※9
	1909							○	○	※9
	2004								○	
	20H2								○	

注記：　※1　このバージョンのプラットフォームにおける NET-G Secure VPN Client のサポートは終息

※3　△ は非推奨環境

※5　Windows 10 Enterprise 2015 LTSB (Long Term Service Branch) エディションのみサポート（それ以外のエディションはすでにサービス終了のため）

※6　Windows 10 Enterprise 2016 LTSB (Long Term Service Branch) エディションを含む

※7　NET-G Secure VPN Client ver.2.6.2 については、そのリリース後に対応を確認

※8　Windows 7 の Microsoft によるサポートが 2020 年 1 月 14 日に終了することにご注意ください。NET-G Secure VPN Client はその日以降の任意の時期に Windows 7 を動作対象から除外する予定です。

※9　NET-G Secure VPN Client ver.2.6.3 については、そのリリース後に対応を確認

使用しているコンピュータの Windows バージョンを（Windows 8.1 から Windows 10 などに）更新する前には、必ず 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てください。

本バージョンの 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 10

プロセッサ	PAE,NX,SSE2 をサポートする 1GHz 以上のプロセッサまたは SoC(32 ビット)、 PAE,NX,SSE2 をサポートする 1GHz 以上のプロセッサまたは SoC (CMPXCHG16b,LAHF/SAHF,PrefetchW を実装する)(64 ビット)
メモリ（RAM)	1GB(32 ビット)、または 2GB(64 ビット) あるいは 2GB(Anniversary Update および以降)
ハードディスク容量	100MB 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 8.1

プロセッサ	PAE,NX,SSE2 をサポートする 1GHz 以上のプロセッサ(32 ビット)、 PAE,NX,SSE2 をサポートする 1GHz 以上のプロセッサ（CMPXCHG16b,LAHF/SAHF,PrefetchW を実装する）

	(64 ビット)
メモリ（RAM）	1GB(32 ビット)、または 2GB(64 ビット)
ハードディスク容量	100MB 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(32 ビット)、または 2GB(64 ビット)
ハードディスク容量	100MB 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

3. ver.2.6.3 からの変更点

(1) Windows 10 May 2020 Update (2004)、October 2020 Update (20H2) に対応しました。また、Windows 10 May 2019 Update (1903)、November 2019 Update (1909) に対応済みであることを、本リリースノートの「動作環境」に記載しました。

(2) Windows 10 May 2020 Update (2004)以降において、OS 側の ARP 通信動作の挙動が変わった影響により、仮想 IP アドレスを使用した VPN 接続において通信が不安定になる場合がある問題を改善しました。

4. 注意事項

(1) 64bit 対応

NET-G Secure VPN Client ソフトウェアの 64bit Edition(x64 版)対応は、ドライバ等のカーネルソフトウェアを 64bit ネイティブ対応とし、システムサービスやアプリケーション等の実行プログラムは 32bit 互換レイヤー(Windows On Windows64: WOW64)で動作させています。このため、64bit Edition におけるインストールフォルダは、システムドライブの “¥Program Files(x86)” の下がデフォルトとなります。

(2) アップグレード（上書き、更新）インストール

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済みで、アップグレード可能な場合、本バージョンのインストーラはこれを自動的に更新します。ポリシー、認証鍵などのコンテンツ（設定データ）は通常の場合、アップグレード前のものを保持します。念のためにアップグレードを実行する前にコンテンツ（設定データ）をメモ書きしておくことをお勧めします。（ポリシーについては「ポリシーのエクスポート（名前を付けて保存）」機能を使用することもできます。）

ただし、Windows バージョンを（例えば Windows 7 から Windows 10 などに）アップグレード（更新）した場合は、既存の NET-G Secure VPN Client は動作しなくなります。この場合、既存の NET-G Secure VPN Client をアンインストール (削除) した後に、新しい Windows バージョンに対応する NET-G Secure VPN Client のインストールを行ってください。以前のバージョンをアンインストール（削除）すると既存のコンテンツ（設定データ）も削除されますので、Windows をアップグレードする前にコンテンツ（設定データ）をメモ書きしておいてください。

既存の NET-G Secure VPN Client をアンインストール（削除）せずに Windows をアップグレード（更新）した場合は、既存の設定はもはや参照できませんが、既存の NET-G Secure VPN Client をアンインストール（削除）することは可能です。

(3) Windows 10 を Anniversary Update に更新する場合

Windows 10 Anniversary Update (バージョン 1607) へのアップグレード（更新）は従来の Service Pack 等とは異なり、本章の上記「(2) アップグレード（上書き、更新）インストール」における Windows バージョンのアップグレード（更新）と同じ扱いとなります。つまり、既存の NET-G Secure VPN Client は動作しなくなり、セキュリティ・ポリシー等の既存のコンテンツ（設定データ）は失われます。この場合、Anniversary Update 以前にロールバックして Anniversary Update への更新を行わないか、Anniversary Update 上で既存の NET-G Secure VPN Client をアンインストール（削除）した後に、もう一度 NET-G Secure VPN Client をインストールしてください。NET-G Secure VPN Client をアンインストール（削除）すると既存のコンテンツ（設定データ）も削除されますので、Windows を Anniversary Update に更新する前に（もしくは Anniversary Update 以前にロールバックしてから)、コンテンツ（設定データ）をメモ書きしておいてください。（ポリシーについては「ポリシーのエクスポート（名前を付けて保存）」機能を使用することもできます。）

(4) ダイアルアップ接続

インストール済みの NET-G Secure VPN Client をアップグレードする場合、インストーラを実行する前に接続中の VPN 接続およびダイアルアップ接続をすべて切断してください。そうでない場合は途中で「しばらくお待ちください」というインストーラのダイアログが表示されたまま、先に進まなくなることがあります。このときは接続中のダイアルアップ接続を切断するとインストール動作を継続します。

(5) 非互換の Windows サービス

NET-G Secure VPN Client は、以下の Windows 標準サービスと互換性がありません。

- IKE and AuthIP IPsec Keying Modules(IKEEXT)
  (Windows XP より新しい Winodws)
- IPsec Policy Agent (PolicyAgent)
  (Windows XP より新しい Winodws)
- IPSEC Services(PolicyAgent)
  (Windows XP)

NET-G Secure VPN Client のインストーラは自動的にこれらのサービスを無効に設定します。NET-G Secure VPN Client を削除したのちに、これらのサービスを使用したいときには、手動でこれらのサービスを有効に設定する必要があります。サービスを

有効に設定する方法については以下の「アンインストール（削除）の手順」を参照してください。

(6) コード・サイニング証明書の SHA-2 対応

Microsoft 社のセキュリティ強化措置に対応して、2016 年 1 月 1 日以降にリリースする NET-G Secure VPN Client ではコード・サイニング証明書のハッシュ・アルゴリズムを SHA-1 から SHA-2 に変更しました。

（詳しくは Microsoft の文書

「 Windows Enforcement of Authenticode Code Signing and Timestamping <http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx> 」

を参照してください）

これにともない、以下の各プラットフォームで動作条件等が変更になりました。

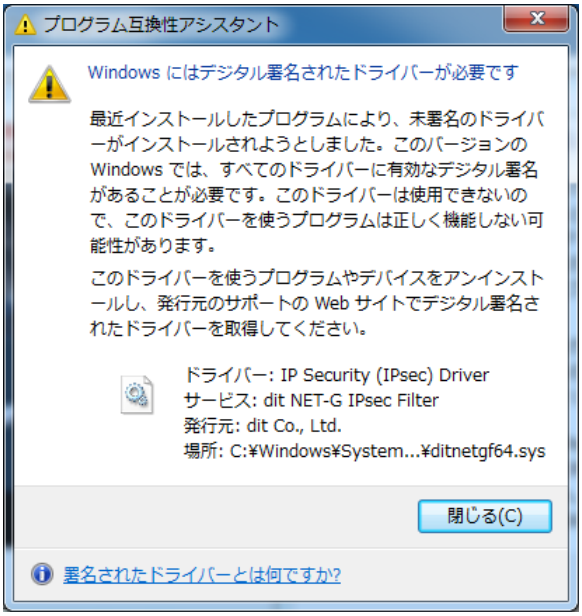
- Windows Vista

NET-G Secure VPN Client ver.2.6.1 以降は Windows Vista に対応しません。

- Windows 7 Service Pack 1 (SP1)

Windows 7 SP1 においては、コード・サイニング証明書の SHA-2 に対応するために更新プログラム KB3033929 を適用する必要があります。Windows Update によって更新プログラムを日常的にインストールしていない場合は、手動で適用する必要があるかもしれません。その場合、KB3033929 の前に KB3035131 を適用する必要があります。Windows 7 SP1 を新規にインストールする場合には、Windows 7 SP1 のリリース以降 2016 年までの更新を総括した convinience rollup KB3125574 を最初に適用することをお勧めします（上記の KB3035131 と KB3033929 も含まれています）。ただし、convinience rollup を適用するためには、事前に KB3020369 を適用する必要があります。

KB3033929 を適用していない場合、NET-G Secure VPN Client のインストール中に、以下のメッセージが表示されることがあります。



このメッセージが表示された場合、NET-G Secure VPN Client のインストールが手順通り終了したように見えても動作しません。上記を参照して KB3033929 を適用してください。

(7) セキュリティ対策ソフトウェア

ウィルスバスター コーポレートエディション XG は、 NET-G Secure VPN Client のインストールを失敗させることがあります。デバイス監視機能を持つセキュリティ対策ソフトウェアを導入済みのシステムに NET-G Secure VPN Client をインストールするときには、まずセキュリティ対策ソフトウェアをアンインストールし、NET-G Secure VPN Client をインストール後に、元のセキュリティ対策ソフトウェアを再インストールすることで、両者を共存させることが可能な場合があります。なお、セキュリティ対策ソフトウェアの削除および再インストールについては、所属する組織のシステム管理者に確認してください。

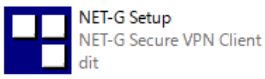
5. インストールの手順

本製品に添付されている文書「NET-G Secure VPN Client ユーザー マニュアル」の第 2 章の項目 2.2.「NET-G Secure VPN Client のインストール」の内容を以下のように訂正します。

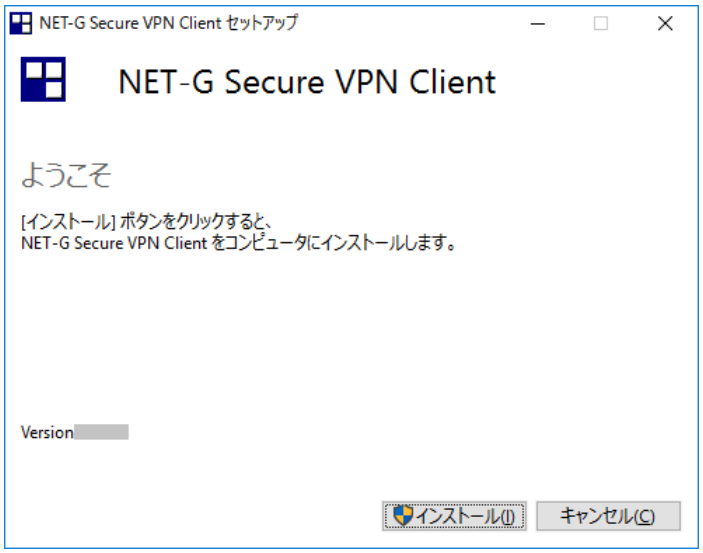
(1) インストールを実行する前に、システムの復元ポイントを作成しておくことができます（任意）。復元ポイントの作成方法は Windows のバージョンによって異なります。

一部のセキュリティ対策ソフトウェアは、NET-G Secure VPN Client のインストールを失敗させることがあります。詳しくは本リリースノートの「注意事項」を参照してください。

CD-ROM からのセットアップの場合、自動実行で表示されるメニューの「インストール」をクリックしてください。
または、CD-ROM を開き、NET-G Secure VPN Client インストーラ アイコン [NET-G Setup.exe] を開いてください。 インストーラは、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。



(2) [ようこそ] ダイアログが表示されます。[インストール]ボタンをクリックしてください。

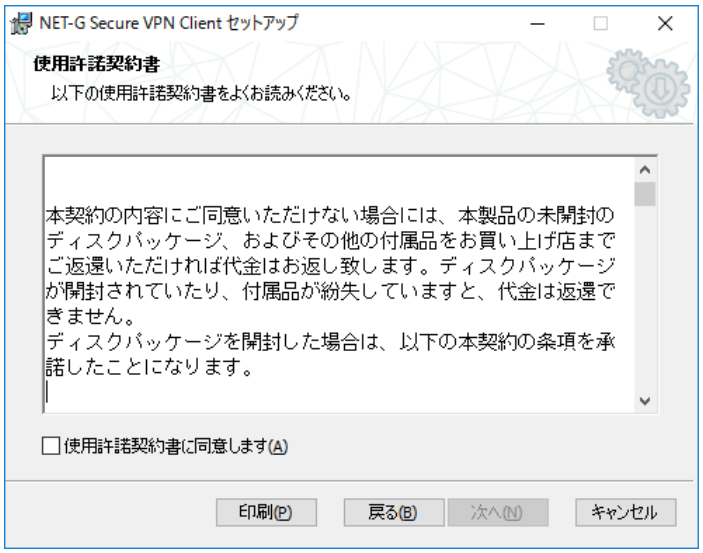


(3) [ユーザー アカウント制御]ダイアログが表示されます。[続行]をクリックしてください。

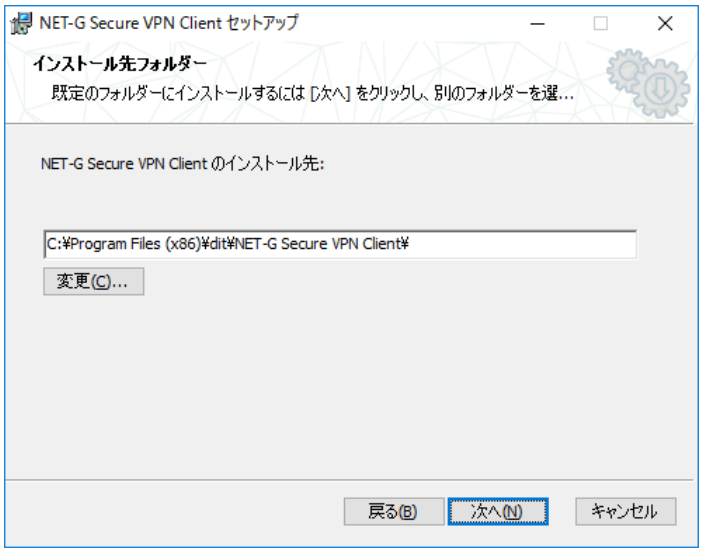
(4) 準備中を示すダイアログが表示されます。しばらくお待ちください。

(5)　[NET-G Secure VPN Client セットアップ]ダイアログが開きます。[次へ]ボタンをクリックします。

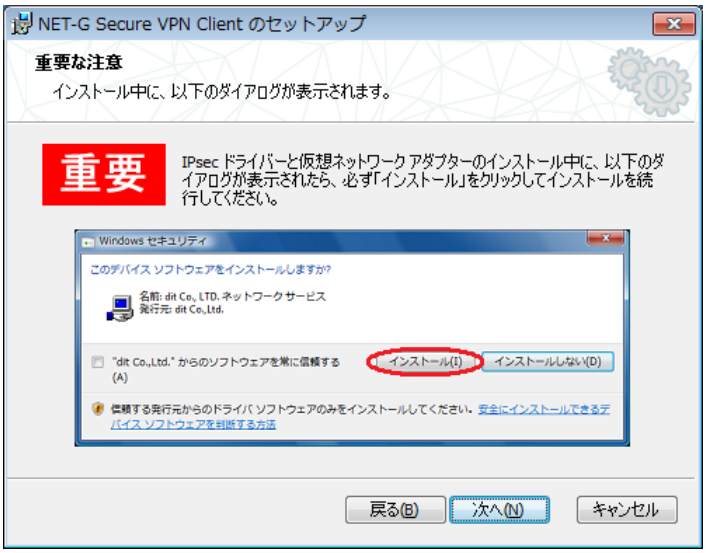
(6)　[使用許諾契約書]画面が表示されます。使用許諾契約書の文面をよく読んでください。契約内容に同意する場合は、[使用許諾契約書に同意します] チェックボックスをチェックし、[次へ] ボタンをクリックします。



(7) [インストール先フォルダー] 画面が表示されます。[変更] ボタンをクリックすると、デフォルトのインストール先のフォルダーを変更することができます。 インストール先のフォルダーが決まったら、[次へ] ボタンをクリックします。

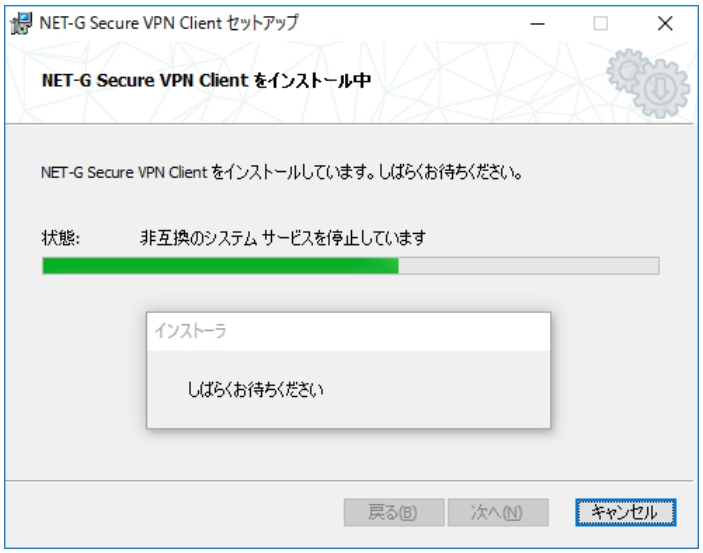


(8) インストール先の Windows のバージョンによっては、以下の[重要な注意]画面が表示されます。この画面は、インストール中に必要となる手動操作の注意点を説明しています。内容をよく読んで、[次へ]ボタンをクリックします。

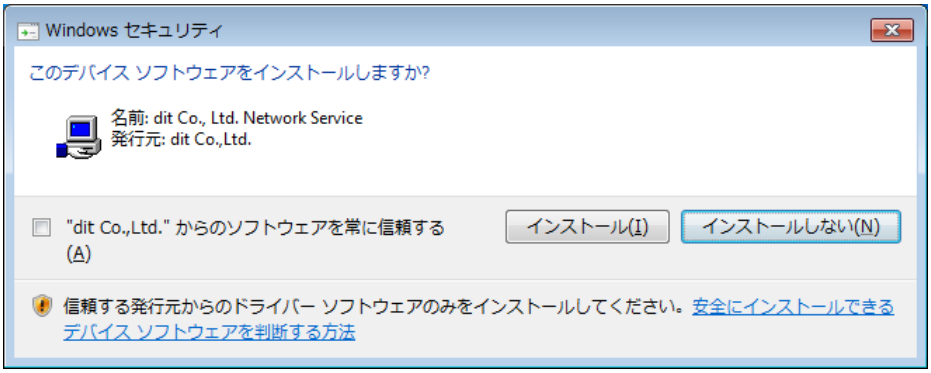


(9) [NET-G Secure VPN Client のインストール準備完了]画面が表示されます。[インストール]ボタンをクリックするとインストール作業を開始します。この画面の後は[キャンセル]ボタン等でインストール作業を中断しないでください。

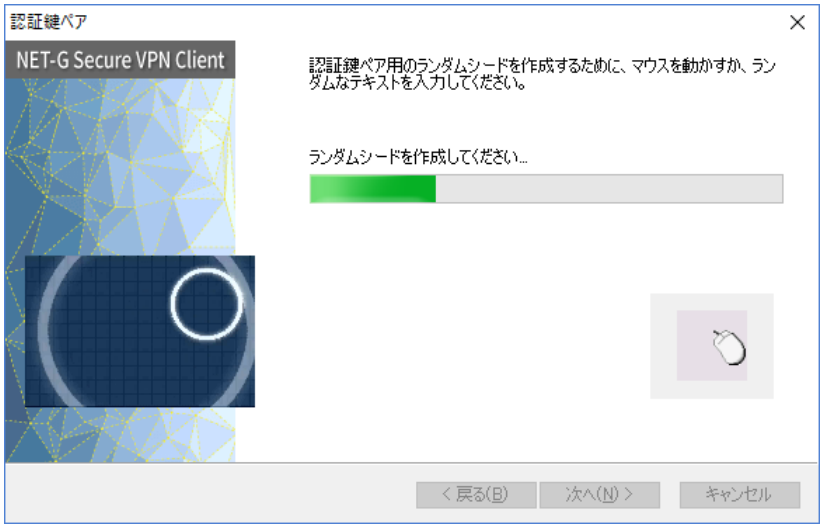
(10) [NET-G Secure VPN Client をインストール中]画面が表示され、インストール作業が実行されます。進行具合に応じて画面が更新されます。時間がかかるときは、[しばらくお待ちください]という[インストーラ]ダイアログが表示されることもありますが、そのままお待ちください。



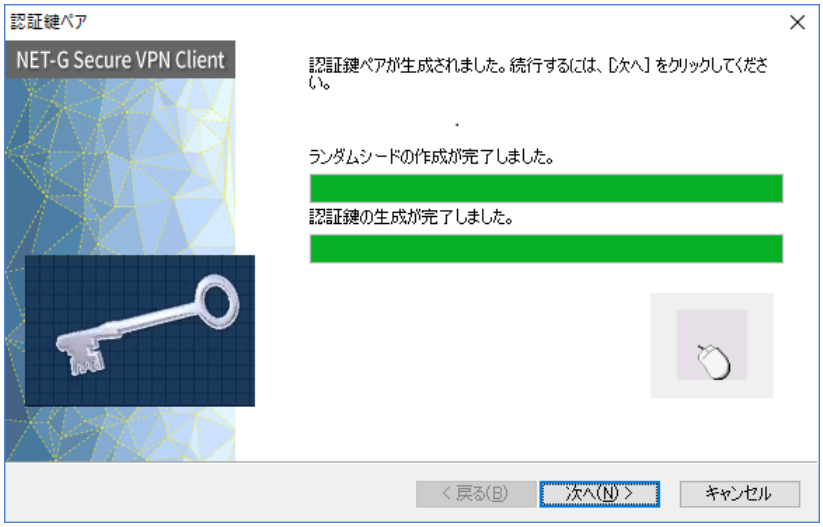
(11) インストール先の Windows のバージョンによっては、[Windows セキュリティ]というタイトルの警告メッセージが数回表示されますが、すべて**[インストール]をクリックしてください**。なお、[インストール]をクリックするときに、["dit Co., Ltd."からのソフトウェアを常に信頼する] にチェックが入っている場合、これ以降のメッセージ表示が省略されます。（Windows 8 以降ではこのオプションはデフォルトで選択されています。その他の Windows では明示的に選択する必要があります。）



(12) NET-G Secure VPN Client の設定ウィザードが起動します。最初に、[認証鍵ペア]画面が表示されます。ここではデフォルトの証明書を作成するための認証鍵を生成します。乱数の初期値を与えるために、マウスを動かすか、キーボードの任意のキーを叩いてください。ランダムシードの作成に足りるまでマウスまたはキーボードの操作を続けてください。

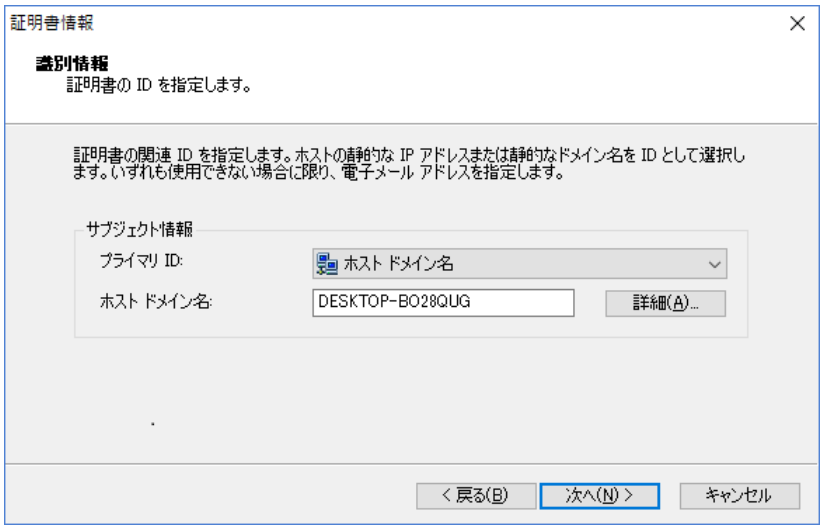


(13) 必要な長さの初期値を収集すると、自動的に認証鍵ペアを生成します。[次へ]ボタンをクリックしてください。

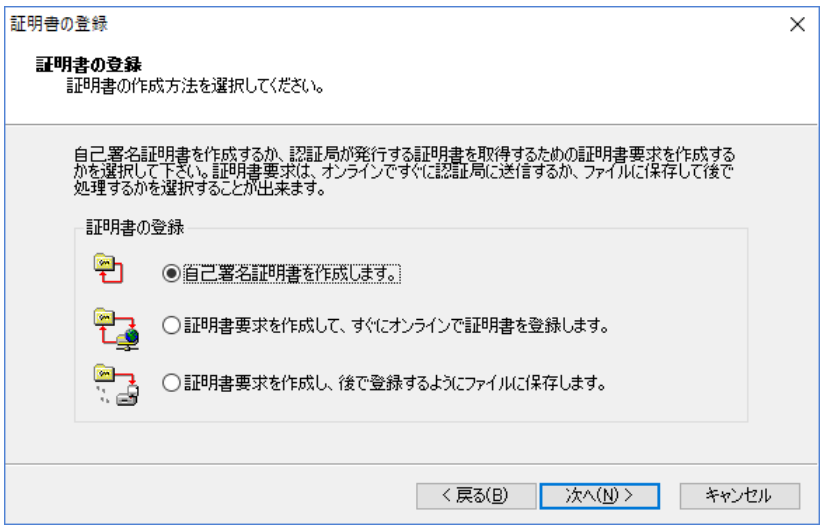


(14) [証明書情報]画面が表示されます。証明書について管理者から指定されている場合は、指定された手順に従ってください。なお、証明書は後ほど[ポリシー エディタ]を使用して作成することもできますので、とりあえず証明書を使用する予定がない場合や証明書についてよくわからない場合はそのまま [次へ]ボタンをクリッ

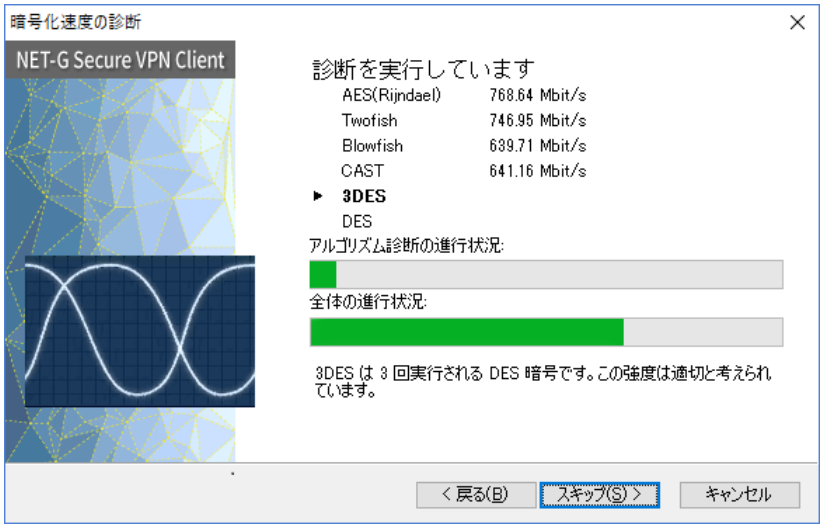
クしてください。

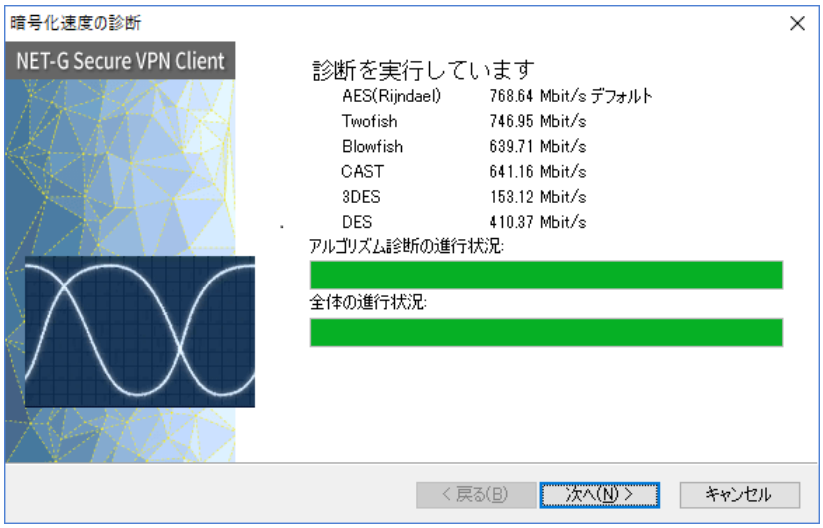


(15) [証明書の登録]画面が表示されます。証明書を作成、保存、登録することができます。証明書について管理者から指定されている場合は、指定された手順に従ってください。なお、証明書は後ほど[ポリシー エディタ]を使用して作成、保存、登録することもできますので、とりあえず証明書を使用する予定がない場合や証明書についてよくわからない場合はそのまま [次へ]ボタンをクリックしてください。

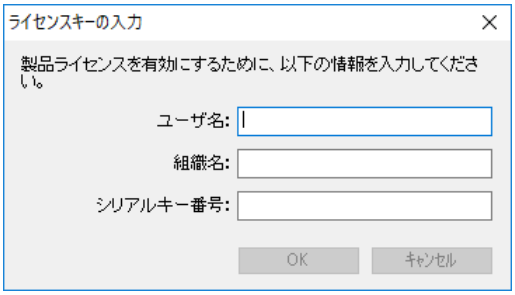


(16) [暗号化速度の診断]画面が表示されます。この画面では、ご使用の PC における暗号化速度の最大値を測定し、画面に表示します。測定された速度は、後ほど暗号化方式を選択するときの目安にすることができます。診断が終了したら[次へ]ボタンをクリックしてください。または、診断中に[スキップ]ボタンをクリックしてください。[スキップ]ボタンで診断を中断しても問題は発生しません。

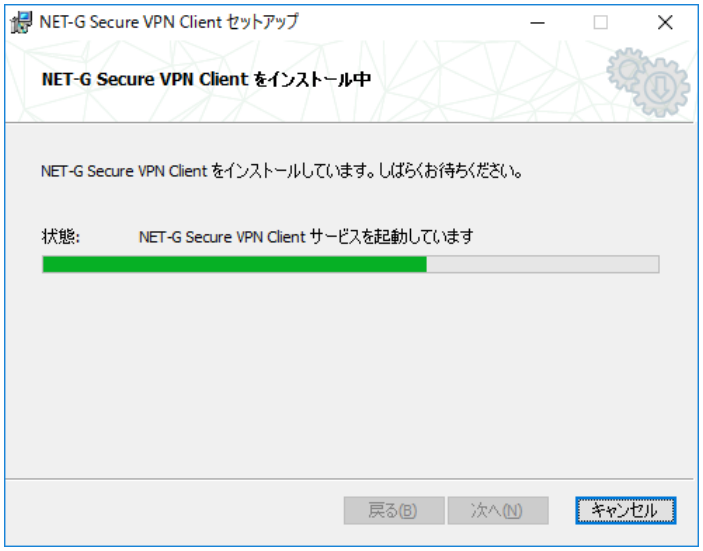




(17) [ライセンスキーの入力]ダイアログが表示されます。[ユーザ名]は必ず入力する必要があります。[会社名]はオプションです。[シリアルキー番号]には製品購入時に通知された番号を入力してください。[シリアルキー番号]を入力しないで[OK]ボタンをクリックすると、期間限定の評価版として動作します。

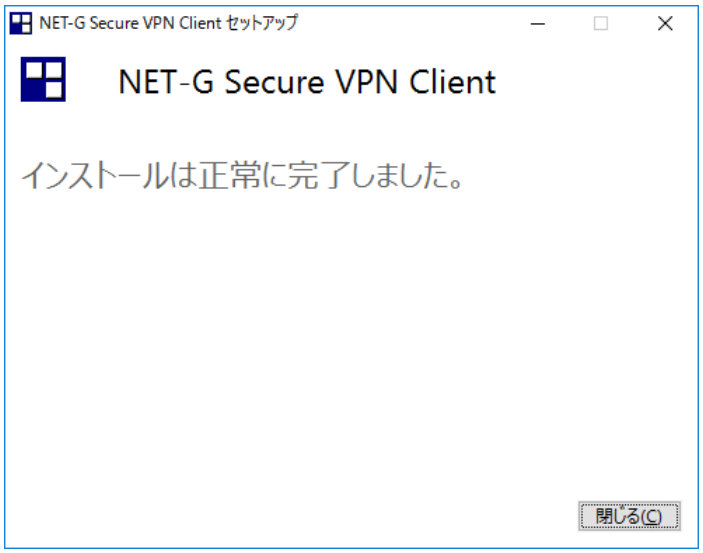


(18) ライセンスキーの入力が完了すると、インストール作業の最後の段階として NET-G Secure VPN Client の起動処理を行います。しばらくお待ちください。



(19) [セットアップ ウィザードを完了しました]画面が表示されます。[完了]ボタンをクリックします

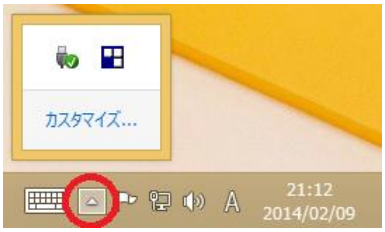
(20) [インストールは正常に完了しました。]画面が表示されます。[閉じる]ボタンをクリックします。NET-G Secure VPN Client はすでに起動しています。



NET-G Secure VPN Client を起動する前にシステムの再起動が必要な場合には、再起動を求める以下の画面が表示されます。[再起動]ボタンをクリックすると、PC は直ちに再起動します。再起動後に NET-G Secure VPN Client は自動的に起動します。

6. インストール後の注意点

(1) コンピュータにログオンすると、Windows タスクバーの右側の通知領域（システムトレイまたはタスクトレイとも言います）に NET-G Secure VPN Client の アイコンが表示されます。Windows 7 および以降の Windows の場合、通知領域のアイコンは通常隠されています。通知領域の▲アイコンをクリックすると隠されているアイコンが表示されます。



Windows 10 の場合は、通知領域の ∧ アイコンをクリックすると隠されているアイコンが表示されます。(通知領域に ∧ アイコンが表示されていないときは、タスクバーを長押しして、メニューから「すべての通知アイコンを表示」コマンドを選択してください。)

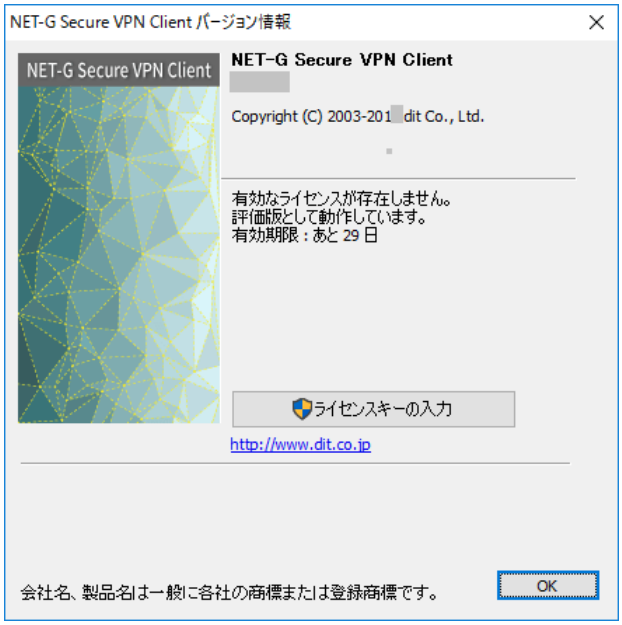
NET-G Secure VPN Client のアイコンを常時表示するためには、アイコンをメニューバーにドラッグ＆ドロップして移動します。

Windows 7 および以降の Windows の場合、上記の操作によって NET-G Secure VPN Client のアイコンを常時表示することをおすすめします。（本書およびマニュアル、ヘルプにおいては、この操作を行った状態を説明に使用しています。）

(2) NET-G Secure VPN Client の通知領域のアイコンの上でマウスの右ボタンをクリ

ックすると、メイン メニューが開きます。

(3) 評価版としての有効期限を確認したり、購入したシリアルキー番号を入力して製品版に移行したりするためには、NET-G Secure VPN Client のメインメニューから[バージョン情報]を選択します。



(4) NET-G Secure VPN Client の通知領域のアイコンが淡色表示になっているときは、ポリシー マネージャ、またはカーネルモードドライバが何らかの理由で正常に動作していません。このとき、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ません。

(5) Windows 7 および以降の Windows において、インストールできる NDIS フィルタドライバの数には制限があります。NDIS フィルタドライバは NET-G Secure VPN Client だけでなく、ウィルス / セキュリティ対策ソフトウェアや、仮想 PC ソフト

ウェアなどでも使用されています。NDIS フィルタドライバの数の制限を超えると、NET-G Secure VPN Client をインストールしても通知領域のアイコンが淡色表示のまま使用可能になりません。レジストリキー HKEY_LOCAL_MACHINE\SYSTEMS\CurrentControlSet\Control\Network の DWORD 値 MaxNumFilters を増やすことによって、この制限を緩和することができます。この値の最小値は 8、最大値は 14 で、デフォルト値は 8 です。

(6) 使用するネットワーク接続の[プロパティ]ページの[詳細設定]タブにプロパティ[IPv4 Checksum Offload]（または [IPv4 チェックサム オフロード] 等の名称のこともあります。もしくは [TCP/IP オフロードのオプション] 等のプロパティ項目を開くと表示されることもあります。）が存在し、その値が[Enabled]（または[On]、[有効]、[使用]等の名称のこともあります。）のとき、NET-G Secure VPN Client の IPsec 接続は行われるのに、当該 IPsec を経由したデータ通信が正常に疎通しない、ということがあります。NAT-Traversal の設定を確認してもなお通信が正常に行えないときは、上記チェックサム オフロードの設定を[Disabled] （[Off]、[無効]、[使用しない]等の名称のこともあります。）に変更してみてください。

(7) Windows 10 Anniversary Update および以降の Windows 10 をプリインストールした PC に、ver.2.6.1 より前の NET-G Secure VPN Client をインストールした場合、PC のセキュアブート(Secure Boot) 設定をオフまたは無効にする必要がありました。 本バージョンの NET-G Secure VPN Client に更新した後は、セキュアブートの設定をオンまたは有効に設定し直してかまいません。なお、セキュアブートの設定方法は PC によって異なりますので当該機種のマニュアル等をご参照ください。

7. 更新（アップグレード）の手順

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、NET-G Secure VPN Client のインストーラを起動すると、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。

インストール パッケージを起動および起動したあとの操作は、本書の章「インストールの手順」と同じです。ただし、更新（アップグレード）においては[使用許諾契約書]画面と[インストール先フォルダー] 画面、そして[重要な注意]画面は表示されません。

NET-G Secure VPN Client の設定ウィザードは起動しません。

[ライセンスキーの入力]ダイアログは必要に応じて表示されます。

8. アンインストール（削除）の手順

Windows バージョンのアップグレード（更新）前に、NET-G Secure VPN Client を削除してください。そして、Windows バージョンのアップグレード（更新）後に NET-G Secure VPN Client を再インストールしてください。例えば、Windows 7 を Windows8 に更新する場合や、Windows 8 を Windows8.1 に更新する場合、Windows 8.1 またはそれ以前の Windows を Windows 10 に更新する場合は、一旦 NET-G Secure VPN Client を削除してください。

通常の Service Pack や Update といった同一バージョンの Windows の更新では、NET-G Secure VPN Client を削除する必要はありません。ただし、Windows 10 から Windows 10 Anniversary Update への更新は特別で、Windows バージョンのアップグレード（更新）と同じ扱いが必要です。つまり、NET-G Secure VPN Client の削除と再インストールが必要となります。

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ーに保存します。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。

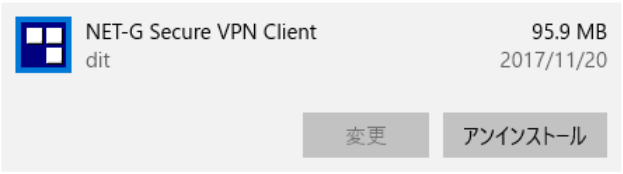
(2) 他のアプリケーションの保存されていないデータもすべて保存し、すべての開いて

いるアプリケーションを終了します。

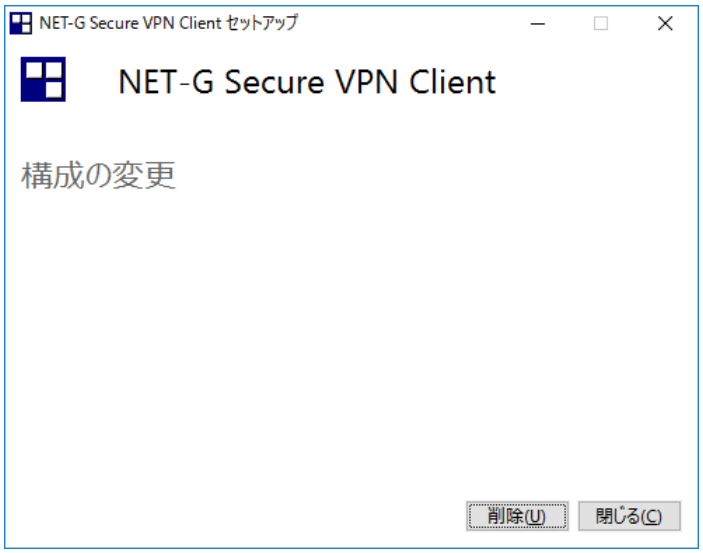
(3) インストールを実行する前に、システムの復元ポイントを作成しておくことができます（任意）。復元ポイントの作成方法は Windows のバージョンによって異なります。

(4) [コントロール パネル]を開き、[プログラムのアンインストール]をクリックするか、[プログラムと機能]を開きます。または、[Windows の設定]を開き、[アプリと機能]を選択します。

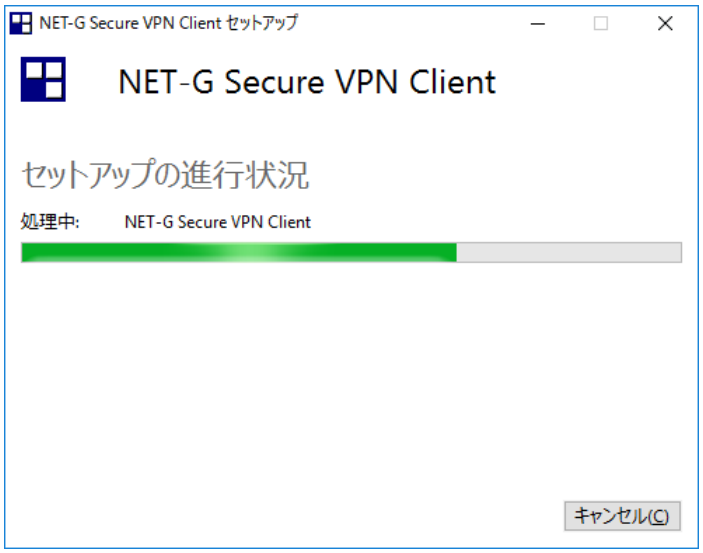
(5) 一覧から[NET-G Secure VPN Client]を選択し、[アンインストール]を選択します。



(6) [NET-G Secure VPN Client セットアップ]の[構成の変更]画面が表示されます。[削除]ボタンをクリックします。



(7) [NET-G Secure VPN Client セットアップ]は進行状況を表示します。しばらくお待ちください。



(8) 削除が完了すると、以下のような再起動を求める画面が表示されます。[再起動]ボタンをクリックするとコンピュータが再起動します。

NET-G Secure VPN Client をアンインストール（削除）したのち、NET-G Secure VPN Client のインストーラが無効にした Windows の各機能を使用したいときには、必要に応じて以下の手順を実行してください。

(1) [コマンド プロンプト]を管理者として実行します。実行の方法は Windows のバージョンによって異なります。

(2) IPv6 テンポラリアドレスを使用するためには、以下のコマンドを入力します。

```
netsh interface ipv6 set privacy state=enabled
```

(3) システム標準の IPsec 機能を使用するためには、以下のコマンドを入力します。
（start=と auto の間には空白を入れてください）

```
sc config PolicyAgent start= auto
```

Windows XP より後の Windows の場合は、さらに以下のコマンドも入力します。
（start=と auto の間には空白を入れてください）

```
sc config IKEEXT start= auto
```

(4) コンピュータを再起動します。

9. 既知の問題点

(1) YAHAMA RTX シリーズのセキュリティゲートウェイとの IPv6 IPsec 通信は行えません。これは、YAMAHA RTX シリーズ側の制限によるものです。

(2) IKE 設定モード（CFGMODE）を使用する VPN 接続において、接続を開始してから IKE Quick Mode が完了するまでの間に対向機器との通信が途絶すると、VPN 接続は正常に完了したと表示されても実際の通信が正常に機能しない状態となることがあります。この場合、いったん切断してから再度接続してください。

(3) PC が接続先機器への複数のルートを持ち、それらのメトリックが同一のとき、CISCO 社製の接続先機器に対して NAT Traversal を使用した VPN 接続を行うと接続に失敗する場合があります。使用するインタフェースまたはゲートウェイのメトリックが他の経路のメトリックより小さくなるように設定を修正してください。

(4) Windows XP より後の Windows において、IPv4 プロトコルをアンインストール（削除）すると NET-G Secure VPN Client は正常に動作しません。

(5) ポリシー エディタでポリシーの追加を行うとき、ポリシー名として“_”(アンダースコア) を含む名前を指定するとエラーとなり、実行できません。ファイル名に“_”を含むポリシーファイルをダブルクリックしたときも同様のエラーとなります。

10. 機能制限

(1) 仮想 IP アドレスのサブネットマスクを all 0 または all 1 に設定すると、IPsec 通信が行えません。サブネットマスクは all 0 でなく、最下位の 2 ビット以上が 0 である必要があります。

(2) 公開暗号鍵方式は動作いたしません。

(3) IPsec は ESP のみ使用可能です。AH の使用は設定できません。

(4) 証明書管理の自動管理では、トランスポートプロトコルとしてHTTPのみをサポートします。LDAP には対応していません。

(5) 証明書失効確認は、LDAP にのみ対応しています。

(6) UDP カプセル化オプションは、IPsec モードが Transport の場合にのみ使用できます。Tunnel モードには対応していません。

(7) IPv6 リンクローカルアドレスおよび IPv6 テンポラリアドレス（プライバシーアドレス）を使用した IPsec 通信には対応していません。

(8) 6to4, ISATAP, 6over4、teredo, hexago トンネルには対応していません。

(9) [インターネット接続の共有]および[ネットワーク ブリッジ]を使用した接続には対応していません。

(10) 一つのネットワークインタフェースに複数の IPv4 アドレスが割り当てられている場合には対応していません。

(11) ホスト名およびゲートウェイ名によるアドレスの解決は、IPv4 アドレスに対してのみ有効です。IPv6 ホストを指定する場合は、IPv6 アドレスを直接指定してください。

11. 改版履歴

ver.2.6.3 での変更点（2019/4/9）

(1) Windows 10 October 2018 Update (1809) に対応しました。また、Windows 10 April 2018 Update (1803)に対応済みであることを、本リリースノートの「動作環境」に記載しました。

(2) Windows 7 のサポート終了に関する注意を本リリースノートの「動作環境」に記載しました。

(3) デバイス監視機能を持つセキュリティ対策ソフトウェアが本ソフトウェアのインストールを阻害する件について、本リリースノートの「注意事項」に記載しました。

(4) Windows 10 において、ポリシーマネージャ（NET-G Secure VPN Client サービス：SSHIPM）が開始するとブルースクリーンが発生することがある、という問題を改善しました。

(5) メモリ不足の際の挙動を改善しました。

(6) ポリシーエディタの VPN 規則のパラメータとして、 [IKE 候補]の[IKE グループ]、および[IPsec 候補]の[PFS グループ]の選択肢に[MODP 2048 (group 14)]を追加しました。

(7) NET-G Secure VPN Client ソフトウェアの削除（アンインストール）を実行しても、NET-G Secure VPN Client 仮想ネットワーク接続アダプタを削除（アンインストール）しない、という問題を修正しました。

(8) 従来バージョンの NET-G Secure VPN Client ソフトウェアでは、Windows 10 October 2018 Update (1809)において、ポリシーエディタの[VPN 接続]の[全般]プロパティの[仮想 IP アドレス]設定で DNS サーバを設定したときの動作が正常に行われない、という問題を修正しました。

(9) インストーラに[修正]機能を追加しました。また、インストーラはドライバ追加時の詳細情報をログファイルに残すようになりました。

ver.2.6.2 での変更点（2018/05/23）

(1) Windows 10 Fall Creators Update (1709) に対応しました。

(2) Windows 10 November Update (1511) を動作対象から除外しました。Windows 10 Anniversary Update (1607) 以降をご使用ください。

(3) Windows 10 において、ポリシーエディタ等のダイアログ表示が、Windows 7 における表示よりも縦長に表示される、という問題を一部改善しました。

(4) ユーザーマニュアルおよびヘルプの記述および画像イメージを更新しました。

(5) ポリシーのエクスポートとインポートを繰り返すと、ポリシーが正しくインポートできなくなることがある、という問題を改善しました。

(6) Windows 7 以降において、PPPoE やダイアルアップ接続を使用して IPsec VPN 接続

を行うと、通信データの受信に失敗するため通信が行えないことがある、という問題を改善しました。

(7) Windows 7 以降において、起動時に自動接続する VPN 接続が失敗し、接続を再起動しても接続できない、という問題が発生することがある、という問題を改善しました。

(8) Windows 7 以降の 32 ビットプラットフォームにおいて、不規則にブルースクリーンが発生することがある、という問題を改善しました。

ver.2.6.1 での変更点（2016/12/20）

(1) Windows XP SP3 を動作対象から除外しました。ただし、既存のユーザーは本バージョンにアップデートすることが可能です。リリースノートから Windows XP における操作手順などの記述を削除しました。

(2) Windows Vista SP2 を動作対象から除外しました。

(3) Windows 8 を動作対象から除外しました。Windows 8.1 をご使用ください。

(4) Windows 8.1 Update（KB2919355）を適用していない Windows 8.1 を動作対象から除外しました。Windows 8.1 Update を適用してください。

(5) Windows 10 Anniversary Update 以降をプリインストールまたは新規インストールした PC に NET-G Secure VPN Client ver.2.6.0.1 をインストールしたとき、Secure Boot を無効に設定しないとネットワーク接続の通信が行えない状態になる、という問題点を修正しました。

(6) ポリシーエディタのパラメータ候補テンプレート”normal”に、IKE 通信の整合性関数 SHA256 を、IPsec 通信の整合性関数 HMAC-SHA256 を追加しました。これらのパラメータをサポートしないルータでは、これらのパラメータが候補に含まれることが接続エラーの原因となることがあります。その場合は、これらのパラメータを選択せず、かつ［選択した値のみを候補に加える］チェックボックスを選択してください。

(7) ポリシーエディタで VPN 接続を新規追加したときのパラメータ候補テンプレート”normal”の整合性関数のデフォルトを、従来の MD-5/HMAC-MD5 から SHA-1/HAMC-SHA-1 に変更しました。

(8) デフォルト応答における整合性関数のデフォルトを、従来の MD-5/HMAC-MD5 から SHA-1/HAMC-SHA-1 に変更しました。

(9) インストーラの名称を［Setup.exe］から［NET-G Setup.exe］に変更しました。また、インストーラの UI を変更しました。

(10) インストーラは、再起動の必要性を判断して再起動を求めるメッセージを表示するようになりました。

(11) プログラムおよびデータ内で使用されている画像イメージの一部を更新しました。

(12) Windows 10 Creators Update に対応しました。

ver.2.6.0.1 での変更点（2016/09/09）

(1) Windows 10 Anniversary Update が動作対象に含まれることを本リリースノートに記載しました。ただし、従来の Windows 10 を Windows 10 Anniversary Update に更新すると、本バージョンを含む NET-G Secure VPN Client は動作しなくなり、既存のポリシー等の設定は失われます。詳しくは本書の「注意事項」内の項目「Windows 10 を Anniversary Update に更新する場合」を参照してください。

(2) Windows 8 が近い将来に動作対象から外れることの予告、および Windows Vista に関する注意点を本リリースノートの「動作環境」に記載しました。

(3) コード・サイニング証明書のハッシュ・アルゴリズムを SHA-1 から SHA-2 に変更しました。これに関連して、本バージョン以降の NET-G Secure VPN Client は、Windows Vista においてのみ従来の ver. 2.6.0 のドライバをインストールします。この結果、本バージョンおよび以降のバージョンの一部の変更点は Windows Vista において適用されなくなります。また Windows 7 Service Pack 1 において KB3033929 の適用が必須となりました。詳しくは、詳しくは本書の「注意事項」の項目「コード・サイニング証明書の SHA-2 対応」をご参照ください。

(4) 【Windows Vista を除く】ネットワーク接続の Hardware Checksum Offload との親和性の向上。ただし、残念ながら全ての場合で問題が解決したわけではありません。問題が発生したときは本書の「インストール後の注意点」を参照してください。

(5) 【Windows Vista を除く】FITELnet ルーターとの接続中に IKE SA の寿命が尽きたとき、その後の IKE SA の再確立に失敗するため接続が切断されることがある、という問題を解決しました。

(6) インストーラは Windows Vista Service Pack 2 より前の Windows Vista をインストール対象から除外するようになりました。また、 Windows 7 Service Pack 1 より前の Windows 7 をインストール対象から除外するようになりました。

ver.2.6.0 での変更点（2015/08/24）

(1) Windows 10 に対応しました。

(2) Windows 8 および以降において、ポリシーマネージャで VPN 接続の「診断」を実行して「詳細」を表示すると、「調査」タブおよび「結果」タブの表示の下端がウィンドウでクリップされてすべて表示されない、という問題を修正しました。

(3) Windows 8 および以降において、NET-G Secure VPN Client の仮想ネットワーク接続のインストール時の名称が「NET-G VPN 接続」ではなく、「イーサネット」と表示されていた問題を修正しました。

(4) ポリシーマネージャで複数のポリシーを作成し適用したとき、ポリシー名が作成順でもソート順でもない不思議な順番で表示される、という問題を修正しました。複数のポリシーはポリシー名の文字列ソート順に表示されるようになりました。

(5) マニュアルの第 2 章「NET-G Secure VPN Client のインストールと削除」の 2.1「要件」に記載されていない Windows 8/8.1/10 における NET-G Secure VPN Client インストールの要件をリリースノートの第 2 章「動作環境」に記載しました。同時に Windows Vista/7 における要件を修正しました。

ver.2.5.0.1 での変更点（2015/05/17）

(1) Windows 8.1 Update が動作対象に含まれることをリリースノートに記載しました。また、Windows XP が動作対象から外れることの予告をリリースノートに記載しました。

(2) Juniper SSG5 への L2TP を使用した VPN 接続で、NAT ルータを介して接続できない、という問題を修正しました。

(3) Windows Vista 以降で、NET-G ドライバは promiscuous モードおよび loopback モードのパケットを通過させるようになりました。これにより、Wireshark などパケットキャプチャリングソフトウェアで送信パケットが見えない、という問題が修正されました。

(4) DPD を使用しないときに DPD リクエストを送信するときがある、という問題を修正しました。

(5) Windows 8/8.1 において、ダイアルアップ接続経由または PPPoE 接続経由のインターネット接続が NET-G によって阻害される、という問題を修正しました。

ver.2.5 での変更点（2014/04/23）

(1) Windows 8、および Windows 8.1 に対応しました。

(2) Windows 7 RTM(Service Pack なし)はもはやサポートされません。この環境における動作は検証されていません。Windows 7 Service Pack 1(SP1)および以降をご使用ください。

(3) Windows Vista Service Pack 1(SP1)および以前 (RTM = Service Packet なし)はもはやサポートされません。これらの環境における動作は検証されていません。Windows Vista Service Pack 2(SP2)をご使用ください。

(4) Windows Vista 以降で使用するフィルタドライバ ditNETGf*.sys の実装を変更しシステムイベントに起因する問題を改善しました。

(5) ポリシーをファイルに保存し、読み込むことを繰り返すと、ルール名に"rule_"が前置されてゆき、ポリシーが読み込めなくなる、という問題を改善しました。

(6) Windows 7 で Intel Wireless アダプタを使用しているとき、スリープ時にブルースクリーンとなることがある、という問題を修正しました。

(7) ポリシーインポート時に日本語の一部が正しくインポートされない、という問題を修正しました。

(8) [仮想 IP アドレスを取得する]の設定が[手動で設定]のとき、かつ分割トンネリングを許可した VPN 接続で、接続を切断したときの処理に誤りがあり、メモリリークが発生するほか、そののちに他の接続先に接続しても通信ができなくなることがある、という問題を修正しました。

(9) デフォルト状態のルールで DHCPv6 が許可されていないため、ネットワークインタフェースに IPv6 アドレスが割り当てられないことがある、という問題を修正しました。

(10) 論理 CPU が複数ある PC で、ポリシー内の設定（接続、規則）等がすべて消えて見えなくなることがある（Windows を再起動すると見えることもある）、という問題を修正しました。

ver.2.4.2.1 での変更点（2011/09/29）

(1) 分割トンネリングを許可した VPN 接続において、ローカルネットワークの IP アドレス範囲が接続先のリモートネットワークの IP アドレス範囲に包含されるとき、ローカルネットワークへの通信およびローカルネットワーク上のデフォルトゲートウェイを経由したインターネットへの通信が行えない、という従来の動作を変更し、ローカルネットワークへの通信およびローカルネットワーク上のデフォルトゲートウェイを経由したインターネットへの通信を許可するようになりました。
ただし、[L2TP]または[IPsec 経由の DHCP]を使用して[仮想 IP アドレス]を割り当てるときは従来と同じ動作となります。
なお、レジストリキー
"HKEY_LOCAL_MACHINE¥SOFTWARE¥dit¥Net-G Secure VPN Client"
の DWORD 値"NoPassLocal"に値 1 を設定したときは、すべての VPN 接続において従来と同じ動作となります。（デフォルトではこの DWORD 値は存在しません。）
（このレジストリを変更したときは、ポリシーマネージャの再起動またはシステムの再起動が必要です。）

(2) ポリシーエディタの VPN 接続の[規則のプロパティ]において、[仮想 IP アドレスを取得する]の設定が[手動で設定]のとき、[詳細オプション]の[分割トンネリングを拒否する]をチェックしても IPsec VPN 通信以外の平文通信が拒否されていなかった、という問題を修正しました。

(3) VPN 接続でリモート ゲートウェイが NAT ルータの内側にいるときは、リモート ID として NAT の内側のアドレスを指定しないと通常 VPN 接続は失敗します。（リモート ID 不整合のため）しかしながら、このとき[診断]機能はリモート ID を指定しなくても正常に接続可能と誤診断する、という問題を修正しました。

ver.2.4.2.0 での変更点（2011/07/15）

(1) 仮想ネットワークアダプタ(接続のデフォルト名[NET-G IPsec VPN 接続]、デバイス名

[dit IPsec Virtual Adapter]）の[プロパティ]->[構成]->[詳細設定]で、仮想ネットワークアダプタのパラメータ[MTU]および[Network Address]を変更する機能を追加しました。ただし、これらのパラメータの変更を有効にするためには Windows の再起動が必要です。

(2) Windows XP において、UQ-WiMAX 経由で仮想アドレスを使用しない IPsec VPN 接続を行うと、接続は成功するが通信が疎通しない、という問題を修正しました。

(3) ポリシーエディタの[診断]機能において、XAUTH を使用するが仮想アドレスを使用しない設定の診断を実行すると、Phase-2 Quick Mode におけるローカルアドレスが正しく設定されず、Quick Mode が正常終了しない、という問題を修正しました。

(4) Windows Vista/7 において、IPv4 Checksum offload または、TCP/UDP Checksum offload 機能が有効なネットワークアダプタを使用しているとき、かつ仮想アドレスを使用しない設定の IPsec VPN 接続を行うと、接続は成功するが通信が疎通しない、という問題を修正しました。

(5) Windows Vista/7 において、PPTP 接続が行えなくなる、という問題を修正しました。

(6) Windows Vista/7 において、アンインストール（削除）のとき、[dit NET-G IPsec Filter] サービスドライバ(ditNETGf)の INF ファイルが正しく削除されない、という問題を修正しました。

(7) アンインストール（削除）のとき、NET-G Secure VPN Client 関連のレジストリが存在しないとエラーが発生し削除が完了しない、という問題を修正しました。

ver.2.4.1.2 での変更点（2011/03/24）

(1) E-Mobile などのダイアルアップ WAN 接続を経由して、リモート ネットワークが 0.0.0.0/0 の VPN 接続を行うと、Windows Vista/7 においては接続時に IKE Phase-1 の失敗が多発する、または接続が成功しても実際の通信が行えない、Windows XP では、一定時間後に接続が切断してしまう、といった問題を修正しました。

(2) UQ WiMAX を経由した IPsec VPN 接続に対応しました。

(3) FOMA HIGH-SPEED 対応（内蔵）PC でかつ Windows Vista/7 において、IPsec VPN 接続を切断するとブルースクリーンが発生することがある、という問題を修正しました

(4) IPv6 の IPsec VPN 接続がうまく行えない、または接続に成功しても通信が行えないことがある、という問題を修正しました。

(5) Windows Vista/7 で IKE 設定モード（CFGMODE）を使用する VPN 接続を使用したとき、IKE Phase-1 SA の更新(rekey)に失敗する、という問題を修正しました。この問題は ver.2.4.1.0 以降で発生していました。

(6) Windows 7 Service Pack 1 (SP1)と Windows 7 Service Pack 1 (SP1) 64bit Edition (x64 版) を動作環境に追加しました。

ver.2.4.1.1 での変更点（2010/12/09）

(1) Windows XP において、ダイアルアップ接続を使用して VPN 接続を行うと接続は確立するが通信を受信できない、という問題を修正しました。

(2) ポリシーエディタの[ネットワーク エディタ]ダイアログで[IP アドレス]入力フィールドの右側のアイコンを選択したときに表示される[IP アドレスを検索する]ダイアログでは、ドメイン名を入力して IP アドレスを参照することができますが、IPv4 アドレスを参照したいのに IPv6 アドレスが参照されるという場合もありました。そこで、[IP アドレスを検索する]ダイアログに[IPv4 アドレス]および[IPv6 アドレス]のチェックボックスを追加しました。

ver.2.4.1.0 での変更点（2010/11/17）

(1) ポリシーエディタの [ポリシーのプロパティ]ダイアログでポリシーの[読み込み専用]属性を設定すると、当該ポリシーを使用した VPN 接続に失敗する、という問題を修正しました。ただし、既存の読み込み専用のポリシーについては、一旦読み込み専用属性を解除して設定を適用したのちに、再度読み込み専用に設定して設定を適用する必要があります。

(2) 接続の診断機能で、対向から送られた”RFC 3947”の ID を正しく表示できていない、という問題を修正しました。

(3) NAT Traversal(NAT-T)を使用する接続の診断を実行すると、診断の終了時に IPsec SA を削除する delete notification が暗号化されずにポート 500 に送られる、という問題を修正しました。

(4) Windows 7 でワイヤレス LAN デバイス（ワイヤレス ネットワーク接続）をインターネット接続に使用しているとき、[Microsoft Virtual WiFi Miniport Adapter]デバイスが[ネットワーク接続]に存在していると NET-G Secure VPN Client が正しく動作しない、という問題を修正しました。

(5) Windows 7 のワイヤレス WAN デバイス（モバイル ブロードバンド接続）に対応しました。

ver.2.4.0.2 での変更点（2010/03/01 リリース）

(1) Windows 7 に対応しました。

(2) 64bit Edition に対応しました。（Windows XP を除く）

(3) RFC3947 NAT Traversal の実装上の問題により、YAMAHA 以外のルータと接続できないことがある、という問題を修正しました。なお、YAMAHA ルータとの接続性を確保するために、従来の動作を行う[YAMAHA]オプションを追加しました。

(4) XAUTH 認証でユーザ名とパスワードを接続時に入力する設定のとき、これらを入力

した直後に ipmui.exe が異常終了することがある、という問題を解決しました。

(5) IKE ログ ウィンドウが開いている状態で、メインメニューから[IKE ログ ウィンドウを表示]を選択しても何も起こらなかったのを修正しました。

(6) IKE ログ ウィンドウを開いている状態でポリシーマネージャを停止したとき、IKE ログ ウィンドウは自動的に終了するようになりました。

(7) IKE ログの[ファイルに保存]オプションをオンにしたときに採集されるログファイルに時間が記録されない、という問題を修正しました。

(8) Windows Vista に新規インストールしたとき、通知領域（タスクトレイ）アイコンが通知メッセージを表示するようになりました。

(9) VPN 接続の IKE Phase 2 終了時に通知領域（タスクトレイ）アイコンがアニメーションしないという問題を修正しました。

(10) Windows Vista で、管理者がログオン中で通知領域（タスクトレイ）アイコンが表示されているとき、ユーザーを一般ユーザーに切り替えると(Fast User Switch)、通知領域アイコンが表示されない、という問題を修正しました。ただし、通知領域アイコンが操作可能な状態で表示されるのは、管理者ユーザー一人、一般ユーザー一人に対してのみです。

(11) Windows Vista において、評価版の使用期限が切れた後にライセンス キーを入力したとき、システムを再起動するまではメインメニューの[VPN を選択]と[ポリシーの選択]が使用できない、という問題を修正しました。

(12) Windows Vista において、ポリシー マネージャ サービス(SSHIPM)が起動に失敗することがあるという問題を改善しました。

(13) ポリシー マネージャ サービス(SSHIPM)は[Windows ログ]の[アプリケーション]イベントログを記録しますが、このログがイベントビューアで正しく表示されていなかったのを修正しました。

(14) Windows XP で、ある管理者ユーザーが通知領域アイコンを表示している状態で、他の管理者ユーザーがプログラムメニューから[YMS-VPN1-CP Agent]を選択するとランタイムエラーが発生する、という問題を修正しました。

(15) Windows XP で、一般ユーザーが VPN 接続を実行したとき、XAUTH 認証情報入力ダイアログが管理者ユーザーの画面に表示されてしまう、という問題を解消しました。

(16) ポリシー エディタで VPN 接続の診断を行ったときの結果のメッセージ表示を改善しました。

(17) Windows Vista で、ポリシー エディタからポリシーの[名前をつけて保存]を実行するとエラーになる、という問題を解消しました。

(18) ポリシー エディタで既知共有鍵のプロパティを開いたとき、[ID]タブで[プライマリ ID]を[ID なし]にしたとき、画面にゴミが表示される、という問題を解消しました。

(19) ポリシー エディタで VPN 接続の[拡張認証]のプロパティの[認証方法の種類を使用す

る]オプションをデフォルトでオンに設定しました。このデフォルトの変更は、既存のポリシーには影響を与えません。

(20) 監査ログを表示するときの日付を英語形式(DDMMYYYY)から日本語形式(YYYY/MM/DD)に変更しました。

(21) ライセンス キー入力ダイアログの[会社名]フィールドの名称を[組織名]に変更しました。

(22) アップグレード インストール等でライセンス キー入力ダイアログの[ユーザ]フィールドに文字列がすでに表示されているにも関わらず、[ユーザ]フィールドに何かを入力するまでは[OK]ボタンが選択可能にならない、という問題を修正しました。

(23) 既存の NET-G をアップグレードするとき、ライセンス キー入力ダイアログの[ユーザ]および[組織名]フィールドに設定済みの値が表示されない、という問題を修正しました。

(24) インストーラは Windows XP の SP2 より前のバージョンや Windows Server へのインストールを拒否するようになりました。

(25) インストーラは、NET-G の仮想ネットワーク接続に、「NET-G VPN 接続」という名前を与えるようになりました。

(26) インストーラは、互換性の無い他社製品 YMS-VPN1-CP を検出したとき、その製品のアンインストール（削除）を求めるようになりました。

(27) インストーラは、NET-G のバージョン 2.3.0 より古い製品を検出したとき、その製品のアンインストール（削除）を求めるようになりました。

(28) インストール中にコマンド プロンプトの画面やタスク アイコンが長い時間表示されていたところを「しばらくお待ちください」というダイアログを表示するように変更しました。

(29) 外部プログラムによって実現されていた「重要な注意」ダイアログをインストール ウィザードの画面に組み込みました。

(30) [コントロールパネル]の[プログラムと機能]で、[NET-G Secure VPN Client]を選択したときに、[変更]オプションは表示されなくなりました。

(31) すでにインストール済みのバージョンの setup.exe を起動したときに表示される「保守」画面のデフォルトを「変更」から「修復」に変更しました。さらに「変更」が選択されているときは「次へ」ボタンを選択できないように修正しました。

(32) 「アップグレード」および「修復」インストールで、シリアルキーの再検証を行い、既存のシリアルキーが正常でないときは「ユーザ情報」画面を表示するようになりました。

(33) アンインストール（削除）後、インストールフォルダに conf および shares フォルダが残る、という問題を修正しました。

(34) マニュアルの記述を変更しました。

(35) ヘルプの記述を変更しました。

ver.2.3.0.7 での変更点（2008/11/11 リリース）

(1) Windows Vista において、VPN 接続先ネットワークが 0.0.0.0/0 のとき、VPN 接続先の一部に到達できないことがある、という問題を修正しました。

(2) Windows Vista において、VPN 接続を使用している間に、通信に使用しているネットワークインタフェースの DHCP アドレスのリース更新に失敗することがある、という問題を修正しました。

(3) Windows Vista において、評価版としてインストールしたとき、[バージョン情報]ダイアログに残り試用期間の表示が正しく行われないことがある、という問題を修正しました。

(4) IKE の脆弱性に関する問題を一部改善しました。

(5) ポリシーマネージャ サービス(SSHIPM)のログメッセージをローカルシステムのアプリケーション ログに記録するようにしました。イベントビューアを使用してログを参照することができます。

ver.2.3.0.6 での変更点（2008/04/03 リリース）

(1) Windows Vista でシステムに最初に認識されるネットワークインタフェース（通常は内蔵 Ethernet）が無効であるか、システムの電力管理などの機能によって自動的に無効状態となったときに VPN 接続を行うと、「次の場所への VPN 接続を開いています...」メッセージを表示した状態でブルースクリーンとなったり、ポリシーマネージャが動作を停止したりすることがある、という問題を修正しました。

(2) ネットワークアダプタを無効にしたときの処理が完了しないことがあり、これによって Windows Vista においてはカーネル資源が無駄に増加したり、Windows XP においてはシステムが再起動したりしてしまうことがある、という問題を修正しました。

(3) インストーラが共有 DLL として誤ったファイルをレジストリに追加する、という問題を修正しました。

ver.2.3.0.5 での変更点（2008/01/27 リリース）

(1) インストール時に[暗号化速度の診断]ダイアログが表示されたままとなりインストールが継続できなくなることがある、という問題を修正しました。

(2) マニュアルおよびヘルプに記載されたシステム要件がリリースノートの記述と合致しない、という問題を修正しました。

ver.2.3.0.4 での変更点（2007/11/14 リリース）

(1) 偽造された RSA PKCS-1 署名の認証に関する実装上の問題に対処しました。

ver.2.3.0.3 での変更点（2007/08/01 リリース）

(1) Windows Vista に対応しました。ドライバおよび実行ファイルの一部は Windows Vista 専用となりました。インストーラは Windows の種類に応じて適切なファイルをインストールします。

(2) Windows Me、Windows 98SE、Windows NT 4.0 はもはやサポートされません。これらの環境に本ソフトウェアをインストールすることはできません。NET-G Secure VPN Client ver. 2.2 シリーズをご使用ください。

(3) Windows XP Service Pack 2 より古い Windows XP はもはやサポートされません。これらの環境における動作は検証されていません。NET-G Secure VPN Client ver. 2.2 シリーズをご使用ください。

(4) Windows Server 2003 Service Pack 1 より古い Windows Server 2003 はもはやサポートされません。これらの環境における動作は検証されていません。NET-G Secure VPN Client ver. 2.2 シリーズをご使用ください。

(5) IPsec 用仮想ネットワークインタフェース(dit IPsec Virtual Adapter)は[ネットワーク接続]ダイアログに表示されるようになりました。

(6) 本ソフトウェアにおいて「IPSEC」や「IPSec」などの記述を「IPsec」に統一しました。

(7) ポリシーエディタの[VPN 接続を追加]、[セキュアな接続を追加]、[セキュアなネットワークを追加]ダイアログにおいて、新しい鍵を作成するためのボタンを追加しました。[認証鍵]ドロップダウンメニューの右側の[...]ボタンをクリックすると、[新しい認証鍵]ダイアログが開きます。

(8) [NET-G Secure VPN Client 統計]ダイアログの[セキュリティの関連付け]タブページにおいて、[セキュリティの関連付け詳細]フィールドの表示に、従来の SA の寿命バイト数に加えて SA の寿命時間が表示されるようになりました。また、同ダイアログの[IPsec 統計]タブページにおいて、[AH]フィールドを廃止し、新たに、[IPv4]、[IPv6]フィールドを追加しました。

(9) 評価版のインストール後にライセンスキーを入力することにより、評価版を製品版にアップグレードすることが可能となりました。ライセンスキーを入力するためには、メインメニューの[バージョン情報]を選択してください。

(10) [IKE Log]ウィンドウに表示される情報、およびログファイルに保存される情報に、イベントが発生した時間を示すフィールドを追加しました。

(11) ポリシーマネージャの[規則のプロパティ]ダイアログの[説明]フィールドに長い日本語文字列を入力すると、表示が"..."のみになってしまう、という問題を解決しました。

ver.2.2.2.01 での変更点（2007/6/20 リリース）

(1) ver.2.2.2 で、セキュリティ ポリシー ファイル(.spl)ファイルをダブルクリックして開

くとエラーとなる、という問題を解決しました。

(2) ver.2.2.2 で、ポリシーのインポートを行うとポリシーマネージャが異常終了する、という問題を解決しました。

(3) ver.2.2.2 で、Dead Peer Detection(DPD)を使用しない対抗機器に対して DPD メッセージを送信することがあり、対抗機器からの応答によっては IPsec VPN 接続を切断するときの Delete SA メッセージを送信しないことがある、という問題を解決しました。

(4) ver.2.1.4.00、ver.2.1.4.01、および ver.2.2.2 のインストーラを使用して、以前のバージョンの上書きアップデートを実行するとドライバの更新が正しく行われない、という問題を解決しました。

(5) ポリシーマネージャの IPsec 後フィルタの[詳細]タブで、[監査]オプションをオンにするとポリシーマネージャが異常終了するため IPsec 通信が行えない、という問題を解決しました。

(6) 監査ログの表示で、IPv4/IPv6 アドレスが正しく表示されない場合がある、という問題を解決しました。

(7) いくつかのメモリリークを解決しました。

(8) IPv6 Router Solicitation メッセージが正常に送信されない、という問題を解決しました。

ver.2.2.2 での変更点（2006/11/08 リリース）

(1) RFC3947 NAT Traversal に対応しました。

(2) RFC3706 Dead Peer Detection に対応しました。これに伴い、[ポリシーエディタ]の[規則のプロパティ]の[詳細]タブに[DPD(Dead Peer Detection) を使用する]オプションを追加しました。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。このオプションは VPN 接続においてのみ有効です。

(3) [ポリシーエディタ]の[規則のプロパティ]の[詳細]タブの[NAT Traversal]オプションにサブオプション[常に使用する]を追加しました。このサブオプションを使用すると、NAT 装置を経由していないと判断できるときにも、NAT 装置を経由しているときと同様にカプセル化を適用するため、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。

(4) [ポリシーエディタ]の[規則のプロパティ]の[詳細]タブの[起動時に開く]オプションの

サブオプションとして、[切断時に再接続する]オプションを追加しました。このオプションを使用すると、VPN 接続に何らかの問題が発生して接続を切断したとき、自動的に再接続を行います。

(5) CISCO VPN Client 用に設定された CISCO 社 VPN サーバ機器に VPN 接続が可能となりました。これに伴い、[ポリシーエディタ]の[既知共有鍵]の[ID]タブで指定できる ID に、[ベンダ固有(CISCO Group ID)]を追加しました。

(6) [ポリシーエディタ]の[規則のプロパティ]の[詳細]タブの[ポートに適用する UDP カプセル化]オプションを[UDP カプセル化]オプションに名称変更しました。

(7) [ポリシーエディタ]の[接続のプロパティ]の[詳細]タブの[NAT-T (Network Address Translation Traversal)]オプションを[NAT Traversal]オプションに名称変更しました。

(8) XAUTH を使用して YAMAHA 社製ルータに接続可能になりました。

(9) IKE 設定モード（CFGMODE）を使用する VPN 接続において、接続時に仮想ネットワークインタフェースへの IP アドレス割り当てに失敗することがある、という現象を改善しました。

(10) IKE 設定モード（CFGMODE）を使用する VPN 接続において、接続時に仮想ネットワークインタフェースへの IP アドレス割り当てに失敗した場合に VPN 接続が切断されない、という問題を修正しました。

(11) Intel 2915ABG Wireless LAN Adapter を使用している PC で、ネットワーク通信が阻害されることがある、という問題を修正しました。

(12) IPv6 リンクローカルアドレスを送信元とする Neighbor Solicitation を受信したとき、応答の Neighbor Advertise の送信に失敗する、という問題を修正しました。

(13) 拡張認証の確認ダイアログを最前面に表示するように修正しました。

(14) 不要な DNS サーバへの問い合わせを低減しました。

(15) VPN 接続の[規則のプロパティ]で、[リモートネットワーク]に 0.0.0.0/0.0.0.0 を指定した時の問題点を修正しました。

(16) レジストリのキー名として正しくない文字列を使用することがあった、という問題を修正しました。

ver.2.1.4.01 での変更点（2006/5/22 リリース）

(1) Windows Server 2003 Service Pack 1 において、IPv6 VPN 接続が正常に行えないという問題を修正しました。

(2) インストーラは、アンインストール時に INF ファイルを削除するようになりました。

(3) IKE 設定モード（CFGMODE）を使用する VPN 接続において、セキュリティの有効期間が経過したときの更新（IKE Rekeying）に失敗した等の理由で接続が切断された後にリモートネットワークに対する通信が発生したときに、誤ったローカルアドレスに基づく SA が生成されることがある、という問題を修正しました。

(4) ポリシーエディタ(sshcpa.exe)をコマンドラインから起動して、複数のポリシーエディタが起動してしまったときに、ポリシーエディタがハングアップすることがある、という問題を修正しました。

(5) VPN 接続において、セキュリティの有効期間が経過したときの更新（IKE Rekeying）に失敗したときに VPN 接続が切断されないことがある、という問題を修正しました。

(6) 鍵の名前として特定の日本語文字を使用すると、鍵は作成できるものの使用と削除ができない、という問題を修正しました。また、鍵の名前として半角記号の‘/’と‘¥’が使用できない、という制限を解消しました。

(7) ポリシーエディタの[ネットワークエディタ]において、不正な IP アドレスとサブネットマスクが入力された場合のチェックを強化しました。IP アドレスにサブネットマスクを適用したときに、ノードアドレス（サブネットマスクでマスクされないビット）が 0 でない場合は不正なアドレスとなります。

(8) ポリシーエディタの[ネットワークエディタ]において、[IP アドレスを検索する]ボタンを使用したときの結果が、IP アドレスおよびサブネットマスクに正しく反映されない、という問題を修正しました。

(9) ポリシーエディタの[仮想 IP アドレス]ウィンドウにおいて、DNS サーバおよび WINS サーバのうち、片方のみを設定することを許可するようになりました。

(10) ポリシーエディタ等の GUI ユーティリティをプライマリモニター以外のモニター画面に移動して操作を行ったときに、ウィンドウやダイアログが正しく表示されないことがある、という問題を修正しました。

(11) WINS サーバを指定した VPN 接続を行うと、従来は Node Type に Peer-Peer を指定していましたが、本バージョン以降はノードタイプの指定を行わないようになりました。この変更によって、Windows XP において VPN 接続を行った後に、ローカルネットワーク上での名前による参照が行われなくなるという問題が修正されました。ただし、以前のバージョンで一度でも WINS サーバを指定した VPN 接続を行ったことがある場合は、本書の「0 注意事項」の**エラー! 参照元が見つかりません。**を参照してレジストリを修正してください。

(12) イベントビューアにおいて、dit IP Security (IPSEC)サービスのメッセージ(ソース sshipsec)のメッセージが正しく表示されない、という問題を修正しました。ただし、この修正は既存の NET-G Secure VPN Client を削除し、本バージョンを新規にインストールした場合にのみ反映されます。（アップデートインストールの場合は反映されません。）

(13) [NET-G Secure VPN Client 統計]ウィンドウの[セキュリティの関連付け]で、接続中の VPN 接続の関連付け（SA）を終了すると、メインメニューの[VPN を選択]サブメニューにある当該 VPN 接続のチェックマークが外れて接続を切断できなくなる、という問題を修正しました。

(14) IPv6 プロトコルスタックがインストールされた Windows XP および Windows 2003 Server で使用すると、[NET-G Secure VPN Client 統計]ウィンドウの[IPSec 統計]の[トリガ済み]の値が何もしていないのに増加していく、という問題を修正しました。
(15) ポリシーエディタの[VPN 接続を追加]ウィンドウ、[セキュアな接続を追加]ウィンドウ、および[規則のプロパティ]ウィンドウで、[ゲートウェイ名]または[ホスト名]フィールドに 256 バイト以上の文字列を入力したときの問題を修正しました。
(16) ポリシーエディタの[VPN 接続を追加]ウィンドウ、[セキュアな接続を追加]ウィンドウ、および[規則のプロパティ]ウィンドウで、[ゲートウェイ名]または[ホスト名]フィールドにホスト名を入力したとき、名前による参照解決に失敗したというメッセージが常に表示される、という問題を修正しました。
(17) ポリシーエディタの[ネットワークエディタ]ウィンドウで不正な IP アドレスを入力したときに表示されるダイアログがモーダルでない、という問題を修正しました。

ver.2.1.4.00 での変更点（2006/4/5 リリース）

(1) Windows Server 2003 Service Pack 1 に対応しました。
(2) 接続の診断において nat-traversal 機能の一部が正常に動作していなかった問題を修正しました。
(3) 一部の PHS カード等を使用したとき、二回目以降の VPN 接続ができないことがあるという問題を修正しました。
(4) セキュアなネットワークおよびVPN接続の新規作成のダイアログのアイコンを変更しました。
(5) administrator 権限の無いユーザーのとき、バージョン情報にユーザ名などを表示しないようになりました。
(6) ユーザーのログオン時に起動するタスクトレイアプリケーションが比較的多いとき、NET-G Secure VPN Client のアイコンが表示されないことがある、という問題を修正しました。
(7) IPv6 を使用する VPN 接続の接続、切断時にタスクバーにプロセスの表示が一瞬現れるという問題を修正しました。
(8) IPv6 VPN 接続のアドレスやルーティング設定は常駐設定ではなく、再起動後に無効となるように設定されるようになりました。
(9) IKE パケットの不正に対するチェックが強化されました。
(10) ポリシーエディタおよびポリシーマネージャのメモリリークを修正しました。
(11) ポリシーファイルのインポートで、ファイル名にアンダースコア('_')が含まれる場合、警告を表示し、インポートできないように修正しました。
(12) ポリシーファイルのインポートで、IPv6 アドレスに含まれる文字がポリシー定義の先頭にあるとき、インポートできない問題を修正しました。

(13) VPN 接続が[起動時に開く]オプションを使用しているとき、通信が途絶して VPN 接続が切断された後にメインメニューから[再接続]コマンドを実行しても再接続を行わない、という問題を修正しました。また、[再接続]コマンド実行時の遅延を削減しました。

ver.2.1.3(01)での変更点（2005/4/12 リリース）

(14) ポリシーエディタで VPN 接続の仮想 IP アドレスを手動で設定したとき、入力した IP アドレスの値に対するチェックを強化しました。

(15) ポリシーエディタで VPN 接続の仮想 IP アドレスを手動で設定したとき、入力した IP アドレスが当該ネットワークにおける最大のノード番号（例えば 192.168.0.254/24）に設定したとき、接続に失敗する、という問題を修正しました。

(16) VPN 接続中にキャンセルしたとき、または起動時に開く VPN 接続を使用中に通信回線を切断して再接続したとき、仮想ネットワークインタフェースにアドレスが割り当てられたままとなり、ポリシーマネージャを停止、起動しないと以後の VPN 接続ができなくなる、という症状を改善しました。また、この症状が発生するときに同時に発生していたメモリリークを修正しました。

(17) [VPN を選択]サブメニューの[再起動]コマンドを選択したときに、接続を切断してから再接続するまでに５秒の遅延を追加しました。

(18) ポリシーエディタの[フィルタ規則のプロパティ]で、ポート番号 4500 のサービス名称[nat-t]を追加しました。

(19) IPv6 をインストールしていない環境で、IKE ログウィンドウに表示されていた不要なメッセージを削除しました。

(20) インストール時の[暗号化速度の診断]ダイアログに表示される文字列を修正しました。

(21) 監査ログの表示に使用する HTML ファイルの charset 設定が不正であるのを修正しました。

(22) オンラインヘルプの文章に含まれていた製品のバージョン番号を削除しました。

ver.2.1.3(00)での変更点（2005/3/18 リリース）

(1) ポリシーエディタでローカルポリシーの追加を行ったときに、新しいポリシーの IPsec 前フィルタ規則がデフォルトのポリシーの設定と異なっている、という問題を修正しました。

(2) ポリシーエディタで VPN 接続時の WINS サーバを指定しても、設定が反映されずに仮想 IP アドレスの値が誤って設定されてしまう、という問題を修正しました。

(3) ポリシーエディタの接続の診断機能で表示される文字列を一部修正しました。

(4) Juniper 社の NetScreen Security Gateway の XAUTH 認証機能の CHAP（Radius-Chap）オプションに対応しました。

(5) VPN 接続の仮想 IP アドレス割り当てで IKECFG 設定モードを使用したとき、対向側

ゲートウェイから複数の DNS サーバまたは WINS サーバが指定された場合に各々２つまでの指定に対応するようになりました。（従来は各々１つ）

(6) ポリシーエディタの接続の診断機能で、Phase-2 エラーが発生したときには診断を直ちに打ち切るように修正しました。

ver.2.1.2(00)での変更点（2004/12/10 リリース）

(1) Ver 2.1.1(00)で IPv6 の IPsec VPN 接続が行えない、という問題を修正しました。

(2) アップデートインストールの場合、シリアル番号入力フィールドに既存のシリアル番号を表示するようにしました。

(3) インストール中に発生する警告ダイアログに関する記述をインストーラに追加しました。

(4) NET-G Secure VPN Client Agent (SSHTray.exe)を複数実行すると異常終了する問題を修正しました。

(5) Windows 2000/XP/Server2003 において、仮想ネットワークアダプタ(dit IPSec Virtual Adapter)が[ネットワーク接続]に表示されないように変更しました。これにより、Windows XP/Server2003 において VPN を接続または切断したときに表示されていたメッセージが消えました。また、Windows XP の Windows ファイアウォール機能など、ネットワークアダプタを参照する設定から仮想ネットワークアダプタが参照されなくなりました。ただし、この修正は既存の NET-G Secure VPN Client を削除し、本バージョンを新規にインストールした場合にのみ反映されます。（アップデートインストールの場合は反映されません。）

(6) メインメニューの[オンラインサポート] -> [サポート要求]で表示されるウェブページへのリンクを修正しました。

(7) インストーラはシリアル番号を入力したときに英小文字を大文字に変換するようになりました。

ver.2.1.1(00)での変更点（2004/11/10 リリース）

(1) 既知共有鍵の作成ダイアログの説明文に不要な記号が入っていたのを修正しました。

(2) NET-G Secure VPN Client 同士の通信で UDP カプセル化を適用したとき、IP 圧縮を同時に使用しないと接続できないという問題を解決しました。

(3) ネットワークエディタで、IP アドレスまたはサブネットマスクに IP アドレスでない文字列を入力してポリシーを適用すると、ポリシーの更新が終了せず、再起動後もポリシーエディタが起動できなくなる、という問題を解決しました。

ver.2.1.0(00)での変更点（2004/8/31 リリース）

(1) 集中管理ポリシーが動作しない問題を解決しました。

(2) デフォルト応答規則の IPsec 応答が動作しない問題を解決しました。
(3) 他の NET-G Secure VPN Client で共有されているポリシーのインポートができない問題を解決しました。
(4) L2TP over IPsec による仮想 IP アドレス割り当てに対応しました。
(5) IP 圧縮の動作確認をしました。
(6) Windows XP 以外の Windows で、ポリシーエディタのセキュアなネットワークの[規則のプロパティ]画面->[全般]タブでネットワークが表示されない問題を解決しました。
(7) セキュアな接続およびセキュアなネットワークに設定されたホストとの IPv6 IPsec の監査ログが保存されない問題を解決しました。
(8) IPv6 VPN 接続（仮想 IP アドレス割り当てなし）を[分割トンネリングを拒否する]設定しても、VPN 接続中にリモートネットワーク以外のホストと通信できる問題を解決しました。

ver.2.0.0(00)での変更点（2004/7/29 リリース）

(1) Windows 98 SE/Me/NT 4.0/2000/Server 2003 に対応しました。
(2) IPv6 の IPsec 後トラフィックフィルタが動作しない問題を解決しました。
(3) IPv6 の IPsec 前トラフィックフィルタのフィルタアクションに拒否を指定した場合、該当するパケットの送信元に終点到達不能メッセージ (ICMPv6 type:1 code:4)を通知しない問題を解決しました。
(4) ポリシーマネージャでポリシー名にアンダースコア('_')を含む文字列を指定できないようチェックを行う機能を追加しました。アンダースコアは内部で特殊文字として扱うため、ポリシー名にアンダースコアを含む文字列が指定されると以下の問題が発生していました。
- アンダースコアがスラッシュ('/')に変更された状態で表示される。
- ポリシーを変更後、適用を行うとポリシーマネージャがストールする。

(5) タスクトレイから[ポリシーマネージャを停止]を選択すると、ポリシーマネージャは終了するもののすぐに起動する問題を解決しました。
(6) 監査ログに IPv6 アドレスが正しく表示されない問題を解決しました。
(7) マニュアル、および、ヘルプを改訂しました。

ver.1.2.0(00)での変更点（2004/5/10 リリース）

(1) 本製品の製品名を

NET-G/Secure VPN Client

から

NET-G Secure VPN Client

に変更しました。

(2) IPv6 パス MTU ディスカバリに関する問題を修正しました。

(3) プライマリ DNS サフィックスを指定した環境では、ローカル IP アドレスの取得に時間がかかるため以下の現象が発生する問題を修正しました。

- Windows XP 起動直後や Windows XP の IP アドレス変更時に、数十秒間、通信が行えない状態になる。
- Windows XP 起動直後や Windows XP の IP アドレス変更時に、数十秒間、IKE ログウィンドウやポリシーエディタが操作できない状態になる。

(4) IPv6 のトラフィックフィルタ機能を追加しました。

(5) Windows XP Service Pack 2(RC1)に対応しました。

(6) ISAKMP Configuration Method 使用時、セキュリティゲートウェイからサブネットマスク all 1 の仮想 IP アドレスが渡された場合、以下のサブネットマスクを設定するように変更しました。

- IPv4 の場合、255.255.255.0
- IPv6 の場合、ffff:ffff:ffff:ffff::

(7) ISAKMP Configuration Method 使用時、リモートネットワークのサブネットマスクに all 0 が指定されている場合、セキュリティゲートウェイから渡されたリモートネットワークアドレスを設定するように変更しました。

(8) ネットワークカードの MTU 値をレジストリから設定できるように変更しました。

[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥sshipsec¥Parameters]

に以下の項目を追加することで MTU 値を設定可能です。

名前： MTU
種類： REG_DWORD
データ： 1280～65535

(9) ポリシーマネージャの VPN 接続→[規則のプロパティ]ダイアログ→[全般]タブ→[仮想 IP アドレス]ダイアログで仮想 IP アドレス割り当てプロトコルから[IPSec 経由の DHCP (Dynamic Host Configuration Protocol)]および[L2TP (Layer Two Tunneling Protocol)]を削除しました（未対応のため）。

(10) 各ウインドウに表示される本製品名を「SSH Sentinel」から「NET-G Secure VPN Client」に変更しました。

(11) インストーラのデフォルトのインストール先を

[C:¥Program Files¥SSH Communications Security¥SSH Sentinel]

から

[C:¥Program Files¥dit¥NET-G Secure VPN Client]

に変更しました。

(12) IPsec ドライバのサービス名を

SSH IP Security (IPSEC)

から

dit IP Security (IPSEC)

に変更しました。

(13) VPN 接続で仮想 IP アドレスを設定する場合に使用する仮想ネットワークカード名を

SSH IPSEC Virtual Adapter

から

dit IPSEC Virtual Adapter

に変更しました。

(14) 本プログラムが使用するレジストリを

[HKEY_LOCAL_MACHINE¥SOFTWARE¥
SSH Communications Security¥SSH Sentinel]

から

[HKEY_LOCAL_MACHINE¥SOFTWARE¥
dit¥ NET-G Secure VPN Client]

に変更しました。

(15) マニュアル、および、ヘルプを改訂しました。

ver.1.1.0(00)での変更点（2004/4/9 リリース）

(1) NetScreen ScreenOS 5.0.0r4.0 対向で、XAUTH に対応しました。

(2) セキュアな接続の接続先ホストに IPv6 アドレスを指定すると、ポリシーマネージャが起動できない問題を解決しました。この問題は以下のバージョンで発生していました。

ver.1.0.0(00)
2004/3/8 リリースバージョン

(3) NIC の有効／無効切り替えツールを削除しました（Windows XP 起動直後に RA による IPv6 アドレスが取得できない問題および無線 LAN インタフェース使用時、Windows XP 起動時に DHCP による IPv4 アドレスの取得ができない問題を解決したため)。

ver.1.0.0(00)での変更点（2004/3/31 リリース）

(1) 本バージョンからバージョン番号を設定しました。本バージョンを ver.1.0.0(00)とします。

(2) NAT Traversal の以下のドラフトに対応しました。

- draft-ietf-ipsec-nat-t-ike-00.txt
- draft-ietf-ipsec-nat-t-ike-01.txt
- draft-ietf-ipsec-nat-t-ike-02.txt

- draft-ietf-ipsec-nat-t-ike-03.txt

(3) Windows XP 起動直後に RA による IPv6 アドレスが取得できない問題を解決しました。

(4) 無線 LAN インタフェース使用時、Windows XP 起動時に DHCP による IPv4 アドレスの取得ができない問題を解決しました。

(5) 仮想 IP アドレス割り当てて VPN 接続する際、VPN 切断後、すぐに再接続を行うと SA 確立するが IPsec 通信が行えない場合がある問題を解決しました。

(6) 仮想 IPv6 アドレス割り当てて VPN 接続中、[分割トンネリングを拒否する] をオフに設定しても、NET-G Secure VPN Client と同一サブネットのホストと通信できない場合がある問題を解決しました。

(7) インストール中、自己証明書作成を開始後はインストールのキャンセルができない問題を解決しました。

(8) ポリシーエディタで名前を付けてポリシーの保存をする際、仮想 IP アドレスが保存できない問題を解決しました。

(9) Windows 2000/XP/2003Server 用の IPsec ドライバ（sshipsec.sys）の実装方式を Filter-hooked Driver から Intermediate Driver に変更しました。