NET-G Secure VPN Client
設定・トラブルシューティング FAQ

第 3 版

株式会社 ディアイティ

2018/08/1

目次

1. 一般、導入に関するお問い合わせ

[Q1-1] インストール時の注意点は？

A1. インストールの際、マルウェア対策ソフトが起動している場合は機能を停止してください。マルウェア対策ソフトの機能により、インストールが正常にできない場合があります。
NET-G Secure VPN Client をインストールする際には、マルウェア対策ソフト(ウィルス対策ソフト)を停止してインストールしてください。

A2. Windows 2000 Server、Windows Server 2003 上でのご利用について
NET-G Secure VPN Client 2.4 では Windows Server 上での動作をサポートしておりません。Server 2008 についても同様です。
Server 2003 でご利用いただく場合、お手数ですが旧バージョン 2.3 をご利用ください。

※ NET-G Secure VPN Client 2.3 についてダウンロード提供などはおこなっておりません。シリアルナンバーも異なりますので、一度弊社までお問い合わせください。

[Q1-2] SafeNet Sentinel からの変更点は？

A. 以下の機能内容が変更されました。

- IPv6 に対応しました。
- Windows XP SP2 に対応しました。
- 一部の無線 LAN カードとの同時利用時の問題を修正しました。
- 他社製 VPN 機器との接続性を改善しました。
- ライセンスパック商品を追加しました。（10、50、100）
- スマートカード用ミドルウェア Accession が別売オプション（価格・提供時期未定）となりました

[Q1-3] 他の VPN クライアントソフトとの併用はできるか？

A. できません。利用されている端末へインストールする VPN クライアントソフトは、いずれか一つにしてください。

[Q1-4]　データ通信カードを利用しての VPN 接続について

A. NET-G Secure VPN Client はモバイルデータ通信カードでの利用制限を設けておりません。弊社環境では、下記のモバイルデータ通信カードでの接続を確認しております。

- イー・モバイル
  - D02HW
  - D41HW　（V2.4.1.2 以降でご利用いただけます。）

    「データプラン B 契約」で契約されている端末は VPN 接続をご利用することはできませんのでご注意ください。詳細に関しては下記イー・モバイル様ホームページをご確認ください。
    http://faq.emobile.jp/faq/view/102828
- UQ WiMAX
  - au KDDI:DATA01（V2.4.1.2 以降でご利用いただけます。）
- FOMA
  - VAIO　VPCY11AFJ（FOMA 内蔵型モデル）

※　ご利用されるバージョンのリリース内容もあわせてご確認ください。

※　条件によっては利用できない機能もあり、上記製品との接続性を保証するものではありません。お客様の環境での利用可否については評価版を利用してお客様の責任においてご確認ください。不明な点についてはお問い合わせください。

2. アップグレード、NET-G Secure VPN Client 設定について

[Q2-1] SafeNET Sentinel からのアップデート方法

A. SafeNet Sentinel から NET-G Secure VPN Client へアップグレードする場合は、一度 SafeNet Sentinel をアンインストールしてください。Sentinel のポリシーのバックアップを取り、それを NET-G Secure VPN Client にインポートすることができます。

※ Sentinel のポリシーのバックアップを取って、それをインポートしても仮想アドレスは 0.0.0.0 のままという不具合があります。ご注意ください。

[Q2-2] NET-G Secure VPN Client 2.4 へのバージョンアップ方法について

A. 現在インストールされているバージョンによって手順が異なります。

OS	旧バージョン	バージョンアップ方法
Windows XP	2.2.2.1 以前	旧バージョン削除後に新規インストール
	2.3.0.X	上書きインストール
Vista	2.3.0.X	上書きインストール

ただし、Windows の OS 自体を更新（例．Windows XP から Windows 7）した場合、NET-G Secure VPN Client は更新することができなくなります。Windows の更新を行う場合は、NET-G Secure VPN Client を削除後に Windows の更新を行い、その後新しいバージョンを新規でインストールしてください。

※ バージョンアップを行う前に、念のため設定バックアップをしていただくことをお勧めします。

[Q2-3] 設定のエクスポート・インポート

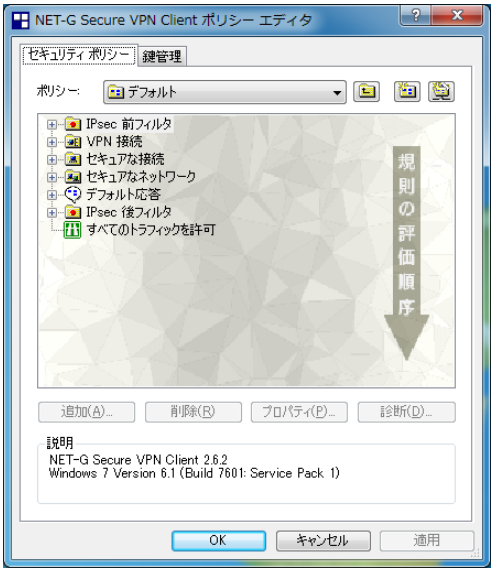
A. NET-G Secure VPN Client では設定をエクスポートし、ファイルとして保存することが可能です。保存したファイルは他の NET-G Secure VPN Client がインストールされた端末へインポートする事が出来ますので、複数の端末への展開にもご利用いただけます

NET-G Secure VPN Client 設定のエクスポート手順

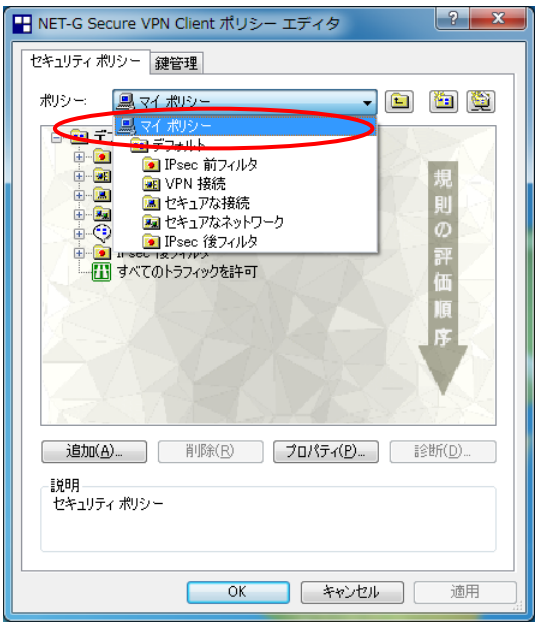
※　NET-G Secure VPN Client では設定のエクスポートは可能ですが、既知の共有鍵のエクスポートはセキュリティの観点から対応しておりません。詳しくは[Q2-4] 既知共有鍵のエクスポート・インポートをご確認ください。

1. Windows デスクトップ画面右下タスクトレイより、NET-G Secure VPN Client のアイコンを右クリックして下記のような画面を開き、“ポリシーエディタを実行（E)…”をクリックします。

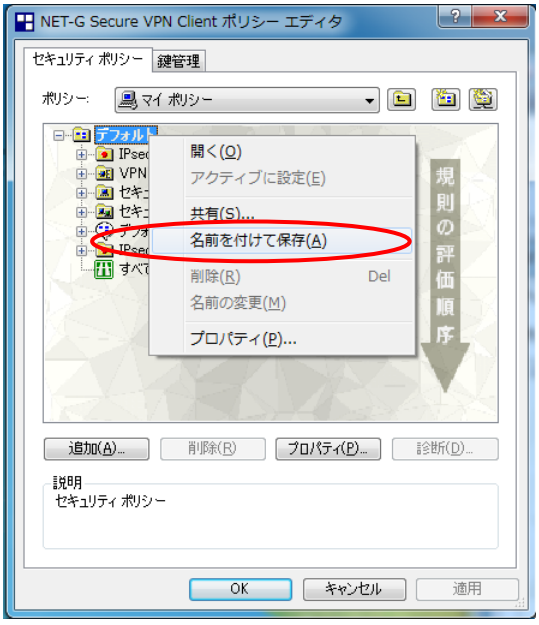
2. “ポリシーエディタを実行(E)…”をクリックすると下記のような画面が表示されます。



3. ポリシーエディタ画面の“ポリシー：デフォルト”を“ポリシー:マイ ポリシー”に変更します。“ポリシー：マイポリシー”に変更すると、画面中央の窓に作成したすべてのポリシーが表示されます。

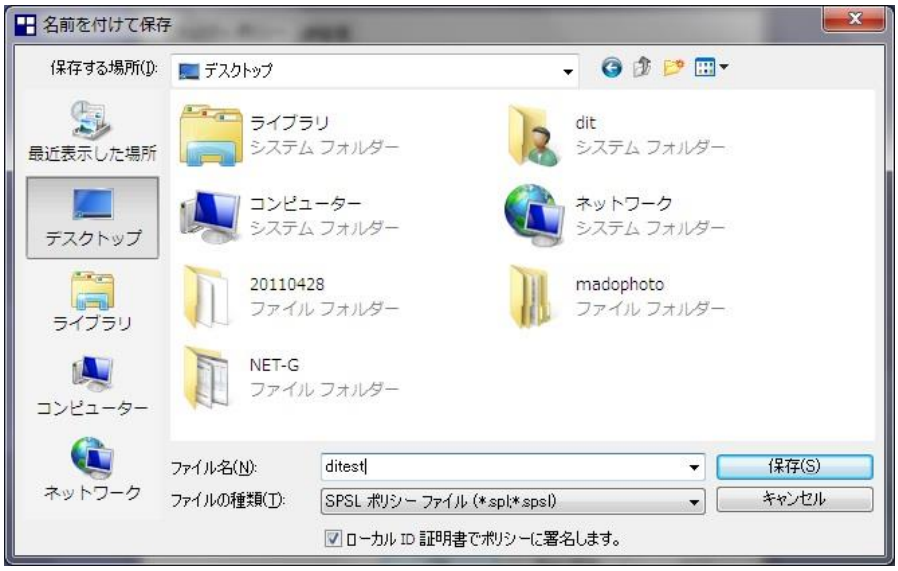


4. 該当のポリシーにカーソルを合わせて右クリックして、“名前を付けて保存(A)”を選択します。

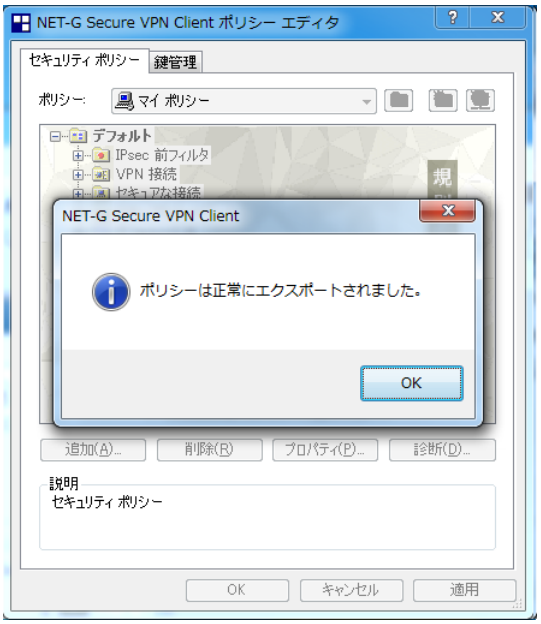


5. “名前を付けて保存(A)”を選択すると下記の保存画面が表示されますので、名前を付けて保存します。

※ 利用できない文字もあるのでご注意ください。



6. 下記のような画面が表示されたら完了です。



7. “名前を付けて保存(A)”で選択した保存先に、エクスポートされたファイル（.spl ファイル）が存在することを確認してください。

[Q2-4] 既知共有鍵のエクスポート・インポート

A. NET-G Secure VPN Client では設定ファイルをエクスポートする際に、既知共有鍵を同時にエクスポートすることができません。また、既知共有鍵だけをエクスポートすることもできません。しかしながら、既知共有鍵のインポートを行うことは可能になります。予め既知共有鍵ファイルを作成し、既知共有鍵ファイルをダブルクリックすることにより NET-G Secure VPN Client にインポートすることができます。ファイルフォーマットは下記の通りとなります。

```
-----BEGIN PSK-----
鍵の名前
鍵の値
Local の ID
Remote の ID
-----END PSK-----
```

設定例

項目	設定内容
鍵名	dittest
パスフレーズ	password
ローカルプライマリ ID (E-メール形式)	dit@dit.co.jp
リモートプライマリ ID	無し

上記のような内容の鍵ファイルを作成する場合、鍵ファイルは下記のように作成します。

```
-----BEGIN PSK-----
Dittest                         /* 既知共有鍵の名称
ditdit                          /* パスフレーズ
usr@fqdn(dit@dit.co.jp)         /* ローカルプライマルID（E-メール形式）
-----END PSK-----
```

※　リモートプライマリ ID がない場合、空白等を設定する必要はありません。

[Q2-5] ポリシー設定を行う際の注意点

A. 通常、IPsec 前フィルタおよび IPsec 後フィルタの設定は、変更しないでください。
VPN や他アプリケーションの接続が正常にできなくなる場合があります。

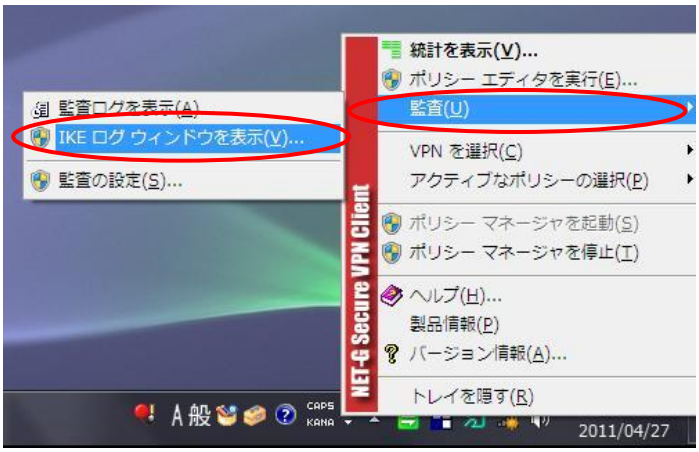
3. トラブルシューティング

[Q3-1] NET-G Secure VPN Client ログ出力について

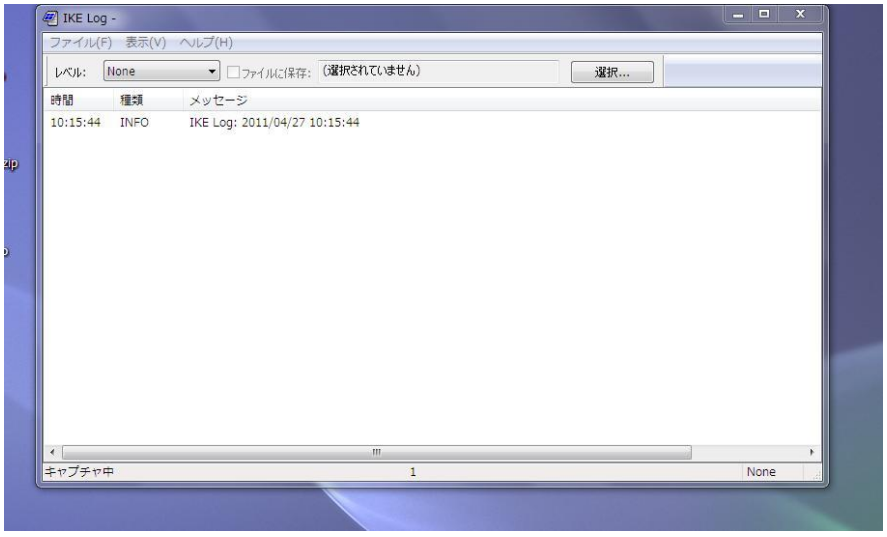
A. NET-G Secure VPN Client では、下記の方法で VPN 接続時のログを出力することが可能です。接続障害時の切り分け等にご利用ください。

NET-G Secure VPN Client ログ取得手順

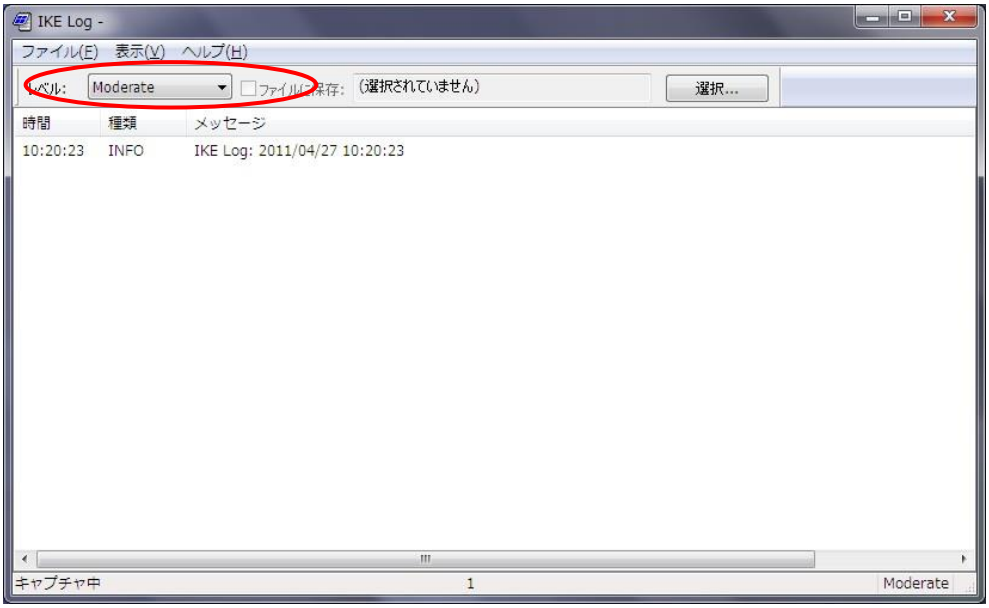
1. Windows デスクトップ画面右下タスクトレイより、NET-G Secure VPN Client のアイコンを右クリックして下記のような画面を開きます。
   “監査(U) ” →“IKE ログウインドウを表示(V)…”をクリックします。



2. “IKE ログウインドウを表示(V) … ”をクリックすると、下記画面が表示されます。

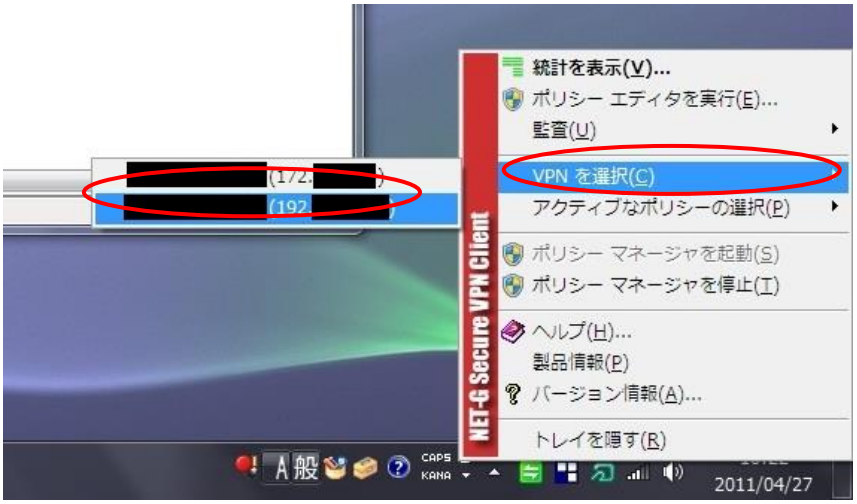


3. IKE Log -画面から画面左上“レベル：”を“None”から“Moderate”に変更します。

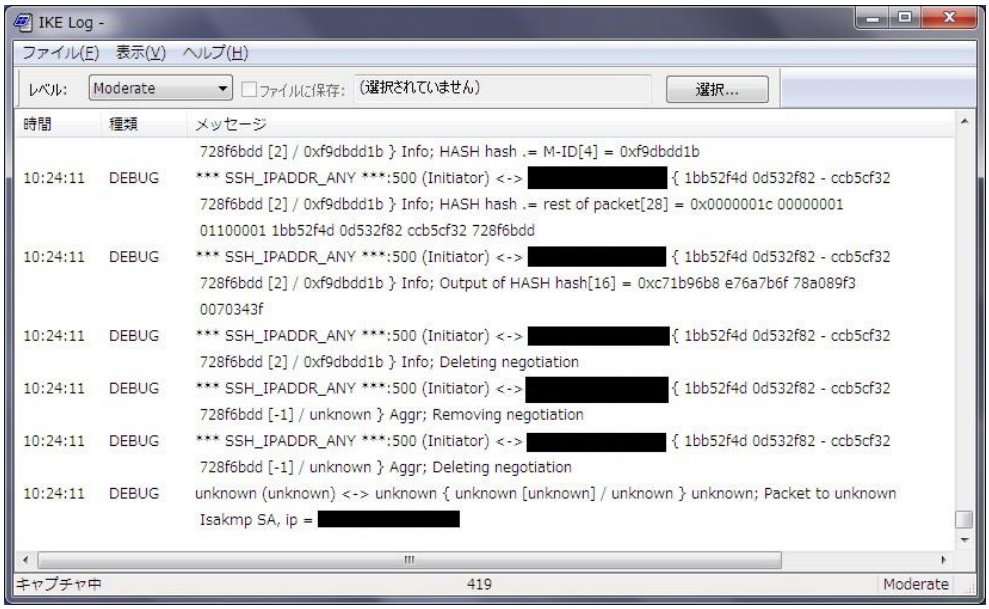


4. NET-G Secure VPN Client ログの取得を開始します。
IKE Log 画面を表示した状態で、VPN 接続を実行します。タスクトレイ内 NET-G Secure VPN Client のアイコンを右クリックして、“VPN を選択(C) ”→“【接続内容】”をクリックしてください。

※ 診断では正確なログを取得することができません。必ず実接続で行ってください。



5. VPN 接続を行うと下記画面のように、VPN 接続時のログが出力されます。
テキストファイルに保存する場合は、画面左上“ファイル”から“画面の保存”を選択して保存することができます。



NET-G Secure VPN Client ログ内容について

NET-G Secure VPN Client で接続不可時に出力されるログの内容、及び考えられる原因ついて記載します。

- **成功時のログ**

  Phase-1，Phase-2 共に、成功(done)していることが確認できます。
  ※あくまでも IPsec 接続が正常に行われている内容を示しております。実際の通信に関しては必ずご確認ください。

```
15:14:30: Auth: Info: Phase-1 [initiator] between
usr@fqdn(udp:500,[0..15]=XXXXXXXX@XXX.com) and
ipv4(udp:500,[0..3]=XXX.XXX.XXX.XXX) done.


15:14:32: Auth: Info: Phase-2 [initiator] done bundle 6 with 2 SA's by
rule 344:`ipsec ipv4(any:0,[0..3]=XXX.XXX.XXX.XXX)<-
>ipv4_subnet(any:0,[0..7]=XXX.XXX.XXX.XXX/24)(gw:ipv4(any:0,[0..3]=XXX
.XXX.XXX.XXX))'
```

```
15:14:32: Auth: Info: SA ESP[866e6fca] alg [aes-cbc/16]+hmac[hmac-
sha1-96] bundle [6,0] pri 0 opts
src=ipv4(any:0,[0..3]=XXX.XXX.XXX.XXX)
dst=ipv4_subnet(any:0,[0..7]=XXX.XXX.XXX.0/24)

15:14:32: Auth: Info: SA ESP[58c8201e] alg [aes-cbc/16]+hmac[hmac-
sha1-96] bundle [6,0] pri 0 opts
src=ipv4_subnet(any:0,[0..7]=XXX.XXX.XXX.0/24)
dst=ipv4(any:0,[0..3]=XXX.XXX.XXX.XXX)

15:14:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 56d45a28 8c11e14f - 2d9eaaae d82d4c8f [0] /
0x7249ced5 } QM; Encode packet, version = 1.0, flags = 0x00000001

15:14:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX.:500 { 56d45a28 8c11e14f - 2d9eaaae d82d4c8f [0] /
0x7249ced5 } QM; Connected
```

- **Phase-1 認証の失敗 (1)**

  考えられる原因：接続先 IP アドレス 接続先ユーザ ID 等

  下記のログの内容は Phase-1 認証に失敗していることを示しています。
  考えられる原因としては、Phase-1 認証失敗の原因が“failed; Timeout.”になっておりますので、宛先 IP の間違いや、NET-G Secure VPN Client 側で設定された接続ユーザ ID が、接続先ルータ側で設定されていない可能性があります。

```
15:19:09: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Retransmitting packet, retries = 5

15:19:11: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Retransmitting packet, retries = 4

15:19:15: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Retransmitting packet, retries = 3
```

```
15:19:23: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Retransmitting packet, retries = 2

15:19:33: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Retransmitting packet, retries = 1

15:19:38: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Removing negotiation

15:19:38: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Connection timed out or error, calling callback

15:19:38: Auth: Info: Phase-1 [initiator] between
usr@fqdn(udp:500,[0..15]=XXXXXX@dit.com) and
ipv4(udp:500,[0..3]=XXX.XXX.XXX.XXX) failed; Timeout.

15:19:38: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c1290ff4 d9550bf7 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Deleting negotiation
```

- **Phase-1 認証の失敗 (2)**

  考えられる原因：暗号化アルゴリズム(Phase-1)

  下記ログの内容も Phase-1 認証で失敗していることを示しております。
  考えられる原因としては、“failed; No proposal chosen.”と出力されておりますので、NET-G Secure VPN Client 側と対向接続ルータ間での Phase-1 認証に用いる暗号化アルゴリズムが、同じものが設定されていない可能性があります。
  Phase-1 認証に用いられる暗号化アルゴリズムについて、NET-G Secure VPN Client、接続先ルータ側ともにご確認ください。

```
15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [0] /
0x00000000 } Info; Packet to old negotiation
```

```
15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [0] /
0x00000000 } Info; Version = 1.0, Input packet fields = 0200 N

15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [0] /
0x00000000 } Info; Received notify err = No proposal chosen (14) to
isakmp sa, delete it

15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [0] /
0x00000000 } Info; Connected

15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [0] /
0x00000000 } Info; Deleting negotiation

15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [-1] /
0x00000000 } Aggr; Removing negotiation

15:31:32: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { a4294cfd 49751620 - 6c2986f4 5fab69ab [-1] /
0x00000000 } Aggr; Connection got error = 14, calling callback

15:31:32: Auth: Info: Phase-1 [initiator] between
usr@fqdn(udp:500,[0..15]=testuser@dit.com) and
ipv4(udp:500,[0..3]=XXX.XXX.XXX.XXX) failed; No proposal chosen.
```

- **Phase-1認証の失敗 (3)**

  考えられる原因：既知共有鍵パスフレーズの設定

  下記ログの内容も Phase-1 認証で失敗していることを示しております。
  考えられる原因としては、“failed; Authentication failed.”と出力されておりますので、接続認証に失敗しております。NET-G Secure VPN Client 側の既知共有鍵に設定されているパスフレーズについて、正しい値が設定されているかご確認ください。

```
15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [-1] /
0x00000000 } Aggr; Output SKEYID_e hash[16] = 0x1fc7100f e754b951
df6bca50 21554660

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [-1] /
0x00000000 } Aggr; Final encryption key[16] = 0x1fc7100f e754b951
df6bca50 21554660

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [-1] /
0x00000000 } Aggr; Output of HASH_R hash[16] = 0x621b3fef 4e785796
a22d69ed 9e298881

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [-1] /
0x00000000 } Aggr; Hash value mismatch

15:29:35: Auth: Info: Phase-1 [initiator] between
usr@fqdn(udp:500,[0..15]=XXXXXXXXX@dit.com) and
ipv4(udp:500,[0..3]=XXX.XXX.XXX.XXX) failed; Authentication failed.

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [-1] /
0x00000000 } Aggr; Error = Authentication failed (24)

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [0] /
0x1d846993 } Info; Sending negotiation back, error = 24

15:29:35: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { 3cc09d31 9d45c143 - a827f1d7 ee60dd3c [0] /
0x1d846993 } Info; Encode packet, version
```

- **Phase-2認証の失敗**

  考えられる原因: 暗号化アルゴリズム(Phase-2)

  下記ログの内容は Phase-1 認証については正常に成功しておりますが、Phase-2

認証に失敗しています。考えられる原因としましては、NET-G Secure VPN Client 側と対向接続ルータ間での Phase-2 認証に用いる暗号化アルゴリズムが、同じものが設定されていない可能性があります。
Phase-2 認証に用いられる暗号化アルゴリズムについて NET-G Secure VPN Client、接続先ルータ側ともにご確認ください。

```
15:32:52: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c58e6b82 115cb132 - c9c6c35e f84d3c07 [-1] /
0x00000000 } Aggr; Encode packet, version = 1.0, flags = 0x00000000

15:32:52: Auth: Info: Phase-1 [initiator] between
usr@fqdn(udp:500,[0..15]=XXXXXXXXX@dit.com) and
ipv4(udp:500,[0..3]=XXX.XXX.XXX.XXX) done.

15:32:52: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c58e6b82 115cb132 - c9c6c35e f84d3c07 [0] /
0xd5abe60c } QM; Start ipsec sa negotiation



15:32:53: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c58e6b82 115cb132 - c9c6c35e f84d3c07 [-1] /
unknown } Aggr; Removing negotiation

15:32:53: DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <->
XXX.XXX.XXX.XXX:500 { c58e6b82 115cb132 - c9c6c35e f84d3c07 [-1] /
unknown } Aggr; Deleting negotiation

15:32:53: Auth: Info: Phase-2 [initiator] for
ipv4(icmp:0,[0..3]=180.7.248.146) and ipv4(icmp:0,[0..3]=192.168.10.1)
failed; Aborted notification.

15:33:32: DEBUG: unknown (unknown) <-> unknown { unknown [unknown] /
unknown } unknown; Packet to unknown Isakmp SA, ip =
XXX.XXX.XXX.XXX:500
```

[Q3-2] VPN 接続をするとインターネットに接続できなくなった

A. VPN 接続を行った場合、デフォルトでは VPN 通信しか行われません。

インターネットへのアクセスも可能にするには、ポリシーエディタ画面より該当のポリシーの“規則のプロパティ”→“詳細”→“分割トンネリングを拒否する”のチェックをはずしてください。

なお、次のような留意点があります。
該当端末に何らかの脆弱性が存在した場合、分割トンネリングを許可することによって VPN 接続先に対して予期しない通信が発生する場合があります。これは、該当の端末にインターネット及び VPN 接続先の両方に接続するパスが許可されるために起こるもので、第三者がインターネットから該当端末を介して VPN 接続先にアクセスすることが可能になる、インターネットへアクセスすることで受ける攻撃によって発生する不正な通信などが考えられます。分割トンネリングの許可は、このようなリスクが存在することを認識いただき、 御社の運用ポリシーにおいて許容される設定かどうかを検討した上で ご利用されることをお薦めいたします。

[Q3-3] VPN 接続後、勝手に VPN が切断される

A. いくつかの原因が考えられますので、下記をご確認ください。

原因 1:アイドルタイムアウトになり切断された。

VPN 接続中であっても、実際の通信が行われない場合には、VPN ルータなどの仕様により自動的に VPN 接続が切断される場合があります。

原因 2：VPN ルータ側で IKE のキープアライブ設定が有効となっている。

対処方法

NET-G Secure VPN Client は IKE のキープアライブに対応しておりません。VPN ルータ側で IKE のキープアライブ設定を無効としてください。

原因 3：V2.2 より追加された DPD 機能について、NET-G Secure VPN Client と VPN ルータそれぞれの設定が一致していない。

対処方法

NET-G Secure VPN Client と VPN ルータそれぞれの正しい DPD 設定は、以下のようになります。

VPN ルータ側 DPD の設定	VPN Client 側 DPD の設定
未対応	OFF
OFF	OFF
ON	ON

原因 4：NET-G Secure VPN Client と VPN ルータそれぞれの IKE 及び IPsec の有効期間（lifetime）が適切な値となっていない。

対処方法

通常、“NET-G Secure VPN Client 側の値”＜“VPN ルータ側の値”が適切と思われます。

原因 5：IKE の有効期間（lifetime）に到達した際、VPN 接続が切断される場合があります。

[Q3-4] 診断は OK だが、実際の VPN 接続ができない

A. 次の設定を再度確認してください。

- リモートネットワークで指定しているアドレスが、 VPN 接続先のネットワークのアドレスと合っているか？
- 仮想アドレスを利用している場合は NET-G Secure VPN Client がインストールされている端末側、リモートネットワーク側の "いずれとも一致しない" アドレスとなっているか？
- VPN ルータ側でパケットのフィルタリングを行っていないか？

また、対向のルータによっては、診断が正しく動作しない場合があります。
NET-G Secure VPN Client の接続を確認するには、NET-G Secure VPN Client の実際の接続でご確認下さい。

[Q3-5] ダイヤルアップ環境でのインターネット接続不具合

A. ダイヤルアップ環境でインターネット接続をされている端末に NET-G Secure VPN Client V.2.1.0 ～ 2.1.3.01 を導入すると、 1 回目のインターネット接続は問題ありませんが、回線切断後 2 回目以降のダイヤルアップ接続時にダイヤルアップ接続その

ものは問題ありませんが、通信などができなくなるという不具合があります。バージョン 2.1.4.01 にて修正されています。また回避策は下記のようになります。

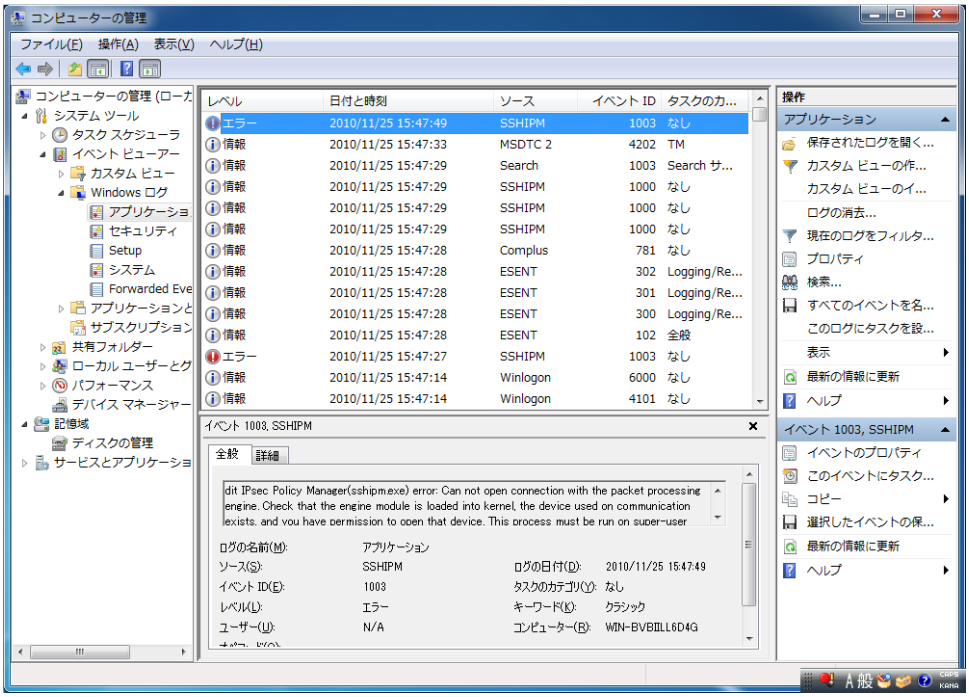
初回ダイヤルアップ接続前にダイヤルアップのエントリ ⇒ プロパティ ⇒ ネットワークから“QoS パケットスケジューラー”をアンインストール。
ただし、QoS 関連を特に利用していない場合に限ります。アンインストール後は念のため端末を再起動してください。

[Q3-6] インストール後、ポリシーマネージャを起動することができない

A. NET-G Secure VPN Client インストール後に再起動を行うと、通常であれば画面右下タスクトレイ内 NET-G Secure VPN Client のアイコンが“青色”になっていますが、NET-G Secure VPN Client のアイコンが“灰色”の状態になりポリシーエディタを起動することができない場合がございます。
本現象の原因について、NET-G Secure VPN Client インストール時にインストールされる仮想ネットワークドライバ（dit IPsec サービスドライバ）が正しくインストールされていない可能性があります。対処方法については下記手順の通りです。

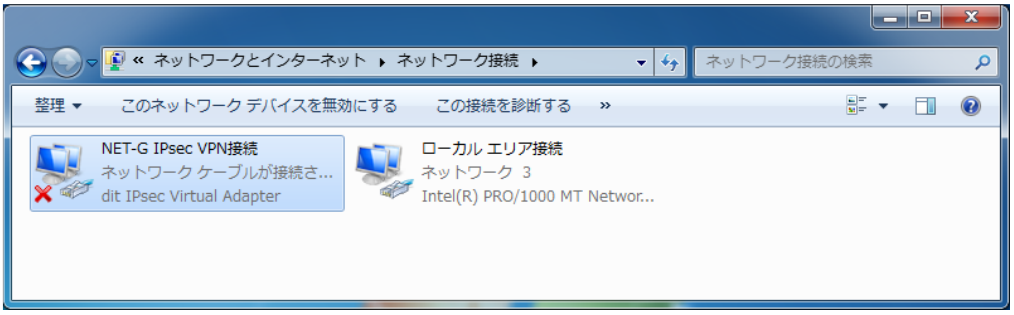
1. dit IPsec サービスドライバのインストール状態を確認します。
   イベントビューア ＞ アプリケーションログから NET-G Secure VPN Client のログを確認してください。
   以下のエラーがイベントログに記録されるときは、dit IPsec サービスドライバが正しくインストールされていません。

   “dit IPSec Policy Manager(sshipm.exe) error Can not open connection with the packet・・・・・・・・”



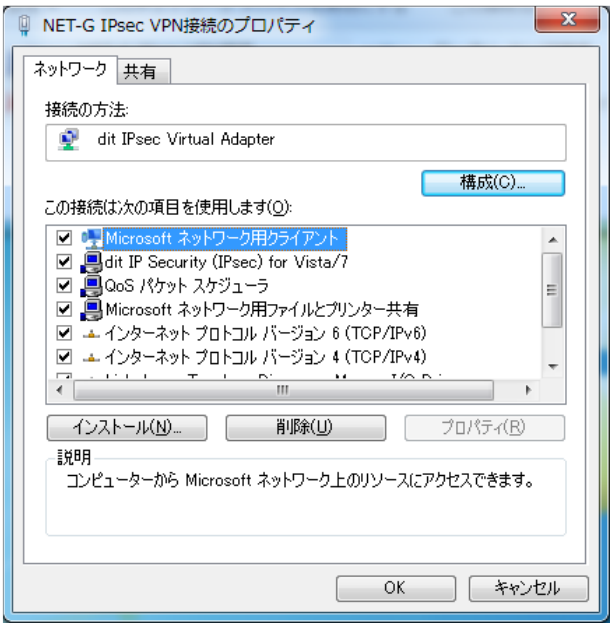
2. 以下の手順で dit IPsec サービスドライバのインストール状態を確認してください。

2-1. [ネットワーク接続]コントロールパネルを開きます。
（手順例：コントロールパネル → [ネットワークとインターネット] → [ネットワークと共有センター] → [アダプターの設定の変更]を順に選択）



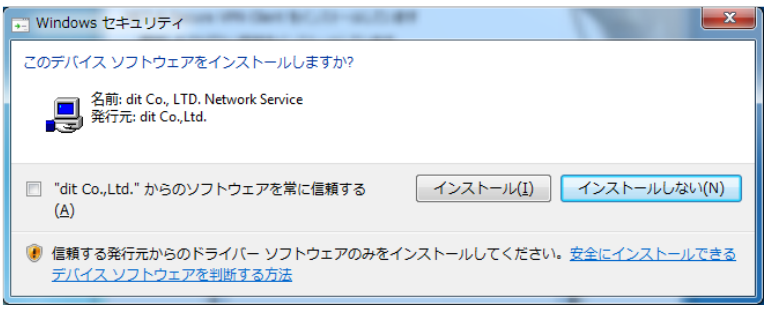
2-2. 任意のネットワーク接続を選択し、右クリックしてドロップダウンメニューから[プロパティ]を選択します。

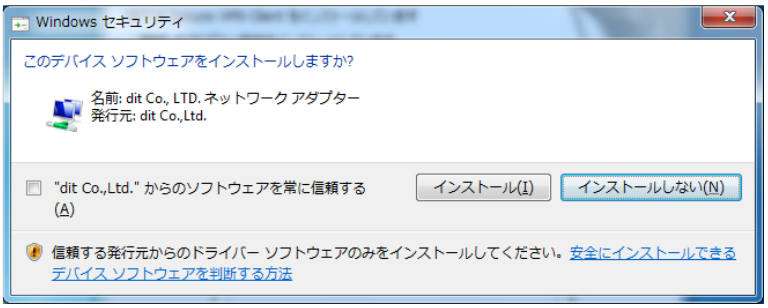
2-3. [接続のプロパティ]ダイアログの項目の一覧に[dit IP Security (IPsec) for Vista/7]サービスドライバが表示されていない場合、dit IPsec サービスドライバがインストールされていません。



dit IPsec サービスドライバは NET-G の再インストールまたは修復インストールを行うことでインストールされます。その際、以下の点にご注意ください。

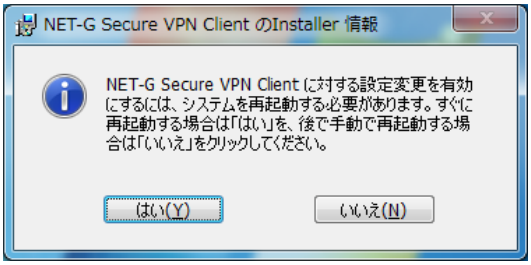
- セキュリティソフトウェアやウィルス対策ソフトウェアなどのなかには、ドライバのインストールを阻害する機能をもつものがあります。それらのソフトウェアをご使用の場合は機能をオフにしてからインストールを実行してください。
- 集中管理 PC や特殊な管理ポリシーが設定されている PC では、ドライバのインストールが阻害される場合があります。組織の管理者にご相談ください。
- NET-G Secure VPN Client 再インストール中、以下のダイアログで操作の誤りがあると正常にインストールが行われません。
    - インストール中に表示される以下の[Windows セキュリティ]ダイアログで、常に[インストール]ボタンを選択してください。





このダイアログのデフォルトは[インストールしない]になっています、単にデフォルトを選択（Enter キーを押すなど）しただけでは、インストールが正常に行われません。必ず[インストール]ボタンを選択してください。なお、このダイアログは複数回表示されますが、そのすべてで[インストール]ボタンを選択する必要があります。

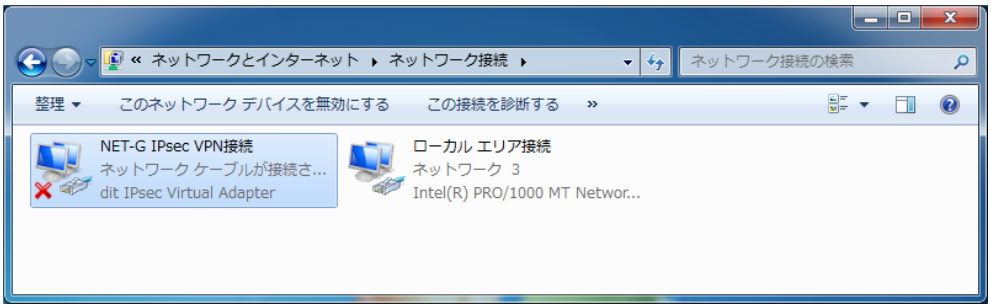
- 以下のダイアログが表示されたときは、必ず[はい]を選択してシステムを再起動してください。



再インストールで NET-G Secure VPN Client の削除 → インストールという手順を実行するとき、削除後の再起動が必要です。また、インストール後の再起動も必要です。

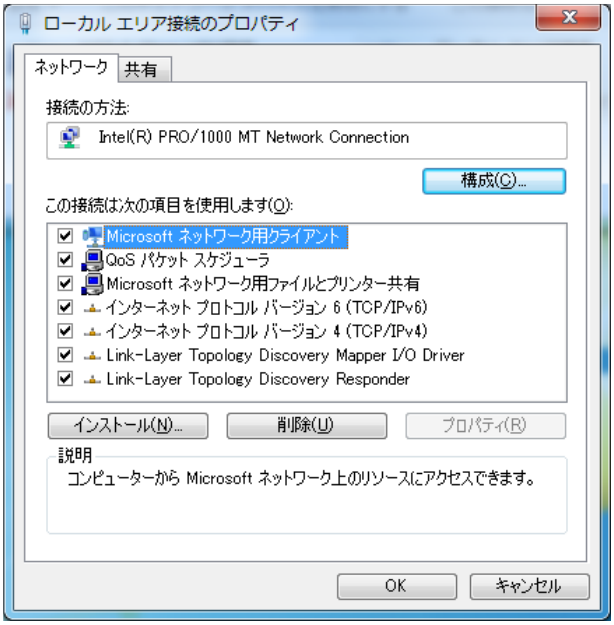
通常は、上記の手順で dit IPsec サービスドライバのインストール状態は正常になりますが、それでも正常にならないというときのため、以下に NET-G Secure VPN Client の IPsec サービスドライバのみを手動でインストールする操作手順を示します。
（なお、以下の手順は、すでに NET-G Secure VPN Client がインストールされていて dit IPsec サービスドライバのみが正常にインストールされていない、という状態を前提にしています。）

1. [ネットワーク接続]コントロールパネルを開きます
   （手順例：コントロールパネル → ネットワークとインターネット → ネットワークと共有センター → アダプターの設定の変更）

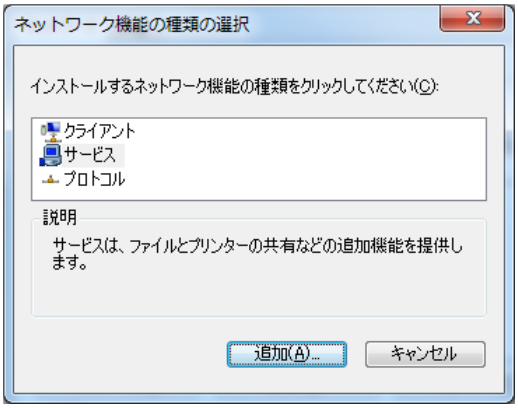


2. 任意のネットワーク接続を選択し、右クリックしてドロップダウンメニューから[プロパティ]を選択します

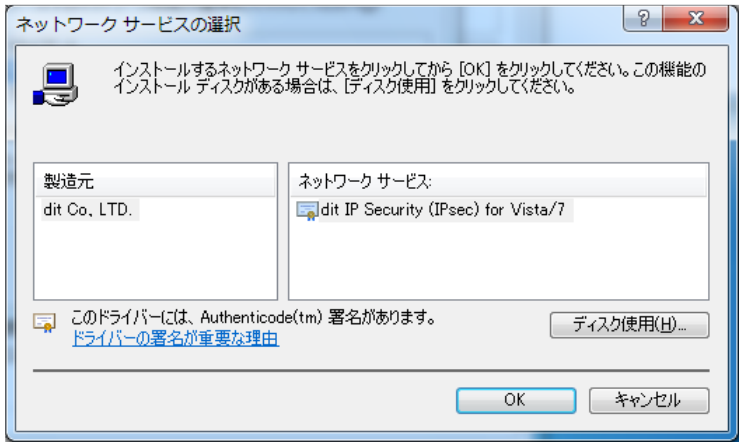
3. [インストール]ボタンを選択します。



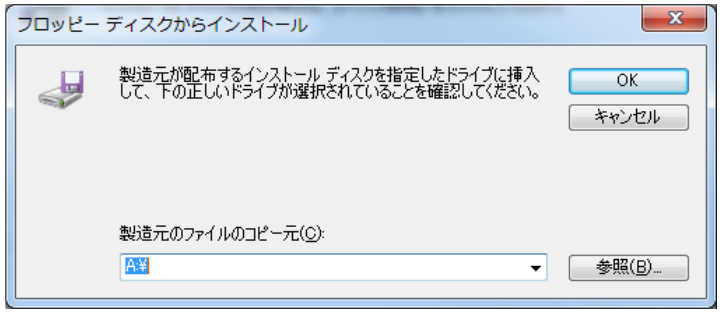
4. [ネットワーク機能の種類の選択]で種類の一覧から[サービス]を選択し、[追加]ボタンを選択します。



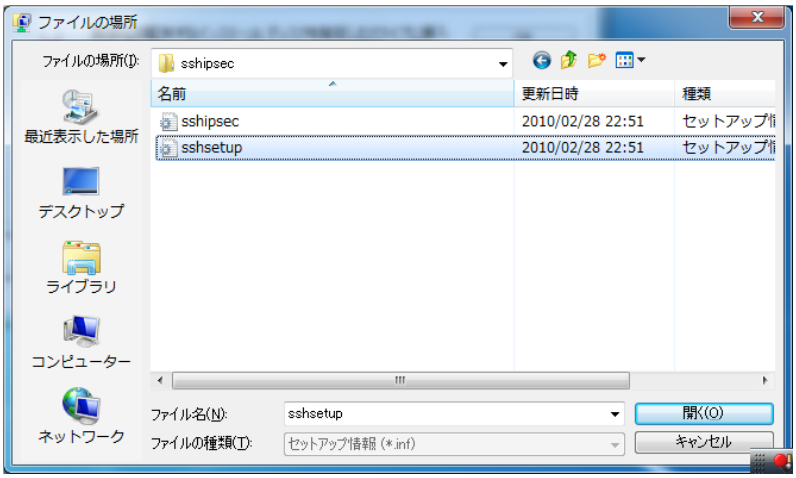
5. [ネットワーク サービスの選択]ダイアログで、[ディスク使用]ボタンを選択します。



6. [フロッピー ディスクからインストール]ダイアログで[製造元のファイルのコピー元]ボックスに NET-G Secure VPN Client のインストールフォルダの[sshipsec]サブフォルダのパス名を入力します。
（デフォルトでは、″C:¥Program Files¥dit¥NET-G Secure VPN Client¥sshipsec″）

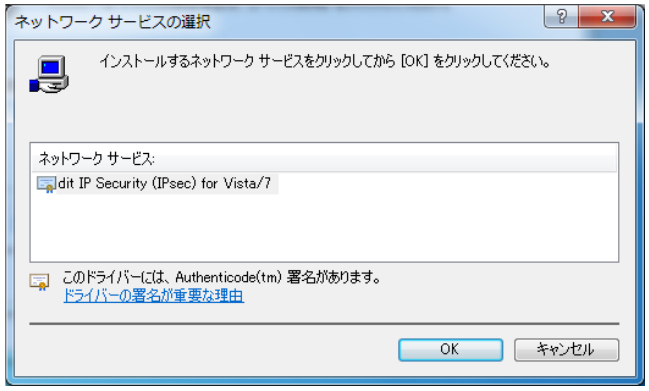


または、[フロッピー ディスクからインストール]ダイアログで[参照]ボタンを選択します。

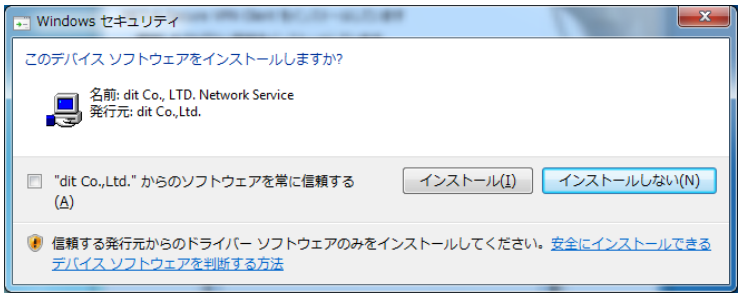


7. [ファイルの場所]ダイアログで、NET-G Secure VPN Client のインストールフォルダの[sshipsec]サブフォルダ内の[sshsetup.inf]ファイルを選択し、[開く]ボタンを選択します。
（デフォルトでは、″C:¥Program Files¥dit¥NET-G Secure VPN Client¥sshipsec¥sshsetup.inf″）

   [フロッピー ディスクからインストール]ダイアログで[OK]ボタンを選択します。

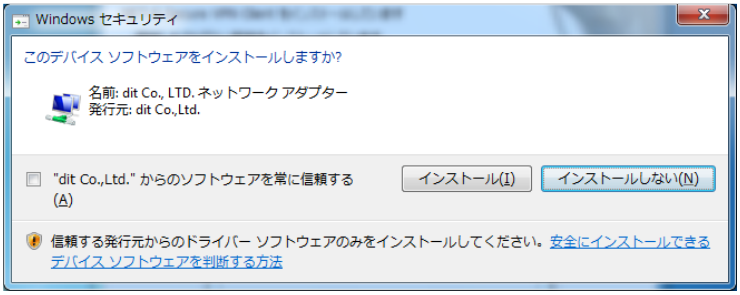


8. [ネットワークサービスの選択]ダイアログで[OK]ボタンを選択します。

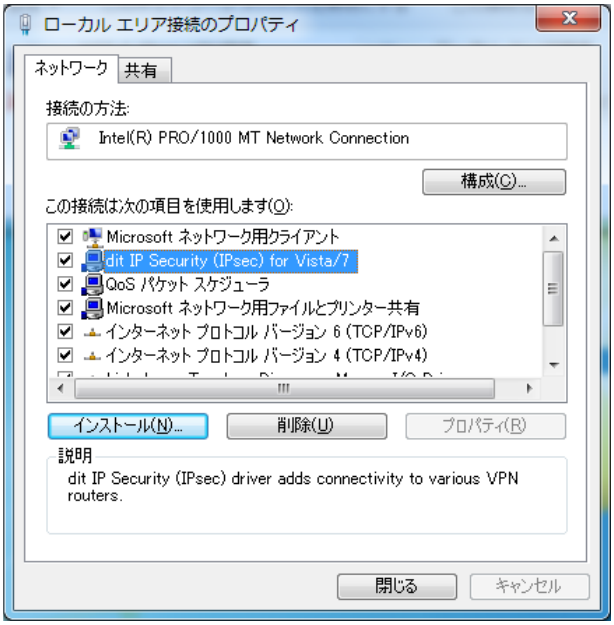


9. インストール中に表示される[Windows セキュリティ]ダイアログで、常に[インストール]ボタンを選択してください。

このダイアログのデフォルトボタンは[インストールしない]なので、単にデフォルトを選択（Enter キーを押すなど）しただけでは、インストールが正常に行われません。必ず[インストール]ボタンを選択してください。なお、このダイアログは複数回表示されますが、そのすべてで[インストール]ボタンを選択する必要があります。



10. [接続のプロパティ]ダイアログボックスの項目の一覧に、[dit IP Security (IPsec) for Vista/7]ネットワークサービスドライバが追加されたことを確認して[閉じる]ボタンを選択してください。



11. システムを再起動してください。

「システムにインストールされているフィルターが限界に達しました」と表示されてしまった場合

通常であれば、手動でインストールしていただければ NET-G Secure VPN Client のドライバがインストールされますが、Windows7/Vista に関しては OS 側の仕様で制

限がかかっている場合がございます。
制限数に達していた場合、下記のようなエラーが出力されます。

エラー内容
「システムにインストールされているフィルターが限界に達しました」

上記エラーが発生した場合、下記二つのどちらかで回避する事が可能です。

- 必要のないソフトウェアをアンインストールする
- レジストリから制限を外す
  [注意]
  この解決方法ではレジストリエディターによるレジストリの編集が必要です。レジストリエディターの使用を誤ると、深刻な問題が発生し、Windows の再インストールが必要になる場合があります。レジストリエディターは自己の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

  1. レジストリエディターから下記のディレクトリを開きます。
     HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Network
  2. 上記フォルダ内の“MaxNumFilters”をクリックします。
  3. 値のデータ(V)が“8”となっております。こちらを“9”に変更します。

[Q3-7] Windows XP で無線 LAN 及びデータ通信カードでの VPN 接続、通信ができない

A. NET-G Secure VPN Client（以下 NET-G）をインストールした Windows XP マシンに新しいネットワークアダプターを追加したとき、追加したネットワーク アダプターを経由した通信で IPsec VPN 通信が行えないことがあります。（IPsec VPN 接続は確立するものの、通信の疎通がない。）
これは、Windows XP が NET-G のドライバを自動的に新しいアダプターにバインドするのを妨げているためで、Windows XP の仕様です。詳細については、「**デジタル署名を取得していない NDIS 中間ドライバの動作に関して**」（マイクロソフト サポート オンライン 文書番号: 813700 http://support.microsoft.com/kb/813700/ja ）を参照してください。
（NET-G の NDIS 中間ドライバには、作成者のデジタル署名が付加されていますが、Microsoft 社の WHQL 認証[Windows ロゴプログラム]は取得していません。）

以下のいずれかの方法によって解決してください。

- **新しいネットワーク アダプターをインストールした後に NET-G を修復インストールまたはアップグレードインストール（上書きインストール）する**
- **新しいネットワーク アダプターをインストールした後に NET-G を手動でバインドしなおす**
- **新しいネットワーク アダプターをインストールしてから、NET-G をインストールする**

以下はそれぞれの方法についての詳細です。

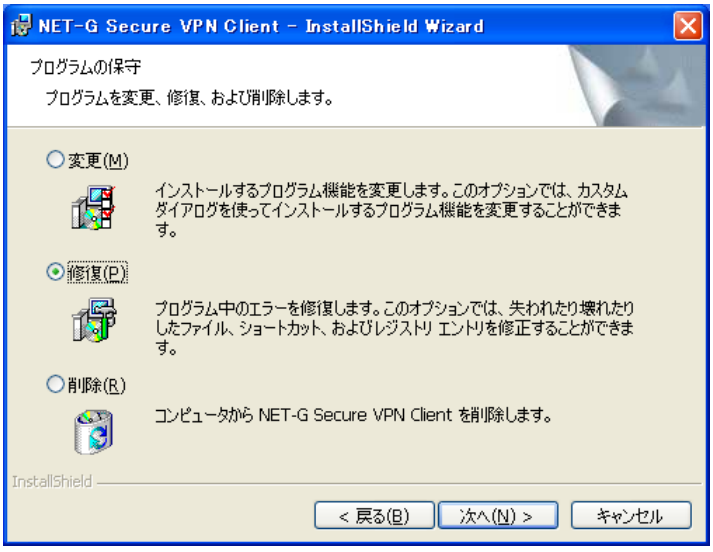
- **新しいネットワーク アダプターをインストールした後に NET-G を修復インストールまたはアップグレードインストール（上書きインストール）する**

  NET-G インストーラを実行することによって、新しいネットワーク アダプターに NET-G ドライバをバインドし直し、正常に動作することが可能となります。

  新しいネットワーク アダプターをインストールした後に、既存の NET-G のインストーラをもう一度実行すると、以下の[プログラムの保守]ダイアログが表示されます。ここで[修復]ラジオボタンが選択されていることを確認して[次へ]ボタンをクリックします。

  後はリリースノートおよびマニュアルに記載の通り、修復インストールを実行してください。

  既存の NET-G より新しいバージョンの NET-G インストーラを実行した場合は、自動的にアップグレードインストールが実行されます。この場合も、リリースノートおよびマニュアルに記載の通りインストールを完了してください。



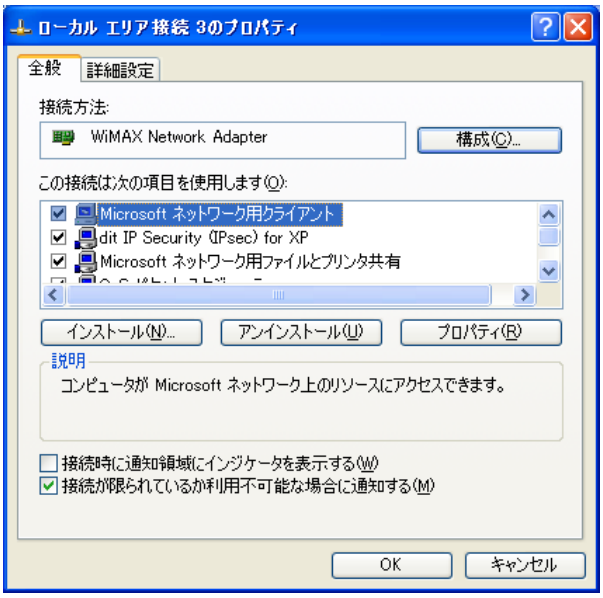
NET-G のインストーラを実行するときに、新しいネットワーク アダプターが物理的に PC に接続されているか、インターネットへ接続されているかどうかは、重要ではありません。当該ネットワーク アダプターおよびそのドライバをインストールした後に、NET-G インストーラを実行してください。

- **新しいネットワーク アダプターをインストールした後に NET-G を手動でバインドしなおす**

  新しいネットワーク アダプターをインストールした状態で、[コントロールパネル] → ([ネットワークとインターネット接続] →) [ネットワーク接続]を開きます。

[ネットワーク接続]コントロールパネルの[LAN または高速インターネット]の一覧から新しいネットワーク アダプターに該当するネットワーク接続をダブルクリックしてください。(アダプターの型名や名称の記述等を参考にして、正しいネットワーク接続を選択してください。)

以下の[...接続のプロパティ]ダイアログが表示されます。



[この接続は次の項目を使用します]リストに[dit IP Security (IPsec) for XP]があり、かつチェックがあることを確認して[OK]ボタンをクリックします。
（[OK]ボタンをクリックするだけで、特に設定を変更する必要はありません。）

- **新しいネットワーク アダプターをインストールしてから、NET-G をインストールする**

  新しいネットワーク アダプターおよび NET-G を新規の Windows XP マシンに導入する場合には、まずネットワーク アダプターとそのドライバをインストールし、次に NET-G をインストールしてください

[Q3-8] NAT 環境からの接続について

A. NET-G Secure VPN Client を利用して NAT 環境から VPN 接続を行う場合、下記のどちらかの設定を行う必要があります。下記どちらの設定も行っていない場合、VPN 接続エラーや、VPN 接続後通信することができないといった現象が発生します。

- NAT-トラバーサル
- VPN パススルー

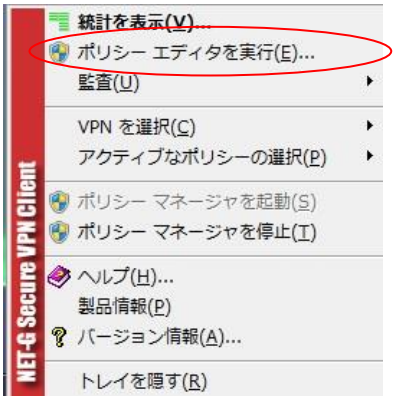
詳細な設定方法は下記の通りです。

NAT-トラバーサルの設定

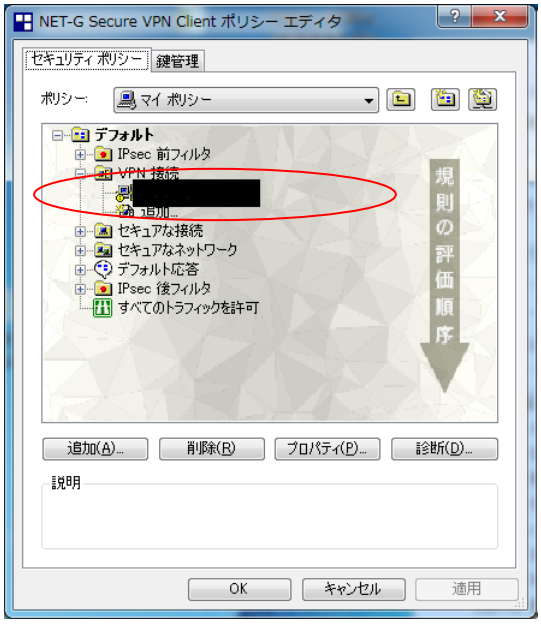
NAT-トラバーサルの機能は、NET-G Secure VPN Client と接続先 VPN ルータ共に NAT-トラバーサルの設定を有効にして頂く必要があります。

1. NET-G Secure VPN Client における NAT-トラバーサルの設定

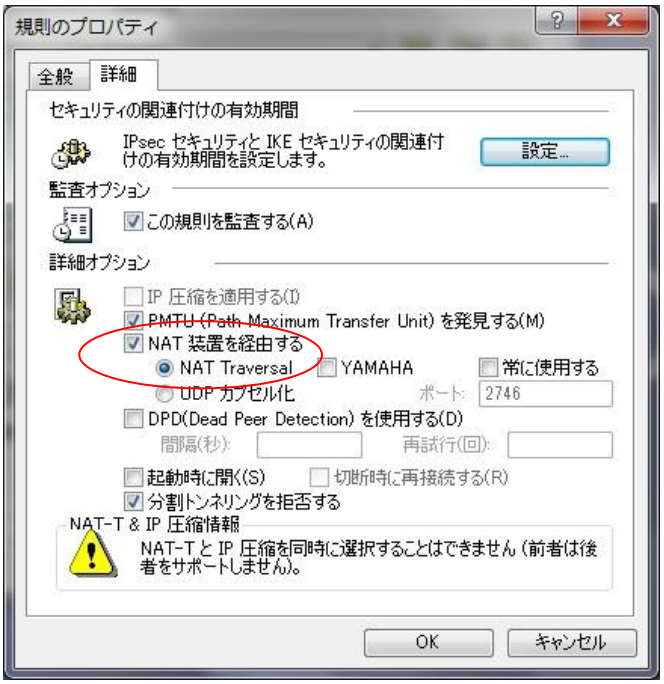
1-1. タスクトレイ内 NET-G Secure VPN Client アイコンを右クリックします。次に下記のような画面が表示されますので、“ポリシーエディタを実行(E)…”をクリックします。



1-2. 下記のような“ポリシーエディタ”画面が表示されますので、“VPN 接続”― “グローバル IP （リモートネットワーク設定）”をクリックします。



1-3. 下記のような“規則のプロパティ”画面が表示されますので、“詳細”**タブ**を選択し、“NAT 装置を経由する”にチェックします。



注意: “YAMAHA”について

NAT トラバーサル機能を有効にする場合、接続先ルータが YAMAHA 様製品の場合で、“YAMAHA”のチェックを入れていただく必要があります。

※ YAMAHA 様製品最新ファームでは、その他のメーカー様製のルータ同様チェックをする必要ないといった情報も確認されております。

NET-G Secure VPN Client の NAT トラバーサルの設定は以上になります。最後にポリシーエディタ画面から設定の適用を行ってください。

2. 接続先 VPN ルータにおける NAT トラバーサルの設定

接続先 VPN ルータの NAT トラバーサルの設定について、接続先 VPN ルータによって設定方法が異なります。詳細な設定方法について各 VPN ルータのメーカー様にお問い合わせください。

VPN パススルーの設定

VPN パススルーは、ローカルネットワーク環境のゲートウェイとなるルータに設定していただく必要があります。設定方法についてご利用されているルータによって異なりますので、詳細な設定方法について各ルータのメーカー様にお問い合わせください。

注意：VPN パススルー機能は、ルータによって機能の名称が異なる場合があります

（VPN パススルー、IPsec パススルー、VPN マルチパススルー等）。

[Q3-9] VPN 接続は確立されるが、接続先に通信することができない

A. NET-G Secure VPN Client から対向の VPN ルータに対して VPN 接続は正常に確立されるが、VPN 接続先の端末と通信することができない現象について、様々な原因が考えられます。

- **NAT 環境から VPN 接続を行い、NAT トラバーサルもしくは VPN パススルー機能が有効になっていない場合**

  NAT 環境から VPN 接続を行う場合、NAT トラバーサルもしくは VPN パススルーを有効にする必要があります。設定方法につきましては、“[Q3-8] NAT 環境からの接続について”をご確認ください。

- **データ通信カードから VPN 接続を行う環境で.NET-G Secure VPN Client のバージョンが Ver2.4.0.2 以前のバージョンの場合**

  最新のデータ通信カード（UQ WiMAX や docomo Xi 等）を利用して NET-G Secure VPN Client から VPN 接続を行う場合、NET-G Secure VPN Client のバージョンが Ver2.4.0.2 以前のバージョンの場合、本現象が発生する場合があります。最新バージョン（Ver2.5：2015/04 現在）へのバージョンアップを行いご確認いただければと思います。

  ※ データ通信カードからの VPN 接続について
  すべてのデータ通信カードでの確認は行っておりません。恐れ入りますが事前のご検証をお願いしております。

- **VPN 接続後通信を行う端末の IP アドレスが、NET-G Secure VPN Client のリモートネットワークアドレス設定に設定された、ネットワークアドレス範囲外の場合**

  NET-G Secure VPN Client から VPN 接続確立後、通信を行える端末は NET-G Secure VPN Client のリモートネットワークアドレス設定に設定されているリモートネットワークアドレスの範囲内のみとなります。例えば下記のような設定の場合は通信することはできません。

  NET-G Secure VPN Client リモートネットワークアドレス：172.16.32.0/24
  接続先 IP アドレス：192.168.1.100/24

- **NET-G Secure VPN Client のネットワーク（ローカルネットワーク）と VPN 接**

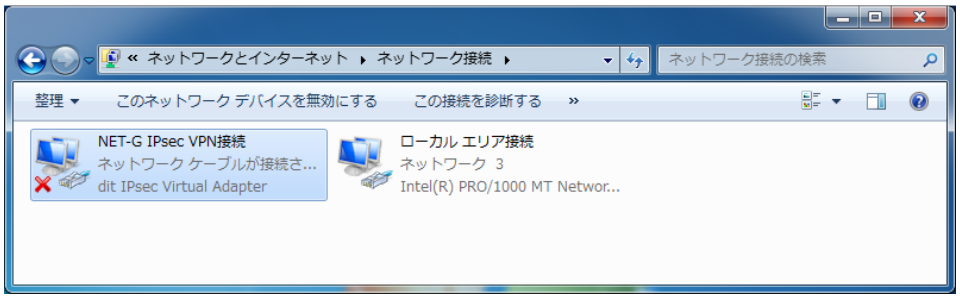
続先のネットワーク(リモートネットワーク)が同一のネットワークアドレスの場合

NET-G Secure VPN Client のネットワーク(ローカルネットワーク)と VPN 接続先のネットワーク(リモートネットワーク)が同一のネットワークアドレスの場合、VPN 接続後リモートネットワーク先に通信を行うことはできません。これは VPN 接続としての仕様となります。

- **外部ネットワークに有線を使用して接続している場合**

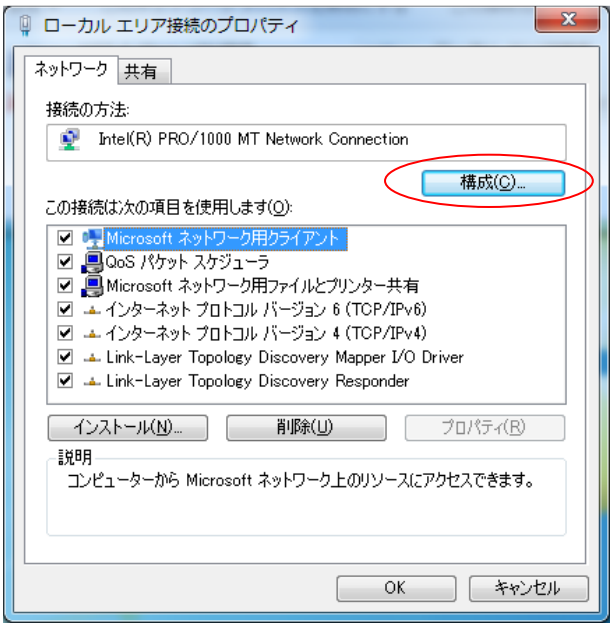
有線にて外部ネットワークに接続している場合、特定のローカルネットワークアダプターにおきましては、NAT トラバーサルを有効にしていても VPN 接続は確立されるが実際の通信ができない現象が発生することがあります。
本現象については NET-G Secure VPN Client の Vista/7 版のドライバの問題で発生する場合があり、回避策と致しましてはローカルネットワークアダプターに下記の設定を行う必要があります。

1. [ネットワーク接続]コントロールパネルを開きます
   （手順例：コントロールパネル → ネットワークとインターネット → ネットワークと共有センター → アダプターの設定の変更）



2. 該当のネットワーク接続を選択し、右クリックしてドロップダウンメニューから[プロパティ]を選択します。

3. [ローカルエリア接続]画面の[構成]ボタンを選択します。

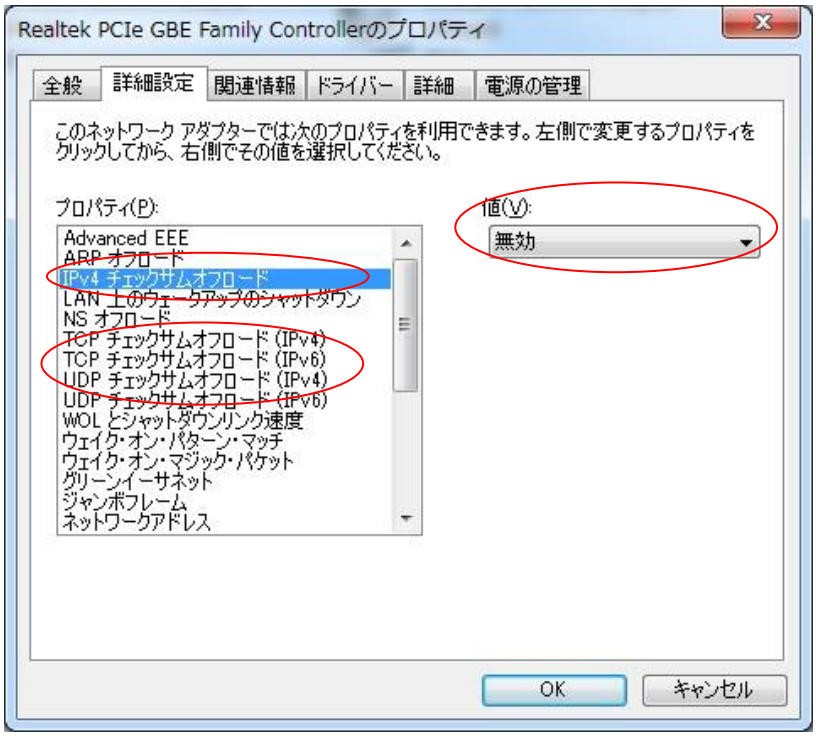


4. [...のプロパティ]画面から[詳細設定]タブを選択します。

5. [プロパティ(P):]の一覧から下記項目を選択し、全てのプロパティの[値(V):]の設定値を以下のいずれかに選択してください。

   ・プロパティ名（アダプターによって名称が異なる場合があります）
   [TCP Checksum Offload (IPv4)] または [TCP チェックサム オフロード (IPv4)]
   [UDP Checksum Offload (IPv4)] または [UDP チェックサム オフロード (IPv4)]
   [IPv4 Checksum Offload] または [IPv4 チェックサム オフロード]

   ・設定値（アダプターによって名称が異なる場合があります）
   [Disabled] または [無効]
   [Rx Enabled] または [Rx 有効]



上記事象につきましては Ver2.4.2.0 にアップデート時に修正されましたが、 一部ネットワークドライバとの組み合わせでは同様の現象が再現される場合があります。

上記チェックサムオフロードの設定は TCP/IP のパケットに付加されるチェックサムの計算を、CPU ではなくネットワークカード（NIC）に処理させる設定となります。本機能を有効にすることにより、CPU の負荷を軽減することができます。

しかしながら本機能については 2001 年頃に実装された機能となり、その当時の CPU のスペックを考慮した機能となります。現在（2015 年）の CPU のスペックは当時に比べ格段に性能が向上しており、チェックサムの計算においては CPU 側で行ったほうが、スループットが向上するといわれております。

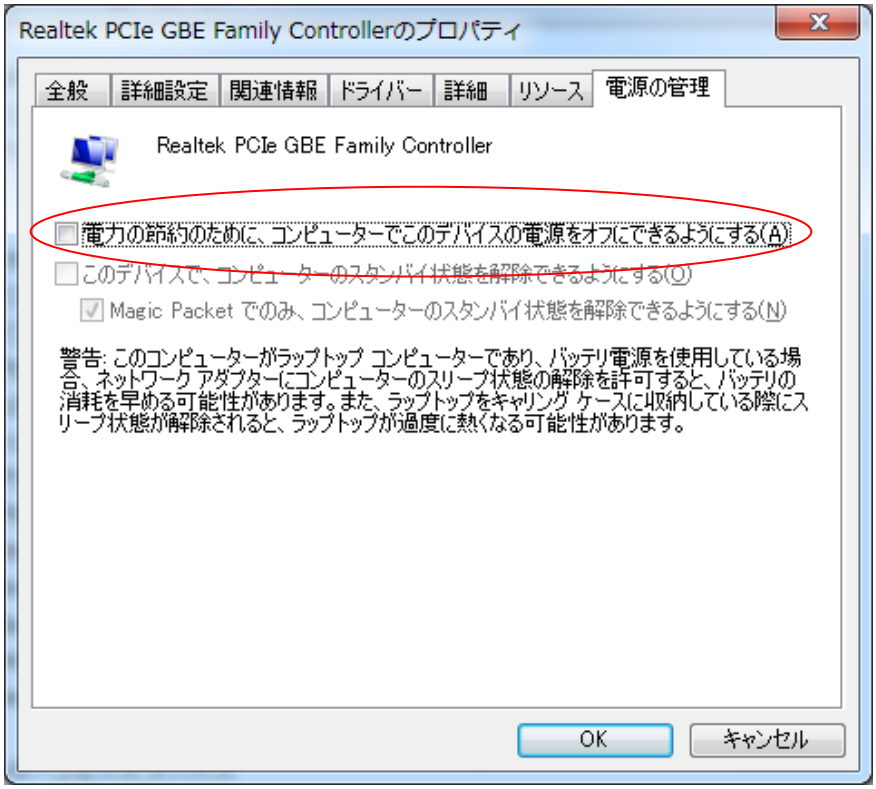
[Q3-10] スリープモードから復旧時、ブルースクリーンが発生する

A. NET-G Secure VPN Client をインストールした端末がスリープモードから復帰した際、ブルースクリーンが発生する場合があります。本現象は、端末にプリインストールされているワイヤレスネットワークドライバと NET-G Secure VPN Client の共存により発生することを確認しています。

本現象につきましては Ver.2.5 にアップデート時に修正されましたが、それ以前のバ

ージョン（Ver.2.4.2.0 以前）におきましては、下記手順にて回避可能です。

1. [コントロールパネル] → [デバイスマネージャー]を開きます。
2. [デバイスマネージャー]画面の[ネットワーク アダプター]ツリーから該当のネットワークアダプターを選択し、右クリックしてドロップダウンメニューから[プロパティ]を選択します。
3. [...のプロパティ]画面から[電源設定]タブを選択します。
[電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする(A)]のチェックを外してください。



注意:上記設定によりスリープ時の電力消費量が若干増加します。

[Q3-11] USB 接続型のイー・モバイル機器を使用時、ブルースクリーンが発生する

A. USB 接続型のイー・モバイル機器を使用してインターネット接続および VPN 接続を行った際、ブルースクリーンが発生することがあります。

本現象は、イー・モバイル機器側で下記設定を行うことにより回避可能です。

回避方法

イー・モバイル機器の通信モードを、“NDIS”から“RAS(modem)”に変更す

る。

本現象については、HUAWEI 社様のモジュールを使用しているイー・モバイル機器において NDIS モードでの通信時に、NET-G Secure VPN Client のモジュールとイー・モバイル機器のモジュールがバッティングすることにより発生することが報告されています。

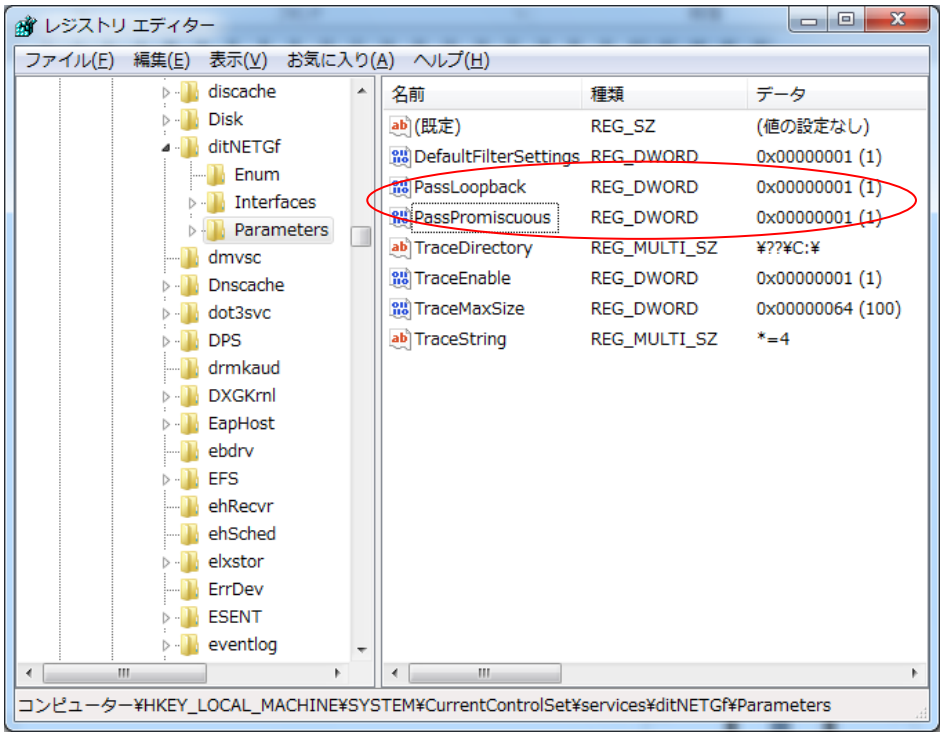
[Q3-12] パケットキャプチャソフトにて、送信パケットがキャプチャできない

A. NET-G Secure VPN Client をインストールした端末上のパケットキャプチャソフトにおいて、VPN 接続の有無にかかわらず、端末からの送信パケットがキャプチャできない場合があります。

本現象は、Ver.2.4.2.0 以降のバージョンで発生することが確認されています。

本現象につきましては、OS のレジストリ値を変更することにより回避可能です。
[注意]
この解決方法ではレジストリエディターによるレジストリの編集が必要です。レジストリエディターの使用を誤ると、深刻な問題が発生し、Windows の再インストールが必要になる場合があります。レジストリエディターは自己の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. [レジストリエディター]で以下のレジストリキーを開きます。
¥¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ditNETGf¥Parameters
2. 新たな DWORD 値“PassPromiscuous”を作成し、値を 1 にセットします。
同様に新たな DWORD 値“PassLoopback”を作成し、値を 1 にセットします。



3. OS を再起動します。

本回避策につきましては、次期バージョンにおいて NET-G Secure VPN Client インストール時にデフォルトで設定されるようになります。