SoftEther Alert

SoftEther Alert 取扱説明書 SoftEther Alert Ver 1.00 対応版

SoftEther Alert の概要、インストール方法、および使用方法に関するドキュメントです。

執筆: ソフトイーサ株式会社
発行: 2004 年 8 月 30 日
http://www.softether.co.jp/

概要

SoftEther Alert は、企業ネットワークなどの管理されたネットワーク内において、ネットワーク外との間の通信回線をモニタリングし、VPN ソフトウェア「SoftEther」の通信を検出することができるソフトウェアです。SoftEther Alert は SoftEther VPN ソフトウェア本体と同様に、フリーウェアとして配布されており、自由にダウンロードしてご利用いただくことが可能です。

ご注意

1. 「SoftEther Alert」はソフトイーサ株式会社が提供する無償のソフトウェアです。SoftEther Alert は一切保証されていない状態で提供されるソフトウェアであり、お客様が SoftEther Alert をインストール、使用した結果、または使用することができなかった場合において発生した一切の損害・不利益について、ソフトイーサ株式会社は一切責任を負いません。
2. SoftEther Alert は SoftEther VPN ソフトウェアの通信を検出することが可能ですが、すべての SoftEther VPN の通信を検出することができることは保証されません。
3. SoftEther Alert のご利用にあたっては、本ドキュメント内に明記されている使用条件に同意していただく必要がございます。
4. 「SoftEther/ソフトイーサ」は、ソフトイーサ株式会社および三菱マテリアル株式会社の登録商標です。その他記載されている商品名または会社名は、一般的に各社の登録商標または商標です。

目次

SoftEther Alert とは

SoftEther Alert の概要

SoftEther Alert をご利用いただき、ありがとうございます。SoftEther Alert は、ネットワークにおける SoftEther VPN ソフトウェアの通信を検出することが可能な IDS[1] (Intrusion Detection System／侵入検知システム) ソフトウェアの一種です。SoftEther Alert は主に企業内ネットワークのネットワーク管理者のために開発され、配布されています。

SoftEther Alert はソフトイーサ株式会社が Web サイト http://www.softether.co.jp/ 上において無償で配布しており、使用条件に同意いただいた上で、社内ネットワークなどにおいて活用していただくことが可能です。

このドキュメントは、SoftEther Alert のインストールおよび使用方法について解説します。

SoftEther の概要

ソフトイーサ株式会社がインターネット上で無償配布している VPN ソフトウェア「SoftEther」は、柔軟かつ強力な VPN (仮想プライベートネットワーク) を構築することができるソフトウェアです。SoftEther VPN クライアント (SoftEther 仮想 LAN カード) は既存のネットワークに設置されているプロキシサーバー、ファイアウォール、および NAT (Network Address Translation／アドレス変換器) を経由して、ネットワークの外側 (インターネット上) に存在する SoftEther VPN サーバー (SoftEther 仮想 HUB) に接続することができます。SoftEther VPN ソフトウェアに関する詳細な情報およびダウンロードにつきましては、http://www.softether.co.jp/ をご覧ください。

SoftEther VPN ソフトウェアは、個人および企業のネットワークのユーザーの間に広く普及しており、有益な利用が行われています。特に、企業ネットワーク内のユーザーは、自社内または個人的な目的で SoftEther VPN ソフトウェアを利用する場合に限り、ネットワーク管理者の承諾または提案を得た上で SoftEther VPN ソフトウェアを利用することにより、インターネットを経由して遠隔地のコンピュータ同士、コンピュータとネットワーク、およびネットワークとネットワーク間を Layer-2 (Ethernet レイヤ) で VPN 接続することができます。

また、SoftEther VPN ソフトウェアのセキュリティを向上させたバージョンである「SoftEther CA」ソフトウェア製品が、三菱マテリアル株式会社 システム事業センター (http://www.kisp.jp/) より 2004 年 8 月 30 日より発売されます。

SoftEther の誤用による危険性

SoftEther VPN ソフトウェアによる通信は、プロキシサーバー、ファイアウォール、および NAT な

[1] 本来の意味での IDS とは、外部ネットワーク (WAN、インターネット等) から内部ネットワークを保護する目的で、悪意のあるユーザーまたはプログラムによる通信を検出する機能を有するソフトウェアまたはハードウェアを指し、SoftEther Alert のような内部ネットワークから外部ネットワークへのアクセスを検出する目的で設計されているものは含みません。

どのネットワーク上の障壁となる装置を経由して行うことが可能であり、例えば既存のファイアウォールに危険な穴を開けることなく拠点間ネットワークが構築できるという特徴があります。

しかしながら、同時にこの長所は、企業のネットワーク管理者が社内ネットワークのユーザーによる SoftEther VPN ソフトウェアを使用した無許可の通信を検出することが困難であるという短所としても認識されています。SoftEther VPN ソフトウェアの利用するプロトコルは仮想的な Ethernet パケット (MAC フレーム) を、インターネット上で一般的に利用されている HTTPS プロトコルにカプセリングすることにより、遠隔地との VPN 通信を可能にしているため、SoftEther プロトコルの HTTPS 通信とそれ以外の HTTPS 通信を区別することが困難であるためです。HTTPS 通信は SSL (Secure Socket Layer) によって強力に暗号化されているため、ネットワークの経由地点にあるファイアウォールや IDS などが通信セッションの内容を判別することは非常に困難です。ユーザーが SoftEther VPN ソフトウェアを社内ネットワークにおいてネットワーク管理者に無断で利用し、利用方法が適切でなかった場合には、本来 IDS やファイアウォールによって安全に保護されているはずの社内ネットワーク内にコンピュータウイルスやワームなどが侵入したり、外部から悪意のあるクラッカーによって攻撃されたり、または内部で共有されている情報が外部に流出してしまったりする危険性が存在します。

そのため、一部の企業ネットワークのネットワーク管理者は、ネットワークのユーザーに対して SoftEther VPN ソフトウェアの無断での利用を禁止しています。このような状況下でも、ごく一部のユーザーが誤って SoftEther VPN ソフトウェアをネットワーク管理者の同意を得る前に無断で社内ネットワーク内のコンピュータにインストールしてしまったり、SoftEther VPN ソフトウェアがインストールされているノートブック コンピュータなどを社内ネットワークに持ち込んでしまったりすることにより、社内ネットワークとインターネット上の無関係の別のホストが SoftEther によって構築される VPN により直接的に接続されてしまう可能性があります。

このような、ネットワークユーザーによる謝った操作による SoftEther VPN ソフトウェアの社内ネットワークにおける無断利用を防止するために、ネットワーク管理者は下記のような対策を行う必要があります。

1. 社内ネットワークのユーザーに対して、社内端末に無断でソフトウェアをインストールしないように周知徹底する。
2. SoftEther VPN ソフトウェアやその他の一般的なソフトウェア製品 (例: オフィス製品など) のインストールには Administrators 権限が必要となるので、一般ユーザーに対して Administrators 権限を付与しないようにする。
3. 社内ネットワークに、社員が自宅などから持ち込んだノートブック コンピュータなどを無断で接続することを禁止する。
4. また SoftEther に限らず、管理者が許可していないソフトウェアのインストール禁止の徹底、可能であればツールによる各 PC の導入ソフトウェアの状況を監視することなども管理として重要である。

しかしながら、一部の社内ネットワークの中には、上記のような必要最低限のポリシーが運用されていない場合や、遵守されていない場合があり、SoftEther VPN ソフトウェアが社内ネットワークにおいてユーザーに誤用されてしまう可能性は依然存在しています。

SoftEther Alert の提供について

ソフトイーサ株式会社は、個人のネットワークユーザー、および企業ネットワークにおけるネットワーク管理者またはシステム設計者の方々のために、SoftEther VPN ソフトウェアを中心としたネットワーク ソフトウェアの開発および様々な施策を行っております。今回、その一環として SoftEther VPN ソフトウェアの通信を容易に検出することができるソフトウェア「SoftEther Alert」を開発いたしました。

SoftEther Alert を使用すると、社内ネットワーク管理者はネットワーク内に SoftEther Alert をインストールしたコンピュータを設置することにより、特定のネットワーク回線上を流れる SoftEther VPN ソフトウェアの通信を検出することが可能となります。

SoftEther Alert は http://www.softether.co.jp/ 上において無償で配布しており、使用条件に同意いただいた上で、社内ネットワークなどにおいて活用していただくことが可能です。

SoftEther Alert の特徴

SoftEther Alert は、Windows 2000 / XP / Server 2003 または Linux 上で動作するソフトウェアです。そのため、一般的な IDS またはファイアウォール機能を提供するハードウェア製品と異なり、導入にあたって特別なハードウェアを購入する必要がありません。また、SoftEther Alert を導入するために既存のネットワーク トポロジを変更する必要もありません。

SoftEther Alert はネットワーク内を流れるパケットをリアルタイムで読み取り、内容を判別して、通信内容に SoftEther プロトコルによる通信が含まれている場合、その通信の時刻、種類、および IP アドレスを画面上に表示することができる他、ログファイルとして自動的に保存します。システム管理者は SoftEther Alert を運用することにより、ネットワーク内における無断での SoftEther VPN ソフトウェアの使用を早期に検出することが可能です。

従来の IDS またはファイアウォールと SoftEther Alert の相違点

通常の IDS またはファイアウォールは、特定のルール (シグネチャと呼ばれる場合があります) に一致するパケットまたはそれに関連する通信セッションを検出し、遮断または記録する機能を有します。しかしながら、SoftEther プロトコルの通信内容は SSL によって暗号化されているため、パターン一致による通信の検出を行うことができず、通常の IDS またはファイアウォールによって自動的に検出または遮断することは困難です。従来の IDS またはファイアウォールに対応した SoftEther プロトコルを検出するルール (シグネチャ) は一般的に不完全であり、SoftEther プロトコルの通信以外の通信を SoftEther プロトコルによる通信であると誤認識したり、逆に

SoftEther プロトコルの通信の検出を行うことができなかったりする場合があります。

SoftEther Alert は、ネットワークの通信パケットを、予め設定されたパケット内のパターンにおける条件比較ではなく、ネットワーク内を流れる特定の IP トラフィックのすべてのパケットをリアルタイムで分析することにより、トラフィック パターンと呼ばれる、特定の TCP/IP セッションのパケットの流量を検査します。すべての検査はリアルタイムで実行されます。TCP/IP セッションの検査の結果、トラフィック パターンが SoftEther 通信の特性と一致した場合のみ、その通信を SoftEther プロトコルによる通信であると断定します。

したがって、SoftEther Alert を使用すると、従来の有償または無償の IDS やファイアウォールでは確実に検出することができなかった SoftEther VPN ソフトウェアによる通信を、非常に高い確率で検出することができるようになります。また、SoftEther プロトコル以外の通信内容を SoftEther プロトコルとして検出する確率は極めて低くなっています。

検出可能な SoftEther プロトコルの種類

SoftEther Alert は以下の SoftEther プロトコル接続を検出することができます。

- 直接的な TCP/IP 接続による SoftEther 接続
- HTTP プロキシサーバーを経由した SoftEther 接続
- SOCKS プロキシサーバーを経由した SoftEther 接続
- SSH サーバーのポート転送機能を経由した SoftEther 接続[2]

[2] SSH 経由接続の SoftEther 通信の検出にはトラフィックパターンは利用されておらず、SSH クライアント識別文字列の特徴点を使用してパターン一致判定を行っています。

SoftEther Alert の使用条件および制限事項

SoftEther Alert の使用条件

SoftEther Alert はフリーウェア (インターネット上で無償配布されるソフトウェア) ですが、現在のところ以下の使用条件がございます。SoftEther Alert を使用される場合は、以下の使用条件に同意していただく必要があります。

SoftEther Alert 使用条件

- **保証内容および免責事項への同意**
  ソフトイーサ株式会社は、SoftEther Alert (以下、本ソフトウェア) を提供するにあたり、同ソフトウェアの機能性、正確性、有用性、特定目的への適合性、コンピュータウイルスその他の有害性を含まないこと等の安全性に関し、一切保証いたしません。本ソフトウェアは一切保証されていない状態で提供されるソフトウェアであり、お客様が本ソフトウェアをインストール、使用した結果、または使用することができなかった場合において発生した一切の損害・不利益について、ソフトイーサ株式会社は一切責任を負いません。
- **ネットワーク管理者の許可の必要性**
  本ソフトウェアを組織内においてネットワーク管理者以外の方が使用される場合、予めネットワーク管理者に通知した上で許可を得る必要があります。
- **禁止事項**
  お客様は、本ソフトウェアの一部または全部をソフトイーサ株式会社の許可無くリバースエンジニアリング (ソフトウェアの仕組みや構成、要素技術などを解析すること)、リバースエンジニアリングの結果を利用して独自のソフトウェアまたはハードウェアを開発・販売すること、改変、再配布、または転載してはなりません。本ソフトウェアの再配布または転載を希望される場合は、事前にソフトイーサ株式会社の許諾を得る必要があります。
- **商用利用の禁止**
  お客様は、SoftEther Alert を商用利用することはできません。
  許可されている使用方法 (非商用利用)
  個人または組織が、その個人または組織が属する法人内のコンピュータネットワーク、またはその個人の家庭内ネットワークを管理・運営・維持するために本ソフトウェアを使用すること。
  禁止されている使用方法 (商用利用)
  商行為 (保守、サービス等を含む) の全て又は一部として、対価の有無を問わず、SoftEther Alert を使用すること。

具体例

許可されている使用方法としては、例えば以下に挙げられるようなものがあります。

- 自宅内ネットワークや、友人や親戚同士を結ぶためのコンピュータネットワークにおいて SoftEther Alert を導入し、SoftEther プロトコルの通信を検出すること。
- 自社内ネットワークの安全を維持するために、その会社に所属するネットワークのユーザーまたはネットワーク管理者が社内ネットワークに SoftEther Alert を導入し運用すること。
- 社内が複数の部署に分かれており、ネットワークを管理する部署が、そのネットワークを利用する同じ会社内のユーザーが無断で SoftEther VPN ソフトウェアを使用しないようにネットワークを監視する目的で SoftEther Alert を使用すること。

禁止されている利用方法としては、例えば以下に挙げられるようなものがあります。

- 自社以外が使用するシステムを設計・開発または構築し、そのシステムを他社に納入する際に、システムの一部として SoftEther Alert を組み込み、または使用すること。
- IT サービス業者 (例えばセキュリティコンサルタント業者やセキュリティサービス業者、インターネットサービスプロバイダなど) が顧客に対して、有償または無償を問わず、SoftEther Alert の導入、運営、または監視などのサービスを提供すること。
- 通信事業者が顧客に対して提供している通信回線上に SoftEther Alert を導入し、運用すること。
- SoftEther Alert の一部または全部を組み込み、またはリバースエンジニアリング結果を利用して製造したソフトウェアまたはハードウェアを有償・無償を問わず配布・販売すること。

SoftEther Alert の使用条件について不明な点がある場合は、このマニュアルの巻末の「お問い合わせ先」にご連絡願います。また、SoftEther Alert の商用目的での利用を希望される場合は別途お問い合わせください。

制限事項

SoftEther Alert には下記のような制限事項が存在します。

1. SoftEther Alert は、SoftEther VPN ソフトウェアの通信 (SoftEther プロトコル) を検出することができるソフトウェアですが、キャプチャ中のパケットの欠落やその他の原因などにより、特にネットワークが混雑している場合は SoftEther プロトコルの検出に失敗する場合があります。
2. SoftEther Alert は IDS 型のソフトウェアであり、ファイアウォール型のソフトウェアではありません。従って、SoftEther Alert を使用して特定のネットワーク上の SoftEther の通信を

検出することはできますが、検出した通信を自動的に遮断することはできません。

3. SoftEther Alert は SoftEther プロトコルを、トラフィックパターンを利用して検出します。そのため、プロトコル仕様が改造された SoftEther (ソフトイーサ株式会社が提供する SoftEther VPN ソフトウェアのコードの一部を不正に改変されたバージョンの SoftEther) が存在する場合、それらのバージョンの SoftEther プロトコルを検出することはできません。
4. SoftEther Alert は SoftEther フリーウェア版の通信を検出することができますが、SoftEther CA (三菱マテリアルより発売されている SoftEther の商用版) の通信を検出することはできません。SoftEther CA の通信を検出するためには、SoftEther CA Gate をご利用ください。

SoftEther Alert の動作に必要な環境

オペレーティング システム

SoftEther Alert は、以下のオペレーティング システム上で動作します。

Microsoft Windows 2000 Professional / Windows 2000 Server
Windows 2000 Advanced Server / Windows XP Professional
Windows Server 2003 Standard Edition
Windows Server 2003 Enterprise Edition
Linux (Red Hat Linux 9 で動作確認)

追加ソフトウェア

SoftEther Alert を使用するには、利用されるオペレーティング システムに対応した以下の追加ソフトウェアが必要になります。

- Windows を使用されている場合
  WinPcap の最新バージョンが必要です。以下の URL からダウンロード可能です。
  http://winpcap.polito.it/

- Linux を使用されている場合
  libpcap の最新バージョンが必要です。以下の URL からダウンロード可能です。
  http://www.tcpdump.org/

追加ソフトウェア (WinPcap または libpcap) の最新版を、予めシステムにインストールしておいてください。

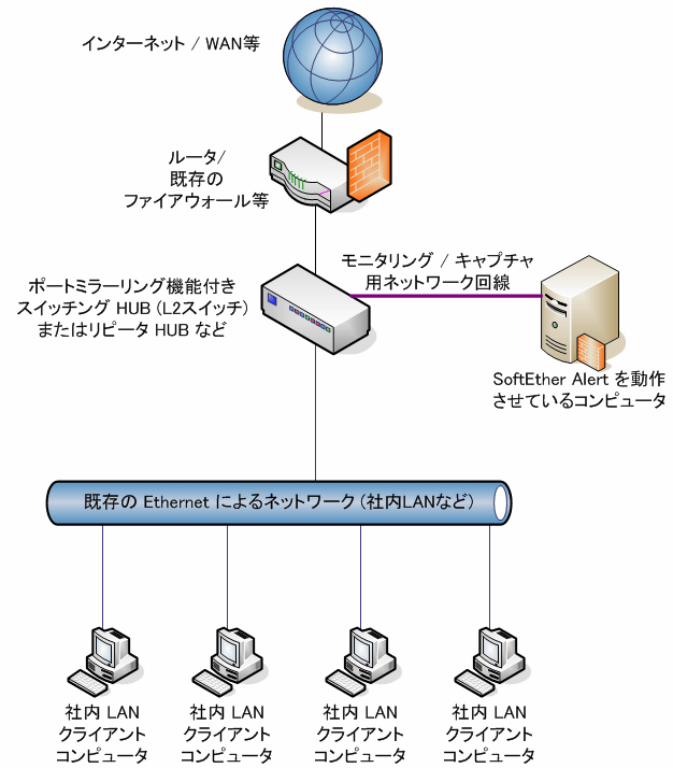
ハードウェア

SoftEther Alert は、既存のネットワーク回線上に接続されたネットワーク アダプタ (LAN カード) をプロミスキャスモードで動作させることにより、ネットワーク上の特定地点を流れるパケットをリアルタイムでキャプチャして SoftEther プロトコルの検出を行います。

SoftEther Alert を使用するためには、10Mbps、100Mbps、または 1000Mbps の Ethernet に対応した LAN カードと、特定のネットワーク上のトラフィックを検出する場合はそのネットワーク上にリピータハブまたはポートミラーリング機能付きのスイッチング HUB が必要となります。

ネットワーク構成例

キャプチャする地点の選択



SoftEther Alert の最も大きな利用目的として、社内ネットワークと外部ネットワーク (インターネットや WAN など) との間で、無断で行われる SoftEther VPN ソフトウェアによる通信を検出するという目的が想定されます。このような目的で SoftEther Alert を利用するには、社内 LAN と外部ネットワークとの間の Ethernet ネットワークの一地点にポートミラーリング機能付きのスイッチング HUB (インテリジェントスイッチ) を挿入します。既に外部ネットワークへの接続点にポートミラーリング機能付きのインテリジェントスイッチが設置されている場合は、そのスイッチを利用することもできます。また、ポートミラーリング機能付きスイッチを用意することができない場合は、一般的なリピータ HUB を利用することができます (既存の通信回線のスループットよりも高速なリピータ HUB が必要になることに注意してください)。つまり、SoftEther Alert はパケット監視型の IDS 装置 (Tap 装置またはセンサ装置と呼ばれます) を設置する場合と同様、既存の Ethernet ネットワークの全パケットをキャプチャ可能な Ethernet ポートが 1 つ必要です。

パケットキャプチャ用 LAN カードに関する注意

SoftEther Alert を使用する場合は、SoftEther Alert を動作させるコンピュータにキャプチャ専用の 1 枚の LAN カードをインストールする必要があります。

SoftEther Alert は、ネットワーク上を流れるすべての通信パケットをリアルタイムでキャプチャし、トラフィック パターンを判別します。そのため、高速な Ethernet ネットワーク上で SoftEther Alert を使用するためには、できる限り高性能な Ethernet LAN カードをご利用になることを強くお勧めします。

一般的に、家庭向けの量販店などで販売されている安価な LAN カードを SoftEther Alert のような監視用ソフトウェアのために使用することはお勧めできません。ソフトイーサ株式会社は、以下の製造元のチップが採用されている LAN カードの使用を推奨します。

- Intel 社
- 3COM 社

一般的に、性能の低い LAN カード (安価な LAN カード) をパケット キャプチャ用途に使用した場合、パケットの取りこぼし (欠落) する確率が高くなり、SoftEther Alert が SoftEther による通信を確実に検出することができる確率が若干低くなってしまいます。

Windows 2000 / XP / Server 2003 での導入と利用

WinPcap のインストール

WinPcap の最新版を http://winpcap.polito.it/ からダウンロードし、インストールする必要があります。WinPcap をインストールするには、コンピュータの Administrators 権限が必要になります。

sealert.exe の起動

SoftEther Alert の Win32 版アーカイブ ファイルから sealert.exe を展開し、任意のディレクトリ上に設置します。

sealert.exe の起動には、必ずしも Administrators 権限は必要ありません。

sealert による通信の監視を開始

sealert の使用方法は、Windows 版、Linux 版共に同一です。詳しくは、この後の章を参照してください。

Linux での導入と利用

libpcap 最新版のインストール

Linux 版 sealert を使用するためには、libpcap (Linux/UNIX 用パケットキャプチャライブラリ) の最新版が必要になります。libpcap は以下の URL からダウンロードできます。

http://www.tcpdump.org/

※ libpcap は、最近の Linux ディストリビューションには標準でインストールされていますが、バージョンが古すぎる場合があります。バージョンが古すぎる場合は、sealert のビルドおよび実行に失敗します。この場合は、最新版の libpcap を上記 URL からダウンロードし、インストールしてください。

※ libpcap のインストール方法については、上記 Web サイトを参照してください。

sealert のビルド

sealert の Linux 版アーカイブ ファイルを展開すると、sealert.s ファイルが解凍されます。sealert.s ファイルはアセンブリ形式のファイルであり、コンピュータ上で起動するためには gcc によるビルドが必要です。

まず、sealert.s を適当なディレクトリ上に設置します。

```
[root@gate se_alert]# ls -l
合計 28
-rw-r--r--      1 root       root          24914   8 月  29 23:24 sealert.s
```

次に、**gcc sealert.s -lpcap -o sealert** と入力し、sealert 実行可能ファイルを生成します。

```
[root@gate se_alert]# gcc sealert.s -lpcap -o sealert
[root@gate se_alert]# ls -l
合計 48
-rwxr-xr-x      1 root       root          18930   8 月  29 23:25 sealert
-rw-r--r--      1 root       root          24914   8 月  29 23:24 sealert.s
```

sealert による通信の監視を開始

sealert の使用方法は、Windows 版、Linux 版共に同一です。詳しくは、この後の章を参照してください。

sealert の使用方法

sealert の起動

sealert の操作方法およびコマンドラインオプションは、Windows 版・Linux 版共に同一です。sealert 実行可能ファイルを準備したら、通常のアプリケーションと同様に起動してください。

Windows 版では、sealert は Administrators 権限を持つユーザー以外でも起動することができます。Linux 版では、root のみが sealert を起動することができます。

キャプチャする LAN カードの選択

sealert を起動すると、コンピュータに装着されている LAN カードの一覧が表示されます。ここで、SoftEther の通信を監視したいネットワークに接続されている LAN カード (詳しくは「ネットワーク構成例」を参照してください) の番号を選択し、入力します。

```
SoftEther Alert Version 1.00
Copyright (C) 2004 SoftEther Corporation.
All Rights Reserved.

Network Devices:
  1: Realtek 8139-series PCI NIC
  2: FreeLAN
  3: NET IP/1394 Miniport
  4: Broadcom NetXtreme Gigabit Ethernet Driver
  5: SoftEther

Device ID>4

Starting Capture Packets at [Broadcom NetXtreme Gigabit Ethernet Driver].
```

なお、sealert のコマンドライン オプションとしてキャプチャする LAN カードの番号を整数値で指定することにより、自動的に指定された LAN カードでの監視を開始することも可能です。

SoftEther プロトコルでの通信を検出した場合のログ記録について

sealert が監視対象のネットワーク上で SoftEther による通信を検出した場合は、sealert を起動しているコンソール上および、sealert を起動したカレントディレクトリ上に自動的に作成されるログファイル sealert.log に通信ログ (検出結果) が保存されます。

保存されるログの種類と内容

sealert が保存する通信ログは、1 回の SoftEther プロトコルによる SoftEther 仮想 LAN カードから SoftEther 仮想 HUB への接続の発生時に、1 つの行として記録されます。下記は、その例です。

```
[2004/08/28 20:01:00] SoftEther 1.0 TCP Connection Detected↓
   (client 192.168.126.229:1027, server 61.197.235.210:7777)    …… ①
[2004/08/28 22:15:19] SoftEther 1.0 SSH Connection Detected↓
   (client 192.168.126.229:1108, server 130.158.86.23:22)       …… ②
```

上の例では、①および②の 2 つの行が通信ログとして保存されています。

それぞれ、SoftEther プロトコルによる通信のクライアント IP アドレスとポート番号、サーバーIP アドレスとポート番号、時刻、およびプロトコルの種類が表示されます。

ログ①では、8 月 28 日の 20 時 1 分に、社内 LAN のアドレス 192.168.126.229 のコンピュータが、インターネット上にある SoftEther 仮想 HUB (アドレス 61.197.235.210) に対して SoftEther プロトコルにより TCP 接続したことを示します。

ログ②では、8 月 28 日の 22 時 15 分に、社内 LAN の 192.168.126.229 のコンピュータが、インターネット上にある SoftEther 仮想 HUB に SSH サーバー (130.158.86.23) を経由した SSH ポート転送接続によって SoftEther プロトコルにより接続したことを示します。

SoftEther Alert に関するよくある質問と回答 (Q&A)

SoftEther Alert に関してよく寄せられると想定される質問と回答を用意いたしました。

質問1. SoftEther Alert はフリーウェアですか?

はい、SoftEther Alert はフリーウェアであり、www.softether.co.jp 上でソフトイーサ株式会社が無償配布しています。ただし、若干の使用条件がありますのでご確認ください。

質問2. SoftEther Alert は SoftEther による通信を確実に検出可能ですか?

いいえ、SoftEther Alert が特定のネットワーク内における SoftEther プロトコルによる通信を 100%確実に検出することができることは保証されていません。いくつかの悪条件 (ネットワークの高負荷状況の発生や SoftEther Alert を実行しているコンピュータの性能不足、ネットワークエラーなど) により、実際には SoftEther による通信が行われているにもかかわらず、通信を検出できない場合があります。

質問3. SoftEther Alert は従来のファイアウォールや IDS とはどのように異なりますか?

従来通常の IDS またはファイアウォールは、特定のルール (シグネチャと呼ばれる場合があります) に一致するパケットまたはそれに関連する通信セッションを検出し、遮断または記録する機能を有します。しかしながら、SoftEther プロトコルの通信内容は SSL によって暗号化されているため、パターン一致による通信の検出を行うことができず、通常の IDS またはファイアウォールによって自動的に検出または遮断することは困難です。従来の IDS またはファイアウォールに対応した SoftEther プロトコルを検出するルール (シグネチャ) は一般的に不完全であり、SoftEther プロトコルの通信以外の通信を SoftEther プロトコルによる通信であると誤認識したり、逆に SoftEther プロトコルの通信の検出を行うことができなかったりする場合があります。SoftEther Alert は、ネットワークの通信パケットを、予め設定されたパケット内のパターンにおける条件比較ではなく、ネットワーク内を流れる特定の IP トラフィックのすべてのパケットをリアルタイムで分析することにより、トラフィック パターンと呼ばれる、特定の TCP/IP セッションのパケットの流量を検査します。すべての検査はリアルタイムで実行されます。TCP/IP セッションの検査の結果、トラフィック パターンが SoftEther 通信の特性と一致した場合のみ、その通信を SoftEther プロトコルによる通信であると断定します。したがって、SoftEther Alert を使用すると、従来の有償または無償の IDS やファイアウォールでは確実に検出することができなかった SoftEther VPN ソフトウェアによる通信を、非常に高い確率で検出することができるようになります。また、SoftEther プロトコル以外の通信内容を SoftEther プロトコルとして検出する確率は極めて低くなっています。

質問4. SoftEther Alert を自社のネットワーク監視業務に利用することはできますか?

はい、可能です。SoftEther Alert の使用条件によると、自社内のネットワーク監視目的で SoftEther Alert をご利用いただくことが可能となっています。

質問5. SoftEther Alert を使用して顧客に対してネットワーク監視サービスを提供することは可能ですか?

いいえ、SoftEther Alert の商用利用は使用条件により禁止されています。商用利用をご希望の場合は弊社までお問い合わせください。

質問6. SoftEther Alert をインストールしたコンピュータを既存のネットワーク内に設置する場合、どの地点に設置するのが最も効率的ですか?

社内ネットワークから外部ネットワーク (インターネットや WAN など) への通信が必ず流れる地点 (通常はルータの直前) に SoftEther Alert をインストールしたコンピュータを設置されることをお勧めします。これにより、社内ネットワークに存在するすべてのコンピュータの外部との SoftEther 通信を検出可能です。

質問7. 社内ネットワークでは複数のクライアント コンピュータがインターネットに接続できるようにするため、NAT を使用しています。SoftEther Alert をインストールしたコンピュータはどの地点に設置するのが最適ですか?

インターネットへの接続に NAT が使用されているネットワークの場合、NAT の内側 (NAT になっているルータ装置またはコンピュータの内部ネットワーク側インターフェイスの出口の部分) に SoftEther Alert を設置することをお勧めします。この場合、通信ログには社内のプライベート IP アドレスによってクライアント コンピュータによる SoftEther 通信が記録されます。NAT の外側に SoftEther Alert を設置した場合、通信ログに記録されるクライアント コンピュータの IP アドレスは NAT の外側インターフェイスの IP アドレスとなります。

質問8. SoftEther Alert は IPv6 に対応していますか?

SoftEther Alert は IPv6 には対応しておりません。

質問9. SoftEther Alert をインストールし、常時 SoftEther Alert を稼動させているコンピュータでは、他のアプリケーションやサーバーソフトウェアを稼動させることはできますか?

はい、可能です。ただし、コンピュータの負荷が高くなり、SoftEther Alert がネットワークを流れるすべてのパケットを検査することができなくなる可能性がありますので、お勧めできません。

SoftEther Alert に関するお問い合わせ先

SoftEther Alert に関するお問い合わせは、以下のメールアドレスまでお願いいたします。

※ メールをお送りいただく際には、ご氏名、会社名、部署名、および返送先メールアドレスを明記していただきますようお願い申し上げます。

※ お送りいただいたメールへの回答には時間がかかる場合がございますので、ご了承ください。

- **SoftEther Alert の使用条件に関するお問い合わせ**
- **SoftEther Alert を商用目的で利用されることを希望される場合のお問い合わせ**
- **SoftEther Alert をインターネット上や雑誌・書籍の CD-ROM などに転載される場合のご連絡先**

  support@softether.co.jp

- **SoftEther Alert に関する技術的なお問い合わせ**
  ソフトイーサ株式会社では、SoftEther Alert に関する技術的なサポートを提供しておりません。ただし、SoftEther に関する情報をユーザーの皆様に交換していただくためにメーリングリストサービスを提供しています。
  softether@softether.co.jp (メーリングリスト)
  http://www.softether.com/jp/ml/

- **報道関係者の方々のためのお問い合わせ先**

  press@softether.co.jp

SoftEther Alert 取扱説明書 SoftEther Alert Ver 1.00 対応版

SoftEther Alert の概要、インストール方法、および使用方法に関するドキュメントです。

執筆: ソフトイーサ株式会社

発行: 2004 年 8 月 30 日

http://www.softether.co.jp/