

Solaris™ 9 オペレーティング環境 における IPsec

Technical White Paper



目次

概要	1
ネットワークに対する脅威	3
セッションの盗聴	4
パスワードの盗難	4
信頼関係の悪用	4
情報の流出	4
ホスト・スプーフィング	4
セッションのハイジャック	5
ネットワーク・サービスの無防備	5
反射攻撃	5
IPsec による防護 - 概要	6
セキュリティ・アソシエーション	7
自動による鍵管理	8
プライベート・ネットワークでの通信	8
仮想プライベート・ネットワーク (VPN)	8
強力なホスト認証機能	9
通信の完全性	9
通信の防御	9
アプリケーションの防御	9
IPv4/IPv6 プロトコル	10
仮想プライベート・ネットワーク (VPN)	11
遠隔サイトの防御	11
モバイル・ユーザの防御	12
ネットワーク資源の分離と防御	13
エンド・システム	14
個別のサービスに対する防御	14
簡単なパケット・フィルタリング	14
強化型システム	15
ネットワークの管理	15
バックアップ・ネットワーク	15
ストレージ・ネットワーク	15
鍵管理	15
ホスト鍵の管理	15
公開鍵インフラストラクチャ (Public Key Infrastructure: PKI)	16
鍵の作成と配布	16
セキュリティ・ポリシーに関する考察	18
特殊なポリシー・ステートメント	18
セキュリティ保護されたネットワーク /VPN の管理	19
サービスの防護面での要請	19
暗号化における最低限の要請	19
法的面での要請	20
まとめ	21

第 1 章

概要

Solaris™ オペレーティング環境 (OE) は、ネットワーク・コンピューティングにおけるセキュリティ機能に関して、常に一步先を行く存在です。Solaris 9 OE に Internet Protocol Security (IPsec) を装備することで、こうしたリードは更に拡大されることになるでしょう。今日のネットワーク・ビジネスの時代において、企業やビジネス・パートナーなどの情報を含めたシステム・データのセキュリティ保護は、戦略的な重要課題となっています。IPsec による防護は、IP レイヤーにおいて細かな設定が可能であるため、ビジネス・データの保護において大きな利点をもたらします。これらの保護は IP レイヤー上で実施されるため、あらゆるタイプのインターネット・トラフィックに対して防護を施すことができ、しかもネットワークを利用するアプリケーションおよびサービスに対しては透過的なものとなります。

IPsec の防護が適用されるレベルとタイプについては、柔軟な設定が可能です。IPsec は、様々な認証および暗号化機構と各種のポリシー・ルールを組み合わせることで、2 つのネットワーク・ノード間の全通信を始め、特定のタイプのトラフィックやアプリケーション固有のセッションを保護し、その他各種の状況に応じた防護を施します。IPsec は追加的な実装が可能で、遠隔ユーザや出先機関の間の通信や、運用組織内のイントラネットおよび外部エクストラネットを対象として、その一部ないし全域をカバーすることができます。個々のアプリケーションが IPsec の存在を意識することがないように、ユーザもシステムの操作法の変更を強いられることはありません。これは、IPsec がネットワークに対して施す防護が透過的なものだからです。ネットワーク管理者は、ネットワーク全域および特定ホストに関するポリシーに対して、必要な判断をした上で施行することができます。

Solaris 9 OE 用に用意された従来のセキュリティ機能である Secure Shell に比べた場合、IPsec はより包括的なソリューションとして提供されます。Secure Shell は強力なセキュリティ・ツールであり、大方のユーザ環境において比較的容易に実装することができます。また Secure Shell は、配備が容易な軽量型アプリケーションでありながらも、ユーザ・セッションに対する強力なセキュリティ機能を装備しており、ユーザによるクライアント・サイドの設定も可能です。これに対して IPsec は、より柔軟で広範なソリューションですが、実装と管理に際してはかなりの手間がかかります。この IPsec は複数のシステムに対して特定の防護を施すもので、その設定は管理者の指定するポリシーにより制御されます。IPsec の機能はアプリケーションに対して透過的で、ネットワーク・トラフィックを防護するに当たって、操作面での特別な変更は不要です。どちらの機能を用いるにせよ、適切な環境に正しく実装することで、遠隔地ないしネットワークでのコンピューティング処理に対する強力なセキュリティ機能を利用できます。

表 1 に、2 つのセキュリティ・テクノロジーの機能に関する比較を示します。

表 1 IPsec と Secure Shell テクノロジーの比較

機能	IPsec	Solaris 9 OE Secure Shell
設定と保守の難易度	比較的複雑	比較的容易
ポリシーの中央制御	あり	なし
アプリケーションに対する透過性	あり	なし
ユーザに対する透過性	あり	rcp などの アプリケーション・ コマンドは類似 (scp)
ネットワーク防護	プライバシー、ホスト・ ツー・ホスト認証、 VPN、完全性、自動 鍵管理	プライバシー、高度な ユーザ認証とホスト 認証、セッション 完全性
X-Window セッションのセキュリティ保護	あり	あり

Solaris OE には、過去に IT ソリューションとしての標準に準拠したテクノロジーを開発してきたという実績があります。Solaris OE における IPsec は、Internet Engineering Task Force (IETF) 標準との密接な関係を意識して実装されています。IPsec の実装に関するその他のメリットとしては、Solaris ソフトウェアに装備されているアプリケーション・プログラミング・インターフェース (API) が、アプリケーション・レベルで IPsec ポリシーを指定できる点があります。これによりアプリケーション開発者は、IPsec の提供するセキュリティ面での追加機能をフルに活用できるはずで

このホワイト・ペーパーでは、ネットワーク運営上の脅威となる存在について解説し、こうした脅威への対抗手段として IPsec がどのように機能するかの概要を紹介します。これらの解説では、IPsec の諸機能と、それを支えるテクノロジーについても言及します。その他にも、主要な管理機能についての情報や、仮想プライベート・ネットワーク (virtual private network: VPN) 環境での IPsec の使用について解説します。

第2章

ネットワークに対する脅威

今日多くの企業が、カスタマ、パートナー、サプライヤとの業務処理にネットワーク・システムを活用しています。新規市場の開拓や、カスタマ、パートナー、サプライヤとの緊密な関係の構築、および総合的な生産性の向上において、インターネットが有用なツールであることは間違いありません。ただし、こうしたメリットを享受する見返りとして、システムの誤用や故障に加えて、外部からの攻撃にさらされる危険性が増大しています。内部および外部との連絡用にネットワークへの依存度が高くなるに従い、より一層重要となるものが、システムのセキュリティ問題です。

現在の企業の大多数は、内部および外部の攻撃によるセキュリティ面でのリスクを抱えています。たとえば『2001 CSI/FBI Computer Crime and Security Survey』には、以下の数字が挙げられています。

- 91%の回答者が、インターネットのアクセス権を乱用している従業員を見つけたと報告
- 85%の回答者が、過去12ヵ月以内に、セキュリティを突破された経験があると報告
- 76%の回答者が、攻撃を仕掛けた犯人として、会社に不満を抱く従業員を疑っていると報告
- 40%の回答者が、外部からの攻撃を検出したと報告
- 78%の回答者が、サービス拒否攻撃を受けたと報告
- 13%の回答者が、トランザクション情報が漏洩されたと報告(2000年の8%から上昇)

セキュリティ面での脅威には、いくつもの種類があります。下記に一覧したものはシステム攻撃に使用されているテクニックで、これらはシステムの可用性や信頼性を損ない、データの破壊や、知的所有権を侵害します。

セッションの盗聴

ユーザ・セッションは、比較的単純な装置やソフトウェアを使うだけで盗聴することができ、キーストローク、データ、ログイン情報を含めた、すべての関連情報が記録されてしまいます。この手口はオリジナルの情報をそのまま入手できるだけでなく、データの転送までの応答時間もかかりません。盗聴を仕掛けられる被害者は、いつから自分の行為が筒抜けになっているかも気付かないまま、ごく普通に仕事をしているだけで、未知のアタッカーに自ら情報を提供することになってしまいます。

パスワードの盗難

通常使用される telnet、ftp、rlogin などの多くのネットワーク・コマンドでは、ログイン・プロセスの一環として、パスワードを暗号化しないまま平文で遠隔ホストへ送信しています。こうしたログイン情報は容易に読み取ることができるので、コンピューティング資源への不正アクセスに利用される危険性があります。また、トロイの木馬形式のコンピュータ・ウイルスの中には、いわゆるキーストローク・ロガーというものが存在し、これを使うと感染先のパスワード情報を不正に入手することができます。その他には、非常にローテクな方法ですが、メモ用紙などに控えてあるパスワードを盗み出すというのもよく使われている手口です。

信頼関係の悪用

アタッカーの中には、信頼関係を逆手にとって、ARP スプーフィングという手法を用いて他のシステムを装い、目的とするシステムへの侵入を果たす者も存在します。こうした攻撃を受ける可能性があるのは、.rhosts ファイルに登録されている信頼されたノードです。攻撃を仕掛ける側のシステムから送信されてくるパケットに、正規のハードウェアの偽造アドレスが付けられていると、その発信元が本物の信頼されたシステムであると信じ込んでしまいます。rsh、rlogin、rcp などのユーティリティやアプリケーションは、ネットワーク外からの接続に対して、その IP アドレスをチェックして .rhosts ファイルに登録されているアドレスに一致するものがあるかのマッチングを行います。この方式は、本質的にセキュリティ面での欠陥を抱えており、.rhosts ファイルに登録されたホストを攻撃の危険にさらしています。

情報の流出

ネットワークを流れる情報は、本質的に無防備な状態に置かれています。そのため、認証化や暗号化などの適切なセキュリティを施さない限り、自分に関するデータが第三者に読み取られていないと保証することはできません。この場合に重要な点は、セグメント化を施して、ビジネス・パートナーやサプライヤなどの様々な発信元から送られてくる情報を防護することです。

ホスト・スプーフィング

あるホストが、ネットワーク上にある別のマシンになりすまし、システム全体をだますという手口があります。こうなると、誤ったシステムに対してデータが送信されたり、スプーフィングしたホストで改竄されたデータが他のシステムに流されるなど、正常なデータの流れが妨げられる危険性が生じます。このもたらす結果は、重大です。たとえば、意図せぬうちにユーザの名前やパスワードあるいはクレジット・カード情報などが送信されたり、発注情報が誤った宛先に送られたり、電子メールその他のデータが間違っただホストに配信される事態などが想定されます。

セッションのハイジャック

TCP セッションのハイジャックとは、2 つのマシン間での TCP セッションを何者かが乗っ取ることです。認証されていないユーザであっても、TCP ストリームを他のマシンにリダイレクトすることで、ログインやワンタイム・パスワードなどによる防護をバイパスしたり、Kerberos などの認証システムをかいくぐることができます。多くの認証システムは TCP セッションの開始時に実施されるだけであるため、ハッカーはこの点についてマシンにアクセスしてきます。接続先のパスに TCP パケット・スニッファやジェネレータを設置するなどが、こうした TCP 接続の脆弱性をついた手口です。

ネットワーク・サービスの無防備

LDAP、NFS、lpd、syslog など多くのネットワーク・サービスには防護が施されていないため、煩雑な設定によるセキュリティを講じる必要があります。たとえば、正確なシステム・ログ・ファイルを維持するに当たっては、シスログ・トラフィックの完全性を保つことが必須です。ところが、こうしたサービスへのセキュリティ保護に要する作業が複雑なものでありすぎると、セキュリティ設定そのものを誤る可能性が高くなり、攻撃に対する防壁として実際には機能していない、というケースも見られます。

反射攻撃

反射攻撃とは、本物のパケットのコピーを入手することで、目的とする侵入先にアクセスする手口です。こうした認証パケットのコピーが流されてしまうと、様々な方法でサービスが妨害される危険性があります。たとえばアタッカーの使う手法としては、「`rm -rf /`」コマンドを含むパケットの再送信などがあります。

第 3 章

IPsec による防護 - 概要

IPsec は、強力かつ広域的なセキュリティを施すために用いられている、ネットワーク層のプロトコルの 1 つです。これは、標準に準拠した暗号化および認証化の機構を利用して、ネットワーク・トラフィックにおけるプライバシーの保護、各種の脅威に対する防衛、ホスト・アクセスの制御を提供するものです。

IPsec による暗号化と認証化は、トランスポート層よりも下層のネットワーク層で実施されるため、電子メール、ファイル転送、Web アクセスなど、すべてのネットワーク・アプリケーションに対して透過的です。IPsec はエンド・ユーザに対しても透過的であるため、ユーザに対するセキュリティ機構についての講習や、ユーザ別の鍵管理情報の発行、脱退ユーザに対する鍵 (キー) の無効化などの処理は不要です。

IPsec では、個々のユーザ別にセキュリティを提供することも可能です。この特性は、オフサイトで働く従業員や遠隔地にあるオフィスを利用する場合に有用です。またインターネット上でのセキュリティ保護された通信リンクの確立には、仮想プライベート・ネットワーク (VPN) が用いられます。

IPsec セキュリティの中核を成すものは、2 つのネットワーク・パケット・プロトコルであり、これにより広範なセキュリティ・オプションが提供されています。

- 認証ヘッダ (*Authentication Header: AH*): これは新規に採用された IP ヘッダで、IP データグラムへのデータ認証、部分シーケンスの完全性 (再送保護)、高度の完全性を提供します。AH が挿入される位置は、IP ヘッダとトランスポート・ヘッダの間になります。またトンネルを利用している場合は、トランスポート・ヘッダとして、TCP、UDP、

ICMP、その他の IP ヘッダを使用できます。ただし AH は、盗聴に対する防御をするものではないため、データをのぞき見される危険性は依然として残されています。

- IP 暗号ペイロード (*Encapsulating Security Payload: ESP*) ヘッダ : これはデータの秘匿化 (暗号化) および、トラフィック分析の防止手段を提供するものです。後者は、特定のエンティティ間を流れるトラフィックについて、そのアイデンティティ、頻度、通信量を不正に解析しようとする盗聴者に対する防御手段の 1 つです。ESP ヘッダはまた、コネクションレスな完全性、データ自体の認証、再送保護など、AH と同様な防御も提供します。なお、ESP ヘッダの認証サービスは、オプションです。

ESP と AH は、1 つのデータグラム上で併用することが可能です。ESP はデータのカプセル化を行います。防護できる対象は、適用開始以後のデータグラム内のデータだけです。TCP パケットの場合、ESP がカプセル化するものは、TCP ヘッダとデータのみです。パケットが IP-in-IP データグラムのものであれば、ESP は内部の IP データグラムを保護します。ソケット単位による自己カプセル化が可能であるため、必要な場合に ESP は、IP オプションのカプセル化を行います。AH とは異なり ESP では、複数の方法でデータグラムの防護を施すことができますが、これは 1 つの方法しか使えないとデータグラムが攻撃にもろくなるためです。たとえば、ESP を秘匿性の維持だけに使用していると、データグラムは、反射攻撃やカット & ペースト攻撃に対しては無防備なままとなってしまいます。同様に、ESP を使用して完全性の確保だけをしていても、盗聴に対する防御にはならず、ある意味 AH よりも脆弱な防護しか施していないことになります。

「トンネル・モード」というのは、IPsec ヘッダによる防御の範囲内にデータグラム全体が収まってはいるが、IP ヘッダには防御がされていない状況を指します。多くの場合、外部にある IP ヘッダの発信元と着信先アドレスは、内部の (防護された) IP ヘッダのものとは異なっています。オリジナルのアドレスが復元されるのは、宛先ホストがパケットを復号化する時です。ESP では通常、このトンネル・モードが利用されています。

「トランスポート・モード」でのデータグラムは、オリジナルの発信元と着信先アドレスには何も手を加えず、データ部 (ペイロード) のみを暗号化します。これが利用されるのは、ファイアウォールの後方や、トランスポート・モードが有効なプライベート LAN です。トンネル・モードに比べて必要な処理が少ない分だけ、スループットの向上が期待できます。

以降の節では、Solaris 9 OE への IPsec の実装に関して、より詳細な解説を行います。

セキュリティ・アソシエーション

IPsec では、セキュリティ・アソシエーション (SA) を用いることで、様々なタイプのデータ・トラフィックごとに提供するセキュリティ・サービスを差別化することが可能です。SA とは通信当事者間での合意事項のことで、IPsec プロトコル、プロトコルのオペレーション・モード (トンネルないしトランスポート・モード)、暗号化のアルゴリズムと鍵、鍵の有効期間、ポリシー・ステートメントなどがこれに該当します。SA は 1 方向にしか使えないので、インバウンドとアウトバウンド・トラフィックで個別に SA を用いる必要があります。

SA を用いる場合、防護の適用範囲が非常に大きく変動してきます。たとえば 1 つの SA で 2 つのホストやネットワーク間のすべての通信を防護することも、特定の種類のトラフィックのみや、アプリケーション固有のセッションだけを防護することもでき、また、

その他のレベルでの防護をすることも可能です。IPsec による防護のレベルとタイプ、およびこうした防護を実施するための鍵強度は、柔軟な設定が行えます。

自動による鍵管理

SA のネゴシエーションは、Internet Key Exchange (IKE) を用いて通信当事者間で行われます。Solaris 9 OE による IPsec の実装では、SA の鍵に関するオンデマンドのネゴシエーションを可能にする、IKE 機構が用いられています。これは、常にその構成が変化し続ける巨大な分散環境での鍵の使用をサポートするものです。また小規模なシステムでは、鍵管理を手動で進めるのが好ましい場合もあり、そうした環境では、システム管理者が手動操作で個々のシステムに対する必要な鍵設定を行えます。

IKE プロトコルは、AH と ESP の利用する暗号化アルゴリズムの選択に関するネゴシエーションに使用され、必要な鍵の準備を整えます。IKE はまた、Solaris 9 OE での IPsec の鍵管理も行います。

プライベート・ネットワークでの通信

IPsec の実装では、通信のプライバシを防護するためにネットワーク・トラフィックを暗号化するよう構成することもできます。IPsec の導入に際しては柔軟な設定が可能で、SA の指定により、ホストやサービスごとに利用する暗号化アルゴリズムを変更することが可能です。Solaris 9 の IPsec で利用される暗号化の機構には、下記のものがあります。

- *Data Encryption Standard (DES)*: これは RFC 2405 の Cipher-Block Chaining (CBC) を利用するものです。実質的な鍵長は 56 ビット (8 つのパリティ・ビットを含めると 64 ビット) で、64 ビットのブロック・サイズを使用します。
- *Triple DES (3DES)*: これは RFC 2451 の CBC を利用するものです。3DES は、3 つの異なる鍵を用いて DES を 3 回行うもので、実質的に DES の鍵長を倍化したことに相当します。鍵のサイズは 192 ビットで、64 ビットのブロック・サイズを使用します。
- *Advanced Encryption Standard (AES)*: これは RFC 2451 の CBC を利用するものです。鍵のサイズは、128、192、256 ビットに設定可能です。鍵長は、サイファー・ブロックごとに実行するラウンド数に影響するので、最終的にはアルゴリズムの実行速度に影響してきます。ブロック・サイズは 128 ビットです。
- *Blowfish*: これは RFC 2451 の CBC を利用するものです。鍵サイズは、32 から 448 ビットの間で可変します。鍵は内部的に、448 ビットに符号化がされます。なお短いサイズの鍵の場合は、448 ビットに達するまでパターンが繰り返されます。ブロック・サイズは 64 ビットです。

仮想プライベート・ネットワーク (VPN)

Solaris 9 の IPsec では、発信元と着信先アドレスを隠すために、トンネルと呼ばれる機能で暗号化を行えます。トンネル・モードは、トラフィック分析を防止するためのものです。この機能は、発信元と着信先の IP アドレスに関する情報を隠すことができるため、VPN 用の媒体としてインターネットなどのパブリック・ネットワークを利用する際に有用です。トンネル・モードは、ネットワーク上のマルチ・ホストに対する防護策として使うことができます。

トンネル・モードの場合、パケット・ヘッダの情報とデータは、新規に採用された IP パケット内にカプセル化されます。発信元でパケットを暗号化する際には、パケットの発信

元アドレスをトンネル・アドレスに置き換えると同時に、パケットの着信先アドレスもトンネル・アドレスに置き換えます。受信先でパケットを復号化する際には、それぞれのオリジナル・アドレスが復元されます。VPN については、次の節でも解説します。

強力なホスト認証機能

Solaris OE の IPsec の特長の 1 つに、ホストその他のネットワーク・アイデンティティを確実に検証するための、強力なホスト認証機能があります。これは標準に準拠した認証機構で、運用組織の内部と外部の双方におけるすべてのコンポーネント間において、優れた相互運用性を確立できます。

認証のアルゴリズムでは、データおよび鍵に基づいて、ダイジェストないしチェックサムによる完全性のチェックを行います。Solaris OE の IPsec では、下記の 2 つの認証機構が使われています。

- *HMAC-MD5*: これは、RFC 2104 の HMAC テクニックおよび MD5 メッセージ・ダイジェスト・アルゴリズムを利用するものです。ここでは、128 ビットの鍵および、96 ビットのダイジェスト (128 ビットから切り捨て) が使用されます。
- *HMAC-SHA-1*: これは、RFC 2104 で公表された HMAC テクニックおよび SHA-1 ハッシュ・アルゴリズムを利用するものです。これは HMAC-MD5 よりも安全なもので、ここでは、160 ビットの鍵および、96 ビットのダイジェスト (160 ビットから切り捨て) が使用されます。

通信の完全性

Solaris OE の IPsec には、転送中のネットワーク・トラフィックに対する改竄防止用の機能が用意されています。これは、トラフィックが送信時そのままの状態を受信され、途中で複製などを盗み取られないことを保証するための一環です。この機能について特筆しておく点は、セッション・トラフィックに対して何らの追加も削除も行われなことです。完全性の検証においては、Message Authentication Code (MAC) を利用します。MAC による検証では、まず格納されたデータグラム全体と AH を対象とした演算を実施します。そして送信先での IP パケットの受信時にも、先と同じ鍵を用いて、同様の計算を繰り返します。この両者の値が等しければ、本物のパケットであると見なされます。

MAC の値はまた、反射攻撃の防止にも利用されます。

通信の防御

IPsec は、TCP、UDP、ICMP プロトコルなどすべての IP トラフィックに対する防護を施します。こうした IPsec による防護は IP レイヤーで展開されるため、あらゆるタイプのインターネット・トラフィックが防御の対象となります。こうした防護は、ネットワークを利用するアプリケーションおよびサービスに対して透過的に実施されます。

アプリケーションの防御

Solaris 9 OE の IPsec は、アプリケーションおよびサービスに対して防護を施すことができます。たとえば Web サービスを処理するホストの場合、SA の設定により、Web クライアントからのリクエストを除いたすべてのパケットを拒否させることが可能です。同様にして、人的資源のデータベースを運用するホストの場合、事前に指定した IP アドレスからのトラフィックのみを受け入れるよう設定し、より厳格な認証機構を準備することが可能です。また、アプリケーションで機密性の高いデータを利用するのであれば、たとえ

ローカル LAN 上で利用するのであっても、すべてのトラフィックを暗号化することもできます。IPsec によるセキュリティ機能は、運用組織全体および、その外部までもカバーするものであり、非常に柔軟性の高い設定が可能です。

IPv4/IPv6 プロトコル

IKE のサポート・プロトコルが IPv4 であるのに対し、IPsec では IPv4 および IPv6 の両プロトコルをサポートしています。IPsec は、IPv6 において欠かせない存在であると同時に、IPv4 および IPv6 の両ネットワークのデータグラムに対して防御を施せます。たとえば IPv6-in-IPv4 トンネルでは、IPv6 パケットを IPv4 パケット内にカプセル化することが可能です。

ホストやルータを IPv6 をサポートするようにアップグレードする場合、IPv4 のみをサポートするノード (ホストとルータ) 付きネットワーク上で、これらを相互運用する必要があります。Solaris 9 OE の場合、ユーザによる IPv4 から IPv6 への移行をサポートするためのツールが用意されています。また RFC 1933 からは、こうした移行を行う際に発生しうる問題点について、詳細なソリューションが提供されています。追加情報については、Solaris のシステム管理 (IP サービス) を参照してください。

第 4 章

仮想プライベート・ ネットワーク (VPN)

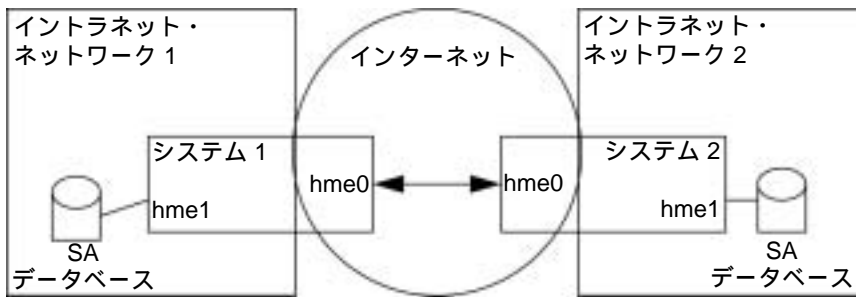
VPN は、パブリック・ネットワークで接続された複数のサイト間での安全な通信を提供するためのものです。VPN 上にあるノード間のトラフィックはすべて暗号化され、パブリック・ネットワーク上にある他のノードからのトラフィックは遮断されます。IPsec に用意された、認証、暗号、ポリシー施行の各機能は、遠隔オフィスやモバイル・ユーザとの接続や、内部ネットワークや資源の分離を行う VPN の構築に最適なものです。

遠隔サイトの防御

遠隔サイトと本社に置かれたビジネス・クリティカル・アプリケーションなどの IT 資源とを接続するに当たって、VPN は費用効率に優れた方法です。通信接続業者に高額を支払って専用回線を確保する代わりに、VPN では、比較的安価なハードウェアやソフトウェア・コンポーネントを利用することで、インターネット上にセキュリティ保護された通信を実現します。VPN は、Solaris の IPsec 環境が持つ柔軟性を活用することができ、各種のセキュリティ・オプションを使えるよう設定することもできます。

セキュリティ面での要請によっては、VPN にセキュリティ・ゲートウェイ以上のものを必要とする場合もあります (ファイアウォールおよびその他のアクセス・ポイントによる、ネットワークのアクセス制御)。通常のファイアウォールはトラフィックに対する認証を行うものであり、IPsec が持つ一連の認証およびセキュリティ・ポリシー機能などは装備されていません。

図 4-1: VPN を利用した企業の支社と本社との接続



典型的なシナリオの 1 つは、エンド・ツー・エンドな認証と暗号を行うことです。この方式の利点は、データ・トラフィックに高度なプライバシー保護を掛けることができ、スプーフィングの危険性を最小限に抑えることができることです。

図 4-1 は、企業の支社が本社とどのように接続するかの 1 つのシナリオです。

- 本社 (ネットワーク 1) のホストは支社のホストとの間で、SA についてネゴシエーションを行う。
- (ネットワーク 2)。
- SA は、必要なセキュリティ・サービス (たとえば、AH ないし ESP パケット・ヘッダ) を用いて、これらのサービスのオペレーション・モード、必要な認証および暗号化アルゴリズムを特定する。
- IKE プロトコルは、必要な認証鍵を生成して、交信するホスト上に配置する。
- 個々のホストの間を流れるパケットは、セキュリティ・ゲートウェイにて、受信先のセキュリティ・ポリシー・データベースとの比較が行われ、受け入れるかどうかの判定がされる。
- パケットを受け入れる場合、セキュリティ・ゲートウェイは、適切な SA の受信先を、SA データベースに問い合わせる。
- パケットの認証は、SA の指定するアルゴリズムを用いて行われる。
- 認証された場合、パケットは宛先ホストに送信される。
- 宛先ホストはパケットを受信すると、SA データベースに問い合わせることで、SA がパケットに適したものを検証する。
- パケットは、転送中に改竄を受けていないことを確認するための認証を受ける。
- 認証された場合、宛先ホストはパケットを受け取り、トラフィック用にネゴシエーションした SA を基に必要な処理を施す。

モバイル・ユーザの防御

モバイル・ユーザの通信環境に防護を施すには、各種の困難が伴います。しかし Solaris OE の IPsec 機能を使えば、ファイアウォールの外側からアクセスしてくる個別な接続に対して、これらをセキュリティ保護するソリューションを提供できます。

現在最も安全なセキュリティ・ソリューションを提供できるのは、Public Key Infrastructure (PKI) です。クライアントに対してはデジタル証明書が発行され、企業ネットワーク上のセキュリティ・ゲートウェイについては、認識された CA から発行される有効な証明書を持つクライアントにのみアクセスを許可するよう設定できます。

ネットワーク資源の分離と防御

Solaris IPsec は、ネットワーク資源の分離と防御に利用することもできます。たとえば Web サーバのセキュリティを保護するには、IPsec を使ってすべての流入するトラフィックをチェックし、この Web サーバ用の DNS クライアントおよび Web クライアントからのリクエストのみを通すようにします。管理用トラフィックなど、その他すべてのトラフィックについては、SA の指定に基づき、IPsec による暗号化と認証を必要とするようにできます。このようにして Web サーバは、多くの一般利用者に対しては開放されたまま、故意ないし事故による有害な操作から防護されます。

IT インフラを運用する企業であれば、その他の中枢機能に対しても、これと同様のコンセプトが適用できるでしょう。そうしたものの 1 つとして内部ネットワークに対する防護は、様々なレベルでの実施が考えられます。また VPN についても、それが高度なセキュリティ保護されたものであれば、アクセスおよびトラフィックの両面から防護が施されているため、認証ユーザ以外の目には「不可視」な存在となるはずですが、これよりも劣るセキュリティしか有さない場合は、トラフィックの暗号化が、より強力な認証システムを必要とするはずですが、そして IPsec プロトコルは、非常に広範な適用範囲を有しています。たとえば、ユーザのリクエストに対してネットワーク・ホストが行う一連の認証手続きについては、内部 LAN からのアクセス時と出先機関からのアクセス時とで異なる方式を適用したい、という状況も考えられます。このような場合は SA を利用することで、ファイアウォール内部のユーザに対しては、暗号化しない平文による通信環境を用意し、ファイアウォール外部のユーザに対しては、すべてのトラフィックを暗号化する、という通信環境を提供できます。これらの機能は、ユーザやアプリケーションに対して透過的なものにするのが可能です。

第 5 章

エンド・システム

Solaris 9 OE に IPsec を実装することで、エンタープライズ IT 環境に対するプラットフォーム・ベースのセキュリティ・ソリューションを提供することができます。IPsec の機能は、単に VPN を提供するだけに止まるものではなく、ネットワーク全体にきめ細かな防護を施すことも可能です。下記の例は、多くの組織に当てはまるシナリオです。

個別のサービスに対する防御

IPsec は、ネットワーク・トラフィックにオーバーヘッドを発生させることなく、特定のサービスに対する防護を施すことができます。特定のサービスを保護するに当たっては、秘匿性や完全性を利用することになります。たとえば、運用組織のセキュリティ・ポリシーでは、正確なログを記録するためにシスログ用のトラフィックを認証化する必要が生じることもあります。IPsec には、すべてのトラフィックの中からこうした UDP サービスに対してのみ防護を施す機能があり、システムの容量やパフォーマンスを圧迫することはありません。

簡単なパケット・フィルタリング

IPsec のポリシー・ファイルでは、ユーザやホストの未使用サービスへのトラフィックをブロックしたり、特定のホストからのトラフィックを拒否するよう設定できます。ただし IPsec はファイアウォールとは異なり、たとえばステートフルなパケットの検査や、プロキシ・サービスなどは行いません。IPsec が行うのは、ホスト・レベルでのアクセス制御です。また流入および流出するトラフィックの双方に対して、特定のルールを適用することも可能です。これらのルールでは、アクセスの許可や禁止および、特定の認証化や暗号化に対する要請が適用できます。なお名前付きポートに宛てられたトラフィックについては、こうしたルールの適用外にすることも可能です。

強化型システム

Solaris Security Toolkit には、Solaris OE システムの最小化、強化、防護をするための機構が用意されています。Solaris 9 OE に IPsec を実装することでシステム管理者は、オペレーティング環境のみならずネットワーク・レイヤーに対する強化を、より簡単に施せるようになります。IPsec によるセキュリティ機能を最大限に享受できる対象としては、Web サーバ、Solaris 管理サーバ、その他のビジネス・クリティカルなサーバなどが挙げられます。

ネットワークの管理

多くの管理用サブシステムは、複数のネットワークに分かれて配置されています。IPsec を利用することでシステム管理者は、ハードウェアを追加することなく、管理用の VPN を構築できます。IPsec は、複数のサーバのより効率的な管理を可能にします。

バックアップ・ネットワーク

バックアップ・ネットワークは通常、パフォーマンス的な要求から用いられるもので、保守トラフィックによる稼働ネットワークの圧迫を避けることを目的としています。これらのネットワーク上では、IPsec のプロトコルを利用した秘匿性と完全性の確保が可能で、機密性が高く重要なデータを含んだこうしたトラフィックを不正な利用や変更から防御します。

ストレージ・ネットワーク

IPsec の典型的な使われ方の一つとしてストレージ・ネットワークでの使用があります。データ保護の実装においては、セキュリティ保護された RPC を用いますが、その設定は複雑なものとなる場合があります。IPsec は、このタイプのネットワークに適しています。この場合、ユーザ・レベルでの認証を行うことなく、ホスト・レベルでの防護を施すことが可能です。

鍵管理

Solaris 9 OE における鍵管理は、IKE 機構の機能を用いて実行されます。IKE は、IPsec SA の間でネゴシエーションを行って、ユーザとサービスの認証および、特定の SA ポリシー・ルールに従う際に必要な鍵の判定をします。このネゴシエーションは、自動的に実行されるため、コスト面で不利となる手動操作は不要です。

IKE デーモンが遠隔ホストの公開暗号鍵を検出すると、遠隔ホストに宛てられたメッセージで、この検出された公開鍵を所有するものは、ローカル・システムで暗号化できるようになります。

IKE デーモンは、鍵を作成するための乱数シードに、Solaris OE の擬似乱数発生関数 (pseudo random number generator: PRNG) を利用しています。また IKE からは Perfect Forward Secrecy (PFS) が提供されます。これは、データ転送防護用の鍵を使って他の鍵を作成されることがないこと、および、データ転送用の鍵の作成に用いた乱数シードは再使用されないことを意味します。

IKE では、下記のコンポーネントと機能が利用されています。

ホスト鍵の管理

IPsec による自動鍵管理は、ISAKMP/Oakley と呼ばれる 2 つのプロトコルにより実行されています。

- *Internet Security Association and Key Management Protocol (ISAKMP)*: これは、ペイロード・フォーマット、鍵交換プロトコルの実装機構、セキュリティ・アソシエーションのネゴシエーションなど、インターネット・鍵管理用のフレームワークを提供するものです。
- *Oakley Key Determination Protocol*: これは、Diffie-Hellman アルゴリズムをベースにセキュリティ面を強化した鍵交換プロトコルです。Diffie-Hellman そのものは、鍵交換を行っている 2 つのエンティティに対する認証をするものではないため、Oakley 機構には認証システムが追加装備されています。

公開鍵インフラストラクチャ (**Public Key Infrastructure: PKI**)

PKI は、X.509 証明書の作成、配布、破棄、管理に必要なポリシーとコンポーネントから構成されています。これは公開鍵暗号に用いる公開鍵を発行するシステムです。PKI を利用することでユーザは、他のユーザやアプリケーションとの情報交換、アイデンティティや鍵の入手と検証、信頼できる第三者機関への登録を行えるようになります。

PKI に含まれるコンポーネントには次のものがあります。

- *Certificate Authority (CA)*: 一連のサブジェクトに対する証明書の発行と破棄を行い、それらの認証責任を負うシステム。CA は、証明書に対する署名と発行を行う前に、そのステータスを監視します。たとえば、証明書には有効期限が付けられていますが、それを CA はチェックし、期限切れとなっているものは破棄します。
- *Registration Authority (RA)*: アイデンティティと登録情報を検証。
- *Public Key Certificate Directory*: 公開鍵の証明書情報を格納。
- *Certification Revocation List (CRL)*: 破棄された証明書を記録しておくためのディレクトリ。CRL は CA により作成されるもので、有効期間内に破棄されたシリアル番号を信頼しないよう、該当するものを記録しておきます。たとえば、証明書の承認期限が切れると、その信頼性が失われるか、対象を証明できなくなるため、これらは廃棄されて CRL に格納されます。
- *Repository*: 証明書および CRL を格納するデータベース。

その他にも PKI には、CA の諸機能が利用する管理プロトコルも規定しています。これらのプロトコルとしては、PKIX Certificate Management Protocol (CMP)、Certificate Management Message Format (CMMF) などのメッセージ・フォーマット、Public Key Cryptography Standards (PKCS) が該当します。

PKI にはまたポリシーおよびガイドラインがあり、証明書の用途を規定するルール、技術および管理面でのセキュリティ制御、CA 契約要求事項、加入者の登録と解除処理などを定めています。

鍵の作成と配布

IKE による 2 つのエンティティ間の接続に対するネゴシエーションが成功すると、Diffie-Hellman アルゴリズムを用いて、鍵の作成と交換が行われます。この 2 つのエンティティは公開鍵を交換する際に、個々の秘密鍵を付けておきます。2 つの処理結果は同一となるはずのものであり、これらのエンティティがセキュリティを確保しながら機密情報を共有する際には、パブリック・ネットワークが用いられます。これが機能するのは、当事者である両者だけが秘密鍵を知っているからです。共有する機密情報は、その他の情報とともに

に、鍵付きハッシュ・アルゴリズムで処理されます。このハッシュの結果は、両者間の通信を暗号化する際の秘密鍵として用いられます。

Solaris 9 OE の新機能の 1 つに擬似乱数発生関数があります。暗号化のアルゴリズムやプロトコルでは、ランダムなビット情報を発生するためにエントロピを必要とします。暗号化処理に用いられるエントロピ・コレクションとは、ランダムなバイト情報の集合のことです。カーネル PRNG の生成する高度なランダム・バイトを実際に生み出しているものが、`/dev/random` です。`/dev/random` を利用すると、十分な量のエントロピ・プールが得られます。IPsec の暗号化機能では、乱数発生システムの入力に必要なランダム値を、このプールからランダム・バイト列を速やかに引き出すことで賄っています。これが、実質的にパフォーマンスを悪化させることなく、十分にランダムなバイト列が作成できるシステムです。

第 6 章

セキュリティ・ポリシーに関する考察

Solaris 9 OE では、トラフィックへ施す防護を、イントラネットの外部にまで拡張することが可能となっています。これには多数の利点が付随しており、そうしたものとしては、IT インフラ全体のセキュリティに対する、より包括的で均一的な監視と管理などがあります。これはまた、サード・パーティ製の装置類の追加がほとんど必要ないため、コストおよびトレーニングの負担を最小化する方向でも貢献します。ただし、セキュリティ機能の大部分を Solaris 環境に移行させる際には、ポリシーに関連する問題を考察する必要があります。

特殊なポリシー・ステートメント

Solaris OE プラットフォームをネットワーク・ルータとして用いる場合、IT スタッフはネットワーク・トラフィック・ポリシーを再考する必要があります。たとえば慎重な方針をとるのであれば、イントラネットの外部も含めたすべてのセッションに対して、その秘密性を維持するため、可能な場合はトラフィックを暗号化することをハイレベル・ポリシーとして設定することが考えられます。

セキュリティ保護されたネットワーク /VPN の管理

このホワイト・ペーパーでもすでに述べたように、IPsec を使うことで VPN を効率的に構築することが可能で、パブリック・ネットワーク上にセキュリティ保護されたポイント・ツー・ポイントの通信環境を確保できます。VPN を使用する目的は、遠隔サイトとの通信をインターネット経由で行うことにあります。この場合 IT スタッフとしては、内部ネットワークの最外縁部に配置する Solaris システムをどう管理するかについて、その方法を考慮する必要に迫られるでしょう。これらのシステムは、ファイアウォールの一角を成すものではなく、オペレーティング環境の一部として扱われるべき存在だからです。その他に留意しておくべき要素としては、下記のものが挙げられます。

- IT 管理者は、VPN の両端でのインストールをどう扱うかについても考察しなければなりません。最初の鍵交換は慎重に実施しないと、パブリック・ネットワークに漏出してしまいう危険性があります。
- /etc/inet/ipsecinit.conf ファイル、/etc/inet/secret/ipseckeys ファイル、/etc/inet/secret/ike.preshareds ファイル、および、/etc/inet/secret/ike.privatekeys ディレクトリ内のファイル群に対しては、特別な配慮が必要です。これらのファイルを秘匿しておかないと、悪意ある者によりファイル内のデータが書き換えられるだけでなく、ポリシー設定を改竄されたり、鍵情報が読みとられてネットワーク・セッションを盗み出される危険性があります。
- ipsecconf(1M)、ipseckey(1M)、ikeadm(1M)、ikecert(1M) コマンドの使用には注意が必要です。最も安全な操作方法は、コンソールないしは直接接続された TTY (TeleTyper) を利用することです。

サービスの防護面での要請

IPsec の提供するきめ細かな制御を活用するにあたっては、サービス単位でセキュリティ・ポリシーを変更する必要に迫られる場合もあります。ネットワーク・アーキテクチャとセキュリティの責任者にとっては、個々のサービスにどのレベルの防護を施すかを指定できるのが望ましいでしょう。こうしたネットワーク・セキュリティ・ポリシーの指定の例としては、http トラフィックは IPsec/IPsec の制御下に置かないが、すべてのデータベース・トラフィックには承認機構によるプロテクトを講じて秘匿性と完全性を保つようにする、という設定などが考えられます。

暗号化における最低限の要請

IPsec では、秘匿性を確保するために施す暗号化において、各種のレベルが利用できます。暗号化のレベルが低すぎると、データのセキュリティ保護も不十分なものとなる可能性があります。一方で、ある種の暗号化アルゴリズムは多くの計算能力を消費するため、システム・パフォーマンスを悪化させる場合もあります。たとえば、AES や Blowfish などの新しいアルゴリズムに比べると、DES はセキュリティ・レベルが低く処理速度も若干遅くなっています。これに対して AES は、高いセキュリティ・レベルを提供しながらも、それほど多くの計算能力を必要としません。

セキュリティ・ポリシーには、防御レベルと処理速度のトレード・オフを管理する一環として個々のサービスに必要な最低限の防護レベルを指定しておく必要があります。たとえばポリシーには、すべてのビジネス・クリティカルな情報に対しては 3DES 以上の防護を施す、などと指定します。

法的面での要請

暗号化については、国内法その他の法令による規制の対象となっている場合があるので、注意が必要です。IPsec による暗号化をインストールないし設定する際に管理者は、該当する法令に違反している点がないことを確認しなければなりません。

Solaris 9 OE に実装された IPsec では、X.509 デジタル証明書が利用可能です。これらは不正な操作を防止するためのデジタル受領書であり、「否認不可」用の署名データに関する PKCS#7 標準をベースとしています。否認不可とは、データの棄却やトランザクションの拒否を防止することです。これは公開鍵暗号を利用したもので、公開鍵の所有者だけが、ドキュメントに署名したりトランザクションの許可を出せることが保証されているからです。否認不可性は、法的に認知されつつある段階ですが、これらは電子商取引トランザクションにおける信頼関係構築の基礎として位置づけられています。

第7章

まとめ

企業活動における従業員、カスタマ、サプライヤ、パートナー間の意思疎通を進める上で、ネットワークは不可欠な存在となっており、強力かつ柔軟なセキュリティ機能を備えたオペレーティング環境に対する必要性が唱えられています。管理者や開発者は個々の状況からの要請に応える形でネットワーク資源の設計や構成をする必要があり、セキュリティ機能はそうしたソリューションを実現ないし補完するものでなければなりません。IPsec は、各種の機構やプロトコルを活用して、ネットワークを流れるトラフィックや資産を防護します。

Solaris 9 OE に実装される IPsec では、下記の機能を提供できます。

- トランスポートおよびトンネル・モードによる、エンド・ツー・エンドな通信の保全
- 鍵管理の自動化による、導入および管理面での負担の軽減
- ユーザおよびアプリケーションに対する透過性

IPsec の機能は、イントラネット上の様々なポイントで使用可能であると同時に、インターネットを経由した遠隔サイト間の安全な接続にも利用可能です。こうしたイントラネットと遠隔サイトを結ぶ上で、IPsec に装備されたトンネル、強力な認証機能、自動による鍵管理の組み合わせは、理想的な手段といえるでしょう。

IPsec の導入には複雑な作業が伴いますが、こうした作業は段階的に進めることも可能です。IPsec によるネットワーク防護は、各種レベルでの構成が可能で、セキュリティとパフォーマンスの間の良好なバランスを維持することができます。ポリシー設定は、システムに必要とする資源やユーザの操作性に重大な影響を与えうるため、ネットワーク設計者およびシステム管理者が事前に慎重な考慮をしておく必要があります。

IPsec に装備された強力な機能は、ネットワークや IT 資源へのアクセス制御、および情報の防護を施すことを目的としています。これは Solaris 9 OE の一部として機能するものであり、エンド・ツー・エンドな統合セキュリティ・ソリューションを提供します。

Copyright 2002 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

本製品およびそれに関連する文書は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。サン・マイクロシステムズ株式会社による事前の許可なく、本製品および関連する文書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company, Ltd. が独占的にライセンスしている米国ならびに他の国における登録商標です。フォント技術を含む第三者のソフトウェアは、著作権により保護されており、提供者からライセンスを受けているものです

Sun、Sun Microsystems、Enterprise JavaBeans、EJB、Forte、iForce、iPlanet、Java、Java Community Process、JavaServer Pages、JSP、J2EE、および SunTone は、米国およびその他の国における米国 Sun Microsystems, Inc. の商標または登録商標です。

サンのロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャに基づくものです。

OPEN LOOK および Sun Graphical User Interface は、米国 Sun Microsystems Inc. が自社のユーザおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems Inc. は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザ・インタフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems Inc. は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは米国 Sun Microsystems Inc. のライセンス実施権者にも適用されます

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われないものとします。



Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA Phone 800 786-7638 or +1 512 434-1577 Web sun.com



We make the net work.

Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India—Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand—Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China—Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland—German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800

FE1821-0