境界セキュリティの限界とエンドツーエンドセキュリティの必要性

SSH コミュニケーションズ・セキュリティ株式会社
橋本　詩保

歴史から学ぶべきことがあるとすれば、それは最強の防衛でさえも突破され得るということです。中世の石造りの砦は、強力な包囲攻撃兵器により攻略され、またその後には火薬の発明によって制圧されました。19 世紀の南北戦争の巨大な要塞であったサムターおよびプラスキでさえも、より強力な銃器により陥落しました。これらの例やその他の数限りない例から、新たな技術およびこれまで以上に狡猾な敵によって、最も強靭と思われていた防衛線でさえも打破されてしまうことがわかります。

同じことが今日の企業 IT セキュリティにも当てはまります。多くの組織が、脅威は「最前線」で抑えられれば良いと考えています。このため、さまざまな外部の脅威から境界線内のイントラネットを保護すべく、情報セキュリティ製品に何百万ドルもの投資が行われています。これらの外部の脅威としては、ハッカー、電子メールウイルスおよび公共インターネットからもたらされるネットワークワームなどが挙げられます。これらの組織が選択するソリューションは主にファイアウォール、アンチウイルスソリューションおよび仮想プライベートネットワーク（VPN）ですが、信頼されていないインターネットから「信頼されている」イントラネットを保護することに重点が置かれています。

しかし現実には、境界線は繰り返し危険にさらされており、企業および政府機関は単に境界線のセキュリティソリューションに依存するだけでは全く不十分であることに気付き始めています。さらに、多くの組織では内部のセキュリティの脅威から身を守るための対策を怠っています。内部の脅威は、より重大かつ悪質な敵となる場合が少なくありません。

エンドツーエンドの通信セキュリティは、企業ネットワークの境界線保護のみに重点を置く今日の企業セキュリティアプローチの限界を打破する新たなアプローチです。エンドツーエンドのセキュリティは、データ通信の開始から終了までを保護し、アプリケーションと IT インフラストラクチャとの間で機能することにより、企業全体のセキュリティソフトウェアおよびセキュリティ ポリシーの双方について一元的な管理を提供し、内部および外部の双方のリスクに対するセキュリティを大幅に改善します。

1. 内なる敵

今日の境界線のセキュリティ防御に対抗するため、ハッカーはさらに巧妙な技術やアプローチを開発しています。代表例として、ポート80経由で内部ネットワークにアクセスすることが挙げられます。内部ネットワークに侵入すると、ハッカーは疑いを持たない内部関係者をだまして境界線の内部に「トロイの木馬」ソフトウェアを仕掛けるウェブサイトを訪問させます。このソフトウェアは機密データを収集してハッカーの元に送信する役割を果たします。また、悪意を持ったあるいは金銭を目的とした内部関係者が顧客情報を持ち出す事件が現実に起こっています。

しかし、これは氷山の一角に過ぎません。今日の真の課題は、内部に存在する IT セキュリティの脅威への対処です。古い時代に、偶然であれ意図的であれ、信頼された内部関係者によって緻密な防衛線内での防御が簡単に打ち破られたのと同様に、IT の防衛線内での防衛も会社の従業員によって打破されるということがあり得ます。

そしてその脅威は、ほとんどの人が考えているよりも大きいのです。Gartnerの調査によると、情報システムへの不正アクセスの70%が社員によるものであり、これらの内部セキュリティ侵害の95%以上が大規模な財務上の損失をもたらしています 。さらに、Computer Security InstituteおよびFBIの調査によると、大規模な組織に対する内部関係者の攻撃により平均270万ドルの損害が生じているのに対し、外部からの攻撃による損害額は平均してわずか5万7,000ドルにとどまっています 。また、金銭的な被害のみならず、顧客情報の漏洩によって企業としての信頼を失うリスクも伴います。

境界線のITセキュリティソリューションのみに依存していては十分ではないことは明白です。社員記録、顧客情報、パスワードやその他の機密データなど、組織に不可欠な情報の大部分は組織のイントラネット全域で無防備な状態で送信されています。多くの場合、悪意のない社員が不注意により組織の内部と外部の双方において同僚に機密情報を漏らしてしまっているケースもあります。機密データを収集するための使いやすいネットワーク・スニッフィング(データ傍受)プログラムは誰でも容易に入手できるため、その動機の如何にかかわらず、初心者でさえもこのような内部攻撃を実行できます。また、P2Pソフトウェアの不注意な使用により本人の気づかないうちに重大な機密情報が漏洩していることもあります。さらに悪いことには、TCP/IPネットワークは本質的に匿名での操作が可能なため、犯人を特定して最終的に捕らえることが極めて困難です。

企業の機密ITデータは内部関係者によってさまざまな形で外部に洩らされます。例えば、以下のような例が挙げられます

- 内部ネットワークへのセキュアでない無線アクセス(WLAN)を行っている際の近隣者による傍受
- 内部LANへの正規のアクセス権を持つ社員で、会社に対して不満を抱いている者や金銭を目的とした者
- 単純なパスワードを使用し、または不注意により機密情報を組織外の人物に漏らす、セキュリティに関する適切な研修を受けていない(悪意のない)社員
- 機密アプリケーションからのログアウトを忘れ、ワークステーションを権限を持たない人物が使用できる状態のままにするユーザ
- インターネットカフェなどの遠隔地からウェブベースのアプリケーションを使用して内部ネットワークにアクセスした後、Webのキャッシュを消去し忘れて、その後に使用するユーザに機密データへのアクセス権を与えてしまうユーザ
- WAP対応の携帯電話またはブルートゥース対応のラップトップ経由で接続された携帯電話を使用して内部ネットワークにアクセスするユーザ
- ウィルスに感染したP2Pソフトウェアによる顧客情報など機密情報の漏洩

新たな技術により、これらのセキュリティの脆弱性が記録的な数で悪用されています。例えば、パスワードの傍受およびIPパケットの隠蔽など、さまざまな攻撃方法を自動化して結合するネットワークワームが出現しており、これらのワームが無防備な内部ネットワークにアクセスできるようになると、相当な損失をもたらす可能性があります。

残念ながら、最近大きく取り上げられている多数のウイルス事件とは異なり、内部セキュリティの侵害はほぼ常に隠れたところで発生しており、一般に知られることはほとんどありません。多くの組織がこのような侵害を公表しない理由としては、不面目となる可能性、長期的な信用の失墜および広報上のマイナス効果などがあります。しかし、こうした事実が広く一般に知られていないために、情報セキュリティベンダおよび組織のIT予算担当者は境界線のセキュリティの強化のみを重視し続けています。

その結果、今日では多くの企業および政府機関において、内部アプリケーションおよびデータレポジトリに企業ネットワーク全体の機密性、データの整合性および強力な認証を提供する、完全なエンドツー

エンドの通信セキュリティソリューションを導入し、既存の境界線のセキュリティを補強するための強いニーズが生まれています。

2. 全体像

内部関係者によるリスク管理には、LANにおけるデータ保護および機密情報への電子的なアクセスの管理などだけではなく、そのほかにも沢山の注意が必要です。機密資料にアクセスするための最も簡単な方法の1つは、これまでと同様に、人をだまして必要な情報を入手することです。このため、すべてのリスクに対する包括的な保護を提供することは、情報セキュリティソリューションのみでは到底不可能です。それよりむしろ、組織におけるリスク管理に不可欠な部分として情報セキュリティを理解すべきです。利用可能な電子セキュリティ技術を組み込むことに加えて、セキュアな組織では人事プロセス、物理的なセキュリティ手法および一般的なセキュリティポリシーなどの分野について検討を行う必要があります。

エンタープライズ・リソース・プラニング(ERP)、顧客関係管理(CRM)および共同設計とワークフローのアプリケーションなど、組織全体で利用するアプリケーションの導入によって、内部ネットワークトラフィックの傍受は、組織の機密情報およびデータに違法にアクセスする上でこれまで以上に効率的な方法になります。その結果、多くの組織ではこれらのすき間を塞ぐためにITセキュリティにより多額の投資を行う必要が生じます。しかし、物理的セキュリティまたはセキュリティ認識に関する社員研修を犠牲にしたITセキュリティ投資は、また別の利己的な利用へとつながります。したがって組織の管理者は、セキュリティの検討にあたっては常に全体的なプロセスを見る必要があります。とは言うものの、全体図の一部としてITセキュリティの改善に重点を置く場合には、対処すべき数多くの重要な要件があります。

3. IT セキュリティ戦略

エンドツーエンドの通信セキュリティシステムが効果を上げるには、単にITの境界線から外の世界のみではなく、ユーザのワークステーションからアプリケーションサーバまでのパス全体でセキュアな通信を提供する必要があります。またこのシステムでは、イントラネット上のコンピュータからだけでなく遠隔地からもインターネット経由で組織ネットワークへのセキュアなアクセスが可能でなければなりません。

ほぼ全ての企業において、エンドツーエンドの通信セキュリティは、可能であればサーバアプリケーションと同じハードウェア上でアプリケーションとネットワークの間で稼動し、アプリケーション自体には何の変更も生じさせないものでなければなりません。この要件は、再プログラミングに多額の費用と時間がかかり、リスクを伴うレガシーアプリケーションにおいて特に重要です。ユーザの認証を行って通信を解読するには、ユーザのワークステーションのクライアントアプリケーションとネットワーク間に、エンドユーザの操作を必要としないクライアントを直接インストールします。互いに離れた場所にある多数のクライアントを管理下に置くには、システムの一元管理が可能である必要があります。

保護されていないアプリケーション通信からのリスクを管理するために技術的な対応策を導入する場合、検討すべき主要なセキュリティサービスは以下の通りです。

- FIPS-140-2認証暗号アルゴリズムを使用して機密情報の傍受を防ぐための通信の機密性保持/暗号化
- 転送中の情報の改ざんを防ぐためのデータ完全性
- アプリケーションへのアクセスを提供する前のユーザIDの確実な検証を容易にするための認証（Authentication）
- ユーザにアクセスを許可する情報を決定するための承認（Authorization）

これらの機能は相互に深く関連しています。例えば、通信が行われる前にユーザIDが検証されなければ、強力なデータ暗号化はほとんど価値がありません。また、通信プロセスの途中で誰でもデータを改ざんできるならば(データ完全性の欠如)、強力な認証は役に立ちません。同様に、ユーザが正しく認証されなければ、強力な承認手続きもほとんど価値がありません。

4. 今日の展望

一般的なIT環境は、サポートインフラストラクチャ(サーバハードウェア、オペレーティングシステム、データベースシステム、ネットワークハードウェアなど)および個別の組織アプリケーション(ERP、CRM、SCMなど)により構成されています。この環境においてセキュアな通信をどこでどのように導入するかに関する決定は、IT部門が効果的なエンドツーエンドの通信セキュリティを維持しながら、組織の主要な事業目標の達成に貢献できるかにも左右されます。

既存のセキュリティソリューションは多くの場合、ITインフラストラクチャまたは実際のビジネスアプリケーション自体が持つセキュリティ機能に基づいています。これらのアプローチのいずれも、実用的で費用効果の高いエンドツーエンドのアプリケーションまたはデータセキュリティの効果的な導入には適しておらず、しばしばその価値よりも多くの問題を引き起こします。

ITインフラストラクチャにセキュリティを統合するには、個々のサーバ専用のセキュリティハードウェアの配置など、複雑で費用のかかる技術的努力が必要となります。これらのアプローチはアプリケーションおよびデータを直接保護しないため、高価で柔軟性に欠ける傾向があり、悪意のある個人が悪用できる「バックドア」の脆弱性を残すことが少なくありません。

一方、既存の組織アプリケーションに暗号化および認証機能を埋め込むには、個々のアプリケーションでコードの修正が必要になります。専用の基幹アプリケーションに多額の投資を行っている大規模な組織では使用中のアプリケーションの数と種類が多いため、この選択肢はほとんど実行不可能です。予測される大きな問題としては、例えば、既存のアプリケーションコードの修正に要する多額の費用、エンドユーザに対する透過性の欠如、アプリケーションの相互運用性に関する課題およびアプリケーションパフォーマンスの低下が挙げられます。

5. 兵器庫の建設および管理

エンドツーエンドの通信セキュリティは、ネットワークおよびアプリケーションサーバ間の強力な認証および暗号化機能を備えたセキュリティソフトウェアの採用により、より優れたアプローチを提供します。アプリケーション自体を変更したり性能の低下をもたらすことなく、透過的にアプリケーションを保護するこのソフトウェアは、各基幹アプリケーションのフロントエンドとして機能し、ビジネスアプリケーションおよびデータへのクライアントのアクセスを制御します。ビジネスアプリケーションにアクセスする各ユーザ(または他のアプリケーション)は、サーバに対してクライアントを認証する小規模なセキュリティクライアントを持ち、メッセージやデータを相互にやり取りするためのセキュアなパイプラインを確立します。

このアプローチに使用されるセキュリティ技術は新しいものではありません。例えば、Secure Shellなどのポイントソリューションは、効果的で使いやすいクライアント/サーバセキュリティを提供し、内部および外部の包括的な保護のための理想的なソリューションとなり得ます。しかし課題となるのは、中規模から大規模な組織の場合はいずれも、何百ものアプリケーションサーバおよび何千、何万ものクライアントが存在する可能性があることです。これほど多数のセキュリティフロントエンドおよびセキュリティクライアントの管理は、物理的に不可能でないとしても、

短期間に極めて多額の費用が必要になります。

このため、大規模な組織が管理可能なセキュリティを実現するための鍵は、すべてのセキュリティサーバおよびクライアントを管理するセキュリティマネージャアプリケーションを加えることにあります。この方法により、ユーザ、ポリシーおよびソフトウェアの更新を一元管理し、組織全体に瞬時に適用することができます。

6. セキュリティの敵に対する戦いの遂行

2500年前、ヘラクレイトスは「万物は流転する」と言いました。この言葉は、絶え間なく変化が起こるセキュリティ業界にこそ最もよく当てはまります。

かつては、物理的なセキュリティのほかに必要とされるものはありませんでした。その後、組織が成功する上で情報の重要性が増すにつれて、セキュリティに関する社員教育が重要になりました。インターネットおよび汎用データ通信の出現により、主に境界線のセキュリティの形で電子的なセキュリティが前面に押し出されました。今日、大規模な組織の内部において共同作業の要件のためにより多くの人々が機密情報をこれまでより容易に利用できることから、私たちはセキュリティが組織の内部から危険にさらされるという不安に直面しており、それが最も大きな脅威となっています。今日の複雑な企業ITネットワークを保護するには、もはや境界線のセキュリティのみに頼ることはできません。

このため、組織はエンドツーエンドのアプリケーションおよびデータセキュリティをITインフラストラクチャに今すぐにも加える必要があります。エンドツーエンドの通信セキュリティは、内部および外部の双方のリスクに対するセキュリティを大幅に改善するだけでなく、エンドユーザにほとんど影響を及ぼすことなく既存の企業IT環境と容易かつシームレスに統合できます。このセキュリティは時の試練を経た技術に基づいており、導入、保守および構築が容易で、厳格な監視機能を提供します。これらの要素は、21世紀の企業がネットワークインフラストラクチャおよび貴重なデータを保護する上で必要となる基本的な要素です。

また、ITセキュリティマネージャがポリシーを容易に維持し、組織に関わる何百種類ものアプリケーションおよび何千人ものユーザに更新情報を素早く適用する上で役立つ一元管理機能を合わせて提供します。結局のところ、最高のセキュリティシステムでさえも、極めて順調に稼動している場合にのみ効果を上げるのです。

ハッカー、不満を抱いている社員、コンピュータ犯罪者およびテロリストが、企業、政府または消費者の機密データの強奪を引き続き企てることに疑いの余地はありません。しかし、境界線のセキュリティという焦点を越え、企業IT環境における重要な脆弱性のすき間を塞ぐことにより、エンドツーエンドの通信セキュリティは内部および外部の双方においてセキュリティの敵を打ち破るための強力な武器となります。