WHITE PAPER

symantec™

インスタント・メッセージングのセキュリティ

INSIDE

INSIDE

インスタント・メッセージング（IM）入門
社内における IM のセキュリティ確保
IM 利用時のベスト・プラクティス

目次

はじめに

当初は単なる友人間のチャットサービスとして登場したインスタント・メッセージング(IM)は、何千万人ものインターネット・ユーザに欠かせない通信手段にまで発展しました。インスタント・メッセージング・システムで著名なものには、AOLのインスタント・メッセンジャー、マイクロソフトのMSN Messenger、インターネット・リレー・チャット(IRC)などがあり、友人、知人、同僚との通信手段に変革をもたらしました。以前はデスクトップ上に限られていたインスタント・メッセージング・システムは現在では各種携帯機器や携帯電話でも利用可能になり、事実上どこからでもチャットを楽しむことができるようになりました。IDCによると、2005年にはインスタント・メッセージングの利用者数は企業ユーザの場合は2億人、一般家庭ユーザの場合は3億人を突破すると予想されています。※1

Palm(R)Pilotと同様に、インスタント・メッセージングは米国企業に徐々に浸透してきました。IMシステムは多くのIT部門では支持を獲得していないにもかかわらず、電子メールや電話よりも高速で便利だと感じた従業員の間で急速にその人気を伸ばしています。IMシステムには人々が通信とビジネスを行う方法を根本から変える能力を持っているのにもかかわらず、残念ながら、今日利用可能なIMシステムの多くは、セキュリティ面で幾つかの課題を抱えています。

現在利用されているIMシステムの多くは、セキュリティ面よりもスケーラビリティを重視した仕様になっています。現在フリーウェアとして配布されている事実上全てのIMプログラムでは暗号化機能が欠如しており、またそのほとんどがすべての企業ファイアウォールを迂回する機能を備えているため、インスタント・メッセージングの利用を制御することは困難です。これらのシステムの多くは、パスワード管理が甘く、アカウント詐称やサービス拒否（DoS）攻撃を受けやすい状態になっています。最後に、IMシステムは、急速に感染を拡大するコンピュータ・ワームや複合型脅威の格好の標的になる条件－至る所に存在すること、通信基盤を供給していること、新たな標的を見つけるために利用可能な統合ディレクトリ（メンバリスト）を備えていること、そして多くの場合、作成が容易なスクリプトで制御可能なこと－をすべて満たしています。※2 さらに、インスタント・メッセージングを介して送受信されるデータのウイルス・チェック機能を備えたファイアウォールは現時点では皆無だということが状況をさらに悪化させています。

本書では、インスタント・メッセージング・システムに潜むセキュリティ上のリスクを詳説した後、企業がそのようなシステムを企業環境下でどのように運用してゆくかに関する意思決定をする際に参考となるガイドラインを紹介いたします。

※1 http://www.computerworld.com/softwaretopics/os/windows/story/0,10801,61141,00.html
※2 複合型脅威はウイルスやワームに似た感染拡大技術、ハッキング、サービス拒否技術を組み合わせることでほとんどの場合、人間の手を介さずに急速に感染を拡大します。NimdaやCodeRedなど、最近の複合型脅威はわずか数時間で数百万台に上るコンピュータに感染を広げ、数十万ドルもの被害を与えました。

インスタント・メッセージング入門

インスタント・メッセージングは新技術のように見えますが、実際には古くから存在していました。インスタント・メッセージング・システムの元祖であるIRCは、1998年にJakko Oikarine氏※3が開発したものであり、現在でも多くのユーザの間で即席のディスカッション、チャット、ファイル交換に利用されています。その後、IRCに続き、ICQ、AOL、MSN Messenger、Yahoo Messengerなど、多数のIMシステムが新規にリリースされました。これらのIMシステムの機能には差異がありますが、ピア・ツー・ピア、リアルタイムでのチャット、ファイル転送機能といった基本的なサービス機能は同じです。

インスタント・メッセージングとクライアント / サーバー通信方式

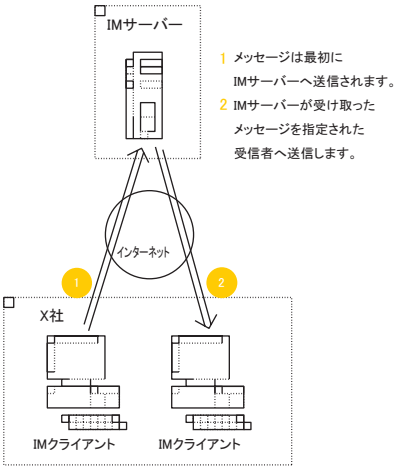

図1. クライアント／サーバー方式のインスタント・メッセージング

事実上すべてのIMシステムは、基本的に同じクライアント/サーバー・アーキテクチャを採用しています。ユーザはインスタント・メッセージング・クライアントを自分のクライアント・マシン－デスクトップ・コンピュータ、無線機器、PDAなどーにインストールします。これらのクライアントは、メッセージング・プロバイダーのインフラストラクチャに設置されている1台のIMサーバーと通信することで、他のユーザの場所を探してメッセージ交換を行います。ほとんどの場合、メッセージが発信側ユーザのコンピュータから直接、受信側ユーザのコンピュータに送信されることはありません。発信されたメッセージはまず、IMサーバーに送信され、その後、IMサーバーから宛先の受信者のコンピュータに送信されます（図1参照）。

大半のクライアント／サーバー型インスタント・メッセージング・システムでは、ユーザ間でやり取りされるデータは外部から簡単に見える状態になっているため、盗聴されやすくなっています。

※3 http://www.irc.org/history_docs/jarkko.html

インスタント・メッセージングとピア・ツー・ピア通信方式

大半のインスタント・メッセージングシステムは全メッセージの送信に中央集中サーバーを使用していますが、システムによってはピア・ツー・ピアのメッセージ通信機能を備えているものもあります。後者の場合、クライアントはまずIMサーバーに他のクライアントを探すようにリクエストを送信します。クライアント・チャット・プログラムが指定されたピアの場所を見つけると、そのピアに直接コンタクトを取ります（図2参照）。

ピア・ツー・ピア通信方式の場合、発信側と受信側両方のユーザが同じローカル・エリア・ネットワーク上にいる時はメッセージはインターネットを経由しないため、クライアント・サーバー・クライアント通信方式の場合よりも安全性が高くなります（図1参照）。しかし、一方のユーザが企業ネットワーク外部に存在する場合は、クライアント・サーバー・クライアント方式の場合と同様、コンピュータ間でやり取りされるメッセージは盗聴される危険が生じます。

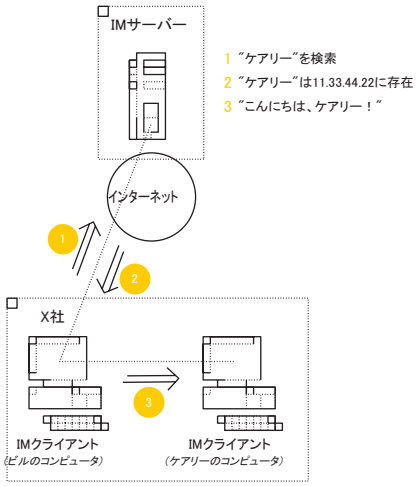

図2. ピア・ツー・ピア方式のインスタント・メッセージング

インスタント・メッセージングと暗号化

今日、メッセージがクライアントからサーバーに送信され、2つ目のクライアントに戻される際にメッセージを暗号化する一般インスタント・メッセージング・システムはほとんど皆無です。このようなデータは、インターネットを通過する途中でも、IMプロバイダーのネットワーク内部からでも外部に見える状態になっている可能性があるため、盗聴されるおそれがあります。また、一般の間で人気のあるIMシステムはピア・ツー・ピア・トラフィックを暗号化しません。図1のように、2人のユーザの席が隣り合わせの場合でも、二者間でやり取りされるメッセージはインターネットを経由するため、秘匿情報が外部に漏洩するおそれがあります。

企業は、インスタント・メッセージの秘匿性の安全度は、公衆メール・サービスを使って社内および社外との電子メールを送信する場合と同程度と考える必要があります。クライアント・サーバー・クライアント通信方式のシステムの場合、2人のユーザ間で発生するトラフィックは暗号化されずにインターネット上を通過するものと考えてください。ピア・ツー・ピア通信方式のシステムの場合でも、一方のクライアントが企業ファイアウォールの外側に存在する場合はすべてのトラフィックが暗号化されずにインターネットを通過することになります。いずれの場合でも、送信されるコンテンツは専用ツールを使用する攻撃者によって傍受される可能性があります。

インスタント・メッセージングとファイル転送

インスタント・メッセージング・システムでは、ユーザ間でメッセージを交換することに加え、ファイル交換を行うことも可能です。現行のシステムは、テキスト・メッセージ転送と同様に、サーバーを経由せずにピア間で直接ファイルを転送します。言い換えると、図2で図解されている技術がファイル転送でも使用されます。このピア・ツー・ピア通信方式は、サーバー中心のファイル転送をプロバイダーのネットワーク上で扱う場合に要求される高帯域の必要性を排除するために使用されています。

現時点では、主流となっているインスタント・メッセージング・システムのうち、クライアント間で転送されるファイルを暗号化するシステムは皆無です。ファイルが直接インスタント・メッセージング・サーバーを経由することはありませんが、インターネット、企業LANまたはWANあるいはその両方を通過する可能性があります。発信側と受信側両方のユーザが同じ会社のネットワーク上に存在する場合、ファイル転送はその会社のネットワーク上にとどまりますが、一方のユーザがネットワーク外部に存在する場合、ファイルは暗号化されずにインターネットを経由して送信されます。

インスタント・メッセージングとスクリプティング

インスタント・メッセージング・プラットフォームの多くは、スクリプティング機能をサポートしており、ユーザはVisual Basic、JavaScript、カスタムのスクリプト・コード、あるいはその他の複雑なプログラムを使用してメッセージング・クライアントの様々な機能を制御できるようになっています。こうした機能は便利ですが、コンピュータ・ワームや複合型脅威の感染拡大を助長するメカニズムにもなっています。このようなスクリプトはインスタント・メッセージング・クライアントに対し、他のユーザへのコンタクト、ファイル送信、設定の変更、悪質な行為の実行など、様々な操作を実行するよう命令することが可能です。この種のセキュリティ関連の問題を取り巻く現状については、次の「インスタント・メッセージングの脆弱性と攻撃」セクションで詳しく説明します。

インスタント・メッセージングとその他の機能

最後に、競争の激しいインスタント・メッセージング市場に対応するために、一部のインスタント・メッセージング企業はメッセージング・クライアントに顧客を獲得するための機能を追加しました。例えば、ICQ には、デスクトップ・コンピュータから小規模の Web サイトを直接実行できるようにする小型の Web サーバーが含まれています。あらゆる Web 対応ソフトウェアと同様、このような機能の存在はサイトがハッキングされ、システムに侵入されるというセキュリティ・リスクを生み出しています。

インスタント・メッセージングの脆弱点と攻撃

このセクションでは、一般的なインスタント・メッセージング・システムで顕著な脆弱性と、その脆弱性を利用する攻撃の種類について解説します。企業をこれらの脅威から守る方法については、後述の「社内におけるインスタント・メッセージングのセキュリティ対策」セクションで紹介します。

盗聴

ほとんどのIMシステムはネットワーク・トラフィックの暗号化を行っていないため、2人のIMユーザ間で行われる会話の内容が、第三者によりパケット盗聴あるいは同様の技術を使って盗聴される可能性があります。前述の通り、この問題はクライアント／サーバー通信方式、ピア・ツー・ピア通信方式のどちらの接続モデルでも発生するおそれがあります。

アカウント・ハイジャック

インスタント・メッセージング・システムの多くは、攻撃者が他人のインスタント・メッセージング用アカウントをハイジャックし、そのユーザになりすまして他のユーザと会話を行うという、アカウント・ハイジャックあるいはアカウント詐称の危険性を秘めています。こうした攻撃を開始するためのツールや方法は現在、多数のWebサイトで紹介されています。

パスワード保護機能はほとんどのインスタント・メッセージング・システムで非常に限定的なものでしかなく、IMシステムによっては、ユーザのパスワードをクライアントのパソコン上にデータファイルとして保管するものもあります。これらのパスワードは暗号化されている場合もありますが、平文として容易に見える状態で保存されているものもあります。現在、某有名IMシステムで採用されているパスワード暗号をクラッキングする方法について詳細に解説しているWebサイトが少なくとも1つ存在することが確認されています。

データへの不正アクセスと改ざん

すべてのインターネット対応ソフトウェアと同様、IMプログラムには攻撃者によってWeb経由で悪用されかねないバグが存在する可能性があります。攻撃者はバッファ・オーバーフローや不正なデータ・パケットなどの攻撃技術を使うことで、脆弱なIMクライアントがインストールされているPCに不正にアクセスする可能性があります。多くのIM製品には大量の補助機能が含まれているため、攻撃を受けるおそれがある領域は大量に存在します。

例えば、2002年5月には、w00w00と呼ばれるハッキング・グループが、某有名インスタント・メッセージング・プログラムのソースコードに脆弱な部分が存在することを突き止めました。その脆弱性は攻撃者によって標的のシステムに対する完全制御を獲得するために悪用され、その後、コンピュータ・ウイルスのインストール、データの盗用あるいは削除、パスワード盗用などの悪事が行われていた可能性があります。幸い、そのIMベンダーはこの事態に迅速に対応し、顧客保護対策として修正プログラムを配布しました。

ワームおよび複合型脅威

インスタント・メッセージング・プラットフォームには、電子メール・システムと同様、ワームや複合型脅威(CodeRedなど）の感染拡大に必要とされる技術が揃っています。

まず第一に、インスタント・メッセージング・ソフトウェアはシステム・ユーザ間で利用可能な通信チャネルを大量に供給します。第二に、事実上すべてのIMソフトウェア製品はユーザが頻繁に連絡を取り合う相手のリスト（メンバリスト）を持っています。電子メールのアドレス帳と同様、メンバリストもIMユーザベースを通じて短時間でワームを広範囲に広げるために利用される可能性があります。最後に、一部のインスタント・メッセージング・システムはスクリプティングあるいはプログラミング可能なため、感染拡大に利用可能なメカニズムを使ってこれらのシステムを標的にした悪意のあるプログラムが作成される可能性があります。

人気インスタント・メッセージング・システムは様々な人々の間で利用されているため、このようなシステムを標的にした複合型脅威は、わずか数時間で何千万台もの個人あるいは企業のコンピュータに広がる恐れがあります。ワームがシステムに侵入すると、データの削除、バックドアのインストール、重要データの持ち出しなどの有害活動を実行するおそれがあります。シマンテックの専門家は、今後10年以内にこの種の攻撃が頻発するようになると予測しています。インターネットへのブロードバンド接続の急成長に伴ない、こうしたセキュリティ上の問題は深刻化する傾向にあります。

複合型脅威およびコンピュータ・ワームがインスタント・メッセージング・システムを使って感染を拡大する方法には、IMのスクリプティング機能を活用する方法と、バッファ・オーバーフローあるいはその他の脆弱性を悪用する方法の計2通りあります。

インスタント・メッセージングのスクリプティング機能を利用する脅威

前述で概説した通り、IMシステムは他のプログラムあるいはスクリプトファイル(Visual BasicやJavaScriptなど）が単純なプログラミング・コマンドを通じてクライアントのIMソフトウェアを制御できるようにするスクリプティング機能をサポートしています。このようなコマンドを活用することで、悪意のあるコードはIMシステムを、自分自身を他のメンバのシステムに送り込んだり、プログラムの設定を変更したり、秘匿情報を盗み出すなど、有害活動を実行するための通信プラットフォームとして利用する可能性があります。従来の電子メール・クライアントにもこれと同様の機能があり、LoveLetterやSirCamなどの悪質なワームによって利用されたことがあります。

IRCを通信プラットフォームとして使用することで繁殖するワームは現に多数実在します。これらのワームはIRCクライアントで有名なソフトウェアが供給しているスクリプティング言語で書かれており、一般に次の形態で動作します。まず、ワームに感染しているコンピュータのユーザがディスカッション・グループに参加し、チャットを開始したとします。その後、同じチャットグループに別の（まだ感染していない）ユーザが参加すると、ワームは新規のユーザを検知し、検知したユーザ全員に自分自身のコピーをスクリプトファイルとして送信します。その場合、受信側のユーザはそのファイルを開くように促されることもあれば、全くの通知なしで受け取る場合もあります。ワームが新たなコンピュータに感染すると、上記と同じサイクルが新たに始まります。

IRCワームに加え、最近になって特定のIMシステムのみを標的にしたWindows(R)ベースのワームが幾つか出現するようになりました。これらのワームはNimda、LoveLetter、SirCamが使用したものと類似したスクリプティング技術を使用し、インスタント・メッセージング・ソフトウェアを介して自分自身をユーザからユーザへ送信することで感染を拡大します。幸い、この経路を使用して感染を拡大したワームは現在のところは皆無です。しかし、これらのワームの出現で、インスタント・メッセージング・プラットフォームがこのような攻撃にもろいことが実証されたのは明らかです。

インスタント・メッセージングの脆弱性を悪用する脅威

Webサーバーのようなインターネット対応ソフトウェア・プラットフォームに存在する脆弱性を悪用することで、ユーザの操作を介さずに感染を広げる複合型脅威を作成可能であることがCodeRedやNimdaの出現で実証されました。今後は、これらの脅威と同様にして、クライアント側のIMソフトウェアに存在するバグやその他の脆弱性を悪用するワームまたは複合型脅威が出現する可能性があります。この種の脅威は、例えば、IMクライアント・プログラムにバッファ・オーバーフロー攻撃を仕掛けることで新たなシステムへのアクセスを獲得し、システム侵入後は、そのユーザのメンバリストにアクセスし、新たなセットの標的を見つけるといった方法を使用することが考えられます。

この種の脅威の感染拡大速度と大量のマシーンに影響を及ぼしかねないことを考慮すると、こうした事態は憂慮に値します。CodeRedの場合はわずか数時間で数十万台ものインターネット・サーバーの攻撃に成功したことを踏まえると、精巧に作られたIMベースのワームであれば、同じ時間内で攻撃の影響を受ける一般家庭のパソコンやワイヤレス機器の数は、数千万台規模に上るおそれがあります。

サービス拒否攻撃

インスタント・メッセージング・プラットフォームはその他の通信システムと同様、サービス拒否攻撃に対して脆弱です。例えば、攻撃者はIMプロバイダーのインフラストラクチャに存在するIMサーバーに不正なTCP/IPパケットを大量に送信することによって、そのシステムを通過する正規のメッセージのトラフィックを妨害する可能性があります。これはここ数年で起こった有名Webサイトへのサービス拒否攻撃と同様の事態を引き起こします。また、別の方法として、攻撃者は大量のパケットを特定のユーザあるいはユーザグループに送りつけ、彼らのコンピュータをチャットやファイル転送リクエストで溢れさせる可能性があります。

インスタント・メッセージング・サーバーの脆弱性

セキュリティの専門家の多くはIMクライアントの脆弱性を注視していますが、IMサーバーの脆弱性についても考慮する必要があります。攻撃者がこれらのサーバーへのアクセスに成功した場合、あらゆる会話内容の盗聴、アカウント詐称、サービス拒否攻撃、悪意ある脅威の拡散といった有害活動がいとも簡単に実行されてしまう可能性があります。さらにIMトラフィックが暗号化されていない場合には、攻撃者はIMサーバーの制御を得るだけで、そのサーバーを経由するあらゆる通信内容にアクセスできるようになります。

社内におけるインスタント・メッセージングのセキュリティ対策

インスタント・メッセージングはビジネスに欠かせないツールになることが予想されます。しかし、安全性が確保されていないIMプラットフォームを社内で利用するのは非常に危険です。このセクションでは、インスタント・メッセージングの社内での利用に伴なうセキュリティ上の課題を解説した後、IMプラットフォームのセキュリティ確保に役立つベスト・プラクティスをご紹介します。

インスタント・メッセージングと企業ファイアウォールの関係

企業・法人のお客様の多くは、社内に設置しているネットワーク・ファイアウォールを使って、安全でないインスタント・メッセージング・システムを介した通信をブロックすることを望んでいます。残念ながら、ファイアウォールの多くは、標準設定では最新世代の人気IMシステムへのアクセスをブロックするのに十分な構成になっていません。最新世代のIMシステムはファイアウォールの存在を考慮して設計されており、企業ファイアウォールの目を逃れてIMサーバーに到達する技術を駆使しています。

IMクライアントはすべて、IMサーバーへの接続に使用するTCP/IPネットワーク・アドレスを1つまたは複数使って設定されており、接続が確立された時点で、クライアントは他のIMクライアントとメッセージ交換が可能な状態になります。企業の多くは境界ファイアウォールを業務に必要な少量のサービス(SMTPメール、HTTP Webサーフィング、DNS等）を除くすべてのインターネット・サービスをブロックするように設定しているため、IMプロバイダーはIMクライアントが一般的に許可されているインターネット・サービスをトンネルで通り抜け、必要であれば企業ファイアウォールをすり抜けることができるように設計したのです※4。

例えば、IMプログラムの多くは、IMサーバーへの接続に障害が生じた場合、ブラウザーがWebアクセスに使用している80番のネットワーク・ポートを使ってIMサーバーへの接続を試みます。ほとんどの企業向けファイアウォールは企業ネットワーク上に存在するすべてのPCがWebにアクセスできるように設定されているため、ポート80を通過する全トラフィックを通過させます。そのとき通過が許可されるトラフィックには、IMクライアントがIMサーバーに接続するために発信した通信も含まれます。これはファイアウォールにとっては、IMクライアントも他のWebブラウザーも同じに見えるためです。しかし実際には、ファイアウォールに気づかれることなく、IMクライアントはWebサーフィング(HTTP)コマンドではなくメッセージング・コマンドをIMサーバーに送信しているのです。※5

インスタント・メッセージング・クライアントが政府当局から逃走中の逃亡者だと想像してください。逃亡者は主要幹線道路に敷かれた警察の検問（ファイアウォール）を抜けてアジト（インスタント・メッセージング・サーバー）に到達して身を潜めたいと考えています。逃亡者は警察が公道の全車線を封鎖していることを知っているため、公道の脇にある自転車専用道路（HTTP、ポート80）を通り抜けることにしました。警察は自転車専用道路を使うのは正規のサイクリスト（Webサーファー）のみと考えているため、逃亡者は検問をたやすくすり抜け、アジトにたどり着くことができます。この例え話は、インスタント・メッセージング・システムがどのようにして企業ファイアウォールの検知から逃れているかをわかりやすく説明したものです。

※4 ほとんどの一般的なインスタント・メッセージング・クライアントでは、Socksプロキシもサポートしています。これにより、クライアントはファイアウォールを介して正式にメッセージ交換ができるようになりますが、セキュリティ強化にはなりません。
※5 Symantec Enterprise Firewallなど一部のアプリケーション・ファイアウォールは、チャットプログラムが通信時に非準拠のプロトコルを使用している場合、標準ポートのこの種のトンネリングを防止する能力を備えています。

要するに、インスタント・メッセージング・クライアントによる通信を社内でブロックするためには、クライアントがIMサーバーに到達できないようにする必要があります。そのためには、ファイアウォールの管理者はサーバーのアドレス名（例：instantmessageserver.chatservice.com）またはサーバーのIPアドレス(例：11.22.33.44, 11.22.33.45)をファイアウォールのブロックリストに加えることですべてのインスタント・メッセージング・サービスをブロックする必要があります。IMシステム(IRCなど）によっては、複数の独立サーバーに接続しているものもあります。これらのシステムをブロックするためにはかなりの調査が必要となりますが、確実を期すためには、それ以外に方法はありません。

インスタント・メッセージングによるファイル転送とファイアウォールの関係

既存のインスタント・メッセージング・システムは、ユーザ間でのファイル交換に（アクセスを許可するために微調整が可能な中央サーバーを通じた通信ではなく）ピア・ツー・ピア通信方式を使用するため、境界ファイアウォールをファイル転送をブロックするように設定することは、単純なメッセージ交換をブロックする場合よりも容易です。

ファイル転送を企業ファイアウォールで最も効果的にブロックする方法は、一般的なIM製品がピア・ツー・ピアによるファイル転送に使用している番号のポートをブロックする規則を追加することです。これにより、このようなIMシステムを使用してファイアウォールの通過を試みるファイル転送を確実に遮断することができます。ただし、社内にいる2人のユーザ間で行われる転送はこの方法でブロックすることはできません。さらに、既存の商用インスタント・メッセージング・システムの中には、企業ファイアウォールを密かに通過することを可能にする転送メカニズムを備えたシステムが少なくとも1つ存在することが確認されています。このような理由から、また、インスタント・メッセージングにより転送されるファイルのウイルスチェックを行う機能を備えた企業ファイアウォール製品は現時点では皆無のため、企業はすべてのデスクトップ・コンピュータにウイルス対策ソフトウェアを導入し、IMサービスを介して感染を試みる脅威を検知できるようにしておく必要があります。

今後、企業とインターネットとの間を往来するIMファイル転送に対してもスキャン能力を備えた新たなファイアウォール製品やその他のプロキシがリリースされることになるでしょう。シマンテックでは現在、この領域に対応する様々なソリューションを調査・研究中です。

インスタント・メッセージング利用時のベスト・プラクティス

シマンテックでは、インスタント・メッセージング・システムを企業内部で安全に利用するための方法として次のベスト・プラクティスの実践を推奨します。

社内におけるインスタント・メッセージング利用ポリシーを確立する

企業は公衆のインスタント・メッセージング・システムの利用に伴なうリスクを考慮し、社内でのインスタント・メッセージング・システム利用を全面的に禁止するか、あるいは、従業員に対し少なくとも業務目的での利用は控えるように通達することを検討してください。

境界ファイアウォールを適切に設定する

システム管理者は、境界ファイアウォールを、社内での利用を認めていないインスタント・メッセージング・システムによる通信をすべてブロックするように設定してください。メッセージングとファイル転送の両方をブロックする必要があるため、それぞれの場合に対応したファイアウォール規則を追加することを推奨します。

メッセージングをブロックするためには、あらゆる有名IMシステムのサーバーへのアクセスをブロックする規則をファイアウォールに追加する必要があります。このような設定が業務上不都合な場合は、IMが一般的に利用しているポート番号をネットワーク上のすべてのクライアントからブロックするよう設定するだけでもかまいません。ただし、その場合、IMクライアントの設定によってはファイアウォールを通過してしまう可能性が残ることに注意してください。

ファイル転送をブロックするためには、システム管理者は各IM製品がピア・ツー・ピアによるファイル転送に使用しているポート番号を特定し、それらのポートを通過するすべての通信をブロックするようにファイアウォールを設定してください。

デスクトップ用ウイルス駆除ソフトウェアを導入、展開する

現行の企業ファイアウォールには、インスタント・メッセージングによるファイル転送に対してウイルス／ワーム／トロイの木馬をチェックする機能はないため、社内のすべてのデスクトップ・コンピュータに最新版のウイルス対策を展開することが不可欠です。IM経由で届く悪質なコードに対して最も効果的かつ唯一の防御手段は現在、デスクトップ用ウイルス駆除ソフトウェアのみです。

パーソナル・ファイアウォールを使ってポリシー遵守の徹底を図る

Symantec(TM) Desktop Firewall(SDF)のようなパーソナル・ファイアウォールは、利用が認められていないIM製品も含め、正式に認証あるいは許可されていないプログラムによるインターネット経由での通信を容易にブロックできるように設計されています。デスクトップ・ファイアウォールは通信トラフィックをプログラムごとに許可あるいは拒否するように設定可能なため（例えば、Aというチャット・プログラムにはインターネットへのアクセスを許可し、Bというチャット・プログラムには許可しないといった設定が可能）、マシン全体に1つのポリシーしか適用できない境界ファイアウォールに比べ、はるかに柔軟に対応できます。

専用インスタント・メッセージング・サーバーを設置する

可能であれば、セキュアなインスタント・メッセージング・サーバーを企業ネットワーク上に展開し、IMクライアントがそのサーバーに接続するように設定してください。

現在多数の企業が企業向けのIM製品を販売しています。また、IRCなどのシステムは、格安（または無償）で入手できます。企業ネットワーク内に1つまたは複数のIMサーバーを設置すれば、社内で行われるすべてのIM通信を企業ファイアウォールの内側に収めることができます。

推奨するインスタント・メッセージング・クライアントの設定値

外部、すなわち、インスタント・メッセージング・プロバイダがサーバーを運用しているインスタント・メッセージング・システムを利用する場合には、次のセキュリティ・プラクティスを念頭に置いて利用することをお勧めします。

1. 安全対策の一貫として、正式に認定されている暗号化システムを採用していない外部のIMシステムは使用しない。
2. すべてのIMクライアントを、従業員のメンバリストで指定されているユーザから発信されたチャット要求以外は受け付けないように設定する。これにより、従業員が明確に指定したユーザ以外はIMを通じて従業員に接触できなくなるため、攻撃者がネットワーク上のコンピュータに接続したり、悪質なコードを送りつけることを防止できます。
3. IMシステムを、ファイル転送をブロックするか、あるいは、メンバリストに登録されているユーザから発信されたファイル転送のみを許可するように設定する。支障がある場合は、ファイル転送の際には必ず従業員に確認を促すメッセージを表示するよう、IMソフトウェアを設定してください。
4. IMシステムを、ウイルス駆除ソフトウェアを使ってファイル転送をスキャンするように設定する（サポートされている場合）。
5. IMアカウントが公開サーバー上に表示されないように設定する。これにより不要なチャット要求を防止することができます。

修正パッチのリリース時には可能な限り早期に適用する

社内で利用されているインスタント・メッセージング・システムにセキュリティ・ホールあるいはバグが発見された場合は、可能な限り早期に最新版の修正パッチを適用してください。CodeRed、Nimda、そして1988年に出現したインターネットワームでさえも、既知の脆弱性を利用して大量のシステムに感染を広げました。今後、同様の技術を使用した攻撃がインスタント・メッセージング・システムに対しても行われる可能性は十分にあります。

脆弱性管理ソリューションによりポリシー遵守の徹底を図る

企業は、ユーザがIMクライアントの設定を会社のポリシーに反する内容に勝手に変更しないようにするために、Symantec Enterprise Security Manager(ESM)のような脆弱性管理(VM)ツールの利用を検討することをお勧めします。脆弱性管理ツールは、IMポリシーの全体的な遵守状況の把握に役立つ情報を供給したり、ポリシーに違反しているコンピュータの更新作業を容易にします。さらに、IMソフトウェアが最新版かどうかや、ユーザがセキュリティホールやバッファ・オーバーフローの脆弱性を持ったバージョンを実行しているかどうか、ユーザが会社指定のウイルス駆除プログラムおよびパーソナル・ファイアウォール製品を実行しているかどうかのチェック作業を容易にする機能を備えています。

今後の展望

インスタント・メッセージングの利用は、今後10年の間に一般家庭、企業、そして電波を通じて無線で爆発的に普及することが予想されています。理想的には、このようなサービスを利用することで人と人とのつながりが緊密になり、業務効率も劇的に向上することが期待されており、インスタント・メッセージングは近い将来、電子メールや電話と同じく社会に欠かせない存在になるかもしれません。しかし、インスタント・メッセージングへの依存が高まるのに伴ない、その基盤となっているIMインストラクチャに課される責任もそれだけ重くなります。これらの通信フレームワークに発生したほんのわずかなセキュリティホールが原因で、人々は社会的にも経済的にも大打撃を受ける可能性があります。

幾つかの推測によると、IM機能を備えたコンピュータは2005年には5億台を突破すると予想されています。※6そのような世界では、IMシステムのインスタント通信機能の特性を併せ持つ電子メールが至るところで利用されるようになるでしょう。さらに、高速で常時接続のブロードバンド接続の一般家庭への普及が進めば、攻撃の標的もそれだけ増えることになります。コンピュータ・ワームや複合型脅威がこのようなインフラストラクチャを標的にするようになれば、IMネットワークを介してCodeRedと同じくらいに猛スピードで感染を拡大し、数千万台あるいは数億台ものコンピュータに被害を及ぼす可能性があります。そのような事態になると、感染したコンピュータの内、脅威によってデータが削除、破壊、あるいは暗号化されてしまったコンピュータがほんの一部だったとしても、経済に深刻な影響が生じる可能性があります。

もう1つの懸念事項は、無線通信です。IMサービスに対応したワイヤレス電話の数は急速に増えています。そのようなシステムに脆弱性が発見された場合、膨大な数に上る電話機に急速に感染を広げるワームや複合型脅威－CodeRedあるいはNimdaの無線バージョン－にさらされることになります。この種の脅威は、ネットワークを介した感染拡大に加え、電話リストの消去、無線によるインターネット接続サービスやあるいは緊急サービスに対するサービス拒否攻撃、音声会話の切断などの悪質な行為を行う可能性があります。そのような攻撃が現実になれば明らかに深刻な社会問題となるでしょう。

私達は、インスタント・メッセージング・システムの一般家庭および企業への普及が進んでいることを踏まえ、それがセキュリティにどのような影響を及ぼすのかを再考し、大攻撃が発生する前に対応策を検討する必要があります。

結論

インスタント・メッセージング・システムは、その効率性と便宜性により、多くの企業にとって非常に重要なツールとなりつつあります。しかし残念なことに、現行のインスタント・メッセージング・システムには十分なセキュリティ対策機能が欠如しているため、一部の企業ではセキュリティ上および経済面で深刻な問題となっています。

理想的には、インスタント・メッセージングの活用を検討中の企業は、企業ネットワーク内にセキュアな企業向けのIMソリューションを導入し、その上に適切なセキュリティ対策システム(ファイアウォール、脆弱性管理、ウイルス駆除ソフトウェアなど)を重ねることが望ましいと思われます。しかし、多くの企業は一般に人気のある無償IMサービスの利用を認めているのが現状です。これらの組織は、一般のIMサービス利用に伴なうセキュリティ・リスクを理解し、しかるべき対策を立てる必要があります。

インスタント・メッセージング・システムの成長により、ビジネス環境全般の作業効率が向上することは明らかです。これらのシステムのセキュリティを徹底さえすれば、企業は完全な経済効果を得ることができるでしょう。

※6 http://www.computerworld.com/cwi/story/0,1199,NAV47_STO61141,00.html

インターネット・セキュリティ・テクノロジー業界で世界をリードするシマンテックは、多岐に渡るコンテンツ・ネットワークセキュリティ・ソリューションを個人ならびに企業・法人のお客様にお届けしています。シマンテックはウイルス対策、コンテンツ・フィルタリング、システム管理、ファイアウォール / VPN、ポリシー監査、脆弱性検査、不正侵入検知におけるソリューション製品および企業・法人向けの各種セキュリティ・サービスの開発・提供を世界規模で展開しています。中でも Norton シリーズ（シマンテックの個人向けセキュリティ対策製品）は、世界 No.1 の売上高を誇り、また、数々のアワードも受賞しています。米国カリフォルニア州クパチーノに本社を置くシマンテックは現在、世界 37 か国に事業所を展開しています。

詳細については、弊社ホームページ www.symantec.co.jp をご覧ください。