情報セキュリティ歳時記 10

不正アクセスの実態と対策（その5）

前川　徹
早稲田大学 国際情報通信研究センター

ファイアウォール

さて，今回は不正アクセスからどのようにしてサイトを守ればよいのかを概観して，この不正アクセスに関するシリーズを終えることにしよう．

まずはきちんとファイアウォールを構築しよう．ルータのパケットフィルタリング機能を利用して外部からのアクセスを禁止する方法もあるが，細かな設定ができないために安全を優先するとインターネットの利便性を大幅に損なうことになるので，アクセス制限をするにはファイアウォールを利用する方法が一般的である．

当然のことながらファイアウォールは適切に設定しないと何の役にもたたない．どのようなアクセスを制限するのか，守るべきサーバ，ファイルは何なのかを決め，正しく設定する必要がある．ファイアウォールを用いれば，特定のプロトコルを禁止することも，特定のプロトコルだけを許可することも可能である．また，最近は単純に内部セグメントと外部セグメントを分けるだけではなく，情報発信用ウェブサーバなどの公開サーバの設置に適しているDMZ（De-Militarized Zone）と呼ばれるセグメントを設定できるものがある．DMZの設定によって，完全にパブリックな外部セグメントとプライベートな内部セグメントの間に，セミ・パブリックなゾーンを設けることができる．たとえば，外部提供用のウェブページでデータベースから動的にコンテンツを作成する場合には，ウェブサーバはDMZに置き，データベースは内部セグメントに置いてウェブサーバより厳しくアクセスを制限するといったような使い方をする．ファイアウォールの設置によってインターネットの利便性がいくらか損なわれるだろう．組織内のユーザから不満が出るかもしれない．しかし，安全のためには多少の不便は我慢しなければいけない．

ちなみに，ファイアウォールには市販のものもあれば，フリーのものもある．その機能や使い勝手，ユーザインタフェースが異なるので，用途と経費に合わせて最善のものを選んでいただきたい．また，ファイアウォールの構築にはネットワークセキュリティに関する幅広い専門知識が必要となる．場合によっては信頼できる専門企業に導入作業を委託したり，専門のコンサルタントを雇うことを検討した方がよいだろう．

侵入検知システム

一般的にIDS（Intrusion Detection System）と呼ばれる侵入検知システムは，システムを監視し，セキュリティポリシーに反するような行為を見つけ出して管理者に警告を発すると同時に，その後の調査分析作業を支援するために必要な情報を蓄積・提供するシステムである．侵入検知システムはファイアウォールなどに比べると新しいもので，まだ製品の種類も導入実績も少ない．

侵入検知システムには，ホストベースのものとネットワークベースのものがある．

ホストベースのものは，監視対象となるホストコンピュータのOSやその上でサービスを提供しているアプリケーションソフトが記録しているログ（利用履歴）情報から不正アクセス行為を検出しようというものである．当然のことながら，ログ情報に残らない不正アクセス行為は検出できないので，利用しているOSやアプリケーションソフトが適切なログ情報をログファイルに保存するように設定しておく必要がある．また，ログ情報の保存のために，そのホストコンピュータの資源（CPUや磁気ディスクなどの記憶装置）を消費するということも考慮に入れておく必要がある．

一方，ネットワークベースの侵入検知システムは，ネットワーク上のパケットを監視し，その内容やパターンによって不正アクセス行為を検出しようというものであり，こちらはデータ収集のために特別の設定を必要としない．ネットワークを流れるパケットのフォーマットは標準化されており，確実に情報が収集できるからである．ただ，侵入検知システムが設置されたネットワーク上を流れるパケット情報を分析しているので，ローカルホスト上で行われている不正アクセス行為は検出できないという欠点がある．

収集したデータから不正アクセス行為を検出する手法は，Misuse DetectionとAnomaly Detectionの2種類がある．Misuse Detectionは，既知の不正アクセス行為のパターンをデータベースとして持っており，それと比較することによって不正アクセス行為を検出するという方法で，検出するためのデータ量が少なくて済むというメリットがある反面，データベースに登録されていないパターンの不正アクセス行為は検出できないという問題がある．

一方，Anomaly Detectionは，不正アクセス行為が通常の利用パターンとかけ離れたものであることを利用して検出しようというものである．たとえば，深夜に利用したことのない利用者が午前2時にホストコンピュータにアクセスしてくれば，クラッカーがなりすましによって侵入してきた可能性が高い．またプログラムのコンパイルをするはずのない一般ユーザがコンパイル作業をしていれば，これも不正アクセス者である可能性が高い．この手法を用いるためには，ユーザごとに利用時間帯や利用サービスなどの利用パターンを分析してその特徴をデータとして蓄積しておく必要がある．また正規のユーザが通常と異なる利用をすると不正アクセス行為と誤認されてしまう可能性もある．

現状では，多くの侵入検知システムがMisuse Detectionを採用しているが，いずれAnomaly Detectionを併用するものも増えてくるだろうと思われる．侵入検知システムを設置したからといってすべての不正アクセス行為を検知できるものではないが，利用価値は十分ある．

リモートアクセス環境

表玄関はしっかり戸締まりしてあったのだけれど，裏口の鍵をかけていなかったというのではお話にならない．インターネットへの接続が表玄関だとすると，リモートアクセス環境が裏口にあたる．リモートアクセス環境は，物理的に外部から組織内のネットワークに接続し，組織内にいる場合と同等のサービスを利用するために設けられることが多い．こうした環境を設けることによって，出張先から社内にいる時と同様に内部のシステムが利用可能になる．ただ，安易にリモートアクセス環境をつくるのはきわめて危険である．たとえば，利用したいホストに直接モデムを接続し，公衆電話回線経由でアクセス可能にしているケースがあるが，これはきわめて危ない．アクセス制御がきちんとできない入り口をつくるのは，セキュリティホールを塞がないでそのままにしているのと同じくらい危険である．電話番号が秘密になっているから安全だと思うかもしれないが，クラッカーはモデムが接続されている電話回線を探し当てるツールを利用して，こうした裏口を簡単に捜し出してしまう．

リモートアクセス環境を設ける場合には，認証サーバなどを利用してユーザや利用できるサービスを限定しなければいけない．たとえば，ユーザの認証には通常利用しているユーザIDとパスワードの他に，ワンタイム・パスワード（使い捨てのパスワード）を利用して本人確認を厳密に行う必要がある．

サーバの設定・管理

前回までにすでに述べてきたことではあるが，ウェブサーバやftpサーバなど外部向けのサーバの設定や管理をきちんと行うことも，不正アクセス防止のためにはきわめて重要である．まず必要のないサービスは停止し，不要なアプリケーションソフトは削除しておこう．クラッカーはツールを用いて絨毯爆撃的に利用可能なサービスポートを調べてくる．別に邪魔にならないからというだけの理由で開かれたままになっているポートから侵入された事例は少なくない．

また（これも何度も書いてきたことだが）既知のセキュリティホールをそのままにしておいてはいけない．セキュリティホールを放置しておくことは，クラッカー用の入り口を設けているようなものだ．またセキュリティホールは次々と新しいものが発見される．すでに発見されたセキュリティホールを塞ぐだけではなく，いつもJPCERT/CCやCERT/CCなどが発表するセキュリティ情報に注意し，すみやかに対策を講じなければいけない．クラッカーも同じようにセキュリティ情報を収集しており，対策が遅れると彼らの餌食になってしまう．既存のセキュリティホールへの対策が万全かどうかをチェックするには，前回紹介したサーバのセキュリティ上の弱点をチェックするツールを利用するのもよいだろう．

ログの収集・分析

不正アクセス禁止法では義務化が見送られたが，ログ情報を記録しておき分析することも不正アクセス防止には役に立つ．最近ではログ情報の収集と集計を自動的に行う便利なツールもある．ログを分析することによってセキュリティ対策の不備が見つかることもあるし，場合によっては不正アクセスの兆候が見つかり，ファイルの破壊や改ざんを未然に防ぐことができることもある．

パスワード管理の徹底とユーザ教育

この連載の第7回で書いたように，パスワード管理は基本中の基本である．すべてのユーザに情報セキュリティとパスワードの重要性について教育し，容易に推測できるようなパスワードをつけさせてはいけない．また，トロイの木馬型のウイルスによってパスワードが盗まれることがないように，安全が確認できないプログラムをダウンロードして利用したり，安易に電子メールの添付ファイルを開いたりしないように徹底する必要がある．

次回からは暗号技術を巡る話題を取り上げる．

今月の参考文献等
1) 侵入検出システム評価の調査研究：http://www.ipa.go.jp/SECURITY/pub/contents/crack/develop/ids/IDS_eval.htm
2) サイトセキュリティハンドブック（RFC2196）：http://www.ipa.go.jp/SECURITY/rfc/RFC2196-00JA.html

（平成11年11月14日受付）