インターネットセキュリティ技術

理工学部研究協力係　佐　藤　勝　人

miri@cc.hirosaki-u.ac.jp

概　要

サーバ管理者は、自分自身が管理運用するサーバに対して、サービスが停止しないように保守することと同時に、不正侵入されないようにネットワークセキュリティに対して管理運用を行うことが不可欠になってきた。本テーマでは、国立情報学研究所が主催した平成15年度第３回情報セキュリティ担当職員研修上級コースを筆者が受講した際に修得した知識と技術を交えながら、ネットワークセキュリティについて解説する。

1．はじめに

ネットワークセキュリティについて、TCP/IPアプリケーションプロトコル上で提供できるサービスは、比較的手軽に実装・使用することができる。しかし、手軽さと引き替えにセキュリティに対しての対策が整備されていない。そこで、ハッカーによる攻撃や不正侵入の現状を把握して、適切な措置を行い、常にサーバサイトを監視することが重要である。本テーマでは、さまざまなサービスの弱点と対策、不正アクセスの検出や発信元の追跡を行うためのログ分析、セキュリティの診断・監視についてどのように対応していけばよいかを解説する。

2．TCP/IPアプリケーションプロトコルの弱点

ネットワークを利用するアプリケーションは、主にトランスポートプロトコルとして、TCP（Transmission Control Protocol）とUDP（User Datagram Protocol）を利用する。今回は、TCPプロトコルの弱点について主に解説する。

2.1　TCPコネクション

TCPコネクションは、3Way-Handshakeという手続きを実施することにより、信頼性のある通信を提供する。送受信されるデータの各バイトに一連の番号（シーケンス番号）が付けられており、データを受け取った側では、どのシーケンス番号までを受け取ったかを送信元へ応答することで、送信側はデータが正しく相手に届いたことを確認する。

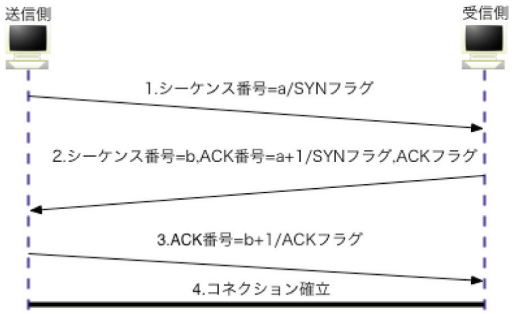


図１.3Way-Handshake

3Way-Handshakeは、送信側のホストから受信側のホストに対してSYNフラグを送信する。次に受信側のホストから送信側のホストに対して、SYN、ACKフラグを送信する。最終的に送信側のホストから受信側のホストにACKフラグが送信されて、コネクションが成立する。その後のやり取りされるデータには全てACKフラグが添付される。

・3Way-Handshakeの正常動作の確認方法

Windowsでは「ネットワークモニタ」ツールを利用すればよい。その他のOSではフリーツールのLANアナライザソフトを使用すればよい。

2.1.1　IP Spoofing Attack（IPなりすまし攻撃）

TCPコネクションを設定する際に行われる3Way-Handshakeの特性を利用して、送信元を同じにしたパケットをインターネット側から送り込むことで、ファイアーウォール内からの通信であるかのように見せかけ、内部へ侵入しようとする不正アクセスの方法である。IP Spoofingは、IPパケットのIPヘッダ情報だけの仕組みを悪用した攻撃である。

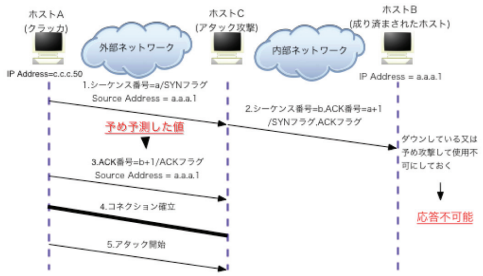


図２.IP Spoofing Attack

・対策

ルータ等の設定で、外部から送られてきた内部アドレスをソースアドレスとして使用しているパケットを廃棄するようにパケットフィルタを有効にする。

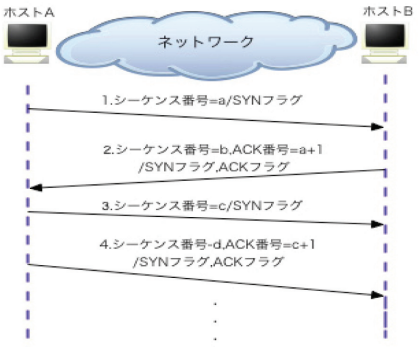
関連RFC：RFC1948シーケンス番号攻撃を防ぐ（Defending Against Sequence Number Attacks）

2.1.2　SYN Flood Attack

TCPコネクションを確立するための３Way-Handshakeを悪用した攻撃方法である。アドレスを偽造したクライアントから大量のSYNパケットをサーバに送りつける。サーバ側が受け取ったSYNパケットに対してACK/SYNパケットを送り返し、

クライアントからのACKパケットの待ち状態に入る。しかし、偽造されたアドレスからのACKパケットの返答がないため、サーバはACKパケットの待ち受けが大量に発生し、正常なアクセスを受け入れられなくなったり、システムクラッシュを引き起こすなど障害が発生する。

図３.SYN Flood Attack



SYN Flood Attackは、受信側のホストでは、SYNフラグを送信してきたときにバッファを確保するが、攻撃側（送信側）は、一方的にSYNフラグだけを大量に送信して一種のDOS攻撃に近い状態になり、受信側のホストが不能になる。

・対策

ネットワーク内でやり取りされるSYNパケットを識別するのは不可能であり、ハッカーも自分がばれないようにいろいろなアドレスを使用してくる。対策としては、OSの機能を利用して以下の設定を行う。

１．HalfOpenの最大コネクション数を制限する。

２．HalfOpenのコネクション数が増加した際に、バッファを確保しないようにする。

ホストの動きが遅くなってきた段階で、そのホストに対して同一のホストからSYNパケットが連続して送信されていることを確認した場合には、ルータやファイアーウォール等のフィルタリング等を行う事後対策を行えばよい。

関連RFC：RFC2827ネットワークのイングレスフィルタリング（Network Ingress Filtering）

2.1.3 IPソースルーティングの悪用

普通のルーティングは、ホップバイホップルーティングといい、各中継ルータが、パケットに記載された宛先ホストアドレスと経路表を参照して経路を決定する。IPソースルーティングは、IPプロトコルのオプションで発信者が宛先に届くまでに中継するホストを指定する。ソースルーティングは、IPヘッダ内の宛先IPアドレスを発信者が経路指定したアドレスで変化させながら通信する。この特徴を悪用して不正侵入を行う。

・対策

ルータ、ファイアーウォール、サーバでIPソースルーティングを禁止する。

2.1.4 フラグメントを利用した攻撃

フラグメントとは、パケット（データ）を分割する機能で、ネットワーク・インタフェースが所属するネットワークのMTU（Maximum Transmission Unit、ネットワークが送信できる最大の伝送単位：Ethernet上で扱えるMTUは1500バイト）サイズ以上のパケットを送信する場合に、元のパケットを分割して、MTUサイズ以下にして送信する。１回細分化されたパケットは、受信したマシン内部で再構成される仕組みになっている。

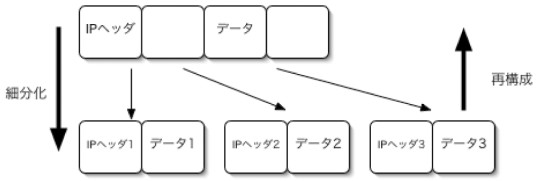


図４.IPパケットの正常な細分化/再構成

このフラグメントの機能を利用して以下の２種類の攻撃がある。尚、これらの攻撃は、IP層のファイアーウォールでのパケットフィルタリングの場合にのみ確立する。

・タイニーフラグメント攻撃

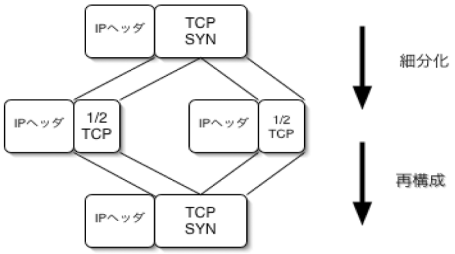


図５.タイニーフラグメント攻撃

IPパケットの分割機能を利用して非常に小さな断片に分割することにより、パケット・フィルタリングをすり抜ける攻撃方法である。IPヘッダの後に続くTCPヘッダが分割されることにより、パケットフィルタリングで確認する際に、TCPヘッダの残りの部分（SYNやACKなどの制御フラグなど）の位置にデータが無かったり、２番目のパケットに入ったりするため、パケット・フィルタリングを不正に通過してしまう。最終的に受信したマシンで再構成されると、TCPヘッダが完成されるため、3Way-Handshakeの１番目のパケットが正常に処理される。

・オーバーラッピングフラグメント攻撃

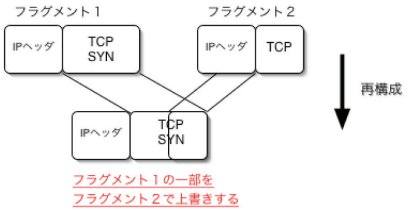


図６.オーバーラッピングフラグメント攻撃

IPパケットの分割機能を利用してオフセットが重複するような断片を生成し、パケット・フィルタリングをすり抜ける攻撃方法である。２番目以降の断片のオフセットを先頭の断片と重複させることにより、パケットフィルタリングを通過できないような

パケットでも通過させてしまう。再分化された状態では、TCPヘッダにSYNが無くても、受信したマシンで再構成されるとSYNが現れる。
その他のフラグメントを利用した攻撃としては、不正なサイズ（極端に大きい又は小さい）フラグメントを送信することで攻撃対象のホストを不能にさせる攻撃もある。
関連RFC：RFC1858IPフラグメントフィルタリングについてのセキュリティ上の考察（Security Considerations for IP Fragment Filtering）

3．TCP/IPアプリケーションプロトコルによるサービス

3.1 DNS：Domain Name System

DNS（ドメイン名解決システム）とは、IPアドレスのように各マシンの識別を数字で行っているが、人間側で数字が扱いにくいことから、文字を使用して名前を付けることが出来るようになっている。
・問題点
1）名前情報漏洩の危険性
DNSサーバは、名前やIPアドレスの問い合わせに対して、持っている情報をすべて答えてしまうことから、ハッカーはこの名前情報（名前とIPアドレスの対応を示す情報）からクラックを実行するための必要な情報を容易に収集することが可能である。また、ハッカーは自分のDNSサーバをセカンダリサーバに設定することで、プライマリサーバ上の名前情報のコピーを入手することも可能である。
2）名前情報改ざんの危険性
ハッカーは、アクセス制限をホスト名で行っている場合は、DNSサーバの情報を改ざんして、自分のIPアドレスと組織内のホスト名を対応付けすることにより、侵入を容易に行うことができる。侵入が成功すると、BSD系UNIXのr系コマンド（rsh、rlogin等）を実行して攻撃される。
・対策
1）名前情報漏洩への対策
インターネットに公開するDNSサーバは、インターネットに公開しているサーバの情報だけを登録する。セキュリティ対策として公開用のDNSサーバは、内部（組織内LANシステム）と外部（例えば、インターネット）の境界に設置するLANセグメント（LANの構成単位）上に設置する。組織内情報を扱うDNSサーバは、組織内ネットワークに設置することにより、組織内のDNSサーバには外部ネットワークからのアクセスを防ぐことができる。
2）名前情報改ざんへの対策
公開用DNSサーバを要塞化して、DNS情報を改ざんされないようにする。名前情報は定期的にチェックして、不審な情報が無いかを確認する。
DNSサーバには必ず逆引きデータを登録しておく。アクセスを受ける側のサーバでは、DNSの逆引きを利用して通信相手のアドレスの正当性をチェックする方法もある。
関連RFC：RFC2535DNSセキュリティ拡張（Domain Name System Security Extensions）
関連RFC：RFC2845DNSのための秘密鍵処理認証（Secret Key Transaction Authentication for DNS（TSIG））

3.2 電子メール（SMTP、POP）

電子メールは、ネットワークアプリケーションの中で一番多く利用されている。このアプリケーションは、非常に高機能であり様々な機能を実現できるが、この機能を悪用された場合には、広範囲に被害が生じる可能性が高い。
・問題点
1）sendmailのセキュリティホールへの攻撃
フリーソフトで有名な電子メールサーバであるsendmailは、多機能な反面、セキュリティホールを多く抱えている。その中で、ハッカーはsendmailが持つデバック機能を悪用することにより、メールサーバに成り済ますことが可能である。sendmailの特有な部分である、受信したメールをスプール中に書き込むための特別な権限を持って動作する機構を悪用されることが多い。
2）ユーザアカウントのパスワードクラック
メールサーバを利用するために登録するユーザのアカウントの数が増加することで、管理が行き届かないところで望ましくない簡単なパスワードを設定するユーザが出てくる。ハッカーにとっては、最適な標的となる。
3）メール爆弾
メールサーバを使用不可にするために、大量のメールを送りつける攻撃である。その結果、メールサーバは過負荷状態になりダウンしたり、メールのスプール領域をあふれさせてメールを使用不可にする。
4）メール内容の盗聴
普段やり取りしているメールの内容は、暗号化されずに平文で送受信される。そのため、途中のネットワークやメールサーバで盗聴される可能性がある。特に、盗聴の危険性を認識していない状態で、機密情報をメールでやり取りするのは機密事項の漏洩につながるので注意が必要である。
5）POPのIDとパスワードの盗聴
メールの内容と同様に、POPを利用してメールサーバ上のメールを読む際にユーザIDとパスワードの入力が必要になるが、この情報も暗号化されない。よって、盗聴することでユーザIDとパスワードを確認することができる。
6）SPAMメール中継
SPAMメールやメール爆弾の中継にメールサーバが利用されることにより、知らないうちに悪用され加害者扱いにされてしまう場合がある。
・対策
1）sendmailのセキュリティホールへの攻撃への対策
セキュリティホールが修正された最新バージョンのsendmailを使用する。sendmailで利用する設定ファイル群（メールをスプールするディレクトリ等）のパーミッション設定に注意する。
2）ユーザアカウントのパスワードクラックへの対策
内部と外部の境界に設置するLANセグメント（LANの構成単位）上にメールサーバを設置して、メールの中継だけを行うように設定する。このメールサーバには、組織内のネットワークに実在するユーザアカウントなどの設定をしないようにする。
3）メール爆弾への対策
根本的な対策はないが、メール爆弾を受けた場合に、攻撃を仕掛けてくるメールサーバからのメールを受信しないように設定することで対応するしかないようである。

４）メール内容の盗聴への対策
SSL等を利用してメールの暗号化を行う。
５）POPのIDとパスワードの盗聴への対策
メールサーバを分散させて信頼できるネットワーク内に限定してPOPを利用できるようにする。また、パスワードを暗号化できるAPOPと呼ばれる認証方式を使用することで、盗聴されずに済む。
６）SPAMメール中継への対策
メールサーバの利用形態のうち、他のサイトから受信したメールを更に他のサイトへメールを中継する場合に、中継を制限していない場合には、SPAMメール中継に不正利用される可能性がある。実際のメールサーバの利用形態は、
㈠ 自サイト内のユーザ間のメール配送
㈡ 自サイトから他サイトへのメール送信
㈢ 他サイトから自サイトへのメール受信
以上の形態で運用すればよい。
「POP before SMTP」や「SMTP Auth」を用いてメール送信時にユーザ認証を行う方法もある。

3.3 ファイル転送（FTP：File Transfer Protocol）

FTPとは、ネットワーク上に設置してあるコンピュータ間でファイル転送を行うようにするプロトコルである。FTPのタイプは、大きく分けて２種類に分かれる。１つは、利用者がFTPサーバに接続を要求する際に、ユーザIDとパスワードの認証を行う方法で、もう１つは、不特定多数の利用者に対して匿名のアカウントで利用できるanonymous-FTPがある。
・問題点
１）ディスク、ファイルのパーミッション設定変更による攻撃
FTPサーバ上のパーミッションの設定で、書き込み禁止の設定漏れを発見して、.rhostsに対して書き込みを行うことで、rlogin等を使用して侵入する攻撃がある。
２）公開用FTPサーバを利用したファイルの受け渡し
情報公開用のanonymous-FTPサーバで、ディレクトリに対して書き込みを許可する設定にしている場合は、ハッカーの情報交換の場としてファイルの受け渡しに使用される可能性がある。
３）公開用FTPサーバへの使用不能攻撃
情報公開用のanonymous-FTPサーバなどで、ディレクトリに対して書き込みを許可する設定にしている場合は、大量のファイルを書き込むことでディスク容量を浪費させる攻撃がある。
・対策
１）ディスク、ファイルのパーミッション設定変更による攻撃への対策
anonymous-FTPを使用する際に、ディレクトリやファイルのパーミッションの設定、アクセス範囲の限定に注意する。その中で、/etc/passwdファイルや実行ファイル等に対してアクセス拒否の設定を行う。更に、chrootコマンドによってanonymous-FTPのルートディレクトリを変更して、設定されたディレクトリの配下以外のアクセスができないように設定する必要がある。できれば、anonymous-FTPの使用は控えるべきである。
２）公開用FTPサーバを利用したファイルの受け渡しへの対策
anonymous-FTPは、読み出し、書き込み両方を許可するディレクトリは作成しないようにする。
３）公開用FTPサーバへの使用不能攻撃への対策
書き込み可能なディレクトリを準備する場合には、そのディレクトリに対して書き込み容量の制限を行い圧迫されないようにする。
関連RFC：RFC2577FTPセキュリティについての考察（FTP Security Considerations）
関連RFC：RFC1579ファイアウォールと親和性のあるFTP（Firewall-Friendly FTP）

3.4 ファイル転送（TFTP：Trivial File Transfer Protocol）

TFTPは、主にディスク装置を持たないX端末やルータ、スイッチングHUB等のネットワーク機器からブートするために必要なファイルを転送する目的で使用されているファイル転送プロトコルである。
・問題点
TFTPは、ユーザ認証機能がないので自由にアクセスできてしまう。UDPを用いてファイル転送を行う際に、ファイアーウォールでのアクセス制限の設定が困難である。
・対策
TFTPの使用は厳禁である。どうしてもやむを得ない場合には、ファイルの書き込みを禁止する。

4．TCP/IPアプリケーションプロトコル以外の問題点

4.1 無線LAN（IEEE802.11）

無線LANは、電波を使用した無線通信で構築されたネットワークをいう。

表１.主なIEEE802.11実装の比較

	802.11g	802.11b	802.11a
最大データレート	54Mbps	11Mbps	54Mbps
最大データレートの有効範囲	18m	45m	12m
周波数帯域	2.4GHz	2.4GHz	5GHz
全世界で利用可能	○	○	○
消費電力	1.5W	1W	2～2.5W

4.1.1 無線LANのセキュリティ管理

・無線LANアクセスポイントのセキュリティ対策
１）SSID（Service Set Identity：通信グループ名）
SSIDは、インフラストラクチャーモード（アクセスポイントを経由した通信）のESS-ID（Extended Service Set Identity）とアドホックモード（アクセスポイントを経由しない２台同士の通信）のBSS-ID（Base Service Set Identity）の総称で、グループ分けに使用する名前で、他の無線LANクライアントからは、通常確認できる。
・SSIDの 問題点
SSIDは、セキュリティの面から見ると、アクセスポイントのメーカー名の一部を用いたり、講座名、教官の名前の一部を用いることで、どの場所で何のメーカーのアクセスポイントを使用しているか容易に確認できてしまう。

・SSIDのセキュリティ対策
　最終的には、アクセスポイントのステルス機能を用いて、SSIDを隠しておくことにする。SSIDのID認証とMACアドレスの認証機能を組み合わせる。
２）MACアドレス（Media Access Control Address)
　MACアドレスは、各イーサーネットカードに固有のID番号で、全世界のイーサーネットカードに１枚ごとに固有番号が割り当てられており、この番号を元にカード間でデータの送受信が行われている。
・MACアドレスの問題点
　MACアドレスは、全世界で１つの固有のID番号であるが、プログラムを利用してMACアドレスを変更することで、詐称することができる。
・MACアドレスのセキュリティ対策
　アクセスポイントで、MACアドレスによるフィルタリングを行い、登録されていないクライアントからのアクセスを拒否する。
３）WEP（Wired Equivalent Privacy）
　無線通信で送信されるパケットを暗号化して有線通信と同様の安全性を持たせるための暗号化技術で、旧方式の64bitのデータを使う方式と、新方式の128bitのデータを使う方式の暗号化キーが用いられている。
・WEP の問題点
　WEPは、ユーザー認証機能が無く、暗号化に脆弱性が存在し、状況によって容易に解読が可能となる。
・WEP のセキュリティ対策
１．128bitで16進数の暗号化キーを用いる（試行期間中はクライアント側の互換性重視して64bitの暗号化キーを用いている。）
２．802.1xのポート単位の認証プロトコルを用いる。
　今現在、本無線LAN構築のシステムにどのようにIEEE802.1xを導入するか検討中である。後の章でIEEE802.1xシステムの仕組みを報告する。

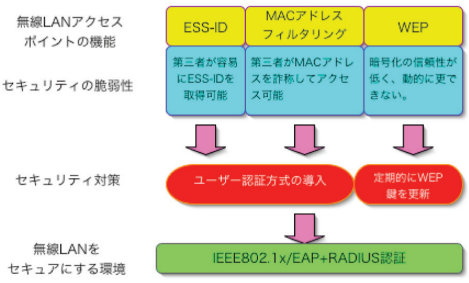


図７.セキュリティ対策

３．ホスト間のデータの送受信時にSSHを利用してSSHトンネリング機能を用いたり、IPsec等を使用して、無線LANに流れるデータを暗号化する。

4.1.2　クライアント側の無線LANセキュリティ対策

１）ネットワークサービスを安全に利用する
　使用していないネットワークサービスを停止する。使用するネットワークサービスについては、ファイアウォールを構築してサービスへのトラフィックを通過させる。WEPでの暗号化と、SSL、SSHの暗号化を組み合わせて利用するとよい。
２）ファイアウォールの構築
　ファイアウォールルール設定として、ループバックネットワークの成り済ましを防ぐ設定、偽のIPアドレスの使用を防ぐ設定を行う。
・MacOSXでのファイアウォール（ipfw）の設定例

```
#ループバックネットワークの成り済ましの防止
ipfw deny log all from any to 127.0.0.0/8
#偽のIPアドレスの使用防止
ipfw deny log all from 0.0.0.0/8 to any in
ipfw deny log all from 169.254.0.0/16 to any in
ipfw deny log all from 192.0.2.0/24 to any in
ipfw deny log all from 224.0.0.0/4 to any in
ipfw deny log all from 240.0.0.0/4 to any in
ipfw deny log all from any to 0.0.0.0/8 in
ipfw deny log all from any to 169.254.0.0/16 in
ipfw deny log all from any to 192.0.2.0/24 in
ipfw deny log all from any to 224.0.0.0/4 in
ipfw deny log all from any to 240.0.0.0/4 in
```

３）スタティックARPアドレスの設定
　ARPポイゾニングによるMITM攻撃を防止するためにARPエントリをスタティックな設定にする。
・MacOSXでのスタティックなARPエントリ設定
　arp -s〈Gateway IP Address〉〈Gateway MAC Address〉
・MacOSXでのスタティックなARPエントリ消去
　arp -d〈Gateway IP Address〉

4.1.3　無線LANをセキュアにするIEEE802.1xシステムについて

・IEEE802.1xは、端末を接続する物理的なLANポートごとに、接続してきた端末を利用するかどうかを認証する規格である。もともと有線LANでの利用を考慮した仕組みであるが、無線LANアクセスポイントと連携させることによって、無線LANをセキュアにすることができる。
・IEEE802.1xの仕組みは、EAP（PPP Extensible Authentication Protocol）認証プロトコルを用いて、RADIUSユーザー認証サーバー、無線LANアクセスポイント、無線端末、CA認証局（Certification Authority）との連携で実現できる。IEEE802.1xの認証方式は、EAP-TLS、EAP-TTLS、EAP-PEAP、LEAP（Cisco-EAP）などがある。

図８.IEEE802.1xの構成

4.2　電磁波漏洩問題（TEMPEST）

　パソコン等の電子機器を使用するときに発生する電磁波を盗聴することで、情報を再生することができるTEMPESTという手法がある。
　パソコンからの電磁波の中でも、イーサネットケーブル・コネクタ、USBケーブル・コネクタ等のシリアル伝送の信号は盗聴されやすい。また、発生する電磁波の小数点以下のレベルの違いを識別することによって、特定のパソコンの電磁波のみを盗聴することができる。更に、電源ケーブル、水道管等の導電性のものを利用した盗聴も可能である。

新情報セキュリティ技術研究会（IST）
URL http://www.j-netcom.co.jp/ist/

5．ログ分析

5.1　不正アクセスの兆候

不正アクセスが行われた場合に起きると思われる現象として以下の兆候が見られる可能性が高い。

・不明なシステムの再起動、シャットダウン
・不明なシステムのクラッシュ
・膨大なディスク領域の増加
・大量データのダウンロード
・急激な処理速度の低下
・ログファイルの急激なサイズの変化
・勤務時間外や休暇中のユーザのログイン
・存在しないアカウントを利用したログイン試行
・異なる電話回線からの同一ユーザによるログイン
・管理者が把握していないユーザアカウント
・見慣れないサイトからのアクセス
・接続禁止サイトからのアクセス
・TFTPによるファイル転送
・システム日付の変更
・不明な管理者権限の使用
・不明なアクセス権の変更
・踏み台にされている形跡がある。

これらの状況を把握するためには、ログイン、ログアウトを行ったユーザ、ホスト、アクセス権限の変更内容とその時刻等の情報を確認する。尚、パスワードに関する情報収集は厳禁である。収集したパスワード情報が不正利用されると大きなセキュリティ問題に発展するからである。

5.2　ログ分析の概要

不正アクセスの検出や発信元の追跡を行うためには、以下のようなログが必要である。

・オペレーティングシステム（UNIX、Windows等）
・ファイアーウォール
・リモートアクセス・認証サーバ（RADIUS等）
・WWWサーバ（Apache、IIS等）
・メールサーバ（sendmail、ExchangeServer等）
・ルータ（CISCOルータ等）

これらのログに関しては、ログの採取方法、ログの内容の出力項目について、ログの出力形式、ログのバックアップ方法を事前に整理する必要がある。

ログファイルの採取については、ログ情報が大量に発生すると、必要な情報を見逃してしまう可能性がある。逆にログ情報が少なすぎると不正アクセスの検出のための情報が不足してしまう。

ログの正確性について、侵入者によるログファイルの書き換え、消去、改ざんされないようにする。複数のシステム間でシステム日付を一致させる。

ログ採取の監査機能は、システムのパフォーマンス低下の要因になるので注意が必要である。

5.3　時間同期の必要性

複数のシステムにまたがってログ分析を総合的に行う場合は、各システム間での日付設定が一致していることが重要である。不正侵入された際に、ログの削除や改ざんのみだけでなく、システムの日付を変更して、ログ分析を困難にすることも考えられる。

・システム日付を合わせる方法

一般的には、NTPを利用する。NTPは、複数台のマシンで階層構造で時間同期を設定できる。

今現在、日本では、共同研究の一環として以下の組織が、日本標準時を提供する試行サービスを行っている。

・独立行政法人通信総合研究所（CRL）
・日本電信電話株式会社（NTT）
・株式会社インターネットイニシアティブ（IIJ）
・インターネットマルチフィート株式会社（MFEED）

これらのサーバは、CRLの日本標準時を刻む原子時計を直接時刻源としているため、時刻のずれ（オフセット）が非常に小さく（1000分の１秒以内）で安定している。

以下のサーバにNTPでアクセスすることで高精度な時刻情報を取得できる。（http://www.jst.mfeed.ad.jp）

・ntp1.jst.mfeed.ad.jp（210.173.160.27）
・ntp2.jst.mfeed.ad.jp（210.173.160.57）
・ntp3.jst.mfeed.ad.jp（210.173.160.87）

5.4　各種ログの種類と特徴

5.4.1　ファイアーウォールとルータのログ

ファイアーウォールとルータから取得したログについては、以下の項目を確認する。

・着信と発信のインターフェース
・発信元と宛先のIPアドレス
・使用プロトコル
・疑わしいポートに対するアクセス
・ポートスキャンのような特定のパターン

5.4.2　UNIXのログ

１）syslogd

UNIXでは、syslogdのデーモンを利用してログの採取を行っている。各サービスから出力されるメッセージをsyslog経由でテキスト形式のファイルへ出力する。syslogd経由でログを出力するためにプログラム（サービス）側とsyslogd（/etc/syslog.conf）側の両方の設定が必要である。

２）lastlog

各ユーザが最後にログインした情報を保存する。この情報は、lastlogを実行することで参照できる。

その他のユーザ情報を確認するコマンドとして以下のものがある。

・ユーザのログインやシステムのシャットダウン、再起動等の情報：lastコマンド（/var/log/wtmp）
・失敗したログインに関する情報：lastbコマンド（/var/log/btmp）
・各ユーザの最終ログイン時刻：lastlogコマンド（/var/log/lastlog）

lastlogの情報を利用して、各ユーザが前回ログインした時刻をチェックするように心がけることで、なりすましの検出が可能になる。

３）utmp

現在ログイン中のユーザー情報は、utmpバイナリファイルに記録される。これらの情報は、who、finger、usersコマンドで確認することができる。

４）wtmp

各ユーザのログイン/ログアウト、システムの再起動/シャットダウンのログ情報は、wtmpバイナ

リファイルに記録される。これらの情報は、lastコマンドで確認することができる。

5）acct

各ユーザが実行したコマンドのログ情報は、acctファイルに記録される。これらの設定は、デフォルトでは無効になっている。これらの設定を有効にする場合は、

/usr/sbin/accton ログファイル名

を実行すればよい。ログファイル名/var/log/pacctを指定することで、lastcommコマンドでログの表示が可能になる。

6）ログのフィルタリング

lastコマンドを使用すると大量にログが表示されるため、以下のオプションを指定することで、フィルタリングが可能になる。尚、lastbコマンドも同じオプション指定が可能である。

last -x reboot　　再起動の情報のみを表示
last -x shutdown　シャットダウンの情報のみを表示
last -n　　指定した行数のみを表示
last ユーザ名　　指定したユーザ情報のみを表示

lastlogコマンドについては、以下のオプションが指定可能である。

lastlog -t 日数　　指定した日数のログを表示
lastlog -u ユーザ名　指定したユーザ情報のみを表示

7）その他

システム起動時間を確認する場合は、uptimeコマンドを使用する。この情報を確認することで、不正な再起動を調査することができる。

/var/log/messsages、/var/log/secureファイルを参照することで、各サービスの情報が確認できる。

5.5　ログ分析

syslogで出力されるログについては、以下のようなキーワードに注意する。

表2.ネットワークサービスの主なキーワード

サービス	キーワード	想定される攻撃
ftp	Login incorrect	BruteForce攻撃
	passwd	Passwdファイルの不正入手・上書き
telnet	Authenticatin failed	BruteForce攻撃
	REPEATED LOGIN FAILURES	BruteForce攻撃
sendmail	reject	メールの不正中継
	rejected	不正なコマンドの実行
	allow,Sorry	不正なコマンドの実行
	Null connection	ポートスキャン
qpopper	-ERR POP EOF received	ポートスキャン
	-ERR Password supplied	BruteForce攻撃
halt	halted	不正なシャットダウン
reboot	rebooted	不正なシャットダウン
shutdown	reboot,halt,shutdown	不正なシャットダウン
login	ROOT LOGIN REFUSED ON	BruteForce攻撃
	ROOT LOGIN FAILURES ON	BruteForce攻撃
su	BAD SU	BruteForce攻撃
getty	〈tty〉	BruteForce攻撃
date	date set by	システム日付の不正変更

疑わしいアタックのパターンとして、以下のような例がある。

・毎日深夜に２回ログインを失敗する
・サーバが早朝に再起動する
・混雑しない時間帯に処理の停滞が発生する。

これらのパターンが検出された場合は、以下の点に注意してログ情報を調査する必要がある。

・異常な時間帯における正常な活動
・ベースラインを逸脱したユーザの活動
・ログイン、ファイルアクセス等の失敗
・シャットダウン、再起動（OS、サービス、デーモン）
・不明なファイルの存在
・急激なディスク空き容量の変動

5.6　メールヘッダの解析（SPAMメールについて）

SPAMメールを受信して、発信元を調べる場合はメールヘッダの解析が必要となる。SPAMメールの発信元を調べるには、Receivedヘッダを確認するのが基本となる。

Received：from AAA by BBB

上記の記述の場合は、サーバAAAからサーバBBBへメールが送信されたことを表す。複数のメールサーバによって転送される場合は、Receivedヘッダが複数存在して、下から順に記述される。

SPAMメールを受信した場合は、次の点について注意する。Fromヘッダのドメイン名とReceivedヘッダ、Message-IDヘッダのドメイン名と一致するかを確認する。この部分が一致しない場合は、発信元のメールアドレスが架空のメールアドレスの可能性がある。Receivedヘッダの偽造が可能であることから、この記述の信頼性について、IPアドレスの整合性を調べることが必要となる。

関連RFC：RFC822ARPAインターネットテキストメッセージの書式のための標準（STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES）

5.7　侵入発見後の流れ

侵入や攻撃が発覚した場合は、

・パニックに陥らない、冷静に判断する。
・手順書、マニュアルを確認する。

侵入や攻撃が発覚した場合の対処方法について、大まかな流れを以下に示す。

1）攻撃されたホストをネットワークから切り離し対処する

ネットワークから切り離して、進行中の攻撃を停止させる。（有線LANの場合：ネットワークケーブルを外す、無線LANの場合：無線の使用をOFFにする）尚、攻撃を受けたホストのシャットダウンの処理は、攻撃の追跡調査に必要な情報が失われる可能性がある。よって、シャットダウンの処理は最後の手段として考えるとよい。

2）被害を受けたホストを修復する

被害の大きい箇所から優先的に修復する。修復作業で一番重要なのは、作業内容や復旧内容を確認しながら、誤って事態を悪化させないようにする。

3）侵入、攻撃の被害状況を関係者に通知する

被害状況を通知する際は、Eメール等のインターネット以外の手段である電話やFAX等を利用する。

4）スナップショットを採取する

攻撃を受けたホストの内容を、DATやディスク

等に保存する。これらの情報を用いて、攻撃手法と脆弱性の調査に役立てる。
5）事後対策
・ハッカーに侵入された場合
ハッカーが侵入に利用したセキュリティホールを塞ぎ、ハッカーが改ざんしたもの、消去したもの、バックドアの作成、ログ等を調査する。最悪の場合は、システムの再インストールを行う必要もある。
・ハッカーに侵入が成功しなかった場合
確信犯的なケースの場合は、しばらく監視を強化して、関係者にも監視するように通知する。
6）インシデントの文書化
将来、同様の問題が発生した場合に備えて、適切な対応ができるように発生した事象について文書化しておくとよい。
7）不正アクセスの届け出を行う
最終的には、「独立行政法人 情報処理推進機構（IPA）セキュリティセンター（ISEC)」へ不正アクセス届出を行えばよい。
URL http://www.ipa.go.jp/security/ciadr/index.html

5.8 侵入発見後の処置（UNIXの場合）

5.8.1 ネットワーク切断前の作業

不正侵入を発見した場合は、これ以上被害が拡大しないように侵入されたホストをネットワークから切り離すことが必要になるが、その前段階でネットワークに接続された状況での情報収集が必要となる。
1）ホストにログインする
ハッカーに警戒されないように可能なかぎり別ホストからのリモートログインを行う。ログインする際には、一般ユーザでログインして、必要な場合にのみroot権限を使用する。
2）ネットワークの接続状況を確認する
ネットワークの接続状況を確認する際には、以下のコマンドを使用する。
・現在のログイン状況：w、whoコマンド
・過去のログイン状況：lastコマンド
これらの情報は、syslogのログが全て消去された場合には取得できない。
・ネットワーク接続状況とListenしているポートの確認：netstat an
不正なポートが確認された場合には、そのポート番号と接続時刻をメモをとって控えておく。
3）プロセスの確認
不審なプロセスの起動状況の確認：ps axf
不審なプロセスが確認された場合には、プロセス名、起動パスについてメモを控えて、後で調査する。
4）設定ファイルの確認
以下のファイルを参照して、不審なプロセスの起動設定がないかを確認する。
確認するファイル
・/etc/passwd,inetd.conf,crontab
・/etc/rc.d/rc,rc.boot,rc.local
確認するディレクトリ
・/etc/rc.d/init.d,rc2.d,rc3.d,rc4.d,rc5.d,crond

5.8.2 ネットワーク切断後の作業

以下の作業は、rootで行う。この作業を行う前にスナップショットを採取しておくとよい。
1）rootのコマンド履歴の確認
rootのコマンド実行履歴を確認して、不審なコマンド実行がないかを確認する。
2）syslogの確認
syslogの情報がハッカーによって消去されていなければ、OSの再起動、ログインの拒否、デーモンメッセージの異常について確認する。
3）不審なプロセスの確認
ネットワークを切断する前に確認された、不審なプロセスや不審なポート番号等について調査する。
・発信元ネットワーク、接続時刻の確認
w,whoコマンド、lastログ、syslog等
・コマンド履歴の確認：suコマンドの不正使用、不正なプログラムのコンパイル
・不正侵入に悪用されたアカウントの正規利用者のログイン状況
netstatコマンドでの接続状況を確認した際に、不審なポートに対する接続が発見された場合には、「バッファオーバーフロー攻撃」と「バックドアへの接続」が想定される。この場合は、不審なポートのオーナを調査するために
fuser -vn tcp/udp ポート番号
ポートとプロセスの関係について確認するには「lsof i」、「netstat -lp」
を実行すればよい。
4）不審なファイルの確認
バックドアが仕掛けられた場合等は、どこかに不審なファイルが残っていたりするため、以下のようなコマンドを実行して、不審なファイルを検出する。
・.で始まるファイル名、ディレクトリ名の検索
find / -name‘.’* -print
・所有者がrootであるファイルの検索
find / -user root
・所有者がrootで、所有者権限で実行可能なファイルの検索
find / -user root -perm -4000 -ls
・更新日付が不審なファイルの検索
x日前に更新されたファイルの表示:find / -mtimex
5）パッケージの整合性の確認（Linuxの場合）
rpmパッケージを利用している場合には、
rpm -Va
上記のコマンドでパッケージの整合性を確認することができる。ただし、構築時に設定ファイルを変更している場合には、不整合と表示されるため注意が必要である。

6．セキュリティ診断・監視

6.1 脆弱性検査

ネットワーク・セキュリティ・スキャナであるnessusを用いて、遠隔地から特定のネットワークを監視して、ハッカーからの被害を受ける可能性をチェックしている。nessusは、サーバ/クライアント型のツールである。
・2004年２月現在のバージョン：2.0.10
・URL：http://www.nessus.org/
・他に必要なツール：GTK+,nmap,openssl
・nessusの設定方法
専用のユーザをnessus-addusersコマンドで作成する。サーバ/クライアント間でSSL通信で使用するためのサーバ証明書（公開鍵と秘密鍵のペア）を

nessus-mkcertコマンドで作成する。
・nessusの動作確認
　クライアントからサーバ（nessusd）へ作成した専用ユーザでログインして、検査するホストやネットワークをチェックする。

6.2　侵入検知システム（IDS：Intrusion Detection System）

　侵入検知システムは、ログやパケット情報を基にして不正侵入を検出するシステムである。
侵入検知システムを導入することによって、
・脅威の確認
・不正侵入の早期発見
・不正侵入の抑止
・管理者の負担軽減
以上の効果が得られる。

6.2.1　侵入検知システムの種類

１）ホストベース侵入検知システム
　ホストベース侵入検知システム（ホストベースIDS）は、OSや各種アプリケーションが生成するログ情報を用して不正侵入を検出する。通常は、保護対象のホストに導入する。
２）ネットワークベース侵入検知システム
　ネットワークベース侵入検知システム（ネットワークベースIDS）は、LANを流れるデータを監視して不正侵入を検出する。スイッチングハブを導入している場合は、注意が必要である。

6.2.2　侵入検知に関わるセキュリティ対策

　ネットワークベース侵入検知システムであるSnortを用いて、侵入検知を行っている。
・2004年２月現在のバージョン：2.1.1
・URL：http://www.snort.org/
・日本Snortユーザ会（Japan Snort Users Group）
　URL：http://www.snort.gr.jp/
・他に必要なツール：libpcap,openssl
・設定ファイル
　ルールセットを利用するためにsnort.confを編集して、専用ユーザ（snort）を作成する。
・Snortの動作確認方法
　有効にしたルールセットに値する攻撃を試みて、Snortのログに記載されるかをチェックする。

6.3　改ざん検出

　トロイの木馬やWebサーバのコンテンツの改ざん等の改ざんをチェックするシステムである。一般的な仕組みとして、以下の処理を行う。
１）MD5、SHA-1等のハッシュ関数の出力結果を事前に保存する。
２）定期的にハッシュ関数を実行して、事前に保存しておいた値と比較する。
３）ハッシュ関数の値が一致しなければ改ざんされたと判断する。

6.3.1　ファイル改ざんに関するセキュリティ対策

　システム内のディレクトリやファイルの書き換えをチェックを行うためのツールとしてTripwireを導入した。
・2004年２月現在のバージョン：2.3-47（フリー版）
・URL：http://www.tripwire.org/
・Tripwireの設定方法
　１．設定ファイルの作成、２．ポリシーファイルの作成、３．ベースラインデータベースの作成の順番となる。
・Tripwireの動作確認
　整合性・レポートをチェックして、ポリシーファイルの調整を行いながら、データベースを管理する。

6.4　盗聴検出

　有線LANの場合は、LANアナライザで利用されるpromiscuousモードで盗聴が行われる。今現在では、promiscuousモードで動作するマシンを検出するツールが存在する。

6.4.1　promiscuousモードで動作するマシンを検出する方法

・ネットワーク上に存在しないIPアドレスにデータを送信して反応を調査する。
・調査対象の全てのマシンにICMPメッセージを送信して、レスポンスタイムを計測する。
・ブロードキャストに対するOS固有の動作とアドレスの解釈を調査する。
・ブロードキャストアドレスの変形を指定したARPの応答を調査する。

6.4.2　盗聴検出ツール

　盗聴を検出するツール「PromiScan」がある。このツールは、Windowsのみで動作する。
・2004年２月現在のバージョン：0.27（フリー版）
・URL：http://www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html
・他に必要なツール：WinPcap
　このようなツールを用いて、盗聴の可能性を検出することが可能となる。

7．おわりに

　筆者は情報セキュリティに携わって以来、独学で対応してきた。今回、国立情報学研究所が主催した平成15年度第３回情報セキュリティ担当職員研修上級コースを受講して、今まで抱えていた誤解を解決することができ、新たな知識・技能を修得することができた。今後の技術・技能のスキルアップを図る上で、今回修得した技術・技能を発展させていきたい。