セキュリティ上の脅威

2002年9月17日

牧之内研D3 尾下真樹

内容

- セキュリティ上の脅威
- 電子メイルにおける脅威
- ウェブサーバにおける脅威

F) セキュリティ実験

35) セキュリティ上の脅威説明

2001年9月10日

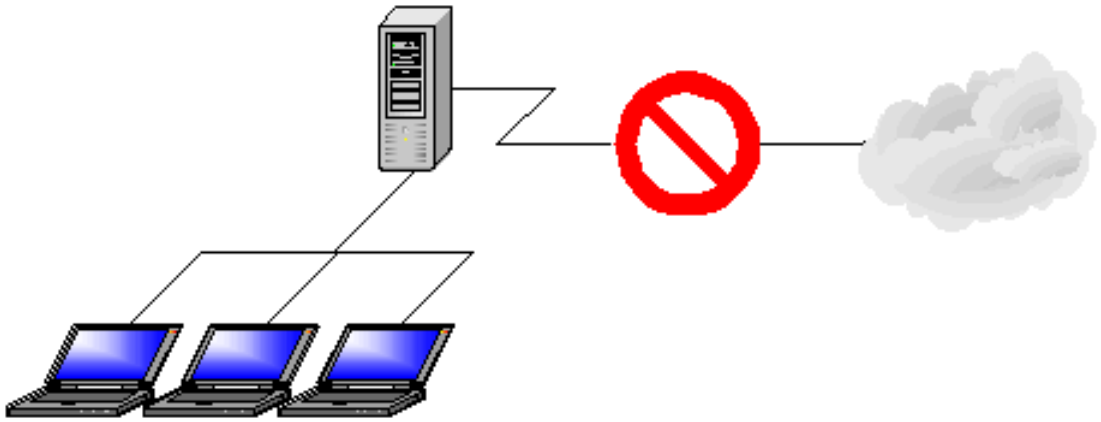
牧之内研究室　学部4年

石川　卓司

ネットワークをとりまく脅威と現状

現在インターネット上ではあちこちで、直接攻撃を受ける、または踏み台として他ネットワークへの攻撃に利用されるということが発生しています。

しかし、闇雲にセキュアな環境を目指すことはできません。 その一つが利便性に問題が出てくるという点です。



物理的に切り離すことによるセキュアな環境

セキュリティ上、「安全である」「大丈夫である」ということは、 構築した時点では言えるかもしれません。 しかし、時間の経過と共にそれはどんどん陳腐化していきます。

セキュアな環境を維持する3要素

最新セキュリティ情報の入手

新たな問題に対する対処

日常の監視

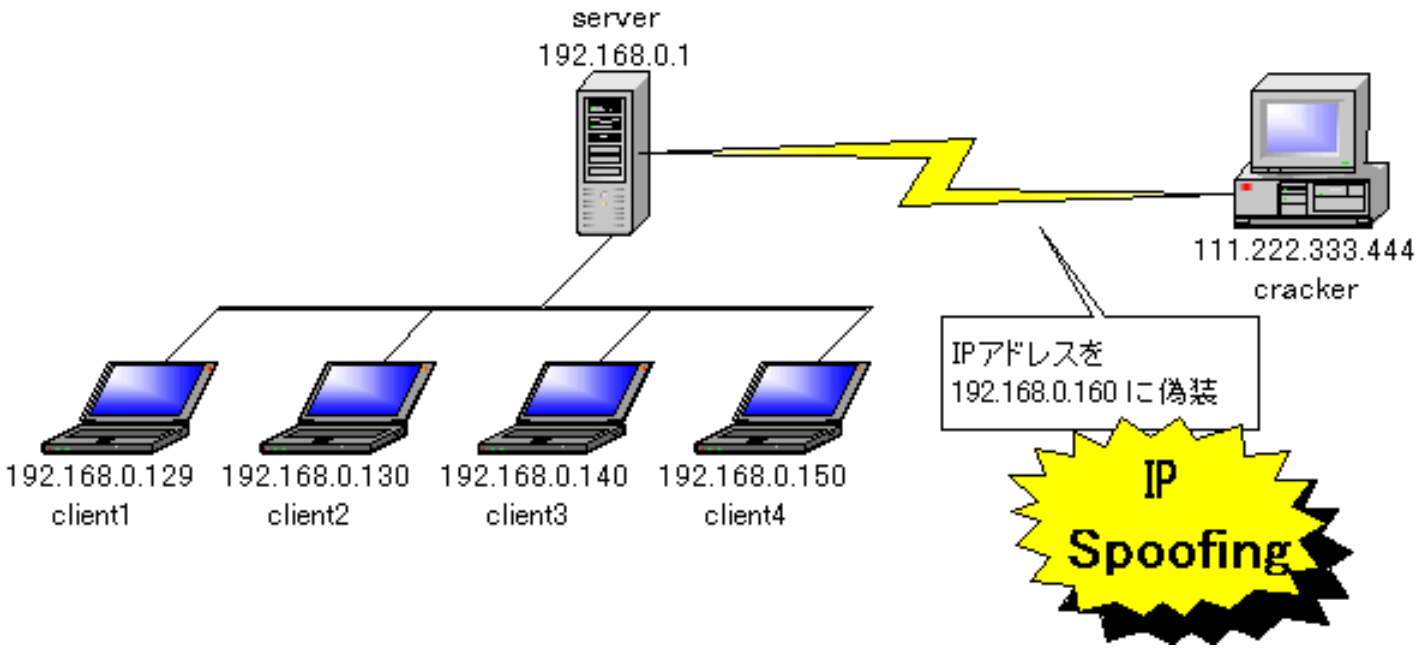
実際にどのような攻撃があるのか

攻撃の実例

ポートスキャン	リモートアクセス
spam	パスワード解析
IP Spoofing	盗聴
DoS	リモートアクセス
バックドア	リモートコントロール
トロイの木馬	Web Page改竄
スクリプト	プロキシの不正利用

IP Spoofing

IP Spoofingとは、IPアドレス偽装攻撃とも呼ばれ、基本的な手法の一つです。



IP Spoofingの一例

rコマンドの危険性

r系コマンドでは、/etc/hosts.equivや.rhostsが信頼しえるホストかどうかの判断に使用されます。 これらのファイルに記述されたホストは信頼できるホストであると判断し、以降の認証が行われません。

例えば、/etc/hosts.equivに以下のようなデータが書かれていた場合を想定します。

host1.sample.com

host2.sample.com

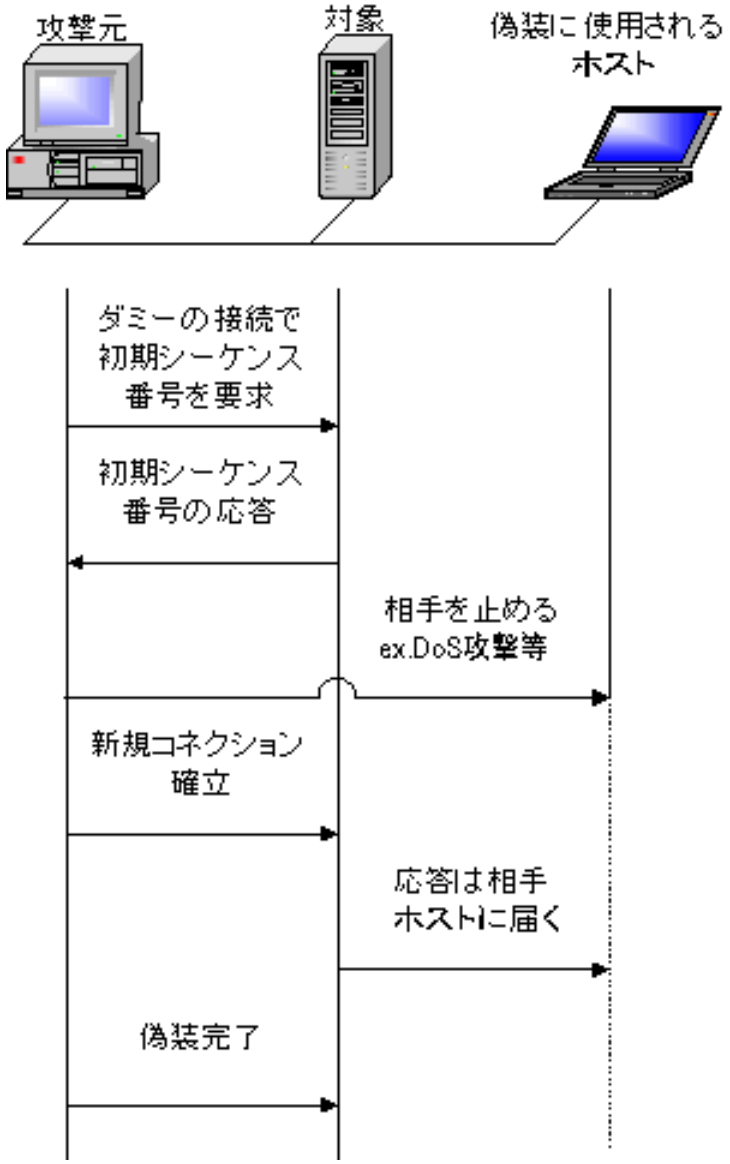
host3.sample.com yamada

この例では、host1とhost2の全ユーザ、host3のユーザであるyamadaさんに関しては、 r系コマンドにおいてパスワードの認証は行われません

IP Spoofingの原理

　まず、攻撃側はr系コマンドを使用する場合、 信頼されているホストを知る必要があります。

　r系コマンドを使用せず、他のホストになりすまし、そこからの攻撃に見せかける場合はそのIPアドレスを知るだけで済みます。



IP Spoofingの原理

シーケンス番号

　シーケンス番号は、TCP/IPのパケットに一連の番号を割り振り、パケットの順序などを識別するために使用されます。パケットを受け取ったホストでは、エラーチェックを行い、正しく受け取った場合は送信元に対してどのシーケンス番号を受け取ったかの応答を行います。

　もし、シーケンス番号の推測に成功すれば、セッションを確立することができます。 そして、攻撃する側のホストが信頼されることとなり、認証が緩くなります。

※シーケンス番号を使用する方法は、現在では古典的な方法であり、 容易には行えません。

DoS攻撃

DoSとは"Denial Of Service"のことで提供するサービスの妨害や停止させるものを指します。

サービスを妨害する攻撃は以下の2種類に分けることができます。

過負荷をかけるもの

例外処理ができないもの

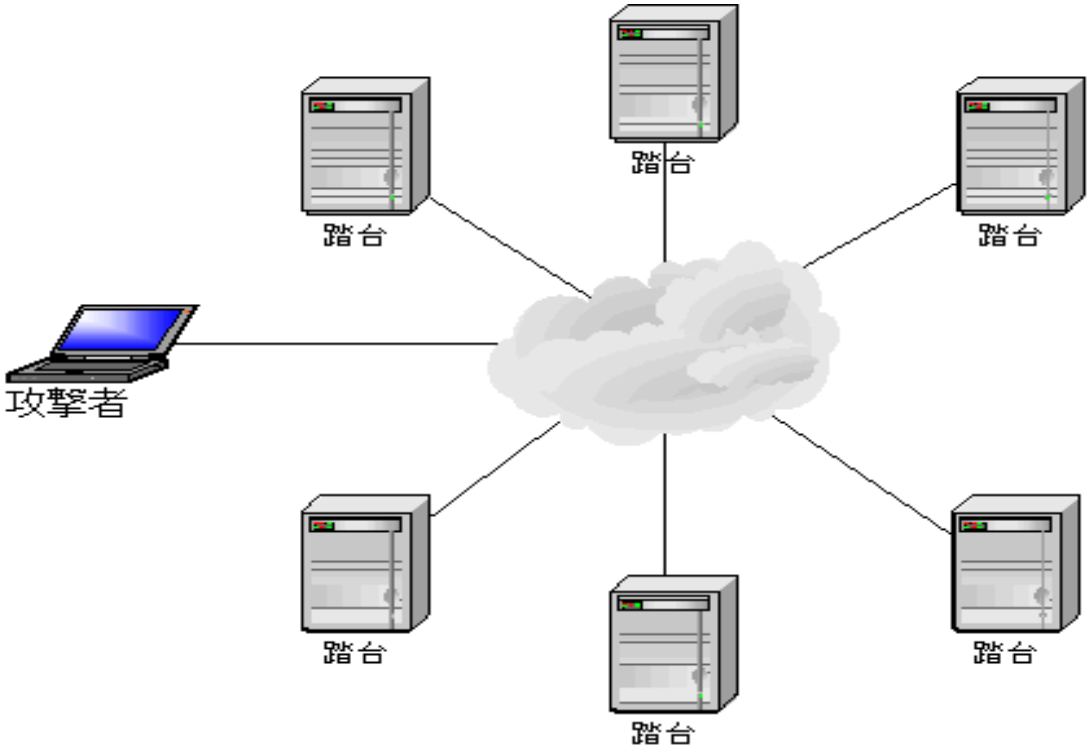
DoS攻撃は、特定の手法を指すものではありません。 言葉の通りサービスの妨害や停止を行う攻撃全般を指す総称です。

DoSの種類

種類	概要
mail bomb	巨大なメールや大量のメールを送りつけメールサーバのディスクやCPU資源、 ネットワークの帯域を潰す。
finger	fingerコマンドで引数の状態によって相手を停止させる。
SYN flood	プロトコルスタックを使用した攻撃の原型。接続要求(SYN)の処理における仕様を突いたものです。防御としてはSYN cookiesというものがあります。
Ping of Death	TCP/IP プロトコルスタックの実装のバグに対する攻撃。
ping flood	pingコマンドで引数の状態によって相手を停止させる。
OOB	ポート139に対しOut of Bandデータを送り相手を停止させる。
Land/Latierra	SYNパケットを送信し相手側を無限ループに陥らせる。
TearDrop/Bonk/Boink	フラグメントパケット処理の実装によって相手を停止させる。
Octopus	相手に対し多くのコネクションをターゲットサーバに張り運用ができないようにするもの。
SSPING/Jolt	ICMPパケットの仕様を利用したもの。
UDP Storm	echoサービスの問題点を利用したもの。

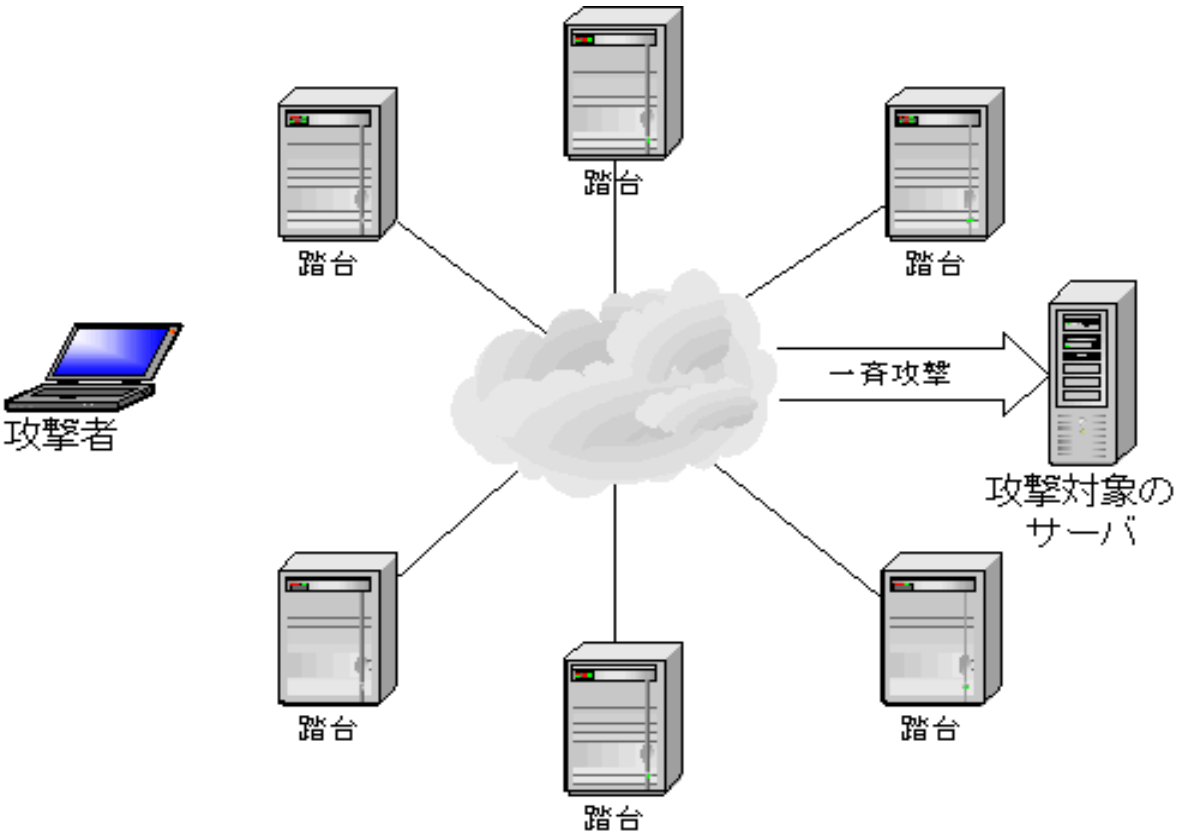
DDoS

　DoS攻撃は単体では行われなくなってきました。 DoSに代わって行われ、強力な威力を持っている手法がDDoSです。
これは、"Distributed Denial Of Service"の略で、DoS攻撃を行うホストがネットワーク上に分散しているものです。
　そして、DDoSは防御の難しい手法の一つです。



踏み台となる各ホストにDDoSのモジュールを埋め込む

DDoSのモジュールに対し、何日の何時何分にどのホストを攻撃するのか設定を行っておきます。 これによって設定した日時に指定されたホストを一斉に攻撃することができます。



時刻や特定のパケットで一斉に攻撃を行う

プロキシサーバの不正利用

アクセス制御を行っていないプロキシサーバは、不特定多数から探索を受けている可能性があります。存在を探知されると、予期しないアクセス中継に悪用される可能性があり、他サイトへの攻撃の踏み台、機密情報への不正アクセスなどが行われます。

踏み台にされると、何もしていないのに、加害者にされてしまい、クレームの対応などに追われることになります。

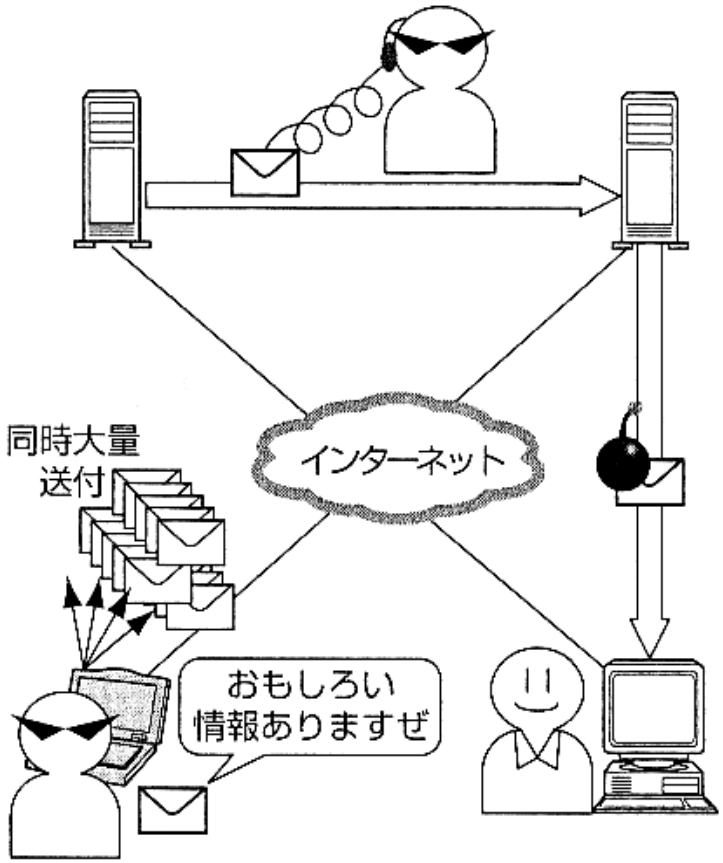
また、信用を損なうなどの被害が発生します。

輪講:電子メールにおける脅威

2001年7月13日

牧之内研D2　尾下 真樹

電子メールにおける脅威



- サーバ
- 通信路
- クライアント
- ユーザ

図は「基礎から分かるTCP/IP」（オーム社）p.217 より

サーバにおける脅威

- サーバへの侵入
  - セキュリティホールを突いた攻撃
  - 対策：頻繁にセキュリティホールを塞ぐ
- 高トラフィック攻撃
  - サーバの許容量を超えるようなメイルを送りつける
  - 対策：ファイアウォールの設置

通信路における脅威

- 通信路を流れる認証情報の盗聴
  → 対策：サーバ・クライアント間通信の暗号化
  – POP3・・・パスワードをそのまま送る
  – APOP・・・パスワード・本文を暗号化して送る
    （設定すると POP3 は使用不能になる）
- 通信路を流れるメイルの盗聴・改ざん
  → 対策：電子メイルの暗号化（PGP）

クライアントにおける脅威

- ウィルス
  - 添付ファイルを実行するとウィルス
  - 対策：メイラーのセキュリティ設定
- 高トラフィック攻撃
  - SPAM
- コンピュータの盗難、不正操作

ユーザにおける脅威

- ソーシャルエンジニアリング
  - アカウント・パスワードの漏洩
    - 対策：安直なパスワードをつけない
    - 対策：パスワードのメモなどを残さない
  - うそメイル
- なりすまし
  - アカウントの漏洩によるなりすまし

気をつけること

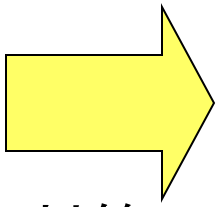
- ユーザとして
  - パスワードの管理
  - コンピュータを放置して席を立たない
  - できる限り APOP を使う
  - そもそも重要な情報はメイルには書かない
  - もし書くとしたら暗号化（PGP、その他）
  - ウィルス対策
- 管理者として
  - メイルサーバのセキュリティ、ファイア・ウォール
  - 上記の注意点を他のユーザに徹底

Webサーバにおける脅威

牧之内研究室
修士2年
中野　裕也

Webにおける脅威

- 侵入
- なりすまし
- 事後否認
- 盗聴
- 改竄
- ウィルス



- ファイアウォール
- ワンタイムパスワード
- ディジタル署名
- データ暗号化
- SSL
- ウィルスチェッカ

改竄の目的

- 愉快犯
- 政治的主張
- 技術力の誇示
- 実利

- ネットワーク上を流れるメッセージの改竄
- 不正侵入によるデータの改竄

Webページの改竄

本来提供していたページが第三者による改竄や、全く別のページと入れ替わること

- 直接の侵入による改竄
  - ページを書換ることのできるアカウントを取得
- DNSのエントリを書換ることによる改竄
  - 攻撃者が用意したWebサーバを指し示すように書き換え
- whoisエントリを書換ることによる改竄
  - 管理者を装いDNS書換の申請

Web改竄対策

- 要因である侵入に対する対策
  - 未使用、不必要なサービスの停止
  - アクセス制限
  - 不適切なCGIプログラムを削除
  - 未使用、不必要なポートまたはプロトコルによる接続を排除
  - 適切なパスワードについてのポリシーを設定
- 被害の軽減
- 侵入の検出
- 事後対応