



UNIX系サーバのセキュリティ概要

富士通株式会社
コーポレートIT推進本部 fujitsu.com室
城崎 徹



目次

1. UNIXにおけるセキュリティホール
2. サーバアプリケーションの設定
3. 運用時の注意事項
4. 被害にあった時には



1. UNIXにおけるセキュリティホール



UNIXでの被害状況

U1 BIND Domain Name System

U2 Web Server

U3 Authentication

U4 Version Control Systems

U5 Mail Transport Service

U6 Simple Network Management Protocol

U7 Open Secure Sockets Layer (SSL)

U8 Misconfiguration of Enterprise Services NIS/NFS

U9 Databases

U10 Kernel

SANS(<http://www.sans.org/top20/>)調べ



日本におけるセキュリティ被害件数

■ JPCERT及びIPAに対する不正アクセス届出件数

| 1999年 | 2000年 | 2001年 | 2002年 | 2003年 | 2004年 |
|-------|-------|-------|-------|-------|-------|
| 843件 | 2375件 | 3403件 | 1435件 | 3457件 | 5811件 |

IPA発行 「情報セキュリティの現状200x年」より

■ 警察庁に報告のあった不正アクセス届出件数

| 2000年 | 2001年 | 2002年 | 2003年 | 2004年 |
|-------|--------------------|-------|-------|-------|
| 106件 | 1253件 ¹ | 329件 | 212件 | 356件 |

警察庁発行 不正アクセス行為の発生状況より

¹ 813件はワーム被害



近年の特徴

- 攻撃コードが出現するまでの期間短縮
- WebApplicationへの攻撃
 - Cross Site Scripting(XSS)
 - OSコマンド/SQLコマンドインジェクション
- sshなどへの Brute Force 攻撃
 - 辞書は日々更新されている
 - ツールの改良(悪?)
- 情報の漏洩
 - 直接のダメージはないが、攻撃のヒントに
- クライアントへの攻撃



パッチだけで十分なのか？

パッチを適用することで，脆弱性への直接的な攻撃を防ぐことはできる．

しかし，パッチの適用だけでは ，

- (初期)設定による問題点
- 脆弱ではないが攻撃の足がかりになるような情報の漏洩

といった問題点を解決できない．



2. サーバアプリケーションの設定



DNS

- 不必要なゾーン情報の公開防止
- 再帰問い合わせの防止
- キャッシュ汚染の予防
- バージョン情報の隠蔽



DNSにおける脅威

脅威

- ゾーン情報による内部情報などの漏洩
- キャッシュ汚染

```
# dig @dns.example.org example.org axfr
; <<>> DiG 9.2.2 <<>> @dns.example.org axfr
...
;; XFR size: 10 records
```

バージョン情報の漏洩

```
# dig @dns.example.org version.bind chaos txt
...
;; ANSWER SECTION
Version.bind.      0      CH      TXT      "9.2.1"
```



BINDにおける対策

named.conf

```
options {
    version "unknown";
    fetch-glue no; # BIND 8
};
zone "EXTERNAL" {
    allow-transfer { SLAVE1; SLAVE2; }
    match-client { any; }
    recursion no;
};
zone "INTERNAL" {
    allow-transfer { none; }
    match-client { 192.168.0.1/24; }
    recursion yes;
};
```



設定の確認方法

ゾーン情報の転送

```
# dig @dns.example.org example.org axfr
; <<>> DiG 9.2.2 <<>> @dns.example.org axfr
...
;; Transfer failed.
```

バージョン情報の確認

```
# dig @dns.example.org version.bind chaos txt
...
;; ANSWER SECTION
Version.bind.          0      CH      TXT      "unknown"
```



Webサーバ

- HTTP TRACEの無効化
- バージョン情報の秘匿
- 保護が不十分な情報の削除
- WebApplicationでの対策



HTTP TRACEの無効化(Apache)

脅威

HTTP TRACEが有効で，XSSの脆弱性が存在すると，
Basic認証の情報を抜き取ることが可能

(US-CERT VU#867593)

httpd.conf

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

- httpsを使用時には個別に設定が必要
- VirtualHost機能使用時も個別に設定が必要
- mod_rewriteを組み込むリスク



HTTP TRACEの無効化の確認(Apache)

TRACEが無効になっているかの確認

```
# telnet www.example.org 80
TRACE / HTTP/1.1
Host: www.example.org
<改行のみ>
HTTP/1.1 200 OK
...
```

ステータスコード(上記下線部分)を確認

200: HTTP TRACE有効(脆弱性あり)

400: コマンド入力ミス

403,404: HTTP TRACE無効(脆弱性なし)



バージョン情報の隠蔽(Apache)

脅威

バージョン情報だけでなく，OS，モジュール情報も漏洩

httpd.conf

```
ServerToken ProductOnly
ServerSignature Off
```

バージョン情報が隠蔽されているかの確認

```
# telnet www.example.org 80
HEAD / HTTP/1.0
<改行のみ>
HTTP/1.1 200 OK
Data: Sat, 21 Aug 2004 04:12:03 GMT
Server: Apache( )
```

ソースを改造することで，“Apache”も隠蔽可能



保護が不十分な情報

- Directory Indexが有効になっていないか
- Webサーバ上に、バックアップファイルが残っていないか
/backup , /test , backup.zip , *.bak
など推測しやすい名前は特に危険
- 管理者画面が外部に公開されていないか
- 不必要なファイルが残っていないか
/manual/ , index.html.* など



Webサーバの監査ツール

■ 443/tcpへの監査方法

- [stunnel](http://www.stunnel.org/)(<http://www.stunnel.org/>)
- [OpenSSL](http://openssl.org/)(<http://openssl.org/>)
 - `openssl s_client -connect <IP Address>:<Port> -state`

■ 監査ツール

- [nikto](http://www.cirt.net/)(<http://www.cirt.net/>)
- [N-Stealth](http://www.nstalker.com/nstealth)(<http://www.nstalker.com/nstealth>)



WebApplicationでの対策

- 入力チェック
 - 入力画面だけでなく，処理する側でもチェック
 - hidden の値もチェックが必要
- サニタイジング
 - 危険な文字を無効化
- エラー画面で， unnecessaryな情報を出力しない
 - データベースのエラーコードなど



メールサービス

- expn / vrfy による情報流出防止
- オープンリレーしないために
- バージョン情報の隠蔽



expn / vrfy による情報流出

脅威

- ID(メールアドレスの流出)
- 取得したIDを利用した攻撃(sshなどへの攻撃に利用)

```
# telnet mail.example.com 25
220 mail.example.com ESMTP Sendmail 8.XX.XX
HELO test.example.com
250 test.example.com Hello .....
EXPN fuji
550 5.1.1 fuji... User unknown
EXPN toru
250 2.1.5 toru@mail.example.com
```



expn / vrfyの無効化(sendmail / Postfix)

sendmail.cf(sendmail)

```
# privacy flags
O PrivacyOptions=authwarnings,noexpn,novrfy
```

sendmail.mc(sendmail)

```
define(`confPRIVACY_FLAGS',
        `authwarnings,noexpn,novrfy')
```

細かく制御しないなら，“goaway”でも

main.cf(Postfix)

```
disable_vrfy_command = yes
```

qmailは無効化されている



expn / vrfy の無効化の確認

```
# telnet mail.example.com 25
220 mail.example.com ESMTP unknow
HELO test.exaple.com
250 test.example.com Hello ....
EXPN fuji
502 5.7.0 Sorry, we do not allow this option
VRFY toru
252 2.5.2 Cannot VRFY user; try RCPT to attempt
delivery (or try finger)
```



SMTPオープンリレーによる不正中継

脅威

設定が不十分なSMTPサービスは、スパムE-mailなどの中継に利用されることがある

```
# telnet mail.example.org 25
220 mail.example.org ESMTP unknown
MAIL FROM: spam@spam.com
250 2.1.0 spam@spam.com
RCPT TO: spam@ahoo.com
250 2.1.5 spam@ahoo.com
DATA
...
```



不正中継対策

対策

リレーを許可するサイトの指定

```
# telnet mail.example.org 25
220 mail.example.org ESMTP unknown
MAIL FROM: spam@spam.com
250 2.1.0 spam@spam.com
RCPT TO: spam@ahoo.com
550 5.7.1 Unable to relay for spam@ahoo.com
```

InterScan VirusWall for UNIX などでは，構成によっては sendmailなどの不正中継だけでなく，InterScanの設定も必要

監査サイト

- ORDB(<http://www.ordb.org/>)



バージョン情報の隠蔽(sendmail)

sendmail.mc

接続時のバージョン情報の隠蔽(sendmail)

```
define(`confSMTP_LOGIN_MSG', 'unknown')dnl
```

メールヘッダ内からの隠蔽

```
define('confRECEIVED_HEADER', '$?sfrom $s
.$?_($?s$|from $.$_)
.$?{auth_type}(authenticated)
$.by $j (unknown)$?r with $r$. id $i$?u
for $u; $|;
.$b')dnl
```

接続時のバージョン情報の隠蔽(Postfix)

```
smtp_banner = $myhostname ESMTP unknown
```



その他のサーバアプリケーションでの設定

- Brute Force 攻撃への対策
- SNMPによる情報漏えいの防止
- HTTP Proxy による第三者中継の防止



ユーザパスワードに対するBrute Force攻撃

脅威

ID/Password 認証を使う限り Brute Force 攻撃に弱い

対策

より強固な認証(RSA認証など)の設定が求められる

sshd_conf

```

RSAAuthentication yes
RhostsAuthentication no
RhostsRSAAuthentication no
PasswordAuthentication no
PerimetRootLogin no
PerimetEmptyPassword no
AllowUsers user1, user2, ...
    
```



SNMP

脅威

- 管理情報，ネットワーク情報の漏洩
- 管理情報を変更

対処

- 必要なければ停止，可能ならば削除
- コミュニティ名のデフォルト値の変更
 - 標準の“public”や“private”
 - ルーターなども忘れずに
- SNMPエージェントのアクセス元を制限

監査ツール

- ADMsnmp(<http://adm.freelsd.net/ADM/>)
- snmpwalk(<http://net-snmp.sourceforge.net/>)



HTTPプロキシ

脅威

- 攻撃の踏み台(SPAM, 他のサイトへの攻撃)
- 内部ホストへのアクセス

```
# telnet proxy.example.com 80
CONNECT mail.example.org:25 HTTP/1.0
<改行のみ>
HTTP/1.0 200 Connection established
220 mail.exaple.org ESMTP ...
```

ステータスコード(上記下線部分)を確認
 200: HTTP TRACE有効(リレー可能)
 403, 405: CONNECT無効(リレー不能)



HTTPプロキシによる第三者中継の防止

対処

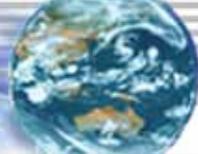
- 内部から外部へのProxyサーバならFireWallなどで外部からの接続を遮断
- ForwardingProxyならば，転送先を制限
- 設定ファイルで適切なアクセス制限

squid.conf

```
acl office src 192.168.1.0/255.255.255.0
http_access allow office
```

監査ツール

- pxytest(<http://www.unicom.com/sw/pxytest/>)



よりセキュアなサーバにするために

- 不必要なサービスは停止・削除する
 - inetd経由(echo , fingerなど)のサービス
 - netstat , nmap
 - RPC(NIS , NFSなど)
 - rpcinfo -p <IP アドレス>
 - R系サービス
 - X-Window
- よりセキュアな運用
 - NIS+ , LDAPなどへの切り替え
 - 必要なときのみ起動するなど , 運用回避



よりセキュアなサーバにするために

- 不必要なコマンドの削除
 - cc(gcc) , wgetなどのアプリケーション
- OSレベルでの防御
 - 不必要な setuid , setgid 設定をなくす
 - iptable , TCP wrapper などによるアクセス制限
- FireWallの設定
 - 中 外のアクセスも制限
- chroot などの利用
 - 被害に合った場合の影響を最小限に

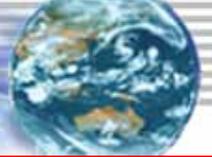


まとめ

- 情報の漏洩の抑止
 - 不必要な情報を漏らさない
 - アカウント情報だけでも，攻撃の足がかりになる
- チェック
 - ツールなどを利用し，リモートからチェック
- サーバの要塞化
 - アプリだけでなくサーバ自身でも防御



3. 運用時の注意事項



メンテナンス

■ パッチの適用

- 緊急度の高いものは即日
- OSだけでなくサーバアプリも
- 緊急度が低いものも定期的に適用

■ サポートが切れたものは使わない

- メンテナンスが終了したOSやソフトウェアを使い続けない



ログの取得

- ログの保存
 - DATなどの記憶媒体に保存が望ましい
- ログの確認
 - ログの量(行数, サイズなど)だけでも日々確認
 - 監視ツールの活用
 - Logwatch : 定期的にログの報告
 - swatch : イベント発生時に動作(通知, コマンド実行等)
- 余裕があれば統計情報なども
 - analog / MRTG

異常状態を知るには定常状態を知る



ログの取得(もしもの為に)

■ FireWallでもログの取得

- Acceptログの取得
- FireWall-1 では , Short Logでも十分

■ 時刻の同期

- ntpなどを利用し , サーバやFireWallの時刻の同期

■ ログサーバの構築

- ログの改ざんなどを防ぐことができる
- ただし , UDP通信なので取りこぼしの恐れがある



定期的な監査

- サーバ自身の改ざんチェック
 - chkrootkit(<http://www.chkrootkit.org/>)
 - tripwire(<http://www.tripwire.co.jp/>)
- 定期的によりリモートより監査
 - Nessus(<http://www.nessus.org/>)
 - QualysGurad(<http://segroup.fujitsu.com/secure/service/attacktest-express/index.html>)

ただし，万能ではないので過信しない



まとめ

- パッチの適用は大事
 - 直接的な攻撃を防ぐ
- 日々の確認が大事
 - 定常状態を知ることによって、異常状態を知る
- ログの保存も大事
 - もしもの時の為、可能な限り取得/保存しておく



4. 被害にあった時には



初期対応

- 当該マシン(セグメント)をネットワークから切り離す
 - 被害の拡大を防ぐ為
- 被害を発見した状況と時刻を記録する
 - 可能であれば，サーバ内時計の誤差も確認
- 関係者に速やかに連絡し，体制を整える
 - 組織として，迅速に決断・行動ができる体制を整える
- 被害マシンで操作を行わない
 - 被害の有無を確認する際も，作業内容を記録し，最小限に

証拠データの保全に細心の注意を

担当者ベースで行動せず組織全体で



警察への連絡

■ 相談先

各都道府県警察本部のハイテク犯罪相談窓口

<http://www.npa.go.jp/cyber/soudan.htm>

■ 届出先

被害者(被害団体・企業)の居所，または，サーバの所在地を管轄する警察署など

被害届けを出す前に相談しておくが良い



インシデント報告

■ JPCERT/CC

- <http://www.jpccert.or.jp/form/>
- 電子メール : info@jpccert.or.jp
- FAX : 03-3518-2177

■ 情報処理推進機構(IPA) ISEC

- <http://www.ipa.go.jp/security/todoke/>
- 電子メール : crack@jpa.go.jp
- TEL : 03-5978-7509
- FAX : 03-5978-7518



復旧

■ 代替機を用意

- 証拠保全の為，別マシンを用意するのが望ましい
- 最悪，HDDだけでも交換(被害HDDは保管)

■ クリーンインストールが良い

- できれば原因が解析できるまで待つのが良い
- バックアップの適用は慎重に

■ 監視強化

- 一度被害にあったマシンは標的になりやすい
- ログの監視、確認など重点的に



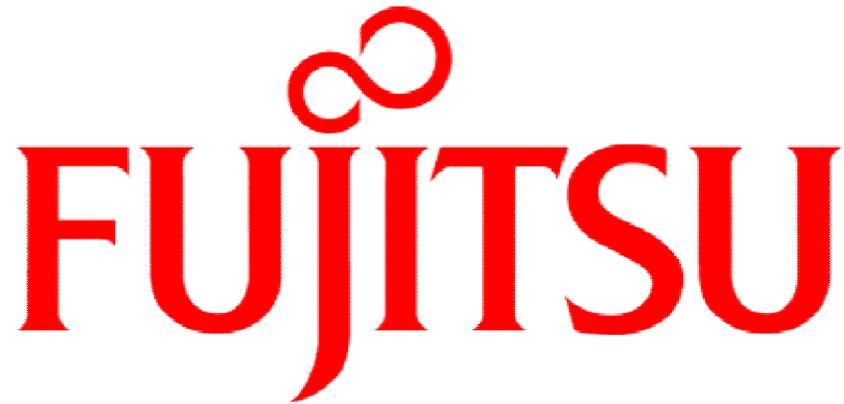
まとめ

- 関係者に速やかに連絡し対応体制を整える
 - 担当者だけで行動しない
- 被害マシンのデータ保全を行う
 - LANを抜き，被害の拡大を防ぐ
 - 不必要な操作は行わない
- 復旧には十二分の注意を
 - できる限りクリーンインストール
 - 監視強化(標的になりやすい)



最後に

- やっぱり，パッチの適用は大事
- その上で， unnecessaryな情報を与えない設定を
 - 攻撃の足がかりを与えない
- 当たり前の対策を確実に
 - 強固なパスワード，アクセス制限など
- 日々の運用
 - まずはサーバの定常状態を知ることから



FUJITSU

THE POSSIBILITIES ARE INFINITE