

## Linux Conference 2002

### インターネットアプリケーションにおける オープンソースシステムのセキュリティ確保

岡田 良太郎

株式会社テックスタイル  
104 0045  
東京都中央区築地2-1-14トミービル5F  
03 5148 5019 / fax 03 5148 0114  
<http://techstyle.jp/>  
[info@techstyle.jp](mailto:info@techstyle.jp)

September, 2002

## - はじめに

- Linux はLinus Torvalds の米国およびその他の国における登録商標あるいは商標です。
- X Window System は、X Consortium, Inc.の商標です。
- Red Hat は、米国 Red Hat Software, Inc. の登録商標です。
- その他、記載されている会社名、製品名は各社の登録商標または商標です。
- 本資料の著作権は岡田良太郎に帰属します。



September, 2002

WEB 改ざん、クロスサイトスクリプティング、データ漏洩の問題が頻発する中、オープンソース基盤のアプリケーションは増大の一途をたどっている。ベンダー保守や開発会社依存のできないオープンソースシステムにおいて、セキュリティ品質確保のために何ができるのか。最近のセキュリティ事情を中心に見据えながら、方針面、技術面における方策について説明する。

- I 最近の「セキュリティ情報」と業務への影響
  - インターネットサーバとオープンソースシステムインフラ
  - アップデート最新事情
  - セキュリティホールの原理の基礎
  
- II 「セキュリティ対応」の考え方と現状の課題
  - 品質確保の考え方
  - 被クラック調査
  - アップデートにまつわる事柄
  
- III Others...

September, 2002

- WEB/Mailなどを中心としたサービス
  - ホスト数はいまだに急増
  - ネットワークインフラの進歩
- しかし、特異なサービスである
  - 「常時」: 想定以上の期待
  - 「不特定」: 顔が見えない
  
- カンタンそうで難しい。
  - 「可用性」と「事業継続性」

September, 2002

「セキュリティ」

- (1) 安全。防犯。安全保障。
- (2) (有価)証券。

■ - 大辞林より

「きわめて経営的な言葉であり、技術用語ではない。」

September, 2002

- 機密性: 対象(人)、内容(データ)の関係を保証
- 完全性: 情報発信側と情報受信側の正確な伝達
- 可用性: 期待されるときはいつでも応じられる

これらは「責任」によって分類されたものである

September, 2002

	情報サービス	EC	銀行	コミュニティ
機密性				
完全性				
可用性				

September, 2002

- 機密性: 対象(人)、内容(データ)の関係を保証
  - 顧客データ漏洩, ID不正利用
- 完全性: 情報発信側と情報受信側の正確な伝達
  - WEBサイト改ざん, ウイルス感染
- 可用性: 期待されるときはいつでも応じられる
  - サーバダウン, タイムアウト

September, 2002

- Samba(2002/6/19)
- Apache (2002/6/20)
- Sendmail(2002/6/25)
- OpenSSH(2002/6/26)
- Resolver(2002/7/10)
- OpenSSL(2002/7/30)
- PHP(2002/9/6)
- OpenSSL Slapper Worm(2002/9/14)

...

September, 2002

- 対象:Apache1.2全バージョン、Apache1.3 ~ 1.3.24、Apache2.0 ~ 2.0.36
- 原因: chunked encodingコードに脆弱性
- 影響:Apache Webサイト全てに影響
- 脅威:サービス停止
- 種別:DoS(denial of service attack )

September, 2002

## chunked encodingとは

「ABCDEFGHIJKLMNOPQRSTUVWXYZ」という文字列を送る場合

chunked encoding しない場合

```
各種ヘッダ
各種ヘッダ
各種ヘッダ
Content-Length: 26

ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

chunked encoding の場合

```
各種ヘッダ
各種ヘッダ
各種ヘッダ
Transfer-Encoding: chunked

0a ←----- バイト数
ABCDEFGHIJ
0a
KLMNOPQRST
06
UVWXYZ
0
```

September, 2002

## Slapper Worm

- OpenSSLの脆弱性をつくWorm(2002/9/14)  
対象：ApacheとApache-SSLを動作させているWEBサーバ
  - Apacheのバージョンをチェック
    - OpenSSLのバージョンと動作状況を確認
  - OpenSSLのセキュリティホール(0.9.6d以前)
    - ソースコード(/tmp/.bugtraq.c, /tmp/.bugtraq)を送り込む
    - コンパイルしてしまう
    - 常駐して2002番ポートから通信を開始

調査部分と侵入路が異なる顕著な例

September, 2002

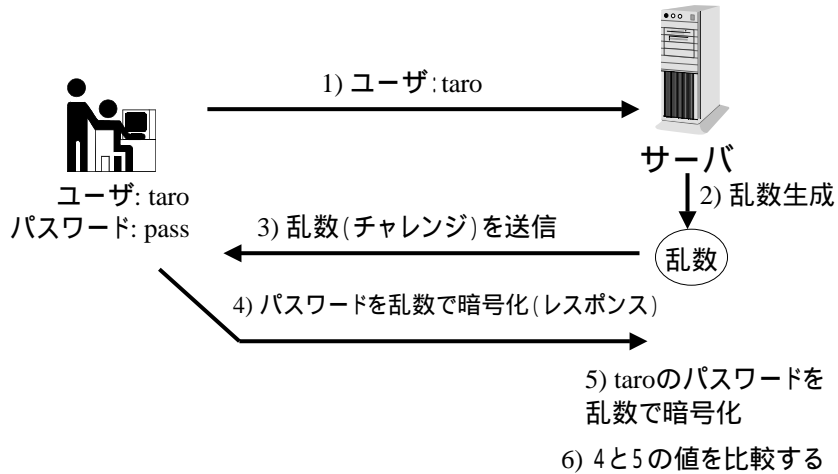
- 1.3.26あるいは2.0.39にアップグレード(推奨)
  - 主要なディストリビューションはリリースしている。
- このさいApache 2へ移行計画を  
(テスト環境の構築にそろそろ意味がでてきた)
- 1.3.26あるいは2.0.40にアップグレード
  - Upgrade your Apache HTTP Server to version 1.3.26 or 2.0.40 or higher. (Unix systems are safe at version 2.0.39.) - [httpd.apache.org](http://httpd.apache.org)
- URL:<http://httpd.apache.org/>

September, 2002

- 対象:OpenSSH 2.3.1p1 ~ 3.3
- 影響:ssh2によるリモート運用管理に影響
- 原因:チャレンジ・レスポンスコードに脆弱性
- 種別:バッファオーバーフロー
- 脅威:リモートから任意のコードを実行
- 対処:3.4にアップグレードあるいは設定変更
- URL:<http://www.openssh.org/>

September, 2002

## チャレンジ・レスポンス認証とは



September, 2002

## OpenSSH対応のおさらい

- 3.4にアップグレードあるいはパッチ適用 (推奨)
  - \*BSD, Debian, Miracle Linuxなどはリリースしている。
  - RHはデフォルトで下記の設定が組み込まれていないので現状では問題ないらしい
- sshd\_configで設定変更 (短期的にOK)  
**ChallengeResponseAuthentication no**  
**PAMAuthenticationViaKbdInt no**  
  
あるいは3.3以降デフォルトになっている**UsePrivilegeSeparation** の利用

September, 2002



- 実は最も深刻な被害を出す可能性のあるサービス
- 設定終了時に忘れられるサービス
- Ping/telnet/ssh の障害でも気づかれないこともある
- ネットの不具合でも影響を受ける
- わかりやすく言えば、**URLやドメインが脅威にさらされる**

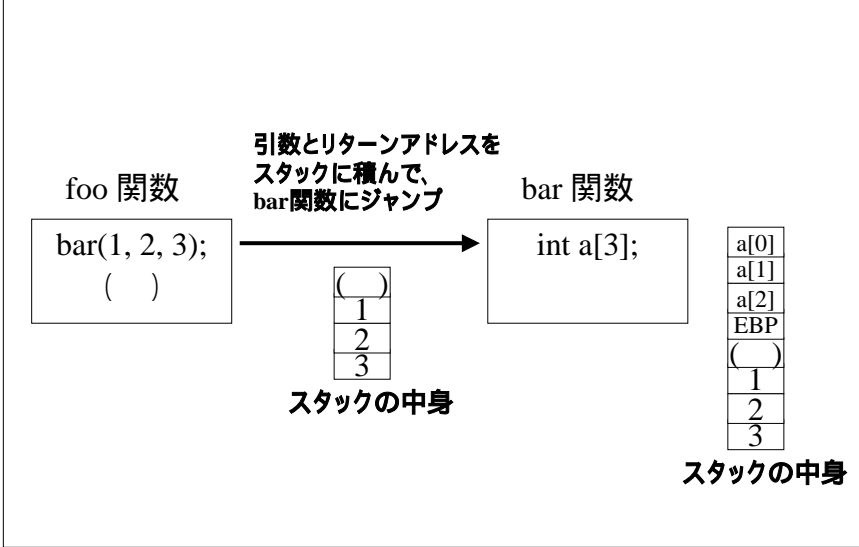
「いいWEBサイト作っても、ドメインごと乗っ取られてどうする」

September, 2002

- DNSの名前解決エンジン部分
- 対象:BSD resolverルーチン(libc)を使用する全アプリケーション
- 原因:Resolverライブラリコードに脆弱性
- 影響:BSD系OSのみ (FreeBSD/OpenBSD/NetBSD) に影響
- 脅威:サービス停止
- 種別:DoS(denial of service attack )
- 対処:アップグレード

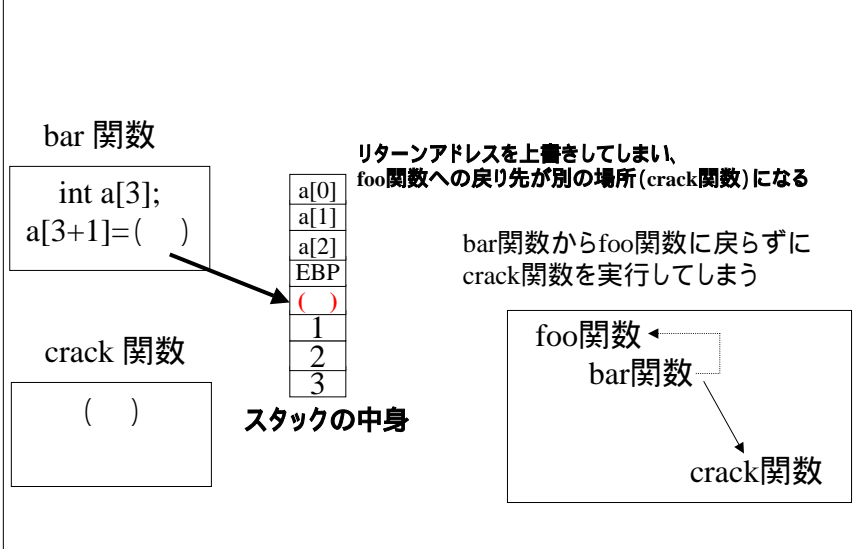
September, 2002

## バッファオーバーフローとは(1/4)



September, 2002

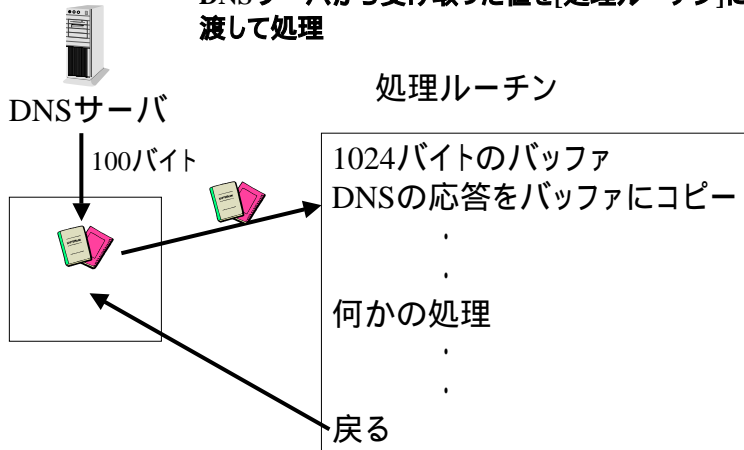
## バッファオーバーフローとは(2/4)



September, 2002

### バッファオーバーフローとは(3/4)

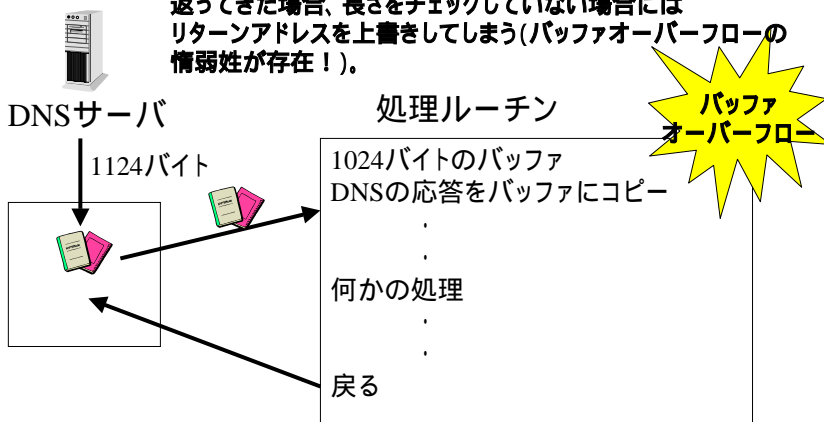
DNSサーバから受け取った値を[処理ルーチン]に渡して処理



September, 2002

### バッファオーバーフローとは(4/4)

[処理ルーチン]で想定している長さ以上の値がDNSから返ってきた場合、長さをチェックしていない場合にはリターンアドレスを上書きしてしまう(バッファオーバーフローの脆弱性が存在!).



September, 2002

## バッファオーバーフロー対策

- 最新版にアップグレード
- StackGuardを利用する  
(<http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/>)
- libsafeを利用する  
(<http://www.avayalabs.com/project/libsafe/index.html>)

StackGuardは各アプリケーションを再コンパイルする必要がある。  
libsafeは導入するだけでOK

September, 2002

## Resolver対応のおさらい

- BSD系OSのみ (FreeBSD/OpenBSD/NetBSD) はパッチがリリースされている
  - Dynamicリンクで使用しているソフトはrestartすれば良い
  - Staticリンクで使用しているソフトはソースからすべて再コンパイルする必要がある

<http://www.cert.org/advisories/CA-2002-19.html>

- glibc2.1.2とそれ以降は関係ない模様。  
<http://www.kb.cert.org/vuls/id/AAMN-5BMSW2>

ただ、組み込みも可能なので、自前で作っているものがあれば要チェック

September, 2002

- 対象: 8.12.0 ~ 8.14.4
- 原因: バッファオーバーフロー
  - TXTレコードの内容によりDNSマップを行う設定になっている場合
- 対策:
  - 8.12.5にアップグレード
  - TXTレコードを読み込まないようにする
- <http://www.kb.cert.org/vuls/id/814627>
- <http://www.sendmail.org/>

September, 2002

- 対象: Samba 2.2.3 以前
  - ( --with-tdbsamオプションが指定された場合のみ )  
デフォルトでは指定されていない
- バッファオーバーフロー
  - SAM の格納先として tdb を利用した場合に、smb.conf から変数を読み込む際のルーチン
- 対策:
  - 2.2.5/2.2.4-ja-1.0にアップグレード
  - --with-tdbsamオプションを利用しない
- <http://www.samba.gr.jp/news-release/2002/20020703-1.html>

September, 2002

## ■ セキュリティ対応のための重要なファクタ

- 事象・原理に関する知識
- ソフトウェア入手の確保
- 実行動作環境
- ソフトウェア配布の手段
- 検証環境・検証プロセス
- 性能要件・機能要件
- 情報源と問題把握
- 予防体制・対応体制

...

September, 2002

- 横断的な判断の難しさ...
- セキュリティ対応に「唯一無二」の方法などない。
- 一体、なにが起こりえるのか？
  - ネットワーク
    - TCP/IP, ルーティング
  - サーバアーキテクチャ
    - Intel アーキテクチャ
    - クラスタリング
  - カーネル
    - DoS対応, ipchainsによる「境界線」など
  - サーバソフトウェア
    - Apache, SSHなど基盤
  - ミドルウェア
    - 開発プラットフォーム
  - アプリケーション
    - 誰が、どんな機能を作っているのか
  - ユーザイメージ
    - どんなユーザがどんな環境で使うのか

September, 2002

- ベンダー依存できるものとできないもの
  - ネットワークからアプリケーションまでの各レイヤーを整理
    - 保守対応でまかなえることとまかなえないこと
  - Debian, RedHat, Turbo, Miracle
  - いずれにせよ、確保できているか
    - RHのup2dateコマンドはよく裏切る...
      - 「すぐに欲しければ金を払え」とか...

September, 2002

- 記録！記録！記録！
  - デジタルデータの良し悪し
- メジャーバージョン
  - 7.2 ? 7.3?
- パッケージ・ライブラリ
  - rpm -rebuilddb
  - rpm -qa
- アプリケーション
  - CVS, RCSなどの管理

September, 2002

- ~ 10台の場合とそれ以上の場合
- up2dateではbusy問題(前述)
- apt-netってあるようなないような

September, 2002

- 検証環境なしでセキュリティはない
- VMwareでもいい
- アプリケーションではどうするか
  - アップデートテスト用のスクリプトを作っておく
  - 設計段階で利用ライブラリ範囲を作る
  - 検収段階で、利用関数の一覧などを作る
  - テストスクリプトをあわせて開発させる
  
- アップデート担当者はテストスクリプトの検証まで行う

September, 2002



- 外部テストの重要性
  - 同一セグメントでは問題が見えないケースが多い
  - abコマンドでできることも多い
  - webalizerで外部からどういうパターンで見られているか確認
  
- 内部テストの重要性
  - テストスクリプト...

September, 2002

- 情報源の特性を知っておく
  - ML
  - WEB
  - ディストリビューション情報
  - TechStyle
  - 最重要：ユーザ
  
- 問題把握
  - その問題は、どうして起きるのか？
  - どこに現れるのか？
  - セキュリティ3要素の何を脅かすのか？（リスク分析）
  - 記録！記録！記録！

September, 2002

- 人間というリソース
  - 最大のセキュリティホール
  - もっとも冗長性が低い
  - もっとも可用性も低い

瞬間最大風速で最適な運用をしていかなければならない  
複雑すぎる手順を、もう少し間便で確実な手順へと改訂

September, 2002

- オープンソースソフトウェアの特異性？
  - MS、Sun、その他の場合と比較してなんら異なることはない
  - 「オープンソース」は開発プロセスだ。

とすると、

- ソフトウェア開発プロセスと、品質要件？
- ソフトウェア開発プロセスと、構築要件？
- ソフトウェア開発プロセスと、運用要件？

September, 2002



Thank You

Quality for All Professionals  
<http://techstyle.jp>

Please feel free to mail me  
[riotaro@techstyle.jp](mailto:riotaro@techstyle.jp)

September, 2002