JPNIC・JPCERT/CC Security Seminar 2005

サーバアプリケーションセキュリティ

1日目(UNIX Day) 2005年10月6日

メールサーバとセキュリティ (迷惑メール対策)

株式会社インターネットイニシアティブ
山本 功司 koji@iij.ad.jp

本日の内容

- 対象
  - メールサーバ/システムのオペレータ
    - 設計、構築、運用を担当する方
  - メールに関わるインシデントに対応する方

メールサーバに対する脅威

- **サーバソフトウェアの脆弱性**
- **不正中継 (第三者中継)**
- **過剰トラフィックによるDoS**
  - spam, virus, bounce
- **メールアドレス収集**
- RBL**等への登録**

サーバソフトウェアの脆弱性

- 脆弱性により引き起こされるインシデント
  - サーバへの侵入
  - 任意コマンドの実行
  - ローカルユーザの特権奪取
- 今回は特に取り上げない
  - 最近、ほとんど例を聞かない
  - qmail, postfix の台頭と sendmail の改良

不正中継 (第三者中継)

- open relay, third party relay **などとも言われる**
- **本来、意図していない送信者からのメールを中継してしまう**
  - **認証のすっぽ抜け**
- **本来、意図していない受信者へのメールを中継してしまう**
  - MX(incoming)**サーバ**

不正中継 (第三者中継)

- 現在、ほぼすべてのMTAでデフォルトで第三者中継をしない設定
  - 明示的に中継を許可しない限り、中継しない
  - 不正中継がされた場合は、なんらかの設定ミスである可能性が高い
- 考えられる要因
  - ケアレスミス
  - 認証絡みの不具合、設定漏れ
  - POP before SMTPとNATの問題
  - 多段中継

不正中継と認証設定

- POP before SMTPの認証DBトラブル
  - 認証済みIPアドレスを一定時間記憶しておくDBに接続できないケース
  - トラブル時、すべて中継を許可する側へデフォルトが倒してあった
    - 結果として、open relayとなる
  - ユーザからのクレーム（送信不可）と、不正中継とを天秤に

POP before SMTP と NAT の問題

- POP before SMTP
  - POP の認証が通ったIPアドレスを一定期間DBに登録
  - DBに登録されているIPアドレスからのSMTPの中継を許可
- NAT
  - NATの裏に複数/多数のクライアントが存在
  - POP認証していないクライアントからのSMTP送信
- 解決のためには、SMTPセッションそのものを認証する必要
  - SMTP AUTH(RFC2554)
  - sendmail, postfix ともに Cyrus-SASL が利用可能

多段中継

- 自サーバが中継を許しているIPアドレスに open relay が存在
  - メールサーバ管理者の管轄外で設置されたマシン等
  - 今でも多くのISPで、自社足回り(ダイアルアップ)から無条件に中継を許す設定がされている
    - POP before SMTP すら要求されていない
  - 途中経路のサーバをすべてRBLに登録するような事例あり
- 中継許可は最小限の範囲に
- クライアント(MUA)からの中継には、SMTP AUTHの必須化

過剰トラフィックによるDoS

- **メールサーバを使用不能とする意図を持って行なわれるもの**
  - mail bomb等
  - **事例としては少ない**
- **意図せず、結果としてメールサーバが過負荷となるもの**
  - **自ドメイン宛**spam, virus
  - **自ドメイン発**spam, virus
  - **自ドメイン発を詐称する**spam, virus**による**bounce

メールシステムを過負荷から守る

- 今日、メールシステムは単体のサーバで構成される事は少ない
  - 送受信ボーダー
  - ウイルスチェック、spamフィルタ
  - 各種データベース、ディレクトリ
  - スプール
- 送受信ボーダーでのフィルタリング、スロットリング
  - ボーダーをカリカリにチューニングしても、システムのボトルネックは他に存在する事が多い
  - 不要なメールはシステムに入れない/システムから出さない

自ドメイン宛spamによる過負荷

- botnet 経由で、ローカルパート辞書攻撃
  - 特定のIPからではないので、レートコントロール等不可
  - 数万ユーザーのドメインに対して、その数十〜数百倍のspam
  - 99%以上が存在しないユーザー宛
- ボーダー(incoming MX)で受け取ってしまうと、後段で大量のbounce発生
  - From は詐称されている (国内他プロバイダ)
  - 先方も大量の偽のbounceで過負荷になり、受け取らない
- ボーダーでのユーザーの存在チェックが必要に
  - ディレクトリハーベスティングの危険性

自ドメイン宛virusによる過負荷

- 基本はspamと同様
- マスメール型virus/wormの挙動は地域性がある
  - 日本からは日本人宛へ数多く送信される
  - 国内ISPの動的IPを指定しての受信拒否が有効な場合も

自ドメイン宛spamによる過負荷

- botnet/zombie 対策
  - 動的IPのフィルタ
    - RBL, DUL 等の利用
    - xSPとしては、受信側ではやりづらい
  - 逆引きの存在チェック
    - 逆引きが存在するところのほうが多数 (効果が薄い)
    - あえて逆引きを設定していないサーバも
  - greylisting
    - temp fail (4xx)を返すことによる遅延
    - 相手側の再送に依存
    - ユーザーからのクレームもあり、xSPではやりづらい

自ドメイン宛spamによる過負荷

- これらの複合した対策
  - スロットリング等の制御を
  - RBLやgreylistingで怪しいIPに対して適用
- いずれにしろ、対症療法
  - 根本的には送信側ISPでの対策が必要
    - Outbound Port25 Blocking
    - 送信ドメイン認証

自ドメイン発spam/virusによる過負荷

- 利用者認証による適切なスロットリングが必要
  - xSPは中身を見ての判断はできない
- IPアドレス単位の制限から、利用者単位の制限へ
  - POP before SMTP から SMTP AUTHへ

自ドメイン発を詐称するspam/virusによる過負荷

- いわゆる、バックスキャッタ問題
- ヘッダチェック等により一部は抑止可能
- 根本的には送信側での詐称防止対策が必要
  - 送信ドメイン認証等
  - SMTP AUTH と From チェックの厳密化

自ドメイン発spam/virusの問題

- 問題は負荷だけではない
  - 社会的責任
  - abuse対応
  - ドメインのレピュテーション/到達性低下
  - 過激なRBLへの登録

メールアドレス収集対策

- IDやホームページURLからのメールアドレスの類推
- webページからのアドレス収集
- ディレクトリハーベスティング
  - ボーダーでの効率的な受信拒否と表裏一体
  - sendmail での BadRcptThrottle のような対策
- さらに進んで携帯のような指定受信、指定拒否へ
  - UNIXのソフトウェアでは難易度は高い

sendmail での不正中継対策

- FEATURE(access_db) (/etc/mail/access)
  - **ほぼ、これだけで基本的な設定はできてしまう**
  - **多様なコントロール**(From: To: Connect: **等**)
  - **その他の応用的なアクセス制御にも利用**
- /etc/mail/local-host-names
- /etc/mail/relay-domains
  - **デフォルトの設定で利用可能**

sendmail でのspam対策

- ConnectionRateThrottle, BadRcptThrottle
- FEATURE(ratecontrol), FEATURE(concontrol), FEATURE(greet_pause)
- FEATURE(dnsbl), FEATURE(enhdnsbl)
  - DNSを使ったRBL
  - xSPでは安易な利用は勧めない

sendmail のチューニング

- sendmail クックブック - 設定と運用のためのレシピ集
  - Craig Hunt(著), 林 秀幸(翻訳)
  - オライリージャパン ISBN 4873111889
- sendmail 2分冊 (通称コウモリ本)
  - まず使うことはないが、辞書的に
  - sendmail 第3版<VOLUME1>運用編, <VOLUME2>設定編
  - オライリージャパン ISBN 4873111765, 4873111803
- きめ細かいspam対策チューニングのためには最新の8.13.xを使う
- Sendmail 8.13 Companion
  - ISBN 0596008457
- cf/README

postfix の不正中継対策

- main.cf
  - mydestination
  - mynetworks
  - relay_domains
- BASIC_CONFIGURATION_README

postfix の spam 対策

- main.cf
  - smtpd_*_restrictions
  - SMTPD_ACCESS_README
- **外部ポリシーサーバ**
  - SMTPD_POLICY_README

postfix のチューニング

- Postfix詳解　ーMTAの理解とメールサーバの構築･運用
  - 荒木 靖宏(著)
  - オーム社 ISBN 4274065766

- ドキュメント和訳
  - 非常に充実、最新版までカバー
  - http://www.postfix-jp.info/