発信者詐称SPAMメールによるDoS攻撃への対策手法

山井　成良

yamai@cc.okayama-u.ac.jp

岡山大学総合情報処理センター

SPAMメールによる被害

- 受信による被害
- 発信（中継）による被害
  - 比較的被害小
  - 対策も比較的容易
- 発信者アドレスの詐称による被害
  - 頻度小（自ドメインに詐称された場合のみ）
  - 被害は甚大
  - 対策も困難

あるSPAMメール

From: ********* ******* <**********@*******.***>
To: ****.*******@********.***.***.*******.**.**
Subject: Take advantage of the Bulk Email Special today? Broadcasting 500.000 Only $ 59.95
Date: Wed, 30 Oct 2002 12:56:30 -0500

MULTILEVEL MARKETING OPPORTUNITIES

PRODUCT ORDER Disks are in TEXT file format and fully EXPORTABL:

1)[ ] 200 Million email addresses all fresh!!!!! ==Only $69.95==
2)[ ] 100 million email addresses all fresh!!!!! ==Only $49.95==
3)[ ] 1.5 Million USA Business FAX NUMBERS, ==Only $29.95==
4)[ ] 7.5 million Chinese e-mail addresses all fresh!!!! ==Only $49.95==
5)[ ] 100 Thousand Toronto Canada business fax numbers ==Only $49.95==

...

90% DELIVERABLE

発信者詐称SPAMの問題点

- 詐称アドレスが自組織のものである場合
  - エラーメールの大量受信
    2億通 ×10% ＝ 2000万通!!
  - MTA・ネットワークの過負荷
    ⇒ 通常メールの配送遅延・停止
  - ディスクの大量消費
    特に実在アドレスの場合

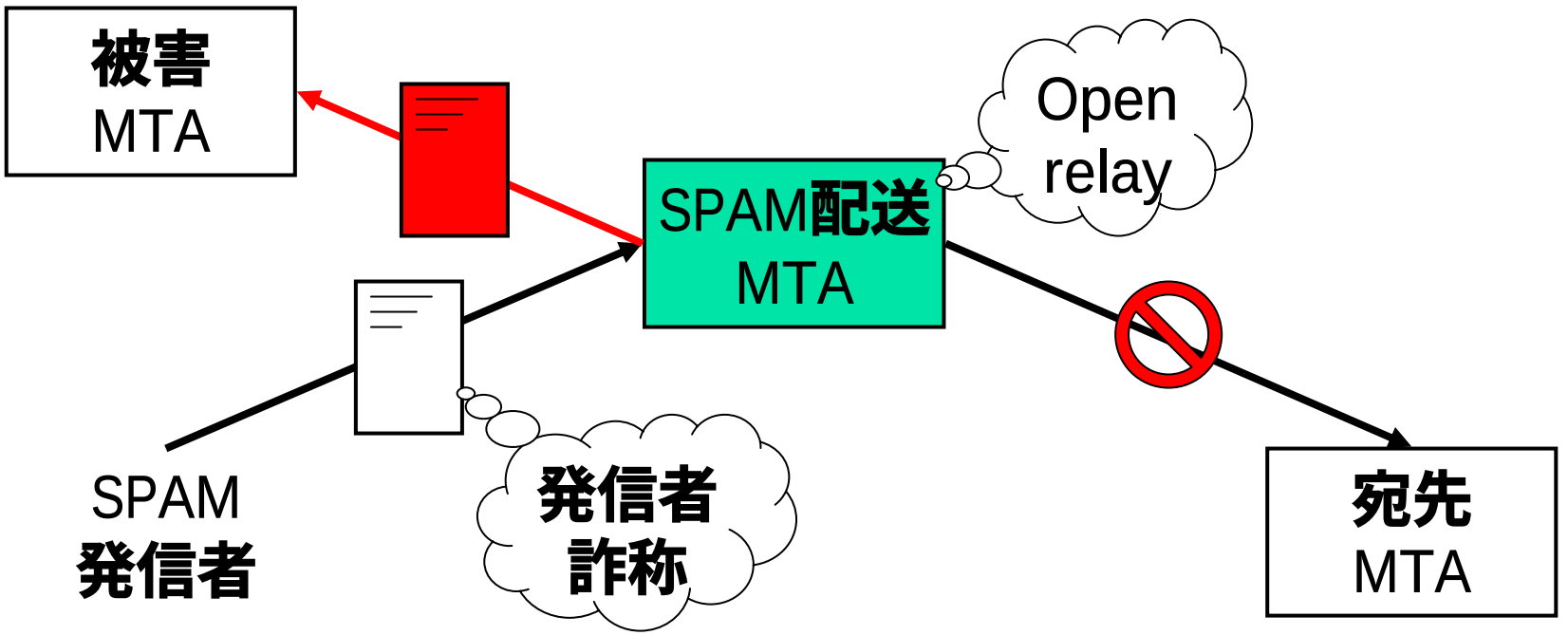
⇒ 事実上のサービス不能 (DoS) 攻撃

発信者詐称SPAMによる被害例

- 2002年11月に国内プロバイダで発生
  - 30万通以上のエラーメール
  - 最大で15時間以上の配送遅延
  - 復旧までに約2日半
    - 11/5 9:30am 〜 11/7 11:00pm
  - 恐らく実在アドレス
    - アドレスリスト中に含まれるものと推察

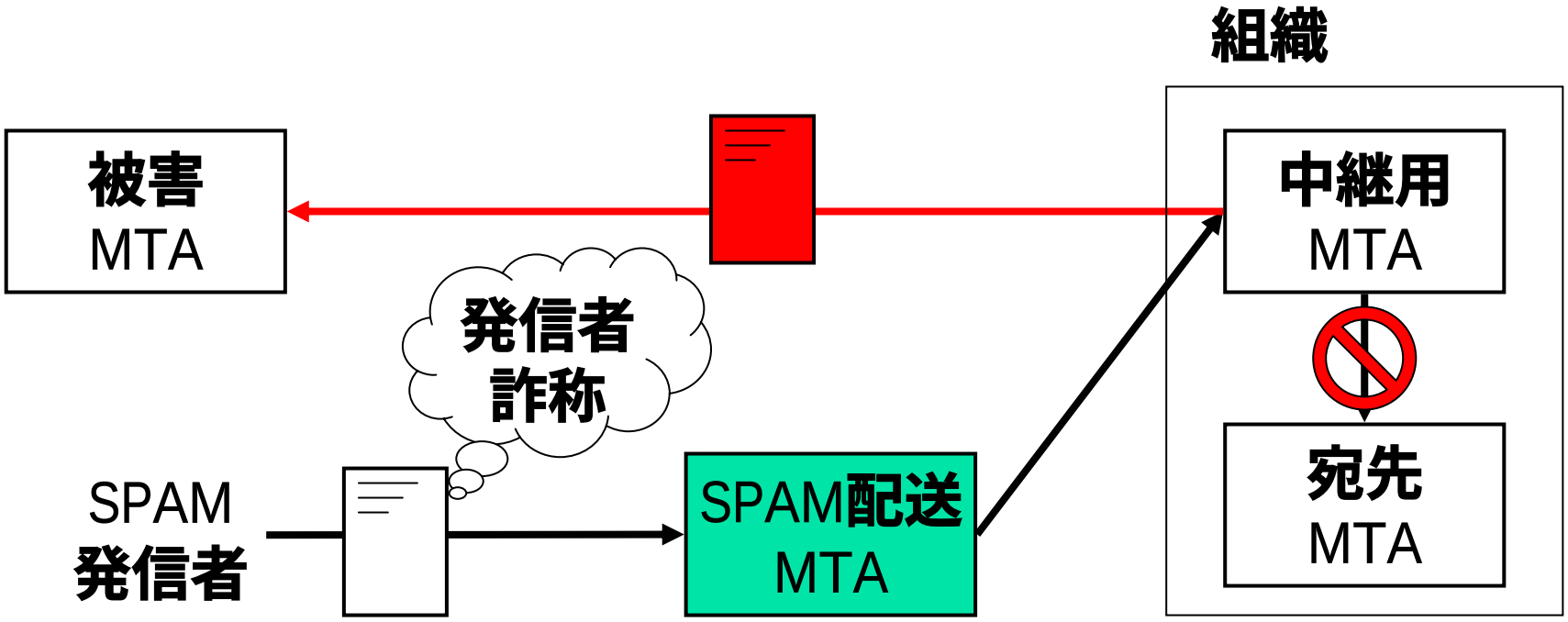
エラーメールの配送(1)

- **直接配送エラーメール**



エラーメールの配送(2)

- **中継配送エラーメール**

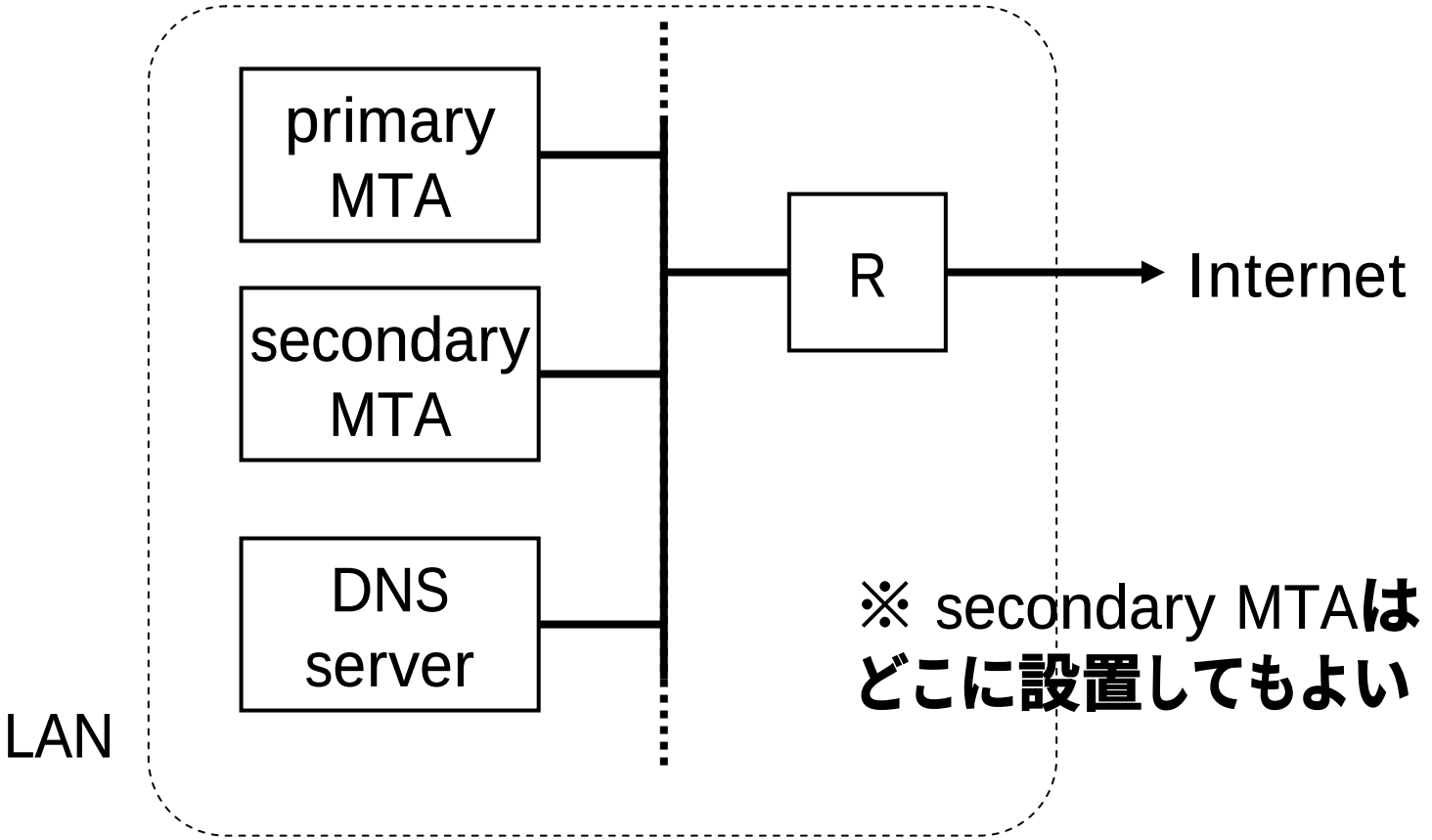


対策方式

- 1台のMTAでは過負荷は不可避
  ⇒ 従来のMTA(プライマリMTA)とは別のMTA(セカンダリMTA)を導入
  - 通常メールは極力プライマリMTAで処理
  - エラーメールは極力セカンダリMTAで処理

※ コネクション確立前におけるエラーメールと通常メールの振り分けが問題

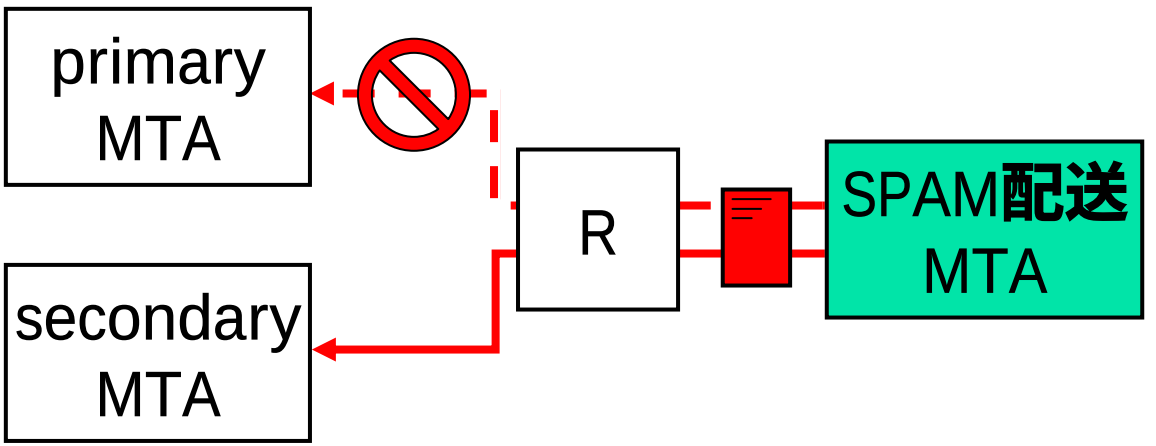
システム構成


primary
MTA
secondary
MTA
DNS
server
R
Internet
LAN
※ secondary MTAは
どこに設置してもよい

直接配送エラーメールの処理

- 1つのMTAから多数のエラーメール

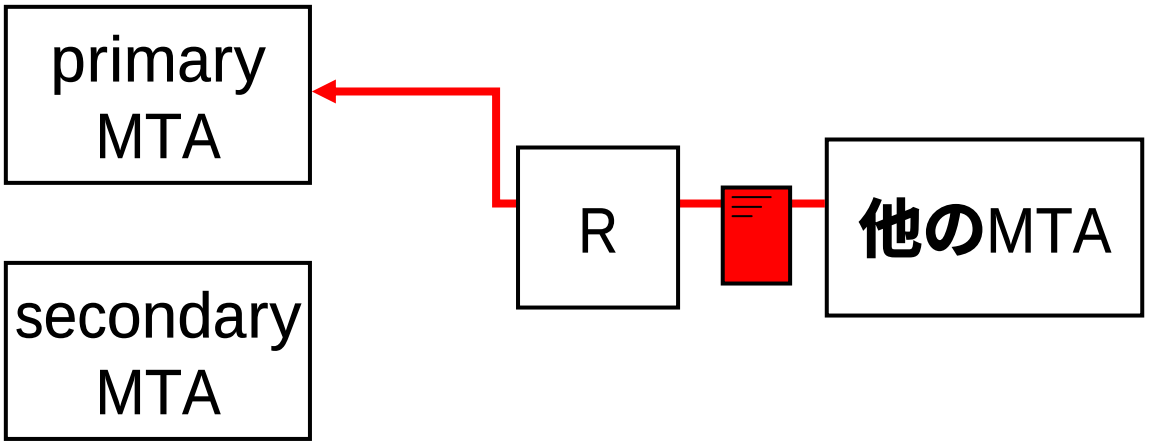
→ ルータでプライマリMTAへの通信を拒否



直接配送エラーメールの処理(続き)

- **他のMTAからメール**

→ プライマリMTAで受信

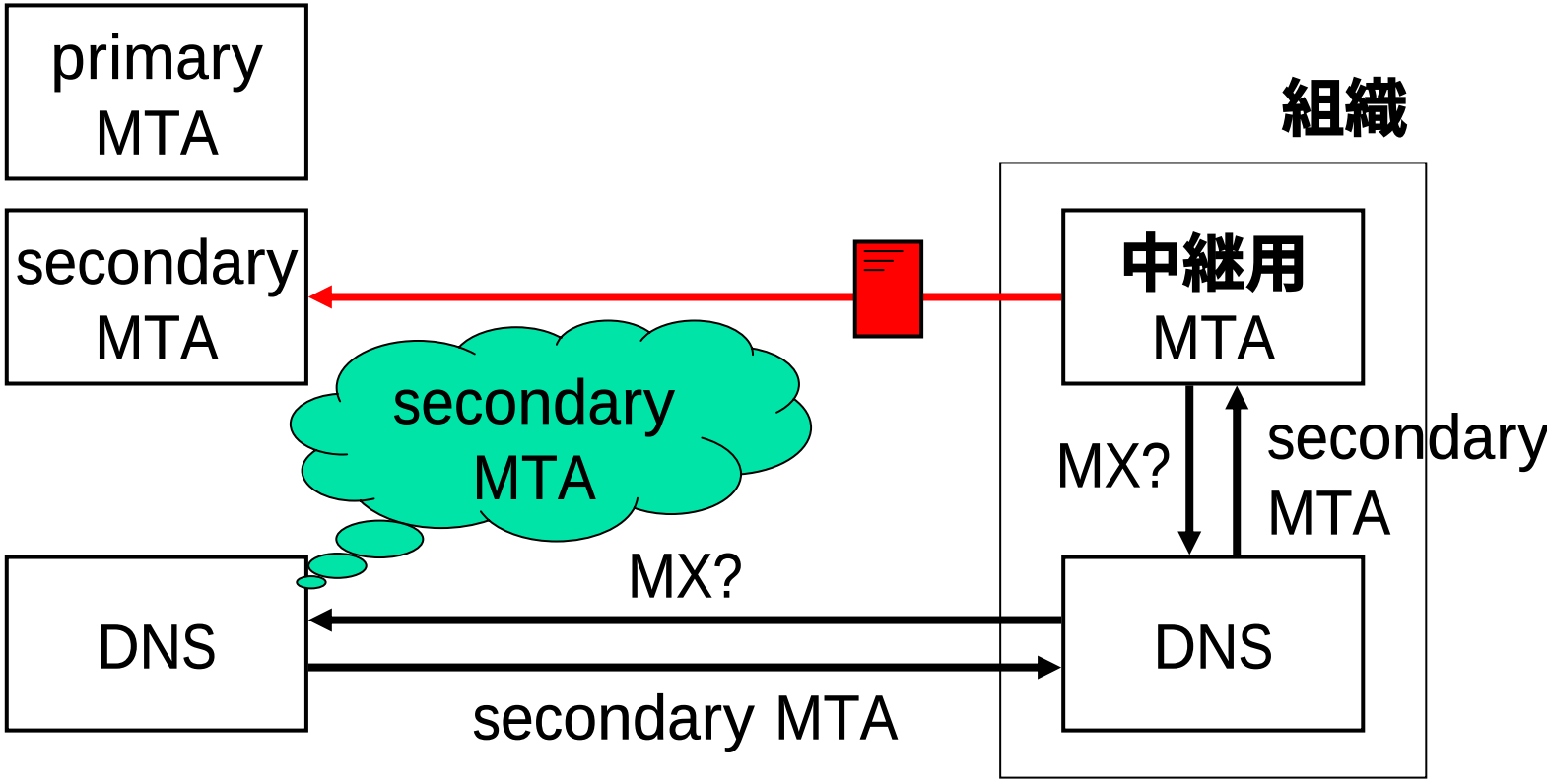


中継配送エラーメールの処理

- 多数のMTAから少数のエラーメール
  - ルータでのフィルタリングは疑問
- MXに対するキャッシュの有無を利用
  - 多くの中継用MTAではミス
  - メールを頻繁に交換するMTAではヒット
- MXを動的に変更
  - 通常はプライマリMTAを応答
  - SPAM対策時にはセカンダリMTAを応答

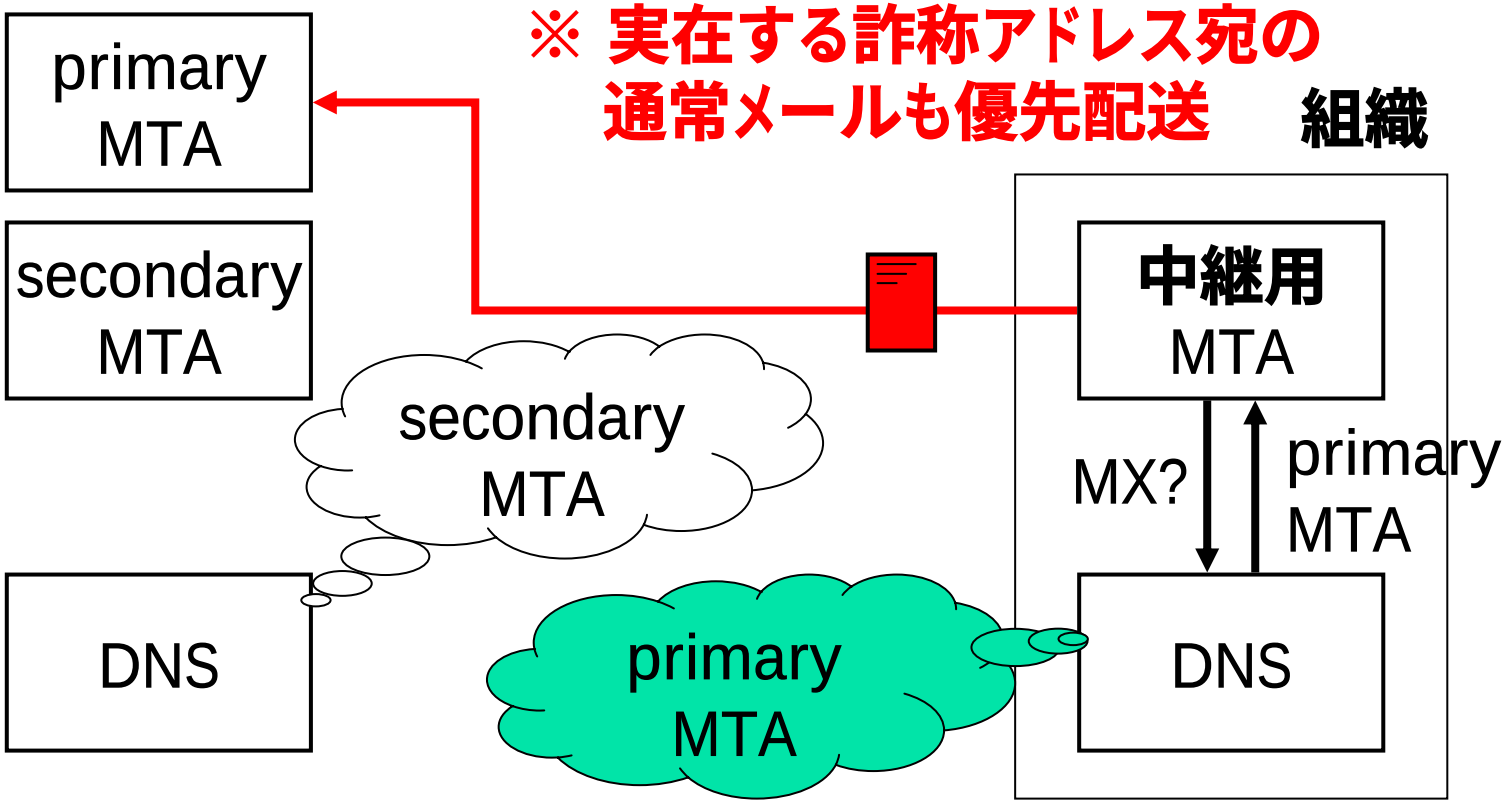
中継配送エラーメールの処理(続き)

- **中継用MTA(キャッシュミス)の場合**



中継配送エラーメールの処理(続き)

- 他のMTA(キャッシュヒット)の場合



エラーメールの処理

- エラーメールのみ早めに拒否/破棄
  - エラーメール処理に負荷をかけない
- 処理手順(プライマリ，セカンダリ共通)

1. Envelope-From，Envelope-Toをチェック
   MAILER-DAEMONから詐称アドレス宛なら
   コネクションを切断
2. ヘッダ中のFrom，Toをチェック
   詐称アドレス宛のエラーメールなら破棄
3. 通常メール/苦情メールと見なして配送

※ 苦情メールの自動返信も可能

SPAM対策の開始･終了

- SPAM処理開始
  1. プライマリMTAにおいて
     特定のアドレス宛のエラーメールを，
     短時間に多数受け取った場合
  2. DNSに対して，
     特定のドメインに対する
     MXの問合せが
     短時間に多数あった場合

※ 誤判定は実害が殆どないため許容

SPAM対策の開始･終了

- SPAM処理終了
  - セカンダリMTAにおいて
    詐称アドレス宛の
    エラーメールが
    一定時間検出されない場合

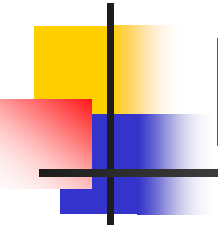
※ プライマリMTAでの検出は殆ど無意味

全体の対策手順

1. **初期状態**
   DNSでプライマリMTAを応答(TTL大)
2. SPAMの検出
   プライマリMTAでのエラーメール監視
   DNSでのMX queryの監視
3. SPAM処理開始
   DNSでセカンダリMTAを応答(TTL小)

全体の処理手順(続き)

4. ルータでのフィルタリング設定
   両方のMTAでのエラーメール処理設定
5. プライマリMTAでのエラーメール監視(検出時は4.へ)
   セカンダリMTAでのSPAM処理終了検出
6. エラーメール処理及びルータでのフィルタリングの解除(全解除でなければ5.へ)
7. 初期状態へ復旧(1.へ)



問題点

- 本手法の評価が困難
  - 多くの要因が影響
    - エラーメールの比率
    - キャッシュの有無など
  - 調整可能パラメータが多い
    - DNSにおけるキャッシュの有効期限
    - 攻撃検出･解除方法

問題点 (続き)

- 自分でSPAMを送るのは問題
- 実際に被害に遭うのも困難

⇒ 多数の組織との連携が必須

- DNSアクセス記録
- エラーメール受信ログ
- (対策システムのインストール)

将来計画

- セカンダリMTAの共有
  - 広域で共通のセカンダリMTAを設置
  - DoS攻撃で浪費する帯域を別のネットワークに誘導
  - 全体的な導入コスト，管理コストも削減可能

まとめ

- 発信者詐称SPAMによるDoS攻撃を回避
  - エラーメールはsecondary MTAへ誘導
  - DNSキャッシュの有無を利用
- 有効性の検証が困難
  - Janog参加者へ協力をお願いしたい
  - メーリングリスト

    anti-spam-request@cc.okayama-u.ac.jp宛に

    subscribe

    end

    の2行だけ (Subject不要) のメールを送付

謝辞

※ 本研究の一部は，以下の経費の補助を受けている．

- 日本学術振興会 科学研究費補助金
  - 研究種目：基盤研究(C)(2)
  - 課題番号：15500039
  - 研究課題名：発信者詐称SPAMメールに起因するサービス不能攻撃への対策

関連発表

- 山井成良，山外芳伸，宮下卓也，大隅淑弘：発信者詐称SPAMメールに対する対策手法，情報処理学会分散システム/インターネット運用技術研究会研究報告，2001-DSM-22-9，pp.~51-56，平成13年7月．
- 田中清，山井成良，岡山聖彦，宮下卓也，中村素典，丸山伸：発信者詐称SPAMメールによるサービス不能攻撃の早期検出手法，情報処理学会第64回全国大会講演論文集，2H-2，平成14年3月．
- 山井成良：発信者詐称SPAMメールによるサービス不能攻撃対策（前編），CYBER SECURITY MANAGEMENT，Japan Cyber Security Institute，Vol.4，No.39，pp.64-67，平成15年1月．
- 山井成良：発信者詐称SPAMメールによるサービス不能攻撃対策（後編），CYBER SECURITY MANAGEMENT，Japan Cyber Security Institute，Vol.4，No.40，pp.71-74，平成15年2月．