

情報セキュリティ基礎

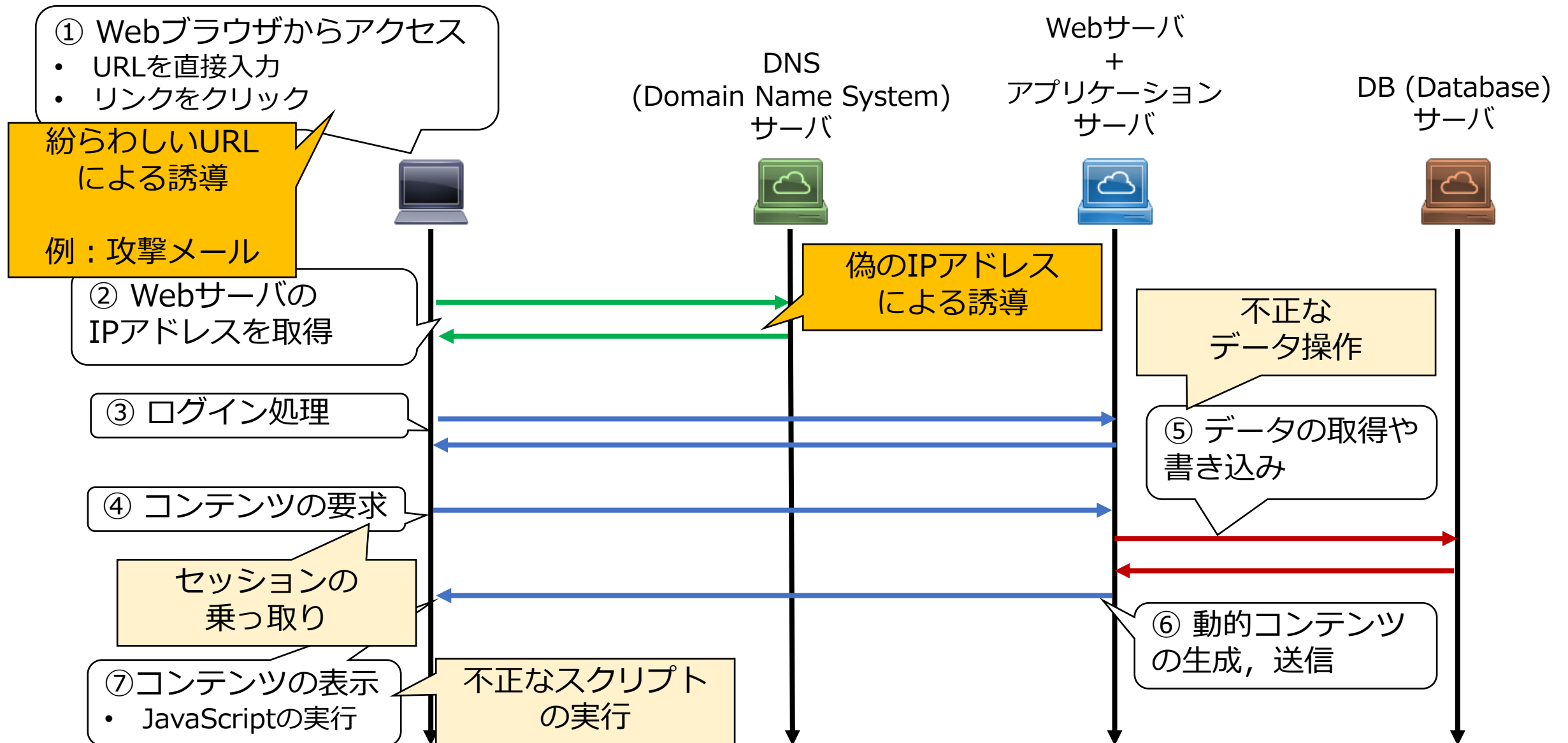
第6回 アプリケーションの通信に関する脅威（2）

藤本 章宏

今回の目標

- DNSと電子メールの仕組みについて確認する
- DNSと電子メールにおけるなりすまし対策を知る

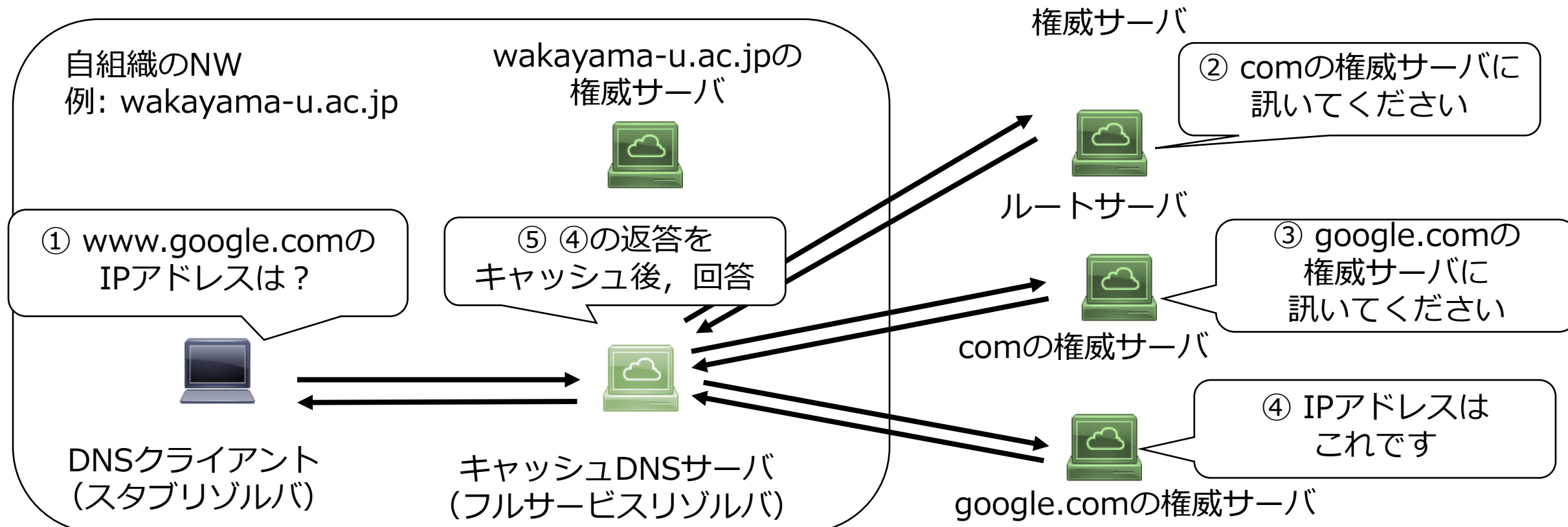
攻撃者が狙うポイント



DNS (Domain Name System)

ドメイン名とIPアドレスを相互に変換するサービス

- ✓ ドメイン名に基づき、階層的に管理
- ✓ リゾルバ（検索を行うプログラム）と
権威サーバ（データを管理するサーバ）から構成



DNSキャッシュポイズニング

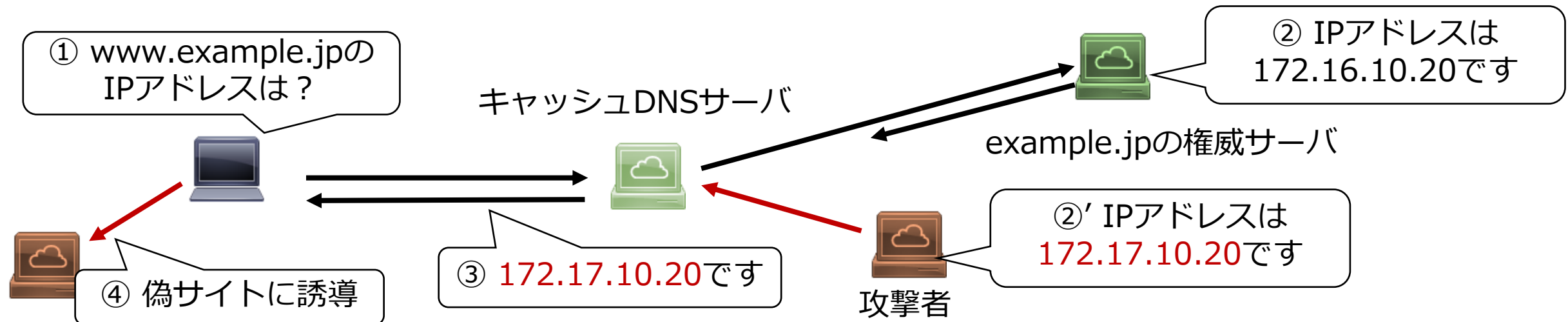
キャッシュDNSサーバのキャッシュを偽の返答により汚染する攻撃

- ✓ 正規の権威DNSサーバが返答する前に偽の返答を注入

キャッシュの有効期間
を延ばすことが対策（とされた）

攻撃成立の条件

1. キャッシュサーバの**キャッシュに登録されていない**名前解決の要求であること
2. キャッシュサーバからの問い合わせに対して**矛盾の無い返答**であること
 - ✓ 問い合わせた際の送信元ポート番号に対して返答
 - ✓ トランザクションIDが一致
3. 正規の権威サーバよりも**早く返答すること**



名前解決に関わる設定ファイル(第2回より再掲・改変)

/etc/resolv.conf

問い合わせ先となるDNSサーバの情報が書かれた設定ファイル

/etc/hosts

ホスト名とIPアドレスの対応関係が書かれた設定ファイル

```
IPアドレス  ホスト名  
127.0.0.1  localhost
```

/etc/nsswitch.conf

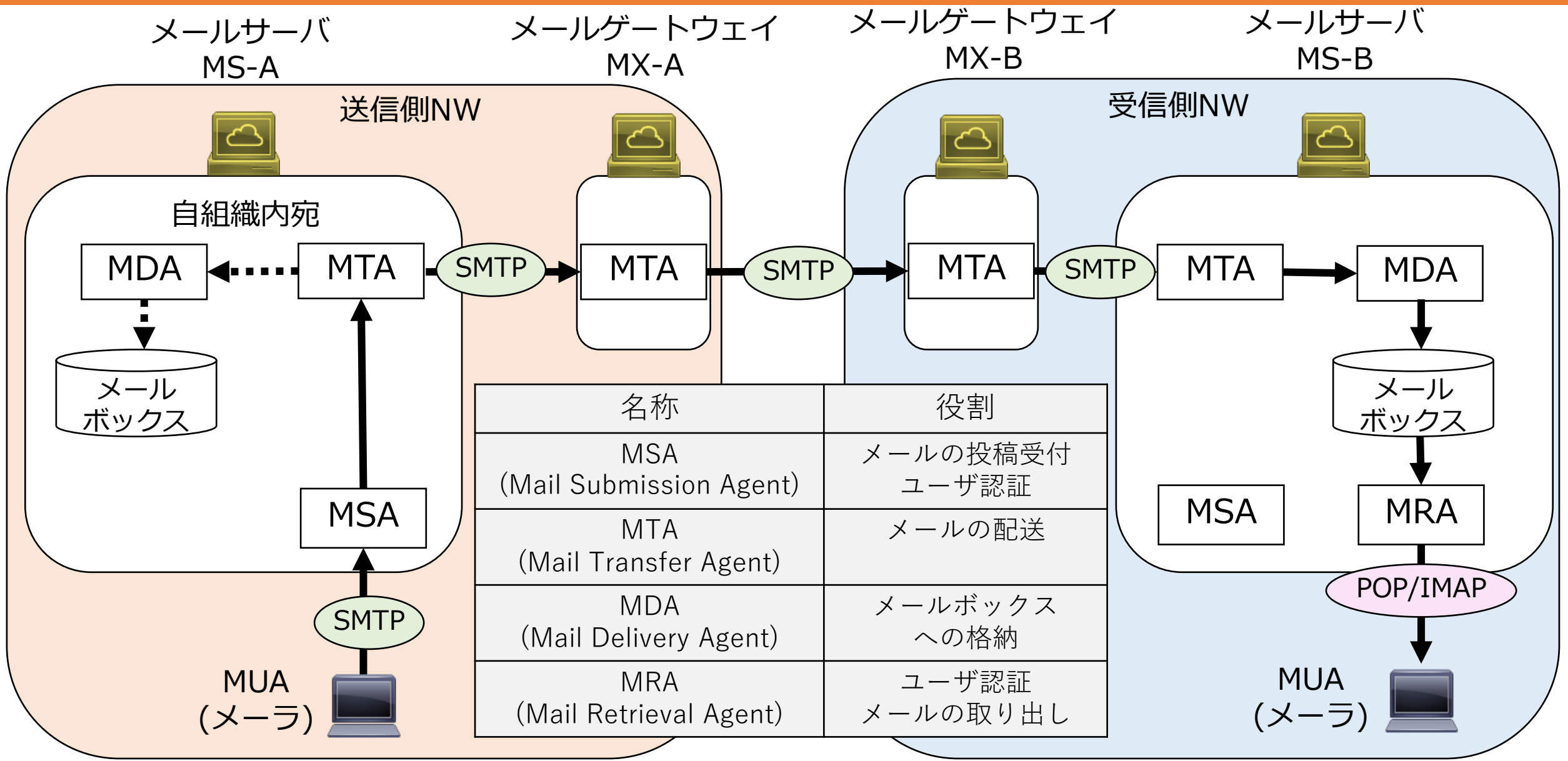
ユーザ名やホスト名をどのように調べるか
書かれた設定ファイル

```
hosts: files dns
```

resolv.confやhostsが
書き換えられると、**悪意ある
サーバへ誘導される**可能性

↑ まず/etc/hostsを調べて、無ければDNSに問い合わせ

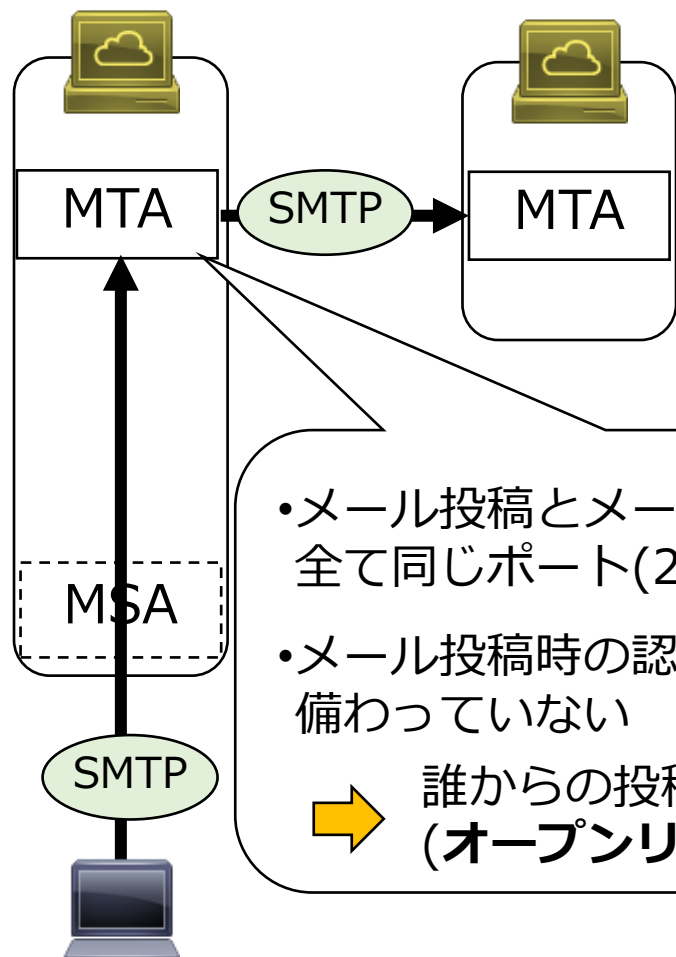
電子メールの通信の流れ



電子メールにおける脆弱性

メール投稿におけるセキュリティへの意識が薄かった

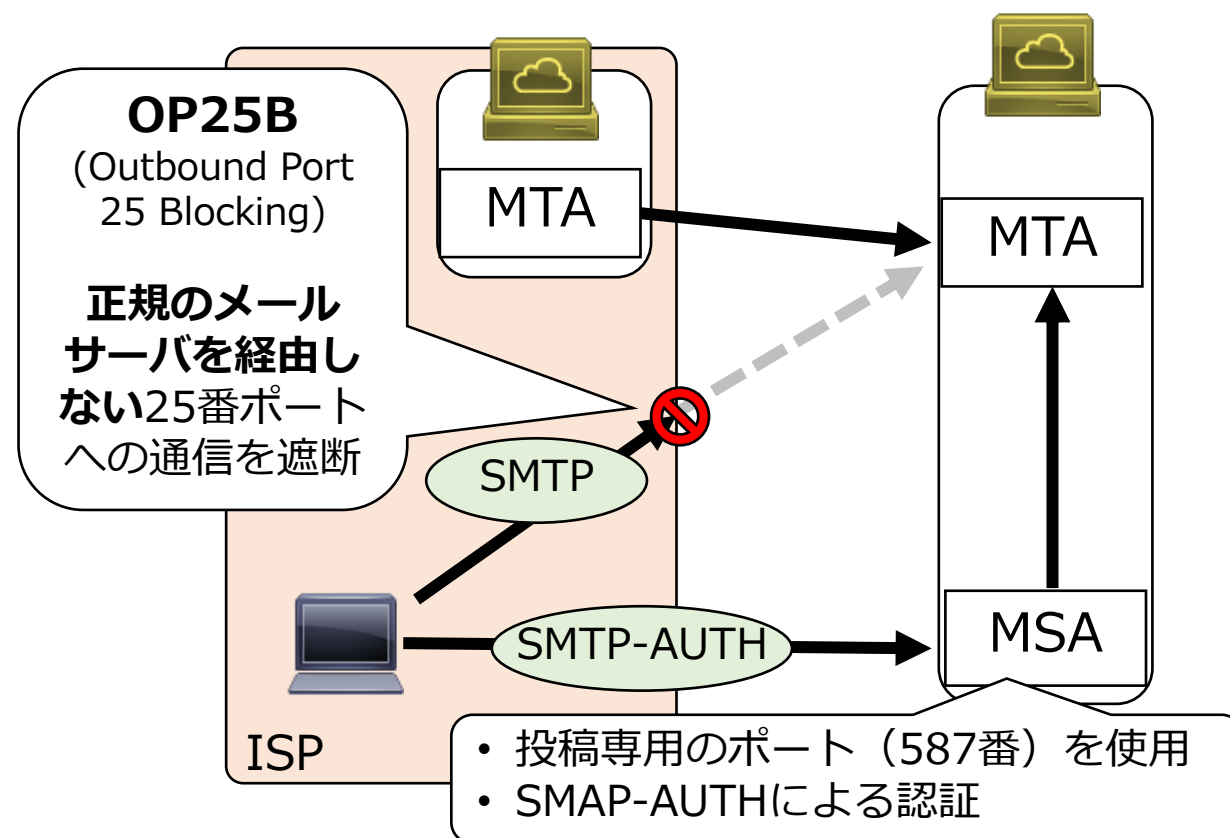
古いメールサーバソフトウェア



- メール投稿とメール転送の区別なく、全て同じポート(25番)で処理
- メール投稿時の認証の仕組みも備わっていない

➡ 誰からの投稿も受付
(オープンリレー)

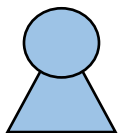
近年のメールサーバソフトウェア
+
ISPの対策



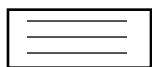
DNSSEC

電子署名の仕組みを応用したレコード検証の仕組み

ゾーン xxx.co.jp
の管理者



リソースレコード
例: Aレコード



① リソースレコードから
署名を生成

登録

xxx.co.jpの
権威サーバ



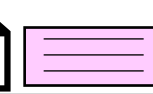
レコード	値
www.xxx.co.jpの Aレコード	
www.xxx.co.jpの Aレコードの署名	
ゾーンxxx.co.jpの検証鍵	

② 権威サーバに登録

キャッシュ
DNSサーバ



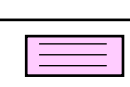
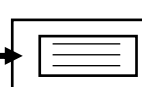
③ www.xxx.co.jpの
IPアドレスを問い合わせ



④ 署名付きで応答



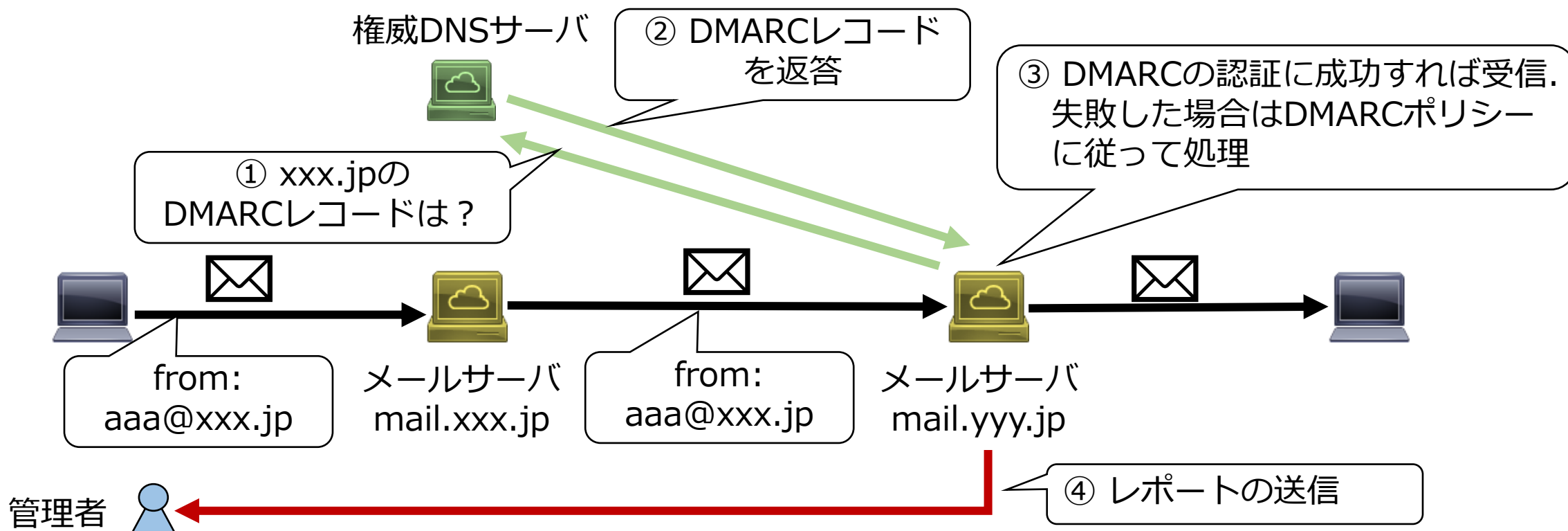
⑤ 検証鍵を取得



⑥ 検証

SPFやDKIMによる送信ドメイン認証を補完する仕組み

- ✓ SPFとDKIMに加え, **ヘッダFrom**に基づく認証
- ✓ 認証失敗時のポリシーの表明
- ✓ 認証に関するレポートの通知



演習：メールのヘッダ情報を読み解く

Return-Path: [REDACTED]@gmail.com
Authentication-Results: spf=softfail (sender IP is 133.42.52.25)
smtp.mailfrom=gmail.com; dkim=fail (signature did not verify)
header.d=gmail.com; dmarc=fail action=none header.from=gmail.com;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning gmail.com discourages use of 133.42.52.25 as permitted sender)
Received: from mgate.wakayama-u.ac.jp (133.42.52.25) by [REDACTED] mail.protection.outlook.com ([REDACTED])

(中略)

Received: by [REDACTED] google.com for fujimoto@center.wakayama-u.ac.jp
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20230601; t=1705951202; x=1706556002; darn=center.wakayama-u.ac.jp;
h=subject:from:mime-version:date:message-id:from:to:cc:subject:date:message-id:reply-to;
bh=電子署名;
b=メッセージのハッシュ

Received: from [REDACTED] ([REDACTED].it. [130. [REDACTED]]) by smtp.gmail.com
Date: Mon, 22 Jan 2024 11:20:01 -0800 (PST)
Content-Type: multipart/alternative; boundary="=====0523238906680888514=="
From: [REDACTED]@gmail.com
Subject: Call for Papers and Contributions | IEEE GEM 2024

上記は私の迷惑メールフォルダに振り分けられたメールのヘッダ部です。

- 何故、迷惑メール扱いされているかを考えてみてください。
- nslookupを用いて、SPF, DKIM, DMARCのレコードが取得できるか試してみてください
 - Windowsのコマンドプロンプト もしくは 演習環境のenshu1で実行できると思います