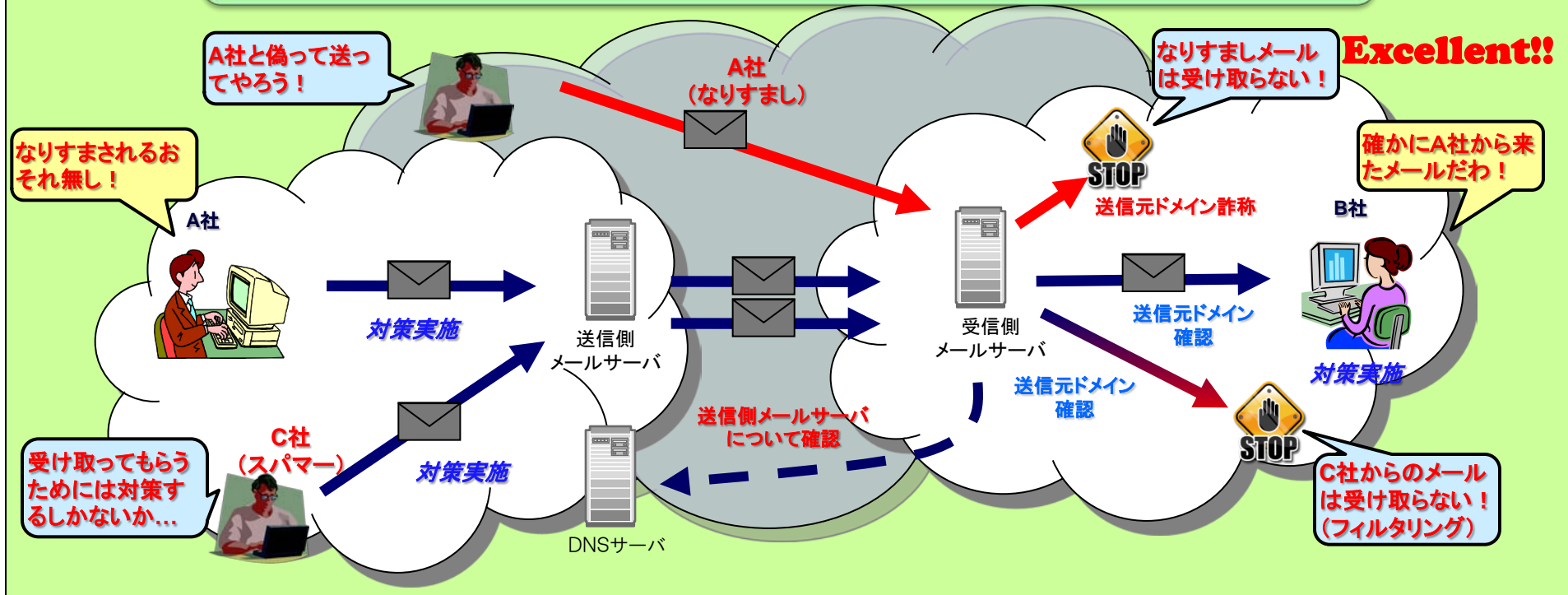


# 送信ドメイン認証技術の概要

別添

送信側・受信側双方で、送信ドメイン認証技術に対応すれば、なりすましかどうか確認することが可能に（信頼性の向上）！



## 概要

- ✓ 送信元情報のうちドメイン名が送信元に対して正当であることを技術的に確認可能
- ✓ 送信元情報をドメイン単位で判断
  - ・ DNS(Domain Name System)サーバと連携
- ✓ 既存のメール配送の仕組み(SMTP)を変更することなく、上位互換的に導入可能

## メリット

【送信側】送信するメールが受け取られやすくなる

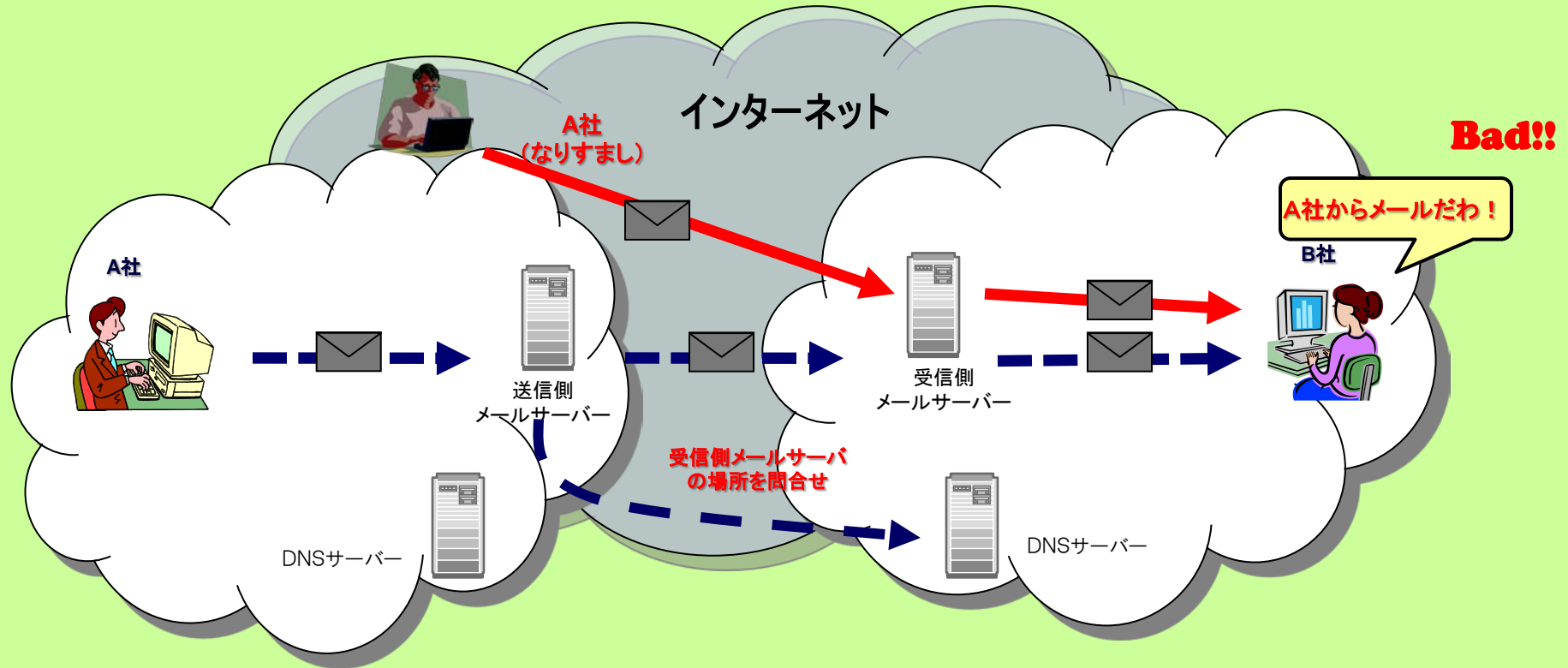
- ・ 自ドメインの信頼性の確保
- ・ 受信側が対応していれば、受け取られやすくなる

【受信側】受ける電子メールを選別することが可能

- ・ なりすましメールは、フィルタリングで処理
- ・ なりすましメールではないものは、さらに、フィルタリング等の他の技術と組み合わせることで、信頼できる送信者かを確認(効率的な迷惑メール対策)

# (参考) 電子メールの信頼性 (なりすましの問題)

- ✓ 特に、電子メールでは送信者情報の偽装 (なりすまし) が非常に容易であり、受信者が不要なメールを受信せざるを得ない状況であり、その信頼性が低下している



- ✓ **電子メールの protocols (通信手順: SMTP (simple mail transfer protocol)) では、電子メールの送受信に当たり、認証等が実施されず、送信者情報の偽装が容易**
  - ・ 送信側では、受信側メールサーバーの場所の問合せを行うため、ドメイン単位での確認はしているが、受信側ではそのような確認は行われない
- ✓ **ひろく定着しているため、これから protocol を変更していくことは、非現実的**
  - ・ 電子メールの基本的な protocol を変更するには、全世界のメールサーバーが一齊に対応することが必要と考えられる