

# 2025年フィッシングの動向と対策 & 最新メールセキュリティ



# ー 今日の流れ

- メール送信者ガイドラインと逆引きDNS設定
- 逆引きDNS(rDNS)がないサーバに対する対策

# 前提

---



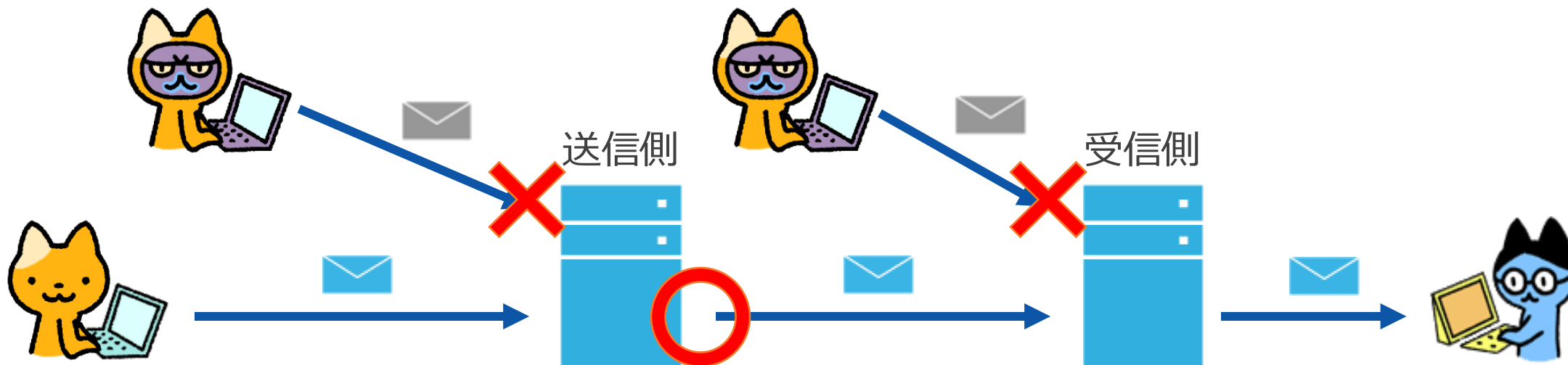
# 【前提】2つの側面でセキュリティ対策が必要

## 受信側での対策

- 送られてきたメールから迷惑メールを判別して届けないようにする

## 送信側での対策

- 迷惑メールを送信しないようにする
- 送信したメールが迷惑メールと扱われないようにする



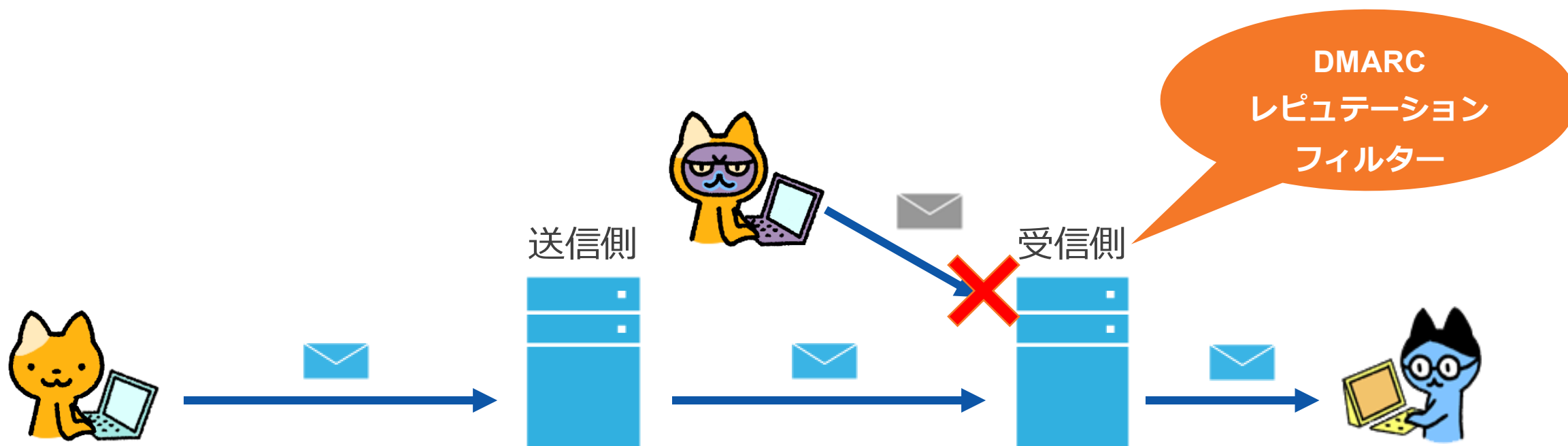
# 【前提】2つの側面でセキュリティ対策が必要

## 受信側での対策

- 送られてきたメールから迷惑メールを判別して届けないようにする

## 送信側での対策

- 迷惑メールを送信しないようにする
- 送信したメールが迷惑メールと扱われないようにする



## 受信側での対策

- 送られてきたメールから迷惑メールを判別して届けないようにする

## 送信側での対策

- 迷惑メールを送信しないようにする
- 送信したメールが迷惑メールと扱われないようにする



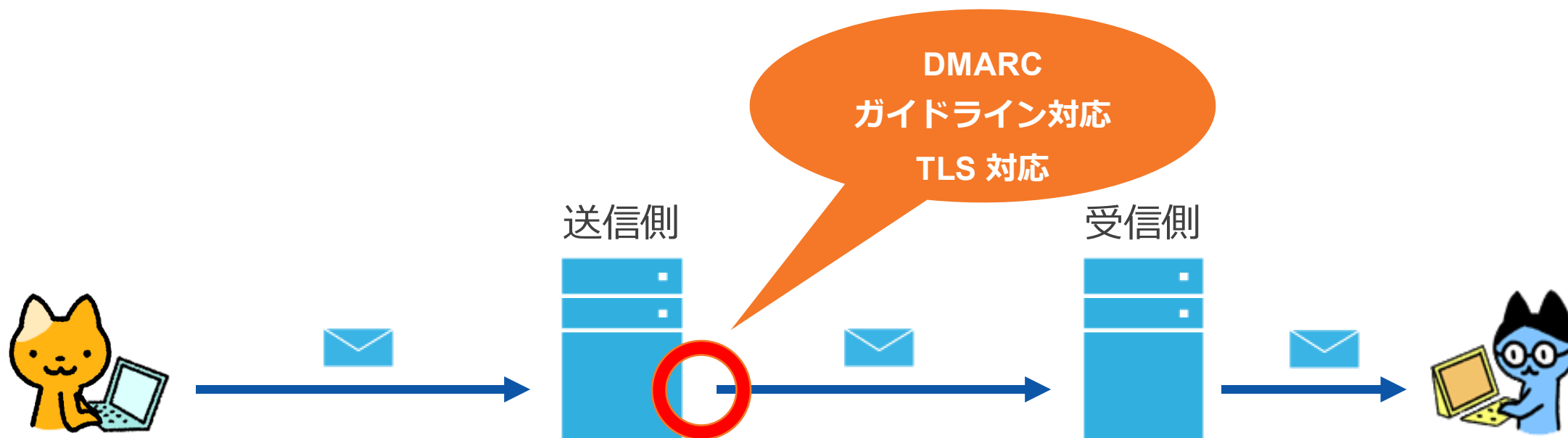
# 【前提】2つの側面でセキュリティ対策が必要

## 受信側での対策

- 送られてきたメールから迷惑メールを判別して届けないようにする

## 送信側での対策

- 迷惑メールを送信しないようにする
- 送信したメールが迷惑メールと扱われないようにする



# メール送信者ガイドライン



# Google/Yahoo(米国) メール送信ガイドライン

2023年10月3日Google/Yahoo(米国)がSPAM削減の為の新基準を発表

- 5000通以上の大量送信者は以下の条件を求められる
  - DMARCを設定すること
  - 購読解除可能にすること
  - SPAMレート0.3%未満であること
- 2024年2月1日から
- 詳細は今後発表されていく



これを満たせない場合は、受取拒否や迷惑メール扱い、流量制限等の何らかの制限を行う

-> Google やYahoo(米国)にメールが届かなくなるおそれ



# 海外メールサービス送信者ガイドラインのまとめ

|              | Google<br> | Yahoo Inc<br> | Apple<br> | Microsoft<br> |
|--------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| ガイドライン対象サービス | Gmail                                                                                       | Yahoo.com, AOL など                                                                                | iCloudメール                                                                                    | Microsoft 365                                                                                    |
| DMARC 対応     | ✓                                                                                           | ✓                                                                                                | ✓                                                                                            | ✓                                                                                                |
| ARC 対応       | メール転送の場合                                                                                    | —                                                                                                | メール転送の場合                                                                                     | メール転送の場合                                                                                         |
| 関連 RFC 準拠    | 5322, 8058                                                                                  | 5321, 5322, 8058                                                                                 | 5321, 5322                                                                                   | 2505, 2920, 5321, 5322                                                                           |
| 送信元サーバの適切な設定 | ✓                                                                                           | ✓                                                                                                | ✓                                                                                            | ✓                                                                                                |
| 正規メールの可視化    | BIMI 表示                                                                                     | BIMI 表示                                                                                          | BIMI 表示                                                                                      | —                                                                                                |
| オプトイン        | ✓                                                                                           | ✓                                                                                                | ✓                                                                                            | —                                                                                                |
| 購読解除リンク      | ✓                                                                                           | ✓                                                                                                | ✓                                                                                            | ✓                                                                                                |
| アドレスクリーニング   | 推奨                                                                                          | ✓                                                                                                | ✓                                                                                            | ✓                                                                                                |
| その他          | スパム率 0.3%以下<br>TLS 対応                                                                       | スパム率 0.3%以下<br>CAN-SPAM 対応                                                                       | 広告メールを明確に分離                                                                                  | CAN-SPAM 対応<br>IPレピュテーションの維持                                                                     |

<https://support.google.com/a/answer/81126>

<https://senders.yahooinc.com/best-practices/>

<https://support.apple.com/en-us/102322>

<https://learn.microsoft.com/en-us/defender-office-365/external-senders-policies-practices-guidelines>

<https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlook%E2%80%99s-new-requirements-for-high%E2%80%90volume-senders/4399730>

## ■ M<sup>3</sup>AAWG(Messaging Malware Mobile Anti-Abuse Working Group)

- メール送信する際のベストプラクティスをドキュメント化

簡便なオプトアウト

通知メールと広告の区別

送信ドメイン認証の対応

送信サーバの適正化

宛先のクリーニング



Messaging, Malware and Mobile Anti-Abuse Working Group

M<sup>3</sup>AAWG 送信者のベストコンプラクティス

第 3.0 版

2015 年 2 月更新

注意:本文書は、メールアドレス収集とデータの透明化の両プロセスに重点を置いて、2011 年 10 月に発行されたバージョン 2.0 を大幅に改定したものです。本文書は、前バージョンに含まれる MAAWG Sender Best Communications Practices および Executive Summary の両文書を置き換えるものです。いずれの文書も、バージョン 3.0 に組み込まれます。

### 要約

本文書は、運用上の技術および実践的なポリシーの側面に焦点を当てながら、商用の電子メッセージの送信に関する現行のベストコンプラクティスの概要を説明します。本文書は、ESP（電子メールサービスプロバイダー）および大規模な送信者で働く配信やコンプライアンスの専門家から、本文書に記載するプラクティスの承認および展開に関わるマーケティングや管理者までを対象読者としています。本文書は、電子メッセージの送信者による受信者メールアドレスの収集、利用および削除に関するプラクティスを取り扱っています。必要に応じて、本文書は所定のテーマに関して、詳細な情報を提供する他の文書へリンクをしています。

# M<sup>3</sup>AAWG Sender BCP

## ■ M<sup>3</sup>AAWG(Messaging Malware Mobile Anti-Abuse Working Group)

- メール送信する際のベストプラクティスをドキュメント化

簡便なオプトアウト

通知メールと広告の区別

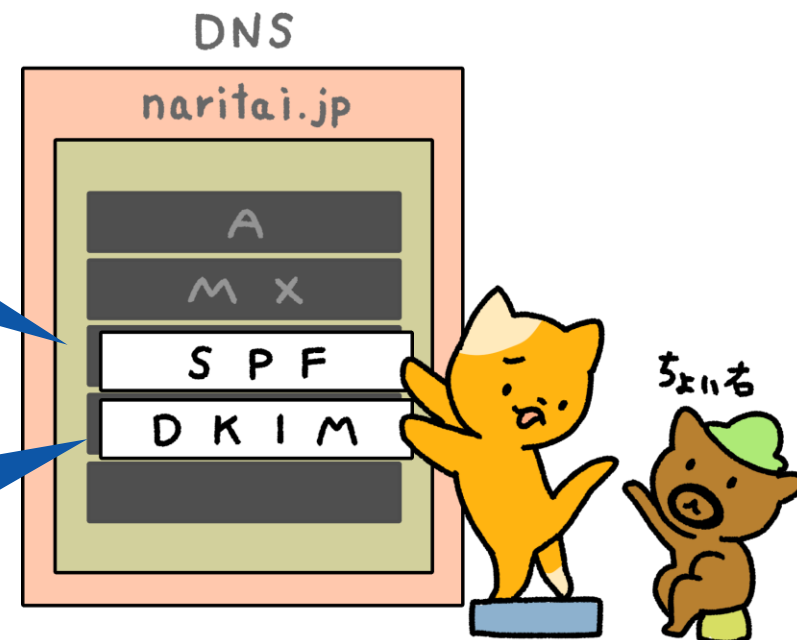
送信ドメイン認証の対応

送信サーバの適正化

宛先のクリーニング

送信元IPの認証

電子署名の認証



# M<sup>3</sup>AAWG Sender BCP

## ■ M<sup>3</sup>AAWG(Messaging Malware Mobile Anti-Abuse Working Group)

- メール送信する際のベストプラクティスをドキュメント化

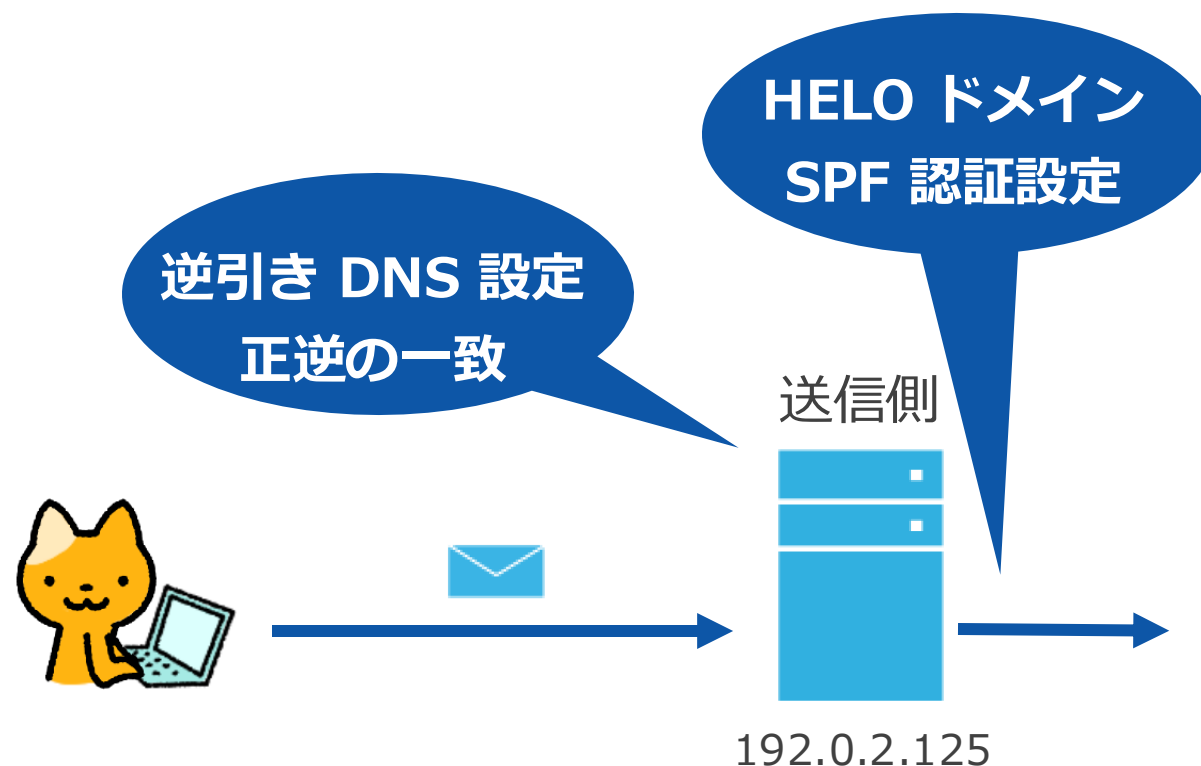
簡便なオプトアウト

通知メールと広告の区別

送信ドメイン認証の対応

送信サーバの適正化

宛先のクリーニング



# 逆引きDNS(rDNS)がないサーバ に対する対策

---



# — 逆引きDNSなし(rDNS)の対策はどのくらい効果があるか？

## ■ 受信側で実現できそうな対策

### ■ ブロッキング

- SMTP 接続時点で恒久エラー切断 (i.e. 5xx 応答)
- SMTP 接続時点で一時エラー切断 (i.e. 4xx 応答)
- SMTP 接続時点でグレイリスティング (i.e. 初回だけ 4xx 応答)

### ■ フィルタリング

- RCPT TO で一時的なエラー (i.e. 4xx 応答)
- メール受信後の振り分けその他のペナルティ

## ブロッキングとフィルタリング

- ・ 技術的にはどちらも同じ
  - ・ 特定サイトへのアクセスをISP設備で遮断すること
- ・ 技術的でない部分で異なる
  - ・ ブロッキング: 無条件に実施
    - ・ ブロッキングされたくない人のための代替手段は用意されない
  - ・ フィルタリング: ユーザの同意を得た上で実施
    - ・ フィルタリングされたくない人(同意しない人)のための代替手段が用意される

<https://www.nic.ad.jp/ja/materials/iw/sc-nara/proceedings/c22/c22-yamaguchi.pdf>

# SMTP 接続時点で恒久エラー切断 (i.e. 5xx 応答)

送信側が rDNS なしの場合は、接続のタイミングで拒否。  
レスポンスがないため、**送信側は拒否理由がわからない。**

203.0.113.100

送信側

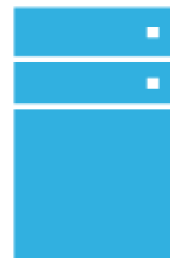


1

Connect



受信側



100.113.0.203.in-  
addr.arpa.

DNS



ユーザA

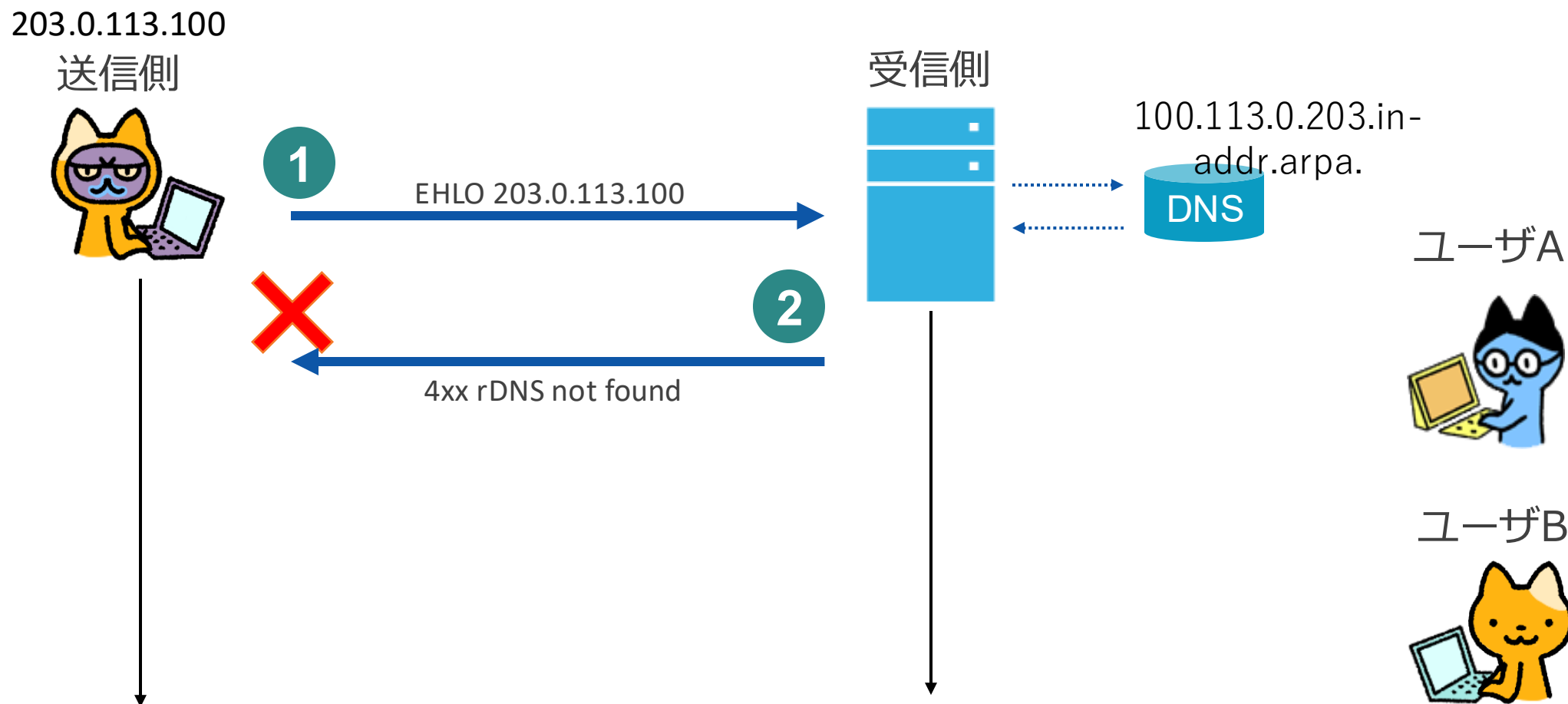


ユーザB



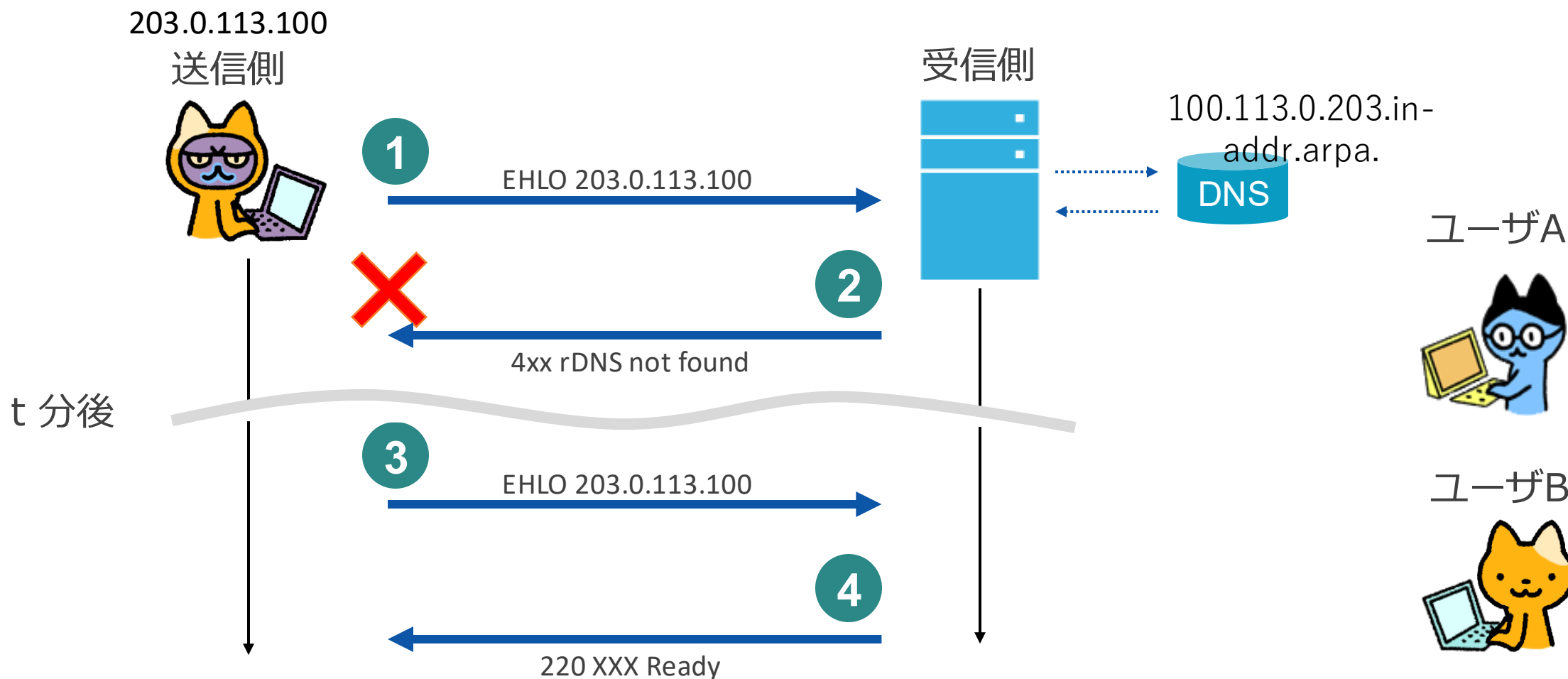
# SMTP 接続時点で一時エラー切断 (i.e. 4xx 応答)

送信側が rDNS なしの場合は、HELO/EHLO のタイミングで切断。  
SMTP 応答で理由が伝えられて、送信側が対応可能。



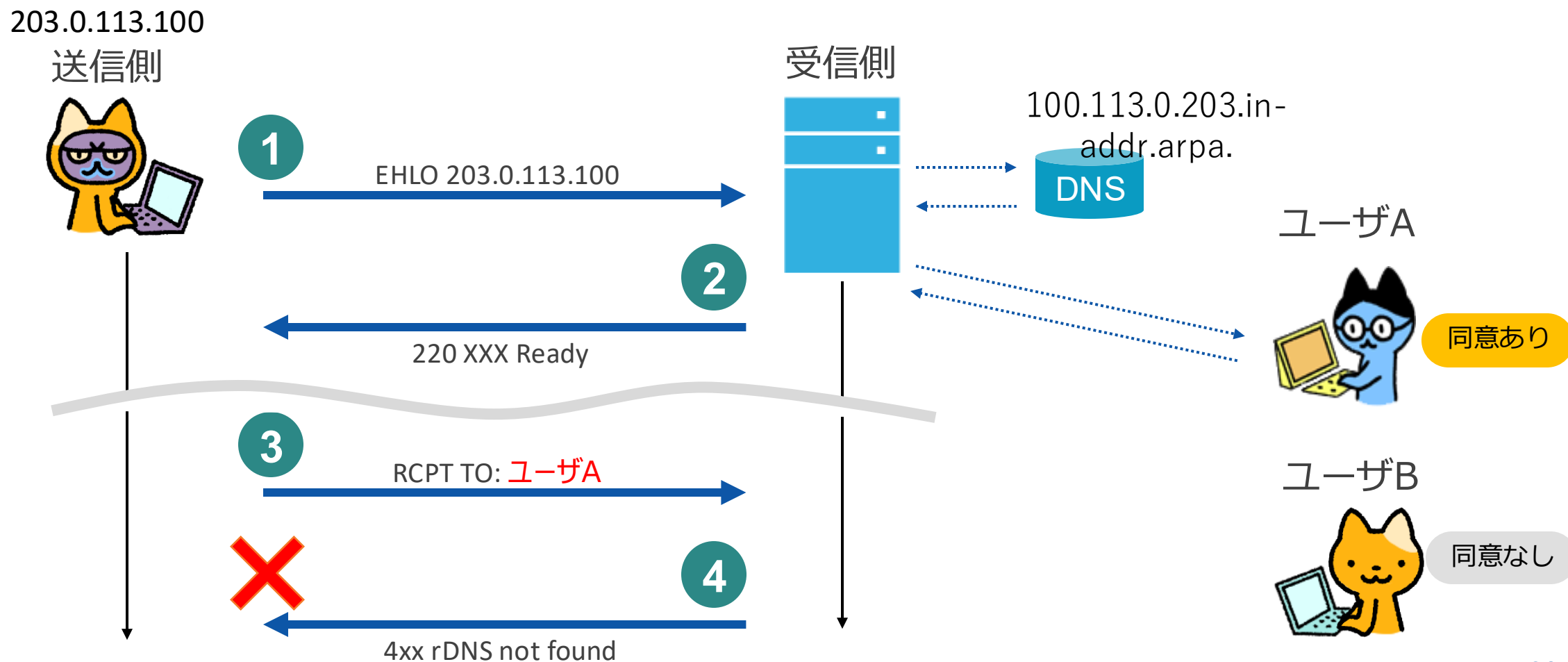
# SMTP 接続時点でグレイリスティング (i.e. 初回だけ 4xx 応答)

送信側が rDNS なしの場合は、HELO/EHLO のタイミングで切断。  
一定回数リトライすることで、未対応サーバでも再送が可能。



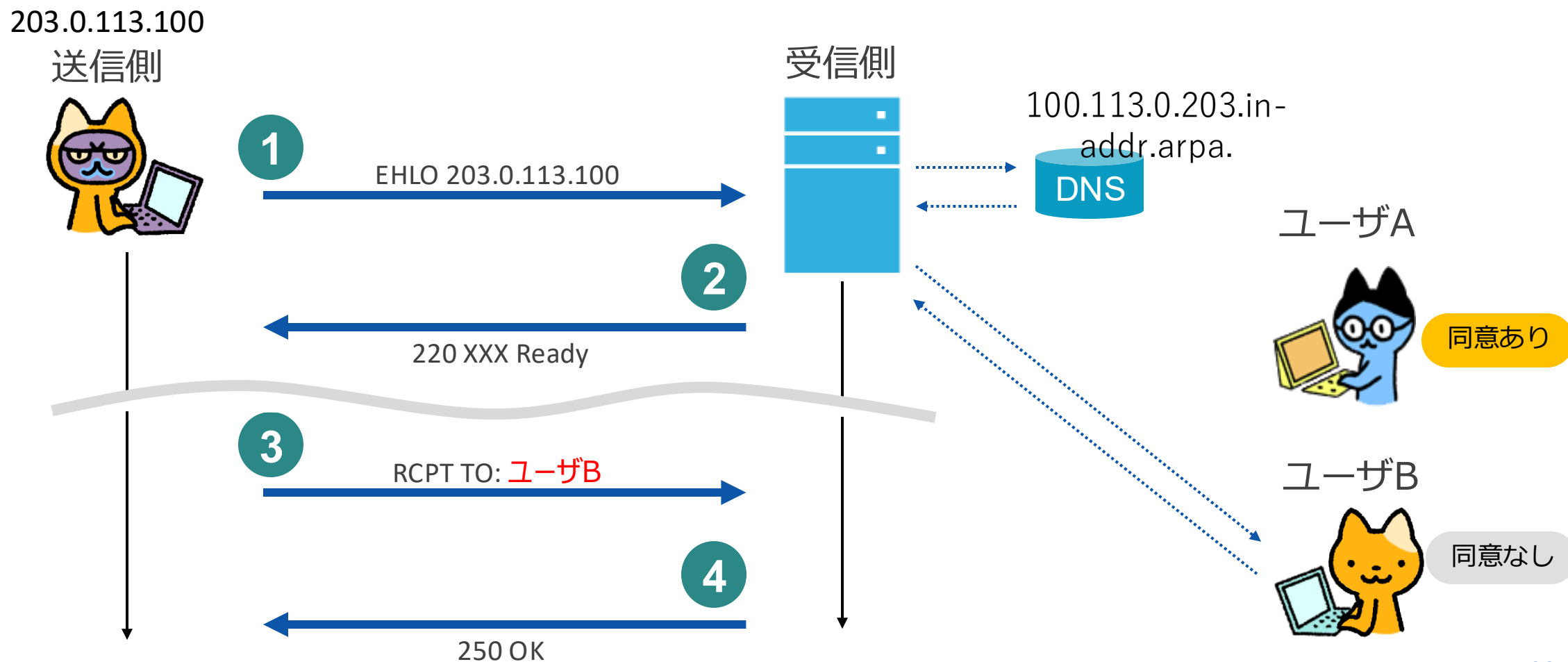
# RCPT TO で一時的なエラー (i.e. 4xx 応答)

送信側が rDNS なしの場合は、RCPT TO で宛先を特定した上で、個別同意があるユーザのみ拒否。



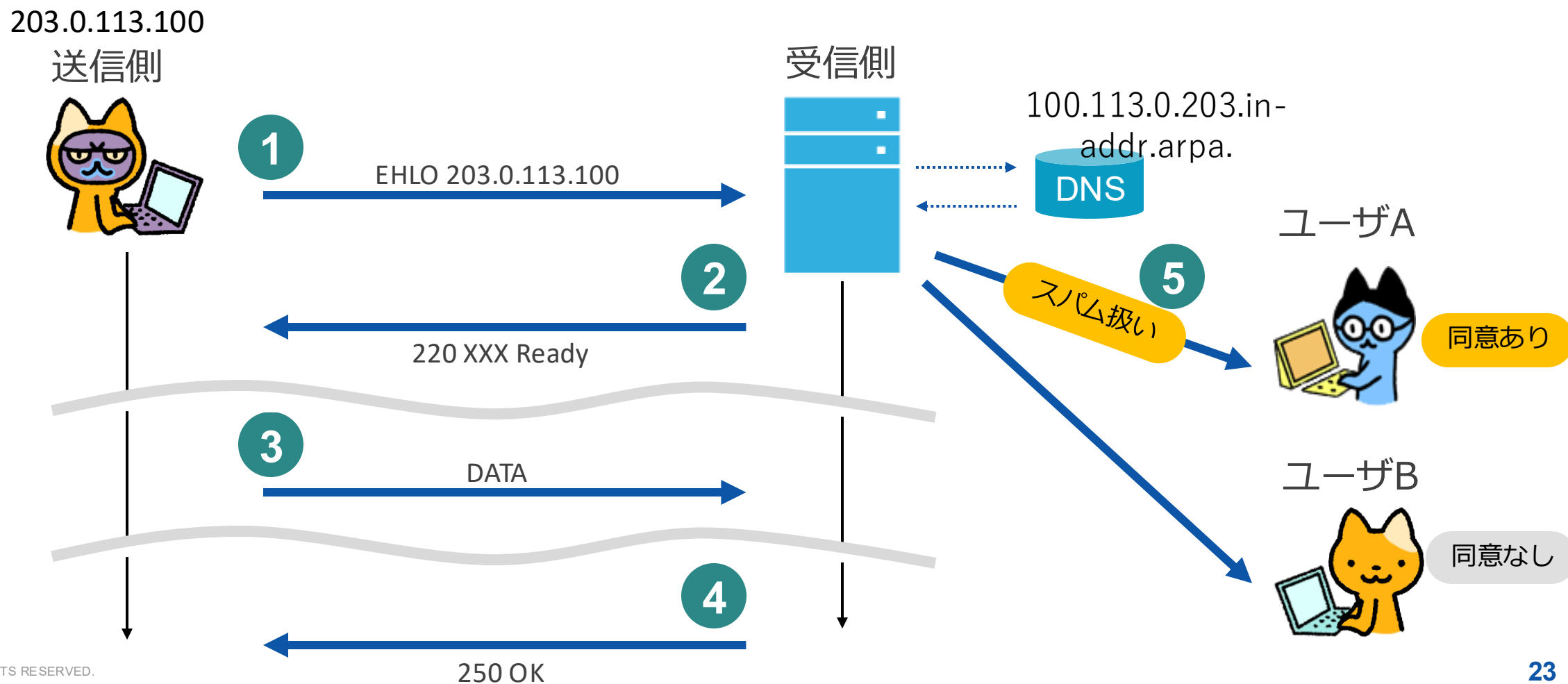
# RCPT TO で一時的なエラー (i.e. 4xx 応答)

送信側が rDNS なしの場合は、RCPT TO で宛先を特定した上で、個別同意があるユーザのみ拒否。個別同意がないユーザは受け付ける。



# メール受信後の振り分けその他のペナルティ

送信側が rDNS なしの場合は、同意があるユーザには「スパム扱い」「転送不可」「WebメールでURL無効化や警告」を実施。



# それぞれの対策の比較（2025.07.01 時点、独自調査）

|              | 接続拒否   | 一時エラー | グレイリスト | 個別エラー   | 受信後対応 |
|--------------|--------|-------|--------|---------|-------|
| 分類           | ブロッキング |       |        | フィルタリング |       |
| 対策の効果        | ○      | ○     | △      | 限定的     | 限定的   |
| FPの悪影響       | ×      | ×     | △      | —       | —     |
| ↳ FP 回避策     | 救済リスト  | 救済リスト | 救済リスト  | —       | —     |
| 理由の通知        | ×      | ○     | ○      | ○       | ×     |
| 実装の難易度       | ○      | ○     | △      | △       | 難     |
| ↳ Postfix 設定 | ○(*1)  | ○(*1) | △(*2)  | △(*3)   | ×     |
| ↳ Rspamd 設定  | ○      | ○     | ○      | ○       | ×     |

\*1: reject\_unknown\_reverse\_client\_hostname と unknown\_client\_reject\_code を利用して設定可能

\*2: Postgrey を milter 利用することで可能

\*3: LDAP や check\_policy\_service を連携させて、個別ユーザごとに適用・利用することで可能

## ー このパートのまとめ

### ■ メール送信者ガイドラインと逆引きDNS設定

- Google/Yahoo.com/Microsoft のガイドライン
- M<sup>3</sup>AAWG Sender BCP
- 送信側のメールサーバは逆引きDNS設定することが大事

### ■ 逆引きDNS(rDNS)がないサーバに対する対策

- ブロッキング(3方式)とフィルタリング(2方式)
- 5つの対策とその比較