IIJ Internet Initiative Japan

2023 年度版 迷惑メール動向と対策事例の紹介

2023/11/07

株式会社インターネットイニシアティブ(IIJ)
ネットワーク本部　アプリケーションサービス部　運用技術課
課長　古賀 勇

Ongoing Innovation

想定所要時間 40分

自己紹介

古賀 勇 (Isamu Koga)

株式会社インターネットイニシアティブ(IIJ)
ネットワーク本部 アプリケーションサービス部 運用技術課 課長
(兼) 社長室

Power Automate エバンジェリスト (自称) **「自動化は正義」**

法人系メールセキュリティサービスの運用

SecureMX

- ウイルス対策
- 迷惑メール対策
- Sandbox
- 送信ドメイン認証
- 顧客サポート
- 執筆活動・公演活動・エンジニアブログ・技報

WIDE Project

M3AAWG

openSUSE (趣味)

昨年(第5回) JPAAWG のおさらい

第5回 JPAAWG のおさらい

「現場発！メールサービスを支える運用者の集い 2022 秋」より

第5回 JPAAWG

A2-6 現場発！メールサービスを支える運用者の集い 2022秋

IIJ Internet Initiative Japan

「悪」と戦うためにやった 2 つのこと

2022/11/08

株式会社インターネットイニシアティブ(IIJ)
ネットワーク本部 アプリケーションサービス部 運用技術課
課長 古賀 勇

Ongoing Innovation

想定時間 5分

第5回 JPAAWG のおさらい

「現場発！メールサービスを支える運用者の集い 2022 秋」より

(1) PPAP 廃止しました、みんなでやめましょう

IIJ の方針表明、2022年 1月 26日に パスワード付き ZIP 運用を全面廃止

https://www.iij.ad.jp/ppap/

https://eng-blog.iij.ad.jp/archives/79

(1) PPAP 廃止しました、みんなでやめましょう

パスワード付き ZIP 廃止までの流れ

約 1年間

- 情報システム部門から危機管理部門・経営層への説明
- 経営層から社内へのリ…
- 情報システム部門での対策実現のための検討
- 情報セキュリティ担当部門…
- 各部門への説明とスケジュールの展開
- お客様・…
- ポリシーの変更

社内の意思決定と色んな所への説明

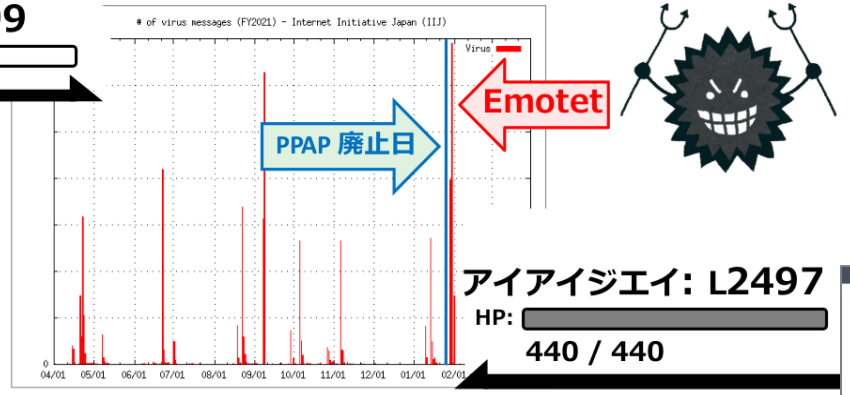
顧客への説明と実行

第5回 JPAAWG のおさらい

「現場発！メールサービスを支える運用者の集い 2022 秋」より

(1) PPAP 廃止しました、みんなでやめましょう

エモテット: L9999
HP:



アイアイジエイ: L2497
HP:
440 / 440

こうかは ばつぐんだ！

(1) PPAP 廃止しました、みんなでやめましょう

サービス説明ページからも消しました

添付ファイル暗号化機能※の利用はおすすめしません

※ 2009年リリース。当時、顧客の要望が大きく本機能の開発を決断した。

PPAP 廃止で
Emotet 一網打尽

第5回 JPAAWG のおさらい

「現場発！メールサービスを支える運用者の集い 2022 秋」より

(2) DMARC p=reject しました、みんなでやりましょう

送信ドメイン認証に失敗したメールは受信拒否してくれていい、という強い意志表明

受信者がなりすましメールを見分けられる

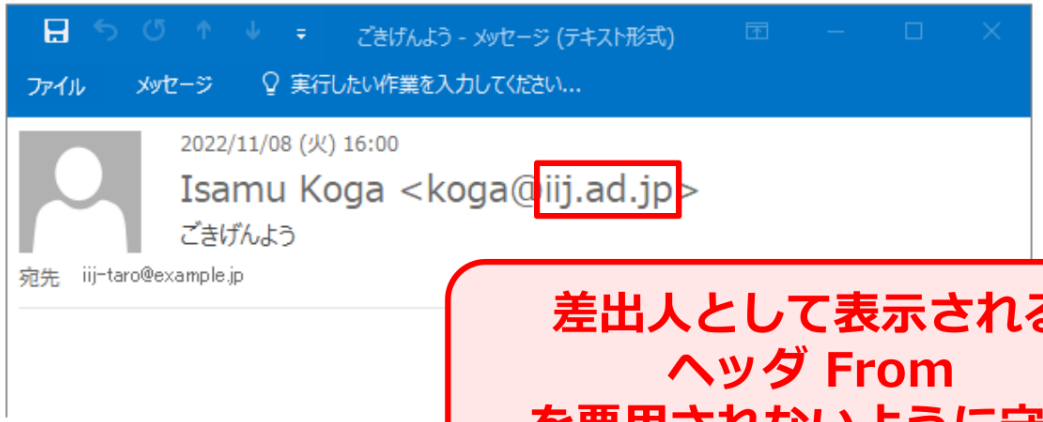
送信者のブランドが守られる

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあり

DMARC で
IIJ ブランドを保護

(2) DMARC p=reject しました、みんなでやりましょう

私たちの守りたい部分

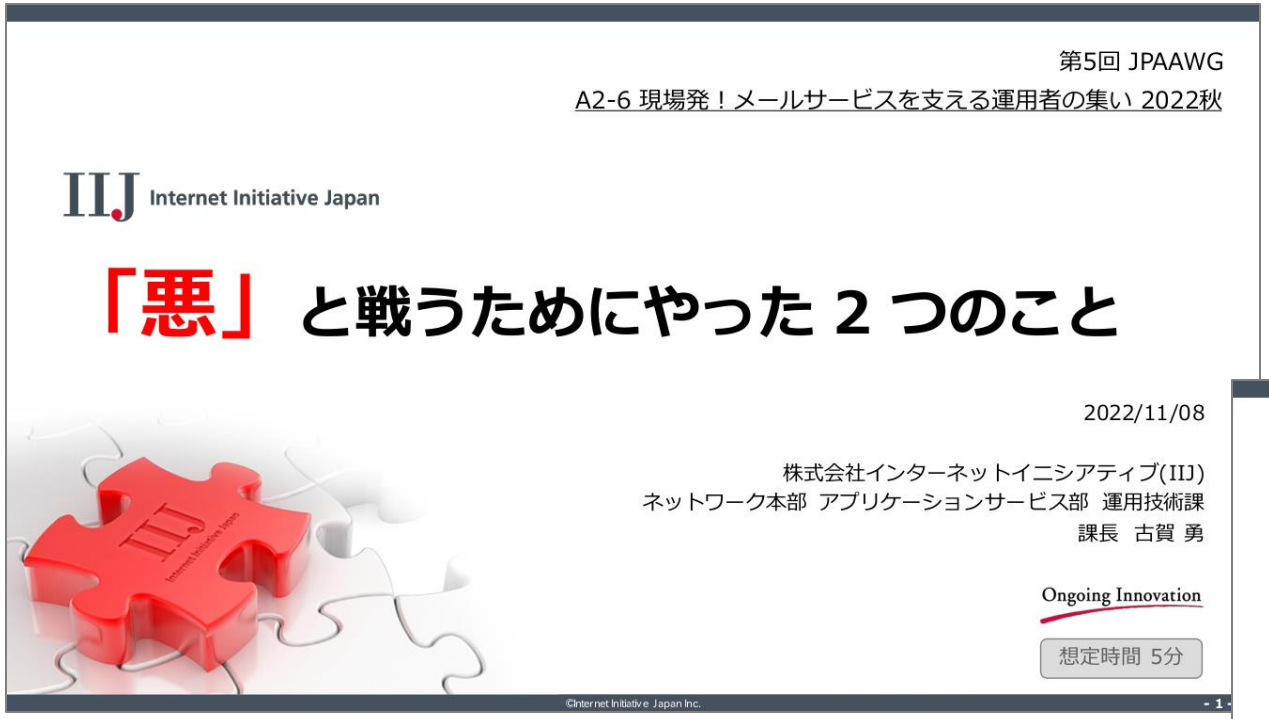


**差出人として表示される
ヘッダ From
を悪用されないように守る**

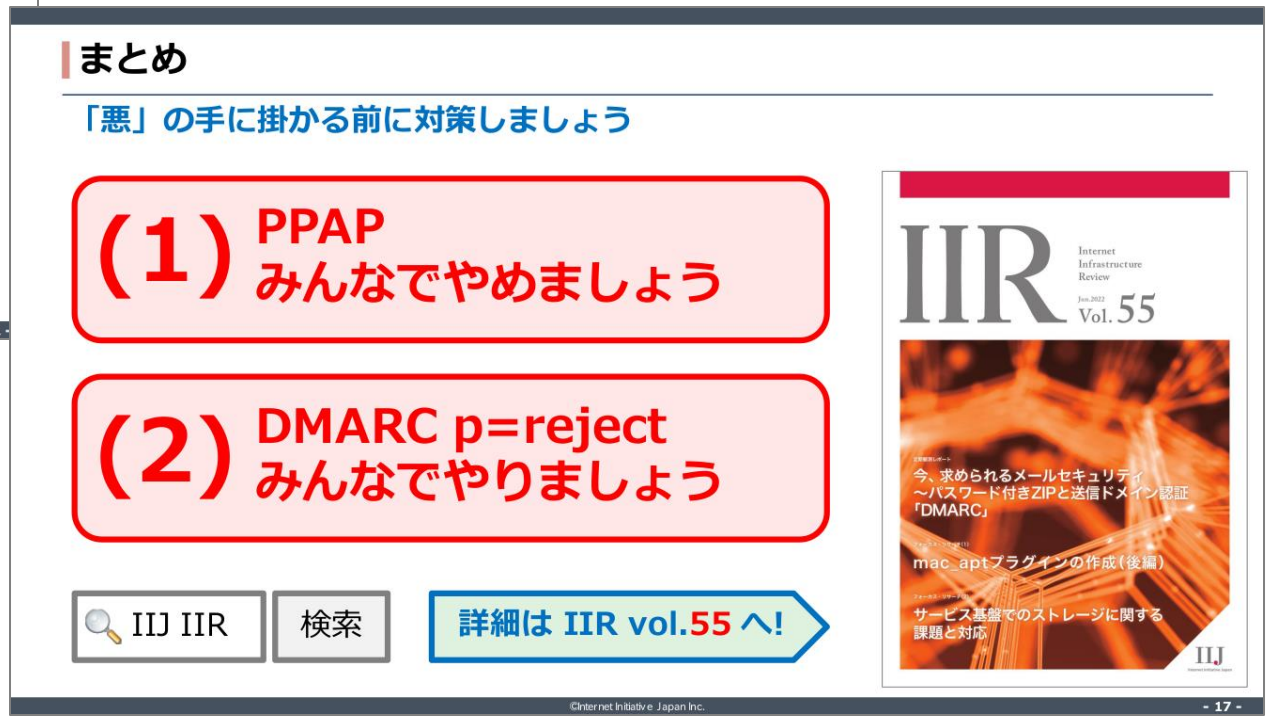
※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

第5回 JPAAWG のおさらい

「現場発！メールサービスを支える運用者の集い 2022 秋」より



PPAP 廃止で
Emotet 一網打尽

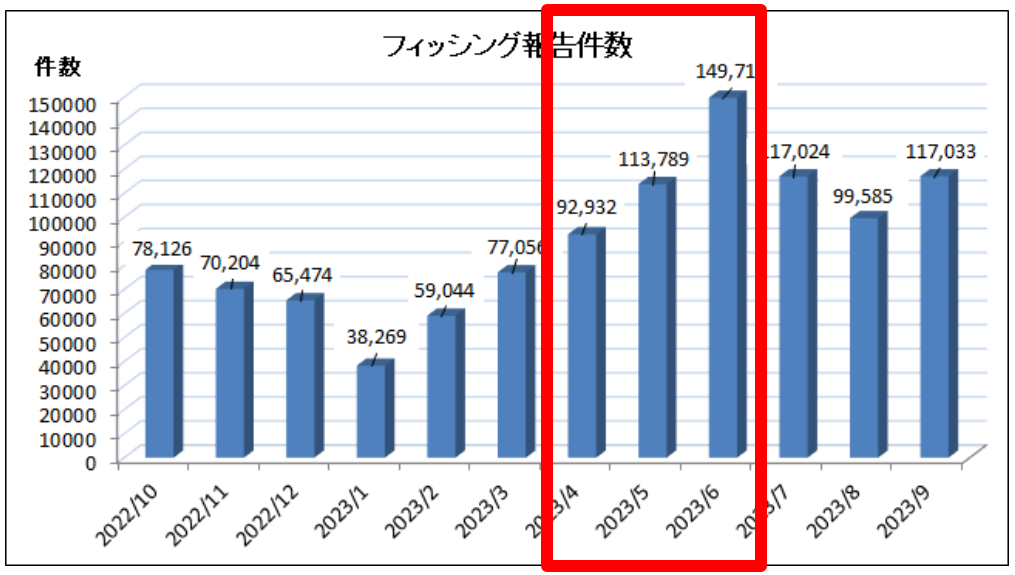


DMARC で
IIJ ブランドを保護

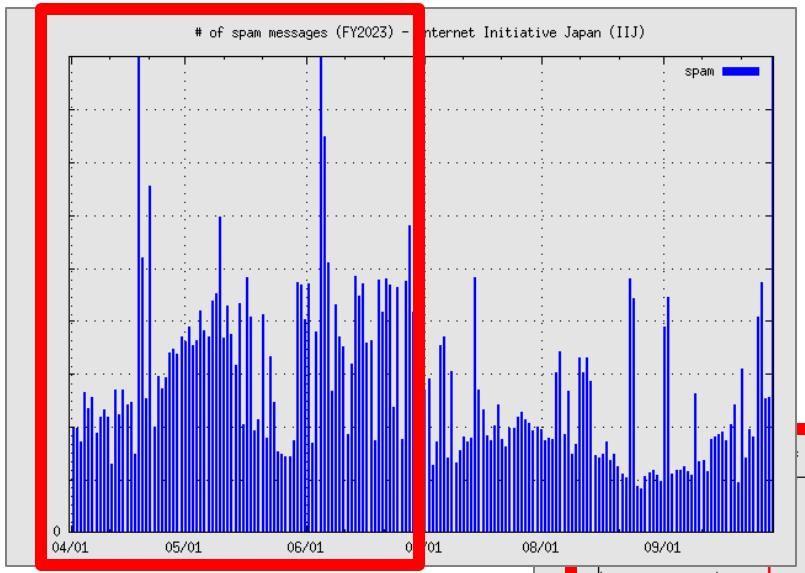
近年のフィッシングメール傾向

2023年度 フィッシングメール・ウイルスメールの傾向

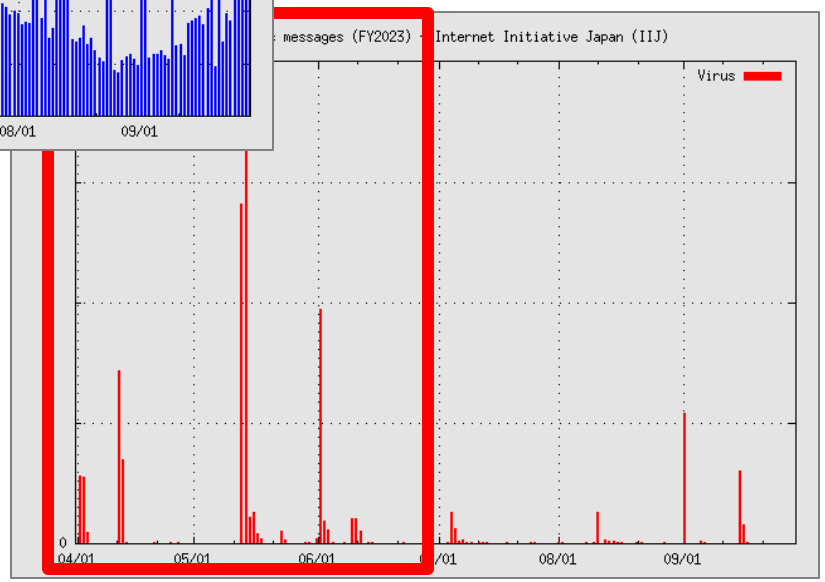
時折スパイクする傾向が見られる



▲ フィッシング対策協議会 月次報告書 (2023/09)
https://www.antiphishing.jp/report/monthly/202309.html



▲ 迷惑メール
(IIJ ハニーポットで計測)



▲ ウイルス (IIJ ハニーポットで計測)

2023年 4～6月に迷惑メールが増加

ちょっと待てよ、この手の話...

何度も聞いてない...?

近年のフィッシングメールの傾向

大手金融機関
が狙われる

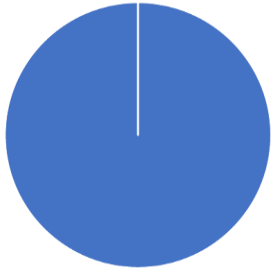
近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関
が狙われる

⇩ **DMARC で対策**

近年のフィッシングメールの傾向



DMARC 対応率
100%

大手金融機関
が狙われる

⇩ **DMARC で対策**

クレジットカード
会社が狙われる

近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関が狙われる

DMARC で対策

DMARC 対応率
100%

クレジットカード会社が狙われる

DMARC で対策

近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関が狙われる

DMARC で対策

DMARC 対応率
100%

クレジットカード会社が狙われる

DMARC で対策

ネットバンキングが狙われる

近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関が狙われる

⇩ **DMARC で対策**

DMARC 対応率
100%

クレジットカード会社が狙われる

DMARC で対策

ネットバンキングが狙われる

⇩ **DMARC で対策**

DMARC 対応率
73%

近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関が狙われる

DMARC で対策

DMARC 対応率
100%

クレジットカード会社が狙われる

DMARC で対策

ネットバンキングが狙われる

DMARC 対応率
73%

DMARC で対策

地方銀行が狙われる

近年のフィッシングメールの傾向

DMARC 対応率
100%

大手金融機関が狙われる

⇩ **DMARC で対策**

DMARC 対応率
100%

クレジットカード会社が狙われる

DMARC で対策

ネットバンキングが狙われる

⇩ **DMARC で対策**

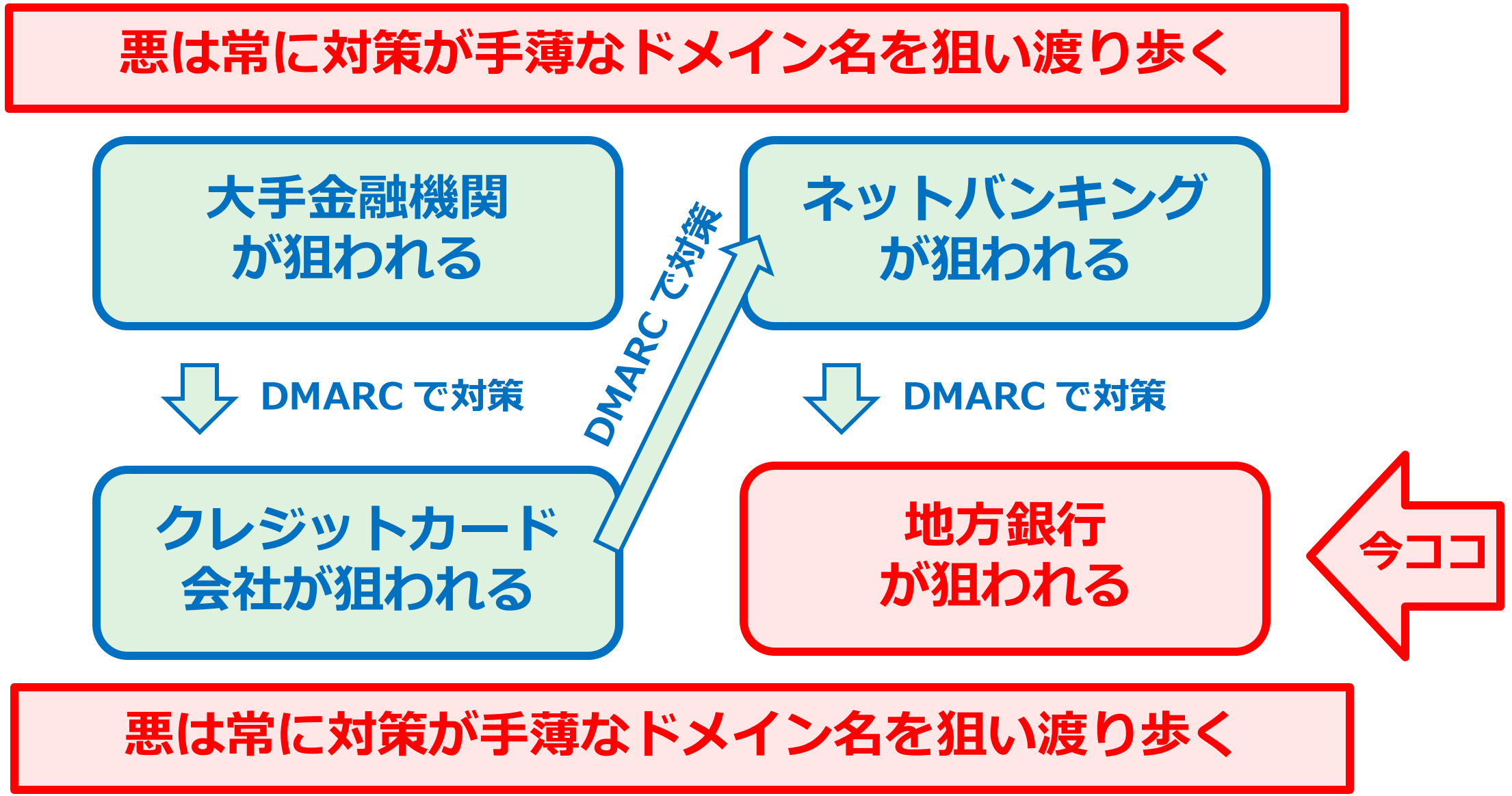
地方銀行が狙われる

DMARC 対応率
73%

今ココ


（結論）
歴史は
繰り返される

近年のフィッシングメールの傾向



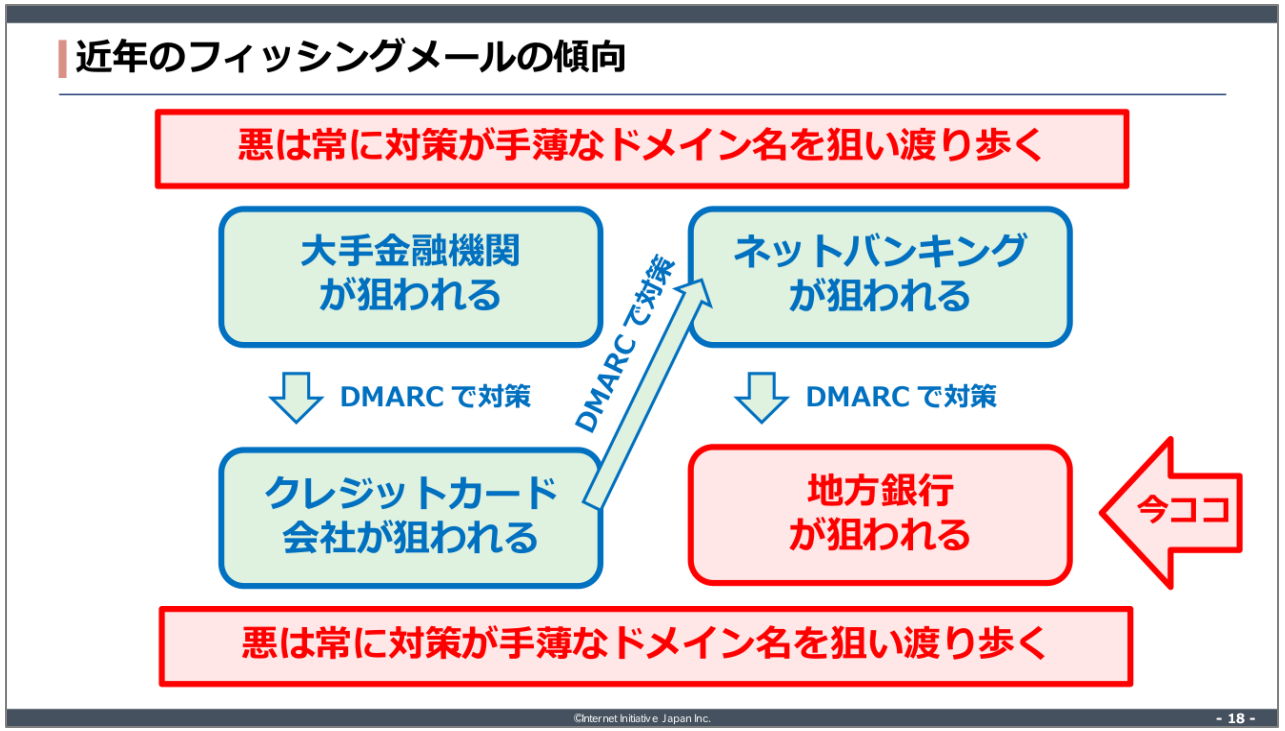
まとめ (1)

悪に狙われる前に、やはり DMARC 対応しましょう

DMARC p=reject みんなでやりましょう

(悪の視点) 送信ドメイン認証に失敗するドメイン名はなりすます価値がない

次、狙われるのは御社のドメイン名かも...



今日の本題

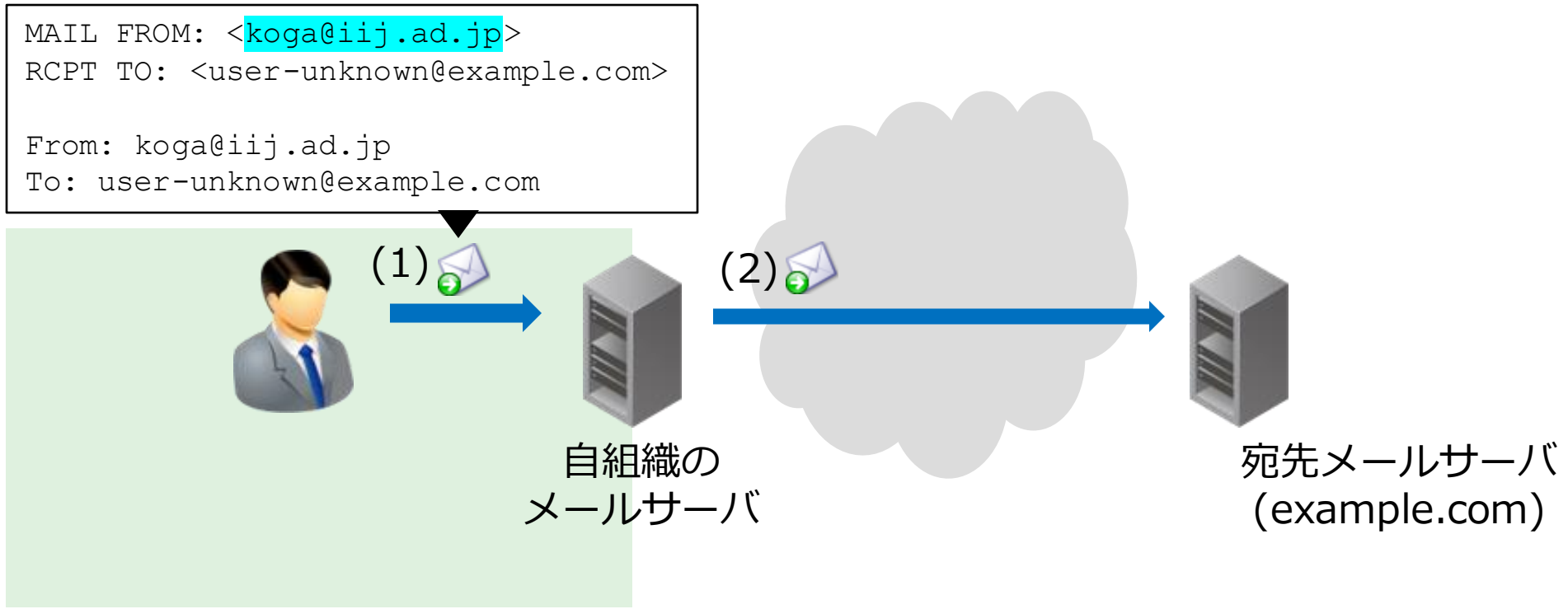
みんなが DMARC 対応したあと
どういう世界が待っているのか

Case 1

通常の送信エラーの例 (宛先不明など)

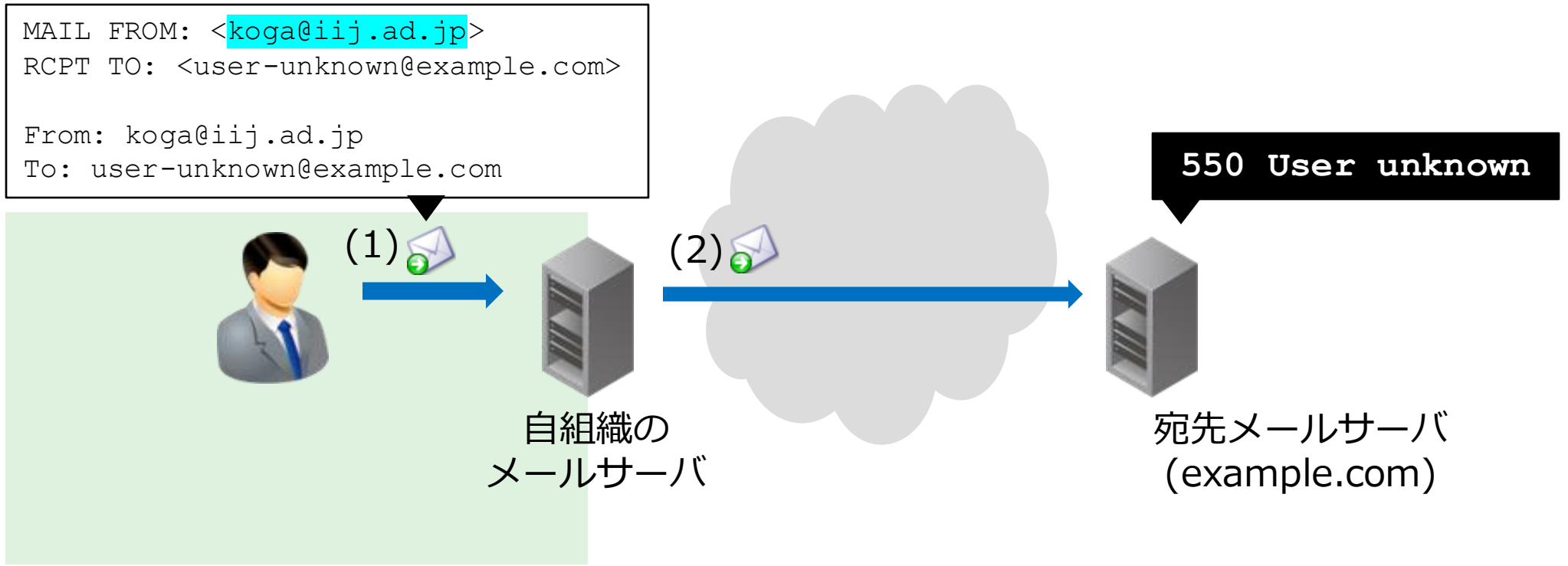
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 1】通常の送信エラーの例 (宛先不明など)



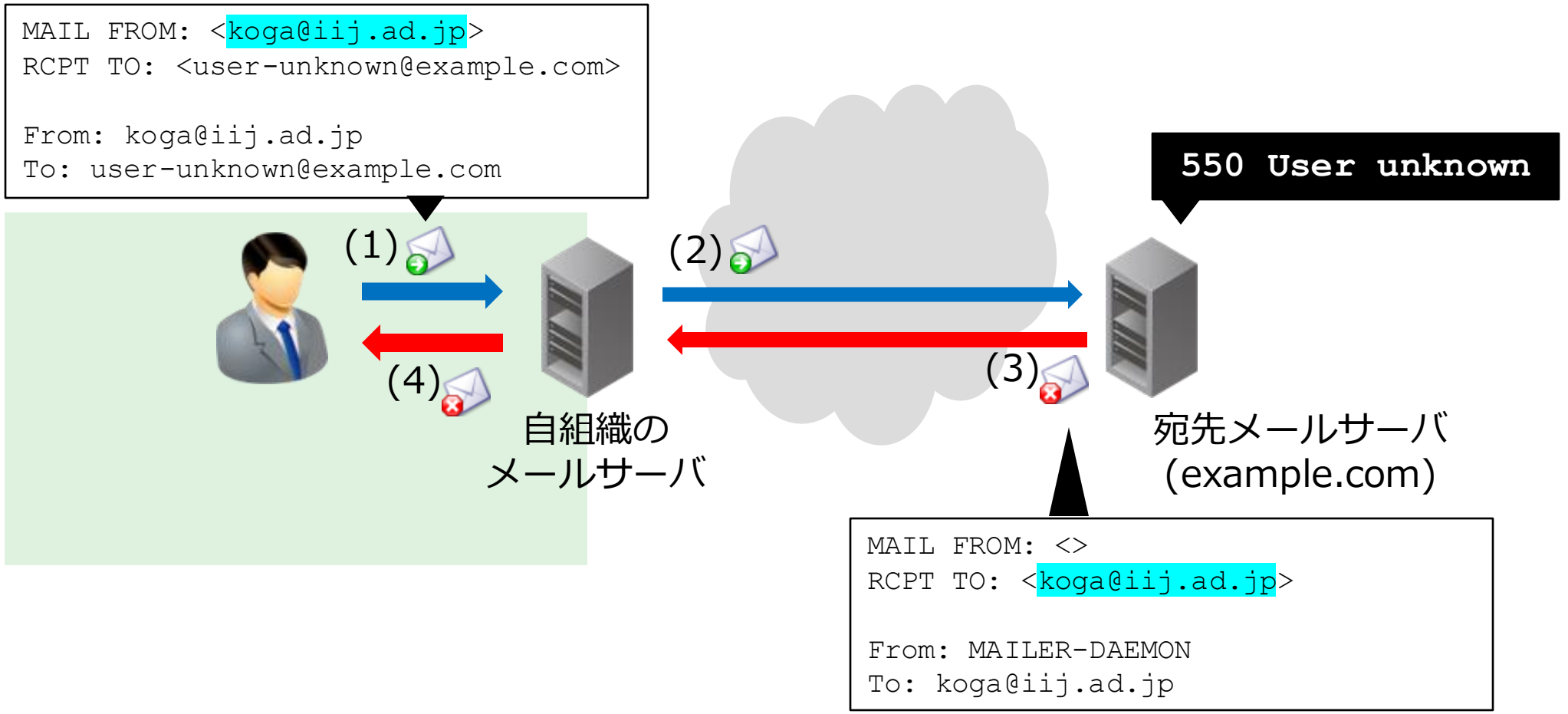
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 1】通常の送信エラーの例 (宛先不明など)



みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 1】通常の送信エラーの例 (宛先不明など)

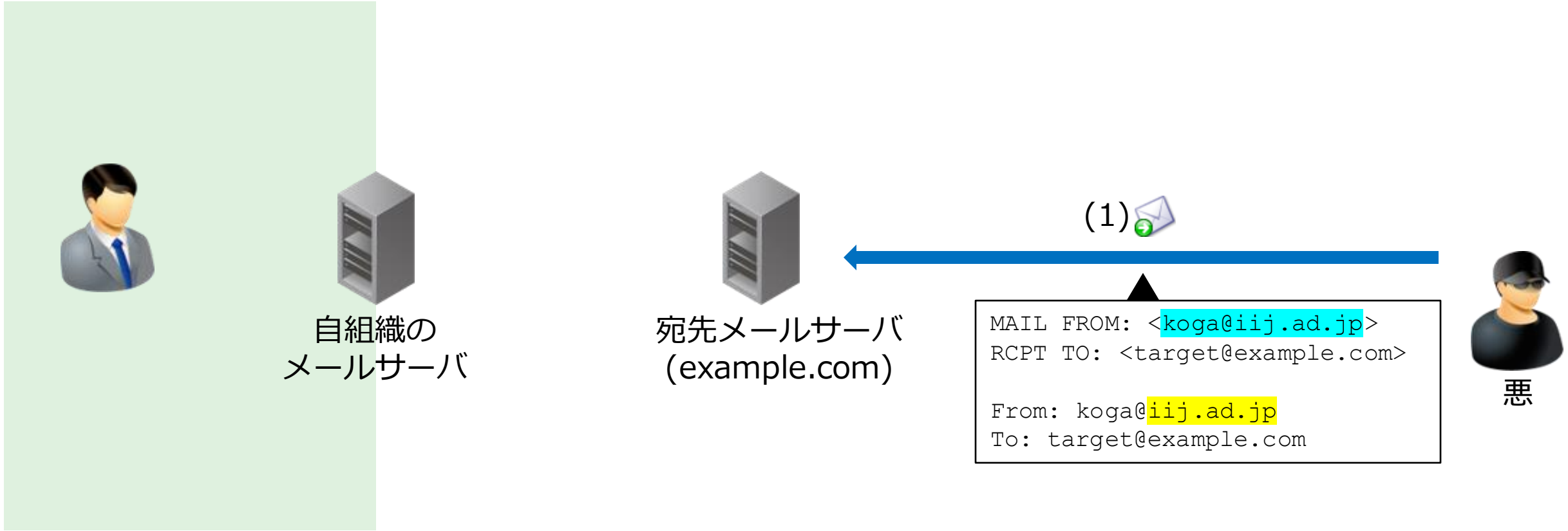


Case 2

悪の組織が なりすましメールを送って エラーになる例

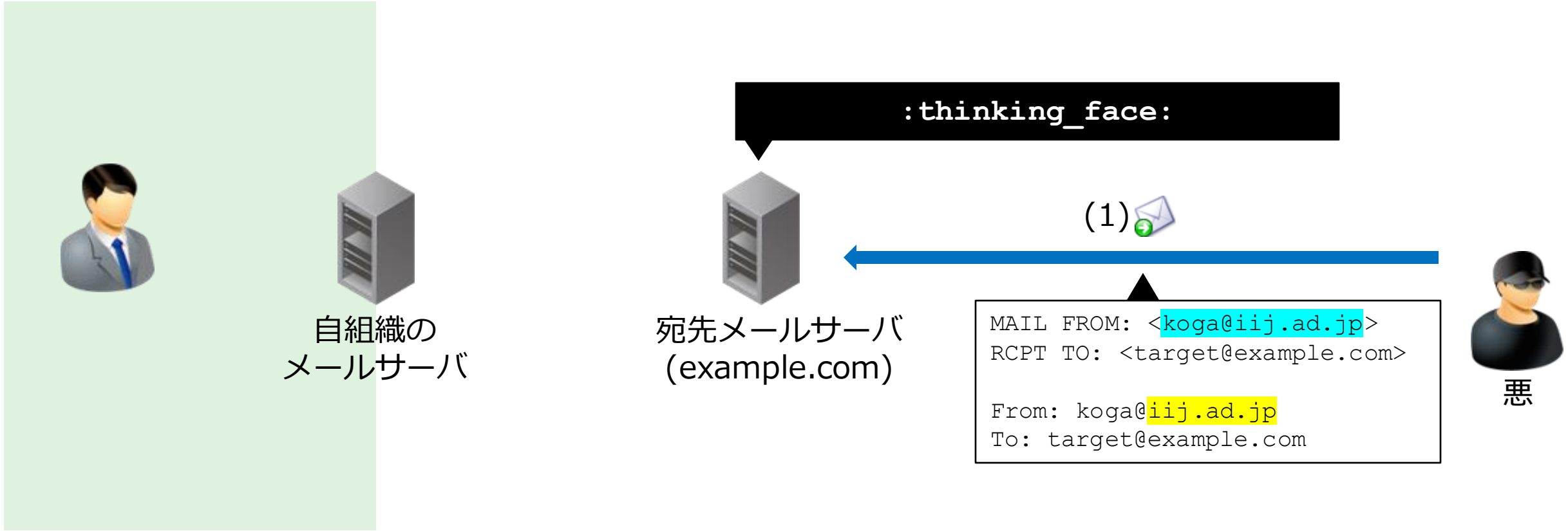
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 2】悪の組織が なりすましメールを送ってエラーになる例



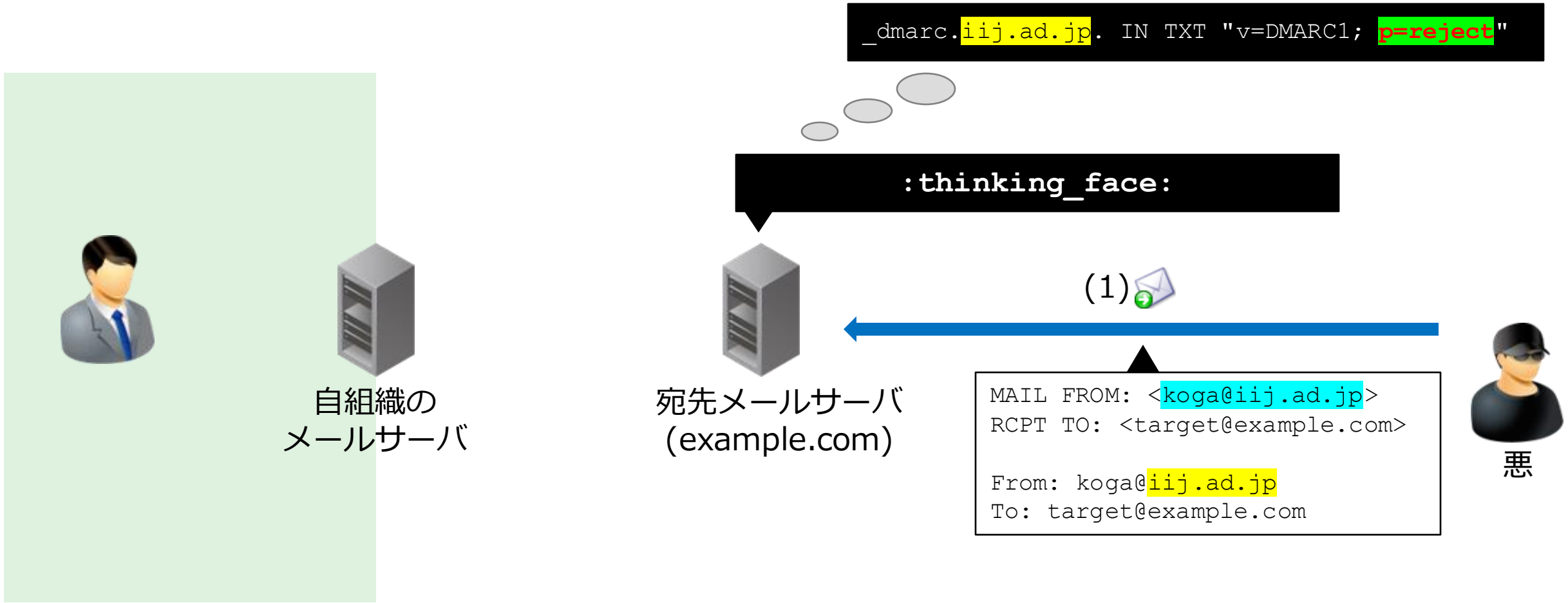
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 2】悪の組織が なりすましメールを送ってエラーになる例



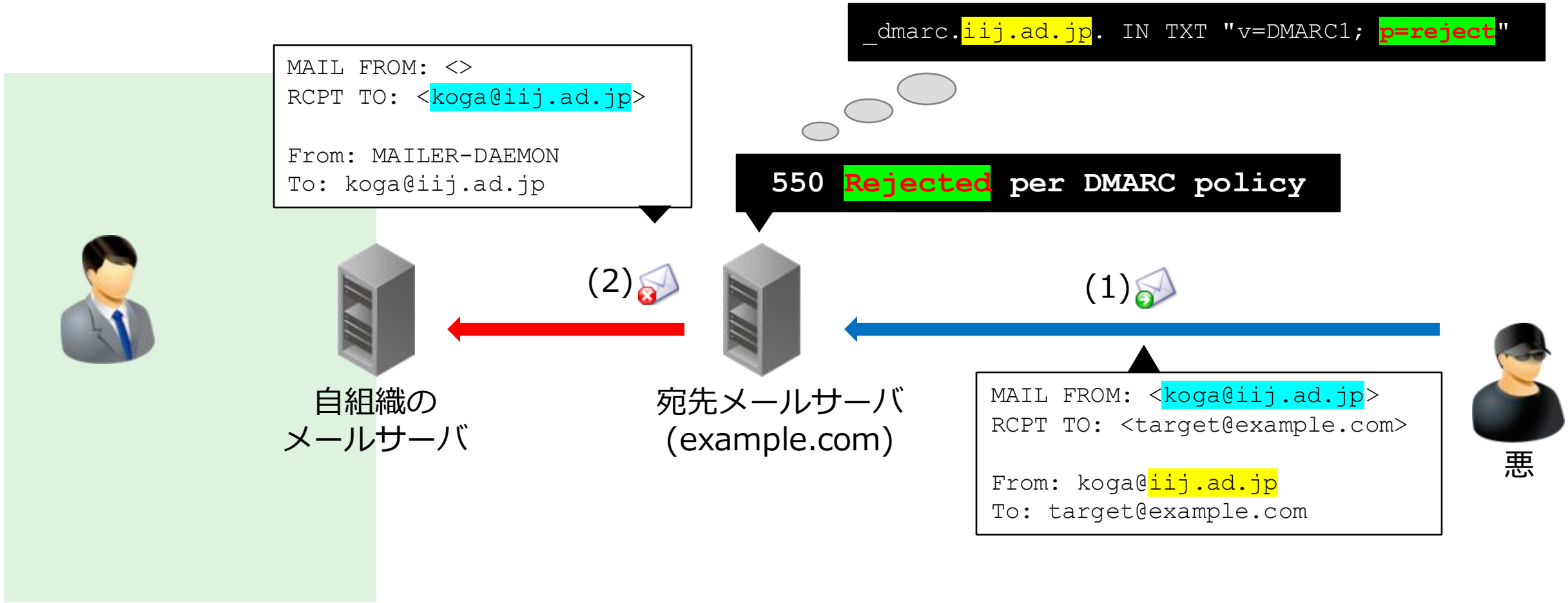
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 2】悪の組織が なりすましメールを送ってエラーになる例



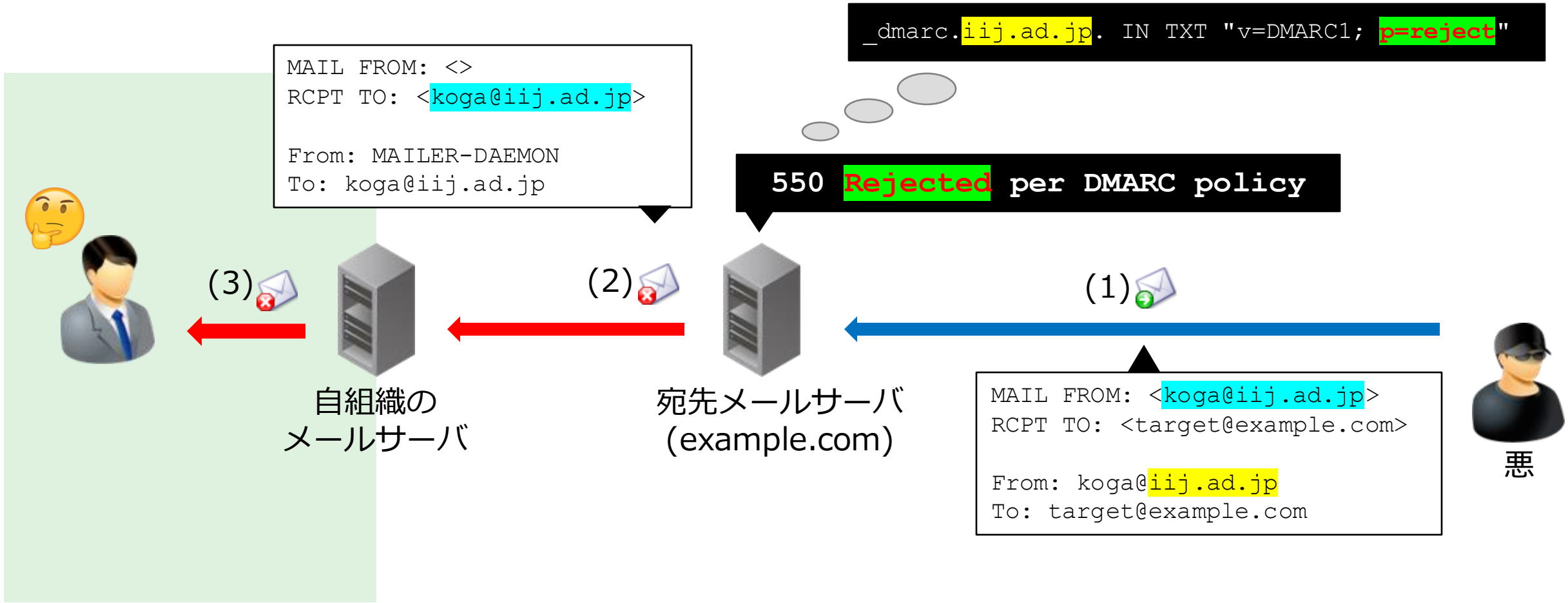
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 2】悪の組織が なりすましメールを送ってエラーになる例



みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 2】悪の組織が なりすましメールを送ってエラーになる例

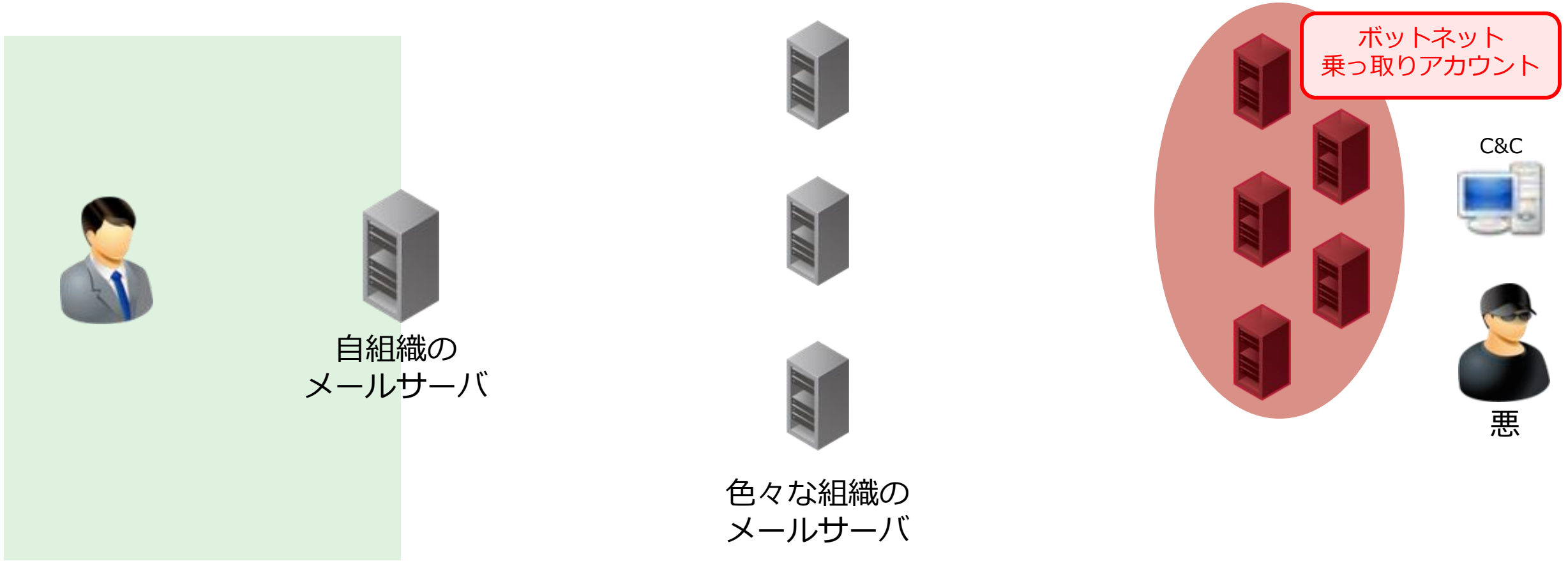


Case 3

悪の組織が なりすましメールを送って
エラーになる例 (大量)

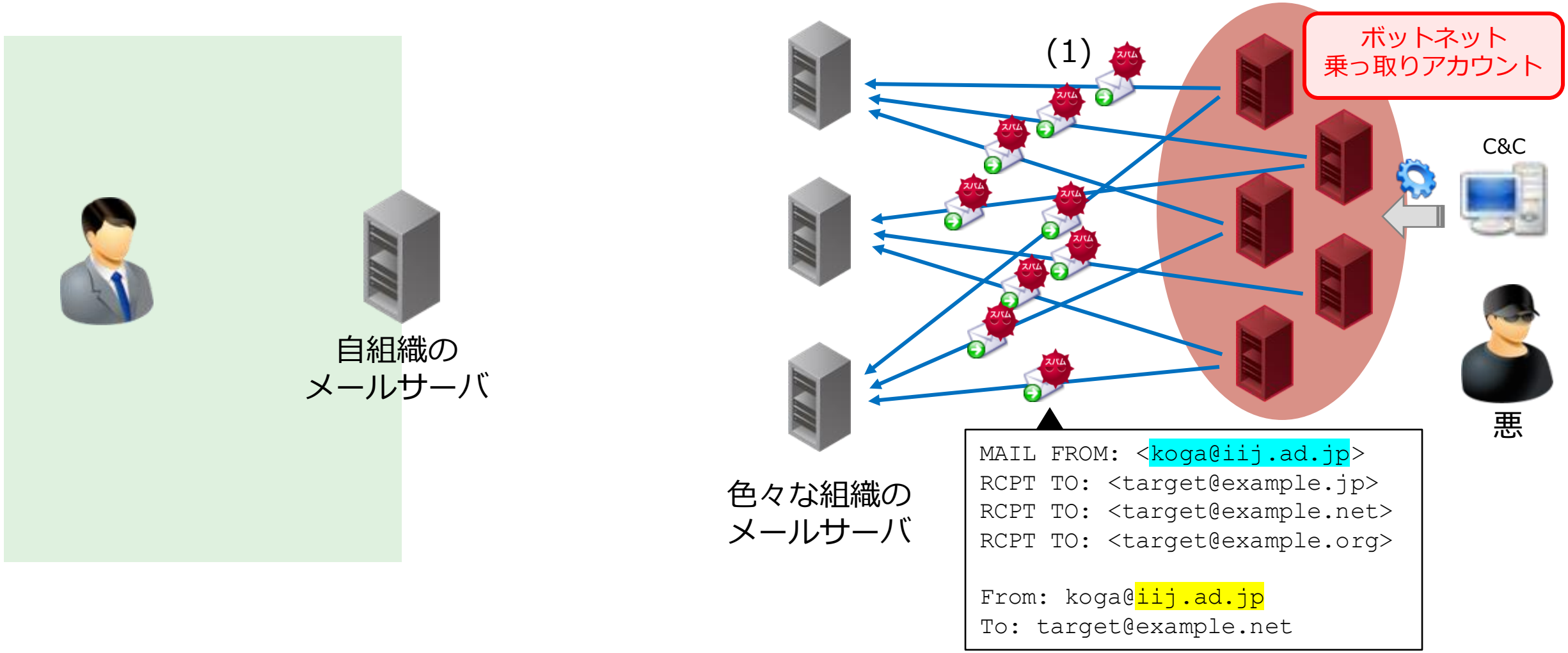
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）



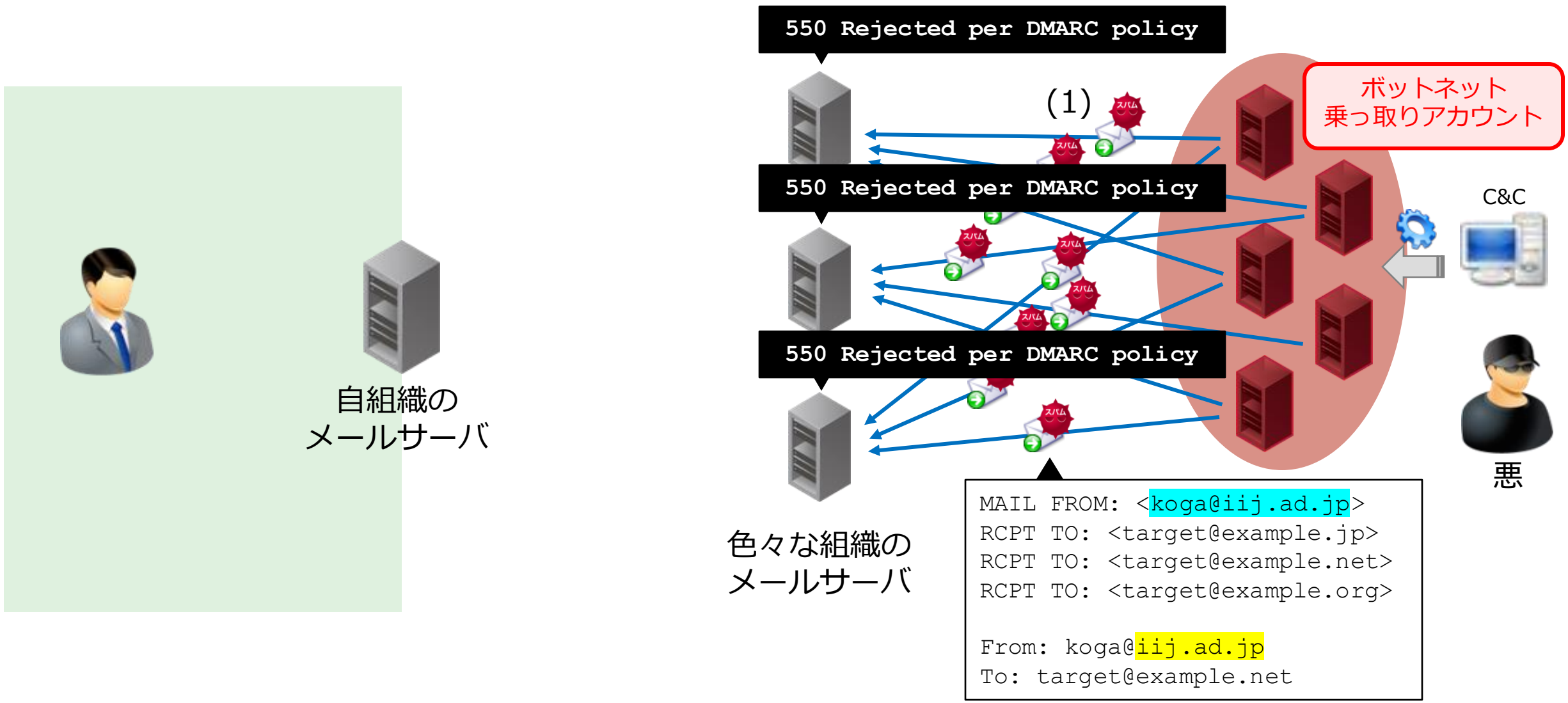
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）



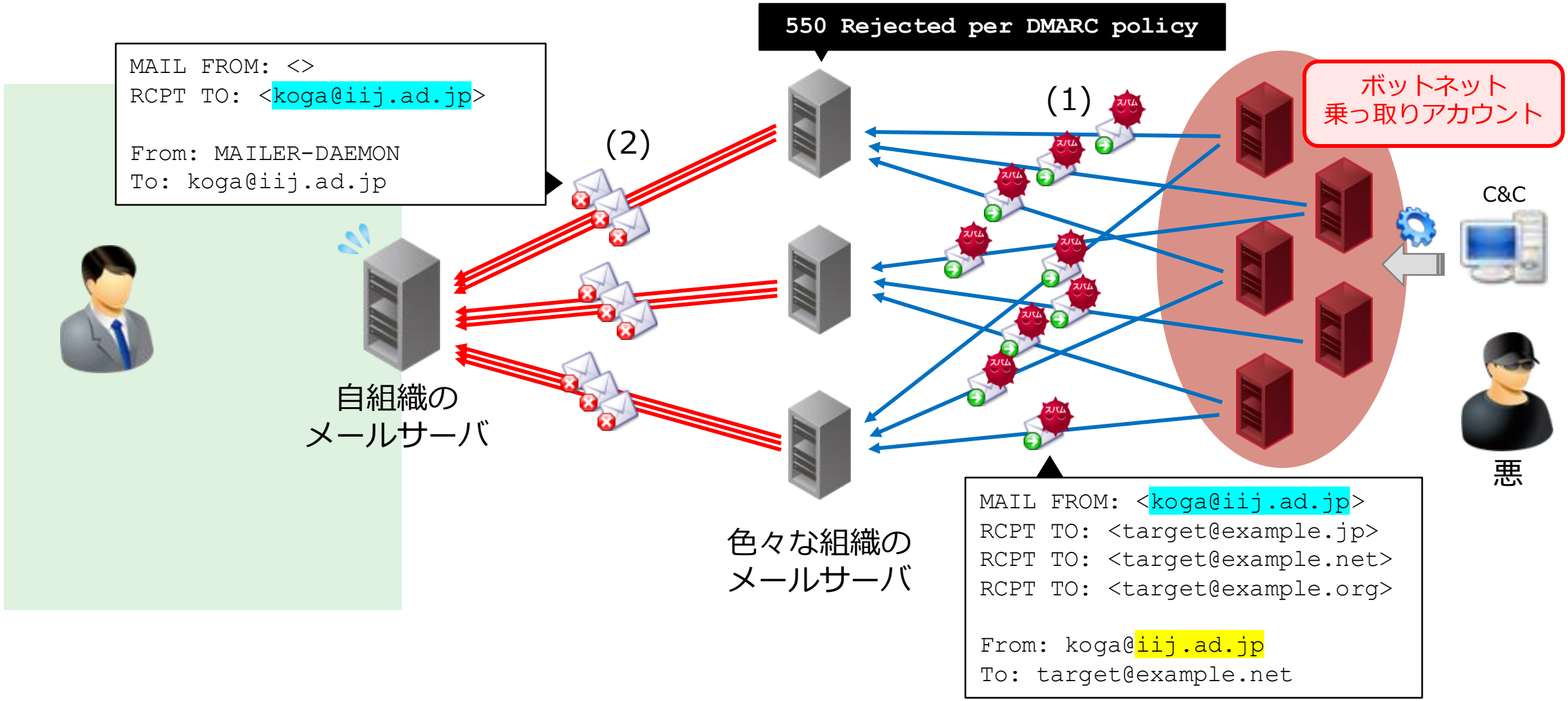
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）



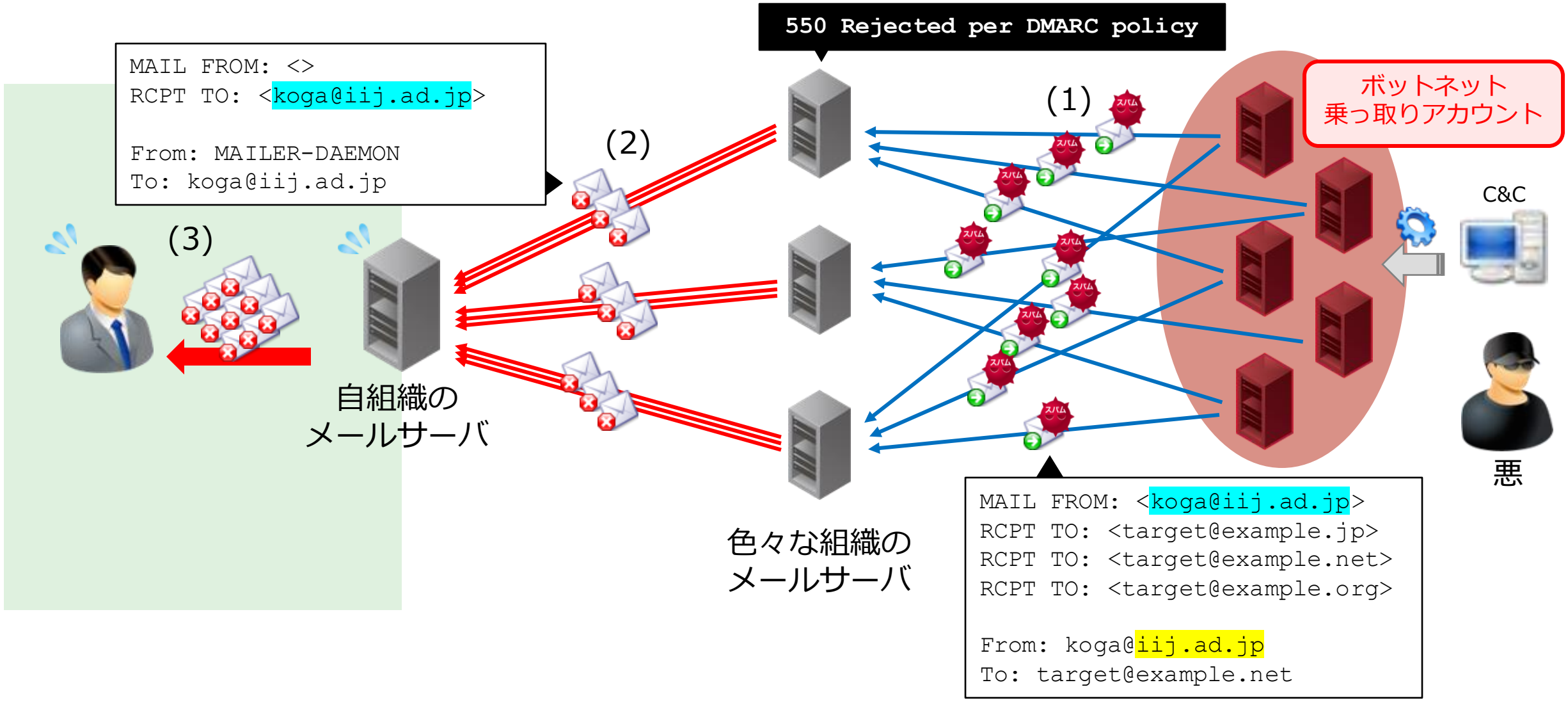
みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）



みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）



みんなが DMARC 対応したあと どういう世界が待っているのか

【Case 3】悪の組織が なりすましメールを送ってエラーになる例（大量）

550 Rejected per DMARC policy

MAIL FROM: <>
RC

ットネット
アカウント

C&C

バックスキャッター問題
Backscatter Issue

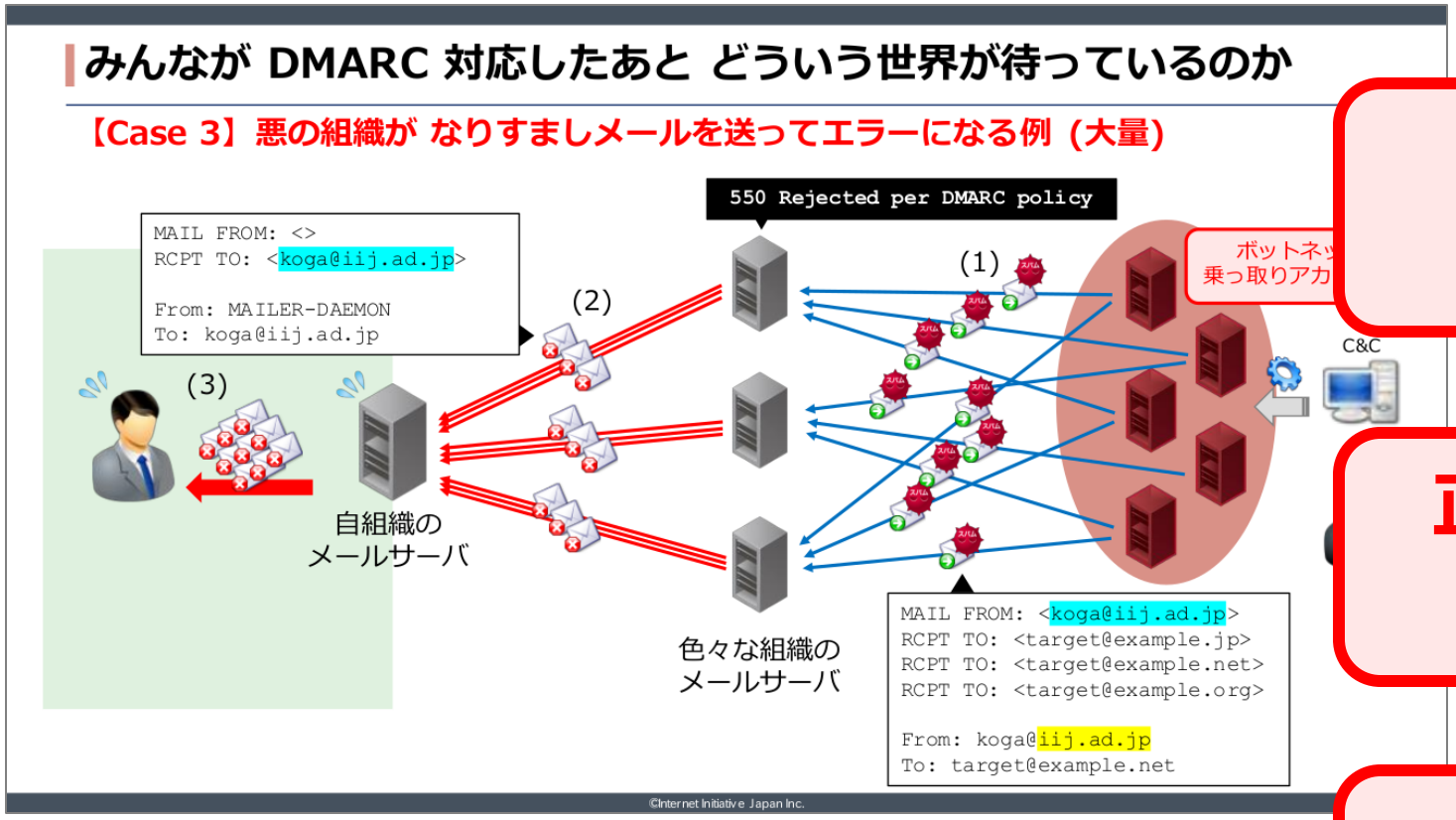
悪

色々な組織の
メールサーバ

```
MAIL FROM: <koga@iij.ad.jp>
RCPT TO: <target@example.jp>
RCPT TO: <target@example.net>
RCPT TO: <target@example.org>

From: koga@iij.ad.jp
To: target@example.net
```

バックスキャッターの問題点



エラー自体は正常な動作

正常なエラーと それ以外の
エラーの区別ができない

エラーメールを送付する
組織も ある意味被害者

実際に観測したバックスキャッター

2023年 9月

IIJ セキュア MX サービスで観測

平時の20～30倍規模

大小複数回続く

当日限定

バックスキャッター対策

バックスキャッター対策(1) - BATV

Bounce Address Tag Validation (https://www.ietf.org/archive/id/draft-levine-smtp-batv-01.html)

1. 利用者はメールを送信
2. 送信サーバは From アドレスにタグを付与
   (エンベロープ From: prvs=KDDDSSSSSS=mailbox@example.jp)
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールの宛先(To)メールアドレスからタグを探す
5. 正しいタグなら**受信**

1. 悪が From を詐称してメールを送信
5. タグがない or タグが不正なら**破棄**

バックスキャッター対策(1) - BATV

Bounce Address Tag Validation (https://www.ietf.org/archive/id/draft-levine-smtp-batv-01.html)

1. 利用者はメールを送信
2. 送信サーバは From アドレスにタグを付与
   (エンベロープ From: prvs=KDDDSSSSSS=mailbox@example.jp)
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールの宛先(To)メールアドレスからタグを探す
5. 正しいタグなら**受信**

1. 悪が From を詐称してメールを送信
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールの宛先(To)メールアドレスからタグを探す
5. タグがない or タグが不正なら**破棄**

✔ **利用者は何もしなくて良い**

✖ **エンベロープ From が謎アドレス**
リプレイアタックに弱い

バックスキャッター対策(2) - 事例 SecureMX

PR

IIJ セキュア MX サービス独自の方法

1. 利用者はメールを送信
2. SecureMX は独自の署名をヘッダに挿入
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールを解析して署名が正当なものか判定
5. 正しい署名なら**受信**

1. 悪が From を詐称してメールを送信
5. 署名がない or 署名が不正なら**破棄**

バックスキャッター対策(2) - 事例 SecureMX

PR

IIJ セキュア MX サービス独自の方法

1. 利用者はメールを送信
2. SecureMX は独自の署名をヘッダに挿入
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールを解析して署名が正当なものか判定
5. 正しい署名なら**受信**

1. 悪が From を詐称してメールを送信
3. 宛先メールサーバでバウンス(エラー)発生
4. 戻ってきたバウンスメールを解析して署名が正当なものか判定
5. 署名がない or 署名が不正なら**破棄**

✔ **利用者は何もしなくて良い**
エンベロープ From 変わらない

✖ **戻ってきたメールが**
解析できないと使えない

バックスキャッター対策(2) - 事例

SecureMX

PR

フィルタの設定に追加するだけ

フィルタの作成

フィルタ情報

フィルタ種別 *

バックスキャッターフィルタ

メモ

0 / 80

動作

配送処理 *

破棄する

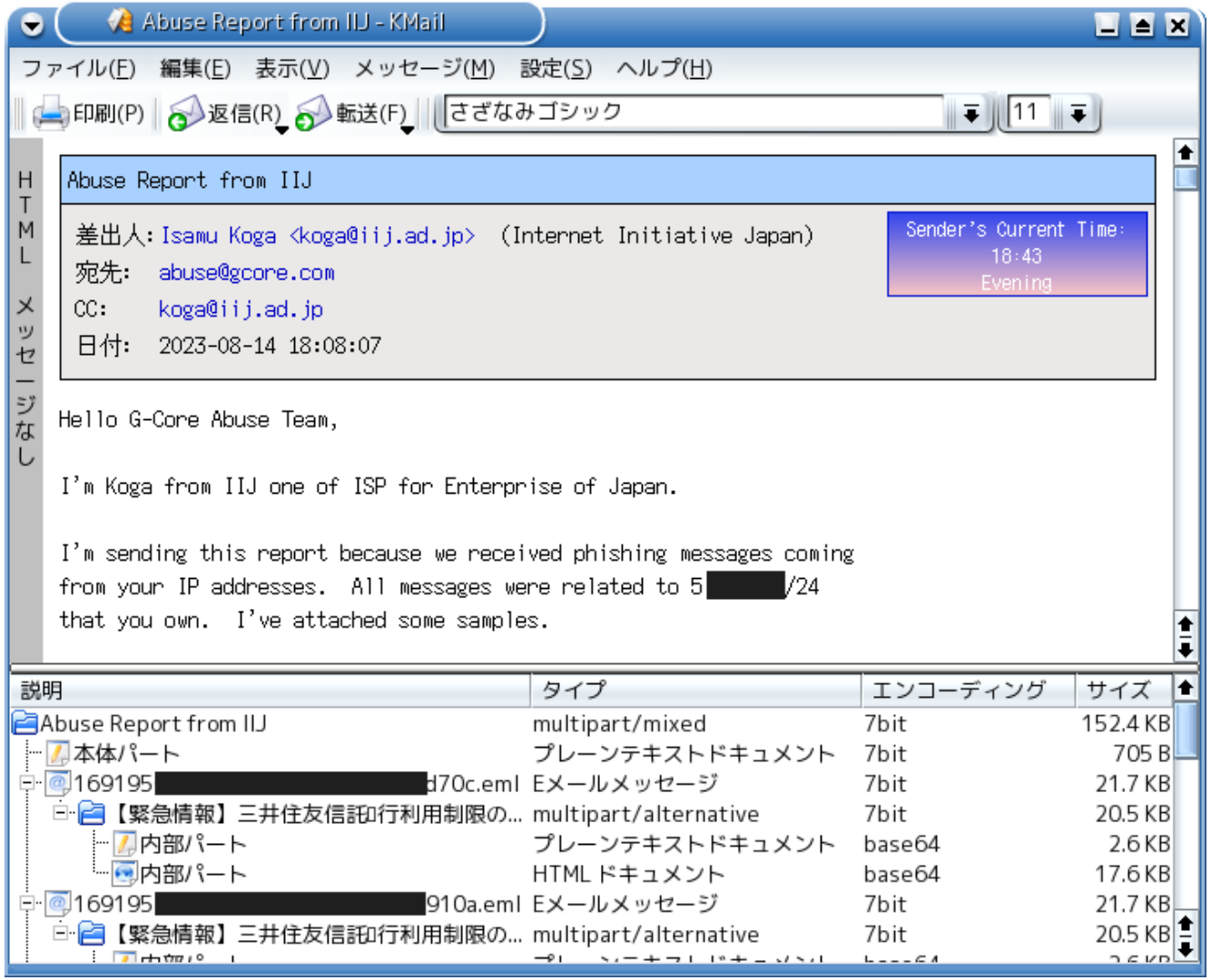
フィルター一覧画面で保存すると、ポリシーに反映されます。

追加

キャンセル

バックスキャッター対策(3) - Abuse する

大量不正契約されていたと思われるホスティング事業者へ連絡してみた

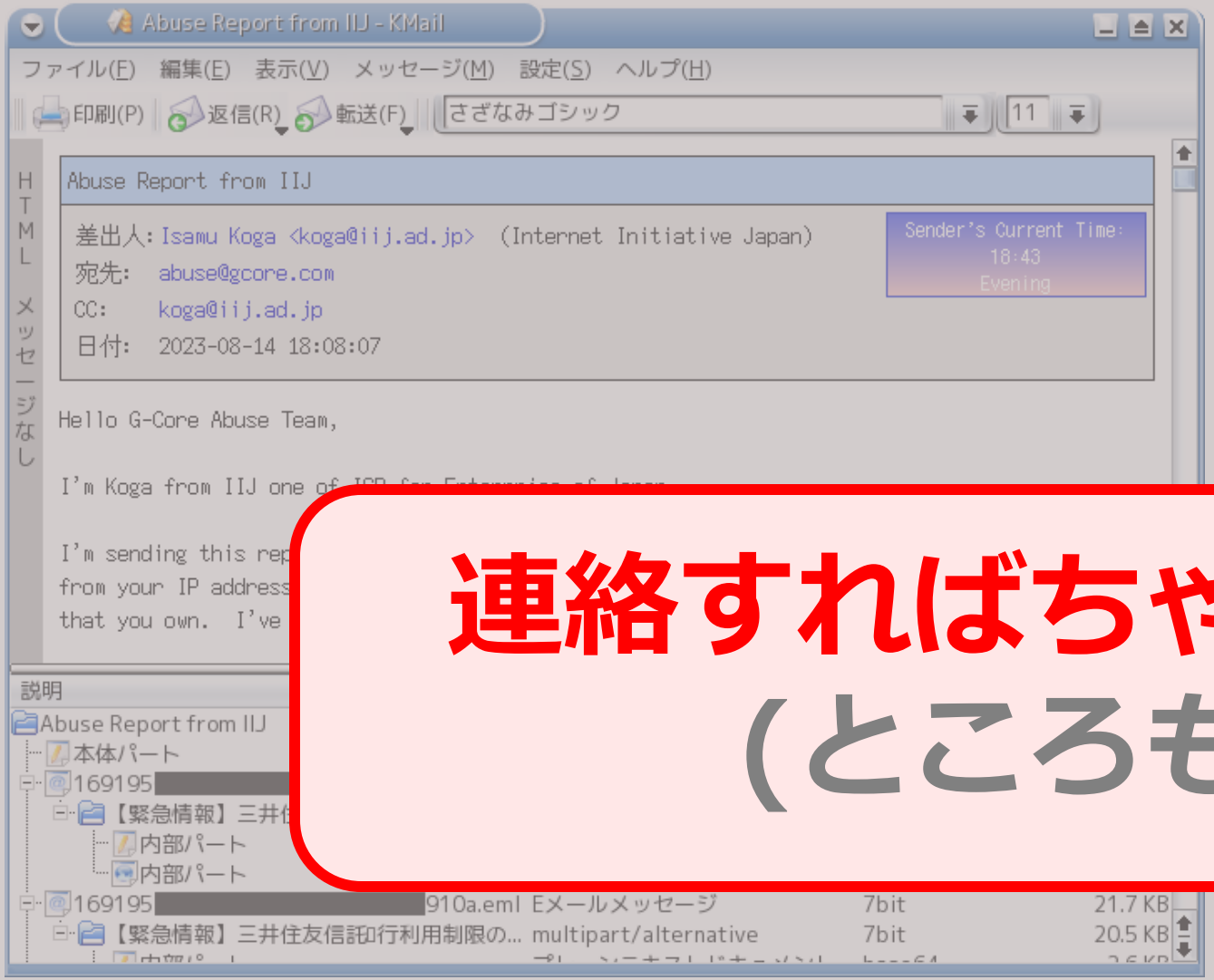


タイムライン

IIJ → Gcore	0分	Abuse 連絡を実施
Gcore → IIJ	24分	確認中とお返事
IIJ	52分	VPS の活動停止を確認
Gcore → IIJ	54分	対策が完了したとお返事
IIJ → Gcore	1時間25分	追加の対策を依頼
Gcore → IIJ	1時間55分	侵害を確認、対策中とお返事
IIJ → Gcore	1時間58分	VPS の一部活動停止を確認
Gcore → IIJ	5時間04分	対象 VPS を停止したとお返事

バックスキャッター対策(3) - Abuse する

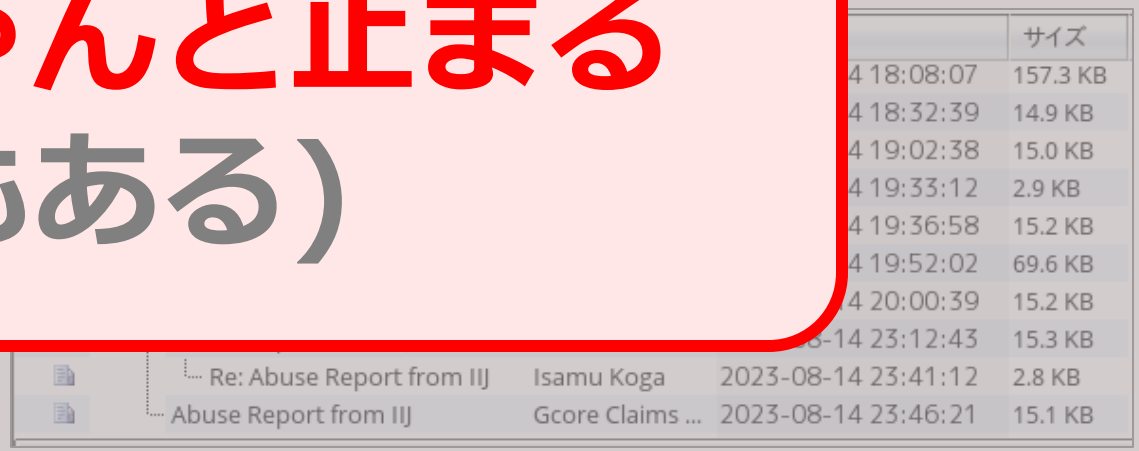
大量不正契約されていたと思われるホスティング事業者へ連絡してみた



タイムライン

IIJ → Gcore	0分	Abuse 連絡を実施
Gcore → IIJ	24分	確認中とお返事
IIJ	52分	VPS の活動停止を確認
Gcore → IIJ	54分	対策が完了したとお返事
IIJ → Gcore	1時間25分	追加の対策を依頼
Gcore → IIJ	1時間55分	侵害を確認、対策中とお返事
IIJ → Gcore	1時間58分	VPS の一部活動停止を確認
		停止したとお返事

連絡すればちゃんと止まる
（ところもある）

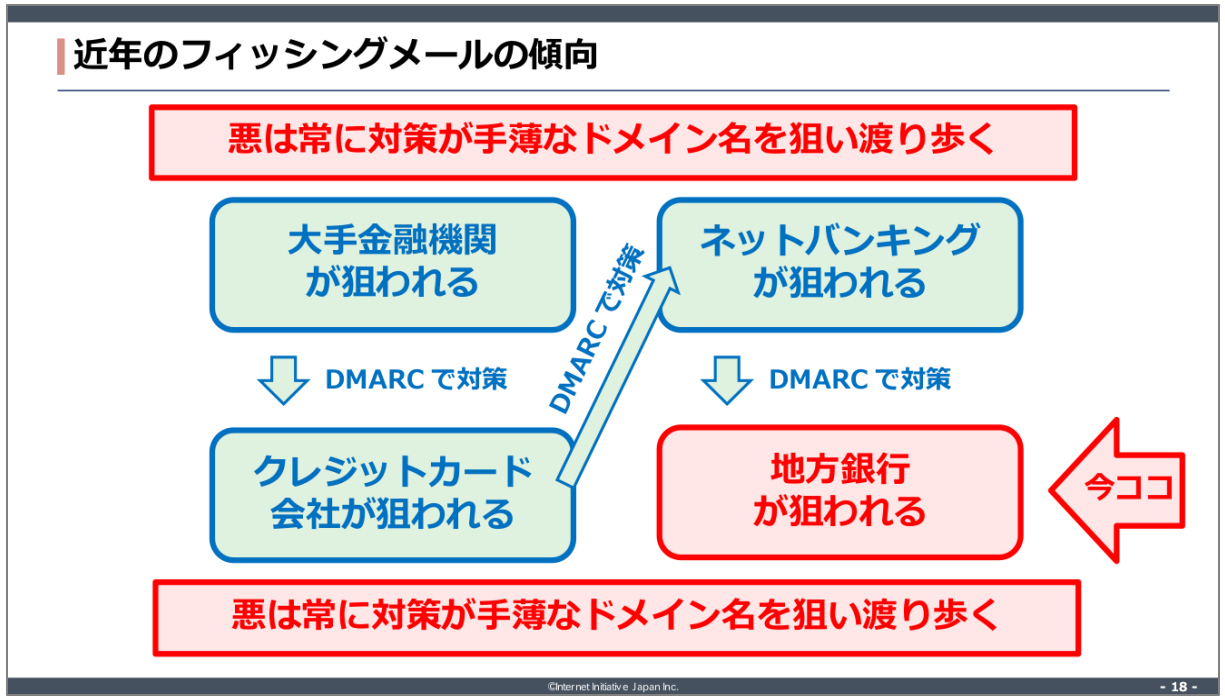


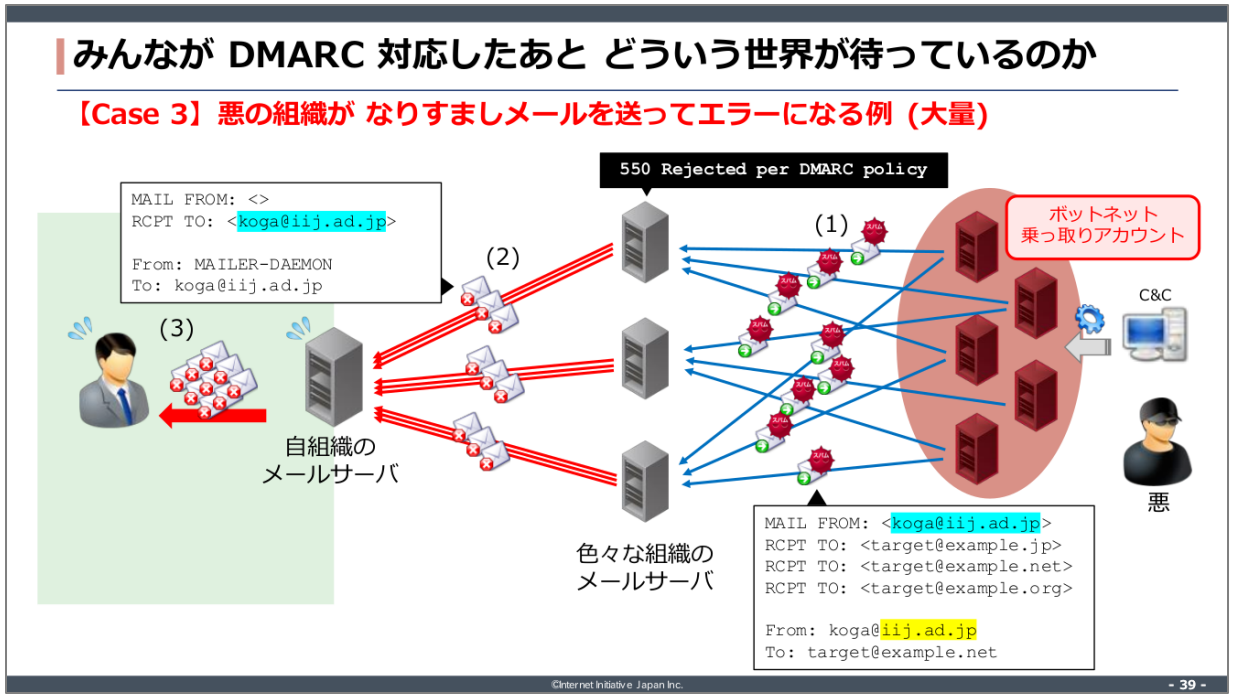
まとめ

悪の組織に狙われる前に今すぐ対策を、できるところから。

**DMARC p=reject
みんなでやりましょう**

**バックスキャッター
に備えましょう**





まとめ

悪の組織に狙われる前に今すぐ対策を、できるところから。

**DMARC p=reject
みんなでやりましょう**

**バックスキャッター
に備えましょう**

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。

Ongoing Innovation