



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
WIDE Project

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP
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



©Internet Initiative Japan Inc.

- 1 -

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

パスワード付きzipファイルが添付されたメールおよび別送のパスワード記載メール (PPAP) に対する当社運用の変更について

メールにファイルを送付して送達する際、「パスワード付きzipファイル」と、そのパスワードを別送する」という手順で行われていた暗号化セキュリティ対策手法、いわゆる「PPAP」につきまして、当社は2022年1月26日より、社外の方からのメールアドレスへのメール送達における対応を、廃止して以下のように変更いたします。

2022年1月25日以前	従来通り、パスワード付きzipファイルが添付されたメールを送信する
2022年1月26日以降	パスワード付きzipファイルをフォルダにより削除し、メール本文のみを送信する

また、IIJより社外の方へパスワード付きzipファイルを送付する機会においても、今後順次対応の手段へ変更いたします。

上記の変更ととも、ファイルを送付するための別の手段を用意し、移行いたします。その利用につきましては、お客様、お取引先様、個別にご連絡申し上げます。

変更に至った背景

メールにパスワード付きzipファイルを送付して送達し、そのパスワードを別送する「PPAP」は、日本において多く見られる暗号化セキュリティ対策の一つですが、効果が薄く、脆弱性を指摘されることが多いため、全面的に廃止することから、全面的なサイバーセキュリティ・インフラセキュリティ強化においてもプロダクトとして廃止されています。

この取り組みを意図したマルウェアは今後も発生することが予想されることから、当社だけでなく、お客様、お取引先様よりお聞きいただくための、対応が必要との考えに至りました。

当社のお客様、お取引先様におかれましては、弊社、ご理解・ご協力のごと、よろしくお願ひ申し上げます。

<https://www.ij.ad.jp/ppap/>

パスワード付き (暗号化) ZIP 廃止の考え方と対策

2022年1月26日 月曜日

【この記事を書いた人】
田原 貴

パスワード付きzipファイルを送付する際、「パスワード付きzipファイル」と、そのパスワードを別送する」という手順で行われていた暗号化セキュリティ対策手法、いわゆる「PPAP」につきまして、当社は2022年1月26日より、社外の方からのメールアドレスへのメール送達における対応を、廃止して以下のように変更いたします。

パスワード付き ZIP 問題

CONTENTS

1. 暗号化されたZIPファイルを送付する目的
2. 暗号化されたZIPファイルを送付する際の注意点
3. どのような場合にパスワード付きZIPを送付すべきか
4. 国内の運用状況
5. IIJがおすすめする代替手段

<https://eng-blog.ij.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説明

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でのリスク評価

各部門への説明とスケジュールの展開

お客様・取引先への説明

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

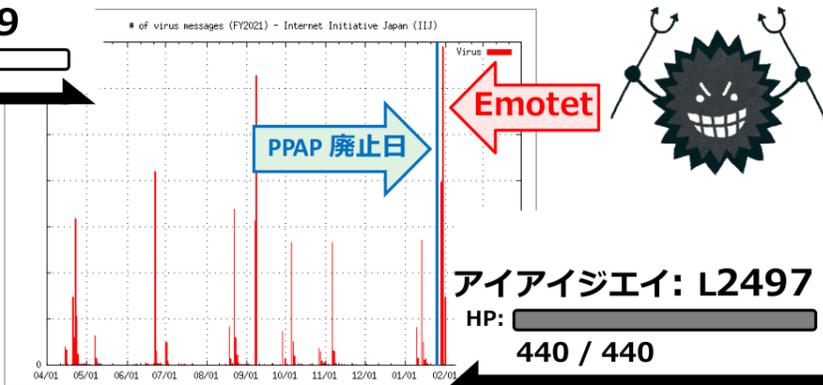


「現場発！メールサービスを支える運用者の集い 2022 秋」より

(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:



こうかは ばつぐんだ！

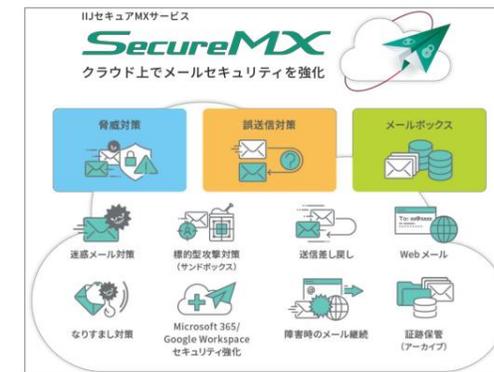
©Internet Initiative Japan Inc.

PPAP 廃止で
Emotet 一網打尽

(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定した。

©Internet Initiative Japan Inc.

- 10 -

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

©Internet Initiative Japan Inc.

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

©Internet Initiative Japan Inc.

- 15 -

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

©Internet Initiative Japan Inc.

- 1 -

DMARC で
IIJ ブランドを保護

PPAP 廃止で
Emotet 一網打尽

まとめ

「悪」の手に掛かる前に対策しましょう

(1) PPAP
みんなでやめましょう

(2) DMARC p=reject
みんなでやりましょう

IIJ IIR

検索

詳細は IIR vol.55 へ!



©Internet Initiative Japan Inc.

- 17 -

近年のフィッシングメール傾向

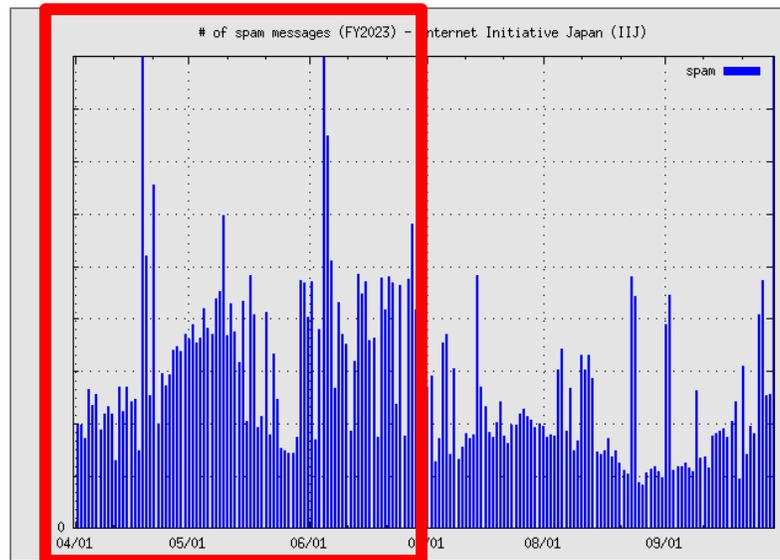


2023年度 フィッシングメール・ウイルスメールの傾向

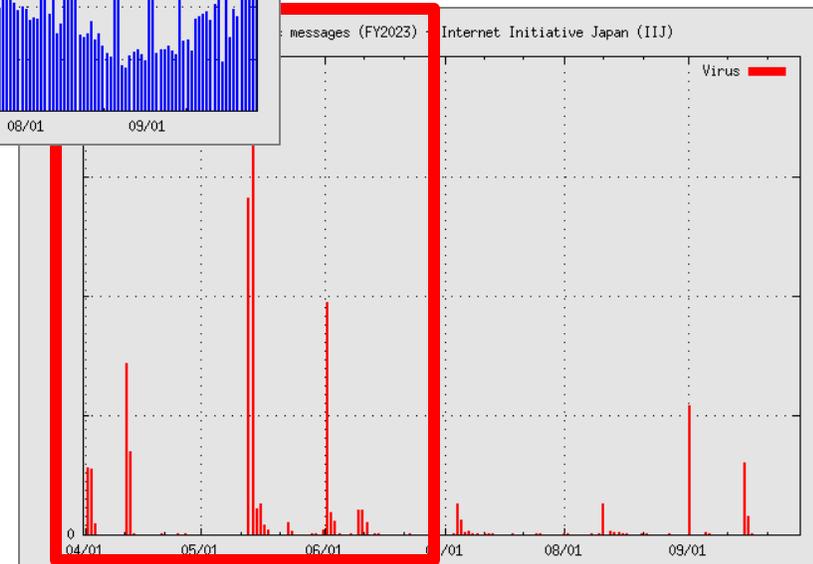
時折スパイクする傾向が見られる



▲ 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...

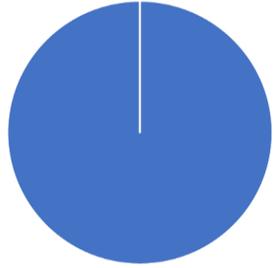


何度も聞いてない...?

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



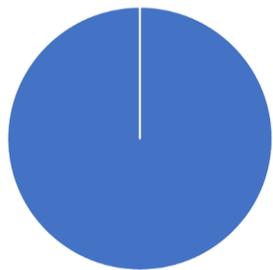
DMARC 対応率
100%

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%

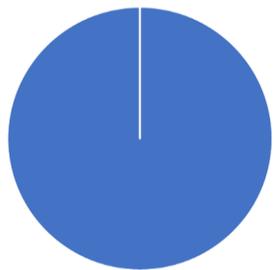
大手金融機関
が狙われる



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



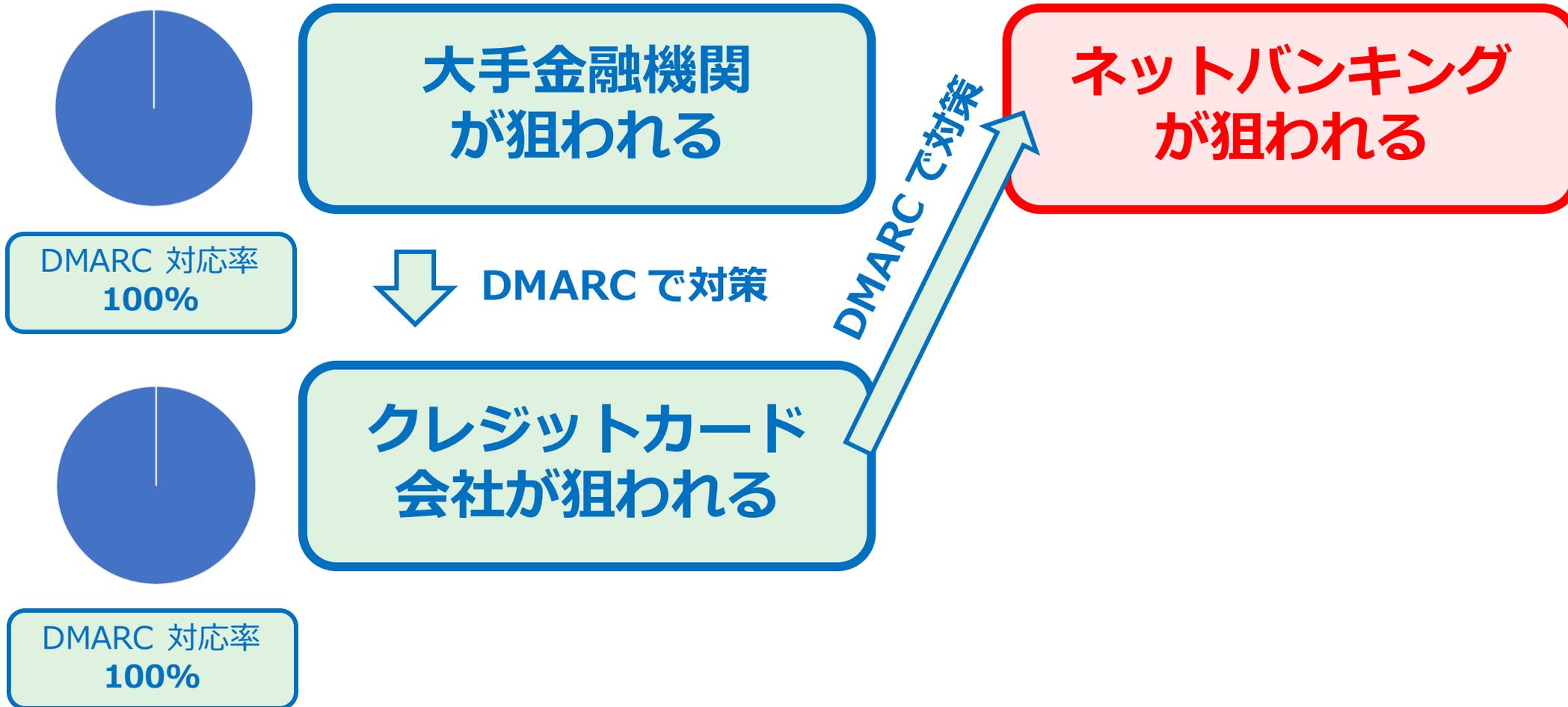
DMARC 対応率
100%

クレジットカード
会社が狙われる

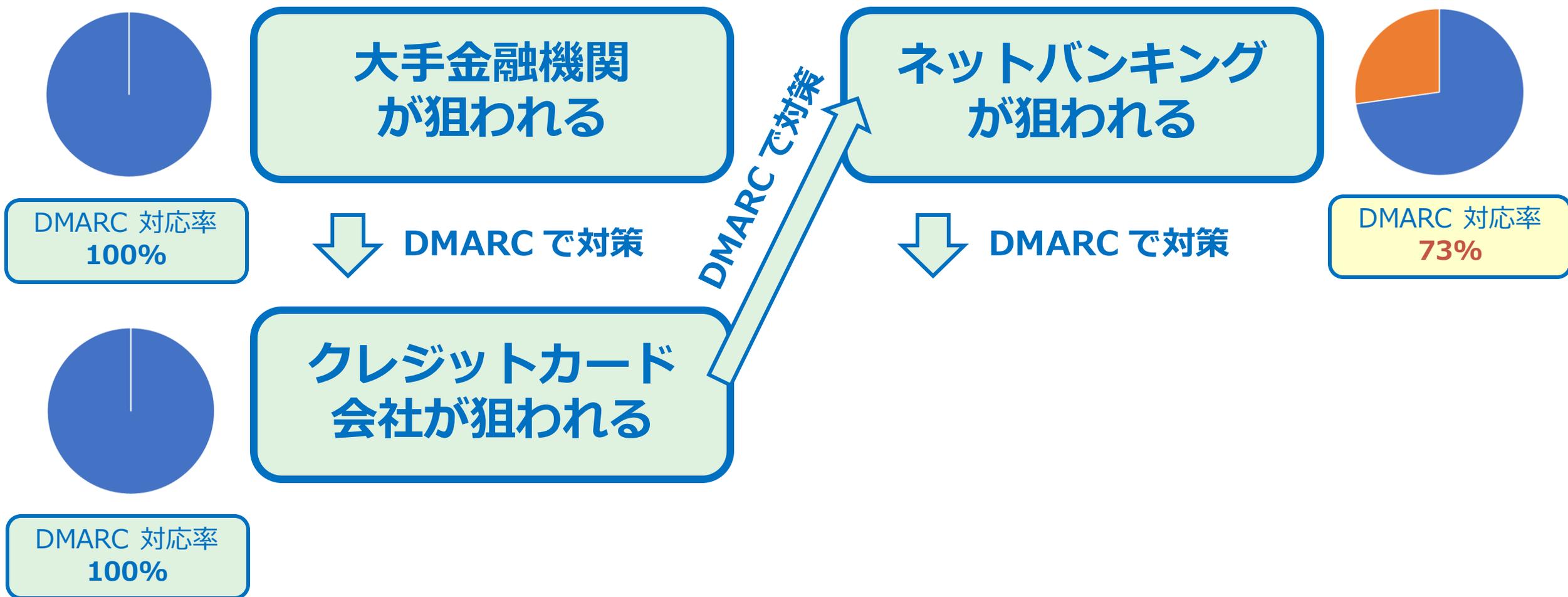


DMARC で対策

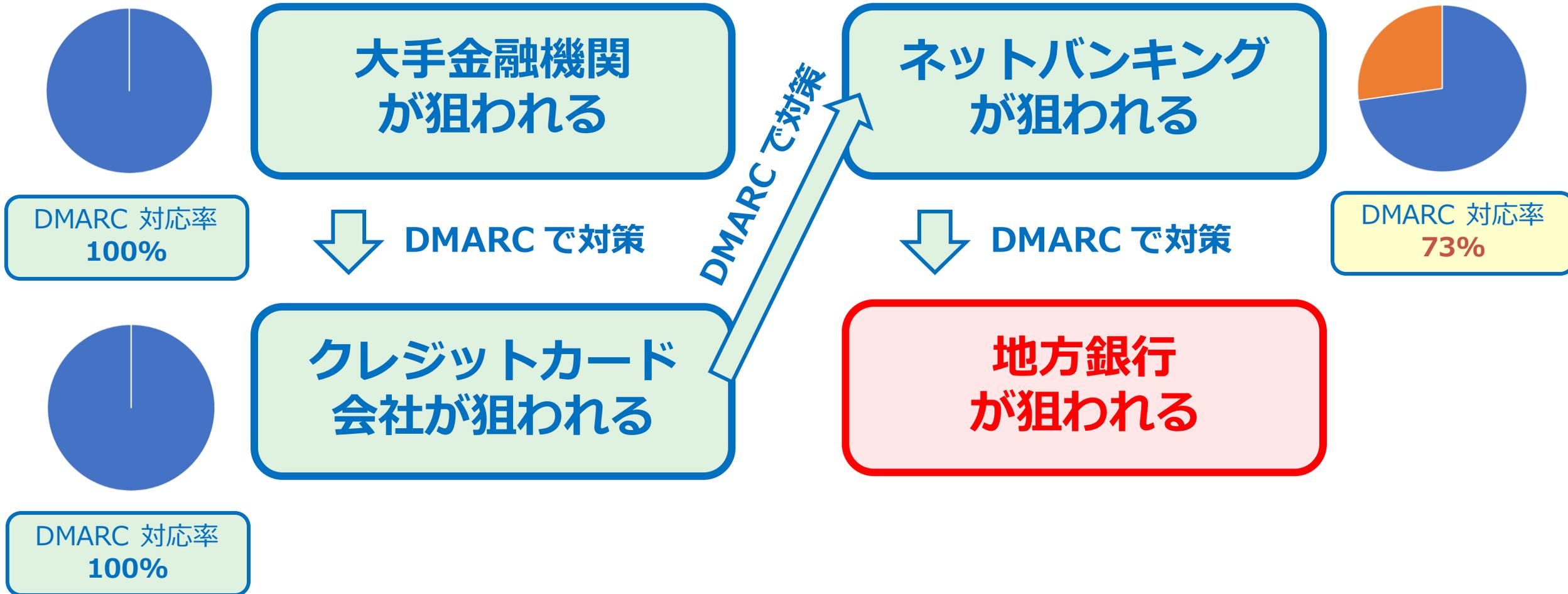
近年のフィッシングメールの傾向



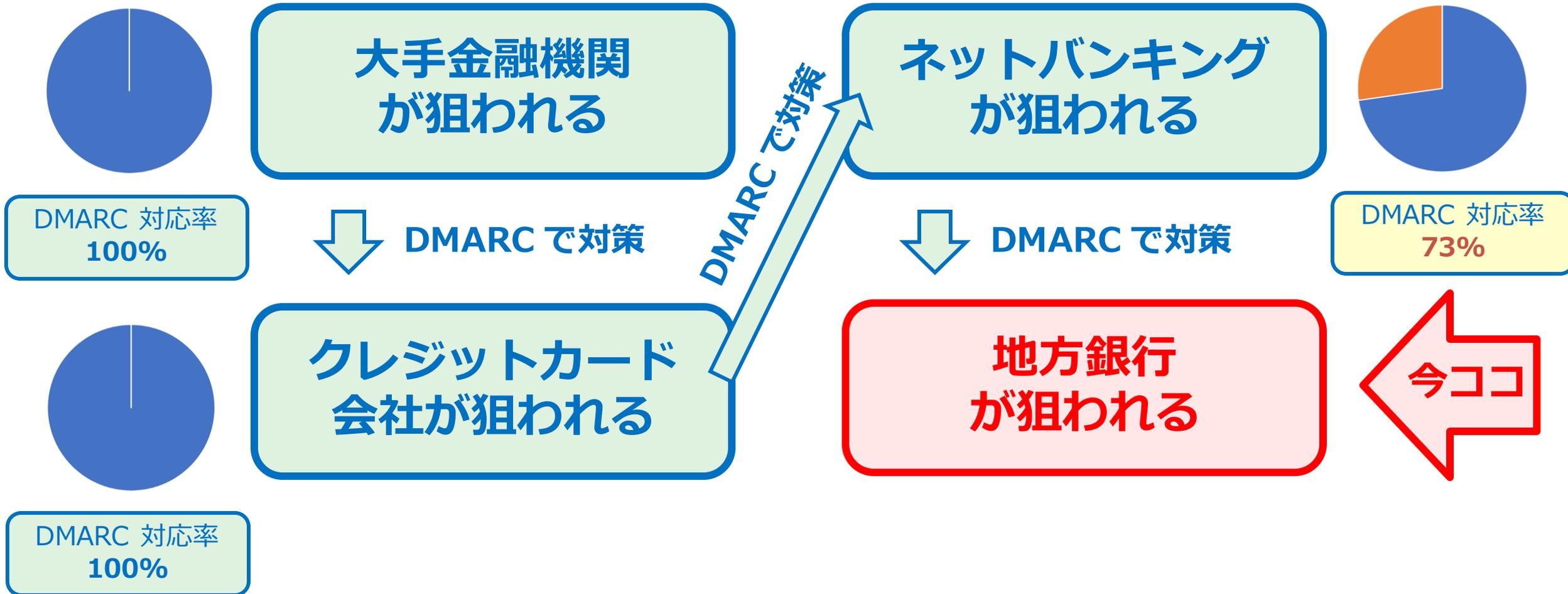
近年のフィッシングメールの傾向



近年のフィッシングメールの傾向



近年のフィッシングメールの傾向



(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

悪は常に対策が手薄なドメイン名を狙い渡り歩く

大手金融機関
が狙われる

↓ DMARC 対策

クレジットカード
会社が狙われる

ネットバンキング
が狙われる

↓ DMARC 対策

地方銀行
が狙われる

DMARC 対策

今ココ

悪は常に対策が手薄なドメイン名を狙い渡り歩く



今日の本題

みんなが DMARC 対応したあと
どういふ世界が待っているのか



Case 1

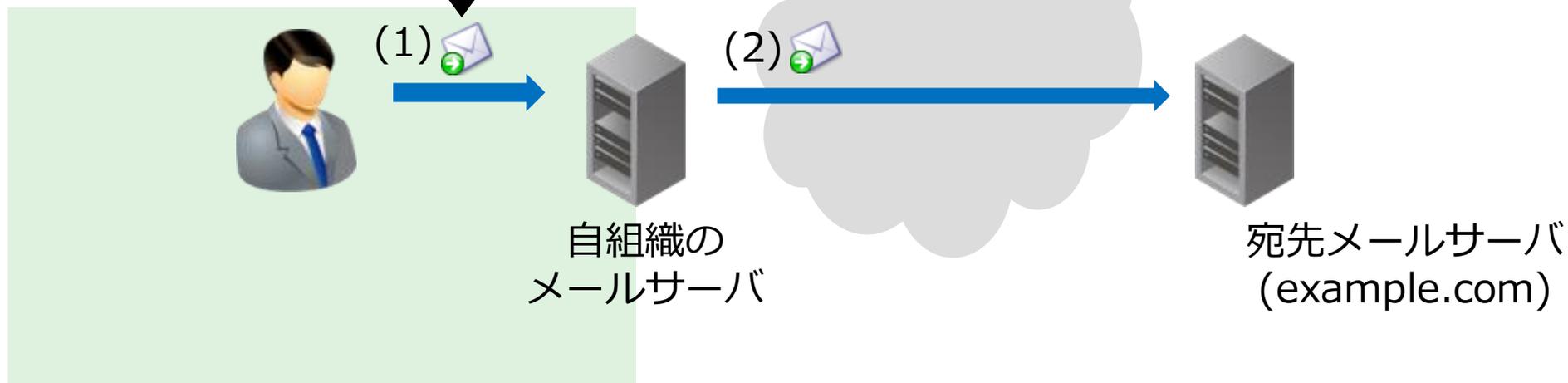
通常の送信エラーの例 (宛先不明など)



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】 通常を送信エラーの例 (宛先不明など)

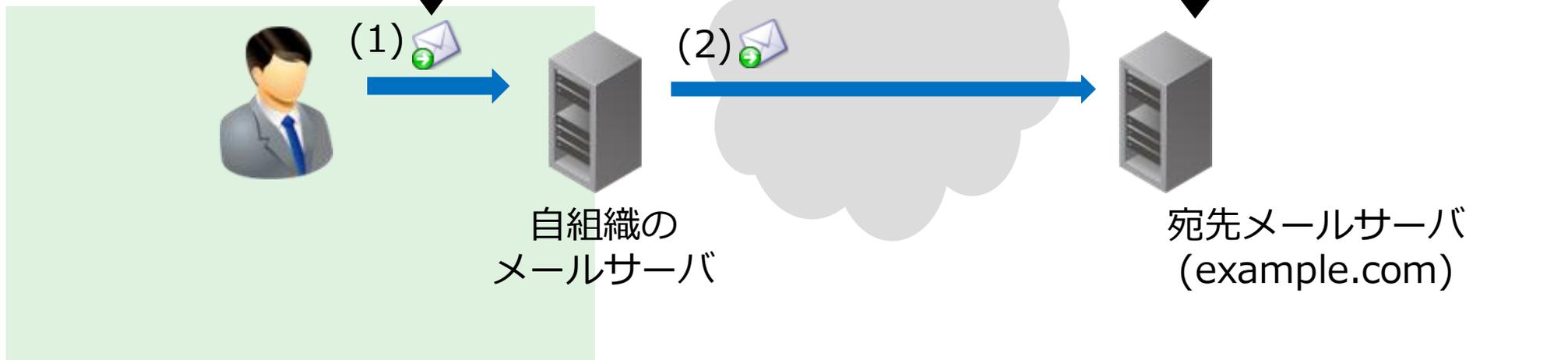
```
MAIL FROM: <koga@iij.ad.jp>  
RCPT TO: <user-unknown@example.com>  
  
From: koga@iij.ad.jp  
To: user-unknown@example.com
```



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

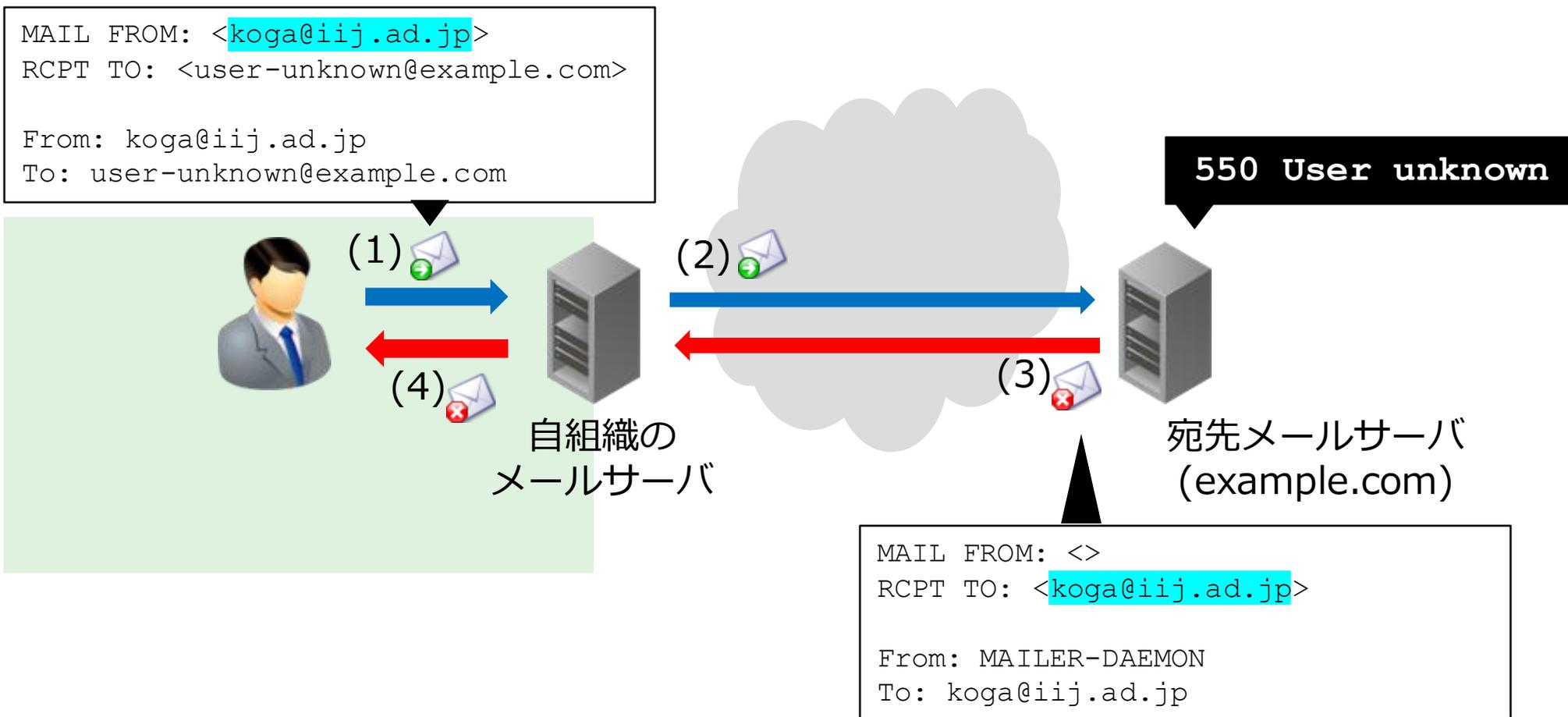
【Case 1】 通常を送信エラーの例 (宛先不明など)

```
MAIL FROM: <koga@iij.ad.jp>  
RCPT TO: <user-unknown@example.com>  
  
From: koga@iij.ad.jp  
To: user-unknown@example.com
```



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】 通常を送信エラーの例 (宛先不明など)





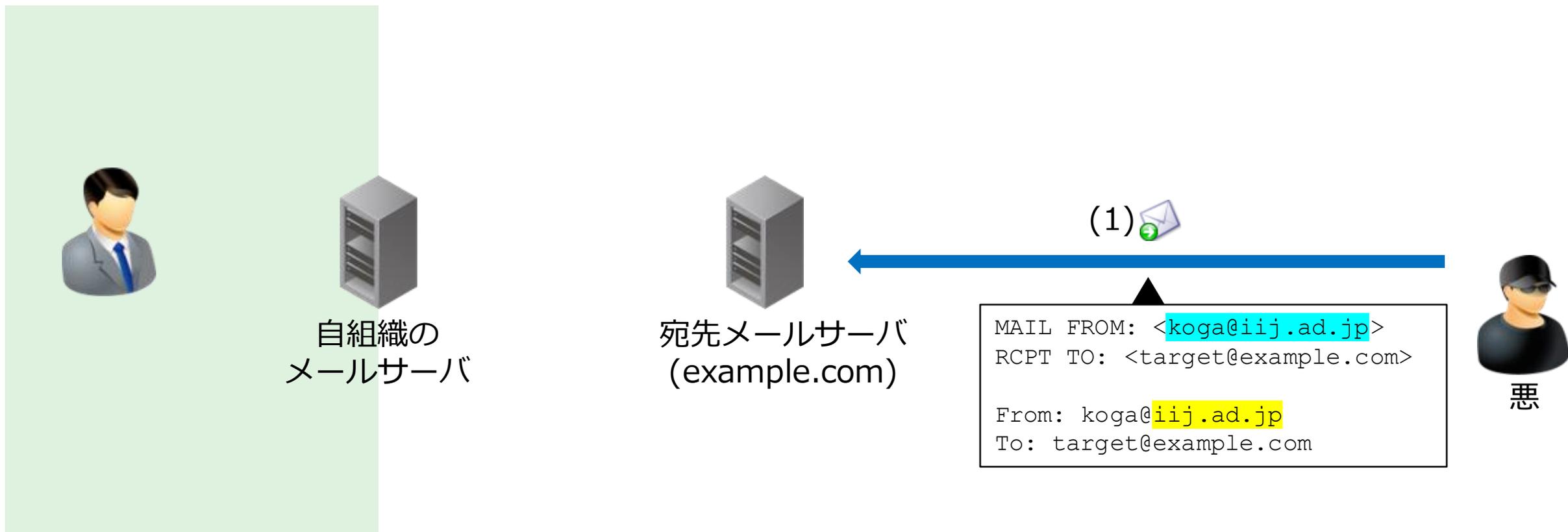
Case 2

**悪の組織が なりすましメールを送って
エラーになる例**



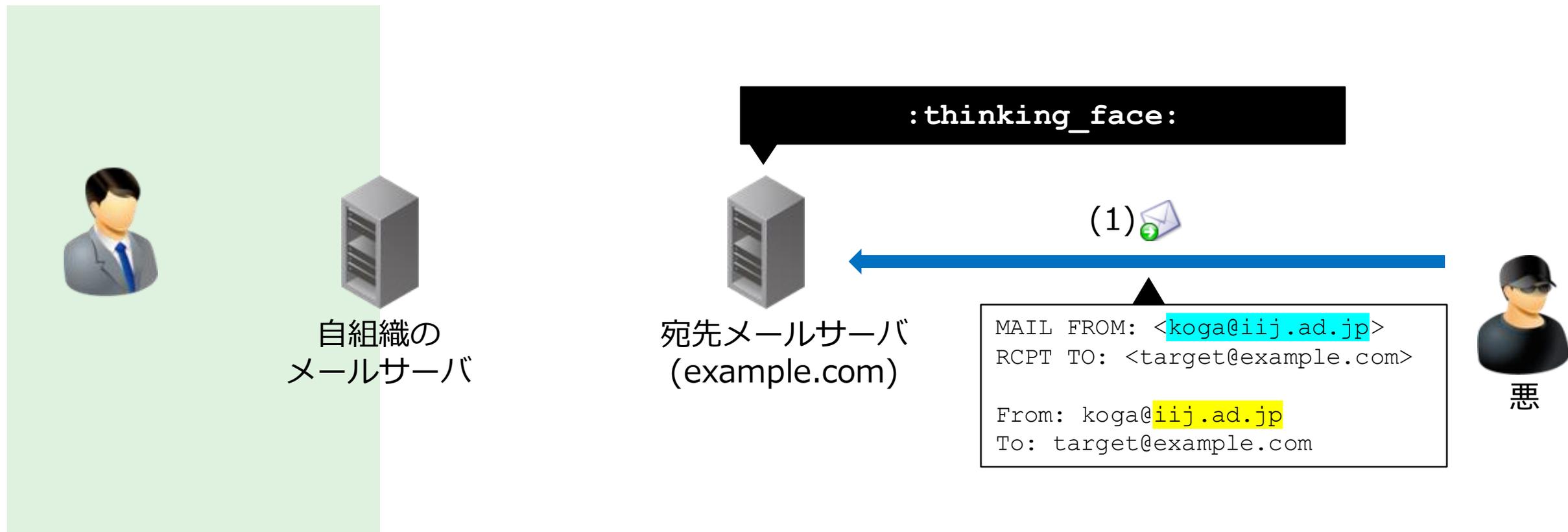
みんなが DMARC 対応したあと どういう世界が待っているのか

【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



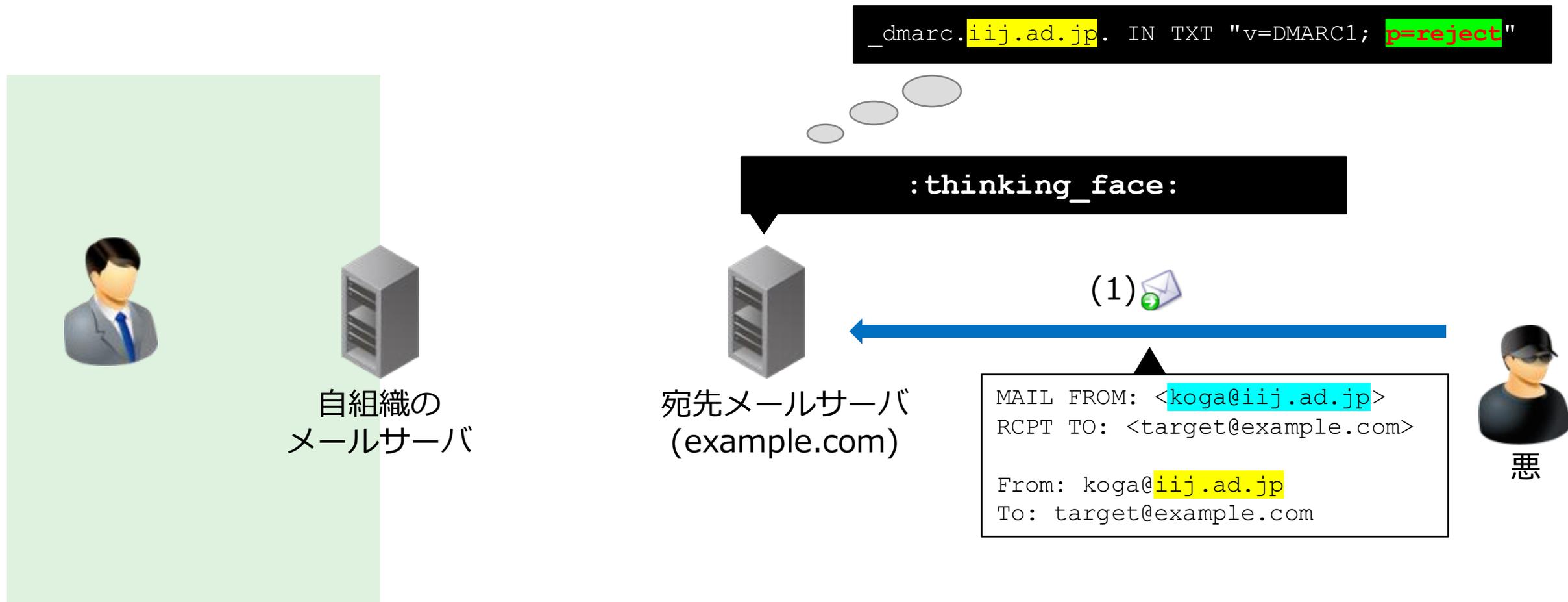
みんなが DMARC 対応したあと どういう世界が待っているのか

【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



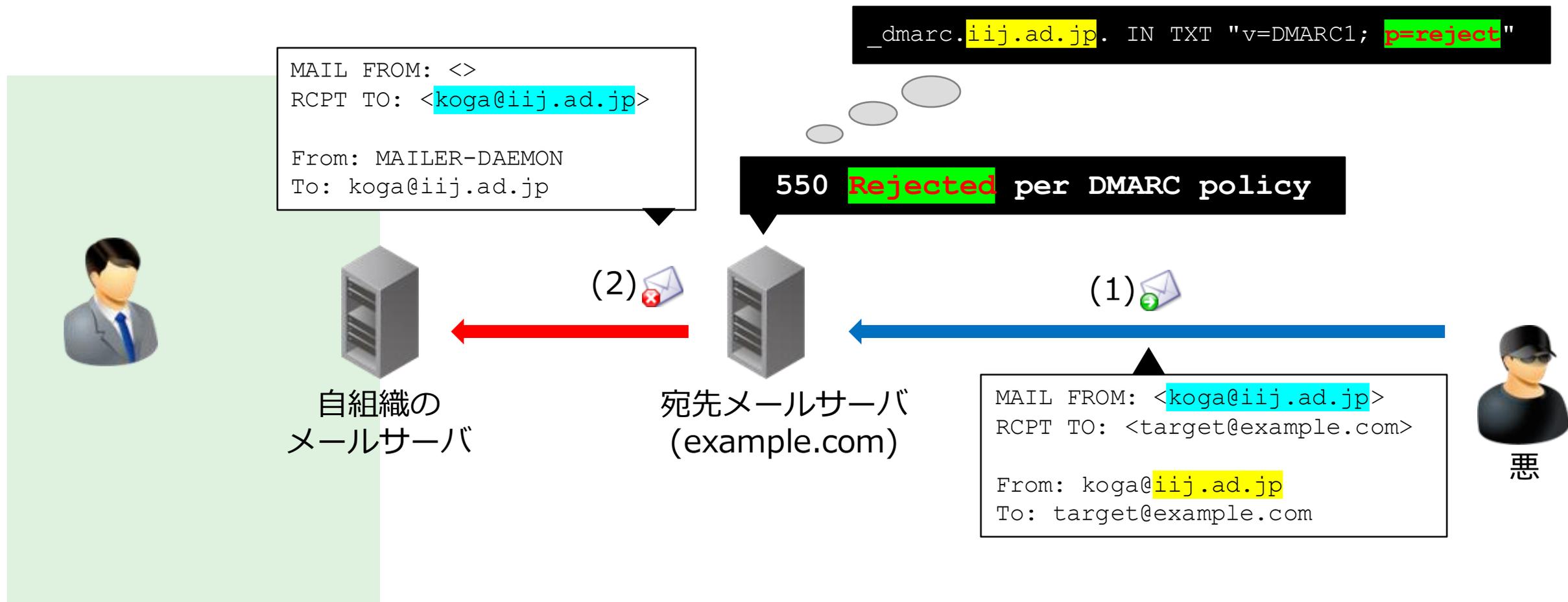
みんなが DMARC 対応したあと どういう世界が待っているのか

【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



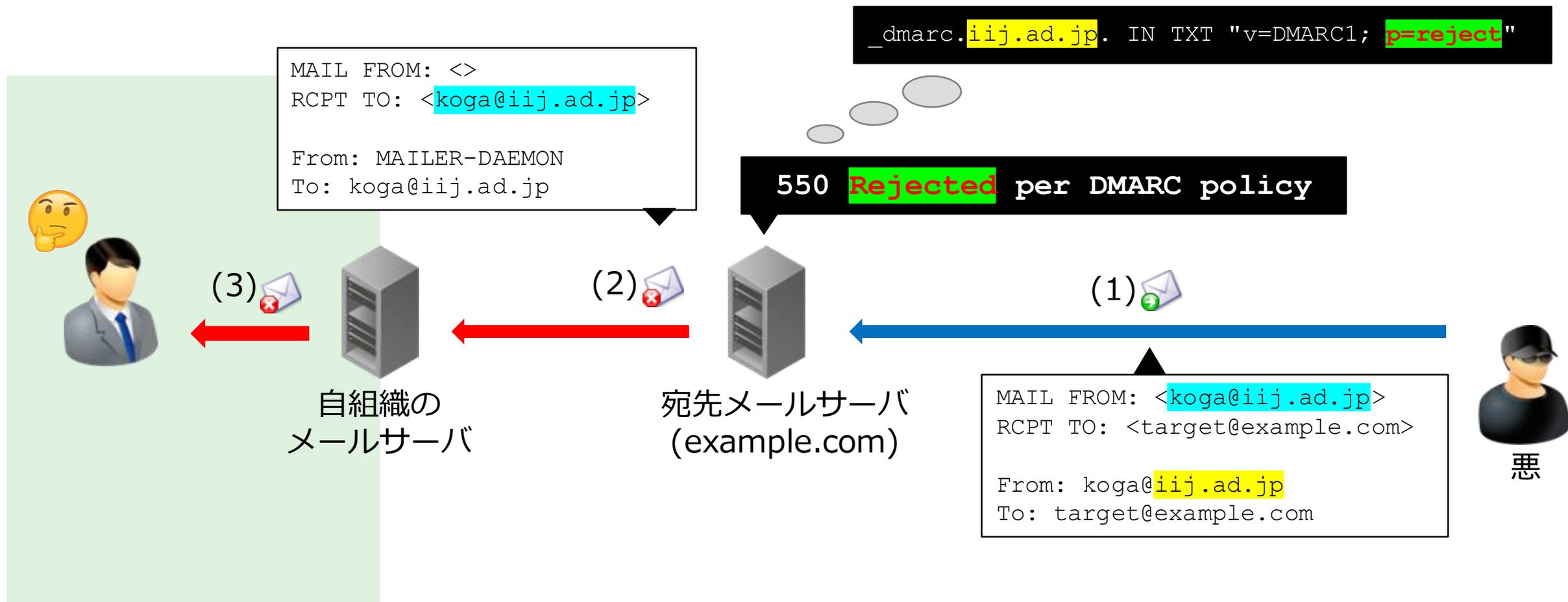
みんなが DMARC 対応したあと どういう世界が待っているのか

【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



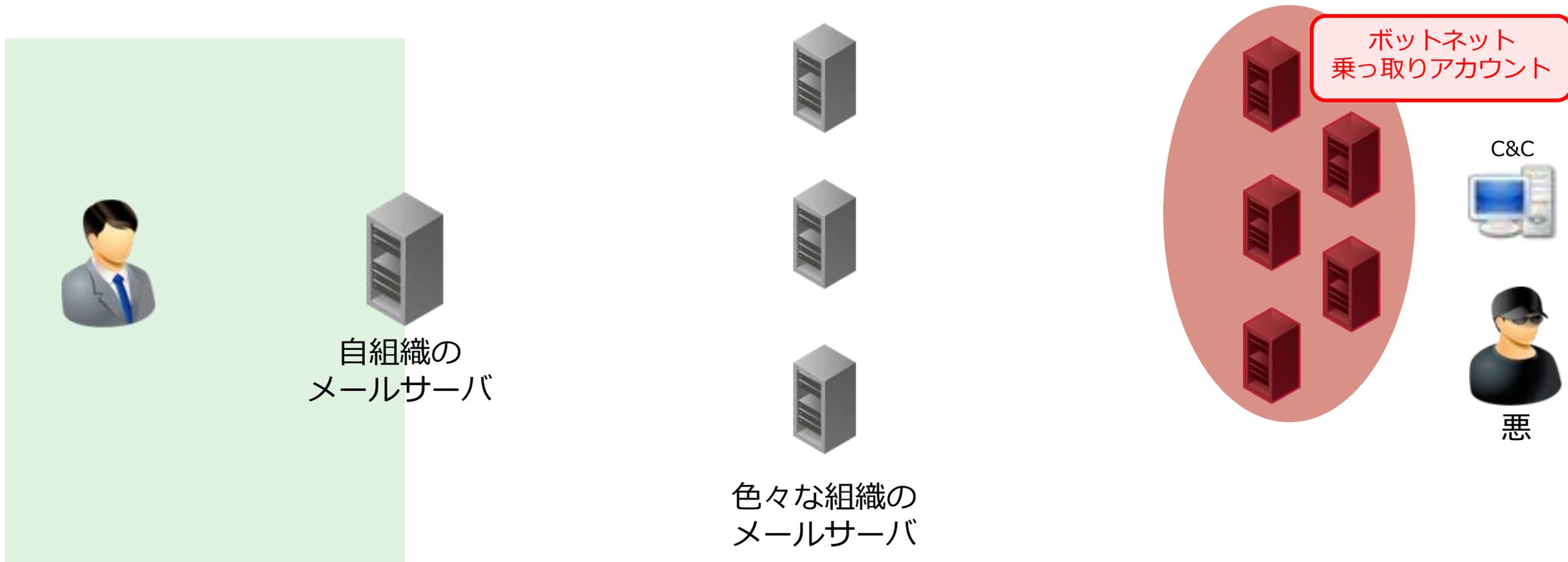
Case 3

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)



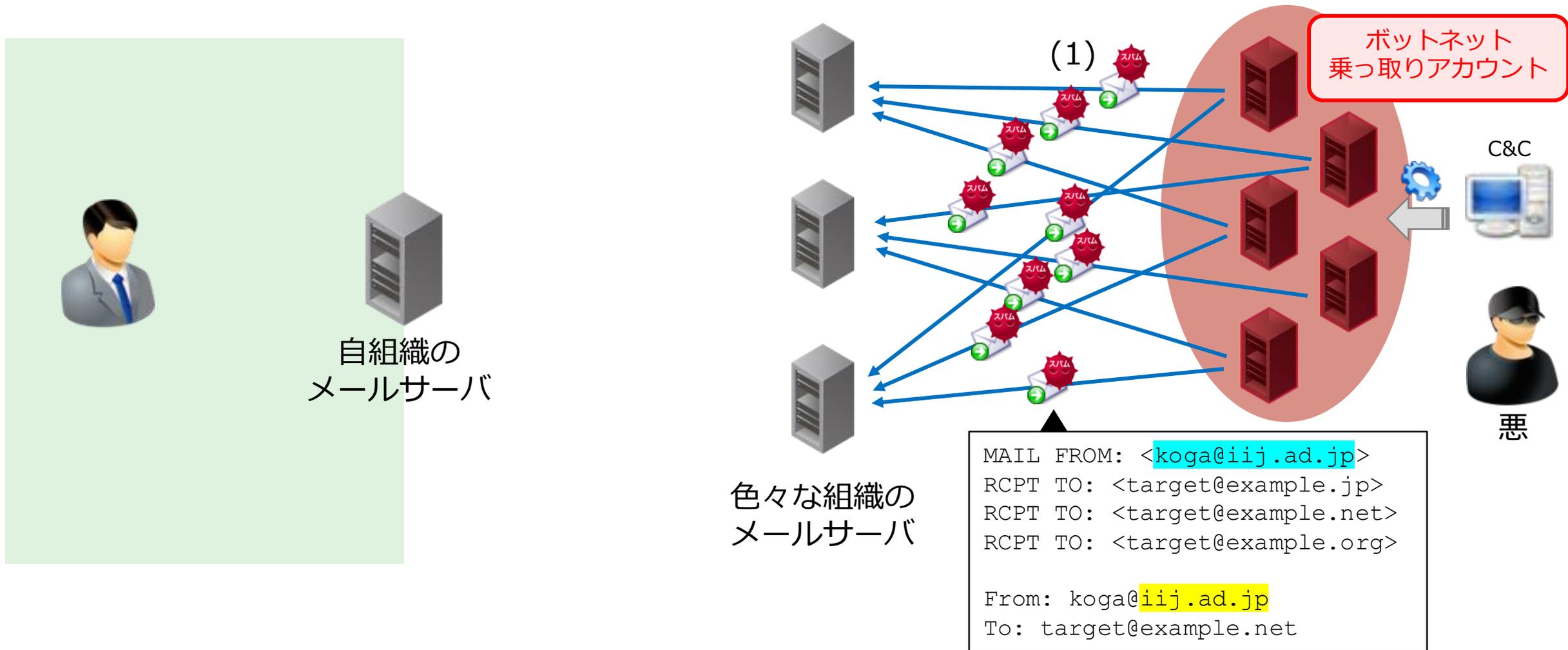
みんなが DMARC 対応したあと どういう世界が待っているのか

【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)



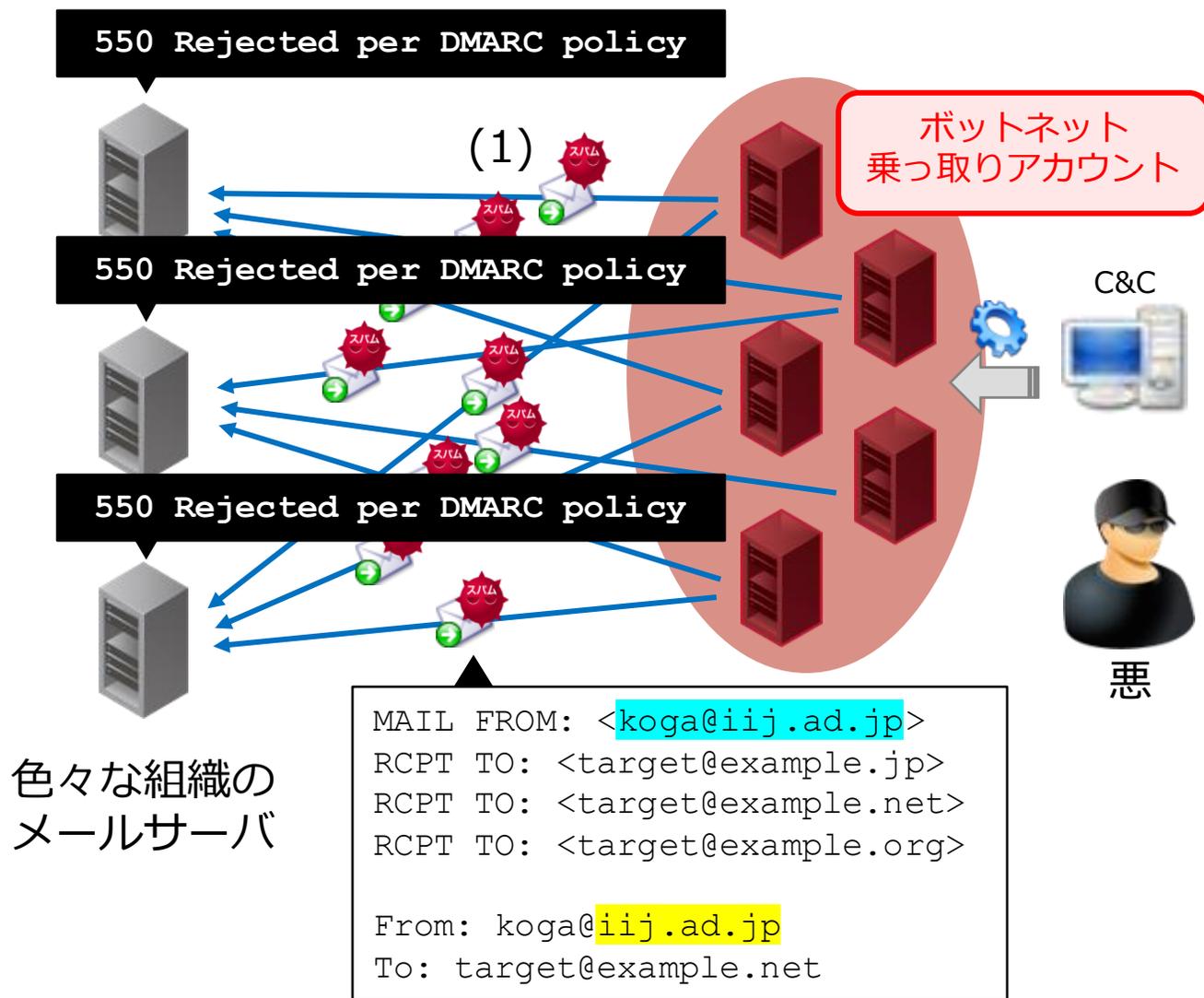
みんなが DMARC 対応したあと どういう世界が待っているのか

【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)



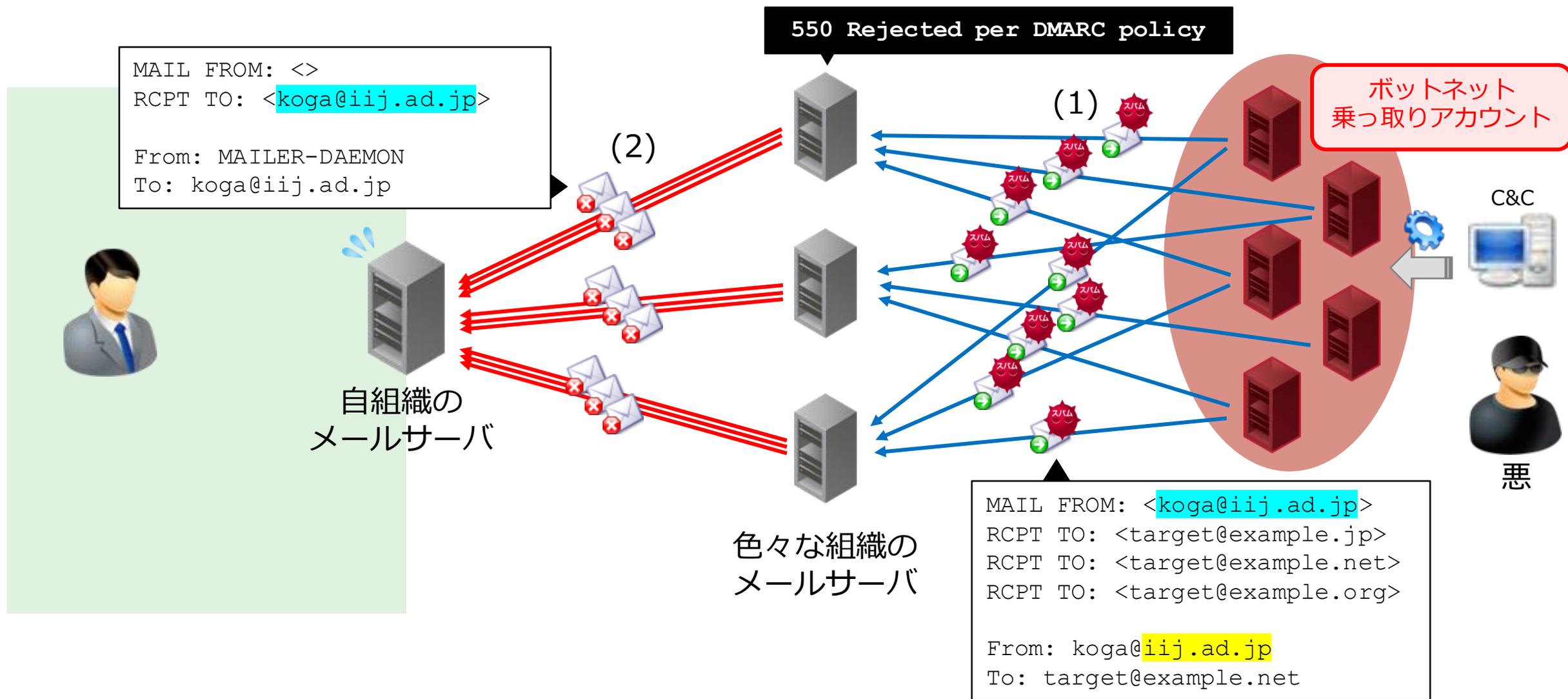
みんなが DMARC 対応したあと どういう世界が待っているのか

【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)



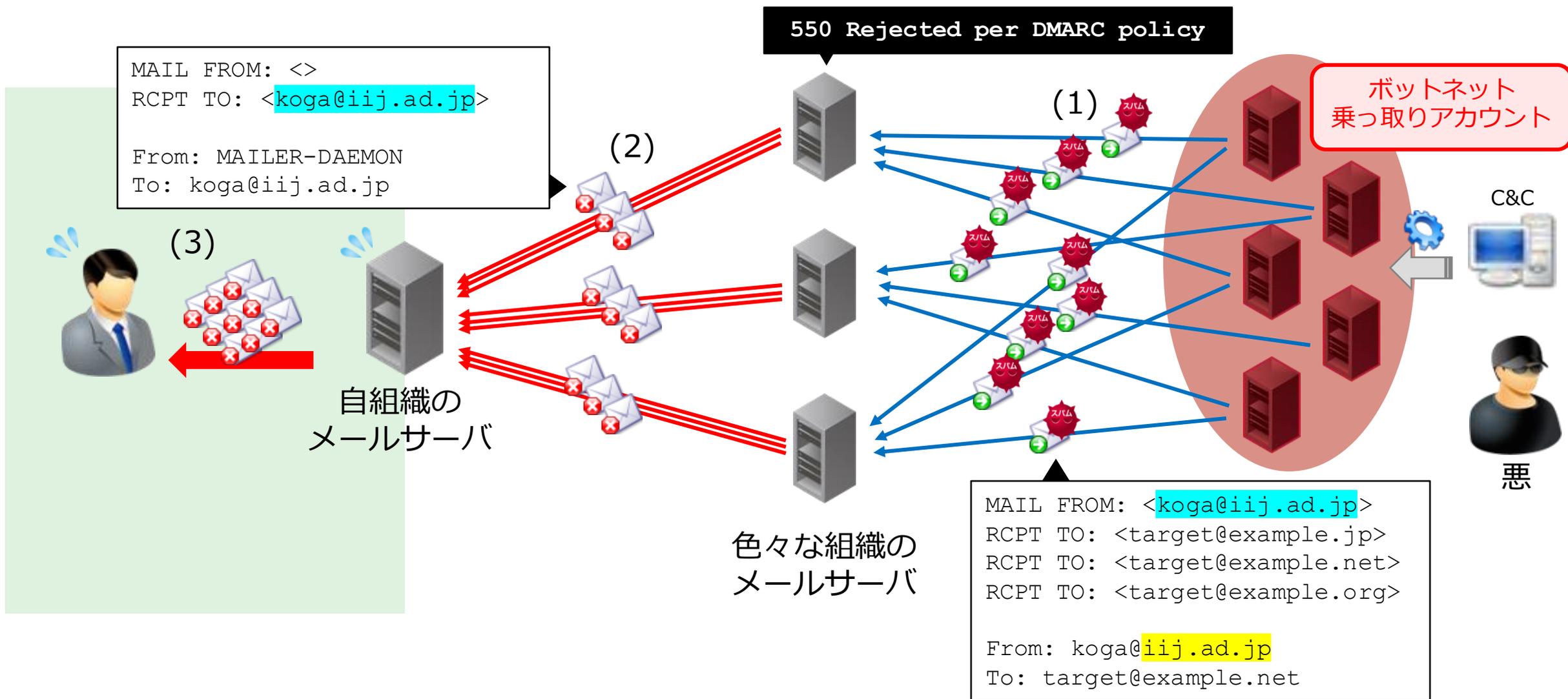
みんなが DMARC 対応したあと どういう世界が待っているのか

【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

バックスキッター問題 Backscatter Issue

MAIL FROM: <>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

RCPT TO: <target@example.org>

RCPT TO: <target@example.jp>

RCPT TO: <target@example.net>

色々な組織の
メールサーバ

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

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

C&C

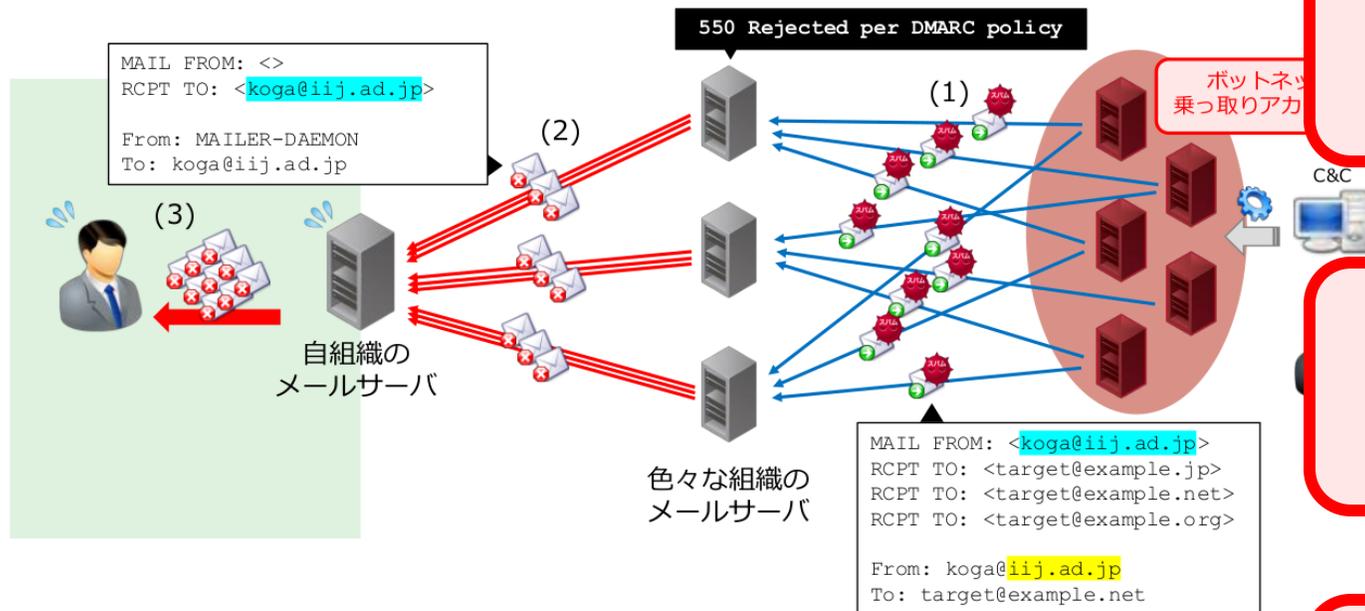


悪

バックスキッターの問題点

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

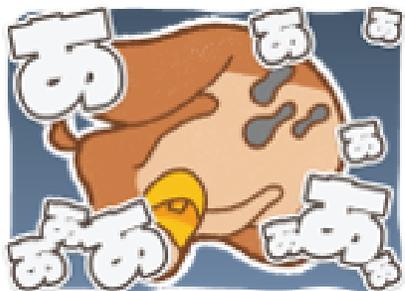
【Case 3】 悪の組織が なりすましメールを送ってエラーになる例 (大量)



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

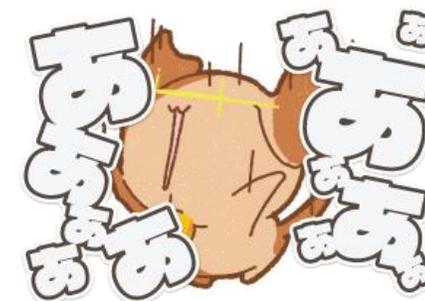
2023年 9月

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



バックスキッター対策



バックスキッター対策(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=KDDSSSSSS=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=KDDSSSSSS=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

✓ 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

III 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**

III 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**

✓ 利用者は何もしなくて良い
エンベロップ 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

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

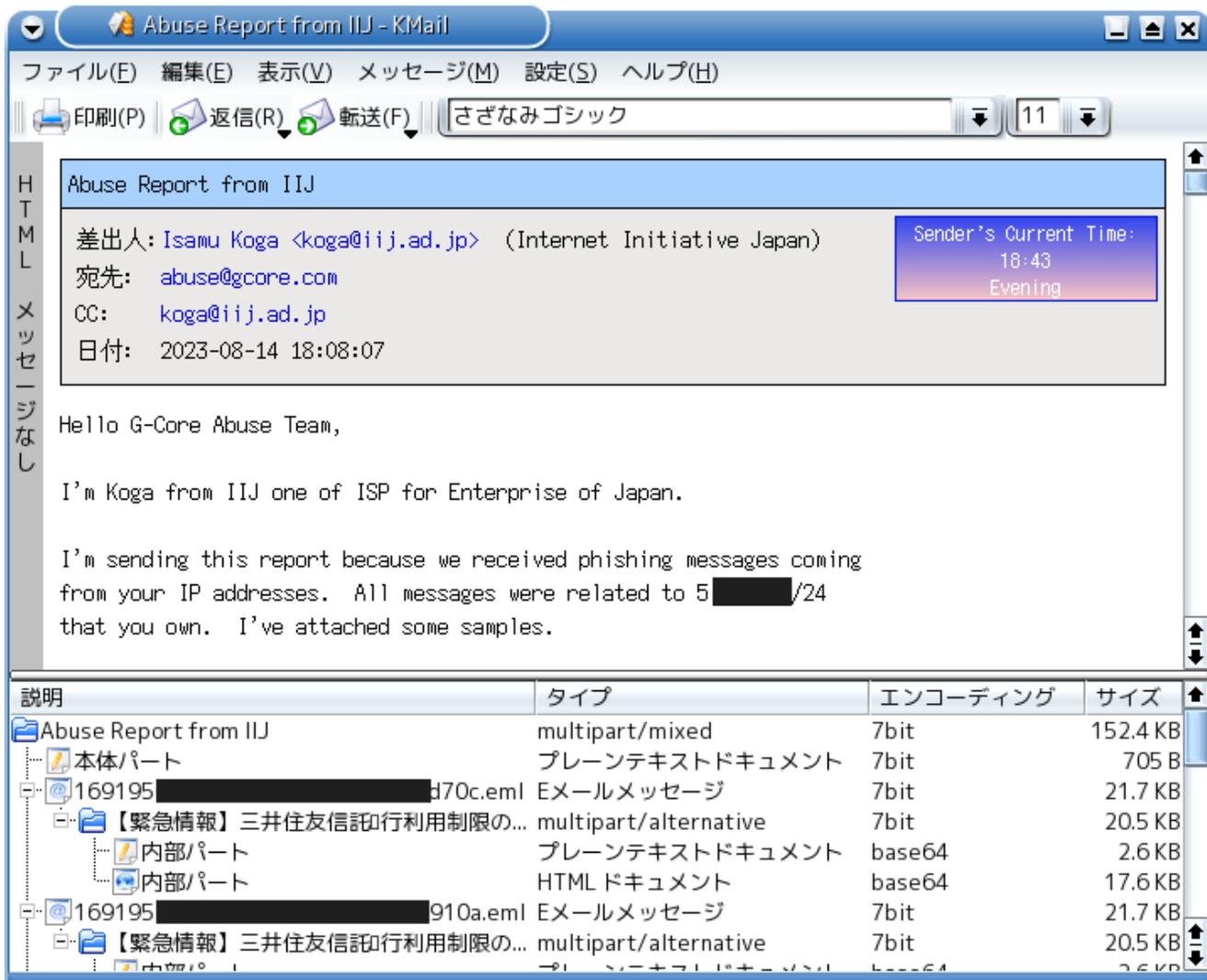
 フィルター一覧画面で保存すると、ポリシーに反映されます。

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



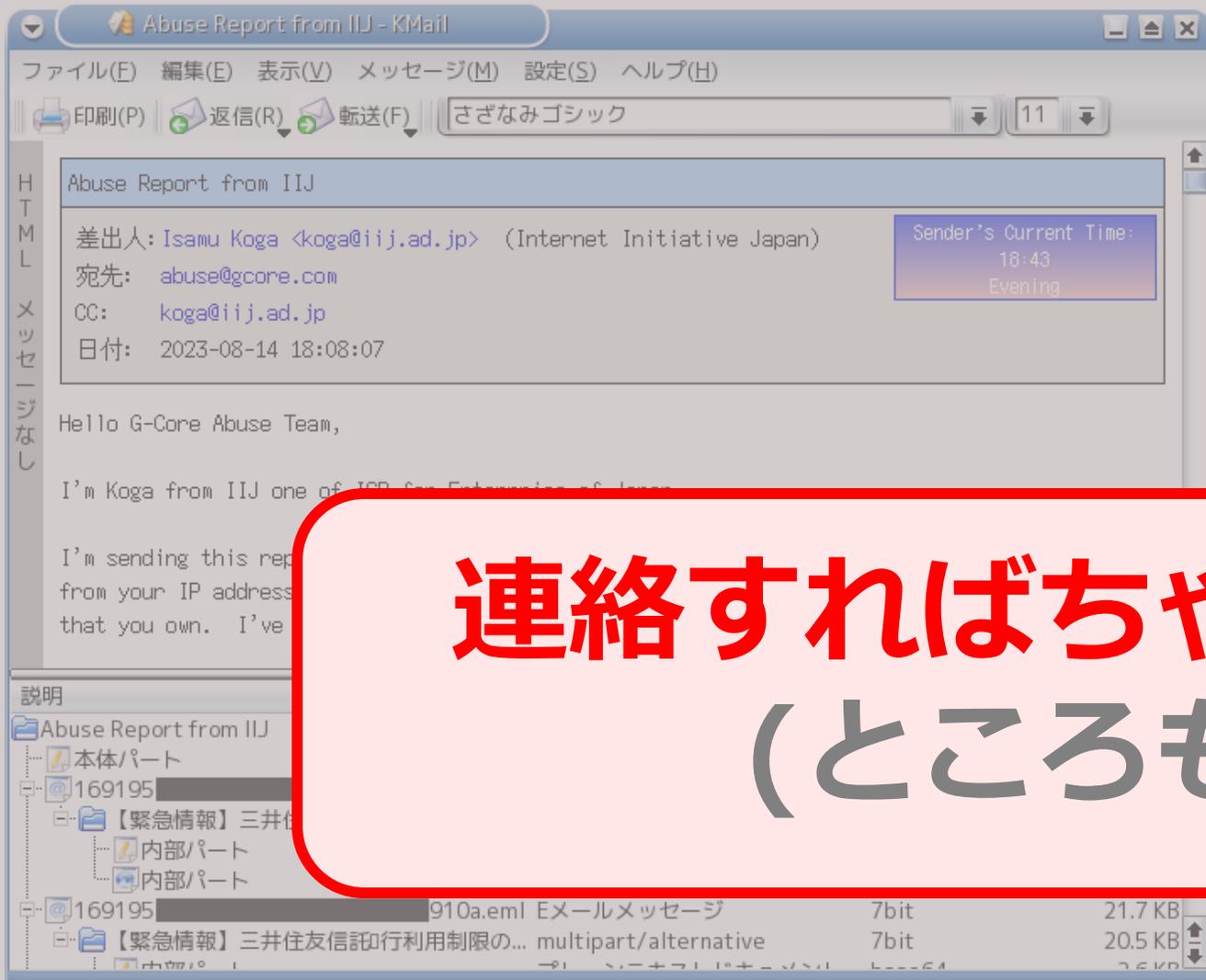
■ タイムライン

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

件名	送信者	日付	サイズ
Abuse Report from IIJ	Isamu Koga	2023-08-14 18:08:07	157.3 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 18:32:39	14.9 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 19:02:38	15.0 KB
Re: Abuse Report from IIJ	Isamu Koga	2023-08-14 19:33:12	2.9 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 19:36:58	15.2 KB
Re: Abuse Report from IIJ	Isamu Koga	2023-08-14 19:52:02	69.6 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 20:00:39	15.2 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 23:12:43	15.3 KB
Re: Abuse Report from IIJ	Isamu Koga	2023-08-14 23:41:12	2.8 KB
Abuse Report from IIJ	Gcore Claims ...	2023-08-14 23:46:21	15.1 KB

バックスキッター対策(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)**

	サイズ
4 18:08:07	157.3 KB
4 18:32:39	14.9 KB
4 19:02:38	15.0 KB
4 19:33:12	2.9 KB
4 19:36:58	15.2 KB
4 19:52:02	69.6 KB
4 20:00:39	15.2 KB
23-08-14 23:12:43	15.3 KB
Re: Abuse Report from IIJ Isamu Koga 2023-08-14 23:41:12	2.8 KB
Abuse Report from IIJ Gcore Claims ... 2023-08-14 23:46:21	15.1 KB

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**

**バックスキッター
に備えましょう**

近年のフィッシングメールの傾向

悪は常に対策が手薄なドメイン名を狙い渡り歩く

大手金融機関
が狙われる

ネットバンキング
が狙われる

DMARCで対策

DMARCで対策

クレジットカード
会社が狙われる

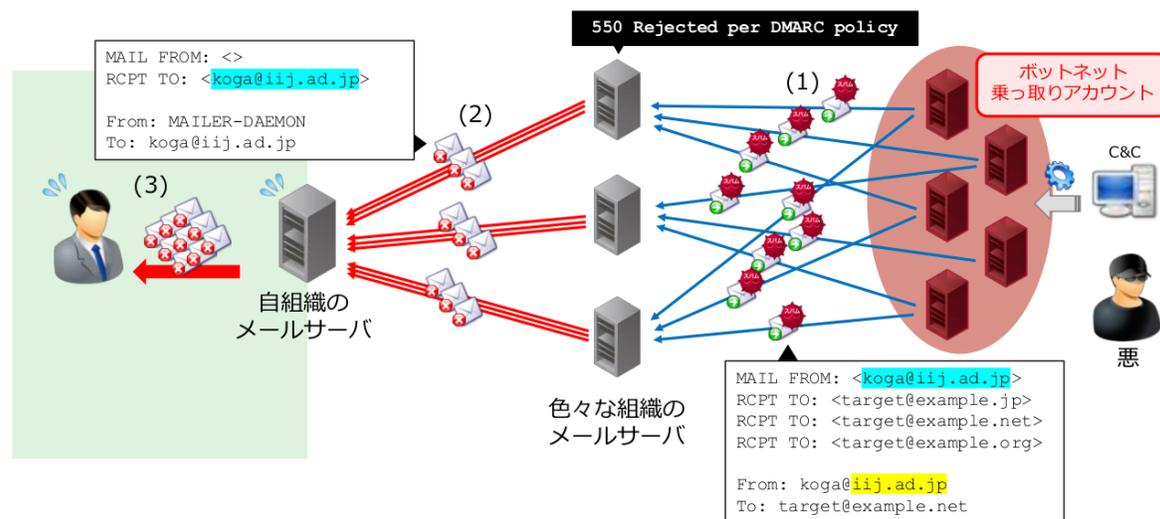
地方銀行
が狙われる

今ココ

悪は常に対策が手薄なドメイン名を狙い渡り歩く

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)



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

バックスキッター
に備えましょう

近年のフィッシングメールの傾向



悪は常に対策が手薄なドメイン名を狙い渡り歩く

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トラブる例 (大量)



Lead Initiative

日本のインターネットは1992年、IIJとともに始まりました。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はいつも始まりであり、未来です。

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。

©Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。