

想定所要時間 **35**分

第7回 JPAAWG (A1-7)  
17:15~18:00

**IIJ** Internet Initiative Japan

# IIJ の新たな取り組み 「ディフェンス対応」

お客様を脅威から保護する取り組み

2024/11/11(月)

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 メールサービス運営課  
課長 古賀 勇

Ongoing Innovation



# 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  
メールサービス運営課・課長

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

M<sup>3</sup>AAWG  
MESSAGING MALWARE MOBILE  
ANTI-ABUSE WORKING GROUP  
M3AAWG

openSUSE

openSUSE (趣味)

# ⚠️ みなさんへのお願い ⚠️

今日ここで聞いた内容を

(仮に友達にいたとしても) spammer に

話さないでください

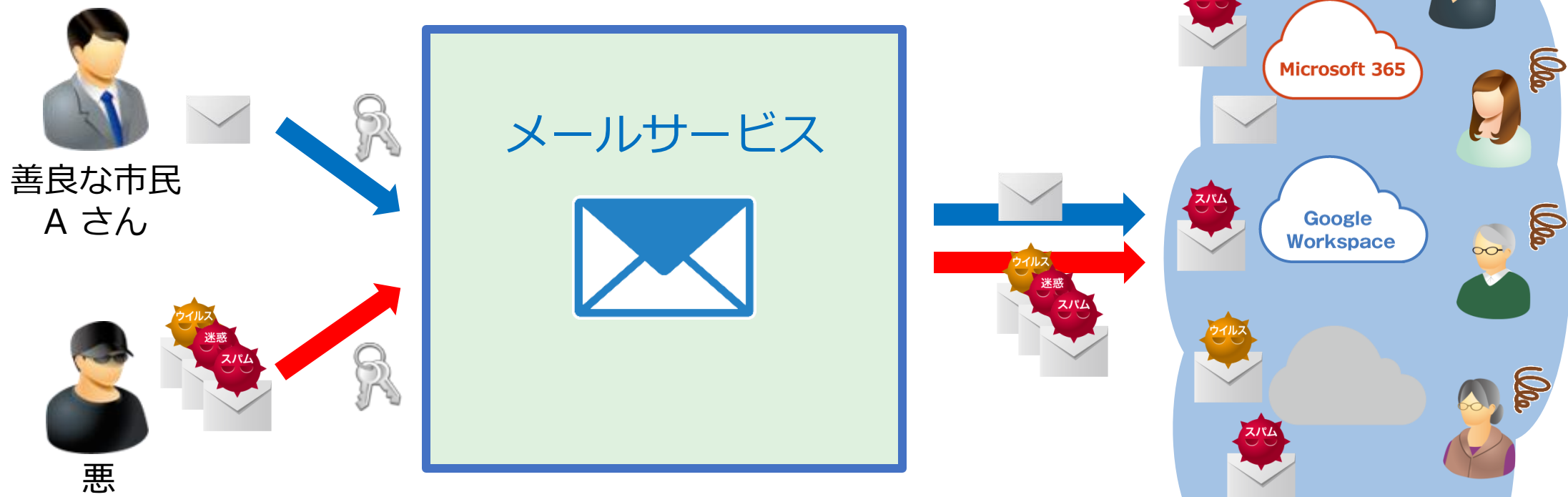
# アビューズ abuse とは

本来の意味は「乱用」とか「虐待」のような意味



# abuse (アビュース) 対応とは

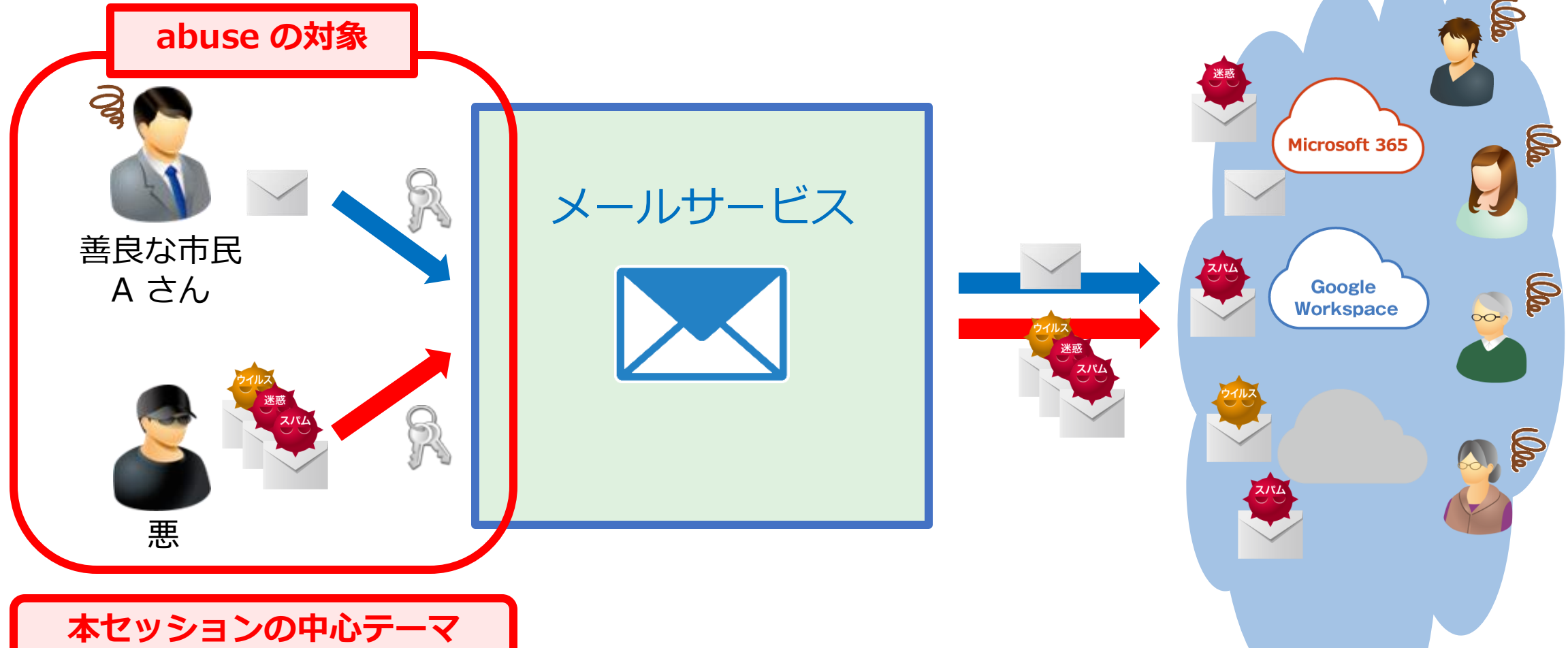
インターネット上での迷惑行為や不正・違法行為の総称



|        |        |        |           |
|--------|--------|--------|-----------|
| 例えば... | DoS 攻撃 | 誹謗中傷   | 権利侵害      |
|        | 名誉毀損   | 不正アクセス | その他迷惑行為全般 |

# abuse (アビュース) 対応とは

インターネット上での迷惑行為や不正・違法行為の総称



本セッションの中心テーマ

(例) メールサービスのアカウントを悪用され(乗っ取られ)、フィッシングメールなどを送信される

# abuse 行為が行われると 何が問題なのか

「悪」によってメールサービスがフィッシングメールの送信に  
不正利用される例



# abuse 行為の目的

## 内容は変化しているが目的は変わっていない

### ■ 古典的な迷惑メール（～2010年頃）

- ・ 偽ブランド広告、出会い系サイト、株価の釣り上げ
- ・ 違法薬物、アダルトサイトへの誘導

### ■ 近年のフィッシングメールの送信

- ・ Web サービス・アプリの ID を盗み出す
- ・ パスワードや銀行口座、クレジットカード番号を盗み出す

「悪」の目的 = 金銭的な利益を得る 💰

#### 第 19 条(禁止事項)

契約者は、次の各号のいずれかに該当する事項を行ってはならないものとします。

- (1) 違法、不当、公序良俗に反する態様において IIJ インターネットサービスを利用すること。
- (2) 当社又は当社のサービスの信用を毀損するおそれがある態様で IIJ インターネットサービスを利用すること。
- (3) 当社のサービスを直接又は間接に利用する者の当該利用に対し支障を与える態様において IIJ インターネットサービスを利用すること。

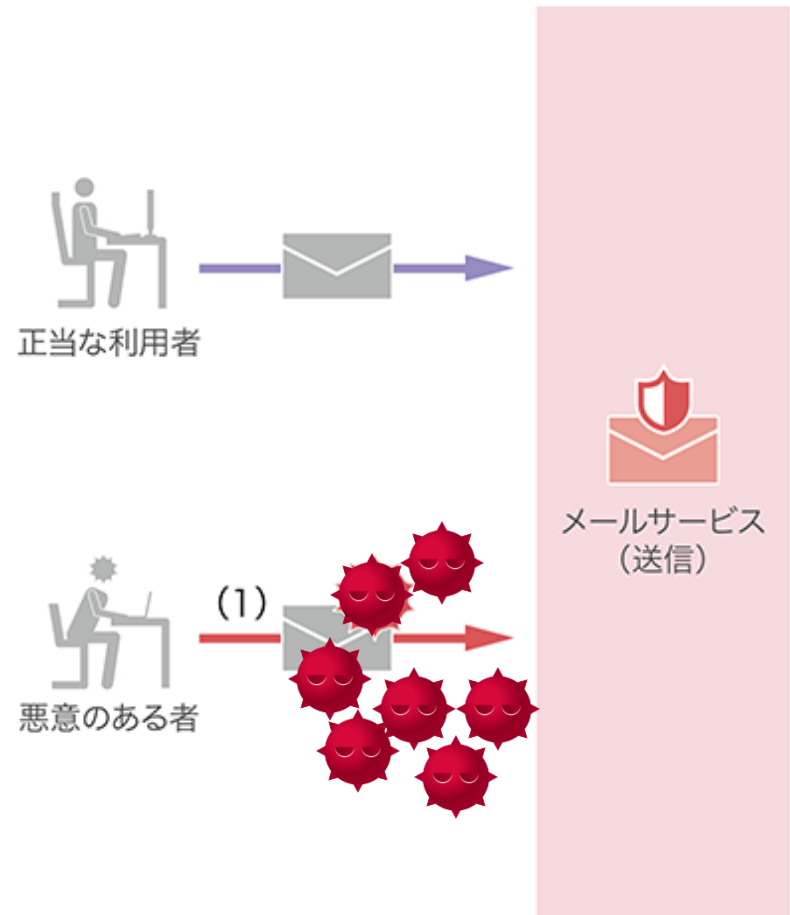
▲ IIJ インターネットサービス契約約款・一般規程

<https://www.ij.ad.jp/svcsol/agreement/>

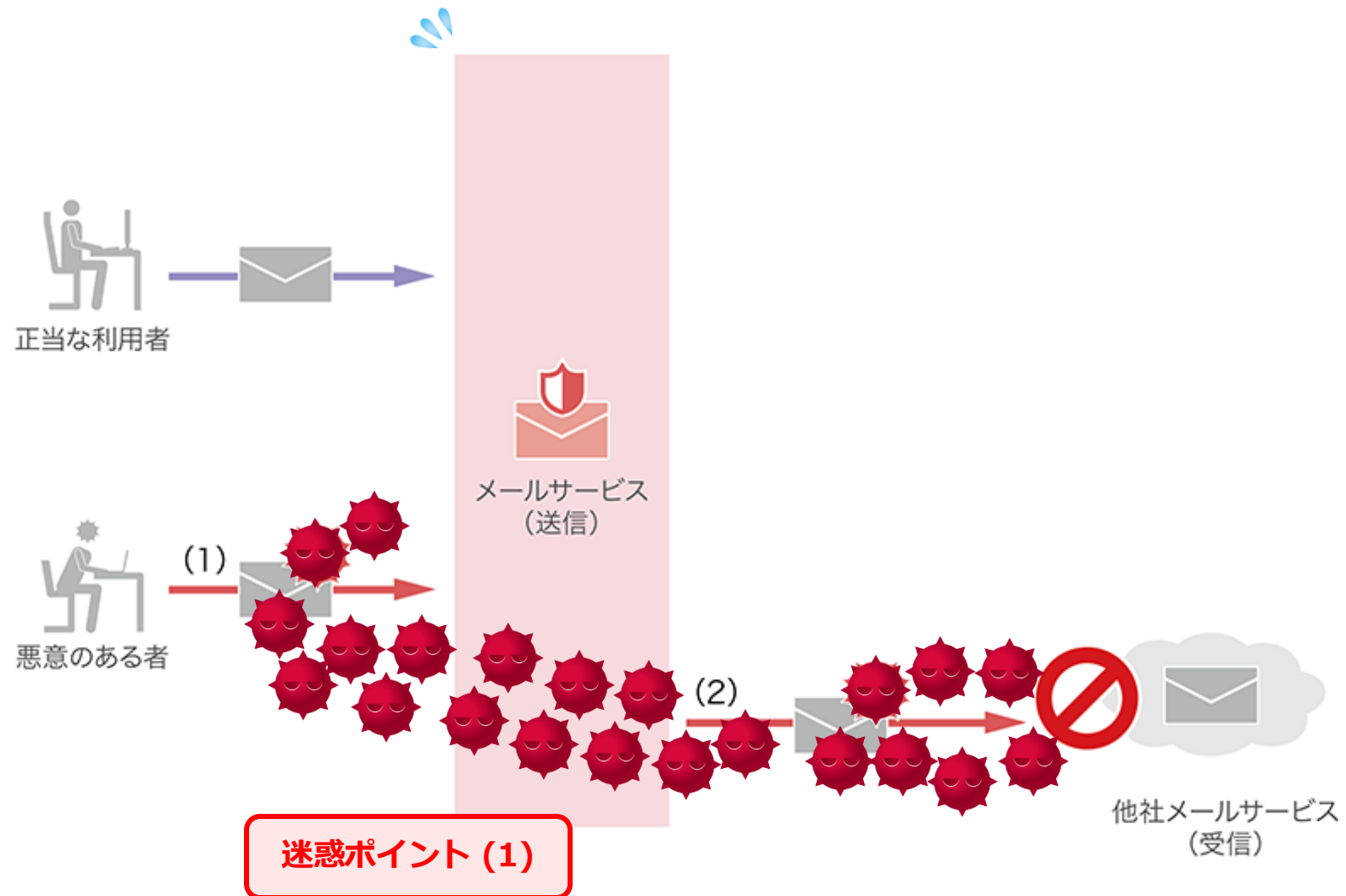




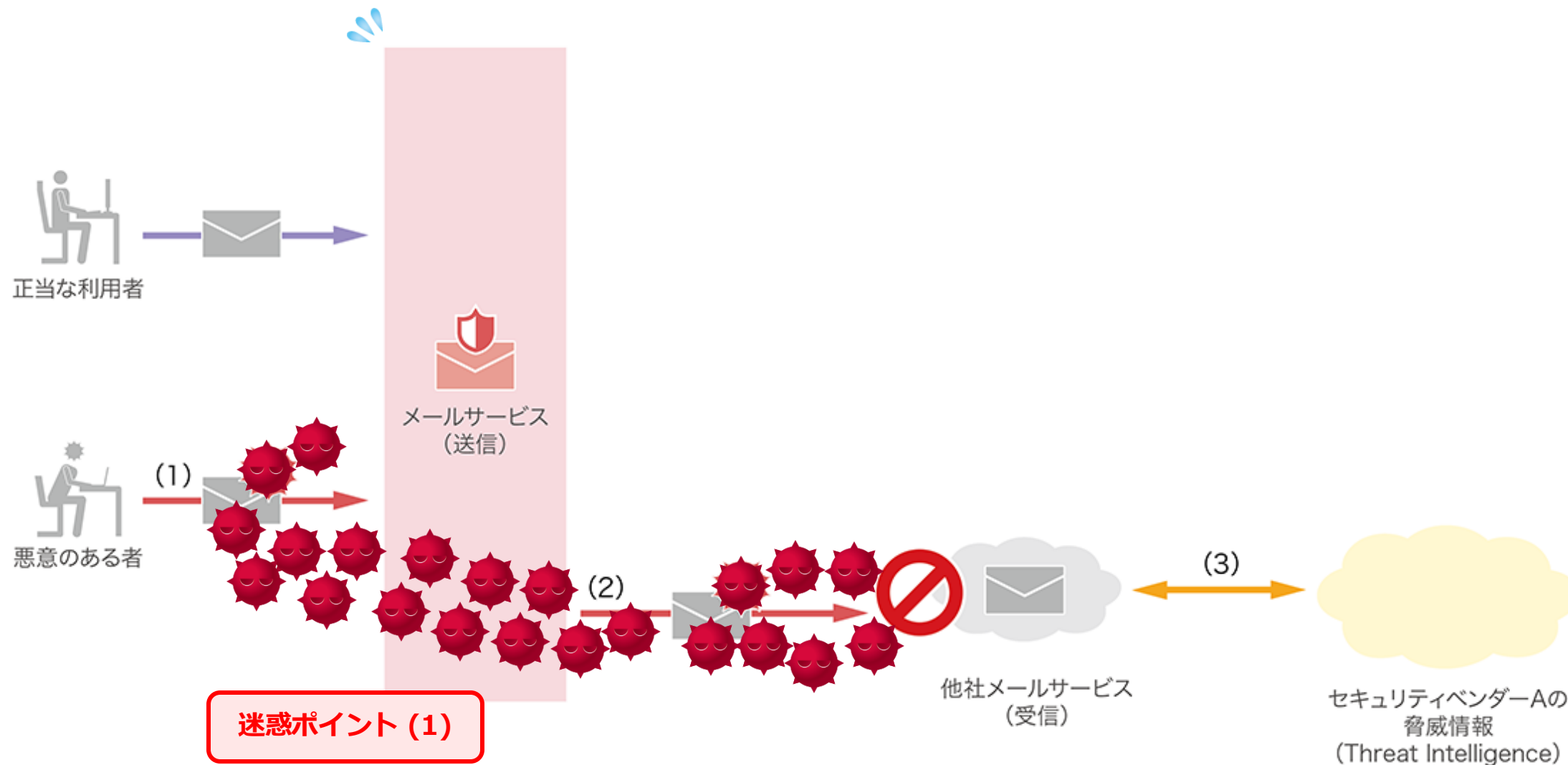
# abuse 行為が行われると何が問題なのか



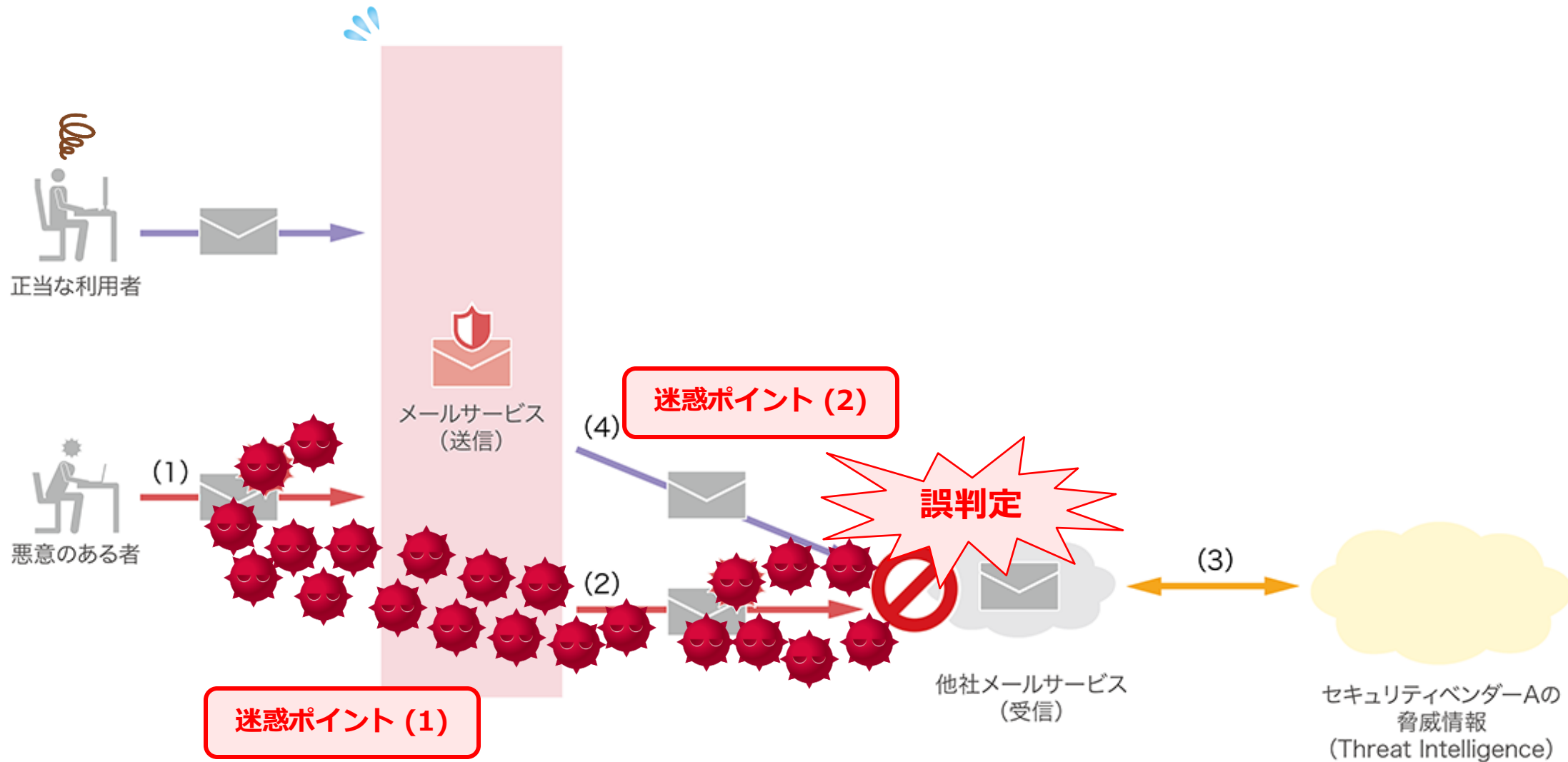
# abuse 行為が行われると何が問題なのか



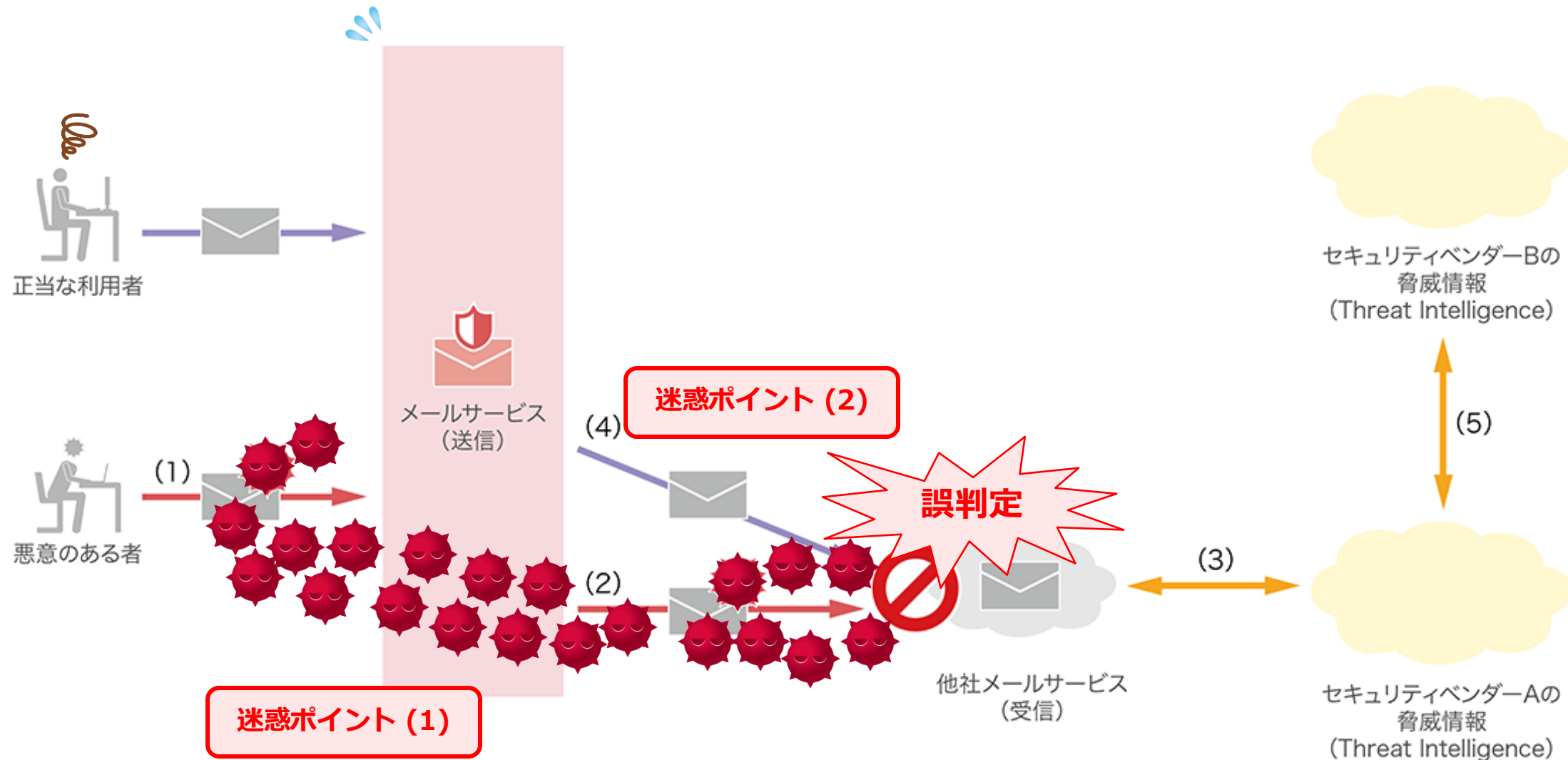
# abuse 行為が行われると何が問題なのか



# abuse 行為が行われると何が問題なのか



# abuse 行為が行われると何が問題なのか





abuse 行為が行われると何が問題なのか

攻撃対象となったユーザへの被害のみならず、メールサービスでも悪影響が発生

# Request for delist

# 誤検知

# 不達調査

## 不具合ですか？

## stop sending abuse mail immediately!!

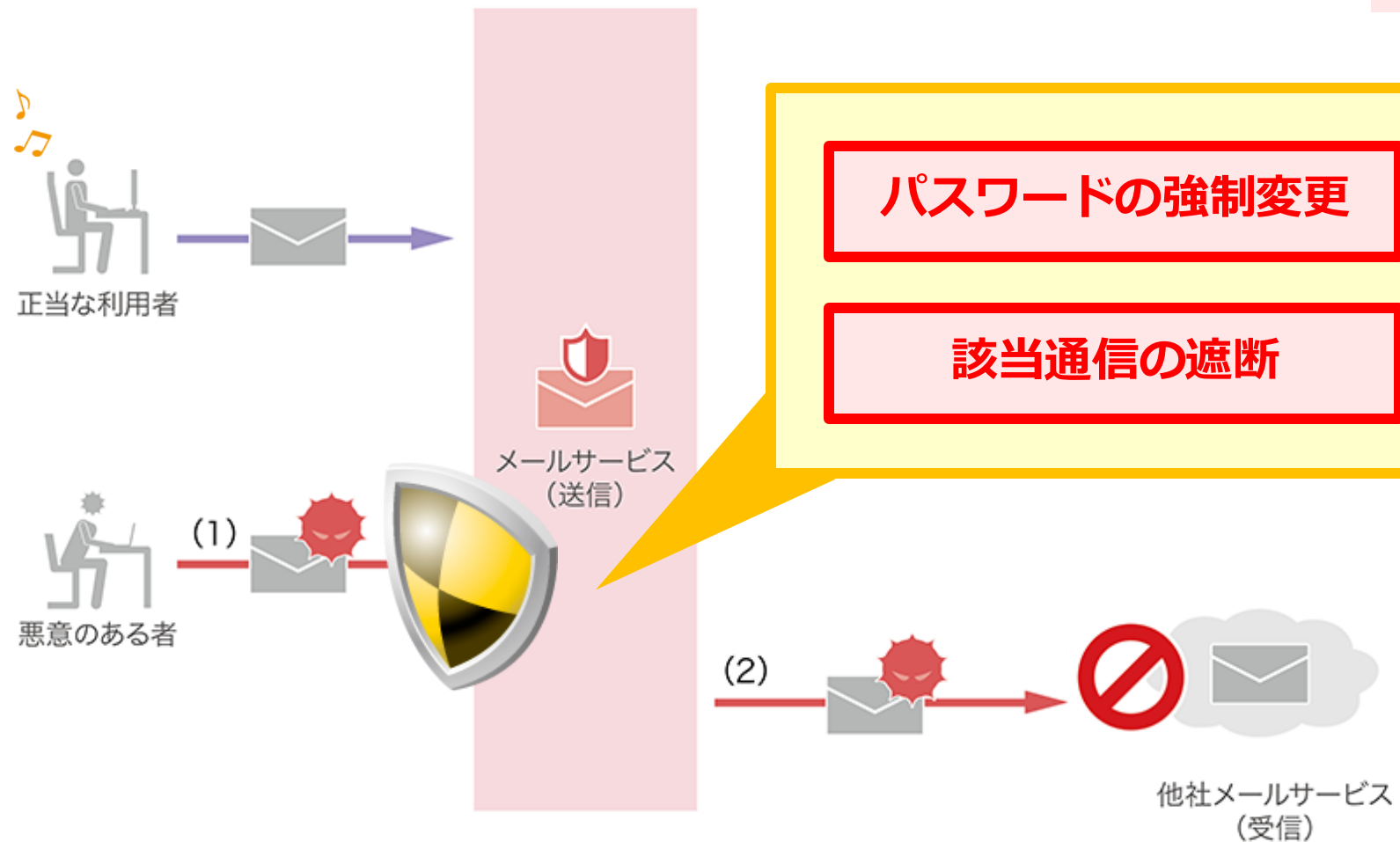
## メールが届かない



# abuse 対応の実施

サービスの安定稼働や他のお客様への悪影響回避のため、事象を検知したら abuse

⇒ ただし、事後対応になる





# abuse と通信の秘密

本セッションで「通信の秘密」について議論を深めることは本質ではありませんので、軽く触れる程度にします



# abuse と通信の秘密

日本では、電気通信事業者が取り扱う電気通信について知得などの行為をすることは、電気通信事業法第4条によって禁止されています。

しかし、abuse 行為の発生が明示的に認知されており、これを放置するとサービス利用者が他人の権利を侵害する不法行為に加担してしまったり、自身が被害に遭ったりする強い蓋然性(がいぜんせい)がある場合に、それらの事態を回避するために電気通信に関与することは、緊急避難や正当業務行為として違法性が阻却され得ると整理されています。

また、IIJ と利用者間の契約において、abuse 行為に相当する行為は禁止されており、契約違反が明らかであるときは、IIJ としても契約当事者としての諸措置をもって対処することができます。

※IIJ 法務部門(コンプライアンス部)からのコメントそのまま

(参考)

「ネットを監視も干渉もしない国は、日本を含むたった4カ国だけ」

(谷脇康彦著「教養としてのインターネット論」日経 BP, 2023年)

米国 NPO 調査 (<https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>)



# 不正利用の準備行為の発見

「悪」の計画的犯行の現場を見た



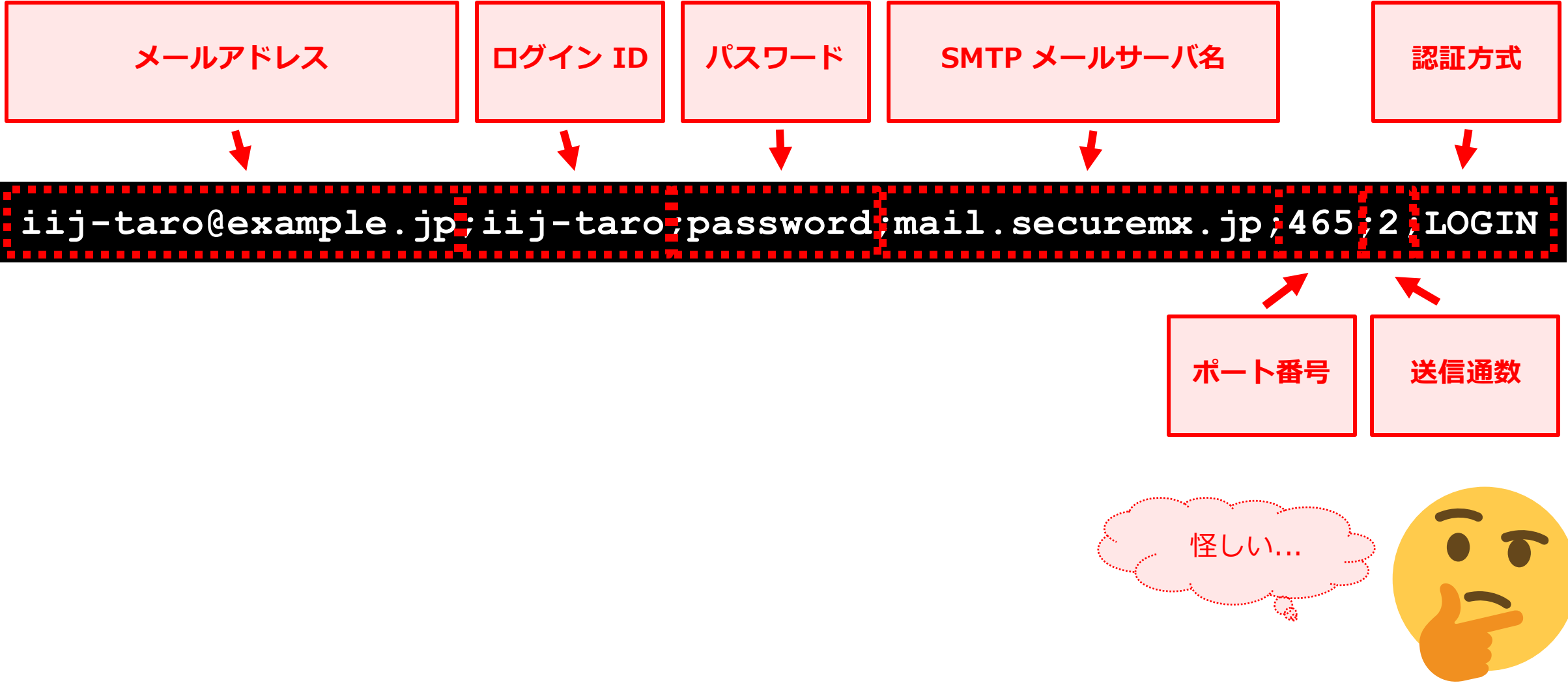
# abuse 対応の事後・影響調査をしていたときに発見したログ

---

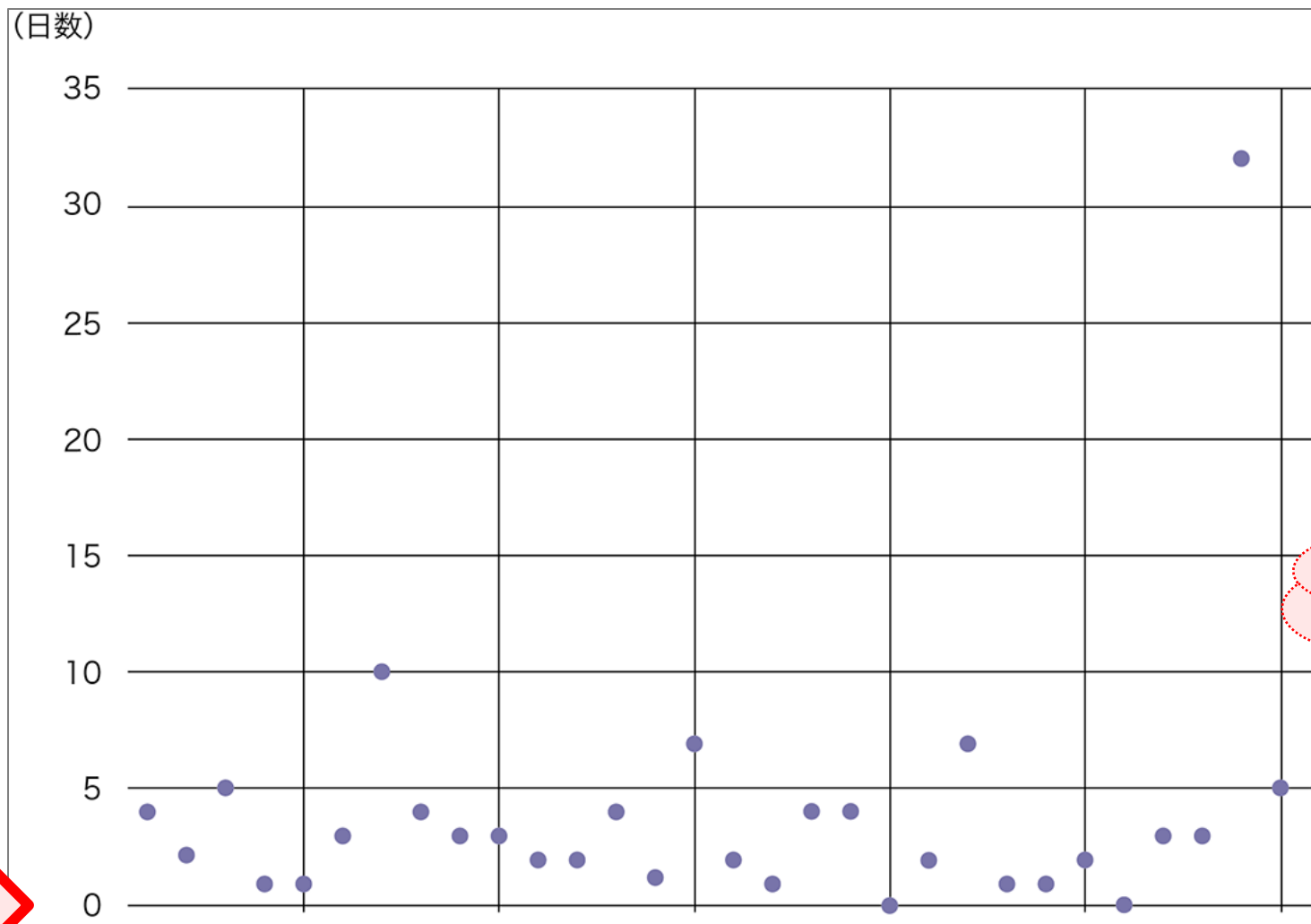
```
ij-taro@example.jp;ij-taro;password;mail.securemx.jp;465;2;LOGIN
```



# abuse 対応の事後・影響調査をしていたときに発見したログ



# 探索行為から実際に abuse 行為がされるまでの日数



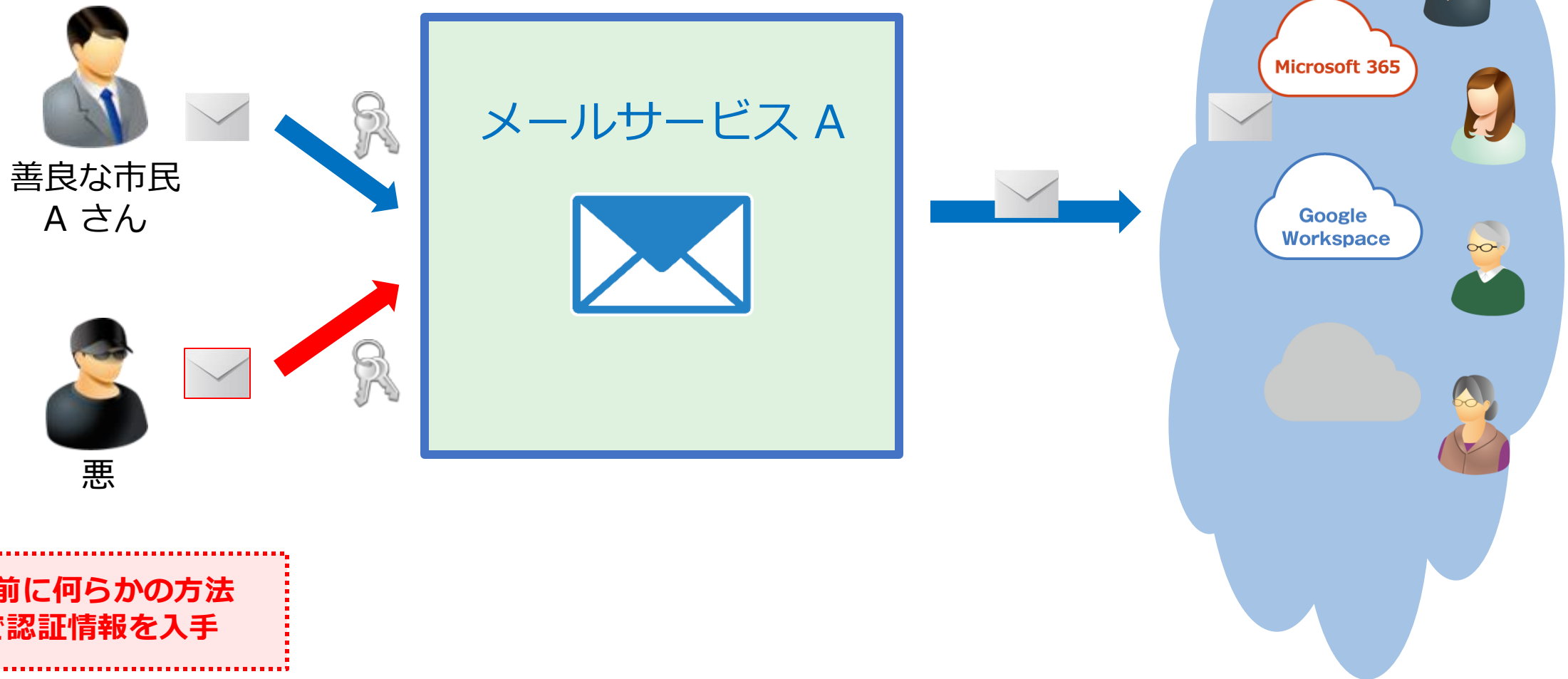
探索行為が  
あった日を 0日

探索行為以前に認証失敗した形跡もなし

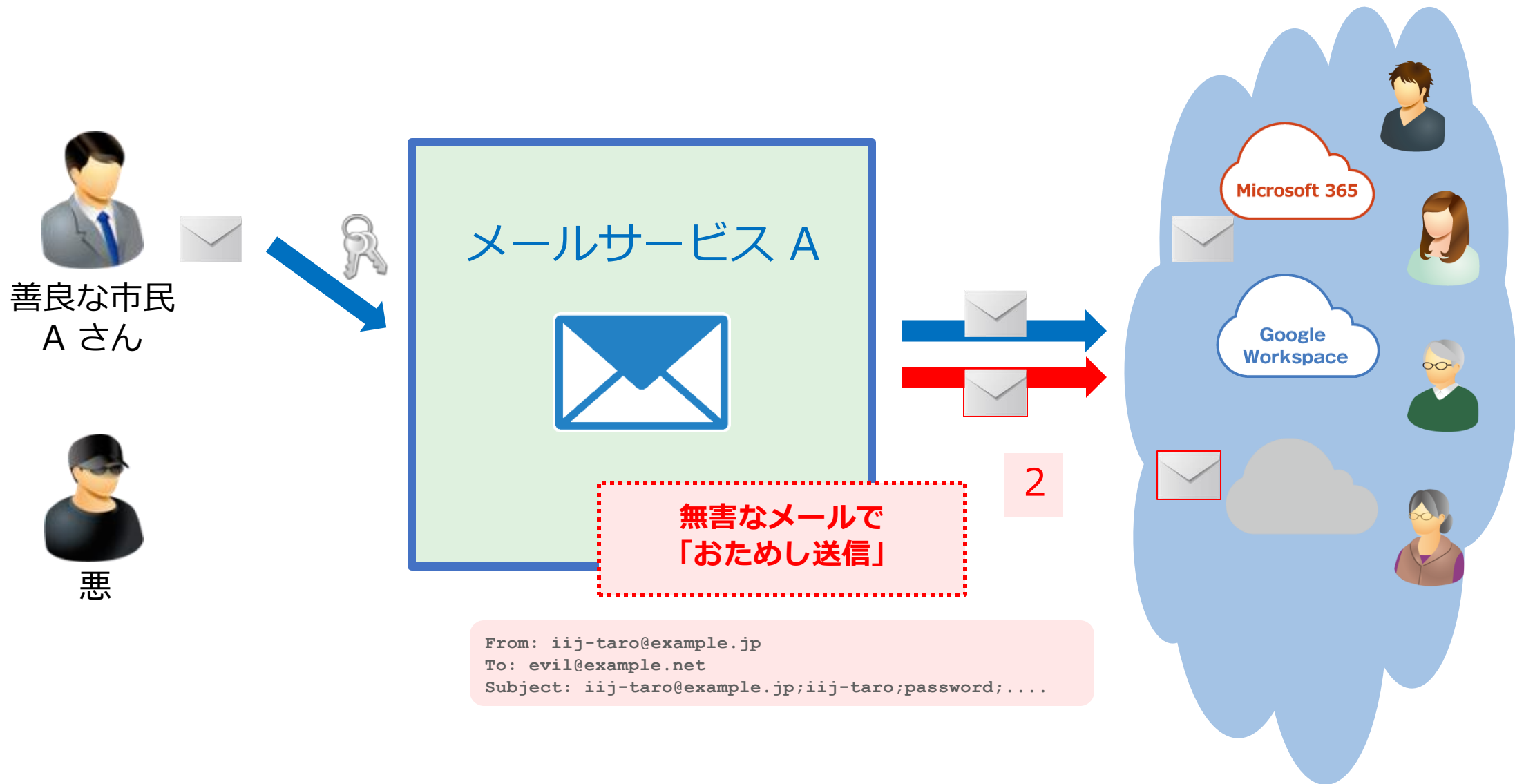
だいたい 1週間以内  
に abuse だと...?



# 不正利用の準備行為の発見

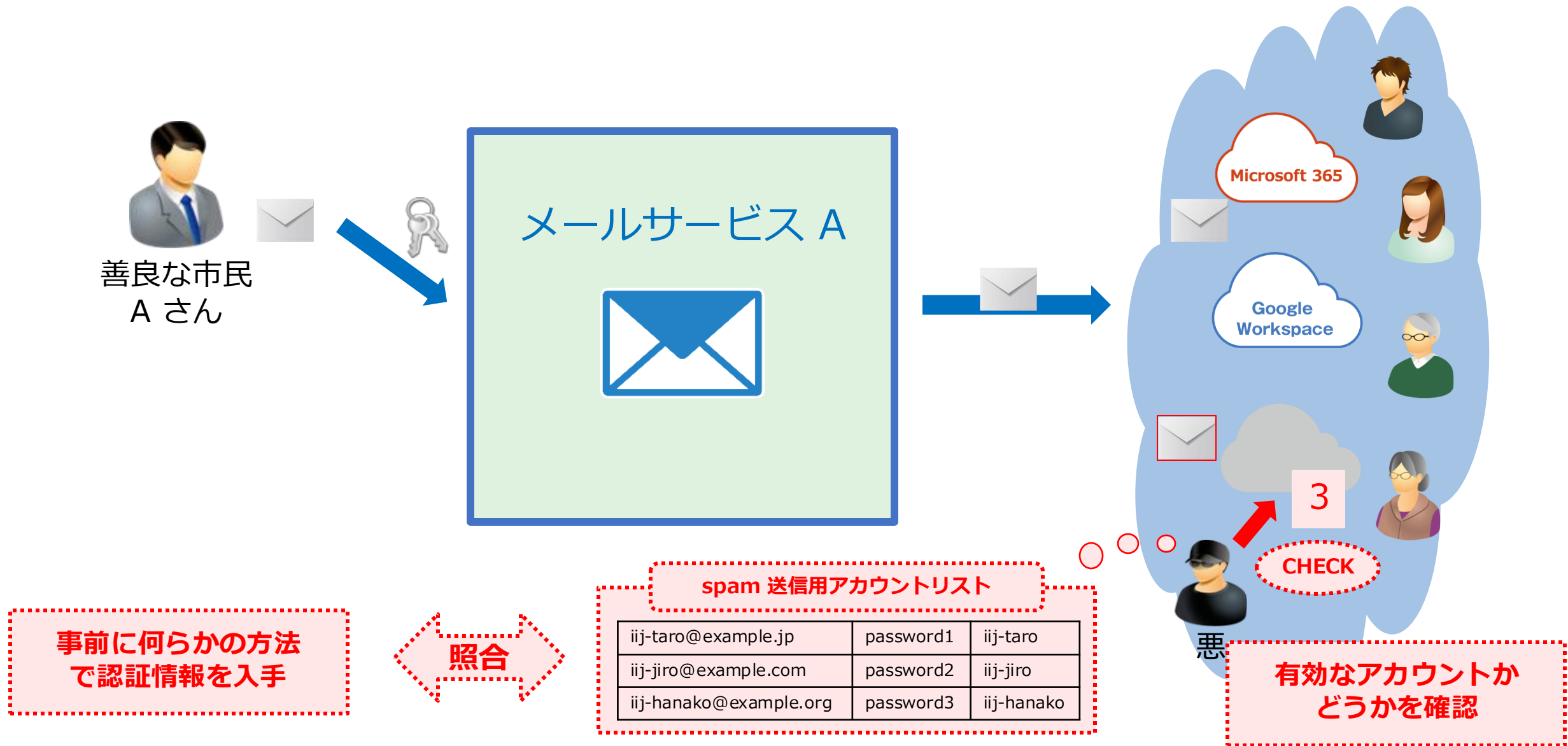


# 不正利用の準備行為の発見



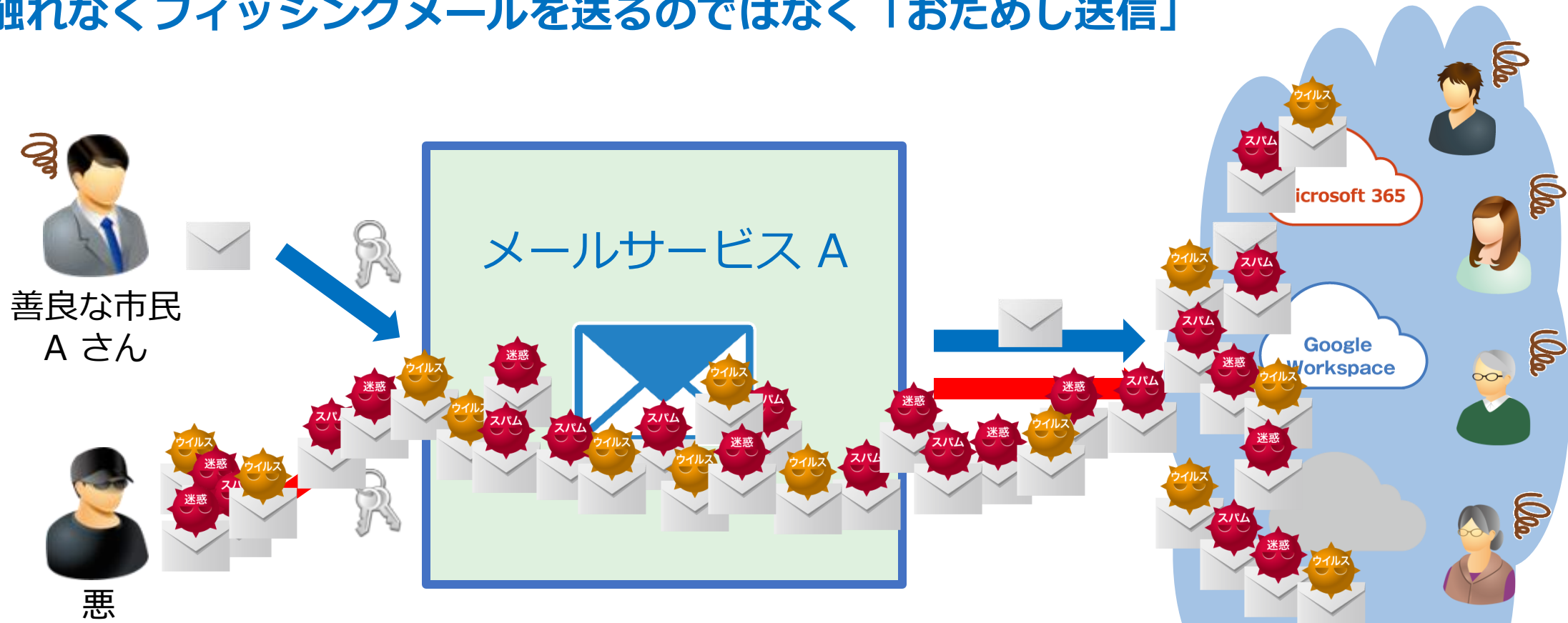


# 不正利用の準備行為の発見



# 不正利用の準備行為の発見

前触れなくフィッシングメールを送るのではなく「おためし送信」



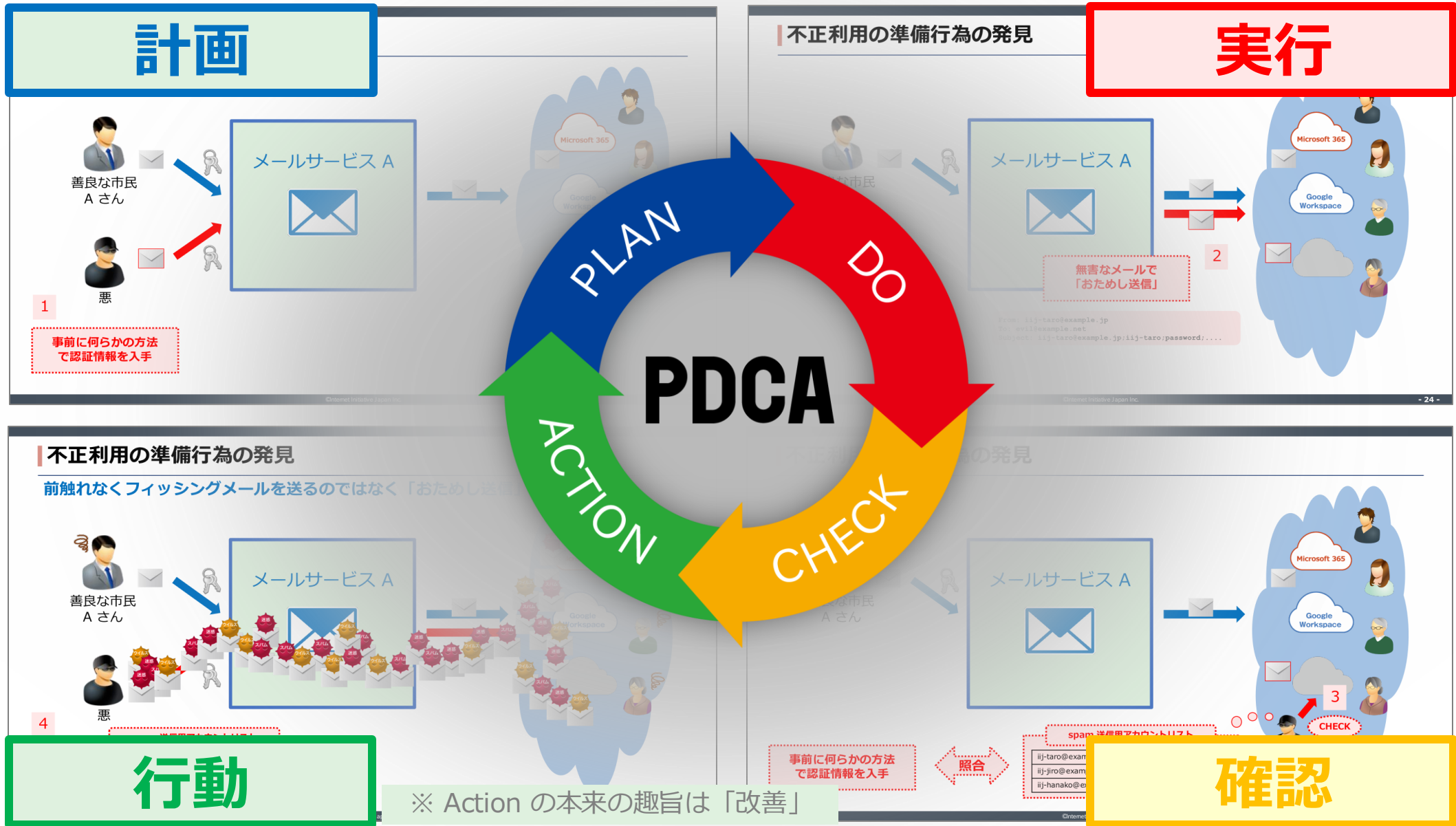
4

spam 送信用アカウントリスト

|                        |           |            |
|------------------------|-----------|------------|
| ijj-taro@example.jp    | password1 | ijj-taro   |
| ijj-jiro@example.com   | password2 | ijj-jiro   |
| ijj-hanako@example.org | password3 | ijj-hanako |



# これ PDCA のサイクルだ！



# 不正利用の準備行為の発見

ただし、このような準備段階の時点では、サービスに影響を与えておらず、「他人の権利を侵害している」とは言い難い

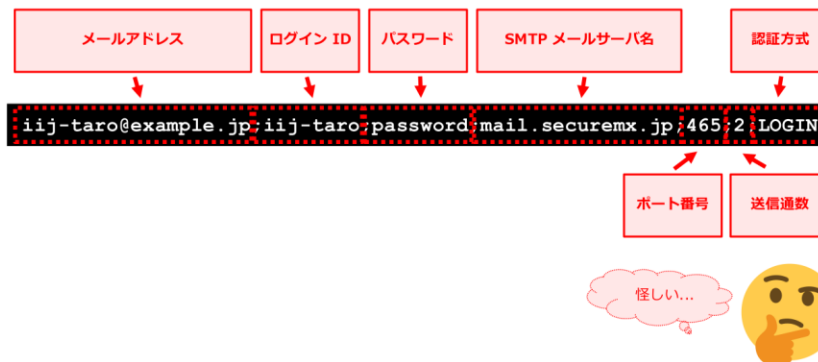
準備行為を察知しつつも、実際に abuse 行為がされるまで、具体的な対処を行う根拠がない

このままではサービスの品質を維持しお客様を保護することができない！

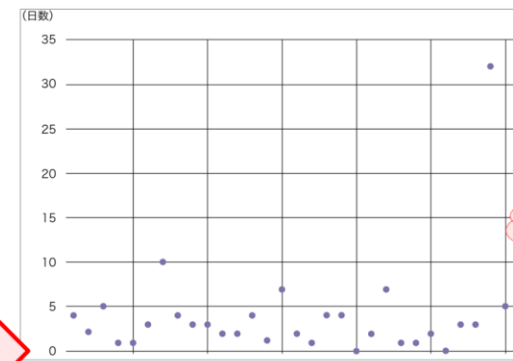
かなしみ



## abuse 対応の事後・影響調査をしていたときに発見したログ



## 探索行為から実際に abuse 行為がされるまでの日数



探索行為があった日を0日

# IIJ の新しい取り組み

お客様を保護し、サービスの品質を維持するために



# IIJ の新しい取り組み

## 新しい枠組みを設計するため、サポート部門、法務部門を巻き込んで議論

### ■ フィッシングメールが送信される前に対策できれば...

| メールサービス事業者(IIJ)視点  | 利用者視点   |
|--|---|
| <ul style="list-style-type: none"><li>メールの大量送信によるサービス障害を回避</li><li>誤判定で宛先に届かない、といった状況を回避</li></ul> | <ul style="list-style-type: none"><li>認証情報が漏えいしている状況を早期に察知</li><li>「悪」によってメールを盗み見られたり、情報流出する被害を最小限に</li></ul> |



### ■ 不正利用のための準備行為を察知した場合

- 実際に**フィッシングメールが送信される前**に必要な範囲で通信の制限を実施することを**契約上の行為として導入**
- これをすべてのお客様に事前に取り組む内容をお知らせ
- メールサービスの個別規程にも具体的な内容を盛り込む

#### 第 12 条(不正利用等のおそれへの対処)

当社は、IIJ セキュア MX サービスの運用上得られた情報に基づき、契約者のアカウントの不正利用及び不正利用のための探索等の準備行為(本条において「不正利用等」といいます。)が行われており、これを放置することにより契約者又は契約者の通信先に被害が生ずるおそれがあると合理的に判断される場合には、契約者に連絡することなく、契約者の通信を必要な範囲で制限する等により不正利用等を抑止するための措置を講ずることができるものとします。

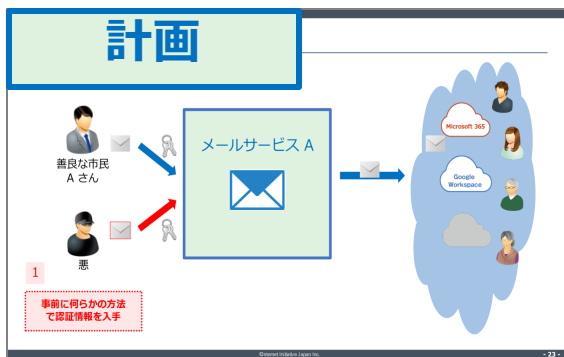
2 前項の措置を講じた場合には、当社は、事後遅滞なく契約者に連絡するものとします。なお、前項の措置は不正利用等を完全に抑止することを保証するものではなく、連絡を受けた契約者は、契約者の裁量と責任において不正利用等に対処するものとします。

IIJ セキュア MX サービス個別規程 (2024年 5月 1日改訂) ▶  
<https://www.ij.ad.jp/svcsol/agreement/>

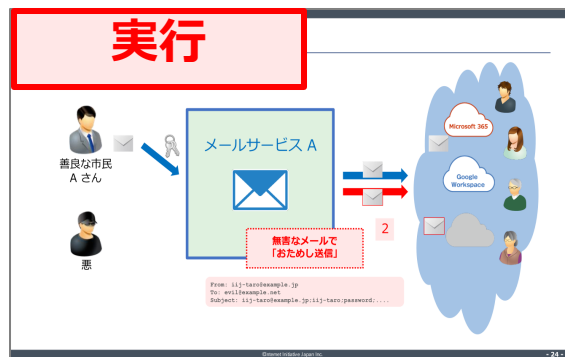


# IIJ の新しい取り組み

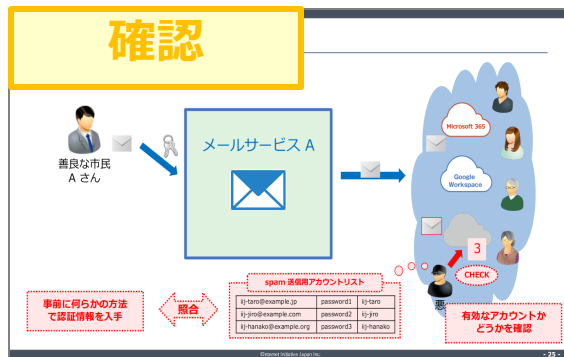
1



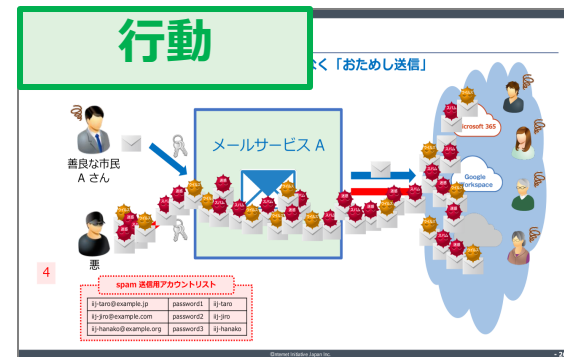
2



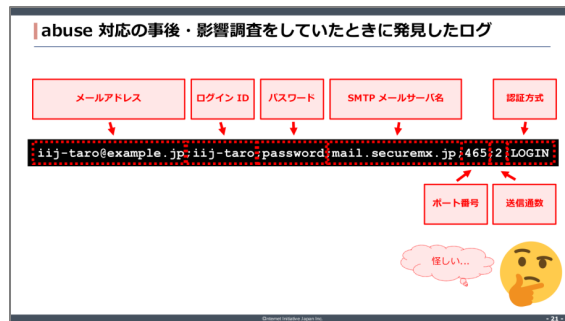
3



4



この間に検知できれば勝ち





# IIJ の新しい取り組み 「ディフェンス対応」

不正利用の準備行為を察知して「事前に」お客様を保護する取り組み

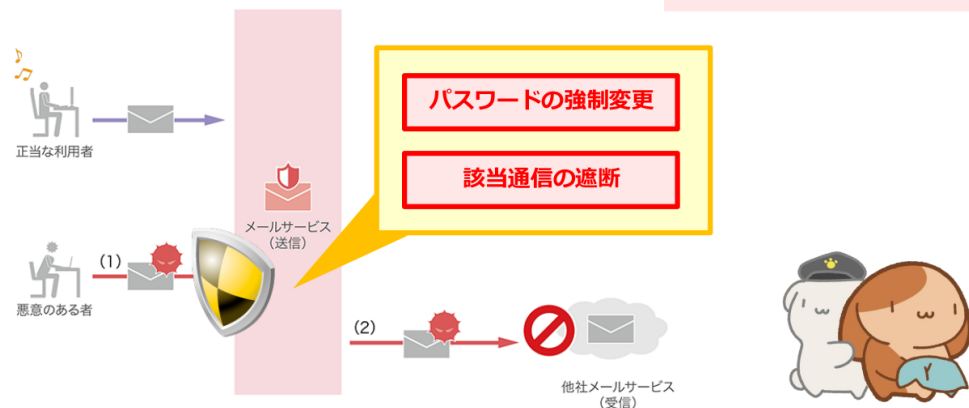
abuse 対応 (事後対応)

ディフェンス対応 (事前対応)

## abuse 対応の実施

サービスの安定稼働や他のお客様への悪影響回避のため、事象を検知したら abuse

⇒ ただし、事後対応になる



©Internet Initiative Japan Inc.

- 16 -

## IIJ の新しい取り組み

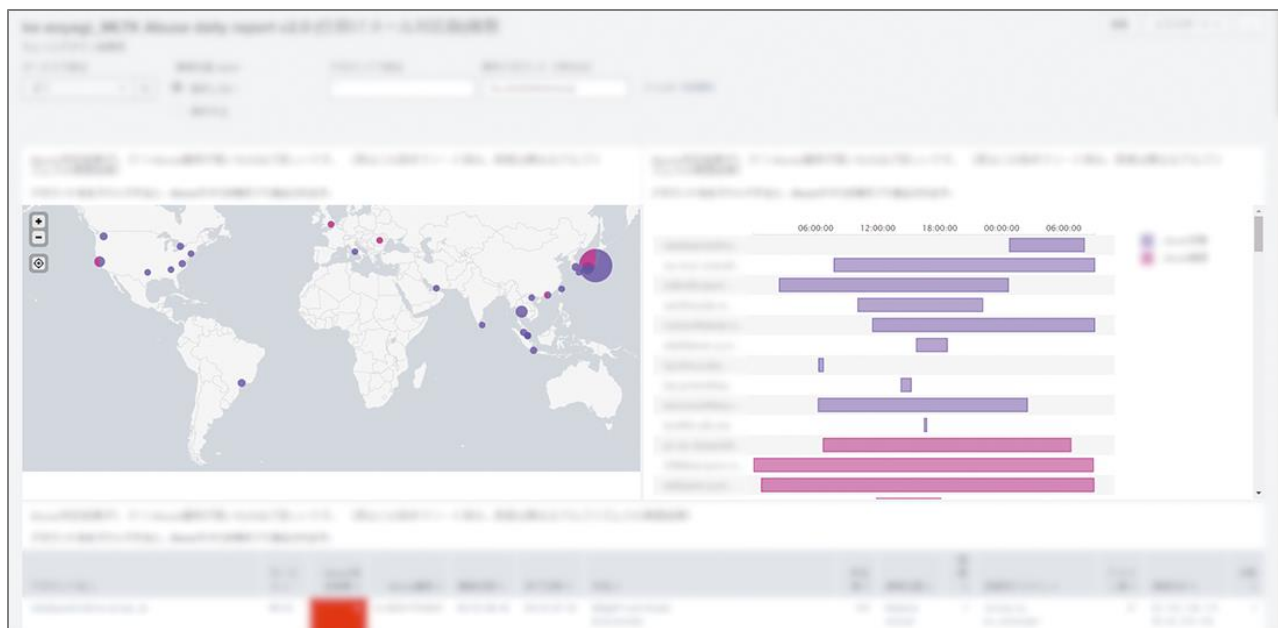


©Internet Initiative Japan Inc.

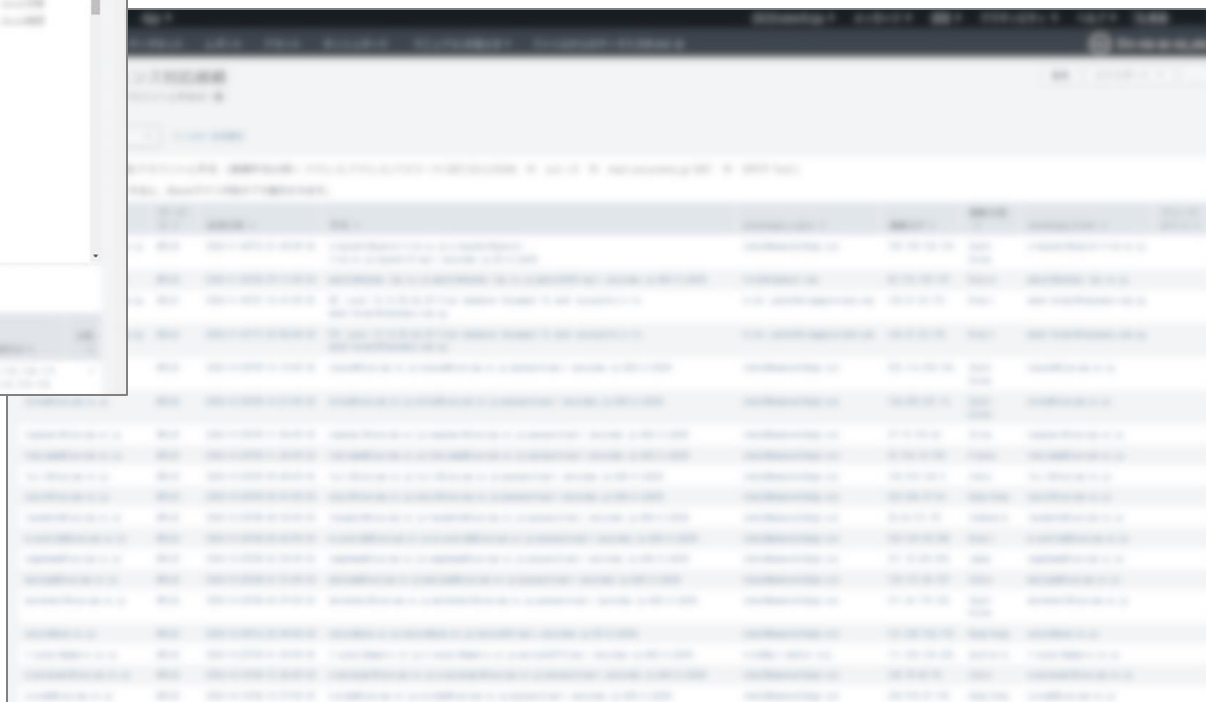
- 32 -

## IIJ の新しい取り組み 「ディフェンス対応」

不正利用の準備行為と思われる事象を大規模ログ分析基盤で検出  
24時間体制で対応

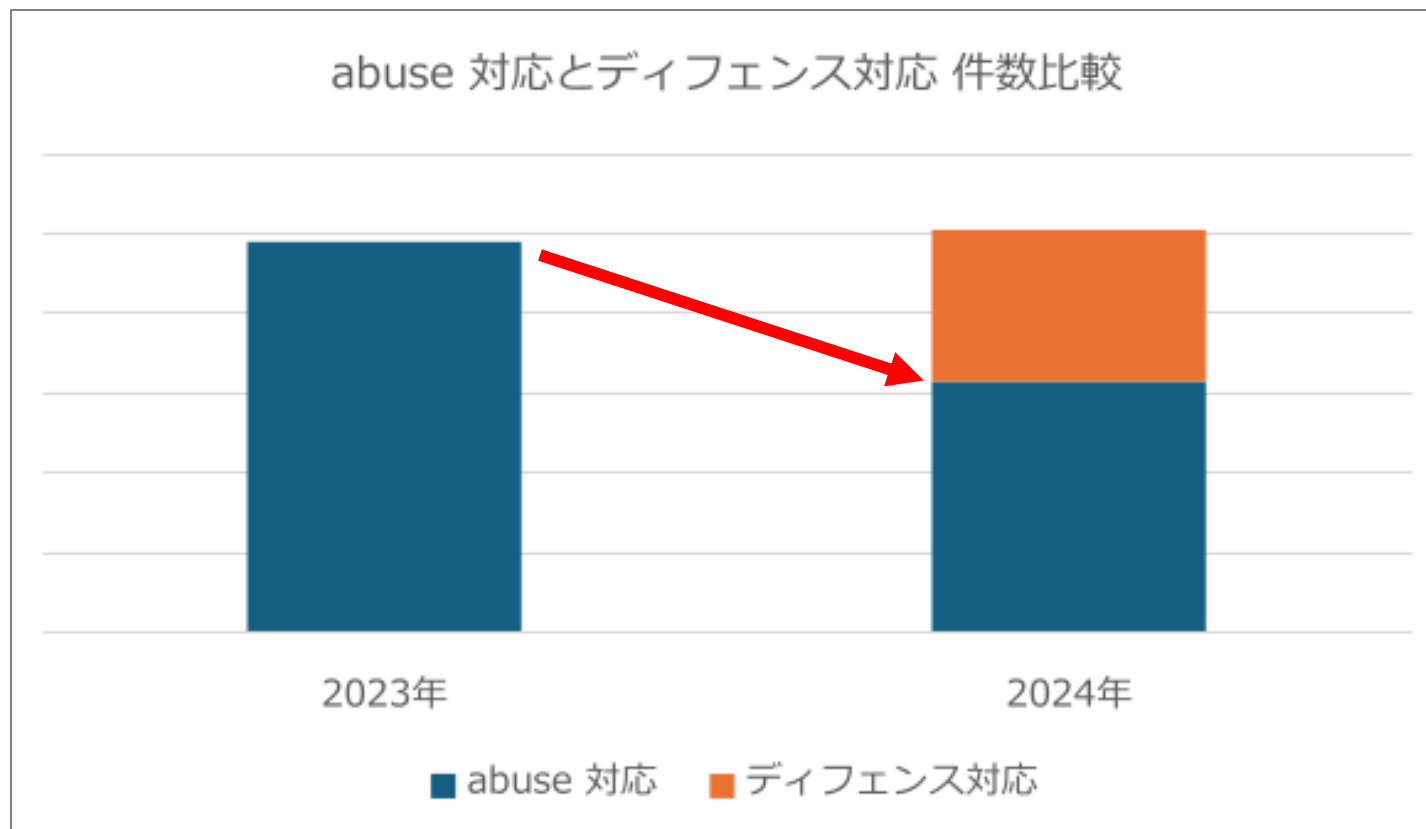


- 探索行為と思われる事象を検出したらアラート
- 24時間運用監視メンバーがログを調査
- 不審な通信であればディフェンス対応を実施



# IIJ の新しい取り組み 「ディフェンス対応」

「ディフェンス対応」によって、abuse 対応が 3割減



※ 集計期間 5月～10月 (2023年は同月の abuse 対応件数を集計)

abuse 対応を **30%**削減

サービス設備の過負荷障害や  
突発的な呼出対応の要因の排除

IIJ 発の迷惑メール **抑制**

ブロックリストへの登録回避

# IIJ の新しい取り組み 「ディフェンス対応」

## 運用を開始して半年、お客様からのクレームもなし

### ■ お客様の反応 (一部)



対象のアカウントは先月末に退職した者だった。  
念のため残していたが不要なので削除した。



転送にしか使っていないアカウントだった。  
消すことにした。



使い終わった契約が残ったままだった。  
解約したい。

(残念ながら契約を放置されるよりは健全)



IIJ からの通知を受けてパスワードを変更したが、その後、従業員が  
使っていない時間帯にログインを試み、失敗した形跡があった。



時系列 ▶

|                  |     |                  |
|------------------|-----|------------------|
| 00:00            | 悪   | 「おためし送信」         |
| 13:37            | IIJ | ディフェンス対応を実施・顧客通知 |
| 31:19 (1日 07:19) | 顧客  | パスワード変更          |
| 58:38 (2日 10:38) | 悪   | 不正ログインの記録 (失敗)   |



# まとめ

IIJ は高度化するサイバー攻撃から、お客様を保護する取り組みを続けてまいります



利用者のみなさまへ

事業者の仲間たちへ

不正利用の準備行為の発見  
前触れなくフィッシングメールを送るのではなく「おためし送信」

# STOP!

メールサービス A  
パスワード使いまわし!

※ 事業者から連絡を受けましたら適切な対応をお願いいたします

|                       |           |           |
|-----------------------|-----------|-----------|
| ij-haro@example.jp    | password1 | ij-haro   |
| ij-jiro@example.com   | password2 | ij-jiro   |
| ij-hanako@example.org | password3 | ij-hanako |

IIJ の新しい取り組み 「ディフェンス対応」  
「ディフェンス対応」 abuse 対応 3割削減

# FIGHT!

悪との戦いに終止符を!

一緒に連携していきましょう

abuse 対応を 30%削減  
脆弱性障害や脆弱性排除  
IIJ 発の迷惑メール抑制  
迷惑メールの登録回避

2023年 一緒に連携していきましょう

■ abuse 対応 ■ ディフェンス対応

※ 集計期間 5月～10月 (2023年は同月の abuse 対応件数を集計)

# IIR

Internet Infrastructure Review  
Jan.2024 Vol. 63

定期発行レポート  
日々高度化するサイバー攻撃からお客様を保護するための取り組み

フォーカス・トピック (1)  
W3C標準化活動 : RDF Dataset Canonicalization

フォーカス・トピック (2)  
IIJにおけるDRMの取り組み



IIJ IIR

検索

IIR vol.63でもお読みいただけます

<https://www.ij.ad.jp/dev/report/iir/063.html>

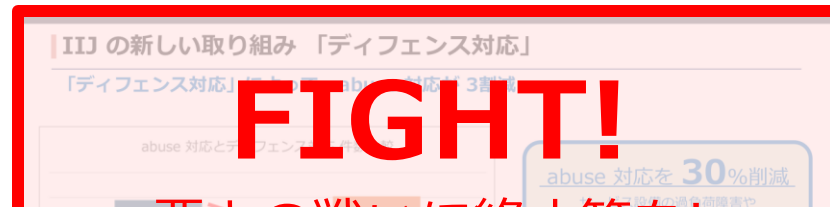
# まとめ

IIJ は高度化するサイバー攻撃から、お客様を保護する取り組みを続けてまいります



利用者のみなさまへ

事業者の仲間たちへ



一緒に働く仲間を募集中！

面白そうなことをしているな、高度な技術で社会貢献しているな、  
などIIJの取り組みに共感した方は、ぜひ一緒に働きましょう

➤ 採用情報は [こちら](https://www.iij.ad.jp/dev/report/iir/063.html)

<https://www.iij.ad.jp/dev/report/iir/063.html>

## 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

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。