D1-5 続・ドメイン名終活
～使い終わったドメイン名１年の観測分析から見えたリスクと対策～

2025年11月26日

NTTドコモビジネス株式会社

スピーカー紹介

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

NTTドコモビジネス

冨樫 良介　イノベーションセンター

セキュリティ技術研究・開発（攻撃インフラの脅威分析）

猪飼 人大　イノベーションセンター

セキュリティ技術研究・開発（攻撃インフラの脅威分析）

本講演の狙い

昨今、廃止したドメイン名が**ドロップキャッチ**され被害にあうケースが多発しています。

その被害を最小限に抑えるために
NTTドコモビジネスでは**利用終了したドメイン名を永年保有する方針**で運用を開始しました。

我々はこの利用終了ドメイン名の情報を中長期的に分析してきました。
本講演では約一年**ドメイン名の「使後の世界」を覗き見ることで得られた内容を共有します。**

施策の背景

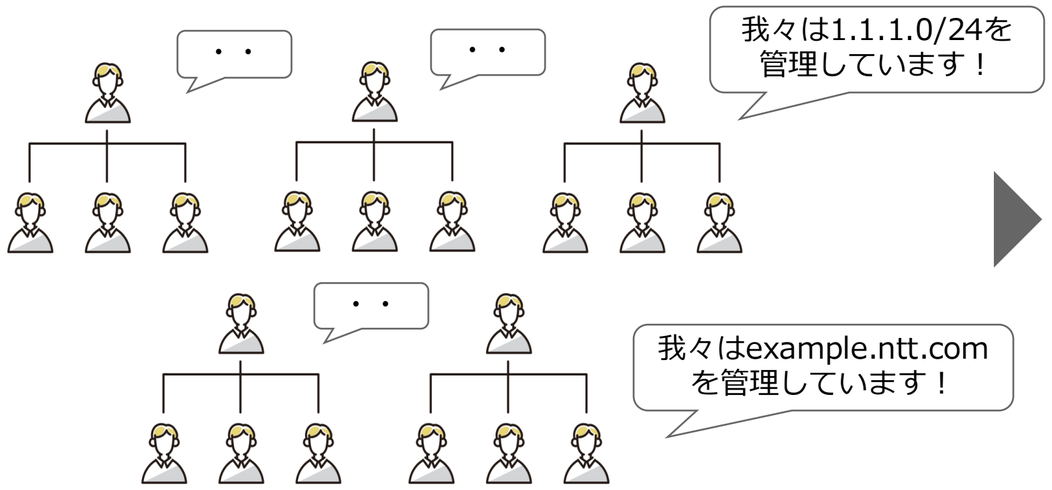
ComNIC設立の背景

ComNICとは

社内のAS番号、IPアドレス、ドメイン名などネットワーク資源を一元管理する組織。以下三つの役割を持つ。

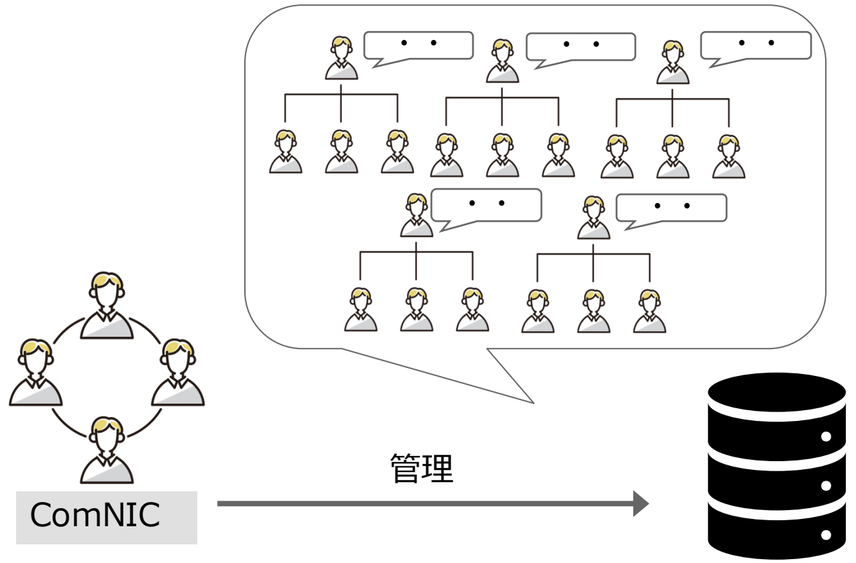
- 管理ポリシー・運用ガイドライン等の策定および社内浸透
- 運用体制・運用フローの整備および運用
- 保有資源ごとの利用状況・利用者情報の一元管理と最新化

ComNIC設立以前



各組織で管理していたため、情報を一元的に見る手段がない
=インシデントが起こった際に被害範囲を特定するのにすごく
時間がかかる

ComNIC設立後



ComNICが情報を一元管理する主体に
誰が (どの組織が) 管理しているかわかる状態に

ドメイン名廃止時の危険性

企業のサービスなどで使われていたドメイン名には価値がある！
- 利用終了したドメイン名がオークションにかけられて高値で売買されたり
- (*)ドロップキャッチにより第三者に悪用されたり
- 簡単に手放すことができない状態になっている

(*)再登録が可能になる瞬間を狙って、 目的のドメイン名を登録しようとする行為
インターネット用語1分解説～ドロップキャッチとは～ - JPNIC

なぜ「ドコモ口座」のドメインがオークションに？ ドコモの見解は（山口健太） - エキスパート - Yahoo!ニュース

【注意喚起】セキュリティリスク回避のため、旧Visionalistをご利用いただいていた法人のお客さまにおける“tracer.jp”タグ削除のお願い

ドメイン名のドロップキャッチによる被害対策
- ✓独自ドメイン名ではなく、ntt.comサブドメイン名の利用促進
- ✓退職者/異動者の定期的な確認 (管理情報の最新化)
- ✓**永年保有ポリシーの策定**

永年保有の課題
ドメイン名の維持料
ドメイン名の健全的な利用への悪影響

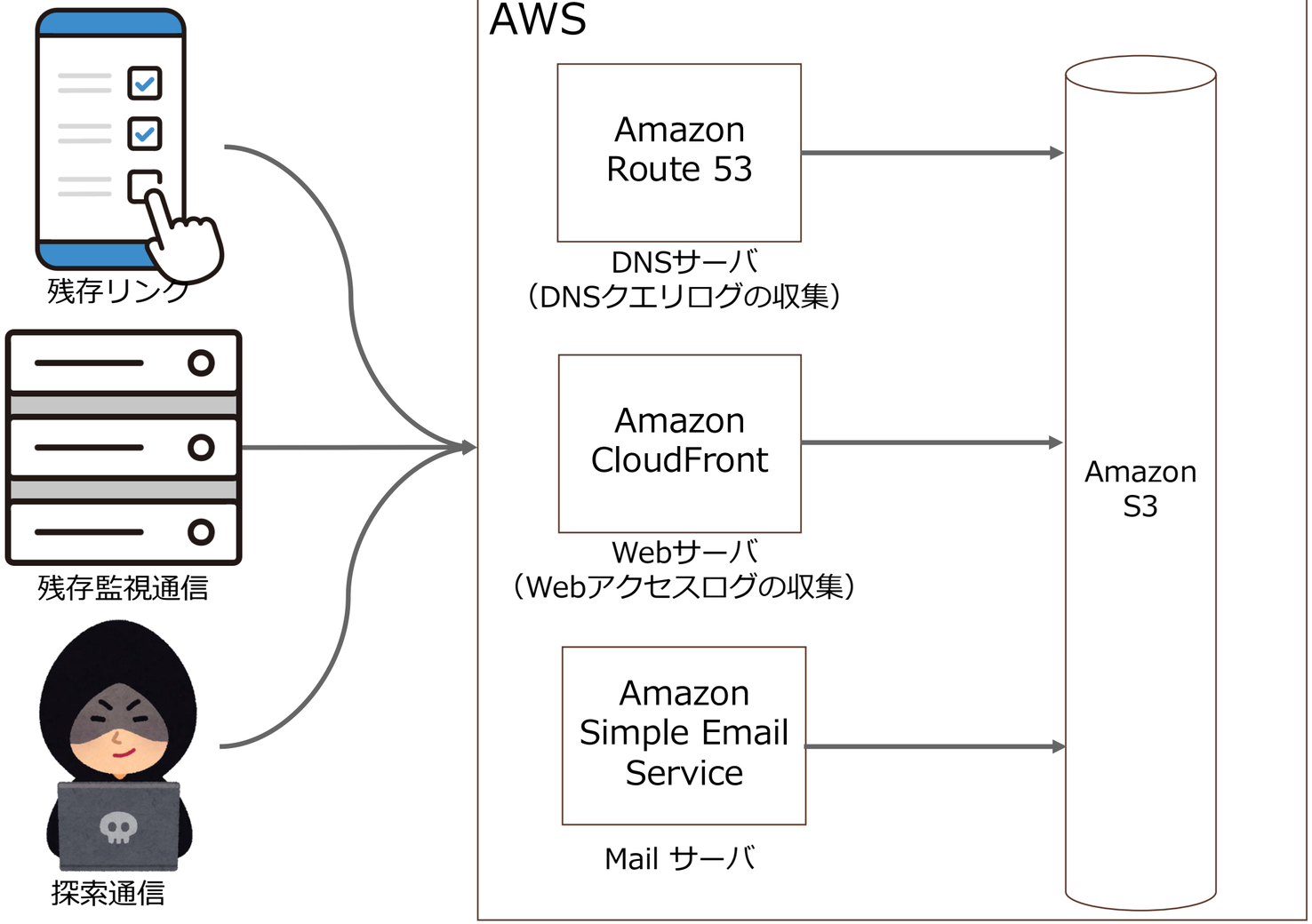
利用終了したドメイン名へのアクセスログとDNSクエリ、メールを監視する基盤を運用中

ログ収集環境

システム構成

想定される送信元

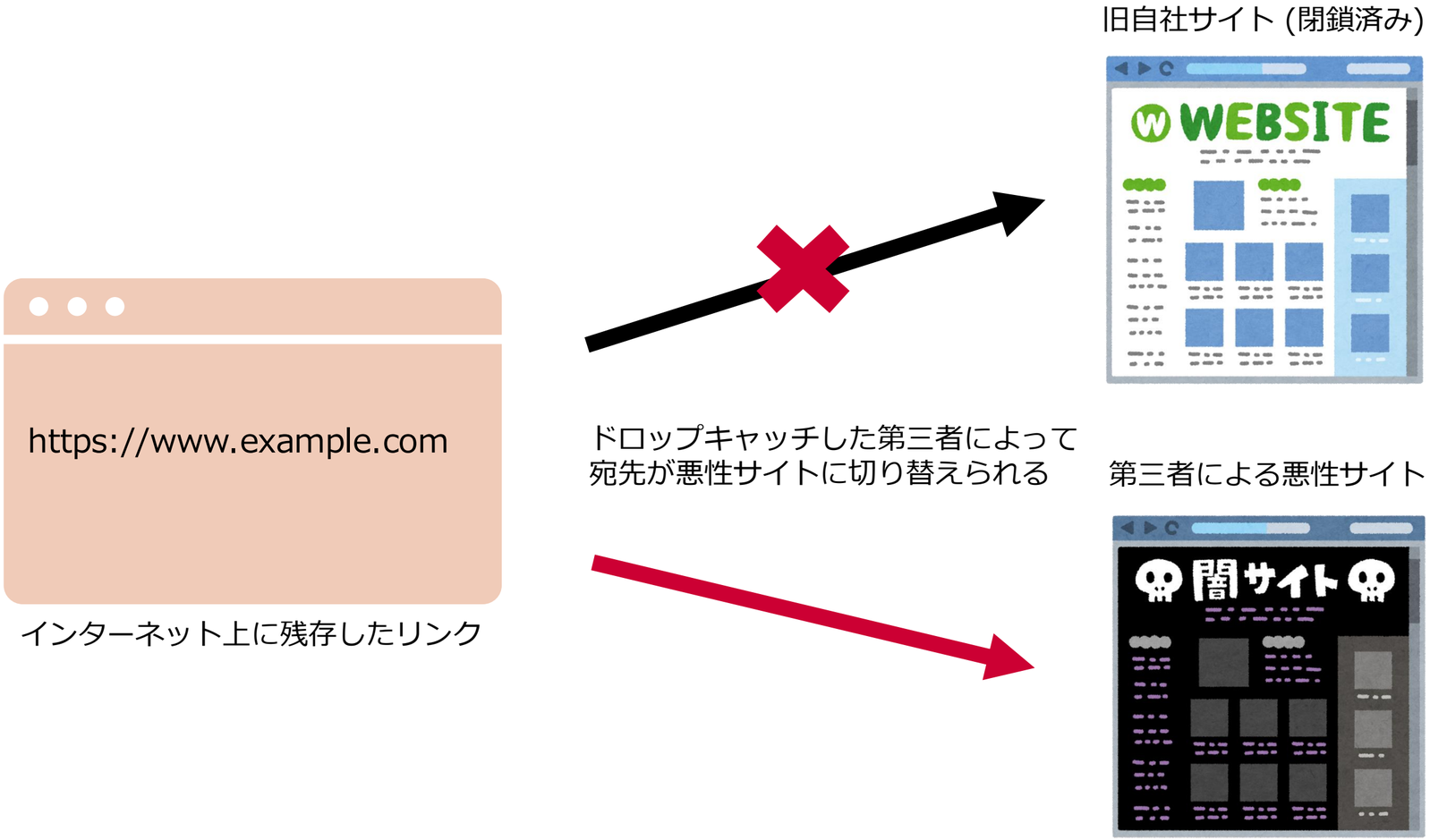
観測



ウェブアクセスログの中長期分析

残存訪問者によるリスク

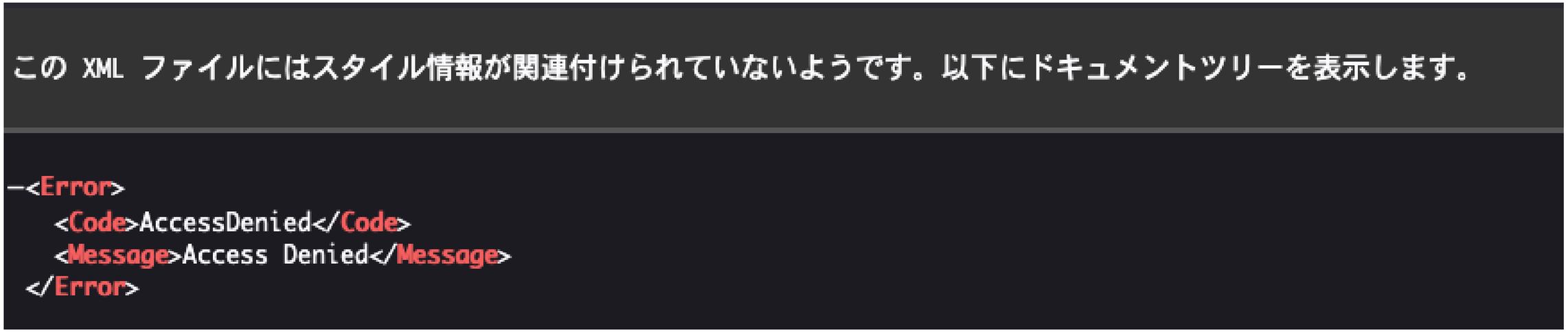
- 弊社ではドメイン名の永年保有をしているが、その理由の 1 つがドロップキャッチした第三者に新規のサイトを作成され、企業のレピュテーションに悪影響が出ることへの懸念
- 例えばインターネット上には旧自社サイトへのリンクが残っていた場合、そこから第三者が作成したサイトに訪問者が誘導されることになる



残存訪問者を把握する必要性

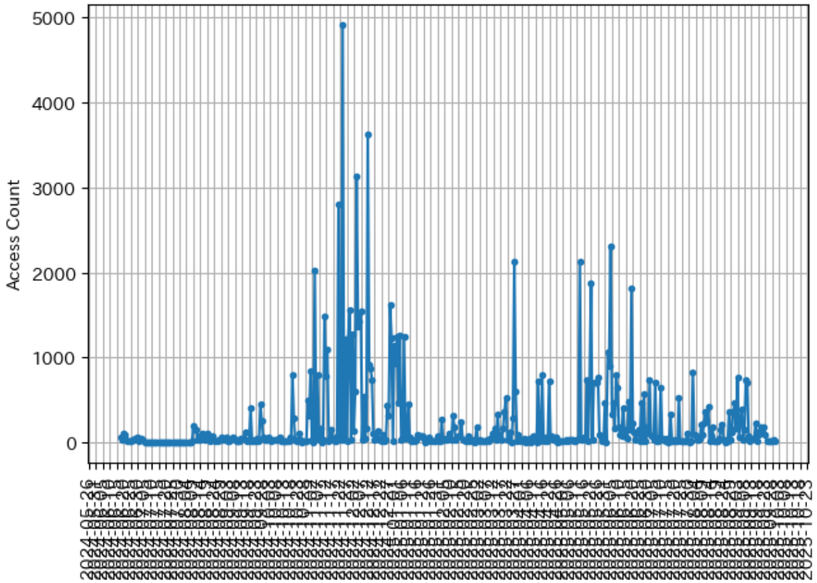
- 「残存訪問者」の数が多いほど、ドメイン名廃止によるリスクは高まる
- ドメイン名廃止によるリスクを見積もるため、下記を把握したい
  - 現在の残存訪問者の数
  - 残存訪問者数の変化

- 弊社の利用終了ドメイン名ではサイトが閉鎖されたことを示すページを表示しており、
  この環境でウェブアクセスログを収集している

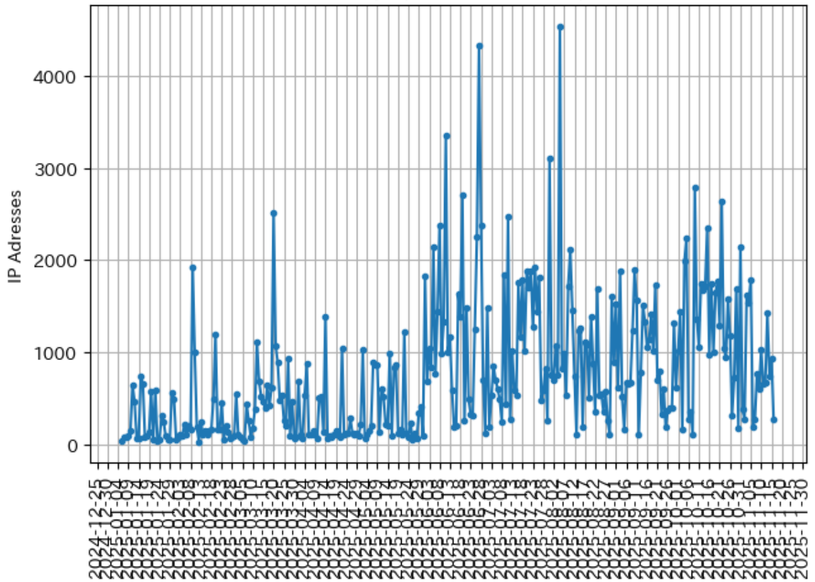


ウェブアクセスログのノイズ

- 残存訪問者の数を調査するために、継続的にウェブアクセスログを収集したが…



ウェブサイトに利用していたドメイン名におけるアクセス数
アクセス数 (中央値)：527



商標保護を目的とした使用実績がないドメイン名におけるアクセス数
アクセス数 (中央値)：930

- 既にサイトが閉鎖されたにも関わらず、アクセス数が多すぎるように見える
- また、ウェブサイトでの使用実績がないドメイン名においても、大量のアクセスが観測されている

➔ これらのアクセスの大部分は人間による訪問ではない可能性

- 「残存訪問者」の数を見積もるためには、人間以外によるアクセス (ノイズ) を除去する必要がある

User-Agent に基づくノイズ判定

各社が運用するボット、クローラは User-Agent に身元と意図を示している場合がある

- Google のクローラー

Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"

- Palo Alto のボット

"Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers' presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com"

- Censys のボット

"Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)"

-> User-Agent 中にボットまたはクローラーであることが明示されたアクセスは **全体の 4%** ほど

reverse-ip に基づくノイズ判定

各社が運用するボット、クローラは IP アドレスの逆引きにも身元・意図を示している場合がある

- スタンフォード大の研究調査

research.esrg.stanford.edu

- パダーボルン大の研究調査

syssec-scanner6.cs.uni-paderborn.de

ただし、reverse-ip からノイズ判定ができた事例は全体のごくわずか

パスに基づくノイズ判定

- ウェブアクセスログから訪問者が指定したパスを確認できる
- このパスを確認することで何らかの意図をもったスキャン活動を抽出することができた

- **脆弱性スキャナー**
  - ウェブシェル/バックドア/管理ツールのファイル名を含むパスへのアクセス
    - "wp-config.php"、"config.php" などの機微情報が含まれるファイル
    - "c99", "r57", "b374k", "alfa" などの有名な悪性ファイル
      - 存在した場合には、攻撃者はこれらの webshell を動作させると考えられる
  - **アクセス全体の 42%** が該当

- **API エンドポイントスキャナー**
  - アクセス先が api endpoint であることを想定して、機微情報を調査するためのアクセス
    - "api-docs", "graphql"、"swagger.json" など
  - **アクセス全体の 34%** が該当

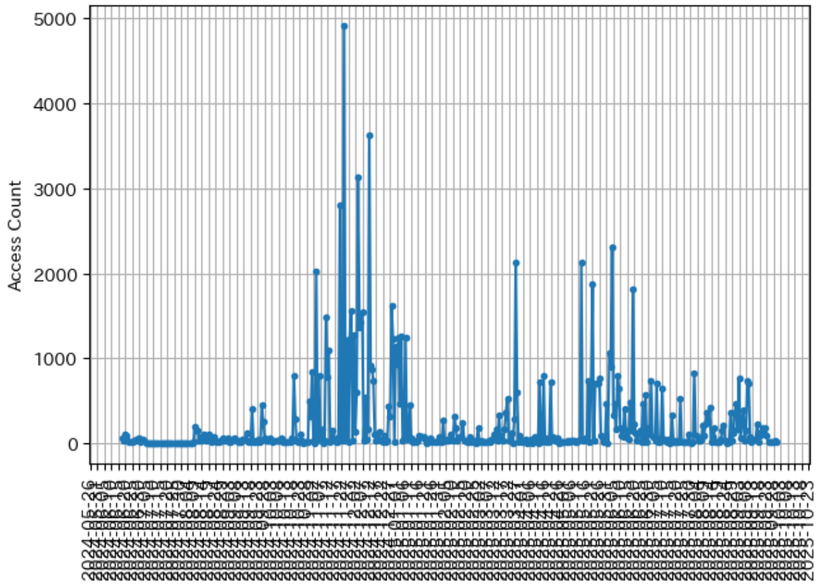
商標保護を目的としたドメイン名を活用した事例

- 既存サービスと似た名前のドメイン名が第三者に取得されることを防止する意図
- これらのドメイン名がWebサイトとして使用された実績は一切ないため、これらへの送信元は機械的な情報取得を目的としたボット、クローラー、スキャナなどに該当する可能性が高い

- 少なくともこれらの送信元については一般的な訪問者とは考えられないため、送信元　IP アドレスをノイズ判定に利用した
    - ただし、それらの中に各種プロキシ、VPN サービスの IP アドレスが含まれており、これらについては一般利用者が同一 IP アドレスを使用していることは起こり得る
    - そのため、外部サービスを使用して IP アドレスがプロキシ、VPN サービスに該当するか確認し、該当したものはノイズとはしなかった

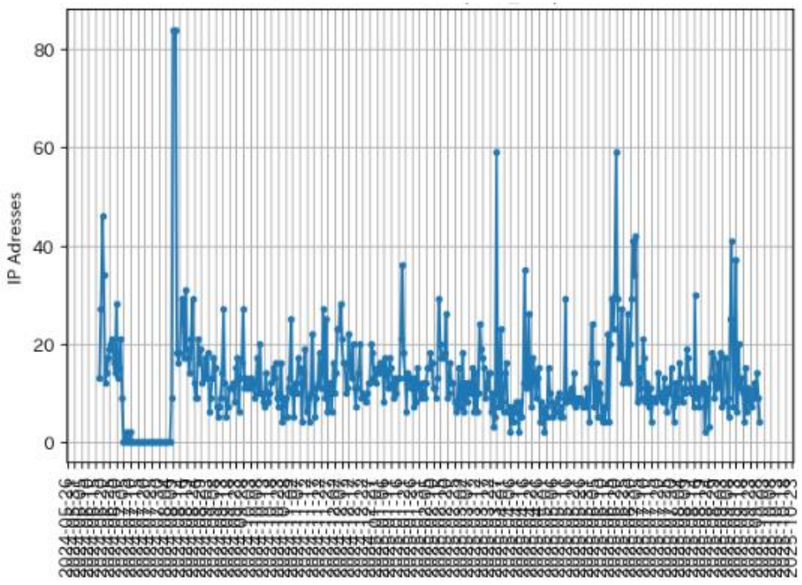
より実態に近い残存訪問者を推計するために

- ドロップキャッチ後のドメイン名悪用による企業のレピュテーションへの影響を考えたとき、クリティカルになるのは**「未だに残存するアクセス数」ではなく「残存訪問者の数」**
- より実態に近い「残存訪問者」の数を推計するために、アクセス元の IP アドレスを日付ごとにユニーク化する処理を行った
  (日付ごとに同一の IP アドレスから複数のアクセスがあった場合に 1 件に丸める処理)
  - これについては排除しきれなかったノイズの影響を最小化する狙いもある



アクセス数 (中央値)：527

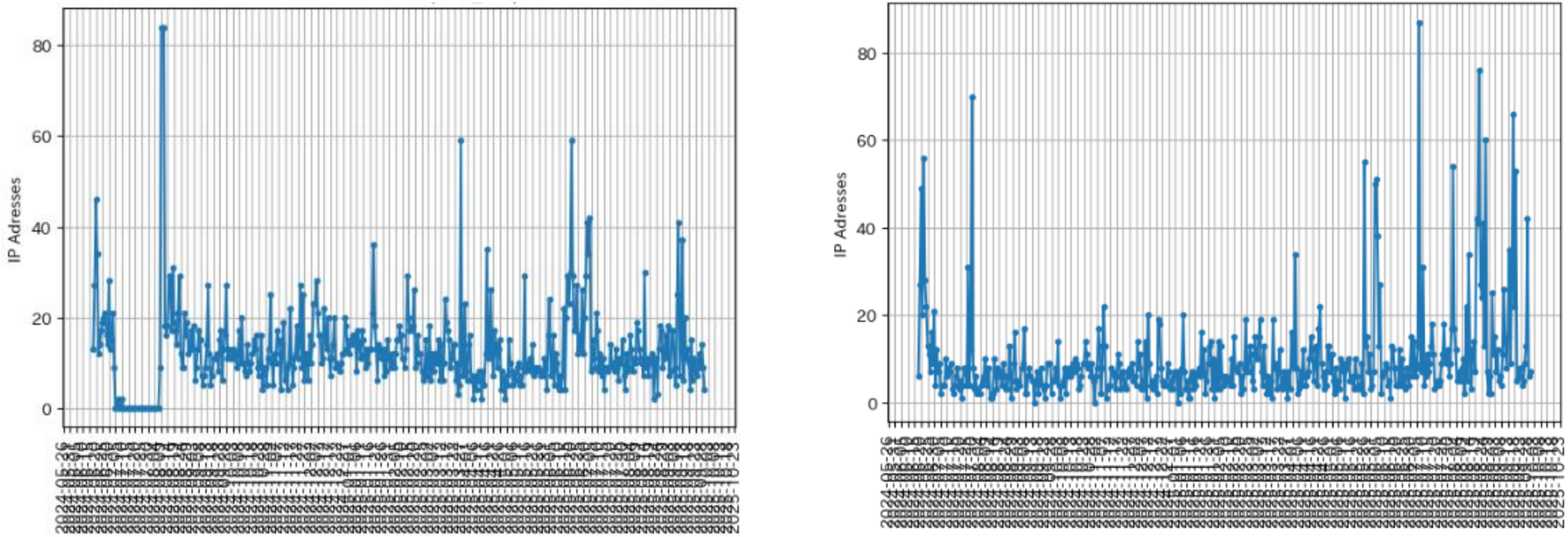
ノイズ除去 & IP ユニーク化



訪問者数 (中央値)：9

残存訪問者数の推移

- 多くのドメイン名において残存訪問者の有意な減少傾向は確認されなかった
- 監視を開始した時点ですでにアクセス数は減少傾向は止まり、収束していた可能性
- 一方、例えば大規模なウェブサイトなどでは減少傾向が長く続く可能性があり、ドメイン名の元々の使用用途に依存すると考える



ウェブサイトに使用していた各ドメイン名における残存訪問者数

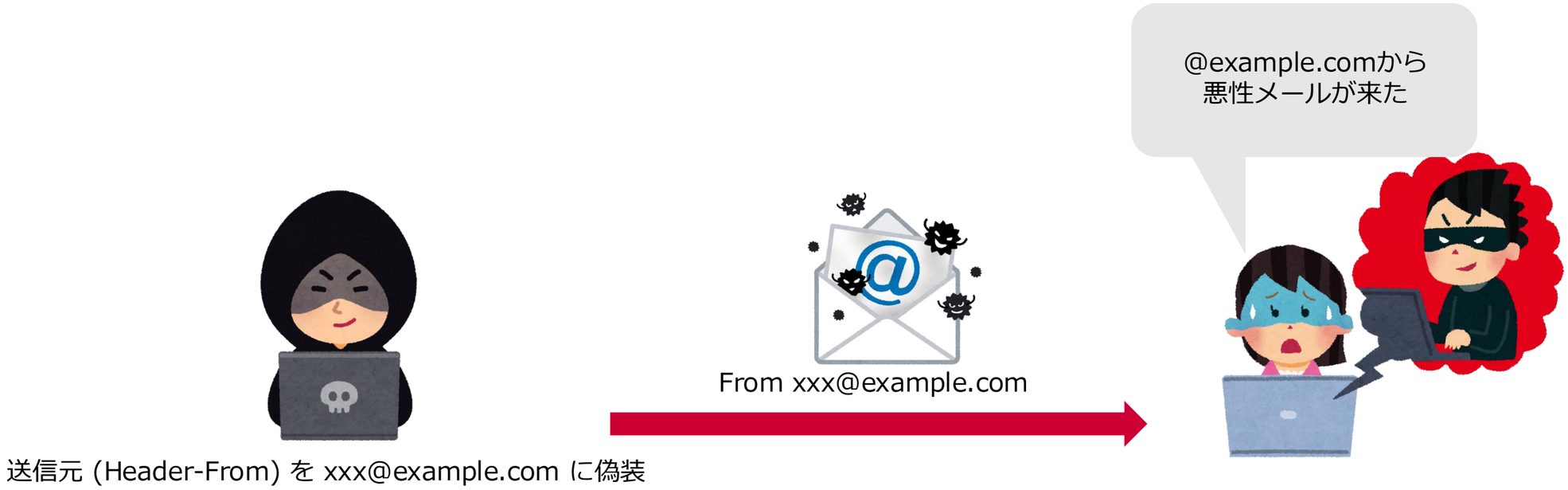
ウェブアクセスログの中長期分析

- 純粋なウェブアクセスログには少なくとも 80% 程度のノイズ (スキャナなど) が含まれる
- ノイズを除去しないと残存訪問者の人数を推計することも、減少傾向 (あったとしても) 把握することはむずかしい

DMARC Report の中長期分析

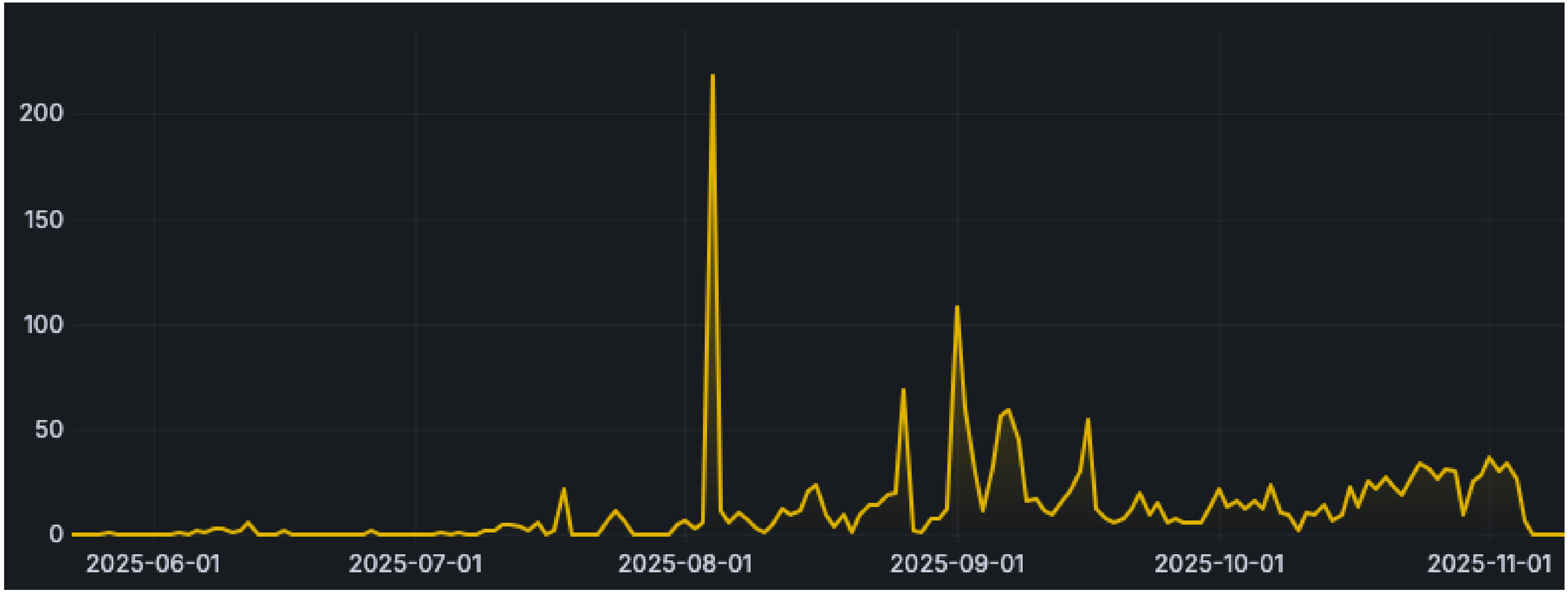
偽装メールのリスク

- ドメイン名の廃止には様々なリスクがつきまとうが、偽装メールもそのうちの 1 つ
- 攻撃者は Header-From を書き換えればよいだけなので、偽装メールを送信するだけなら難しくない
- 我々は各種 DNS レコードを設定することで偽装メールの受信防止と DMARC Report の収集をしている
- 収集した DMARC Report から**利用終了ドメイン名においても、偽装メールの送信元として詐称**されていることを確認している



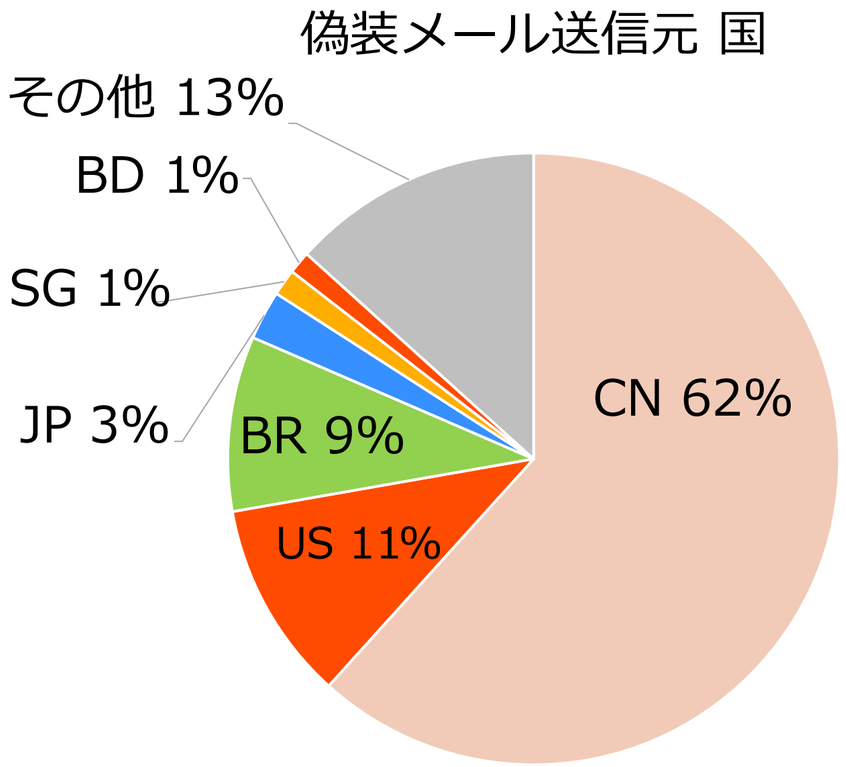
観測した偽装メール 件数

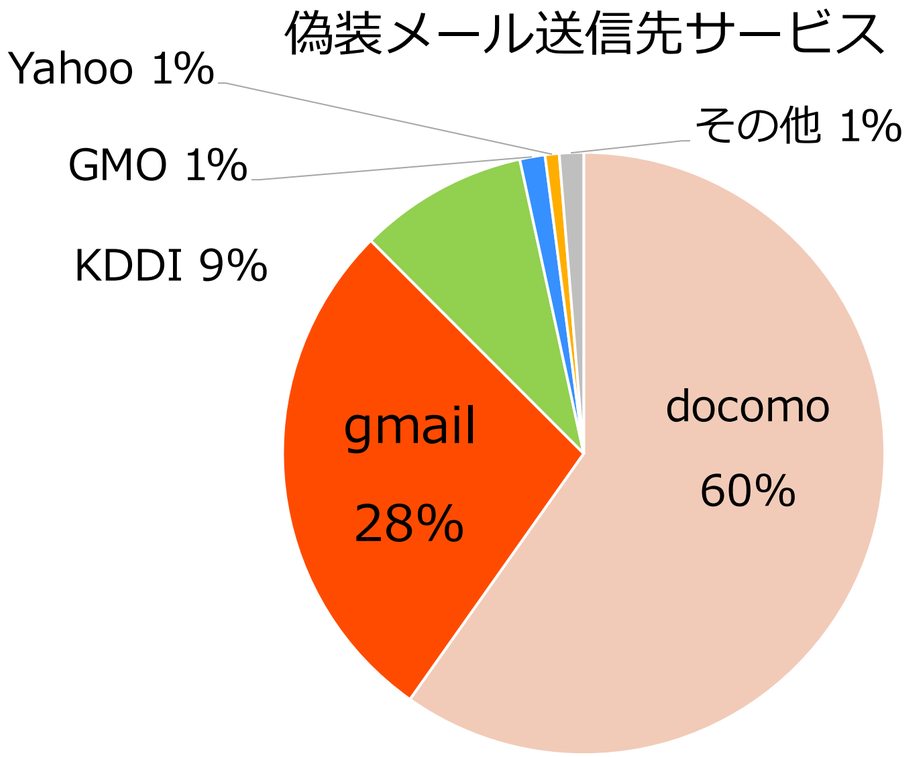
- 観測期間：2025 年 6 月 ~ 11 月上旬
- 対象としたドメイン名の数：149 個 (そのうち 60 個で偽装メールの存在を確認)
- 偽装メール総数：2083 件



偽装メールの統計情報

- 偽装メール総数 (2025/06 ~ 10)：2083 件
- 偽装メールの送信元の半数以上が中国
- 偽装メールの宛先の半数以上がドコモ





DNS レコード

各種 DNS レコードを設定しており、
自社の利用終了ドメイン名を騙ったメールの対策と DMARC レポートの収集をしている

- DMARC: *"v=DMARC1; p=reject; aspf=s; rua=mailto:rua@example.com; ruf=mailto:ruf@example.com"*

SPFの認証に失敗したメールの受取を拒否することを推奨するポリシー
指定したメールアドレス宛にレポート (RUA と RUF) の送信を依頼

- SPF: *"v=spf1 -all"*

あらゆる送信元 IP アドレスからのメールを不正メールとして処理する

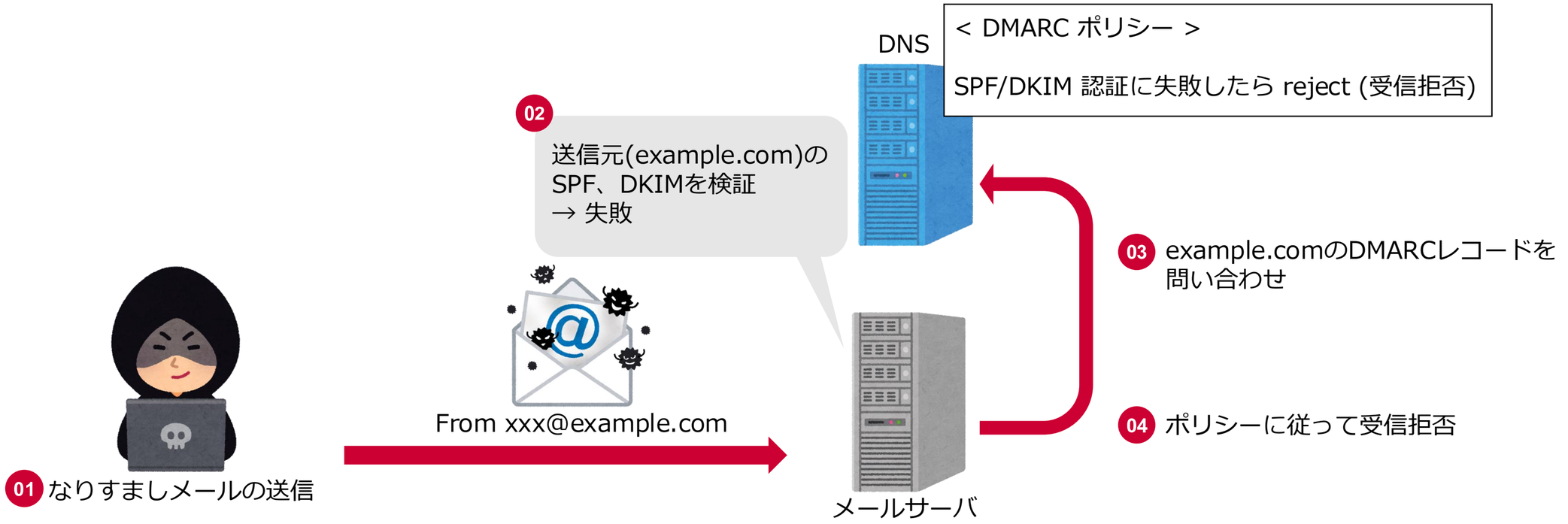
- MX: *0 .*

レコードが設定されたドメイン名でメールの受信をしないことを明示している

- ドメイン名がドロップキャッチされた場合偽装メールが受信される可能性が高まる

DMARC 認証

- 受信者は公開された DMARC レコードからそのメールの SPF、DKIM 認証に失敗したときに、メールをどのように扱うべきか判断する



DMARC 認証

- SPF 認証で使用する Envelope-From と DKIM 認証で使用する DKIM Signature がそれぞれ、Header-From と一致しているか確認し、不整合があった場合にはポリシーに従って対応する

Return-Path: <hoge@malicious.example.net>

...

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d= malicious.example.net; s=selector1; ...

...

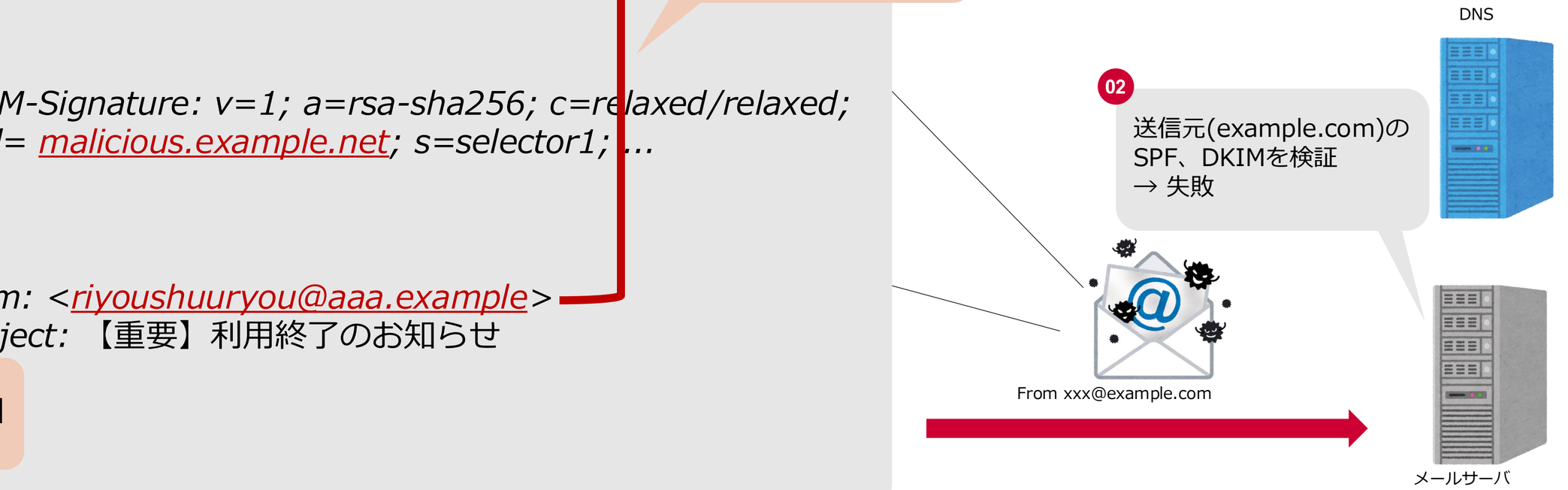
From: <riyoushuuryou@aaa.example>
Subject: 【重要】利用終了のお知らせ

SPF Aligned Fail

DKIM Aligned Fail

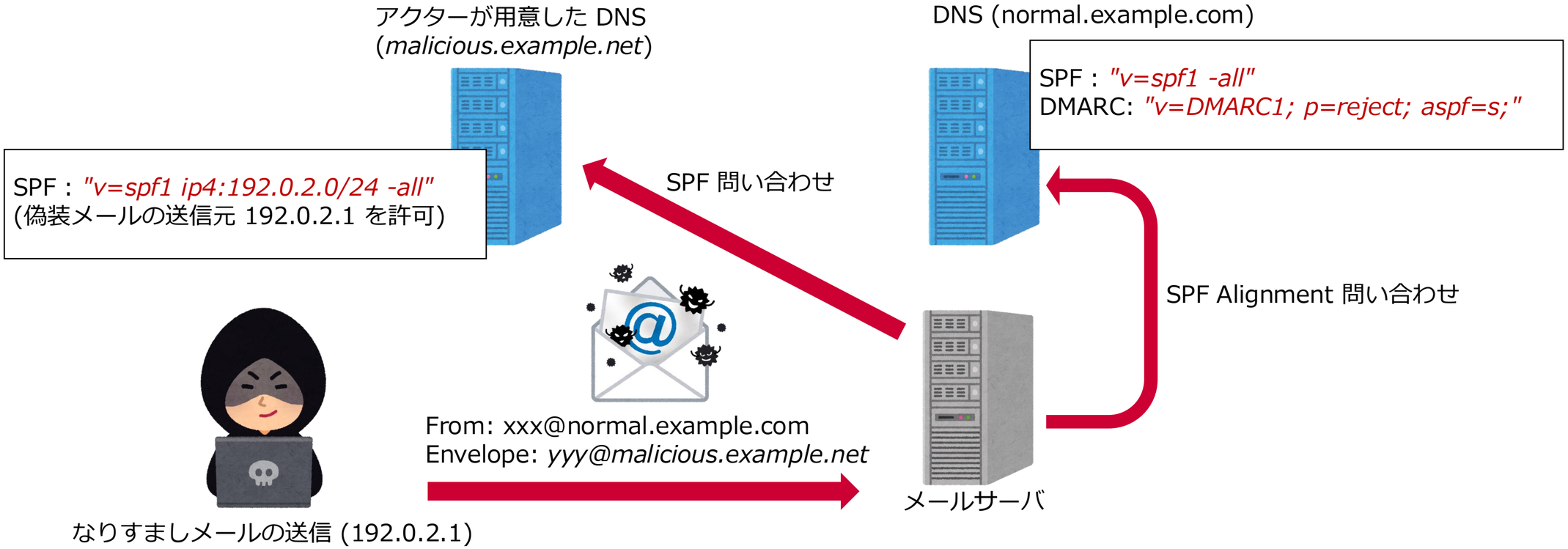
< DMARC ポリシー >

SPF/DKIM 認証に失敗したら reject (受信拒否)



SPF、DKIM Pass 事例

- SPF: *"v=spf1 -all"* が設定してあるにも関わらず、SPF がパスする事例が散見された
  - SPF で検証されるのは Header-From ではなく Envelope-From
  - 攻撃者は Header-From を利用終了ドメイン名にして、Envelope-From に攻撃者が用意したドメイン名を入れる
  - 攻撃者は Envelope-From の SPF レコードで送信元 IP アドレスを許可している



- つまり SPF 単体ではバイパスする手法があるため、対応するには DMARC レコードを設定しアライメントを検証させる必要がある (2083 件中 274 件で SPF がパスした)

結局どんなドメイン名が狙われる？

- 利用終了ドメイン名の元々の用途ごとに偽装メールに悪用されたドメイン名の数を集計した

用途	悪用されたドメイン名の数	比率
元コーポレートドメイン	1 個 (全 2 個)	50.0 %
元ウェブサイト	4 個 (全 8 個)	50.0 %
商標保護	51 個 (全 127 個)	40.1 %
元メール用	2 個 (全 6 個)	33.3 %

- 用途による悪用発生率に有意な差は見られなかった

結局どんなドメイン名が狙われる？

- 利用終了ドメイン名の TLD ごとに偽装メールに悪用されたドメイン名の数を集計した

TLD	悪用されたドメイン名の数	比率
.jp	56 個 (全 127 個)	44.1 %
.com	4 個 (全 15 個)	26.7 %
.dev	0 個 (全 1 個)	0.0 %
.net	0 個 (全 2 個)	0.0 %
.app	0 個 (全 1 個)	0.0 %
.tel	0 個 (全 1 個)	0.0 %
.org	0 個 (全 1 個)	0.0 %
.biz	0 個 (全 1 個)	0.0 %

- TLD が .jp のドメイン名については詐称元に利用されやすいという結果になった

結局どんなドメイン名が狙われる？

- 詐称に多く利用されたドメイン名には一般的な認知度があるフレーズが含まれることが多かった
- 逆に国際化ドメインは極端に少なかった

ドメイン名 (すべて .jp)	用途	特徴	件数
aaa.example	商標保護	通信に関連する用語	415
bbb.example	元ウェブサイト	弊社提供サービスでの利用	281
ccc.example	元コーポレートドメイン	弊社関連会社の名前を含む	280
ddd.example	商標保護	弊社関連のスポーツチームを想起する	248
eee.example	元ウェブサイト	弊社提供サービスでの利用	174
fff.example	商標保護	一般的な用語の組み合わせ	173

結局どんなドメイン名が狙われる？

- TLD が .jp のドメイン名が詐称に悪用される傾向にあった
- 認知度があるフレーズが含まれる (意味が通りやすい) ドメイン名は詐称に悪用される傾向にあった

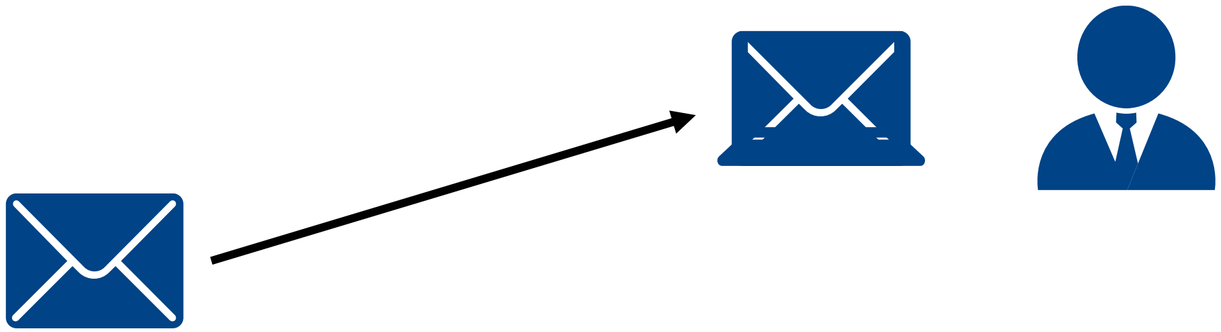
➔ 偽装メールに悪用されやすい特徴を持つドメイン名は攻撃者にとって価値が高い可能性があり、廃止のリスクが高い

➔ 運用時においても、SPF、DMARC レコードを登録することで偽装メールに対処することが好ましい

メール分析

メール分析

- メールアドレスとして使用されていたドメイン名を手放した際のリスクを調査・分析



旧メールアドレス用ドメイン名
old.example

新メールアドレス用ドメイン名
new.example

メール分析

- メールアドレスとして使用されていたドメイン名を手放した際のリスクを調査・分析
  - 重要なメールが届いている状態でドメイン名を手放すとドロップキャッチにより受信される可能性

メール分析

- メールアドレスとして使用されていたドメイン名を廃止した際のリスクを調査・分析
  - 重要なメールが届いている状態でドメイン名を廃止するとドロップキャッチにより受信される可能性

⇨ ドメイン名を廃止する際は受信しているメール考慮する必要

- 複数の利用終了後のドメイン名を分析
  - 受信したメールの分類
  - 業務上重要なメールを受信するか
  - メール用ドメイン名の廃止について

対象としたドメイン名

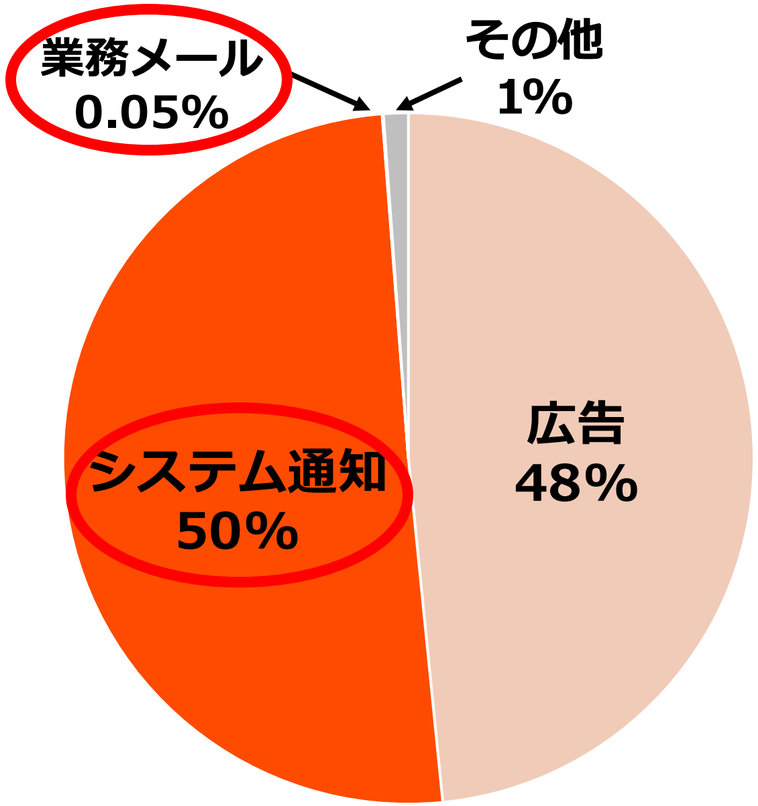
- 観測ドメイン名　：7個
- 観測期間　　：～ 2025/9/30

ドメイン名	元々の用途	メール数 (件)	観測期間
aaa.example	コーポレートドメイン名	109,694	9ヶ月
bbb.example		436	3ヶ月
ccc.example	運用担当者用	2,493	9ヶ月
ddd.example		1,507	9ヶ月
eee.example	ヘルプデスク用	286	5ヶ月
fff.example	機能検証	3	5ヶ月
ggg.example		0	8ヶ月

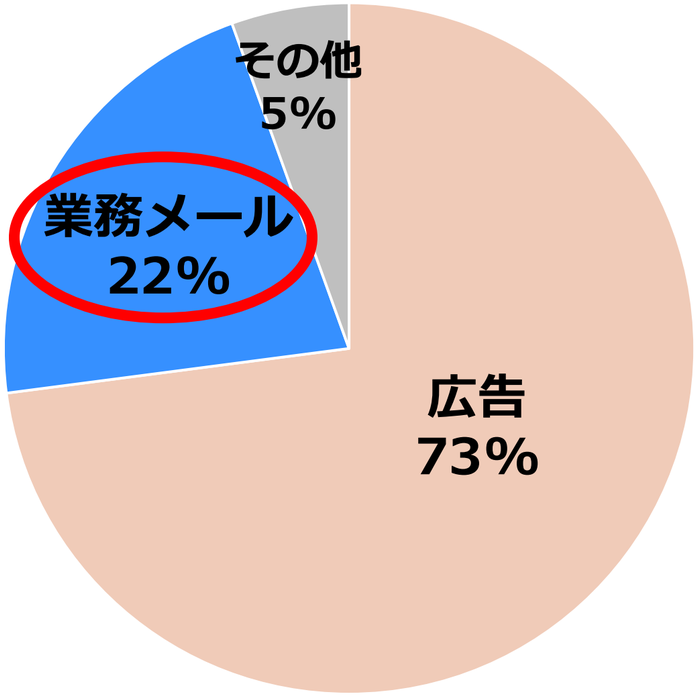
メール分類結果 コーポレートドメイン名

・顧客情報・業務情報を含むメールを受信している

aaa.example
合計：109,694件



bbb.example
合計：1,507件



広告
・広告・宣伝目的のメール

システム通知
・業務で使用していたシステムからの通知

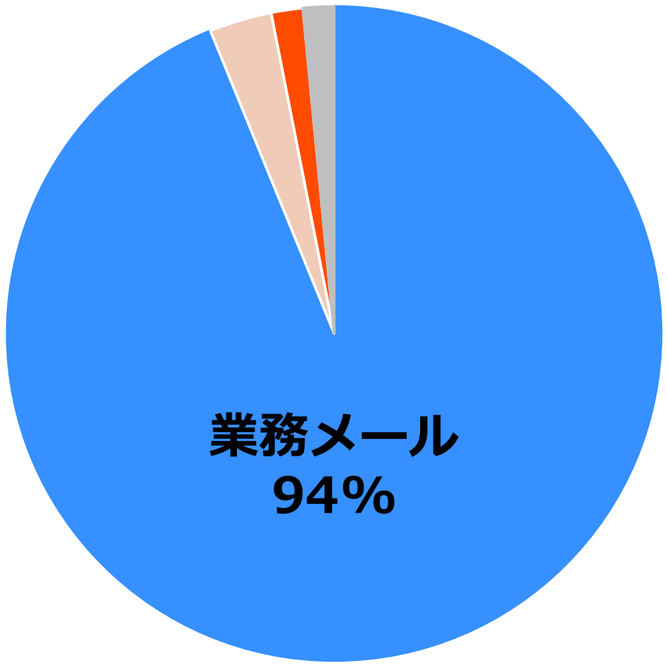
業務メール
・社内外の人物・部署からの業務メール

その他
・フィッシング・スパムメールなど

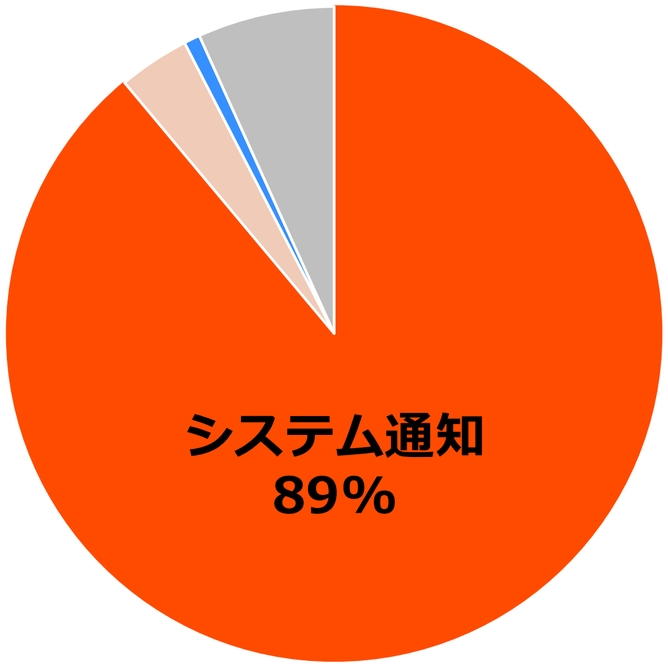
メール分類結果 運用・ヘルプデスク向け

・業務メール・システム通知を受信
・今回の観測対象は、監視通知や定期的な報告が受信メールの大半を占める

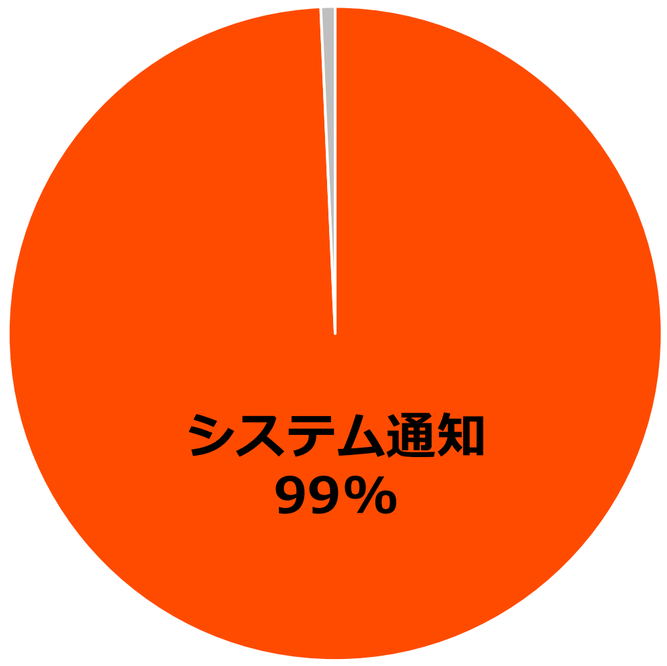
ccc.example
合計: 2,493件
用途: 運用担当者用



ddd.example
合計: 436件
用途: 運用担当者用



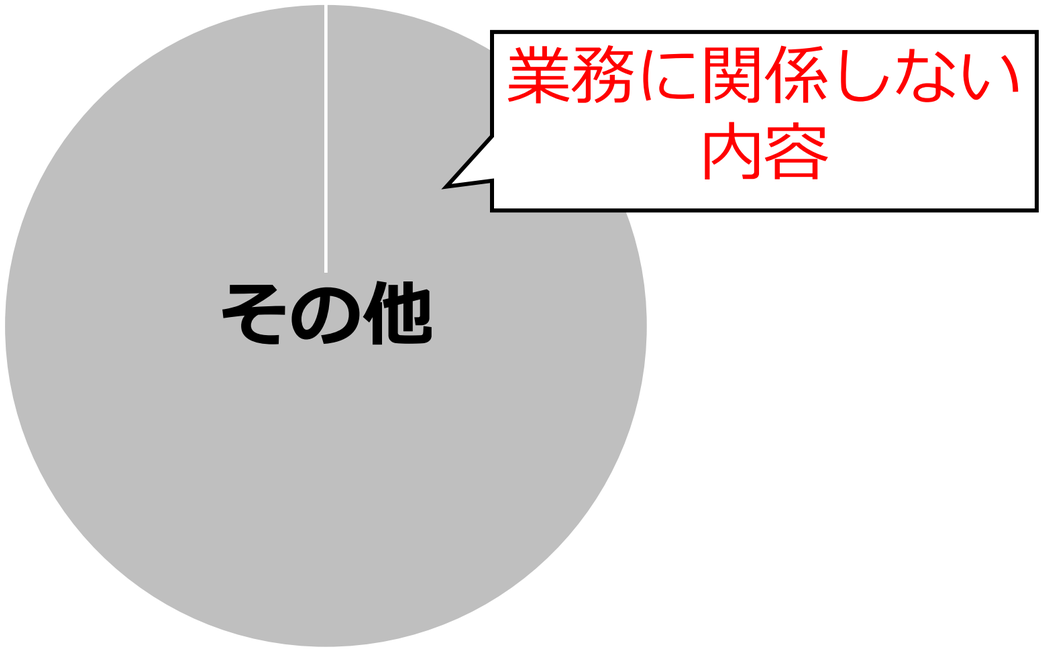
eee.example
合計: 286件
用途: ヘルプデスク用



メール分類結果 機能検証

・用途が機能検証であり、現在はメールをほぼ受信していない

fff.example
合計：3件
機能検証



ggg.example
合計：0件
機能検証

業務上重要なメールは受信するか

結論：受信する (特に元コーポレートドメイン名)

- コーポレートドメイン名
  - **aaa.example**
    - 顧客情報が記載されたシステムメール
    - 顧客企業との業務内容を含むやり取り
  - **bbb.example**
    - 経営層宛てのメール

当時の作業関係者として
追加された可能性

- 運用向け・ヘルプデスク用ドメイン名
- コーポレートドメイン名ほど重要な内容は受信していない
  - 社内向けの業務内容を含むやり取り
  - 過去使用していたシステムからのメール

業務上重要なメールは受信するか

- 今回の観測結果は、あくまで一例
  - メールを受信し続けているドメイン名は存在
- 利用終了して数カ月～数年経過しても受信
  - 社内外の人物から To / CC / BCC に指定され受信
  - 当時連携していたシステムから受信

メール用ドメイン名の廃止について

実運用でメールに使用していたドメイン名は廃止が難しい

- 「人」 or 「システム」からメールが届く
- **人が送信**：内容・タイミングの予測が困難
  - 利用終了後でも、現在進行形の業務内容を受信する
  - 突然、当時の関係者として送信先に追加される
- **システムが送信**：内容・タイミングの予測は比較的容易
  - 特定の送信元からフォーマットに従ったメールを受信する
  - 送信元・送信トリガー・通知内容を把握できる

⇨ システムからの受信停止は可能だが、人から届く可能性を捨てきれない

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
NTT docomo Business

まとめ

まとめ

- ウェブアクセスログの中長期的な分析を行った
  - ドメイン名廃止時のリスクを見積もるためには「残存訪問者」の数を把握する必要がある
  - ウェブアクセスログには大量のノイズ (スキャナ等) が含まれているため、残存訪問者の数を推計するためにはそれらを取り除く必要があり、その手法を共有した
- 収集した DMARC Report の分析を行った
  - 偽装メールに利用されるドメイン名の傾向を確認した
- 利用終了後のドメイン名に届くメールの分析を行った
  - 業務上重要なメールを、利用終了後でも受信しているドメイン名の存在を確認した
  - 人が送信するメールは、タイミングや内容の予測が困難である
  - 実運用でメールに使用していたドメイン名は、人からの受信が考えられるため廃止が難しいのではないか