使後の世界
～利用終了した独自ドメインのその後～

NTTコミュニケーションズ
森山 美保　平木 康介　冨樫 良介

スピーカー紹介

NTTコミュニケーションズ

森山 美保　情報セキュリティ部

社内ネットワーク資源管理 (ComNIC)、セキュリティツール運用

平木 康介　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）

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）

本講演の狙い

昨今、廃止したドメインが**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コミュニケーションズでは**利用終了したドメインを永年保有する方針**で運用を開始しました。

ただ、
一組織が使用していないドメインを保有し続けることは**インターネットの健全性**に悪影響を及ぼす可能性があります。

われわれは
ドメインの「使後の世界」を覗き見ることで得られた、
利用終了ドメインとの付き合い方を皆さんに共有します。

施策の背景

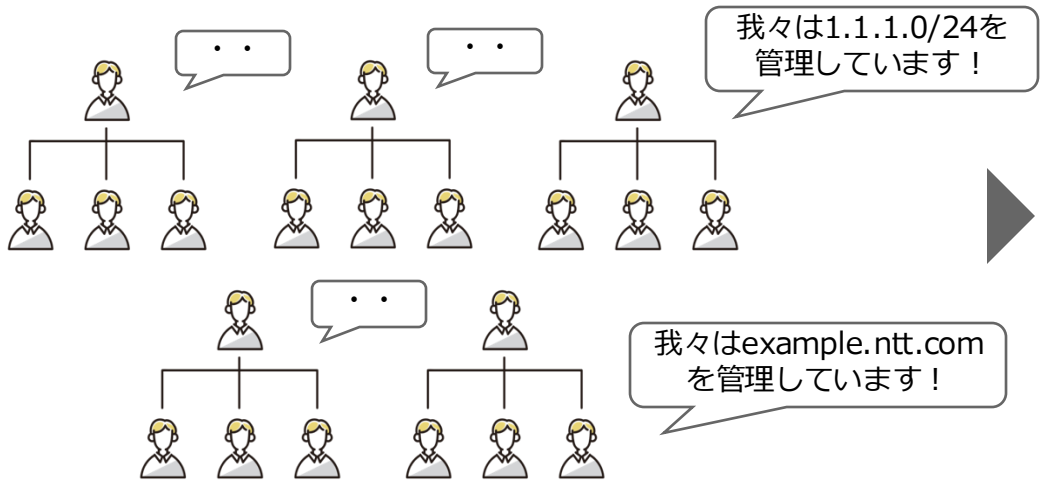
ComNIC設立の背景

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。

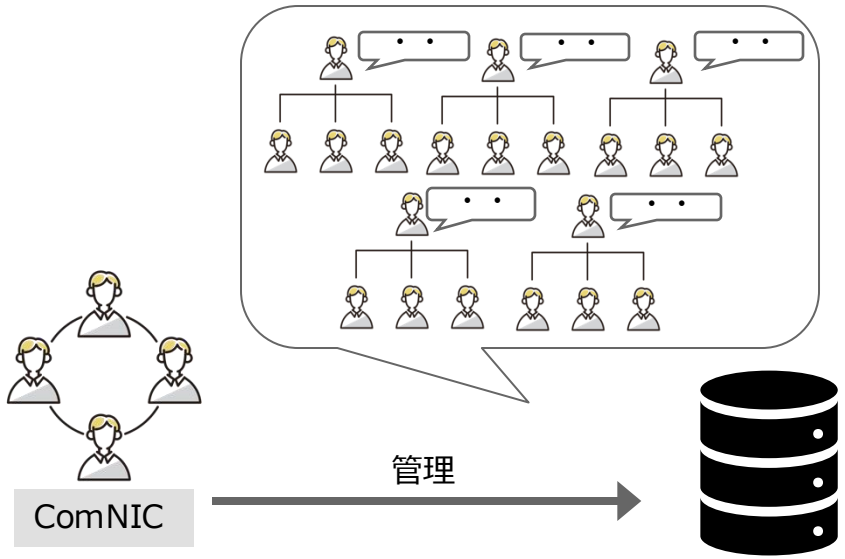
- 管理ポリシー・運用ガイドライン等の策定および社内浸透
- 運用体制・運用フローの整備および運用
- 保有資源ごとの利用状況・利用者情報の一元管理と最新化

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



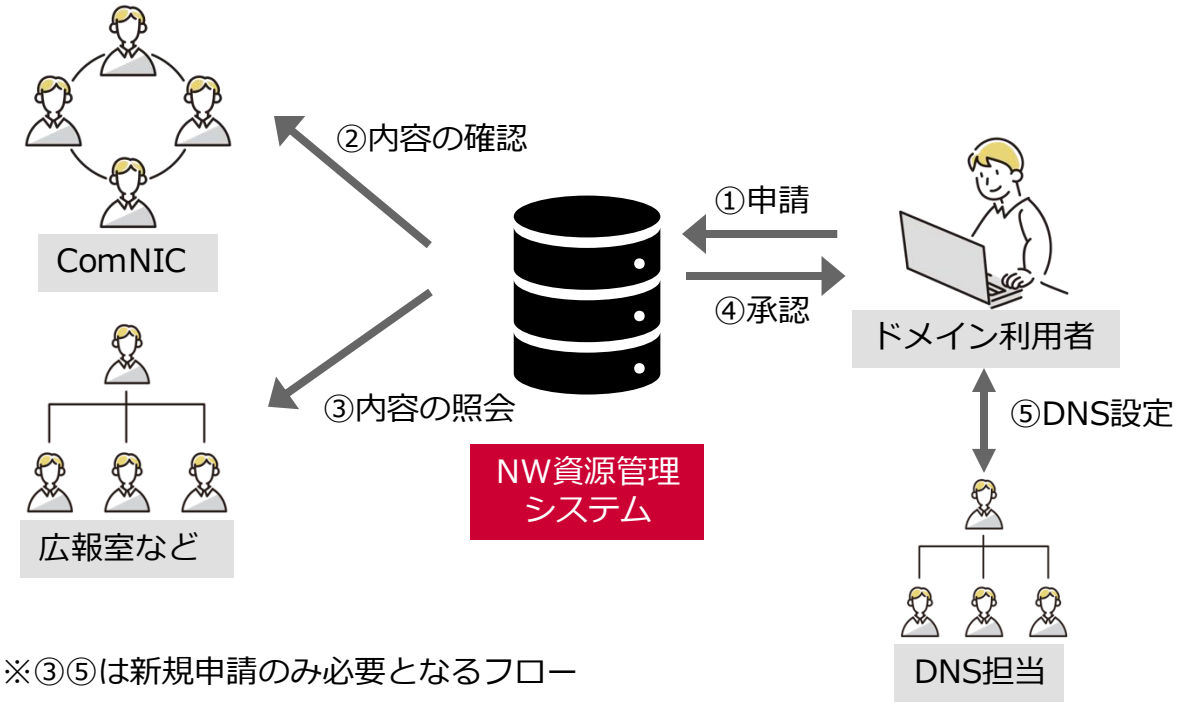
ComNICが情報を一元管理する主体に
誰が (どの組織が) 管理しているかわかる状態に

ドメイン管理の体制・プロセス

申請プロセスと管理方法

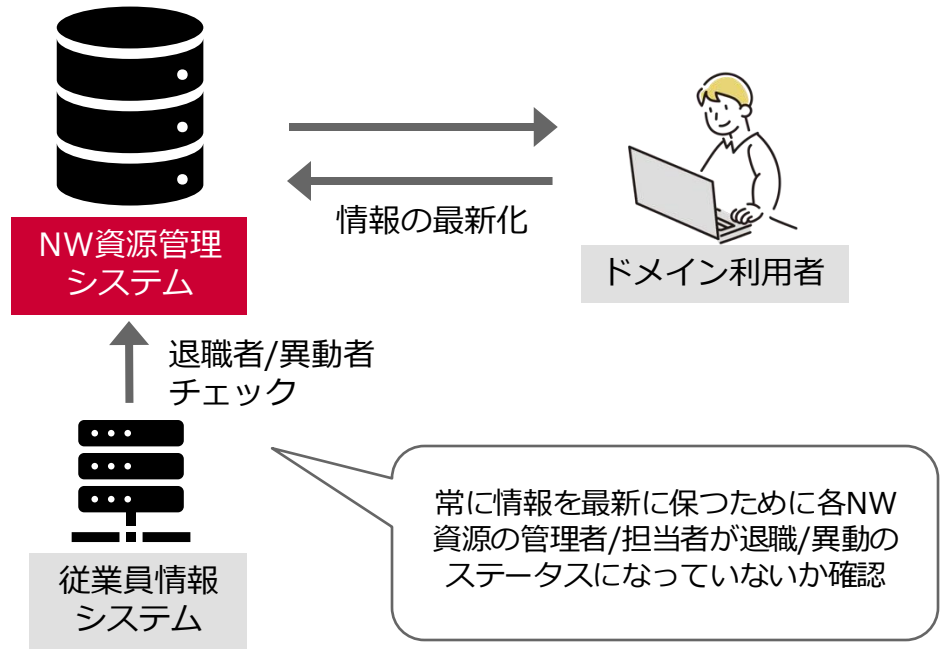
- 基本的にComNICが管理する ”ネットワーク資源管理システム (NW資源管理システム) ” を通じて申請してもらう
- 申請できるドメインは基本 “ntt.comサブドメイン” としているが、用途がそぐわない場合に限り “独自ドメイン” も申請可能
- ドメインの利用中は ”NW資源管理システム” の情報が最新に保てているように利用者に棚卸を依頼

新規申請/廃止申請



※③⑤は新規申請のみ必要となるフロー

ドメイン利用中



ドメイン廃止時の危険性

企業のサービスなどで使われていたドメインには価値がある！
- 利用終了したドメイン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

ドメインのドロップキャッチによる被害対策
- ✓独自ドメインではなく、ntt.comサブドメインの利用促進
- ✓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
ドメインの維持料
ドメインの健全的な利用への悪影響

利用終了したドメインへのアクセスログとDNSクエリを監視する基盤を作成、運用中

ログ収集環境の開発・運用

ログ収集環境の開発・運用

・ログ収集環境の要件・システム構成

・運用の工夫点

・コスト

ログ収集環境の開発・運用

・ログ収集環境の要件・システム構成

・運用の工夫点

・コスト

主な要件

01 DNSクエリログおよびWebアクセスログを収集する
- DNSクエリログに加え、発信者特定等の情報も取るべくWebアクセスログも収集
- Webアクセスログについては”ドメイン”および”サブドメイン” を登録
  （過去に実際に使われていたと思われるサブドメインを登録）

02 AWSで観測し、DLXHUB（NTT Comの社内分析環境）で分析を行う構成とする
- AWSは、興味があり採用
- DLXHUBは、社内リソース有効活用のため採用

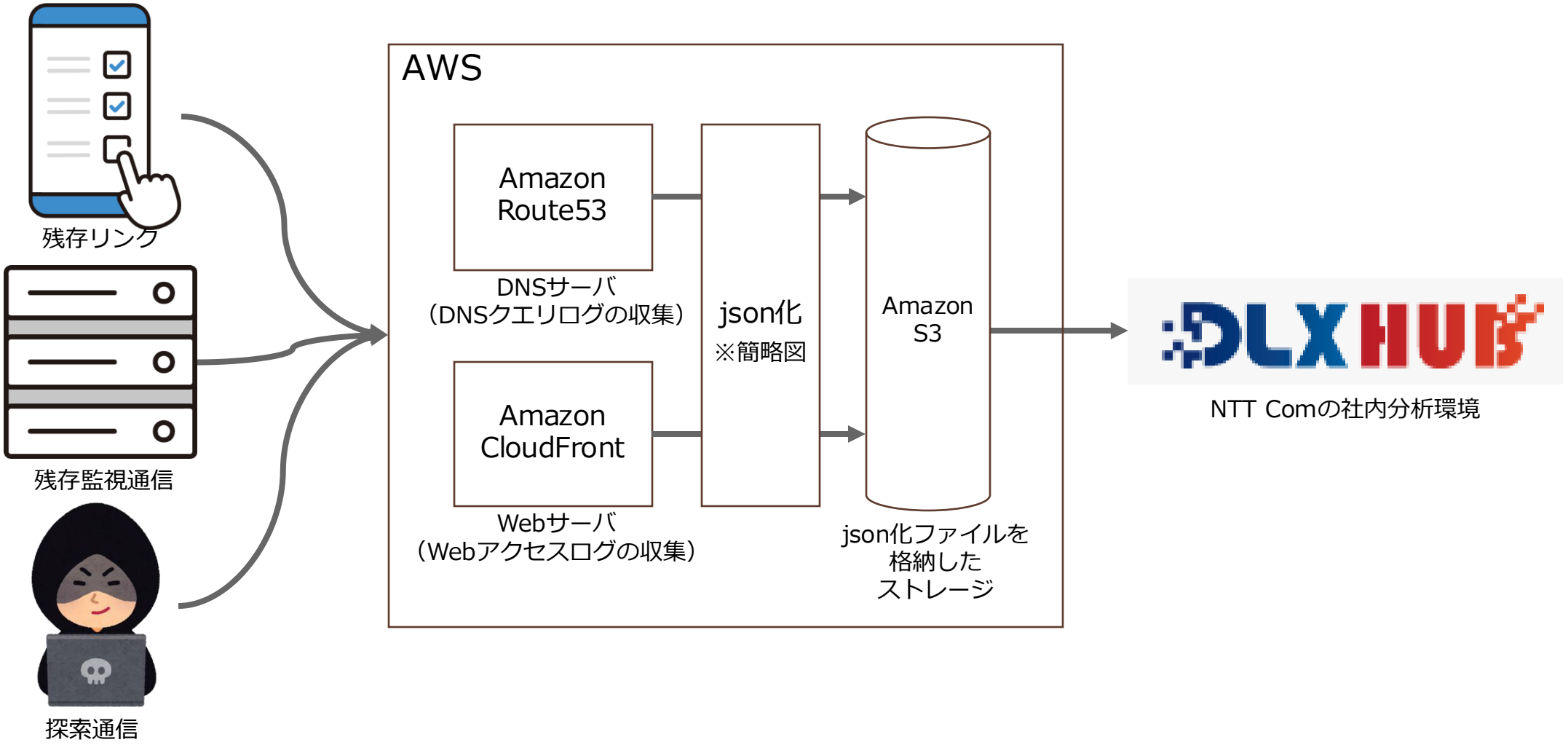
03 サーバレスでセキュアな環境とする
- 運用者による脆弱性管理の手間を減らしながらもセキュリティを担保すべく、
  マネージドサービスやサーバレス環境を活用

システム構成

想定される送信元

観測

分析



ログ収集環境の開発・運用

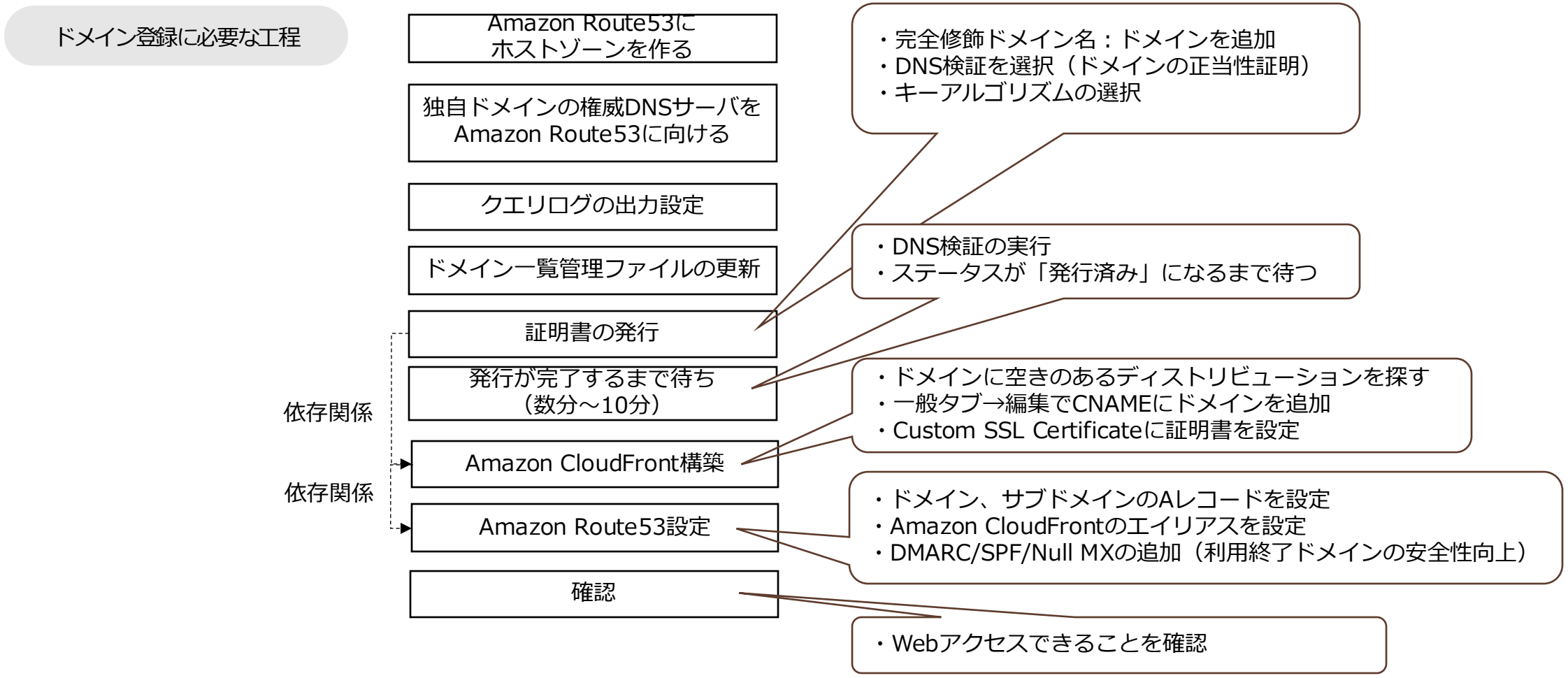
・ログ収集環境の要件・システム構成

・運用の工夫点

・コスト

ドメイン数増加に伴い登録負荷が高まる

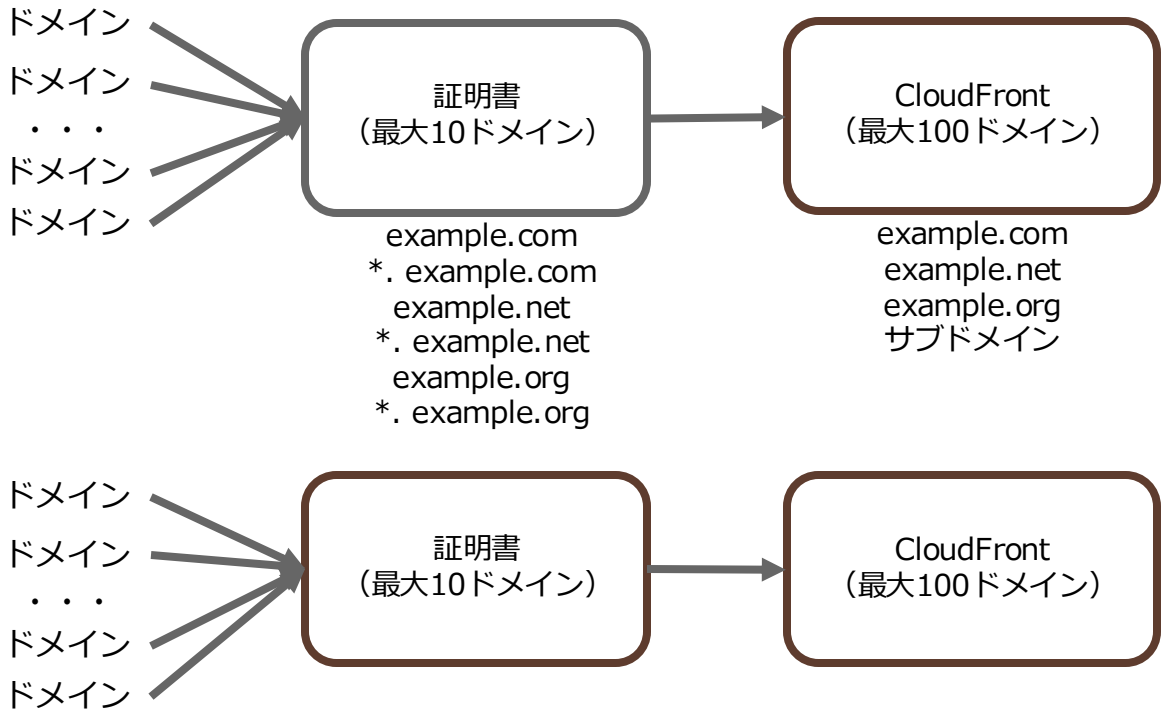
数十箇所に及ぶ設定項目の中から、必要な箇所を見つけ、正しく設定する難しさ
⇨ 自動化の必要性



自動化のためのアーキテクチャ改善

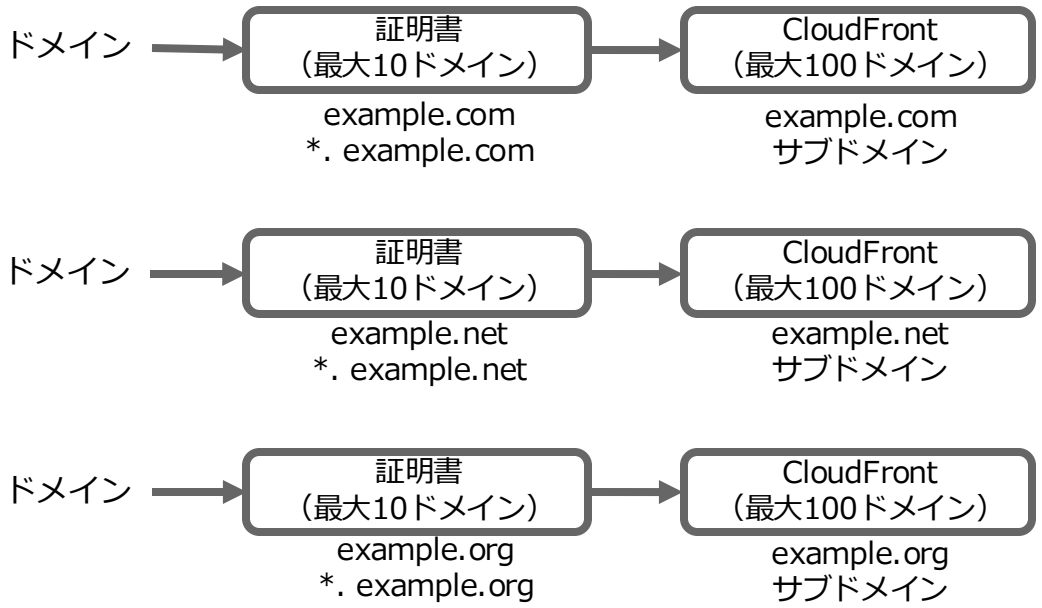
今までAWSのマネジメントコンソールから構築・設定を行っていたが、
そのまま自動化するとアルゴリズムが複雑になるため、アーキテクチャを改善

変更前



上記アーキテクチャの場合、自動化のアルゴリズムが複雑になる
（負の遺産となりうる）

変更後



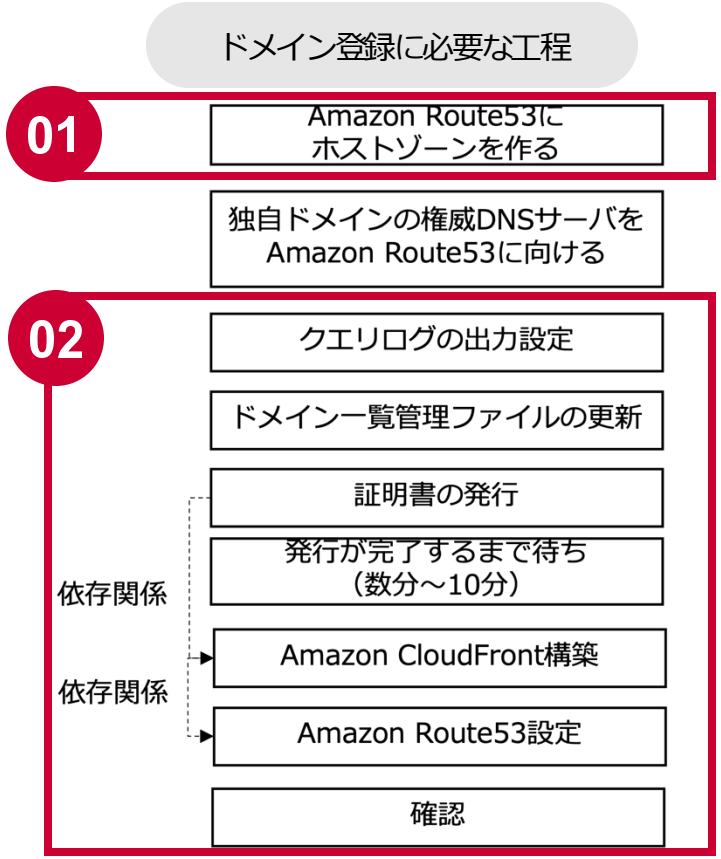
自動化しやすいアーキテクチャに変えることで、
アルゴリズムをシンプルにできる

自動化

メンテナンス性を考慮し、自チームで使われているpython3で開発

01 Amazon Route53（DNSサーバ）ホストゾーンを作成するスクリプト
※作成後、利用終了ドメインの所有者（ComNIC）にAWSに向けてもらう

02 構築スクリプト



ログ収集環境の開発・運用

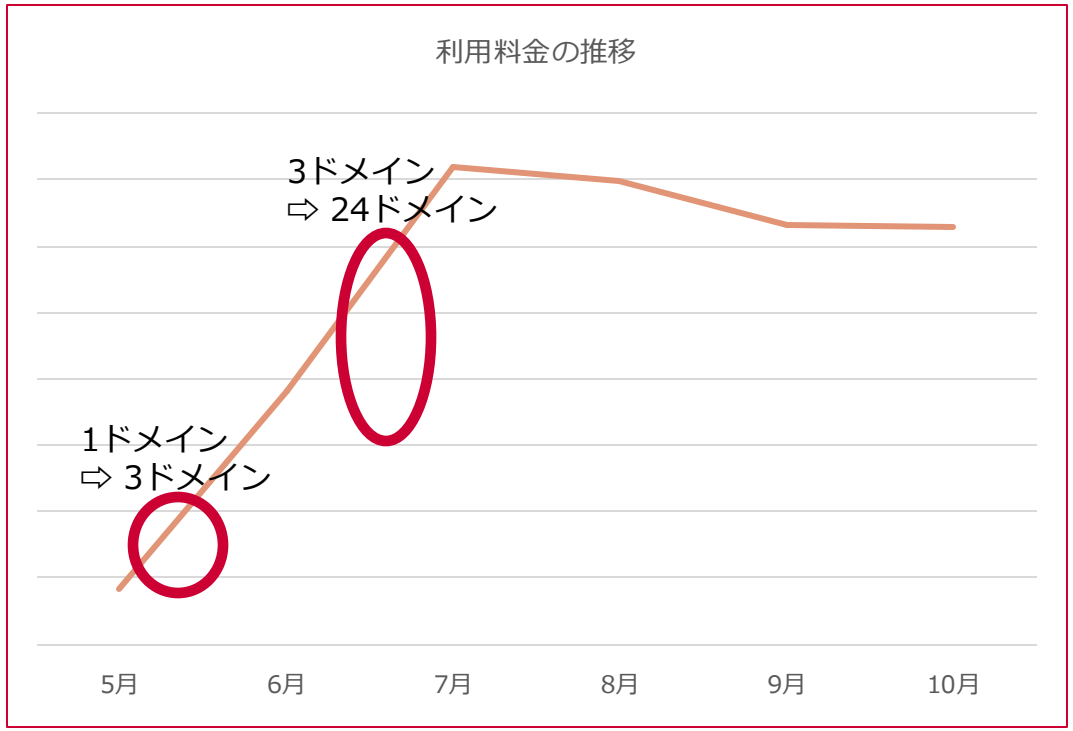
・ログ収集環境の要件・システム構成

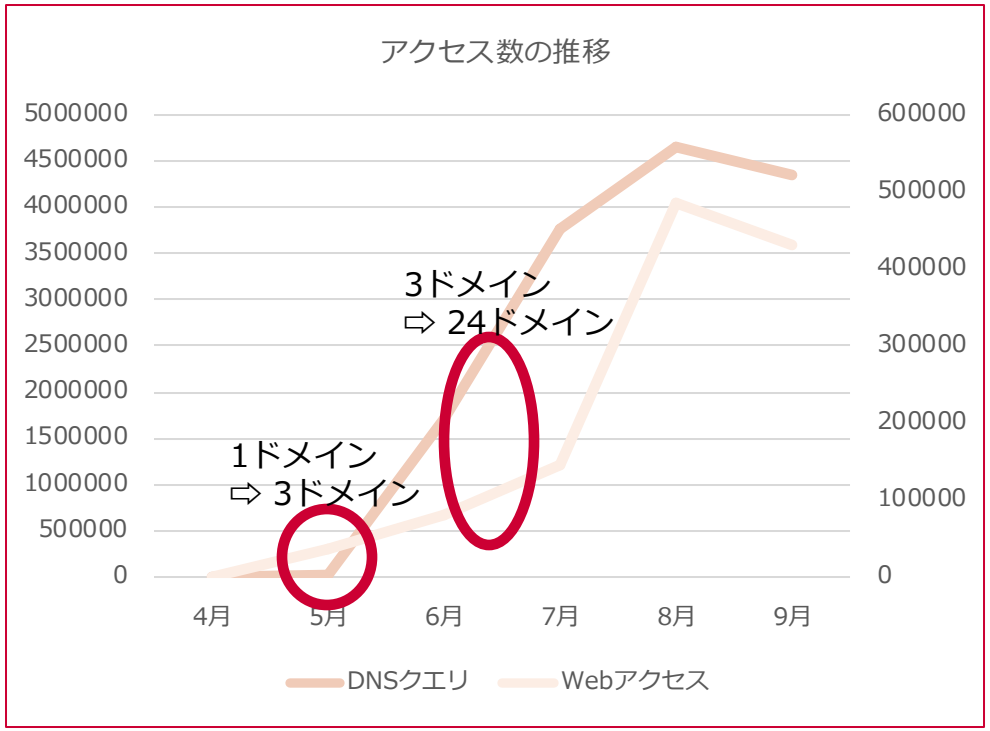
・運用の工夫点

・コスト

コスト（AWS利用料金）

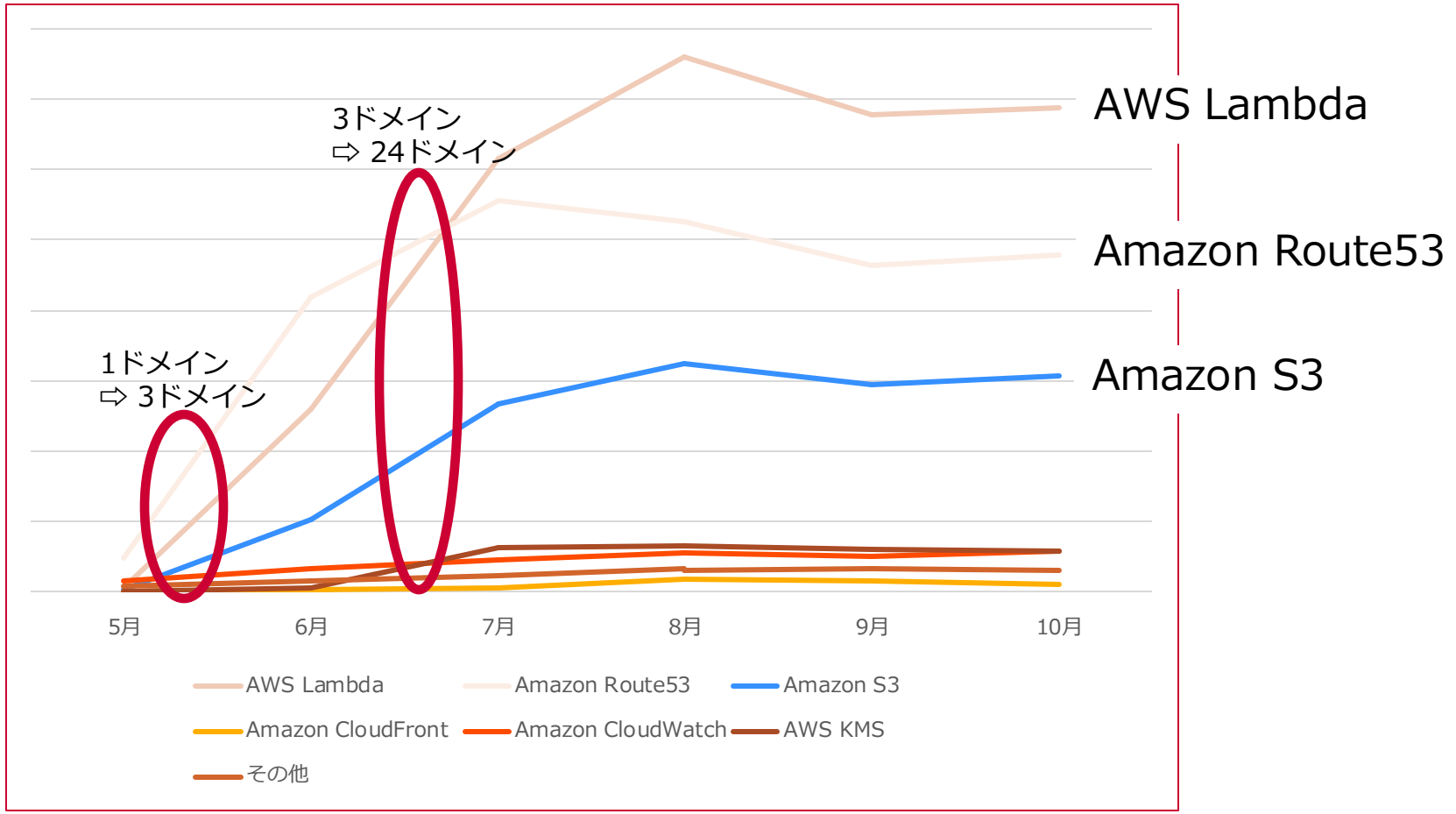
- AWSの利用料金について分析（ドメインの維持費用は含まない）
- 今回の環境では、24ドメインの収集で月額 数万円程度（＜ 2万円）となった





コスト（AWS利用料金）

- システム構成がある程度固まった5月以降の詳細を分析
- AWS Lambda、Amazon Route53、Amazon S3が主なコスト要因と分かる
  （※）Amazon CloudFrontは「何もコンテンツを返さない」ことで支出を月数十円に抑えられている。



ログ分析結果について

ログ分析結果について

- 今回の施策の目的の1つは収集したDNSクエリ、Webアクセスログから適切なドメインを手放す時期を評価すること
- ただし、現状の手持ちのデータのみではその結論に至らなかった

- そのため、今回は収集したデータの全体傾向と分析を通して発見した有用なドメイン管理の方法について紹介する

ログ分析結果について

・全体傾向について

・分析過程で発見した事例について

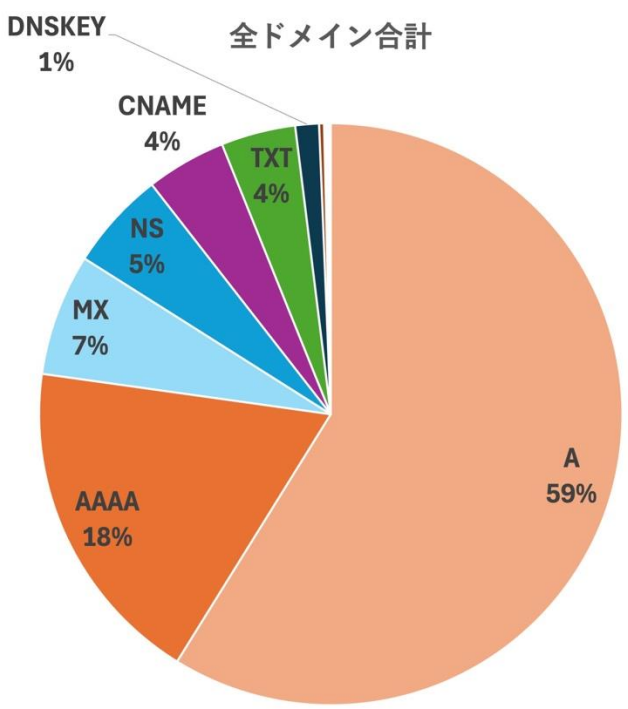
ログ分析結果について

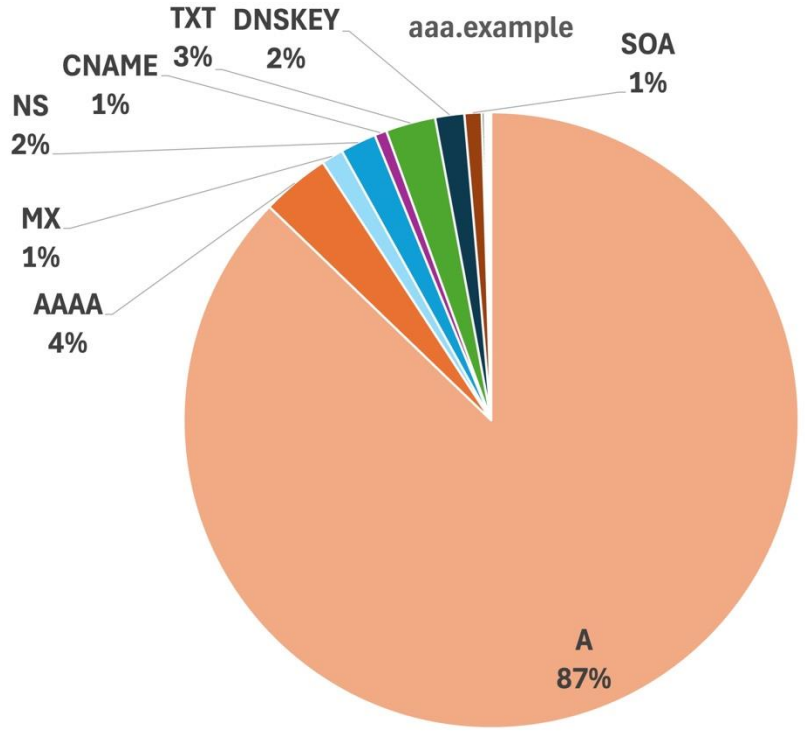
・全体傾向について

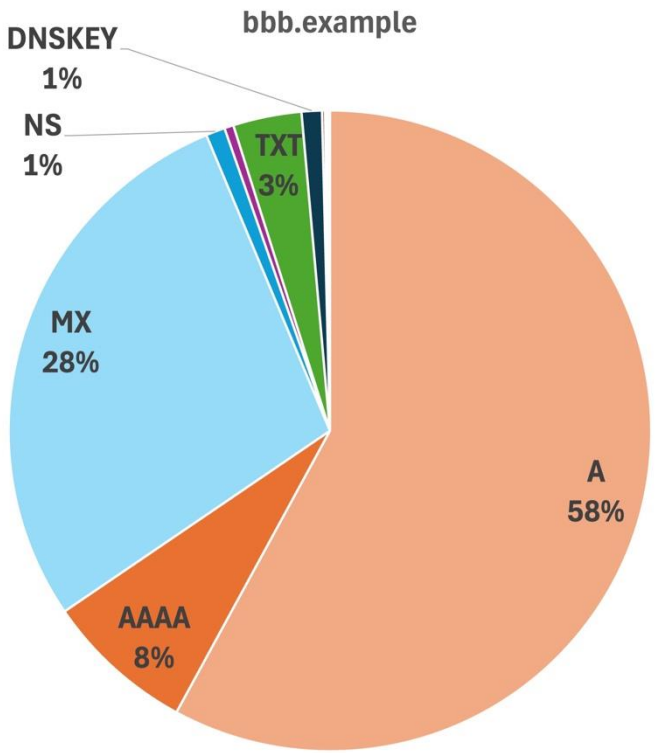
・分析過程で発見した事例について

DNSクエリログ

7/1 ~ 11/11 の期間に利用終了ドメイン宛に送信された18,360,458件のDNSクエリのタイプを集計した

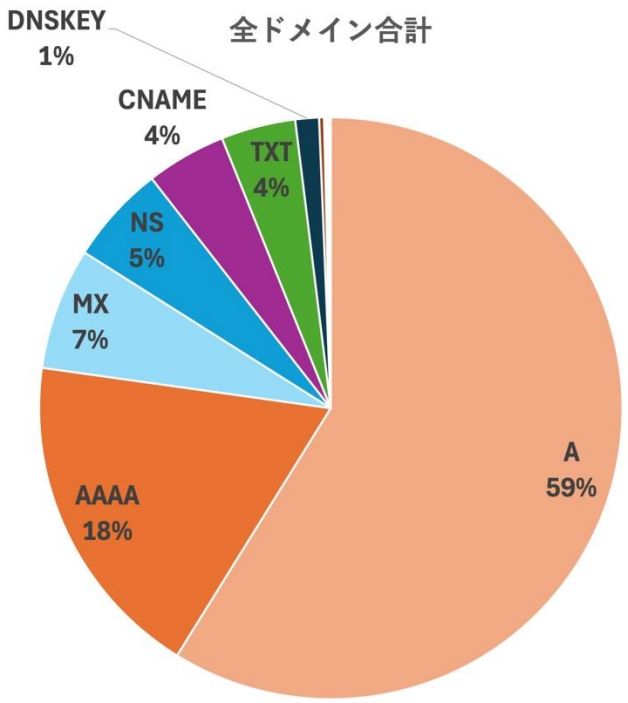


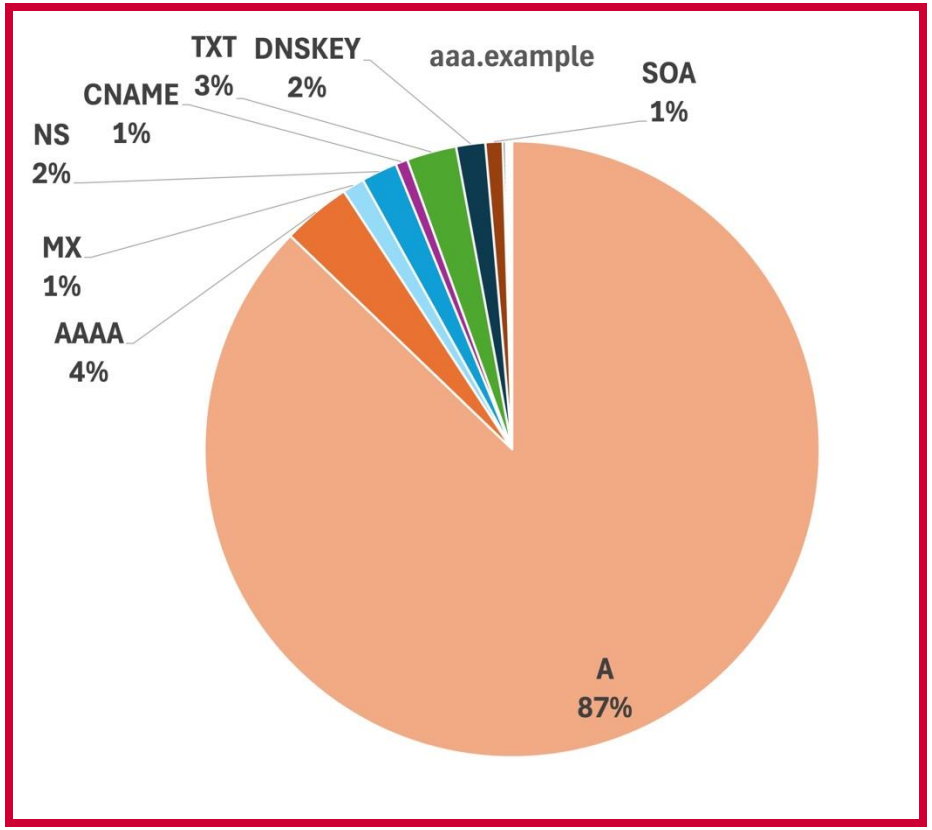


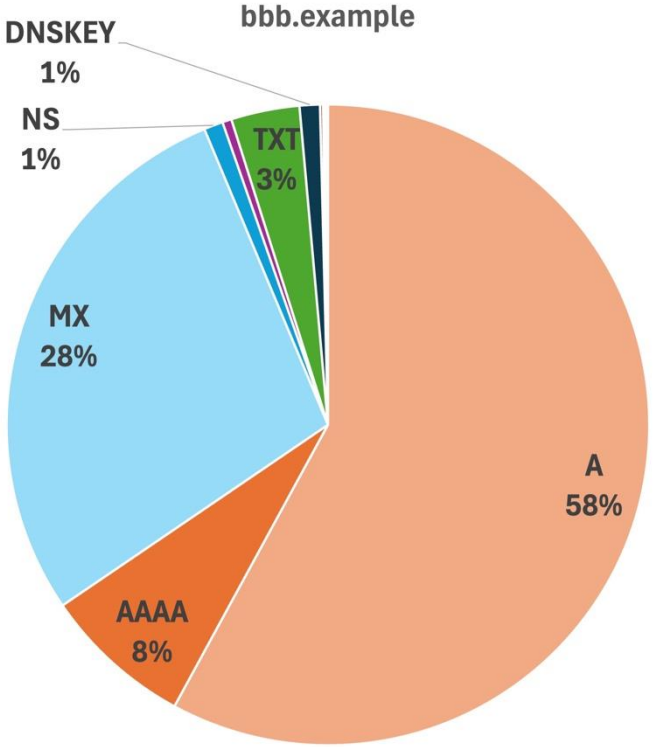


DNSクエリログ

- aaa.exampleはWebサイトとして利用されていたドメイン
- Aレコードが全体の87%を占める
- インターネット上の残存リンクなどによりAレコードの比率が高い可能性

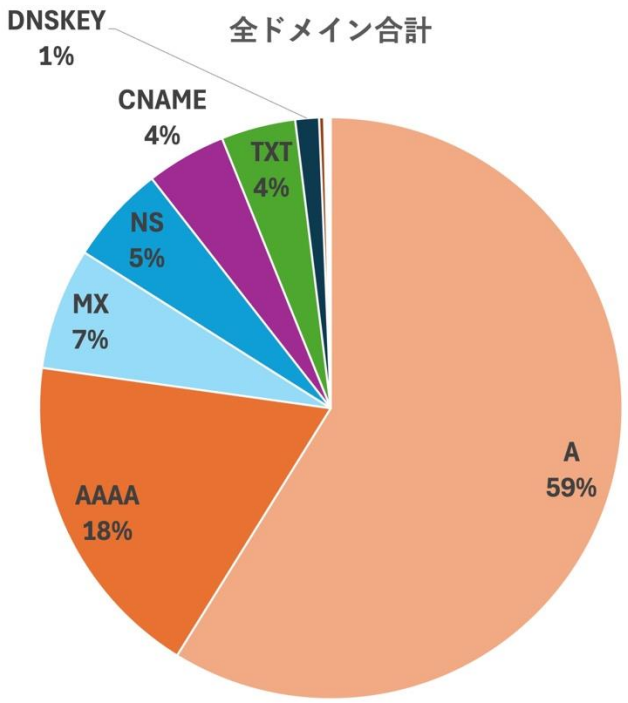


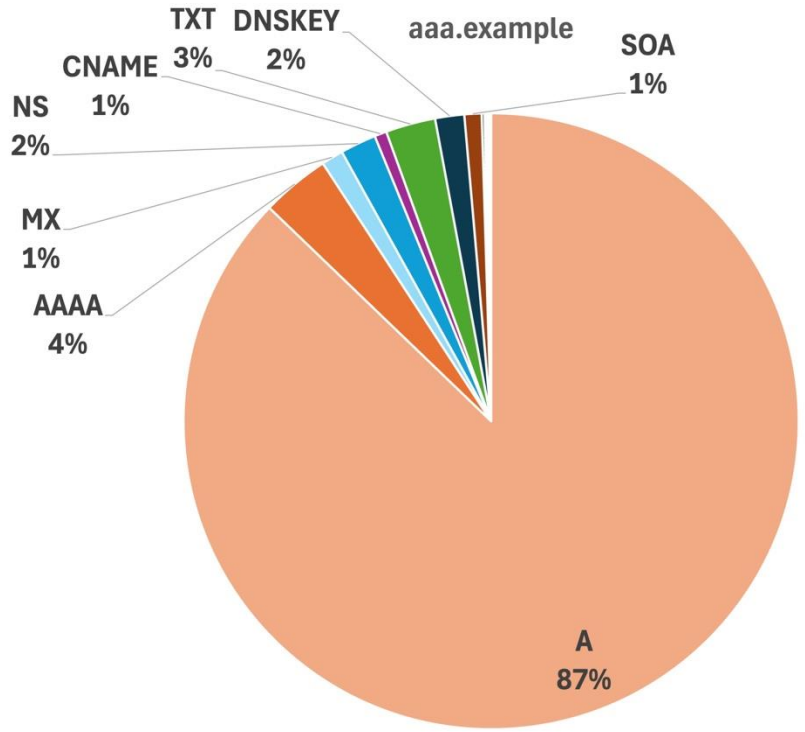


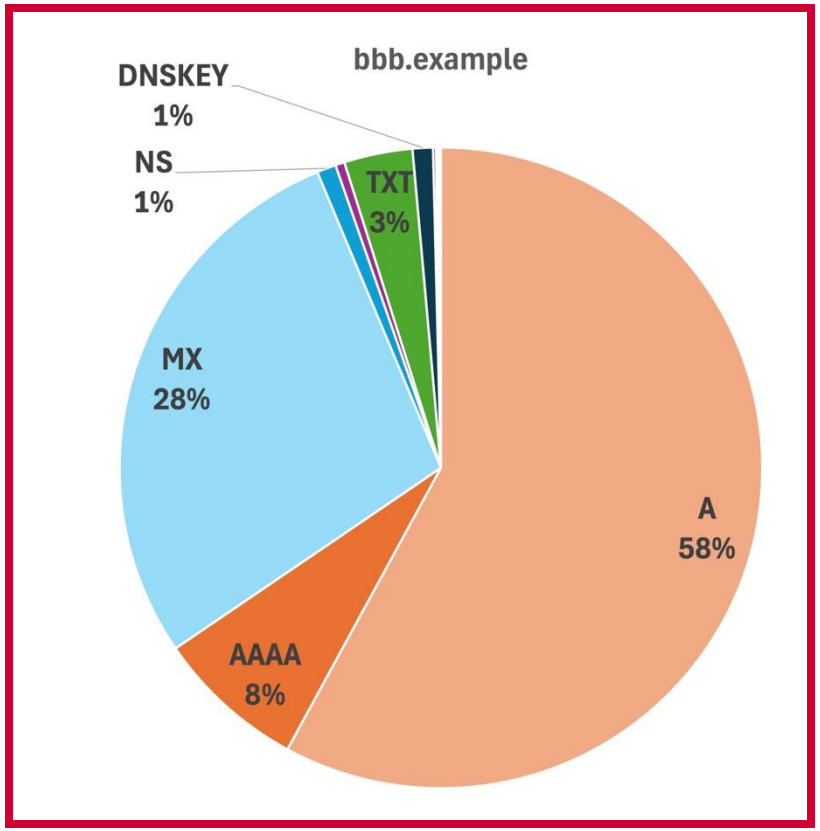


DNSクエリログ

- bbb.exampleはコーポレートドメインとして利用されていた
- MXレコードの割合は28%であり他のドメインと比較すると高い傾向
- メールアドレスとしても利用されていたことから現在でもメールが送信されている可能性

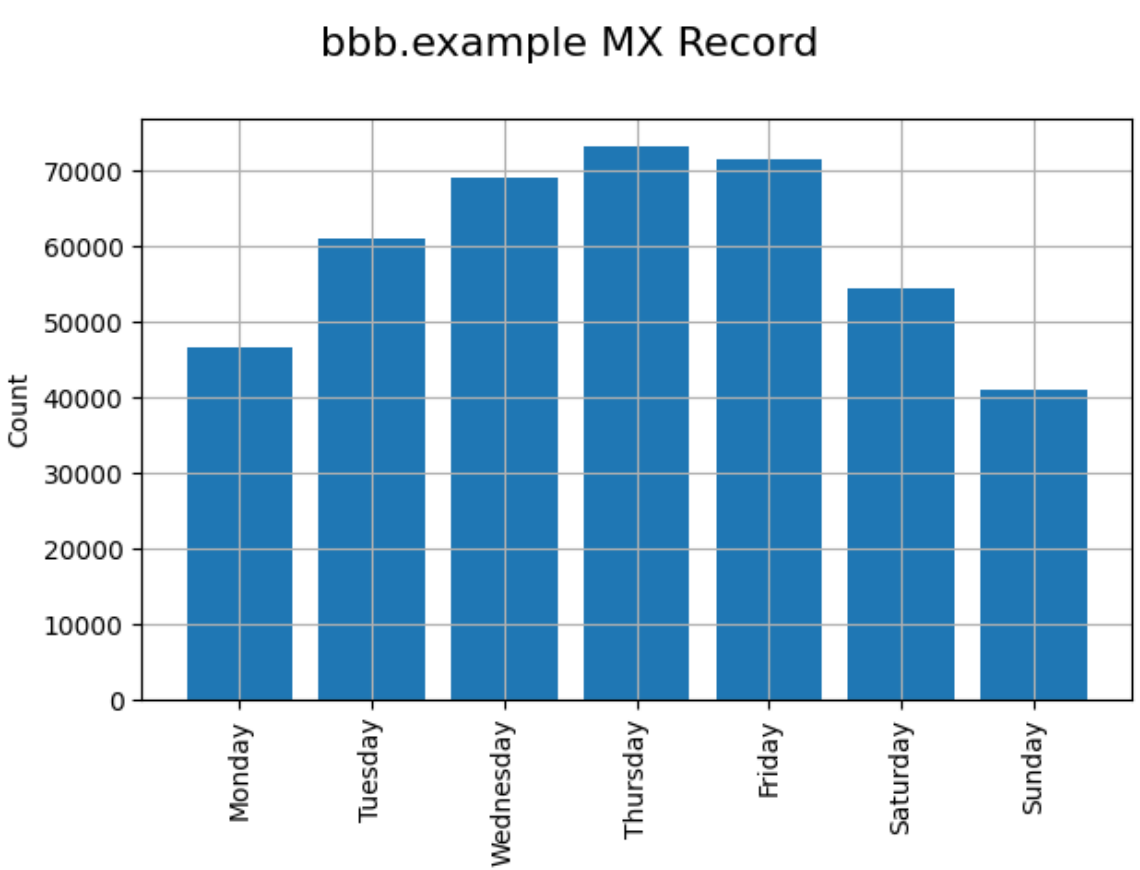


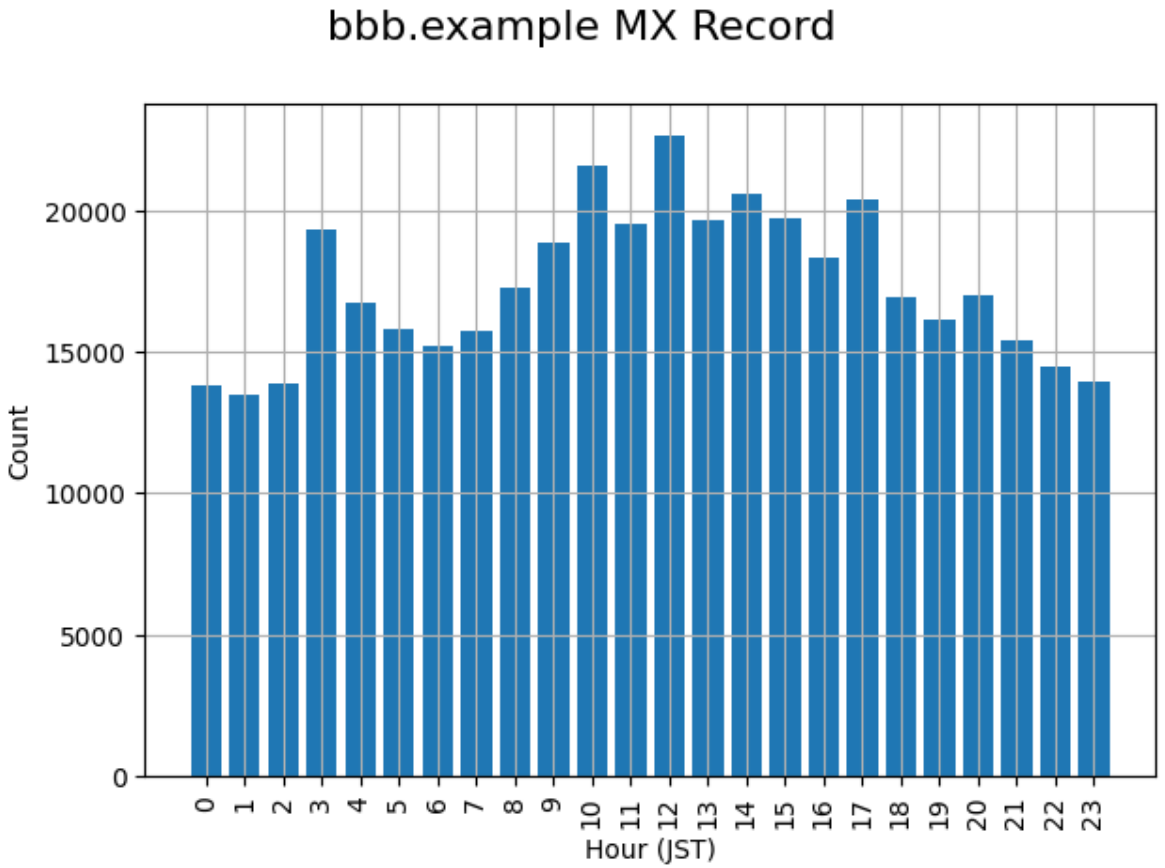




DNSクエリログ

- bbb.exampleのMXレコードに絞ってクエリが来た曜日、時間を集計
- 平時、日中のカウントが比較的高い





Webアクセスログ

6/18 ~ 11/11 の期間における1,764,208件の利用終了ドメインへのWebアクセスログを収集した

- 今回はアクセスログのuser-agentに注目しクライアントの特性を分析した
- 下記は実際に取得したuser-agentでありクライアントのデバイス、ブラウザ、OSなどの情報が含まれている

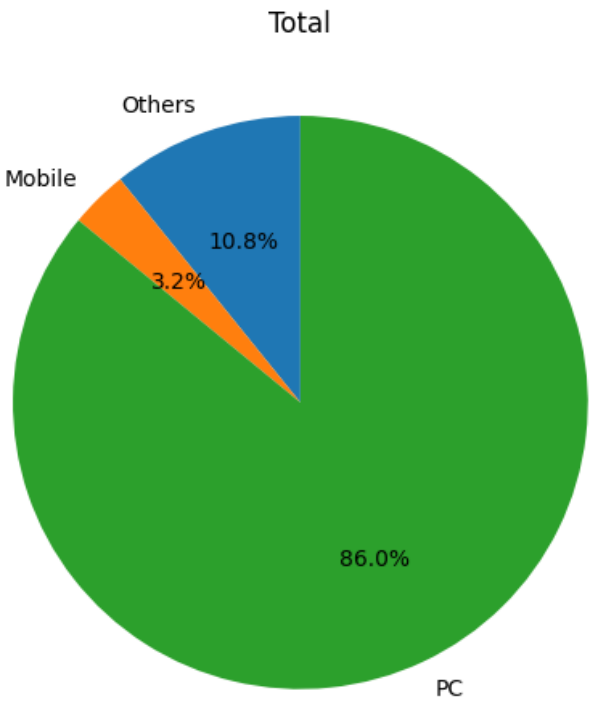
"Mozilla/5.0 (Linux; Android 6.0 Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.1719.1634 Mobile Safari/537.36"

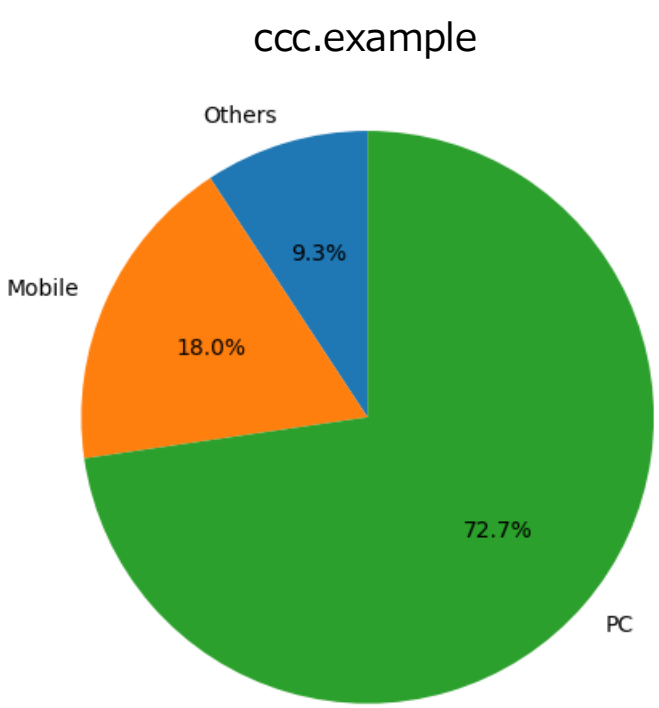
OS　デバイス　ブラウザ

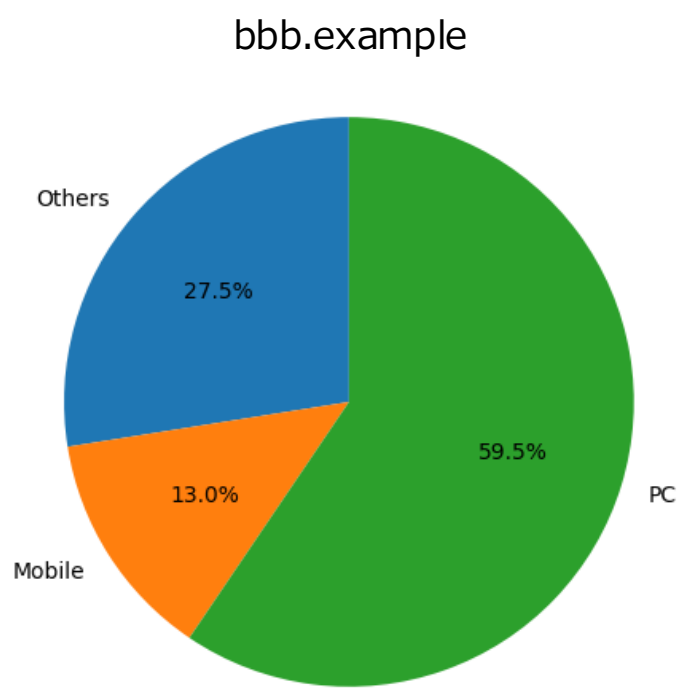
※ user-agentを変更することは容易であり、あくまでもクライアントからの自己申告に近いものである

Webアクセスログ

user-agent から分類したクライアント端末の PC / Mobile の内訳

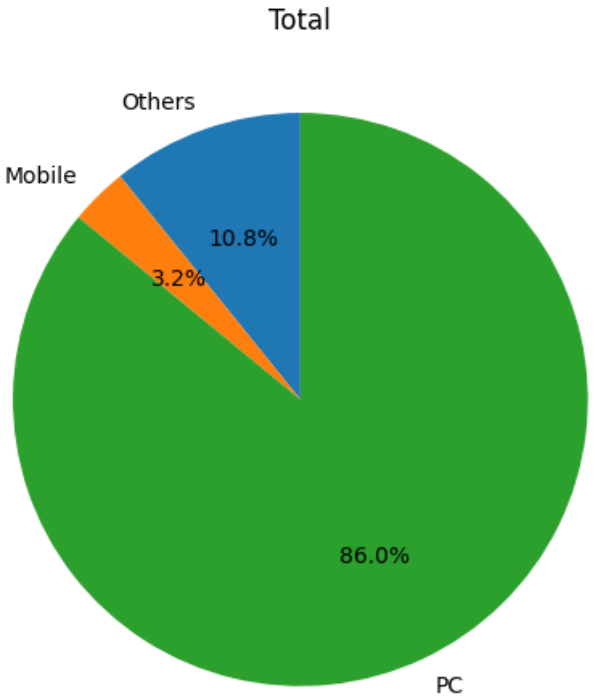


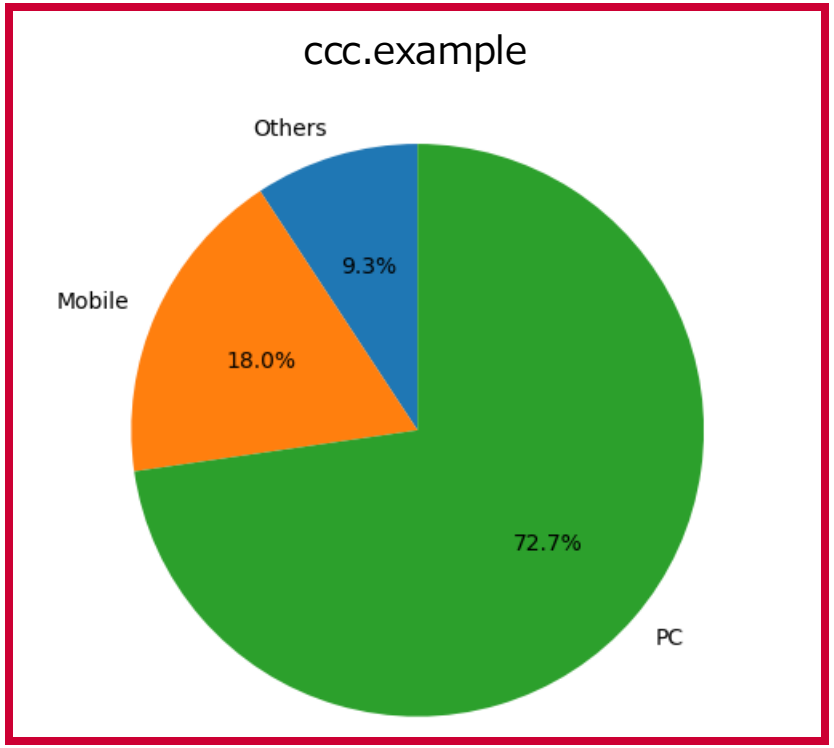


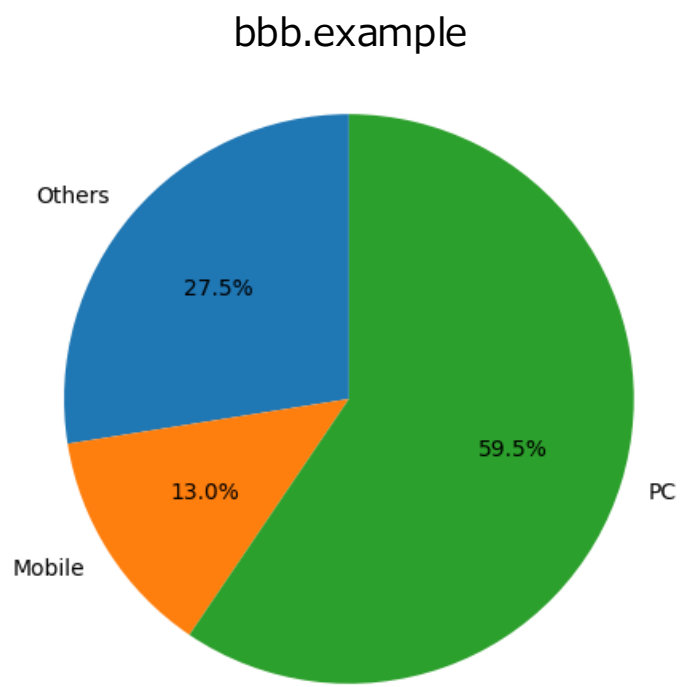


Webアクセスログ

- ccc.exampleはNTTコミュニケーションズと関連するスポーツチームのホームページに利用されていたドメイン
- モバイルの割合は18%であり、他のドメインと比較すると高い傾向
- 利用者の嗜好によるアクセスのためモバイルの比率が高い可能性がある

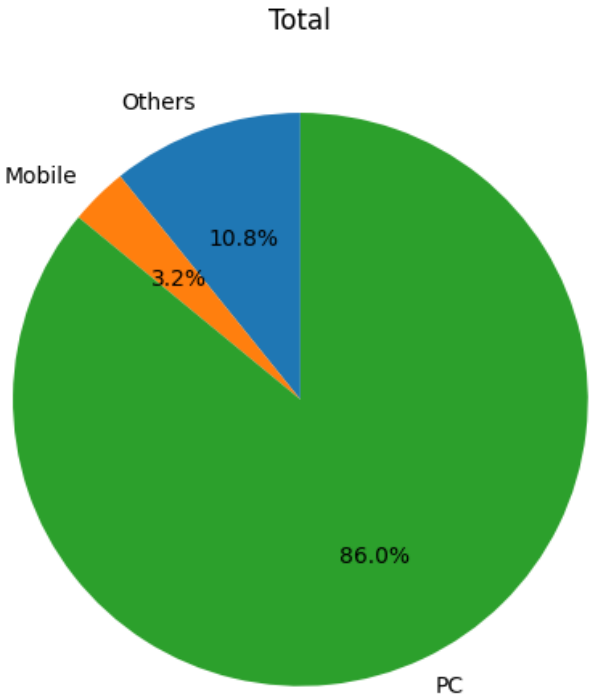


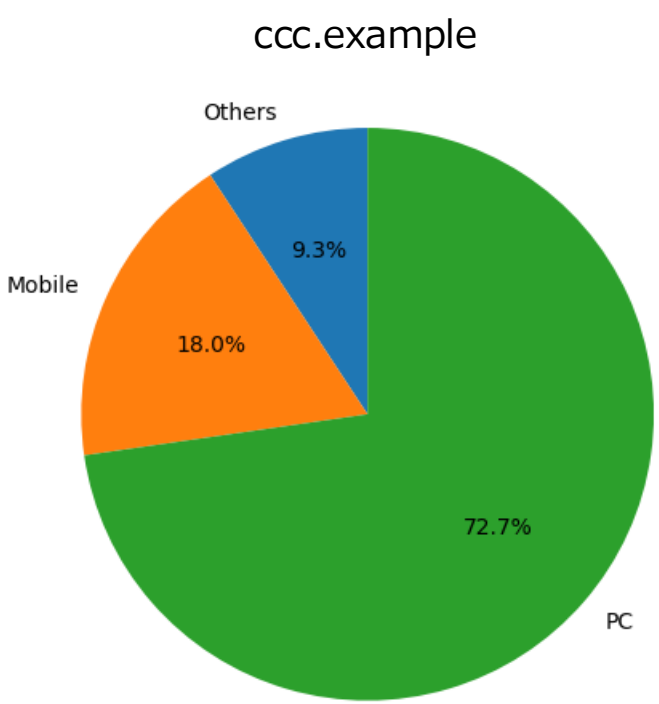


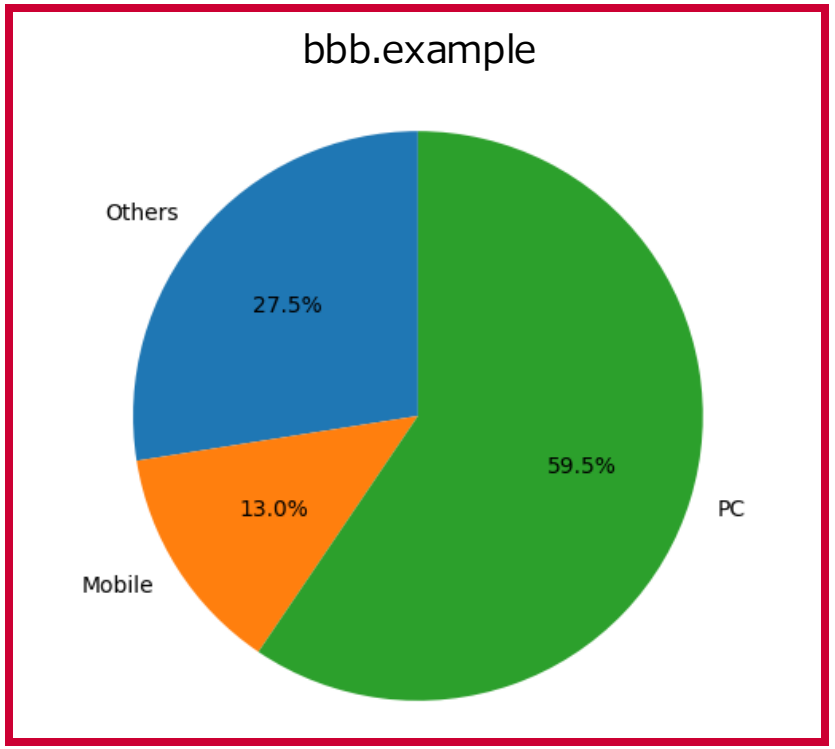


Webアクセスログ

- bbb.exampleはコーポレートドメインとして利用されていたドメイン
- 未分類の割合は27.5%であり他のドメインと比較すると高い傾向



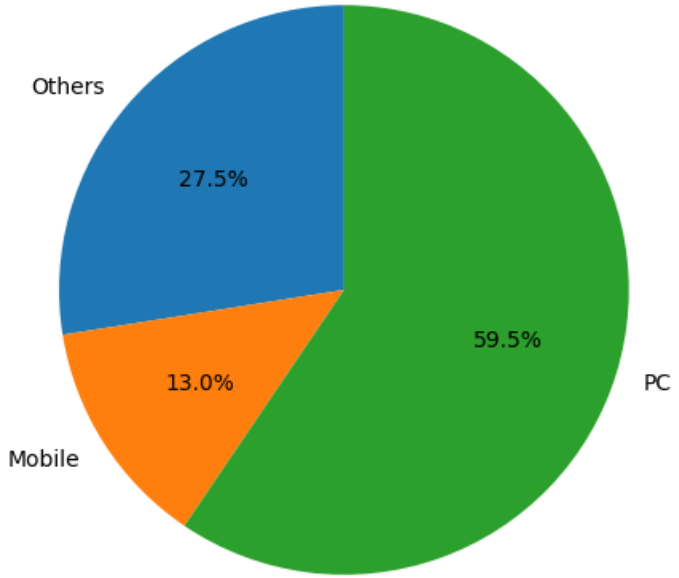




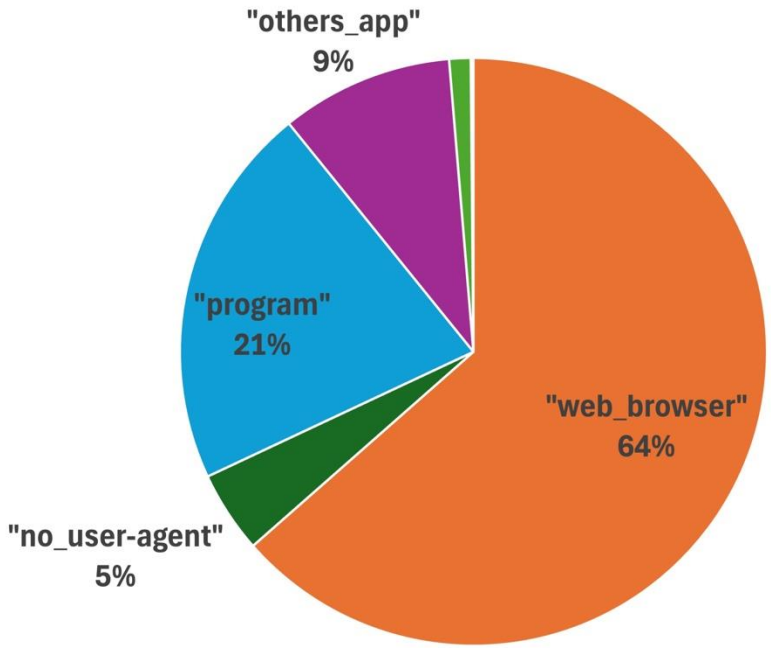
Webアクセスログ

- 右図はbbb.exampleのuser-agentを元にアクセスを種類分けしたもの
- "program" (Go、Pythonなど) からのアクセスが左図のOthersの近いことを確認した
- コーポレートドメインであったことを考慮すると、企業宛ての偵察活動や社内監視ツールの残りなどの可能性がある

bbb.example

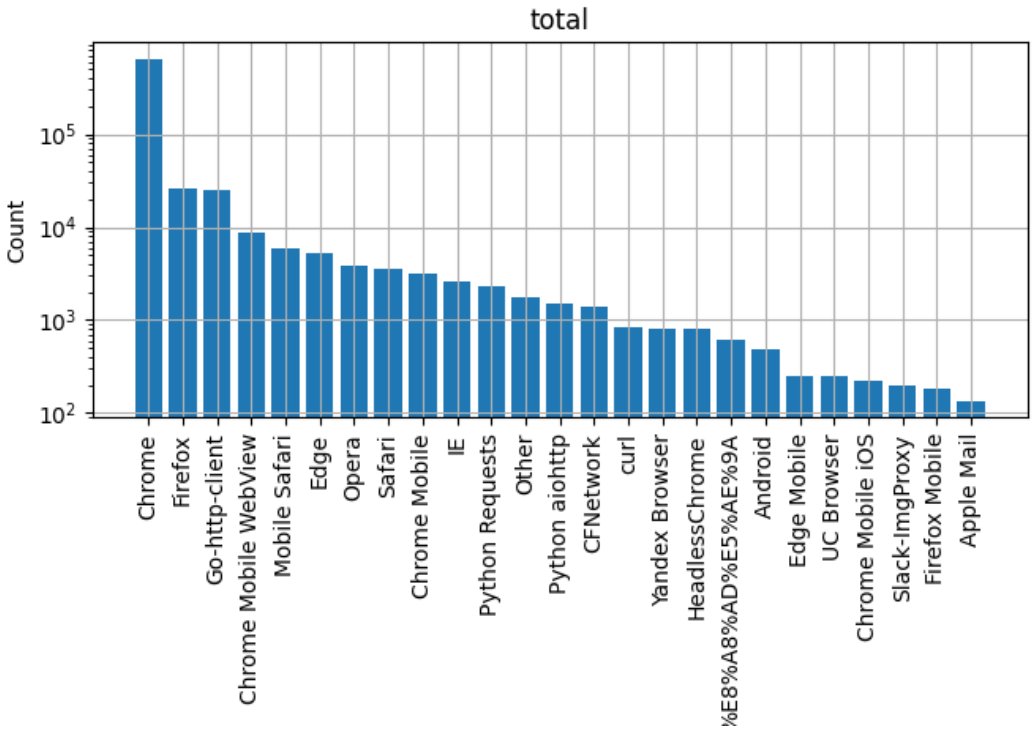


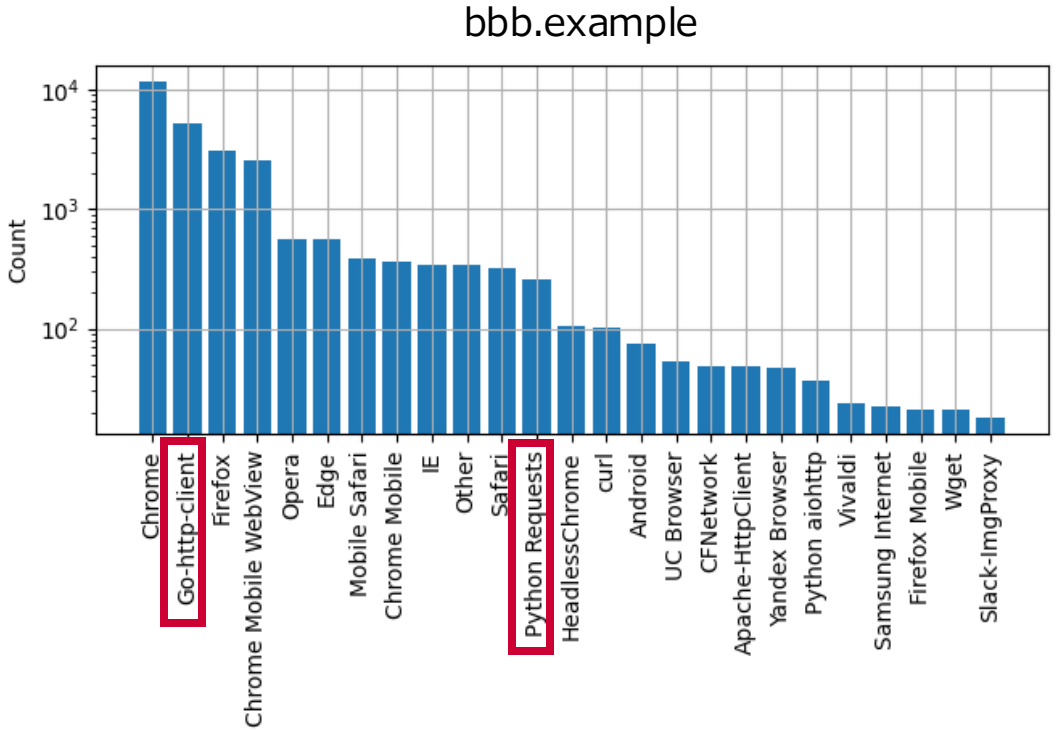
bbb.example



Webアクセスログ

user-agent から分類した各ブラウザからのアクセス数

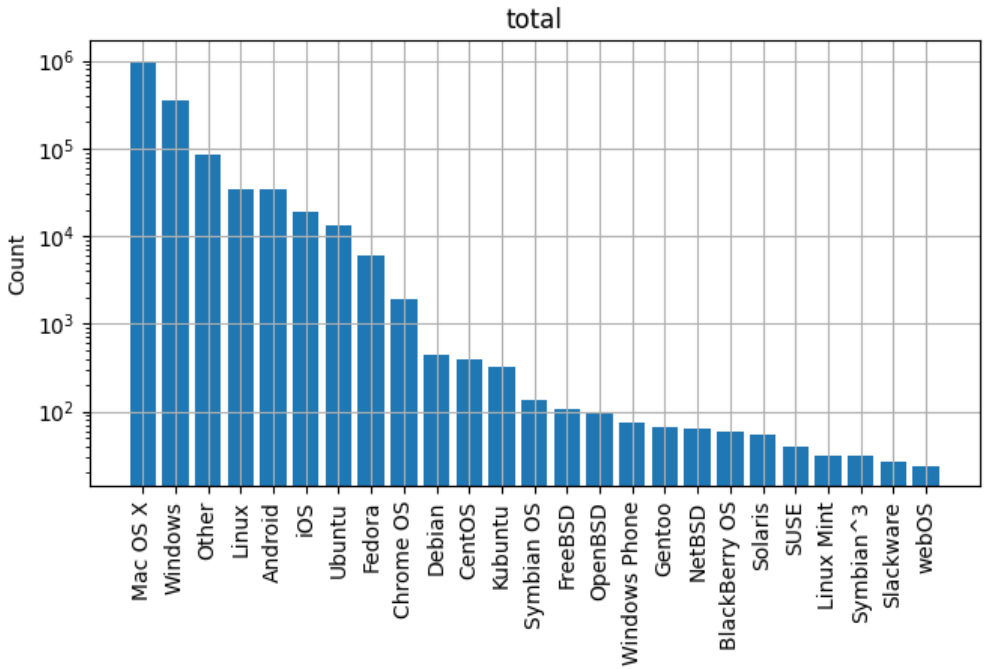


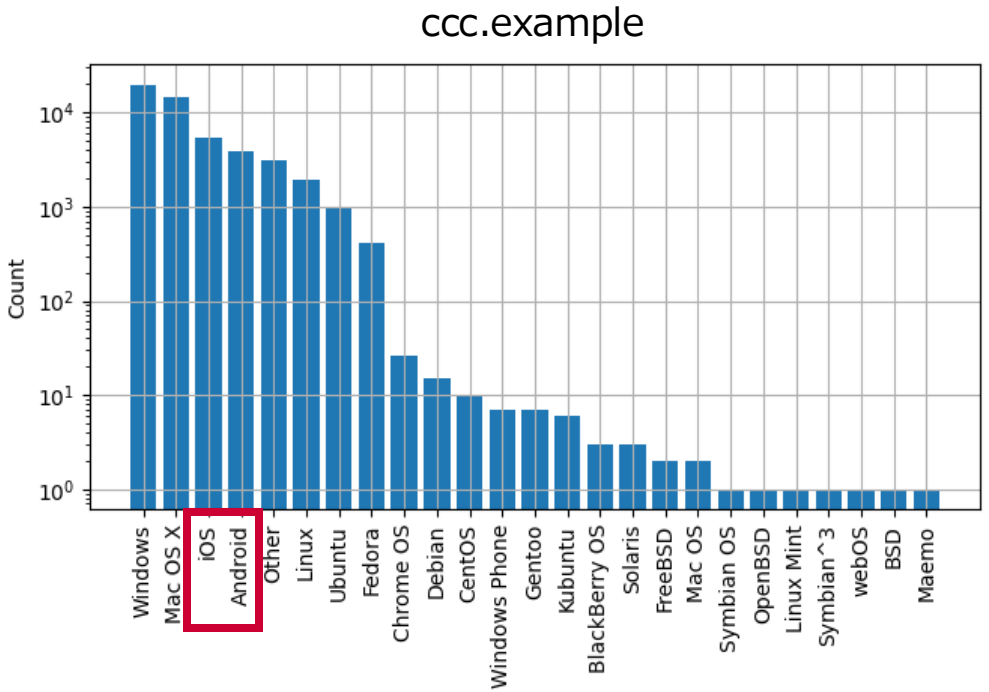


- 右図はbbb.exampleへのアクセスを示している
- Goからのアクセスが多い

Webアクセスログ

user-agent から分類した各OSからのアクセス数

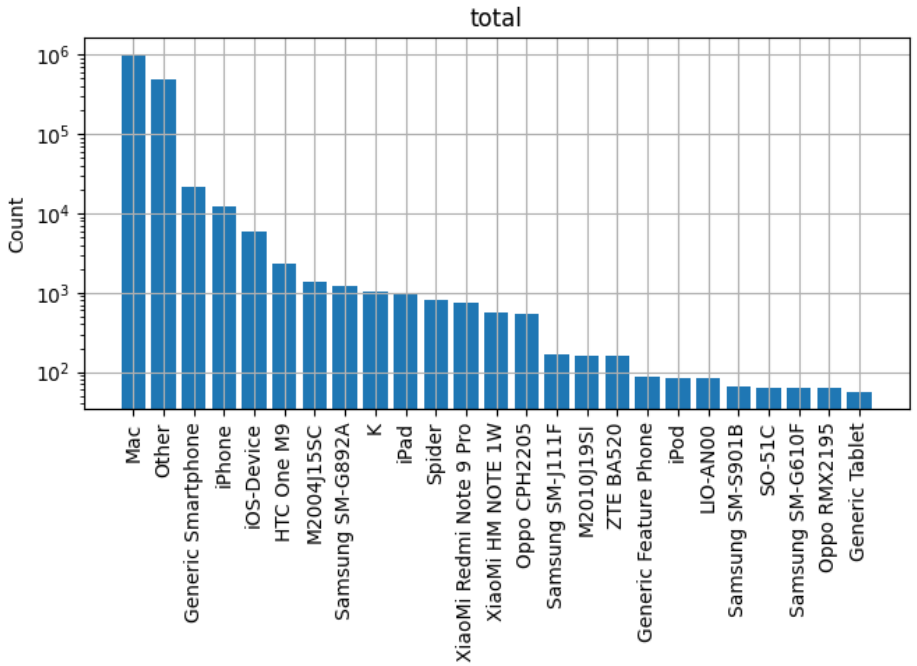


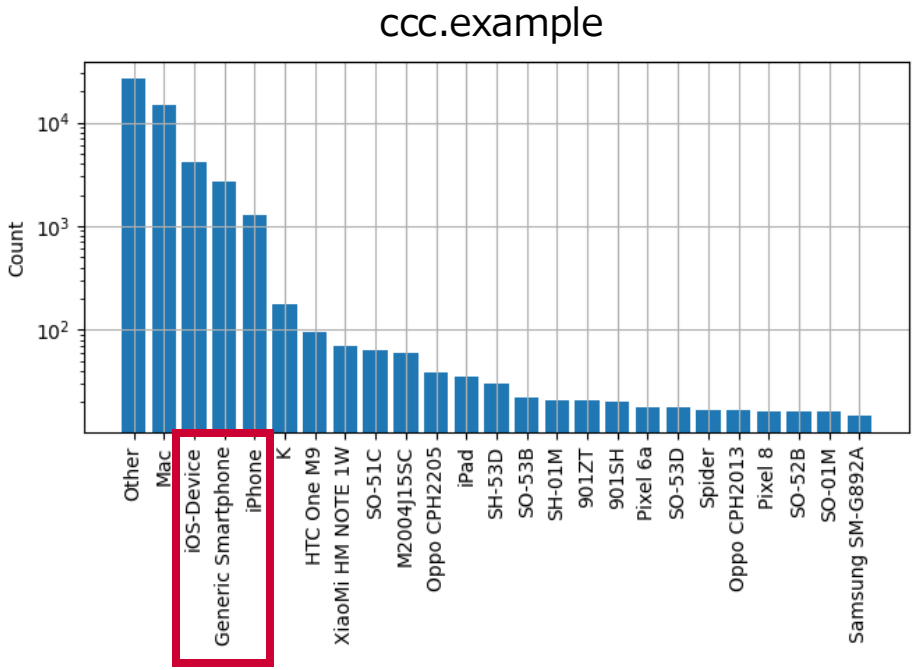


- 右図はccc.exampleへのアクセスを示している
- iOS、Android (モバイル) の件数が多い

Webアクセスログ

user-agent から分類した各デバイスからのアクセス数





- 右図はccc.exampleへのアクセスを示している
- iPhoneなどのモバイルからの件数が多い

ログ分析結果について

・全体傾向について

・分析過程で発見した事例について

分析過程で発見した事例1

一般的に、利用終了ドメインは保持することでドロップキャッチなどのリスクに対応することができる

ただし、今回は「保持することで発生するリスク」について紹介する

メールの送信元偽装

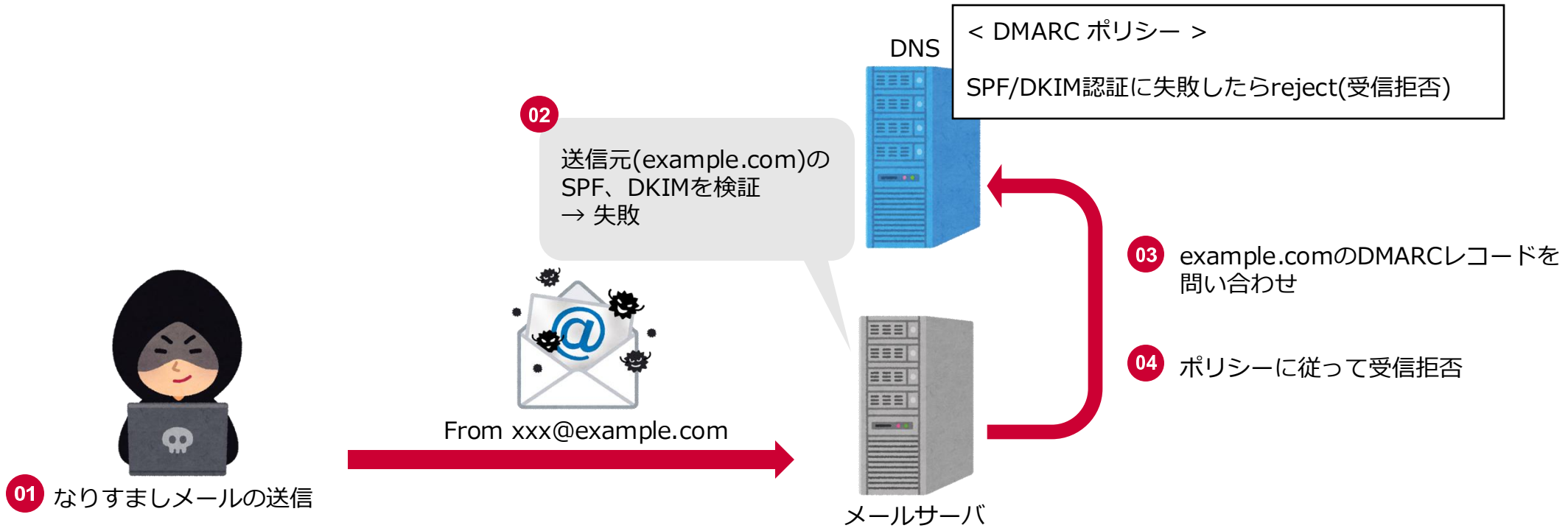
メールのFromヘッダーは書き換えができるため、送信元アドレスを偽装した
メールの送信が可能

このような「なりすましメール」は、受信者へのフィッシングやマルウェア感染に
利用されるだけではなく、送信元として利用されたドメインの保有者の
社会的信用を毀損する恐れがある

DMARCによる対策

保有するドメインが「なりすましメール」に利用されることを防止するために、
DMARCポリシーをDNS上で宣言することが有効

保有ドメインからのメールがSPF、DKIMによる認証に失敗したときに、
受信者はそのメールをどのように扱うべきか判断することができる

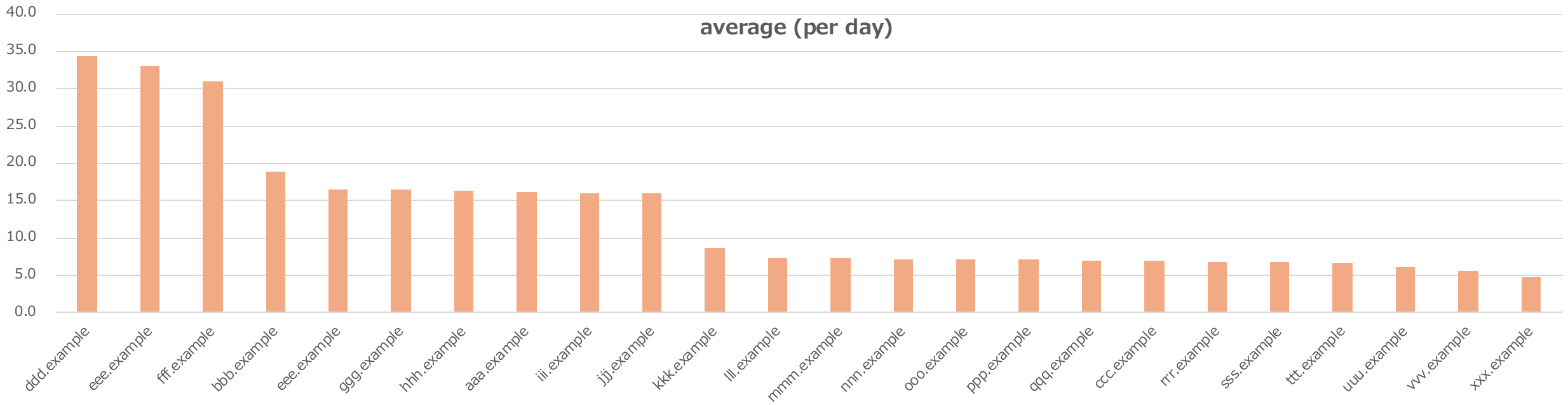


利用終了ドメインへのDMARCクエリ

下図は各ドメイン宛のDMARCクエリの1日あたりの件数を示している

< dmarc クエリ サンプル >

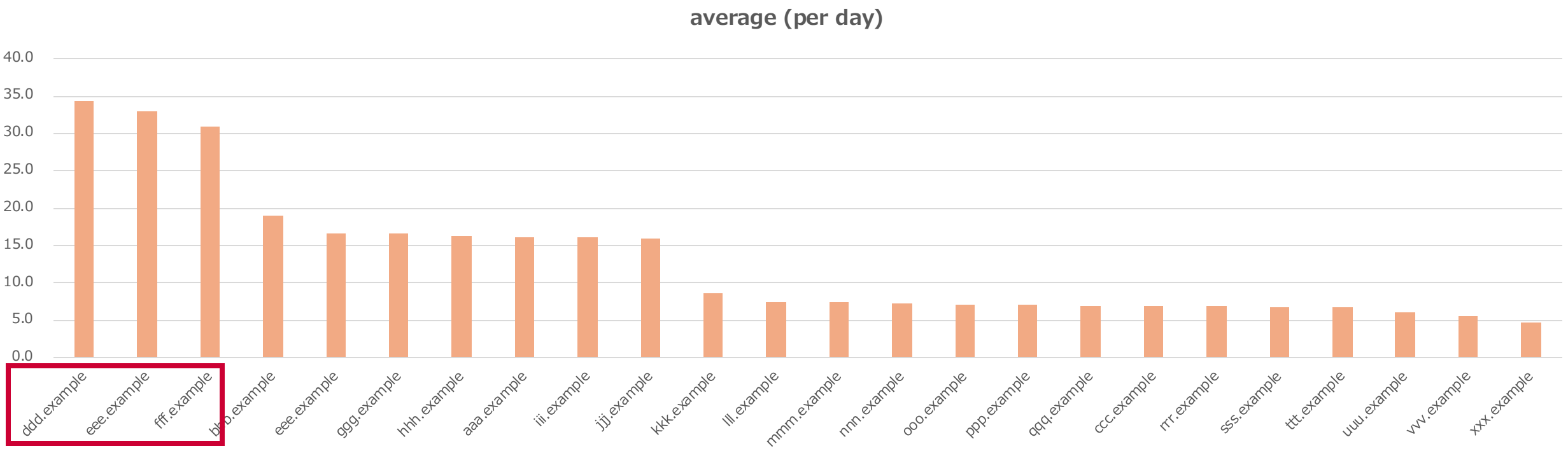
"_dmarc.example.com"



7/1 ~ 11/11 までの DMARC クエリ件数

利用終了ドメインへのDMARCクエリ

- 利用終了ドメインはメールの送信元としても使われていないため、これは利用終了ドメインを送信元とした「なりすましメール」が送信された可能性を示している
- ddd.example、eee.exampleはかつて提供していたサービスに関連するドメイン
- fff.exampleは前述したスポーツチーム (ccc.example) の偽サイト防止の為に取得したドメイン



7/1 ~ 11/11 までの DMARC クエリ件数

DNSレコードの設定

今回調査対象とした利用終了ドメインでは、以下のレコードを設定し「なりすましメール」に対する対策を講じた

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

あらゆる送信元IPからのメールを不正メールとして処理する

- DMARC: *"v=DMARC1; p=reject; aspf=s"*

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

- MX: *0 .*

レコードが設定されたドメインへのメールの受取が拒否される

ComNICでは、利用終了前の独自ドメインについてもメールに使用しない場合には上記の設定を推奨とすることを検討している。

分析過程で発見した事例2

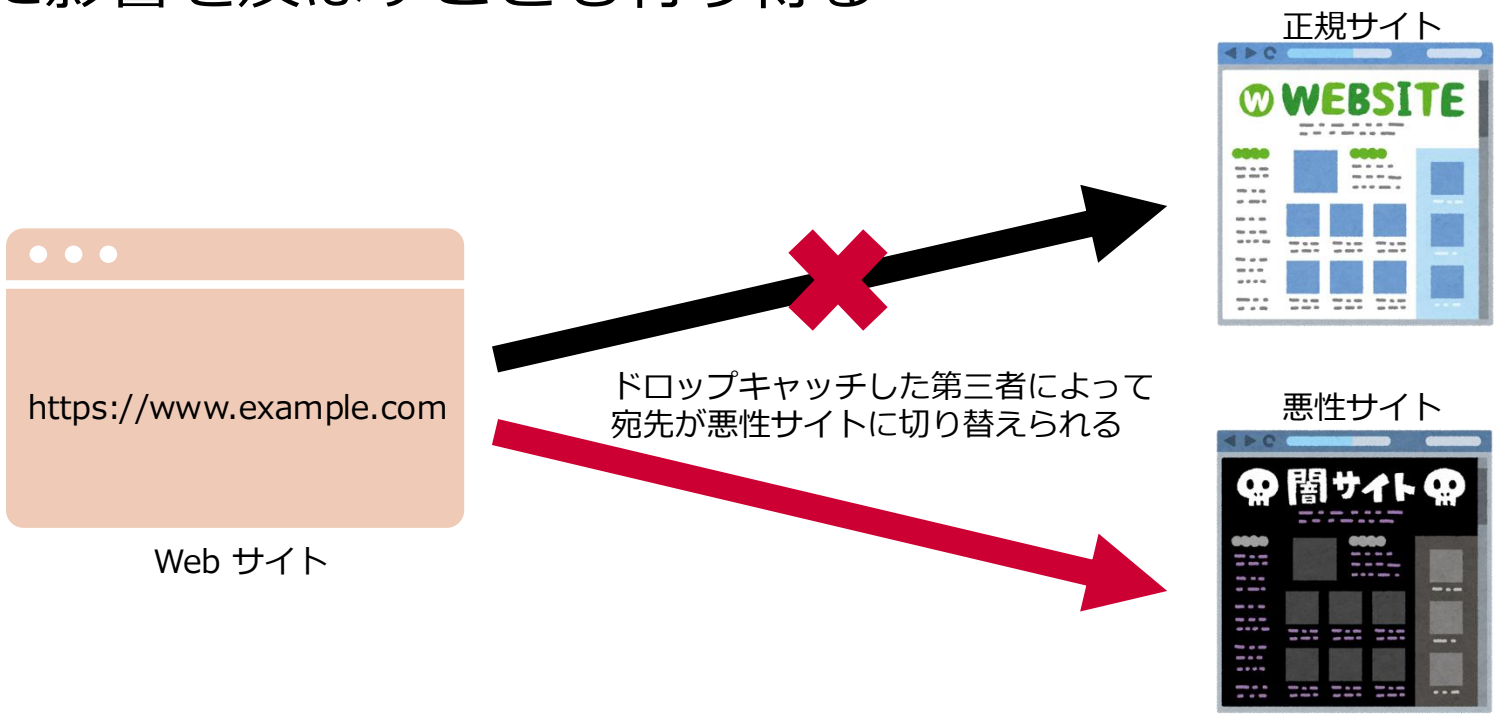
利用終了ドメインを破棄する際にドロップキャッチは大きな懸念事項になる

今回は収集したWebアクセスログを利用してドロップキャッチによるリスクを緩和するための対策を行った

残存リンクの危険性について

Webサイト上に廃止済みドメイン宛のリンクが残存していた場合、
そのドメインをドロップキャッチされると一般ユーザが意図しないサイトに
誘導されることになる

これはユーザを危険にさらすだけではなく、そのドメインの元々の所有者の
社会的信用に影響を及ぼすことも有り得る



Referrerをもとに残存リンクを調査

Web アクセスログに含まれる Referrer を参照することで訪問者が
どのサイトから来たのかを確認することができ、そのサイトには残存リンクが存在する可能性がある

ただし、Referrerにはpathを含めた全てのURLが残る場合とpathが残らない
場合がある

< path あり >
https://www.acquia.com/jp/blog/acquia-japan-celebrates-winners-of-acquia-certification-awards-japan

< path なし >
https://ja.m.wikipedia.org/

Google Dorksによる残存リンクの調査

今回はGoogle Dorksを用いて残存リンクの調査を行った
(Google Dorks: Googleのクエリオプションを活用した調査手法)

今回は下記のクエリで検索を行い複数の残存リンクを発見することができた

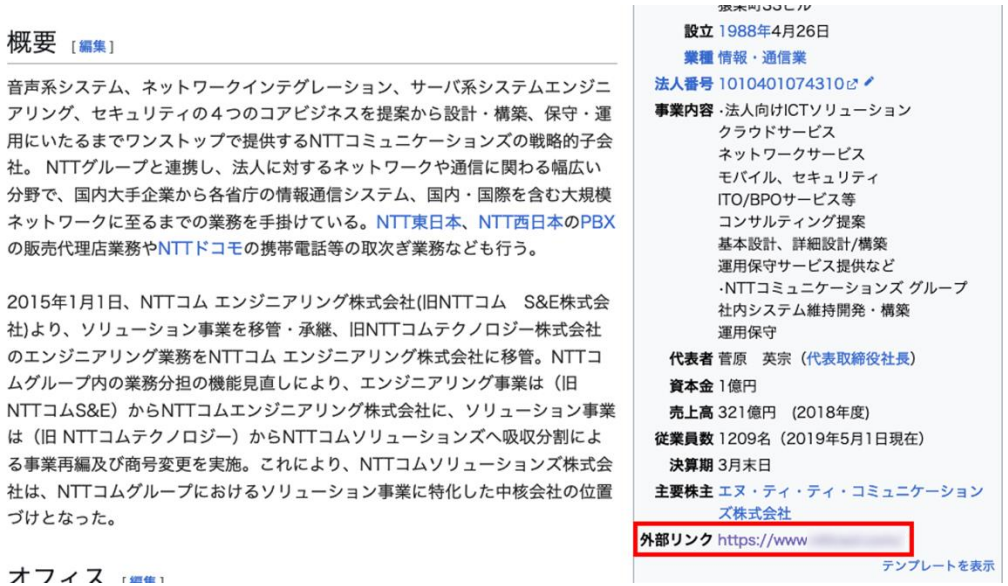
< 検索オプション >
site:<referrer から確認したサイトのドメイン> *link:*<利用終了ドメイン>

< 検索例 >
site:wikipedia.org link:bbb.example

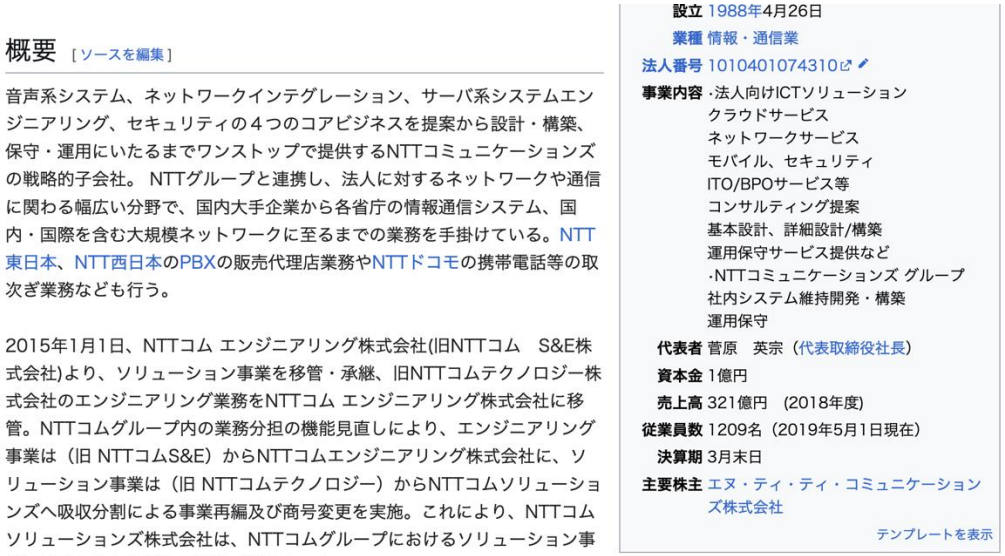
残存リンクの削除

- 今回発見したWikipediaの残存リンクは自ら削除することができた
- 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



まとめ

まとめ

- NTTコミュニケーションズにおけるドメイン管理について紹介した。
- ドメインの永年保有には課題があり、ドメイン廃止の目安を評価することを目的としたログ観測・分析を行った。
- ドメイン廃止の目安の評価には至らなかったが、全体傾向と調査の過程でドメイン管理において有益な成果があったので今回はそれについて報告した。
  - ドメインを廃止する際に懸念されるドロップキャッチなどのリスクを緩和するために有効な、残存リンクの調査と消去を行った。
  - 一方でログを分析する過程で「なりすましメール」によるドメインを保持することによるリスクが明らかになったため、各種レコードを設定することで対処した。
- 今後も収集したデータの分析を継続することで、適切なドメイン廃止のタイミングを評価し別場での発表をしたい。

ご清聴ありがとうございました