Yahoo!メールにおける Abuse対策の最新事情

LY Corporation / Communication Company

Masaharu Nakamura

LINEヤフー

自己紹介

中村 成陽（なかむら まさはる）

2013/04〜 経路探索サービスを提供する会社 エンジニア

2016/11〜 ヤフー株式会社(現 LINEヤフー株式会社) エンジニア

Yahoo!メールの迷惑メール対策チームに配属

2020/04〜 チームのマネージャーとなる

2021/10 “第11代黒帯〜メッセージング技術〜” を拝命

2022/10 “第12代黒帯〜メッセージング技術〜” を拝命

JPAAWG

3rd General Meeting
「**Yahoo!メールにおけるなりすましメール対策 DMARC導入とブランドアイコン表示**」

4th General Meeting
「**現場発！メールサービスを支える運用者の集い 2021 秋**」

5th General Meeting
「**大手メールサービスにおけるセキュリティ・なりすまし対策の最新の取り組み**」

Agenda

01

直近のフィッシングメールの流行状況

02

日本におけるスパムメール対策の難しさ

03

Yahoo!メールでのフィッシングメール対策
〜 スパムメールの対象データ蓄積

04

Yahoo!メールでのフィッシングメール対策
〜 DisplayName / TLD 不整合検知

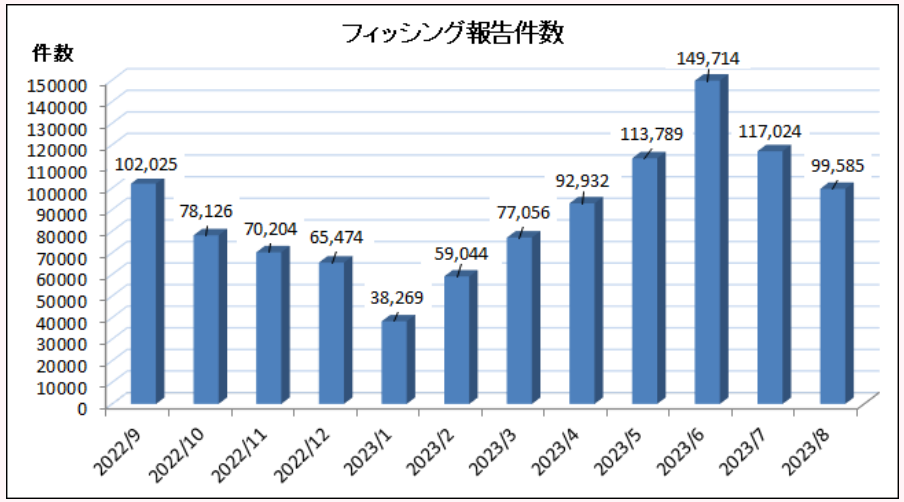
05

さいごに

直近のフィッシングメールの流行状況

直近のフィッシングメールの流行状況

- フィッシング対策協議会が発表しているフィッシングの報告件数は増加傾向

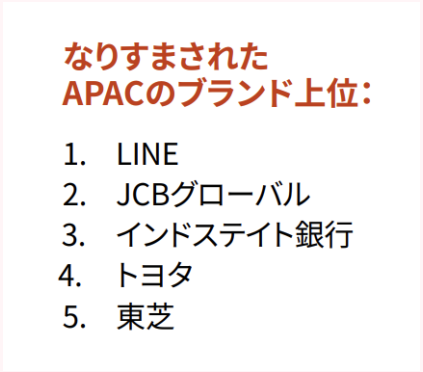


※コロナ禍前の2019/06には6,218件
（出典：https://www.antiphishing.jp/report/monthly/202308.html）

- Yahoo!メールを利用しているユーザーからの関連問い合わせも直近増加している
- 大手ECや銀行などを騙るフィッシングメールが後を絶たない

直近のフィッシングメールの流行状況

- Cloudflare が8月に発表した「フィッシング脅威レポート2023」によると
  フィッシング詐欺でなりすまされたブランドの
  日本を含むアジア太平洋（APAC）地域1位は LINE であった



（出典：https://release.nikkei.co.jp/attach/660827/03_202308171055.pdf）

- Yahoo!メールで受信したメールの DMARC の認証失敗通数は
  2023年9月の一ヶ月分で昨年の同月比で約 69.2% の増加となっている

日本における
スパムメール対策の難しさ

ユーザー嗜好

日本におけるスパムメール対策の難しさ

- （あくまで私見）日本のメールユーザーの嗜好
  - 届くはずのメールが届かない（誤検知）を非常に嫌う傾向にある

- 必要十分にスパムメールをブロックするのが理想だが、これは非常に難しい
  - フィッシングメールは日々巧妙化しており、対策をしてもいたちごっこ
  - そもそもそのメールが必要かどうかはユーザーによって異なる

- 厳しい条件によるメールブロックは技術的には難しくないが、現実的でない
  例）送信ドメイン認証に通過していないメールは全てブロックする、など…

- 可能な限り誤検知をなくす方針で対策を講じることになる
  - つまり検知漏れは増加する

法律

日本におけるスパムメール対策の難しさ

- 個人情報保護法や通信の秘密といった法律に準拠する必要がある
  - ユーザーのためのスパム対策であったとしても、
    個人情報を含む情報には最大限配慮する必要がある
  - 流行しているスパムメールの解析、分析をするとしても、
    通信の秘密（いつ誰とどんな通信をしているかといった情報を、
    第三者に知られないということ）に関する課題は常につきまとう

- 新しい対策を検討しても常に法務との確認が必要となり
  対応ができない、あるいはできたとしても
  当初よりも効果が薄いと見込まれてしまう方法での導入しかできないケースも多い

- DMARCの導入に関しては
  これらについて法的な留意点を総務省が整理し、公開している

まとめ

日本におけるスパムメール対策の難しさ

- 法律を遵守した上で、約款の範囲内でルールベースのスパムメール対策を行うことになる

- ユーザー嗜好から誤検知によるスパム判定を可能な限りなくす方針とせざるを得ない
    - 一方で検知漏れによるすり抜けにも厳しい意見はいただく

この前提のもと、Yahoo!メールでは様々なフィッシングメール対策を行なっています

スパムメールの対象データ蓄積

Yahoo!メールでのフィッシングメール対策

スパムメールの対象データ蓄積

Yahoo!メールでのフィッシングメール対策

対象のスパムメール

- 根強く届き続けているウイルス添付ファイル付きメール
    - 有償会員向けにウイルススキャンサービスを提供しているが全ユーザーに対策を提供する

- 性的脅迫を行いビットコインアドレスへの振り込みを要求するセクストーションメール
    - 5年ほど前から断続的に流行している
    - 内容がセンシティブであることから、受信時のユーザー問い合わせが多く発生してしまう

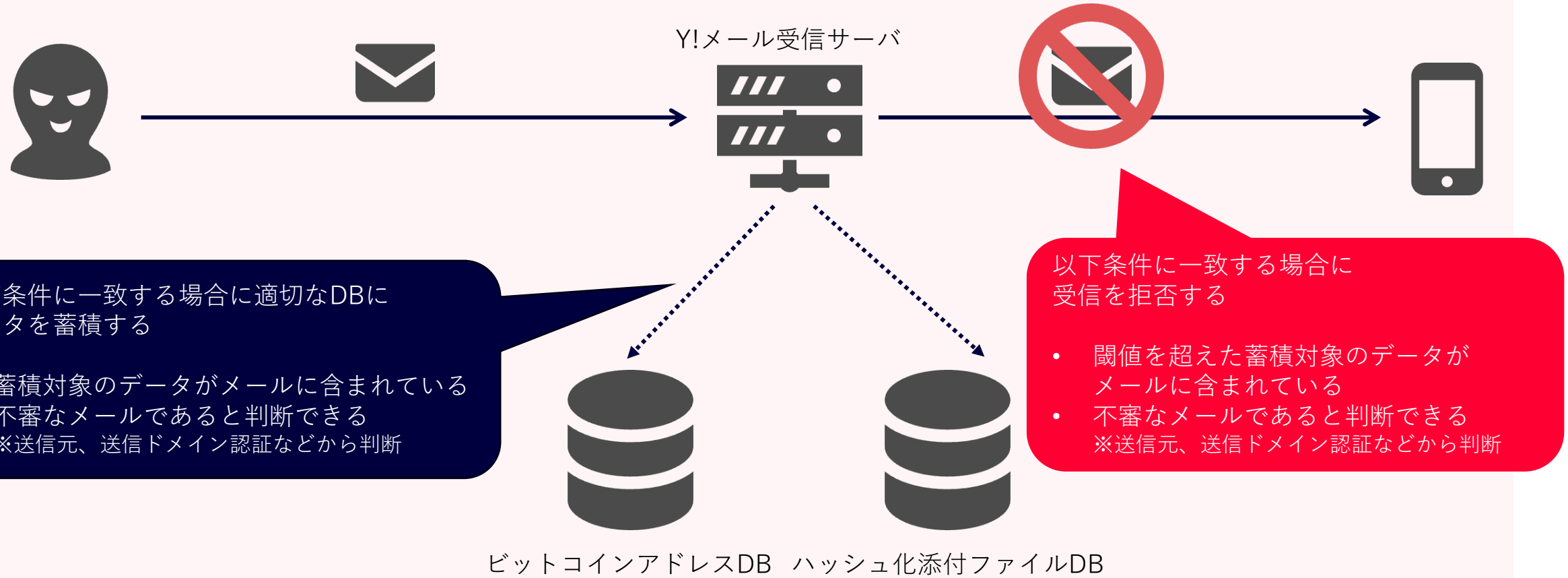
対策概要

- 不審な送信方法の対象データ※ を蓄積し、
一定期間に閾値を超える通数を受信した場合にそのメールの受信を拒否する

※ハッシュ化した添付ファイルデータ、ビットコインアドレス

処理の流れ

スパムメールの対象データ蓄積



スパムメールの対象データ蓄積

Yahoo!メールでのフィッシングメール対策

Achievement

- 多い日では数100万通程の該当メールをブロックしている
- セクストーションメールの受信に関する
  ユーザーからの問い合わせはほぼ 0 になった
- Y!メールからの送信の場合でも同様のDBを参照し
  不正利用防止に役立てている
- ハッシュ化添付ファイルについては特許を取得（特願2017-215181 /特開2019-087902）

Assignment

- 閾値に到達するまでには受信をしてしまうことになる
- データの蓄積、およびブロック対象とする
  「不審なメール」の判定条件はチューニングが必要

DisplayName/TLD 不整合検知

Yahoo!メールでのフィッシングメール対策

DisplayName / TLD 不整合検知

Yahoo!メールでのフィッシングメール対策

対象のスパムメール

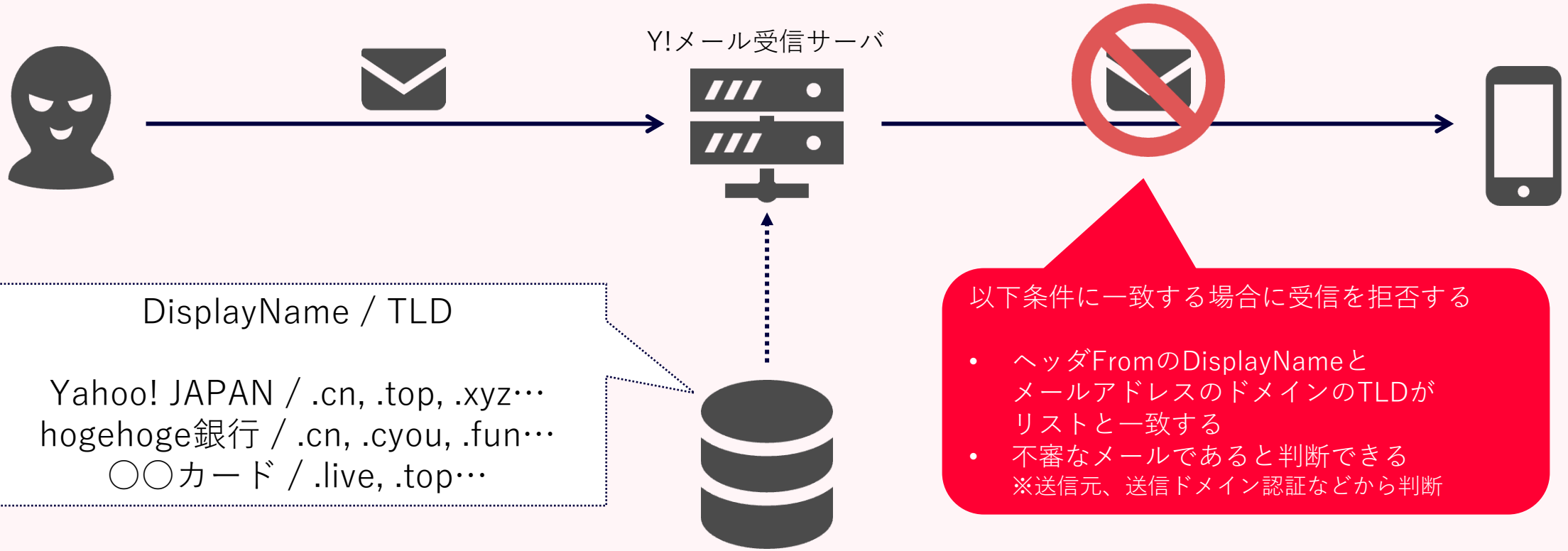
- フィッシングメールのうちDisplayNameで有名サービスを詐称するもの
  - 例）From: Yahoo! JAPAN <yahoojapan@example.xyz>
  - こういったメールはDMARCでのブロックができないため、課題となっている

対策概要

- 詐称されたサービスを表すDisplayNameと
  そのサービスで利用されないトップレベルドメインの組み合わせの場合に受信を拒否する

処理の流れ

DisplayName / TLD 不整合検知



DisplayName / TLD 不整合検知

Yahoo!メールでのフィッシングメール対策

Achievement

- 多い日では数1500万通以上の該当メールをブロックしている
- DMARCでは捕捉しきれないDisplayNameを詐称した
  フィッシングメールをブロックできる

Assignment

- 自社以外、対象サービスが正規のメールで利用している
  メールアドレスのドメインは自分達で収集せざるを得ない
- データの蓄積、およびブロック対象とする
  「不審なメール」の判定条件はチューニングが必要

さいごに

- 「ユーザー嗜好に合わせ可能な限り誤検知を減らす方針で、
  法律の範囲内で様々なスパムメール対策を実施する」というのがYahoo!メールでの方針
- 今回紹介した以外にも様々なロジック（ルールベース）や技術を利用した
  スパム対策を行なっている

- 受信側であるYahoo!メールのみでの対策では限界もあるため
  メールの送信を行う皆さんにも以下の対応を是非お願いしたい
  - DMARCへの対応（ポリシーのquarantine or reject化）
  - BIMIやYahoo!メールブランドアイコンへの対応
  - 正規メールで利用されるメールアドレス等の情報展開

LINEヤフー