JP AAWG JAPAN ANTI-ABUSE WORKING GROUP

IT初心者向けメールセキュリティ

2025/02/27

ソフトバンク株式会社 熊沢明生

【講師紹介】
ソフトバンク株式会社
熊沢 明生

【経歴・担当業務】
2007年1月1日入社(中途採用)
メールシステムの開発業務を18年やってます。
当時も迷惑メールが多い状況。
サーバ高負荷を回避対策を実施するのが日課でした・・

JPAAWG

トレーニングの目的

電子メールは、注意をして利用しないと本人が意図するしないに関わらず
自身や会社に大きな被害 をもたらすことがあります。

今回はメールセキュリティトレーニングを通して**安心・安全にメール**
を利用できるように知識を習得 しましょう。

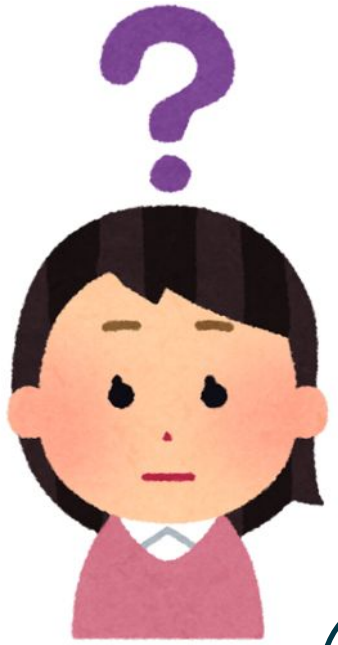
・電子メールについての基礎的な知識の習得
・電子メール利用における危険性の認識
・電子メール利用を安心して利用するための勘所

電子メールの基礎知識

- メールアドレス
- 電子メールの配送概要

JP AAWG

いまさら、電子メール？



普段、SNSを利用して
います。電子メールは
使っていません

現在でも色々な場面で利用されています
- 多くの企業が電子メールを利用している
- 長くビジネスで利用されてきた実績
- 世界中の多くの人も利用している
- 送受信に費用がかからない
- 証跡が残る。（法的にもログが有効）

SNS/コミュニケーションツール

- 1社のサービスや製品に縛られる
- **運営会社の方針変更 で利用サービス内容の変更や課金内容が大幅に変わる**
- **運営会社が倒産等するとサービス自体が 利用不能になる事も 。**
- 高機能/高い利便性

email

- **RFCで定義された標準 規格** であり
  好きな製品の利用や
  自分で開発する事もできます。
- インターネット初期からの
  コミュニケーションツールとして発展。
  インフラが脆弱な国でも利用ができるよ
  うになっており **世界中の人が利用可能** です。

JPAAWG

電子メールアドレス

電子メールを利用するにはメールアドレスを利用して相手を特定します。

taro@example.co.jp

ローカルパート

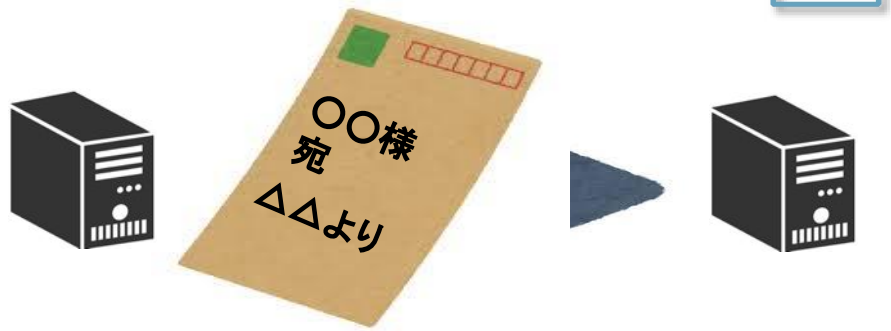
ドメイン

ローカルパート はそのドメイン内の誰かを特定するために利用します。
ドメイン はインターネット上での住所（場所）を表すものとして例えられます。電子メールでは組織を表すものとイメージすると理解しやすいかもしれません。
上の例では　example.co.jp に所属する taroさん宛のメールアドレスを示す例になります。

電子メールの要素

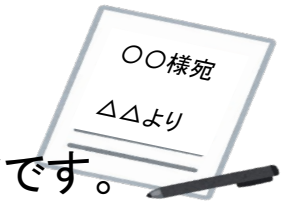
電子メールには大きく分けて3つの要素があります。

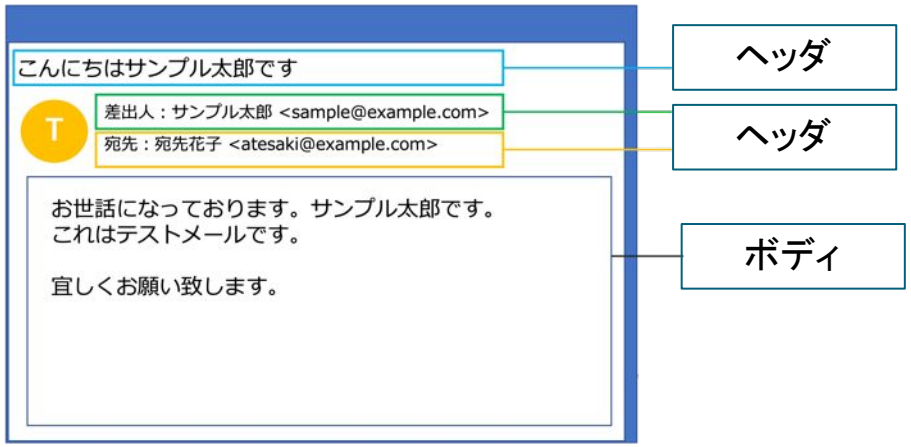
1. **エンベロープ**
   サーバがメール配送時に用いる宛先や差出人情報等になります。通常、メールクライアントはエンベロープ情報を表示しません。

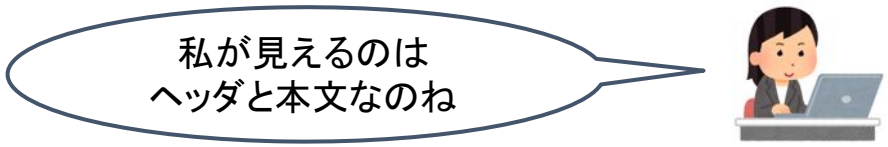


2. **メールヘッダ**
   メールクライアントが表示する差出人、宛先の情報になります。

3. **メールボディ**
   いわゆるメール本文や添付ファイル等のコンテンツです。

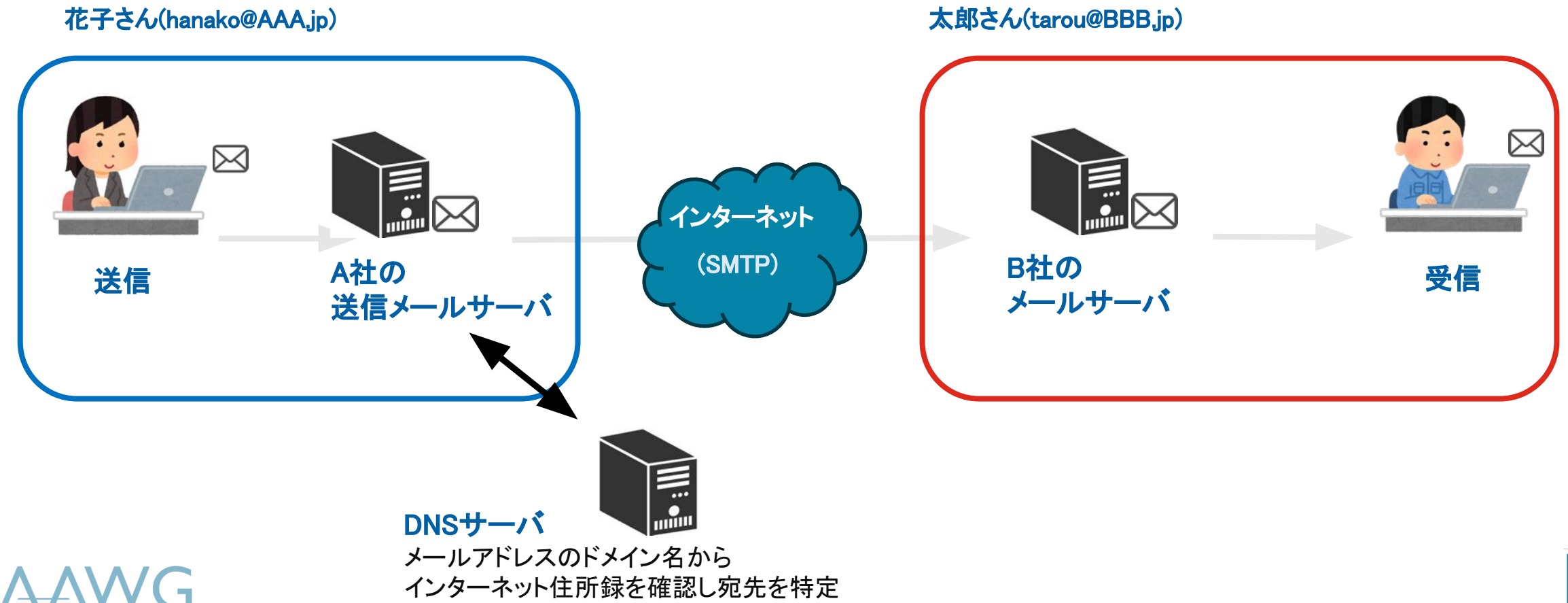






電子メールの配送

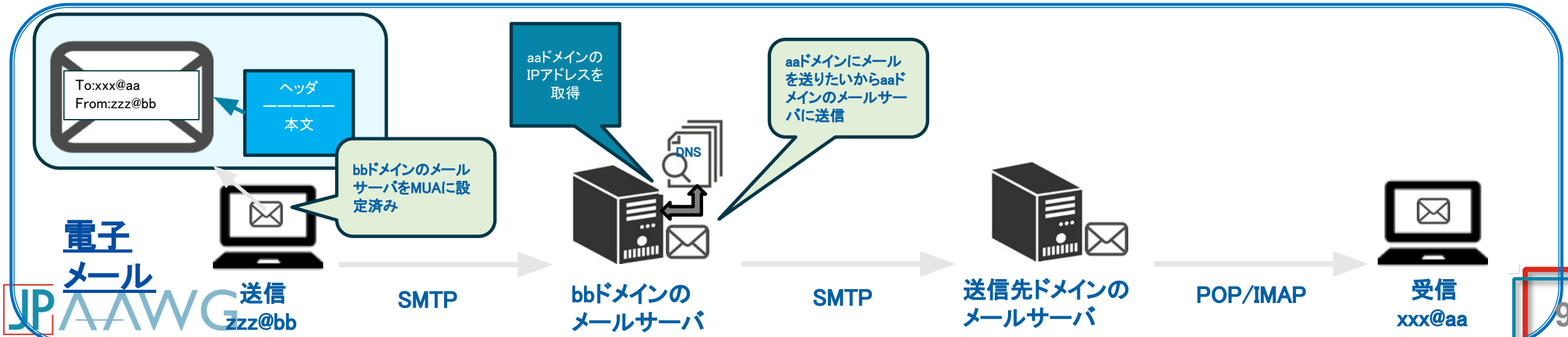
電子メールはどのように配送されるのでしょうか？
花子さんから太郎さんへメールを送付するイメージを説明します。



SMTPの概要

少しSMTPについて掘り下げます。

#	必要な主な情報	内容
1	送信者情報	自分のメールアドレス
2	受信者情報	相手先のメールアドレス
3	送信先サーバの情報	送信を依頼するメールサーバの情報。 メールクライアントには通常自分が利用するメールサーバの情報を固定的に設定します。
4	メール本文	メールの中身です。文章や添付ファイルが該当します。 メールヘッダとメールボディになります。
5	その他	オプション的な機能が多数あります。 例えばSMTPサーバに接続する時に認証を要求させたり、暗号化を行う機能等があります。



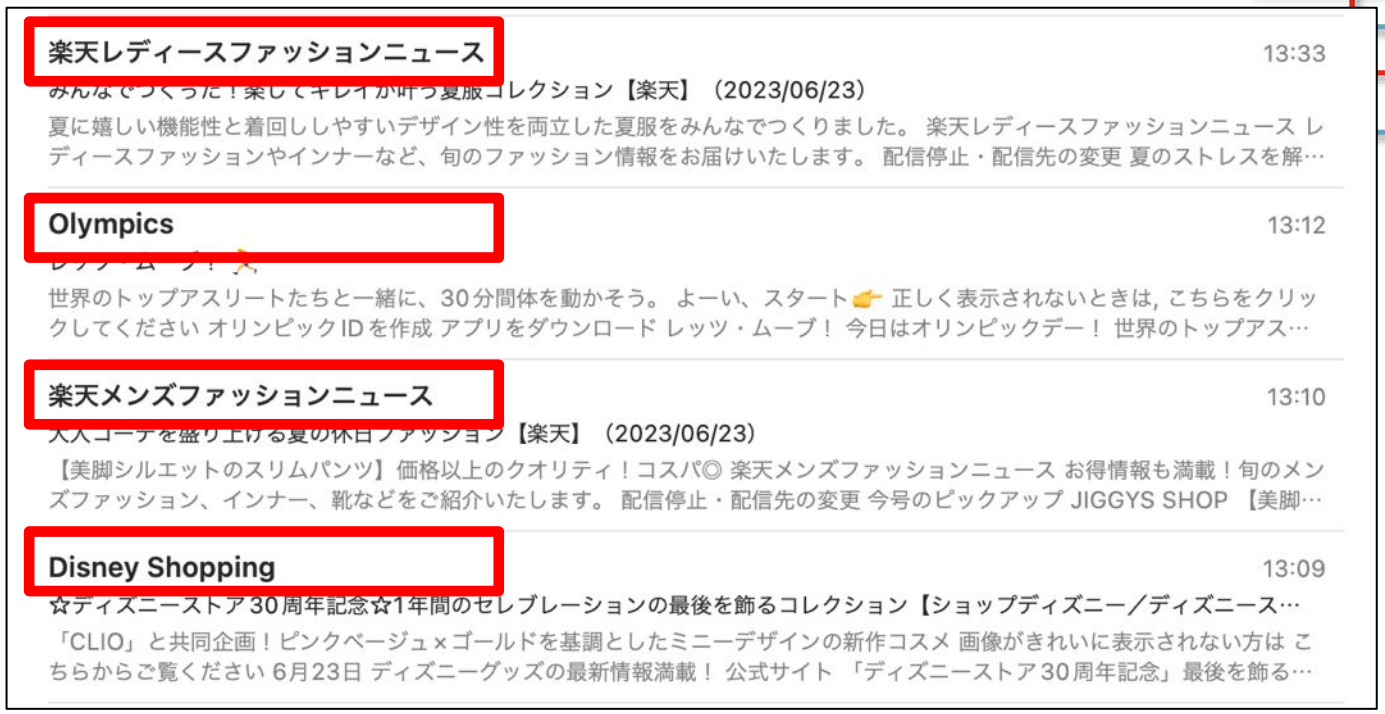
ディスプレイネーム

メールクライアントの設定によって差出人の情報がメールアドレスではなくディスプレイネームで表示される場合があります。

メール作成時にメールヘッダのFromヘッダの部分に送信者がディスプレイネームを設定することで表示が可能です。

例）
[ディスプレイネーム]<メールアドレス>

このディスプレイネームは送信者が好きに設定できますので最もらしい名称にすることで受信者に誤解を与えなりすましを行うことが可能です。



電子メールの基礎知識 まとめ

- ✔ SMTPとはメールを配送するためのインターネットプロトコルのこと
- ✔ SMTPはメールサーバ間でメール配送を行う場合とメールクライアントがメールサーバへメールを送る場合に利用される
- ✔ メールの配送はエンベロープ情報の宛先にメール配送される
- ✔ メールクライアントが表示する差出人、宛先はヘッダ情報を表示している
- ✔ ディスプレイネームを使うことで日本人にもわかりやすい差出人表示が可能

電子メールでの
セキュリティ被害

- 情報セキュリティの脅威
- サイバー犯罪とは？
- 主な電子メールを利用した
  セキュリティ被害

JPAAWG

この数字は？

401.9 億円 → **クレジットカードの不正利用被害**
（令和5年1月 － 9月）

474.6 %増
（前年比）
→ **インターネットバンキングの不正送金（約87.3億円）**（令和5年）

令和5年におけるフィッシングの報告件数は、119万6,390件(前年比で23.5%増加)と過去最多であり、クレジットカード事業者等を装ったものが多くを占めている。

※数値は警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」より引用

JPAAWG

(再び)この数字は？

3億2850万円

セキュリティインシデントに起因した組織あたりの年間平均被害額
（トレンドマイクロ社 2021年 報告）

企業が被る多数の被害


信用失墜

謝罪対応

事後対応


賠償や損害


業務停止

※数値は総務省の公開資料 「令和5年度版 サイバーセキュリティに関する問題が引き起こす経済的損失より　引用」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd24a220.html

JPAAWG

騙されただけなのに‥

私は何もしてないのに！

被害者

- 金銭的損害
- 業務影響
- 信用や株価の低下

犯人は私じゃない！！

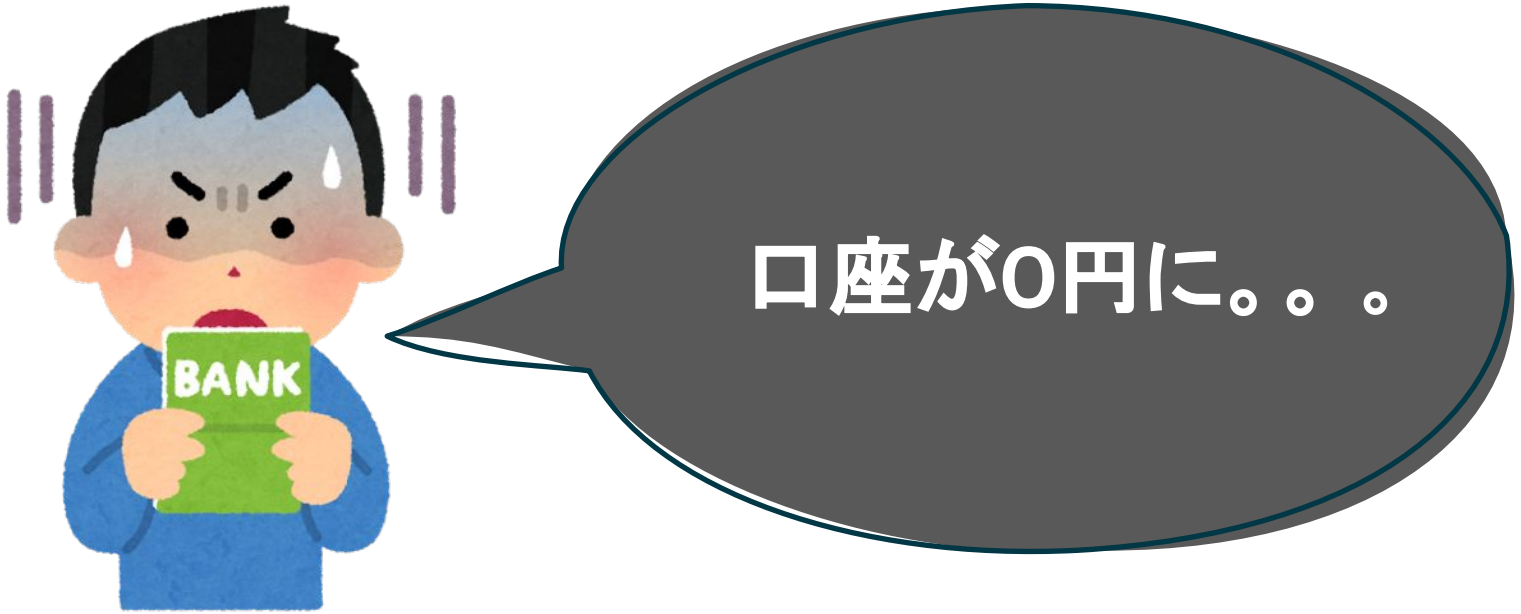
加害者

- 冤罪
- ウイルス拡散
- 踏み台

企業が被る多数の被害

個人が被る多数の被害

貯金がなくなる‥



信じられないかもしれませんが、実際にこのような事件が発生しています。

なぜ、こんなことが？？

サイバー犯罪の入口として電子メールが原因となる事例が多数報告されています。

サイバー犯罪とは？

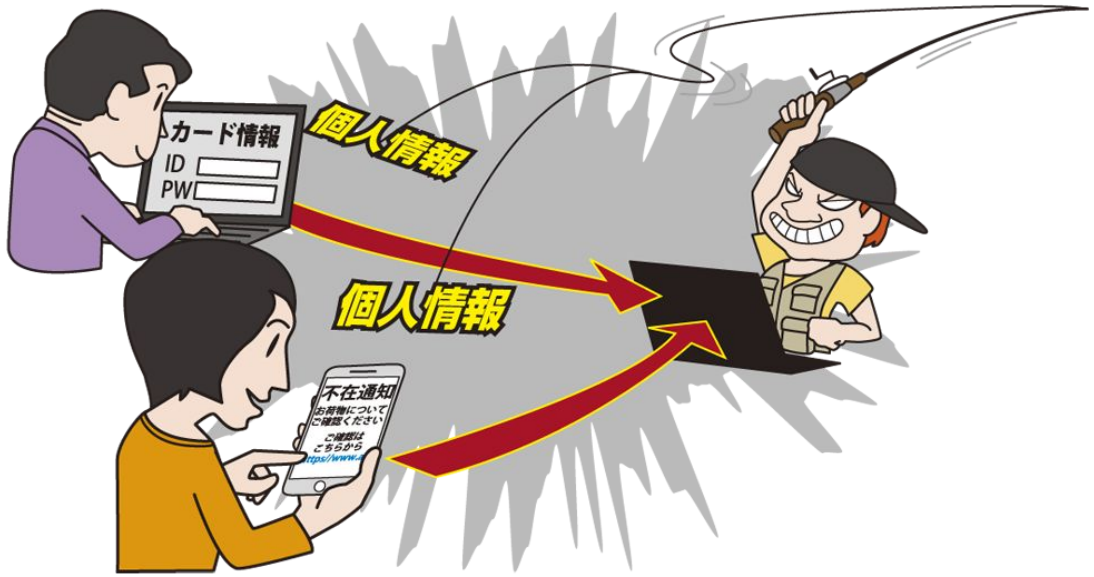
インターネット等の高度情報通信ネットワークを利用した犯罪
コンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪
（警察庁の定義）

特にお金や大切な情報が盗まれる
被害を**サイバー詐欺**と呼ぶ

情報セキュリティの脅威(2024)

情報セキュリティ10大脅威 2024(*)でも、メールを悪用した被害が注目。

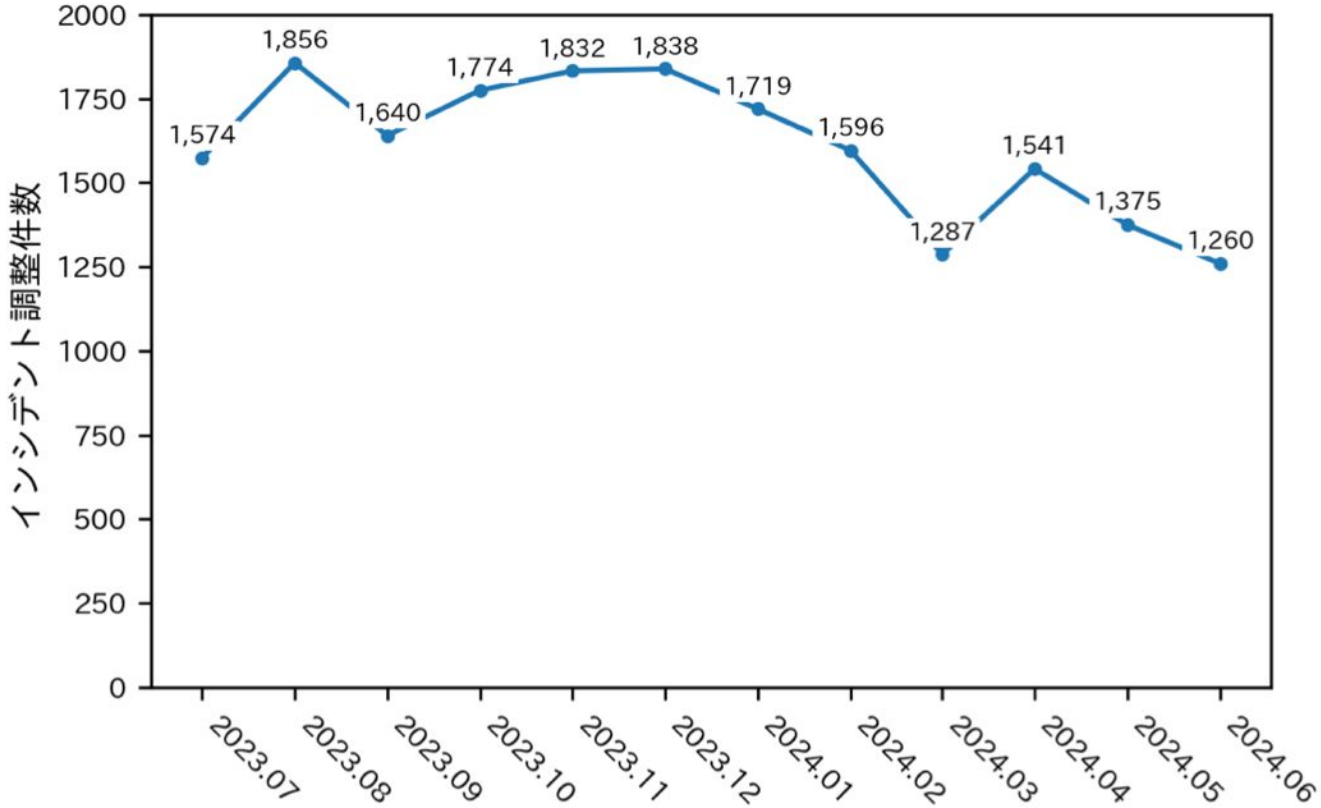
ビジネスメール詐欺による被害
（7年連続7回目）



フィッシングによる個人情報等の詐取
（6年連続6回目）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求
（6年連続6回目）

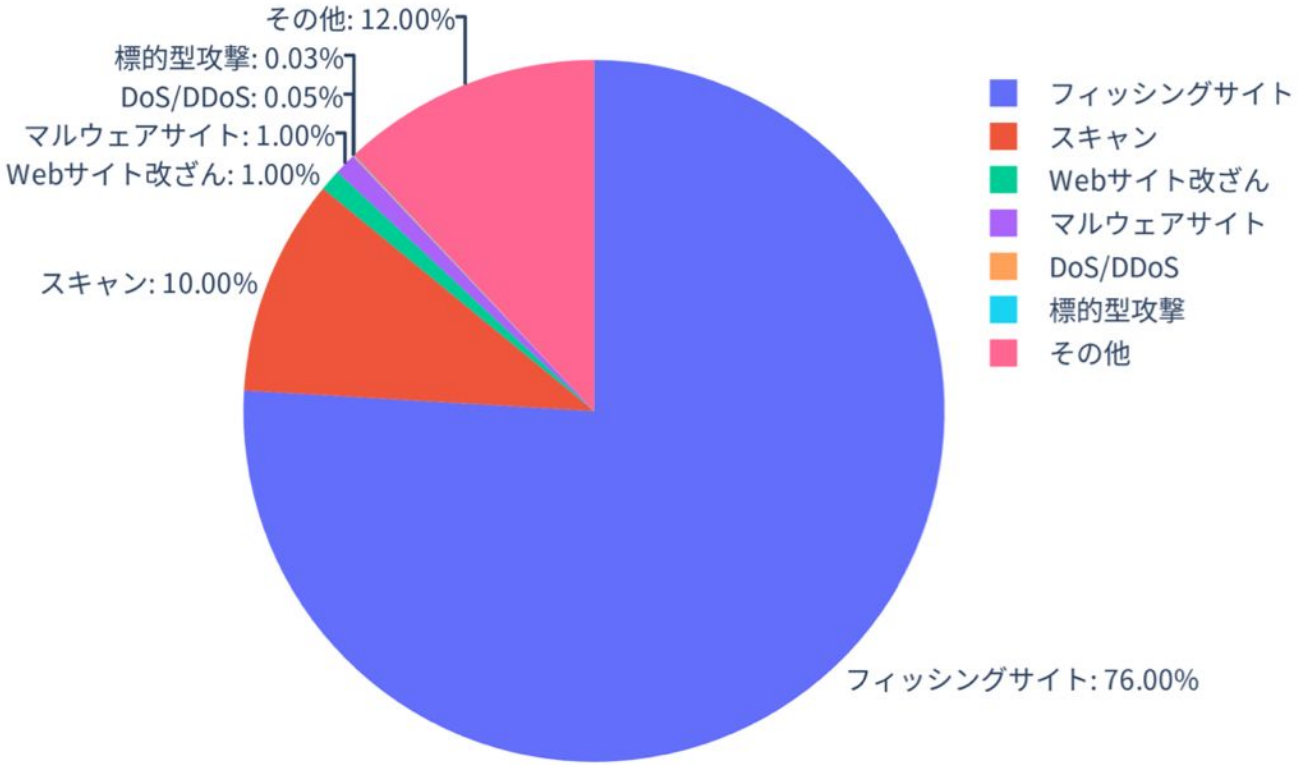
- https://www.ipa.go.jp/security/10threats/10threats2024.html

JPCERT/CCへのインシデント報告



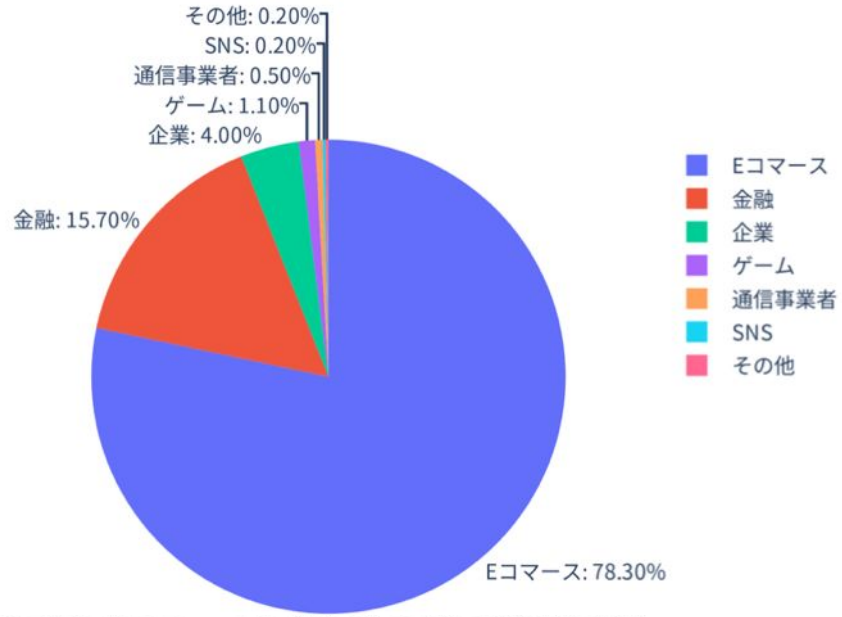
出典：JPCERT/CC インシデント報告対応レポート 2023年1月1日 ~ 2023年3月31日
JPCERT/CC インシデント報告対応レポート 2023年4月1日 ~ 2023年6月30日
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf

JPCERT/CCへのインシデント報告



インシデント報告件数のカテゴリー別内訳

国内ブランドのフィッシングサイトの件数の業界別の割合



国外ブランドのフィッシングサイトの件数の業界別の割合

出典： JPCERT/CC インシデント報告対応レポート 2023年4月1日 ~ 2023年6月30日
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf

昨今のセキュリティ被害状況

- 電子メール、SNSやSMSを利用したなりすましやフィッシングによる被害。
- マルウェア感染によるランサムウェア被害の増加

公的機関を語り 金銭を要求	「消費者庁」「国民生活センター」を語り、架空の和解金を要求するケースや警察のアカウントを装い個人情報を搾取する事例が発生しています。 現金の要求ではなく暗号資産で金銭を要求する事例も発生しています。
個人情報搾取 による金銭被害	フィッシングメール等から誘導したURLにアクセスをさせたり、なりすまし等にてアカウント情報やカード情報が搾取される金銭的な被害が多く発生しています。 特に昨今はオンライン決済が非常に増えてきており被害の増加が見えます。 決済サービスをしているサイトに直接攻撃を仕掛けアカウントを搾取する事例も増えています。
ランサムウェア による被害	Emotetに代表されるマルウェアを介し、ランサムウェアに感染をさせデータを人質に取り金銭を要求する事例が増加しています。 ランサムウェア被害に遭うとデータが利用できなくなり業務が停止するのみならず、データを外部に漏洩させると脅し金銭を要求されることになります。

電子メールでのセキュリティ被害

- ✔ セキュリティに関する被害報告は年々増加
- ✔ フィッシングによる被害報告が過半数以上を占める
- ✔ 公的機関等の権威や信用を持つものになりすまして情報を詐取したり、金銭を要求する事例が多い
- ✔ ランサムウェア被害が多く発生。業務停止だけではなく情報漏洩の危険もあり多大な損害が発生する場合も
- ✔ 闇バイトの勧誘にも電子メールが利用されている

被害に遭わないために

- 被害に遭わないために知っておくべきこと
- 基本的には自分で見抜こうとしない
- どうしても判断が必要な場合に見るべき点

JP AAWG

詐欺の手法(例)

返報性の原理

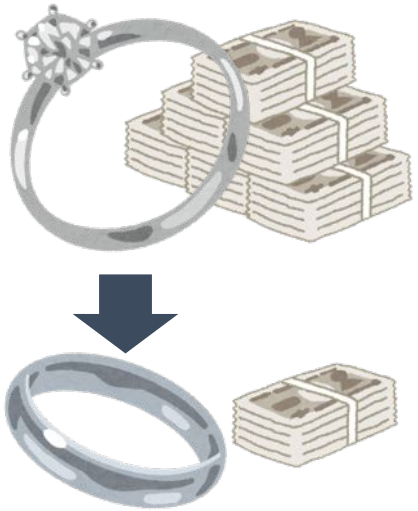
相手に優しい言葉をかけられたり、先にサービスを受けると、相手に協力したくなる心理

動揺→指示

相手を一旦不安にさせた後で、直後にその不安から逃れるための具体的な指示を行うと相手はそれに従いやすくなる。

ドア・イン・ザ・フェイス

最初に大きな要求を行いその後に最初の要求よりも小さな要求を行ううとで相手がこちらの要求を承認しやすくなる心理



どれも営業行為でよく使われる手法ですね。

JPAAWG

サイバー犯罪から身を守る

セルフコントロール能力とは「 より大きな満足を得るために目の前にある短期的な欲求充足を抑制することができる能力 」
サイバー犯罪対策には個人のセキュリティ意識が重要となりますが
この能力の低い人は、その行動から得られる短期的な満足への衝動を抑えることができずにリスキーな行動をとってしまう傾向がある。

1 思いつきで行動することが多い

2 ややこしくなってくると諦めやすい

3 ただスリルを味わいたくて時々危険なことをする

4 他の人に迷惑をかけることになっても、自分第一

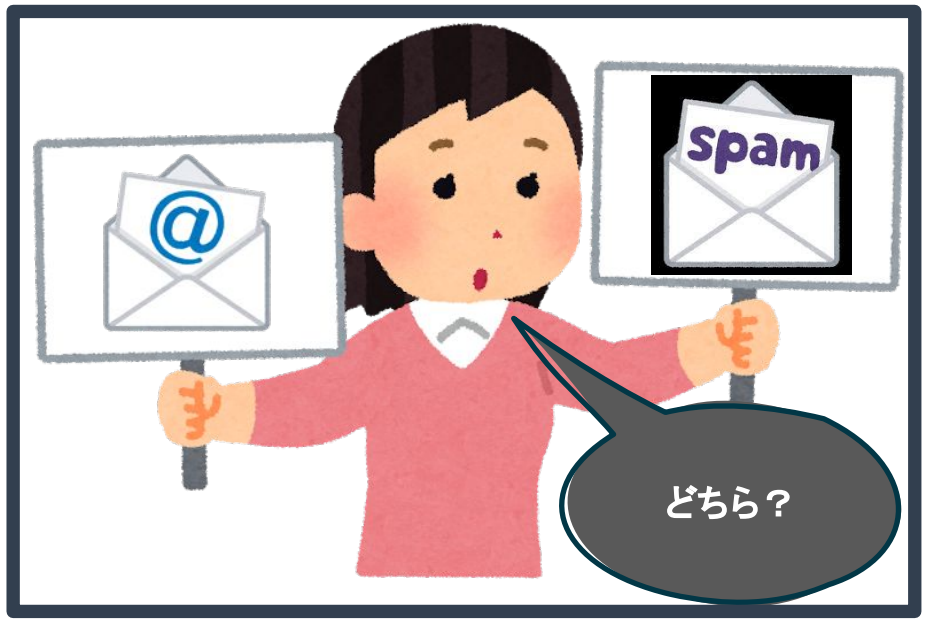
5 キレやすい

6 じっと考えるより、動き回っている時の方が気分が良い

7 誰かに対して怒っている時、理由を説明するよりその人をやりこめたり傷つけたい。

JPAAWG

これは迷惑メール？



検索して確認

気になる場合はメッセージ外の方法で確認する

- **文中URLではなく、検索エンジンを使い、サービス名で検索してアクセス**　する
  「◯◯銀行から緊急のお知らせ」-> 検索エンジンで◯◯銀行にアクセス
- URLは偽装可能なので見た目が大丈夫だからといってクリックせず必ずメッセージ外から確認する
- 文中にLINE IDが書かれている場合でもメッセージは送らない
  ->検索エンジンで公式サイトにアクセスして公式LINEアカウントを探す

JPAAWG

迷惑メールに返信すると

迷惑メールや不審なメールに
返信してしまうことで被害につながる

心情的には…	実際には返信してしまうと…
• もう送ってこないで欲しいので意思を伝えたい • 通報しました！と脅せば来なくなるのでは？	• 攻撃側はメールアドレスが生きていることがわかる • 「誰」がメールを読んだのかもわかる • やり取り型の攻撃の起点にもなる

攻撃者の認識

この受信者は迷惑メールを開いて読んでくれる＝カモ発見！

フィッシング被害に遭わないための基本

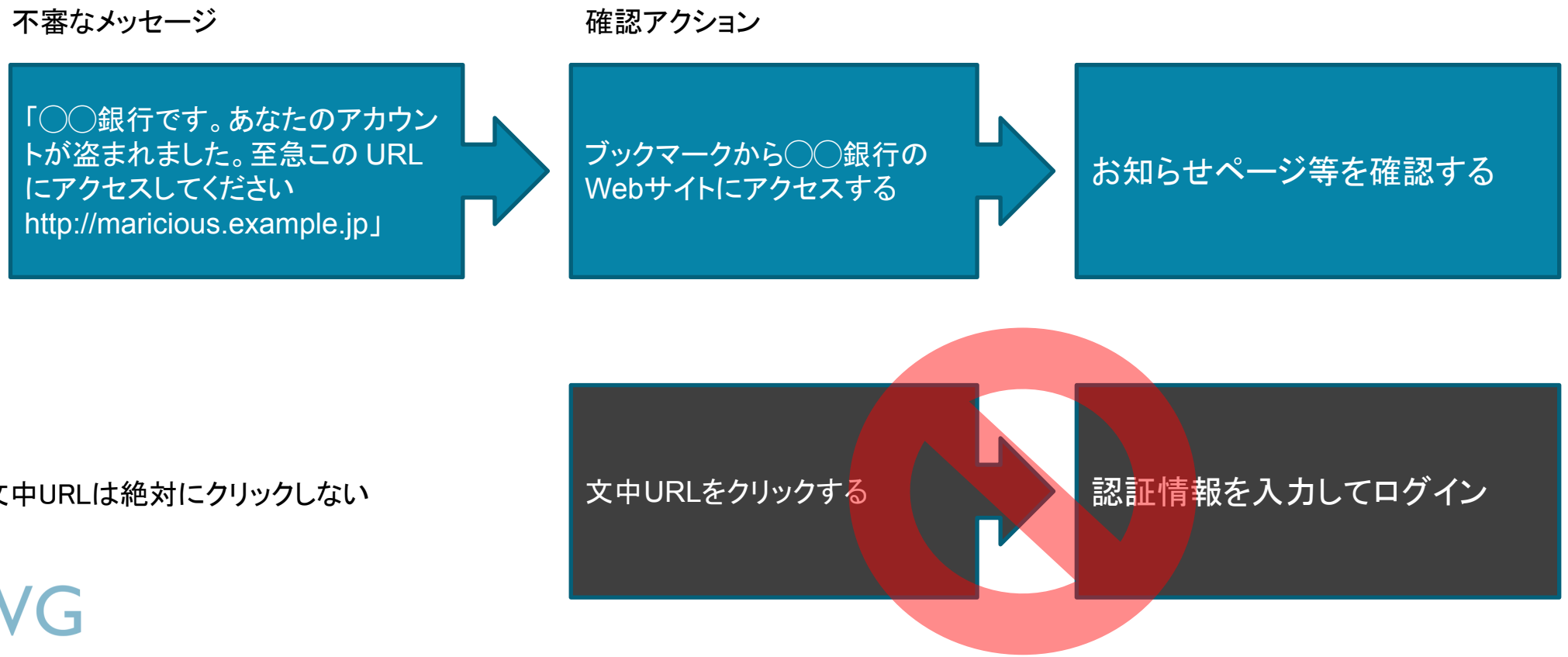
基本は**無視**

- 緊急性を煽ったり、危機感や射幸心を煽ったりとにかく受信者側の平常心を乱す
- 一旦深呼吸をしてから再度読み直し、冷静になることが大切
- **心当たりがなければ無視する** ことが一番

JPAAWG

正規サイトを登録＆確認

- サービスに**新規登録する際に正規サイトのURLをブックマーク**　しておく
- 以後、気になる点がある場合はそのブックマークを利用する
- サイトによっては正規URLや正規ドメインについての告知ページがある為、そこも参考にする
  →ただし、先述の通りURLは偽装が可能な為、見抜く材料にはしない



正規サイトを登録＆確認

- どこのサービスなのか不明なケースはクリックしがち
  -> 宅配便の様な自分でサービス事業者を選べないケースは要注意

- この様なメッセージはフィッシングの可能性が高い為、無視をする
- **少なくとも以下の会社はSMSでの不在通知を行っていない**　為、それらを名乗るのは全てフィッシング

佐川急便　：　https://www2.sagawa-exp.co.jp/whatsnew/detail/721/
ヤマト運輸　：　https://faq.kuronekoyamato.co.jp/app/answers/detail/a_id/2507/
日本郵政　：　https://www.post.japanpost.jp/notification/notice/fraud-mail.html

- 心当たりがある場合は通販サイトを確認し配送会社を確認後、その会社のWebサイトに検索エンジン経由でアクセスしてSMSでの不在通知をしているか確認する

日本語がおかしかった

ー昔前は海外の脅威アクターが送ってくるメールは日本語の文法がおかしかった

100万円当選した。今すぐ振り込めください。

あなたのパソコンにウィルスが検出しました。解決したい場合今すぐこの添付ファイルにインストールください。

- 正規メールをコピペしてURLだけ置き換える手法だとURL以外は正規
- **AI / Chat GPT** の発達によって攻撃者側も進化
  – フィッシングの為のキーワードを幾つか与えることで**きれいな文法のメールが作れる**
- 非日本語話者の外国人であっても**完璧な日本語** のメール送信が可能
  海外検証事例では、フィッシングメールではなく、正規メールのみにスペルミスがあったという結果も
- **文法が正しいから安全であるというような判断は命取り**

- **一部研究結果では悪意のあるメールの生成においてAI生成よりも人間作成の方が騙されやすいという結果もあります。**

セキュリティスキャンは完璧？

- 通常の企業の電子メールはセキュリティスキャナでスキャンされ保護されている
- スキャン済であれば安全と判断しても大丈夫か

ゼロデイ/ゼロアワー攻撃

- 発覚直後や公表前の脆弱性を突いた攻撃
- **定義ファイル更新が間に合わずセキュリティスキャンをすり抜けてしまう**　場合がある

暗号化された添付ファイル

- **暗号化されたファイルはセキュリティスキャナがスキャンできない**
- マルウェアが抜けてくる原因になる

セキュリティスキャナのチェックを抜けるものがあるため添付ファイルは100%安全とは限らないため、複数の要素で安全性を確認した方がよい

- 送信ドメイン認証をパスした正しい相手なのか
- パソコン側のセキュリティスキャンでも問題がでないか
- それでも不安な場合は電話で送信相手に確認を取る

被害に遭わないために

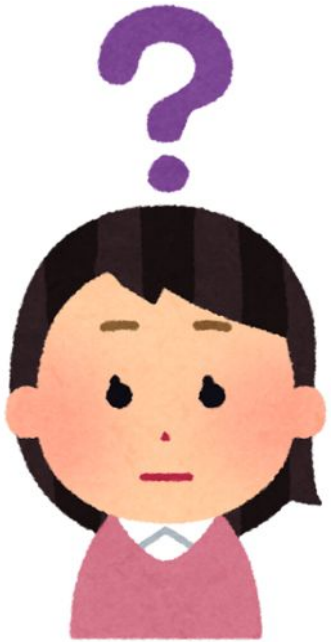
- ✔ 100%安全な対策は存在しない
- ✔ 見抜こうと思わない
- ✔ メールに記載のURLを安易に開かない
  あやしいと感じたら正規サイトを確認する
- ✔ 金融機関からクレジットカード番号やID/パスワードをメールでヒアリングすることはありません
  パスワードの再設定を促すメールはフィッシングメールです
- ✔ 知らない相手から高額のバイト勧誘は闇バイトの勧誘メールです

最後に

- メールサーバの対策

JPAAWG

電子メールは危険？



メールサーバで
対策できないの？

いいえ。
様々な対策を実施しています。
このあとのセッションで詳しく解説します。

Thank you for your listening!