JPAAWG若手メールエンジニア向け
メールセキュリティトレーニング(2025/2/27)

メールの受信防御の取り組み ～攻撃とは？そして防御とは？～

KDDI株式会社
中島　直規

2025/02/27

Tomorrow, Together
KDDI
おもしろいほうの未来へ。
au

お断り

本トレーニング資料は、

- 個人の見解を述べたものであり、会社・業界としての見解ではありません。
- 一部イラストには著作権フリーイラストを利用させて頂きました。
- 一部分かりやすくするために細かい事象等を省いて解説しております。

予め、ご了承ください。

講演者紹介

中島 直規
(Naoki Nakajima)

KDDI株式会社
エンジニアリング推進本部
プラットフォームエンジニアリング部

座右の銘

めげるな、しょげるな、いじけるな！
明日は明日の風が吹く！

[2007年～2011年]セキュリティ対応部門(SOC)

システム監査、NW/AP脆弱性診断
総務省サイバー攻撃対応演習運営

[2012～2018年]メール開発部門

主にISPメール設備開発を担当

[2018～2020年]メール運用部門

キャリアメール/ISPメール
運用リーダー

[2020年～]メールシステム　DevOps

KDDIメール設備の開発・運用全般(DevOps)

- 迷惑メールフィルタ
- メール配信システム
- メールボックスシステム

メール設備への攻撃手法（TwoFive様資料抜粋

各種攻撃手法

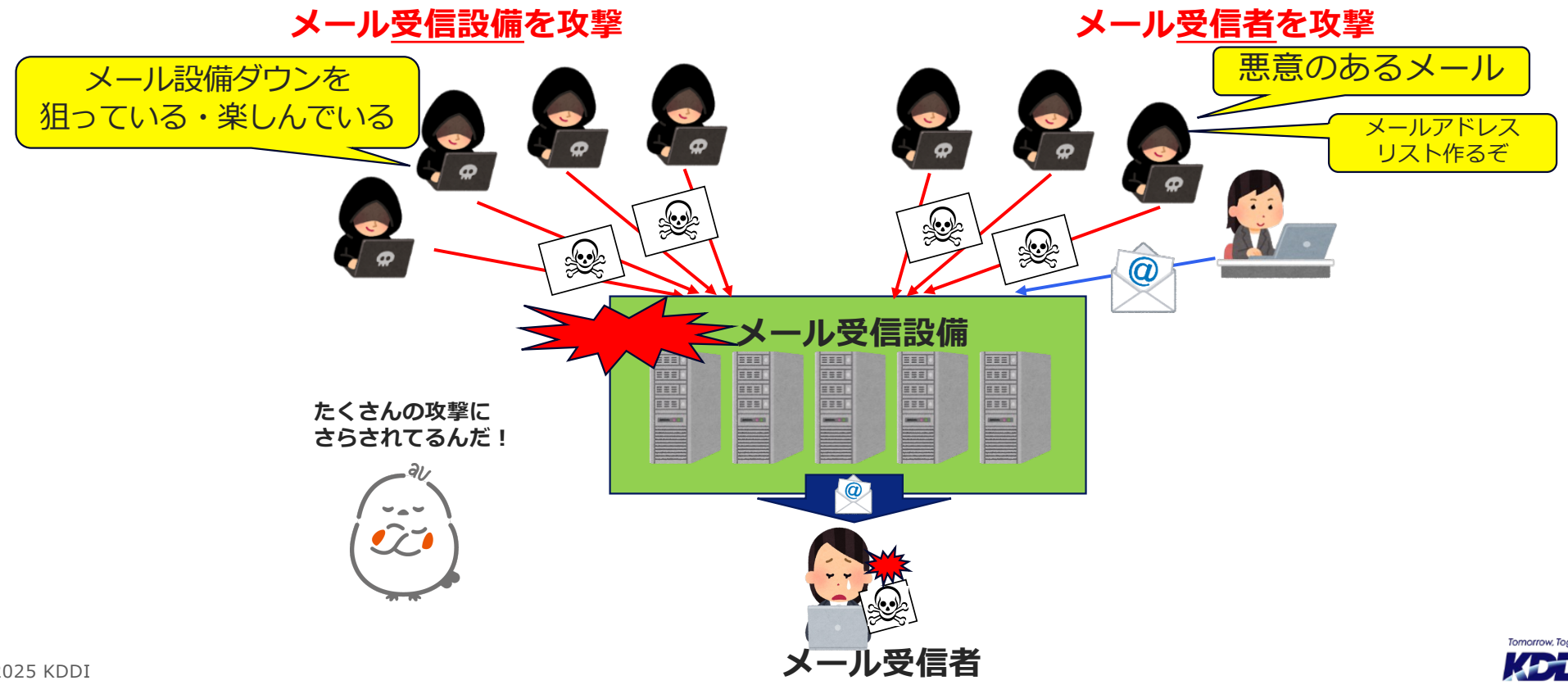
- メールサーバ側で考慮しないといけない攻撃手法は無数に存在する
- 以下は一例であり全てではない

攻撃手法	概略
DoS攻撃	大量のもしくは大サイズのリクエストやメールを送り付ける等によってサーバ機能をダウンさせる
メールボム	大量のメールを送り付けるDoS攻撃の一種
Zipボム	非常に大きなサイズのファイルをZip圧縮しファイルスキャナのリソース飽和を狙うDoS攻撃の一種
ブルートフォース攻撃	総当たりの手法でパスワード等を盗む
DHA(Directory Harvesting Attack)	総当たりの手法でメールを送り、エラーを解析してサーバ上のメールアドレスを一覧化する
バックスキャッター攻撃	送信元情報を偽装して、バウンスメールを攻撃に用いる
不正中継	正規の権限を持たないサーバを中継しメールを送信する
メール盗聴	経路上で電子メールを盗聴する

- 既知の攻撃手法はサーバ製品側の機能や設定で防衛可能なことが多い
- 古いサーバを長く使っている場合には定期的にバージョンアップの検討や、設定や設計の見直しを行う

メール「受信」への攻撃とは？

Eメール「受信」への攻撃は大きく分けてふたつ…
「メール受信者」への攻撃と、「メール受信設備」への攻撃



メール受信者への攻撃について

メール「受信者」への攻撃

「メール受信者」とは、
メールを正しく利用されているお客様のこと。

「攻撃」とは
　情報搾取（個人情報）を試みたり…
　マルウェア感染へ誘導したりして金銭搾取を行ったり…

3. auの迷惑メールを防ぐ仕組み(迷惑メールとは)

【迷惑メール】
受信者の意にそぐわないメール
・宣伝メール
・フィッシングメール

過去には**商品購入を狙うもの**（そして商品が届かないなど
今は**何らかの情報**を取得する目的の迷惑メールがほとんど
⇒　最終目的のほとんどは**主として“金銭搾取”**

金銭搾取に必要なIDやパスワードなどの情報を得る目的として
「フィッシングメール」で悪意のあるWebサイト・アプリへアクセスさせる

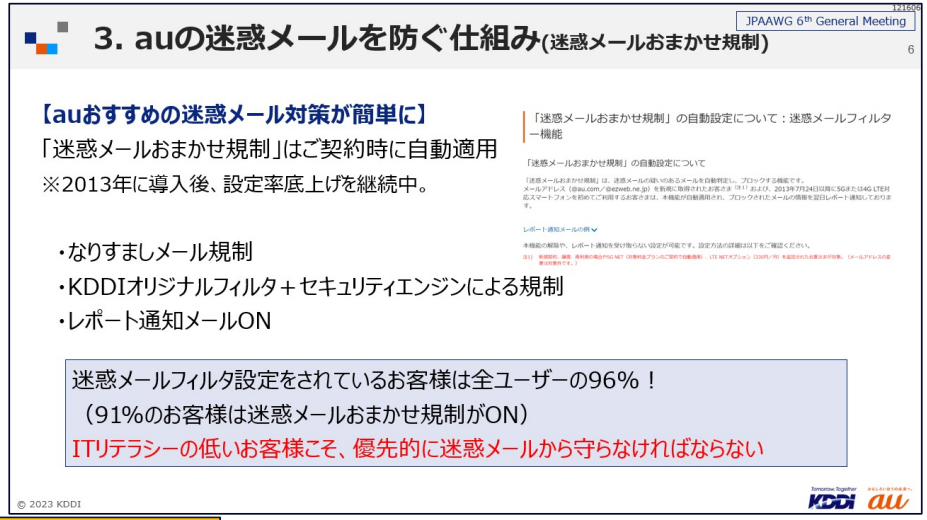
メール「受信者」への攻撃

「メール受信者」への攻撃
- 巧妙なフィッシングメールにより金銭的搾取
- 標的型攻撃・ランサムウェア等の感染により被害

攻撃者

「攻撃」のためのメールを送り付ける
- フィッシングURLへの誘導メール
- ランサムウェアのURL・添付
- 出会い系サイト等への巧みな誘導

メール受信者

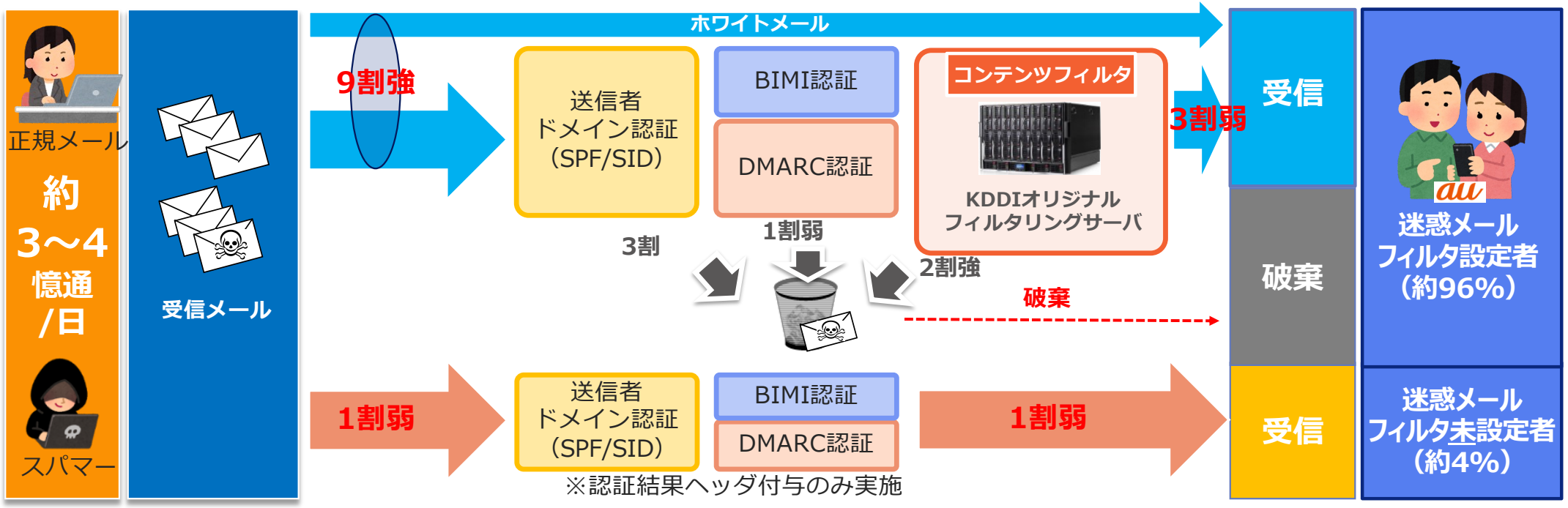


【被害の一例】
- フィッシングにより多額の現金を振り込み
- ランサムウェアにより大切な資料や写真などが暗号化され **大切なデータが毀損**＋身代金要求による**金銭・精神被害**
- 出会い系サイトへ登録してしまい**多額の課金**

メール「受信者」への攻撃（攻撃を見分けて防御

・送信ドメイン認証（SPF/DMARC等）で正当性を確認しやすくする
・DMARCポリシーを厳しくし、正しくなりすましメールを拒否する

※お客様個別設定のホワイトリストマッチなどは破棄せず



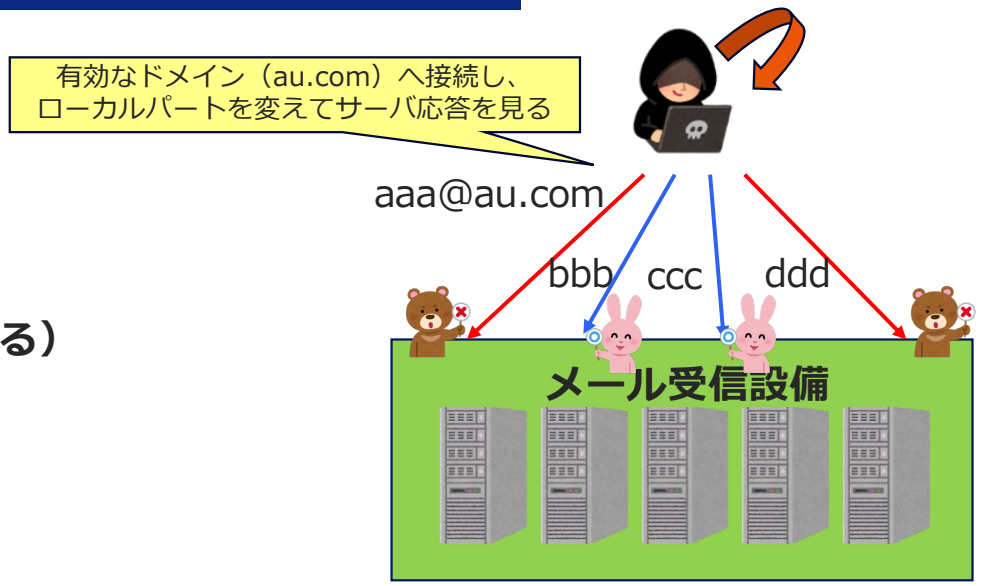
※認証結果ヘッダ付与のみ実施

メール「受信者」への攻撃（準備行為

「メール受信者」への攻撃の「準備」
- **メールが届きそうなメアドリストを準備**
- **短時間に高速に準備を行う**

DHA攻撃（Directory Harvest Attack）と呼ばれる

届いたメアド	届かないメアド
bbb@au.com	aaa@au.com
ccc@au.com	ddd@au.com



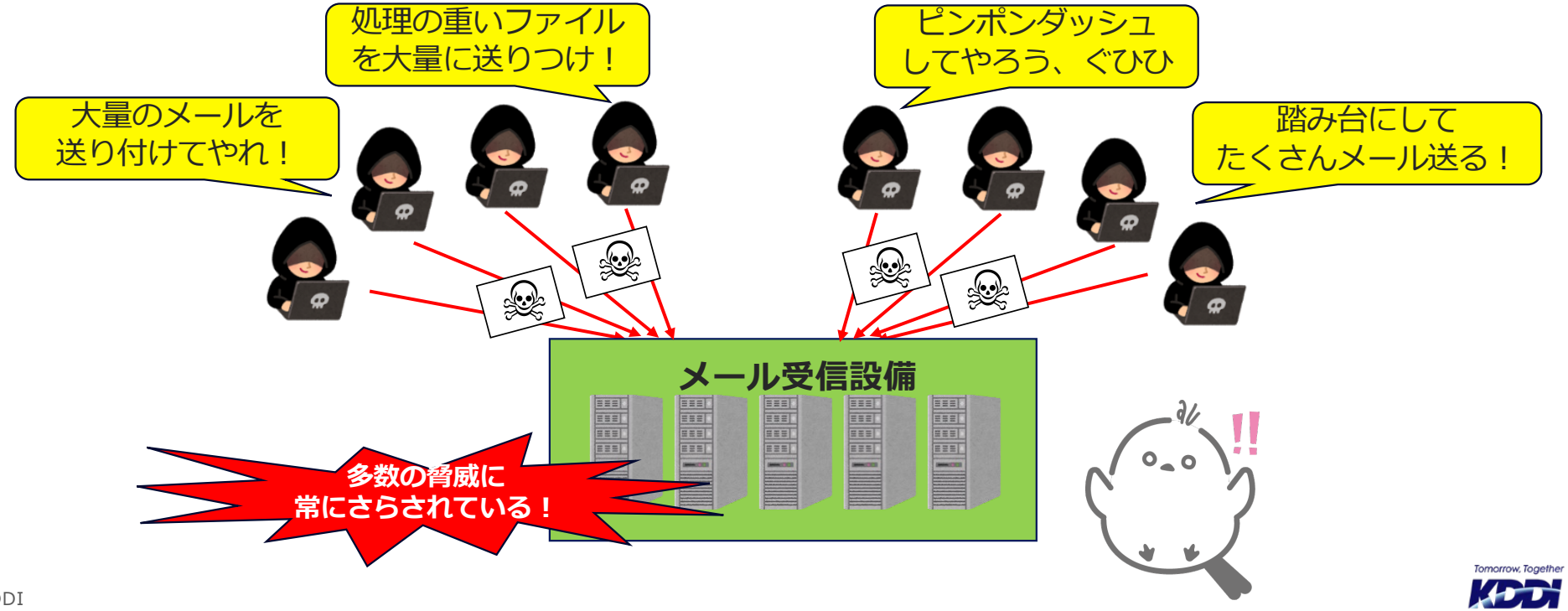
- **一定時間あたり多数のアクセス**
  ⇒必要以上に多数のアクセスは異常
- **メール送信を行っていない（完了までせず切断している）**
  ⇒通常のメール送信行為ではない可能性大
- **同じセッション内で多数の宛先を送信している**
- **宛先のうち不明の割合が多い**
  ⇒違う目的で何かをやっている可能性大

前述の送信元からの接続の応答を遅らせる、接続を一時的に遮断する等の防御策を発動する

メール受信設備への攻撃について

メール「受信設備」への攻撃

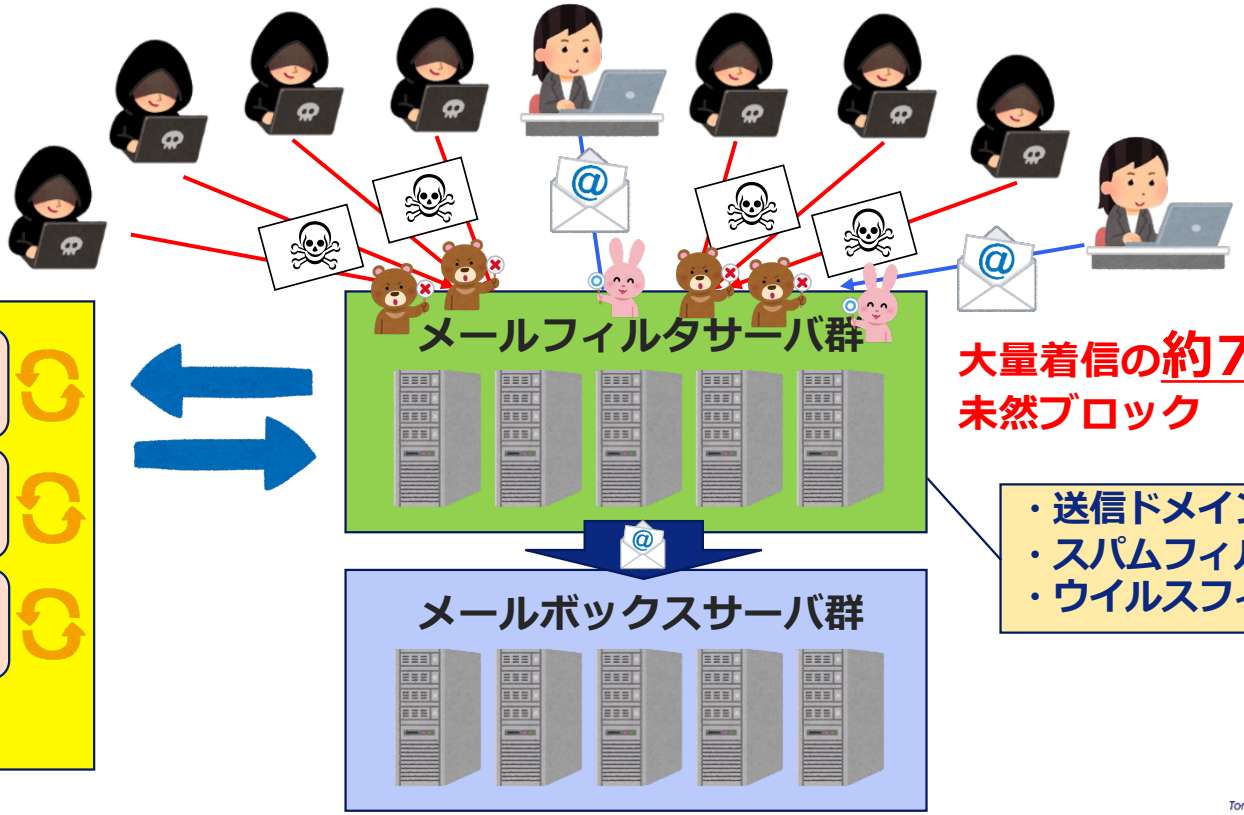
「メール受信設備」への攻撃
- サーバの負荷が上がり、受信不能に・・・
- 大量受信により、保存領域がいっぱいになって受信不可に・・・
- 踏み台にされて、多数のエラーメールをバラまかれ・・・



メール受信設備への攻撃を防ぐ仕組み(リアルタイム着信制御)

**攻撃者からの迷惑メール大量着信とメール設備への攻撃を防止するために、
送信元を「IPアドレス／ドメイン」等でレーティング＋リアルタイムに着信制御**

ひたすら分析・・・



- 宛先不明メール 大量送信元のレーティング
- 送信ドメイン認証結果× 大量送信元のレーティング
- 異常セッション状態監視（セッション時間・コマンドエラー等々）

制御サーバ

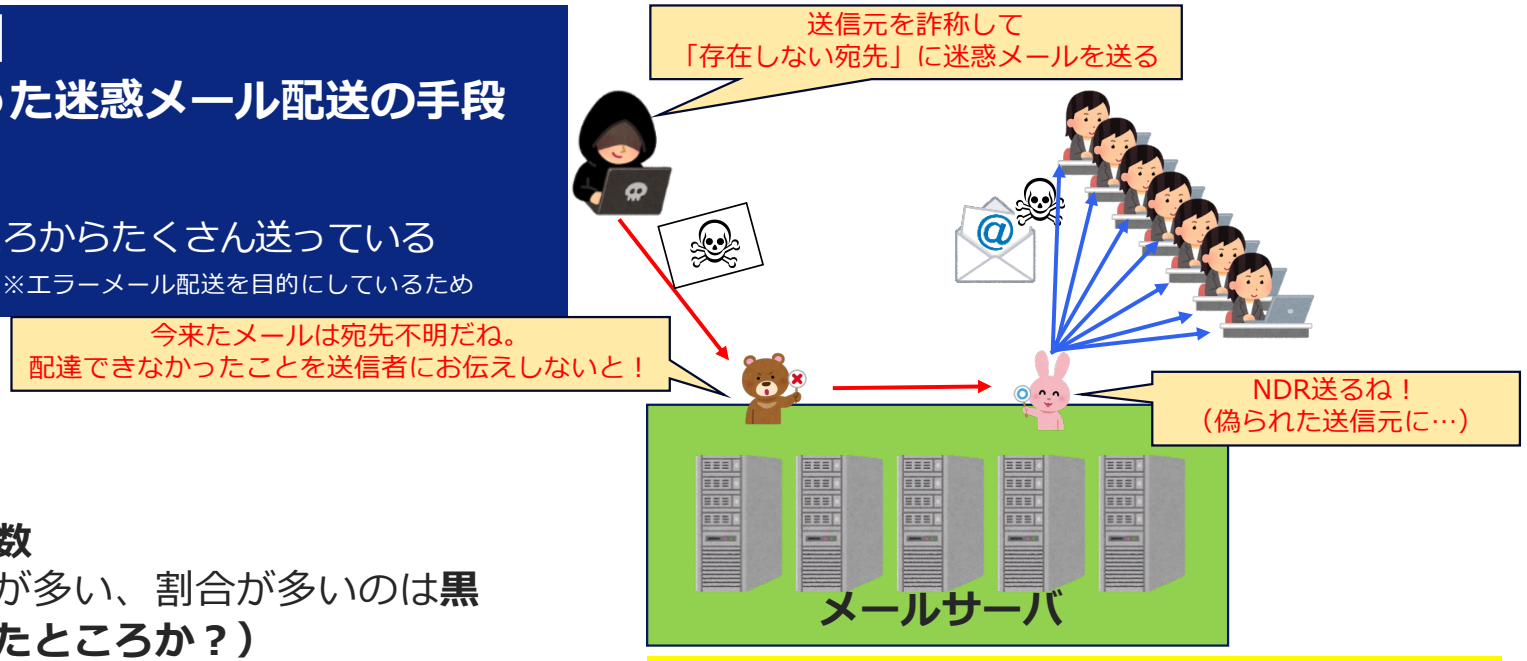
大量着信の約7割を未然ブロック

- 送信ドメイン認証
- スパムフィルタ
- ウイルスフィルタ

「バックスキャッタ」を防ぐ

【バックスキャッタ】
「NDR」の仕組みを使った迷惑メール配送の手段

■攻撃者の特徴
- 宛先不明のメールを同じところからたくさん送っている
- 送信元のメアドがバラバラ　※エラーメール配送を目的にしているため



- **一定時間あたりの宛先不明数**
  ⇒必要以上に宛先不明数が多い、割合が多いのは**黒**
- **送信元の情報（ちゃんとしたところか？）**
  ※送信元が逆引きできるか、MTAの振る舞いは適切か？等
  ⇒逆引きすらできない等は使い捨てサーバやbotの**可能性高**
- **送信ドメイン認証（SPF）結果を見る**
  ⇒配送希望先(E-From)でSPF認証するので大多数失敗

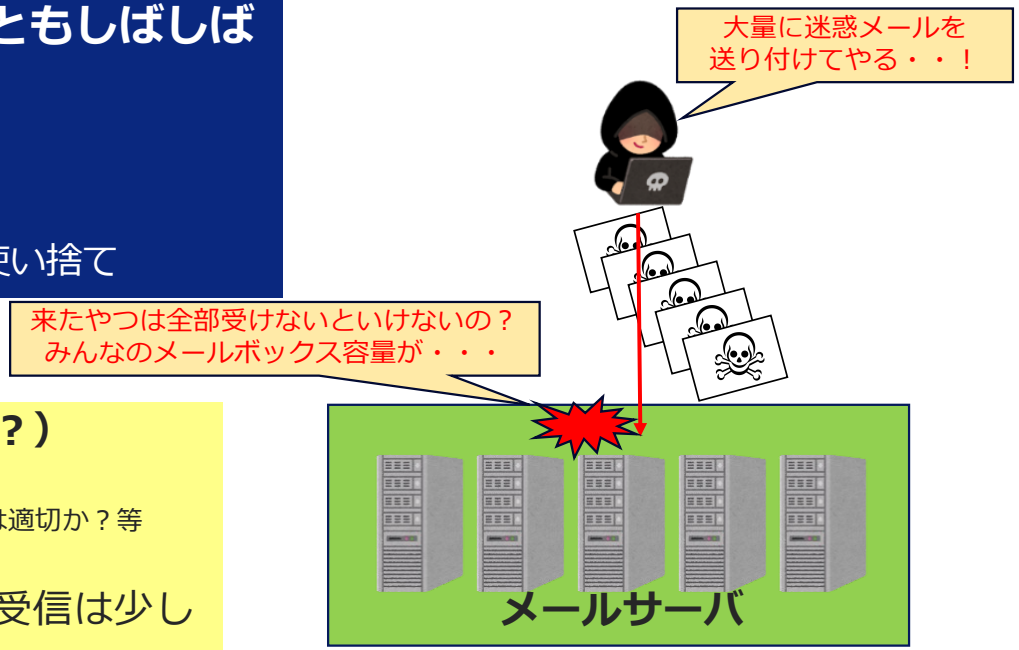
正しい行為（NDR返送）が
⇒迷惑メール配送行為にされてしまう
⇒多数の配送でメールサーバの負荷にもなる

前述の送信元からのメールには応答を遅らせる等の防御策を発動する

「大量受信」を防ぐ

【大量受信】
特定の送信元から、たくさんのメールが着信する
正規でないメール（迷惑メール）であることもしばしば

■攻撃者の特徴
・送信ドメイン認証結果が失敗のことが多い
・一か所、同様のネットワークから大量に送っている
・送信元情報（逆引きNG等）が怪しいことが多い（使い捨て



・メールの送信ドメイン認証結果（失敗が多数？）
・送信元の情報（ちゃんとしたところか？）
※送信元が逆引きできるか、MTAの振る舞いは適切か？等

などをチェックし、その送信元からのメールの受信は少し厳し目にチェックして拒否するなどで防御

大量の受信メールは
・迷惑メール受信の増加（であることがほとんど）
・メールボックス容量をムダに消費する

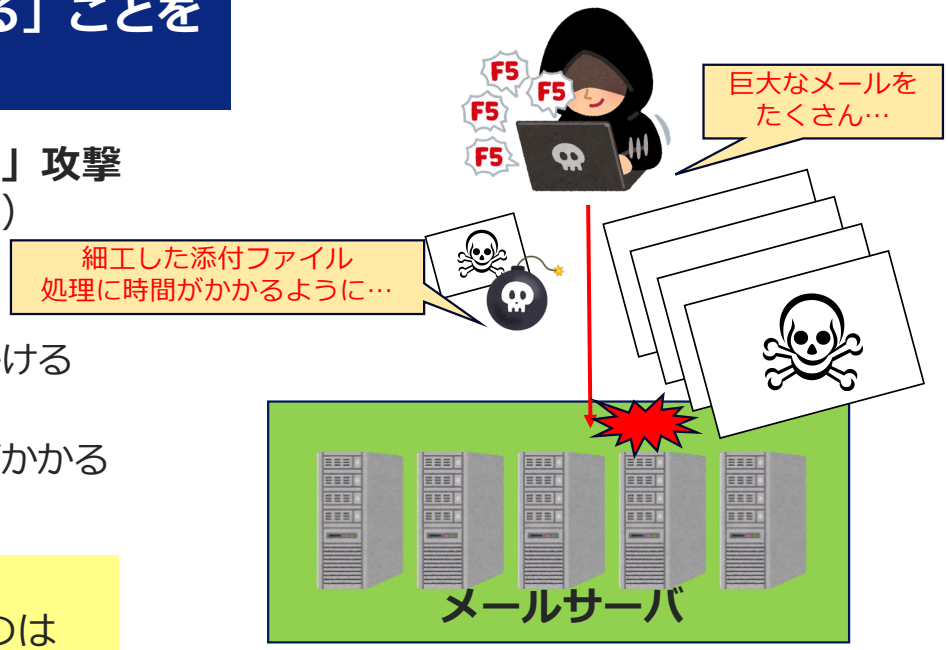
「大量受信（ボム攻撃）」を防ぐ

【大量受信（ボム攻撃）】
大量メールの中でも、「メール設備を不全に陥れる」ことを目的とした攻撃で、DoS攻撃の一環でもある

大量メール攻撃の中でも、悪質なものは「ボム（爆弾）」攻撃
（迷惑メールを送るのとはそもそも違う目的で行われる）

・ZIPファイルで大きなファイルを何度も圧縮して
⇒ウイルスチェックの時間・処理を重くして設備へ負荷をかける
・大きなサイズのメールを多数の受信者に一斉に投げる
⇒メールが大きく、多数の受信者に保存すると設備へ負荷がかかる

■設備での防御
ZIPファイルの圧縮が特殊（階層が深すぎるなど）なものは処理を軽減する、メールサイズ上限を設ける＆多数を一定時間内に送りつけてくる送信元からのメールは受けづらくする・・・などで防衛する



設備を落とす／困らせることを目的として
DoS攻撃の一種として知られる「ボム」系攻撃

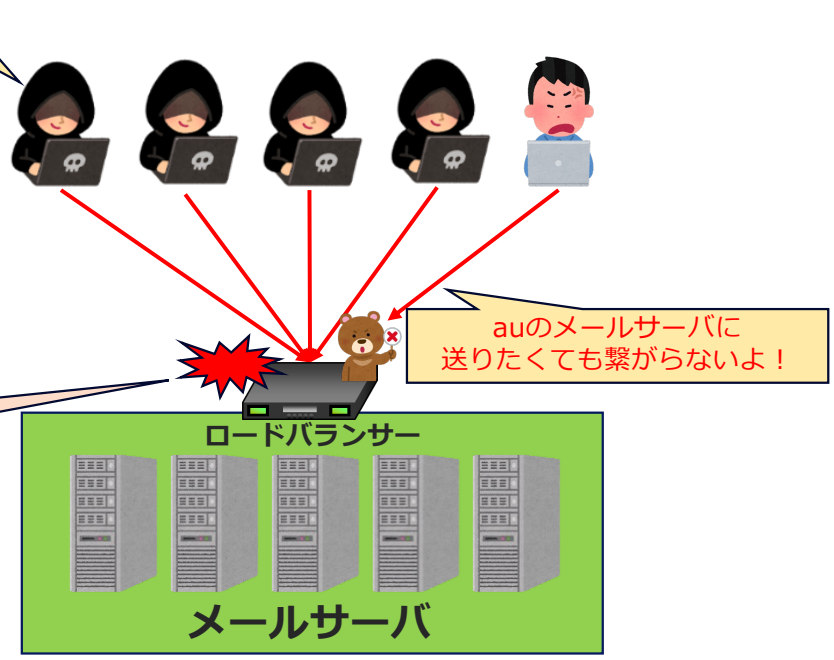
「異常セッション攻撃」を防ぐ

【異常セッション攻撃】
ピンポンダッシュのように、「本来の受け答えをしないまま」にし、メール設備のセッションを枯渇させる攻撃

「ピンポンダッシュ」
ピンポーンと音が鳴って、応答するも…誰もいない…
これにも20秒くらい時間を使いますよね？

メールでも、同様の攻撃があります。
セッションをつなぎに来て、最初だけor途中まで応答して、放置。
途中まで繋がっているのですぐに切るわけにも行かず、
サーバは待ち続けてしまい、待ち行列ができてしまう。

ロードバランサで一定数でコネクション数を制限している設備が多いため、
「待ち行列」でコネクションが埋まると、正規の接続も受けられなくなってしまう！



※「正しいメールだが、遅いサーバ」もいるので
どんどん切ってしまうわけにもいかない…

・セッション保持時間（どれくらいの長さか？）
・受信結果（正常に受信しているか？）
異常セッションの兆候を確認した場合、
セッションを受け付けないように一時的に制御するなどで防御

まとめ

メール受信の防御のために

メール受信設備への攻撃は常に発生している
攻撃が発生してから対処…**では遅い！**
（すでに多数が配信されたり、着信したり、設備が高負荷になってしまう

インバウンドトラフィックの監視を常に行い、
異常な傾向を検知したら、未然に防ぐことが重要

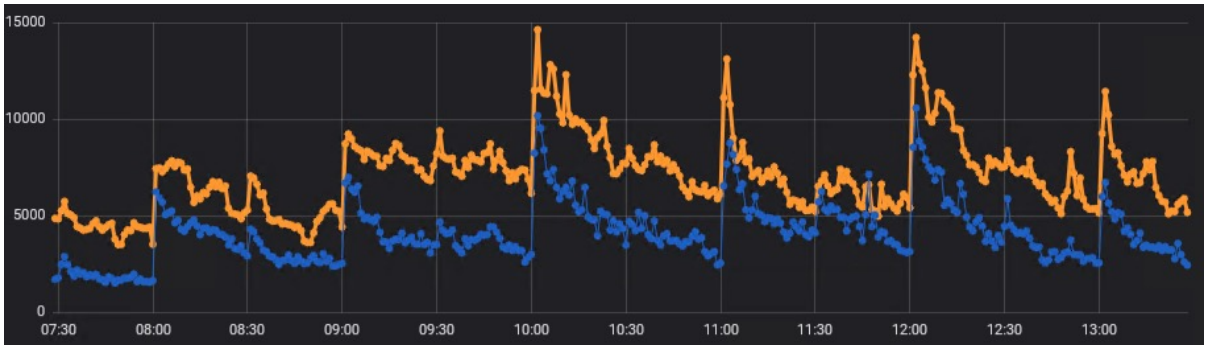
受信傾向を監視する
- 受信数
- セッション数
- 受信所要時間（セッション維持時間）
- 送信元国傾向　など

迷惑メール／ウイルス数を監視する
- 検知数
- お客様からの迷惑メール報告数

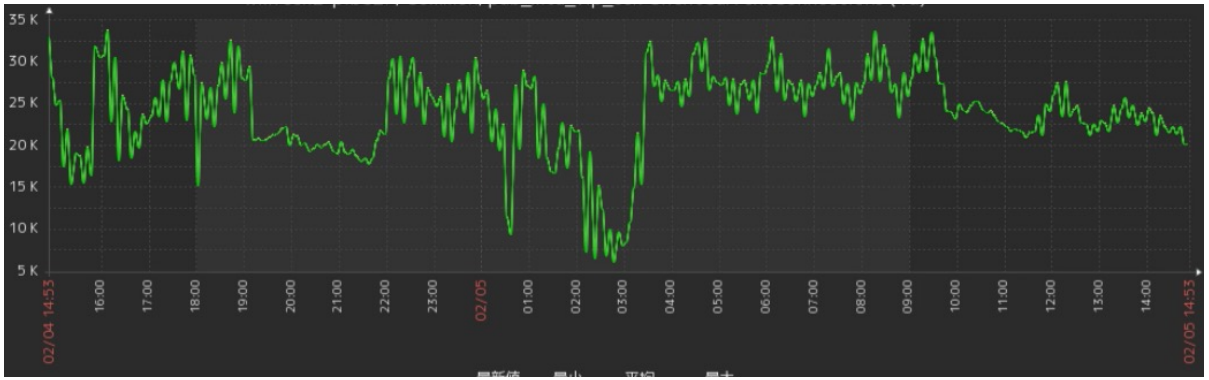
NDR通数を監視する
- NDR発生通数

異常検知したら
可能な限り自動＋迅速に
防御措置を発動する

最近の例



【メールトラフィック数】
前週（青線）と比較して、なぜこんなに多い？？
⇒大量に迷惑メールが撃ち込まれていた・・・
（すり抜けている



【セッション数】
急に高くなっているところ、落ちるところがある
⇒高くなっているところはセッション保持時間が長い「ピンポンダッシュ」が多数行われていた
（いろいろなところから

異常検知、すぐにALMで対処　⇒　それでも間に合わないときもある。。
ということで、生成AIの活用を模索しています。
皆で考え、皆で守って、安心安全なメールサービスの実現を！

Tomorrow, Together
KDDI
おもしろいほうの未来へ。
au

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030