なりすましメールとDMARCを考える
～総務省～

２０２５年１１月２０日

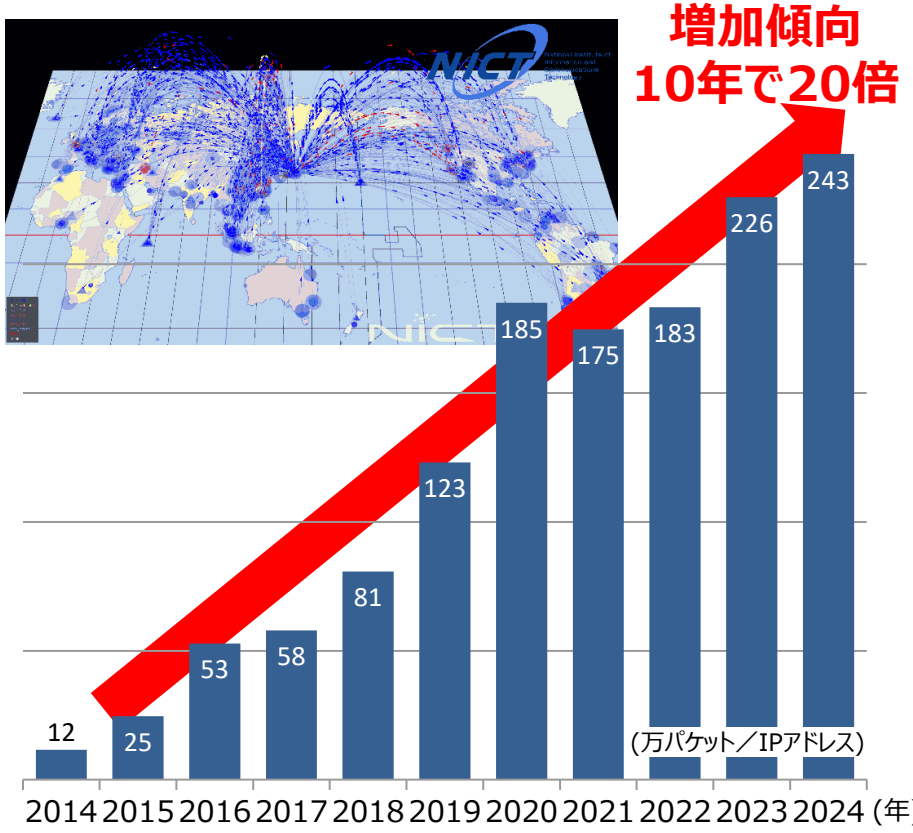
総務省　サイバーセキュリティ統括官室　企画官
梅城 崇師

インターネットを通じたサイバー攻撃の脅威の増大

➢ **サイバー攻撃**は**巧妙化・深刻化**しており、**質・量両面でサイバー攻撃の脅威は増大。**

サイバー攻撃関連通信数の推移

総務省所管の情報通信研究機構(NICT)は、インターネット上の大規模サイバー攻撃観測網「NICTER」において、サイバー攻撃関連通信を継続的に観測しており、2024年は過去最多。



（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2024」等を基に作成

サイバー攻撃の発生事例

政府機関や重要インフラ事業者等をターゲットにする、国家を背景とするものを始めとした巧妙化・高度化されたサイバー攻撃は、我が国にとっても現に直面する安全保障上の脅威

＜ロシア背景＞
- ✓サイバー攻撃を軍事的・政治的目的達成のために利用
- ✓2022年のウクライナ侵略前に、同国の政府機関や重要インフラ事業者等の情報システムへ攻撃

＜中国背景＞
- ✓政府・企業等の情報窃取や機能妨害・機能破壊
- ✓**SaltTyphoon**：世界中の電気通信事業者等を標的
- ✓**VoltTyphoon**：米軍・政府機関や重要インフラを標的

＜北朝鮮背景＞
- ✓身分を偽って仕事を受注し、不法な資金を調達
- ✓TraderTraitor：暗号資産関連事業者から資産を窃取

＜その他＞
- ✓ 名古屋港：業務停止に陥らせたランサムウェア攻撃
- ✓ NISCやJAXAへの攻撃

2025年は日本のサイバーセキュリティ政策の転換点

2000年02月 内閣官房 情報セキュリティ対策推進室 設置

- ✓ **中央省庁のHPが相次いで改ざん**される被害が発生(2000.1)
- ✓ **政府機関**向け「情報セキュリティポリシーに関するガイドライン」策定(2000.7)
- ✓ 「**重要インフラ**のサイバーテロ対策に係る特別行動計画」策定(2000.12)

2006年02月 第１次情報セキュリティ基本計画 策定

- ✓ 内閣官房 **情報セキュリティセンター**設置(2005.4)
- ✓ **情報セキュリティ政策会議**設置(2005.5)
- ✓ 「**政府機関**の情報セキュリティ対策のための統一基準」(2005.12)
- ✓ 「**重要インフラの**情報セキュリティ対策に係る行動計画」策定(2005.12)

2014年11月 サイバーセキュリティ基本法 公布

- ✓ 法令で初めて「**サイバーセキュリティ**」という用語が使用
- ✓ 法律に基づき、「**サイバーセキュリティ戦略本部**」が設置(2015.1)
- ✓ 法律に基づき、「**内閣サイバーセキュリティセンター**」が発足(2015.1)
- ✓ 法律に基づき、「**サイバーセキュリティ戦略**」が閣議決定(2015.9)

2025年05月 サイバー対処能力強化法 公布

- ✓ 「**能動的サイバー防御**」の具体化
- ✓ 事故報告の義務化、通信情報の利用、攻撃サーバの無害化等

サイバーセキュリティ政策の推進体制（2025.7.1～）

内閣

サイバーセキュリティ推進専門家会議

意見聴取

サイバーセキュリティ戦略本部

本部長　**内閣総理大臣**
副本部長　**内閣官房長官、サイバー安全保障担当大臣**
本部員　**全大臣**

意見

国家安全保障会議（NSC）

内閣官房　国家サイバー統括室
【戦略本部の事務局、各府省の総合調整】

緊密連携

国家安全保障局（NSS）

内閣サイバー官　併任 国家安全保障局次長

総合調整

＜全府省庁＞
〔自組織・所管独立行政法人等のセキュリティ確保の推進〕

＜サイバーセキュリティ政策推進省庁＞
〔所掌に基づくサイバーセキュリティ施策の実施〕

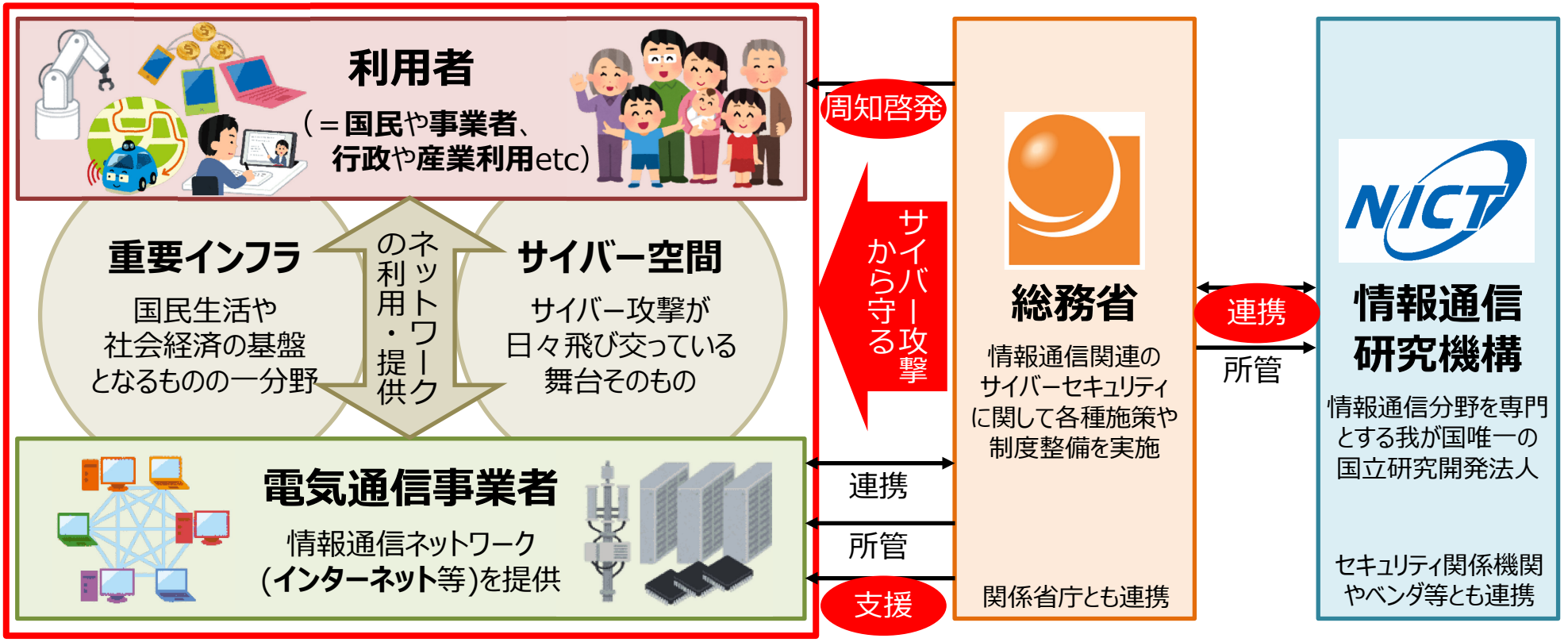
内閣府（経済安全保障）
警察庁（治安の確保）
デジタル庁（デジタル社会形成）
総務省（通信・ネットワーク政策）
－ NICT（(国研)情報通信研究機構）
外務省（外交・安全保障）
経済産業省（情報政策）
－ IPA（(独)情報処理推進機構）
防衛省（国の防衛）
文部科学省（セキュリティ教育）　等

重要インフラ所管省庁

金融庁（金融）
総務省
（政府・行政サービス、情報通信）
厚生労働省（医療）
経済産業省
（電力、ガス、化学、クレジット、石油）
国土交通省
（鉄道、航空、物流、水道、空港、港湾）

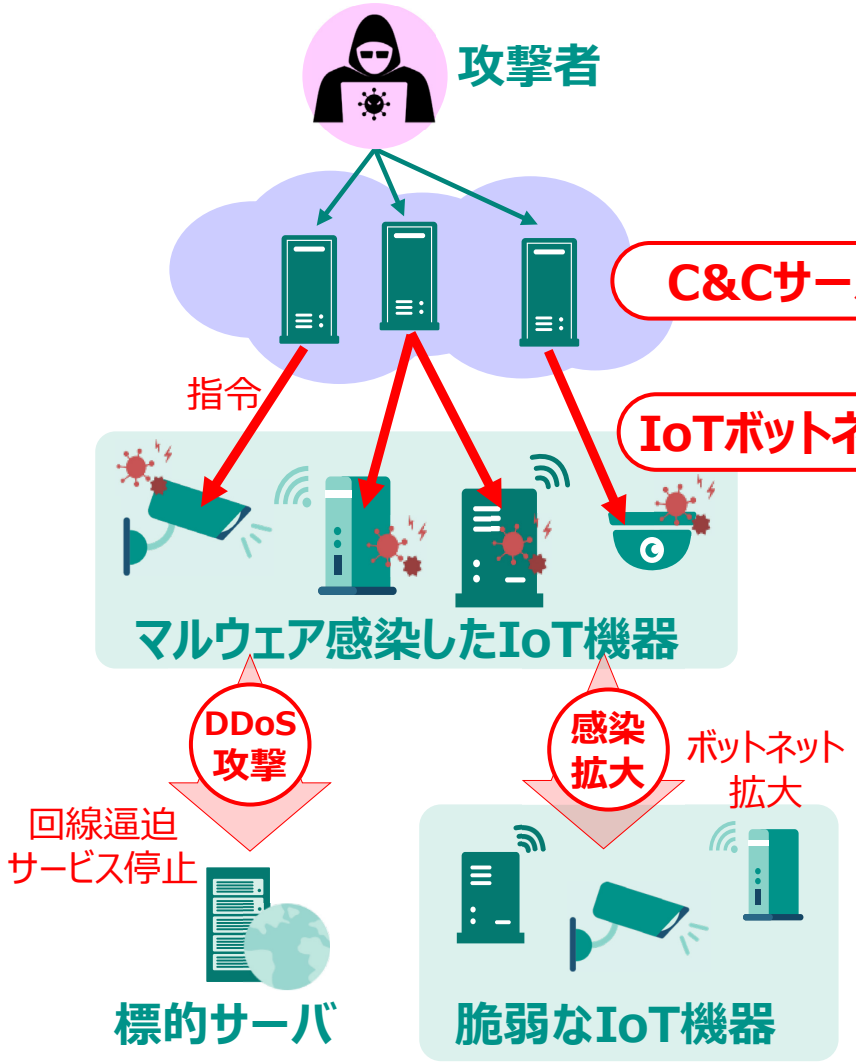
サイバーセキュリティにおける総務省の役割

- 総務省所管である**電気通信事業者～情報通信ネットワーク（インターネット）**は２つの側面
  - 機能停止すれば国民生活や経済社会に甚大な影響が発生する**重要インフラ**（国の基盤となる15分野の一つ）
  - サイバー攻撃が飛び交う**サイバー空間そのもの**（サイバーセキュリティ確保のための重要な役割）
- **情報通信研究機構(NICT)**は、**サイバー攻撃**に関する**観測・分析**を長年行い、**高度な技術・人材**を保有
- **総務省**はNICTや電気通信事業者等と連携し、**ネットワークや利用者**を**サイバー攻撃から守る**取組を実施
  （加えて、脅威情報・技術の国産化プロジェクトを推進し、我が国自らの力で脅威を検知し対抗できる基盤を構築）



IoT機器を悪用したサイバー攻撃(DDoS攻撃等)への対策

- IoT機器の急増に伴い、**IoT機器を悪用**した大規模なサイバー攻撃（**DDoS攻撃**等）が発生
- DDoS攻撃は**ネットワーク全体の速度低下**を引き起こしかねないほか、**標的側での対応が難しい**
- 総務省・ISP等が協力して、攻撃指令を行う**C&Cサーバ**と、攻撃役となる**脆弱なIoT機器**の両面から対策



ネットワーク側の対策

IoTボットネットに対して指令通信を出す
C&Cサーバへの対処

電気通信事業者がネットワークの管理のために普段から利用している**情報を分析**することで、**C&Cサーバを検知**
→ 対策に活用するための**実証事業を実施中**

機器側の対策

マルウェアに感染した/感染する危険性が高い
脆弱なIoT機器への対処

サイバー攻撃に悪用されるおそれのある**IoT機器を調査**し、
（サイバーセキュリティに知見のあるNICTにおいて調査を実施）
電気通信事業者を通じ、**IoT機器の利用者に注意喚起**

＜調査＆注意喚起の対象＞
① 既にマルウェアに感染している機器
② ファームウェアの脆弱性等がある機器
③ ID・パスワードの設定に脆弱性がある機器

→「**NOTICE**」プロジェクト

ネットワークセキュリティの確保

- インターネットは歴史的に、接続性と可用性を重視し、信頼できる限られた環境での使用が想定
  →仕様に脆弱な部分があり、**通信経路(BGP)やDNSのハイジャック、なりすましメール**などが発生・懸念
- **セキュリティ向上策（電子認証技術を活用したRPKI／DNSSEC／DMARC）**が国際標準化
- 費用や導入インセンティブの面から、国内での普及が進まないため、**ガイドライン策定**により導入を後押し

BGPハイジャックへの対応策

Border Gateway Protocol＝ネットワーク間で経路情報を交換するためのプロトコル

RPKI (Resource Public-Key Infrastructure)

IPアドレスとAS(ネットワークの集まり)番号の正当な所有者が、デジタル署名付きの情報を登録
受け取った経路情報が登録情報と一致するか確認することで、経路情報が正当かを確認
※登録情報をROA(Route Origin Authorization)、確認検証プロセスをROV(Route Origin Validation)という

→IPアドレスの分配を受けた者と、AS運用者の対策をガイドライン化→JPNICから公開
https://www.nic.ad.jp/ja/rpki/guideline/

DNSハイジャックへの対応策

Domaine Name System＝ドメイン名をIPアドレス等に紐付けるための技術

DNSSEC (Domain Name System SECurity Extensions)

ドメインに関する正当な情報を保持するDNSサーバ(権威DNSサーバ)で、登録情報にデジタル署名を付与
DNS情報を読み取る側(フルリゾルバ)がデジタル署名を確認することで、DNS情報が正当かを確認

→ドメイン登録者、DNS運用者の対策をガイドライン化→ガイドライン公開に向け調整中

なりすましメールへの対応策

DMARC (Domain-based Message Authentication, Reporting and Conformance)

ドメインの正当な所有者(メール送信側)が、処理方針をDNS上で宣言
受信側は、SPFやDKIMの検証を実施し、検証失敗時に送信側の処理方針に従って処理
※SPF：送信元IPアドレスを確認し、正当なドメインからのメールかを確認する仕組み
※DKIM：メールにデジタル署名を追加し、内容の改ざんを防ぐ仕組み
※処理方針：認証失敗時の処理方針として、何もしない(none)/隔離(quarantine)/拒絶(reject)を記載

→送信側、配信事業者、受信側の対策をガイドライン化→迷惑メール対策推進協議会から公開
https://www.dekyo.or.jp/soudan/aspc/report.html

さらに総務省において、国際標準の改訂に向けた議論内容(IETFのWG)の調査や、システム運用者向けの勉強会(ハンズオン)を継続的に実施して普及展開を支援

なりすましメール対策の必要性

- キャッシュレス決済等が進む中、**不正送金等を行うフィッシングによる被害等が拡大**。
- 2025年７月には、政府として「**国民を詐欺から守るための総合対策2.0**」を策定し、その中で、「**DMARC等への更なる対応促進**」のため**関係省庁が連携**して取り組むこととされた。
- 2025年９月には、**総務省から業界団体※に対して**、なりすましメール対策として有効な、**DMARCの導入やDMARCポリシーの設定（隔離、拒否）について要請**を実施。

※(一社)電気通信事業者協会、(一社)テレコムサービス協会、(一社)日本インターネットプロバイダー協会、(一社)日本ケーブルテレビ連盟

国民を詐欺から守るための総合対策2.0

送信ドメイン認証技術(DMARC等)への更なる対応促進

（略）例えば、令和６年中の**インターネットバンキングに係る不正送金事犯の手口をみると、フィッシングサイト等に誘導する手口のうち約58パーセントが電子メール**であるなど、詐欺等にドメイン名のなりすましが用いられていることから、その**対策を更に推進する必要**がある。引き続き、利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関、EC事業者、物流事業者、行政機関等のメール送信側事業者等に対して、導入状況も踏まえ、**送信ドメイン認証技術(DMARC等)の導入推進**を継続して実施するとともに、送信側事業者等に対してなりすましメールの受信拒否を要求するポリシーでの運用を検討するよう働き掛ける。また、関係省庁等が連携し、なりすましの対象となる事業者等に対して、必要に応じて、DMARC等の導入状況等を確認するなどのフォローアップを行う。

総務省からの要請文書(2025年9月1日)

(1) フィルタリングの判定技術の向上や迷惑メール判定におけるAIの活用等、メールのフィルタリングの精度の一層の向上を積極的に図ること。また、迷惑メールのフィルタリング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメールフィルタリングを目指すこと。

(2) なりすましメール対策として有効な**DMARCの導入やDMARCポリシーの設定（隔離、拒否）を行うこと**。送信側だけでなく受信側についても、適切なDMARCポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、**BIMI**、踏み台送信対策等の更なる対策の**導入を積極的に検討**していくこと。

(3) 提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一層の周知・啓発を行うこと。

→ DMARCは、なりすましメールによるサイバー犯罪抑止の中核対策

政府機関等におけるDMARCへの対応

- 政府機関や独立行政法人等において遵守が求められる「**政府機関等のサイバーセキュリティ対策のための統一基準群**」において、**電子メールの送受信**を行う場合に、**DMARC対策は必須**。
- さらに、DMARCポリシーを**隔離（quarantine）**又は**拒否（reject）**とすることを求めている。
- 加えて、**BIMI**（Brand Indicators for Message Identification）の導入についても求めている。

政府機関等の対策基準策定のためのガイドライン（令和７年度版）

※わかりやすさのため一部記載を省略しています

【基本対策事項】

6.2.2(1)-3 以下を全て含む送信ドメイン認証技術による**電子メールのなりすましの防止策を講ずること**。

○ **DMARCによる送信側の対策を行うこと**。対策を行うためには、SPF、DKIMのいずれか又は両方による対策を行う必要がある。

○ **DMARCによる受信側の対策を行うこと**。対策を行うためには、SPF、DKIMの両方による対策を行う必要がある。

【解説】

DMARCポリシーが**”p=none”の場合**、受信側に特別な処理を要求しないため、機関等に**なりすましたメールによって受信側が被害に遭うリスクを必ずしも低減させることができない**。

そのため、**以下を例とする対策**をDMARCの導入から一年以内に実施する等、DMARCポリシーに**”p=none”を設定する期間が可能な限り短くなるように期間を設けた上で実施することが望ましい**。

- **より強固なDMARCポリシー（quarantine又はreject）を設定**する。例えば、機関等になりすました電子メールが送信されていることや、機関等が送信した電子メールが受信側においてSPF、DKIMの認証に失敗することが少ないことがDMARCレポートの分析結果等から確認できた場合は、より強固なDMARCポリシーを設定するとよい。
- **電子メールを利用していないドメインについて、DMARCのポリシーを"p=reject"と設定**する。

また、DMARCによって認証された**電子メールの視認性を向上させるBIMI**（Brand Indicators for Message Identification）の導入を検討するとよい。送信側がBIMIを設定すると、受信側のBIMIに対応する電子メールクライアントに送信側のロゴの表示ができるため、機関等が送信した電子メールであることが視覚的に分かりやすくなる。

総務省におけるDMARCポリシーの強化

- **総務省**では、soumu.go.jpやそのサブドメインについて、多数の部局が多様な方法で電子メールを利用。
- 2025年7月に、**サブドメインを含めて**、**DMARCポリシーを「none」ら「quarantine」に変更**。
- 2025年11月からは、**BIMIにも対応**。

総務省のDMARCポリシー

_dmarc.**soumu.go.jp** text =
"v=DMARC1; **p=quarantine; sp=quarantine;**
pct=100;adkim=r;aspf=r;
rua=mailto:rua-report@soumu.go.jp;
ruf=mailto:ruf-report@soumu.go.jp"

BIMIの導入

ポリシー変更時の留意点

- **ポリシー変更前**に、送信されてきた**DMARCレポートを分析**し、メールの到達状況を把握・集計
  （独自分析が難しければ外部サービスの利用も有効）
  → **一定期間行うことで、なりすましメールの状況や、正当なメールがfailとなっているドメインが把握可能**
- **全システムが完全に対応してから変更するのではなく、quarantineの利点（＝削除されない）を活用**
  → **まずはquarantineに変更し、改めてレポート分析を行い、更に対応が必要なシステムを把握**
  （システム担当に連絡 → ベンダー等と調査・対応 → 対応が完了すればrejectへの変更）
- なりすましメールの状況（**数万/日レベル**）を把握し、**関係者に対応に協力してもらう必要**
  → **レポートの分析状況を可視化し情報提供**
- レポートの分析の結果から、**外部サービス利用等によるシャドーITが見つかることも**（例：メールマガジン配信等）
  → **担当者に1から説明し理解してもらい適切に対応してもらう**