資料７

安全基準等策定ガイドライン案の検討
（総務省）

なりすましメール対策としてのDMARC

- 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**している中で、**なりすましメール対策**として、関係省庁が連携して「**DMARC等の導入推進**」を図ることとされた。
- **総務省から業界団体※に対し**ても、**DMARCの導入**を単に行うだけでなく、**DMARCポリシー**を「none」ではなく「**隔離(quarantine)**」又は「**拒否(reject)**」とすることを**要請。**
  ※(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
- DMARCの設定は、通信事業者だけが対応するのでは効果は限定的であり、**メールサーバやドメインを運用している方が幅広く対応する必要**

国民を詐欺から守るための総合対策2.0 (2025.7)

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 (2025.9.1)

(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**