おさえておきたい基本や、
最新動向を解説するコーナーです。

No.84号 10:00min.

01 はじめに

電子メールは、インターネット初期から利用されているコミュニケーション手段ですが、最近では「個人間のコミュニケーション(C to C)」よりも「ビジネスシーン(B to B)」「個人向けサービス提供の一部(B to C)」としての側面が大きいです。そして、利用シーンが変化するとともに、電子メールに関連した脅威も変化してきました。近年では、電子メールのなりすましや、それらを起因としたフィッシング被害が継続して発生している状況※1です。

これらの脅威に対抗するために、2000年以降、電子メールに関連する技術として「送信ドメイン認証」が開発され、徐々に普及してきました。DMARCは、その技術の一つとして知られており、多くの企業やサービス提供事業者が導入しています。とは言うものの、まだDMARCという技術の恩恵を受けていない企業にとっては「気安く近づけない」技術かもしれません。ここでは、DMARCについて、関連技術を含めた技術的な説明や導入と運用の勘所などを整理していきたいと思います。

※1 https://www.antiphishing.jp/report/monthly/202305.html

02 送信ドメイン認証技術のおさらい

電子メールのなりすまし(ここでは、差出人ドメインのなりすましを指します)を確認する技術として、SPF※2とDKIM※3が一般的に知られています。いずれもDNS上に真正であることを確認するための情報が宣言されており、前者は真正な送信元メールサーバーのIPアドレスが、後者は真正なメールに付与される電子署名の公開鍵が宣言されています。

SPFとDKIMは、なりすましメールと真正なメールを見極めることが可能ですが、共通して言えることとして、受信ユーザーが目にする差出人情報(ヘッダーFrom)を保護しないという問題点があります。加えて、なりすましと判定されたメールをどう取り扱うかについては、受信側のメールサービスに委ねられている点も注意が必要です。言い換えますと、なりすましを防ぎたいドメイン管理者は、受信ユーザーの安全性に対して、十分に関与できないということです。つまり、せっかくこれらのなりすまし対策技術を導入したとしても、受信ユーザーがなりすましたメールを誤って閲覧、悪意のある添付ファイルを開くこと、そしてリンクをクリックしてしまうことを防ぎづらいのです。

● 送信ドメイン認証技術 ●

ドメイン単位で送信者が名乗っている情報(メールドメイン)が正しいか確認する技術

SPF	規格	DKIM
RFC 7208	ドキュメント	RFC 6376 (STD 76)
IPアドレスで判定	認証方法	電子署名で判定
エンベロープ From ドメイン	保護する対象	署名ドメイン
DNS に設定を記述	対応の難しさ	サーバーに実装
Authentication-Results ヘッダー	確認方法	Authentication-Results ヘッダー
転送に弱い ヘッダー From 詐称が可能	問題点	メーリングリストに弱い ヘッダー From 詐称が可能

表1 SPFとDKIMの違い

※2 https://datatracker.ietf.org/doc/html/rfc7208
※3 https://datatracker.ietf.org/doc/html/rfc6376

［テーマ］

なりすましメール対策のための DMARCとその導入・運用

―送信ドメイン認証「DMARC」とは―

03 DMARCの特徴とその狙い

そこで新たに登場したDMARC※4は、二つの問題点を解決することに役立ちます。DMARCという技術も、DNS上にドメイン管理者の宣言（DMARCレコード）を記述することは二つの技術と似ています。DMARCレコードに記載するタグ情報のうち、ポリシー（p=）には、ドメイン管理者がなりすましと判定されたメールの取り扱い方法を「そのまま受信（none）」「隔離（quarantine）」「拒否（reject）」という3段階で指定することが可能です。このポリシーはDMARCの重要なタグの一つであり、noneの場合は文字通りなりすましメールと判定されたとしてもそのまま受信してしまうため、保護された状態とは言えません。強制力のあるポリシー（quarantineやreject）を設定することが、DMARC導入の目標と言えるでしょう。

また、真正のメールであるかどうかのDMARCによる判定は、前述のSPFとDKIMの判定結果を利用して「いずれか一方が成功している」ことが必要ですが、加えてヘッダーFromドメインと認証対象ドメインが一致することも求められます。具体的には、SPFの認証が成功した場合はエンベロープFromドメインとの一致性を、DKIMの認証が成功した場合は署名ドメインとの一致性を必要とします。これにより、結果としてDMARCではヘッダーFromドメインの保護につながるのです。なお、この一致性を「アライメント」と呼びます。

● ドメイン管理者はどのように DMARC 対応するか ●

- SPF と同じようにDNS の TXT レコード（_dmarc.example.com）に以下のような宣言をする
- 親ドメインに設定することで、配下のサブドメインすべてに適用が可能

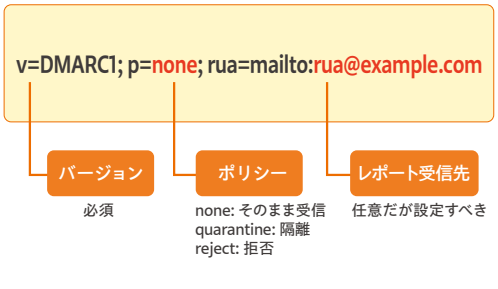
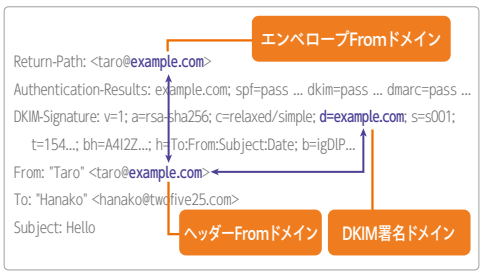


図1 DMARCレコードの例

● イン・アライメント例 ●



- SPF識別子アライメント
  - ヘッダーFromドメイン= エンベロープFromドメイン
- DKIM識別子アライメント
  - ヘッダーFromドメイン= DKIM署名ドメイン（DKIM-Signatureのd=タグ）

図2 アライメント

※4 https://datatracker.ietf.org/doc/html/rfc7489

04 SPFやDKIMとの関連性

端的に表現すれば、DMARCはSPFの認証でアライメントが成立するか、DKIMの認証でアライメントが成立するか、少なくとも一方のアライメントが成立すればなりすましではないと言えます。ですが、一般的にはSPFよりもDKIMを優先することが推奨されています。というのも、SPFの認証ではメールの転送処理や再配送による影響が大きく、その場合は真正なメールにもかかわらずDMARCによって隔離や拒否される蓋然性が高いのです。また、最近では自組織が管理するメールサーバーだけではなく、第三者メール送信サービス（クラウドサービス）からの送信が増えてきています。これらのケースでは、アライメントが成立しないこと、SPFの認証制限（ルックアップ数の上限）が影響してエラーになることなどの可能性があるため、同様にDMARCの導入では注意が必要です。

それに対して、DKIMの認証では電子署名を利用しているため、オリジナルのメールデータを加工さえしなければメールの転送処理や再配送によって認証結果やアライメントの成立には影響しにくいと言えます。

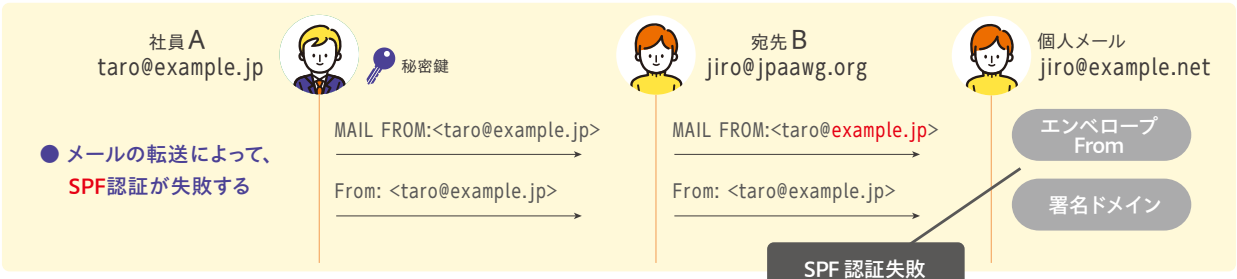


図3-1 メール転送時のSPF

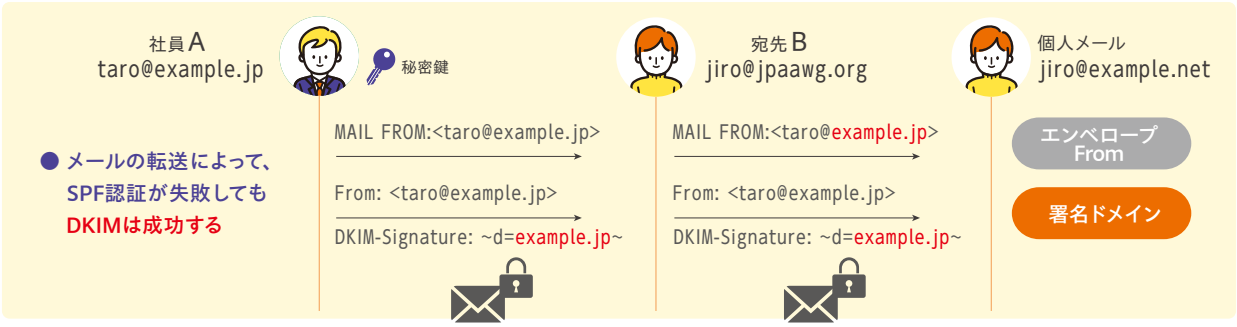


図3-2 メール転送時のDKIM

05 組織・企業がDMARCを導入・運用していくためには

以上の内容を整理しますと、DMARCという技術でなりすましメール対策を講じて、かつ、真正なメールを届けるためには、「DMARCレコードの宣言」「強制力のあるポリシーの設定」、そして特に「DKIM電子署名」が重要です。そしてこれは、どんな組織・企業であっても電子メールを利用するのであれば最低限必要な設定とも言えます。では、これら三つについて注意したいところや勘所を紹介したいと思います。

まず、DMARCをこれから導入しようと考えている場合には、DMARCレコードをどのように宣言するかがポイントとなります。必ず設定するタグとしては、必須の「v=DMARC1」「p=none」の二つですが、それらに加えてオプションである「rua=mailto:受信先メールアドレス」を設定することが望ましいです。「rua=」を設定することで、定期的に世界中のメールサービスからDMARCの認証結果に関するフィードバック（DMARC集計レポート）が得られます。そのため、必須ではありませんが設定することが推奨されています。また、ポリシー「p=none」から始めることもポイントです。これは、モニ

タリングと呼ばれる状態であり、DMARC集計レポートを受信しつつも、設定不備などの誤判定によるメールの到達性への影響をなくすことができるのです。

次に、送信に利用している環境（自組織が管理するメールサーバーや契約しているクラウドサービス）を調査して、DKIMの認証が成功するように電子署名を付与する設定をします。どの環境にDKIM電子署名の対応が必要であるかを知るためには、組織内に把握しているメールサーバーの情報をヒアリングする、あるいは委託先の一覧情報から契約中のクラウドサービスを把握する、という方法もあります。ですが、前述のDMARC集計レポートからも読み取ることが可能です。ここでは細かい説明は省略しますが、DMARC集計レポートには、認証結果と送信元メールサーバーの情報が含まれており、それらが対応に必要な環境を把握する参考となるのです。

ここで注意したいこととしては、DKIM電子署名が「第三者ドメインによる電子署名」ではなく「自組織ドメインによる電子署名」が必要となる点です。DMARCにおける「アライメント」で説明しましたが、DMARC認証においてはDKIM電子署名の認証成功だけではなく、そのドメインの一致性（ヘッダーFromドメインとDKIM署名ドメインの一致性）も求められます。例えば、クラウドサービスを利用した送信では、DKIM電子署名に対応しているものの、クラウドサービス側の管理するドメインでのみDKIM電子署名しているケースが見られます。この場合は、DMARC認証としては「アライメント」が成立しません。クラウドサービス側で「利用企業（自組織）のドメインでDKIM電子署名が可能かどうか」を確認するようにしましょう。なお、Amazon SES※5、sendgrid※6など大手クラウドサービスでは基本的に対応しています。

そして、これらの準備・対策が十分適用できたと判断された後、当初設定していたDMARCレコードのポリシー「p=」をモニタリングから強制力のあるポリシー（quarantineやreject）に切り替えます。この状態になれば、ついにあなたの組織のドメインがDMARCで保護された、と言えるでしょう。

※5 https://aws.amazon.com/jp/ses/　※6 https://sendgrid.com/

06 まとめとその他情報

電子メールを起点としたサイバー攻撃、特になりすましメールやフィッシング攻撃には、ここで紹介したDMARCという送信ドメイン認証技術を利用することで一定の効果が期待されます。当然、DMARCは差出人情報（ヘッダーFromドメイン）の真正性を認証するものですので、すべてのなりすまし手法に効果があるわけではありません。これまでのフィルタリング対策やレピュテーション対策などとうまく組み合わせながら、効果の最大化を図ってみてください。

また、DMARCを導入・運用していく過程において、自組織のメール環境の可視化やアセスメントにもつながりますので、ぜひとも皆さんもモニタリングから始めてみてはいかがでしょうか。

今回の記事では紹介しませんでしたが、2004年に創立された国際的なワーキンググループであるM³AAWG※7（マアグ：The Messaging, Malware and Mobile Anti-Abuse Working Group）や、2019年から活動を開始したJPAAWG※8（ジェイピー・アーグ：Japan Anti-Abuse Working Group）でもDMARCを含むなりすましメールへの対策技術については頻繁に議論されています。前者のM³AAWGは年3回の会合が開催されていますが、メンバー限定となっているために敷居は高いです。ですが、後者のJPAAWGが開催する年1回のGeneral Meeting※9は無料で参加ができますし、一部M³AAWGからの招待講演もあります。DMARCに関する動向※10だけではなく、電子メールに関連するセキュリティ対策に興味がある方はぜひ参加ください。

JPAAWG プログラム委員 ／
株式会社TwoFive CTO　加瀬正樹

※7 https://www.m3aawg.org/　※8 https://www.jpaawg.org/　※9 https://meetings.jpaawg.org/
※10 https://meetings.jpaawg.org/5th2022/wp-content/uploads/2022/11/A1-2_Keynote-2_Jones.pdf