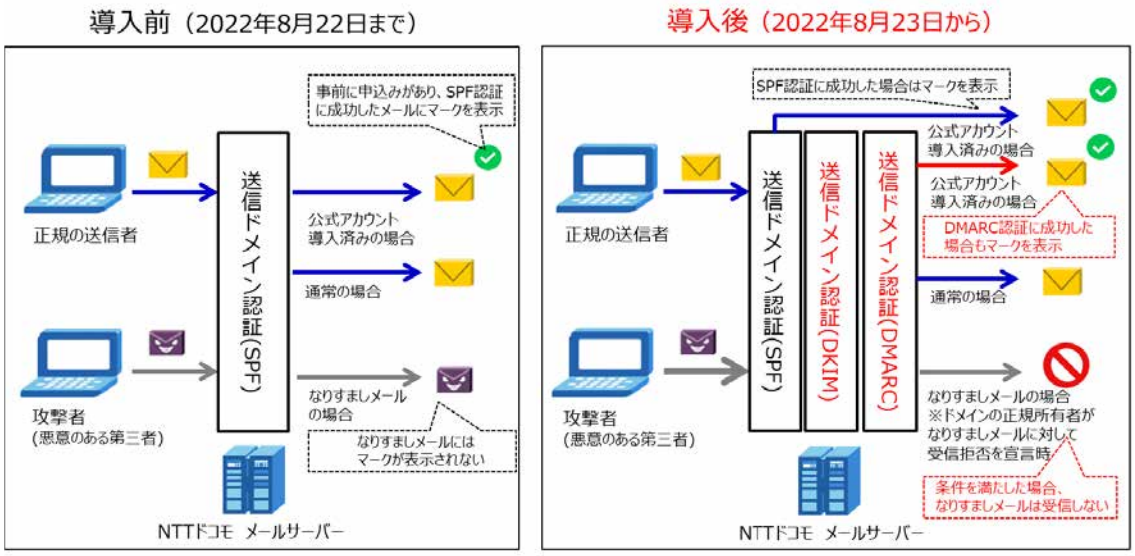
トピックス

2022 年 8 月 23 日
株式会社 NTT ドコモ

ドコモメールに送信ドメイン認証技術「DMARC」「DKIM」を導入
～なりすましメールの判別精度向上によりフィッシング詐欺の対策を強化～

株式会社 NTT ドコモ（以下、ドコモ）は、お客さまにドコモメールをより安心してご利用いただくため、ドコモメールに送信ドメイン認証技術「DMARC※1」「DKIM※2」（以下、本技術）を、2022 年 8 月 23 日（火）から新たに導入いたします。本技術により、送信ドメインによる認証が強化され、なりすましメールの判別精度が向上いたします。



送信ドメイン認証によるなりすまし対策の概要

本技術は、送信ドメインの情報により、悪意のある第三者が送信するなりすましメールを、より高い精度で判別できる技術です。なりすましメールと判別した場合、お客さまにメールは届かないため、フィッシング詐欺による被害などを低減することが可能です。加えて、正規の送信者によるメールであることを証明する「ドコモメール公式アカウント」の機能についても、本技術が認証方法に追加されることで、公式アカウントマークの表示が増えるため、お客さまはより安心してドコモメールのサービスをご利用いただけます。

2021 年 5 月 25 日に提供開始した「ドコモメール公式アカウント」は、送信ドメイン認証技術の一つ SPF※3 を採用しました。公式アカウントから送信された正規のメールと判定できた場合に、公式アカウントマークを表示することで、お客さまがフィッシング詐欺メールではないと判別できる機能です。

今回、メールヘッダに含まれる送信ドメインを認証する DMARC、および DMARC の認証手段として DKIM を新たに導入したことで、SPF に加えて DMARC によって公式アカウントから送信された正規メールと判定できた場合についても公式アカウントマークを表示します。認証方法が増えることで公式アカウントマークの表示が増えるため、より多くの企業・団体の皆さまに、ドコモメールを効果的にご活用いただけます。

なお、本技術は、ドコモメールの「迷惑メールおまかせブロック」「詐欺／ウイルスメール拒否」「ドコモメール公式アカウント」機能を通じて、お客さまへご提供いたします。「詐欺／ウイルスメール拒否」「ドコモメール公式アカウント」機能について、ご利用料金は無料※4 です。

また、メールを送信する多くの企業・団体が DMARC を設定いただくことで、ドコモメールのお客さまになりすましメールが届かなくなります。

ドコモは、これからもお客さまにあんしんしてサービスをご利用いただくため、セキュリティ機能の強化に努めてまいります。

迷惑メール対策推進協議会 座長代理 櫻庭秀次様からのコメント

「このたびのドコモによる DKIM と DMARC の導入を心より歓迎いたします。迷惑メール対策推進協議会では、電気通信事業者や関係省庁など迷惑メール対策に関わる多くの関係者と連携し、効果的な迷惑メール対策を推進しています。迷惑メール対策において、送信ドメイン認証技術の SPF、DKIM、またそれらを活用する DMARC は、メール利用者にとって、またメールを送信する多くの事業社にとってもメールの受け取りを判断するための重要な技術です。特に、送信者をなりすますフィッシングメールを防止する観点でも重要であり、当協議会でも推進してきた技術となります。ドコモの導入によって国内での迷惑メール対策技術の普及がさらに促進することに期待しております。当協議会は、関係各位との連携を強化し、迷惑メールの根絶に向けて最前線で活動してまいります」

※1 DMARC(Domain-based Message Authentication, Reporting, and Conformance):DKIM、SPF を通じてメールドメインの認証を行い、メールドメインの正規所有者定めたポリシーに従い受信側がなりすましメールを取り扱う技術(RFC7489)です。

※2 DKIM(DomainKeys Identified Mail):メールに付与されている電子署名を用いて、該当のメールドメインから正しく送信されたメールかどうか確認、およびメールの改ざんが行われていないかを確認する技術(RFC6376)です。

※3 SPF(Sender Policy Framework):メールの送信元情報を用いて、該当のメールドメインから正しく送信されたメールかどうかを確認する技術(RFC7208)です。

※4 sp モード(有料)またはドコモメール持ち運び(有料)をご契約の場合は本機能を無料でご利用いただけます。迷惑メールおまかせブロックのご利用にはあんしんセキュリティのご契約(有料)が必要です。メールの送受信、クラウドサーバーとの同期の際は通信料がかかります。

本件に関する報道機関からのお問い合わせ先
株式会社 NTT ドコモ プロダクトデザイン部　ライフスタイルイノベーション・ヘルスケア担当 ライフスタイルイノベーション部セキュリティサービス担当 Mail:pb-security1-ml@nttdocomo.com

別紙

送信ドメイン認証技術「DMARC」について

1. DMARC 概要

DMARC とは、メールのなりすましや改ざんを検知し、メールドメインの正規所有者がなりすましメールに対して受信側で受け取りを拒否させるなどの規定が可能なメールセキュリティ技術の一つです。ドコモでは本認証結果に従い「迷惑メールおまかせブロック」および「詐欺／ウイルスメール拒否」機能にてなりすましメールの取り扱いを行います。
また、DMARC によって Header from ドメインの正当性が担保できる場合、「ドコモメール公式アカウント」の導入を希望される企業・団体は Header from ドメイン単位でドコモメール公式アカウントのお申込みが可能となります。
なお、DMARC は、内閣府消費者委員会（2020 年 12 月 3 日付「フィッシング問題への取組に関する意見」）や「政府機関などの対策基準策定のためのガイドライン（令和 3 年度版）」などで導入の促進が提言されており、急増するフィッシング詐欺メールなどの受信防止対策として期待されています。

2. 迷惑メールおまかせブロックについて

お客さまが受信したメールの件名、本文、ヘッダ情報などにより、迷惑メールを自動で判定し、ブロックするサービスです。DMARC 導入により、メールドメインの正規所有者がなりすましメールに対し「reject（受信拒否）」、または「quarantine（隔離）」と宣言している場合は、該当のなりすましメールを迷惑メールの専用フォルダに隔離します。
参考：https://www.docomo.ne.jp/service/omakase_block/

3. 詐欺／ウイルスメール拒否について

フィッシング詐欺などの危険な送信元からのメールや危険 URL が含まれるメールを拒否するサービスです。DMARC の導入により、メールドメインの正規所有者がなりすましメールに対し「reject（受信拒否）」と宣言している場合は、該当のなりすましメールはフィッシング詐欺などの危険なメールと判断し拒否します。
参考：https://www.docomo.ne.jp/info/spam_mail/rejection_setup/

4. ドコモメール公式アカウントについて

ドコモメールのフィッシング詐欺メール対策を目的に、ドコモおよびお申込み企業さま・団体さまの公式アカウントから送信されたメールに、ドコモメール上で公式アカウントのマークを表示する機能です。
お客さまは一目で公式アカウントからのメールであることがわかるので、あんしんしてメールの内容をご確認になれます。
DMARC の導入により、既存の SPF に加え DMARC にて送信ドメイン認証が成功する場合もお申込みいただくことが可能になります。
参考：https://www.docomo.ne.jp/info/spam_mail/official_account/

公式アカウントのマーク

5. 新たなりすまし対策の提供開始日

2022 年 8 月 23 日（火）

6. ご利用料金とご利用方法

（1）ドコモメールをご利用のお客さま

・ご利用料金　無料

・ご利用方法　新規お申込み時はすべてのお客さまに、自動で適用させていただいております

※sp モード(有料)またはドコモメール持ち運び(有料)をご契約の場合は無料でご利用いただけます。

※メールの送受信、クラウドサーバーとの同期の際は通信料がかかります。

※ご利用されないお客さまは、My docomo から設定変更いただけます。

（2）ドコモメール公式アカウントの導入を希望される企業・団体

・ご利用料金　無料

・ご利用方法　コーポレートサイトからお申込みいただけます

※ご利用には一定の条件があります。

https://www.ntt.com/business/services/official_account.html