トピックス

2024 年 5 月 22 日
株式会社 NTT ドコモ

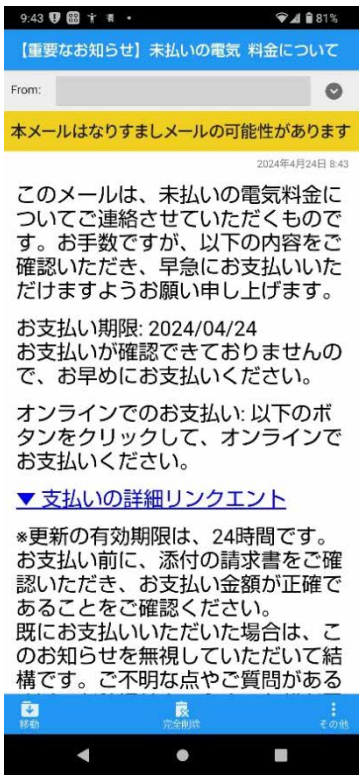
ドコモメールにフィッシング詐欺対策を目的とした「なりすましメールの警告表示機能」を導入

～フィッシング詐欺の可能性がある不審なメール開封時に警告を表示～

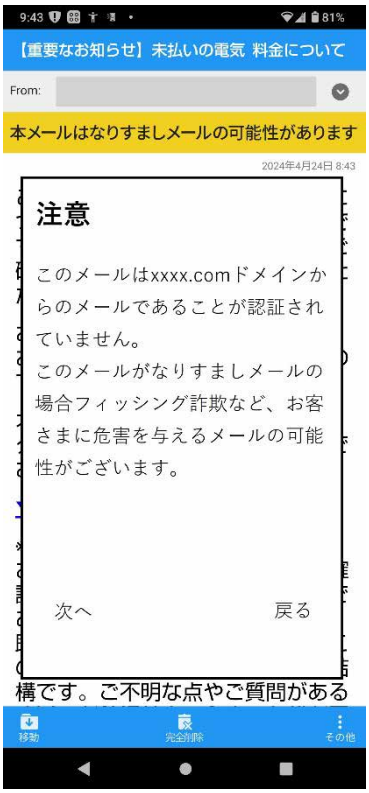
株式会社 NTT ドコモ（以下、ドコモ）は 2024 年 10 月（予定）から、フィッシング詐欺対策を目的にドコモメールにおける「なりすましメールの警告表示機能」（以下、本機能）を導入いたします。

本機能は、フィッシング詐欺の可能性がある不審なメールについて、なりすましメールの危険性があることを、メール本文表示の際や、本文中の URL 等から WEB ページに遷移する際に警告を表示することにより、お客さまが事前にフィッシング詐欺に気づく仕組みを設け、詐欺被害の発生を未然に防止します。

＜警告画面イメージ＞



メール本文閲覧時に警告表示



WEB 遷移前に再度警告

送信されたメールの発信元が正しい送信者であるかの確認は日本、及び世界各国で普及が進んでいる送信ドメイン認証技術「DMARC」※1 によって行います。「DMARC」の認証に失敗する、または送信元で「DMARC」未導入のメールを開封時に、なりすましメールの危険性があることの警告表示を行います。

また、本機能提供に際し、正しい送信元※2 からのメールにブランドロゴを表示させる国際標準技術「BIMI（Brand Indicators for Message Identification）」※3 を導入し、メール送信元の正当性を目視確認できる手段を拡張します。詳細は別紙をご確認ください。

ドコモは、今後もお客さまにあんしん・安全にサービスをご利用いただけるよう、フィッシング詐欺への対策※4 に努めてまいります。

※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　DMARC によって、正当性が担保されている送信元をさします。

※3　BIMI(Brand Indicators for Message Identification):DMARC 認証が成功した場合にメール送信者が公開している認証マーク証明書（VMC）やロゴデータを受信サーバで確認し、メールアプリ上で公式ロゴを表示させるアイコン表示標準技術です。

※4　ドコモのおけるフィッシング詐欺対策に関する取り組みついては、以下サイトをご確認ください。
フィッシング詐欺への対策 被害に遭わないために
https://www.docomo.ne.jp/info/anti-phishing/prevention/

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 第一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

「なりすましメールの警告表示機能」「BIMI」の概要

1. 「なりすましメールの警告表示機能」について

ドコモメールにおけるフィッシング詐欺の可能性がある不審なメールについて、なりすましメールの危険性があることをメール本文表示の際や、本文中の URL 等から WEB ページに遷移する際に警告を表示することにより、お客さまが事前にフィッシング詐欺に気づく仕組みを設け、詐欺被害の発生を未然に防止する機能です。送信ドメイン認証「DMARC」によって、メールアドレスのなりすましを検知する仕組みであり、「DMARC」の認証が成功している場合、該当のメールはなりすましメールではないと判断が可能となります。

ドコモメールでは以下の条件のいずれかを満たす場合、なりすましメールである可能性があるメールとして取り扱い警告を表示します。

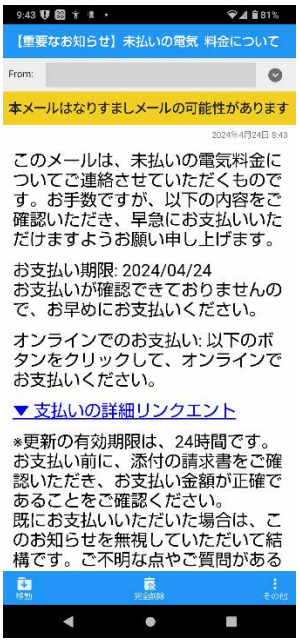
＜警告が表示される条件＞

・送信ドメイン認証「DMARC」によって認証されていないメール（認証失敗※1、または未導入）

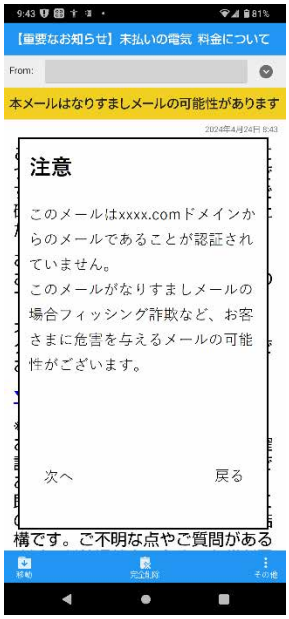
・フィッシング詐欺を行うなりすましメールの特徴を含むメール

＜警告画面＞

メールの本文、およびメールヘッダ画面にてわかりやすく警告を表示します。



メール本文内の URL を押下した際に、再度なりすましメールの危険性について警告します。



2. ブランドロゴを表示させる国際標準技術「BIMI」導入について

正しい送信元からのメールにブランドロゴを表示させる国際標準技術「BIMI（Brand Indicators for Message Identification）」を導入し、メール送信元の正当性を目視確認できる手段を拡張します。

ドコモメールでは 2021 年より、「ドコモメール公式アカウント」にお申込みいただいた企業さま・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サービスを提供してまいりましたが、「BIMI」の導入により、ドコモメール公式アカウント未導入のメールにおいてもお客さまが正規メールであることが判別できるようになり、より安心してドコモメールをご利用いただけます。

＜正規メールの判別手段＞

これまで	新しい対策導入後
・ドコモメール公式アカウント	・ドコモメール公式アカウント ・ブランドロゴ（BIMI によって指定された送信元組織が登録したロゴ）※2

＜ドコモメール公式アカウントマーク、および BIMI によりブランドロゴ(例:docomo)が表示されたメール画面＞

3. 提供開始日

2024 年 10 月（予定）以降

4. ご利用料金とご利用方法

（1）Android スマートフォンにてドコモメールをご利用のお客さま

・ご利用料金　無料

・提供開始　2024 年 10 月（予定）

・ご利用方法　提供開始以降にドコモメールアプリを最新版にアップデートいただくことでご利用が可能なります

（2）iPhone/iPad、ドコモケータイ、パソコン等にてドコモメールをご利用のお客さま

・ご利用料金　無料

・提供開始　2025 年 1 月（予定）

・ご利用方法　提供開始以降にブラウザ版ドコモメールにアクセスいただくことでご利用が可能になります

5. 【法人のお客さまへ】ドコモメール宛に E メールを送信する場合の依頼事項

■DMARC の導入（強く推奨）

送信ドメイン認証「DMARC」の導入されていない場合は、なりすましメールである可能性があるメールとして取り扱い、メール閲覧時に警告を表示します。企業または団体さま等の独自のドメインからドコモメール宛に E メールを送信する場合は 2024 年 9 月までに「DMARC」の導入をお願いいたします。

■ドコモメール公式アカウントの導入（推奨）

お客さまのあんしん安全のため、ドコモメール公式アカウントの導入についてご検討をお願いいたします。ドコモメール公式アカウントはこちらからお申し込み可能です。ご利用料金は無料です。

＜申し込み先＞

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

※1　「DMARC」の宣言が「none」「quarantine」「reject」いずれの場合も適用されます

※2　ブランドロゴはサービス開始時、メールヘッダ画面に表示予定です。