2023.04.03

サイバーセキュリティニュース ＜2022 No.003＞

サイバー空間における安心・安全なコミュニケーションとは

【要旨】
■ メールや SMS（ショートメッセージサービス）を起因とした事件・トラブルは増加傾向にある。
■ 本稿では、メールや SMS を起因とした事件・トラブルが増加している背景・要因と、サイバー空間における安心・安全なコミュニケーションのポイントについて解説する。

１．メールや SMS 起因の事件・トラブルは増加傾向に

メールや SMS（ショートメッセージサービス）を起因とした事件・トラブルは増加傾向にある。独立行政法人日本情報処理推進機構（ＩＰＡ）「情報セキュリティ 10 大脅威 2023」では、個人編においては 6 つ、組織編においては 4 つがメールや SMS を攻撃手口・起因とするものがランクインした。また、警察庁の調査「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」によると、インターネットバンキングに係る不正送金事件については、2020 年以降、発生件数、被害額ともに減少傾向が続いていたが、昨年下半期に急増し、その被害の多くがフィッシングによるものとみられている。

コロナ禍を乗り越え、多様な働き方や効率的な業務フローが浸透しつつある現代において、メール（以下、SMS を含む）はビジネスや個人間のコミュニケーションに不可欠なツールである。メールには、機密情報、金融情報、個人情報、業務上の秘密など、多くの重要な情報を含んでいることがあり、メールに対する不正アクセスや情報漏えいは、業務上の損失や個人情報の漏洩など、深刻な経済的、社会的影響をもたらすことがある。また、メールはフィッシング、スパムメール発信、マルウェア感染などのサイバー攻撃の手段としても利用されることがあり、これらの攻撃によって、個人や企業の機密情報や資産が危険にさらされることがあるのは「情報セキュリティ 10 大脅威 2023」で示されているとおりである。

【表 1 】「情報セキュリティ 10 大脅威 2023」2023 年 1 月 25 日公開（独立行政法人情報処理推進機構）

	個人編	組織編
1位	フィッシングによる個人情報等の詐取	ランサムウェアによる被害
2位	ネット上の誹謗・中傷・デマ	サプライチェーンの弱点を悪用した攻撃
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	標的型攻撃による機密情報の窃取
4位	クレジットカード情報の不正利用	内部不正による情報漏えい
5位	スマホ決済の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	不正アプリによるスマートフォン利用者への被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	偽警告によるインターネット詐欺	ビジネスメール詐欺による金銭被害
8位	インターネット上のサービスからの個人情報の窃取	脆弱性対策情報の公開に伴う悪用増加
9位	インターネット上のサービスへの不正ログイン	不注意による情報漏えい等の被害
10位	ワンクリック請求等の不当請求による金銭被害	犯罪のビジネス化（アンダーグラウンドサービス）

２．事件・トラブル（＝サイバー攻撃）増加の背景、要因

メールを手口とするサイバー攻撃の大半において「なりすまし」が行われている。すなわち、実在する人物になりすましてメールを送りつけ、何度かメールのやり取りを行うことで信用させた後に攻撃を実行するケースが多くみられる。「なりすまし攻撃（Spoofing）」は、決して新しい攻撃手法ではなく古くからあるものだが、なぜ増加傾向にあるのか考察する。

（理由１）攻撃技術の進歩

メールヘッダーを偽装することで、あたかも実際とは異なる送信者によるメールであるかのようにみせかけるのはもはや常套手段となっている。近年の攻撃メールでは、メールヘッダーだけでなくメール本文も巧妙に作り込まれている。これまで日本語は「特殊かつ難解な言語」のために、攻撃グループのターゲットとなる優先順位は決して高くなかったが、自動生成ＡＩの普及により「言語の壁」はなくなりつつある。

（理由２）メールは盗聴されている

メールクライアント方式では、標準では暗号化の機能を備えていないため、メールそのものやその通信経路に「鍵をかける（暗号化）」する必要がある。攻撃者は暗号化対応していないメール通信を盗聴し、前述の「巧妙なメール本文」を作成するための情報を収集している。日本企業においては、後述の「PPAP」方式が広く普及しているためにメールそのものの暗号化は進んでいないとみられている。

（理由３）働き方の多様性と利便性が仇に

テレワークやオンラインショッピングが増えたことでメールの使用頻度が高まり、これに伴ってメールを使ったサイバー攻撃が増加している。従業員自宅のネットワークセキュリティは企業のネットワークセキュリティと比べて脆弱であることが多く、また、すぐそばに相談できる人間がいないことも攻撃成功の確率を高めている要因といえる。

日本国内では、金融機関を装ったフィッシングメールが圧倒的に多いが、近年では、宅配業者の不在通知や通信事業者の料金支払い確認を装った SMS や、政府になりすまして新型コロナウイルスに関する情報提供と称したメールを発信、フィッシングサイトに誘導する手口が多くみられる。また、経営者や財務担当役員になりすまして従業員に攻撃者が用意した口座へ資金を振り込ませたり、取引実績のある企業の担当者になりすまして偽の請求書を送りつけて金銭を振込させるビジネスメール詐欺が増えているのは、上記の働き方の多様性の広がりと無関係ではないだろう。

（理由４）日本独自のメール文化

日本企業においては、添付ファイル付きのメールをやり取りする際、「PPAP」と呼ばれる手順が広く用いられている。PPAP とは、パスワード（Password）付きファイルの送付、パスワード（Password）の送付、暗号化（Angouka）、プロトコル（Protocol）の頭文字を取って作られた造語である。この方式は、以下 2 つの観点からセキュリティ対策として不十分どころか、かえって危険性が増す。

① 同じ通信経路を辿ってメールを 2 回送信（1 通目：ファイル、2 通目：パスワード）するため、1 通目のメールが盗聴されてしまえば、パスワードが付された 2 通目も盗聴可能

② パスワード付き zip ファイルの中身は暗号化されるため、マルウェアが仕込まれていたとしてもウイルスチェックを回避してしまい、マルウェアが組織内ネットワークへ侵入・感染してしまう

2020 年にマルウェア「Emotet」が流行した際には、パスワード付き zip ファイルからの感染を狙い、日本の企業が標的にされた。同年 11 月、政府が PPAP 廃止の方針を打ち出し、大手企業や先進的な IT 企業では脱 PPAP が進むも、実態はまだまだ PPAP 方式でメールやり取りをする企業が多い。

（理由５）「ヒトの脆弱性」は解消できない

テレワークをはじめとした場所を問わない多様な働き方の浸透によって、その環境やテレワーク製品の脆弱性だけでなく、人間の心理や行動の脆弱性を突いた攻撃も根強い。焦りの感情や認知的なバイアス、手順のショートカットやスキップといった軽微な違反を完全に排除することは不可能である。攻撃者はそれを知ったうえで十分な調査・内偵活動を重ね、攻撃プランを計画している。

３．安心・安全なメールコミュニケーションに必要な対策

「盗まれない」「なりすましをされない」「メールとは別の手段を使う」「だまされない」観点から、以下にて安心・安全なメールコミュニケーションに必要な対策について解説する。

（１）「盗まれない」対策

攻撃者になりすましをされないよう、自身のアカウントやメールのやり取りを保護する対策としては、以下が挙げられる。

① メールソフトやメールサーバーのアップデートを定期的に行う
セキュリティホールの修正や新しいセキュリティ機能の追加を受けることで、メールアカウントへの攻撃や不正アクセスのリスクを最小限に抑える。

② メールアカウント認証を強固なものにする
メールアカウントを乗っ取られてなりすましの「踏み台」にされないよう、パスワードは長さが十分にある、大文字小文字や数字、特殊文字が含まれているものを使用したり、二段階認証や多要素認証を導入し、メールアカウントに対するセキュリティレベルを向上させる。

③ メールを暗号化する
配信中のメールが盗み見られないよう、通信経路は SSL/TLS 方式を使用する。SSL/TLS は該当のサーバーが第三者機関によって安全が保障されていることを認証する仕組みである。また、通信経路だけでなくメールそのものと添付ファイルを暗号化と電子署名のために使われるプロトコル S/MIME（Secure Multipurpose Internet Mail Extensions の略）方式も推奨する。盗聴防止だけでなく、送信メールに「電子署名」をすることで、受信者側はその本人から送信されていることが確認でき、また改ざんを検知することができる。

（２）「なりすましをされない」対策

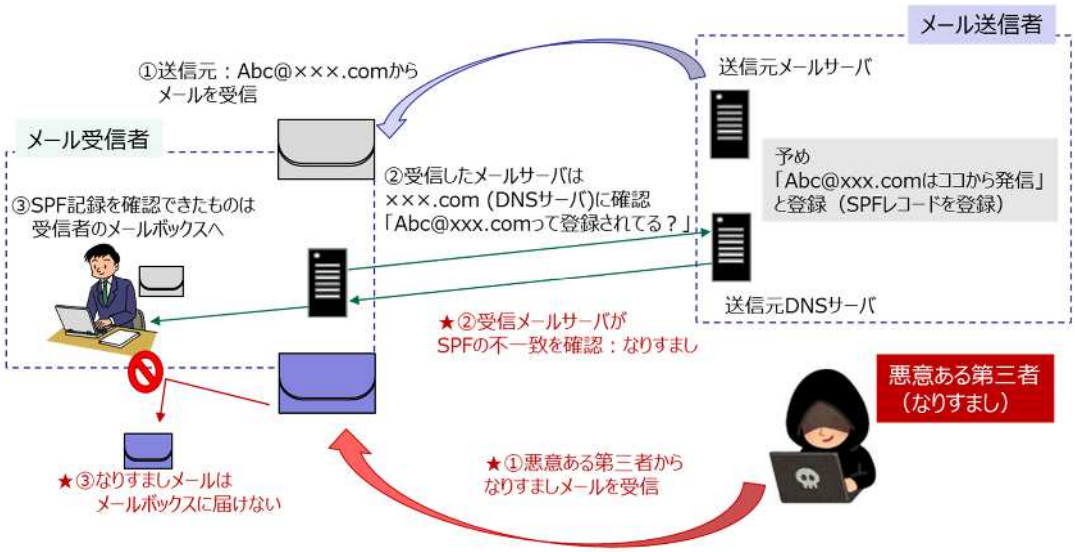
自身がなりすましをされていないことを証明する手段として、「送信ドメイン認証」が有効である。送信ドメイン認証とは、送信元メールサーバーの IP アドレス認証や電子署名の仕組みを利用して、メールがなりすまされているかを判断する仕組みであり、大きく以下の３種類がある。

① SPF（Sender Policy Framework）
予め送信元の DNS（ドメインネームシステム）サーバーに正当な SPF レコード（例：Abc@xxx.com はこのサーバーから発信する）を記述、メール受信者は、メール送信元 DNS サーバーにある SPF レコードを照合してなりすましがないかを確認する仕組み。ただし、転送されたメール等は、SPF レコードに登録した以外のメールサーバーを経由することから正しく判定できず、メールソフト上で表示される差出人（ヘッダ From）や本文の詐称はチェ

ックできない。また、送信されてきたメールを認証できないときは、それがなりすましメールなのか技術的な問題で認証できないだけか、受信側では判断ができない点に留意されたい。

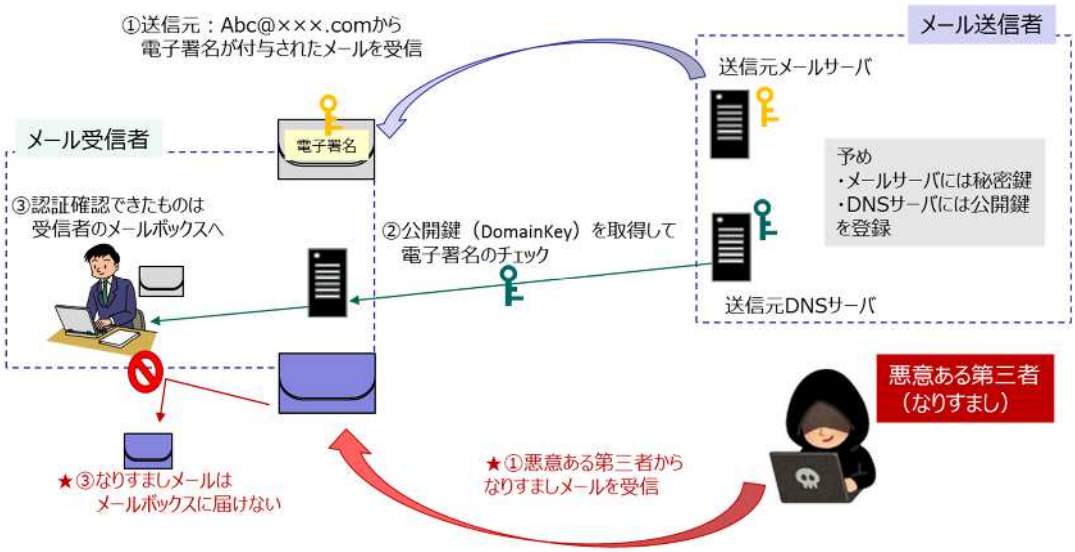
② DKIM（DomainKeys Identified Mail）

メールにデジタル署名をつけることで、送信者が本当にそのメールを送信したことを確認する仕組み。SPF と違って転送されてきたメールを誤判定せず、メールの本文やヘッダが改ざんされていないかもチェックできるが、SPF に比べ負担が大きく専門知識が必要とされる。また、送信されてきたメールを認証できないときは、それがなりすましメールなのか技術的な問題で認証できないだけか、受信側では判断ができない点は SPF と同様である。



【図１】SPF のしくみ

（ＭＳ＆ＡＤインターリスク総研が作成）



【図２】DKIM のしくみ

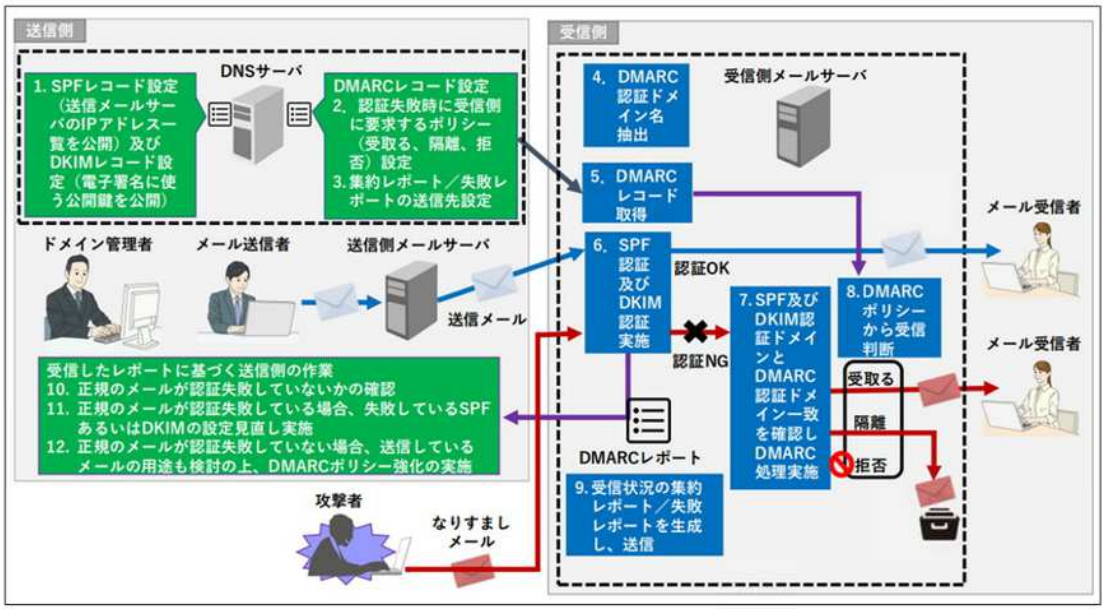
（ＭＳ＆ＡＤインターリスク総研が作成）

③　DMARC（Domain-based Message Authentication、Reporting and Conformance）

SPF や DKIM のような送信元認証技術を組み合わせて、偽装メールを検知し、送信元ドメインの偽装を防止する仕組み。

DMARC は、送信メールの認証失敗時（正当なメールと判断できないとき）に、受信者がそのメールに対してとるべき処理方法を指定しておくことができる。また、メールの処理結果を受信側のメールサーバーから送信側メールサーバーへレポートする機能もあり、送信側は、送信したメールが受信側でどのように処理されたかを把握できる。ただし、導入と運用には DKIM 以上に負担が大きくかかり、専門知識が必要とされる。

2023 年 2 月 1 日に経済産業省、警察庁および総務省は、利用者保護の観点から、クレジットカード会社等において適切な対応が取られることが必要として、クレジットカード会社等に対して DMARC の導入をはじめとするフィッシング対策の強化を要請している。なお、総務省「令和４年度情報通信白書」によると、日本企業（≒JP ドメインを利用するもの）における、なりすましメールを防止するための送信ドメイン認証技術の導入状況は、SPF は約 67.5%、DMARC は約 2.1%と決して高くない。



【図３】DMARC のしくみ

（出典：迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル」）

（３）「メールとは別の手段を使う」

前述のとおり、大手企業や先進的な IT 企業では脱 PPAP が進み、以下の手段を用いてファイルの共有やコミュニケーションを行うケースが見られる。いずれも PPAP で指摘されるリスクの低減に向けた配慮がなされているが、運用にあたっては追加のコストがかかり、また一定の課題がある。自社と取引先で取り扱うデータに応じて、セキュリティと利便性の適切なバランスの取れた手段を選択する必要がある。

【表２】「脱 PPAP」として利用される手段の例

手段	概要	課題
ファイル転送サービス	ファイルのダウンロードリンクをメールに記載して相手先に送付し、相手がファイルをダウンロードする	リンク案内メールの誤送信リスクが残る
ビジネスチャットツール	ビジネスチャットツールに直接アップロードしてファイルを共有	自社、相手企業の両方でアカウントを持っている必要がある
クラウドストレージ	クラウドストレージに ID とパスワードでログインしてファイルを共有する	共有範囲の設定ミスやユーザー権限の設定ミス、共有リンクの送り間違いなど情報流出のリスクがある

（４）「だまされない」対策

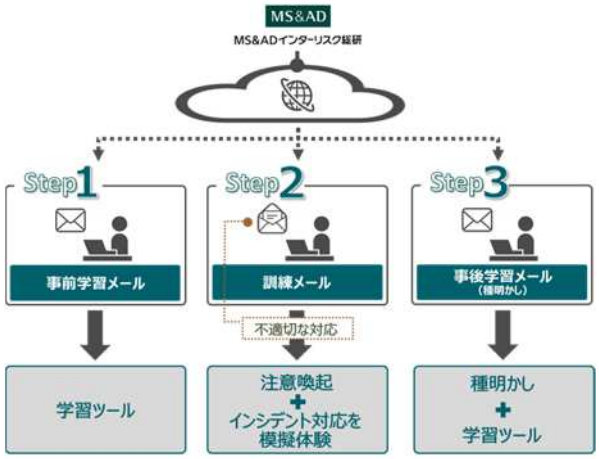
これまでの述べた対策を実施したとしても、不審なメールが一切届かなくなることはなく、ICT 機器を利用するすべての者に対して適切な教育と注意喚起が欠かせない。不審なメールに気付くポイント（タイトル、送信者アドレス、メール本文の言い回し、添付ファイルの内容など）を習得させることは最低限必要であり、万が一不審なメールを開封した際に、迅速かつ適切な対応ができるよう、初動対応の手順を役職員に習得させることも必要である。受動的な教育・研修だけでなく、想定されるインシデント発生局面に応じたシナリオを用いた訓練の実施も有効である。訓練は、参加者の習熟度、訓練実施の目的に応じたプログラムを企画することが肝要である。

本稿がサイバー空間における安心・安全なコミュニケーションの参考となり、サイバーセキュリティ対策強化の一助となれば幸いである。

ＭＳ＆ＡＤインターリスク総研株式会社
リスクマネジメント第三部 サイバーリスクグループ
マネジャー・上席コンサルタント　岡田　道雄

ＭＳ＆ＡＤインターリスク総研株式会社では、標的型攻撃を巧妙に模した「訓練メール」を訓練参加者に送信し、その対応を個々人に評価する「標的型メール訓練サービス」を提供しています。

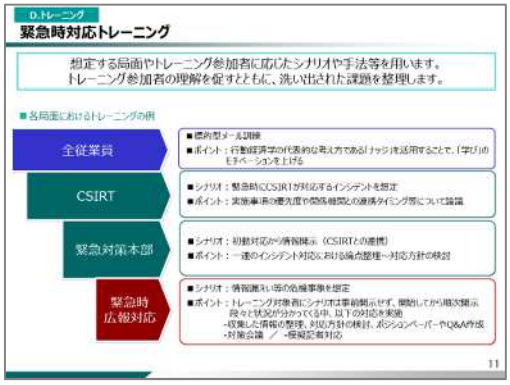
本サービスは、行動経済学の代表的な考え方である「ナッジ」を活用することで、「学び」のモチベーションを上げることを志向するとともに、訓練結果報告書に基づいて従業員個々人の不審なメールに対するリスク感度や学習の深度に応じたフォローアップを行うことができます。

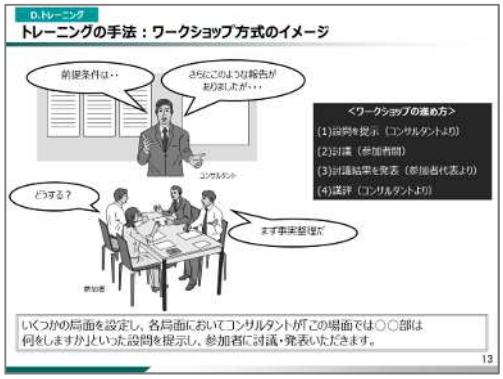


【学習コンテンツのイメージ】

また、危機発生時において求められる、事実確認、情報共有化、意思決定、対策実行、情報開示に関するトレーニングを企画、お客さまの実践力を検証します。

想定する局面やトレーニング参加者に応じたシナリオや手法等を用いて、トレーニング参加者の理解を促すとともに、洗い出された課題を整理します。





ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第三部 サイバーリスクグループ
東京都千代田区神田淡路町2-105 **TEL.03-5296-8932**
https://www.irric.co.jp/