フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングメール詐欺：手口と対策
解説ドキュメント

2024 年 2 月

フィッシング対策協議会
証明書普及促進ワーキンググループ

目次

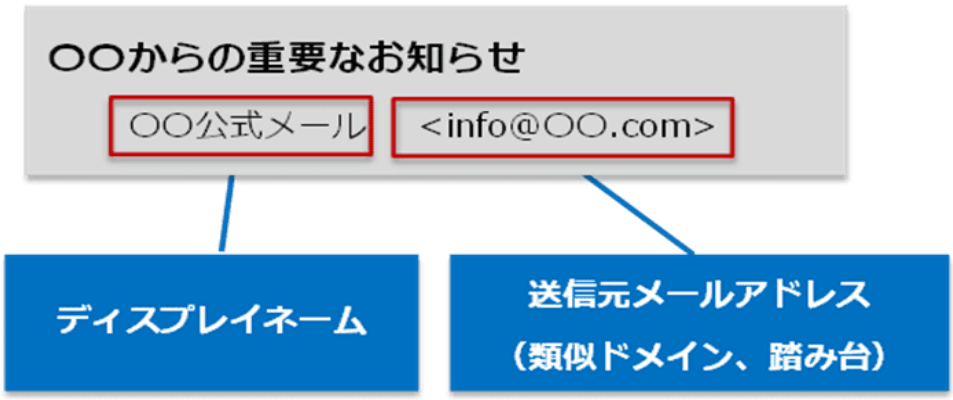
1　はじめに

本ドキュメントは、日本国内のフィッシング詐欺における、なりすましメールの手口とその対策方法について解説しています。2023 年 2 月に経済産業省、警察庁および総務省は、クレジットカード番号などの不正利用の原因となるフィッシング被害が増加していることを鑑み、クレジットカード会社などに対して、送信ドメイン認証技術（DMARC：ディーマーク）*1* の導入をはじめとするフィッシング詐欺対策の強化を要請した。*2*

2023 年に 6 月にフィッシング対策協議会の技術・制度検討ワーキンググループが公開した「フィッシングレポート 2023」*3* によると、送信元メールアドレスに正規サービスのドメインを使用した「なりすまし」送信メールが継続していて、観測している受信メールアドレスで受信したフィッシングメールの内、平均約 71.6%、最大で 89.9%が「なりすまし」送信メールだった。利用者を保護するために、S/MIME 署名や送信ドメイン認証技術（DMARC）、正規メールにはブランドアイコンが表示される（BIMI（VMC 証明書））などフィッシング対策を強化しているサービス事業者もある。なりすましメールの手口やその対策方法を理解することで、フィッシング詐欺に遭わないための一助になれば幸いです。

2　なりすましメールの手口

本章では、なりすましメールの代表的な手口である、ディスプレイネーム、類似ドメインと踏み台について解説する。



1 DMARC: Domain-based Message Authentication, Reporting, and Conformance の略称。電子メール認証プロトコルの一つで、電子メールのドメイン所有者が、保有するドメイン認証を通さずに利用されること（なりすましメール、フィッシングメール、詐欺メールその他の脅威)を防止できることを目的に設計された。

2 https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

3 https://www.antiphishing.jp/report/wg/phishing_report2023.html

2.1　類似ドメイン

2.1.1 類似ドメインとは？

類似ドメイン名とは、「正規のドメイン名と視覚的に似たドメイン名（例えば、異なる TLD [4] を利用することや文字列の一部を置き換えるなど）」を利用して、正しい宛先からのメールであることをかたる手口であり、そのうち異なる言語を組み合わせて視覚的に似たドメイン名をホモグラフドメインと呼ぶ。

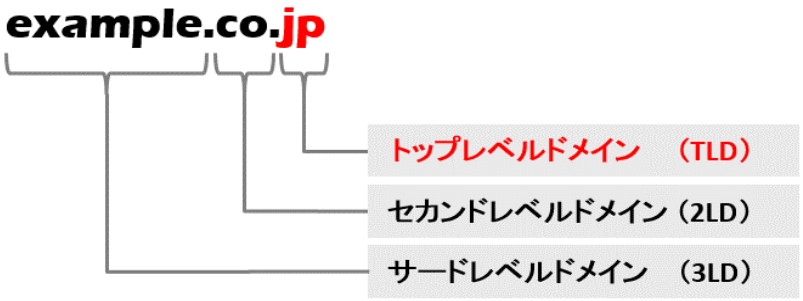


図 1 TLD（出典：株式会社日本レジストリサービス）

【類似ドメインによるなりすましの例】

- Amᵃzon.com（ホモグラフドメインを利用）
- Amaz0n.com（PSL [5] レベルで類似なものを利用）
- Amazon.example（TLD を変える）
- Amazon.com.asdfasdfa.xyz（サブドメインが同一、ドメイン名は別のもの）

---

4 Top Level Domain の略称。インターネットのドメインは、ルート（.）と呼ばれる頂点を持ち、そこから木を逆さまにしたような形（階層構造）で構成されています。ルートの最初の分岐（ルートの直下）がトップレベルドメイン（TLD）で、以降、セカンドレベルドメイン（2LD）、サードレベルドメイン（3LD）というように階層構造が構成される。

5 Public Suffix List の略称。インターネットのドメイン名を階層化する際に、個々のトップレベルドメイン（TLD）の一部として扱われるべきかどうかを定義するリストです。

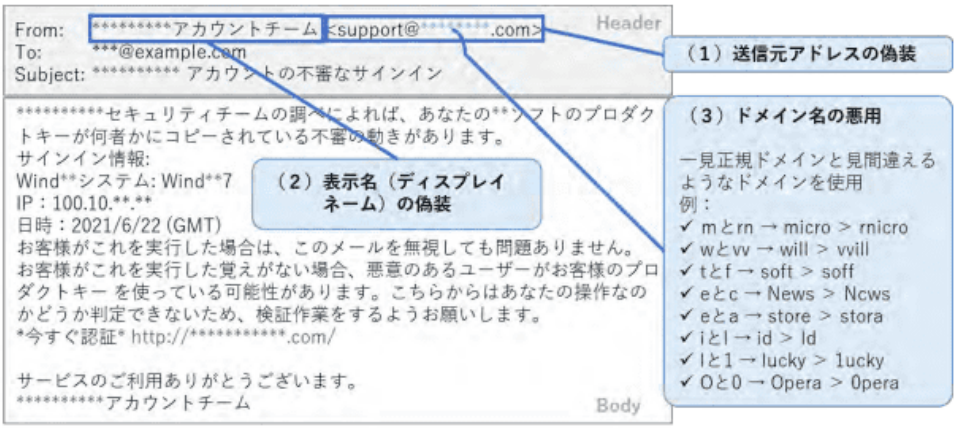


図 2 送信元の偽装（出典：迷惑メール白書 2021）

■本物のメールアドレス	alice @ company-□ . com	
■偽物のメールアドレス	① alice @ compnay-□ . com	一文字入れ替える
	② alice @ companys-□ . com	一文字追加
	aalice @ company-□ . com	
	③ alice @ comp ny-□ . com	一文字削除
	④ alice @ cornpany-□ . com	誤認しやすい文字へ変更
	⑤ alice @ company-□ . net	トップレベルドメインを変更
	⑥ alice-company-□ @ freemail.com	フリーメールアドレスを使う

図 3 攻撃者が使用する使う詐欺メールアドレスのパターン例

（出典：IPA ビジネスメール詐欺（BEC）の特徴と対策）

【類似ドメインによるなりすましの見分け方】

・ アドレス帳に入っているものと突き合わせて同じものか確認する

・ 迷惑メールフィルターで怪しいとなったものには注意する

2.2 ディスプレイネーム

2.2.1 ディスプレイネームとは？

ディスプレイネーム（表示名）とは、メールの一覧画面や受信画面でメールアドレスの補足情報として、送信者の名前で表示される情報のことで、この情報は送信者が自由に設定可能であるため、悪意ある送信者が第三者をかたるという手口である。

【ディスプレイネームによるなりすましの例】

・ 正しいドメイン名を表示名に入れる、「サポートチーム」といった名称を入れる など

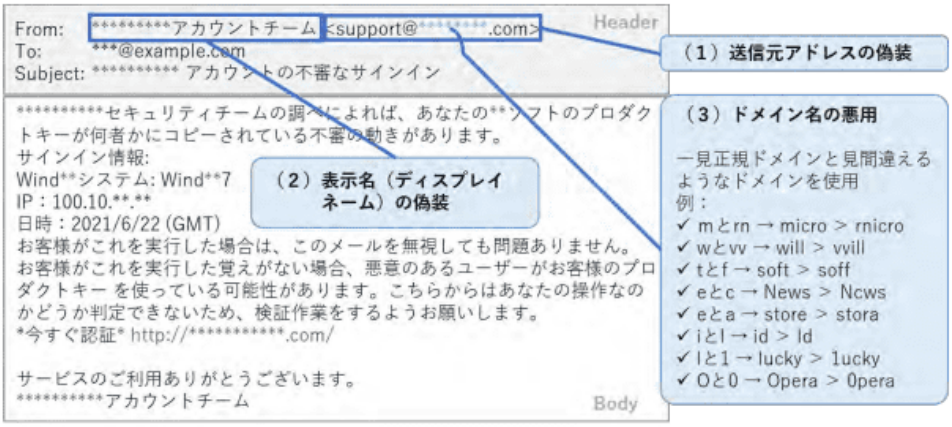


図 4 送信元の偽装（出典：迷惑メール白書 2021）

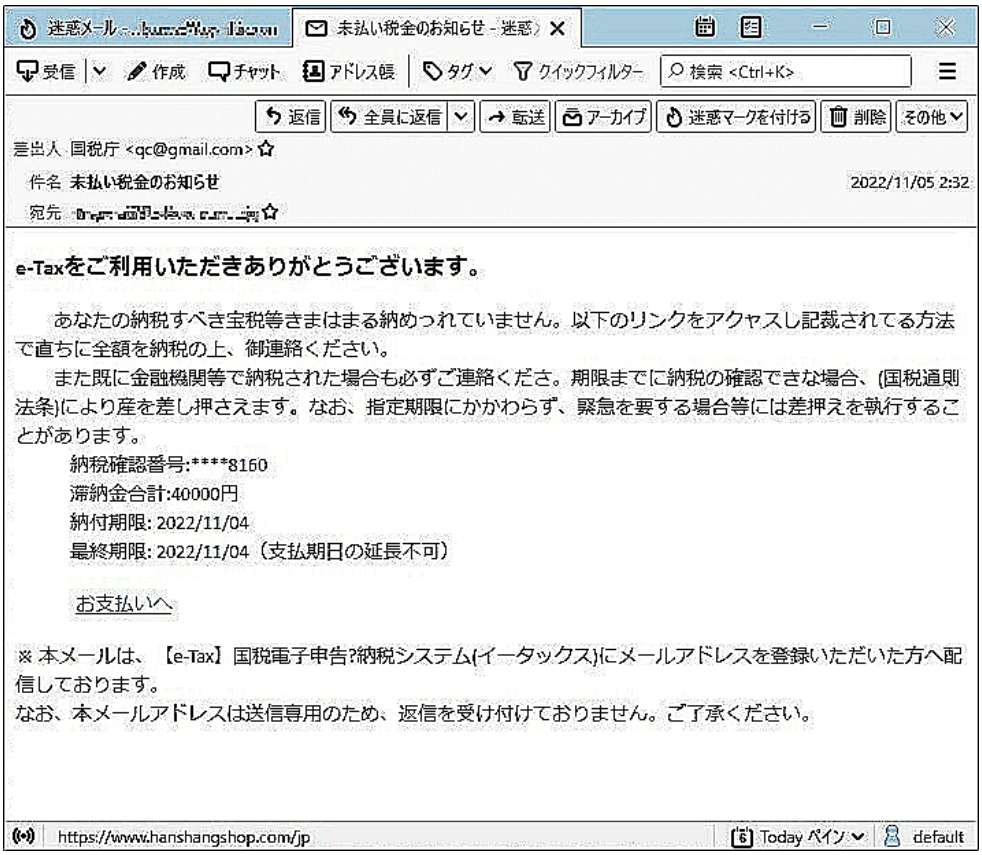


図 5 国税庁をかたる例（出典：インプレス「INTERNET Watch」）

【ディスプレイネームによるなりすましの見分け方】

・ 表示名（ディスプレイネーム）は補足情報なので、メールアドレスもあわせて確認する

・ 表示名にメールアドレスを書く手口もあるので気を付ける

2.3 踏み台

2.3.1 踏み台とは？

正当なドメイン名所有者ではない、もしくは所有者からの委託を受けていない第三者のメール

サーバーから、正当なドメイン名の From アドレスをもったメールを送信する手口（利用された第三者のメールサーバーを踏み台と呼ぶ）。もしくは、第三者がメールサーバーをたてて、正当なドメイン名の From アドレスをもったメールを送信する手口である。

【踏み台によるなりすましの例】

・ From アドレスが自分の管理化にあるものか確認しないメールサーバーを利用して、正当なドメイン名の From アドレスをもったメールを送信する

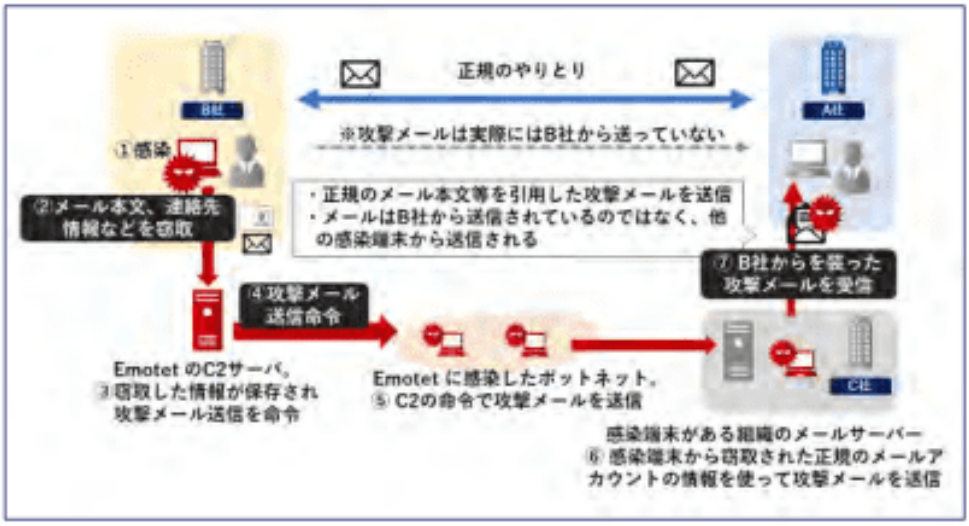


図 6 Emotet のなりすましメール送信イメージ（出典：迷惑メール白書 2021）

【踏み台によるなりすましの見分け方】

・ 送信者認証の結果を確認する

・ 内容が怪しかったら開かない

3　なりすましメールの事例

巧妙に URL リンクをクリックさせるような件名、送信者名（表示名・メールアドレス）メール本文で配信する。スマートフォンから見ると、正規のものであると誤認させるような URL も多々見受けられる。

3.1　EC サイトを装ったなりすましメール

「アカウントの支払い方法を確認できず、注文をキャンセル（または出荷）できません。」や「情報の有効期限が切れ、アカウントの使用が停止されました。」と言った、企業・組織の名前を騙ったなりすましメールが報告されている。

3.1.1 Amazon のなりすましメール

【メール件名（例）】

プライムの自動更新設定を解除しました。

【メール文面（例）】

図 7 Amazon のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/amazonQR_20230105.html

3.1.2 三越伊勢丹のなりすましメール

【メール件名（例）】

「三越伊勢丹 WEB 会員」のアカウントは終了いたしますのでお知らせいたします

【三越伊勢丹】WEB 会員停止のお知らせ

三越伊勢丹 WEB 会員　ログインのお知らせ

【メール文面（例）】

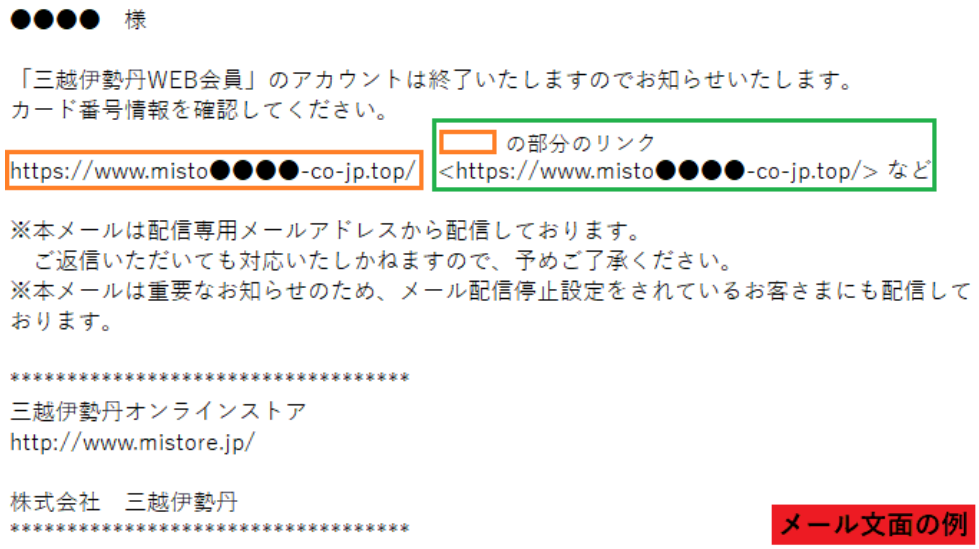


図 8 三越伊勢丹のなりすましメール文面（例）のイメージ

【詳細な情報】https://www.antiphishing.jp/news/alert/mistore_20220624.html

3.1.3 出前館のなりすましメール

【メール件名（例）】

出前館アプリ・サイトのメンテナンスについて

【重要】「出前館 アカウントの自動退会処理について

【メール文面（例）】

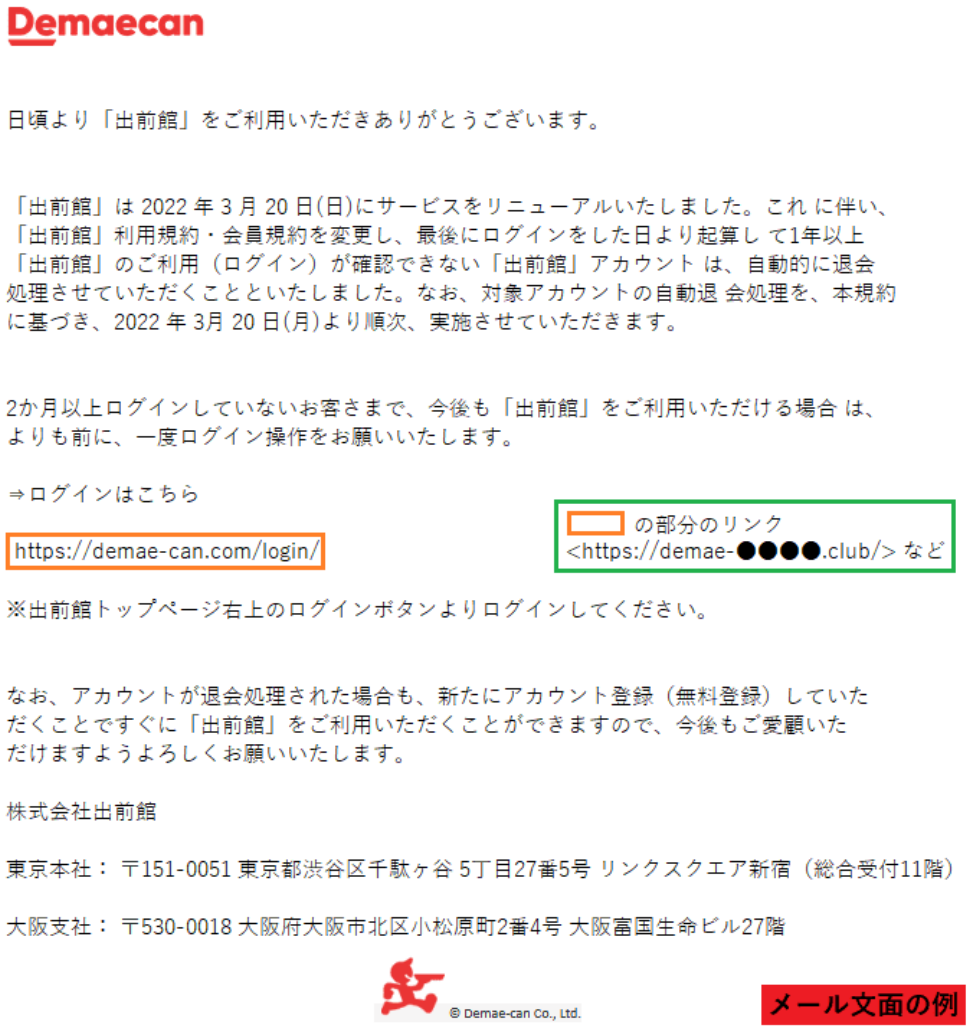


図 9 出前館のなりすましメール文面（例）のイメージ

【詳細な情報】https://www.antiphishing.jp/news/alert/demaecan_20220325.html

3.1.4 ZOZOTOWN のなりすましメール

【メール件名（例）】

ZOZOTOWN カスタマーサポートセンターよりご連絡

【メール文面（例）】

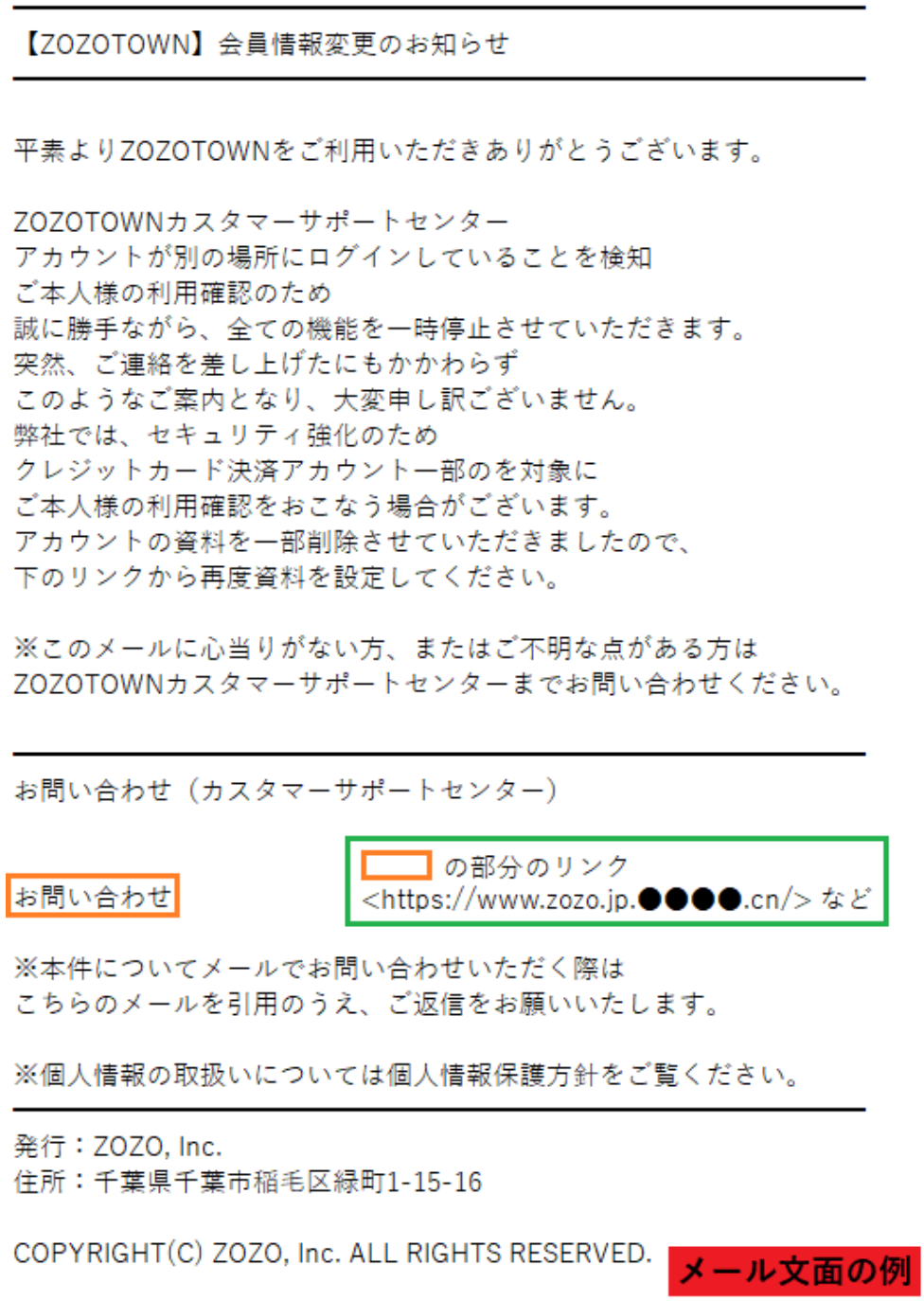


図 10 ZOZOTOWN のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/zozotown_20220415.html

3.1.5 Uber Eats のなりすましメール

【メール件名（例）】

【重要】ウーバーイーツ ご注文内容の確認 [メールコード UE●●●●]

【重要】Uber Eats ご注文内容の確認 [メールコード UE●●●●]

【メール文面（例）】

この度はEウーバーイーツをご利用頂きまして誠にありがとうございます。
以下のご注文内容がご利用店舗まで届いております。
※本メールは、お客様のご注文情報を受けた時点で送信される自動配信メールです。

店舗から、ご注文内容の確認後、ご連絡いたします。

合計金額：5,252円（税込）
支払金額：5,252円（税込）

▶注文確認

の部分のリンク
<https://www.●●.uob●●●●.com/> など

■STEP1　注文受付
↑ただ今こちら
■STEP2　注文受付完了
■STEP3　受渡完了

＜注文内容＞

[注文番号] 3082
[注文日時] 2022/1/27 15:24:15

[注文店舗] 餃子の王将大岡山店
[店舗住所] 東京都大田区北千束1-42-2
[注文者名] [redacted]
[支払方法] クレジット
[受取日時] 2022/1/27
[受取方法] 店内受取

[注文商品]
肉まん　3個 612円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
油淋鶏　1個 597円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
酢豚　1個 550円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
回鍋肉　2個 1,056円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
極王炒飯　1個 744円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
ニラレバ炒め　1個 528円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
キムチ炒飯(大盛)　1個 636円
　　お持ち帰りの箱代を別途いただいております。: 1商品につき箱代 +10円
醤油ラーメン　1個 529円

合計金額：5,252円（税込）
支払金額：5,252円（税込）

▶注文確認

※ご注文された店舗の受取り時間を参照のうえご連絡ください。
※当メールは送信専用メールアドレスから配信されています。

メール文面の例

図 11 Uber Eats のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/uber_eats_20220128.html

3.2　EC サイトで商品を購入した際のなりすましメール

決済に失敗したような内容でリンクのクリックを促す

【メール件名（例）】【楽天市場】アカウントの支払い方法を確認できず、注文を出荷できません。

【メール文面（例）】

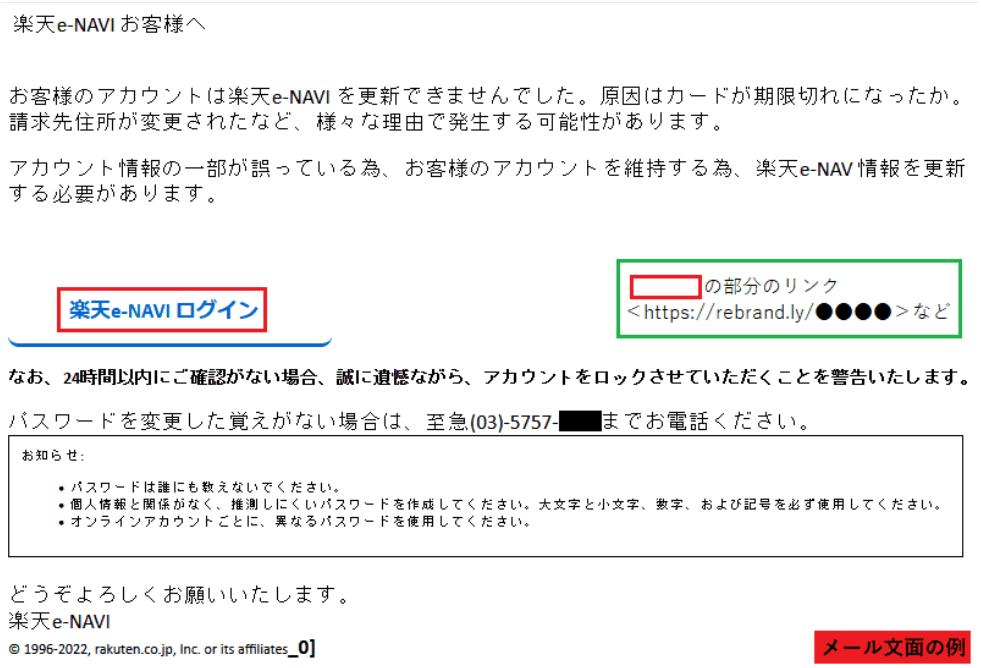


図 12 EC サイトで商品を購入した際のなりすましメール文面例

3.3　官公庁や公共サービスを装ったなりすましメール

3.3.1　警察庁のなりすましメール

【メール件名（例）】【警察庁】重要なお知らせ、必ずお読みください。

【メール文面（例）】

図 13 警察庁のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/npa_20221026.html

3.3.2 金融庁のなりすましメール

【メール件名（例）】

【金融庁緊急連絡】重要なお知らせ

【メール文面（例）】

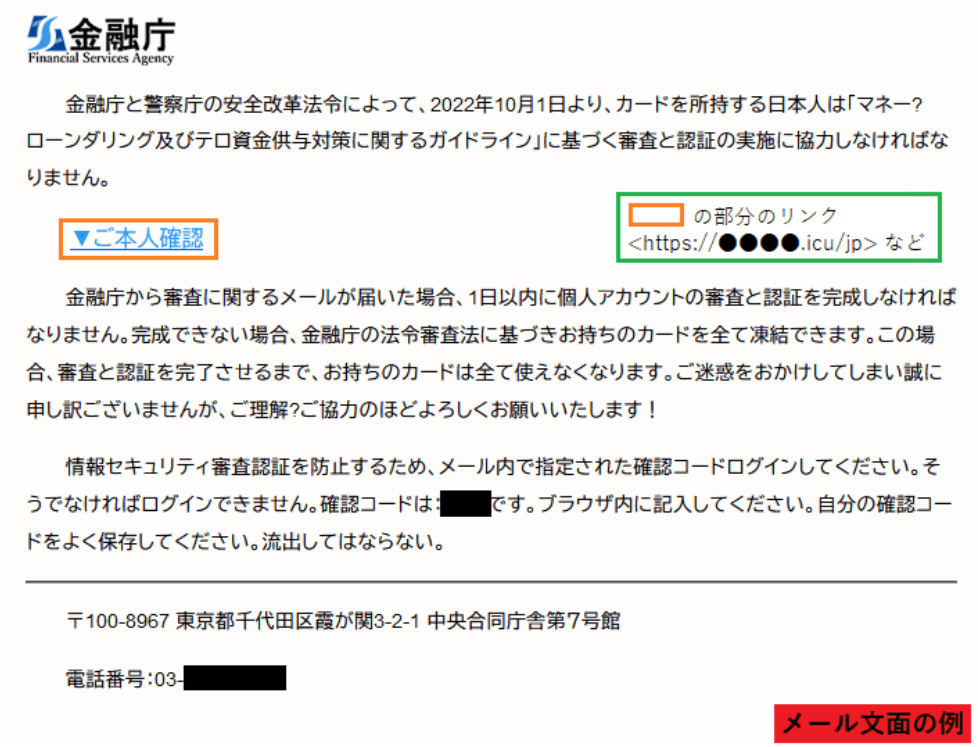


図 14 金融庁のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/fsa_20221004.html

3.3.3 国税庁のなりすましメール

【メール件名（例）】】

税務署からのお知らせ【申告に関するお知らせ】

未払い税金のお知らせ

【未払い税金のお知らせ】

税務署からの【未払い税金のお知らせ】

【督促状】滞納した税金がございます

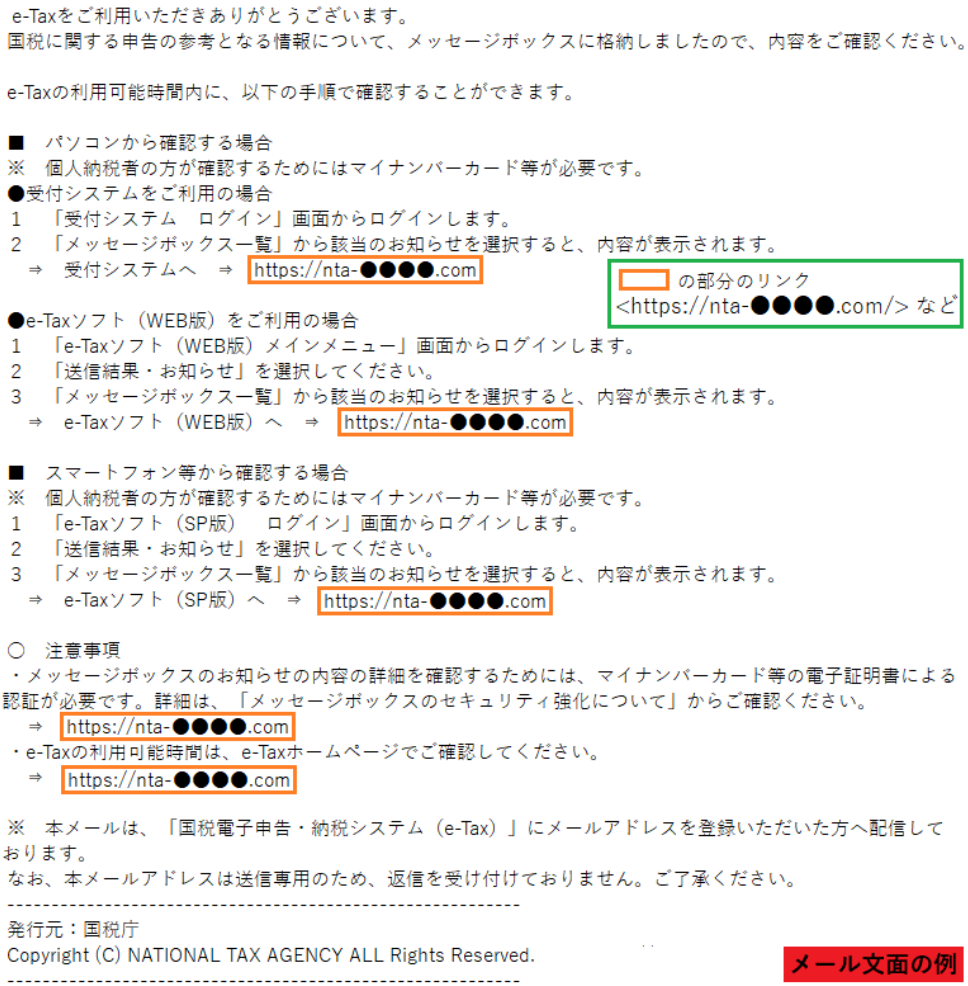
【国税庁】最終通知

【国税庁】差押最終通知

＜未払い税金のお知らせ＞

NV TRUST カー ドお取引のご確認 番号:M****

【メール文面（例）】


e-Taxをご利用いただきありがとうございます。
国税に関する申告の参考となる情報について、メッセージボックスに格納しましたので、内容をご確認ください。

e-Taxの利用可能時間内に、以下の手順で確認することができます。

■　パソコンから確認する場合
※　個人納税者の方が確認するためにはマイナンバーカード等が必要です。
●受付システムをご利用の場合
1　「受付システム　ログイン」画面からログインします。
2　「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
　⇒　受付システムへ　⇒　https://nta-●●●●.com

□ の部分のリンク
<https://nta-●●●●.com/> など

●e-Taxソフト（WEB版）をご利用の場合
1　「e-Taxソフト（WEB版）メインメニュー」画面からログインします。
2　「送信結果・お知らせ」を選択してください。
3　「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
　⇒　e-Taxソフト（WEB版）へ　⇒　https://nta-●●●●.com

■　スマートフォン等から確認する場合
※　個人納税者の方が確認するためにはマイナンバーカード等が必要です。
1　「e-Taxソフト（SP版）　ログイン」画面からログインします。
2　「送信結果・お知らせ」を選択してください。
3　「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
　⇒　e-Taxソフト（SP版）へ　⇒　https://nta-●●●●.com

○　注意事項
・メッセージボックスのお知らせの内容の詳細を確認するためには、マイナンバーカード等の電子証明書による認証が必要です。詳細は、「メッセージボックスのセキュリティ強化について」からご確認ください。
　⇒　https://nta-●●●●.com
・e-Taxの利用可能時間は、e-Taxホームページでご確認してください。
　⇒　https://nta-●●●●.com

※　本メールは、「国税電子申告・納税システム（e-Tax）」にメールアドレスを登録いただいた方へ配信しております。
なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁
Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.

メール文面の例

図 15 国税庁のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/nta_20220920.html

3.3.4　日本赤十字社のなりすましメール

【メール件名（例）】

【COVID-19】コロナ対策、慈善寄付

【メール文面（例）】

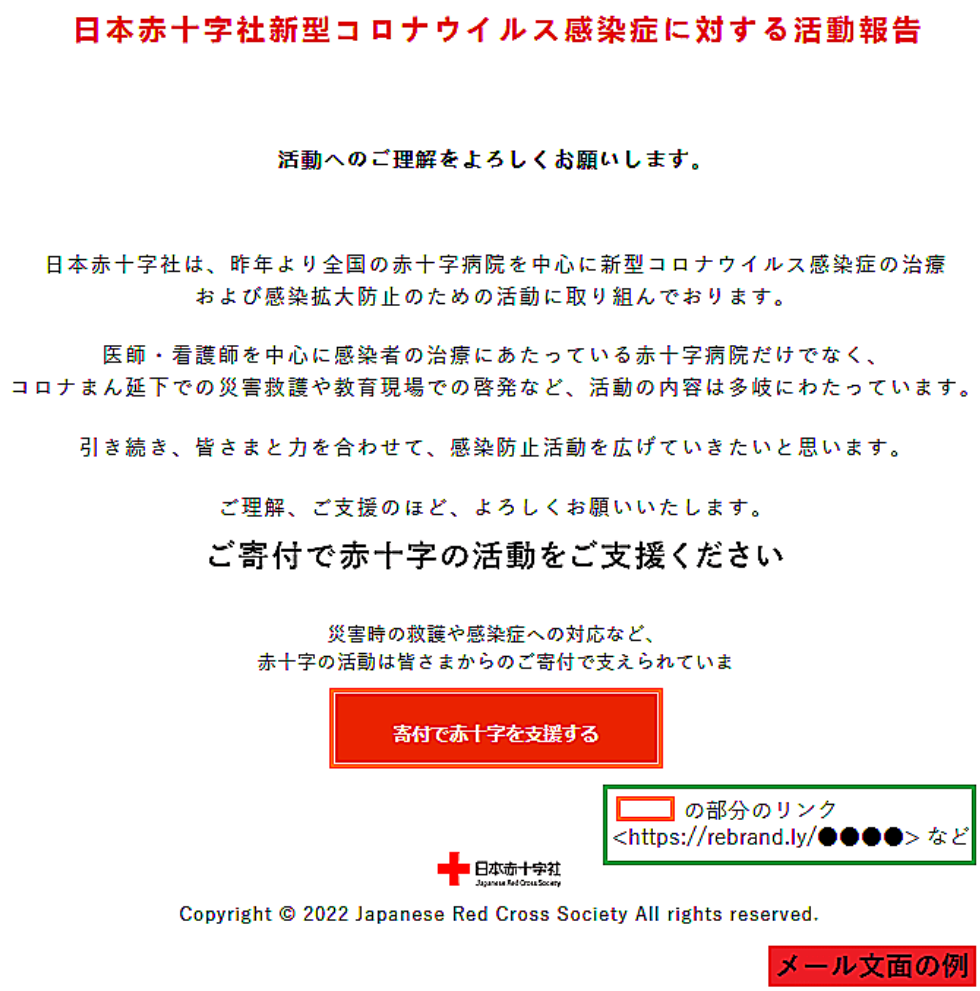


図 16 日本赤十字のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/jrc_20220920.html

3.3.5 経済産業省 エネルギー庁のなりすましメール

【メール件名（例）】

[経済産業省・電力需給対策] お客様の電力使用情報が不正確なので要確認 <電力需給ひっ迫警報・注意報>

【メール文面（例）】

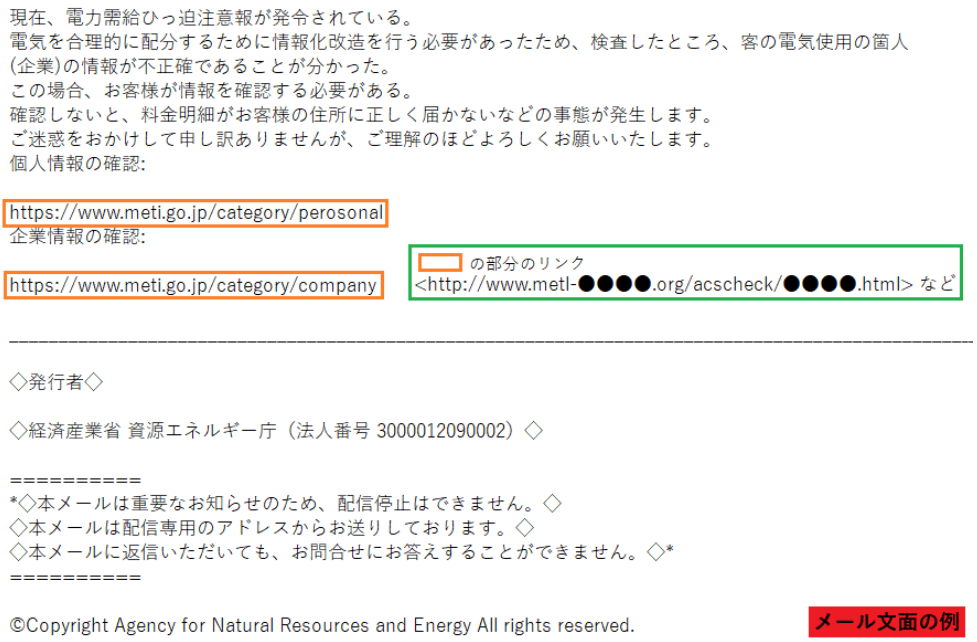


図 17 経済産業省 エネルギー庁のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/meti_20220809.html

3.3.6 東京電力のなりすましメール

【メール件名（例）】

【東京電力エナジーパートナー】カード情報更新のお知らせ

【メール文面（例）】

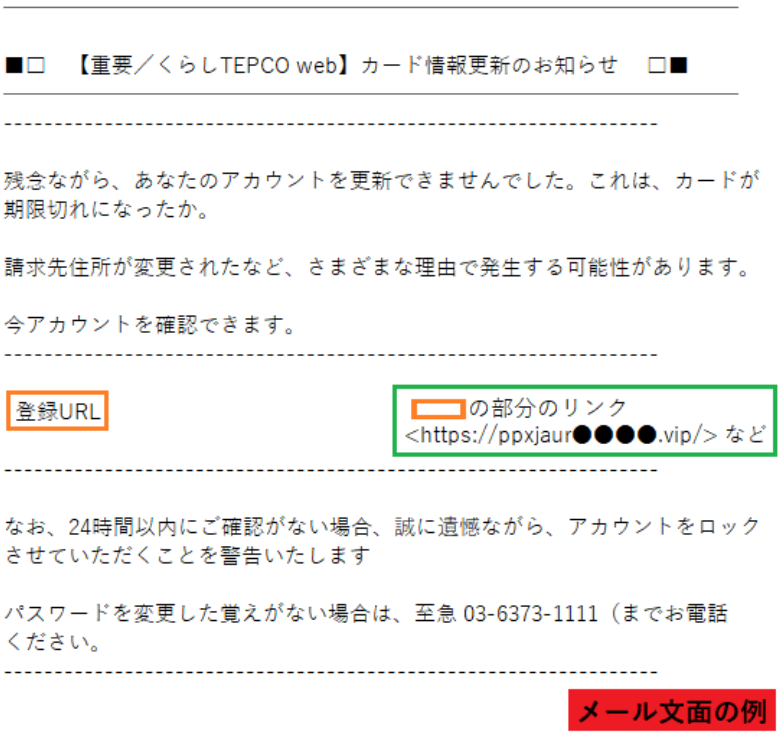


図 18 東京電力のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/tepco_20220602.html

3.3.7 NHK のなりすましメール

【メール件名（例）】

【NHK】ご利用手続きメール

【NHK】アップグレード通知

【メール文面（例）】

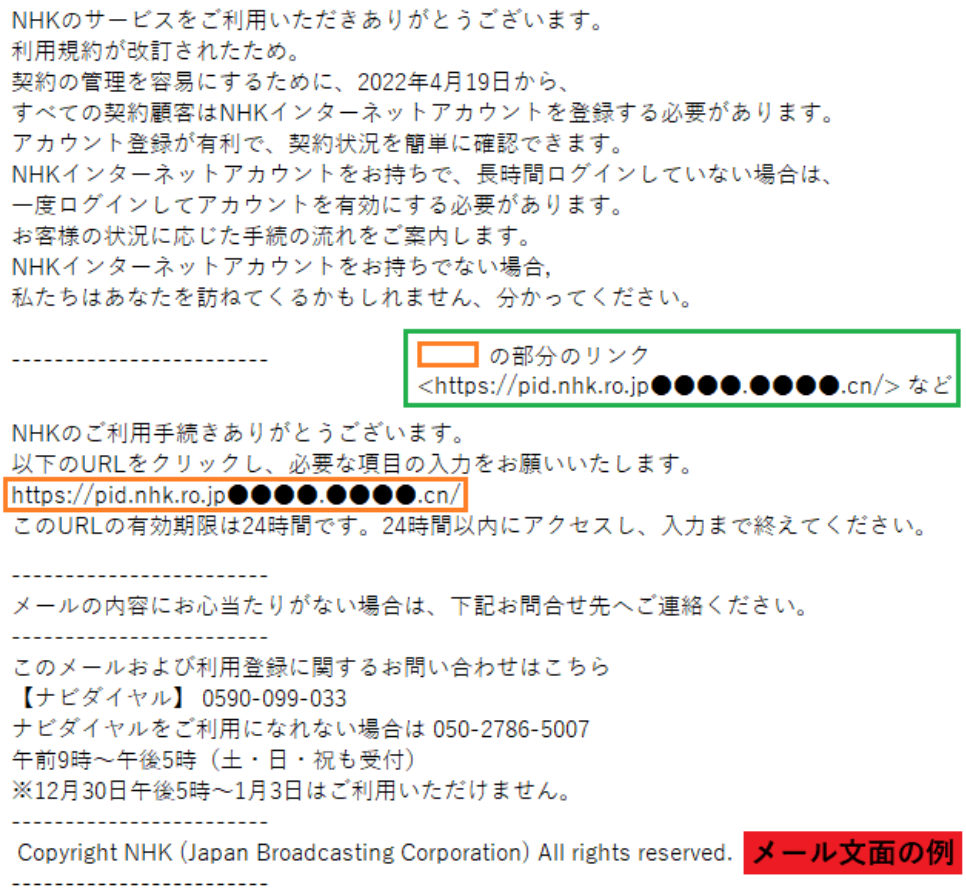


図 19 NHK のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/nhk_20220419.html

3.3.8 日本年金機構（ねんきんネット）のなりすましメール

【メール件名（例）】

国民年金（基礎年金)アカウント停止通知

【メール文面（例）】

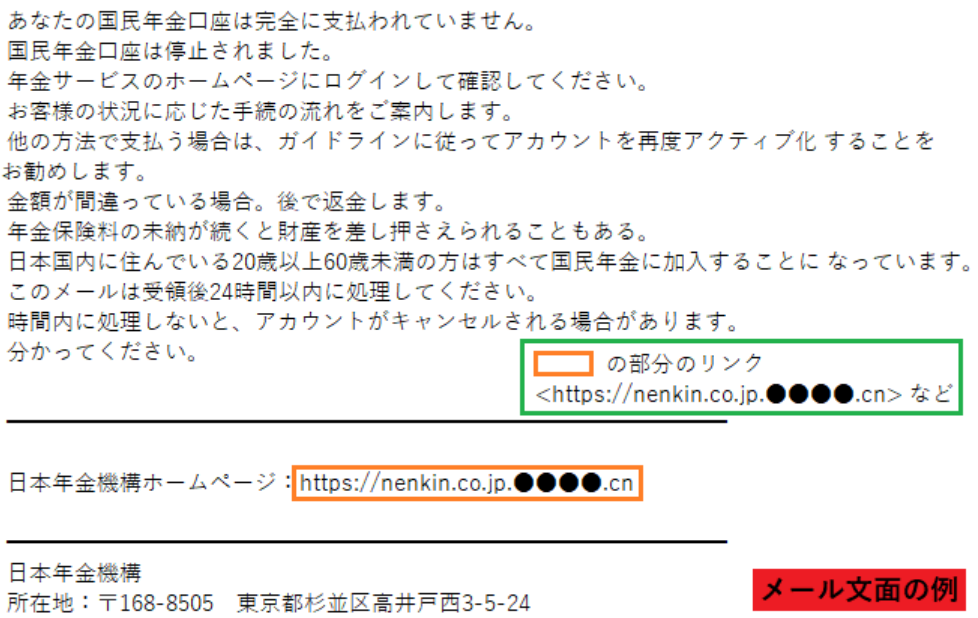


図 20 日本年金機構のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/nenkin_20220418.html

3.3.9 厚生労働省（コロナワクチンナビ）のなりすましメール

【メール件名（例）】

【重要】自衛隊 大規模接種センターの概要　予約サイト案内（予約・受付案内）

新冠ワクチン接種のお知らせ

【メール文面（例）】

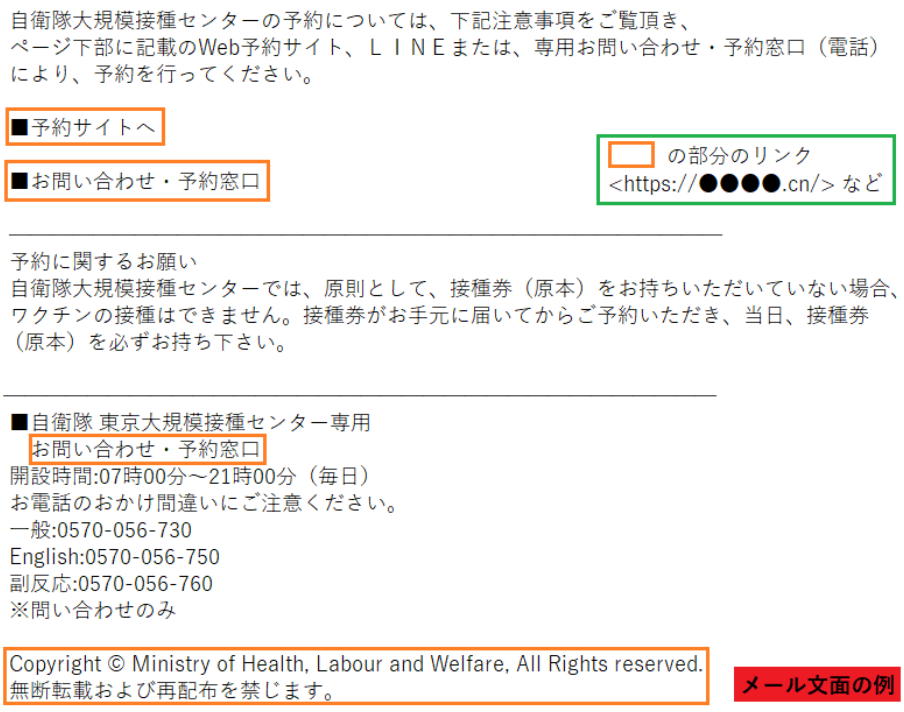


図 21 厚生労働省のなりすましメール文面例

【詳細な情報】https://www.antiphishing.jp/news/alert/mhlw_20220413.html

3.4　パスワードリセットのなりすましメール

【メール件名（例）】

【au ID】パスワードリセット

【メール文面例】

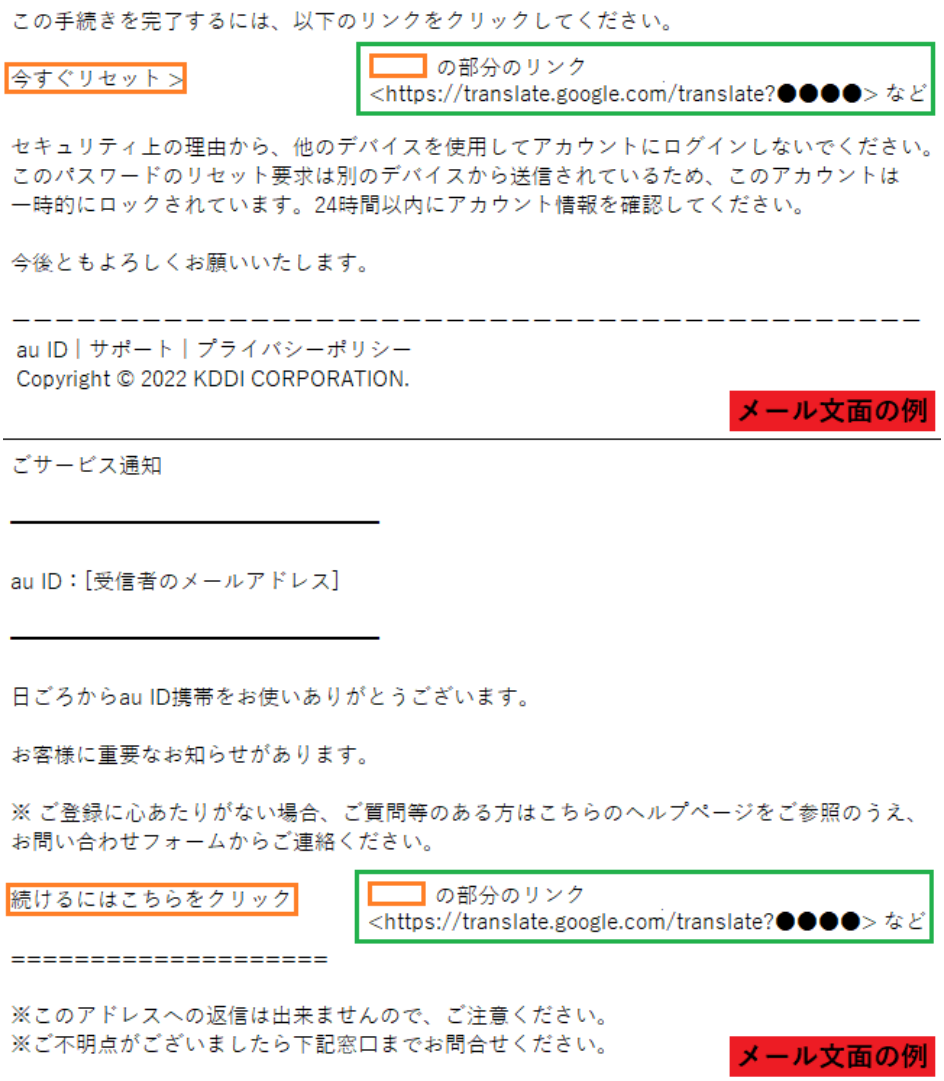


図 22 パスワードリセットのなりすましメール文面例

3.5　クレジットカードや決済サービスを装ったなりすましメール

【メール件名（例）】

・お支払い金額のお知らせ

・【重要】緊急の連絡

・必ずお読みください

・本人確認のお知らせ

・事務局からのお知らせ

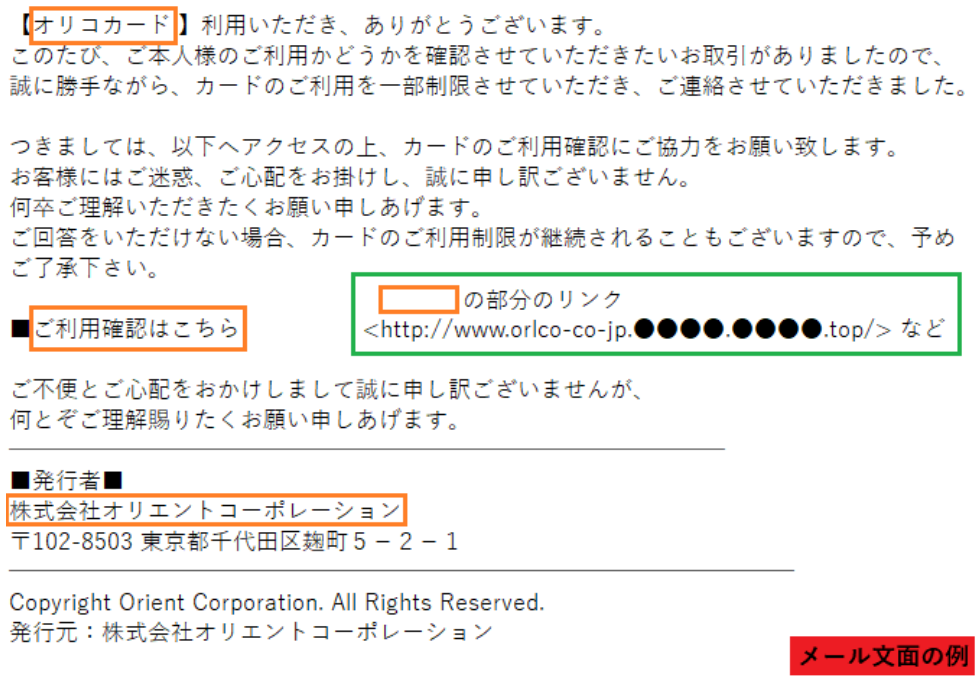
・ワンタイム URL のお知らせ

・お支払方法変更のご案内

（2022 年になりすましを確認した企業）

PayPay カード、ORICO カード、ビューカード、楽天カード、MyJCB、九州カード、FamiPay、LINE Pay

【メール文面例】


【オリコカード】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、
誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

の部分のリンク
<http://www.orlco-co-jp.●●●●.●●●●.top/> など

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

■発行者■
株式会社オリエントコーポレーション
〒102-8503 東京都千代田区麹町５－２－１

Copyright Orient Corporation. All Rights Reserved.
発行元：株式会社オリエントコーポレーション

メール文面の例

図 23 クレジットカード会社のなりすましメール文面例

3.6　銀行を装ったなりすましメール

【メール件名（例）】

お客様情報に関するご協力のお願い

【緊急】○○銀行が不正利用を検知

【重要】○○銀行入金制限のお知らせ

【重要】○○銀行本人確認のお知らせ

【○○銀行】アカウント異常活動の通知！通知番号：XXXXXXXXXXX」

【重要・緊急】○○銀行入金制限確認のお知らせ

重要：○○銀行入金制限のお知らせ

【メール本文（例）】

図 24 銀行のなりすましメール文面例

（2022 年になりすましを確認した企業）

ゆうちょ銀行、ソニー銀行、新生銀行、スルガ銀行、りそな銀行、PayPay 銀行、住信 SBI ネット銀行、千葉銀行

3.7　配達通知を装ったなりすましメール

【メール件名（例）】

お荷物お届けのお知らせ

会員情報の更新に関するお知らせ

【メール本文（例）】

図 25 宅配便会社のなりすましメール文面例

（2022 年になりすましを確認した企業）

ヤマト運輸、日本郵便

3.8　旅行関係サービスを装ったなりすましメール

【メール件名（例）】

○○○にシステムを更新する

「○○○」アカウントの自動退会処理について

「○○○e チケットサービス」○○○アカウントの自動退会処理について。メール番号:

●●●●

【重要なお知らせ】○○○アカウントの本人確認のお知らせ、情報を更新してください。

全国旅行支援、20000 円旅行期間限定受け取り。

【メール本文（例）】

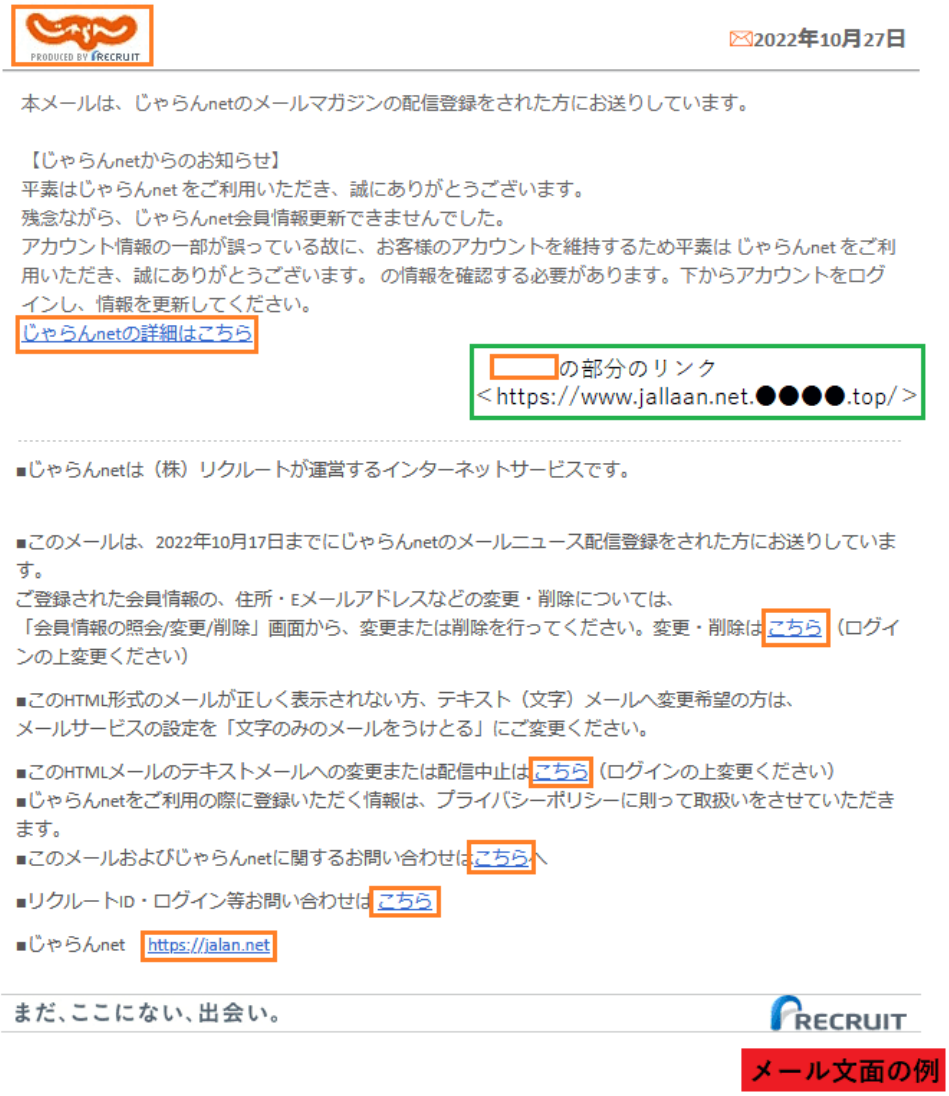


図 26 旅行関係サービスのなりすましメール文面例

（なりすましを確認した企業）

JR 東日本、JR 西日本、えきねっと、じゃらん

3.9　クラウドサービスを装ったなりすましメール（電子契約サービスなど）

【メール件名（例）】

【重要】Evernote アカウントの自動退会処理について。

【メール本文（例）】

「Evernote」日頃よりをご利用いただきありがとうございます

「Evernote」は 2022 年 5 月30 日にサービスをリニューアルいたしました。これ に伴い、「Evernote」利用規約・会員規約を変更し、最後にログインをした日より起算し て 2 年以上「Evernote」のご利用（ログイン）が確認できない「Evernote」アカウント は、自動的に退会処理させていただくことといたしました。なお、対象アカウントの自動退 会処理を、本規約に基づき、2022 年 6 月 25 日より順次、実施させていただきます。

2 年以上ログインしていないお客さまで、今後も「Evernote」をご利用いただける場合 は、2022 年 6 月 25 日よりも前に、一度ログイン操作をお願いいたします。

◆Evernote 【ログインはこちら】
https://evernote.com.●●●●.com/

□ の部分のリンク
<https://evernote.com.●●●●.com/> など

Tokyo, Japan
Evernote K.K.
c/o WeWork
Tokyo Square Garden 14F
3-1-1, Kyobashi, Chuo-ku
Tokyo, 104-0031
Japan

メール文面の例

図 27 クラウドサーのなりすましメール文面例ビス

3.10 インターネットプロパイダーを装ったなりすましメール

【メール件名（例）】

【さくらのクラウド】クレジットカードご確認のお願い [年/月/日 時刻]

・ご利用額確定のお知らせ

・ご請求のご案内

・クレジットカードご確認のお願い

【メール本文（例）】

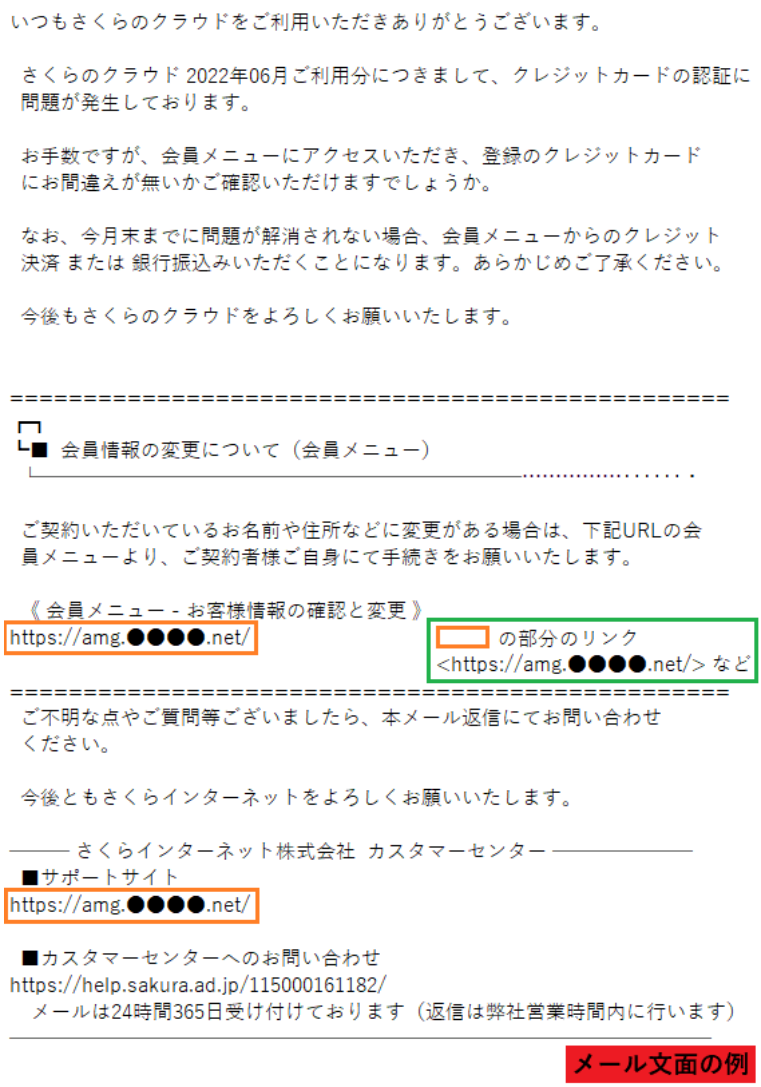


図 28 インターネットプロバイダーのなりすましメール文面例

（なりすましを確認した企業）

BIGLOBE、OCN、さくらインターネット、So-net、@nifty

3.11 ビジネスメール詐欺（BEC）

ビジネスメール詐欺（Business Email Compromise：BEC）とは、巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して攻撃者の用意した口座へ送金させる詐欺の手口です。米国連邦捜査局（Federal Bureau of Investigation：FBI）や米国インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）が公開している情報等によると、年々その被害は増加傾向にあり、ビジネスメール詐欺の脅威がより深刻なものになっています。

3.11.1 ビジネスメール詐欺の事例

社長になりすましてグループ企業役員に金銭の支払を要求した事例

A 社の社長になりすました攻撃者から、B 社の役員に対するメールが送られてきた。メールには M&A 案件の対応依頼で早急にメールを返信して欲しいという内容が記載されていた。メールの差出人には、A 社社長の氏名と、メールアドレスが記載され、メール本文の署名欄には、A 社社長の氏名が記載されていた。

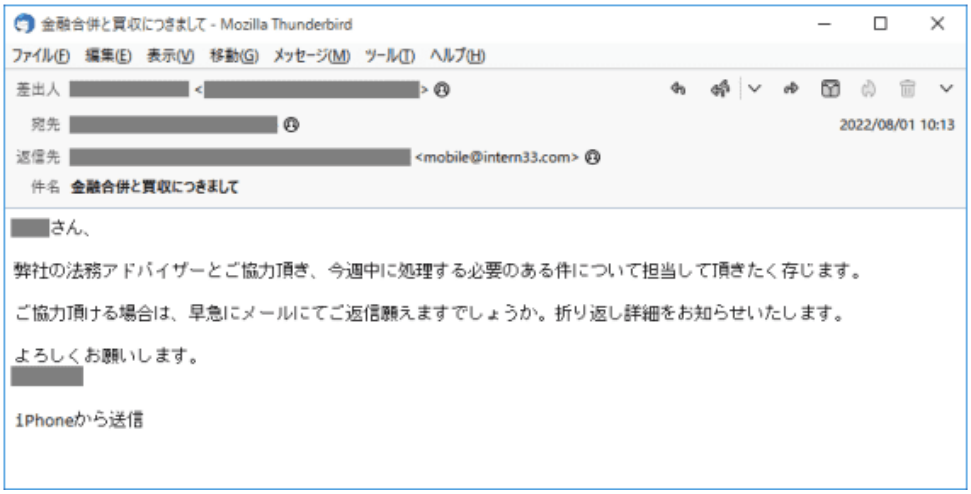


図 29 ビジネスメール詐欺のメール文面例

（出典）独立行政法人情報処理推進機構（IPA）「ビジネスメール詐欺（BEC）対策」

4　なりすましメールに反応してしまったらどのような被害に遭うのか？

もし、なりすましメールの手口に引っ掛かってしまった場合には、どういう被害があるのか知っておく必要があります。実在するサービスや企業を騙り、偽のメールや SMS（携帯電話のショートメッセージ）で偽サイト（フィッシングサイト）に誘導し、ID やパスワード、クレジットカード番号などの情報を盗んだり、マルウェアに感染させたりします。情報を盗まれることで、アカウントを乗っ取られて金銭を奪われたり、インターネット通信販売サイトで勝手に買い物をされたりします。また、マルウェアに感染してしまうと、スマートフォンに登録された電話帳の情報が盗まれたり自分のスマートフォンがフィッシングＳＭＳの発信源になってしまうこともあります。

＜入力を求められる情報の例＞

- クレジットカード番号、金融機関の口座番号、暗証番号
- 住所、氏名、電話番号、生年月日
- 電子メール、インターネットバンキング、SNS アカウント等の ID・パスワード
- 運転免許証、マイナンバーカードの画像情報　など

＜偽メッセージの例＞

- あなたのアカウントに不正アクセスがありました。至急以下のサイトからアクセスしてログインしてください。ログインしないとあなたのアカウントは安全のため失効します。
- ○○に関する申告の参考となる情報について、メッセージボックスに格納しましたので、内容をご確認ください。
- お客さまのアカウントは○○サービスを更新できませんでした。カードが期限切れになった可能性があります。

図 30 実在する金融機関、通信事業者等のログイン画面や支払いページを模した偽画面の例

（出典）警察庁

普段からログインを促すようなメールや SMS を受信した際は、正規のアプリやブックマークした正規の URL からサービスへログインして情報を確認し、クレジットカード情報や携帯電話番号、

認証コード、口座情報、ワンタイムパスワード等の入力を要求された場合は、入力する前に一度立ち止まり、本当に必要な手続きなのか、その入力先サイトが本物かを確認してください。特に初めて利用するサイトの場合は、運営者情報や問い合わせ先などを確認し、似たようなフィッシングや詐欺事例等がないか、確認するようにしてください。

5　なりすましメールの対策方法

5.1　S/MIME

電子メールセキュリティの標準規格である「S/MIME（Secure / Multipurpose Internet Mail Extensions：エスマイム）」[6]は、インターネット技術の国際標準を議論策定している IETF（The Internet Engineering Task Force：インターネット技術特別調査委員会）によって、1998 年に最初の規格は策定された。S/MIME は、電子メールの公開鍵方式による暗号化とデジタル署名が行える仕組みです。

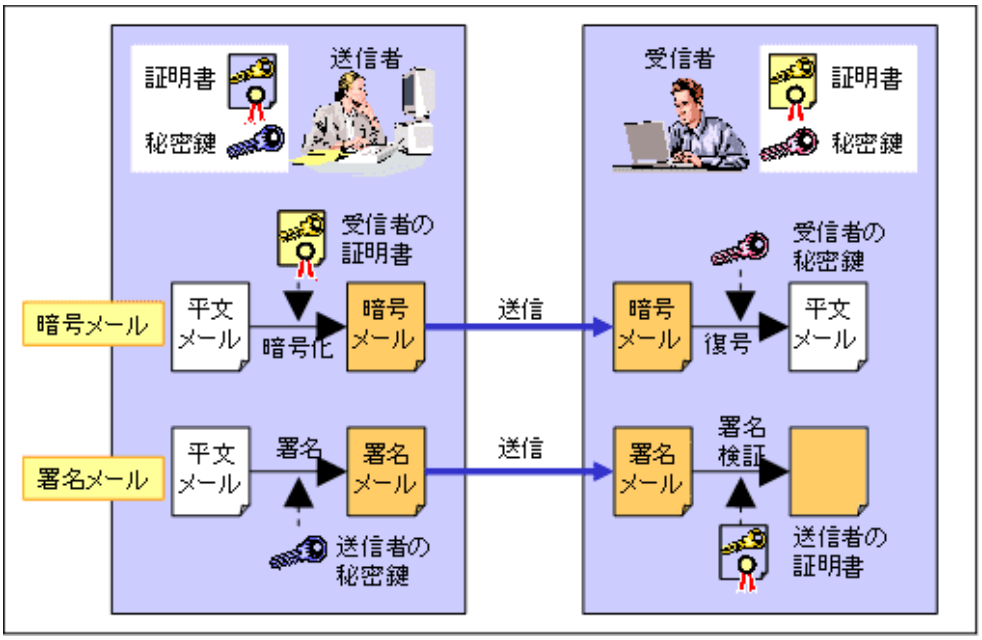


図 31 S/MIME の利用イメージ

（出典）独立行政法人情報処理推進機構（IPA）

S/MIME は、メールセキュリティ規格で、Microsoft Outlook、Mozilla Thunderbird、Gmail や iPhone 標準アプリなどの電子メールソフトに、電子証明書による暗号化技術を使い、メール送信者のなりすまし防止などが行える。

---

6 電子証明書を用いた電子メールのなりすまし対策技術の一つ。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。送信内容を秘匿する暗号化をすることもできる。

メーラー名	OS	メーラーのバージョン/ Webブラウザのバージョン	S/MIME電子署名		S/MIME暗号化	
			受信(検証)	送信	受信(復号)	送信
Outlook（アプリ）	Windows10 Pro	2008	○	○	○	○
Outlook（Webブラウザ）	Windows10 Pro	（edgeのバージョン:91.0.864.59）	○	○	○	○
Outlook（アプリ）	iOS 14.6	4.2124.0	○	○	○	○
Outlook（アプリ）	Android 11	4.2123.2	○	○	○	○
Thunderbird（アプリ）	Windows10 Pro	78.11.0	○	○	○	○
Gmail（Webブラウザ）無料版	Windows10 Pro	（Chromeバージョン:91.0.4472.114） （Firefoxのバージョン:89.0.2）	○	×	×	×
Gmail（アプリ）無料版	iOS 14.6	6.0.210530	○	×	×	×
Gmail（アプリ）無料版	Android 11	2021.05.16.380255809	○	×	×	×
Yahoo!メール（アプリ）	Android 11	4.11.2	×	×	×	×
Yahoo!メール（アプリ）	iOS 14.6	8.6.0	×	×	×	×
Yahoo!メール（Webブラウザ）	Windows10 Pro	（Firefoxのバージョン：89.0.2）	×	×	×	×
iPhone標準メール（アプリ）	iOS 14.6	―	○	○	○	○
		対応数	9	6	6	6
		対応割合	75.0%	50.0%	50.0%	50.0%

図 32 S/MIME のメーラー対応状況

（出典）一般財団法人日本情報経済社会推進協会（JIPDEC）「S/MIME のメーラー対応状況」[7]

※2021 年 9 月時点

有効な S/MIME メールを受信すると以下のように表示されます。

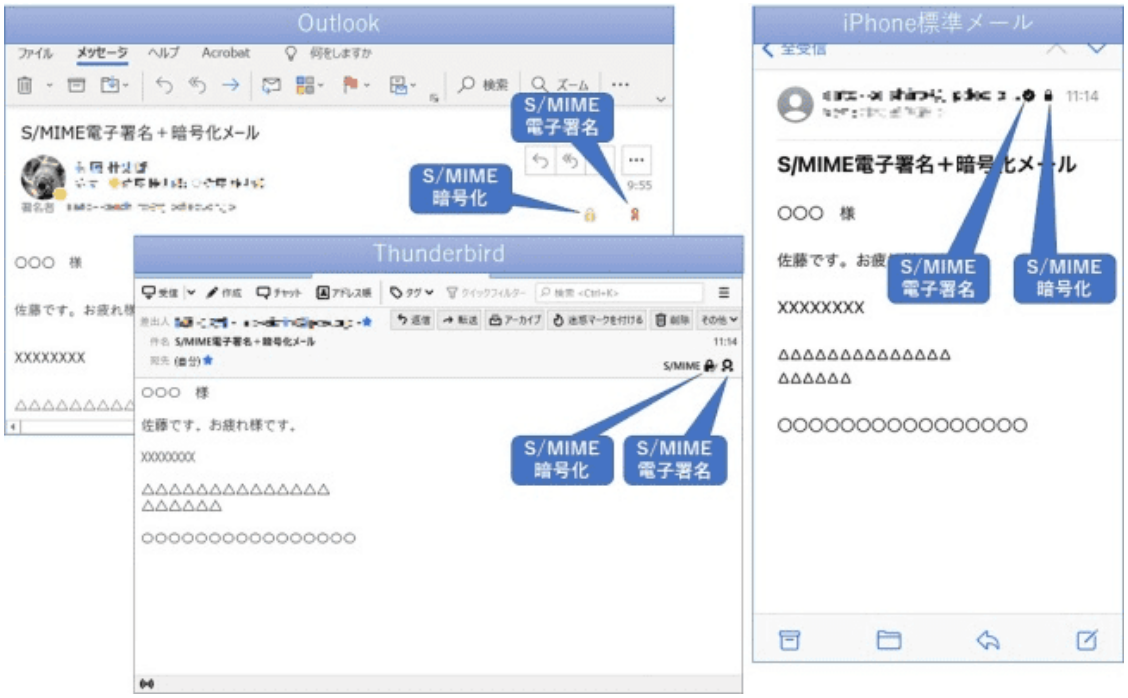


図 33 S/MIME の表示例

（出典）一般財団法人日本情報経済社会推進協会（JIPDEC）

S/MIME メールは S/MIME 対応メーラーではマークが出ますが、非対応メーラーでは添付ファイルが付いているように見えるだけです。無害化ソフトの中には、この添付ファイルを有

7 https://www.jipdec.or.jp/news/pressrelease/2021/20210928.html

害扱いして、無害化するケースもあるようです。

	S/MIME対応メーラー（表示例）			S/MIME 非対応メーラー
	Outlook	Thunderbird	iphone	
S/MIMEメール				添付ファイル表示（p7sファイル）
S/MIME されていないメール	表示なし	表示なし	表示なし	表示なし

図 34 S/MIME の対応有無による表示の違い例

（出典）一般財団法人日本情報経済社会推進協会（JIPDEC）

5.2 SPF

SPF（Sender Policy Framework）[8] は RFC7208 で規定されている、ネットワーク方式で電子メールのなりすましを判断することができる技術です。

具体的には、送信側で、送信者情報である電子メールアドレスのドメインの DNS 上に、当該ドメイン名を用いる電子メールアドレスが用いる送信メールサーバーの IP アドレスなどの情報と、それらに該当した場合の認証結果を記号で示したものを記述し（SPF レコード）、受信メールサーバーで、受信する電子メールの電子メールアドレスのドメインの DNS を確認し、送信メールサーバーの IP アドレスが、当該 DNS で記述された IP アドレスと一致しているかを確認

することにより、送信ドメインの認証を行う仕組みです。

8 Sender Policy Framework の略称。メール送信ドメインの認証技術の一つで、送信者のドメインの詐称を防ぎ、送信ドメインの正当性を検証することができます。

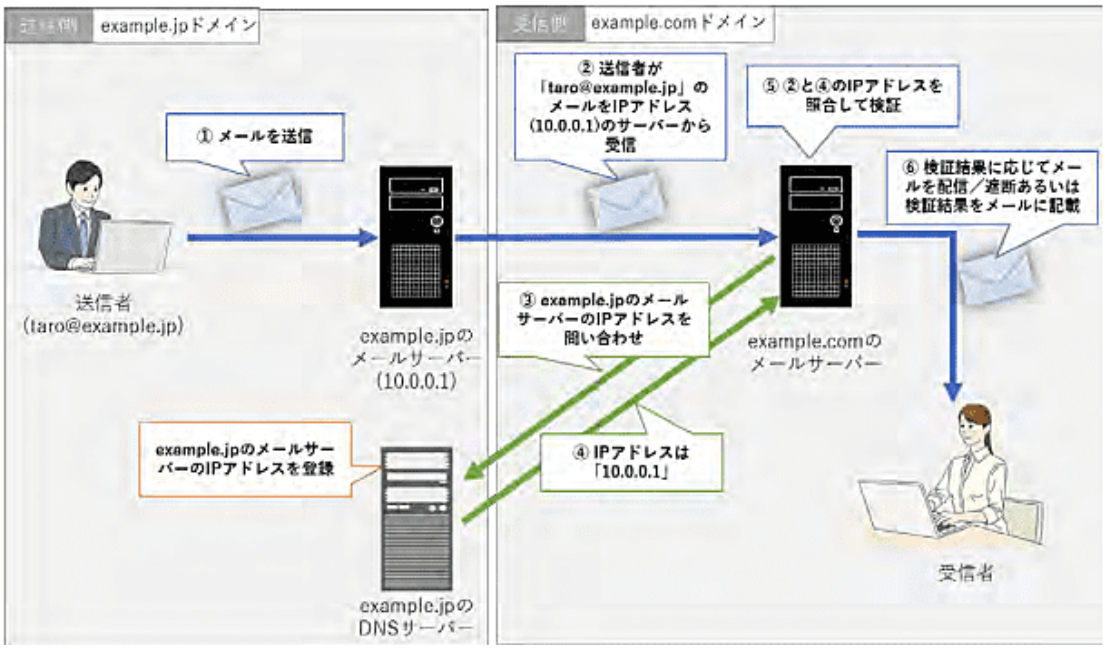


図 35 SPF の仕組み

（出典）迷惑メール白書 2021

5.3 DKIM

DKIM（Domainkeys identified Mail）[9] は STD76 で規定された、電子署名を利用して電子メールのなりすましを判断することができる技術です。

具体的には、送信メールサーバーで、電子メールの送信時に、送信メールサーバーのみが保有する秘密鍵を用いて 1 通ずつ電子署名を作成し、メールヘッダーに関連情報とともに追記して送信するとともに、送信者情報であるメールアドレスのドメインの DNS 上に公開鍵などを公開し、受信メールサーバーで、当該 DNS から入手した公開鍵を用いて電子署名を検証することにより、送信ドメインの認証を行う仕組みです。

9 Domain Keys Identified Mail の略称。電子署名を用いて送信ドメインの認証を行う仕組みです。

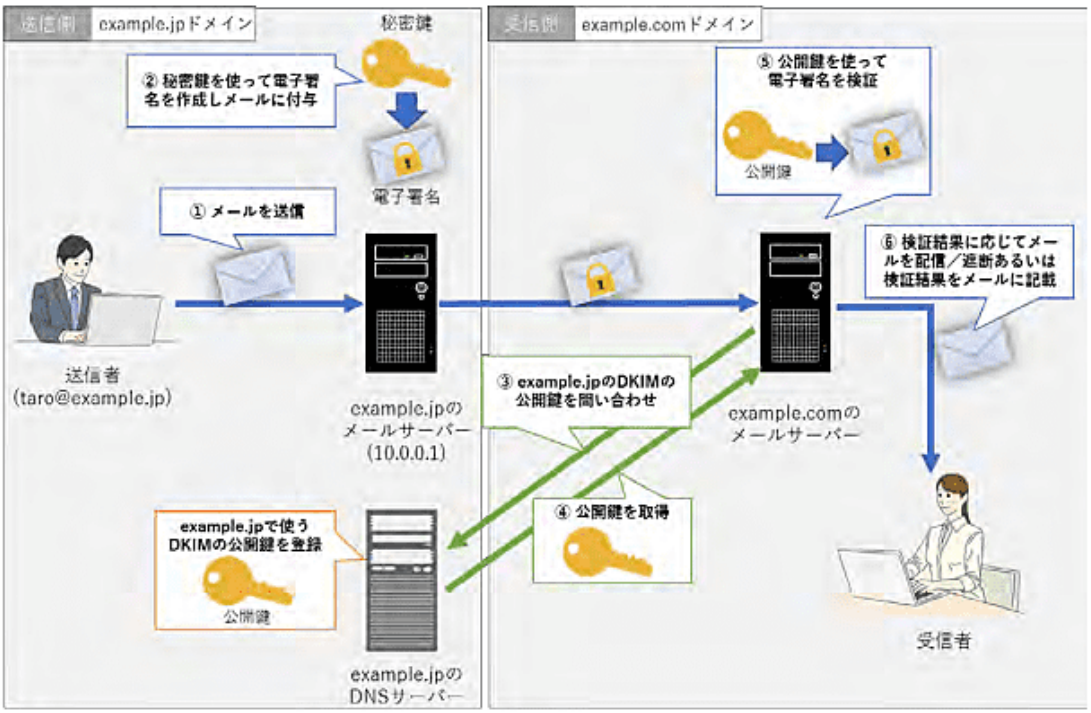


図 36 DKIM の仕組み

（出典）迷惑メール白書 2021

5.4 DMARC

DMARC（Domain-based Message Authentication, Reporting, and Conformance）は RFC7489 で規定されている技術で、大きく 3 点の特徴があります。

1 点目は、SPF の認証および DKIM の認証に成功した配送上の送信者情報（Envelope-From）と、メールヘッダー上の送信者情報（Header-From）を突き合わせて、一致している場合にはなりすましがないものと判断します。

2 点目は、送信側が、認証に失敗したメールの処理方法を決めることができます。具体的には、「何もしない（none）」、「隔離する（quarantine）」、「受信拒否する（reject）」の 3 つの処理方法を、電子メールアドレスのドメインの DNS 上で指定し、受信メールサーバーではそれを参照して取り扱いを決めることができます。

3 点目は、認証結果のレポートを送信側が電子メールで受け取るレポーティング機能です。具体的には、送信者情報である電子メールアドレスのドメインの DNS 上で、レポートの送付先や送付頻度などを設定し、受信メールサーバーではそれを参照し、認証結果のレポートを送付します。

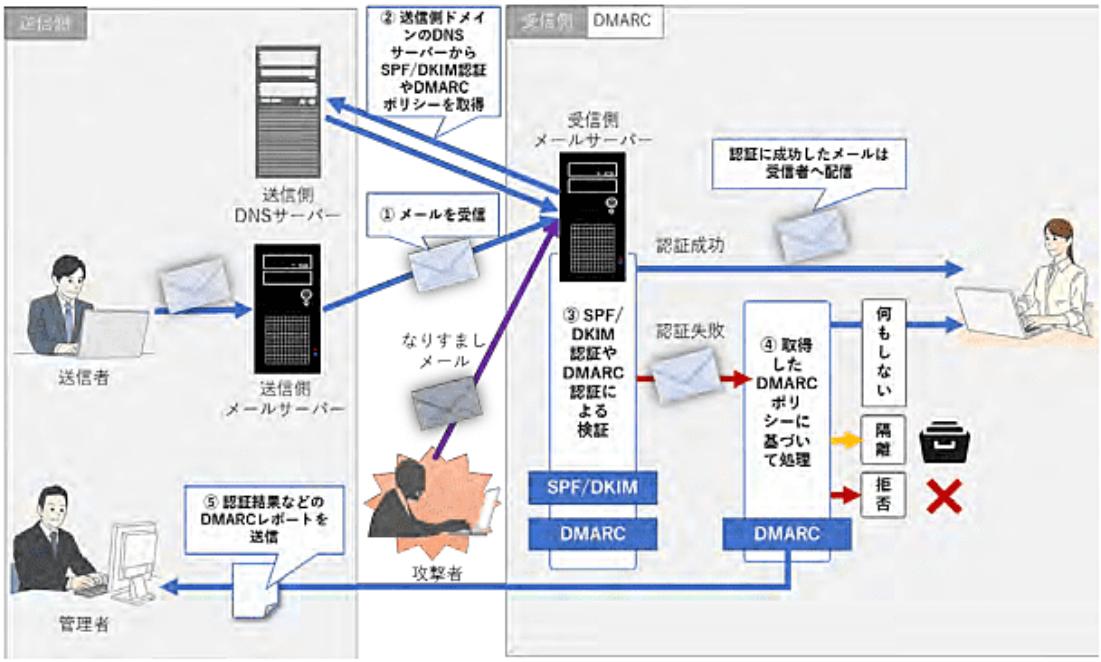


図 37 DMARC の仕組み

（出典）迷惑メール白書 2021

5.5 BIMI（認証マーク証明書/VMC）

BIMI とは、Brand Indicators for Message Identification（メッセージ識別のためのブランドインディケータ）の略で、サポートしているメールクライアントに組織のロゴを表示することで DMARC 保護の普及を促す新たな電子メールの仕様です。VMC（認証マーク証明書）は、その BIMI の仕様を満たした組織向けに発行される新しいタイプの証明書で、組織はブランドロゴを顧客の受信トレイの「送信者」フィールドの横に表示することができます。これにより、顧客メッセージを開く前にロゴを見てどの組織が送ったメールであるかを確認でき、信頼できるメールであることを視覚的に確認できます。VMC を購入する際に証明書を発行する認証局は、ロゴが正式に商標登録されている（官公庁のマークの場合は誰もが確認できる公式文書に正しく定義されている）かも含め、組織の身元と購入意思を厳格に認証します。

5.5.1 メール送信

メール送信者側がブランドロゴを受信者のメールソフトで表示するためには、BIMI 準拠が必要になり、代表的なアクションとしては DMARC の施行(p=reject)、BIMI の基準を満たしたロゴの準備、認証マーク証明書の取得、それらの DNS レコードでの公開などが必要とされます。

5.5.2 メール受信

メール受信側で BIMI に対応したメーラーで組織のロゴが表示されますが、メーラーごとに対

応が必要です。2023 年 8 月現在、Apple、Google が対応を行い PC やタブレット、スマートフォンのメーラーでロゴが表示されるようになっています。

スマートフォン Gmail アプリの例

受信メールの一覧が BIMI 対応なしの場合、送信者のイニシャルなどで表示されるため送信者が誰であるかといった特徴が見つけられませんが、DMARC を設定の上、BIMI 規格に準じたメールは組織のロゴが表示されます。

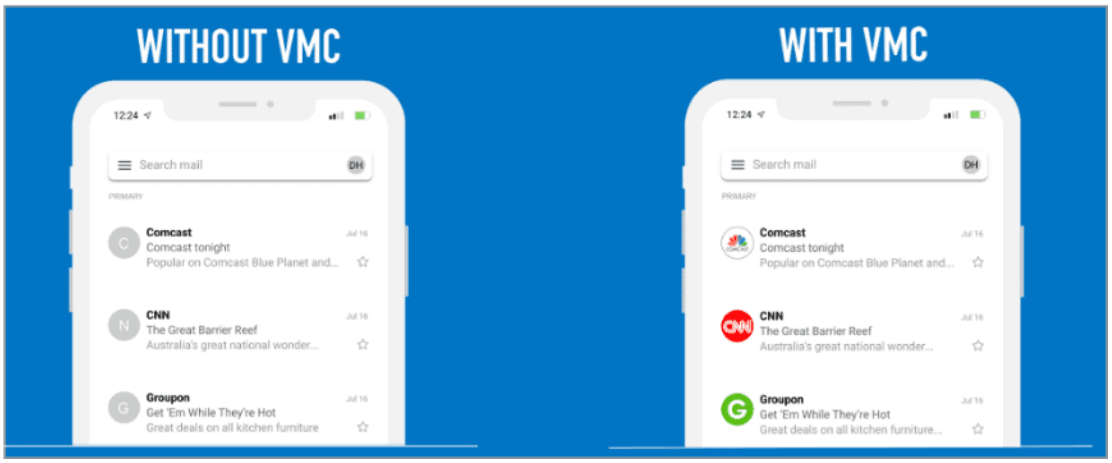


図 38 スマートフォン Gmail アプリの表示例

ブラウザー経由の Gmail の例

受信したメールを開くとスマートフォンアプリの場合同様組織のロゴが表示されます。さらに送信者の名前の横に青いチェックマークが表示され、それをクリックした際にどの組織から送られたのか認証情報も受信者に開示されます。

図 39 ブラウザー経由の Gmail の表示例

6 Appendix

6.1 ドメイン統制の概要

インターネットでサービスを提供するためには、ユーザーが当該サービスを特定してアクセスを可能とするための固有のドメイン名（アドレス）が必要となります。一度サービスを開始すると、そのドメイン名（アドレス）は Web 記事・新聞雑誌記事・メールアドレス・ブックマーク・Web アーカイブ・検索エンジンのデータベースなどさまざまなメディアに記録され、次のアクセスに役立てられます。記録されたドメイン名（アドレス）の寿命は、登録されたドメイン名の寿命とは無関係であり、かつ、記録の更新は保証されないため、ドメイン名の登録者が変わりサービスやコンテンツが変わっても、それが記録に反映されるとは限りません。ユーザーが次のアクセスをするのは、サービスやコンテンツが第三者のものに変わってからかもしれません。例えば悪意ある第三者が当該ドメイン名を新たに登録してフィッシングサイトを運営するなどをした場合、ブランド価値や信用の毀損、利用者に対する被害を招く恐れがあり、大きなリスクとなります。

特に企業において登録・利用するドメイン名においては、自社のブランドとして大切に管理するため、ドメイン名管理のためのルール・手順を社内で確立することが重要です。具体的には、ドメイン名の管理を行う部門・担当者を定めておく、ドメイン名の廃止の注意事項に留意するなどが考えられます。ここではドメイン名の廃止の注意事項について解説いたします。

6.2 ドメイン名の廃止の注意事項

利用を終えたドメイン名を廃止する際は慎重な検討が必要です。最も有効な対策は、一度登録・利用したドメイン名は、その後も登録を継続し続けることです。止むを得ず利用終了後にドメイン名を廃止する際は、すぐに廃止するのではなく、他の参照されているサイトでの対応や利用者の対応を考慮し、数年間は確保した後に廃止するなどの対策が考えられます。

なお、廃止したドメイン名と同じ文字列が第三者によって登録された場合、当事者同士の話し合いや訴訟を通じて、ドメイン名を取り戻す（=「ドメイン名の移転」を行う）ことは、多額の費用や時間がかかってしまう可能性が高いこと、また、確実に取り戻せる保証はない点に留意が必要です。

トラブルを避けるためにも、「ドメイン名の管理=ブランドの管理」という認識のもと、十分な検討・対策・準備をすることが大切です。

【参考情報】

https://jprs.jp/registration/suspended/presentation20230309.pdf

7　フィッシング詐欺対策に関するドキュメント

フィッシング対策協議会では、事業者向けならびに利用者向けフィッシング対策ガイドライン、フィッシングレポート、フィッシング報告状況をとりまとめた各種ドキュメントを公開しています。

7.1　フィッシング対策ガイドライン（事業者向け）

本ガイドラインは、フィッシング対策事項を集約し、利用者が被害にあわないために行うべき対応や不幸にして被害を受けた時に行うべき対応を整理しています。

https://www.antiphishing.jp/report/guideline/

7.2　利用者向けフィッシング詐欺対策ガイドライン

本ガイドラインは、フィッシング対策の心得や今すぐにできるフィッシング対策方法について整理しています。

https://www.antiphishing.jp/report/guideline/

7.3　フィッシングレポート

本レポートは、フィッシングの被害状況、フィッシングの攻撃技術・手法などをとりまとめています。

https://www.antiphishing.jp/report/wg/phishing_report2023.html

7.4　フィッシング報告の緊急情報

一般および事業者から受け付けたフィッシング報告のうち、消費者への影響が大きいと考えられるフィッシングについて、フィッシングメールやフィッシングサイトの実例を都度公開しています。

https://www.antiphishing.jp/news/alert/

7.5　フィッシング報告状況

毎月、前月分のフィッシングに関する報告件数、フィッシングサイト URL 件数、悪用されたブランド数をグラフにまとめています。また、それらをもとにした総評、事業者の皆さまや、一般利用者の皆さまへの注意喚起を掲載しています。

https://www.antiphishing.jp/report/monthly/

8　まとめ

本ドキュメントで解説したように、フィッシング詐欺における、なりすましメールにはさまざまな手口が存在する。利用者はこれらの手口が存在することを理解し、実在する企業・組織からのメールであるのか、または詐欺メールであるのかを見極め、フィッシング詐欺被害に遭わないように気を付けていただきたい。そして事業者は、利用者が安全にサービスを利用できるように「なりすましメールの対策方法」で解説した対策方法を多層的に実装し、自社が実施している対策について利用者に周知することも必要ではないかと考えている。フィッシング詐欺の手口は今後も変化することが予想されるため、フィッシング対策協議会が発信する最新の情報を参考に対策されることを推奨する。

フィッシング対策協議会　証明書普及促進ワーキンググループ

構成メンバー

（敬称略・順不同）

【主査】

田上 利博　　サイバートラスト株式会社

【副主査】

稲葉　厚志　　GMO グローバルサイン株式会社

【構成員】

市原 創　　キヤノン IT ソリューションズ株式会社

大久保 智史　　デジサート・ジャパン合同会社

林 正人　　デジサート・ジャパン合同会社

加藤 孝浩　　TOPPAN エッジ株式会社

町田 隼人　　株式会社日本レジストリサービス

米谷 嘉朗　　株式会社日本レジストリサービス ※

中津 圭輔　　HENNGE 株式会社

福田 誠　　HENNGE 株式会社

稲森 伸介　　株式会社ラック

関 海斗　　株式会社ラック

又江原 恭彦　　株式会社ラック

大泰司 章　　一般財団法人日本情報経済社会推進協会（JIPDEC）

高倉 万記子　　一般財団法人日本情報経済社会推進協会（JIPDEC）

【事務局】

一般社団法人 JPCERT コーディネーションセンター

※ 2023 年 9 月まで