

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	4
2	なりすましメールの手口	4
2.1	類似ドメイン	5
2.1.1	類似ドメインとは？	5
2.2	ディスプレイネーム	6
2.2.1	ディスプレイネームとは？	6
2.3	踏み台	7
2.3.1	踏み台とは？	7
3	なりすましメールの事例	8
3.1	ECサイトを装ったなりすましメール	8
3.1.1	Amazon のなりすましメール	9
3.1.2	三越伊勢丹のなりすましメール	9
3.1.3	出前館のなりすましメール	10
3.1.4	ZOZOTOWN のなりすましメール	11
3.1.5	Uber Eats のなりすましメール	12
3.2	ECサイトで商品を購入した際のなりすましメール	14
3.3	官公庁や公共サービスを装ったなりすましメール	14
3.3.1	警察庁のなりすましメール	14
3.3.2	金融庁のなりすましメール	15
3.3.3	国税庁のなりすましメール	15
3.3.4	日本赤十字社のなりすましメール	16
3.3.5	経済産業省 エネルギー庁のなりすましメール	17
3.3.6	東京電力のなりすましメール	18
3.3.7	NHK のなりすましメール	19
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	19
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	20
3.4	パスワードリセットのなりすましメール	21
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	21
3.6	銀行を装ったなりすましメール	22
3.7	配達通知を装ったなりすましメール	23
3.8	旅行関係サービスを装ったなりすましメール	24
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）	25

3.10	インターネットプロバイダーを装ったなりすましメール	25
3.11	ビジネスメール詐欺（BEC）	26
3.11.1	ビジネスメール詐欺の事例	27
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？	27
5	なりすましメールの対策方法	29
5.1	S/MIME	29
5.2	SPF	31
5.3	DKIM	32
5.4	DMARC	33
5.5	BIMI（認証マーク証明書/VMC）	34
5.5.1	メール送信	34
5.5.2	メール受信	34
6	Appendix	36
6.1	ドメイン統制の概要	36
6.2	ドメイン名の廃止の注意事項	36
7	フィッシング詐欺対策に関するドキュメント	37
7.1	フィッシング対策ガイドライン（事業者向け）	37
7.2	利用者向けフィッシング詐欺対策ガイドライン	37
7.3	フィッシングレポート	37
7.4	フィッシング報告の緊急情報	37
7.5	フィッシング報告状況	37
8	まとめ	38

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ると視覚的に似たドメイン名をホモグラフィドメインと呼ぶ。

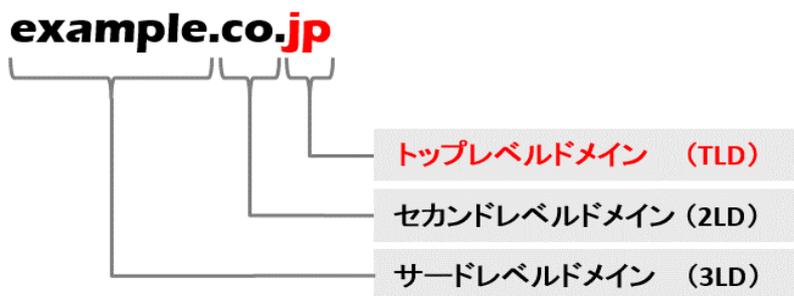


図 1 TLD（出典：株式会社日本レジストリサービス）

【類似ドメインによるなりすましの例】

- ・ Am^azon.com（ホモグラフィドメインを利用）
- ・ 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。

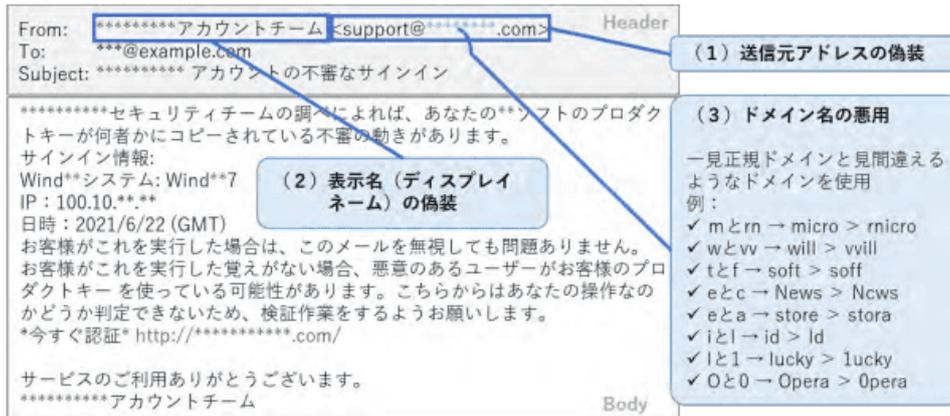


図 2 送信元の偽装 (出典: 迷惑メール白書 2021)

■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 @ compn <u>a</u> y-□ . com	一文字入れ替える
	② alice @ compan <u>y</u> s-□ . com	一文字追加
	aalice @ company-□ . com	
	③ alice @ comp <u>;</u> ny-□ . com	一文字削除
	④ alice @ co <u>m</u> pany-□ . 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

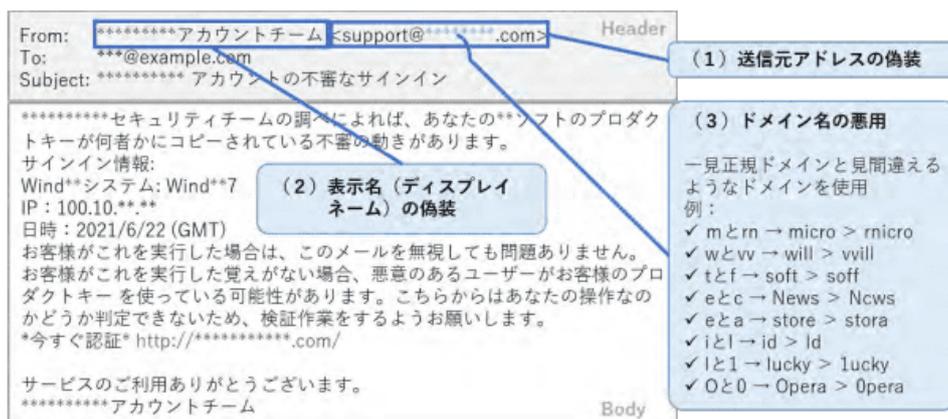


図 4 送信元の偽装 (出典 : 迷惑メール白書 2021)

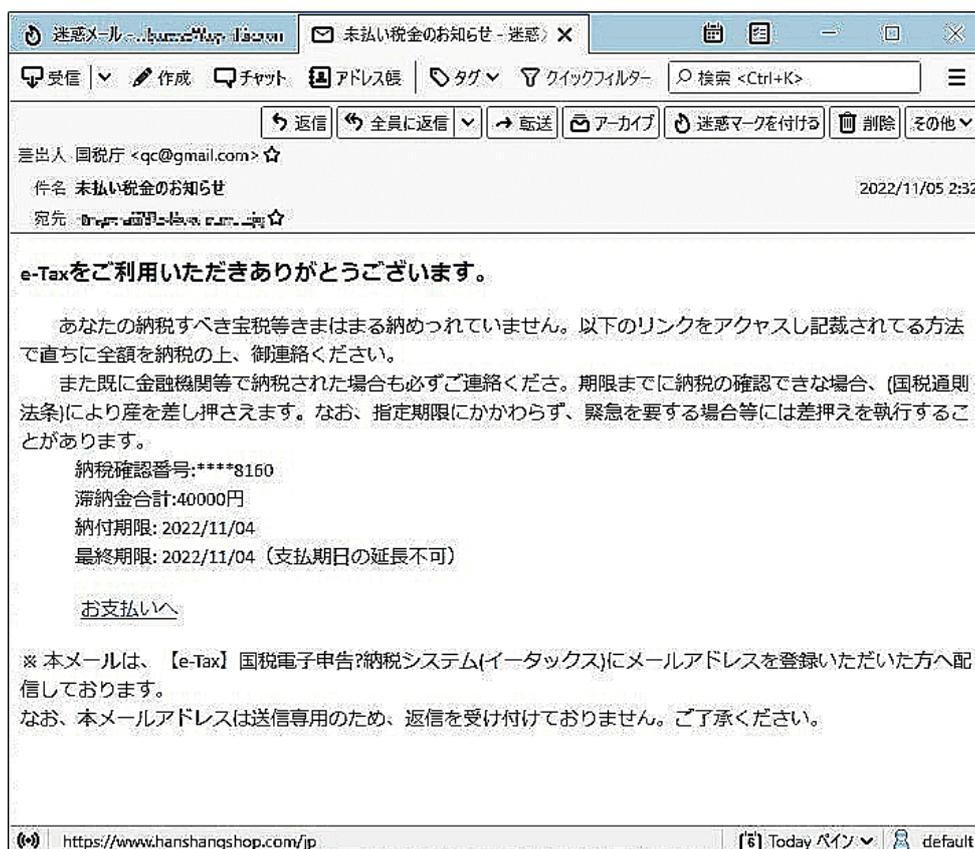


図 5 国税庁をかたる例 (出典 : インプレス「INTERNET Watch」)

【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

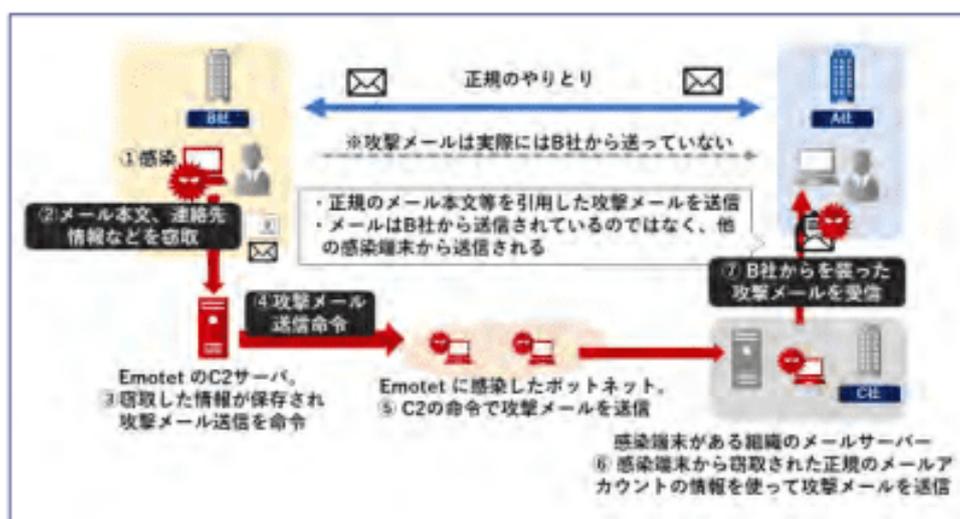


図 6 Emotet のなりすましメール送信イメージ (出典：迷惑メール白書 2021)

【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）】

お支払方法に問題があり、プライム特典をご利用いただけない状況です。

[支払方法を更新する](#)

の部分のリンク
<http://www.amazon-●●●●.biz/>など

Amazon利用いただきありがとうございます。

ご指定いただいたお客様のお支払い方法が承認されないため、。Amazonは無料ですが、ご登録の際には適用可能なお支払い方法を確認させていただきます。これは、ご登録時にご同意いただいたように。

1日以内に、アマゾンからの請求へのお支払いが確認できない限り、お客様のAmazon登録はキャンセルされ他の有効な支払方法を更新・追加し、Amazonをご利用されたい場合は、以下の手順に従って更新してください。Webページが乗っ取られないようにするためにご本人認証下記携帯電話でQRコードをスキャンする確認ください



>>>>

の部分のリンク
<https://zjg●●●●/jp/>など

1. お客様のお支払い方法にアクセス
2. Amazon登録したAmazon.co.jpのアカウントを使用してサインイン
登録済みのお支払手段の有効期限を更新、または新しく支払い手段を追加し、「続行」ボタンをクリック現在ご指定のお支払い方法が承認されない原因は、提携会社(クレジットカード会社等)の事情により異なりますが、利用可能限度額の超過、有効期限切れ、カード利用不可などが考えられます。大変お手数ですが詳細についてはサービスの提供元会社に直接お問い合わせください。

Amazon.co.jpをご利用いただき、ありがとうございます。
今後ともAmazon.co.jpをよろしく願いたします。

Amazon.co.jpカスタマーサービス

メール文面の例

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）】

●●●● 様

「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。
カード番号情報をご確認ください。

<https://www.misto●●●●-co-jp.top/>

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

※本メールは配信専用メールアドレスから配信しております。
ご返信いただいても対応いたしかねますので、予めご了承ください。
※本メールは重要なお知らせのため、メール配信停止設定をされているお客さまにも配信しております。

三越伊勢丹オンラインストア
<http://www.mistore.jp/>

株式会社 三越伊勢丹

メール文面の例

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）】

Demaecan

日頃より「出前館」をご利用いただきありがとうございます。

「出前館」は2022年3月20日(日)にサービスをリニューアルいたしました。これに伴い、「出前館」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1年以上「出前館」のご利用(ログイン)が確認できない「出前館」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3月20日(月)より順次、実施させていただきます。

2か月以上ログインしていないお客さまで、今後も「出前館」をご利用いただける場合は、よりも前に、一度ログイン操作をお願いいたします。

⇒ログインはこちら

<https://demaecan.com/login/>

の部分のリンク
<<https://demaecan-club.com/>> など

※出前館トップページ右上のログインボタンよりログインしてください。

なお、アカウントが退会処理された場合も、新たにアカウント登録(無料登録)していただくことで「出前館」をご利用いただくことができますので、今後もご愛顧いただけますようお願いいたします。

株式会社出前館

東京本社：〒151-0051 東京都渋谷区千駄ヶ谷5丁目27番5号 リンクスクエア新宿(総合受付11階)

大阪支社：〒530-0018 大阪府大阪市北区小松原町2番4号 大阪富国生命ビル27階



© Demae-can Co., Ltd.

メール文面の例

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)】

【ZOZOTOWN】会員情報変更のお知らせ

平素よりZOZOTOWNをご利用いただきありがとうございます。

ZOZOTOWNカスタマーサポートセンター
アカウントが別の場所にログインしていることを検知
ご本人様の利用確認のため
誠に勝手ながら、全ての機能を一時停止させていただきます。
突然、ご連絡を差し上げたにもかかわらず
このようなご案内となり、大変申し訳ございません。
弊社では、セキュリティ強化のため
クレジットカード決済アカウント一部を対象に
ご本人様の利用確認をおこなう場合がございます。
アカウントの資料を一部削除させていただきましたので、
下のリンクから再度資料を設定してください。

※このメールに心当たりがない方、またはご不明な点がある方は
ZOZOTOWNカスタマーサポートセンターまでお問い合わせください。

お問い合わせ（カスタマーサポートセンター）

お問い合わせ

の部分のリンク
<https://www.zozo.jp.●●●●.cn/> など

※本件についてメールでお問い合わせいただく際は
こちらのメールを引用のうえ、ご返信をお願いいたします。

※個人情報の取扱いについては個人情報保護方針をご覧ください。

発行：ZOZO, Inc.
住所：千葉県千葉市稲毛区緑町1-15-16

COPYRIGHT(C) ZOZO, Inc. ALL RIGHTS RESERVED.

メール文面の例

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スーパ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）



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] XXXXXXXXXX
[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）



※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。

© 2022 Uber Technologies Inc.

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）】

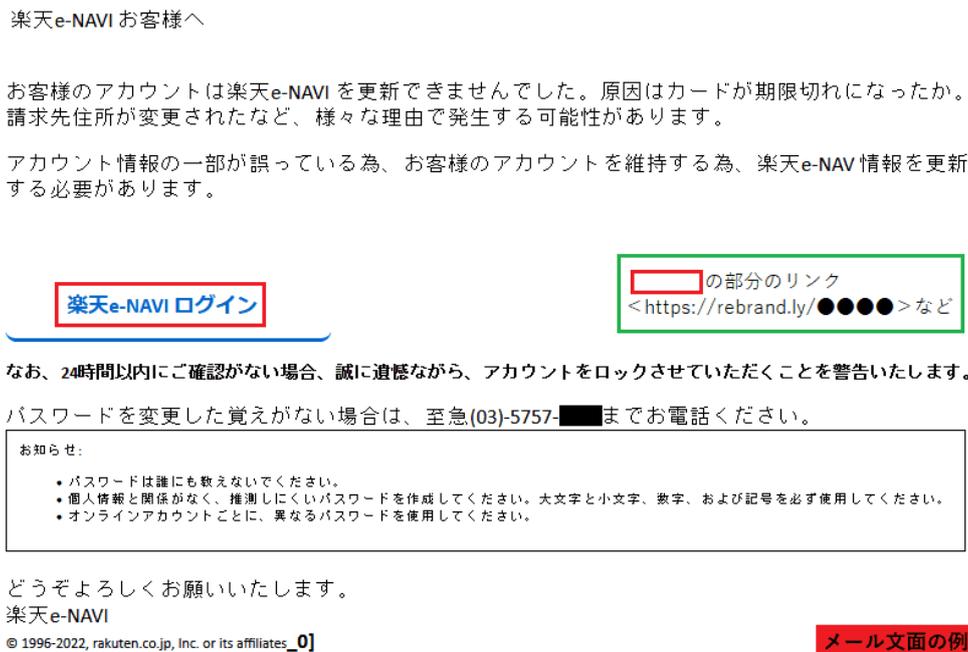


図 12 ECサイトで商品を購入した際のなりすましメール文面例

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）】

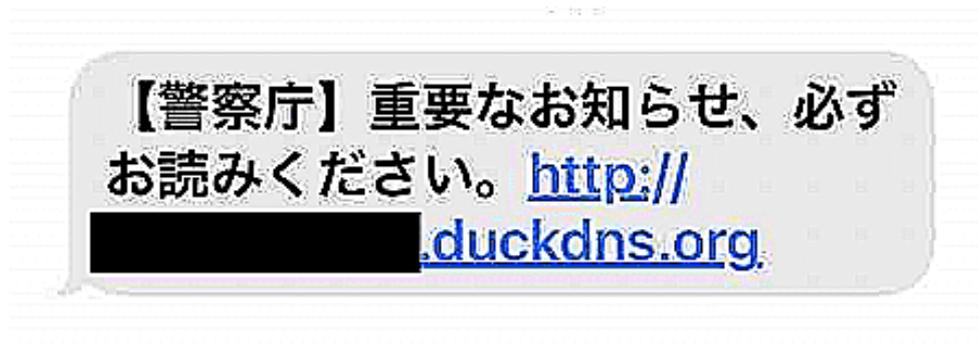


図 13 警察庁のなりすましメール文面例

【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）】

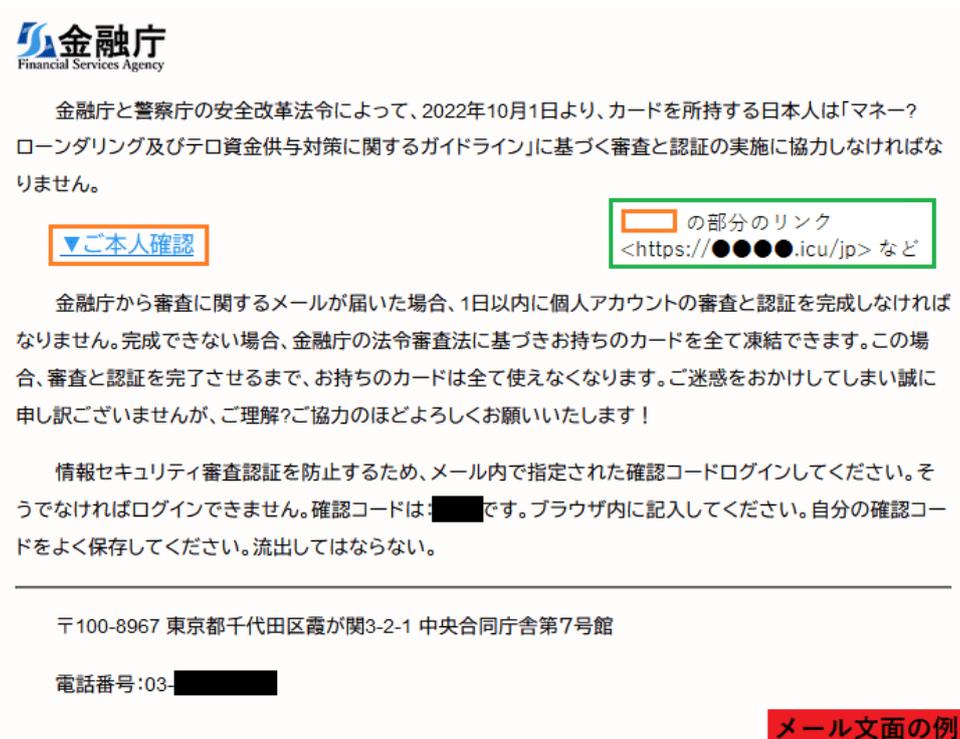


図 14 金融庁のなりすましメール文面例

【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）】

日本赤十字社新型コロナウイルス感染症に対する活動報告

活動へのご理解をよろしくお願いします。

日本赤十字社は、昨年より全国の赤十字病院を中心に新型コロナウイルス感染症の治療および感染拡大防止のための活動に取り組んでおります。

医師・看護師を中心に感染者の治療にあっている赤十字病院だけでなく、コロナまん延下での災害救護や教育現場での啓発など、活動の内容は多岐にわたっています。

引き続き、皆さまと力を合わせて、感染防止活動を広げていきたいと思っております。

ご理解、ご支援のほど、よろしくお願いいたします。

ご寄付で赤十字の活動をご支援ください

災害時の救護や感染症への対応など、赤十字の活動は皆さまからのご寄付で支えられています。

寄付で赤十字を支援する



Copyright © 2022 Japanese Red Cross Society All rights reserved.

の部分のリンク
<https://rebrand.ly/●●●●> など

メール文面の例

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）】

現在、電力需給ひっ迫注意報が発令されている。
電気を合理的に配分するために情報化改造を行う必要があったため、検査したところ、客の電気使用の箇入(企業)の情報が不正確であることが分かった。
この場合、お客様が情報を確認する必要がある。
確認しないと、料金明細がお客様の住所に正しく届かないなどの事態が発生します。
ご迷惑をおかけして申し訳ありませんが、ご理解のほどよろしく願いたします。
個人情報の確認:

<https://www.meti.go.jp/category/personal>
企業情報の確認:

<https://www.meti.go.jp/category/company>

の部分のリンク
<<http://www.meti-.....org/acscheck/.....html>> など

◇発行者◇

◇経済産業省 資源エネルギー庁 (法人番号 3000012090002) ◇

=====

*◇本メールは重要なお知らせのため、配信停止はできません。◇

◇本メールは配信専用のアドレスからお送りしております。◇

◇本メールに返信いただいても、お問合せにお答えすることができません。◇*

=====

©Copyright Agency for Natural Resources and Energy All rights reserved.

メール文面の例

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)】

■□ 【重要／くらしTEPCO web】カード情報更新のお知らせ □■

残念ながら、あなたのアカウントを更新できませんでした。これは、カードが期限切れになったか。

請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

今アカウントを確認できます。

登録URL

の部分のリンク
<<https://ppxjaur.....vip/>> など

なお、24時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただくことを警告いたします

パスワードを変更した覚えがない場合は、至急 03-6373-1111 (までお電話ください)。

メール文面の例

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/tepeco_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）】

NHKのサービスをご利用いただきありがとうございます。
利用規約が改訂されたため。
契約の管理を容易にするために、2022年4月19日から、
すべての契約顧客はNHKインターネットアカウントを登録する必要があります。
アカウント登録が有利で、契約状況を簡単に確認できます。
NHKインターネットアカウントをお持ちで、長時間ログインしていない場合は、
一度ログインしてアカウントを有効にする必要があります。
お客様の状況に応じた手順の流れをご案内します。
NHKインターネットアカウントをお持ちでない場合、
私たちはあなたを訪ねてくるかもしれません、分かってください。

の部分のリンク
<<https://pid.nhk.ro.jp●●●●●●●●●●.cn/>> など

NHKのご利用手続きありがとうございます。
以下のURLをクリックし、必要な項目の入力をお願いいたします。
<https://pid.nhk.ro.jp●●●●●●●●●●.cn/>
このURLの有効期限は24時間です。24時間以内にアクセスし、入力まで終わってください。

メールの内容にお心当たりがない場合は、下記お問合せ先へご連絡ください。

このメールおよび利用登録に関するお問い合わせはこちら
【ナビダイヤル】 0590-099-033
ナビダイヤルをご利用になれない場合は 050-2786-5007
午前9時～午後5時（土・日・祝も受付）
※12月30日午後5時～1月3日はご利用いただけません。

Copyright NHK (Japan Broadcasting Corporation) All rights reserved. **メール文面の例**

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）】

あなたの国民年金口座は完全に支払われていません。
国民年金口座は停止されました。
年金サービスのホームページにログインして確認してください。
お客様の状況に応じた手順の流れをご案内します。
他の方法で支払う場合は、ガイドラインに従ってアカウントを再度アクティブ化することをお勧めします。
金額が間違っている場合、後で返金します。
年金保険料の未納が続くと財産を差し押さえられることもある。
日本国内に住んでいる20歳以上60歳未満の方はすべて国民年金に加入することになっています。
このメールは受領後24時間以内に処理してください。
時間内に処理しないと、アカウントがキャンセルされる場合があります。
分かってください。

の部分のリンク
<https://nenkin.co.jp.●●●●.cn> など

日本年金機構ホームページ: <https://nenkin.co.jp.●●●●.cn>

日本年金機構
所在地: 〒168-8505 東京都杉並区高井戸西3-5-24

メール文面の例

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）】

自衛隊大規模接種センターの予約については、下記注意事項をご覧ください、
ページ下部に記載のWeb予約サイト、LINEまたは、専用お問い合わせ・予約窓口（電話）
により、予約を行ってください。

■予約サイトへ

■お問い合わせ・予約窓口

の部分のリンク
<https://●●●●.cn/> など

予約に関するお願い
自衛隊大規模接種センターでは、原則として、接種券（原本）をお持ちいただいていない場合、
ワクチンの接種はできません。接種券がお手元に届いてからご予約いただき、当日、接種券
（原本）を必ずお持ち下さい。

■自衛隊 東京大規模接種センター専用

お問い合わせ・予約窓口

開設時間:07時00分～21時00分（毎日）
お電話のおかけ間違いにご注意ください。
一般:0570-056-730
English:0570-056-750
副反応:0570-056-760
※問い合わせのみ

Copyright © Ministry of Health, Labour and Welfare. All Rights reserved.
無断転載および再配布を禁じます。

メール文面の例

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】

この手続きを完了するには、以下のリンクをクリックしてください。

今すぐリセット >

の部分のリンク
<<https://translate.google.com/translate?>●●●●●> など

セキュリティ上の理由から、他のデバイスを使用してアカウントにログインしないでください。このパスワードのリセット要求は別のデバイスから送信されているため、このアカウントは一時的にロックされています。24時間以内にアカウント情報を確認してください。

今後ともよろしくお願いいたします。

au ID | サポート | プライバシーポリシー
Copyright © 2022 KDDI CORPORATION.

メール文面の例

ごサービス通知

au ID : [受信者のメールアドレス]

日ごろからau ID携帯をお使いありがとうございます。

お客様に重要なお知らせがあります。

※ ご登録に心あたりがない場合、ご質問等のある方はこちらのヘルプページをご参照のうえ、お問い合わせフォームからご連絡ください。

続けるにはこちらをクリック

の部分のリンク
<<https://translate.google.com/translate?>●●●●●> など

=====

※このアドレスへの返信は出来ませんので、ご注意ください。
※ご不明点がございましたら下記窓口までお問合せください。

メール文面の例

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上げます。
 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上げます。

■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】〇〇銀行が不正利用を検知

【重要】〇〇銀行入金制限のお知らせ

【重要】〇〇銀行本人確認のお知らせ

【〇〇銀行】アカウント異常活動の通知！通知番号：XXXXXXXXXXXX

【重要・緊急】〇〇銀行入金制限確認のお知らせ

重要：〇〇銀行入金制限のお知らせ

【メール本文 (例)】

いつも新生銀行をご利用いただきありがとうございます。

当社では、犯罪収益移転防止法に基づき、お取引を行う目的等を確認させていただいております。
また、この度のご案内は、当社ご利用規約第9条2項6に基づくご依頼となります。

お客様お客様の直近の取引についていくつかのご質問がございます、下記のリンクをアクセスし、ご回答ください。

お取引確認

の部分のリンク
<https://shinnsei●●●●.life/>など

※一定期間ご確認いただけない場合、口座取引を一部制限させていただきます。
※回答が完了しますと、通常どおりログイン後の手続きが可能になります。

お客様のご返信内容を確認後、利用制限の解除を検討させていただきますので、できる限り詳細にご回答ください。

◎申し訳ございませんが電子メールでのご質問等は受け付けておりません。
メールでのご返信はご遠慮ください。
お問い合わせは新生パワーコールへお願いいたします。

株式会社新生銀行/Shinsei Bank, Limited. All Rights Reserved.

メール文面の例

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)】

【日本郵政】いつも大変お世話になっております。

重要なお荷物が届きましたが、荷物に不備があり、受取人と連絡が取れませんでした。
お客様がこの荷物の受取人であるかどうかを確認したく、ご連絡させていただきました。
そのため、下記をご覧いただき、受取情報をご確認ください。
できるだけ早く、再度の配送を手配いたします。

一確認はこちら

の部分のリンク
<https://●●●●postsecure.top/index.php> など

お客様にはご不便、ご心配をおかけして申し訳ございませんでした。
ご理解いただきますようお願いいたします。
48時間以内に確認が取れない場合、お荷物は返却されますのでご注意ください。

日本郵便輸送株式会社

Copyright(C) 2015 JAPAN POST TRANSPORT Co.,Ltd. All Rights Reserved. Powered by リクオプ

メール文面の例

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）】

〇〇〇にシステムを更新する

「〇〇〇」アカウントの自動退会処理について

「〇〇〇e チケットサービス」〇〇〇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】 〇〇〇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）】

本メールは、じゃらんnetのメールマガジンの配信登録をされた方にお送りしています。

【じゃらんnetからのお知らせ】
平素はじゃらんnetをご利用いただき、誠にありがとうございます。
残念ながら、じゃらんnet会員情報更新できませんでした。
アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため平素はじゃらんnetをご利用いただき、誠にありがとうございます。の情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。

[じゃらんnetの詳細はこちら](#)

の部分のリンク
<<https://www.jallan.net.●●●●.top/>>

■じゃらんnetは（株）リクルートが運営するインターネットサービスです。

■このメールは、2022年10月17日までにじゃらんnetのメールニュース配信登録をされた方にお送りしています。
ご登録された会員情報の、住所・Eメールアドレスなどの変更・削除については、「会員情報の照会/変更/削除」画面から、変更または削除を行ってください。変更・削除は[こちら](#)（ログインの上変更ください）

■このHTML形式のメールが正しく表示されない方、テキスト（文字）メールへ変更希望の方は、メールサービスの設定を「文字のみのメールをうけとる」にご変更ください。

■このHTMLメールのテキストメールへの変更または配信中止は[こちら](#)（ログインの上変更ください）

■じゃらんnetをご利用の際に登録いただく情報は、プライバシーポリシーに則って取扱いをさせていただきます。

■このメールおよびじゃらんnetに関するお問い合わせは[こちら](#)へ

■リクルートID・ログイン等お問い合わせは[こちら](#)

■じゃらんnet <https://jalan.net>

まだ、ここがない、出会い。

RECRUIT

メール文面の例

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）】

いつもさくらのクラウドをご利用いただきありがとうございます。

さくらのクラウド 2022年06月ご利用分につきまして、クレジットカードの認証に問題が発生しております。

お手数ですが、会員メニューにアクセスいただき、登録のクレジットカードにお間違えが無いかご確認いただけますでしょうか。

なお、今月末までに問題が解消されない場合、会員メニューからのクレジット決済または銀行振込みいただくことになります。あらかじめご了承ください。

今後もさくらのクラウドをよろしくお願いいたします。

☐ ■ 会員情報の変更について (会員メニュー)

ご契約いただいているお名前や住所などに変更がある場合は、下記URLの会員メニューより、ご契約者様ご自身にて手続きをお願いいたします。

《会員メニュー - お客様情報の確認と変更》

<https://amg.●●●●.net/>

☐ の部分のリンク
<<https://amg.●●●●.net/>> など

ご不明な点やご質問等ございましたら、本メール返信にてお問い合わせください。

今後ともさくらインターネットをよろしくお願いいたします。

—— さくらインターネット株式会社 カスタマーセンター ——

■ サポートサイト

<https://amg.●●●●.net/>

■ カスタマーセンターへのお問い合わせ

<https://help.sakura.ad.jp/115000161182/>

メールは24時間365日受け付けております (返信は弊社営業時間内に行います)

メール文面の例

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。

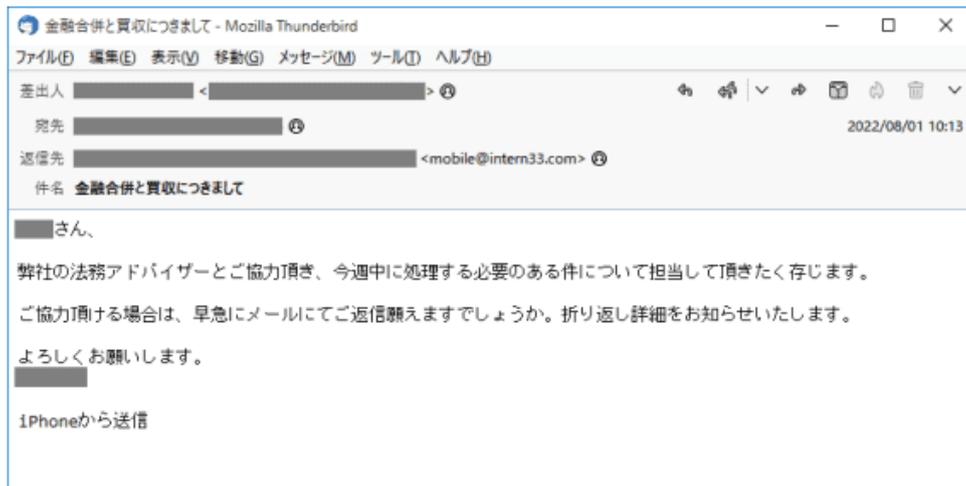


図 29 ビジネスメール詐欺のメール文面例

(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、どのような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。

ログインはこちら

会員ID

パスワード

ご利用者の生年月日 西暦 年 月 日

画像認証 画像に表示されている文字を入力してください。
クリックすると別の文字に変わります。
アルファベットの小文字と数字で5文字です。

ログイン

[> ID・パスワードをお忘れの場合はこちら](#)
[> プリペイド残高のみのご検証はこちら](#)

【重要】不正ログインを防止するために以下の点をご確認ください
1.他社サービスとは違うログインID・パスワードを設定する。
2.パスワードは定期的に変更し、過去に使用したものは極力使用しない。
3.第三者が容易に推測できるパスワードを使用しない。

お支払い方法の更新

お客様の個人情報を安全に送信するためにSSL暗号化通信を利用し、第三者によるデータの改ざんや盗用を防いでいます。

クレジットカード名義人

カード番号

有効期限:
01 2021

セキュリティコード
CVV/CVV2

生年月日
日 月 年

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。

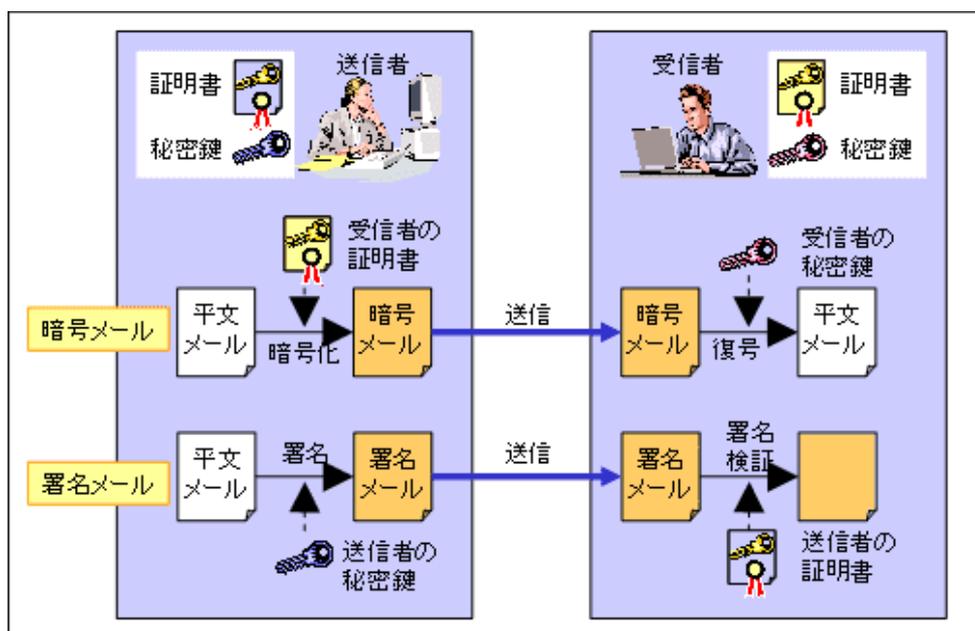


図 31 S/MIME の利用イメージ

(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。

メーカー名	OS	メーカーのバージョン/ 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のバージョン: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	2021.05.16.38025809	○	×	×	×
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 のメーカー対応状況

(出典) 一般財団法人日本情報経済社会推進協会 (JIPDEC) 「S/MIME のメーカー対応状況」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 対応メーカーではマークが出ますが、非対応メーカ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。

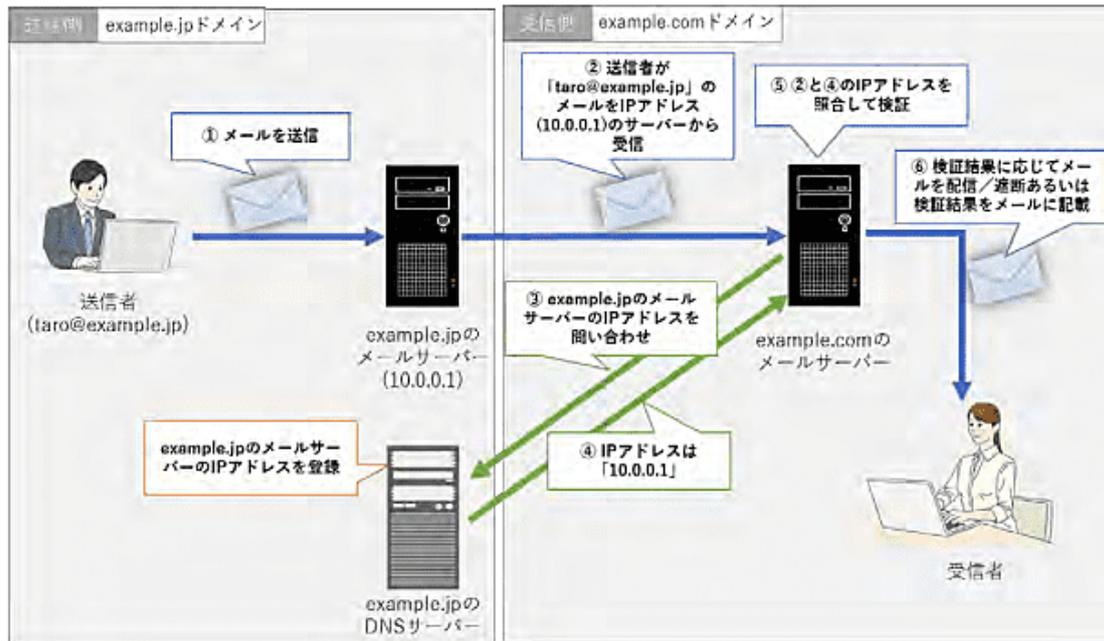


図 35 SPF の仕組み

(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。

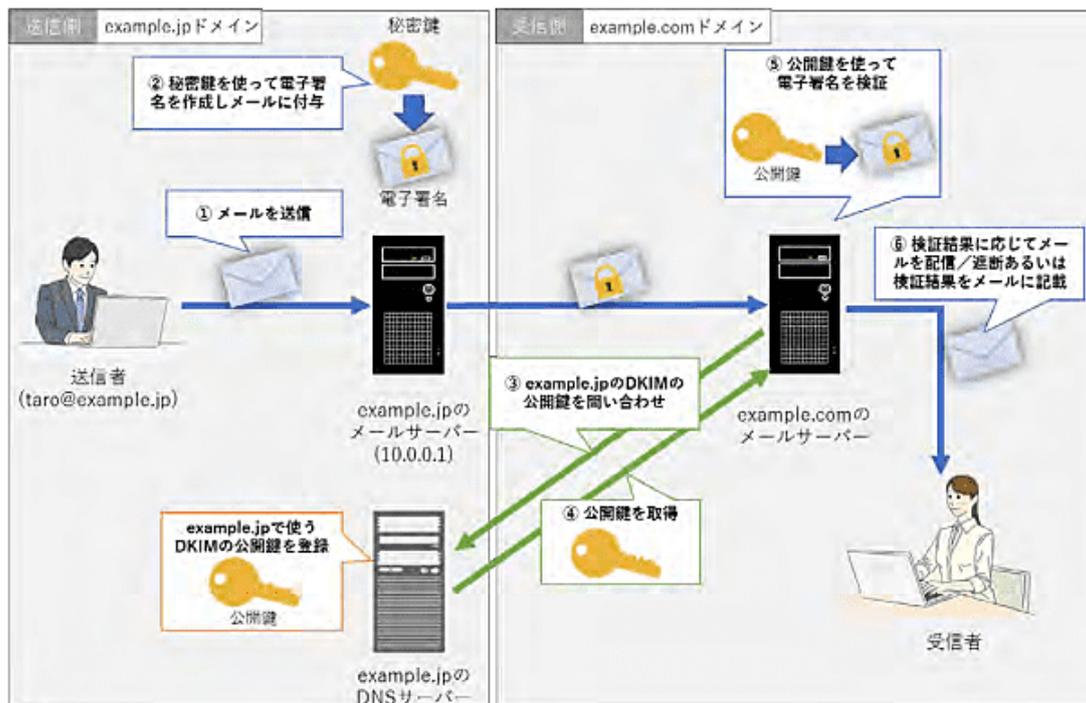


図 36 DKIM の仕組み

(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無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ト機能です。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。

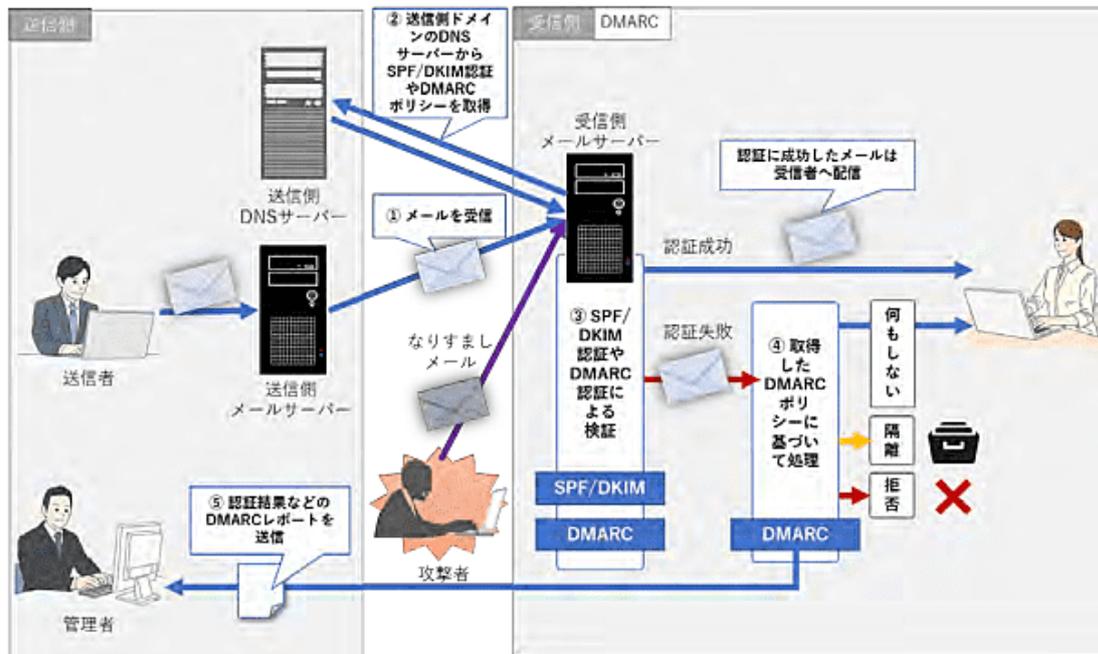


図 37 DMARC の仕組み

(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きます。

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。

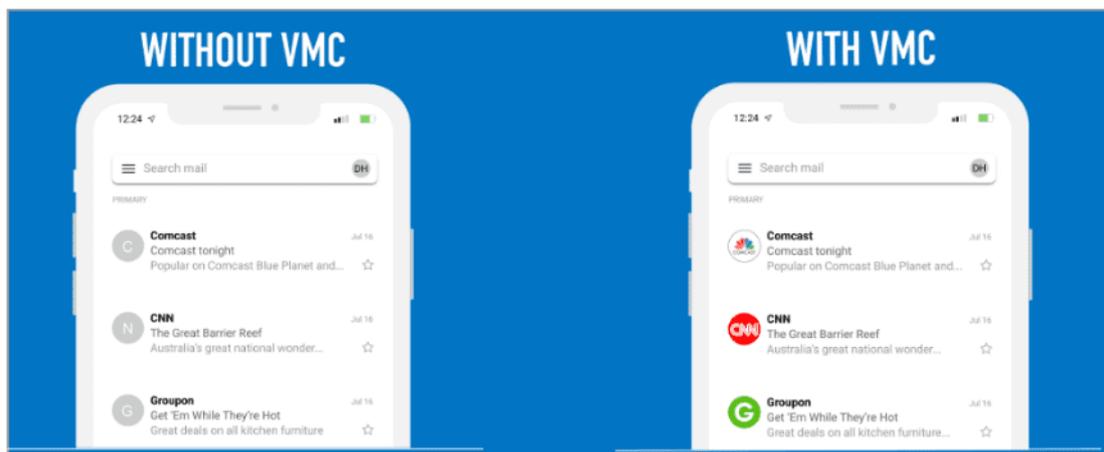


図 38 スマートフォン Gmail アプリの表示例

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取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行うことが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・手法などを取りまとめています。

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