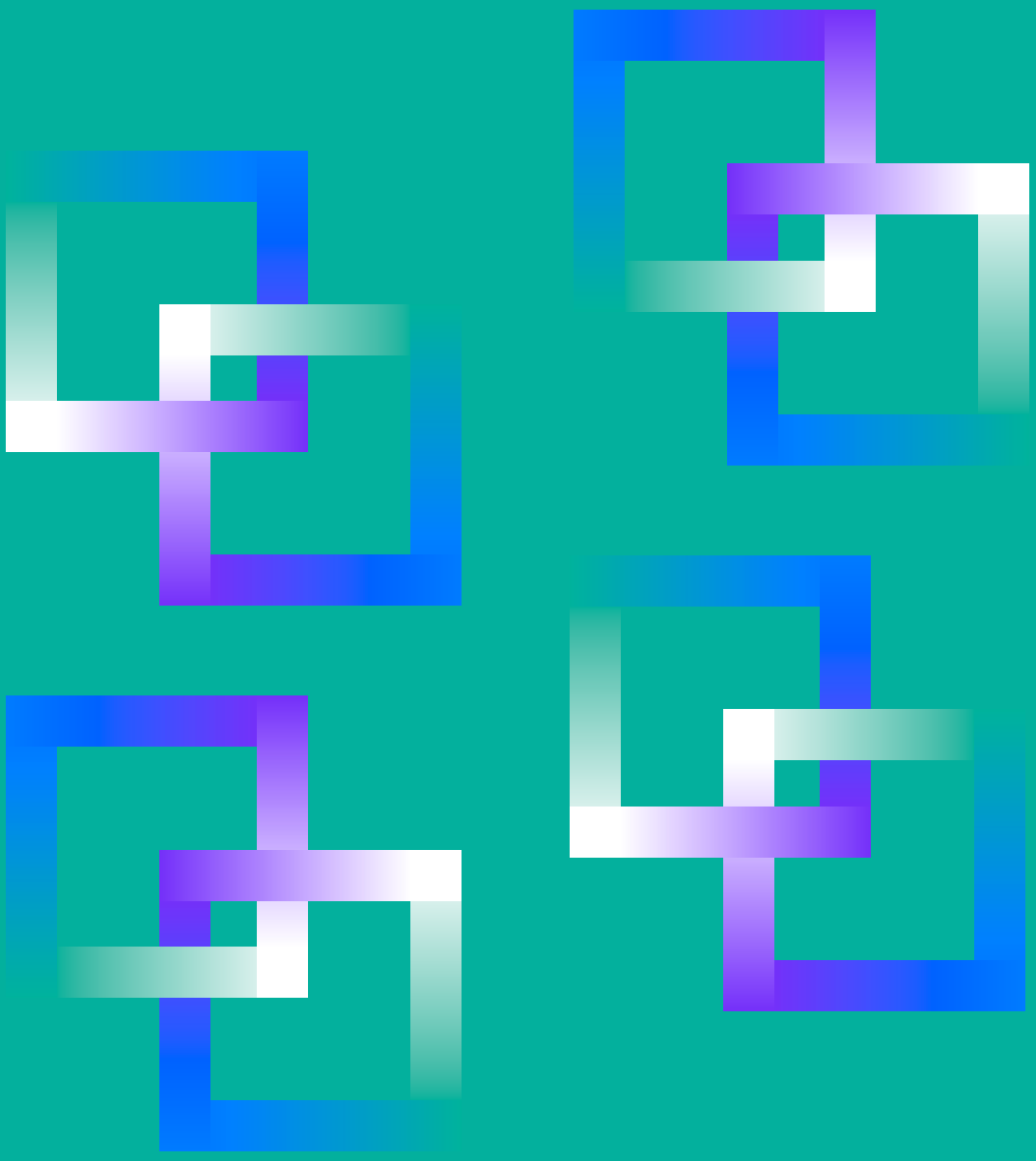
# WHITE PAPER

## ビジネスメール詐欺の最新事例と報告訓練の必要性



HENNGE

# はじめに

ビジネスメール詐欺は、企業・組織・政府機関などを狙った詐欺手法の一種です。取引先や上司などになりすました攻撃者が、企業の従業員や経営者宛てに不正なメールを送り、偽の請求書や送金指示を提示することで金銭を騙し取ります。

ビジネスメール詐欺による金銭被害は、国内外を問わず年々増加しています。IPA（独立行政法人 情報処理推進機構）では、「組織」部門で９位にランクインし、2016年以降８年連続で10位以内に入り続けています。

これまでメールを悪用した詐欺は、組織よりも個人を標的にしたケースが大多数でした。しかし近年では、その対象は個人・組織と規模を問わずとなっており、大企業を標的とした攻撃も珍しくありません。
本書では、企業が狙われたビジネスメール詐欺の事例と、対策について解説します。

出典：IPA（独立行政法人 情報処理推進機構）「情報セキュリティ10大脅威 2025」
https://www.ipa.go.jp/security/10threats/10threats2025.html

# 目次

# #1　近年のビジネスメール詐欺の事例

## ①医療製品メーカーの事例

国内に本社を置く某医療製品メーカーは、2024年1月25日、送金詐欺により自社の資金が流出したと公表しました。

■概要

同社は2023年12月、取引先を装ったメールに誘導され、攻撃者が指定した偽の口座に支払いをおこなったと報告しています。

被害の経緯として、まず同社は本来、取引先A社に対して約86万USドルの原料代金を支払う予定がありました。そこへ、A社を装った攻撃者から、支払い先の銀行口座を変更する依頼メールが届きます。同社はそれを偽メールだと気づかないまま、指示のとおり支払い先口座を変更。結果、偽の口座へと支払いを完了させてしまいました。
さらにそのあと、2024年1月初旬にも、A社を装った攻撃者から追加の支払い要請が発生。その際、支払い先としてさらに別の口座を指定され、指示どおりの口座へと支払いをおこないました。

被害に気づいたのは2024年1月中旬。B社を騙る者から、A社と同様に支払い口座の変更依頼メールが送られてきました。しかし、B社に確認をおこなったところ、メールを送信した事実はないとの回答が届きます。
これをきっかけに、A社とのやり取りについても不審を抱き調査したところ、被害が発覚したという流れです。同社では、警察と外部専門機関に依頼して調査をおこなっているものの、2024年1月段階では本件における犯人は判明しておらず、流出した資金の回収もできていないと報告しています。

■対策

被害を防げなかった最大の原因として、偽メールを疑わず本物とし、攻撃者の指示のままに支払い先口座を変更してしまった点が挙げられます。
同社とA社では長年取引が続いていたこと、受け取った偽メールが本来のA社とのやり取りと地続きの内容であったことなど攻撃の手口も巧妙であったため、偽メールの内容を疑わず、メールの本人確認手続きを省略してしまったと同社は説明しています。

このように、標的型攻撃メールは一見疑いを抱きにくいよう巧妙化されています。
そのため、どのような場合であっても、確認のプロセスは必須であると認識する必要があります。
同社においても、再発防止のために関係者への周知を徹底する、本人確認や送金プロセスを見直す、アカウントのパスワードを再設定するなどの対策を実施したと報告しました。

## ②大手法人グループ企業の事例

2023年8月21日、テレビ局傘下で文化事業を手がける企業が、ビジネスメール詐欺による資金流出の被害に遭ったことを公表しました。

■概要
報告によると同社は、取引先を装った偽メールに添付されていた請求書を受け取り、指示された内容に基づいて不正な口座へと送金をおこないました。しかし、のちに本物の取引先から「入金がされていない」と連絡が入ったことで事件が発覚しました。

同社はビジネスメール詐欺の被害に遭ったとして、事件について警察と金融機関に被害申告をおこない、対応を依頼。事件詳細については調査中であり、情報開示を制限しているとしつつも、再発防止を徹底すると報告しています。

■対策
同社は再発防止策として、関連団体への注意喚起と、幹部向けミーティングでの対策共有を実施。また、グループ会社の経理局と連携した確認体制の強化をおこなうとともに、特命監査の実施と再発防止研修を計画していると報告しました。

同社の監査委員会からは、本来の契約と異なる口座に振り込んだ、送金確認手続きの不備が指摘されています。
同時に、監査委員会は不正な口座を開設させた金融機関側の落ち度やなりすましメールが送信された取引先の情報セキュリティの脆弱性についても言及。自社だけでなく、関係各所と連携して調査をおこなうとしています。

# ＃2　IPA『ビジネスメール詐欺の事例集』より主要な事例を抜粋

ここからは、実際のビジネスメール詐欺事例について、IPAの『ビジネスメール詐欺の事例集』から一部抜粋して紹介します。

## ①銀行口座証明書類を偽造し、振込先口座の変更を依頼してきた事例(※1)

2021年3月に、国内の輸入販売業A社が送金詐欺被害に遭った事例です。

■概要

A社は、取引先である中国の企業B社とのやり取りをしていました。その最中にB社担当者から、送金先の口座を変更してほしいという旨のメールを受け取ります。A社は要望どおりに振込先の口座を変更し、送金しました。

しかし、口座変更を依頼したB社担当者は、実はなりすましによる偽者で、口座も偽の口座でした。つまりA社は、B社担当者になりすました攻撃者のメールによって、本来B社に支払うべきであった資金を偽口座に支払ってしまっていたのです。

このことに気づいたのは、送金後に攻撃者から「口座の問題で、送金されたお金が振り込まれなかった」といった内容のメールが届いたことがきっかけでした。
不審に思ったA社の担当者が、B社の社長に直接電話で確認をしたところ、B社が口座変更依頼をおこなった事実はないことが発覚。詐欺被害に遭ったと気づいたA社は、すぐに銀行に組戻し（資金返却）を依頼しましたが、資金の回収には至りませんでした。

■攻撃の手口

A社がなりすましメールに気づけなかった理由に、攻撃者の巧妙な手口が隠されています。攻撃者は以下の手法を使い、A社担当者の目を欺きました。

▼正規メールアドレスを悪用

攻撃者はB社になりすますにあたって、B社担当者の正規メールアドレスを不正利用していました。偽アドレスであれば、A社が違和感に気づけた可能性もありますが、正規アドレスからメールが届いたため、なりすましであると気づけなかったのです。

また、なりすましメールを送信する際も、単にメールを送るのではなく、A社が送信していた本物の請求メールに返信する形で送付していました。

さらに、通常であればメール送信時に入っている同報(Cc)も、本物のB社関係者のアドレスを偽のアドレスに置き換え、B社に不正メールを見られないように細工していました。

▼それらしい口座変更理由を偽装し、銀行口座証明書も偽造

攻撃者は口座変更の違和感をA社に悟られないよう、送金先変更の理由として、税務調査や監査の都合であると申告することで真実味を持たせています。

さらに、口座変更などの手続きの際に必要となる銀行口座証明書を精巧に偽造することで、A社を信用させました。

実際のメール

図 3 攻撃者からのメール 1 通目(2021年3月22日 18:11)


(※1)出典：IPA(独立行政法人 情報処理推進機構)「ビジネスメール詐欺(BEC)の詳細事例2
~銀行口座証明書類を偽造し振込先口座変更を依頼してきた事例~
https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000103087.pdf

## ②毎月の支払い方法を変更させられ、数か月間偽口座へ送金してしまった事例(※2)

国内の海外関連企業が、2021年2月から4月までの3か月間、偽口座に送金を続けてしまった事例です。

■概要

海外関連企業A社は、取引のあるアメリカの運送企業B社から、支払いの際は小切手で支払うよう依頼されていました。それがある日、B社から支払い方法を銀行振込に変更するよう指示がありました。それに従ったA社は、それ以降、2021年2月から4月までの間、B社に銀行振込で支払いをおこなっていました。

しかし、同年5月になってB社から「支払いが滞っている」といった旨の問い合わせが入ります。そこで初めて、支払い方法変更の依頼メールがなりすましであったこと、被害に気づくまで3か月もの間、偽の口座へと送金を続けてしまっていたことに気づきました。

■攻撃の手口

これまでの事例と同じく、被害発覚が遅れた理由には、メールの本人確認を怠ったことや、振込が問題なくおこなわれたかについてB社との確認が不足していたことなどが挙げられます。しかし、そもそもなぜ支払い方法変更依頼メールを偽物と疑えなかったのか。それは、攻撃者が以下のような手口で巧妙な細工をしていたからです。

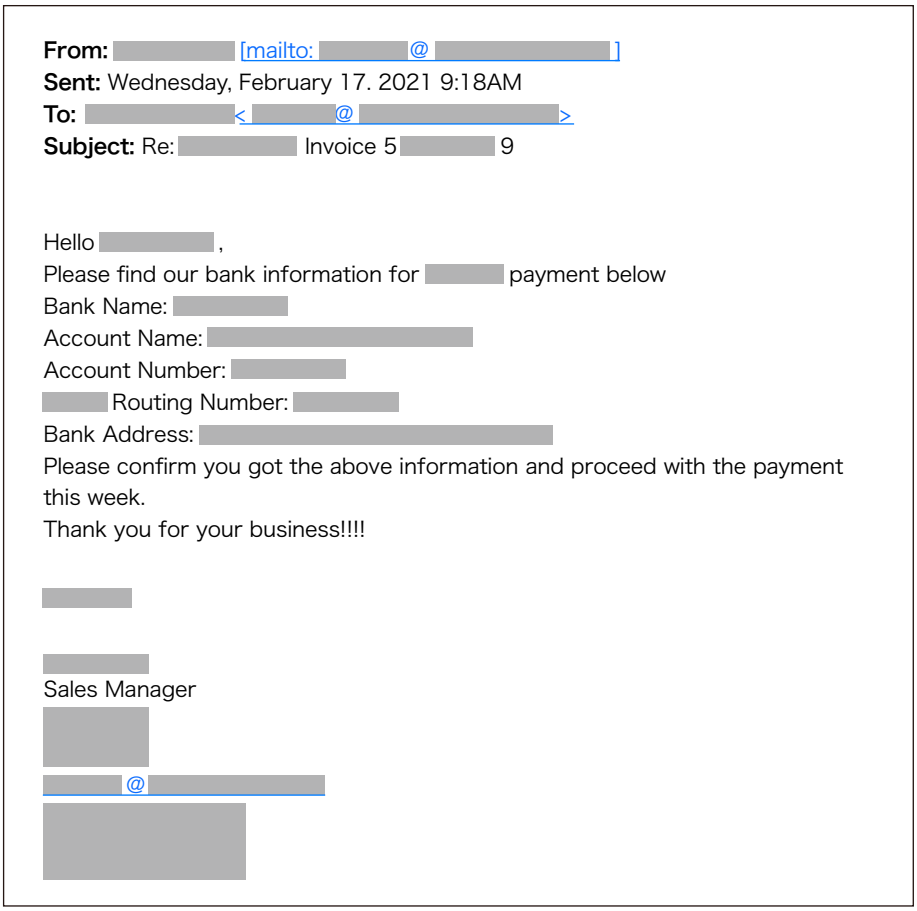
▼詐称用メールアドレスを使用

攻撃者はB社になりすますために、B社の正規ドメインに酷似したドメインを作成してメールを送っていました。たとえば、本来のドメインが「example.com」であれば、「eaxmple.com」のドメインを使ってメールを送るといった巧妙な置き換えをおこなうことで、A社の目を欺いていたのです。

▼メールの転送設定を悪用

詐称用ドメインを用意するだけでなく、攻撃者はあらかじめB社のメールアカウントに不正アクセスをおこない、メールの転送設定を操作していました。A社と本物のB社のメールを攻撃者宛に転送する設定に書き換え、二社間にどのようなやり取りが起こっているかを盗み見たうえで周到に詐欺行為をおこなっていたため、A社は届いたメールがなりすましメールだと気づけませんでした。

実際のメール
図2 攻撃者からのメール 1 通目（2021年2月17日）



**From:** [redacted] [mailto: [redacted] ]
**Sent:** Wednesday, February 17. 2021 9:18AM
**To:** [redacted] < [redacted] >
**Subject:** Re: [redacted] Invoice 5 [redacted] 9

Hello [redacted] ,
Please find our bank information for [redacted] payment below
Bank Name: [redacted]
Account Name: [redacted]
Account Number: [redacted]
[redacted] Routing Number: [redacted]
Bank Address: [redacted]
Please confirm you got the above information and proceed with the payment this week.
Thank you for your business!!!!

[redacted]
[redacted]
Sales Manager
[redacted]
[redacted] @ [redacted]
[redacted]

(※2)出典：IPA（独立行政法人 情報処理推進機構）「ビジネスメール詐欺（BEC）の詳細事例3
～毎月の支払方法を変更させられ数か月間偽口座へ送金してしまった事例～」
https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000104237.pdf

## ③国内企業社長になりすまし、グループ企業役員に金銭の支払いを要求した事例(※3)

ここまでは、国内企業がビジネス詐欺メール・なりすましによって金銭奪取の被害に遭った事例を紹介しました。最後に取り上げるのは、国内企業が攻撃者によってメールを乗っ取られたことで、ほかの企業がなりすましの被害に遭ったというパターンの事例です。

■概要

2022年8月、国内企業A社の社長は、東南アジアのグループ企業B社より連絡を受けます。内容は、「先日A社から依頼のあったM&A案件」についての確認でした。しかし、A社からB社に対してそのような依頼をした事実はありません。このことから、何者かがA社になりすまし、B社を標的とした詐欺行為を働いていることが発覚しました。

B社の説明では、A社から「M&A（企業の合併買収）について協力してほしい」といった旨のメールを受け取っていたとのことでした。しかし、B社がやり取りを続けていると、途中でA社からの連絡が途切れます。そこでB社からA社に対して、メールではなく電話で確認をおこなったところ…、というのが詐欺発覚の経緯でした。

本物のA社とB社の間で連絡が取れた時点で本件は、何者かがA社を騙りB社に詐欺行為を働いていると双方で認識されていました。
そのため、後日B社宛てに偽のA社から金銭の支払いを求めるメールが届いたものの、要求には応じなかったため、金銭的な被害はありませんでした。

■攻撃の手口
B社が直接A社に確認を取ったことで、幸いにも金銭的な被害は未然に防がれました。しかしB社は、偽メールを受け取った当初は、若干の不審を抱きながらも、メールのやり取りを続けていました。
B社が疑いを抱きにくかったのは、以下の手口が使われていたからです。

▼返信先（Reply-To）ヘッダの悪用
A社になりすました攻撃者は、メールの差出人（Fromヘッダ）に、A社社長の正規のメールアドレスを設定していました。しかし、返信先（Reply-Toヘッダ）には攻撃者のメールアドレスを設定しました。

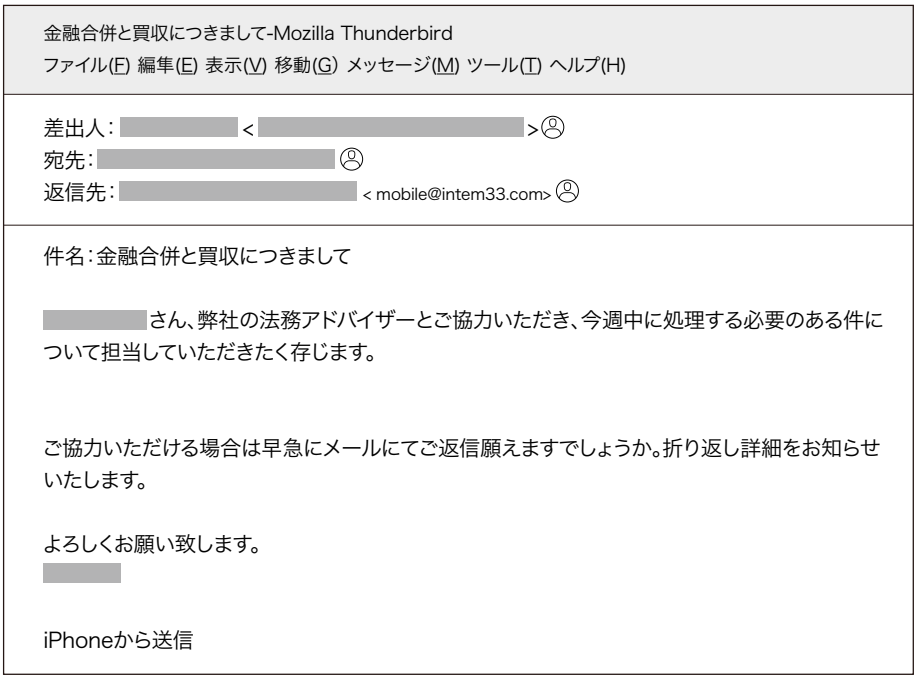
つまり、一見すると本物のA社から届いたメールに見えるものの、そのメールに返信をすると、メールはA社ではなく攻撃者のもとへ届いてしまうという設定にされていたのです。
そのためB社は、届いたメールが偽物であると疑うことが難しく、かつ、A社は自社のメールアドレスが悪用されていることに気づく余地もない、という状態でした。

▼機密性の高い案件と見せかけ判断ミスを誘発
M&Aは、企業の買収合併をおこなうという案件であるため、機密性と緊急性が非常に高いのが特徴です。社外はもちろん、社内であっても機密性を保って案件を進行する必要があることから、メールの内容を周囲に相談しにくいという性質があります。
攻撃者はこの性質を悪用し、メールの趣旨をM&AとすることでB社が確認や相談をできなく

し、判断ミスを誘発するという手口を使いました。

また、M&Aは企業の買収合併であるため、案件の進行プロセスには弁護士の力が必要となります。その弁護士の名前も、実在すると思われる弁護士名を記載することで、メールの信憑性を高めていました。

実際のメール
図2 攻撃者からのメール 1 通目


金融合併と買収につきまして-Mozilla Thunderbird
ファイル(F) 編集(E) 表示(V) 移動(G) メッセージ(M) ツール(T) ヘルプ(H)

差出人：[redacted] < [redacted] >
宛先：[redacted]
返信先：[redacted] < mobile@intem33.com>

件名：金融合併と買収につきまして

[redacted]さん、弊社の法務アドバイザーとご協力いただき、今週中に処理する必要のある件について担当していただきたく存じます。

ご協力いただける場合は早急にメールにてご返信願えますでしょうか。折り返し詳細をお知らせいたします。

よろしくお願い致します。
[redacted]

iPhoneから送信

(※3)出典：IPA(独立行政法人 情報処理推進機構)「ビジネスメール詐欺(BEC)の詳細事例6
～国内企業社長になりすまし、グループ企業役員に金銭の支払を要求した事例～」
https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/case6.pdf

# コラム：SIMスワップ

「SIMスワップ」という手法をご存じでしょうか。SIMスワップは、携帯電話のSIMカードを悪用した手法で、もとは海外で横行していた詐欺手法が、日本国内にも流入してきたものです。

SIMカード（Subscriber Identity Module）はご存じのとおり、携帯電話やスマートフォンなどの端末で使用される小型のICカードです。このカードには、契約者の識別情報や電話番号、暗号化キーが保存されています。端末にカードを認識させることで、音声通話・SMS・データ通信などのサービスが利用可能となります。

このSIMを、攻撃者が被害者になりすまして乗っ取るのがSIMスワップです。SIMを乗っ取ることで、攻撃者は被害者の電話番号を自分の端末で使用できるようになります。すると、SMS認証や通話を通じた、個人情報や金融アカウントへの不正アクセスが可能になるのです。そのためSIMスワップは、特に多要素認証を回避し、銀行口座や暗号資産ウォレットを狙うケースで使われます。

## SIMスワップの事例：警察の取り組み

SIMスワップを利用した悪質な詐欺犯罪は年々増加していて、警察でも大掛かりな捜査が実施されています。

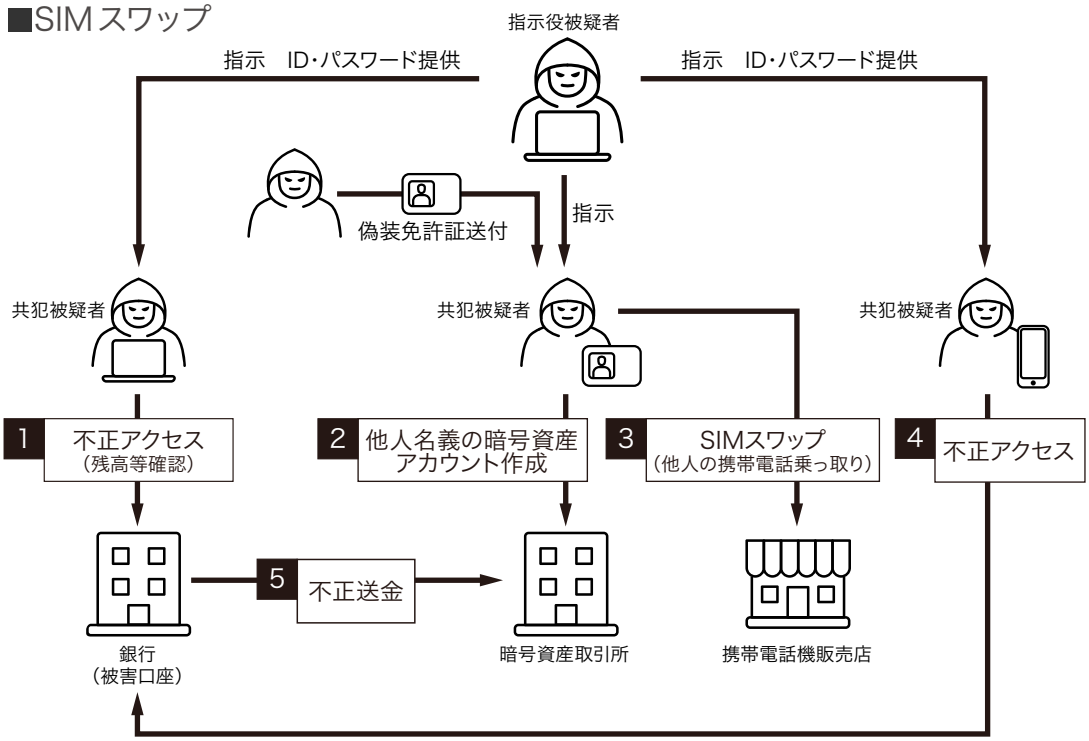
2024年、警察庁サイバー警察局は、2022年から2023年にかけて発生したインターネットバンキングでの不正送金事件について、犯行グループの指示役を特定・逮捕したと報告しています。
同事件の捜査では、関係都道府県警察が得たサイバー犯罪に関する情報を、サイバー特別捜査部が集約・分析。さらに、暗号資産の追跡捜査や関係被疑者のSNSアカウントを捜査しました。
その結果、2022年から2023年にかけて多発したインターネットバンキングでの不正送金事件が、すべて同一の犯行グループによるものと判明しました。

さらなる調べにより、犯行グループの犯行手口と実態が解明され、犯行グループの指示役とみられる男も特定され、2024年7月には男の逮捕に至りました。
犯行グループによってもたらされた被害は甚大で、被害件数は少なくとも20件、被害総額は1億2,000万円にのぼることが明らかとなっています。

## SIMスワップの事例：犯行の手口

本事件において、犯行グループが利用した手口がSIMスワップです。同グループはSIMスワップの手法を駆使し、組織的に不正送金をおこなっていました。

この事件で主な標的となっていたのは、インターネットバンキングです。インターネットバンキングでは、送金の際に、SMS認証による本人確認が求められます。SMS認証は、口座開設者が登録した電話番号宛てに送られるため、通常であれば第三者が不正に利用することはできません。
この防壁を突破するために、SIMスワップが利用されました。




出典：警察庁サイバー警察局「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

手口全体の流れとして、まず犯行グループの指示役が、ダークウェブ上で売買されているインターネットバンキング口座の識別符号（ID やパスワード）を入手します。あるいは、不正プログラムを使って識別符号を窃取します。これにより、口座への不正ログインが可能となります。
次に、不正ログインによって口座の登録情報を盗み見て、被害者の電話番号を入手。入手した電話番号を使って、SIMスワップを実行します。

指示役は、SIMスワップの実行役を用意するために、被害者と見た目や年齢が近い者を探します。被害者になりすまし、携帯電話の事業者を騙すためです。
実行者探しにはSNSが使われることが多く、「バイトを紹介する」「割のいい副業を教える」などと称して募集をかけます。つまり、実行役はいわゆる「闇バイト」の応募者です。

指示役は別の仲間に、被害者の運転免許証などの身分証明書を偽造させます。もちろん顔写真も、SIMスワップ実行役の写真です。そして、偽造身分証をSIMスワップの実行役に渡します。

偽造身分証を持った実行役は、被害者になりすまして携帯電話事業者の店舗に赴きます。あるいは、インターネット窓口に相談の連絡をします。そして、偽造身分証を提示したうえで、担当オペレーターに「携帯電話を紛失したのでSIMカードを再発行したい」「携帯のキャリアを変更したい」などの申し出をすることで、被害者の電話番号を乗っ取ります。
そうすることで、被害者の電話番号をSIMスワップ実行者が利用できるようになり、インターネットバンキングの送金時に送られるSMS認証のコードも、実行者が確認できるようになります。
最後に認証コードを実行役から指示役に伝えれば、指示役はインターネットバンキングのSMS認証を突破し、不正送金が実行されます。

これが、SIMスワップを使った不正送金手口の一連の流れです。

## SIMスワップを防ぐ方法

SIMスワップの被害に遭わないためには、まず「インターネットバンキングの識別符号を知られない」「電話番号などの個人情報を知られない」といった注意が求められます。
では、具体的にどういった方法を取るべきなのか。これについて、ユーロポール（欧州刑事警察機構）が、以下の内容を推奨しています。

- デバイスのソフトウェアを最新の状態に保つ。
- 不審なメールにあるリンクのクリックや、添付ファイルのダウンロードをおこなわない（マルウェアやフィッシングによる個人情報などの漏えいを防ぐため）
- 不審なメールに返信したり、個人情報を要求する発信者と電話でやり取りしたりしない
- オンラインで、個人情報をむやみに公開しない
- 二要素認証は SMS ではなく、認証アプリやワンタイムパスワード用のトークンデバイスを使用する

- 可能であれば、電話番号を機密性の高いアカウントに紐づけない（銀行に登録する電話番号は本人確認に使われる可能性があるため、携帯電話ではなく固定電話にする）
- SIM に PIN を設定する（SIM の盗難による悪用を防止）

現時点では、SIM スワップによる送金詐欺は、個人への被害に留まっています。しかし、インターネットバンキングの利用や、電話番号と口座の紐付けなどは、個人に限らず企業でももちろんおこなわれています。
つまり将来的には、企業が攻撃のターゲットになることも十分に考えられるということです。この攻撃がもしも企業に向けば、金額や規模においても甚大な被害を被ることとなります。そのため、「個人が標的だから大丈夫」と考えずに、企業でも上記の対策を取ることが強く推奨されます。

# #3　まとめ

メールを悪用した詐欺は、これまでは個人が標的にされることが多く、注意喚起や対策も個人に向けたものがほとんどでした。しかし、時代が進むにつれて、メール詐欺は個人だけの問題ではなく、企業や組織を脅かすことも多い重大なリスクとなりました。

詐欺の手法は年々巧妙化しています。新たなテクノロジーやサービスが台頭すれば、併せて新たな詐欺犯罪も現れるため、際限がありません。
特にビジネスメール詐欺は、成功すれば多額の金銭が得られるのに加え、企業の対策もおくれを取りがちで騙しやすいといった点から、犯罪者からすればいわば「トレンド」の詐欺方法ともいえます。
企業は卑劣な犯罪者の脅威から自社を守り、安心してビジネスを展開するためには、常に最新の情報を把握し、十分すぎるほどの対策をすることが求められるでしょう。

中でも、従業員一人ひとりの「気づき」を促す教育や訓練は、技術的対策と並ぶ重要な柱です。HENNGE が提供する標的型攻撃メール訓練サービス「Tadrill」は、ドメイン偽装など実際の手口に即した訓練を通じて、一見すると問題がないように見えるメールに潜む違和感を見抜く力を高めることが可能です。

## Tadrill によるビジネスメール詐欺（BEC）対策と報告訓練

### ■巧妙化する BEC 攻撃に備える「人の目」の強化

＃2の②でご紹介した毎月の支払い方法を変更させられ、数か月間偽口座へ送金してしまった事例にあるように、攻撃者は巧妙なドメイン偽装や文面の工夫で、受信者が不審に感じにくいメールを送付します。こうした脅威に対抗するには、技術的な対策だけでなく、「受信メールをそのまま信じない」というセキュリティリテラシーを従業員一人ひとりが身につけることが不可欠です。

### ■報告訓練で運用を定着させ、被害拡大を防ぐ

- Tadrill の訓練でリテラシー向上：実際のドメイン偽装メールを模した訓練により、受信メールの真偽を見抜く力を養います。
- 迅速な報告体制の構築：不審なメールを発見した際、あるいは万が一返信してしまった場合は、速やかに報告することが被害拡大を防ぐ鍵です。

- 報告アドオンで簡単報告：Tadrill の報告アドオンを使えば、不審メールをワンクリックで簡単に管理者に対して、報告ができます。この手軽さが、緊急時の対応フローを運用として定着させ、全社的な啓蒙に繋がります

Tadrill を活用した報告訓練の導入により、「メールを受け取る現場」における気づきと行動のレベルを引き上げ、組織全体で被害の未然防止に取り組むことが可能となります。

# #４　HENNGE Oneで実現する クラウドセキュリティ

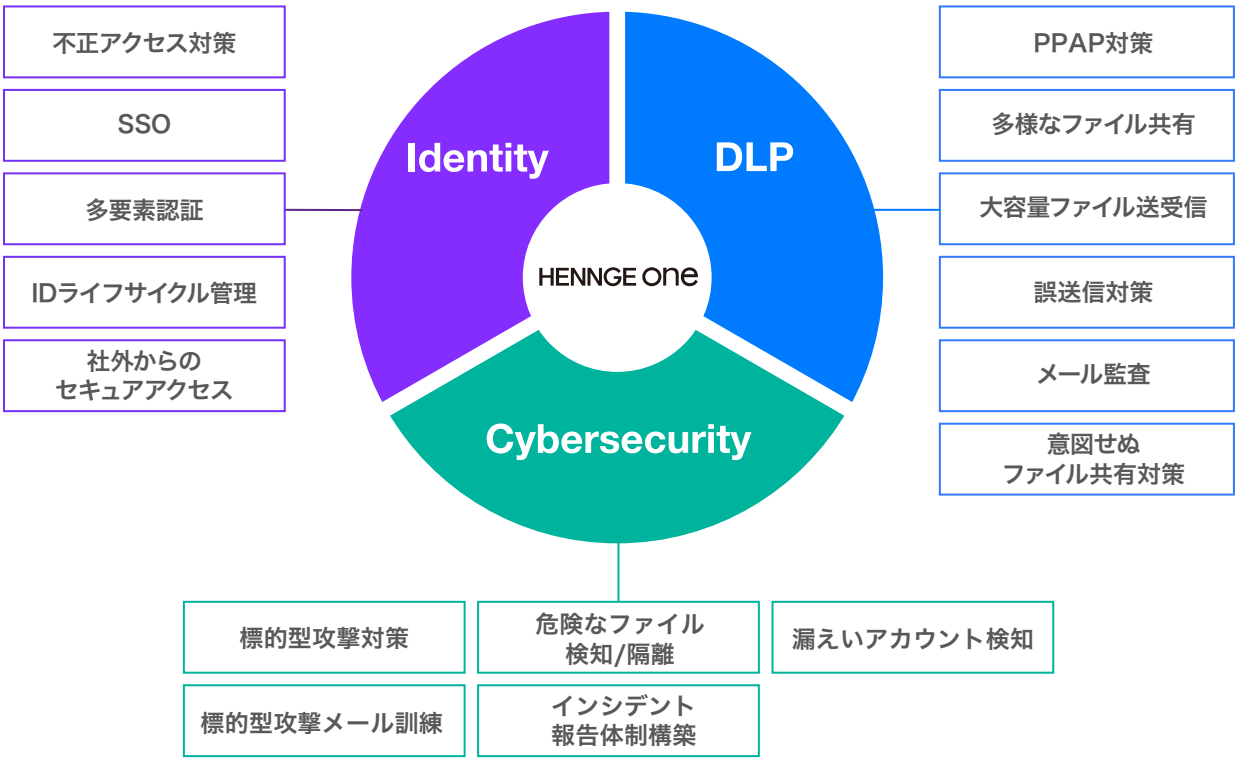
## HENNGE Oneについて

サイバーセキュリティの手口は巧妙さを増してきていますが、『攻撃の糸口』は似通っています。それを防ぐための基本的な対策は変わらないものも多いため、まずは１つのソリューションを導入するなどできることから対策を始めるのがおすすめです。

HENNGE Oneはあらゆる組織の“ちょうどいい”を実現する国内シェアNo.1（※4）のクラウドセキュリティサービスです。

具体的には、HENNGE Oneは大きく３つのEditionで構成されています。
シングルサインオンによって組織に存在する様々なシステムのIDを統合し、多要素認証によってアクセス制御・不正アクセス対策を実現する「Identity Edition」。
企業内に散在するデータの意図せぬ情報漏えいを防止する「DLP Edition」。そして、テクノロジー、人、プロセスの全方位で組織をサイバー攻撃から守る「Cybersecurity Edition」。
時代の変化に合わせて、全ての組織に最適なクラウドセキュリティを提供します。

https://hennge.com/jp/service/one/




(※4)ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2025」IDaaS市場：ベンダー別売上金額シェアにて2021年度、2022年度、2023年度、2024年度予測の４年連続で１位を獲得

# 会社概要

| | |
|---|---|
| 会社名 | HENNGE 株式会社（HENNGE K.K.） |
| 役員 | 代表取締役社長　小椋 一宏 |
| 設立 | 1996 年 11 月 5 日 |
| URL | https://hennge.com/jp/ |
| 事業内容 | HENNGE One の開発、販売、サポート |