

～ 手口と対策を知る ～
ビジネスメール詐欺（BEC）に
ご注意ください！

2026年4月30日

世界が進むチカラになる。



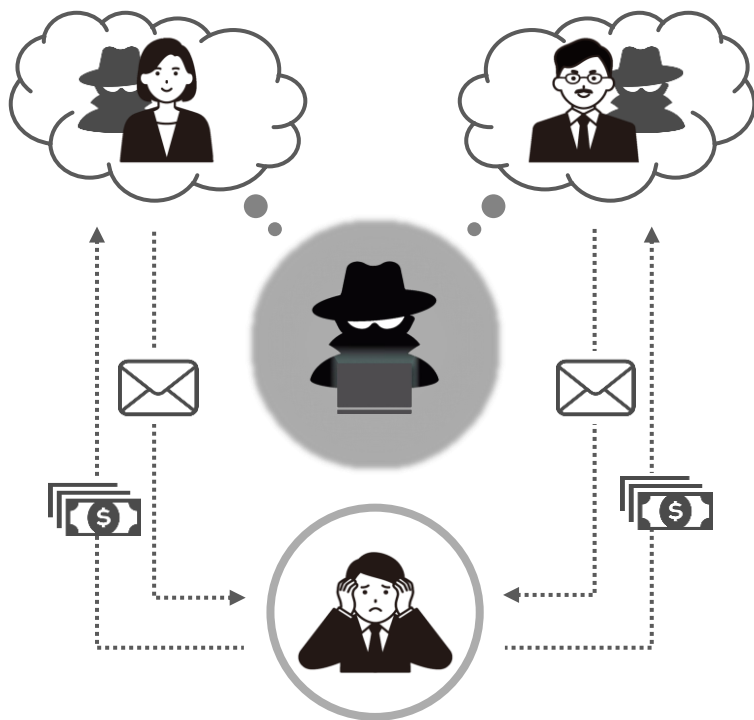
目次

ビジネスメール詐欺（BEC）とは？	03
BECの主な手口について	04
各手口におけるチェックポイント	06
具体的な対策方法／事例	07
BEC被害発生時の対応／ご参考コンテンツ	08
国内振込をさせるCEO詐欺の手口について	09
国内振込をさせるCEO詐欺被害発生時の対応／ご参考コンテンツ	10
Appendix：事例紹介	11

ビジネスメール詐欺（BEC）とは？

ビジネスメール詐欺（BEC：ビーイーシー）とは？

犯罪者がEメールのやりとりを不正アクセスなどで盗み見た後、偽のメールアドレスを使用したり、サーバーを乗っ取ることで、取引先や親会社のCEO等になりすまし、Eメールを送り付けて犯罪者の口座に送金を依頼するという手口の詐欺です。



BECの被害に遭われた方たちの声

Q 被害発生時¹BECを知っていましたか？

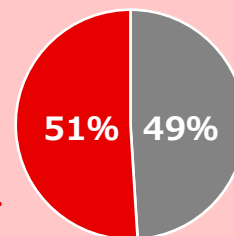
(注) 1. 対象期間：2022年6～12月

BECという詐欺は初耳だった。

知らなかった 知っていた

BECは知っていたが、まさか自分が騙されるとは思っていなかった。

いつものお取引先からのメールだと信じてしまい、少しおかしい点があったが大丈夫だろうと思った。



BECは英語圏を中心に、国や地域を問わず世界中で発生しています。会社の規模も問わず標的となっています。被害金額は1億円以上も珍しくなく、何十億円にも上る巨額な被害も発生しています。ぜひ本資料をご活用いただき、BEC対策を進めていただけますと幸いです。



BECの主な手口について

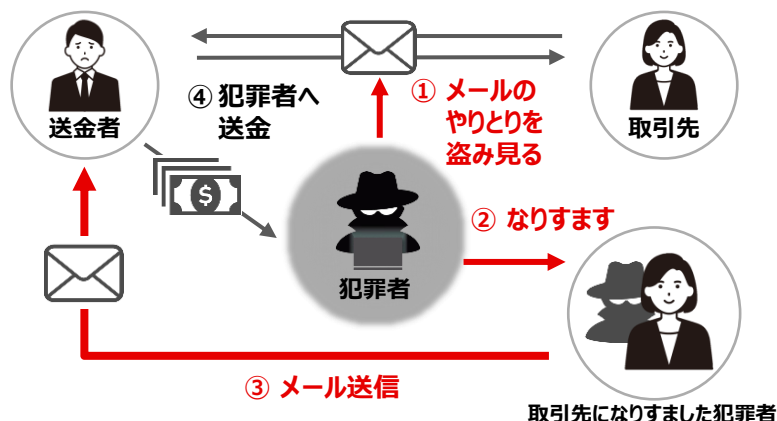
ベンダー詐欺とは？

犯罪者は、送金者と海外の取引先とのメール上での商談を盗み見ます。そして取引先になりすまし、送金者が商品等の代金を送金する際、送金先口座番号・名義等の変更を指示し、犯罪者の口座へ送金するよう依頼します。

長年取引のある先と新規取引先、どちらもなりすましの対象となります。

送金先口座の変更の際は、何らかの理由をつけて送金者を信じ込ませます。

- ・今回はグループ会社宛に送金して欲しい
 - ・会社合併により口座名義が変更になった
 - ・社内監査中（Audit）で口座が利用できない …など
- イギリスへの送金を指示するケースが多く発生しています。



具体的な事例

From : satou@wxyz.jp To : tanaka@xxx.jp
代金のお支払いは以下の口座をお願いします。

受取銀行	●●Bank	口座番号	1234567
受取銀行所在国	USA	受取人所在国	USA
口座名義	MUFG.co.ltd		

取引先 (佐藤さん)

送金者

From : tanaka@xxx.jp To : satou@wxyz.jp
分かりました。明日支払います。

翌日

From : satou@vxyz.jp To : tanaka@xxx.jp
昨日誤った口座を案内してしまいました。以下の口座に送金してください。

受取銀行	▲▲Bank	口座番号	7654321
受取銀行所在国	UK	受取人所在国	USA
口座名義	MUFG.co.ltd		

取引先に なりすました 犯罪者

なんでUKの口座なんだろう。でも期限が迫ってるし。佐藤さんはいつも正確だから信用しよう。

From : tanaka@xxx.jp To : satou@vxyz.jp
承知致しました。今日▲▲Bankに送ります。

数日後

From : satou@wxyz.jp To : tanaka@xxx.jp
まだ代金が支払われていないようです。

取引先 (佐藤さん)

送金者

From : tanaka@xxx.jp To : satou@wxyz.jp
言われた通り▲▲銀行に送りましたよ！

From : satou@wxyz.jp To : tanaka@xxx.jp
▲▲銀行への送金依頼はしていません。

途中からメールアドレスのドメインが違っている！

犯罪者の口座へ 送金実行

BECの主な手口について（続き）

CEO詐欺とは？

犯罪者が自社・親会社のCEOや役員等になりすまし、M&Aの資金が必要などと偽り、犯罪者の口座へ送金を指示します。
国内外に子会社や現地法人を持つ法人は、より注意が必要です。
犯罪者は送金者の周囲に気づかれないよう、Eメール内で情報統制を指示します。

- ・ 本件は極秘（Confidential）事項、社内でも口外不可
- ・ 本送金は至急（Urgent）対応が必要 …など

Eメールだけでなくディープフェイクボイス（AIで生成した偽音声）を利用し、CEO等の声色・口調に酷似した「電話」をかけてくるケースも発生しています。

弁護士など「権威ある第三者」を騙る人物が登場し、信用させるケースも発生しています。

香港への送金を指示するケースが多く発生しています。

電話の場合、
「ディープフェイクボイス」の
手口も発生



送金者



or/and

② 犯罪者へ
送金



自社・親会社CEO等
になりすました犯罪者

① メールや電話で
「極秘」「至急」等の送金指示

具体的な事例



部下

（大役をまかされてしまった…）かしこまりました。



誰にも
言わないよう
気をつけよう

突然だが極秘PJでM&A案件を進めていて、指定の口座へ●億円
送金してほしい。送金先は後ほどメールで伝えるから至急で頼む。

CEOになりすました
犯罪者



From : ceo@vxyz.jp To : tanaka@wxyz.jp
先ほどの件だが、▲▲Bank、口座番号……に送金してほしい。
情報漏洩すると契約違反になるから口外しないように。



From : tanaka@wxyz.jp To : ceo@vxyz.jp
至急送金します。

数日後



From : ceo@vxyz.jp To : tanaka@wxyz.jp
この間ありがとう。追加資金で今度は■億円を至急送金してほしいんだ。



From : tanaka@wxyz.jp To : ceo@vxyz.jp
かしこまりました…。

数時間後



短期間で2回も高額な送金ってやっぱりおかしいな。
不安だからCEOに念の為に再度確認しよう

先ほどのM&Aの追加資金ですが、
▲▲Bankに■億円の送金で間違いはないでしょうか。

私はそのような送金指示はしていないよ。



あれは偽物のCEOからの電話とメールだったんだ。
騙された…。



CEO
(本人)

犯罪者の口座へ
送金実行

各手口におけるチェックポイント

下記のような状況にはご注意ください!



ベンダー詐欺の気をつけるポイント

- ☐ 「監査中で従来の口座が使えない」「口座情報が誤っていた」等の理由で、送金直前に送金実績のない口座への変更を依頼された
- ☐ INVOICEの内容が正しいかをチェックしていない
(口座情報変更の言及無く、さりげなく送金先口座が変更されたINVOICEが送付されるケースもある)
- ☐ 受取人所在国と受取銀行所在国が異なる
- ☐ INVOICE受領部署と支払実行部署が違う
(部署ごとでBECの知識・対応に差がでしまう)
- ☐ 従来の実務担当者・責任者が出張・休暇・異動等で不在のタイミングに依頼を受けた
- ☐ 取引先のメールアドレスが正しいかを確認していない
(メールアドレスの一部が相違している可能性がある。
例: mufg.jp ⇒ **rn**mufg.jp)
- ☐ 取引先のメールアドレスが正しいことを確認したため、取引先へ電話等で送金先口座について事実確認をしていない (取引先のメールアドレスと乗っ取られ、なりすまされている可能性がある)
- ☐ 取引開始したばかりで初めて送金するため、取引先へ送金先口座について事実確認をしていない (取引開始時になりすまされるケースがある)
- ☐ 送金先口座について事実確認する際、取引先からのメールに「返信」する形で確認している (なりすましメールに返信している可能性がある)

CEO詐欺の気をつけるポイント

- ☐ 親会社CEOや役員を名乗る人物よりM&Aプロジェクトのための資金等と言われ送金指示を受けた
- ☐ 数千万円、数億円と高額な送金指示を受けた
- ☐ 「極秘で進めてほしい」「情報漏洩しないように」「至急対応してほしい」などの指示があった
- ☐ 送金指示を受けた際、昇進をほのめかす言葉や「今後大きな仕事を任せる」などの言葉をかけられた
- ☐ CEO等のメールアドレスが正しいかを確認していない
- ☐ CEO等のメールアドレスが正しいことを確認したため、送金について電話等で事実確認をしていない (メールアドレスと乗っ取られ、なりすまされている可能性がある)
- ☐ 送金先口座について事実確認する際、CEO等からのメールに「返信」する形で確認している (なりすましメールに返信している可能性がある)
- ☐ 弁護士等の権威ある第三者を名乗る人物を、仲介人として紹介された
- ☐ CEO等の声色・口調 (英語・日本語等) に酷似した電話がかかってきた
- ☐ 表示された電話番号がCEOや親会社等の電話番号と一致していた (電話番号表示は偽造の可能性がある)
- ☐ 業務連絡で使用しているLINEやWhat's App等でも送金指示を受けた (メールだけではなくメッセージアプリでもなりすましに遭う可能性がある)

具体的な対策方法／事例

具体的な対策方法

送金依頼メールを受信した際の対策

□ 相手方への事実確認は電話で実施

- ・「口座変更」の依頼には、Eメールではなく**電話にて**確認してください
- ・電話で確認する際は**Eメールに記載されている番号ではなく**、必ず名刺や事前に登録・届出済の番号で確認してください
- ・連絡手段がEメールのみの場合、「**返信**」ではなく「**転送**」にて、改めて「（名刺等に記載された）正しいメールアドレス」を入力し返信してください（但し、相手方のメールアドレスが乗っ取られている可能性に留意が必要です）

□ 送金時は単独で対応せず**複数名**で確認

- ・「極秘」「至急」等と指示を受けても、まずは周囲の方に相談しましょう

日頃の対策

□ 資金管理・送金時承認プロセス等の見直し

- ・送金時の**社内独自のルールを制定する**等対策をとり、社内牽制体制を構築してください
- ・銀行取引権限者が休暇や異動で代わる場合は、引継ぎの際にBECについて確り担当者にお伝えし、備えてください

□ 社内のセキュリティ対策の見直し

- ・ハッキングされる原因の一つとして**ウイルス感染**が考えられます。不審メールの添付ファイルは開かないよう日頃から注意し、セキュリティソフトを導入のうえ最新の状態にアップデートしてください
- ・**メールアドレスへの不正アクセス**も原因の一つとして挙げられます。過去に引っかかったフィッシングサイトへの自分のアドレス・パスワード等の入力がかかけの可能性があります。**安易なパスワードの設定をしない**、他のサービスと**同じパスワードを使い回さない**ように社員一人一人が気をつけましょう

対策事例

対策① 新規取引開始時・送金先口座変更時の口座確認の徹底

- ・新規取引開始時に「**BANK STATEMENT**」（銀行取引を証明する書類）の受入れをお勧めします
- ・「**振込先変更依頼書**」を独自で作成し、取引先より受入れることをお勧めします
- ・上記書類は**対面もしくは郵送にて**受入れてください（メールでの送受信では偽造される可能性があります）

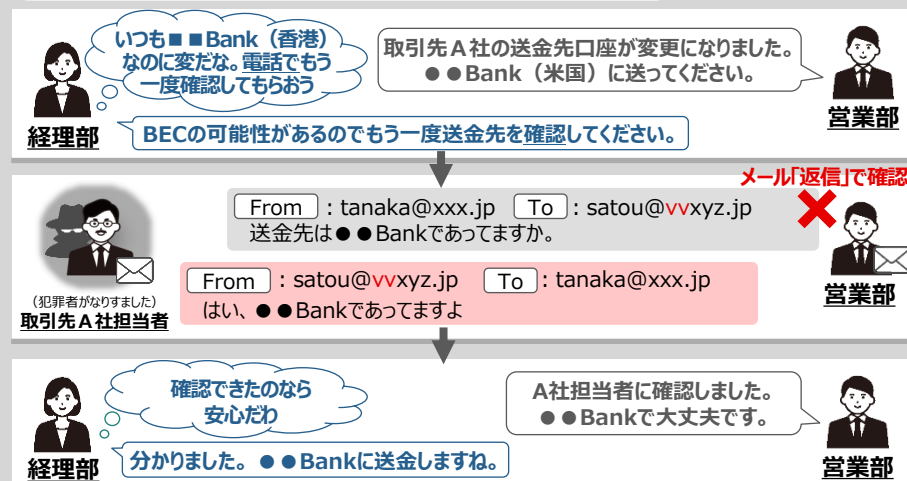
対策② 送金時のルールの制定

- ・「受取人所在国と受取銀行所在国が違う場合は電話で確認」、「役員からの送金指示は必ず経理部長に確認する」など独自のルールを制定

対策③ 社内で勉強会を実施

- ・部署ごとで知識の差がでないよう、**送金プロセスに関係する部署（含む国内外の子会社等）は全員**正しい知識を身に付けるようにしてください

BECに関する知識に差があるため正しく確認できないケース



このケースでは営業部の知識不足により、電話で確認すべきことをメールに「返信」する形で確認してしまいました。

BEC被害発生時の対応／ご参考コンテンツ

BEC被害発生時の対応

□ 受取銀行への至急の組戻依頼

- ・ 詐欺が発覚した場合、直ちに**取引銀行（仕向銀行）にて組戻し手続きを実施**してください
- ・ **“FRAUD（詐欺）／Business Email Compromise”**を理由として組戻しを実施してください



□ 警察への相談・被害届提出

- ・ 日本の警察だけでなく、**現地（受取銀行所在国）の警察**への相談・被害届を提出することも重要です。捜査を促すケースもあります
- ・ 組戻しの際、受取銀行から被害届（Police Report）の提出を要求されることもあるため、極力ご対応ください



□ セキュリティ点検と対策実施

- ・ 機密情報や顧客情報もハッキングされている可能性があります。**システム周りの点検**を実施してください
- ・ 不正アクセスの原因究明をしたうえで、該当取引メールを授受している関係者の**パスワードや署名**を一斉変更してください
- ・ **取引先・自社どちらがハッキングされているかは、本格的な調査をしないと分かりません。**
二次被害防止のため早期対処が重要です



ご参考コンテンツ ～勉強会等にてご活用ください～

コンテンツ①

- ・ 当行HPに動画「BECを知る ～被害に遭わないために～」を掲載しております（日本語版・英語版）（視聴時間：約4分30秒）
- ・ 経理・財務のご担当部署のみならず、営業・購買・国際部署、国内外の関連会社等幅広く、また実務ご担当の方から管理職・経営層の皆さまに至るまで、海外送金取引に関わる全ての方にご覧頂くようご案内いただけますと幸いです
URL https://www.bk.mufig.jp/info/security/caution_bec.html

日本語版



英語版/
中国語
字幕版



コンテンツ②

- ・ 当行HPにBEC疑似体験サイトを掲載しております（日本語版・英語版）
- ・ 体験サイトでは、BECの被害に遭う流れを疑似体験いただけます。その恐ろしさを実感するとともに、被害に遭わないためにはどこに気を付けたいのか、ぜひご体験ください

[BEC疑似体験サイト（日本語版）](#)

[BEC Simulator（英語版）](#)



コンテンツ③

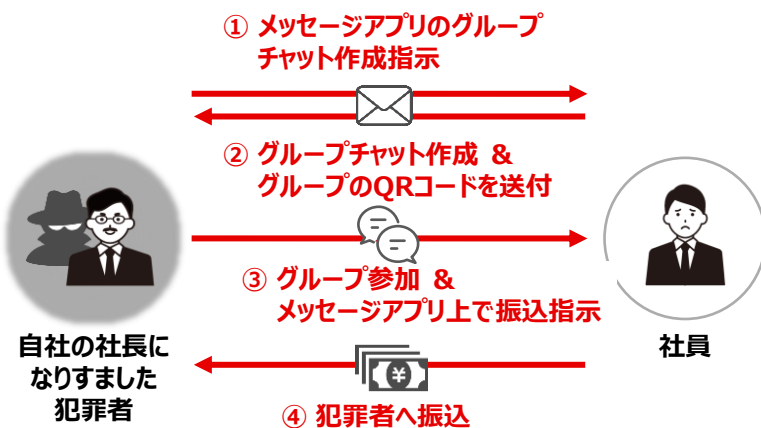
- ・ 独立行政法人 情報処理推進機構／IPA（外部機関）がBEC対策の映像コンテンツ（What's BEC? ～ビジネスメール詐欺手口と対策～）を作成しています（日本語版・英語版）（視聴時間：約12分）
URL <https://www.ipa.go.jp/security/videos/list.html>

国内振込をさせるCEO詐欺の手口について

国内振込をさせるCEO詐欺とは？

会社の社長などを騙るメールを社員に送り、メッセージアプリ（LINE等）のグループチャットに誘導します。その後、会社の口座から国内振込を指示する手口です。

- ・ 犯罪者はメールで、「業務上必要なため、至急LINEのグループを作成し、グループの二次元コードを本メール宛てに送付してください」などと指示します。
- ・ 社員が二次元コードをメールで送信すると、社長を騙るアカウントがグループチャットに参加します。
- ・ 会社の口座情報（店番・口座番号・残高等）を尋ねた後、国内振込を指示します。



社長を騙る犯罪者から受信するメールの例

差出人：＜自社の社長の名前＞

件名：＜会社名＞

【重要なお知らせ】

業務上必要なため、至急、新しいLINEグループを作成してください。

【グループ作成時の注意事項】

- ・ 他の方は一切招待しないでください。
- ・ グループは「作成のみ」で結構です。グループの作成が完了しましたら、LINEグループのQRコードを本メール宛に直ちに送付してください。私がグループに参加し、業務指示およびメンバー追加はすべてグループ内で行います。速やかに対応のうえ、必ず返信してください。

<社長名>

2026.XX.XX

被害を防ぐために

□ 相手方へ電話・対面で事実確認を実施

- ・ LINE等のメッセージアプリのグループ作成や振込に関するメールを受信した場合は、送信元のメールアドレスが**真の社長のメールアドレスと一致しているか**確認してください
- ・ 加えて、**口頭**や**電話**等の**Eメール・メッセージアプリ以外の手段**で本人に事実確認を実施してください
- ・ 電話で確認する際は、**Eメールやメッセージアプリに記載されている番号ではなく、必ず事前に登録済の番号や名刺に記載の番号に連絡**してください。



国内振込をさせるCEO詐欺被害発生時の対応／ご参考コンテンツ

国内振込をさせるCEO詐欺被害発生時の対応

□ 振込先銀行への連絡

- ・ 詐欺が発覚した場合、**振込先の口座がある銀行**に連絡してください。
各銀行の連絡先は下記をご参照ください。
- ・ 「ビジネスメール詐欺の被害を受け、そちらの銀行（振込先の銀行）の口座に資金を振り込んだ」旨を伝えてください。
- ・ 連絡先

振込先が三菱UFJ銀行口座の場合

振り込め詐欺救済法照会ダイヤル
0120-860-413（平日9時～17時）

振込先が三菱UFJ銀行以外の口座の場合

（全銀協）金融犯罪に遭った場合のご相談・連絡先

<https://www.zenginkyo.or.jp/hanzai/information/>



□ 警察への相談（被害届の提出）のご案内

- ・ 詐欺が発覚した場合、最寄りの警察へのご相談・被害届のご提出をご検討ください。



ご参考コンテンツ

コンテンツ①

- ・ 国内振込をさせるCEO詐欺の注意喚起を目的としたチラシを警察庁が作成しています。ぜひご活用ください
- ・ 「法人を対象とした詐欺（ニセ社長詐欺）に注意！」
URL：
<https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260213/01.html>



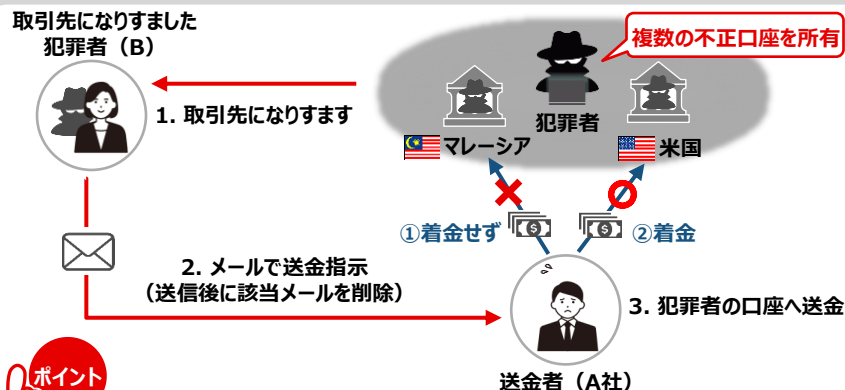
（出所）警察庁

Appendix : 事例紹介

- ベンダー詐欺、CEO詐欺の事例を紹介します。普遍的なケースをもとに作成しており、実際に発生した事案ではございません。

ベンダー詐欺

- A社と従来の取引先とのメールのやりとりの中で、取引先よりタイの口座への送金依頼あり。
- 翌日、メールアドレスを乗っ取り、取引先になりすました犯罪者（B）より、監査中で従来のタイの口座が使えないためマレーシアの口座へ送金するよう、指示あり。
- A社はBの指示通り、マレーシア向けに送金を実施。
- マレーシアの受取銀行より、銀行判断（詳細不明）により返金される。
- 送金できなかったことをBへ伝え、今度は米国の銀行への送金を打診され、A社は送金を実施。
- 後日、真の取引先より商品代金未着の照会あり。
- 取引先が調査したところ、メールボックスに隠しフォルダが作成されており、A社より受信したメールが、気付かないうちに格納されていたことが判明し、詐欺が発覚。尚、犯罪者が取引先担当者になりすましてA社に送信したメールは、削除されていた。

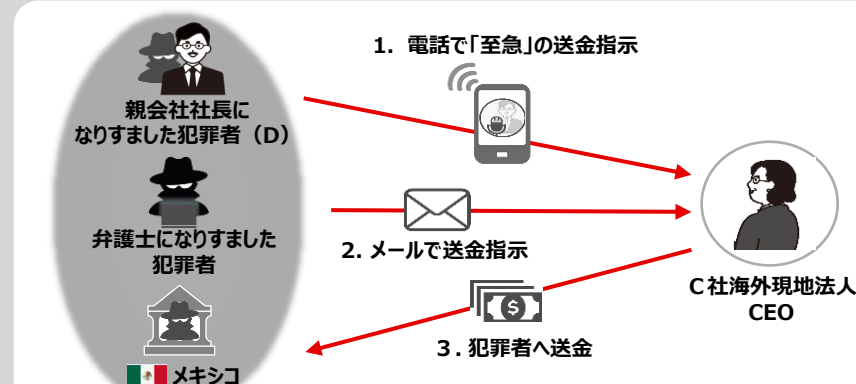


ポイント

- メールアドレスを乗っ取られた場合、なりすまされた本人が気づかないうちに、メールの送受信が操作されてしまう。そのため、詐欺発覚までに時間を要することがある
- 犯罪者は組織化しており、複数の国に不正口座を保有。送金が失敗しても、手持ちの口座を次から次へと提示してくる
- 受取銀行より入金を拒否されたり、複数回送金先の変更がある場合は、BECの可能性大

CEO詐欺

- C社の海外現地法人CEOは、C社社長を騙る人物（D）より受電。グループ会社への貸付金を立替えてほしいと依頼あり、メキシコにある口座に●億円送金するよう指示を受ける。
- DはCEOに対し至急送金するように指示し、送金先情報については担当弁護士とやりとりするよう依頼。
- その後、担当弁護士を名乗る人物より、送金先情報をメールにて受信。CEOは指示通りに送金を実施。
- 送金後、立替金が返金されないことを不審に思い、C社社長の携帯電話に連絡。グループ会社への貸付の予定がないことが判明し、詐欺が発覚。



ポイント

- M&A資金の他、グループ会社間の貸借を背景とした送金指示もある。立替金は「一時的なもの」「すぐに返金する」などと伝え、送金者を安心させる
- 発生件数のうちの殆どをベンダー詐欺が占めるが、CEO詐欺は、1件あたりの送金額が高額になる傾向があるため、被害発生後の対応の負担が大きい
- 公開情報を悪用しているため、弁護士に関してネットで検索すると該当情報はあがるが、実在の弁護士は送金とは無関係

本プレゼンテーションにより、貴社と株式会社三菱UFJ銀行の間には何ら委任その他の契約関係が発生するものではなく、当行が一切法的な義務・責任を負うものではありません。

本資料は信頼できると考えられる各種データに基づいて作成されていますが、当行はその正確性、完全性を保証するものではありません。ここに示したすべての内容は、当行の現時点での判断を示しているに過ぎません。また、本資料に関連して生じた一切の損害については、当行は責任を負いません。その他専門的知識に係る問題については、必ず貴社の弁護士、税理士、公認会計士等の専門家にご相談の上ご確認下さい。

本資料は当行の著作物であり、著作権法により保護されております。当行の事前の承諾なく、本資料の全部もしくは一部を引用または複製、転送等により使用することを禁じます。

Copyright 2026 MUFG Bank, Ltd. All rights reserved.



株式会社 三菱UFJ銀行

〒100-8388 東京都千代田区丸の内1-4-5

<https://www.bk.mufg.jp/index.html>