ビジネスメール詐欺（BEC）の詳細事例 7

～取引先のメールアカウントが乗っ取られ
詐欺メールを送信された事例～

2024 年 5 月 16 日

独立行政法人情報処理推進機構
セキュリティセンター

目次

1. 概要

本事例は、2023 年 11 月から 12 月にかけて、国内企業（A 社：支払側）と海外取引先企業（B 社：請求側）間の取引の中、B 社の担当者になりすました攻撃者が A 社の担当者に、取引の送金先口座変更を求める偽のメールを送りつけて金銭を詐取したものです。こちらは、「ビジネスメール詐欺（BEC）対策特設ページ」の「ビジネスメール詐欺のパターンとは [1]」で紹介している「タイプ 1：取引先との請求書の偽装」に該当します。

この事例では、攻撃者が海外取引先担当者のメールアカウントを乗っ取っていたとみられ、正規のメールアカウントから偽のメールを送付した点等の特徴的な点が確認されました。これらの特徴を知っていただき、被害防止に役立てていただくため、ここに紹介します。

なお、今回の事例でやりとりされたメールはすべて英文でした。

1.1. IPA への情報提供の経緯

本事例については、A 社から IPA のコンピュータ不正アクセス届出窓口 [2]に届出があり、そこから攻撃者とやりとりしたメール等の詳細な情報をご提供いただきました。

---

1 IPA：ビジネスメール詐欺（BEC）対策特設ページ
ビジネスメール詐欺のパターンとは
https://www.ipa.go.jp/security/bec/bec_pattern.html

2 IPA：コンピュータウイルス・不正アクセスに関する届出
コンピュータウイルス・不正アクセスに関する届出について
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

1.2. 本事例の関係者

本事例の関係者を表 1 に示します。

表 1 本事例の関係者一覧

名前	説明
A 社	日本国内の企業。支払側。
A 社担当者	A 社の本件における取引担当者。攻撃者からの偽メールを受信し、やりとりを行った。
B 社	海外(以降、X 国)にある A 社の取引先企業。請求側。
B 社製品担当者	B 社の本件における製品担当者。攻撃者にメールアカウントを乗っ取られたとみられる。
B 社会計担当者	B 社の本件における会計担当者。A 社担当者と本件の支払いに係るやりとりをしていた。
B 社責任者	B 社の本件における責任者。被害発生後、やりとり中の不審点に気が付いた A 社担当者から相談を受けた。
攻撃者	ビジネスメール詐欺によって A 社から金銭を詐取した。 B 社製品担当者のメールアカウントの乗っ取り、及び B 社メールアドレスのドメインと類似した詐称用ドメインの取得を行い、B 社製品担当者と B 社会計担当者になりすました。
C 銀行	A 社の口座がある日本国内の銀行。
D 銀行	攻撃者が指定した口座のあるスペインの銀行。なお、X 国はスペインではない。

1.3. 本事例の流れ

本事例では、攻撃者が二度にわたり口座変更依頼を行ってきたこともあり、A 社担当者と攻撃者との間で多数のメールのやりとりが行われました。本節ではやりとり全体の流れを概説し、続く 2 章でやりとりを 4 つのブロックに分割してそれぞれの流れについて詳説します。

まずは、全体の流れを図 1 に示します。

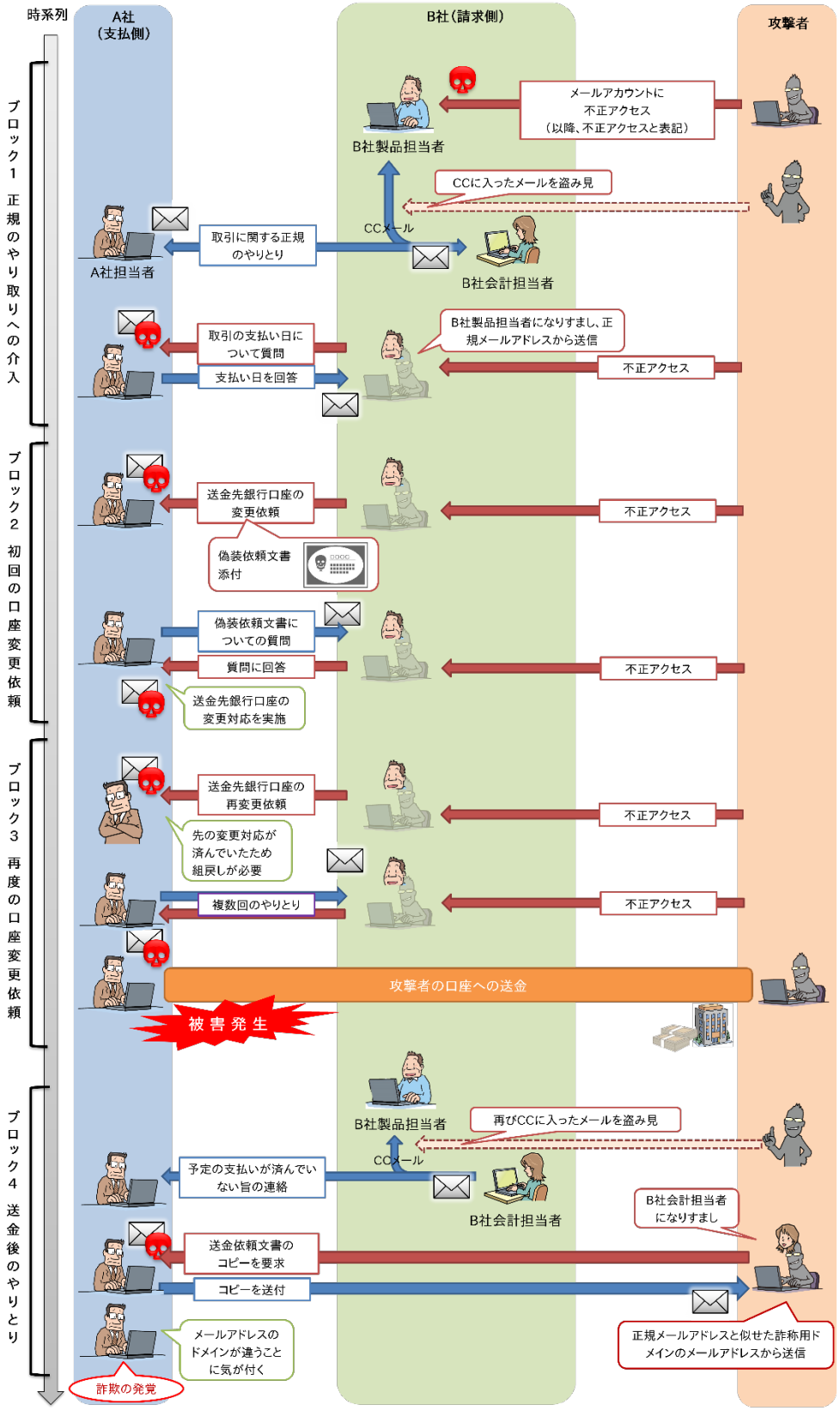
時系列
A社
（支払側）
B社（請求側）
攻撃者
ブロック1 正規のやり取りへの介入
ブロック2 初回の口座変更依頼
ブロック3 再度の口座変更依頼
ブロック4 送金後のやりとり
メールアカウントに
不正アクセス
（以降、不正アクセスと表記）
B社製品担当者
CCに入ったメールを盗み見
CCメール
取引に関する正規
のやりとり
A社担当者
B社会計担当者
取引の支払い日に
ついて質問
支払い日を回答
B社製品担当者になりすまし、正
規メールアドレスから送信
不正アクセス
送金先銀行口座の
変更依頼
偽装依頼文書
添付
偽装依頼文書に
ついての質問
質問に回答
送金先銀行口座の
変更対応を実施
送金先銀行口座の
再変更依頼
先の変更対応が
済んでいたため
組戻しが必要
複数回のやりとり
攻撃者の口座への送金
被害発生
再びCCに入ったメールを盗み見
予定の支払いが済んでい
ない旨の連絡
B社会計担当者
になりすまし
送金依頼文書の
コピーを要求
コピーを送付
メールアドレスの
ドメインが違うこと
に気が付く
正規メールアドレスと似せた詐称用ド
メインのメールアドレスから送信
詐欺の発覚

図 1 攻撃全体の流れ

図 1の通り、本事例は、攻撃者がB社製品担当者のメールアカウントに不正アクセスをして、A 社 B 社間の取引に係るメールのやりとりを盗み見たことから始まったものと推測されます。攻撃者は、盗み見た情報等を基に B 社製品担当者のメールアカウントから A 社担当者に偽の送金先口座変更依頼を送り付け、複数回のやりとりを経て A 社から金銭を詐取するに至りました。

また、この事例では、支払い予定日後にB 社会計担当者からA 社担当者に支払いが済んでいないという問い合わせのメールが送付された際、攻撃者は詐称用ドメインを使い B 社会計担当者になりすまし、偽メールを A 社担当者に送付していました。こちらの詳細は後述しますが、詐欺の発覚を少しでも遅らせる狙いがあったと推測されます。

なお、攻撃者による正規やりとりへの最初の介入から、最終的に詐欺が発覚するまでの期間は、約 1 ヵ月でした。

2. 攻撃の詳細

本章では、本事例の攻撃の詳細について 4 つのブロックに分けて説明します。各ブロックの内容については、図 1 の左部に記載した次の通りとなります。

- ブロック 1:正規やりとりへの介入
- ブロック 2:初回の口座変更依頼
- ブロック 3:再度の口座変更依頼
- ブロック 4:送金後のやりとり

2.1. 正規やりとりへの介入

はじめに、攻撃者による A 社 B 社間の正規やりとりへの介入について説明します。
まずは、本ブロックの流れを図 2 に示します。

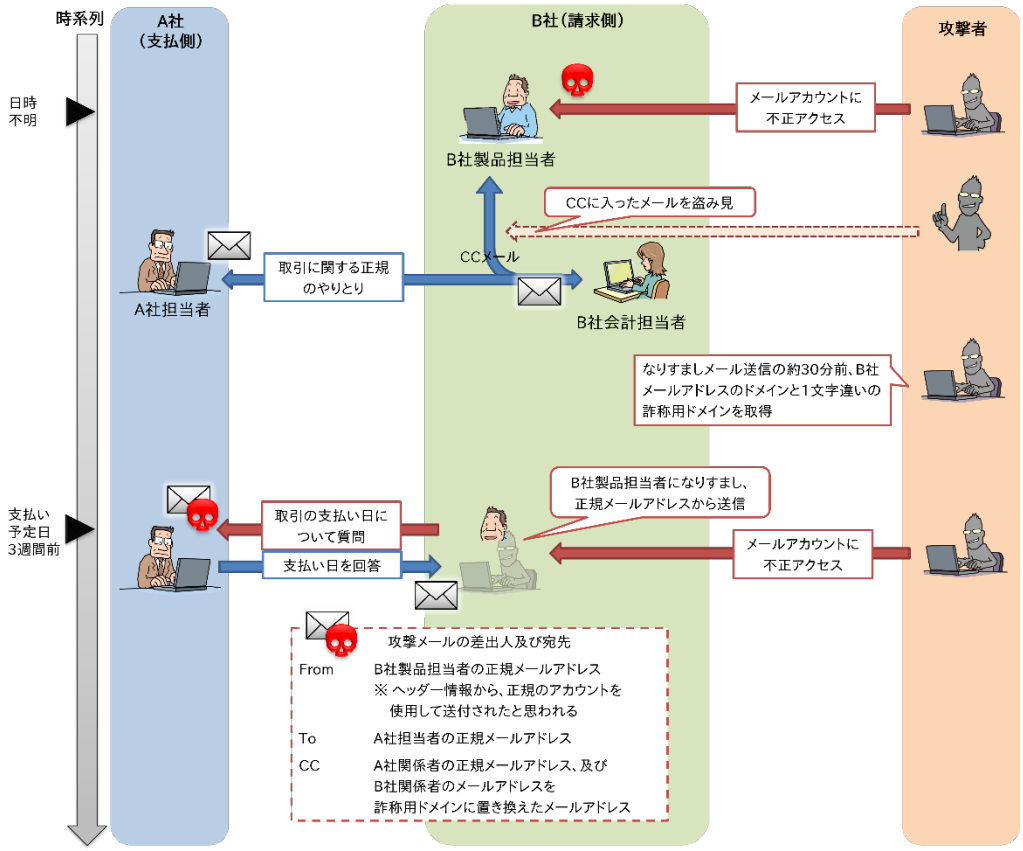

図 2 正規やりとりへの介入までの流れ

A 社と B 社間のメールのやりとりは、主に A 社担当者と B 社会計担当者との間で行われており、メールの同報先(CC)には B 社製品担当者を含む双方の関係者が設定されていました。

支払いに関するやりとりを幾度か繰り返し、支払いの予定日まで約 3 週間と迫った頃、攻撃者が A 社担当者宛てに、B 社製品担当者のメールアカウントを送信元とした 1 通のメールを送信しました。当該メールは、本取引に係る A 社担当者と B 社会計担当者間のメールのやりとりの返信であり、CC に設定された A 社関係者のメールアドレスは正規のものでしたが、B 社関係者のメールアドレスは正規ドメインと 1 文字違いの詐称用ドメインに差し替えられていました。また、各メールアドレスに紐づけられた表示名は、全て正規のメールと同様に各担当者の氏名が設定されており、これは以降の攻撃者からのメールでも同様でした。なお、この詐称用ドメインはメールが送信される約 30 分前に取得されたものでした。

使用された詐称用ドメインと正規ドメインの差分イメージを図 3 に、着信したメールを図 4 に示します。

本物のメールアドレス　：　[B社関係者の正規ローカル部] @ abc●●company.com

偽のメールアドレス　：　[B社関係者の正規ローカル部] @ adc●●company.com

→ 社名部分を一文字のみ変更

（この例では「b」を「d」に変更）

図 3 使用された詐称用ドメインのイメージ

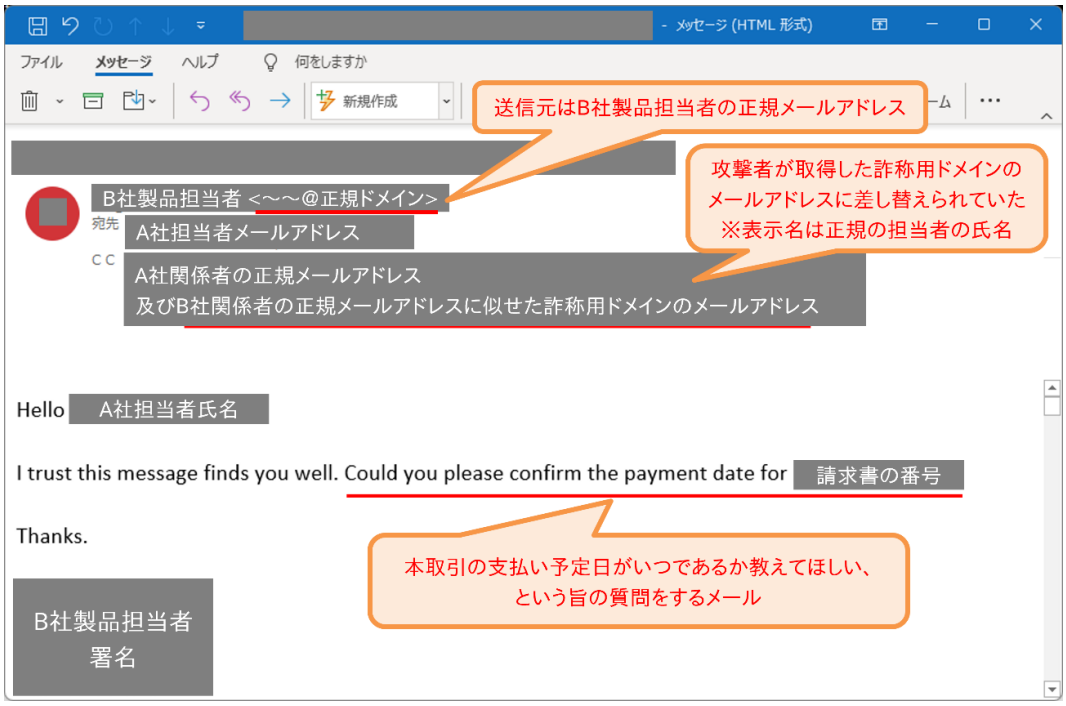

図 4 攻撃者から最初に着信したメール

このメールの内容は「本取引の支払い予定日を確認させてほしい。」というものでした。また、このメール及び以降の攻撃者からのメールでは、CC に設定された B 社関係者のメールアドレスは詐称用ドメインのものに差し替えられていたため、B 社製品担当者以外の B 社関係者のもとには着信していませんでした。

本事例では、このメールを皮切りに攻撃者による取引への介入が開始されました。メールのヘッダー情報から、当該のメールは正規経路を通って送受信されたものである可能性が高く、攻撃者が B 社製品担当者のメールアカウントを乗っ取って、そこから攻撃メールを送信したと推測されます。なお、攻撃者が B 社製品担当者のメールアカウントへの不正アクセスに成功した時期は不明です。従前よりB 社製品担当者のメールを盗み見ていた可能性もあれば、攻撃メール送信の直前に盗み見が始まり、メールボックス内の過去のメールを見られた可能性もあります。

このメールを受信した A 社担当者は、支払い予定日を回答するメールを返信してしまいました。攻撃者が正規のメールアカウントから送信してきたことで、A 社担当者としては違和感に気付くことが困難であったと推測されます。

2.2. 初回の口座変更依頼

続けて、攻撃者からの口座変更依頼について説明します。

まずは、本ブロックの流れを図 5 に示します。

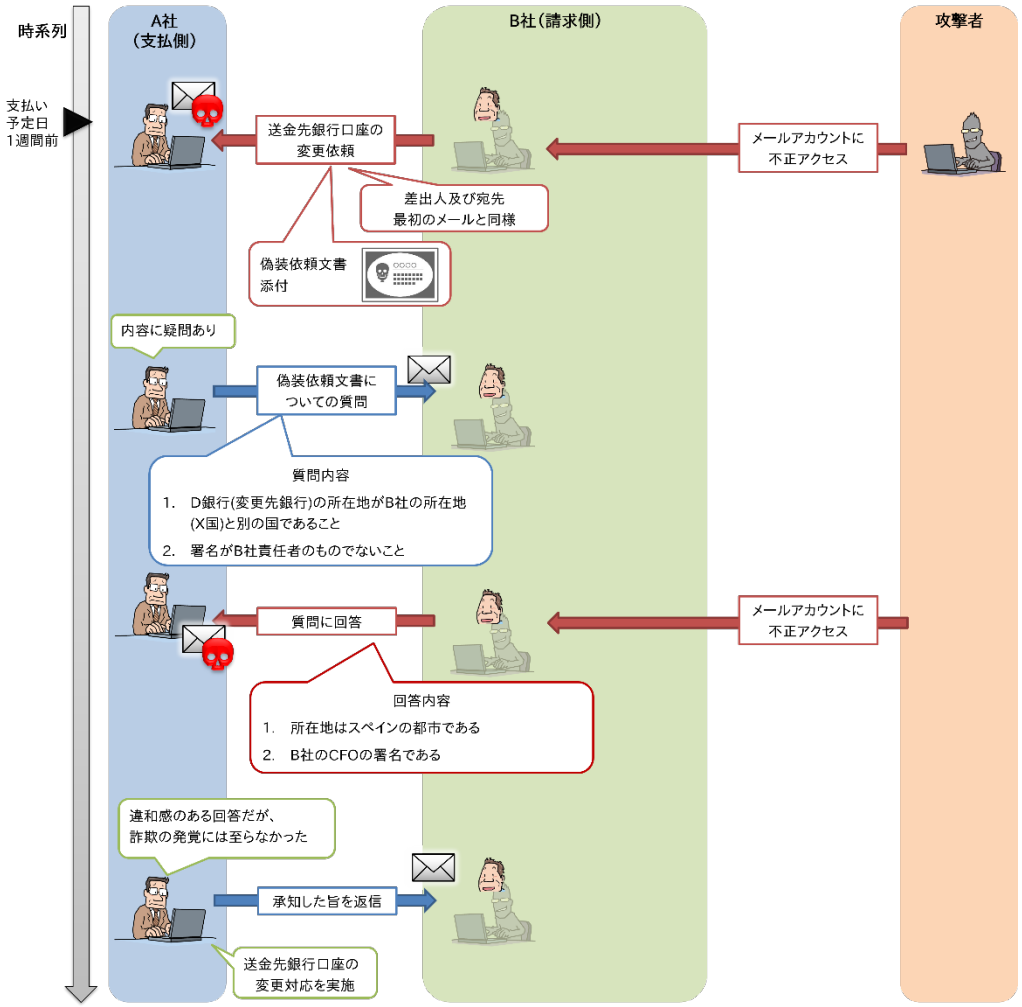

図 5 攻撃者からの口座変更依頼の流れ

攻撃者による正規やりとりへの最初の介入から約 10 日後、予定されていた支払い日まで残り 1 週間ほどに迫ったタイミングで、再度攻撃者から A 社担当者に偽のメールが着信しました。本メール並びに以降の攻撃者からのメールは、基本的に初回のメールと同様に B 社製品担当者のメールアカウントから送信されており、CC の B 社関係者のメールアドレスは図 3 の詐称用ドメインのものに差し替えられていました。

メールの内容は、「会計監査上の理由により、送金先の銀行口座を D 銀行に変更してほしい。」というものであり、変更先の銀行口座の情報が記載された PDF ファイルが添付されていました。

この添付ファイルのイメージを図 6 に示します。

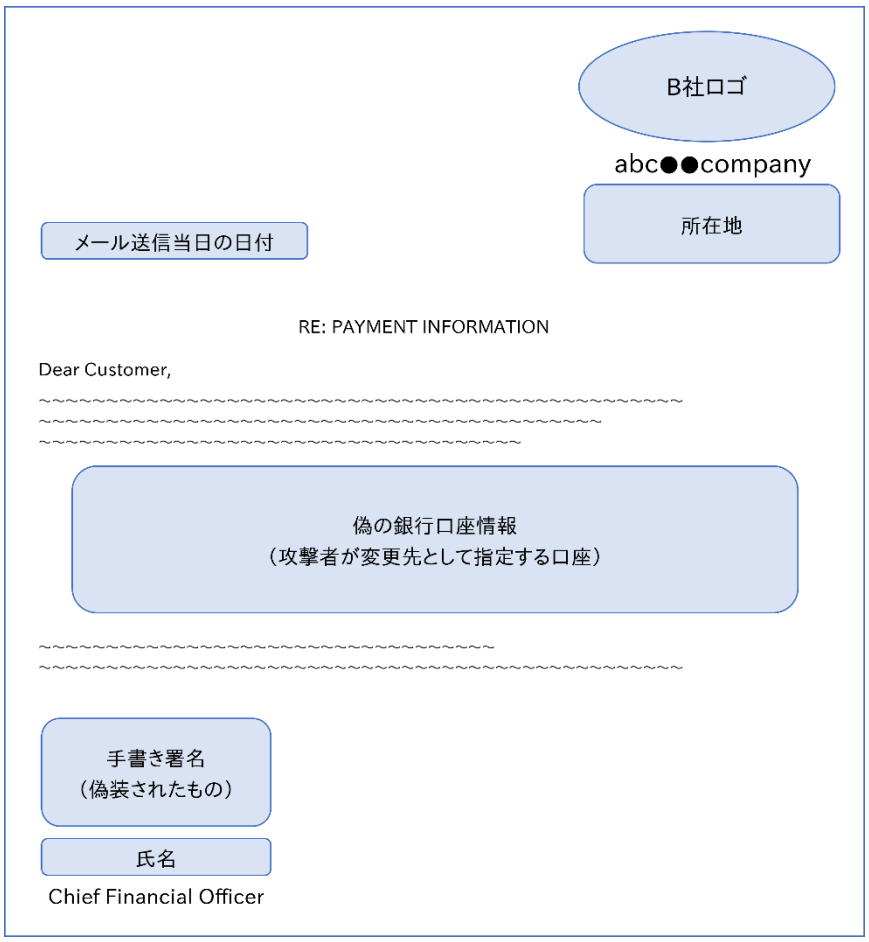

図 6 口座変更依頼メールの添付ファイルのイメージ

メールを受け取った A 社担当者は、添付ファイル中で指定された変更先の D 銀行の所在地が B 社の所在する X 国ではなくスペインであったこと、並びに、ファイル中に記載された署名が B 社責任者のものでないことに疑問を持ち、その旨を質問するメールを返信しました。すると、攻撃者からは、それぞれ以下のような回答がありました。

- 質問：「D 銀行の所在地が B 社の所在国(X 国)でないことについて」
  攻撃者からの回答：「スペインの都市の名前である。」
- 質問：「署名が B 社責任者のものでないことについて」
  攻撃者からの回答：「B 社 CFO(Chief Financial Officer：最高財務責任者)のものである。」

これらの回答について、A 社担当者の質問意図とは異なるものであったと推測されますが、詐欺が発覚するまでには至らず、A 社担当者は攻撃者からの指示に従い、送金先を攻撃者指定の口座に変更する手続きを進めました。

2.3. 再度の口座変更依頼

続けて、攻撃者からの二度目の口座変更依頼について説明します。

まずは、本ブロックの流れを図 7 に示します。

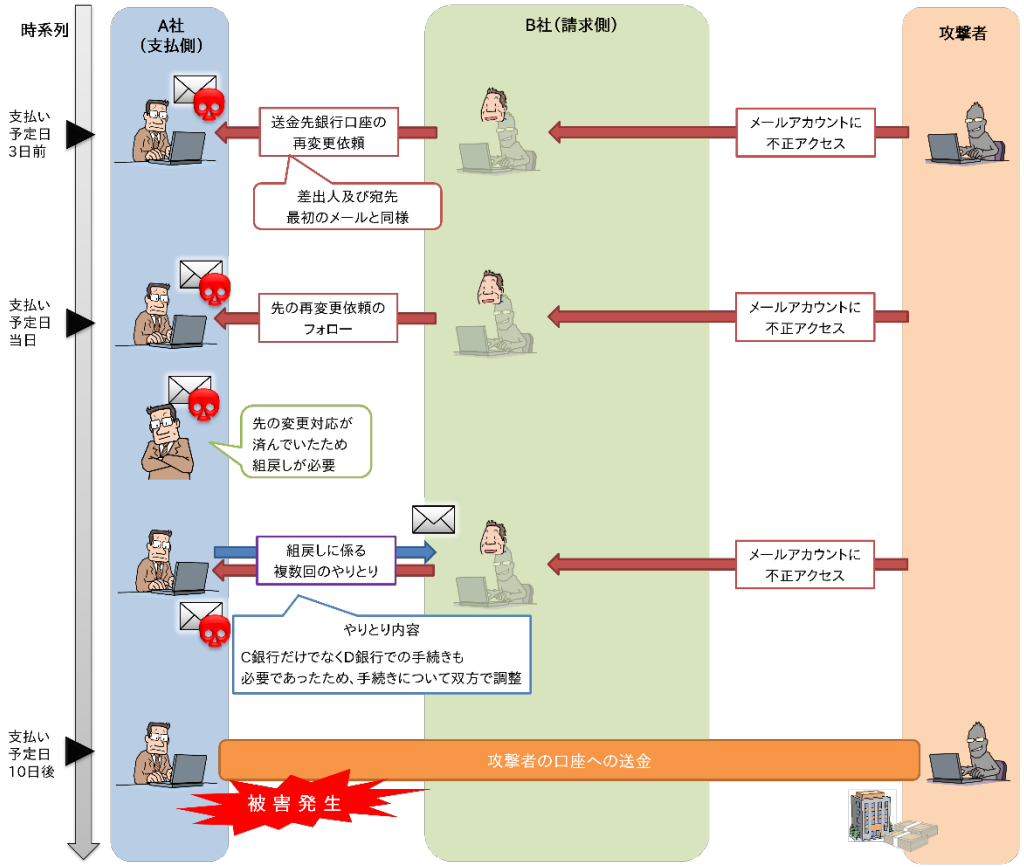

図 7 攻撃者からの口座変更依頼の流れ

初回の口座変更依頼メールから 4 日後、支払い予定日まで 3 日と迫ったところで、攻撃者から A 社担当者に、再度の口座変更依頼メールが着信しました。このメールでも、初回の口座変更依頼同様に PDF ファイルが添付されており、当該ファイルの作成・編集日時から、図 6 に示した初回のメールで使用したものを編集して作成したものと推測されます。なお、指定された口座は初回の依頼時と同じ D 銀行のものでした。

この添付ファイルのイメージを図 8 に示します。

図 8 再度の変更依頼メールの添付ファイルのイメージ

図 8 に示した通り、このファイルは初回の変更依頼メールの添付ファイルを一部変更したのみであり、手書き署名を含めた大部分は使いまわしであったとみられます。

攻撃者が再度の口座変更依頼を行った理由は不明ですが、当初の変更先口座が引き出しのできない状態になったなど、攻撃者にとって何らかの不都合が生じたことが推測されます。

このメールを受けた A 社担当者は、依頼に従い、再度の送金先口座変更を行おうとしましたが、この時点で既に初回で指示された口座への送金手続きが完了してしまっていました。そのため、組戻し後に再変更先口座への送金手続きを行うこととし、B 社製品担当者になりすました攻撃者にメール返信するとともに手続きを進めました。なお、組戻し手続きには C 銀行だけでなく D 銀行での手続きも必要であったため、A 社担当者と攻撃者の双方で調整しつつ進められました。

再度の変更依頼メールから 2 週間弱経過後、当初の支払い予定日から 10 日ほど遅れで送金処理が完了しました。なお、本事例では、1 千万円を超える金額が攻撃者によって詐取されてしまいました。

2.4. 送金後のやりとり

最後に、送金後に詐欺被害が発覚するまでのやりとりについて説明します。

まずは、本ブロックの流れを図 9 に示します。

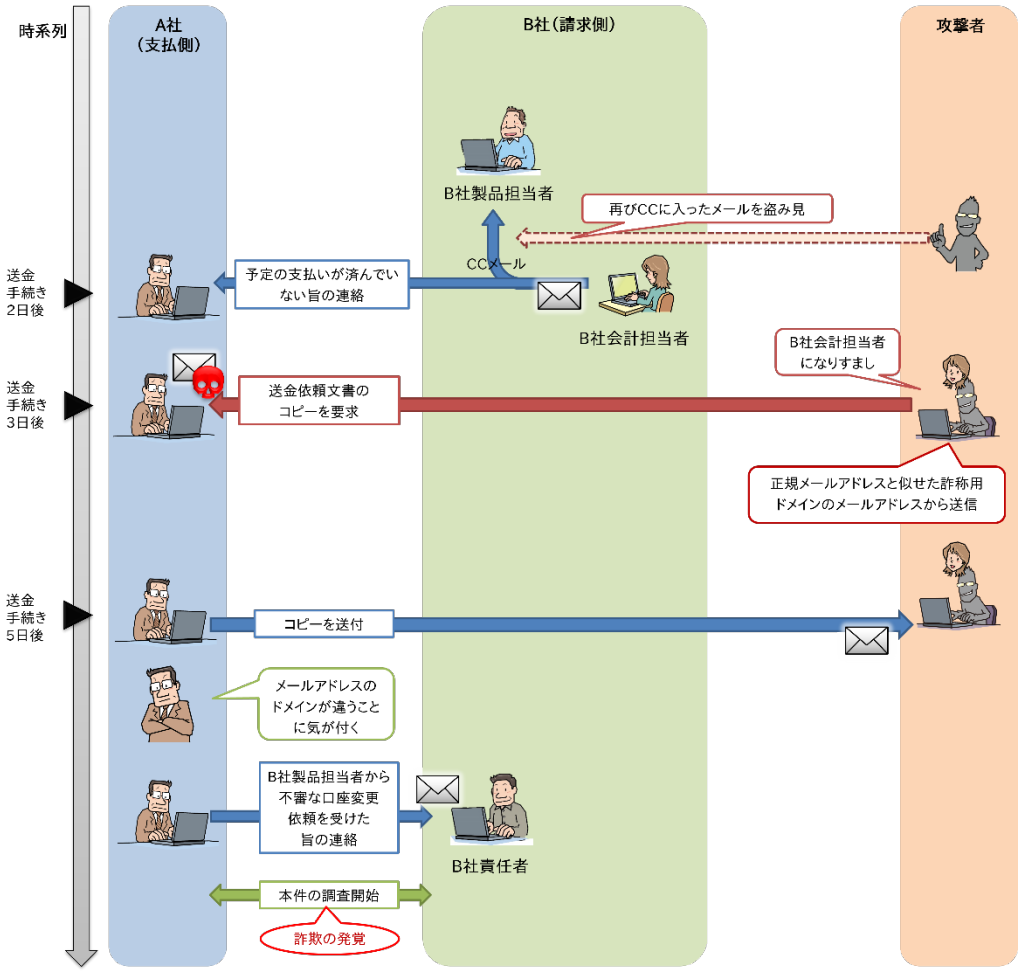

図 9 送金後のやりとりの流れ

攻撃者の口座への送金手続き完了から 2 日後、B 社会計担当者から A 社担当者宛てに、予定されていた支払いが行われていない、という問い合わせのメールが送付されました。このメールは、日本時間で金曜日の午後 6 時頃に届いていました。

すると、翌土曜日の午前 2 時頃、攻撃者は B 社会計担当者のメールアドレスと似せた図 3 の詐称用ドメインのメールアドレスを使って B 社会計担当者になりすまし、正規の B 社会計担当者のメールの返信から作成したように装ったメールを A 社担当者に送信しました。メールの内容は、送金手続きが済んでいることを確認するために銀行への送金依頼文書のコピーを送付してほしい、というものでした。これには、A 社担当者が正規の B 社会計担当者からのメールに返信することで、正規の B 社関係者にメールが着信し、詐欺の発覚に至ることを

避ける狙いがあったものと推測されます。

A 社担当者は翌月曜日の午前 8 時頃、攻撃者からのメールに返信しました。メールの内容は、B 社製品担当者からの予定日直前での送金先変更により支払いが遅延しているが、送金処理は手配済みである、という旨を連絡するとともに、要求された文書のコピーを添付にて送付するものでした。

ここで行われたやりとりのイメージを図 10 に示します。

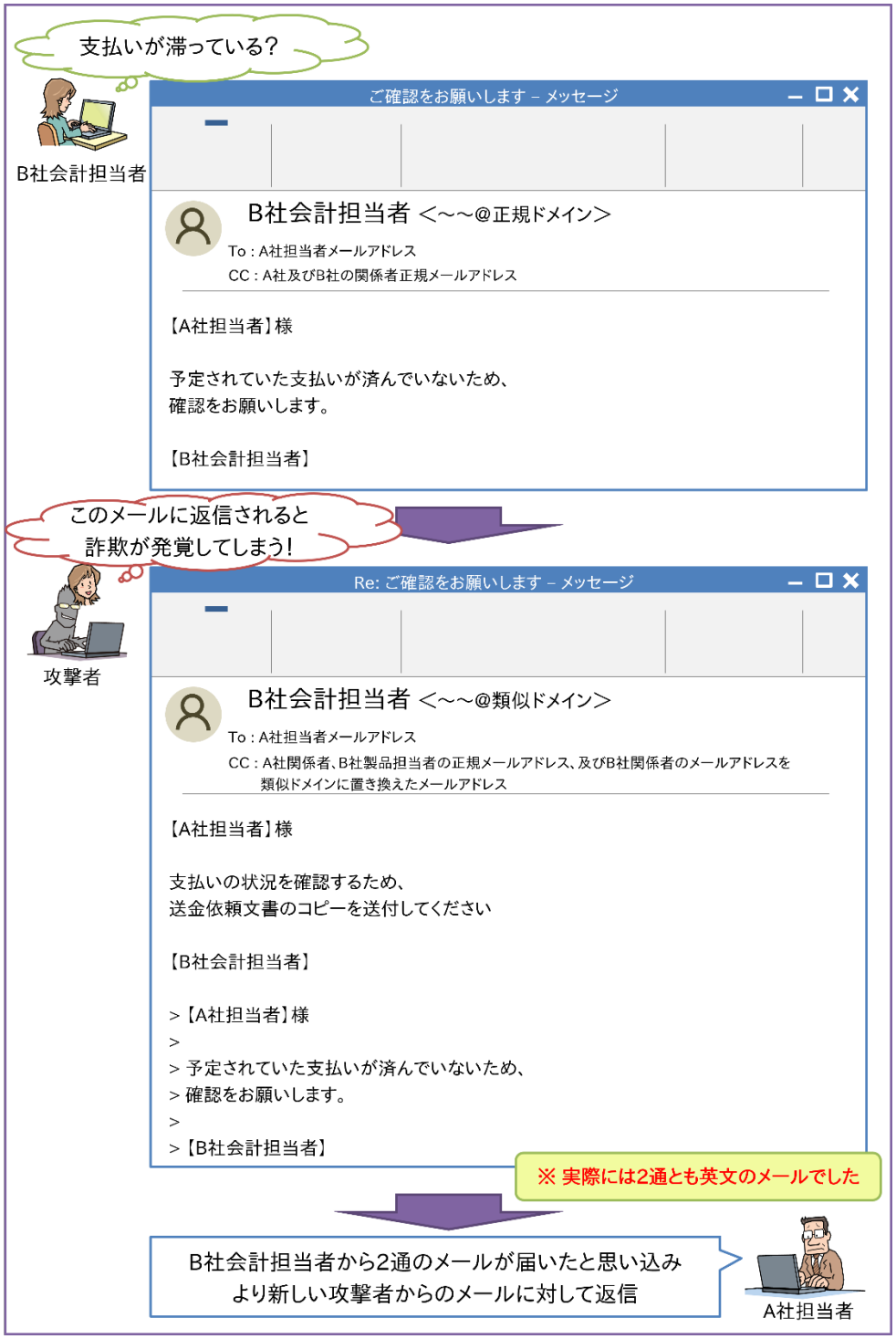

図 10 送金後のメールのやりとりのイメージ

このメールの送付後、A 社担当者は相手のメールアドレスが正規のものでないことに気が付き、B 社責任者に連絡をとるとともに調査を開始し、詐欺被害を受けたことが発覚しました。

3. 攻撃の手口

本事例の攻撃手口について、次の 3 つを説明します。

- 正規メールアカウントからの偽メール送信
- 支払日直前での口座変更依頼
- 詐欺発覚を遅らせるための偽メール送信

3.1. 正規メールアカウントからの偽メール送信

本事例では、攻撃者が B 社製品担当者のメールアカウントを乗っ取って、B 社製品担当者の正規のメールアカウントから A 社担当者にメールを送信していたとみられ、メールの配送経路も A 社 B 社間の正規メールと同様の経路を辿っていました。

B 社製品担当者が、自身のメールアカウントが乗っ取られて不正にメール送信されていることに気付かなかった理由は不明ながら、不審なメールが B 社製品担当者の目に入らないよう、攻撃者が何らかの細工をしていた可能性があります。考えられる細工の手口としては、メールボックスに不正な転送・削除ルール設定を行うものなどが挙げられます。また、IPA のサイバー情報共有イニシアティブ（J-CSIP）の運用状況 [2023 年 10 月～12 月][3]に記載のあるように、メールの仕分けルールを悪用して、攻撃者から送ったメールの返信メールを通常の受信トレイから Microsoft Outlook の RSS フィードフォルダのような利用者が普段確認しないフォルダに移動させる手口が使用されたことも可能性の一つとして考えられます。

3.2. 支払日直前での口座変更依頼

攻撃者は、最初のメールで支払い予定日を確認した後、立て続けに口座変更依頼を行うのではなく、支払日が残り 1 週間と迫ってから口座変更依頼メールを送信してきました。ここから、攻撃者が意図的に支払日直前で口座変更依頼を行ってきたことが推測されます。

これには、残り時間が短い中で依頼をすることで標的の人物に対応を急がせ、正当な依頼であるかの確認に十分な時間を与えないことで、詐欺発覚の可能性を低減させる狙いがあったと推測されます。

---

[3] IPA：サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）
サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 10 月～12 月]
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q3-report.pdf

3.3. 詐欺発覚を遅らせるための偽メール送信

本事例では、攻撃者指定の口座への送金処理から数日後、B 社会計担当者から A 社担当者に、予定されていた送金が行われていないことについて確認するメールが送付されました。このメールの送付先は、全て A 社及び B 社の正規関係者のメールアドレスとしていましたが、攻撃者は B 社製品担当者のメールアカウントへの不正アクセスに成功していたために、そのメールの内容を盗み見ることが可能な状況でした。

攻撃者はそのメール送信から半日足らずで、B 社会計担当者のメールアドレスに似せた詐称用ドメインのメールアドレスから A 社担当者にメールを送信しました。メールの内容は送金依頼文書のコピーを送付してほしい、というものであり、送信先に含まれる B 社関係者のメールアドレスは、B 社製品担当者のもの以外は詐称用ドメインのものに置き換えられていました。なお、このメールは、直前に送付された B 社会計担当者から A 社担当者へのメールの返信から作成したよう装われていました。

これらのメールを確認した A 社担当者は、B 社会計担当者から 2 通のメールが着信したものと思い込み、より新しく着信した攻撃者からのメールに対して返信をしてしまいました。

これら 2 通のメールを受信した場合の、一般的なメーラー上での表示イメージを図 11 に示します。

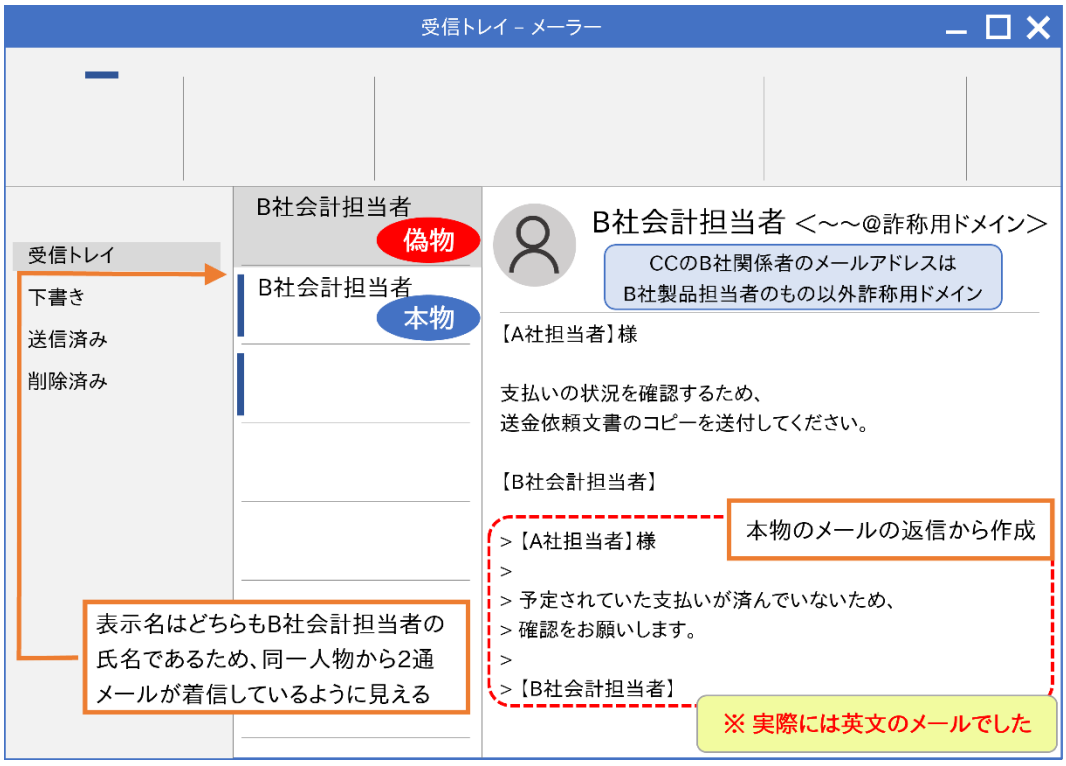

図 11 メーラー上での表示のイメージ

図 11 の通り、2 通のメールで同じ送信元の表示名を設定していた場合、メーラー上では、同一人物から着信しているようかのように見えてしまいます。また、一般的なメールのやりとりでは、相手から送られてきた最新のメールに対して返信メールを作成することが多いことから、A 社担当者からのメールに重ねて送付することで、偽のメールにのみ返信させる狙いがあったと考えられます。これにより、A 社担当者からの返信メールが B 社の正規関係者の元に着信しないようにすることで、詐欺の発覚を少しでも遅らせる意図があったと推測されます。

4. まとめ

本事例は、「取引先との請求書の偽装」のタイプのビジネスメール詐欺が行われたものでした。このタイプのビジネスメール詐欺では、攻撃者が事前に何らかの方法で正規のメールのやりとりを盗み見た上で、標的の人物に違和感を与えないような巧妙な詐欺メールを送付するケースが多く、IPA でも類似の事例を複数確認しています。

また、本事例で使われた攻撃の手口から、常習的にビジネスメール詐欺を行っている人物による犯行の可能性も考えられ、標的とされた人物が詐欺であることに気付くことは非常に困難であったと推測されます。このため、急な振込先や決済手段の変更が発生した際には、取引先にメール以外の方法で確認をとるなど、送金に係る社内規定やチェック体制の整備や見直しが重要となります。

なお、本レポートで紹介した手口以外にも、攻撃者がなりすまし対象の所属組織内での口座変更に係るやりとりのメールを偽造し、組織内で調整済みの口座変更依頼であるかのように見せかけたメールを標的に送信するなどといった、非常に悪質な手口も確認しています。さらに、昨今のビジネスメール詐欺に係る報道では、メールだけでなく、ディープフェイクを悪用して、声色や容姿を似せた電話やビデオ通話を併用する手口も報じられており [4]、標的とされた人物が個人で詐欺を見抜くことがより困難な状況になっていると考えられます。

このため、「ビジネスメール詐欺（BEC）対策特設ページ」の「ビジネスメール詐欺（BEC）の特徴と対策」[5]等をご参照いただき、組織全体でビジネスメール詐欺対策に取り組むことを強く勧めます。

－以上

[4] Cable News Network.：Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’
https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[5] IPA：ビジネスメール詐欺（BEC）対策特設ページ
ビジネスメール詐欺（BEC）の特徴と対策
https://www.ipa.go.jp/security/bec/hjuojm0000003cg1-att/000102392.pdf