ビジネスメール詐欺（BEC）の詳細事例４

～銀行と協力し、偽口座への送金を防げた事例～

2022 年 12 月 26 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、2021 年 4 月に、日本国内の製造業の企業（A 社：請求側）と、中国の企業（B 社：支払側）との間で取引が行われる中、A 社の担当者になりすました攻撃者から B 社へ、送金先銀行の変更を要求する偽のメールが送られたものです。この際、A 社が事前に指定していた正規の送金先銀行の口座について、税務監査で利用できなくなった、という偽の理由が使われました。

B 社の担当者は、振込先の変更に加え、変更後の請求書に記載されていた銀行口座の名義が変更されていたことに疑念を抱いたため、偽の銀行口座へ送金手続きをする際、銀行口座の名義については変更しませんでした。その後、B 社の担当者が、送金の証明として送金依頼書の写しを攻撃者に送信したところ、攻撃者から「銀行口座の名義が誤っている」という旨のメールが届きました。これを受けて、B 社担当者は銀行口座の名義の変更について、A 社に直接電話して事実確認を行い、本件が詐欺であることが発覚しました。

すぐに A 社が偽の送金先銀行へ通報を行ったところ、攻撃者が指定した銀行口座への振込が実施される前であったこと、および銀行口座の名義が一致していなかったことから、送金が停止・返金され、金銭的な被害には至りませんでした。ただし、数時間の対応の遅れで実害が生じていた可能性があり、A 社では送金プロセスのチェック等の対策の強化を行ったとのことです。

今回の事例でやり取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

本事例は 2021 年 5 月 7 日に、A 社から IPA に対し、原因の調査方法や連絡すべき通報先等について相談がありました。その中で、攻撃者と B 社の間で行われた複数回のメールのうち、攻撃者から送られたメールについての情報提供を受けて、IPA で確認を行いました。

1.2. 本事例の関係者

本事例の関係者を次に示します。

表 1 本事例の関係者一覧

名前	説明
A 社	日本国内の製造業の企業。請求側。
A 社担当者	A 社の担当者。B 社担当者と取引に係るやり取りを行っていた。
B 社	中国の企業。支払側。
B 社担当者	B 社の担当者。A 社担当者になりすました攻撃者とメールでやり取りを行った。
攻撃者	A 社担当者になりすまし、ビジネスメール詐欺によって B 社から金銭を詐取しようとした。
正規の送金先銀行	A 社の正規の口座が存在し、振込先として指定していた、日本国内にある銀行。
偽口座のある送金先銀行	攻撃者が指定した偽の口座が存在する、日本国内にある銀行。
A 社のメインバンク	A 社に代わり、偽口座のある送金先銀行への情報連絡を行った。
警察	日本の警察。

本事例については、次の 2 つの構成で説明します。また、本事例で使われた攻撃の手口について 4 章で説明します。

- 攻撃者の介入から詐欺が発覚するまでのやり取り
- 詐欺発覚後の対応

2. 攻撃者の介入から詐欺が発覚するまでのやり取り

本件において、攻撃者の介入から詐欺が発覚するまでのやり取りの概要（図 1）について、次に示します。

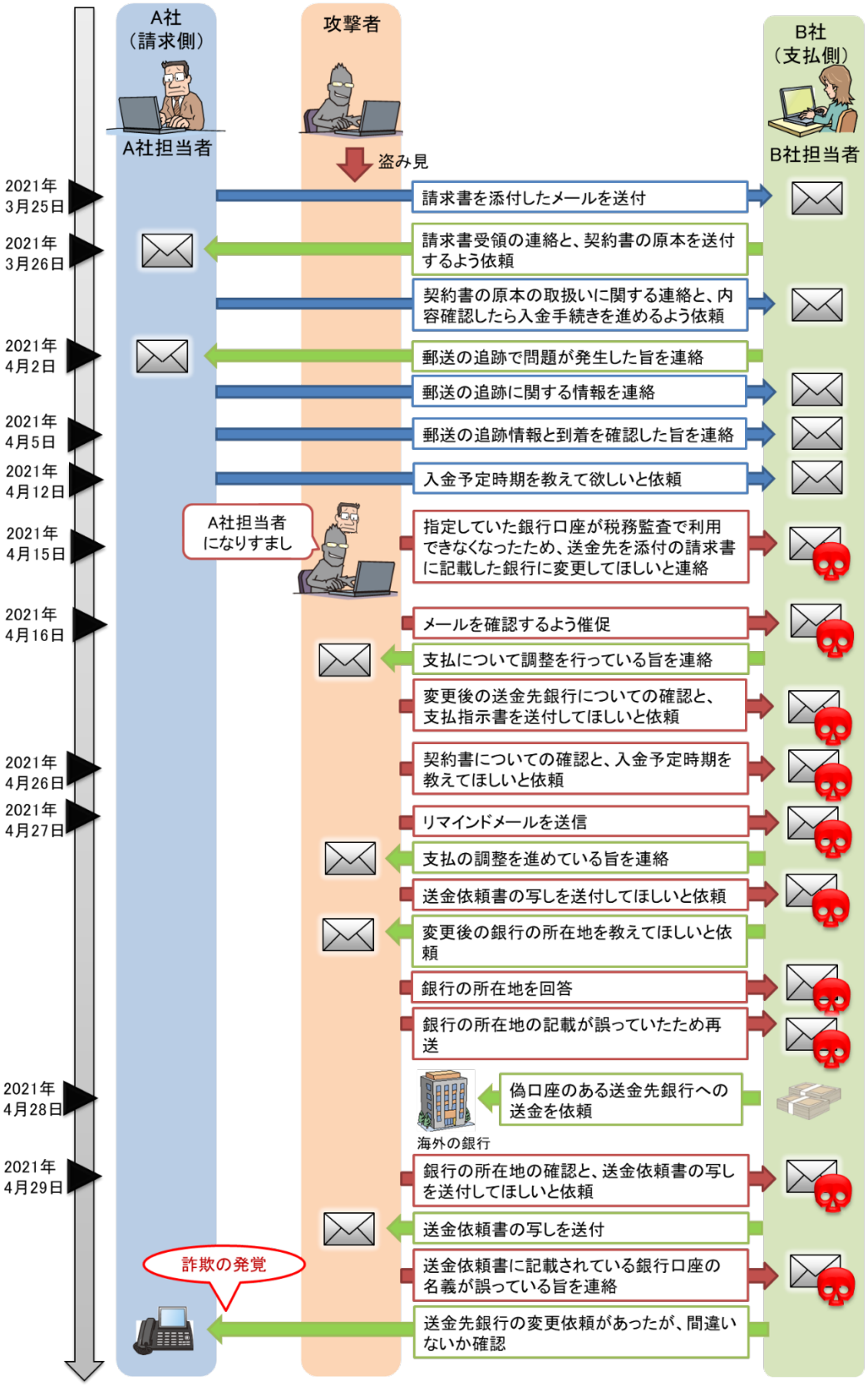

図 1　　攻撃者の介入から詐欺が発覚するまでのやり取り

2021 年 4 月 15 日、A 社の担当者になりすました攻撃者から、B 社の担当者に、偽メールが着信しました（図 2）。その偽メールには、A 社が事前に指定していた正規の送金先銀行の口座について、税務監査で利用できなくなったこと、そのため送金先を変更したいという旨と、変更後の口座の情報を記載した請求書が添付されていました。この偽の送金先には、日本国内の銀行（以降、「偽口座のある送金先銀行」）が指定されており、また、偽メールの後半部分には、直前にやり取りした本物のメールが引用されていました。

攻撃者は、最初の偽メールが着信した 4 月 15 日の前から、A 社と B 社間でやり取りしていた取引に関するメールを何らかの方法によって盗み見ていたと考えられますが、その方法については明らかになっていません。

このメールを発端として、B 社の担当者と攻撃者の間で複数回のメールのやり取りが行われ、最終的に偽の銀行口座への送金に至っています。

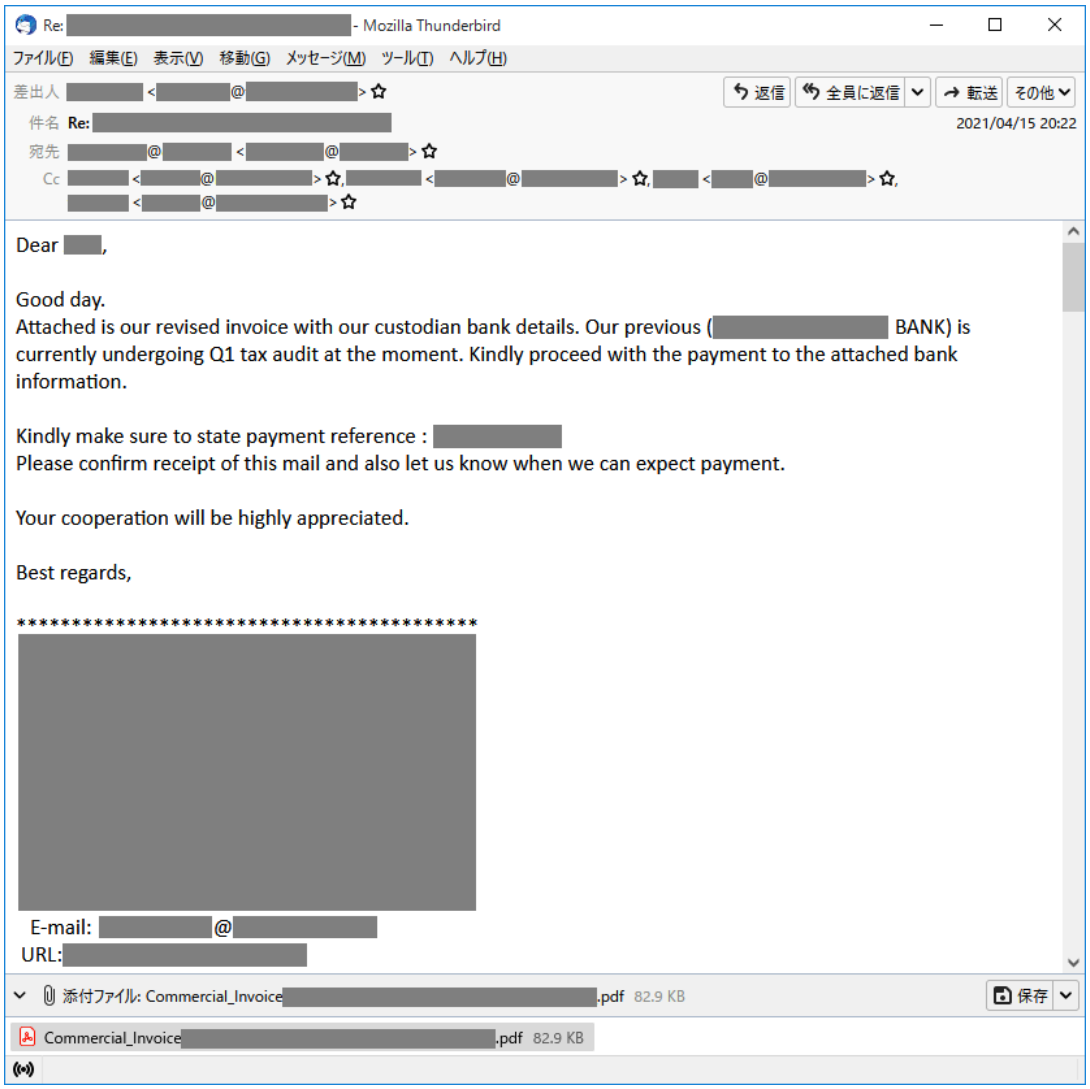

図 2 攻撃者からのメール（2021 年 4 月 15 日 20:22）

翌日の 4 月 16 日、B 社の担当者に対して、送信したメールの確認を催促するメールが送られてきました（図 3）。

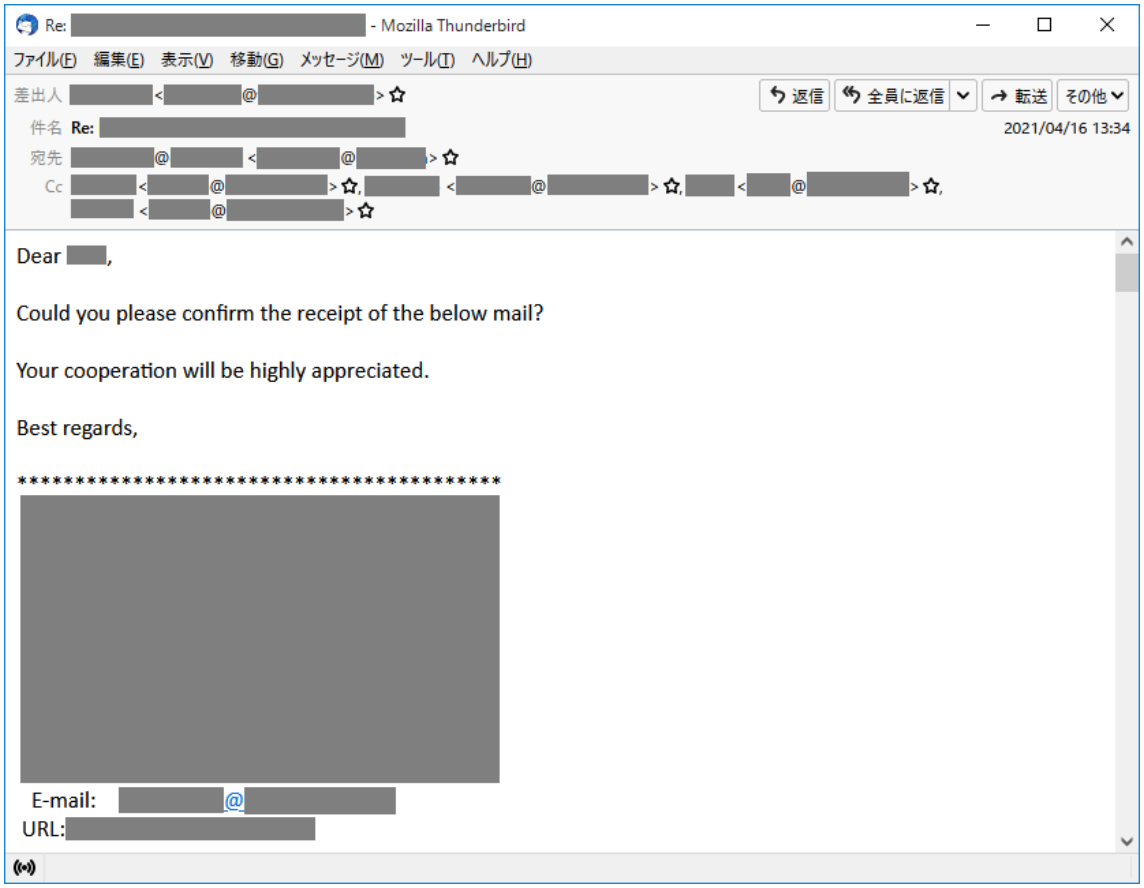

図 3 攻撃者からのメール（2021 年 4 月 16 日 13:34）

このメールに対し、B 社の担当者が「支払い手続きの調整を行っている」という旨のメールを返信したところ、攻撃者より、「変更後の送金先の詳細は確認したか。請求書の支払期限は 10 日以内に予定されている」、「手続きが進んだら支払指示書を送付してほしい」と、支払いを促す旨のメールが送られてきました（図 4）

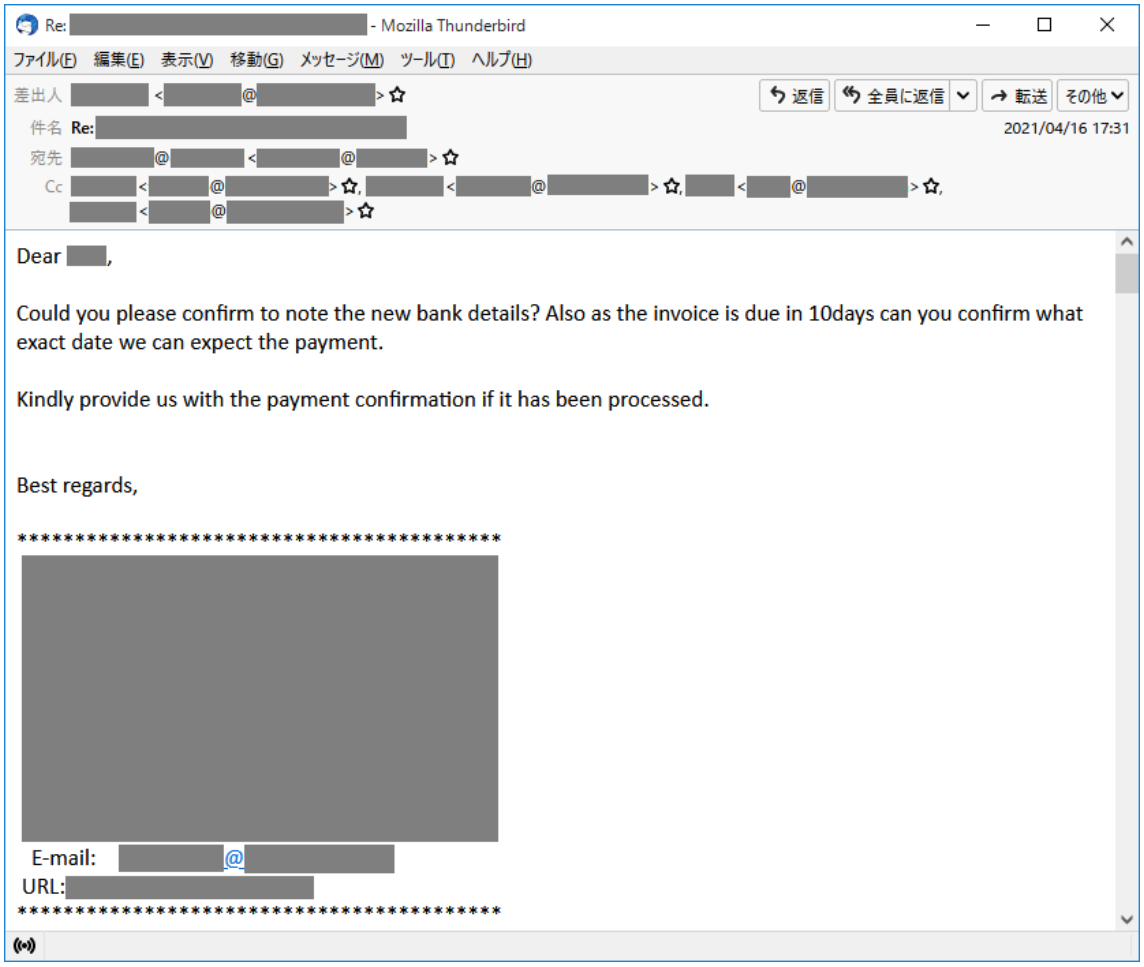

図 4 攻撃者からのメール（2021 年 4 月 16 日 17:31）

4 月 26 日、攻撃者から「契約書は受け取れているか。支払い手続きを進めている場合は知らせてほしい」という旨のメールが送られてきました（図 5）

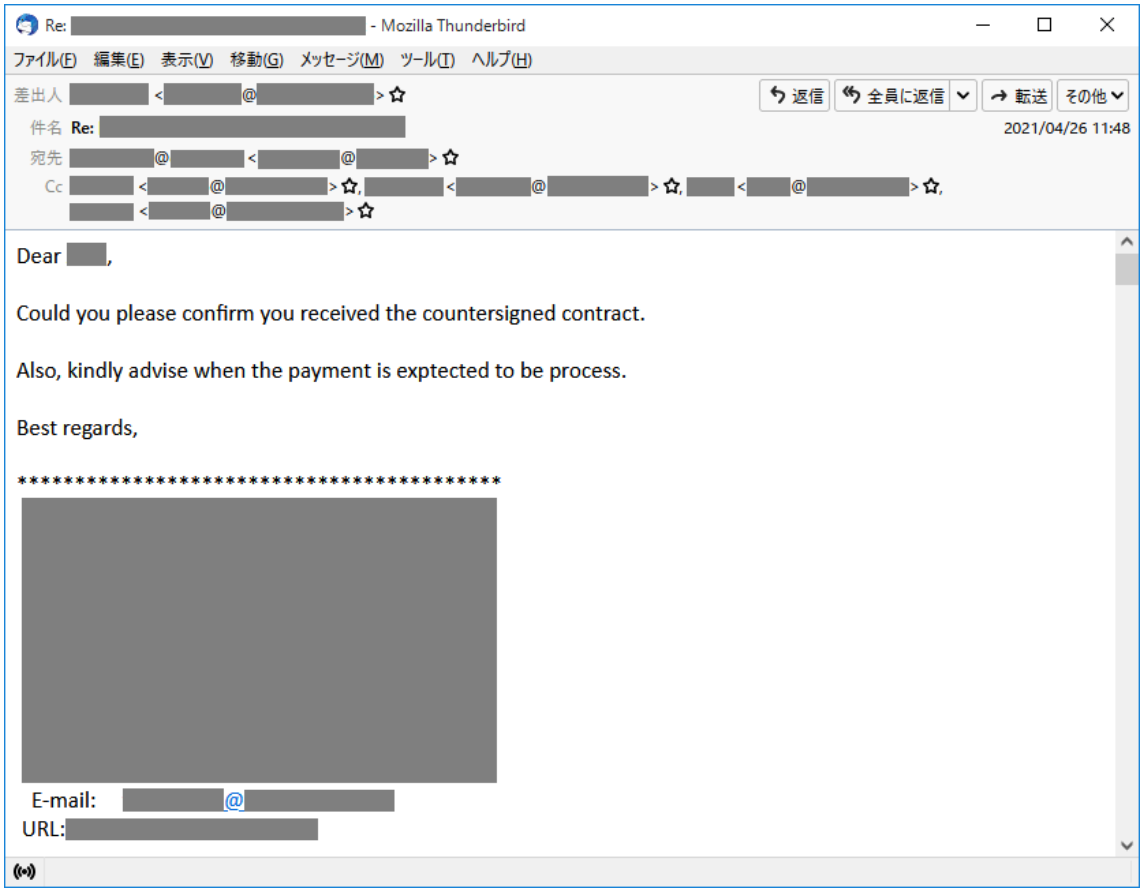

図 5 攻撃者からのメール（2021 年 4 月 26 日 11:48）

翌日の 4 月 27 日、攻撃者は重ねてリマインドのメールを送り、B 社の担当者に昨日のメールを確認するよう催促しています（図 6）。

このメールから、メール本文の署名に記載されていた、A 社担当者のメールアドレスと A 社の会社 URL 等が削除されていました。これは署名に記載されたメールアドレスと URL のドメイン情報から、ヘッダに設定している偽のメールアドレスを気づかせないようにする目的があったものと考えられます。

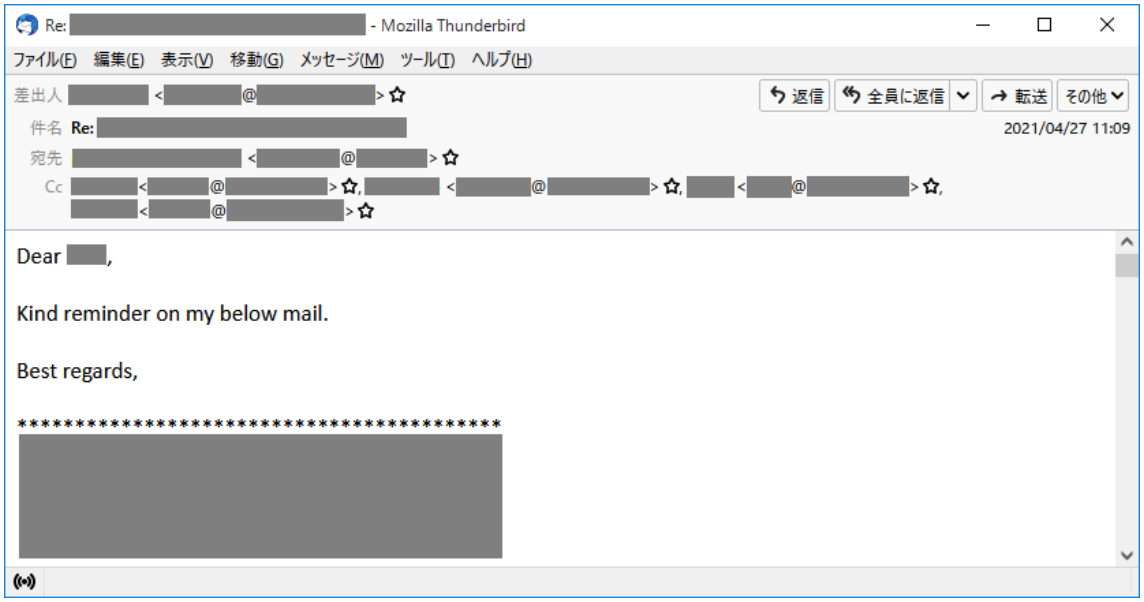

図 6 攻撃者からのメール（2021 年 4 月 27 日 11:09）

このメールに対し、B 社の担当者が「支払い手続きを進めているが、5 月中旬までかかる見込みである」という旨のメールを返信したところ、攻撃者より「送金依頼書の写しを送付してほしい」という旨のメールが送られてきました（図 7）。

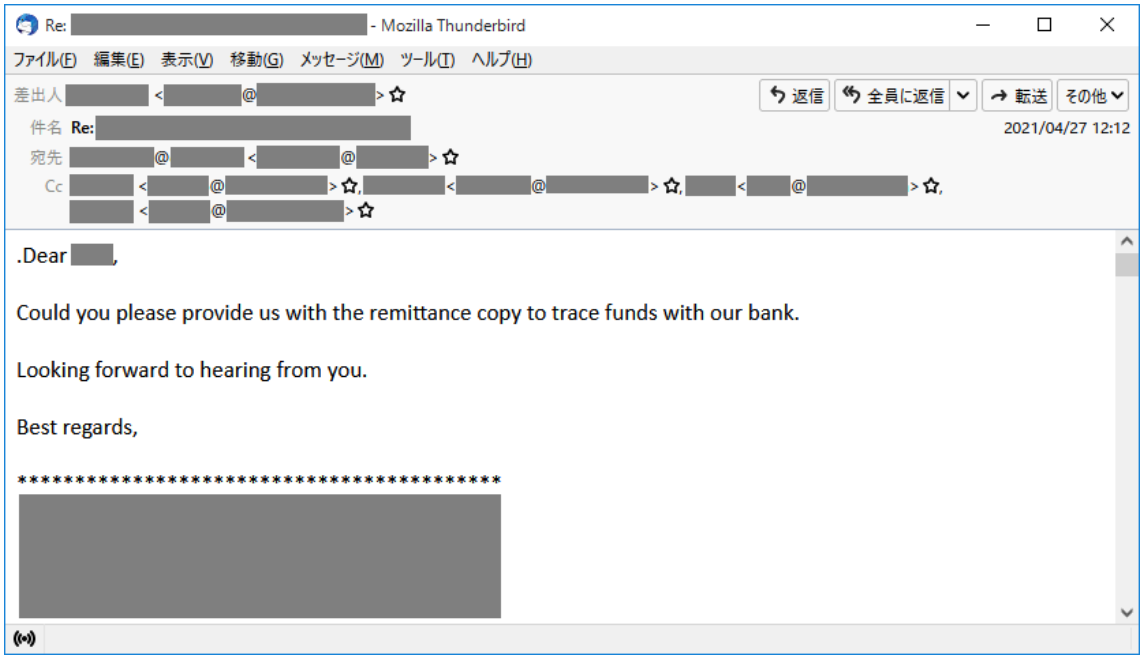

図 7 攻撃者からのメール（2021 年 4 月 27 日 12:12）

このメールに対し、B 社の担当者は「送金のため、変更後の銀行の所在地の情報が必要である」という旨のメールを返信したところ、攻撃者より、送金先銀行の所在地の情報が記載されたメールが送られてきました（図 8）。

なお、当該メールは攻撃者がミスしたものとみられ、攻撃者が用意した偽の請求書にも記載されていない、別の銀行の情報が書かれていました。攻撃者は複数の詐欺を並行して行っていたか、本件のような偽口座を複数保持している可能性が伺えます。

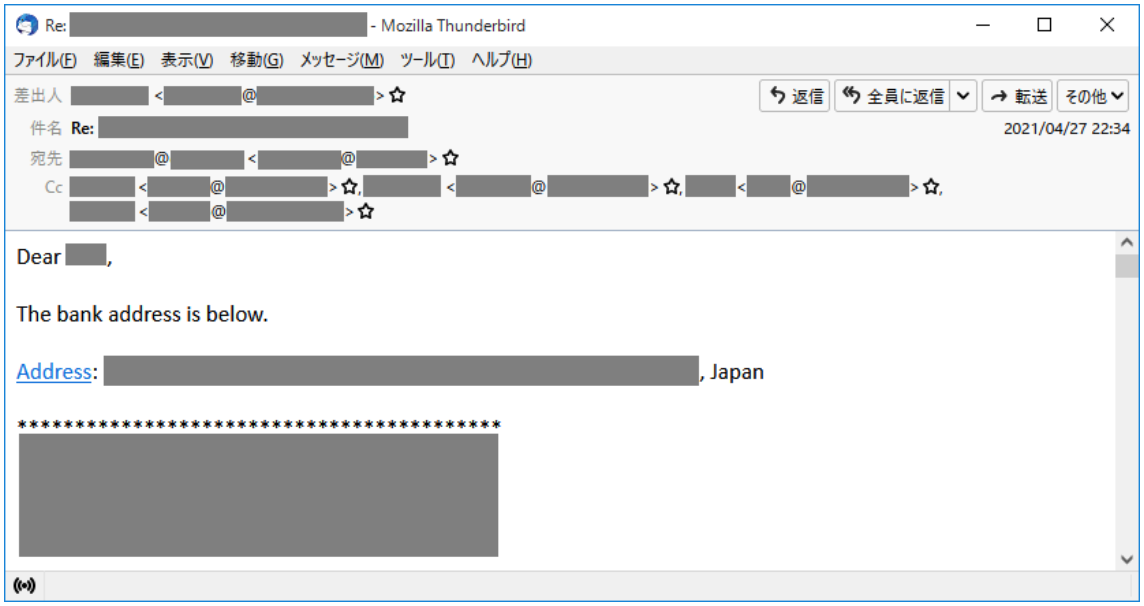

図 8 攻撃者からのメール（2021 年 4 月 27 日 22:34）

攻撃者は、送信したメールの内容が誤っていることに気づき、約 1 時間後、B 社の担当者に対し、メールを再送してきました（図 9）。当該メールには、偽の請求書の内容と対応する、偽口座のある送金先銀行の正しい情報が書かれていました。

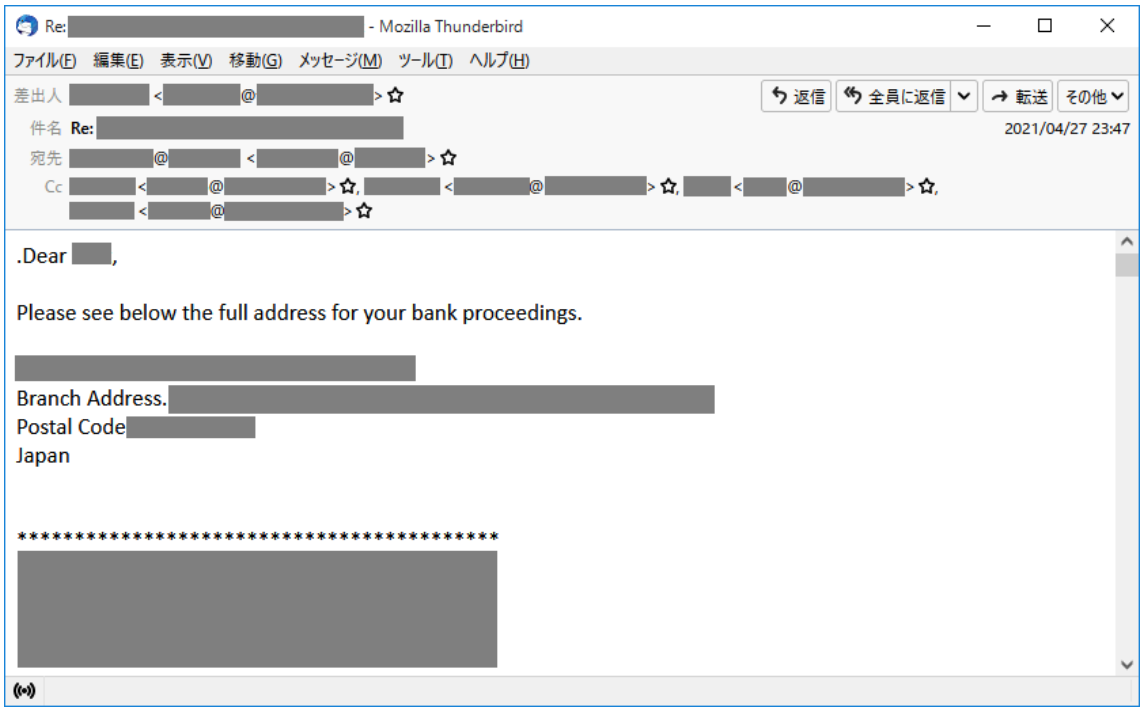

図 9 攻撃者からのメール（2021 年 4 月 27 日 23:47）

翌日の 4 月 28 日、B 社の担当者は、攻撃者が指定した偽口座のある送金先銀行へと送金する手続きを行ってしまいました。なお、B 社の担当者は送金する際、銀行名や口座番号等は指定された内容へと変更しましたが、銀行口座の名義については、A 社とは異なるものへと変更することに疑念を持っていたため、変更せずに送金を実施したとのことです。

更に翌日の 4 月 29 日、攻撃者から再び「送金依頼書の写しを送付してほしい」という旨のメールが送られてきました（図 10）。

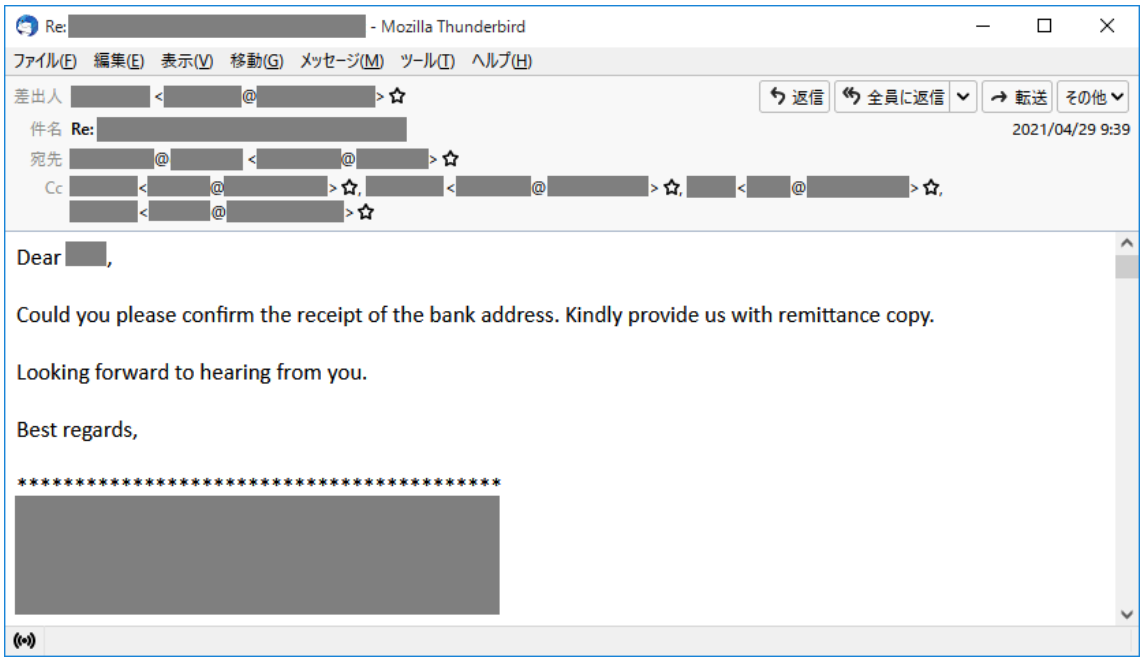

図 10 攻撃者からのメール（2021 年 4 月 29 日 9:39）

これに対し、B 社が送金依頼書の写しを送付したところ、攻撃者から「銀行口座の名義が誤っている」という旨と、偽口座のある送金先銀行の情報がもう一度記載されたメールが送られてきました（図 11）。これは、先に述べた通り、B 社が意図的に名義を本物の A 社のものから変更していなかったためですが、攻撃者は、この名義違いにより送金が失敗することを恐れたものと思われます。

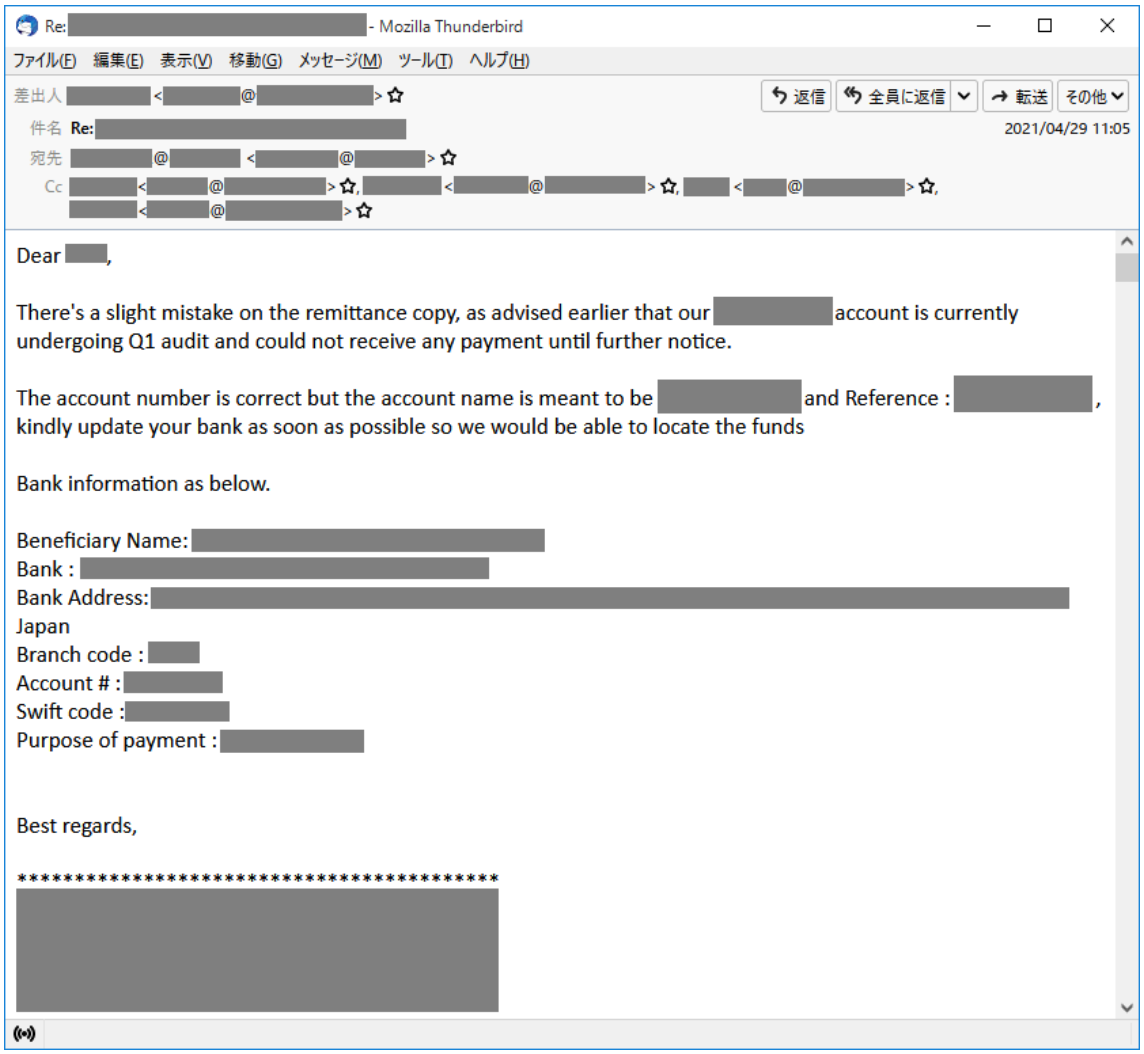

図 11 攻撃者からのメール（2021 年 4 月 29 日 11:05）

ここで B 社は、指定された銀行口座の名義が A 社と関係のない組織名となっていることに疑念を持っていたため、A 社に電話し、送金先銀行の変更依頼に間違いがないか事実確認を行ったところ、本件がビジネスメール詐欺であることが発覚しました。

本件は 4 月 28 日時点で送金手続きを行っていましたが、偽の銀行口座への振込処理が行われる前に A 社が迅速に通報等の対応を行ったため、最終的には金銭的な被害を回避することができました。

3. 詐欺発覚後の対応

本事例において、ビジネスメール詐欺が発覚してから、偽口座のある送金先銀行で返金処理が行われるまでの対応の流れ(図 12)について、次に示します。最終的に送金先から返金されるか否かは事例により異なりますが、送金してしまった後に金銭を取り戻すことができた一つの例として参考にしてください。なお、本件は、偽の送金先として国内の銀行が指定されていたため、返金処理に係る対応のほとんどは国内で行われました。

A 社は、B 社からの電話連絡によって詐欺を把握した後、偽口座のある送金先銀行に対し、振込処理の停止の要請をしました。これに対し、当該銀行から「警察からの連絡がないと対応ができない」との回答があったため、A 社は警察への通報と被害届の提出、さらに A 社のメインバンクを介しての情報連絡を行いました。これと並行し、A 社は親会社の IT 部門等に協力を依頼して、原因調査を進めるとともに、IPA へ連絡・相談しました。

結果としては、A 社は詐欺の被害者本人ではないため、警察への被害届は受理されない形となりましたが、A 社からの偽口座のある送金先銀行に対する通報や、A 社のメインバンクからの情報連絡等によって、偽口座のある送金先銀行が、本件を振込先の名義不一致を理由に振込処理を停止させる判断をした、とのことでした。また、同日中に B 社への返金対応も行われたとのことです。

本件は、B 社の担当者が攻撃者に騙され、送金まで行ってしまった事例であり、数時間の対応の遅れで、偽の銀行口座への振込処理が行われ、攻撃者に金銭を引き出されていた可能性もありました。しかし、B 社からの電話連絡があって、はじめて状況を把握した A 社が、ビジネスメール詐欺であることを認識し、すぐに対応を開始したことで、B 社の被害を回避することが出来ました。本件のように、即座に通報等の対応を行うことが被害の防止につながる場合もありますので、予め組織内外を含めた連絡体制の整備や、このような詐欺の発生時の対応フローの策定等をしておくことが重要です。

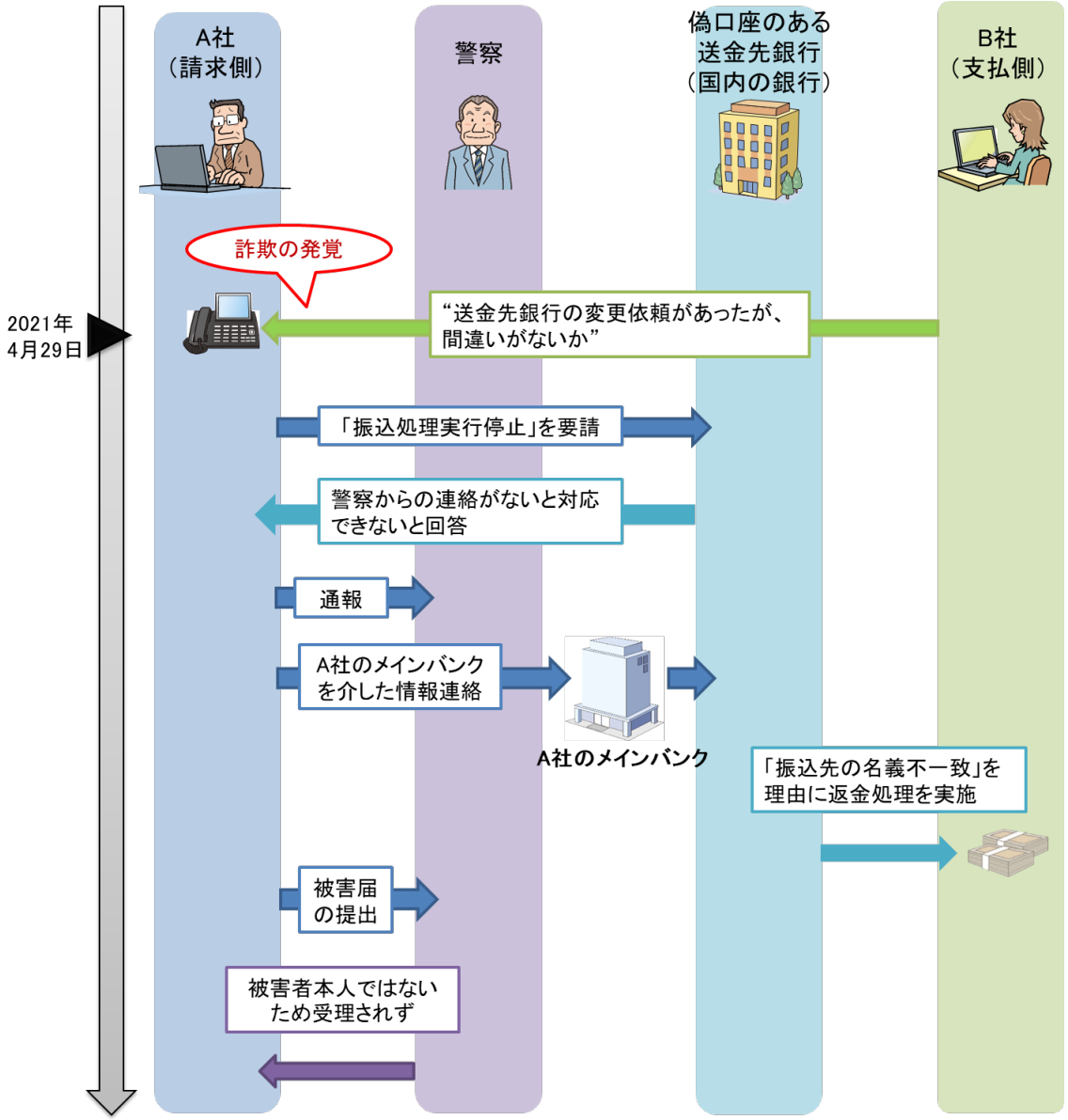

図 12 詐欺発覚後の対応の流れ

4. 本事例の攻撃手口

本事例では、次の攻撃の手口が使われました。

- 税務調査や監査を理由とした送金先の変更
- 正規メールの悪用
- 詐称用メールアドレスの使用
- 請求書の偽造

これらは、これまでに確認されているビジネスメール詐欺でも多く使われる手口です。

4.1. 税務調査や監査を理由とした送金先の変更

本事例では、攻撃者がＢ社の担当者に対し、正規の送金先銀行の口座が税務監査で利用できなくなったという偽の理由を示してきました。

攻撃者が別の口座への送金を依頼する際、銀行口座が税務調査や監査を受けているという偽の理由を示してくるのは、これまでIPAが確認してきたビジネスメール詐欺の事例においても、多く確認されている手口です。

4.2. 正規メールの悪用

攻撃者が最初に送ってきたメールは、本物のＡ社の担当者とＢ社の担当者がやり取りしていた正規メールを引用したものでした。本物のメールへの返信を装うことで、Ｂ社の担当者に偽のメールであることに気づかれないようにする意図があったものと考えられます。

4.3. 詐称用メールアドレスの使用

本事例では、攻撃者が偽のメールを送る際、差出人(From)と同報先(CC)のメールアドレスに、詐称用ドメインを設定していました。この詐称用ドメインには、A 社の正規のドメインに似通ったものと、本取引の受注活動時から関与していたA社の中国にある現地代理店の正規のドメインに似通ったものの 2 つの詐称用ドメインが使われていました[1]。

この詐称用ドメインは、どちらも次の例に示す形式のドメインであり、どちらも同じ日に取得されていました。

【本物のメールアドレス】alice @●●● . co . jp
【偽物のメールアドレス】alice @●●● **－jp . co** →「.」を「－」へと変更
「co」と「jp」を入れ替え

※説明のための例であり、実際に悪用されたメールアドレスとは異なる。

4.4. 請求書の偽造

詐欺の発生前にA社とB社間で交わした正規の請求書と、攻撃者によって偽造されて送られてきた請求書を比較したところ、請求書内の送金先に係る箇所のみが改変されていました(図 13)。A 社が指定していた正規の送金先銀行の箇所は、偽口座のある送金先銀行へと書き替えられ、銀行口座の名義については、A 社の社名から A 社とは異なる組織のものへと書き替えられていました。この書き替えられた箇所は、既存の文字フォントとは異なっていました。

また、攻撃者は、PDF で作成された正規の請求書をもとに偽の請求書を作成する際、「RAD PDF」と呼ばれる PDF の編集ツールを利用していました。当該ツールはビジネスメール詐欺の過程で攻撃者が使用することが多く[2]、IPA で確認している他の事例においても当該ツールが使われていたことを確認しています。なお、当該サービスを利用して作られているからといって、必ずしも悪意のある PDF ファイルというわけではありません。

---

1 本メールの同報先(CC)には、A 社担当者とは別の A 社の担当者のメールアドレスと、A 社の中国現地代理店のメールアドレスが設定されており、どちらのメールアドレスも偽の詐称用ドメインであった。

2 APWG Q1 2021 Report
https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

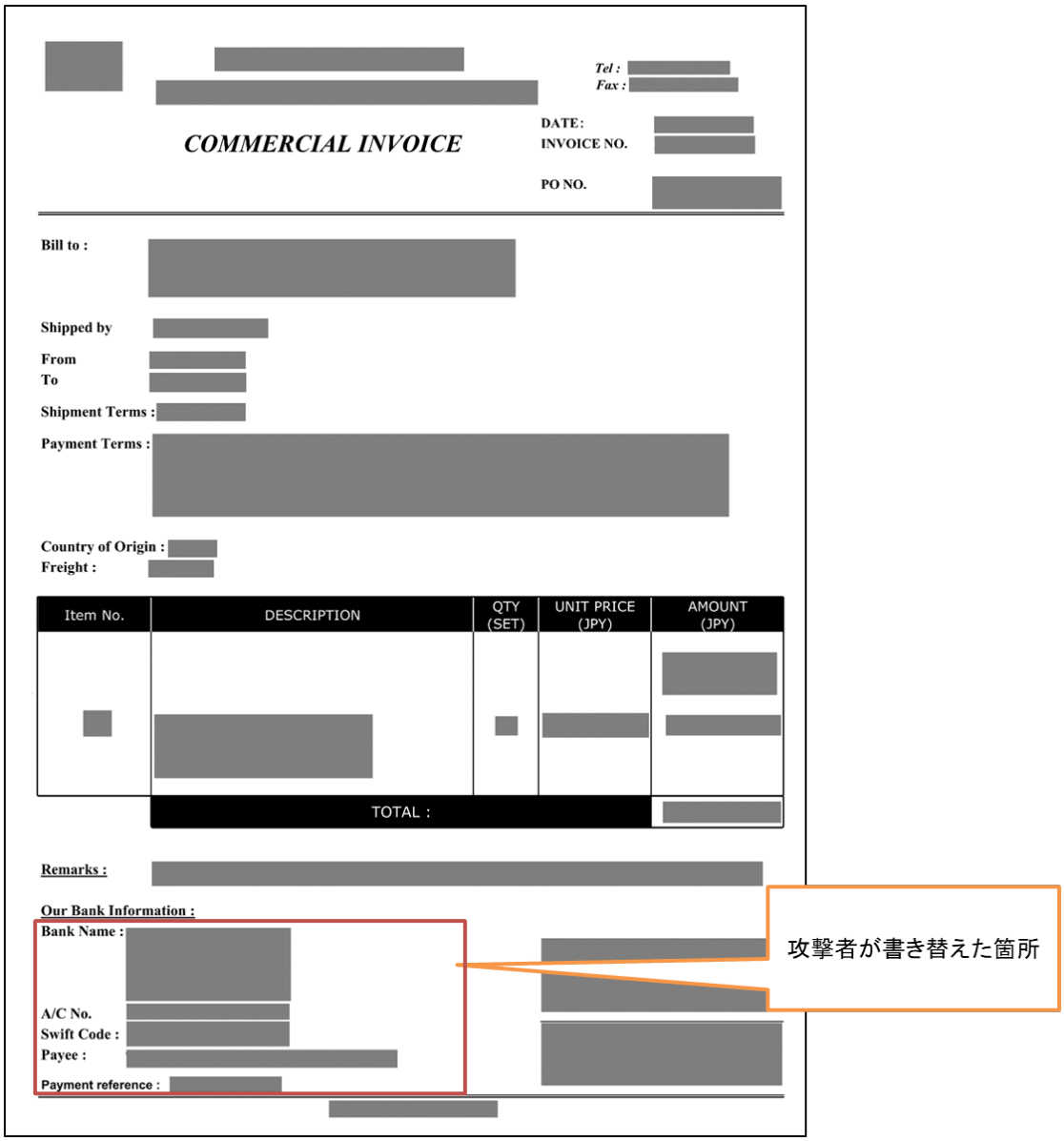

図 13 偽造された請求書

以上