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～

2022 年 11 月 29 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 2 月から 4 月にかけて、国内組織の海外関連企業（A 社：支払側）と、アメリカの運送企業（B 社：請求側）との間で取引を行っている中、B 社の担当者になりすました攻撃者から、偽の口座への振込を要求するメールが送られたものです。口座変更の（嘘の）理由は、新型コロナウイルスの影響とのことでした。

これまでの A 社と B 社の正規の取引は、小切手で支払いを行う形態でした。2021 年 2 月、攻撃者から A 社へ、支払方法について口座振込へ変更を依頼する内容のメールが送られ、A 社の担当者は攻撃者に騙され、偽の振込先へ送金を行ってしまいました。その後、3 月に再度攻撃者から別の振込先の指示が A 社へ送られ、被害に気付くまでの期間、3 月と 4 月にも続けて送金を行ってしまいました。5 月に入って、振込がないことについて B 社から A 社へ問い合わせがあり、本件が発覚しました。

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、2021 年 6 月 4 日、J-CSIP の参加組織から情報提供がありました。

攻撃者と A 社の間では複数回のメールのやりとりが行われていた中、そのうち一部の攻撃者からのメールについて情報提供され、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	国内組織の海外関連企業。支払側。
A 社担当者	A 社の担当者。本事案で攻撃者から偽メールを送り付けられた。
B 社	アメリカの運送企業。請求側。
B 社担当者	B 社の担当者。A 社担当者と最初に取引に係るやりとりを行っていた。
攻撃者	B 社の担当者になりすまし、ビジネスメール詐欺によって A 社から金銭を詐取した。

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。

- 口座変更に係る攻撃者とのやりとり
- 詐欺の発覚までに時間がかかった要因

2.　口座変更に係る攻撃者とのやりとり

2021 年 2 月～4 月に発生した、攻撃者からの口座変更に係る偽メールのやりとりと、偽口座への送金の概要（図 1）について次に示します。

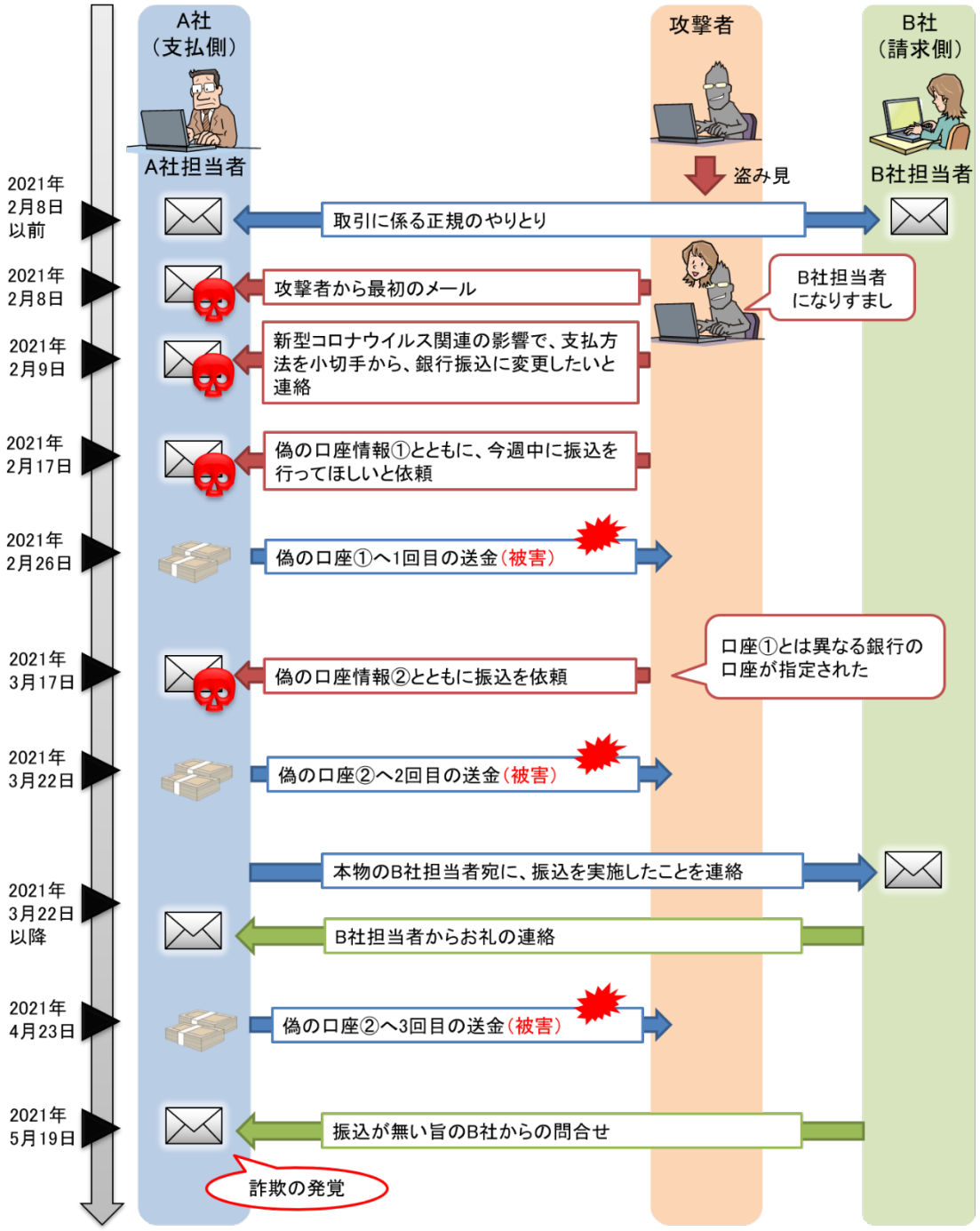


図 1 攻撃者とのやりとり

2021 年 2 月 8 日、A 社担当者宛に攻撃者からの最初のメールが着信しました。その翌日（2 月 9 日）、攻撃者から新型コロナウイルスに関する影響により、支払方法を小切手から銀行振込に変更したいという旨のメールが着信しました。このメールに対して A 社側でも何らかの返信等を行っていたものと思われます。

その後、2 月 17 日、攻撃者から偽の振込先口座の情報とともに、今週中に振込を実施してほしいという内容のメールが着信しました（図 2）。A 社は、2 月 26 日、攻撃者から指定された偽の口座へ送金を行ってしまいました。

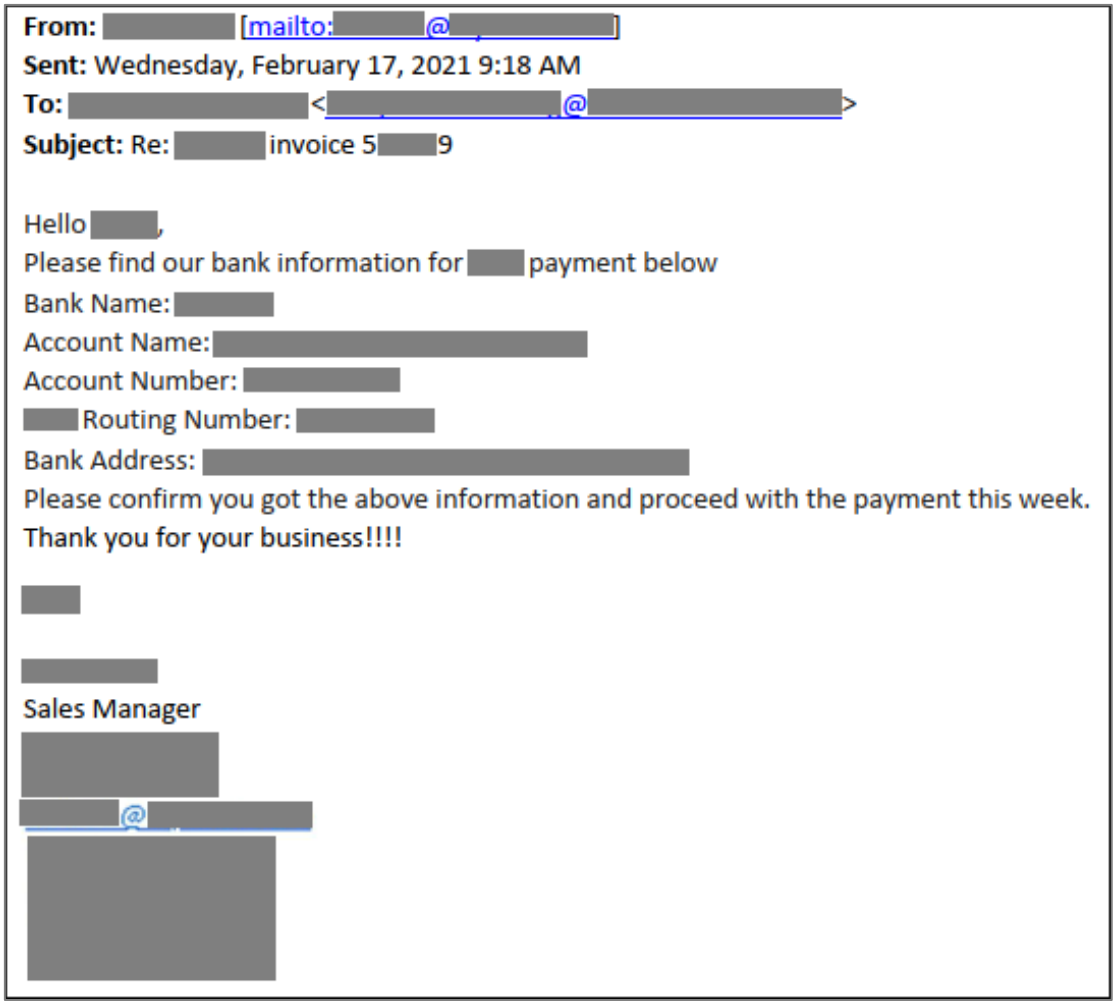
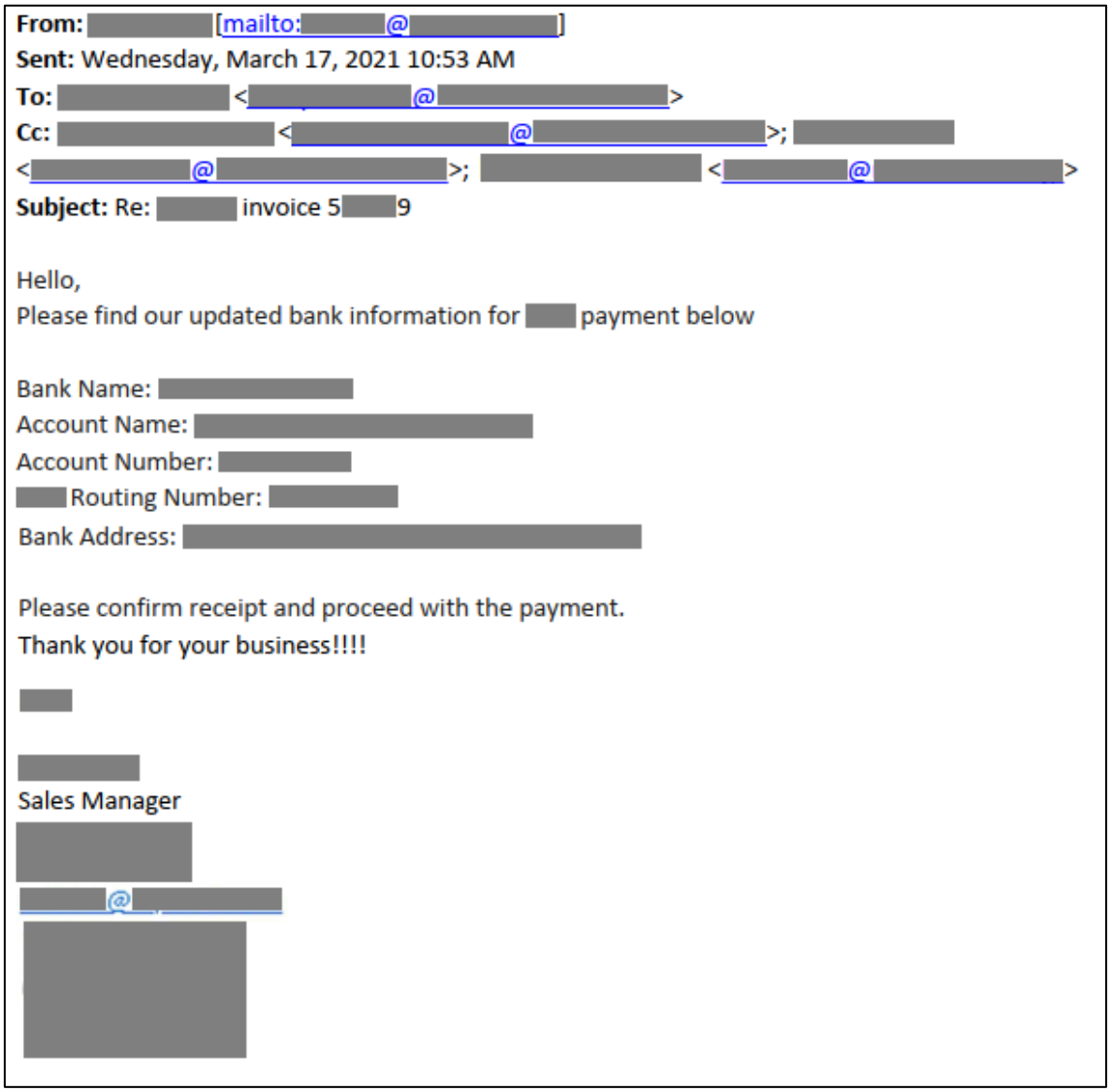


図 2 攻撃者からのメール（2021 年 2 月 17 日）

2 月 17 日以降も攻撃者から偽メールが着信したか否かは情報提供外のため不明ですが、3 月 17 日、攻撃者から再び、別の銀行の振込先口座の情報とともに、振込を依頼する旨の内容が書かれたメールが A 社担当者へ着信しました（図 3）。この時のメールには、同報先（Cc）に A 社の別の担当者も設定されていましたが、その担当者もこれが偽メールであると気付いていませんでした。



From: [redacted] [mailto:[redacted]]
Sent: Wednesday, March 17, 2021 10:53 AM
To: [redacted]
Cc: [redacted]
Subject: Re: [redacted] invoice 5[redacted]9

Hello,
Please find our updated bank information for [redacted] payment below

Bank Name: [redacted]
Account Name: [redacted]
Account Number: [redacted]
[redacted] Routing Number: [redacted]
Bank Address: [redacted]

Please confirm receipt and proceed with the payment.
Thank you for your business!!!!

[redacted]

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

図 3 攻撃者からのメール（2021 年 3 月 17 日）

3 月 22 日、A 社は攻撃者から送られてきた 2 つ目の偽の口座へ送金を行ってしまいました。その後、A 社担当者は、本物の B 社担当者にメールで振込を行った旨を連絡したところ、B 社担当者からはお礼のメールが着信したとのことです。B 社担当者は実際に入金されたか否かを確認しておらず、送金したという連絡に対するお礼を返信したに過ぎなかったものと思われます。

続いて、4 月 23 日にも、A 社は攻撃者から送られてきた 2 つ目の偽の口座へ送金（3 回目の送金）を行いました。

5 月 19 日になり、本物の B 社から振込が無い事への問合せを A 社で受けたため、詐欺であることが発覚しました。A 社では発覚後、偽の口座がある銀行へ連絡し、捜査機関へも届出をしたとのことです。

3.　詐欺の発覚までに時間がかかった要因

本事例では、攻撃者から偽のメールが送られた後、3 回の振込を行った後に詐欺が発覚しています。この詐欺が行われていることに気づくのが遅れた主な要因としては、次の 3 つが考えられるとのことでした。

- 口座変更の依頼に対して、不審に思わず対応を進めてしまった。

- A 社が 2021 年 3 月に攻撃者の用意した偽の口座へ振込を行った後、B 社の担当者宛にメールで振込完了の連絡を行ったところ、B 社の担当者からお礼の連絡があったため、A 社では取引に問題等は発生していないと考えていた。

- 本取引は月次の支払いであったが、B 社から未入金の連絡が来るまで長いタイムラグがあった。

4. 本事例の攻撃手口

本事例の攻撃では、次の攻撃の手口が使われました。

- 詐称用メールアドレスの使用
- メールの転送設定の悪用による盗み見

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

4.1. 詐称用メールアドレスの使用

本事例の攻撃では、攻撃者はB社の担当者になりすますため、B社の正規のドメインに似通った詐称用ドメインを使用していました。

【本物のメールアドレス】alice @ example . com
【偽物のメールアドレス】alice @ e**ax**mple . com → ドメイン名を一文字入れ替え

※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。

なお、本件で悪用された詐称用ドメインは、攻撃者が最初にA社へメールを送った2021年2月8日の4日前の2月4日に取得されていました。

4.2. メールの転送設定の悪用による盗み見

本件では、その後の調査により、B社のメールアカウントにおいて意図しないメールの転送設定が確認されたとのことでした。攻撃者は何らかの方法でB社のメールアカウントへ不正アクセスし、メールを攻撃者の元へ転送するように設定していたものと考えられます。当該設定を行うことで、攻撃者は、B社のメールアカウントに定期的にアクセス(ログイン等)することなく、A社とB社のやりとりを継続的に盗み見ることができていたものと推測しています。

なお、いつ頃メールの転送設定がなされたのかという点については不明でした。

以上