ビジネスメール詐欺（BEC）の詳細事例5

～取引相手から騙し取った証明書類が使われた事例～

2023 年 2 月 9 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 6 月に、日本国内の企業（A 社：支払側）と、中国の取引先企業（B 社：請求側）との間で取引に関するやりとりを行っている中、攻撃者が A 社と B 社の双方の担当者になりすまし、偽のメールを送ってきたものです。

攻撃者はメールを盗み見した上で、送金先を別の銀行口座へ変更するよう、偽のメールを A 社へ送信しました。不審と感じた A 社担当者が、メールの相手が本物の B 社であるか確認すべく、証明書類の提示を求めたところ、攻撃者は A 社の担当者になりすまし、B 社からそれら証明書類を騙しとり、A 社へ提示してきました。

最終的には、A 社の担当者が送信元のメールアドレスが B 社担当者のものと異なっていることに気づき、B 社担当者の正しいメールアドレスに直接連絡を取ったことで、本件が詐欺であることが発覚したため、金銭的な被害はありませんでした。

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

2021 年 6 月 29 日、IPA の情報収集活動の中で、国内企業である A 社に関連したビジネスメール詐欺が疑われる情報を発見したため、A 社に連絡したところ、本事例について情報を提供いただきました。

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	建設業の国内企業。支払側。
A 社担当者	A 社の担当者。B 社担当者と取引に係るやりとりを行っていた。B 社担当者になりすました攻撃者とメールでやりとりを行った。
B 社	調達、検査、認証、技術支援サービスを提供する中国の企業。請求側。
B 社担当者	B 社の担当者。A 社担当者と取引に係るやりとりを行っていた。A 社担当者になりすました攻撃者とメールでやりとりを行った。
攻撃者	A 社および B 社担当者になりすまし、ビジネスメール詐欺を試みた。

2.　攻撃全体の流れ

攻撃全体の流れについて、図 1～図 2 に示します。

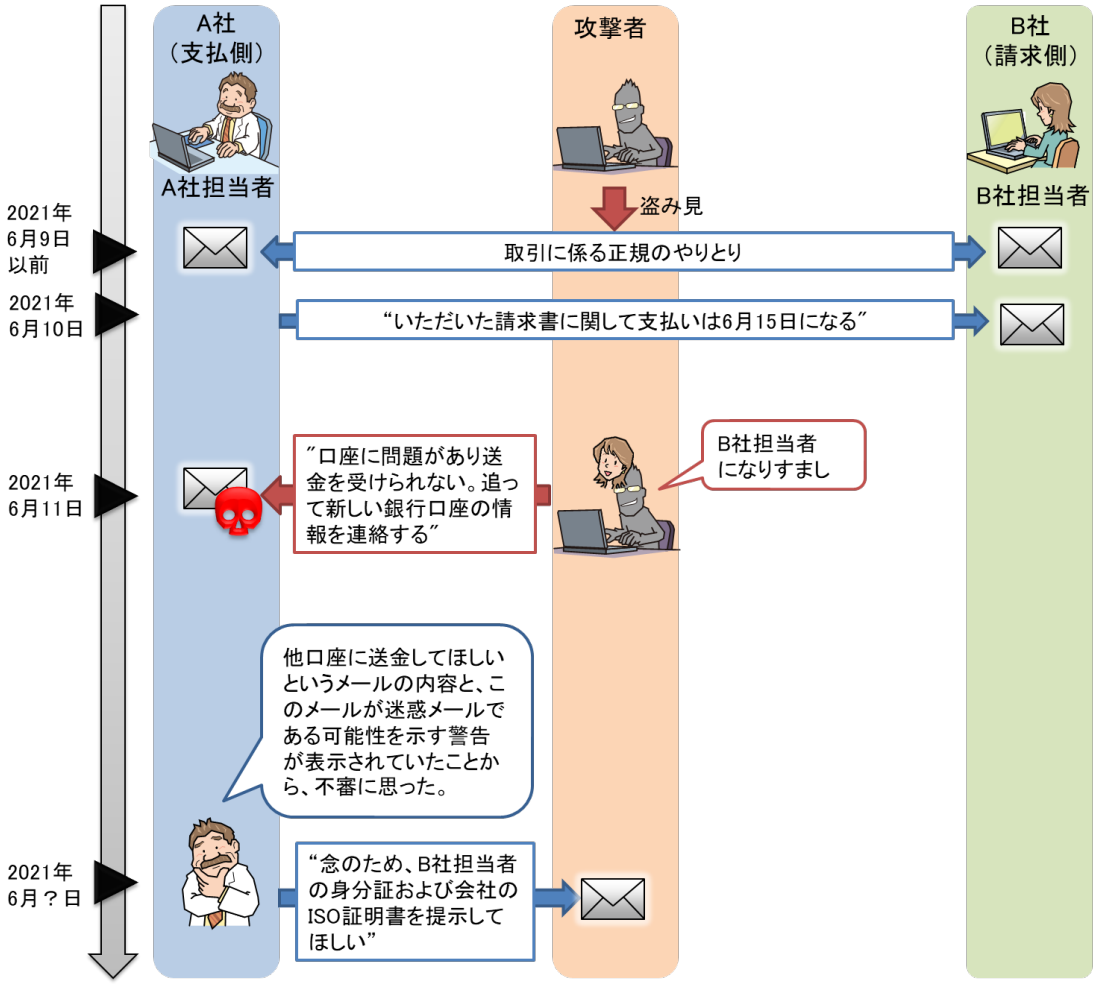


図 1 攻撃全体の流れ(1)

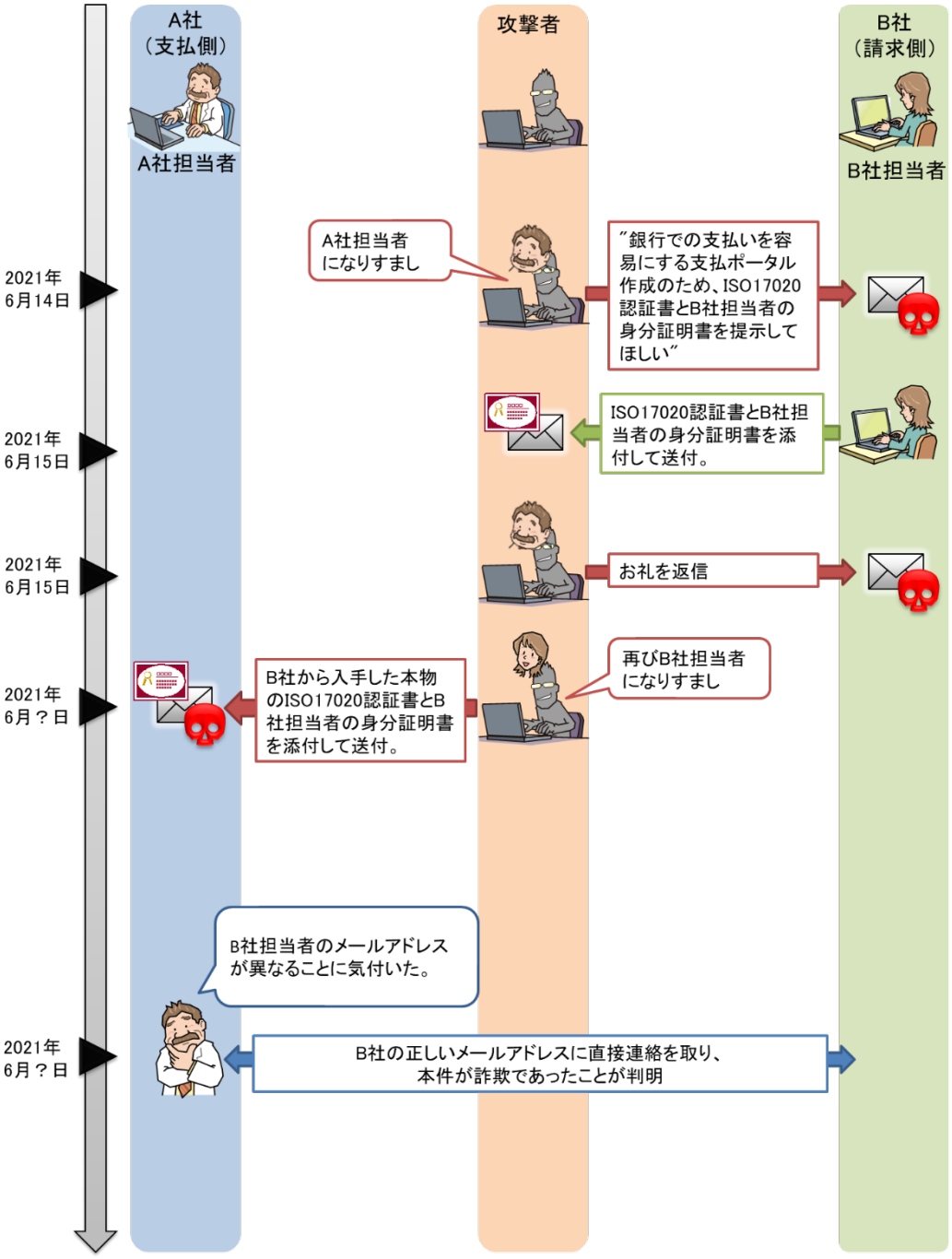

A社
（支払側）
攻撃者
B社
（請求側）
A社担当者
B社担当者
2021年
6月14日
A社担当者
になりすまし
″銀行での支払いを容
易にする支払ポータル
作成のため、ISO17020
認証書とB社担当者の
身分証明書を提示して
ほしい″
2021年
6月15日
ISO17020認証書とB社担
当者の身分証明書を添
付して送付。
2021年
6月15日
お礼を返信
2021年
6月？日
B社から入手した本物
のISO17020認証書とB
社担当者の身分証明書
を添付して送付。
再びB社担当者
になりすまし
B社担当者のメールアドレス
が異なることに気付いた。
2021年
6月？日
B社の正しいメールアドレスに直接連絡を取り、
本件が詐欺であったことが判明

図 2 攻撃全体の流れ(2)

2021 年 6 月 10 日以前から、A 社と B 社では取引に係るメールのやり取りを行っていました。攻撃者は何らかの方法でこれらのメールを盗み見ていたと思われます。

6 月 10 日、A 社担当者から B 社担当者へ、「いただいた請求書に対する支払いを 6 月 15 日に行う」という旨をメールしたところ、翌日の 6 月 11 日に、B 社の担当者になりすました攻撃者から、A 社担当者に偽のメール（図 3）が送られてきました。

このメールは、「本件の支払いを待ってください。政府の税金に関する銀行口座の問題を修正しようとしているため、我々の口座では支払いを受け取ることができません。本日の業務終了前に、我々から状況をお知らせするか、支払いのための新しい銀行口座の詳細をお知らせします。」という内容でした。なお、このメールには、6 月 10 日に A 社担当者から B 社担当者へ送ったメールが引用されており、署名部分も B 社担当者が過去のメールのやり取りで使用していたものと同一であり、偽のメールであると見破りにくいものでした。

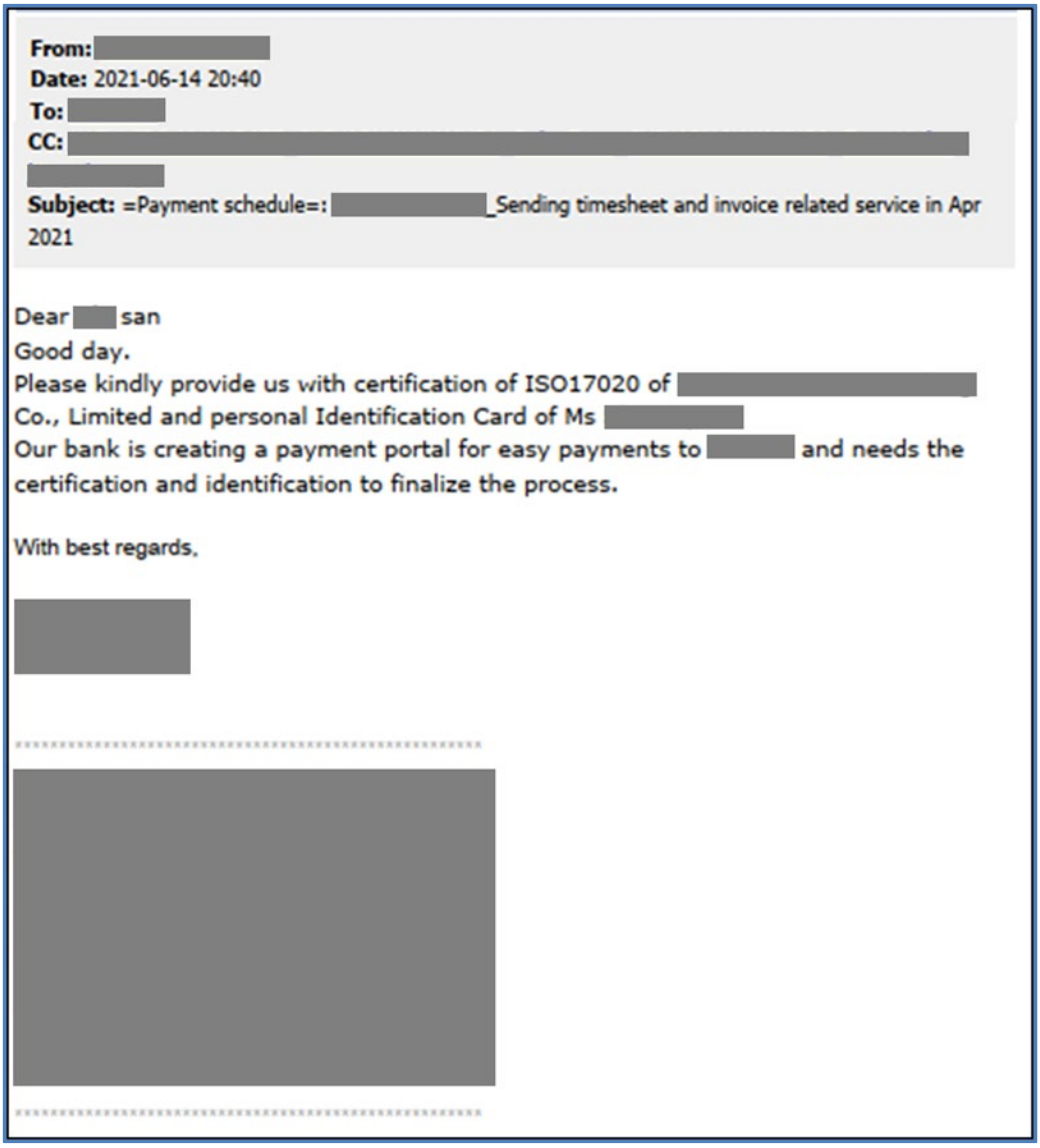
この偽のメールには、どのような判定基準によるものかは不明ながら、A 社のメールシステムによって、迷惑メールである可能性を示す警告が件名に付与されていました。

メールを受信した A 社担当者は、他口座に送金してほしいという依頼の内容と、警告表示の 2 点から不審に感じ、メールの相手が本物であるかを確認すべく、B 社担当者の身分証明書と B 社の ISO17020 証明書（B 社が検査機関として認定を受けた証明書）の提示をもとめるメールを返信しました。

しかし、このとき、差出人に設定されていたメールアドレスは、詐称用ドメインを使った偽のメールアドレスであったため、本物の B 社担当者ではなく、攻撃者に向けてメールが送られてしまいました。

図 3 A 社担当者へ送られた攻撃者からのメール（2021 年 6 月 11 日）

身元の確認を求めるメールを受けた攻撃者は、6 月 14 日、今度は A 社担当者になりすまして、B 社担当者へそれら証明書類の提示を依頼し、騙し取ろうとしました（図 4）。このメールでは、「我々の銀行で、支払いを容易にするための支払ポータルを作成するため」という嘘の理由が使われました。


From: [redacted]
Date: 2021-06-14 20:40
To: [redacted]
CC: [redacted]
Subject: =Payment schedule=: [redacted]_Sending timesheet and invoice related service in Apr 2021

Dear [redacted] san
Good day.
Please kindly provide us with certification of ISO17020 of [redacted]
Co., Limited and personal Identification Card of Ms [redacted]
Our bank is creating a payment portal for easy payments to [redacted] and needs the certification and identification to finalize the process.

With best regards,

[redacted]

[redacted]

図 4 B 社担当者へ送られた攻撃者からのメール 1 通目（2021 年 6 月 14 日）

B 社担当者は、攻撃者が A 社担当者になりすましていることに気がつかず、攻撃者へ証明書類を返送してしまいました。

数時間後には攻撃者からお礼のメール（図 5）が B 社担当者へ着信しています。

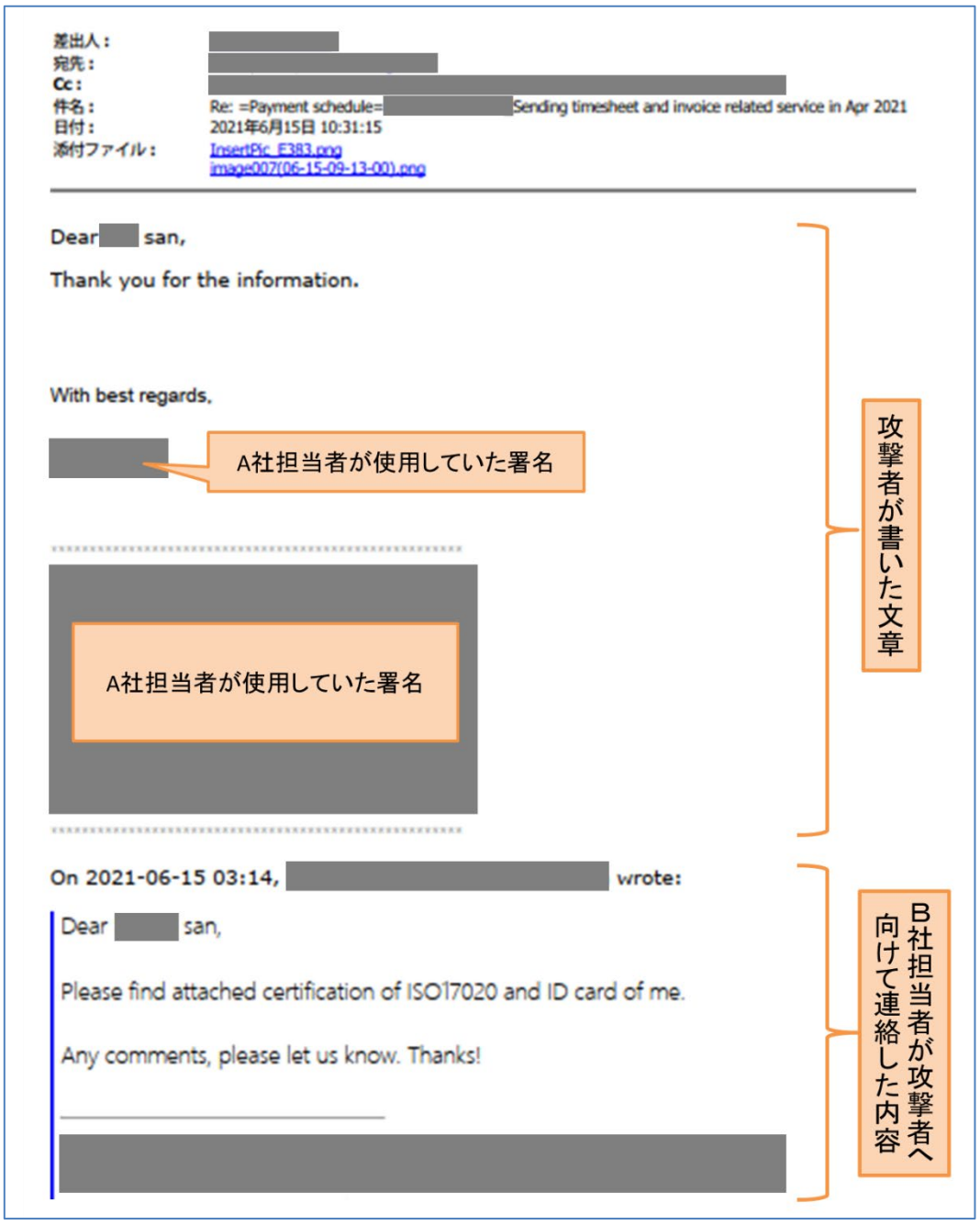


図 5 B 社担当者へ送られた攻撃者からのメール 2 通目（2021 年 6 月 15 日）

以降のメールは情報提供されていませんが、攻撃者は騙し取った B 社の証明書類を A 社担当者へ提示してきたとのことです。このタイミングで、A 社担当者は、そのメールの差出人メールアドレスが B 社担当者のものと異なることに気付きました。そして B 社担当者の正しいメールアドレスに直接連絡を取ったことで、本件が詐欺であったことが判明しました。

本件を受けて A 社では、攻撃者が使用していたメールアドレスをブロックしました。また、関係者への注意喚起、および不審メールの見分け方についての全社教育を実施したとのことです。

3. 本事例で使用された攻撃手口

本事例の攻撃では、次の攻撃の手口が使われました。

- 偽口座への送金先の変更
- 身元確認に応じるための証明書の詐取
- 正規メールの悪用
- 正規のメールアドレスに似せた詐称用ドメインの悪用

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ている攻撃手口です。

3.1. 偽口座への送金先の変更

本事例では、攻撃者が A 社担当者に対して送金先の変更を依頼する際、「銀行口座が政府の税金に関する問題で入金を受け取ることができない」という嘘の理由を示してきました。

口座に何らかの問題が生じているという嘘は、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、多く確認されています。

3.2. 身元確認に応じるための証明書の詐取

本事例では、攻撃者から最初に受信した偽のメールの時点で、A 社担当者は不審と気付いています。一方で、ビジネスメール詐欺の典型的な手口である、メールのやり取りを全て盗み見られている状況までは想定しえなかったため、B 社担当者の身分証明書などの提示を求めることで、本物であるかを確認しようとしました。

攻撃者は、詐欺が露見しそうな状況であるにも関わらず、狡猾に B 社から本物の証明書類を騙し取ることで詐欺を継続しようとしました。結果的には A 社担当者が偽のメールアドレスに気付くことができましたが、危ないところであったかもしれません。

ビジネスメール詐欺では、こういった巧妙な手口が使われるということ、また、相手が本物であるかの確認をメールのやり取りで行おうとすると、有効な方法とはならず、騙されてしまう可能性があるということを、ビジネス関係者全体で知っておくことが重要です。

3.3. 正規メールの悪用

攻撃者が A 社および B 社に送信したメール（図 3 と図 5）は、A 社担当者と B 社担当者が直前にやり取りしていた請求に関する本物の正規メールを引用したものでした。引用されたメールには、CC に A 社および B 社の担当者以外の社員のメールアドレスも含まれていましたが、攻撃者からのメールでは、これら CC の宛先も偽のメールアドレスに置き換えられていました。また、署名についても A 社および B 社担当者が普段使用しているものを流用しており、本物のメールへの返信の形とすることで、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。

攻撃者は A 社と B 社のメールでのやり取りの内容を把握していたとみられ、A 社と B 社との間のメールが何らかの方法で盗み見られていた可能性が高く、原因を調査中とのことでした。

3.4. 正規のメールアドレスに似せた詐称用ドメインの悪用

本事例では、攻撃者は A 社担当者および B 社担当者に偽のメールを送る際、それぞれの会社の正規のメインに似せた詐称用ドメインを新規に取得し、使用していました。

詐称用ドメインは、次の例に示すようなもので、それぞれメールを送信する数時間～数日前に取得されていました。

A 社の正規ドメインに似せた詐称用ドメイン
【本物のメールアドレス】 alice @ 123company-a . com
【偽物のメールアドレス】 alice @ 1123company-a . com
（「1」を一文字追加）
B 社の正規ドメインに似せた詐称用ドメイン
【本物のメールアドレス】 bob @ abccorporation-b . com
【偽物のメールアドレス】 bob @ abcorporation-b . com
（「c」を一文字削除）

※実際に悪用されたものとは異なる。

攻撃者はこのドメインを悪用し、A 社担当者にメールする際は、自身は B 社担当者になりすまし、CC を含めた B 社社員のメールアドレスを偽のメールアドレスに置き換えていました。また、B 社担当者にメールする際も同様に、自身は A 社担当者になりすまし、CC を含めた A 社社員のメールアドレスを偽のメールアドレスに置き換えていました。

これにより、メール受信者には自社の同僚が CC に含まれているように見えます。異常があれば誰かが気付くだろうというような偽の安心感を与えることで、詐欺に気付かれにくくすることを狙っていると考えられます。

4. 本事例のまとめ

本事例は典型的なビジネスメール詐欺が行われた状況で、A 社と B 社間のメールの盗み見、そして両方になりすまして両者を騙そうとしたものでした。

繰り返しとなりますが、メールを不審と感じた A 社担当者が試みた、身分証明書の提示による本人確認は的確な手段ではありませんでした。ただ、これは、「メールのやり取りが全て盗み見られており、攻撃者は A 社と B 社両方になりすましできる」という、普段からは想像もつかない状況であったため、無理もありません。しかし、ビジネスメール詐欺の手口や事例を知っていれば、より的確な確認方法、すなわち電話などの使用を思い立ったかもしれません。

また、この事例では、攻撃者からのメールが「迷惑メール（スパムメール）の可能性あり」と判定されていた点も特徴的です。詐欺メール・偽メールであるとまで判定できていたわけではないと思われますが、過去の他の事例においても、メールの送信元などが複数の観点でチェックされ、迷惑メールと判定されていた、迷惑メールフォルダに振り分けられていたということがありました。これもまた、何らか不審に気付けるきっかけとなるかもしれません。

本事例のように、不審と感じた場合、あるいは送金先の変更を依頼されたような場合、正規の担当者に、安全な手段で確認することが重要です。他のビジネスメール詐欺の事例ではメールアカウントが乗っ取られていたこともあるため、メール以外での連絡先を事前に確立しておき、確認の際はその連絡経路を使用する必要があります。また、そのような社内規定をあらかじめ設けておくことも対策として有効です。

この事例では、メールが盗み見られていた原因の特定に至っていません。メールが盗み見られていることが疑われる状況となった場合、端末のウイルスの確認、不審なログオンの確認、関係者のメールアカウントに身に覚えのない転送設定が施されていないかなどを確認することを勧めます。

以上