ビジネスメール詐欺（BEC）の詳細事例6

～国内企業社長になりすまし、グループ企業役員に金銭の支払を要求した事例～

2023 年 4 月 13 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、2022 年 8 月に、国内の企業（A 社）の社長になりすました攻撃者から、東南アジアのグループ企業（B 社）の役員に対して、M&A（企業の合併買収）について協力してほしいと称するメールが送られたものです。

攻撃者とのメールのやり取りの中で、B 社の役員が、進め方について社内の誰に相談すればよいかを質問したところ、回答がなかったため不審に思い、A 社の社長に電話で確認を行ったことで、本件が詐欺であることが発覚しました。

その後、B 社の役員は、攻撃者から金銭の支払を要求するメールを受信しましたが、詐欺であると認識しており、要求には応じなかったため、金銭的な被害は発生しませんでした。

今回の事例でやり取りされたメールは、すべて日本語でした。

なお、本事例は、2020 年 4 月に IPA が行ったビジネスメール詐欺に関する注意喚起 [1]にて紹介している事例と同様の手口のビジネスメール詐欺です。注意喚起以降も継続して、このビジネスメール詐欺を複数件確認しているため、今後も注意が必要です。

1.1. IPA への情報提供の経緯

2022 年 8 月 3 日、B 社から本事例の報告を受けて対応を行っていた A 社から IPA に対し、対応内容について妥当性の確認やアドバイスをしてほしい旨の相談がありました。IPA が相談対応を進める過程で、A 社から本事例に関する情報を提供いただきました。

[1] ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）
2.1 事例 1「日本語化」された 社長 詐称の攻撃
https://www.ipa.go.jp/archive/files/000081866.pdf

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	国内の企業。
A 社社長	A 社の社長（日本人）。攻撃者によってなりすまされた。
B 社	A 社の東南アジアのグループ企業。
B 社役員	B 社の役員（日本人）。攻撃者からのメールを受信し、その後、複数回にわたり、攻撃者とメールによるやり取りをした。
攻撃者	A 社の社長になりすまし、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。

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。

- 攻撃者とのメールのやり取り
- 詐欺発覚後の対応と再発防止策

2.　攻撃者とのメールのやり取り

本事例における、B 社役員と攻撃者とのメールのやり取りについて、図 1 に示します。

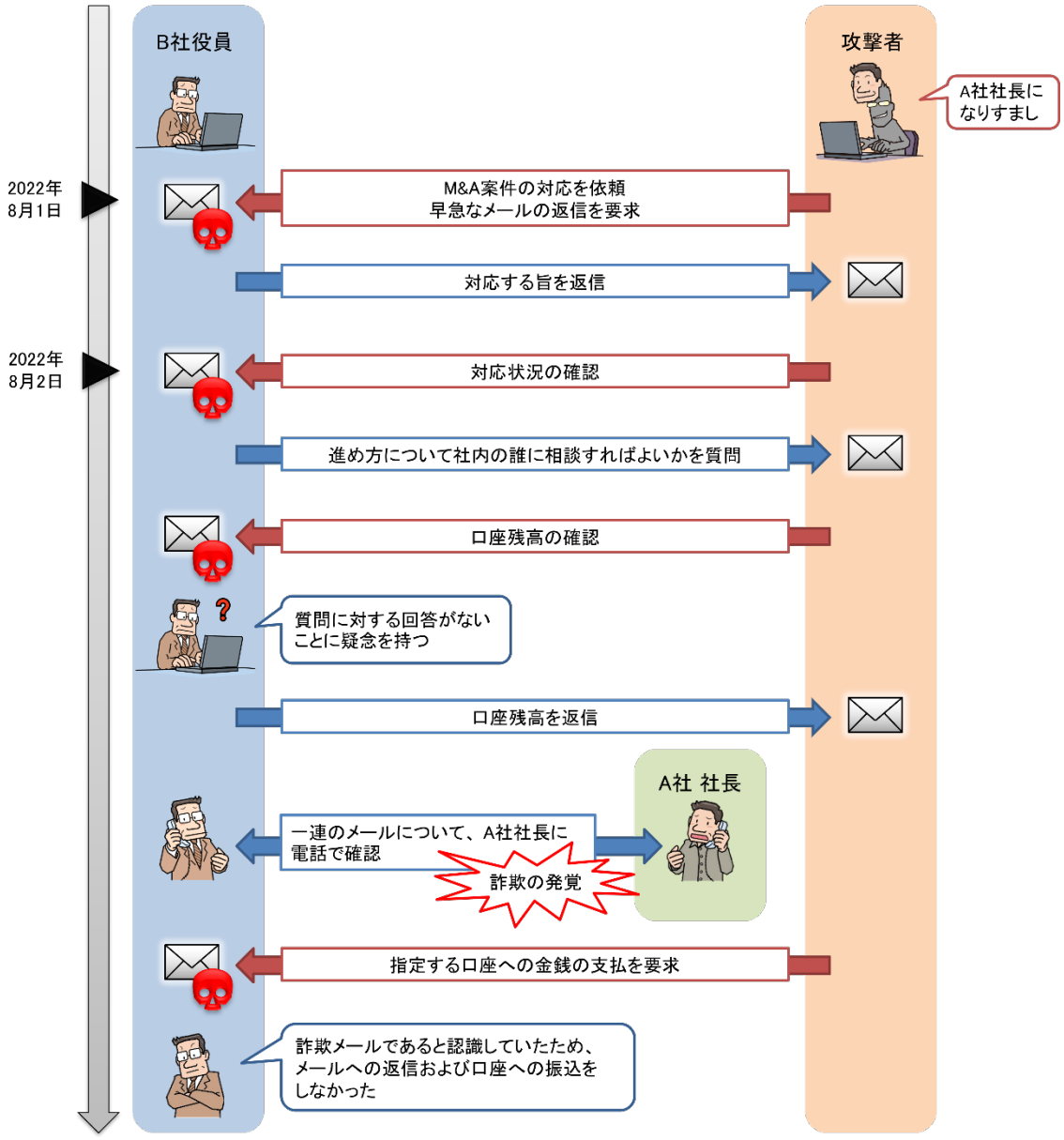

図 1 攻撃者とのメールのやり取り

2022 年 8 月 1 日、A 社社長になりすました攻撃者から、B 社役員に対する 1 通目のメール（図 2）が送られてきました。メールには、M&A 案件の対応依頼および早急にメールにて返信してほしいといった内容が記載されていました。

当該メールの差出人（From ヘッダ）には、A 社社長の氏名（英語表記）とメールアドレスが設定され、メール本文の署名には、A 社社長の氏名[2]が記載されていました。

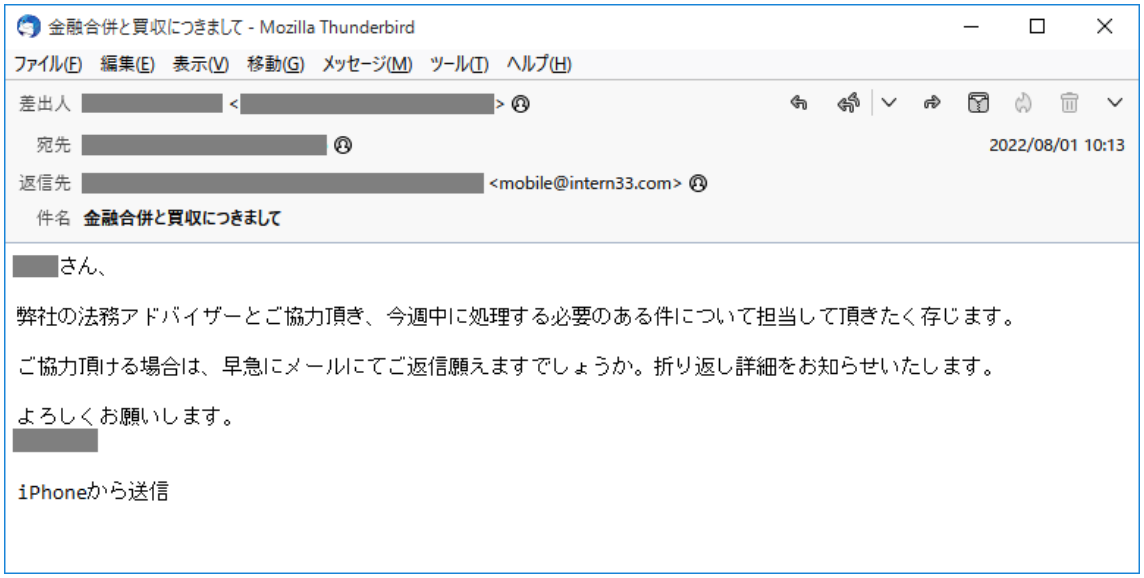

図 2 攻撃者からのメール 1 通目

[2] A 社社長の氏名は漢字が 1 文字誤っており、攻撃者のミスである可能性が考えられます。

攻撃者からの 1 通目のメールを受信した B 社役員は、攻撃者からのメールと気づかず、対応する旨のメールを返信したところ、翌日、攻撃者からの 2 通目のメール（図 3）が送られてきました。

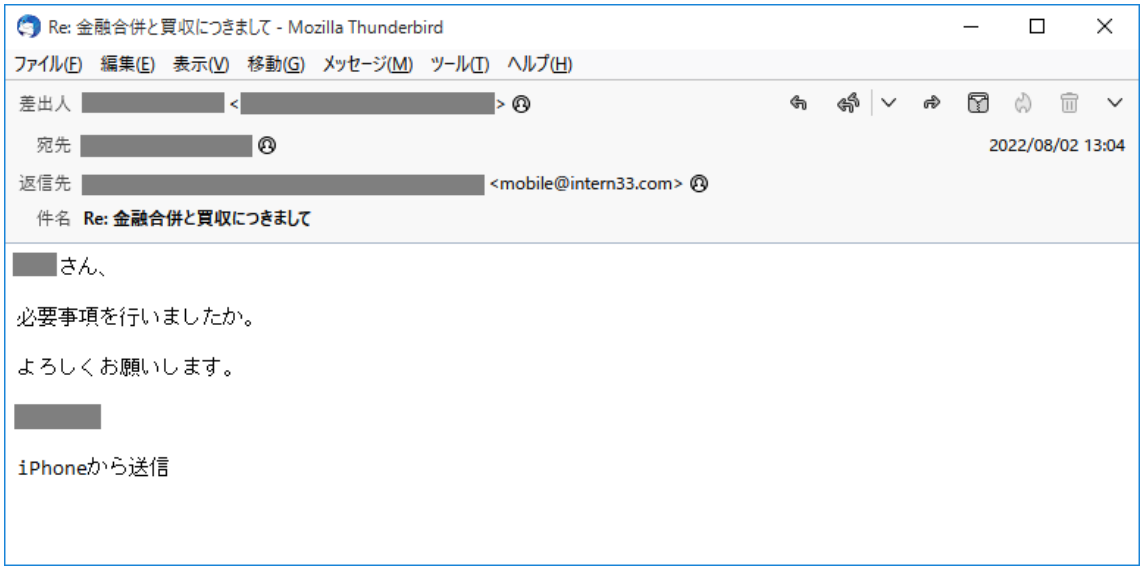

図 3 攻撃者からのメール 2 通目

B 社においては、投資案件の振込を行う際、B 社および A 社の取締役の承認が必要な取り決めとなっていました。このため、B 社役員は 2 通目のメールに返信する際に、本件の進め方について社内の誰に相談すればよいかを質問しました。

しかし、攻撃者からの 3 通目のメールは、質問への回答ではなく、口座残高を確認する内容でした。B 社役員は、質問の回答がなかったことに対して疑念を持ちながらも、口座残高を攻撃者に返信しました。

メール返信後、質問の回答がなかったことを不審に思った B 社役員は、一連のメールについて A 社社長に電話で確認を行いました。その結果、A 社社長は当該メールを送信していないことが判明し、本件がなりすましメールによる詐欺であることが発覚しました。B 社役員は、A 社に対して、A 社社長になりすました攻撃者による詐欺メールがあったことを報告しました。

その後、攻撃者から、指定する口座に金銭の支払を要求する 4 通目のメール（図 4）が送られてきました。メール本文には、実在すると思われる弁護士の氏名が記載されていました。

しかし、B 社役員は、本メールが詐欺メールであると認識していたため、当該メールへの返信および指定された口座への振込を行いませんでした。

この結果、金銭的な被害は発生しませんでした。

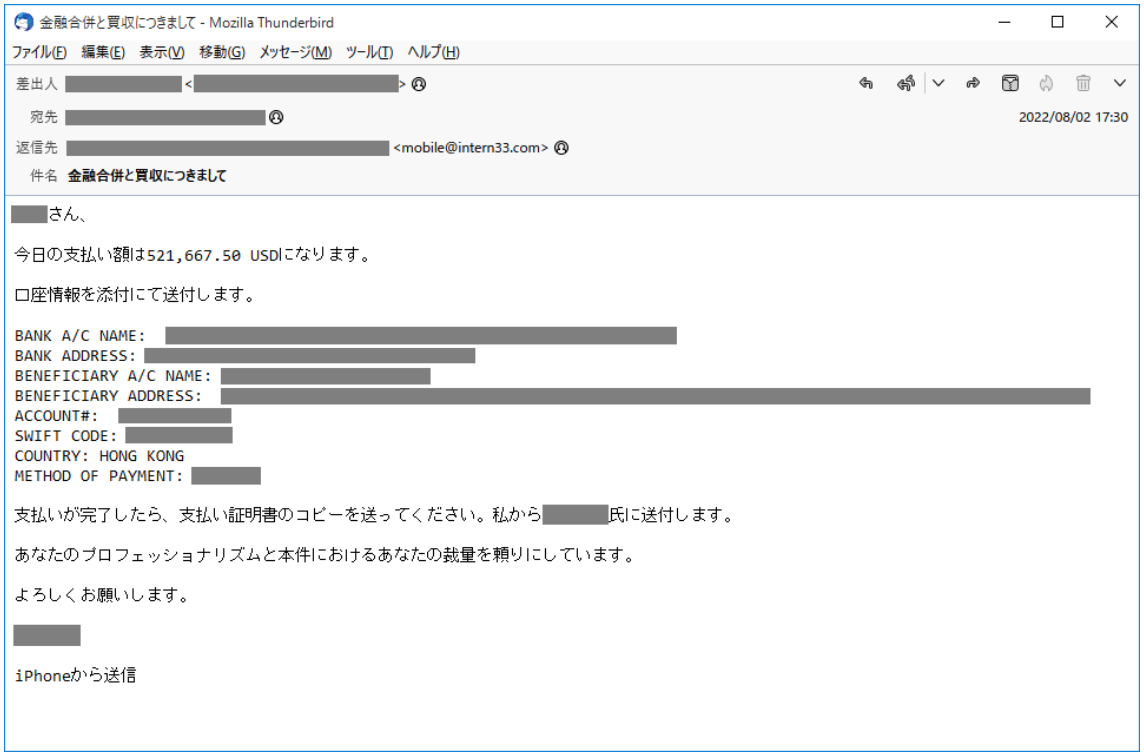

図 4 攻撃者からのメール 4 通目

3. 詐欺発覚後の対応と再発防止策

B 社役員から、詐欺メールについての報告を受けた A 社は、A 社社長のメールアカウントが乗っ取られている可能性を考慮して、A 社社長が使用しているメールアカウントのパスワード変更およびパソコンのウイルススキャンなどを行いました。その後の調査により、A 社社長のメールアカウントは乗っ取られておらず、攻撃者が A 社社長の氏名とメールアドレスを騙っていただけであったことが判明しました。

A 社および B 社は、なりすましメール対策として、以下の対応を行いました。

- 送信ドメイン認証(SPF)の設定変更による、なりすましメールのブロック
- 新たな送信ドメイン認証(DMARC)の導入検討

また、従業員に対する教育・啓発として以下の対応を行いました。

- ビジネスメール詐欺に関する注意喚起の連絡
- IPA が公開しているビジネスメール詐欺対策の啓発動画 [3]の視聴指示

[3] 映像で知る情報セキュリティ ～映像コンテンツ一覧～
「What’s BEC？ ～ビジネスメール詐欺 手口と対策 ～」
https://www.ipa.go.jp/security/videos/list.html

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。

- 詐欺の成功率を上げるための偽の依頼
- 返信先（Reply-To ヘッダ）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る攻撃手口です。

4.1. 詐欺の成功率を上げるための偽の依頼

本事例の攻撃者からのメールの内容は、M&A 案件に関して今週中に対応してほしいといったものであり、機密性と緊急性が高いと思わせるような依頼でした。このような偽の依頼をすることで、B 社役員を焦らせ、冷静な判断や他の従業員への相談をさせにくくすることで、詐欺の成功率を上げようとする目的があったと考えられます。

さらに、法務アドバイザーと協力する旨の指示や、実在すると思われる弁護士の氏名を記載することで、偽の依頼にリアリティを持たせ、本物の依頼メールであると信じ込ませようとしていたと考えられます。

4.2. 返信先(Reply-To ヘッダ)の悪用

本事例の攻撃者は、メールの差出人(From ヘッダ)に、A 社社長のメールアドレスを設定し、返信先(Reply-To ヘッダ)には、攻撃者が使用するメールアドレスを設定していました。

From: A 社社長の氏名 < A 社社長のメールアドレス >

Reply-To: A 社社長の氏名とメールアドレス < 攻撃者のメールアドレス >

このように設定された状態では、B 社役員が返信ボタンをクリックするなどして作成したメールの宛先には、差出人(From ヘッダ)に設定されている A 社社長のメールアドレスではなく、返信先(Reply-To ヘッダ)に設定されている攻撃者のメールアドレスが設定されます。このとき、メールソフトの画面上、宛先部分には、A 社社長の氏名とメールアドレスも表示されます(図 5)が、実際に送付されるメールアドレスは攻撃者のメールアドレスのみとなります。

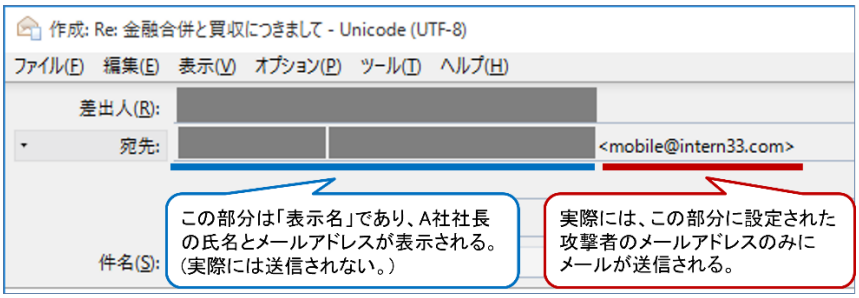

図 5 返信メールの宛先

攻撃者は、メールを受信した B 社役員に対し、メールが本物であると錯覚させつつ、B 社役員からの返信メールを、A 社社長には届かないようにしていました。

以上