ビジネスメール詐欺（BEC）の詳細事例1

～偽口座送金後、一部資金を回復できた事例～

2022 年 9 月 28 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、2019 年 9 月に国内の輸入販売業の企業（A 社：支払側）と、イタリアの輸入元企業（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、偽の口座への振り込みを要求するメールが送られたものです。

この事例では、A 社の担当者が攻撃者に騙され偽の口座へ送金を行ってしまい、攻撃者によって資金の約半額を引き出されてしまったため実被害がありました。しかし、偽口座に残っていた資金の残額について、B 社やイタリア警察を交えた対応により、残金を取り戻すことができたということです。

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、2019 年 10 月 1 日、A 社より、イタリアの取引業者（B 社）とのメールのやり取りの中で、海外送金時に取引先になりすましたメールが着信したということで IPA へ情報提供いただいたところから始まります。

情報提供いただいた内容を確認したところ、2019 年 9 月に取引先になりすました攻撃者から、偽の口座への変更を依頼する内容のメールが送られていることがわかりました。A 社に協力いただきながら情報を整理している中で、A 社から 2019 年 5 月にも口座変更を依頼する不審メールがあったということで、IPA へ情報提供いただきました。この情報を確認したところ、同一と思われる攻撃者が、2019 年 5 月にも取引先になりすましたビジネスメール詐欺を企図した攻撃メールを A 社に送り付けていたことがわかりました。

A 社では、2019 年 9 月に偽の口座へ送金を行ってしまいました。約半額が攻撃者によって引き出されてしまったものの、残りの半額について資金を取り戻すべく対応を行い、2020 年 4 月に資金を取り戻すことができました。この対応についても IPA へ情報提供をいただきました。

1.2. 本事例における関係者について

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	国内の輸入販売業の企業。支払側。
A 社担当者	A 社の CEO であり、本事案で攻撃者から偽メールを送り付けられた。
B 社	イタリアの輸入元企業。請求側。
B 社担当者 1	B 社の担当者。A 社担当者と最初に取引に係るやり取りを行っていた。
B 社担当者 2	B 社の担当者。途中から A 社担当者との取引に係るやり取りへ加わった。A 社担当者と電話による対応も行った。
攻撃者	B 社の担当者 1 と 2 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。また、詐欺の発覚後はハッカーを名乗り A 社へ偽のメールを送り付けた。
イタリアの銀行	偽口座があるイタリアの銀行。
イタリア警察	本件で捜査を行ったイタリアの警察。
C 社	攻撃者によって悪用された偽口座を保有しているイタリアの企業。

本事例については、次の 3 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 5 章で説明します。

- 口座変更に係る攻撃者とのやりとり（2019 年 5 月）
- 偽口座への送金に至る攻撃者とのやりとり（2019 年 9 月）
- 偽口座に残る資金回復に至るまでの対応

2.　口座変更に係る攻撃者とのやりとり（2019 年 5 月）

本事例では、2019 年 9 月に実際に偽口座への送金に至る前にも、攻撃者から口座変更に係るやりとりがありました。攻撃者とのやりとりの概要（図 1）について次に示します。

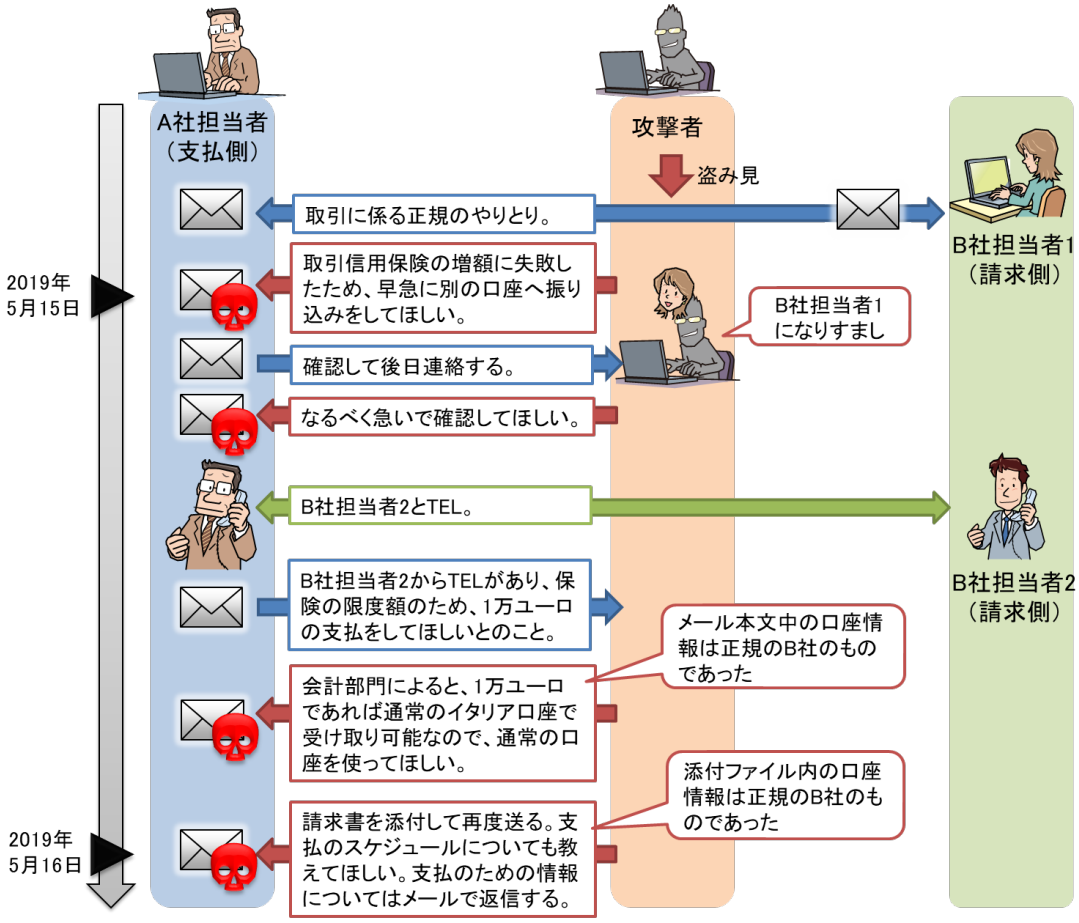

図 1 攻撃者とのやりとり（2019 年 5 月）

2019 年 5 月 15 日、A 社と B 社で取引に係るメールのやりとりを行っている中で、攻撃者から次のメール（図 2）が着信しました。

このメールは、B 社担当者 1 になりすました攻撃者から、取引信用保険の増額に失敗したためという理由で、早急に別の口座へ送金してほしいと依頼する内容でした。また、メールには別口座への送金の理由として、主要口座は現在監査中であると記載されていました。銀行口座が監査を受けているという理由で別の口座への送金を要求する内容は、これまで IPA が確認してきたビジネスメール詐欺でも多く使われるものでした。

図 2 攻撃者からのメール 1 通目(2019 年 5 月 15 日)

このメールに対し、A 社担当者は、確認して後日連絡をすると回答をしたところ、攻撃者からなるべく早く確認してほしいという内容のメール(図 3)が着信しました。

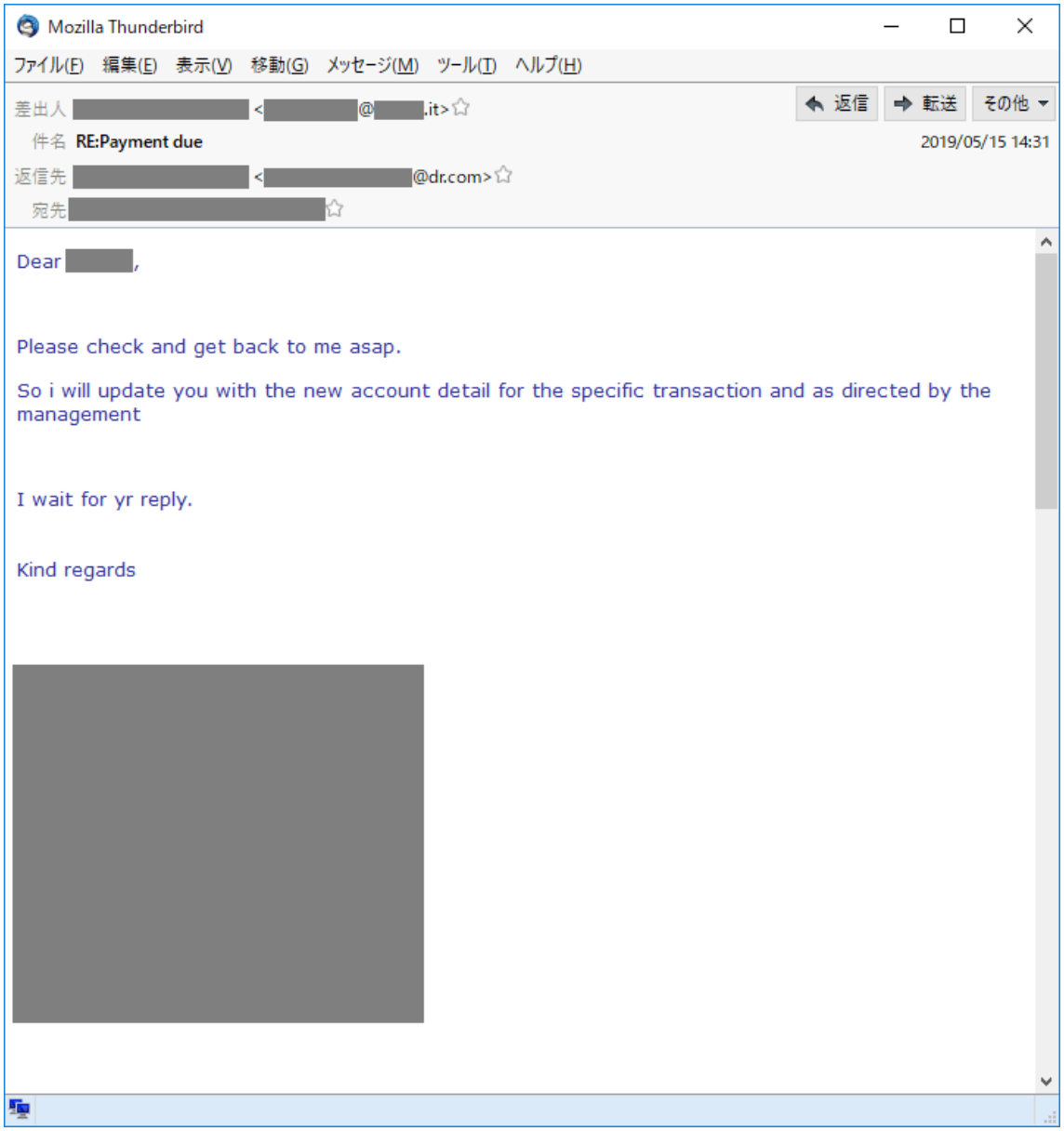

図 3 攻撃者からのメール 2 通目（2019 年 5 月 15 日）

この 2 通目のメールの後、A 社担当者と、B 社担当者 2 が電話による会話を行い、A 社担当者は、攻撃者（B 社担当者 1 へなりすまし）へ保険の限度額のために 1 万ユーロを支払ってほしいと連絡を受けたということをメールにて返信しました。

その後、攻撃者は A 社の担当者に対し、1 万ユーロであれば通常の口座での支払いができるので、イタリアの口座へ支払いをしてほしいという内容のメール（図 4）を送ってきました。このとき、メール本文中に書かれていた口座は、正規の B 社の口座情報が書かれていました。これは、A 社担当者が B 社の人物と電話をしたということから、偽のメールであることがばれてしまうことを避けるために本物の口座への支払いを要求したものと推測できます。

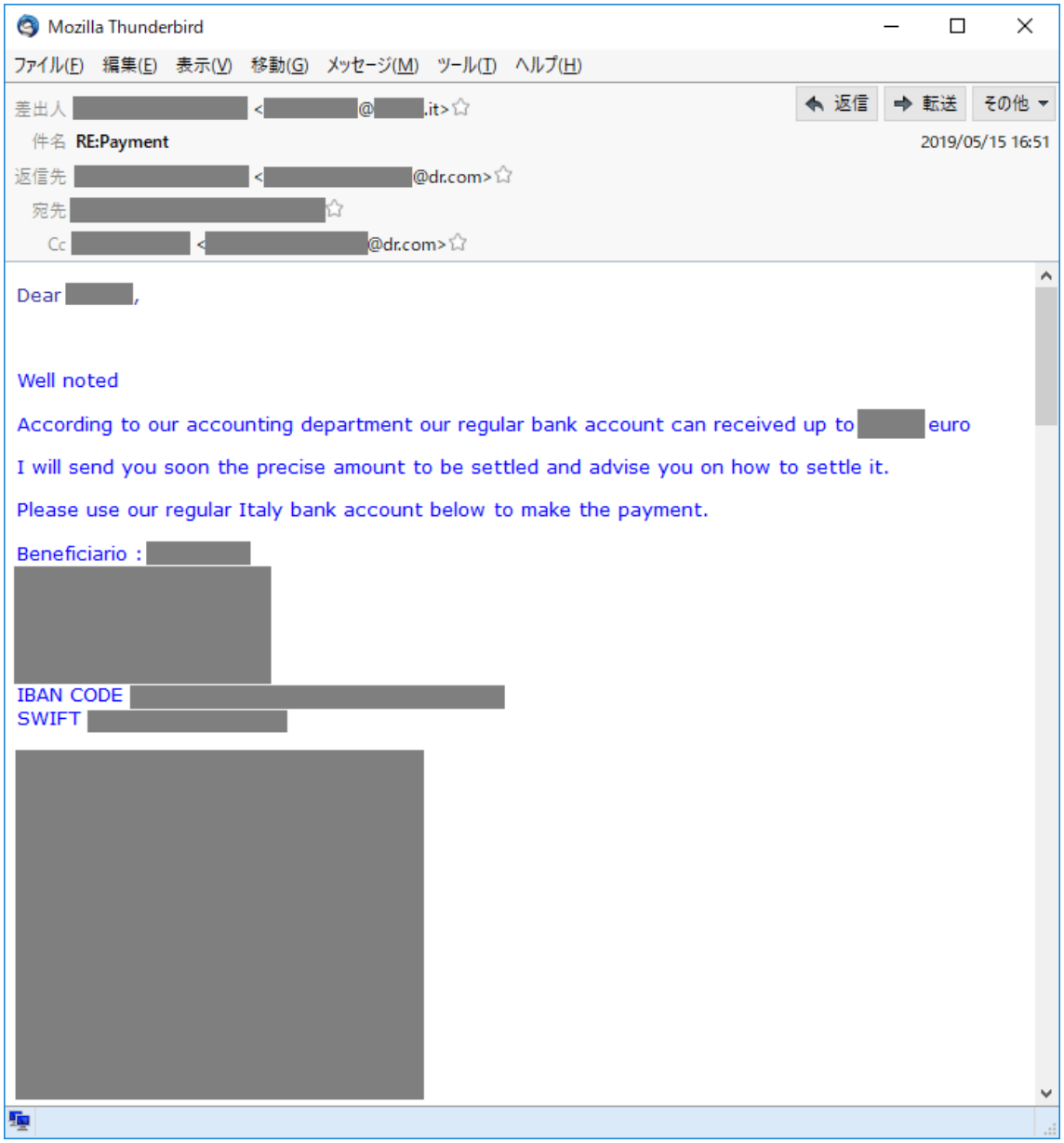

図 4 攻撃者からのメール 3 通目（2019 年 5 月 15 日）

さらに、翌日、攻撃者から請求書が添付されたメール（図 5）が送られてきました。このメールでは支払いスケジュールについて教えてほしいという内容が書かれていました。この添付ファイルには支払いの口座情報が書かれていたが、正規の B 社の口座情報でした。

結果として、5 月のタイミングでは攻撃者は金銭の窃取を行うことができてはいないが、偽のメールであることを A 社担当者が見抜けていないことから、別の取引での金銭の窃取を狙うように変更した可能性もあります。

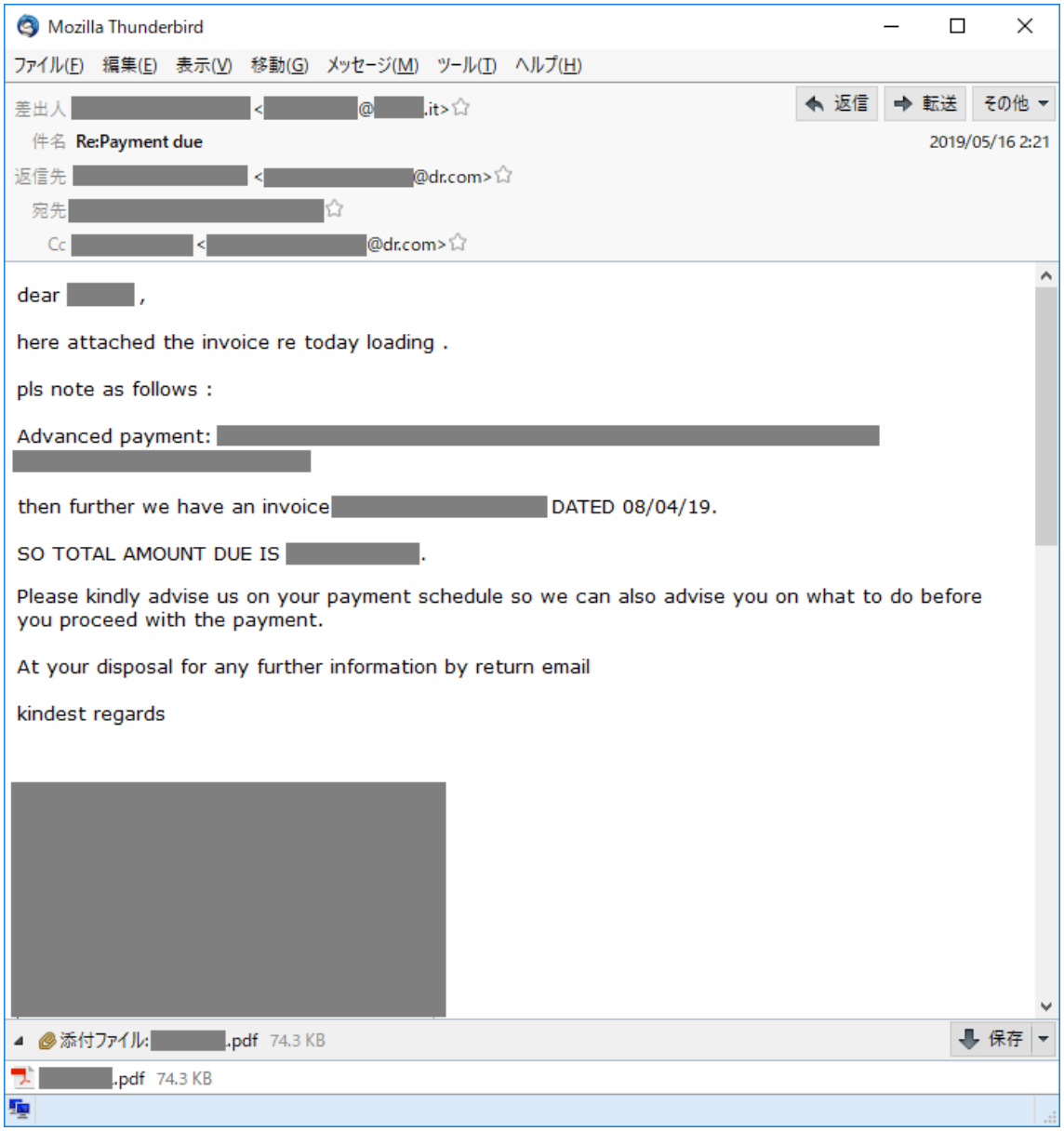

図 5 攻撃者からのメール 4 通目(2019 年 5 月 16 日)

3. 偽口座への送金へ至る攻撃者とのやりとり（2019 年 9 月）

2019 年 9 月、A 社と B 社の取引に関するメールのやりとりの中で、B 社担当者になりすました攻撃者から偽の口座への送金を要求するメールが A 社担当者へ送られました。A 社担当者は、偽のメールであると気づかず攻撃者とのメールのやりとりを行い、偽の口座へ送金を行ってしまいました。

攻撃者とのやりとりの概要について、図 6、図 7、図 8 に示します。

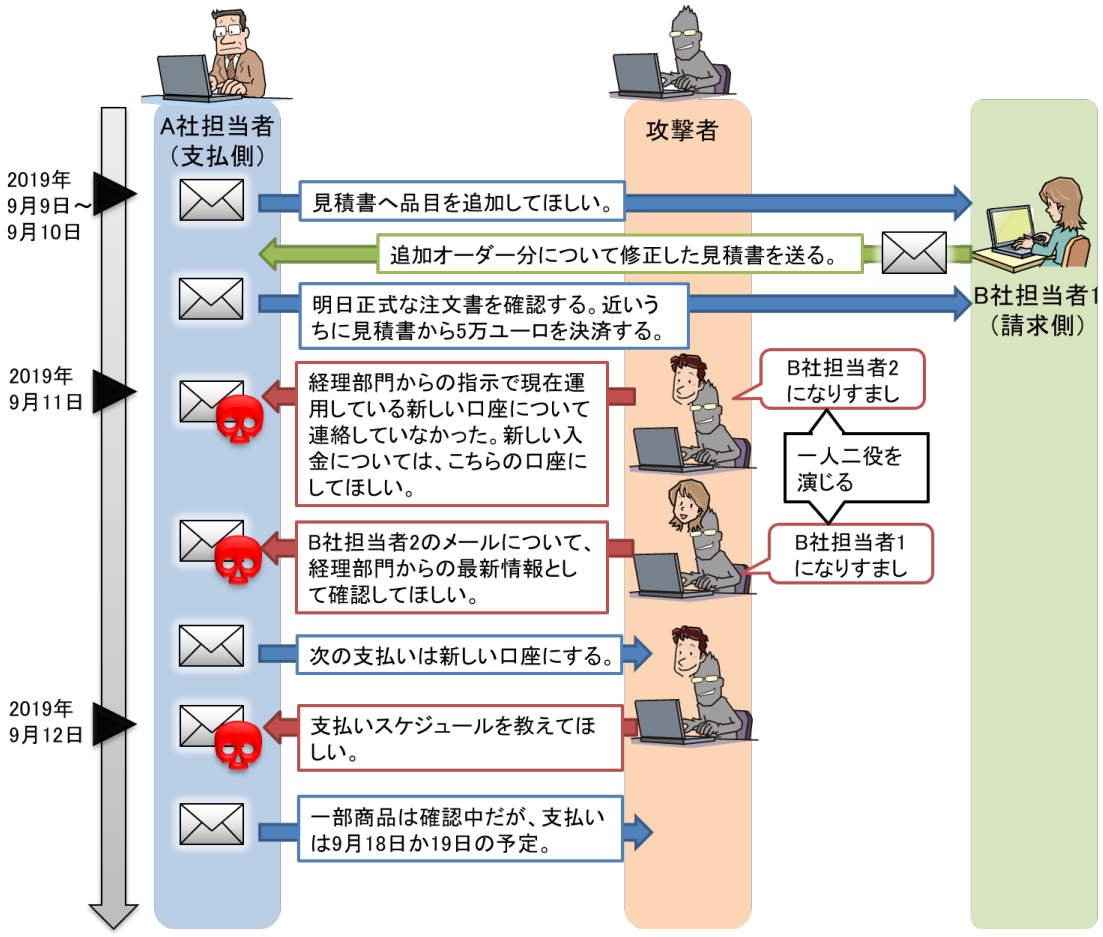

図 6 攻撃者とのやりとり 1（2019 年 9 月）

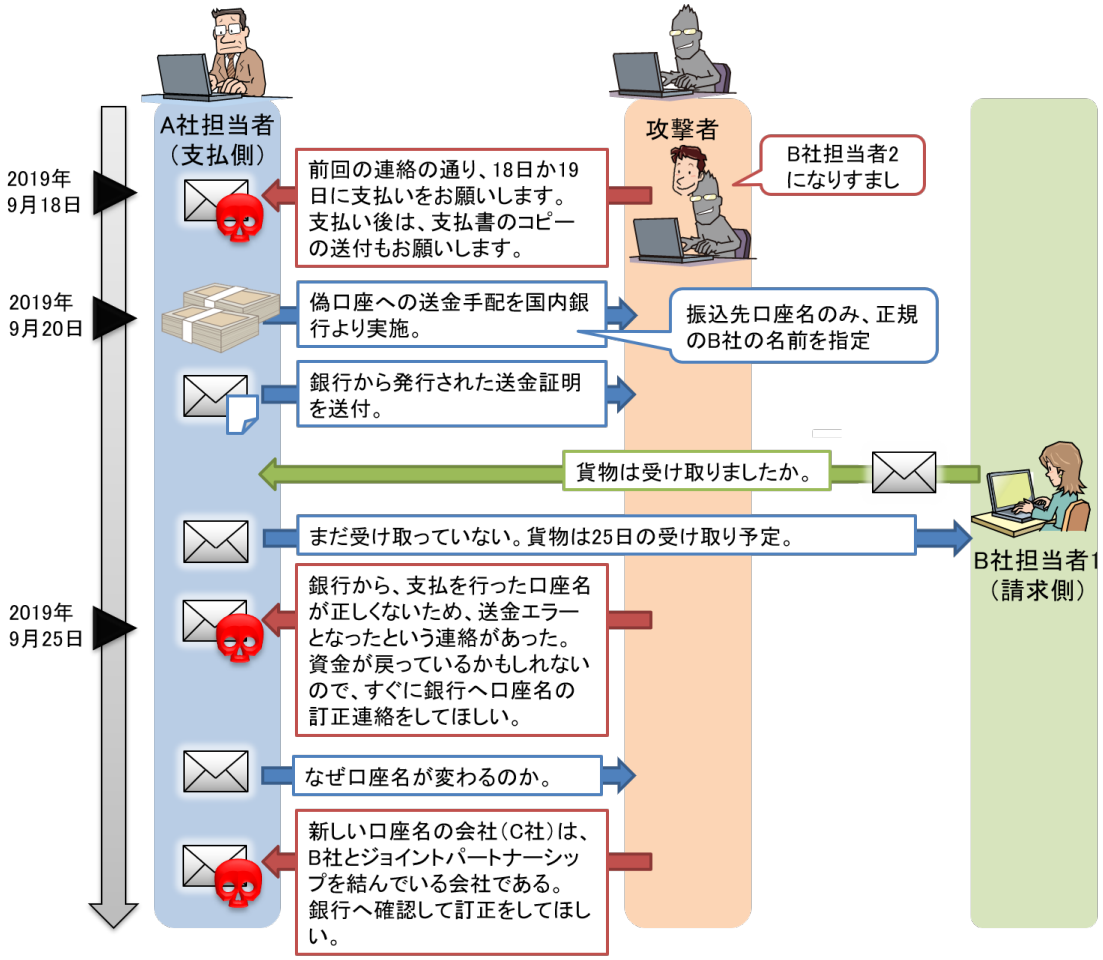

図 7 攻撃者とのやりとり 2（2019 年 9 月）

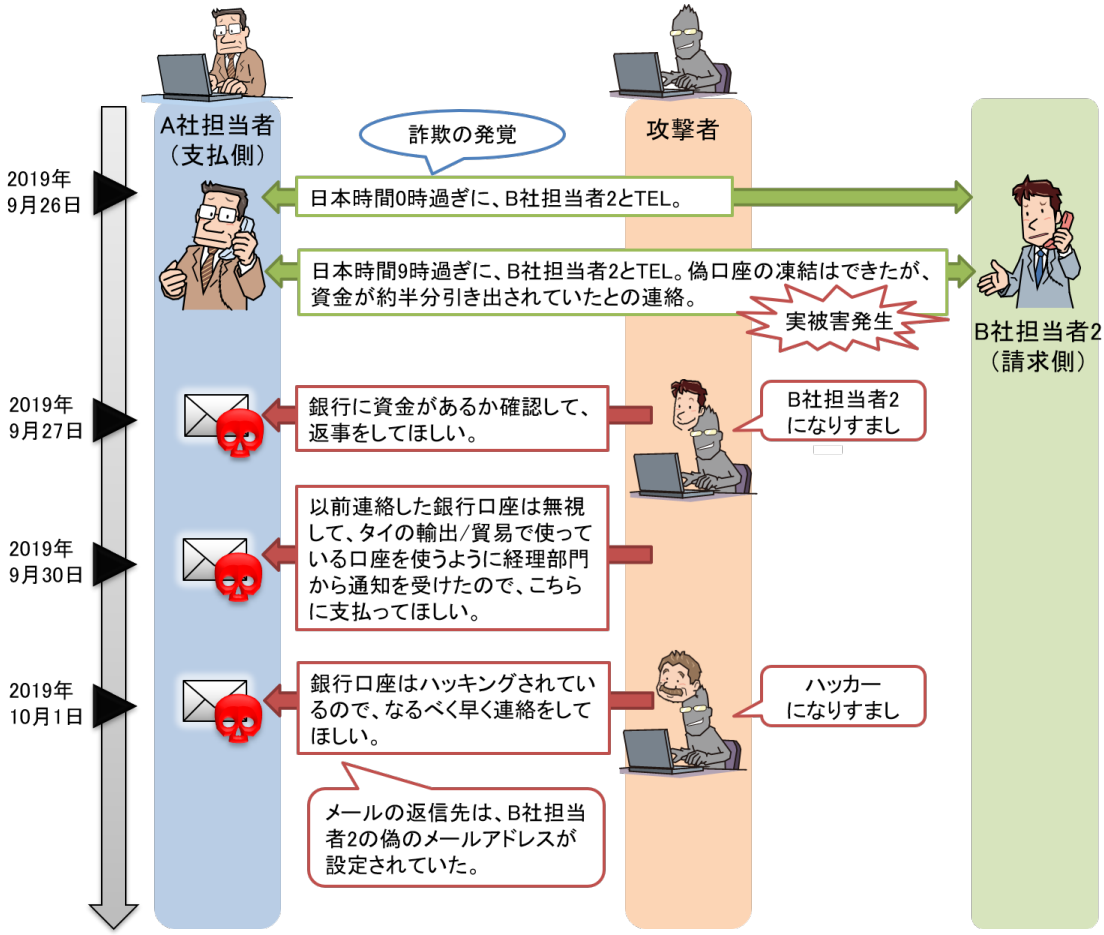

図 8 攻撃者とのやりとり 3（2019 年 9 月～10 月）

2019 年 9 月 9 日～10 日にかけて、A 社担当者と B 社担当者 1 の間で取引に係るメールのやりとり（追加オーダーと見積書のやりとり）を行っている中で、9 月 11 日に B 社担当者 2 になりすました攻撃者から次のメール（図 9）が着信しました。

このメールでは、経理部門からの指示で現在運用している新しい口座への支払いをしてほしいという理由で、偽の口座への送金を要求する内容が記載されており、メールの本文中に、偽の口座が記載されていました。この偽の口座はイタリアにある銀行であり、取引先もイタリア企業であることから不審に思われにくいように、同じ国内の偽の口座を使ったものと推測されます。

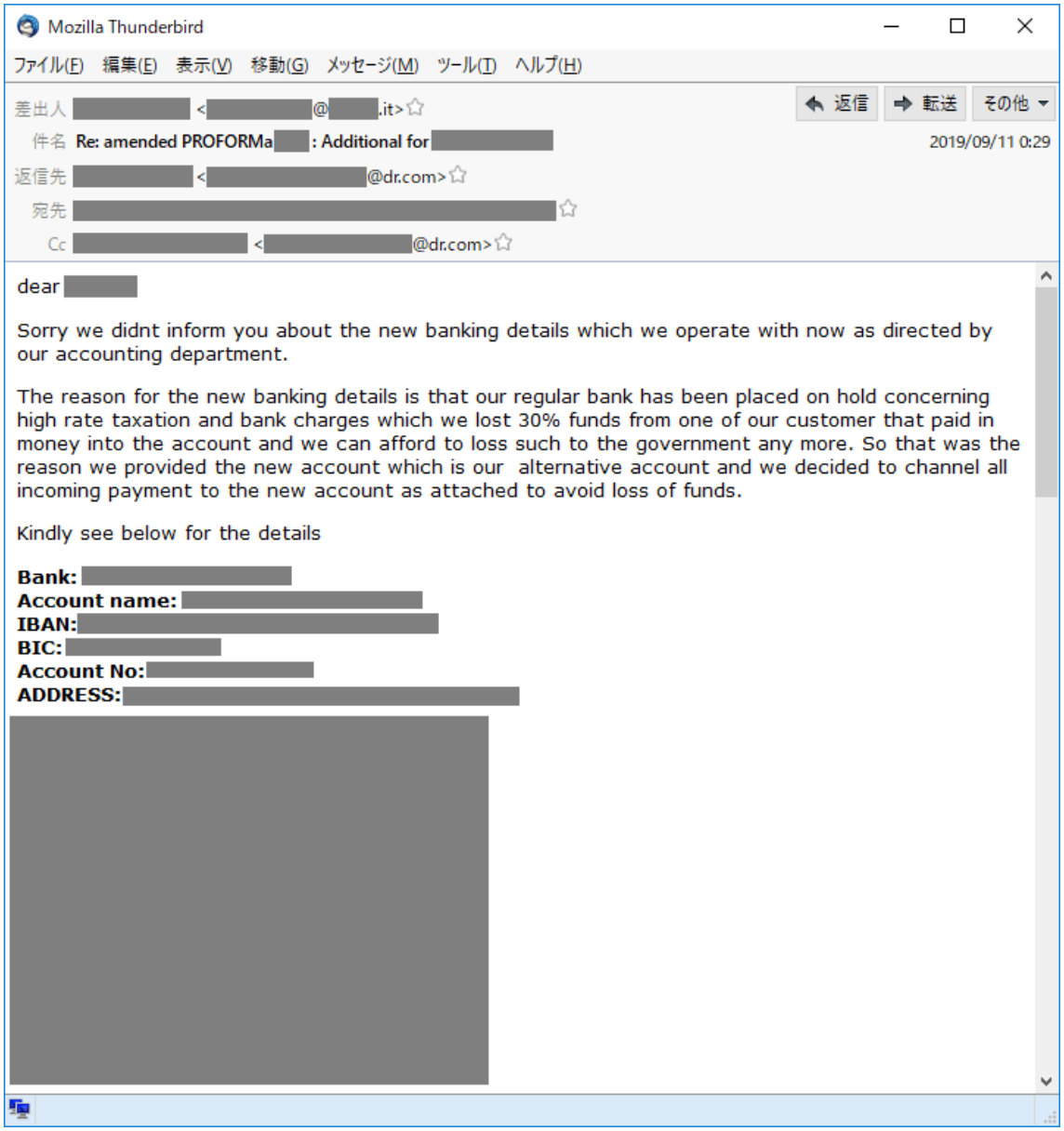

図 9 攻撃者からのメール 1 通目（2019 年 9 月 11 日）

さらに、攻撃者は 1 通目のメールが送られた約 7 分後に、B 社担当者 1 になりすました攻撃者から 2 通目のメール（図 10）が送られました。

このメールには、攻撃者がなりすまして送った B 社担当者 2 のメール（1 通目）を引用しつつ、経理部門からの最新情報として確認してほしいという内容が記載されていました。

ビジネスメール詐欺では、攻撃者が一人二役を演じて、相手を騙すこともあり、本件でも攻撃者が A 社担当者を騙すために、B 社担当者 1 と 2 の二役を演じていたものと思われます。

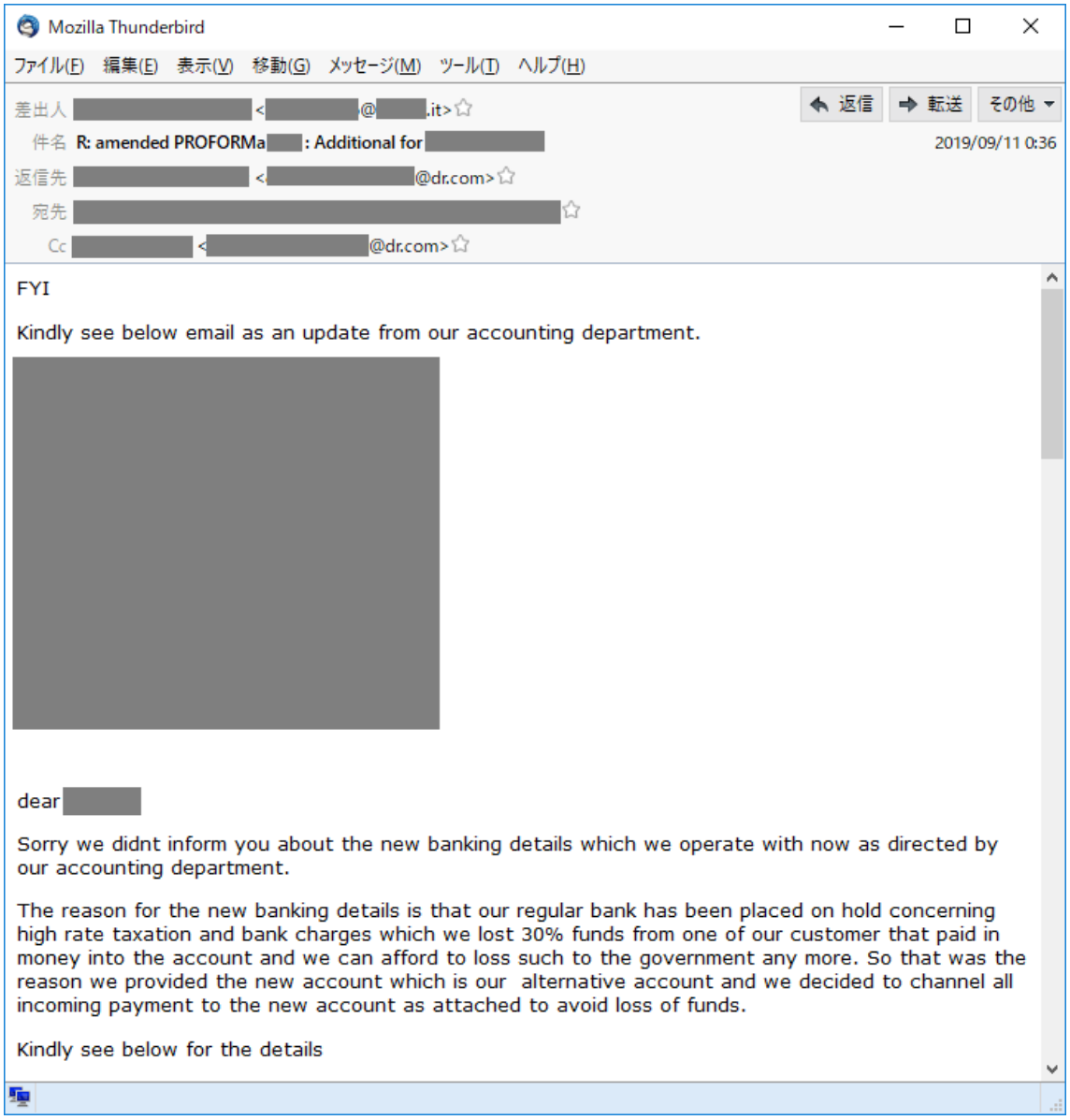

図 10 攻撃者からのメール 2 通目 (2019 年 9 月 11 日)

これら 2 通のメールを受け取った A 社担当者は、B 社担当者 2 になりすました攻撃者からのメール(1 通目)に対し、「次の支払いは新しい口座へ送金する」と連絡をしました。

その翌日(9 月 12 日)、攻撃者から支払いスケジュールを教えてほしいというメール(図 11)が着信しています。このメールへの返信として、A 社担当者は、「一部商品は確認中だが、9 月 18 日か 19 日に支払う予定」という内容のメールを送っています。

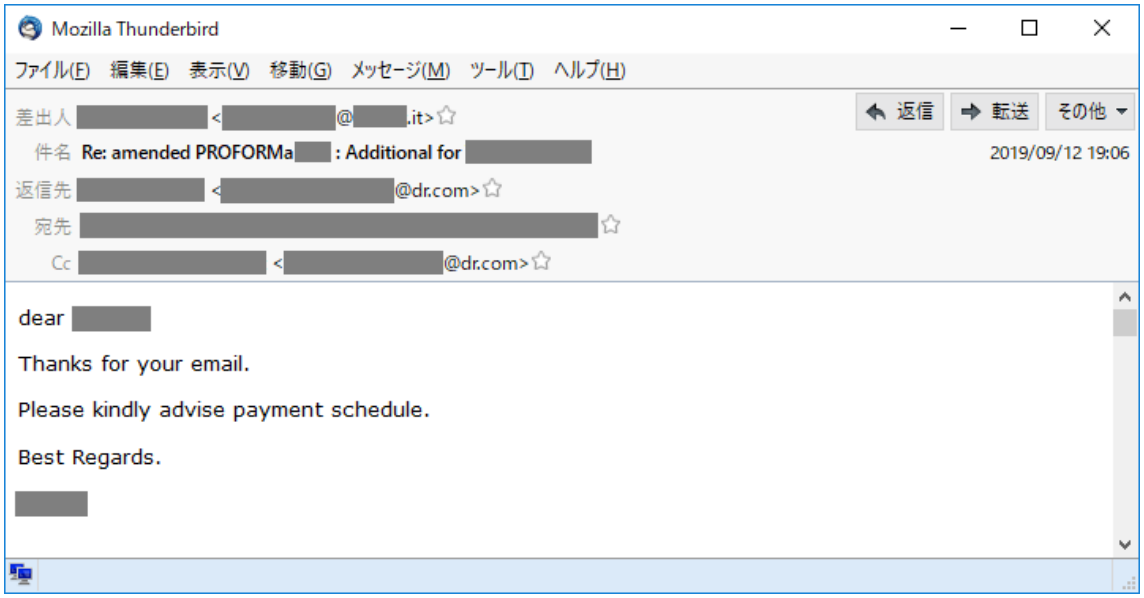

図 11 攻撃者からのメール 3 通目（2019 年 9 月 12 日）

その後、支払予定日である 9 月 18 日に攻撃者は、A 社担当者に対し、前回の連絡の通り、18 日か 19 日に支払いを依頼するという内容と、支払い後に支払書のコピーの送付を依頼するメール（図 12）を送り付けています。

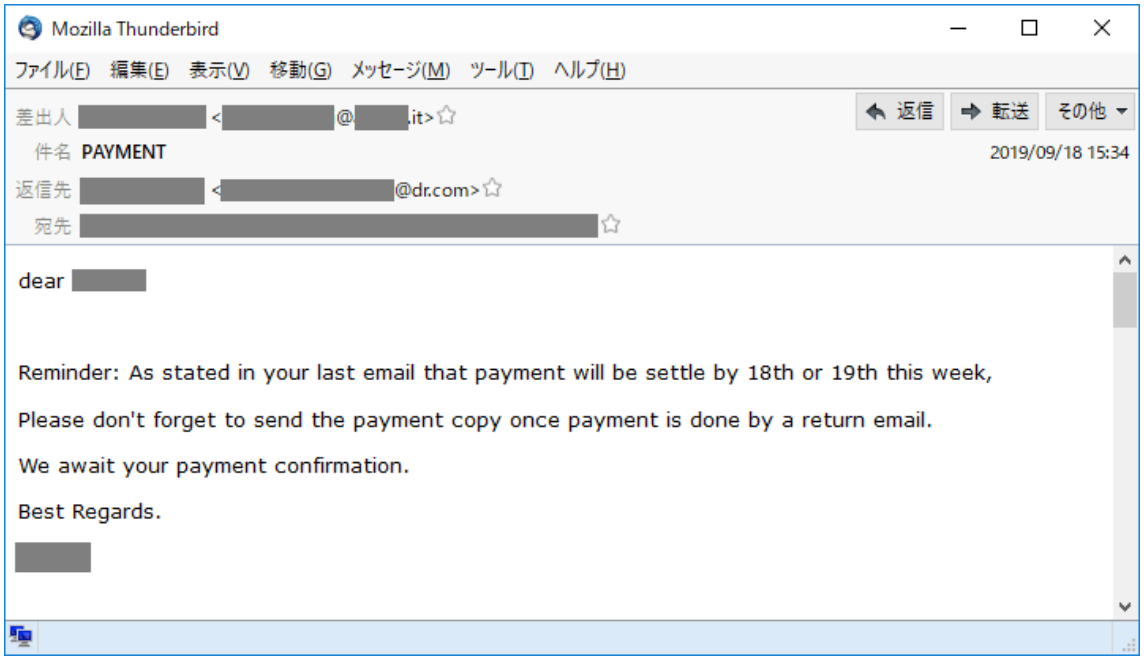

図 12 攻撃者からのメール 4 通目（2019 年 9 月 18 日）

A 社担当者は、日本時間の 9 月 20 日(金)に、国内の銀行から偽の口座に対して送金手続きを行いました。このとき、振込先の口座名のみ、正規の B 社の口座名を使って手続きを行っています。その後、銀行で発行された送金証明を添付し、「本決済は、次の月曜に行われる予定である」といった内容のメールを攻撃者へ送付しました。

また、同日正規の B 社担当者 1 から「貨物は受け取ったか」という問い合わせのメールが A 社担当者へ送付され、これに対して、A 社担当者は「まだ受け取っていない、貨物は 25 日に受け取る予定である」という連絡をやりとりしています。

これらのやりとりの後、9 月 25 日になり、B 社担当者 1 になりすました攻撃者から、「銀行から、支払を行った口座名が正しくないため、送金エラーとなったという連絡があった。資金が戻っているかもしれないので、すぐに銀行へ口座名の訂正連絡をしてほしい」というメール(図 13)が送られました。これは、A 社担当者が送金手続き時に口座名を攻撃者が指定した偽の口座名(C 社)ではなく、正しい B 社の口座名を指定していたために起こったものと推測されます。

なお、この 9 月 25 日のメールから攻撃者が送ってくるメールの偽メールアドレスが変更になっています。

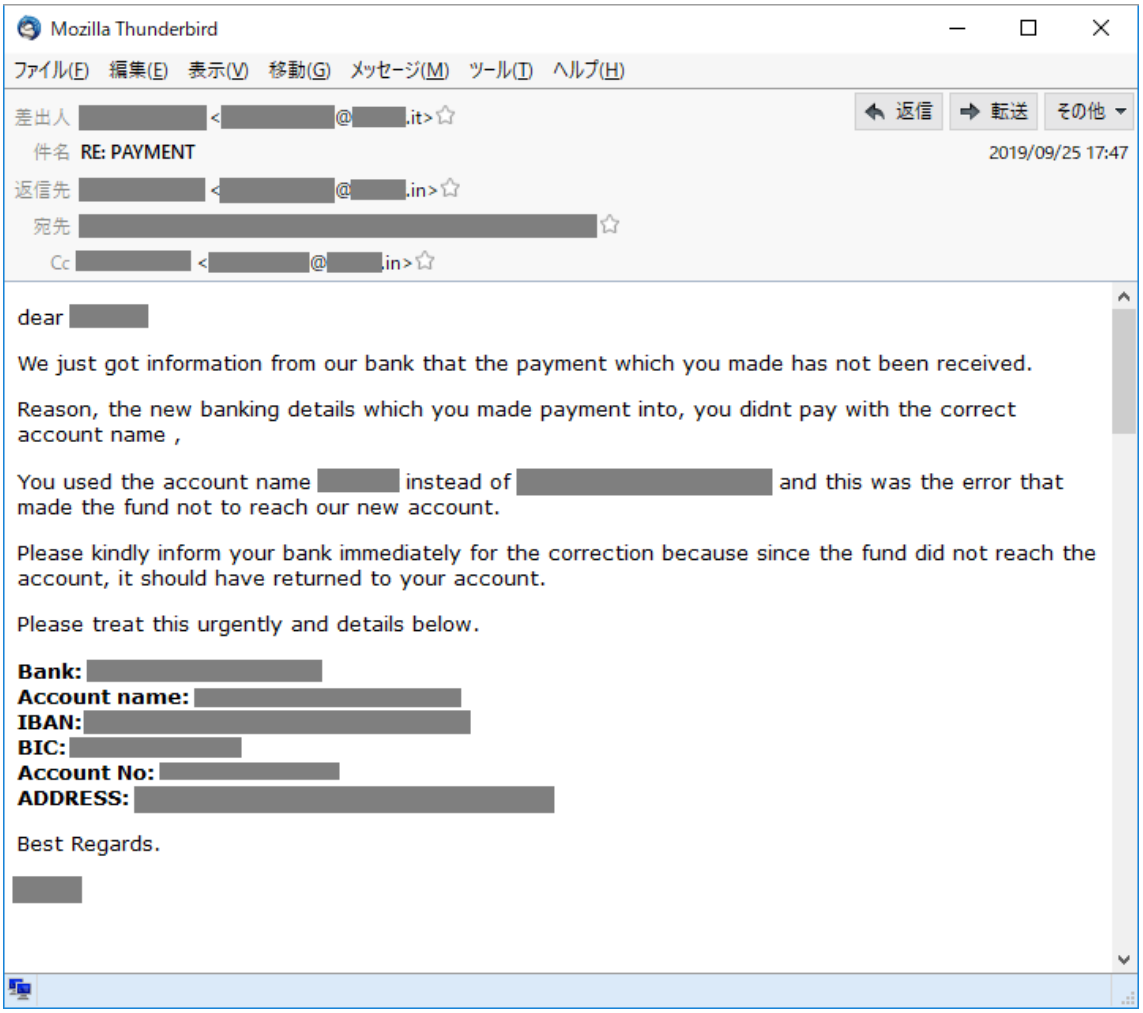

図 13 攻撃者からのメール 5 通目 (2019 年 9 月 25 日)

このメールに対し、A 社の担当者が、「なぜ口座名が別の企業名に変更になるのか」とメールを返信したところ、攻撃者から「新しい口座名の企業(C 社)は、B 社とジョイントパートナーシップを結んでいる会社である」という理由で、銀行へ訂正を依頼するメール(図 14)が送られました。

図 14 攻撃者からのメール 6 通目 (2019 年 9 月 25 日)

攻撃者から送られた 6 通目のメールの後、日本時間の 9 月 26 日の 0 時過ぎに、A 社担当者と、正規の B 社担当者 2 が電話にて連絡を取ったところ、一連のメールが詐欺メールであると発覚しました。その後、日本時間の 9 時過ぎに再度 B 社担当者 2 と電話を行い、このとき偽口座の凍結はできたが、資金が半分引き出されていたことが発覚しました。

偽口座への送金から、一部資金の損失と残金の回復については、別の章(4)で述べます。

その後、詐欺が発覚した後も、攻撃者は B 社担当者 2 になりすまし、残資金を詐取するべく偽のメールを送り付けてきましたが、A 社担当者は攻撃者へ一切返信を行っていません。

まず、9 月 27 日に、「銀行に資金があるか確認して返信をしてほしい」というメール(図 15)が A 社担当者へ送られました。

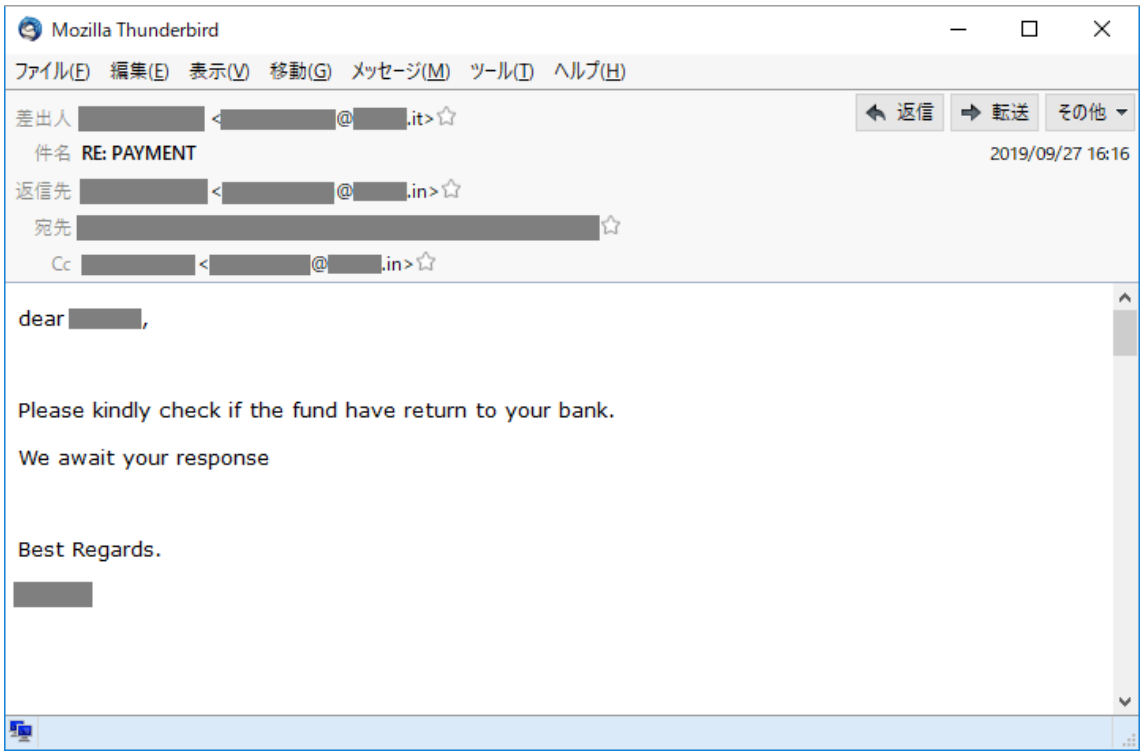

図 15 攻撃者からのメール 7 通目 (2019 年 9 月 27 日)

その後、9 月 30 日に攻撃者から、「以前連絡した銀行口座は無視して、タイの輸出/貿易で使っている口座を使うように経理部門から通知を受けたので、こちらに支払ってほしい」という内容の偽のメール(図 16)が送られました。

この時のメールから、再度攻撃者は偽のメールアドレスを変更しています。

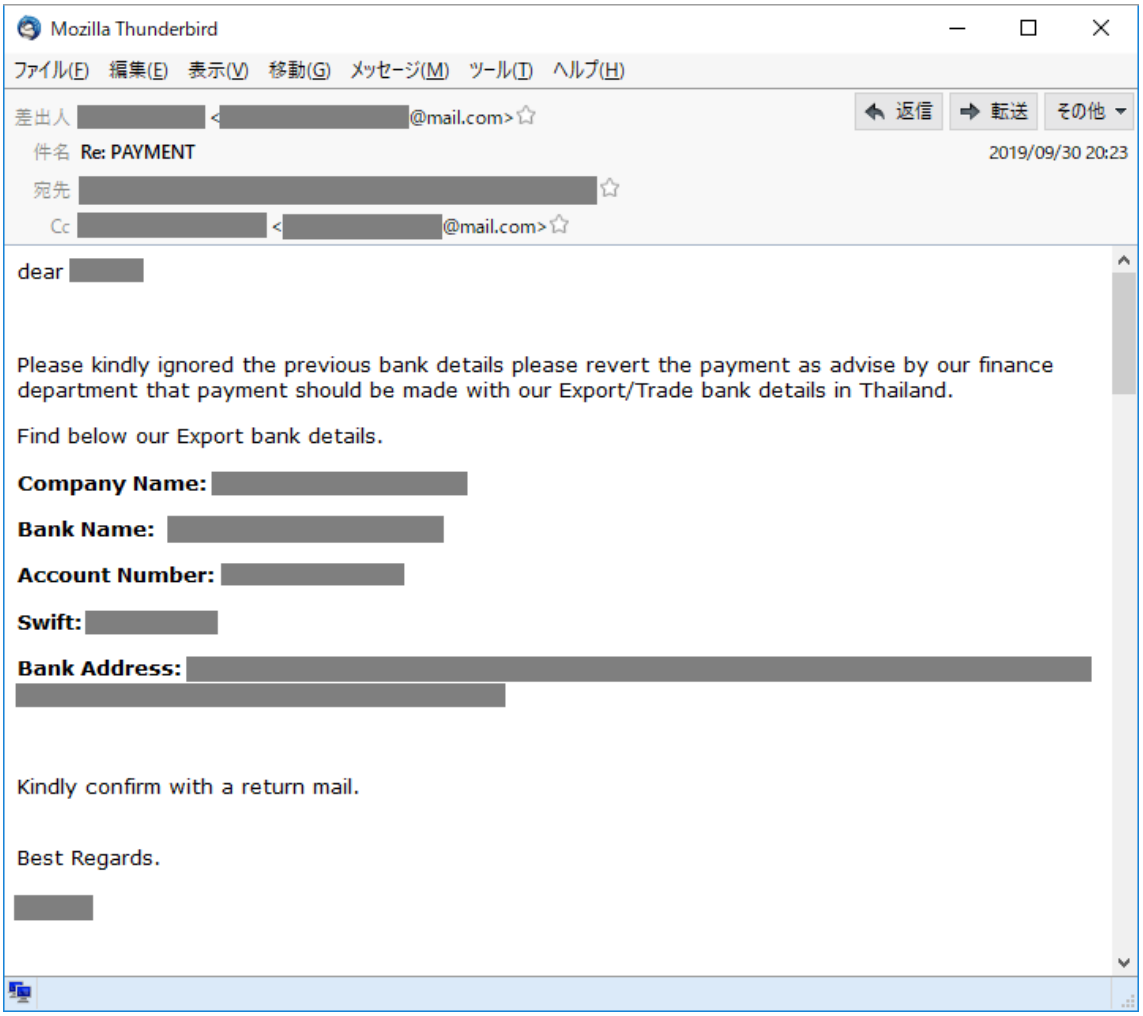

図 16 攻撃者からのメール 8 通目 (2019 年 9 月 30 日)

そして 10 月 1 日、攻撃者はさらに本件とは全く関連のない、人物(ハッカー)になりすまし、「銀行口座はハッキングされているので、なるべく早く連絡をしてほしい」といったメール(図 17)を A 社担当者へ送り付けてきました。

このメールの差出人(From ヘッダ)にはハッカーになりすましたと思われる人物の名前とメールアドレスが設定されていましたが、返信先(Reply-To ヘッダ)には 9 月 30 日に送られた B 社担当者 2 になりすました偽のメールアドレスが設定されていました。このため、攻撃者は A 社担当者の不安を煽るためにハッカーになりすましたメールを送ってきたものと推測しています。

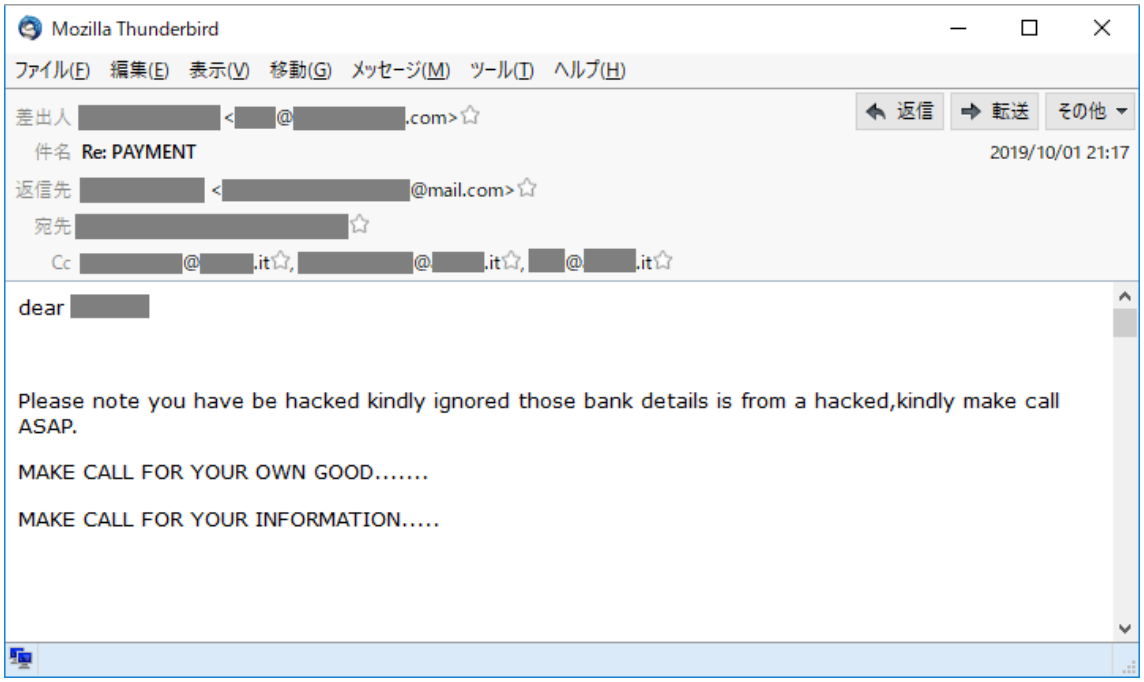

図 17 攻撃者からのメール 9 通目（2019 年 10 月 1 日）

4.　偽口座に残る資金回復に至る対応

2019 年 9 月 26 日に、B 社から A 社に対して、偽口座へ送金した資金の約半額が攻撃者によって引き出され、口座の凍結には成功したと連絡があってから、資金回復に至るまでの各社の対応について説明します。

2019 年 9 月 20 日、A 社担当者は、攻撃者から送られた偽の口座へ向けて、送金手続きを実施しました。このとき、A 社担当者は口座名のみ正しい B 社の口座名を指定し、その他の送金手続きに必要な項目は偽の口座情報で手続きを行っています。なお、9 月 20 日は金曜日であり、国内銀行での送金処理は 9 月 24 日の火曜日に行われたものと推測しています（2019 年 9 月 23 日月曜日は、秋分の日の祝日であるため）。

その後、9 月 26 日の夜に A 社担当者と、B 社担当者 2 で電話による会話の中で詐欺であることが発覚し、26 日の朝（銀行が開店後）に B 社担当者 2 から偽口座の銀行へ口座の凍結依頼と、イタリアの現地警察への通報を行っています。しかし、すでに偽口座からは資金の半額が引き出された後であったため、攻撃者は 9 月 24 日から 25 日にかけて偽口座から資金を引き出したものと推測しています。

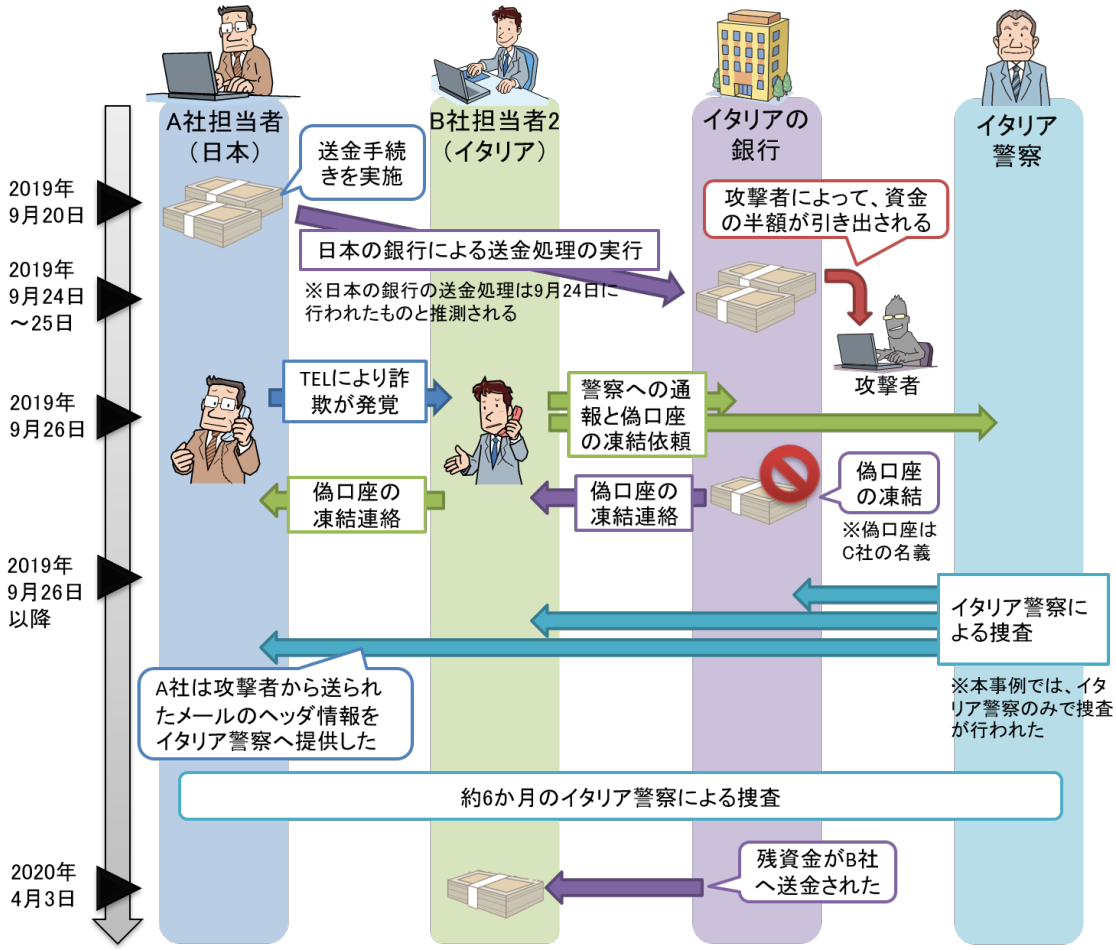

図 18 残資金回復までのやりとり

偽口座については、残資金が残っている状態で凍結され、その情報は B 社担当者 2 経由で A 社担当者の元へ 9 月 26 日に連絡されました。以降、イタリア警察による捜査が、約 6 か月に渡り行われました。この事例では、すべての捜査がイタリア内で行われましたが、A 社担当者は、イタリア警察に攻撃者から送られたメールのヘッダ情報を提出しています。

その後、イタリア警察による捜査が 2020 年 4 月 3 日に完了し、偽口座に残された資金については、B 社の元へ送金される形で残資金の回復が行われました。

本事例では、支払側である日本企業の A 社ではなく、請求側である B 社主導の元、イタリア内で捜査が行われました。支払側が直接金銭被害を受けるため、警察への相談や捜査についても支払側が主導するものと思われますが、ビジネスメール詐欺ではメールの盗み見の原因調査等、双方の企業が協力して行わなければならないため、本件の事例のように、お互いに協力して対応していくことが望ましいでしょう。

5. 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。

- 複数の偽メールアドレスの使用
- 返信先(Reply-To ヘッダ)の悪用
- 同報(CC)メールアドレスの改変
- メールの引用部分の改変

これらの攻撃手口は、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手口でした。

5.1. 複数の偽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、3 つの偽のメールアドレスを使用していました。

説明のため、本物のメールアドレスを次のようにした場合で説明します。

【本物のメールアドレス】 alice @ b-company . it

表 2 偽物のメールアドレスのパターン

項番	偽物のメールアドレスパターン	攻撃に使われた期間
1	alice @ dr.com	2019 年 5 月 15 日～9 月 18 日
2	alice @ b-company . in	2019 年 9 月 25 日～9 月 27 日
3	alice.b-company.it @ mail.com	2019 年 9 月 30 日～10 月 1 日

項番 1 と 3 のメールアドレスは、「mail.com[1]」という、海外のサービスで無料取得できるドメインのものでした。このサービスから取得されたフリーメールアドレスを使ったビジネスメール詐欺については本事例以外にも複数の攻撃事例で確認しています。当該サービスで取得可能なメールアドレスから送付されるメールには注意を払っておくことが望ましいと考えます。

[1] 2022/7 時点で、当該サービスでは 191 のドメインから選択してメールアドレスを取得することが可能です。

項番 2 のメールアドレスは、本物のメールアドレスから、トップレベルドメイン（TLD[2]）を変更したメールアドレスであり、偽のメールが送られる当日（2019/9/25）に取得されたものでした。これは、不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられます。

また、項番 2 のメールアドレスのドメインをウイルスの不正接続先として使った攻撃を、2019/11 から 2020/8 の期間で複数件観測しており、BEC との関連性は不明ながら、攻撃者は一度取得した偽のドメインを別の攻撃で使い回しているということも考えられます。

5.2. 返信先(Reply-To ヘッダ)の悪用

攻撃者は、B 社担当者になりすまして、A 社担当者へなりすましメールを送る際、メールの返信先（Reply-To ヘッダ）に次のようなメールアドレスを設定し、細工を行っていました。

Reply-To: B 社担当者の本物の表示名 〈偽物のメールアドレス〉

このように細工された状態では、受信者が「返信」ボタンをクリックするなどして、そのメールへの返信メールを作成すると、メールの作成画面では、差出人（From）ではなく、Reply-To ヘッダに設定した偽物のメールアドレス（2.5.1 の表 2 で示したメールアドレス）が宛先となります。ただし、表示名の部分には B 社担当者の本物の名前が表示されます。攻撃者は A 社担当者に対し、メールが本物であると錯覚させつつ、実際のメールのやりとりは B 社担当者本人に届かないようにして、攻撃を行っていたものと思われます。

5.3. 同報(CC)メールアドレスの改変

攻撃者が B 社担当者になりすまして A 社の担当者へ送り付けた偽のメールでは、同報先（Cc）に指定した、B 社担当者のメールアドレスを偽のメールアドレスに改変していました。

同報されているメールアドレスを改変することで、メール受信者にとっては、自分以外の多くの関係者が宛先に入っているように見える（衆人環視の中でのやりとりに見える）が、実際には攻撃者が狙ったメール受信者のみに送られており、メール受信者は騙されていることに気づきにくくなります。また、本来の同報先には、この偽メールが届かないため、詐欺が行われていることに気づくことができません。

[2] Top Level Domain（トップレベルドメイン）。ドメイン名のもっとも右側に記載されている文字列。「.jp」のような各国／地域に割り当てられた TLD には、1 文字違いのものも多く存在します。

5.4. メールの引用部分の改変

攻撃者は、A 社と入金確認に関するメールをやりとりする際、メールの過去のやり取り部分（引用部分）も改変していました。

メールソフトによっては、過去のメールを引用すると、メール本文以外に、差出人（From）、宛先（To）、同報先（Cc）、件名（Subject）といった、メールのヘッダ情報も併せて記載されることがありますが、攻撃者はこれらの情報を削除し、過去のやりとり部分でメールヘッダの確認をさせないようにしていました。

この細工も、これまでの手口と同じく、A 社担当者に偽のメールであると気づかせにくくする狙いがあるものと考えられます。

また、不審だと見破って調査を行う際にも、引用部分にあるメールのやりとりの経緯は信用できない前提で対応する必要があります。どこから本物と偽物（攻撃者）が入れ替わったのかを特定するためには、過去のメールも可能な限り回収し、調査する必要があるでしょう。

以上