J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan

【添付資料】
ビジネスメール詐欺の事例から見る騙しの手口

ビジネスメール詐欺「BEC」に関する事例と注意喚起

～ サイバー情報共有イニシアティブ（J-CSIP）の活動より ～

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

【添付資料】 ビジネスメール詐欺の事例から見る騙しの手口

ビジネスメール詐欺「BEC」に関する事例と注意喚起
～ サイバー情報共有イニシアティブ（J-CSIP）の活動より ～

目次

【添付資料】 ビジネスメール詐欺の事例から見る騙しの手口

ビジネスメール詐欺「BEC」に関する事例と注意喚起

～ サイバー情報共有イニシアティブ(J-CSIP)の活動より ～

2017 年 4 月 3 日
IPA(独立行政法人情報処理推進機構)
技術本部 セキュリティセンター

本書は、J-CSIP の活動の中で参加組織より情報提供をいただいた、ビジネスメール詐欺(BEC)の 4 つの事例について説明する添付資料です。各事例は、レポート本紙の 2 章で概要を記しています。

本書では、それぞれの事例の内容や攻撃の経緯を、一部詳細に、また攻撃で使われた騙しの手口の解説を交えて紹介します。なお、偽のメールアドレスの細工など、事例を越えて同じような手口が使われていることもありますが、省略することなく説明しています。

1. 事例 1 で使われた攻撃手口

事例 1 では、詐欺の過程において、次の 4 点の手口が使われました。

（1） 偽の口座を伝えて振り込ませる
（2） 言い回しを変えての振り込み要求
（3） 詐称用ドメインによる B 社へのなりすまし
（4） 同報のメールアドレスを改変し、関係者にメールが届かないようにする

上記 （1）、（2）の手口が詐欺の本質的な部分（金銭の詐取）ですが、これを成功させるため、あるいは発覚を遅らせるために、（3）、（4）の手口が併用されたと思われます。

本事例では、被害は発生していませんが、時間をおいて 2 回のビジネスメール詐欺による攻撃がありました。A 社と B 社でのやりとりは 2 件とも同一人物間で行われていたもので、攻撃者は同一の人物になりすましています。攻撃者は、一度失敗しても、やり方を変えて攻撃を仕掛けてきたということになります。

1.1. 攻撃手口（1）- 偽の口座を伝えて振り込ませる

本事例は、2015 年 12 月、A 社と B 社（本物）が正規の請求書のやりとりを行った後に、攻撃者によって偽の口座への振り込みが要求されるという手口でした。

攻撃者が行った、偽の口座への振り込み要求の流れを次に示します。

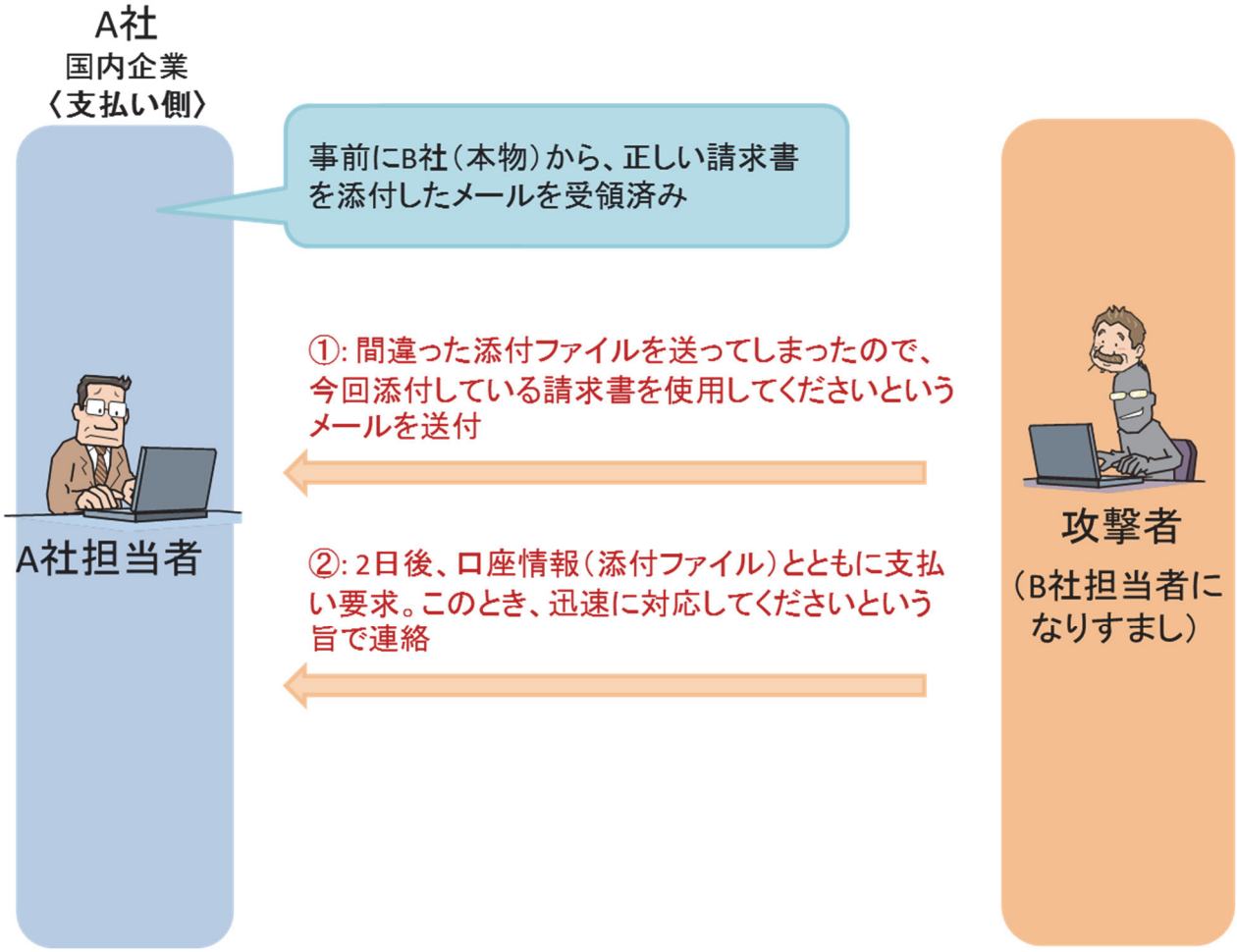

図 1-1 事例 1：2015 年 12 月のやりとりにおける振り込み要求の流れ

これは、ビジネスメール詐欺で最も一般的に使用されうる手口と思われます。攻撃者は、B 社の担当者になりすまし、「A 社と B 社（本物）が取り交わした請求書に誤りがあった」と連絡し、攻撃者の用意した偽の口座へ振り込みを要求しています。

1.2. 攻撃手口（2）- 言い回しを変えての振り込み要求

この攻撃者は、攻撃手口(1)で行った振り込み要求に加えて、2016 年 1 月に、再び別の請求事項についても偽の口座への振り込み要求を試みています。その攻撃の流れを次に示します。

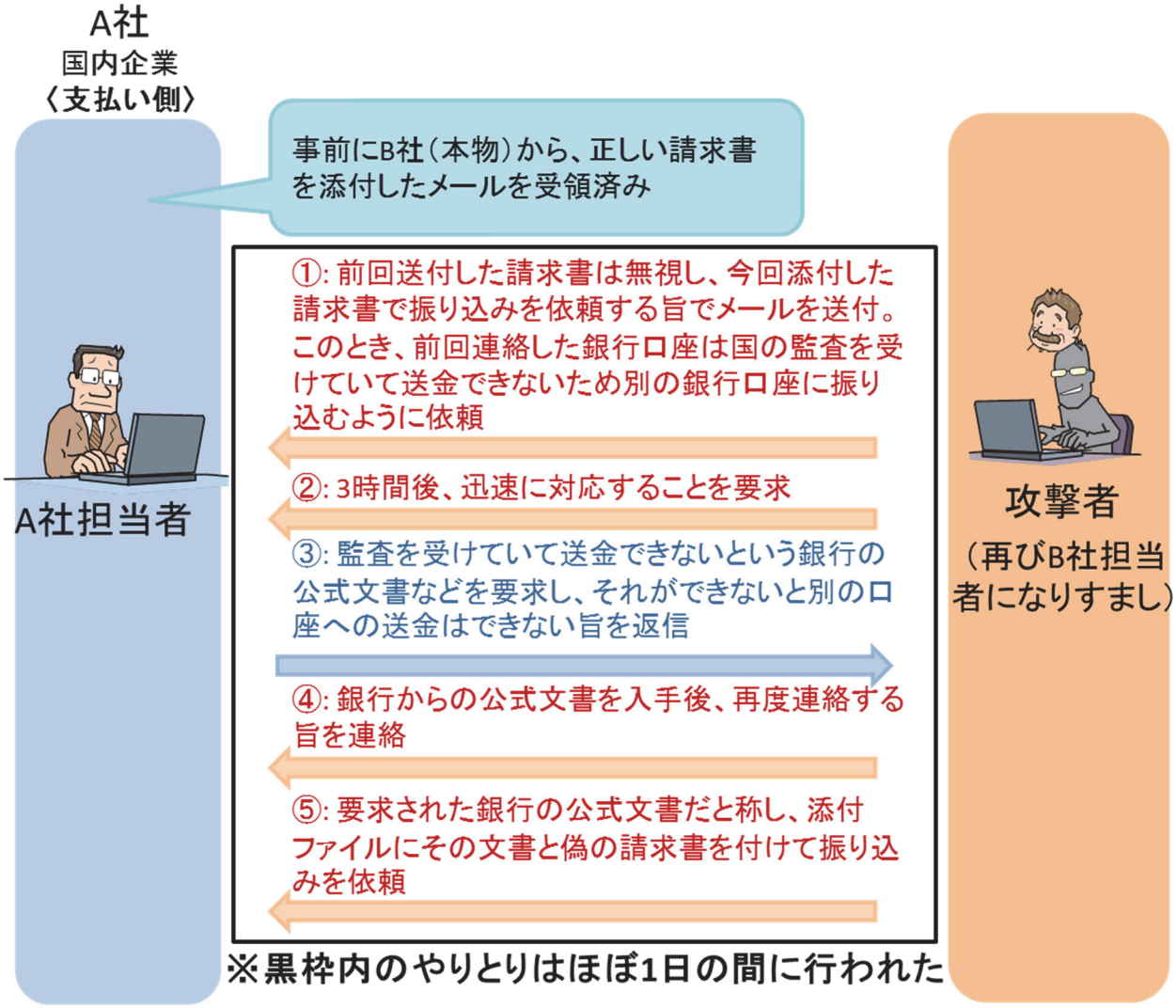

図 1-2 事例 1:2016 年 1 月のやりとりにおける振り込み要求の流れ

B 社の担当者になりすましている点は攻撃手口(1)と同じですが、この攻撃では、「銀行口座が国の監査を受けているため振り込みができない」という理由をつけて、偽の口座への支払いを要求してきました(図 1-2 ①)。

このとき、A 社から「銀行の正式な文書がなければ社内のルール上振り込み先を変更することはできない」という旨を連絡(図 1-2 ③)すると、攻撃者からは、その文書だと称した偽のファイルが送付されてきました(図 1-2 ⑤)。

この一連のやりとりは、**ほぼ 1 日の間に行われました**。攻撃者は非常に手際よく詐欺を仕掛けてくることが分かります。

なお、攻撃者は、攻撃手口(1)と同一の人物を装っていましたが、別のメールアドレスを使ってこの攻撃を行っています。

1.3. 攻撃手口（3）- 詐称用ドメインによるB社へのなりすまし

本事例の 2 件のメールのやりとりにおいて、攻撃者は次のような「詐称用ドメイン」を使い、B 社へのなりすましを行いました。

◆ **2015 年 12 月のやりとりにおける B 社のなりすまし**

1 件目の攻撃の際、攻撃者がなりすましに使用したメールアドレスは、次の例に示すように、本物のメールアドレスのドメイン部分から、アルファベット **1 文字が逆になっている**ものでした。この例では、仮に、本物のメールアドレスのドメイン名を「company-a . com」としています。

図 1-3 2015 年 12 月のやりとりにおける詐称用ドメインの例

◆ **2016 年 1 月のやりとりにおける B 社のなりすまし**

2 件目の攻撃の際、攻撃者がなりすましに使用したメールアドレスは、次の例に示すように、本物のメールアドレスのドメイン部分から、アルファベット **1 文字を逆にし、末尾に 1 文字を追加したもの**でした。

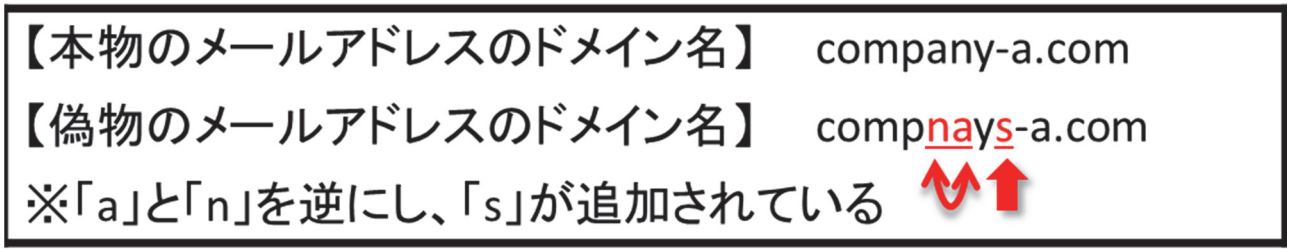

図 1-4 2016 年 1 月のやりとりにおける詐称用ドメインの例

◆ **B 社のなりすましに使用された 2 つの「詐称用ドメイン」**

2 件の攻撃で使用された 2 つの「詐称用ドメイン」は、それぞれの偽メールが送信された時期に、攻撃者と思われる同一人物によって取得されていた形跡が、ドメイン登録情報（whois 情報）から確認できています。

攻撃者は、ビジネスメール詐欺を行う際、何らかの方法でなりすましをする必要がありますが、この事例のように**「詐称用ドメイン」を次々と取得し、攻撃を仕掛けてくる**という様子が伺えます。

1.4. 攻撃手口（4）- 同報のメールアドレスを改変

攻撃手口(3) で、攻撃者は B 社の担当者になりすました上でメールを送信しています。

この際、詐欺が行われていることの発覚を遅らせるため、あるいは受信者がメールを偽物だと見破りにくくするため、攻撃者は同報先（Cc）にある B 社の別の担当者のメールアドレスについても、偽のメールアドレスを設定していました。

これにより、メールを受信した A 社の担当者から見ると、あたかも B 社の複数の担当者が Cc に入った状態で自社へメールが届いているかのように見えますが、**実際には、このメールはＢ社の担当者にはひとりとして届いておらず、詐欺を行っていることに気付かれにくい**ように細工されています。

元々は A 社とＢ社との間で、それぞれ複数の従業員が宛先に入ったメールで請求と支払いに関するメールを授受していましたが、攻撃者がなりすましをして送ってきたメールでは、攻撃手口（3)と同じように B 社の同報メールアドレスを改変していました。また、メールソフトによって表示される表示名は、本物の B 社担当者の名前が表示されるように細工していました。

この手口について、次の登場人物とそれぞれの役割、メールアドレスを例として説明します。

登場人物はＡ社とＢ社、それぞれ３名の実在する職員がいるものとします。Ａ社は支払側であり、「alice」が支払に係る主担当者、Ｂ 社は請求側であり、「dave」が請求主担当者であるとします。攻撃者は、Ｂ 社の「dave」になりすますため、「dave」のメールアドレスによく似た、偽のメールアドレスを用いるものとします。

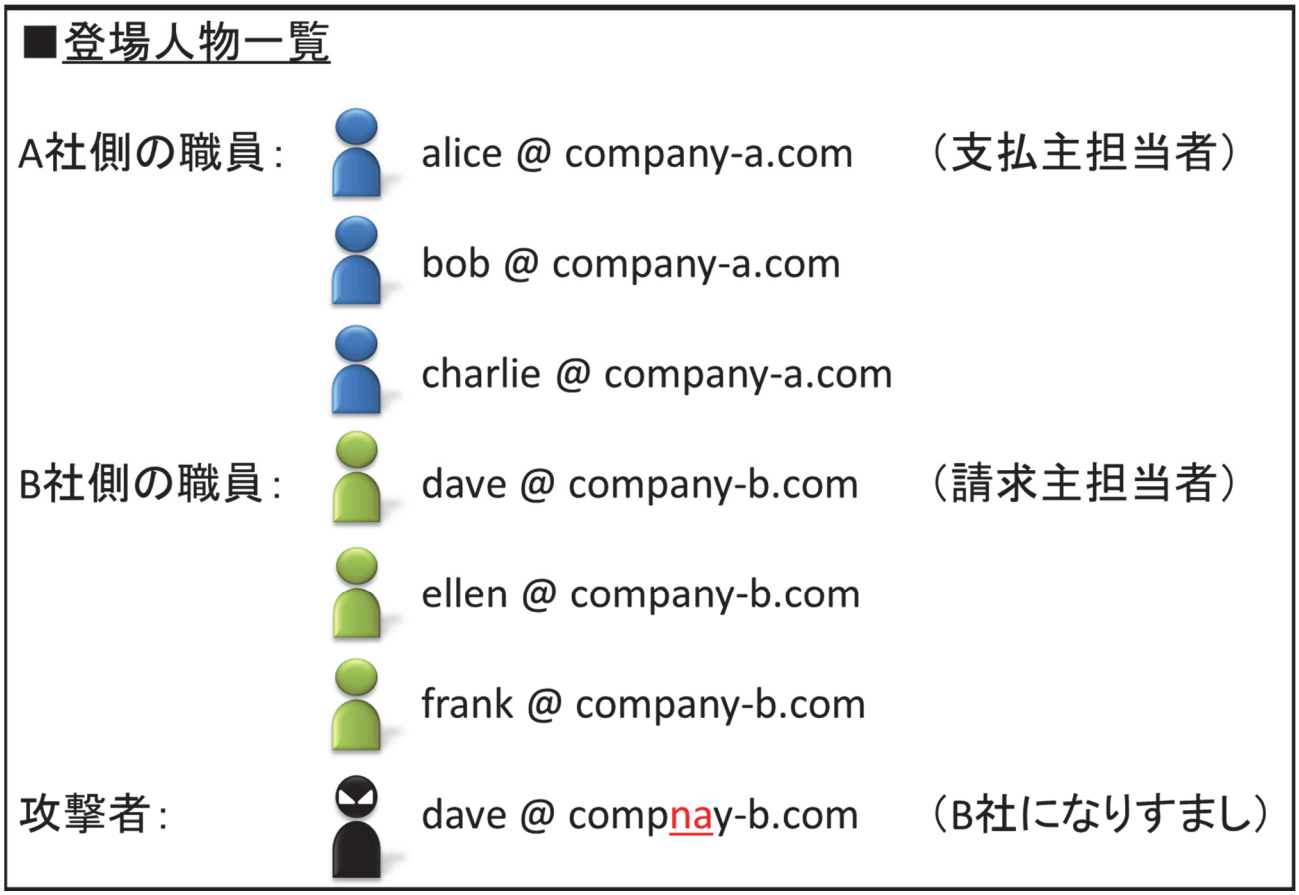

図 1-5 登場人物

このとき、正常な状況ではＢ社からＡ社へ、請求に係る内容のメールが送付された場合、次のようなメールになるでしょう。

送信元（From）は請求の主担当者である Ｂ 社の「dave」、宛先（To）は支払いの主担当者である Ａ 社の「alice」へのメールです。同報先（Cc）には、Ａ社とＢ社の複数の関係者のメールアドレスが含まれます。

図 1-6 正規のメール例

1 件目、2015 年 12 月のやりとりでは、攻撃者は図 1-3 に示す例のように、B 社のなりすましのメールアドレスを使ってメールを送ってきました。**このとき、Cc に含まれている B 社の関係者(「ellen」と「frank」)のメールアドレスのドメイン部分も同じように改変していました。**

これによって、B 社の関係者には、この偽メールが一切届かないことになります。この状態で、A 社の担当者(alice)がメールを全員返信したとしても、B 社関係者にはメールが届かないため、攻撃に気付きにくい状況になっています。

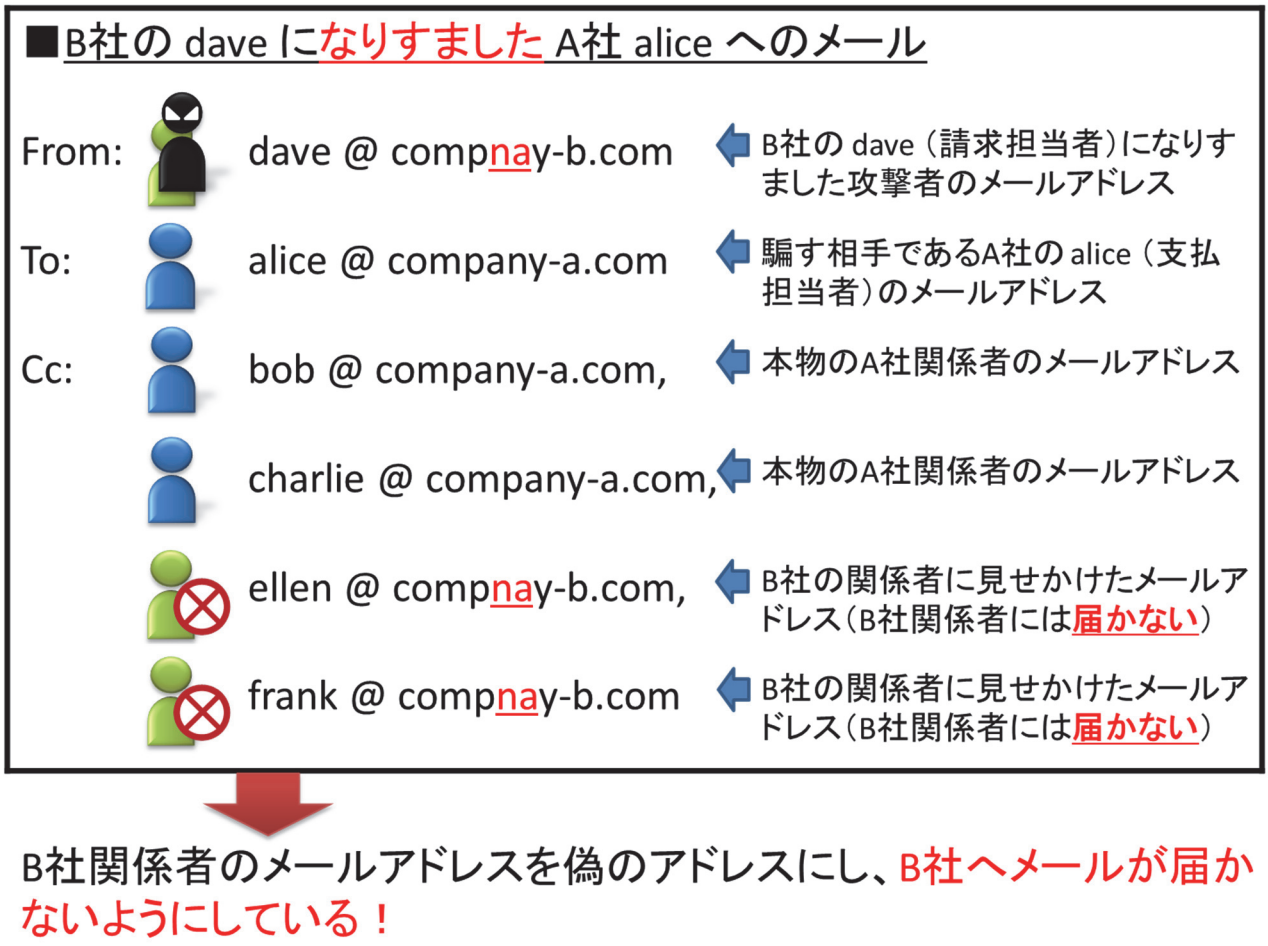

図 1-7 事例 1:2015 年 12 月のやりとりにおける同報メールアドレスの改変の様子

2 件目、2016 年 1 月のやりとりでも、攻撃者は図 1-4 に示したなりすましのメールアドレスを使ってメールを送ってきました。このとき、やはり Cc に含まれている B 社の関係者（「ellen」と「frank」）のメールアドレスのドメイン部分も同じように改変していました。

これによって、1 件目と同様に、B 社の関係者にはこの偽メールが届かないようになっており、攻撃に気付きにくい状況になっています。

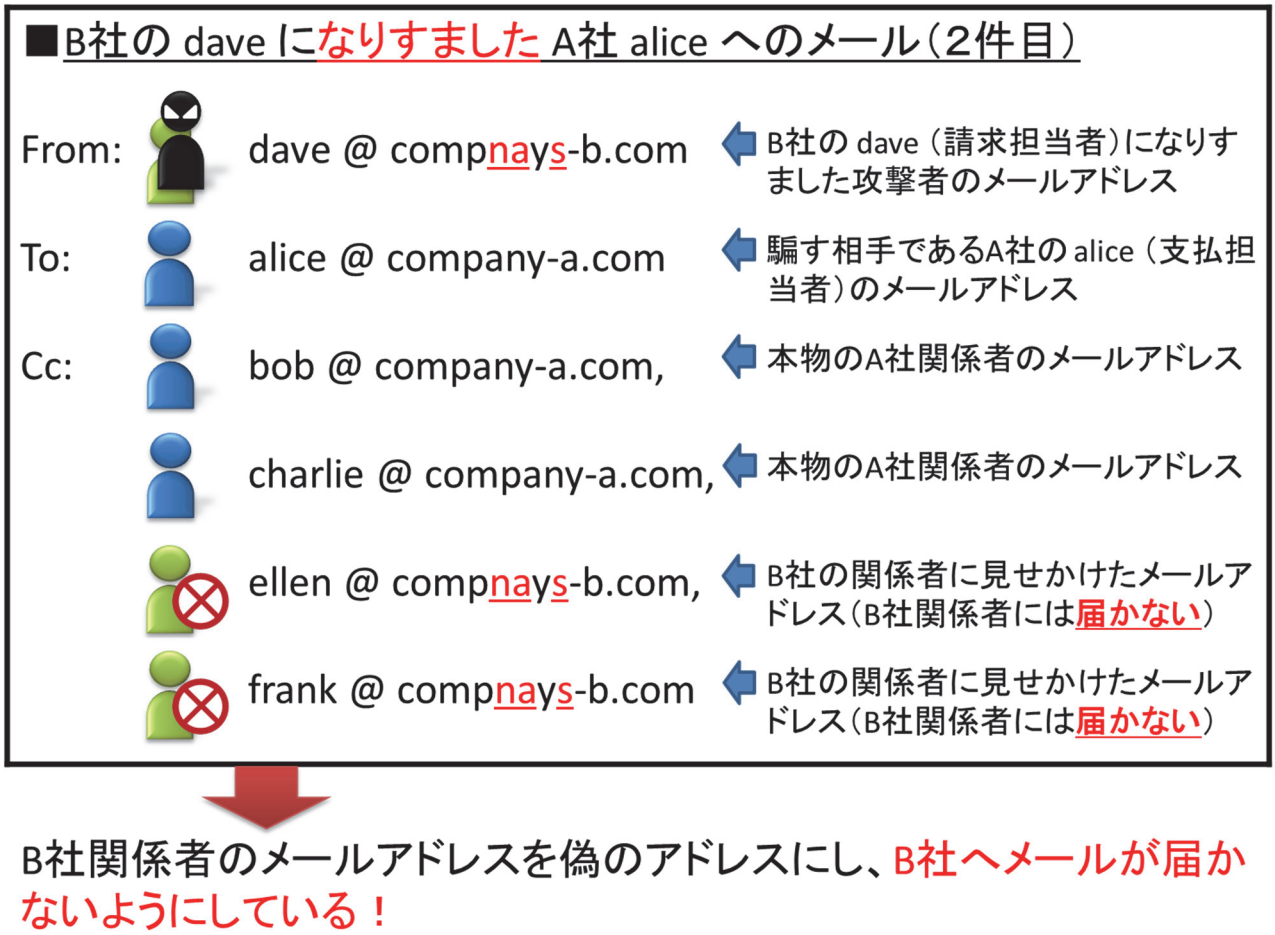

図 1-8 事例 1：2016 年 1 月のやりとりにおける同報メールアドレスの改変の様子

ビジネスメール詐欺において、攻撃者は、メールの文面のみならず、詐欺が発覚しないように様々な細工を施してきます。詐称用ドメインの使用や、同報先メールアドレスの改変は他の事例でも確認しており、単純な手口のように見えますが、「このような攻撃方法がある」と意識していなければ、見逃してしまう可能性があると思われます。

2. 事例 2 で使われた攻撃手口

事例 2 では、詐欺の過程において、次の 4 点の手口が使われました。

（1） 偽の口座を伝えて振り込ませる
（2） A 社と B 社の両方になりすまし、それぞれに偽のメールを送る
（3） 同報のメールアドレスを改変し、関係者にメールが届かないようにする
（4） メールの引用部分で攻撃者に都合が悪い部分を改変する

上記 （1） の手口が詐欺の本質的な部分（金銭の詐取）ですが、これを成功させ、あるいは発覚を遅らせるために、（2）、（3）、（4） の手口が併用されたと思われます。

また、本事例では、最後に攻撃者からのメッセージと思われるようなメールが送られてきていることが特徴的です。

2.1. 攻撃手口(1) - 偽の口座への振り込み要求

本事例は、2015 年 8 月、A 社と B 社（本物）が、複数ある正規の請求書の支払いに係るやりとりを行った後に、攻撃者によって偽の口座への振り込み要求がなされるという手口でした。

攻撃者が行った、偽の口座への振り込み要求の流れを次に示します。

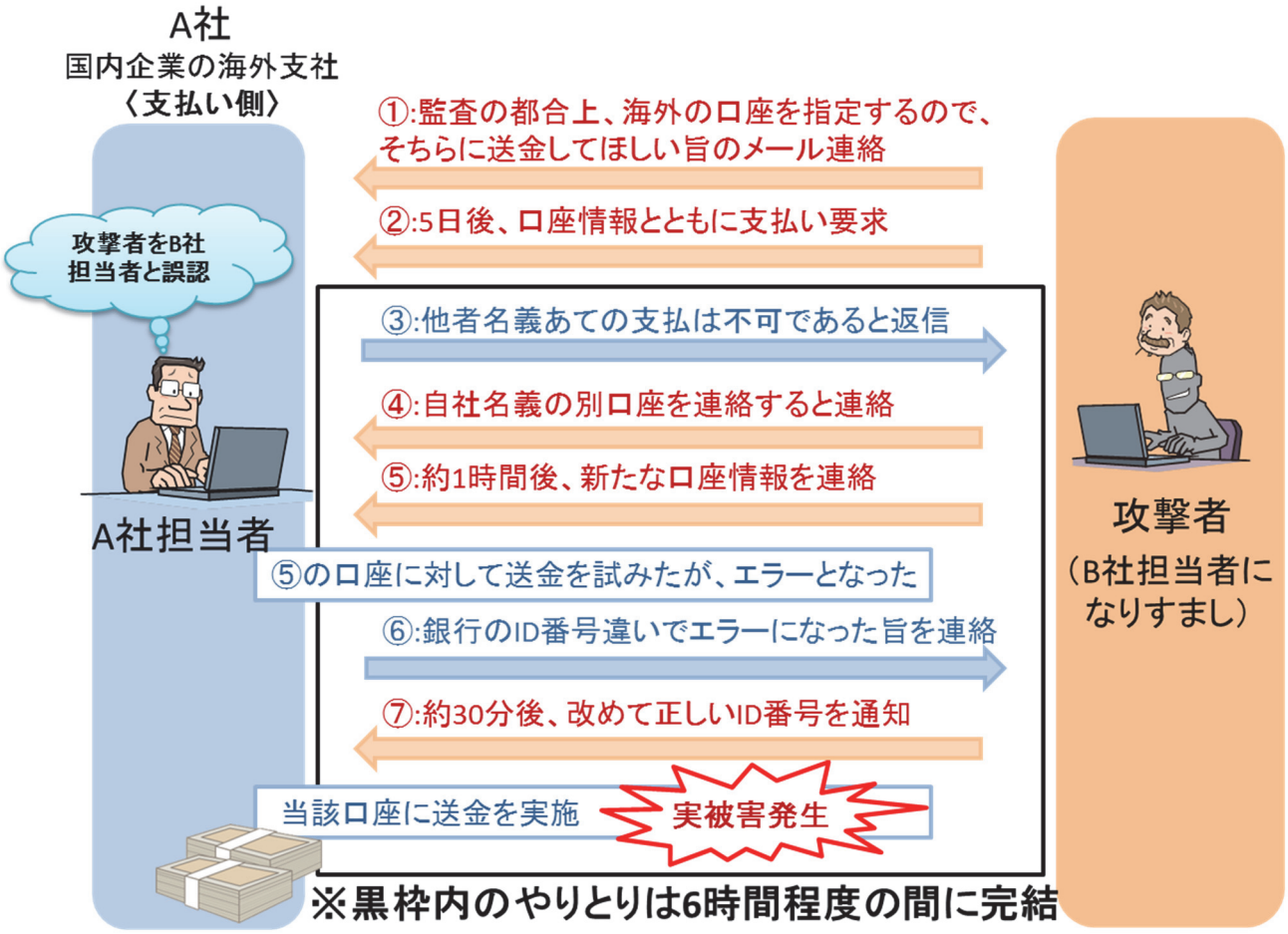

図 2-1 事例 2:振り込み要求の概要

攻撃者の騙しの手口自体は、B 社になりすまし、A 社に対して「監査の都合上」というもっともらしい理由をつけて偽の口座情報を伝え、その口座への支払いを要求するという単純なものでした。しかし、**実際に支払い処理の段階（図 2-1 の黒枠内のやりとり）に入った後の攻撃者の対応が速い**ことが特徴的です。

特に、図 2-1 の⑤において連絡してきた攻撃者の別口座の情報は、対応の速さからあらかじめ予備などの目的で確保していたと思われ、攻撃者の用意周到さが垣間見えるものでした。

また、銀行の ID 番号違い（国内用と国際用の違いによる）でエラーが発生した旨の連絡を受けた際（図 2-1 の⑥）には、メールでの連絡にも関わらず、**確認から折り返しまで約 30 分で回答していることから、攻撃者はまさしく張り付きの状態で攻撃していた**と思われます。

こういった攻撃者の迅速な対応が、A 社に本物の B 社への事実確認をとる隙を与えなかったことに繋がり、攻撃者の当該口座に送金してしまうという実被害にまで至ったものと考えられます。

2.2. 攻撃手口(2) - A 社と B 社の両方になりすまし

A 社は、期日が過ぎている請求分は支払いが済んでいるという認識、かつ B 社は期日を過ぎても支払いが行われていないという認識の状況で、攻撃者は次のように振る舞いました。

◆ A 社のなりすまし

攻撃者は A 社の人物になりすまし、B 社に対し、「支払いの事実関係を確認中であり、しばらく待つよう」に依頼しました。これは、詐欺の発覚を遅らせようとしたものと思われます。

◆ B 社のなりすまし

攻撃者は B 社の人物になりすまし、A 社に対して、「支払いの確認ができていない分だけでなく、これから支払期限が到来する別の請求についても、次の支払いのタイミングで同時に（前倒しで）支払うよう」要求していました。これは、より多くの金銭を詐取しようと画策したものと思われます。

なお、この際攻撃者がなりすましに使用したメールアドレスは、以下に示すように、**本物のメールアドレスに近いものをフリーメールで取得したもの**でした。ここでは仮に、悪用されたフリーメールサービスのドメインを「freemail . com」としています。

図 2-2 事例 2 におけるメールアドレスの偽装例

2.3. 攻撃手口(3) - 同報のメールアドレスを改変

攻撃手口(2) で、攻撃者は A 社と B 社の人物になりすました上でメールを送信しています。

この際、詐欺が行われていることの発覚を遅らせるため、あるいは受信者がメールを偽物だと見破りにくくするため、攻撃者はメールの Cc にある送り先の部分をすべて偽のメールアドレスに改変していました。

これにより、メールを受信した A 社の担当者から見ると、あたかも送金取引に関連する担当者が Cc に入った状態のように見えますが、**実際には、このメールは A 社の担当者以外にはひとりとして届いておらず、騙されていることに気付きにくいように細工しています。**送金取引に関連する担当者には、攻撃者の偽メールが届いていないため、詐欺が進行中であることに気付くことはできません。

本事例では、元々は A 社と B 社との間で、それぞれ複数の従業員が宛先に入ったメールで請求と支払いに関するメールを授受していましたが、攻撃者がなりすましをして送ってきたメールでは、その大多数のメールアドレスについて、アルファベットを 1 文字追加する手口によって改変されていました。

なお、事例 1 とは、メールアドレスのドメイン部分には改変を加えていない点が異なっています。

この手口について、次のような登場人物とそれぞれの役割、メールアドレスを例として説明します。

登場人物はＡ社とＢ社、それぞれ３名の実在する職員がいるものとします。Ａ社は支払側であり、「alice」が支払に係る主担当者、Ｂ 社は請求側であり、「dave」が請求主担当者であるとします。攻撃者は、Ｂ 社の「dave」になりすますため、「dave」のメールアドレスに近いものをフリーメールで取得した、偽のメールアドレスを用いるものとします。

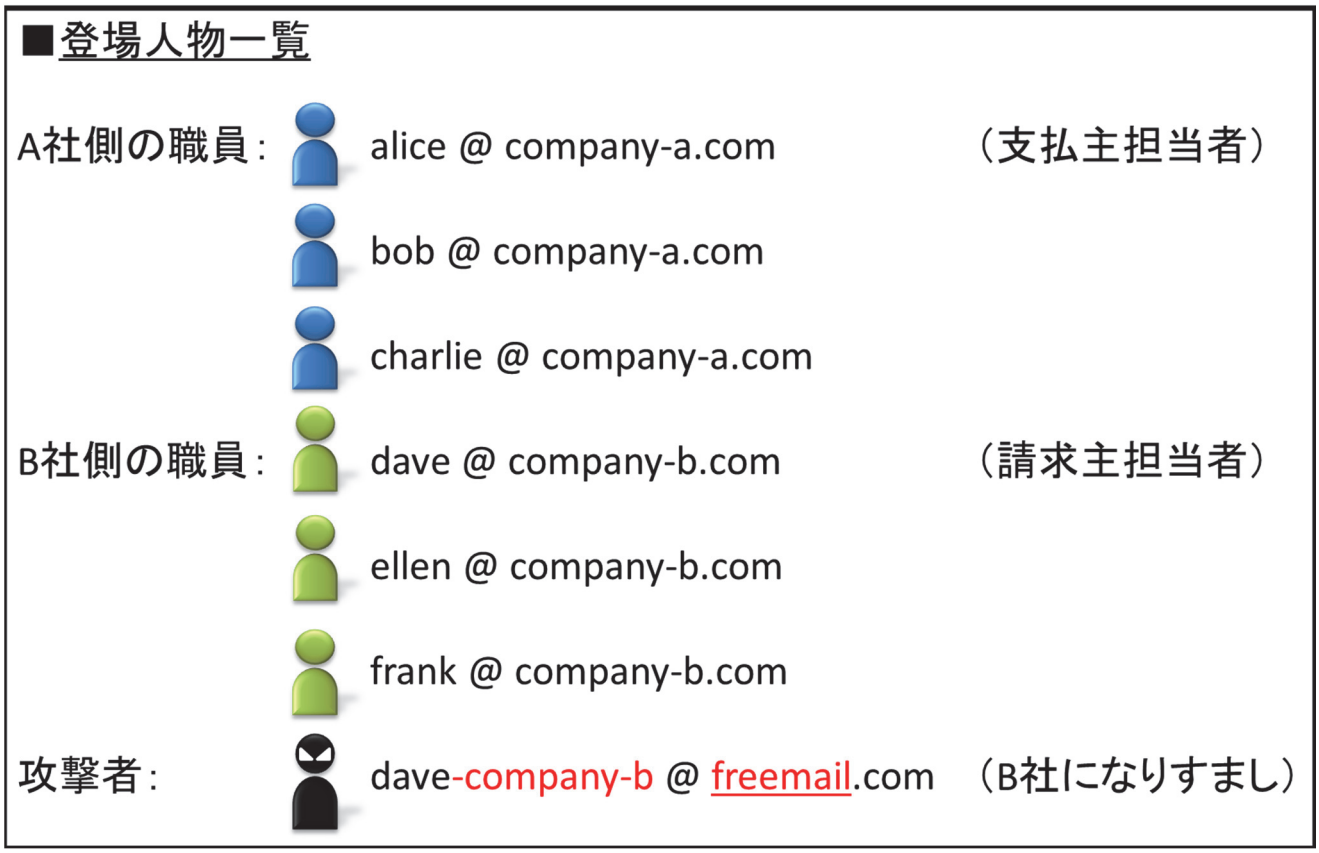

図 2-3 登場人物

このとき、正常な状況ではＢ社からＡ社に対して、請求に係る内容のメールが送付された場合、次のようなメールになるでしょう。

送信元（From）は請求の主担当者である Ｂ 社の「dave」、宛先（To）は支払いの主担当者である Ａ 社の「alice」へのメールです。同報先である Cc には、Ａ 社と Ｂ 社の複数の関係者のメールアドレスが含まれます。

図 2-4 正規のメールの例

事例 2 では、攻撃者は図 2-2 に示す例のように、なりすましのメールアドレスを使ってメールを送ってきました。このとき、Cc に含まれているすべての関係者のメールアドレスも**アルファベットを 1 文字追加**して改変していました。

これによって、支払担当者である「alice」以外の関係者に、攻撃が行われたメールが一切届いていないことになります。この状態で、A 社の担当者（alice）がメールを全員返信したとしても、攻撃者以外にはメールが届かず、攻撃に気付きにくい状況になっています。

図 2-5 事例 2 における同報メールアドレスの改変の様子

なお、この A 社側の従業員がこのような攻撃者からのメールに「全員返信」をした場合、当然ながら複数のエラーメールを受信することになるため、不審であると気付けるチャンスはあったと思われますが、本事例で当事者がどう状況を認識していたかは不明です。

メールアドレスでスペルミスをしているというのは、実際にあり得る状況かもしれませんが、このように**意図的に誤ったメールアドレスを指定する手口がある**ということは、認識しておいた方がよいでしょう。

2.4. 攻撃手口(4) - メールの引用部分の改変

攻撃手口(2)、攻撃手口(3) を使いながら、攻撃者はＡ社とＢ社の双方にメールを送信していました。詐欺を発覚しにくくするためか、攻撃者は**メールの引用部分**についても、攻撃者にとって都合が悪い部分や矛盾が生じた部分を改変していた形跡がありました。

- **引用部分にある過去メール本文の一部を削除または改変している**
- **引用部分にある過去メールの From/To/Cc のメールアドレスの一部を削除または改変している**

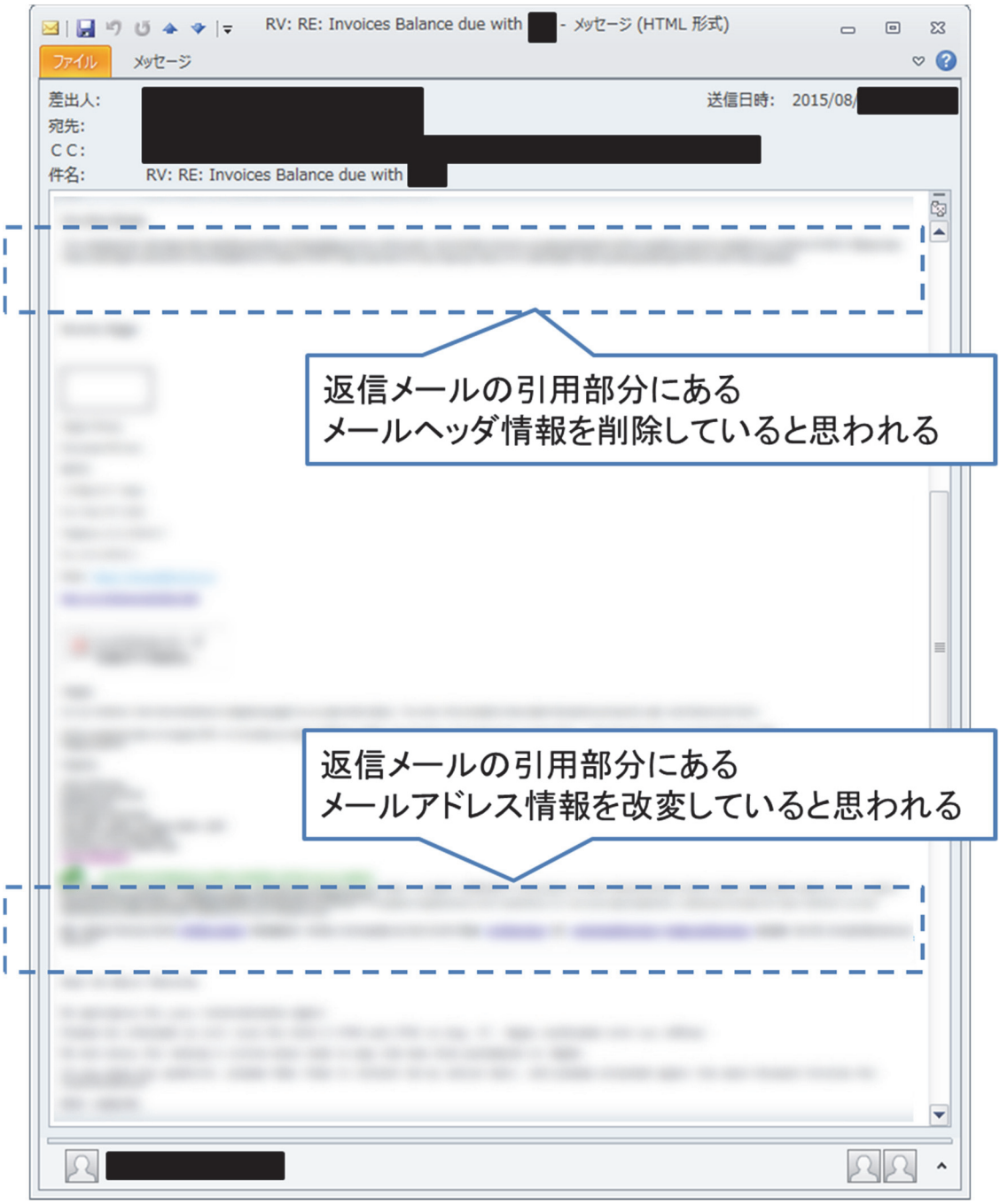

図 2-6 メールの引用部分の改変の様子

2.5. 攻撃者からのメッセージ

攻撃（詐欺）が成功した後、A 社と B 社との間で送金被害の状況をメールで連絡している最中、攻撃者からのメッセージと思われるメールが A 社に届きました。

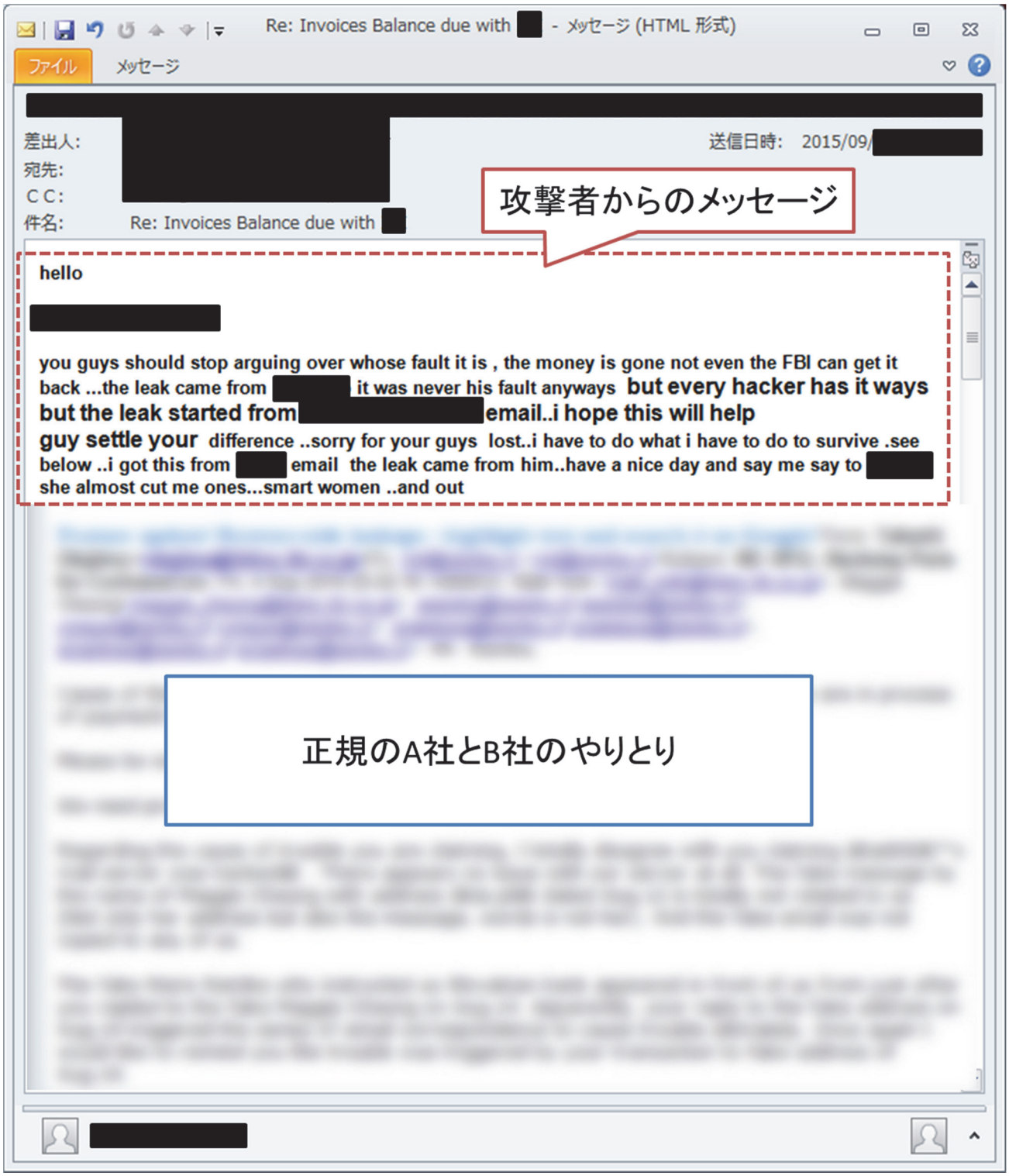

図 2-7 攻撃者からのメッセージメール

3. 事例 3 で使われた攻撃手口

事例 3 では、詐欺の過程において、次の 4 点の手口が使われました。

（1） 偽の口座を伝えて振り込ませる
（2） 正規ドメインに似た詐称用ドメインを取得し、詐欺に悪用する
（3） 詐称用ドメインを取得した当日に、なりすましメールを送信する
（4） A 社と B 社の両方になりすまし、それぞれに偽のメールを送信する

上記 （1） の手口が詐欺の本質的な部分（金銭の詐取）ですが、これを成功させ、あるいは発覚を遅らせるために、（2）、（3）、（4） の手口が併用されたと思われます。

本事例の攻撃者は、攻撃手口を確立し、本事例以外にも複数のビジネスメール詐欺による攻撃を行っている可能性があるものでした。

3.1. 攻撃手口(1) - 偽の口座を伝えて振り込ませる

本事例は、2016 年 9 月、A 社（本物）と B 社が、B 社顧客とのオーダーとその請求書支払いに係るやりとりを攻撃者によって仲介され、さらに攻撃者によって偽の口座への振り込みを要求される手口でした。

攻撃者が行った、偽の口座への振り込み要求の流れを次に示します。

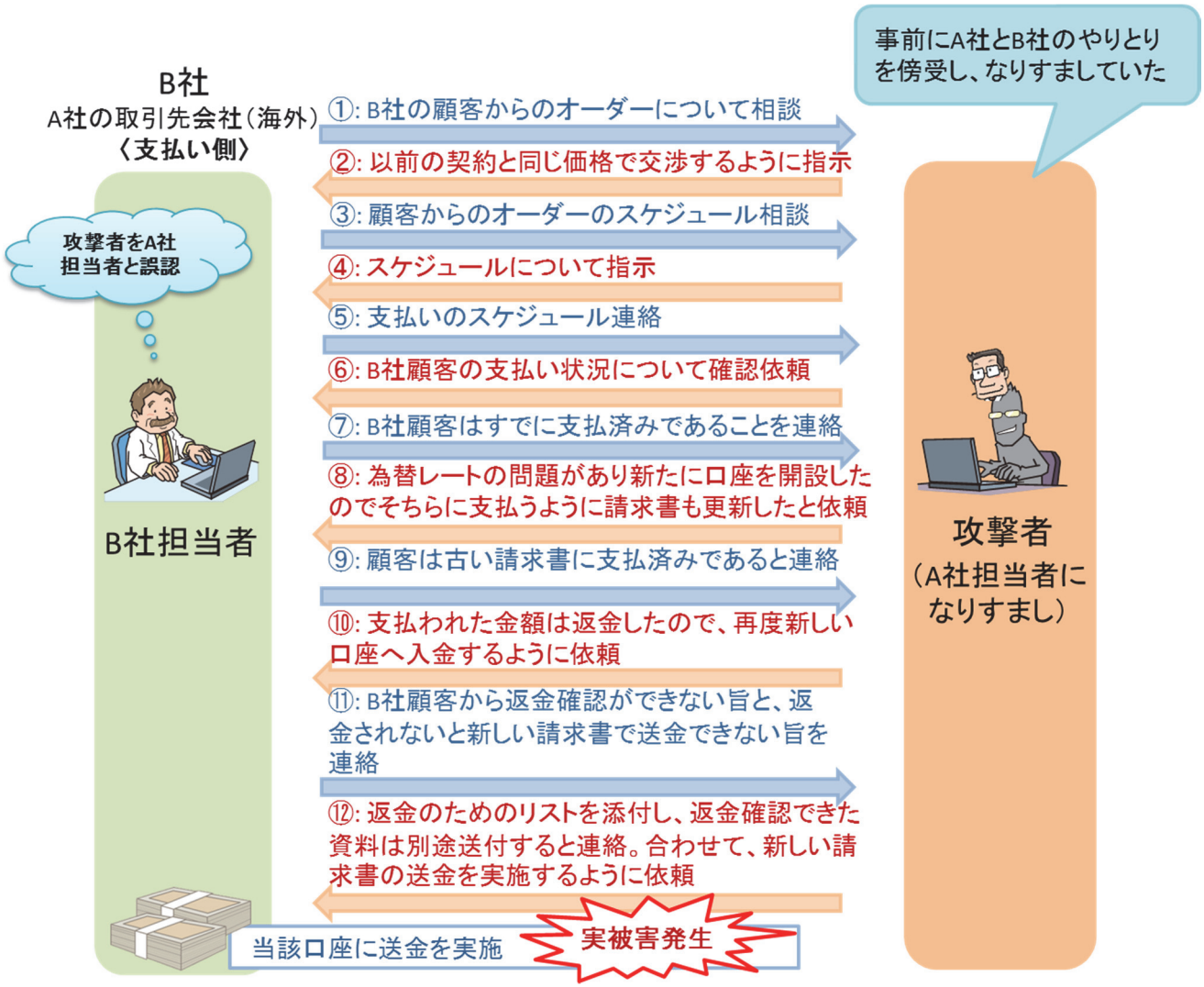

図 3-1 事例 3 の振り込み要求の概要

攻撃者は事前に A 社と B 社になりすまし、A 社と B 社のやりとりを傍受し仲介していました。本事例では、B 社顧客の契約に係る内容について、攻撃者は A 社になりすまして指示を出しています（図 3-1 ②、④）。B 社の顧客はすでに前もって取り交わしていた請求書の内容で送金を済ませていましたが（図 3-1 ⑦）、攻撃者は為替レートの問題があるなどと、もっともらしい理由を付けて偽の口座を伝えています（図 3-1 ⑧）。

このとき、攻撃者はすでに送金済みの金銭は返金したと虚偽の申告をしていますが、B 社の顧客はその返金が確認できていないと B 社に連絡していました。このタイミングで、B 社は A 社が偽者でありビジネスメール詐欺による攻撃ではないかと疑うことができた可能性はありますが、B 社担当者は攻撃者により巧みに誘導され、送金被害にまで至ってしまったものと考えられます（図 3-1 ⑨～⑫）。

3.2. 攻撃手口(2) - 詐称用ドメイン取得

攻撃者は、A 社と B 社の正規ドメインに似通った、「詐称用ドメイン」を新たに取得し、DNS やメールサーバの設定も実施しています。これにより、詐称用ドメインを用い、実際のメールの送受信が行われました。

当該ドメインの DNS 情報には SPF レコードも存在しており、SPF[1]検証も「Pass」する状態となっていました。

注意していれば、ドメイン名が異常であること、アドレス帳にあるアドレスと異なることに気付けるかもしれませんが、「フリーメールに警告を付与する」「SPF 検証を行う」といった対策は効果が無いことになります。

なお、A 社・B 社向けに取得された詐称用ドメインは、次の例のように、**正規ドメインの中心付近にあるアルファベット 1 文字を削除されたもの**でした。この例では、仮に本物と想定するメールアドレスのドメイン名を「company-a . com」としています。

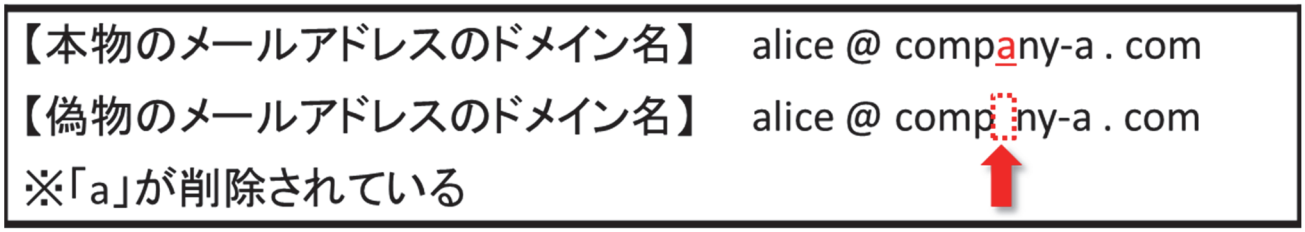

図 3-2 詐称用ドメインの例

[1] なりすましメール撲滅に向けた SPF（Sender Policy Framework）導入の手引き（IPA）
http://www.ipa.go.jp/security/topics/20120523_spf.html

この攻撃者は、本件で詐称した A 社・B 社の他にも、本事例とは無関係の、**実在する企業のドメイン名に似たドメインを同様に複数取得**していた形跡が、ドメイン登録情報（whois 情報）から確認できています。

攻撃者は、詐称用ドメインの取得やメールサーバなどの準備について、攻撃手口として確立し、攻撃を繰り返しているものと推定できます。

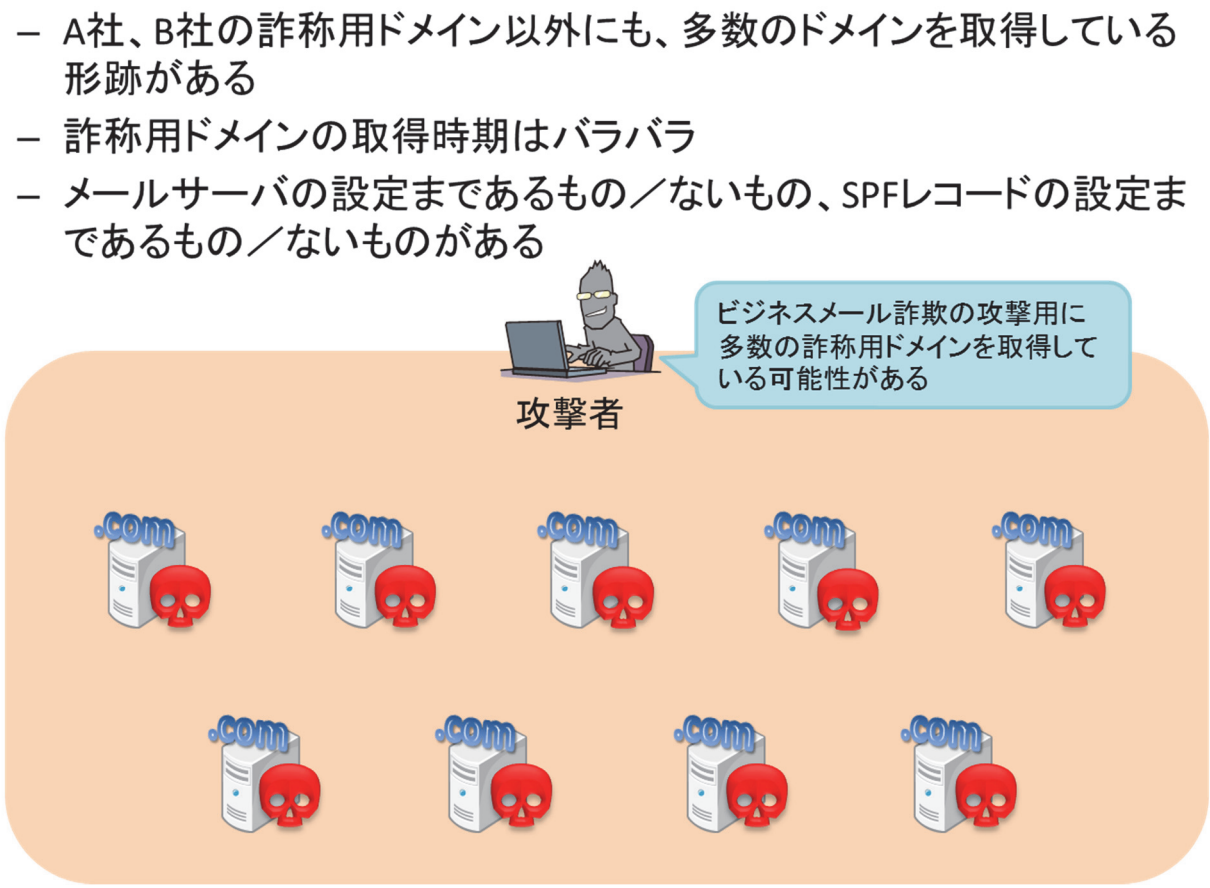

図 3-3 攻撃者が取得していた複数の詐称用ドメイン

3.3. 攻撃手口(3) - 詐称用ドメインの取得タイミング

本事例では、攻撃者は詐称用ドメインを事前に取得して用意しておくのではなく、**なりすましメールを送信する「当日」にドメインを取得していました。**A 社と B 社へメールが送信された日が異なるため、A 社・B 社の詐称用ドメインは別々の日に取得されています。

企業によっては、フィッシング詐欺などの予防のため、自組織ドメイン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ますが、そういった対策を攻撃者は警戒している可能性があります。あるいは、詐欺がうまく進みそうな場合のみ、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動をしているとも考えられます。

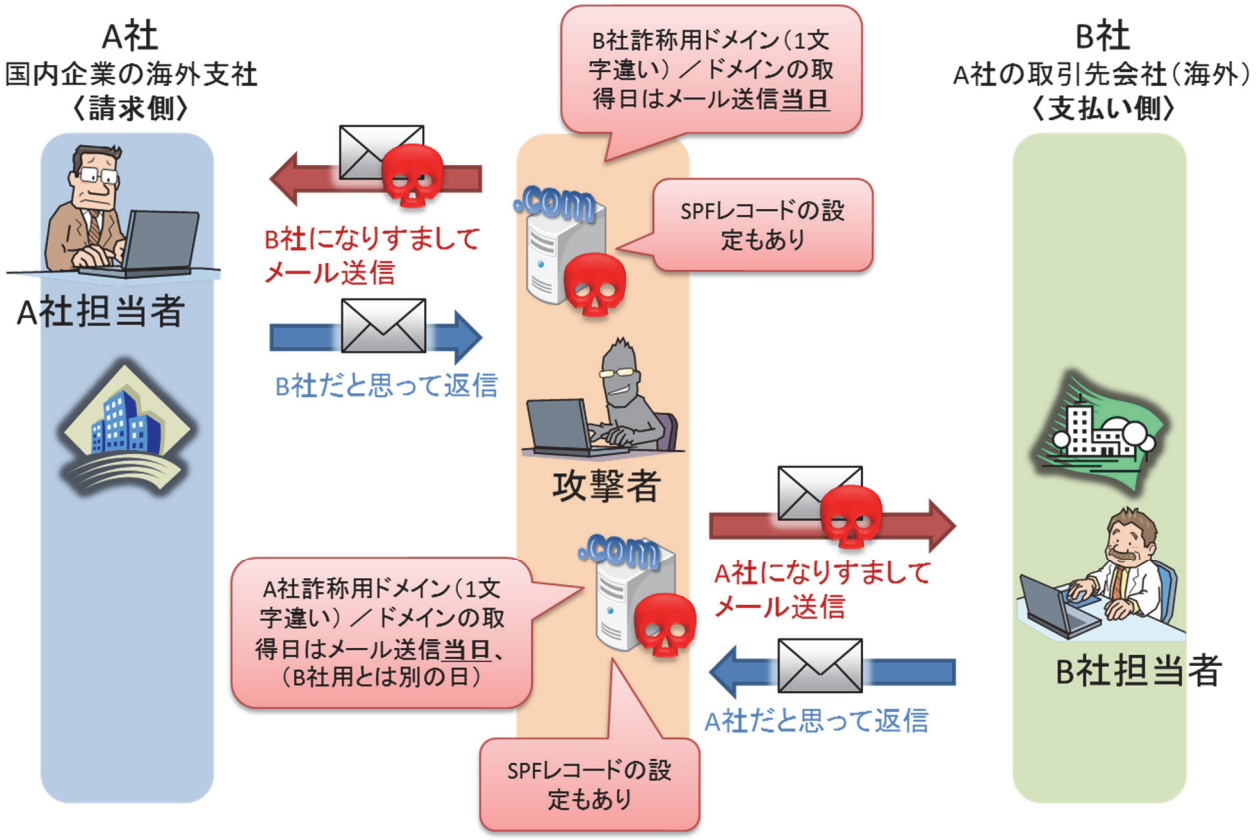

図 3-4 詐称用ドメイン取得のタイミング

3.4. 攻撃手口(4) - A 社と B 社の両方になりすまし

A 社と B 社がやりとりしている正規のメールに返信するかたちで、攻撃手口(2)で示した詐称用ドメインを用いて、攻撃者は次のように振る舞いました。

【A 社から B 社への正規のメール】

2016 年の 8 月に、A 社から B 社へ、「見積書を後ほど送付する」旨の内容が記載された正規のメールが送られた。

◆ **B 社のなりすまし**

B 社になりすました攻撃者から A 社へ、「見積書の送付をお待ちしております」という旨のメールを送付

◆ **A 社のなりすまし**

翌日、A 社になりすました攻撃者から B 社へ、何らかのメールが届いた（今回の情報提供の対象外）。

以降の展開の詳細は不明な点がありますが、A 社・B 社共に、攻撃者からの偽メールに返信するかたちで、攻撃者とメールのやりとりを行ってしまった形跡があります。すなわち、A 社は偽の B 社、B 社は偽の A 社にメールを送信しており、これらのメールは、攻撃者が用意した詐称用ドメインのメールボックスに届いたものと思われます。

その結果、**攻撃者が A 社と B 社のメールを全て仲介する状態**となり、メール内容の窃取および改ざんを自由に行われてしまう状況下で、実被害にまで至る詐欺に繋がったものと考えられます。

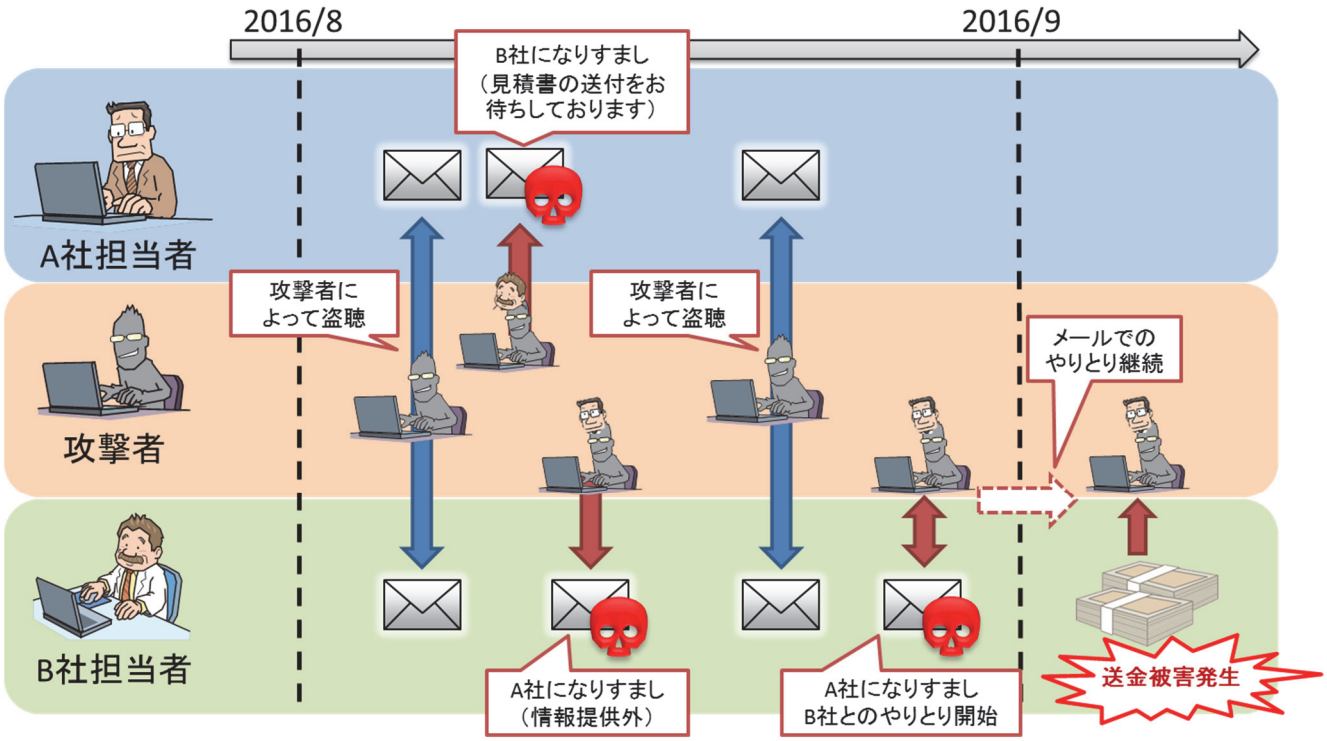

図 3-5 なりすましの経緯

4. 事例 4 で使われた手口

事例 4 では、詐欺の過程において、次の 3 点の手口が使われました。

（1） 偽の法律事務所の担当者と連絡を取り送金するよう指示する
（2） メールの表示名を偽装する
（3） 今後個人メールアドレスへ連絡することを要求する

上記 （1） の手口が詐欺の本質的な部分（金銭の詐取）ですが、これを成功させるため、あるいは発覚を遅らせるために、（2）、（3） の手口が併用されたと思われます。

本事例は、攻撃者が「一人二役」を演じる詐欺を試みた可能性があるものでした。

4.1. 攻撃手口(1) - 偽の法律事務所の担当者と連絡を取り送金するよう指示する

本事例は、2015 年 7 月、A 社の社長になりすました攻撃者から、A 社の海外関係企業（子会社）である B 社の社長に対して、「緊急かつ秘密の案件」と称して、不正に送金を要求する手口でした。

攻撃者が行った、不正送金要求の流れを次に示します。

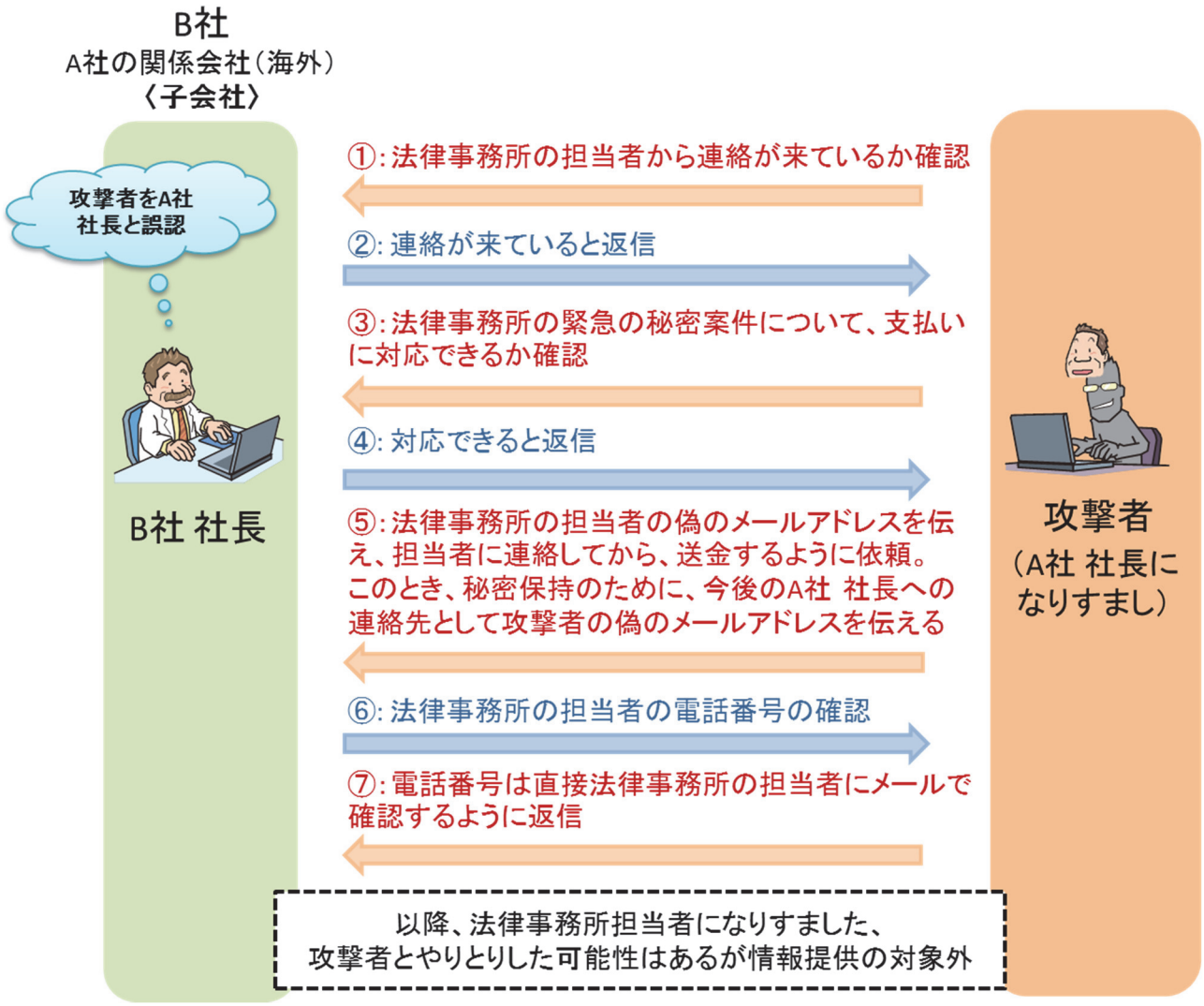

図 4-1 事例 4 の振り込み要求の概要

攻撃者は、A 社の社長になりすまし、B 社の社長に対して、「緊急かつ秘密の案件」を担当している法律事務所の担当者へ連絡するよう（図 4-1 ③）指示しました。このとき、「秘密保持のため」と称し、現在やりとりで使っているメールアドレスではなく、今後は**A 社の社長の個人メールアドレスと称したフリーメールアドレス**へ連絡するようにも伝えていました（図 4-1 ⑤）。

B 社の社長は、攻撃者によって**偽の法律事務所**のメールアドレスを伝えられているため（図 4-1 ⑤）、メールでこの担当者に連絡を取った場合、法律事務所の担当者になりすました攻撃者によって詐欺が行われた可能性がありますが、今回の情報提供の対象外となっています。

本件では、図 4-1 の①から⑦までは、約 20 分の間にやりとりが行われていました。この攻撃者は、周到な準備の上で攻撃を行ってきたものと考えられます。

4.2. 攻撃手口(2) - メールの表示名を偽装する

攻撃者は、A 社の社長になりすまし、B 社の社長に対して緊急かつ秘密の案件について法律事務所の担当者に連絡し、送金を要求していました。

この際、攻撃者がなりすましに使用したメールの差出人表示名は、以下の例に示すように、本物のメールアドレスに近いメールアドレスを長く表示させるような表示名にしていました。

これによって、あたかも A 社の社長から送付されてきたメールであるように見せかけていますが、**実際のメールの送受信で使われるメールアドレスをわかりにくくさせるように細工しています**。また、実際に送受信で使われるメールアドレスは、フリーメールを使用していました。

この例では、仮に本物と想定するメールアドレスを「alice ＠ company-a ． com」とし、フリーメールを「freemail ． com」としています。

【本物のメールアドレス】:	alice@company-a.com
【偽装された表示名部分】:	alioe <alice@company .com> alice@company .com
【実際に送受信で使われるメールアドレス】:	attcker@freemail.com
(表示例: alioe <alice@company.com> alice@company.com [mailto:attcker@freemail.com])	

図 4-2 表示名の偽装

このように、表示名部分の名前を、似た文字（「c」と「o」）を使って 1 文字変更し、本物のドメインに近いドメイン（「-a」を削除）を表示させ、長く表示させるようにしていました。

4.3. 攻撃手口(3) - 個人メールアドレスへ連絡することを要求する

A 社の社長になりすました攻撃者が、B 社の社長に対して送金を要求するメールを送り付けた際に、「秘密保持のため」に、個人用のメールアドレスで連絡するように要求してきました。A 社の社長本人へ、本件に関する連絡がなされないよう、工作したものと思われます。

この「社長の個人用のメールアドレス」は、メールのヘッダに記載される接続元の IP アドレスの情報を隠すことができるといった秘匿性の高いフリーメールサービスが使われていました。これは、**攻撃者が自身の身元を追跡されないようにする**ためという意図も考えられます。

なお、「社長の個人用のメールアドレス」として提示されたメールアドレスと、偽の法律事務所のドメイン取得に使われたメールアドレスには、同一のフリーメールサービスが使われていました。これは、**攻撃者が A 社の社長と法律事務所の担当者の「一人二役」を演じようとした**可能性を裏付けています。

いわゆる特殊詐欺（振り込め詐欺など）においても、「劇場型」と呼ばれる、複数の会社や人物を装って騙す手口がありますが、ビジネスメール詐欺でも、これに似た手口が使われることがあると思われます。攻撃者は詐欺を成功させるため、舞台がサイバー空間になろうとも、あらゆる手口を使ってくるという認識が必要だと考えられます。

以上