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

ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）

～ あらゆる国内企業・組織が攻撃対象となる状況に ～

IPA 独立行政法人情報処理推進機構
セキュリティセンター

ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）

～ あらゆる国内企業・組織が攻撃対象となる状況に ～

目次

ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）

～ あらゆる国内企業・組織が攻撃対象となる状況に ～

2018 年 8 月 27 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

本書の要旨

本レポートは、IPA（独立行政法人情報処理推進機構）が運営しているサイバー情報共有イニシアティブ[1]（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan、ジェイシップ）の参加組織をはじめ、国内企業の方々から情報提供いただいたビジネスメール詐欺「BEC」の事例と騙しの手口について紹介し、注意喚起を行うものです。

本書の対象読者

本書では、次の方々を主な対象読者と想定しています。

- 企業の経理・財務部門といった金銭管理を取り扱う部門の方
- 取引先と請求書などを通して金銭的なやりとりを行う方

なお、本書で紹介する事例や手口は、営業秘密の詐取や標的型サイバー攻撃とも通じるところがあり、組織・企業の従業員の方々全般へも参考にしていただける内容となっています。

[1] サイバー情報共有イニシアティブ（IPA）
https://www.ipa.go.jp/security/J-CSIP/

1　はじめに

IPA は、J-CSIP の情報共有の活動[2]で得られた情報をもとに、2017 年 4 月、ビジネスメール詐欺（BEC）に関する注意喚起[3]（以降、2017 年 BEC 注意喚起）を行いました。

その後も、J-CSIP 参加組織のみならず、一般の企業からもビジネスメール詐欺の発生について IPA へ情報提供が続いています。その中で、**2018 年 7 月、IPA としては初めて、「日本語でのビジネスメール詐欺」について、実際のメールの内容とともに情報提供を受けました**（この事例は 2.1 章で説明しています）。これまでのビジネスメール詐欺は、英語のメールのやり取りを伴う海外取引で多く発生していましたが、攻撃者が本格的に日本の企業を対象として活動を行うようになった可能性を示しています。すなわち、**あらゆる国内企業・組織が攻撃対象となりうる状況**となった可能性があります。

日本語での攻撃事例が確認されただけでなく、ビジネスメール詐欺は、2017 年 12 月に国内で大規模な被害事例が報道されるなど、非常に注意が必要な状況になりました。本書は、**2017 年 BEC 注意喚起の続報**として、ビジネスメール詐欺の事例と、その騙しの手口について紹介し、改めて注意喚起を行うものです。読者の方々へは、本書を通じて、この脅威について知っていただき、十分な対策を講じ、同様の手口による被害を避けていただきたいと考えています。

1.1 ビジネスメール詐欺「BEC」の概要

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃です。詐欺行為の準備として、企業内の従業員などの情報が狙われたり、情報を窃取するウイルスが悪用されることもあります。

BEC は、「ビジネスメール詐欺」以外にも、「ビジネス電子メール詐欺」や「外国送金詐欺」などとも呼ばれています（本書ではビジネスメール詐欺と呼びます）。

米国連邦捜査局（Federal Bureau of Investigation：FBI）によると、2013 年 10 月から 2018 年 5 月までに、米国インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）を含む複数の情報源に報告されたビジネスメール詐欺の発生件数は 78,617 件、被害総額は約 120 億（12,536,948,299）米ドル（未遂を含む）にのぼっています[4]。1 件あたりの平均被害額は約 16 万米ドル（日本円では約 1,800 万円）にもなり、非常に大きな被害をもたらす脅威となっています。

また、トレンドマイクロ社による「ビジネスメール詐欺に関する実態調査 2018」[5]では、日本在住の法人組織の情報セキュリティ・社内 IT・経理責任者ら 1,030 人を対象に調査を行い、全体の約 4 割（39.4%）がビジネスメール詐欺の攻撃を受けた経験があることが分かりました。更に、送金依頼メール受信者（253 人）のうち 8.7%にあたる 22 人が、実際に騙されて送金してしまったとのことです。この調査結果からも、ビジネスメール詐欺が日本国内の企業・組織に対する脅威であることがうかがえます。

---

[2] J-CSIP は、IPA を情報のハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みです。

[3] 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[4] Business E-mail Compromise The 12 Billion Dollar Scam （IC3）
https://www.ic3.gov/media/2018/180712.aspx

[5] 「ビジネスメール詐欺に関する実態調査 2018」を発表 （トレンドマイクロ）
https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html

本書では、攻撃者によって行われたビジネスメール詐欺の実事例を紹介し、その巧妙な騙しの手口について説明します。「このような詐欺がある」ということすらも知らなければ、受信したメールなどに多少不自然な点があっても、騙されてしまいかねません。実際に、IC3 に報告されている被害件数や被害額の多さは、攻撃者の巧妙な手口によって、多数の組織・企業の担当者が騙されていることを示しています。

企業での送金取引に関係する担当者、特に経理・財務部門など金銭管理を取り扱う部門の担当者においては、ビジネスメール詐欺について知っていただくことが非常に重要です。攻撃者に騙されないよう、本書および 2017 年 BEC 注意喚起の事例をもとに、組織内の対策や意識の向上に役立ててください。

なお、メールを駆使した巧妙な騙しの手口は、主に諜報活動を目的とする「標的型サイバー攻撃」とも通じるところがあり、経理・財務部門などに限らず、組織・企業の従業員全般へも参考になると思われます。

本書は、まず 1.2 節でビジネスメール詐欺の 5 つのタイプを紹介し、次に 2 章でこれまで J-CSIP に情報提供のあった事例を整理し、5 つの事例を紹介します。

そして、3 章でビジネスメール詐欺への対策について説明します。

参考：国内でのビジネスメール詐欺の逮捕者 [6]

2018 年 7 月、詐欺と組織犯罪処罰法違反（犯罪収益の隠匿）の容疑で、東京都の会社役員（邦人）の男性ら 4 人の男女が逮捕されたとの報道がありました。米国の農業関連会社から約 7800 万円を不正に銀行口座へ送金させた上、2017 年の 7 月 4 日から 21 日にかけて、6020 万円を引き出した疑いとのことです。

手口などの詳細は明らかではありませんが、組織的に行われたビジネスメール詐欺で、日本国内に関与した者が存在したという点において、脅威がより身近なものになったと考えられる事例です。

[6] 7千万円送金させた疑い ビジネスメール詐欺で逮捕 （日本経済新聞）
https://www.nikkei.com/article/DGXMZO32602020U8A700C1CC1000/

1.2 ビジネスメール詐欺の 5 つのタイプ

IC3[7]やトレンドマイクロ社 [8]では、ビジネスメール詐欺の手口を主に次の 5 つのタイプに分類しており、本書でも、この分類のどれに該当するかを示している箇所があります。

この 5 つのタイプについては、IPA の 2017 年 BEC 注意喚起で説明しています。本書では詳細を省略しますので、必要に応じそちらを参照してください。

- タイプ 1：取引先との請求書の偽装
  - （例）取引のメールの最中に割り込み、偽の請求書（振込先）を送る
- タイプ 2：経営者等へのなりすまし
  - （例）経営者を騙り、偽の振り込み先に振り込ませる
- タイプ 3：窃取メールアカウントの悪用
  - （例）メールアカウントを乗っ取り、取引先に対して詐欺を行う
- タイプ 4：社外の権威ある第三者へのなりすまし
  - （例）社長から指示を受けた弁護士といった人物になりすまし、振り込ませる
- タイプ 5：詐欺の準備行為と思われる情報の詐取
  - （例）経営層や人事部になりすまし、今後の詐欺に利用するため、社内の従業員の情報を詐取する

---

[7] Business E-mail Compromise: The 3.1 Billion Dollar Scam （IC3）
https://www.ic3.gov/media/2016/160614.aspx
※ 5 つのタイプの原典はこちらを参照してください。

[8] 多額の損失をもたらすビジネスメール詐欺「BEC」（トレンドマイクロ）
http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Billion-Dollar+Scams%3A+The+Numbers+Behind+Business+Email+Compromise

2　ビジネスメール詐欺事例と手口の紹介

ビジネスメール詐欺は、警察、国内の金融機関やセキュリティ事業者から注意喚起がなされています。本書では、J-CSIP の参加組織等において実際に発生した事例を、情報提供元の許可のもと、詳細な内容を紹介し、攻撃者が詐欺の過程で使った騙しの手口について解説します。

IPA では、2015 年から 2018 年 7 月にかけて発生したビジネスメール詐欺に関する **17 件**の情報提供を受けており、うち **5 件**で金銭的被害が確認されています。次の表は、これまで IPA が情報提供を受けたビジネスメール詐欺の事例を一覧としたものです[9]。「★」印の事例は、本章で詳しく手口を説明するものです。

表 1 ビジネスメール詐欺の事例概要

項番	情報提供日		事例概要	被害の有無	備考
1.	2015 年	11 月 17 日	2015 年 7 月、日本国内の企業（親会社）の、スイスにある海外関係企業（子会社）において、日本国内の企業（親会社）の社長になりすますビジネスメール詐欺が試みられた。	不明	2017 年 BEC 注意喚起に記載
2.	2016 年	1 月 8 日	2015 年 12 月と 2016 年 1 月の 2 回、日本国内の企業（支払い側）と、アメリカにある企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	2017 年 BEC 注意喚起に記載
3.		1 月 14 日	2015 年 8 月、日本国内の企業の海外支社（支払い側）と、チリにある企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が発生した。	**あり**	2017 年 BEC 注意喚起に記載
4.		9 月 16 日	2016 年 9 月、日本国内の企業の海外支社（請求側）と、ベトナムにある企業（支払い側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が発生した。	**あり**	2017 年 BEC 注意喚起に記載
5.	2017 年	6 月 2 日	2017 年 5 月、企業の経営者（CEO）を詐称し、財務責任者（CFO）を騙そうとしたビジネスメール詐欺が試みられた。	なし	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2017 年 4 月～6 月]に記載 （★本書：事例 3）
6.		6 月 6 日	2017 年 6 月、企業の経営者（CEO）を詐称し、財務責任者（CFO）を騙そうとしたビジネスメール詐欺が試みられた。 異なる業界の企業への着信だが、メールの内容、攻撃者のメールアドレスが項番 5 の攻撃と同一であった。	なし	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2017 年 4 月～6 月]に記載 （★本書：事例 3）

[9] これらの事例の一部は、ビジネスメール詐欺が行われた具体的な国名を挙げていますが、これらの国の企業との取引が特に危険ということではありません。あらゆる国の企業がこの攻撃の対象となる可能性があります。

項番	情報提供日		事例概要	被害の有無	備考
7.		6 月 21 日	2017 年 4 月、日本国内の企業（請求側）と、海外の企業（支払い側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が発生した。	**あり**	ー
8.		10 月 24 日	2017 年 10 月、日本国内の企業の海外支社（支払い側）と、海外取引先（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が発生した。	**あり**	ー
9.		12 月 26 日	2017 年 12 月、日本国内の企業（支払い側）と、海外の企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2017 年 10 月～12 月]に記載
10.	2018 年	1 月 5 日	2017 年 12 月、日本国内の企業（支払い側）と、東南アジアの企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	ー
11.		2 月 16 日	2018 年 2 月、日本国内の企業が、海外のカンファレンスのブース出展に関するメールをやりとりしている中で、攻撃者が海外のカンファレンス事務局の担当者になりすまし、偽の口座情報を連絡して送金させようとするビジネスメール詐欺が発生した。	**あり**	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2018 年 1 月～3 月]に記載 （★本書：事例 2）
12.		3 月 12 日	2018 年 3 月、日本国内企業の海外関連会社において、同社の CEO になりすました攻撃者から、偽の振り込みを要求するビジネスメール詐欺が試みられた。	なし	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2018 年 1 月～3 月]に記載 （★本書：事例 4）
13.		5 月 17 日	2018 年 5 月、日本国内に本社のある関連企業（請求側）と、海外取引先（支払い側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2018 年 4 月～6 月]に記載
14.		6 月 4 日	2018 年 6 月、日本国内の企業（請求側）と、海外関連企業（支払い側）との取引において、攻撃者が請求側企業の担当者になりすまし、偽の振り込みを要求するメールを送り付けるビジネスメール詐欺が試みられた。	不明	サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2018 年 4 月～6 月]に記載

項番	情報提供日		事例概要	被害の有無	備考
15.		7 月 6 日	2018 年 7 月、日本国内の企業の CEO を詐称し、海外関連企業の CEO へ偽のメールが送られた。 なお、同一文面のメールを用いたビジネスメール詐欺が、本件と無関係なドイツの企業に対しても行われたと思われる情報も確認。国や業界に関わらず、攻撃者が複数企業を狙って活動しているものと推測。	不明	ー
16.		7 月 9 日	2018 年 7 月、日本国内企業の CEO を詐称し、同企業内の担当者に対して、仮想通貨を購入するための準備と称して、国際送金させようとするビジネスメール詐欺が試みられた。 本事例では、**日本語のメール**が攻撃者から送られてきた。	なし	（★本書：事例 1）
17.		7 月 19 日	2018 年 7 月、日本国内の関連企業（請求側）と、海外取引先企業（支払い側）との取引において、攻撃者が請求側企業の担当者になりすまし、偽の振り込みを要求するメールを送り付けるビジネスメール詐欺が試みられた。	なし	（★本書：事例 5）
情報提供数の合計：**17** 件					

2.1 節以降は、これら 17 件の事例の中から、既に J-CSIP の運用状況レポート[10]で公開したものの再掲を含め、新たな手口や特徴がみられた 5 件の事例を紹介します。

◆ 事例 1 国内企業の CEO を詐称する日本語メールの攻撃（2018 年 7 月）
- タイプ 2：経営者等へのなりすまし
- 日本国内企業の CEO を詐称し、同企業内の担当者に対して攻撃
- 攻撃者は日本語のメールでやりとり

◆ 事例 2 海外のカンファレンス事務局担当者を詐称する攻撃（2018 年 2 月）
- タイプ 1：取引先との請求書の偽装
- カンファレンスのブース出展に関するメールのやりとりを盗聴し、割り込み
- 「クレジットカードの決済ができなくなったため、電子送金にしてほしい」と騙して金銭を詐取

◆ 事例 3 同一と考えられる攻撃者からの複数組織への攻撃（2017 年 5 月～6 月）
- タイプ 2：経営者等へのなりすまし
- 短期間（1 週間）のうちに、業種が異なる国内企業 2 社へと連続して、同一と思われる攻撃者からビジネスメール詐欺が試みられた

◆ 事例 4 海外関係企業の CEO を詐称する攻撃（2018 年 3 月）
- タイプ 2：経営者等へのなりすまし
- 日本企業の海外関係企業の CEO を詐称し、同企業内の担当者に対して攻撃

◆ 事例 5 海外取引先を狙った攻撃（2018 年 7 月）
- タイプ 1：取引先との請求書の偽装
- 日本国内の企業と、海外の取引先企業との取引メールを盗聴し、割り込み
- トップレベルドメインの部分のみ異なる「詐称用ドメイン」を使用

[10] サイバー情報共有イニシアティブ 公開レポート（IPA）
https://www.ipa.go.jp/security/J-CSIP/

2.1 事例 1 国内企業の CEO を詐称する日本語メールの攻撃

2018 年 7 月、日本国内の企業（A 社）の従業員に対し、A 社の CEO を騙る攻撃者から、仮想通貨を購入するための準備と称して、国際送金をさせようとするビジネスメール詐欺が試みられました。メールの差出人として、本物の CEO の氏名とメールアドレスが使われています。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 2：経営者等へのなりすまし」に該当します。

本事例では、A 社の担当者がやりとりの途中で不審であると気づくことができたため、金銭的な被害は発生していません。

なお、本事例では、**攻撃者から送られてきたメール 2 通で日本語が使われていました**（これまで IPA で確認してきたビジネスメール詐欺の事例では、海外取引や CEO を騙るもの等がありましたが、すべて英語のメールでした）。**普段、英語のメールでのやりとりを行わないような国内企業・組織であっても、今後は攻撃対象となりうる状況**となった可能性があります。

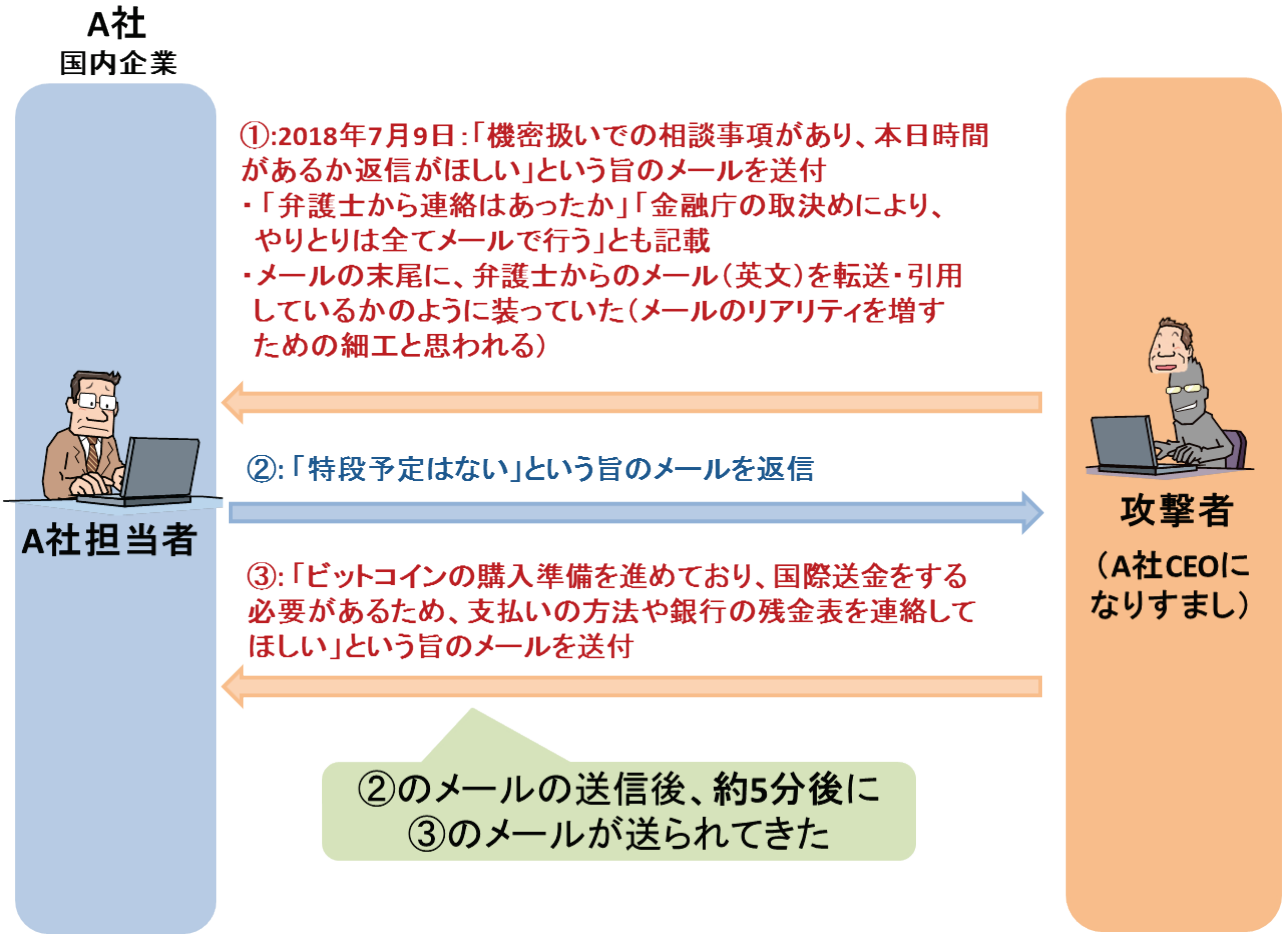

図 2-1 事例 1：攻撃者とのやりとり

2018 年 7 月 9 日、攻撃者は、A 社の CEO になりすまし、機密扱いでの相談事項があるという内容のメールを送り付けてきました。このとき、A 社担当者へ特段予定はないという連絡を攻撃者に返信しています。

A 社担当者からメールを返信した約 5 分後、攻撃者からビットコインの購入準備のために国際送金が必要であるという内容で、支払方法や銀行の情報を聞き出そうとするメールを送り付けてきました。

（1）攻撃者からのメール

実際に攻撃の中でやりとりされたメールは次の通りです。

攻撃者からの最初のメールは、A 社担当者に対して返信を要求する内容が日本語で書かれていました。更に、メールのリアリティを増すため、国際法律事務所の日本人弁護士とのやりとり（英語）を装った内容を転送・引用しているように見せかけ、その弁護士にもメールの写し（CC）を送るよう指示していました。

この法律事務所のドメインも、実在する国内の法律事務所に似せた偽のドメインであり、攻撃者が使用した「詐称用ドメイン」と同じ経路（レジストラ）で、約 10 分差で取得されたものです。すなわち、指定された弁護士のメールアドレスへメールを送っても、結局は同じ攻撃者にメールが届く仕掛けになっており、攻撃者は必要に応じ CEO と弁護士の一人二役を演じるつもりであったものと思われます。

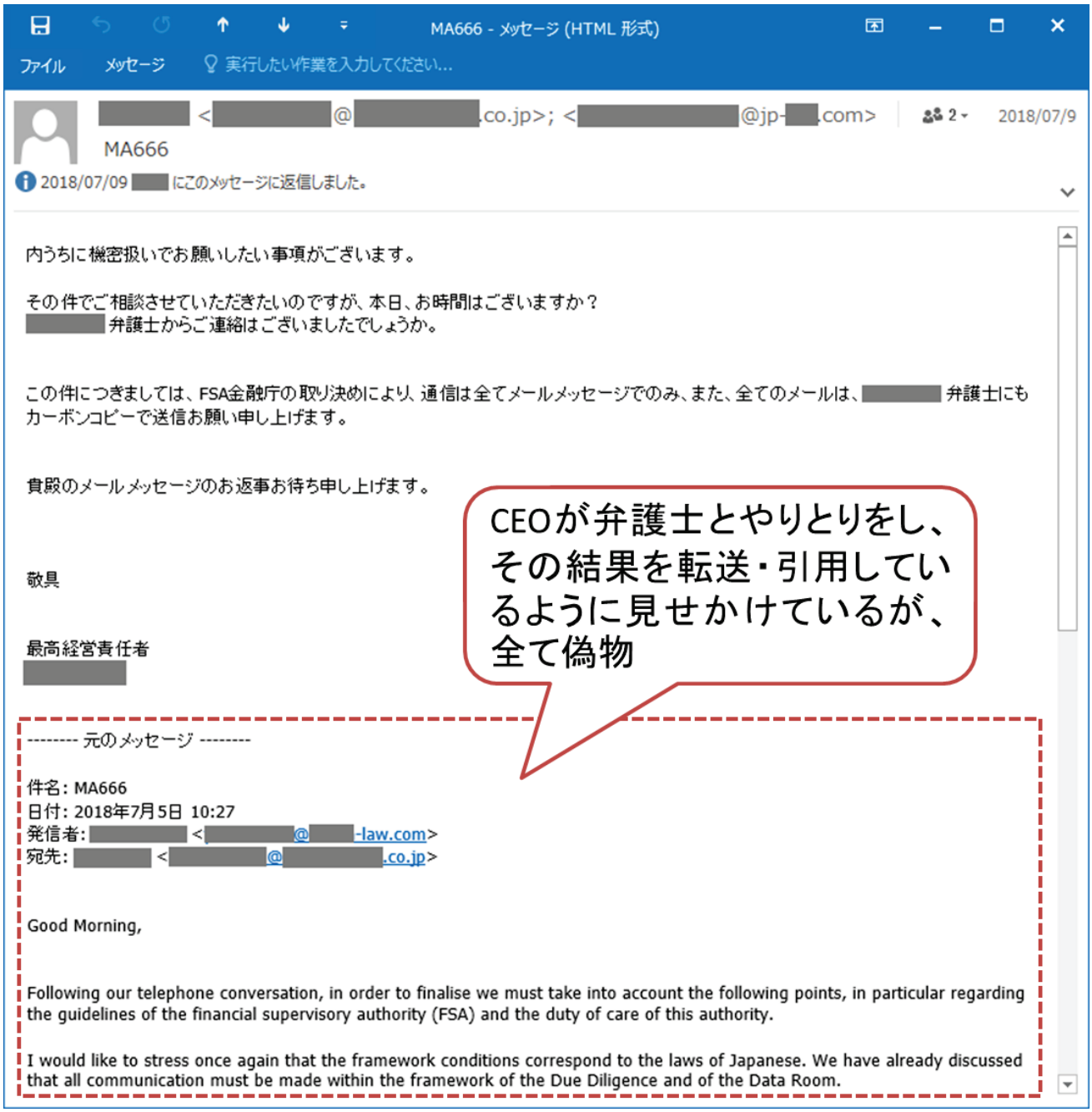

図 2-2 事例 1：攻撃者からのメール 1通目

さらに、先ほどのメールに対して、A 社担当者が日本語で返信をすると、次のメールが攻撃者から送られてきました。この中で、ビットコインの購入準備と称し、国際送金を行う必要があるとしています。また、支払方法や銀行残高等の情報を聞き出そうとしており、A 社担当者がこのメールに返信をした場合、攻撃者から偽の口座への振り込みを指示するような内容のメールが送られてきたものと思われます。

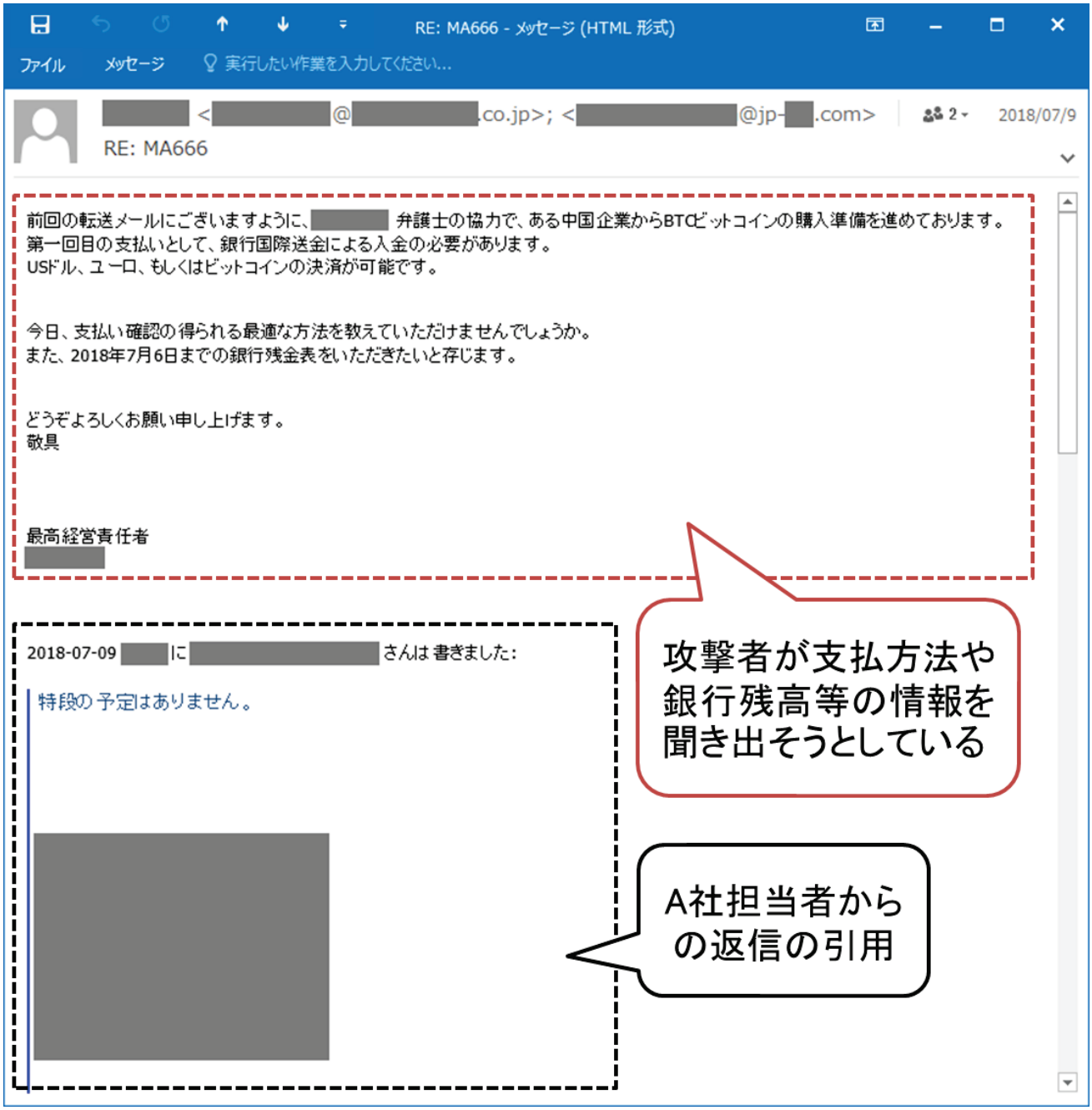

図 2-3 事例 1:攻撃者からのメール 2通目

（2）詐称用ドメインの取得と悪用

本事例の攻撃者は、日本の金融庁の正規のドメインに似通った、偽の「詐称用ドメイン」を新規に取得し、DNS やメールサーバの設定も実施していました。この詐称用ドメインの DNS 情報には、SPF（Sender Policy Framework）レコードも存在しており、SPF 検証 [11]も「Pass」する状態でした。このため、本事例のケースでは、一般的に不審なメールを判断するためのシステム的対策である、「フリーメールアドレスからのメールに警告を付与する」や「SPF 検証を行う」などの対策は効果がないことになります。そのため、メール受信者がメールアドレスに注意して、ドメイン名が異常であることに気づくことが重要になります。

本事例の攻撃者が送信したメールの From メールアドレスは次のような内容でした。

A 社 CEO の名前 <A 社 CEO の正規のメールアドレス> ; <金融庁に見せかけた偽のメールアドレス> （例：山田 太郎 <taro.yamada@company.com> ; <sample@jp-fakefsa.com> ）

※実際に悪用されたものとは異なる。

本事例では、攻撃者から送られてきたメールの From メールアドレスに本物の A 社 CEO の名前とメールアドレスが表示されますが、そのメールアドレスに返信メールが届かないようにする（攻撃を行っていることに気付かれないようにする）細工が仕掛けられていました。

このメールに対して返信すると（返信メールを作成すると）、次の図 2-4 のように宛先メールアドレスが設定されます。一見すると、A 社の CEO と（偽の）金融庁の二者宛てのメールとなっているように見えますが、A 社の CEO の名前とメールアドレスが表示されている部分は「見せかけ」であり、実際にはメールは送信されません [12]。偽の金融庁のメールアドレス（攻撃者のメールアドレス）にのみメールが送信されます。

図 2-4 事例 1：返信先のメールアドレスを詐称する手口の例

要するに、この攻撃は、メールの内容に日本語が使われただけでなく、差出人欄で本物の CEO の氏名とメールアドレスを詐称しつつ、被害者がメールを返信する際にも、画面上にはその情報が表示される仕組みとなっており、巧妙な細工が施されていた事例と言えます。

---

[11] 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

[12] メールアドレスの「表示名」の部分に細工が施されています。

2.2 事例 2 海外カンファレンス事務局担当者を詐称する攻撃

2018 年 2 月、日本国内の企業（A 社）が海外のカンファレンスのブース出展に関するメールをやりとりしている中で、攻撃者が海外のカンファレンス事務局の担当者（B 氏）になりすまし、偽の口座情報を連絡して送金させようとするものでした。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当します。

本事例において、支払側である国内組織の担当者は**攻撃者の指示した偽の口座への送金を行ってしまったため、金銭的な被害が生じています**。

本事例の関係者は次の通りです。

A 社	国内企業。海外のカンファレンスへ出展を行おうとしている。
B 氏	海外のカンファレンス事務局の担当者。
攻撃者	B 氏になりすまし、ビジネスメール詐欺によって A 社から金銭を詐取した。

（1） 正規のメールアドレスに似せた、フリーメールアドレスを詐称に使用する

攻撃者は、B 氏の正規のメールアドレスと同一のローカル部[13]のフリーメールアドレスを取得し、偽のメールを送信してきました。ビジネスメール詐欺では、偽のメールを送るため、本物に似せた詐称用ドメインを取得する手口がありますが、本事例ではそのような手口は使われてはいませんでした。

【本物のメールアドレスのドメイン名】alice . brown @ company-b . com
【偽物のメールアドレスのドメイン名】alice . brown @ **freemail . com** ⇒ フリーメールドメイン

※実際に悪用されたものとは異なる。

なお、本事例では、偶然ではありますが、攻撃者から偽のメールが送られてくる約 1 か月前に、本物の B 氏から A 社の担当者に対してメールアドレスを変更した旨の、本物の連絡が送られていました。

このため、A 社の担当者は攻撃者とメールのやりとりを続ける中で、メールアドレスのドメイン部分が異なっていることに気付いたものの、同様のメールアドレスの変更が 1 か月前にもあったことから、それが不審であると見抜くことは難しい状況であったと言えます。

[13] ローカル部：メールアドレスの＠より左側の部分。

（2）決済手段の変更を装い、偽の振込先に誘導する

本事例では、決済手段としてＡ社からカンファレンス事務局へクレジットカードで支払いを行うこととなっていました。このとき、攻撃者は、Ｂ 氏になりすましたメールの中で、「技術的な問題により、クレジットカードでの支払いを受け付けられなくなった」と理由をつけて、電子送金による振り込みを行うよう要求してきました。

これまで、ビジネスメール詐欺の手口で多く使われている「振込先口座の変更」は、実際のビジネスにおいては、そう多くは発生しないと思われ、それが不審であると気づくこともできるかと思われます。一方、クレジットカード決済は、システムのメンテナンス等により一時的に停止するといったケースが現実的に起こりえるため、それが不審であると見抜きにくく、攻撃者はその点を狙った可能性が考えられます。

ビジネスメール詐欺の対策として、急な振込先口座の変更だけでなく、急な「**決済手段の変更**」にも警戒する必要があります。

（3）ビジネスメールの授受に割り込み、詐欺を試みる

今回の事例では、2017 年の夏頃からＡ社とＢ氏の間で、海外のカンファレンスブース出展に関するメールのやりとりが行われていた中で、フリーメールを使い Ｂ 氏になりすました攻撃者が割り込み、詐欺を試みてきました（図 2-5）。攻撃者は、何らかの方法でメールを盗聴していたものと考えられます。

Ａ社と攻撃者の間で数回のメールのやりとりが行われ（図 2-6）、Ａ社が攻撃者から送られた振込先口座に振り込みを行ってしまい、実被害を受けました。

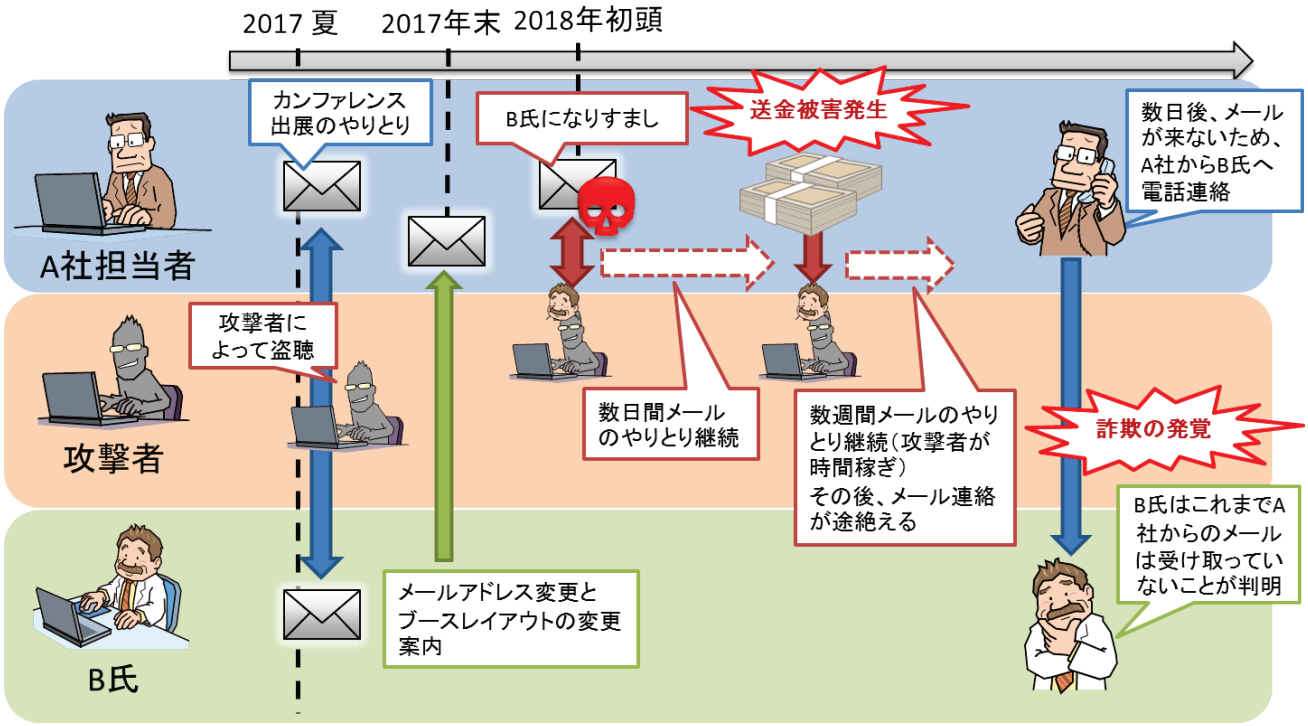

図 2-5 事例 2：本事例の概要

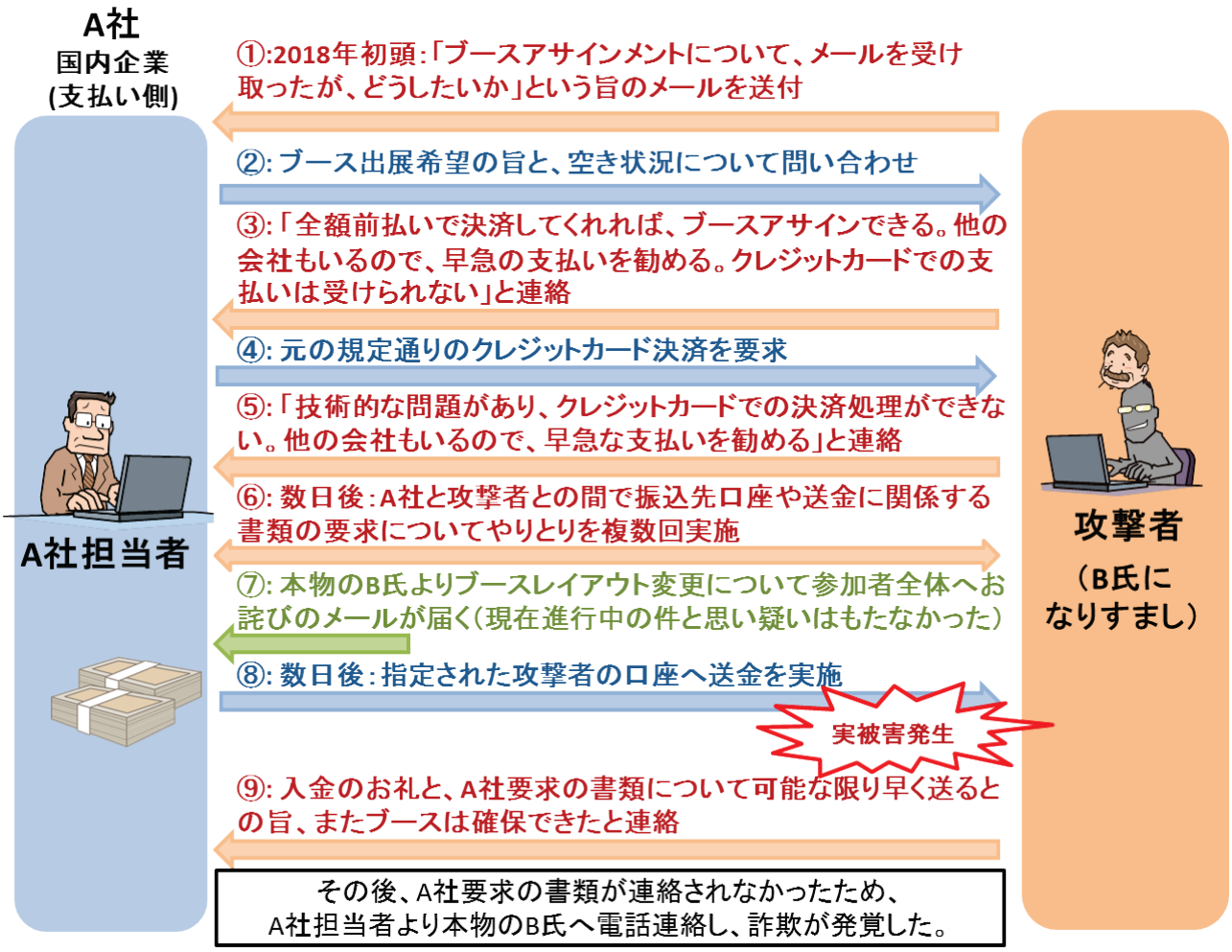

図 2-6 事例 2:攻撃者とのやりとり

本件の攻撃者は、長い期間メールのやりとりを繰り返して、A 社よりカンファレンスのブース出展料を詐取しましたが、クレジットカードでの支払いが前提の金額であり、ビジネスメール詐欺でよく問題となるような、大きな金額ではありませんでした。しかし、本件の攻撃者は、カンファレンスのブース出展の窓口である B 氏へのなりすましに成功していることから、同時期にこのカンファレンスに出展しようとしていた他の企業からも、同じ手口で金銭の詐取を試みた可能性もあります。

すなわち、1 つの組織を対象にして大きな金額を詐取するのではなく、クレジットカード決済が集中する組織とタイミングを見計らい、比較的少額ながら複数の相手を同時に騙すという手口であった可能性が考えられます。攻撃者がどこまで広範囲に攻撃を行ったかは不明ですが、「警戒度が低い少額のやりとり」「現実的に起こりえる、クレジットカード決済から口座振込への変更」等、典型的なビジネスメール詐欺への警戒や対策をすり抜ける手口であったと考えられます。

2.3 事例 3 同一と考えられる攻撃者からの複数組織への攻撃

2017 年 6 月、J-CSIP の情報共有活動を通じて、**同一と考えられる攻撃者から、J-CSIP 内の国内企業 2 社へビジネスメール詐欺（BEC）が試みられていたことが判明しました**。

2017 年 6 月 2 日、J-CSIP の参加組織のひとつ（以下、A 社）より、被害には至らなかったが、ビジネスメール詐欺が試みられた（メールは英語だった）という情報提供がありました。このため、IPA は、A 社で確認された攻撃手口等の情報を整理し、6 月 6 日に、J-CSIP 内で情報共有を行いました。

この情報共有を行った日（6 月 6 日）、**別の業界（SIG）の参加組織（以下、B 社）から、情報共有を行ったメール本文と、返信先に使われている攻撃者のメールアドレスの情報が一致するメールが着信していた**との情報提供がありました。これによって、同一と考えられる攻撃者から、B 社に対しても同じようにビジネスメール詐欺が試みられていたことが判明しました。

すなわち、短期間（1 週間）のうちに、**業種が異なる国内企業 2 社へと連続してビジネスメール詐欺が試みられた**ということになります。

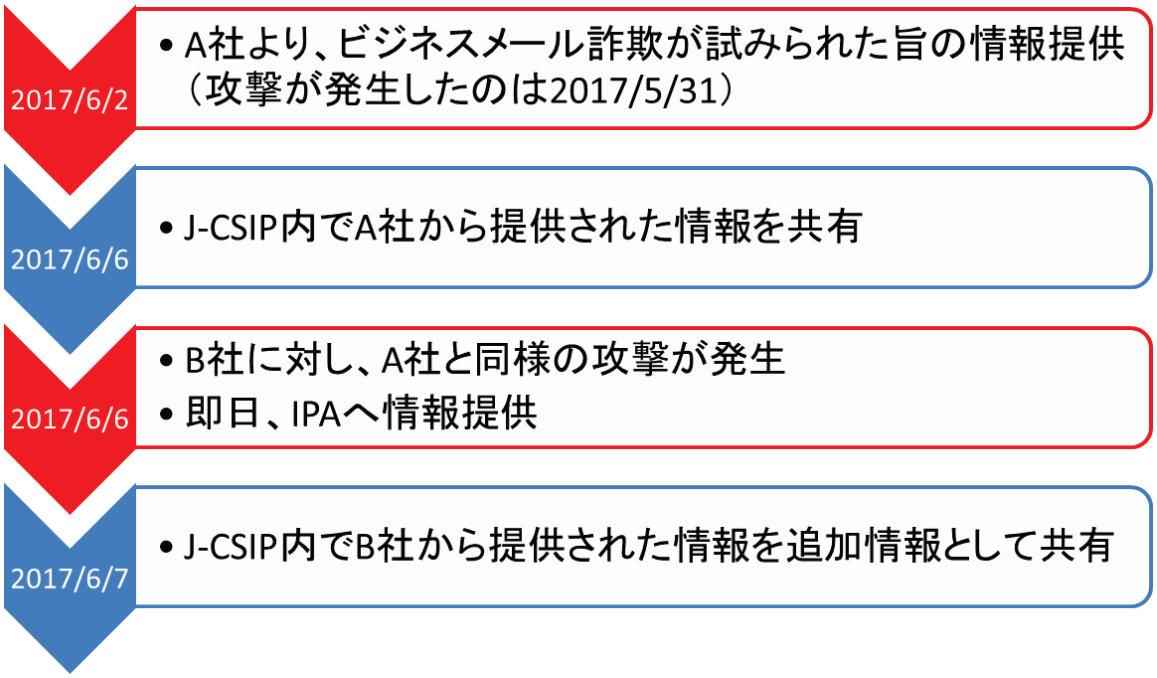

図 2-7 事例 3:ビジネスメール詐欺の 2 件の情報提供と共有の流れ

今回確認されたビジネスメール詐欺の手口は、企業の経営者（CEO）を詐称し、財務責任者（CFO）を騙そうとするものでした。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 2:経営者等へのなりすまし」に該当します。

今回の 2 件の事例では、**「送信元（From）メールアドレスを本物のメールアドレスに偽装し、返信先（Reply-to）メールアドレスを攻撃者のメールアドレスにする」**という手口が使われました。

（1）攻撃手口の詳細

今回の事例では、攻撃者が A 社および B 社の CEO になりすまし、次のようなメールを送信してきました。

- メールの送信元（From ヘッダ）には、本物の CEO の名前やメールアドレスを設定
- メールの返信先（Reply-To ヘッダ）には、攻撃者が取得したメールアドレスを設定

電子メールの仕組み上、From ヘッダは、メールを送信する側が任意の内容に指定する（偽装する）ことができます。そして、メール受信者のメール表示画面には、この From ヘッダの内容が「差出人」として表示されるため、あたかも本物の CEO から送信されたメールのように見えます。

この状態でメールに返信すると、返信メールの送り先は Reply-To ヘッダを基に設定されるため、From ヘッダに書かれた本物の CEO のメールアドレスではなく、攻撃者のメールアドレスとなります。よって、返信メールの作成画面で、この異常に気づくことができなければ、攻撃者とメールをやりとりしてしまうことになってしまいます。

A 社の事例では、A 社と攻撃者の間で数回のメールのやりとりが行われましたが、幸い、A 社側が途中で不審であると気づくことができたため、被害には至りませんでした（図 3）。また、その後の調査で、他の 2 名の社員へも同一の本文のメールが着信していたことが判明し、**計 3 名**へ攻撃が試みられていたことが分かっています。

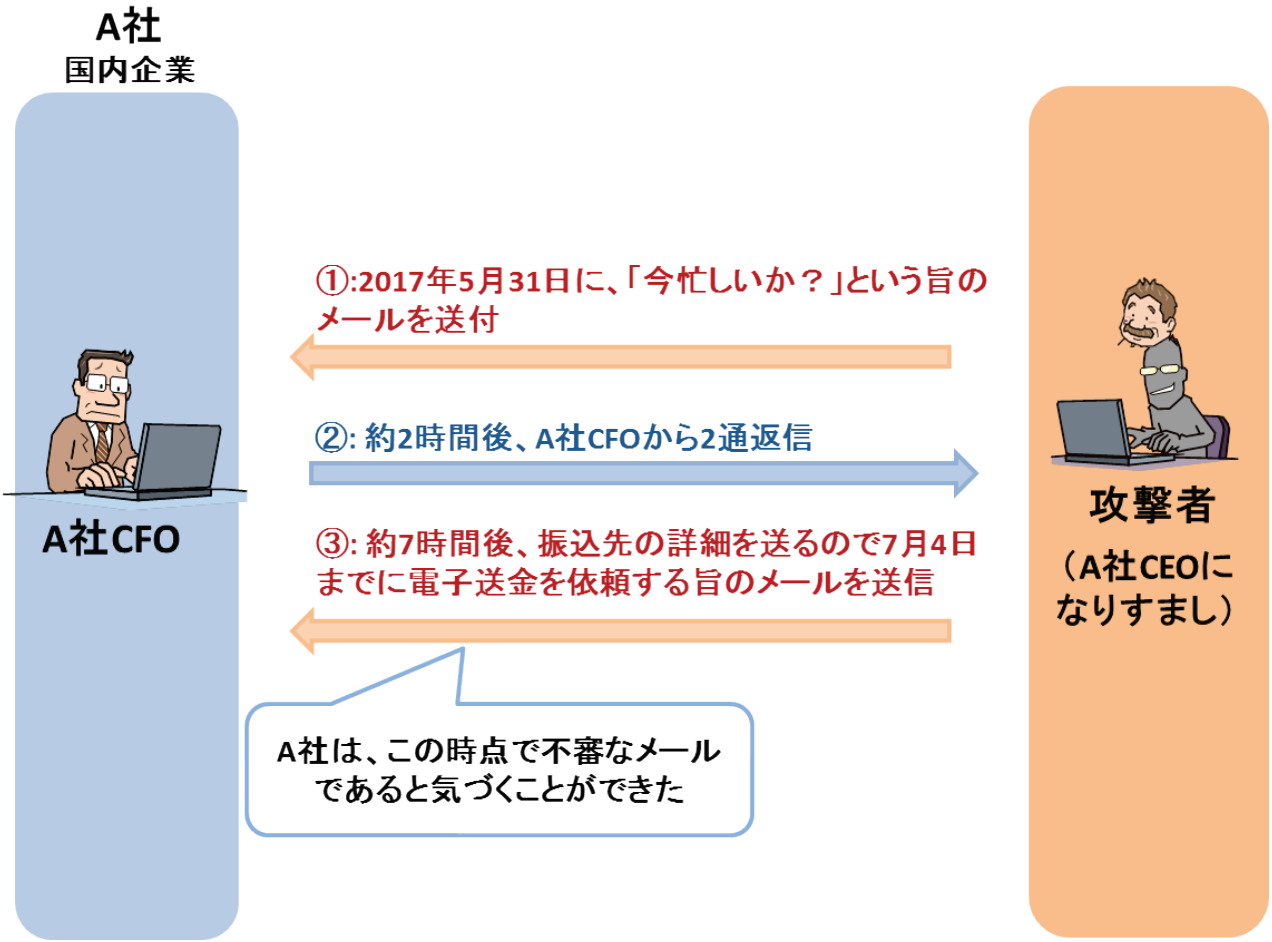

図 2-8 事例 3：攻撃者とのやりとり（A 社の事例）

（2）攻撃者からのメール

続いて、B 社において、A 社と同等の攻撃を確認したとの情報提供がありました。

B 社に着信したメールは、A 社に最初に着信したものと件名は異なっていましたが、Reply-To ヘッダに設定されている**攻撃者のメールアドレスや本文の内容が同一**であり、From ヘッダと Reply-To ヘッダを使って詐称を行う手口も同じでした。

攻撃者は B 社の CEO になりすまし、B 社の現職の CFO と前任の CFO の **2 名**に対して同様のメールを送り付けていました。B 社は、攻撃者からのメールへ返信せず、被害に至りませんでしたが、仮に B 社が攻撃者へメールを返信していた場合、A 社と同じくビジネスメール詐欺が試みられたものと推測しています。

参考までに、B 社に対して送付された攻撃メールを図 2-9 に示します。

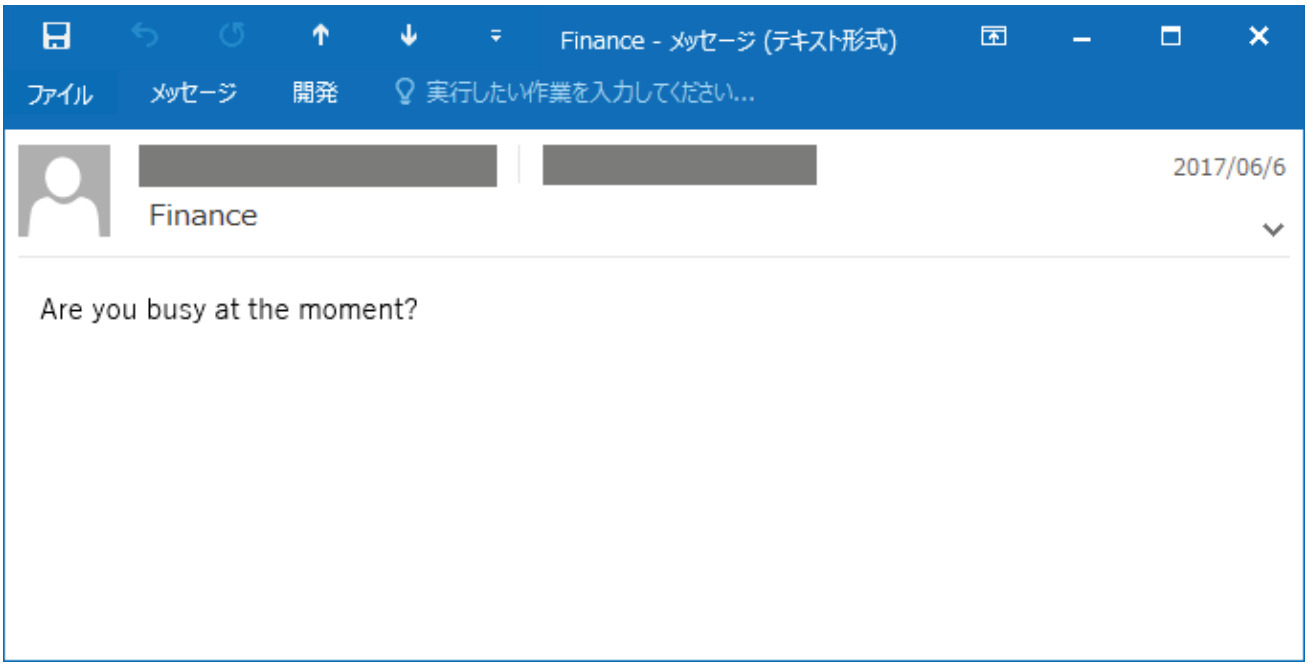

図 2-9 事例 3:攻撃者からのメール（B 社の事例）

2.4 事例 4 海外関係企業の CEO を詐称する攻撃

2018 年 3 月、日本国内組織の海外関連企業（A 社）において、A 社の CEO になりすました攻撃者から、偽の振り込みを要求するメールを送り付けられるというビジネスメール詐欺が試みられました。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 2：経営者等へのなりすまし」に該当します。

本事例では、支払側である A 社の支払い手続きの中で、メール受信者とは別の担当者がメールを確認したところ、不審な点に気づくことができたため、被害は発生しませんでした。

（1） 攻撃の手口の詳細

本事例では、詐欺の過程において、A 社の CEO になりすました攻撃者が、次のようなメールを送信してきました。

- メールの送信元（From ヘッダ）には、本物の CEO のメールアドレスを設定
- メールの返信先（Reply-To ヘッダ）には、攻撃者のメールアドレスを設定

これは、事例 3 の手口と同じ手口です。

本件の攻撃者が送信したメールの Reply-To ヘッダには、次のメールアドレスが指定されていました。

Reply-To ヘッダ： 【A 社 CEO の正規のメールアドレスのローカル部】 @ ●●ipad . com

※ドメイン部は一部伏せている。

メールアドレスのドメインが「●●ipad . com」となっているのは、受信者がメールの返信先が通常とは異なることに気づいた際に、「これは A 社の CEO が、iPad でメールを送受信しているからであろう」と受信者が錯誤することを狙った[14]ものである可能性があります。

[14] メールの末尾に、iPad からの送信である旨の記載もありました。

（2） 攻撃者からのメール

本事例では、図 2-10 のメールを起点として、図 2-11 に示すように、A 社の担当者と攻撃者との間でメールのやりとりが行われましたが、幸い、A 社の支払い手続きの中で、メールの受信者が、別の担当者へ偽メールが転送したところ、別の担当者が不審であると気づくことができたため、被害には至りませんでした。

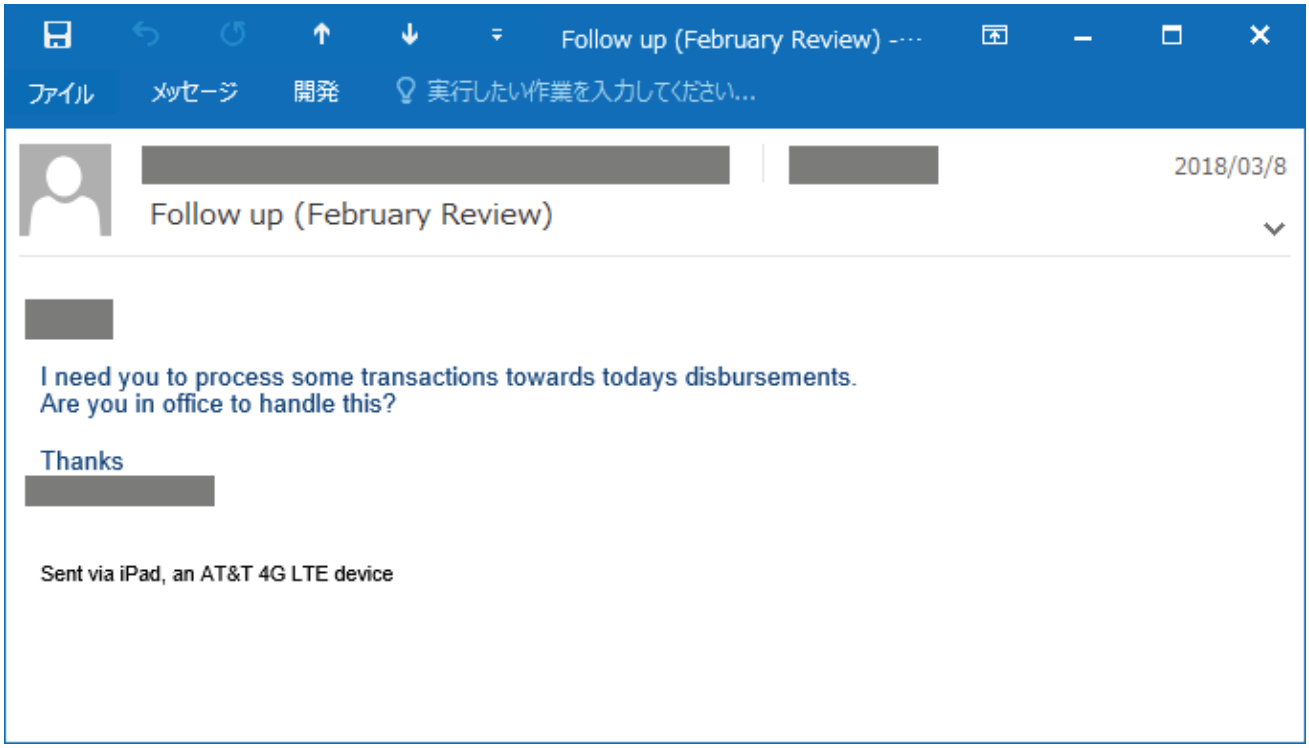

図 2-10 事例 4:攻撃者からのメール

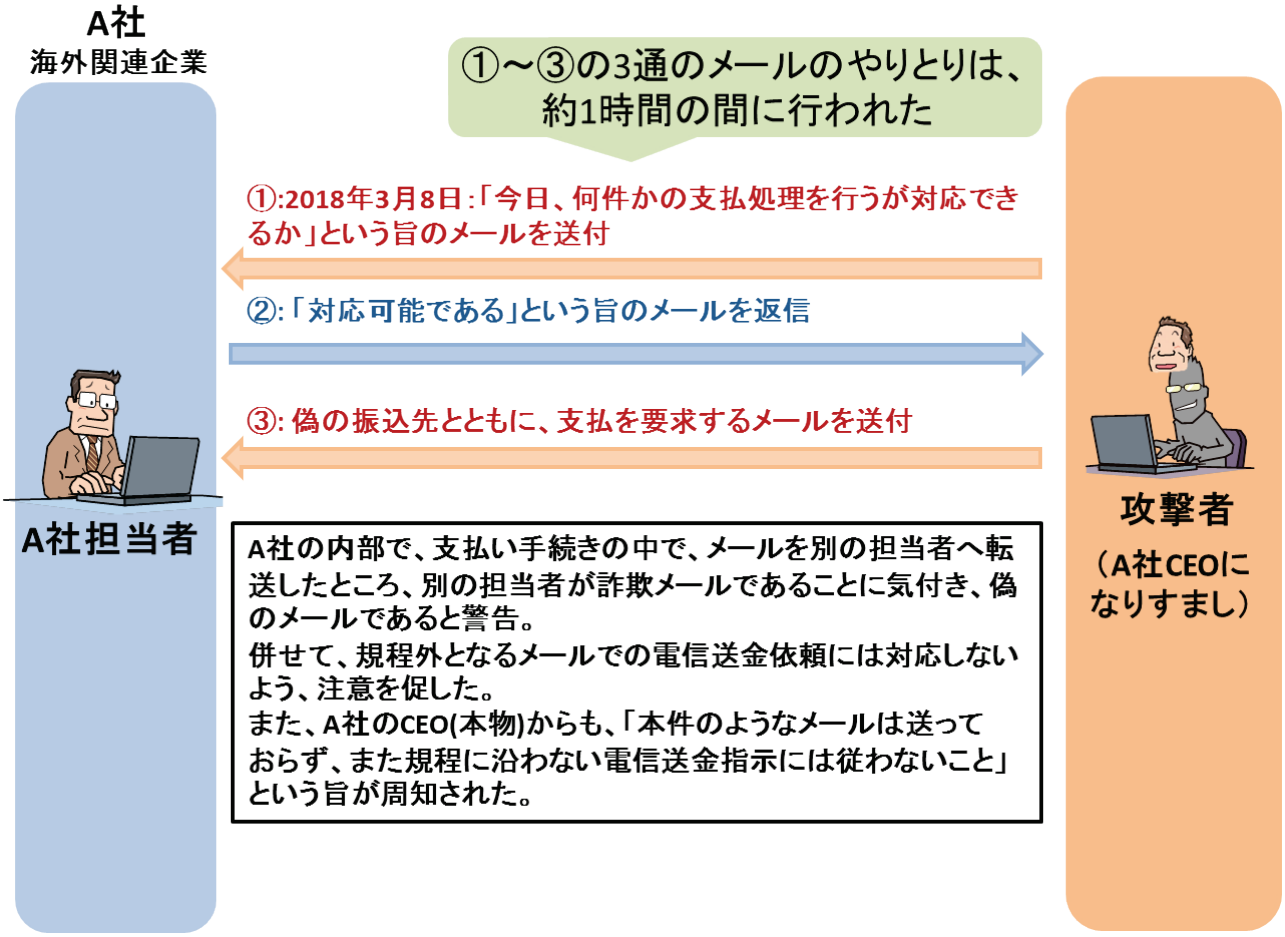

図 2-11 事例 4:攻撃者とのやりとり

本件の攻撃者は、典型的なビジネスメール詐欺の手口で攻撃を行ってきました。しかしながら、メールのやりとりが約 1 時間の間に行われていることから、攻撃者は周到に準備した上で攻撃を行っているものと考えられます。

A 社で徹底されている通り、ビジネスメール詐欺への対策を念頭に置いた電信送金に関する社内規程を整備すること、複数の担当者が確認するといった対策が有効であると考えます。

2.5 事例 5 海外取引先を狙った攻撃

2018 年 7 月、日本国内の企業（請求側）と、海外の取引先企業（支払い側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が発生しました。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当します。

本事例では、海外の取引先企業の担当者が、不審であると気づき、請求側である日本国内の企業へ問い合わせを行ったことで、詐欺であることが発覚し、金銭的な被害には至っていません。

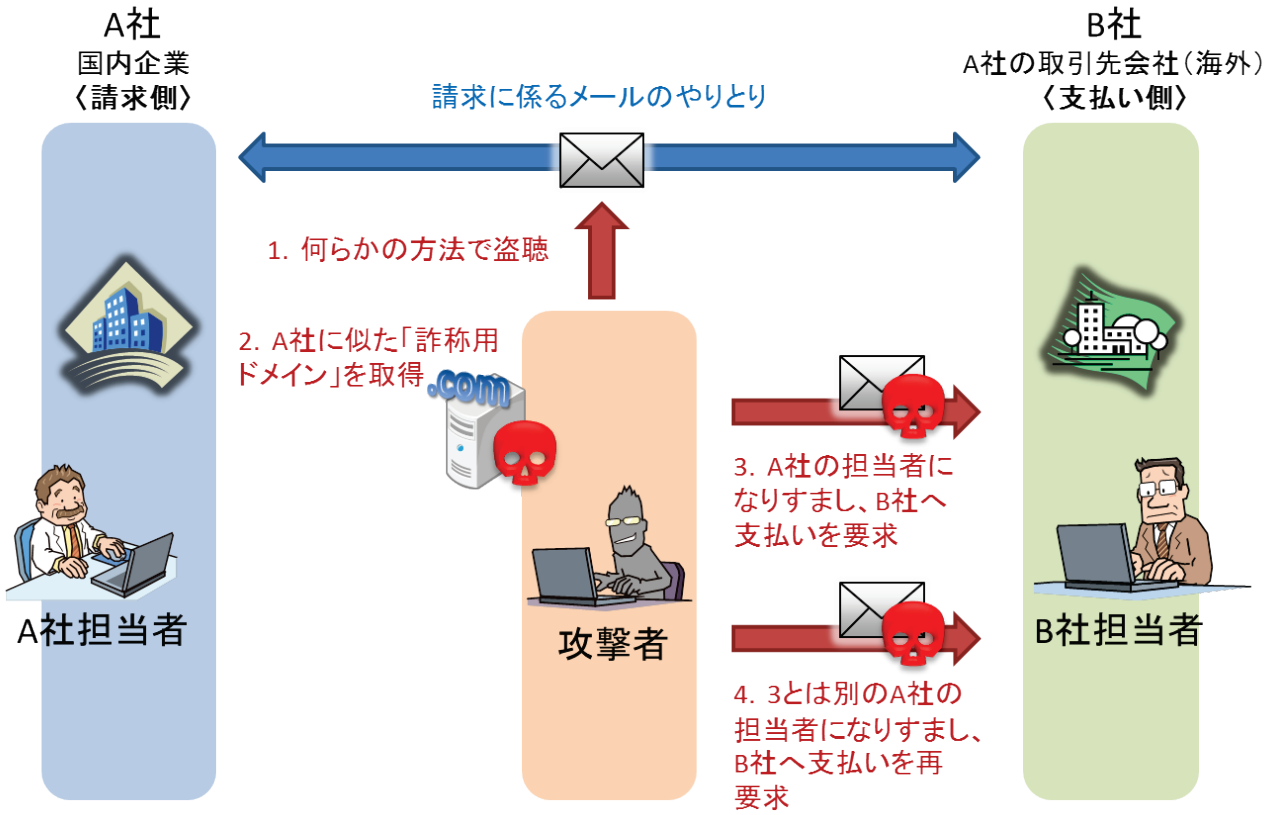

図 2-12 事例 5 の概要

本事例の関係者は次の通りです。

A 社	国内企業。請求側。
B 社	A 社と取引を行っていた海外企業。支払い側。
攻撃者	A 社の担当者になりすまし、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。

本事例では、攻撃者は何らかの方法で、A 社と B 社との間で行われていた請求に係るメールのやりとりを盗み見ていたと思われます。

2018 年 7 月、攻撃者は A 社のドメインに似た「詐称用ドメイン」を取得し、A 社の担当者になりすまして、B 社へ攻撃者が用意した偽の口座へ支払いを行うように依頼するメールを送り付けてきました。その約 30 分後、同じ B 社の担当者へ、先ほどとは異なる A 社の別の担当者になりすまして、再度攻撃者が用意した偽の口座へ支払を行うように依頼するメールを送り付けてきました。

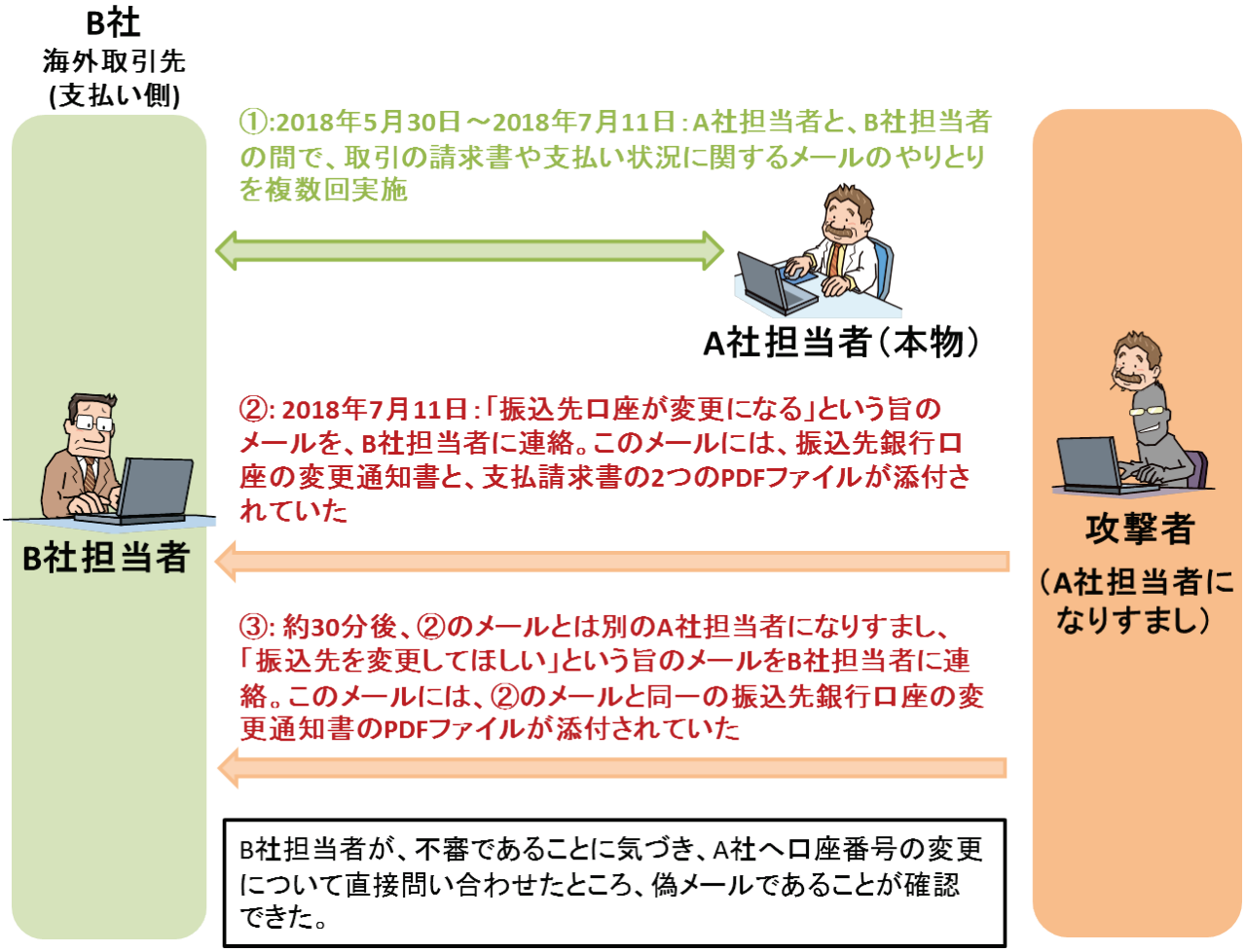

図 2-13 事例 5:攻撃者とのやりとり

実際の攻撃者とのやりとりのメールでは、偽の振り込み先銀行口座の変更通知書と、支払請求書の PDF が送られてきました。この支払請求書の PDF には、A 社の組織のロゴが使われており、本物のように見せかけられていました。

本事例では、B 社の担当者が、不審なメールであると気づき、A 社に対して口座番号変更について直接問い合わせを行ったことで、偽のメールであると確認することができたので、被害はありませんでした。

(1) 詐称用ドメインの取得と悪用

本事例の攻撃者は、A 社の正規のドメインに似通った、偽の「詐称用ドメイン」を新規に取得し、なりすましメールを送信してきました。

本事例の攻撃者が使用した偽のメールアドレスは、次のようにトップレベルドメインが異なるメールアドレスでした。

【本物のメールアドレスのドメイン名】alice @ company . com
【偽物のメールアドレスのドメイン名】alice @ company . **net** ⇒ トップレベルドメインが異なる

※実際に悪用されたものとは異なる。

攻撃者から送られてきたメールの送信元（From）メールアドレスは、A 社の本物のメールアドレスでしたが、メールの返信先（Reply-To）には、詐称用ドメインを使用した偽のメールアドレスが使われていました。（事例 3 や事例 4 と同様の手口）

Reply-To ヘッダ： "alice @ company . com" <alice @ company . net>

※実際に悪用されたものとは異なる。

このメールに対して返信すると（返信メールを作成すると）、次の図 2-14 のようになります。表示名の部分（通常、名前等が表示される部分）が、本物の A 社の担当者のメールアドレスの文字列となっており、一見すると、正しく A 社の担当者へメールを返信しているように見えます。しかし、実際にこのメールが送信される先は、詐称用ドメインのメールアドレス（攻撃者のメールアドレス）となります。

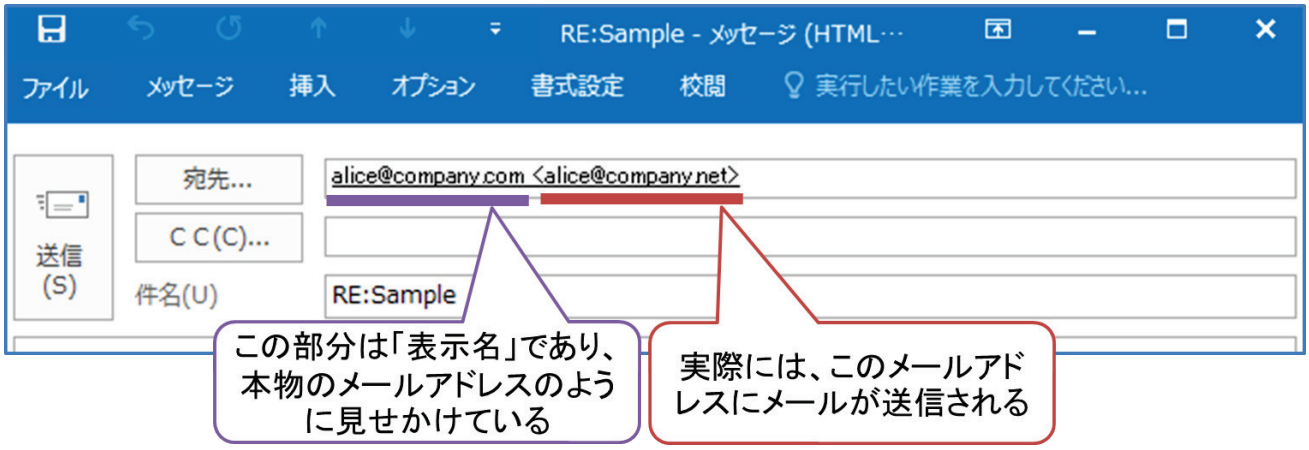

図 2-14 事例 5：返信先のメールアドレスを詐称する手口の例

3　ビジネスメール詐欺への対策

本書で示したように、ビジネスメール詐欺では、巧妙なソーシャルエンジニアリングの手口の応用など、様々な手法を駆使した攻撃が行われます。また、企業や組織の、どの従業員が、いつ攻撃の対象となるかは分かりません。このような攻撃に対抗するため、ビジネスメール詐欺について理解するとともに、不審なメールなどへの意識を高めておくことが重要です。

ビジネスメール詐欺の被害にあわないようにするには、次のような対策を行うことが望ましいと考えます。これらの対策は、諜報活動を目的とするような標的型サイバー攻撃における、標的型攻撃メールへの対策とも共通する点があります。

◆　取引先とのメール以外の方法での確認

振込先の口座の変更といった、通常とは異なる対応を求められた場合は、送金を実施する前に、電話やFAX などメールとは異なる手段で、取引先に事実を確認することを勧めます。メールに書かれている署名欄は攻撃者によって偽装されている可能性があるため、信頼できる方法で入手した連絡先を使ってください。

特に、突然の振込先の変更や、急な行動を促すような請求や送金の依頼メールは、ビジネスメール詐欺ではないか、よく確認することを勧めます。

また、急な決済手段の変更を求められた場合にも、ビジネスメール詐欺ではないか、確認することを勧めます。

◆　社内規程の整備

「メール以外の方法での確認」といった手順を含む、ビジネスメール詐欺への対策を念頭に置いた、電信送金に関する社内規程を整備することも必要です。複数の担当者によるチェック体制を徹底するといった対策も有効です。

◆　普段とは異なるメールに注意

ビジネスメール詐欺では、海外取引におけるメールでのやりとりで多く発生しています。英語が母国語ではない国との取引の場合、多少間違った英語でのメールが着信したとしても不思議ではありません。しかし、その中でも、普段とは異なる言い回しや表現の誤りには注意が必要です。

◆　不審と感じた場合の組織内外での情報共有

ビジネスメール詐欺に限らず、メールは様々なサイバー攻撃の入口の一つであり、注意深く扱うべきです。不審なメールに担当者が気づけることは重要ですが、それと同時に、その情報を適切な部門に報告できる体制が重要です。不審なメールなどの情報を集約することで、他の担当者に届いた攻撃メールに気づくことができ、自組織に対する悪意ある行為を認識することで、対策に繋げることができるかもしれません。

ビジネスメール詐欺の場合、何らかの不審な兆候が、取引先への攻撃を明らかにする可能性もあります。従って、取引先との連絡・情報共有も重要です。

また、例えば自組織を詐称したビジネスメール詐欺を認知した場合、取引先全体あるいは一般に向けて注意喚起を公開することを検討してもいいでしょう。

◆　ウイルス・不正アクセス対策

ビジネスメール詐欺では、攻撃や被害に至る前に、何らかの方法でメールが盗み見られている場合があります。原因は、メールの内容やメールアカウントの情報を窃取するウイルス、メールサーバへの不正アク

セスなどが考えられます。

「不審なメールの添付ファイルは開かない」、「セキュリティソフトを導入し、最新の状態を維持する」、「OSやアプリケーションの修正プログラムを適用し、最新の状態を維持する」といった、基本的なウイルス対策の実施が不可欠です。

また、特に、メールアカウントやメールサーバ（サービス）に対する防御が重要です。「メールアカウントに推測されにくい複雑なパスワードを設定する」、「他のサービスとパスワードを使い回さない」、「多要素認証を設定する」、「社外からアクセス可能なメールサーバやクラウドサービスを使用している場合、アクセス元を制限したり、不審なログインを監視する」といった、職員のメールを不正アクセスから守る対策が必要です。

◆　電子署名の付与

取引先との間で請求書などの重要情報をメールで送受信する際は、電子署名を付けるといった、なりすましを防止する対策も有効です。

◆　類似ドメインの調査

ビジネスメール詐欺の攻撃者は、自組織のドメイン名に似た「詐称用ドメイン」を取得し、取引先へ攻撃を行うことがあります。ビジネスメール詐欺に限らず、自組織を詐称するフィッシング攻撃などへの対策としても、定期的に、自組織に似たドメイン名が取得されていないかを確認し、必要であれば注意喚起を行うといった対応も検討してください。

この他、こうした詐欺の存在を前提とした、送金前のチェック体制を強化するなど、「多層防御」の考え方に基づき、ビジネスメール詐欺の攻撃を検知するため、複数の防御層を設けるようにしてください。

参考： IC3 によるビジネスメール詐欺への対策

IC3 のサイトにも、次に挙げるビジネスメール詐欺への対策が掲載されています [15]。

- ウェブベースの無料電子メールアカウントは利用せず、会社用のドメイン名を取得し、そのドメイン名を利用してください。
- ソーシャルメディアや企業のウェブサイトに投稿されている、職務や組織内の階層関係、不在にする時間の情報に注意してください。
- 内密にお願いしますという要求や、迅速な行動を求める要求に対しては、ビジネスメール詐欺の攻撃ではないか疑ってください。
- 既存の財務プロセスに対して、2 段階認証プロセスの実施などを含め、次のようなセキュリティシステムや手順を検討してください。
  - 請求にかかる重要な手続きの確認のため、電話など他の通信チャネルを持つようにしてください。このとき、攻撃者からの傍受を防ぐため、なるべく早く手段を確立してください。
  - 取引による電子メールでのやりとりは、双方の電子署名を使用するようにしてください。
  - 不審なメールを受信した場合、組織内の適切な部署に報告し、そのメールを削除してください。ウイルスが含まれている可能性があるため、添付ファイルの開封や、メール内の URL などはアクセスしないでください。
  - 電子メールを相手に返信する場合、「返信」ではなく「転送」を選択し、正しいメールアドレスを入力して返信をしてください。
  - 企業の電子メールアカウントに 2 つの要素による認証を実装することを検討してください。2 つの要素は、当事者しか知りえない情報（パスワードなど）と、当事者しか持たないもの（トークンなど）を使ってください。
- 企業間のやりとりで使われていたメールアドレスの変化（個人メールアドレスへ連絡を要求されるなど）が発生した場合、そのリクエストは不正である可能性があるため、電話などによって正しい相手であるかを確認してください。
- 企業の電子メールに似た記号をもつ電子メールにフラグを立てるなどの侵入検知システムのルールを作成してください。例えば、abc_company.com という正規のメールアドレスに対して、abc-company.com のようなメールアドレスのメールが着信した場合、不正な電子メールであるとフラグを立てるものです。
- 実際の企業ドメインとは若干異なるすべてのドメインをメールフィルタなどに登録してください。
- 支払いに係る変更があった場合、組織内の 2 人以上の署名が必要など 2 段階認証を設定してください。
- 電話による相手確認を行う場合、電子メールの署名に記載されている電話番号ではなく、既知の電話番号を使用して確認してください。
- 取引相手の慣習、取引にかかる送金の遅延とその理由、支払金額などを把握してください。
- 送金先の変更などに関するすべての電子メールの要求を注意深く精査し、その要求が正規のものであるかを判断してください。

上記以外の追加情報などは、米国司法省のサイト [16]にある「Best Practices for Victim Response and Reporting of Cyber Incidents」に掲載されています。

---

[15] Business E-mail Compromise: The 3.1 Billion Dollar Scam (IC3)
https://www.ic3.gov/media/2016/160614.aspx

[16] United States Department of Justice （DOJ）
https://www.justice.gov/

4　おわりに／謝辞

ビジネスメール詐欺は、攻撃が成功してしまうと組織に多額の損失を与えうる脅威であり、その被害件数も増加傾向にあります。国内でも一部事件となっていますが、詳しい事例の情報は、まだ多くありません。

この状況を受け、2017 年 4 月に、ビジネスメール詐欺の注意喚起を行いました。注意喚起後も、J-CSIP の参加組織からは継続してビジネスメール詐欺の情報提供があり、また 2017 年 12 月にはビジネスメール詐欺による大規模な被害が報道されるなど、ますます注意が必要になっています。今回、日本語のビジネスメール詐欺の事例を確認したことで、英語のメールによるやりとりを行わない企業や組織も攻撃対象となりうる（攻撃の範囲が拡大した）状況となったため、再び注意喚起を行うこととしました。

本書では、J-CSIP の参加組織から情報提供をいただき、J-CSIP 内で情報共有を行った、実際のビジネスメール詐欺の事例とその手口について、情報提供元から開示許可をいただいた上で、詳しく紹介しました。情報提供元の組織様においては、匿名とすることが前提とはいえ、一部は金銭被害にまで至っている、このような貴重な情報の提供と開示許可をいただいていることに、深く謝意を表します。

J-CSIP は、今後も情報共有の運用を着実に行い、また、参加組織の拡大、情報共有の効率向上等を図っていくとともに、情報の集約と横断分析によって得られる情報など、共有する情報の拡充を進めていきます。そして、J-CSIP 外の組織とも連携を進めながら、情報の共有と集約を通し、サイバー攻撃に対する組織および組織群の防衛力の向上を推進していきます。

以上