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

～ 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

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

本書の要旨 1
1　はじめに 2
1.1　ビジネスメール詐欺「BEC」の概要 2
1.2　ビジネスメール詐欺の 5 つのタイプ 4
2　ビジネスメール詐欺事例の紹介 8
2.1　事例 1 国内企業を狙った攻撃 9
2.2　事例 2 国内企業の海外支社を狙った攻撃 12
2.3　事例 3 海外取引先を狙った攻撃 14
2.4　事例 4 海外関係企業を狙った攻撃 16
3　ビジネスメール詐欺の騙しの手口 17
3.1　メールアドレスのなりすましの手口 17
3.2　同報メールアドレスの改変の手口 18
3.3　攻撃に利用するドメインの手口 21
4　ビジネスメール詐欺への対策 22
5　おわりに／謝辞 25

添付資料

・【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）の活動において、参加組織から情報提供いただいたビジネスメール詐欺「BEC」の事例および騙しの手口について情報を共有し、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

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。

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」について、事例の紹介と、その騙しの手口について紹介し、注意喚起を行うものです。

ビジネスメール詐欺の手口による事件は海外[2]のみならず国内でも発生し、初の逮捕者が出る[3,4]など、ビジネスメール詐欺は、今後ますます注意が必要な状況となりつつあります。読者の方々へは、この脅威について、本書を通じてまず知っていただき、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が、本書ではビジネスメール詐欺と呼び説明します。

米国連邦捜査局（Federal Bureau of Investigation：FBI）によると、2013 年 10 月から 2016 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）に報告されたビジネスメール詐欺の被害件数は 15,668 件、被害総額は約 11 億（1,053,849,635）米ドルにのぼっています。その後、2016 年 6 月 14 日までに被害件数は 22,143 件、被害総額は約 31 億（3,086,250,090）米ドルへと増加しました[5]。1 件あたりの平均被害額は約 14 万米ドル（日本円では約 1,600 万円程度）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。

本書では、実際に攻撃者によって行われたビジネスメール詐欺の事例を紹介し、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、組織・企業の担当者が騙されていることを示しています。

企業における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の脅威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にするために、本書での事例をもとに組織内のセキュリティ意識の向上に役立ててください。

また、これらの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。

---

[2] 振り込め詐欺、標的は CFO　巨額の詐取金狙い（日本経済新聞）
http://www.nikkei.com/article/DGXLASDZ27IZK_V10C17A3EA6000/

[3] メールをハッキング、詐欺容疑などでナイジェリア人逮捕（朝日新聞デジタル）
http://www.asahi.com/articles/ASK2J5VP9K2JUTIL040.html

[4] メールに細工、振込先変更=不正引き出し容疑で男逮捕-警視庁（時事ドットコム）
http://www.jiji.com/jc/article?k=2017021601136&g=soc

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

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 章で実際に確認された 4 つの事例（国内企業を狙った攻撃、国内企業の海外支社を狙った攻撃、海外取引先を狙った攻撃、海外関係会社を狙った攻撃）を紹介します。

そして、3 章でこれら 4 つの事例で用いられた、特筆すべき「騙しの手口」について解説し、4 章ではビジネスメール詐欺への対策について説明します。

参考：BEC の日本国内での呼び方

本書では、BEC（Business E-mail Compromise、ビーイーシー）を「ビジネスメール詐欺」と呼んでいますが、現時点では国内の様々な機関によってその呼び方が異なっています。参考までに、それらの呼び方を示します。これらは全て同じ脅威を指しています。

- ビジネスメール詐欺[6,7]
- ビジネス電子メール詐欺[8]
- 法人間の外国送金の資金をだまし取る詐欺[9,10]
- 外国送金の資金を騙し取る詐欺（外国送金詐欺）[11]
- 外国送金詐欺[12]
- 外国送金の送金先口座を変更させる偽の電子メール等[13]
- 企業を標的としたオレオレ詐欺[14]

---

[6] 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

[7] 信頼関係を築いてから電信送金を指示する形に進化した、新しい BEC 詐欺（シマンテック）
http://www.symantec.com/connect/blogs/bec-2

[8] 組織に被害をもたらすビジネス電子メール詐欺（マカフィー）
http://blogs.mcafee.jp/mcafeeblog/2016/08/post-c210.html

[9] 法人間の外国送金の資金をだまし取る詐欺にご注意！（一般社団法人 全国銀行協会）
http://www.zenginkyo.or.jp/topic/detail/nid/3561/

[10] 法人間の外国送金の資金をだまし取る詐欺にご注意ください（三井住友銀行）
http://www.smbc.co.jp/security/attention/index15.html

[11] 偽のビジネスメールにより外国送金の資金を騙し取る詐欺（外国送金詐欺）にご注意ください！（三菱東京 UFJ 銀行）
http://www.bk.mufg.jp/info/phishing/20141121.html

[12] 法人のお客さまにおいて発生している外国送金詐欺にご注意ください（みずほ銀行）
https://www.mizuhobank.co.jp/crime/info_houjin_soukin.html?rt_bn=cp_top_warn1

[13] 外国送金の送金先口座を変更させる偽の電子メール等にご注意ください（ゆうちょ銀行）
http://www.jp-bank.japanpost.jp/crime/crm_gaikokusokin.html

[14] BEC（business email compromise）詐欺に注意（たちばな総合法律事務所）
http://www.law-tachibana.jp/column/saiken/665/

1.2 ビジネスメール詐欺の 5 つのタイプ

IC3[15]やトレンドマイクロ社[16]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います。

- タイプ 1：取引先との請求書の偽装
- タイプ 2：経営者等へのなりすまし
- タイプ 3：窃取メールアカウントの悪用
- タイプ 4：社外の権威ある第三者へのなりすまし
- タイプ 5：詐欺の準備行為と思われる情報の詐取

ここでは、IC3 やトレンドマイクロ社が分類しているそれぞれのタイプの概略を説明します。

なお、本書では、IC3 などの考え方に沿い、「ソーシャルエンジニアリング[17]の手法を応用したメールなどを組織・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、直接的に金銭を狙うサイバー攻撃」を、ビジネスメール詐欺と位置付けています。

参考：国内で発生したビジネスメール詐欺の手口による事件[18,19]

2017 年 2 月、詐欺と組織犯罪処罰法違反（犯罪収益の隠匿）の容疑で、ナイジェリア国籍の男性が逮捕されたとの報道がありました。この事案は、東京の貿易会社からフィリピンの農業用肥料販売会社に送信されたメールを不正に差し替えられたことで、不正な振込先に送金させられたとのことです。このとき、逮捕者は両社のメールのやりとりを監視し、貿易会社のアドレスを偽装してフィリピンの企業へなりすましメールを送っていました。

この手口は、「ビジネスメール詐欺の 5 つのタイプ」のうち、タイプ 1 に相当すると思われます。

一方、別の事例[20]では、ビジネスメール詐欺に似た手口を使い、競合相手の営業秘密（見積書）の入手を試みたという事案も発生しています。今後、金銭に限らず、営業秘密も同様の手口で詐取する攻撃も増えていく可能性があり、組織・企業側は、従業員ひとりひとりの注意が必要です。

---

[15] 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。

[16] 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

[17] なりすましなどを行い、騙す相手（人間）の心理的な隙やミスにつけこんで情報を盗む技術。

[18] メールをハッキング、詐欺容疑などでナイジェリア人逮捕（朝日新聞デジタル）
http://www.asahi.com/articles/ASK2J5VP9K2JUTIL040.html

[19] メールに細工、振込先変更=不正引き出し容疑で男逮捕-警視庁（時事ドットコム）
http://www.jiji.com/jc/article?k=2017021601136&g=soc

[20] 「ビジネスメール詐欺」国内外で続発、注意！…狙いは企業情報・マネー　大阪府警が初摘発（産経 WEST）
http://www.sankei.com/west/news/170131/wst1701310011-n1.html

● **タイプ 1:取引先との請求書の偽装**

このタイプは、「偽の請求書詐欺(The Bogus Invoice Scheme)」や、「サプライヤー詐欺(The Supplier Swindle)」、「請求書偽装の手口(Invoice Modification Scheme)」などと呼ばれています。

海外の企業との取引を行っている企業が主に被害にあう傾向があります。

この攻撃は、請求に係るやりとりをメールなどで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書などを送りつけ、振り込みをさせるというものです。

このとき、攻撃者は取引に係るやりとりをなんらかの方法によって事前に盗聴し、取引や請求に関する情報や、関係している従業員のメールアドレスや氏名などを入手していることがあります。

図 1-1 取引先との請求書の偽装

● **タイプ 2:経営者等へのなりすまし**

このタイプは、「CEO 詐欺(CEO Fraud)」や、「企業幹部詐欺(Business Executive Scam)」、「なりすまし詐欺(Masquerading)」、「金融業界送金詐欺(Financial Industry Wire Frauds)」などと呼ばれています。

企業の財務担当者などの金銭管理を行う部門が被害にあう傾向があります。

この攻撃は、攻撃者が企業の経営者や企業幹部などになりすまし、企業の従業員に攻撃者の用意した口座へ振り込みをさせるというものです。

このとき、事前に攻撃者はなんらかの方法によって、企業の経営者などのメールアドレスを調べ、より本物らしくなりすましを行う場合もあります。

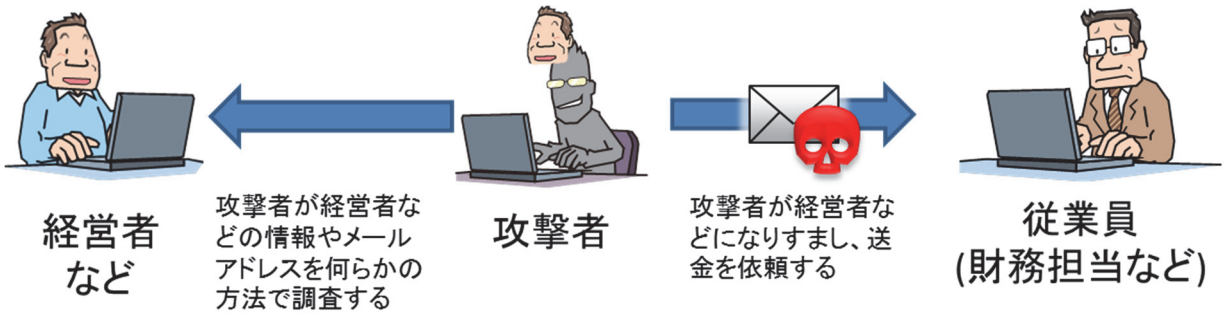

図 1-2 経営者等へのなりすまし

● **タイプ 3:窃取メールアカウントの悪用**

この攻撃は、攻撃者が従業員のメールアカウントをなんらかの手段を用いて窃取し、乗っ取った上で、そのメールアカウント(従業員)の取引実績のある別の企業の担当者へ、攻撃者の用意した口座に差し替えた偽の請求書などを送りつけ、振り込みをさせるというものです。

メール受信者は、あたかも正当な相手からのメールであるかのように見えるため、攻撃であると気づきにくいことが特徴です。

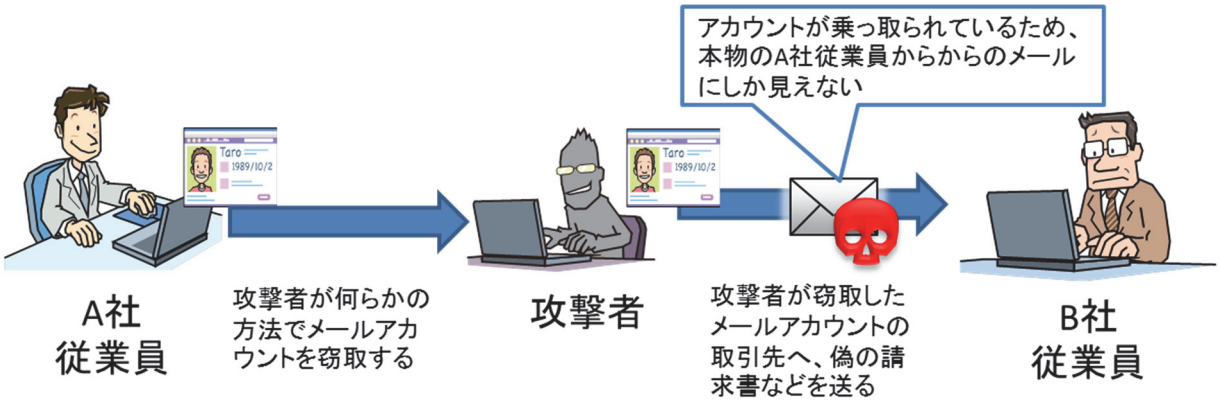

図 1-3 窃取メールアカウントの利用

● **タイプ 4:社外の権威ある第三者へのなりすまし**

この攻撃は、攻撃者が弁護士や法律事務所といった社外の権威ある第三者へなりすまし、企業の財務担当者などに対して、攻撃者の用意した口座への振り込みをさせるというものです。

この攻撃では、例えば、攻撃者は企業の社長の代理人弁護士になりすまし、緊急を要する機密案件であるかのような旨をその企業の担当者に伝え、秘密裏かつ迅速に対応するべきであるかのように圧力をかけて詐欺を仕掛けてきます。

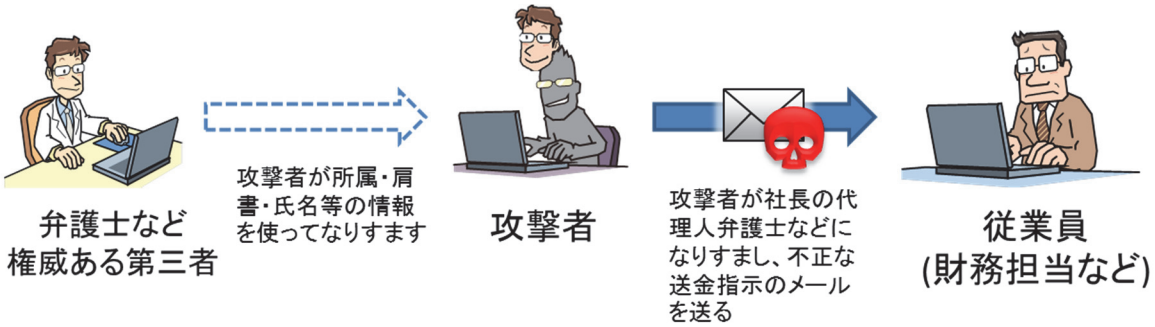

図 1-4 社外の権威ある第三者へのなりすまし

- **タイプ 5:詐欺の準備行為と思われる情報の詐取**

この攻撃は、攻撃者が詐欺の標的とする企業の経営者や経営幹部、または人事担当などの特定任務を担う従業員になりすまし、企業内の他の従業員の個人情報などの情報を詐取しようとするもので、不正な送金要求の前段階として行われることがあります。

この攻撃によって詐取された情報は、攻撃者のサーバなどに送られ、別の攻撃などに悪用されることがあります。この攻撃はタイプ 1～4 と異なり、金銭の詐取ではなく、詐欺を行うための情報を得ることが目的と思われます。

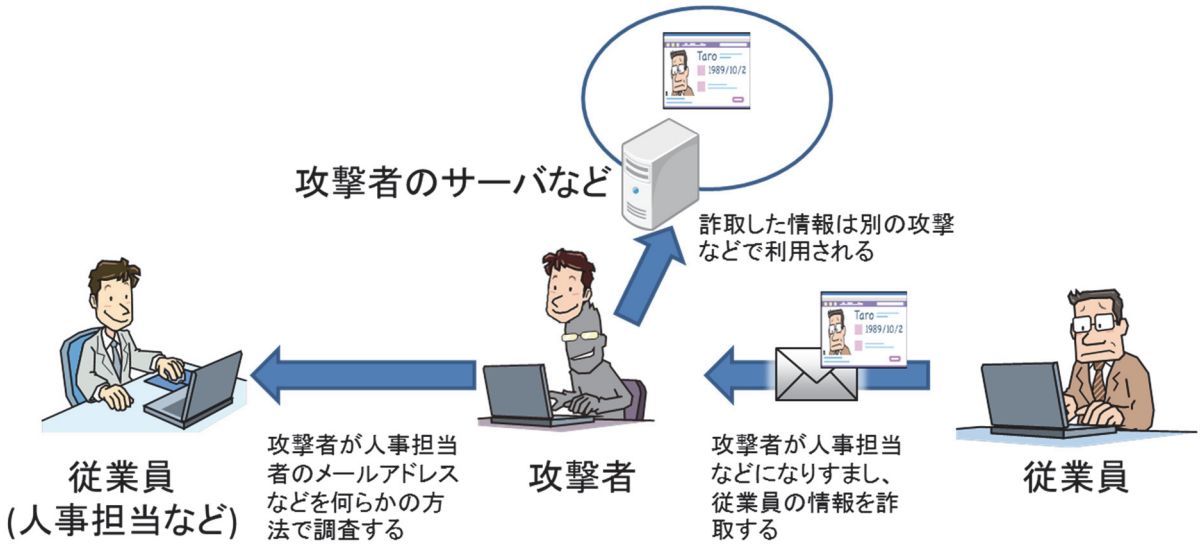

図 1-5 詐欺の準備行為と思われる情報の詐取

2　ビジネスメール詐欺事例の紹介

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。

J-CSIP では、2015 年から 2016 年にかけて発生したビジネスメール詐欺に関する 4 件の情報提供を受けています。攻撃は業界分野に関わらず発生しており、具体的には、3 つの SIG（Special Interest Group：類似の産業分野同士が集まったグループ）において情報提供を受け、その情報について J-CSIP 内で情報共有を実施しています。

この 4 件の事例のうち、3 件は海外企業との請求に係るメールでのやりとり（タイプ 1）で攻撃を受けています。残りの 1 件は、国内企業の社長を騙り、海外関係企業に対して送金依頼をする攻撃（タイプ 2）を受けています。また、攻撃者から送られてきたメールはすべて英語が使われていました。

日本語の偽メールや、国内企業間での被害事例は J-CSIP 内では現在までに確認されていませんが、今後注意が必要です。本書で解説するように、攻撃者は巧妙な手口を用いてくるという認識のもと、偽のメールに注意を払うように心がけてください。

本章では、次の 4 件の事例を紹介します[21]。

- ◆ 事例 1 国内企業を狙った攻撃
- ◆ 事例 2 国内企業の海外支社を狙った攻撃
- ◆ 事例 3 海外取引先を狙った攻撃
- ◆ 事例 4 海外関係企業を狙った攻撃

[21] これらの事例では、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。

2.1 事例 1 国内企業を狙った攻撃

2015 年 12 月と 2016 年 1 月に、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ました。

本事例では、支払い側である国内企業で攻撃者からの不審なメールに気付くことができたため、金銭的な被害は発生していません。

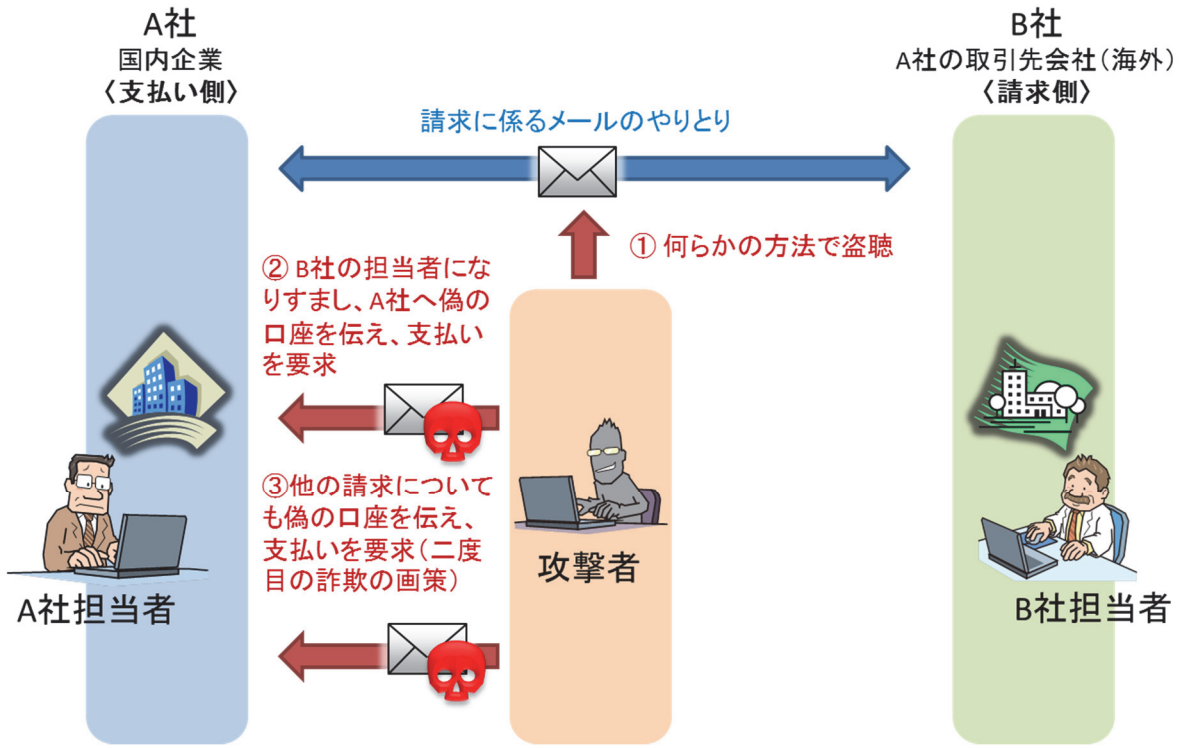

図 2-1 事例 1 の概要

本事例には、次の 3 者が関係しています。

A 社	国内企業。取引における支払い側。攻撃者からのメールを偽物であると見破ることができ、金銭的被害は発生しなかった。
B 社	A 社と取引を行っていた海外企業。請求側。
攻撃者	B 社の担当者になりすまし、ビジネスメール詐欺を使って A 社から金銭を詐取しようとした。

まず、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（図 2-1 ①）。

2015 年 12 月、攻撃者は請求内容が決まった後に、B 社の担当者になりすまして、A 社へ攻撃者が用意した偽の口座に支払いを行うよう依頼する内容のメールを送りつけてきました（図 2-1 ②）。このとき、A 社は攻撃者からのメールを偽物であると気づくことができたため、偽の口座への送金を行うことなく、金銭的被害を免れました。

さらにこの攻撃者は、2016 年 1 月にも、引き続き B 社の担当者になりすまし、A 社へ未払いの他の請求について、新たに攻撃者が用意した偽の口座に支払うよう要求してきました（図 2-1 ③）。一度は攻撃に失敗していますが、それでも詐欺を画策したものと考えられます。このときも、A 社は攻撃者からのメールを偽物であると気づくことができたため、偽の口座への送金を行うことなく、金銭的被害を免れました。

実際に攻撃に利用されたメールは、次のようなものでした。どちらのメールも、A 社と B 社のメールでのやりとりの最中に、B 社になりすました攻撃者が割り込むように、偽の口座への振り込みをさせようとしています。

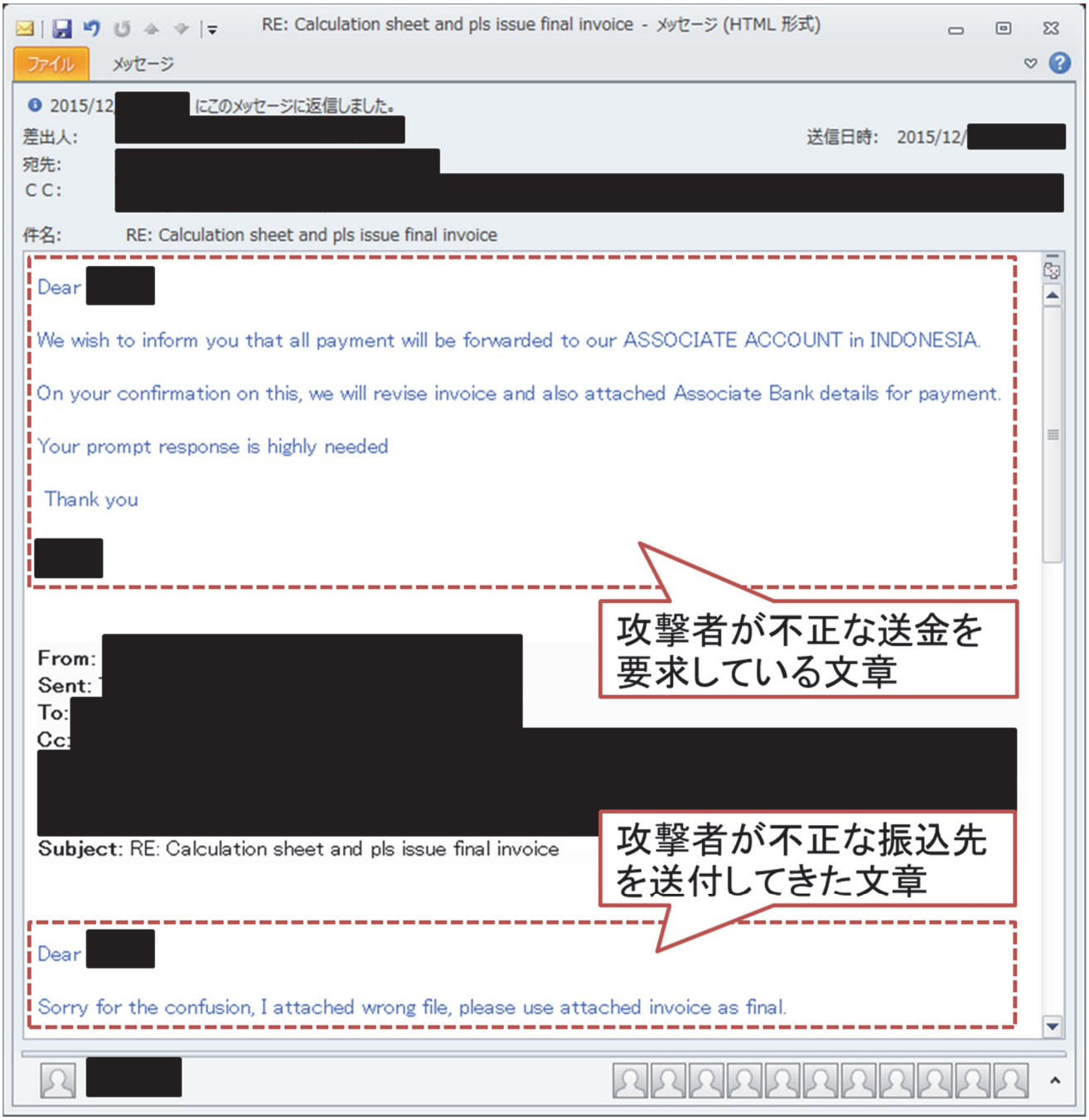

図 2-2 2015 年 12 月に攻撃者から送られてきた攻撃メール

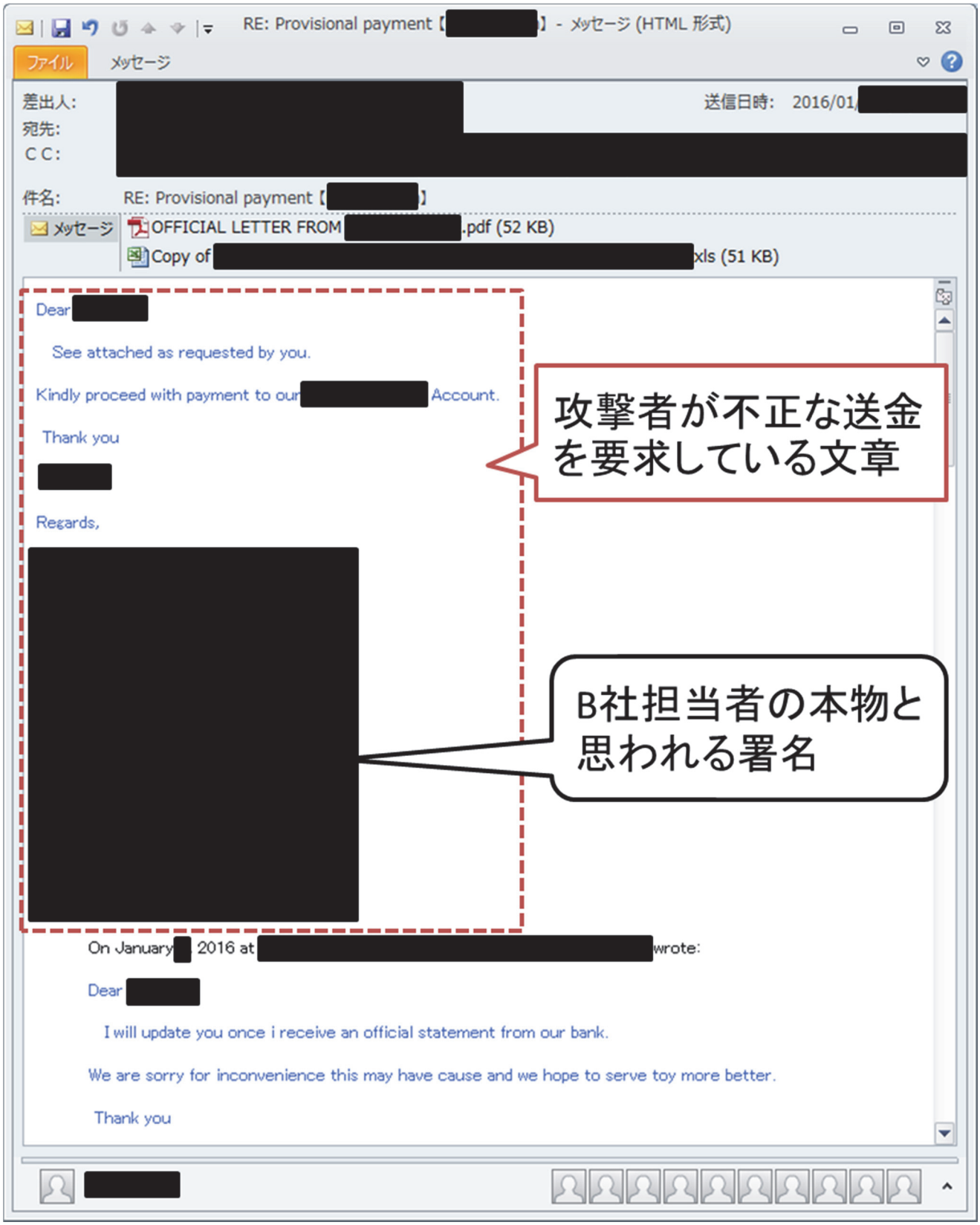

図 2-3 2016 年 1 月に攻撃者から送られてきた攻撃メール

2.2 事例 2 国内企業の海外支社を狙った攻撃

2015 年 8 月に、日本国内に本社のある企業の海外支社（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ました。

本事例では、国内企業の海外支社が、攻撃者の用意した偽の銀行口座への送金を行ってしまい、金銭的な被害を受けています。

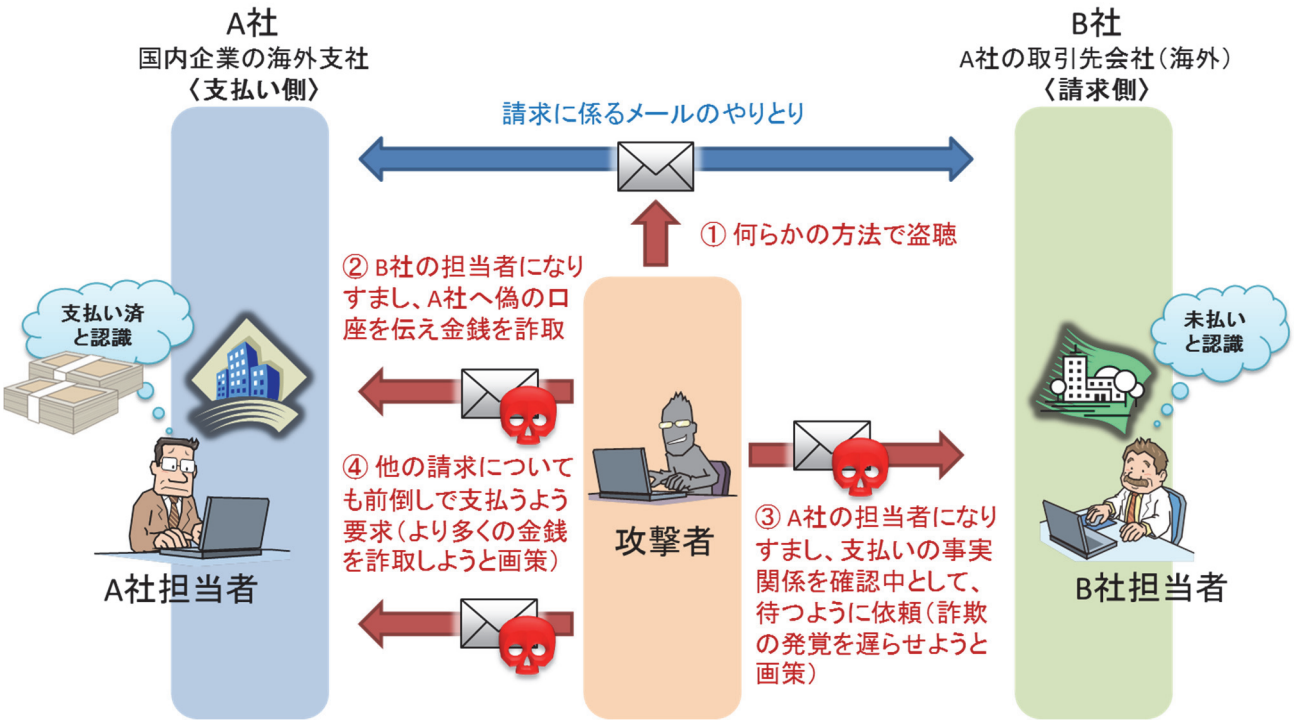

図 2-4 事例 2 の概要

本事例には、次の 3 者が関係しています。

A 社	国内企業の海外支社。支払い側であり、金銭的被害を受けた。
B 社	A 社と取引を行っていた海外企業。請求側。
攻撃者	A 社の担当者と B 社の担当者、両方になりすまし、ビジネスメール詐欺を使って A 社から金銭を詐取した。

まず、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（図 2-4 ①）。

タイミングを見はからい、攻撃者は B 社の担当者になりすまして、A 社へ攻撃者の用意した偽の口座に支払いを行うよう依頼する内容のメールを送りつけてきました（図 2-4 ②）。このとき、A 社は偽の口座への送金を行っていますが、詐欺であると認識せず、支払い済みと認識していたようです。一方、B 社は A 社からの支払いが行われていないため、支払遅延が発生していると認識していました。

この攻撃者は、同時に A 社側の担当者にもなりすまして、B 社に対し、A 社からの支払いを事実関係を確認中なので待つように依頼していました（図 2-4 ③）。攻撃者はこの連絡により、B 社に対して、「A 社側でも支払いが遅れていると認識している」と誤解させ、A 社への電話などによる直接的な確認を思い留まらせることで、詐欺が発覚することを遅らせようと画策したものと考えられます。

さらにこの攻撃者は、不正な送金要求で金銭の詐取が成功した後も、引き続き B 社の担当者になりすまし、支払い予定日がまだ来ていない他の請求事項についても、支払い遅延が発生したことを理由に、前倒しで（攻撃者の口座へ）支払うようA 社へ要求しています（図 2-4 ④）。これは、より多くの金銭を詐取しようと画策したものと考えられます。

実際に攻撃の中でやりとりされたメールのうち、攻撃者が A 社と B 社の両方になりすまし、支払遅延を理由とした前倒しの支払いを要求するメールは、次のようなものでした。過去のメールからの引用部分が長く、企業の担当者と攻撃者がやりとりを繰り返していることが伺える内容となっています。

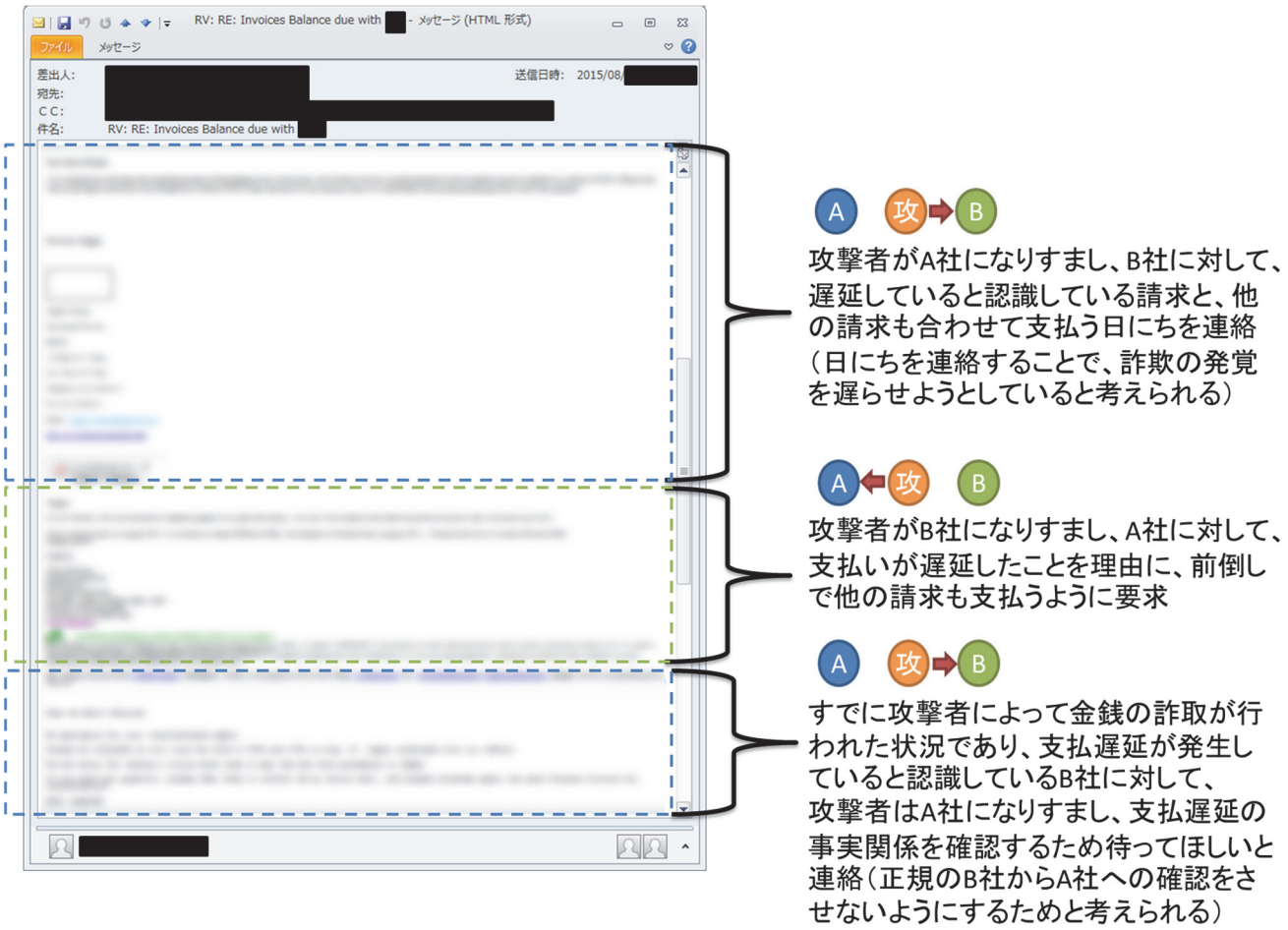

図 2-5 攻撃に使われたメール

2.3 事例 3 海外取引先を狙った攻撃

2016 年 9 月に、日本国内に本社のある企業の海外支社（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ました。

本事例では、国内組織の海外支社の取引先である海外企業が、攻撃者の用意した偽の銀行口座への送金を行ってしまい、金銭的な被害を受けています。

本件は、情報提供元である企業（の海外支社）が、攻撃者によるなりすましの対象となり、これにより、取引先の企業が金銭被害を受けることとなりました。情報提供元企業には直接の金銭被害は発生しませんでしたが、取引に関わる情報が何らかの原因によって攻撃者に漏れていた可能性が高く、詐取された損害の補償を両社によってどう扱うのか、また、訴訟の可能性の有無などが憂慮される事例です。

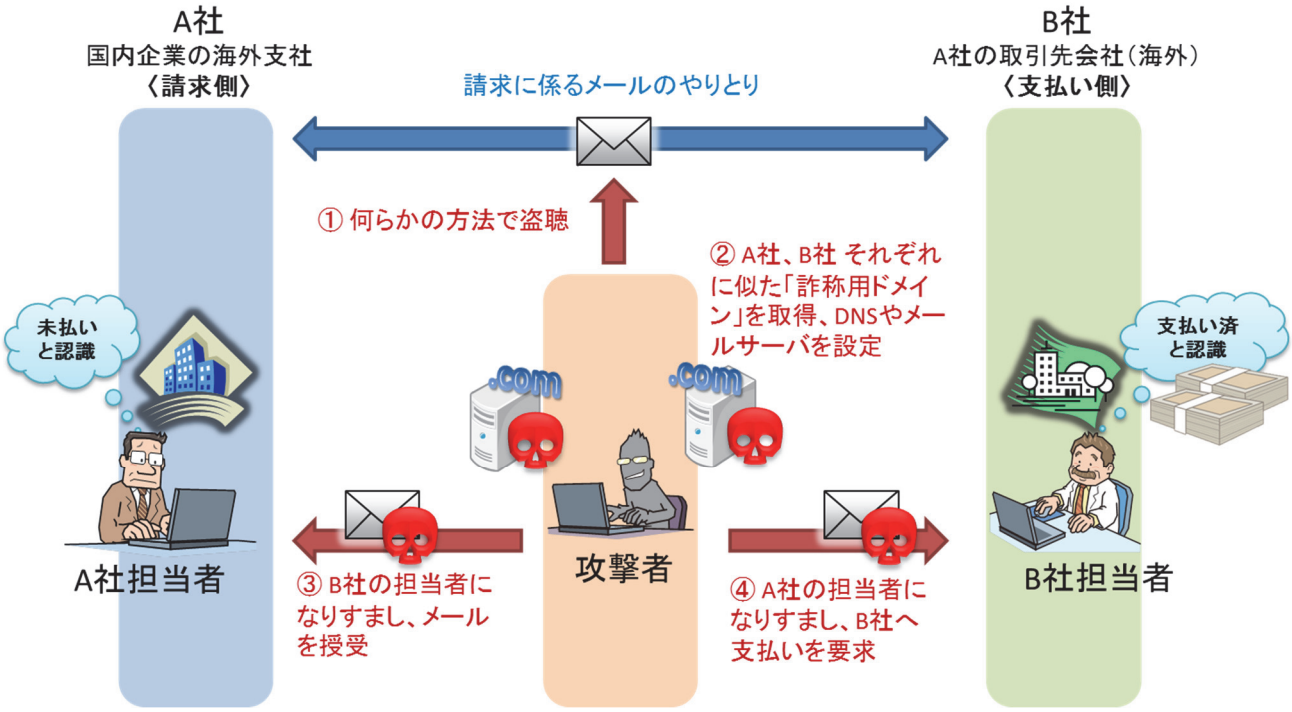

図 2-6 事例 3 の概要

本事例には、次の 3 者が関係しています。

A 社	国内企業の海外支社。請求側。
B 社	A 社と取引を行っていた海外企業。支払い側であり、金銭的被害を受けた。
攻撃者	A 社の担当者と B 社の担当者、両方になりすまし、ビジネスメール詐欺を使って B 社から金銭を詐取した。

まず、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（図 2-6 ①）。

攻撃者は A 社と B 社それぞれの企業のドメイン名に似た**「詐称用ドメイン」**を取得し、なりすましメールを送受信するための DNS（Domain Name System）サーバやメールサーバを設定しました（図 2-6 ②）。

タイミングを見て攻撃者は B 社の詐称用ドメインを使って B 社の担当者になりすまし、A 社に対し、請求に係る書類の送付を促すようなメールを送付し、A 社と攻撃者はメールのやりとりを行いました（図 2-6 ③）。

その後、攻撃者は A 社の詐称用ドメインを使って A 社の担当者になりすまし、B 社へ偽の口座への口座変更と支払いを要求するメールを送付しています（図 2-6 ④）。おそらく、A 社とのやりとりの中で攻撃者が得た情報が悪用されており、このとき、B 社は偽の口座へ送金を行い、金銭的被害を受けています。

実際に攻撃に利用されたメールのうち、攻撃者が A 社になりすまし、B 社へ新しい口座へ送金を要求する内容のメールは、次のようなものでした。事例 2 と同様、企業の担当者と攻撃者で、メールのやりとりを繰り返しているため、過去のメールからの引用部分が長くなっています。

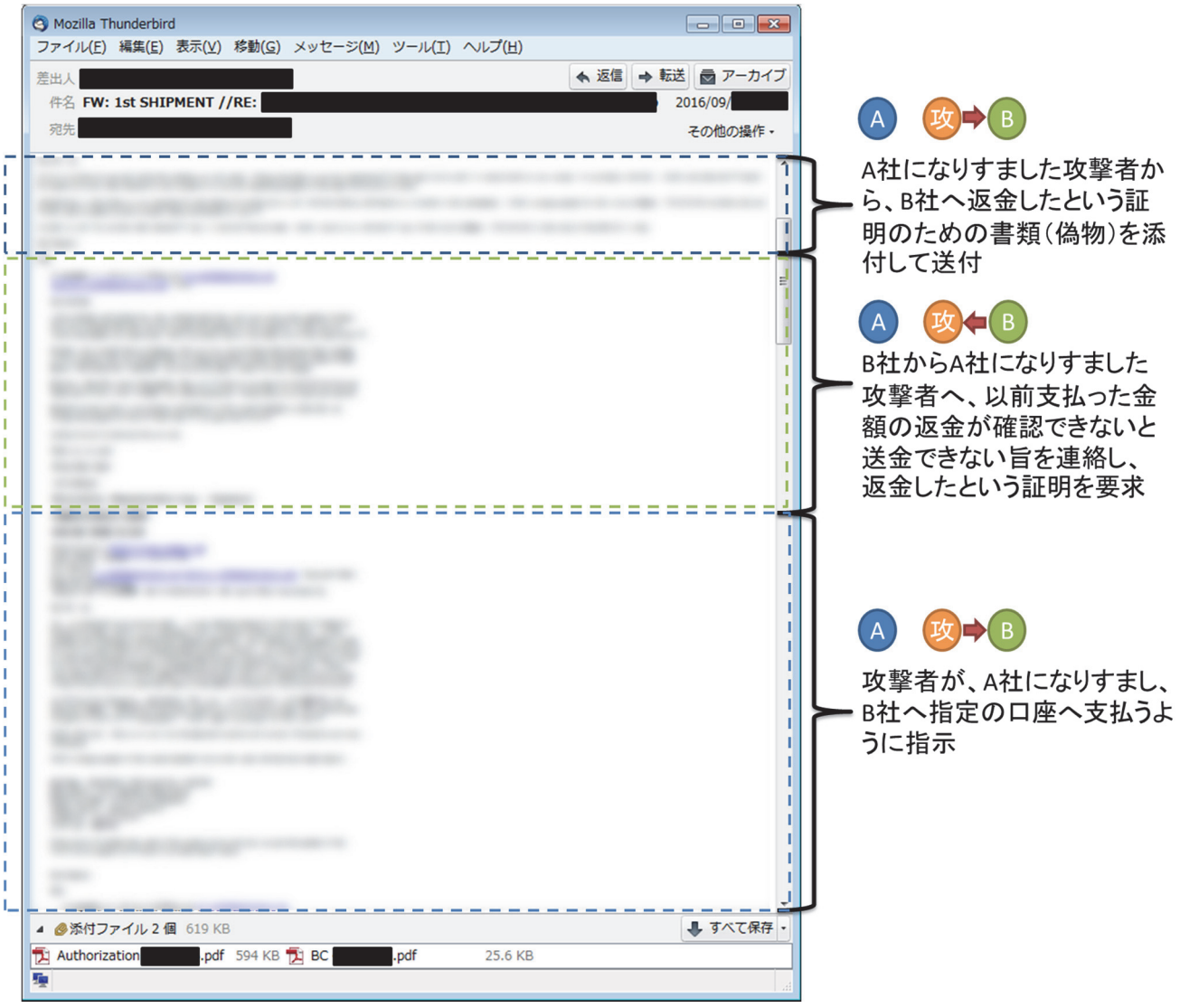

図 2-7 攻撃に使われたメール

2.4 事例 4 海外関係企業を狙った攻撃

2015 年 7 月に、日本国内に本社のある企業（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発生しました。

海外関係企業（子会社）が、金銭的な被害に至ったか否かは確認できていません。

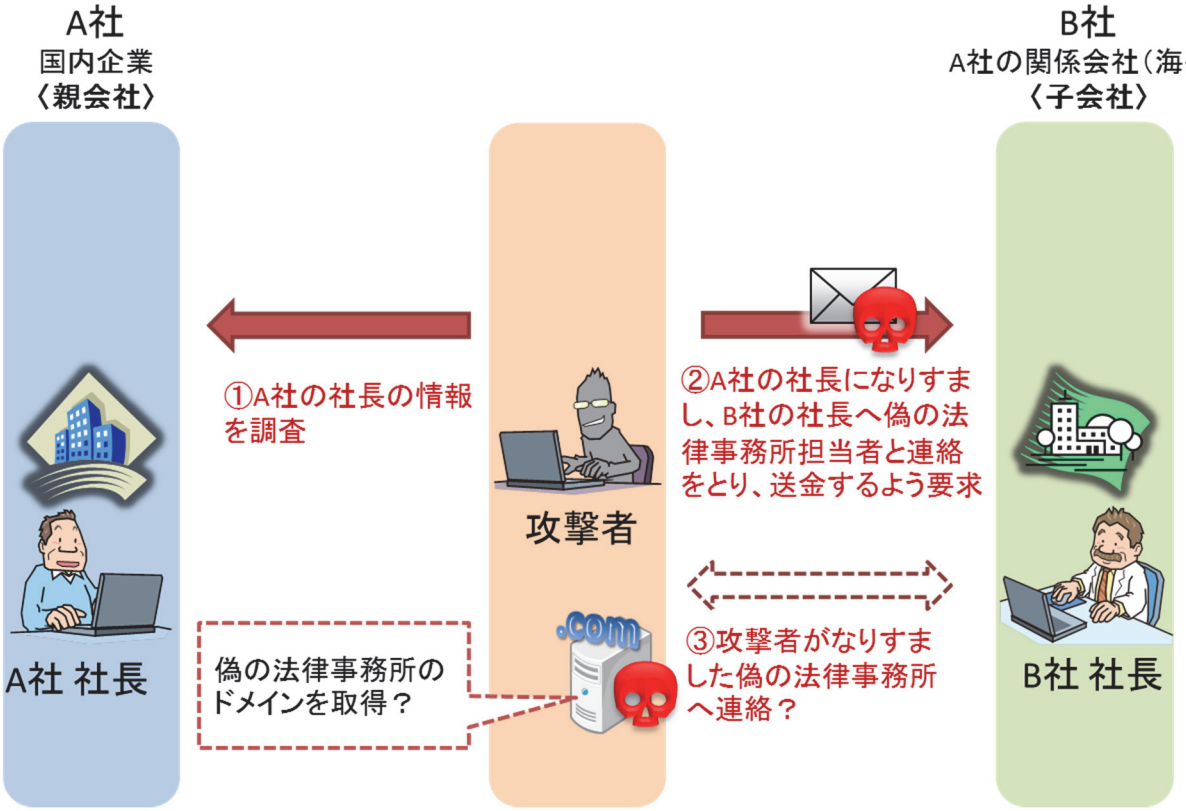

図 2-8 事例 4 の概要

本事例には、次の 3 者が関係しています。

A 社	国内企業。B 社の親会社。
B 社	A 社の海外関係企業で、A 社の子会社。
攻撃者	A 社の社長になりすまし、ビジネスメール詐欺を使って B 社の社長へ海外送金を指示した。

本事例では、攻撃者は何らかの方法で、A 社の社長に関する情報を調査（図 2-8 ①）し、A 社の社長になりすました上で、B 社の社長に対してメールを送付してきました（図 2-8 ②）。このとき、攻撃者は、B 社の社長に対し、海外の法律事務所の担当者と連絡を取って送金を行うように指示しています。攻撃者からのメールには、その法律事務所の担当者であるというメールアドレスが記載されていました。

攻撃者が提示した法律事務所のメールアドレスのドメインは、**実在する法律事務所のドメインによく似た偽のドメイン**でした。ドメイン登録情報（whois 情報）を確認すると、この偽のドメインは同じ攻撃者によって取得された可能性を示しており、攻撃者が**「一人二役」**を演じる詐欺を試みた可能性があります。

B 社の社長が、攻撃者から送られてきたメールに記載されている法律事務所の担当者と、その後連絡をとった可能性もありますが、今回の情報提供の対象外となっています（図 2-8 ③）。

3　ビジネスメール詐欺の騙しの手口

本章では、4 つの事例において、実際に攻撃者によって使われた、ビジネスメール詐欺の騙しの手口の要点について説明します。攻撃者の手口を知ることで、ビジネスメール詐欺に騙されないように心がけていただきたいと考えます。

また、本書の「添付資料」では、これらの各事例における詐欺行為が行われた経緯と、用いられた騙しの手口のより詳しい情報を載せています。必要に応じて参照してください。

3.1 メールアドレスのなりすましの手口

ビジネスメール詐欺では、攻撃者は標的とした人物を騙すため、単純に他の人物を詐称するだけでなく、「メールアドレスの見た目」によるなりすましの手口を用いてきます。

この手口では、攻撃者がなりすましに使う、偽のメールアドレスの作り方に特徴があります。本書の事例を含めて、次のような偽のメールアドレスが使われる傾向があります。

① メールアドレスを 1 文字入れ替える
② メールアドレスに 1 文字追加する
③ メールアドレスを 1 文字削除する
④ メールアドレスの一部を誤認しやすい文字に置き換える（例：m（M） → rn（RN））
⑤ フリーメールサービスを使いそれらしいメールアドレスを作る

ここで、本物のメールアドレスを、「alice ＠ company-a ． com」とした場合、攻撃者がなりすましに使ったメールアドレスはどのようなものであるかを、次の図に示します（ここではフリーメールのドメインを、「freemail ． com」としています）。

図 3-1 攻撃者によるメールアドレスのなりすましの例

これに加えて、メールの「差出人表示名」（メールソフトの画面上で表示される名前）に、本物のメールアドレスに似せた長い文字列を使うことで、偽物のメールアドレスであることに気付きにくくさせる手口も確認しています。

3.2 同報メールアドレスの改変の手口

攻撃者がなりすましメールを送っていることの発覚を遅らせるため、あるいは、受信者に本物のメールであると錯覚させるため、攻撃者がメールの To（宛先）や Cc（同報先）に設定するメールアドレスへ細工する手口を確認しています。

本書の事例では、攻撃者がメールの同報メールアドレスに細工することによって、**あたかも複数の担当者が同報でメール送信されているかのように見せかける**という手口で攻撃が行われました。

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。

ここでは、A 社と B 社という企業が、送金取引によるメールをやりとりすると仮定し、A 社と B 社それぞれ 3 名ずつの職員がこの取引に関係しているものとします。A 社は請求側であり、「alice」が請求に係る主担当者、B 社は支払い側であり、「dave」が支払い主担当者であるとします。そして、攻撃者は、A 社の「alice」になりすますため、「alice」のメールアドレスによく似た偽のメールアドレスやドメインを用意し、攻撃を行うものとします。

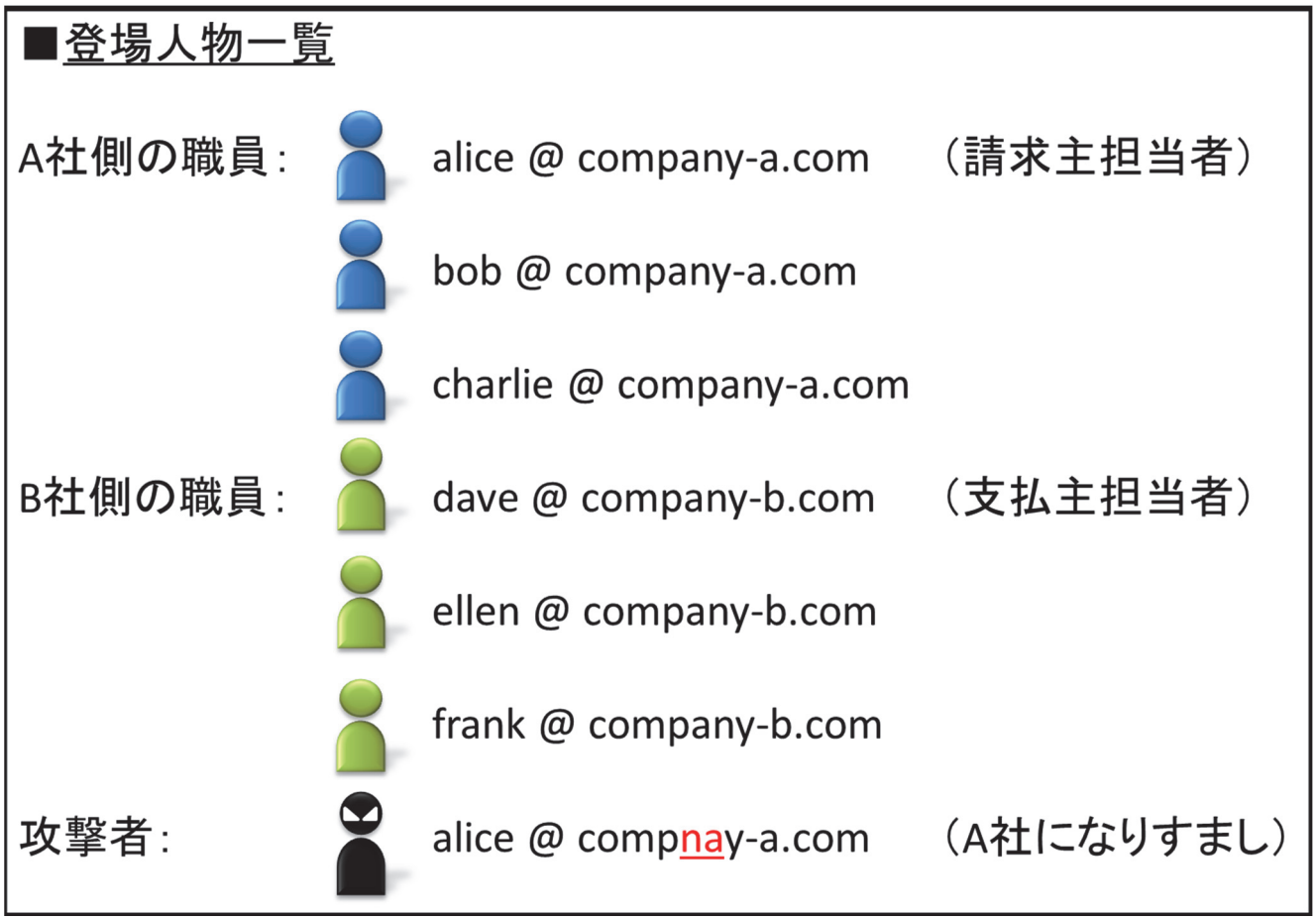

図 3-2 登場人物一覧

このとき、正常な状況で、A 社から B 社に対して、送金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）は請求の主担当である A 社「alice」、宛先（To）は支払いの主担当である B 社「dave」へのメールです。同報先（Cc）には、A 社と B 社の双方の関係者のメールアドレスが含まれます。ビジネス上、このようなやりとりは自然と行われるものです。

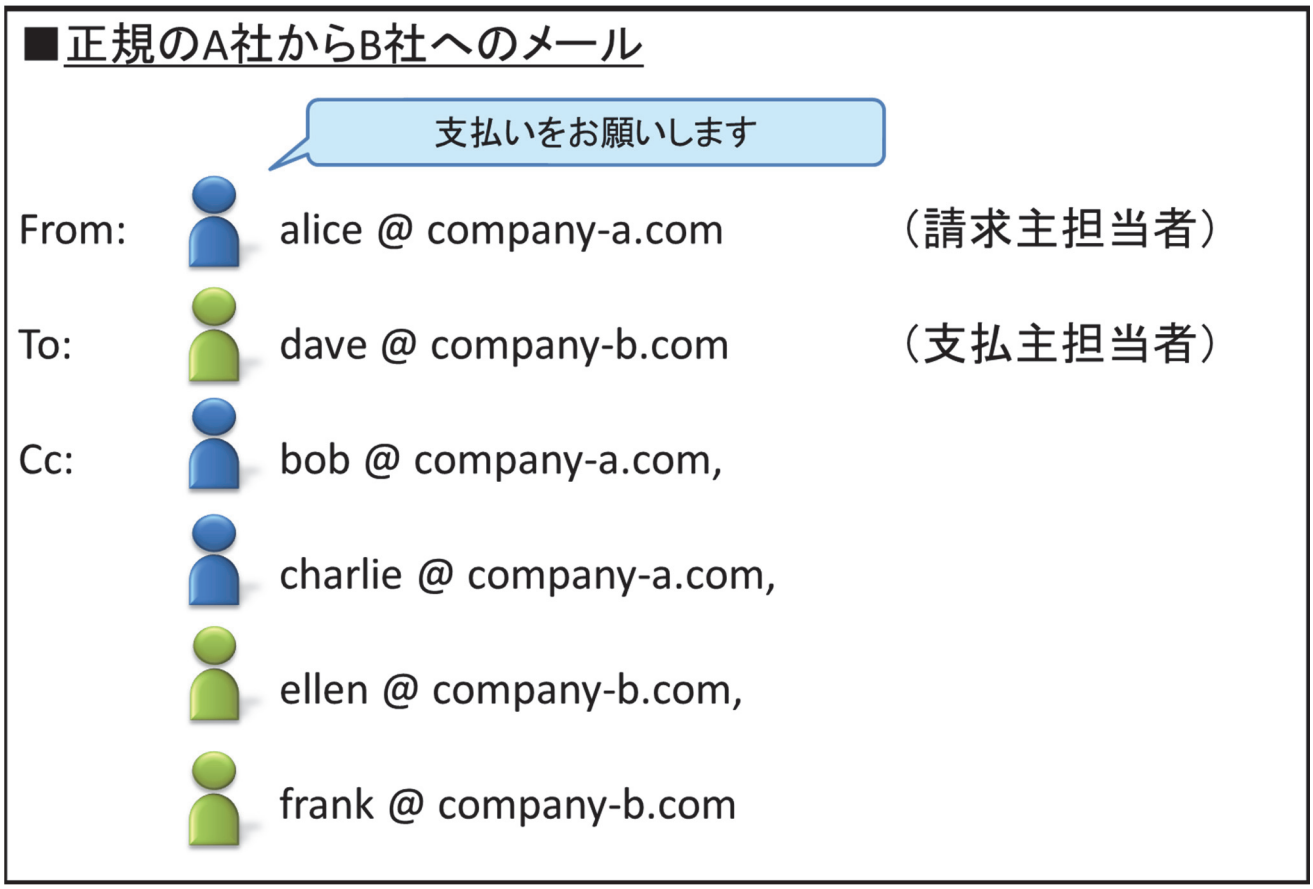

図 3-3 正規のメール例

これが、攻撃者が送ってきた偽のメールでは、次のように同報メールアドレスを部分的に改変することにより、**取引の多数の関係者に対して同報されているメールのように錯覚させつつ、実際には騙す相手だけにメールが届く**ように細工されていました。

ケース①：Cc にある A 社関係者の同報メールアドレスのみ偽のメールアドレスへ改変
ケース②：Cc にある全員分の同報メールアドレスを偽のメールアドレスへ改変

次の図は、攻撃者が A 社の「alice」になりすまし、B 社の「dave」へ偽のメールを送った際に、A 社関係者の同報メールアドレスを偽のメールアドレスに改変（ケース①）した場合の例です。

図 3-4 攻撃者による同報メールアドレスの改変の例

このメールでは、B 社に対し、次のような**錯覚**を与えます。

- A 社の alice から届いたメールである
- A 社の他の担当者も Cc で同報されている

しかし、実際には次のような状況です。

- A 社の alice から届いたメールのように見える**が、偽物からのメールである**
- A 社の他の担当者も Cc で同報されているように見える**が、実際には一人も届いていない**
- すなわち、このメールは **B 社（騙す相手）の担当者にのみ届いている**（A 社は詐欺に気付けない）

なお、ケース②では、**更に、Cc にある B 社の同僚（ellen、frank）のメールアドレスも改変されていました**。見た目上は、取引先 A 社と、自社 B 社の同僚と、多数の関係者が並んでいる、いわば衆人環視の中でのメールのような体裁となっていましたが、**実際にメールを受信しているのは B 社の dave（騙す相手）一人のみ**、となっていた状況でした。

3.3 攻撃に利用するドメインの手口

攻撃者は、なりすましを行う上で、正規のドメインに似通った、偽の「**詐称用ドメイン**」を取得して攻撃をしてくることがあります。攻撃メールにフリーメールサービスなどが使われた場合は、偽物であることが見破られやすいと思われます。一方、詐称用ドメインが使われた場合、メールの受信者が、送信元メールアドレスのドメイン名部分の異常に気付かない限り、攻撃者はそのままメールをやりとりして、詐欺を行うことができます。

本書の事例では、攻撃者がなりすましを行う企業のものとよく似た「詐称用ドメイン」を新たに取得し、DNS サーバやメールサーバの設定を行っていたものがありました。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[22]も「Pass」する状態でした。

このような攻撃を受けた場合、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。

参考として、次の図に、攻撃者によって詐称用ドメインが取得され、DNS サーバに SPF レコードが設定されている場合における、なりすましメールの配送の流れを示します。

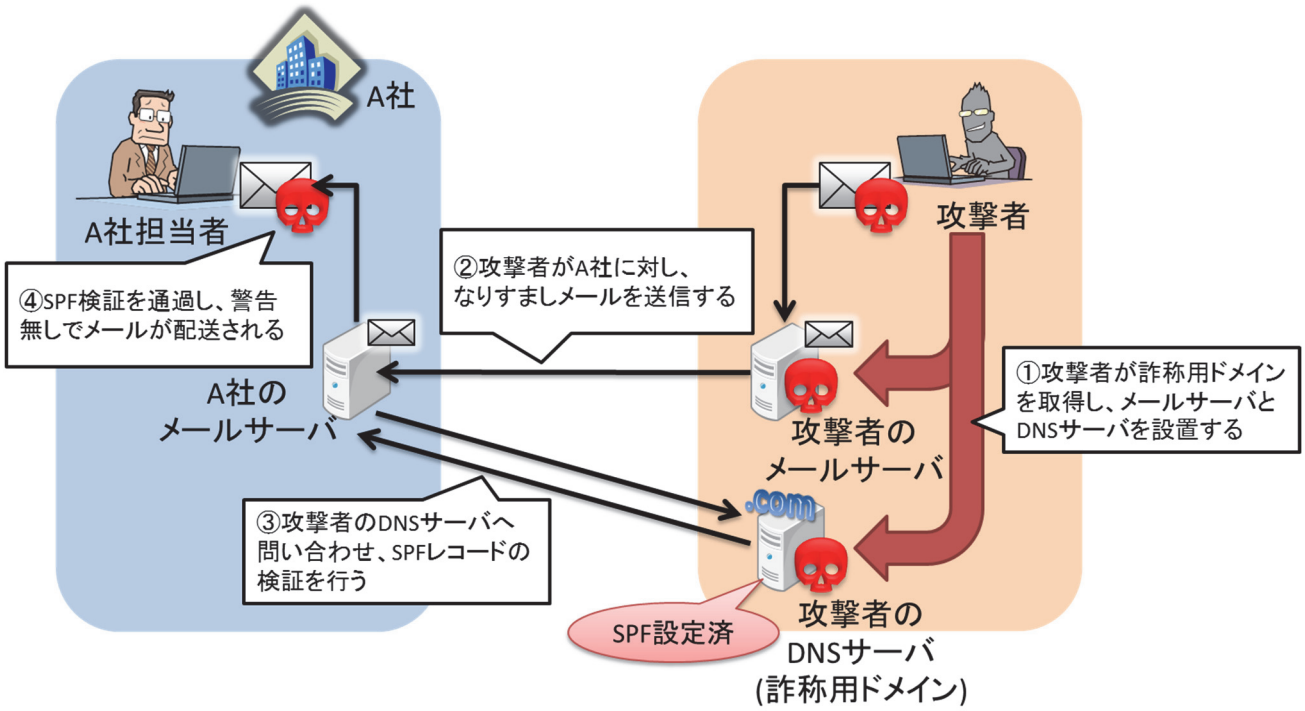

図 3-5 SPF レコード設定済みの詐称用ドメインによるなりすましメールの配送

[22] 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

4　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。

◆　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。

◆　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。

◆　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、「メールアカウントには複雑なパスワードを設定する」、「社外からアクセス可能なメールサーバがある場合、不審なログインなどのアクセスを監視する」といった、不正アクセスへの対策も重要です。

◆ 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。

このほか、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[23]。

- 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[24]にある「Best Practices for Victim Response and Reporting of Cyber Incidents」に掲載されています。

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

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

5　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、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、注意喚起とすることとしました。

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