ビジネスメール詐欺（BEC）の詳細事例2

～銀行口座証明書類を偽造し
振込先口座変更を依頼してきた事例～

2022 年 10 月 27 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、2021 年 3 月に国内の輸入販売業の企業（A 社：支払側）と、中国の企業（B 社：請求側、A 社の輸入先）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、送金先の銀行口座の変更を依頼するメールが送られたものです。

A 社は過去に B 社以外の中国の企業と行った正規の取引でも、送金先の変更を依頼されたことがあり、取引の過程で送金先を変更することは今回が初めてではありませんでした。このため、A 社の担当者は、攻撃者からの偽のメールによる送金先の変更依頼を本物と認識し、最終的に偽の銀行口座に送金してしまいました。

詐欺に気づいたのは、送金後に攻撃者から送られてきた、「送金されたお金が、口座の問題で振り込まれなかった」という内容のメールがきっかけでした。A 社の輸入責任者はこのメールを不審に思い、B 社の社長に直接電話し、メールの内容について確認したところ、B 社社長から、送金先の変更は指示していないという回答が返ってきたため、A 社輸入責任者は詐欺にあったことに気づきました。

詐欺発覚後、A 社輸入責任者は銀行に組戻し（資金返却）依頼を行ったものの、IPA が A 社から改めて状況説明を受けた 2021 年 7 月時点では、現地の銀行からの連絡はなく、資金の回収には至っていないとのことでした。

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

2021 年 4 月 2 日、送金に利用していた国内銀行の紹介により、A 社から IPA に対し、本件に関して今後の対策や注意すべき点について相談がありました。今回なりすまされた B 社は、A 社以外の国内企業とも取引があることもあり、A 社から他の企業に対するビジネスメール詐欺の被害防止に役立ててほしいとのことから、攻撃者とのやりとりのメール一式が IPA に情報提供されました。

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	国内の輸入販売業の企業。支払側。
A 社担当者	A 社の担当者。B 社担当者になりすました攻撃者とメールでやりとりを行った。
A 社輸入責任者	A 社担当者と共に、B 社の取引に係わっていた。攻撃者から送られてきたメールの内容に不審に思い、B 社への電話での確認や、国内銀行への送金の組戻り（資金返却）の対応を行った。当初はメールの同報先に含まれていたのみであったが、最終的に攻撃者から直接メールを受け取った。
B 社	中国の企業。請求側。A 社の輸入先。
B 社担当者	B 社の担当者。A 社担当者と取引に係るやりとりを行っていた。
B 社社長	B 社の社長。A 社輸入責任者から電話を行い、本件が詐欺である（本物の B 社からのメールではない）ことを確認した。
攻撃者	B 社の担当者になりすまし、ビジネスメール詐欺によって A 社から金銭を詐取した。

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。

- 攻撃者の介入から偽の銀行口座に送金するまでのやりとり
- 送金後の攻撃者とのやりとりと詐欺発覚後の対応

2. 攻撃者の介入から偽の銀行口座に送金するまでのやりとり

2021 年 3 月、A 社と B 社で取引に関するメールをやりとりする中で、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 社担当者らへ送られてきました。A 社担当者らは、偽のメールであると気づかず攻撃者とやりとりを行い、偽の口座への送金を行ってしまいました。

攻撃者の介入から偽の銀行口座に送金するまでのやりとりの概要（図 1、図 2）について、次に示します。（図中の赤い丸に白抜きで示した数字は、以降「攻撃者からのメール〇通目」という番号に対応しています）

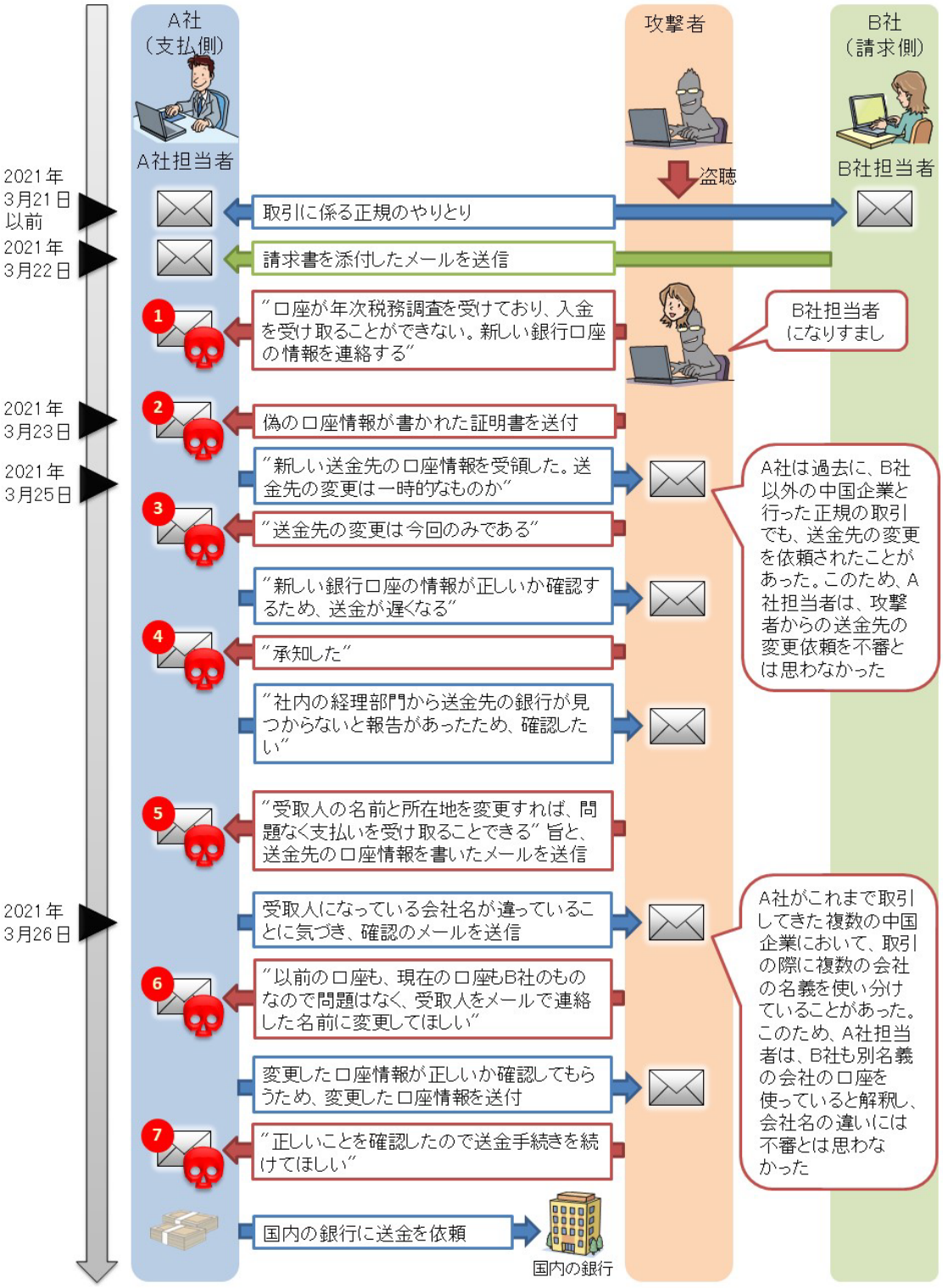


図 1 攻撃者の介入から偽の銀行口座に送金するまでのやりとり(1)

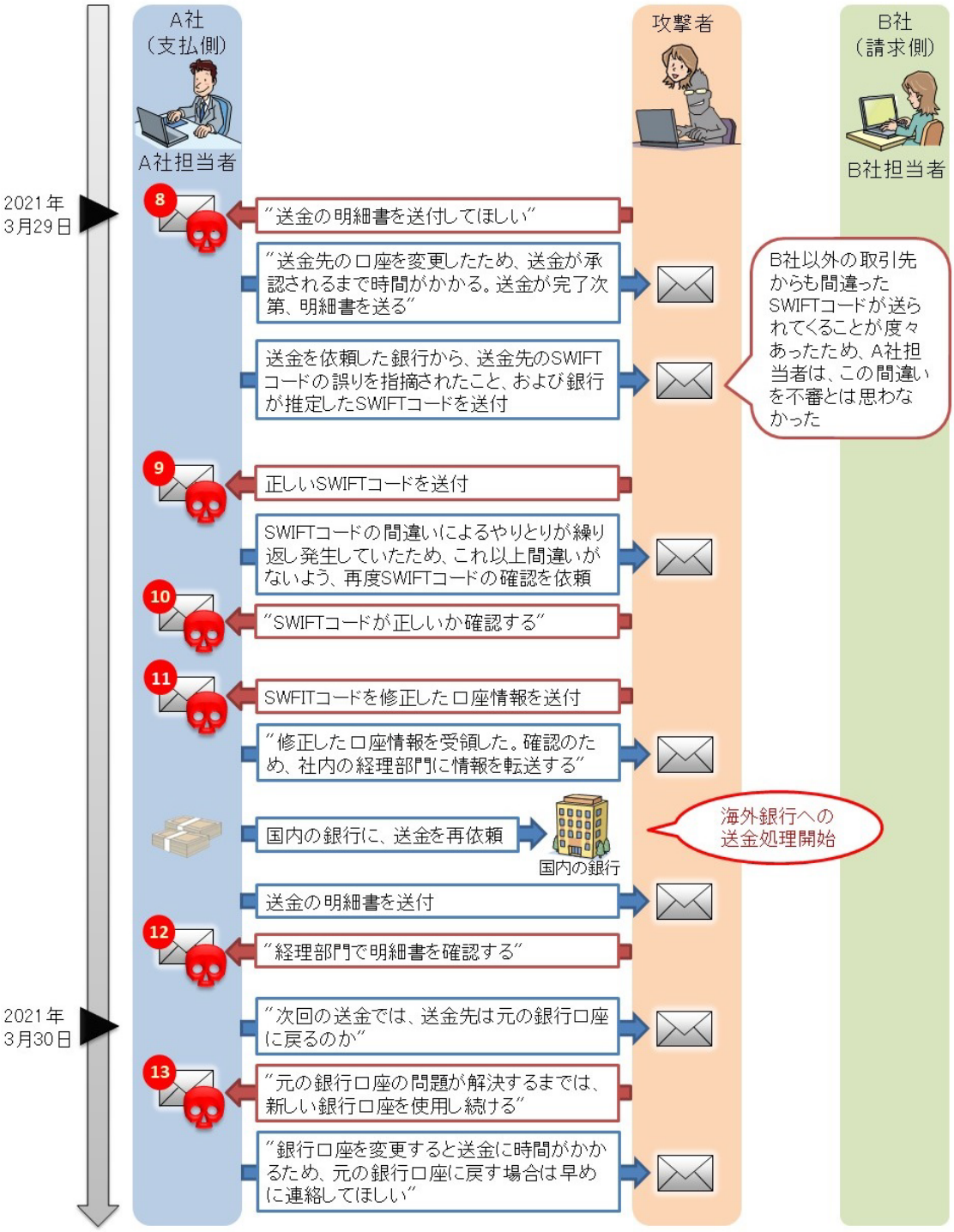
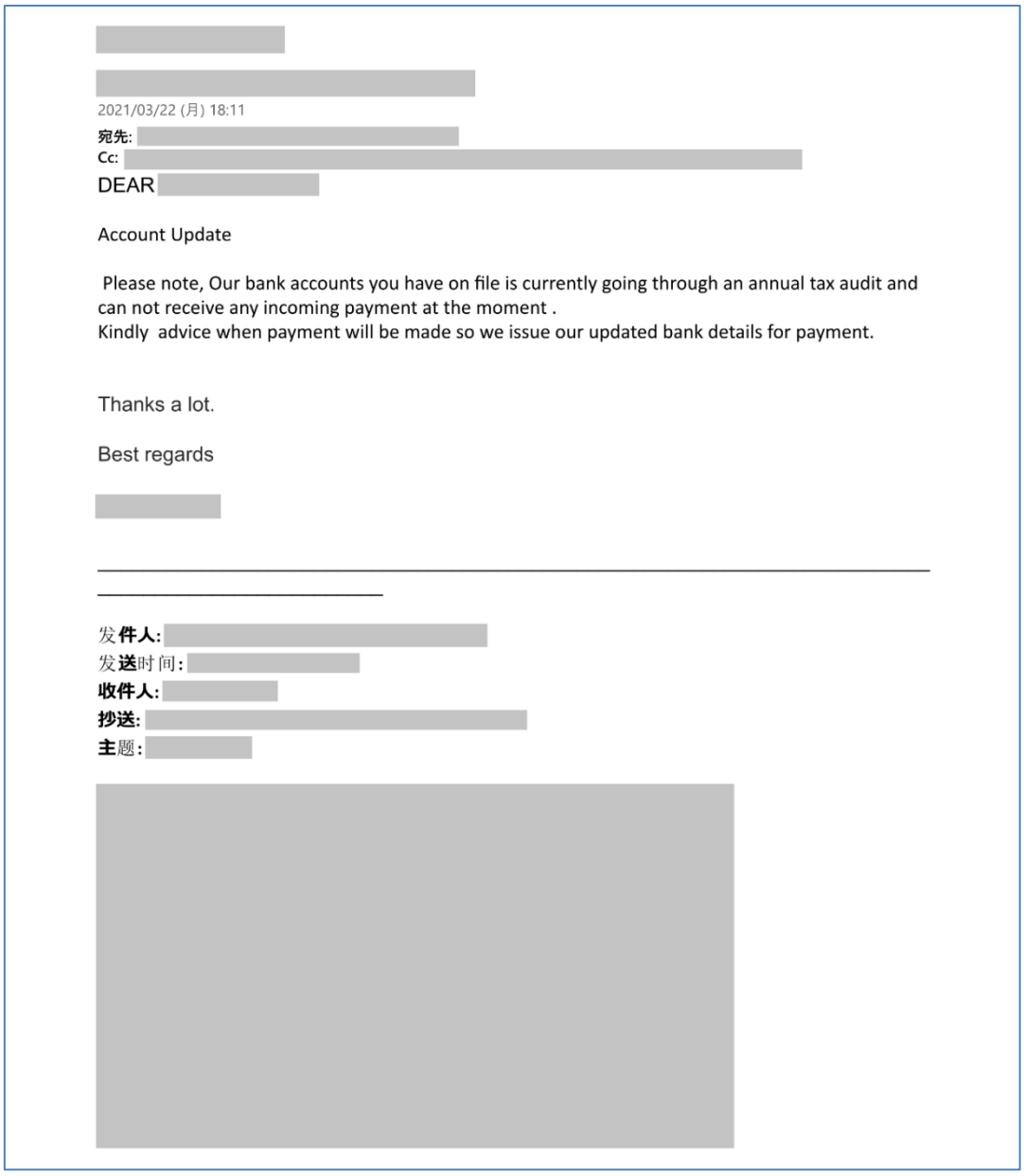


図 2 攻撃者の介入から偽の銀行口座に送金するまでのやりとり(2)

2021 年 3 月 21 日以前から、A 社と B 社では取引に係るメールのやりとりを行っていました。3 月 22 日、本物の B 社担当者が A 社担当者に対し、この取引の請求書をメールで送付したところ、その約 1 時間後、B 社の担当者になりすました攻撃者から A 社担当者に対し、「銀行口座が使用できなくなったため、新しい銀行口座の情報を連絡する」という内容のメール（図 3）が送られてきました。

このメールには、口座変更の理由として、口座が年次税務調査中で入金を受け取ることができないと書かれていました。このメールを発端として、A 社担当者と攻撃者の間で複数回のメールのやりとりが行われ、最終的に偽の口座への送金に至っています。



2021/03/22 (月) 18:11

宛先:

Cc:

DEAR

Account Update

Please note, Our bank accounts you have on file is currently going through an annual tax audit and can not receive any incoming payment at the moment .
Kindly advice when payment will be made so we issue our updated bank details for payment.

Thanks a lot.

Best regards

发件人:
发送时间:
收件人:
抄送:
主题:

図 3 攻撃者からのメール 1 通目（2021 年 3 月 22 日 18:11）

翌日（3 月 23 日）、攻撃者から A 社担当者に対して、偽の口座への送金を依頼するメールが送られてきました（図 4）。このメールには、口座情報の偽の証明書類（銀行名や SWIFT コード等が書かれた書類をスキャンしたもの）が添付されていました。

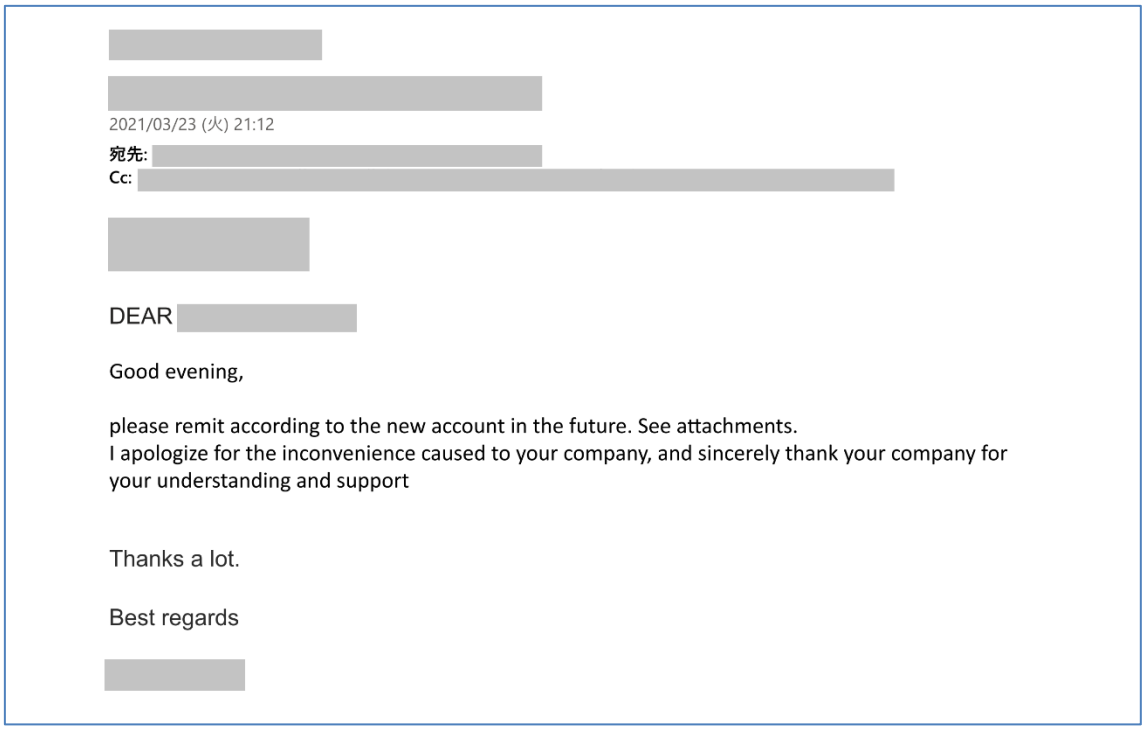


図 4 攻撃者からのメール 2 通目（2021 年 3 月 23 日 21:12）

A 社は過去に、B 社以外の中国の企業と行った正規の取引において、送金先の変更を依頼されたことがあり、取引の過程で送金先を変更することは今回が初めてではありませんでした。このため、A 社担当者は、攻撃者からの送金先の変更依頼を本物と判断した上で、「新しい送金先の口座情報を受領した。送金先の変更は一時的なものか」と返信しました。

この質問に対し、攻撃者から、送金についての連絡へのお礼とともに、質問への回答として、口座の変更は今回のみである旨のメールが送られてきました（図 5）。

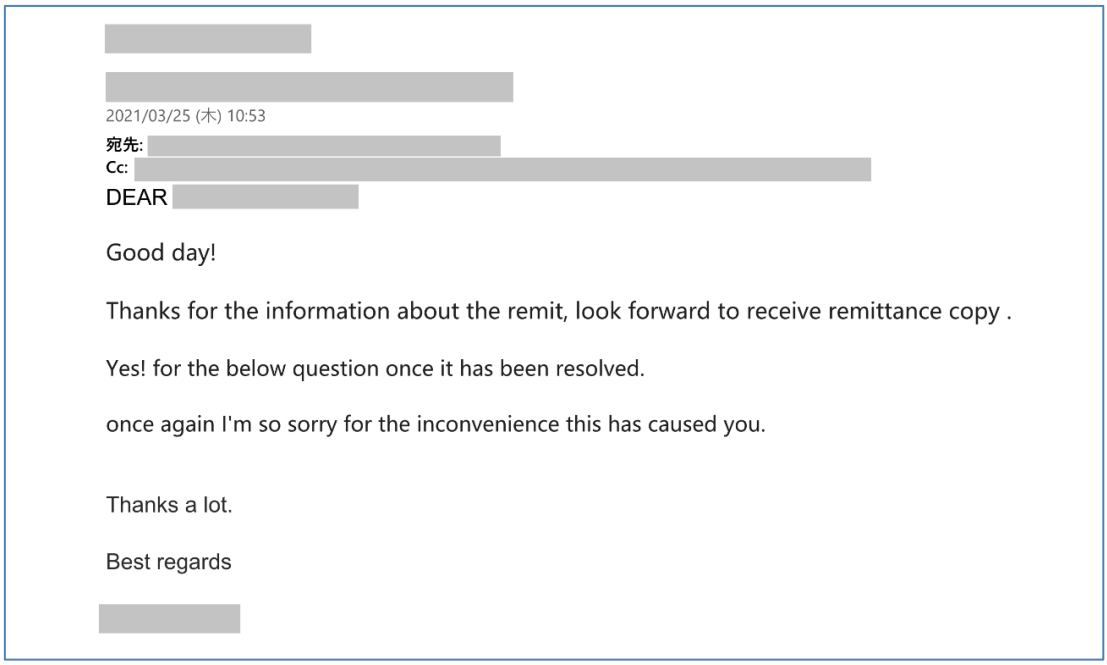


図 5 攻撃者からのメール 3 通目（2021 年 3 月 25 日 10:53）

その後、A 社担当者は、「新しい銀行口座の情報が正しいか確認するため、送金が遅くなる」という内容のメールを送信しました。

これに対し、攻撃者からは、承知したという内容のメールが送られてきました（図 6）。

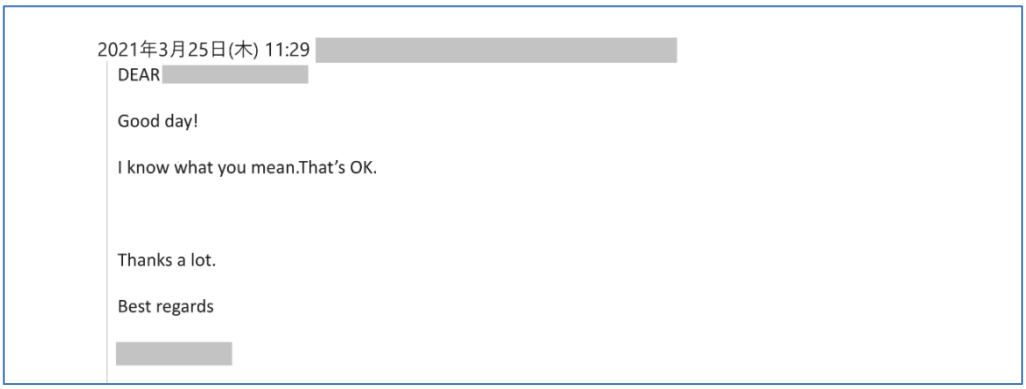
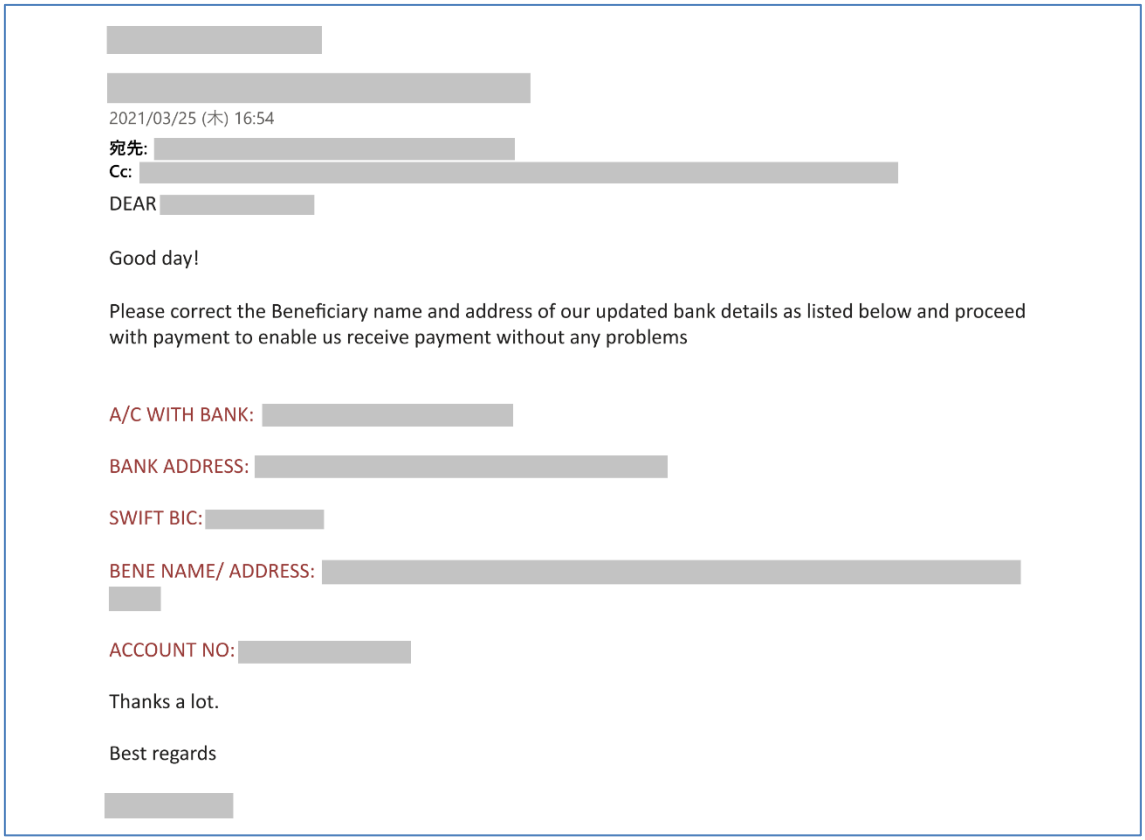


図 6 攻撃者からのメール 4 通目（2021 年 3 月 25 日 11:29）

A 社担当者は、攻撃者から受け取った口座情報をもとに、社内で口座情報の変更手続きを進めました。ところが、経理部門から口座がある銀行が見つからないという報告があったため、その旨を伝えるメールを攻撃者に送信しました。

これに対し、攻撃者から、受取人の名前と所在地を修正すれば、問題なく支払いを受け取ることができるという旨と、受取人の所在地が追加された口座情報が書かれたメールが送られてきました（図 7）。



[redacted]

[redacted]

2021/03/25 (木) 16:54

宛先: [redacted]

Cc: [redacted]

DEAR [redacted]

Good day!

Please correct the Beneficiary name and address of our updated bank details as listed below and proceed with payment to enable us receive payment without any problems

A/C WITH BANK: [redacted]

BANK ADDRESS: [redacted]

SWIFT BIC: [redacted]

BENE NAME/ ADDRESS: [redacted]

[redacted]

ACCOUNT NO: [redacted]

Thanks a lot.

Best regards

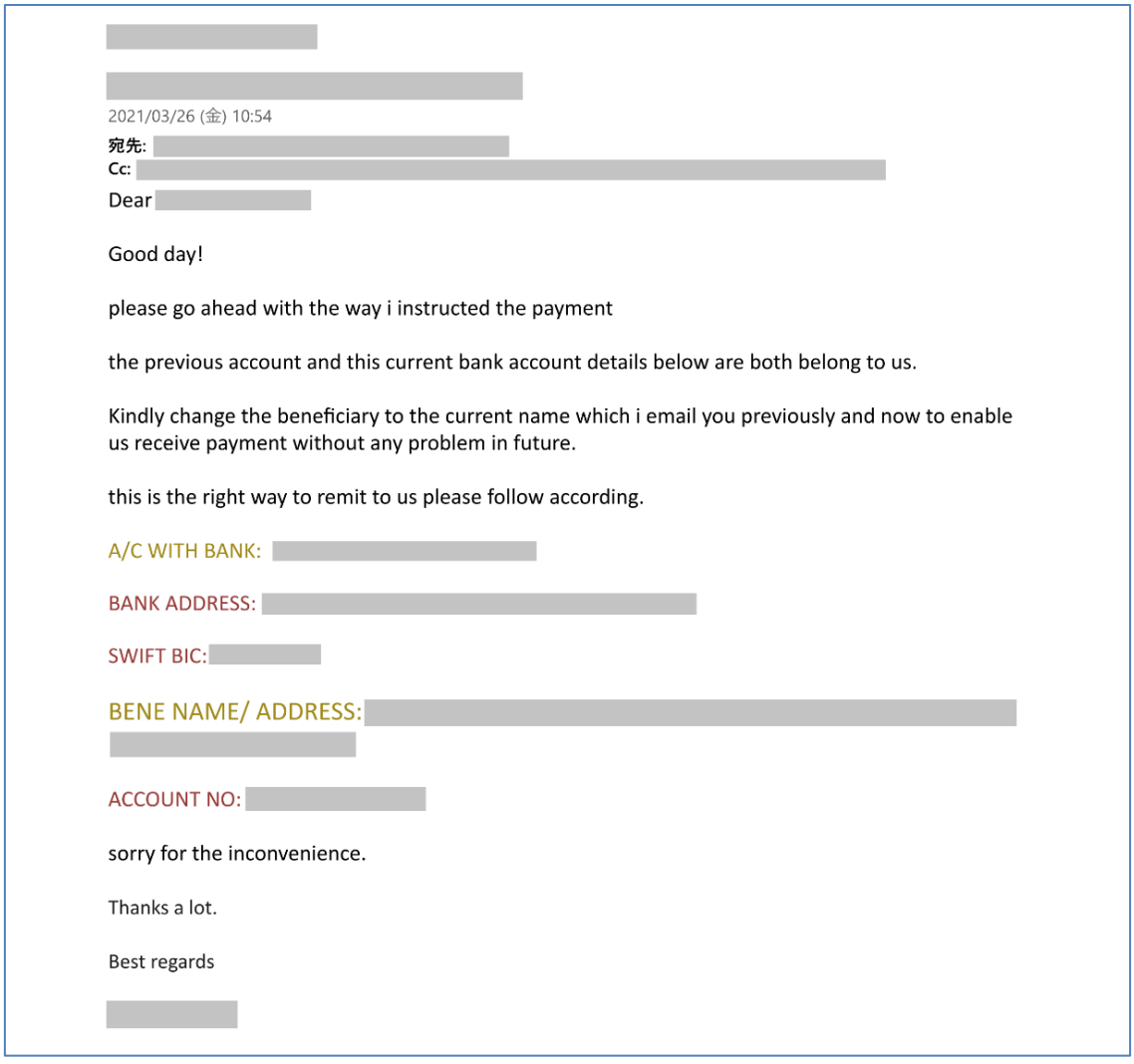
[redacted]

図 7 攻撃者からのメール 5 通目（2021 年 3 月 25 日 16:54）

翌日（3 月 26 日）、A 社は、受取人になっている会社名が B 社と異なっていることに気づき、攻撃者に確認のメールを送信しました。

これに対し、攻撃者から、以前の口座も現在の口座も B 社が保有しているものであるため問題はなく、指示した通り、受取人をメールで連絡した名前に変更してほしい、これが正しい方法である、という内容のメールが送られてきました（図 8）。

A 社がこれまで取引してきた複数の中国企業では、税金対策などの目的であるのか詳細な理由は不明ながらも、複数の会社の名義を所有していることが多かったため、A 社担当者は、B 社についても B 社自身が所有する別名義の会社の口座を使っているものと解釈し、口座の会社名の違いには不審に思いませんでした。



2021/03/26 (金) 10:54

宛先:

Cc:

Dear

Good day!

please go ahead with the way i instructed the payment

the previous account and this current bank account details below are both belong to us.

Kindly change the beneficiary to the current name which i email you previously and now to enable us receive payment without any problem in future.

this is the right way to remit to us please follow according.

A/C WITH BANK:

BANK ADDRESS:

SWIFT BIC:

BENE NAME/ ADDRESS:

ACCOUNT NO:

sorry for the inconvenience.

Thanks a lot.

Best regards

図 8 攻撃者からのメール 6 通目（2021 年 3 月 26 日 10:54）

A 社担当者は、変更した口座情報が正しいか確認してもらうため、変更後として設定する口座情報を改めて送付しました。

これに対し、攻撃者から、正しいことを確認したため送金手続きを続けてほしいという内容のメールが送られてきました（図 9）。

その後、A 社担当者は国内の銀行に送金依頼を行いました。

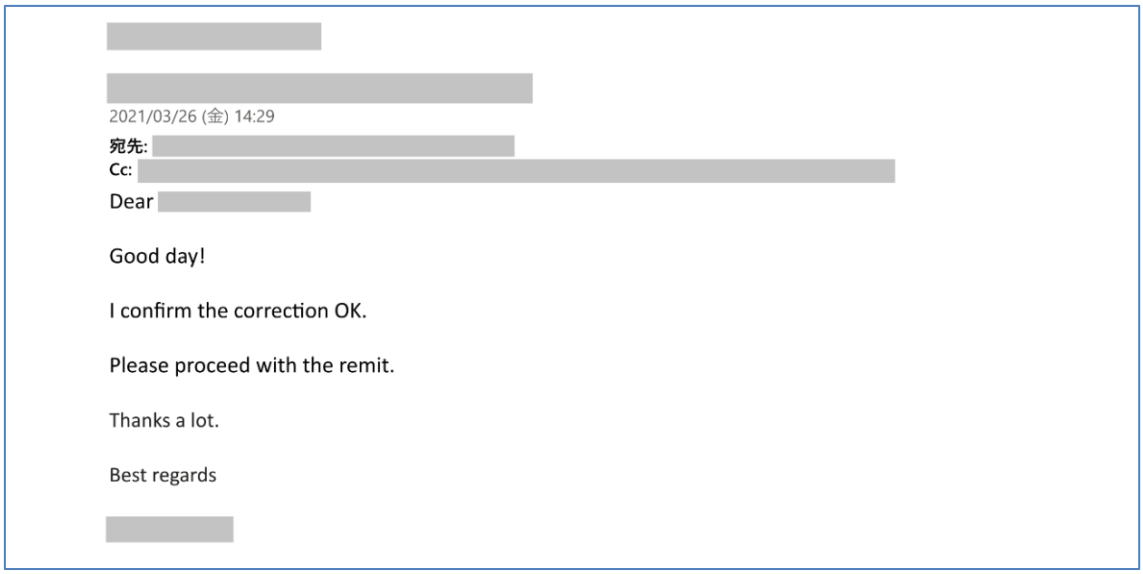


図 9 攻撃者からのメール 7 通目（2021 年 3 月 26 日 14:29）

3 月 29 日、攻撃者から A 社担当者に対して、送金の明細書を送ってほしいという内容のメールが送られてきました（図 10）。

これに対し A 社担当者は、「送金先の口座を変更したため、送金が承認されるまで時間がかかる。送金が完了次第、明細書を送る」と返信しました。

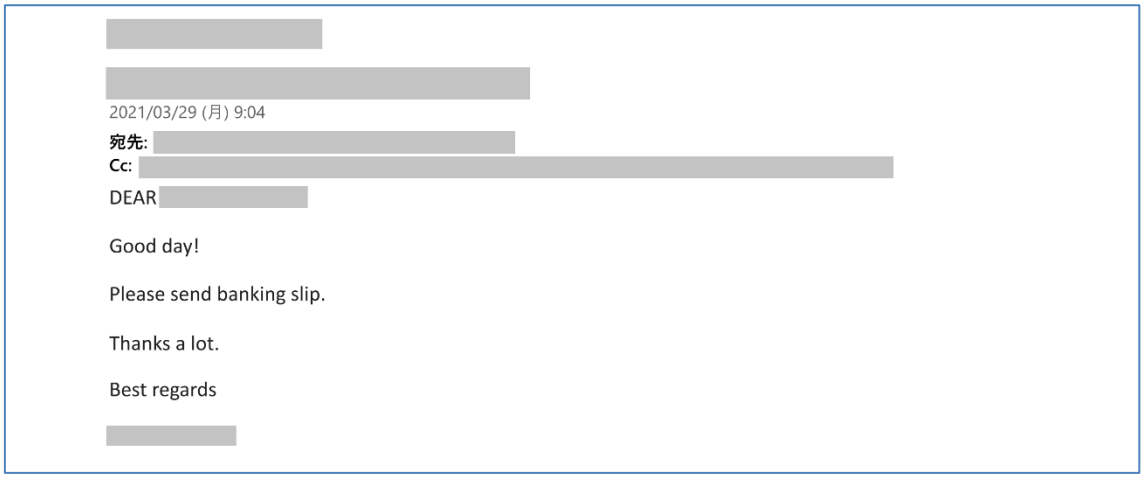


図 10 攻撃者からのメール 8 通目（2021 年 3 月 29 日 9:04）

その後、A 社担当者は、送金を依頼していた銀行から、送金先の SWIFT コードが間違っている（実在しない銀行の SWIFT コードであった）と指摘を受けたため、攻撃者に SWIFT コードを確認するメールを送信しました。A 社では B 社以外の中国の取引先からも、間違った SWIFT コードが送られてくることが度々あったため、この点についても A 社担当者は不審とは思いませんでした。

これに対し、攻撃者から、お詫びとともに「正しい SWIFT コード」を連絡するメールが送られてきました（図 11）。

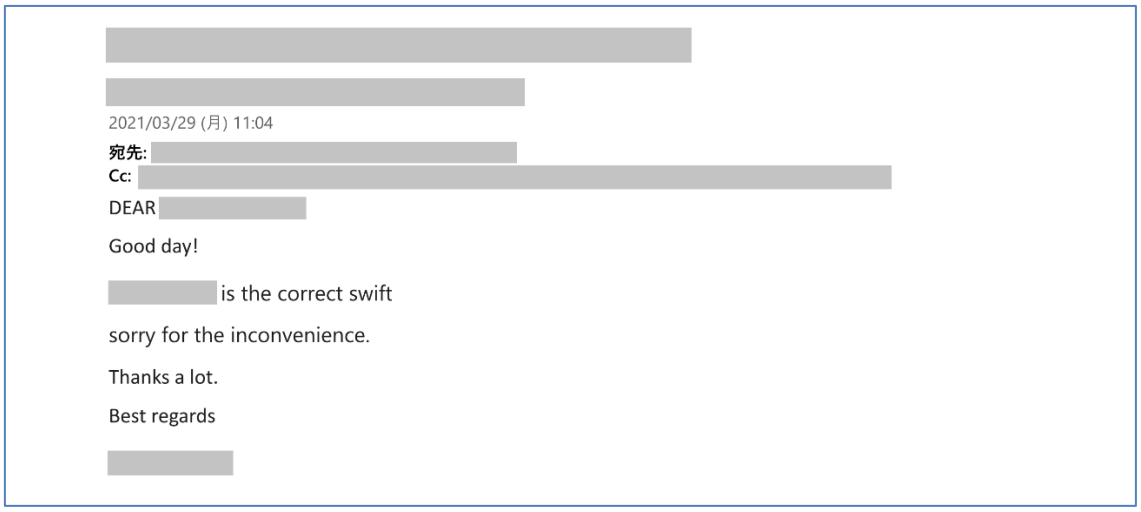


図 11 攻撃者からのメール 9 通目（2021 年 3 月 29 日 11:04）

A 社担当者は、これまでに SWIFT コードの間違いによるやりとりが繰り返し発生していたため、これ以上間違いがないよう、その SWIFT コードが本当に正しいか、明示的に再確認を依頼するメールを送信しました。

これに対し、攻撃者から、確認するという内容のメールが送られてきました（図 12）。

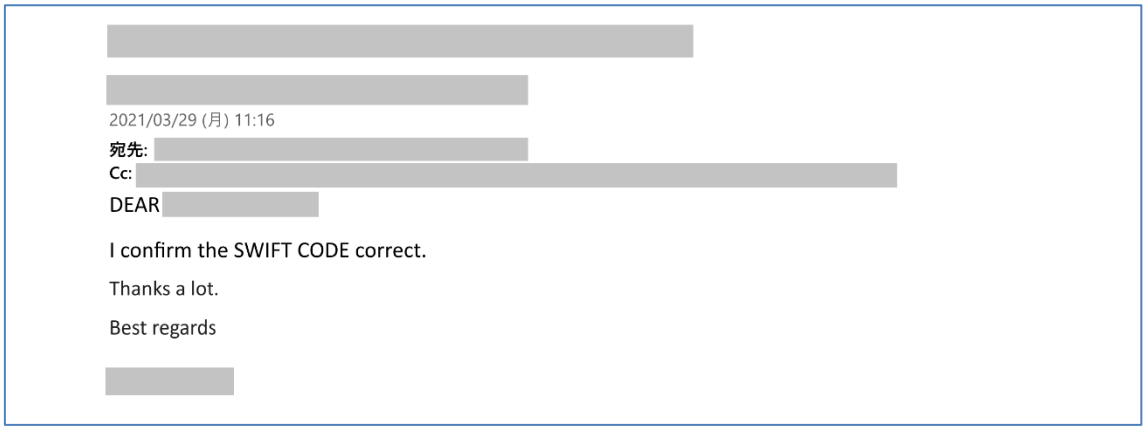
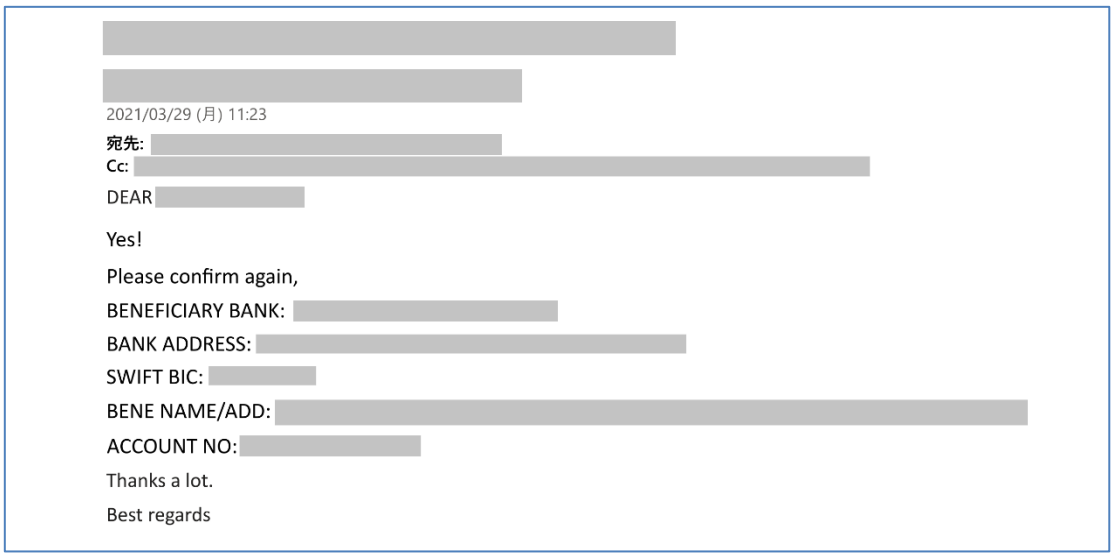


図 12 攻撃者からのメール 10 通目（2021 年 3 月 29 日 11:16）

その後すぐ、攻撃者から、先に「正しい SWIFT コード」として提示された SWIFT コードを含む口座情報全体がメールで送られてきました。（図 13）。


[redacted]

2021/03/29 (月) 11:23

宛先: [redacted]

Cc: [redacted]

DEAR [redacted]

Yes!

Please confirm again,

BENEFICIARY BANK: [redacted]

BANK ADDRESS: [redacted]

SWIFT BIC: [redacted]

BENE NAME/ADD: [redacted]

ACCOUNT NO: [redacted]

Thanks a lot.

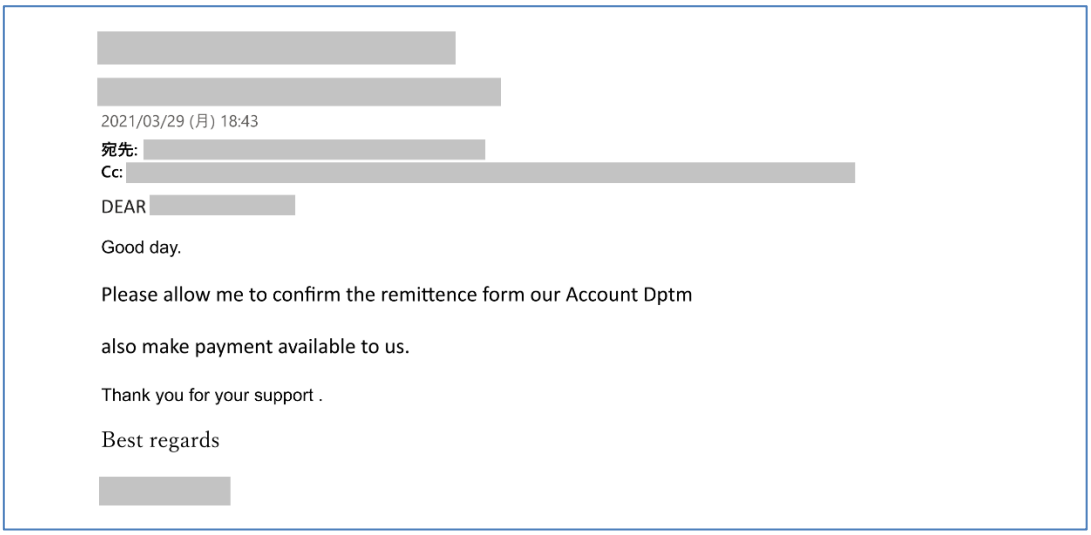
Best regards

図 13 攻撃者からのメール 11 通目（2021 年 3 月 29 日 11:23）

A 社担当者は攻撃者に対し、「修正した口座情報を受領した。確認のため、社内の経理部に情報を転送する」という内容のメールを返信しました。

その後、A 社担当者は、国内の銀行に送金の再依頼を行いました。今度は送金依頼が銀行で受理されたため、当該送金の明細書を攻撃者に送信しました。

これに対し、攻撃者からは、経理部門で明細書を確認するという内容のメールが送られてきました（図 14）。


[redacted]

2021/03/29 (月) 18:43

宛先: [redacted]

Cc: [redacted]

DEAR [redacted]

Good day.

Please allow me to confirm the remittence form our Account Dptm

also make payment available to us.

Thank you for your support .

Best regards

[redacted]

図 14 攻撃者からのメール 12 通目（2021 年 3 月 29 日 18:43）

翌日（3 月 30 日）、A 社担当者は攻撃者に対し、「次回の送金では、送金先は元の銀行口座に戻るのか」と質問するメールを送信しました。

これに対し、攻撃者から、元の銀行口座の問題が解決するまでは、新しい銀行口座を使用し続けるという内容のメールが送られてきました（図 15）。

図 15 攻撃者からのメール 13 通目（2021 年 3 月 30 日 8:50）

A 社担当者はこのメールに対し、「銀行口座を変更すると送金に時間がかかるため、元の銀行口座に戻す場合は早めに連絡してほしい」と返信しました。

3. 送金後の攻撃者とのやりとりと詐欺発覚後の対応

送金後の攻撃者とのやりとりと、詐欺発覚後の対応の概要（図 16）について、次に示します。

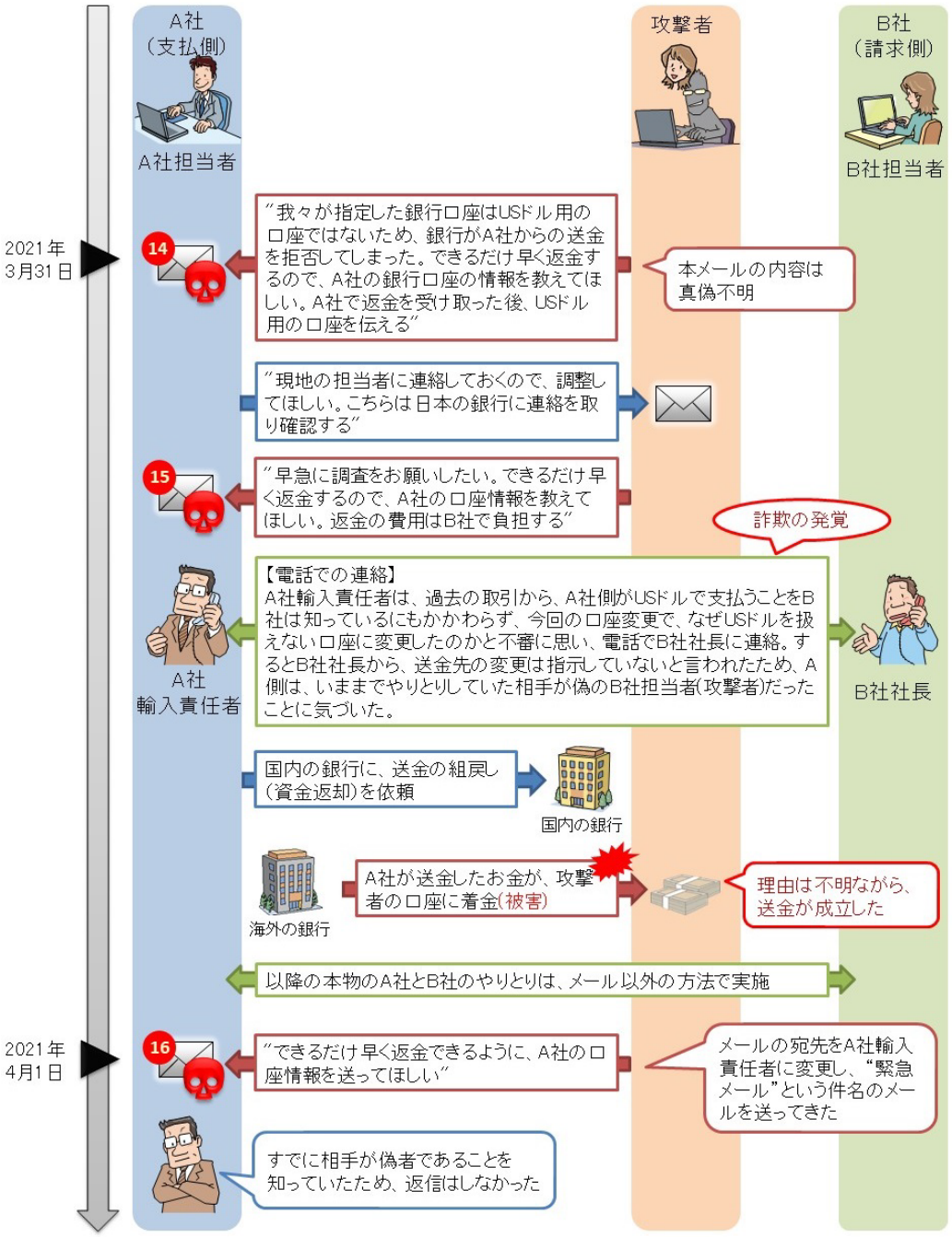
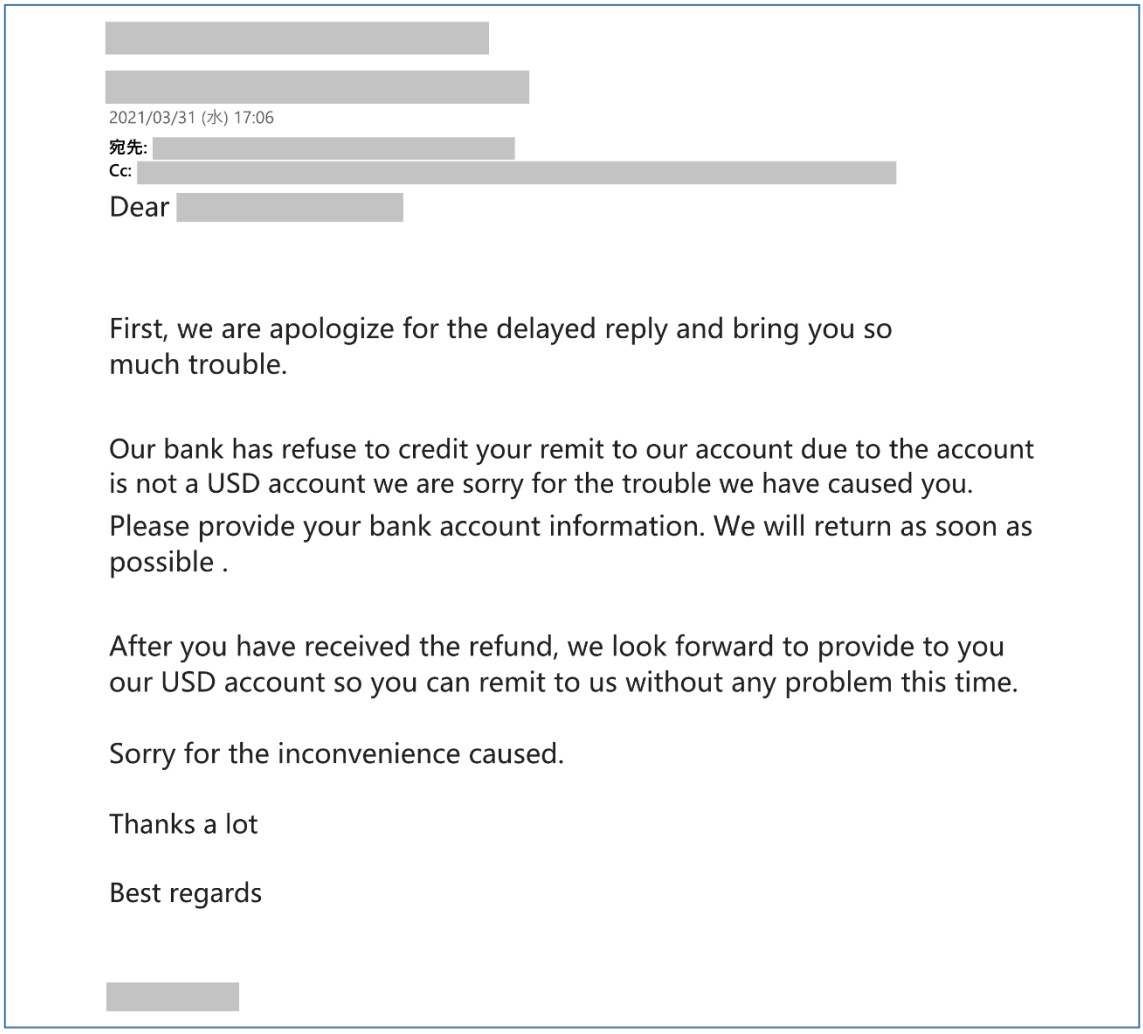


図 16 送金後の攻撃者とのやりとりと詐欺発覚後の対応

3 月 31 日、攻撃者から A 社担当者に対し、「我々が指定した銀行口座は US ドル用の口座ではないため、銀行が A 社からの送金を拒否してしまった」という内容のメールが送られてきました（図 17）。また、このメールには、返金を行い、US ドル用の口座を別途伝えるため、A 社の銀行口座の情報を教えてほしいとも書かれていました。

このメールの内容について、攻撃者が本当にミスをして、口座が USドルを受け取れない状態となっていたのか、別の理由があり嘘をついていたのかは不明です。例えば、出金するまでの時間稼ぎや、一旦返金すると言いながら、二重に金銭を騙し取ろうとした可能性も考えられます。



2021/03/31 (水) 17:06

宛先:

Cc:

Dear

First, we are apologize for the delayed reply and bring you so much trouble.

Our bank has refuse to credit your remit to our account due to the account is not a USD account we are sorry for the trouble we have caused you.
Please provide your bank account information. We will return as soon as possible .

After you have received the refund, we look forward to provide to you our USD account so you can remit to us without any problem this time.

Sorry for the inconvenience caused.

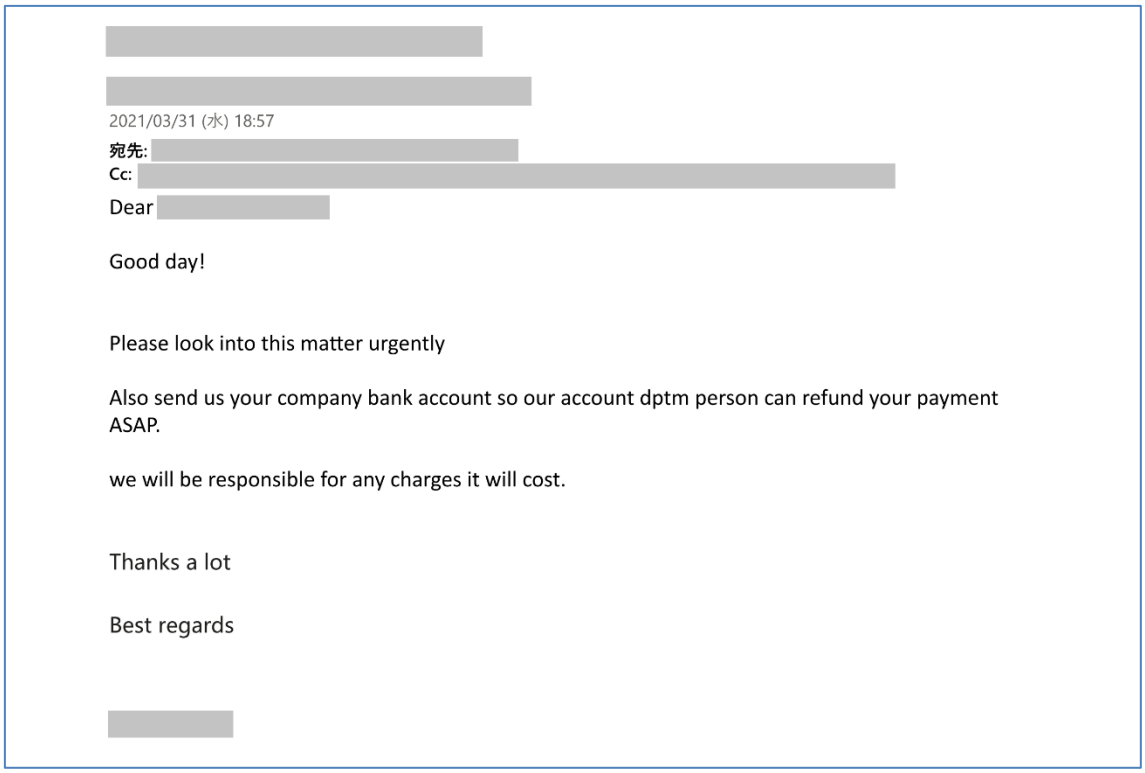
Thanks a lot

Best regards

図 17 攻撃者からのメール 14 通目（2021 年 3 月 31 日 17:06）

これに対し A 社担当者は、「現地の担当者に連絡しておくので、調整してほしい。こちらは日本の銀行に連絡を取り、確認する」と返信しました。

すると攻撃者から、早急に A 社側での調査を願う旨と、できるだけ早く返金するため、A 社の口座情報を教えてほしいという内容のメールが送られてきました。このとき、攻撃者のメールには返金の費用負担について、B 社で負担するとも書かれていました（図 18）。



2021/03/31 (水) 18:57

宛先:

Cc:

Dear

Good day!

Please look into this matter urgently

Also send us your company bank account so our account dptm person can refund your payment ASAP.

we will be responsible for any charges it will cost.

Thanks a lot

Best regards

図 18 攻撃者からのメール 15 通目（2021 年 3 月 31 日 18:57）

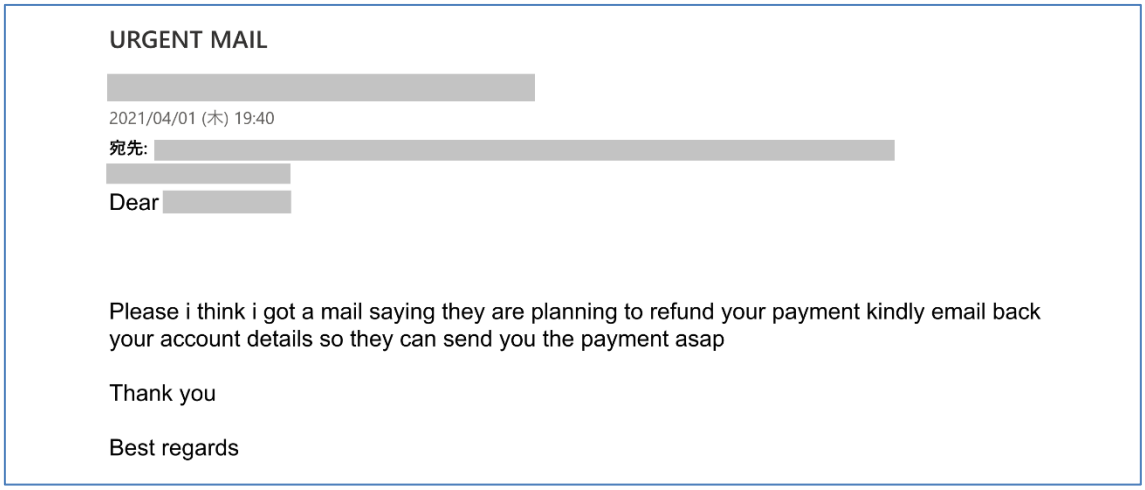
このタイミングで A 社の輸入責任者は、過去の取引から、A 社側が US ドルで支払うことを B 社は知っているにもかかわらず、今回の口座変更で、なぜ US ドルを扱えない口座に変更したのかと不審に思い、電話で B 社の社長に連絡しました。すると B 社社長から、送金先の変更は指示していないという回答が返ってきたため、A 社輸入責任者は、いままでやりとりしていた相手が偽者であり、詐欺に遭ったことに気づきました。

A 社輸入責任者はすぐに、送金を依頼した国内の銀行に対し、送金の組戻し（資金返却）を依頼しました。また、この詐欺が発覚した時点以降、B 社とはメール以外の方法を使用して連絡を行うこととしました。

なお、その後の調査で、具体的な時間帯は不明ながら、3 月 31 日中には、送金したお金が攻撃者の口座に着金していたことが分かっています。攻撃者からのメールには、攻撃者側の銀行が送金を拒否したと書かれていましたが、嘘であったのか、あるいはそれが本当であったとした場合、なぜ一度拒否されたはずの送金が成立したのかについては不明です。

翌日（4 月 1 日）、攻撃者はメールの宛先を A 社輸入責任者に変え、「緊急のメール」という件名のメールを送ってきました。このメールには、できるだけ早く返金できるように、A 社の口座情報を送ってほしいという内容が書かれていました（図 19）。A 社輸入責任者は、すでに相手が偽者であることを知っていたため、返信はしませんでした。

攻撃者が、なぜこのタイミングで A 社の別の担当者へ連絡してきたのかについては不明です。詐欺が発覚しかけていることに感づいたのか、騙す相手を変えるなどして、引き伸ばしを試みたのかもしれません。


URGENT MAIL

[redacted]

2021/04/01 (木) 19:40

宛先: [redacted]

Dear [redacted]

Please i think i got a mail saying they are planning to refund your payment kindly email back your account details so they can send you the payment asap

Thank you

Best regards

図 19 攻撃者からのメール 16 通目（2021 年 4 月 1 日 19:40）

その後、A 社は国内の銀行に対して引き続き送金の組戻しを依頼しているものの、IPA が A 社から状況説明を受けた 2021 年 7 月時点において、数か月経っても送金先の銀行からは何の連絡もなく、資金の回収には至っていませんでした。

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。

- 税務調査や監査を理由とした送金先の変更
- 正規メールの悪用
- 正規メールアドレスの悪用
- 同報(Cc)メールアドレスの変更
- 銀行口座の証明書類の偽造

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ている攻撃手口です。

4.1. 税務調査や監査を理由とした送金先の変更

本事例では、攻撃者が A 社に対して送金先の変更を依頼する際、「口座が年次税務調査中で入金を受け取ることができない」という嘘の理由を示してきました。

攻撃者が別の口座への送金を依頼する際、自社の使用している銀行口座が税務調査や監査を受けているという嘘の理由を示してくるのは、これまで IPA が確認してきたビジネスメール詐欺の事例においても、多く確認されている手口です。

4.2. 正規メールの悪用

攻撃者が最初に送ってきたメール（図 20）は、本物のＢ社担当者がＡ社担当者に送った、請求書が添付された正規メールを引用したものでした。本物のメールへの返信のような形態とすることで、A 社側に偽のメールであることに気づかれないようにする意図があったものと考えられます。

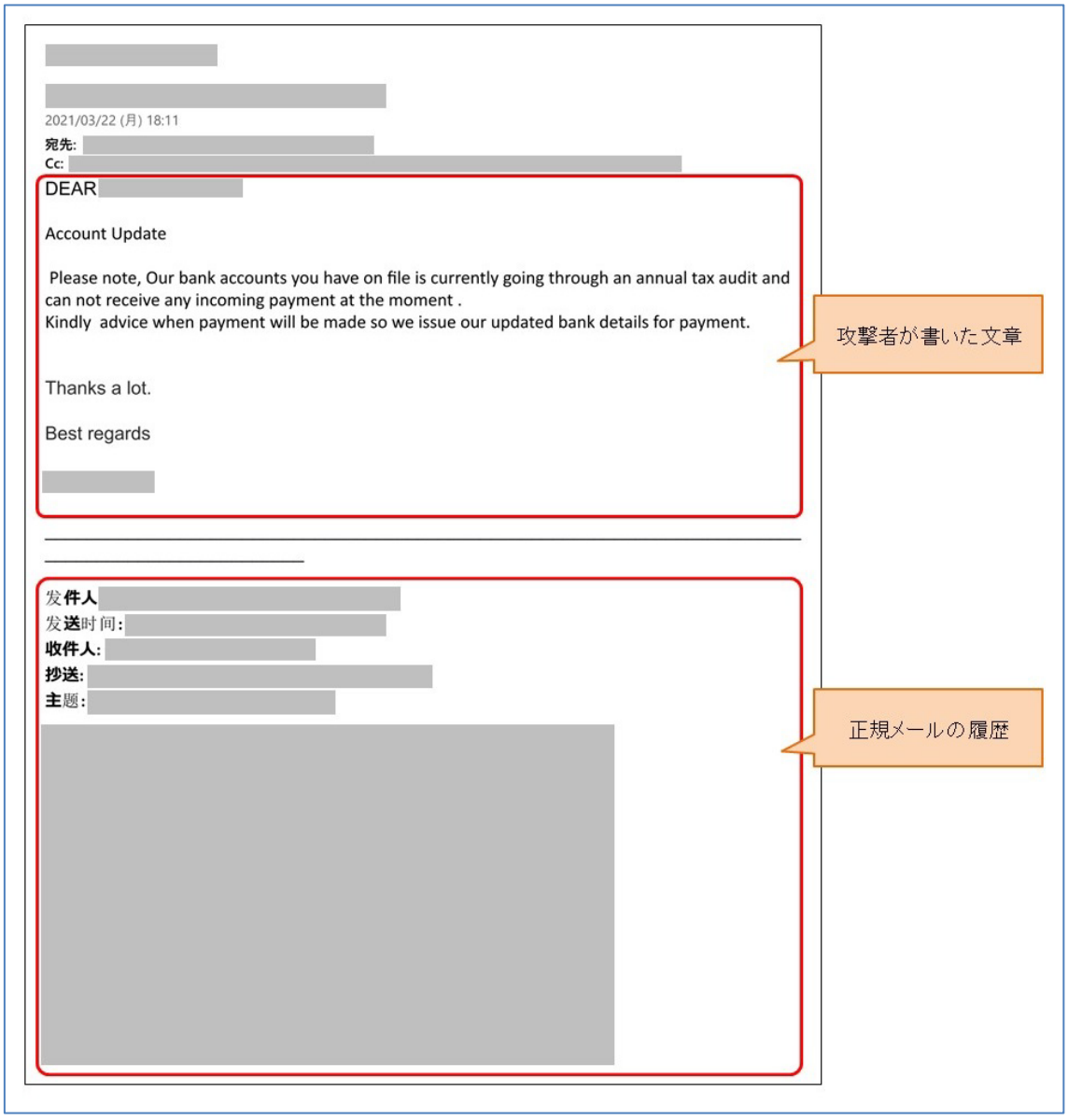


図 20 攻撃者が最初に送ってきたメール

4.3. 正規メールアドレスの悪用

攻撃者から送られてきたメールは、送信元（From）のメールアドレスに B 社担当者の正規のメールアドレスが使われていました。また、A 社担当者は詐欺が発覚するまでの間、B 社担当者の正規のメールアドレス宛にメールを送信していました。

一方、本物の B 社担当者は、この詐欺のやりとりを把握していませんでした。攻撃者は B 社担当者のメールアカウントに不正アクセスし、B 社担当者になりすましていたことに加えて、具体的な手口については不明ながら、例えばメールの振り分けルールや転送ルールを設定するなどして、A 社担当者とやりとりしているメールを本物の B 社担当者に見られないようにしていたものと思われます。

4.4. 同報（Cc）メールアドレスの変更

攻撃者は、最初のメールを送信する際、同報先（Cc）の B 社関係者のメールアドレスをフリーメールサービスのものに変更していました。これは、A 社側には B 社関係者が同報先（Cc）に含まれているように見せかけつつ、本物の B 社の関係者には偽のメールを届かないようにすることで、詐欺が発覚しにくくする意図があったものと考えられます。

【本物のメールアドレス】alice @ ●●●.com
【偽物のメールアドレス】alice @ ▲▲▲.com （フリーメールアドレス）

※実際に悪用されたものとは異なる。

4.5. 銀行口座の証明書類の偽造

攻撃者から送られてきた 2 通目のメール（図 4）には、偽造された銀行口座の証明書類のスキャン画像（図 21）が添付されていました。詐欺発覚後、過去に B 社から受け取った正規の証明書類と、今回偽造された証明書類を比較したところ、押されていた印影の名義が、B 社の工場長から B 社の社長に変わっていたことが分かりました。しかしながら、これまでは印影の名義を確認してなかったことと、記載内容自体に不審な点はなかったため、受け取った時点では、偽造された証明書類であることには気づけなかったとのことです。

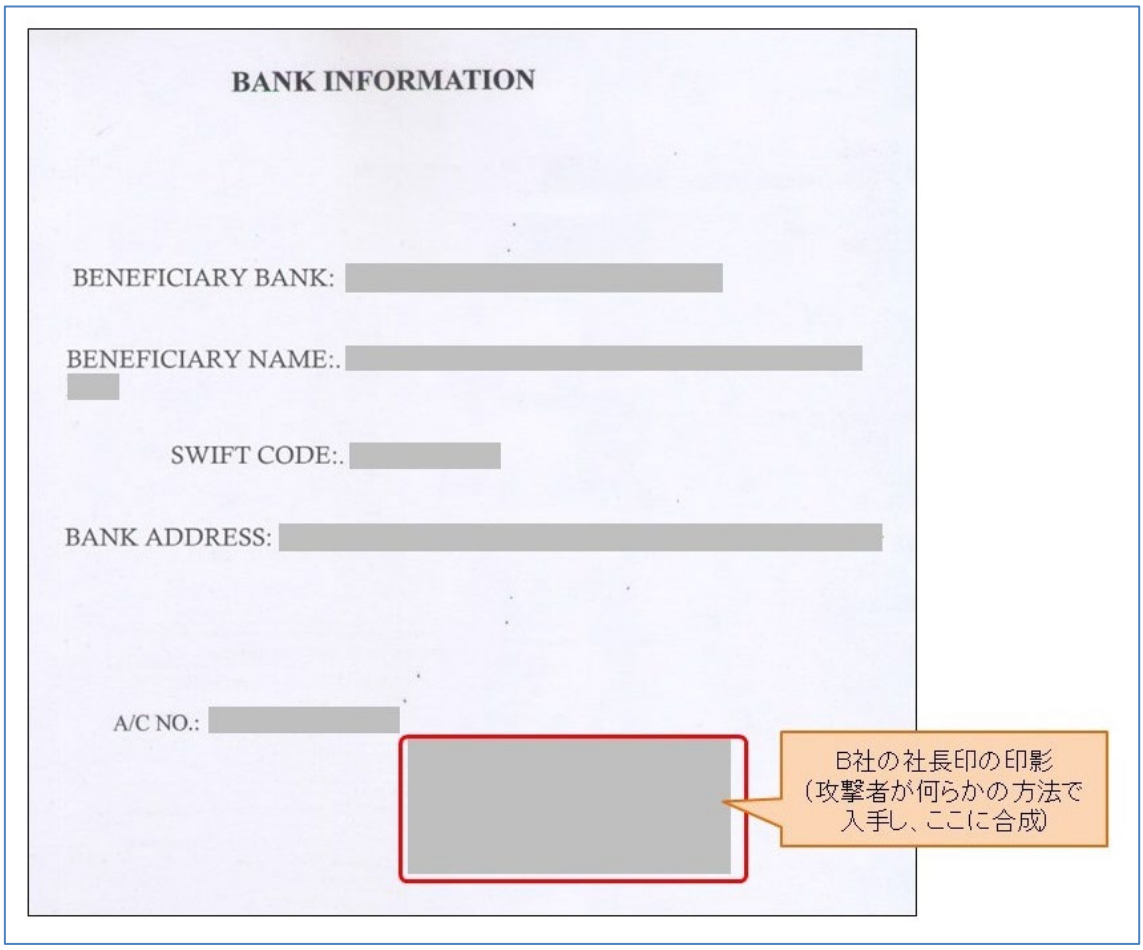


図 21 偽造された銀行口座の証明書類のスキャン画像

以上