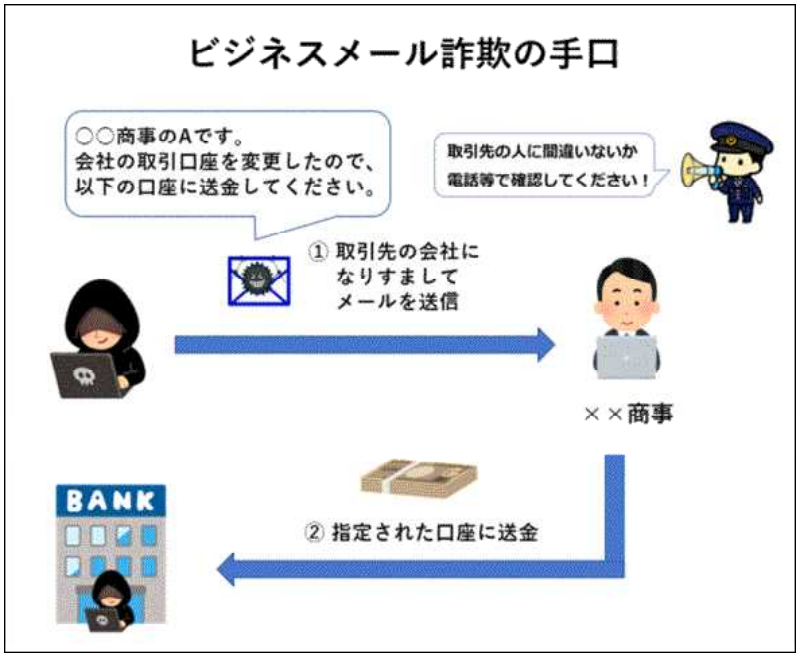
ビジネスメール詐欺対策

○　ビジネスメール詐欺とは

ビジネスメール詐欺とは、取引先や自社の経営者等になりすまして、偽の電子メールを送って入金を促す詐欺のことで、BEC（**Business Email Compromise**）とも呼ばれています。ビジネスメール詐欺は、世界中で大きな被害をもたらしており、我が国においても高額な被害が確認されています。

○　ビジネスメール詐欺の手口

ビジネスメール詐欺では、攻撃者が実際の取引先や自社の経営者層等になりすまし、メールを使って振込先口座の変更を指示するなどして、攻撃者が指定する銀行口座へお金を振り込ませようとします。これらのビジネスメール詐欺の多くは、海外の銀行口座を振込先として指定してきますが、一旦海外に送金してしまうと、回収することは非常に困難です。



※実際のメールの例は、下記レポートを参照してください。

- **独立行政法人情報処理推進機構**
  「ビジネスメール詐欺「BEC」に関する事例と注意喚起」（外部サイト）
  （https://www.ipa.go.jp/archive/files/000058478.pdf）

○　ビジネスメール詐欺の被害に遭ったら

(1) 原因調査等を行う

・　パソコンに対するウイルスチェックの実施及びメールアカウントのパスワードを変更する。
・　メールアカウントに対する不正アクセスの有無や外部へのメールの転送設定、普段見ないフォルダへの振り分け設定等がないか調査をする。
・　社員に対して、不審なメールを開いていないか、メールアカウントのパスワードは他のサービス等と使い回しをしていないか聴取する。

(2) 送金のキャンセル等の手続を行う

攻撃者から指定された銀行口座に送金してしまった場合は、速やかに送金元の銀行に送金のキャンセルや組戻の手続を依頼してください。

(3) 時系列をまとめる

被害の全体像を把握するため、どのような経緯でメールが送られてきたかなどについて時系列にまとめてください。

また、取引先に対して攻撃者からメールが送られている場合があるため、取引先に対してもメール受信の有無等について調査を依頼してください。

なお、内部犯行による可能性も考えられるため、調査の際には最少限の関係者で調査を行うなどの注意が必要です。

(4) メール等を保存する

攻撃者から送信されたメールやメールヘッダ情報等を保存してください。

また、取引先に対してもなりすましメールが送られている場合があるため、取引先にメールやメールヘッダ情報等を保存するよう依頼してください。

(5) 警察に通報・相談する

ビシネスメール詐欺被害に遭ってしまった場合は、攻撃者から送信されたメール等を持参して、最寄りの警察署又はサイバー犯罪相談窓口（Tel：088-875-3110）まで通報・相談してください。

警察署案内
（https://police.pref.kochi.lg.jp/police-docs/2024012200010/）

なお、事前に電話で担当者と日時や持参する資料の調整をしていただくと対応がスムーズに進みます。

○　被害防止対策

(1) メール以外の方法で確認する

送金に関するメールを受信した際には、送信元とされている取引先担当者に、電話

や FAX 等のメール以外の方法で送金内容を確認してください。ただし、メールに記載されている電話番号などの連絡先は偽装されている可能性がありますので、名刺や自分のアドレス帳などに載っている連絡先を使用してください。

(2) 送金先の変更や緊急の送金に注意する

特に送金先の変更や緊急の送金に関するメールを受理した場合は、そのメールの送信元メールアドレスをよく確認してください。本来のメールアドレスによく似たメールアドレスに偽装されている場合があります。

また、メールに記載されている内容に不自然なところがないか、確認してください。

(3) 添付ファイルやリンク先を不用意に開かない

攻撃者はタイミング良く振込先の変更に関するメールを送付したり、メールの体裁も本物と同じように作成していることなどから、事前にコンピュータ・ウイルス（不正プログラム）等により、普段のメールのやりとりを盗み見ている可能性があります。

したがって、日頃からコンピュータ・ウイルスへの感染防止対策を講じる必要があります。

- 動画サイト等のウェブサイト閲覧時には不審な広告バナーやダイアログボックス等をクリックしない。
- 知っている人や企業等からのメールであっても、内容をよく確認して、心当たりのない内容であれば不用意に添付ファイルを開いたり、リンクをクリックしたりしないように注意する。

(4) ウイルス対策ソフト、OSを最新の状態に更新する

ビジネスメール詐欺の被害に遭わないためには、

- OS やソフトウェアを最新の状態に保つこと。
- ID やパスワードを適切に管理すること。
- ウイルス対策ソフト等を導入すること。

などが重要です。

(5) 電子署名等の機能を使う

取引相手との電子メールに電子署名機能を用いることでなりすましを見破ることができます。また、添付ファイルにパスワードを付すことも第三者の介在を防ぐために有効な対策ですので、このような機能を積極的に活用してください。

(6) 組織内外で情報共有をする

ある社員がメールの不審点に気づいて、ビジネスメール詐欺の被害を食い止めたとしても、攻撃者は社内の他の社員も同じ手口で騙そうとしてくるかもしれません。社内での情報共有体制を整え、不審なメールや犯罪の手口等の情報を集約し、会社全体でのセキュリティを高めてください。また、日頃から社内及び取引先等との情報共有を密にしておけば、攻撃者から送られてきた不審なメールも対応できる可能性が高ま

るとも言えます。

まずは、こうしたビジネスメール詐欺という犯罪が発生していることを社内に周知し、情報共有を図って、被害に遭うことがないようしっかりと対策を講じてください。

○　参考リンク

- **独立行政法人情報処理推進機構（IPA）**
  「ビジネスメール詐欺（BEC）対策」（外部サイト）
  （https://www.ipa.go.jp/security/bec/index.html）