# 私が出会った詐欺師たち
# 騙されないために

HSBC　アムステルダム支店
Head of Japan Desk Europe
IIA Certified Internal Auditor
澤田　誠

2021年１月22日

# 本日のポイント

1. 偽メールによる送金詐欺被害（ビジネスメール詐欺）が後を絶たない状況

2. 詐欺師はテレワークの弱点をついてくる

3. 詐欺のパターン
   - ① ターゲットを孤立させ・隔離し
   - ② 混乱させ、パニックに陥れて
   - ③ 決断させる
   - ④ 発覚するまで騙し続ける

4. 詐欺被害を防ぐには
   - ① 孤立しない・させない
   - ② 急がない・慌てない。「至急」は疑ってみる。
   - ③ 一人で決断しない・させない。相談する・させる。
   - ④ 特に、支払・送金に関する変更については確認手続きを定めて、実施し随時確認を行う。
   - ⑤ SNS等での、従業員による個人情報の開示にも注意が必要。
   - ⑥ 統制環境(Control Environment)の整備・向上

5. 送金詐欺被害にあった場合には、速やかに
   - ① 警察に通報
   - ② 送金仕向銀行に通報し、送金の取消手続きを取る
   - ③ 取引情報の漏洩をチェックする

# ケース１

## 仕入先を装った偽メール・インボイスによる振込詐欺

- 偽メール・インボイスを送り付け、支払先、振込先を変更させるビジネスメール詐欺（Payment Diversion, Payment Redirection, Imposter Email, Invoice Fraud）
- 東欧のA社は、日系企業B社の顧客・納入先
- B社は納入毎にインボイスをA社あてにEメールと郵便で送付
- 決済はユーロ建てのクロスボーダー銀行送金
- A社は2020年4月から、管理部門は自宅でのテレワーク（Work From Home）を実施していた。
- A社の支払担当者は、仕入先であるB社を装った者からEメールと郵便で、インボイスを受け取った。
- Eメールには、振込先銀行口座の変更指示が記載されていた（ロンドンのX銀行からY銀行への変更指示）。
- A社の支払担当者は、口座変更の指示に従い4件のインボイスについて銀行送金を行った。
  - **偽インボイスの形式、見かけは真正のものと見分けがつかないものであった。**
  - **偽メールの差出人アドレスは一見しただけでは見分けがつかなかった（i,m,n,l,rなどの文字）。**
    - **本物アドレスの例　　BBB@sample.com**
    - **偽アドレス　　BBB@sarnple.com　（ｍではなくてｒとｎ）**
  - **偽メールはA社の複数のスタッフにCCされていた。**
  - **支払口座の変更に関して、B社に確認をしなかった。**
- B社からの支払遅延に関する問合せにより、振込詐欺と発覚。
- 送金仕向銀行からロンドンの被仕向Y銀行に対して、詐欺による送金取消を通知。
- Y銀行では、仕向銀行からの通知を受け資金の追跡調査を行ったが、全額が中東の銀行あてに既に送金されており、回収不能となった。

- **偽メールの発信者（詐欺の犯人）は、A社とB社の決済担当者のメールアドレスと、B社のインボイス書式を正確に知っていた。内部情報の漏洩が疑われるケース。**

# ケース2

## 社内CEO,経営幹部等を装った偽メールによる振込詐欺

- 偽メールや、なりすましメールを送金担当者に送り付け、特別な支払い、振込を行わせるビジネスメール詐欺(Business Email Compromise, CEO Fraud, Chairman Fraud, Imposter Email)
- 東京のC社は、香港のD社と不定期の取引による支払いがあった。
- 決済は米ドル建てのクロスボーダー銀行送金
- C社の支払担当者は、同社の社長を装った者からEメールで、D社への銀行送金の指示を受け取った。
- Eメールには、振込先銀行口座が指定されていた。
- 「特別な事情」により「至急扱い」せよとの指示がメールに記載されていた。
- C社の支払担当者は、同社社長からのメールによる指示に従い2件の銀行送金を行った。
  - **C社の社長は香港・中国に出張中であった。**
  - **偽メールの差出人アドレスは、社長の真正のメールアドレスであった。**
  - **「至急扱い」であったので、C社内で支払に関して確認をしなかった。**
  - **C社では、経営幹部からのイレギュラーな支払指示に関して、社内規定はなかった。**
- C社社長の帰国後、なりすましメールによる振込詐欺と発覚。
- 送金仕向銀行から香港の被仕向Z銀行に対して、詐欺による送金取消を通知。
- Z銀行では、仕向銀行からの通知を受け資金の追跡調査を行ったが、全額が他行あてに既に送金されており、回収不能となった。

- **C社のメールアドレスとパスワード、社内組織、担当者情報等の漏洩が疑われるケース。**
- **サイバーセキュリティの強化が必要。外部からのシステムアクセス制限だけではなく、全ユーザー・スタッフへのフィッシング（Vishing)に関する注意喚起・研修を行う。「フィッシング・メール演習」を実施して、リスクの理解度が低いスタッフについては再研修を行う。**
- **組織における統制環境の不備。**

# ケース3

## 銀行支払保証を偽造し、現金化する詐欺

- 銀行による支払保証書を偽造し、第三者を操って偽造保証書を現金化する、あるいは「融資準備金」、「手続きに必要な工作資金」などの名目で資金を詐取。

- 類似の事例として「原油権益証書」や「アフリカ某国亡命者の隠し預金」などにも注意。
- **反社会的勢力の関与が疑われる場合が多い。**
- **関連国などでの「重要人物とのコネクション」を強調する傾向がある。**
- かつては頻繁に発生していた。減少傾向にあるが、いまだに詐欺師に操られる第三者がいる。

- 多くの場合、銀行保証や証書の額面が巨額。数十億から数百億米ドルの表示がある場合も。
- 偽造された銀行保証書には、発行銀行の会長・頭取などが署名
- 文面はスタンダードだが、どこか不自然な部分がある。例えば発行銀行のロゴマークの色など。
- 偽造者・詐欺師は表には出てこない。第三者を操って、偽造銀行保証書を取引銀行に提示して、現金化を試みる。
- 「現金化に成功したら、取り分10%」などの言葉を信じた第三者が銀行を訪問し、偽造書類を提示。

- 金額と発行銀行の名前と署名者（会長・頭取など）に惑わされ、このような明らかな詐欺話に、まともに対応して詐欺事件に巻き込まれたり、反社会的勢力とかかわりを持ってしまう恐れがある。

- **対策は「まともに対応しない」。**
- **「濡れ手で粟」の「おいしい」話など無い。**

# ケース4

## 不正会計・粉飾決算による融資金詐欺が疑われる事例

- 会社会計を不正に行い、金融機関、債権者を欺いて融資金・出資金を詐取。

- IT系の非上場企業。創業者社長は「IT専門家」
- 業容は急拡大。5年間で売上高10倍超。財務諸表上では成長企業として理想的な経営状況。
- 都市銀行、地方銀行、保険会社など約30行・社から、相対および協調融資で借入。
- 中国の大学と提携し、現地にR&Dセンターを設立準備。
- 電機大手とも取引があった。
- 東京都心の有名ビルに豪奢なオフィス。従業員専用のレクリエーション室、バー、茶室などを併設。

- ある日突然、財務担当者と取締役数名が辞任。
- 借入金の約定返済が停止。主力行の支援は得られず、約6か月後に破産手続きを開始。
- 会社破綻の原因は循環取引とその破綻。売上高と利益の水増しによる粉飾決算。
- 中国への多額の投資も回収不能となった。

- 破綻の兆候
  - **「急成長」は Too good to believe.　貸借対照表の不必要な膨張。**
  - **いわゆる「IT系」であり、当時は銀行・保険会社などにとっても比較的新規の分野。**
  - **財務担当者と取締役の突然の辞任。**
  - **不透明な投資。**
- 経営トップ・幹部の不正と、内・外部との共謀がある場合には、不正行為が発覚しにくい。
- 取引先企業の統制環境・ガバナンスのレベルを、取引開始時だけでなく定期的に審査する必要がある。

## ケース5

# 不動産投資ローンに関する疑わしい事例

- F氏は、面会の約束もなく銀行支店にフェラーリに乗って来訪。
- アジア某国出身で数年前に日本に帰化。
- インターネット検索エンジンを提供する、米国登記のIT企業創業者で社長。

- 東京でマンション投資をしたいので、30億円ほどの融資を要請。
- 銀行の審査部門では以下についての追加情報を求めた。
  - ①　出身国での経歴照会　－＞　申請者はこれを拒絶
  - ②　米国会社の税務申告書－＞　コピーに、米国税務当局の受付印なし

- 日本での会社所在地は、訪問してみると六本木の小さなアパートの一室

- 借入から申告された経歴とバックグラウンドの詳細、真正性の証明が得られず、融資の申し出を断った。

- **「IT」というマジックワード**
- **銀行の個人向け営業部門では、業績拡大への過大なプレッシャーがあった**
- **組織には「アクセル」役と共に「ブレーキ」役が必要。**

# ご参考：リスク管理の考え方について

- リスク量　＝　想定最大損失ｘ発生確率-リスク低減処置
  - リスク低減処置：当該業務の停止、削減、予防処置、検査、トレーニング、保険など
- リスク・トーレランス（許容量）を設定する。
- 詐欺のリスク量　＞　リスク・トーレランス　であれば低減処置によりリスク量を許容範囲内に収める。
- 低減処置の実効性に注意
- 例えば、支払先の変更承認手続は内規でマニュアル化されているが、実際にはマネージメントの判断により例外処理が頻繁に行われれている場合などには、リスク低減処置が実際には機能していない。
- 統制環境の整備が重要。Three Lines of Defense（三線管理）の導入など。

# 本日のポイント

1. 偽メールによる送金詐欺被害（ビジネスメール詐欺）が後を絶たない状況

2. 詐欺師はテレワークの弱点をついてくる

3. 詐欺のパターン
   - ① ターゲットを孤立させ・隔離し
   - ② 混乱させ、パニックに陥れて
   - ③ 決断させる
   - ④ 発覚するまで騙し続ける

4. 詐欺被害を防ぐには
   - ① 孤立しない・させない
   - ② 急がない・慌てない。「至急」は疑ってみる。
   - ③ 一人で決断しない・させない。相談する・させる。
   - ④ 特に、支払・送金に関する変更については確認手続きを定めて、実施し随時確認を行う。
   - ⑤ SNS等での、スタッフ個人情報の開示にも注意が必要。
   - ⑥ 統制環境(Control Environment)の整備・向上

5. 送金詐欺被害にあった場合には、速やかに
   - ① 警察に通報
   - ② 送金仕向銀行に通報し、送金の取消手続きを取る
   - ③ 取引情報の漏洩をチェック。