AMT/NEWSLETTER
Cyber & AI Security

2026 年 11 月 4 日

経営者の顔と声が「攻撃面」になる時代の危機管理

―国内上場会社の資金流出事案とディープフェイクを素材に―

弁護士　中原 隆雅

Contents

Ⅰ. はじめに

Ⅱ. 国内事例が示す「技術以前」の脆弱性
1. 事案の経緯
2. 承認も警告も存在したが、止まらなかった
3. ディープフェイクが加わると何が変わるか

Ⅲ. 顔・声・肩書が「攻撃面」になる
1. 社内の判断を誤らせる類型
2. 社外の信認を標的とする類型
3. 国内の状況と当局の動き

Ⅳ. 複合危機としての初動と平時の備え
1. 三つの時計が同時に動く
2. 誰が三つの時計を束ねるのか
3. 「実質的な確認」を伴う承認とエスカレーション経路
4. 外部拡散への備え
5. 机上演習による検証

Ⅴ. 規制の現在地
1. EU AI 法の透明性義務
2. 令和 8 年改正個人情報保護法と「特定生体個人情報」

Ⅵ. おわりに

Ⅰ. はじめに

2026 年 4 月、東証グロース市場に上場する企業（以下「A 社」という。）において、従業員が警察関係者を名乗る第三者

の指示に従った結果、11 億円を超える会社資金が外部に流出した。A 社は特別調査委員会を設置し、同年 7 月 24 日に調査報告書（開示版）を公表している。公表された調査報告書上、AI による音声又は映像の合成が用いられたことをうかがわせる記載はない。すなわち、高度な合成技術を用いるまでもなく、指示の真正性を確認する仕組みと資金移動に対する牽制が機能しなければ、巨額の資金流出が生じ、特別損失の計上、業績予想の修正、調査委員会による検証、さらには経営責任の議論にまで波及し得るということである。

他方、海外では、権威ある人物の顔・声・肩書に対する信頼を悪用し、社内の従業員や社外の消費者・投資家を欺く攻撃が現実化している。ディープフェイクは、これまで企業が「本人であること」の根拠としてきた顔や声そのものを、攻撃者が利用可能な資源へと変えつつある。

本稿では、①国内の資金流出事案が示す「技術以前」の脆弱性、②顔・声・肩書が攻撃面となる類型の広がり、③資金保全・捜査対応、開示・ガバナンス及びレピュテーションが同時に動く複合危機としての初動と平時の備え、④EU AI 法及び令和 8（2026）年改正個人情報保護法を中心とする規制の現在地について整理する。

II. 国内事例が示す「技術以前」の脆弱性

1. 事案の経緯

2026 年 4 月 24 日、A 社は本件資金流出事案を適時開示した。調査報告書によれば、同月 20 日朝、詐欺グループは同社経理部長の私用携帯電話に架電し、大規模な資金洗浄事件の捜査を進めていること、同部長自身にも関与の疑いがあり出頭が必要であることなどを告げた。いずれも虚偽であったが、家族等への口外を禁じられて心理的に孤立した同部長は、捜査への協力を優先し、振込及び資金移動に関する通常の業務フローや社内の情報セキュリティ・ルールを逸脱した。具体的には、業務利用が認められていないリモートデスクトップアプリを業務用端末で実行し、その後、不正送金が実行されるに至った。資金流出額は合計 11 億 7,981 万円に上った。

2. 承認も警告も存在したが、止まらなかった

本事案で注目すべきなのは、統制が全く存在しなかったわけではないという点である。

調査報告書によれば、当該経理部長は、「給与出金の準備」を名目として担当取締役に 3 億円の資金移動の承認を求め、承認を得ている。また、同日午後には、取引先銀行の担当者から同取締役に対し、詐欺で用いられることの多い金額の入金が複数回あり、スクリーニングの対象となっている旨を含む照会があった。もっとも、同取締役は、自ら承認した給与支払の準備に関連する資金移動であると理解し、口座の入出金を直接確認しなかった。

さらに、経理部員からも、口座残高の減少や見知らぬ相手先への資金移動について疑義が示されていた。しかし、当該経理部長から状況を把握済みである旨の回答を受けたことで、別系統へのエスカレーションには至らなかった。また、通常の業務フロー上は振込データの作成・申請と承認を分離することとされていたにもかかわらず、オンラインバンキング上は当該経理部長のアカウントに双方の権限が付与され、単独で振込を完結できる状態にあった上、承認上限額も実質的な上限として機能していなかった。

すなわち、承認者は存在し、外部からの照会も、内部からの違和感の指摘も届いていた。それでも止まらなかったのである。

教訓は、承認者や職務分掌を形式上設けるだけでは足りないということである。承認者が資金使途、送金先及び金額等を起案者の説明とは別の情報源により確認するとともに、システム上も作成・申請と承認の権限分離が確保されていなければ、実効的な統制とはいえない。また、金融機関からの照会や現場の疑義が生じた場合には、起案者本人への確認だけで処理を終えず、当該取引に関与していない責任者等に報告し、取引内容の独立した確認や必要に応じた送金停止につなげる仕組みが必要である。

3. ディープフェイクが加わると何が変わるか

本事案について、公表された調査報告書上、合成音声や合成映像が用いられたことをうかがわせる記載はない。すなわち、高度な合成技術が用いられなくとも、指示の真正性を確認する手順や資金の流出を止める統制が機能しなければ、巨額の被害が生じ得るということである。

その上で、電話の声やビデオ会議の相手が本人と区別できないものとなれば、現場が違和感を抱く余地はさらに狭まる。もっとも、作成・申請と承認の権限がシステム上分離されていれば、当該経理部長のアカウントのみで送金を完結することはできず、攻撃者は追加の手段を要したことになる。少なくとも社内の不正送金との関係では、ディープフェイクは、全く新しい危機を生むというより、既存の業務プロセスにある「本人であることを信用する」という弱点を増幅するものと捉えるべきである。

III. 顔・声・肩書が「攻撃面」になる

1. 社内の判断を誤らせる類型

企業向けの合成メディア詐欺の代表例として広く知られているのが、エンジニアリング企業 Arup の事案[1]である。2024 年 1 月、香港の従業員は、英国本社の最高財務責任者を名乗る者からのメールを端緒として、機密取引を名目とするビデオ会議に招かれ、その後、指示に従って現地の 5 口座に送金し、約 2 億香港ドル（約 2,500 万米ドル）の被害が生じた。

香港警察の説明によれば、ビデオ会議には、公開されている動画及び音声を素材として事前に生成された映像が用いられており、会議中、被害者と詐欺グループとの間にリアルタイムの双方向のやり取りはなかった。会議終了後の送金指示は、インスタントメッセージングソフトを通じて行われた。偽の「本人」を長時間リアルタイムで再現する必要はなく、最初に相手を本人であると信用させることで、その後は通常の通信手段でも詐欺を継続できることを示す事例である。

2. 社外の信認を標的とする類型

これに対し、近年目立つのは、企業や機関の「外」にいる者を標的とする類型である。2026 年 6 月、イングランド銀行は、同行総裁が政治家と乱闘しているかのような AI 生成の動画及び画像が SNS 上で拡散し、偽のニュース記事風のページを経由して投資スキームの宣伝に用いられているとして、一般に注意を呼びかけた[2]。同年 6 月 18 日に公表されたインタビューで、ベイリー総裁は、自らがどのように描かれたかよりも、偽コンテンツが公衆に対する詐欺に利用されていることを懸念している旨を述べている[3]。

この類型において攻撃者が利用しているのは、権威ある人物の顔・声・肩書に対する信頼そのものである。直接の金銭的被害を受けるのは一般の消費者・投資家であっても、「あの企業・機関の人物が関与していた」という印象が残れば、その信用は毀損される。自社の役員の肖像が、自社と何の関係もない投資詐欺の広告塔として用いられる場面を、あらかじめ想定しておく必要がある。

---

[1] 香港特別行政区政府保安局長の立法会における書面回答「LCQ9: Combating frauds involving deepfake」（2024 年 6 月 26 日）https://www.info.gov.hk/gia/general/202406/26/P2024062600192.htm。同回答は被害企業を特定していない。被害企業については、Arup, "Annual and ESG Report for FY 2023/24" https://www.arup.com/globalassets/downloads/corporate-documents/annual-report/arup-annual-and-esg-report-fy202324.pdf 参照。

[2] Bank of England, "Scams, impersonation and fake videos"。同行は、同行及びその職員が金融商品を推奨し、又は宣伝することはない旨を明示した上で、偽動画等を発見した場合の対応を案内している。 https://www.bankofengland.co.uk/contact/scams-and-fraud

[3] Bank of England, "Transcript of the Governor's pooled broadcast interview given on 18 June 2026" https://www.bankofengland.co.uk/news/2026/june/the-governor-interview-transcript-18-june-2026

3. 国内の状況と当局の動き

国内でも、AI を悪用したサイバーリスクやなりすましへの警戒は高まっている。

独立行政法人情報処理推進機構が 2026 年 1 月に公表した「情報セキュリティ 10 大脅威 2026」では、「AI の利用をめぐるサイバーリスク」が組織向け脅威として初めて選出された[4]。

また、2026 年 8 月 7 日には、消費者庁、警察庁、金融庁、デジタル庁、総務省、法務省及び経済産業省の 7 府省庁が、Google、LINE ヤフー、Meta、TikTok 及び X の 5 社に対し、SNS 等におけるなりすまし詐欺広告への対策強化を共同で要請した[5]。要請には、広告主の本人確認の確実な実施、広告の透明性向上、削除要請への対応の徹底等が含まれ、各社に対応状況の報告も求められている。

注目すべきは、同要請が、ディープフェイク等によって著名人の肖像や音声を利用したなりすまし広告について、詐欺被害だけでなく、なりすまされた者の社会的信頼への影響も問題としていることである。企業にとっても、直接的な財産被害が生じていなくても、自社の役職員の肖像や音声が悪用された場合には、レピュテーション上の危機として対応を要する場面がある。

Ⅳ. 複合危機としての初動と平時の備え

1. 三つの時計が同時に動く

なりすまし又は合成メディアによる事案を、「情報セキュリティの問題」あるいは「経理の不正送金の問題」とだけ捉えると、対応は後手に回りやすい。一つの事案について、期限も判断主体も異なる三つの時計が同時に動くからである。

第一に、資金保全・捜査対応の時計である。送金の組戻しや口座凍結に向けた金融機関への連絡、証拠保全、被害額の把握、捜査機関への相談・被害申告等は、可能な限り早期に着手する必要がある。

第二に、開示・ガバナンスの時計である。上場会社であれば、適時開示の要否、業績への影響や会計処理、調査体制、経営責任等について、並行して検討を進める必要がある。

第三に、レピュテーションの時計である。偽動画等が外部で拡散している場合には、顧客、投資家及び取引先に対し、何が偽物であり、どこを公式情報源として参照すべきかを迅速かつ一貫して伝える必要がある。

A 社でも、事案発生後、適時開示、特別調査委員会の設置、特別損失の計上と業績予想の修正、調査報告書の公表、再発防止策の策定といった対応が、相次いで進められた。

2. 誰が三つの時計を束ねるのか

三つの時計は、それぞれ判断事項や担当部署が異なる。したがって、平時から、これらを誰が統括し、初動に必要な判断を誰が行うのかを明確にしておく必要がある。

具体的には、危機対策本部の設置権限に加え、本部設置前の段階で、送金停止、金融機関への連絡、社内通達、対外公表等の初動判断を誰が行うのか、また、法務、経理・財務、情報システム、IR 及び広報を誰が招集するのかをあらかじめ定めておくことが重要である。

---

[4] 独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2026」(2026 年 1 月 29 日公表)。組織向け脅威の第 3 位。
https://www.ipa.go.jp/security/10threats/10threats2026.html

[5] デジタル庁ほか「SNS 等におけるなりすまし詐欺広告に関する対策強化のための 7 府省庁合同要請の実施」(2026 年 8 月 7 日)。要請文は、なりすまし詐欺広告について、広告を閲覧した消費者・利用者に財産上の被害をもたらすおそれのみならず、なりすまされた者の社会的信頼を著しく損なうおそれもあるとしている。要請文本体は、消費者庁ウェブサイト掲載の別紙参照。
https://www.digital.go.jp/news/b96e34b8-0af0-4fe3-b6b5-2191726c8cc5
https://www.caa.go.jp/notice/assets/caa_cms204_260807_01.pdf

さらに、その判断権限を持つ役員等自身がなりすましの対象となった場合に備え、代替的な指揮・承認ルートも設けておく必要がある。権限を持つ役員等からの指示に見えることによって、通常の確認やエスカレーションが抑制され得る点こそ、この種の攻撃の特徴だからである。

3.「実質的な確認」を伴う承認とエスカレーション経路

重要な資金移動について承認手続を設けることは出発点であるが、それだけでは十分ではない。

承認者が、資金使途、送金先及び金額等を、起案者の説明とは別の資料や経路によって確認する手順となっているか、また、振込データの作成・申請と承認が、運用上だけでなくシステム上も分離され、単独で送金を完結できない設定となっているかを確認する必要がある。

さらに、金融機関から異常な取引について照会を受けた場合や、現場の従業員が疑義を抱いた場合に、起案者本人への確認だけで処理を終えず、当該取引に関与していない責任者等に報告し、取引内容の独立した確認や必要に応じた送金停止につなげる仕組みも重要である。オンラインバンキングの権限・限度額についても、実際の職責や取引規模に応じて設定し、定期的に見直す必要がある。

重要なのは、承認者を形式上置くことではなく、起案者から独立した確認と権限分離を実際に機能させることである。

4. 外部拡散への備え

自社の経営者等の肖像や音声を用いた偽動画や偽広告が外部で拡散した場合には、証拠保全と並行して、プラットフォームに対する削除申出を迅速に行う必要がある。

令和 6(2024)年改正により、いわゆるプロバイダ責任制限法は「特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律」(以下「情報流通プラットフォーム対処法」という。)へ改称され、大規模なプラットフォーム事業者について、権利侵害情報の削除申出の方法を定めて公表すること、申出を受けた場合に必要な調査を行うこと等が義務付けられた(同法 22 条・23 条)[6]。この規律は令和 7(2025)年 4 月 1 日から施行されている。

危機発生後に各プラットフォームの窓口や必要資料を一から調べるのではなく、主要なサービスごとに、削除申出窓口、申出に必要な情報及び社内で申出を行う権限者を平時から整理しておくことが望ましい。事案によっては、肖像権等に基づく差止めや発信者情報開示、不正競争防止法その他の法的手段も併せて検討することになる。

また、自社が発信した正規コンテンツの来歴を確認しやすくする取組も考えられる。C2PA(Coalition for Content Provenance and Authenticity)は、デジタルコンテンツの作成・編集等の来歴情報を付与・検証するための技術標準を策定しており、これに基づく Content Credentials を活用することも一案である[7]。ただし、来歴情報は再加工等によって失われ得る一方、来歴情報が付与されていないこと自体は、そのコンテンツが偽物であることを意味しない。そのため、真正性確認の補助手段の一つとして位置付ける必要がある。

5. 机上演習による検証

以上のような対応を規程に定めるだけでなく、机上演習を通じて実際に機能するかを確認することが重要である。

例えば、①経営者の音声を模した緊急送金の指示、②捜査機関を名乗る者から秘密裏の協力や遠隔操作ソフトウエア

---

[6] 総務省「インターネット上の違法・有害情報に対する対応(情報流通プラットフォーム対処法)」。同法 21 条に基づき届出のあった各事業者の削除申出の窓口及び削除基準が公表されている。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html

[7] C2PA, "Content Credentials Deployment Guidance 1.0"(2026 年 7 月 8 日)。C2PA は、デジタルコンテンツの作成・編集等の来歴情報を記録・検証するための技術標準を策定している。同文書は、スクリーンショットやメタデータを削除するツールによる再書き出し等により来歴情報が失われ得ることにも留意を促している。 https://c2pa.org/wp-content/uploads/sites/33/2026/07/Content-Credentials-Deployment-Guidance.pdf

の実行を求められる場面、③自社役員の偽動画を用いた投資詐欺広告が SNS 上で急速に拡散する場面といったシナリオが考えられる。

演習で確認すべきなのは、参加者がディープフェイクを見破れるかではない。いったん手続を止め、別経路で確認し、適切な部署・責任者にエスカレーションし、その判断過程を記録できるかである。演習結果を記録して改善につなげておくことは、事案発生後の検証や、平時の備えを外部に説明する際にも有用である。

Ⅴ. 規制の現在地

1. EU AI 法の透明性義務

EU AI 法（Regulation (EU) 2024/1689）50 条は、2026 年 8 月 2 日から適用され、AI 生成・加工コンテンツとの関係では、AI システムの提供者と利用主体（deployer）に、それぞれ異なる透明性義務を課している。提供者には、一定の場合に、AI 生成・加工コンテンツを機械的に識別可能とする措置が求められ（同条 2 項）、ディープフェイクに該当する画像・音声・映像コンテンツを生成・加工する AI システムの利用主体には、原則として、そのコンテンツが人工的に生成・加工されたものであることを開示する義務が課される（同条 4 項）[8]。EU AI 法は、EU 域外の事業者であっても、EU 市場に AI システムを投入する場合や、AI システムの出力が EU 域内で利用される場合等には適用され得るため、日本企業にも無関係ではない。

なお、2026 年 7 月の Digital Omnibus on AI（Regulation (EU) 2026/1744）により、高リスク AI に関する一部義務の適用時期は延期された。他方、50 条の透明性義務は原則として 2026 年 8 月 2 日から適用されており、同日より前に市場投入された合成コンテンツを生成する AI システムについて、提供者に課される同条 2 項の義務に限り、同年 12 月 2 日までの経過措置が設けられている[9]。

2. 令和 8 年改正個人情報保護法と「特定生体個人情報」

「個人情報の保護に関する法律等の一部を改正する法律」（令和 8（2026）年法律第 56 号）は、2026 年 7 月 10 日に成立し、同月 17 日に公布された[10]。改正法は、一部を除き、公布の日から起算して 2 年を超えない範囲内において政令で定める日から施行される。

本稿との関係で注目されるのが、新設された「特定生体個人情報」に関する規律である。特定生体個人情報とは、特別の技術又は多額の費用を要しない方法で取得することができ、かつ、その取得を本人が容易に認識できない身体的特徴に係る情報として政令で定めるものを変換した「特定生体個人識別符号」を含む個人情報をいう。顔特徴データ等がその対象となることが想定されている。改正法は、特定生体個人情報について、その利用目的等の一定事項をあらかじめ本人に通知し、又は本人が容易に知り得る状態に置くことを義務付けるほか、利用停止等請求の要件を緩和し、オプトアウト制度による第三者提供を禁止している[11]。

---

[8] Regulation (EU) 2024/1689（EU AI 法）50 条。European Commission, “Guidelines on transparency obligations for providers and deployers of AI systems” (20 July 2026). https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems

[9] Regulation (EU) 2026/1744（2026 年 7 月 8 日。いわゆる Digital Omnibus on AI）。2026 年 7 月 24 日に EU 官報に掲載され、同月 27 日に発効した。附属書Ⅲ関係の高リスク AI に係る義務の適用時期が 2027 年 12 月 2 日に延期された一方、50 条 2 項のマーキング等に関しては、2026 年 8 月 2 日より前に市場投入された合成音声、画像、動画又はテキストを生成する AI システム（汎用 AI システムを含む）の提供者について、2026 年 12 月 2 日までの経過措置が設けられている。 https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng

[10] 個人情報保護委員会「「個人情報の保護に関する法律等の一部を改正する法律」の公布について」（令和 8（2026）年 7 月 17 日） https://www.ppc.go.jp/news/press/2026/260717/

[11] 改正法の条文、新旧対照表及び概要については、個人情報保護委員会「令和8年 改正個人情報保護法について」参照。

もっとも、この改正を「ディープフェイク規制」と捉えるのは適切ではない。特定生体個人情報に関する新たな規律の対象は、本人識別に用いられる一定の生体情報を変換したデータを含む個人情報であり、単に顔が写った写真や動画そのものが直ちに「特定生体個人情報」に該当するわけではない。したがって、経営者の偽動画そのものが、この新規律によって包括的に規制されるわけではない。

個人情報保護委員会では、政令・規則・ガイドライン等による具体化の検討が進められており[12]、対象範囲や実務上の取扱いについて引き続き確認が必要である。

Ⅵ. おわりに

本稿で取り上げた国内事案が示すのは、指示の真正性を見極めることだけに頼らず、手順と権限設計によって不正な資金移動を防ぐことの重要性である。

承認者が実質的な確認を行わず、金融機関からの照会や現場の違和感が適切なエスカレーションにつながらないのであれば、合成メディアが用いられたか否かにかかわらず、同種の危機は起こり得る。そして、顔や声の合成精度が高まるほど、「見れば偽物だと分かる」「声を聞けば本人だと分かる」という前提は置きにくくなる。

企業が直ちに着手できるのは、自社の統制と指揮系統を、「本人に見えるものを必ずしも信用できない」という前提で見直すことである。重要な送金に係る独立した確認手順とシステム上の権限分離、異常を別系統へ上げるエスカレーション経路、危機対策本部の設置・初動判断権限、外部でなりすましが発生した場合の削除申出ルートを平時から整備し、机上演習を通じて実際に機能するかを検証することが出発点となる。ディープフェイク時代に問われるのは、偽物を見抜く目というより、目の前の「本人」を信用できない状況でも、組織として安全に止まり、確認し、動き直せるかという危機管理の設計である。

以上

---

https://www.ppc.go.jp/personalinfo/legal/r8kaiseihogohou/

[12] 個人情報保護委員会「個人情報の保護に関する法律等の一部を改正する法律 政令・規則・ガイドライン等の整備に関する今後の進め方について」（令和 8（2026）年 9 月 9 日決定）。同委員会は、これに先立ち、令和 8（2026）年 7 月 31 日に「今後の取組」を、同年 8 月 26 日に「政令・規則等で定める事項の全体像について」を、それぞれ決定している。
https://www.ppc.go.jp/files/pdf/260909_kongonosusumekatanitsuite.pdf

- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

- 本ニュースレターの執筆者は、以下のとおりです。
  弁護士 中原 隆雅　takamasa.nakahara [at]amt-law.com
  ※メールを送信する際には、[at]を@に変更してお送りください。

- ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

- ニュースレターのバックナンバーは、こちらにてご覧いただけます。