NISHIMURA
& ASAHI

昨今の企業不祥事・リモート環境を踏まえたコンプライアンス

2022年2月17日

西村あさひ法律事務所
弁護士　木目田　裕

目次

NISHIMURA & ASAHI

1. 近時の企業不祥事

近時の企業不祥事

NISHIMURA & ASAHI

- コロナ禍で在宅勤務の増加（牽制が弱まる、他人の目が気にならなくなる等）
  →会社の金の横領や、顧客からの金銭詐取等の新規発生や発覚
- 総務省や農水省などの接待問題
  国家公務員倫理法・倫理規程を改めて確認
  →「この程度は許されている」、「実害は何もない」が通用しない時代。ルールに文字通り違反していれば制裁あり。業法等も同様に留意が必要
- モラル違反(コンダクト・リスク)というだけで厳しく責任を問われる
  →倫理感・インテグリティが一層重要
- 製品不正、カルテル
  →継続・新規発生、「昔の話」は通用しない
- ランサムウェア攻撃、ビジネスメール詐欺、アカウント乗っ取り、機密情報や個人情報の漏洩
- サプライチェーン（特に人権と環境：強制労働・児童労働、紛争鉱物、CO2、パーム油と熱帯雨林の破壊）、経済安全保障（防衛、先端技術等）
  →企業の社会的責任の増大、NGOや活動家を先入観で毛嫌いしない

コロナ禍での横領・詐欺

NISHIMURA & ASAHI

- 在宅勤務の増加→上司が担当者に、ネットバンキングのワンタイム・パスワード発生器を一時的に貸与→悪用
- 印紙を横領して金券ショップで換金、コロナ以前は帳簿改ざん等で発覚回避→コロナで糸が切れたのか、帳簿改ざん等せず発覚
- ウェブ商談などの非対面取引の増加→詐欺を行いやすくなる（新規取引先なのに社屋訪問もしないなど、身元や与信のチェックが甘くなる）

  ※　取り込み詐欺が増加（日経新聞2022年1月14日）

（参考）国家公務員倫理法・倫理規程

NISHIMURA & ASAHI

利害関係あり

- 金銭・物品の贈与や接待を禁止
- 割り勘の場合でもゴルフや旅行を禁止

➢ 利害関係者：
- ✓ 許認可等の申請者
- ✓ 補助金等の交付
- ✓ 立入検査、監査、行政処分
- ✓ 行政指導
- ✓ 所管する業界において事業を営む企業
- ✓ 契約関係

利害関係者との間でも禁止されない行為の例
- ✓ 宣伝用物品・記念品を受領すること
- ✓ 学生時代の友人からの香典・祝儀
- ✓ 職務として出席した会議での簡素な飲食
- ✓ 立食パーティー

利害関係者でも、自分の飲食代を自己負担（不明なら割り勘）で会食できる
(1万円超は倫理監督官への事前の届出)

利害関係なし

- 本省課長補佐級以上が5千円超の贈与等を受けたときは、各省庁の長へ報告
- 2万円超については公開の対象となる

- 違反した場合、公務員は懲戒処分の対象となる
- 地方公務員や独立行政法人も、国家公務員倫理法と概ね同内容の倫理規程あり

＜公務員の声＞
利害関係者でなくても5千円超は贈与等報告
「会費制」「割り勘」の方がよい
お土産などは貰いたくない

品質不正問題に終わりはない

NISHIMURA & ASAHI

- 今でも新たな不正等が新規に発生している
- 現場では、何が不正か理解されていないのかもしれない

現場で
問題意識なし

- ✓ 実際の製品とは異なる部品や材料を使用して、公的な認定・認証を取得した
- ✓ 実際の製品とは異なる図面を使用して、公的な認定・認証を取得した
- ✓ 顧客から要求されている仕様とは異なる手順書を作成した
- ✓ 決められている手順を省略したり、順番を変えて装置や部品を製造した
- ✓ 決められている材料や部品とは異なる材料や部品を使って製造した
- ✓ 決められている手順を省略したり、順番を変えて装置や部品の性能を検査した
- ✓ 3回の測定で合格しなかった場合には不合格にすると決められているのに、4回目の検査で合格したので、合格したと報告した

- 教育、継続的アンケート、社内リニエンシー、外部者の有効活用

（参考）品質不正問題に共通すること

NISHIMURA & ASAHI

【会社ないし従業員の言い分】

○「製品の安全性・品質に問題ない。自社で出荷基準として定めていた数値が過剰だっただけ。
これまでも不合格品でお客さんからクレームや事故等はなかった。
それなのに不合格にすると、必要な数量の出荷が遅れることになって、お客さんにかえって迷惑をかける」

- 問題ないなら、客先に説明すればよかったはず
- 品質偽装の発覚で、出荷停止、客先での製品の再検査・エンドユーザー向け説明、客先製品のイメージ悪化など、結局、客先に大きな迷惑をかけた
- 自社出荷基準が過剰ならば、客先と相談して変更すればよかった。単に手抜きをしただけではないか
- 自社出荷基準が定められた理由・経緯を検討したのか？

○「出荷遅れで採算悪化するのを回避したい」

○「先輩も上司もやってきたこと。なぜ今になってダメだと言われるのか分からない。自分だけが良い子になることもできない。」

【対策】

○過剰な出荷基準の是正
○過度の収益目標の是正
○1人に依存せず、複数チェック
○検査データ等のマニュアル処理の排除

○意識改革
- 顧客目線で考える＝真の意味の「客先のため」
- 外部に胸を張って明らかにできないことは、間違っている
- 真の意味の「会社のため」とは、問題があれば声を上げること
- 前任者からの引継ぎの時こそが大事
- 品質不正の相次ぐ発生
  →社会の動きと自分の仕事を結び付ける

（参考）品質不正問題に共通すること(続き)

NISHIMURA & ASAHI

【工場・事業所内での組織上の問題】

○ 工場・事業所内での品質保証・検査部門の独立性の欠如
- 製造部門との間の人事異動
- 同じ職場で仲良し・顔見知り
- 製造部門出身の工場長らが人事評価
- 品質保証・検査部門の立場の弱さ

○ 品質保証・検査部門のリソース不足
- 人手が足りない
- 設備投資が足りない

○発見の遅れ

○不正の長期化

○五月雨的発覚

【対策】

○人事異動パターンの見直し

○工場内の縦のラインだけでなく、本社品質管理部門も工場等の品質管理部門の人事評価を横から行う仕組みを作れないか？

○品質保証・検査部門を軽視していないか？

○ 全社・全グループでの水平展開

○ 新入社員の声、後任者の気づき⇒定期的な人事異動と声を拾い上げる仕組み

○「隠すな」という単純素朴なメッセージのくり返し

（参考）カルテルの未然防止のための注意点

NISHIMURA & ASAHI

- ○ 個別の価格、生産量などの情報交換は、ほぼカルテル
- ○ 官公庁発注案件だけでなく、民・民の取引でも、カルテルがあれば摘発
- ○ 競合他社の「原料価格が上がってますから、製品も値上げしないと厳しいですね」に対し、「そうですね」だけで、カルテル。特に何も発言せず、黙って聞いていただけでも、状況によってはカルテル
- ○ 客先から値下げを要求され、競合他社から「うちは頑張るつもりだが、貴社はどうするの」と聞かれ、「うちも頑張りますよ」とだけ伝えた。これだけで、状況によってはカルテル
- ○ お互いの商圏・既得権を尊重する合意もカルテル
- ○ 意識改革（正当化させない）
  - 「中小の保護、技術継承、品質確保」は通用しない(橋梁談合その他)
  - 汗かきルール、既設ルール、客先意向も、立派な談合(重電談合その他)
  - 「厳しい値下げ要求に対抗するため」は通用しない(自動車部品カルテルその他)
- ○ 同業他社を信用しない(相手はリニエンシー申請中かもしれない。海外案件では、おとり捜査かもしれない)

ランサムウェア（身代金攻撃）

NISHIMURA & ASAHI

- ハッカーが会社のシステムに侵入し、システムを凍結、凍結解除に暗号資産等の支払いを要求。顧客情報をダークウェブで売る等と脅迫。
- 身代金支払いに応じるかどうかは経営判断の問題だが、蛇の目ミシン事件（最判平成18年4月10日民集60巻4号1273頁）に注意
- 最近までは、米国では、自治体、企業、病院等が費用対効果で支払うことが珍しくなかった。これに対して、ランサムウェア攻撃を助長しているとして、払うべきでないとの声が高まっている（次頁参照）
- また、米国の制裁対象国に支払うと、米国からOFAC規制違反で制される可能性（次頁参照）
- 日本企業としては、身代金支払いに応じるかどうか、慎重な検討が必要。単なる費用対効果ではなく、顧客や役職員等の生命身体の保護に必要な場合などに限定すべきか

(参考)ランサムウェア：当局見解

NISHIMURA & ASAHI

① FBI Internet Crime Report 2020
② 2021 年 5 月 11 日　CISA(Cybersecurity & Infrastructure Security Agency)“DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks”
③ 2021年5月13日 The White House“Press Briefing by Press Secretary Jen Psaki, May 13, 2021”
　⇒ ①、②、③いずれも、ランサムウェアの攻撃者に身代金を支払わないよう勧告
④ 2020 年 10 月 1 日　米国財務省“Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments”
⑤ 2020年10月1日 FinCEN Advisory“Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payment”
　⇒ ④、⑤OFACやFinCENは、身代金の支払いがOFAC規制等になるリスクがあるとする
⑥ 2020年12月18日　経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」
　⇒ 「こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。」
⑦ 2021年10月11日　JPCERT/CC「ランサムウエア対策特設サイト」
　⇒ 身代金を支払ったとしてもデータやシステムの制限が解除される保証はないため支払うべきではない

(参考)不正が発覚した際にとるべき初動の例

NISHIMURA & ASAHI

○ いずれも迅速かつ徹底的な事実調査が最優先・大前提

不正の発覚	とるべき初動
内部監査や会計監査等で粉飾決算の疑い	事実調査⇒速報的適時開示・東証向け説明、第三者委員会立ち上げ、取引先・銀行・所管官庁等への公表タイミングでの説明、SESCへの課徴金減額申請　等
カルテルの嫌疑で公取の立入審査	適時開示・リリース、調査対象事実の課徴金減免申請、取締役会決議の段取り、全社・全グループに広げた事実調査と課徴金減免申請、判別手続に注意　等
内部監査や会計監査等で横領等の疑い	事実調査（通帳等の早期確保、共犯者に注意、自宅待機）⇒刑事告訴・告発、懲戒解雇、民事保全や弁済交渉、逮捕等の時点での適時開示・リリースの準備　等
セキュリティ・インシデント	事実調査（対象システムのオフライン化、ログ等の保存・検証、影響可能性のある範囲の早期確定）、二次被害の有無の見通し、公表・リリース、NISC・IPA・所管官庁への情報提供　等
米国司法省から米国子会社にFCPA（外国公務員等贈賄）の嫌疑で資料等提出要請やサピーナ送達	事実調査、米国・日本・第三国（贈賄等の舞台）の弁護士事務所の起用・協働関係構築、弁護士依頼者秘密特権の確保、米国当局との間でフォレンジック手法の調整、日本当局への申告の要否、リーク報道への対応準備　等

（参考） 日本取引所自主規制法人「上場会社における不祥事対応のプリンシプル」（2016年2月24日）

NISHIMURA & ASAHI

企業活動において自社(グループ会社を含む)に関わる不祥事又はその疑義が把握された場合には、当該企業は、必要十分な調査により事実関係や原因を解明し、その結果をもとに再発防止を図ることを通じて、自浄作用を発揮する必要がある。その際、上場会社においては、速やかにステークホルダーからの信頼回復を図りつつ、確かな企業価値の再生に資するよう、本プリンシプルの考え方をもとに行動・対処することが期待される。

① 不祥事の根本的な原因の解明

不祥事の原因究明に当たっては、必要十分な調査範囲を設定の上、表面的な現象や因果関係の列挙にとどまることなく、その背景等を明らかにしつつ事実認定を確実に行い、根本的な原因を解明するよう努める。

そのために、必要十分な調査が尽くされるよう、最適な調査体制を構築するとともに、社内体制についても適切な調査環境の整備に努める。その際、独立役員を含め適格な者が率先して自浄作用の発揮に努める。

(参考) 上場会社における不祥事対応のプリンシプル (続き)

NISHIMURA & ASAHI

② 第三者委員会を設置する場合における独立性・中立性・専門性の確保

内部統制の有効性や経営陣の信頼性に相当の疑義が生じている場合、当該企業の企業価値の毀損度合いが大きい場合、複雑な事案あるいは社会的影響が重大な事案である場合などには、調査の客観性・中立性・専門性を確保するため、第三者委員会の設置が有力な選択肢となる。そのような趣旨から、第三者委員会を設置する際には、委員の選定プロセスを含め、その独立性・中立性・専門性を確保するために、十分な配慮を行う。

また、第三者委員会という形式をもって、安易で不十分な調査に、客観性・中立性の装いを持たせるような事態を招かないよう留意する。

③ 実効性の高い再発防止策の策定と迅速な実行

再発防止策は、根本的な原因に即した実効性の高い方策とし、迅速かつ着実に実行する。この際、組織の変更や社内規則の改訂等にとどまらず、再発防止策の本旨が日々の業務運営等に具体的に反映されることが重要であり、その目的に沿って運用され、定着しているかを十分に検証する。

④ 迅速かつ的確な情報開示

不祥事に関する情報開示は、その必要に即し、把握の段階から再発防止策実施の段階に至るまで迅速かつ的確に行う。この際、経緯や事案の内容、会社の見解等を丁寧に説明するなど、透明性の確保に努める。

2. コロナとコンプライアンス

コロナとコンプライアンス

NISHIMURA & ASAHI

○ サプライチェーンの混乱、企業業績の悪化等
- 2000年代前半や2010年前後のように粉飾決算や不公正ファイナンス
- 業績プレッシャーから、企業不祥事やカルテル等
- 監査での実査・往査や在庫棚卸し等が簡略化⇒過去の不正が露見しにくく、新たな不正を行いやすくなる、特に海外に注意

○ 製造現場での人的リソースの不足を正当化事由として、製品不正や検査不正の新たな発生

○ 取引先や下請けへのしわ寄せ等＝独禁法違反(優越的地位の濫用)、下請法違反の代金減額、買いたたき等

○ 小売業などのリテールでは、コロナ対応を謳った製品・サービスの表示の問題(景品表示法の優良誤認、健康増進法違反(食品の虚偽・誇大広告)等)や、マスクと高額商品の抱合せ販売等の問題

※ 消費者庁「業者が講ずべき景品類の提供及び表示の管理上の措置についての指針」

コロナとコンプライアンス(続き)

NISHIMURA & ASAHI

○ テレワーク・在宅勤務の一般化

- 部下と上司のコミュニケーション低下、牽制が少ないことに起因する不祥事増加リスク
- 在宅勤務や出社日数減⇒役職員らの会社への帰属意識の希薄化、上司や同僚らの目が気にならなくなる⇒役職員らによる使い込みといった横領等
- 決裁時の承認印が電子メール承認で代替、一部のプロセスの事後承認化⇒不正の余地
- 営業部門、コンプライアンス部門等における出社人数の減少⇒企業不祥事の端緒となる情報や内部通報等の把握・社内伝達・事実調査等の対応がスムーズに進まず（リスク兆候把握能力の低下・問題の拡大）
- 内部通報者から見ると、会社の通報窓口の留守電にメッセージを何回録音しても会社側のレスポンスがないといった不満・不信を抱くかも
- 在宅・出社シフト等⇒同一職務を複数人が交代で務めることが増える⇒過去の不正が発覚する可能性が高まる

コロナとコンプライアンス(続き)

NISHIMURA & ASAHI

○ テレワークに伴う個人情報・営業秘密等の持ち出しと漏洩リスク

在宅勤務における私用デバイスやネットワーク利用⇒サイバー攻撃に対する脆弱性を高める

○ テレワークに伴う役職員の負担

ウェブ会議での自宅居室の映り込み等、プライバシーとの関係
「音声はよいが、カメラはオフにしたい」
メンタルへの影響(人とのつながりの希薄化、ウェブ会議の連続による疲労、夜間や休日労働の増加、公と私の境界の曖昧化)

○ リモートハラスメント(異性社員の自室や服装等をあれこれ言及、目の前にいない部下は働いていないと思っている上司の激怒)、パワハラの増加

○ 業務態勢がリモートに対応していない→担当者の個人ID・PWの他人への貸与・使い回し、担当者の突発的な休みに対応できない等

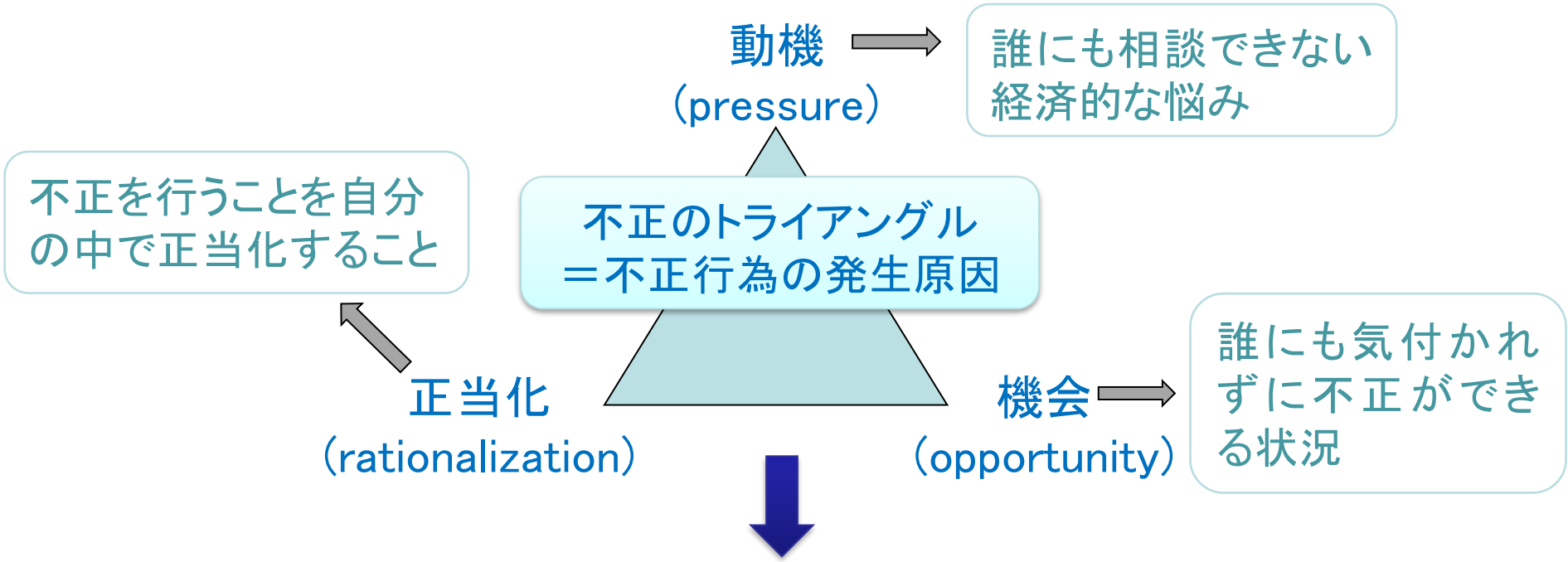
コロナとコンプライアンス(続き)

NISHIMURA & ASAHI

不正のトライアングル

⇓

コロナやリモートワークは、動機、機会、正当化とも強める



不正行為の再発防止策を検討する前提として、
当該不正行為について、どのような点に動機・機会・正当化の
要素があったのか、整理が必要

（参考） 不正のトライアングル

NISHIMURA & ASAHI

動機

- ✓ ギャンブル、愛人との交際
- ✓ 一定のレベルの人たちと付き合いたい
- ✓ 発注のミスで、会社に損失を与えてしまった

- 年収に不釣り合いな不動産を購入
- 急にブランド品を身に着ける
- 頻繁に夜の飲食店に出かけ、羽振りがよくなる

基本的には個人の問題だが、経営環境の悪化に基づく従業員へのしわ寄せや無理な指示など、会社の行為によって作り出される場合もある

機会

- ✓ 業務特性上、専門性が高い
- ✓ 単独業務が多い
- ✓ 同僚の業務や行動に無関心な雰囲気
- ✓ 行動管理ができていない

- 長期間同一の役職・部署で勤務し、異動・昇進を望まない
- 特定の業者や顧客と親密な関係にあり、その関係を他の者と共有しない
- 担当している職務を他の者に分担させない
- 夏休み等、長期休暇を取得せず、取得しても出勤する

内部統制システムの問題：気付かれない状況、誰もチェックしていない状況を減らす

- ● 人事ローテーションの活性化
- ● 中堅幹部(現場を見通せる人)による抑止
- ● 同僚同士の相互抑制
- ● いきいきとした、風通しの良い職場
- ● 監査スタッフ・内部通報制度の充実

正当化

- ✓ 一時的に借りるだけ(後で返す)
- ✓ 会社のみんながやっている
- ✓ 会社のためにやっている
- ✓ お客様のご要望に沿ったもの
- ✓ 会社への貢献に見合った収入・待遇を得ていない
- ✓ 上司からひどい待遇を受けている

- 会社や上司への不満を言わなくなる
- 会社の人間との付き合いを避けるようになる
- 目立たないように振る舞うようになる

「正当化」は、個人の内面の問題(道徳意識、倫理観、プライドなど)でもある。不正を「正当化」しないという組織風土や組織文化が必要。

コンプライアンス上の着眼点

NISHIMURA & ASAHI

- ○ 過度の業績プレッシャーが生じていないか
- ○ リモートを前提とした原本確認や実査の手法の工夫
- ○ 業務上のレポートラインを通じた情報・指示の伝達経路や決裁経路の検証・徹底
  - 在宅勤務による報告や決裁等の混乱→ポテンヒット、単独業務化による牽制欠如
  - 職務分離、承認権限、証跡の観点で再検証
- ○ 従業員が業務を抱え込んでしまい、見えなくなる可能性
  ⇒上司や先輩に相談しやすい雰囲気、コミュニケーション確保により注力
- ○ ウェブ会議、サテライトオフィスの活用などface to faceを意識したコミュニケーションの励行
- ○ 緊急事態宣言下等で急遽導入した業務プロセス（事後承認化等）の見直し、拡大解釈の戒め、重点的な内部監査
- ○ リモートハラスメントに即した研修（具体的なNGケースの周知）
  ※ パワハラでは、トップメッセージ（全く許されないことの明確化）、NGケース・処分例の社内周知、業務指導とパワハラの区別、見て見ぬ振りは共犯者、パワハラ予備群の教育
- ○ テレワーク等に即した情報セキュリティの見直し・周知
- ○ 今後は、取引先等の与信管理等の一層の徹底も

非対面取引の増加

NISHIMURA & ASAHI

- 顧客に対する説明を十分に行い、顧客の理解をチェックすること
  ⇒説明義務違反、虚偽説明などを理由に、契約無効取消し・損害賠償などの民事上のトラブル
- 録画録音が残る（虚偽説明、金融商品の断定的判断の提供など）
- 「画面の向こう側の顧客の横に誰かいるみたい。顧客がその人の言いなりになっているかも？」
  - 高齢者の顧客が誰かの言いなりになって取引内容やリスク等を理解しないまま取引をしようとしているかもしれない
  - 商品の解約・出金の場合など、特殊詐欺かもしれない
  - 顧客にまずは確認し、不審な点があれば、上長や法務・コンプラに報告するように現場に徹底
- 顧客の「なりすましリスク」
  - 映像はごまかせるということを意識。電話や遠隔会議システムで話す際も、おかしな点がないか、アンテナを張る必要
  - 取り込み詐欺その他の詐欺に注意
- 説明書面、契約書等への署名捺印。善意で「お客さんが店舗まで来るのは大変だから」等と、代筆、代印の可能性
  - お客さんが口頭で代筆代印でよいと言っていても、後で必ずトラブルになる
  - 電子署名や郵送を活用
- メールアドレス変更の通知メールに注意
  - 不正送金・・・担当者と上司の二重承認で送金許可のところ、上司の登録メールアドレスを勝手に変更
  - キャッシュレス決済の不正利用等・・・登録メールアドレスの勝手な変更

3. リモート環境下での不正調査・内部監査

調査・監査手法・・・ヒアリング

NISHIMURA & ASAHI

- ヒアリング、資料精査、フォレンジック
- リモート環境下でのヒアリング
  - 対面の方がベターなことは否めない
  - 複数の資料を広げて、相互に突合・参照する必要
  - 相手の態度や雰囲気
  - リモートの場合、発言のタイミングをつかみにくく、丁々発止のやり取りは難しい
- リモートの場合、相手が秘密録音している可能性→相手の承諾の下で録音、改変対策にもなる
  - 相手が秘密録音をSNSで公開→法的手段には限界あり。事案によってはそれを覚悟しつつヒアリング時の言動に注意
  - リモートであっても、必ず顔を表示し合ってヒアリングを行う
- 相手が言いたくない話を聞き出すためには、やはり対面がよいか
- リモートは、ヒアリング調整が容易(特に海外等の遠隔地)⇒今後はリモートと対面を併用したハイブリッド型のヒアリングが普及するのだろう

  ⇒ 相手が言いたくない話を聞き出すためには対面、会社の上司や同僚に情報提供を知られたくない場合は自宅からのリモートなど、使い分け

調査・監査手法・・・資料精査

NISHIMURA & ASAHI

○ リモートでは、原本確認や実査ができない

※　三現主義（現地、現物、現実）。例えば、工場や倉庫が整然としているか。

○ 紙資料のPDF化（改ざんしやすい）、電子データも改ざんしやすい（プロパティの改ざんはツールがあれば簡単）

○ 預貯金の残高証明の改ざんは横領の典型的手段

○ 監査等では、画面上で原本の紙を映してもらう等の工夫、ただし限界あり

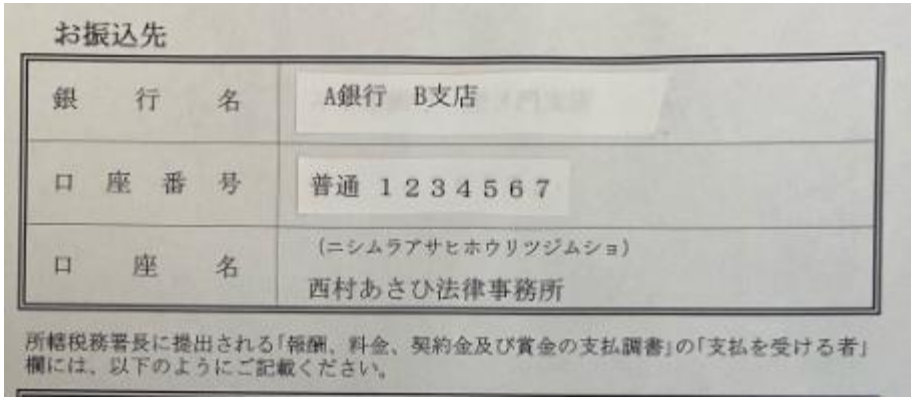
○ 原本確認が必須の文書かどうかの見極めが重要。契約書や発注書、検収書、残高証明など、取引相手方や銀行等の（との）文書で、その証明力に強く依存するものは、原本確認が原則必要と考えるのが無難

※　まずはPDF等を精査し、後日、少人数でPDF等と原本との照合をする手もある

○ 不正調査等で、オンライン・ストレージ・サービス(ベンダーが提供しているクラウド上でのファイル共有の仕組み）での文書共有が増えている

調査・監査手法・・・資料精査(続き)

NISHIMURA & ASAHI

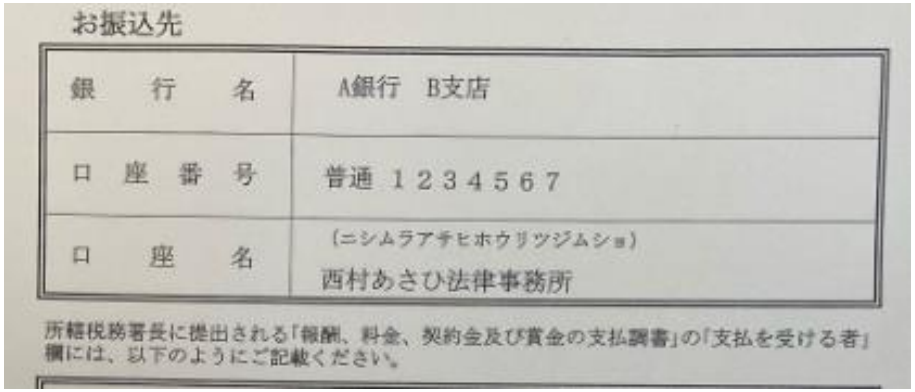


お振込先

銀　行　名	A銀行　B支店
口　座　番　号	普通　１２３４５６７
口　座　名	（ニシムラアサヒホウリツジムショ） 西村あさひ法律事務所

所轄税務署長に提出される「報酬、料金、契約金及び賞金の支払調書」の「支払を受ける者」欄には、以下のようにご記載ください。

① 原本に紙を貼って変造したもの

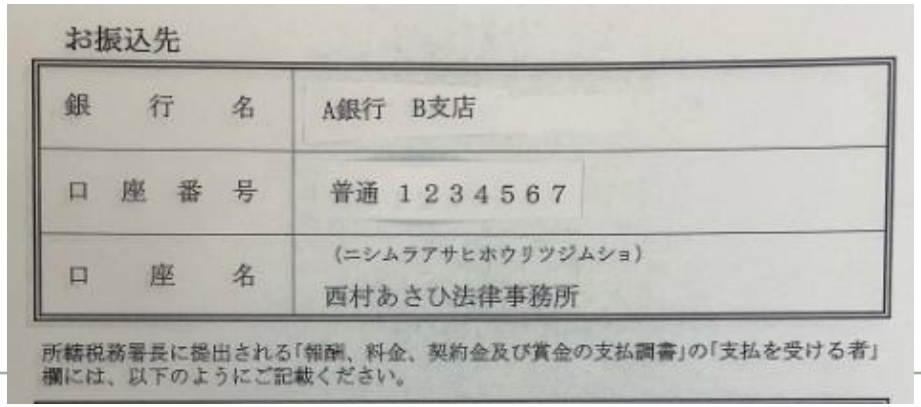


お振込先

銀　行　名	A銀行　B支店
口　座　番　号	普通　１２３４５６７
口　座　名	（ニシムラアサヒホウリツジムショ） 西村あさひ法律事務所

所轄税務署長に提出される「報酬、料金、契約金及び賞金の支払調書」の「支払を受ける者」欄には、以下のようにご記載ください。

② ①のカラーコピーをとったもの



お振込先

銀　行　名	A銀行　B支店
口　座　番　号	普通　１２３４５６７
口　座　名	（ニシムラアサヒホウリツジムショ） 西村あさひ法律事務所

所轄税務署長に提出される「報酬、料金、契約金及び賞金の支払調書」の「支払を受ける者」欄には、以下のようにご記載ください。

③ ②と比較して、やや雑なもの

調査・監査手法・・・実査・往査

NISHIMURA & ASAHI

○架空循環取引や、過大な棚卸し資産計上、在庫の不正横流しなどを防ぐには、実査が重要

※ 日本公認会計士協会「リモートワークに対応した提言・留意事項」の中のリモート棚卸立会の留意事項」、「PDF に変換された証憑の真正性に関する監査上の留意事項」等は有益

○リモートで実査できないと、上司等のダブルチェックといった社内牽制のみに異存することになり、脆弱化

○ウェブ会議の画面を通じた実査、比較的近隣の工場・営業所からのピンチヒッターによる実査など

※ ウェブ画面を通じて、抜き打ち実査を行うことも出来る

※ 将来は、ドローンを使ってリアルタイムの映像配信か

○海外の実査は、現地のスタッフ、監査法人等に依存

⇒ 本社からは、特に現地の体制面のチェックを重点的に（システム上の抜け穴、上位者チェック、職務分掌上の牽制不足、モニタリング不足等々）

調査・監査手法・・・実査・往査(続き)

NISHIMURA & ASAHI

○電子データ主体の監査＝グループ共通でクラウド上のストレージにファイル保管、データ形式・項目のグループ内での統一

※ 過大なPDF化の戒め

※ 海外案件では、欧州GDPRなど個人情報移転の越境規制にも注意

※ 中長期的には、監査等のIT・DX化・・・過去データの集積から異常取引（特定の相手方との取引の集中等、不正リスクシナリオ）の検知（機械学習など）、さらには常時・リアルタイムのモニタリングへ

○リモート監査の定着へ

物理的な移動時間等を気にしなくてよい、監査対象の拠点・部署をリアルよりも増やすことができる

実査・往査との適切な役割分担を今後検討していく必要

当たり前のことを当たり前に

NISHIMURA & ASAHI

- コロナやリモートは、不祥事リスクを高めるが、不祥事の内容や手口等は変わらない。
- 不祥事の防止等のためには、常日頃から当然行うべきことを遺漏なく実施し、随時、PDCAで見直していくことが重要
- 例えば
  - トップからの単純素朴なメッセージ・動機付けを繰り返す（顧客のため、隠さない、カルテル・贈賄等の違法行為による儲けは一切不要等々）
  - 企業規範、ポリシーの明示・・・インテグリティ、倫理
    ※　ハウ・ツーとしてのコンプライアンスから、組織文化・企業文化へ
  - 風通しの良い組織、コミュニケーション、意識調査アンケート等
  - 社内規程の整備（ルール・ベース、決裁等を通じたチェック）、職務分掌上の牽制の確保、適時の人事異動
  - 教育研修（トップメッセージやインテグリティ・倫理の強調、各企業にカスタマイズした具体例の提示、過去の思いを風化させない）
  - 内部監査の強化（キャリアパスの確立等）
  - 内部通報の適正な運用(通報者の秘匿、報復禁止、デュアル・レポーティング等)、グローバル内部通報制度

上場会社は、不祥事（重大な不正・不適切な行為等）を予防する取組みに際し、その実効性を高めるため本プリンシプルを活用することが期待される。この取組みに当たっては、経営陣、とりわけ経営トップによるリーダーシップの発揮が重要である。

［原則1］ 実を伴った実態把握

自社のコンプライアンスの状況を制度・実態の両面にわたり正確に把握する。明文の法令・ルールの遵守にとどまらず、取引先・顧客・従業員などステークホルダーへの誠実な対応や、広く社会規範を踏まえた業務運営の在り方にも着眼する。その際、社内慣習や業界慣行を無反省に所与のものとせず、また規範に対する社会的意識の変化にも鋭敏な感覚を持つ。

これらの実態把握の仕組みを持続的かつ自律的に機能させる。

［原則2］ 使命感に裏付けられた職責の全う

経営陣は、コンプライアンスにコミットし、その旨を継続的に発信し、コンプライアンス違反を誘発させないよう事業実態に即した経営目標の設定や業務遂行を行う。

監査機関及び監督機関は、自身が担う牽制機能の重要性を常に意識し、必要十分な情報収集と客観的な分析・評価に基づき、積極的に行動する。

これらが着実に実現するよう、適切な組織設計とリソース配分に配意する。

［原則3］ 双方向のコミュニケーション

現場と経営陣の間の双方向のコミュニケーションを充実させ、現場と経営陣がコンプライアンス意識を共有する。このためには、現場の声を束ねて経営陣に伝える等の役割を担う中間管理層の意識と行動が極めて重要である。

こうしたコミュニケーションの充実がコンプライアンス違反の早期発見に資する。

［原則4］ 不正の芽の察知と機敏な対処

コンプライアンス違反を早期に把握し、迅速に対処することで、それが重大な不祥事に発展することを未然に防止する。

早期発見と迅速な対処、それに続く業務改善まで、一連のサイクルを企業文化として定着させる。

［原則5］ グループ全体を貫く経営管理

グループ全体に行きわたる実効的な経営管理を行う。管理体制の構築に当たっては、自社グループの構造や特性に即して、各グループ会社の経営上の重要性や抱えるリスクの高低等を踏まえることが重要である。

特に海外子会社や買収子会社にはその特性に応じた実効性ある経営管理が求められる。

［原則6］ サプライチェーンを展望した責任感

業務委託先や仕入先・販売先などで問題が発生した場合においても、サプライチェーンにおける当事者としての役割を意識し、それに見合った責務を果たすよう努める。

（付録）テレワークの情報セキュリティ

企業のセキュリティインシデント

NISHIMURA & ASAHI

経路	攻撃やミスの一例
メール	メールアカウントの乗っ取り：脆弱なパスワードや使い回し
	詐欺メール、フィッシングメール：類似ドメイン、発信元偽装
	マルウェア(ウイルス)感染：Word、PDF等の添付ファイル、標的型攻撃
	送信ミス：宛先間違い、BCCの宛先をCCに入力、添付ファイル間違い
Webサイト	管理者アカウントの乗っ取り：脆弱なパスワードや使い回し
	Webサイト改ざん：閲覧者にマルウェア感染させる、悪意あるサイトへ遷移
	使用不能：DoS攻撃、DDoS攻撃
その他	SNSアカウント：乗っ取り(脆弱なパスワードや使い回し)、凍結、類似アカウントを作成してなりすまし
	ランサムウェア：マルウェア感染(ファイルの暗号化、公開するとの恐喝)
	VPNサーバの乗っ取り：脆弱性を攻撃、VPNサーバのユーザ乗っ取り
	ファイルの設定ミス：公開状態

内部不正

NISHIMURA & ASAHI

- セキュリティ・インシデントは、外部からの不正アクセスだけでなく、役職員による内部不正も等しく問題
- 役職員による情報の持ち出しや売却、腹いせのためデータ削除、転職時のお土産（転職先を利するためでなく、自己の業務上の便宜目的の場合も）等
  - 子会社の従業員が金欲しさから顧客のIDを使って電子ギフト券を不正に入手
  - 社長や会社の対応に不満があり、会社のパソコンに不正にアクセスし、全データを消去
- 退職者、短期アルバイト等、利用していない者のアカウント管理
  - 退職後もIDやパスワードの変更をしていなかったため、不正アクセスが可能になった事案
- 委託先管理、再委託先管理、再々委託先管理
- 廃棄するHDDの処理の問題

サイバーセキュリティ(内部不正対策を含む)

NISHIMURA & ASAHI

- ガイドライン・マニュアルの整備、役職員への周知・教育、内部監査による事後チェック等が基本
- システムの導入だけではセキュリティ対策の入口に過ぎない。究極の脆弱性は人であり、ソーシャル・ハッキング(ソーシャル・エンジニアリング)をシステムで防ぐことは困難
  ※ビジネスメール詐欺、Twitterでの著名人なりすまし事件等
- ネットワークセキュリティとID及びアクセス管理のセキュリティの仕組みを構築
- 実務的対策のポイント
  - データへのアクセス制限とアクセスログを取得する(誰が、いつ、何を等)
  - 侵入を防御することに注力しつつ、侵入を100%防ぐことは不可能と理解
  - 内部ネットワークへの侵入後であっても、検知・防御する方法・体制(外部へのデータ送信量のモニタリング等)を構築する
  - クラウドの構成・設定ミスは致命的なサイバー攻撃・データ漏えいにつながる
  - セキュリティに関する認証を取得、システム監査を受けたからと安心は禁物
    →サイバー攻撃を受けた場合に被害を最小化したり、被害経路、被害原因、被害状況等を完全に把握できる指標ではない
- 内閣サイバーセキュリティセンター(NISC)、独立行政法人情報処理推進機構(IPA)などの発信情報に注意

セキュリティリスクの増大

NISHIMURA & ASAHI

- テレワーク＝在宅勤務、サテライトオフィス勤務、モバイル勤務
- 情報漏洩リスク増大
  - ネット利用の増大、自宅のネット環境等の脆弱性
  - 業務用ではなく私物の端末を使用
  - マルウェアを含んだファイルのダウンロード等→社内システムにも侵入される（昨年等の防衛関連企業へのサイバー攻撃）
  - 図書館・喫茶店等での執務（無料Wi-Fiスポット等の脆弱性、資料置き忘れ、のぞき見等）
- VPN製品、ウェブ会議システム等における脆弱性（社団法人JPCERTコーディネーションセンター）
  - VPN製品の脆弱性の修正アップデートの確認など必要な対策例を示していたが、2020年8月、38社の日本企業でID・パスワードの漏洩等によるVPNへの不正アクセス
- ウェブ会議システムを利用する際に、カメラを通じて機密情報を含む書類等が映り込んでしまう、大声での電話会議で周囲に聞かれる
- 世界的にランサムウェア攻撃が蔓延（日本企業の工場、最近の米国では病院や教育委員会も）、またビジネスメール詐欺にも注意
- 事前の万全な対策＋事後の不正検知・早期対応

具体的な方策①

NISHIMURA & ASAHI

【総論】

○ テレワークに即したセキュリティポリシー及びルールの整備

○ 役職員への周知と注意喚起

✓ セキュリティ対策に関するメッセージを端末画面上に表示

✓ テレワーク勤務者が、出勤時に目をとめやすいところにポスターとして掲示

○ テレワークによるセキュリティインシデント発生に備え、あらかじめインシデント発生時の対処方法、連絡方法を定めて周知

【機器等のハードやソフトウェア】

○ テレワーク用にノートPC・タブレット等を配布

○ ノートPC・タブレット・スマートフォン等の紛失リスク→暗号化のほか、遠隔操作で端末内のデータを削除できるようにする

○ VPN（通信暗号化）やVDI（仮想デスクトップ）など

○ システムで用いるパスワードは他者から容易に推測されない堅牢なものとし、多要素認証が使用できる場合は活用する

○ OSやソフトウェア、アプリ、機器の脆弱性を確認したうえで、アップデートを自動化

○ アクセスログだけでなく、操作ログもとらないと追跡できない

具体的な方策②

NISHIMURA & ASAHI

【テレワーク可能な業務と情報の振り分け】

○ 業務用のデータについて、重要度に応じたレベル分け

○ テレワークによる利用可否、データの取扱い方法（端末へのダウンロード禁止、プリントアウト禁止など）を定める

・システムでは、画像リスク(スマホで撮影してSNSアップ）までは防ぐことができない

【個々の役職員レベル】

○ 許可を受けていないアプリケーションをインストールしない

○ ウイルス対策ソフトを常に最新の状態に保つ

○ 身に覚えない電子メールの添付ファイルを開封したり、URLをクリックしない

・業務を装ったメール、コロナをテーマにしたメール等に注意

○ ウェブ会議や電話会議の場所等に注意するよう周知

○ TwitterやInstagram等のSNSに投稿したテレワークの写真に、機密性の高い文書や業務情報が映り込む事例→テレワークの写真の掲載は禁止

【その他、総務省「テレワークセキュリティガイドライン」、内閣サイバーセキュリティセンター「テレワークを実施する際にセキュリティ上留意すべき点について」等を参照】

講師略歴等

NISHIMURA & ASAHI

木目田　裕(きめだ　ひろし)

西村あさひ法律事務所　弁護士

1991年東京大学法学部卒、1993年検事任官、東京地方検察庁特別捜査部、米国ノートルデイム・ロースクール客員研究員、法務省刑事局付、金融庁総務企画局企画課課長補佐等を経て、2002年8月より弁護士。2015年経済産業省「外国公務員贈賄の防止に関する研究会」委員、2021年現在 楽天証券株式会社、株式会社アドバンスクリエイトの各社外取締役、株式会社小糸製作所の社外監査役。

＜主な著作＞

『銀行等金融機関のコンプライアンス』(共著、経済法令研究会、2020年)、「企業不祥事の事後対応と監査役等の役割」(月刊監査役692号、2019年)、『危機管理法大全』(共著、商事法務、2016年)、『実務に効く　企業犯罪とコンプライアンス判例精選』(共同編集、有斐閣、2016年)、『インサイダー取引規制の実務(第2版)』(共著、商事法務、2014年)、『実例解説　企業不祥事対応－これだけは知っておきたい法律実務(第2版)』(共著、経団連出版、2014年)、『インサイダー取引規制と未然防止策～取引事例と平成25年改正を踏まえたポイント～』(共著、経済法令研究会、2014年)、『経済刑法 － 実務と理論』(共著、商事法務、2017年)、『コーポレートガバナンスと企業・産業の持続的成長』(共著、商事法務、2018年)、「日本版司法取引と企業の対応」(金融・商事判例1548号、2018年)、「日本版司法取引制度への実務対応 －平時の備えを中心に－」(共著、商事法務2167号、2018年)、「企業不祥事の現状と展望」(座談会録、ジュリスト1498号、2016年)、「米国クラスアクション(集団訴訟)の近時の動向と日本企業の対応」(共著、公正取引791号、2016年)、「外国公務員等への贈賄リスク － 経産省・贈賄防止指針の改訂を受けて」(座談会録、ジュリスト1488号、2016年)、「米国反トラスト法における日本企業が関わる刑事事件について」(公正取引777号、2015年)、「企業の危機管理と第三者委員会との間の緊張関係等」(商事法務2084号、2015年)等。

連絡先　：西村あさひ法律事務所
(〒100-8124　東京都千代田区大手町1-1-2　大手門タワー)
電話：03-6250-6405、FAX：03-6250-7200
電子メール：h.kimeda@nishimura.com