NEWSLETTER

近時の企業不祥事とコンプライアンスについて(その 2)

危機管理ニューズレター　　2024 年 7 月 31 日号

執筆者:
木目田 裕
h.kimeda@nishimura.com
宮本 聡
s.miyamoto@nishimura.com
西田 朝輝
a.nishida@nishimura.com
澤井 雅登
ma.sawai@nishimura.com
寺西 美由輝
m.teranishi@nishimura.com

目次

Ⅰ　近時の企業不祥事とコンプライアンスについて(その 2)

執筆者: 木目田 裕

本稿では、モラル違反、品質不正、サイバー攻撃、営業秘密持ち出しについて述べます。本稿は、危機管理ニューズレター2023 年 8 月 31 日号に掲載した拙稿「近時の企業不祥事とコンプライアンスについて(その 1)」の続編です。「その 1」もそうですが、これは、2023 年前半に私が行った講演の録音結果に手を入れたものです。

1. モラル違反

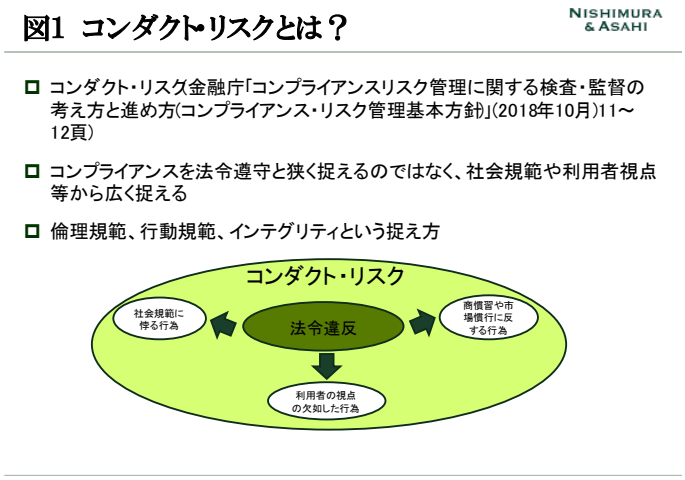
従来は、コンプライアンスや企業不祥事では、法令違反が中心とされていましたが、最近数年間では、具体的な法令違反がなくても、ある意味で「モラル」の違反があれば、それだけでも大きく問題とされることがあります。

ちょうど、コンプライアンスの文脈で、細かいルールも大事だが、それよりも、「顧客のため」や「インテグリティ」など、シンプルで役職員の心に刺さるメッセージが重要であると日本で言われ出したことと [1]、因果関係の有無は分かりませんが、軌を一にしているように思われます。

また、金融庁も、「コンプライアンスリスク管理に関する検査・監督の考え方と進め方(コンプライアンス・リスク管理基本方針)」(2018 年 10 月)ではじめて「コンダクト・リスク」という言葉を使うようになりました。コンダクト・リスクについては、図 1 のとおりです。

[1] 企業不祥事でモラル違反が特に注目を浴びるようになった時期よりも、シンプルで刺さるメッセージが注目されるようになった方が、時系列的には先行すると思われます。私なども、こうした点について最初に物を書くなどしたのは、2017 年 10 月 4 日付け日本経済新聞・朝刊の拙稿「不祥事を防ぐ組織風土追求を」あたりだと思います。

© Nishimura & Asahi 2024



法令違反ではなく、モラル違反が問題とされた事案ですが、例えば、2019 年に、ある証券会社が東証の市場再編の動向に関するいわゆる早耳情報(東証の有識者懇談会における時価総額基準等の検討状況)を外部の機関投資家だけに情報提供した、ということで、金融庁から業務改善命令を受けたケースがありました。これは、インサイダー取引があったというわけでもなく、また法令違反でもありませんが、一部の特定顧客の優遇であり、一般投資家から見て、資本市場の公正性・信頼を著しく損ないかねない、ということで、問題にされました。

これも 2019 年の事例ですが、就職情報会社による内定辞退率予測データ問題がありました。これは、就活生から個人情報利用の同意を得ていたものの(ただし、一部は同意なし)、そうした情報を使って、学生の内定辞退を予測して企業に販売するビジネスが倫理的に問題とされました。同意を取っていれば、当時の個人情報保護法上は問題ないわけですが、そうは言っても、学生自身に情報を提供させて内定辞退を予測してそれを売り込むと、その学生に不利益を与えるのではないか、ということで、ビジネスのモラルが問題とされた事案でした。

最近の事案でも、例えば、みなし公務員によるサイド・ビジネスのような事案で、職務関連性があったかどうか疑問の余地があるものの、贈収賄罪が問題とされている事案があります。これも、ある意味ではモラル違反という捉え方がされて、それに引きずられて刑事事件として摘発されたケースという見方もできるかもしれません。

当たり前のことではありますが、「法令を守っていればそれでよい」、「法令の形式的文言には合致する」は、決してコンプライアンスではありません。コンプライアンスの本質は「正しいことをしよう」にあります[2]。個々の法令等のルールの遵守とそのための研修や牽制・チェックの仕組みにとどまらず、表現の仕方は「インテグリティ」など企業によって様々だと思いますが、コンプライアンスの本質について、経営者からの日頃のメッセージやコンプライアンス基本方針・行動指針等を通じて役職員への浸透をはかり、そうした組織風土・組織文化を構築するとともに、モラルという観点からも自社のビジネス・モデルについて検証していく必要があります。

[2] 拙稿「危機管理及びコンプライアンスにおける本質は「正しいことをしよう」にあり」危機管理ニューズレター2024 年 4 月 30 日号参照。

© Nishimura & Asahi 2024

2. 品質不正問題[3]

（1） 品質不正が絶えない要因

本来、品質不正として大問題なのは、薬害、食中毒など人の死傷につながる製品役務の不具合や、不良建築など実害が発生し得るケースです。しかし、2017 年の大手製造業における品質不正事件を契機に、規格・認証の不適合や契約仕様の違反などがあれば、必ずしも実害に結びつかなくても、「品質不正」として厳しい批判を受けるようになったと思います。ここでは、人の死傷や不良建築などの実害をあまり伴わない、いわば B to B での品質不正(検査不正、認証不正という問題も含む)を主に念頭において論じます[4]。

こうした品質不正は、「性能に問題がない」といった正当化が働きやすいことから、引き続き発生(厳密には「発覚」)が相次いでいます。厳しく批判されたり、不正競争防止法違反(虚偽表示)で会社や役職員個人が罰金刑で処罰される等しているにもかかわらず、今日まで続いています。

なお、「性能に問題がない」といっても、品質不正の発覚後、顧客からは補償や代金の一部返還等を求められることもあります。また、顧客の製造ラインで支障が生じることもあります。だから、実際問題としては、「性能に問題ない」とは必ずしも言えないのですが、問題なのは、こうした正当化が働きやすいという点にあります。

ア　正当化

品質不正が長期間にわたって続いたり、発覚しない理由のうち大きな理由は、どうしても不正に対する正当化が働きやすい、ということです。

例えば、顧客の要求仕様を満たさないスペックの製品を出荷したというケースでは、「性能に問題ない。顧客の要求仕様が無用にハイスペックなだけ。だから出荷しても問題ない」という正当化がよくあります。実際、性能に基本的には問題ないことも多いので、こうした正当化への対処はなかなか難しいものがあります。

自社の出荷基準・検査基準を満たさない製品を出荷した、というケースでも同じように、「自社の出荷基準や検査基準が高すぎる。性能に問題ないのだから、基準に未達でも、納期が逼迫していて、納期に間に合わないとお客さんに迷惑をかけてしまうから、このまま出荷した」という正当化がよくあります。製品の規格や認証では、認証の取得の際に申請した設計や材料とは違う製品を作って、認証品として出荷するパターンがあります。これまた同じような話で、「性能に問題ない。収益計画上、早く認証を取得して製品化したい」という正当化です。検査の一部省略というケースでも、「開発案件の試験や出荷段階の別の検査でカバーできているので、この検査はしなくてもよい。納期も逼迫していて、検査設備も足りないから、実質的に問題ないのだから出荷してしまおう」という話になります。

こうした正当化をいかに防いでいくか、あるいは正当化があったとしても、品質不正が起きないよう

---

[3] 品質不正問題については、拙稿「品質不正の防止に向けて」危機管理ニューズレター2024 年 6 月 28 日号もご参照ください。

[4] 本稿に記載した原因や再発防止策は、実害がある品質不正についても当てはまるところが少なくありませんが、実害がある品質不正では、性能や安全への軽視が主な問題であり、この点にどのように対処すべきかが重要なポイントになります。他方、実害があまりない B to B での品質不正では、一般的には、性能や安全への軽視が問題なのではなく、むしろ、性能に問題ない等との正当化を背景にした、顧客説明や、手続軽視、契約軽視等といった点が問題になります。そのため、本文記載のとおりの限定した範囲で論じています。もちろん、実害の有無といっても、その差異は相対的なものであり、ヒヤリハットやハインリッヒの法則が指摘するとおり、性能に問題ない等の正当化による手続軽視が将来における実害のある品質不正を招来し得るという点で、連続している問題ではあります。

© Nishimura & Asahi 2024

な仕組みや牽制チェックはどうしたらよいかを考えていく必要があります[5]。

イ　手続やプロセスによる品質の証明という発想の馴染みにくさ

いくつかの品質不正案件で、いろいろな方のお話を実際に聞いて思うところなのですが、みなさん、自分の会社の品質やものづくりに自信があります。うちの製品は、物はいい、お客さんからも信頼されて任されている、と思っていますが、その反面として、検査やプロセスで顧客に品質を証明するという発想が馴染みにくいことがあります。契約等で要求されている検査を行って検査結果で品質を証明する、そうしたプロセスで品質を証明すると言っても、そんなことをしなくても物さえよければ大丈夫だ、という具合です。専門家の方からお聞きした話ですが、この点は欧米企業と違う、日本企業の特徴だという説があるそうです。欧米、特に米国の企業はあまり従業員を信用してないから、手続やプロセスで品質を証明しないといけないという発想に馴染んでいるが、他方、日本企業は、自信があるだけに、そうした発想に乏しいのではないか、ということです。こうしたステレオタイプな特徴論が実態にどの程度合致するかは実証的な検討が必要ですが、一理はあるのかもしれません。

それから、ISO などいろいろな国際規格や認証について、やや極端な言い方をしますが、ある意味で外圧的に受け止められている面もあって、例えば「外国で物を売るために必要とされてしまったから、やむなく規格を取っているが、うちの製品はそのような規格や認証よりはるかに性能はよい」、「規格や認証は外国で物を売るためのパスポート(あるいは国内で物を売るための通行手形)みたいなものにすぎない」等といった捉え方です。そうすると、製品化時期が迫ってきたり、納期の逼迫などがありますと、規格や認証を完全には充足していない場合でも、「物は規格や認証よりも優れているのだから」という正当化が生じやすくなります。

その意味で、検査にせよ、規格や認証にせよ、手続やプロセスで品質を証明するという発想を根付かせることは、正当化を防止するためにも必要なのだと思います。

ウ　設計・開発部門の重視と検査・品管部門の軽視

設計や開発部門が重視され、検査部門(ここでは、品質管理部門を含む趣旨で「検査部門」と言います。)が軽視されがち、という実態も一部にあるようです。極端な言い方になりますが、設計・開発の役職員の中には、ときに、品質上の問題点等について検査に話しても検査は理解できないだろう等といった意識もないではなく、設計・開発が検査を信頼していない面もあったりしますし、会社や工場等で出世するのは大概が設計・開発の人というケースも多いと思われます。そうした関係性の中で、検査が顧客仕様を満たさない検査データを設計・開発に示して、スペック変更を求めても、設計・開発からは、検査方法や条件設定に問題があるのであって、設計変更は不要と突き返されたり、あるいは、設計・開発や製作の過程で手戻り等が想定を超えて発生することで工程遅延を招くと、最後の工程は検査なので、「それなら検査を省略してしまえ」等となって、品質不正という問題に至ることもあります。

その一方で、会社や工場によっては、設計・開発、製作、検査の間で人事異動をする等の工夫をすることで、縦割りや壁、サイロ化を取り除こうとしているところもありますが、それはそれで、今度は、お互いに各自の事情や悩みが分かるものですから、検査(特に、出荷停止権限を持つ品質管理部門)による牽制が働かなくなってしまうこともあって、実に、こうした組織間の協力と牽制という相反性のある

---

[5] 正当化との関係では、日本企業の過剰スペック体質という問題もときどき指摘されます。いろいろな理由から、社内の出荷基準、検査基準が、お客さんと握ったスペックよりも高く設置されている場合がありますが、そこまで高い基準にする必要が本当にあるのか、という問題です。無用に高い基準に設定してあると、かえって守らなくてよい、という正当化につながります。

© Nishimura & Asahi 2024

問題は、対応に一律の正解はありません。
　また、検査軽視という点からは、検査設備への設備投資が後回しにされがちであって、それが検査設備の質ないし量からの能力不足となって、検査省略等といった品質不正を招くこともあります。

エ　非コア業務や子会社・関連会社
　品質不正に限りませんが、不祥事というのは、非コア業務や子会社・関連会社で発生することが少なくありません。非コア業務や子会社・関連会社ですと、どうしても単独業務だったり、手作業依存が大きい、担当者が長期間にわたり固定している等ということで、品質不正などの問題が、本社やコア業務に比べると、起こりやすいと思います。コンプライアンスに熱心な企業が本社で一生懸命に旗を振っても、本社から組織や人事という面で距離が離れている現場となると、なかなか、本社の思いは届かないという現実があるように思います。

オ　先輩や上司との仲間意識
　品質不正問題で問題に関わっていた役職員の方をヒアリングすると、よく出てくる話なのですが、「不正だと分かっていたのに、どうして今まで声をあげなかったんですか。内部通報や内部監査などの機会もあったのに」と聞くと、多くの方が「先輩や上司もやってきたこと、先輩や上司から教わってきたことです。それなのに、自分だけが声をあげて、いい子になることはできません。先輩や上司を売ることはできません」と答えます。私なども気持ちはものすごく良く分かるところなのですが、そうは言っても、こういった点をどうにかしないと、品質不正問題の早期解明や根絶は難しいと思います。

カ　顧客説明の回避
　品質不正問題について、声をあげて対応することの手間や負担、軋轢等から声をあげない、という問題もあります。品質の問題が見つかりましたとなれば、上司に説明して上司の決裁を取った上で、お客さんに説明しに行かないといけない、となります。上司は「もっと別の方法で検査すれば、仕様を達成できるんじゃないのか」などと言ってきて、もう 1 回検査して来いとなるかもしれません。そのほかにも上司からはいろいろな説明や資料を求められるでしょう。ようやく上司をクリアしました。そしたら、次はお客さんです。品質不正がありましたと顧客に話す際の心理的な負荷を頑張って乗り越えて、顧客に説明しました。顧客からは、「その製品について性能に問題ないことは分かったけれども、他の製品はどうなんですか。過去に納品してきた製品はどうなんですか」等々と質問や資料・データの要求が相次ぎます。顧客の担当者も自分の上司に説明が必要ですから、これは当たり前のことです。そんなことで、勇気を振り絞って声をあげても、上司や顧客への説明や資料作りで、心理的負荷どころか、物量的にも大きな負担を負うことになって、残業続き、休日出勤の連続となりかねません。こうした顧客や上司への説明負担の回避も、声があがらない大きな要因の 1 つです。

キ　現場では何が不正か理解されていないこと
　品質不正の問題について、現場では何が不正か、理解されていないことがあります。従業員の方にアンケートを取ったり、ヒアリングをする時などに、「品質不正がありましたか」などと聞いても、なかなか答えは返ってきませんが、「実際のものとは違う部品や材料を使うことにしたり、あるいは実際とは違う図面で、認証を取得したことがありますか？」などと、具体的かつなるべく価値ニュートラルな聞き方で聞くと、「問題はないと思っていますが、こういうことがありました」などと答えが返ってくることがあります。

© Nishimura & Asahi 2024

そのほか、質問するなら、例えば、「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ことがありますか」、「決められている手順を省略したり、順番を変えて製作したことがありますか」、「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作したことがありますか」、「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ことはありますか」などと聞く方がよいと思います。

前述した正当化という問題もありますが、そもそも、従業員の方は入社して、あるいは配属されて、先輩に教わって仕事を覚えてきているわけで、先輩から教わったやり方に従って、不正の意識とか罪悪感などはあまり抱かずに仕事をしてきたというパターンがむしろ一般的です。ですので、品質不正があったのかと質問しても出てこないのです。

このように、正当化も含め、現場ではあまり不正とか悪いと思ってやっていない、そのために品質不正は起きやすく、長く続きやすいのです。

ク　その他

そのほか品質不正が絶えない原因としては、内部監査や品質監査等の監査機能が重視されていない、技術力・開発力不足の場合もある(規格・認証や法規制等が改正された場合に、改正内容を充足する製品をタイムリーに開発できないなど)といった点があります。

(2)　品質不正の防止・早期発見

ア　機会の防止

品質不正の機会を防ぐために牽制チェックを働かせることです。牽制チェックが正当化への対処にもなります[6]。具体的には、例えば、業務過程において、1人に依存することなく、別の者によるチェックが入るようにすること(職務分離)、マニュアル処理をできるだけ排除して、検査等の自動化・データ保存をすること(証跡保存、見える化)、品質監査ではインからアウトまで(顧客仕様から作業規程、検査成績書・出荷試験等まで)記録や実データを突合して見ていくこと、定期的な人事異動を活性化することなどが考えられます。

イ　正当化の防止

正当化を防ぐための手法や着眼点ですが、過剰な出荷基準や過度な収益目標、過度なノルマといったものがあると正当化が生まれやすくなるので、そうした過剰な基準や目標等は見直していくことが必要です。

そもそも、冒頭でも述べましたが、「性能に問題はない」といった正当化自体が正しいのか、顧客の立場に立って役職員に考え直してもらう必要もあります。

正当化を防ぐには、経営から常にメッセージを送ったり、日頃の OJT や教育を通じて、個々の役職員の意識を変えていくことも必要です。どのように意識を変えていくのか、ですが、独りよがりに「物さえよければいいんだ」ではなく、「手続やプロセスで品質を証明する」という意識づけをしていく。他社の品質不正の事例などを素材にした教育も役に立つでしょう。

規格や認証についても、単に外圧だと思うのではなく、検査やフォローアップ・サービスの機会を有効活用しようと発想の転換をする。なお、作業の意味合いや目的が分かっていないために、役職員が本

6　この点、拙稿「企業不祥事の防止―機会の防止の重要性」危機管理ニューズレター2022 年 11 月 30 日号もご参照ください。

© Nishimura & Asahi 2024

来必要もない検査結果の書き換えなどを行って不正が起きることもあるので、作業の意味や目的の教育も重要です。

実質的に性能は問題ない、お客さんから信頼されて任されているといった正当化との関係では、ヒアリング等でそう仰る方に「それなら、どうしてお客さんにそう説明しなかったのですか。お客さんに話して了解を取っておけば問題なかったはずでは？」と聞くと、皆さん、答えに窮するわけです。結局、そうした正当化をしていても、実際は顧客に説明できなかったわけです。顧客に胸をはって堂々と言えないことは、やはり間違っているのです。そうした認識をもってもらうことが大事です。

似たような話として、品質不正に限らず、様々な不祥事で「会社のため」だったという正当化もよく聞きますが、本当の意味での「会社のため」は、問題があったら声をあげることであって、それを役職員の皆さんには分かって頂きたいところです。「あいつは正論ばかり言っていて･･･」などと言っているような組織ではダメなわけです。

ウ　後任者の気づきの奨励

教育や意識喚起という観点では、役職員をして、人事異動時や前任者からの引継ぎ時に意識をもってもらうことが大事です。品質不正に限らず、横領や独禁法違反などのケースでも等しく当てはまりますが、異動があって、後任者が前任者の仕事のやり方に疑問をもって、不正が判明するというケースは多く見られます。だから、前任者からの引継ぎの時に、後任者において、前任者の仕事を何の疑問もなしに盲従するのではなく、どこかに問題はないか、間違っているところはないかといった目で見ていくことが大切です。

エ　全員参加で品質不正問題に取り組む必要性

品質不正の問題があった企業における再発防止策という観点からは、工場の全員が一体となって品質問題に取り組んでいくことが重要です。例えば、過去に、ある事業拠点で品質不正問題があって、全社を挙げて再発防止の取組をしたが、その際には問題を掘り起こし切れておらず、今回、別の拠点で別の品質不正問題が発覚したといったケースがあるとします。ヒアリングなどで「以前の問題のとき、会社は再発防止策として、いろいろな取組をしていたのに、何故、その時に対応しなかったのですか」と聞くと、「当時、それは品質部門がやっていたことで、私は担当ではなかったので、あまり意識していませんでした」といった回答が返ってくることもあります。当否はともあれ、本社や工場等の品質部門の取組に対し、現場の多くの方が自分とは関係ないと距離をおいてしまうこともないではなく、そうなると、なかなか足元の問題を取り上げようとしない、改善しようとしない、その結果として不正が続く、となります。理想論かもしれませんが、組織横断的に PT を作るなど、工場の全員が一体となって全員参加で対応していくことができる体制や環境を整備することが大事です。

オ　品質部門の独立性確保・強化

牽制・チェックを強化するために、品質部門の独立性の確保・強化も重要です。

指揮命令系統や人事評価ですが、工場内の「工場長⇒品質管理部長・品質保証部長」という縦のラインだけでなく、本社の品質部門からも工場の品質部門を直接指揮監督し、人事評価なども行う仕組みは検討に値します。工場長からの工場の中だけの指揮命令系統ですと、設計や開発が優位ですし、工場自体の採算性の問題もあるから、品質部門に出荷停止権限があると言っても、納期逼迫の場合など、問題があっても、工場長の意向や工場の中の何となくの空気に抵抗して、出荷停止だとは言いにくい場合もあります。品質部門が自信を持って出荷停止と言えるようにするために、指揮命令系統や人事評価は工場

© Nishimura & Asahi 2024

長だけでなく、本社の品質部門とつなげることも、一つの方法としてはあります。
　また、工場内の人事異動のパターンを牽制・チェックの観点から見直すことも必要です。設計・開発、製作、検査の間で、総合に人事交流をすることにも大いに利点はありますが、先ほども述べたように、相手の事情が分かると、品質部門がきついことを言いにくくなって牽制・チェックが働きにくくなることもあります。
　それと、人材や設備投資の点で品質部門を軽視していないかどうかの検証は大事であり、企業内で、あるいは業界で、品質保証や品質管理の専門家を育成していくこともできるとよいと思います。
　特に、検査設備の更新や増強などの「守りの」設備投資は、採算性向上に直ちに結びつくものではないとのイメージがあるので(そのイメージ自体がそもそも間違っていると私も思いますが)、数字に責任を持っている事業部門や事業拠点では、先送りしがちになります。だから、こうした「守りの」設備投資こそ、経営トップなどの経営陣が率先して予算を配賦するなどしていくべきであり、まさに経営者の「経営判断」が求められるところです。

カ　上司・同僚に相談しやすくする、声をあげやすくする(心理的安全性)
　品質不正事案では、上司にあげて顧客と相談しておけば何の問題もなかった事案が多いと思います。実際、性能は良い、顧客の要求仕様や自社の出荷基準がハイスペック過ぎた、といったことで、品質不正問題の発生後、顧客に丁寧に説明して回ったら、顧客から今回は特採(トクサイ)でよいと言われて、補修や損害賠償・補償といった問題にならずに済んだり、あるいは、顧客も受入検査でスペックが仕様に足りないのを分かっていたので何も問題なしで終わったり、ということは珍しくありません。もっとも、それだけに正当化が生じやすい、という面もあって悩ましいのですが・・・。
　このように、もっと早く上司に相談して、顧客に説明しておけば、品質不正などという問題にならずに済んだ、というケースが多いのです。
　ただ、残念ながら、先ほど申し上げたように、声をあげること、上司や顧客に相談することの物理的・心理的負担から、声があがらないで、品質不正という問題になってしまう。対応負担の重さや心理的負担だけでなく、先輩・同僚に迷惑をかける、職場で孤立するかもしれない等々があって、声があがらない。
　そこで、最近のはやり言葉ですが、「心理的安全性」を確保して、問題があったら声をあげやすくすることが非常に重要になってくるわけです。
　では、その「心理的安全性」をどうやって確保するのか、声をあげやすい組織風土・組織文化を作るには、どうしたらよいのか、これが実際には難しいのです。「心理的安全性」と言葉で言うのは簡単ですが、これがなかなか正解はありません。
　組織風土・組織文化というのは、先輩や上司が長い年月をかけて作ってきたものであり、会社というのは、やはり、社長など経営者の言動に役職員は注目します。いくら心理的安全性と言っても、経営者が、部下の問題指摘を突っ返していたら、役職員は誰も「なんだ、心理的安全性なんて、ただの建前か。うちの会社は、やはり、物言えば口寒し、だな。」なんていうことになってしまいます。だから、まずは、経営者がメッセージを繰り返し、自らの言動でもって、部下が相談しやすい雰囲気を作っていかなければなりません。
　では、心理的安全性を高めるために、もっと具体的な方法はないのかですが、一つには、声をあげた人に対する、周囲のサポート体制です。上司に声をあげたはいいが、上司からは「そんな問題があったのか。ありがとう。君の方で検討して対策を作ってくれ」と言われ、結局、ボールが自分たちに(自分だけに)戻ってくる。自分一人(あるいは少数の担当者)で問題を抱えこんで、残業や土日出勤の連続で、資

© Nishimura & Asahi 2024

料をまとめて、何度も上司から指摘を受けては資料を作り直し、やっとお客さんのところに説明に行って、今度はお客さんから「あれはどうなっている。これはどうなっている」となるようでは、馬鹿らしくて声をあげようともしなくなります。だから、原因究明・是正措置にしろ、顧客説明にしろ、声をあげた人に対する組織やチームでのサポート態勢を作ること(あるいは、声をあげた人に対応責任を負担させないこと)、そうしたサポート体制があることを社内に十分に周知して、まさに安心を醸成することが大切になります。

また、解決策の提示を直ちに求めないなど、声をあげやすくするための中間管理職の意識改革も必要です。日本企業に特有なのかどうか分かりませんが、会社でも官庁でも、責任感の強い人ほど、上司に問題点を相談するに際して、解決策も検討しないで、ただ「問題がありました。どうしましょう」というだけの話を上司にあげるのは、部下としてどうなのか、という意識があります。解決策を持っていかないと、上司に相談できない、と思って、そのために報告や対応が遅れてしまい、そのうち別の緊急案件が生じて放置されてしまい、品質不正が続く。まずは声をあげてもらうことが大事なので、中間管理職も、問題点の報告があったら解決策の提示を直ちに求めないようにする、むしろサポート体制をきちんと作る、その方がはるかに大事です。「問題がある」と言いっぱなしにするだけでよいのです。中間管理職だけでなく、担当も含めて社員の意識をこのように変えていかないと、なかなか声はあがりにくいと思います。

中間管理職といえば、どの会社でも、業務の効率化や所管範囲の拡大、新規業務の発生などにより、中間管理職が昔より、はるかに忙しくなっている、という話を聞きます。そのため、課長なのに工場の現場に足を運ぶ頻度が少なくなっている、部下が上司に相談しようにも上司が「忙しいオーラ」を出していて相談できない、中間管理職の機能不全が品質不正の一因ではないか、といった話を聞きます。簡単に中間管理職を増やすわけにもいかないのでしょうが、それでも、IT 技術なども駆使しつつ、中間管理職が本当に「管理」できるように組織を見直すことも、理想論かもしれませんが、検討が必要だと思います。

それと「先輩同僚に迷惑をかけるから今まで言えなかった」という話も結構多いのですが、そういう方に「先輩や同僚が大事なのも分かりますが、問題解決を先送りすれば、後輩に、どえらい迷惑をかけることになると思いませんでしたか」と聞くと、「確かに後輩のことを思って、もっと早く声をあげるべきでしたね」となります。後輩に迷惑をかけるという発想を日頃の教育等で訴えることも一つの方法だと思われるところです。

キ　継続的な取組の必要性(品質不正あぶり出しのための第三者窓口による顕名アンケートの定期的実施プラス社内リニエンシーなど)

品質不正を完全に発見したり防止したりするのは現実的には難しいと思います。中には、品質不正問題での調査委員会の調査中に、新しい品質不正が始まったりもします。だから、継続的に、不正を防止したりあぶり出したりするための努力を続けていく必要があります。

この観点からは、品質不正あぶり出しのための第三者窓口による顕名アンケートの定期的実施(状況に応じて、社内リニエンシーなども組み合わせること)が考えられます。

具体的には、3 年ごと、5 年ごとなどに、本社・グループ会社の役職員を対象に、(品質)不正等に関する情報提供や自主申告を促すアンケートを、匿名回答ではなく、顕名の回答という方式で行います。匿名ですと、回答があっても回答者により詳細な情報提供を求めることができず、その後の調査に支障があることが少なくないため、顕名回答にしますが、そうすると役職員が情報提供や申告を躊躇する懸念があるので、回答は、外部の弁護士事務所など第三者に対して行うこととし、その第三者窓口は、氏

© Nishimura & Asahi 2024

名その他回答者の特定に結びつく情報は、回答者の明示の承諾がない限り、会社側に一切伝えないこととして、それを役職員に事前に告知した上で、顕名回答でのアンケートを行います。

もちろん、こうしたアンケート自体は、外部の弁護士事務所等が担当している外部の内部通報窓口が主体で行って、顕名での回答も外部の通報窓口に対して行うこととしても、構いません。「品質不正あぶり出しのための第三者窓口による・・・」とする趣旨は、役職員に対して、特別で重要なアンケートであり、(毎年の恒常的なアンケートとは異なり、)必ず真摯に回答しなければならないものだと強く認識してもらうために、特別感・非常時感を出すための言い方に過ぎません。

社内リニエンシーというのは、要は、違法不当な行為を発覚前に自主的に申告(つまり「自首」です)したら、懲戒処分を一切しない、あるいは一段階、二段階引き下げると、事前に予告して、自主的申告を促すものです。私どもの経験上、必要的減免型の社内リニエンシー付きで(「必要的減免」というのは、自主的申告があれば、必ず懲戒処分を減免する、と約束して行うものです。つまり、「減免できる」という会社の裁量型ではなく、「減免する(しなければならない)」と役職員に約束するものです)、こうしたアンケートを行うのは、品質不正に限らず、違法行為の自主的な申告を促す上で、効果的です。

ただし、効果的な反面、社内リニエンシーには、モラルハザード問題もあります。例えば、上司の指示で部下が不正を行っていたとします。上司が自主的に申告して、必要的減免で上司は懲戒処分を一切受けず(あるいは、本来、懲戒解雇のところ、減給で済むなど)、部下は懲戒解雇になる、というのは、どうなのか、ということです。そのため、社内リニエンシーを導入するにしても、必要的減免型を常設の制度として設ける例は、ほとんどないと思います。他方、就業規則等で、自主的申告であれば、会社は懲戒処分を減免「できる」とする例は数多く見られるところであり、そもそも、懲戒処分の要否等を判断する上で総合考慮すべき事情の一つとして自主的申告や調査協力を斟酌することは当たり前のことなので、裁量型は、役職員に対するアピール効果を別にすれば、本来は「社内リニエンシー」と呼ぶ必要もないものではあります。

この点、3 年ごと、5 年ごとに行うものであれば、そのアンケートのときに限定して、必要的減免型の社内リニエンシーをつけて行っても、モラルハザードなどの弊害はそれほど気にしなくても大丈夫だと思われます。なお、社内リニエンシーを行うときには、同時に、「今回のアンケートで自主的に申告しないで、他の役職員のアンケート回答や後日の会社の調査で不正が判明した場合には、懲戒解雇を含む重い懲戒処分を行う」旨をセットで告知することも重要です。

そのほか、継続的取組という点では、品質不正などの大きな事件が発覚した日や会社が起訴された日などの特定の日を選んで、「コンプライアンスの日」などと銘打ち、全社をあげて、毎年、その日に、事件を風化させず、全役職員がコンプライアンスを再確認する取組を行っている会社もあります。

3. 情報セキュリティ・サイバー攻撃

(1) サイバー攻撃等の典型例

サイバー攻撃や情報セキュリティ・ミスの典型例としては、例えば、次のようなものがあります。

- メールアカウントの乗っ取り(脆弱なパスワードやパスワードの使い回しが特に問題、ダークウェブで他人のパスワードの売買などもある)
- 詐欺メール、フィッシングメール(類似ドメイン使用、発信元偽装など巧妙)
- メール送付による標的型攻撃を通じたマルウェア感染(添付ファイルを開かない)
- メール送信ミス(宛先間違い、BCC の宛先を CC に入力、添付ファイル間違い等)
- Web サイトの管理者アカウントの乗っ取り(脆弱なパスワードやパスワードの使い回し)

© Nishimura & Asahi 2024

- 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させる等)
- Web サイト使用不能(DoS 攻撃、DDoS 攻撃等)
- SNS アカウントの乗っ取り(脆弱なパスワードやパスワードの使い回し)、SNS アカウントの凍結、類似アカウントを作成してなりすまし
- ランサムウェア攻撃(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等による)
- ファイルの設定ミスによるデータのネットへの公開状態・アクセスフリー

そのほか、実際のインシデントの相当部分は、実は外部からの攻撃ではなく、役職員による内部不正です。例えば、職員による情報の持出しや売却、腹いせのためのデータ削除、転職時のお土産(転職先を利するために限らず、自己の業務上の便宜目的の場合もある)などです。外部も大事ですが、内部についても決して注意を怠らないということです。

(2)　テレワーク・リモートワーク(以下では一括して「在宅勤務」と言います。)対応

在宅勤務との関係で、自宅等のネット環境の脆弱性、私物の端末の使用、図書館・喫茶店等の公衆の場所における脆弱性等に起因して、情報漏洩リスクが増大しています。どの企業も、こうしたリスクに対応して、公衆 LAN への接続や私物端末の私用禁止など、情報セキュリティに係る社内ルールやハード面での対応を見直しているところですが、悩ましいのは画像リスクです。

まず、図書館や喫茶店、列車・電車等で PC 等の端末を使うと、隣の席の人や後ろにいる人等から画面をのぞき見られ、場合によってはスマホで画面を撮影されてしまいます。この対策としては、こうした場所での端末使用を禁止することや端末の画面のフィルムを貼って真正面から以外の角度では画面を見られないようにすること等があります。

より悩ましいのは、在宅勤務での内部不正対策です。「自宅から社員が会社のサーバーにアクセスして個人データにアクセスするが、社員の端末 PC にはデータは保存できないようにしてあります。だから、個人情報は大丈夫です」というわけにはいかなくて、その場合でも、端末に表示された個人情報を役職員が私用スマホで撮影するということはあり得ます。例えばコールセンター業務などでは、オフィスの執務場所への私用スマホの持ち込みは禁止して、勤務中はロッカーか何かに保管しておくという対応が通常と思いますが、在宅勤務ですと、こうした対応をとることもできません。もちろん、画像リスクといっても、昔から手書きでメモして情報を持ち出すという例はありましたが、スマホで撮影となると、手軽にかつ大量の情報を持ち出すことが可能になります。業務の効率性を念頭に置きつつも、リスクの高低に応じて、在宅勤務で、どのような情報へのアクセスを可能にするのかの振り分けなどを行っていく必要があります。

(3)　ビジネスメール詐欺

ビジネスメール詐欺が在宅勤務の普及で増えています。ハッカーが、お客さんや自分の会社の社長や財務担当などのメール・アカウントを不正に乗っ取って、お客さんや社長等の振りをしてメールを送ってきます。例えば、この取引の代金は(いつもとは違う)この銀行口座に払って欲しいというメールを送ってきます。言われたとおりにお金を銀行に振り込んで、お金をだまし取られる。これがビジネスメール詐欺です。最近も、数百万ドルといったレベルで著名企業の米国子会社が被害に遭っていたと報道されていました。被害に気づいても、1日、2日経っていると、お金は複数の銀行口座の間を転々と送金されて東欧等で出金されていたり、暗号資産にされていて所在を追跡できない、となります。

こうした被害を防ぐには、仕事の基本に忠実に対応することです。メール一本で、すぐにそのとおりに行動するから、こうした被害に遭うわけでして、本来は、お客さんに電話して、「送金指定先が当社で登録され

© Nishimura & Asahi 2024

ている銀行口座と違いますが、大丈夫ですか。何かの間違いではないですか」と、電話 1 本すればいいのです。社長や役員についても同様で、財務経理の担当に確認するなど、確認方法はいくらでもあるわけです。

それと、昨今は、経済安全保障の観点で、基幹インフラへのサイバー攻撃への対処等に注目が集まっています。この点については今後政府の動向などを注視していく必要があります。

（4） ランサムウェア攻撃

ランサムウェア攻撃では、ハッカーが会社のシステムに侵入して、システムの全体又は一部を暗号化して使えなくします。暗号化を解除して欲しかったら、暗号資産等で金を払えと会社に要求します。つまり、システムを人質に取って身代金を払えと要求するわけです。ハッカーは、会社に身代金を払わせるために、システムに不正アクセスして盗み出した個人情報や営業秘密、技術上の秘密をいわゆるダークウェブで公開する、それが嫌なら身代金を払え等と脅迫してくること(二重の脅迫)もあります。さらに、被害企業だけでなく、その顧客や取引先もハッカーから情報をダークウェブで売る等の脅迫を受ける場合(三重の脅迫)もあります。

最近までは、日本企業の場合は日本語の壁に守られていました。多くの欧米企業が被害に遭う中で、日本企業は、ここ2、3年ぐらい前までは、海外拠点を別にすれば、ほとんど被害に遭ってきませんでした。しかし、最近は日本の病院に対するランサムウェア攻撃なども報道されていましたが、ハッカーは既に日本語の壁も超えてしまったと考えられています。翻訳ソフトや AI の進歩なども背景にあるのでしょう。日本企業のランサムウェア被害が増えつつあります。

ランサムウェア攻撃では、システム復旧や個人情報等の回収のために、ハッカーに身代金を払うかどうかが問題になります。身代金支払いに応じるかどうかは経営判断の問題ですが、蛇の目ミシン事件(最判平成18 年 4 月 10 日民集第 60 巻 4 号 1273 頁)に注意する必要があります。蛇の目ミシン事件では、取締役が脅迫されて会社からお金を払ったことが善管注意義務違反であるとして、取締役個人の損害賠償義務が認定されています。ランサムウェア攻撃に対する身代金支払いについても同様に取締役の善管注意義務違反が問われる可能性があります。米国では、自治体、企業、病院等は費用対効果で割り切ってハッカーに身代金を払っていたようですが、米国でも、2、3 年くらい前から身代金支払いがランサムウェア攻撃を助長するので、払うべきでないという声が強まっています。また、身代金が北朝鮮など米国の制裁対象国に流れているとして米国政府から経済制裁規制違反に問われるリスクもあります。身代金を払う際にはハッカー側と金額の減額や段取りを交渉するのが常とはいえ、本当にハッカーが約束を守ってシステム暗号化を完全に解除するか(マルウェアを仕込ませていないか)等の問題もあります。

そのような次第なので、日本企業の現在の趨勢は、単なる費用対効果では、そうそうは身代金を払わない、ということだと思います。身代金を払うのは、病院に対するランサムウェア攻撃で緊急手術もできず、必要な医療情報を参照できないなど、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という考えが強いと思います。

だから、ランサムウェア攻撃にあってシステムが暗号化されたとしても業務が回るように、データのバックアップやシステムの複線化・冗長化などで、攻撃に備えておくことが重要です。

（5） サイバーセキュリティ

サイバーセキュリティですが、基本的な枠組みはコンプライアンス一般や危機管理一般の問題と同じです。ガイドラインやマニュアルを整備し、役職員の教育を行う、内部監査等でチェックして PDCA をまわしていくということです。

サイバーセキュリティに固有の方策としては、ソフトウェア(OS、VPN 等)のアップデートによる脆弱性の

© Nishimura & Asahi 2024

是正、バックアップデータの保全や冗長化、Need to know に基づく社内でのアクセス制限、機密情報はスタンド・アローンにしておく(USB 接続を通じたマルウェアに注意)等といった点です。

それから、アクセスログです。どの会社もアクセスログは取っているのですが、データ保存量などの制約から、操作ログはあまり取っていない。サイバー攻撃や社員の個人情報の持ち出し等があった際に、操作ログを取っていないと困ります。例えば、サーバー上のこのフォルダーのこのファイルに誰がいつアクセスしたのか、ダウンロードしたのかどうか等のログです。操作ログがないと、不正アクセスがあったのは分かっても、被害に遭ったのかどうか、被害範囲はどれだけか等が分かりません。費用対効果の問題ではありますが、できれば操作ログも取るようにした方がよい。

それから、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です。休眠させるべきアカウントが生きているとハッカーに乗っ取られてサイバー攻撃の踏み台にされます。

次に、委託先管理、再委託先管理、再々委託先管理です。コンプライアンスやサイバーセキュリティの意識の高い会社ですと、本社は問題ないのですが、再々委託先くらいになってくると、個人情報の持ち出しや名簿屋への売却などの問題が起きることがあります。委託先管理は、委託先が勝手なことをするのを効果的に制御する手段がなく、非常に難しいのですが、起用時の適格性のチェック、委託契約における報告徴求や検査受け入れ、再委託先起用の事前許可の義務づけ等といった手当てで最善の努力をしていくことだと思います。

サイバー攻撃や不正なシステムへの侵入については、100%未然防止することは不可能という前提に立って、侵入後であっても検知・防御する方法や体制(外部へのデータ送信量の常時モニタリング等)を整備して、できるだけ早く掴んで被害を最小化するという発想も大事です。こうしたテクニカルな部分は、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)などの政府関係機関の発信情報をウォッチすることが有益です。また、在宅勤務では、総務省の「テレワークセキュリティガイドライン」なども有益です。

4. 営業秘密持ち出し

(1) 営業秘密持ち出し

回転寿司店運営会社の役員による営業秘密持ち出し(不正競争防止法違反)が最近大きく報道されました。今後、この種の営業秘密持ち出しの事件は増えていくと思います。会社の役員や幹部レベルであっても手土産感覚で営業秘密を持ち出すこともあり、今の日本では、営業秘密の持ち出しについては罪に当たるという意識が必ずしも高くありません。だから、経営幹部も含めて、改めてそういうのは駄目なんだ、刑事罰に問われるぞ、と研修や教育を十分に行う必要があります。

営業秘密の持ち出しは、役職員の退職や転職の際に発生します。どの会社でも励行していると思いますが、退職者から誓約書を取ったり、会社と退職者との間で、持出しを禁止する情報(顧客名簿、社内の開発資料等)と許す情報(個人管理の名刺、手帳・ノート等)とを区分けして両者で確認するといったことが重要です。

また、退職者に、誓約書で競業避止義務や同業他社への転職制限をかけることも検討が必要になります。どの程度の範囲や期間で競業避止義務などをかけることができるかは、退職者の地位・職責、退職金等の代償措置の十分さ、期間の限定(3 ヶ月か半年か、それ以上か)等を踏まえ、個別に検討する必要があります。

テクニカルには、IT システムやコピー機について、アクセスログのみならず操作ログもとる、USB の接続を制限すること等も予防策として有益です。加えて、退職者から回収した端末などの IT 機器についても、必要性やリスクに応じて、中身を検証したり、検証まではしなくても一定期間保管しておくことも考えられま

© Nishimura & Asahi 2024

す。

それと、文書や電子ファイル等に対する営業秘密の表示です。不正競争防止法で営業秘密として保護されるためには、有用性、非公知性、秘密管理性といった要件があり、要は「マル秘」等と表示して役職員がそう認識できるように営業秘密を管理しないといけません。

（2）　中途採用者に対して(受入れ企業側)

転職してきた人が前職の会社から営業秘密を持ち出して、自分の会社で利用した、というケースがあります。そのために、自分の会社も不正競争防止法違反で摘発されたり、前職の会社から、損害賠償を求めて訴えられることになります。

だから、中途採用者が他社から営業秘密を自社に持ち込まないようにすることも非常に大事です。具体的な方法としては、日頃の研修(上司同僚が中途採用者に対し、元の勤務先の情報を求めたり、利用したりしない)、中途採用者の入社時の研修、誓約書(転職元の秘密情報を保有していない)等です。

そのほか、G メールの監視も重要です。USB は自社のシステムにつなげないか、ログが残るようにしている会社も少なくありません。そこで、営業秘密を持ち出す場合には、前職の会社のメール・アカウントから、例えば、G メール・アカウントの方に送り、その G メール・アカウントから転職先の会社の自分のメールアドレスに送る、という方法が散見されます。だから、転職者について、G メールで送られてくる情報については特に気をつけてチェックをすることなども重要です。

以　上

Ⅱ　最近の危機管理・コンプライアンスに係るトピックについて

執筆者:　木目田 裕、宮本 聡、西田 朝輝、澤井 雅登、寺西 美由輝

危機管理又はコンプライアンスの観点から、重要と思われるトピックを以下のとおり取りまとめましたので、ご参照ください。

なお、個別の案件につきましては、当事務所が関与しているものもありますため、一切掲載を控えさせていただいております。

【2024 年 6 月 25 日】

経済産業省、「企業情報開示のあり方に関する懇談会 課題と今後の方向性(中間報告)」を公表

https://www.meti.go.jp/press/2024/06/20240625001/20240625001.html

経済産業省は、2024 年 6 月 25 日、同省が設置した「企業情報開示のあり方に関する懇談会」がまとめた、日本企業の情報開示の課題と今後の方向性に関する中間報告書を公表しました。

本報告書は、今後の情報開示の在り方として、①会社法に基づく事業報告・計算書類等、金融商品取引法に基づく有価証券報告書及び証券取引所上場規程に基づくコーポレート・ガバナンスに関する報告書について、一体開示を目指していくこと、②事業報告・計算書類等を含む法定開示書類について、定時株主総会の十分前に開示されるようにすること、③法定開示書類について、日本語・英語両方での開示を進めていくこと、④AI 等を用いて報告書が読まれることが増えてきていることを踏まえ、開示書類について、XBRL 形式でタグ付けを行うことにより、情報収集の容易性、機械可読性を向上させること等の意見を挙げています。

© Nishimura & Asahi 2024

【2024 年 6 月 26 日】

政治資金規正法の一部を改正する法律が公布

https://www.sangiin.go.jp/japanese/joho1/kousei/gian/213/pdf/s0902130132130.pdf

2024 年 6 月 26 日、政治資金規正法の一部を改正する法律が公布されました。
本改正においては、例えば、以下の項目について改正が行われています。

- 国会議員関係政治団体の代表者の責任の強化(会計責任者の監督義務、会計帳簿等の随時又は定期の確認義務の新設、収支報告書への代表者の確認書の添付等)
- 政治資金監査の強化(国会議員関係政治団体の政治資金は原則預貯金の方法で保管すること、登録政治資金監査人による政治資金監査の確認事項の追加等)
- 政治資金の透明性向上のためのデジタル化の推進(収支報告書等のオンライン提出の義務化、インターネットでの公表等)
- 政治資金パーティーへの対価支払者の氏名等の公開基準を 20 万円超から 5 万円超に引下げ
- 政治資金パーティーの対価の支払方法を預貯金口座への振込み等に制限
- いわゆる政策活動費の使途の明細の公開の導入
- 政党から公職の候補者個人への政治活動(選挙運動を除く。)に関する寄附の禁止
- 国会議員関係政治団体から寄附を受けた政治団体の政治資金の透明性の確保のための措置の導入(国会議員関係政治団体以外の政治団体について一定金額以上の寄附を受けたものについて、国会議員関係政治団体の特例規定の適用対象とすること等)
- 個人寄附者等の個人情報の保護等(収支報告書に記載された個人寄附者等の住所は、都道府県、郡及び市町村名部分等のみ公表)

【2024 年 6 月 26 日】

個人情報保護委員会、「個人情報保護法　いわゆる 3 年ごと見直しに係る検討の中間整理」を公表

https://www.ppc.go.jp/personalinfo/3nengotominaoshi/

個人情報保護委員会は、2024 年 6 月 26 日、個人情報保護法の 3 年ごと見直しに係る検討の中間整理を公表しました。

本中間整理においては、以下の事項の見直しについて検討する必要があること等が指摘されております。

- 要保護性の高い個人情報(生体データ)の取扱い
- 「不適正な利用の禁止」(個人情報保護法 19 条)、「適正な取得」(個人情報保護法 20 条 1 項)の規律の明確化
- 第三者提供規制の在り方(オプトアウト届出事業者が一定の場合に情報提供先の身元等を確認する義務の新設等)
- こどもの個人情報等に関する規律の在り方
- 個人の権利救済手段の在り方(差止請求制度等の新設等)
- 課徴金、勧告・命令等の行政上の監視・監督手段の在り方
- 刑事罰の在り方
- 漏洩等報告(個人情報保護法 26 条 1 項)、本人通知の在り方
- 本人同意を要しないデータ利活用等の在り方
- 民間における自主的な取組の促進

© Nishimura & Asahi 2024

【2024 年 6 月 27 日】

証券取引等監視委員会、「金融商品取引法における課徴金事例集～不公正取引編～」を公表

https://www.fsa.go.jp/sesc/jirei/torichou/20240627.html

証券取引等監視委員会は、主に、2023 年 4 月から 2024 年 3 月までの間に、金融商品取引法違反となる不公正取引に関し、勧告を行った事例を取りまとめ、公表しました。本事例集に記載されている 2023 年度における課徴金勧告事案の主な特徴は以下のとおりです。

【インサイダー取引】

- 上場会社の役員・社員から伝達を受けた者によるインサイダー取引を複数勧告
- 上場会社の社員が職務上知得した内部情報を悪用し、借名口座を使用してインサイダー取引を行った事案を複数勧告
- 海外に居住する上場会社の中国子会社の役職員が、知人名義の証券口座を使用してインサイダー取引を行った事案を勧告
- 公開買付対象者の役員が多数の知人に対して情報伝達・取引推奨に及んだ事案を勧告
- 子会社のバスケット条項を適用した事案を勧告

【相場操縦】

- 他人名義を含む複数の証券口座を使用し、売り見せ玉と買い見せ玉を交互に繰り返し発注することで株価を人為的に変動させていた事案を勧告
- 海外に居住する個人投資家が店頭デリバティブ取引において、見せ玉手法により相場操縦を行った事案を勧告
- 違法な安定操作が行われたと認められた事案を勧告

【偽計】

- 登録高速取引行為者の電子情報処理組織を用いた高速取引行為による偽計事案を勧告

【2024 年 6 月 28 日】

金融庁、「マネー・ローンダリング等対策の取組と課題(2024 年６月)」を公表

https://www.fsa.go.jp/news/r5/amlcft/20240628/20240628.html

金融庁は、2024 年 6 月 28 日、「マネー・ローンダリング等対策の取組と課題(2024 年 6 月)」を公表しました。

本レポートは、マネー・ローンダリング・テロ資金供与(以下「マネロン等」といいます。)対策に関し、2023 事務年度(2023 年 7 月～2024 年 6 月)における日本の金融機関等を取り巻くリスクの状況や、金融機関等における対応状況、金融庁及び財務局の取組等を紹介しています。マネロン等に関する取組については、以下のものを紹介しています。

- 「マネロン・テロ資金供与・拡散金融対策に関する行動計画(2024-2026 年度)」の策定
- 金融庁によるリスクベース・アプローチに基づく検査・モニタリングの実践
- 「マネロン・テロ資金供与対策ガイドラインに関するよくあるご質問(FAQ)」の改訂
- 各地域における金融機関等の連携強化(業態横断フォーラムの開催)
- 金融サービスの不正利用対策に関する注意喚起等の実施

© Nishimura & Asahi 2024

【2024 年 6 月 28 日】

公取委、「イノベーションと競争政策に関する検討会」最終報告書を公表

https://www.jftc.go.jp/houdou/pressrelease/2024/jun/240628_keitorikikaku.html

公取委は、2024 年 6 月 28 日、「イノベーションと競争政策に関する検討会」最終報告書を取りまとめました。本検討会は、企業行動がイノベーションに与える影響メカニズム等について、経済学的知見等に基づき理論的・体系的に整理することを目的として、令和 5 年 3 月以降開催されているものです。

本最終報告書においては、競争当局が、独占禁止法におけるイノベーションへの影響を評価する際の着眼点等として、以下の点を挙げる等しています。

① 研究開発競争に着目した市場画定
製品等が存在しない時点においても、研究開発の目的等に鑑み、将来的に生まれると想定される商品又は役務の市場画定を行い、競争への影響を評価することが適当であること等。

② 長期的視点からのイノベーションへの影響評価の着眼点
イノベーションによる長期的な競争促進効果についても適切に評価することが必要であり、短期的な競争制限効果と長期的な競争促進効果が同時に見込まれる場合は両効果を総合的に考慮して独占禁止法上問題となるか否かを判断すべきこと等。

③ イノベーションの影響評価における事業者からの適切な情報提供及び立証の在り方
イノベーションを促進する旨の主張をする事業者は、その主張に係る客観的な証拠を積極的に提出することを推奨すること等。

【2024 年 7 月 3 日】

公正取引委員会事務総長、独占禁止法上の確約手続の運用を強化することを公表

https://www.jftc.go.jp/houdou/teirei/2024/jul_sep/240703.html

2024 年 7 月 3 日、公正取引委員会事務総長は、定例会見において、以下のとおり、独占禁止法上の確約手続の運用を強化することを公表しました。

- 確約手続を適用した事案における確約措置の履行期間は、従前全ての事案について 3 年間とされていたが、今後は原則として 5 年間以上とすること
- 従前、確約措置については、基本的に当該事業者が自ら履行し、それを当委員会に報告するという形が採られていたが、今後、確約措置全体の履行について、外部専門家による監視を積極的に活用すること
- 特に必要があると判断される場合には、公正取引委員会が、罰則付きの調査権限(独占禁止法 68 条、47 条)に基づき、直接の関係者のみならず、取引先事業者や競合他社などに対しても、確約措置の履行状況の確認などを行うこと

【2024 年 7 月 10 日】

米 FTC ほか、ダークパターンの使用に関する調査結果を発表

https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

米国連邦取引委員会(Federal Trade Commission)、消費者保護及び執行のための国際ネットワーク(International Consumer Protection and Enforcement Network)、グローバルプライバシー執行ネット

© Nishimura & Asahi 2024

ワーク(Global Privacy Enforcement Network)は、2024 年 7 月 10 日、ダークパターンの使用に関する調査結果を発表しました。ダークパターンとは、ユーザーを騙したり誤認等させる、ウェブサイトの記載やデザイン等の手法のことを指します。

本調査結果によれば、調査対象とした、世界各国においてサブスクリプションサービスを提供している合計 642 のウェブサイトとモバイルアプリのうち、76%近くが 1 つ以上のダークパターンを使用しており、67%近くが複数のダークパターンを使用していたとのことです。また、ダークパターンの内容としてよく見られた手法は、消費者の意思決定に影響を与える可能性のある情報を隠したり開示を遅らせたりする手法(スニーキング)や、重要な情報を不明瞭にしたり、事業者に有利な選択肢をデフォルト設定にしておく手法(インターフェイス干渉)でした。

【2024 年 7 月 19 日】

総務省、有識者会議による「デジタル空間における情報流通の健全性確保の在り方に関する検討会とりまとめ(案)」を公表

https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000416.html

総務省は、2024 年 7 月 19 日、同省が設置した「デジタル空間における情報流通の健全性確保の在り方に関する検討会」が作成した「デジタル空間における情報流通の健全性確保の在り方に関する検討会とりまとめ(案)」を公表しました。総務省は、2024 年 8 月 20 日までの間、本とりまとめ(案)について意見を募集しています。

本とりまとめ(案)では、情報伝送プラットフォーム事業者[7]等に対し、例えば、以下のような対応を求めるなどしています。

- 違法な偽・誤情報に対し、行政機関からの申請を契機とした削除等の対応を迅速化
- 悪質な発信者に対する情報の削除やアカウントの停止・削除を確実に実施する方策の具体化
- 違法ではないが有害な偽・誤情報への対応として、情報の可視性に直接の影響がないコンテンツモデレーション(収益化停止等)を中心とした対応の具体化
- 将来にわたる社会的影響の事前予測と、軽減措置の検討・実施(特に災害時における影響)
- 情報流通の健全性への影響の軽減(サービスアーキテクチャや利用規約等の変更による社会的影響の予測・軽減措置の実施等)
- マルチステークホルダーによる連携・協力の枠組みの整備
- 広告事前審査の確実な実施と実効性向上のための、審査基準の策定・公表、審査体制の整備・透明化、本人確認の実施等

以　上

[7] 本とりまとめ(案)では、SNS、動画投稿・共有サービス、検索サービス、ブログ・掲示板サービス、ニュースポータルサービス等、インターネット上で第三者が投稿等発信したコンテンツやデジタル広告を不特定の者が閲覧等受信できるように伝送するプラットフォームサービスを情報伝送 PF サービスとしており、これを提供する事業者を情報伝送 PF 事業者と定義しています。

© Nishimura & Asahi 2024

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。
また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ 広報課 newsletter@nishimura.com

© Nishimura & Asahi 2024