NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松 法律事務所
NO&T Compliance Legal Update
危機管理・コンプライアンス ニュースレター

2024年7月12日　No.95

サイバーセキュリティリスク対応についての、有事対応をみすえた平時における実務上のポイント(2)

弁護士 工藤 靖
弁護士 早川 健
弁護士 郡司 幸祐
弁護士 河原健二郎

はじめに

前回の本テーマのニュースレター[1]では、近時のサイバーセキュリティに対する脅威状況をご紹介すると共に、重大な結果を生じさせる傾向にあるランサムウェア攻撃による不正アクセス事案や従業者の持ち出し事案を念頭に、インシデントの発生時にまず問題となる初期調査、その後の当局やステークホルダーとのコミュニケーションについての対応、そして、これらの有事対応をみすえた平時対応における実務上のポイントについて紹介した。本ニュースレターでも引き続き、以下の同様の各事案を素材として、ランサムウェア攻撃の場合に特有の攻撃者からの金銭の支払要求への対応、また、各事案のそれぞれについて、損害賠償対応、原因分析を踏まえた再発防止策の検討・実施について紹介する。

ランサムウェア攻撃による不正アクセス事案
社会保険労務士の事務所等のユーザに対して社会保険/人事労務業務支援システムを SaaS 環境でサービス提供していた事業者において、同社のサーバーが不正アクセスを受けた。このランサムウェア攻撃により、本件システム上で管理されていた当該ユーザの顧客である企業や事務所等の役職員に係る個人データ等が暗号化され、漏えい等のおそれが発生した事案

従業者の持ち出し事案
多数の民間事業者、独立行政法人及び地方公共団体等から委託を受けていたコールセンター事業者が、システムの保守運用をグループ会社に委託したところ、当該グループ会社の従業者が、民間事業者、独立行政法人及び地方公共団体等の顧客又は住民等に関する個人データ等合計約 928 万人分を不正に持ち出したことにより、漏えいが発生した事案

ランサムウェア攻撃の場合の攻撃者からの金銭の支払要求への対応

ランサムウェア攻撃の場合には、その特有の問題として、暗号化されたデータの復旧やデータを公開しないこと

[1] 危機管理・コンプライアンスニュースレター第 93 号「サイバーセキュリティリスク対応についての、有事対応をみすえた平時における実務上のポイント(1)」

と引き換えに、身代金として金銭の支払いを要求される場合がある。このような場合、金銭の支払いに応じることは、攻撃者の資金源となること、攻撃者が同種犯罪を継続するモチベーションになりうること、さらには、金銭を支払ったとしてもデータが公開されない保証はなく、追加で金銭を要求される可能性もあることなどから、一般論としては、金銭の支払いをすべきでないとされている。しかし、実際上は、経営判断の問題として支払いの是非を検討せざるを得ない場合もある。

有事対応をみすえた平時における実務上のポイント

✓ 攻撃者に対する金銭の支払いについては、海外におけるマネー・ローンダリング関連規制（特に米国法上の OFAC 規制）や、国内における外国為替及び外国貿易法における資産凍結等の措置対象による法令違反のリスクも懸念され、実務上は、関連法令の適用状況、事業継続可能性や事業復旧費用・損害賠償リスクといった事項を考慮して経営判断することが想定される。その検討には時間的な制約があることが想定される一方で、時間的制約があるからといって経営判断について取締役の善管注意義務の水準が軽減されるわけではない旨を判示する判例があること（最判平成 20 年 1 月 28 日・集民第 227 号 43 頁）を踏まえると、単に時間的な余裕がないことを理由として情報収集等が不足していてもよいということにはならない。そのため、判断プロセスを平時から整備（事業継続計画（BCP）における意思決定手続の整備）し、被害シナリオを想定したリスク検討を事前に行っておくことが望ましい。

損害賠償 [2]

不正アクセスの場合、従業者による情報の持ち出しの場合のそれぞれについて、企業として、漏えいにより損害が生じた本人や取引先等の第三者から損害賠償請求を受ける場合がある。この場合には、レピュテーションリスクも考慮して、一律の補償実施や示談・和解も検討することになるが、法的に損害を賠償する義務が生じるか、義務がある場合にどの程度の金額を支払うべきか、また、法的義務まではないものの今後の取引継続も考慮して補償を行うかなどについては、事案における個別事情によることになる。そのため、過去の裁判例も念頭に置きながら当該インシデントにおける各事情を考慮していくことが必要となる。

有事対応をみすえた平時における実務上のポイント

✓ 実務上は、インシデントの発生により企業が損害を被った場合（本人への補償・損害賠償や取引先等の第三者への損害賠償等を含む）などにおいて、当該企業や取引先に対し取締役が善管注意義務違反に基づく損害賠償責任を負う可能性があるという点にも留意が必要である [3]。この場合、内部統制システムの構築義務の一環として、取締役はサイバーセキュリティ体制を構築する義務を負うと解されており [4]、これを踏まえてセキュリティリスクの管理体制に不備があったとして当該義務違反を主張されることがありうる。

✓ また、リスク管理体制の構築・運用について、通常想定される不正行為（リスク）を防止しうる程度の管理体制の構築・運用が行われたか否か、発生した不正行為を予見すべき特別の事情（過去に同種の事案が生じていたかなど）の有無を判断基準にしている判例がある [5]。そのため、過去にインシデントを経験している場合には、経験していない場合と比較して、「特別の事情」が認められることにより、構築・運用が求められるリスク管理体制（再発防止等の是正対応）の水準が高まる可能性があるという点には留意が必要である。

---

[2] このほか、企業において損害が発生した場合には、サイバー保険に加入している場合にはサイバー保険による補償がどの程度なされるのかについて、サイバー保険における具体的な契約条項を元に確認していくことも必要となる。

[3] 会社法 423 条 1 項・847 条、429 条 1 項

[4] 例えば、サイバーセキュリティ戦略本部の「重要インフラのサイバーセキュリティに係る行動計画」は、「組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。経営層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。」と述べている。また、経済産業省の「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」も、グループ単位の内部統制システムの重要性について「親会社の取締役会は、『企業集団（グループ）』全体の内部統制システムの構築に関する基本方針を決定し、『企業（法人）』単位と並びグループ単位での『内部統制システム』を構築・運用することが求められている」と述べている。

[5] 最判平成 21 年 7 月 9 日（日本システム技術事件判決）集民第 231 号 241 頁

原因分析を踏まえた再発防止策の検討・実施

ランサムウェア攻撃による不正アクセス事案や従業者による情報の持ち出し事案といったインシデントが発生した場合、信頼回復のための取組を行っていくことが企業価値の維持のためには不可欠であり、また、上記のとおり、再度、同種のインシデントが発生した場合には経営陣が善管注意義務違反を問われるリスクも高まるため、原因分析を踏まえた実効的な再発防止策を策定することの検討・実施はその中核をなすものといえる。

(1) ランサムウェア攻撃による不正アクセス事案における発生原因と再発防止策

発生原因のポイント

ランサムウェア攻撃による不正アクセス事案では、一般的には、システムの脆弱性が直接的な原因となることが多く、技術的安全管理措置や物理的安全管理措置に関する不備が要因となることが多い。しかし、より根本的な原因として、人的安全管理措置や組織的安全管理措置の不備が要因となることも多い。例えば、医療機関に対して委託システムを経由してランサムウェア攻撃が行われた事例では、その調査委員会の報告書[6]において、以下の発生要因が指摘されている。

- ✓ 技術的発生要因
  - ➢ 外部接続の管理不備：サプライチェーンにおける VPN 機器の脆弱性の放置等
  - ➢ 内部のセキュリティの脆弱性：管理者権限の設定の不備等
- ✓ 組織的発生要因
  - ➢ 情報システムにおける共通セキュリティ仕様に基づく調達の不徹底
  - ➢ システム担当部署により管理されていない情報システムの存在
  - ➢ 各システムベンダとの契約におけるセキュリティに関する責任範囲の不明確性
  - ➢ 複数のシステムベンダが関与する契約における各ベンダ間の責任分担の不明確性等

個々のインシデントの発生原因は様々であり一律に論ずることができないものの、上記のような発生原因はどの企業にも存在しうる要因といえる。このため、平時からの対応としては、これらの不備に関するリスクを把握した上で、後述するように、組織的安全管理措置・人的安全管理措置・物理的安全管理措置・技術的安全管理措置、さらには委託先管理の観点からそれぞれ手当てをしていくことが求められる。

再発防止策の検討にあたって考慮すべき視点

具体的な再発防止策については個々のインシデントの発生原因に応じて検討する必要があるものの、以下に記載する個人情報保護法ガイドライン（通則編）3-4-2 及び同 10「（別添）講ずべき安全管理措置の内容」は情報セキュリティ確保のための一般的な視点から構成されている。そのため、インシデント発生により漏えい等の対象となるデータは個人データには限られないが、再発防止策を策定するにあたっての基本的な視点として参考になるものと考えられるため紹介する。

① 組織的安全管理措置
  - ✧ 組織体制の整備、個人データの取扱いに係る規律に従った運用、個人データの取扱状況を確認する手段の整備、漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直し

② 人的安全管理措置
  - ✧ 従業員の教育

③ 物理的安全管理措置
  - ✧ 個人データを取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止、個人データの削除及び電子媒体等の廃棄

④ 技術的安全管理措置

[6] https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf（調査報告書・概要版）

✧ アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報システムの使用に伴う漏えい等の防止

また、委託先におけるインシデントの場合には、これに加えて、委託先の管理（個人情報保護法 25 条）の観点から「適切な委託先の選定」、「委託契約の締結」、「委託先における個人データ取扱い状況の把握」についての必要かつ適切な措置といえるかという視点で再発防止策を検討すべきこととなる[7]。

なお、内閣官房内閣サイバーセキュリティセンターは、2023 年 7 月に「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」を公表している。同手引書では「重要インフラ事業者等」[8]を想定してリスクマネジメントのフレームワークとして①リスクマネジメントにおけるコミュニケーション及び協議、②組織の状況の特定、③リスクアセスメント、④リスク対応、⑤コンティンジェンシープラン及び事業継続計画（BCP）の策定、⑥運用、⑦モニタリング及びレビュー、⑧記録及び報告のプロセスを挙げているものの、このプロセスについては、「重要インフラ事業者等」以外の事業者にとっても実務上参考になる。

有事対応をみすえた平時における実務上のポイント

✓ 再発防止策を講じる場合には、脆弱性への手当てとして新たなルールやチェックリストを設けるといった対応が必要になる場合も多いが、業務プロセスの負荷が大きいような場合にはルール外の行為（例えば、会社が把握していないデバイスやクラウドサービスの利用等）が行われたりすることにより再発防止策が形骸化し、実効性が確保されないおそれが生じる。このため、「しなければならない」事項を増やすだけでなく、セキュリティの脆弱性を生じさせない行為をとることを促すといった従業員の意識の醸成を検討することが望ましい。

✓ そして、従業員の意識の醸成にあたっては、経営者がリーダーシップをとり[9]、セキュリティの重要性を繰り返し従業員に対して説明すると共に、中間管理職を含めた従業員による実践を繰り返すことで意識の浸透を図っていくことが重要である。また、併せて、セキュリティの脆弱性につながりうるような状況を発見して手当てすることを奨励するなど、セキュリティの向上につながる行動を人事評価上も積極的に評価し、逆にセキュリティの脆弱性につながりかねない行為については厳正に処分を行うといった施策を講ずるなどして、セキュリティ確保に向けた行動をインセンティブづけするような社内制度・仕組みを設計していくことも重要である。そして、内部監査等を通じた業務プロセスにおける対応状況・事例の収集、アンケート調査や個別の従業員へのヒアリング等を通じて得られた施策の実効性について定期的に評価し、必要に応じて社内制度・仕組みを見直していくことにより PDCA サイクルを回していくことが望ましい。

(2) 従業者の持ち出し事案における発生原因と再発防止策

発生原因のポイント

従業者の持ち出し事案では、一般的には、悪意をもった従業者による情報の持ち出しを阻止するための技術的管理措置や物理的管理措置の不備が直接的な原因となることが多い。例えば、冒頭で紹介した個人情報保護委員会が令和 5 年度の重大な事案として挙げていた従業員の持ち出し事案において、その調査委員会は、従業者による持ち出しが可能となった原因として、主に以下の発生要因を指摘している。

---

[7] なお、委託先がグループ会社の場合、委託先グループ会社における安全管理措置のレベルの向上について統括会社・本社が関与することも実際上可能な場合も多いと考えられるため、統括会社・本社が委託先グループ会社におけるサイバーセキュリティ対策の支援を平時から行っていくのが望ましい。この点について、先述の経済産業省の「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」も参考になる。

[8] サイバーセキュリティ戦略本部の「重要インフラのサイバーセキュリティに係る行動計画」別紙 1 「対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定されているものをいう（例えば、重要インフラ分野ごとに、「主要な電気通信事業者」、「銀行」、「主たる定期航空運送事業者」、「一般送配電事業者」等が挙げられている。具体的な内容は、当該別紙を参照されたい。）。

[9] 本ニュースレターでの詳細な紹介は割愛するものの、経済産業省・独立行政法人情報処理推進機構（IPA）が公表している「サイバーセキュリティ経営ガイドライン Ver 3.0」で、経営者が自らのリーダーシップのもとで対策を進めることが必要である旨が指摘されているとおり、経営者によるリーダーシップはサイバーセキュリティリスクへの対応の観点からは極めて重要なポイントである。

- ✓ 直接的原因：技術的な管理措置に係る重大な不備
  - ➢ サーバーから顧客データのダウンロードを制御する措置の不存在
  - ➢ 私有 USB メモリ等の外部記録媒体への書き出しを防止する措置の不存在
  - ➢ 保守端末からのインターネット接続を制限する措置の不存在
  - ➢ ログ監視の不存在
  - ➢ 私有端末によるアクセスを制限する措置の不存在
- ✓ 組織的原因：内部者による情報漏えいリスクを高める業務運営体制
  - ➢ 持ち出しを行った従業者が長年にわたりサーバーの運用保守及びサポート業務に従事し豊富な知見を有しており業務を当該従業者に依存することが長きにわたり固定化して業務監視も機能していなかったこと

再発防止策の検討にあたって考慮すべき視点

従業者による情報の持ち出しは、内部不正に該当するため、再発防止策を検討する上では、独立行政法人情報処理推進機構（IPA）が公表している「組織における内部不正防止ガイドライン」（本ニュースレター執筆時は改訂版第 5 版）が参考になる。同ガイドラインは、①基本方針、②秘密指定、③アクセス権指定、④物理的管理、⑤技術・運用管理、⑥原因究明と証拠確保、⑦人的管理、⑧コンプライアンス、⑨職場環境、⑩事後対策、⑪組織の管理等、10 の観点のもと 33 項目の対策を示しており、上記の事案において従業者による持ち出しを許した原因との関連でも、再発防止策として検討されるべきといえる。

有事対応をみすえた平時における実務上のポイント

- ✓ 従業者による情報の持ち出しという内部不正の再発防止のためには、上記に述べた IPA の「組織における内部不正防止ガイドライン」でも述べられているような、多岐にわたる対応が求められる。そして、実際上は、想定されるリスクに応じて、特に手当てをすべき課題を特定して対応する必要があるが、他社事例等も勘案しながら自社の対応を省みるといったアプローチもありうる。例えば、IPA が 2023 年 4 月 6 日に公表した「企業の内部不正防止体制に関する実態調査」報告書では、以下のような観点での具体的な課題が指摘されており、参考になる。
  - ➢ 内部不正防止に関する知識の取得・周知・教育のあり方
  - ➢ 内部不正防止に関する組織の体制のあり方
  - ➢ 内部不正防止対策の課題

(3) 再発防止策の実施に関する留意点等

サプライチェーン全体でのリスク対応の必要性

前回の本テーマのニュースレターで紹介した、本年 1 月 25 日付で独立行政法人情報処理推進機構（IPA）が公表した「情報セキュリティ 10 大脅威」においては、サプライチェーンの弱点を悪用した攻撃は「組織」向け脅威の 2 位となっており、複数年にわたって脅威となっていることが示されている。上記で紹介したランサムウェア攻撃による不正アクセス事案や医療機関に対して委託システムを経由してランサムウェア攻撃が行われた事例もサプライチェーンの弱点を攻撃された事例とも考えられる。このようなサプライチェーンにおけるサイバーセキュリティリスク対応は、取引先や委託先を含むサプライチェーン全体で行う必要がある。そのため、新たな取引先や委託先との取引を開始するにあたっては、予め策定された取引先選定基準・委託先選定基準に従って選定を行った上で、契約条項において、セキュリティ対策上の要求事項を具体的に定めておく必要がある。

具体的にどのような契約条項を定めるべきかは、委託先との取引内容・委託内容等に照らして検討する必要があるが、例えば、取引先・委託先が実施すべきセキュリティ対策の内容のほか、秘密保持義務、セキュリティ対策の実施状況に対する検証を可能にするための証拠の確保・共有や監査への協力、再委託の禁止又は制限・管理策、契約終了後の提供情報・データの取扱い、ベンダーロックインを回避するためのデータ移行等に関する協力義務、イ

ンシデント発生時の対応協力義務や発生した損害の責任負担等が考えられる[10]。

また、サプライチェーン全体でのリスク対応については、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（いわゆる経済安全保障推進法）における基幹インフラ役務の安定的な提供の確保に関する制度において参照されるリスク管理措置も参考になる。この制度は、基幹インフラ役務の提供を阻害する海外からのサイバー攻撃等に対する対応として、特定社会基盤事業者を指定し、電気、ガス等の指定基幹インフラ役務の安定的な提供のため、特定社会基盤事業者が、①その事業の用に供する重要な一定の設備、機器、装置又はプログラムの導入を行う場合や、②他の事業者に対してこれらの設備、機器、装置又はプログラムの導入を委託する場合には、予め計画書を提出し、主務大臣による審査をうけることが求められる。この計画書には、一定のリスク管理措置の記載が求められ、主務大臣による事前審査の対象となる。このリスク管理措置について、国は、各特定社会基盤事業者が実施すべきリスク管理措置は、その事業に関するリスクの内容及びリスクの程度に応じて定めるべきものとして、その考え方を公表しており、その内容はサプライチェーンにおけるセキュリティ対応にとって示唆に富むものとなっている[11]。

取引先や委託先に対するセキュリティ対策実施要請における国内法上の留意点

もっとも、取引先や委託先に対してセキュリティ対策の実施を要請する場合には、取引先や委託先に一定のコスト負担を要請することとなるため、独占禁止法・下請法との関係で一定の留意が必要である。すなわち、これらに対してサイバーセキュリティ対策の実施を要請すること自体が直ちに独占禁止法・下請法との関係で問題となるわけではないものの、その対策実施について双方が合意に至った場合であっても、その背景にある事実関係や実施内容によっては、独占禁止法上の優越的地位の濫用[12]や下請法上の親事業者の禁止行為[13]として問題となりうる。

例えば、取引上の地位が相手方に優越している事業者が、取引の相手方に対し、①サイバーセキュリティ対策の実施要請を行い、サイバーセキュリティ対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合（対価の一方的決定）、②セキュリティ対策費等の名目で金銭の負担を要請し、当該セキュリティ対策費の負担額及びその算出根拠等について、取引の相手方との間で明確になっておらず、取引の相手方にあらかじめ計算できない不利益を与えることとなる場合（セキュリティ対策費の負担の要請）、③サイバーセキュリティ対策の実施の要請に際して、合理的な必要性がないにもかかわらず、自己の指定する商品の購入や役務の利用を強制する場合（購入・利用強制）などの場合には問題になりうる[14]。

このため、実務上の対応としては、取引先や委託先に対してセキュリティ対策の実施を要請するにあたり、十分な周知期間を確保した上で、丁寧な説明・協議を行い、これらの説明・協議の結果合意に至るプロセスを適切に記録化（議事録・説明資料の保管等）しておくことが肝要である。

海外法令によるサプライチェーン全体でのリスク対応への影響

紙幅の関係上、本ニュースレターではその詳細には触れないが、2024 年 3 月 12 日、欧州議会(European Parliament)は、サイバーレジリエンス法(Cyber Resilience Act)を採択した[15]。このサイバーレジリエンス法は、EU 市場内のデジタル要素を含む製品（Products with digital elements）[16]に不可欠なサイバーセキュリティについて統一的な法的枠組みを定め、製品の信頼性向上と利用者の安全を図ることを目的としている。規制対象者とし

---

[10] 詳細については、工藤靖「サプライチェーンにおけるサイバーセキュリティリスク対応」（上）・（下）NBL1222 号 36 頁、NBL1223 号 31 頁も参照されたい。

[11] 2024 年 5 月 17 日付、内閣府政策統括官「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」の「第 2 部リスク管理措置の解説」参照

[12] 独占禁止法 2 条 9 項 5 号

[13] 下請法 4 条 1 項、2 項

[14] 2022 年 10 月 28 日付、経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」参照

[15] https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products

[16] サイバーレジリエンス法において、デジタル要素を含む製品とは、あらゆるソフトウェア又はハードウェア製品及びその遠隔データ処理ソリューションをいい、本体とは別に市場流通するソフトウェア又はハードウェアのコンポーネントも含むものと定義されている（3 条 1 号）。そして、その重要性に応じて対象製品が分類され、異なる規制が課されている。例えば、重要な製品としては、ID 管理システム、VPN 機能を有するデジタル製品、OS、ルータなどがあげられている。

て、当該製品の製造業者、輸入業者及び流通業者が定められており、製造業者に課される主な義務として、①市場流通前に当該製品のサイバーリスク評価を実施すること(当該製品を構成する第三者からのコンポーネントに関するデューデリジェンスも含む)、②当該製品のライフサイクルにおいて、その脆弱性を効果的に継続管理すること、③当該製品に影響を及ぼす脆弱性の悪用を認識し又は重大なインシデントの発生を認識してから 24 時間以内に関係当局に報告すること、適時のタイミングでこれらの影響を受けるユーザへ通知することなどが定められている。これらの製造業者に課された義務違反に対しては、1,500 万ユーロ又は前会計年度の全世界売上高の 2.5%のいずれか高い方を上限とする制裁金が課されることとなっており、違反リスクは無視できないものと考えられる。今後、サイバーレジリエンス法は、欧州理事会(Council of the European Union)で正式に採択された後に発効することとなる。その発効後 36 ヶ月以内に各義務が適用されるが、製造業者による上記の報告義務は発効から 21 ヶ月以内に適用されるとされている。

上記のとおり、サイバーレジリエンス法に定められた各種義務の適用開始には時間があるものの、対応する製品を取り扱う製造業者は、製品のライフサイクルを踏まえた継続的な脆弱性管理や脆弱性・インシデント報告義務を果たすため、取引相手方との契約上の手当を含む製品サプライチェーンを踏まえた対応が必要となることが想定され、その準備は不可欠なものと考えられる。

まとめ

サイバーセキュリティリスクは、悪意ある第三者による攻撃や内部による犯行・協力により、インシデントとしての顕在化を予測することが困難である一方で、その被害件数は引き続き高い水準で推移していることから、企業において平時からの不断の取組が求められるところである。当事務所においても、インシデント対応について助言させていただくことが多くなっており、平時の対応の必要性を改めて認識していただく必要があると考え、本ニュースレターにて実務上のポイントをご紹介した。今後も、サイバーセキュリティリスクについて実務上の対応として参考になる情報をご紹介していく予定である。

2024 年 7 月 12 日

[執筆者]

工藤 靖（弁護士・パートナー）
yasushi_kudo@noandt.com, 03-6889-7396（直通）

2007 年に長島・大野・常松法律事務所へ入所後、2014 年から 2018 年にかけて、金融庁検査局及び証券取引等監視委員会事務局へ出向し、金融機関のガバナンス・コンプライアンスの検査や上場企業による開示規制違反の調査等、幅広く法執行に携わる。復帰後は、業種を問わず、行政・刑事事件対応を含む危機管理・不祥事対応、コンプライアンス、金融・証券規制を含む各種レギュレーションに関するアドバイス、サイバーセキュリティ・データプライバシー、コーポレートガバナンスその他一般企業法務を幅広く取り扱う。近時は、サイバーセキュリティにおけるサプライチェーンリスクマネジメントなどの法務リスク・コンプライアンス管理体制の構築・運用についても注力している。2004 年東京大学法学部卒。2006 年東京大学法科大学院、2013 年 The University of Chicago Law School 卒業（LL.M.）。

早川 健（弁護士）
takeshi_hayakawa@noandt.com, 03-6889-7669（直通）

2010 年に長島・大野・常松法律事務所へ入所。2017 年から 2018 年にかけてヤフー株式会社へ出向し、その後、2018 年から 2020 年にかけて個人情報保護委員会事務局へ出向し、個人情報保護委員会事務局では欧州、米国、アジアなど世界の個人データ保護法令の動向についての情報収集等に携わる。復帰後は、セキュリティインシデント対応を含むデータをめぐる法的問題や危機管理対応、さらにはこれらを踏まえた平時におけるコンプライアンス対応について助言している。2006 年東京大学法学部卒、2009 年早稲田大学大学院法務研究科修了、2016 年 Duke University School of Law 卒業（LL.M.）。

郡司 幸祐（弁護士）
kosuke_gunji@noandt.com, 03-6889-7396（直通）

2019 年長島・大野・常松法律事務所入所。危機管理・コンプライアンス、民事・商事争訟、独占禁止法、労働法等を中心に、企業法務全般を取り扱う。

河原 健二郎（弁護士）
kenjiro_kawahara@noandt.com, 03-6889-8930（直通）

2020 年東京大学法学部卒業、2022 年弁護士登録（第 75 期，第一東京弁護士会）、同年・長島・大野・常松法律事務所入所。

コンプライアンス・アセスメントのご案内

当事務所の危機管理・コンプライアンスチームでは、事業環境を踏まえ企業のコンプライアンスリスクを分析した上、社内規程その他のコンプライアンス体制の改善に向けたアドバイスを提供するコンプライアンス・アセスメントをご提供しています。対象とする分野を限定した初期的なアセスメントを実施することも可能です。

役員研修、コンプライアンス研修等のご案内

当事務所の豊富な実務経験を活かした実践的な研修プログラムを各種実施しています。最近の不祥事事件からの教訓や、コーポレートガバナンスコード対応を含む最新の法令動向を踏まえ、各社のニーズに沿った内容とさせて頂いています。

ご興味をお持ちの場合や、さらに詳しい情報を知りたい場合は、遠慮なく下記編集者までお問い合わせください。

[編集者]

垰 尚義　パートナー
takayoshi_tao@noandt.com

眞武 慶彦　パートナー
yoshihiko_matake@noandt.com

工藤 靖　パートナー
yasushi_kudo@noandt.com

福原 あゆみ　パートナー
ayumi_fukuhara@noandt.com

深水 大輔　パートナー
daisuke_fukamizu@noandt.com

辺 誠祐　パートナー
tomohiro_hen@noandt.com

長島･大野･常松 法律事務所　www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、約 600 名の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。
（*提携事務所）