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4日　No.93

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)

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：近時のインシデント事例

警察庁は本年3月14日「令和5年におけるサイバー空間をめぐる脅威の情勢等について」を公表している。令和5年におけるランサムウェアによる被害件数は197件（前年比で14.3%減少）であり、引き続き高い水準で推移し、手口としては、データの暗号化のみならず、データを窃取した上、企業・団体等に対し「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝（ダブルエクストーション）が多くを占める。また、独立行政法人情報処理推進機構は本年1月25日「情報セキュリティ10大脅威」を公表し、その「組織」向け脅威においては、ランサムウェア攻撃が1位になっているが、2016年以降の取扱いをみると、2位のサプライチェーンの弱点を悪用した攻撃、3位の内部不正による情報漏えい等の被害など、いずれも、複数年にわたり、脅威であることが示されている。そして、本年6月に公表された「令和5年度個人情報保護委員会年次報告」の概要版では、重大な事案として以下のような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等を挙げている。

▎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

こうしたランサムウェア攻撃により保有する情報が暗号化され、漏えいするおそれ、また、従業員による情報の持ち出しといったインシデントが発生した場合には、まずは初期調査の実施、当局への報告その他ステークホルダーとのコミュニケーションの開始など、有事対応を迅速かつ適切に進め、また、適切な再発防止策の検討・実施をしていくことが重要である。

そして、インシデントが発生したことのある企業はもちろんのこと、まだ重大なインシデントの発生を経験して

いない企業であっても、予め上記の対応事項を念頭に置いて平時対応をしていくことが、サイバーセキュリティリスクの低減につながる。このため、本ニュースレターでは、上記のような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おいたサイバーセキュリティー・インシデントの有事対応、これらの有事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 2 回に分けて紹介していく。第 1 回は、インシデントの発生時にまず問題となる初期調査と、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紹介し、第 2 回は、同様の事案を素材として、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、損害賠償対応、原因分析をふまえた再発防止策の検討・実施について紹介する。

初期調査

インシデントの発生を検知した場合には、まず初期調査により迅速に被害拡大防止を図る必要がある。ランサムウェア攻撃による**不正アクセスの場合**には、CSIRT (Computer Security Incident Response Team)の指揮のもと、システム部門及びその委託を受けた IT・セキュリティベンダ [1]が、技術的観点から、攻撃者・攻撃対象・攻撃が始まったタイミングや侵入経路・どのようにして攻撃しているのか、などを確認することになる（なお、ダークウェブモニタリングも並行して実施することも多い）。また、**従業員の情報の持ち出しの場合**にも、当該従業員がいつ、どのような情報を持ち出したのか、持ち出された情報が誰に渡されたのか、といった事実関係を該当部署がシステム部門と協働して迅速に確認することが重要となる。そして、当該従業員に対してヒアリングを実施し、持ち出されたデータを破棄させ、今後第三者に対して提供・漏えいしないことの誓約書を徴求するなどして、漏えいの拡大を防止することが必要となる。

さらに、不正アクセスについて社内に協力者がいることが疑われる場合や、従業員による情報の持ち出しの場合には、従業員に対してヒアリングを実施することはもちろんのこと、当該従業員のメールを解析するといったことも対応としては必要となり、この場合、社内の関係部門や社外の弁護士や IT・セキュリティベンダと連携して対応する必要が出てくる [2]。このような調査は、メールレビュー等のコンプライアンス事案における一般的な調査手法を活用することとなる。また、インシデントの影響を受ける本人の数が多数にわたるなど社会的に影響が大きい事案である場合には、調査委員会や第三者委員会を立ち上げて調査を実施することがある。

有事対応をみすえた平時における実務上のポイント

- ✓ 被害拡大の防止に向けた調査の実施については迅速性が重要であり、平時より、インシデントの発生を検知した場合に社内でどのように対応していくかについて関係部門においてインシデント対応マニュアル等を整備し、また事前の訓練をすることでこれらのマニュアル等の課題を洗い出した上で見直しを図っていくことが望ましい。
- ✓ また、どのような IT・セキュリティベンダ等の外部専門家に依頼するかについても平時から検討し、コミュニケーションをとっておくことが、有事の際の迅速な対応につながる。

当局やステークホルダーとのコミュニケーション

インシデントの発生を検知した後、上記の初期調査と並行して、関係当局やインシデントにより情報が暗号化、漏えいすることにより影響を受けるであろう個人顧客や取引先などのステークホルダーとのコミュニケーションを検討する必要がある。

(1) 個人情報保護委員会への報告

[1] なお、クレジットカード情報の漏えいの場合の調査機関としては、PCI SSC から正式な認定を受けた PFI（PCI Forensic Investigator）に依頼することが実務上必要とされている点には留意が必要である。

[2] 対象となる従業者が退職済みである場合には、人事部に連絡をとり、ヒアリングへの任意の協力を求めることとなる。会社と利害が対立する場合には任意の協力が得にくい場合もあるが、退職の際に、退職後も会社の必要な調査に協力するといった同意書を徴求しておくなどといった対応を予めとることとしておくことも検討に値する。

不正アクセスにより個人データが漏えいした場合や従業者が顧客の個人データを不正に持ち出して第三者に提供した場合には、「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データの漏えい等が発生し、又は発生したおそれがある事態」[3]に該当し、個人情報保護委員会への報告義務[4]及び本人への通知義務[5]を負うこととなる。

報告義務の履行

個人情報保護委員会に対しての報告は、①**速報**を「報告対象事態を知ったときは、速やかに」[6]、すなわち個人情報取扱事業者が当該事態を知った時点から概ね 3～5 日以内[7]に、②**確報**を事態を知った日から 30 日以内（不正アクセスや従業者による不正な持ち出しのような「不正なく目的をもって行われたおそれがある（以下略）」の要件に該当する場合には 60 日以内。）に、それぞれ個人情報保護委員会のウェブサイトを通じて実施する必要がある[8]。

有事対応をみすえた平時における実務上のポイント

✓ 報告期限に関しては、個人情報保護委員会に対する報告のフォームの中に「事態の概要」として「発覚日」を記載する項目があることから、提出時点が時間的制限を満たしているかどうかは報告書面からも明らかである。報告期限を徒過する場合にはその理由を個人情報保護委員会に対して説明する必要が生じ、場合によっては行政指導の対象にもなりかねないため、当該期限を満たせるような社内の対応プロセスを整えておくことが必要である[9]。

報告の主体

報告義務の主体は、個人データの取扱いについて委託関係がある場合[10]、委託元と委託先がそれぞれ個人情報取扱事業者として個人情報保護委員会への報告義務を負うのが原則であるが、委託先は、委託元に通知することにより個人情報保護法上は報告義務を免除される[11]。

有事対応をみすえた平時における実務上のポイント

✓ 委託元及び委託先の連名で報告することも許容されており[12]、実務上は、事実関係を直接に調査・把握できるのは委託先であることが多く、また、委託元の事業者の数が多い場合など、委託先が主導して報告することが適切な場合には、連名を選択することも多い。この場合、特に速報の際には報告期限が短いため、

[3] 個人情報保護法施行規則 7 条 3 号
[4] 個人情報保護法 26 条 1 項
[5] 個人情報保護法 26 条 2 項
[6] 個人情報保護法施行規則 8 条 1 項柱書き
[7] 個人情報保護法ガイドライン（通則編）3-5-3-3
[8] なお、漏えい等が発生した「おそれ」とは、個別の事案ごとの蓋然性をいい、その時点で判明している事実関係からして漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当するが、抽象的な可能性をもってみとめられるものではないと考えられている（個人情報保護法ガイドライン（通則編）3-5-3-1、「『個人情報の保護に関する法律についてのガイドライン（通則編）の一部を改正する告示案』に関する意見募集結果」(2021 年 8 月 2 日に結果公示)の 188 番参照）。その上で、初期調査の結果「おそれ」がないと考えていたものの、その後の継続調査により「おそれ」が判明した場合には、その時点を起算点として報告すべきことになる。
[9] 個人情報保護委員会事務局の監視・監督室の責任者・担当者が執筆する、連載「個人データ等の漏えい等の発生時の対応と安全管理措置～個人情報保護委員会の監視・監督活動の視点から」（株式会社商事法務・NBL No.1265(2024 年 5 月 1 日号)）の「第 2 回　漏えい等報告の義務と報告の種類」においても、「報告期限を徒過すると、場合によっては行政指導がなされるので注意していただきたい」との注意喚起がされており、個人情報保護法ガイドライン（通則編）10-3(4)でも、「漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない」としている。
[10] なお、冒頭で紹介した「ランサムウェア攻撃による不正アクセス事案」に関し、本年 3 月 25 日に個人情報保護委員会は事業者に対する処分を公表している。この公表において、個人情報保護委員会は、①利用規約において、保守・運用上等必要であると判断した場合といった特定の場合には、ユーザの個人データを使用等できることとなっていたこと、②事業者が保守用の ID を有し、ユーザの個人データにアクセス可能な状態となっており、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと、③ユーザと確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていたことをあげて、個人データの取扱いの委託があったと認定している。
[11] 個人情報保護法 26 条 1 項ただし書き
[12] 個人情報保護法ガイドライン（通則編）3-5-3-2

あらかじめデータの取扱いを委託した委託先との手順を決めておくなど、迅速に報告を実施できるようにしておくことが望ましい[13]。

個人情報保護委員会からの照会事項への対応

個人情報保護委員会への報告に関して、事業者における個人情報保護法の遵守を念頭に置いて報告内容に含まれている事項についての質問を受けることがあり、適切に対応することが必要となる。

有事対応をみすえた平時における実務上のポイント

- ✓ 個人情報保護法及びガイドラインに沿ってどのような安全管理措置をとっていたのか（個人情報保護法 23 条）や、委託先における漏えい等について委託元が報告を行っている場合には、委託先の監督（個人情報保護法 25 条）について、「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」をどのように実施していたのかについては説明をする必要が出てくるため、平時から安全管理措置や委託先管理の実施状況を整理しておくことが望ましい。
- ✓ また、このような整理をしておくことは、適切な有事対応の実施につながるだけではなく、インシデント発生の予防にもつながるものとなる。

(2) 本人通知・取引先への連絡・公表

本人への通知

個人情報保護委員会への報告義務を負う場合には、漏えい等が生じた個人情報から特定される本人に対しても、「事態の状況に応じて速やかに」通知する義務を負う（ただし、本人への通知が困難である場合は、例外的に、本人の権利利益を保護するために事案の公表等の必要な代替措置を講ずることによる対応が認められる[14]）。なお、本人に対してどの時点で通知するかの判断については実務上悩ましい場合もあり、例えば、不正アクセス等の場合で事案がほとんど判明しておらず本人通知をすることによってかえって混乱が生じることが懸念される状況であれば、事案がほとんど判明していないタイミングでは本人の通知は実施せず、調査が進展してより事案が判明してから本人への通知を行うような対応も考えられる[15]。

有事対応をみすえた平時における実務上のポイント

- ✓ 漏えい等したデータについて、第三者が、当該データだけから特定の個人を識別できる場合と、当該データだけでは特定の個人が識別できない情報である場合が想定される。後者の場合について、個人情報保護法ガイドライン Q&A6-10 では、「漏えい等した情報が個人データに該当するかどうかは、当該情報を取り扱う個人情報取扱事業者を基準に判断する」という、いわゆる漏えい元基準で考えられているため、インシデントが生じた事業者が保有する情報・データに基づき特定の個人を識別できる場合には、漏えい等が生じたデータだけでは第三者が特定の個人を識別できない情報についても、漏えい等が生じたデータが「個人データ」に該当することを前提として本人への通知を行うことが必要となる[16]。この点については、平時から社内で周知し、個人データの漏えい等の発生時に円滑な対応を進められるようにしておくことが望ましい。

取引先への連絡

漏えいした情報に取引先の役職員らの情報が含まれていた場合、まずは本人通知の一環として当該取引先に連絡

[13] なお、実務上、連名で報告する場合で報告フォームに入力しきれない等の事情がある場合は、「(9)その他参考となる事項」で別途リストを提出する旨を記入した上で、個人情報保護委員会が指定する方法によりリストを提出することが想定されている。以下の、「クラウドサービス利用事業者の報告を、クラウドサービスの提供事業者が代行する場合の記入例」参照。
https://www.ppc.go.jp/files/pdf/kisairei_cloud_daikou.pdf

[14] 個人情報保護法ガイドライン（通則編）3-5-4-5

[15] 個人情報保護法ガイドライン（通則編）3-5-4-2 でも、このような場合には「その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して通知の時点を判断することが望ましい」としている。

[16] なお、本人通知の場面だけでなく、個人情報保護委員会への漏えい等の報告の要件該当性についてもこのような漏えい元基準を前提に考えるべきことにも留意が必要である。

することが一般的であると考えられるが、取引上の機密情報などが含まれている場合には、契約上の義務として取引先に対する通知義務が課されている場合がある。このため、初期調査の結果、取引先との取引上の機密情報等が含まれていることを把握した場合には、契約上の通知義務の有無とその範囲を検討する必要がある。

有事対応をみすえた平時における実務上のポイント

- ✓ 取引先との取引上の機密情報等が漏えいした場合、契約上の通知義務が発生するかの確認はもちろんのこと、取引先との間で損害賠償についての交渉をすることを想定し、契約上の損害賠償の予定に関する条項等を確認する必要がある。また、取引先に損害が発生することが想定される場合、その拡大を防止する（自社に対する取引先からの補償・損害賠償請求の範囲を限定する）ため、契約上の通知義務の有無に拘わらず、早急に状況を共有し、損害拡大防止に向けて協力することが必要となる場合も想定される。
- ✓ いずれにせよ、これらの確認を迅速に行うためには、事業部毎に管理している契約について、インシデント対応において確認することが想定される内容を事前に整理し、インシデント発生時には IT システム・セキュリティ部門と迅速に共有・参照できるようにすることで、これらの部門が把握する保有情報の被害範囲を踏まえた検討を容易にするなど、平時から準備しておくことが望ましい。

公表

個人データの漏えい等のインシデントが生じた場合、個人情報保護法上、「公表」は義務とはされていないが、事業者が保有する個人データの中に本人の連絡先が含まれていない場合など本人への通知が困難である場合には、本人への通知義務を果たすために、本人の権利利益を保護するために必要な代替措置として事案の公表をするといった対応をすることがある。また、このような代替措置として事案の公表を行わない場合であっても、当該事態の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、公表を行うことが望ましいとされている。

また、上場企業の場合には、これに加えて、証券取引所の上場規程において会社情報の適時開示に関して投資者の投資判断に著しい影響を及ぼす事実が発生した場合等に適時開示を行うべき旨を定めるいわゆるバスケット条項[17]、有価証券報告書上のリスク開示[18]、（株主総会を控えている場合）事業報告における報告[19]、さらには任意の開示実務[20]などを考慮に入れる必要がある。

有事対応をみすえた平時における実務上のポイント

- ✓ 非上場企業であって、法的な義務として公表義務が課されていない場合において、公表を行うことがかえって自社のレピュテーションを著しく毀損することが想定されるときには、個人情報保護法に基づく本人通知の代替措置として公表以外の方法を検討することも想定される。例えば、B to B の取引を行っているため、取引先である法人顧客の個人データは保有しているものの個人顧客の個人データは保有していないという場合には、当該取引先を通じた代替措置をとることにも相応の合理性があるものと思われる。
- ✓ いずれにせよ、公表等についての方針は、有事においてはレピュテーションの観点から論点になることも多く、基本的な方向性については、平時から、広報部門等の関連部門も含めて考え方のすり合わせをしておくことが望ましい。

コールセンターの設置・広報対応

インシデント対応においては、広範囲の情報漏えい等が発生した場合（例えば大量の個人データの漏えいが認められた場合など）には、専用のコールセンターを設けることにより、事案を対外的に開示・公表した後の個別の問い合わせに対応する場合もある。また、これに加えて、社会的に影響が大きい事案である場合には、報道機関、取引先、個人顧客や一般株主からの問い合わせや質問への対応が必要となる。この場合、予め、Q&A リストを作成し、回答先の属性に応じた適切な回答を統一的に行えるようにしておくことが望ましい。

有事対応をみすえた平時における実務上のポイント

[17] 有価証券上場規程（東京証券取引所）402 条 2 号 x など。

[18] 企業内容等の開示に関する内閣府令第三号様式記載上の注意(11)、第二号様式記載上の注意(31) a 等

[19] 会社法施行規則 120 条 1 項 8 号・9 号

[20] 適時開示や法令上開示の必要がない場合でも、被害拡大の防止やレピュテーション維持の観点から公表の要否を検討することもあり、被害拡大のおそれの程度や、公開することによりかえって被害が拡大するおそれの有無等も考慮しながらインシデントの事案の性質に応じて判断する必要がある。

- ✓ Q&A リストを作成する場合、その内容としては個別の事案により分かれるものの、大きく分けて、①事案の事実関係（事案の概要、発生原因、漏えいした情報の内容）と、②今後の対応（損害賠償等の本人や影響を受ける当事者への対応、当局対応）などが考えられる。Q&A リストの作成の際の留意点として、事実関係については、セキュリティの脆弱性やそれに対する是正状況についての情報が外部に出ないように表現振りには配慮する必要がある。
- ✓ また、今後の対応についても、事後に対応の方向性を修正するとなると関係者へのコミュニケーションの負荷がかかるため、関係部署において対応の方向性について十分にすり合わせできるように、平時から連携体制を整えておくことが望ましい。

(3) 警察への相談

ランサムウェア攻撃による不正アクセスにより被害を被った場合には、警察からの情報提供・助言を得るためにも警察署やサイバー犯罪相談窓口への通報・相談を検討することが望ましく[21]、また、従業者による情報の持ち出しの場合にも、不正競争防止法違反等に関する刑事告発を検討すべき場合がある。

有事対応をみすえた平時における実務上のポイント

- ✓ 企業として適切な事案対応をしているということを対外的に示す上でも警察への相談は重要であり、従業者による情報の持ち出しのような場合には対内的にも厳正に対処していることを示す意味でも重要である。
- ✓ また、この点にも関連して、インシデントが発生した場合はもちろんのこと、それ以外にも情報セキュリティについての社内手続違反などのサイバーセキュリティリスクにつながりうるような事案について、平時より厳正な社内処分を行うと共に従業員に対して注意喚起していくことも重要といえる。

まとめ

上記では、ランサムウェア攻撃による不正アクセスの場合と従業者による情報の持ち出しの場合を念頭に、初期調査と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特に論点になりうる実務上のポイントを紹介したが、有事の際には、初期調査を迅速かつ適切に行うと共に、当局対応やそれ以外の多岐にわたるタスクを同時並行で行う必要があり、各プロセスにおいて優先順位の判断、優先性を踏まえた社内リソースの配分、外部専門家の利用とその範囲といった判断を迅速・適切に行って（状況に応じて修正して）いく必要がある。そして、有事対応においてこれらの判断を迅速・適切に行うためには、平時から準備しておくことが必要になるため、有事をみすえた平時の実務上のポイントとして記載した点について、社内で対応できているかについてはぜひご確認いただきたい。

次回の本テーマのニュースレターでは、引き続き、ランサムウェア攻撃による不正アクセス事案と従業者の持ち出し事案を素材として、ランサムウェア攻撃に特有の攻撃者からの金銭の支払要求への対応、損害賠償対応、原因分析をふまえた再発防止策の検討・実施について紹介する。

2024 年 7 月 4 日

[21] 例えば、警察庁は、2024 年 2 月に、ランサムウェア LockBit による暗号化被害データに関する復号ツールの開発をしたと公表している。https://www.npa.go.jp/news/release/2024/release2.pdf

[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）