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

2025年8月　No.110

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の近時の動向（3）　～DDoS・ランサムウェア攻撃におけるインシデント報告様式の統一化等～

弁護士　工藤　靖

はじめに

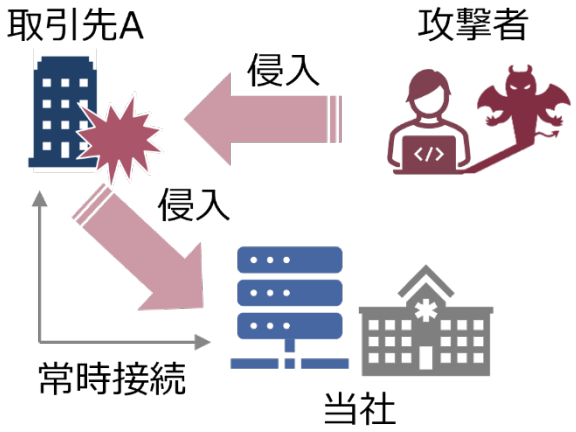
前回のニュースレターでは、取引先等のシステム・セキュリティ上の脆弱性が攻撃者に悪用され、何らかのネットワークによってつながれた自社システム上で生じるセキュリティリスクや、取引先等における事業停止等により生じる自社の事業リスクへの対応について、設例を用いて取引先・委託先が実施すべきセキュリティ対策上の水準や要求事項のほか、セキュリティ対策の実施状況に対する検証を可能にするための資料提出や監査への協力について解説しました。今回のニュースレターでは同様の設例を用いて、再委託先等の管理策、インシデント対応における留意点等について解説します。

［設例］の再掲

(1)　攻撃者は、**取引先 A のシステム構築事業者がリモート保守のために設置した VPN 機器の脆弱性**を利用して取引先 A のシステムに侵入した。

(2)　**取引先 A のデータセンターの ID・パスワードの設定が脆弱**であったため、攻撃者は不正アクセスが可能となり、取引先の端末から当社のサーバ認証情報も窃取した。

(3)　攻撃者は、**取引先 A と当社が常時接続のリモートデスクトップ通信で結ばれていた**ことから、取引先 A の端末から窃取した当社のサーバ認証情報を利用して、当社サーバに侵入し、ランサムウェア攻撃を実施した。



1　サプライチェーン上の取引先・委託先管理上の問題点について

上記の設例では、当社→取引先 A→システム構築事業者というサプライチェーンの中でサイバー攻撃が行われていますので、取引先・委託先との契約上の規律においては、その先にいる再委託先や取引先に対する部品納入業者等の管理の問題も生じます。これらの管理は、サプライチェーンにおけるサイバーセキュリティの確保という観点からは、ますます重要になっています。2024 年 10 月、米国の National Institute of Standards and Technology（NIST）が初期公開のドラフトとして公表した SP1326「サイバーセキュリティ サプライチェーンリスクマネジメント：デューデリジェンス・アセスメント・クイックスタートガイド」でも、サプライチェーンの階層構造を明らかにすることが重要であり、それを樹形図のような形で可視化すべきであると言及されている一方で、その階層が重なるほど対応の難易度とコストは指数関数的に高まるとされています。そのため、どのようにセキュリティ対策の水準を明確化しその遵守状況の可視化を高めていくかは重要なポイントになります。再委託先や取引先に対する部品納入業者等との間には契約に直接的に拘束力を及ぼすことはできません。例えば、再委託先に対する管理については、再委託を同意事項とし、同意に際して再委託先におけるセキュリティ対策の実施事項等を確認するといった対応が一般的です。

1.　経済安全保障推進法における基幹インフラ制度上のリスク管理措置

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（同法第 3 章）は、電気、ガスなどの特定の基幹インフラサービスの安定的な提供のため、海外からのサイバー攻撃など基幹インフラ事業を阻害する行為に対する対応として、特定社会基盤事業者を指定し、その事業の用に供する重要な設備、機器、装置等（特定重要設備）の導入を行う場合や、他の事業者に対してこれらの維持・管理等を委託する場合には、原則として予め計画書を提出し、主務大臣による審査を受けることが必要となります。この事前審査対象となる計画において、特定社会基盤事業者は一定のリスク管理措置をとることが求められています。このリスク管理措置の実施に際して、特定重要設備の供給者やその維持管理の委託先との間で締結する契約において、当該供給者の取引先（構成設備の供給者）や当該委託先の再委託先との関係でも一定の手当をすることが推奨されています。例えば、参考規定案類型 I の第 7 条解説では、当該供給者や当該委託先が特定社会基盤事業者又は主務大臣に提出する当該供給者の取引先や当該委託先の再委託先に関する情報の正確性を担保するため、これらの者と直接の契約関係にある当該供給者や当該委託先が、当該供給者の取引先や当該委託先の情報の正確性を表明保証させる仕組みを構築することが挙げられています。また、同第 8 条解説では、リスク管理措置[1]について当該供給者の取引先や当該委託先の再委託先からの協力が必要となることも想定され、これらの者と直接の契約関係にある当該供給者や当該委託先が、当該供給者の取引先や当該委託先の再委託先に特定社会基盤事業者によるリスク管理措置の実施に協力することを定めた場合が挙げられています。このような契約上の手当は、特定社会基盤事業者に限らず、広くサプライチェーンにおける取引先・委託先の先にいる再委託先や納入業者等の管理における契約上の手当について参考になるものと考えられます。

2.　日本自動車工業会（JAMA）及び日本自動車部品工業会（JAPIA）によるセキュリティガイドライン

このようなサプライチェーンにおける再委託先や取引先に対する部品納入業者等におけるセキュリティ対策状況の可視化・遵守の実効性を高める自主的な取り組みとして、日本自動車工業会（JAMA）及び日本自動車部品工業会（JAPIA）が共同で策定したセキュリティガイドラインが挙げられます。これは業界自主規制の位置づけにはなりますが、サプライチェーンを意識し、実施すべき項目を、最低限実装すべき項目、標準的に目指すべき項目、到達点として目指すべき項目、の 3 つのレベルに分け、関係する会社の規模や位置づけに合わせて選択するようになっています。このようなサプライチェーン上の会社の規模・位置づけに合わせたセキュリティ対策のレベル分けとその実施は、業種を問わず参考になるものと思われます。

[1] 例えば、不正な変更防止措置（悪意のあるコードの混入防止、情報セキュリティ要件の実装、品質保証体制の確立、製造工程における不正な変更の確認、製造環境へのアクセス制限等）、保守・点検等に関する措置（故障対応や脆弱性対応等のサービス保証の実施）、不正な妨害の兆候把握体制（アクセス制御、不正アクセス監視）、法令・基準遵守状況の確認（国内関連法規や国際的に受け入れられた基準の遵守状況の確認）等が含まれます。

2　サプライチェーンにおけるインシデント対応上の留意点

セキュリティインシデントが発生した場合の対応においては、①関連する当局に対する報告やその他開示が必要となり、②これらの準備のためサプライチェーン上の各当事者間において行われる情報共有を想定した合意をしておくことが望ましいものと考えられます。

1.　インシデント報告先の一元化や報告様式の統一化等

まず①については、近時サイバー攻撃による被害報告件数は増加の一途を辿っており、報告先となる政府機関が多岐にわたるため、被害組織に過度な報告負担がかかっているという課題が指摘されていました。これを受けて、2024 年 11 月 29 日付け「サイバー安全保障分野での対応能力の向上に向けた提言」では、被害組織の負担軽減と政府の対応迅速化を図るため、インシデント報告先の一元化や報告様式の統一化等を進めるべきであることが提言されています。そして、2025 年 5 月 28 日、関係省庁は「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」を策定し、特にインシデント発生時からサイバー攻撃であることが明白で、初動対応中の報告となり件数も多い DDoS 攻撃事案とランサムウェア事案について、共通様式が先行的に導入されることとなりました。これにより、被害組織は、個人情報保護法に基づく個人情報保護委員会への報告、警察への相談、及び電気通信、金融、電気といった重要インフラに関する業法・各種ガイドラインなどに基づく報告に際して、それぞれの共通様式の利用が可能となります。これらの共通様式には、報告者の概要、業務への影響、影響を受けたシステム、事実経過（時系列）、攻撃技術情報（分類、通信プロトコル、送信元・送信先情報、通信量、ランサムウェアの特徴など）、公表状況、今後の対応などが含まれます。これらの共通様式に基づいて報告を受けた官公署は、報告者の同意がある場合に、当該内容を国家サイバー統括室に共有し、国内で発生しているこれらの事案の情報を集約し、国家サイバー統括室は集約された情報を整理・分析し、被害者が特定されないようにした上で、被害拡大防止のための注意喚起などに活用することになります。なお、「重要インフラのサイバーセキュリティに係る行動計画」に定める重要インフラ事業者等が報告者である場合は、その同意の有無にかかわらず国家サイバー統括室に共有される場合があるとされています。

そして、将来的には、重要電子計算機に対する不正な行為による被害の防止に関する法律（いわゆるサイバー対処能力強化法）第 5 条の施行により、同法に定める「特別社会基盤事業者」に対するインシデント報告が義務化されますが、この報告義務に基づき、共通様式による報告が行われる場合の窓口を一元化するよう調整を進める計画です。

この DDoS 攻撃事案共通様式とランサムウェア事案共通様式を用いた報告についてはパブリックコメントに付され（2025 年 8 月 9 日付けで受付終了）、必要な修正等を経て、令和 7 年 10 月 1 日から適用される予定です。

なお、個人情報保護法における漏えい等の報告（個人情報保護法第 26 条 1 項）において、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、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になりますが、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ます（個人情報保護法第 26 条 1 項ただし書き）。ただ、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、委託元及び委託先の連名で報告することも許容されていました（個人情報保護法ガイドライン（通則編）3-5-3-2）。このような実務的な対応が、上記の報告様式の統一によりどのように整理されるかも注視する必要があるものと思われます。

2.　インシデント対応におけるジレンマ

次に②について、システムの運用・保守・管理や自社情報の取扱いに関する委託先、クラウドサービスの提供者、取引先等においてインシデントが発生し、自社の業務への影響や保有情報の漏えいが発生した場合、これら委託先・取引先からのインシデント発生状況やその原因等に関する情報提供が、自社における①の報告や開示に不可欠になります。この場合、実務的には、インシデント発生状況と、その原因分析・再発防止の対応状況に関する情報共有

を受け、当局報告・開示に備える必要がありますが、これらの内容は委託先や取引先等にとっては自らの帰責事由の評価につながる可能性は否定できません。そのため、相手方に対する補償も意識して情報共有が行われることになります。相手方が重要インフラを担う会社であり、関連する業法やガイドラインにより監督官庁への報告義務を負担している場合、実務的には当該監督官庁から直接的又は間接的に原因や再発防止の説明を求められることがあり[2]、その説明内容に関して当事者間において一定の緊張関係が生じることも否定できません。このような観点からも、予め責任範囲を明確化しておくことやサイバー保険による危険の移転を図っておくことは検討に値します。

3　最後に

以上、今回のニュースレターでは再委託先等の禁止又は制限・管理策、インシデント対応や責任分担の明確化等について解説しました。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への対応は、DX 化や IoT 化の進展に伴うシステム連携の増加、及びサイバー攻撃の高度化・巧妙化により、益々対応が困難となっており、サプライチェーン全体でのセキュリティ対策の水準の明確化と可視化が業種を問わず求められています。前々回及び前回のニュースレターとあわせ、今回のニュースレターがそのような対応の参考になれば幸いです。

[2] 例えば、金融庁は、銀行法第 24 条 2 項・同第 25 条 2 項等の関連業法に基づく権限を根拠として特に必要があると認めるときは、その必要の限度において、外部委託先に対しても、報告徴求命令の発出や立入検査を実施する権限等を有している。

[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.）。

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

渡辺 翼　パートナー
tsubasa_watanabe@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、600 名以上の弁護士が所属する日本有数の総合法律事務所として、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ています。東京、ニューヨーク、上海、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及びロンドンに拠点を構え、多種多様なニーズに迅速かつきめ細やかに対応する体制を整えており、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）