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.109

# 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（2）　～サプライチェーン全体でのサイバーセキュリティ強化に向けたサプライチェーン対策評価制度の整備等について～

弁護士　工藤　靖

## はじめに

前回のニュースレターでは、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管理の近時の動向として、SBOMの作成・利用を通じたシステム・ソフトウェアにおける脆弱性への対応についてご紹介しました。

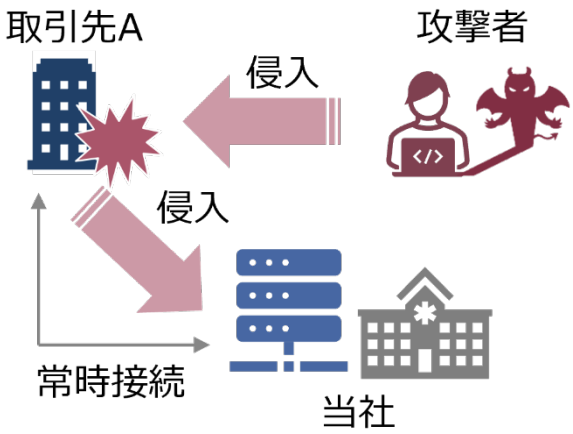
今回のニュースレターでは、取引先等のシステム・セキュリティ上の脆弱性が攻撃者に悪用され、何らかのネットワークによってつながれた自社システム上で生じるセキュリティリスクや、サイバー攻撃によって発生した取引先等における事業停止等により生じる自社の事業リスクへの対応について、設例を用いて解説します。

## 1　設例

(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。




上記の設例において、取引先Aや当社における技術的な管理措置として、どのような対応が考えられたかを検討

しますと、まず、取引先 A においては VPN 機器の脆弱性対応やその診断を実施していることが重要であったと考えられます。前回のニュースレターでも紹介しました、警察庁が 2025 年 3 月 13 日付けで公表した「令和 6 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」においても、VPN 機器の脆弱性を狙った攻撃によるランサムウェア被害の割合は有効回答中の約 6 割を占めており、慎重なセキュリティ対応が求められます。また ID/パスワードについても、重要なシステム・ネットワークであれば、より一層厳重なログイン管理・運用が求められていたものと考えられます。

また、上記の設例ですと、最終的には当社は、リモートデスクトップ通信からの侵入により被害を受けています。そこで、多要素認証化し不正ログインの可能性を少なくする、仮に認証成功されたとしても、その認証成功・失敗状況を記録し、可能であればリアルタイムに監視し、予定されていた作業と一致した挙動であるか確認するなどにより対応しておくことが考えられます。また、接続元となる取引先 A の端末のセキュリティレベルなどを事前にヒアリングし、自社と同等レベルのセキュリティ対策を求めるといった対応も考えられます。

上記を踏まえると、当社として取引先 A に対して、どこまで踏み込んだ対応を求めるべきであったかという問題につながっていきます。当社が取引先 A に対し、必要と考える一定の対応を求めるには、契約により合意し、その条項においてセキュリティ対策上の具体的な要求事項を定めておく必要があります。取引内容・委託内容に照らして検討する必要がありますが、一般論としては、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エビデンスの提出や監査への協力、サイバー保険の付保、再委託の禁止又は制限・管理策、インシデント対応や責任分担の明確化、契約期間中に関係するシステム等に脆弱性が確認された場合には情報を共有し対応について協議すること、などが考えられます。

## 2　取引先・委託先に対して求めるセキュリティ対策等と一定の制約

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に合意し、その実施状況に対する検証を可能にするためにエビデンスの提出や監査協力を求める場合、実務的には一定の制約があります。

すなわち、取引先や委託先に対して一定のセキュリティ対応を求めるにあたっては、私的独占の禁止及び公正取引の確保に関する法律（いわゆる独禁法）上の優越的地位の濫用や下請代金支払遅延等防止法（いわゆる下請法）の規制にも注意が必要となります。経済産業省・公正取引委員会は、「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」を公表しており、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を要請する一方で、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、②セキュリティ対策費などの名目で金銭の負担を要請するなどして、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、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などには、上記規制上の問題になりえます。このため、実務上の対応としては、委託先等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・協議を行い双方の負担を合意する、これらの説明・協議のプロセスを適切に記録化（議事録・説明資料の保管等）しておくことなどが肝要です。

なお、本年 5 月、下請法の改正が成立し、改正法は 2026 年 1 月 1 日から「製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律」に名称変更の上で施行されます。同改正により、新たな委託事業者の禁止事項として、協議を適切に行わない代金額の決定の禁止が追加されました[1]。本号は、従来から親事業者による下請代金の一方的な減額や買いたたきが禁止されていたものの、コスト上昇局面における価格転嫁等に対する問題意識があったことから導入されることとなりました。従来から、公正取引委員会は、下請法の運用上、コスト上昇局面における価格転嫁に関する必要性について明示的に協議せず、又は、下請事業者からの価格引き上げ要請について理由も示さずに従来通り価格を据え置く行為は買いたたき行為に該当すると解釈しており、その意味においては、従来から上記行為は規制対象であったとも考えられます。しかし、本号の追加により禁止行為として

[1] 「中小受託事業者の給付に関する費用の変動その他の事情が生じた場合において、中小受託事業者が製造委託等代金の額に関する協議を求めたにもかかわらず、当該協議に応じず、又は当該協議において中小受託事業者の求めた事項について必要な説明若しくは情報の提供をせず、一方的に製造委託等代金の額を決定すること」（改正法第 5 条 2 項 4 号）

法律上明確化されたことから、今後、公正取引委員会がこの種の行為に対する法執行を厳格に行うこととなる可能性は否定できない点に留意が必要です。

## 3　セキュリティ対策のモニタリング上の制約について

また、セキュリティ対策上の水準や要求事項の合意に至った後の検証や監査については、①セルフチェックリストを送付し回答を求める、②外部監査法人等によるセキュリティ監査を実施している場合は、その監査報告を確認する方法などがありますが、①は正確なリスク把握ができないおそれがあり、②はそのような外部者によるセキュリティ監査を強制することまではできないという問題点があります。

こうした中で、関係当局や自主規制団体は、サプライチェーン全体でのセキュリティ水準の向上と、そのセキュリティ対策の実施状況の可視化の推進を目的とするガイドライン等を公表しており参考になります。

経済産業省は、サプライチェーン全体でのサイバーセキュリティ強化に向けたサプライチェーン対策評価制度の整備を進めています[2]。サプライチェーンを通じた情報漏えい・事業中断のリスクが深刻化しており、中小企業を含む受注側に過重なセキュリティ対応要求が発生している中で、発注者側も取引先の対策の実施状況が不明確な状況にあることを背景としています。現時点では中間取りまとめが公表された段階ですが[3]、自社の IT 基盤（オンプレミス＋クラウド環境）を中心としたサプライチェーン企業（特に中小企業）を対象組織として、★3：基礎的な対策（自己評価）、★4：包括的な標準対策（第三者評価）、★5：到達点として目指すべきベストプラクティスに基づく対策（第三者評価）の評価段階を設けることが想定されています。対策には、経営責任、サプライチェーン防御などが盛り込まれ、要求事項の具体例として、ネットワーク境界管理、アクセス権管理、パッチ適用などランサムウェア対策の基本措置も掲げられており、ISO27001 や海外の情報セキュリティ制度との整合性を持たせる形式でのベンチマークが検討されています。この制度の活用を通じて、発注企業にとっては取引先の対策状況を把握しやすくなり、サプライチェーンに起因するリスクを低減することを可能とし、受注企業にとっては自社がとるべき対策水準が明確となり、セキュリティ投資と説明責任を果たすことが可能となります。

## 4　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に関する関連ガイドライン

経済産業省は、事業の性質上、安定供給・稼働が要求されることからその利用を停止させることが基本的には想定されていないビルシステムや、工場・プラント、発電所等を保有・利用する業種に関するサイバーセキュリティ対策に向けたガイドラインも公表しています。これらのガイドラインは、同種の施設を保有・利用する業種や、同様の性質を有するシステムを保有・利用する事業者にとって参考になる対応が含まれています。

まず、ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（第 2 版）は多種多様な関係者（マルチステークホルダ）が関与していることを背景に、サプライチェーンを構成する各関係者が共通して参照できるサイバーセキュリティ対策の指針として策定・公表されています。

次に、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインでは、工場システムは IoT 化や自動化の進展に伴いネットワーク接続の機会が増加しており、サイバー攻撃のリスクが増大していることから、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的としてガイドラインが策定されています。このガイドラインでは、「サプライチェーン対策」という独立した項目を設けており、その重要性を強調し、対策として、「取引先や調達先に対するセキュリティ対策の要請、対策状況の確認」などが挙げられています[4]。そして、現在、様々な業種の中でも、半

[2] ワーキンググループ 1（サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html
[3] サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20250414_report.html
[4] 契約開始時や定期的なセキュリティ教育、脆弱性情報の迅速な共有、サプライチェーンにおける脅威や影響度、対応状況の把握が含

導体産業の経済及び安全保障上の重要性やサイバー脅威/リスクの高まりを踏まえ、重層的なサプライチェーンにより成り立っている半導体産業における安定供給を維持するため、高度なサイバー攻撃に対するサプライチェーン全体でのセキュリティ対策の指針を示すことを目的として、半導体デバイス工場における OT セキュリティガイドライン（案）が検討されています[5]。このガイドラインの対象には、半導体デバイスメーカーの製造部門だけでなく、製造装置メーカーや素材メーカーの製造部門も含まれます。その中では、デバイスメーカーと装置メーカーの間のセキュリティ連携強化が求められており、「既存の装置ツール調達プロセスにおける調達仕様書及び運用時の保守契約書に、セキュリティ要件（SEMI E187/E188 Capability Requirements 等）を追加することが重要である」とされています。

また、電力制御システムに関するサプライチェーンリスクに対するサイバーセキュリティ対策を支援・促進することを目的として、電力制御システムに関するサプライチェーン・セキュリティ対策の手引きが策定されています[6]。「電力制御システムのサプライチェーンリスク」とは、電力制御システムが電気事業者に納入されるまでの開発や製造に関する一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般におけるサイバーセキュリティ上のリスクを意味します。具体的な事例として、ネットワークスイッチの偽造品に不正プログラムが埋め込まれていた事例や、半導体の偽造品流通の増加が挙げられています。この手引きの対象には、電力制御システムを運用する電気事業者に加え、「委託先等」（委託先、再委託先、発注先、すなわちサプライチェーンに関係する全事業者）が含まれるとされ、「サプライチェーンリスク管理」として、委託先等の役割と責任範囲の明確化、サプライチェーンの依存関係と委託先等のセキュリティ対策状況の把握、及びリスク管理の実施が求められています[7]。また、「セキュリティ仕様の確認」として、電力制御システムの調達時にセキュリティ仕様を明確にし、その準拠性を確認すること、及び仕様変更時の適切な管理が重要とされ、不正プログラム対策の管理や感染防止機能の要件化が推奨されています。そして、「機器の適切な管理」として、機器のライフサイクルを通じて管理・保護することが求められ、これには、機器の選定・設置、管理者・利用者の登録、データバックアップ、故障対応、廃棄方法、保存データの抹消までが含まれるとされています。

これらのガイドラインは、それぞれの産業分野の特性（ビルシステムにおける多種多様な関係者（マルチステークホルダ）による関与、半導体工場の国家安全保障上の重要性、電力制御システムの社会基盤性など）を踏まえつつ、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管理の重要性とその具体的な対策の方向性を示しています。特に、ライフサイクル全体にわたるセキュリティ要件の明確化、サプライヤーとの連携、そしてインシデント発生時の迅速な対応と情報共有の体制構築は、これらの産業分野に限られず、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として一般的に参考になるものと考えられます。

## 5　最後に

今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、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サイバー攻撃により発生した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エビデンス提出共有や監査への協力等について解説しました。次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、インシデント対応等について解説します。

---

まれています。

[5] https://www.meti.go.jp/press/2025/06/20250627009/20250627009.html

[6] https://www.meti.go.jp/press/2025/06/20250603001/20250603001.html

[7] この中で、発注先・委託先の選定基準として、管理体制の構築、インシデント発生時の連絡体制、再委託の制限、従業員教育、意図しない変更が行われない管理体制、不正変更時の追跡調査協力、外国の法的環境による契約違反の報告などが具体的に挙げられています。

[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）