

2026 年 10 月 5 日 SSL 研究プロジェクト

神橋論文「サプライチェーンセキュリティ（SCS）に関するダブルループ・フレームワークの提案」に対する感想と独禁法観点からの検討

金子啓子

1. 初めに

前回の SSL で、神橋先生から、標記論文が提示された。報告者の理解では、ポイントは以下の 2 点である。

- (1) 従来のアプローチ（Static SCS）では、特定時点のセキュリティ状況しかわからず、また、自己評価の場合が多く、故意かどうかは別として、嘘をつかれる可能性がある。そこで、常時システム的にシステムの設定状況や不正アクセスリスクへのシステム的な対応状況などをモニタリングしてエビデンスを取り、要求される対策ができているかを自動的に評価するシステムを提案。
特に、個別企業内では、ゼロトラスト原則に基づき、動的なアクセス制御と即時的な機能回復を重視。（ミクロループ）
- (2) Society 5.0 や Cyber-Physical Systems（CPS）で提唱されているように、現代では、多様かつ多数の組織、サービス、IoT/OT 機器、API などが物理空間とサイバー空間を跨いで相互に動的に接続し続けるエコシステムを形成している。この状況に対するサプライチェーンセキュリティは、Static SCS では間に合わないため、①のアプローチが必要であり、異常を検知すればすぐに切断することができる制度を提案。（マクロループ）

(1)については、社内のセキュリティガバナンス、リスク把握にも有益であろう。現在、シャドウ IT も含めて、網羅的にシステムを設定なども含めてモニタリングできるシステムがあるのか、モニターした結果に基づいて自動的に遮断したり是正するシステムがあるのか、運用はどうなるのか、それがどのくらいのコストがかかるのか、など、報告者はわからないが、EDR・XDR などがそれにあたるのかもしれない。

神橋先生から、独禁法上の懸念が示されたが、それは、むしろ他の事業者との関係になる(2)の点にあると思われる。

サプライチェーンのセキュリティ、と言っても、CPS のようなシステムが相互に動的に接続し続けるエコシステムのようなものから、個人情報の処理の委託や町工場に営業秘密を渡して物を作ってもら場合まで、幅が広い。(2)の要請がその事業にどの程度必要なのか、によって、判断も異なる。そこで、以下のように分類して独占禁止法のフレームワークを見つつ、検討してみる。

① 部品製作→ユニット製作→完成品製作など、取引自体は本質的にシステム接続が必要ではないが、管理能力の向上、事務量の軽減、事務の迅速化等の業務工程の見

直しによる効率性の向上のため、EDIなどで接続している場合
(垂直型)

②本質的にシステムを接続することが必須であるサプライチェーン (垂直型)

③ 銀行決済システムなど、同業者が、現実的には本質的にシステムを接続したプラットフォームを利用せざるを得ない取引 (水平型)

④ CPSのようなシステムが相互に動的に接続し続けるエコシステムのようなもの (水平型+垂直型)

なお、製造委託先に開示した営業秘密を守るために、オフラインも含めたセキュリティを要請するケースは、神橋提案とは無関係か、①に該当するので、今回は対象外とする。

2. 独占禁止法等の関連規範

独占禁止法の目的は市場における企業活動の公正かつ自由な競争の促進であり、主な禁止類型は、不当な取引制限・不公正な取引方法・私的独占である。また、不公正な取引方法には、17¹の禁止行為類型が定められており、その一つである優越的地位の濫用と、その下位の法律である中小受託取引適正化法（旧下請法 以下取適法という）が、まずは本件のようなケースには関係すると思われる。

過去、実務家の中では、中小企業にサイバーセキュリティ対策を要請することに対し、優越的地位の濫用や取適法違反となる懸念から迷いがあったが、中小企業へのサイバー攻撃から取引先にも影響することなどから、2020年から公正取引委員会と中小企業庁は、指針となる発信をしており、大変参考になる。²

¹ 独占禁止法2条9項と一般指定を併せて重複するものを引いた数

² 2020年下請中小企業振興法 振興基準改正で、「下請事業者は、管理能力の向上、事務量軽減、事務の迅速化等の業務工程の見直しによる効率性の向上のため、必要なセキュリティ対策と合わせて、次の事項に積極的に対応していくものとする」と下線部分が追加され、自ら行うべきものであることが明示された。また、親事業者の支援協力義務も定められた。

2022年経済産業省・公正取引委員会共同で、「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、丁寧な説明、適切な要求水準、費用発生を前提とした取引価格交渉への対応、自己の指定する商品の購入やサービスの利用の要請などをしないこと、など、指針を示している。
https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

特に、2025 年に公表された「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た想定事例及び解説」は大変参考になる。

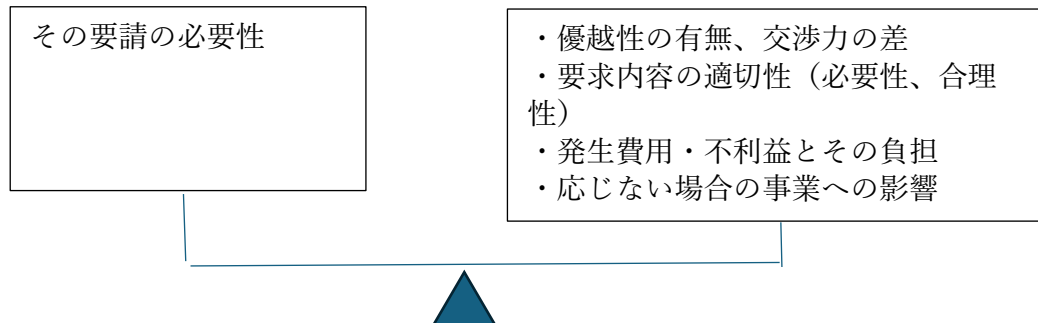
観点としては、

- ・ パートナーシップの構築
- ・ 必要性についての丁寧な説明（サプライチェーンを通じたセキュリティの維持など）
- ・ 適切な要求水準（SCS 評価制度は、必要性、合理性がある）
- ・ 費用発生を前提とした取引価格交渉への対応（一応、セキュリティ確保は経営者の責任、としているため、一方的に要請者の負担を求めるわけではないが、価格転嫁について、真摯に交渉に応じることを要請）
- ・ お助け隊や経産省の補助金制度の紹介など適切な助言

が挙げられ、下記のような場合など、要請の方法や内容によっては優越的地位の濫用となる、とされている。

- ・ パートナーシップを構築せず一方的に要請
- ・ 合理的な必要性がないのに対策を強制
- ・ 特定の商品・サービスの購入を義務付ける

これを基準として、下記のように衡量して分析することができると思われる。



3. 検討

1. で述べた③、④については、問題があったときの社会的な影響も大きく、必要性が高いため、これらの要請は優越的地位の濫用で問題になることは考えにくい。

更に、2025 年、この指針の「想定事例及び解説」を示し、問題とならない想定事例をわかりやすく解説している。https://cms03.jftc.go.jp/security_jirei.html

また、参加者もマイクロループ構築にある程度コストをかけることができる事業者であると考えられる。

もちろん、そのために必要な範囲から切り離された、全社的なマイクロループを対象にすることは、必要な範囲を超えるものとして、問題になり得る。また、マイクロループを総括した結果だけでなく、各システムの設定や利用状況までは提供させる場合は、その必要性が問題となる。技術的に総括した結果が出せない、などの場合にはやむを得ないのかもしれないが、その場合の機密保持、目的外利用の禁止、実際にどう管理するか、などを決めておく必要がある。無用な情報の提供を甘受しなければ、そのプロジェクトに参加できない、となると、その点での優越的地位の濫用の問題が生じ得る。

②のケースについて、通常の物の売買、製造委託のサプライチェーンにおいて、売買契約自体はシステム接続が必須ではない。しかし、看板方式のシステム化のような、ビジネスの観点から本質的にシステムを接続することが必須である場合を想定した。社会的インパクトの大きい③、④ほど、マクロループ方式を取る必要性はないが、小島プレス事件のように、そのサプライチェーンに与える影響は大きいため、ある程度、必要性は認められる。この場合、中堅・中小企業にマイクロループを実現するための費用を負担できるか、が問題となるが、この場合こそ、価格転嫁が説得力を持ち、その転嫁を受けてでもそのようなシステムにして高速に受発注することが妥当かどうかを、それを主催する会社が判断することになる。

①のケースは、現実には不正アクセスやマルウェア感染が発生した場合に切断することは考えられるが、社内のシステム設定状況を動的・自動的に監視し、その結果を動的に把握して自動的に切断するところまでの必要性は、現在のところないのではないか。マイクロループ構築・運用の費用にもよるが、単なるセキュリティ対策より高額と思われ、それを価格転嫁を受けてまで、マクロループを構築しようというコンセンサスが発注側企業群で得られるとは思えない。ただ、何もない所からマイクロループを作る方がリープフロッグ的にあまり変わらない費用で可能である、ということであれば、可能性はあるかもしれない。

水平型については、すべての同業者の取決めを独禁法違反とするのではなく、競争領域と協調領域、という概念で判断している。不当な取引制限（カルテル）として取り上げられるのは競争領域であり、基本的に、価格、数量、地域など、いわゆる本業の競争要素について合意があって競争を妨げることに繋がる場合である。その他の取決めは、効率化などにより、より多様な商品・サービスの登場を促すなどして結果的に競争が促進される場合がある、との捉え方で、その競争への影響などを分析して判断する。これをわかりやすくするために様々なガイドラインを出し、また、事前相談なども受け付け、Q&Aが公開されている。本件のような、システム接続やその条件は協調領域に属する。従って、競争者がマイクロループの詳細を見ることができ、それが何らかの形で本業の競争要素が推測され得るのであれば、問題となる可能性はある。

むしろ、不合理なセキュリティ要件を定め、これを満たさなければ接続できず、結果的にその事業に参入できない、などがあれば、不公正な取引方法の一つである共

同ボイコットになる可能性はある。もしも、経済安全保障上の理由などで、参入を制限する必要があるシステム・ネットワークであれば、政府によるアクションによって、可能とする必要がある。独禁法が厳しく活用されている米国においては、政府の法令などによる場合は、独禁法上免責されるという State Action Doctrine がある。日本でも独禁法にかつて事業法令に基づく正当な行為を免責する包括的な条文があったが、規制緩和の流れの中で削除されている。しかし、他の法令によって別の観点から規制され、その結果、競争が制限されることは正当行為と言えるだろう。昭和 59 年の最高裁判決で、行政指導による価格カルテルが正当化できないことが明確になった。やはり、法律的な根拠が必要であろう。

4. 接続を切断する行為について

契約上、一定のセキュリティレベルを要求し、この動的なモニタリングによってそれを満たさないことを検知した場合には切断する旨を定めているのであれば、問題はないと思われる。

ただ、切断自体は契約上可能であっても、それを理由に取引自体を解消する場合については、より、本業の競争に与える影響が大きいため、独禁法上は、取引停止の判断が合理的かつ公正かどうか、が問題となる。その際、取引の内容から見て、システム接続の要求を満たさないことだけで解消すべき取引か、その要求が必要、適切であるか、十分な説明があったか、取引停止に至るまでに改善の機会を与えたか、などのプロセスが判断されることになる。

以上