Outcome-basedアプローチを活用したサプライチェーンのセキュリティ対策

Supply Chain Security Measures Using Outcome-based Approach

福田　有希　　河村　勇　　窪田　好宏　　綿口　吉郎

あらまし

近年，サプライチェーンのセキュリティ対策が不十分な企業や組織を狙ったサイバー攻撃の増加や，各国独自のセキュリティ規格制定によって，企業や組織におけるセキュリティ対策の負担が増加している。従来のサプライチェーンのセキュリティ対策では，この負担増加に対応できているとは言い難い。このような状況に対して，富士通は一部のセキュリティ規格の制定元や標準化団体などで利用が広がりつつある「Outcome-basedアプローチ」を活用することで，サプライチェーンのセキュリティ対策に貢献できると考えている。本アプローチは，セキュリティ対策で達成される結果のみを要求事項として記載し，その達成方法である具体的なセキュリティ対策の選択は対策元に委ねて進めていく。これにより，サプライチェーンに関わる委託元・委託先双方の負担軽減などのメリットが得られると考えている。

本稿では，本アプローチの導入方法やメリットについて紹介する。

Abstract

In recent years, the increasing cyberattacks targeting companies and organizations that have supply chains without sufficient security measures and the fragmentation of security standards in various countries, e.g. similar but not identical and/or sometimes conflicting, have caused an increase in the burden of security measures on companies and organizations. Conventional supply chain security measures can hardly resolve the adverse effects of this fragmentation. To deal with this situation, Fujitsu thinks that it can contribute to supply chain security measures by making use of the outcome-based approach, which is increasingly being used by some regulators and standardization organizations. In this approach, only the results to be accomplished by security measures are specified as requirements, and the selection of the specific security measures is left up to those taking the security measures. This will provide benefits that include a reduction in the burden on both purchaser and suppliers involved in supply chains. This paper presents the method of introduction of this approach and its benefits.

1. まえがき

IoTやAI（人工知能）といった技術をベースとしたデジタルビジネスの拡大によって，あらゆるモノやサービスがネットワークに接続される「つながる社会」が実現されつつある。これによって，様々なデータの授受やサービスをボーダレスに享受可能な時代となった。

その一方で，高まるセキュリティリスクへの対応やプライバシー侵害への対策などを目的としたセキュリティ規格，基準，ガイドラインなど（以下，セキュリティ規格）の整備が各国で進んでいる。しかし，この状況がグローバルでのセキュリティ規格増加をもたらし，様々な場面で混乱を招いている。

その影響を受けているのがサプライチェーンである。サプライチェーンがグローバルに広がることで，複数のセキュリティ規格への対応が求められており，企業の負担が増加しつつある。

このような状況を踏まえて，富士通はサプライチェーンのセキュリティ対策を向上させるために，Outcome-basedアプローチの活用を検討した。Outcome-basedアプローチはグローバルに増加するセキュリティ規格への負担軽減を目指し，一部のセキュリティ規格の制定元や標準化団体などで利用が広がりつつある。

本稿では，サプライチェーンが抱える問題や従来のセキュリティ対策の課題を示し，富士通の提案するOutcome-basedアプローチの導入方法やメリットを紹介する。

2. 国内外におけるサプライチェーンの問題点

本章では，サプライチェーンが抱える問題について述べる。

2.1 サプライチェーンに関わる企業のセキュリティリスク

国内の大企業では，マルウェアなどのサイバー攻撃に備えたセキュリティ対策への投資が進んでいる。一方で，中小企業においては，セキュリティに対する投資額が低い傾向も見えている。[(1)]

サプライチェーンに関わる中小企業の中には，セキュリティ対策の手薄な委託先もあり，攻撃者もこれらを踏み台として委託元を攻撃するケースが増加している。実際に，サプライチェーンの委託先を通じて，委託元の製品の設計データや，個人情報，営業秘密情報などが流出した事例が発生している。このような事例は，業種，業態，規模に関わらず，サプライチェーンを構成する全ての企業で発生し得る問題であり，誰もが被害者あるいは加害者（被害の助長者）になる可能性を秘めている。

2.2 国ごとに異なるセキュリティ規格

現在，米国，欧州，そして日本をはじめとするアジア各国において，セキュリティ規格の整備が進められている。例えば，米国では米国国立標準技術研究所（NIST：National Institute of Standards and Technology）のSP（Special Publication）シリーズの発行や，米国政府によって使用されているクラウドサービス調達のセキュリティ基準FedRAMP（Federal Risk and Authorization Management Program）制度の運用などがある。

また欧州では，イギリスのPSN認定（Apply for a Public Services Network connection compliance certificate）やドイツのBSI-Standard（Bundesamt für Sicherheit in der Informationstechnik-Standard）などが存在している。

日本でも内閣サイバーセキュリティーセンターや独立行政法人情報処理推進機構（IPA）などから，様々なセキュリティ規格が提供されており，企業や組織において活用されている。

これらのセキュリティ規格は，各国が独自に作成しているものが中心であり，対策の目的や実施後に得られる結果がほぼ同じセキュリティ要求であっても，各国の規格間で求める手段やアプローチが異なることがある。その結果，複数のセキュリティ規格への対応には重複した作業が要求され，対応にも長時間を要したり，コストの増加を招いたりする恐れがある。

例えば，セキュリティ規格の監査では，国ごとにセキュリティ対策への評価手段，確認されるエビデンスが異なる。また評価元も，政府機関である場合

や，民間団体，企業である場合など，様々なケースが存在し，たとえセキュリティ要求の水準を満たしていても，監査対応や第三者証明のための工数が個別に発生してしまう。

3. 委託元・委託先のセキュリティ対策実施における課題

前章で述べたように，サプライチェーンのセキュリティには二つの問題点が存在する。そのような状況の中，サプライチェーンのセキュリティにおいて現在主流となっているのは「契約・手続きに関する対策」である。

ISO/IEC 27036（外部から製品やサービスを調達する際の情報セキュリティリスクのマネジメントに関する指針を示した規格）[(2), (3)]では，調達に伴う情報セキュリティ対策として，選定，契約，契約履行の管理や保証などの各フェーズで実施すべき管理策の指針を示している。これに対して日本では，2015年に経済産業省が「サイバーセキュリティ経営ガイドライン」を公開している。また，同年に内閣サイバーセキュリティセンターが「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」で，調達に伴う情報セキュリティ対策を示している。

これらの施策の中から，サプライチェーンの委託元に向けたサイバー攻撃リスクを低減するポイントを以下に挙げる。

・委託先の選定時におけるセキュリティレベルの確認
・契約によるセキュリティ責任分界点の明確化
・インシデント発生時の対処方法の明確化
・監査などによる定期的なセキュリティマネジメント体制の確認
・再委託先の管理

しかし上記の施策には，委託先に求めるセキュリティ要求に関する記載はなく，委託先の対応は委託元の判断に委ねられている。その結果，委託先へセキュリティ対策を要求するに当たって，以下の二つの課題が存在する（図-1）。

(1) 委託先のセキュリティ対策の柔軟性を阻害

委託元は，自社のセキュリティ対策をそのまま委託先に要求するケースが多い。委託先ごとにセキュリティ要件を管理すると，委託元の作業負担が増えて運用の効率が悪くなるためである。その結果，上述した委託先の対応コストが増加するとともに，委託先のセキュリティ対策の柔軟性が阻害される。

例えば，委託元からセキュリティ要求としてログの収集自動化が求められたが，予算不足によって自動化ツールが導入できない委託先があったとする。この場合，委託先が手動収集などで同等レベルの代替策を実施したとしても，セキュリティ要求に未対応という評価が下されてしまう。柔軟性の阻害とは，このように委託先のセキュリティ対策が委託元からの要求によって制限されることである。これによってサプライチェーン上で重要な委託先であっても，セキュリティ評価を落とさざるを得ず，委託先の選定の幅を狭めることにもなりかねない。

(2) 委託元のセキュリティ対策脆弱性の露呈リスク

委託元が自社の製品・サービスのセキュリティ対策を委託先に要求することは，裏を返せばセキュリティ対策や実現レベルを他社に公開していると捉えられる。秘密保持契約（NDA：Non-disclosure agreement）などを結んでいても，委託元のセキュリティ上の脆弱性特定に利用される可能性は払拭できない。例えば，委託元のセキュリティ監視周期をセキュリティ要求としてそのまま委託先に要求したとする。この場合，監視周期の間は，悪意ある操作が検出できないことを委託元は委託先に公開していることになるといえる。

4. 富士通が提案するOutcome-basedアプローチ

富士通は，上述したサプライチェーンの現状とセキュリティ対策の課題に対応するために，Outcome-basedアプローチの適用の可能性を検討した。本アプローチは，セキュリティ対策で達成される結果のみを要求事項として記載するものである。その際，要求事項に対する具体的な達成方法や手段は委託先が選択できる。これにより，委託元・委託先の負担を軽減できる。

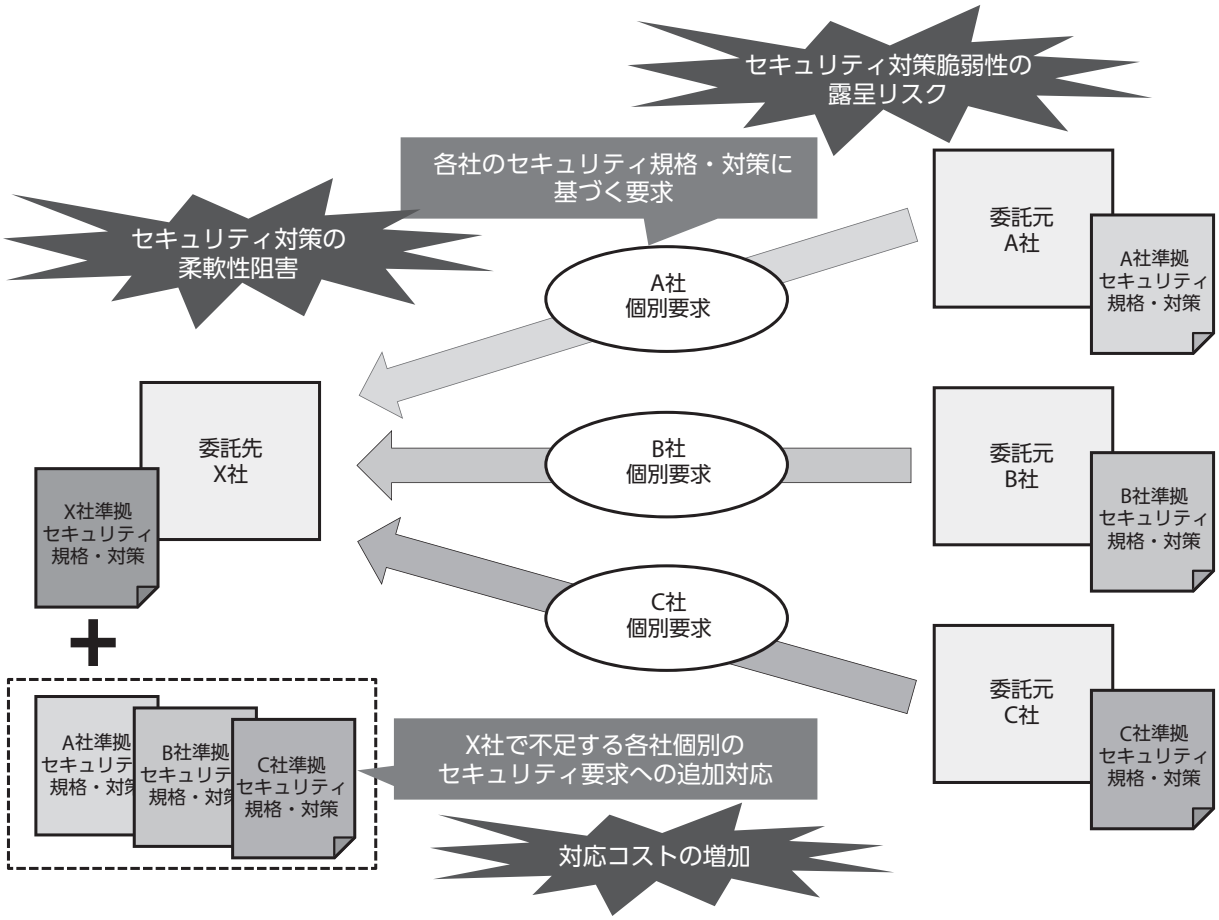

図-1　セキュリティ要求における委託先・委託元の課題

4. 1　Outcome-basedアプローチの概要

本アプローチは，2.2節で示した問題に対し，一部のセキュリティ規格の制定元や標準化団体などで2000年代中頃から利用が始まり，徐々に広がりつつある。現在，本アプローチを取り入れている規格の一つがNIST SP800-171である。[4] これは，NISTのSPシリーズの一つであり，CUI（Controlled Unclassified Information）の取り扱いに関するセキュリティ対策ガイドラインである。なおCUIとは，機密情報に指定されていないが，管理が必要な重要情報であり，一例としてクレジットカード情報や医療データ，兵器システムの開発情報などがある。

NIST SP800-171の要求項目を例に挙げると，「3.6.1 適切な準備、検知、分析、抑制（封じ込め）、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。」とある。これが，本アプローチに準じたセキュリティ規格であることを示している。

また，NISTが作成・発行しているCSF（Cybersecurity Framework）[5] も，本アプローチを取り入れたサイバーセキュリティの規格である。CSFのフレームワークコアでは，特定，防御，検知，対応，復旧の5機能が定義されており，それに基づいたセキュリティ要求が本アプローチに準じた記述で示されている。

CSFは，現在協議が進められているISO/IEC TR 27103（ISO/IEC 27001等をサイバーセキュリティの観点で活用する為のガイダンス）[6] にも採用されている。このほかにも，日本を含む複数の国のセキュリティ規格で利用・参照されるなど，今後普及が進むと考えられる。

4. 2 Outcome-basedアプローチの導入手順

富士通は，本アプローチに準じたセキュリティ規格を，委託元や委託先が実際に実装しているセキュリティ規格の間に設置することで前述した課題の克服を考えている。具体的には，図-2に示すように，委託先，委託元双方のセキュリティ対策の間に本アプローチに準じたセキュリティ規格を中間言語として設置する。その中間言語を介して，委託元は委託先のセキュリティ達成状況を評価する。これにより委託先は委託元からのセキュリティ個別要求への対応負担軽減やセキュリティ対策の選択柔軟化につながる。また，委託元は委託先選定・評価の負担軽減や委託先自身の詳細なセキュリティ対策を秘匿できる。

以下，自組織やサプライチェーンの委託先に本アプローチを導入するための手順を紹介する。

(1) セキュリティ規格の採択

委託元による中間言語の設定である。準拠しているセキュリティ規格が本アプローチに準じたセキュリティ規格であれば，そのセキュリティ規格に示されるOutcome-basedに記述されたセキュリティ要求から，必要な項目を選択して中間言語とする。また，本アプローチに準じたセキュリティ規格に準拠していない場合は，本アプローチに準じたセキュリティ規格を中間言語として新たに採用し，現行のセキュリティ対策をこれにマッピングする。

特に，NIST SP800-171は米国の防衛産業に関わるサプライチェーン上の全企業において，2017年12月から準拠が必須となっている。そのため，日本国内の防衛装備品や重要インフラ分野の調達にも採用される可能性が高く，サプライチェーンのセキュリティ対策の中間言語として活用が推奨される。また，CSFもサイバーセキュリティの中間言語として広く使われ始めているため，こちらを中間言語としても良い。

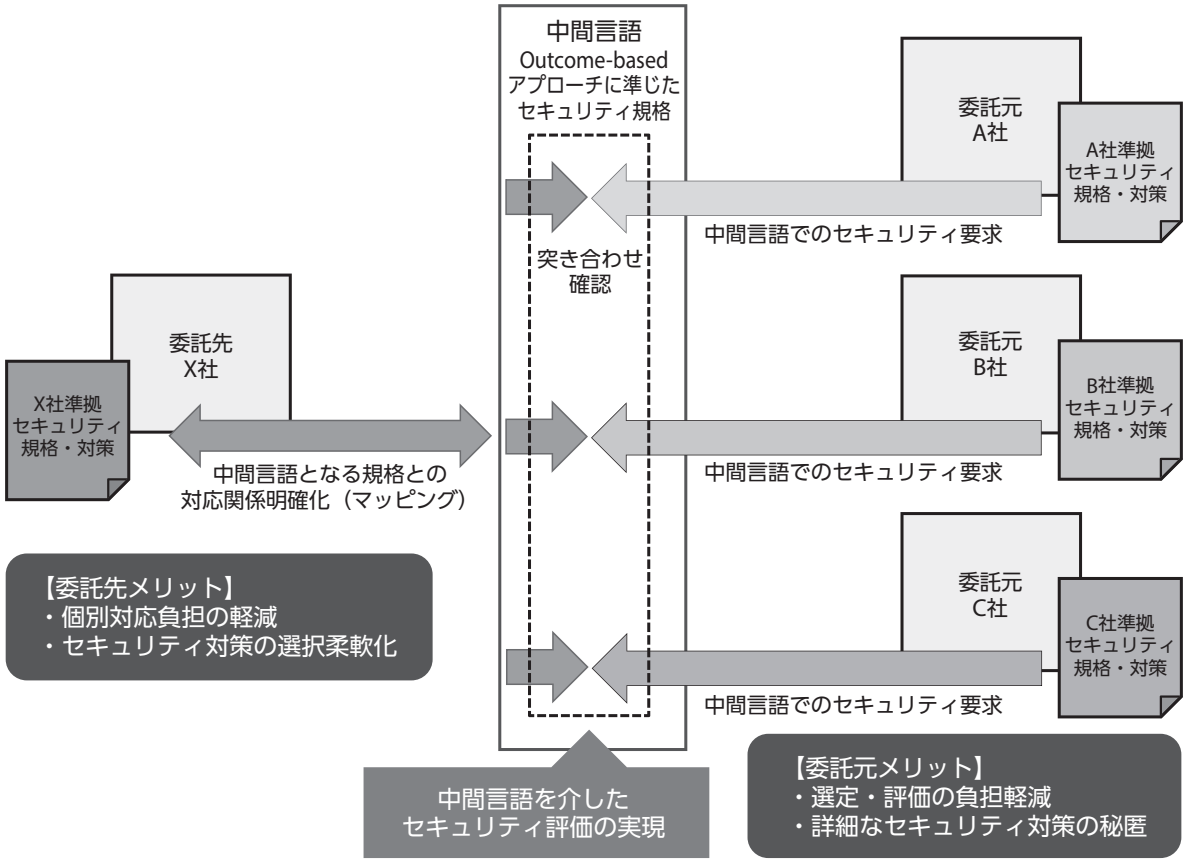

図-2　Outcome-basedアプローチを利用したセキュリティ要求の構造

(2) 委託先のセキュリティ規格の評価

委託元は，中間言語とした本アプローチに準じたセキュリティ規格に沿って，委託先が準拠しているセキュリティ規格を評価する。具体的には，委託元の提示する本アプローチに準じたセキュリティ規格の要求に対して，委託先にセキュリティ対策のマッピング作業を実施させ，そのマッピング結果と達成レベルを申告させる。委託元は申告内容を基に，セキュリティ対策状況の評価を行う。

5. Outcome-basedアプローチのメリット

本章では，サプライチェーンのセキュリティ対策に本アプローチを取り入れた場合の具体的なメリットを示す。

(1) セキュリティ要求を実現する委託先のメリット

本アプローチによって，セキュリティ要求の実現に当たって達成される結果は同じでも，委託先ごとにその過程である実施手段やアプローチが異なるといった課題に対応できる。例えば，複数の委託元から様々なセキュリティ要求を個別に課されていた委託先は，セキュリティ対策費用を削減できる。

また，本アプローチは，委託先のセキュリティ対策の選択が自由になることで，実現方法の柔軟性も向上する。3章 (1) で挙げた，セキュリティ要求を自動化するツールの未導入についても，手動対応や監視強化などの代替策でも，要求と同レベルの対応であれば，目標を達成したことになる。これによって，委託元からの選定の可能性が高まる。

(2) セキュリティ要求を提示する委託元のメリット

委託元は，委託先に対して本アプローチを用いてセキュリティ要求を提示することで，委託先が達成できていないセキュリティ要求事項のみに是正を指示すればよい。そのため，最初からセキュリティ規格に準拠させる必要はなく，調達コストの増加やスケジュール遅延を防止できる。

また委託元でも，現在のセキュリティ実現方法と今後のマイルストーンを評価することで，自社の製品・サービス提供に重要な委託先を柔軟に選定・評価できるメリットがある。

更に，本アプローチでは，委託元は中間言語となるセキュリティ規格を通じて，委託先にセキュリティ要求を行うことになる。その結果，自社の詳細なセキュリティ対策 (具体的な実現方法) を委託先へ開示する必要がないため，セキュリティの弱点が特定されるリスクを回避できる。

6. むすび

本稿では，サプライチェーンのセキュリティ対策の国内外の問題点と，委託元および委託先の課題を述べ，それらを解決へと導くためにOutcome-basedアプローチを活用した対策を紹介した。サプライチェーンのセキュリティは，2019年2月に公開された情報セキュリティ10大脅威2019[7]の組織編4位にランクインするなど，世の中での関心も高まりつつある。富士通ではこのような動向も踏まえつつ，自社の委託先評価制度に本アプローチを用いたセキュリティ評価の適用を検討している。今後，自社の結果を踏まえながら本アプローチを活用して，委託元と委託先の双方がサプライチェーンのセキュリティ対策を強化し，安心・安全に事業を推進できるよう，本活動を広く展開していきたいと考えている。なお，本稿で紹介したNIST SP800-171に関連したサービスとして，NIST SP800-171対応コンサルティングサービスを2017年10月から提供を開始している。[8], [9]

参考文献

(1) 独立行政法人情報処理推進機構：2016年度中小企業における情報セキュリティ対策の実態調査－調査報告書－，p.70-75.
https://www.ipa.go.jp/files/000058502.pdf

(2) ISO/IEC 27036-1:2014, Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts.
https://www.iso.org/standard/59648.html

(3) ISO/IEC 27036-3:2013, Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security.
https://www.iso.org/standard/59688.html

(4) 米国国立標準技術研究所：NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
(5) 米国国立標準技術研究所：Framework for Improving Critical Infrastructure Cybersecurity.
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
(6) ISO/IEC TR 27103:2018, Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards.
https://www.iso.org/standard/72437.html
(7) 独立行政法人情報処理推進機構：情報セキュリティ10大脅威2019.
https://www.ipa.go.jp/security/vuln/10threats2019.html
(8) 富士通：米国連邦政府機関外の組織および情報システムに対するセキュリティ対策基準 NIST SP800-171に対応するコンサルティングサービスを提供開始.
http://pr.fujitsu.com/jp/news/2017/10/19.html
(9) 富士通：迫り来るセキュリティ対策基準「NIST SP800-171」への準拠 防衛装備庁の最新動向と日本の企業が取り組むべき対応.
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/event/nist-seminar/index.html

著者紹介

福田　有希（ふくだ　ゆうき）
富士通（株）
品質保証本部
グローバルセキュリティ品質確保に向けた研究開発に従事。

河村　勇（かわむら　いさむ）
富士通（株）
品質保証本部
グローバルセキュリティ品質確保に向けた研究開発に従事。

窪田　好宏（くぼた　よしひろ）
富士通（株）
グローバルサイバーセキュリティビジネスグループ
サイバーセキュリティに係る国際標準化動向の調査・対応に従事。

綿口　吉郎（わたぐち　よしろう）
富士通（株）
グローバルサイバーセキュリティビジネスグループ
エンタープライズシステムセキュリティの社内実践に従事。