サプライチェーンセキュリティにおけるビジネスの可能性

著者：樋崎 充、鈴木 裕士

近年高まりを見せているサプライチェーン攻撃の脅威に対応するためには、グローバルでの議論が必要となる。この議論の先には新たなビジネスの出現、既存ビジネスモデルの変貌の可能性が垣間見えるが、これらのビジネスを積極的に取り込むためには、議論を先導していく姿勢が必要となるだろう。

サプライチェーン攻撃に対する脅威の高まり

近年、サプライチェーン上のサイバーセキュリティに対する脅威が高まってきている。サプライチェーンの一連の過程でマルウェアに感染させる攻撃はサプライチェーン攻撃と呼ばれており、いくつかの事例も公表されている。

2017年、ウクライナの税務会計パッケージソフトMEDocの正規更新システムに何者かが管理者権限でログインし、ルート権限を取得、更新プログラムを改ざんすることでバックドアが埋め込まれた。バックドアはマルウェアの一種で、バックドアが存在するとサイバー攻撃者が容易にシステムに侵入できるようになってしまう。改ざんされた更新プログラムをインストールしたユーザーはバックドア型マルウェアに感染してしまい、ネットワークを通じて別のユーザーにも感染が広がっていった。ユーザーはその多くがウクライナの国内企業や組織、また同国と取引のある多国籍企業で、被害はウクライナから欧州全域に広がった。

また、同年には別の深刻な事例も報告されている。世界で数百社の大手企業にサーバー管理ツールを提供している、韓国のNetSarangが配信したソフトウェアのアップデートに、バックドアが埋め込まれていることが発見された。このバックドアは、NetSarangの正規ソフトウェアの更新プログラムが改ざんされて仕込まれており、この更新プログラムをインストールすると、攻撃者によるデータの窃取、外部送信が可能な状況となっていた。ロシアのセキュリティベンダーであるKaspersky社からの連絡を受けたNetSarangは、直ちにバックドアを削除した更新プログラムをリリースすることで解決した。これまでのサプライチェーン攻撃の中でも最大規模の一つと言われており、素早く検知、解決していなければ、世界中の数百もの組織が攻撃の被害に遭っていた可能性があった。

これらの事例も受け、Kaspersky社は、2018年脅威予測レポートにおいてサプライチェーン攻撃の増加を予測し、世間の認識が高まる契機となった。公表されている事例以外にもサプライチェーン攻撃は多く存在していると考えられており、実際に、2018年にセキュリティベンダーのCrowdStrike社が行ったアンケート調査によると、回答企業の3分の2がサプライチェーン攻撃を受けた経験があり、そのうちの半分（全体の3割超）が直近1年以内に攻撃を受けていた（図表1参照）。また、Kaspersky社による2019年の脅威予測レポートにおいても、サプライチェーン攻撃は継続され、引き続き注意が必要であると警告されている。

米国では、疑わしい企業を排除することでサプライチェーン上のセキュリティを確保しようとしており、中国ハイテク企業に対して強硬姿勢を打ち出している。その根拠となっているのが2018年8月に可決された「2019年度米国防権限法（NDAA2019）」で、同法は2019年8月13日以降、政府機関・軍・政府所有企業が中国ハイテク5社（ファーウェイ、ZTEなど）の製品や部品を組み込んだ他社製品を調達することを禁じている。さらに、2020年8月13日以降に適用される規制では、当

樋崎 充（といざき・みつる）
mitsuru.toizaki@pwc.com

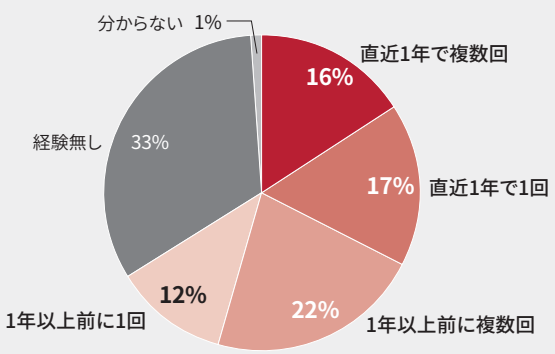
PwCコンサルティング、Strategy&のパートナー。約15年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトを手がけてきた。

鈴木 裕士（すずき・ひろし）
hiroshi.suzuki@pwc.com

PwCコンサルティング、Strategy&のアソシエイト。製造業・商社などのクライアントに対するセキュリティ技術調査支援、新市場参入戦略策定などのプロジェクトに取り組む。

図表1
ソフトウェアサプライチェーン攻撃の経験時期・回数

（n=1,300）



出所：CrowdStrike Supply Chain Survey 2018（July, 2018）

該5社の製品を社内で使用しているだけで、米政府機関と取引ができなくなる。このような強硬策を打ち出している理由の一つに、これらの企業の製品にバックドアが仕込まれ、機密情報の漏洩や、有事の際に製品の性能低下・無力化が行われるのではないかという懸念がある。日本においても、企業の名指しはしないものの、安全保障上の脅威がある場合は、政府調達で制限できる仕組みの導入が発表された。

米国のように疑わしい調達先を排除することでセキュリティを高めることも可能ではあるが、外交上の問題が生じることもあり、簡単ではない。また、調達の代替先も完全に安全とは言い切れないため、実際には別途対策をとる必要がある。

製品の調達時にセキュリティを検査する技術として、静的解析や動的解析が存在する。静的解析では主にソースコード検査が行われ、セキュリティ上のリスクがある既知のコードを検出する。動的解析では主にファジングと呼ばれる検査が行われ、検査対象に問題が起きそうなさまざまなデータを入力して異常な動作が起きないかを確認することで、問題を検出する。実務的にはこれらの手法を組み合わせて効率的・効果的な検査を試みている。また、外部接続されたネットワークを通じて疑似的な侵入テストを行いシステムやネットワークのセキュリティをチェックする、ペネトレーションテストも存在する。しかし、個々の企業では、これらの検査技術は開発工程には組み込まれている場合はあるものの、調達時にはほとんど実施できていないのが現状である。

図表2
開発プロセス内でのセキュリティ評価・検証方法

プロセス	セキュリティ評価・検証	概要
製品企画・設計（要件定義）	• 脅威分析	• 守るべき資産の想定、想定される脅威とビジネスインパクトの分析、対策方針と設計方針決定
	• セキュアプログラミング	• 必要なセキュリティ対策が設計書に含まれているか確認
調達	• 受け入れ検査	• 一般的な手法が確立されておらず、受け入れチェックは ほぼできていない
実装	• ソースコード検査	• コーディング規約に基づく実装が行われているかどうかや、脆弱性*を検証
テスト	• ファジング	• 不正データを検査対象に送信、挙動から脆弱性を検出
	• 脆弱性スキャン/ペネトレーションテスト	• ツールを用いて脆弱性を検出し、脆弱性からシステムに侵入が可能か、侵入された場合の影響の大きさを検証
運用	• 運用時対策/脆弱性対策	• 脅威や脆弱性情報の収集、定期的な修正プログラムの適用など

* 脆弱性：プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥

出所：IPA「ファジング活用の手引き」（2018年7月）を基にStrategy&が作成

セキュリティリスクに対する海外の取り組み

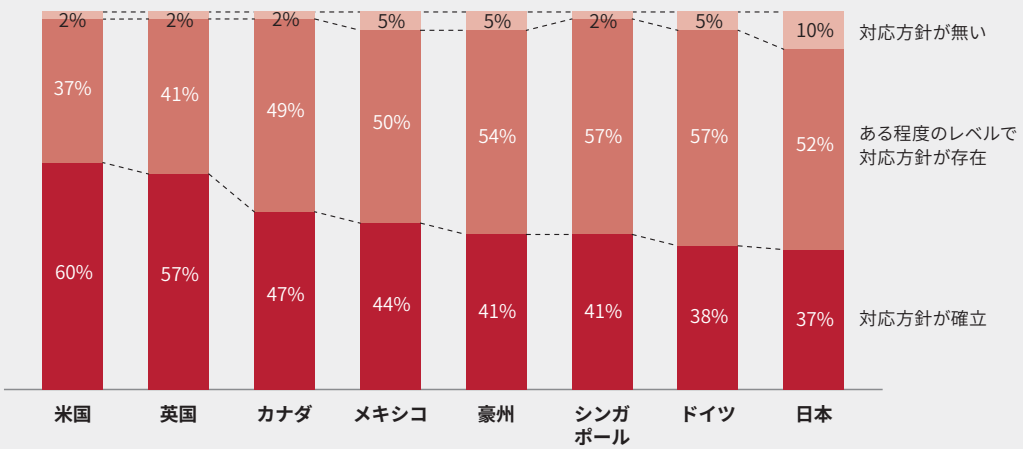
図表3は、ソフトウェアサプライチェーン攻撃を受けた際の対応方針の有無の企業割合を、国別に示している。いずれの国も日本より対応方針が確立されている割合が大きく、特に米国で、サプライチェーン上のリスク認識が高いように見受けられる。

米国では、米国国立標準技術研究所（NIST）により、Cybersecurity FrameworkやNIST SP800-171のような、サプライチェーンリスクに対応したフレームワークが制定されている。2014年2月にVersion 1.0が策定されたCybersecurity Frameworkでは、サイバーセキュリティ対策の全体像が示されており、「特定」「防御」「検知」「対応」「復旧」に分類して対策が記載されている。Version 1.1が2018年4月に策定され、そこではサプライチェーンのリスク管理の重要性が説かれており、サプライチェーン全体でセキュリティ対策を実施することが要求されている。NIST SP800-171は2015年6月に発表され、2018年6月にはアップデート版が発表されている。米国政府機関が調達する製品や技術を開発・製造する企業に対して求められるセキュリティを担保するためのものであり、既に米国防総省は取引事業者に準拠を求めている。

さらに、IoT機器のサイバーセキュリティについて、米国政府が第三者認証を準備していることが確認されている。2016年2月に発行されたCybersecurity National Action Plan にて、米国土安全保障省（DHS）がIoT環境下でつながる機器を試験・認証するためのサイバーセキュリティ保証プログラムの開発において、民間の第三者認証機関であるUL社や産業界

図表3
ソフトウェアサプライチェーン攻撃を受けた際の対応方針の有無

(n=1,300)



出所：CrowdStrike Supply Chain Survey 2018 (July, 2018)

と協力をしているとの記述がある。UL社は2015年よりCyber Assurance Program (CAP) というサイバーセキュリティ認証プログラムを開発しており、一部はANSI (米国国家規格協会) 規格となっている。今後、ISO (国際標準化機構) やIEC (国際電気標準会議) において標準化される可能性も考えられる。

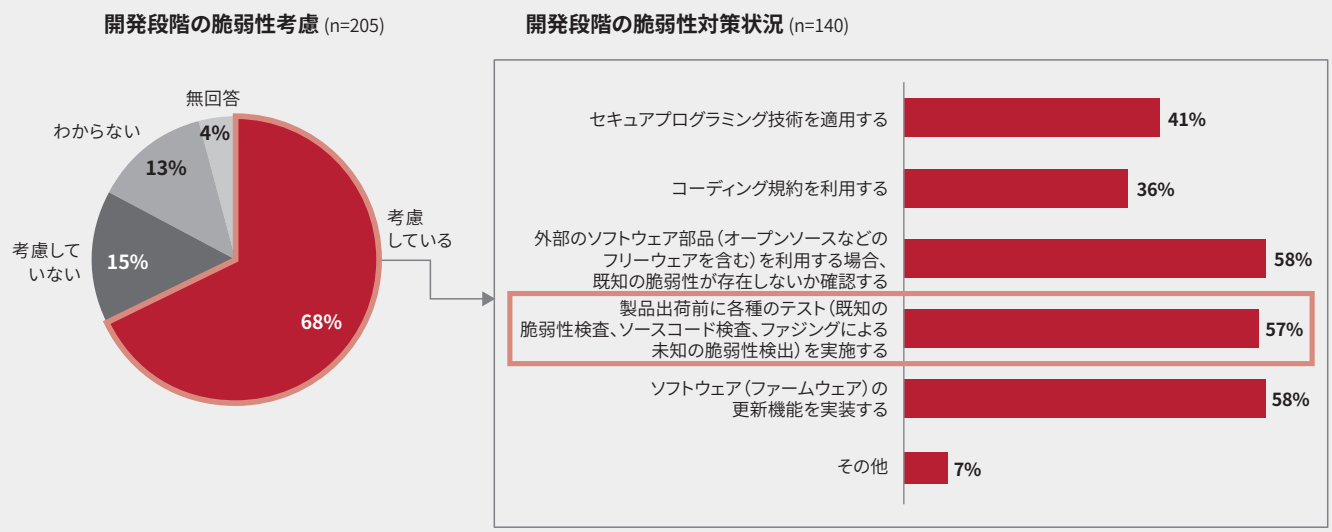
また、サプライチェーン上のセキュリティ向上のために、米国商務省電気通信情報局 (NTIA) 主導で、ソフトウェアコンポーネントの透明性向上への議論も進められている。ここでは、ソフトウェアの構成要素リストであるSBOM (Software Bill of Materials) の構造・共有方法・活用方法の標準化、ユースケース策定などが目的とされている。

日本の現状と課題

一方、日本に目を向けてみると、図表3に示した通り、サプライチェーン攻撃に対する認識が他国に比べて低い。IPA (独立行政法人情報処理推進機構) のアンケート調査によると、ITシステム・サービスの調達側が、開発側 (委託先) が実施すべき具体的な情報セキュリティ対策を仕様書などで明記できているのは30%程度でしかない。また、IPAの別の調査によると、開発段階でセキュリティを考慮している企業は68%程度であり、そのうち製品出荷前にテストを行っているのは57% (全体に対しては39%) にとどまっている (図表4参照)。開発側で十分なセキュリティ検査が行えていないため、調達側で製品受け入れ時に検査を実施する必要があるが、実際には調達側でもできていない状況にある。防衛省の備品や自動車のようなセキュリティが重要なものですらできていないといわれている。不正なプログラムが組み込まれてしまった場合でも、調達時にはチェックができておらず、運用中に偶然に発見されているのが現状である。

各企業でサプライチェーンセキュリティへの取り組みが進んでいない理由として、日本の制度作りが遅く、取り組み意義や実施すべき内容が不明確であることが一因と考えられる。最近になって制度作りへの取り組みが進められるようにはなっ

図表4
開発段階の脆弱性考慮・対策状況



出所：IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年3月）。小数点以下は四捨五入

たが、他国の後を追うような状況となっている。日本ではサプライチェーンリスクに関するフレームワークがなかったため、米国から日本政府に、サプライチェーンリスクに対応するよう働きかけられていた。2017～2018年度にかけて、経済産業省主体のワーキンググループにより、サイバーセキュリティに関するフレームワークの検討が進められた。本フレームワークにより米国のCybersecurity FrameworkやNIST SP800-171などへの対応がとられることとなったが、米国での規制内容・範囲が変更されれば、それに準じて日本でも再び対応を迫られることになると考えられる。議論が遅れたことから対応が後手に回り、日本企業も今後のビジネス環境を見通しづらい状況となっている。

今後の議論の展望とビジネスの可能性

これまで見てきた通り、他国（特に米国）ではサプライチェーンセキュリティに関する制度化・ルール化が進められており、ソフトウェアコンポーネントの透明性向上に向けた新たな議論も進められている。このような中、今後日本での議論が遅れると、再び他国で決められた枠組みへの対応を迫られることになりかねない。その場合、日本企業には不都合な枠組みにより既存のビジネス環境が悪化、あるいは最悪の場合グローバルサプライチェーンからはじき出されてしまうことも考えられる。他国から取り残されないために、さらにはグローバルのビジネスを先導していくために、今後必要となる議論を日本主導でも進めていくべきではないだろうか。

そして、今後必要となる議論として、サプライチェーンの透明

性向上があると考えられる。昨今ではサプライチェーンが複雑化しており、ソフトウェアにどのようなパッケージやコードが含まれているのか、誰が開発に関わったのかが分かりづらい状況であることが、サプライチェーン攻撃が発生する下地となっており、この不透明性の解消が必要と考えられる。

サプライチェーンの透明性向上のためには、製品自体の情報（ソースコード情報、コンポーネント情報など）、開発者の情報（誰がいつ、どの部分の開発に関わったのかなど）について、サプライチェーン関係者間で共有したり、第三者認証機関を設置して認証を取得する仕組みを作ったりするなどの方向性が考えられる。製品自体の情報が開示されることで調達側（もしくは第三者認証機関）でもセキュリティの検査ができるようになり、さらに開発者の情報が開示されることで、問題が生じた際に原因を追究することが可能となる。また、このような透明性の向上は、不正プログラム混入に対する抑止力にもなりうると考えられる。

このような議論が進んだ場合、新たなビジネスとして、製品情報や開発者情報の開示に用いる共通プラットフォームの提供や、第三者認証機関としてのサービス提供などが考えられる。当初からルール作りの議論に関わることで、このようなビジネスチャンスの取り込みが可能になるだろう。参入できればソフトウェアに関するデータが大量に集まるようになり、独占的なポジションが確立され、新たなデータビジネスへの道も開かれるのではないだろうか。一企業による独占は難しいかもしれないが、複数企業により運営企業を共同設立するという方向性も考えられる。

また、プラットフォームにソースコード情報やコンポーネント情報が集まるようになれば、今までは個別に行われていたソースコード検査や、コンポーネントのバージョンチェックなどが、プラットフォーム上で実施できるようになるかもしれない。その場合、個別に提供されていたサービスがプラットフォーム上に統合されていき、これらのサービスもプラットフォームと相まって強固なポジションを築くことになると想定される。ここでの統合に乗り遅れた場合、市場でのポジションを失うことになりかねない。第三者認証機関を設置した場合でも、同様な事象が生じると考えられる。

プラットフォームビジネスの獲得、あるいはプラットフォームに統合するサービスの提供、いずれにしてもサプライチェーン透明性向上の議論に当初から関わり、ビジネス獲得に有利なポジションを築いていくことが今後重要となるのではないだろうか。