桑名レポート：サイバーセキュリティの現場から（2）

# サプライチェーンへのセキュリティ攻撃問題

NTT アドバンステクノロジ株式会社
常務取締役　セキュリティ事業本部
本部長　桑名 栄二
博士（工学）、CISSP

サプライチェーンのセキュリティ問題として、委託先の不注意や発注元の管理の不備等により、知的財産情報や機密情報が漏えいした事案は過去数多く発生しているが、本稿では一般的に正規と思われるサプライチェーンを介したサイバー攻撃による被害事案や機密情報の漏えい・流出事案について報告する。

## 業務委託先へのサイバー攻撃による被害

企業の知的財産、機密情報や国家の安全保障に関連する情報をねらったサイバー攻撃が後を立たない。省庁、重要インフラ、大企業等はある程度のセキュリティ対策が実施されているが、その海外事業所、系列企業、取引先となると必ずしもそうではない。例えば、米国防総省（DoD）関連の情報漏えいは、DoD 本体や直接契約会社からではなく、孫請けやさらにその再委託先会社から多く発生していると報告されている [1]。日本も同様で委託先から情報が漏えいしたインシデントが相次いでいるし、委託先が情報を軽んじたための被害も発生している [2][3]。

最近では企業側の防御対策は進展してきていることもあり、攻撃側がより効果的に攻撃や情報窃取を行うために、企業本体だけでなくサプライチェーン全体の中から脆弱な部分を探し出して攻撃が仕掛けられているようである。

## サプライチェーンを介した攻撃

IT 運用や空調機器システム等、各種業務の委託先のセキュリティ管理の不備を狙った攻撃は従来から数多くの事案が報告されているが [4]、ここではサプライチェーンの視点から攻撃事案を考察する。一般的に正規と思われるサプライチェーンを介した攻撃や、機密情報の漏えい・流出はいくつかの事例に分けることができる。

**①ソフトウェアへの攻撃**

これは、攻撃者がソフトウェアベンダーの開発現場に侵入し、そのソフトウェアのパッチモジュールにマルウェアを仕掛け、正規のダウンロードルートを用いて利用者を攻撃する仕組みである。例えば、攻撃者がメーカー、サプライヤー、ユーザー間の信頼関係に付け込んでマルウェアを拡散させた例がある。ウイルス対策ソフトウェアメーカー Avast Software 傘下で開発された、Windows 環境のクリーンアップ用フリーソフト「CCleaner」のアップデートモジュールにバックドアが仕掛けられ、正規のダウンロードサーバを通じて配布されていた [5]。この事案は不特定多数へのばらまき型攻撃である。

一方、同じソフトウェアへの攻撃でも、ターゲットを絞り、かつダウンロードさせやすい時期を狙った標的型攻撃として、2017 年のウクライナの事案がある。同年 6 月に、ウクライナの多くの企業で利用されている M.E.Doc 社の会計ソフト「MEDoc」のアップデートを通じて、ランサムウェア NotPetya がウクライナの主要機関をはじめ欧米 64 カ国に拡散した [6]。この攻撃は、同国における確定申告の時期を狙ったとみられている。

**②ハードウェア・トロイ**

これは、回路コンパイラや EDA（Electronic Design Automation）ツールが狙われたり、半導体チップの製造工程でバックドアが仕掛けられるハードウェア・サプライチェーンへの攻撃である [7]。最近でも、最悪の事態には至っていないが、台湾の半導体チップ製造メーカーの製造ツールがウイルスに感染してしまい、製造ラインを数日止めざるを得なかったとの報告もなされている [8]。IoT 時代において大変厄介な問題である。

**③クラウド上のプロバイダへの攻撃**

これは、世界各国の MSP（マネージドサービスプロバイダ）を攻撃し、それらを踏み台として、公共、製造業、小売、電力、製薬、通信等の顧客企業の知的財産情報や取引情報の窃取を行おうとする攻撃である [9]。近年、多くの企業は業務システムや情報資産をクラウドに移行してい

る。代表的なクラウドサービス（いわゆるTier-1型）は、強固なセキュリティ技術導入と運用で顧客情報を守っているが、中堅中小のクラウド事業者サービスを利用する場合は注意が必要である[10]。

## サプライチェーンセキュリティ強化の動き

上記のサプライチェーンを狙った攻撃に対して、米国ではNIST SP800-171（Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations）やNIST Cyber Security Framework 1.1（2018年4月）等でサプライチェーンのセキュリティ向上の検討が進められている。日本でも経産省の「サイバーセキュリティ経営ガイドライン」[11]や産業サイバーセキュリティ研究会で検討が進められている。

例えば、米国防総省（DoD）では契約業者に対してSP800-171への準拠を義務化した。また、NISTのCyber Security Framework 1.1では、サプライチェーン管理（Cyber Supply Chain Risk Management（SCRM））が追加され、潜在的に悪意のある機能、偽物もしくは脆弱性がある製品やサービスを特定、評価、軽減することが盛り込まれた。

日本のサイバーセキュリティ経営ガイドラインでは、サイバー攻撃から企業を守る観点で、経営者が認識すべき「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」が整理されている。サプライチェーンに関しては、3原則の第2原則で「自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要」と謳い、「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」と指示（指示9）している。

## サプライチェーンセキュリティ管理

では、企業はサイバーセキュリティの観点から、サプライチェーンを管理するためにどのようなツールや仕組みを導入すればよいのだろうか？

自社で管理するか、第三者にその管理を委託するかに限らず、まずやるべきことは、契約書へのセキュリティ対策の明記である。契約書には、場合によっては再委託の禁止、再委託が必要な場合はエンドまでのセキュリティ対策が適用されること、重大インシデント発生時の一定期間内通知の義務化等の明記も必要である。また、機密情報の扱いについては、その受領・作成、利用、配布、持ち出し、保管、返却・破棄方法等について取り決めを交わしておく必要もあるし、監査などを通じた状況確認、把握も忘れてはならない。契約書や仕様書作成時の参考としてNISCの「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」[12]がある。

一方、契約書やガイドラインにサプライチェーンのセキュリティ管理を盛り込んだとしても、正規ルートのプロセス内に紛れ込む攻撃による侵害を100%防ぐのは難しい。となると、当面出来る対策は、地道な対策（例えば、OSとWebを含むアプリケーションシステムを最新の状態にしておく、パッチを当てておく、変更管理を運用する、特権IDを管理しておく、多要素認証を導入しておく、ログ管理等）しかない。また、たとえ侵害を許してしまったとしても早期に不審な動きを検知できる、例えばEDR(Endpoint Detection and Response)製品の導入や、リスクの移転という意味からサイバー保険の検討も必要と考える。

今日、自社だけで事業が成り立っていることは稀であり、海外事業所、子会社、パートナー企業などから構成されるエコシステムで事業は成立している。サイバー攻撃者は目的を達成するために様々な方法を駆使し弱い箇所を探し出し仕掛けてくる。これによりエコシステム全体が危険にさらされるのであれば、全体のレベル引き上げ、強化を、経営者は重要課題と位置づけなければならない。


[1]http://www.sjac.or.jp/common/pdf/kaihou/201803/20180304.pdf
[2]https://www.nikkei.com/article/DGXMZO30643680X10C18A5CN8000/
[3]http://www.security-next.com/095238
[4]https://www.ipa.go.jp/files/000062279.pdf
[5]http://www.itmedia.co.jp/enterprise/articles/1709/19/news051.html
[6]http://www.itmedia.co.jp/enterprise/articles/1706/29/news057.html
[7]https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf
[8]https://www.bloomberg.com/news/articles/2018-08-04/tsmc-takes-emergency-steps-as-operations-hit-by-computer-virus
[9]https://blog.trendmicro.co.jp/archives/14690
[10]Neil MacDnald, The State of Cloud Security 2018, Gartner SRM Summit 2018
[11]http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf
[12]https://www.nisc.go.jp/active/general/pdf/risktaiou28.pdf