サイバー戦入門　その７

－サプライチェーン・リスク－

三村　守（防大情報工学科）

１　はじめに

調達のグローバル化やオープン化に伴い、一般競争入札によって物品の調達が行われる機会が増えてきている。一般競争入札では、一定の条件さえ満たしていれば、原則としてどのような企業でも入札に参加することが可能である。一般競争入札がきちんと機能した場合には、調達の公平性を確保しつつ、合理的に低コストで調達を実施することが可能である。しかしながら、一般競争入札では、調達の仕様さえ満たしていれば、あとは価格だけですべてが決まってしまうという価格至上主義の側面が指摘されることもある。情報システム等の大規模で複雑な調達においては、必要な要件を詳細に仕様に落とし込むのは非常に困難であるか、あるいはとてつもなく労力を必要とする場合が多い。また、あまり仕様を細かく記載してしまうと、製品が限定されて入札に参加できる企業が少なくなってしまう。これが故意に特定の製品となるように実施された場合には、調達の公平性が損なわれてしまう。したがって、本当に必要な要件だけを記載した理想的な仕様を作成するのは、現実的には不可能である場合が多い。そのため、故意に低価格で落札し、最低限の仕様を満たした劣悪な製品を納品するといったいわゆるサプライチェーン・リスクの問題が浮上するようになった。最低限の仕様を満たした製品を納品するのは、落札した企業にとっては合理的な活動である。しかしながら、この調達の盲点が悪用された場合には、さらに深刻な事態を引き起こす可能性が指摘されるようになった。例えば、情報通信機器等の調達においては、その内部に不正な機能を埋め込んだチップを埋め込み、不正アクセスのためのバックドア[1]を設置するといったことが可能である。実際に、中国製のコンピュータ、スマートフォン、家電等からは、不正なバックドアの機能が発見されたというニュースを目にする機会が増えてきている。２０１３年７月には、英国の情報機関が中国のＬｅｎｏｖｏ社のコンピュータからバックドアが発見されたことを公表している。これに対し、米国製のネットワーク機器等の製品においても、出荷後にバックドアの機能が埋め込まれていることが、元ＮＳＡ[2]の職員であるスノーデン氏に暴露されて話題となった。また、ＷｉｋｉＬｅａｋｓ[3]が暴露したＣＩ

---

[1]後から不正アクセスを実施するための裏口

[2]NSA (National Security Agency)　アメリカ国家安全保障局

[3]Julian Paul Assange 氏が設立した匿名で政府、企業、宗教等に関する機密情報を公開するウェブサイト

Ａ[4]の秘密文書[5]によると、ネットワーク機器の未知の脆弱性を把握しているにもかかわらず、修正のための積極的な措置をとっていないことが推測される。未知の脆弱性は、バックドアとして利用することが可能なためである。しかも、脆弱性は故意に作成したか否かの判断が難しいため、仮に発見されたとしても言い逃れが可能である。このような背景もあり、各国は情報通信機器等の調達の安全審査の基準を厳格化するとともに、相手国の製品を使用しないように規制を強化するようになった。このように、サプライチェーン・リスクは、国家主体の大規模なサイバースパイ活動や、さらには重要施設等へのサイバー攻撃に密接に関係している。したがって、サイバーセキュリティの文脈におけるサプライチェーン・リスクの問題は、もはや国家の安全保障を考える上での重要な要素となっている。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試み、「サイバー戦入門　その２　－サイバー戦の概念と作戦－」ではサイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。その３からは、サイバー戦に関する各トピックスをより掘り下げて平易に解説することを試みている。本稿では、サプライチェーン・リスクをとりあげる。以下、第２節ではサプライチェーン・リスクの具体例を挙げ、第３節ではサプライチェーン・リスクの概要について説明する。第４節および第５節では、その対策について説明し、第６節ではサプライチェーンの応用した監視システムに触れる。最後にまとめと今後の課題について述べる。

２　サプライチェーン・リスクの具体例

（１）ハードウェアの事例

公表された最初の事例としては、２０１２年にイギリスの研究者らがイギリス情報局保安部、ＮＳＡ[6]等の依頼を受け、中国製のシリコンチップを調査した事例が挙げられる。ケンブリッジ大学の研究者らは、シリコンチップ内の未知のバックドアを発見し、その秘密の鍵を抽出することに成功している[7]。この鍵を使用してチップにアクセスすることができれば、そのチップを使用不能にしたり、あるいは機能を改変したりすることが可能であるとされている。これらのチップは、武器、誘導、飛行制御、情報通信等の軍事製品や、原子力発電、航空宇宙、公共交通等の産業で使用されている。以後、様々なハードウェアにおいてバックドア等の不正な機能が発見されるようになった。

---

[4]CIA (Central Intelligence Agency) アメリカ中央情報局

[5]Vault 7: CIA Hacking Tools Revealed

[6] NSA (National Security Agency) アメリカ国家安全保障局

[7]Sergei Skorobogatov and Christopher Woods (2012). "Breakthrough silicon scanning discovers backdoor in military chip"

２０１３年１０月にはロシアにおいて、中国から輸入したアイロンから不正なチップが発見された。このチップは、半径２００ｍのパスワードが設定されていない無線ＬＡＮに接続し、マルウェアを送信するように設計されていたとのことである。なお、類似のチップは中国製の携帯電話、自動車、カメラ等からも発見されており、スパムメールの送信等に利用されていたのではないかと考えられている。２０１３年１１月には、韓国のＬＧ社製のスマートテレビにおいて、利用者の意思にかかわらず、閲覧した番組やＵＳＢメモリのファイル名を外部に送信していることが発覚した。このようなネットワークを介した不正な機能は、ハードウェアを直接解析する環境を保有していなかったとしても、ネットワークを傍受することで解析することが可能である。

２０１７年3月には、中国製のネットワーク機器に隠しアカウントがあり、遠隔でアクセス可能となるバックドアあるいは脆弱性があることが公表された[8]。ネットワーク機器に関しては、米国の製品についても情報機関等が脆弱性を認識しているにもかかわらず、あえて積極的に修正しない場合があることが確認されている。このようなバックドアは、意図して設置したバックドアなのか、意図せずできてしまった脆弱性かの判断が難しい場合が多い。

２０１７年5月には、ＨＰ[9]社製のノートパソコンおよびタブレット端末において、キーロガー[10]が発見された。このキーロガーは、オーディオチップを開発したＣｏｎｅｘａｎｔ社のデバイスドライバに含まれており、利用者が入力したキーボードの入力内容を秘密裏に収集していた。この事例では収集した内容を外部に送信する機能は確認されていないが、他の手段と組み合わせることにより、パスワード等の機密情報が摂取される可能性が指摘されている。

２０１９年１２月には、オークションでハードディスクの落札者がデータを復元したところ、神奈川県の公文書情報とみられるデータが発見される事件が発生した。出品者は廃棄業者の元社員であり、本来は破壊すべきハードディスクをオークションで転売していた。ハードディスクは暗号化されておらず、破壊手段の指定や立会による確認も実施されていなかった。このように、サプライチェーン・リスクは納品時だけでなく、運用から破棄までの一連のライフサイクルに影響する。

（２）スマートフォンの事例

２０１４年3月には、韓国のサムソン社のＡｎｄｒｏｉｄ搭載スマートフォンであるＧａｌａｘｙシリーズにおいて、保存されているファイルの読み込み、書き込み及び削除を可能とするバックドア機能が組み込まれていることが発見された[11]。

---

[8]Neil Kettle (2017). "Undocumented Backdoor Account in DBLTekGoIP"

[9] HP (Hewlett-Packard)

[10] 利用者のキーボードの入力内容を秘密裏に記録するソフトウェア

[11]Paul Kocialkowski (2014). "Replicant developers find and close Samsung Galaxy backdoor"

２０１４年春には、中国のＰＬＡ[12]の元軍人が設立したＨｕａｗｅｉ（華為技術）社をはじめ、Ｌｅｎｏｖｏ社、Ｘｉａｏｍｉ（小米）社等のスマートフォンに、あらかじめ利用者の個人情報、位置情報、メール、通話等を監視する機能が組み込まれており、同機能を取り除くことは不可能であることが確認された。さらに２０１４年７月には、米国のＡｐｐｌｅ社製のｉＯＳ[13]において監視用と思われるバックドアが発見された[14]。このバックドアはファームウェアに組み込まれており、暗号化機能をバイパスして端末の個人データにアクセスすることを可能としている。

２０１６年８月には、中国のＦｏｘｃｏｎｎ（鴻海）社製のＡｎｄｒｏｉｄ端末のファームウェアにおいてバックドアが発見された[15]。このバックドアはメンテナンス用と思われるが、第三者が悪用した場合には、認証を回避して端末にアクセスすることが可能である。

２０１６年１１月には、中国のＢＬＵ社製のＡｎｄｒｏｉｄ搭載スマートフォンにおいて、通話記録や個人データを中国のサーバに無断で送信する機能が組み込まれていることが確認された[16]。この機能が組み込まれたスマートフォンやスマート機器は７億個以上に及び、そのほとんどはＨｕａｗｅｉ社やＺＴＥ（中興通訊）社製であるとされている。さらに、管理者権限で任意のプログラムを実行可能な機能が、ファームウェアに埋め込まれていることも確認されている。

２０１７年４月には、スマートフォンやタブレットに使用されるＢｒｏａｄｃｏｍ社製のＷｉｆｉチップに、遠隔から任意の命令を実行できる脆弱性が見つかった[17]。このチップは，ｉＰｈｏｎｅやｉＰａｄなどのｉＯＳ搭載製品、Ｎｅｘｕｓシリーズ、Ｇａｌａｘｙシリーズ等、広範囲で使用されている。この脆弱性を使用すれば、同一のＷｉｆｉネットワーク内にある端末の制御を奪うことが可能である。

２０１８年３月には、中国のＨｕａｗｅｉ社、Ｘｉａｏｍｉ社、韓国のＳａｍｓｕｎｇ社等のＡｎｄｒｏｉｄ搭載スマートフォンにおいて、ＲｏｔｔｅｎＳｙｓと呼ばれる不正に広告を表示するマルウェアがインストールされていることが確認された[18]。このマルウェアはＳｙｓｔｅｍ　Ｗｉ－Ｆｉ　Ｓｅｒｖ

[12]PLA (People's Liberation Army) 中国人民解放軍

[13]iphone、ipod、ipad 等のほとんどの端末で採用されている OS

[14]Jonathan Zdziarski (2014). "Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices"

[15]Jon Sawyer (2016). "Pork Explosion Unleashed"

[16]Matt Apuzzo and Michael S. Schmidt (2016). "Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say"

[17]Gal Beniamini (2017). "Over The Air: Exploiting Broadcom’s Wi-Fi Stack"

[18] Feixiang He et al. (2018). "RottenSys: Not a Secure Wi-Fi Service At All"

ｉｃｅという名称に偽装されており、不当なアクセス権限を要求し、指令サーバから追加のプログラムをダウンロードして実行する。

このように、スマートフォンは、主にファームウェアやアプリケーションに不正な機能を埋め込むことにより、個人情報や機密情報の窃取に積極的に活用されている。

（３）ソフトウェアの事例

２０１３年１２月には、Ｂａｉｄｕ　ＩＭＥ[19]およびＳｉｍｅｊｉ[20]というソフトウェアが、利用者の同意なしに入力した情報を外部に送信する機能を有していることが発覚した。これは、入力内容を外部のサーバで共有して変換の質を改善したり予測したりするクラウド入力と呼ばれる機能に起因しており、機密情報が外部に流出する可能性が指摘されている。

出荷時のパソコンにあらかじめインストールされたソフトウェアにバックドアの機能が埋め込まれた例としては、２０１４年に出荷されたＬｅｎｏｖｏ社製のパソコンが挙げられる。これらのパソコンには、Ｓｕｐｅｒｆｉｓｈ[21]と呼ばれるソフトウェアがあらかじめインストールされており、暗号化された通信を解除できてしまったり、不審なサイトを信頼させてしまったりするという脆弱性をかかえていた。そのため、Ｓｕｐｅｒｆｉｓｈは手の込んだバックドアではないのかという指摘がなされている。

より深刻な例としては、２０１５年にロシアのカスペルスキー社のウイルス対策ソフトを経由し、ＮＳＡの職員のパソコンから機密情報が流出したとされる事案が挙げられる。この報道に対しカスペルスキーは、当該パソコンはすでにマルウェアに感染していたとされる中間報告[22]を公表しているが、真偽のほどは定かではない。２０１７年９月には、米政府機関は同製品の使用を禁止する措置を取り、１２月には英政府機関でも同様の措置を取っている。

（４）ソフトウェアのアップデートによる事例

２０１３年６月には、韓国においてＳｉｍＤｉｓｋと呼ばれる正規ソフトウェアのインストーラが改変され、ソフトウェアの自動更新機能を悪用して不正なＷｅｂサイトに接続する機能が確認された[23]。ＳｉｍＤｉｓｋはファイル共有機能やオンラインストレージを提供する正規のＷｅｂサイトである。この事例では、攻撃者はこの正規のＷｅｂサイトを改ざんし、改変したインストーラを設置している。改変したインストーラは、ソフトウェアの自動更新機能によりユーザの端末にインストールされ、不正なＷｅｂサイトに接続させる。

---

[19]中国の Baidu 社が開発したパソコンにおいて日本語を入力するためのソフトウェア

[20]中国の Baidu 社が開発した Android 端末において日本語を入力するためのソフトウェア

[21]Visual Discovery というソフトウェアの通称であり、広告を表示する機能を有する。

[22] Kaspersky (2017). Preliminary results of the internal investigation into alleged incidents reported by US media

[23] Trend Micro (2013). "Compromised Auto-Update Mechanism Affects South Korean Users"

２０１８年７月には、韓国で遠隔支援ツールの電子証明書が窃取され、そのツールの更新プロセスを悪用してマルウェアを配布する攻撃が確認された[24]。遠隔支援ツールは、利用者のトラブルの解決を遠隔からリアルタイムで支援するためのツールであり、通信、画面共有、遠隔操作等の機能を有している。改ざんされた更新サーバは、特定の範囲のＩＰアドレスからアクセスされた場合にのみ不正ファイルを配信するように設定されており、特定の企業のみを攻撃対象としていたことが推測される。

２０１９年3月には、台湾のＡＳＵＳ社のＬｉｖｅ　Ｕｐｄａｔｅの自動更新機能を利用して、２０１８年６月から１１月の間にマルウェアが配信されていたことが判明した[25]。Ｌｉｖｅ　ＵｐｄａｔｅはＡＳＵＳ社のコンピュータに事前にインストールされているアプリケーションであり、ハードウェア固有のアプリケーションの自動更新に使われている。

（５）諸外国の規制

サプライチェーン・リスクに関する諸外国の規制については、具体的な事例が公表される以前から実施されている。２０００年代中旬、英国の研究機関がＬｅｎｏｖｏ社製のコンピュータのハードウェアやファームウェアにおいて、コンピュータを外部から制御可能とする脆弱性を発見したことから、Ｌｅｎｏｖｏ社製のパソコンを使用しないように注意喚起がなされたとされている。２００６年５月には、米国務省がＬｅｎｏｖｏ社から購入したパソコンを、機密を取り扱わない部署のみで使用すると発表した。２０１０年１１月には、インド政府が一部の中国製の情報通信機器について、安全検査を厳格化する措置をとった。これに対して２０１０年１１月には、Ｈｕａｗｅｉ社は第３者による製品の独立した評価を可能とする組織を設立した。しかしながら、２０１１年１１月には、米下院情報委員会が、Ｈｕａｗｅｉ社およびＺＴＥ社をスパイ疑惑で調査している。２０１２年３月には、豪政府が通信網の敷設事業の入札について、Ｈｕａｗｅｉ社の応札を拒否した。さらに２０１２年１０月には、米下院情報委員会は、Ｈｕａｗｅｉ社およびＺＴＥ社の製品を政府機関から排除するように提言した[26]。フランス、オーストラリア、カナダ、インド、台湾等でも同様の動きがみられ、注意喚起がなされている。２０１３年３月には、米国にて中国政府に関係する企業が製造した情報システムの政府機関への導入を禁止する法律が制定され、同４月にはＨｕａｗｅｉ社は米国市場からの撤退を表明した。２０１３年７月には、英国の情報機関が中国のＬｅｎｏｖｏ社のコンピュータからバックドアが発見されたことを公表した。これに対し２０１４

[24] Trend Micro (2018). "Supply Chain Attack Operation Red Signature Targets South Korean Organizations"

[25] Kaspersly (2019). "Operation ShadowHammer"

[26] House Permanent Select Committee on Intelligence (2012). "(Investigative Report on the U.S. National Security Issues Posed Chinese Telecommunications Companies Huawei and ZTE"

年５月には、中国政府は米マイクロソフト社製のＯＳ[27]であるＷｉｎｄｏｗｓ８を政府機関から排除するとともに、情報通信機器やサービスに関する安全審査制度を導入した。わが国においては２０１４年５月、政府機関統一基準[28]にサプライチェーン・リスク対策の強化に関する事項がはじめて追加された。さらに、翌２０１５年５月には、外部委託等における情報セキュリティ上のサイプライチェーン・リスク対応のための仕様書策定手引書が作成された。２０１８年８月には、米国においてＨｕａｗｅｉ社およびＺＴＥ社の製品を政府機関およびそれにかかわる企業が利用することが禁止された[29]。これに呼応するように、オーストラリア政府は次世代通信規格の無線ネットワークへの参入禁止をＨｕａｗｅｉ社に通告している。わが国においても、Ｈｕａｗｅｉ社およびＺＴＥ社を情報システム導入時の入札から除外することを検討している。また、ロシアについても同社の通信設備に対する輸入規制を検討している。

３　サプライチェーン・リスクの概要

（１）サプライチェーン・リスクとは？

サプライチェーン・リスクとは、本来は物品の調達から廃棄までのサプライチェーンの全般において想定される脅威のことである。例えば、２０１１年３月に発生した東日本大震災において、被災のために現地の工場での生産が停止したため、物品の調達が不可能となり、事業の継続が困難になってしまうことなどもこれに含まれる。サプライチェーン・リスクは、サイバーセキュリティの文脈においてはより限定的な意味を持つ。すなわち、情報通信機器等の調達において、不正なバックドア等の機能を埋め込まれた機器を納品されるリスクのことを指す場合が多い。情報通信機器とは、主に情報システムや通信機器のことであり、これらはコンピュータ等のハードウェアや、アプリケーション等のソフトウェアから構成される。これらの情報通信機器を構成するハードウェアやソフトウェアは、共通の仕組みで動作する民生品で構成されることが多いため、インターネットを経由した不正アクセスのためのバックドア等を埋め込むことが可能である。具体的には、ハードウェアを意図的に不正改造したり、情報システムやアプリケーションに不正なプログラムを埋め込んだりする等、発注者の意図しない変更を攻撃者が加えることにより、機密情報等を窃取する脅威が想定される。さらに、今日では情報通信機器以外にも、無人機、家電等のあらゆる機器がスマート化しており、いわゆるＩｏＴ[30]機器が急速に普及してきている。ＩｏＴ機器や組み込み機器には、ファームウェアと呼ばれる機器を

---

[27]OS (Operating System)

[28]内閣サイバーセキュリティセンター(2014).「政府機関の情報セキュリティ対策のための統一基準（平成２６年度版）」

[29] John S. McCain (2018). H.R.5515, National Defense Authorization Act for Fiscal Year 2019

[30]IoT (Internet of Things) モノのインターネット

制御するためのソフトウェアが組み込まれている。そのため、サイバーの文脈におけるサプライチェーン・リスクの範囲は、もはや情報通信機器に限らず、あらゆる電子機器に対象が拡がりつつある。

（２）不正な機能の追加手法

次に、不正な機能の追加手法に関して、ハードウェアとソフトウェアに分類してその違いを考察する。不正な機能の追加に関するハードウェアとソフトウェアの特徴を表１に示す。

表１：不正な機能の追加手法に関するハードウェアとソフトウェアの特徴

	改ざんの可否	必要な環境	実施主体
ハードウェア	困難	高	製造業者か国家
ソフトウェア	可能	低	誰でも可能

ハードウェアの場合には、一般的に改ざんが困難であるため、製造工程において不正な機能を埋め込む必要がある。製造工程においては、はじめから不正な機能を有するチップを基板に埋め込む手法が考えられる。製造後の製品に不正な機能を追加するためには、新たに基板等を追加することになる。さらに、この基板の作成と追加のためには、その内部の信号等の仕様を熟知し、かつ基板を製造するための設備が必要である。

このように、ハードウェアの場合には、作成のための環境を構築する敷居も高い。そのため、製造工程に関与するか、あるいはその機器の内部の構成に熟知していなければ、不正な機能を埋め込むことは難しい。そのため、ハードウェアに不正な機能を埋め込むことができる能力を有する主体は、非常に限られている。実質的には製造工程に関与する業者か、あるいは国家に限られてくるのではないかと考えられる。

ソフトウェアの場合には、改ざんが容易であるため、不正な機能を追加することも容易である。ソフトウェアのソースコード[31]を保有している場合には、単純にそのソースコードにその言語で記述したバックドア等の不正な機能を追加すればよい。ソースコードを保有しておらず、実行形式のファイル[32]のみ保有している場合には、その機械語を専用のソフトウェア等を用いて解析する[33]必要がある。専用のソフトウェアを用いてソースコードに逆変換できる[34]場合には、ソースコードを保有している場合と同様に容易に追加することが可能となる。例えば、スマートフォンのプラットフォームであるＡｎｄｒｏｉｄのアプリケーションについては、容易にソースコードに逆変換することが可能であ

[31]ソフトウェアの開発時に人間が読みやすい形式で記述する文字列

[32]コンピュータで実行できる形式にコンパイル（変換）されたファイル

[33]リバース・エンジニアリングと言う。

[34]逆コンパイルと言う。

る場合が多い。ソースコードに逆変換できない場合には、機械語と１対１に対応した命令群に変換[35]して内容を解読し、機械語で記述したバックドア等の不正な機能を追加することが可能である。この手順を自動化し、正規のアプリケーションに見せかけたトロイの木馬[36]を生成するツールも確認されている。

（３）サプライチェーン・リスクの全体像

内閣サイバーセキュリティセンターが作成した手引書[37]によると、サプライチェーン・リスクの全体像は図１に示すとおりである。

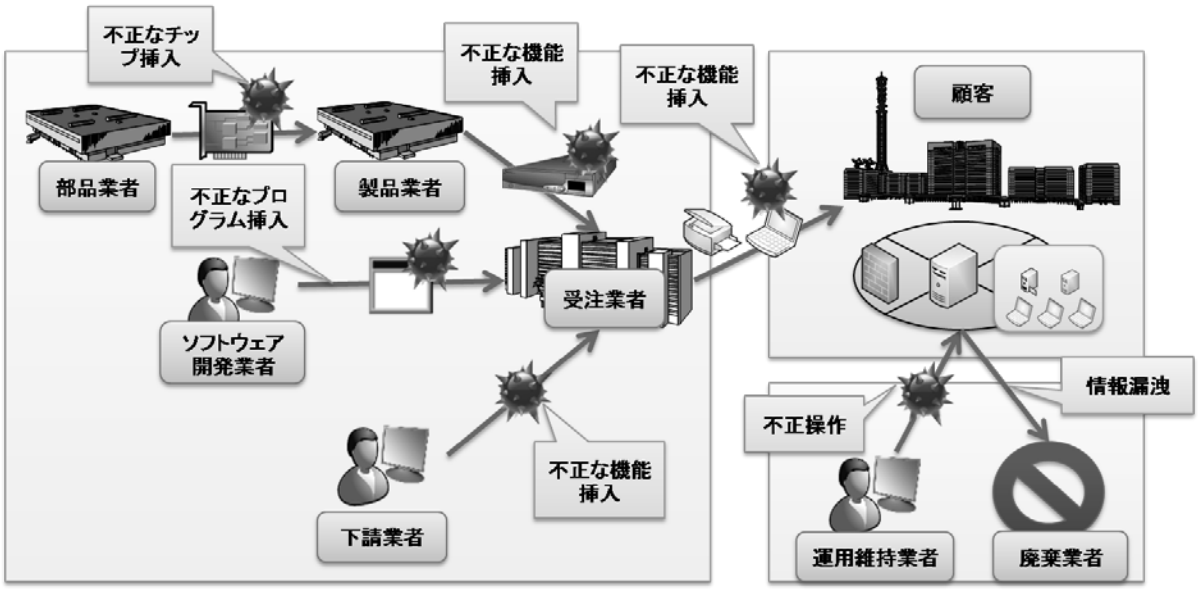

図１：サプライチェーン・リスクの全体像

一般に、情報システム等の大規模で複雑な調達においては、受注業者（ＳＩ[38]）が一括して契約を受注し、顧客に情報システム等の製品を納品する。この時、納品物である情報システム等に、不正な機能が挿入されている可能性が考えられる。さらに、受注業者は情報システムの構築に必要なハードウェア、ソフトウェアおよびサービスを他社に発注する。ハードウェアに関しては、この時に製品業者から納品される製品に不正な機能が挿入されている可能性が考えられる。さらに、その製品の製造業者は、製造に必要な部品を部品業者に発注する。この時も同様に、部品業者から納品される部品に不正なチップが挿入されている可能性が考えられる。ソフトウェアに関しては、ソフトウェアの開発業者から納品されるアプリケーションに、不正なプログラムが挿入されている可能性が考えられる。その他のサービスについても同様に、何らかの納品物に不正な機能が挿入されて

[35]逆アセンブルと言う。

[36]正規の製品に見せかけた不正な機能を有するプログラム

[37]内閣サイバーセキュリティセンター (2015).「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」

[38]SI (System Integrator)システム構築を業務とする企業の総称

いる可能性が考えられる。このように、サプライチェーン・リスクの影響は顧客である発注者だけでなく、ＳＩ等のサプライチェーン上にあるすべての業者に及ぶ。

さらにサプライチェーン・リスクの問題は、情報システム等が納品された後にも影響する。情報システムの調達においては、その後の情報システムの運用や維持管理についても役務契約を締結する場合がある。その場合には、運用維持業者が施設内に立ち入ることになる。また、保守作業等のために一時的な立ち入りを必要とする場合もある。このような部外者により、情報システムが不正に操作され、不正なプログラムが挿入されてしまう可能性がある。

情報システム等の破棄においては、廃棄業者がドキュメントの処分やハードディスク等の記憶媒体の消去を適切に実施せず、機密情報が漏洩してしまう可能性もある。

４　技術的な対策

（１）ハードウェアの場合

ハードウェアに埋め込まれた不正な機能については、発見は非常に困難である。これは、作成のための環境構築の敷居が高いことにも関係している。

ハードウェアに埋め込まれた不正な機能を検出する手法としては、元の回路と電流値や回路の遅延を比較する手法、信号確率が低いノードを活性化する手法、監視のための回路を実装する手法等が提案されている。これらの対策手法は、不正な機能がある特別な条件下で起動することが多いという特徴に基づいている。そのため、このような特徴を有しない不正な機能を検出することは困難である。また、このような対策手法を実施するためには、特別な設備を必要とするだけでなく、追加のコストや時間も必要となる。さらに、ある条件が閾値を越えると動作するようなアナログ的な手法をトリガーとする非常に巧妙なバックドアも作成可能であることが示されている[39]。

したがって、サプライチェーン・リスクの対策として、すべてのハードウェアを技術的に調査するのは現実的とは言えない。

（２）ソフトウェアの場合

ソフトウェアの場合には、高度なスキルを必要とする場合もあるが、特別で入手困難な機材を必要としないため、ハードウェアと比較すると容易に不正な機能を追加することが可能である。そのため、対策についても昔から考慮されている。最も一般的かつ容易な対策は、当該ソフトウェアとオリジナルのソフトウェアのハッシュ値[40]を比較することにより、改ざんの有無を検知すること

---

[39]Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin and Dennis Sylvester (2016). "A2: Analog Malicious Hardware"

[40]ソフトウェアの指紋のようなものであり、その値が一致すれば両者が同一であることが確認できる。

である。この手法においては、オリジナルのハッシュ値が正しいことを前提としている。したがって、このオリジナルのハッシュ値は、信頼できる確実な情報源から入手することが重要である。また、高度なスキルさえ保有していれば、ソフトウェアを解析することにより、不正な機能が埋め込まれているかどうかを調査することも可能ではある。しかしながら、このような調査は時間との戦いである。あらかじめ、何らかのヒントがない場合には不正な機能の発見は難しく、完全な調査には非常に時間を要する場合が多い。例えば、あるアプリケーションに不正な機能が混入されていることが疑われる場合、そのソースコードを納品させていれば、そのソースコードを解読して調査を実施することが可能である。ここで、その不正な機能がバックドアであると判明している場合、ネットワークに関係する機能を重点的に調査すれば良い。このようなヒントがない場合には、何らかの見当をつけ、分析者の直感と経験に基づいて調査せざるを得ない。したがって、その精度は分析者の能力に大きく依存する。ソースコードを納品させていない場合には、専用のソフトウェアを用いてソースコードに逆変換するか、あるいは難しい場合には機械語に逆変換して解析を実施することになる。機械語を解析する場合には、この作業はさらに難解となる。納品されたソースコードを調査する場合には、納品された実行ファイルが確かにそのソースコードから生成[41]されたことを確認することも重要である。なぜならば、攻撃者が実行ファイルを置き換える可能性があるためである。この作業は、ソースコードから生成した実行ファイルと納品された実行ファイルを比較することで、容易に実施することが可能である。

このように、ソフトウェアの場合においては特別な機材を必要としないが、不正な機能がないことを確認するには高度なスキルと多大な労力を要する。そのため、ソフトウェアの場合においても、サプライチェーン・リスクの対策として、すべてのソフトウェアを調査するのは現実的とは言い難い。

５　現実的な対策

（１）管理体制の確認

サイバーセキュリティにおけるサプライチェーン・リスクの技術的な対策は、ハードウェアの場合は特に困難であり、すべての調達品に適用するのは現実的ではない。そこで、調達時に仕様書等でサプライチェーン・リスクを含めた管理体制を要求し、その実効性を確認することが現実的な対策となる。

例えば、企画段階においては、サプライチェーン・リスクを含めた情報セキュリティ対策の管理体制を明示させ、必要な場合に監査を実施できるようにして透明性を確保する。調達や構築時には、そのような管理体制が整っており、従事者の身元や専門性を証明する情報や、インシデントに関する対応や再発防止策を開示できる事業者を選定する。また、再委託を禁止する場合にはその旨

[41]コンパイルと言う。

を明示し、禁止しない場合にも委託元の許可を得ることを要件とする。運用・保守や廃棄等の場合には、情報セキュリティ対策の実施状況を確認し、実施手順を定めて遵守させる。

このような対策は、事業の効率とトレードオフの関係にあり、両者のバランスをとることが重要である。また、従事者の身元や専門性を証明する情報については機微な情報となる可能性があるため、どこまで踏み込むかについては慎重に考慮する必要がある。したがって、現実的には顧客と受注業者間の信頼関係の問題に帰属する可能性がある。そのため、過去の実績等も考慮し、普段から良好な信頼関係を構築しておくことは重要である。しかしながら、調達の公平性が損なわれないように十分に留意する必要がある。

（２）多層防御

調達における仕様書等における対策は、本質的には顧客と受注業者間の信頼関係の問題である。したがって、十分なセキュリティ対策を実施してしたとしても、攻撃側が高度な手法を用いた場合には、バックドア等の不正な機能を発見できない可能性はある。また、人為的なミスあるいは故意により、セキュリティ対策が機能しない場合もあり得る。

そこで、調達品において何らかの不正な機能が発見されたとしても、その部分を分離し、他の階層で防御することができる多層防御の体制を構築しておくことが重要である。その調達品が重要な機能をはたす場合には、代替の機能を他社製品で構築することも一案である。

６　監視システム

サプライチェーン・リスクのより大規模な事例としては、世界規模で通信内容を傍受（盗聴）する監視システムの存在が挙げられる。これらは、通信経路を構成する機器やソフトウェアを受注する業者であれば、それらに不正な機能を追加することで構築することが可能である。インターネットや携帯電話網のような誰もが利用する通信経路であれば、その影響範囲はより広くなる。監視システムの表向きの必要性は犯罪やテロの捜査であるが、国家のインテリジェンス活動において非常に有益である点は否定できない。

（１）米国の監視システム

米国の代表的な監視システムとしては、２０１３年にスノーデン氏によって暴露されたＰＲＩＳＭやＸＫｅｙｓｃｏｒｅが挙げられる。

ＰＲＩＳＭは米国の国家安全保障局[42]が２００７年から運用する監視システムであり、マイクロソフト、Ｇｏｏｇｌｅ、Ｆａｃｅｂｏｏｋ、Ａｐｐｌｅ、ＹｏｕＴｕｂｅ等のサービスから、利用者のメール、文書、画像、通信記録等を収集して監視している。この監視プログラムでは、これらの人気サービスのすべての利用者が監視対象となる。したがって、これらのサービスを利用しな

[42] NSA (National Security Agency)

ければ、監視システムの影響を受けることはない。しかしながら、これらのサービスは非常に利便性が高いため多くの人々が利用しているため、完全に利用を停止することは困難である。

ＸＫｅｙｓｃｏｒｅも国家安全保障局が運用する監視システムであり、通信内容や検索エンジンに入力された単語等が傍受できるとされている。その情報源は、在外米国大使館および領事館、他国が利用するデータ処理衛星からの傍受、海底ケーブルの盗聴、同盟国の施設で収集した電波等であると考えられている。

このように、米国の監視システムの多くは世界規模であり、その情報は主にファイブアイズ[43]と呼ばれる同盟国で活用されている。

（２）中国の監視システム

中国の監視システムとしては、１９９８年から運用されているグレート・ファイアウォール（金盾）[44]が知られている。グレート・ファイアウォールは中国本土（香港とマカオを除く。）のインターネット検閲システムであり、通信の傍受だけでなく、政府に都合が悪い特定の用語を含む通信の遮断も実施している。また、インターネットを完全に遮断する機能も有している。

２０１５年４月には、Ｇｒｅａｔ　Ｃａｎｏｎ[45]と呼ばれるサイバー攻撃に用いられる機能の存在も確認されている。Ｇｒｅａｔ　Ｃａｎｏｎでは、傍受した通信を改ざんして乗っ取る中間者攻撃が可能であるとされている。さらに、その通信元に悪意あるコンテンツを送付して実行させることで、サイバー攻撃を実施させることも可能であると考えられている。２０１５年３月に発生したＧｉｔＨｕｂ[46]と呼ばれるサイトへのＤＤｏＳ攻撃では、グレート・ファイアウォールを回避する技術に関する文書の閲覧を妨害するために、この機能が用いられと考えられている。

さらに近年では、ＰＬＡ[47]と深いつながりがあるとされるＨｕａｗｅｉ社が、各国の次世代通信網である５Ｇ[48]の基地局や機器を受注しようと画策している。

このように、中国の監視システムはもともと国内を監視する用途で運用されてきたが、その対象を世界に広げようとする試みが見え隠れするようになってきている。

（３）その他の監視システム

その他の国家規模の監視システムとしては、ロシアのＳＯＲＭが挙げられる。ＳＯＲＭは１９９５年から運用されているロシア国内の電話、インターネ

---

[43] 米国、英国、カナダ、オーストラリア、ニュージーランドの諜報機関の協定

[44] Wired (2015). “The Great Firewall of China”

[45] The Citizen Lab (2015). “China’s Great Cannon”

[46] インターネットを活用して共同でソフトウェアを開発するためのサービス

[47] 人民解放軍

[48] 第５世代移動通信システム

ット等の監視システムであり、２０１４年にはソーシャル・メディアもその監視対象に含まれるようになった。

7　おわりに

本稿では、サイバー戦の一環としてのサプライチェーン・リスクをとりあげた。第２節ではサプライチェーン・リスクの具体例をハードウェア、携帯電話及びソフトウェアに分類して列挙するとともに、諸外国の規制について示した。第３節ではサプライチェーン・リスクの定義、不正な機能の追加手法及び全体像について説明した。第４節ではサプライチェーン･リスクの技術的な対策手法とその困難性について述べ、第５節では現実的な対策である管理体制の確認と多層防御について示し、最後にサプライチェーンの集大成とも言える大規模な監視システムの概要について述べた。

本稿で具体例を示したように、サイバーセキュリティの文脈におけるサプライチェーン・リスクはもはや現実のものであり、その脅威は顕在化していると言える。サイバー戦の特性を考慮すると、これらの顕在化している脅威は氷山の一角である可能性が高く、さらに多くの製品にバックドアが仕込まれている可能性は否定できない。スノーデン氏に暴露されなければ、米国製のネットワーク機器等に仕込まれたバックドアの発見はさらに遅れるか、あるいは発見されなかった可能性すらある。また、脆弱性は故意に作成したり、発見したとしても故意に放置したりすることにより、バックドアとして利用することができる場合もある。このようなバックドアとして利用することができる脆弱性は、故意に作成されたのか否かの判断が難しい。それに加え、ＩｏＴ機器の急速な普及に伴い、サプライチェーン・リスクの範囲もあらゆる電子機器に対象が拡がっている。そのため、あらゆる電子機器の製造に関与する業者等が、サイバーセキュリティの問題に直面するようになってきている。しかしながら、電子機器の製造に関与する業者等の当事者意識は低く、意図せず脆弱性のある製品を製造してしまう例は珍しくない。また、脆弱性があることを指摘されたとしても、サイバーセキュリティに関する知識不足のためその指摘内容が理解できず、脆弱性が修正されずに放置されてしまう場合すらある。あるいは、その業者に悪意があり、意図的に脆弱性を修正しない可能性も考えられる。このように、サプライチェーン・リスクの問題は根が深いだけでなく、その対象範囲も大幅に拡大している。そのため、すべての人々が当事者意識を持ち、その脅威を十分に認識するとともに、現実的な対策を確実に実施することが重要である。