DIR SOC Quarterly

2022 vol.2

大和総研

Daiwa Institute of Research

目次

はじめに

本冊子は、サイバー攻撃の状況と対策の動向をタイムリーにお伝えすることを目的としています。今回は第 2 四半期の話題を取り上げます。

本冊子は三部構成となっています。第 1 部は、サイバー攻撃対策が国家主導の下に行われており、それを指揮する行政機関の動向をウォッチすることが不可欠であるため、この点にフォーカスしています。また実際のインシデント事例は、組織がさらされているサイバー攻撃の状況を端的に示すと同時に、組織の対策のあるべき姿を浮かび上がらせるものです。第 2 部はこの点に注目しています。また第 3 部では、注目度の高いサイバーセキュリティ関連の話題を「トピックス」として詳しく説明します。

今回の第 1 部では 2022 年第 2 四半期におけるわが国の政策・法制度の動向を取り上げます。昨今クラウドサービスの設定ミスによる情報流出が数多く発生しており、それを受けて総務省から『クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）』が公表されました。クラウドサービスを利用する上では「適切な設定」がいかに重要かということが官民ともに認識されつつあると言えます。また同じく総務省から『ICT サイバーセキュリティ総合対策 2022』が公表されました。ここに記載されている諸施策は、ますます巧妙化・高度化するサイバー攻撃に対し、サプライチェーンも含めて迅速に対処してく必要性を示しています。このことは、昨今話題に挙がることが増えた「積極的サイバー防御」にも通じます。

第 2 部では 2022 年第 2 四半期に注目を集めたインシデント事例を取り上げます。1 つ目のインシデント事例は、これまで有効とされてきたセキュリティ対策もサイバー攻撃の巧妙化により突破される危険性があることを示しています。2 つ目のインシデント事例は第 1 部で取り上げた『クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）』と関連し、最近の情報流出の傾向と組織全体として対策していくことの重要性を端的に表していると言えます。

最後に、第 3 部では国内外で注目を集める SBOM について解説します。SBOM は「ソフトウェア部品表」であり、サプライチェーンのセキュリティ確保に関して有効な対策となりえますが、重要なポイントはソフトウェア開発ライフサイクル全体の中で SBOM を活用していくということです。

上記トピックスのいずれかが皆様の日々の活動に関連する何らかの「気づき」や「きっかけ」となれば幸いです。

2022 年 11 月　株式会社大和総研執筆者一同

1. 『クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）』に対する意見募集

クラウド設定ミスにもとづく事故の多発

総務省は 2022 年 7 月 25 日、「クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）」に対する意見公募手続（パブリックコメント）を開始しました（8 月 24 日終了）。パブリックコメントの結果を踏まえて、今秋に策定・公表される予定です。

近年、クラウドサービスの利活用が急激に拡大する中で、利用者がクラウドサービスを利用する際の、またクラウド再販事業者が他事業者のクラウドサービスを調達し提供する際の、設定ミスに起因する情報漏洩や障害といった事故が多発しており、クラウドサービスの利用におけるリスクとして社会的に問題になっています。

また IPA の調査(*1)によると、不正アクセスの原因別比率では、設定不備が全体のおよそ 17.7%で第 2 位（前年は第 1 位）と相変わらず多く、このような社会問題を引き起こす原因として無視できなくなっています。こうした動向を踏まえ、本ガイドラインの策定に至りました。

ガイドラインの構成

このガイドラインでは、クラウドサービスを巡る最近の動向を踏まえ、クラウドサービスの設定に関する責任共有の考え方、利用側、提供側が取り組むべき対策を以下の章立てで取りあげています。

1. 序編
2. 前提および概要
3. クラウドサービス利用側に求められる対策
4. クラウドサービス提供側に求められる対策
5. 対応一覧

上記 4 つの章の概要や具体的な対策例は下表のとおりです。

章	主な対策内容、対策例など
Ⅰ. 序編	本ガイドラインの目的・位置付け・利用方法、使用している用語の定義など
Ⅱ. 前提および概要	クラウドサービスの利用例、クラウドサービスの提供側に共通して認識すべき基本的事項、設定不備によるリスク、設定不備の要因と対策など
Ⅲ. クラウドサービス利用側に求められる対策	利用側において設定ミスを抑止・防止するための対策。対策例として、クラウド利用における社内ガバナンスの確保や、支援ツールや外部診断サービスの活用など
Ⅳ. クラウドサービス提供側に求められる対策	提供側において設定ミスを抑止・防止するための対策。対策例として、正しく、十分で、わかりやすく、タイムリーな情報の提供や、設定項目管理ツールの提供など
ANNEX　対策一覧	利用側における対策及び提供側における対策の対策項目

表：『クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）』から抜粋

(*1) 独立行政法人情報処理推進機構（IPA）「コンピュータウイルス・不正アクセスの届出状況 2021 年」

本ガイドラインの特徴

わが国のクラウドサービスに関するガイドラインは、利用側、提供側向けに下記が整備されています。ただし、いずれも設定不備の抑止・防止について言及されていません。そこで、本ガイドラインは下記のガイドライン等をベースにしつつ、昨今のインシデントの発生を踏まえて、クラウドの利用場面、提供場面における適切な設定を促進するための対策に焦点を絞ったガイドラインとなっています。

【わが国のクラウドサービスに関する主なセキュリティガイドライン】

- 「政府情報システムのためのセキュリティ評価制度（ISMAP）」（内閣官房）
- 「政府機関の情報セキュリティ対策のための統一基準」（NISC）
- 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（経済産業省）
- 「クラウドサービス提供における情報セキュリティ対策ガイドライン」第 3 版（総務省）

本ガイドラインからの示唆

注目したいのはクラウドサービスの設定不備を防止する対策として、ツールの利用を推奨していることです。本ガイドラインで、「ツール」という単語は 71 回登場していますが、上位 3 つは「支援ツール」（24 回）、「診断ツール」（9 回）、「管理ツール」（7 回）です。これは、目視等による手動での対応の限界を示唆しています。

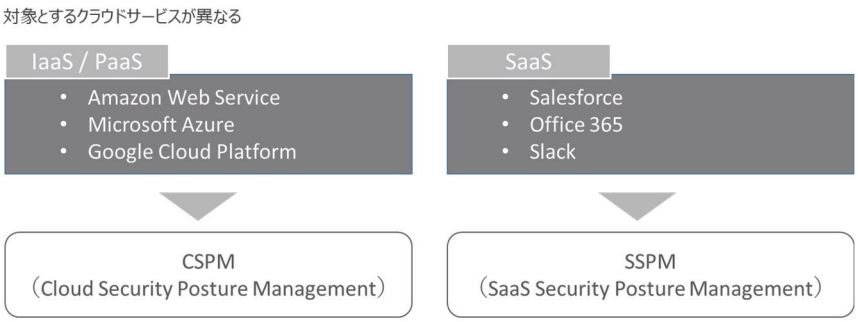
わが国では、企業がクラウドの運用の全部または一部をシステム・インテグレーター等に委託する形態をとることが少なくありません。システム・インテグレーター等がクラウドを利用してサービスを提供する場合、クラウドサービスの提供側、利用側の両方の立場を兼ねることになります。そのどちらの立場でも言えることですが、クラウドサービスを使いこなすうえで、設定項目量の増加や、整合性の確保といった設定項目の複雑化への対応が課題と言えるでしょう。

これらの課題に対処するため、設定値全体の整合性監視やルールを外れた設定値を警告・復元するなどの支援ツールを利用することが有効です。本ガイドラインでは、クラウドサービス利用側に求められる対策のベストプラクティスとして、SASE（Secure Access Service Edge ）など のセキュリティゲートウェイを通すことや CSPM（Cloud Security Posture Management）といったツールの必要性が記載されていました。

特に CSPM は、クラウドセキュリティの状態管理ツールと呼ばれるもので、主にクラウドセキュリティの構成ミス、管理不備などへ対応するためのものです。クラウドの設定ミスによる情報漏洩に対して有効なソリューションとして注目されています。具体的には、IaaS/PaaS(*1)といったクラウドに対して API 連携により、クラウド側の設定を自動的に確認し、セキュリティの設定ミスや各種ガイドライン等への違反が無いかを継続してチェックすることができます。また、機能の一つとして CSPM を提供しているモニタリングサービスもあります。効率的な運用ツールの利用を考慮して、このようなモニタリングサービスと合わせて検討すると効果的でしょう。

SaaS アプリケーションに焦点を当てた SSPM

クラウドの設定不備による事故を予防するためのソリューションとして、類似したものに SaaS Security Posture Management （SSPM）があります。SSPM は、 SaaS を対象とした設定ミスを監査するソリューションです。Salesforce 等のクラウドサービスはクラウド上でサービスが提供されているため随時機能が追加されます。本来はこのようなサービスの追加は利用者にとって好ましいものです。しかしながら、新機能の追加によりアクセス権限が変更され意図せぬ情報漏洩等が発生することが問題視されるようになってきました。こういった設定ミスを機械的に対処するためのソリューションとして SSPM が注目を集めています。



出典：大和総研作成

DX が進む中、様々な形態のクラウドサービス利用されていると思います。クラウドサービスの利用における設定の運用を今一度点検することは、ツール利用等のリスクコントロール策を講じる良い機会だと考えます。

(*1) IaaS は"Infrastructure as a Service"の略記。CPU、メモリ、ストレージやネットワークといったリソースを提供するモデルです。PaaS は"Platform as a Service"の略記。アプリケーション開発に必要な実行環境を提供するモデルです。

2. ICT サイバーセキュリティ総合対策 2022 の公表

「総合対策 2022」の概要

総務省のサイバーセキュリティタスクフォース(*1)は 2022 年 8 月に「ICT サイバーセキュリティ総合対策 2022」（以下、総合対策 2022 と略記）を公表しました。この総合対策 2022 では、サイバーセキュリティを巡る最近の動向を踏まえ、総務省において今後重点的に取り組むべき施策の柱として以下の 4 つをあげています。

1. 情報通信ネットワークの安全性・信頼性の確保
2. サイバー攻撃への自律的な対処能力の向上
3. 国際連携の推進
4. 普及啓発の推進

上記 4 つの柱の概要や具体的な施策例は下表のとおりです。以降では、総合対策 2022 であげられている施策のうち、昨今話題となっている「積極的サイバー防御」と関わる施策である「**電気通信事業者による積極的サイバーセキュリティ対策の推進**」と、国内外で急速に関心が高まっている「SBOM」に言及している施策である「**情報通信分野におけるサプライチェーンリスク対策**」を取り上げます。

No.	施策の柱	主な施策内容、施策例など
1	情報通信ネットワークの安全性・信頼性の確保	電気通信事業者による積極的サイバーセキュリティ対策の推進、IoT におけるサイバーセキュリティの確保、情報通信分野におけるサプライチェーンリスク対策確保、トラストサービスの普及など。
2	サイバー攻撃への自律的な対処能力向上	国内でのサイバーセキュリティ情報生成や、人材育成を加速するエコシステムの構築、サイバーセキュリティに係る実践的な研究開発推進、実践的サイバー防御演習の実施など。
3	国際連携の推進	各国政府・民間レベルでの情報共有や国際標準化活動への積極的な関与、開発途上国に対する能力構築支援、国内企業のサイバーセキュリティ分野における国際競争力の向上を図る取り組みなど。
4	普及啓発の推進	事業者向け、個人向けそれぞれについて、ターゲット（中小企業、地方企業、子供、高齢者）の課題と特性に合わせた普及啓発の推進、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の年内策定など

表：『ICT サイバーセキュリティ総合対策 2022』（ https://www.soumu.go.jp/main_content/000829941.pdf ）から抜粋

(*1) 総務省のサイバーセキュリティタスクフォースは、IoT/AI 時代のサイバーセキュリティの確保を強力に進めることを目的として、2017 年 1 月以降、継続的に開催されています。2019 年以降は毎年、サイバーセキュリティ確保のための施策をまとめた「総合対策」を公表しています。

電気通信事業者による積極的サイバーセキュリティ対策の推進

総務省では 2013 年 11 月より「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を開催し、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取り組みを講じていくことが可能となるよう検討を行ってきています。

この研究会では、電気通信事業者が C&C サーバ(*1)を検知したり、C&C サーバの情報を共有したりすることについてその適法性を議論・検討してきましたが、一定の整理ができたとして（詳細は次ページを参照）、2022 年および 2023 年には C&C サーバの検知技術の実証や検知精度の高度化、検知結果の事業者間共有の実証などを行う方針としています。

また、通信の秘密に配慮しつつ電気通信事業者によるより迅速なサイバー攻撃対策を実現するために、既存の法的整理に関する現状及び課題や諸外国における法制度の状況を整理した上で、制度改正の必要性を含め検討を行うことも今後の取り組みとして示しています。

このような施策は、サイバー攻撃を事前に、もしくはその早期の段階で検知し、迅速にサイバー攻撃に対処していこうとする試みであり、いわゆる「積極的サイバー防御」として位置づけられる施策と言えます。「**積極的サイバー防御**」は、政府が 2021 年 9 月に公表した「サイバーセキュリティ戦略」(*2)において、「**サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じていく取組のこと**」と定義されています。この「サイバーセキュリティ戦略」では、包括的なサイバー防御を着実に実施していくための環境整備の一つとして「『積極的サイバー防御』に係る諸施策」をあげており、今後もこのような「積極的サイバー防御」として位置づけられる施策が増えていく可能性があります。「積極的サイバー防御」に関するその他の施策については後述します。

(*1) Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータ（いわゆる踏み台もしくはボット）を多数利用したサイバー攻撃（例：DDoS 攻撃）において、攻撃者側から踏み台（ボット）に対して命令を送り、制御を行うサーバコンピュータのことです。C2 サーバと呼ばれることもあります。そして、多数のボットが組織化されたネットワークをボットネットと呼びます。

(*2) 「サイバーセキュリティ戦略」 p23 (https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf)

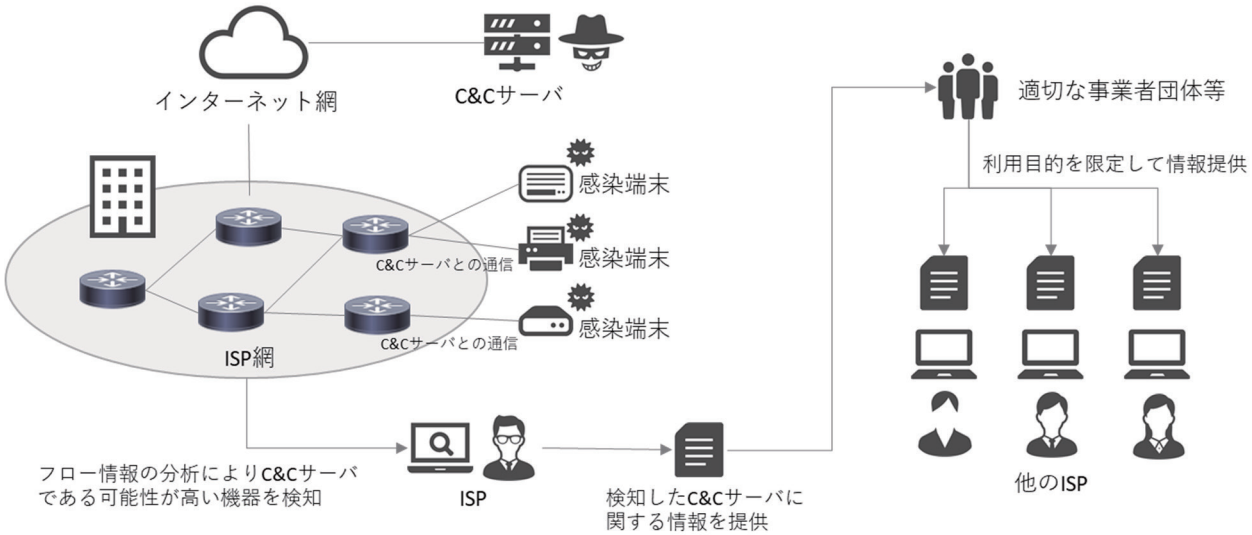
参考：2021 年 11 月の研究会とりまとめ

「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」では、2021 年 11 月に「第四次とりまとめ」（https://www.soumu.go.jp/main_content/000779208.pdf）を公表し、この中で以下 2 点の整理を行っています。

① 平時において、電気通信設備を通過する通信データのうち、IP アドレス・ポート番号やタイムスタンプ等の情報（フロー情報）を収集・蓄積・分析して、C&C サーバである可能性が高い機器の検知をすることは正当業務行為である

② 上記①により検知した C&C サーバに関する情報を共有することは通信の秘密の保護規定に直ちに抵触するとまではいえない

なお、「通信の秘密」は、基本的人権の一つとして憲法上保護されているものであり、電気通信事業者が侵してはならないものです。たとえば、電話会社は、通話の内容を盗み聞きすることは許されません。また、「正当業務行為」とは電気通信事業者の業務遂行上、正当かつ必要な行為であり、通信の秘密の侵害に該当しないものです。例えば、料金請求のために必要最低限度で通信履歴を確認する行為などです。



図：フロー情報を収集・蓄積・分析して検知した C&C サーバに関する情報についての共有

出典：「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」の概要（https://www.soumu.go.jp/main_content/000779408.pdf）に掲載の図を基に大和総研作成

情報通信分野におけるサプライチェーンリスク対策

総務省は、2022 年 4 月に公表した「5G セキュリティガイドライン第 1 版」(*1)について、国内の 5G ネットワークオペレータ（電気通信サービスプロバイダ及び 5G システムを展開して運用するその他の組織）への普及を図り、5 G サービスのサプライチェーン全体のセキュリティ確保に取り組むとしています。このガイドラインは 5G ネットワークのオペレータ向けに作成されたものですが、5G オペレータはベンダーの選択プロセス、調達プロセス及びソリューションのライフサイクル全体にサプライチェーンセキュリティを組み込む必要がある旨が記載されています。

また総務省は、Apache Log4j(*2)など広く利用されているソフトウェアの構成部品の脆弱性への対処が重要となっている状況に鑑み、ソフトウェア製品の構成部品を管理して脆弱性に迅速に対応することを可能とする仕組みである SBOM（Software Bill of Materials)について、情報通信分野における導入の可能性を検討していくとしています。

注目施策からの示唆

上記で取り上げた「電気通信事業者による積極的サイバーセキュリティ対策の推進」は、サイバーセキュリティの文脈において昨今話題となっている「積極的サイバー防御」に関わる施策です。また、「情報通信分野におけるサプライチェーンリスク対策」では、米国における 2021 年 5 月の大統領令で触れられて以降、日本でも話題となっている SBOM について言及されています。いずれの施策も直接関わるのは電気通信事業者等であり、その他の事業者や組織には直接的には関係がありません。しかし「積極的サイバー防御」の考え方や SBOM の仕組みは、情報通信業界以外の組織も理解を深め、自組織のセキュリティ対策に取り入れていくことにより、セキュリティレベルの向上に役立てていくことが可能です。「積極的サイバー防御」については次ページの「3. 積極的サイバー防御と関係する施策」で、「SBOM」については第 3 部のトピックスで扱います。

(*1) https://www.soumu.go.jp/main_content/000812253.pdf

(*2) 2021 年 12 月に、Java の OSS ライブラリ Apache Log4j に、深刻な脆弱性が発見されました。この脆弱性は悪用が容易なこと、そして、Apache Log4j は多くのソフトウェアやアプリケーションが利用するログ出力ライブラリであることにより、世界中で大問題となりました。

3. 積極的サイバー防御と関係する施策

「積極的サイバー防御」の定義について

「積極的サイバー防御」という用語およびその基になっている「アクティブ・ディフェンス」や「アクティブ・サイバー・ディフェンス」という用語の定義を巡っては、「反撃」や「攻撃」の意味を含むかどうかを巡って多くの議論(*1)(*2)がなされているようです。しかし元々の定義では、「反撃」や「攻撃」の意味は含まれていないようです。7 ページに記載したとおり、日本政府は「積極的サイバー防御」を「**サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じていく取組のこと**」と定義しています。また、「アクティブ・ディフェンス」や「アクティブ・サイバー・ディフェンス」については、代表的な定義として以下のようなものがあります。

「アクティブ・サイバー・ディフェンス」（米国の国家安全保障局（NSA）の Web ページに記載されている内容 (*3)）

> 重要なネットワークやシステムへの脅威に対して、リアルタイムな検知、分析、緩和を同期させることにより、予防的で革新的なサイバー防御の試みに寄与するものであり、この概念は国防総省だけでなく、すべての米国政府機関や重要インフラネットワークに適用できるものである。アクティブ・サイバー・ディフェンスは**攻撃的なものではなく**、その機能は**防御するネットワークの範囲内にのみ影響を及ぼす**ものである。

「アクティブ・ディフェンス」（セキュリティ関連の著名な教育機関である SANS Institute が発行しているホワイトペーペーの定義 (*4)）

> **ネットワークに内在する脅威に対して**、分析者が監視し、対応し、理解を深め、そして知見を適用するプロセス

いずれも「積極的に」自組織内の脅威を検知し、対処していくようなプロセスとして定義されていると言えます。

(*1) 「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か ―より具体的な議論に向けて必要な観点について―（https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html）

(*2) アクティブディフェンスとその先行事例について（https://jpn.nec.com/cybersecurity/blog/220204/index.html）

(*3) Active Cyber Defense (ACD)（https://apps.nsa.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm）

(*4) The Sliding Scale of Cyber Security（https://www.sans.org/white-papers/36240/）

積極的サイバー防御と関わる施策

7 ページで触れた電気通信事業者による C&C サーバの検知および情報共有のような施策以外にも、積極的サイバー防御と言えるような施策には以下のようなものがあります。いずれも積極的に攻撃者および攻撃対象の情報を収集し、事前もしくは攻撃の早い段階で防御していこうとする取り組みと言えます。

サイバー攻撃に悪用される恐れのある IoT 機器に関する注意喚起（NOTICE 注意喚起）

総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダは、相互に連携し、サイバー攻撃に悪用される恐れのある IoT 機器の調査及び当該機器の利用者への注意喚起を行っています。これは、2018 年の国立研究開発法人情報通信研究機構法の改正に基づく取り組みであり、2019 年 2 月から 2024 年 3 月までの時限措置です。なお、この取り組みは「NOTICE 注意喚起」(*1)と呼ばれており、NOTICE とは National Operation Towards IoT Clean Environment の略です。

マルウェアに感染している IoT 機器に関する注意喚起（NICTER 注意喚起）

総務省、NICT、一般社団法人 ICT-ISAC、インターネットプロバイダ各社は、相互に連携し、国立研究開発法人情報通信研究機構（NICT）の NICTER プロジェクトによりマルウェアに感染していることが検知された IoT 機器に対して、インターネットプロバイダから利用者へ注意喚起を行っています。NICTER（Network Incident analysis Center for Tactical Emergency Response の略）とは、無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システムのことです(*2)。また前述の注意喚起は「NICTER 注意喚起」(*3)と呼ばれています。NICTER プロジェクトでは、このシステムを用いてサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施しています。

(*1) https://notice.go.jp/

(*2) https://www.nicter.jp/

(*3) https://notice.go.jp/nicter

認定送信型対電気通信設備サイバー攻撃対処協会の業務追加

2022 年 6 月に「電気通信事業法の一部を改正する法律」が成立しました。この中で、「認定送信型対電気通信設備サイバー攻撃対処協会」の業務として、電気通信事業者が DDoS 攻撃(*1)等のサイバー攻撃を受けた場合に加えて、**攻撃の準備行為の標的となった場合も**、そのサイバー攻撃についての調査・研究、および、攻撃への対処支援などを行うことが定められました。

なお、「送信型対電気通信設備サイバー攻撃」とは、主に DDoS 攻撃のことを差します。またこの「認定送信型対電気通信設備サイバー攻撃対処協会」として、現在は一般社団法人 ICT-ISAC が指定されています。(*2)

(*1) Distributed Denial of Service の略であり、インターネット上の多数のコンピューターから攻撃先の機器や設備に大量のパケットを送り付けることによって、その機器や設備を機能不全（サービス停止）に陥らせる攻撃のことです。

(*2) https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000057.html

「積極的サイバー防御」という概念の有用性

このように積極的サイバー防御（アクティブ・サイバー・ディフェンスおよびアクティブ・ディフェンス）の考え方は政府の政策に取り入れられつつありますが、一般の民間組織にとっても、この概念からは学ぶべきことが多いと思われます。

たとえば、米国の国家安全保障局（NSA）の Web ページでは、アクティブ・サイバー・ディフェンスを実装する上で、以下の 5 つのコンポーネントが必要であるとしています。

① ネットワークの現状を報告するセンサー
② そのネットワークの現状を理解するための分析機能
③ 分析結果に基づいて自動で意思決定を下す機能
④ 意思決定結果に基づいてネットワークを防御するために対応する機能
⑤ 上記 4 つ機能間のリアルタイムコミュニケーションを可能にするメッセージング機能

そして、これらにより、瞬く間にデータが拡散していくサイバー空間にふさわしいスピードでの脅威の検知や緩和が可能になるとしています。このコンポーネントについて、果たして自分たちの組織は「サイバー空間にふさわしいスピードでの検知や緩和」が可能か問うてみてはいかがでしょうか。そして、もしできない場合、どのような分野でどのくらいできる必要があるのかを検討してみると良いでしょう。

1. 多要素認証疲労攻撃　ユーザーが「承認」するまで繰り返される

概要

米国 Uber は 2022 年 9 月 15 日（現地時間）、国際的ハッカー集団「LAPSUS$」のメンバーから内部システムへのハッキングを受けました。これに対して、米国のセキュリティ会社 Malwarebytes は 9 月 22 日(米国時間)、多要素認証疲労攻撃（MFA Fatigue）によるものだったと報じています。
Uber への攻撃は、攻撃者が事前に何らかの手段で従業員のユーザー名とパスワードの組み合わせを入手して、この従業員のアカウントに何度も繰り返しアクセスを試みていました。

Uber では認証に多要素認証（MFA： Multi-Factor Authentication）を採用しており、攻撃者がログインを試みると、従業員に対して承認をリクエストするプッシュ通知が届きます。従業員には 1 時間以上にわたり、大量のログイン承認を確認するプッシュ通知が送信され続けました。この後、攻撃者は欧州や米国で広く普及しているメッセージングアプリ（Slack）を介して従業員に接触し、Uber の情報システム担当のふりをして繰り返される通知を止めるには承認するしかないというメッセージを送り、従業員をだまして承認させ、結果、その従業員になりすまして内部システムへの侵入を成功させました。

プッシュ通知による認証のイメージ

出典：大和総研作成

多要素認証とは

サイバー攻撃者は一般的に、不正アクセスを目的に「ブルートフォース攻撃」「辞書攻撃」「パスワードリスト攻撃」、「ソーシャルエンジニアリング攻撃」など様々な手法を使用してパスワードの漏洩を狙い、従業員の資格情報にアクセスを試みます。これに対して、仮にパスワードが狙われたとしても、更に別の認証方法を伴わないとログインができないようにするのが多要素認証（MFA：Multi-Factor Authentication）です。この多要素認証（MFA）の普及に伴って、増えてきているサイバー攻撃の一つが、多要素認証疲労攻撃（MFA fatigue）です。

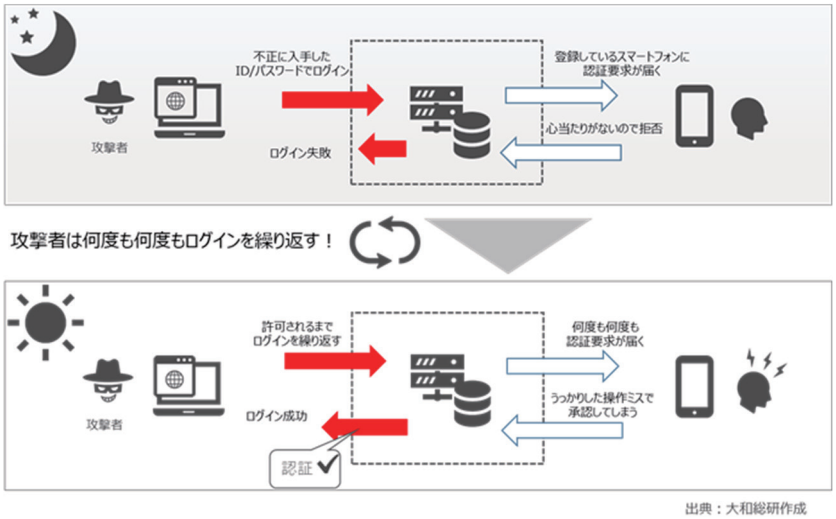
多要素認証疲労攻撃とは

多要素認証疲労攻撃は、「MFA プッシュスパム」と呼ばれることもあり、ユーザーがアカウントを安全に保つために使用する多要素認証を突破することを目的としています。プッシュ通知を利用する多要素認証に対して、故意にプッシュ通知を乱発することで、ユーザーがうっかり「承認」することを期待する攻撃手法です。この攻撃の前提となるのは、ID とパスワードの情報漏洩により攻撃者が ID とパスワードを知っているということです。

人間の脆弱性を突く巧妙な罠

Uber で利用されていた多要素認証は、ログイン時にユーザー名とパスワード（ SYK：Something You Know）の入力と、事前に登録されたスマートフォン（ SYH：Something You Have）内の SMS アプリへ送られるプッシュ通知の「承認」を組み合わせたものです。

仮に心当たりのない通知があなたのスマートフォンに届いた場合はどうでしょうか。不審に思い通知を拒否するのは自然で容易なことです。しかし、寝静まった夜に 1 時間続けざまに、あなたのスマートフォンにプッシュ通知が来たとしたらどうでしょうか。周りにはすぐに相談できる同僚はおらず、大量に通知が来ると必要な通知が埋もれかねない状況です。眠くて十分に頭が働かない中ですべての通知を拒否するわけですが、うっかり操作を誤り「承認」を押してしまう可能性はゼロではありません。Uber への攻撃は更に巧妙で、別途 Slack を介して自社の情報システム担当と名乗る人から連絡が来て、この通知を止めるための方法としてまず承認することを指示してきます。この情報システム担当者は実は偽物で、ソーシャルエンジニアリング攻撃と組み合わせた一連の流れによる攻撃でした。



出典：大和総研作成

対策

MFA の利用し始めはこの攻撃に慣れていないため、大量に届く通知をただちに無くなって欲しいと思う人や、自分が何をやっているのか分からず通知を機械的に受け入れる人もいるようです。このような中で、すべての従業員が大量の通知の裏にある脅威を見抜くことはなかなか困難です。そのため、組織としてできる手段としては、まずはパスワードの流出を防ぎ、次に流出した場合は迅速に検知できる対策を徹底することが何より重要であると考えます。

多要素認証疲労攻撃の対策として下記が考えられますが、根本的にはヒューマンエラーを誘う攻撃に対する防御になります。

対策１：パスワードを変更する、またはロックアウトする

プッシュ通知を受信し続ける場合は、あなたのユーザー名とパスワードが盗まれて利用されている可能性があります。そのため、パスワードを変えてしまえば、通知は届かなくなります。

対策２：セキュリティ監視チームに通知が届くように体制を整備する

SOC（ Security Operation Center）等と連携し、ある一定期間内に認証要求が閾値を超えたり、通常ログインしている地域外からの認証要求回数が閾値を超えたりした場合、利用者へ警戒するように連絡する体制を整えておきます。

対策３：第二の認証に「承認」「否認」の二択を促すだけのプッシュ通知を使用しない

攻撃者は、第二の認証要求がプッシュ通知による「承認」ボタンをクリックするだけという「利便性」を悪用してきます。利便性は低下しますが第二の認証をプッシュ通知から、ソフトウェアトークンやセキュリティキー方式に変更することで、「うっかり承認ボタンをクリックしてしまう」といった誤操作を軽減することが期待できます。

今後の対策の潮流

NISC（内閣サイバーセキュリティセンター）の「インターネットの安心・安心ハンドブック」をはじめ、NIST SP800-63B や PCI DSS 4.0 では、多要素認証に SMS 認証の活用を避けることを推奨しています。SMS を使ったワンタイムパスワード受信は、海外で SIM ハイジャックという攻撃により破られた例があり、セキュリティの面においても懸念があるためです。

出典：大和総研作成

多要素認証は不正アクセス防止に有効です。クラウド利用が一般的になりつつあり、技術面でもコスト面においても導入の壁が低くなりつつあります。多要素認証だから安全だという過信は禁物です。多要素認証を導入する際には、認証方法のメリット・デメリットを考慮して、認証の組み合わせを決定するのが良いでしょう。

2. 多発するクラウド設定ミスによる情報漏洩

概要

教育や与信管理などを事業展開する「リスクモンスター株式会社」は 2022 年 7 月 5 日、社員研修支援サービス「サイバックス Univ.」の運用サーバに登録した個人情報が Google などの検索エンジンからアクセス可能だったと発表しました。事態を把握した後は、すぐにサーバのネットワーク設定を変更して社外からアクセスできないようにしましたが、クラウドのネットワーク設定を行った 2020 年 2 月 16 日から 2022 年 6 月 29 日の 2 年超の間、登録者約 25 万人の個人情報が外部からアクセス可能な状態でした。

また、少なくとも過去 3 ヶ月の内、Google 検索エンジンからのアクセスが 18 件確認されており、その内 1 件は 5,934 件の個人情報がダウンロードされた痕跡が確認されています。なお、5,934 件の個人情報をダウンロードしたとみられる実行者に対しては、データの削除の依頼および、削除済みであることが確認されているとのことです。

クラウドにおける利用者責任の範囲

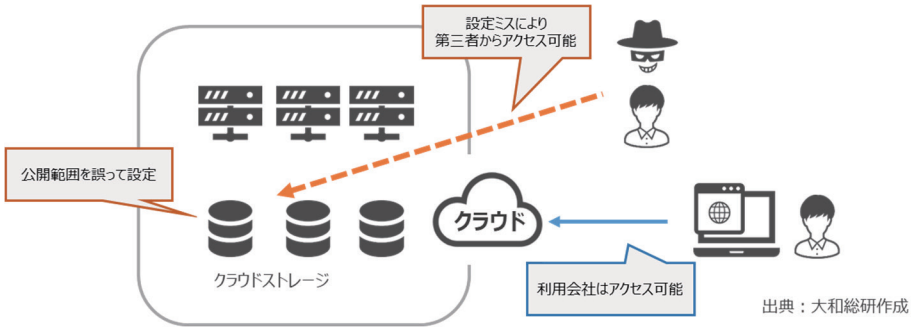
クラウドサービスを利用する上で大切なことは、クラウドに保管されている重要な情報（データ）を、内部、外部からの盗用や漏洩、消失などから保護することです。クラウドではクラウドサービス提供側のデータセンター内でデータが管理されるため、利用側はシステムの管理やメンテナンスのために技術を持った人材を用意する必要がなく、オンプレミス(*1)に比べてコストが抑えられる長所があります。

ただし、クラウドサービスの利用で注意したいのが、誰がどの範囲まで責任を持つのかクラウドサービス利用側と提供側の間で認識を共有することです。これをクラウド責任共有モデルと呼び、クラウドサービス利用側と提供側がそれぞれ運用責任を共有するという考え方を指しています。クラウドの形態により責任範囲が変わりますが、どの形態であってもデータや設定情報などについては利用側の責任であることを認識する必要があります。

（*1）システムの稼働やインフラの構築に必要となるサーバ、ネットワーク機器、ソフトウェアなどを自社で保有し運用するシステムの利用形態です。

設定のリスク

クラウドの設定ミスなどのセキュリティホールは気づかないことが多く、トレンドマイクロ社の調査(*1)によると 4 割以上のインシデントが外部からの指摘により発覚しています。クラウドサービスの利用において、管理やメンテナンスのための専門技術を持った人材を用意する必要がないため、IT やセキュリティに詳しい利用者ばかりとは限らず、セキュリティ意識が高くない場合もあります。そのため、環境構築時の利便性を優先した権限設定のままリリースしてしまったり、クラウドサービスの仕様を正しく把握していない状態で誤った設定をしてしまったりするケースが発生します。このようなリスクを把握したうえで、日々変化するクラウドの設定や管理をどのように行っていくかを意識する必要があります。



【クラウド設定ミスの例】

・ アクセス制限の不備

（例）AWS S3 バケット（データ保存領域）が一般に公開されるケースや、

攻撃者がデータにアクセスし攻撃者自身にアカウント権限を付与できるケースがある。

（*1）トレンドマイクロ 2021 年上半期セキュリティラウンドアップ（ https://resources.trendmicro.com/jp-docdownload-form-m381-web-20211h-securityroundup.html ）

・ セキュリティグループポリシー

（例）AWS EC2 サーバへ誰でもリモートアクセスが許可されているケースがある。

結果、遠隔による攻撃を許してしまう。

クラウドのセキュリティ対策

クラウドの設定ミスによる情報流失事案の増加を受け、総務省は 2022 年 7 月 25 日、クラウドサービス利用・提供における適切な設定を推進するため、設定におけるリスクと対象に特化した「クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）」を作成し、当該ガイドライン案について意見の募集を行いました。

その他、総務省ではクラウドサービスを取り巻く環境の変化を踏まえ、クラウドサービスにおける責任分界のあり方や国際規格等との整合性の観点から、2021 年 9 月に「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」として取り纏めています（2014 年初版、2018 年第二版）。本ガイドラインでは、クラウドサービスにおける責任共有の考え方に触れ、利用側と提供側でクラウドサービスの内容やクラウドサービス利用条件・環境ごとに、責任範囲と内容について契約で明示することが重要であるとされています。

「クラウドサービス事業者とクラウドサービス利用者の責任」（総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」に記載されている内容 (*1)）

> クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方（責任共有モデル）を多くのクラウドサービス事業者が採用している。ただし、責任共有モデルにおけるクラウドサービス事業者とクラウドサービス利用者の責任範囲・内容は一律に決まるものではなく、クラウドサービスの内容やクラウドサービス利用条件・環境ごとに、**両者で責任範囲と内容について合意し、契約で明示することが重要**である。

（*1）総務省 クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）
（ https://www.soumu.go.jp/main_content/000771515.pdf ）

一般的に、管理するデータや設定情報はクラウド利用側の責任であることから、利用側はどのように対策をとっていけば良いでしょうか。「クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）」で対策の代表例としてあげられた CSPM 等の管理ツールを利用するのが有効だと考えます。

クラウドサービスの利用が今後も増える見込みであることから、設定ミスはセキュリティ上の脅威であり続けると予想されます。利用者が増え、利用ケースが広がれば、それだけミスも増えるでしょう。また、クラウド提供側はサービス拡充のため機能を増やし、利用側も自分たちの環境に合わせてクラウドの構成や利用方法が変化していくと考えられます。結果として、想定していなかった新しい設定不備が次々に出てくるかもしれません。目視等による手動での対応は既に限界に来ており、CSPM 等の管理ツールの導入は、重要な情報（データ）を守るために必要な対策ではないでしょうか。

1. SBOM

SBOM とは

SBOM（エスボム）は Software Bill of Materials の略称で、日本語ではソフトウェア部品表と訳されています。ソフトウェアを構築する際に使用される様々なソフトウェアコンポーネント（部品）やそれらの依存関係の情報をリスト化したものです。ソフトウェアコンポーネントは OSS や商用ソフトウェアに関係なく、ソフトウェアが内蔵するすべての部品を指します。SBOM を活用することで、ソフトウェアの透明性が実現でき、内蔵したソフトウェアコンポーネントが脆弱性やライセンスなどのリスクを有していないか判断することができます。

SBOMの例（SPDXフォーマット）

出典：「https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf」を基に大和総研作成

コンポーネントの名称やバージョンなど SBOM で管理すべきと考えられる項目（情報）を定めた規格は複数ありますが、なかでも 2021 年 8 月に ISO/IEC 5962:2021 として公開され国際標準となった「SPDX」が注目を集めています。SPDX はソフトウェアコンポーネントの情報を組織で共有できることを目的にしており、仕様書や SPDX を作成できるツールを提供しています。また人が読みやすいデータ形式（テキストによるタグ形式）にも対応しています。たとえば、YAML や JSON など多くのデータ形式に対応しています。

他にも代表的なフォーマットとして、セキュリティやサプライチェーンを分析するために設計された軽量な仕様の CycloneDX や ISO/IEC 19770-2:2015 で国際標準となっている SWID Tag があります。

規格	SPDX	CycloneDX	SWID
正式名称	Software Package Data Exchange	Cyclone DX	Software Identification Tags
団体	Linux Foundation	OWASP	-
標準化	ISO/IEC 5962:2021	-	ISO/IEC 19770-2:2015
データ形式	RDF/XML、XLSX、tag-value、XML、JSON、YAML	XML、JSOM、Protocol Buffers(protobuf)	XML

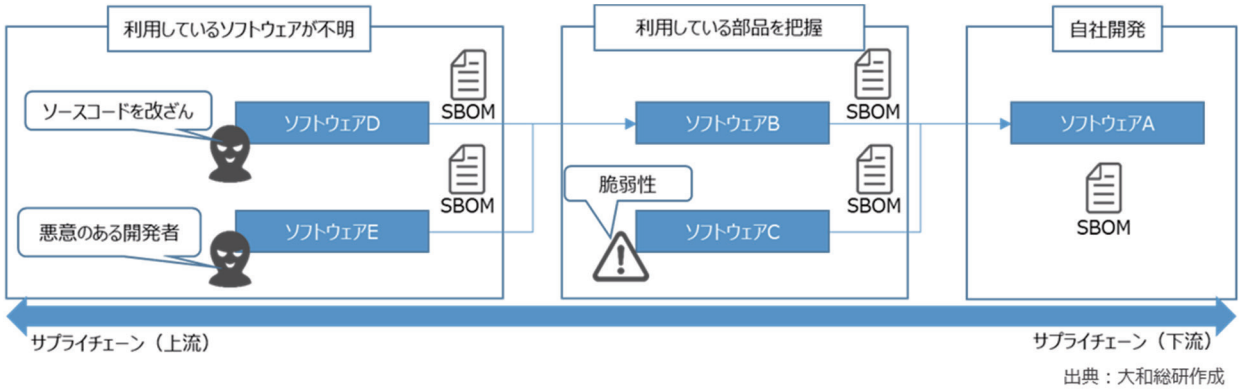
表：代表的な SBOM 規格「https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf」を基に大和総研作成

SBOM の重要性

近年のソフトウェア開発において OSS の利用は当たり前になっています。 Synopsys の調査によると分析した 2,409 のソースコードのうち、OSS が含まれていた割合は 97%と発表されています。今や OSS を利用せずにソフトウェア開発を行うことは困難といえます。しかし、OSS を利用することでコストを削減し開発を効率的に行うことができる一方で、ソフトウェアサプライチェーン（*1）を狙った攻撃も多く、ソフトウェアに組み込まれている OSS の脆弱性がシステム全体に影響を及ぼす可能性があります。

これまで商用ソフトウェアは構成管理されることが多かったですが、OSS について構成管理されないことが大半です。そのため、OSS に新たな脆弱性が公開された場合、自社が利用しているソフトウェアに影響があるか判断できるまでに時間がかかります。また、脆弱性が含まれるコンポーネントを利用していた場合、対処が遅れることで実際に攻撃されてしまう危険性があります。

SBOM を活用することで、ソフトウェアで利用されているコンポーネントや依存関係を正確に把握することができ、新たな脆弱性が公開された場合でも素早く対応することができます。



出典：大和総研作成

（*1）ソフトウェアサプライチェーンとはソフトウェアの開発からエンドユーザに使用されるまでの流通、その後の運用・保守に関与する組織の活動や資源等を指します。

米国の動向（大統領令 14028 について）

2021 年 5 月 12 日にバイデン米大統領が署名した「 Executive Order on Improving the Nation's Cybersecurity （国家のサイバーセキュリティの向上に関する大統領令）」は SBOM が注目を浴びるきっかけとなりました。この大統領令は世界的に深刻な影響を及ぼした SolarWinds 社が受けたサプライチェーン攻撃や Colonial Pipeline 社が受けたランサムウェア攻撃などを背景に発令されました。この大統領令には国家のサイバーセキュリティを強化するために連邦政府および連邦政府と連携する企業が満たすべきセキュリティ要件が示されています。主な要件は次のとおりです。

- 脅威情報を共有するために障壁を取り除く
- 連邦政府のサイバーセキュリティの近代化
- ソフトウェアサプライチェーンのセキュリティ強化
- サイバーセキュリティ安全審査委員会の設置
- サイバーセキュリティの脆弱性やインシデント対応のための標準化
- 連邦政府のネットワークにおける脆弱性とインシデントの検出の向上
- 連邦政府の調査能力および修復機能の向上

「ソフトウェアサプライチェーンのセキュリティ強化」では、政府が調達するソフトウェアに対してセキュリティ基準を作成することを要求しています。そのセキュリティ基準のひとつとして、「SBOM を購入者に提供すること」を要求しています。大統領令の発令以降、NIST や NTIA などから SBOM に関するガイドラインが発行されています。現状では期限の指定はされていませんが、今後大統領令を基に連邦調達規則（FAR）が見直され要件を満たさないソフトウェアは政府調達から削除される予定です。

Section	ソフトウェアサプライチェーンのセキュリティ強化
4.(e)	商務長官は、以下の内容を含めたソフトウェアサプライチェーンのセキュリティを強化するガイドラインを発行する。
(i)	セキュアなソフトウェア開発環境を利用する。・隔離されたビルド環境の使用　・信頼関係の監査　・多要素かつリスクベースの認証および条件付きアクセスの確立　・ソフトウェア開発に使う環境の商用製品への依存関係を文書化し最小化　・データの暗号化の採用　・運用とアラートを監視し、インシデントへ対応
(ii)	購入者から要求された場合、本セクション(e)-(i)に定めるプロセスへ適合していることを示す成果物を提供する。
(iii)	信頼できるコードサプライチェーンを維持するため、自動化ツールまたは同等のプロセスを採用し完全性を確保する。
(iv)	既知および潜在的な脆弱性をチェックし、修正する自動化ツールまたは同等のプロセスを採用すること。これは定期的に少なくとも製品、バージョン、更新プログラムのリリース時に行う。
(v)	購入者から要求された場合、本セッション(e)-(iii)および(iv)に記載されている成果物を提供し、評価および軽減されたリスクの概要を含む、これらのアクションの完了に関する情報を公開すること。
(vi)	正確かつ最新のデータ、コード、コンポーネントの来歴（起源）、内部およびサードパーティのソフトウェアコンポーネント、ツール、サービスの管理と監査を定期的に実施する。
(vii)	SBOM を購入者に直接提供するか、公開 Web サイトに公開することにより提供する。
(viii)	報告および開示プロセスを含む脆弱性対応プログラムに参加する。
(ix)	安全なソフトウェア開発手法に準拠していることを証明する。
(x)	製品の一部で使用されている OSS の完全性と来歴を、実行可能な範囲で保証し、証明する。

表：国家のサイバーセキュリティの向上に関する大統領令　セクション 4.(e) の要求事項

「https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/」を基に大和総研作成

国内の動向

国内においては、「Society5.0」におけるサプライチェーン全体のセキュリティ確保のため、経済産業省が設置する「産業サイバーセキュリティ研究会ワーキンググループ１」内の「ソフトウェアタスクフォース」を中心に SBOM の普及に向けた議論が進められています。「ソフトウェアタスクフォース」はソフトウェアの管理手法に関する課題や脆弱性対応、ライセンスリスクへの対応など OSS の利活用に関する課題について議論するために設置されました。主な取り組みとしては次のとおりです。

- 規制が見込まれる医療機器分野、自動車分野、ソフトウェア分野を対象に SBOM 実証を実施
- 分野ごとに期待される SBOM の活用モデルや取引モデルの検討
- SBOM に関する知見をまとめたガイダンスの作成

まとめ

SBOM はソフトウェアに組み込まれているソフトウェアコンポーネントの情報をリスト化したもので、ソフトウェアの透明性が実現できます。これにより、例えば自社が使用しているソフトウェアに脆弱性を含むソフトウェアコンポーネントが使われていないかを検索することができます。しかし、頻繁に更新される脆弱性情報から、SBOM だけを利用して該当する脆弱性を見つけるのは、多くの作業時間がかかり、また見落としがあるかもしれません。そのため、ソフトウェア開発のライフサイクルにおいて、ソフトウェア構成分析（SCA）ツールなどを利用し SBOM を DevSecOps（*1）に組み込み自動化することが必要です。継続的に SBOM を管理しソフトウェアの脆弱性を自動検知することで、ソフトウェアサプライチェーンのセキュリティをより強化することができます。

国内の動向からも分かるように、国内においても SBOM の普及に向けた検討が進められており、自動車業界や医療業界など生命に関わる業界では先行する可能性が高まっています。業界ごとの取り組みに温度差はありますが、あらゆる業界でソフトウェアサプライチェーンの強化は必要になるため、SBOM は幅広い業界で普及が進むと考えられます。政府が規制やガイドラインとして定めるのを見守るのではなく、今から SBOM の有効性を確認しておくことが重要です。

（*1）DevSecOps とは DevOps にセキュリティを組み込み、リリースサイクルの短縮と高いセキュリティレベルの実現を両立する開発手法です。DevOps とは開発チームと運用チームのプロセスを統合・自動化することで開発スピードと品質の向上を狙う手法のことです。

バックナンバーはこちら

DIR SOC Quarterly 2022 the first issue （2022 年 9 月 29 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2210.html

DIR SOC Quarterly 2022 Vol.2
2022 年 11 月 21 日発行

著者　大和総研
発行所　株式会社大和総研　フロンティア研究開発センター
印刷・製本　セキ株式会社

お問い合わせ先　https://www.dir.co.jp/contact/solution/input.php

大和総研
Daiwa Institute of Research