クラウドサービスのサプライチェーン
リスクマネジメント調査

調査報告書

2022年5月発行

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

改版履歴

年月日	版数	内容
2022 年 3 月 30 日	1.0	発行
2022 年 5 月 31 日	1.1	改訂 インシデント及び脆弱性情報の選定基準を見直したことに伴う集計結果および 2.1.2.1.2 収集項目を変更。変更に伴い、3.1、図表 3-1-2 に記載した情報収集件数および分析にかかわる数値を修正。

目次

1. 本調査の背景と目的 5
1.1. IT サプライチェーンリスクマネジメントに関するこれまでの調査 5
1.2. クラウドサービス活用を取り巻く社会情勢 5
1.3. クラウドサービスの拡大に伴うセキュリティの懸念 6
1.4. 本調査の目的 8
1.5. SaaS 事業者が抱える課題の想定 8
1.5.1. 課題の想定 8
1.5.2. 課題の整理 9
2. 調査方法 11
2.1. インシデント及び脆弱性情報の調査 11
2.1.1. 調査対象とするインシデント及び脆弱性情報の条件 11
2.1.2. 調査方法 12
2.2. インタビュー調査 13
2.2.1. 調査対象 13
2.2.2. 調査方法 14
2.2.3. 調査内容 14
3. 調査結果 15
3.1. インシデント及び脆弱性情報調査結果 15
3.1.1. インシデント及び脆弱性情報の整理 15
3.1.2. インシデント概要図 21
3.2. インタビュー調査結果 35
3.2.1. 課題案に関するインタビュー結果 36
3.2.2. 開発工程に係る考慮すべき課題やリスクに関するインタビュー結果 43
3.2.3. 開発工程以外の課題やリスクに関するインタビュー結果 50
3.2.4. その他得られた観点 56
4. 本調査のまとめ 58
4.1. 想定した課題との違い 58
4.2. 新たに指摘された課題 58
4.3. 団体・有識者の課題認識 59
4.4. SaaS が抱える脅威・リスク 60
4.5. 今後深堀すべきポイント 61

付録 インシデント及び脆弱性情報一覧

(空白のページ)

1. 本調査の背景と目的

本章では、クラウドサービスのサプライチェーンリスクマネジメント調査を実施することとした背景として、これまでの調査や 2022 年現在における日本のクラウドサービス活用の状況や、想定されるクラウドサービスにおけるセキュリティの課題について述べ、本調査で明らかにする目的を示す。

1.1. IT サプライチェーンリスクマネジメントに関するこれまでの調査

企業における IT システムの活用は単なる業務の効率化、一部のデジタル化にとどまらず自社の事業戦略に欠かせない存在となっている。日本においては特に基幹系システムをはじめとする、自社のビジネスモデル及び独自のオペレーションと密接に関係するシステムの開発に際して、SIer（System Integrator：システムインテグレーター）等ソフトウェア開発事業者へ個社に合わせたシステムの開発依頼をする形で IT システムの調達が行われてきた。

このような IT システム開発においては、機能・非機能問わず求められる要件が複雑であり、認識の齟齬等によって開発時や運用時にトラブルが発生しやすく、そのため設計・開発・運用等を委託する委託元と受託する委託先との責任範囲の明確化が必要となる。委託先がさらに別の企業へ外部委託するケースも多く、そのような外部委託が連鎖する委託体系（以下、「IT サプライチェーン」とする）において、直接契約を結ぶ委託先の管理をするだけでは情報セキュリティに関するリスク把握が困難となる。

そのような背景から、独立行政法人 情報処理推進機構（以下、「IPA」とする）では IT サプライチェーンにおけるリスクマネジメントに関する調査を行ってきた。開発委託におけるリスクマネジメントの方法としては、成果物や開発作業におけるセキュリティの取り決めを明確化し、契約における遵守事項や責任範囲を明らかにすることで、リスクの低減や対応の迅速化を図ることなどが挙げられる。2017 年に実施した「情報セキュリティに関するサプライチェーンリスクマネジメント調査」[1]では、再委託先以降の企業におけるセキュリティ対策の状況を把握できていない委託元は約半数であることが明らかとなり、「情報セキュリティ管理を定めたルール遵守の徹底の負担を、委託元だけでなく、委託先や再委託先、再々委託先以降も含めたサプライチェーン全体で低減してくことが重要な課題になる」とした。続く調査の結果では、「契約締結時にソフトウェアの詳細な仕様が明確になっていることは少なく」、「契約締結時に責任範囲を明確化する」ことが IT サプライチェーンリスクマネジメントへの取り組みを向上させる一因になり得ることが示唆された[2]。

1.2. クラウドサービス活用を取り巻く社会情勢

IT サプライチェーンは、システムやソフトウェアといったものを開発、購入するだけでなく、サービスを利用

---

[1] 独立行政法人 情報処理推進機構(2017). 情報セキュリティに関するサプライチェーンリスクマネジメント調査, https://www.ipa.go.jp/security/fy28/reports/scrm/index.html, [参照 2022 年 2 月 18 日].

[2] 独立行政法人 情報処理推進機構(2019). IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査, P89-90, https://www.ipa.go.jp/security/fy30/reports/scrm/index.html, [参照 2022 年 2 月 18 日].

するという形態も含まれている。そのサービスの代表的なものがクラウドサービスである。自社の業務に合わせて開発し、運用するという IT システムの利用形態は、サービスを選定し、必要な機能を必要なだけ利用するという形態に変わりつつある。

また、2019 年 12 月を発端として世界中に感染が拡大した新型コロナウイルス感染症（COVID-19）の影響により、2020 年、2021 年にはニューノーマルと呼ばれる新たな働き方や生活様式が求められることとなった。企業におけるニューノーマルでは、特に在宅での勤務やサテライトオフィスを利用したワークスタイルであるテレワークへの急速な移行に伴い、以前より拡大傾向のあったクラウドサービスの活用は、一層の加速という様相を呈している。テレワーク時のコミュニケーション手段としての Web 会議システムや、出社せずとも契約締結や承認作業を可能とする紙・押印といった事務手続きの電子化サービスなどが規模を拡大しており、ニューノーマルでの企業活動にはこれらのクラウドサービスの利用が必須ともいえよう。一般社団法人 日本情報システム・ユーザー協会（JUAS）の 2020 年度調査「企業 IT 動向調査報告書 2021」[3]では、中小企業含めて SaaS 導入済みの企業が 6 割を超えている状況から「多くの企業でクラウドサービスへ移行している傾向が鮮明」であるとしている。

また、2021 年 4 月から 2021 年 9 月にかけては日本で 3 回目となる緊急事態宣言が発令され、2022 年には新たな変異株が世界的に流行し、再び感染者数が増大する状況を迎えている。このような直近の状況を鑑みると、長期にわたってニューノーマルが定着することにより、今後も継続的にクラウドサービスを活用する必要が見込まれ、クラウドサービスの拡大というトレンドはさらに加速していくものであると考えられる。

1.3. クラウドサービスの拡大に伴うセキュリティの懸念

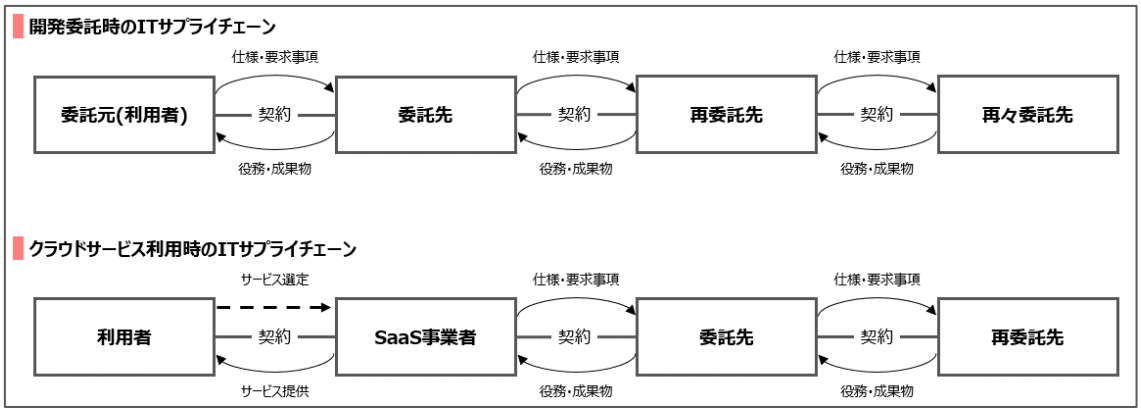
クラウドサービスは利便性が高い反面、利用する際の課題も存在する。例えば、クラウドサービスの利用拡大によって、利用者が直接マネジメントできない IT サプライチェーンのリスクや、IT やセキュリティに明るくない利用者による調達・管理のリスク等セキュリティ上の懸念が生じるといったことが挙げられる。

自社業務に応じたソフトウェアの開発を SIer 等に委託する場合は、委託先との個別契約があるため、ソフトウェア納品後の運用段階であっても仕様に見合った責任範囲を取り決めることも一定程度可能である。また、委託先との個別契約の中で、IT システムを開発する上でのセキュリティ対策や委託先社内でのセキュリティガバナンス、OSS 等ソフトウェアの利用を含める再委託先の管理方針に関する確認及び要求を行うことも難しくはなく、自社のセキュリティガバナンスが行き届く契約形態であったと言える。一方、SaaS のようなクラウドサービスの場合は、基本的にクラウドサービス事業者（委託先）があらかじめ用意した利用規約に明記された責任範囲で契約をするケースが多く、利用者側が望むセキュリティ対策等の履行・責任範囲の変更をするような契約は少ないことが想定される。このような背景から、クラウドサービス利用時のセキュリティ対策は約款に定められた責任範囲で実施されており、利用者のセキュリティガバナン

[3] 一般社団法人 日本情報システム・ユーザー協会(JUAS) (2021). 企業 IT 動向調査報告書 2021-ユーザー企業の IT 投資・活用の最新動向-(2020 年度調査), P4, https://juas.or.jp/library/research_rpt/it_trend/, [参照 2022 年 2 月 18 日].

スが行き届きにくい状況であることが考えられる。下記にソフトウェア開発委託時の IT サプライチェーンとクラウドサービス利用時の IT サプライチェーンを図示した（図表 1-3-1）。開発委託時の委託元は、委託先に対して仕様や要求事項を伝え、委託先は役務や成果物を提供するが、クラウドサービス利用時では利用者は SaaS 事業者へ仕様を伝えるのではなく、機能や仕様・サービス約款に基づいて選定を行い、SaaS 事業者からサービス提供を受けることになる。

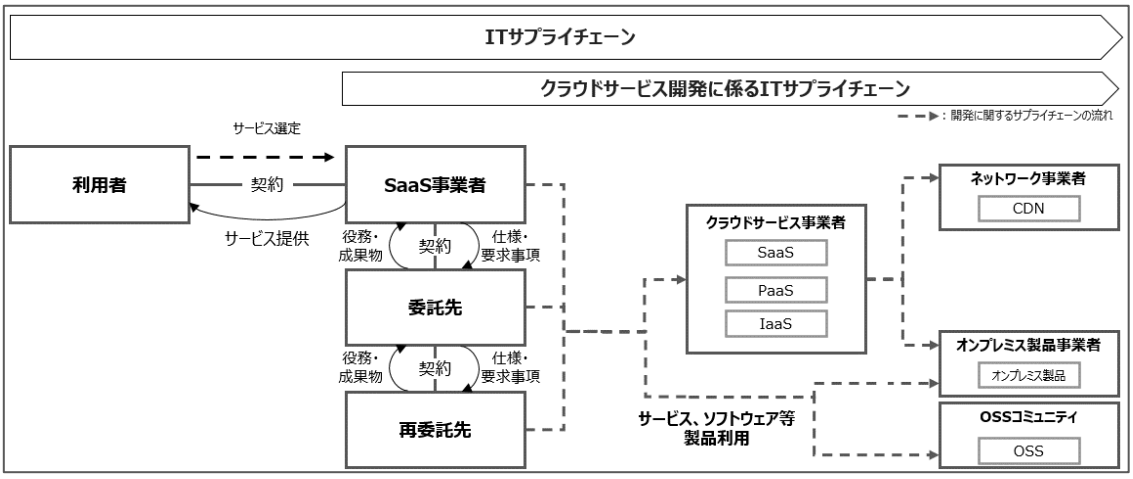
図表 1-3-1 開発委託時及びクラウドサービス利用時の IT サプライチェーンのイメージ



利用者の視点からは、利用を検討しているクラウドサービスが事業者側で開発される際のセキュリティ対策や委託先内のセキュリティガバナンス等についても、事前に詳細の確認及びセキュリティに関する要求は難しく、クラウドサービス事業者が用意した利用規約に合意せざるを得ない場面がある。したがって、委託元がクラウドサービス利用におけるサプライチェーン上のリスクマネジメントを推進するためには、クラウドサービス事業者が用意する利用規約だけでなく、クラウドサービスそのものがセキュアに開発されているか、クラウドサービス事業者内でセキュリティ対策としてどのようなことが行われているか等具体的な施策まで把握し、リスクを十分確認したうえで利用を検討することが望ましい。

下記にクラウドサービス開発に係る IT サプライチェーンを図示した（図表 1-3-2）。図のように、SaaS 事業者が自社のサービスとして開発するにあたり、SaaS やオンプレミスの製品、OSS 等を利用、すなわち委託先を抱えており、また、SaaS 事業者が自社のサービス開発のために外部へ開発業務の委託を行うこともある。このような場合クラウドサービス開発に関わるサプライチェーンは長大で複雑な構造になり得るとともに、サプライチェーン上で潜在的なリスクが存在すると考えられる。

図表 1-3-2 クラウドサービス開発に係る IT サプライチェーンのイメージ



また、クラウドサービスの中でも SaaS は、IT に関する知識・経験が少ない利用者にも手軽に導入できる反面、SaaS を安全に利用するための知識・経験を獲得することは容易ではないため、選定時のリスク検討が不十分なまま導入するケースもあり、機密情報が漏洩する等のインシデントへ発展する可能性がある。近年では委託先がクラウドストレージ上にデータを暗号化せず保存していたことで、多くの個人情報が流出したインシデントも報告されている。

1.4. 本調査の目的

このような背景から、本調査ではクラウドサービスの中でも特に利用されている SaaS に焦点を当て、日本での SaaS をはじめとしたクラウドサービスおける IT サプライチェーンのリスクマネジメントに資することを目的に、SaaS およびそのサプライチェーンが抱えるセキュリティ上の脅威やリスク等について調査を行うこととした。

特に本取り組みは、SaaS を選定し利用する際に考慮すべき事項や、SaaS そのものが抱える脅威・リスク等について、今後継続的に解明すべきポイントや解決するべき課題等を明らかにするための取り組みとして位置づけ、調査を行った。

1.5. SaaS 事業者が抱える課題の想定

本節では、調査を実施するにあたってクラウドサービスや SaaS を開発する事業者が、セキュリティリスクマネジメントに関してどのような課題をもっているかについて、調査開始前の想定を述べる。

1.5.1. 課題の想定

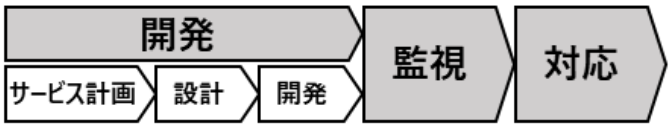
調査を実施するにあたり、SaaS に係るサプライチェーンや、SaaS 事業者が抱えるセキュリティ上の課題について、「1.3. クラウドサービスの拡大に伴うセキュリティの懸念」で述べたような懸念を念頭に、想定される課題案を作成した。今回の調査における範囲が SaaS の開発工程や運用におけるセキュリティ取り組み状況に踏み込むことから、ソフトウェア開発ライフサイクルの考え方を参考に、課題案として考えられ

るものを列挙した。

1.5.2. 課題の整理

本調査で対象とする工程を大まかに「開発」・「監視」・「対応」の 3 つに分け、それぞれどのような課題を抱えていると考えられるかを検討し、整理を行った（図表 1-5-1、図表 1-5-2）。本調査では SaaS を対象としている点を鑑み、開発の工程には自社の SaaS 製品にどのような機能を持たせ、どのような情報を取り扱うか企画する「サービス計画」の工程、外部サービスの調達や OSS の利用検討といった具体的なソフトウェアの「設計」工程、実装とテスト・リリースといった「開発」の工程をまとめている。また、セキュリティ課題について着眼していることから、監視の工程には運用時の脆弱性や攻撃の監視といった工程、対応工程では脆弱性対応アップデートや発生したインシデント・被害への対応といった工程を想定して整理した。

図表 1-5-1 本調査で対象とした工程



図表 1-5-2 SaaS 事業者が抱える課題案

工程	No.	課題案
開発工程	1	開発時に機能開発が優先され、セキュリティ対策が十分でないのではないか
	1-1	非機能要件定義時に、セキュリティに関する項目が十分に含まれていないのではないか
	1-2	インシデントを考慮したアーキテクチャ（冗長構成等）を検討、採用できていないのではないか
	1-3	セキュリティ要件を確認するテスト項目が作成されていないのではないか
監視工程	2	セキュアな監視ナレッジが十分でないのではないか
	2-1	脆弱性や機能（設定値）のアップデートに関する情報を収集できていないのではないか
	2-2	境界・エンドポイント型の検知システムを活用できていないのではないか
対応工程	3	インシデント対応・準備が十分でないのではないか
	3-1	発生時の責任者や確認箇所・項目に関して策定できていないのではないか
	3-2	インシデント対応完了の基準を作成していないのではないか

1.5.2.1. 開発工程

開発の工程にはサービスの計画や設計・開発の工程を含めた。ここでは、SaaS 開発に当たって、サービスや機能の拡充のための開発が事業上優先され、セキュリティについての考慮や対策の実施が十分ではないのではないかという課題案（図表 1-5-2 の課題案 1）を作成した。また、計画や設計・開発ではそれぞれ下記の課題案を考えた。

(ア) サービス計画

セキュリティに関する非機能要件が検討されていないのではないか（図表 1-5-2 の課題案 1-1）

(イ) 設計

冗長構成といった、インシデント対応のためのアーキテクチャを採用出来ていないのではないか（図表 1-5-2 の課題案 1-2）

(ウ) 開発

リリースに向けてセキュリティ要件をチェックするテスト項目の作成がなされていないのではないか（図表 1-5-2 の課題案 1-3）

1.5.2.2. 監視工程

監視の工程では、クラウドサービスが拡大するに伴いセキュアな運用についてのナレッジを持つ組織や人材が足りなくなっているのではないかという課題案（図表 1-5-2 の課題案 2）に立ち、利用する OSS やクラウドサービスといったサプライチェーン由来のリスク監視や、インターネットに公開されているエンドポイントの監視といった監視対象毎の課題案を立案した（図表 1-5-2 の課題案 2-1、2-2）。

1.5.2.3. 対応工程

対応については、迅速な対応の成否は事前の準備に依るところが大きい（図表 1-5-2 の課題案 3）として、体制や手順の整備状況に着目して課題案を立案した（図表 1-5-2 の課題案 3-1、3-2）。

2. 調査方法

本調査では、近年 IT サプライチェーンにおいて SaaS が活用される状況を背景とし、SaaS 利用時に考慮すべき点や SaaS 自体が抱える脅威、リスク等を明らかにするため「インシデント及び脆弱性情報の調査」、「インタビュー調査」の 2 工程に分けて調査を実施した。

2.1. インシデント及び脆弱性情報の調査

IT サプライチェーンにおける SaaS 利用時のリスクや SaaS 自体が抱える脅威・リスク等を明らかにするため、SaaS 事業者及び SaaS 利用者に影響を与えた、IT サプライチェーン上のインシデント及び脆弱性の情報を収集、整理した。また、収集したインシデントのうち 3 つについてはインシデントの概要図を作成し、本調査において深堀が必要と考えられるポイントを取り上げた。さらに、インシデント及び脆弱性の発生箇所や影響範囲、対策等を整理することで、SaaS のサプライチェーンに関して今後深堀する必要がある脅威、リスク、課題等に関する示唆が得られないか検討を行った。

2.1.1. 調査対象とするインシデント及び脆弱性情報の条件

下記条件に該当するインシデント及び脆弱性情報を調査対象として収集した。

(ア) SaaS の開発・運用に関連し、SaaS 事業者または SaaS 利用者に影響があると考えられるもの
- SaaS の開発・運用に関して業務委託を行っている場合は、SaaS 事業者に影響を及ぼす「委託先で発生したインシデント」や「委託先で利用するソフトウェア等に関する脆弱性」についても調査対象とした

(イ) SaaS 利用時の設定ミス等、SaaS 利用者に起因するインシデント

(ウ) 日本国内に限らず海外のインシデントも対象とした

なお、本調査における「インシデント」と「脆弱性」の定義は下記のとおり。

- インシデント

  組織、個人等が利用するコンピュータやネットワーク、アプリケーション等 IT システムにおける、通常利用として想定されない挙動またはそれを引き起こす攻撃と、想定されない挙動が及ぼす情報漏洩等の被害発生までの一連の事象。

- 脆弱性

  悪意のある行為（攻撃）によって悪影響を及ぼす可能性のある、ソフトウェア、ハードウェア上の欠陥またはその欠陥に対してどのような攻撃をされ得るかを表す性質。なお、本調査において「脆弱性」と表現するものは、それを原因とするインシデントの有無に関わらず、脅威の所在の一つとして取り扱う。

2.1.2. 調査方法

インシデント及び脆弱性情報の調査に関連して「2.1.1. 調査対象とするインシデント及び脆弱性情報の条件」の条件を満たす情報の収集方法や収集項目等を示す。またこれらの情報を整理・考察し、いくつかのインシデントについては概要図を作成した。

2.1.2.1. インシデント及び脆弱性情報の収集

インシデント及び脆弱性情報の収集方法、収集項目、収集対象期間を示す。

2.1.2.1.1. 収集方法

書籍、ニュース等公開情報を基に、「2.1.1. 調査対象とするインシデント及び脆弱性情報の条件」で記した対象範囲に該当するインシデント及び脆弱性情報の収集を行った。同一のインシデントまたは脆弱性によって複数企業が影響を受けた場合、当該インシデントまたは脆弱性を 1 件としている。

2.1.2.1.2. 収集項目

インシデントおよび脆弱性情報の収集に当たっては、下記項目を充足するよう調査を行なった。ただし、広く公開されている媒体から情報収集を行っているため、一部項目に関する情報の収集が困難であったインシデント及び脆弱性も存在する。

- 分類（インシデント or 脆弱性）
- 発生箇所
- 概要
- 公表年
- 発覚の経緯
- 原因
- 被害内容
- 対応内容
- 再発防止策

2.1.2.1.3. 収集対象期間

本調査で調査対象とするインシデント及び脆弱性情報は、2020 年 4 月から 2021 年 9 月末に公表されたものとする。

2.1.2.2. インシデント及び脆弱性情報のリスクや課題の整理

(ア) リスクや課題の示唆

インシデント及び脆弱性情報の収集結果を整理することによって、SaaS 自体が抱える脅威やリスク、利用者が安全に利用するための課題について、示唆される事柄がないか検討を行った。

(イ) リスクの所在よる整理

SaaS のソフトウェア開発におけるサプライチェーンの中に、収集対象期間中のインシデントおよび脆弱性といったリスク情報を配置することによって、リスクのパターンや頻度といった傾向をつかめないか検討行った。

2.1.2.3. インシデント概要図の作成

いくつかのインシデントに関しては、インシデントがどのように発生するのか、どのように影響が広がるのか、どんな組織・システムがどう関連したのか、責任範囲はどこまでだったのかを明らかにした概要図を 3 件分作成した。概要図に取り上げるインシデントの選定基準は「3.1.2. インシデント概要図」に示した。

2.2. インタビュー調査

SaaS 利用時に考慮すべき点や SaaS 自体が抱える脅威、リスク等実態を把握し、クラウドサービスのサプライチェーンリスクマネジメントに関する今後深堀すべきポイントを明らかにするため、IT サプライチェーンにおける SaaS 利用時のリスクマネジメント及び SaaS 開発時の脅威やリスクに関して 5 つの組織（計 13 名）にインタビュー調査を実施した。

2.2.1. 調査対象

下記いずれかに該当する 5 組織をインタビュー調査対象とした。

- SaaS 事業者が加盟している組織
- SaaS の研究や普及啓発活動を行っている組織
- 上記組織に属する SaaS 事業者

また、インタビュー調査対象の選定時には下記等基準を設け、全てまたは一部を満たす組織をインタビュー調査対象とした。

- 2019 年 10 月から 2021 年 9 月末の期間に、クラウドサービスのセキュリティ対策に関する刊行物を発行している。
- 2019 年 10 月から 2021 年 9 月末の期間にクラウドサービスのセキュリティ対策に関するイベントを実施している。
- SaaS 開発時のセキュリティ対策に関する専門性を持つ人物が所属している。

2.2.2. 調査方法

- 実施時期　：2022 年 1 月
- 時間　：各組織につき約 1 時間
- 実施形式　：Web 会議ツールを利用し、オンラインでのインタビュー実施
- 総対象者数　：13 名
- 補足
  - インタビュー対象へは、事前に「インタビュー内容は本調査報告書に組織の見解として記載し、組織名及び個人名は記載されない」旨伝え、了承を得ている。
  - また、インタビュー内容に対する認識齟齬を防ぐため、インタビュー実施後にインタビュー内容に関する議事を対象者へ共有し確認を取った。

2.2.3. 調査内容

「2.1. インシデント及び脆弱性情報の調査」にて得られた分析結果や「1.5. SaaS 事業者が抱える課題の想定」にて作成した課題案に関して組織から見解を得る形でインタビュー調査を行った。

- インシデント及び脆弱性情報の調査結果に対する見解
  考慮すべき SaaS の脅威、リスクまたは重要と思われるインシデント及び脆弱性等について聞き取りを行った。

- SaaS 自体が抱える脅威やリスク、SaaS 開発時のセキュリティ対策に関する課題案に対する見解
  課題案の整理において不足する観点や、作成した課題案と SaaS 利用者、事業者から見た実態との相違について聞き取りを行った。

3. 調査結果

本章では、IT サプライチェーンに関連するインシデント及び脆弱性情報調査、並びに、インタビュー調査を実施して得られた情報や示唆を含む調査結果について記載する。

3.1. インシデント及び脆弱性情報調査結果

本節では、収集したインシデント及び脆弱性情報の発生箇所に着目し、SaaS 事業者や委託先等 IT サプライチェーン上の関係者ごとに整理し、IT サプライチェーンにおける SaaS 利用時のリスクや SaaS 自体が抱える脅威・リスク等について検討した。

2020 年 4 月 1 日から 2021 年 9 月 30 日までに公表されたクラウドサービスの開発、利用、提供に関連するインシデント及び脆弱性情報を 57 件分収集し、そのうちインシデント情報は 37 件、脆弱性情報は 20 件であった。インシデントおよび脆弱性情報は、網羅的に収集したものではなく、典型的でかつ 2022 年 5 月 20 日時点で書籍、ニュース、企業の公開情報から内容が確認できたもののみとした。インシデントでは設定ミスによる人為的な原因や、ランサムウェアを用いた攻撃によって発生するものが見られ、脆弱性ではソフトウェアコンポーネントや開発工程に関連するコード管理等のサービス上で報告されたものが見られた。

また、以下にインシデント及び脆弱性情報の調査結果の全体像を示した。

図表 3-1-1：インシデント及び脆弱性情報の調査結果目次

章番号	内容
3.1.1.	インシデント及び脆弱性情報の整理
3.1.2.	インシデント概要図
3.1.2.1.	SolarWinds 社に係るインシデントの概要図
3.1.2.1.1.	インシデントの概要
3.1.2.1.2.	考察
3.1.2.2.	Codecov 社に係るインシデントの概要図
3.1.2.2.1.	インシデントの概要
3.1.2.2.2.	考察
3.1.2.3.	ネットマーケティング社に係るインシデントの概要図
3.1.2.3.1.	インシデントの概要
3.1.2.3.2.	考察

3.1.1. インシデント及び脆弱性情報の整理

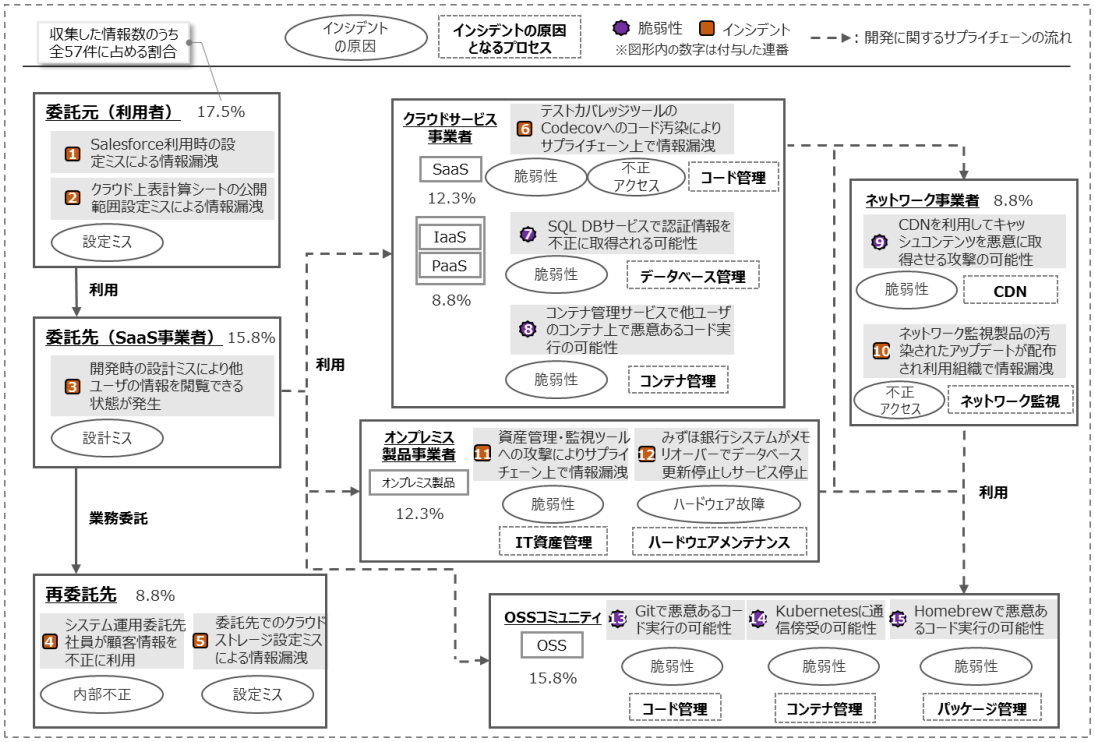
本項では、SaaS に係る IT サプライチェーン上でどのような箇所がリスクとなりやすいかを明らかにするためにインシデント及び脆弱性情報を整理した結果を示す。

整理の方法としては、収集したインシデント及び脆弱性がどのようにして発生するか、どのような箇所で

発生するかに着目して、インシデント及び脆弱性の原因や発生箇所において共通する点を抽出した。また、図表 1-3-2 中の IT サプライチェーン上の関係者ごとに考慮すべきと考えられるインシデントの原因やインシデントの原因となるプロセス及び関連するインシデントまたは脆弱性情報を、図表 1-3-2 を基にして作成した SaaS に係る IT サプライチェーンの図に掲載した（図表 3-1-2）。なお、図表 3-1-2 に示した「インシデントの原因となるプロセス」は、同図に示した脆弱性（7,8,9,13,14,15)の場合、脆弱性の原因となったプロセスを示すものではなく、同図に示した脆弱性によって攻撃された場合に「インシデントの原因なることが考えられるプロセス」であることを意味している。

インシデントの原因やインシデントの原因となるプロセスを IT サプライチェーン上の関係者ごとに整理した、SaaS に係る IT サプライチェーン上のリスクのイメージは以下の通り。図 3-1-2 に示したインシデントおよび脆弱性は、本調査で収集した 57 件のうちの代表的なものである。収集した個々のインシデント及び脆弱性情報は付録の「インシデント及び脆弱性情報一覧」を参照のこと。

図表 3-1-2：SaaS に係る IT サプライチェーン上のリスク所在のイメージ



図表 3-1-2 中の用語に関する説明を図表 3-1-3、図表 3-1-4 に記した。

図表 3-1-3：IT サプライチェーン上で考慮すべきインシデントの原因に関する説明

用語	説明
設定ミス	適切でない値を設定すること。想定していた設定値が実際に設定されていない場合を含む。
設計ミス	IT システムの開発時に、セキュリティ対策として考慮されるべき項目の実現が確認されていないままリリースされることで予期せぬ動作を引き起こすこと。
内部不正	事業者の社員が顧客の情報を盗み悪用または情報流出させる等、インシデントの原因を引き起こした人物が所属する組織と被害を受ける組織が同一のケースを指す。
不正アクセス	利用する権限を与えられていない IT システムに対して、不正に接続しようとすること。
脆弱性	コンピュータの OS やソフトウェアにおける、プログラム上の不具合や設計ミスによって生じる情報セキュリティ上の欠陥のこと。
ハードウェア故障	IT システムにおける機械（サーバを含む）、装置、設備、部品といった物理的な構成要素であるハードウェアが、正常な働きを損なうこと。

図表 3-1-4：IT サプライチェーン上で考慮すべきインシデントの原因となるプロセスに関する説明

用語	説明
コード管理	IT システムを構成するコードを円滑に利用や保管、バージョンの管理、更新を行うためのサービスまたは開発における 1 つのプロセスを指す。
データベース管理	データベースのバージョン変更や修正プログラムの適用、バックアップ等の設定値や利用状況を統合的に確認、操作することが可能なサービスまたは開発における 1 つのプロセスを指す。
コンテナ管理	コンテナ技術を利用して作成したサーバやアプリケーション等の設定値や利用状況を統合的に確認、操作することが可能なサービスまたは開発における 1 つのプロセスを指す。
CDN	Contents Delivery Networking の略称。様々なロケーションに設置されたサーバが Web ページのキャッシュを保持する等により、ソフトウェアの利用者に対して高速な Web ページの読み込みを実現するためのサービスあるいは IT システムの構成を指す。
ネットワーク監視	ネットワークに対して性能の低下や障害発生状況等を定期的に確認することを指す。
IT 資産管理	PC やスマートフォン、ディスプレイ等 IT システムに関連する機器を管理することを指す。
ハードウェアメンテナンス	仮想的に作られたものではなく、物理的に存在するサーバやサーバを構成する製品等、IT システムに関連する物理的な機器の不具合の修正や新たな部品を付け替える等機能を維持するための管理を指す。
パッケージ管理	ソフトウェアのインストールを記録し、新しいソフトウェアのインストールや削除、バージョンの更新を行うことを指す。パッケージとは、実行プログラム・設定ファイル・ドキュメント等のファイル群をひとまとめにしたもの。

収集したインシデント及び脆弱性情報を、IT サプライチェーン上の関係者、インシデント及び脆弱性の原因や発生箇所に着目して整理した結果、SaaS に係る IT サプライチェーン上のリスクに関して以下 3 点の示唆が得られた。

(ア) IaaS や PaaS、ネットワーク関連よりも SaaS やオンプレミス製品、OSS に関連したインシデントが発生する頻度、脆弱性が発覚する数が多い可能性が考えられる。

(イ) IaaS や PaaS に比べて脆弱性情報の報告数が多い SaaS や OSS、オンプレミス製品においてインシデントに発展するリスクが考えられる。

(ウ) SaaS 事業者や OSS コミュニティ等から利用者に対して利用時の設定に関する留意すべき箇所や設定値等ソフトウェアの変更に関する案内を行うことで、利用者側の設定ミスが低減する可能性が考えられる。

以下に示唆に関する詳細を記す。

第一に、図表 3-1-2 の IT サプライチェーン上の関係者「ネットワーク事業者」、「OSS コミュニティ」、「オンプレミス製品事業者」、」「クラウドサービス事業者」に含まれる「SaaS」、「IaaS」及び「PaaS」の、収集したインシデント及び脆弱性の情報数のうち全 57 件に占める割合をみると、「クラウドサービス事業者」に含まれる「IaaS」と「PaaS」は 8.8%、「ネットワーク事業者」は 8.8%であるのに対して、「クラウドサービス事業者」に含まれる「SaaS」は 12.3%、「オンプレミス製品事業者」は 12.3%、「OSS コミュニティ」は 15.8%であることから、IaaS や PaaS、ネットワーク関連よりも、オンプレミス製品や OSS に関連してインシデントが発生したり、脆弱性が発見されたりする数が多いことが読み取れる。IaaS や PaaS 事業者はグローバルにサービスを展開している場合が多く[4,5]、セキュリティに対して投じられるリソースが十分に存在していること[6]、IaaS や PaaS 自体が SaaS と比較してソフトウェアコンポーネントが少ないこと、また、様々な利用者から要求される高レベルのセキュリティ要件を満たしていると考えられるため[7,8,9]、IaaS や PaaS 自体が原因で発生するインシデントが少ないことは実態と大きく乖離している訳ではないと思われる。IaaS や PaaS、ネットワーク関連も OSS 等外部のソフトウェアを利用した IT サプライチェーンが存在しているが、IaaS や PaaS、ネットワーク関連と OSS 等が関連するインシデントや脆弱性情報は本調査ではあまり収集されなかった。一方、SaaS 事業者が利用する SaaS や OSS に関連するインシデントや脆弱性は比較的多く収集されており、攻撃対象となる頻度や脆弱性自体が発見される数が多いと考えられる。

第二に、図表 3-1-2 の IT サプライチェーン上の関係者「ネットワーク事業者」、「OSS コミュニティ」、「オンプレミス製品事業者」、」「クラウドサービス事業者」に含まれる「SaaS」、「IaaS」及び「PaaS」の、収集したインシデント及び脆弱性の情報数のうち全 57 件に占める割合と、図表 3-1-2 に基づいて得られた示唆（ア）を加味すると、SaaS や OSS、オンプレミス製品に関するサービスでの脆弱性自体の報告数が多いと考えられるため、脆弱性起因でインシデントに発展する頻度が高いことが読み取れる。OSS であるロギングライブラリ Apache Log4j（以下、「Log4j」）は、プログラミング言語の一つである Java をベースとしており、アクセスログやエラーログ等のログ出力という基本的な機能を提供していることもあり世

---

[4] 株式会社富士通キメラ総研(2021). マーケット情報-パブリッククラウドの国内市場を調査, https://www.fuji-keizai.co.jp/press/detail.html?cid=21065, [参照 2022 年 2 月 23 日].

[5] Synergy Research Group. “Amazon, Microsoft & Google Grab the Big Numbers – But Rest of Cloud Market Still Grows by 27%”, https://www.srgresearch.com/articles/amazon-microsoft-google-grab-the-big-numbers-but-rest-of-cloud-market-still-grows-by-27, [参照 2022 年 2 月 23 日].

[6] 一般社団法人 日本情報システム・ユーザー協会(JUAS) (2021). 企業 IT 動向調査 2021, P265,268, https://juas.or.jp/cms/media/2021/04/JUAS_IT2021.pdf, [参照 2022 年 2 月 23 日].

[7] Amazon Web Services, Inc., AWS コンプライアンスプログラム, https://aws.amazon.com/jp/compliance/programs/, [参照 2022 年 2 月 23 日].

[8] Microsoft. Azure コンプライアンス ドキュメント, https://docs.microsoft.com/ja-jp/azure/compliance/, [参照 2022 年 2 月 23 日].

[9] Google LLC, Compliance resource center, https://cloud.google.com/security/compliance, [参照 2022 年 2 月 23 日].

界中で利用されていた[10]。2021 年 12 月に確認された Log4j の脆弱性は、脆弱性発覚後公開された「攻撃を実証するコード」が悪用されることもあり、世界中の IT システムに大きな影響を及ぼした[11,12]。Log4j は大規模な非営利団体である The Apache Software Foundation[13]がプロジェクトを管理し、メンテナンスを行っていることから安定した OSS であると考えられていたが、そのような OSS であっても大規模なインシデントに発展することが示唆されたと言える。また、広範囲に甚大な被害を及ぼすような広く世間に知られたインシデントでは原因が明らかにされていないものもあるが、コード管理や資産管理に特化して利用者数が多い SaaS や OSS 等に関する脆弱性を利用した可能性もある。報告される脆弱性の数が多いソフトウェアやサービスに対して攻撃が画策されることも考えられるため、脆弱性情報の報告数が少ない IaaS や PaaS に比べて SaaS や OSS、オンプレミス製品の方で大規模なインシデントに発展するリスクがうかがえた。

第三に、図表 3-1-2 の IT サプライチェーン上の関係者「委託元（利用者）」の、収集したインシデント及び脆弱性の情報数のうち全 57 件に占める割合が 17.5%であることから、SaaS に関する情報流出インシデントの中では SaaS 事業者や SaaS 開発に係るサプライチェーン起因のものだけでなく、SaaS 利用者による設定ミスが原因とされるインシデントも存在し、SaaS の使い方を考慮した設計や、SaaS 利用者に対する安全な利用方法に関する案内も SaaS 事業者には求められることが読み取れる。近年話題となった Salesforce の設定によって外部から機密情報へのアクセスが可能であったインシデント[14]も SaaS 利用者の設定ミスが原因と考えられている。設定ミスに関しては、SaaS 利用者側の設定値それ自体や設定の変更が及ぼす影響に対する理解が不足していた可能性もあるが、昨今組織で利用される SaaS の数や種類は増加しており、利用者側が継続的に SaaS の設定に対する理解に努めることは容易ではない。また、SaaS の設定値や設定の影響の変更は SaaS 事業者が利用する SaaS や OSS の更新によって生じる可能性もあると思われる。その場合は SaaS 事業者側でも認識しない間に SaaS 利用者へ影響が及ぶことになるが、IT サプライチェーン上の SaaS 事業者や OSS を開発するコミュニティが、開発するソフトウェアの変更に関する案内を利用者に対して行うことで、最終的に SaaS 利用者の設定ミスによるインシデント発生リスクを低減することにもつながる可能性が考えられる。

SaaS に係る IT サプライチェーン上のリスクについては、SaaS 利用時及び SaaS 開発時にも存在し、特に脆弱性が多く報告される SaaS や OSS 等が考慮されるべき箇所に挙げられると言える。オンプレミス

---

[10] JetBrains s.r.o., Java プログラミング - インフォグラフィック：2021 年開発者エコシステムの現状, https://www.jetbrains.com/ja-jp/lp/devecosystem-2021/java/, [参照 2022 年 2 月 23 日].

[11] 一般社団法人 JPCERT コーディネーションセンター. Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起, https://www.jpcert.or.jp/at/2021/at210050.html, [参照 2022 年 2 月 18 日].

[12] 一般社団法人 JPCERT コーディネーションセンター. 2021 年 12 月に公表された Log4j の脆弱性について, https://www.jpcert.or.jp/newsflash/2021122401.html, [参照 2022 年 2 月 18 日].

[13] The Apache Software Foundation. “Apache Log4j 2”, https://logging.apache.org/log4j/2.x/, [参照 2022 年 2 月 24 日].

[14] Salesforce サイトおよびコミュニティにおけるゲストユーザのアクセス制御の権限設定について https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/

製品の脆弱性も確認されているため引き続き注意を払う必要があるが、SaaS の開発工程で利用する IaaS に関する脆弱性やインシデント情報は比較的少数であった。今回のインシデント及び脆弱性情報調査では、IaaS を利用することが SaaS 事業者にとってリスクヘッジとなるかについて明らかにならなかったが、今後、OSS 等を活用する際のリスクだけでなく IaaS 利用時の課題や安全性に関する調査の必要性も示唆された。

3.1.2. インシデント概要図

本項では、収集したインシデント情報のうち、整理した結果 SaaS に係る IT サプライチェーン上のリスク低減のために特に有用と判断したインシデントについて、インシデントがどのように発生するのか、どのように影響が広がるのか、どんな組織・システムがどう関連したのか、責任範囲はどこまでだったのかを含める概要を図に示した。なお、インシデント概要図に選定する基準は以下の通り。

図表 3-1-5：インシデント概要図に選定する基準

No.	概要図に取り上げるインシデント選定基準
1	SaaS 利用者、SaaS 事業者に対して広く被害が発生したインシデント
2	クラウドサービスや OSS 等、SaaS 開発における利用（委託）先に起因するインシデント
3	SaaS 事業者に起因する、クラウドサービスや OSS の設定を誤る等 SaaS 開発における利用（委託）の管理不備に関するインシデント

以下に、図表 3-1-5 の選定基準を作成した理由を記す。

選定基準 No.1 の作成理由は次の通り。IPA が 2006 年から開始した「前年に発生した情報セキュリティ事故や攻撃の状況等から脅威を選出し、上位 10 位を公表」する「情報セキュリティ 10 大脅威」では、2019 年に「サプライチェーンの弱点を悪用した攻撃の高まり」が 4 位にランクイン[15]してから 2020 年、2021 年も 4 位[16][17]と継続的に考慮すべき脅威として考えられており、2022 年には 3 位と順位を上げている[18]。今回収集したインシデント及び脆弱性情報には、IT サプライチェーン攻撃と呼ばれる、IT サプライチェーン上で広く被害が発生し、世界中に影響が及ぶほどの大規模なインシデントが存在した。攻撃手法が類似しているインシデントであっても大規模なインシデントに発展するインシデントと局所的な影響にとどまるインシデントが収集されたが、収集した情報の限りでは、インシデント被害や影響が大きかった事

[15] 独立行政法人 情報処理推進機構（2019）. 情報セキュリティ 10 大脅威 2019, https://www.ipa.go.jp/security/vuln/10threats2019.html, [参照 2022 年 2 月 18 日].
[16] 独立行政法人 情報処理推進機構（2020）. 情報セキュリティ 10 大脅威 2020, https://www.ipa.go.jp/security/vuln/10threats2020.html, [参照 2022 年 2 月 18 日].
[17] 独立行政法人 情報処理推進機構（2021）. 情報セキュリティ 10 大脅威 2021, https://www.ipa.go.jp/security/vuln/10threats2021.html, [参照 2022 年 2 月 18 日].
[18] 独立行政法人 情報処理推進機構（2022）. 情報セキュリティ 10 大脅威 2022, https://www.ipa.go.jp/security/vuln/10threats2022.html, [参照 2022 年 2 月 18 日].

業者と小さかった事業者で実施していたセキュリティ対策に決定的な差があるとは断定し難かった。大規模なインシデントを図示することは、IT サプライチェーン上のどのような要素によって被害が広まったのかを理解する際に有効であると考えられる。そこで本項では SaaS 事業者や SaaS 利用者にも広く被害が発生した IT サプライチェーン攻撃の大規模なインシデントがどのように発生するのか、どのように影響が広がるのか等を図示することで、SaaS を含む IT サプライチェーン抱えるリスクを明らかにする際の一助になると考え、No.1 をインシデント概要図に選定する基準の 1 つとした。

選定基準 No.2 の作成理由は次の通り。図表 3-1-2 に示したように、SaaS 事業者は IT サプライチェーンのうち、開発工程で様々なソフトウェアやサービスを利用、すなわち委託しており、さらに委託先が別のサービスを利用している等、多くの関係者が連鎖的に関与している。インシデント及び脆弱性情報を収集し、各関係者におけるインシデントの発生割合及び脆弱性情報が確認された割合を図表 3-1-2 に整理した結果、IaaS、PaaS やネットワーク事業者での割合は高くなかったが、IaaS、PaaS やネットワーク事業者も別の OSS や SaaS、オンプレミス製品を利用している可能性は考えられる。したがって、SaaS 事業者が利用するクラウドサービス、OSS 等ソフトウェアやサービスでインシデントが発生した場合は IT サプライチェーン上の関係者に影響が波及すると考えられるが、委託先が多い中で SaaS 開発に係る IT サプライチェーンでは実際にどのようなリスクがあるのかを明らかにするため No.2 をインシデント概要図に選定する基準の 1 つとした。

選定基準 No.3 の作成理由は次の通り。「3.1.1. インシデント及び脆弱性情報の整理」で記載した、収集したインシデント及び脆弱性情報から得られた示唆「（ウ）SaaS 事業者や OSS コミュニティ等から利用者に対して利用時の設定に関する留意すべき箇所や設定値等ソフトウェアの変更に関する案内を行うことで、利用者側の設定ミスが低減する可能性が考えられる」では、主に SaaS 利用者の設定ミスについて取り上げたが、SaaS 事業者も SaaS の開発時に IaaS、PaaS をはじめ、コード管理ツールに SaaS や OSS を利用する場合があることからクラウドサービス・OSS の利用者であると言える。SaaS 等クラウドサービスや OSS の種類や数も増えているため SaaS 事業者のクラウドサービスや OSS の利用も増加している可能性があり、SaaS 利用者同様に、すべてのソフトウェア・サービスに対する理解が追い付いていない場合も考えられる。それにより、各種設定や責任範囲を含む利用（委託）時の管理が行き届かない箇所が生じる可能性があり、具体的にどのような点がインシデントに発展しているかを図示することで、利用（委託）先の管理における IT サプライチェーンで考慮すべきリスクを明らかにするため No.3 をインシデント概要図に選定する基準の 1 つとした。概要図に取り上げるインシデントの選定基準と実際に概要図に取り上げたインシデントの対応は以下の通り。

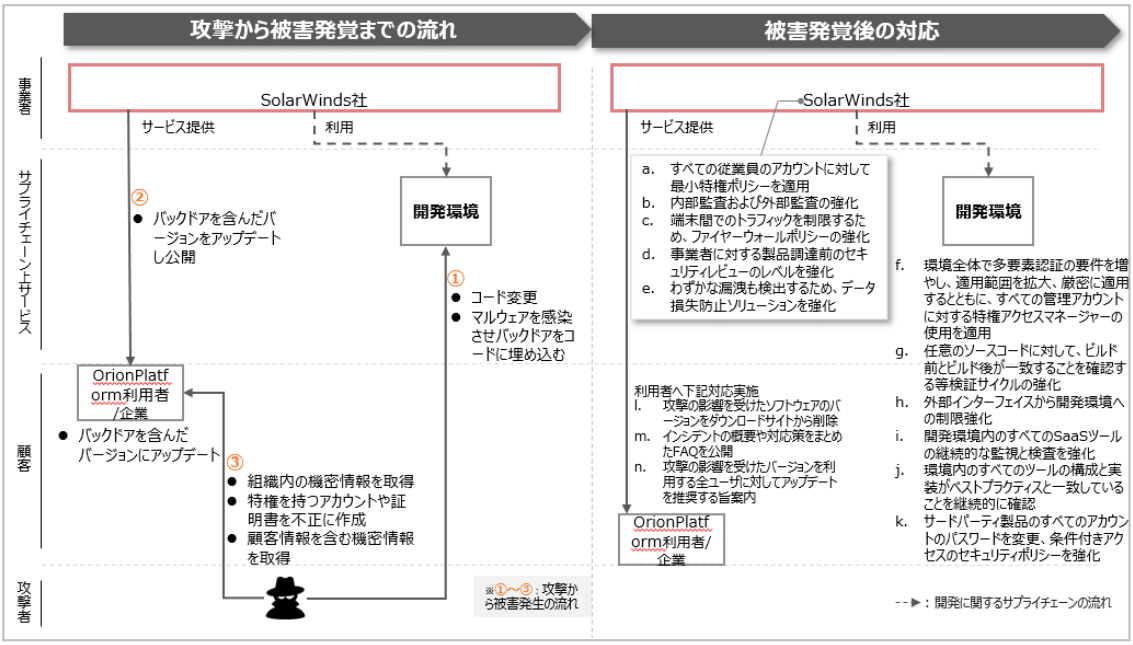
図表 3-1-6：概要図に取り上げるインシデントの選定基準と
実際に概要図に取り上げたインシデントの対応

概要図に取り上げるインシデント選定基準	概要図に取り上げたインシデント
No.1 SaaS 事業者、SaaS 利用者に対して広く被害が発生したインシデント	図表 3-1-7：SolarWinds 社に係るインシデント
No.2 クラウドサービスや OSS 等、SaaS 開発における利用（委託）先に起因するインシデント	図表 3-1-10：Codecov 社に係るインシデント
No.3 SaaS 事業者に起因する、クラウドサービスや OSS の設定を誤る等 SaaS 開発における利用（委託）の管理不備に関するインシデント	図表 3-1-14：ネットマーケティング社に係るインシデント

3.1.2.1. SolarWinds 社に係るインシデントの概要図

SolarWinds 社が提供するネットワーク管理・監視製品「Orion Platform」は、開発工程でのマルウェア感染により、バックドアの役割を持つ改ざんされたコードを混入され、バックドアを含んだバージョンにアップデートした Orion Platform の利用組織は、管理者権限や証明書を盗取された上、別システムを経由する等して機密情報漏洩する等の被害を受けた。以下に本インシデントの概要図を示す。
(Orion Platform は SaaS 製品ではないが、管理・監視の対象に SaaS 製品が含まれている。そのため、Orion Platform を利用している SaaS 事業者が、バックドアが含まれた Orion Platform にアップデートすることにより、SaaS にも影響が発生する可能性があるという 観点から掲載している)

図表 3-1-7：SolarWinds 社に係るインシデントの概要図



図表 3-1-8：SolarWinds 社に係るインシデントの概要図に関する用語説明

用語	説明
開発環境	SolarWinds 社の製品を開発するための環境。本インシデントに関する詳細な経路については不明であったためサーバやサービス単位ではなくまとめた表記をしている。

3.1.2.1.1. インシデントの概要

SolarWinds社は、ネットワーク管理・監視サービスである「Orion Platform」を運営していた。2019

年 10 月には①Orion Platform のコードが改ざんされた可能性があるものの[19]、その改ざんが発見されたのは 2020 年 12 月と、攻撃から 1 年以上の期間が経過していた。2020 年 3 月から 6 月にかけて行われた②Orion Platform のアップデートにより、利用者の情報を盗取可能なように改ざんされたコードを含んだバージョンが公開され、Orion Platform 全体の利用者約 30 万組織のうち約 18,000 の組織がアップデートの影響を受けたとされている[20]。攻撃者は、Orion Platform へマルウェアを感染させ、そのマルウェアによって特定バージョンの Orion Platform に脆弱性を組み込んだ[21]。さらに Orion Platform に組み込まれた脆弱性は、利用者が Orion Platform を実行するサーバ内から情報を盗取できるバックドアの役割を果たしていた。③このバックドアを通じて Orion Platform 利用組織の管理者権限等を取得し、サインイン時に必要なトークンや署名証明書にアクセスすることで特権を持つアカウントや信頼される証明書を不正に発行することが可能であったと考えられている[22]。インシデント発生の原因としては、公表や修正が行われる前の脆弱性への攻撃であるゼロデイ攻撃かサードパーティのアプリまたはデバイスと考えられているが[23]詳細な原因は公表されていない。

2020 年 12 月 13 日に SolarWinds 社は、本インシデントを含める Orion Platform に関するセキュリティアドバイザリを公開した。また、米国の国土安全保障省やサイバーセキュリティソリューションを提供する企業等も本インシデントに関する対策や調査結果を公開しており、攻撃発覚後もアップデートされている[24][25]。後日公開・アップデートされたこれらの情報を含めて、図表 3-1-9 に SolarWinds 社が実施した被害発覚後の対応をまとめた[26]。

---

[19] REVERSINGLABS BLOG. “SunBurst: the next level of stealth”, https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth, [参照 2022 年 2 月 18 日].

[20] SANS Institute. “What You Need to Know About the SolarWinds Supply-Chain Attack”, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/, [参照 2022 年 2 月 18 日].

[21] SolarWinds. “SolarWinds Security Advisory”, https://www.solarwinds.com/ja/sa-overview/securityadvisory, [参照 2022 年 2 月 18 日].

[22] Microsoft. “Important steps for customers to protect themselves from recent nation-state cyberattacks”, https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/, [参照 2022 年 2 月 18 日].

[23] European Network and Information Security Agency (ENISA) (2021). “Threat Landscape for Supply Chain Attacks”, p16, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, [参照 2022 年 2 月 18 日].

[24] The U.S.-The Department of Homeland Security. “Mitigate SolarWinds Orion Code Compromise”, https://cyber.dhs.gov/ed/21-01/, [参照 2022 年 2 月 18 日].

[25] FIREEYE. “Global Intrusion Campaign Leverages Software Supply Chain Compromise”, https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html, [参照 2022 年 2 月 18 日].

[26] SolarWinds. “An Investigative Update of the Cyberattack”,

図表 3-1-9：インシデント発覚後の SolarWinds 社の対応

対応先	記号	対応内容
開発に利用するソフトウェアやサービス	a.	すべての従業員のアカウントに対して最小特権ポリシーを適用
	b.	内部監査および外部監査の強化
	c.	端末間でのトラフィックを制限するため、ファイヤーウォールポリシーの強化
	d.	すべての事業者に対する製品調達前のセキュリティレビューのレベルを強化
	e.	わずかな漏洩も検出するため、データ損失防止ソリューションを強化
	f.	環境全体で多要素認証の要件を増やし、適用範囲を拡大させ、厳密に適用するとともに、すべての管理アカウントに対する特権アクセスマネージャーの使用を適用
	g.	任意のソースコードに対して、ビルド前とビルド後が一致することを確認する等検証サイクルの強化
	h.	外部インターフェイスから開発環境への制限強化
	i.	開発環境内のすべての SaaS ツールの継続的な監視と検査を強化
	j.	環境内のすべてのツールの構成と実装がベストプラクティスと一致していることを継続的に確認
	k.	サードパーティ製品のすべてのアカウントのパスワードを変更、条件付きアクセスのセキュリティポリシーを強化
Orion Platform 利用者	l.	攻撃の影響を受けたソフトウェアのバージョンをダウンロードサイトから削除（2020 年 12 月 13 日）[27]
	m.	インシデント概要や対応策をまとめた FAQ を公開（2020 年 12 月 15 日）[28]
	n.	攻撃の影響を受けたバージョンを利用する全ユーザーに対してアップデートを推奨する旨案内（2020 年 12 月 15 日）

3.1.2.1.2. 考察

当時、世界中で約 30 万組織が利用していた SolarWinds 社の製品が狙われた本インシデントは、

https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/, [参照 2022 年 2 月 18 日].

[27] SolarWinds. “SolarWinds Security Advisory-ABOUT SUNBURST”, https://www.solarwinds.com/ja/sa-overview/securityadvisory, [参照 2022 年 2 月 24 日].

[28] SolarWinds. “FAQ: Security Advisory”, https://www.solarwinds.com/sa-overview/securityadvisory/faq, [参照 2022 年 2 月 24 日].

近年の IT サプライチェーン攻撃を象徴する事例となった。被害発覚後の対応としては、社内システムのアクセス権限を確認、多要素認証の徹底やデータ損失防止のためのソリューションの強化の他に、開発時に利用する SaaS 等のツールに対しても監視の強化、計画した構成、実装がベストプラクティスと一致していることの確認等を実施しており、開発時のソフトウェアやサービス利用の潜在的なリスクにも対処する姿勢が見られた。サプライチェーン上の関係者に対しては、SaaS や IaaS を含むすべての事業者に対する製品調達前のセキュリティレビューのレベルを強化することでソフトウェアやサービス利用以前にもリスクを排除する試みがなされた。また、開発工程へも具体的な再発防止の対応をとっており、異なる工程間でソースコードが一致しているかを検証する工程を追加することを発表している。

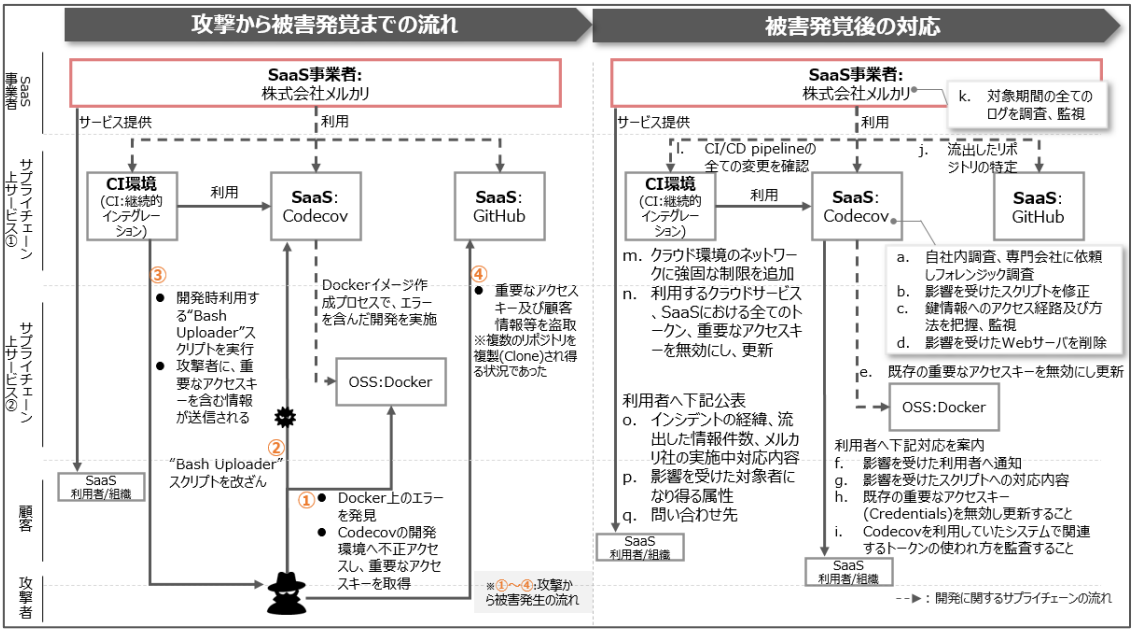
本インシデントでは、ネットワーク管理・監視サービスという利用組織のシステムが関連しており、攻撃時点よりも古いバージョンを中心に攻撃の影響を受けていた。利用組織のシステム全般への影響等を考慮してバージョンのアップデートを行っていなかった組織も影響を受けたが、最も多数の攻撃方法が確認されたのは 2020 年 3 月及び 2020 年 6 月に公開したバージョンである。最新版へアップデートについては、SolarWinds 社が最新版へのアップデートを推奨している場合や、組織によっては事業者が提供するソフトウェアはすぐに最新にするといったポリシーを定めている場合も考えられるが、そのような組織も被害を受けた可能性がある。こうしたソフトウェアの最新バージョン配布経路が攻撃されることで広範囲に被害が及ぶことは IT サプライチェーンにおける脅威の一つと言える。

SaaS 事業者として考慮すべき IT サプライチェーンのリスクとしては、SolarWinds 社が被害発覚後に対応したような、既に利用しているソフトウェアやサービスのセキュアな運用や開発工程でのテスト及びテスト結果確認の徹底等、開発時に利用するソフトウェアやサービスに対して評価する機会を設けず攻撃され得る隙を放置してしまうことが考えられる。

3.1.2.2. Codecov 社に係るインシデントの概要図

コーディングの検証率を計測するテストカバレッジツール「Codecov」を提供する Codecov 社は、2021 年 1 月から 2021 年 4 月にかけて自社 SaaS のスクリプトを改ざんされる攻撃を受けた。スクリプトの改ざんにより、Codecov の利用者の開発環境の情報が攻撃者へ漏洩し、さらに漏洩した情報を悪用され被害が広がる事態に至った。以下に本インシデントの概要図を示す。

図表 3-1-10：Codecov 社に係るインシデントの概要図



図表 3-1-11：Codecov 社に係るインシデントの概要図に関する用語説明

用語	説明
CI 環境（CI：継続的インテグレーション）	CI は Continuous Integration の略称。自動的にコードのエラーや仕様通りの機能が実装されて いるか等テスト、ビルドを実行する環境を指す。
Codecov	コーディングの検証率を計測するテストカバレッジツールを指す。
GitHub	コードのバージョン管理ツールとして利用されるソフトウェア開発のプラットフォームを指す。コードの共有や公開が可能で、コードレビューやプログラムに関する課題の管理にも利用される。
Docker	コンテナ仮想化を用いてアプリケーションを作成・配布・実行するためのプラットフォームを指す。
Docker イメージ	Docker コンテナの実行に必要な、設定値等が含まれたファイル群を指す。 Docker 社が提供する Docker Hub を利用して公開、共有も可能。

3.1.2.2.1. インシデントの概要

Codecov 社はテストカバレッジツールの「Codecov」を運営していた。2021 年 1 月 31 日から 2021 年 4 月 1 日の間に攻撃者により、①Codecov 社が利用するコンテナ環境へ不正アクセスされ、②Codecov を利用した開発時に利用する"Bash Uploader"スクリプトが改ざんされた。③Codecov 利用者が、改ざんされた Bash Uploader を実行した際に、Codecov 利用者の情報が攻撃者へ送信されていた[29]。Codecov を利用していた株式会社メルカリ（以下、「メルカリ社」）は、改ざんされた Bash Uploader 実行時に、認証情報等重要なアクセスキーを攻撃者に取得され、④コードを管理していた GitHub へ不正にアクセスされた。その結果、メルカリ社は顧客・取引先・従業員情報等約 29,000 件が流出する等の被害を受けた[30]。インシデントの原因としては、Codecov 社が利用していたコンテナ管理サービスである「Docker」のイメージ作成時のエラーであり、当該エラーは Bash Uploader に変更を加えるための認証情報を盗取され得るものであったとされる[31]。

Codecov 社への攻撃期間は 2021 年 1 月 31 日から 2021 年 4 月 1 日とされており、Codecov 社からは 2021 年 4 月 15 日にインシデントの概要や対応内容について発表された。メルカリ社への攻撃は 2021 年 1 月 31 以降数回、その後 2021 年 4 月 13 日から 2021 年 4 月 18 日にかけて集中的に不正アクセスがあった。メルカリ社からは 2021 年 5 月 21 日にインシデントの概要や対応内容について発表された。後日公開された対応内容を含めて、図表 3-1-12 に Codecov 社、図表 3-1-13 にメルカリ社が実施した被害発覚後の対応をまとめた[32]。

---

[29] Codecov. "Bash Uploader Security Update", https://about.codecov.io/security-update/, [参照 2022 年 2 月 18 日].

[30] 株式会社メルカリ. 「「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について」, https://about.mercari.com/press/news/articles/20210521_incident_report/, [参照 2022 年 2 月 18 日].

[31] European Network and Information Security Agency (ENISA) (2021). "Threat Landscape for Supply Chain Attacks", p34, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, [参照 2022 年 2 月 18 日].

[32] Mercari, Inc. "Attacking and Securing CI/CD Pipeline", https://speakerdeck.com/rung/cd-pipeline?slide, [参照 2022 年 2 月 18 日].

図表 3-1-12：インシデント発覚後の Codecov 社の対応

対応先	記号	対応内容
SaaS 開発に利用するソフトウェアやサービス	a.	自社内調査、専門会社に依頼しフォレンジック調査
	b.	影響を受けたスクリプトを修正
	c.	重要なアクセスキーへのアクセス経路及び方法を把握、監視
	d.	影響を受けた Web サーバを削除
	e.	Bash Uploader の変更を可能にするために利用されたキーを含む、インシデントに関連する既存の重要なアクセスキーを全て無効に更新
Codecov 利用者	f.	本インシデントで影響を受けた利用者へ通知（2021 年 4 月 15 日）
	g.	影響を受けたスクリプトを修正した旨を対応内容と共に利用者へ公表（2021 年 4 月 15 日）
	h.	既存の重要なアクセスキーを無効にして更新することを案内（2021 年 4 月 15 日）
	i.	Codecov を利用していたシステムに関連する、トークンの使われ方を監査するよう案内（2021 年 4 月 15 日）

図表 3-1-13：インシデント発覚後のメルカリ社の対応

対応先	記号	対応内容
SaaS 開発に利用するソフトウェアやサービス	j.	被害を受けたリポジトリの特定
	k.	攻撃対象期間等のログの調査、監視
	l.	CI/CD pipeline の全ての変更を確認
	m.	クラウド環境のネットワークに強固な制限を追加
	n.	利用するクラウドサービス、SaaS における全てのトークン、重要なアクセスキーを無効にし、更新
メルカリ利用者	o.	インシデントの経緯、流出した情報件数、メルカリ社実施中の対応内容の公開
	p.	流出した情報の種類や流出した情報に関連するサービス等、影響を受けた者の対象になり得る属性の公開
	q.	インシデントに関する専用の問い合わせ窓口の設置

3.1.2.2.2. 考察

本インシデントの発端となる攻撃を受けた Codecov 社は、Bash Uploader に関するキー以外にも、重要なアクセスキーを無効化し、その後も継続的な監視を設定した。また、Codecov 社が更新した最

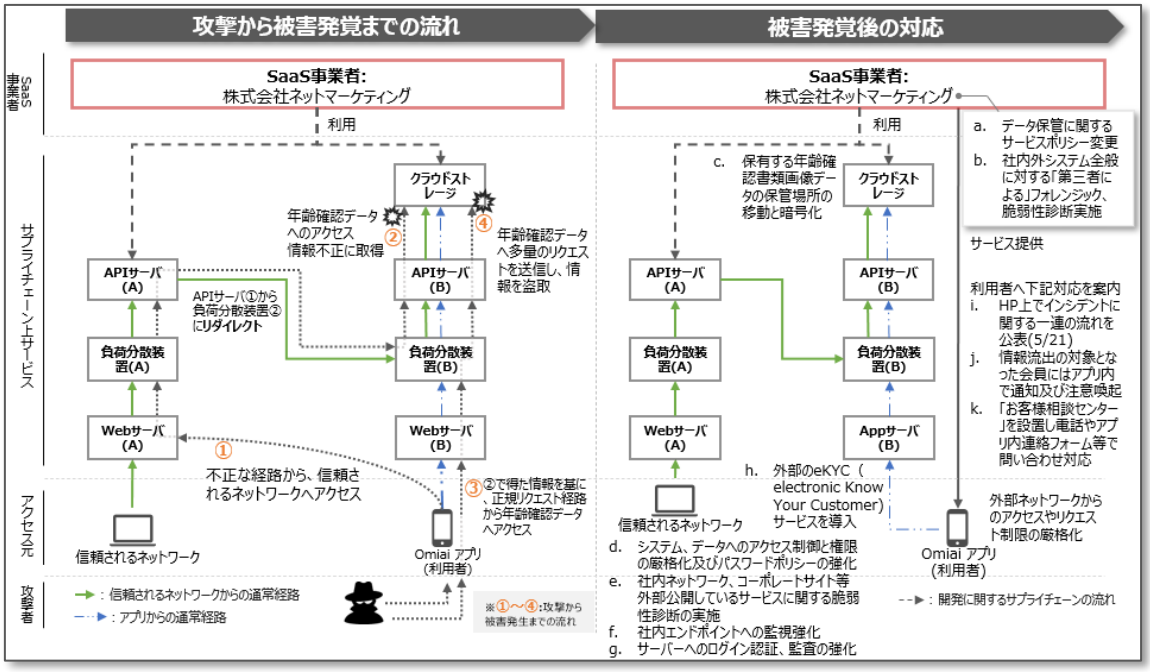
新バージョンの Codecov へは Codecov 利用者にて更新が必要であるため、対象かどうかを確認する方法と共にバージョン更新方法を公開した。Codecov 利用者に対しても可能な限り再発防止策を実施してもらうため、バージョン更新に加えて、Bash Uploader を利用した CI 環境で利用される重要なアクセスキー、トークンを全て変更することが推奨される旨案内している。

本インシデントでは、Codecov 社が利用するコンテナ管理サービスの利用プロセスでエラーが発生し、そのエラーにより Codecov 社の SaaS が汚染されている。さらに、汚染された SaaS を開発工程で利用していた SaaS 事業者の情報が盗まれた上、盗まれた情報が悪用されることで最終的には顧客情報の漏洩につながる等、SaaS の開発に係る IT サプライチェーン上で連鎖的に影響があった事例と言える。開発工程で利用されるコードには、開発時に利用するソフトウェアやサービスへのアクセス情報を含むことがあり、そのアクセス情報を利用された場合に、顧客に関連する情報や個人情報等の機密情報を含むクラウドストレージ等にアクセスされる可能性がある。したがって、SaaS の開発工程におけるソフトウェアやサービスの利用は、コードに含まれる機密情報によって連鎖的に影響が波及する可能性があり、SaaS に係る IT サプライチェーンのリスクとしてこと考慮すべきポイントであることが示唆されたと言える。

3.1.2.3. ネットマーケティング社に係るインシデントの概要図

株式会社ネットマーケティング（以下、「ネットマーケティング社」）が提供するマッチングアプリサービスの「Omiai」は、2021 年 4 月に行われた攻撃で、年齢確認データが保存されるストレージへのアクセス情報を盗まれた。さらに正規のリクエストを利用した不正アクセスをされ、年齢確認データ約 171 万件が流出する被害を受けた。以下に本インシデントの概要図を示す。

図表 3-1-14：ネットマーケティング社に係るインシデントの概要図



図表 3-1-15：ネットマーケティング社に係るインシデントの概要図に関する用語説明

用語	説明
ファイルストレージサービス	ネットマーケティング社公式発表資料に記載された表記。データを保管するためのストレージを提供するサービスを指す。
信頼されるネットワーク	ネットマーケティング社公式発表資料に記載された表記。ネットマーケティング社公式の解説はないが、ネットマーケティング社の社内環境等を利用した接続によって一定以上セキュアであると考えられるネットワークが想定される。

3.1.2.3.1. インシデントの概要

ネットマーケティング社はマッチングアプリサービスの「Omiai」を運営していた。2021 年 4 月に攻撃者により、①不正な経路から信頼されるネットワークを通じて、②年齢確認データが保存されているストレージへのアクセス情報が盗取された。さらに当該アクセス情報をもって③正規のリクエストを多量に送信して不正アクセスが行われ、④年齢確認データ約 171 万件が流出する事態が発生した[33]。インシデント発生の原因としては、マルウェア感染や脆弱性ではなく偽装したリクエストによる不正アクセスと考えられるが、不正な経路から信頼されるネットワークへアクセスした原因については公表されていない。

攻撃期間は 2021 年 4 月 20 日から 2021 年 4 月 26 日とされており、2021 年 4 月 28 日にはインシデントを認識し、2021 年 5 月 21 日には公式 HP にてインシデントに関する影響や対応状況について情報を公開した[34]。後日公開された対応内容を含めて図表 3-1-16 に、ネットマーケティング社が実施した被害発覚後の対応をまとめた。

[33] 株式会社ネットマーケティング. 不正アクセスによる会員様情報流出の調査結果と今後の対応について, https://www.net-marketing.co.jp/news/6001/, [参照 2022 年 2 月 18 日].

[34] 株式会社ネットマーケティング. 不正アクセスによる会員様情報流出に関するお詫びとお知らせ, https://www.net-marketing.co.jp/news/5873/, [参照 2022 年 2 月 18 日].

図表 3-1-16：インシデント発覚後のネットマーケティング社の対応

対応先	記号	対応内容
サービスポリシー	a.	Omiai 会員に関するデータ保管期間を「退会後一律 10 年間」から短縮して変更（2020 年 12 月 1 日より適用）。年齢確認データは提出後 72 時間とし、それ以降は自動的に削除される。会員個人情報は退会後 90 日間とした。ただし被害にあった約 171 万アカウントを除く。
SaaS 開発に利用するソフトウェアやサービス	b.	社内外システム全般に対する「第三者による」フォレンジック、脆弱性診断実施
	c.	被害にあった約 171 万アカウント分は、二次被害発生時の事実確認や諸対応に必要なため、データ暗号化した上でインターネットから遮断されたサーバへ保存
	d.	システムや情報へのアクセス制御と権限の厳格化及びパスワードポリシーの強化
	e.	社内ネットワーク、コーポレートサイト等外部公開しているサービスに関する脆弱性診断の実施
	f.	社内エンドポイントへの監視強化
	g.	サーバへのログイン認証、監査の強化
業務プロセス	h.	年齢確認プロセス厳格化のため、外部の eKYC（electronic Know Your Customer）サービスを導入
Omiai 利用者	i.	ネットマーケティング社 HP 上でインシデントに関する一連の流れを公表（2021 年 5 月 21 日）
	j.	情報流出の対象となった会員にはアプリ内で通知及び注意喚起
	k.	「お客様相談センター」を設置し電話やアプリ内連絡フォーム等で問い合わせ対応（2021 年 5 月 21 日）

3.1.2.3.2. 考察

約 171 万件の情報流出という比較的規模の大きなインシデントであり、被害を受けた原因が脆弱性に対する攻撃ではないため、社内のシステム全般に対する第三者によるフォレンジックを実施する等全社的な対応が行われている。再発防止策として、システムや情報へのアクセス権限強化や監視の強化を行っているが、自社内だけの対応ではなくサービスポリシーの変更や利用者に対しても、より安全に利用してもらうためのプロセスを依頼しており、改めてインシデントが SaaS 事業者へ与える影響がうかがえる。

本インシデントの攻撃経路に着目すると、ネットマーケティング社が利用していたファイルストレージサービスへのアクセス権限を取得された後データを不正に取得されている。ファイルストレージサービスがネットマーケティング社にて構築されたものか IaaS 等のクラウドストレージであるかは明らかにされていないが、再発

防止策としてファイルストレージ上のデータを暗号化して、一部データについては暗号化に加えて別のネットワークに移動させ保管している。そのことを踏まえて本インシデントからは、ストレージ上にあるデータの保護やアクセス権の管理が原則 SaaS 事業者にあることは IT サプライチェーンのリスクとして考慮すべきポイントであることが示唆されたと言える。

3.2. インタビュー調査結果

インタビュー調査では、事前に作成した図表 1-5-2 及び、インタビュー質問項目を用意しインタビューを実施した。

質問項目は図表 3-2-1 に示す。インタビュー結果は、課題案に関するもの（図表 3-2-1 の質問 1,2,3）と課題案としては挙げていないがインタビューの中で聞くことが出来た SaaS が抱える脅威やリスクに関する観点についての結果（図表 3-2-1 の質問 4）を分けて記載している。なお、質問項目は以下の通り。

図表 3-2-1：インタビュー質問項目

質問番号	質問内容
質問 1	SaaS 事業者が抱える課題案と SaaS 事業者の認識との乖離はあるか
質問 2	「開発」、「監視」、「対応」の工程軸で整理し、SaaS 事業者が抱える課題案を作成した（図表 1-5-2）が、他に考慮すべき軸や各工程で考慮すべき事項はあるか
質問 3	SaaS 開発に係る IT サプライチェーンにおいて、特に重要と思われる脆弱性の発生箇所やインシデントパターンはあるか
質問 4	開発に限らず、SaaS に関する IT サプライチェーンにおいて、SaaS 事業者が抱える課題や、SaaS 事業者にとって今後リスクとなり得るものはあるか

また、以下にインタビュー調査結果の全体像を示した。

図表 3-2-2：インタビュー調査結果目次

セクション	インタビュー内容	
3.2.1. 課題案に関するインタビュー結果	3.2.1.1.	開発時のセキュリティ対策の実施状況について
	3.2.1.2.	セキュリティに関する監視ナレッジについて
	3.2.1.3.	インシデント発生時の対応・準備について
	3.2.1.4.	SaaS 事業者が抱える課題案に対する観点について
3.2.2. 開発工程に係る考慮すべき課題やリスクに関するインタビュー結果	3.2.2.1.	考慮すべき脆弱性の発生箇所やインシデントパターンについて
	3.2.2.2.	OSS に対するセキュリティの評価について
	3.2.2.3.	API に対するセキュリティの評価について
	3.2.2.4.	クラウドサービスの利用者に起因するインシデントについて
3.2.3. 開発工程以外の課題やリスクに関するインタビュー結果	3.2.3.1.	SaaS の可用性確保について
	3.2.3.2.	個人情報等機密データの保護について
	3.2.3.3.	クラウドサービス事業者のセキュリティに関する情報公開について
	3.2.3.4.	SaaS とオンプレミスソフトウェアの違いについて
3.2.4. その他得られた観点	3.2.4.1.	「B to B SaaS」と「B to C SaaS」における違い

3.2.1. 課題案に関するインタビュー結果

本項では、調査開始時に作成した「SaaS 事業者が抱える課題案」（図表 1-5-2）に対して行ったインタビュー結果を記載した。各々の課題案が肯定される結果とはならなかったが、各工程や課題案に関連して、自社の SaaS に対する責任をもって慎重に設計したり、開発時のセキュリティレベルの確保や脆弱性情報収集において工夫したりといった、SaaS 事業者のセキュリティ対策への取り組みの実態をヒアリングすることができた。

3.2.1.1. 開発時のセキュリティ対策の実施状況について

以下の課題案についてインタビューを実施した。その結果を図表 3-2-3 に示した。

- 課題案 1：開発時に機能開発が優先され、セキュリティ対策が十分でないのではないか
  - 課題案 1-1：非機能要件定義時に、セキュリティに関する項目が十分に含まれていないのではないか
  - 課題案 1-2：インシデントを考慮したアーキテクチャ（冗長構成等）を検討、採用できていないのではないか
  - 課題案 1-3：セキュリティ要件を確認するテスト項目が作成されていないのではないか

図表 3-2-3：開発時のセキュリティ対策の実施状況に関するインタビュー調査結果

回答	コメント内容
組織 A	・「開発時に機能開発が優先され、セキュリティ対策が十分でない」という傾向はあるかもしれないが、「組織としてセキュリティ対策に注力する体力が不足している」という表現の方が実態に近い。
組織 B	・ SaaS 事業者は開発、提供する SaaS 及び利用者に対して責任を持ち、損害発生時のリスクも担っているため、検討を重ねて企画、開発やリリースを実施している。 ・ 開発時のセキュリティ対策に関するリスクヘッジとして PaaS 等を利用することもあり、セキュリティ対策が十分ではないまま SaaS 提供を行うとは言い難い。
組織 D（SaaS 事業者）	・ 自社では、PSIRT（Product Security Incident Response Team）が設計内容を確認することでセキュリティレベルを確保している。 ・ 受託開発等で契約上、リリースや納期に期日が設けられている場合は機能の完成を優先してセキュリティに対する意識が疎かになる可能性も考えられるが、SaaS 事業者は自社で製品を開発しているため、セキュリティレベルに関して柔軟な運用が可能な面もあると言える。 ・ これまではウォーターフォール開発をしていたため、テスト工程等セキュリティについて確認するタイミングが明確に存在していたが、アジャイル開発ではセキュリティに関する確認タイミングを確立し難く、各 SaaS 事業者の共通課題として挙げられる。 ・ SaaS 事業者のセキュリティレベルの維持・向上に有用なガイドライン等の情報やサービスが増加しているため、各 SaaS 事業者はそれらを参考にしつつ開発に取り組んでいる。 ・ 自社ではセキュリティに関する検証チームを設け、各製品の検証工程を開発フローに組み込むことでセキュリティレベルを確保するための体制を整えている。
組織 E	・ SaaS を一から設計・開発する工程ではセキュリティを含めて比較的慎重に設計するが、SaaS リリース後に機能を追加・改修（バージョンアップや機能の移行等を含む）する工程では変更に伴う影響が十分に考慮されていない可能性が考えられる。

3.2.1.1.1. インタビューから分かったこと

インタビューの結果、SaaS 事業者が SaaS 及び利用者に対して負う責任の実態や、開発時に利用するサービス・ソフトウェアの管理コスト低減や有事の際のリスクヘッジのために利用可能な PaaS や IaaS が存在するため、概ね SaaS 事業者が開発時にセキュリティ対策を疎かにしてしまう場面は多くない可能性が示唆された。したがって、課題案 1「開発時に機能開発が優先され、セキュリティ対策が十分でないのではないか」は大きく支持されなかったが、「受託開発等で契約上、リリースや納期に期日が設けられている場合は機能の完成を優先してセキュリティに対する意識が疎かになる」という可能性や「機能を追加・改修する工程では変更に伴う影響が十分に考慮されていない」可能性も考えられる等、特定の場面においては留意したい IT サプライチェーン上のリスクとして存在し得ると言える。

課題案 1-1 及び課題案 1-2 に関しては、昨今セキュリティ対策のためのガイドラインが増えており、実際に SaaS 事業者が参考にして開発していることからも、非機能要件のセキュリティに関する項目は一定以上カバーされ、インシデント発生時を考慮した冗長化構成等が採用・実装されていることがうかがえる。課題案 1-3 に関しては、SaaS 事業者内でセキュリティレベルを確保するためのチームを設置し、設計内容の確認や開発フロー内における検証工程を担う等、セキュリティ要件を確認する以上の工夫を実施している SaaS 事業者も存在することがうかがえた。また、単にテスト項目を追加するのではなく、組織の体制や仕組みからセキュリティ対策を実施することで、現在主流なアジャイル開発下でもセキュリティに関する確認タイミングや確認時間がある程度確保可能との指摘も得た。

3.2.1.1.2. 今後深堀が必要なポイント

「組織としてセキュリティ対策に注力する体力が不足している」点は SaaS 事業者の課題に挙げられる。セキュアな開発のために組織体制を変更することはどの SaaS 事業者でもできるとは言い難い。そのため今後は、公開されている有用なガイドラインを活用する等によって、限られたリソースの中で開発時のセキュリティを維持・向上させることが求められると考えられる。

3.2.1.2. セキュリティに関する監視ナレッジについて

以下の課題案についてインタビューを実施した。その結果を図表 3-2-4 に示した。

- 課題案 2：セキュアな監視ナレッジが十分でないのではないか
  - 課題案 2-1：脆弱性や機能（設定値）のアップデートに関する情報を収集できていないのではないか
  - 課題案 2-2：境界・エンドポイント型の検知システムを活用できていないのではないか

図表 3-2-4：セキュリティに関する監視ナレッジに関するインタビュー調査結果

回答	コメント内容
組織 A	・ 「セキュアな監視ナレッジが十分ではない」印象は少なからずある。 ・ SaaS 事業者が SaaS に関するログを利用者に提供し、利用者が SaaS を監視可能な状態にする等 SaaS 利用者視点でセキュアな運用に資する工夫も考えられる。
組織 D（SaaS 事業者）	・ OSS の脆弱性情報収集については利用する OSS の数及び脆弱性情報の量も多いため、OSS のリスト化や脆弱性情報収集に関するツールを用いても抜けもれなく収集することは困難であるが、収集のタイミングを週次や日次等定期的または開発完了時等特定のイベント発生時に行う等工夫をし、可能な範囲で対応している。 ・ 製品に関する脆弱性情報を発見した際、関係する製品の開発チームへ共有され、開発チームにて脆弱性情報が製品へ及ぼす影響評価及び修正実行の判断をしている。 ・ 近年、脆弱性情報が公開された後、関連する攻撃手口（テストコード）情報が短期間で共有される傾向があるため、脆弱性情報公開から SaaS に対する脆弱性の影響調査・対応判断及び実際の対応までを比較的短い期間で行うことが求められる印象がある。
組織 E	・ SaaS 事業者は、ネットワークの境界やエンドポイントの管理よりも SaaS 自体への監視について課題を抱えている様子がある。

3.2.1.2.1. インタビューから分かったこと

調査結果からは、OSS をはじめとした SaaS 開発時に利用するソフトウェアやサービスの数や多様さゆえに全般的には「セキュアな監視ナレッジを十分に保有し、活用できている」とは言い難い状況がうかがえ、課題案 2 については一定程度支持されると考えられる。

また、近年の傾向として脆弱性情報の公開後、その脆弱性を実際に利用する攻撃手口が共有され実際に攻撃が始まるまでの期間が、年々短縮されているという指摘も得られ、より迅速な脆弱性対応が事業者に求められていると言える。

3.2.1.2.2. 今後深堀が必要なポイント

課題案 2-2 に関連して、「境界・エンドポイント型の検知システム活用」より「SaaS 自体への監視」について課題を抱えている等、監視の体制や監視手法の実現において困難がある可能性もうかがえる。監視について課題を抱えている状況からは、昨今の開発スタイルや開発に関するサービスの変化に対応した、より効率的な監視手法を採用することが求められている可能性も考えられる。

また、課題案 2-1 に関しては、脆弱性や機能(設定値)のアップデートに関する情報収集において「利

用している OSS をリスト化し、情報収集ツールを活用して定期的に脆弱性情報を収集」し、さらに脆弱性情報を収集するチームと脆弱性の影響を評価・判断する開発チームを分けて運用している SaaS 事業者の話もうかがえたが、現実的にはベストエフォートで対応せざるを得ない状況がうかがえる。特に、小規模で SaaS 開発を行う事業者にとっては、利用している OSS をリスト化しリストの継続的な更新を行うことも業務量としては小さくない。しかし、脆弱性情報の公開後攻撃手口が共有されるまでの期間が短縮されている傾向もあるとされ、SaaS 事業者各々の取り組みとして情報収集ツール等を活用して効率的に脆弱性や機能のアップデートに関する情報収集を行うだけでなく、監視に関する組織体制の強化等が課題として挙げられよう。

3.2.1.3. インシデント発生時の対応・準備について

以下の課題案についてインタビューを実施した。その結果を図表 3-2-5 に示した。

- 課題案 3：インシデント対応・準備が十分でないのではないか
  - 課題案 3-1：発生時の責任者や確認箇所・項目に関して策定できていないのではないか
  - 課題案 3-2：インシデント対応完了の基準を作成していないのではないか

図表 3-2-5：インシデント発生時の対応・準備に関するインタビュー調査結果

回答	コメント内容
組織 A	・ 課題案「インシデント対応・準備が十分でない」については、OSS 等には何らかの脆弱性が存在することを前提としてインシデントに備えた体制を整えることが重要と感じている。 ・ インシデントへの対応時には、脆弱性の修正パッチ適用等の技術的な対応を行うことに加えて、原因・影響に関する詳細情報の公開等、利用者からも受け入れられる誠実な対応が必要。
組織 C	・ 事業者規模の大小や、オンプレミスソフトウェア事業者か SaaS 事業者かによって、脆弱性の発覚時またはインシデント発生時の対応の早さに大きな違いはない印象がある。 ・ SaaS 事業者の本社がある国以外の国（以下、”現地”とする）で、SaaS に関する問題が発生した場合、本社内で「設計の確認」や「修正の判断」が行われることがあるため、現地で脆弱性やインシデントに関する問い合わせを受けたとしても即座に対応できないケースがある。したがって、SaaS を利用する際は、本社の場所を確認することを含めて、脆弱性発覚やインシデント発生時の対応にかかる時間や問い合わせ手続き等を事前に把握しておくことが良い。

3.2.1.3.1. インタビューから分かったこと

インシデント発生時の対応については対応の姿勢や事業者ごとの差異についてコメントを得た。開発時に利用する数や種類が多いと考えられる OSS をはじめ、脆弱性が存在する前提でインシデントに備えた体制を整えることが実際のインシデント対応時に有効な準備であると言える。

3.2.1.3.2. 今後深堀が必要なポイント

今回の調査では、課題案 3-1,3-2 等に関する詳細なインシデント対応に関するルール等の回答を得られなかったが、予期せぬインシデントに対して詳細に確認箇所や項目を事前に決めておくことは、リソースの限られた SaaS 事業者にとって負担が少なくないと考えられるものの、「開発時に利用するソフトウェアやサービスに関する問い合わせ先を整理しておくこと」、「インシデント発生時の利用者に対する案内や説明等 SaaS 利用者に向けた対応」をすることも、インシデント発生時に速やかな対応を取るうえで必要であると考えられる。脆弱性の修正パッチ適用といった技術的な対応に限らない、平時からの準備が求められる。

3.2.1.4. SaaS 事業者が抱える課題に対する観点について

SaaS 事業者がセキュリティリスクマネジメントに関して抱えている課題案について、インタビューを通してどのような観点が他にありうるのかといった内容についてインタビューを実施した。

図表 3-2-6：SaaS 事業者が抱える課題案に対する観点に関するインタビュー調査結果

回答	コメント内容
組織 E	・ クラウドサービスベンダー等が公開するプラクティスは、あるべき姿を示す指針として役立つが、どのようにして実現するかを把握できていない SaaS 事業者は多い。例えば「OWASP TOP10 の A08:2021-Software and Data Integrity Failures[35] で示される検証の方法や A09:2021-Security Logging and Monitoring Failures [36]でのセキュリティ監視方法。 ・ ログの監視だけでなく OS や利用するソフトウェアの監視をどう実現するか等は普及していない。 ・ あるべき姿への実現を手助けするリファレンスが広く認知されていないことも、SaaS 事業者が課題を抱える要因の一つ。CIS（Center for Internet Security）Benchmarks[37]等は、SaaS事業者も利用可能なリファレンスであり、項目の確認方法や設定値の書き方についても具体的に記載されている。また、OWASP Cheat Sheet Series[38]もコードの実装例まで記載されているものもあり、多様なセキュリティプラクティスを実現する際の手助けとなる。 ・ SaaS の開発ライフサイクルを回す際、「SaaS をサービスとして設計する際に、扱う情報自体及びその管理方法含めた検討を行う」等、開発や監視等各工程でどのようなことを行うべきかを把握し実行することは重要である。 ・ セキュリティ上のリスクを低減するためにも、開発ライフサイクル自体を評価するリスクアセスメントのサイクルも回すことが望ましい。特にスモールスタートで SaaS 開発を開始した事業者は、リスクアセスメント含めた、SaaS に関する全体のサイクルが回せていないことがある。

[35] Open Web Application Security Project (OWASP) (2021). “OWASP TOP10 A08:2021 – Software and Data Integrity Failures”, https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/, [参照 2022 年 2 月 18 日].

[36] Open Web Application Security Project (OWASP) (2021). “OWASP TOP10 A09:2021-Security Logging and Monitoring Failures”, https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/, [参照 2022 年 2 月 18 日].

[37] Center for Internet Security(CIS), “CIS Benchmarks”, https://www.cisecurity.org/cis-benchmarks/, [参照 2022 年 2 月 18 日].

[38] Open Web Application Security Project (OWASP), “CHEAT SHEET SERIES PROJECT”, https://cheatsheetseries.owasp.org/, [参照 2022 年 2 月 18 日].

3.2.1.4.1. インタビューから分かったこと

「3.2.1.1. 開発時のセキュリティ対策の実施状況について」、「3.2.1.2. セキュリティに関する監視ナレッジについて」、「3.2.1.3. インシデント発生時の対応・準備について」にて、「開発」「監視」「対応」の各工程における課題案に関するインタビュー調査結果を扱ったが、その他質問項目への回答とは別に SaaS 事業者の抱える課題や考慮すべき点についてもコメントを得た。

本調査は 3 つの工程に分けて課題案を作成したが、さらにリスクアセスメントを繰り返し実施することにより、リスクの低減を図ることの必要性を示唆された。ただし、小規模な SaaS 事業者は人的リソース等の不足もあり、リスクアセスメントを繰り返し実施することが困難な可能性がある。

SaaS 事業者が抱える課題や SaaS の開発に係る IT サプライチェーン上の脅威・リスクを把握するためには、SaaS 事業者の主な事業モデルは「システムを作成して納品する形」ではないことを理解し、新しい開発スタイルであるアジャイル開発や SaaS が継続的に開発・運用されている状況等を加味したうえで課題案を作成することの必要性が示唆された。

3.2.1.4.2. 今後深堀が必要なポイント

SaaS 事業者が抱える課題として、「セキュリティ対策の具体的な実現方法がわからない」ということが考えられる。SaaS 事業者が必要としているセキュリティ対策のガイドラインや注意すべき脅威に関する情報は公開されているものの、実際にどのようにしてベストプラクティスのような設計を実現できるかといった実践的な情報が限られている様子がうかがえる。CIS Benchmarks 等一部の領域については具体的な設定方法まで公開された情報も存在するが、ログ監視に関する情報はあるが OS やソフトウェアへの監視に関しては情報が少ない等、情報が公開されている開発工程やコンポーネントと情報が公開されていないものが存在しており、ガイドラインやプラクティスだけではなく、具体的な設計や実装方法についての情報が求められていると言えよう。

3.2.2. 開発工程に係る考慮すべき課題やリスクに関するインタビュー結果

本項では、「SaaS 事業者が抱える課題案」（図表 1-5-2）以外に、開発工程に係る考慮すべき課題やリスク、「3.1. インシデント調査結果」に対する意見について実施したインタビュー調査結果を記載した。CI/CD や OSS、API 等開発段階で考慮すべき技術的な観点に加えて、利用者に起因するインシデントを含め、SaaS 事業者内で完結せず IT サプライチェーン上の関係者にも注意を払うべき課題がうかがえた。

3.2.2.1. 考慮すべき脆弱性の発生箇所やインシデントパターンについて

インシデント調査結果から得られたリスク所在やインシデントのパターン、およびそこから示唆される事項について、SaaS 事業者の実態と照らし合わせてどのように考えられるか、他に考慮すべき点はあるかについてインタビューを実施した結果を示す。

図表 3-2-7：考慮すべき脆弱性の発生箇所やインシデントパターンに関するインタビュー調査結果

回答	コメント内容
組織 E	・ CI/CD（Continuous Integration / Continuous Delivery）に関しては、OWASP TOP10:2021 でも言及されており[39]、重要なデータの整合性が検証されずにコードが公開される等の可能性があるため、今後の普及見込みを踏まえると考慮すべきパターンと言える。 ・ ソフトウェアの開発者が企業買収によって変更となることや、開発者がソフトウェア開発に関する管理権限を他者に渡すことによって、これまで利用していたソフトウェアが悪意のあるソフトウェアとなる可能性がある。 ・ 「SaaS 設計段階で Secure Design のプラクティス等を参考にせず脆弱な設計を実装してしまう状態」や、「利用しているソフトウェアに関する脆弱性情報に気付かず、組み込まれた脆弱性を維持してしまっている状態」等、SaaS 開発者が、利用しているソフトウェア、コンポーネント等の性質を十分に理解しないまま利用している場合にも注意が必要。 ・ 複数の SaaS 開発者が共同で開発を行っている場合、自社が対応すべき範囲及び共同開発相手が対応すべき範囲の誤認識が相互に生じることがある。責任所在に対する相互の誤認識の結果、互いに「自社の責任範囲ではない」と認識された範囲の設計が脆弱なままリリースされ得るため考慮すべきパターンの 1 つと言える。 ・ SaaS との連携を行う際には連携先に与える認可の範囲が広く不明瞭なものも存在する。OAuth で連携する際には、連携先が他にどのようなアプリケーションと接続されているかが利用者から確認できず、必要以上の権限を許可してしまうことがある。また、SaaS 連携時に求められる認可の範囲が広いが、求められる認可の範囲を十分に確認せずに、SaaS 利用者が意図している以上の権限を許可してしまう場合もある。

3.2.2.1.1. インタビューから分かったこと

インタビューを通して、SaaS 開発のサプライチェーン上のリスク所在箇所について、以下の事柄について指摘を受けた。

- 近年注目されている CI/CD については、「3.1.2.2. Codecov 社に係るインシデントの概要図」でも取り上げた。CI/CD では効率的にコードの管理・検証及び本番環境へのリリースが可能であるが、CI/CD 上での設定ミスや不具合を見過ごした場合は、SaaS に直接影響が発生する。特に自動更新設定については、OWASP TOP10:2021 にも記載があり、十分に検証されないまま攻撃

[39] Open Web Application Security Project (OWASP) (2021). "OWASP TOP10 A08:2021 – Software and Data Integrity Failures", https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/, [参照 2022 年 2 月 18 日].

者がアクセスできる範囲に重要なコードを公開してしまう可能性が指摘されている。SaaS 開発者が、利用しているソフトウェアコンポーネント等の性質を十分に理解しないまま開発してしまう場合も、OWASP TOP10:2021 にて「A04:2021-Insecure Design」として取り上げられているリスクの一つである[40]。

- SaaS 同士の連携に関して、連携先 SaaS から求められる認可の範囲が不明瞭な場合は、連携先に問い合わせる等で可能な限りセキュリティ対策を実施することが必要である。利用している OSS をリスト化することに倣い、SaaS 連携時の連携先についても把握できるよう工夫することも有効である。

3.2.2.1.2. 今後深堀が必要なポイント

SaaS 開発工程で考慮すべき脆弱性の発生箇所やインシデントパターンとして、具体的な開発手法や開発時に利用するサービスに関する脆弱性に加えて、設計段階での意図しないセキュリティ考慮不足や委託先等との共同開発時における不明瞭な責任範囲等の人為的に誘発されるインシデントパターンが挙げられた。

利用しているソフトウェアが買収されることで悪意のあるソフトウェアへ変化することも考慮が必要と考えられるが、脆弱性情報とは異なる情報の収集であるため、対策が及ばない SaaS 事業者も存在する可能性がある。

複数の SaaS 事業者が共同で SaaS を開発する場合や、再委託先を利用する場合は、詳細な責任範囲の明確化が必要であると言える。開発前に締結した契約書上での取り決めだけでは SaaS の詳細な機能ごとの仕様や検証責任について曖昧な領域が生じる可能性があるため、定期的に委託先・委託元間で仕様や契約に関する認識を合わせることの重要性もうかがえた。

[40] Open Web Application Security Project (OWASP) (2021). “OWASP TOP10 A04:2021 – Insecure Design”, https://owasp.org/Top10/A04_2021-Insecure_Design/, [参照 2022 年 2 月 18 日].

3.2.2.2. OSS に対するセキュリティの評価について

SaaS 開発の際に利用される OSS について、SaaS 事業者がサプライチェーン上のリスクとしてどのように評価しているかについて、インタビューを実施した結果を示す。

図表 3-2-8：OSS に対するセキュリティの評価に関するインタビュー調査結果

回答	コメント内容
組織 A	・ OSS に対しては、セキュリティの専門家が確認をしておりセキュリティレベルがある程度確保されていると考えられる。
組織 B	・ 組織に所属している SaaS 事業者からは「OSS を利用したことでインシデントが発生した」という話を現時点ではあまり聞くことがない。 ・ CIS（Center for Internet Security）が提供する Hardened Images 等セキュリティレベルが一定程度保証された OSS を利用することで、OSS の脆弱性やバージョンに関するリスクを低減する選択肢も存在する。
組織 C	・ OSS は、基本的にソースコードが公開されているため脆弱性が発見される機会が多いが、OSS ではないソフトウェアと比べて脆弱性が多いからといって、「セキュアに開発されていない」ということではない。反対に、国内のみで開発、利用されているソフトウェアに脆弱性が発見されていないからといって、セキュアに開発されているとは限らない。
組織 D（SaaS 事業者）	・ 自社では OSS を選定する際の基準を設け、「OSS が定期的にアップデートされていること」や「OSS に関する情報が十分に公開されていること」を確認している。 ・ 自社では OSS を選定、導入する責任を各担当チームが担っている。仮に導入した OSS のアップデートが停止された場合であっても、開発チーム内で、当該 OSS に関する機能の維持や必要な修正を行うことを承知の上、OSS を導入している。 ・ オンプレミスソフトウェア、SaaS に関わらず、OSS 利用時には「再配布等ライセンス違反に該当しないか」等 OSS のライセンスを定期的に確認することが必要。
組織 E	・ OSS には個人が開発したものや OSS コミュニティの数人が開発、維持するものも存在する。最終更新から数年経過している OSS では、開発者自身が公開した OSS の開発から離れている可能性もあり、脆弱性が発覚した場合でも迅速な対応が可能とは限らない。また、OSS の脆弱性が深刻で、連日迅速な対応が必要と考えられる場合であっても、OSS 開発者は日々OSS の開発のみを行っている訳ではないため、開発者数人ではリソースが不足し、修正パッチの公開や案内等に時間を要することがある。 ・ OSS を利用する際には OSS の開発体制を考慮しつつ、OSS 管理ソフトウェアを利用して、OSS に関する情報を把握することが必要。 ・ OSS 導入後に脆弱性有無や更新停止の発表等の情報を確認した場合、OSS 導入基準と同様に、OSS の利用停止基準や OSS 更新停止が発生した際の対応等を計画しておくことが良い。

3.2.2.2.1. インタビューから分かったこと

インタビューの結果、OSS に関するリスクやマネジメント方法について、以下のような指摘を得た。

- OSS はソースコードが公開されているため、ソフトウェア開発事業者が作成するソフトウェアに比べて多くの脆弱性が報告される傾向があるが、OSS そのもののセキュリティに関しては「セキュリティの専門家が確認」している場合もあり、OSS がインシデントの直接的な原因になった事例があまり見られない印象を持つ組織もいることから、等必ずしも発見された脆弱性の数とセキュリティレベルは比例しないと考えられる。

3.2.2.2.2. 今後深堀が必要なポイント

- 機能追加や脆弱性の修正等メンテナンスの継続性に関しては OSS 特有のリスクも存在する。特に、最終更新から期間が経過している OSS や少人数で開発している OSS では、脆弱性が発覚した際に速やかな対応が実施できるとは言い難い。また、OSS の開発・修正は基本的に無償で実施されるため、OSS 利用者からの度重なる修正依頼へ対応できるリソースやそれに見合った報酬が不足していることにより OSS の更新が停止される場合もあるなど、開発者起因のリスクは考慮が必要と言える。
- OSS 特有のリスクを低減するために、OSS の選定基準を設ける等組織的な取り組みも実施することが有効な可能性もうかがえる。インタビューを実施した SaaS 事業者では、OSS の更新頻度や情報公開状況を加味した選定に加え、各開発チームで OSS の利用に対する責任を徹底させる等 OSS に対するセキュリティ意識を根付かせている様子がうかがえた。選定基準の他に、OSS の脆弱性発覚や更新停止を事前に想定して OSS の利用停止基準を作成することや、一定程度セキュリティレベルが確保された OSS を利用することも取り組みの 1 つに挙げられており、様々なセキュリティ対策を実施する必要があると考えられる。

3.2.2.3. APIに対するセキュリティの評価について

OSS と同様、API の利用に関してもセキュリティ上どのようなリスクがあるかインタビューを実施した結果を図表 3-2-9 に示す。

図表 3-2-9：API に対するセキュリティの評価に関するインタビュー調査結果

回答	コメント内容
組織 B	・ クラウドサービス事業者が提供する API は、責任を取らない旨明記されていることもあるが、SaaS 事業者が API を利用する際にはどのようにリスク（脆弱性等）を管理、対応しているかについても情報があるとよい。また、SaaS 事業者が API を提供する際、考え得るリスクを低減するための API 設計における工夫についても情報があるとよい。
組織 E	・ クラウドサービスを利用する場合、API はどのサービスとも関連していると言えるが、API に対するセキュリティはある程度コントロール可能と考えられる。コントロールするためにはどの API が攻撃の起点にされ得るかをあらかじめ把握しておくことが必要になる。 ・ API を利用する際には、「認可を渡す範囲」や「認可をもってアクセスできる情報自体」等権限の設計が重要な観点である。 ・ API を取り扱う実行基盤に対しては攻撃を防ぐ方法はあるものの、WAF（Web Application Firewall）を追加で実装する等 SaaS 事業者側で対策を考え実行する必要がある。 ・ API のアクセスログ、トラフィックログに対しても監視する必要があるが、監視を実施している SaaS 事業者は多くない。

3.2.2.3.1. インタビューから分かったこと

インタビューの結果から、API については、「3.2.2.1. 考慮すべき脆弱性の発生箇所やインシデントパターンについて」の調査結果に含まれる「SaaS 連携」と大いに関連するポイントであるが、SaaS に限らずクラウドサービス全般において考慮が必要であることがうかがえた。API 利用時の認可の範囲や渡す情報自体を確認・設計しておくことに加えて、API 経由の攻撃等リスクを低減するためのサービス利用や API に関するログ監視を実施することによる対策の検討が必要と考えられるが、API 利用時の権限付与設計やリスクの管理方法については十分に情報が公開されていない状況も示唆された。

SaaS 連携による SaaS 利用者のニーズを満たした機能の提供及び SaaS・PaaS・IaaS 等の API を活用することによる開発の効率化等、API の利便性を安全に享受するためには、各 SaaS 事業者が、利用している API の数、関連するサービスの把握や API の利用規約に記載される責任範囲等の確認を実施し API に関するリスクをコントロールしていくことが必要と考えられる。

3.2.2.4. クラウドサービスの利用者に起因するインシデントについて

昨今指摘されるクラウドサービスの設定ミスといった、利用者に起因するリスクについてもインタビューを実施した。

図表 3-2-10：クラウドサービスの利用者に起因するインシデントに関するインタビュー調査結果

回答	コメント内容
組織 A	・ イギリスのリサーチ会社 Gartner 社も、「2025 年に向けて、99%のクラウドセキュリティインシデントは利用者のミスが原因になるだろう」と見解を述べており[41]、今後利用者起因のインシデントは増加することが考えられる。 ・ クラウドサービスの利用者側がセキュリティに関するプラクティスに準じていくことが求められてきているが、それはサービス提供者側のセキュリティレベルが向上してきたとも考えられる。なお、SaaS 事業者は、クラウドサービスの利用者であり、提供者でもあるため、セキュリティ対策状況が注目されている。
組織 B	・ SaaS 利用者側で発生したインシデントに関して、「SaaS 事業者側で配慮が足りなかった点等はどのあたりか」等利用者への対応については、団体に加盟している SaaS 事業者も注目している。
組織 E	・ クラウドサービス利用者の設定ミスは今後も注意する必要がある。OWASP TOP10:2021 では「アプリケーションの 90%には何らかの設定ミスが含まれる」として取り上げられており[42]、開発に関するすべてのサービスに精通することは不可能であることからも、SaaS 事業者が開発時に利用するクラウドサービスの設定ミスは十分に起こり得ると言える。また、SaaS 事業者は、クラウドサービス側が「クラウドサービス利用者の設定ミスへの対策や設定値自体に関する案内をしているか」等、クラウドサービス利用者に対する公開情報をクラウドサービス選定基準の一つとすることもリスクマネジメントとして有効と考えられる。

3.2.2.4.1. インタビューから分かったこと

インタビューの結果から、クラウドサービスにおける利用者起因のインシデントは、今後も考慮されるべきインシデントであることが示唆された。

設定ミスによってインシデントへ発展する可能性があり、多くの組織が注意を払うべきポイントでありなが

[41] Gartner (2019). “Is the Cloud Secure?”, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure, [参照 2022 年 2 月 18 日].

[42] Open Web Application Security Project (OWASP) (2021). “OWASP TOP10 A05:2021-Security Misconfiguration”, https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, [参照 2022 年 2 月 18 日].

ら、利用しているクラウドサービスの数によっては常に安全な設定をしておくことは容易ではないと考えられる。

設定ミスに関しては、CSPM （Cloud Security Posture Management）のような、クラウドサービスの設定ミス、構成の誤りや情報流出の検出等をサポートする製品を活用することも設定ミスを防ぐ方法の一つに挙げられるが、そうしたサービスを利用するためにも一定以上の知見が求められる。

3.2.2.4.2. 今後深堀が必要なポイント

利用者が設定ミスを犯しやすいポイントについては、あらかじめクラウドサービス事業者側でも案内が必要とも考えられていることがうかがえた。利用者側への配慮に注目している SaaS 事業者も存在しており、利用者に対する公開情報をクラウドサービス選定基準の一つとすることがリスクマネジメントとして有効と考えられる点からも、クラウドサービス利用者側だけでなくクラウドサービス事業者側も、利用時の設定値の把握・管理や設定に関する仕様そのものに対しても注意を払う必要性が示唆された。

3.2.3. 開発工程以外の課題やリスクに関するインタビュー結果

本項では SaaS の IT サプライチェーン上のリスクにおいて、開発工程以外の部分についての課題に関して、インタビューを実施した際に触れられた事柄を示す。

3.2.3.1. SaaS の可用性確保について

IT サプライチェーンのリスクとしては、サービスの提供に関わる可用性も重要な要素であるとインタビューの中では指摘を受けた。SaaS における可用性の確保の取り組みに関してインタビューでうかがえた内容を示す。

図表 3-2-11：SaaS の可用性確保に関するインタビュー調査結果

回答	コメント内容
組織 A	・ SaaS は常に利用者が存在しており、SaaS 利用者に対する SLA（Service Level Agreement：サービス品質保証）があるため、開発している SaaS 及び SaaS 事業者が利用する IaaS の SLA も考慮して、可用性に対するリスクマネジメントが必要になる。
組織 B	・ SaaS 事業者が自社の SaaS に対する可用性を確保する際には、利用する IaaS や PaaS の SLA に依存することに留意する必要がある。 ・ 大規模に利用されている IaaS 自体が止まった際、SaaS 自体が影響を受けることについては、SaaS 利用者との利用契約時に同意してもらう場合があるため大きな問題になることは多くない印象がある。
組織 C	・ 「SaaS 事業者が IaaS や PaaS を利用する際の可用性維持や可用性に関するリスク」については、オンプレミスソフトウェアを開発する際にデータセンターを利用する場合と同様の観点であると言える。

3.2.3.1.1. インタビューから分かったこと

インタビューの結果から、以下の事柄について示唆を得た。

- SaaS 事業者は SaaS の開発時に IaaS や PaaS 等クラウドサービスを利用する場面もあり、その際に IaaS や PaaS の SLA が自社で開発している SaaS の可用性に大きな影響を及ぼすことに留意が必要と考えられる。これは従来のオンプレミスソフトウェア開発におけるデータセンターの利用等と同様の観点であると言えるが、SaaS はオンプレミスソフトウェアに比べて利用者数が多く、国を跨いで異なる時間帯で利用されることも踏まえるとより広範囲に可用性を検討する必要があるとも言える。
- また、SaaS 事業者にとっては利用している IaaS や PaaS が停止した場合の自社で開発している SaaS への影響については事前に利用者との契約自に合意をし、SaaS が停止することによる影響以上に契約に関する大きな問題に発展しないようリスクをある程度コントロールすることも重要である。

3.2.3.2. 個人情報等機密データの保護について

個人情報といった重要情報の保護に関して、SaaS 開発に係るサプライチェーン上でどのような課題があるかインタビューを実施した結果を示す。

図表 3-2-12：個人情報等機密データの保護に関するインタビュー調査結果

回答	コメント内容
組織 A	・ IaaS 事業者と SaaS 事業者では個人情報の取扱いに対する立場表明が異なる場合がある。データ保護に関する法令の観点では、データを管理する者（Data Controller）が個人情報に関する責任を持つ。例えば GDPR（General Data Protection Regulation：EU 一般データ保護規則）では、多くの場合事業者側がデータを処理する者（Data Processor）になり、利用者側が Data Controller となる。IaaS 事業者は利用者のデータの中味については関与せずあくまでも IaaS の基盤に関するデータを扱うことを表明していることが多いが、SaaS 事業者は、サービスの特性上「利用者の個人情報を直接扱う」場合があり、事業者側だが Data Controller となり個人情報について責任を持つことがある。 ・ SaaS では、1 つのデータベースで複数の利用者情報を扱う場合があるため、確実にマルチテナント構成を取り、取り扱う複数の利用者情報が混在しないような配慮が必要。
組織 D（SaaS 事業者）	・ SaaS を日本以外の海外に展開する場合は、個人情報取扱関連の法令に関しては、各国の法令に対応する必要がある。 ・ SaaS のシステムアーキテクチャの変更までは迫られることはあまりないと考えられるが、各国の SaaS 利用者に対して、どの法令・基準に準拠しているか等は各国に応じて異なる示し方が必要である。
組織 E	・ SaaS 開発時に利用するクラウドストレージ上のデータは SaaS 事業者側で暗号化・復号可能であるが、暗号化を行わないことに問題意識が薄い SaaS 事業者も一部存在する。 ・ クラウドサービス上でデータを管理する場合、金融業界であれば FISC（The Center for Financial Industry Information Systems）安全基準に準拠する必要があり、データを暗号化した上で管理することが求められる等、クラウドサービス利用時に SaaS 事業者が担う責任が明確に基準として存在する業界もある。一方、監督省庁不在で事業をしている SaaS 事業者は、クラウドサービス上にデータがある場合であってもデータ管理の責任が SaaS 事業者側にあることを認識していない可能性がある。 ・ 個人情報保護の観点では、SaaS 事業者が個人情報にアクセス可能かどうかが重要な要素の一つとなる。アクセス可能な場合は特に、事業者側にデータ管理の責任があることを認識しておく必要がある。 ・ データ保護のプラクティスの一つに、「クラウドサービス上でデータを管理する際データの暗号鍵を含めた管理」（BYOK：Bring Your Own Key）がある。ただし、BYOK を謳っているサービスであっても、クラウドサービス事業者側で鍵の管理が不適切な場合は BYOK が成立しなくなり、データ自体に対する利用を制御することができなくなるので注意が必要。

3.2.3.2.1. インタビューから分かったこと

インタビューを通して、個人情報等の機密データの保護に関して主に「法令・認証規格への準拠」及び「データの暗号化」について下記のコメントを得た。

- クラウドサービス事業者が利用者の個人情報にアクセス可能な場合には、データ管理の責任があることを認識し、GDPR や個人情報保護法等の法令に関する解釈もあらかじめ確認しておくことが求められている。複数の国でサービスを展開する場合には、各国の法令に準拠した上で、各国の利用者に対する個人情報保護の姿勢や関連する法令・認証規格への準拠状況の公開が必要な場合もある。
- 利用者の個人情報にアクセスできないクラウドサービス事業者であっても、利用される業界で満たすべきとされるセキュリティ基準が設けられている場合もあり、クラウドストレージサービスに関わらず利用するクラウドサービス上に保存している機密データに対して暗号化を行う等、クラウドサービスを過信せずにセキュリティ対策を検討することが必要と言える。
- クラウドサービス上のデータは SaaS 事業者側で暗号化・復号化を実施可能な場合等、クラウドサービス利用時のリスクをある程度コントロール可能な場合がある。特に BYOK に対応しているクラウドサービスについては、暗号鍵自体を利用者側で保管可能であり、クラウドサービス利用者はクラウドサービス事業者自体が攻撃された場合の部分的なリスクヘッジを実施可能である。
- 法令・認証規格への準拠やデータの暗号化以外にも、個人情報保護のためには SaaS 自体の構成についても留意が必要であり、法令等準拠時に SaaS 自体の構成変更を求められる場面は多くないと考えられるが、複数の利用者にサービスを提供する際のマルチテナント構成を利用する際は「取り扱う複数の利用者情報が混在しないよう」に設計を検討・確認する必要がある。

3.2.3.2.2. 今後深堀が必要なポイント

個人情報の取扱いに対する立場表明について、「IaaS 事業者は IaaS 利用者が格納する情報について関知・管理しない立場をとる傾向があるが、SaaS 事業者は SaaS に格納される個人情報を管理しない表明をしがたい」という違いもうかがえた。SaaS 事業者の個人情報保護に対する姿勢や施策の積極性は今後も継続的に求められると言える。

3.2.3.3. クラウドサービス事業者のセキュリティに関する情報公開について

「1. 本調査の背景・目的」にもあるように、利用者は SaaS・クラウドサービスの選定にあたり、事業者の敷くセキュリティガバナンスを受け入れるケースが多い。本項では事業者によるセキュリティ取り組みの開示についてのインタビュー結果を示す。

図表 3-2-13：クラウドサービス事業者のセキュリティ情報公開に関するインタビュー調査結果

回答	コメント内容
組織 A	・ 日本では「セキュリティに関する情報を公開するとリスクが上がる」という考え方が主流のため公開されにくい現状がある一方、欧米ではセキュリティ対策自体がクラウドサービス事業者の差別化要因となっており、各クラウドサービス事業者は“セキュリティの透明性“をアピールしている。クラウドサービスの利用者としては、事業者がどのような開発を行っているかまで確認したいため、利用者に対して「開発におけるセキュリティレベルを確保するためのベースライン」、「ISO/IEC 27034 等開発手法に関する規格の取得状況」、「開発の考え方や、利用している製品群、開発手法」等開発に関する情報を公開することも重要であり日本においても更なるセキュリティ情報の透明性が求められる。

3.2.3.3.1. インタビューから分かったこと

セキュリティ対策や SaaS 事業者が抱える課題とは別に、クラウドサービス事業者として自社製品のセキュリティに関する情報公開についてもインタビューで指摘された。必要以上にセキュリティに関する情報を公開することはセキュリティ上のリスクが一部上がることに繋がるという考え方もあるが、既にサービスをグローバルに展開しているクラウドサービス事業者の公開状況を踏まえると、情報の公開は一定可能であると考えられる。

3.2.3.3.2. 今後深堀が必要なポイント

認証規格取得状況については日本でも多くの事業者が公開しているが、開発時に利用している製品群や開発におけるセキュリティのベースライン等の公開については普及していない状況がうかがえる。今後さらに SaaS を含め、クラウドサービスが増えていく中で、利用者がサービスを選定する際の参考となる情報を公開していくことは、事業者の姿勢として求められるべきことであり、そのような認識の醸成は業界の課題であろう。

3.2.3.4. SaaS とオンプレミスソフトウェアの違いについて

SaaS とオンプレミスソフトウェアを比較して、セキュリティ上の課題にどのような差異があるかをインタビューした結果を示す。

図表 3-2-14：SaaS とオンプレミスソフトウェアの違いに関するインタビュー調査結果

回答	コメント内容
組織 C	・ SaaS 自体が常にパブリックなインターネットに接続されているため、オンプレミスソフトウェアと比較して、SaaS に特有なインシデントの一例には「リモートコード実行」に関連するものが考えられる。ただし、オンプレミスであっても WAF が突破されることで、リモートコード実行等パブリックなインターネット上の攻撃を受ける可能性はある。 ・ SaaS 特有のリスクとしては、「SaaS はバージョンやカスタマイズ度合等ほぼ同様の仕様で提供されるため、SaaS に関連する脆弱性が発覚した場合は全ての利用者に影響が及ぶ」ことが挙げられる。一方、オンプレミスソフトウェアでは利用者ごとにネットワークの設定やセキュリティ対策が異なることが考えられるため、1 つの脆弱性が発見された際、必ずしもすべての利用者が影響を受けるとは限らない。 ・ 基本的に SaaS は利用者に対して同様の仕様で提供するため、SaaS 事業者側がアップデートを一斉に実行することができる点は SaaS 特有の利点と言える。オンプレミスソフトウェアでは利用者側で個別対応が必要なため、オンプレミスソフトウェアに広く影響を与える問題が発生した場合は、SaaS に比べて対応の時間を要すると考えられる。ただし、SaaS 事業者側は一斉に対応できる利点を活かすためにもどのコンポーネントにも脆弱性がある前提で利用し、脆弱性対応やインシデント発生時の対応体制を整えることが重要。 ・ アクセス状況やネットワークの死活監視等に関しては、SaaS 事業者側で監視機能を提供できるため、SaaS 利用者側でそれぞれ設定する手間が少ない点も SaaS の利点と言える。ただし、SaaS では監視等の設定をカスタマイズできる範囲に限りがある一方、オンプレミスソフトウェアの利用者側で監視設定等を高度にカスタマイズしている場合は、WAF の追加やアクセス権限設定の強化等 SaaS よりも詳細な監視ができることがある。

3.2.3.4.1. インタビューから分かったこと

インタビュー結果から以下の指摘・示唆を得た。

- 一点目の SaaS とオンプレミスソフトウェアの違いについては、オンプレミスソフトウェア開発であっても SaaS 開発時同様に OSS の利用や開発業務の委託を行う場合があり、その点では SaaS とオンプレミスソフトウェアの IT サプライチェーンにおけるリスクは同様のものも存在すると考えられるが、調査の結果、オンプレミスソフトウェアと比較して SaaS 特有に考慮すべき点は「常にパブリックなインターネットに接続されている」及び「同一の仕様で提供している」に関連することがうかがえた。ただしオンプレミスソフトウェアであってもリモートコード実行を含めて、パブリックなインターネット経由で攻撃されることがあるため、脅威として考慮は必要である。

- 二点目の SaaS とオンプレミスソフトウェアの違いについては、利用者に対して一斉にアップデートを実施可能か否かである。SaaS が利用者に対して同様の仕様で提供されることは、SaaS に関連する脆弱性が発覚した際の影響が即座にすべての利用者に及ぶ可能性があることを意味する。しかし、SaaS の場合は利用者に対して監視機能を一斉に提供することや、脆弱性や不具合が発覚した際にもアップデートを一度に実行することが可能であり、その点は SaaS の利点とも言える。一方、オンプレミスソフトウェアでは WAF の追加やアクセス権限設定の強化等ネットワーク設定、セキュリティ対策のカスタマイズが利用者ごとに可能な場合があり、利用するオンプレミスソフトウェアに関連した脆弱性が発覚した際、影響はすべての利用者に及ぶとは限らないが、オンプレミスソフトウェア事業者が利用者個別の状況への対応に迫られる可能性も示唆された。

利用者の立場ではこのような SaaS とオンプレミスソフトウェアの違いを踏まえて IT サプライチェーン上のリスクを把握すること、事業者の立場では、自社で開発するソフトウェアによって利用者への対応の仕方及び事前の対策に異なる点があることにも注意を払う必要があると考えられる。

3.2.4. その他得られた観点

本項では、IT サプライチェーンにおける SaaS 事業者が抱える課題や、考慮すべき脆弱性またはインシデントに関する調査結果とは別に、インタビュー調査で得られた今後 SaaS をはじめとするクラウドサービスのサプライチェーンを調査する上で検討すべき観点を記載した。

本調査開始時点では、SaaS を「B to B SaaS」[43]と「B to C SaaS」[44]で区別しなかったが、インタビューを行う中では「“SaaS“と聞いたときには B to B の SaaS を想起する」との回答もあった。

3.2.4.1. 「B to B SaaS」と「B to C SaaS」における違い

インタビューの中でうかがえた、B to B SaaS と C to C SaaS によるセキュリティの課題に関する差異となる事項を以下に示す。

[43] B to B SaaS：Business to Business の略称である B to B は、個人ではなく企業が企業に対してサービスやモノを提供するビジネスモデルのこと。B to B SaaS は、企業から企業に SaaS を提供するビジネスモデルを指すこともあるが、本調査では、「企業が『企業が利用することを想定して設計した』SaaS」を指す。

[44] B to C SaaS：Business to Consumer（または Customer）の略称である B to C は、企業がサービスやモノを直接個人（一般消費者）に提供するビジネスモデルのこと。B to C SaaS は、企業から個人に SaaS を提供するビジネスモデルを指すこともあるが、本調査では、「企業が『個人が利用することを想定して設計した』SaaS」を指す。

図表 3-2-15：「B to B SaaS」と「B to C SaaS」における違いに関するインタビュー調査結果

回答	コメント内容
組織 B	・ B to B SaaS では、利用者の機密情報の扱いに関しては、原則利用者側に責任がある旨利用規約上に記すことが多い印象がある。B to C SaaS も利用者の個人情報取扱いに関しては、利用者に責任がある旨利用規約上に記載しているものもあるが、個人情報流出等インシデントが発生した場合には、社会通念上 SaaS 事業者が責任を取る形で対応せざるを得ない場合がある。
組織 C	・ B to B と B to C では、SaaS の可用性維持に関する利用者への責任が異なり、インシデント発生時の対応も同様とは言い難い。例えば、B to B SaaS では、SaaS 利用者との個別の SLA 等可用性に関する契約をすることもあり、インシデントや脆弱性への対応を理由にサービス提供を一時停止することが困難な場合がある。B to C SaaS では、脆弱性対応等を理由にサービス提供を停止した際、比較的利用者側で大きな問題（特に経済的な問題）に発展することが少ないと考えられるため、メンテナンス等でサービスの一時停止を実施しやすい。
組織 D（SaaS 事業者）	・ B to B SaaS であっても B to C SaaS であっても、SaaS 事業者としては利用者への対応やサービス自体に対する責任に大きな違いはないと考えられる。自社では、利用者への個別の SLA とは異なる SLO（Service Level Objective）として可用性維持に関する表明を行っている。

3.2.4.1.1. インタビューから分かったこと

インタビュー結果からは、B to B SaaS と B to C SaaS では、「機密情報の取扱いに対する責任」や「メンテナンス時の対応」が異なることがうかがえた。B to B SaaS では個別の SLA に関する契約を行う場合もあり、その場合は、SLA で合意した可用性のレベルを下回らないように脆弱性対応等を実施することが求められると考えられる。一方 B to C SaaS では利用者と個別の SLA に関する契約を行わないことやサービスを一時停止した際に利用者が被る影響が B to B SaaS の場合ほど大きくないため、脆弱性対応等のメンテナンスを理由にサービスの一時停止を実施しやすいと言える。

また、B to B SaaS、B to C SaaS ともに利用規約上には個人情報等機密情報の取扱いについて責任の所在を明記しているが、B to C SaaS については情報漏洩等個人情報に関するインシデントが発生した場合、その取扱いについて事業者側が責任を取る対応をせざるを得ない場面があり、社会通念上も B to B SaaS と B to C SaaS に対して見方が異なることが示唆された。

しかし、インタビューを行った SaaS 事業者からは「B to B SaaS であっても B to C SaaS であっても、SaaS 事業者としては利用者への対応やサービス自体に対する責任に大きな違いはないと考えられる」とあることから、利用者のデータ保護のためにセキュリティ対策を可能な限り実現する等の基本的な姿勢が B to B SaaS と B to C SaaS で同様であることや、「3.2.1.3. インシデント発生時の対応・準備について」で述べられたインシデント発生時の「利用者からも受け入れられる対応」が B to C SaaS での実施内容に近い形で B to B SaaS でも広まりつつある可能性が考えられる。

4. 本調査のまとめ

本調査では、SaaS に係る IT サプライチェーンについて、事前に作成した SaaS 事業者が抱えるセキュリティ上の課題に関する想定に基づき、インシデント及び脆弱性情報を収集・整理した後、前述の想定課題、インシデント及び脆弱性情報調査の結果、さらに今後の SaaS のサプライチェーンにおけるセキュリティ上の課題として考えられることについて、5 つの組織にインタビューを実施した。

本章では、本調査で得られた、結果についてまとめた。

4.1. 想定した課題との違い

インタビューの結果、「1.5.SaaS 事業者が抱える課題の想定」と異なった点を示す。

- 開発時に機能開発が優先されセキュリティ対策が十分でないのではないか（図表 1-5-2 No.1、1-1、1-2、1-3）
  - 開発時のセキュリティの検討は十分検討を行っているものの、セキュリティに割くリソースの不足や、継続的なリリースの中で機能の複雑化に対応できず検討が不十分になる可能性などが指摘された。
- セキュアな監視ナレッジが十分でないのではないか（図表 1-5-2 No.2、 2-1、 2-2）
  - 課題案 2-1 や 2-2 のような情報収集の方法の課題よりも、監視対象である脆弱性情報が多く、それらを利用した攻撃の開始までの猶予が短くなってきているなど、環境の脅威が挙げられた。

4.2. 新たに指摘された課題

インタビューの結果、新たな課題として以下が挙げられた。

- SaaS 事業者側でのセキュアな実装や監視の実現方法についての情報の普及が不十分（3.2.1.2.）
- SaaS 開発時の SaaS 間の連携や SaaS 事業者側での API の利用時における API 提供側等事業者間の責任範囲の明確化（3.2.2.1.）
- SaaS 事業者側での OSS の脆弱性情報といった脅威の情報共有の体制強化や、そのためのツールの普及（3.2.2.2.）
- SaaS 利用者によるセキュリティ設定ミスに関して、SaaS 事業者から SaaS 利用者への安全な利用方法の周知と案内（3.2.2.4.）
- SaaS 事業者側での個人情報保護の方針を含めた、セキュリティ情報の開示の慣習の確立（3.2.3.2.及び 3.2.3.3.）

4.3. 団体・有識者の課題認識

インタビューをしていく中で様々な課題についての意見や指摘を得たが、インタビューを実施した団体・有識者が特に課題として認識していた事項について示す。

- 全体で見たセキュリティ体制の強化

  OSS の利用を例にとっても、脆弱性といった脅威のマネジメントが必要であるが、情報取得体制の構築や利用に関するルールの徹底が必要となり、事業者ごとの取り組みにばらつきが生じる。特に立ち上がり間もない事業者などはリソースに限りがあり懸念される。

- セキュリティノウハウの情報格差

  セキュアな実装や監視の具体的実現方法について、ノウハウや知見に関して SaaS 事業者の間で格差が生じている。

- セキュリティ情報開示の習慣

  日本においては SaaS 事業者自身が、自社のセキュリティについての取組について広く開示する習慣が根付いておらず、利用者に評価され辛く、競争優位としても認識されていない。

4.4. SaaS が抱える脅威・リスク

本調査の背景と目的で示したように、IT の調達は、SIer 等へのシステム開発の委託から SaaS を利用する形態がへと変わりつつある。こうした変化の中で、SaaS の開発における脅威やリスクだけでなく、これまで委託元が委託先に対して実施していたセキュリティに係る確認が SaaS を利用するようになったことで困難になり、SaaS 利用者が考慮すべき脅威・リスクが不明瞭なままであるという懸念がある。本章では、調査の結果から得られた SaaS が抱える脅威・リスクについて述べる。

調査の結果得られた脅威・リスクについて図表 4-4-1 に示す。

図表 4-4-1 調査の結果から得られた脅威とリスク

No.	脅威	リスク
1	セキュリティレベルを確保するための体制構築が難しい。	事業者によりセキュリティ対策のレベルにばらつきが発生する。
2	ガイドラインやプラクティスが公開されていても、どのように実現すればよいかわからず、正しく使われない。	脆弱な SaaS が開発されている可能性がある。
3	Secure Design のプラクティス等を参考にせず脆弱な実装をしている。	
4	SaaS に組み込んだソフトウェアの脆弱性に気付いていない。	
5	SaaS の機能や使い方が複雑になっている。	SaaS 利用者の設定ミスが発生する
6	SaaS 事業者は、サービスの特性上個人情報について責任を持つことがある。	SaaS 利用者と事業者の間の責任分界点が曖昧なまま契約している可能性がある。 SaaS 利用者がセキュリティ対策の状況を理解しないまま契約している可能性がある。
7	SaaS 利用者からは SaaS 事業者が利用している IaaS や PaaS および、それらの SLA 契約の内容を確認することができない。	

4.5. 今後深堀すべきポイント

本章では、インタビューから得られた「SaaS のサプライチェーンにおいて今後深堀すべきポイント」を、本調査で対象とした「開発」「監視」「対応」の工程に分けて整理した。総じて対応工程に多くのポイントが挙げられる結果となった。開発工程では OSS の利用やセキュアコーディングに関するポイントが挙げられた。監視・対応工程ではノウハウの普及や体制構築の強化、情報開示の拡充などのポイントが挙げられた。

開発・監視工程で挙げられたポイントは、ソフトウェアの開発においても当てはまるものであり、SaaS ならではのポイントとしては（図表 4-5-1 No. 9 から 11）、主に対応工程における個人情報保護の方針を含めた SaaS のセキュリティを保証する情報の開示や、セキュリティの高い状態で SaaS を利用してもらうための情報提供という結果が得られた。図表 4-6-1 に工程ごとの今後深堀すべきポイントを示す。

図表 4-5-1 今後深堀すべきポイント（工程ごと）

工程	No.	深堀すべきポイント
開発 監視 対応	1	SaaS 事業者の組織としてセキュリティ対策に注力するリソースの不足を、どのように改善させていくか。
開発	2	セキュリティプラクティスの実践における具体的な設計・実装についての情報の蓄積と蓄積された情報への SaaS 事業者間での共有。
	3	SaaS の設計開発におけるセキュアコーディングの実施をどのように推進していくか。
	4	SaaS 事業者が利用する OSS のメンテナー・開発体制の評価方法をどのように確立し、広めていくか。OSS 利用に先んじた上記評価の徹底について、どのようにして慣習化するか。
監視	5	SaaS 事業者の、脆弱性情報や攻撃に対する監視体制をどのように強化し、効率的な監視手法についての情報をどのように広めていくか。
対応	6	SaaS 事業者内での、インシデント対応手順作成や問い合わせ先の整理、顧客説明といった平時の準備にどのようなことが必要か。
	7	SaaS 連携における事業者間での責任範囲の明確化をどのように推進していくか。
	8	利用者に起因するインシデントを防止するため、SaaS 事業者は利用者に向けてどのような情報を提供していくべきか。
	9	個人情報管理に関するセキュリティ対策への積極的な姿勢・SaaS 事業者としての立場の明確化といった文化・慣習をどのように形成し、維持していくか。
	10	利用者が安心してクラウドサービス を利用できるようにするために、SaaS 事業者はセキュリティ情報をどこまで開示するべきか。
	11	SaaS 業界を挙げたセキュリティ情報の開示をどのように促進していくか。

本調査では、様々な観点で SaaS のサプライチェーンにおける課題や今後深堀すべきポイントを得る事

ができた。その中でも、開発工程におけるセキュリティプラクティスの実践に係る情報共有やセキュアコーディングの推進、OSS の利用に係る評価体制などについては SaaS ならではのポイントでなく、ソフトウェア開発全般にも当てはまる内容であると言える。よって、SaaS ならではのポイントと言える、個人情報保護の方針を含めた SaaS のセキュリティを保証する情報の実態や、セキュリティの高い状態で SaaS を利用してもらうための情報提供の実態について調査することで SaaS のサプライチェーンのリスクマネジメントを深堀りしていく必要があると考えられる。

以上