2021年度
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
概要説明資料

2022年5月　1.1版

独立行政法人　情報処理推進機構
セキュリティセンター
セキュリティ対策推進部
分析グループ

目次

1 調査実施概要

背景・目的
調査概要
課題の想定

2 調査結果

インシデント及び脆弱性情報の調査結果
インタビュー調査結果
今後深堀すべきポイント

1　調査実施概要

背景と目的

背景

トレンドの変化(オンプレミスからクラウドへ)

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。

ニューノーマルへの対応にはクラウドが必須

新型コロナウイルスの感染防止対策や働き方改革の手段の一つとしてテレワークが定着したことによるニューノーマルでの企業活動にはコミュニケーションの活性化や作業の効率化においてクラウドサービスの利用が必須である。

クラウドサービスが抱える課題

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・管理のリスクといったセキュリティ上の懸念が生じるなど）

目的

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、ITサプライチェーンのリスクマネジメントの向上に資するため、以下を明らかにする。

- SaaSのサプライチェーンには**どのような脅威やリスク**があるのか
- SaaSのサプライチェーンにおける**今後の課題**
- 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**

調査概要（全体の流れ）

本調査では、インシデントおよび脆弱性情報の調査とインタビュー調査を実施した結果を分析し、SaaSのサプライチェーンにおける脅威・リスク、今後深堀すべきポイントについてとりまとめた。

①インシデントおよび脆弱性情報の調査	②課題案 インタビュー項目の作成	③インタビュー調査	④とりまとめ
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および脆弱性の情報を収集、整理。 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	ソフトウェア開発ライフサイクルを参考にSaaSのサプライチェーンに関して課題案を作成 課題案と整理したインシデントおよび脆弱性の情報からインタビュー項目を作成	②で作成したインタビュー項目に対して、SaaSにかかわる組織および有識者へのインタビューを実施	③で実施したインタビュー結果からSaaSのサプライチェーンにおける脅威・リスク、今後深堀すべきポイントについて整理

調査概要(インシデント及び脆弱性情報の調査)

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情報（原因、影響範囲など）の収集と整理**を実施した。

また、収集したインシデント情報のうち、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(3件）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などを示した**インシデント概要図を作成**した。

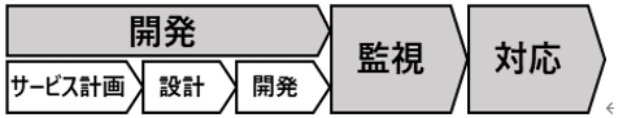
項目	概要
収集と整理をしたインシデントおよび脆弱性の条件	・SaaSの開発・運用に関連し、SaaS事業者またはSaaS利用者に影響があると考えられるもの ・SaaSの開発・運用に関して業務委託を行っている場合は、SaaS事業者に影響を及ぼす「委託先で発生したインシデント」や「委託先で利用するソフトウェア等に関する脆弱性」についても調査対象とした ・SaaS利用時の設定ミス等、SaaS利用者に起因するインシデント ・日本国内に限らず海外のインシデントも対象とした
収集方法	書籍、ニュース等公開情報（同一のインシデントまたは脆弱性によって複数企業が影響を受けた場合、当該インシデントまたは脆弱性を1件としている。）
収集項目	インシデントor脆弱性の分類・発見場所・公表年・発見の経緯・区分・原因 被害内容・対応内容・再発防止策
収集期間	2020年4月～2021年9月末に公表されたもの

課題案

本調査の範囲をSaaSソフトウェアの開発工程や運用におけるセキュリティの取り組み状況も対象としたことから、ソフトウェア開発ライフサイクルの考え方を参考に「開発」「監視」「対応」の3つのフェーズに分けて、**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想定されるSaaS事業者が抱える課題案を立案**した。

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、対応の工程では脆弱性対応やセキュリティインシデントの対応を考慮した。

本調査で対象とした工程



SaaS事業者が抱える課題の想定

工程	課題案		
開発	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	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	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

調査概要(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、リスクなどの実態を把握し、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して、今後深堀すべきポイントを明らかにするため、インタビュー調査を実施した。

項目	概要
インタビュー調査をした組織の選定条件	以下のいずれかに該当する組織を対象として選定 ・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 ・2019年10月から2021年9月の間に 　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組織 　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組織 ・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組織
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を実施 総対象者数　：13名
調査内容	インシデント及び脆弱性情報の調査で得られた分析結果および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想定される課題案に対して、以下の見解を得る。 ・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 ・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

2 調査結果

インシデント及び脆弱性情報の調査結果(1/2)

収集したインシデントおよび脆弱性情報

57件（インシデント：37件　脆弱性情報：20件）の情報を収集し、整理した。P11参照

収集したインシデント情報の中から３件の概要図を作成

＜マッチングアプリサービス「Omiai」への不正アクセスによる情報漏えい＞ P13参照

株式会社ネットマーケティングが提供するマッチングアプリサービスの「Omiai」が不正アクセスされ、年齢確認データ約171万件が漏えいした。

＜テストカバレッジツール「Codecov」のスクリプト改ざんによる情報漏えい＞ P14参照

Codecov社が自社のSaaSのスクリプトを改ざんされ、ツール利用者の開発環境の情報が攻撃者へ漏えいし、漏えいした情報を悪用された。

＜ネットワーク管理・監視製品「Orion Platform」からの情報漏えい＞

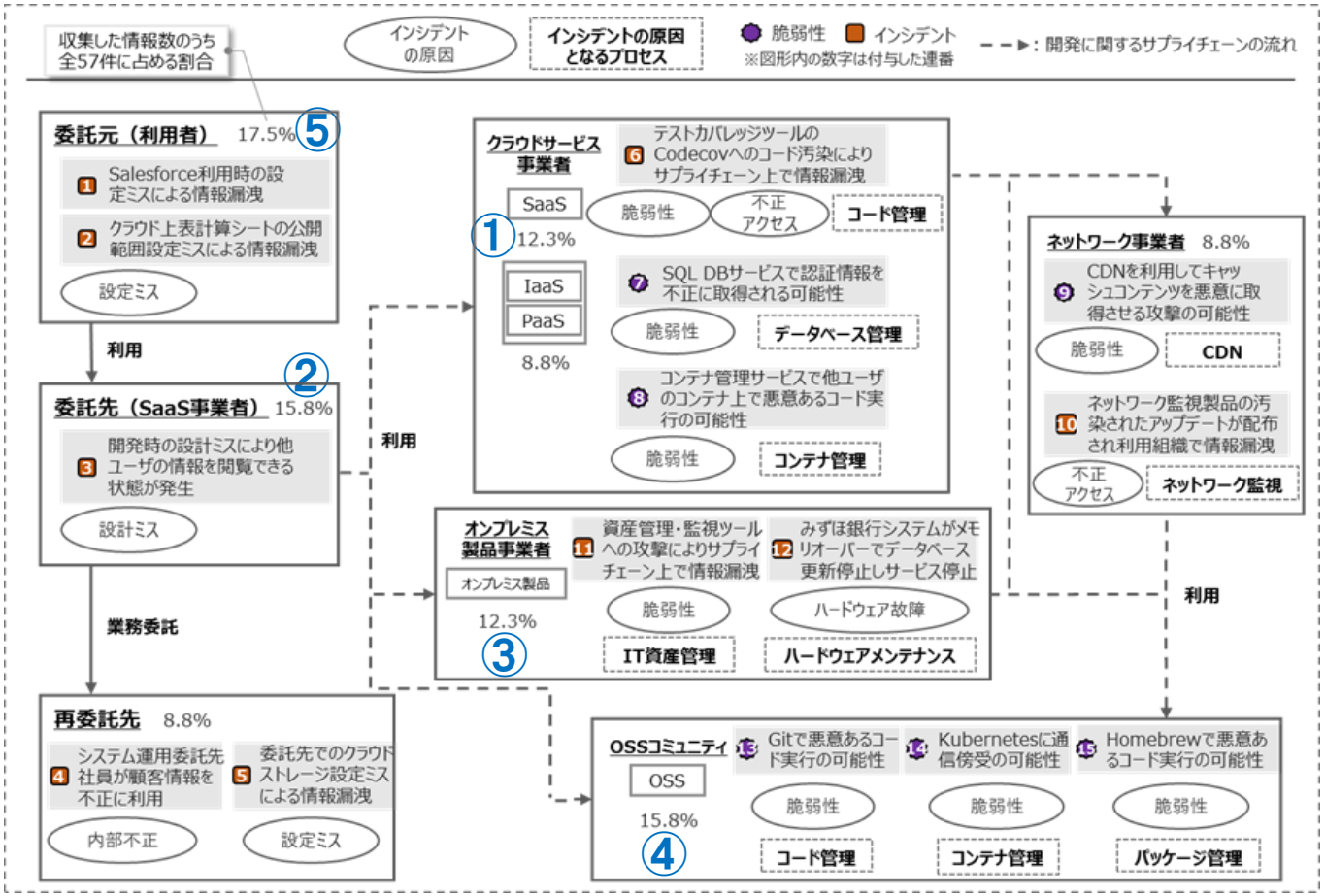
SolarWinds社の「Orion Platform」の開発工程でマルウェアに感染し、バックドアがしこまれた。バックドアを含んだVersionにUpdateしたOrionPlatformの利用組織から機密情報が漏えいした。

収集したインシデント及び脆弱性情報の整理から示唆されたこと

- IaaS、PaaS、ネットワーク事業者などと比較すると、SaaSやオンプレミス製品、OSSにおいてインシデントや脆弱性が発生する割合が高く、インシデントに発展するリスクが高いと考えられる。
- SaaS利用者による設定ミスなどが原因のインシデントが多く発生。SaaS事業者から利用者に対して、設定時に留意すべき箇所や設定値等を通知することで、利用者による設定ミスの低減につながる可能性が考えられる。

インシデント及び脆弱性情報の調査結果(２/2)

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



以下２点が示唆された

①②③④から
IaaS、PaaS、ネットワーク事者と比較すると、SaaSやオンプレミス製品、OSSに関連したインシデントや脆弱性が発生する割合が高い。
SaaSやOSSなどの方がインシデントに発展するリスクが高いと考えられる。

⑤から
委託元（利用者）による設定ミスなどが原因で発生するインシデントが最も多い結果(17.5%)となった。
SaaS事業者から利用者に対して、設定時に留意すべき箇所や設定値等を通知することで、利用者による設定ミスが低減する可能性が考えられる。

「インシデントの原因となるプロセス」は、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、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。

インシデント一覧（一例）

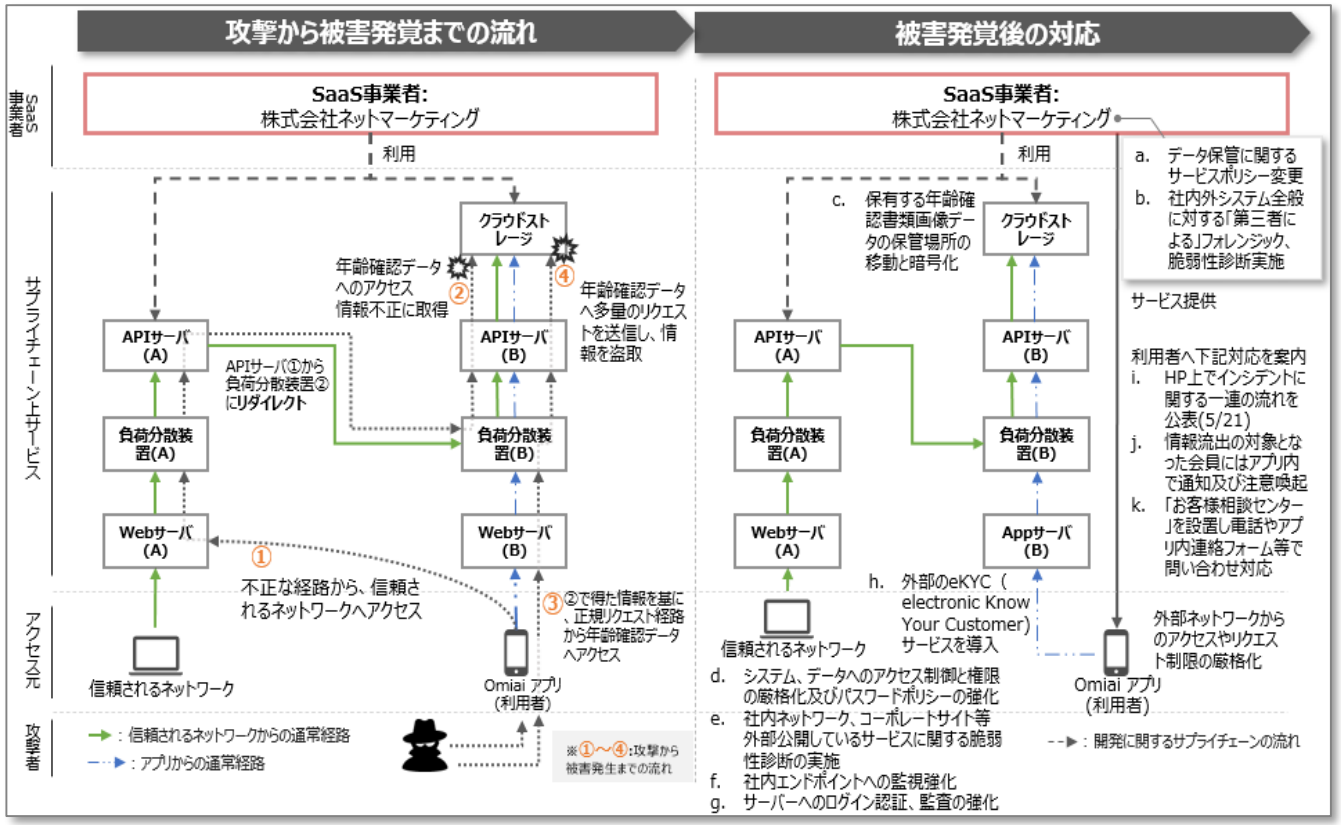
インシデント一覧には以下に示す項目を整理した。

分類	発生箇所	概要	公開年	発覚の経緯	原因	被害内容	対応内容	再発防止策
インシデント	SaaS事業者	システム更新時のプログラム破損により、クラウドシステムに障害が発生した。	2021	システム更新作業後、翌営業日の業務が不可となったことで発覚。	システム更新作業時のミスにより更新ファイルが破損、破損したファイルがクラウド環境に配布・自動適用され、障害が発生した。	システムを利用する百数十の団体で書類の印刷や発行ができなかった。	—	システム更新作業に関する管理手順等の見直しや社員教育を徹底した。
脆弱性	SaaS	メールアプリの脆弱性を悪用し、標的型攻撃が実施された。	2020	米国のサイバーセキュリティ関連企業がデジタルフォレンジック、及びインシデントレスポンスの調査を通じて脆弱性を発見した。	・nmapの脆弱性 ・MIMEのライブラリであるMFMutableの脆弱性	脆弱性の標的となった企業は数社。 メーカーは顧客へ損害を与えるため悪用された形跡は見つかっていないとしている。	修正アップデートを配布。	—

公開情報から確認できなかった場合は「－」としている。

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が提供するマッチングアプリサービスの「Omiai」で情報漏えい



インシデント概要

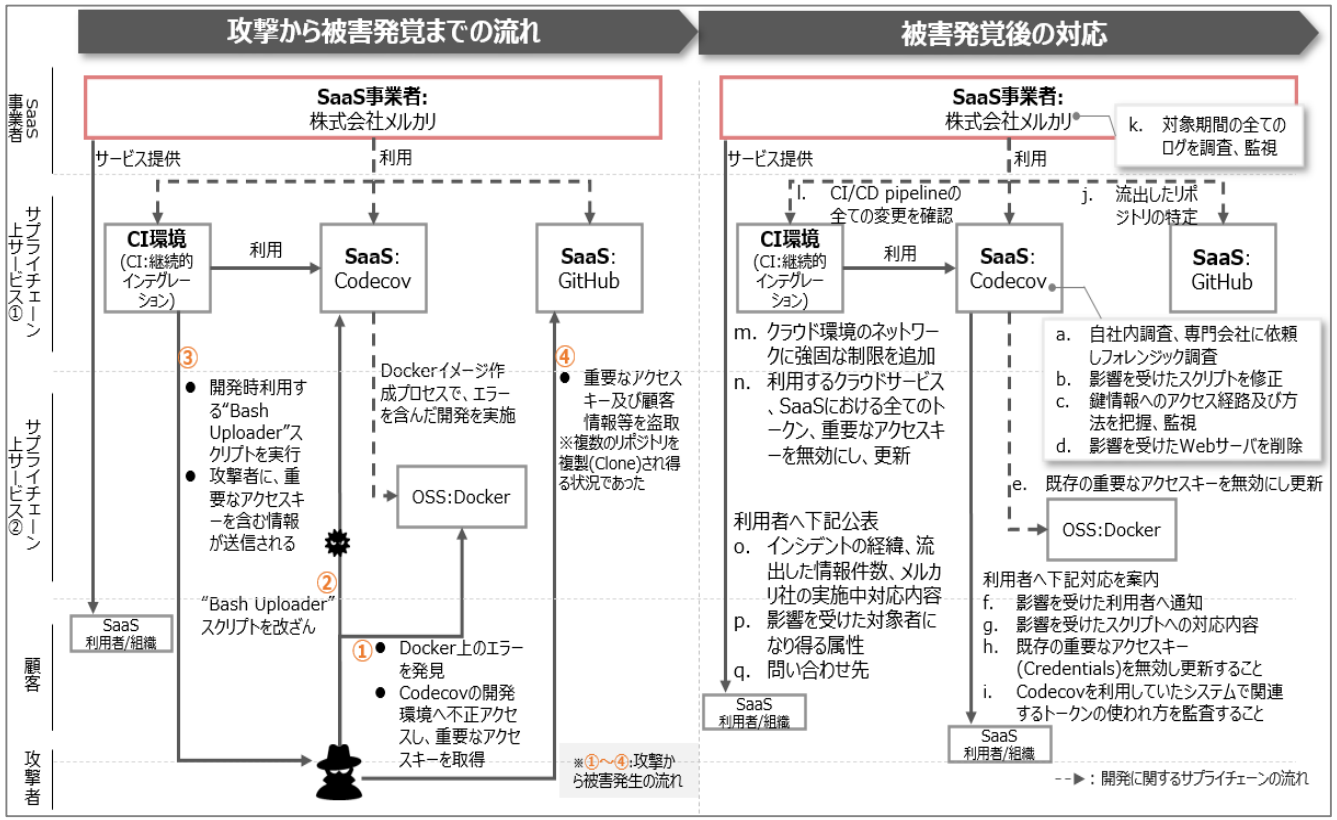
不正な経路から信頼されるネットワークを通じて、年齢確認データが保存されているストレージへのアクセス情報が盗取された。当該アクセス情報をもって正規のリクエストを多量に送信して不正アクセスが行われ、年齢確認データ約171万件が漏えいした。

インシデント発生の原因

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原因は公表されていない。

Codecov社に係るインシデントの概要図

テストカバレッジツール「Codecov」のスクリプトが改ざんされて利用者から情報漏えい



インシデント概要

Codecov社が利用するコンテナ環境が不正アクセスされ、開発時に利用する"Bash Uploader"スクリプトが改ざんされた。
改ざんされた"Bash Uploader"スクリプトを利用した株式会社メルカリから認証情報などが搾取され、コードを管理していたGitHubに不正アクセスされ、顧客・取引先・従業員情報等約29,000件の情報が漏えいした 。

インシデントの原因

Codecov社が利用していたコンテナ管理サービス「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 。

インタビュー調査結果

想定した課題との違い（インタビューの結果、支持されなかった課題案）

開発時のセキュリティ検討が十分でない

概ね支持されなかった。

「セキュリティに割くリソースの不足」「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。

セキュリティの監視ナレッジが十分でない

概ね支持されたが、情報収集の方法よりも「監視対象である脆弱性情報の量が多い」やそれらを利用した「攻撃の開始までの猶予が短くなる」など、環境の脅威が挙げられた。

新たに指摘された課題（インタビューを通して得られた課題）

④⑤はSaaSならではの課題、①②③は開発にもあてはまる課題

①SaaS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

②SaaS間連携などにおけるAPI提供事業者間の責任範囲の明確化

③脅威情報(OSSの脆弱性情報など)共有の体制強化やそのためのツールの普及

④個人情報保護の方針を含めたセキュリティ情報(*1)の開示の慣習の確立

⑤SaaS利用者への安全な利用方法(*2)の周知と案内(SaaS利用者のセキュリティ設定ミスへの対策)

(*1) SaaSのセキュリティを保証する情報
たとえば「SaaS事業者の開発におけるセキュリティの対策内容」「利用している製品」「連携している組織」「認証取得情報」など

(*2)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
たとえば「セキュリティにおけるSaaS事業者と利用者の責任分界点」「セキュアな設定方法」など

今後深堀すべきポイント

インタビューの結果からえられたこと

- 総じて**対応工程に多くのポイント**が挙げられた。
- 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**ものであった。
- SaaSならではのポイントは主に対応工程における**「セキュリティ情報の開示」**や**「セキュリティ情報の提供」**という結果が得られた。（SaaSならではのポイントに★印を付与）

工程	今後深堀すべきポイント
全工程共通	・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	・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をどのように実施していくか。 ・セキュリティプラクティスの実践に関して蓄積された情報へのSaaS事業者間での共有をどのように向上させていくか。 ・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。 ・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	・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ていくか ・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	・インシデント発生時に必要となる対応内容（技術的内容だけでなく問い合わせ先の整理、顧客への対応など） ★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。 ★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。 ★個人情報管理に関するSaaS事業者としての施策をどのように実施していくべきか。 ★利用者が安心してクラウドービス 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。 ★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。

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 改訂理由　調査報告書改訂に伴う修正。 改訂箇所　P10,11　数値の修正。 P12　収集項目（表頭）の修正。