海外のクラウドサービス評価制度の実施状況調査

成果説明用資料

株式会社野村総合研究所

2024年3月21日

NRI

Share the Next Values!

目次構成

海外のクラウドサービス評価制度の実施状況調査の概要

【目次】

１．海外のクラウドサービス評価制度の実施状況調査の概要

２．各調査の状況報告

調査の背景と目的

■背景

- 政府は、2018年6月に、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成30年6月7日 各府省情報化統括責任者（CIO）連絡会議決定）を定め、その中で政府情報システムを整備する際に、クラウドサービスの利用を第一候補とする「クラウド・バイ・デフォルト原則」を掲げている。
- これを受けて、2020年6月に、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度である、「政府情報システムのためのセキュリティ評価制度（以下、「ISMAP」とする。）」の運用が開始されている。これにより、以降の政府情報システムの調達については、原則、ISMAPクラウドサービスリストに登録されたクラウドサービスから調達することとなっている。
- ISMAPは、運用開始から3年を経過し、運用を通じた課題も明らかになってきており、ISMAPの信頼性・安定性の保持を前提としつつ、制度運用の合理化・明確化といった観点からの制度見直しに向けた検討が、制度所管省庁や、ISMAP運用支援機関である独立行政法人情報処理推進機構（以下、「IPA」という。）によって進められているところである。

■目的

- このような背景のもと、グローバルの観点からISMAPを客観的に検証するため、海外の類似制度について調査・比較し、基礎的（定点観測）な情報を整理するとともに、ISMAPの改善に向けた重点課題であるクラウドサービスを取り巻くセキュリティインシデントについて、インシデント予防・対応、供給者管理に関わる規程類等の調査・比較を行い、制度見直しに向けた検討に資することを目的として、本調査を執り行う。

全体概要

■ 全体概要

- (1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）
  - 海外の類似制度である、アメリカ（FedRAMP）、イギリス（G-Cloud）、ドイツ（C5）、オーストラリア（IRAP）を調査対象とする。
  - このうち、アメリカ（FedRAMP）、イギリス（G-Cloud）、ドイツ（C5）においては、IPAが2020年～2022年度に実施した過去の調査結果からの情報の更新を行うため、直近の制度の状況変化に関する動向調査を実施する。他方、オーストラリア（IRAP）においては、制度の概要、規程類、認証プロセス、監査体制に関する基礎調査や、直近の制度の状況変化に関する動向調査を実施する。
  - 上記の調査結果をもとに、IPAから提示されたこれまでの調査結果を記載した「別紙1_海外諸制度調査表.xlsx」を更新するとともに、各制度の特徴や制度課題に対する取り組み状況、最新動向について分析を行い、分析結果をもとにISMAPの改善に向けた提言を作成する。
- (2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）
  - 海外の類似制度である、アメリカ（FedRAMP）、イギリス（G-Cloud）、ドイツ（C5）、オーストラリア（IRAP）を調査対象とする。
  - インシデント事例調査として、国内外のインシデント件数や情勢、国内外のクラウドサービスインシデントに関する事例について調査してまとめる。 また、インシデント制度調査として、調査対象制度におけるインシデント予防・対応、供給者管理に関わる規程およびガイドライン、管理策の記述内容について調査・比較を行うとともに、ISMAPで検討が必要な考え方や項目について分析を行う。

１．海外のクラウドサービス評価制度の実施状況調査の概要

２．各調査の状況報告

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ The Federal Risk and Authorization Management Program（FedRAMP）

- 直近のFedRAMPにおいては、以下に示すような状況変化が見られた。

直近の制度の状況変化	概要
覚書M21-31や覚書M22-09に対応した要件の追加	● FedRAMPの認定を受けたCSOのクラウドサービスにおいて覚書M21-31の要件に準拠した実装を可能とするため、「FedRAMP Security Controls Baseline」で提供されている管理策の一部に覚書M21-31の要件を反映し、CSOに対してその遵守を求めている。 ● 覚書M22-09においては、サイバー脅威に対する政府の防御力を強化するため、各政府機関に対して、2024年度末までに特定のサイバーセキュリティ基準と目標を達成することを求めており、その中でCISAに対しては、FedRAMPと協力して、暗号化された電子メール（転送中の電子メール）に対する政府全体で実行可能なソリューションについて評価するともに、評価結果をもとにOMBに対する推奨事項を作成し、今後、政府全体がとるべき措置を通知するための勧告をOMBに提出することを求めている。
FedRAMP Security Controls Baselineの改訂	● NIST SP800-53が、2020年9月23日にRev.4からRev.5に改訂されたことを受けて、GSAは、2023年5月30日にRev.5を反映した「FedRAMP Security Controls Baseline」の改訂を行っている。 ● その後、GSAは、NIST SP800-53のRev.5への改訂や「FedRAMP Security Controls Baseline」の改訂に伴い、同様の改訂を関連するテンプレート及びガイダンスに対しても行っている。
3PAO Obligations and Performance Guideの改訂	● 3PAOがクラウドサービスのセキュリティ評価を実施する際に必要となる品質や独立性、FedRAMPの知識取得を保証するためのガイダンスとして、GSAが提供する「3PAO Obligations and Performance」において、評価者（職員）の経験、トレーニング、資格取得及び熟練した技術を身に付ける活動に関する基準が新たに追加されている。

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ The Federal Risk and Authorization Management Program（FedRAMP）（前ページからの続き）

直近の制度の状況変化	概要
FedRAMP Collaborative ConMon Quick Guide	● GSAは、「FedRAMP Continuous Monitoring Performance Management Guide」のContinuous Monitoringに関わるセキュリティ管理策（CA-7）において、協調的なContinuous Monitoringのアプローチを実装することを求めている。 ● GSAは、CSPが活用可能な協調的なContinuous Monitoringのフレームワークを提供するガイドとして、2023年8月30日に「FedRAMP Collaborative ConMon Quick Guide」を公表している。
FedRAMP Incident Communications Proceduresの改訂	● GSAは、2021年4月14日に、インシデントコミュニケーションプロセスにおける、FedRAMPの関係者が果たすべき役割とその責任や、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）が発令する緊急指令に対する対応について反映した「FedRAMP Incident Communications Procedures」の改訂を行っている。 ● その中で、FedRAMPのJAB P-ATOまたはAgency ATOの承認を受けたCSPに対して、クラウドサービスやクラウドサービスが保存、処理、送信するデータやメタデータの機密性、完全性、可用性が損なわれ、実際の損失や潜在的な損失がもたらされたと疑われるインシデントや実際に確認されたインシデントについて、インシデントの影響を受ける、または影響を受ける可能性のある顧客（省庁）やUS-CERT、CSPのFedRAMP連絡窓口であるFedRAMP POC、JAB POCといった関係者に対して、インシデントが特定されてから1時間以内に報告することを義務付けている。

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ G-Cloud

- 直近のG-Cloudにおいては、以下に示すような状況変化が見られた。

直近の制度の状況変化	概要
Digital Marketplaceの使用不能とそれに代わるPublic Procurement Gatewayの運営開始	● 政府のデジタル調達に関するステートメントである「Digital Outcomes & Specialists 6」に基づきコールオフ契約が締結された政府機関が購入可能なクラウドホスティング、クラウドソフトウェア、クラウドサポート等のクラウドサービスについては、Digital Marketplaceを使用して調達することができなくなっている。 ● Digital Marketplaceが使用不能になったことに伴い、2023年4月20日より、それに代わる政府のデジタル調達のための新たな手段として、Public Procurement GatewayがThe Crown Commercial Service により運営されている。

■ C5

- C5の公式ホームページ上において特段、制度の状況変化は見られなかった。

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ Inforsec Registered Assessors Program（IRAP）

- IRAPにおける制度の概要、規程類、承認（認証）プロセス、評価（監査）体制、直近の制度の状況変化について、以下に示す。

項目	概要
制度の概要	● IRAPは、組織がセキュリティ評価を受けた高品質のサービスにアクセスできるようにすることを目的として、オーストラリア政府の信号局（Australian Signals Directorate、以下ASDという。）が提供する登録セキュリティ評価者プログラムである。 ● ASDは、IRAPを通じて、ICTシステムやクラウドサービス、ゲートウェイ、ゲートキーパー、FedLinkに対するセキュリティ評価と、IRAP評価者向けのトレーニングをサポートしている。IRAP自体は、クラウドサービスに特化したプログラムではない。
規程類	● IRAPにおいては、以下に示す規程類が存在する。 • IRAPのメンバーシップの条件やメンバーシップを維持するための要件、メンバーシップを取り消す条件、IRAP管理者の責任について規定した「IRAPポリシーと手順（IRAP Policy and Procedures）」 • 政府機関やCSP、IRAP評価者等が、CSPと提供するクラウドサービスの包括的な評価を行う際の方法論を示したクラウドセキュリティガイダンス • IRAP評価者が行うクラウドサービスに対するセキュリティ評価の対象となる管理策を規定した「情報セキュリティマニュアル（Information Security Manual）」 • 政府機関の安全保障に関わる機密情報を保持またはアクセスする非政府組織に適用されるフレームワークを提供する「保護セキュリティポリシーフレームワーク（Protective Security Policy Framework）」 ● クラウドセキュリティガイダンスには、クラウドサービスの評価と承認に関するガイダンス、クラウドサービスの評価と承認に関するよくある質問、クラウドサービスのセキュリティ評価レポートのテンプレート（Cloud Security Assessment Report Template）、クラウドコントロールマトリックス（Cloud Controls Matrix、以下CCMという。）のテンプレートが含まれている。

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ Inforsec Registered Assessors Program（IRAP）（前ページからの続き）

項目	概要
承認（認証）プロセス	● IRAP評価者の承認を受けようと考えている申請者（以下、スターターという。）は、申請時において、以下に示す要件を満たすことが求められる。 • オーストラリア国民であること • 少なくとも2年間のASDが提供するISM及び関連ドキュメントを使用してシステムを保護した情報セキュリティ経験を含め、少なくとも5年間の技術面のICT経験を有すること • ASDが指定するICT資格を保有していること • ASDが指定する監査資格を保有していること • ASDが承認したIRAPトレーニングプロバイダーが提供するIRAP評価者の新しいスターター向けトレーニングコース（5日間）を修了していること、かつASDの新しいスターター向けIRAP評価者試験に合格していること
評価（監査）体制	● クラウドサービスのセキュリティ評価には、Phase1（1a、1b、1c）、Phase2（2a、2b）、Phase3の手順が規定されている。 ● Phase 1aでは、IRAP評価者がCSP自体のセキュリティ基礎（セキュリティ対策、サイバーセキュリティ体制、ガバナンス体制、管理環境、サポート環境、クラウド基盤）を評価し、CSPの組織が安全に機能し、安全なクラウドサービスを開発しているかどうか、またクラウドサービスの利用者データを安全に処理するのに適しているかどうかを判断する。IRAP評価者は、評価結果、セキュリティ管理策の有効性を確認するための証拠、推奨される修復措置を、クラウドセキュリティ評価レポートテンプレートを用いて文書化する。 ● Phase 1bでは、組織がCSPのクラウドサービスを利用する際に、以下に示すような状況が発生した場合にのみ、IRAP評価者または当該組織によるクラウドサービスのセキュリティ評価が必要になる。 • 利用するクラウドサービスがCSPのクラウドセキュリティ評価レポートの対象外であった場合 • CSPが、クラウドセキュリティ評価レポートの完成後に新しいクラウドサービスをリリースした場合 • CSPが、クラウドセキュリティ評価レポートに記載されているクラウドサービスに対して、セキュリティに影響を与える大幅な変更を加えた場合

(1)クラウドサービス評価に係る海外諸制度の基礎調査及び動向調査（定点観測）

■ Inforsec Registered Assessors Program（IRAP）（前ページからの続き）

項目	概要
評価（監査）体制（前ページからの続き）	● Phase 1cでは、CSPのクラウドサービスを利用する組織が、Phase 1aで作成されたクラウドセキュリティ評価レポートや、必要に応じてPhase 1bで補足されたクラウドサービスレポートを確認して、CSPとそのクラウドサービスが当該組織のセキュリティ要件とリスク許容度を満たしているかどうかを判断する。 ● Phase 2aでは、CSPのクラウドサービスを利用する組織が開発したクラウドシステムが、当該組織のセキュリティ要件とリスク許容度を満たしていることを確認するために評価を行う。 ● Phase 2bでは、CSPのクラウドサービスを利用する組織の承認担当者（またはその代理人）が、CSPとそのクラウドサービス、自社のクラウドシステムで構成されるクラウド環境の運用が承認される前に、クラウド承認パッケージに含まれる情報をレビューして、当該クラウド環境が当該組織のセキュリティ要件を満たし、リスク許容度を超えていないかどうかを判断する。 ● Phase 3では、CSPとCSPのクラウドサービスを利用する組織が、進化するサイバーセキュリティリスク、脆弱性、脅威、管理策、インシデントを継続的に監視して認識し、これらの変化に対する継続的なセキュリティ評価を実行する。 ● ASDは、IRAP評価者が行うクラウドサービスのセキュリティ評価の品質を保証するため、IRAP評価者またはセキュリティ評価レポートの所有者をサンプル抽出し、セキュリティ評価レポートとその証跡の提出を要求するとともに、レビューを行っている。
直近の制度の状況変化	● ASDは、元々クラウドサービスの認証機関として、IRAPとクラウドサービス認定プログラム（Cloud Services Certification Program、以下CSCPという。）の2つのプログラムを提供し、認定したクラウドサービスを、認定クラウドサービスリスト（Certified Cloud Services List、以下CCSL）に登録していたが、その後、2020年3月2日にCSCPを終了し、更に同年7月27日にCCSLを廃止している。 ● これにより、ASDはクラウドサービスの認証機関ではなくなるとともに、これを受けて、「IRAPポリシーと手順（IRAP Policy and Procedures）」の更新や、新しいIRAP評価者向けのトレーニングのリリースを行っている。

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント事例調査

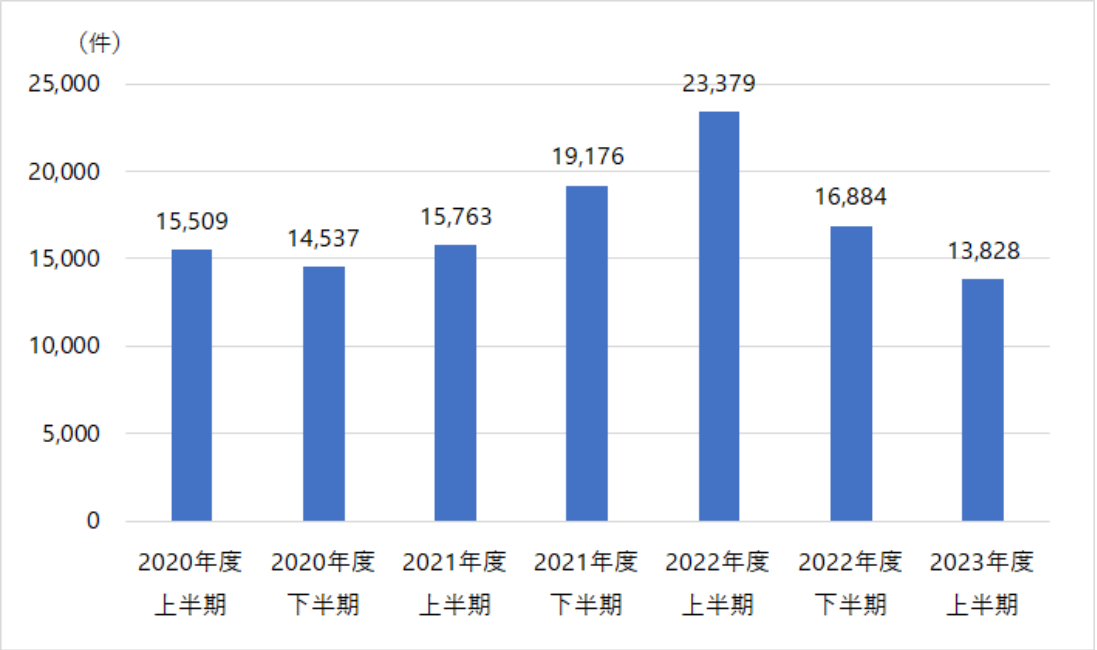
- 国内のインシデントの情勢について、IPAが毎年公表している「情報セキュリティ10大脅威」についてみると、国内の組織で発生しているインシデントのうち、上位を占め、社会的に大きな影響を及ぼしているものは、「ランサムウェアによる被害」、「サプライチェーンの弱点を悪用した攻撃の高まり」、「標的型攻撃による機密情報の窃取」である。
- 国内のインシデント事例件数について、直近にJPCERTコーディネーションセンターが報告を受けたインシデントについてみると、同一インシデントの重複分を除いたインシデント件数は、2022年度上期の23,379件をピークにその後減少に転じており、2023年度上期には13,828件にまで減少している。

情報セキュリティ10大脅威（組織を対象、上位5位）

	1位	2位	3位	4位	5位
2019年	標的型攻撃による被害	ビジネスメール詐欺による被害	ランサムウェアによる被害	サプライチェーンの弱点を悪用した攻撃の高まり	内部不正による情報漏えい
2020年	標的型攻撃による機密情報の窃取	内部不正による情報漏えい	ビジネスメール詐欺による金銭被害	サプライチェーンの弱点を悪用した攻撃	ランサムウェアによる被害
2021年	ランサムウェアによる被害	標的型攻撃による機密情報の窃取	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	ビジネスメール詐欺による金銭被害
2022年	ランサムウェアによる被害	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい
2023年	ランサムウェアによる被害	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃

(出所)情報セキュリティ10大脅威2019～2023（IPA）を基に作成

インシデント件数の推移



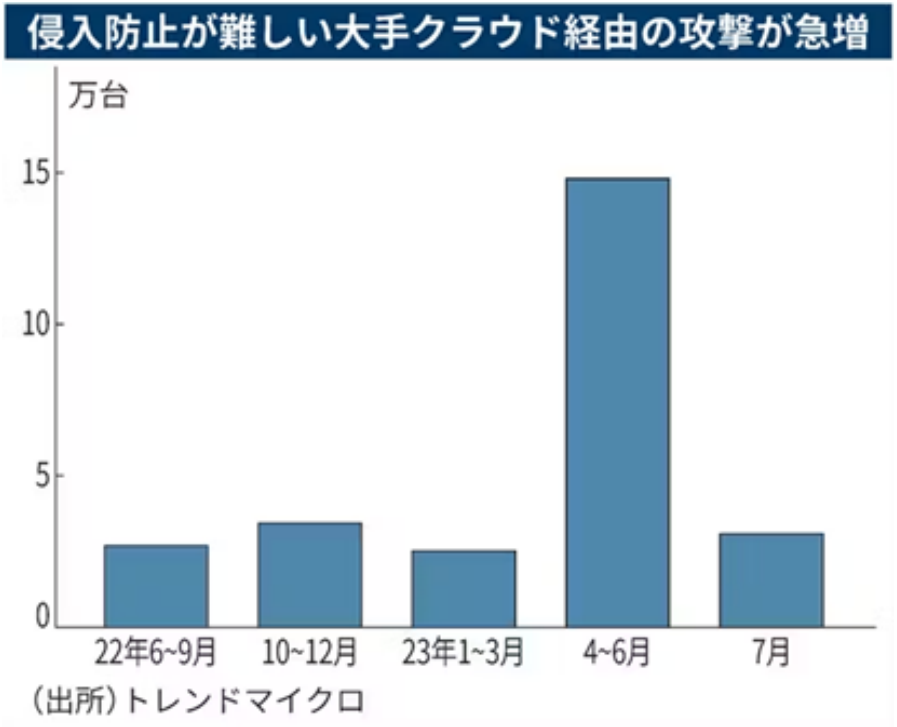
(出所)JPCERT/CC インシデント報告対応レポートを基に作成

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント事例調査（前ページからの続き）

- クラウドサービスに関わるインシデントについて、トレンドマイクロが過去1年間の顧客データを解析した結果についてみると、大手クラウドサービスプロバイダーが提供するクラウドサービスを悪用したサイバー攻撃の被害が増えており、2023年4月～6月には同攻撃による影響を受けたパソコン等の端末の被害台数は、延べ14万8千台に上っている。
- 直前の2023年1月～3月の端末の被害台数が2万5千台であったため、約6倍に急増しており、攻撃者がサイバー攻撃の手口として、侵入検知が難しいクラウドサービスの悪用を本格化させつつある状況が伺える。

大手クラウドサービスを悪用したサイバー攻撃による影響を受けた端末の被害台数の推移

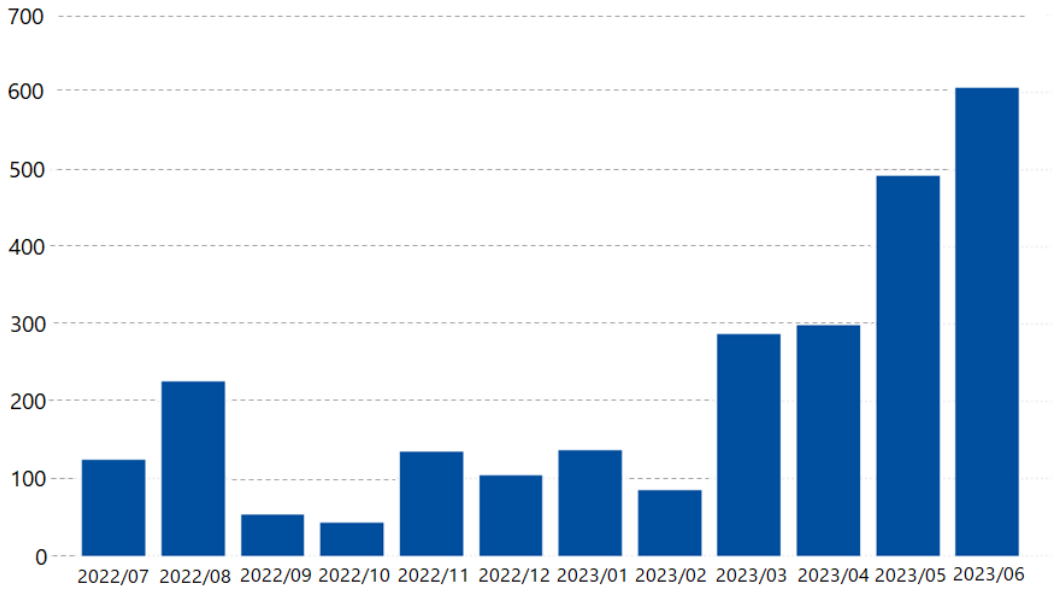


(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント事例調査（前ページからの続き）

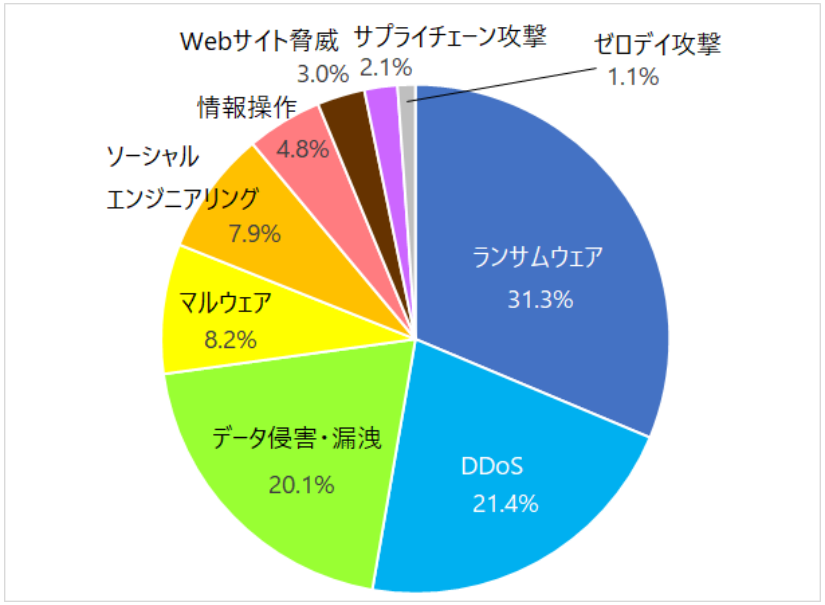
- 海外のインシデントの情勢について、EU加盟国からインシデントの報告を受けている欧州ネットワーク・情報セキュリティ機関（以下、ENISAという。）が毎年公表する「ENISA THREAT LANDSCAPE 2023」についてみると、2022 年 7 月から 2023 年 6 月までの間に報告されたインシデントの脅威タイプの内訳についてみると、ランサムウェアが最も多く、全体の31.3％を占めている。また、次いで多いのは、DDoSの21.4％、データ侵害・漏洩の20.1％の順となっている。
- 海外のインシデント事例件数について、「ENISA THREAT LANDSCAPE 2023」についてみると、EU内におけるインシデントの発生状況を捉えると、2023年6月のEU内におけるインシデント報告件数は約600件であり、2023年に入ってからインシデント報告件数が急増している。

EU内におけるインシデント報告件数（月次）



(出所)ENISA THREAT LANDSCAPE 2023（OCTOBER 2023, ENISA）

EU内において報告されたインシデントの脅威タイプ別内訳



(出所)ENISA THREAT LANDSCAPE 2023（OCTOBER 2023, ENISA）

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査

- FedRAMPにおいては、インシデント予防、対応に関する規程およびガイドラインとして、GSAが提供する「FedRAMP Security Controls Baseline」において、RA（リスクアセメント）ファミリーの一部として、脆弱性の監視及びスキャンに関する管理策が、また、IR（インシデント対応）ファミリーの一部として、インシデント対応に関する管理策が示されている。

○脆弱性の監視及びスキャンに関する管理策
- RA-5 脆弱性の監視及びスキャン
- RA-5 (2) スキャンする脆弱性の更新
- RA-5 (3) カバレッジの幅及び深さ
- RA-5 (4) 検出可能な情報
- RA-5 (5) 特権アクセス
- RA-5 (8) 過去の監査ログのレビュー
- RA-5 (11) 公開開示プログラム

○インシデント対応に関する管理策
- IR-1 ポリシー及び手順
- IR-2 インシデント対応トレーニング
- IR-2 (1) シミュレーションイベント
- IR-2 (2) 自動化されたトレーニング環境
- IR-3 インシデント対応テスト
- IR-3 (2) 関連計画との調整
- IR-4 インシデント対応
- IR-4 (1) 自動化されたインシデント対応プロセス
- IR-4 (2) 動的再構成
- IR-4 (4) 情報の相互関連付け
- IR-4 (6) インサイダー脅威
- IR-4 (11) 統合インシデント対応チーム
- IR-5 インシデント監視
- IR-5 (1) 自動化された追跡、データ収集及び分析
- IR-6 インシデント報告
- IR-6 (1) 自動化された報告
- IR-6 (3) サプライチェーンとの連携
- IR-7 インシデント対応支援
- IR-7 (1) 情報及びサポートの可用性のための自動化されたサポート
- IR-8 インシデント対応計画
- IR-9 情報流出対応
- IR-9 (2) トレーニング
- IR-9 (3) 流出後の運用
- IR-9 (4) 認可されていない職員への露出

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査（前ページからの続き）

- FedRAMPにおいては、供給者管理に関する規程およびガイドラインとして、GSAが提供する「FedRAMP Security Controls Baseline」において、SA（システム及びサービスの取得）ファミリーの一部として、外部システムサービスに関する管理策が示されている。加えて、SR（サプライチェーンのリスクマネジメント）ファミリーの一部として、サプライチェーンのリスクマネジメントに関する管理策が示されている。

○外部システムサービスに関する管理策
- SA-9 外部システムサービス
- SA-9 (1) リスクアセスメント及び組織承認
- SA-9 (2) 機能、ポート、プロトコル及びサービスの特定
- SA-9 (5) 処理、保管及びサービスの場所

○サプライチェーンのリスクマネジメントに関する管理策
- SR-1 ポリシー及び手順
- SR-2 サプライチェーンのリスクマネジメント計画
- SR-2 (1) サプライチェーンリスクマネジメント（SCRM）チームの設立
- SR-3 サプライチェーンの管理策及びプロセス
- SR-5 取得戦略、ツール、及び方法
- SR-6 サプライヤーのアセスメント及びレビュー
- SR-8 通知協定
- SR-9 耐タンパー性及び検知
- SR-9 (1) システム開発ライフサイクルの複数の段階
- SR-10 システムまたはコンポーネントの検査
- SR-11 コンポーネントの真正性
- SR-11 (1) 偽造防止トレーニング
- SR-11 (2) コンポーネントのサービス及び修理のための構成管理
- SR-12 コンポーネントの廃棄

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査（前ページからの続き）

- G-Cloudにおいては、インシデント予防、対応に関する規程およびガイドラインとして、英国国家サイバーセキュリティセンター（National Cyber Security Centre、以下NCSCという。）が提供する「Cloud Security　Guidance」において、クラウドセキュリティ原則（The cloud security principles）が示されており、原則5：運用のセキュリティの一要素として、脆弱性管理、インシデント管理に関する目標や推奨される実装アプローチが、また原則13：監査情報と顧客への警告として、同原則の目標や推奨される実装アプローチが規定されている。
- また、供給者管理に関する規程およびガイドラインとして、「Cloud Security　Guidance」において、原則8：サプライチェーンのセキュリティとして、同原則の目標や推奨される実装アプローチが規定されている。

○脆弱性管理に関する推奨される実装アプローチ
- ・脅威の監視
- ・脆弱性管理プロセス
- ・緩和策を適用するためのタイムスケール

○インシデント管理に関する推奨される実装アプローチ
- ・ISO/IEC 27035-1:2016、CSA CCM v3.0.1、ISO/IEC 27001:2013 などのインシデント管理に関する標準規格を参照しつつ、自ら選択した目標に基づいて認定を受けることができる。

○監査情報に関する推奨される実装アプローチ
- ・監査情報を攻撃がいつ、どのように発生したか、及びその攻撃の影響を特定するためのフォレンジック調査で主に使用する。
- ・その他にも、データ形式、記録される情報、基盤サービスから取得されるログ、監査情報の保護が含まれる。

○セキュリティ警告に関する推奨される実装アプローチ
- ・ニーズを満たす形式（自動分析用の構造化された機械可読形式、運用担当者用のテキスト形式を含む）を使用して、セキュリティアラートを迅速に配信する。
- ・配信するさまざまな種類のアラートを文書化し、実際のインシデントを待たずにアラート通知の処理を定期的に確認できるよう、アラート通知を模擬的に実践することができる手段を提供する。

○サプライチェーンのセキュリティに関する推奨される実装アプローチ
- ・クラウドサービスの多くがサードパーティのIaaS製品またはPaaS製品の上に構築されている中で、どのセキュリティ機能の実装をどの当事者が担当するかを特定する。
- ・その他にも、分離、機密データ、データ共有が含まれる。

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査（前ページからの続き）

- C5においては、インシデント予防、対応に関する規程およびガイドラインとして、ドイツ情報セキュリティ庁（Federal Office for Information Security、以下BSIという。）が提供する「Cloud Computing Compliance Criteria Catalogue - C5:2020」において、運用に関する基準が提供されており、その1つのパートとして脆弱性、誤動作及びエラーの管理に関する基準（基本的な基準、追加の基準、補完的な顧客基準）や、セキュリティインシデント管理に関する基準（基本的な基準、追加の基準、補完的な顧客基準）が規定されている。
- また、供給者管理に関する規程およびガイドラインとして、「Cloud Computing Compliance Criteria Catalogue - C5:2020」において、サービスプロバイダー及びサプライヤーの管理及び監視に関する基準（基本的な基準、追加の基準、補完的な顧客基準）が規定されている。

○脆弱性、誤動作及びエラーの管理に関する基準
- OPS-18 脆弱性、誤動作及びエラーの管理 – コンセプト
- OPS-19 脆弱性、誤動作及びエラーの管理 – 侵入テスト
- OPS-20 脆弱性、誤動作及びエラーの管理 – 測定、分析及び評価手順
- OPS-21 インシデント発生時におけるクラウドサービスの顧客の関与
- OPS-22 既知の脆弱性に対するテスト及び文書化
- OPS-23 脆弱性、誤動作及びエラーの管理 – システムの強化

○サービスプロバイダー及びサプライヤーの管理及び監視に関する基準
- SSO-01 サードパーティを管理及び監視するためのポリシー及び指示
- SSO-02 サービスプロバイダー及びサプライヤーのリスク評価
- SSO-03 サービスプロバイダー及びサプライヤーの登録台帳
- SSO-04 要件に準拠しているかどうかの監視
- SSO-05 ベネフィットを得るための出口戦略

○セキュリティインシデント管理に関する基準
- SIM-01 セキュリティインシデント管理ポリシー
- SIM-02 セキュリティインシデントの処理
- SIM-03 セキュリティインシデントの文書化及び報告
- SIM-04 セキュリティインシデントを中央の対応組織に報告するユーザーの義務
- SIM-05 評価及び学習のプロセス

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査（前ページからの続き）

- IRAPにおいては、インシデント予防、対応に関する規程およびガイドラインとして、ASDが提供する情報セキュリティマニュアル（Information Security Manual）において、システム管理に関するガイドラインが提供されており、その中の1つのパートとして、システムのパッチ適用に関する管理策が規定されている。また、サイバーセキュリティインシデントに関するガイドラインが提供されており、同ガイドラインは、「サイバーセキュリティインシデントの管理」と「サイバーセキュリティインシデント対応」の2つのパートで構成されている。

〇システムのパッチ適用に関する管理策
- ・パッチ管理プロセス及び手順
- ・ソフトウェアレジスタ
- ・不足しているパッチまたはアップデートのスキャン
- ・脆弱性にパッチを適用するタイミング
- ・サポートの終了

〇サイバーセキュリティインシデント対応に関する管理策
- ・サイバーセキュリティインシデント対応計画の策定
- ・データ流出に対する処理及び封じ込め
- ・悪意あるコードの感染に対する処理及び封じ込め
- ・システム侵入に対する処理及び封じ込め
- ・証跡の完全性の維持

〇サイバーセキュリティインシデントの管理に関する管理策
- ・サイバーセキュリティインシデント管理ポリシー
- ・サイバーセキュリティインシデント登録台帳
- ・信頼できるインサイダープログラム
- ・十分なデータソース及びツールへのアクセス
- ・サイバーセキュリティインシデントの報告
- ・ASDに対するサイバーセキュリティインシデントの報告
- ・顧客及び一般の人々に対するサイバーセキュリティインシデントの報告

(2)海外クラウドサービス認証制度におけるインシデント対応の調査（重点課題）

■ インシデント制度調査（前ページからの続き）

- 供給者管理に関する規程およびガイドラインとして、調達及び外部委託に関するガイドラインが提供されており、同ガイドラインは、「サイバーサプライチェーンのリスク管理」と「マネージドサービス及びクラウドサービス」の2つのパートで構成されている。

○サイバーサプライチェーンのリスク管理に関する管理策
- ・サイバーサプライチェーンのリスク管理活動
- ・供給者関係の管理
- ・アプリケーション、ICT機器及びサービスの調達
- ・アプリケーション、ICT機器及びサービスの提供

○マネージドサービス及びクラウドサービスに関する管理策
- ・マネージドサービス
- ・マネージドサービスプロバイダーの評価
- ・外部委託されたクラウドサービス
- ・外部委託されたクラウドサービスプロバイダーの評価
- ・サービスプロバイダーとの契約上のセキュリティ要件
- ・サービスプロバイダーによるシステム及びデータへのアクセス


Share the Next Values!