クラウドインシデントレスポンス（CIR）フレームワーク

cloud security alliance®

The permanent and official location for the Cloud Incident Response Working Group is https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/.

Acknowledgments

Lead Authors:

Soon Tein Lim
Alex Siow
Ricci Ieong
Michael Roza
Saan Vandendriessche

CSA Global Staff:

Hing-Yan Lee
Ekta Mishra
Haojie Zhuang
AnnMarie Ulskey (cover design)

Special Thanks:

Bowen Close

Key Contributors:

Aristide Bouix
David Chong
David Cowen
Karen Gispanski
Dennis Holstein
Christopher Hughes
Ashish Kurmi
Larry Marks
Abhishek Pradhan Michael Roza
Ashish Vashishtha

Reviewers:

Oscar Monge España
Nirenj George
Tanner Jamison
Chelsea Joyce
Vani Murthy
Sandeep Singh
Fadi Sodah

About the Cloud Incident Response Working Group (WG)

With today's emerging and rapidly evolving threat landscape, a holistic cloud incident response framework that considers an expansive scope of factors for cloud outages is necessary. The Cloud Incident Response (CIR) Working Group (WG) aims to develop a holistic CIR framework that comprehensively covers fundamental causes of cloud incidents (both security and non-security related) and their handling and mitigation strategies. The aim is to serve as a go-to guide for cloud users to effectively prepare their detailed plan to respond and manage the aftermath of cloud incidents. The CIR is also a transparent and common framework for cloud service providers to share their cloud incident response practices with cloud customers. This framework's development includes imperative factors of cloud incidents such as operational mistakes, infrastructure or system failure, environmental issues, cybersecurity incidents, and malicious acts.

日本語版提供に際しての告知及び注意事項

本書「クラウドインシデントレスポンス（CIR）フレームワーク」は、Cloud Security Alliance（CSA)が公開している「Cloud Incident Response(CIR) Framework」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2021 年 06 月 03 日	日本語版 1.0	初版発行

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定
　CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限
　本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
　ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等

本書が Cloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「クラウドインシデントレスポンス（CIR）フレームワーク」は、CSA ジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

上田　将司　CISSP, 情報処理安全確保支援士
小野　貴博
昆　　資之
塩田　英二
神保　冬和子
高瀬　一彰
高橋　久緒
鶴田　浩司
福井　将樹
松浦　一郎　CISSP, CISM, CDPSE
三浦　貢造
満田　淳
諸角　昌宏
山澤　昌夫
渡邉　浩一郎　CISA,CISSP

目次

1. はじめに

今日のコネクテッド時代において、包括的なインシデントレスポンス戦略は、リスクプロファイルの管理と低減を目指す組織にとって不可欠な要素です。しっかりとしたインシデントレスポンス計画を持たない多くの組織や企業は、クラウドインシデントに初めて遭遇したときに、唐突に気づかされます。重大なダウンタイムは、自然災害、ヒューマンエラー、もしくはサイバー攻撃など、様々な理由で発生します。優れたインシデントレスポンス計画によって、組織はいつでも十分な体制で臨むことができます。しかし、クラウドベースのインフラストラクチャやシステムのインシデントレスポンス戦略に関しては、その責任共有の性質もあり、多くの検討事項があります。[1]

インシデントレスポンスのフレームワークは、従来のオンプレミス型の情報技術（IT）環境を対象とした「*NIST 800-61r2 Computer Security Incident Handling Guide*」や「*SANS Institute Information Security Reading Room Incident Handler's Handbook*」など、多くの政府機関や業界のガイドラインで既に文書化されています。しかし、クラウドコンピューティング環境が関わる場合は、様々なクラウドサービスモデルや配備モデルに対して、従来のインシデントレスポンスフレームワークで定義されていた役割と責任を、クラウドサービスプロバイダ（CSP）とクラウドサービスカスタマ（CSC）の役割と責任に合わせて、修正および改良する必要があります。

本書の目的

本書は、クラウドインシデントレスポンス（CIR）のフレームワークの提供を目的としています。これは、CSC が、破壊的なイベントのライフサイクル全体を通して、クラウドインシデントに対して効果的に備え、管理するための指針として役立ちます。また、CSP がクラウドのインシデンスレスポンスの手法を CSC と共有するための透明性のある共通フレームワークとしても役立ちます。

対象読者

主な対象は CSC です。本フレームワークは、CSC が自らの組織のセキュリティ要件を把握し、適切なレベルのインシデント保護を選択するための指針を提供します。これにより、CSC は CSP と交渉でき、あるいは対策済みのセキュリティ機能を選択でき、セキュリティの役割と責任の境界を明確に理解することができます。

2. 規範となる文献

本 CIR フレームワークは、クラウドインシデント、緩和するための戦略、および事後分析を計画・準備するため、業界で受け入れられているいくつかの標準やフレームワークを参照しています。

[1] Cloud Security Alliance, Cloud Incident Response, https://cloudsecurityalliance.org/research/ working-groups/cloud-incident-response/

- CSA Security Guidance For Critical Areas of Focus In Cloud Computing v4.0
  （訳注：「クラウドコンピューティングのためのセキュリティガイダンス v4. 0」として日本語版公開）
- NIST 800-61r2 Computer Security Incident Handling Guide
- ITSC Technical Reference (TR) 62 – Cloud Outage Incident Response (COIR)
- FedRAMP Incident Communications Procedure
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
- SANS Institute Information Security Reading Room Incident Handler's Handbook
- ENISA Cloud Computing Risk Assessment

図 1 は、CIR の各フェーズと主な参考文献の関係を表しています。

Phase 5.1 Preparation	Phase 5.2 Detection and Analysis	Phase 5.3 Containment, Eradication and Recovery	Phase 5.4 Postmortem
CSA Sec. Guidance v4.0 9.1.2.1 Preparation	**CSA Sec. Guidance v4.0** 9.1.2.2 Detection and Analysis	**CSA Sec. Guidance v4.0** 9.1.2.3 Containment, Eradication, and Recovery	**CSA Sec. Guidance v4.0** 9.1.2.4 Postmortem
NIST 800-61r2 3.1 Preparation	**NIST 800-61r2** 3.2 Detection and Analysis	**NIST 800-61r2** 3.3 Containment, Eradication, and Recovery	**NIST 800-61r2** 3.4 Post-Incident Activity
TR 62 0.1 Cloud Outage Risks	**TR 62** 4.2 COIR Categories 5.1 Before Cloud Outage: CSC 6.1 Before Cloud Outage: CSP	**TR 62** 5.2 During Outage: CSC 6.2 During Outage: CSP	**TR 62** 5.3 After Outage: CSC 6.3 After Outage: CSP
FedRAMP Incident Comm. Procedure 5.1 Preparation	**FedRAMP Incident Comm. Procedure** 5.2 Detection and Analysis	**FedRAMP Incident Comm. Procedure** 5.3 Containment, Eradication, and Recovery	**FedRAMP Incident Comm. Procedure** Post-Incident Activity
NIST (SP) 800-53 r4 3.1 Selecting Security Control Baselines Appendix F-IR IR-1, 1R-2, 1R-3, IR-8	**NIST (SP) 800-53 r4** Appendix F-IR AT-2, 1R-4, IR-6, 1R-7, IR-9, SC-5, SI-4	**NIST (SP) 800-53 r4** Appendix F-IR 1R-4, IR-6, IR-7, IR-9	**Incident Handlers Handbook** 7 Lessons Learned 8 Checklist
Incident Handlers Handbook 2 Preparation 8 Checklist	**Incident Handlers Handbook** 3 Identification 8 Checklist	**Incident Handlers Handbook** 4 Containment 5 Eradication 6 Recovery 8 Checklist	
ENISA Cloud Computing Security Risk Assessment Business Continuity Management, page 79			

図 1: インシデントライフサイクルと規範となる文献

3. 定義

- 資産: 資産とは、どのような物でも、組織にとって価値を持つ物のこと。資産には、抽象的な資産（プロセスや評判等）、仮想的な資産（データ等）、物理的な資産（ケーブルや機器等）、人的資源、金銭等があります。[2]
- インシデント：ネットワークや情報システムのコアサービスの運用に支障をきたす課題のこと。
- 報告義務のあるインシデント：法令や規制に基づき、社外に報告する必要があるほど重大な影響を与えると判断されるインシデントのこと。
- インシデントハンドリング[3]:セキュリティプラクティスや推奨されるプラクティスに対し違反となる課題/インシデントに対処するための是正措置のこと。
- インシデントレスポンス計画:組織がインシデントの準備、検知、分析、および復旧を行う際に役立つ明確な手順のこと。
- インシデントの報告：報告当事者（クラウドプロバイダまたはクラウド事業者）が、アドホックに、インシデントに関する情報を記載した報告書を、国の管轄当局に提出する手順のこと。
- インパクト：1 件のインシデントが解決するまでに起こりうる被害の大きさを示す指標のこと。
- 根本原因：インシデントを引き起こした理由（究極的な根本原因）のこと。（根本原因分析では、複数の「原因と結果」を特定できますが、根本的な原因は 1 つになるでしょう）。
- 脅威：脅威とは、情報システムに対し破壊、漏えい、有害なデータの改変、サービス妨害などの被害を与える可能性をもつ状況や事象のこと。[4]
- 脆弱性：特定のシステム、モジュール、またはコンポーネントの欠陥や弱点で、攻撃や災害、または他の原因により侵害されやすい状態にするもの。

4. CIR の概要

CIR は、クラウド環境でのサイバー攻撃に対処するために設計されたプロセスとして定義され、次の 4 つのフェーズで構成されます。

- フェーズ 1：準備
- フェーズ 2：検知と分析
- フェーズ 3：封じ込め、根絶、および復旧
- フェーズ 4：事後分析

CIR システムには、ガバナンス、責任共有、および可視性など、クラウド以外のインシデンスレスポンス（IR）システムとは異なるいくつかの重要な側面があります。

[2] ENISA 2015, Technical Guideline on Threats and Assets, https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets.

[3]NIST.SP800-61r2:NIST 800-61r2 Computer Security Incident Handling Guide

[4]NIST SP 800-32 under Threat NSTISSI 4009

ガバナンス

クラウド内のデータは、おそらく異なる CSP を使用して、複数の場所に存在します。さまざまな組織と共同してインシデントを調査することは、大きなチャレンジとなります。また、大量のクライアントを抱える大規模な CSP にとっては、大量のリソースが必要になります。

責任共有

クラウドサービスの利用者、CSP、サードパーティプロバイダは、クラウドセキュリティを確保するための役割をそれぞれ担っています。一般に、利用者は所管するデータに責任を持ち、CSP は彼らが提供するクラウドインフラストラクチャおよびサービスに責任を持ちます。クラウドインシデントレスポンスは、常にすべての関係者間で調整する必要があります。

CSP と CSC の間における責任共有の範囲は、選択したクラウドサービスモデル（Software-as-a-Service（SaaS）、Platform-as-a-Service（PaaS）、Infrastructure-as-a-service（IaaS）など）に応じて異なります。この考えはよく理解する必要があります。たとえば、IaaS では、オペレーティングシステム（OS）の管理責任は CSC にあります。したがって、OS に対するインシデントレスポンスの責任も CSC にあります。

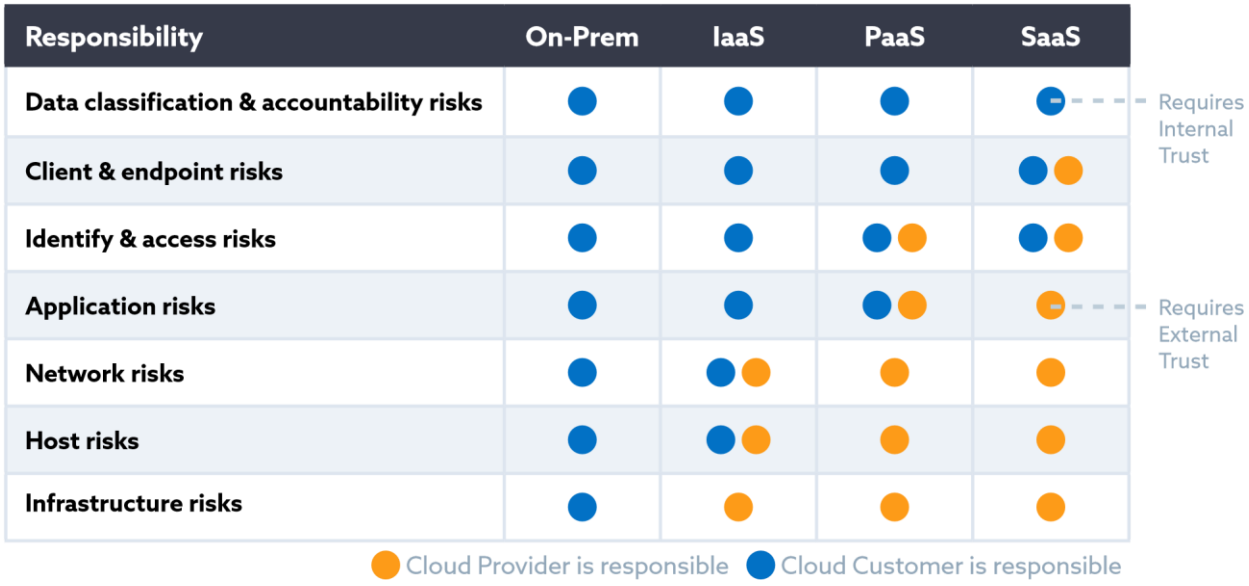

図 2: CSC と CSP 責任共有リスクマトリックス[5]

CSP との契約またはサービスレベル合意書（SLA）で、役割とガバナンスが明確で十分に文書化されていることを – 詳細なレベルで – 議論することが不可欠です。 CSC は、実施できないポリシーを作成した

[5] Microsoft TechNet 25 October 2019, Shared Responsibilities for Cloud Computing, https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

り、取りまとめたりしてはいけません。組織は、その組織に割り当てられたガバナンスや責任共有を外部委託することは決してできないことを理解する必要があります。

サービスプロバイダの多様性

組織は、CSC、CSP、およびサードパーティのクラウドプロバイダとの連携に向けて、一貫性のある明確に定義されたマルチクラウド戦略/フレームワークを持っている必要があります。単一の CSC、CSP、またはサードパーティのクラウドプロバイダで「すべてをまかなう」戦略を採用している組織は、サービスプロバイダ側で障害が発生する場合に関しては、間接的に単一障害点を導入していることになります。

クラウドサービスの提供に単一の CSP を採用するアプローチは、CSC / CSP で組織が制御できない障害が発生した場合に、組織のビジネスが継続的に停止する可能性をもたらします。このシナリオは、事業運営に大きな影響を与え、事業継続計画（BCP）戦略によって復旧できない可能性を高め、結果として全社的な CIR イベントが発生します。

CIR の観点からサービスプロバイダの多様性に取り組む場合、組織は、計画の中でデジタルサービスの主権の側面（データの保管場所、データの主権など）を考慮することも推奨されます。

可視性

クラウドでの可視性の欠如は、迅速に修正できた可能性のあるインシデントがすぐに対処されず、さらに深刻化するリスクがあることを意味します。クラウドを適切に活用すれば、より速く、より安く、より効果的な IR を実現できます。CSP とそのパートナーが提供する組み込みのクラウドプラットフォームツール、情報ソース、サービス、および機能はすでに多く存在し、検出、対応、復旧、およびフォレンジック機能を大幅に強化することができます。従来のデータセンターモデルの代わりにクラウドアーキテクチャを活用する場合は、IR プロセスとドキュメントを開発する際に注意が必要です。CIR は、プロアクティブかつ、プロセス全体を通じて障害に耐えられるように設計されている必要があります。

5. CIR フレームワーク

インシデントレスポンスと管理は、インシデントの発生による被害を最小限に抑えるための対応策と見なされます。これは、CSA の「クラウドコンピューティングのためのセキュリティガイダンス v4.0」[6]の第 9 ドメインで述べられているように、あらゆる情報セキュリティプログラムの重要な側面です。適切なインシデンスレスポンスプロセスと計画を定義することで、CSC は、検知されたインシデントを確実に管理および制御できるようになります。

この文書の第 2 章に記載されているように、インシデンスレスポンスおよび管理フレームワークは多くの組織によって開発および文書化されています。さまざまなフレームワークには、それぞれの目的と対象者があります。このフレームワークは、*CSA の「クラウドコンピューティングのためのセキュリティガイダンス v4.0」*および「*NIST Computer Security Incident Handling Guide (NIST 800-61rev2 08/2012)」*で説明されている一般的に受け入れられている「インシデンスレスポンスライフサイクル」を採用しています。

5.1 フェーズ 1：準備とそれにともなうレビュー

準備段階では、組織がインシデントに対応できるように、インシデンスレスポンス機能を確立する必要があります。言い換えれば、環境と「敵」を知ることが不可欠ということです。

インシデントが発生した場合、CIR の目的は次のことを達成するべきです：

- 迅速な検知、分離、および封じ込めを提供します
- 個人データ、所有する情報、機密情報の露出と侵害を最小限に抑えます
- ビジネスおよびネットワーク運用の中断を最小限に抑えます
- エビデンスの取得と処理のための統制を確立します
- 影響を受けるすべての関係者にインシデント状況の正確な情報流通を提供します
- 正確なレポートと有用な対処方法を提供します
- 組織の評判と資産を保護します
- インシデンスレスポンスから得た教訓に基づいて従業員を教育します
- 上記から得た教訓に基づいて CIR 計画を見直し、改善します

[6] Cloud Security Alliance 2017, Security Guidance for Critical Areas of Focus in Cloud Computing v4, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

組織のインシデンスレスポンス機能を理解するためには、従来の IR フレームワークと CIR フレームワークの重要な違いの 1 つである、CSC と CSP の間に「責任共有モデル」が存在することを理解しなければなりません。従来の IR フレームワークでは、システムを所有する組織がシステムに対して単独で責任を負います。コンピュータインシデンスレスポンスチーム（CIRT）は、セキュリティインシデントを含むさまざまなタイプのインシデントを処理するためのプロセス、手順、計画、およびプレイブックを作成しなければなりません。組織が単独でシステムを管理するため、CIRT の司令官またはリーダーは、影響を受けるすべてのシステムに対して調整、管理、および監督を行い、それらのシステムから必要なログとアーティファクトを収集することができるはずです。

しかし、クラウド環境では、CSC がすべてのシステムの所有者であるとは限りません。採用されたサービスモデルとそれに対応する責任共有モデルに応じて、一部のアーティファクトとログは CSP によって管理されます。サードパーティの IR プロバイダが関与している場合、CIR 計画では彼らもプロセス全体に含める必要があります。そうすることで、組織はサードパーティの IR ベンダーが緊急対応時に必要なリソースに素早くアクセスできるかを審査できる適切な機会を得ることができます。

組織は、インシデント発生時にいち早く活性化できるよう、CSP の事業継続性と災害復旧機能を日頃からよく理解して十分に活用するよう意識しておかねばなりません。したがって、CSC は CSP の IR 手順を理解し、SLA と契約を通じてそれらと整合をとる必要があります。この取り組みを管理および実行するには、CIR 計画に次のものを含める必要があります。

1. 既存の環境、クラウドアーキテクチャ、および責任モデルの分析。
    a. [CSC] 使用するクラウドサービスのインベントリ、サービスコンポーネント、および対応するサービスモデルと配備モデルを特定して準備します。
    b. [CSC] コンプライアンス要件（データプライバシーや地域の規制要件など）を確認し、データ侵害の報告時間要件などのコンプライアンス要件を抽出します。
    c. [CSC] 既存の契約と SLA を収集し、責任共有モデルに従って、クラウドアーキテクチャにおけるさまざまな関係者の役割と責任、およびそれらの義務を決定します。役割と責任を明確に記述することで、タスクの重複や見落とし、およびインシデント発生中に役割を割り当てる際の不必要な時間の浪費を防ぎます。
    d. [CSC] さまざまな関係者（内部チーム、マネージドサービスプロバイダ、CSP、またはその他のサードパーティ）間の連絡方法をとりまとめます。インシデントレポート体制には、電話番号や電子メールアドレスなどの連絡先情報を含める必要があります。
    e. [CSC] CSP からインシデント支援チームを集めます。**インシデント支援チーム**には、ヘルプデスク、フィールドサポートチーム、およびセキュリティオペレーションセンターや SOC などの他の支援サービスが含まれます。
    f. [CSC] スーパーユーザと同じレベルの特権で CSC のテナントにアクセスするため、CSP に委任された管理権限をレビューします。CSP は CSC のテナントに対して強力なセキュリティ制御を実施する場合がありますが、CSP を侵害する脅威アクターにより CSC の環境にアクセスが可能となる恐れがあります。したがって、CSC は、CSP がこれらの管理権限の委任を必要とするかどうかを確認する必要があります。CSP が委任された管理権限を必要とする場合、CSC は、潜在的な誤用を CSC に通知するために、監視などの適切な制御が CSP に実装されていることを確認する必要があります。CSP は、必要に応じて、条件付きアクセスポリシーを利用して、CSC の環境へのアクセスを制限する必要もあります。CSP が委任された管理権限を必要としない場合、CSC は、この特権が CSP から削除されていることを確認する必要があります。最後に、CIR 組織（CSC および CSP における）を設立します。
    g. [CSC] 収集した連絡先と組織内で特定された関係者で、インシデントレスポンスチームを編成します。
    h. [CSC] CIR 組織構造を定義し、インシデントレスポンスコマンダ、関係するシステムの所有者、テクニカルリーダ（複数も可）、テクニカルコーディネータ（複数も可）を任命します。前のステップ（既存環境、クラウドアーキテクチャ、責任モデルの分析）で特定された役割と責任に応じて、CSC は IaaS に実装されたシステムをサポートできる技術的な対応責任者を割り当てたり、次のフェーズのためにインシデントやログの連絡やサポート指標の収集を行うテクニカルコーディネータを手配したりする必要があります。[フェーズ 2：検知と分析]。すべてのクラウドコンポーネントがそれぞれの責任を持つ担当組織によって処理されていることを確認します。

2. 効果的かつ効率的な CIR 対応と是正のためのインシデントハンドリング計画、プロセス、手順／プレイブック（CSC および CSP）を確立します。
    a. 電話番号や電子メールアドレスなどの連絡先を記載した**インシデント報告プロセス及び手順を作成します**。
    b. インシデントの状況を記録・追跡するための**課題追跡システム**。
    c. **第三者との調整や危機管理コミュニケーションを含むインシデンスレスポンスプロセスと手順を策定し**、役割と責任を明確にした上で連絡先を確立し、エスカレーションプランを定義し、スタッフを割り当て、手順を決定し、責任を正式に割り当てます。
    d. 組織変更に応じて、**CIR プランを更新するプロセスを策定します**。
    e. **獲得した教訓のアーカイブにアクセスできるようにし**、チームメンバー全員が参照できるようにします。
    f. 現在および潜在的な脅威に関する知識を得るために**第三者の脅威インテリジェンスサービスに加入します**。
    g. スタッフ研修の一環として、模擬インシデントシナリオを用いて **CIR プランをテストします**； 理想的には、この計画を毎年見直して更新します。どんなに考え抜かれた計画であっても、従業員が十分な準備をしていなければ計画は破綻します。
    h. 責任範囲内のタスクに関するスタッフ向けの**継続的なトレーニングプロセス**を開発します。これにより、スタッフは厳しい時代に対応するために必要な知識を身につけることができます。
    i. CIR 計画と手順で、CIR 組織の**連絡先を定義して文書化します**。連絡先リストは定期的に更新する必要があります。
3. 運用上の欠陥や悪意のある活動の兆候をプロアクティブに監視するための技術レベルの準備（CSC および CSP）。
    a. [CSC] 役割と責任は、前のステップ（既存の環境、クラウドアーキテクチャ、責任モデルの分析）から導き出されるべきです。CSC は、アーキテクチャ全体を確認して、アーキテクチャ内にギャップが存在するかどうかを判断する必要があります。CSC は、責任共有モデルによるインシデンスレスポンスプロセスを、対応する内部チームによって、次に述べるフェーズで実行します。 CSC は、CSP によって処理されるログと健全性の状況を CSP から収集する必要があります。
    b. [CSC] CSC は、CSP（複数も可）から収集されたログと健全性の状況を、CSC が定義したログと健全性の状況のリストと比較し、分析に必要なログが収集されていることを確認する必要があります。 CSC は、CSP から収集されたログとアーティファクトの制限、特に予想されるログの可用性と保持期間についても理解する必要があります。
    c. [CSP] CSP は、システムやデータセンターの健全性の状況やネットワークの監視をプロアクティブにスキャンすることで、**インフラストラクチャとアプリケーションを常に監視**する必要があります。
    d. [CSC] CSC は、重要なオペレーションとストレージの冗長性、ストレージのバックアップ、侵入検知システムと侵入防止システム、ファイル完全性監視システム、アンチウイルスソリューション、脆弱性の是正、ファイアウォールなどの**予防策**を定義し、セキュアなソフトウェア開発ライフサイクル（SDLC）の実践を採用しなければなりません。
    e. [CSC] CSC は、集中ログ管理およびログ分析施設の場所を特定する必要があります。多くの CSC 環境では、ログは異なる CSP 施設や CSC が設立したクラウドサーバに保存されており、場合によってはオンプレミスのサーバにも保存されています。効果的なインシデンスレスポンスと分析のために、ログを統合する必要があります。

f. [CSC] セキュリティ体制を改善するために、脅威検知機能を含む脆弱性とリスクの**定期的な評価**を実施します。
g. [CSC] デジタルフォレンジックのためのログファイルの保持、バックアップの復元、レポート作成などのために、**インシデント分析用のハードウェアとソフトウェアを維持**します。
h. [CSC] 支援要請や情報配信のための**自動化されたサポートメカニズムを確立**します。CSC は、自社のクラウド環境でのインシデントレスポンスにおいて、発生時にすぐ使うツールキット（jumpseat toolkit）を特定し、準備することも必要です。
i. [CSC] ポートリスト、資産リスト、ネットワーク図、現在のネットワークトラフィックベースラインを含む**内部資料**を確認します。
j. [CSC] 堅牢な**事業継続計画（BCP）**は、インシデントを管理・復旧するための組織の運営のレジリエンスを大幅に強化します。その範囲には、CSP が提供するサービスを含めるべきです。
k. [CSC] クラウドインシデントの潜在的な財務的影響を軽減するのに役立つ可能性があるため、 利用可能な場合は**サイバー保険**に加入します[7]。
l. [CSC] CSC は、CSP のロギング構造と、オンプレミスのログ構造がどのように異なるかを理解する必要があります。動的フィールドの使用は、CSC がセキュリティ情報およびイベント管理（SIEM）ソリューションで必要なデータを照会し、効率的なアラートを作成する能力を制限する可能性があります。
m. [CSC] CSC は、CSP 製品が集中型 SIEM で必要なログ収集をサポートする機能を備えていない可能性があるため、ログ要件を文書化する必要があります。

4. 通信チャネルの準備（CSC および CSP）
   a. [CSC] CSP とのすべてのコミュニケーションのためのプライマリかつ単独の連絡先として、社内チームを編成します。
   b. [CSC] CSP などの外部との危機コミュニケーションプロトコルを作成します。インシデント発生中に円滑なコミュニケーションを可能にするために、組織内外の主要な関係者に連絡できるような**コミュニケーション方法**を準備しておく必要があります。
   c. [CSC] チームが内部および外部の関係者の最新の連絡先リストを持つようにします。**緊急連絡先リストには**、組織内外の他の IR チーム、呼び出し可能なスタッフの情報、法律顧問、法執行機関、その他の重要なインシデントハンドラに不可欠な施設を含める必要があります。

-

[7] Wikipedia, Cyber insurance, https://en.wikipedia.org/wiki/Cyber_insurance
AIG, Cyber insurance, https://www.aig.com/business/insurance/cyber-insurance
CHUBB, Cyber Insurance https://www.chubb.com/sg-en/business/cyber-insurance.html

前述のリストは、インシデントレスポンスの準備段階で準備すべき主なアクションをまとめたものです。以下は、上記のアクションから得られる成果物のリストです：

1. IR 計画、ポリシー、手順を作成します。
2. 資産一覧を作成します（クラウドサービス、サーバ、アカウントリスト、実装されているセキュリティ防御機構、想定するログファイル、設備を含む）。
3. インシデントレスポンスの役割マトリックスを作成します（CSC の CIRT と CSP からの参加者の役割を含む）。
4. インシデントレスポンス訓練のテスト計画とテスト結果。
5. インシデント発生時にすぐ必要になるツールのセット（jumpseat toolbox）。

5.1.1 文書化

組織は、IR プロセスを通じて、インシデントの文書化を維持し、インシデントと教訓を効率的にレビューするための体系的な記録を確保しなければなりません。組織は、インシデント記録について以下の情報を管理する必要があります：

1. インシデントの現在のステータス（「新規」、「進行中」、「調査依頼中」、「解決済み」など）。[8]
2. インシデントの概要。
3. インシデントに関連する侵害のインジケータ(Indicator of Compromise)。
4. 当初のインシデントに関連するその他のインシデント。
5. このインシデントハンドラが取った措置。
6. 該当する場合、証拠の連続性（Chain of Custody）。
7. インシデントに関連する影響評価。
8. 他の関係者（システム所有者、システム管理者など）の連絡先情報。
9. インシデント調査中に収集した証拠のリスト。
10. インシデントハンドラからのコメント。
11. 計画された次のステップ（例：ホストの再構築、アプリケーションのアップグレード）。
12. インシデント記録には、規制やコンプライアンスに関わる機密情報、IP アドレス、悪用された脆弱性、ビジネス上の機密情報などが含まれている可能性があるため、アクセスを適切な担当者のみに制限します。
13. 振り返り／学んだ教訓：成功事例、改善点、回避すべき行動、結果を改善するための新たな手順など、学んだ教訓を文書化します。

[8] NIST.SP800-61r2, Computer Security Incident Handling Guide

5.2 フェーズ 2:　検知と分析

5.2.1 発生源

5.2.1.1 クラウドインシデントの原因

この文書で定義されているクラウドインシデントとは、IaaS、PaaS、Desktop-as-a-Service（DaaS）、SaaS、および CSP が提供する関連サービスの運用に悪影響を与える出来事です。クラウドインシデントは、クラウドの停止（クラウドサービスが利用できない期間）を引き起こす可能性があります。クラウドインシデントの原因とダウンタイムは、次のいずれかのカテゴリに分類できます：

1. 自然災害（例えば洪水、火事）
2. システムの問題
    a. 内部（例：ソフトウェアのバグ、ハードウェア故障）
    b. 外部（例：電源供給の喪失、電気通信会社のネットワーク接続の障害）
3. 人為的
    a. 非意図的（例：　ヒューマンエラー）
    b. 意図的（例：　政府による制裁、ハッカー/DoS 攻撃、ランサムウエア）

5.2.1.2 インシデントの兆候

通常、インシデントの前には兆候があります。米国国立標準技術研究所（NIST）の定義によると、兆候を構成するシナリオには次のものが含まれます：

- 前兆（将来インシデントが起こるかもしれない兆候）
- インジケータ（インシデントが起こったか、現在起こっている兆候）

	前兆	インジケータ
自然災害	悪天候の予報 • いくつかのソフトウェアサービスにおける応答遅延 • 脆弱性スキャナの使用を示す Web サーバのログ	複数回にわたる電源断
システムの問題		• 複数回にわたる電源断 • ある程度の期間にわたる電源供給の変動 • 直流電源における継続的な温度上昇 • データベースサーバに対してバッファオーバーフローの試行の発生を、ネットワーク侵入検知センサが警告
人為的	• 組織のメールサーバの脆弱性を狙った新しいエクスプロイトの公表 • あるグループが組織を攻撃することを示唆する犯行声明	• ウイルス対策ソフトウェアは、ホストがマルウェアに感染していることを検知したと警告 • システム管理者が、異常な文字を含むファイル名を検出

図 3：インシデントの兆候

5.2.1.3 前兆とインジケータの一般的なソース

CSP と CSC には、これらの兆候を検知するためのシステムまたはプロセスが必要です。これにより、実際の発生を防止できる可能性があります。前兆とインジケータの一般的なソースは以下のとおりです：

1. アラート
2. ログ
3. 侵害のインジケータ（IOC）
4. 業界におけるイベント
5. マーケットアナリストレポート
6. 脅威インテリジェンスレポート
7. 公開情報
8. 人
9. ソーシャルメディア

システムログ、アラート、SIEM、セキュリティ運用センターから統合運用センターに至るまで、これらの前兆とインジケータを収集および分析するためのシステムを導入することをお勧めします。理想的には、統合運用センターを介して、さまざまなアラート、ログ、イベント、通話、およびログを監視およ

び相互に関連付け、包括的なサイバー状況を認識することができます。いずれの場合も、収集と分析の範囲は、配備された資産だけでなく、クラウドの管理プレーンをカバーする必要があります。

5.2.2 影響を特定するためのインシデント分析

5.2.2.1 インシデント分析

インシデント情報収集の取り組みの一部は、セキュリティイベントが false positive 又は false negative かを判断することです[9]。その判断の結果、もし問題が誤ったアラームである場合は、チケット等の文書に評価結果を記録して、問題をクローズする必要があります。正当性を判断するには、各インジケータを評価する必要があります。

インシデント分析の推奨事項は次のとおりです:[10]

1. ネットワークとシステムを評価する：ベースライン等のシステムのプロファイリングは、変更が発生したときの識別を改善し、変更をより適切に識別できるようにします。
2. 通常の動作を理解する：ログレビューを実施することで、アナリストは、時間の経過に伴う傾向や異常なイベントなど、インシデントを示す可能性の傾向に気付くことができます。
3. イベント相関の実行：インシデントの証拠は、異なるデータタイプを含むいくつかのログに記録される場合があります。ファイアウォールログに送信元 IP アドレスが含まれ、アプリケーションログにユーザ名が含まれている場合があります。
4. パケットスニファを実行して追加データを収集する：場合によっては、インジケータが十分な詳細を記録していないため、ログからは何が発生しているかを理解できません。インシデントがネットワーク経由で発生した場合、必要なデータを収集する最も速い方法は、パケットスニファにネットワークトラフィックをキャプチャさせることです。
5. データ分析を活用してすべてのデータセットを分析します：膨大なインジケータに対処するための効果的な方法の 1 つは、重要ではないと思われるインジケータのカテゴリを除外することです。もう 1 つの方法は、最も重要なインジケータのタイプのみを表示することです。 ただしこのアプローチは、あたらしい悪意のあるアクティビティが選択済みのインジケータカテゴリに分類されていない可能性があるため、かなりのリスクが伴います。したがって、収集されたすべてのインジケータを監視・分析することができるデータ分析を用意することが最も良い方法です。

9 The SANS Institute, 2011, Following Incidents into the Cloud

10 NIST, Computer Security Incident Handling Guide, SP.800-61r2

5.2.2.2 インシデント通知

インシデンスレスポンス計画は、ビジネスおよびサービスの運用への影響を最小限に抑えるために体系的に編成する必要があり、インシデントが発生したときに関係者に通知する必要があります。インシデントのエスカレーションは、インシデントの影響の重要度に基づいて行う必要があります。非常に複雑なクラウド環境ではインシデントが大量に発生するため、上級管理職には重大で影響の大きいインシデントについてのみ通知する必要があります。CSP および CSC は、エスカレーションマトリックスを開発し、契約や SLA に統合する必要があります。注：CSP は、CSP のインフラストラクチャと運用に脅威を与える可能性があるため、CSC の重大インシデントを CSP に通知するよう、CSC に義務付ける場合があります。
正確なインシデント報告をレポートするために、インシデントの報告者、また可能であれば影響を受けた環境から、次の重要な情報（5W）を収集する必要があります：

1. 何（What）が発生したか？ユーザはインシデントの前後に何かアクションを実行したか？
2. インシデントはどこ（Where）で発生したか？封じ込められたか？又は他の領域が影響を受けたか？ 影響を受けていないとするゾーンの信頼水準はどれくらいか？
3. いつ（When）発生したか？
4. 誰（Who）が発見したか？誰が影響を受けて、誰が影響を受けていないか？ どのようにして発見されたか？
5. インシデントはなぜ（Why）発生したか？原因、または最初の被害者は分っているか？

5.2.2.2.1 インシデント通知のタイミング

時間は重要です。インシデントを迅速に解決する必要がありますが、関係する利害関係者に迅速に通知を行い、インシデントの影響を減らすための助言やアクションを実行できるように、関係者が状況を理解することも同様に不可欠です。インシデントの間、危機コミュニケーションは、サイバー攻撃を含め、インシデントに関係するすべてのサービスまたはビジネスの停止をカバーする危機管理計画の不可欠な部分です。インシデント管理が不十分だと、規制上の罰金、評判の低下、顧客の信頼の喪失、深刻な経済的損失につながる可能性があります。

- 最初のインシデント通知は、CSC / CSP /サードパーティプロバイダが実施する横断的な調査を手助けするために、最初の 2～8 時間以内に内部および外部の主要な利害関係者に通知する必要があります。
- 最初の情報提供のためのインシデントレポートでは、（インシデントの影響に応じて）内部の利害関係者に対して、最初の 4～48 時間以内に少なくとも最初の 4W（What, Where, When, Who）を共有する必要があります。必要に応じて、外部の利害関係者（CSP /サードパーティプロバイダ）が調査と封じ込めに関与する必要がある場合があります。 必要に応じて、外部の利害関係者も関与する必要があります。
- CSC / CSP は通常、一般化された契約条件に従って、合意できる時間枠内で自己報告を行います。 組織は、この報告のしきい値が要件を満たし、組織のインシデント管理フレームワーク全体と一致しているかについて、レビューを実施することをお勧めします。
- 組織は、事業を行う国/地域/地区に適用される規制要件を認識している必要があります。例えば、EU の一般データ保護規則（GDPR）では、企業は違反に気付いてから 72 時間以内に違反を報告する必要があります（可能な場合）。 この義務は、EU 域内の人々に関連するデータを対象と

するか収集するか、EU 市民または居住者の個人データを処理する限り、どこの組織にも課せられます。

エスカレーションワークフローに応じて、組織は合意された媒体（電話、SMS、電子メールなど）を介して迅速に通知を送信する必要があります。インシデント重大度レベルに応じて、CIR（インシデントレスポンス）計画で合意されている通りに、実務者及び管理者にエスカレーションする必要があります。ビジネスの継続性や評判に重大な影響がある場合、組織は BCP や危機管理計画（CMP）を実行する必要があります。

5.2.2.3 インシデント影響

インシデント影響モデルは、イベントの評価、影響度、通知、および適切な対応をするために必要なアクションに関して一貫性を確保するために、事前に開発し、CSP と CSC とで利用すべきです。インシデント優先度マトリックス（影響と緊急性のマトリックス）は、影響の重大性と緊急性レベルから導き出されます。損傷度合いを判断するためには、迅速かつ適切な影響評価を実施する必要があります。次の例は、CSP と CSC の双方が一緒に検討すべき影響タイプです。

- ビジネス：ビジネス重要度の規模とレベル
- 財務：ダウンタイムによる損失または評判への影響
- 規制／法務：データプライバシーと契約条件

組織は、自組織のリスクの許容範囲とリスク選好度に基づいて影響の重大度レベルの適切な分類を確立し定義する必要があります。欧州ネットワーク情報セキュリティ庁(ENISA)のクラウドセキュリティインシデントレポートでは、一つ以上のパラメータにより影響レベルの評価を行うことができます。例：１日におよぶダウンタイムと 70%の地理的広がりがある場合は、インシデント影響度は「レベル２／レベル１」となります。この決定に基づいて、ユーザは「レベル２／レベル１」影響のインシデントに対する封じ込めガイドラインを参照する必要があります。ガイドラインで与えられた数値は例として提供されているものであり、組織の性質、優先順位およびビジネス目標を反映するように数値を調整する必要があることに注意することが重要です。

緊急度レベルは、以下の考慮事項を使って最低（レベル５）から最高（レベル 1/2）の範囲となります。

- 現在影響を受けているシステムまたはサービスは重要なものか？
- 展開できる回避策や緩和策は存在するか？
- どの程度のユーザが影響を受けているのか？
- このインシデントを効果的に封じ込めることができるか？
- このインシデントはゆっくりまたは急速に広がり、他のユーザやシステムに影響を及ぼしているか？
- その他の考慮事項はあるか？例えば、法的または規制上の影響がある可能性は？

このセルフアセスメントは必要なリソースを導出し、要求された時間枠内でインシデントを迅速に管理および無効化するために必要なアクション範囲を決定します。例えば、影響と緊急度が最も高いインシ

デント（レベル１）は、通常、P1（優先度１）指定となり、組織の危機管理計画(CMP)のトリガーとなり、上級管理職および／または取締役会へのエスカレーションを行う危機である可能性があります。

ユーザが影響の重大性やビジネス運用に対するクラウドサービスの可用性に関する重要性を評価できるように、組織はいくつかの標準やガイドラインで使われているインシデント分類尺度を採用すべきです。以下は、CSP の現在の運用トレンドに基づくポリシーセットです：

優先度= インシデント尺度	インシデント影響度	目標応答時間	目標解決時間
1	クリティカル	5 分以内 24 時間対応チームによる	1 時間以内
2	高	15 分以内（就業時間中） 2 時間以内（営業時間対応チームの就業時間後） サイトによっては 4-8 時間	4 時間以内
3	中	15 分以内（就業時間中） 2 時間以内（営業時間対応チームの就業時間後） サイトによっては 4-8 時間	8 時間以内
4	低	15 分以内（就業時間中） 2 時間以内（営業時間対応チームの就業時間後） サイトによっては 4-8 時間	24 時間以内
5	極低	システムオートフィルタにより応答の必要なし	--

図 4: インシデンスレスポンスポリシー

組織は、ビジネス影響分析(BIA)または組織のパラメータに固有の脅威、脆弱性、リスク評価(TVRA)を実施し、クラウドにおけるインシデントの潜在的な財務的影響を軽減するためにサイバー保険の購入を検討することもできます。

5.2.3 証拠収集と取り扱い

調査に関連するデータを特定することは、インシデントの根本原因を決定し、インシデントが繰り返し発生することを回避するための教訓を特定する上で不可欠です。識別されたデータは、似たようなインシデントを防止するための有益な情報共有イニシアチブをサポートすることに対しても役立ちます。

GDPR または他のコンプライアンス要件により、CSP によってはログの保持期間が制限される場合があることに注意してください。 ログの可用性は必要な証拠収集に影響を与えるため、これらの制限を理解し、インシデンスレスポンス計画で考慮する必要があります（状況は選択したクラウドサービスによって異なる）。

仮想インスタンスに接続されたストレージドライブやインスタンスのメモリスペースは、関連データが存在する場所の候補です。インスタンスのスナップショットなどの CSP 機能を利用することで、CIR チームは、インシデントに関連した仮想化ストレージドライブのスナップショットを取得し、それらをさらに分析や発見に利用することができます。これらのスナップショットは、広く利用されているフォレンジック分析ツールを使って、精査のためにデジタルフォレンジック調査環境にマウントできます。

収集された証拠は、ハッシュ値を計算しておくべきです。これにより収集された情報の完全性が確保され、データが元のソースから変更されていないことが保証されます。この取り組みは法的手続きに関する証拠の許容性を確保することにも役立ちます。法的に認定されるために、（ハッシュされた元のデータではなく）収集された証拠のコピーに対してフォレンジック作業を実施するようにします。

サイバーセキュリティインシデントでは、攻撃しているホストを特定するために、次の手順を実施する必要があります：

- 攻撃しているホストの IP アドレス／ドメイン／電子メール／その他の情報を検証
- 検索エンジンを使って攻撃しているホストを調査
- インシデントデータベースを利用
- 攻撃者の通信チャネルをモニタリング
- 攻撃しているホストを見つけるために、SIEM または他のツールへの IoC アラートを作成

収集された証拠は、収集されたデータの完全性を確保するためにハッシュアクティビティを利用すべきです。このプロセスは証拠が元のソースから変更されていないことを確認するために使用でき、法的手続きにおける許容性を確保することに役立ちます。

5.3 フェーズ 3: 封じ込め、根絶、 復旧

封じ込め：セキュリティインシデントに対処し被害を抑える方法はインシデントや組織によってそれぞれ異なります。インシデントを正確に識別し、インシデントタイプに基づき、実行するアクションをリスト化する必要があります。封じ込めとは感染したシステムを隔離することです。

注：インシデントとその影響によっては、封じ込め、根絶、復旧がすべて同じプロセスの一部になる場合があります。

セキュリティインシデントを検知した際、攻撃者の活動とシステムへの再侵入を防ぐためには、封じ込めが極めて重要です。未確認のアクティビティはリソースの圧迫や、被害の増大をもたらす可能性があります。攻撃者の視点でいうと、まず初期の侵害から開始し、マルウェアのダウンロード、特権の昇格、ネットワーク探索によって攻撃基盤を確立する、が典型的な攻撃パターンです。この時点で攻撃者は端末 1 台へのアクセスに留まっており、データを盗み出すまでには至っていません。

次に、攻撃者は水平方向に移動し、数台の端末へマルウェアを仕込み、永続性の確立を試みます。これにより、初期の侵害が見つかってしまってもネットワークへ再侵入する方法が確保され、見つかってしまうリスクを低く抑えることが可能になります。攻撃者はこのシステムに腰を据え、ミッションの実行を開始します。

インシデント検出の際、対象の組織は、システムのオフライン化、システムの検疫、接続制限など、事前に定義した CIR 計画(フェーズ 1：準備 で規定)を実行する必要があります。その際、盲目的に脅威を削除しないことが極めて重要です。もし削除してしまうと、CIR 計画の修正に必要なフォレンジックの証拠が破壊されてしまいます。封じ込めは復旧計画を準備するための時間を確保します。この封じ込めに重要な要素は意思決定です(例：システムのシャットダウン、ネットワークからの切断、API キーの削除、ユーザ名の無効化)。このような決定について、インシデントを封じ込めるために事前に準備しておいた計画と手順を用いて行うのが簡単な方法です。計画と手順を定義し文書化するには、IR チームはプレイブックやランブックを用いてタスクを簡素化する必要があります。

組織はインシデントに対処する際に許容可能なリスクを定義し、それに応じた計画を定義する必要があります。封じ込めの計画はインシデントの種類によって異なります。例えば、E メールを介したマルウェア感染を封じ込める手順と、ネットワークベースの DDoS アタックを封じ込める手順とはまったく異なります。組織は意思決定を容易にするために明確に文書化された基準を用いて、主要なインシデントの種類別にそれぞれの封じ込め計画を作成しておく必要があります。

適切な計画を決定するための基準は以下のとおりです：

- ビジネスへの影響
- 潜在的なリソースの搾取と被害
- 証拠保全の必要性
- サービスの可用性（例：ネットワークの接続性、外部向け提供サービスなど）
- 計画の実行に必要な時間とリソース
- 計画の有効性（例：一部封じ込め、完全な封じ込め）
- 封じ込めに要する期間、複雑さ（例：4 時間で削除される緊急の回避策、2 週間で削除される一時的な回避策、恒久的な解決策）
- リソースの可用性（特に技術的な専門知識）
- バックアップ／コピー／スナップショットの可用性と完全性
- サンドボックス／ハニーポット環境の可用性

適切な封じ込め計画の最終目標は、攻撃者の動きを制限し、サービスの中断を最小限に抑えつつ、できるだけ短時間に不正アクセスや感染を防ぐことです。適切な封じ込め計画は調査に必要なフォレンジックの証拠を保持しつつ、さらなる被害の発生を防ぎます。

5.3.1 封じ込め計画の選択

場合によっては、組織は攻撃者をサンドボックス(ハニーポットに似た封じ込めの手法)へ誘導し、攻撃者の活動を監視できるようにする方法があります。(通常、追加の証拠を収集するため) IR チームは実現可能性を判断するために、この計画について法律の専門家と話し合う必要があります。

組織は攻撃者の活動を監視するための代替手段(サンドボックス以外)を実装すべきではありません。組織がシステムの侵害を検知したものの、その侵害を見逃すと判断した場合、攻撃者が侵害したシステムを使用して他のシステムを攻撃することがあるため、組織は責任を問われる可能性があります。

封じ込め計画を意図的に遅らせるのは危険です。なぜならば、攻撃者が不正アクセスを拡大し、他のシステムを危険に晒す可能性があるからです。その他の潜在的な問題はいくつかの攻撃が封じ込められた後に更なる被害を引き起こす可能性があります。例えば、侵害されたホストが別のホストに対して定期的に ping を送信する悪意のあるプロセスを実行する、などです。インシデントハンドラが侵害されたホストをネットワークから切り離し封じ込めることで、その後の ping は失敗するでしょう。

Ping に失敗したことにより、悪意のあるプロセスがホストのハードドライブにあるすべてのデータを上書きしてしまう、または、暗号化してしまうケースがあります。ホストがネットワークから切断された後であっても、ホストに対するさらなる被害が防止されると過信しないようにしてください。

5.3.2 根絶と復旧

根絶：問題を取り除くこと。これは損失や情報の盗難、サービスの中断などを最小限に抑え、脅威を排除することが含まれます。影響を受けるすべてのシステムの運用レベルを復旧するには、根絶するための手順が必要になる場合があります。システムを運用レベルに戻すためには、脅威、感染、被害を取り除かなければなりません。この際、ディスクを完全に消去し、侵害されたコードやユーザアカウントを削除する場合もあります。

復旧：コンピューティングサービスを安全かつ迅速に復元すること。[11] 復旧プロセスとはシステムを元の状態(または拡張された状態)に戻すことです。この手順では、パッチの適用、システムのキーファイルの再構築、アプリケーションの再インストール、パスワードの変更やバックアップからのファイルを復元することで、本番環境へ復旧します。

5.4 フェーズ 4: 事後分析

CIR プロセスの最終フェーズは事後分析です。この極めて重要なフェーズの目的は、将来のインシデント処理手順を改善するために、企業と CSP チームがどのようにインンシデントを処理し管理したかを評価し、今後のインシデント処理手順を改善することです。評価は、インシデントのデータと、「教訓」

[11] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

を含む事後レポートの確認によって裏付けられます。[12] ここで重要なのは、「何がもっとうまくできたのか」ということです。このフィードバックは、新たな対策としてフェーズ 1 に反映されるべきものです。

5.4.1 インシデント評価

インシデントの特徴を分析することで、少なくとも、セキュリティ上の弱点や脅威、クラウド構成上の弱点、インシデントの傾向の変化などを示すことができます。このデータは、リスクアセスメントのプロセスにフィードバックループとして追加され、追加のコントロール、プロセス、予防措置の選択と実装につながる可能性があります。

また客観的な事後分析を行うことで、収集した情報をもとに CIR プロセスの全体的な効果を評価することができます。

質問には次のようなものがあります：

- 彼らはどのように対応しましたか？
- 彼らの強みと弱みは何でしたか？
- 彼らが学んだ教訓は何でしたか？

インシデントデータが適切に収集・保存されれば、IR チームのいつくかのうまくいった（あるいは少なくとも実施した）対策が浮かび上がるでしょう。

5.4.1.1 インシデント評価指標

インシデントデータを収集して、時間の経過に応じて注目すべき傾向が存在するかどうかを判断することもできます。これらのパターンは、定められた期間中にチームがどのように行動しているか、および改善点（インシデント数の減少）または注意を喚起すべき領域（セキュリティ関連インシデントの急増など）があるかどうかを明らかにすることができます。規制産業では、特に重大なインシデントにおいては、通常これらの情報を規制機関や経営陣に報告しなければなりません。CSC はこれらの要求事項を満たすために、必要なデータをタイムリーに、正確に、かつ完全な形で収集することが求められます。

不正アクセスや不審なトラフィックを確認するために、フローログや他のトラフィックログなどのデータを収集する必要があります。

収集されたインシデントデータは、次の情報を把握する指標（パフォーマンス インジケータ）から構成される必要があります：

[12] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

- **平均検知時間 （Mean time to detect、MTTD）**： セキュリティインシデントを検知するまでの平均時間。インシデントが発生してからチームがそれに気づくまでどれくらいの時間がかかったか? これは、攻撃者の滞留時間（攻撃者が侵入し、それを検知するまでの時間）に直結します。
  平均確認時間（Mean time to acknowledge、MTTA）： セキュリティオペレータがシステム警告に応答するのにかかる時間。MTTD は攻撃者に気付く前の時間を測定しますが、MTTA はセキュリティ警告に応答するセキュリティオペレータの時間を測定し、分析を開始することに重点を置いています。
- **平均復旧時間（Mean time to recovery、MTTR）**：システムを稼働状態に戻すのに必要な時間（フェーズ 3 にリンク）。
- **平均封じ込め時間（Mean time to containment、MTTC）**：インシデントの検知、対応、根絶、およびインシデントからの回復に要する平均時間。MTTC は、対象となるすべてのインシデントの MTTD、MTTA、MTTR を加算し、対象となるインシデントの数で割ることで算出できます。この指標は、インシデンスレスポンスチームがどれだけうまく組織化されているかを示すもので、主要指標（Key Performance Indicator、主要業績評価指標、または KPI） と見なされます。MTTC の上昇は、一部のサブプロセスがインシデンスレスポンス時に最適でないことを示します。MTTC の低下は、チームが非常に組織化されていることを示します。
- 脅威の指標（例：DDoS 攻撃の場合の Gbps や Tbps）
- 脅威の行為者の TTPs（戦術、技術、手順）。フィッシングやアカウント操作などがこれに含まれます。その他の例は MITRE の ATT&CK® Cloud Matrix に掲載されています。[13]

5.4.1.2 インシデント分類

重大度と緊急度の分類（H/M/L）は事後分析によって変化する可能性があります。

個人を特定できる情報（PII）や保護医療情報（PHI）の機密性／完全性が損なわれ、かなりの数のお客様がサービスを利用できなくなるような重大度の高いインシデントは、大きな財務的影響を及ぼす可能性があります。その例を以下に示します。

- PII/PHI の漏洩が確認された場合
- 本番稼働システムのルートレベルのセキュリティ侵害が成功した場合
- 金融犯罪マルウェア
- 重大な機能停止を引き起こすサービス妨害（Denial of Service）攻撃

重大度が中程度のインシデントは、PII を漏洩する試み（失敗している可能性がある、またはまだ成功していない）、または可用性/財務上の影響が限定されたインシデントを指します。

- PII/PHI の侵害が疑われる場合
- 本番稼働システムを侵害する標的型攻撃の試み
- 限定的なシステムの劣化やその他のパフォーマンス問題を引き起こす DoS 攻撃

[13] MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques
https://attack.mitre.org/matrices/enterprise/cloud/

深刻度の低いインシデントは、PII、可用性、企業や顧客への財務上の影響はありません。例としては以下のようなものがあります：

- 重要ではないシステム（例：ステージング/テスト用インスタンス）の侵害の試み
- 特定の従業員に関係したインシデント
- 顧客に目立った影響のない DoS 攻撃

5.4.2 インシデントクロージングレポート

インシデントがクローズした際、インシデントイベントを統括した CIR チームは従前のフェーズとインシデントの検証から得られたデータを使用して公式の事後レポート（AAR: After Action Report）を作成すべきです。このタスクは事後分析フェーズにおいて基本的なもので、教訓がまだ 記憶に新しいうちに実施されるべきです。タスクの実行が遅れた場合、重大な詳細が失われるか忘れ去られてしまい、将来的なインシデントレスポンスにおいて大きな差を生み出してしまう可能性をもたらします。CIR チームはインシデントのクローズから 2 週間以内に鍵となるステークホルダへ AAR を提出すべきです。[14]適切な対策は（上級）管理職によって策定・検証されなければなりません。AAR は報告書が一貫性を持ち、期待された基準を満たすよう、正式に承認されたレポーティングテンプレートを用いて作成することがベストです。インシデントレポートは以下を包括すべきです：

- インシデントの日時
- インシデントクローズの日時
- インシデントのスコープ
- インシデントを報告した人の名前
- 影響を受けた人の組織・事業部
- インシデントの記述
- 影響を受けたクラウドシステム、プロバイダまたはオンプレミスのリソース（ハードウェア、ソフトウェア、場所）とそれぞれの SLA
- ビジネスサービスオーナと CSP の連絡先（該当する場合）、インシデント管理に関連する CSP 担当者（該当する場合）
- インシデントの分類（深刻度の分類）
- 企業・顧客への影響分析
- 解決策
- 推奨事項
- 成功例と必要な改善案を定義し、将来的なインシデントの防止のためのより一層の対策を開発するための「教訓」セクション

レポート作成時には以下の要素について配慮します:

- インシデントのタイムラインと CIRT、CSP CIRT による観察を確認すること
- 事象の原因となった全ての要因を特定・レビューするために「5 Why’s （5Y）」手法による原因分析（root-cause analysis）を実行すること

[14] SANS Institute 2021, Incident Handler's Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

- 類似の事象が将来再発する可能性を減らすために緩和策の優先順位をつけること
- 新しいチームメンバーに経験のあるチームメンバーがいかにインシデントに対応しているかを知ってもらうため、AAR をトレーニング資料として利用すること
- AAR を（分類レベルごとに）一元化してインデックス化し、各インシデントのフォローアップレポートを作成すること。報告書は、将来発生する同様のインシデントに対処する際の貴重な参考資料となります。
- CSP<->CSC 間のコミュニケーションチャンネルの見直しと必要な場合のアップデートを行うこと
- フォレンジック能力のレビューをし、「クラウド・ジャンプ・キット」に欠けている要素がないかどうかを判断すること [15]
- 攻撃されたセキュリティの脆弱性、機微情報の詳細、および影響を受けた PII/PHI の詳細といった、インシデントで特定されたデータを確認すること
- 侵害報告の通知期限（GDPR など）やプロセスのレビューを行うこと
- CSC においてはインシデントレスポンスにおけるプロバイダのサポート状況を見直し、より幅広いプロバイダのサポートを得るために契約の変更・修正が必要か検証を行うこと

企業間でのインシデント情報の共有を促進するために、トップマネジメントに情報を報告した後、より広く一般に向けて報告書を公開することが必要であると考えられることが多いです。このような透明性は同様の企業がリスクをより的確に把握・コントロールすることに役立てられます。

5.4.2.1 教訓

セキュリティインシデンスレスポンスの最後のステップは、教訓を明らかにすることです。インシデンスレスポンス中に、人材、プロセス、または技術に関連するギャップが発見された場合は、それらに対応する必要があります。イベントをクローズした人は、セキュリティインシデントに関して、「教訓」と呼ばれる振り返りのレビューを確実に行う必要があります。「教訓」は、CIR 計画の修正と強化に利用しなければなりません。各インシデントレスポンスチームは、将来のインシデントレスポンスの改善のため、新たな脅威、技術の向上、教訓を反映して積極的に進化する必要があります。[16]

セキュリティガイダンス：データ収集の制限に特に注意を払い、今後の問題に対処する方法を決定します。クラウドデータは複数の場所に存在するため（そしておそらく様々な CSP に存在するため）、次のような点がこのプロセスの段階での課題となります：

- 様々なサードパーティプロバイダ（インターネットサービスプロバイダ）からインシデントデータ収集を入手し、調整することに関する課題
- サードパーティプロバイダのリソースへの依存（クライアント数の規模に依存する可能性があります）

以下の質問例は、CSC が自身の振り返りをする際の参考になります：

- サービス層のどの部分に影響がありましたか？影響を受けたアプリケーションとユーザへのインパクトは何ですか？
- どのくらいの期間、問題が発生しましたか、いつまで続きましたか？
- 問題の原因が特定されましたか？
- この事象の発生を防止または軽減するための教訓は何ですか？

15 CSA Security Guidance For Critical Areas of Focus In Cloud Computing v4.0, section 9.1.2

16 NIST.SP.800-61r2 Computer Security Incident Handling Guide

- どのようなアクションが取られるべきだったか？
- セキュリティの面から何か疑わしいことはなかった？
- プロバイダまたはブローカは、インシデントサポートをどの程度、またはどの程度迅速に提供しましたか？（該当する場合）
- フォレンジックな証拠収集のためのテクノロジーはどの程度よく識別されていたか？
- 誰かが、または自動監視システムやその他スキャンシステムが、リモート接続における不正アクセスや疑わしいトラフィックを検知しましたか？またインシデント発生時からインシデントのライフサイクルを通じて、役割と責任は明確でしたか？
- テクノロジーによりアラートはあがりましたか？
- 過去に発生した「下位」分類のインシデントを根本原因に結びつけることができるか？

5.4.3 インシデント証拠の保管期間

「フェーズ 2 検知および分析」で収集されたすべての識別された証拠は、企業に適用される法律、規制、業界、または契約上の義務について定められた要件に従って保全されなければなりません。証拠は以下の 3 つの目的で保管されます：

- 規制を遵守するための要件（例：特定のレベルと粒度の監査ログ、アラートの生成、活動報告、およびデータ保全）。データ保全は、プロバイダの標準的なサービス契約に含まれていない場合があります。
- 法務：PII/PHI または企業システムの侵害に対する訴追をサポートします。
- リスクマネジメント：新しい脅威、戦術、および戦略を反映・再評価します。
- トレーニング：将来的なインシデントに対するチームの準備を促進し、適応型インシデント学習を取り入れます。[17]

企業のフォレンジックモデルは、必要とされる証拠の保存期間や使用する技術を促進する能力を備えていなければなりません。[18]CSA の従来のガイダンスによると、CSC は CSP と共同でインシデントハンドリングを検証すべきです。クラウド環境でのデジタルフォレンジックの証拠保全は CSP と CSC の統合モデルとして捉えられなければなりません。[19]

17 Incident Response Teams – Challenges in Supporting the organizational Security Function, Ahmad, Hadgkiss & Ruighaver 2012; Shedden, Ahmad & Ruighaver 2011
https://www.sciencedirect.com/science/article/pii/S0167404812000624?via%3Dihub

18 CSA Security Guidance For Critical Areas of Focus In Cloud Computing v4.0

19 An integrated conceptual digital forensic framework for cloud computing, Martini and Choo
https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X

6. 調整と情報共有

インシデンスレスポンスの観点から責任共有モデルの複雑さに対処するには、クラウドユーザと CSP による多様で事前の投資が必要です。これらの投資を効果的に使用することは、効率的かつ効果的な CIR を確保するために重要です。すべてのクラウドの利害関係者は、CIR の短期的および長期的な目標を共同で開発する必要があります。長期的な目標のいくつかの例には、影響を受けるユーザを関与させて損失を軽減するためのフレームワークの構築/継続的な強化、およびビジネス復旧方法の戦略化が含まれます。

プロバイダとユーザ間の通信パスを適切に確立する必要があります。影響を受けるユーザは、損失を軽減し、ビジネスの復旧方法を戦略化するために、定期的な更新を利用できるようにする必要があります。効果的な調整とコミュニケーションは、顧客への報告だけではありません。

クラウドコンピューティングは共有利用の性質を有するため、攻撃は通常、複数の組織に同時に影響を及ぼします。したがって、インシデント情報の共有は、関係する組織を同じ脅威から保護するのに役立つという点で相互に有益です。 CSA は、参加している CSP 間のインシデントデータ共有を容易にするクラウドサイバーインシデント共有センター（CloudCISC）[20] を運用しています。
主要なパートナー、他の部門の IR チーム、および法執行機関との調整により、CIR 機能が大幅に強化されます。このコミュニケーションは、最初から計画段階で設定し、必要に応じて CIR プロセス全体を通じて維持する必要があります。

次のインフォグラフィックは、危機の場合に効果的なコミュニケーションを確保するために組織が移行するさまざまな段階を例示しています：[21]

図 5：効果的な危機コミュニケーションステージ

20 More information on CloudCISC: https://cloudsecurityalliance.org/research/working-groups/cloudcisc/

6.1 調整

6.1.1 関係者間の調整

すべての利害関係者が協力して、クラウドセキュリティインシデント時の役割と責任を明示的に特定する必要があります。従来、これらの役割は、責任分担モデルにおける義務と密接に関連しています。例えば：

- PaaS または SaaS アプリケーションのプラットフォームまたはサービスレイヤで発生するセキュリティインシデントは、CSP によって推進される必要があります。
- PaaS アプリケーションのアプリケーションレイヤで発生するセキュリティインシデントは、CSC によって推進される必要があります。
- IaaS インフラストラクチャクラウドのプラットフォームレイヤで発生するセキュリティインシデントは、CSC と CSP が共同で推進し、CSC の環境で発生したのか CSP の環境で発生したのかを判断する必要があります。

通常、すべてのインシデントは、効果的なインシデント管理のために CSC と CSP の間の緊密な協力を必要とします。

利害関係者は、そのようなインシデントシナリオを、その役割と責任とともに積極的に特定する必要があります。また、関係者が情報を効率的に共有する方法を理解できるように、インシデント発生中に使用する通信チャネル（電子メール、ビデオ/電話会議の詳細など）を特定する必要があります。

利害関係者とのコミュニケーション：コミュニケーションの推奨事項は、さまざまなファーストレスポンダの可能性に基づいている必要があります（たとえば、ファーストレスポンダとしての CSP とファーストレスポンダとしてのクラウドユーザ）。

6.1.2 契約と報告要件の共有

利害関係者が自分の役割と責任を特定したら、契約でこれらの関係を正式なものにすることが不可欠です。これらの契約には、すべての利害関係者が情報（企業の最も機密性の高い情報を含む）を機密情報として共有できるように、機密保持契約（NDA）を含める必要があります。外部組織と情報を共有しようとしている組織は、調整作業を開始する前に法務部門に相談する必要があります。話し合いが行われる前に締結しなければならない契約またはその他の合意がある場合があります。

組織は、インシデント情報を情報共有分析センター（ISAC）と共有したり、インシデントを上位レベルの CIRT に報告したりするなど、既存のレポート要件も考慮する必要があります。

21 REBIT Cyber Crisis Communications Playbook https://rebit.org.in/playbooks-and-presentation/ cyber-crisis-communications

6.2 情報共有のテクニック

クラウドの利害関係者は、脅威を特定し、主な利害関係者とセキュリティ情報を共有する能力を備えている必要があります。多くの場合、利害関係者は、インシデントに関する重要な情報を発見または共有し、その能力を客観的に評価するための最適な方法に関して明確な方向性を持っていません。相互接続性とレジリエンスを確保しながら、利害関係者の負担を軽減するための有効性を決定するには、共有技術を評価する必要があります。非常に小さな組織でさえ、前向きな結果を実現するために、インシデント情報を他組織やパートナーと共有する能力を持つ必要があります。組織は、インシデンスレスポンスのライフサイクル全体を通じて情報を共有すべきです。インシデントが完全に解決されるまで待つべきではありません。

情報共有は、組織間の調整を可能にするための基本的な要素です。

1. アドホック
2. 一部自動化
3. セキュリティの考慮

6.3 適切な情報共有

また、組織は情報共有のメリットと、機密情報を共有することによるデメリットを比較検討する必要があります。企業は、必要なデータのみを適切な関係者と共有すべきです。理想的には、すべての関係者が NDA を締結し、機密情報や所有者の情報を契約によって保護することです。

6.3.1 ビジネスインパクトに関する情報

クラウドセキュリティインシデントは、ビジネス上の問題であると同時に IT 上の問題でもあります。クラウドセキュリティインシデントは、経済的損失（サービスの利用不能、ビジネス不能をもたらすコンプライアンス認証の喪失、インシデンスレスポンスコストなど）、評判への影響（顧客の信頼の喪失）、企業秘密の開示、知的財産権の盗難、機密データの漏洩など、さまざまなビジネス上のマイナスの影響を引き起こす可能性があります。

ビジネスインパクト情報は、影響を受ける企業のミッションを保全することに関心のある組織に報告する場合にのみ有用です。多くの場合、IR チームは、明確な価値提案や正式な報告要件がない限り、ビジネスインパクト情報を外部組織と共有することは避けるべきです。しかし、場合によっては、規制や法的要件のために、組織がこの情報を公に共有することを余儀なくされることもあります。

ビジネスインパクト情報は、ミッションへの影響、財務への影響など、インシデントが組織にどのような影響を与えるかを説明するものです。このような情報は、少なくとも要約レベルでは、インシデントの被害見積もりを伝えるために、より上位の調整用 IR チームに報告されることが多いです。

6.3.2 技術情報

クラウドサービスプロバイダは、多くの顧客にサービスを提供しているため、攻撃者は同じ弱点を利用して複数のクラウドサービスプロバイダの顧客を侵害することがよくあります。クラウドサービス利用

者/クラウドサービスプロバイダは、攻撃や新たな脅威に関する技術的な詳細を抽出すると、そのデータを配布して特定の攻撃に対する防御を強化することができます。

今日のデジタル経済では、スピードと効率が不可欠です。サイバー犯罪者の行動の速さは、ネットワークを攻撃から守ることを使命としている者にとっては不安材料となります。進化する脅威に対応するためには、より多くのセキュリティ・インテリジェンスを同業他社と共有する必要があります。企業は内部のインジケータを収集することで価値を得ることができますが、パートナー組織から受け取ったインジケータを分析したり、内部のインジケータを外部の分析や利用のために共有することで、さらなる価値を得ることができます。組織は、自分たちが見たことのないインシデントに関する外部のインジケータデータを受け取った場合、そのインジケータデータを使用して、インシデントが発生した時点でそのインシデントを特定することができます。同様に、組織は外部のインジケータデータを利用して、特定のインジケータデータを捕捉するための内部リソースが不足していたために気付かなかった進行中のインシデントを検知することができます。

技術的なインジケータデータは、組織が実際のインシデントを特定するために有用です。しかし、外部ソースから受信したすべてのインジケータデータが、受信した組織に関連するとは限りません。外部データは、受信した組織のネットワーク内で"False Positive"を発生させ、存在しない問題に不必要なリソースを割り当てる原因となることがあります。

組織は、内部のインジケータを収集することで価値を得ることができますが、パートナー組織のインジケータを分析したり、内部のインジケータを外部の分析や利用のために共有することで、さらに価値を得ることができます。組織は、自分たちが見たことのないインシデントに関する外部インジケータデータを受け取った場合、そのインジケータデータを利用して、インシデントが発生し始めた時点でそのインシデントを特定することができます。同様に、組織は外部のインジケータデータを利用して、内部のリソースが不足しているために気付かなかった進行中のインシデントを検知することができます。また、組織は内部のインジケータデータを外部の組織と共有することで、利益を得ることができます。

組織は、可能な限り多くの情報を共有すべきです。しかし、セキュリティ上の理由や責任上の理由から、悪用された脆弱性の詳細を伏せることができる場合があります。

技術的なインジケータデータは、組織が実際のインシデントを特定できる場合に有用です。しかし、外部ソースのインジケータデータのすべてが、そのデータを受け取った組織に関係するとは限りません。場合によっては、このような外部データが受信側の組織のネットワーク内で偽陽性を発生させ、存在しない問題に不必要なリソースを割り当てることになります。

6.3.3 CSP ダッシュボード

クラウドセキュリティプロバイダ は、インシデントをユーザに通知するセルフサービスのカスタマイズ可能なダッシュボードを提供し、顧客に最新情報を提供する必要があります。これらのダッシュボードは通常、多数の顧客に影響を与えるインシデントを伝えるために使用されます。クラウドセキュリティプロバイダは、クラウド警告をカスタマイズし、関連するインシデントの分析、クラウド・リソースの影響の監視、ガイダンスやサポートの提供、詳細や最新情報の共有のためのパーソナライズされたダッシュボードを作成するための構成オプションもサポートする必要があります。これらのダッシュボードは、クラウド・リソースに関する単一の情報源として設計することができ、ユーザは自身に影響を及ぼす可能性のある問題をより明確に把握することができます。

6.4 机上演習とインシデントシミュレーション

一握りの先進的な企業を除いて、ほとんどの企業が具体的な「現実の世界」での経験をもとにセキュリティインシデントに備えることは困難です。現実的な演習では、無害な（しかし本物の）セキュリティ脆弱性を導入し、外部からの攻撃をシミュレートすることで、組織の準備状況を評価します。このような活動では、少数の組織チームが演習を認識します。それ以外の人には、演習はありません。あるのは、本当のセキュリティインシデントです。

机上演習には、攻撃シナリオの純粋なシミュレーションと、セキュリティインシデントの準備活動の価値があります。机上演習では、模擬的なインシデントシナリオへの対応プロセスを参加者に指導することで、組織が様々なセキュリティ・インシデント・シナリオを検討し、潜在的なサイバー脅威に備えることができます。この体験は、参加者に実践的なトレーニングを提供し、インシデントレスポンスプロセスの欠陥を浮き彫りにすることができます。

机上演習は、どのような組織でも行うことができるはずです（高度な技術力と運用能力を必要とする顧客環境にバグを導入するのとは異なり）。さらに、机上演習は、「実世界」でのシミュレーションに比べて、はるかに少ないリソースで行うことができます。

机上演習は、インシデント発生時に、インシデンスレスポンスの全体的な態勢やチーム全体の準備と意思決定プロセスを改善するのに役立ちます。演習では、まずインシデントレスポンス計画を作成し、それに対するチームのパフォーマンスを評価します。ほとんどの組織はクラウドセキュリティインシデントに対する準備ができていないため、十分に実行された IR 計画を持つことが重要です。

7. サマリー

ベンジャミン・フランクリンの言葉に「準備を怠れば、失敗する準備をすることになる」というものがあります。

多くの点で、サイバー攻撃の脅威にさらされている企業にとって、この所感は的を射ています。企業は、いかなる潜在的なインシデントに備えるために、インシデンスレスポンスプロセスと自社のインシデンスレスポンス能力についてしっかりと理解しておく必要があります。

このドキュメントでは、クラウドインシデントレスポンスフレームワークと、インシデントに効果的に対応するために必要な準備について説明しました。クラウドインシデントレスポンスフレームワークは、クラウドサービスカスタマがクラウドインシデントの準備と管理を、破壊的イベントのライフサイクル全体を通して行うための基本的なガイドとなります。また、クラウドサービスプロバイダとクラウドサービスカスタマがクラウドのインシデンスレスポンス方法を共有するための透明性のある共通のフレームワークを提供しています。

クラウドインシデントレスポンスフレームワークは、4 つのフェーズで構成されています（加えて、最後に調整と情報共有のセクションがあります）。

準備は、クラウドのインシデントが発生する前に必要な戦略と行動を処理します。効果的なインシデンスレスポンス計画には、クラウドインシデントレスポンスチーム（CIRT）の結成、戦略の立案と準備、手順の策定、技術的な準備、コミュニケーションプランの作成などが含まれます。

検知と分析では、クラウドのインシデントを早期に発見するために、様々な兆候や考えられる原因を取り上げています。また、根本的な原因を特定するためには、複数の手段を検討します。また、インシデントの早期通知のスピード（およびビジネスへの影響に基づく解決のタイミング）についても、クラウドサービスプロバイダ/クラウドサービスカスタマが考慮すべき点として取り上げています。

「封じ込め」「根絶」「復旧」では、調査やフォレンジックが行われている間に、攻撃者によるシステムへのさらなる被害を阻止するための適切な戦略を選択することが重要です。

事後分析プロセスでは、人員、プロセス、または技術のギャップを特定し、これらを準備段階で取り込まなければならない「教訓」に変換します。この終結段階の主な目的は、将来のインシデント処理を改善することです。企業のセキュリティ能力を向上させるためには、クラウドサービスプロバイダ（該当する場合）のインシデント／フォレンジックサポート、イベント分析をサポートするための利用可能な技術ツール、行為者が使用する攻撃手口、フォレンジック調査の実施などを検討することが重要です。

「調整と情報共有」では、クラウドに対する脅威が複雑に絡み合っているため、損失を軽減するために関係者がセキュリティ情報を調整・共有する必要があることを説明しています。

結論として、このフレームワークは、クラウドサービスカスタマがセキュリティ要件と適切なインシデント保護レベルを 決定する際の指針となります。さらに、クラウドサービスカスタマはこのフレームワークを利用して クラウドサービスプロバイダやサードパーティと交渉し、能力や責任の分担を確認することができます。