

---

# NIST サイバーセキュリティ フレームワーク (CSF)

AWS クラウドにおける NIST CSF への準拠

---

2019年 1月



【セキュアなクラウドの採用】



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

## 注意

本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品および対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。



# 目次

要約 .....	3
対象読者 .....	1
はじめに .....	1
NIST CSF の採用がもたらすセキュリティ上のメリット .....	3
NIST CSF 導入のユースケース.....	4
医療.....	4
金融サービス.....	4
各国の採用状況.....	4
NIST CSF への準拠を可能にする AWS サービス.....	5
CSF のコア機能: 識別 .....	6
CSF のコア機能: 防御.....	10
CSF のコア機能: 検知.....	12
CSF のコア機能: 対応.....	14
CSF のコア機能: 復旧.....	16
AWS サービスにおける CSF への準拠 .....	18
まとめ.....	19
付録 A – CSF への準拠に関する AWS サービスの責任範囲とお客様の責任範囲のマトリクス .....	20
付録 B – 第三者評価機関の検証 .....	21

## 要約

世界各地の政府、産業界、組織において、NIST サイバーセキュリティフレームワーク (CSF) がサイバーセキュリティの推奨ベースラインであり、システムのサイバーセキュリティリスク管理およびレジリエンスの改善に有効であるという認識が徐々に高まっています。このホワイトペーパーでは、NIST CSF の評価と、NIST CSF への準拠によるサイバーセキュリティ体制の改善に向けて公的部門および商業部門のお客様が使用できるさまざまな AWS クラウドサービスの評価を行います。また、AWS サービスが NIST CSF のリスク管理手法に準拠しており、AWS 全体にわたってお客様のデータを適切に保護できることを確認する第三者機関による証明も紹介します。



## 対象読者

本文書の対象読者は、組織へのサイバーセキュリティフレームワークの新規導入または導入済みのサイバーセキュリティフレームワークの改善に向けて、その方策を検討しているサイバーセキュリティ専門家、リスク管理担当者、その他の組織全体の意思決定者です。本文書および関連する[お客様向けワークブック](#) (付録 A を参照) で取り上げている AWS サービスの構成方法の詳細については、担当の [AWS ソリューションアーキテクト](#) にお問い合わせください。

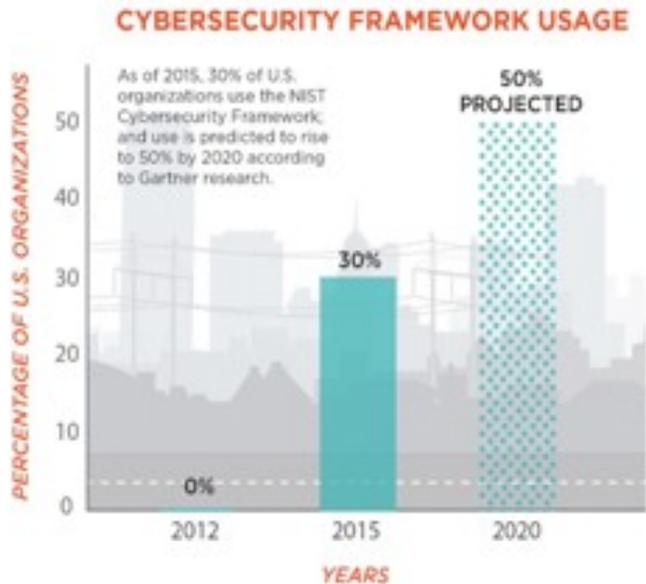
## はじめに

NIST 発行の「重要インフラのサイバーセキュリティを改善するためのフレームワーク」(NIST サイバーセキュリティフレームワーク (CSF)) は、米国大統領令 13636 号「重要インフラのサイバーセキュリティの改善」を受けて、2014 年 2 月に初版が発行されたものです。同大統領令では、システムのサイバーセキュリティ、リスク管理、レジリエンスを改善しようとする組織を支援するため、自発的フレームワークの開発が要請されています。NIST は、合意に基づく一連の強固なガイドラインおよび実施手順を策定するために、政府、産業界、学界の広範な関係者と 1 年以上にわたって協議を重ねました。

2014 年の米国サイバーセキュリティ強化法は、2017 年 5 月 11 日に署名された大統領令「連邦政府のネットワークおよび重要インフラのサイバーセキュリティ強化」によって米国のすべての連邦機関に CSF の採用が義務付けられるまで、CSF および法律への CSF の自発的採用を成文化することにより、CSF の正当性と権威を強めるものでした。

CSF を構成している一連の基礎的なサイバーセキュリティ規則は、重要インフラでの採用を意図したものではありませんが、政府および産業界では、部門や規模を問わず、あらゆる組織で用いる推奨ベースラインとして支持されています。産業界では、CSF が徐々にサイバーセキュリティのデファクトスタンダードとして参照されつつあります。

2018 年 2 月、国際規格機構 (ISO) は、"ISO/IEC 27103:2018 — Information technology— Security techniques -- Cybersecurity and ISO and IEC Standards." を発行しました。この Technical report では、既存の規格を活かしてサイバーセキュリティフレームワークを実装するためのガイドラインが提供されています。実際に、ISO 27103 では NIST CSF に盛り込まれているものと同じ概念やベストプラクティスが奨励されています。具体的には、セキュリティ対策を 5 つの機能 (識別、防御、検知、対応、復旧) と基本的なアクティビティに編成したものであり、既存の規格、認定、フレームワークとも重なる部分があります。このアプローチを採用すると、セキュリティ対策を実現できる一方で、毎回やり直すのではなく、再利用することで効率が高まるというメリットも得られます。



著作権: Natasha Hanacek/NIST <https://www.nist.gov/industry-impacts/cybersecurity>

スクを管理し、低減するための標準」として参照されています。2016 会計年度の FISMA 議会報告によれば、米国監察総監評議会 (CIGIE) は、監察総監 (IG) 評価指標を CSF の 5 つの機能に準拠したものとしています。目的は、政府機関における取り組みの状況を評価し、最高情報責任者 (CIO) や監察総監による評価において、一貫性のある比較可能な評価指標および基準の使用を奨励することです。

CSF のごく一般的な応用例としては、以下の 3 つのシナリオがあります。

1. CSF モデルと照らし合わせた評価を実施することにより、組織における、全社規模のサイバーセキュリティ体制および成熟度 (現在のプロファイル) を評価する。目標とするサイバーセキュリティ体制 (ターゲットプロファイル) を決定し、ターゲットプロファイルの実現に向けてリソースや取り組みを計画し、優先順位を設定することが目的。
2. CSF のカテゴリおよびサブカテゴリに合致したセキュリティ目標を達成するため、現行の製品やサービスおよびその導入案を評価する。機能のギャップを洗い出し、効率化に向けて、機能の重複を減らす余地がないかどうかを見きわめることが目的。
3. セキュリティチーム、プロセス、トレーニングを改革するための参考情報。

このホワイトペーパーでは、米国の連邦/州/出先機関、グローバル規模の重要インフラの所有組織および運用組織、グローバル規模の民間企業が、CSF への準拠 (クラウドのセキュリティ) に向けてグローバルに活用できる AWS サービスの重要な機能を紹介します。

1 <https://www.nist.gov/industry-impacts/cybersecurity>

2 同ページ。



また、FedRAMP Moderate<sup>3</sup> および ISO 9001/27001/27017/27018<sup>4</sup> を含むコンプライアンス基準を尺度として、AWS クラウドサービスが CSF に準拠していること (クラウド自体のセキュリティ) が第三者評価機関によって検証済みであるという裏付けも示します。つまり、AWS サービスによって、CSF で規定されているセキュリティ上の目標および成果を確実に達成できるというだけでなく、CSF および義務付けられているコンプライアンス基準への準拠についても AWS のソリューションを利用して確実に達成できるということを意味します。特に米国連邦機関の場合は、AWS のソリューションを活用することによって FISMA の報告評価指標に容易に準拠できます。重要なワークロードを AWS クラウドに移行するにつれて、このような成果が積み重ねられ、データのセキュリティとレジリエンスに関する信頼度が高まります。

## NIST CSF の採用がもたらすセキュリティ上のメリット

CSF は、コア、ティア、プロファイルという 3 つの要素によるシンプルながら効果的な構成となっています。コアは、識別、防御、検知、対応、復旧という 5 つのリスク管理機能を支援するための、一連のサイバーセキュリティ上の実施手順、成果、技術上/運用上/管理上のセキュリティ管理策です (「参考情報」と呼ばれます)。ティアは、CSF の機能と統制の管理に関して、組織の適性と成熟度を特徴に沿って分類するものです。プロファイルは、サイバーセキュリティ体制に関する組織の現状と理想像を表現することを目的としています。これらの 3 要素を複合的に用いることで、組織がビジネスや使命におけるニーズに沿ってサイバーセキュリティリスクに優先順位を設定し、対処することが可能になります。

重要な点として、コア、ティア、プロファイルの導入について責任を負うのは、CSF を採用する組織 (政府機関、金融機関、スタートアップ企業など) であるということです。このホワイトペーパーでは、CSF のコアを支え、セキュリティ対策 (サブカテゴリ) の達成を可能にする AWS のソリューションと機能について記載します。また、FedRAMP Moderate と ISO 9001/27001/27017/27018 に基づいて認定されている AWS サービスが、どのような形で CSF に準拠しているのかについても説明します。

コアとは、広く採用され、国際的に認知されている ISO/IEC 27001、NIST 800-53、情報および関連技術のための統制目標 (COBIT)、サイバーセキュリティ評議会 (CCS) のクリティカルセキュリティコントロール (CSC) の上位 20 項目、ANSI/ISA-62443「工業用のオートメーションシステムおよび制御システムに関する標準セキュリティ」などの規格を典拠とするセキュリティ管理策のことを言います。これらは広く認知されている規格であり、CSF では、組織のニーズに最も適したコントロールカタログを使用することが奨励されています。また、CSF は、規模、セクター、国を問わないものとなるよう構成されているため、公共セクターと民間セクターの組織は、その組織の種別や所在地にかかわらず、CSF を適用できることが保証されています。

CSF では、組織のニーズに最も適した任意のコントロールカタログを使用することが奨励されています。また、CSF は、規模、セクター、国を問わないものとなるよう構成されているため、公共セクターと民間セクターの組織は、その組織の種別や所在地にかかわらず、CSF を適用できることが保証されています。

- 3 FedRAMP (Federal Risk and Authorization Management Program) は、連邦政府共通のクラウドサービス調達のためのセキュリティ基準です。FedRAMP の「一度の認証を何度も用いる (do once, use many times)」というアプローチによって得られる大きなメリットとしては、セキュリティ管理策の評価における一貫性と信頼性の向上、サービスプロバイダと政府機関系のお客様にとってのコストの削減、同一のサービスを利用しようとする複数の機関で重複している認可評価の合理化などがあります。
- 4 ISO 27001/27002 は、広く採用されているグローバル規模のセキュリティ基準です。絶えず姿を変える脅威のシナリオに対応するための定期的なリスク評価に基づき、企業情報と顧客情報を管理する体系的なアプローチの要求事項とベストプラクティスを定めています。ISO 27018 は、クラウドでの個人データの保護に焦点を当てた実施基準です。ISO 27002 規格 (情報セキュリティ) に基づくもので、パブリッククラウド上の個人識別情報 (PII) に適用される ISO 27002 管理策の導入のガイドラインを定めています。また、既存の ISO 27002 管理策では対処できないパブリッククラウド上の PII 保護の要求事項に対処することを目的とした、一連の追加的な管理策および関連ガイドラインも定めています。



# NIST CSF 導入のユースケース

## 医療

米国保健福祉省 (HHS) は、1996 年の医療保険の相互運用性と説明責任に関する法令 (HIPAA)<sup>5</sup> のセキュリティルールと、NIST CSF との対応付けを完了しました。HIPAA では、保護されるべき医療情報の機密性、完全性、可用性を保証するため、適用対象である事業者およびその取引先に HIPAA セキュリティルールの順守が義務付けられます<sup>6</sup>。HIPAA には、評価または正式な認定プロセスの基準となる一連の管理策が含まれていないため、AWS など、適用対象である事業者およびその取引先は、NIST 800-53 セキュリティ管理策に準拠することで HIPAA 対応条件を満たし、検査および検証を経て、HIPAA 対応リストにサービスを掲載できるようになります。NIST CSF の一定のカテゴリに関して実施される評価は、それに対応する HIPAA セキュリティルールの要求事項に関して実施されるものと比較して具体的かつ詳しい内容となる可能性があるため、NIST CSF と HIPAA セキュリティルールの対応付けによりセキュリティがさらに高まります。

## 金融サービス

70 の金融サービス組織、機関、公共事業者/取引所で構成される米国の金融サービスセクター連携評議会<sup>7</sup> (FS-SCC) は、このセクターに固有のプロファイルを開発しました。このプロファイルでは、金融サービスセクター特有の局面と規制上の要求事項に対処するために NIST CSF の内容が改訂されています。規制当局と共同で草案が作成された [The Financial Services Sector Specific Cybersecurity profile] は、サイバーセキュリティ関連の規制上の要求事項を他の要求事項と統合化するための手立てです。たとえば、FS-SCC は「リスク管理戦略」カテゴリを 9 項目の規制上の要求事項と対応付けて、表現と定義が異なっているものの、概して同一のセキュリティ目標に対処するものであると決めました。

## 各国の採用状況

米国以外の多くの国で、NIST CSF を民間セクターおよび公共セクター向けに活用しています。イタリアは NIST CSF をいち早く採用し、5 つの機能に照らし合わせて国家サイバーセキュリティ戦略を策定しました。英国では 2018 年 6 月に、すべての政府部門に義務付けられる最小サイバーセキュリティ基準を CSF の 5 つの機能と対応付けました。イスラエルと日本では NIST CSF を自国語に翻訳し、イスラエルは独自の NIST CSF 翻案文書に基づいてサイバー防衛手順を策定しました。ウルグアイは、国際的なフレームワークとの結びつきを強化するため、CSF と ISO 規格との対応付けを実施しました。スイスや、スコットランド、アイルランド、バミューダ諸島でも、公共セクターと民間セクターの組織全体で NIST CSF を使用したサイバーセキュリティおよびレジリエンスの改善に取り組んでいます。

5 HIPAA には、保護されるべき医療情報 (PHI) のセキュリティとプライバシーを保護するための規定が含まれています。PHI には、保険と請求の情報、診断データ、臨床ケアデータ、画像や検査結果などの分析結果をはじめ、個人を特定可能な各種の健康データおよび健康関連データが含まれます。HIPAA のルールは、患者および患者データに直接接触する病院、保健医療機関、雇用者提供の健康保険、研究施設、保険会社を含め、対象となる事業者に適用されます。PHI の保護に関する HIPAA 要求事項は、これらの組織の取引先にも適用されます。

6 PHI には、保険と請求の情報、診断データ、臨床ケアデータ、画像や検査結果などの分析結果をはじめ、個人を特定可能な各種の健康データおよび健康関連データが含まれます。

7 <https://www.fsscc.org/About-FSSCC>



## NIST CSF への準拠を可能にする AWS サービス

このセクションでは、CSFのコアへの対応によって「クラウドのセキュリティ」を実現する上で利用できるAWSの機能について概要を示します。付録Aには、機能のカテゴリおよびサブカテゴリに対応したAWSサービスの一覧を記載しています。これらのツールを企業テクノロジーポートフォリオの要素として統合し、革新的かつ安全な自動化されたソリューションを構築することで、サイバーセキュリティ体制の強化を促進できます。

以下の基準を満たすため、独立した第三者評価機関によってCSFコアの各「サブカテゴリ」についての評価と判定が実施されました。

- 該当するAWSサービスへの対応付けの実施
- FedRAMP Moderate または ISO 9001/27001/27017/27018 (あるいはその両方) に基づく、該当するAWSサービスの認定取得

このセクションでは、「クラウドのセキュリティ」対策に加えて、「クラウド自体のセキュリティ」の実現に向けて、AWSサービスがどのような形でCSFに準拠しているかについても確認します。第三者機関による証明とは、CSFのサブカテゴリ(具体的にはFedRAMP Moderate およびISO 9001/27001/27017/27018)に対応付けられたコンプライアンス基準を満たしていることを根拠として、AWSサービスがCSFに準拠していることを立証するものです。つまり、CSFで規定されているセキュリティ上の目標をAWSサービスによって確実に達成できるだけでなく、AWSのソリューションを利用することにより、セキュリティおよびレジリエンスに関してCSFで規定されているベストプラクティスおよび成果についても確実に達成できます。

このホワイトペーパーは、ビジネス上および使命上の目標をサイバーセキュリティ関連のアクティビティへと結びつけて、組織のライフサイクルにおけるリスク管理を実現するためのリソースとなるものですが、AWS環境に移行しようとしているお客様や(AWSクラウド導入フレームワーク)、AWS上で実行されるソリューションを設計、構築、最適化しようとするお客様向けに(Well-Architectedフレームワーク)、その他のベストプラクティスのリソースも提供しています<sup>8</sup>。これらのリソースは、クラウドにおけるサイバーセキュリティリスク管理のプログラム、プロセス、実施手順を確立して成熟度を高めようとする組織を後押しする補完的な手立てになります。具体的には、クラウドにおけるCSFのセキュリティ対策を達成するためのオーバーレイとしてクラウド導入フレームワークまたはWell-Architectedフレームワークを用いた上で、このNIST CSF用ホワイトペーパーを前述のベストプラクティスガイドのいずれかと併用すると、セキュリティプログラムの基盤を形成できます。

クラウドに移行しようとしているお客様は、AWSクラウド導入フレームワーク(AWS CAF)のガイドラインに従うことにより、クラウドコンピューティングで提供されるサービスを最大限に活用するためにスキルの更新、既存プロセスの調整、新規プロセスの導入をどのようにして行うかを各部門に知識として浸透させることができます。

世界各地の数千の組織がAWS CAFを取り組みの指針としてすでに利用し、AWS環境へのビジネス移行を完了しています。AWSおよびAWSパートナーは、知識獲得と移行のためのあらゆるステップについて、有用なツールとサービスを提供しています。

[https://d1.awsstatic.com/whitepapers/aws\\_cloud\\_adoption\\_framework.pdf](https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf)

<sup>8</sup> AWS Well-Architected フレームワークは、信頼性、安全性、効率、費用対効果に優れたシステムをクラウドで設計して運用するためのアーキテクチャに関するベストプラクティスを文書化したものです。一連の基本的な質問が提示され、具体的なアーキテクチャがクラウドのベストプラクティスに準拠しているかどうかを把握できます。

[https://d1.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)



識別	防御	検知	対応	復旧
資産管理	アクセス制御	異常とイベント	対応計画の作成	復旧計画の作成
ビジネス環境	意識向上および トレーニング	セキュリティの継続的な モニタリング	コミュニケーション	改善
ガバナンス	データセキュリティ	検知プロセス	分析	コミュニケーション
リスク評価	情報を保護するための プロセスおよび手順		低減	
リスク評価戦略	保守		改善	
サプライチェーン リスク管理	保護技術			



**サブカテゴリ**  
(108 の結果に基づく  
セキュリティアクティビティ)

## CSF のコア機能: 識別

このセクションでは、「識別」機能を構成する 6 つのカテゴリである、資産管理、ビジネス環境、ガバナンス、リスク評価、リスク管理戦略、サプライチェーンリスク管理を取り上げます。これらは、「システム、人員、資産、データ、機能に対するサイバーセキュリティリスク管理を組織で把握する」ためのものです。AWS サービスと個々の「サブカテゴリ」との詳細な対応付け、AWS とお客様の責任範囲に関しては付録 A に記載しています。

### CSF のコア機能「識別」のサブカテゴリ:

**資産管理 (ID.AM):** 組織のビジネス目的達成を可能にするデータ、要員、デバイス、システム、施設を、ビジネス上の目標および組織のリスク戦略から見た相対的な重要度と矛盾しない形で識別し、管理します。

**ビジネス環境 (ID.BE):** 組織の使命、目標、利害関係者、アクティビティを理解し、優先順位を設定します。この情報は、サイバーセキュリティの役割、責任範囲、リスク管理上の意思決定を通知するために使用します。

**ガバナンス (ID.GV):** 組織の規制上の要求事項、法的要求事項、リスク上の要求事項、環境上の要求事項、運用上の要求事項が理解されているかどうかを管理および監視し、サイバーセキュリティリスクをシニアマネジメント層に通知するための方針、手順、プロセスです。

**リスク評価 (ID.RA):** 組織の運営 (使命、機能、イメージ、社会的評価を含む)、組織の資産、個人に対するサイバーセキュリティリスクを組織が把握することです。

**リスク管理戦略 (ID.RM):** 組織の優先順位、制約、リスク許容度、前提を明確化し、運用リスクに関する意思決定の裏付けとして利用します。

**サプライチェーンリスク管理 (ID.SC):** 組織の優先順位、制約、リスク許容度、前提を明確化し、サプライチェーンリスクの管理に関する意思決定の裏付けとして利用します。組織は、サプライチェーンリスクを識別、評価、管理するためのプロセスを確立し、導入しています。



## お客様の責任範囲

効果的な IT ガバナンスとセキュリティの第一歩は IT 資産を識別して管理することですが、これはきわめて困難な作業でもあります。Center for Internet Security (CIS)<sup>9</sup> は資産インベントリの根本的な重要性を認識し、物理的および論理的な資産のインベントリを上位 20 項目の管理策の 1 番目および 2 番目としています。一方で、物理的な資産と論理的な資産の両方について正確な IT インベントリを作成し、維持管理する作業は、組織の規模やそのリソースの種類や数に関係なく、困難な作業です。組織のすべての IT 資産を識別して報告するというインベントリソリューションの能力は、さまざまな理由から限定的なものとなっています。たとえば、ネットワークがセグメント分けされているために企業ネットワークの各所を参照して報告することができない、エンドポイントソフトウェアエージェントを全体にわたってデプロイまたは運用することができない、多種多様なテクノロジーの間に互換性がないといった理由です。不都合なことに、そうした「埋もれた」(つまり、詳細不明の) 資産は、最大のリスク要因になります。そのような資産の追跡を行っていない場合、最新のパッチやアップデートを受け取れなかったり、寿命になっても資産が交換されなかったりする可能性が高くなります。その場合は、マルウェアによる資産の悪用や掌握が容易になってしまいます。

AWS への移行によって得られる 2 つの重要なメリットを活かすと、オンプレミス環境内の資産インベントリの維持管理に伴う課題を低減できます。まず、AWS クラウドインフラストラクチャを構成している物理的な資産の管理を AWS が全面的に担うようになります。つまり、ワークロードが AWS でホストされているお客様の場合、物理的な資産の管理という負担を大幅に低減できます。お客様の環境に残す装置の物理的な資産インベントリについては、引き続きお客様が維持管理します (データセンター、オフィス、デプロイ済みの IoT、モバイルワーカーなど)。2 つ目のメリットとして、お客様の AWS アカウントでホストされている論理的な資産を深いレベルまで可視化し、資産インベントリを作成することができます。これは大胆な主張であるかのように映るかもしれませんが、EC2 インスタンス (仮想サーバー) がオンとオフのどちらであるか、エンドポイントエージェントがインストールされ実行されているかどうか、資産がどのネットワークセグメントにあるかといった要素に無関係であることから、事実であることはすぐに明らかになります。ポイント操作とクリック操作による視覚的なインターフェイス、コマンドラインインターフェイス (CLI)、アプリケーションプログラミングインターフェイス (API) のいずれかで AWS コンソールを使用しているかにかかわらず、AWS サービス資産をクエリして可視化できます。結果として、インベントリに関するお客様の負担は、EC2 インスタンスにインストールするソフトウェアおよび AWS に格納するデータ資産のみに軽減されます。また、AWS には、この機能を実行できる Amazon Macie<sup>10</sup> などのサービスも用意されています。Amazon Macie では、Amazon S3 に格納されているデータの識別、分類、ラベリング、ルール適用が可能です。

自組織の使命、利害関係者、アクティビティを把握していれば、複数の AWS サービスを利用してプロセスを自動化し、IT システムに対してビジネスリスクを割り当て、ユーザーの役割を管理できます。たとえば、Identity and Access Management (IAM) を利用して、要員やサービスのビジネス役割に基づいてアクセス役割を割り当てるのが可能です。サービスとデータにタグを付加すると、自動化されたタスクに優先順位を設定し、事前設定済みのリスクに関する意思決定および担当者のストップゲートを導入することによって、提示されるデータを評価し、システムが進むべき方向を決定できます。

<sup>9</sup> <https://www.cisecurity.org/controls/>

<sup>10</sup> <https://aws.amazon.com/jp/macie/>



ガバナンスは、サイバーセキュリティにおける「陰の立役者」です。ガバナンスによって、要員、プロセス、テクノロジーの基盤を確立し、基準を設定します。AWS は、AWS IAM、AWS Organizations、AWS Config、AWS Systems Manager、AWS Service Catalog をはじめとするさまざまなサービスや機能を提供しています。これらを利用してガバナンスを導入、監視、強制することができます。AWS は FedRAMP、ISO、PCI DSS<sup>11</sup> などの 50 を超える規格に準拠しており、お客様はこのメリットを活かすことができます。リスクとコンプライアンスプログラムに関して AWS が提供する情報を利用すると、AWS の管理策をお客様のガバナンスフレームワークに取り入れることが可能になります。この情報は、AWS を重要な要素として位置付け、統制とガバナンスのフレームワーク全体を文書化する上で有用です。Amazon Inspector などのサービスを利用すると、テクノロジー上の脆弱性を識別して、リスク対応の把握と管理のプロセスに提供できます<sup>12</sup>。クラウドが提供する情報の可視性が高まるため、お客様のリスク対応把握の精度が向上して、より実態的なデータに基づいてリスクに対する意思決定を行えるようになります。

## AWS の責任範囲

AWS は、業務遂行上、正当な理由で特権が必要となる従業員および請負業者に対してのみ、データセンターへのアクセスおよび情報を提供することによって、厳格なアクセス制御管理を維持しています。従業員は、業務遂行上、当該の特権が不要となった時点でただちにアクセス権が取り消されます。これは、引き続き Amazon またはアマゾン ウェブ サービスの従業員である場合も同様です。AWS の従業員によるデータセンターへの立ち入りは、規定に沿ってすべてログに記録され、監査されます。所定の統制によってシステムおよびデータへのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO 27001、PCI、ITAR、FedRAMP の監査中に独立監査人によって確認されます。

AWS のリスク管理アクティビティには、システム開発ライフサイクル (SDLC) が含まれています。このサイクルには業界のベストプラクティスが採用されており、AWS セキュリティチームによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS のシニアマネジメント層は、リスクを低減または管理するために、リスクの特定や管理策の導入など、戦略的な事業計画を開発してきました。また、少なくとも半年に一度、この戦略的な事業計画を再評価しています。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS 統制環境は、さまざまな内部および外部の監査とリスク評価の対象となります。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて情報セキュリティフレームワークと方針を確立し、ISO 27002 の管理策、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services

11 PCI DSS (PCI データセキュリティスタンダード) は機密情報に関するセキュリティ基準であり、American Express、Discover Financial Services、JCB International、MasterCard Worldwide、Visa Inc. が設立した PCI Security Standards Council (<https://www.pcisecuritystandards.org/>) によって管理されています。PCI DSS は、加盟店、プロセッサ (決済処理代行事業者)、カード会社、サービスプロバイダを含め、カード所有者データ (CHD) や機密認証データ (SAD) を保存、処理、転送するすべての団体に適用されます。

12 <https://aws.amazon.com/jp/inspector/>



Principles)、PCI DSS 3.2 版、米国国立標準技術研究所 (NIST) 出版物 800-53 Rev4 (Recommended Security Controls for Federal Information Systems) に基づいて ISO 27001 認証フレームワークを実質的に統合しています。AWS は、セキュリティ方針を維持し、従業員に対するセキュリティトレーニングを提供し、アプリケーションのセキュリティレビューを実施しています。これらのレビューは、情報セキュリティ方針に対する適合性に加え、データの機密性、完全性、可用性を評価するものです。

AWS セキュリティは、インターネットに接続しているすべてのサービスエンドポイントの IP アドレスを対象として、脆弱性の有無を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。脆弱性が見つかったら、修正のために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実施されます。これらの評価で得られた発見や推奨事項は、分類整理された上で AWS シニアマネジメント層に報告されます。これらのスキャンは、基礎となる AWS インフラストラクチャの健全性と実行可能性を確認するためのものであり、お客様固有のコンプライアンスの要求事項に適合させるためにお客様自身が行う脆弱性スキャンの代わりとなるものではありません。

AWS では、主要なサードパーティーサプライヤーと正式な契約を締結し、ビジネスでの関係に合わせた適切なリレーションシップ管理メカニズムを実装しています。AWS のサードパーティ管理プロセスは、SOC および ISO 27001 規格への AWS の継続的な準拠の一環として、独立監査人によって確認されます。ISO 27001 規格に合わせて、AWS の担当者が AWS 独自のインベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤーとの関係を維持しています。詳細については、ISO 27001 規格の附属書 A ドメイン 8 を参照してください。AWS は、ISO 27001 認証規格への適合を評価する独立監査人から、審査および認証を受けています。



## CSF のコア機能: 防御

このセクションでは、「防御」機能を構成する 6 つのカテゴリである、アクセス制御、意識向上およびトレーニング、データセキュリティ、情報を保護するためのプロセスおよび手順、保守、保護技術を取り上げます。また、この機能の要求事項に準拠する上で利用できる AWS ソリューションも紹介します。AWS サービスと個々の「サブカテゴリ」との詳細な対応付け、AWS とお客様の責任範囲に関しては付録 A に記載しています。

### CSF のコア機能「防御」のサブカテゴリ:

**アイデンティティ管理とアクセス制御 (PR.AC):** 物理的な資産と論理的な資産、関連施設にアクセスできるのは正当な権限のあるユーザー、プロセス、デバイスのみ限定され、正当な権限のあるアクティビティやトランザクションへの不正アクセスに関して想定されている、評価済みのリスクに矛盾しない形で管理されている。

**意識向上およびトレーニング (PR.AT):** 組織の要員およびパートナーに対して、サイバーセキュリティに関する意識教育が提供され、関連する方針、手順、取り決めに従ってサイバーセキュリティ関連の義務および責任を果たすためのトレーニングが実施されている。

**データセキュリティ (PR.DS):** 情報およびレコード (データ) が組織のリスク戦略に従って管理され、情報の機密性、完全性、可用性が保護されている。

**情報を保護するためのプロセスおよび手順 (PR.IP):** セキュリティ方針 (目的、範囲、役割、責任、経営者のコミットメント、組織間の連携を取り扱ったもの)、プロセス、手順が維持管理され、情報システムと資産の保護を管理するために利用されている。

**保守 (PR.MA):** 工業用制御システムと情報システムを構成している要素の保守および修理が、方針および手順に従って実施されている。

**保護技術 (PR.PT):** システムと資産のセキュリティおよびレジリエンスを確保するために、関連する方針、手順、取り決めに従って技術的なセキュリティソリューションが管理されている。

## お客様の責任範囲

機密性、完全性、可用性という 3 つのセキュリティ目標を達成しようとするとき、可用性については、データセンターが 1 か所もしくは 2 か所しかないオンプレミス環境の場合はきわめて困難になり得ます。大規模なクラウドサービスプロバイダ、特に AWS では、他に類を見ないアーキテクチャのインフラストラクチャを採用しているため、この点に関して大きなメリットを得られます。リージョン内で障害を分離するための論理ゾーンである複数のアベイラビリティゾーン (AZ) にアプリケーションを分散できます。高度なキャパシティー管理と自動スケーリングの機能を実装した上で適切にアーキテクチャを構成した場合、1 か所のデータセンターが稼働停止となっても、アプリケーションやデータは影響を受けません。3 つ以上の AZ が存在しているリージョン内ですべての AZ を利用すると、2 か所のデータセンターが稼働停止に陥った場合も、アプリケーションが影響を受けることはありません。同様に、Amazon Simple Storage Service (S3) などのサービスでは、リージョン内の 3 つ以上の AZ にお客様のデータが自動でレプリケートされ、99.99% の可用性と 99.999999999% のデータ耐久性が保証されます。



機密性を実現するためには、保存時や転送時に Elastic Block Store (EBS) 暗号化、S3 暗号化、RDS においては SQL Server および Oracle の Transparent Database Encryption、VPN ゲートウェイなどの AWS の暗号化サービスを使用するか、お客様の既存の暗号化ソリューションを使用します。AWS では、すべての API エンドポイントで TLS/SSL 暗号化がサポートされており、VPN トンネルを作成して転送時にデータを保護できます。また、保存時にデータを暗号化するための Key Management Service および専用設計のハードウェアセキュリティモジュールアプライアンスも提供しています。AWS 提供の機能を利用してデータを保護することも、お客様独自のセキュリティツールを利用することもできます。

完全性は、さまざまな手段で促進できます。Amazon CloudWatch と Amazon CloudTrail の完全性チェック機能、API 呼び出しとログへのデジタル署名付加機能、Amazon S3 の MD5 チェックサム機能を利用できます。さらに、AWS パートナーから数多くのサードパーティソリューションが提供されています。AWS Config で変更を監視して、お客様の AWS 環境の完全性を確認することも可能です。

お客様の AWS 環境では、AWS IAM、AWS Cognito、AWS Single Sign-On (SSO)、AWS Cloud Directory、AWS Directory Service などのサービスや Multi-Factor Authentication (MFA) などの機能を利用して、ユーザーの ID、認証規格、アクセス権限を実装、管理、保護、監視、レポートできます。

従業員およびエンドユーザーに対する、環境管理の方針と手順についてのトレーニングの実施は、お客様の責任となります。技術的なトレーニングに関しては、ソリューションアーキテクト、システムオペレーション (SysOps) 担当者、デベロッパー、セキュリティチームなど、さまざまな役割を対象とする包括的なトレーニングを AWS および AWS トレーニングパートナーが提供しています<sup>13</sup>。

## AWS の責任範囲

AWS は最小権限という概念を採用しており、従業員は、ビジネス上および職務上の必要性に基づいてアクセス権限を付与されます。提供されるのは、役割に応じた、その時々が必要となっているリソースおよびデータへの一時的なアクセス権限です。

AWS は、承認を受けた従業員に対してのみ、データセンターへの物理的なアクセスを許可します。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最小権限の原則に基づいて許可されますが、アクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物が審査して承認し、請求した期限が過ぎた後、アクセスが取り消されます。入場を許可された担当者が立ち入れるのは、その権限で指定されたエリアのみです

第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最小権限の原則に基づいて許可されますが、アクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。これらの申請は権限を持つ人物が審査して承認し、請求した期限が過ぎた後、アクセスが取り消されます。入場を許可された担当者が立ち入れるのは、その権限で指定されたエリアのみです。訪問者バッジを受け取った担当者は、現場への到着後身分証明書を提示します。署名後に入場が許可され、権限を持つ職員が常に付き添います。

AWS は、セキュリティ意識向上およびトレーニングに関して、従業員および請負業者向けの文書化された正式な方針と手順を導入済みです。この方針と手順では、目的、範囲、役割、責任、経営者のコミットメント、組織間の調整、コンプライアンスを取り上げています。

<sup>13</sup> オンラインで提供されています。クラスルームトレーニングについては、<https://aws.amazon.com/jp/training/> をご覧ください。AWS の多くの局面を取り上げたさまざまな文書が用意されています。<https://www.amazon.com> で「AWS」を検索してご覧ください。AWS のホワイトペーパーは <https://aws.amazon.com/jp/whitepapers/> で参照できます。



AWS の FedRAMP および ISO 27001 認証では、AWS の環境とインフラストラクチャに対するあらゆる変更を運用、維持、制御、承認、デプロイ、レポート、監視するための方針および手順が詳しく記載されています。AWS の物理インフラストラクチャの冗長性と緊急対応をどのように提供しているかについても説明しています。さらに、不正アクセスの防止に向けて、AWS サービスに関するあらゆるリモート保守がどのように承認、実施、記録、審査されているのかが詳しく記載されています。媒体の内容を消去し、データを破壊する方法も取り上げています。AWS は、NIST Special Publication 800-88 (媒体のサニタイズに関するガイドライン) に準拠した製品および手順を採用しています。データ保護に関する方針、プロセス、手順の準備は、お客様の責任範囲でもあります。

請求と保守の要求事項に対応するため、AWS の資産は、AWS 独自のインベントリ管理ツールを利用して所有者が割り当てられ、追跡され、監視されています。AWS 資産の所有者による保守の手順は、特定のチェック機能を備えた独自のツールを利用して実施され、文書化された保守スケジュールに沿って完了することが義務付けられています。第三者である独立監査人が、資産の所有者が文書化されていること、文書化された資産管理方針に沿って資産の状態が可視化されていることを確認して、AWS による資産の管理統制を検査します。

AWS サービスは、お客様によるシステム保守の管理および実施についても、きわめて大きな改善効果をもたらします。まず、アベイラビリティゾーン (AZ) を採用した前述の AWS インフラストラクチャを基盤として、アプリケーションが複数の AZ に分散される可用性の高いアーキテクチャとすることによって、保守作業の分離が可能になります。保守のために AZ 内の資産をオフラインにした場合も、他の AZ にある重複資産がスケールアウトして負荷を引き継ぐので、アプリケーション全体のパフォーマンスは影響を受けません。保守は一度に 1 つの AZ に対して実施可能であり、ストップゲートを利用して自動化し、必要に応じてレポートを生成できます。また、アーキテクチャ全体を開発テスト (ブルー) 環境から運用 (グリーン) 環境に切り替えることも、必要に応じてこの逆方向に切り替えることもできます。

## CSF のコア機能: 検知

このセクションでは、「検知」機能を構成する 3 つのカテゴリである、異常とイベント、セキュリティの継続的なモニタリング、検知プロセスを取り上げます。また、この機能の要求事項に準拠する上で利用できる主な AWS ソリューションの概要も紹介します。AWS サービスと個々の「サブカテゴリ」との詳細な対応付け、AWS とお客様の責任範囲に関しては付録 A に記載しています。

### CSF のコア機能「検知」のサブカテゴリ:

**異常とイベント (DE.AE):** 異常なアクティビティを的確なタイミングで検知し、当該のイベントが及ぼす潜在的な影響を把握する。

**セキュリティの継続的なモニタリング (DE.CM):** 情報システムと情報資産を別個の間隔で監視して、サイバーセキュリティイベントを洗い出し、保護手段の有効性を検証する。

**検知プロセス (DE.DP):** 異常なイベントがタイムリーかつ適切に認識されるように、検知のプロセスおよび手順を維持管理し、検査する。



## お客様の責任範囲

セキュリティ関連のイベントを収集、統合し、アラートを出す能力は、あらゆるサイバーセキュリティリスク管理プログラムの根本となるものです。クラウドテクノロジーは、APIによって駆動されるという性質上、これまで不可能であった新たなレベルの可視性と自動化を実現できます。AWS では、実行される操作ごとに監査レコードが 1 つもしくは複数生成されるため、アカウント構造内の多彩なアクティビティ情報を利用できます。ただし、データの量自体が課題になることもあります。「干し草の山に埋もれている針」という表現があるように、膨大なデータの中から必要な情報を見つける作業は容易ではありませんが、AWS 環境で提供される処理能力と機能は、そうした課題の解決に適しています。適切なログ処理インフラストラクチャ、自動化、データ解析を導入すると、フォールスポジティブや影響の小さいリスク、許容可能なリスクを除外しつつ、重大なイベントをほぼリアルタイムで検知し、それに対応できます。

AWS は、包括的なセキュリティオペレーション戦略の一環として継続的なモニタリングおよび脅威検知に利用できる多種多様なサービスを提供しています。基礎となるレベルでは、すべての API 呼び出しをログに記録する AWS CloudTrail<sup>14</sup> などのサービスがあります。ログにデジタル署名と暗号化を付加した後、安全な Amazon S3 バケットに保存できます。Virtual Private Cloud (VPC) フローログ<sup>15</sup> は、VPC を発信元および宛先とするすべてのネットワークアクティビティを監視します。お客様の AWS 環境を監視し、セキュリティ情報およびイベント管理 (SIEM) システムと同様のアラートを生成するサービスであり、お客様のオンプレミス SIEM に組み込むことが可能な Amazon CloudWatch<sup>16</sup> もあります。

また、追加的なリスクコンテキストとアノマリ検出法を得られる脅威インテリジェンスを複数のソースから取得して、AWS 環境内のアクティビティの相関関係を分析する Amazon GuardDuty<sup>17</sup> など、他の高度なサービスも提供しています。もう 1 つの高度なサービスとして、センシティブデータを特定、分類、ラベリングし、位置とアクセスを追跡できる Amazon Macie があります。お客様のご希望に応じて、AWS の人工知能 (AI) サービスおよび機械学習 (ML) サービスを利用し、ログデータをモデル化して解析することも可能です。

## AWS の責任範囲

AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。

論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。

AWS の従業員は、疑わしいセキュリティインシデントの見分け方と報告先についてトレーニングを受けています。条件に該当する場合は、インシデントが関係機関等に報告されます。AWS は、AWS サービスに影響を及ぼすセキュリティイベントおよびプライバシーイベントをお客様にお知らせする AWS Security Bulletin

14 <https://aws.amazon.com/jp/cloudtrail/>

15 [https://docs.aws.amazon.com/ja\\_jp/vpc/latest/userguide/flow-logs.html](https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/flow-logs.html)

16 <https://aws.amazon.com/jp/cloudwatch/>

17 <https://aws.amazon.com/jp/guardduty/>



ウェブページ<sup>18</sup>を運営しています。Security Bulletin の RSS フィードに登録すると、Security Bulletin ウェブページでの最新のセキュリティ通知を常に把握できます。お客様サポートチームは、可用性に広範な影響を及ぼしている問題についてお客様にアラートを出すサービス状態ダッシュボードのウェブページ<sup>19</sup>を運営しています。

## CSF のコア機能: 対応

このセクションでは、「対応」機能を構成する 5 つのカテゴリである、対応計画の作成、コミュニケーション、分析、低減、改善を取り上げます。また、この機能の要求事項に準拠する上で利用できる主な AWS ソリューションの概要も紹介します。AWS サービスと個々の「サブカテゴリ」との詳細な対応付け、AWS とお客様の責任範囲に関しては付録 A に記載しています。

### CSF のコア機能「対応」のサブカテゴリ:

**対応計画の作成 (RS.RP):** 検知されたサイバーセキュリティイベントにタイムリーかつ確実に対応できるよう、対応のプロセスおよび手順を実践し、維持管理する。

**低減 (RS.MI):** イベントの拡大阻止、影響の低減、インシデントの除去に向けたアクティビティを実施する。

**コミュニケーション (RS.CO):** 該当する場合に、司法当局による外部からの支援を含めるよう、社内および外部の利害関係者と対応アクティビティについて協議する。

**分析 (RS.AN):** 十分な対応の保証および復旧アクティビティの支援に向けて、分析を実施する。

**改善 (RS.IM):** これまでの検知/対応アクティビティから得られた教訓を採り入れて、組織の対応アクティビティを改善する。

18 <https://aws.amazon.com/security/security-bulletins>

19 <http://status.aws.amazon.com/>



## お客様の責任範囲

検知から対応までの経過時間が重要です。入念に練られた、繰り返し適用可能な対応計画を策定することで、脅威にさらされる危険性が最小限に抑えられ、復旧が迅速になります。クラウドによる自動化機能を活用すると、入念な計画書を規範として導入し、対応時間を大幅に短縮できます。

Amazon EC2 インスタンスにタグ付けするだけで、インスタンスの分離や、フォレンジックスナップショットの取得、分析ツールのインストール、疑わしいインスタンスのフォレンジックワークステーションへの接続、チケットのサイバーセキュリティアナリストへの登録などの自動化を実現できます。以下で紹介する機能を利用すると、自動プロセスの作成が容易になり、インシデント対応プロセスのスピードと一貫性を向上できます。さらに、コミュニケーション履歴を保持してイベント処理後の審査で使用できます。

AWS 環境では、情報の収集と配布を合理化して促進する機能が提供されますが、対応時には常に人を介した連携が必要になります。サイバーセキュリティ分析には、調査活動、フォレンジック、インシデントの把握が必要だからです。必然的に、一定レベルの人的な相互連携が必要になります。AWS サービスでは直接的なインシデント分析は提供されませんが、正式なプロセスの実施および影響の大きさの評価を支援するサービスが提供されています。



## AWS の責任範囲

AWS は、インシデント対応に関して、文書化された正式な方針およびプログラムを導入しています。この方針では、目的、範囲、役割、責任、経営者のコミットメントが取り上げられています。

AWS は、以下の 3 つのフェーズに分かれるインシデント管理アプローチを採用しています。

1. アクティベーションと通知のフェーズ
2. 復旧のフェーズ
3. 再構成のフェーズ

AWS のインシデント管理計画から確実な効果が得られるように、AWS はインシデント対応のテストを実施します。このテストでは、その時点の未知の不具合と障害モードについて広い範囲を検出対象としてカバーします。さらに、Amazon のセキュリティチームおよびサービスチームは、お客様への潜在的な影響の有無についてシステムをテストし、検知と分析、封じ込め、除去、復旧、インシデント処理後のアクティビティなど、インシデントの処理に携わる要員を準備することが可能になります。

インシデント対応計画と併せて、インシデント対応テスト計画を年 1 回作成します。AWS のインシデント管理の計画を作成し、テストを実施し、テスト結果は、第三者の監査人による審査を受けます。

## CSF のコア機能: 復旧

このセクションでは、「復旧」機能を構成する 3 つのカテゴリである、復旧計画の作成、改善、コミュニケーションを取り上げます。また、この機能の要件に準拠する上で利用できる主な AWS ソリューションの概要も紹介します。AWS サービスと個々の「サブカテゴリ」との詳細な対応付け、AWS とお客様の責任範囲に関しては付録 A に記載しています。

### CSF のコア機能「復旧」のサブカテゴリ:

**復旧計画 (RC.RP):** 復旧のプロセスおよび手順を実践し、維持管理して、サイバーセキュリティイベントの影響を受けたシステムまたは資産をタイムリーかつ確実に復旧する。

**改善 (RC.IM):** 得られた教訓を以後のアクティビティに採り入れて、復旧の計画およびプロセスを改善する。

**コミュニケーション (RC.CO):** 復旧のアクティビティについて、コーディネートセンター、インターネットサービスプロバイダ、攻撃側システムの所有者、被害者、他の CSIRT、ベンダーなど、社内および外部の当事者と協議する。

## お客様の責任範囲

お客様は、アプリケーションとデータの復旧オペレーションを計画、テスト、実施して、事業継続性を維持する責任を負うものとします。稼働停止に至る原因は多種多様です。AWS サービスでは、自己修復および自動復旧に利用できる高度な機能を数多く提供しています。たとえば、複数のアベイラビリティゾーンにわたる Auto Scaling グループを利用すると、EC2 インスタンスの状態をインフラストラクチャで監視して、障害が発生しているインスタンスを新しい Amazon Machine Image (AMI) ですぐに置き換えることができます。



また、Amazon CloudWatch、AWS Lambda などのサービスやサービス機能を利用すると、AWS 環境全体とアプリケーションのデプロイから、別の AWS リージョンへのフェイルオーバー、バックアップからのデータ復元などに至るまで、あらゆる復旧操作を自動化できます。

最後に、広報活動、レピュテーション管理、および復旧アクティビティの通知を含む対応措置では、組織の環境に影響を及ぼしたイベントの当該組織における取り扱い状況を表しています。この場合の組織とは、お客様です。

## AWS の責任範囲

AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。

AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の 3 フェーズのアプローチが詳しく記載されています。

- アクティベーションと通知のフェーズ
- 復旧のフェーズ
- 再構成のフェーズ

このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。

AWS は、すべてのリージョンにわたるユビキタなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント (N 個) に対して、少なくとも 1 つの独立したバックアップコンポーネント (+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルが AWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。



## AWS サービスにおける CSF への準拠

AWS は、「クラウドのセキュリティ」を実証するため、AWS クラウドサービスの CSF への準拠についての評価を実施しました。相互接続がますます進む現代社会では、相互接続される各システムに対して、厳格なサイバーセキュリティリスク管理の実施手順を適用し、データの機密性、完全性、可用性を保護することが必要不可欠です。AWS の公共セクターおよび民間セクターのお客様は、AWS クラウドサービスの保護に業界屈指のセキュリティが採用されていると考えており、そのシステムでデータの処理および保存が行われていることを期待しています。データとシステムを大規模かつ効果的に保護するには、セキュリティが後付けではなく、システムライフサイクル管理の不可分の要素となっていなければなりません。AWS のセキュリティは、フェーズ 0 (システムの運用開始時) から始まり、AWS のサービスデリバリーモデルに当初から織り込まれて継続的に提供されています。

公共セクターおよび民間セクターのお客様に現在ご利用いただける AWS ソリューションは、NIST CSF への準拠が第三者の監査人によって確認されています。これらの各サービスは、FedRAMP Moderate および/または ISO 27001 規格に基づく最新の認定を維持しています。AWS のソリューションをデプロイしようとする際に、組織は、CSF に定義されているリスク管理上のベストプラクティスを AWS サービスが順守しているという保証を得られます。また、お客様が独自に CSF に準拠しようとする際、これらのソリューションを活用できます。

AWS は、サービスのセキュリティおよびお客様データの保護に関して、リスクに基づく厳格なアプローチを実践しています。AWS のサービスについては、独自の内部セキュリティアシュアランスプロセスを実施しています。このプロセスは、サービスのレジリエンスに影響を及ぼす最新あるいは新出のセキュリティ脅威からの保護において欠かせない、管理上、技術上、運用上の統制の効果を評価するものです。AWS など、大規模な商用クラウドサービスプロバイダには、世界各地の公共セクターおよび民間セクターのお客様によって特定されたリスク事案に適切に対処するための、特定の業界向け、国内向け、または国際的なセキュリティ認証 (FedRAMP、ISO 27001、PCI DSS、SOC など) という形で、厳格なセキュリティ上の要求事項が既に適用されています。

AWS は、すべてのお客様を対象として、すべてのサービスにわたり、AWS の "high watermark" アプローチに基づく高水準のセキュリティ基準線を採用しています。つまり、AWS クラウドサービスで送受信および保存されるデータを最高位の分類レベルに設定し、それと同一レベルの保護をすべてのサービスやお客様に適用しています。これらのサービスは、最高位のコンプライアンス基準に照らして順番に認証を受けます。クラウドで処理および保存されるお客様のデータは、高いレベルの保護を受けることができます。公共セクターおよび民間セクターのお客様に現在ご利用いただける AWS ソリューションは、CSF コアへの準拠が第三者の監査人によって確認されています。これらの各サービスは、FedRAMP Moderate および/または ISO 27001 規格に基づく最新の認定を維持しています。AWS のソリューションをデプロイしようとする際に、組織は、CSF に定義されているリスク管理上のベストプラクティスを AWS サービスが順守しているという保証を得られます。また、お客様が独自に CSF に準拠しようとする際、これらのソリューションを活用できます。第三者による保証のメール文面については、付録 B をご覧ください。



## まとめ

公共セクターおよび民間セクターでは、それぞれの組織環境に NIST CSF を採用することで、セキュリティ上の効果が得られることを認識しています。特に、米国の連邦政府関係機関は、サイバーセキュリティリスク管理の手順および報告の手順を CSF 準拠とするよう指令が出されています。米国の州政府および地方自治体、米国以外の政府、重要インフラの運営事業者、営利団体が CSF への準拠を評価する際、安全で規格に準拠したシステムおよび組織のリスク対応体制を確立するには、適切なツールとソリューションが必要です。

AWS を組織のテクノロジー環境の要素として活用し、自動化された革新的かつ安全なソリューションを構築して、CSF で定められているセキュリティ対策を達成すると、サイバーセキュリティ体制を強化できます。AWS サービスは、CSF で定められている徹底的なリスク管理実施手順も採用しており、その点は第三者の監査人によって検証されていることから、さらなるセキュリティが得られます。



## 付録 A – CSF への準拠に関する AWS サービスの責任範囲とお客様の責任範囲のマトリクス

[CSF への準拠に関する AWS サービスの責任範囲とお客様の責任範囲のマトリクス](#) スプレッドシートを活用すると、NIST CSF に対するお客様の準拠の度合いが明らかになります。このスプレッドシートは、AWS コンプライアンスウェブサイトの「リソース」セクションにある「ガイドとワークブック」タブに掲載されています。



## 付録 B – 第三者評価機関の検証

2018年9月19日:  
アマゾン ウェブ サービス  
Security - Growth Strategy  
サービスデザイン担当シニアマネージャ  
Jennifer Gray 様



Kratos SecureInfo  
14130 Sullyfield Circle,  
Suite H  
Chantilly, VA 20151  
Tel: 1-888-677-9351  
[www.kratossecureinfo.com](http://www.kratossecureinfo.com)

Gray 様

ご依頼に従って、2018年4月16日付のアメリカ国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク (CSF) バージョン 1.1 で定められている要求事項を検討するタスクと、機能および規制に関する NIST CSF の記述で概説されている要求事項を AWS および関連クラウドコンピューティングリファレンスアーキテクチャとの関連において分析するタスクを担当させていただきました。これらの要求事項は、NIST Special Publication (SP) 800-53 に文書化されている NIST 策定のセキュリティ制御の要求事項で上書きされました。

検討のタスクにおいては、NIST SP 800-53 のセキュリティ制御の要求事項と対応している NIST CSF の引用部分を検証しました。AWS サービスについても、FedRAMP Moderate および ISO 9001/27001/27017/27018 認証を取得しているもので、お客様がデプロイ可能な引用部分 (つまり制御の要求事項) を満たしているものを検討しました。サービスの検証中に、利用可能な対象範囲のサービスで、要求事項を満たすものが存在するかもしれない他の引用部分を洗い出しました。ここで対象に含めることを推奨されたすべてのサービスが、AWS FedRAMP Moderate および ISO の認証の対象範囲であることが検証されました。

この分析の結果として、AWS は、現時点では特定のコンプライアンスフレームワークで要求事項となっているわけではないものの、AWS サービスを通じてこれらの引用部分 (FedRAMP および ISO の対象範囲) の目的に適合していることが判明しました。

AWS で作成した「CSF Core Mapping Workbook」の分析および当社の AWS 環境に対する解釈に基づいた Kratos SecureInfo の見解は、次のとおりです。AWS は、対応する FedRAMP および ISO のセキュリティ制御を実装することにより、NIST CSF に準拠しているということが実証されました。

私が担当した設計レビューに関してご不明な点がある場合は、(571)-308-3397 に直接お電話いただくか、[Emily.Cummins@KratosSecureInfo.com](mailto:Emily.Cummins@KratosSecureInfo.com) までメールでお問い合わせください。

敬具

Emily Cummins  
セキュリティコンサルタント主任  
Kratos SecureInfo