[AWS Black Belt Online Seminar]
AWS Artifact

サービスカットシリーズ

Head of Security Assurance, Japan
松本 照吾
2021/3/10

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

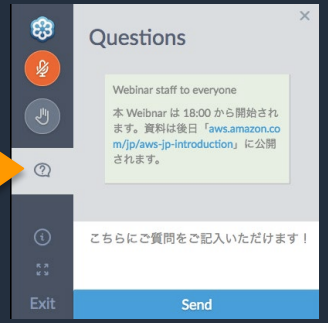
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2021年3月10日現在のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。

- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。

- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

松本照吾 （matshogo@amazon.co.jp）

アマゾン ウェブ サービス ジャパン 株式会社
セキュリティ アシュアランス本部 本部長

元PCI DSS QSA, システム監査人

好きなAWSサービス：AWS Artifact, AWS Config

ISACA東京支部 CISA委員会　委員長
JASA　クラウド監査実技WG　リーダー

CISA, CISSP, MBA
(University of Massachusetts Lowell)

本日のお話する内容

- 監査って何のため？
- AWS Artifactとは？
- AWS Artifactの利用（レポート）
- レポートの活用（SOCを中心に）
- AWS Artifactの利用（契約）

AWS Artifactは、AWSのコンプライアンス管理を効率化してくれるサービスです。

本日のお話する内容

- **監査って何のため？**
- AWS Artifactとは？
- AWS Artifactの利用（レポート）
- レポートの活用（SOCを中心に）
- AWS Artifactの利用（契約）

世の中をよりよくするためのものとしての監査

御社の財務状況を評価させてください。

御社の財務状況を詳しく知りたいので帳簿見せてください。

帳簿見るのが趣味なので、帳簿みせてください。

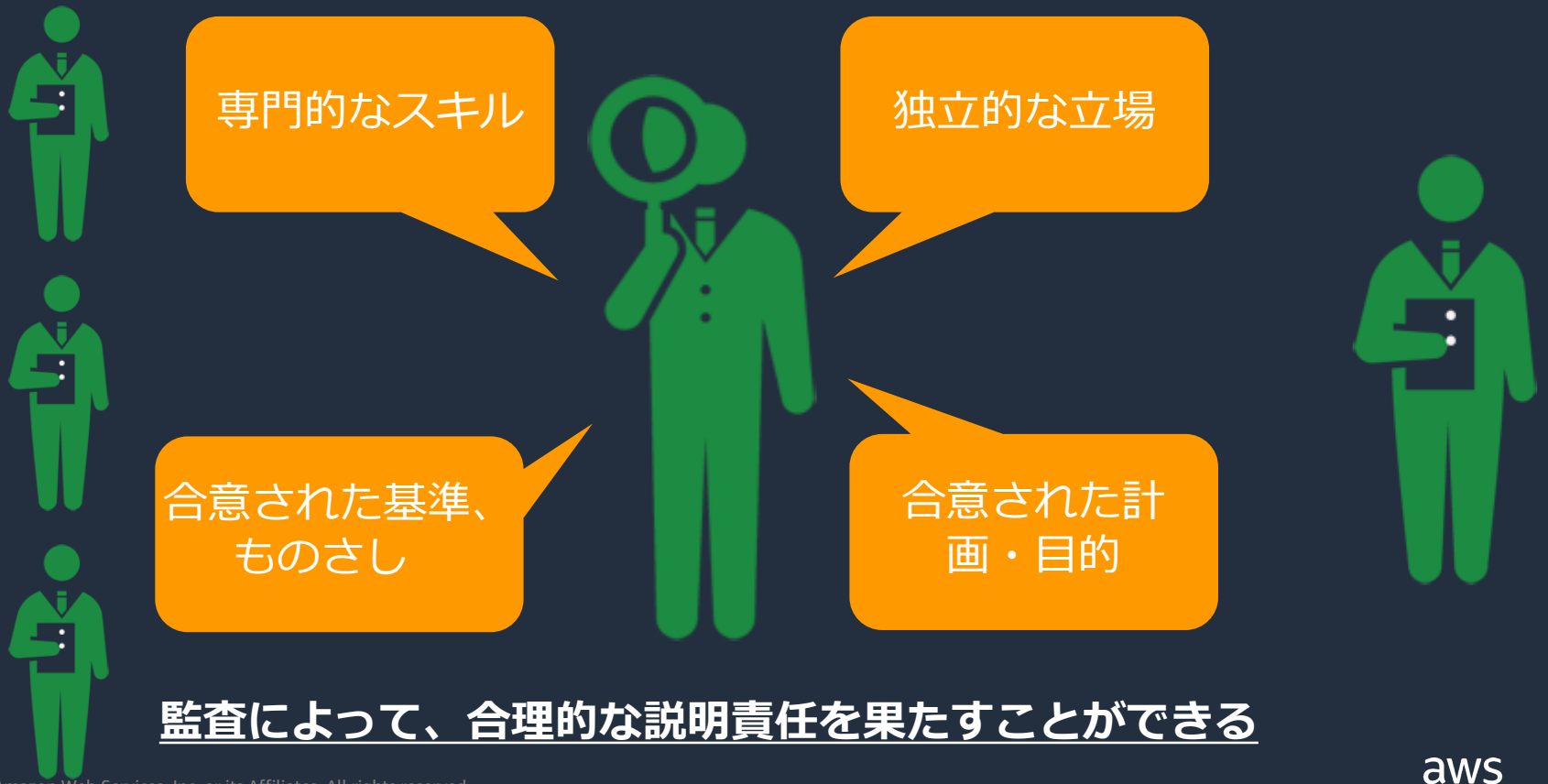
ちゃんとやっています、自分でいっても信頼性に乏しい

そこまでを開示しなければいけないのかな

対応する側もコストがかかる

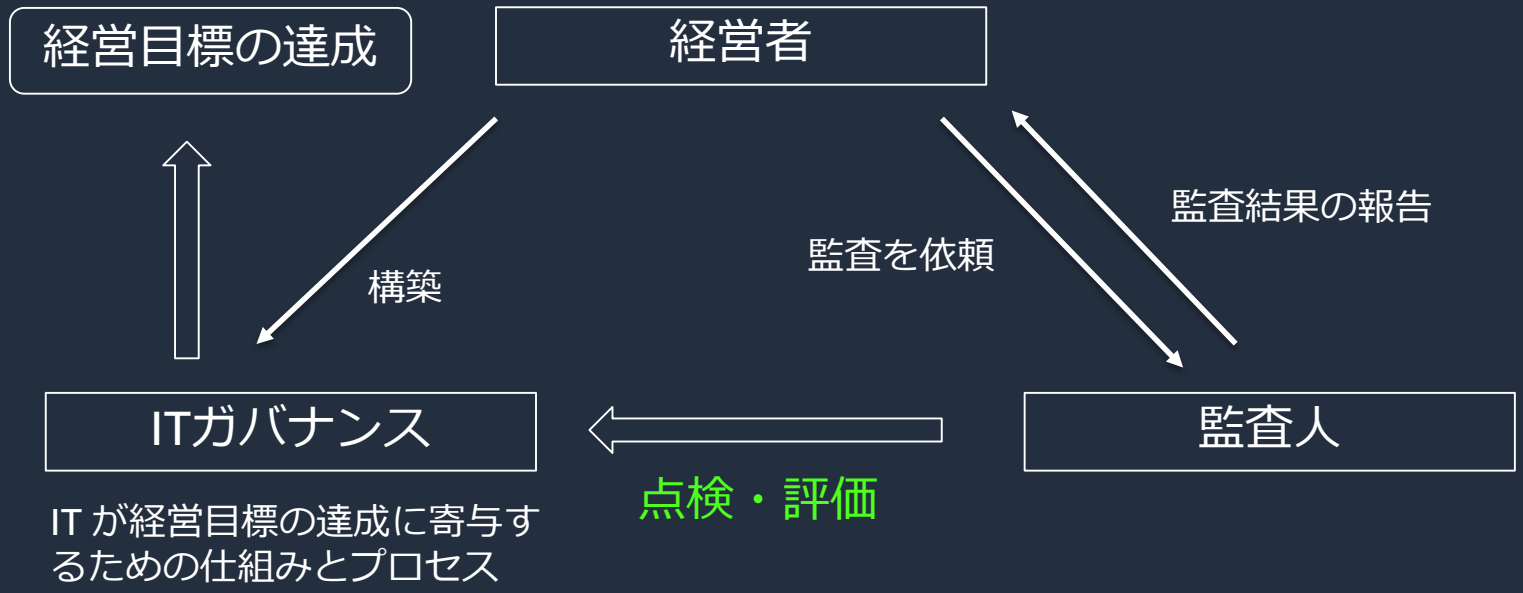
aws

世の中をよりよくするためのものとしての監査



監査によって、合理的な説明責任を果たすことができる

IT 監査/システム監査とは



個人情報保護法の施行や、金融商品取引法による内部統制報告、監査が必要になったことを背景に、経営者に代わって監査人がITガバナンスの点検、評価をして経営者に提言を行い改善をすることが必要になった

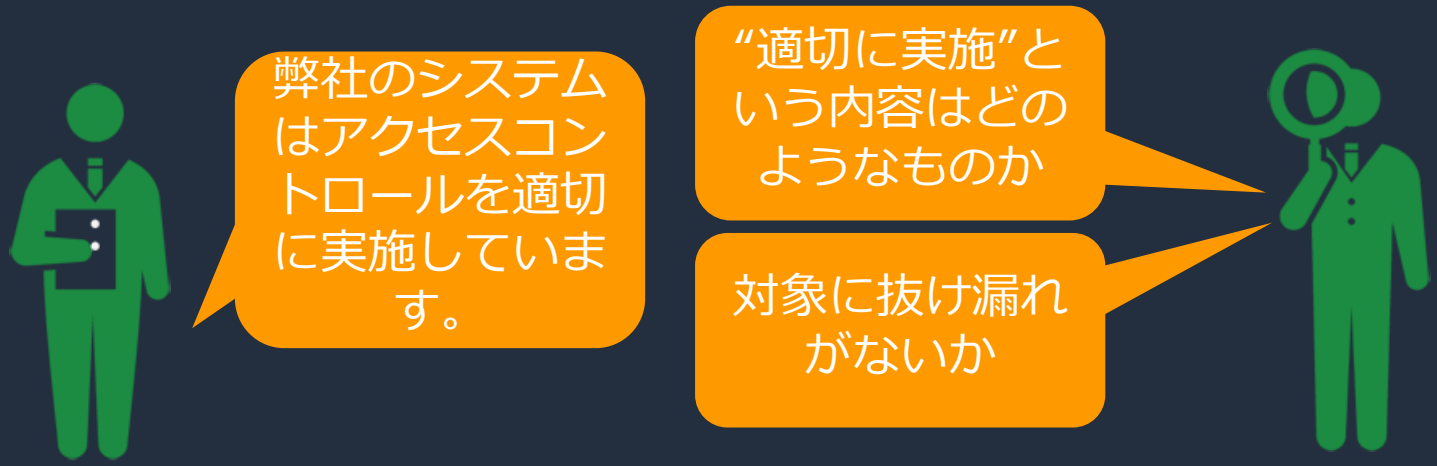
監査の種類

いくつかの観点で監査を分類することが出来る

監査形態	保証型監査	一定の基準を満たしているかについて監査人が保証意見を提示する監査（会計監査、SOC監査）
	助言型監査	問題点を検出し、改善を提言する監査
監査主体	内部監査	組織内の内部統制の一貫として行われる監査
	外部監査	組織とは利害関係のない外部の専門家によって行われる、一定規模の企業や業種で義務付けられている
監査目的	システム監査	システム全体に対する監査。経済産業省が作成したシステム監査基準が存在する
	セキュリティ監査	情報セキュリティを対象とした監査。ISO 27001,27002のようなベストプラクティスや基準がある
	認証取得のための監査	PCI DSS, ISMS, FedRAMPなどの認定取得のための監査
	内部統制監査	企業の財務統制を評価する監査（J-SOX監査等）

“保証”の意味　ーこまかく開示することが目的ではないー

“間違いがない、大丈夫であると認め、責任をもつこと”



監査人は、“保証”できるだけの証拠の収集や分析を深く行わなければいけない
ー＞より高いレベルの責任が求められるのが保証型監査
ー＞一定の“時点”よりも“期間”にわたって統制が保たれている方が信頼性は高い

コンプライアンス標準と監査の例

コンプライアンス基準	監査の目的	管轄組織	監査対象	立ち入り監査の有無	一時点監査 or 運用監査？	監査人
SOC（Systems and Organization Controls）	SOC1：財務報告に影響する内部統制の評価 SOC2：システムの有効性の評価	AICPA（米国公認会計士協会）	ポリシー、プロセス、組織、体制、システム実装、システム運用	Yes	Type1（一時点の監査），Type 2（半年以上の運用状況監査）	第三者監査法人（資格CPAが必要）
PCI DSS	クレジットカード情報の安全な取り扱い	PCI Security Standards Council	クレジットカード情報を取り扱うシステム	Yes	一時点	第三者監査法人（資格QSA が必要）
ISO/IEC 27001（日本ではISMS）	情報セキュリティマネジメントシステムが構築され、適切に管理しているかを確認	ISO/IEC 日本工業標準調査会	情報システムに関わるマネジメントシステム	Yes	一時点	第三者監査法人（資格が必要、ISMSでは審査員）
FedRAMP	米国政府期間が利用するクラウドサービスのセキュリティ認証	米国政府	米国政府期間が利用するクラウドサービス・プロバイダー	Yes	運用監査あり	認定された第三者機関
ISMAP	政府利用のための安全なクラウドサービス・プロバイダ認定	ISMAP運営委員会, IPA	日本政府、自治体が利用するクラウドサービス・プロバイダー	Yes	初年度は一時点	ISMAP 運営委員会が認定した監査法人

本日のお話する内容

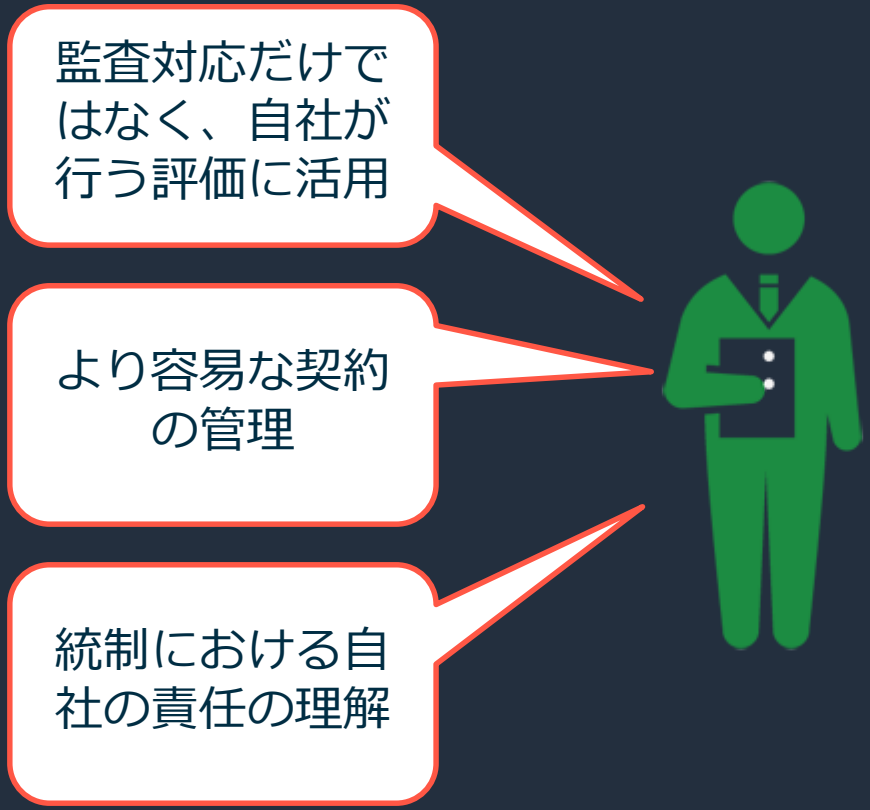
- 監査って何のため？
- **AWS Artifactとは？**
- AWS Artifactの利用（レポート）
- レポートの活用（SOCを中心に）
- AWS Artifactの利用（契約）

AWS Artifact 概要

- [レポート] AWS Artifact では、AWS ISO 認定、Payment Card Industry（PCI）、Service Organization Control (SOC) レポートなどの AWS セキュリティおよびコンプライアンスドキュメントをオンデマンドでダウンロードできます。
- [契約] 特定のAWS との契約を確認、承認、管理できます。組織内の現在および将来のすべてのアカウントに AWS の契約を適用できます。
- 重要：**AWS Artifact内の情報は“契約”に基づいて開示する秘密情報です。**

AWS Artifact 概要 ー お客様が得られるメリット ー

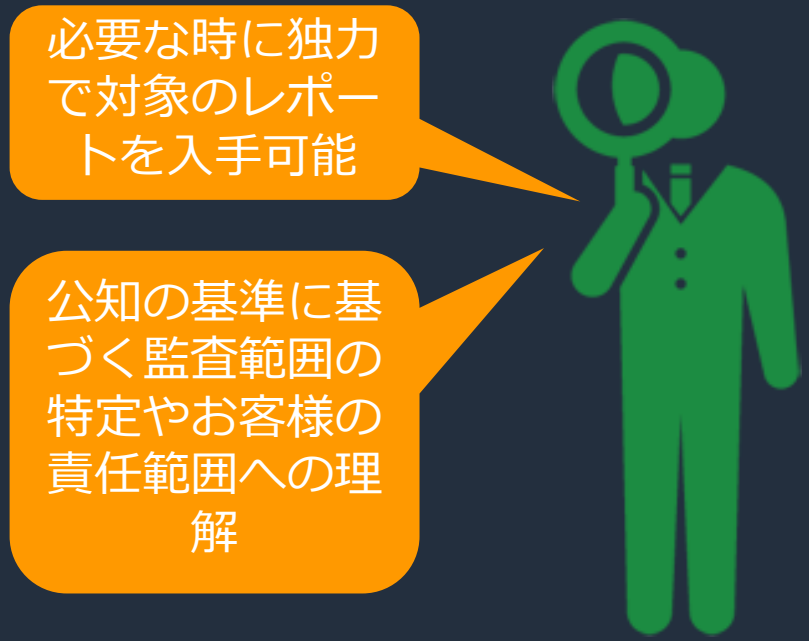
- AWS Artifact では、AWS ISO 認定、Payment Card Industry（PCI）、Service Organization Control (SOC) レポートなどの AWS セキュリティおよびコンプライアンスドキュメントをオンデマンドでダウンロードできます。
- AWS との契約を確認、承認、管理できます。組織内の現在および将来のすべてのアカウントに AWS の契約を適用できます。



AWS Artifact 概要　ー監査人が得るメリットー

- 監査人が得るメリット

AWS のデューディリジェンスを実施し、AWS のセキュリティ管理環境の高い透明性を保ちます。AWS のセキュリティとコンプライアンスを継続的にモニタリングし、新しいレポートをすぐに確認できます。



本日のお話する内容

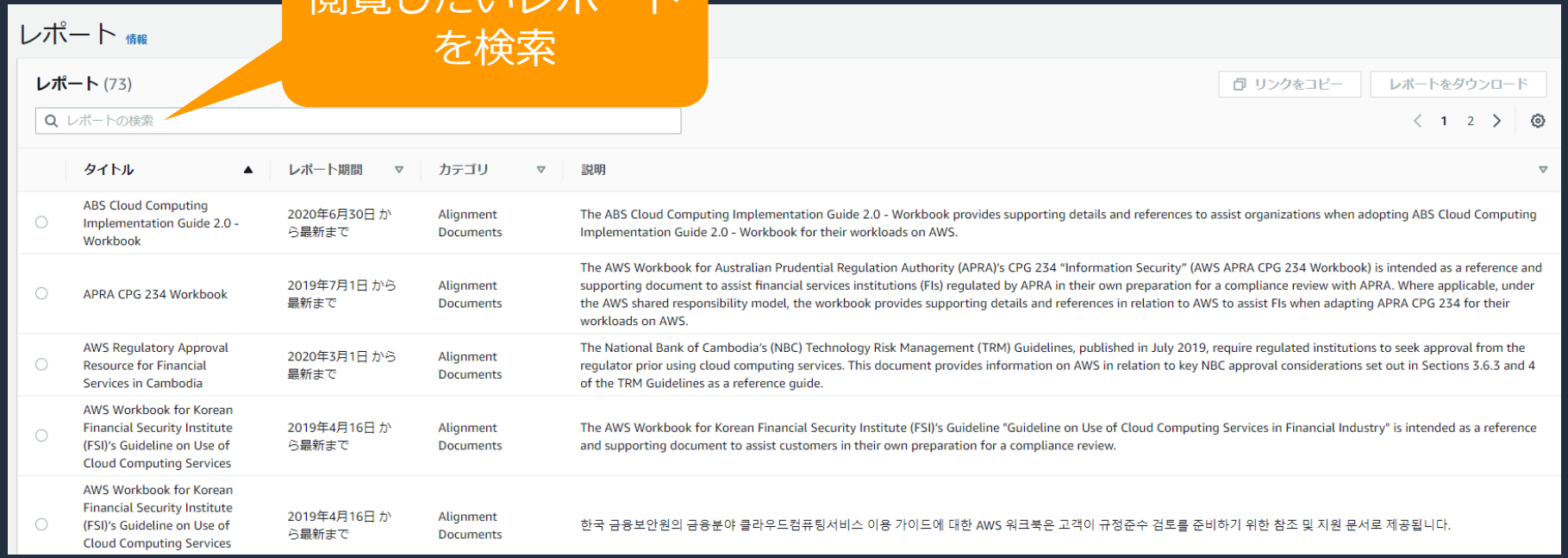
- 監査って何のため？
- AWS Artifactとは？
- **AWS Artifactの利用（レポート）**
- レポートの活用（SOCを中心に）
- AWS Artifactの利用（契約）

AWS Artifactの利用開始

- マネジメントコンソールからAWS Artifactを選択（検索でもOK）
- Code Artifactとは違うサービスであることに注意
- 料金は無料
- IAMで権限管理可能

レポートの閲覧

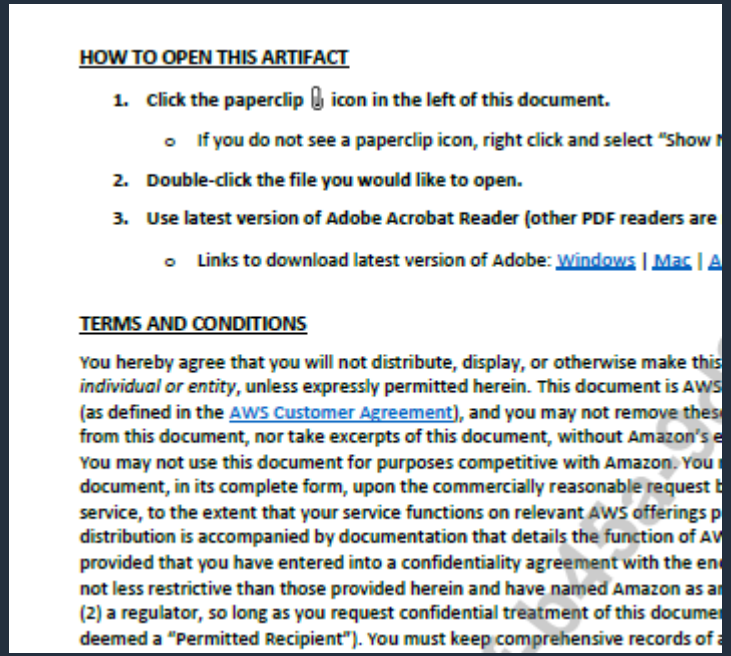
閲覧したいレポートを検索



タイトル	レポート期間	カテゴリ	説明
ABS Cloud Computing Implementation Guide 2.0 - Workbook	2020年6月30日 から最新まで	Alignment Documents	The ABS Cloud Computing Implementation Guide 2.0 - Workbook provides supporting details and references to assist organizations when adopting ABS Cloud Computing Implementation Guide 2.0 - Workbook for their workloads on AWS.
APRA CPG 234 Workbook	2019年7月1日 から最新まで	Alignment Documents	The AWS Workbook for Australian Prudential Regulation Authority (APRA)'s CPG 234 "Information Security" (AWS APRA CPG 234 Workbook) is intended as a reference and supporting document to assist financial services institutions (FIs) regulated by APRA in their own preparation for a compliance review with APRA. Where applicable, under the AWS shared responsibility model, the workbook provides supporting details and references in relation to AWS to assist FIs when adapting APRA CPG 234 for their workloads on AWS.
AWS Regulatory Approval Resource for Financial Services in Cambodia	2020年3月1日 から最新まで	Alignment Documents	The National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines, published in July 2019, require regulated institutions to seek approval from the regulator prior using cloud computing services. This document provides information on AWS in relation to key NBC approval considerations set out in Sections 3.6.3 and 4 of the TRM Guidelines as a reference guide.
AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline on Use of Cloud Computing Services	2019年4月16日 から最新まで	Alignment Documents	The AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline "Guideline on Use of Cloud Computing Services in Financial Industry" is intended as a reference and supporting document to assist customers in their own preparation for a compliance review.
AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline on Use of Cloud Computing Services	2019年4月16日 から最新まで	Alignment Documents	한국 금융보안원의 금융분야 클라우드컴퓨팅서비스 이용 가이드에 대한 AWS 워크북은 고객이 규정준수 검토를 준비하기 위한 참조 및 지원 문서로 제공됩니다.

レポートを利用する上での注意

- ダウンロードしたレポートを閲覧する際、PDFのトップページに、Artifactの開き方とTerms and Conditionsが表示される（閲覧者はこの利用規約に同意して利用するものとみなされる）
- 一部レポート（SOC 1など）は、ダウンロード時にTerms and Conditionsが表示され、明示的な利用規約への同意が求められる。



HOW TO OPEN THIS ARTIFACT

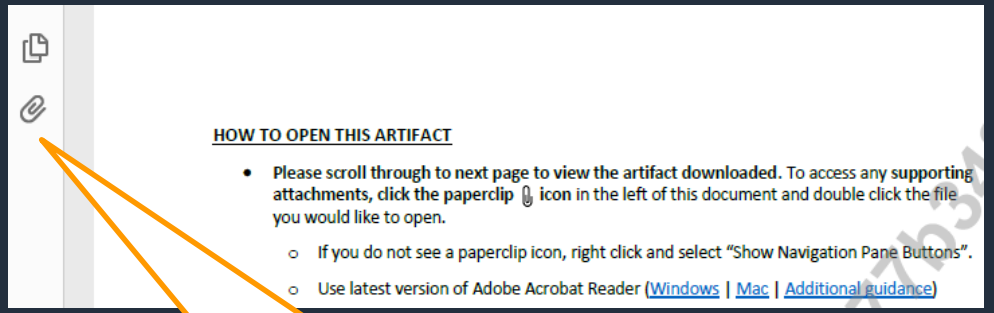
1. **Click the paperclip icon in the left of this document.**
   - If you do not see a paperclip icon, right click and select "Show
2. **Double-click the file you would like to open.**
3. **Use latest version of Adobe Acrobat Reader (other PDF readers are**
   - Links to download latest version of Adobe: Windows | Mac | A

TERMS AND CONDITIONS

You hereby agree that you will not distribute, display, or otherwise make this
individual or entity, unless expressly permitted herein. This document is AWS
(as defined in the AWS Customer Agreement), and you may not remove these
from this document, nor take excerpts of this document, without Amazon's e
You may not use this document for purposes competitive with Amazon. You
document, in its complete form, upon the commercially reasonable request b
service, to the extent that your service functions on relevant AWS offerings p
distribution is accompanied by documentation that details the function of AW
provided that you have entered into a confidentiality agreement with the en
not less restrictive than those provided herein and have named Amazon as a
(2) a regulator, so long as you request confidential treatment of this docume
deemed a "Permitted Recipient"). You must keep comprehensive records of

レポートの利用（複数のファイルがある場合）

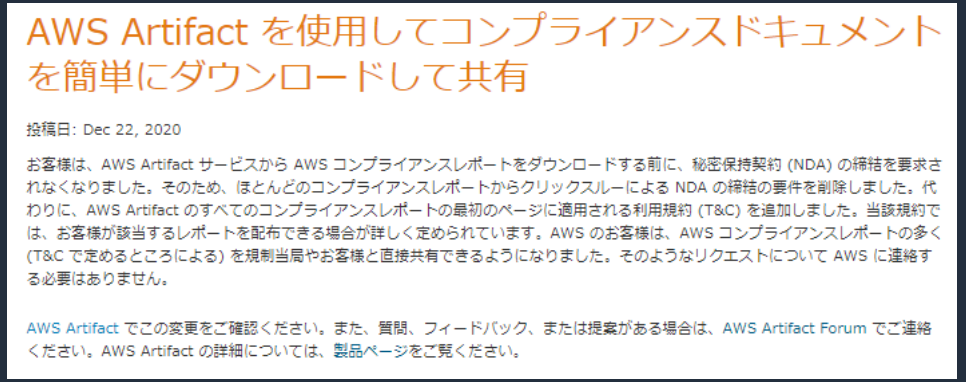
- 一つのレポートに複数の文書が含まれている場合、PDFの中に添付として保管されています。
- 文書によっては、Excelによる管理策の一覧や、利用者とAWSの責任範囲を示す AWS Services and Customer Responsibility Matrix が添付されています。



複数の文書が含まれている場合にはこのクリップマークアイコンをクリック

レポートの利用（第三者への開示）

- 明示的に許可されている場合をのぞいて外部に公開しない（AWSの機密情報にあたる）
- エンドユーザーからの合理的な要求がある場合に、Terms and Conditionに従ったうえで完全な形でレポートの開示が可能（お客様のサービスが関連するAWSオファリングの機能を説明する文書を添付）
- AWSへの連絡は不要（ただし、必要に応じて、記録を管理）



AWS Artifact を使用してコンプライアンスドキュメントを簡単にダウンロードして共有

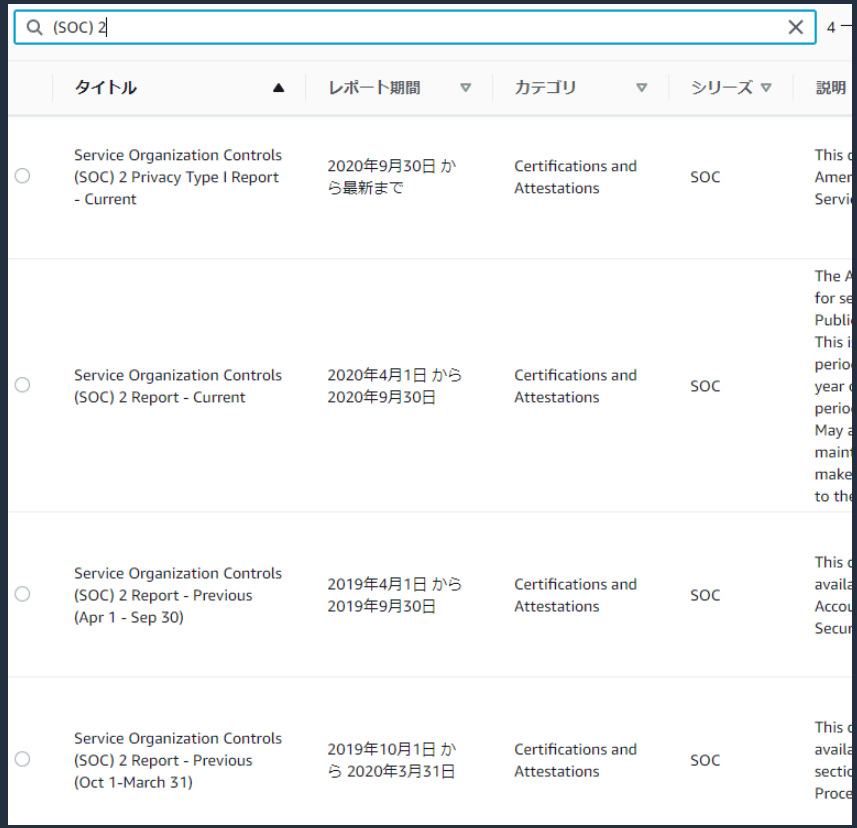
投稿日: Dec 22, 2020

お客様は、AWS Artifact サービスから AWS コンプライアンスレポートをダウンロードする前に、秘密保持契約 (NDA) の締結を要求されなくなりました。そのため、ほとんどのコンプライアンスレポートからクリックスルーによる NDA の締結の要件を削除しました。代わりに、AWS Artifact のすべてのコンプライアンスレポートの最初のページに適用される利用規約 (T&C) を追加しました。当該規約では、お客様が該当するレポートを配布できる場合が詳しく定められています。AWS のお客様は、AWS コンプライアンスレポートの多く (T&C で定めるところによる) を規制当局やお客様と直接共有できるようになりました。そのようなリクエストについて AWS に連絡する必要はありません。

AWS Artifact でこの変更をご確認ください。また、質問、フィードバック、または提案がある場合は、AWS Artifact Forum でご連絡ください。AWS Artifact の詳細については、製品ページをご覧ください。

時期の近いによるレポートの違い

- 例えば“（SOC）２”と検索した場合、複数のレポートが表示されます。
- “Current”と表示されているものは現行のレポートであり、“Previous”と表示されているものは、以前のレポートとなります。
- SOCレポートの場合、半期に一度発行をされますので、一年間分の統制を評価する場合には、過去のものも適宜参照してください。



本日のお話する内容

- 監査って何のため？
- AWS Artifactとは？
- AWS Artifactの利用（レポート）
- **レポートの活用（SOCを中心に）**
- AWS Artifactの利用（契約）

Service Operations Controls （SOC保証報告書）

- 米国公認会計士協会（AICPA）が定義した内部統制保証報告の仕組みです。
- SOC1,SOC2,SOC3に大別されます。（次ページ参照）
- 監査の対象期間によってType Ⅰ（時点監査）、Type Ⅱ（期間監査）にわかれます。
- Trustサービスの原則および基準に対して、クラウド事業者が言明を行い、監査人が評価を行います。

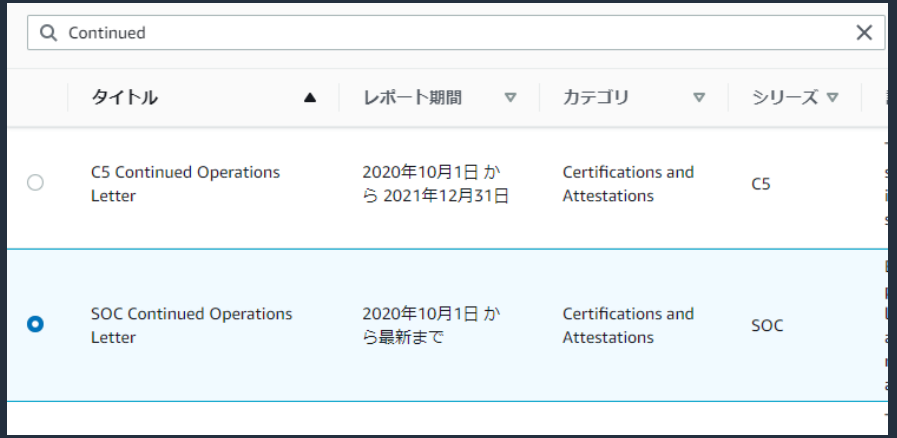
https://aws.amazon.com/jp/compliance/soc-faqs/

SOCレポートの目的の違い

	SOC 1	SOC 2: セキュリティ、可用性、機密性	SOC 2: プライバシー	SOC 3: セキュリティ、可用性、機密性
レポートの内容	AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明	AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性の原則および基準を満たす AWS 統制の外部監査に関する説明	AWS の統制環境に関する説明、および AICPA の信頼サービスのプライバシー原則と基準を満たす AWS 統制の外部監査に関する説明	AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性の原則および基準を満たしていることを実証する公開レポート
監査レポートの実行の基盤となる規格	SSAE No.18、Attestation Standards: Clarification and Recodification (AICPA, Professional Standards), which includes AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting。AICPA ガイド、Service Organizations: Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)	SSAE No.18、Attestation Standards: Clarification and Recodification, which includes AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, 2017 Trust Services Criteria)	SOC 2: セキュリティ、可用性、機密性と同じ	SSAE No.18、Attestation Standards: Clarification and Recodification, which includes AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, 2017 Trust Services Criteria)
レポートの主目的	財務報告に係る内部統制に関連する可能性がある AWS の統制環境について、お客様に情報を提供すること 財務報告に係る内部統制 (ICOFR) の有効性に関する評価および意見について、お客様とその監査人に情報を提供すること	システムのセキュリティ、可用性、機密性に関連する AWS の統制環境について、ビジネスニーズのあるお客様およびユーザーに独立した評価を提供すること	AWS のシステムの独立した評価と、AWS のプライバシーコントロールの設計の適合性について、お客様に提供すること SOC 2 プライバシー信頼原則は、米国公認会計士協会 (AICPA) によって策定され、企業の目標を達成するために、個人情報を収集、使用、保持、開示、処分する方法に関連したコントロールを評価する基準を確立する	システムのセキュリティ、可用性、機密性に関連する AWS の統制環境について、AWS の内部情報を開示せずに、ビジネスニーズのある顧客およびユーザーに独立した評価を提供すること
レポートの主な確認者	顧客管理およびその監査人	ビジネスニーズのあるユーザー	プライバシーに関連する AWS の統制を理解するというビジネスニーズのあるユーザー	公開情報
AWS レポートの対象期間	6 か月: 10 月 1 日～3 月 31 日、および 4 月 1 日～9 月 30 日	6 か月: 10 月 1 日～3 月 31 日、および 4 月 1 日～9 月 30 日	時点 (報告日現在)	6 か月: 10 月 1 日～3 月 31 日、および 4 月 1 日～9 月 30 日

レポートの期間とContinued Operations letter

- SOC レポートは、一定期間にわたって実行される監査であり、有効期限はありません。AWS 監査人は年に 2 回、10 月 1 日～3 月 31 日と 4 月 1 日～9 月 30 日の 6 か月の期間にわたって、SOC 監査を実施しています。監査期間が終了すると、AWS 監査人は監査レポートを作成し、5 月と 11 月にレポートを発行しています。
- また、SOC Continued Operations Letter をダウンロードすることもできます。このレターでは、最新の SOC レポートで監査および説明されたセキュリティコントロールとシステム環境を AWS が引き続き維持していることが示されています。



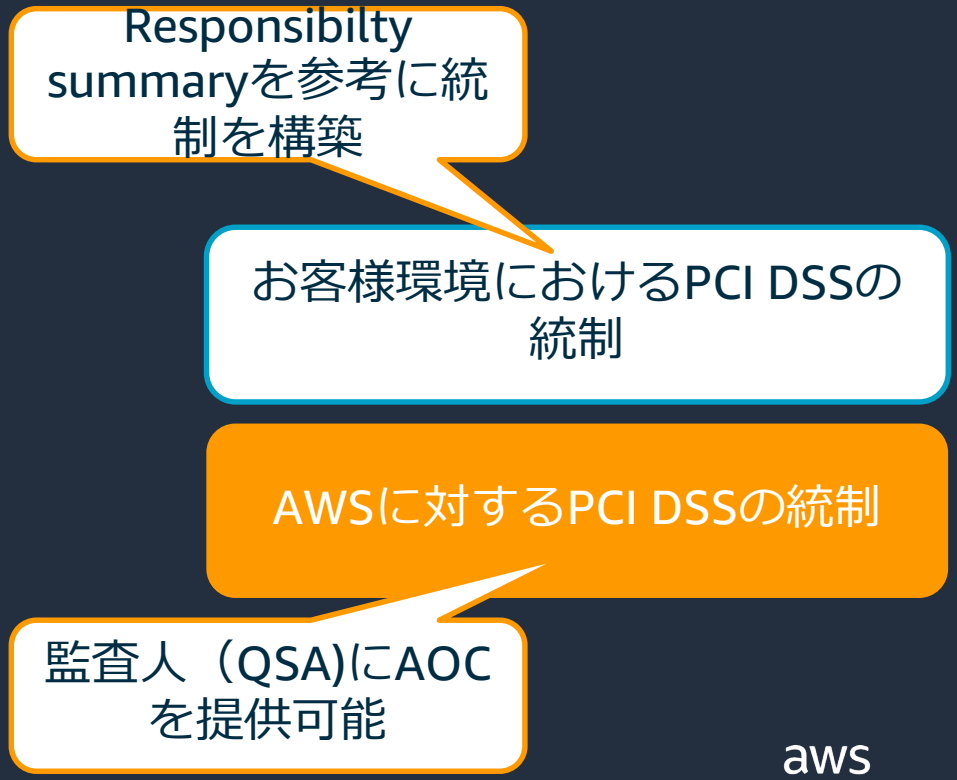
参考：SOC３レポートは公開ウェブサイトから入手可能

- 秘密保持の管理が困難である場合や、統制を説明することを目的とした場合は、一般ユーザー向けに公開されているSOC３レポートを活用することが可能です。

https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf

主なレポート：PCI DSS

- Payment Card Industry Data Security Standard (PCI DSS) はカード所有者のデータ（CHD）や機密性の高い認証データ（SAD）を保存、処理、転送するエンティティに適用されるセキュリティ標準です。
- 明確な基準に基づく評価をおこないます。
- PCI DSS Attestation of Compliance (AOC) および Responsibility Summaryを入手可能です。



Artifactのレポートは監査だけではない。

- 「日本におけるAWSリージョンのレジリエンシー」ホワイトペーパーでは、東京リージョンおよび大阪リージョンにおける日本固有の事業継続上の耐障害性を解説しています。
- 本ホワイトペーパーは日英両方で提供しています。

Amazon Web Services ブログ

「Resiliency in Japan-日本におけるAWSリージョンのレジリエンス-」ホワイトペーパーがAWS Artifactから入手できるようになりました。

by matshogo | on 03 MAR 2021 | in Announcements, General, Security, Identity, & Compliance | Permalink | Share

多くの日本のお客様にとって地震災害は事業継続上の重大な関心事となります。2021年3月に開設されたAWSの大阪リージョンの活用により、日本の多くのお客様は、日本国内で地理的に離れたマルチリージョンの設計による高い耐障害性を備えたサービスを設計および運用することが容易になりました。

一方、自然災害や事業の継続に対する設計や運用は引き続き客様にとっての関心事であり、AWSでは「データセンターのセキュアな設計」ページや、「Disaster Recovery of Workloads on AWS: Recovery in the Cloud」などのホワイトペーパーを通じて、AWSにおけるレジリエンスの確保およびお客様の設計を踏まえたサービスレジリエンスの向上の支援をしています。

この度、AWSリージョンやデータセンターの設計を踏まえ、日本における地震災害において、どのようにAWSが高い耐障害性を確保しているか、また、マルチリージョンの活用により、お客様がどのように高いレジリエンスを確保できるかを解説したホワイトペーパーを、AWS Artifactにおいて公開しました。

AWSのアカウントをお持ちのお客様はマネジメントコンソールより、AWS Artifactを選択し、「レポートの表示」から当該レポートを入手することができます。本レポートは日本語、および英語で作成されております。
日本語の場合は、"日本におけるAWSリージョンのレジリエンス"、英語の場合は"Resiliency in Japan"で検索いただけると表示されます。(下記のように"日本"で検索すると、日本語版が容易に検索できます。)

また、AWS Artifactからは、お客様自身が、様々な監査レポートなどAWSのコンプライアンスプログラムに関連した様々なレポートを入手し、評価を行う上での手助けとなります。

https://aws.amazon.com/jp/blogs/news/resiliency-in-japan/

本日のお話する内容

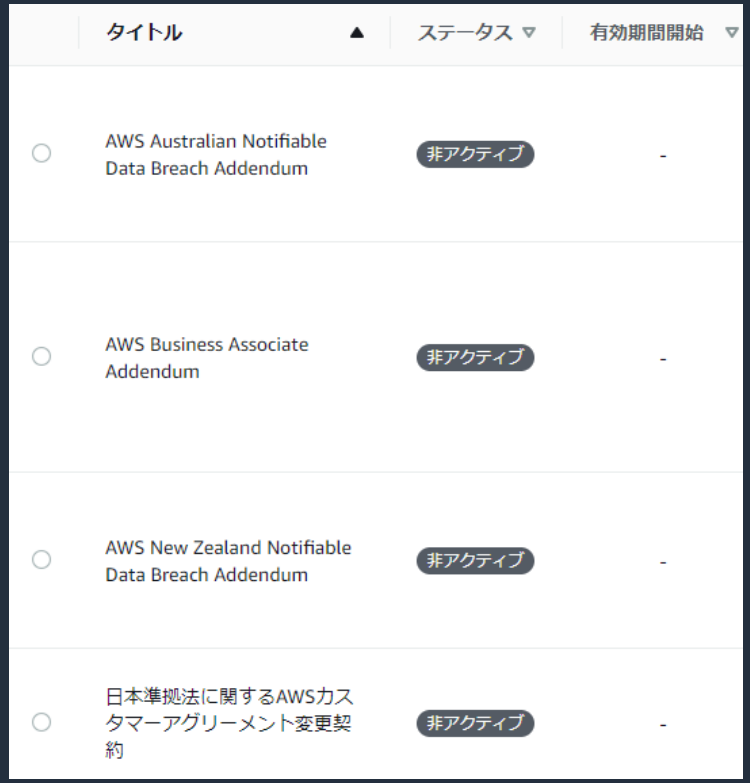
- 監査って何のため？
- AWS Artifactとは？
- AWS Artifactの利用（レポート）
- レポートの活用（SOCを中心に）
- **AWS Artifactの利用（契約）**

AWS Artifactを通じた契約の変更

- AWS Artifact Agreements は AWS Artifact サービス (監査およびコンプライアンスポータル) の機能で、個々のアカウントおよび AWS Organizations で組織に含まれる全アカウントの AWS との特定の契約を確認、受諾、管理できます。
- また、以前に受諾した契約が不要になった場合に、AWS Artifact を使用して終了することもできます。

AWS Artifactによる契約の変更

- 対象となる契約を選択したのち、NDAを受諾（合意をクリック）し、ダウンロードします。
- 契約内容を確認し、問題がなければ、“契約の受諾”をクリックし、表示される利用規約に合意して契約の受諾を行います。



AWS Artifact Organization Agreementsの活用

- AWS Artifact Organization Agreements は組織内のすべてのアカウントに代わって 1 つの契約を受諾することで、複数の AWS アカウントの契約管理を簡素化します。
- マスターアカウントで作業を行うと、一括してメンバーアカウントへその設定が適応されます。（作業後、新たに新規で追加されたメンバーアカウントにもその設定は自動で反映）
- 一部のメンバーアカウントのみの契約を受諾したい場合は、各アカウントに個別にサインインし、AWS Artifact Account Agreements ([**Account agreements**] タブ) から関連する契約を受諾する必要があります。

Amazon Web Services ブログ

AWS Organizationsによる、日本準拠法に関する AWS カスタマーアグリーメントの一括変更について

by AWS Japan Staff | on 17 AUG 2020 | in AWS Artifact, AWS Organizations, General, Security, Identity, & Compliance | Permalink | Share

みなさん、こんにちは。アマゾン ウェブ サービス ジャパン、
シニアアドボケイトの亀田です。

今日は、AWS Organizationsによる、日本準拠法に関する AWS カスタマーアグリーメントの一括変更について、日本のお客様にとって重要なアップデートをお届けします。AWS Organizationsは複数のAWSアカウントにおいて、請求の一元管理や、アクセス、コンプライアンス、セキュリティの制御、AWS アカウント間でのリソースの共有などを実現するサービスです。

AWSのアカウントは開設直後、"AWS カスタマーアグリーメント"は準拠法、かつ管轄裁判所が米国ワシントン州法となっています。2017年11月に我々は、お客様が自動で"日本準拠法に関する AWS カスタマーアグリーメント変更契約"を締結可能とするAWS Artifactの機能をリリースしました。
https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/

これによりお客様は、自身で複雑な処理を行うことなく、AWSのマネージメントコンソール上でAWS カスタマーアグリーメントの変更契約締結が可能となり、準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができるようになりました。

この作業はアカウント単位で行う必要があり、企業内で複数のAWSアカウントを保有し、AWS Organizationsで管理されている場合、AWSアカウントの数だけその作業を行う必要がありましたが、このアップデートにより、マスターアカウントで作業を行うと、一括してメンバーアカウントへその設定が適応されます。また、設定作業後、新たに新規で追加されたメンバーアカウントにもその設定は自動で反映されるため、従来個別に作業を行う必要があったときに懸念されていた、作業漏れを防ぐことも可能です。

また、リセラーなど実運用にいおけるマスターアカウントとメンバーアカウントの管理母体が異なる場合は、本機能によるAWS カスタマーアグリーメント変更契約の一括締結には十分な注意を払う必要があります。

使い方は簡単です。

日本準拠法への変更に関する留意事項

- 日本準拠法に関する AWS カスタマーアグリーメントは、請求連絡先アドレスが日本国内にあるアカウントに対してのみ提供されるものです。
- 既に個別に書面でカスタマーアグリーメントの準拠法および裁判管轄を変更する契約を取り交わしているお客様については、再度締結いただく必要はございません。
- リセラーなど実運用におけるマスターアカウントとメンバーアカウントの管理母体が異なる場合は、本機能によるAWS カスタマーアグリーメント変更契約の一括締結には十分な注意を払う必要があります。

まとめ

本日のお話する内容

- 監査って何のため？
- AWS Artifactとは？
- AWS Artifactの利用（レポート）
- レポートの活用（SOCを中心に）
- AWS Artifactの利用（契約）

AWS Artifactは、AWSのコンプライアンス管理を効率化してくれるサービスです。

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能
- 申込みはイベント告知サイトから

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive