Internet Week 2021

C16 セキュリティ基準、標準、規制との付き合い方

中島 智広
セキュリティソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社

自己紹介

名前：中島 智広（なかしま ともひろ）

職種：セキュリティソリューションアーキテクト

業務：お客様のセキュリティ＆コンプライアンスの取り組みを

クラウドの利活用の視点からご支援

- セキュリティアーキテクチャ、運用設計の支援
- 各種コンプライアンスプログラムへの準拠支援
- 公式トレーニング「Security Engineering on AWS」インストラクター など

はじめに / プログラム概要から

セキュリティに取り組む中で基準、標準、 規制といったものを意識することがあります。 これらに対してどのような印象をお持ちでしょうか？

実はこれらは上手く活用することで、 みなさんの組織のセキュリティを効率よく最適化することができます。 一方、活用の仕方を誤ってしまうと、 ただただ面倒なものになってしまいがちです。

そこで、本プログラムではエンジニアやセキュリティ担当者がこれらがどのように付き合っていけば良いのかの、 昨今のトレンド、クラウド活用による変化なども含めて、 プラクティスを解説します。

https://www.nic.ad.jp/iw2021/program/detail/#c16

コンプライアンス

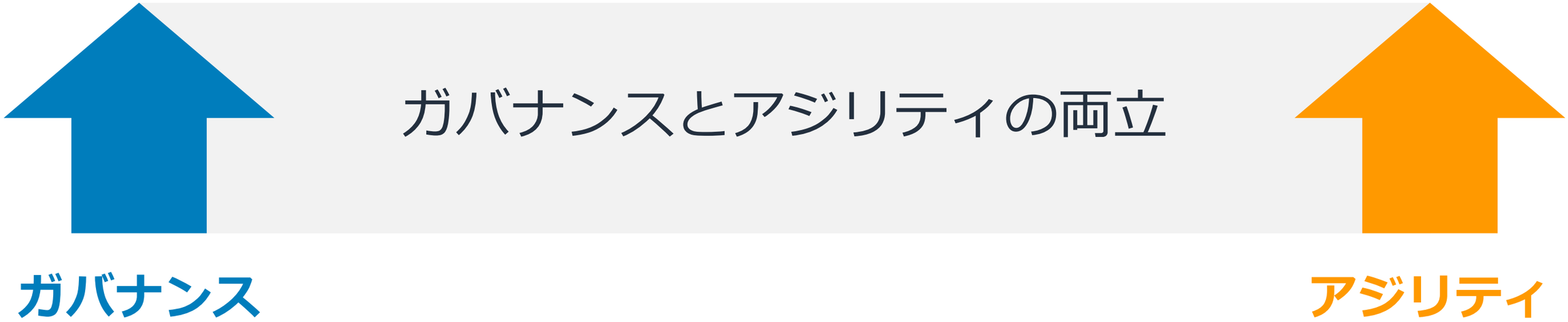
- 「法令遵守」と訳されることが多いが、その対象は法令に限らない規範全般
    - 基準、標準、規制、指針、社会通念、モラル、etc...
- セキュリティ、ことさら本資料の文脈では

情報システムの統制が**定められた水準以上**にあることを確かにする

さらにはそのことをステークホルダーに**説明可能**とすること

コンプライアンスの目指すべき姿

- 企業は事業の成長のためにジャストフィットな統制が欲しい
- イノベーションや事業の成長を阻害するコンプライアンスは本末転倒
- 組織や情報システムの説明責任を下支えする「手段」



お話しすること

基準、標準、規制などのコンプライアンスプログラムを活用することで
なぜセキュリティを効率よく最適化できるのか？（＝ベネフィット）

コンプライアンスプログラムを活用して
セキュリティを効率よく向上、最適化する方法や勘所（＝アプローチ）

クラウドでコンプライアンスプログラムへの対応が楽になる？
クラウドを活用する動き、その理由（＝トレンド）

コンプライアンスプログラムのベネフィット

さまざまなコンプライアンスプログラム

規制法、標準、指針 （第三者審査あり）	規制法、標準、指針 （第三者審査なし）	固有のルールや ベストプラクティス
ISO27000シリーズ	NIST SP800	組織ポリシー
SOC	FISC安全対策基準	運用ルール
PCI DSS	HIPAA/3省2ガイドライン	など
ISMAP	など	
など		

審査機関による
要件の解釈と審査

組織内で要件の解釈と審査

たとえば、PCI DSS

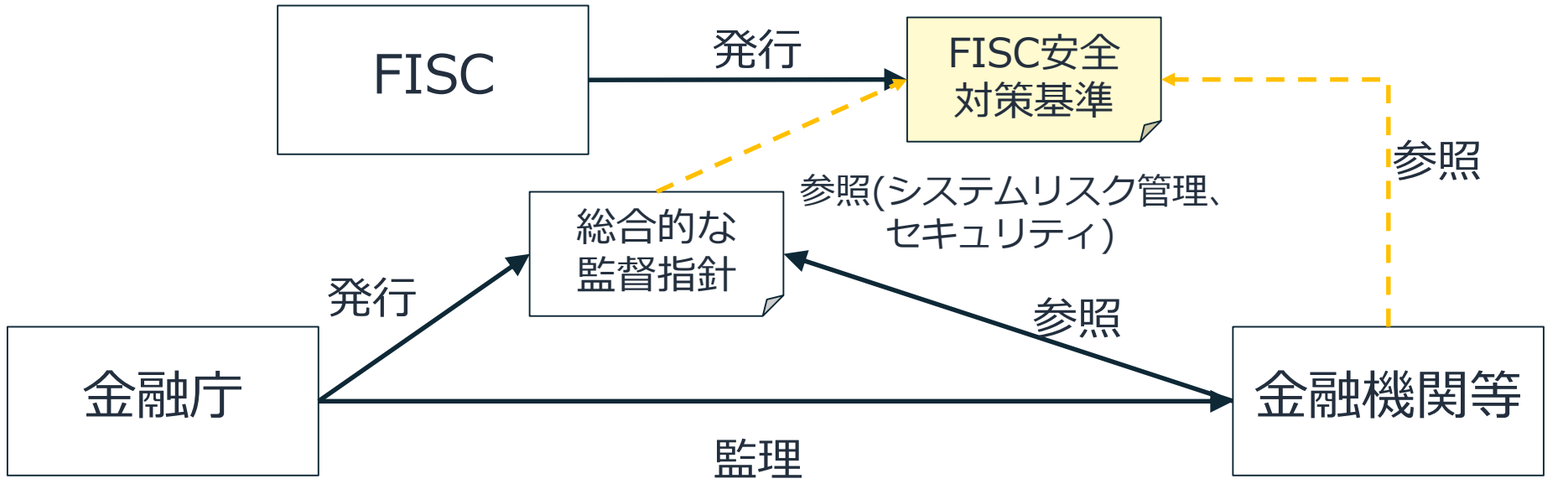
- カード情報を安全に取り扱うことを目的として策定されたセキュリティ基準
- カードブランドや監督省庁、相互に接続する事業者が準拠を要求
- 認定審査人（QSA）の審査結果である準拠証明書（AOC）を以て準拠を説明
- 12の要件、200以上の項目からなる
- 要件の具体性が高く、外部から参照されることが多い

PCI DSS遵守の対応が想定されるお客様
イシュアー、アクワイアラー、サービス・プロバイダー、加盟店
業界例
金融業：クレジットカード会社、クレジットカード発行金融機関
流通業： 大手百貨店、スーパー、量販店、鉄道、航空会社
通信/メディア/公共：携帯電話会社、通信会社、ユーティリティ、新聞
製造業：石油業界 他

Source : https://www.jcdsc.org/pci_dss.php

たとえば、FISC安全対策基準

- 金融機関等のよりどころとなるべき共通の安全対策基準
- 金融庁の「総合的な監督指針」ではシステムリスクの参考資料および、セキュリティに関する基準の参考文書として記載
- 直接の強制力や認証評価制度はなく、自らが要件を解釈し適合性を評価する



コンプライアンスプログラムのベネフィット

- やるべきこと、確認するべきことが明確になる
- 実装方法やノウハウを組織やシステムを横断して共通化、再利用できる
- 委託先/取引先のセキュリティチェックを効率化できる など

もし、コンプライアンスプログラムがなかったら・・・

- 組織やシステムに必要なセキュリティは全て自前で考える（車輪の再発明）
- 自前で考えたセキュリティの妥当性を第三者に説明し理解を得る手間が生じる
- 委託先/取引先のチェックに多大な労力がかかる

求められる統制はオーバーラップしている

- 基本的な統制の観点はプログラムに依存しない/共通項が多い

  例：特権管理、構成管理、変更管理、環境分離、ログ保全、発見的統制、etc…

- プログラム自体が共通化、再利用、整合性を意識して策定されている

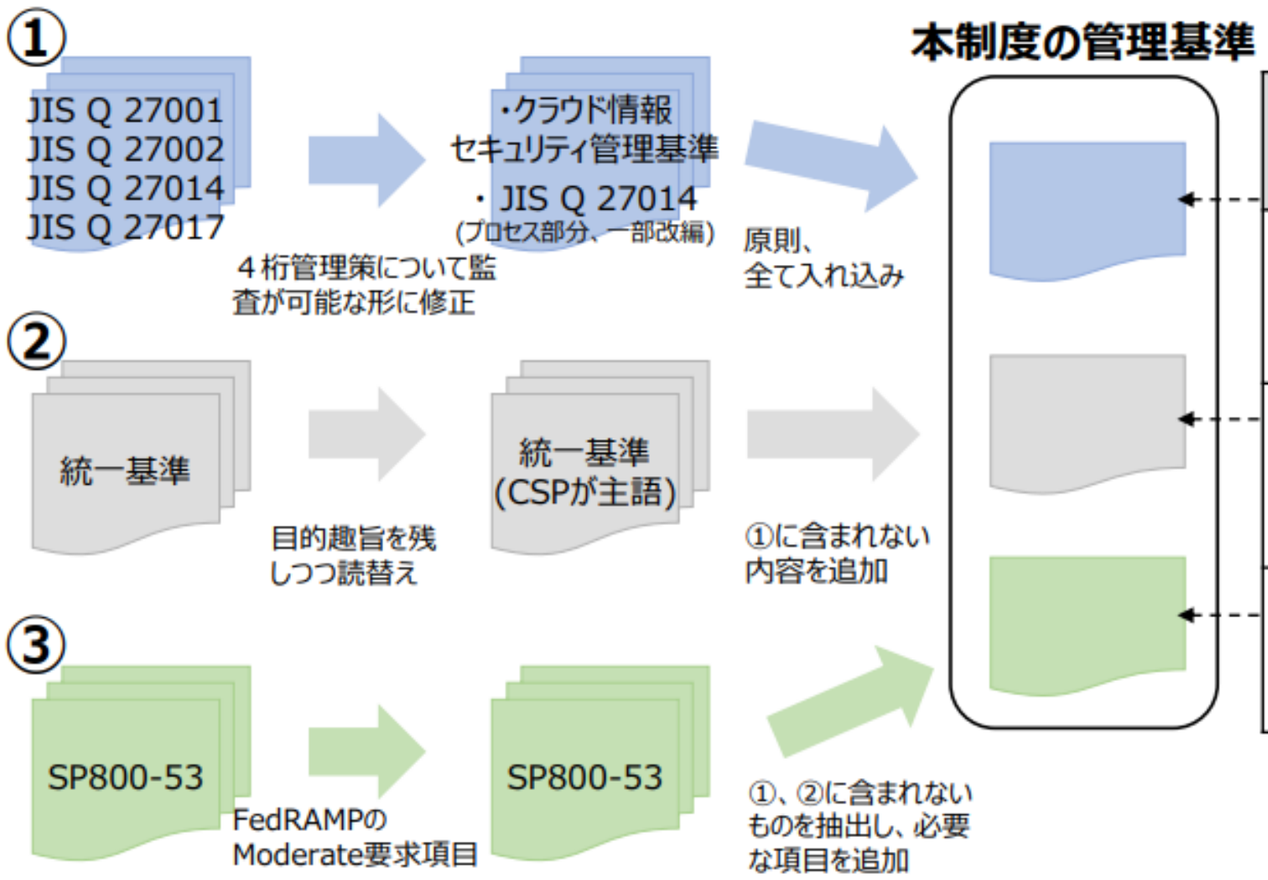
  例：ISMAPにおけるISO27000シリーズ/NIST SP800-53の参照 など

- あるプログラムと、別のプログラムの統制のマッピングもよく行われる整理

  例：HIPAAとISO27000シリーズのマッピング、NIST CSFとCIS Controlsのマッピング など

プログラムに依らず為すべきことの本質は変わらない（＝リスクへの対応）

たとえば、ISMAP管理基準の構成



項目数※1

管理策基準 3桁：121 4桁：1074	マネジメント基準 3桁：21 4桁：64	ガバナンス基準 4桁:18
全て入れ込み	全て入れ込み	ISO27014の内容をベースに再整理を実施
ISOの項目数で ・**6項目**追加 ・**3項目**追記※2	(定型管理策１に該当するため、原則ISOを採用)	(該当なし)
ISOの項目数で ・**22項目**追加 ・**29項目**追記	・**4項目**追記	(該当なし)

※１：項目数は、作業ファイル上の行数でのカウントであるため、実際の管理策数は多少増減する見込み
※２：情報の提供を求める項目については、管理基準とは別の要求事項として要求する項目も存在する。

「政府情報システムのためのセキュリティ評価制度（ISMAP）の概要」スライドより抜粋
Source: https://www.kantei.go.jp/jp/singi/it2/cio/dai87/siryou3-3.pdf

コンプライアンス対応を通じてセキュリティを最適化する

- コンプライアンスプログラムはベストプラクティスと密接な関係性
- 実装している統制を各プログラムの基準によって多面的に評価する
- コンプライアンスプログラムとのギャップが大きい場合、セキュリティ以外の観点でもベストプラクティスと乖離、リスクやオーバーヘッドを抱えている可能性

コンプライアンスプログラムを知ることは
よりよいアーキテクチャを知ること

コンプライアンスプログラムへのアプローチ

プログラムを乗りこなし楽をする

&

Simple is the BEST

目的と手段を違えないために

「自分たちが何をやりたいのか」

そのために「こういったセキュリティが必要である」という意味付け

- 意味づけが不十分だと目的/手段の入れ替わりが生じる
- 目標疲れを防ぐためにも、意味が必要
- この種のメッセージングはリーダーシップ層から行うことがセオリー

【参考】目的と手段がときに入れ替わるのはなぜか？
Source: https://globis.jp/article/4953

コンプライアンスの要件はベストプラクティスとの認識からスタートする

- ベストプラクティスに則ることが多くの場合最もリーズナブル、リファレンスとなる事例やソリューションも多い
- 共通する基本的な統制からスタートすることが手戻りを避けるよいアプローチ、基本を疎かにすると取り繕うために雪だるま式に運用コストがかさむ
  例：開発環境と本番環境の分離（ISO27001 附A.12.1.4/PCI DSS 6.4.1等）
- 直感や経験に基づく先入観に気をつける（認知バイアス）
- 「とはいってもね」と否定からスタートすると上手くいかない

運用を犠牲にしないためのコンセンサス

- 運用担当者は運用を変えたくない、だからといって運用を変えないために、運用のオーバーヘッドが増加することは不幸
- 運用の**変更に敏感である一方、追加に鈍感**であると陥りがち
- このことがコンプライアンスは面倒であると誤った印象を与えることに
- 特に、代替コントロールを許容するプログラムにおいて「要件に関連するリスクを十分に軽減していると示す追加の統制」は一般に煩雑

コンプライアンスプログラムは手順を増やすことを求めているわけではない

運用を楽にするにはどうすればいいのかを徹底的に考える/議論する

技術的安全管理措置

いわゆる保護メカニズムの設計・実装

- アクセスコントロール
- 暗号化と鍵管理
- 発見的統制 など

- 要求の粒度、具体性はコンプライアンスプログラム次第
- 第三者審査のあるプログラムでは、審査員（監査人）とのコンセンサスが重要
- 具体性に乏しい場合、他の基準や製品やサービスのプラクティスの再利用が有効

非技術的な管理措置

特に法律に基づくプログラムの場合、リーガル的な対応が求められるケースがある

たとえば、契約面での対応

- GDPRにおける標準契約条項（SCC）
- HIPAAにおける事業提携契約（BAA）

  など

各社の法務部門で内容を精査し、その解釈によって対応が必要（特に海外）

非技術的な管理措置の存在は予め織り込んでおく

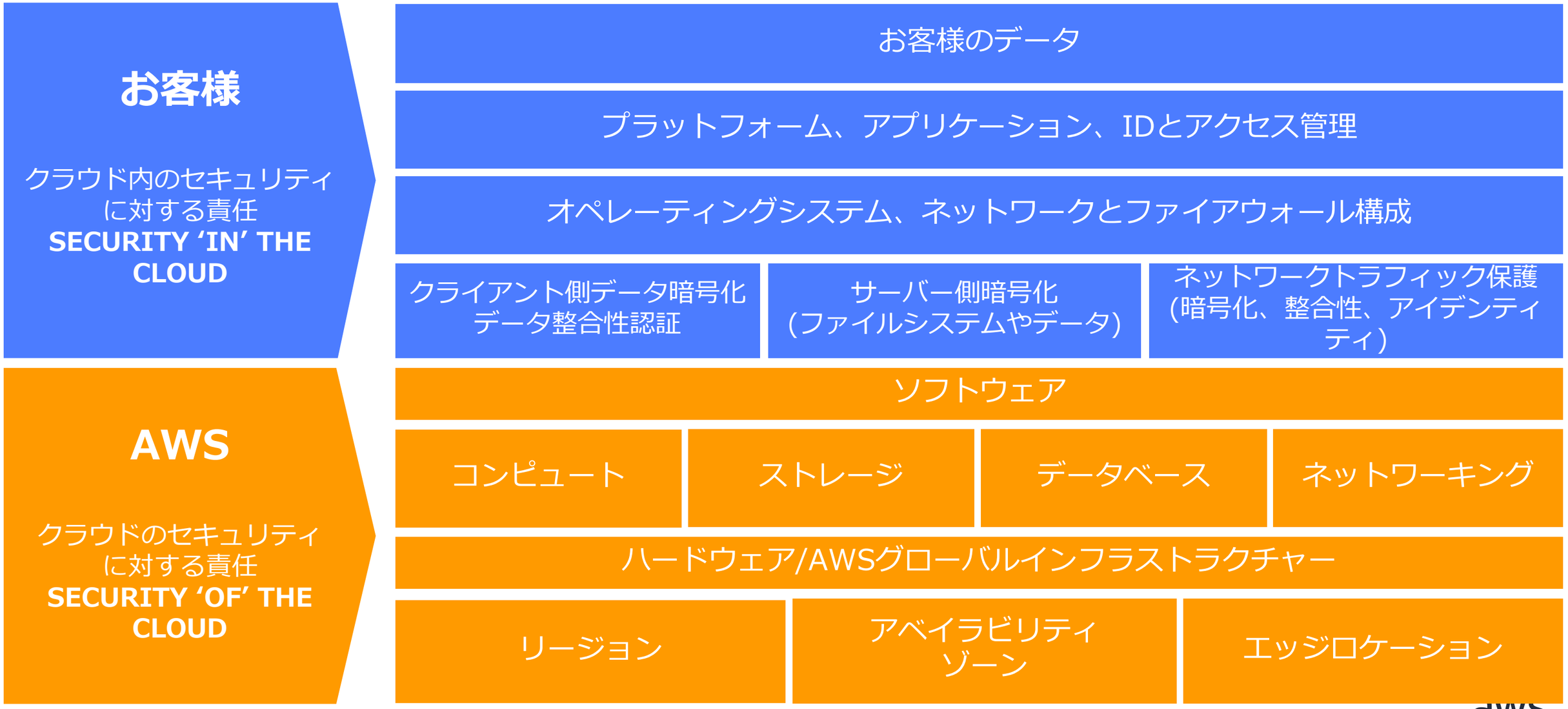
コンプライアンス対応で苦しまないために

- コンプライアンス担当者と運用担当者との良好な関係性は何より大事
- 運用担当者と目線をあわせて会話できる担当者をアサイン、あるいは育成する
- コンプライアンス担当者と独立監査部門は似て非なるもの、混同しない

外部の専門家の支援を得る場合にも重要なポイント

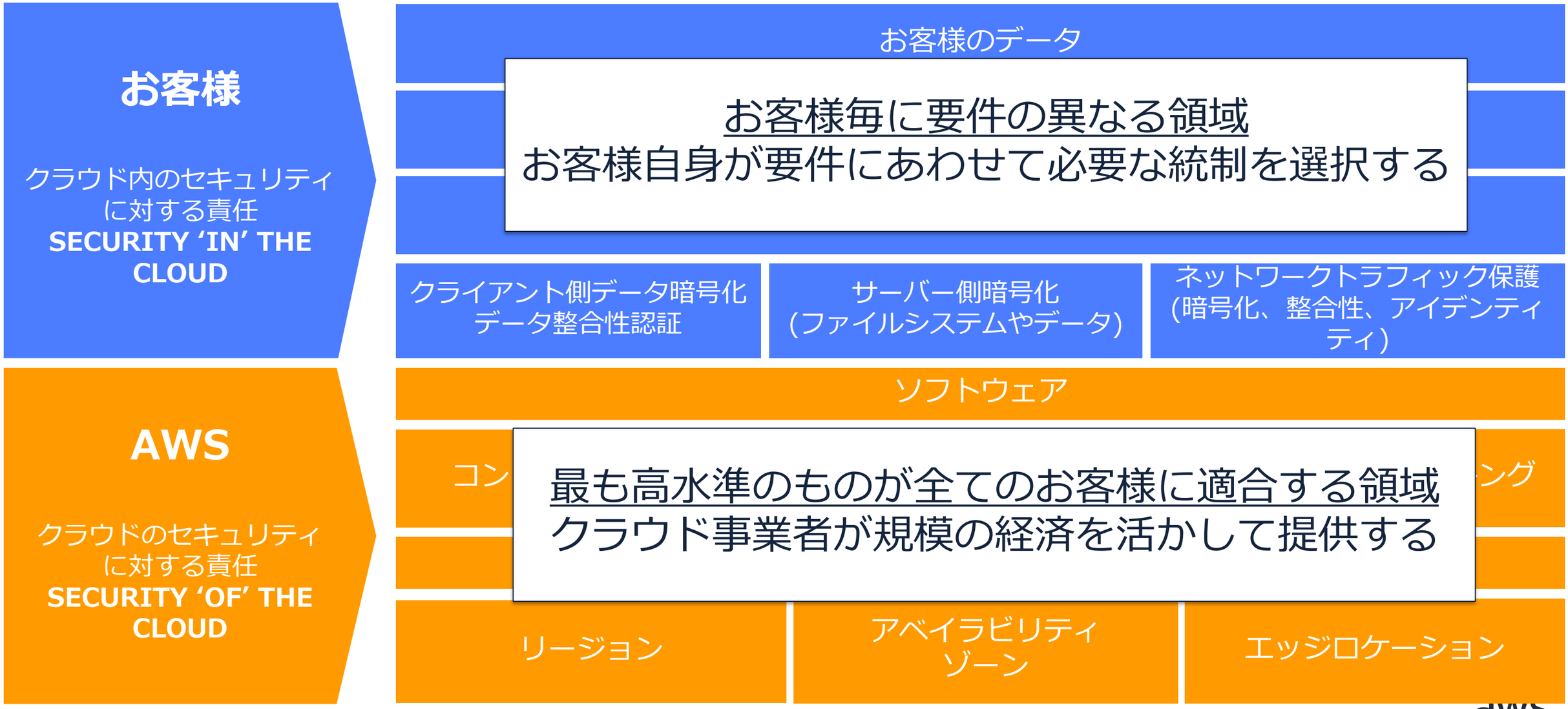
クラウドにおけるコンプライアンス対応

クラウドセキュリティの基本：責任共有モデル



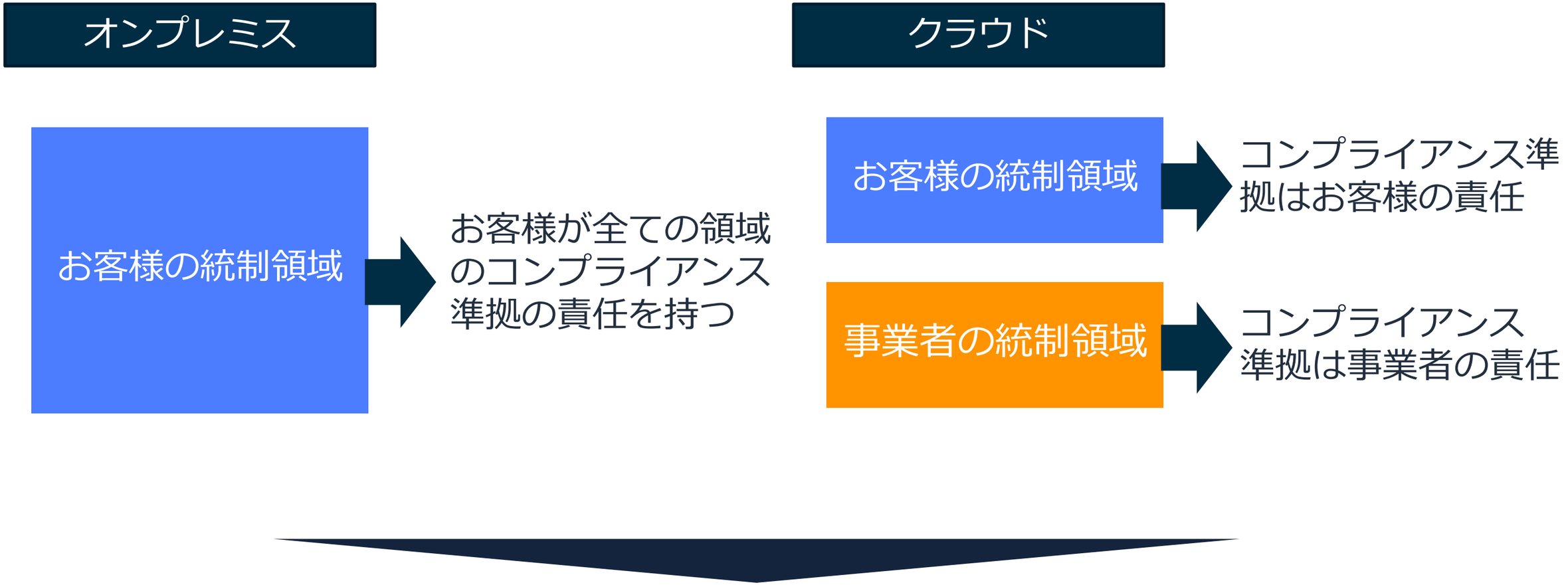
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

クラウドセキュリティの基本：責任共有モデル



https://aws.amazon.com/jp/compliance/shared-responsibility-model/

コンプライアンス対応も責任共有モデル



コンプライアンス対応の多くを事業者にオフロード出来ることを意味する

クラウド事業者“の”コンプライアンス対応

- たとえば、AWSでは世界各国のコンプライアンスプログラムに準拠している
- あらゆるワークロードをクラウドで動かすため規模の経済を生かし投資を継続している
- コンプライアンスは標準で付帯するサービスの性質、対応にあたって**利用者に追加の費用負担は発生しない**

など

準拠済みコンプライアンスの一覧
https://aws.amazon.com/jp/compliance/programs/

クラウド事業者の取り組み、その背景

クラウド事業者の都合

大規模なマルチテナント環境であるため、
お客様個別のリクエストに応えられない

× データセンターへの入館

× 運用担当者へのヒアリング

× 固有の質問への回答

利用者の本質的なニーズ

○ サービスを安心して使いたい

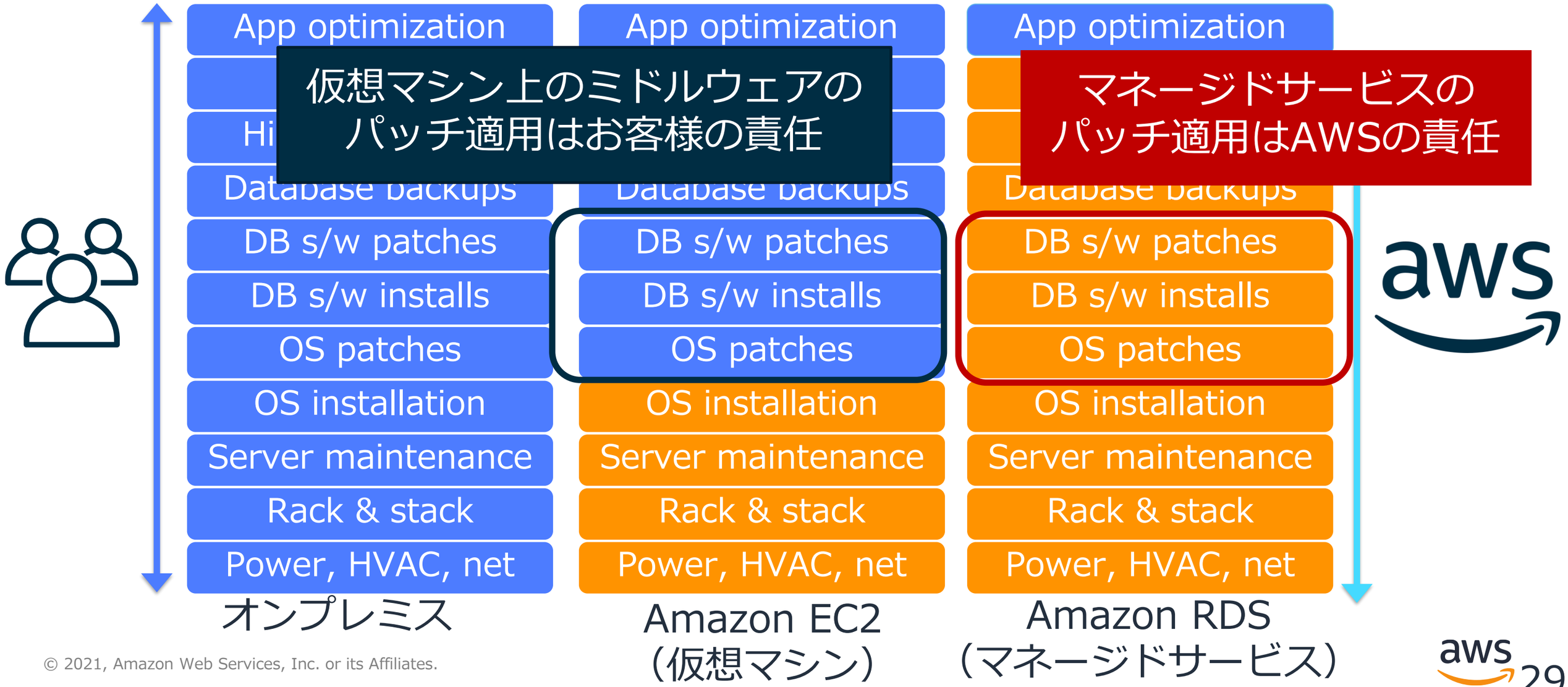
○ 統制が適切であることを説明したい

× 事業者を監査したい

統制の適切さを評価しお墨付きを出せる組織（＝独立監査人）に代表してチェックを依頼し、お客様にはその保証意見を確認して頂く

マネージドサービスの選択でより多くをオフロード可能に

たとえば、AWSにおけるデータベース管理



たとえば、AWSにおけるPCI DSS

- AWSはサービスプロバイダーとしてPCI DSSに準拠済み
- AWS のサービスは、お客様に代わってカード会員データを保存、処理、または送信しているかのようにその統制が審査されている
- お客様が効率的に準拠するための豊富なドキュメントをAWSから提供
- お客様は、お客様の責任範囲と明記されている統制を実装する責任がある
- サービス仕様はすべてのお客様で共通、プラクティスは変わらない（再利用可）

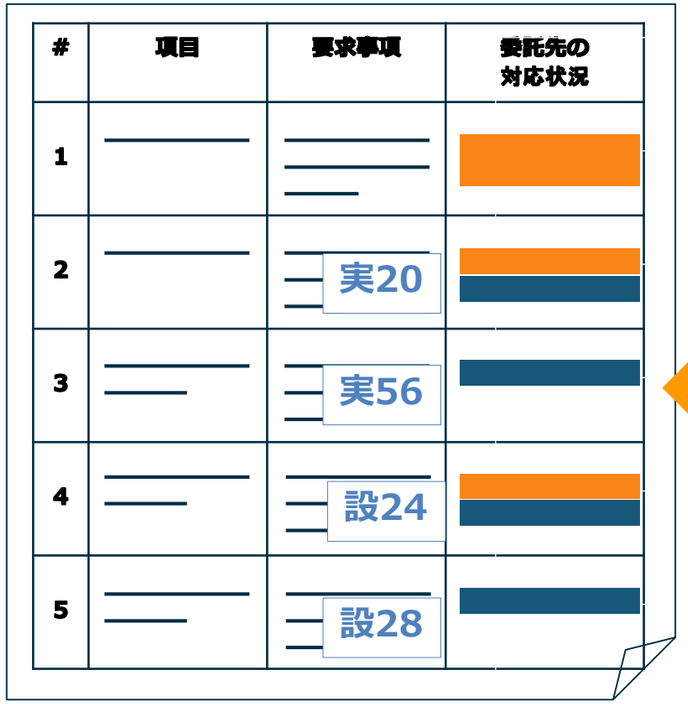
など

PCI コンプライアンス – アマゾン ウェブ サービス (AWS)
https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/

たとえば、AWSにおけるFISC安全対策基準

- 基準の要件とAWSの統制をマッピング、準拠性を容易に確認できるようにリファレンスを提供

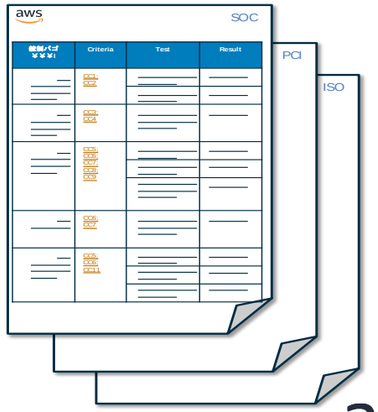
お客様の外部委託先チェック項目
（FISC安全対策基準ベース）



AWS FISC 安全対策基準
リファレンス

各項目番号への対応状況
を参考資料として提供

AWSホワイトペーパー



AWS Artifacts
（コンプライアンスレポート）

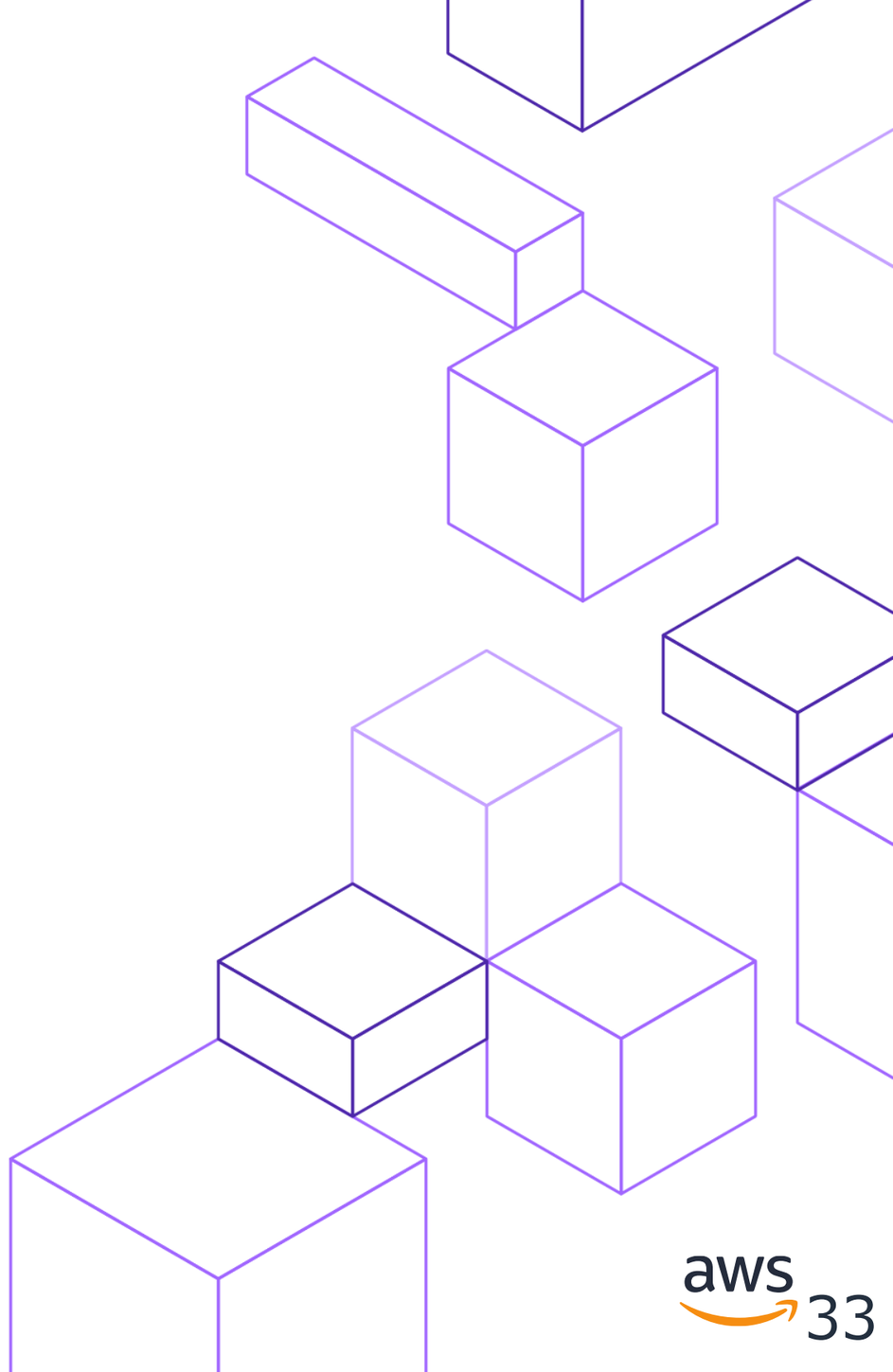
クラウドを使ってコンプライアンス対応を楽にしよう

- 責任共有モデルによってコンプライアンス対応を事業者にオフロードできる
- クラウド“の”コンプライアンス対応に追加の費用は不要
- 1対1の外部委託とは異なり、契約毎にプラクティスは変わらない

コンプライアンス対応を分担し利用者がやるべきことへの集中をもたらす

これがクラウドセキュリティの基本/責任共有モデル

まとめにかえて



コンプライアンスをセキュリティの友に

- 最も重要なことはコンプライアンス対応を通じてセキュリティを最適化すること
- コンプライアンスプログラムは本質的にベストプラクティスの集合体
- **再構築より再利用**、リファレンスとして賢く使う、車輪の再発明をしない

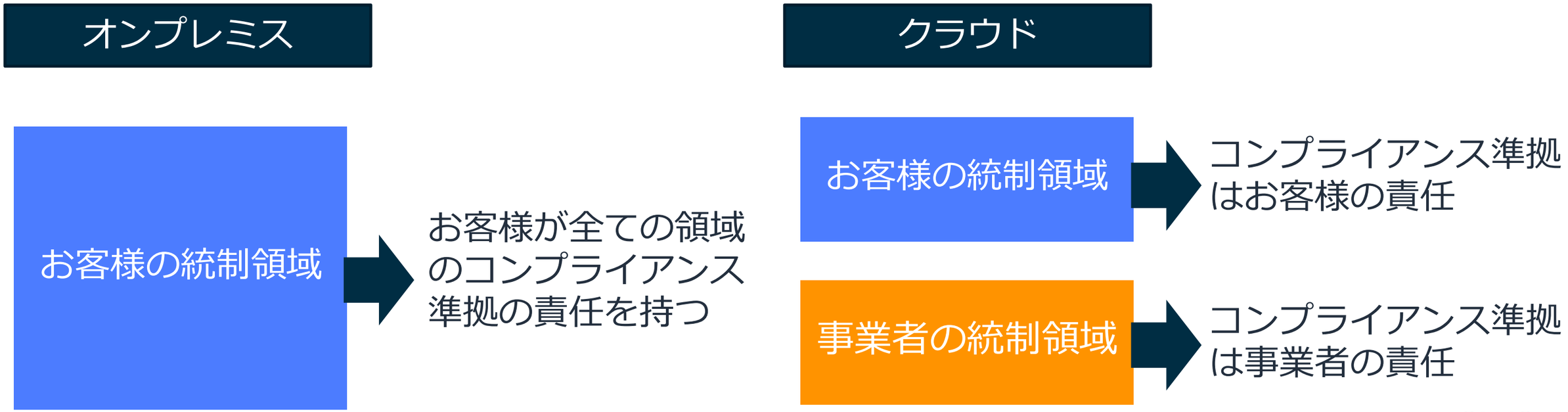
組織に必要なのは活用できるリソースを効率よく利用し、
かつ限りある経営資源を組織の強みにリンクすること

Simple is the BEST/アンチパターンを避けて楽をする

- コンプライアンスプログラムに倣うことはベストプラクティスに倣うこと
- 場当たり的な対応は運用コストを増大させる
- 意味づけを丁寧に、手段を目的にしない
- 運用担当者と目線をあわせて会話できる担当者をアサイン、あるいは育成する

クラウドがコンプライアンス対応を楽にする

- コンプライアンスはクラウドに標準で付帯する性質、追加費用なし
- 対応の多くを事業者にオフロードできる、**マネージドサービスで更に楽をする**
- コンプライアンス対応の効率化/省力化はクラウドが選ばれる理由のひとつ



お話したこと

基準、標準、規制などのコンプライアンスプログラムを活用することで
なぜセキュリティを効率よく最適化できるのか？（＝ベネフィット）

コンプライアンスプログラムを活用して
セキュリティを効率よく向上、最適化する方法や勘所（＝アプローチ）

クラウドでコンプライアンスプログラムへの対応が楽になる？
クラウドを活用する動き、その理由（＝トレンド）

後続プログラムのご案内

18:00
～
18:45

セキュリティ

C17 ISMAP(政府情報システムのためのセキュリティ評価制度)との付き合い方

講演者

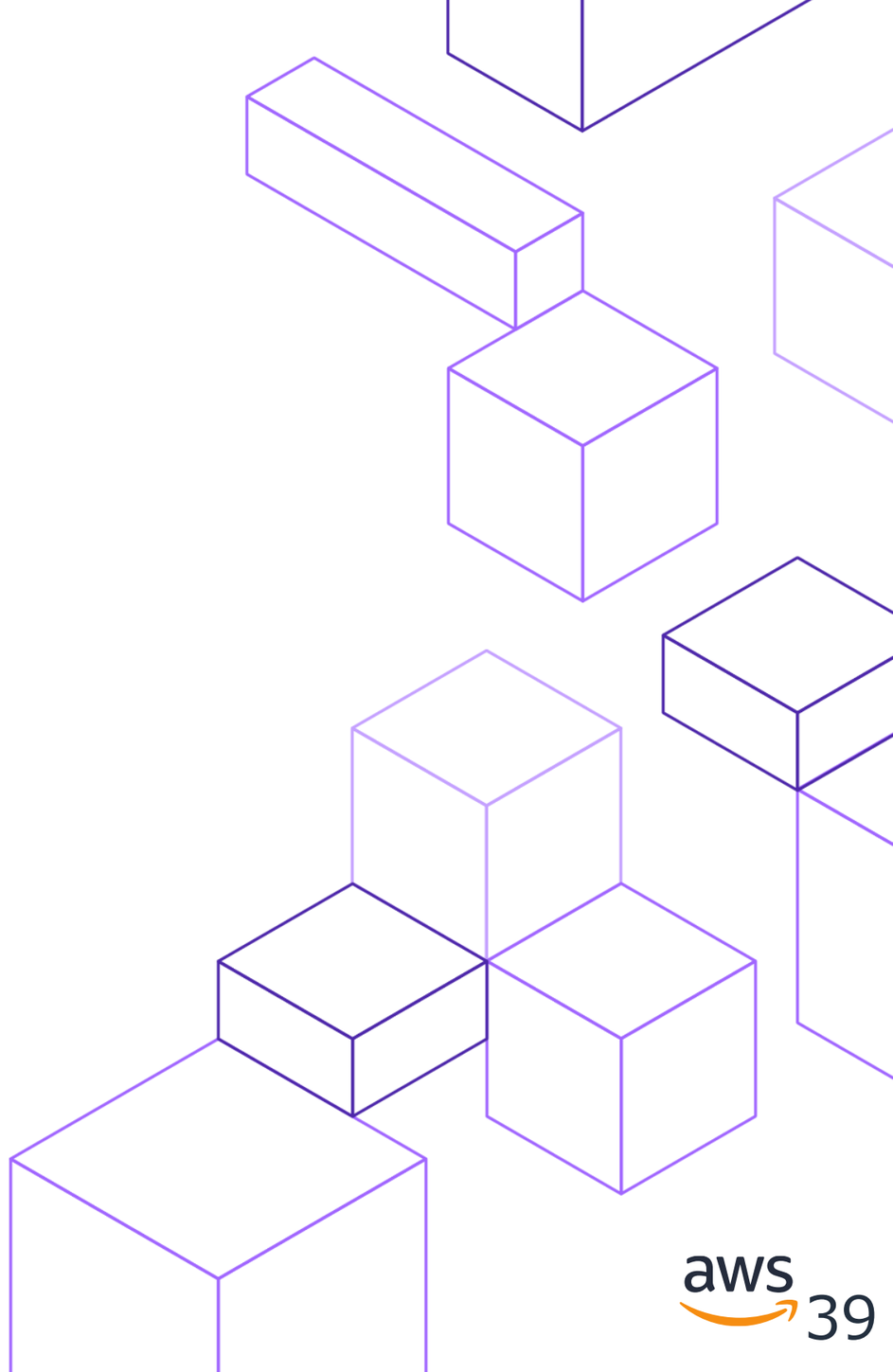

満塩 尚史

満塩 尚史(デジタル庁 戦略・組織グループ セキュリティ危機管理チーム セキュリティアーキテクト)

概要

政府情報システムのためのセキュリティ評価制度(Information system Security Management and Assessment Program:通称、 ISMAP(イスマップ)は、 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、 政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、 各府省の調達時のセキュリティ基準の対応の確認を効率化し、 結果としてクラウドサービスの円滑な導入に資することを目的とした制度です。 本プログラムでは、ISMAPの概要と現状を説明しつつ、 制度の利用者である政府情報システムの調達側が、 ISMAPをどのように利用するべきかについて解説し、更には、今後の展望について説明します。

Q&A



Thank you!