2019/02/23(土)@TOC五反田メッセ

【JAWS DAYS 2019】

Hトラック 14:10～15:00

Orchestrating a brighter world NEC

資料公開版 セッション後に一部のページについて追記や修正をしています。

【AWSセキュリティ入門】
徒然なるままに責任共有モデルの下から上までそこはかとなく解説

日本電気株式会社
サービスプラットフォーム事業部
クラウドアライアンスグループ（AWS担当）
大竹 孝昌

自己紹介

- 名前：大竹 孝昌
- 所属：日本電気株式会社
  SI・サービス＆エンジニアリング統括ユニット
  サービスプラットフォーム事業部
  クラウドアライアンスグループ
- 経歴：ft Server ⇒ CLUSTERPRO ⇒ AWS
- 好きなAWSサービス：Amazon S3

【個人活動】

ユーザーコミュニティの運営を少々

Security-JAWS
https://s-jaws.doorkeeper.jp/

SORACOM UG Tokyo
https://www.facebook.com/soracomug/

SORACOM 敏腕カメラマンによる思い出の一枚！
いつもありがとうございます！(if-up　2019にて)

※ SORACOM if-up 2019
https://if-up2019.soracom.jp/

本日のおしながき

つれづれなるままに、日暮らし、ＡＷＳに向かひて、心にうつりゆくセキュリティごとを、そこはかとなく書きつくれば、クラウドネイティブな気分だなぁ。

特に意味はありません

第壱段 ・・・責任共有モデルを理解する

第弐段 ・・・責任共有モデルの下の方

第参段 ・・・責任共有モデルの上の方

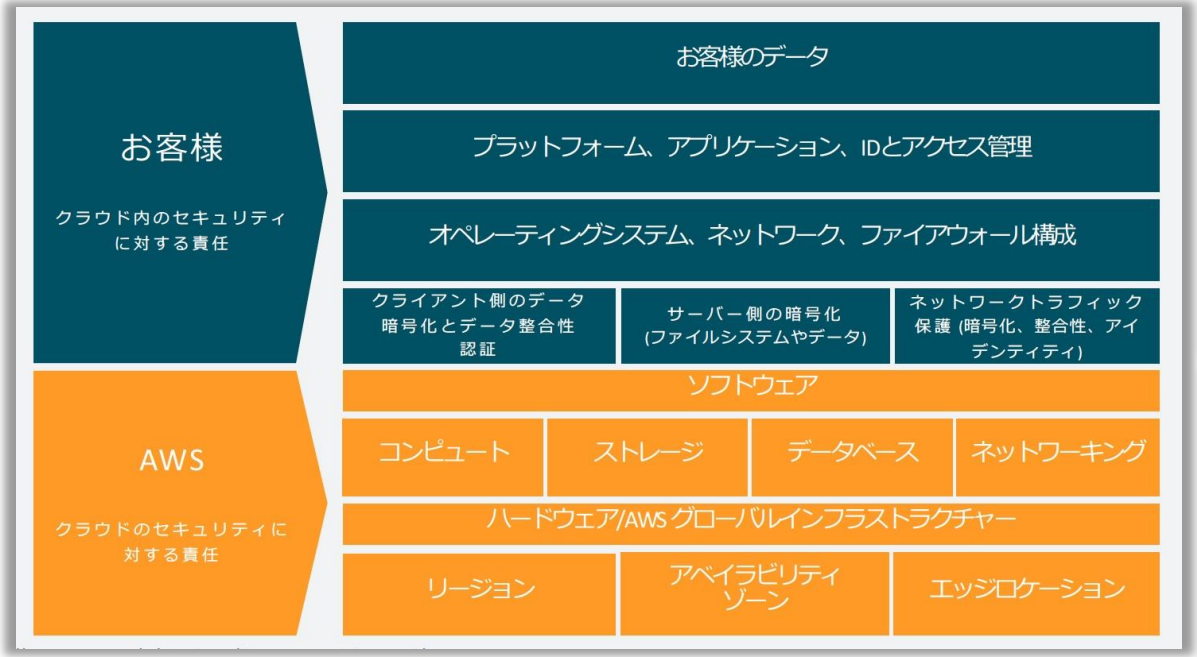
おまけ ・・・セキュアなアーキテクチャを目指して

【第壱段】

責任共有モデルを理解する

AWSの責任共有モデル

『セキュリティとコンプライアンスの責任』をAWSとお客様の間で共有



Security in the Cloud

お客様の責任範囲は、お客様が選択する AWS クラウドのサービスによって異なる。お客様が選択するサービスによって、セキュリティに関する責任の一環としてお客様が実行する必要がある構成作業の量が決まる。

『適切な使用』が重要

Security of the Cloud

AWSは、AWS クラウドで提供されるサービスすべてを実行するインフラストラクチャーの保護に責任を負う。

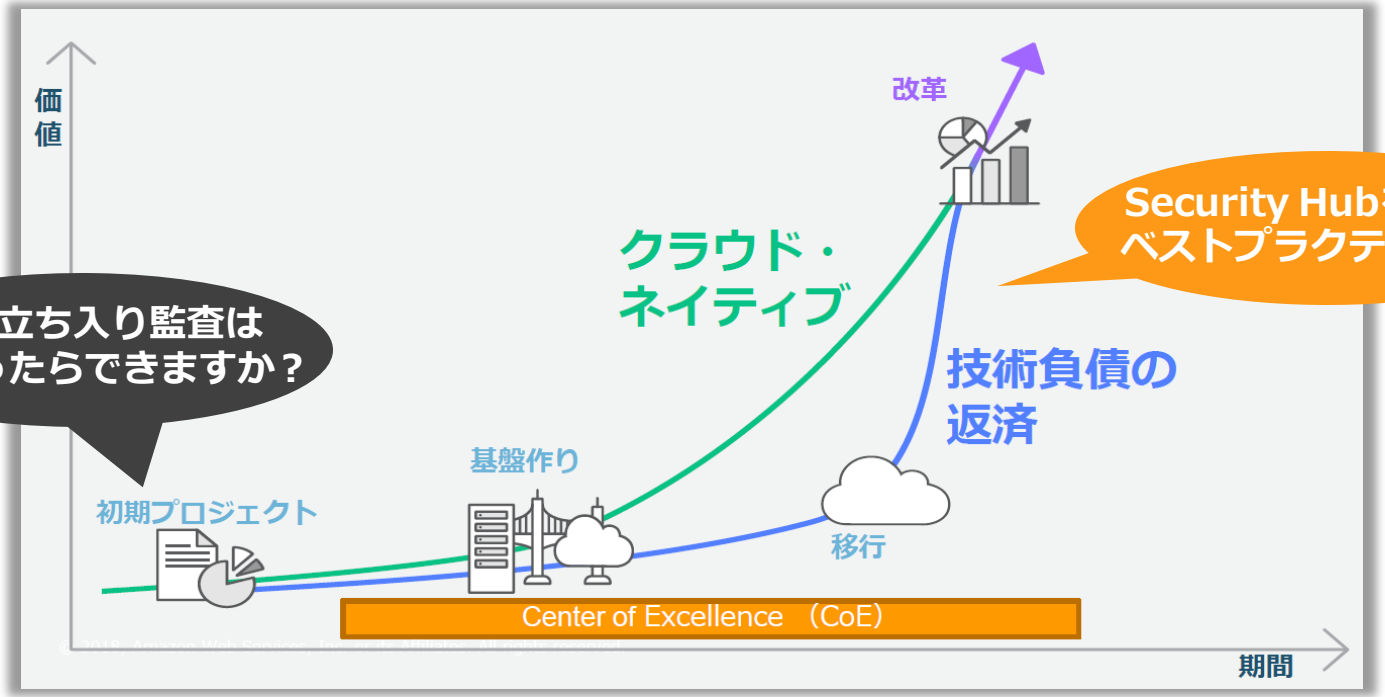
『正しい認識』が必要

※ 以下より抜粋：責任共有モデル
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

クラウドジャーニーと責任共有モデルに対する興味

皆さん、最初は下の方が気になって、次第に上の方に興味が移るようです

実体験に基づく
個人的な見解



※ 以下より抜粋：[AWS White Belt Online Seminar] クラウドジャーニー (AWSへの移行プロセスと移行ツール) 資料及び QA 公開
https://aws.amazon.com/jp/blogs/news/webinar-bb-migration-2018/

セキュリティに対する考え方

セキュリティは、AWSの最優先事項です。

- 基本的に内部の技術情報は非公開だが、公開されている情報は多岐にわたる

安全で規制に準拠したクラウド環境を運用できるように要件に合わせる形で様々なコンプライアンス報告書、証明書、認定書を提供している

明確な目的や目標もない状態で
内部の技術情報を求めても意味なし

AWS利用のポイント

コスト削減と拡張性を実現しながら、堅牢なセキュリティと規制の準拠を維持することが可能

【参考】
AWS Well-Architected Framewokにて
『セキュリティと運用上の優秀性は、通常、他の柱とトレードオフになることはありません。』との記述あり(他の柱…信頼性、パフォーマンス効率、コスト最適化)

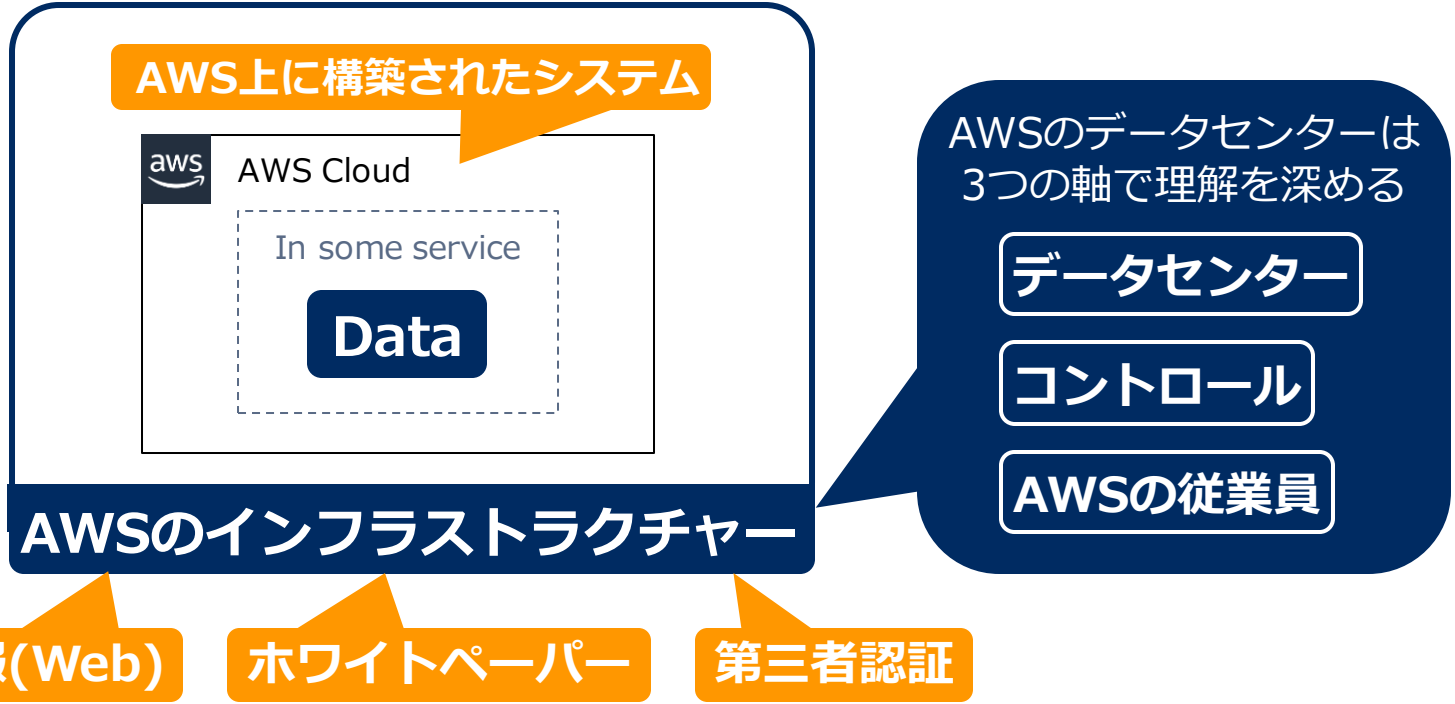
※ 詳しくは下記を参照：AWS のセキュリティ動画(日本語)の公開について
https://aws.amazon.com/jp/blogs/news/introducing-security-video-series/

【第弐段】

責任共有モデルの下の方

まずはこんな感じで理解

AWSのインフラストラクチャーは3つの視点で理解を深める



AWSのデータセンターを理解する

データセンター：境界防御レイヤー

- アクセスの綿密な検査
  - 業務上の正当な理由で立ち入る必要がある人々に限定して、物理的なアクセスを許可
- 立ち入りの規制と監視
  - 入り口ゲートには警備員を配置し、監視カメラで警備員と訪問者を監視する監督者も配置
- AWS データセンターの従業員も綿密な検査の対象
  - AWS の従業員は、職務に基づいて施設の該当するエリアへのアクセスを許可(毎回綿密に検査)
- 未承認の立ち入りに対する監視
  - サイトへの未承認の立ち入りは、ビデオ監視、侵入検出、およびアクセスログ監視システムを使用して継続的に監視
- AWS セキュリティオペレーションセンターによるグローバルなセキュリティ監視
  - 世界中に配置され、データセンターのセキュリティプログラムのモニタリング、対処順位の決定、実行を行う

※ 詳しくは下記参照：境界防御レイヤー
https://aws.amazon.com/jp/compliance/data-center/perimeter-layer/

AWSのデータセンターを理解する

データセンター：インフラストラクチャー・レイヤー

レイヤーごとのアクセスレビュー

他のレイヤーと同じように、インフラストラクチャー・レイヤーへのアクセスは業務ニーズに基づくように制限

装置の保守点検は日常業務の一環

マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働していることを確認

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築

※ 詳しくは下記参照：インフラストラクチャー・レイヤー
https://aws.amazon.com/jp/compliance/data-center/infrastructure-layer/

AWSのデータセンターを理解する

データセンター：データレイヤー

- テクノロジーとチームの連携によるセキュリティの強化
  - 承認されたユーザーによる、アクセス申請の確認と承認をしつつ、脅威検知システムと電子的な侵入検知システムで監視
- 物理的および技術的な侵入の阻止
  - サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護
- サーバーとメディアの厳重な監視
  - デバイスの設置、修理、および破棄 (最終的に不要になった場合) の方法について厳格な基準あり
    →ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止
- サードパーティーの監査者によるプロシージャとシステムの検証
  - AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けている

※ 詳しくは下記参照：データレイヤー
https://aws.amazon.com/jp/compliance/data-center/data-layer/

AWSのデータセンターを理解する

データセンター：環境レイヤー

不測の事態への備え

自動センサーと応答装置でデータセンターを保護
・漏水検知 ⇒ 自動ポンプの作動と従業員への通知
・自動火災検知 ⇒ 消火装置の作動と従業員と消防士への通知

複数のアベイラビリティーゾーンによる高可用性

各アベイラビリティーゾーンは 1 つ以上の相互に独立したデータセンターで構成
各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを装備

途絶のシミュレーションと反応の測定

定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施

AWS クラウドでのグリーン化の促進

100% の再生可能エネルギーを使用することを長期的な取り組みとしている
→ AWSへの移行にて、自社のDCを使用した場合と比較して、通常、サーバー数が 77% 減り、電力が 84% 減少

※ 詳しくは下記参照：環境レイヤー
https://aws.amazon.com/jp/compliance/data-center/environmental-layer/

AWSのデータセンターを理解する

コントロール：セキュアな設計

サイトの選択

場所を選択する前に、始めに環境評価および地理的評価を実施し、洪水、異常気象、地震活動などの環境リスクを軽減

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計
→ 障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動
→ 重要なアプリケーションは N+1 の基準でデプロイされている

可用性

各アベイラビリティーゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計
→ 重要なシステムコンポーネントは、アベイラビリティーゾーンにバックアップ

キャパシティの計画

サービスの利用状況を継続的にモニタリング
→ アベイラビリティーに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：ビジネス継続性と災害復旧

- BCP(BUSINESS CONTINUITY PLAN)；事業継続計画

環境に起因するサービス障害の回避および軽減措置について記載
→ まざまなシナリオのシミュレーションを含むテストによってサポート
→ テスト中およびテスト後は、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録(継続的な改善)

- パンデミックへの対応

パンデミック対応ポリシーと手順を災害復旧計画に組み込み(感染症の爆発的な流行の脅威に対して迅速に対応するため)

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：物理アクセス

従業員によるデータセンターへのアクセス

権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可

第三者のデータセンターへのアクセス

承認された AWS の担当者が申請する必要あり
→ 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あり
→ 申請は最少権限の原則に基づいて付与

AWS GOVCLOUD データセンターへのアクセス

米国市民または永住者であると確認された従業員または請負業者に制限

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：モニタリング & ロギング

- モニタリング & ロギング
  - データセンターへのアクセスは、定期的に確認
- データセンターのアクセスログ
  - AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持
- データセンターへのアクセスの監視
  - AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、専門の保安要員によって厳重に管理
(サーベイランスシステム、侵入検知システム、その他の電子的システムが用いられてる)

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置
→ セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われる

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：デバイスの管理

アセットの管理

インベントリ管理システム※を通じて、一元管理
※AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡

メディアの破壊

デバイスの設置、修理、および破棄 (最終的に不要になった場合) の方法について厳格な基準あり
→ ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：運用サポートシステム

パワー

データセンターの電力システムは、完全に冗長化され、運用に影響を与えることなく管理が可能
→ 電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証

空調と温度

サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズム
→ 作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロール

火災検出と鎮火

自動火災検出システムおよび鎮火システムが設置

漏水検出

水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムを備えている

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

必読！

【ちょっと息抜き】
AWSを利用すべきもう1つの理由は「メカニズム」の実装である
http://ascii.jp/elem/000/001/773/1773604/
https://www.slideshare.net/KamedaHarunobu/jaws-festa-2018

AWSのデータセンターを理解する

コントロール：インフラストラクチャーのメンテナンス

設備の保守

電気および機械に関連する設備をモニタリング
→ 予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持

環境管理

モニタリングは継続的な監査ツールと、建物管理および電気的なモニタリングシステムを通じて提供される情報を利用

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

コントロール：ガバナンスとリスク

継続的なデータセンターのリスク管理

AWS セキュリティオペレーションセンターは、データセンターの脅威と脆弱性の確認を定期的に実施

第三者によるセキュリティ認証

AWS データセンターに対する第三者の検証
→ AWS がセキュリティ認証取得に必要となるルールを確立するためのセキュリティ対策を適切に実装していることが保証
→ 外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施

※ 詳しくは下記参照：AWSのコントロール
https://aws.amazon.com/jp/compliance/data-center/controls/

AWSのデータセンターを理解する

AWSの従業員：DC勤務かどうかに関わらずセキュリティが最優先

AWSのカルチャー

続きはWebで！

※ 詳しくは下記参照：AWSの従業員
https://aws.amazon.com/jp/compliance/data-center/people/

AWSのグローバルインフラストラクチャを理解する

20のリージョンと60のアベイラビリティゾーン(2019年2月時点)

複数のアベイラビリティーゾーンによる高可用性

各 AWS リージョンには複数のアベイラビリティーゾーンとデータセンターが存在
(アベイラビリティーゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続)

リージョン間レプリケーションによる継続性の向上

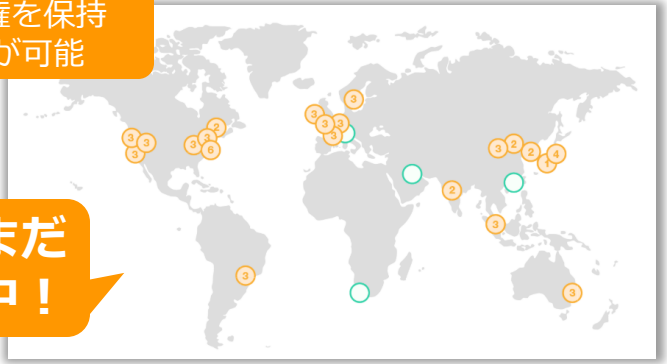
地理的リージョンを越えたデータレプリケーションにより冗長性と耐障害性を増大させることも選択可能
(アベイラビリティーゾーンを使用した同一リージョン内でのアプリケーションやデータのレプリケーション)

コンプライアンスおよびデータレジデンシー要件を満たす

データが物理的に存在するリージョンについてはお客様が完全な管理権と所有権を保持
→ 地域的なコンプライアンス要件およびデータレジデンシー要件を満たすことが可能

地理的拡張

12 のアベイラビリティーゾーンを追加して拡張する予定
(2019年 2 月時点の情報)



※ 詳しくは下記参照：グローバルインフラストラクチャ
https://aws.amazon.com/jp/about-aws/global-infrastructure/

AWSのデータプライバシーを理解する

コンテンツの所有権と管理権はAWSの利用者が持つ

アクセス

お客様は、お客様のコンテンツに対するアクセスと、AWA サービスおよびリソースに対するユーザーアクセスを管理可能
『お客様の同意を得ることなく、お客様のコンテンツにアクセスしたり、それを使用したりすることはありません』by AWS

保存

お客様は、コンテンツを保存する AWS リージョンを選択可能

『お客様の同意を得ることなく、お客様が選択したAWSリージョンの外にコンテンツを移動したり複製したりすることはありません』by AWS

セキュリティ

お客様は、コンテンツを保護する方法を選択可能

カスタマーコンテンツの開示

『AWSがカスタマーコンテンツを開示することはありません』by AWS
(法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令に従うために必要な場合を除く)

セキュリティ保証

セキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、個別に検証

※ 詳しくは下記参照：データプライバシー
https://aws.amazon.com/jp/compliance/data-privacy-faq/

日本における災害対策を理解する

一般的なDR対策に使用されるアーキテクチャの多くを実装可能

- 災害対策と事業継続
  - 災害対策は災害に対しての用意と復旧の両方を含むもの
- 責任共有モデル: DR/BCにおけるAWSサービスの使用について
  - AWSのシステムは、お客様への影響を最小限に抑えながら、システムまたはハードウェア障害に耐えられるように設計
    (アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに接続)
- 日本のデータセンターのレジリエンシー
  - 日本のデータセンターは日本の震災に関する規格に準拠するように設計

※ 詳しくは下記参照：日本の災害対策関連情報
https://aws.amazon.com/jp/compliance/jp-dr-considerations/

AWS Direct Connect をサポートする APN パートナー
https://aws.amazon.com/jp/directconnect/partners/

AWSのホワイトペーパーで理解を深める

リスクとコンプライアンス

AWSリスクとコンプライアンス概要(2017年1月)

ホワイトペーパーより抜粋

責任共有環境
お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。

リスク管理
AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性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）。

統制環境
当社では従業員に対し、その職務と AWS 施設へのアクセスレベルに応じて、法律および規制が許可する範囲内での学歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。

情報セキュリティ
公開ウェブサイトでは、お客様がデータを保護するために有効な方法を解説したセキュリティホワイトペーパーを公開しています。

※ 以下より抜粋：AWS リスクとコンプライアンスの概要 (2017 年 1 月)
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Overview_JP.pdf

AWSのホワイトペーパーで理解を深める

リスクとコンプライアンス

AWSリスクとコンプライアンス(2015年12月)


アマゾン ウェブ サービスのリスクとコンプライアンス 2015 年 12 月

amazon web services

アマゾン ウェブ サービス: リスクとコンプライアンス

2015 年 12 月

(本書の最新版については、http://aws.amazon.com/compliance/aws-whitepapers/

を参照してください)

ページ 1 - 108

最新情報は別ホワイトペーパーにて
⇒ 主要なコンプライアンスに関する質問とAWSの回答

コンプライアンスに関するよくある質問

AWSクラウドコンピューティングに関する質問

データセンター訪問。クラウドプロバイダーでは、ユーザーによるデータセンター訪問を許可していますか?

AWSの情報

いいえ。AWS のデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポートの一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。この広く受け入れられているサードパーティーによる検証によって、お客様は実行されている統制の効果について独立した観点を得ることができます。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。データセンターの物理的なセキュリティの個別の確認も、ISO 27001 監査、PCI 評価、ITAR 監査、FedRAMPsm テストプログラムの一部となっています。

ホワイトペーパーより抜粋

※ 以下より抜粋：AWS リスクとコンプライアンス (2015年 12 月)
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

AWSのホワイトペーパーで理解を深める

リスクとコンプライアンス

AWSリスクとコンプライアンス(2015年12月)

最新情報は別ホワイトペーパーにて
⇒ CSA Consensus Assessments Initiative Questionnair

付録 A: CSA Consensus Assessments Initiative Questionnaire v3.0.1

統制グループ
アイデンティティおよびアクセス管理(IAM-09.2)

コンセンサス評価の質問
申請があった場合、ユーザー (従業員、請負業者、お客様 (テナント)、ビジネスパートナー、サプライヤーなど) がデータおよび所有/管理する (物理または仮想) アプリケーション、インフラストラクチャシステム、およびネットワークコンポーネントにアクセスできるようにしますか?

AWSの回答
AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。すべての認定とサードパーティーによる証明で、論理アクセスの予防統制と検出統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています

ホワイトペーパーより抜粋

※ 以下より抜粋：AWS リスクとコンプライアンス (2015年 12 月)
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

AWSのホワイトペーパーで理解を深める

リスクとコンプライアンス

主要なコンプライアンスに関する質問とAWSの回答(2017年1月)

ホワイトペーパーより抜粋

AWSクラウドコンピューティングに関する質問
特権的アクションは監視および統制されていますか?

AWSの情報
所定の統制によってシステムとデータ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可能にしています。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、および FedRAMPsm の監査中に独立監査人によって確認されます。

AWSクラウドコンピューティングに関する質問
保守目的でシステムを停止する予定が決められていますか?

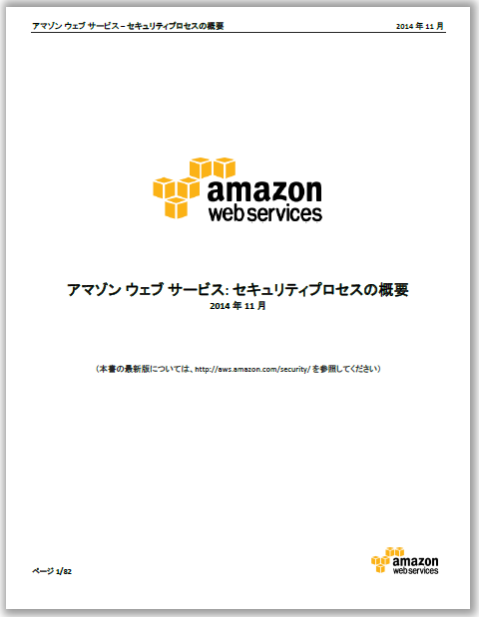
AWSの情報
AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要はありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。インスタンス自体の保守はお客様が統制します。

※ 以下より抜粋：主要なコンプライアンス に関する質問と AWSの回答 (2017 年 1 月)
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

AWSのホワイトペーパーで理解を深める

セキュリティプロセス

AWS: セキュリティプロセスの概要 (2014年 11月)



ホワイトペーパーより抜粋

AWS グローバルインフラストクチャのセキュリティ

物理的および環境のセキュリティ 物理的および環境のセキュリティ

ストレージデバイスの廃棄

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は、DoD 5220.22-M（「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。廃棄された磁気ストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。

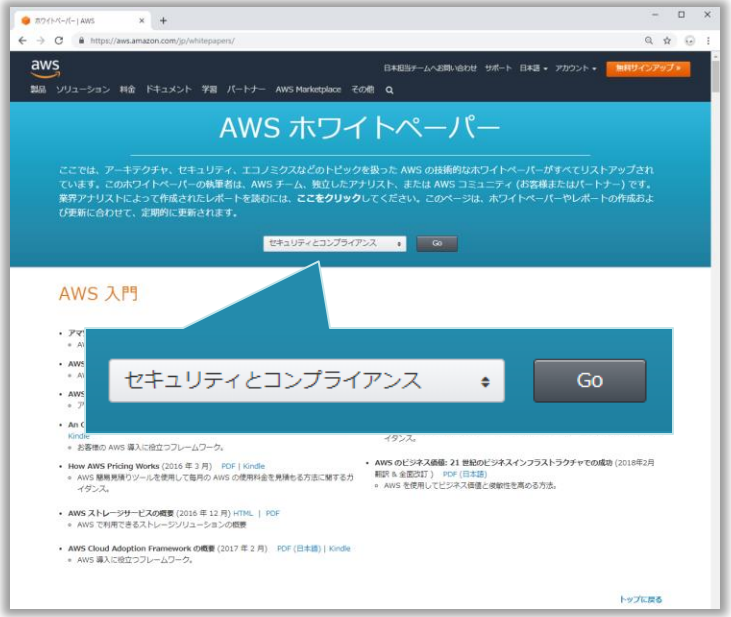
※ 以下より抜粋：AWS: セキュリティプロセスの概要 (2014年 11 月)
https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWSのホワイトペーパーで理解を深める

更に理解を深めたい！⇒日本語化されているものから攻めるべし

- HIPAA向けのホワイトペーパーもオススメ！

※ 詳しくは下記を参照：HIPPA
https://aws.amazon.com/jp/compliance/hipaa-compliance/

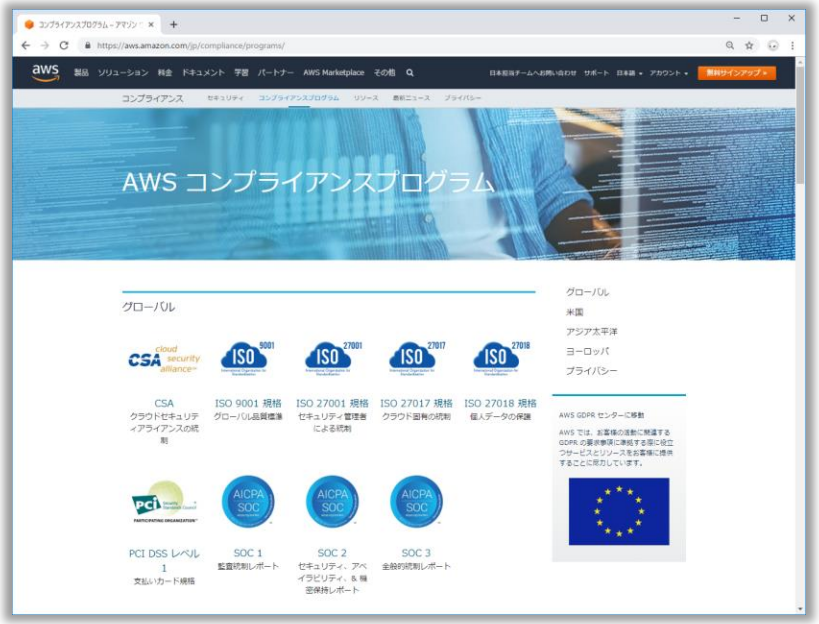


※ 詳しくは下記を参照：AWSホワイトペーパー
https://aws.amazon.com/jp/whitepapers/

AWSに対する第三者評価で理解を深める

AWS コンプライアンスプログラム

グローバル

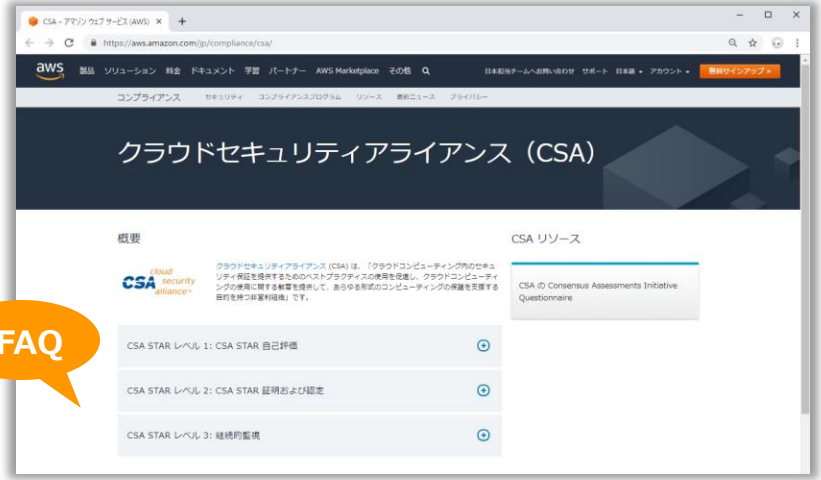


※ 詳しくは下記を参照：AWSコンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

AWSに対する第三者評価で理解を深める

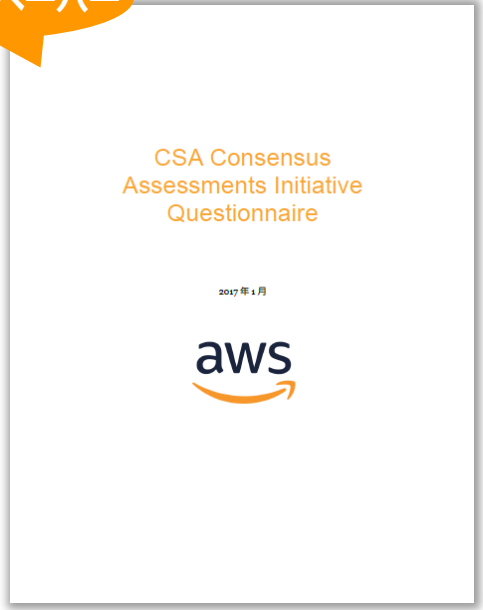
AWS コンプライアンスプログラム

クラウドセキュリティアライアンス（CSA）



FAQ

ホワイトペーパー



※ 詳しくは下記を参照：AWSクラウドセキュリティアリアンス(CSA)
https://aws.amazon.com/jp/compliance/csa/

※ 詳しくは下記を参照：CSA Consensus Assessments Initiative Questionnair（2017 年 5 月）
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/CSA_Consensus_Assessments_Initiative_Questionnaire_JP.pdf

AWSに対する第三者評価で理解を深める

AWS コンプライアンスプログラム

PCI DSS への準拠

FAQ

PCI DSS : Payment Card Industry Data Security Standard
⇒ クレジットカード業界の機密情報のセキュリティ標準

AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

以下は AWS Artifact より取得

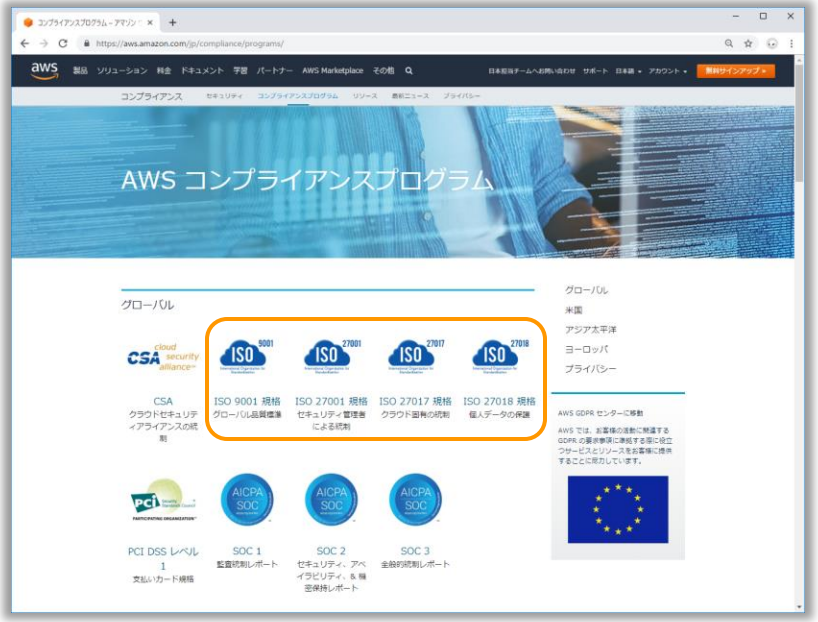
PCI DSS Attestation of Compliance (AOC) and Responsibility Summary

※ 詳しくは下記を参照：PCI DSS への準拠
https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/

AWSに対する第三者評価で理解を深める

AWS コンプライアンスプログラム

ISO 9001、ISO 27001、ISO 27017、ISO 27018



※ 詳しくは下記を参照：AWSコンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

ISO：国際標準化機構
(International Organization for Standardization)

ISO 9001　：品質
ISO 27001：情報セキュリティ
ISO 27017：クラウド向け情報セキュリティ
ISO 27018：クラウド向け個人情報保護

詳しくは下記を参照
ISO 9001：https://aws.amazon.com/jp/compliance/iso-9001-faqs/
例えば、

AWSにおける『品質』の定義
『機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能』

ISO 27001：https://aws.amazon.com/jp/compliance/iso-27001-faqs/
ISO 27017：https://aws.amazon.com/jp/compliance/iso-27017-faqs/
ISO 27018：https://aws.amazon.com/jp/compliance/iso-27018-faqs/

AWSに対する第三者評価で理解を深める

AWS コンプライアンスプログラム

SOC 1、SOC 2、SOC 3

- SOC 1 レポート – AWS Artifact でダウンロードする
- SOC 2: セキュリティ、可用性、機密性レポート – AWS Artifact でダウンロードする
- SOC 3: セキュリティ、可用性、機密性レポート

以下は AWS Artifact より取得

Service Organization Controls (SOC) 1 Report
Service Organization Controls (SOC) 2 Report
Service Organization Controls (SOC) 3 Report

日本語版はレポートの有効期限に注意が必要

など

AWS SOC3 レポート
(AWS SOC 2レポートの要約)

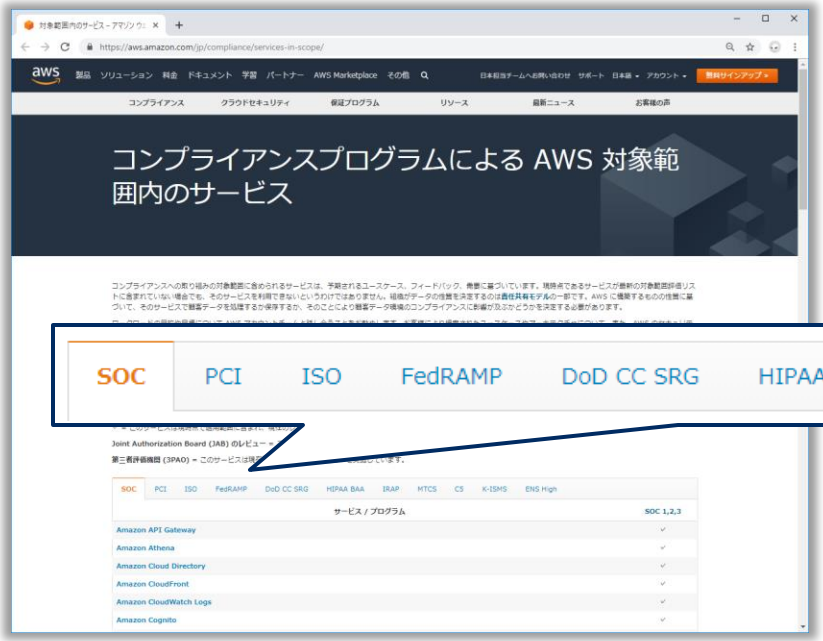
ホワイトペーパーとして公開
(秘密保持契約(NDA)が不要)

※ 詳しくは下記を参照：SOC コンプライアンス
https://aws.amazon.com/jp/compliance/soc-faqs/

AWSに対する第三者評価で理解を深める

コンプライアンス要件の厳しいシステムではサービス単位で確認すべし

- コンプライアンスプログラムによる AWS 対象範囲内のサービス



※ 詳しくは下記を参照：コンプライアンスプログラムによる AWS 対象範囲内のサービス
https://aws.amazon.com/jp/compliance/services-in-scope/

AWSに対する第三者評価で理解を深める

AWS コンプライアンスプログラム

アジア太平洋

責任共有モデルの『上の方』に効く
ネタがたくさん詰まっているので
ジャンル違いでも眺める価値あり！

※ 詳しくは下記を参照：AWSコンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

【第参段】

責任共有モデルの上の方

AWSを利用するその前に

翻訳はあくまで参考 ⇒ 正確な/最新の情報は英語版をチェックすべし

法務関連

- **AWS カスタマーアグリーメント** – このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです
- **AWS サービス条件** – この追加条件は、お客様による特定のサービスのご利用に対して適用されます
- **AWS サービスレベルアグリーメント** – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます
- **AWS 適正利用規約** – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
- **AWS 商標使用ガイドライン** – この商標使用ガイドラインは、商標およびその他の表示の利用に関するガイドラインを記載したものです
- **AWS サイト規約** – このサイト規約は、お客様による AWS ウェブサイトのご利用について規定するものです
- **プライバシー規約** – このプライバシー規約は、お客様の情報をどのように使用し、共有するかについて記載したものです
- **AWS 税務ヘルプ** – このページでは、当サービスに適用される税に関する情報を提供します
- **AWS Europe** – このページでは AWS Europe に関する情報を提供します

下記4点は要チェック！

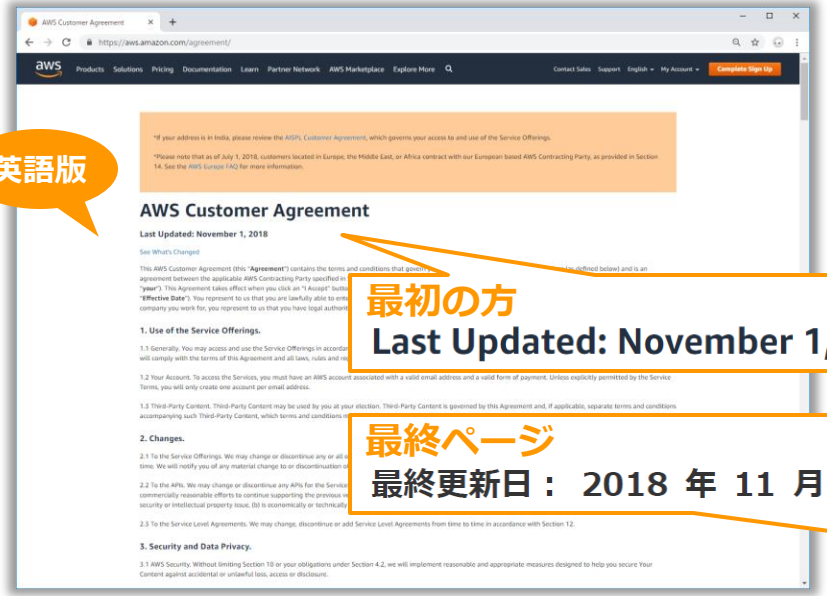
- **AWS カスタマーアグリーメント**
- **AWS サービス条件**
- **AWS サービスレベルアグリーメント**
- **AWS 適正利用規約**

※ 詳しくは下記を参照：法務関連
https://aws.amazon.com/jp/legal/

AWSを利用するその前に

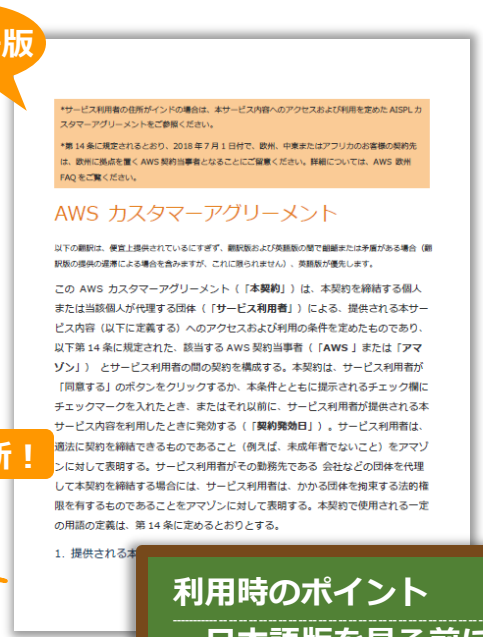
AWSのサービスは『合意』をして利用するもの

AWSカスタマーアグリーメント



最初の方
Last Updated: November 1, 2018

最終ページ
最終更新日： 2018 年 11 月 1 日



最新！

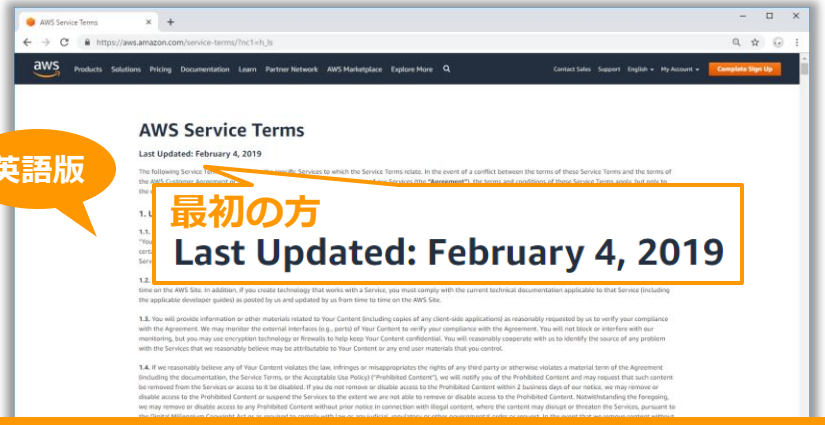
利用時のポイント
- **日本語版を見る前に英語版の更新日を確認**
- **『頻繁に更新されるもの』として扱う**

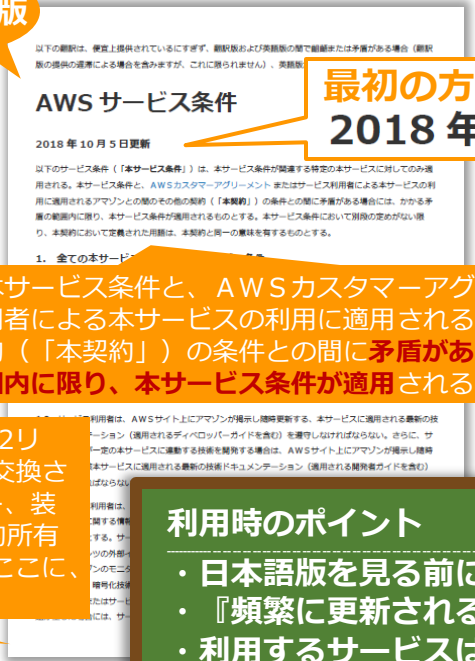
※ 詳しくは下記を参照：AWS カスタマーアグリーメント
https://aws.amazon.com/jp/agreement/

AWSを利用するその前に

AWS全体、各サービスについて大事な記載があるので要チェック！

AWSサービス条件





本サービス条件と、ＡＷＳカスタマーアグリーメント またはサービス利用者による本サービスの利用に適用されるアマゾンとの間のその他の契約（「本契約」）の条件との間に**矛盾がある場合には、かかる矛盾の範囲内に限り、本サービス条件が適用**されるものとする。

4.11 Amazon EC2を利用することの一環として、サービス利用者は、Amazon EC2リソースが、故障、リタイアメントまたはその他のＡＷＳ要件を理由として終了または交換される場合があることに同意する。 （中略）Amazon EC2の利用は、AWSのサーバー、装置、不動産、動産、またはその他の財産への物理的アクセス、またはそれらの物理的所有に関する権利をサービス利用者に与えるものではなく、また、サービス利用者は、ここに、かかる権利を放棄する。

利用時のポイント

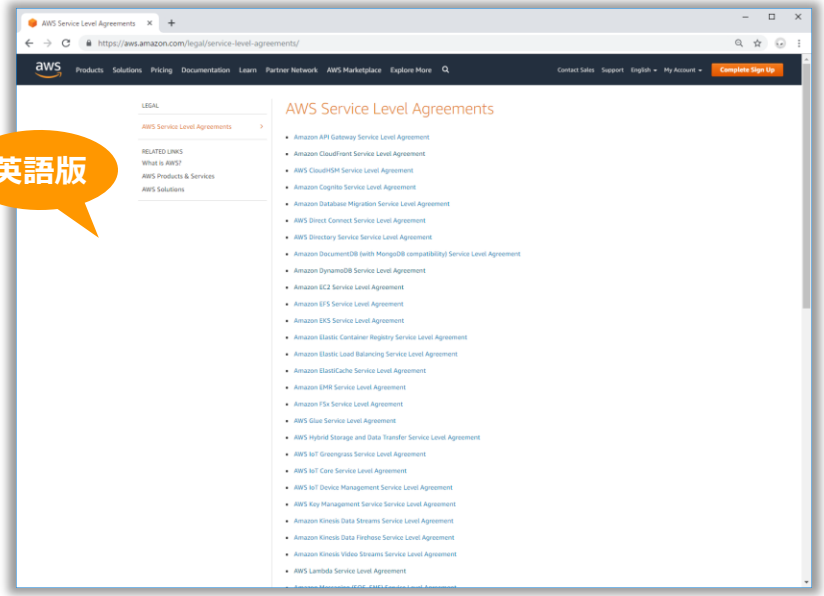
- **日本語版を見る前に英語版の更新日を確認**
- **『頻繁に更新されるもの』として扱う**
- **利用するサービスは事前に確認するのが吉**

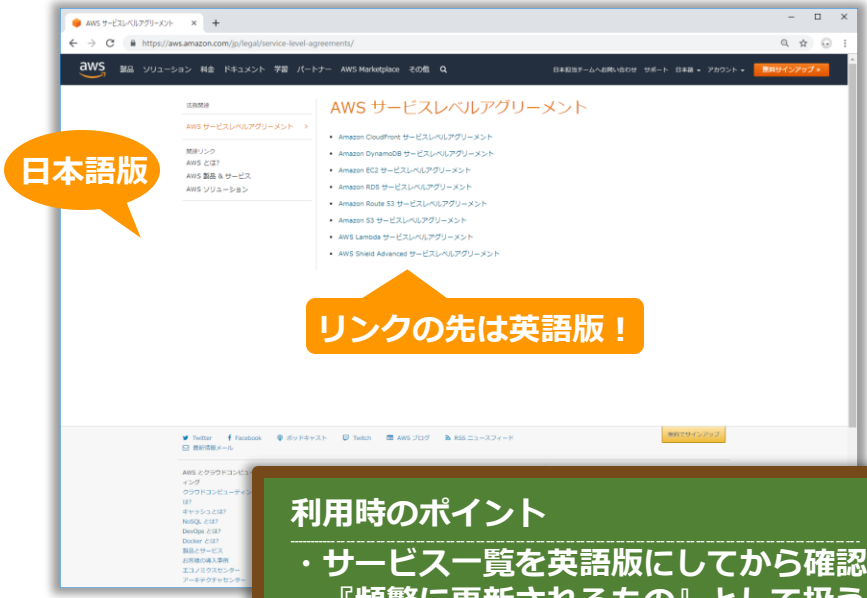
※ 詳しくは下記を参照：AWS カスタマーアグリーメント
https://aws.amazon.com/jp/agreement/

AWSを利用するその前に

システムのSLAを定義する前に利用するサービスのSLAを確認すべし

AWSサービスレベルアグリーメント





利用時のポイント

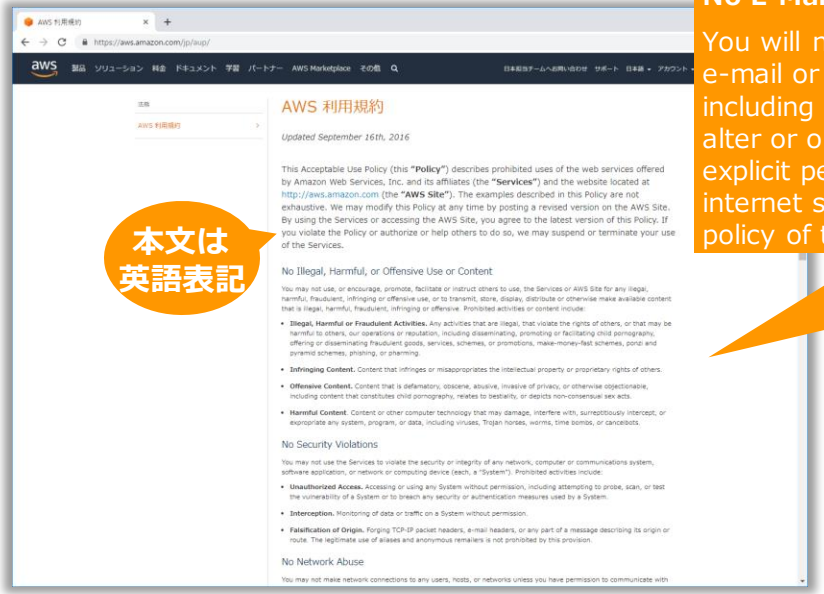
- サービス一覧を英語版にしてから確認
- 『頻繁に更新されるもの』として扱う（更新頻度はサービスに依存）

※ 詳しくは下記を参照：AWS サービスレベルアグリーメント
https://aws.amazon.com/jp/legal/service-level-agreements/

AWSを利用するその前に

ルールを守って正しく使おう！

AWS利用規約



本文は英語表記

No E-Mail or Other Message Abuse

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (**like “spam”**), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

利用時のポイント

- **検証時に意図せず違反してしまうリスクあり**
  → 申請が必要なケースあり※
- **SES利用時に意図せず違反してしまうリスクあり**
  → SESのFAQやガイド、ホワイトペーパーなど関連するドキュメントをしっかり確認しよう！

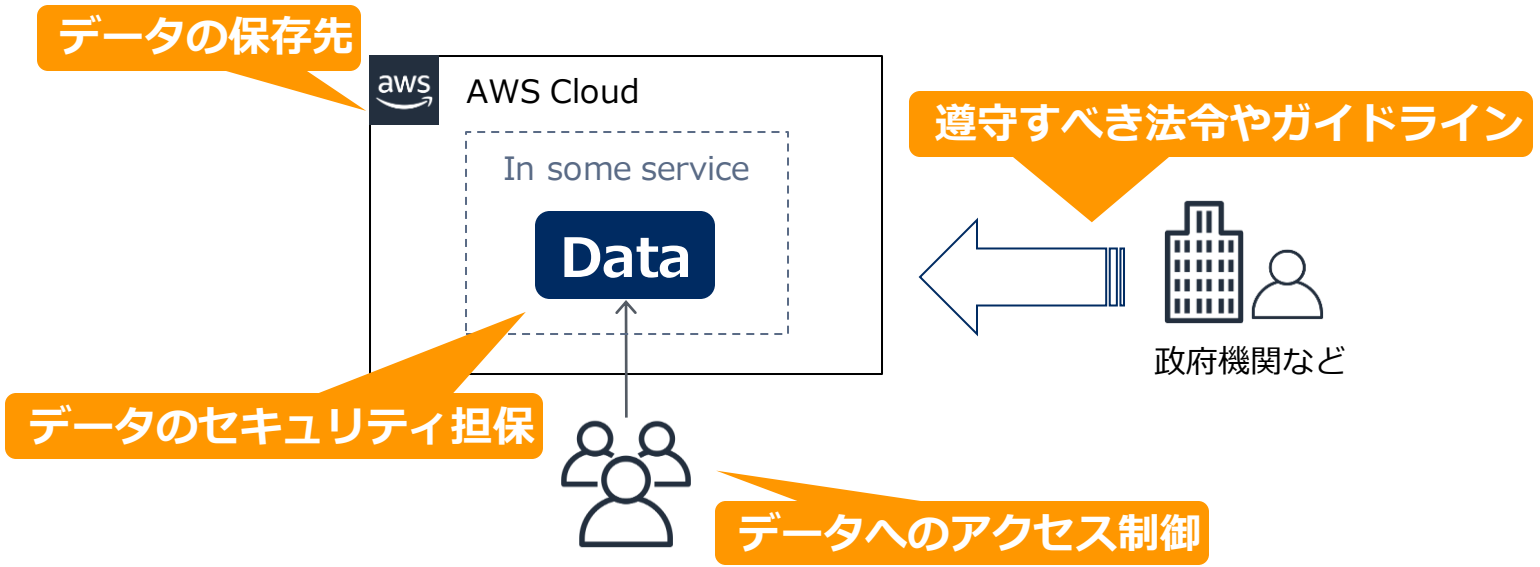
※ 詳しくは下記を参照：AWS サービスレベルアグリーメント
https://aws.amazon.com/jp/legal/service-level-agreements/

※ ネットワークが絡むテストは要注意
・Amazon EC2 Testing Policy → https://aws.amazon.com/jp/ec2/testing/
・侵入テスト → https://aws.amazon.com/jp/security/penetration-testing/

責任共有モデルの上の方＝クラウドにおけるセキュリティ

データの所有権と管理権はユーザーが保有する

- データを中心に4つの観点で検討



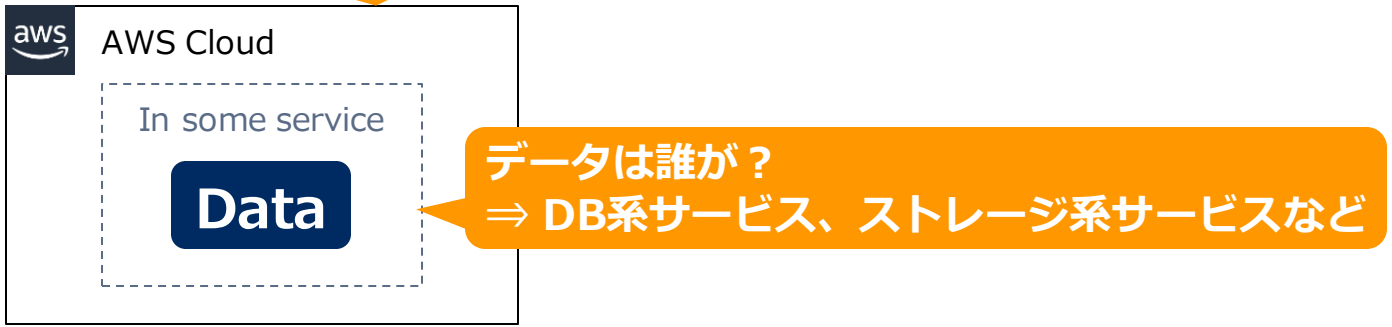
※ 参考：ホワイトペーパー「日本におけるプライバシーに関する考慮事項に照らした AWSの利用」の公開
https://aws.amazon.com/jp/blogs/news/using_aws_in_the_context_of_japanese_privacy_considerations/

データの保存先

データは『誰』が『どこ』で保持するのかを意識すべし

- 『誰(サービス)』はデータ特性、『どこ(ロケーション)』は要件※で決める　※セキュリティ要件や法令など

データはどこ？
⇒ リージョン、ローカルリージョン、アベイラビリティゾーンなど



データは誰が？
⇒ DB系サービス、ストレージ系サービスなど

データの保存先

データは『誰』が『どこ』で保持するのかを意識すべし

- 『誰(サービス)』はデータ特性、『どこ(ロケーション)』は要件※で決める

※セキュリティ要件や法令など

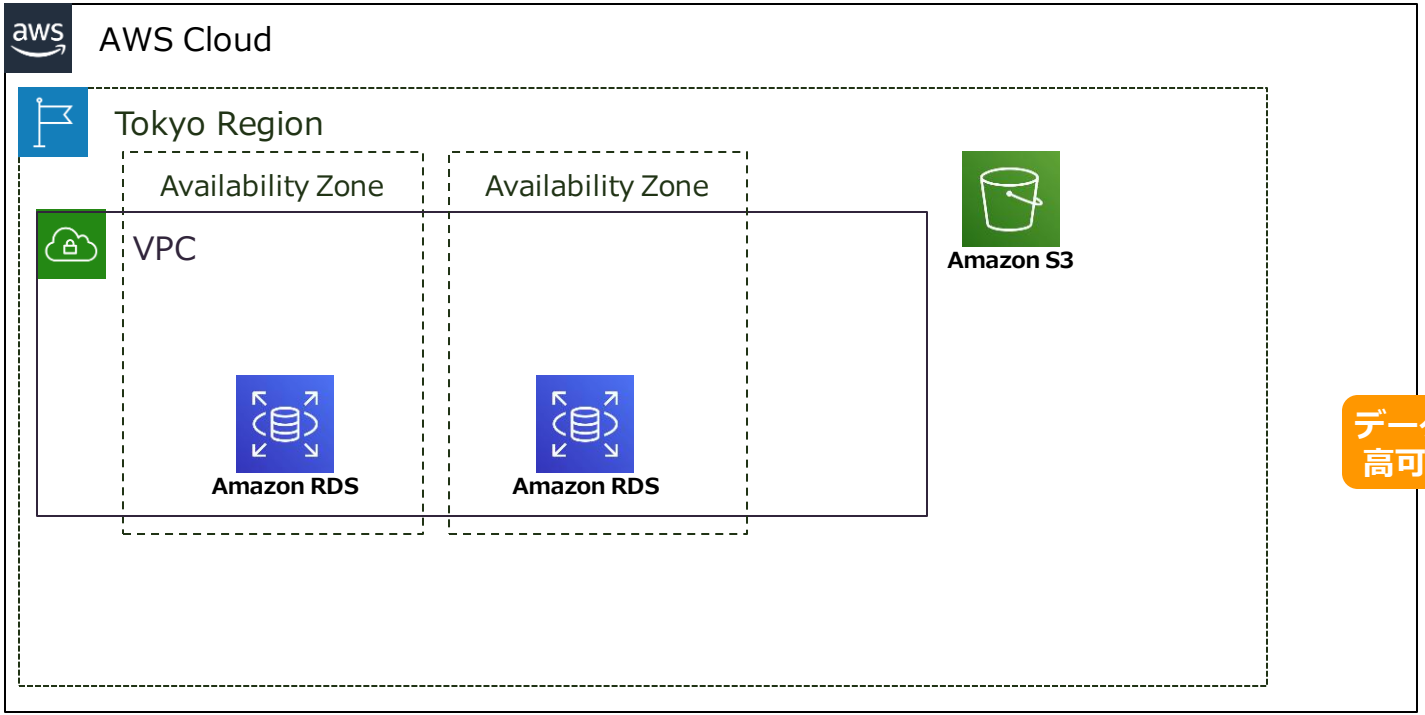
データの保存先

サンプル構成

データは『誰』が『どこ』で保持するのかを意識すべし

- 『誰(サービス)』はデータ特性、『どこ(ロケーション)』は要件※で決める

※セキュリティ要件や法令など

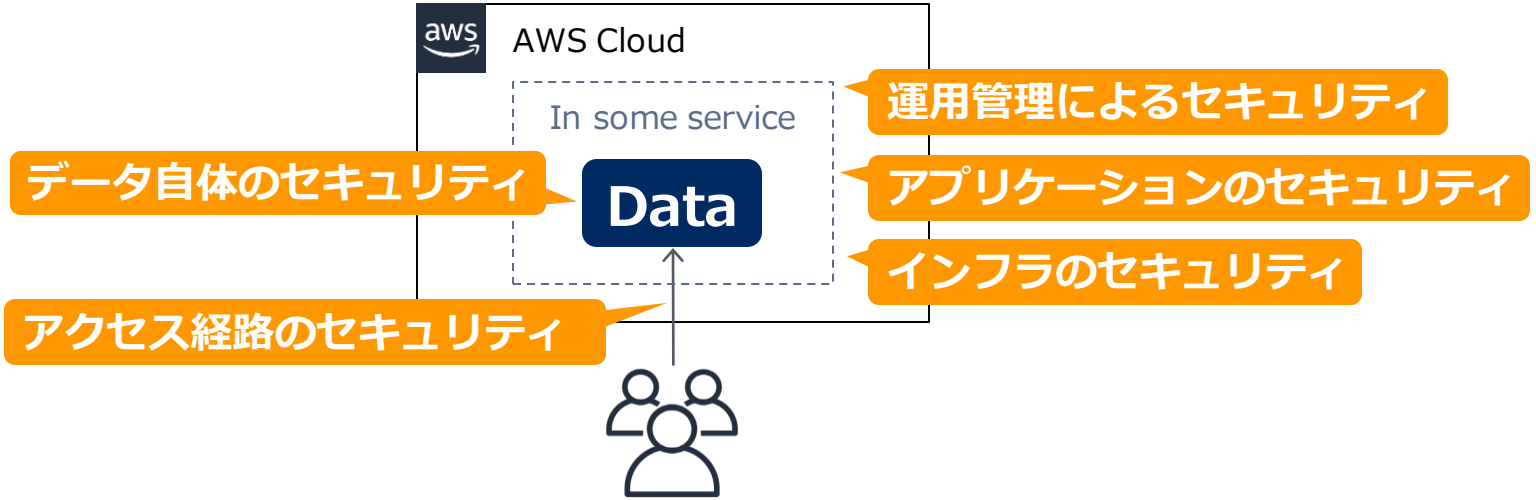


データは国内のみに保持し
高可用性とDR対策は必須

データのセキュリティ担保

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

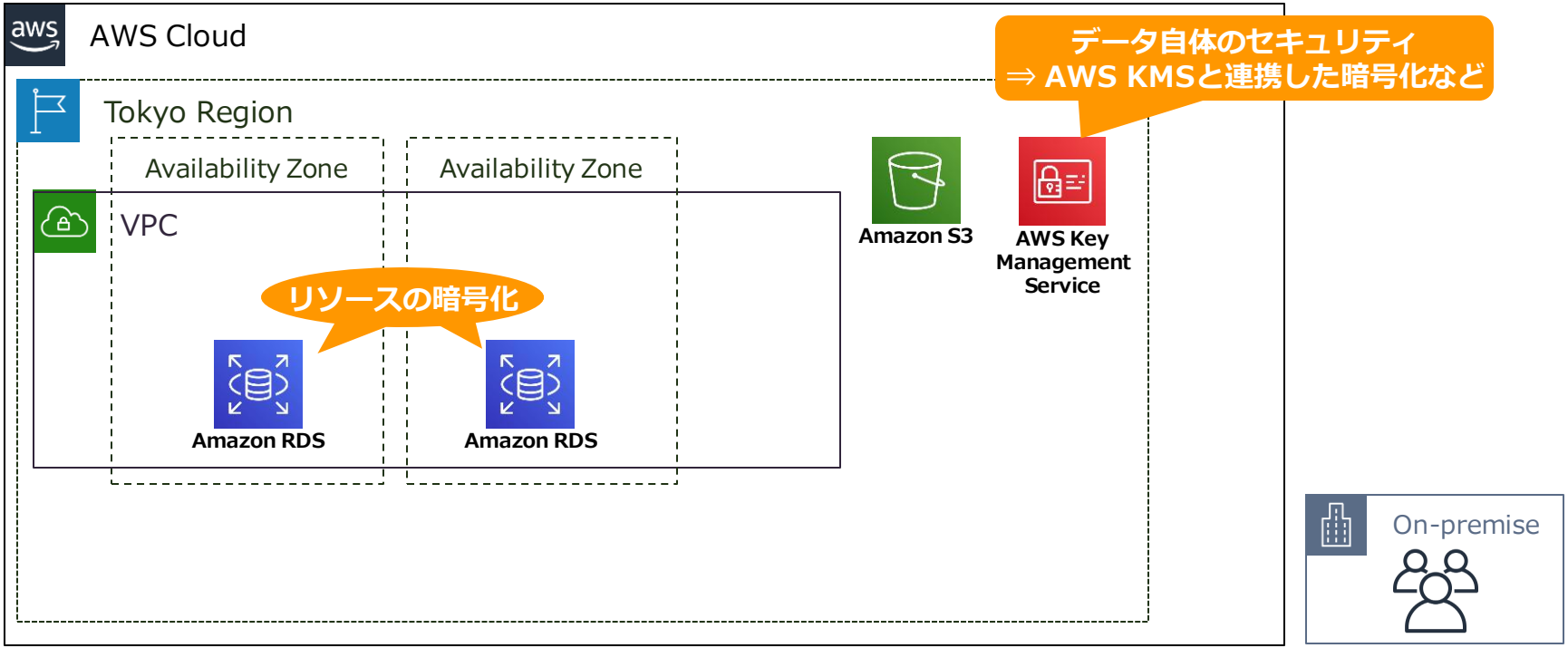


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

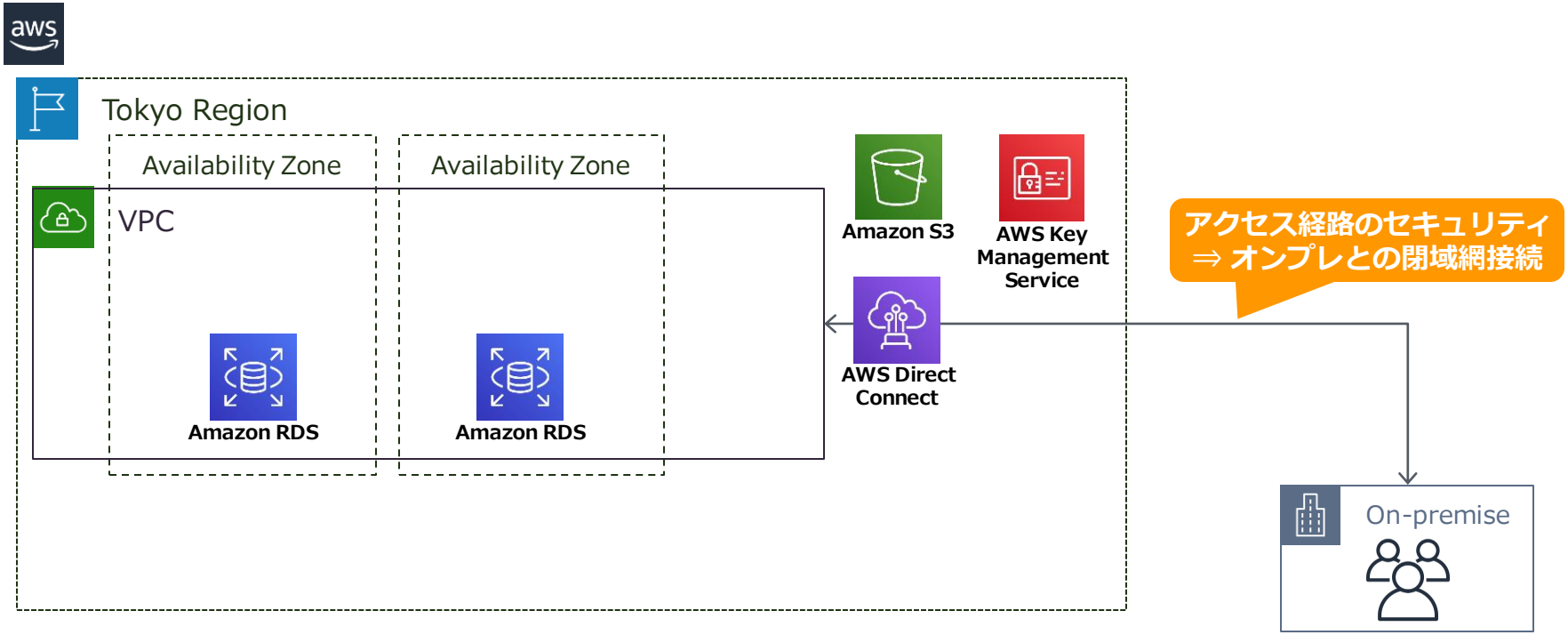
- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用



データのセキュリティ担保

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

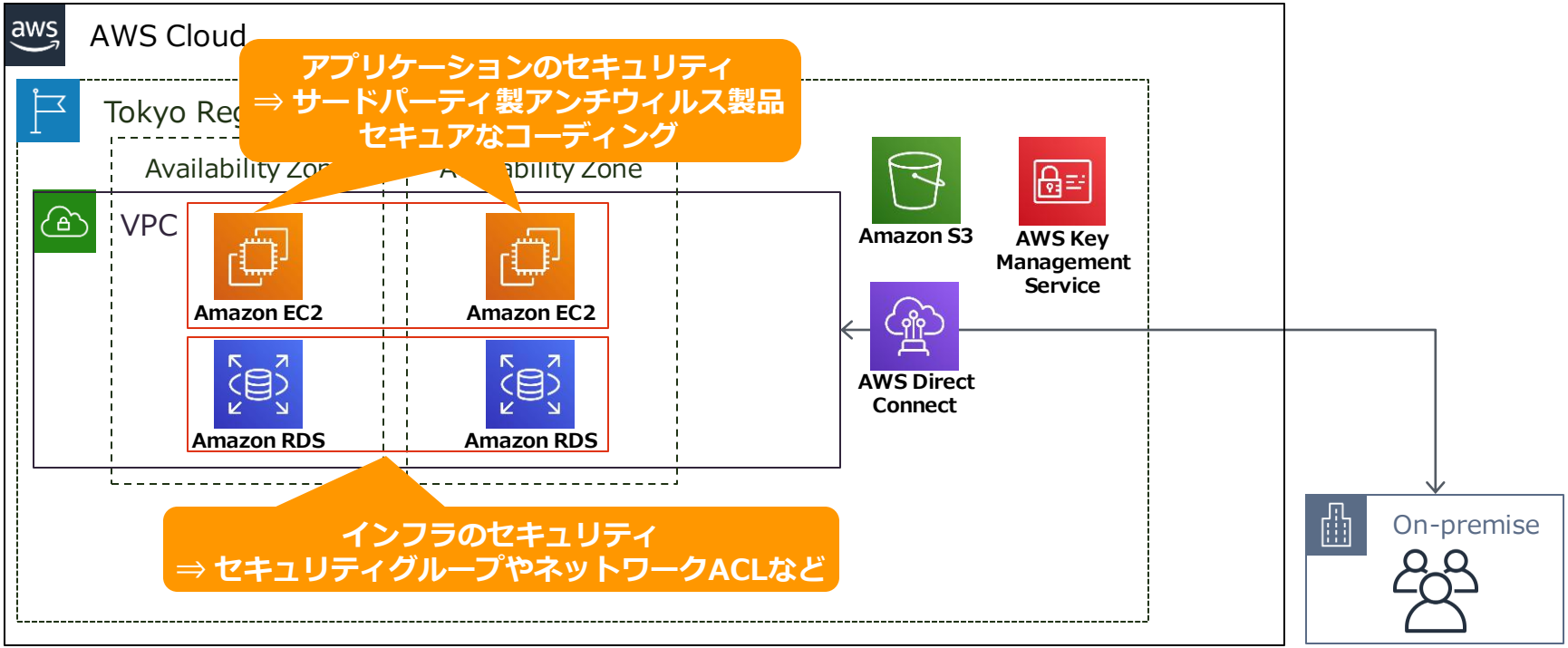


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

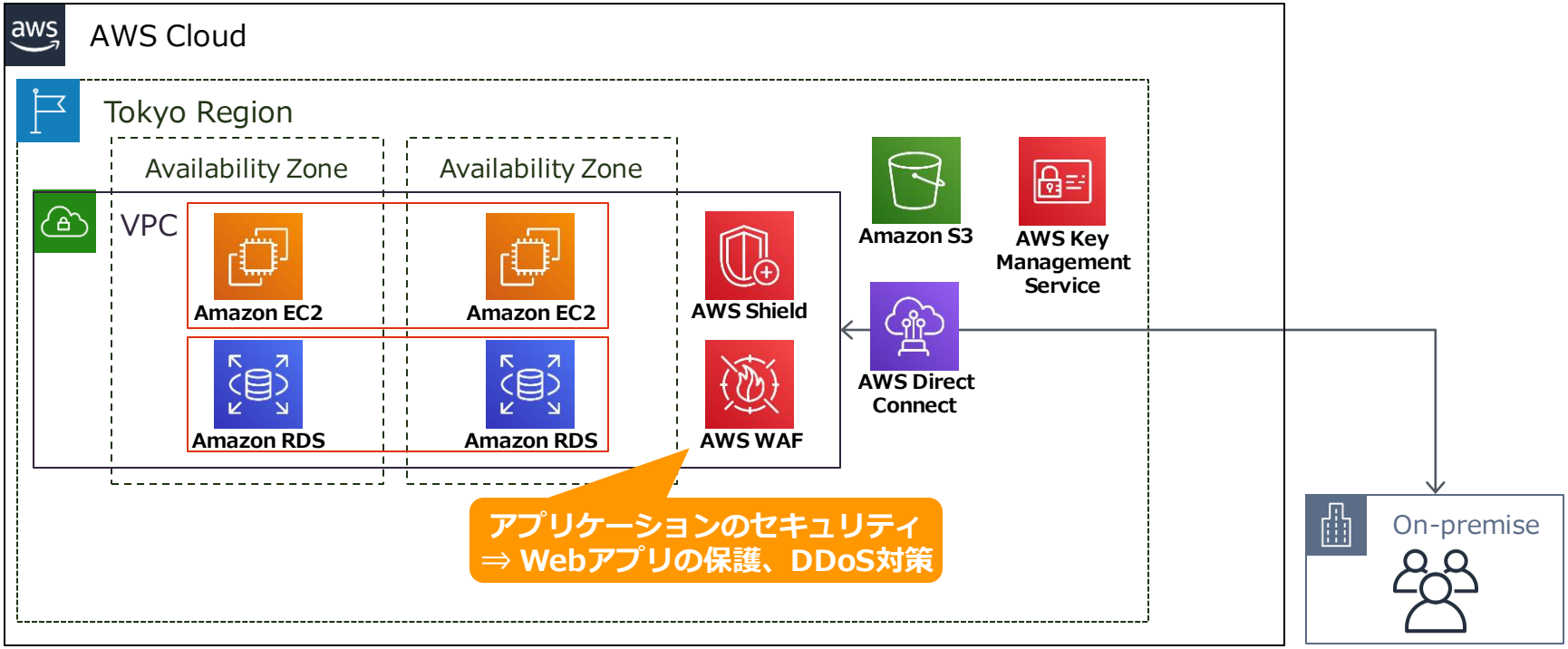


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

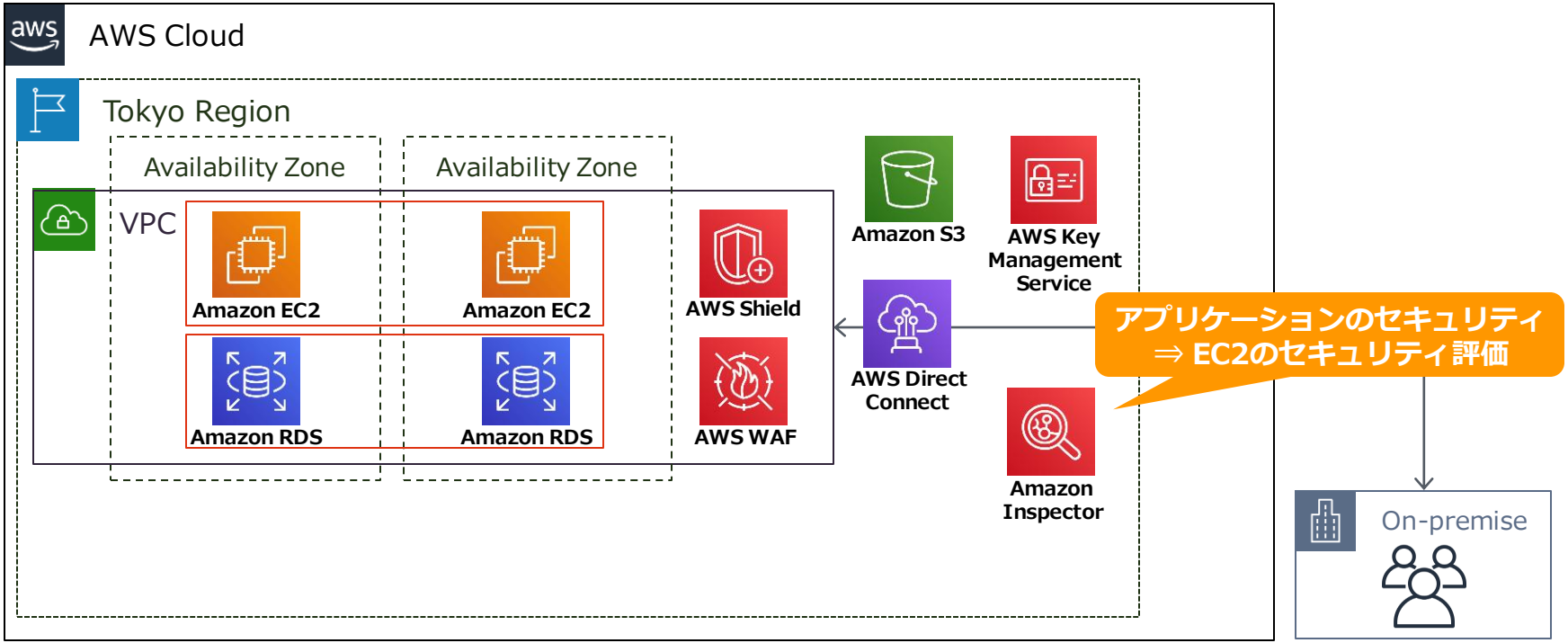


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

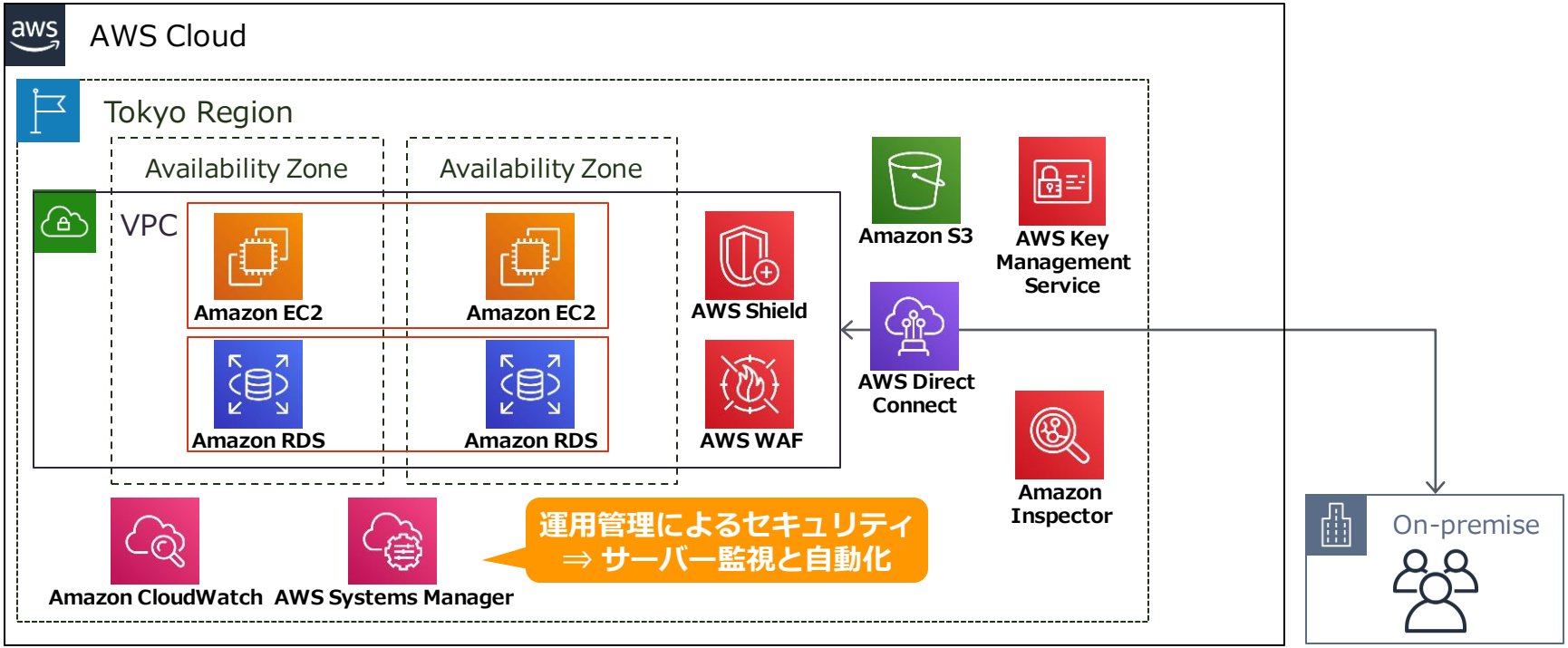


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

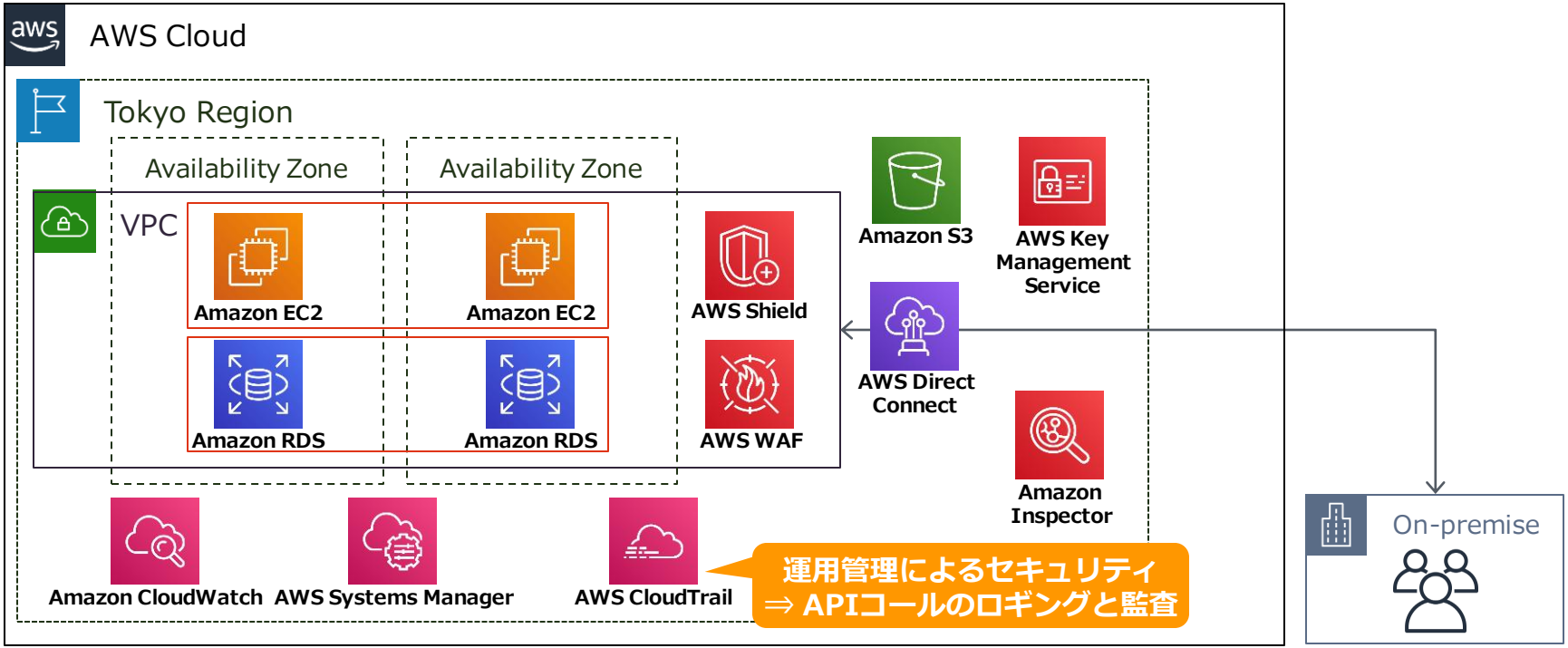


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用

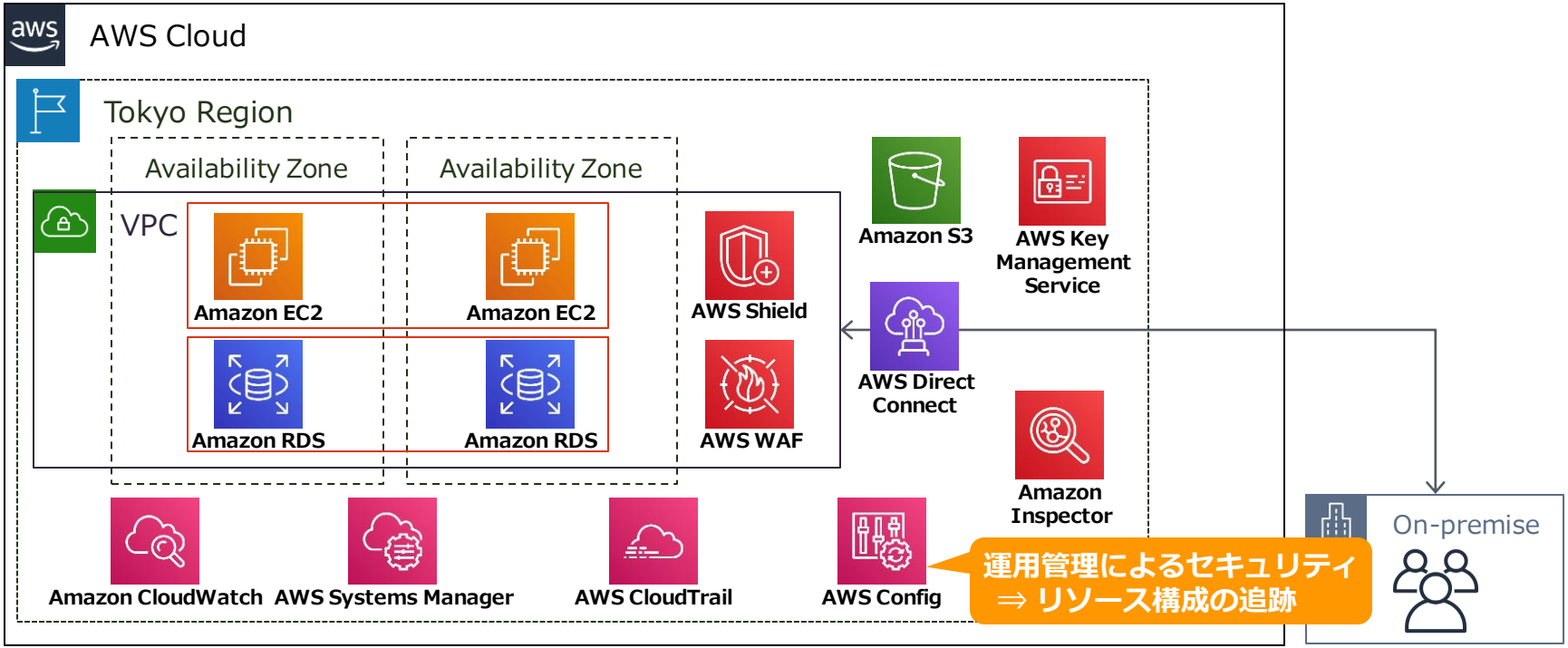


データのセキュリティ担保

サンプル構成

システムのアーキテクチャ設計だけでなく運用管理まで含めて検討すべし

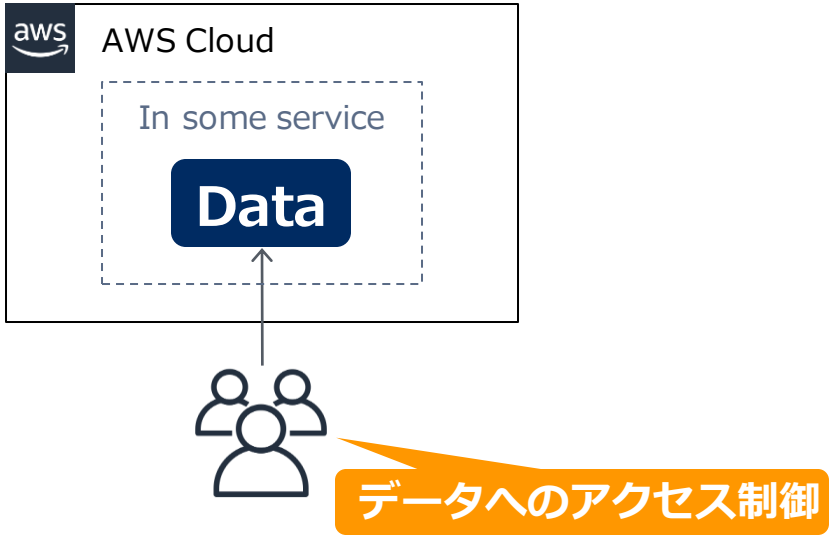
- セキュリティ系サービスだけでなく、各サービスのセキュリティ系機能もうまく活用



データのアクセス制御

誰(人、AWSのリソース)がどのデータにアクセスできるのかを意識すべし

- アクセスポリシーやロールの定義と実現方式を検討

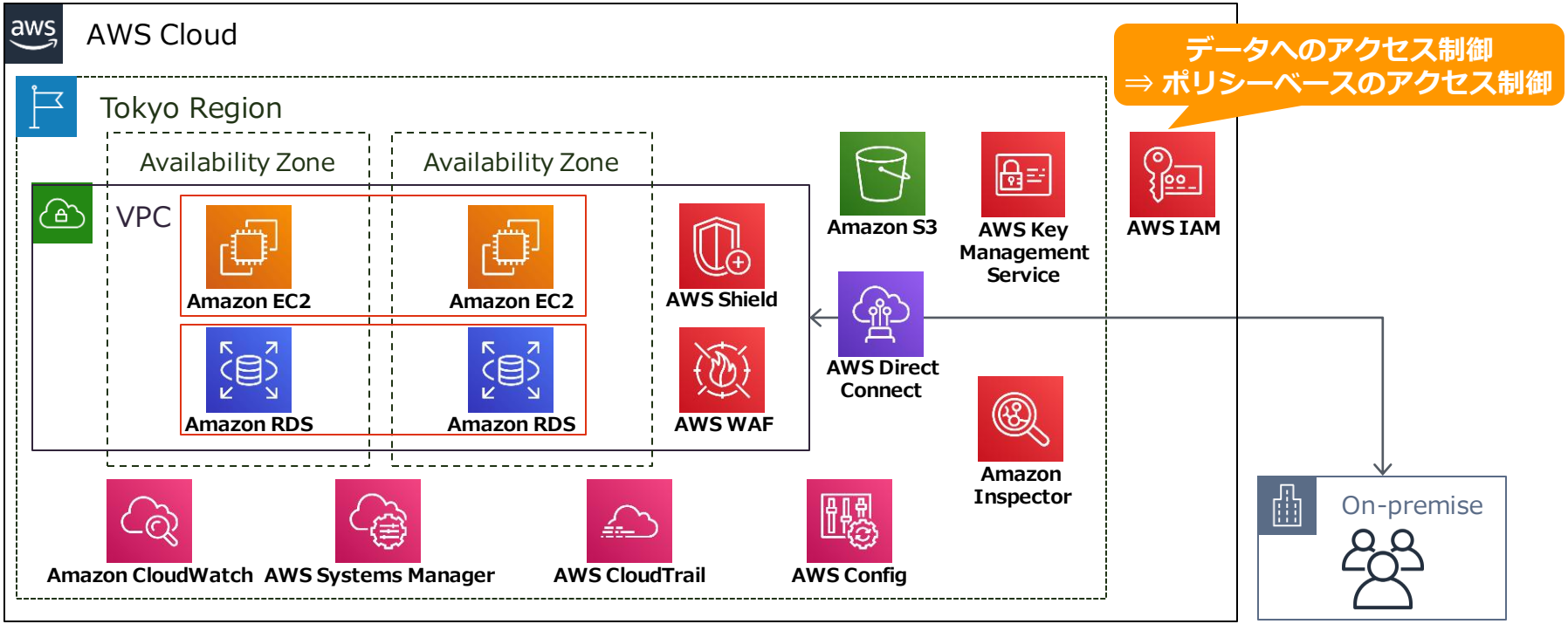


データのアクセス制御

サンプル構成

誰(人、AWSのリソース)がどのデータにアクセスできるのかを意識すべし

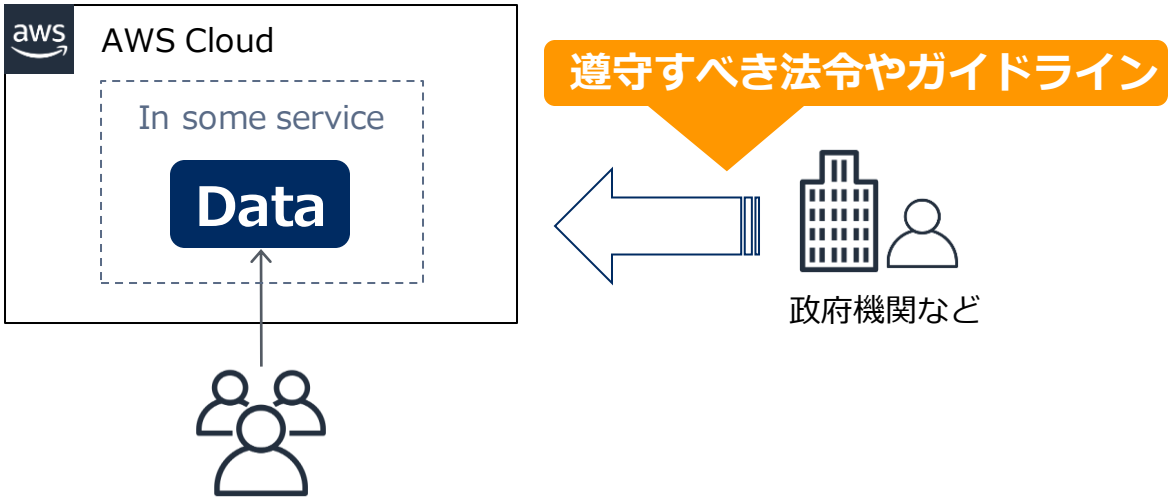
- アクセスポリシーやロールの定義と実現方式を検討



遵守すべき法令やガイドライン

システムが扱うデータや目的に応じて要件を確認すべし

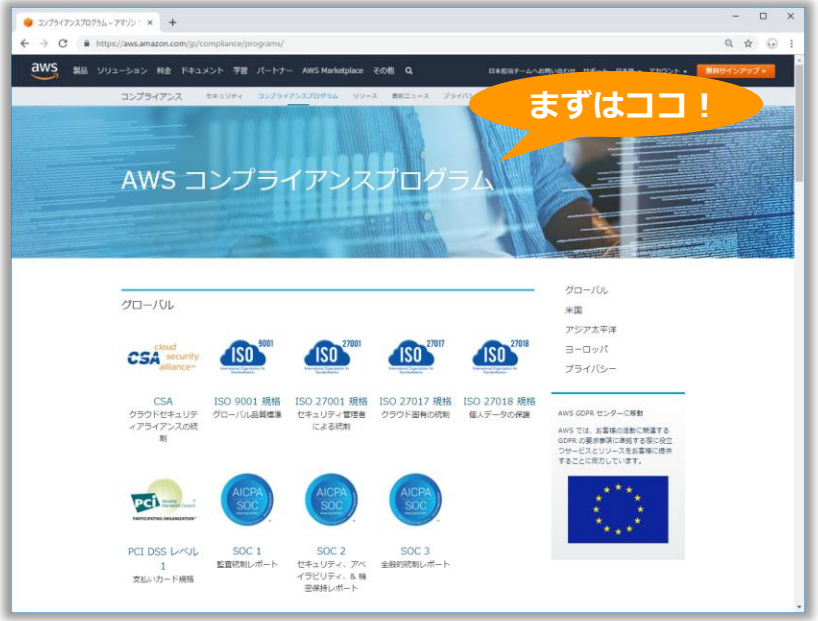
- まずは適用可能なリファレンスやベストプラクティスの有無を確認するところから



遵守すべき法令やガイドライン

システムが扱うデータや目的に応じて要件を確認すべし

- 適用可能なリファレンスやベストプラクティスの有無を確認するところから始める



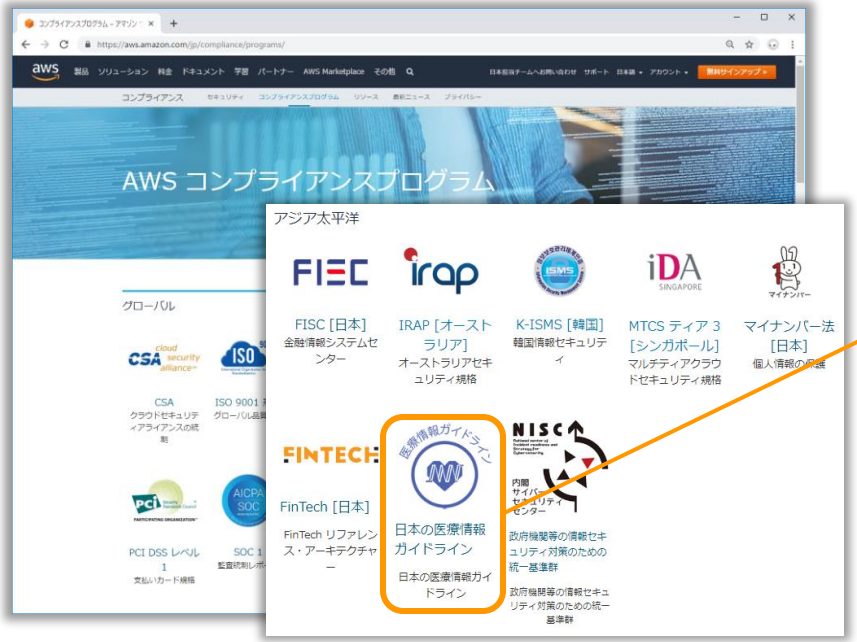
※ 詳しくは下記を参照：AWSコンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

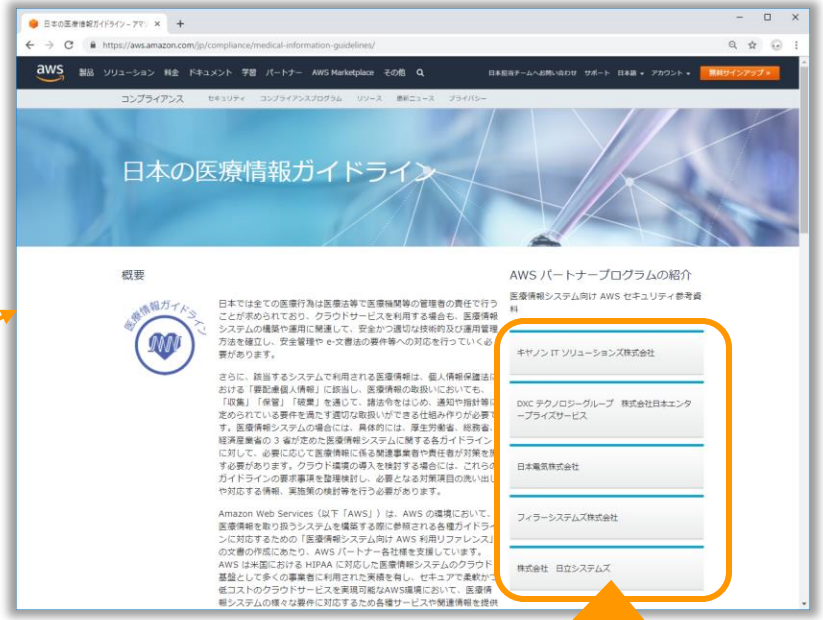
※ 詳しくは下記を参照：AWSホワイトペーパー
https://aws.amazon.com/jp/whitepapers/

遵守すべき法令やガイドライン

システムが扱うデータや目的に応じて要件を確認すべし

- 例えば『医療情報システム向けAWS利用リファレンス』





※ 詳しくは下記を参照：AWSコンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

遵守すべき法令やガイドライン

システムが扱うデータや目的に応じて要件を確認すべし

例えば『医療情報システム向けAWS利用リファレンス』

```
> ls
eula.pdf
Iryougl-Guide-v1.0.pdf
Iryougl-v2-METI-Reference-v1.0-ForPrint.pdf
Iryougl-v2-METI-Reference-v1.0.xlsx
```

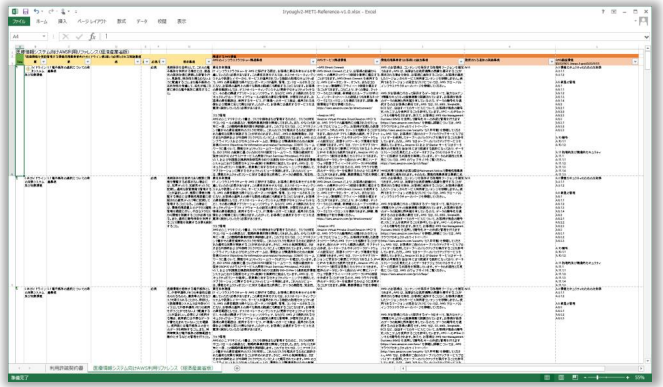
経済産業省版の
Zipファイルの中身

利用許諾契約書

概要の説明

AWS利用リファレンス（印刷用）

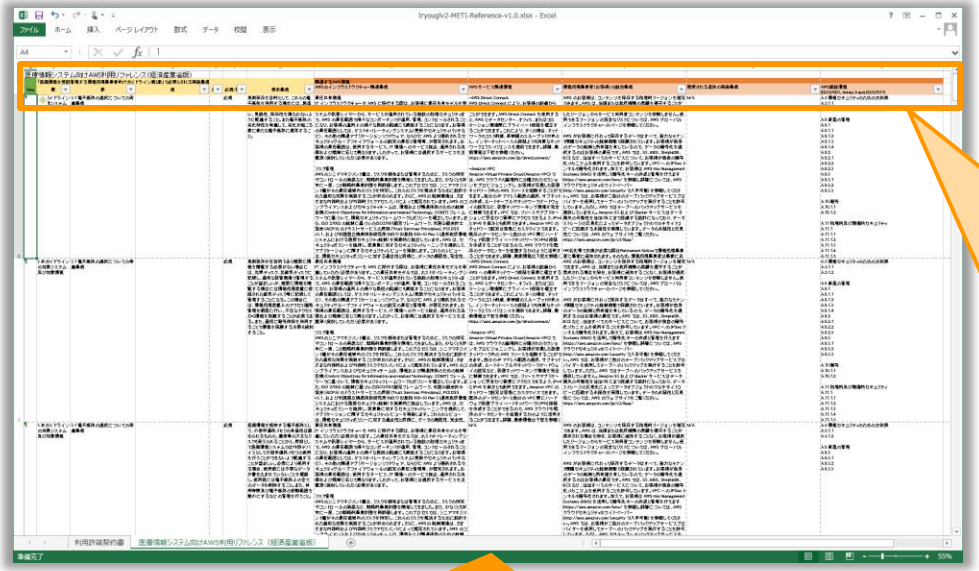
AWS利用リファレンス



遵守すべき法令やガイドライン

システムが扱うデータや目的に応じて要件を確認すべし

- 例えば『医療情報システム向けAWS利用リファレンス』



Webサイトやホワイトペーパーなどの
公開情報を基に要求事項に対する回答を記述

ガイドラインの要求事項

AWS情報

- AWSのインフラストラクチャー関連
- AWSサービス関連
- 情報処理事業者(お客様)の該当事項
- 推奨される追加の実施事項
- AWS認証情報
  (ISO27001, Annex.A and ISO27017)

【おまけ】

セキュアなアーキテクチャを目指して

クライドネイティブ化を加速せよ！

Design for Failure

https://aws.amazon.com/jp/whitepapers/designing-fault-tolerant-applications/

AWS Well-Architected Framework

https://aws.amazon.com/jp/architecture/well-architected/

Security by Design

https://aws.amazon.com/jp/compliance/security-by-design/

※ セキュリティ系ブログ(単なる一例)
How AWS Meets a Physical Separation Requirement with a Logical Separation Approach
https://aws.amazon.com/jp/blogs/security/how-aws-meets-a-physical-separation-requirement-with-a-logical-separation-approach/
Amazon Web Services ブログ(セキュリティ系のカテゴリは2つ？)
https://aws.amazon.com/jp/blogs/news/category/security-identity-compliance/
https://aws.amazon.com/jp/blogs/news/category/security-identity-compliance/security/

ご清聴ありがとうございました。

併せて読みたい JAWS DAYS 2019 セキュリティトラック

- 1日でSSHをやめることができた話 ~AWS Systems Manager Session Manager 導入と運用Tips~
  https://speakerdeck.com/3utama/1ri-tesshwoyamerukotokatekitahua
- AppStream 2.0を活用してユーザ端末に依存しない運用にしよう
  https://speakerdeck.com/nasrinjp/jawsdays2019-appstream20

踏み台なんてもういらない！！
セキュアなリモート操作とは？

- [初心者向け]AWS環境のセキュリティ運用(設計)をはじめてみよう
  https://dev.classmethod.jp/cloud/aws/jaws-days-2019-a-security/

AWSにおける設計や運用に関する
具体的なTipsが盛りだくさん！！
(まるでチートシート！？)

- PenTesterが知っている危ないAWS環境の共通点
  https://www.slideshare.net/mobile/zaki4649/pentesteraws

『このセッションを聞かないと
AWSのRootを盗られます！』
(セッション開始前の刺激的なアナウンスより)


Orchestrating a brighter world
NEC