『自治体行政システムにおけるAWSの活用とクラウド上のセキュリティ』

本セッションでは自治体の方から頻繁に頂くセキュリティの質問を整理することで、
AWSの安全性を正しく理解頂き、利用者がAWS上で構築するシステムとデータ
をどのように守ることが出来るか分かり易く説明します。

アマゾンウェブサービスジャパン株式会社
パブリックセクター　豊原 啓治
2019年7月23日

内容についての注意点

- 本資料では2019年7月19日時点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が東京リージョンを使用する場合、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.

公共セグメントの動向

地方自治体におけるDX推進

首相官邸・総務省・内閣官房IT室など、関係機関が地方自治体におけるクラウド活用のための論点整理と検討を実施

内閣官房IT室

クラウド・バイ・デフォルト基本方針 ＋ パブリッククラウド利用に関するディスカッションペーパー
(2018年6月、 2019年4月)

政府情報システムは、「クラウド・バイ・デフォルト原則」とし**クラウドサービスの利用を第一候補として、その検討を行う**旨、各府省庁情報化統括責任者（CIO）連絡会議にて決定

首相官邸 未来投資会議

「スマート公共サービス」会合(第3回) 総務省 提出資料
(2019年4月)

総務省地域力創造グループ地域情報政策室より、

- **「パブリッククラウドへの接続方法の検討」**
- **「パブリッククラウドに係る今後の取組」**
- **「想定されるパブリッククラウドの利用パターン（検討中の案）」**

等の論点を提示

自民党 政策調査会

「令和」時代・経済成長戦略
(2019年5月)

「政府・情報システムの予算・調達の一元化、**『クラウドバイデフォルト』の徹底**』といった表現と併せ、「地方自治体におけるDX推進」のためにも“自治体ごとにカスタマイズされ硬直化したレガシーシステムを刷新し、**パブリッククラウド等を活用することが不可欠**”、“国の制度と連携しつつ［中略］**自治体におけるパブリッククラウド等の活用促進のための技術的要件を速やかに周知**すべき”等の記載

- 上記の諸方針との整合性を取りながら、**地方自治体版の「クラウド」活用推進施策の策定が急務**

日本国内の公共機関におけるAWSクラウド利用動向

	これまでのクラウド利用形態	今後のクラウド利用形態
中央省庁	WEB、新サービス、開発環境	基幹システム
地方自治体	災対バックアップ、各種シミュレーション、オープンガバメント	官民連携、スマートシティ、地方創生、、内部・基幹システム
教育機関 研究機関 教育産業	業務系、教育系、エドテック	スパコンの代替、 アダプティブラーニング
ヘルスケア	医用画像・病院情報システム バックアップ、BCP	精密医療、医用画像AI診断支援、 電子カルテ、オンライン診療
特殊法人	WEBからバックオフィス、基幹システム	クラウド全面移行

先進的な取り組みにおけるAWSクラウド利用例

主にPublic Safety ,市民向けデジタルトランスフォーメーションで活用が進む

名称	概要
県庁	健康増進モバイルアプリ
県庁	ドローン防災システム
静岡県	GIS
埼玉県	県民向けモバイルアプリ、DX
某JA	農業センサー　水やり
某市	避難所開設通知
某市	スマートシティ、市民向けポータル
某市	オープンデータ、GIS、バス車両情報、河川洪水センサー(IoT)
つくば市	電子投票(Blockchain)
某市	GIS防犯見守り、郵便車両管理
浜松市	市民向け音声窓口Skill（アレクサ）
某市	市民向け防災連絡Skill（アレクサ）
北九州市	LGWAN経路とした官民データ連携（目録検索）

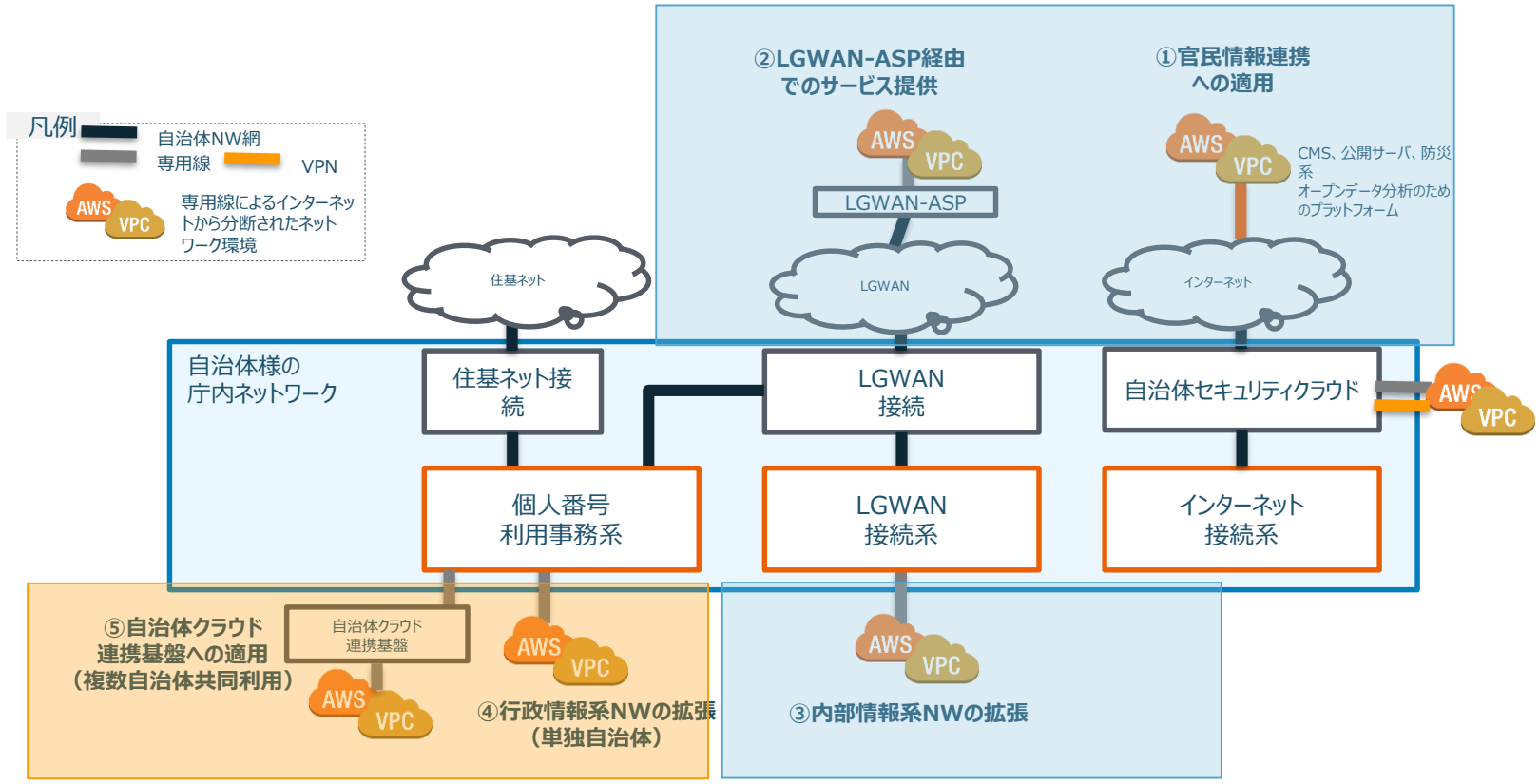
TOBE：　自治体での段階的移行

自治体NW環境とAWS接続パターン

強靭化により下記図で示すように、3層のネットワークに分離されている。自治体システムの3層構造とAWSの接続形態提案を表している。

利用中

取組中



北九州市 様

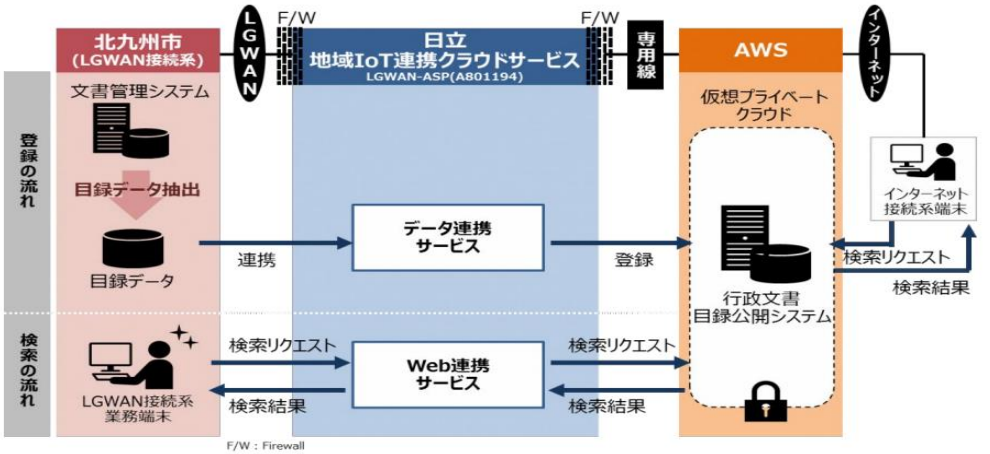
目的

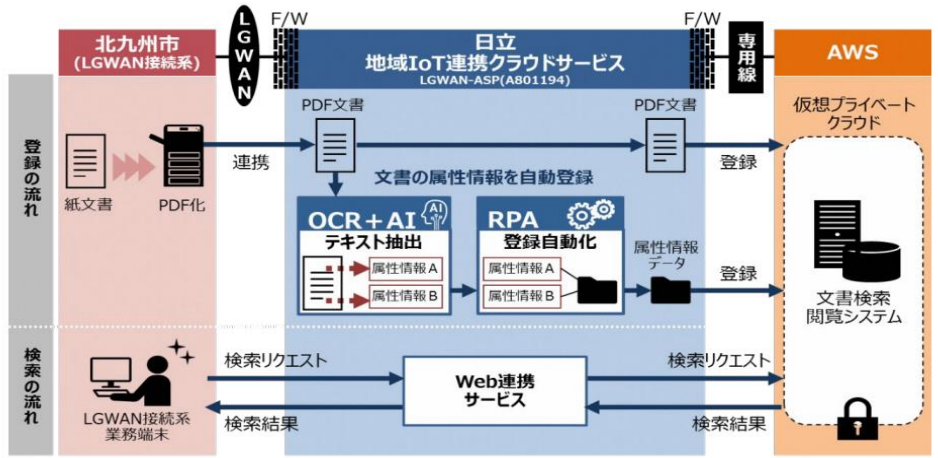
- 地方公共団体事務の利便性向上、共同利用を見据えメガクラウドの安全性、有効性確認
- 強靭性向上モデルで導入された3層分離へ配慮
- **LGWAN経由でAWS上のDBに文書目録データ登録**
- AI-OCR,RPAなどの先進技術の実証を通して庁内文書事務の効率化を確認（紙文書の属性抽出）

得られたこと

- 日立の「地域IoT連携クラウドサービス」を経由してAmazon VPC（バーチャルプライベートクラウド）への安全な接続
- 庁内からLGWAN経路でのデータ登録作業
- クラウドで短期間で効率的にシステム稼働させる手法の検証、セキュリティ要件等の確認（取組中）

https://www.city.kitakyushu.lg.jp/soumu/15300228.html
https://www.hitachi.co.jp/New/cnews/month/2019/02/0227.pdf





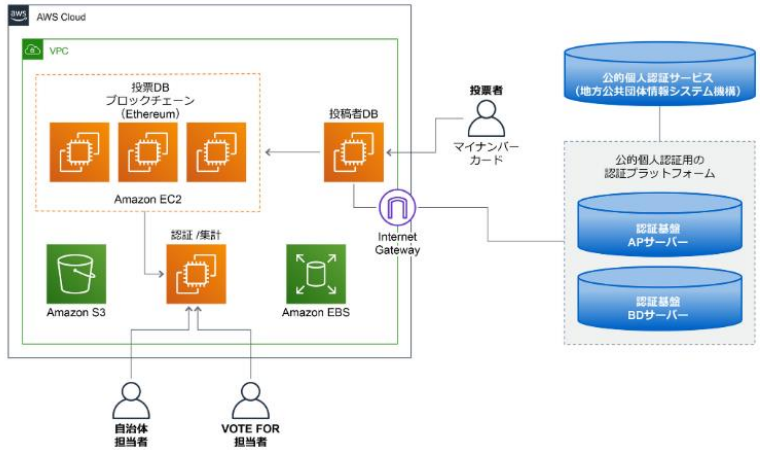
つくば市 様　ブロックチェーンとマイナンバーを活用して機密性を保持した投票システムを構築

課題

- 研究学園都市として先端技術の研究開発を支援
- SDGs、Society 5.0 につながる先端技術の社会実装に向けた実証実験の推進
- ネット投票を支えるセキュアかつ安定性に優れたシステムの早期構築

効果

- ブロックチェーン技術に要求される高スペックなインフラ基盤
- 予測が困難なシステムリソース量の増減に対しても柔軟に対応可能
- 3 か月という短期システム構築が可能



事例資料より抜粋

つくば市は 株式会社VOTE FOR とともに**IT 活用政策コンテストの**ネット投票を支えるシステムインフラの検討を進め、AWS を採用しました。仕組みとしては、**市民が投票を行う際、マイナンバーカードの読み取りによって個人認証を行います。一方、仮想通貨と称される暗号資産基盤技術として知られるブロックチェーンを活用して投票データの改ざんや消失を防止するなど、完全性を保持して安全な管理を実現しようというものでした。**

「実際に行われたネット投票では、投票を行う市民が市庁舎内に置かれた専用端末からコンテストのサイトにアクセスするとログイン画面が表示されます。そこでカードリーダー経由でマイナンバーカードによる個人認証を行うと、『つくば Society 5.0 社会実装トライアル支援事業』にエントリーしている企業や研究機関、教育機関などの候補が一覧表示され、そこから候補を選択するというかたちです。」インターネットを使った投票システムが普及すれば、投票用紙やポスターなどの紙資源、掲示板といった木材の大量消費を抑制することになり、SDGs にもつながります。また、場所を問わず参加できるため、住民票を居住地に移していない学生や国外に居住する日本人も投票できるようになります。

埼玉県　様　「ポケットブックまいたま」を活用した市民サービス向上

課題

- 県民への情報提供の偏り（若い世代の広報誌離れ）
- 県民はスマホ、インターネット利用割合が高いにも関わらず、県の情報が伝わっていない
- ポケットブックまいたまの利用率の低さ
- 情報発信（安心・安全、イベント、観光、割引サービス）

効果

- ダウンロード集中にも耐えうるスケール性
- AWSのマネージドサービスの利用による費用削減（AWS WAF等）
- 庁内とのセキュアな専用線接続（Amazon VPCとDirect Connect)によるクラウドの積極的な利用
- 今後の期待はデータ分析基盤としての活用

事例資料より抜粋

1　軽くて便利に機能が大幅に強化

旧まいたまの使い勝手を改善するとともに、便利な機能が追加されます

2　配信ジャンルが大幅に増加　16ジャンル　39課

配信ジャンルが大幅に増加し、利用者が見たいジャンルを設定できるようになります

広報全般（まいたまホーム）	安心・安全	観光	農産物（おいしい埼玉）
婚活（婚活サポート）	移住・定住（住むなら埼玉！）	健康・医療	教育（学び！生き生き！埼玉教育）
食の安心・安全	採用（採用情報）	就職（就職応援！）	地域振興（ちちぶ）
プレゼント一覧	ふれてみたい文化・芸術	生涯学習	いぬねこペット

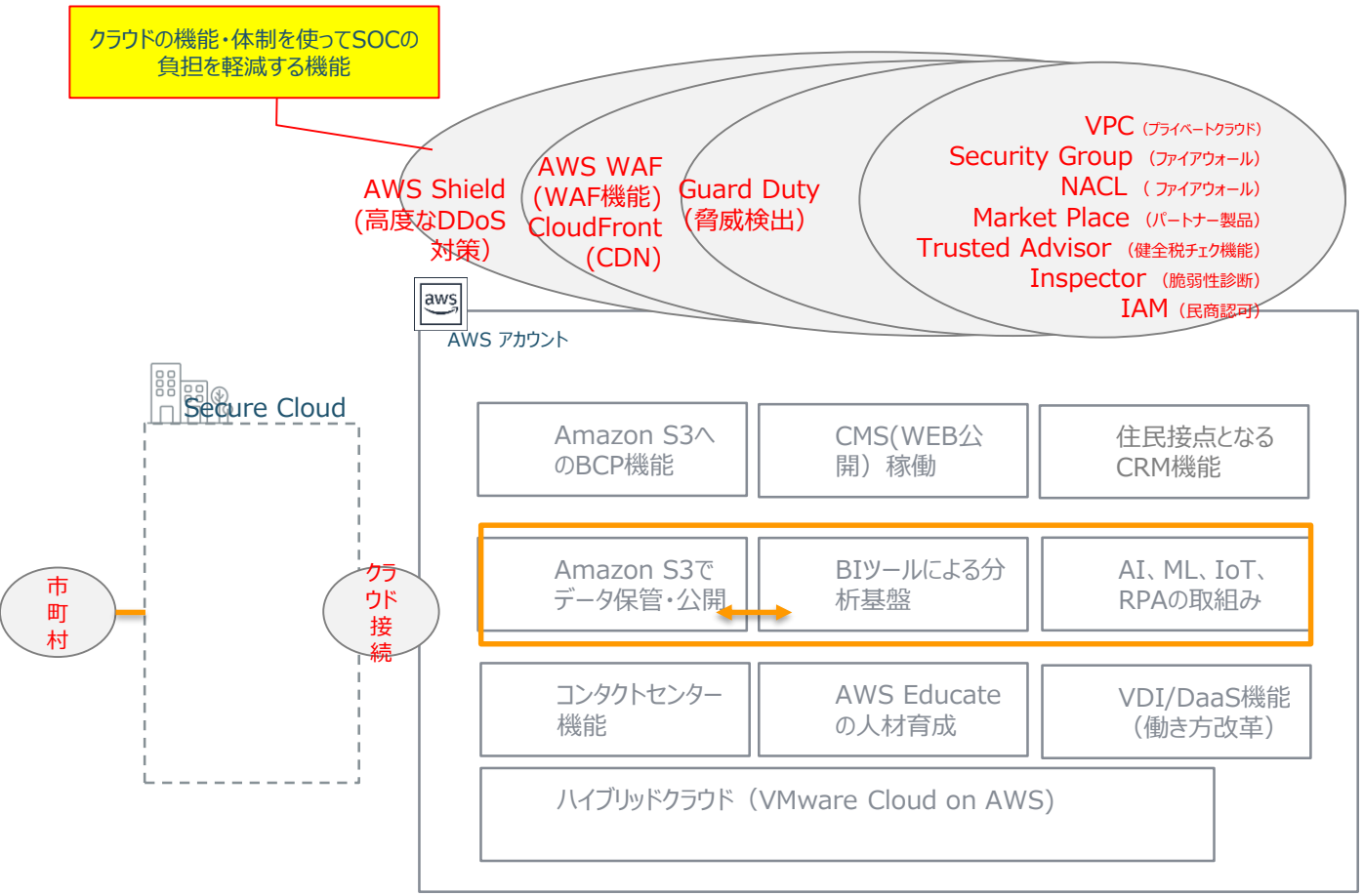
3　施設やイベントなどでアプリ活用が可能　13サブアプリ 28課 県立学校

サブアプリ（アプリの中のアプリ）により、施設やイベントでアプリの活用ができるようになります

さいたまスーパーアリーナサブアプリ	スマート連絡網（学校と保護者の連絡）	埼玉県立博物館・美術館サブアプリ	埼玉県立げんきプラザサブアプリ
埼玉県立図書館サブアプリ	埼玉で開催！Tokyo2020サブアプリ	パパ・ママ応援ショップサブアプリ	ラグビーワールドカップ2019サブアプリ
献血!!この指とまれ	公園イベントサブアプリ	ちちぶ路線バスの旅サブアプリ	自動車税「納めてプラス！」キャンペーン	埼玉県版だれでもゲートキーパーサブアプリ

TOBE: 県セキュリティクラウドの拡張、移行

TOBE:セキュリティクラウド on AWS



メリット：

・県セキュリティクラウドのゲートウェイをAWSに移す、あるいは拡張する形でAWSをプライベートに接続し、クラウド機能を利活用してサービス価格の軽減、迅速性、柔軟性を目指す

・インターネットゲートウェイをAWSのものを利用することでマネージドサービス利用によるコスト軽減とスケール性を担保

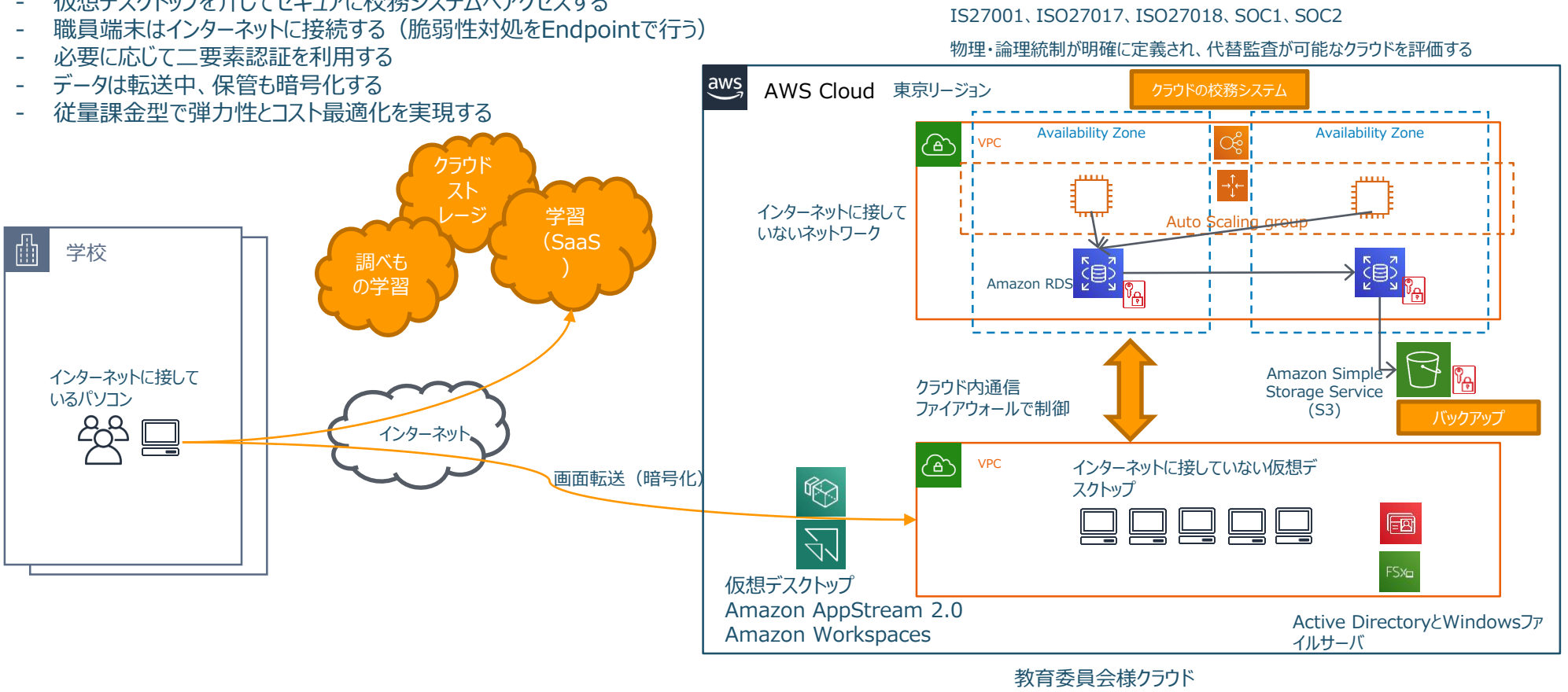
・県による一括契約による（ボリュームディスカウント、契約煩雑さの軽減）

・クラウドの教育による庁内・地域・パートナー・学生の知識の底上げ

TOBE　小中高等学校での校務システムの移行

利用シナリオ:

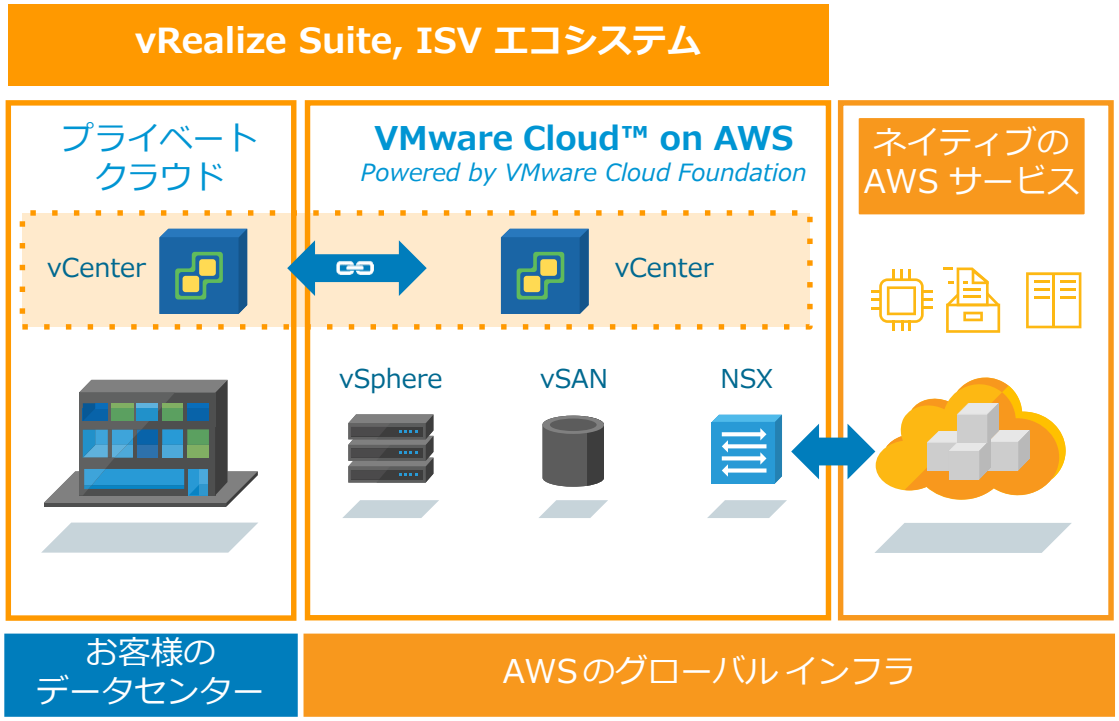
- セキュアに校務システムをクラウドでホストする（機微なデータはクラウド側で安全に保管する、インターネットに接しない仮想デスクトップを利用する）
- 仮想デスクトップを介してセキュアに校務システムへアクセスする
- 職員端末はインターネットに接続する（脆弱性対処をEndpointで行う）
- 必要に応じて二要素認証を利用する
- データは転送中、保管も暗号化する
- 従量課金型で弾力性とコスト最適化を実現する



新たな選択肢：ハイブリッドクラウド化で運用を踏襲

プライベートクラウド（VMware)を拡張する選択肢

仮想デスクトップHorizonを構築可能！



ハイライト

- AWS ベアメタル上で実行される VMware SDDC
- VMware が販売、運用、サポートを提供
- コンテナと仮想マシンのサポート
- オンデマンドのキャパシティと柔軟な利用
- オンプレミスの SDDC との完全な運用の一貫性
- ワークロードのシームレスな移行
- AWS のネイティブ サービスへの直接アクセス
- AWS のグローバルなフットプリントを基盤と
  した可用性の高いサービスの利用
- パートナーエコシステムとの連携

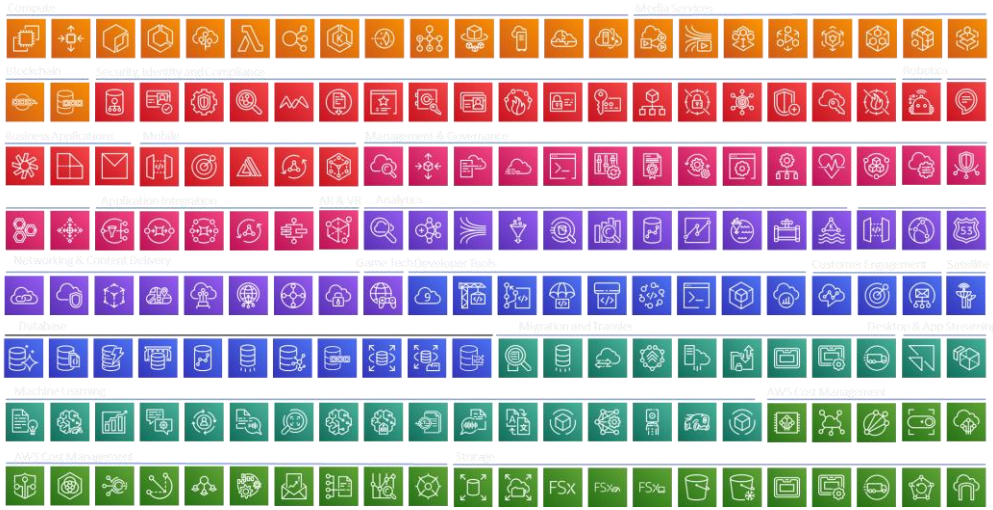
なぜAWSなのか？

なぜAWSなのか？

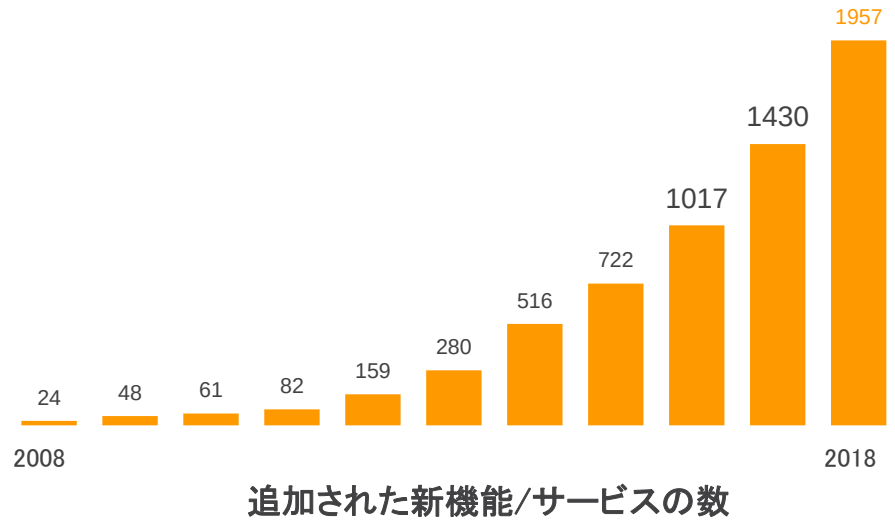
1 . 幅広いサービスと機能

テクノロジーへの投資を継続し、革新的な機能を提供します

165を超えるサービス数



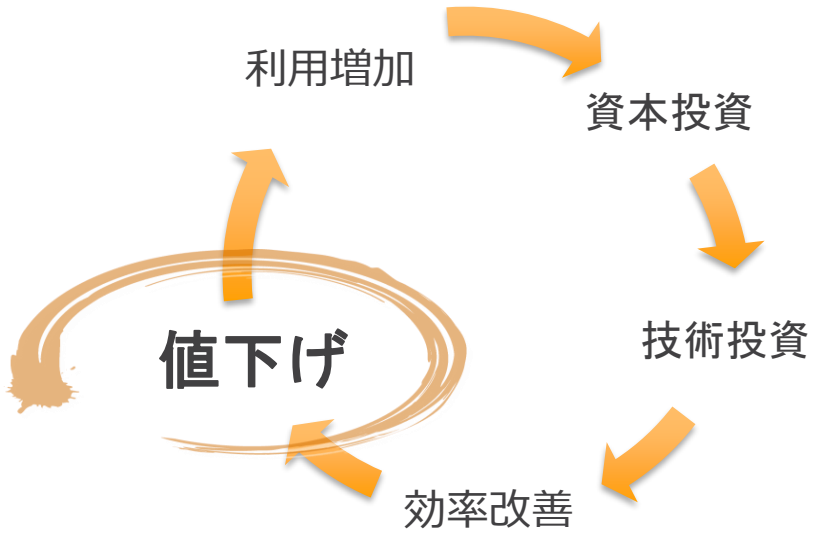
加速するイノベーションのペース



なぜAWSなのか？

2．コスト削減

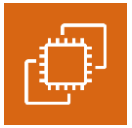
資本と技術への投資により得られた効率を値下げにより還元します



- 過去72回の値下げ
- お客様の初期投資不要
- 利用した分のみの従量課金制

初期費用不要・低額な利用料金（一例）

そもそも低価格

仮想サーバ(EC2)		＝　¥0.68 ($0.0068)～ / 時間
冗長化SSD（EBS）		＝ ¥12（$0.12）～/ 1GB / 1ヶ月
高可用性保存領域(S3)		＝ ¥2.5($0.025)～/ 1GB / 1ヶ月
アーカイブ領域 (Glacier Deep Archive)		＝　¥0.5($0.005)/ 1GB / 1ヶ月

※ 2019年4月時点での東京リージョンの金額
※為替1$＝108円で計算

なぜAWSなのか？

日本では…2030年までに約60万人のIT人材が不足（経済産業省調べ）

LinkedIn Learningの「持つべきハードスキル トップ10 2019」 1位にクラウドのスキル

3．人材育成

aws educate

クラウド実習用クレジットと技術の学習の機会を学生に提供する無料プログラム

教育機関

大学・高専・高校・
専門学校・職業訓練機関

加盟校の教員・学生メンバーは2 倍の AWS クレジットが提供されるなど追加の支援があり、より多様な教育への利用が可能になります。

学生

14歳以上

自習型オンライン学習コース、AWS の利用クレジットが提供され、実際にAWSを使いながら学べます。求人情報へのアクセスができます。AWS アカウントが無くても参加可能です。

教員

クラスルームの運営、自身の授業に組み込めるオープンソースコンテンツ、トレーニングリソース、コミュニティへのアクセスが可能です。

過去20年にわたる機械学習の投資、経験

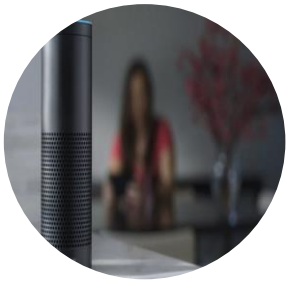
4. 機械学習の経験で得たノウハウを汎用化

Eコマース
レコメンデーション

配送センター
自動化・インベントリ

ドローン配送

自然言語処理



新しい買い物体験

アマゾンのフルフィルメントは従来のモデルをディープラーニングベースに変更することで13.9%の予測精度向上を実現しました。現在では、200万以上の売り手が、Amazonの倉庫に最適な量の在庫を仕入れ、需要を満たすために予測を利用しています。

なぜAWSなのか？

5．パートナーエコシステム

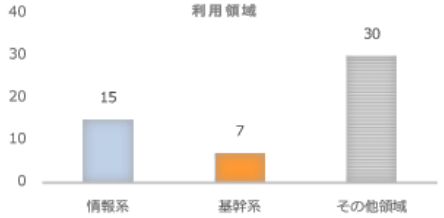
自治体のお客様の声
現在地

自治体のお客様の声　（2019年　弊社調べ）

クラウドを利用したいが“個人情報”を AWS クラウド上に置くことが可能なのか。
物理的安全管理措置と削除処理をどのように考えれば良いか、といった問いが多い。

既にクラウド導入に取り組んでいる自治体の活用例

▶市民系のサービスとしては地図システムが最多。GISを活用した地図情報システムのほかは、施設予約システムや図書予約システムなどが挙がった
▶情報系（庁内システム）としては業務システム全般が挙がった 申請系のツール、グループウェア、人事給与・財務会計システム、 ファイル交換、メールサーバー等



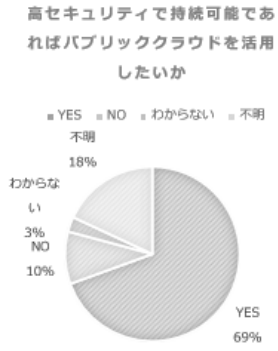
GISを活用した地図情報システム	7
電子申請ツール	3
財務会計システム	3
グループウェア	2
業務システム全般	2
人事給与システム	2
防災システム	2
施設予約システム	2
ファイル交換ツール	1
図書予約システム	1
市民から情報を受けるシステム	1
メールサーバー	1
文書管理システム	1
住民税	1
その他領域	17

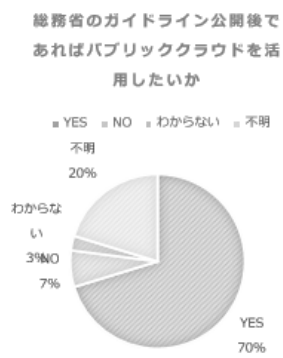
※集計対象：導入済41件うち回答のあった自治体
複数回答

調査時期：2019年2月18日～3月15日
対象団体：県庁を含む、10万人以上の地方自治体 有効回答数：228団体

検討・興味への壁は「セキュリティ面」

現在検討がなくとも、条件さえそろえばパブリッククラウドの活用 意向がある自治体が70%





※母数：共に未検討75件

一方で、「セキュリティ面に懸念がある」が 45%

セキュリティ面に懸念があるため	29	38.7%	45.3%
システムの見直し予定が未定のため	7	9.3%	10.9%
総務省のガイドライン次第のため	4	5.3%	6.3%
コスト面に懸念があるため	4	5.3%	6.3%
良く知らないため	2	2.7%	3.1%
自治体クラウドの導入検討があるため	2	2.7%	3.1%
プライベートクラウドを検討中・導入中のため	4	5.3%	6.3%
直近での予定はないため	3	4.0%	4.7%
情報収集段階のため	4	5.3%	6.3%
その他	5	6.7%	7.8%
回答拒否	2	2.7%	-
担当外のため不明	1	1.3%	-
未聴取	8	10.7%	-
合計	75	100.0%	-

※母数：未検討75

クラウド採用の流れ

現在地

Business Value

FOSTER INNOVATION

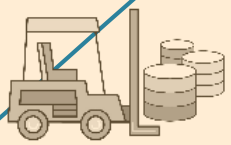
- AWSは、特定の要件を解決するために、プロジェクト毎に利用される
- お客様はクラウドが効果的なオプションかを検証する
- 組織全体としてはAWSスキルセットが蓄積されにくい

プロジェクト

- 既存のデータセンターとAWSが接続される
- 多くのプロジェクトが立ち上がる
- 少数のエンタープライズアプリケーションがAWS上で本番稼働する
- Cloud Centre of Excellenceの立ち上げに取り組む
- セキュリティ・コンプライアンスモデルを規定する

基礎作り

資産償却



移行

- 長期のクラウドオペレーションの準備に入る
- Cloud Centre of Excellenceが確立する
- IT部門のロールが再定義される
- 多くの本番アプリケーションの移行やデータセンターの移行が実施される

最適化 & 改革

- クラウドはデフォルト選択肢となる
- 新しいビジネスモデルが生み出される
- “なぜクラウド”が“なぜクラウドでないのか”に変わる
- アーキテクチャのみならず、クラウド最適な運用、プロセスに移行していく

Time

実証実験、現課毎に利用するシステムがバックエンドでAWSクラウドが利用されているフェーズ

情報システム部門管理のもと専用線を所有しAWSと接続。クラウド利用ポリシーを策定するフェーズ。
情報システム部門管理の情報系システムでノウハウ蓄積

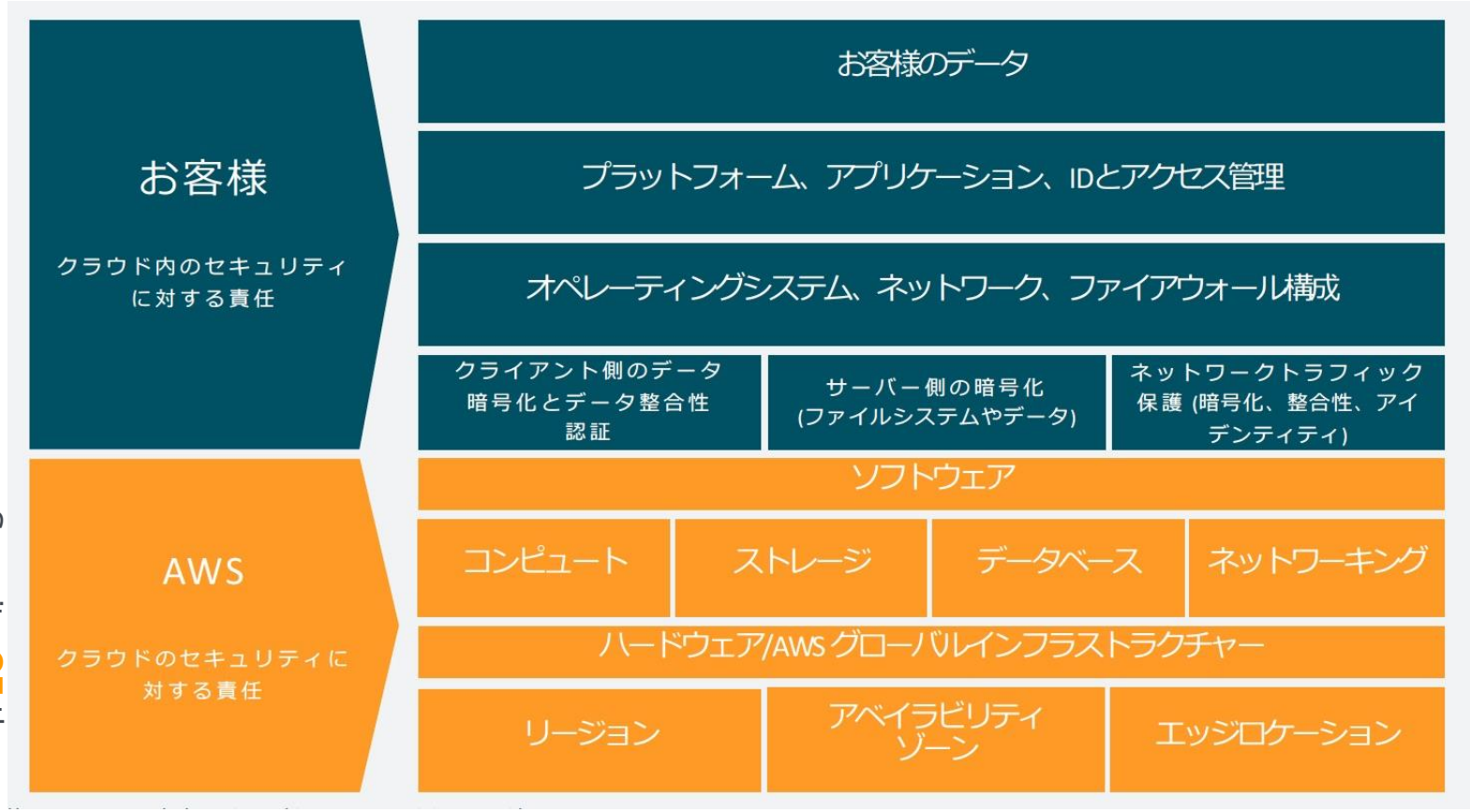
クラウドファーストが共通理解となり、基幹系システムの移行。
ノウハウが定着。

基幹系システムがクラウドネーティブに最適化される。
クラウド内でデータ連携が簡潔するフェーズ。

AWSの安全性の理解

AWSはリソースを自らによって制御できるクラウド

責任共有モデルとは



お客様ないしはクラウドサービスを利用するSierは、自ら果たすべき安全管理措置の一環として、**AWSにあるデータについて、適切な安全管理措置を講ずる必要**があります。

AWSはサービスを安全に運用するために、ISO27001・ISO27017・ISO27018等安全性評価に関わる認証を取得しています。

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

データプライバシー

● AWSは、法令対応等の遵守する必要な場合を除き、お客様のデータ(コンテンツ)を開示しません。

- **データの所有権と管理権はお客様に**あります。
- **データとサーバを配置する物理的なリージョンはお客様が指定**することが可能となります。
- **AWS** は、法令遵守または政府機関の要請によりやむをえない場合を除き、**お客様のコンテンツを指定されたリージョンから移動しません**
- 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を遵守するために必要な場合を除き、**お客様のコンテンツを開示することはありません**
- そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、お客様が開示からの保護を求められるようカスタマーコンテンツの開示に先立ってお客様に通知します
- AWSでは、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。(サーバサイド暗号化、クライアントサイド暗号化、鍵の保管・管理方法等)

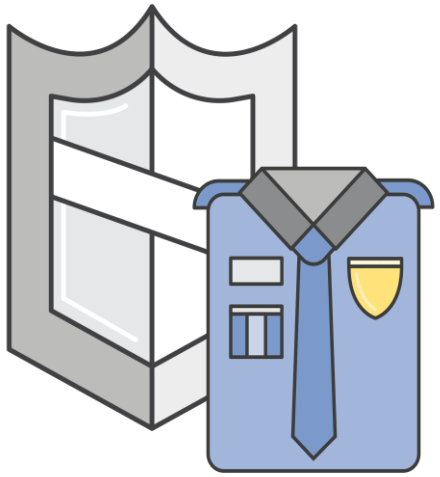
AWSが誇るセキュリティとコンプライアンス

- 業界における認定と独立した第三者機関による保証型報告書を取得
- AWS のセキュリティと統制に関する情報をホワイトペーパーおよびウェブサイトコンテンツで公表
- FISC（金融情報システムセンター）安全対策基準対応のセキュリティリファレンスの提供
- NDA に従いAWS のお客様に証明書、レポートなどの文書を直接提供

aws.amazon.com/jp/security
aws.amazon.com/jp/compliance

データセンターの安全性

● AWSは、以下の考えに基づき物理的なセキュリティ(データセンタ)に関するセキュリティ対策を講じています。

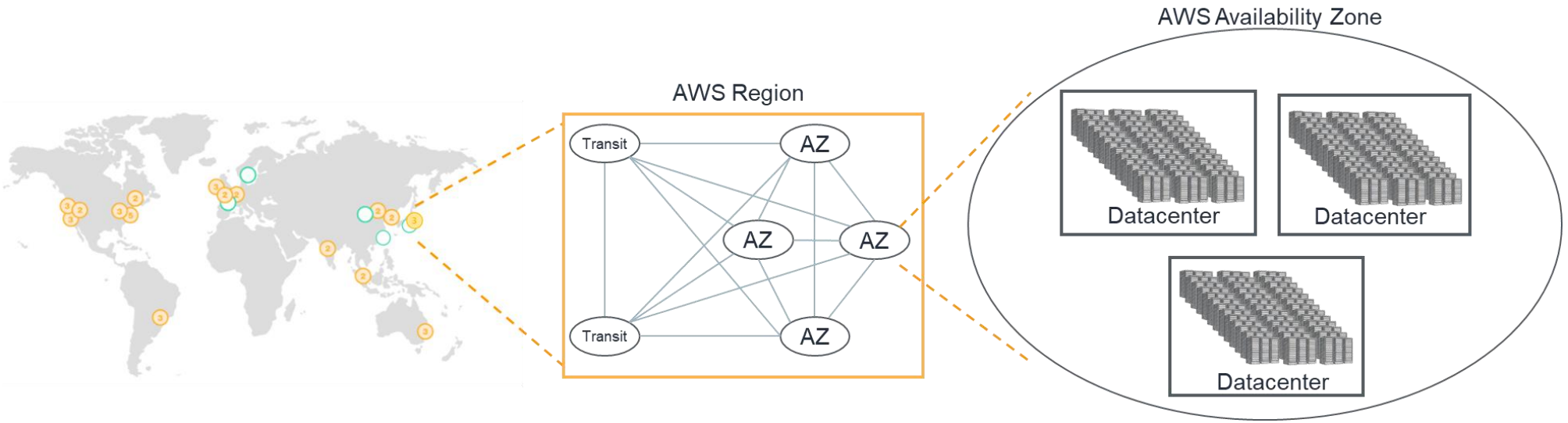


- Amazonは十数年間にわたり、大規模なデータセンタを構築
- 重要な特性:
  - ✓ 場所の秘匿性
  - ✓ 立地条件
  - ✓ 周囲の厳重なセキュリティ
  - ✓ 物理アクセスの厳密なコントロール
  - ✓ 多要素認証を2回以上で管理者がアクセス
- 完全管理された、必要性に基づくアクセス
- 全てのアクセスは記録され、監査対象となります
- 職務の分離

AWSのデータセンタ https://aws.amazon.com/jp/compliance/data-center/data-centers/

データセンター耐障害性/高可用性

●各リージョンは、複数のアベイラビリティゾーン(AZ)で構成されています。（一部のローカルリージョンを除く。）
●AZは1つ以上のデータセンタで構成されており、互いに低遅延な専用線で接続されています。
●複数AZでシステムを構成する事で、高い耐障害性を実現できます。



日本では東京リージョンに4つのAZがあり、1つの大阪ローカルリージョンがある

- 物理的に離れた場所に設置
- 洪水を考慮、地盤が安定している場所に設置
- 無停止電源(UPS)、バックアップ電源、異なる電源供給元
- 冗長化されたTier-1ネットワーク

https://aws.amazon.com/jp/about-aws/global-infrastructure/

【参考】アマゾン ウェブ サービス：セキュリティプロセスの概要

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf

電力

データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1 日24時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。

可用性

世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。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重複して接続しています。

AWS の使用量は、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。

クラウドプラットフォームとしての安全性

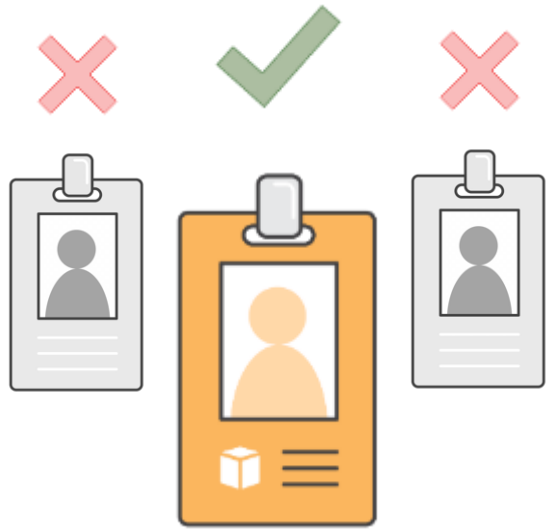
● AWSは、以下の考えに基づきネットワークに関するセキュリティ対策を講じています。

- Distributed Denial of Service (DDoS)対策:
  - ✓ 効果的かつ標準的な緩和対策を実施
- 中間者攻撃対策:
  - ✓ 全エンドポイントはSSLによって保護
  - ✓ 起動時に新しいEC2ホストキーを生成
- IPなりすまし対策:
  - ✓ ホストOSレベルで全て遮断
- 許可されていないポートスキャニング対策:
  - ✓ AWSサービス利用規約違反に該当
  - ✓ 検出され、停止され、ブロックされる
  - ✓ インバウンドのポートはデフォルトでブロックされているため、事実上無効
- パケットの盗聴対策:
  - ✓ プロミスキャスモードは不許可
  - ✓ ハイパーバイザレベルで防御

AWSコンプライアンス https://aws.amazon.com/jp/compliance/

クラウドプラットフォームとしての安全性

● AWSは、以下の考えに基づきハイパーバイザ等に関するセキュリティ対策を講じています。



- ハイパーバイザ(ホストOS)
  - ✓ AWS管理者の拠点ホストからの個別のログイン
  - ✓ 全てのアクセスはロギングされ、監査される
- ゲストOS(EC2インスタンス)
  - ✓ お客様による完全なコントロール
  - ✓ お客様が生成したキーペアを使用
- Firewall機能の標準提供
  - ✓ AWS標準機能としてInbound/Outboundに対するFirewall
  - ✓ AWSのお客様の権限、責任で設定

AWSコンプライアンス https://aws.amazon.com/jp/compliance/

クラウドプラットフォームとしての安全性

● AWSは、以下の考えに基づきハードウェアデバイスの廃棄を講じています。

- データを配置する物理的なリージョンはお客様が指定
- AWSは、法令遵守等やむをえない場合を除き、お客様のデータを指定されたリージョンからお客様への通告なしに移動しません
- お客様のデータが 権限のない人々に流出しないようにするストレージ 廃棄プロセスを保持
  - ✓ DoD 5220.22-M(米国国防総省方式)
    - 3回の書き込みでの消去を実施
    - 固定値→補数→乱数
  - ✓ NIST 800-88(メディアサニタイズのための ガイドライン)
    - 情報処分に対する体制、運営やライフサイクルに関するガイドライン
    - 情報処分に対しする組織的に取り組み
- 上記の手順を用い ハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊します

AWSコンプライアンス https://aws.amazon.com/jp/compliance/

AWSのデータセンターへの立ち入りにつきまして

- 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 TypeII レポート（SSAE 16）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 1Type 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。

https://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

クラウド利用時の評価方針　変わる点

自治体様のクラウド利活用拡大に向けた検討論点例
（従来型システムとの相違点として特に整理しておくべきと思われるテーマ）

地方公共団体におけるASP･SaaS導入活用ガイドライン

6.6.1 データセンターへの現地調査・立入り

従来の委託契約を通じたシステム構築の場合は、システムの監査や障害対応が必要なときは地方公共団体の職員がデータセンターなどへ現地調査や立入りを行う旨の条項が含まれている場合が多い。他方、ASP･SaaSを利用する場合、ASP･SaaSのデータセンターの場所は（日本国内であっても）機密事項とされている場合も多い[14]。よって、システムの監査や障害対応におけるデータセンターへの地方公共団体職員の立入りの可否[15]やデータセンターに関する情報開示については、調達の段階で事前にASP･SaaS事業者やデータセンターに確認しておく必要がある。

[14] 総務省が2009年2月26日に発表した「データセンターの安全・信頼性に係る情報開示指針」においては、データセンターの所在国名、日本の場合は地域ブロック名（関東、東北、など）の開示が必須項目として求められている。
[15] 地方公共団体の職員によるデータセンターの現地調査や内部への立入りをASP･SaaSの調達の際の必須要件とすると、データセンターによってはこれに応じることがセキュリティポリシーに違反する場合もある。

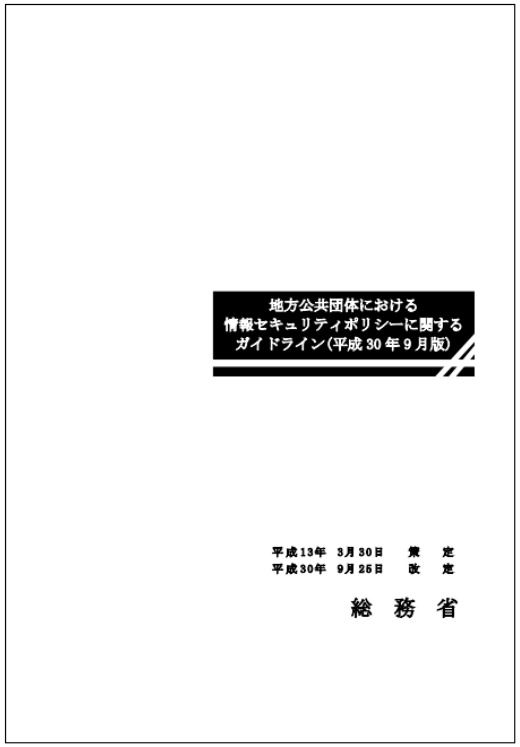
（準拠法）
第６条　本契約の成立、効力、履行及び解釈に関する準拠法は、日本法とする。

（条文解説）
日本国内でのサービスを前提としているため、準拠法も日本法とする。

評価方針	国内法の及ぶ国内にあるデータセンターを前提とするクラウドサービスを利用する

クラウド利用時の評価方針　変わる点

自治体様のクラウド利活用拡大に向けた検討論点例
（従来型システムとの相違点として特に整理しておくべきと思われるテーマ）



【参考】地方公共団体における情報セキュリティポリシーに関するガイドライン(平成30年9月版)

（平成30年9月改定、総務省）

⑪地方公共団体による監査、検査

外部委託事業者が実施する情報システムの運用、保守、サービス提供（クラウドサービス含む）等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001等)の取得等によって確認する。

【参考】政府情報システムにおけるクラウドサービスの利用に係る基本方針
（2018年6月7日、各府省情報化統括責任者（CIO）連絡会議決定）

４．１　セキュリティクラウド認証等

クラウドサービスの情報セキュリティ機能の実態を利用者が個別に詳細に調査することは困難である。そのため、パブリック・クラウドに関しては、第三者による認証や各クラウドサービスの提供している監査報告書を利用することが重要である。
パブリック・クラウドにおいては、以下のいずれかの認証制度の認証を取得し、又は監査フレームワークに対応していることが推奨される。

1）認証制度

(1) ISO/IEC 27017による認証取得

https://isms.jp/isms-cls/lst/ind/index.html

(2) JASAクラウドセキュリティ推進協議会CSゴールドマーク

http://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/

(3)米国FedRAMP

https://marketplace.fedramp.gov/#/products?status=Compliant

2）監査フレームワーク

AICPA SOC2（日本公認会計士協会 IT7号）

AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2号）

評価方針	クラウド事業者は、ISO27001、ISO27017、ISO27018認証を取得していること。 SOC1、SOC2、SOC3監査に対応していること

セキュリティ・コントロール

ユースケース（統制目標）	オンプレミス	AWS
DCの監視カメラにより発見できるリスクはどのようなものか	データの所在を知りうる可能性のある作業者の操作や行動	データの所在を把握およびアクセスすることが出来ない作業者の操作や行動
物理アクセス可能な作業者は意図的に対象となるデータへのアクセスが可能か	内部犯行の場合、可能性あり（データの所在を認識しているからこそ、犯行におよぶ）	**不可能**（仮想環境上にデータがあるため、データの所在を特定できない）
物理アクセス可能な作業者は通常時にデータへのアクセス権を有するか	内部犯行の場合、アクセス権を有する可能性がある	**不可能**（論理環境へのアクセスと物理環境のアクセスや職務分離を適用済）
特定のサーバにアクセスしたログはどこまでを取得できるか（OSレイヤ以上）	システムの実装に依存。OS以上のログにより多層のログ管理は実装可能。	システムの実装に依存（**オンプレミスとかわらない**）。OS以上のログにより多層のログ管理は実装可能。
特定の物理サーバにアクセスしたログはどこまでを取得できるか（OSレイヤ以下）	**＜監視カメラの統制＞** 設置されている範囲の入退室記録装置、監視カメラまで （サーバへの直接の行為は記録できず、間接的）	**＜CloudTrail＞** API Call（AWSのインフラ上での操作一般、サーバの構築、NWの構成変更、閲覧など）を記録可能のため、**より個人を特定した証拠保全が可能**
OSレイヤ以下のログの記録管理はどこまで保証できるか	事業者の統制による（長期保管が可能な場合でもメディアの劣化等に対する統制の保証は困難）	S3における耐久性の保証（**消失、劣化等の懸念は小さい**）

AWSでは、物理的なレイヤの作業を行う従業員と論理的なレイヤの作業を行う従業員は完全に分離しており、その統制は第三者による監査において評価されています。

評価方針	**セキュリティ事故発生等に備え、受託事業者はクラウドプロバイダーが提供するアクティビティログ機能等を十分に活用した構成とし、運用を行うこと。また、セキュリティ事故発生等にあっては、これら機能を活用し、県(市）への情報提供に協力すること**

政府機関向け「アマゾン ウェブ サービス」対応セキュリティリファレンス

アクセンチュア、NTTデータ、PwCあらた、富士ソフトの4社にてAWSクラウド利用における政府機関向けセキュリティリファレンスを作成
（昨年3月より各社HPなどで提供開始）

アマゾンのクラウド安全利用

手引書を公開へ

NTTデータなど行政向け

NTTデータやアクセンチュアなど4社は、行政機関が米アマゾン・ドット・コムのクラウドサービス「アマゾン・ウェブ・サービス（AWS）」を安全に利用するための手引書を月内に公開する。行政機関が取るべき情報セキュリティー対策を列挙した政府の指針に基づき、行政機関でも安全にAWSを使えるようにする。

政府の指針では、情報漏洩を防ぐことやデータを海外に保存することの法的リスクを考慮することなど、広範囲にわたる対策を示している。手引書では、AWSが情報漏洩対策に関する国際的な認証を受けていることや、データの保存場所を日本に指定する機能が備わっていることなど、政府の指針に沿ってAWSを利用する方法を解説する。

政府は内閣サイバーセキュリティセンター（NISC）が公表した「政府機関の情報セキュリティ対策のための統一基準」と「府省庁対策基準策定のためのガイドライン」で指針を定めている。NISCは2016年8月の改訂版でクラウドに関する項目を加えた。

これを受けて日本でAWSを運用するアマゾンウェブサービスジャパンの呼びかけに応じたNTTデータとアクセンチュア、PwCあらた、富士ソフトの4社が約半年をかけて手引書を策定した。4社は手引書を公表することで、AWSを利用する可能性のある政府機関をコンサルティングや情報システム構築の顧客として獲得したい考えだ。手引書はアクセンチュアを除く3社のウェブサイトから入手できるようにする。

アマゾンは米国や英国、オーストラリア、シンガポールなどでも同様にAWSの利用手引書を策定している。日本では今回の行政機関向けの手引書のほかに、すでに金融機関向けの手引書を情報セキュリティー大手のトレンドマイクロやシーエーシーなどの協力を得て公開している。

評価方針	利用予定のクラウドサービスについて、業界において知見と実績が蓄積し、「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）」へのリファレンスがまとめられていること。

クラウド利用時の評価方針　変わる点

自治体様のクラウド利活用拡大に向けた検討論点例
（従来型システムとの相違点として特に整理しておくべきと思われるテーマ）

平成 29 年5月 19 日
個人情報保護条例の見直し等について（通知）

5　オンライン結合制限

個人情報保護条例におけるオンライン結合（通信回線を通じた電子計算機の結合をいう。）による個人情報の提供について、多くの地方公共団体では制限されているが、個人情報保護審議会等の意見を聴いた上で、公益上の必要があると認める場合などには、個人情報保護条例に基づきオンライン結合が認められている。

一方、行政機関個人情報保護法では、オンライン結合を禁止しておらず、地方公共団体においても、ＩＴの活用により行政サービスの向上や行政運営の効率化が図られていることから、オンライン結合制限については、行政機関個人情報保護法の趣旨を踏まえながら、その見直しを行うなど、各地方公共団体において適切に判断する必要がある。

政府方針を踏まえながら、各自治体で、適切に判断し見直しを行う

クラウド利用時に求めるべき要件

従来の区分	クラウド利用時の文言案	評価方針	適用先
DC	クラウド事業者は、ISO27001、ISO27017、ISO27018認証を取得しており安全性が評価されていること	政府方針に沿うため左記ISOを取得しているクラウド事業者を評価する	クラウド事業者
DC	利用予定のクラウドサービスについて、業界において知見と実績が蓄積し、「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）」へのリファレンスがまとめられていること。	政府方針に適応するクラウドの利用方法が整理されている事業者を評価する	クラウド事業者
DC	クラウド事業者が適切に入退室管理等が実施され運用されていることを、第三者の監査機関による監査を受け、その内容を確認できること。	監査結果を自由に閲覧できるクラウド事業者を評価する	クラウド事業者
DC	クラウド事業者は国内法の及ぶ国内に、距離の離れた複数のデータセンタ群を保有し、利用者がデータ保管するデータセンタ群を指定できる仕組みを提供すること。	国内を前提とする	クラウド事業者
DC	クラウド事業者は、ISO/IEC27001に準拠して、データ流出がないよう、NIST800-88に詳述された技術を用いてデータ破壊を行う廃棄プロセスを確立していること。また、このことに関し、第三者の監査機関による監査を受け、その内容を確認できること。	物理的削除処理方法が明確に定義され、実施されているクラウド事業者を評価する	クラウド事業者
DC	データセンターの住所地を非公開とし、データセンターに対する物理的なアクセスを権限のある人物のみに制限するなど、データセンターに与える物理的な影響を最小限に抑えていること。	非公開とする事で物理的な安全性とセキュリティ向上を考慮しているクラウド事業者を評価する。	クラウド事業者
運用	クラウド事業者はクラウド事業者の責任範囲となるリソースへのインシデントレスポンスが定義され実行されていることを、第三者の監査機関による監査を受け、その内容を確認できること。	監査結果を自由に閲覧できるクラウド事業者を評価する	クラウド事業者
運用	**セキュリティ事故発生等に備え、受託事業者はクラウドプロバイダーが提供するアクティビティログ機能等を十分に活用した構成とし、運用を行うこと。また、セキュリティ事故発生等にあっては、これら機能を活用し、県(市）への情報提供に協力すること**	API操作ログによりクラウドリソースへの作業実行状況を記録・活用し、迅速に県（市）へ情報提供が可能な受託者を評価する	受託者
運用	外部要因（DDOS,クラウド事業者責任範囲のインシデント対応）の有無を迅速に確認するサポート体制を取ること。	インシデント対応時にクラウド事業者のサポートと迅速に連携できる体制をもつ受託者を評価する	受託者

AWS検討において頻繁にご質問頂くこと

クラウドの安全性	AWSでは
国内DCであること	東京リージョン（4箇所のDC群）及び大阪ローカルリージョンを利用可。AWSは顧客データを移動しない。
国内法が適用されること	AWSカスタマーアグリーメントの準拠法を日本法に、第一審裁判所を東京地方裁判所に変更可。
データ所有権、統制権は利用者が持つ	AWSは利用者のデータにアクセスしない契約である。データ所有権、統制権は利用者が持つ。 利用者は適切な安全措置を行う。（ネットワーク、ファイアウォール設定、認証、暗号化実施など）
他テナントから隔離されること	AWSはディフォルトで各テナントは隔離されており他利用者のサーバ、ネットワーク、データにアクセスしえない。必要に応じて（BYOL時、VMware Cloud on AWS ）、専用ホストにより物理サーバの専有化が可能。
第三者認証による評価	ISO27001,ISO27017,ISO27018,SOC1,SOC2, etc

データ経路（接続パターン）	AWSでは
専用線接続ができること（内部扱い）	マルチキャリアの専用線をサポートしており、全サービスに専用線経路にて閉域接続可能。
LGWAN経路の接続ができること	パートナーソリューションを介して可能。
インターネットに接しない構成	Amazon VPC（バーチャルプライベートクラウド）は、お客様専用プライベートネットワークを提供している。インターネットに接しない構成が取れる。

特定個人情報の取り扱い	AWSでは
クラウド事業者は、番号法上の委託に該当するか	個人情報保護委員会が公開する「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」のQ&Aでは、クラウド事業者が個人番号を含むデータを取り扱わない場合は、委託に該当しないと整理いただいている。利用者は、クラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、適切なアクセス制御を行うように留意する。https://www.ppc.go.jp/legal/policy/faq/
立ち入り監査	個人情報保護委員会のガイドラインに記載されている「実地の監査、調査等」は番号法上の委託先に対して行うものであり、上記Q&Aの整理によれば、あくまで、特定個人情報を取扱うシステムの委託事業者に対して行うもの。他方、委託事業者が利用するクラウド事業者では、ISO27001等安全性評価に関わる認証を取得し、第三者による監査を受ける（クラウドの安全性を代替監査で評価する）。
データ消去証明	ISO/IEC27001に準拠して、データを復元できないよう電子的に完全に消去または廃棄する。データ消去、廃棄が適切に実施されていることを、第三者の監査機関による監査を受けた内容を提供することが可能である。利用者はデータ暗号化した暗号鍵の消去、ワイプ処理など追加対策も取れる。

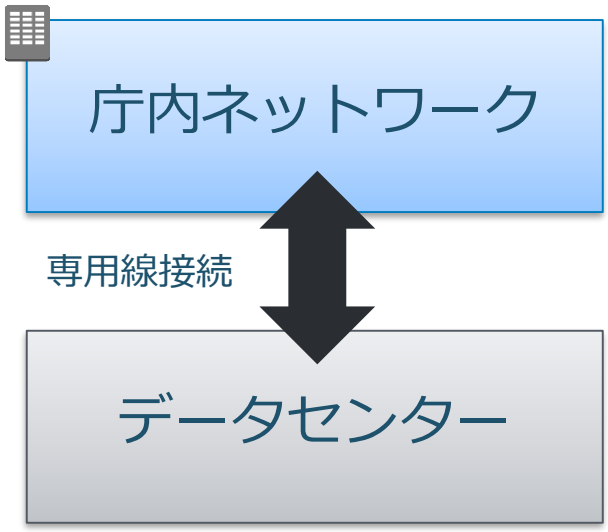
自治体のお客様が実施する
具体的な安全措置

※内部情報、基幹系を視野に

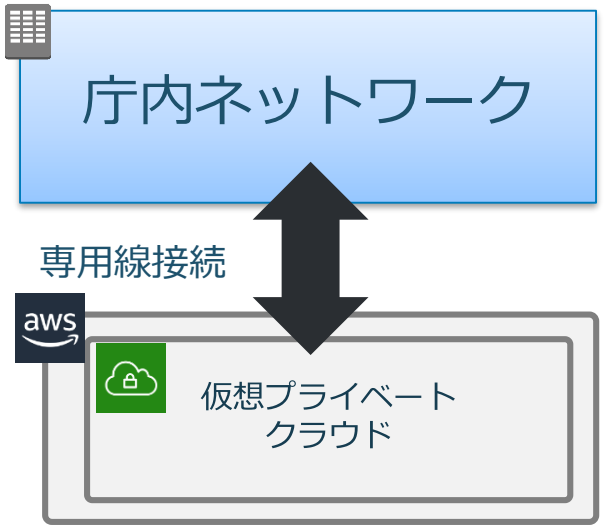
インターネットと分離されたプライベートクラウド環境

AWSは、各サービスを「プライベートクラウド型（バーチャルプライベートクラウド＝VPC)」で活用することで、セキュリティのコントロール、コスト削減の双方を実現することが可能です。

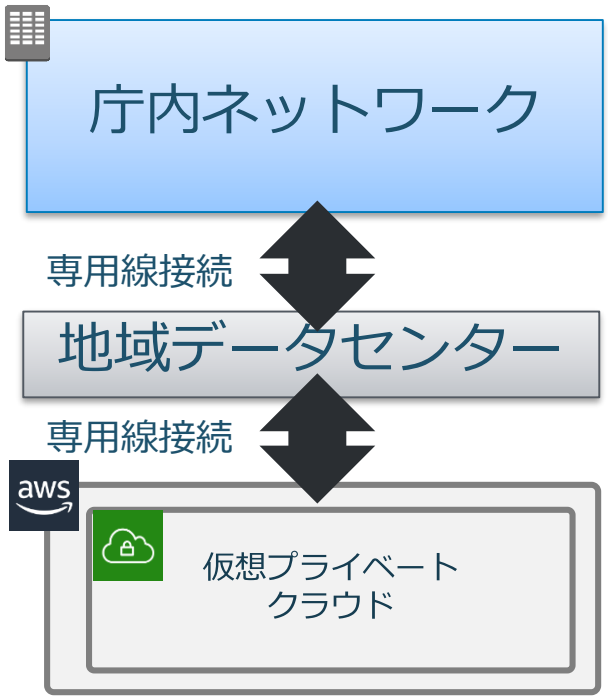
- VPC（仮想プライベートクラウド）はインターネットと分離されており、庁内ネットワークと専用線接続することで、既存のデータセンターと同等なセキュリティ環境を提供することが可能



既存自治体の外部DCへの委託構成



クラウドに閉域接続し、仮想プライベートクラウドに専用領域を構築する構成

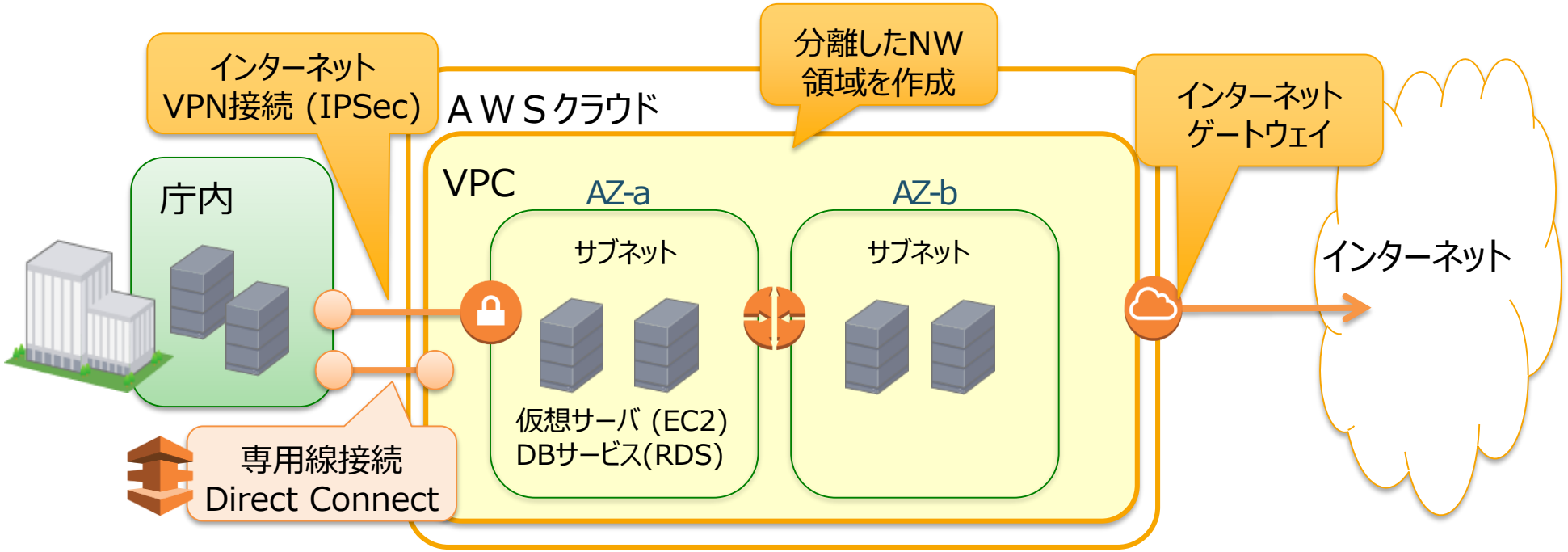


既存自治体の地域DCをハブとしたクラウド接続

バーチャルプライベートクラウドの利用

AWSはお客様専用のプライベートクラウドとして利用することが可能です

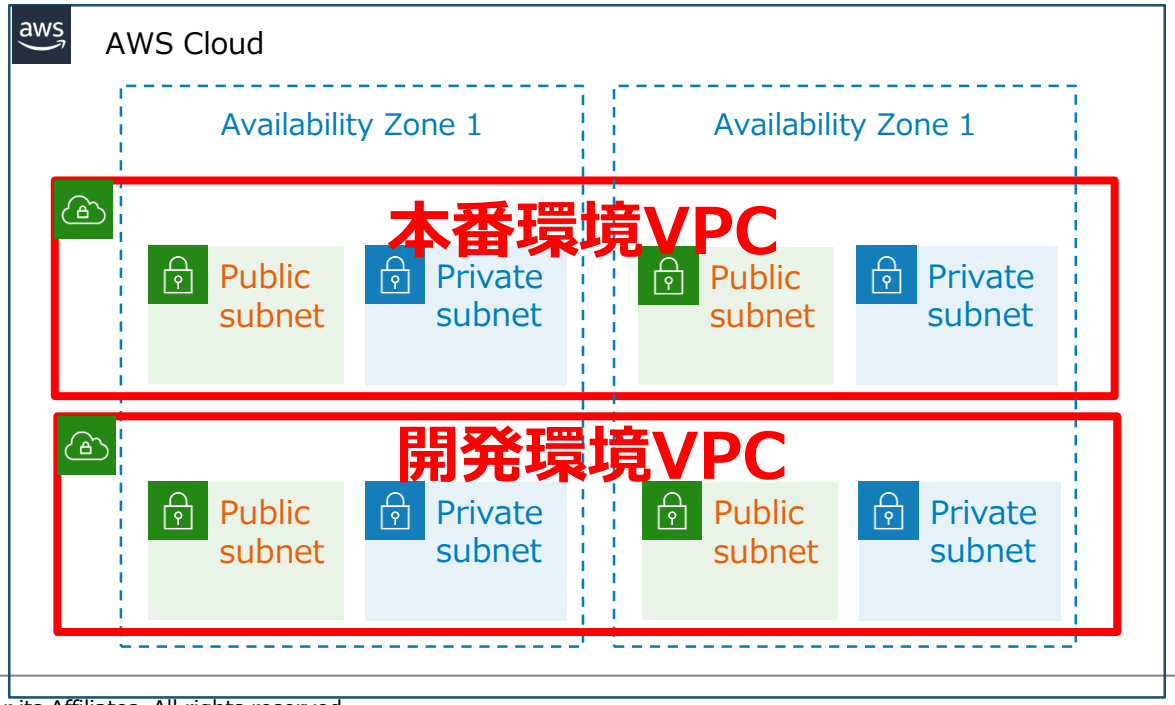
リージョン内にお客様専用のバーチャルプライベートクラウド（VPC)を構築
VPCは複数のデータセンター(AZ)にまたがる。VPC内に仮想サーバを分散配置が可能
庁内ネットワークからAWSへは、インターネットVPN、専用線やキャリアの閉域網で接続可能



Amazon VPC

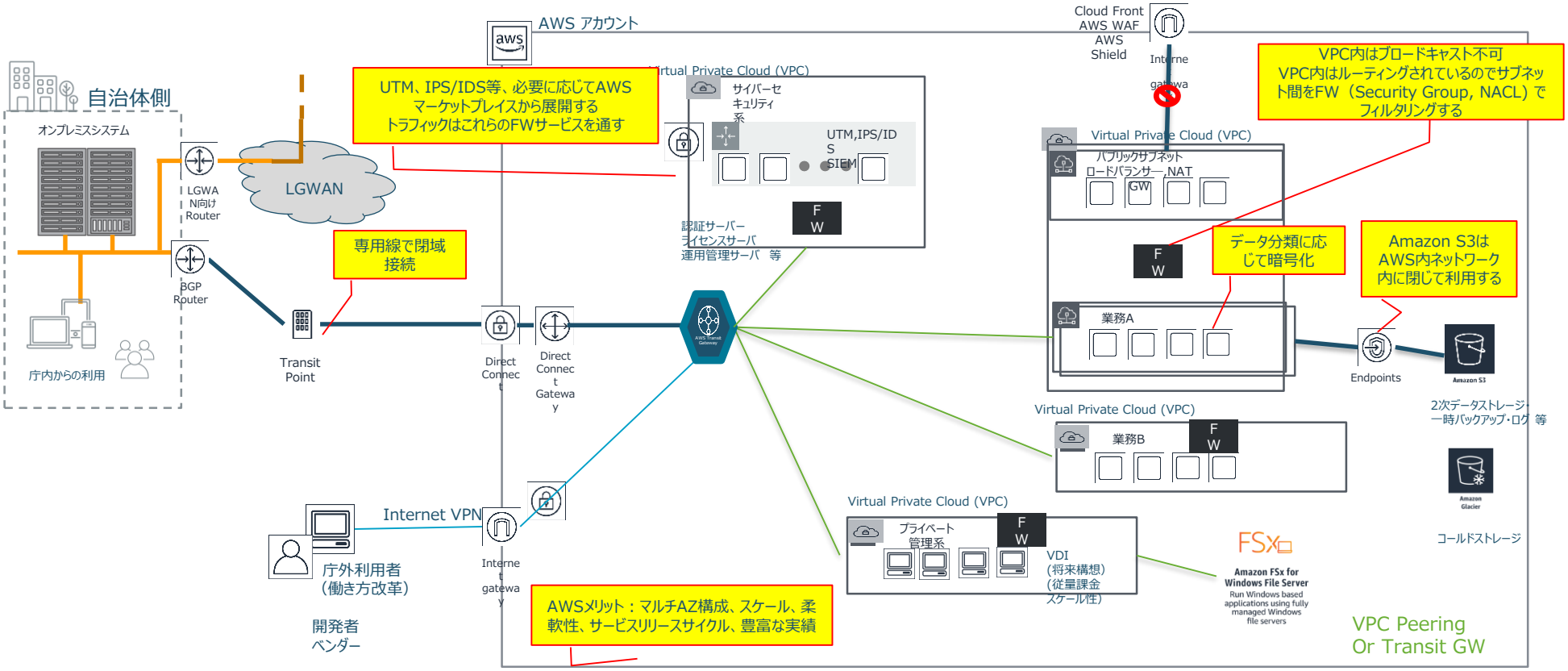
- Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。

  - アカウント毎に独立したプライベートネットワーク (VPC)を提供
  - 1アカウントで複数VPCを構成することも可能
  - アカウント間で共有可能なShared VPCも提供
  - 本番/開発環境/サンドボックス環境などでVPC(またはアカウント)を分ける
  - 事業部やプロジェクト毎にVPC(またはアカウント)を分ける(システムA、システムB、共通基盤等)



自治体NWとAWS　デザインパターン

IS27001、ISO27017、ISO27018、SOC1、SOC2
物理・論理統制が明確に定義され、代替監査が可能なクラウドを評価する



- ✓ 業務システムはインターネットに接しない構成を取る。
- ✓ 用途ごとにVPCを分割し、明示的に、通信可能なネットワークをPeeringする。
- ✓ VPC内のサブネット間はNACLやSecurity Groupのファイアウォールでフィルタリングする。
- ✓ IAMユーザー、ポリシーにより、利用リソースにガードレールを設ける。

AWSクラウドで共通基盤利用化の検討ポイント

仮想化共通基盤のように、情報政策部門がガバナンスを利かせてクラウド利用する場合の、ステップ（最低限）を記載します。

ステップ 1

AWSアカウント
VPC設計
FW設計

- 組織形態にあったアカウント利用
- 開発と本番
- 情シス部門主導でAWS接続の設計（専用線等）

ステップ 2

IAM管理

- 認証認可
- サービス単位、リソース単位
- 開発と運用の分離

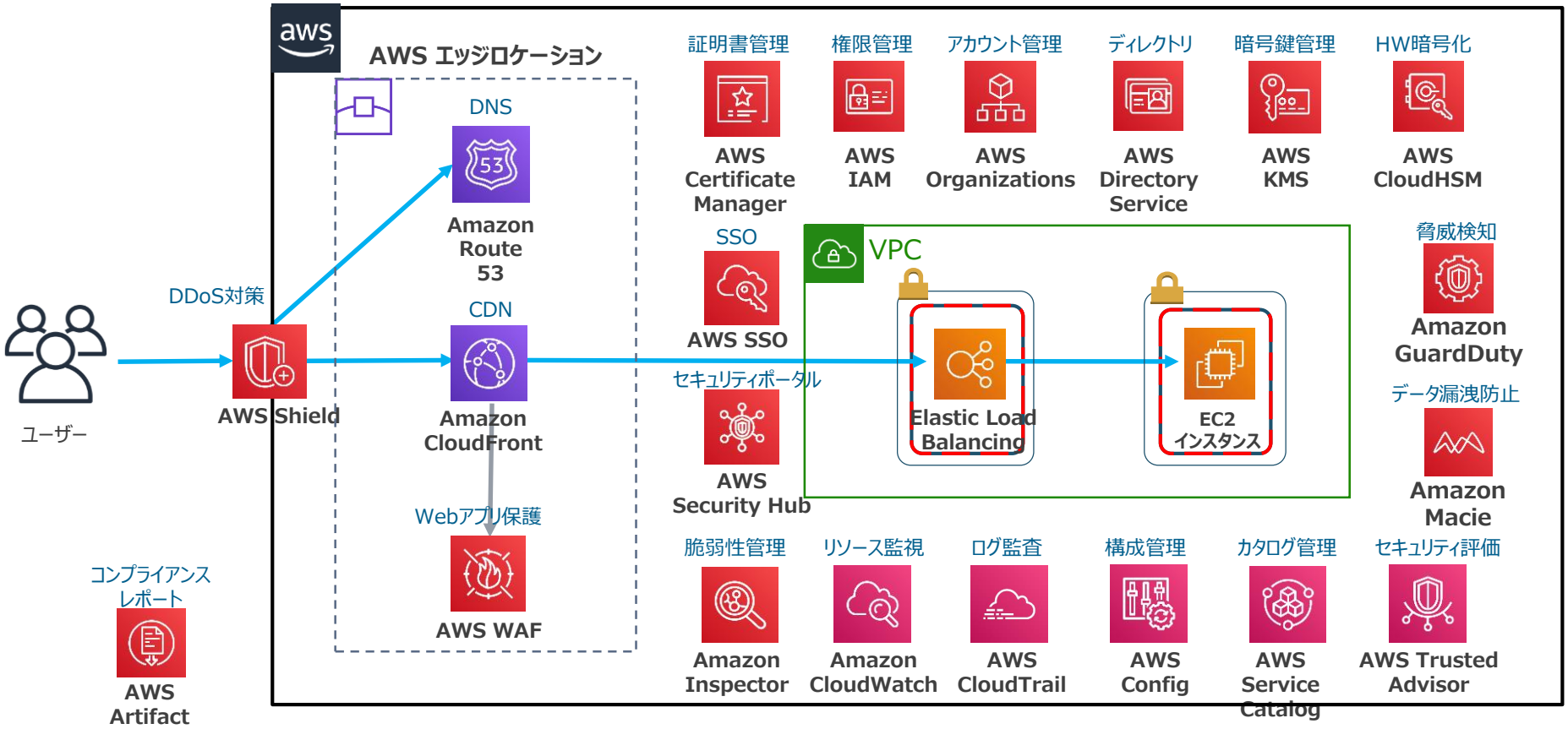
ステップ 3

監視
ログ分析

- AWSのサービス利用を検討
- 一元管理
- UTM等は3rdパーティ

セキュリティツール群を利用する

- AWSは多層防御の考え方。必要なツールを適切に利用する



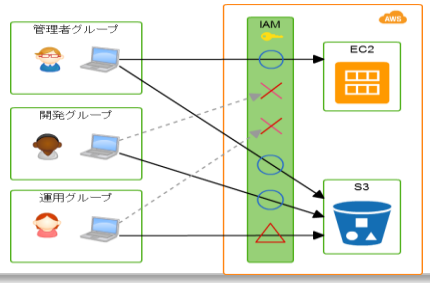
アクセス権限管理とテンプレート化

共通基盤として最低限決めることは、セキュリティポリシー、AWSアカウント管理、ベースとなるネットワーク設計です。
AWSクラウドはIAMという認証認可の仕組みがあり、誰がどのリソースにアクセスが出来るか細かい粒度で設定が可能です。設定はテンプレート化することが可能であり、どのネットワークセグメントにサーバを配置するか、どのFWルールを適用するか、など管理者が予めテンプレートとして組織の設定を作ることで、原課とそのシステムベンダーに設定を徹底させることが可能です。

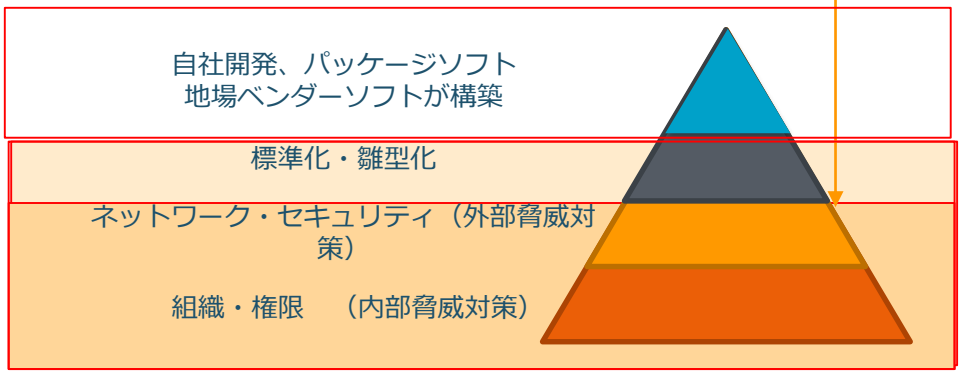
IAM（認証認可）

- アカウントごとのユーザとグループの作成
- セキュリティクレデンシャル（認証情報）
  - アクセスキー
  - ログイン/パスワード
  - 多要素認証デバイス(オプション)

- AWS APIを使ったポリシーコントロールアクセス
- AWSマネージメントコンソールのユーザログオンサポート
- OSやアプリケーションレベルのログインではない。



まずは組織として最低限必要なポリシーをテンプレートに定義する



・実現したい目的ごとにテンプレート化
・開発の内製・外注や、外注範囲に合わせてどの階層までテンプレートを使うかを柔軟に選択
・新しい取り組みの案件からフィードバックし新たな標準化・雛型化に取り込み

ファイアウォール

●通信制御機能として、Network ACLsとSecurity Groupがあります。それぞれの相違点は以下の通りとなります。

NACL(Network Access Clontrol List)

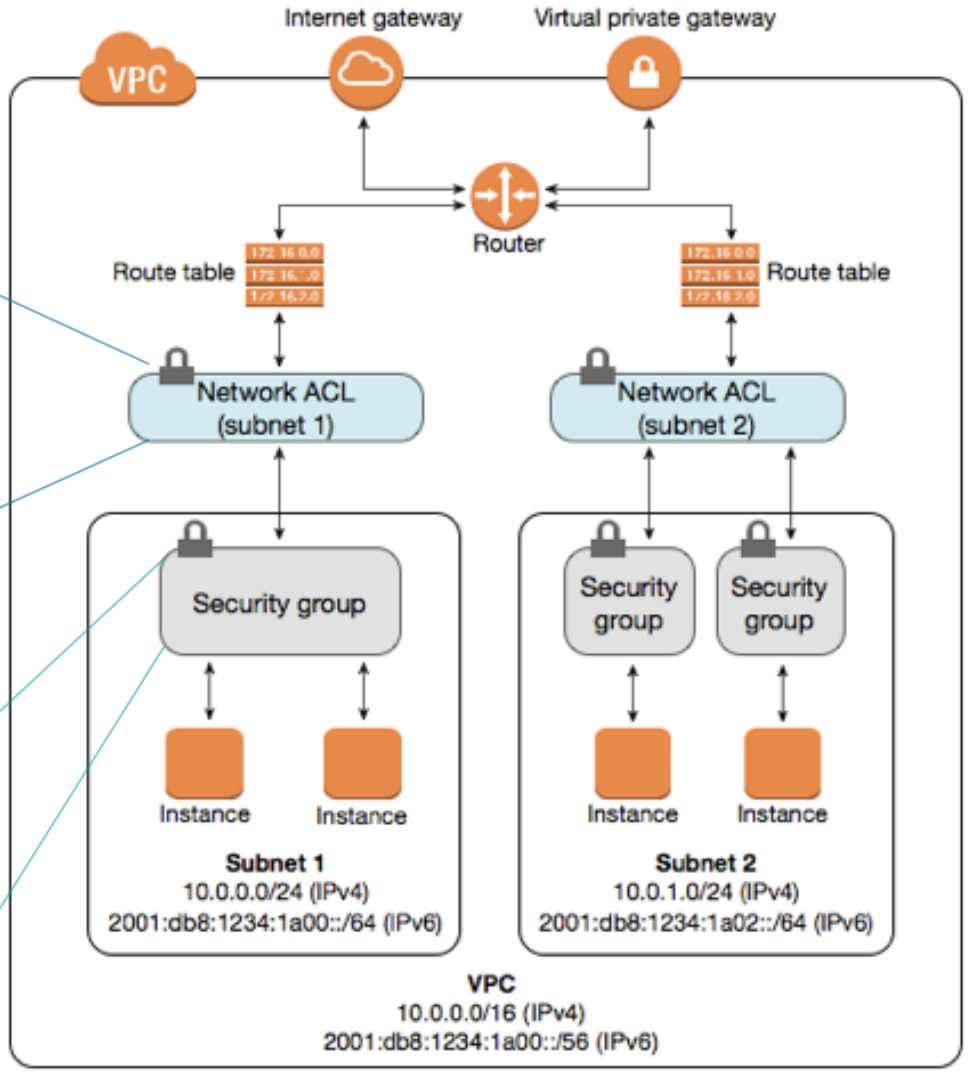
- サブネット毎のFW
- InboudとOutboudのルール
- ステートレス

タイプ	プロトコル	ポート範囲	送信元	許可/拒否
HTTP	TCP	80	0.0.0.0/0	ALLOW
HTTPS	TCP	443	0.0.0.0/0	ALLOW
SSH	TCP	22	192.0.2.0/24	ALLOW
すべて	すべて	すべて	0.0.0.0/0	DENY

Security Group

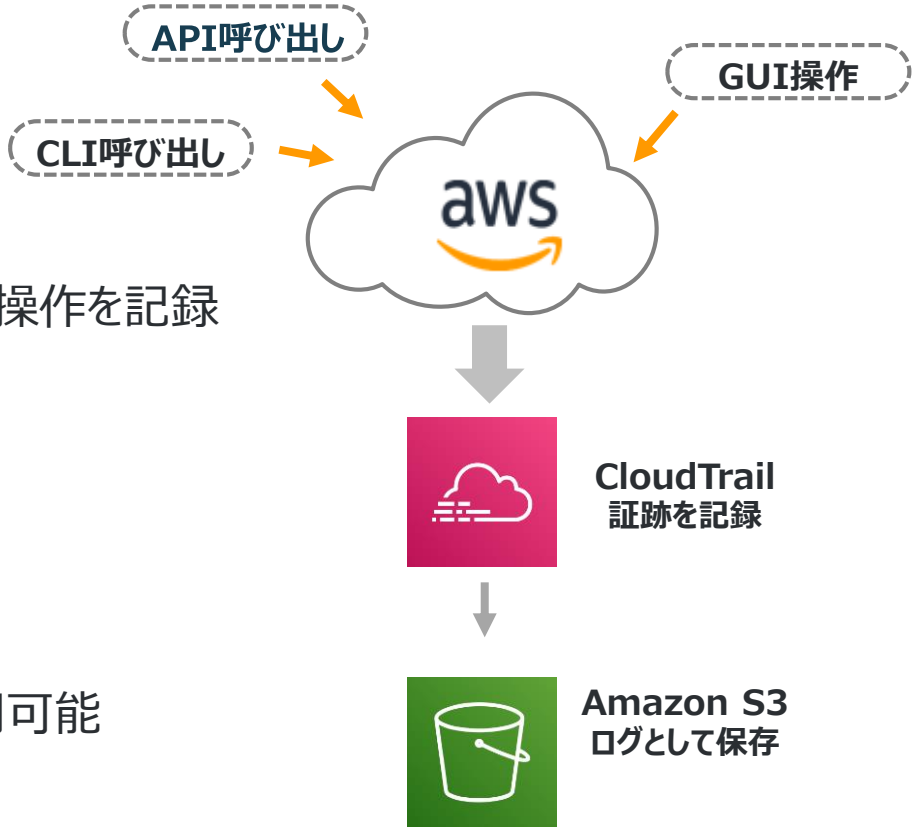
- インスタンス・インターフェース毎のFW
- InboudとOutboudの許可ルール(ホワイトリスト)
- ステートフル

タイプ	プロトコル	ポート範囲	送信元
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	sg-bastion
MYSQL/Aurora	TCP	3306	sg-appl



AWS CloudTrail

- AWS CloudTrail を使用すると、AWS アカウント内で行われた操作のイベントログが自動的に記録および保存されるため、コンプライアンス監査を簡素化できます。



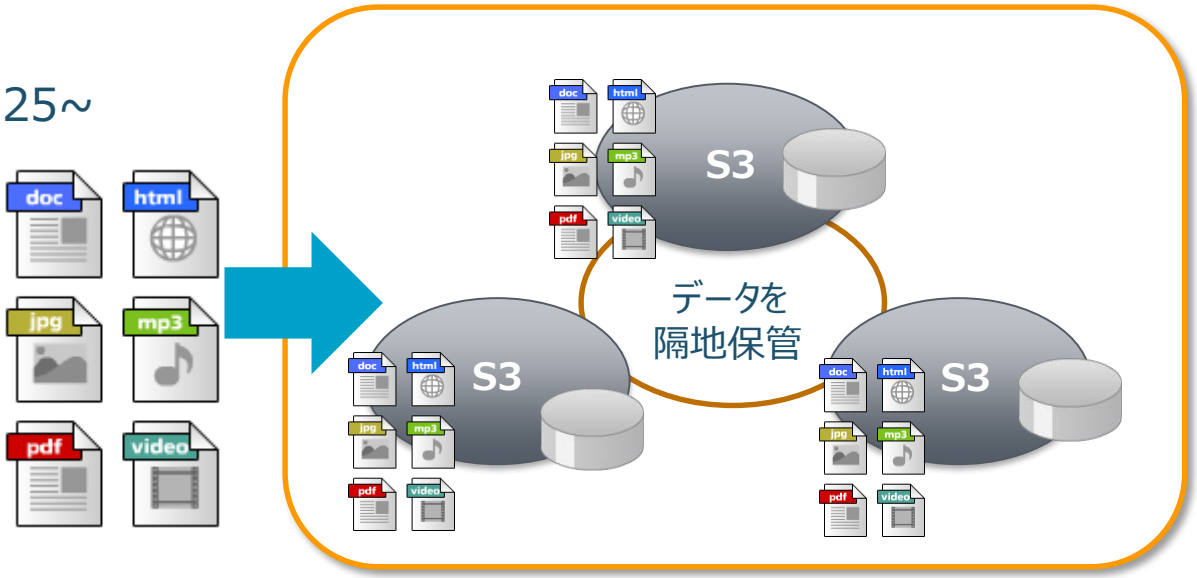
- AWS アカウントの GUI / API レベルの操作を記録
  - ✓ 呼び出し / 操作したID
  - ✓ 呼び出し / 操作したIDのIPアドレス
  - ✓ リクエスト内容（パラメータ）と応答結果
- 操作結果はS3へログファイルとして保存
- セキュリティ分析, 変更の追跡などに利用可能

Amazon S3

- Amazon S3 (Simple Storage Service)は、容量無制限で冗長化された利便性の高いオブジェクトストレージとなります。

- データ保存・バックアップ用途に向くオブジェクトストレージ
- Immutable ファイルを改ざんできないように出来る
- WEBの静的コンテンツ配信機能
- 自動的に3箇所以上のAZに隔地保管
- データ耐久性は、99.999999999%
- 容量無制限、サイジング不要
- 従量課金 1GByteあたり月間 $0.0125~
- 長期アーカイブ用なら$0.00099～

※ 2019年4月時点での米国東部の金額



データの暗号化

- AWS Key Management Service (KMS) を使用することで、キーを簡単に作成・管理し、幅広い AWS のサービスやアプリケーションで暗号化の使用を制御できるようになります。
- AWS KMS はセキュアで弾力性の高いサービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。
- AWS KMS は AWS CloudTrail と統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。

- **暗号鍵の作成、管理、運用サービス**
  - ✓可用性、物理的セキュリティ、ハードウェアの管理をAWS が担当するマネージドサービス
  - ✓暗号化キーを保存および使用するための安全なロケーションを提供
  - ✓暗号鍵の可用性、機密性を確保。低コストで使用可能
  - ✓SDKにより客様の独自アプリケーションデータも暗号化可能

- **S3, EBS, RDS, Redshift等の様々なAWSサービスとの統合**
  - ✓AWS CloudTrail と連動したログの生成による組み込み型監査
  - ✓中国リージョンを除く全てのリージョンで利用可能

https://aws.amazon.com/jp/kms/

サポートを活用する

AWS社員による日本語でのサポートを２４時間３６５日提供します。プロダクション利用ではビジネスサポートないしはエンタープライズサポートを推奨します。サポートタイプは運用中に切り替えることが可能です。初期導入フェーズは専任エンジニアが就くエンタープライズサポートで対応し、落ち着いてきたらビジネスサポートへ切り替えるなど、柔軟な対応が可能です。また、AWSサポートは障害以外のお問い合わせ（操作方法の支援やサービスの説明）やサービス提供に含まれるOSに関する問題の簡易切り分けも対応致します。

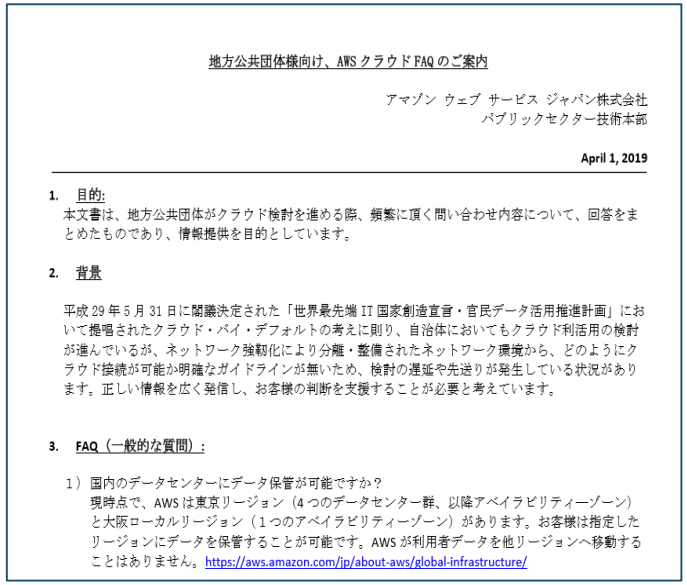
	ベーシック	デベロッパー	ビジネス	エンタープライズ
サポートフォーラム ドキュメント	利用可能	利用可能	利用可能	利用可能
サポートへの コンタクト	ヘルスチェックによる サポート	メール	電話、チャット、 メール、画面共有	電話、チャット、 メール、画面共有、TAM（専任スタッフ）
最速初回応答時間	不可	12時間以内 （営業時間内）	1時間以内	１５分以内
連絡先登録	N/A	1	5	無制限
24/365対応	なし	なし	あり	あり
AWS Trusted Advisor の利用	4項目	4項目	すべての項目	すべての項目
上級サポートエンジニア への直接ルーティング	なし	なし	あり	あり
専任スタッフ(TAM)	なし	なし	なし	あり
特別サポート	なし	なし	なし	あり
概算料金（月額）	無料(AWSの利用料に含まれる)	$49/月	AWS利用総額の10%~ ※最低料金:$100/月	AWS利用総額の10%~ ※最低$15,000/月

自治体様向け　検討促進のご支援について

・自治体向けFAQ集をまとめています。
・個別配布が前提のためお問い合わせください。

・自治体向け基礎ハンズオン（Amazon VPCを理解する）を開催します。
・2019年8月29日　13時～@弊社目黒オフィス
※定員10名まで

・自治体情報政策課様向けクラウドワークショップ（概算・AWS概要設計簡易版）を無償提供します。
・条件、日程は都度ご相談



地方公共団体様向け、AWS クラウド FAQ のご案内

アマゾン ウェブ サービス ジャパン株式会社
パブリックセクター技術本部

April 1, 2019

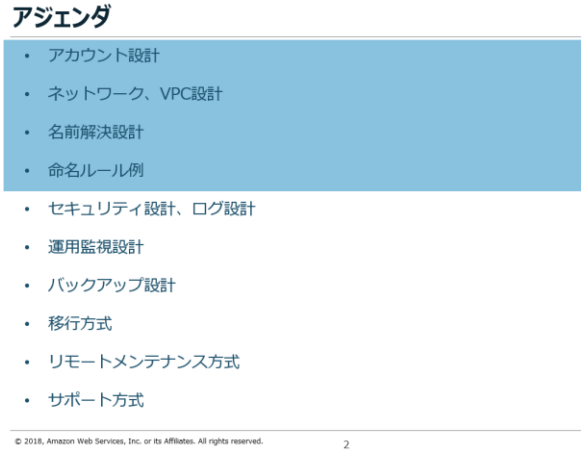
1. 目的:
本文書は、地方公共団体がクラウド検討を進める際、頻繁に頂く問い合わせ内容について、回答をまとめたものであり、情報提供を目的としています。

2. 背景

平成 29 年 5 月 31 日に閣議決定された「世界最先端 IT 国家創造宣言・官民データ活用推進計画」において提唱されたクラウド・バイ・デフォルトの考えに則り、自治体においてもクラウド利活用の検討が進んでいるが、ネットワーク強靭化により分離・整備されたネットワーク環境から、どのようにクラウド接続が可能か明確なガイドラインが無いため、検討の遅延や先送りが発生している状況があります。正しい情報を広く発信し、お客様の判断を支援することが必要と考えています。

3. FAQ（一般的な質問）:

1）国内のデータセンターにデータ保管が可能ですか？
現時点で、AWS は東京リージョン（4 つのデータセンター群、以降アベイラビリティーゾーン）と大阪ローカルリージョン（1 つのアベイラビリティーゾーン）があります。お客様は指定したリージョンにデータを保管することが可能です。AWS が利用者データを他リージョンへ移動することはありません。https://aws.amazon.com/jp/about-aws/global-infrastructure/



お問い合わせ先：　aws-jpps-qa@amazon.com

まとめ

- ✓ 行政サービスの100%デジタル化の実現へ向けて、政府方針はクラウドファーストであり、自治体においてもクラウド利用が必要不可欠
- ✓ AWSはコンプライアンス、ガイドライン等への対処が整理ができている
- ✓ 利用者がAWSリソースを制御可能であり、データ所有権を持つ
- ✓ 政府機関、地方公共団体においてすでにAWS利用ははじまっている
- ✓ 値下げ文化、従量課金でさらにコスト削減、最新技術を利用(AI, IoT)
- ✓ まずはAmazon VPCを使ったプライベートクラウド型利用で進め、セキュリティツール類を使って情報資産を保護する
- ✓ AWSの公共パートナーと共に企画構想・設計・構築をご支援