

【AWS Solution Days 3】

NTTドコモのAWS利用とセキュリティ対策



2015年9月17日
株式会社NTTドコモ
イノベーション統括部
森谷 優貴



○ 森谷 優貴 (Yuki Moritani, Ph.D)

- R&Dイノベーション本部 イノベーション統括部
 - ✓ ドコモのアセットを活用したビジネス創出
 - ✓ 他企業との協創促進

○ 内部システムのアーキテクト, インフラエンジニア

- クラウド/オンプレのシステム/セキュリティ設計, 構築, 運用
- AWSアカウント管理, ガバナンス担当
- 社内コンサルティング, 共通ツール/基盤の作成, 運用
- **docomo** cloud package の主管



NTT ドコモのAWS利用

- Webサービスシステム (しゃべってコンシェル, 等)
2012年～



- 業務系システム (データ分析システム, 等)
2014年～



- ミッションクリティカルシステム

- しゃべってコンシェルのリリースはスピードが必須だった
 - 2011年11月のトップオーダー，2012年3月のリリース
- 当時は社内で不安視する声も数多くあった
 - 信頼性，万が一の際は誰が補償してくれるのか？
 - ✓ クラウドと言っているサービスにおける事故
 - 可用性，落ちたらどうする？
 - セキュリティ
- サーバ調達時間， 需要予測， 開発， 等の条件でクラウドを選択

- ドコモの音声エージェントサービス
 - ユーザの入力に応じて適切な答えを返す

入力＝音声

→ 音声認識

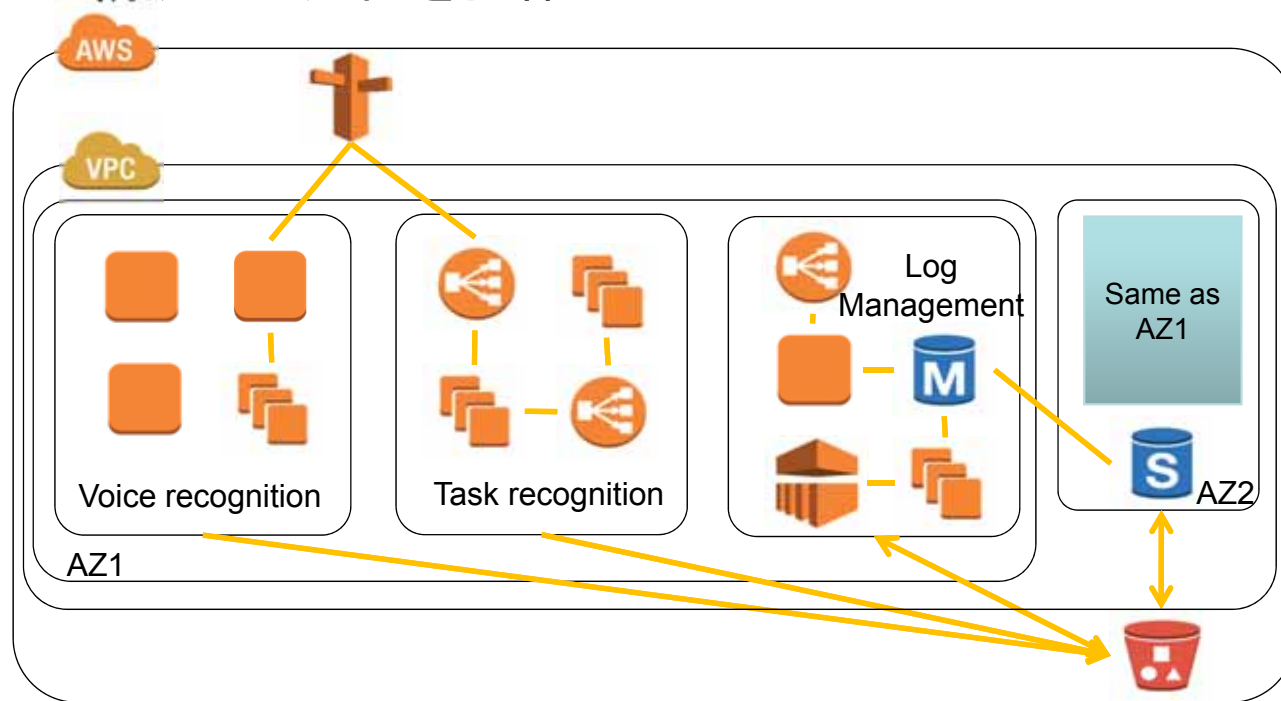
→ 意図解釈

→ 出力（文字＆音声）



○ クラウドの特性を活用したシステム構成

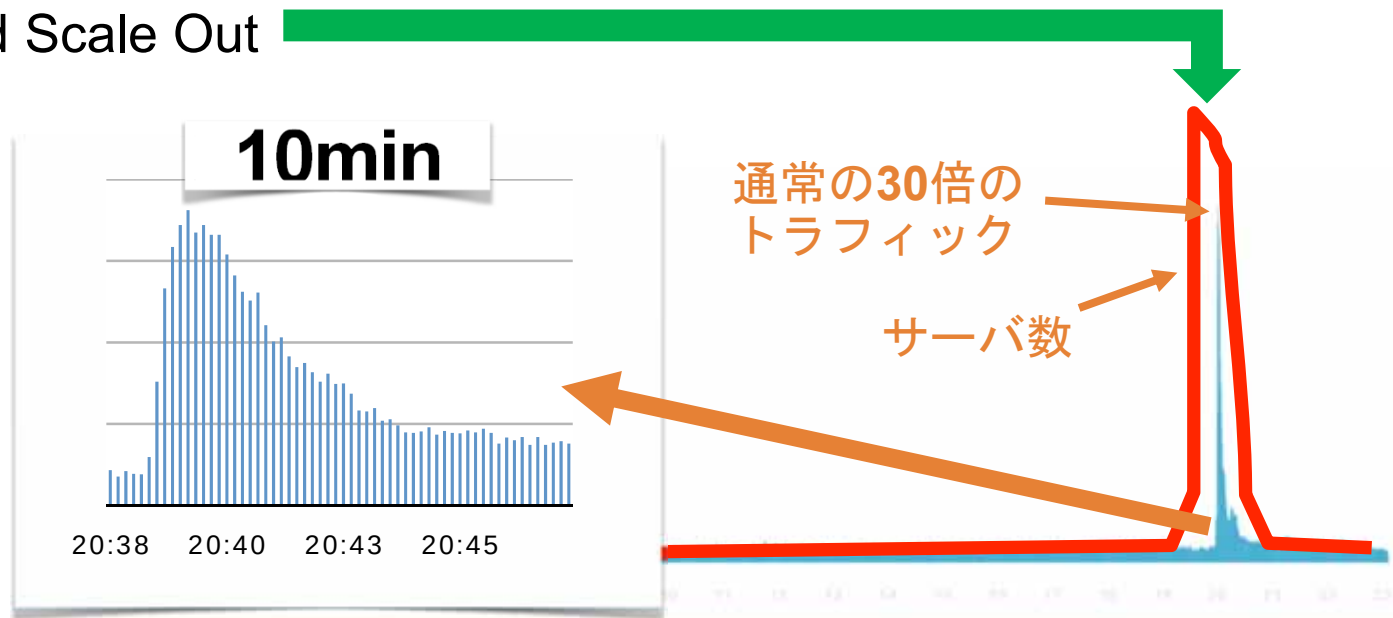
- 音声認識，意図解釈，ログ管理の各マイクロサービスの疎結合システム
- Multi-AZ構成で可用性を担保



- サービス開始と共にトラフィックが急増
 - 当初は国内の別クラウドを2つ利用していたがリソース問題が発生
→ AWSを使い始めた最大の理由
- 2012年4月 AWSの北カリフォルニアリージョンに移行
 - トラフィック増加は続く
- 2012年9月 東京リージョンへ再移行
 - 遅延の改善
- AWSのリージョン間差異がないこと，CDPを利用したCloud Nativeな構成としたことの恩恵で，上記が実現できた

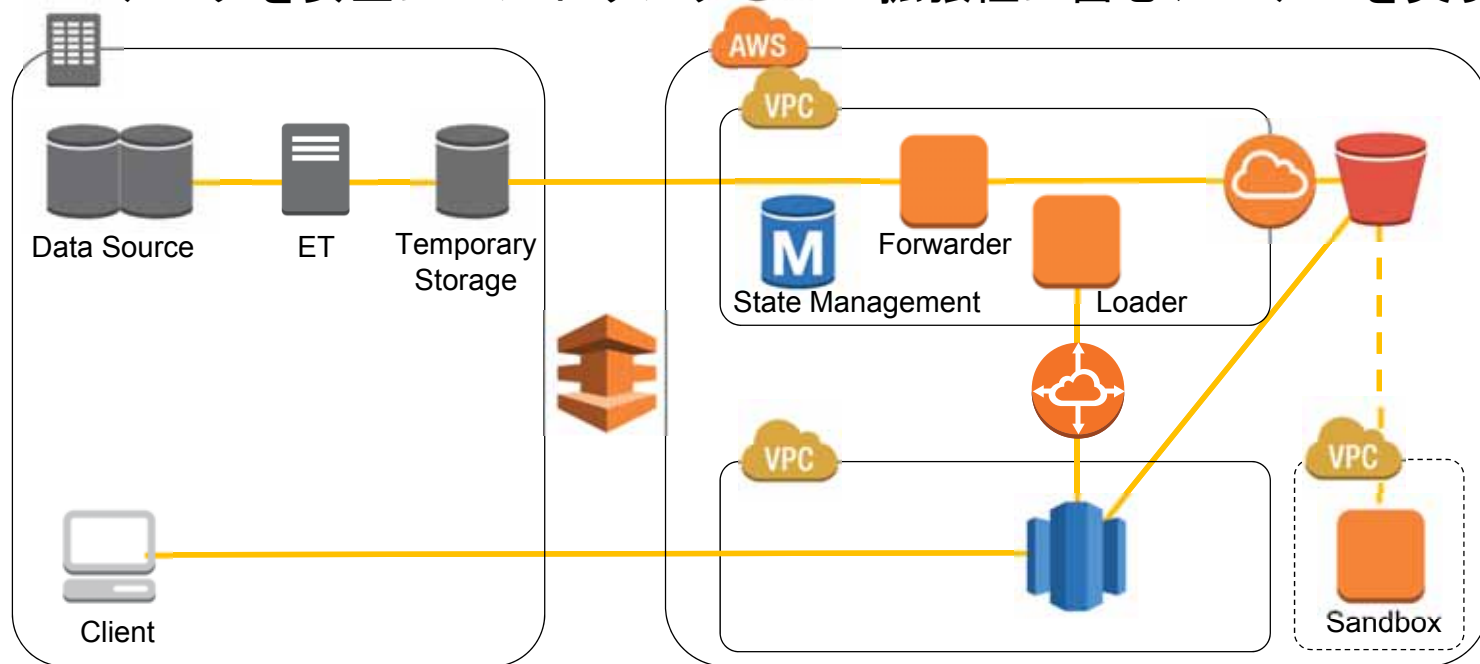
○ 使っているCDP

- Multi-Datacenter
- Clone Server
- Scale Out
- Scheduled Scale Out
- etc.

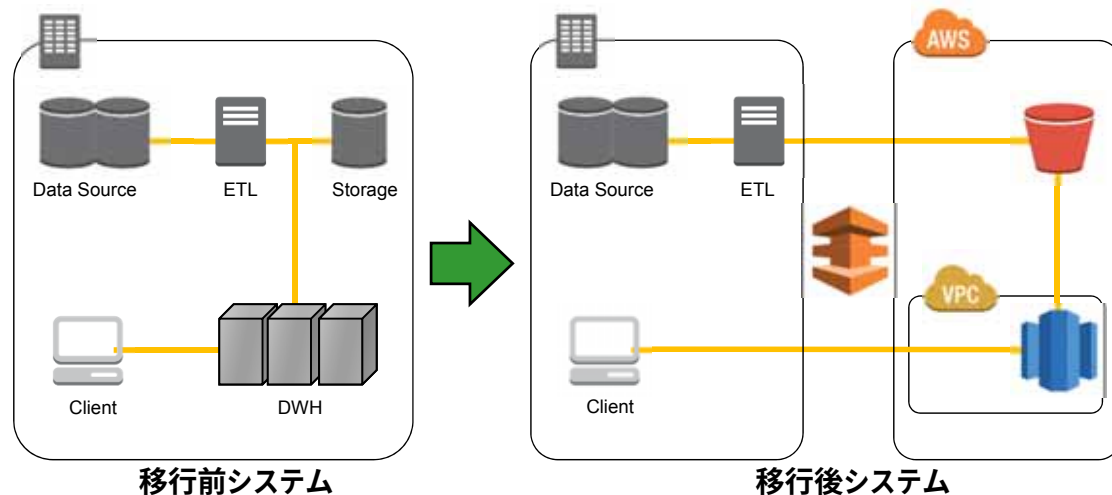


○ オンプレミスとAWSのハイブリッド構成

- オンプレミス環境にてデータを収集，加工，暗号化
- 可用性，信頼性の高いクラウドストレージ上でデータを保管，分析
- PBクラスのデータを安全にハンドリングしつつ拡張性に富むシステムを実現



- オンプレの更改に合わせてシステムをクラウドへ移行
 - オンプレ環境と比較してユーザビリティを下げない
 - セキュリティを担保しつつ、クラウドのメリットと既存資産を活用
- 移行を決めるまでには性能やセキュリティ等、様々な面を検証
 - 具体的なセキュリティ対策については後ほど
- 運用開始後もデータソースの増加（クラウド側）やAWS機能拡充により随時構成変更中



○ 公開しているもの

- docomo Developer Supportの各種API（一部を除く）

docomo Developer support

誰でも、簡単に、マッシュアップ！

○ NTTドコモが公開している開発者向けのAPI提供サイト

- <https://dev.smt.docomo.ne.jp/>（下記リスト以外にも多くのAPIを掲載）



画像認識

画像に写っている物体の情報を取得



ジオフェンシング

仮想フェンス内へのチェックイン/アウトを判定



発話理解

要求を理解して、適切な機能を提示



知識Q&A

今知りたいことにピンポイントで回答



音声合成

入力した文字を読み上げ



雑談対話

自然な会話をやり取り



音声認識

話した内容を即座に文字に変換



言語解析

入力した文字列を解析

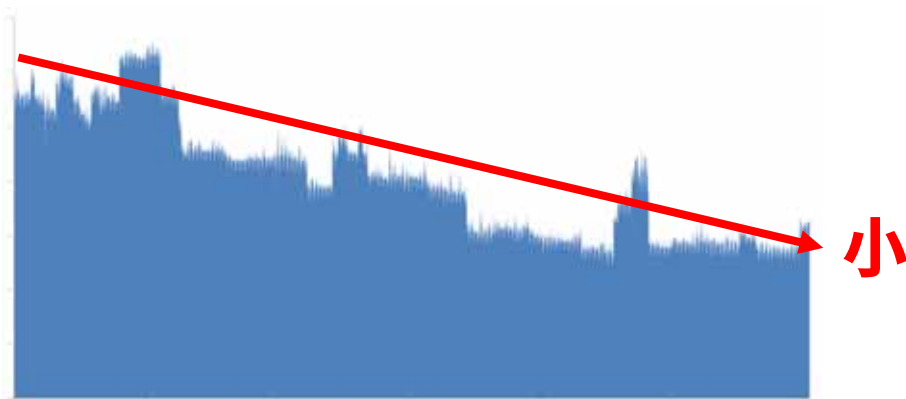
- 4 桁のEC2インスタンスが稼働中
 - Auto-scalingやカスタムチェックによって日々増減
 - ✓ 各サービスでのコスト最適化も継続的に実施
 - Consolidated BillingでRIをShare
 - ✓ 登録アカウント数は継続的に増加中
- コスト分析結果は随時各サービスにフィードバックして改善

EC2利用台数の変遷



- 最初は小さく作り，需要増加と共に大きくスケールさせる典型的な使い方
- 一方で，ドコモにはサービス開始当初の需要が読めないケースも存在（リリースに伴う一斉アクセス，等）
 - 最初はリリース時の高負荷に耐えるために大きく作り，需要の固定化と共に小さくスケールさせていく使い方を多用
 - ✓ EC2インスタンス数/サイズ，DynamoDBキャパシティ，等は時間経過と共に実データを分析して最適化し，固定EC2インスタンス，RDS等はRIを購入
 - ✓ 結果として半年後に時間当たりのコストが約半分になったケースもある

リソース, コスト大



- 単一アカウント vs. 複数アカウント
 - ドコモでは複数アカウントのスタイル
 - ✓ 基本的にはサービス毎にアカウントを作成
 - ・ 開発, 検証, 本番等, 1サービスでアカウントを分割するケースも存在
- 一元管理 vs. サービス側で管理
 - ドコモではサービス側で管理するスタイル
 - サービス毎の独立性を重視
 - ✓ クラウドを利用した理由: スピード&アジリティ
 - ガバナンスのためにクロスアカウント設定 (Role/Policy) を多用
- Consolidated Billingへの加入も強制ではない
 - サービス側でコスト含め全て管理できるのであればそれでも良い
 - ただし, セキュリティ基準を満たすシステム構築・運用は必須

AWSセキュリティ対策

- 情報セキュリティ部
 - 個人情報保護法対策や情報漏えい等に対する全社的なマネジメントの実施、及び社内管理情報に関する方針策定、規程類の制改定等、一元的な情報管理の体制の整備・構築を行う部門
- 情報システム部
 - 主に社内情報システムの構築・運用を担う部門
- ユーザ部門（R&D, 事業部, 等）
 - 社内情報システムの利用部門, かつ社外情報システムの構築・運用部門
- 基本的にドコモで構築する全てのシステムは情報セキュリティ部による審査, 診断を受ける必要がある
 - 情報セキュリティ部＝第三者機関

オンプレ/クラウドを問わず各種規定類に準拠する必要がある

- 情報管理規定
 - 情報管理細則
 - 故意による不正行為抑止
 - セキュリティ対策基準
 - サイバー攻撃対応
 - 情報管理マニュアル
 - 顧客情報管理マニュアル
 - etc.
- 
- 内部・外部のログ
 - 権限付与ルール
 - アカウント管理
 - 入退室管理
 - データ暗号化
 - 情報セキュリティ監査
 - etc.

○ セキュリティ対策として実施しなければならない項目



280



お客様の統制



共有の責任



AWSの統制



お客様のデータ
ユーザー権限管理
アカウント管理
アプリケーション
セキュリティ構成
ネットワーク構成
ゲストOS

お客様固有の要件



仮想化レイヤー
コンピューター・インフラ
ストレージ・インフラ
ネットワーク・インフラ
施設・物理セキュリティ
AWSグローバル・インフラ



- 物理的対策, 運用・監視・体制, ログ・情報保護, 個別対策, 等のセキュリティ対策要件について以下の点を確認
 - AWS自体で満足しているか?
 - AWSの機能を利用して対策可能か?
 - ドコモが独自に対策可能か?
- ドコモが手を出せない部分で未対策の項目がないか?

NTT docomo	アプリケーション		
	OS/ミドルウェア		
AWS docomo	アカウント管理	Firewall/NACL	ログ管理
AWS	仮想インフラ		
	物理インフラ/ネットワークインフラ		
	ファシリティ/物理セキュリティ		

○ AWSのIaaSとしてのセキュリティ

- 各種認証取得要件および内容の確認
- AWSセキュリティチームからのヒアリング

○ 利用可能なセキュリティオプション

- IAM, SG/NACL, CloudTrail, 等
- 暗号化オプション
- サービス毎のログ
- etc.



○ ドコモ側で適切に対応することで実現できるセキュリティ

- 暗号危殆化対策
- etc.

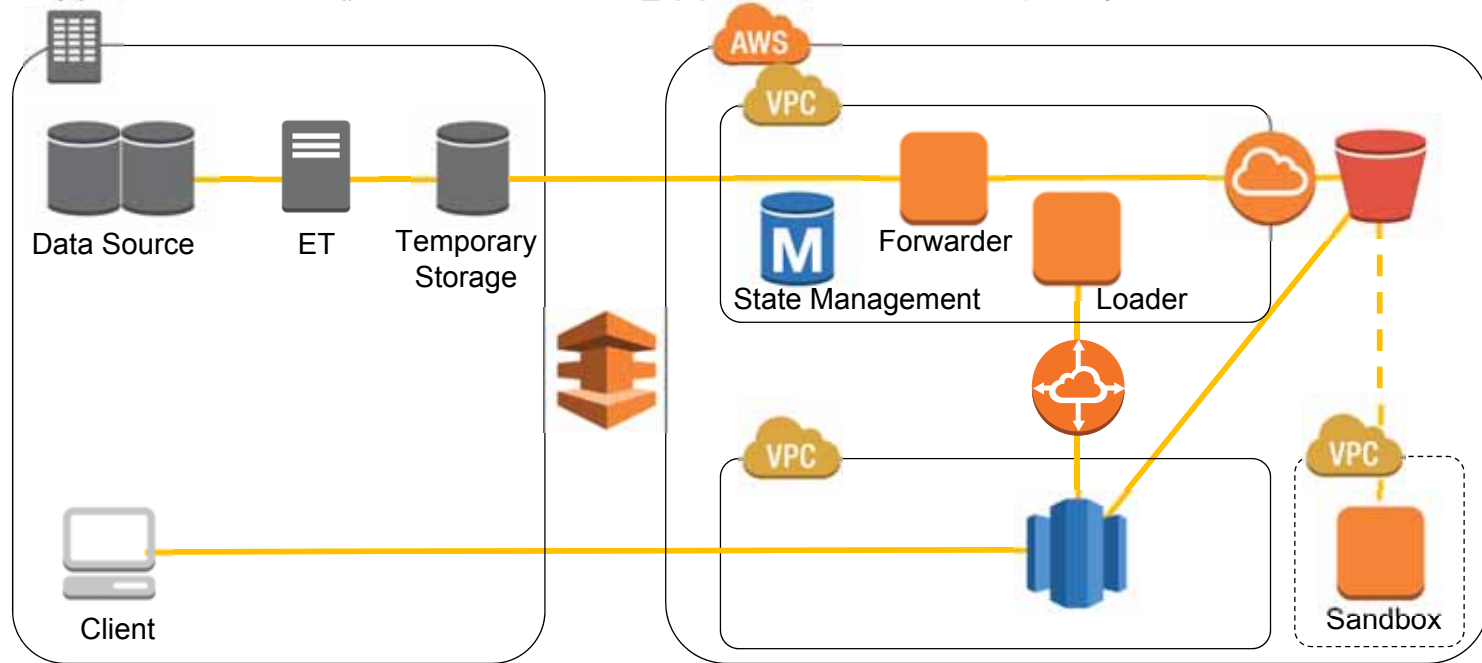
○ 結論

- AWS上でドコモが適切な対策をすればセキュリティ要件を全て満足可能

具体的なセキュリティ対策事例

○ データの漏洩防止

- 外部攻撃だけでなく，内部犯行も防止したい
- データの出口はオンプレ側のみ限定（RedShiftからのUnloadはRevoke）
- 管理者も単独では復号化データを持ち出せないように設計



○ アカウント管理

- AWSアカウントはMFAを設定の上、MFAはこのシステムへのアクセス権を持たない者が保管
 - ✓ 利用する場合は社内承認が必須
- 2種類の管理権限グループを用意し、各管理者はどちらかのIAM権限のみを持つ
 - ✓ 単独では復号化されたデータを持ち出すことは不可能な設計
- 分析者はAWSリソースへのアクセス権を持たず、RedShift (DB) のアカウントのみ保有



○ 暗号化

- オンプレミス
 - ✓ 従来通りに暗号化利用
- S3
 - ✓ SSEに加えてCSEを利用
 - ✓ CSE鍵の管理はオンプレミスで実施
- RedShift
 - ✓ Cluster暗号化オプションを利用
- EBS
 - ✓ 暗号化オプションを利用
- 通信路
 - ✓ SSL利用



※利用する暗号化方式は最も堅牢なものを選択

○ アクセス制御

➤ VPC機能の活用



- ✓ 管理者用VPC（オンプレで暗号化したデータをS3に格納）と分析用VPC（RedShiftのみが存在し、分析者のみアクセス）を分割
 - ✓ RedShiftへのデータCopyは管理者側のEC2で実施
 - VPC-Peeringを利用し、分析者は管理者側にアクセス不可
 - データCopy用EC2はIAM Roleでアクセス先および権限を制限（オンプレの鍵管理DBとRedShiftのみと通信可能でInternet Gatewayへの経路なし），かつSGでInboundアクセス不可，Outboundも制限
 - ✓ 分析用VPCはInternet Gatewayなし
 - 分析後のデータはオンプレ側にのみ持ち出し可能
 - オンプレ側にはドコモ社内のセキュリティ対策があり，データを外部に出す場合は管理職の承認が必須
- S3はBucket Policyでアクセス元を制限
- Direct ConnectではオンプレからS3への直接経路は設けていない
- ✓ 管理者も暗号化されていないデータをS3に格納できない



○ ログ管理



➤ 全ての操作ログを取得

- ✓ CloudTrail, S3/RedShift/RDSログ, 等
- ✓ EC2の操作ログ等も収集しデータとは別のS3 Bucketに保管
 - ・ 削除防止のためMFA Deleteを使用

➤ 収集したログデータは定期的に監査される

- ✓ 監査レポートを, このシステムのアクセス権を保有しない管理職が確認

○ EC2の管理



➤ 基本的にSSH等の直接アクセス不可

➤ Copy等はレポジトリから取得したコードを実行するのみ

➤ セキュリティパッチ適用が必要な場合は別環境で適用したAMIを利用

○ オンプレミス側の管理

➤ 全てドコモのセキュリティ基準に準拠する形で構成, 運用

➤ 管理/分析環境にアクセスできるのはセキュリティルームのみ

- システム拡張や機能拡充に伴い新たな対策が必要に
- 検討と検証を繰り返し、現在も改善中
 - S3 VPCエンドポイントの導入
 - ✓ 機能検証および設計、設定を完了し、運用中
 - ✓ NACLでS3アクセス許可が必要なためVPCエンドポイントのポリシー制限が可能になり、Elastic IPが不要になるが管理者権限は依然として分離が必要
 - ✓ RedShiftがS3 VPCエンドポイントに対応して欲しい！
 - 社外データの取り込み
 - ✓ 社外からデータを受け取り社外データ用のS3に格納
 - ✓ 社外データ用S3からRedShiftにCopy

セキュリティ対策は終わらない

- ドコモ側担当者はAWSに詳しくなく，基本的には開発ベンダに丸投げしたい
 - ただしコストは下げたいのでConsolidated Billingには加入
 - Consolidated Billing利用条件では，AWSアカウントはドコモ管理，また一部のドコモ保有IAMアカウントもドコモで管理（コスト確認，IAMの設定，等）
- コンサルチームで開発ベンダが利用するIAM Group/Roleをあらかじめ作成し，開発ベンダの管理者用IAMアカウントを発行
 - ユーザ管理，グループの適用，ロールの付与，等は開発ベンダで実施
 - 想定外の利用ケースのみ開発ベンダからの依頼を受けてコンサルチームで追加する対応とした

設定したポリシー（抜粋）

- ドコモIAMアカウントに対する操作禁止
- 特定IPアドレス（ベンダ環境）からのみの操作制限, に加えて

```
{"Statement": [{"Effect": "Deny",  
  "Action":  
["iam:DeleteGroup","iam:DeleteGroupPolicy","iam:DeleteRole","iam:DeleteRole  
Policy","iam:DeleteUserPolicy","iam:PutGroupPolicy","iam:PutRolePolicy","iam:  
PutUserPolicy","iam:CreateGroup"],  
  "Resource": ["*"]  
}]}
```

- 事前に用意しておいたRoleやGroupのAttach/Detachは実行可能なため、
開発ベンダで作成したIAMユーザやEC2インスタンスに権限付与が可能

- 特段問題なし，ベンダさんの依頼でGroupやRoleを随時追加した程度
- 2015年2月：IAM Managed Policyリリース
- それまでのPolicyはインラインポリシーとなり，IAMの権限管理が一新
 - 前述のポリシーではAWS Managed PolicyがAttachできるため，AdministratorAccess権限も付与可能となってしまった



- AWS Managed Policyのみ付与不可とするポリシーを追加

{

 "Effect": "Deny",

 "Action":

 ["iam:AttachUserPolicy","iam:AttachGroupPolicy","iam:AttachRolePolicy"],

 "Condition": {"ArnEquals": {"iam:PolicyArn":

 "arn:aws:iam::aws:policy/*"}},

 "Resource": ["*"]

}

- 一方でAWS Managed Policy利用のメリットを享受できないため、改善検討中

- **AWSの仕様が変更することもあるためセキュリティ対策は随時対応していく必要有**
リソースもセキュリティ対策も運用後のカイゼンが大事！

- セキュリティ審査・診断を通すことが目的化してしまう
 - 審査・診断に通ることでセキュリティが担保されるという勘違い
 - 審査・診断はベースライン，目的に応じて追加の対策が必要
- よくわからないのでIAM権限はAdminとRead-onlyの2種類のみ
 - 環境変更をする時はAdmin，監視はRead-only，等
 - Read-onlyが安全なわけではない，S3やDynamoDBのRead権限があるということはデータを閲覧できる権限があるということ
 - ✓ 持ち出しもできるので，扱う情報次第でCSE等を併用する必要がある
- 暗号化というと通信経路の対策ばかりに気をつかう
 - 前項とも関連するが，VPN，SSL/TLS，Direct Connect等の対策ばかりに気をつかい，データの暗号化はSSEのみ
 - ✓ KMSで適切な権限設定する等の例外はあるが，SSEは内部不正に対しては効果があまりない（アクセス権=復号化権）
 - ✓ セキュリティは全レイヤで考える必要がある

ガバナンスの必要性

- クラウドでもセキュリティ対策基準に準拠可能ではあるが、一方で誤った使い方をすると大変
 - セキュリティ的に問題のある構成，運用
 - 小さく作って大きく伸ばすことも，大きく作って最適化することもできない構成
 - オンプレでの開発に慣れていると陥りやすいこともある
 - アカウント数が増えてくると全システムを細かくコンサルティングするのは困難
- 間違った使い方をしないためにはガバナンスが重要
 - クラウドを使う場合の考え方，お作法
 - 気をつけるべきセキュリティ観点
 - どういう機能を使って何をすればよいのか等を利用者，開発者に正しく理解してもらう

○ クラウド開発ガイドラインの作成, 展開

- AWSを使う場合の考え方やお作法, ドコモの開発フローにおける各フェーズで考慮・実施すべき指針を記載 (現在180ページ程のボリューム)
- 特に構成・セキュリティ等は重点的に網羅し, 間違った使い方を抑止

クラウド開発ガイドライン

NTTドコモ
サービスイノベーション部
第3サービス開発担当

docomo

本ガイドラインについて

docomo

□ 対象

クラウド(特にAWS)を利用して開発を行う方

□ 本ガイドラインのカバーしている内容

- ・ クラウドの特性の解説
- ・ クラウドに開発における前提となる考え方
- ・ 開発時に必ず実施すべきことと注意点
- ・ ドコモ開発フローに沿ったクラウド利用ノウハウ



□ 本ガイドラインの利用方法

本ガイドラインはボリュームが多いため、クラウド利用時に分かっておかなければいけないことを記載しております。開発フローごとにまとめているので各フェーズに差し掛かった際に必要箇所を読むといった利用をしてください。

※本ガイドラインではクラウド利用の場合に限定して作成しており、オンプレミス利用時と共通となる考え方などは極力省いて解説しております。

Copyright © 2014 NTT DOCOMO

DOCOMO, INC. All Rights Reserved

3

考慮すべき点

- **Design for failure**

あらゆるものはいつでも故障する
前提で設計する

- **コンポーネントの疎結合化**

コンポーネントを独立させ、ブ
ラックボックス化する

- **スケーラブルな構成**

伸縮自在性があり、再起動が可能
な構成にする

- **全レイヤでのセキュリティ**

AWSとの責任分担モデルを理解
し、全てをAWSに任せない

- **並列処理の実装**

アプリケーションやバッチ処理の
並列化を検討する

- **ストレージの使い分け**

EBSやデータベース、S3などの
ストレージを使い分ける

- AWSデザインパターン（セキュリティ対策）の作成，展開
 - AWSを利用する際に必要となるセキュリティ要件を記載
 - 考慮漏れを抑制し，ドコモのセキュリティ基準に対する準拠性を高める

AWSデザインパターン ～SS対策基準対応要求仕様編～

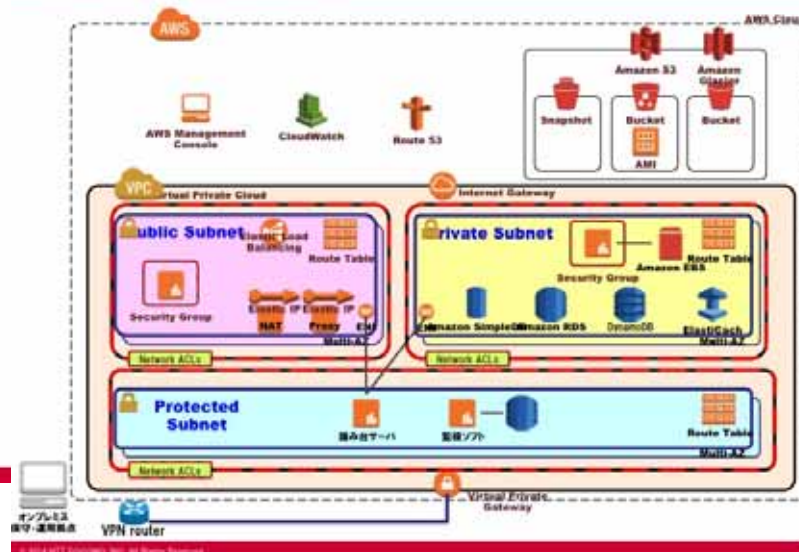
サービスイノベーション部

© 2014 NTT Docomo, Inc. All Rights Reserved.

ドコモ
docomo

構成の前提(対応コンポーネント)

docomo



© 2014 NTT Docomo, Inc. All Rights Reserved.

- セキュリティ対策を満足するテンプレート作成, 展開
 - マニュアルと共にCloud Formationのテンプレートを提供
 - デプロイのベースとして利用してもらい, 意識と実環境のずれを抑制

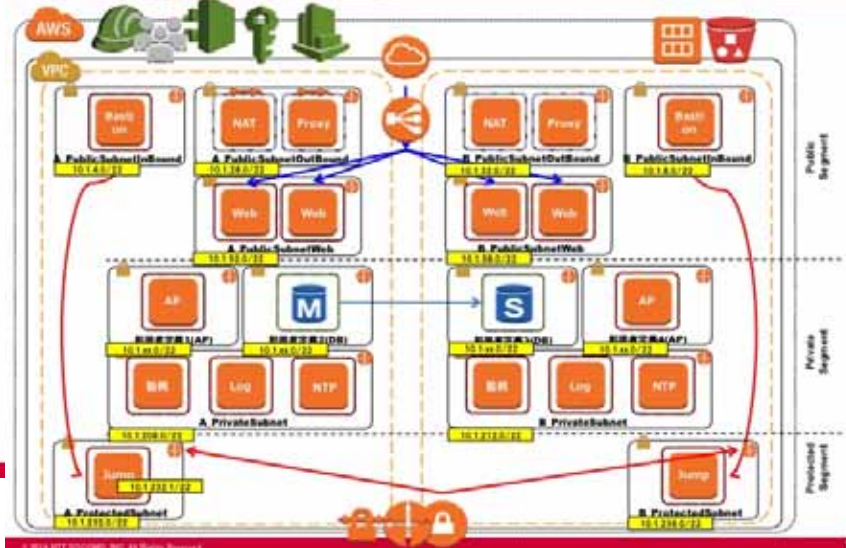
AWSデザインパターン 実装編

サービスイノベーション部
開発推進担当

NTT
docomo

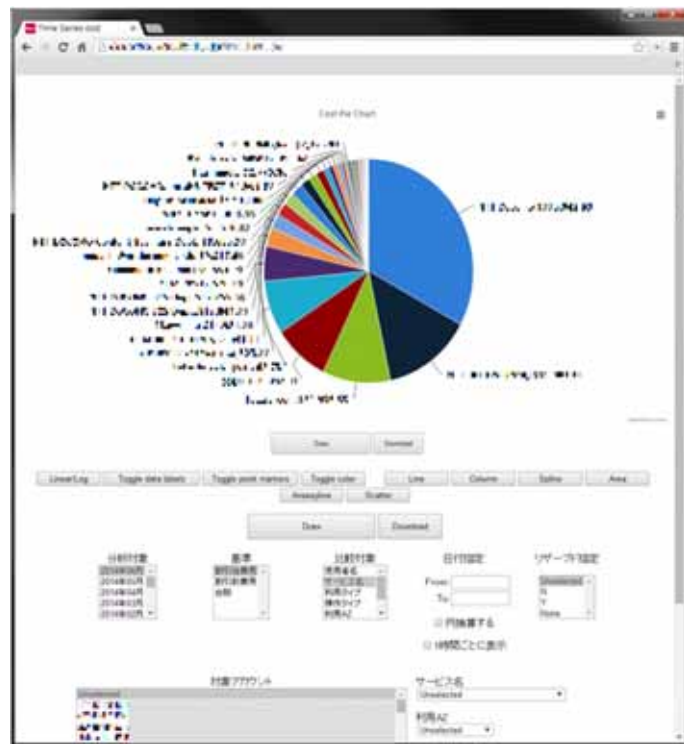
ベースとなる構成パターンイメージ

NTT
docomo



○ コスト管理ツール（Cost Visualizer）の作成，展開

➤ アカウント，サービス，日時，等に応じたコスト変遷，利用率等を表示



時系列でのコスト表示

- ・ 利用料表示
- ・ 利用台数表示
- ・ 利用アカウント別
- ・ 利用サービス別
- ・ 日付指定
- ・ 円換算 (為替反映)
- ・ 1時間毎/1日毎
- ・ リザーブド(RI)指定
- ・ 利用サービス絞込
- ・ 利用AZ絞込

表示形式

- ・ 利用アカウント別
- ・ 利用サービス別
- ・ 日付指定
- ・ 1時間/1日毎
- ・ リザーブド(RI)指定
- ・ AZ
- ・ インスタンスタイプ

RIの有効利用度表示

- ・ 有効なRI数
- ・ RI利用数
- ・ RI利用率
- ・ RI余剰数

○ 標準提供メニュー

- クラウド開発ガイドライン
- AWSセキュリティデザインパターン
- AWSセキュリティテンプレート
- etc.

○ オプションメニュー

- コンサルティング
- コスト可視化ツール

docomo cloud package

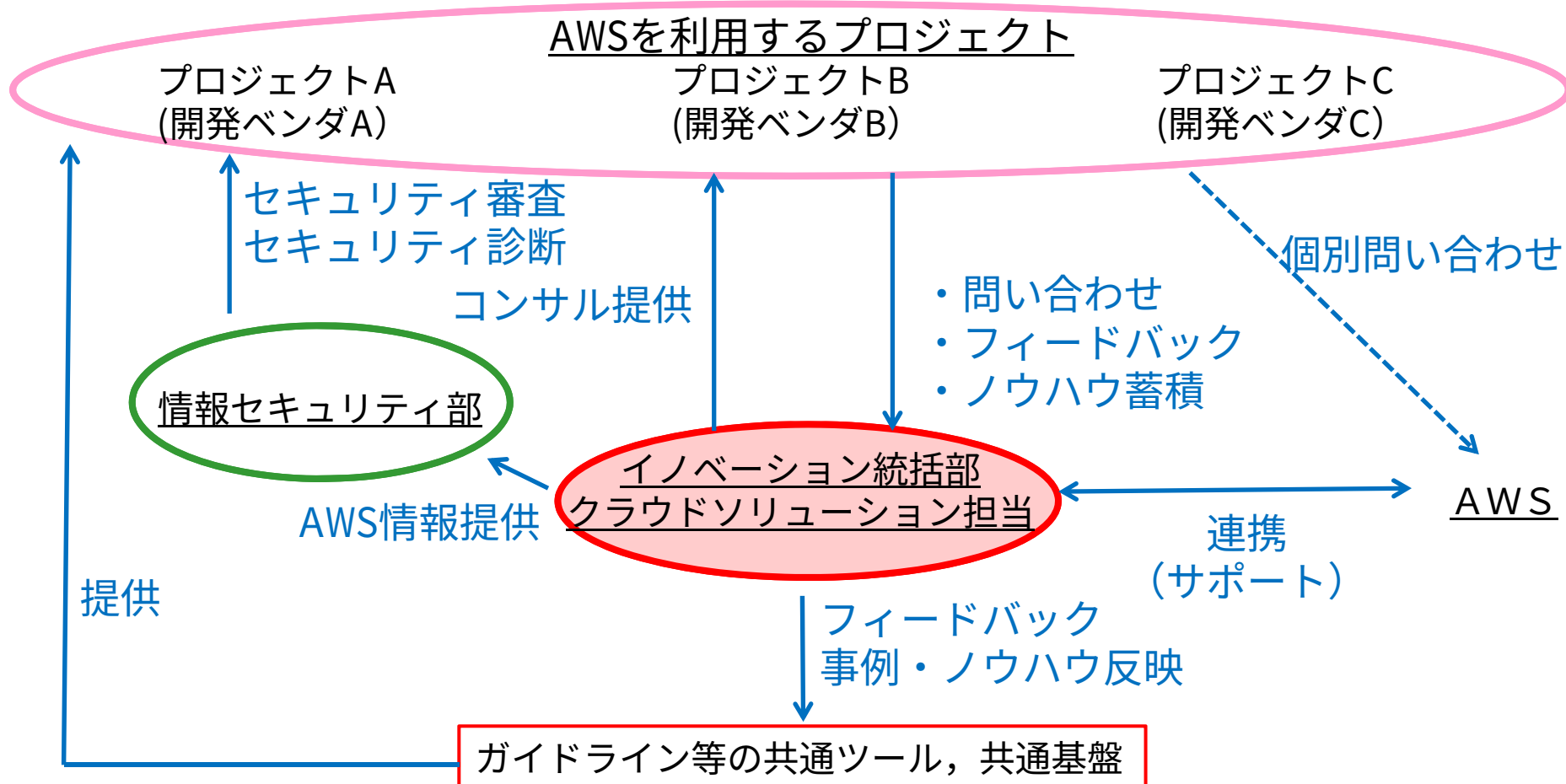
「ドコモ・クラウドパッケージ」
を利用しなかった場合



「ドコモ・クラウドパッケージ」
を利用した場合

ご興味があれば以下にメールしてください

dcm-cloudconsulting-ml@nttdocomo.com



- サービス開始はゴールでなくスタート
 - 運用の中で改善（コスト， リソース， 構成）することが大事
 - ✓ むしろ最初はリソースはアバウトに設定して， 後から最適化する
 - AWSの新機能提供， 関連する法律の変更， 等， 自社以外の要因も多い
- 開発・運用ベンダさんとの関係
 - 後から改善することを前提にして選定する
 - システム開発や運用を丸投げしたとしても， 全ては投げない
 - ✓ 最悪でもマスターアカウントやIAM設計はドコモで管理
 - ✓ コストコントロールの必要性
 - ✓ サービス主管部門で対応できない場合は代理で管理
- ガバナンス
 - 強制はしない， Give&Takeを基本に
 - 情報収集等のクロスアカウント設定はテンプレート/マニュアル化

○ 過去のセキュリティ対策基準

- 「クラウドを含む第三者提供サービス（ドコモが物理的に保有しないシステム）には個人情報を含むデータの保管は禁止」という規則があった

○ セキュリティ評価を踏まえての対策基準

- 「個人情報を含むデータの保管は禁止」ではなくなったが、クラウドである必然性が必要であり、あくまでオンプレ>クラウドの位置付け

○ その後の運用・監査を踏まえての対策基準

- オンプレであれクラウドであれセキュリティ基準に準拠できるのであればデータの保管場所は問わない

○ 時間を要したが情報セキュリティ部を含む社内意識が変化

- 最近は（適切に対策すれば）クラウド>オンプレのケースも

○ AWS環境の基本的なチェックを実施してくれるツール



➤ 以下のセキュリティチェック結果を表示（一部はサポートプラン依存）

- ✓ Security GroupのRuleチェック
- ✓ AWSアカウントのMFA利用チェック
- ✓ IAMの利用チェック, Password Policyチェック
- ✓ S3のBucket Policyチェック
- ✓ CloudTrail利用確認
- ✓ Route 53のRecordチェック
- ✓ RDSのSecurity Groupチェック
- ✓ ELB Security Group, Listener Securityチェック

○ NTTドコモのAWS利用

- しゃべってコンシェル
- データ分析システム
- docomo Developer support
- 利用・運用状況のご紹介

○ AWSセキュリティ対策

- 社内セキュリティ対策基準
- 具体的なセキュリティ対策事例
- 社内体制とガバナンス

docomo cloud package

クラウドのシステムは作ることより作ってからが勝負です！



docomo cloud package

連絡先

森谷 優貴 (Yuki Moritani)

moritaniy@nttdocomo.com

dcm-cloudconsulting-ml@nttdocomo.com