

2018年2月21日

PC・ネットワークの管理・活用を考える会

ITトレンド勉強会@東京

テーマ：

クラウド移行時に心配なセキュリティ対策



クラウドの進化と真価 メガバンクがクラウドに移行する背景

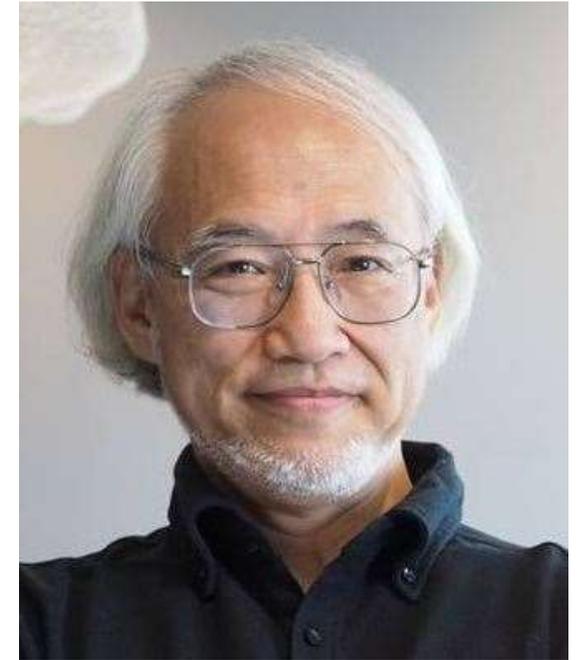
一般社団法人 クラウド利用促進機構 運営委員

渥美 俊英

自己紹介

渥美 俊英 (あつみ としひで)

一般社団法人 クラウド利用促進機構 運営委員(CUPA)
クラウドセキュリティアライアンス日本支部 副会長(CSAJ)
特定非営利活動法人 日本セキュリティ監査協会(JASA)
JASA-クラウドセキュリティ推進協議会 アドバイザー



- 2010年黎明期からクラウドによるIT業界変革の活動をしています。
- 元：AWSJ エンタープライズエバンジェリスト、その前はISID
- 今：ユーザ企業、ITベンダ数社の非常勤顧問、アドバイザー
- 役割：クラウドの業界動向、セキュリティ、統制の講演、案件支援

関心事は、ITの民主化、組織変革、人材教育、最新動向

経歴

- 1983年 電通国際情報サービス(ISID)入社
GE + 電通の合併、RCS(遠隔コンピュータ利用)、元祖クラウド！？
- 80年代：銀行、証券の国際間システム開発、Fortran言語
- 90年代：オープンシステム、WindowsNT、Java金融適用
 - ✓ 日本興業銀行 国際CMS(WindowsNT、SSL128bit日本初)
 - ✓ 東京三菱銀行 インターネットバンキング(Java日本初)
 - ✓ 三和銀行 アイデントラス(世界大手銀行間B2B電子認証基盤)
 - ✓ 東京三菱銀行 アカウントアグリゲーションサービス(今でいうFintech)
- 2000年代：ISID技術統括、OSS、CMMI、セキュリティ出荷判定
- 2010年頃から、クラウドに着目、以来、クラウドエバンジェリスト

経歴

- 2011年 ISIDがAWSパートナーシップ認定、MS、Googleとも協業
- 2012年 FISC対応AWSセキュリティリファレンス策定コアメンバ
- 2013年 経産省クラウドセキュリティガイドライン活用ガイド策定メンバ
- 2015年 Azure FISC対応セキュリティリファレンス策定支援、MS MVP認定

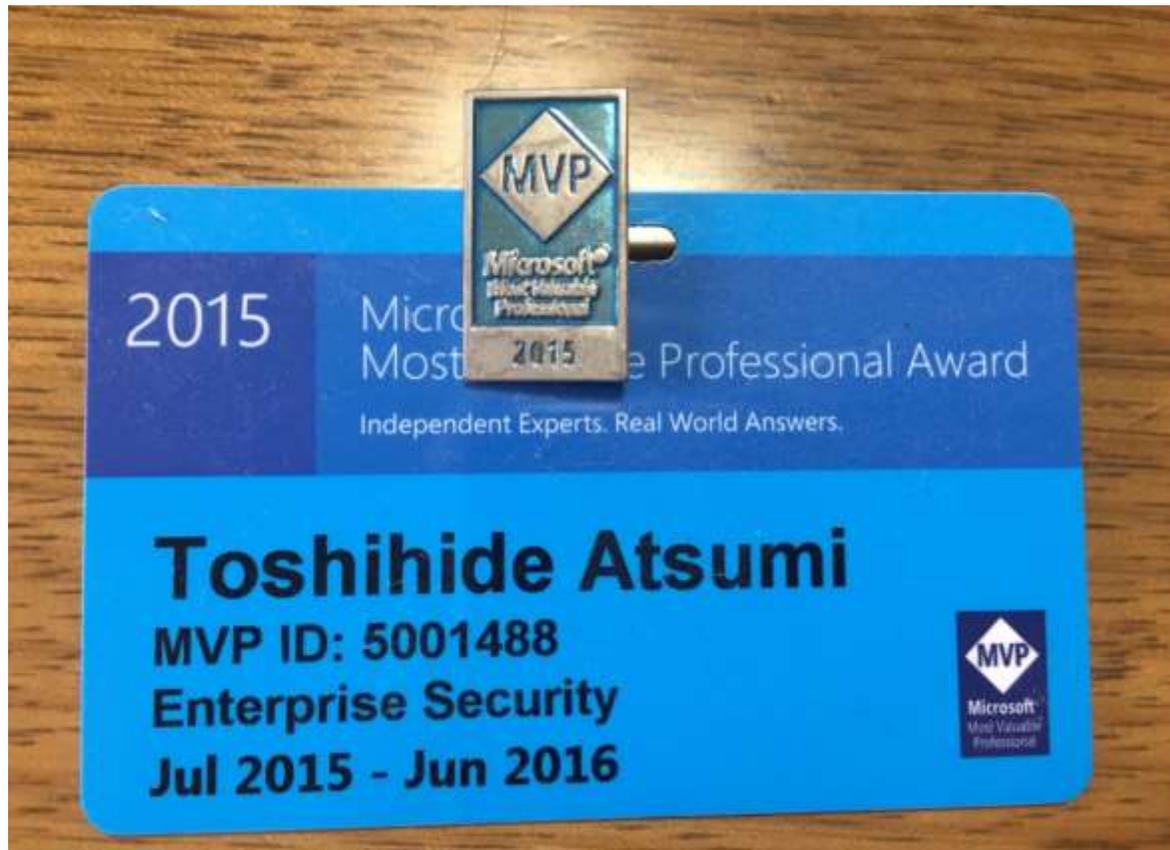
- 2015年6月 ISID定年退職、7月からAWSジャパン入社
エンタープライズエバンジェリストとして1年余り活動、講演、サポート
- 退職後も変わらずクラウド推進活動、業界団体、ユーザ会、個社向けの講演
- 半分は、勉強、 세미나、コミュニティ参加、資格取得など
- 半分は、いくつかのクラウド利用企業、開発パートナーの顧問・アドバイザー

クラウド利用推進のお手伝い、クラウドを使う側の変革に注力

自己紹介

Microsoft MVP取得！

➤ Enterprise Security (2015)



今日、お伝えしたいこと

- クラウドの進化と真価 ～インフラを越えるもの
- クラウドのセキュリティと統制、メガバンクの利用
- AWSはかつてない異形のITベンダ
- re:Invent が毎年IT業界を揺り動かす

AWSの市場シェア 44%

売上ほぼ50%の伸び、2017年度は推定180億\$(2兆円)



AWS re:Invent 2017 基調講演より (市場成長率は講師追記)

- 市場成長率を越えるクラウドベンダは上位片手の数社。
- Forrester予測：Amazon、Microsoft、Googleの3社で、2018年76%、2020年80%。
- 世界のクラウド市場の資源の大半は、数年のうちに片手に満たない上位数社が寡占。

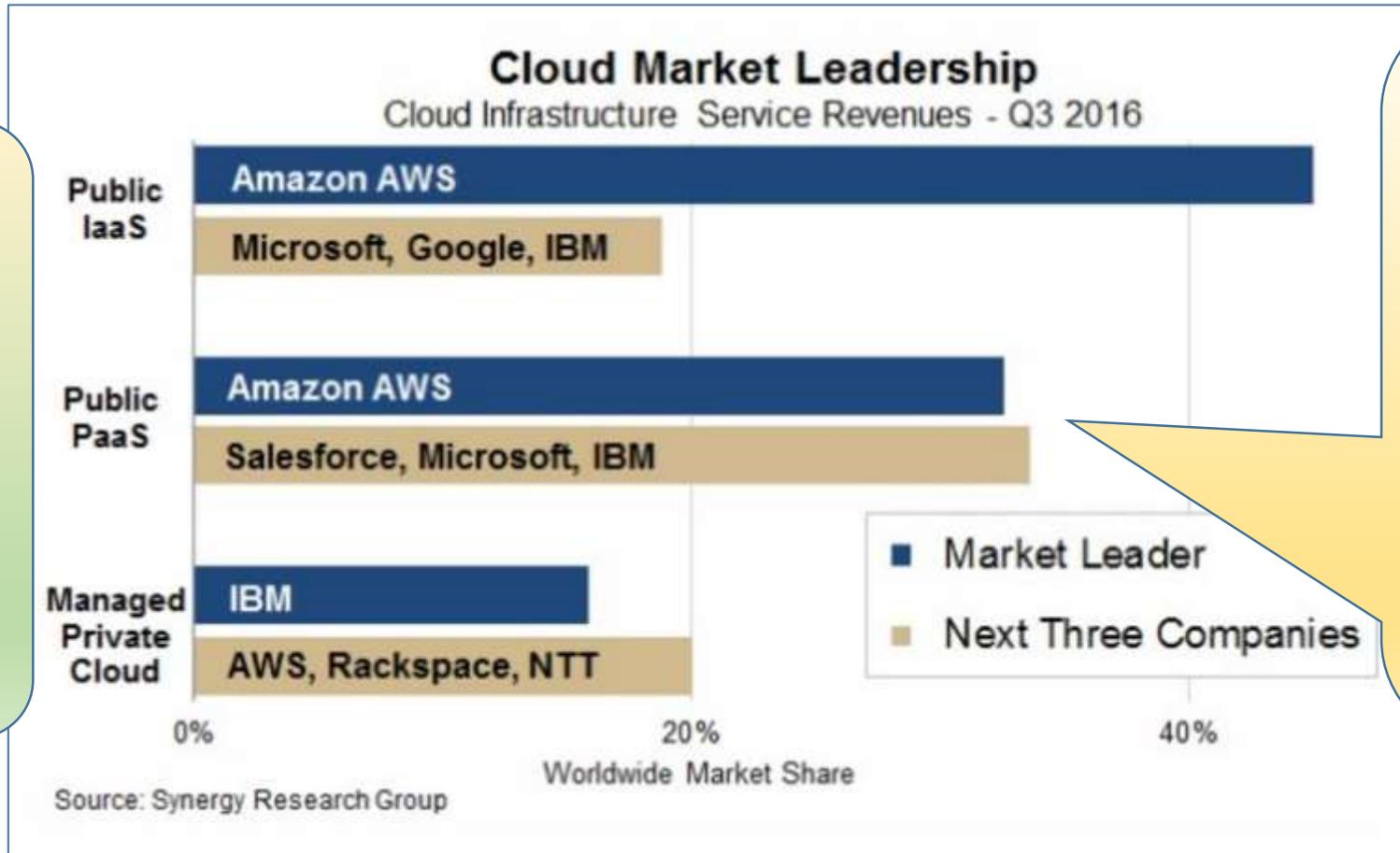
IaaS/PaaS市場の動向

パブリッククラウド IaaS市場の45%、MS,Google,IBM3社計を上回る
実は、PaaS市場でも、他3社合計に並ぶ

IaaS
インフラ

PaaS
開発ミドル

SaaS
アプリケーション



AWS=IaaSは
大きな見誤り

クラウドの価値は
システム開発生産性

さらに言えば
組織、ビジネス変革
より安全な仕組み

AWSの機能拡張・改善のスピード

1300以上

2017年は、1300を超える数

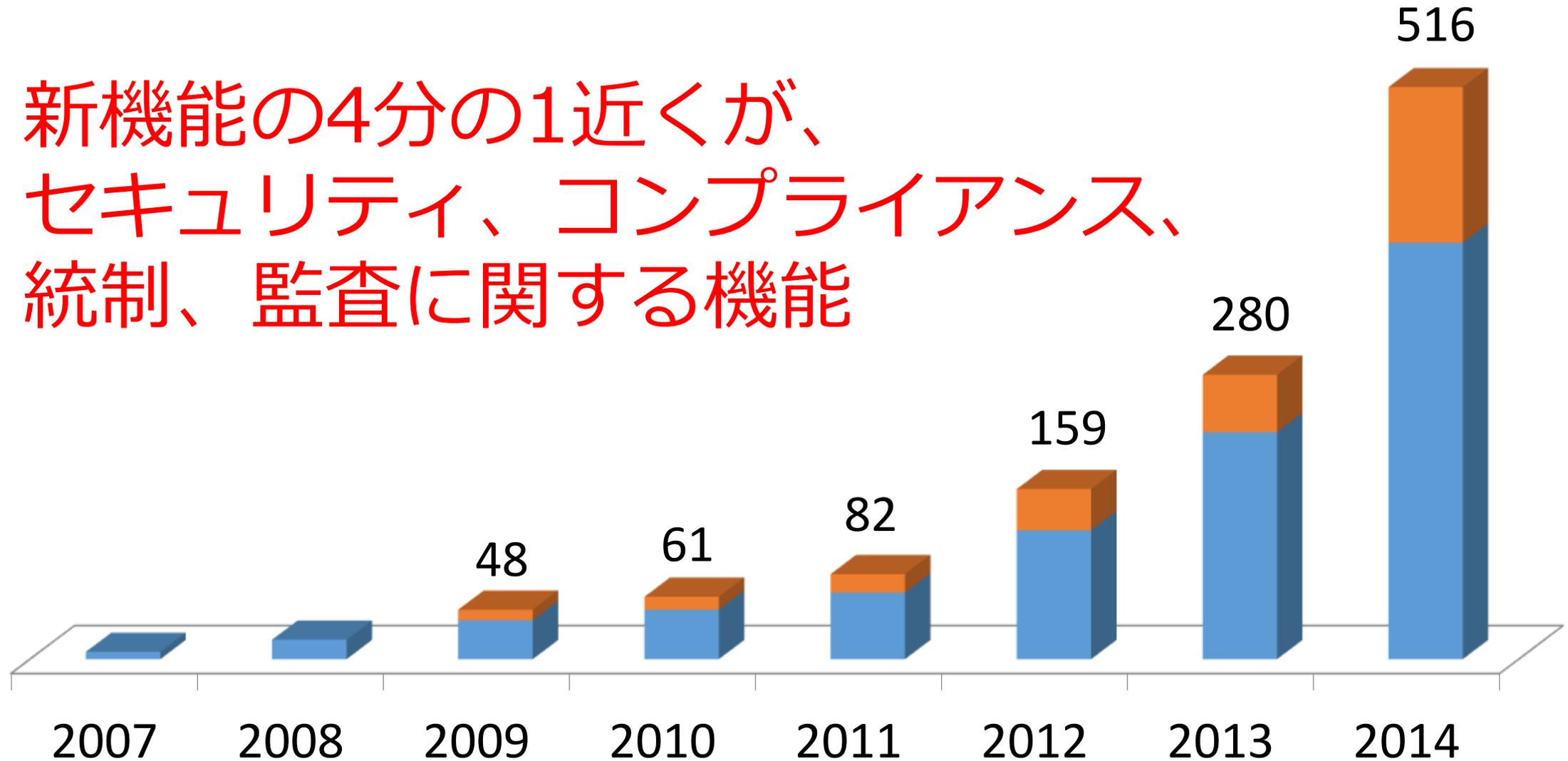
イノベーションが急加速

続々と新しい上位サービス
オンプレミスの代替から
クラウドならではの価値を提供



AWSの機能拡張・もう1つのポイント

新機能の4分の1近くが、
セキュリティ、コンプライアンス、
統制、監査に関する機能



IT市場の将来を読む：

2017年 世界の企業の研究開発投資額順位（1億\$） アマゾン1.7兆円

順位	社名	変化	国	業種	R&D	売上高	※
1	アマゾン	↑	米	ソフトウェア・インターネット	161	1,360	★
2	グーグル	↑	米	ソフトウェア・インターネット	139	903	★
3	インテル	↑	米	コンピュータ・エレクトロニクス	127	594	★
4	サムスン	↓	韓	コンピュータ・エレクトロニクス	127	1,677	★
5	フォルクスワーゲン	↓	独	自動車	121	2,294	—
6	マイクロソフト	→	米	ソフトウェア・インターネット	120	853	★
7	ロシエ	→	ス	医薬・ヘルスケア	114	518	—
8	メルク	↑	独	医薬・ヘルスケア	101	398	—
9	アップル	↑	米	コンピュータ・エレクトロニクス	100	2,156	★
10	ノバルティス	↓	ス	医薬・ヘルスケア	96	494	—

Strategy&社調査

- ・ ★印は、クラウド、インターネット、スマホ、ソフトウェアを主事業とする企業
- ・ 製造業上位は、トヨタ11位、GE13位、ダイムラー15位、ホンダ19位
- ・ IT、インターネットでは、オラクル17位、シスコ18位、Facebook20位、IBM22位

IT市場の将来を読む：

6年前、2011年 世界の企業の研究開発投資額順位 (1億\$)

順位	社名	国	業種	R&D
1	メルク	独	医薬・ヘルスケア	110
2	ロシエ	ス	医薬・ヘルスケア	99
3	ファイザー	米	医薬・ヘルスケア	94
4	ノバルティス	ス	医薬・ヘルスケア	91
5	マイクロソフト	米	ソフトウェア・インターネット	87
6	サムソン	韓	コンピュータ・エレクトロニクス	77
7	フォルクスワーゲン	独	自動車	72
8	ジョンソン&ジョンソン	独	医薬・ヘルスケア	68
9	インテル	米	コンピュータ・エレクトロニクス	66
10	トヨタ	日	自動車	66
11	ノキア	フ	コンピュータ・エレクトロニクス	62
12	IBM	米	コンピュータ・エレクトロニクス	60

Strategy&社調査

- 上位の業種は、医薬・ヘルスケア、携帯 ⇒ クラウド、スマホ、ソフトウェアへ
- 主流は、ハードウェア・製造業 ⇒ ソフトウェア・システム開発へ

IT市場の将来を読む：

世界の企業の時価総額順位（1億\$） [2018年1月]

順位	社名	変化	国	業種	時価総額	※
1	アップル	→	米	コンピュータ・エレクトロニクス	8,596	★
2	グーグル	→	米	ソフトウェア・インターネット	8,171	★
3	マイクロソフト	→	米	ソフトウェア・インターネット	7,315	★
4	アマゾン	→	米	ソフトウェア・インターネット	6,991	★
5	テンセント	↑	中	ソフトウェア・インターネット	5,580	★
6	フェイスブック	↓	米	ソフトウェア・インターネット	5,430	★
7	バークシャー・ハサウェイ	→	米	投資ファンド	5,302	—
8	アリババ	→	中	ソフトウェア・インターネット	5,167	★
9	中国工商銀行	↑	中	金融	4,251	—
10	JPモルガン・チェース	→	米	金融	4,013	—

- ・ 11～20位は、金融4社、石油2社、医薬・製造・流通・食品各1社
- ・ ★印は、クラウド、インターネット、スマホ、ソフトウェアを主事業とする企業

**伸び続ける市場と株価、巨大化・寡占化、潤沢な資金、優れた人材
ソフトウェア+クラウドで規模と競争が拡大し続けるのは不可避、不可逆**

AWSクラウドはインフラ？

100以上のAWSサービス群

お客様のアプリケーション

ライブラリ & SDKs
Java, PHP,
.NET,
Python, Ruby

管理インター
フェイス
Management
Console, CLI

認証とログ
IAM, Cloud Trail,
Cloud HSM,
Config

ディレクトリ
Directory
Service

モ
Cloud
Tru

と自動化
Elastic
Beanstalk,
Data
Formation,
Elastic
Works



エンタープライズアプリケーション
WorkSpaces, WorkDocs, WorkMail



データベース
RDS, DynamoDB,
Redshift, ElastiCache



アプリケーション
CodeCommit, CodeBuild, CodeDeploy, CodePipeline



コンピュー処理
EC2, Auto Scaling, Lambda
Elastic Load Balancing,
EC2 Container Service



ストレージ
EBS, S3, Glacier, Storage
Gateway



コンテンツ配信
CloudFront



ネットワーク
VPC, Route 53, Direct Connect

従来のインフラ
サーバー
ストレージ
ネットワーク
データセンター



グローバルインフラ
リージョン、アベイラビリティゾーン、エッジロケーション



100以上のAWSサービス群

お客様のアプリケーション

ライブラリ & SDKs
Java, PHP, .NET, Python, Ruby

管理インターフェイス
Management Console, CLI

認証とログ
IAM, Cloud Trail, Cloud HSM, Config

ディレクトリ
Directory Service

モニタリング
Cloud Watch, Trusted Advisor

コード管理
CodeDeploy, CodeCommit, CodePipeline

デプロイと自動化
Elastic Beanstalk, Cloud Formation, OpsWorks

エンタープライズアプリケーション
WorkSpaces, WorkDocs, WorkMail

モバイルサービス
Mobile Analytics, Cognito, SNS

データベース
RDS, DynamoDB, Redshift, ElastiCache

アプリケーションサービス
AppStream, Cloud Search, SWF, SQS, SES,

データ分析
Quick Sight, Athena, Kinesis, Data Pipeline

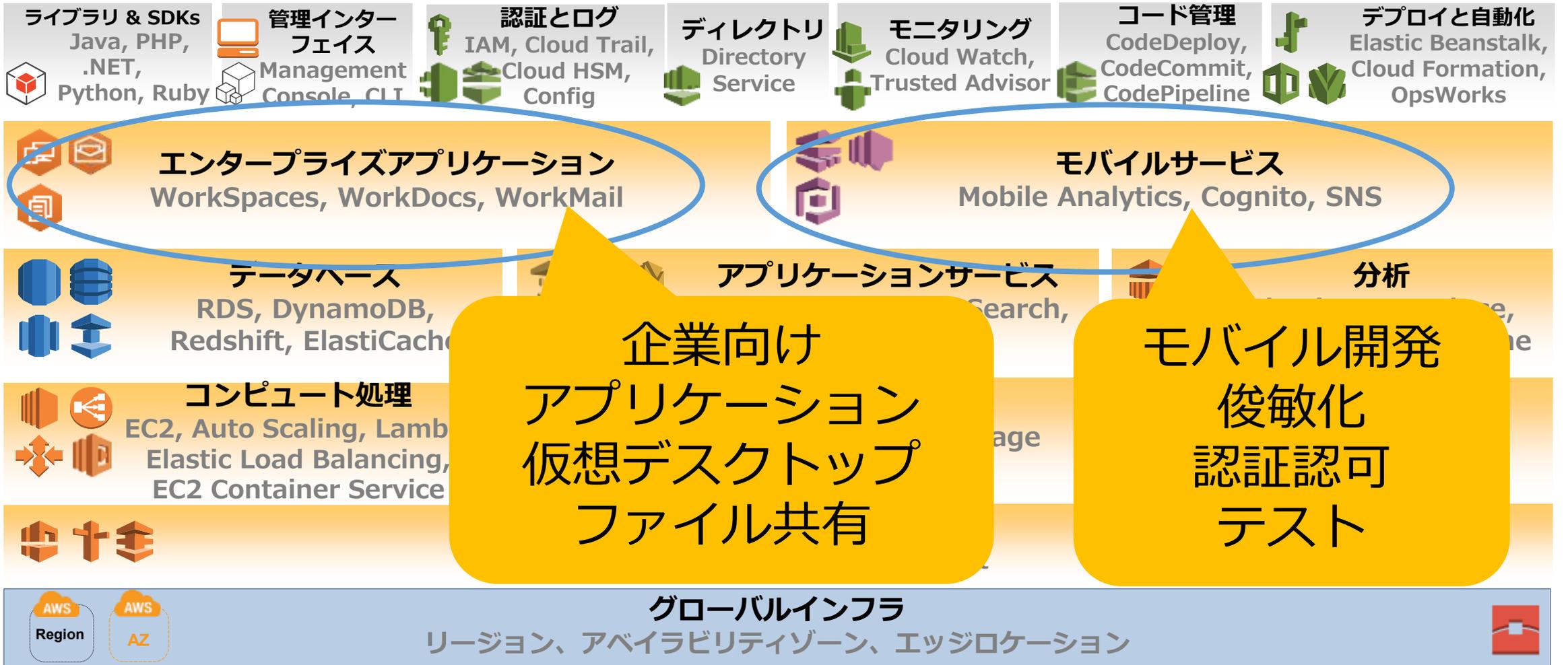
RDB, NonSQL, DWH
DBマネージドサービス
バックアップ/リカバリ
自動化

アプリ開発支援
検索、メッセージ、
キューイング、
ストリーミング

BigData BI
SQLクエリ
ストリーム処理
データフロー

100以上のAWSサービス群

お客様のアプリケーション



100以上のAWSサービス群

お客様のアプリケーション

ライブラリ & SDKs
Java, PHP,
.NET,
Python, Ruby

管理インター
フェイス
Management
Console, CLI

認証とログ
IAM, Cloud Trail,
Cloud HSM,
Config

ディレクトリ
Directory
Service

モニタリング
Cloud Watch
Trusted Advisor

コード管理
CodeDeploy,
CodeCommit,
CodePipeline

デプロイと自動化
Elastic Beanstalk,
Cloud Formation,
OpsWorks

APIの充実
ライブラリ/SDK
管理コンソール
コマンドIF

統一的権限管理
全てのロギング
構成管理
暗号化、鍵管理
ディレクトリ

リソース監視
ログ監視
構成変更監視
設定評価
アドバイス

コード管理
リポジトリ
ビルド, テスト
配備自動化
DevOps

エンタープライズアプリケーション

ビルドサービス

Elastic Load Balancing
EC2 Container Service

ネットワーク
VPC, Route 53, Direct Connect

グローバルインフラ

リージョン、アベイラビリティゾーン、エッジロケーション

AWSサミットで語られたこと



Enterprise Day

野村総合研究所 楠理事

三菱東京UFJ銀行 村林専務

NTTドコモ 栄藤執行役員

日本経済新聞社 渡辺執行役員



「クラウドは安いからではなく
企業文化を変えるために使う」

- 既存システム載替でコスト削減、+イノベーションの基盤(MUFG)
- とにかく使ってみる、開発のスタイルを変えられる (NTTドコモ)
- 従来メディアは生き残りをかけてクラウドで先鋭化する (日経新聞)
- マイクロサービス、サーバーレスでクラウドネイティブで内製開発

先進企業が語るAWSの価値

Enterprise Day Executive Track (大手企業トップ向け限定)

◆KDDI様

「KDDIの新規事業“auでんき”をクラウドスピードでサービスイン」
AWSの環境構築をコード化、柔軟に変更、システム開発を高速化

◆ジャパンネット銀行様

「ジャパンネット銀行におけるクラウド活用への取り組み」
金融機関もコスト削減、一般業務をクラウド化、新サービスに注力

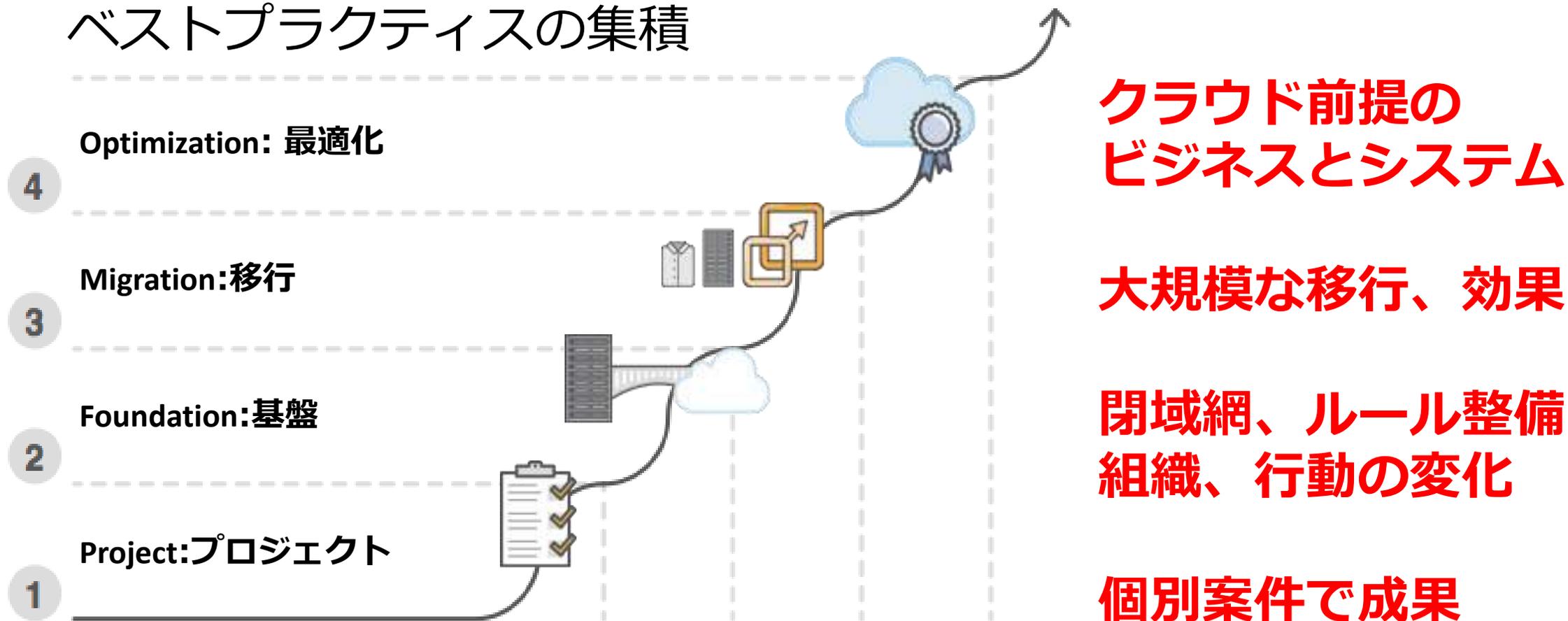
◆キヤノン様

「AWSがもたらす開発部門の変革について」
マネージドサービスを活用、アプリに集中、システム開発を高速化

システム開発のコアに注力、俊敏化 → クラウドの価値

クラウドジャーニー：クラウドならではの進化

ベストプラクティスの集積



日本でも2～3年余りの全面移行を経て、最適化段階のユーザが続々と。ローソン、協和発酵キリン、東急ハンズ、旭硝子、スシロー、大創など。

ユーザが語るクラウドの価値

- X オンプレの安い早い代替え
- システム開発、運用全般に及ぶ機能と価値
- 開発のスタイル、組織の在り方に及ぶ
- 金融機関も高いセキュリティと統制を評価
- IaaS上位のマネージドサービス活用がカギ

ソフトウェア重視、使いこなす技術が求められる

今日、お伝えしたいこと

- クラウドの進化と真価 ～インフラを越えるもの
- メガバンクの利用、クラウドのセキュリティと統制
- AWSはかつてない異形のITベンダ
- re:Invent が毎年IT業界を揺り動かす

メガバンクが本格的にAWS採用へ

三菱UFJがパブリッククラウド「AWS」採用、国内メガバンクで初

高槻 芳 = 日経コンピュータ

2017/01/23

日経コンピュータ

目次一覧

シェア 405 共有 7 B!ブックマーク 37 Pocket ツイート 保存する

三菱UFJフィナンシャル・グループ（MUFG）が、社内システムの一部をパブリッククラウドサービスのAmazon Web Services（AWS）上に刷新すると決めたことが2017年1月23日に分かった。5年で100億円規模のコストを削減するのに加えて、システム構築の期間を短縮し、フィンテック分野などで重要性が増している迅速なシステム開発を実現する。

文字通り “クラウドファースト”

<http://itpro.nikkeibp.co.jp/atcl/news/17/012300193/>

<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/022400847/>

三菱UFJ、勘定系システムのAWS移行も

矢口 竜太郎 = 日経ITインベーターズ 兼 日経コンピュータ

2017/02/24

日経ITインベーターズ

目次一覧

シェア 937 共有 5 B!ブックマーク 78 Pocket ツイート 保存する

「Amazon Web Services（AWS）に移行するシステムに“聖域”はない。現時点では計画していないものの、勘定系システムをクラウド化する可能性は十分にある」。三菱東京UFJ銀行の執行役員である亀田浩樹システム本部長兼システム企画部長（写真）は日経BP社の取材に対してこう話した。

三菱UFJフィナンシャル・グループ（MUFG）は2017年1月、AWSを本格的に採用する方針を公表した。メガバンクで初めてのAWS採用宣言に、国内IT業界の注目の的になっていた。



写真1 ● 三菱東京UFJ銀行の亀田浩樹執行役員システム本部長兼システム企画部長

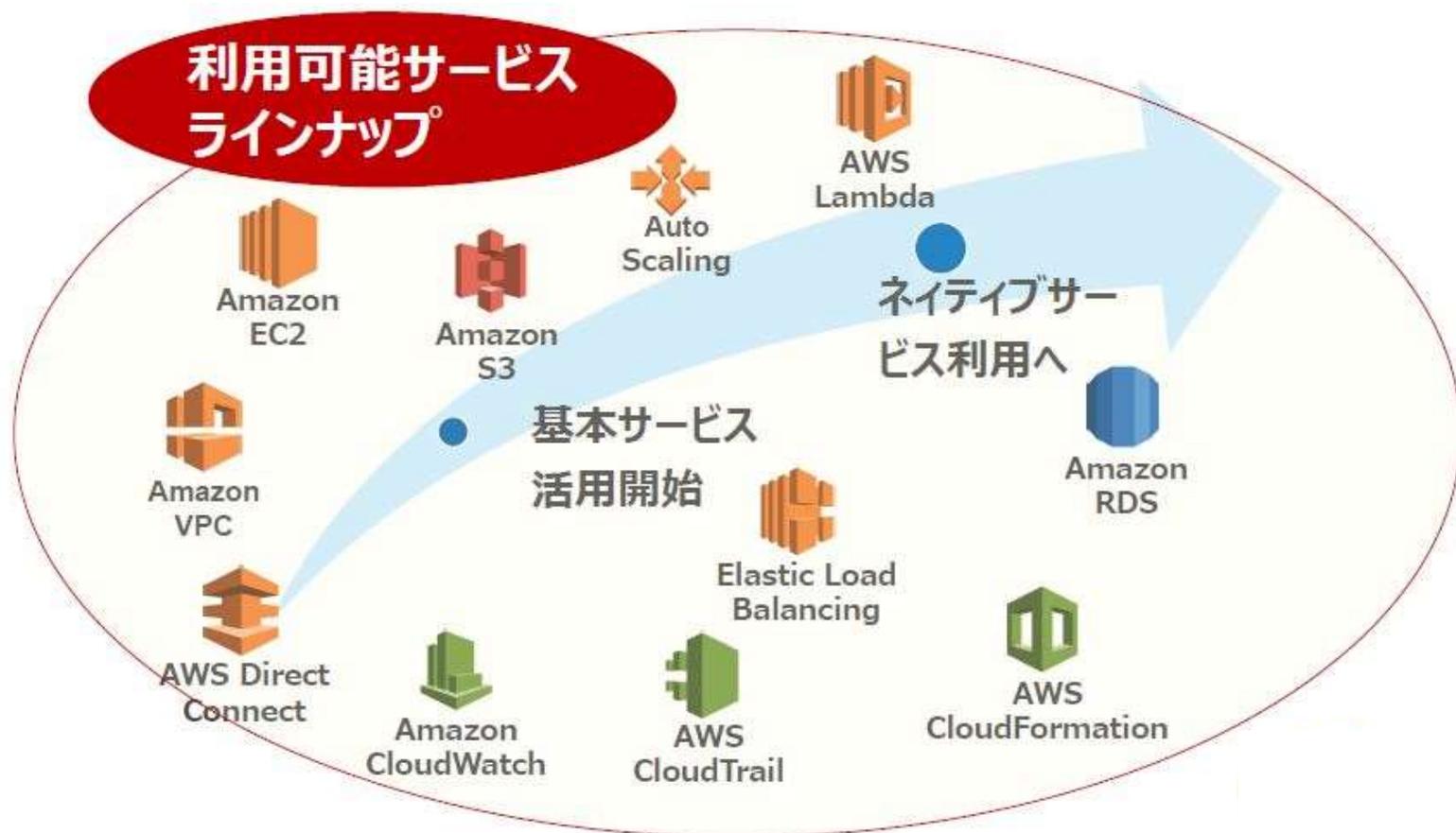
記事に記されていること

- 社内システムをAWS上に刷新、5年で100億円のコスト削減
 - ・ハード、共通基盤活用による設計も費用低減
 - ・フィンテック分野などで迅速なシステム開発
 - ・従来4か月かかった基盤構築を1か月で行う
 - ・グループ共通のシステム基盤とする
- 共通のクラウド基盤として利用に向けて組織的取組み
 - ・既にグループのIT部署 数百人に対してAWS研修を実施

**三菱UFJのAWS大規模採用を契機にクラウド
人材不足はもっと深刻になる**

AWSサミット2017 村林常務基調講演

- 全行共有基盤
- 基本機能サービス
- ネイティブサービス
- セキュリティ共通
- ログと監視
- 構成配備自動化



AWSサミット2017 公開資料

<https://aws.amazon.com/jp/summit2017-report/details/>

クラウドが金融/IT業界を変えている

ソニー銀行、ジャパンネット銀行に続き、MUFGも情報公開
メガバンクの役員がAWS用語で講演する時代
イベント講演ではクラウド独特の言葉が一般化

Info EXPO 2017速報

「どんなシステムもAWSで動かさないかを検討する」、MUFGの亀田氏

日川 圭三 -ライター 2017/10/12

Show 483 | ブックマーク | Pocket | ツイート | 保存する

「勘定系ではオンプレミス環境のメインフレームに一日の長があるが、新規システムのプロジェクトを始める際には、クラウドファーストであることを義務付けた。どのようなシステムであっても、まずはアマゾンウェブサービス（AWS）の上で動かすことを第一に検討することになっている」。



IV クラウドの活用 - サービス視点で

- VPC内サービス「インフラストラクチャサービス」「コンテナサービス」より活用開始。
- 「抽象化サービス」は、エンドポイント機能を有するサービスを中心に利用するが、エンドポイント機能の無い「抽象化サービス」の利用は現時点では限定的に。（セキュリティ観点）
- 各サービスは、機能・セキュリティ等の確認プロセスを経て、社内で共通サービス化。
- 金融コア業務に適用範囲を拡大するには、セキュリティ面を中心にサービスの進化は必須。エンドポイント機能の対象サービス拡大、新サービスの日本国内リリース早期化など、AWS社には継続的に要請中。



VPC内 (一部開発検討中も含む)

インフラストラクチャサービス: Amazon EC2, Amazon VPC, Amazon EBS

コンテナサービス: Amazon RDS, AWS Lambda, Amazon Redshift, Amazon EMR

VPC外 (一部開発検討中も含む)

抽象化サービス: Amazon S3, Amazon Glacier, Amazon API Gateway, Amazon CloudFront

Copyright © 2017 Mitsubishi UFJ Financial Group, Inc. All rights reserved. MUFG

2017 8.28

週刊金融財政事情

Financial Affairs

特集

どこまで進むかクラウド活用

新たなステージに突入した銀行システム

金融機関で活用が進むアマゾンのクラウドサービス

業務の最適化を図るうえでクラウド活用は不可欠

クラウドサービスの安全対策とリスク管理の考え方

これからの銀行システムに求められる課題と方向性

米債務上限問題、市場の読みは「押し目買いのチャンス」

AWSのセキュリティ、統制

- セキュリティはAWSにおいて最優先されるべき事項
テクノロジー、専門組織、プロセスに継続的に投資
- セキュリティと統制の要求が厳しい企業、組織の要求を個別にではなく、ソフトウェアで対応、サービス化



- これを全てのユーザーに安価に提供、利用料に込み

主要な認証/標準に準拠

SSAE 16/ISAE 3402、SOC1(旧SAS70)、SOC2、SOC3 監査報告書
ISO 27001、ISO 27017、ISO 27018、ISO 9001、PCI DSS Level 1
FISMA moderate、FedRAMP、HIPPA、ITAR、DoD(国防総省暫定認証) 等



SOC2監査報告書とは？



- 米国会計士協会(AICPA)の基準による保証型監査報告の制度
- SOC2は財務報告向け(旧SAS70)からクラウドに特化した基準
- 重要な統制項目を、専門の監査人が実地で確認した監査報告書
- 半年毎に、繰り返し、継続的に、監査を現地で実施
- AWSユーザは、NDA締結によりSOC2を受領可能
- サマリーを記したSOC3は一般公開されています

★ AWSの東京リージョンは、SOC2の対象

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

AWSのコンプライアンス公開情報

AWSセキュリティ監査のガイドライン ベストプラクティス

AWS セキュリティ監査のガイドライン

セキュリティ設定を定期的に監査し、現在のビジネスのニーズに対応していることを確認する必要があります。監査では、不要な IAM ユーザー、ロール、グループ、およびポリシー、IAM ユーザーグループ、および IAM ポリシーに対して必要なアクセス権限だけを与えるようにすることができ

以下では、セキュリティのベストプラクティスを実践するために、AWS リソースの監査を行うためのガイドラインを示します。

トピック

- いつセキュリティ監査を行うか
- 監査のための一般的なガイドライン
- AWS アカウントの確認 認証情報
- IAM ユーザーの確認
- IAM グループの確認
- IAM ロールの確認
- SAML 用 IAM プロバイダおよび OpenID Connect (OIDC) 用 IAM プロバイダの確認
- モバイルアプリの確認
- Amazon EC2 セキュリティ設定の確認
- 他のサービスの AWS ポリシーの確認

クリック

AWS コンプライアンス

<https://aws.amazon.com/jp/compliance/>

監査のための一般的なガイドライン

アカウントのセキュリティ設定を確認する際は、以下のガイドラインに従います。

- 徹底して行う。定期的には使用しないものを含め、セキュリティ設定のあらゆる面について調べます。
- 推測しない。セキュリティ設定のある面 (例: 特定のポリシーやロールの存在の背後にある根拠) が良くわからない場合、満足するまでビジネスニーズを調査します。
- 作業を単純にする。監査(および管理)を容易にするために、IAM グループ、一貫した命名スキーム、単純なポリシーを使用します。

AWS アカウントの確認 認証情報

AWS アカウント認証情報を監査するときは、次の手順に従います。

1. アカウントのルートアクセスキーを使用していない場合は、**削除**しますAWS での日常作業には、ルートアクセスキーを使用するのではなく、IAM ユーザーを作成することを**強く推奨**します。
2. アカウントのアクセスキーを保持する必要がある場合は、**定期的**に**更新**します。

IAM ユーザーの確認

AWS 責任共有モデル

お客様

お客様自身で
クラウドを
コントロール可能



お客様のアプリケーション・コンテンツ

ネットワーク
セキュリティ

サーバー
(OS)
セキュリティ

データ
セキュリティ

アクセス
コントロール

お客様はこの部分の
統制に関して

AWSにおまかせ
することが可能

AWS 基本サービス

コンピューート

ストレージ

データベース

ネットワーク

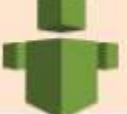
AWS
グローバル
インフラストラクチャ

アベイラビリティゾーン

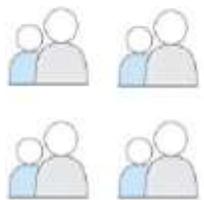
リージョン

エッジ
ロケーション

セキュリティと統制を強化するサービス群

Service	Type
 CloudTrail	APIログの取得
 CloudWatch	リソース・ログ監視
 AWS Config	変更管理・継続評価
 Inspector	オンデマンドの評価
 Trusted Advisor	定期的な評価

AWS Security and Compliance

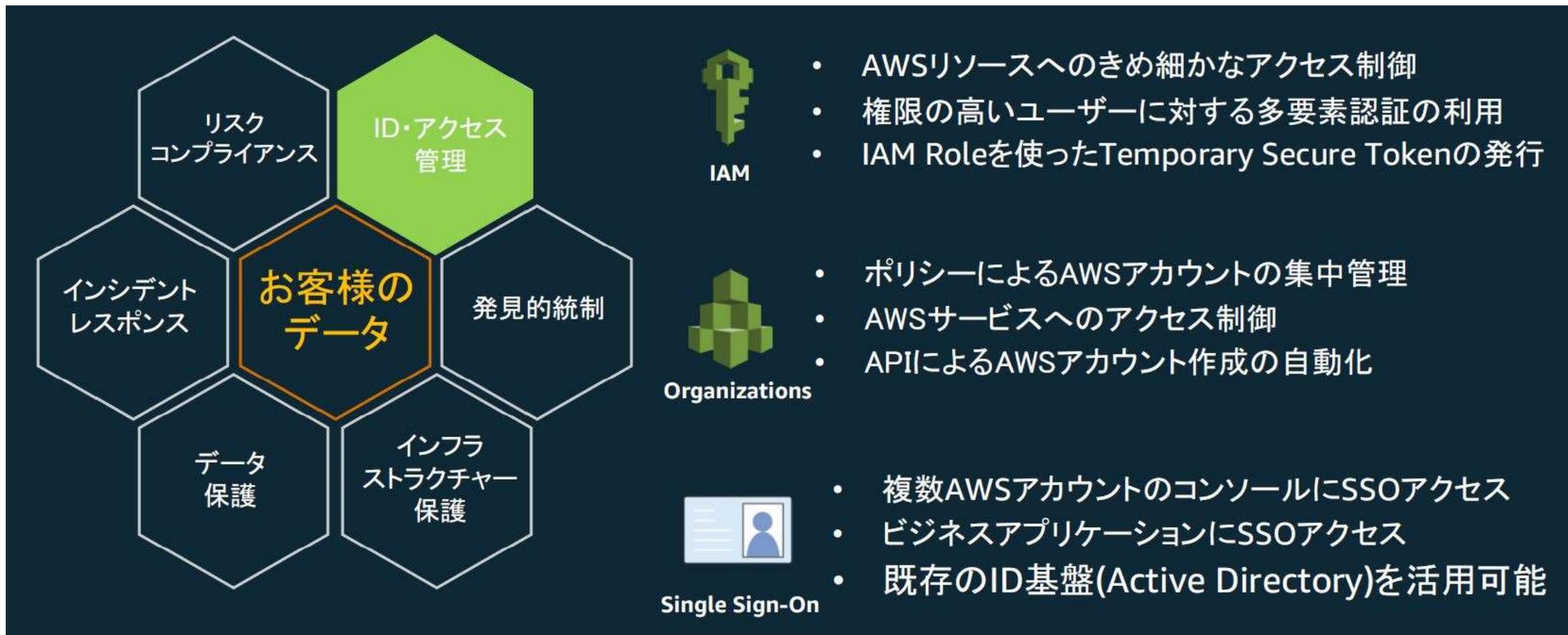

Security IN the Cloud
のためのサービス群

Security OF the Cloud

セキュリティと統制をどのように強化するか



セキュリティと統制を強化するサービス群



セキュリティと統制を強化するサービス群

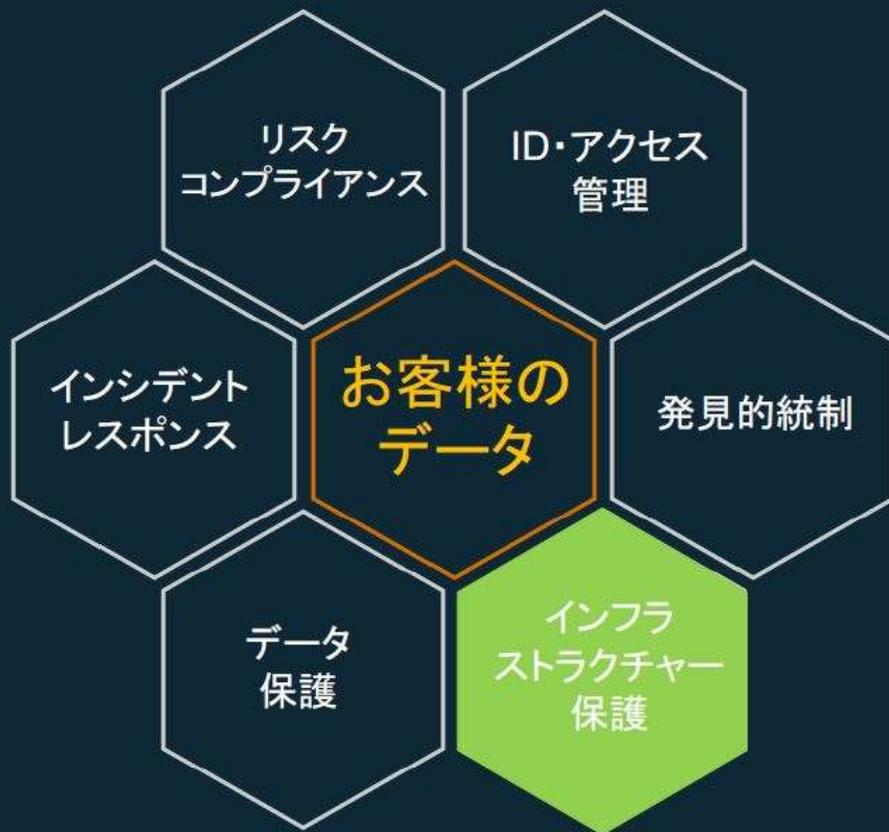


- 
- CloudWatch
- AWSサービスのリソース モニタリング
 - ログモニタリング (CloudWatch Logs)
 - プロアクティブ モニタリング (CloudWatch Events)

- 
- CloudTrail
- 呼び出されたAPIに関するイベントを継続的にロギング
 - コンプライアンスの簡素化
 - セキュリティの自動化

- 
- GuardDuty
- セキュリティ脅威リスクを検知・可視化
 - 悪意のあるIPアドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威

セキュリティと統制を強化するサービス群



AWS Shield

- AWS Platformが提供するDDoS保護サービス
- L3/L4レイヤーへの攻撃からのプロテクション機能
- アプリケーションへの影響を与えず、攻撃を軽減



WAF

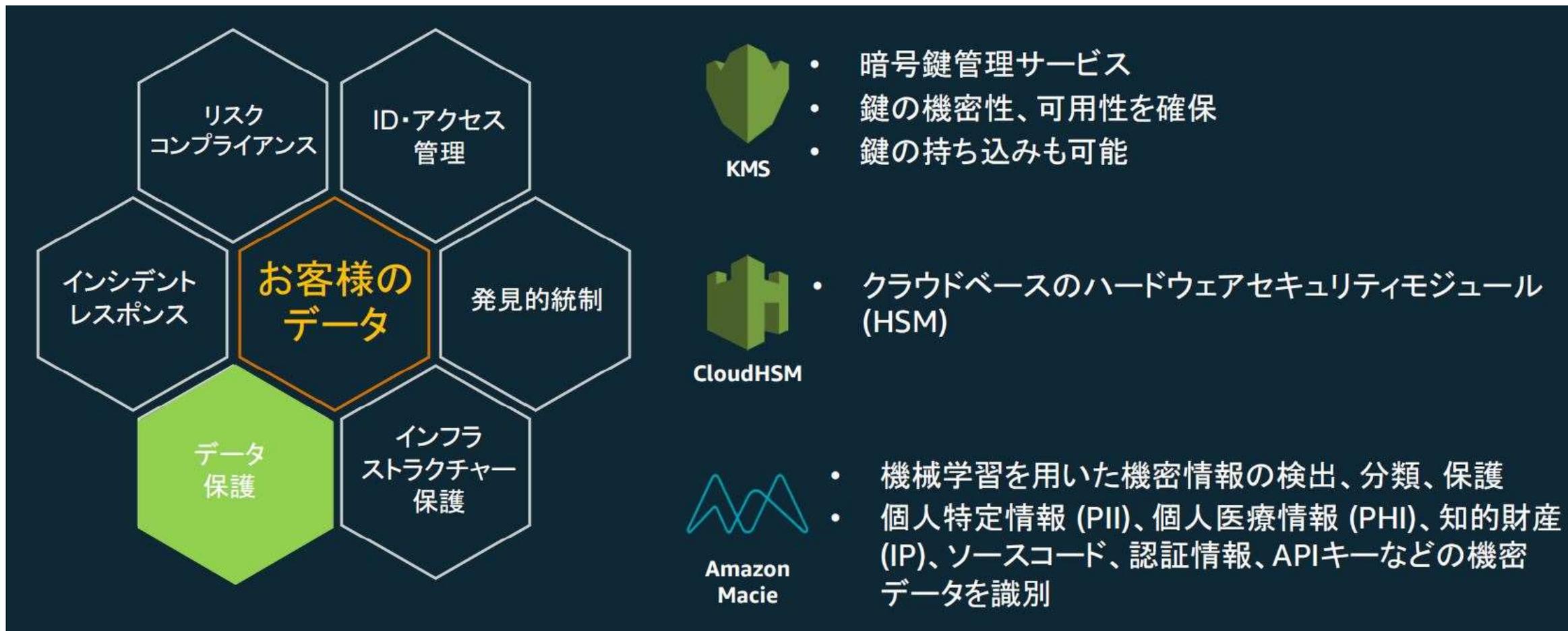
- AWSが提供するウェブ アプリケーション ファイアーウォール フレームワーク
- カスタムルールによるアクセス制御
- SQLインジェクションやXSS攻撃などへの対応



security group

- AWSリソース間のアクセスを制限するファイアーウォール
- ルールをベースにリソース間トラフィックを制限

セキュリティと統制を強化するサービス群



セキュリティと統制を強化するサービス群



Lambda

- イベントをトリガーにコードを実行
- OS、キャパシティ等インフラの管理不要



CloudWatch

- AWSサービスのリソース モニタリング
- ログモニタリング (CloudWatch Logs)
- プロアクティブ モニタリング (CloudWatch Events)



AWS
Systems Manager

- システムの自動構成と継続的な管理
- Run Commandによるサーバーのリモートアクション
- インベントリによるサーバー構成情報管理

セキュリティと統制を強化するサービス群



Trusted
Advisor

- AWSサービスの使用、構成に関して分析、推奨事項をご提案
- 50を超えるチェック項目のベストプラクティス



AWS
Config

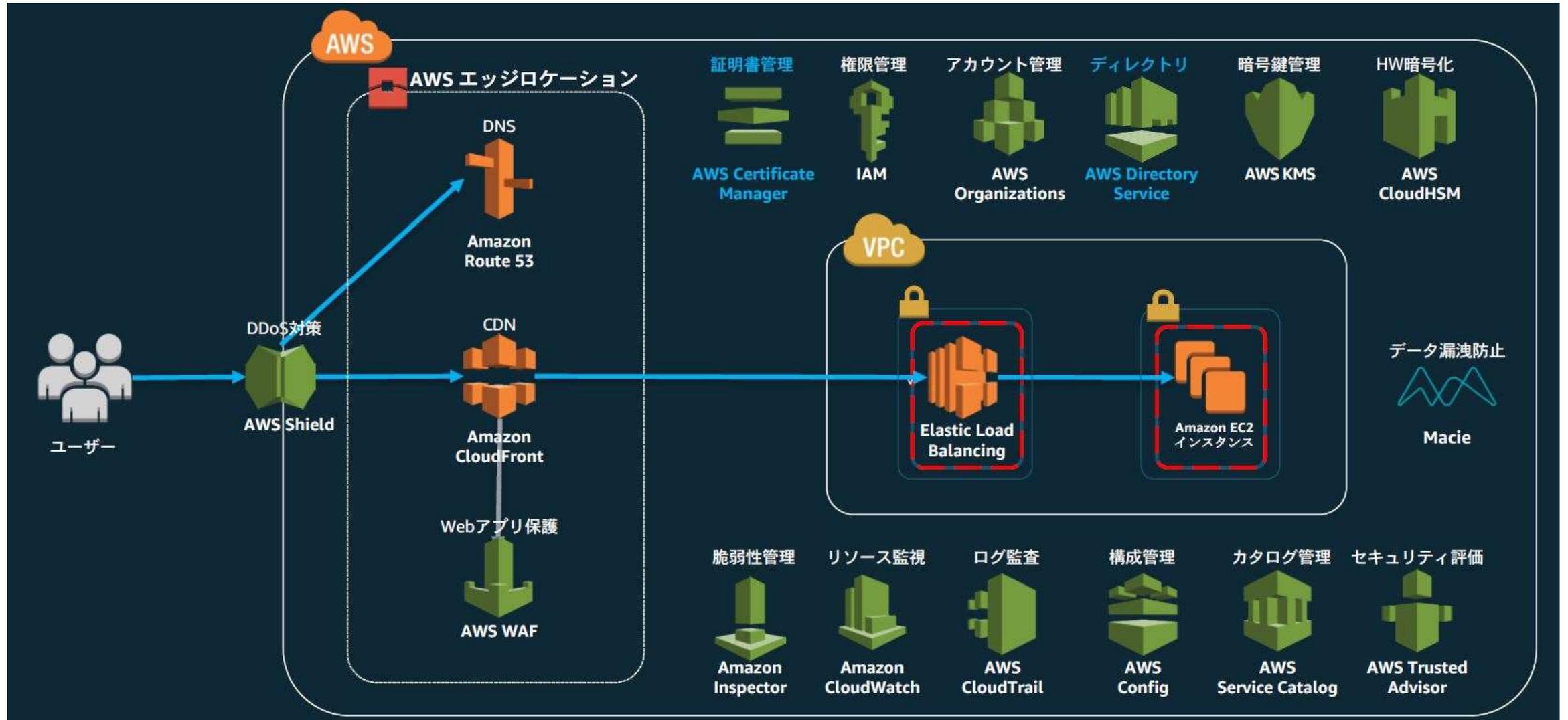
- AWSリソースの構成管理・変更管理
- 継続的モニタリング・評価
- Compliance as Code



Amazon
Inspector

- 自動化されたセキュリティ評価・診断サービス
- CVE(共通脆弱性識別子)、CIS業界ベンチマーク、AWSセキュリティベストプラクティスなどに基づくルールパッケージを提供

セキュリティと統制を強化するサービス群



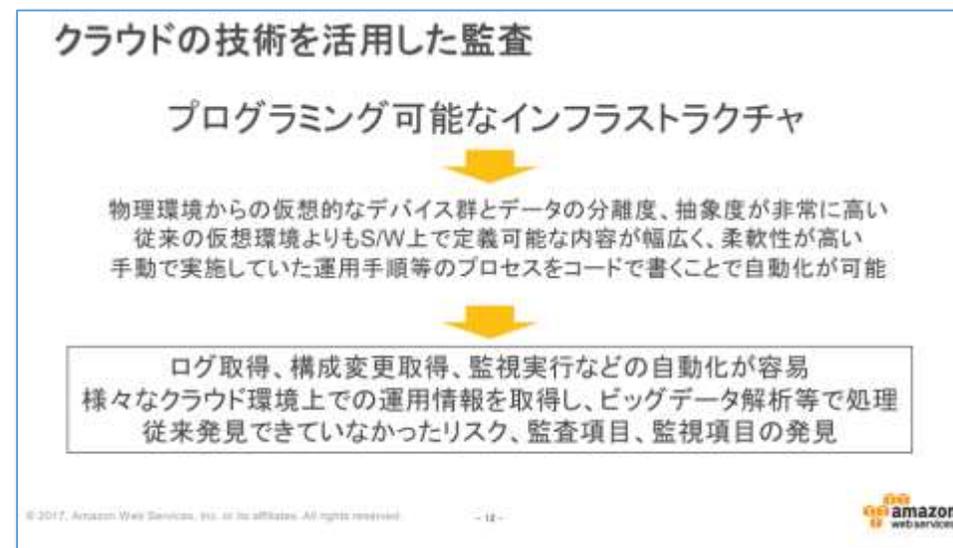
金融情報システムセンター（FISC） FINTECH有識者検討会の議論

- X クラウドは不安だからリスク管理を強化する
- O クラウドを適切に使えば、より安全な仕組みが実現可能

APIによる継続的監査、リアルタイム監査など、オンプレでは実現が難しいが、クラウドでは容易に実現

AWSの委員からの意見が採用されて、検討報告書に記載されました。

報告書は2017年6月にFISCから公開



今日、お伝えしたいこと

- クラウドの進化と真価 ～インフラを越えるもの
- メガバンクの利用、クラウドのセキュリティと統制
- AWSはかつてない異形のITベンダ
- re:Invent が毎年IT業界を揺り動かす

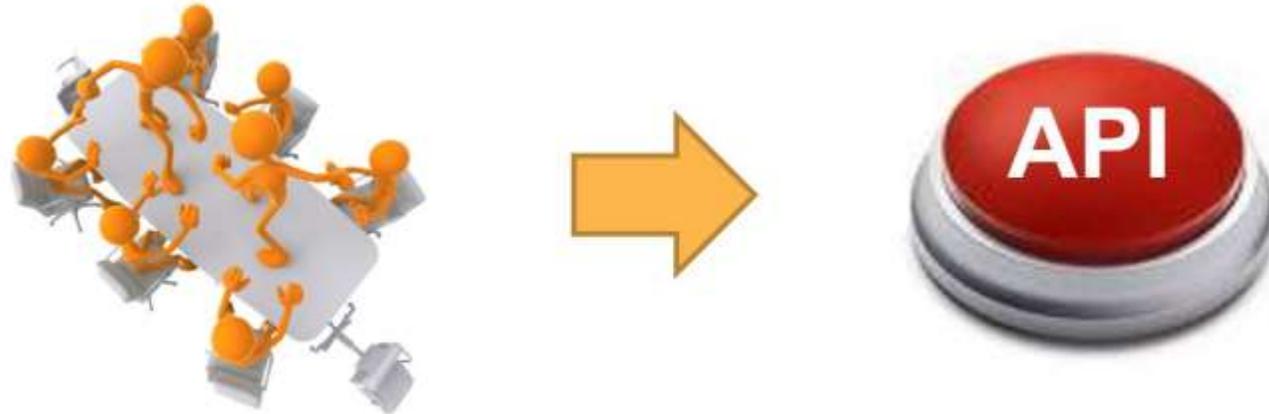
AmazonとAWS (Amazon Web Services)

- Amazon 世界最大のEC企業、1994年設立、売上15兆円、世界小売業3位
- AWSはAmazonのクラウド事業部門、2006年外販サービス開始
2017年見込 売上180億\$、約2兆円



AmazonからAWSが生まれた背景

アマゾン社内の
ビジネス課題を解決するために
生まれた



急成長するビジネスを支えるコンピューティングを
ECサイトのようにWebクリックで調達

全く人出を介さずに、ソフトウェア、APIで実現

2012年 re:invent 第1回目の衝撃 ～自分を変えたもの

re:Invent 2012 AWS初のグローバル ラーニングイベント

➤ re:Inventの名前の由来は「再発明」

- ・再発明 1: クラウドでエンタープライズシステムを実現
- ・再発明 2: 「車輪の再発明」は無駄、マネージドサービスを利用

➤ **我々はかつてない異形のITベンダ、異なる常識、行動様式**

- ・従来のITベンダの、高価格、高利益志向と真反対
- ・中間業者に渡す金はない、利益は全て投資と値下げ
⇒ これまでのIT業界のビジネスモデルと真逆、極めて辛い、、

しかし、確実に顧客の見えざる手は進んでいる

AWSは、かつてない異業種参入ITベンダ
従来のハードベンダとそのパートナーによる、物販中心の
ITビジネスの在り方、50年来の歴史を根底から変える。

◆ これまでのITベンダのビジネスモデル

- ⇒ ハードウェア、ソフトウェアの利ざや、高付加価値、高粗利、保守
- ⇒ 顧客の懐具合から個別対応、物販+エンジニア費、コンサル費

◆ AWSのビジネスモデル

- ⇒ 徹底的な顧客志向、完全自前のソフト開発
- ⇒ 投資した、買収した故の「回収」「在庫」という考えが無い
- ⇒ 大きなシステム製品ではなく、サービスを部品として組み合わせる
- ⇒ 顧客が困っている課題は、次々とソフトウェアサービスで実現

顧客のITの不満、不自由、コスト削減を着実に解決

今日、お伝えしたいこと

- クラウドの進化と真価 ～インフラを越えるもの
- メガバンクの利用、クラウドのセキュリティと統制
- AWSはかつてない異形のITベンダ
- re:Invent が毎年IT業界を揺り動かす

AWSのこの1～2年の急成長ぶりと
破壊的創造、領域の拡大、
クラウドセキュリティのゆく姿を
re:Invent から読み解く

AWS re:Invent とは



- AWS 世界最大の“学習型イベント”（≠マーケティング）
- 年に1回 Las Vegasで開催、2012～2017、昨年6回目
- 昨年は3つのキーノート、1200以上のセッション
- 参加者 43,000人、日本からユーザ、SIer 1000名余が参加
- 今後のクラウド業界を一新する多数の新サービス発表

セッションは主に、ユーザ事例、製品解説、新発表サービス紹介
講義形式から、対談放談形式、ワークショップ、技術討論など

re:Invent 2017 会場

- イベント規模が急拡大、更にホテル3か所から7か所に一気に急増
- 南北4 km、東西2 km、およそ渋谷～新宿位、数万人が臨時バスで移動

メイン会場の他、

- ・ IoT, AI系
 - ・ APN系
 - ・ イベント系
- などに分散

基調講演も2か所
ナイト基調講演
深夜イベントも



re:Invent 2017
ホテル会場
@Las Vegas

AWS re:invent に集まる人々

(万人)

	参加者数	セッション数	日本から
2012	6,000人	150セッション	80人
2013	9,000人	175セッション	200人
2014	13,500人	273セッション	300人
2015	19,000人	278セッション	400人
2016	34,000人	400セッション	700人
2017	43,000超	1200セッション	1200人



AWS re:Invent 振り返り

- 2012年 re:Invent第1回目、S3値下、RedShift
- 2013年 Cloud Trail、WorkSpaces ⇒ API基盤、SaaS
- 2014年 **“New Normal”**
Aurora(OracleRAC対抗)、Lambda(サーバーレス)、ECS(コンテナ)、Code3兄弟(ソース管理～配備)、KMS(鍵管理)、Config(構成管理)
⇒ **エンタープライズ利用向け、システム開発～運用を横断するサービス**
- 2015年 **“破壊的創造”、“7つの自由”**
AWS IoT(コードレス統合開発運用)、Inspector(セキュリティ自動評価)、Config Rule(ルールベース構成管理)、Quick Sight(BI)、Snowball(Data移行)
⇒ **ソフトウェアでできることは次々と自動化、クラウドで更に安心、安全**

1 昨年、AWS re:invent 2016 が示したものの（1部）

あるとすごくいいな、と誰もが思える新サービス

- AWS Organization 大規模利用時のアカウント管理
- AWS Snowmobile エクサバイトデータ移行
- AWS Shield マネージド DDoS保護
- EC2 Systems Manager オンプレ含めて資産管理、パッチ自動化
- AWS Step Function ワークフロー管理

さらに、誰もが想定を超える新しい領域にも新サービス

- Lambda@Edge エッジでコード実行(クラウドDCから外へ)
- AWS Greengrass IoTデバイスでサーバーレスコード実行
- AWS X-Ray アプリコードを横断的トレース(APM製品)

エンタープライズ向け上位マネージドサービスが次々と拡張
SIer、ISVの製品、サービス領域にも続々と越境

昨年、AWS re:invent 2017 が示したものの

AWS re:Invent 前後で約60の新サービス発表 (主要な項目のみ)

従来のIT発想の延長で、誰もが嬉しい新サービス

◆エンタープライズ分野

- Amazon Aurora Multi-Master
- Amazon Aurora Serverless
- AWS Systems Manager
- Amazon MQ Apache ActiveMQ
- AWS Fargate コンテナ運用

◆動画分野

- AWS Media Services 動画ビジネス
- Amazon Kinesis Video Streams

◆機械学習、音声、翻訳分野

- Amazon Rekognition Video 動画認識
- Amazon Comprehend 自然言語理解
- Amazon Translate 多言語観翻訳
- Amazon Transcribe Speech-to-Text

◆基盤分野

- EC2 i3.metal ベアメタル
- AWS PrivateLink
- Direct Connect Gateway

今年、AWS re:invent 2017 が示したものの

AWS re:Invent 前後で約60の新サービス発表 (主要な項目のみ)

誰もが想像を超える、新しい領域の新サービス

◆全く新しい分野

- GuardDuty 継続的脅威検出統合監視(NW,アクセス,API)
- AWS WAF ManagedRule ISVパートナーがWAFルールをサービス提供
- AWS Cloud9 初のクラウドネイティブIDE統合開発環境
- Alexa for Business Alexaのビジネス利用、会議システムなど
- Amazon Sumerian VR/AR/3Dコンテンツ複合開発
- AWS DeepLens 開発者向け深層学習ビデオカメラデバイス
- Amazon SageMaker 開発者向け深層学習モデル開発環境
- Amazon Neptune グラフDBマネージドサービス

今年、AWS re:invent 2017 が示したものの

AWS re:Invent 前後で約60の新サービス発表 (主要な項目のみ)

誰もが想像を超える、新しい領域の新サービス

◆全く新しい分野

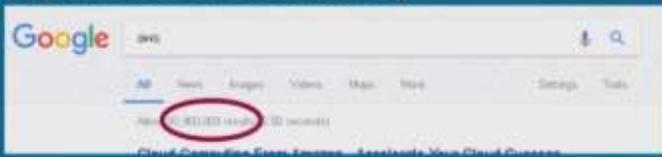
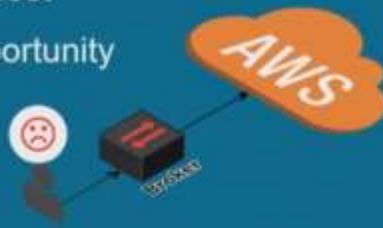
- GU ✓ 既存ITベンダ、IT製品領域に続々と越境
- AI Alexa for Business(会議), Sumerian(VR,AR,開発),
- AI WAF ManagedRule
- AI
- AI ✓ インフラ基盤からコード開発～最強RDB～監査全域へ
- AI Cloud9, Aurora Multi-Master, GuardDuty
- AI
- AI ✓ 機械学習の新段階 ⇒ デバイスからモデル開発迄網羅
- AI DeepLens, SageMaker(開発), Comprehend(理解)

バークレイズ銀行のセッション

1) Cloud Brokers

Control at the entry point to cloud

- Optimisation limited by broker capability—high cost
- Innovation limited by broker capability—lost opportunity
- Abstraction is a myth
- Arbitrage is a false economy
- Impair the power of the community



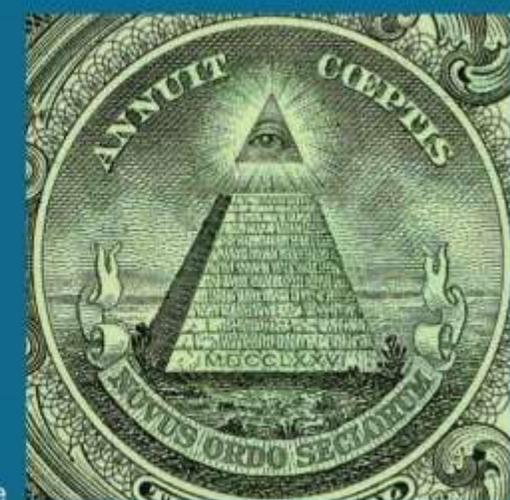
93 M pages of help of no use!

13 | Barclays & AWS | November 2017

BARCLAYS

Continuous Compliance

Historically enterprises have strongly favoured preventative controls, but these can hamper DevOps practices



Track all activity

Monitor controls integrity

Automatically converge anomalies

More focus on detective and automated reactive controls

Annuit Coeptis - "approves our undertakings"

23 | Barclays & AWS | November 2017

BARCLAYS

マルチクラウド、クラウドブローカーの検討は意味がない
クラウドの意味がなくなる。**クラウドネイティブがAWSの価値**
監査まで一気通貫でやれるのがクラウド。

クラウドで 日本をイノベーション

ご紹介：対談集が発行されています

翔泳社の技術者向けイベント「Developers Summit(デブサミ)」の連動企画書籍。翔泳社代表の岩切さんとの対談です。



- Sierに新卒入社して定年退職まで33年、自分を技術者として育んだ金融案件などを振り返り、その後、AWS入社に至るITチャレンジを対談で語っています。
- よろしかったら、是非クリックを。
Amazon内で「渥美俊英」検索
- Kindle版はUnlimited対象で無料です。