クラウドファースト環境でのクラウドセキュリティのあり方

一般社団法人　日本クラウドセキュリティアライアンス

業務執行理事/事務局長　諸角昌宏

CCSP, CCSK, CSAリサーチフェロー

2018年6月8日

アジェンダ

1. Cloud Security Allianceについて
2. クラウドを取り巻く環境
3. クラウド環境におけるセキュリティ上の利点・欠点
4. クラウドセキュリティに向けたガイドライン
5. *まとめ*

1. Cloud Security Allianceについて

Cloud Security Allianceについて

- CSA本部：　グローバルな非営利活動法人
  - 創立：2009年
  - 会員数
    - 個人会員　8万5千人以上
    - 地域支部　85以上(日本を含む)
    - 企業会員　400社以上
  - 33のワーキンググループと調査研究プロジェクト
  - 政府、研究機関、専門家団体、企業との戦略的パートナーシップ

- 次世代ITのための実践規範の構築
- 調査研究と普及啓発

“

クラウドコンピューティングにおけるセキュリティ保証に向けた実践規範活用の促進と、クラウド利用のための教育を通じてあらゆるコンピュータ利用のセキュリティを高めるための活動への取組み

一般社団法人日本クラウドセキュリティアライアンス設立の趣旨・背景

- 目的
  - Cloud Security Alliance(CSA)の開発するガイドラインやツールを日本で展開・活用するための取組みを中心に活動
  - CSAの活動の活発化、世界的プレゼンスの向上
  - 各国での支部の設立、法人化の進行
  - ますます浸透するクラウドの活用とそのセキュリティ課題の重要性に対応

- 経緯
  - 2010年6月に任意団体として発足
  - 2013年12月にCSA日本支部を法人化（一般社団法人へ）
    - 日本におけるクラウドセキュリティへの取組みの中心を担うべく、法人化し、活動基盤の強化充実を図る
- 会員数
  - 企業会員：32社（2018年5月1日時点）
  - 個人会員：約80名

CSAにおけるWG活動とその相互連携

＜参考＞

CAI™

CSA STAR™
Security, Trust & Assurance
Registry

CCM™
Cloud Controls Matrix

他の

ISO27001/ISO27010/
HIPAA/ HITECH Ac/
AICPA/COBIT/ENISA/
FedRAMP/ PCI DSS

CCSK™
Certificate of
Cloud Security Knowledge

WGや研究活動

INTERNET of THINGS

Big Data

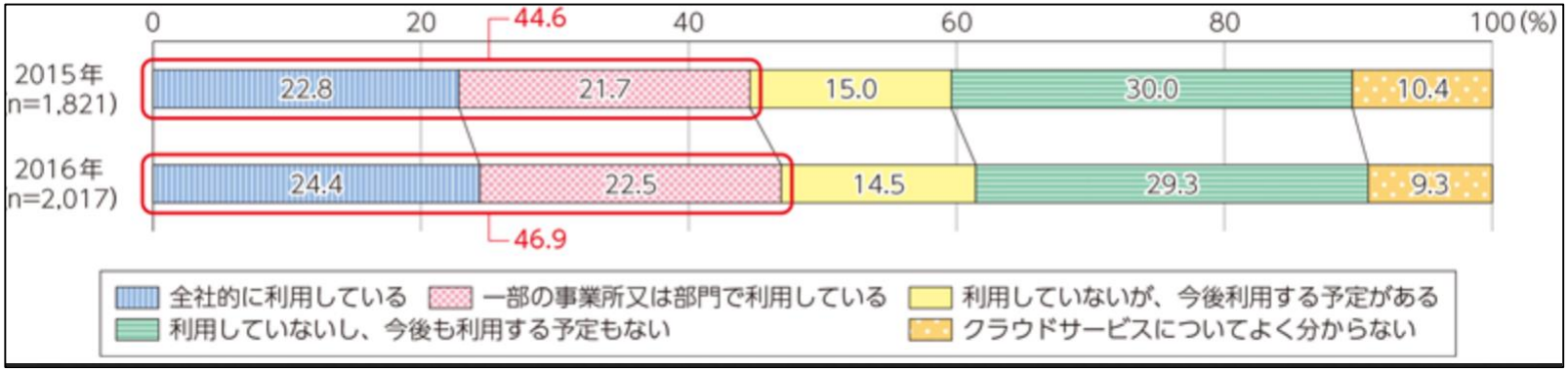
HIM

SecaaS

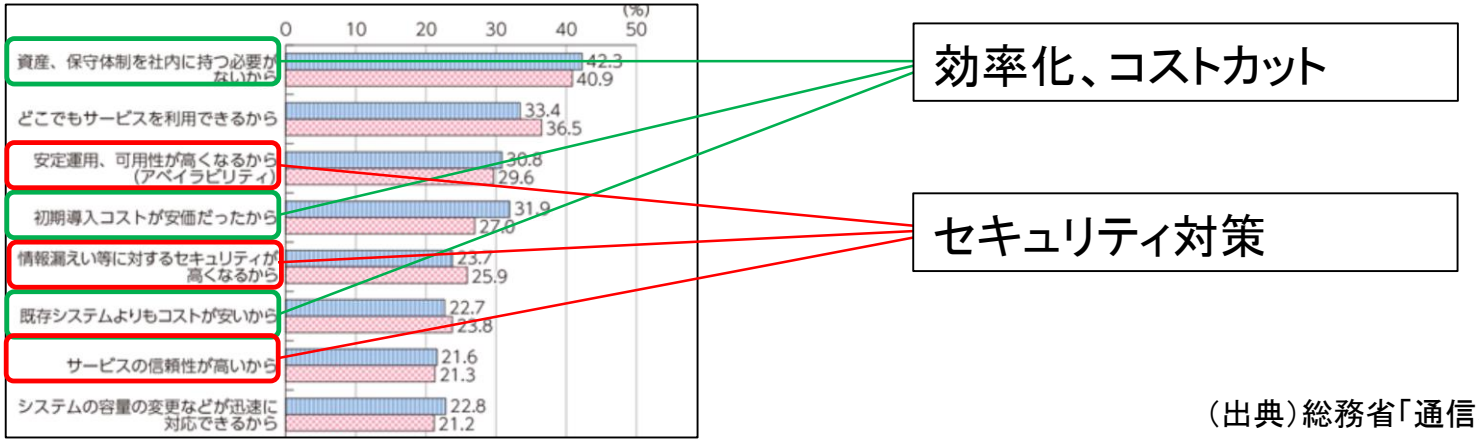
2.クラウドを取り巻く環境

クラウドの利用状況(1)

- 企業におけるクラウド利用状況



- クラウドを利用する理由



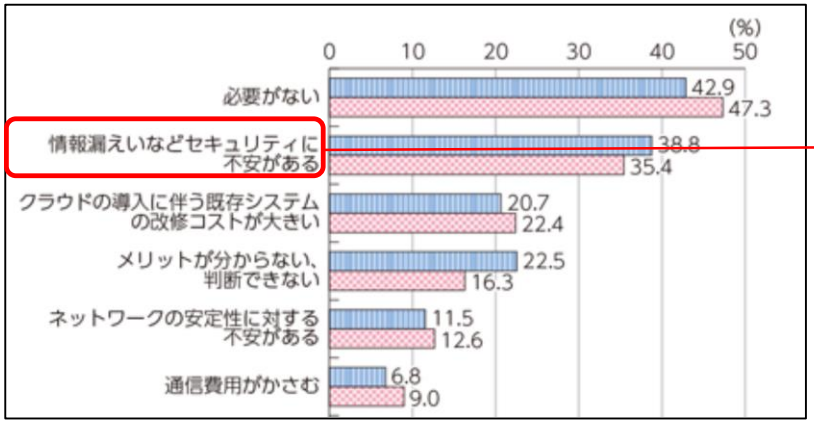
効率化、コストカット

セキュリティ対策

（出典）総務省「通信利用動向調査」

クラウドの利用状況(2)

- クラウドサービスを利用しない理由



セキュリティに対する懸念

（出典）総務省「通信利用動向調査」

- クラウドに対する期待

順位	パブリッククラウドサービス	HPCサービス	EPC	インダストリークラウド
1	ITセキュリティの強化	ITセキュリティの強化	ITセキュリティの強化	ITセキュリティの強化
2	ビジネスの迅速性向上	ビジネスの迅速性向上	ビジネスの迅速性向上	業務部門におけるITの利活用の向上
3	IT部門の生産性向上／人員の最適化	業務部門におけるITの利活用の向上	ITの標準化と簡易化の促進	IT部門の生産性向上／人員の最適化
4	ITの標準化と簡易化の促進	IT予算のCAPEXからOPEXへの変革	IT部門の生産性向上／人員の最適化	IT予算の削減
5	IT予算の削減	新しい機能の迅速な導入	IT予算のCAPEXからOPEXへの変革	新しい機能の迅速な導入

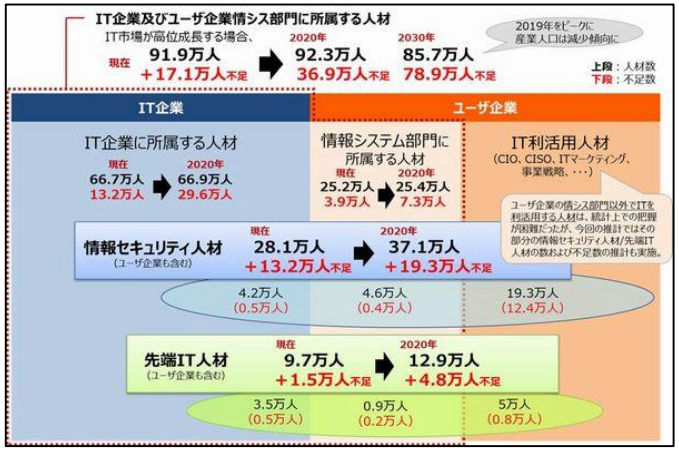
（出典）IDC Japan　クラウドに関わるユーザー動向調査「CloudView 2017」

- 従来の「IT予算の削減」は、過年度調査と比較して優先順位が大幅に低下
- クラウド導入の促進要因として「ITセキュリティの強化」を最も重要視

クラウドの利用状況(3)

- クラウドの利用における最大の懸念は引き続き「セキュリティ」
- クラウドの利用に対する最大の期待は「セキュリティ」の強化

- 背景
  - セキュリティ人材の不足
    - 企業独自のセキュリティ確保は限界
  - クラウド・プロバイダーのセキュリティ強化
    - セキュリティをソフトウエアで解決



(出典)経済産業省「IT人材の最新動向と将来推計に関する調査結果について」

3.　クラウド環境におけるセキュリティ上の利点・欠点

クラウドコンピューティングの利点(1)

- リソースの所有が不要
  - システムに対する初期投資（設備投資）が不要
    CAPEX(設備投資)→ OPEX(運用コスト)
  - ハードウエア、ソフトウエアに対するメンテナンスが不要
    使用期限、EOL(の生産終了や販売終了、ソフトウェア製品などのサポート終了、修正・更新プログラムの提供終了)等が不要

- リソースの自由な割り当て
  - 迅速性
  - セルフサービス
  - 拡張性（基本的に無限のリソースを利用）

- リソースの利用率の向上
  - プロバイダ：　リソースの有効活用（リソースプール）
  - カスタマ：　リソースの平準化（処理のピークに合わせた準備が不要）

クラウドコンピューティングの利点(2)

- 利用したリソースの量に応じて課金（Pay-for-Use）
- 可用性
  - プロバイダの障害対策、24時間運用等、稼働時間を確保
- 自由なアプリケーション、情報の展開が可能
  - オンプレ、クラウドの選択

クラウドコンピューティングのセキュリティ上の主なリスク(1)

組織のリスク

- ロックイン
  - データ、アプリケーションのポータビリティが確保されていない場合、プロバイダに依存する
  - プロバイダを変更するときに非常に大きなコストを必要とする
- ガンバナンスの喪失
  - 管理責任をプロバイダ側に移譲
  - カスタマが、必要な管理策/セキュリティ対策を実施することができない
- コンプライアンスの課題
  - プロバイダは、カスタマが必要とするコンプライアンス要件を満たしているか？
- サプライチェーンにおける障害
  - プロバイダが別のプロバイダを利用
- プロバイダの業務停止
  - プロバイダが、サービスを継続できない（倒産、ビジネスの変更など）

出展：「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」（ENISA）

クラウドコンピューティングのセキュリティ上の主なリスク

技術的リスク

- リソースの枯渇
- 隔離の失敗
- クラウドプロバイダ従事者の不正
- 管理用インターフェースの悪用
  - インターネット経由（誰でもアクセス可能）での管理用インターフェース
- データ転送途上における攻撃
- データ漏えい
  - マルチテナント環境でのデータ漏えい、データ転送中のデータ漏えい
- 不完全なデータ削除
  - リソースの再利用に伴う問題

出展：「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」（ENISA）

クラウドコンピューティングのセキュリティ上の主なリスク(3)

法的なリスク

- 司法権の違いから来るリスク
  - データ、アプリケーションがおかれる場所で適用される法律

クラウドインフラのリスク

- 技術的リスク
  - ITインフラの統合・集中のリスク（SPOF（単一障害点）など）
  - プロバイダには、大規模なプラットフォームを管理・維持に必要なより高い技術スキルが要求される
  - 技術的なリスクに対する管理策がプロバイダに移行
- 仮想化のリスク
  - VM間のリスク
    - ハイパーバイザや他のゲストOSへの侵入
  - スナップショット、イメージのセキュリティ

出展：「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」（ENISA）

クラウドコンピューティングのセキュリティ上の利点(1)

- 大規模化による利点とセキュリティ
  - セキュリティ対策は、システムの規模が大きいほど、より低コストで実装可能
  - セキュリティ人材の確保、集中が可能
- 市場での差別化要因となるセキュリティ
  - プロバイダが提供するセキュリティサービスのレベルの把握（プロバイダの透明性）
  - セキュリティ強化およびセキュリティ機能の競争によるレベルアップ
- リソースの迅速かつ洗練されたスケーリング
  - 動的なリソース配置によるセキュリティ防御
  - 耐障害性の向上
- リソースの集約化がもたらす利点
  - 低コストでの物理的境界の構築や、リソース単位での物理的アクセス制御
  - 包括的なセキュリティポリシーや管理策

出展：「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」（ENISA）

クラウドコンピューティングのセキュリティ上の利点(2)

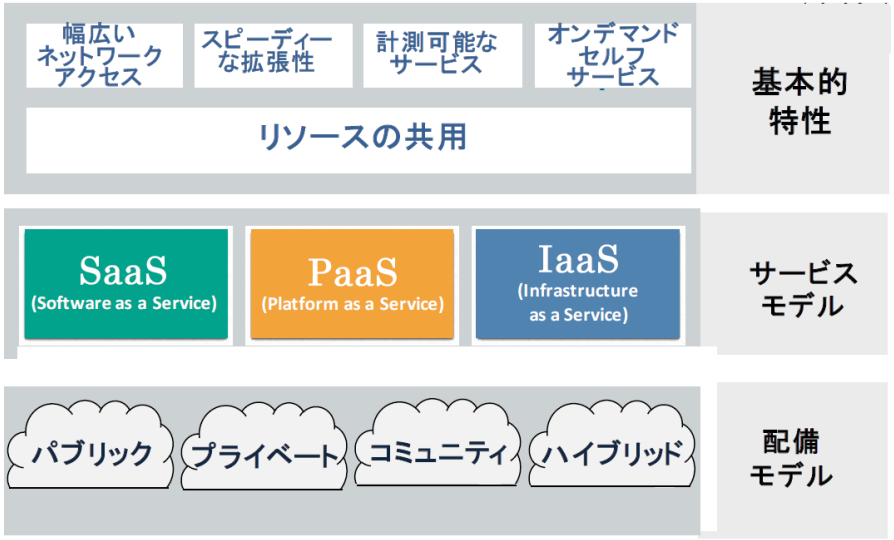
- 監査および証拠収集
  - オンデマンドによる仮想マシンのクローニング(cloning)機能を用い、オフラインでのフォレンジック分析が可能
  - パフォーマンスを低下させることなく、広範囲のログを記録することが可能
- よりタイムリーで有効かつ効率的なアップデート
  - 最新のパッチやセキュリティ設定等により、あらかじめセキュリティを強化したり、システムを最新の状態に保つ
- 監査やSLAにより導かれるより有効なリスクマネジメント
  - クラウドプロバイダに対し課せられる頻度の高い監査

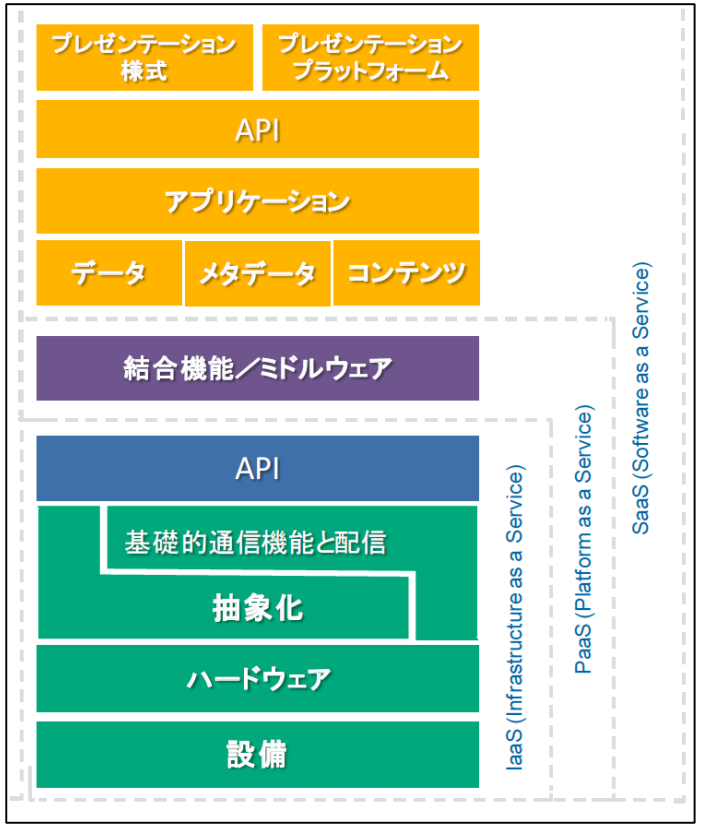
出展：「クラウドコンピューティング　情報セキュリティに関わる利点、リスクおよび推奨事項」（ENISA）

4. クラウドセキュリティに向けたガイドライン

クラウドサービスモデル

- NIST定義の採用　（SP800-145）
- SPIモデル
  - Software as a Service
  - Platform as a Service
  - Infrastructure as a Service



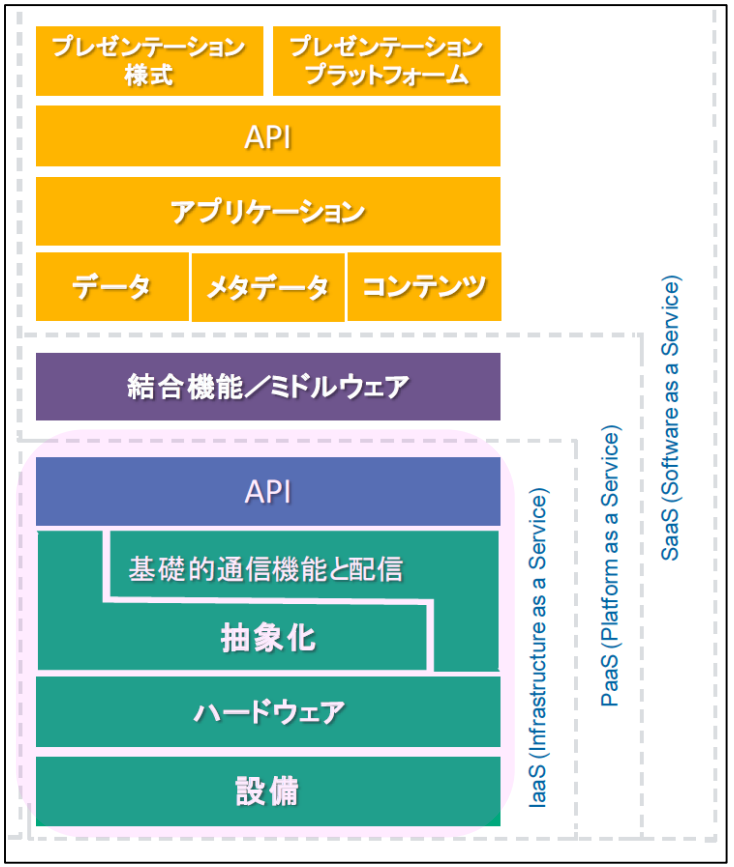


（クラウドコンピューティングのためのセキュリティガイダンス　V4.0から引用）

サービスモデルごとの特徴およびメリット

IaaS

- 特徴
  - ストレージ、ハードウエア、サーバ、ネットワーク等を、利用者がサービスとして（as a Service）利用できるモデル
- メリット
  - 拡張性、縮小性
  - 資源をプールとして統合し利用
  - セルフサービス、オンデマンドに自由に容量等を設定
  - 高信頼性、レジリエンス
  - TCOの削減

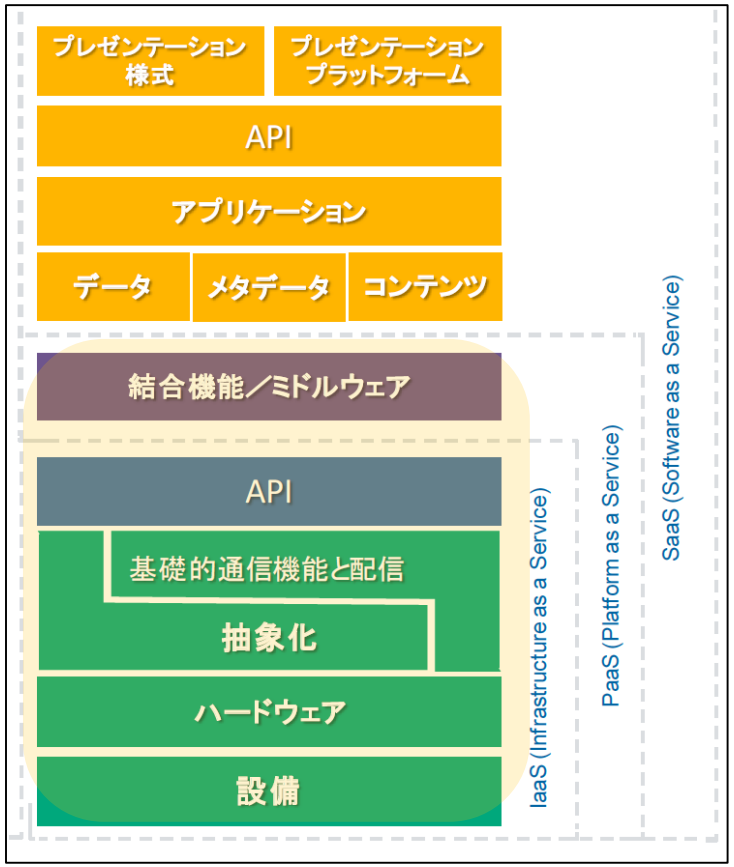


（クラウドコンピューティングのためのセキュリティガイダンス　V4.0から引用）

サービスモデルごとの特徴およびメリット

PaaS

- 特徴
  - プロバイダが提供するAPI、プログラミング言語を使用し、利用者がアプリケーションを作成可能
  - 利用者は、クラウドのインフラを意識せずアプリケーションを展開可能
  - アプリケーション開発用フレームワーク、ミドルウエア機能、データベース、メッセージング、キューイングなどの機能を提供
- メリット
  - ハードウエア、OS、下位のソフトウエアの購入・管理が不要

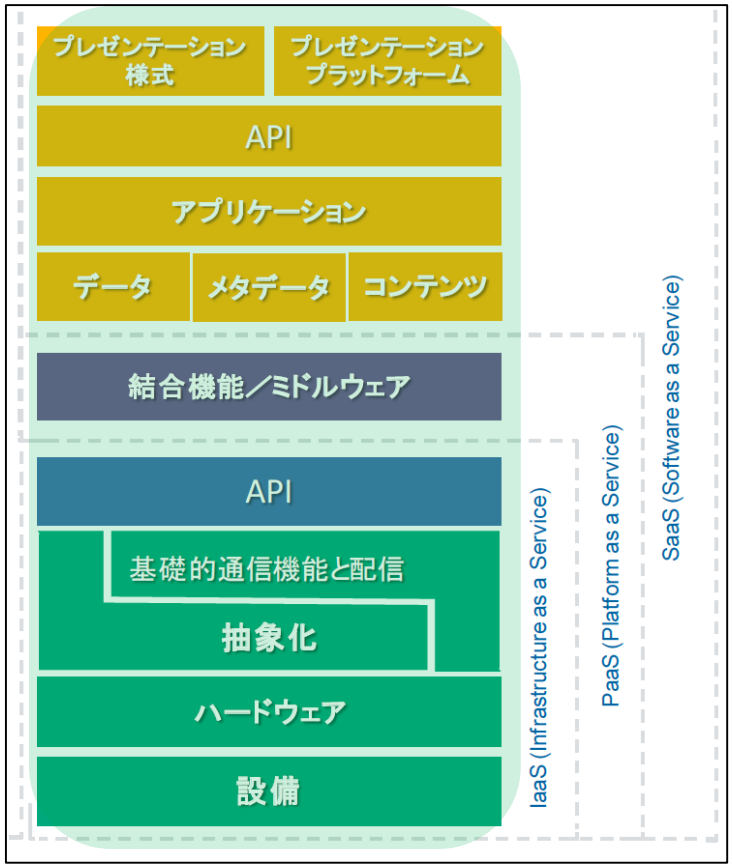


（クラウドコンピューティングのためのセキュリティガイダンス　V4.0から引用）

サービスモデルごとの特徴およびメリット

SaaS

- 特徴
  - プロバイダが提供するサービス、アプリケーションを利用者が使用
  - 利用者は、クラウドのインフラを意識せずアプリケーションを展開可能
- メリット
  - アプリケーションに、どこからでも、いつでもアクセス可能
  - アプリケーション、ソフトウエアのライセンス管理が不要
  - サポートコストの縮小

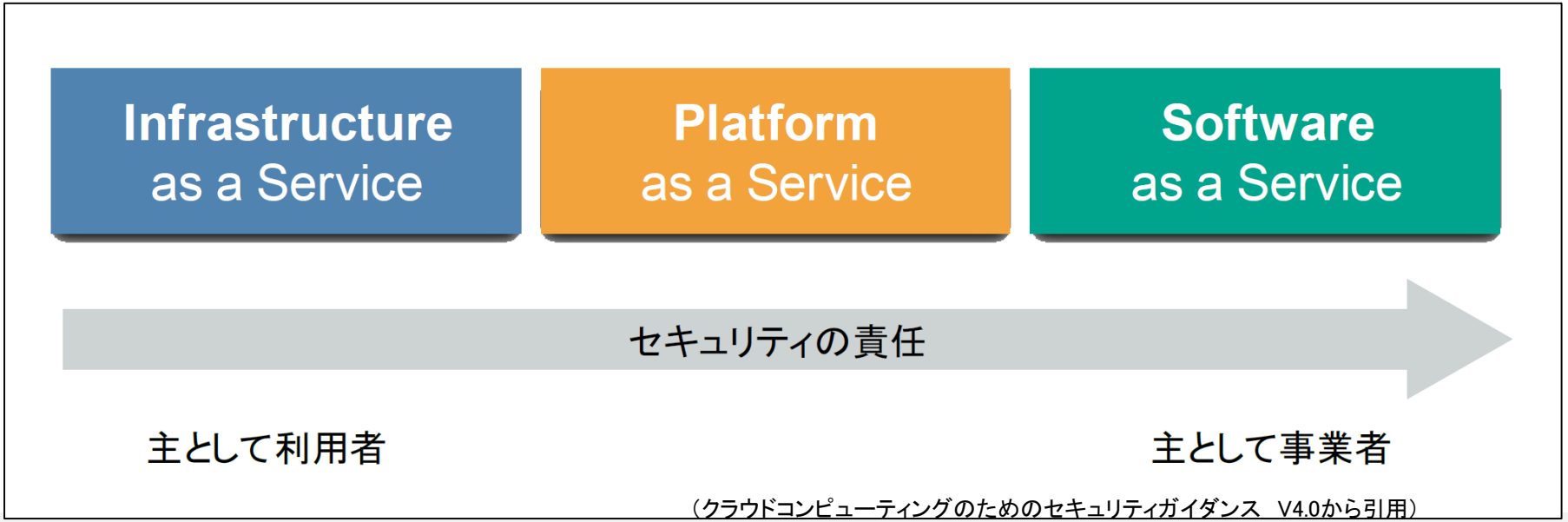


（クラウドコンピューティングのためのセキュリティガイダンス　V4.0から引用）

クラウドセキュリティの原則

責任共有モデル

- クラウド事業者は、一定のリスクに対する責任を負い、クラウド利用者はその先のすべてに責任を持つ
- SaaSにおいてはクラウド事業者が、IaaSにおいてはクラウド利用者がより多くのリスクを管理する
- **クラウド利用者は、リスクを所管する最終的な責任を負っており**、クラウド事業者にはリスクマネジメントの一部を転嫁しているに過ぎない



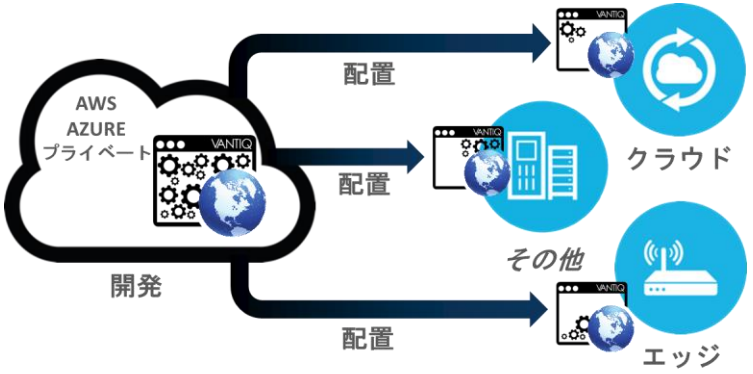
（クラウドコンピューティングのためのセキュリティガイダンス　V4.0から引用）

クラウド利用の新たな流れ

- クラウドコンピューティング環境の変化
  - 新しくフォーカスされている技術
    - コンテナ、マイクロサービス、サーバレス
  - 「オンプレ vs クラウド」=>「適材適所へのコンポーネントの配備」への移行
    - Application Platform SaaS

プラットフォーム化

- クラウドにどのように移行するかではなく、クラウドを含めたプラットフォーム全体をどのようにセキュアにするか
- クラウドサービスモデルの責任境界の考え方だけでなく、コンポーネントがどこで稼働しているかをコントロールすることが必要になる。



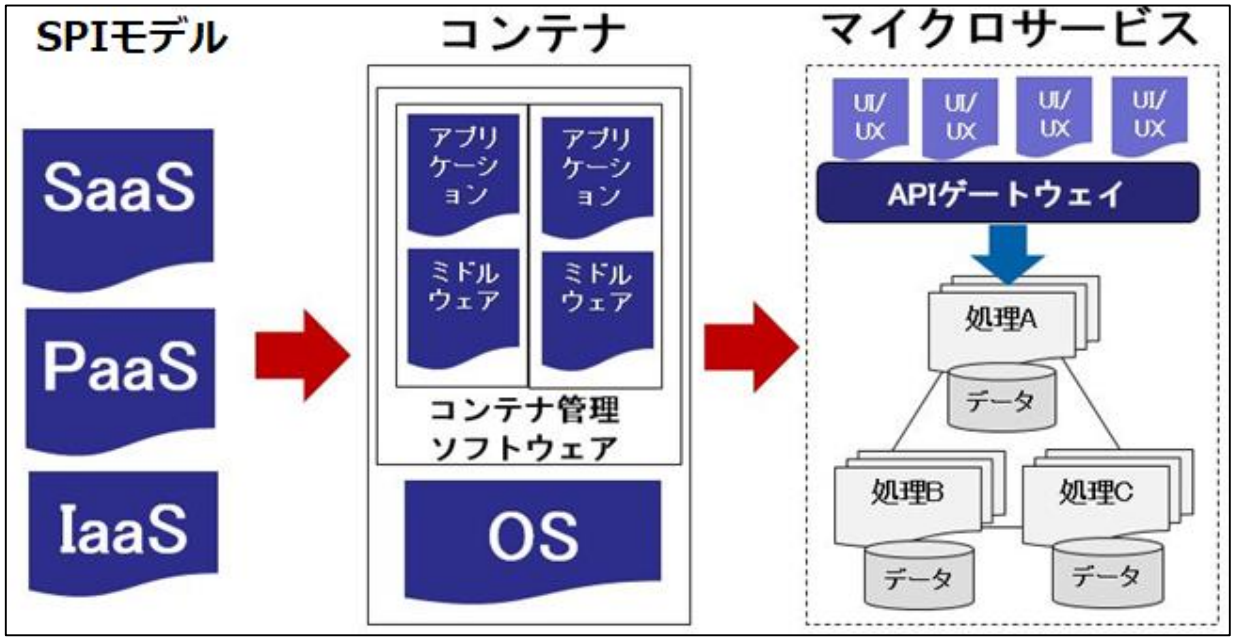
CSA勉強会 「IoT環境を支えるイベント・ドリブン・アーキテクチャ（EDA）とそのセキュリティ」 資料より引用

クラウドの新たな流れ

- コンシューマードリブンなビジネスモデルは**SaaS**から**マイクロサービスのプラットフォーム**へ（例：Fintechサービス）

モノリシックな三層型
アーキテクチャから

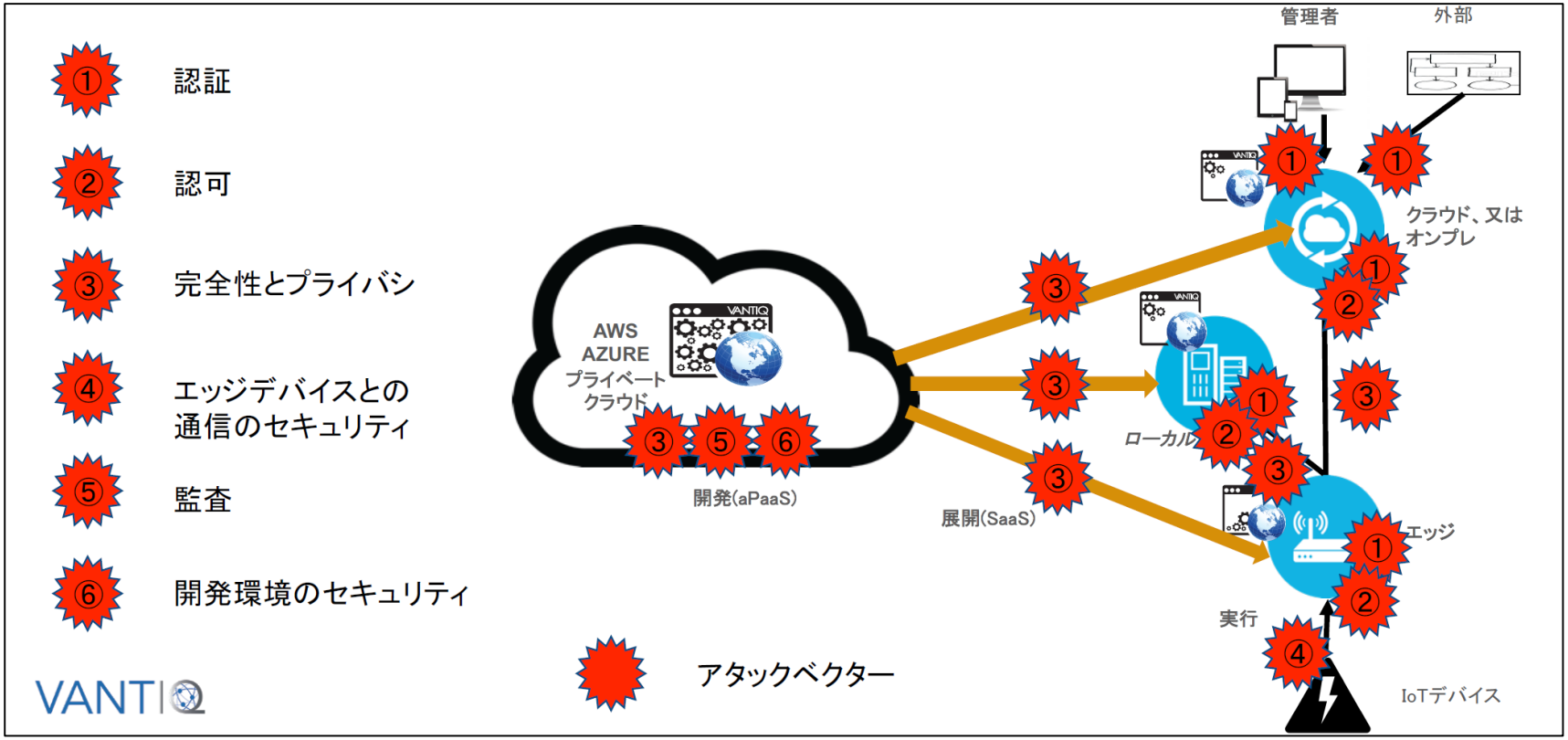
自律サービスの疎結合型
プラットフォームへ



出典：ヘルスケアクラウド研究会（2015年11月）を基に作成

プラットフォームでのセキュリティ

- 開発/運用から配備まで全体的なセキュリティ対策が必要
- プロバイダーによる一気通貫のセキュリティ対策が必要



CSA勉強会 「IoT環境を支えるイベント・ドリブン・アーキテクチャ(EDA)とそのセキュリティ」 資料より編集

新たなクラウドセキュリティ

- 開発/運用だけでなく配備も含めたセキュリティ
  - **ワークロード**
    - ワークロード　＝　処理の一単位
    - 仮想マシンのOS上で稼働するアプリケーションから、GPU,FPGAベースに特殊化されたタスクまでを含む。
    - クラウド利用モデルに関係なく、ワークロードが物理的にどこで稼働するかをコントロールする必要がある。
  - **イミュータブル（immutable)**
    - 変更無用という考え方
    - 新しいイメージで稼働しているインスタンスを完全に置き換える
      - 一部、OS更新だけのために新しいイメージをプッシュする場合がある
    - 基本的には、全て自動であり、手動で操作することはない。
    - ログインは基本的に無効化される。

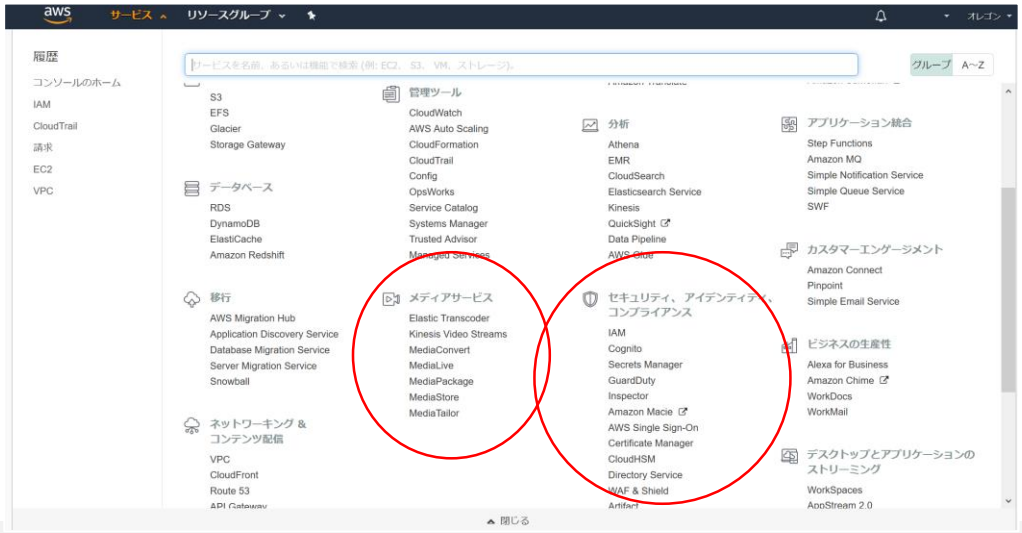
新たなセキュリティの優位性

- ワークロードのセキュリティ
  - ワークロードのセキュリティ（隔離等）は基本的にクラウドプロバイダの責任
  - イミュータブルを利用することでワークロードのセキュリティが高まる
    - リモートアクセスを無効にする
    - イメージ作成の中にセキュリティテストを組み入れる
    - ファイルの完全性モニタリングを使用し未承認の変更を監視する
    - 稼働してるインスタンスにパッチをあてるのではなく、イメージをバージョンアップする
    - セキュリティは非常に強化される（SSHを用いたアクセスが不要）

プロバイダーによるセキュリティ強化

- AWSの例：
  - サービスとして新たに提供された機能の1/4がいわゆるセキュリティ機能
  - セキュリティを、ソフトウエアおよびサービスで提供
  - サービス化されたガバナンス、ポリシーを利用可能
  - グローバルで一貫したセキュリティ機能
  - 企業の規模にとらわれないセキュリティ対策

CSAジャパンブログ 「第3回クラウド利用者会議 レポート」より引用（2016年10月3日）



5.まとめ

まとめ

1. クラウドセキュリティの原則：
   責任共有モデル

2. 開発/運用から配備までのセキュリティ対策：
   プラットフォーム・セキュリティ

3. クラウドが変えるセキュリティ：
   セキュリティはソフトウエアが解決する

https://cloudsecurityalliance.jp

info@cloudsecurityalliance.jp

ありがとうございました