# 安全なクラウド利用環境に向けた クラウドセキュリティ対策

2017年11月27日

日本クラウドセキュリティアライアンス

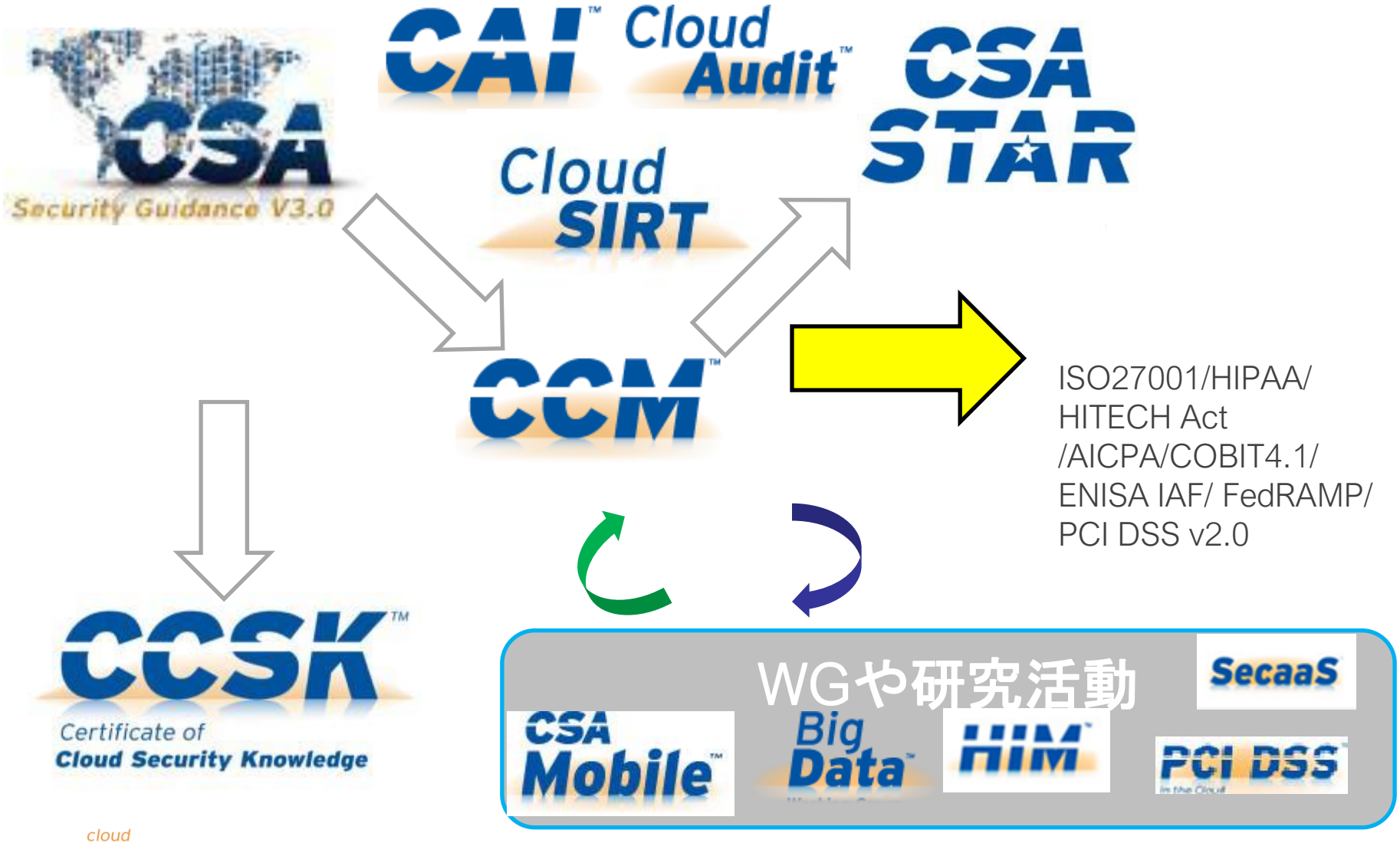
業務執行理事/事務局長　諸角昌宏

# CSAジャパンの今までの活動

- CSA本部の事業の日本における展開
  - ガイダンス、CCM、STAR、CCSK等
- WGを中心とした調査研究活動
  - CSA本部WGとの協業
  - CSAジャパン独自のWG
  - 日本発グローバルWG
- 情報発信活動
  - セミナー、シンポジウム
    - Summit、Congress、月例勉強会等
  - ホワイトペーパ等の翻訳、公開

# CSAにおけるWG活動とその相互連携

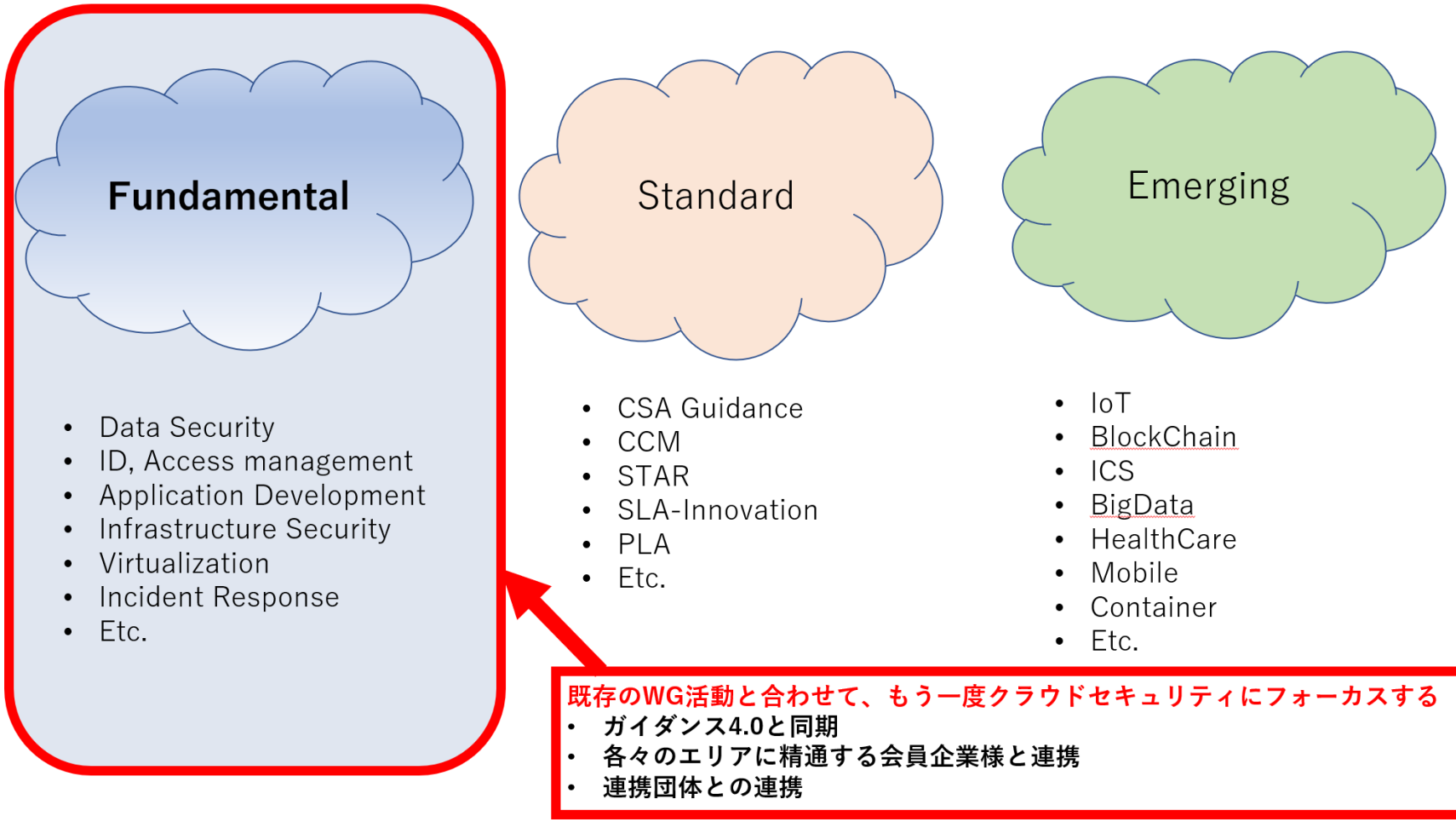
〈参考〉



# CSAジャパンで活動中のWG

- Big Data ユーザWG
- 医療情報ユーザWG
- モバイルユーザWG
- IoT WG
- CCM/STAR WG
- SDPWG
- ガイダンス　WG
- CASB WG
- SLA Innovation WG
- Blockchain WG
- Cloud Data Center Security WG
- クラウドプライバシー WG
- クラウドセキュリティ WG

# 2017年度　WG活動イメージ



# クラウドセキュリティWG

- 目的
  - クラウドセキュリティの各分野に対して、推奨事項、技術的対策についてフォーカスし、クラウドセキュリティとして、技術的なベースラインを明確にすることで、より安全なクラウド利用に向けてのガイドラインを作成する
- 対象とするクラウドセキュリティの分野
  - インフラセキュリティ
  - データセキュリティ（暗号化を含む）
  - ID、アクセス管理
  - アプリケーション開発
  - 仮想化
  - インシデント管理

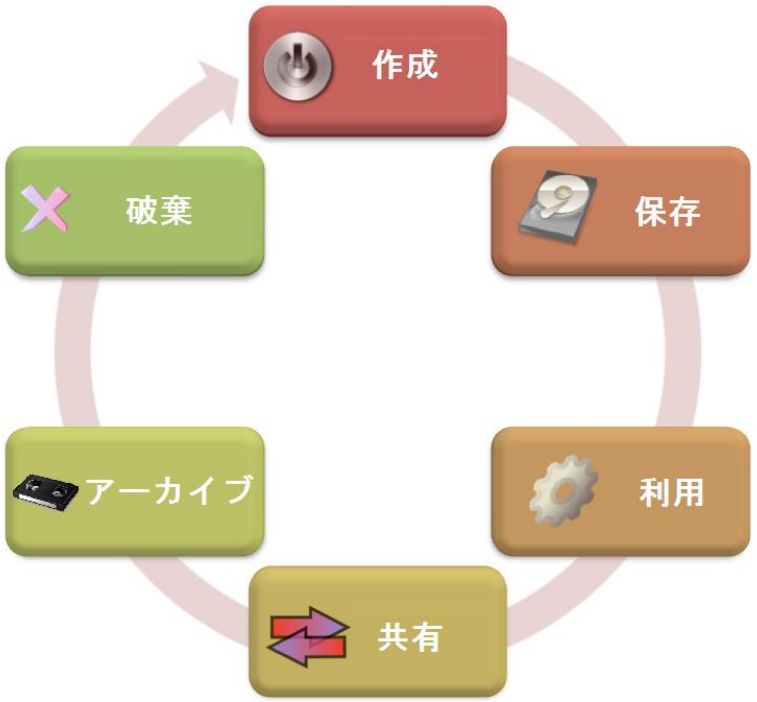
# インフラセキュリティ　考慮点

- IaaS
  - パッチ適用、不要なサービスの停止などのホストの安全化
  - クライアントとクラウドの間の通信の暗号化
  - サーバ接続に用いるホスト鍵の保護
  - アクセスできる人を限定する
  - プラットフォームのセキュリティ対策について、プロバイダに確認する
- PaaS
  - アプリケーション設計を厳密に行う。アプリケーションに必要なセキュリティ機能を組み込む。
  - プラットフォームのセキュリティ対策について、プロバイダに確認する
- SaaS
  - プロバイダのセキュリティ対策について、プロバイダに確認する

# データセキュリティ　考慮点

データセキュリティライフサイクル

- 各フェーズにおけるデータセキュリティ
  - 作成（Create）
    - データの作成/変更/更新/修正
    - 情報の機微性、価値に基づいて分類
  - 保存（Store）
    - データベース、ストレージ等にデータを格納
    - データの保護（暗号化、アクセス管理）
  - 利用（Use）
    - データの利用（アプリケーション等）
    - モニタリング、アクセス制御（DLP、DRM）
  - 共有（Share）
    - 他のユーザとデータを共有
    - ポリシー、DLP
  - アーカイブ（Archive）
    - 使用頻度の落ちたデータの保管
    - 「保存」と同じレベルのデータ保護
  - 破棄（Destroy）
    - データの完全な削除・破棄（物理的あるいは論理的）
    - 法律、規制にも注意が必要
    - 利用者側での破棄：　クリプトシュレッディング




（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　V3.0から引用）

# ID、アクセス管理　考慮点

クラウド環境での課題

- 機密情報がファイアウォールの外に出ていることを前提としたポリシー設定およびセキュリティ対策が必要
- 様々なデバイス、様々な場所からのアクセス
- クラウドサービスごとに必要となるID、アクセスの管理

クラウド環境でのID,アクセス管理の推奨事項

- 連携（フェデレーション、Federation）
- プロビジョニング

新しいテクノロジー

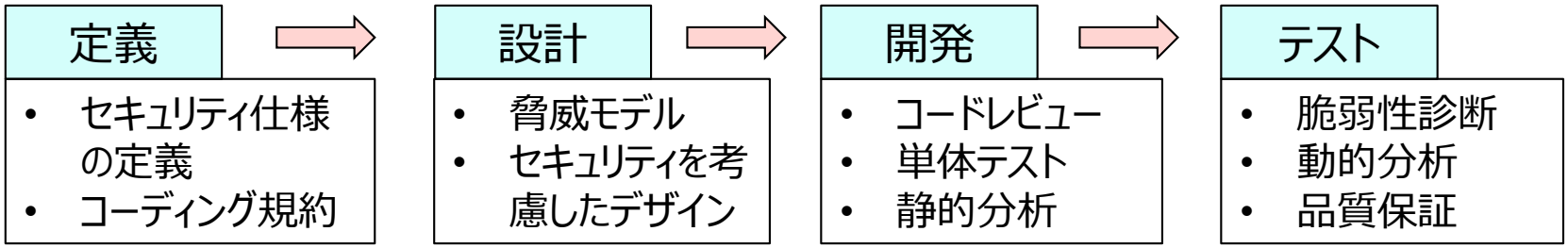
- IDaaS（ID as a Service）
- ID、アクセス管理をクラウドで展開

# アプリケーション開発　考慮点

ソフトウエア開発ライフサイクル（Software Development LifeCycle, SDLC）

- 定義
  - ビジネスおよびセキュリティ要件を決定
  - アプリケーションの目的、ビジネス要件を満たすために必要なことを定義
- デザイン
  - 脅威モデル、セキュリティを考慮したデザイン
- 開発
  - コードレビュー、ユニットテスト、静的分析
- テスト
  - 脆弱性診断、動的分析、機能テスト、品質保証（QA）

**＊セキュリティチームが、開発のすべてのフェーズに関わることが重要**



# 仮想化　考慮点

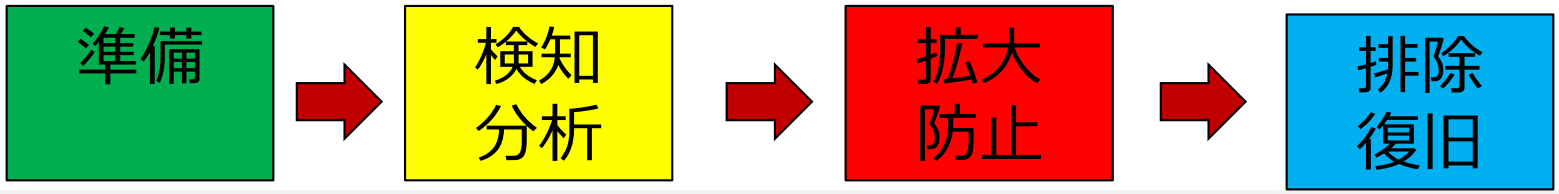
## 仮想化環境のセキュリティ

- ハイパバイザのセキュリティ
  - ハイパバイザの構成管理、運用管理の徹底
    - ログの監視等
  - ハイパバイザの脆弱性対策
    - パッチ適用等
- ゲストVMのセキュリティ
  - 仮想マシンの暗号化（イメージに対する改ざんの防止等）
  - VMの移動時の管理

# インシデント管理　考慮点

インシデント管理プロセス

- 準備
  - データの処理、保存場所等の確認
  - プロバイダとのSLA,契約の理解
    - プロバイダの連絡先、役割、責任、インシデントの連絡方法等
  - インシデント管理の計画を立てる
- 検知、分析
  - データの入手、解析
    - プロバイダ提供のデータと利用者が収集するデータの両方
  - フォレンジック
- 拡大防止
  - 利用者の責任において実施。プロバイダは支援する
  - インスタンスの一時停止、アクセス制御等
- 排除と復旧
  - 利用者の責任において実施。プロバイダは支援する

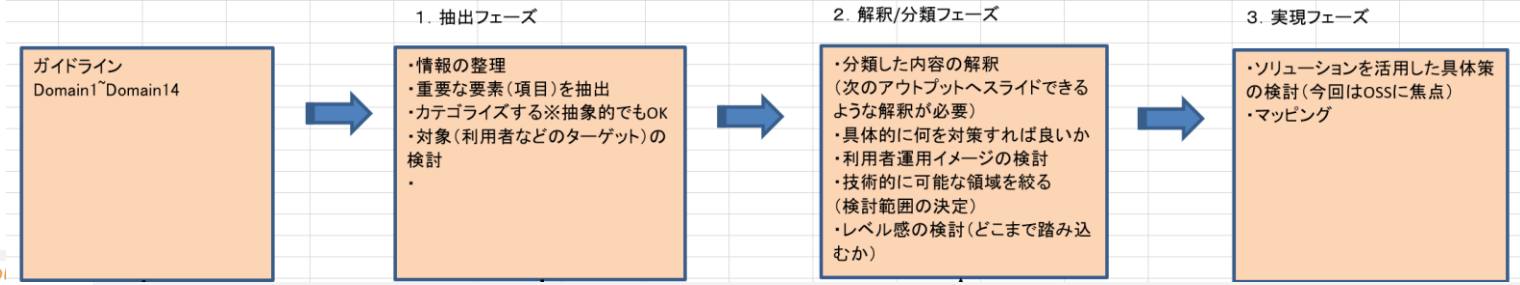


# クラウドセキュリティWG　課題

- 新たにガイドラインが必要か？
  - すでに、CSAのガイドラインがあり、また、様々な団体がガイドライン的な資料を公開している状況で、新たなガイドライン（解説本）は不要？
  - クラウドセキュリティは、すでに、提案書ベースでビジネスとして進めている段階になっている。つまり、ビジネスとしての実装段階である。
  - 実装に向けて専門家を育てていく段階であり、新たなガイダンスを作る段階ではない。
  - 製品を含めたリファレンスを作成するということであればメリットがある。ただし、ベンダーニュートラルにする必要がある。
- クラウドセキュリティWGの意義はあるのか？
  - すでに知識のある人にとっては、新たなガイドラインを作成することに関するモチベーションは少ない。
  - ボランティアベースのWGとして、参加者にメリットがある活動にするにはどうすればよいか？
    - 新しいトピックが必要（例：IoT、BlockChain）。

# クラウドセキュリティWG アプローチ

1. 抽出フェーズ
   - ガイドラインから、フォーカスすべき要素を抽出
   - 抽出した要素のカテゴリ分け
2. 解釈/分類フェーズ
   - 各要素の内容の理解
   - 利用者運用イメージの検討
   - 技術的対策について検討
3. 実現フェーズ
   - ソリューションを活用した具体策の検討
     - OSSベースでのソリューションのマッピング、解説



# 専門家を育てていく取り組み

- CSAアカデミーの開始
  - 2017年度当初目標の実現
  - クラウドセキュリティのリテラシ向上の取り組み。
  - 会員のCCSK取得を支援
  - 新しいガイダンス4.0を活用

*クラウドセキュリティWGの活動、CSAアカデミーを両輪にして、クラウドセキュリティそのものの底上げを図っていきたい。*



# *Thanks!*