



2021年9月15日

30分でわかる！ AWS 基本的なセキュリティ



自己紹介

□ 馬場 潤一 (Junichi Baba)

□ 株式会社スタイルズ

- ▶ AWS上でのアプリ開発・インフラ構築
チームリーダー

□ 好きなAWSサービス

- ▶ CloudFormation、Systems Manager



本日、お話しする内容

□対象

- ▶ これからAWSを使おうと考えているがセキュリティ的に不安
- ▶ AWSを使い始めたので最低限のセキュリティ対策を知りたい

□ゴール

- ▶ AWSクラウド基盤のセキュリティレベルを知る
- ▶ AWSのセキュリティに関する責任範囲を知る
- ▶ 初歩的なセキュリティ設定を知る

AWSクラウド基盤のセキュリティレベル

AWS データセンターのセキュリティ

▶ データセンターへの入場

- ・ 入場は許可制、アクセスが必要な最小限のデータセンターレイヤーを指定して申請
- ・ 権限を持つ人物のみが承認
- ・ 期限が過ぎたらアクセス取り消し



▶ データセンター設備

- ・ カメラによる録画
- ・ 許可された方法以外での侵入を検知
- ・ 電力やネットワーク設備の冗長化
- ・ 火災検出、漏水検出等の仕組み
- ・ 安全なメディアの廃棄

NIST（アメリカ国立標準技術研究所）の
ガイドラインに準拠

AWS セキュリティ認証

▶ 第三者によるセキュリティ認証

- ・ 様々な認証を取得（下記は一例）



AWS ネットワーク、セキュリティ機能

▶ 様々なネットワーク接続が選択できる

- ・インターネット
- ・VPN
- ・専用線

インターネット接続のない
閉じたネットワークも構成可能

▶ セキュリティ機能

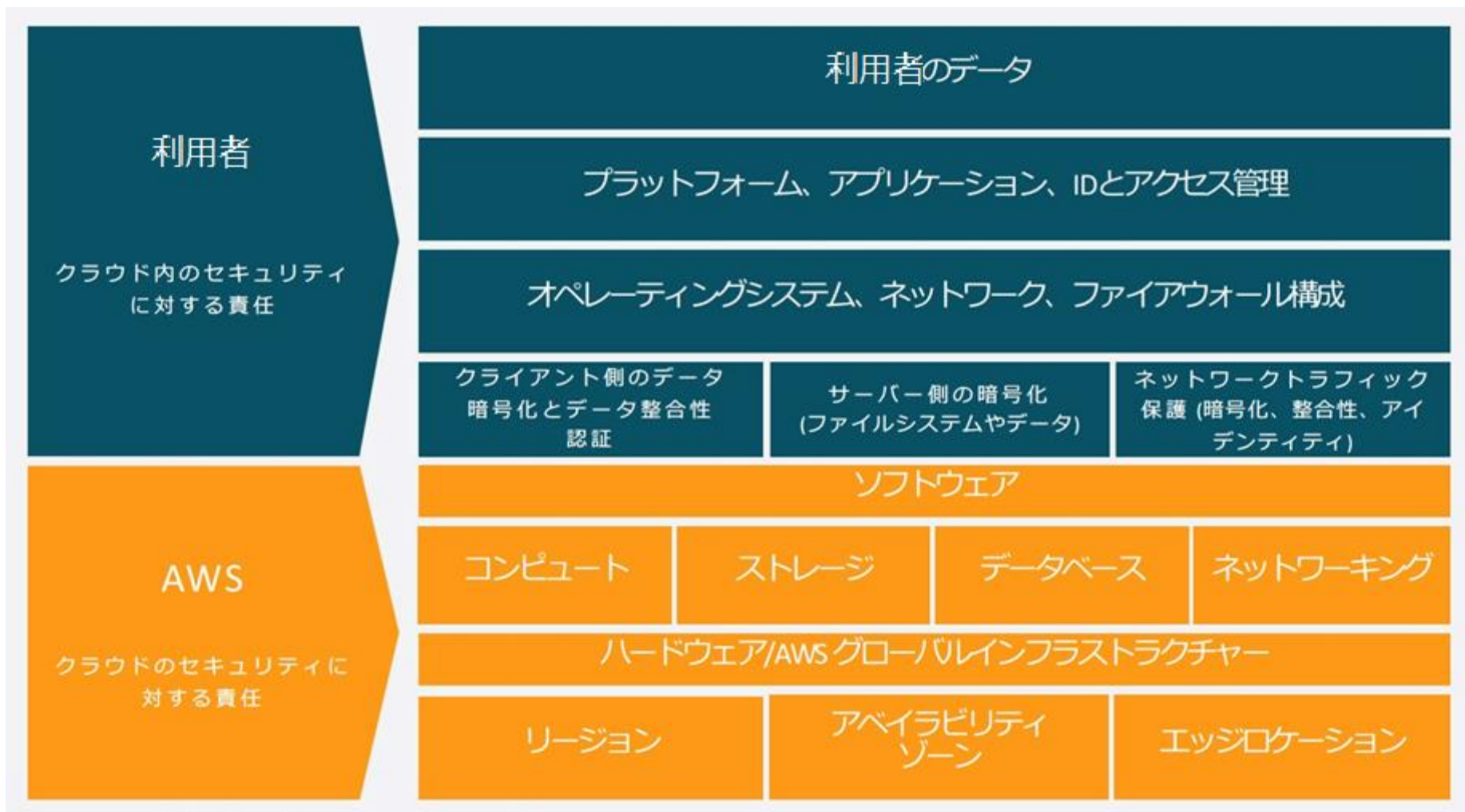
- ・ 監査ログ保管、WAF、不正アクセス検知、マルウェア検知、脆弱性検知、ディスク暗号化 等の対策を導入可能
- ・ マネージドサービスとして提供

サーバ、OS、ソフトウェアはAWSが管理運用

AWSのセキュリティに関する責任範囲

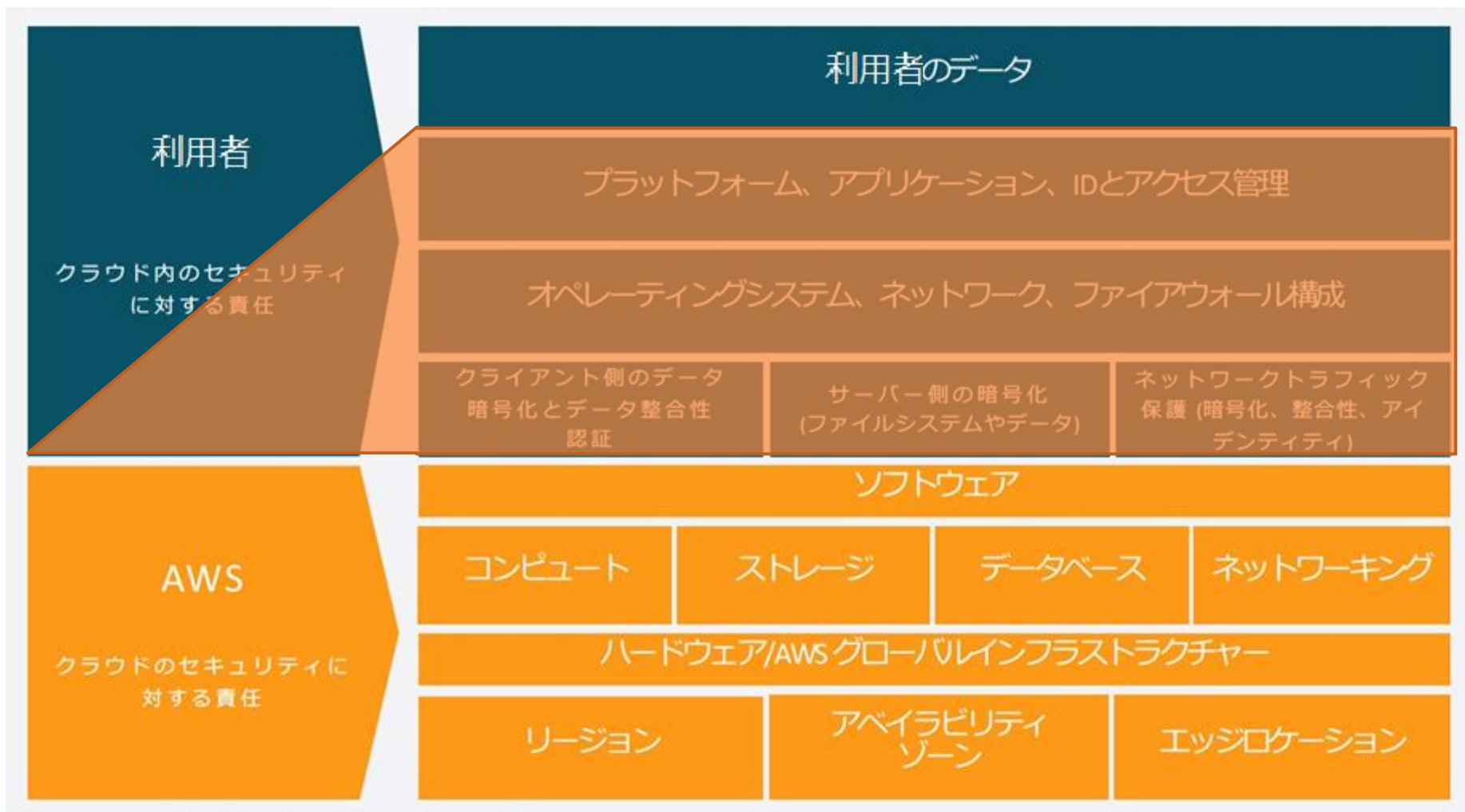
責任共有モデル

AWSが責任を持つ部分とサービス利用者が責任を持つ部分を明確に分ける考え方



責任共有モデル

マネージドサービスを利用する事で、ユーザの責任範囲は縮小する



初歩的なセキュリティ設定

アカウント

➤ Rootアカウントは利用しない

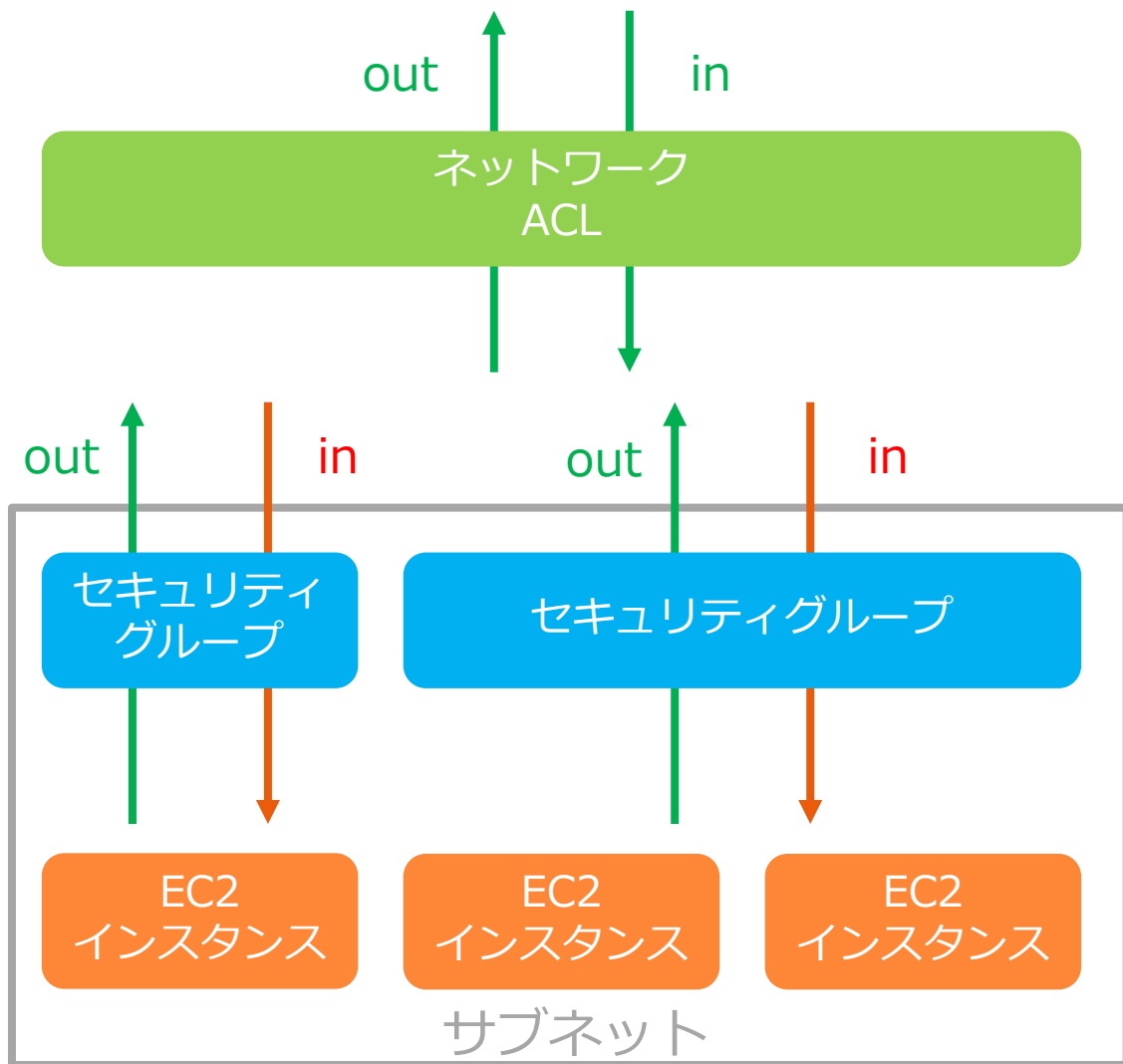
- ・ Rootアカウント = AWS申込時に作成するアカウント（メールアドレスとパスワード）
- ・ 強権限を有するため、漏洩時のリスク大
- ・ MFA（多要素認証）を設定して利用しないように

➤ IAMを個人単位で作成&最小権限

- ・ IAM（アイアム） = AWSリソースへのアクセスを管理するサービス
- ・ 監査ログにはIAMユーザ単位で行動履歴が記録
- ・ 最小権限を与えることで、漏洩時のリスクを低減

細かすぎると管理負荷が増える・・・

ネットワークACL と セキュリティグループ



【ネットワークACL (アクセスコントロールリスト)】

- ・サブネット単位の制御
- ・ステートレス（通信の返りも明示的に設定）
- ・許可/拒否を指定
- ・デフォルト：in out 制限なし

【セキュリティグループ】

- ・インスタンス単位の制御
- ・ステートフル（通信の返りは動的に許可）
- ・許可のみを指定
- ・デフォルト：in : 許可なし
out : 制限なし

ネットワークACL と セキュリティグループ

➤ (個人的に) 推奨する設定方針

- ・ ネットワークACLはサブネット単位でゆるめに制限
構成や規模によっては設定しないケースも多い
- ・ セキュリティグループで通信ポートと送信元IPで細かく制御

ステートレスで細かい制御はツライ

Type ▼	Protocol ▼	Port range ▼	Source
すべてのトラフィック	すべて	すべて	0.0.0.0/0

インバウンドで通信全開放はNG！

まとめ

まとめ

□ AWSのクラウド基盤としてのセキュリティレベルを知る

- ▶ 厳密な管理と障害を考慮したデータセンター
- ▶ 第三者認証を数多く取得
- ▶ 様々なネットワーク構成、セキュリティ機能を簡単に利用できる

□ AWSのセキュリティに関する責任範囲を知る

- ▶ 責任共有モデルという考え方
- ▶ マネージドサービスを利用する事で、ユーザ側の責任範囲と管理負荷は縮小

□ 初歩的なセキュリティ設定を知る

- ▶ rootアカウントは使用しない
- ▶ IAMアカウントを個人単位で作成 & 最小限の権限
- ▶ ネットワークACLとセキュリティグループを利用して通信制御



**実績豊富なエンジニア集団の技術と開発ツールで
「開発期間/コスト削減」「品質向上」を実現**

株式会社スタイルズ

<https://www.stylez.co.jp>

東京都千代田区神田小川町1-2 風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進