【議事3】 梅谷委員プレゼン資料

クラウドの技術を活用した監査

2017/03/23
梅谷晃宏
Amazon Web Services Japan K.K.

クラウドを使うことの利点

システム上の利点

- IT資産を資本経費から変動経費に変更可能。ITコストの最適化
- クラウドベンダーのもつ資産のスケーラビリティを活かせる
- IT適用のスピード向上と効率化
- クラウドベンダーが展開するグローバルインフラを活用可能

統制上の利点

- セキュリティ、コンプライアンス面で監査済みのインフラ
- 構成や操作のログの取得容易性
- 監査や監視の自動化が可能
- セキュリティ/コンプライアンス/品質要件を設計段階から織り込むことが可能
- 可用性を考慮した設計が容易

クラウドの技術の要点

プログラミング可能なインフラストラクチャ

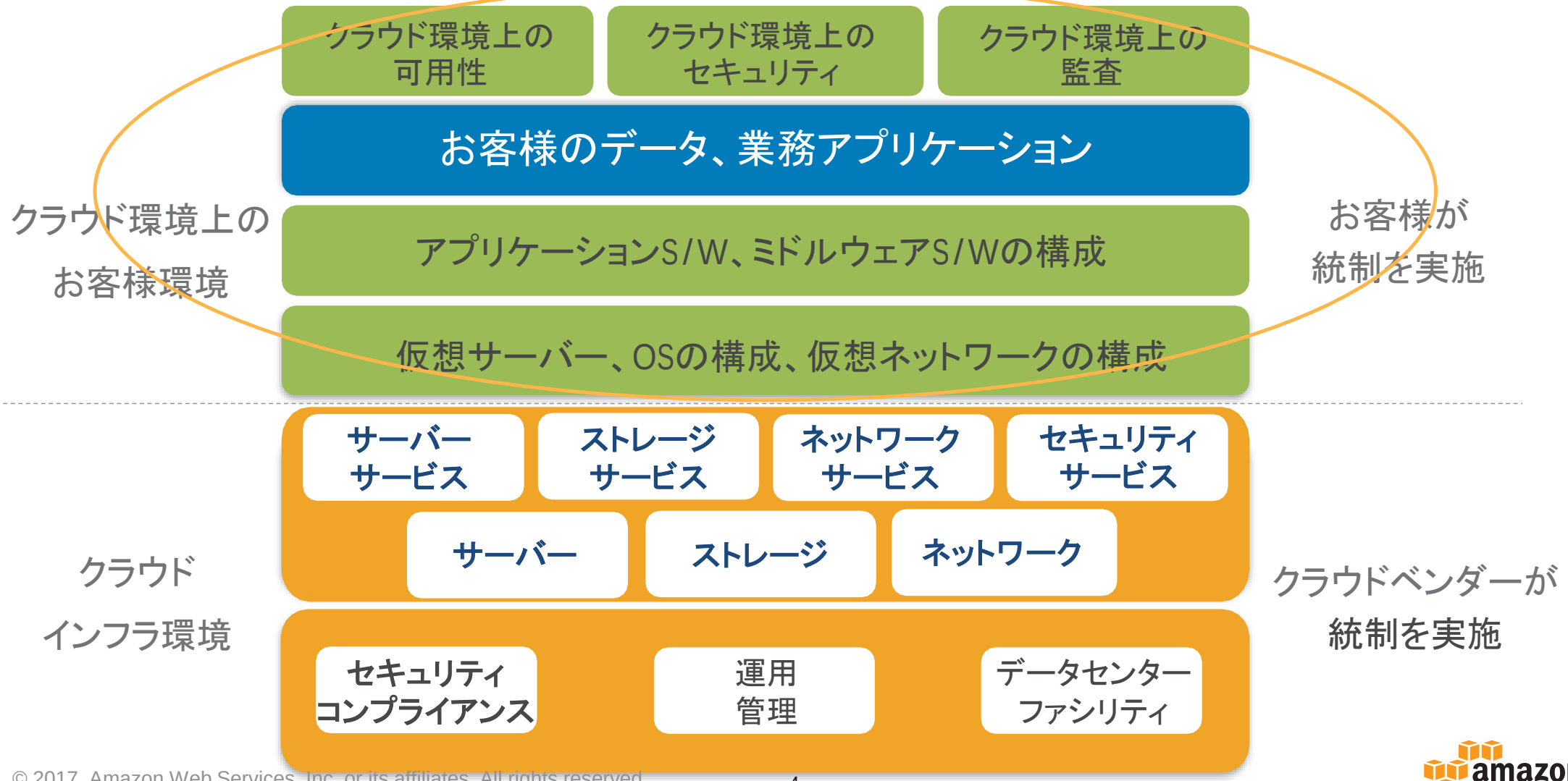
物理環境からの仮想的なデバイス群とデータの分離度、抽象度が非常に高い

従来の仮想環境よりもS/W上で定義可能な内容が幅広く、柔軟性が高い

手動で実施していた運用手順等のプロセスをコードで書くことで自動化が可能

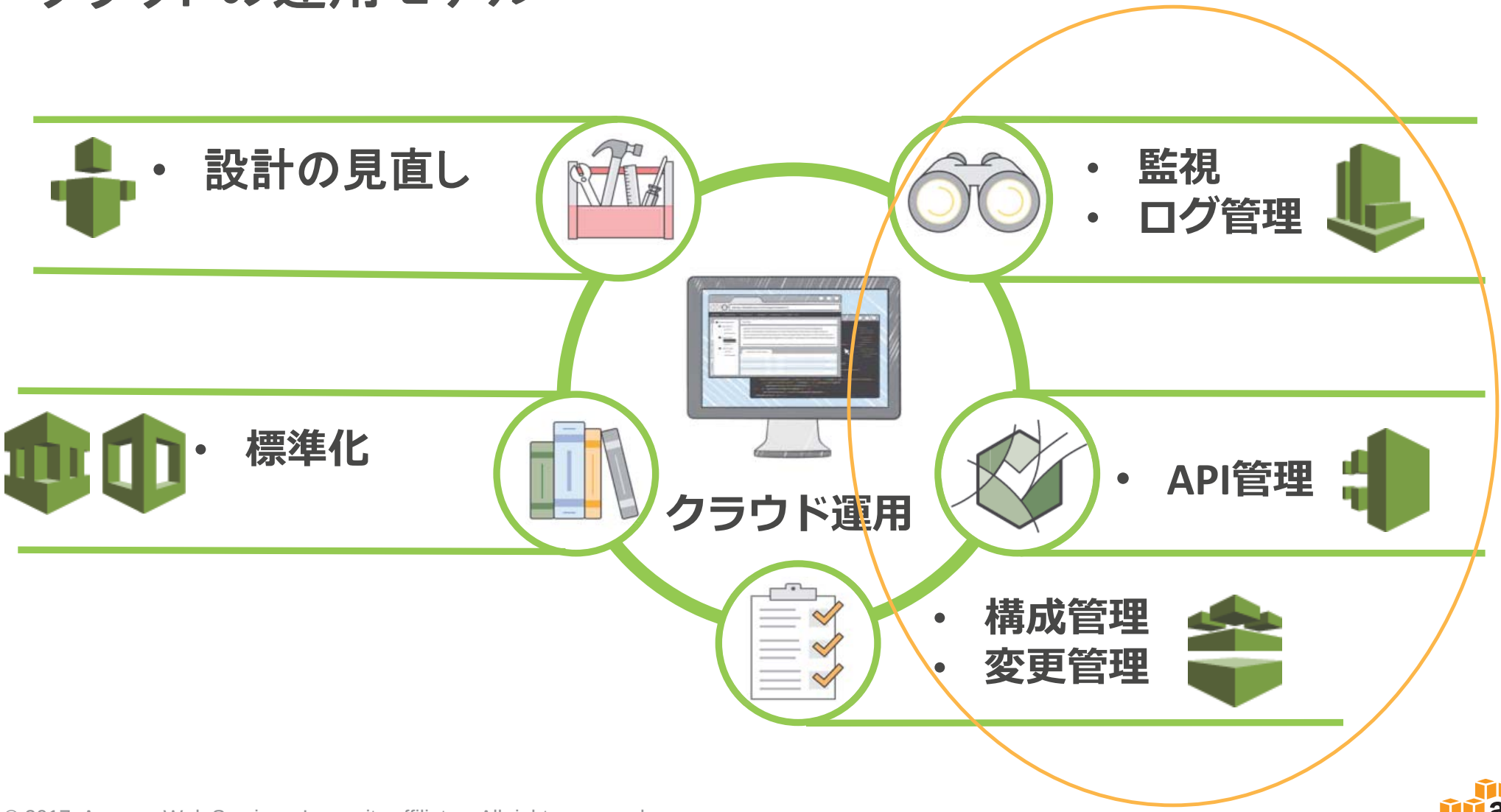
amazon web services

クラウドの責任共有モデル



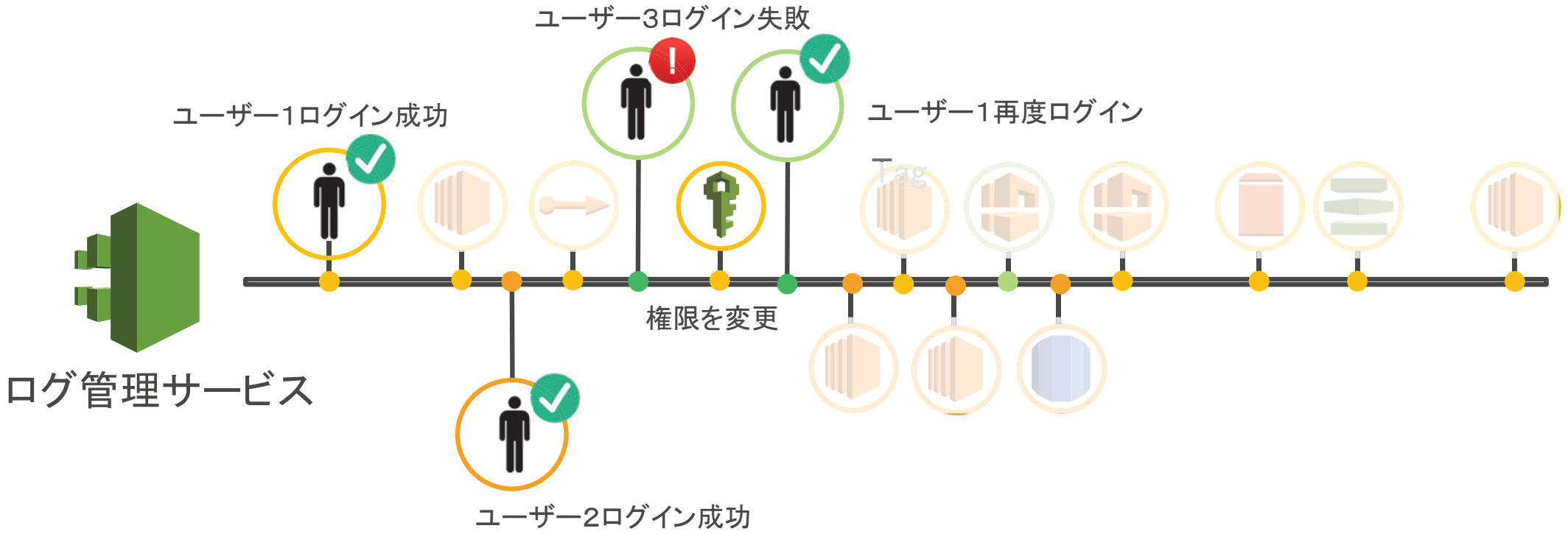
amazon web services

クラウドの運用モデル



amazon web services

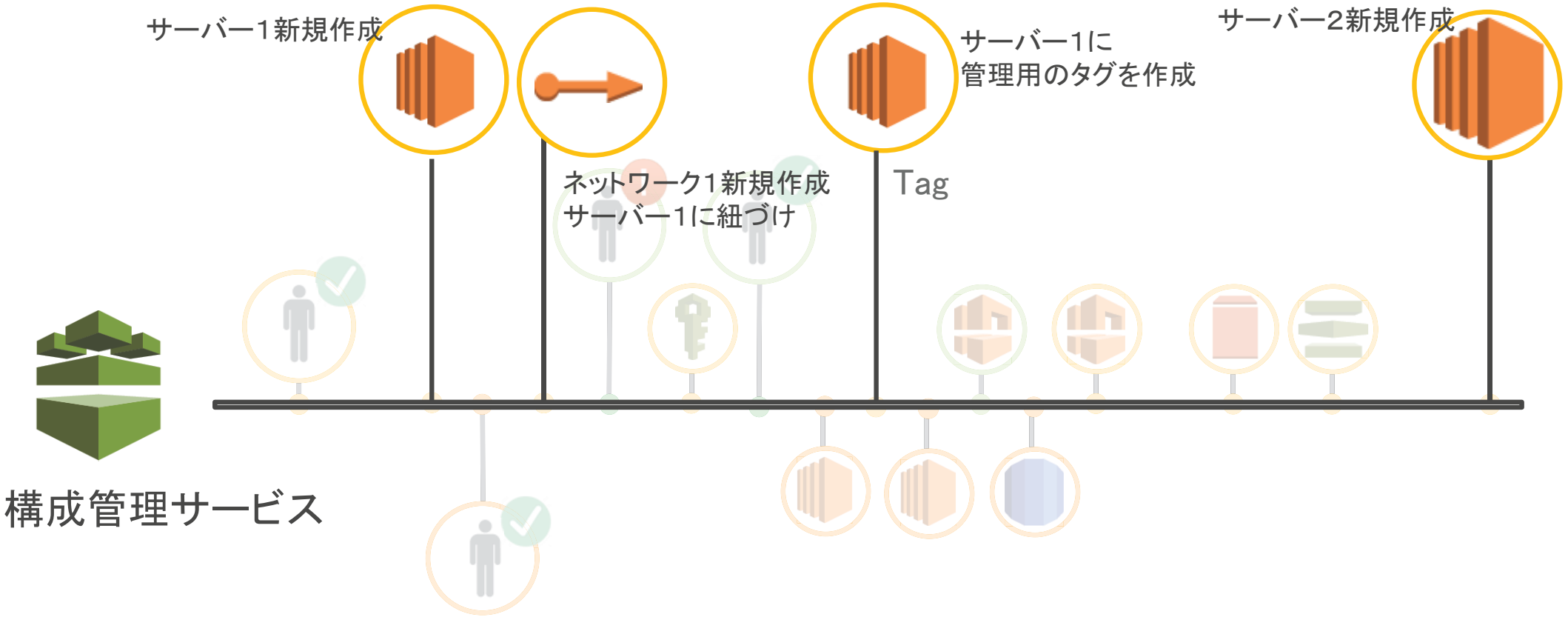
クラウド環境上におけるユーザー活動



”ユーザーアクティビティ“ を切り口に時系列ベースでロギング

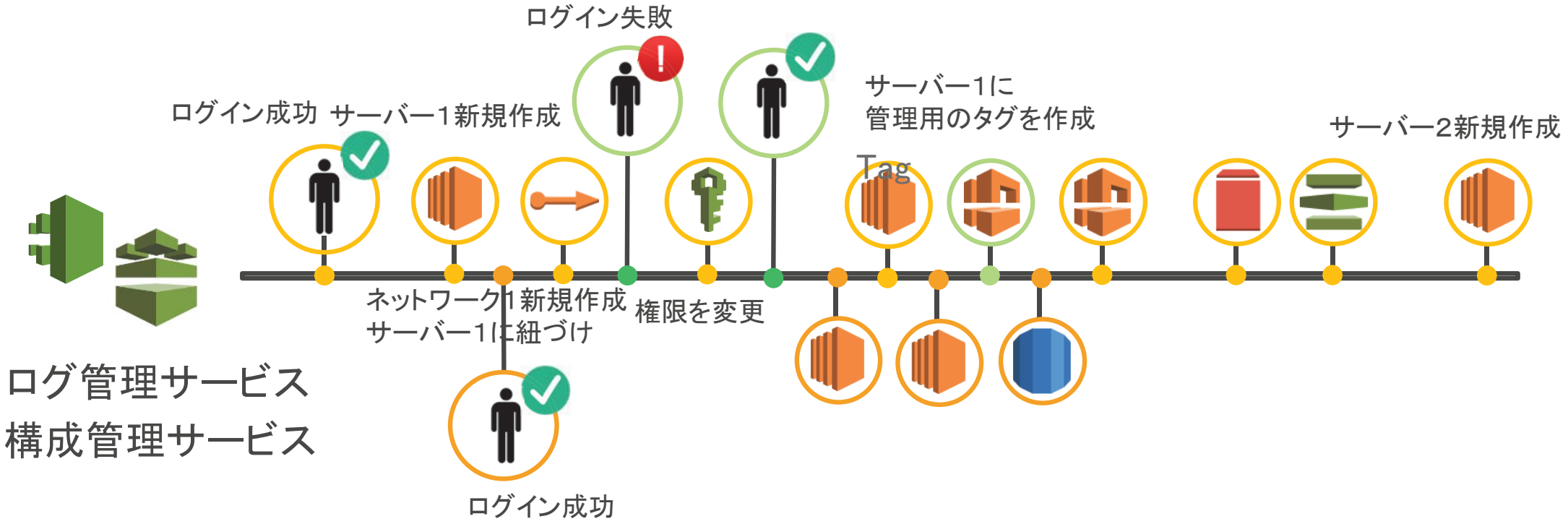
amazon web services

クラウド環境上における構成要素の変更



”クラウド上の構成要素“ を切り口に時系列ベースでロギング

クラウド環境上での様々な主要な活動をログとして取得



”クラウド上の構成要素“ に対して、どのような
”ユーザーアクティビティ“が実行されたのか把握可能

amazon web services

構成管理、ログ管理サービスによるポリシー適合の評価

ポリシーに従って、準拠すべきルールを事前に設定し、その内容に沿った構成変更が実施されているか、逸脱はないか等の評価、監視、通知を自動化することが可能

- ポリシー上必須とされているストレージの暗号化が実施されているか
- 仮想サーバーに運用管理上必須のタグが一意に設定されているか
- 管理者権限でのログインと実行
- ユーザー認証失敗
- ユーザー操作権限やアクセス設定の変更
- 仮想サーバー、仮想ネットワークの構成変更監視
- ネットワーク上のパケットログの監視

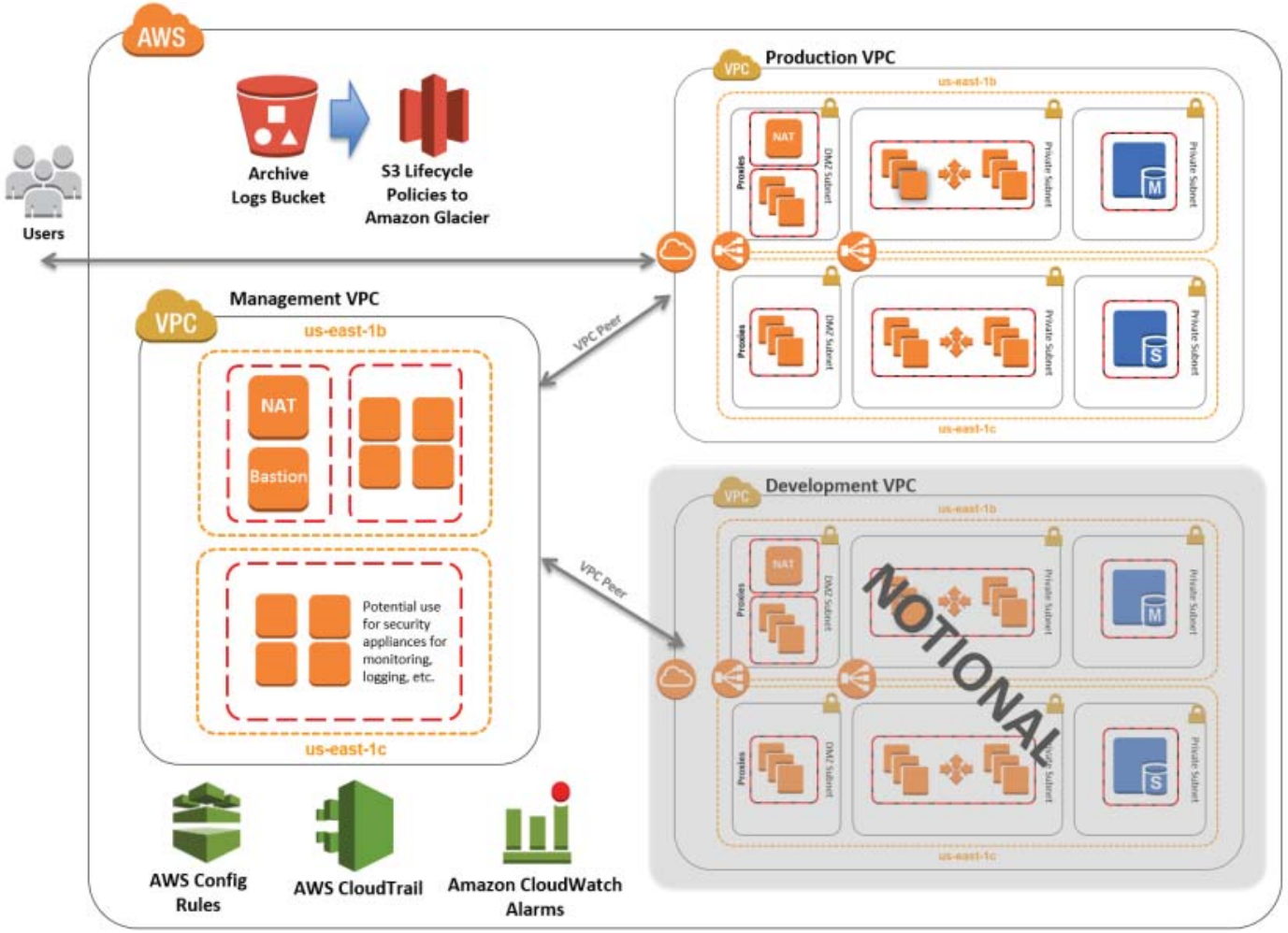
PCI DSSの要求事項とクラウド機能、要素のマッピング

PCI DSS Requirements v3.0	Milestone	Applicable in AWS Reference Architecture	Description of AWS Implementation	AWS Resource Type(s)	AWS CloudFormation Template Name (Stack)	Additional AWS Guidance
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	N	N/A	N/A	N/A	N/A
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1	Y	Architecture Diagram in the Deployment Guide	N/A	N/A	Applies to operational procedures/practices
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	1	Y	Architecture Diagram in the Deployment Guide	N/A	N/A	Applies to operational procedures/practices
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the Internal network zone	2	Y	Segmented using Security Groups in VPC, use of a VPC public subnet to simulate a traditional DMZ network zone	AWS::EC2::SecurityGroup AWS::EC2::NetworkAcl AWS::EC2::NetworkAclEntry	template-vpc-management template-vpc-production	N/A
1.1.5 Description of groups, roles, and responsibilities for management of network components.	6	Y	IAM configuration description and template	All resources in template	template-iam	N/A
1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2	2	N	N/A	N/A	N/A	N/A
1.1.7 Requirement to review firewall and router rule sets at least every six months.	6	N	N/A	N/A	N/A	N/A

https://aws.amazon.com/jp/quickstart/

amazon web services

PCI DSSの要求事項を織り込んだシステム全体のテンプレート



ログ取得、アーカイブ
システム構成変更
ユーザー権限設定
ネットワーク構成
サーバー構成
アクセス・権限設定

<u>セキュリティ要件や</u>
<u>監査要件を当初から</u>
<u>織り込んだシステム</u>
<u>構成が実装可能</u>

https://aws.amazon.com/jp/quickstart/

amazon web services

クラウドの技術を活用した監査

プログラミング可能なインフラストラクチャ

物理環境からの仮想的なデバイス群とデータの分離度、抽象度が非常に高い
従来の仮想環境よりもS/W上で定義可能な内容が幅広く、柔軟性が高い
手動で実施していた運用手順等のプロセスをコードで書くことで自動化が可能

ログ取得、構成変更取得、監視実行などの自動化が容易
様々なクラウド環境上での運用情報を取得し、ビッグデータ解析等で処理
従来発見できていなかったリスク、監査項目、監視項目の発見