AWS Summits 2014

Security Deep Dive

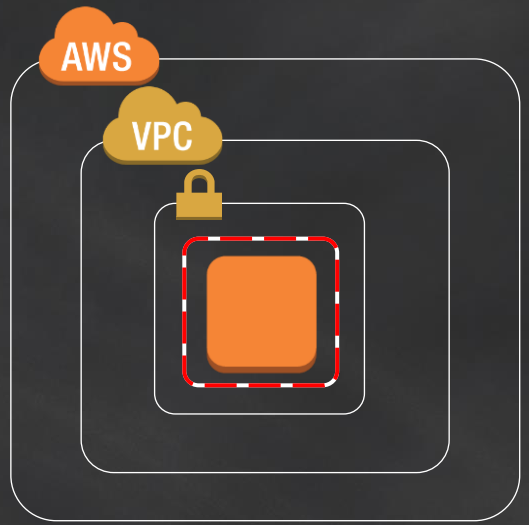
Tomomi Takada, Akihiro Umegai

July 14,2014

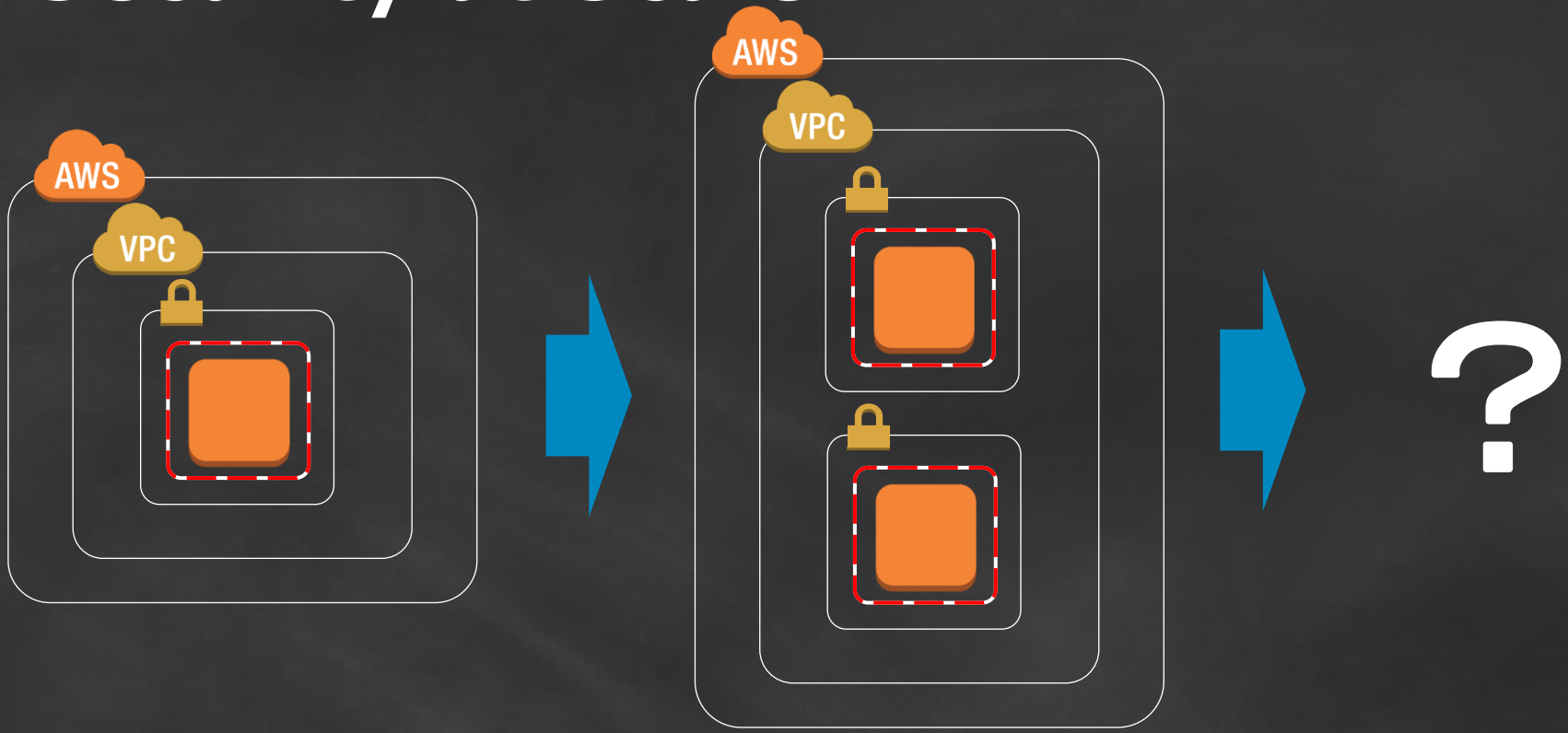
Session #TA-03

amazon web services

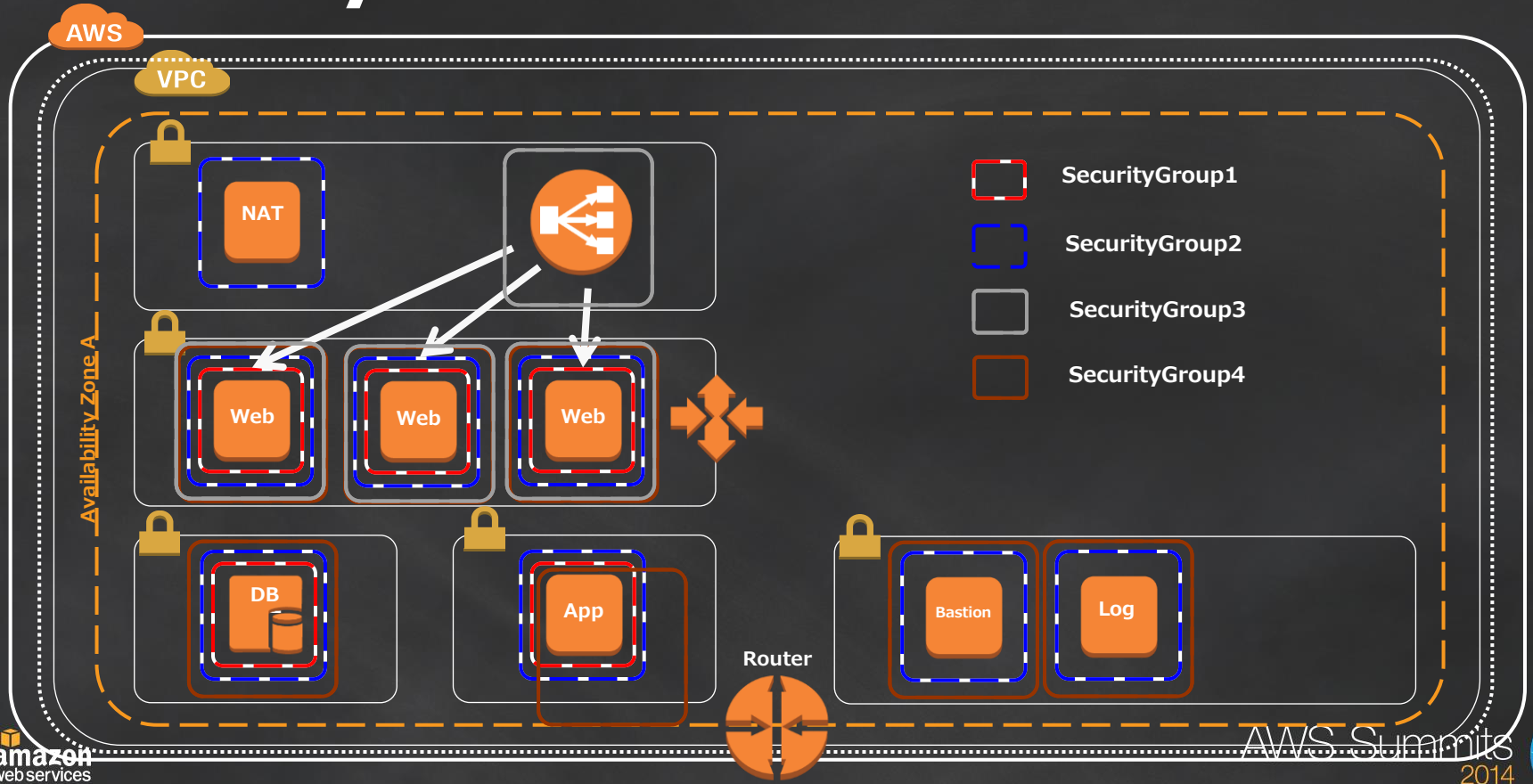
Security at Scale



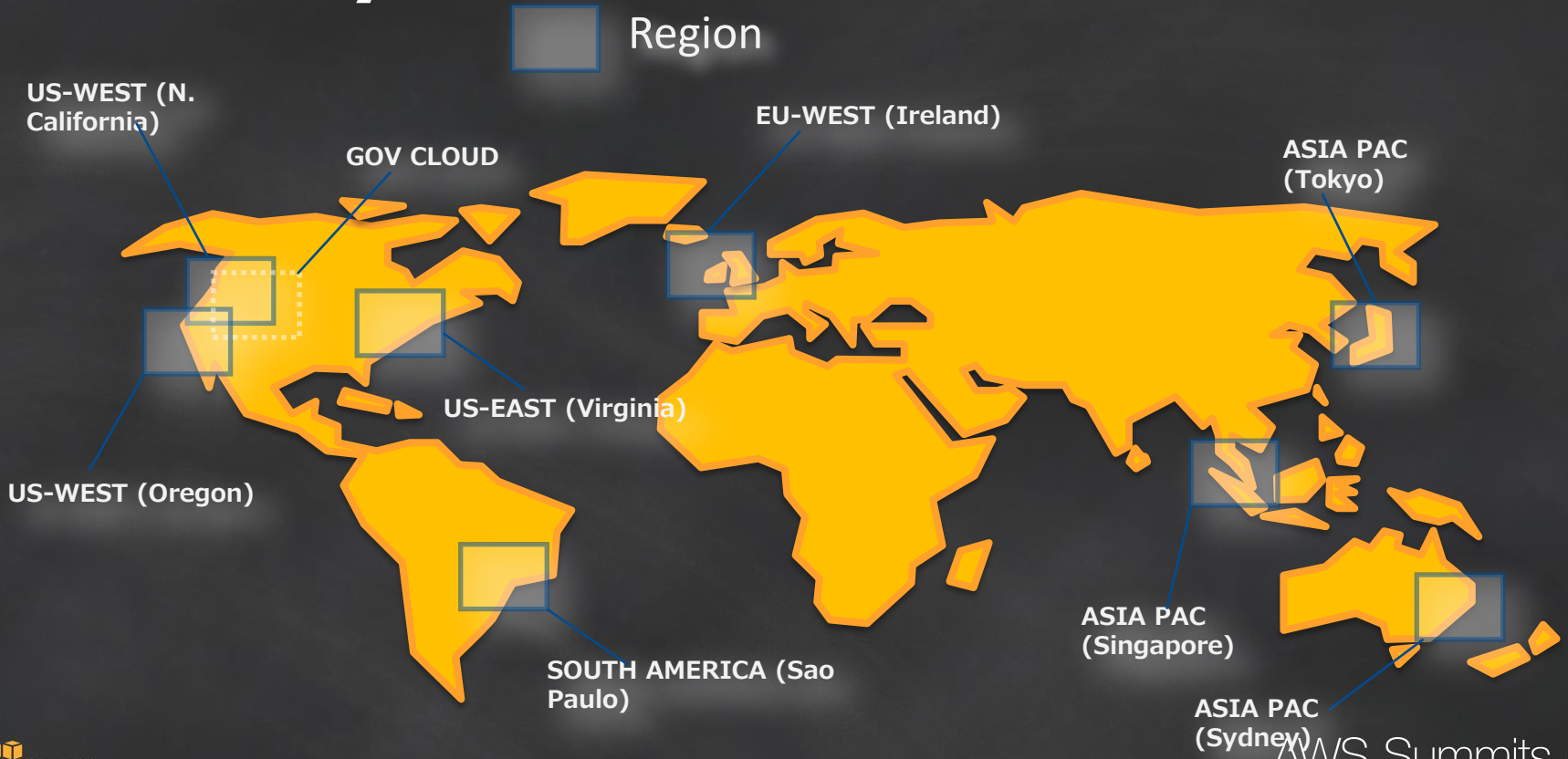
Security at Scale



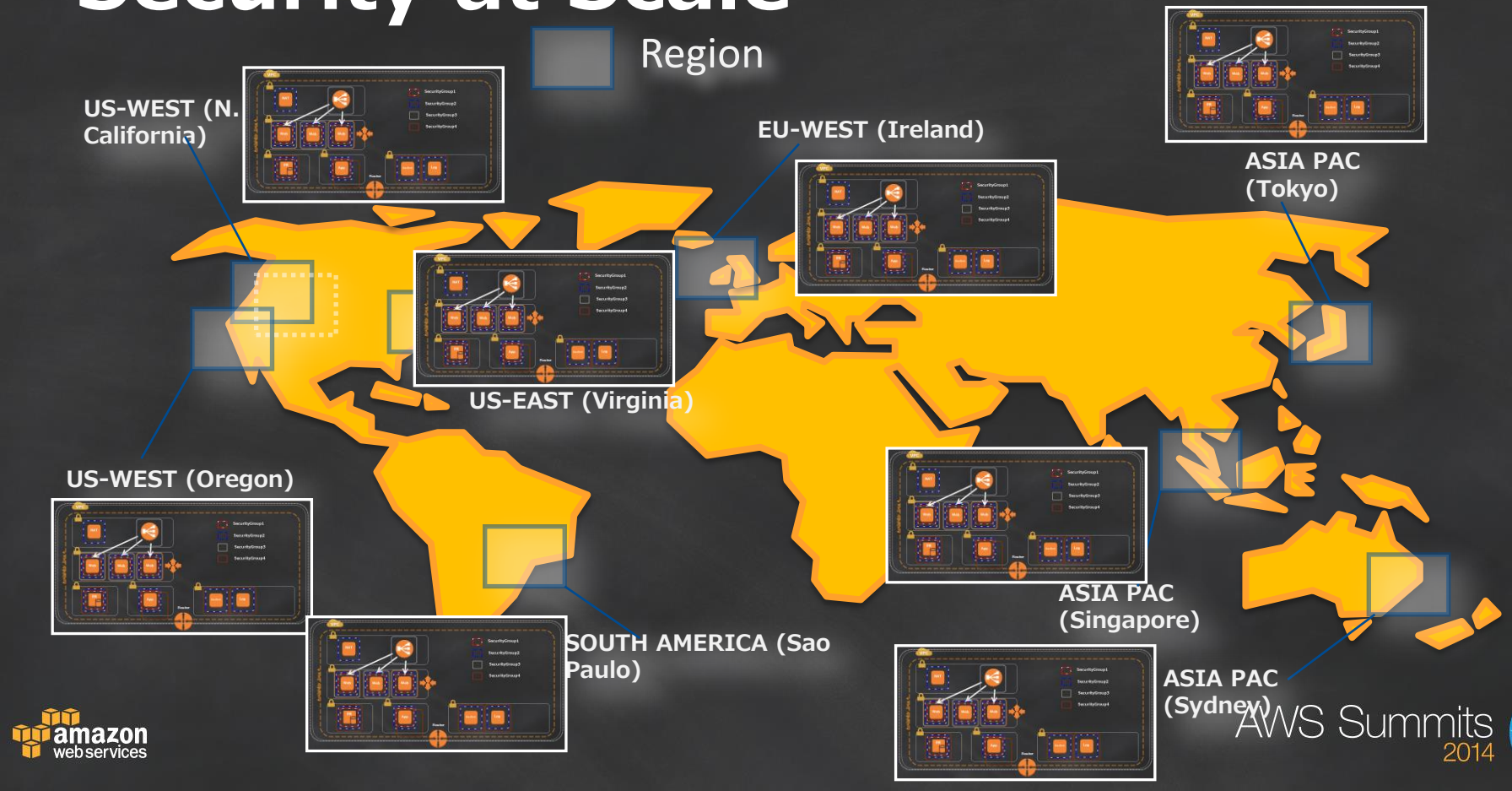
Security at Scale



Security at Scale



Security at Scale



Security at Scale

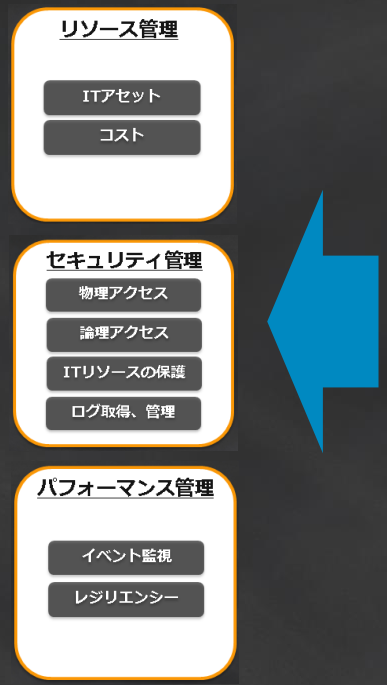
Security at Scale: Governance in AWS

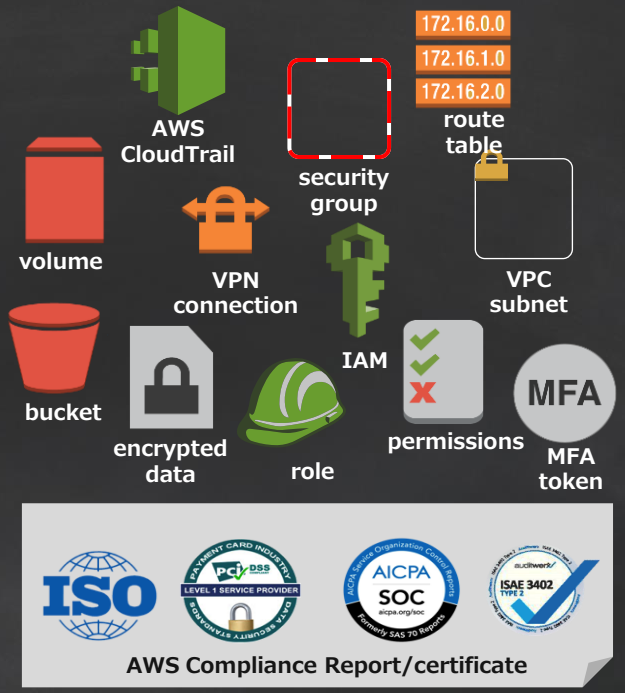
各ＩＴガバナンスの共通の主要な項目

http://aws.amazon.com/jp/compliance/

AWS “Built-in” Security feature

お客様固有の
ガバナンス/
コンプライアンス/
セキュリティ要件

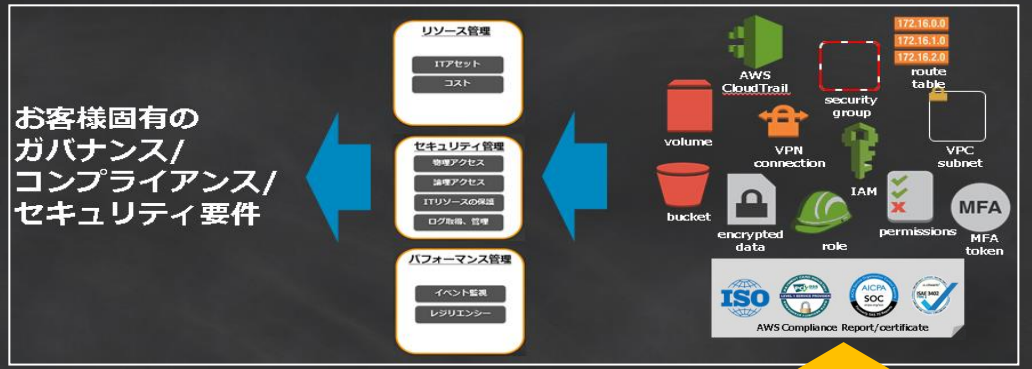




http://aws.amazon.com/jp/compliance/

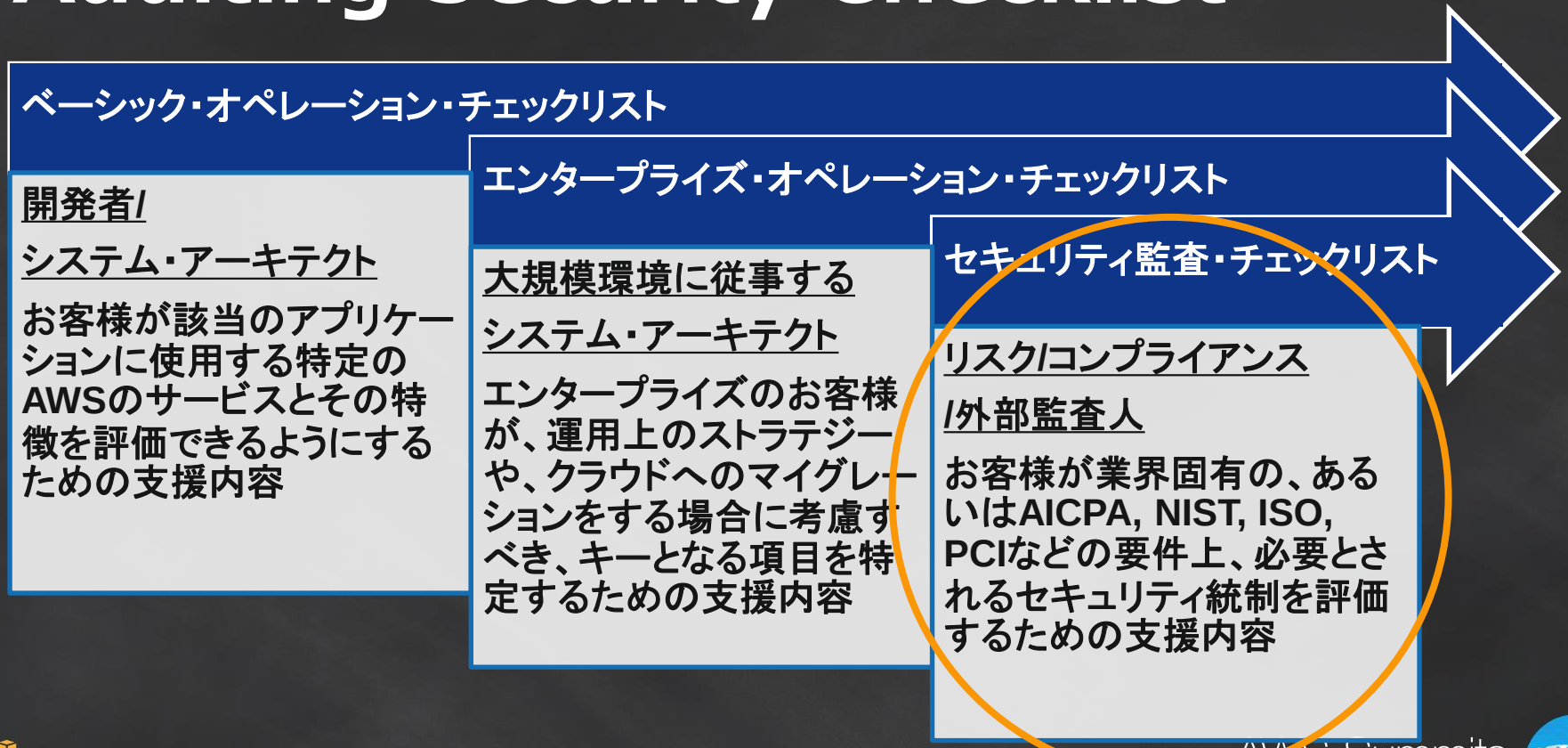
責任共有モデル

Security
IN the Cloud



Security
OF the Cloud

Auditing Security Checklist



http://aws.amazon.com/jp/compliance/

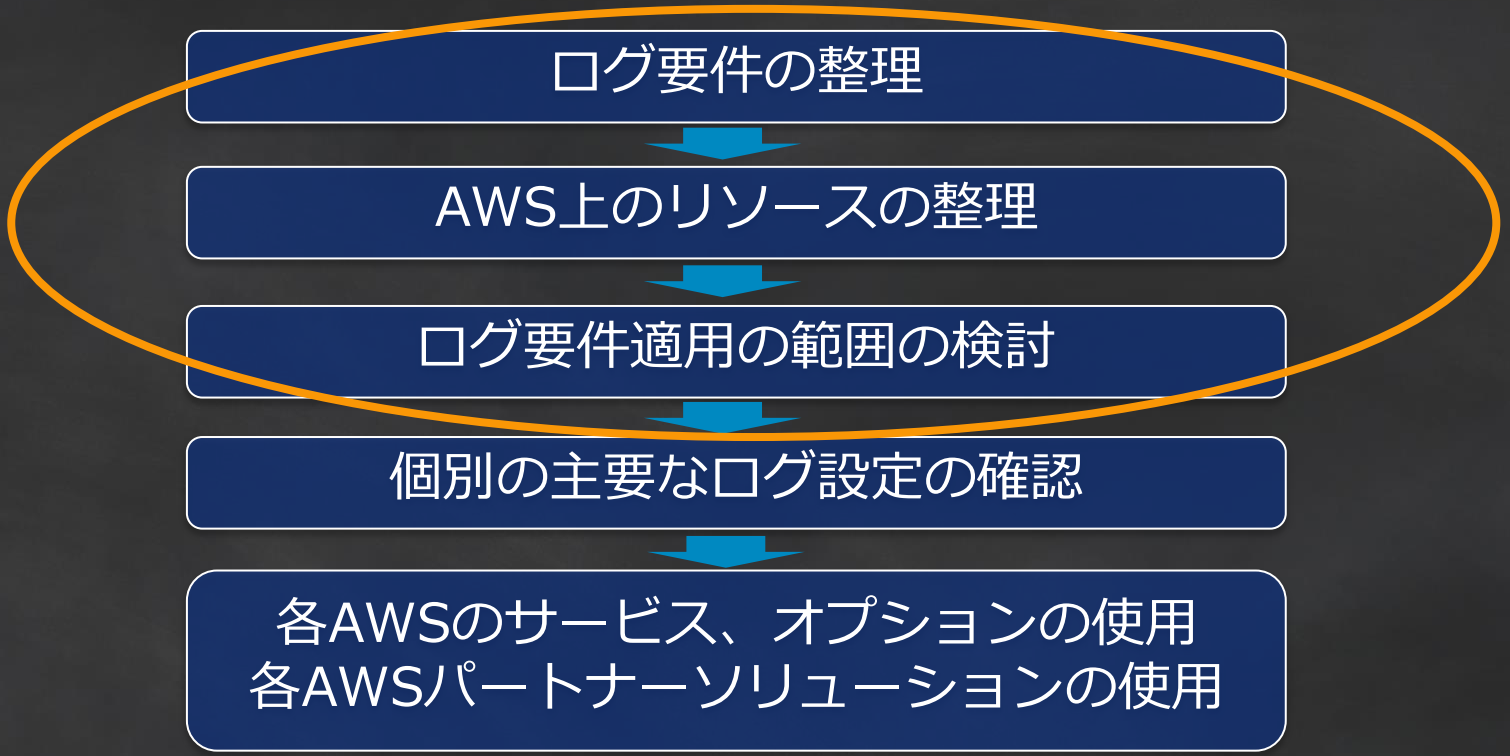
Auditing Security Checklist

資産の設定と管理	資産のセキュリティ、安定性、および整合性を保護するため、オペレーティングシステムやアプリケーションのセキュリティ上の脆弱性を踏まえた管理していますか?
論理アクセス制御	AWS環境上でユーザーとそのパーミッションがどのように設定されているか理解していますか? AWSアカウントに関連付けられている認証情報を安全に管理していますか?
データの暗号化	データがシステム上のどこに保存され、どのように保護されているか理解していますか?
ネットワークの設定と管理	AWS環境上のリソースに関連して、ネットワークアーキテクチャを理解していますか？
セキュリティログと監視	AWS環境上のシステムにおいて、適切なロギングとモニタリングが実施されていますか?
セキュリティインシデント対応	インシデント管理計画とプロセスに、AWS 環境内のシステムは含まれていますか?
障害復旧	障害復旧施策（DR, BCP）に、AWS 環境上のシステムは含まれていますか?

Auditing Security Checklist

資産の設定と管理	資産のセキュリティ、安定性、および整合性を保護するため、オペレーティングシステムやアプリケーションのセキュリティ上の脆弱性を踏まえた管理していますか?
論理アクセス制御	AWS環境上でユーザーとそのパーミッションがどのように設定されているか理解していますか? AWSアカウントに関連付けられている認証情報を安全に管理していますか?
データの暗号化	データがシステム上のどこに保存され、どのように保護されているか理解していますか?
ネットワークの設定と管理	AWS環境上のリソースに関連して、ネットワークアーキテクチャを理解していますか？
セキュリティログと監視	AWS環境上のシステムにおいて、適切なロギングとモニタリングが実施されていますか?
セキュリティインシデント対応	インシデント管理計画とプロセスに、AWS 環境内のシステムは含まれていますか?
障害復旧	障害復旧施策（DR, BCP）に、AWS 環境上のシステムは含まれていますか?

セキュリティログと監視



ログ要件の整理

コンプライアンス要件、組織固有のポリシー、
業務上の処理手順等を考慮し、該当環境のログ要件を決定

ログ要件のシナリオ例
- 特権的、あるいは強い管理者権限をもった個人によるすべての活動
- 不正、あるいは誤りによる論理的アクセスの試み
- 不正、あるいは誤りによるシステムリソースの変更
- 不正、あるいは誤りによるデータ資産へのアクセスや操作
- 監査証跡へのアクセスなどすべての操作
- Firewall等セキュリティ上重要なコンポーネントへの全ての操作

AWS上の資産の整理

AWS上のアセットのインベントリーを整理し、ログ取得の観点から、該当するどのAWS上のアセットにログ要件を適用するのかを決定。重要リソースについては、変更、追加、修正、削除等のどのようなログエントリーを取得するのか考慮。

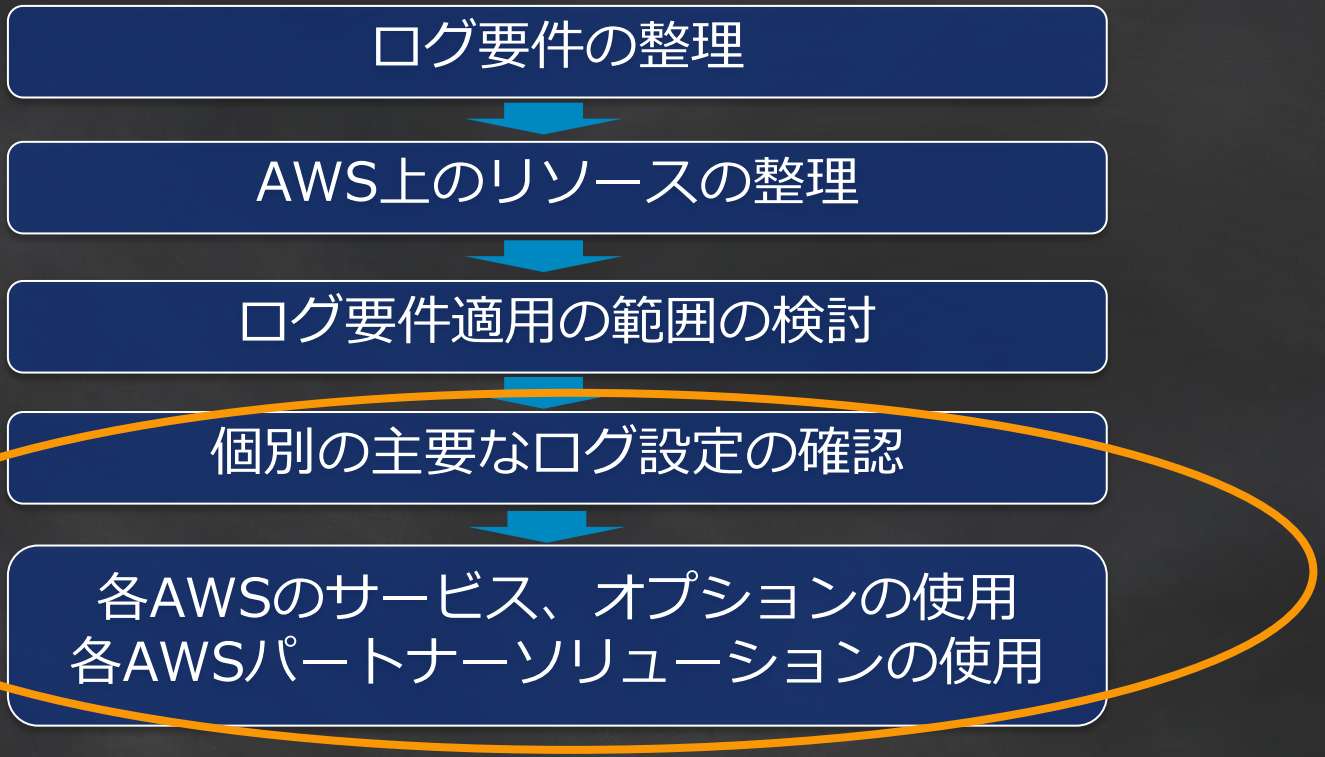
ログエントリーの例
- ユーザーＩＤ
- イベントの種類
- 日付と時刻 = タイムスタンプ
- 成功、失敗などの兆候
- イベントの発生元
- 影響の受けるデータ、システム・コンポーネント、各種リソース

ログ要件適用の範囲の検討

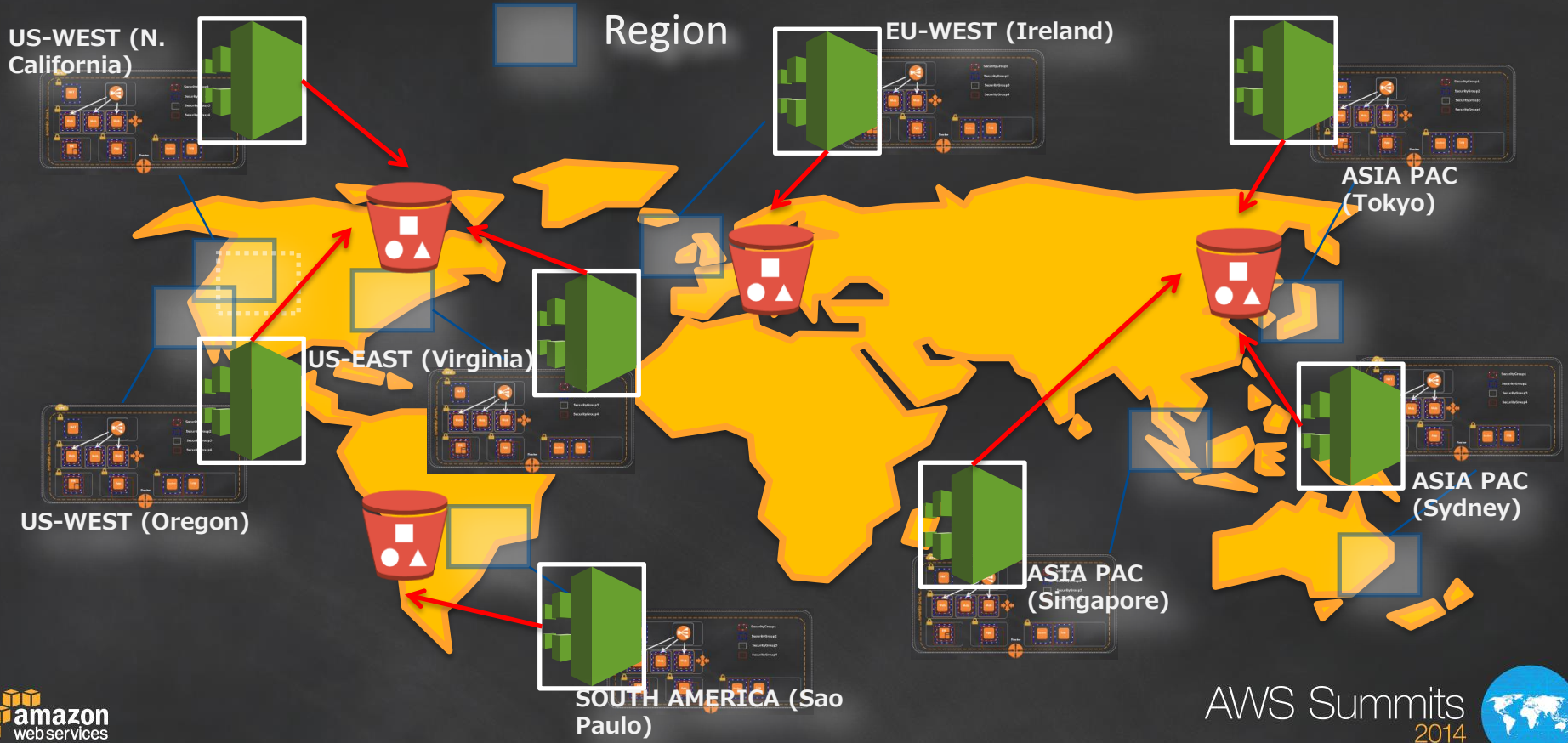
整理したログ要件とAWS上の資産インベントリーから、関連するAWS上のシステムにおいてログが有効かされているか、漏れがないかどうかを確認する。

ログ要件の適用範囲の例
- OSレベルのログ
- ミドルウェア・レベルのログ
- アプリケーション・レベルのログ
- AWSサービス単位のログ
- ログの集中管理
- ログの分析対象

セキュリティログと監視



Security at Scale: Logging in AWS



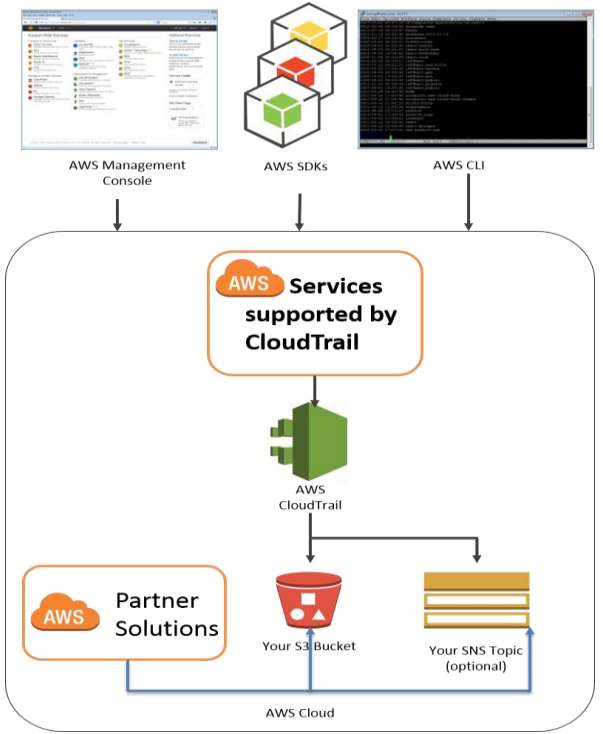
AWS CloudTrail

AWS CloudTrailはAWSアカウントで利用されたAPI Callを記録しログに保存するサービスです。

記録される情報には以下のようなものが含まれます。

- APIを呼び出した身元（Who）
- APIを呼び出した時間（When）
- API呼び出し元のSource IP（Where）
- 呼び出されたAPI（What）
- APIの対象となるAWSリソース（What）

CloduTrail Logging



- CloudTrailはアカウントで利用されたAPI CallのログをS3に保存します。
- 通常、15分内に呼び出されたAPI callのイベントをS3に届けます。
- ログファイルは大よそ5分毎に保管されます。
- ログの分析には様々なパートナー企業がソリューションを提供しています。

対応サービス

対応サービス（7/17現在）：

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Load Balancing (AWS ELB)
- Amazon EMR
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud (Amazon VPC) / Direct Connect
- AWS Identity and Access Management (AWS IAM)
- AWS Security Token Service (AWS STS)
- AWS CloudFormation
- AWS OpsWorks
- AWS Elastic BeansTalk
- Amazon CloudFront
- Amazon Kinesis
- AWS CloudWatch
- Amazon Simple Workflow
- AWS CloudTrail

対応リージョン

対応リージョン（7/17現在）：

- 米国東部 (北バージニア)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジア太平洋 (シドニー)
- EU (アイルランド)
- **アジア太平洋 (東京) - *New!***
- アジア太平洋 (シンガポール) - New!
- 南米 (サンパウロ) - New!

ユースケース

- セキュリティ調査
- リソース変更トラッキング
- トラブルシューティング
- コンプライアンス監査

ユースケース – コンプライアンス対応

CloudTrailによるAPI Callの履歴は企業の内部ポリシーや規制基準におけるコンプライアンス対応をより容易にします。

- SANS Top20
  - クリティカルコントロール12:管理権限のコントロールされた使用
  - クリティカルコントロール14：監査ログの保守、モニタリング、および分析
  - クリティカルコントロール16：アカウントのモニタリングおよびコントロール

http://www.sans-japan.jp

- PCI DSS
  - 要件10 ： ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

https://ja.pcisecuritystandards.org/

ログファイルのアクセスコントロール

- 監査証跡ファイルを不正な変更から保護する。
- 監査証跡の表示を、業務上の必要がある人物のみに制限する。

- CloudTrailの監査ログに対する権限のないアクセスの防止
  - 監査ログへのアクセスはRead-Onlyを基本に
    - IAMによる権限管理
    - S3のバケットポリシーの利用
  - ログを保管しているS3のバケットに対してMFAの有効化
    - MFA Delete for AWS Root アカウント
    - IAM ポリシーによるAPIのMFA Protection

ログ生成及び設定ミスの際のアラート

- ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする
- 監査証跡ファイルを不正な変更から保護する。

- CloudTrailの監査ログの設定ミスに関する通知
  - 管理コンソール上で設定ミスに関する即時通知
- CloudTrailの監査ログ生成の通知
  - S3にログを記録する毎にNotificationの送付が可能
  - ログの生成に関するイベントについてほぼリアルタイムに対応可能
  - S3のログ機能の有効化

AWSリソース及びログに対する変更管理

- システムレベルオブジェクトの作成および削除
- 変更できないよう、監査証跡をセキュリティで保護する。

- システムレベルオブジェクトの作成及び削除を含む、システムコンポーネントの変更に関するログの取得
  - 管理コンソール、コマンドライン、3rd party等APIコールされる全ての変更が対象
  - 全てのリージョンでCloudTrailの利用
  - サポートされているAWSサービスの確認
- 変更や失敗に関するログの改ざん防止
  - デフォルトでCloudTrailのログはS3のサーバーサイド暗号化を利用
  - IAMとMFAによるS3のバケットに対するread-onlyアクセスの強制

ログファイルの保管

- 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。
- 監査証跡の履歴を少なくとも 1年間保持する。

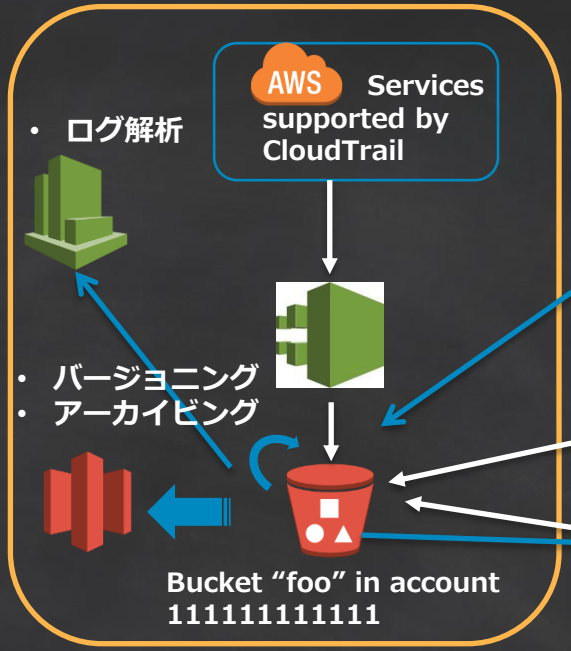
- 保管期間
  - 少なくとも1年間のログの保存
  - 組織が必要とする期間のログの保存
  - S3のLifeCycle機能を用いた保持期間とアーカイブの設定
- 保管場所
  - 複数のRegionのログを一つのBucketに集めることが可能
  - 複数のアカウントのログを一つのBucketにあつめることも可能
- 保管場所の信頼性
  - S3に保管
  - 99.999999999%の堅牢性
  - 99.99%の可用性

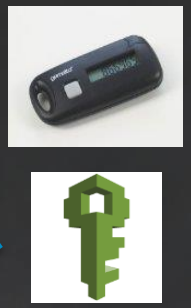
ログデータからのレポート生成

- 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。
- 新たに発見されたセキュリティの脆弱性を特定し、リスクのランク分けを割り当てるためのプロセスを確立する

- CloudTrailの監査ログの網羅性
  - AWSアカウント、IAMユーザー、IAMロールを含む全ての呼び出しもと
  - CloudTrailの監査ログ自体も含む全てのリソース
- CloudTrailの監査ログ生成の頻度
  - ほぼリアルタイムにログを生成
  - 約15分内にS3に送付
- CloudTrailの開始及び停止自体のログも取得
- AWSの内部時刻サービスによるログの時刻表示
- 監査ログに求められる詳細なイベントの記録

ログの集約とアクセスコントロールの例





IAMとMFAによるログの保護
- Read-only
- MFA Delete
- MFA API Protection

Bucketポリシーによるログの集約
- 複数リージョン
- 複数アカウント

“arn:aws:s3:::foo/KBJInc/AWSLogs/222222222222/*”,
“arn:aws:s3:::foo/KBJInc/AWSLogs/333333333333/*”

CloudTrailのログフォーマット


```
{"eventVersion":"1.01",
      "userIdentity":{
            "type":"Root",
            "principalId":“XXXXX0663284",
            "arn":"arn:aws:iam::XXXXX663284:root",
            "accountId":“XXXXX663284",
            "userName":“XXXXX",
            "invokedBy":"autoscaling.amazonaws.com“
            },
      "eventTime":"2014-07-13T09:53:33Z",
      "eventSource":"ec2.amazonaws.com",
      "eventName":"RunInstances",
      "awsRegion":"ap-northeast-1",
      "sourceIPAddress":"autoscaling.amazonaws.com",
      "userAgent":"autoscaling.amazonaws.com",
……..
```

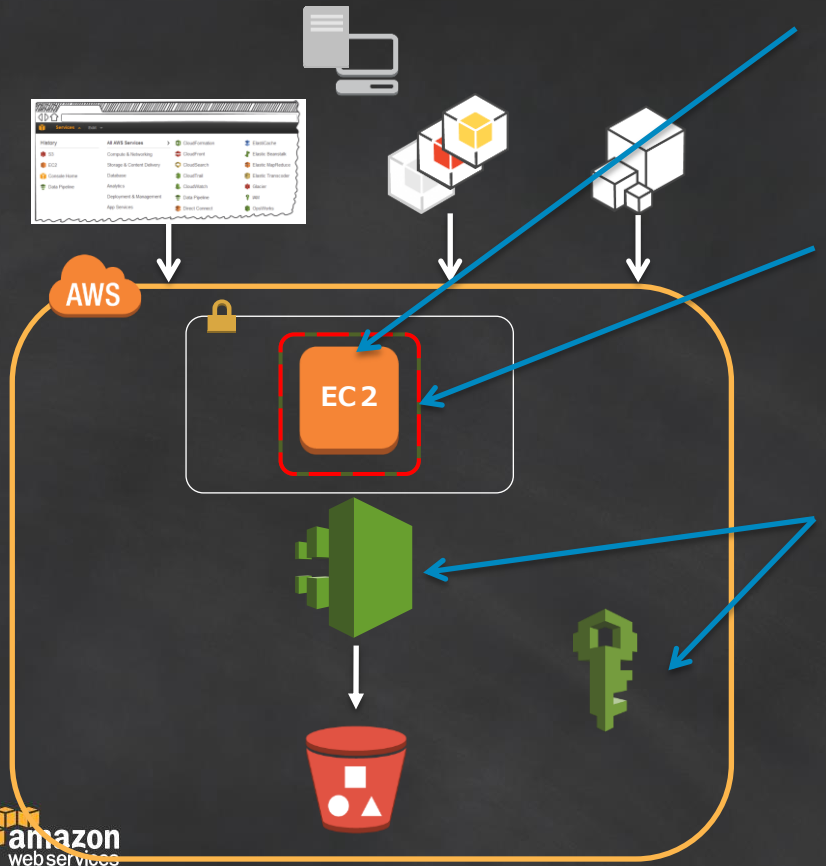

監査証跡となる以下の項目を網羅

- 「ユーザID」
- 「イベントのタイプ」
- 「日付と時刻」
- 「成功または失敗の表示」
- 「イベントの起点」
- 「 影響を受けたデータ」
- 「システムコンポーネント」
- 「リソースの識別子もしくは名前」

主要な重要イベント

- システムコンポーネントの生成と削除
- ネットワークアクセスコントロールの変更
- アカウント・パーミッションの変更
- 認証の成功と失敗
- 重要情報へのアクセスや変更に関するイベント

イベント発生の例



1）未承認のEC2の作成

2）意図しない
セキュリティグループの変更

3）重要機能への
権限のないアクセス

未承認のEC2の作成


```
{"eventVersion":"1.01",
"userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDAI4TLYIBOK753HLQ6Q",
        "arn":"arn:aws:iam::XXXXXXX3284:user/IAMTEST",
        "accountId":“XXXXXXX3284",
        "accessKeyId":“XXXXXXXXSOMJ3PFIJA",
        "userName":"IAMTEST",
        "sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2014-07-15T23:05:34Z"}},
        "invokedBy":"signin.amazonaws.com"},
"eventTime":"2014-07-15T23:07:08Z",
"eventSource":"ec2.amazonaws.com",
"eventName":"RunInstances",
"awsRegion":"ap-northeast-1",
"sourceIPAddress":"signin.amazonaws.com",
"userAgent":"signin.amazonaws.com",
"requestParameters":{
        ……
        ……
}
```


APIをコールしたIdentityの確認
・type/userNameの確認

システムコンポーネントの生成と削除
・eventNameの利用
・Run*|Create*|Launch*による検索
・Delete*|Terminate*による検索

セキュリティグループの変更


```
{"eventVersion":"1.01",
"userIdentity":{
        . . . . . .
        . . . . . .
"eventSource":"ec2.amazonaws.com",
"eventName":"AuthorizeSecurityGroupIngress",
"awsRegion":"ap-northeast-1",
"sourceIPAddress":"signin.amazonaws.com",
"userAgent":"signin.amazonaws.com",
"requestParameters":{
        "groupId":"sg-636b8d0c",
        "ipPermissions":{
        "items":[{
                "ipProtocol":"tcp",
                "fromPort":22,
                "toPort":22,
                "groups":{},
                "ipRanges":{"items":[{"cidrIp":"0.0.0.0/0"}]}}
        ]
}
```


アクセスコントロールの変更
- eventNameの利用
- AuthorizeSecurityGroup*による検索
- CreateNetworkAclEntry*による検索

特に注意すべき事項
- 0.0.0.0/0のようなParameter
- ”fromPort”:0, “toPort”:65535

権限のないアクセス– CloudTrailの設定変更

{"eventVersion":"1.01",
・・・・・・・・・・・・・・
・・・・・・・
"eventTime":"2014-07-15T23:09:46Z",
"eventSource":"cloudtrail.amazonaws.com",
"eventName":"DescribeTrails",
"awsRegion":"ap-northeast-1",
"sourceIPAddress":"signin.amazonaws.com",
"userAgent":"signin.amazonaws.com",
"errorCode":"AccessDenied",
"errorMessage":"User: arn:aws:iam::XXXXXX663284:user/IAMTEST is not authorized to perform: cloudtrail:DescribeTrails",
"requestParameters":null,
"responseElements":null,
"requestID":"1d0521cb-0c75-11e4-8149-dbd9a270b160",
"eventID":"fd833454-936c-4154-bfc2-468a2f59658f"},

認証の失敗によるエラーの抽出
- errorCodeの利用
- Unauthorized*による検索
- AccessDeniedによる検索

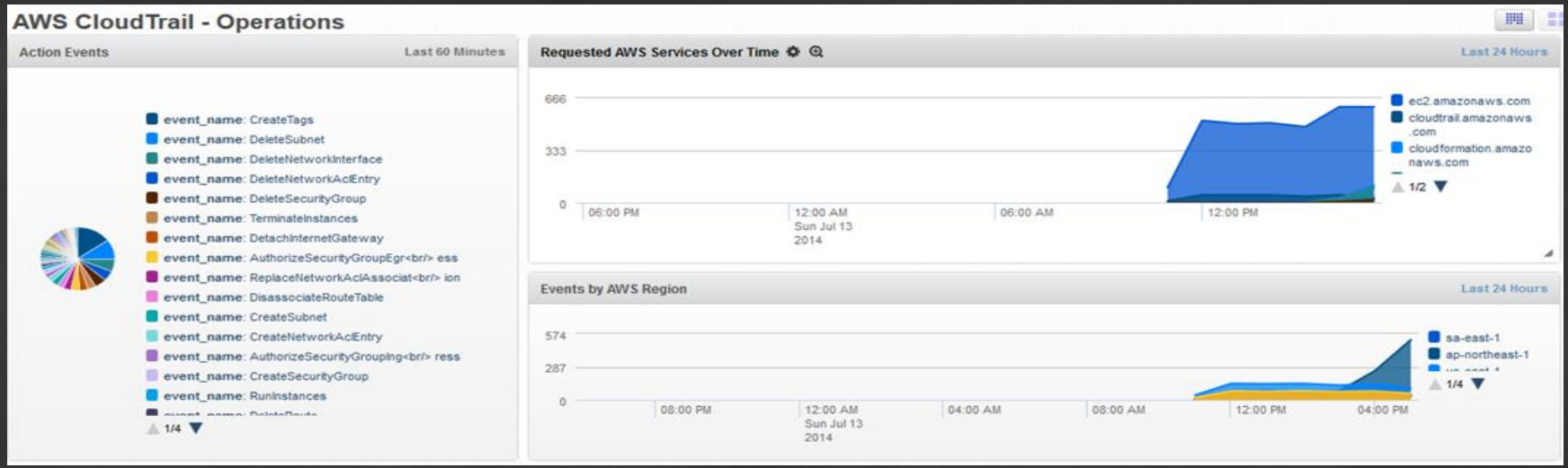
権限のないアクセス– IAMの設定変更

{"eventVersion":"1.01",
"userIdentity":{
. . . . . .
. . . . . .
"eventTime":"2014-07-15T23:09:53Z",
"eventSource":"iam.amazonaws.com",
"eventName":"ListAccountAliases",
"awsRegion":"us-east-1",
"sourceIPAddress":"signin.amazonaws.com",
"userAgent":"signin.amazonaws.com",
"errorCode":"AccessDenied",
"errorMessage":"User: arn:aws:iam::336580663284:user/IAMTEST is not authorized to perform: iam:ListAccountAliases",
"requestParameters":null,"responseElements":null,
"requestID":"20df00b9-0c75-11e4-a5b4-c9bb5d6be211",
"eventID":"964edea9-9d1a-4754-89fb-4362cd90640e"},

認証の失敗によるエラーの抽出
- errorCodeの利用
- Unauthorized*による検索
- AccessDeniedによる検索

CloudTrail, AWS Solution Partner

http://aws.amazon.com/jp/cloudtrail/partners/



FOGHORN WEBSERVICES splunk> boundary sumologic Smartronix Cloud ASSURED ALERTLOGIC Security. Compliance. Cloud.

Cognizant STACKDRIVER DATAPIPE 2ND WATCH loggly

amazon web services

AWS Summits 2014

Conclusion

- AWSではスケーラブルな環境においてお客様固有のセキュリティ要件を満たすための多くの機能が提供されています。
- セキュリティログと監視においては、ログの要件と保護すべきAWS上のリソースの整理が重要
- CloudTrailは東京リージョンを含むAWSのグローバルインフラストラクチャーでAWSのAPIログの透過的に取得する機能
- CloudTrailの監査ログの適切な保管には、組織の権限分掌と情報に対するアクセスコントロール、暗号化機能を利用

Reference

http://aws.amazon.com/jp/compliance

http://aws.amazon.com/jp/security

http://aws.amazon.com/jp/cloudtrail/