AWS Certificate Manager

AWS Black Belt Online Seminar

Arisa Hase
Solutions Architect
2023/10

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
  アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

内容についての注意点

- 本資料では2023 年 10 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(https://aws.amazon.com)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

長谷 有沙（はせ　ありさ）

技術統括本部 西日本ソリューション本部
ソリューションアーキテクト

前職までの経験

コンサルタントとしてデータマネジメント系中心にシステム導入や要件定義を経験

好きなAWSサービス

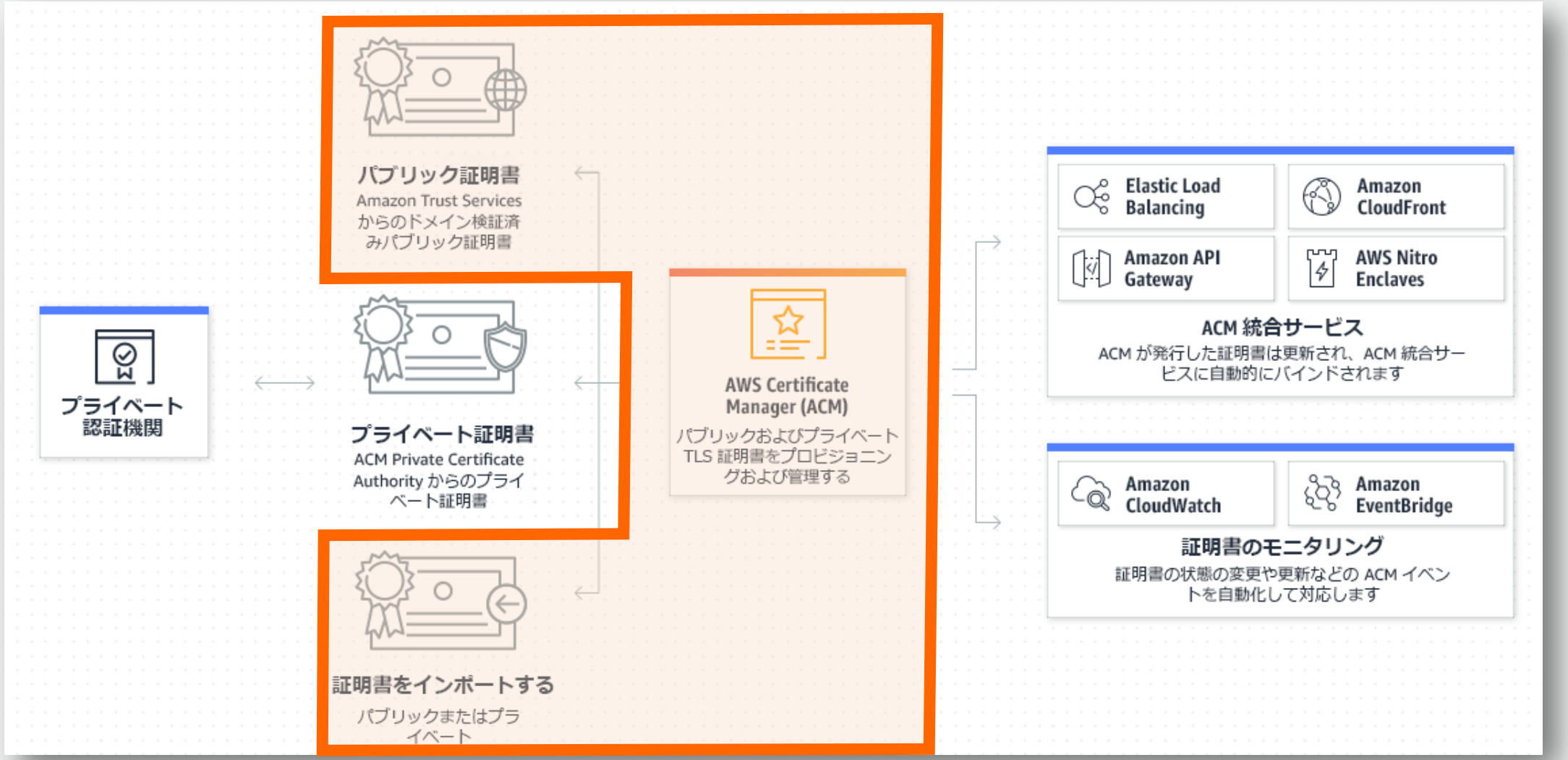
AWS Certificate Manager

本セミナーの対象者・ゴール

- **対象者**
  - これからAWS Certificate Manager (ACM) をご利用されたい、もしくは理解を深めたい
  - SSL/TLS サーバ証明書管理、その運用にに興味・関心がある
  - Web サーバの SSL/TLS による暗号化の仕組みについて理解されている

- **本資料の対象外サービス**
  - AWS Private Certificate Authority (AWS Private CA)

本セミナーのスコープ

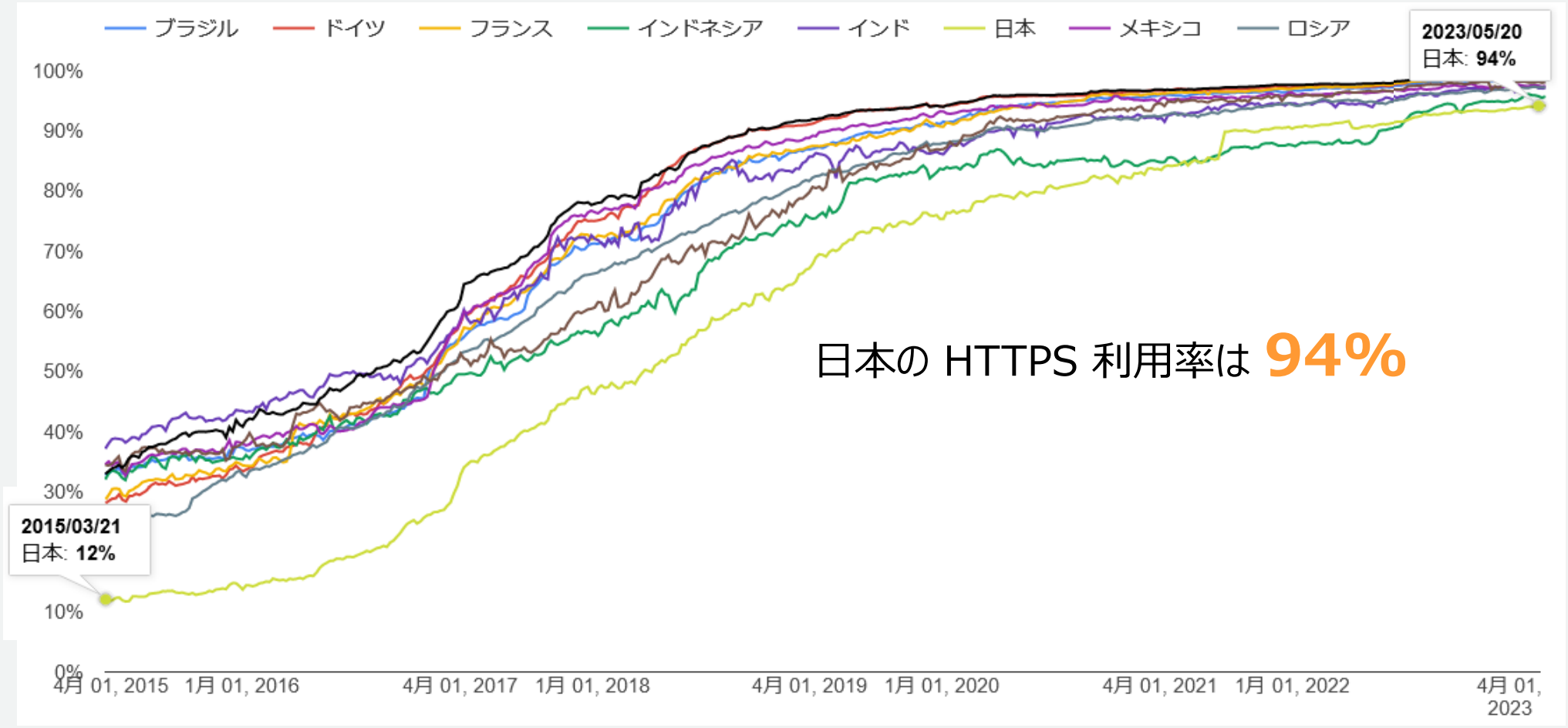


アジェンダ

1. HTTPS の現状と課題
2. サービス概要
3. サービス機能詳細
4. サービス利用時の留意事項
5. 料金とリージョン
6. まとめ

1. HTTPS の現状と課題

HTTPS の利用状況



世界各国におけるHTTPSの利用状況(*1)

(*1) 出典：Google Transparency Report
https://transparencyreport.google.com/https/overview?hl=ja

HTTPS を利用する代表的な理由

・「盗聴」「改ざん」「なりすまし」への対策

・CA/Browser Frum によるガイドライン策定
（例：HTTPS 採用サイトの視認性向上など）

・常時 SSL/TLS によるメリットの享受
＋Cookie 情報の盗聴防止
＋SEO の順位向上
など

参考：総務省https://www.soumu.go.jp/main_content/000615559.pdf

サーバ証明書の運用課題の例

HTTPS を実装するためにはサーバ証明書が必要となり、同時に運用者は**証明書の運用管理が必要**となります

簡単かつ効率的にサーバ証明書の運用をしたい！

2. AWS Certification Manger（ACM）サービス概要

AWS Certificate Manager (ACM) とは

- SSL/TLS サーバー証明書のプロビジョニング、管理、デプロイを簡単に実現するサービス
- SSL/TLS サーバー証明書の購入・アップロード・更新という手間のかかるプロセスの自動化・簡素化

AWS Certificate Manager (ACM) のメリット

証明書を集中管理する

AWS リージョンでの SSL/TLS 証明書すべてを集中管理できます。

安全なキー管理

ACM は、SSL/TLS 証明書で使用される秘密鍵を保護し管理するよう設計されています。

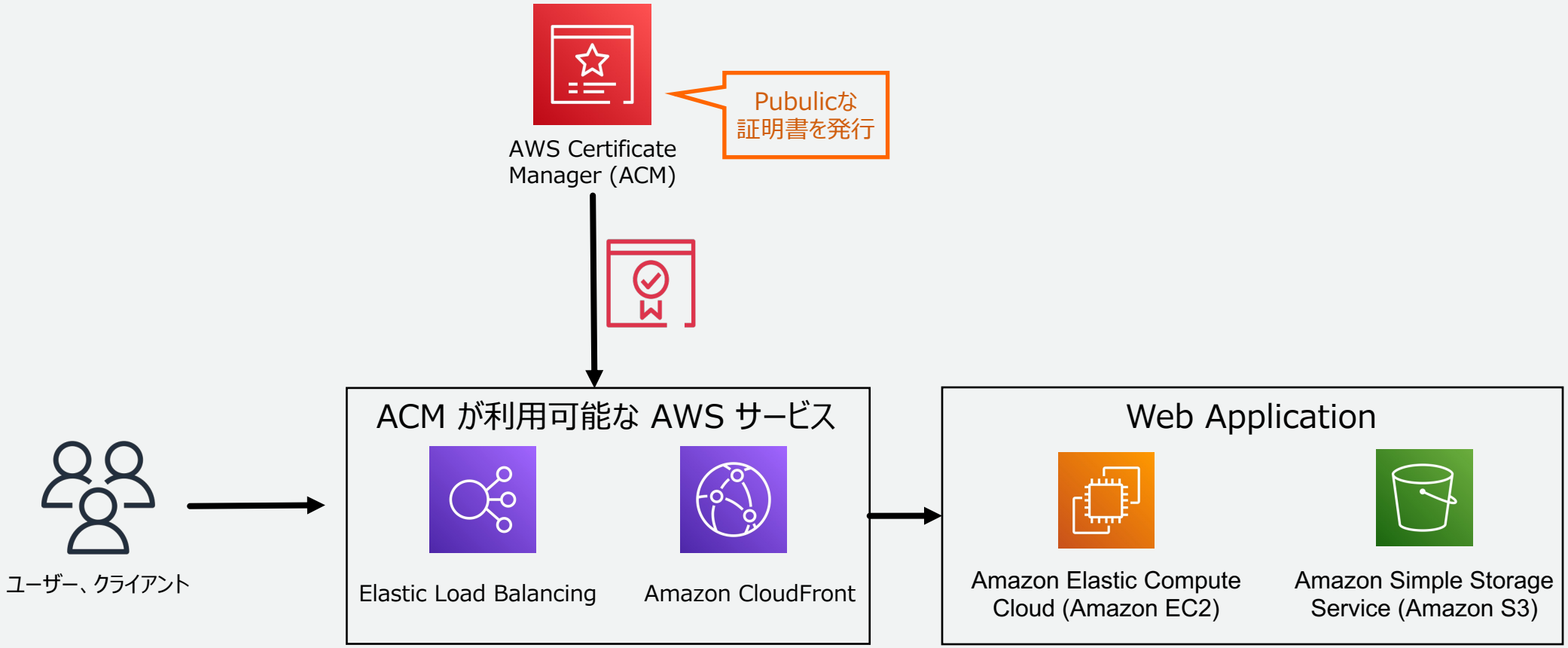
AWSのサービス統合

SSL/TLS 証明書をプロビジョニングし、Elastic Load Balancingや Amazon CloudFront ディストリビューション、Amazon API Gateway でデプロイできます。

サードパーティーの証明書をインポートする

サードパーティーの認証機関 (CA) により発行される SSL/TLS 証明書をインポートし、統合可能な AWS サービスに簡単にデプロイできます。

ACMの典型的な利用例



3. サービス機能詳細

機能概要

a. 証明書を発行する機能

- 証明書の発行とインポート
- ACM で発行できる証明書と種類
- 利用できるドメイン名
- ドメイン検証方法
- インポートできる証明書
- サポートされるキーアルゴリズム
- ACM が発行する証明書のルート証明書について

b. 証明書を管理する機能

- 証明書の自動更新
- 証明書の失効
- ACM 証明書が利用可能な AWS サービス

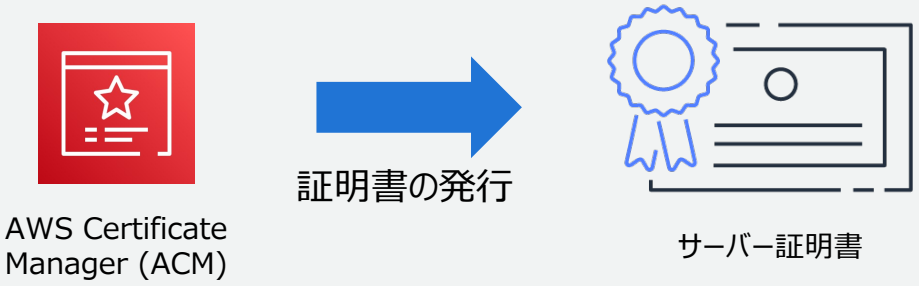
c. モニタリング・ロギング機能

- モニタリングとロギングの概要
- Amazon EventBridge でサポートされるイベント
- CloudWatch でサポートされるメトリクス
- CloudTrail でサポートされる ACM API

a. 証明書を発行する機能

証明書の発行とインポート

証明書の発行



ACM では Amazon 発行のパブリック証明書を発行する事ができます。発行した証明書は Amazon CloudFront 、Elastic Load Balancing 、 Amazon API Gateway などの ACM 統合サービスで利用でき、証明書の更新とデプロイを管理します。

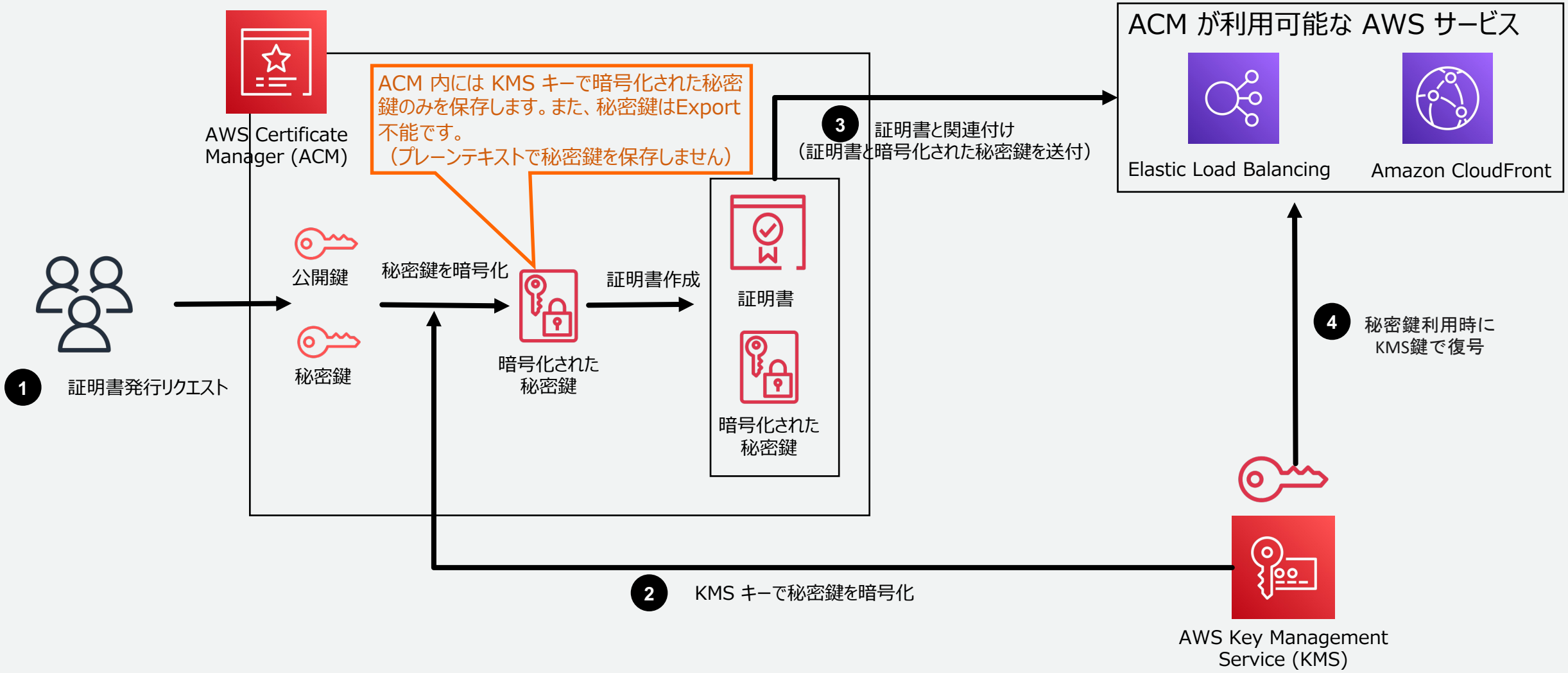
AWS CLI による証明書リクエスト方法
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/gs-acm-request-public.html

証明書のインポート

Amazon CloudFront、Elastic Load Balancing、Amazon API Gateway などの ACM 統合サービスでサードパーティの証明書を使用する必要がある場合は、証明書を ACM にインポートできます。インポートされた証明書を更新することはできませんが、更新プロセスの管理をサポートします。

・AWS CLI による証明書インポート方法
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/import-certificate-api-cli.html
・インポート時の前提条件の詳細
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/import-certificate-prerequisites.html

サーバ証明書の発行と秘密鍵保護の仕組み



ACM で発行できるパブリック証明書と種類

証明書種類	説明
ドメイン認証 (DV) 証明書	サーバの運営組織が、サーバ証明書に記載されるドメインの利用権を有することを確認したうえで発行される証明書。
組織認証 (OV) 証明書	ドメイン名の利用権に加えて、サーバ運営組織の実在性の確認やドメイン名と運営組織との関係などについても確認した上で発行される証明書。
拡張認証 (EV) 証明書	OV 証明書と同様、ドメイン名の利用権に加えて，サーバ運営組織の実在性等の確認やドメイン名と運営組織との関係などについても確認した上で発行される証明書。

項目	パブリック証明書
発行できる証明書	ドメイン認証 (DV) 証明書
有効期間	有効期間は、**13か月(395日)** 固定
アプリケーション、ブラウザのサポート	Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari を含む主要なブラウザと Java
サブジェクト	有効なパブリック DNS 名
ルート CA	パブリックルート CA (*)
検証方法	DNS 認証あるいは E メール認証で検証

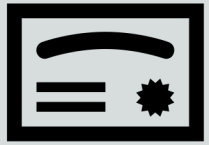
参考：TLS 暗号設定ガイドライン Ver. 3.0.1
https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.0.1.pdf

*: Amazon Trust Services 自社認証局があらゆるところで確実に使えるようにするために、2005年以降のほとんどのブラウザで信頼されているルート認証局である Starfield Services の認証局の一つを購入しております。詳細は、以下を参照ください。
https://www.amazontrust.com/repository/

利用できるドメイン名

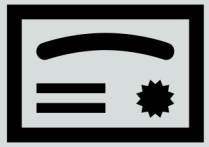
- DNS に準拠するサブジェクト名であれば利用可能
  - 国際化ドメイン名(e.g. 日本語を使ったドメイン名)
    - Punycode 要件(RFC3492) に準拠
  - Zone Apex (ネイキッドドメイン)でも利用可能
    - E.g. *example.com* ドメイン検証が必要
  - ドメイン検証を実施する必要がある。
- 複数ドメイン名もサポート
  - １つの証明書に複数ドメイン名を追加可能
- ワイルドカード名
  - ドメイン名にアスタリスク (*) を使うことで、同じドメイン内の複数サイトを保護できるワイルドカード名の利用可能

ドメイン名 *.example.com で作成



dev.example.com ✅
pro.example.com ✅
example.com ☒

ドメイン名 *.example.com, example.com の複数ドメインで作成



dev.example.com ✅
pro.example.com ✅
example.com ✅

ドメイン検証方法

DV 証明書を発行する際の、ドメイン検証方法は以下の 2 つから選択

- DNS 検証 **(推奨)**
  - DNS に CNAME レコード (ACM が指定) を追加し、ACM で自動的に検証
  - 外部 DNS, AWS の DNS サービスである Route 53 (ワンクリックで検証)の両方可能
  - 証明書更新時、CNAME レコードが残っていれば、検証は自動で実施され、運用負荷軽減
- E メール検証
  - WHOIS データベースに記載されている連絡先(ドメイン登録者、技術担当者、ドメイン管理者)と各ドメインに対して指定した 5 つの共通システムのアドレスに E メールを送信し検証を行い、少なくとも 3 つのメール対応が必要
  - 証明書更新時に都度対応が必要
  - E メール検証を使用して証明書を作成後、DNS による検証に切り替え不可

インポートできる証明書

- 以下の種類の外部認証機関で発行された証明書をインポート可能
  - ドメイン認証 (DV) 証明書
  - 組織認証 (OV) 証明書
  - 拡張認証 (EV) 証明書

サードパーティーの証明書をすでに取得している場合、または ACM 発行の証明書によって満たされないアプリケーション固有の要件がある場合に行います。

サポートされるキーアルゴリズム

種類	ACMで発行する証明書	ACMにインポートする証明書
RSA	RSA 2048 ビット (RSA_2048)	RSA 1024 ビット (RSA_1024)（*） RSA 2048 ビット (RSA_2048) RSA 3072 ビット (RSA_3072) RSA 4096 ビット (RSA_4096)
ECDSA	ECDSA 256 ビット(EC_prime256v1) ECDSA 384 ビット (EC_secp384r1)	ECDSA 256 ビット(EC_prime256v1) ECDSA 384 ビット (EC_secp384r1) ECDSA 521 ビット (EC_secp521r1)

*: RSA 1024 bit 証明書のインポートは可能ですが、セキュリティ観点で、2048bit 以上の証明書を利用されることを推奨します。

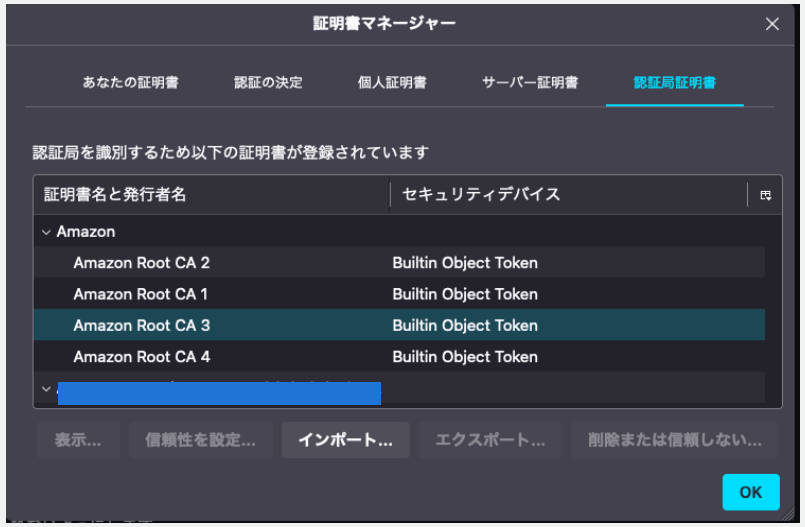
参考：TLS 暗号設定ガイドライン Ver. 3.0.1
https://www.ipa.go.jp/security/crypto/guideline/qmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.0.1.pdf

ACM が発行する証明書のルート証明書について

Amazon ルートCAはFirefoxやChromeやMicrosoft Edgeといた主要なブラウザに登録されているため追加設定をせず利用できます。

- ACM パブリック証明書は Amazon の認証機関 (CA) で検証されます。Amazon Root CA 1
- Amazon Root CA 2、Amazon Root CA 3、Amazon Root CA 4、Starfield サービスルート認証機関証明書 - G2 を含むブラウザ、アプリケーション、OS では、ACM 証明書が信頼されます。

Firefox



Chrome

SHA 256 Hash	Subject
[redacted]	[redacted]
18ce6cfe7bf14e60b2e347b8dfe868cb31d02ebb3ada271569f50343b46db3a4	CN=Amazon Root CA 3,O=Amazon,C=US
1ba5b2aa8c65401a82960118f80bec4f62304d83cec4713a19c39c011ea46db4	CN=Amazon Root CA 2,O=Amazon,C=US
568d6905a2c88708a4b3025190edcfedb1974a606a13c6e5290fcb2ae63edab5	CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,L=Scottsdale,ST=Arizona,C=US
8ecde6884f3d87b1125ba31ac3fcb13d7016de7f57cc904fe1cb97c6ae98196e	CN=Amazon Root CA 1,O=Amazon,C=US
e35d28419ed02025cfa69038cd623962458da5c695fbdea3c22b0bfb25897092	CN=Amazon Root CA 4,O=Amazon,C=US

参考：Amazon Trust Services Repository
https://www.amazontrust.com/repository/
参考：ACM証明書の特徴
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-certificate.html

b. 証明書を管理する機能

証明書の自動更新

自動更新対象の証明書

- Elastic Load Balancing や Amazon CloudFront などの AWS サービスに関連付けられている証明書
  ※インポートした証明書の更新は対象外、また有効期限切れの更新は対象外

証明書更新プロセス(DNS検証の場合)

- 有効期限切れの 60 日前までに DNS 検証を実施
- 自動更新対象の証明書かどうか、ACM が指定した CNAME レコードにアクセスできるどうかを確認
- DNS 検証できない場合、 AWS Health イベントと Amazon EventBridge イベントを通じて有効期限切れの 45 日、30 日、15 日、7 日、3 日、1 日前に送信されます

特記事項

- 証明書の更新時、証明書の Amazon リソースネーム (ARN) は変更されません
- **自動更新による HTTPS 通信の瞬断は発生しません**

証明書の失効

サービス提供の終了など何らかの理由で
サーバ証明書の有効期間内であってもサーバ証明書を失効させる

- マネジメントコンソール、CLI を利用して証明書を削除(*1)
- サポートに依頼して証明書を失効させる(*2)

ACM から発行された証明書の有効性については、以下で確認可能

- Online Certificate Status Protocol (OCSP)
- Certificate Revocation List (CRL)

(*1) 証明書の削除
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/gs-acm-delete.html
(*2)ACM パブリック証明書を取り消すにはどうすればよいですか?
https://aws.amazon.com/jp/premiumsupport/knowledge-center/revoke-acm-public-certificate/

ACM証明書が利用可能なAWSサービス

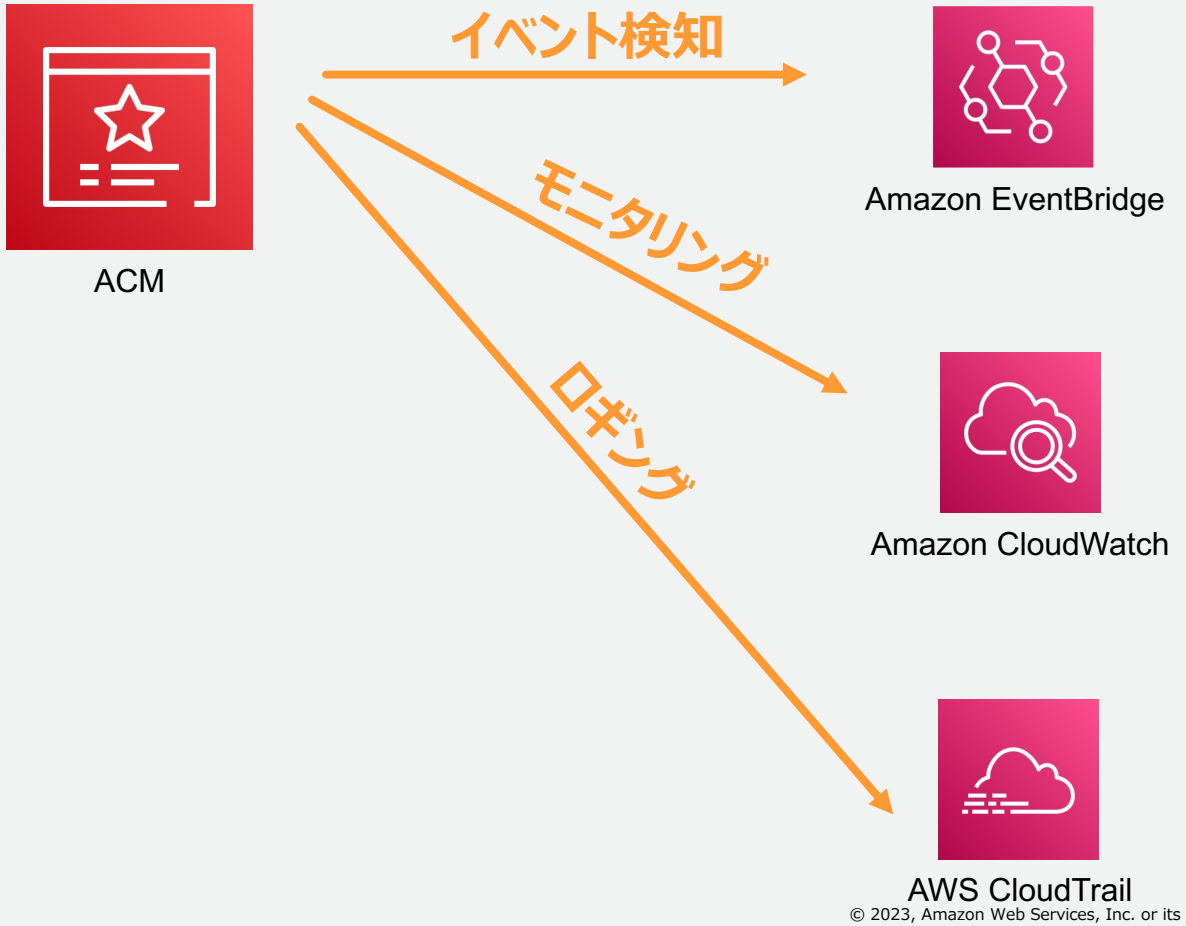
- Amazon CloudFront
- Elastic Load Balancing
- Amazon API Gateway
- AWS Nitro Enclaves
- Amazon Cognito
- AWS Network Firewall
- AWS Elastic Beanstalk
- AWS App Runner
- AWS CloudFormation
- AWS Amplify
- Amazon OpenSearch Service

2023年7月時点の情報です。最新情報は以下のURLからご確認ください。
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-services.html

c. モニタリング・ロギング機能

モニタリングとロギング概要

イベント管理、モニタリング、ロギング機能をAWSサービスと連携して提供



イベント管理機能

- イベントは、ニアリアルタイムで Amazon EventBridge に配信
- イベントを使用して、AWS Lambda 関数、AWS Batch ジョブ、Amazon SNS トピックと連携が可能

モニタリング機能

- メトリクスの収集と追跡、アラーム設定が可能
- 証明書の有効期限が切れるまで、アカウント内の証明書ごとにデイリーでメトリクスを更新

ロギング機能

- ACM コンソールからの呼び出しや SDK/ACM API 経由での操作を含む、API コールをイベントを記録

Amazon EventBridge で通知可能なイベント（1/2）

証明書の有効期限

- 有効期限日の45日前から、すべての有効な証明書有効期限イベントを毎日送信

証明書期限切れ

- 証明書の有効期限が切れた場合にアラートを送信

証明書利用可能

- 証明書が使用可能になったときに通知を送信

Amazon EventBridge で通知可能なイベント（2/2）

証明書更新アクション

- 証明書を更新するためにアクションが必要な時にアラートを送信
  - 例えば、証明書の更新を妨げる CAA レコードを追加した場合、
    有効期限の45日前に自動更新が失敗したときにこのイベントを通知
- アクションされないことが継続される場合、 30日、15日、3日、1日の時点でアラートを再送

ヘルスチェック

- 証明書を正常に更新した場合にステータスを通知
- 証明書更新を行うためのアクションを実行する必要があるとき、ステータスを通知
  - AWS_ACM_RENEWAL_STATE_CHANGE, CAA_CHECK_FAILURE,
    AWS_ACM_RENEWAL_FAILURE

CloudWatch でサポートされているメトリクス

証明書の有効期限が切れるまでの日数

- メトリクス：DaysToExpiry
- 証明書の有効期限が切れるまでの日数をデイリー更新。
- 証明書の有効期限が切れると更新しません。

CloudTrail でサポートされる ACM API

API	内容
AddTagsToCertificate	証明書へのタグの追加
DeleteCertificate	証明書の削除
DescribeCertificate	証明書についての説明
ExportCertificate	証明書のエクスポート
ImportCertificate	証明書のインポート
ListCertificates	証明書の一覧表示
ListTagsForCertificate	証明書のタグの一覧表示
RemoveTagsFromCertificate	証明書からタグを削除
RequestCertificate	証明書のリクエスト
ResendValidationEmail	検証 E メールの再送信
GetCertificate	証明書の取得

4.サービス利用時の留意事項

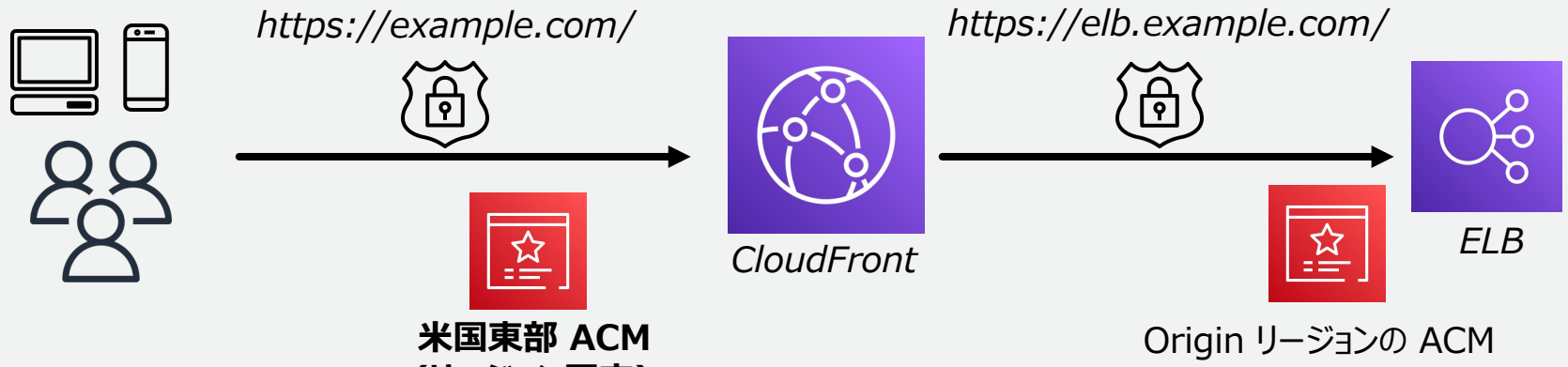
サービス利用時の留意事項の概要

以下２つのケースにおける留意事項について、ご紹介します

- Amazon CloudFront と連携するケース
- AWS CloudFormation を利用して開発、テスト環境など複数環境で ACM 証明書のプロビジョニングをするケース

Amazon CloudFront と連携するケース

- **米国東部（バージニア北部）**リージョンの ACM で証明書を管理
- ACM で発行した証明書を利用する場合、サポートするキーアルゴリズムは、**RSA 2048bit** あるいは **ECDSA 256 bit**
- Amazon CloudFront とオリジンとの間で HTTPS を必須にする場合、オリジンとして Elastic Load Balancing を使用していれば、任意の AWS リージョンで証明書をリクエストあるいはインポート可能



AWS CloudFormation を利用して開発、テスト環境など複数環境で ACM 証明書のプロビジョニングをするケース

- プログラムバージョン、テストフェーズごとに証明書を発行すると、ACM の証明書発行数の上限値に達する可能性
  - 対策として、以下を事前に検討しておく
    - ワイルドカード証明書の活用する
      - 例えば、<version>.service.example.com の場合、 <*>.service.example.com のワイルドカード証明書を作成する
    - サポートに上限値緩和を申請する

サービス上限

項目	デフォルト上限
ACM 証明書の数 **アカウントごとに各 AWS リージョンに適用されます。** 期限切れの証明書と失効した証明書もカウントされます。	2,500
1 年間の ACM 証明書の数 (過去 365 日間) 年間でリージョンおよびアカウントごとに、ACM 証明書のクォータを最大2倍に増やすことをリクエストできます。たとえば、クォータが2,500の場合は、年間でリージョンおよびアカウントごとに、最大5,000の ACM 証明書をリクエストできます。ただし一度に所有できる証明書は 2,500 のみです。2,500を超える証明書が必要な場合はその都度 AWS サポートセンター連絡する必要があります。	アカウント上限の 2 倍

サービス上限（1/2）

項目	デフォルト上限
インポートされた証明書の数	2,500
1 年間にインポートされた証明書の数 (過去 365 日間)	アカウント上限の 2 倍
ACM 証明書ごとのドメイン名の数	10

詳細については、以下を参照ください。
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-limits.html
上限緩和については AWS Support センターへお問い合わせください。
https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-acm

5. 料金とリージョン

料金

ACM で管理するパブリック SSL/TLS 証明書は、**料金はかかりません**

- ウェブサイトあるいはアプリケーションを実行するために作成する AWS リソースのみに料金が発生

- 最新の ACM の料金情報については、以下を参照
  - AWS Certificate Manager サービス料金表
    http://aws.amazon.com/certificate-manager/pricing/

サポートされるリージョン

バージニア北部	**東京**
オハイオ	**大阪**
北カリフォルニア	北京
オレゴン	寧夏
米国東部	ジャカルタ
米国西部	ハイデラバード
米国中部	バーレーン
サンパウロ	ケープタウン
香港特別自治区	フランクフルト
メルボルン	アイルランド
ムンバイ	ロンドン
ソウル	ミラノ
シンガポール	パリ
シドニー	スペイン
バーレーン	ストックホルム
アラブ首長国連邦	チューリッヒ

32 リージョンで利用可能
(2023年10月現在)

最新情報は、以下を参照ください
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-regions.html

6. まとめ

まとめ

- **証明書を集中管理と効率化**
  - AWS リージョンでの集中管理
  - Amazon EventBridge や Amazon CloudWatch で有効期限の可視化や通知が可能
  - 証明書の更新、デプロイ、プロビジョニングの自動化・簡素化
  - 秘密鍵を安全に管理
- **サーバ証明書費用の最適化**
  - AWS Certificate Manager でプロビジョニングされたパブリックSSL/TLS証明書は無料

参考情報

AWS Certificate Manager メインページ

https://aws.amazon.com/jp/certificate-manager/

AWS Certificate Manager ドキュメント

https://docs.aws.amazon.com/ja_jp/acm/

AWS Certificate Manager の料金

https://aws.amazon.com/jp/certificate-manager/pricing/

AWS Certificate Manager のよくある質問

https://aws.amazon.com/jp/certificate-manager/faqs/

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

Thank you!