迫るSSL/TLS短縮化、ライフサイクル管理の新常識

GlobalSign® by GMO

目次

はじめに

業界ルールはどのように決定されているか

SSLサーバ証明書を含む、電子証明書サービスのルールや方針はどのように策定されているかご存知でしょうか？SSLサーバ証明書の標準基準や方針は、CA/ブラウザフォーラムと呼ばれる電子認証事業社及び、ブラウザベンダーを主な構成メンバーとする世界レベルの任意団体にて議論され、決定されております。

有効期間短縮化の背景と業界動向

有効期間短縮化の目的

SSLサーバ証明書の有効期間短縮化は、「証明書の信頼性をより高い水準で維持する」ことを軸に進められており、その背景には大きく3つの目的があります。

1. **証明書および組織情報の鮮度向上**
   更新頻度の増加で審査間隔が短くなり、情報を最新に保てます
2. **秘密鍵解読リスクの低減**
   使用期間を短くすることで鍵の不正解読リスクを抑えられます
3. **脆弱性発見時の影響軽減**
   更新周期を短くすることで脆弱性発生時の影響を抑えられます

短縮化のスケジュール

下記タイムラインからもわかるように、SSLサーバ証明書のライフサイクルは運用の自動化を前提とした形で、これまでにないスピードで短くなっていきます。

日付	最大有効期間	ドメイン審査情報再利用期間
現在	397日	397日
2026年3月15日	200日	200日
2027年3月15日	100日	100日
2029年3月15日	47日	10日

短縮化は「不可逆な流れ」

SSLサーバ証明書の有効期間は、2014年当時の約5年から3年、2年へと段階的に短縮され、2020年には1年にまで縮められてきたように、短縮化の流れは以前から続いています。さらに2029年までの短縮化の方針はすでにCA/ブラウザフォーラムで可決され、主要ブラウザやOS、認証局でも対応が進められているため、早い段階から自動化を前提とした運用体制を整えることが非常に重要となります。

CA/ブラウザフォーラムにて有効期間短縮の仕様が正式に承認

Chromeなどのブラウザ WindowsといったOS 各認証局が実装を準備

自動化など高度な運用スキームの確立が求められる

運用現場に起こる変化とリスク

手動運用の限界

現在は更新・ドメイン検証(※1)も年に1回程度で済んでいますが、2029年には最大有効期間が47日間となるため、更新は年8回以上、ドメイン検証は再利用期間が10日に短縮されることで月3回以上必要になります。こうした作業回数の増加により、従来の手動運用では対応が困難となるため、自動化による効率化が不可欠です。

（※1）SSLマネージドサービスをご利用の場合

日付	更新作業の回数（年間）
現在	約１回 
2029年3月15日	約８～１０回 

作業負担が8倍以上に

短縮化により想定される運用課題

課題①

棚卸し業務の複雑化

証明書の発行枚数が増え、どの環境やドメインで利用されているかの所在管理がより困難に

課題②

期限管理の負荷増大

更新サイクルの短縮により、有効期限の管理に伴う工数・負担が増加

課題③

更新漏れリスク

更新回数の増加により、手動運用では更新漏れや設定ミスの発生リスクが高まる

自動化は「便利」ではなく「必須」へ

SSLサーバ証明書の有効期間短縮化が進むにつれ、更新サイクルは一段と短くなり、運用負荷は増大していきます。さらに、管理対象のSSLサーバ証明書が増えるほど、人的ミスによる更新漏れのリスクも高まり、手動運用を継続することは現実的ではありません。実際、世界的なコミュニケーションツールではSSLサーバ証明書の更新漏れが原因で、数時間にわたりアクセス障害が発生し、ログイン・メッセージ送受信など主要機能が停止する事態となり、多数のユーザに影響が及びました。原因は、有効期限の管理や自動更新の仕組みが十分に整備されていなかったことにあります。このような事態を防ぐためには、更新作業の自動化に加え、SSLサーバ証明書がどこで使用され、どの状態にあるのかを可視化することが重要です。

※引用元：https://www.exoprise.com/2020/02/04/teams-outage-expired-certificate/

グローバルサインが提供する
自動化ソリューション

2つのソリューション

弊社では、自動化に対応するソリューションとして、主に次の2つをご提供しています。なお、CLMはACMEに対応した環境をほぼすべて網羅しており、クラウド環境への展開にも有効です。

ACME

証明書の発行・更新を自動化

ACME

対応環境	サーバOS	✓
	ロードバランサー	-
	クラウドキーストア	-
価格	無償	

CLM

ライフサイクル管理を自動化

CYBERARK LifeCycleX

対応環境	サーバOS	✓
	ロードバランサー	✓
	クラウドキーストア	✓
価格	有償	

※対応環境の詳細についてはお問い合わせください。

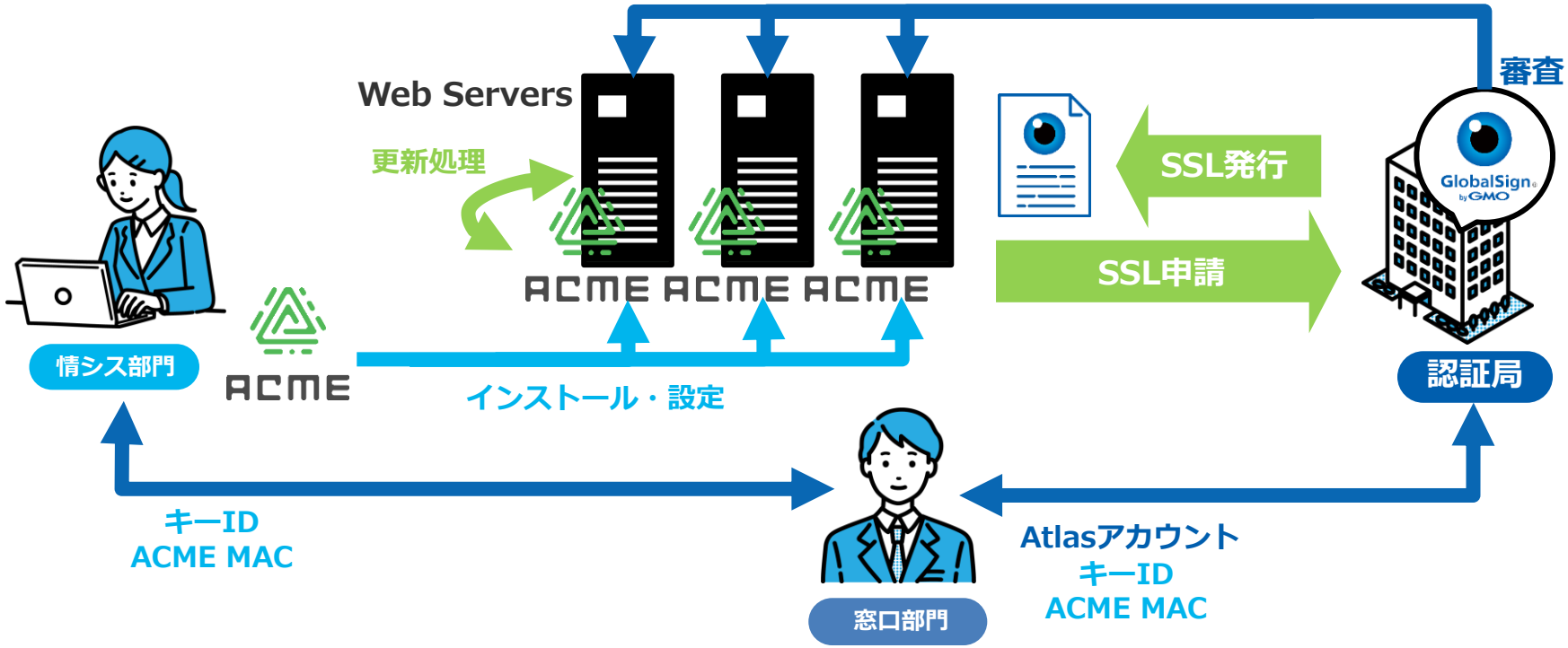
ACMEとは

ACMEとは、SSLサーバ証明書の更新を自動化できる仕組みです。証明書リクエスト元のサーバにACMEクライアントをインストールして利用し、鍵・CSR の生成から、SSLサーバ証明書の取得・設置までを自動化できます。

※ACMEとは、Automatic Certificate Management Environment（自動証明書管理環境）の略称

標準的なOSSで既存環境に導入しやすく、自動更新を実現

ACMEで自動更新されるまでの流れ



サーバ・サービス側で設定しておけば自動更新が可能

ACMEだけでは解決できないこと

1

管理対象が増えると全体把握が困難

機器ごとにACMEクライアントを導入するため、複数環境・複数証明書の管理は複雑化し、全体把握が困難

2

棚卸・履歴管理まではカバーしきれない

ACMEは更新自動化に限定されており、証明書の所在管理や監査対応は不可

3

適用機器が限定的（Webサーバ中心）

ロードバランサーやネットワーク機器、クラウドサービスなどには非対応の場合がまだまだ多い

ACMEでは届かない管理をCLMで実現

CLMとは

CLMはSSLサーバ証明書をディスカバリー機能で可視化して管理可能な状態としてモニタリングし、申請・取得・適用・検証・失効のライフサイクル管理を自動化することができるソリューションです。

※ CLMとは、Certificate Lifecycle Management（証明書ライフサイクル管理）の略称

1

管理対象の全体把握

ダッシュボード機能で直感的に環境内の証明書ステータスを把握

2

棚卸・履歴管理

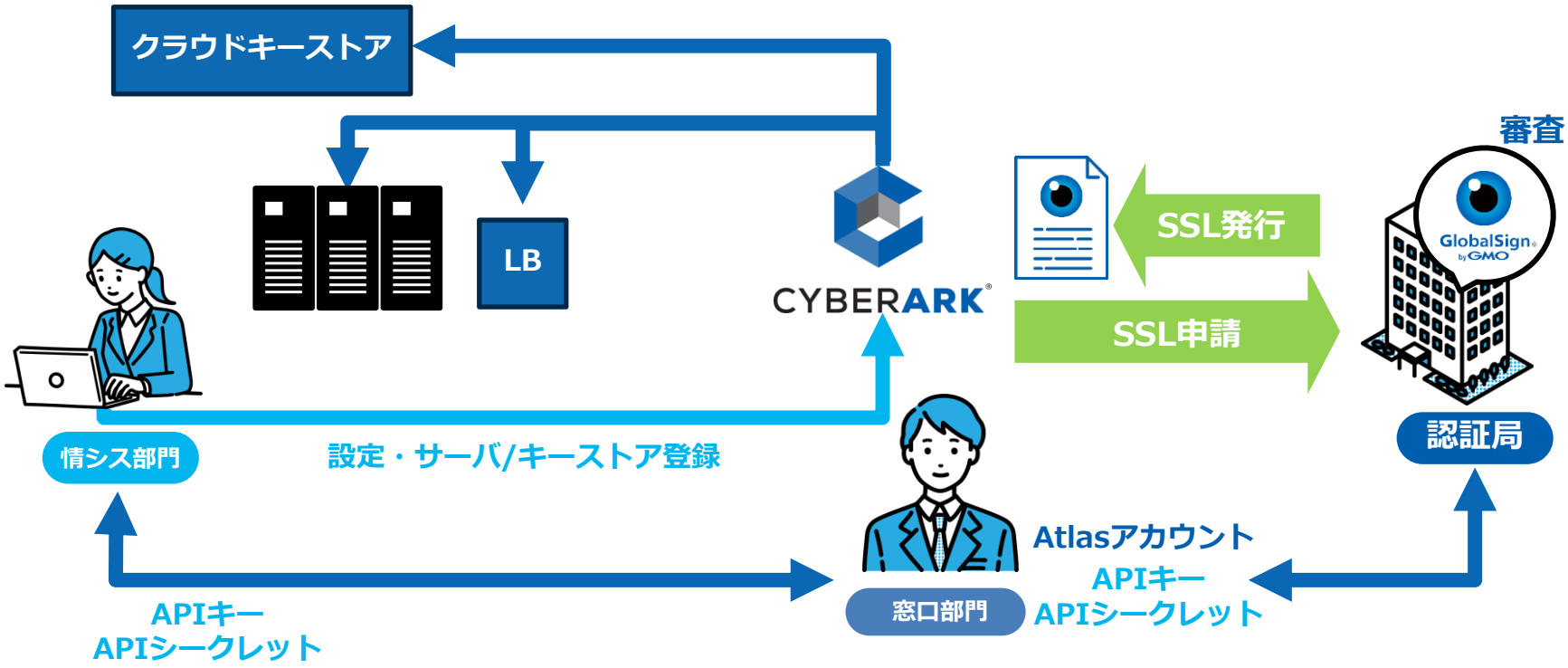
複数認証局からの証明書発行履歴などを管理可能

3

ロードバランサー・クラウドキーストア対応

証明書運用の効率化によって各種LB・AWS ACM, Azure KeyVault等のキーストアにシームレスに適用、更新の管理を実現

CLMで自動更新されるまでの流れ



CLMで証明書のステータスを管理、更新コントロールも可能

2つのCLMソリューション

	LifeCycleX byGMO	CyberArk Certificate Manager	
提供形態	オンプレミス （インストーラー）	SaaS	オンプレミス （インストーラー）
SSL枚数	200枚～	50枚～	500枚～
動作環境	Windows Server Active Directory IIS, SQL Server	SaaS + 中継サーバ(Linux)	Windows Server IIS, SQL Server

ご利用環境や運用体制に合わせて導入可能

自動化へのステップ

自動化に向けたステップ

自動化ソリューションの導入に向けたステップとしては、まず管理対象のSSLサーバ証明書のドメインや配置状況、運用プロセスを可視化し、現状を正確に把握することが重要です。そのうえで、ACMEやCLMの有効性を検証し、将来の運用やシステム構成を踏まえて、最適なソリューションを検討していきます。

まずは現状把握

管理対象のSSLサーバ証明書、
運用手順・関係部門を可視化

トライアル

ACME・CLMの有効性を検証し、
最適な方式を検討

まとめ

まとめ

有効期間短縮化が進む現在、求められるのは「更新作業をこなす」ことだけではなく、SSLサーバ証明書を安全かつ継続的に運用できる仕組みそのものを確立することです。更新頻度の増加に伴い、SSLサーバ証明書の設定状況や利用環境を正確に把握し、適切なタイミングで更新を行える体制が不可欠になります。そのためには、SSLサーバ証明書のライフサイクル全体を一元管理し、自動化と可視化を組み合わせた運用が重要です。弊社では、お客様の環境や運用体制に応じて柔軟に導入支援を行っておりますので、ぜひお気軽にご相談ください。

SSLサーバ証明書に関する
お問い合わせ

03-4545-2300 （受付時間 平日10:00-18:00）

https://jp.globalsign.com/contact/ssl/

GMOグローバルサイン株式会社

〒150-0043
東京都渋谷区道玄坂1-2-3　渋谷フクラス
https://jp.globalsign.com/