自動化の事例：
業界のトレンドは有効期間の短いSSLサーバ証明書

一元管理の実現

SSLサーバ証明書は、依然としてITネットワーク、デバイス、アプリケーション間の通信を保護するための世界標準です。サイバーセキュリティ業界は有効期間1年のSSLサーバ証明書へと移行しているため、Digicertではビジネスの効率を上げ、証明書管理を改善し、ヒューマンエラーを減らすための自動化ツールセットを推奨しています。

Digicertは、有効期間が短い証明書が業界のベストプラクティスであると考えています。この変更を受け入れることで、お客様は会社のセキュリティに対する体制を改善し、運用効率を向上させ、最高レベルのビジネス継続性を維持しながらリスクを削減できます。

TLS/SSL管理の最近の課題

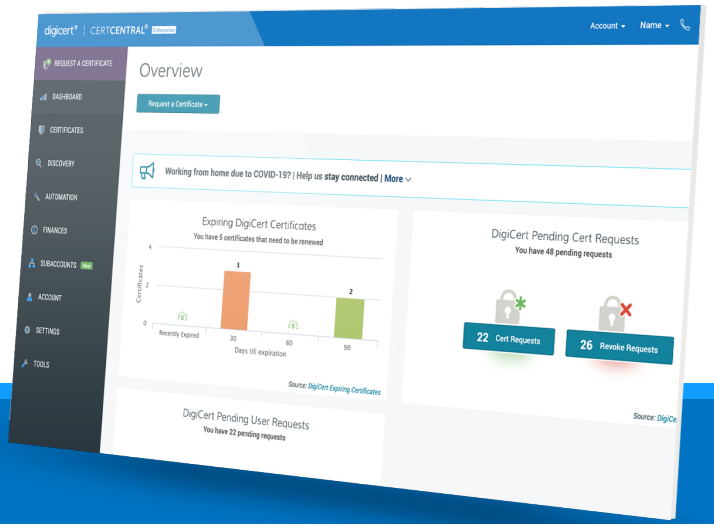
Heartbleed Bugのような歴史的なセキュリティの課題や業界が定めた変更（SHA-1のサポート廃止も含む）は、短期間でのTLS証明書の再配布を必要とするため、管理者にとっては大仕事になります。今日の経済状況では、多くの企業がコスト削減と統合対策に重点を置いています。ITスタッフも複数の環境の継続的な管理、インフラストラクチャの移行、新しい依頼へのトラブルシューティングなどの課題に直面しています。これらの要因と将来量子コンピューターによるセキュリティ侵害に対する懸念の高まりを考慮すると、ほとんどのTLSの専門家がプロセスの自動化を推奨していることが分かります。

必要な証明書自動化ツールをすべて提供

Digicertは、お客様が思い通りに仕事ができ、自信を持って自動化できるように最適な証明書自動化ツールを提供しています。SSLサーバ証明書の自動化は、オプションが制限されていたり、プロセスを簡素化できる証明書管理ツールを使用していなかったり、必要なサポートを得られないと面倒な作業になります。

DigiCert® CertCentralは、賞を獲得している証明書管理ツールでSSLサーバ証明書の自動化を容易にし、時間を節約するためのツールも提供します。証明書ディスカバリー、脆弱性スキャン、SAMLシングルサインオン、あわせて複数年プランなどのオプションをご利用いただけます。サポートが必要な場合は、世界中どこでもDigicertの受賞歴のあるサポートスタッフが対応します。

Digicertの証明書自動化オプションの中から最も最適的なものを選択し、より安全で効率的な環境を実現してください。



1年証明書をサポートする自動化オプション

自動化オプション	推奨される企業規模	概要
ACME（単一サーバ）	小～中規模	シンプルなネットワークの場合、サーバ上で実行するACMEクライアントを使用して、証明書のインストールを自動化します。
自動化ツール	中規模	複数のサーバに及ぶ大規模なネットワーク、自動化、ディスカバリーの場合、センサーとACMEコントローラを使用してスケーラビリティを実現します。
API	中規模	既存のシステムをDigiCertと統合することで、証明書プロセスを最大限に制御できます。
CertCentral 設定項目	すべて	CertCentralのコンソールで自動更新設定を有効にします。
複数年プラン	小～中規模	SSLサーバ証明書の有効期間が最大6年になり、毎年の請求の煩雑さが解消され、割引きやその他の特典は変わりません。

ACME：EVおよびOV証明書を対象とした証明書レベルの自動化です。WindowsおよびLinuxサーバで実行されるACMEクライアントを選択します。CertCentralは、UIから複数のACMEクライアントを管理できるため、企業は証明書の実装を証明書枚数に関係なく効率的に自動化することができます。さらに、CertCentralのDiscoveryセンサーを使用することで、ネットワークでACMEを使用する際のセキュリティを強化することもできます。このセンサーは、ACMEクライアントが安全ではない部外者と直接通信をしないようにする安全なブリッジとして機能します。より詳細な技術情報については、テクニカルドキュメントをご覧ください。

自動化ツール：DigiCert自動化ツールは、F5、Citrix、その他のOEMソリューションとシームレスに統合します。ネットワーク全体にセンサーを実装し、ネットワークの複雑さも意識することなく、すべての証明書を検出できるようにします。または、ACMEコントローラを使用して、ACMEを管理し、大規模に実装します。最終的に、固有のニーズに合わせて自動化ソリューションをカスタマイズできます。

APIから自動化のカスタマイズが可能：CertCentralは、DigiCertツールと任意のシステム、プラットフォームを直接統合できるようにして、既存の環境に最適なソリューションを提供します。現時点でDigiCert APIによってサポートされている自動化ソリューションの詳細については、次のセクション（3ページ）をご覧ください。より詳細な技術情報については、テクニカルドキュメントをご覧ください。

証明書更新用の自動化されていないツール：何らかの理由で自動化機能を使用したくない場合でも、CertCentralにはすべてのSSLサーバ証明書を管理するために役立つツールが組み込まれています。更新通知マネージャー、自動証明書更新設定、証明書ディスカバリーを含む包括的なレポートなどのツールがあります。コンソールから、証明書更新通知をカスタマイズして、送信対象により異なる日を設定できる柔軟性があります。どの通知もAPIでカスタマイズできます。

複数年プランのSSLサーバ証明書：最長6年の有効期間を持つSSLサーバ証明書を購入することで、証明書の失効や証明書のライフサイクル管理の煩わしさをさらに削減し、セキュリティに対する体制を向上させ、効率的でコスト効果の高い方法です。

優れたサポート：DigiCertのお客様は、世界中どこでも弊社の受賞歴のあるサポートをご利用いただけます。

現在サポートされている自動化ソリューション

Webサーバ/ネットワークギア/DevOpsツール		お客様の選択肢			
タイプ	**プラットフォーム**	**自動化ツール**	**ACME**	**CertCentral API**	**サードパーティーの統合**
Webサーバ	Apache HTTP Server	あり	あり	利用可能**	
	Apache Tomcat Server	あり	あり	利用可能**	
	IBM HTTP Server	あり	あり	利用可能**	
	IIS	あり	あり	利用可能**	
	NGINX	あり	あり	利用可能**	
	ACME対応クライアント	あり	あり	利用可能**	
ロードバランサー	F5	あり（センサー）		利用可能**	あり
	NetScaler	あり（センサー）		利用可能**	あり
	A10	あり（センサー）		利用可能**	あり
DNSプラットフォーム	ほとんどのプラットフォームをサポート*			利用可能**	予定あり
クラウドプラットフォーム	ほとんどのプラットフォームをサポート*	あり	あり	利用可能**	予定あり

Webサーバ/ネットワークギア/DevOpsツール		お客様の選択肢			
タイプ	**プラットフォーム**	**自動化ツール**	**ACME**	**CertCentral API**	**サードパーティーの統合**
ACMEクライアント	ほとんどのプラットフォームをサポート*	あり	あり	利用可能**	予定あり
Webホスティングプラットフォーム	Plesk			利用可能**	あり
DevOpsツール	Azure Key Vault	あり	あり	利用可能**	あり
	AWS ELB	あり	あり	利用可能**	予定あり
	Kubernetes	あり	あり	利用可能**	予定あり
	Chef	あり	あり	利用可能**	予定あり
	Ansible	あり	あり	利用可能**	予定あり
	SaltStack	あり	あり	利用可能**	予定あり
	Terraform	あり	あり	利用可能**	予定あり
	Puppet	あり	あり	利用可能**	予定あり
	Istio	あり	あり	利用可能**	予定あり
	HashiCorp Vault	あり	あり	利用可能**	予定あり
	NGINX	あり	あり	利用可能**	予定あり
	ACME対応クライアント	あり	あり	利用可能**	予定あり

* DigiCertは、証明書発行のためのSCEP、ESTをサポートし、ほとんどのDNS、クラウドプラットフォーム、ほとんどのACMEクライアントをサポートします。

** 統合に利用可能なREST APIのリストについては、弊社Webサイト（https://dev.digicert.com/ja/）をご覧ください。

お問い合わせ

DigiCertは、お客様とお客様のビジネス自動化のニーズをサポートするために、最適な製品、ツール、専門家をご用意しおります。ご不明な点がありましたら、担当者までお問い合わせください。