

# DIGICERT CERTCENTRAL® DISCOVERY & AUTOMATION

# DigiCert CertCentral Discovery & Automation

## SSL/TLSサーバ証明書（以下、SSLサーバ証明書）の包括的な管理

### 一元管理の実現

DigiCert CertCentral®マネージャーは、環境内のあらゆる証明書に対する完全な可視性とライフサイクル制御を提供し、リスクの低減、脅威への迅速な対応、運用コストの管理を可能にします。

Discovery機能とAutomation機能は、カスタマイズ可能なソリューションで、組織のニーズに合わせて証明書の管理を簡単かつ効率的にします。デジタル証明書の監視と更新を支援するため、組織のインフラに最適なオプションを複数提供します。

### 技術仕様

- クラウドおよびオンプレミスでの検出
- プライベート証明書とパブリック証明書の両方を検出
- セキュリティ分析と制御用センサーのインストール
- 自動化：ACME、専用のエンタープライズオートメーション、APIにより実現
- ACMEコントローラーエージェントがCertCentral UI内でのACMEクライアント管理を許可（Beta版）
- 統合が容易：ほとんどのWebサーバ（Apache、IBM、NGINX）、ロードバランサー（F5 Networks、Citrix NetScaler、A10 Networks）、DevOpsツール（Azure、AWS、SaltStack）など。
- カスタマイズされた自動更新と個々のユーザー別に指定されたタイミングで送信する更新通知
- 証明書ステータスのリアルタイム監視：すべての証明書の承認、発行、失効、更新
- CSR自動生成と自動インストール
- AutomationはハイアシュランスSSLサーバ証明書（OVおよびEV）をサポート

### 証明書管理の完全な可視化

DigiCert CertCentral管理コンソールでは、規模や複雑さを問わずネットワーク全体で期限切れや不正な証明書を検出することができます。このような証明書は、それらの問題により障害や脆弱性を引き起こす恐れがあります。単一コンソールから証明書ポートフォリオ全体を簡単に管理、監視し、レポートを取得できるため、問題を見過ごすことはありません。

複数のスキャンオプションにより、認証局（CA）を問わず、すべてのプライベートおよびパブリック証明書を検出し監視できます。証明書が検出されると、発行した認証局、証明書の有効期限、署名アルゴリズム、暗号などの詳細が表示されます。

### Discoveryの2つの手法

1. クラウド：高速で簡単なオプションは、インストールが不要で、瞬時に動作し、追跡されていない証明書を期限切れになる前に識別して、問題が発生する可能性を回避します。
2. オンプレミス：専用のエンタープライズセンサーテクノロジーを使用して、証明書インベントリ全体を検出、分類、レポートすることで、リスクを緩和し管理を強化します。

## 証明書ワークフローの自動化

CertCentralの自動化機能により、IT管理者は証明書の発行、更新、アップデート、失効、ライフサイクルのすべての手順を合理化できます。同時に、どのユーザーに対してもデバイスに対しても、証明書の迅速なプロビジョニングと発行が可能になります。

- **ACME** : EV (Extended Validation) 証明書と企業認証 (OV) 証明書を対象とした自動化です。
  - WindowsかLinuxで稼働している複数のACMEクライアントを管理し、枚数に関係なく証明書の実装を自動化する効率的な方法を提供します。
  - CertCentralの検出センサーにより、ネットワークでACMEを使用する際のセキュリティを強化します。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。
- **API** : 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。
  - DigiCert REST APIは、管理者が証明書ライフサイクルを管理し、ネットワークを介してSSLサーバ証明書を購入し実装するプロセスを自動化するための、安全でシンプルな方法を提供します。
- 専用のエンタープライズ統合 : F5、Citrix、その他のOEMソリューションとシームレスに統合する専用の検出・自動化機能を実現します。
  - 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。
  - 固有のニーズに合わせて自動化をカスタマイズします。

## 個々のビジネスニーズに応じたカスタマイズ

CertCentralのDiscoveryおよびAutomation機能は、柔軟性とカスタマイズへを検討している企業にとって最善のソリューションです。この2つの機能は、どちらも他のプラットフォームとシームレスに統合し、組織に最適なオプションを提供します。

## AutomationとDiscoveryの5つの主なメリット

1. **可視性** : ネットワーク内のすべてのパブリックおよびプライベートSSLサーバ証明書を検出し監視します。発行した認証局 (CA) は問いません。
2. **効率性** : ITチームがSSLサーバ証明書とネットワークアクセスの管理に使用する時間、費用、リソースを削減します。
3. **柔軟性** : 組織のニーズに最適な自動化手法を使用することで、予期せぬ証明書の有効期限切れを回避します。ACME、REST API、GraphQLなど、すべての統合オプションを活用します。
4. **整合性** : レポートを実行して、すべての証明書に許可された鍵長、ハッシュアルゴリズム、認証レベルが使用されていることを確認することで、組織のセキュリティポリシーとベストプラクティスを維持します。Discovery機能とAutomation機能を同時に導入することで、証明書実装のエラーを削減します。
5. **スケーラビリティ** : 1つのプラットフォームから発行、追跡、およびワークフローの自動化を行える証明書・ユーザーアイデンティティの数に制限はありません。証明書のタイプやネットワーク上のデバイスに実装されているかどうかは関係なく、すべての証明書を検出し制御します。

詳細については、<https://www.digicert.com/jp/>  
をご覧ください。

© 2020 DigiCert, Inc. All rights reserved. DigiCertは、米国およびその他の国における登録商標です。  
その他のすべての商標および登録商標は、それぞれの所有者に帰属します。

digicert<sup>®</sup>