TLS 自動化成熟度評価の結果について

組織の現在の自動化成熟度、リスクレベル、改善の機会に関する評価です。

digicert®

自動化されていない部分が脆弱性の原因に

TLS 証明書管理の最新のベストプラクティスを明らかに

今日の IT リーダーたちは、組織のデジタルセキュリティ保護について効率と敏捷性を高める方法を模索しています。増え続ける TLS 証明書の管理とリスクへの対応に費やす時間が増加の一途をたどっているからです。その結果、IT の専門家の多くが、複雑なワークロード管理を改善しようと、TLS 自動化ソリューションに注目し始めています。

自動化は喫緊の課題

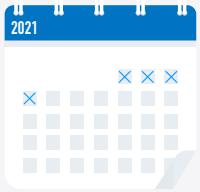
企業が今後の脆弱性に備えるには TLS の自動化が最も確実な方法であることに、デジタルセキュリティの専門家も同意しています。その大きな理由のひとつは、自動化が証明書の管理という複雑な作業の簡素化につながることです。DigiCert CertCentral® の検索機能のようなツールを使えば、企業はネットワークの内外にある、あらゆる証明書を自動的に追跡、識別できるようになります。

また、TLS 証明書のライフサイクル全体を自動化すれば、証明書の予期せぬ期限切れや失効による機能停止を回避して、組織のセキュリティ態勢を維持することができます。しかも、証明書のライフサイクル管理を自動化している企業は、広範な業界全般にわたり、認証局（CA）に、証明書の迅速な置き換えやタイムリーな再発行を必要とするコンプライアンス関連のイベントに、さらには将来的に耐量子コンピュータ暗号にいたるまで、迅速に対応することができます。こうした理由から、企業にはデジタルセキュリティを維持できる敏捷で効率的なプロセスが必要です。

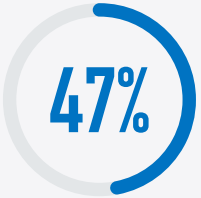
現在のセキュリティ態勢のランクを知る

DigiCert の TLS 自動化成熟度評価は、お客様の組織における TLS 証明書の検索および自動化ツールの現在の使用状況を評価し、改善すべきセキュリティ態勢の領域を明らかにすることを目的として設計されています。こうした評価があれば、組織に最も適した配置モデルを決定する際の指針になります。DigiCert は、種類・量ともに膨大な証明書を扱う大規模から中小規模まで、あらゆる規模の企業に向けたソリューションを用意しています。どの組織もひとつひとつ異なるので、それぞれの IT に関するニーズとリソースに最も貢献する自動化ソリューションこそ、お客様の組織に最適であると考えています。

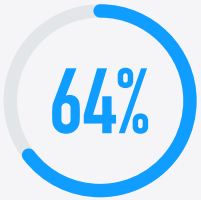
数字で見るデジタルセキュリティ



証明書の管理に毎月費やしている時間は延べ 1 ～ 4 日



IT の専門家が証明書の管理に費やしているのは平均で全時間の 47%

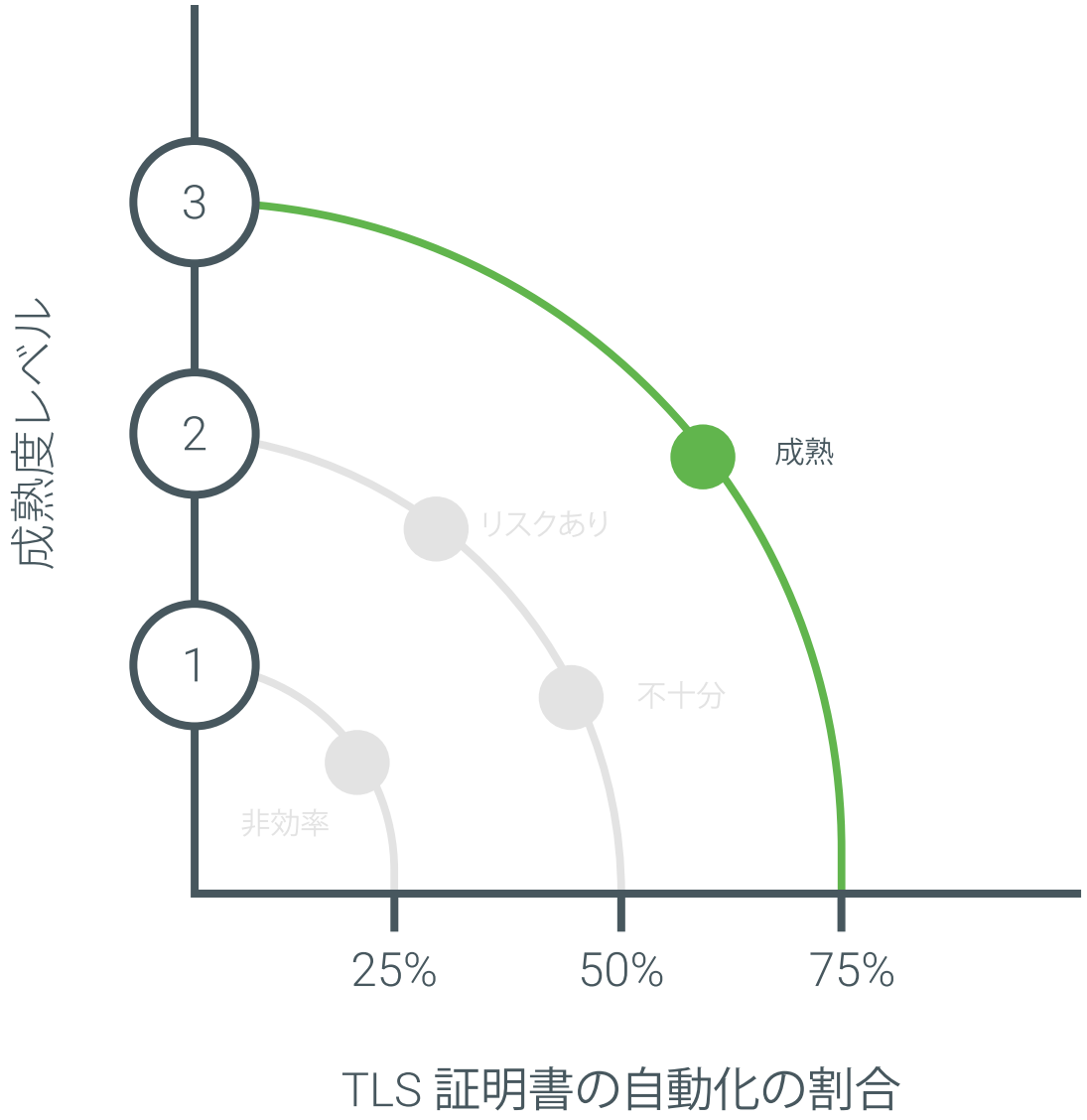


追跡されていない証明書が毎月見つかるのは 64%

証明書の管理にかかる時間が大きな課題であると考えているのは 38%

出典: TLS Certificate Automation Research YouGov Report (TLS 証明書の自動化に関する調査の YouGov レポート) 2021 年 2 月

TLS 自動化成熟度モデル



評価結果

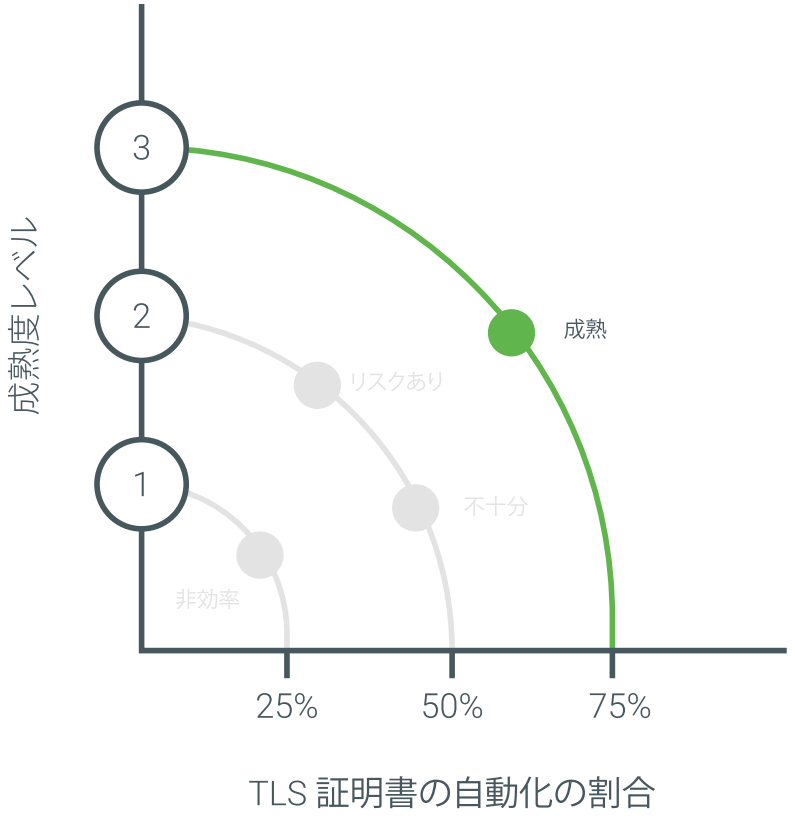
現在のセキュリティ態勢を把握するための指針

Security Posture:
PROACTIVE & MATURE

リスクの概要: 低

すでに、制御された効率的な自動化プロセスを実施し、現在の環境にあるすべての TLS/SSL 証明書をしっかりと把握しています。コンプライアンス上の問題にも、将来的な業界イベントや、証明書停止の可能性にも先行して備えられる企業です。成熟度の高い企業は、証明書のインベントリ全体を管理し、証明書を最大 75% まで自動化しています。また、自動化が組織のセキュリティポリシーの標準化の一環になっています。

証明書の機能停止や、将来的な耐量子コンピュータ暗号に備えて迅速に証明書を置き換えるなど、今後の脅威に完全に備えられるように、証明書のインベントリをさらに 100% まで自動化する方法もご検討ください。



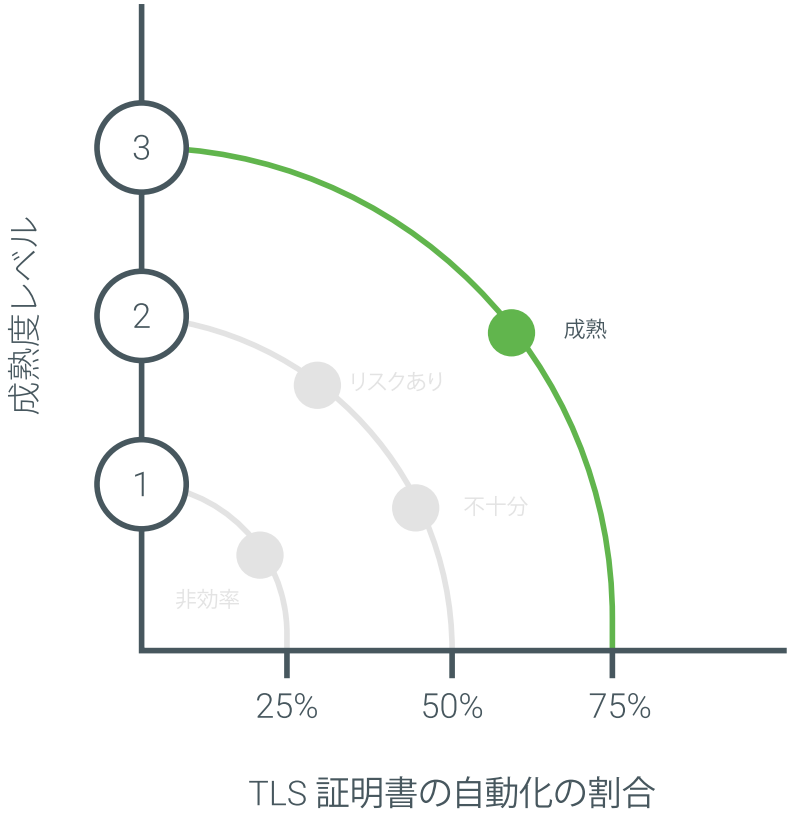
今後の方向性

セキュリティ態勢を強化する次のステップ

Security Posture:
PROACTIVE & MATURE

以下の対策を特にお薦めします。within the next year

- 引き続き、自動化を証明書管理の標準化ポリシーとします。
- 各種のモデル（ホステッドやオンプレミスの配置）を用いて複数の配置を自動化します。
- プライマリ Web ドメイン、または完全修飾ドメイン名（FQDN）すべてについて証明書検索スキャンを毎月スケジューリングします。
- Automation Manager の使用を検討する: ファイアウォールの内側にあるすべての TLS 証明書に対して単一の安全な接続を作成する、DigiCert のオンプレミス型、コンテナ型、センサーベースの管理ツール。
- センサーベースの自動化を試みる: CertCentral UI を介して容易に管理できるホステッド型の自動化。
- 自動化ツールを継続的に使用し、耐量子コンピュータ暗号などの将来的な脅威に対応して、暗号化の俊敏性を維持します。



TLS セキュリティの比較

3 つの評価の概要で現在のセキュリティ態勢を比較する

セキュリティ態勢:
受動的

リスクの概要: 高

現在の証明書管理戦略は、予期せぬ証明書の停止、脆弱性、あるいは CA の事故に対して組織の対応が後手に回る原因になっています。セキュリティに対して特に大きな脅威となるのが、認識不足とタイムリーな行動の欠如です。非効率な手動プロセスに依存していたのでは、あらゆる種類のセキュリティイベントにさらされる危険性があります。

小規模な組織ほど、証明書のインベントリを記録していても、証明書設定の不備、あるいは鍵、暗号スイート、ハッシュの脆弱性といった見逃しやすい証明書関連の問題については、対処法がわからずそのままになっている可能性があります。一方、大規模な組織になると、証明書のインベントリをすべて追跡すること自体が困難です。そのため、組織のさまざまな場所から、気づかないうちに偽の証明書がインストールされてしまえば、盲点が生じたり、マルウェア攻撃の入口になったりする可能性があります。このようなレベルの企業は、証明書の停止によって危険性にさらされる可能性が高いといえます。

Security Posture:
NEEDS IMPROVEMENT

リスクの概要: 中

集中型の TLS/SSL 証明書マネージャのようなツールを使用すれば、組織は堅実なスタートを切ることができます。しかし、機能停止などの問題を迅速に修正するには、引き続きチームの敏捷性を高める必要があります。自動化ツールがないと、潜在的な問題の修正に要する時間が、特に分散した環境や複雑な環境においては、煩雑で非効率となり、時間もかかってしまいます。また、(自己署名されていたり、鍵が弱かったりすることが多い) ベンダー証明書の置き換えや、正しい証明書の配置の管理といったアクションを一括して実行しなければならない場合にも、やはりネットワークに非効率性が見られます。

効率化を考えるとき、自動化は万能ではなく、オンプレミス、クラウド、ハイブリッドなど、ソリューションの配置によって最適な方法が異なります。

Security Posture:
PROACTIVE & MATURE

リスクの概要: 低

すでに、制御された効率的な自動化プロセスを実施し、現在の環境にあるすべての TLS/SSL 証明書をしっかりと把握しています。コンプライアンス上の問題にも、将来的な業界イベントや、証明書停止の可能性にも先行して備えられる企業です。成熟度の高い企業は、証明書のインベントリ全体を管理し、証明書を最大 75%まで自動化しています。また、自動化が組織のセキュリティポリシーの標準化の一環になっています。

証明書の機能停止や、将来的な耐量子コンピュータ暗号に備えて迅速に証明書を置き換えるなど、今後の脅威に完全に備えられるように、証明書のインベントリをさらに 100% まで自動化する方法もご検討ください。

DIGICERT のお勧め

実装すべき TLS ソリューションについて詳細を知る

セキュリティ態勢:
受動的

以下の対策を特にお薦めします。within the next 90 days

- 管理ツールを使って証明書を一元管理する: DigiCert® CertCentral は、単一のコンソールからあらゆる証明書の追跡、発行、失効、置き換えを行えるツールです。
- 検索スキャンツールを配置して、証明書のインベントリをすべて確認する: 限定的なスキャンを実行することで、システム環境内で発生するあらゆる変化を追跡し、証明書に伴う潜在的な問題について様々な視点からの情報を得ます。
- TLS管理のベストプラクティスに集中する: 従業員を指導・訓練して、証明書のインベントリ全体を追跡し、標準化されたキーストレージ、ライフサイクルコンポーネント、廃止プロセス、CT ログによるモニタリングによって環境を保護できます。
- 自動化プロセスを大規模に設定する: プロファイル、スケジュール、アラート、サードパーティ統合を使用します。

Security Posture:
NEEDS IMPROVEMENT

以下の対策を特にお薦めします。within the next six months

- ビジネスに合わせた自動化プロセスを導入する: ACME URL から API、Managed ACME Agent、Sensor Automation、そしてまったく新しい Automation Manager まで、お客様のセキュリティニーズに合わせてカスタマイズされたソリューションを提供します。
- プライマリ Web ドメイン、または完全修飾ドメイン名 (FQDN) すべてについて証明書検索スキャンを毎月スケジューリングします。
- TLS スタックを検討し、システムや予算を統合する機会を検討する: イノベーション、プロセス向上、効率化を中心に考えます。
- 組織の TLS/SSL 証明書管理ポリシーおよびライフサイクル管理において、自動化を標準化の一環とします。
- DigiCert の自動化ウィザードを使用する: DigiCert の業界独自のウィザードは、適切な配置モデル選択する際に役立ちます。

Security Posture:
PROACTIVE & MATURE

以下の対策を特にお薦めします。within the next year

- 引き続き、自動化を証明書管理の標準化ポリシーとします。
- 各種のモデル (ホステッドやオンプレミスの配置) を用いて複数の配置を自動化します。
- プライマリ Web ドメイン、または完全修飾ドメイン名 (FQDN) すべてについて証明書検索スキャンを毎月スケジューリングします。
- 証明書の大規模な配置には Automation Manager の使用を検討します。
- 自動化ツールを継続的に使用し、耐量子コンピュータ暗号などの将来的な脅威に対応して、暗号化の俊敏性を維持します。

業界最高のアドバイスを利用

DigiCert の自動化ソリューションは、万能ではありません。お客様の組織のセキュリティニーズに最適な自動化ソリューションについては、アカウントマネージャーにご相談いただくか、contactus@digicert.com までメールにてお問い合わせください。

digicert®