拡張性に富んだPKIを構築するための5つのステップ: セキュリティエンジニア向けガイド

Darin Andrew

digicert®

目次

1 はじめに
1 PKIを構築するための5つのステップ
2 対応が不可欠なネットワークセキュリティのリスクを列挙する
2 PKIにより軽減されるネットワークセキュリティのリスクを特定する
2 プライベートPKIとパブリックPKIの適正なバランスを見極める
4 インハウス型（社内認証局）の構築かクラウド型（ホスト型認証局）を購入するか決定する
8 証明書の配布の自動化
9 DigiCert Managed PKI

はじめに

Tomは会社でセキュリティエンジニアリングを担当しています。売上の急速な増加に伴い、経営陣は新たなプロジェクトへの投資計画と人材の増員を発表しました。企業の発展に備えたネットワークセキュリティの強化は、Tomとセキュリティエンジニアリングチームに一任されました。

しかし、Tomは上司に計画を提示する来週のミーティングにプレッシャーを感じています。この計画には公開鍵インフラストラクチャ（PKI）が必要だと考えていますが、自分の考えを検証し、同様の状況下で大手企業がとった方策を見極めたいと思っています。計画を詳細まで立てられない場合、来週のミーティングではせめて上司の質問に自信を持って答えたいと考えています。

問題は、信頼性の高いPKIアーキテクチャの構築は複雑で、時間も費用もかかることです。IDGによると、適切な情報テクノロジーが導入済みと確信している情報セキュリティの意思決定者は27%に留まります。

そこでTomは、疑問点を列挙してみました。企業の成長への対応に必要なセキュリティ対策をどうすれば構築できるのか。どのような新技術を採用する必要があるのか。新しい分野のネットワークセキュリティをサポートするためにどんな人材が必要なのか。同様のリスクを軽減するために大手企業は何を行なったのか。

このような苦労に共感しているなら、きっとこのガイドが役立ちます。この文書では、ビジネスの成長に合わせて拡張可能なPKIの計画と構築について説明します。

適切な情報テクノロジーが導入済みと確信している情報セキュリティの意思決定者は27%に留まります。

IDG

拡張性に富んだPKIを構築するための5つのステップ

Tomにように、継続的に経営陣の信頼に応えるのは、一筋縄ではいきません。会社の業務にとって不可欠な要素に対する責任を負うからです。実際のところ、61%のCEOは、セキュリティが企業の成長に及ぼす影響を懸念しています。

61%のCEOは、セキュリティが企業の成長に及ぼす影響を懸念しています。

第19回年次グローバルCEOアンケート調査/2016年1月

成長に対するセキュリティの影響への不安を解消すれば、CEOは自信をもって会社を発展させていくことができます。そのために、ここではPKIの構築を5つのアクションに簡略化して説明します。

1. 対応が不可欠なネットワークセキュリティのリスクを列挙する
2. PKIにより軽減されるネットワークセキュリティのリスクを特定する
3. プライベートPKIとパブリックPKIの適正なバランスを見極める
4. インハウス型（社内認証局）の構築かクラウド型（ホスト型認証局）を購入するか決定する
5. デバイスに証明書を自動発行配布する方法を決める

digicert®

1. 対応が不可欠なネットワークセキュリティのリスクを列挙する

PKIの技術的な側面については、ステップ3から説明します。まず最初に、自社で対応が不可欠なリスクの概要を把握しておく必要があります。以下のようなセキュリティのリスクが考えられます。

- ウェブサービスへの不正アクセスの防止
- データベースに格納された情報への不正アクセスの防止
- 社内ネットワークへの不正アクセスの防止
- ネットワーク上で通信されるメッセージの真正性の検証

このような基本的リスクを定義しておくと、PKIで解決できる問題を特定しやすくなります。

2. PKIにより軽減されるネットワークセキュリティのリスクを特定する

PKIを使用するとネットワークのセキュリティレベルが大幅に向上します。PKIは識別情報を公開鍵に紐付けます。すると暗号化、電子署名、認証を通じてリスクを軽減することができます。暗号化は機密情報の漏洩リスク軽減に役立ちます。電子署名は整合性リスクの軽減に効果的です。認証証明書はアクセスコントロールのリスクを軽減します。これはさまざまなアプリケーションに適用できます。

PKIの一般的な使用事例:

- ウェブページのセキュリティ確保
- ファイルの暗号化
- S/MIMEを使用した電子メールの認証と暗号化
- スマートカードを使用したログインの認証
- ワイヤレスネットワークに接続するノードの認証
- VPNへの接続の認証
- TLS相互認証による企業データを含むサイトおよびサービスへの接続の認証

3. プライベートPKIとパブリックPKIの適正なバランスを見極める

対応が不可欠なネットワークのセキュリティリスクのうち、PKIで対応可能なものを特定したら、次にPKIアーキテクチャの計画を立てます。

成熟期にある企業の多くは、パブリックPKIとプライベートPKIの両方を含むハイブリッドアーキテクチャを構築しています。通常は一般向けのウェブサイトとサービス保護するためにパブリックPKIを使用し、社内向けのサービスにはプライベートPKIを使用します。証明書の配布プロセスを自動化する方法も異なります。

組織に適正なPKI構成を見極めるには、プライベートPKIが必要な場面とパブリックPKIが有効な場面を特定する必要があります。ここからはPKIの技術的側面で考慮すべき点をいくつかを詳しく見てみましょう。

プライベートPKIと パブリックPKI

PKIでは、署名プロセスを通じて識別情報を公開鍵に紐付けます。その署名はルートまたはルートにチェーンする中間証明書を介して行われます。信頼するルートから発行された証明書のみが有効と認められます。

識別情報を公開鍵に紐付けられたルートが信頼ストアにある場合、公開鍵に紐付けられた識別情報を信頼することができます（証明書の主体者を信頼）。これはすべて、証明書が信頼するルートによって発行されたためです。

では、パブリックルートとプライベートルートの違いは何でしょうか。それぞれのいつ、どのように使用すべきでしょうか。

パブリックルートを使用する場合

証明書の署名に使用される技術は、プライベートルートを使用する場合もパブリックルートを使用して署名する場合も同じです。公開されている信頼できるルートが既にブラウザ、オペレーティングシステム、携帯電話などに配布されている点が異なります。ユーザがサイトにアクセスしようとすると、ブラウザ（Google Chrome、Mozilla Firefoxなど）は証明書を発行したルートが信頼できるルートリストにあるかどうかを確認します。

ウェブページの場合を確認してみましょう。会社のウェブページに接続しているブラウザがルートを所有していますか？これは組織の管理下にあるコンピュータからのアクセスかどうかで異なります。組織の管理下にあるデバイスの場合、プライベートルートをその信頼ストアに配布できます。ブラウザは、たとえプライベートルートから発行された証明書であっても、自分の信頼ストアに配布されたすべてのルートから発行された証明書を信頼します。

では、世界中の誰もがアクセスできる公開ウェブページの場合どうなるでしょうか？ページ訪問に使用されたデバイスすべてにプライベートルートを配布（不可能ですが）していないと、信頼されたルートから発行された証明書ではないため、証明書を信頼できないという警告メッセージが表示されます。

ブラウザによっては重大な警告メッセージを表示します。ユーザーがページにアクセスできなくなったり、設定を変更して接続することを強制されます。これは望ましいソリューションではありません。

ブラウザによっては重大な警告メッセージを表示します。ユーザーがページにアクセスできなくなったり、設定を変更して接続することを強制されます。

プライベートルートを使用する場合

プライベートルートの主な使用事例は、社内サービスの認証です。例えば、プライベートルートは、仮想プライベートネットワーク（VPN）、社内のWi-Fi、Wikiページ、または多要素認証に対応したその他のサービスへの接続の認証に役立ちます。

このすべての場合で、証明書の有効性をチェックするサーバインスタンスを制御するので、プライベートルートが理想的です。社内の運用チームは自社のプライベートルートを証明書の発行者として指定できます。有効性のチェック中に、自社の信頼されたプライベートルートが発行したものかどうかを確認することができます。

プライベートルートから証明書を発行することにより発行プロセス、証明書プロファイル、証明書の主体者をきめ細かくコントロールできます。

認証時のプライベートルートの利点は、コントロールできる点です。自社のプライベートルートから証明書を発行する権利を持っているのは、自社のみです。これにより発行プロセス、証明書プロファイル、証明書の主体者をきめ細かくコントロールできます。

4. インハウス型（社内認証局）の構築かクラウド型（ホスト型認証局）を購入するか決定する

社内サービスでプライベート証明書が必要な場面が特定できましたが、次はインハウス型PKIの構築かクラウド型（ホスト型）PKIサービスの購入かを決定します。

どちらの選択肢にも優れた利点があります。この決定は、PKIに割り当て可能なリソースと人員に依存します。ホスト型サービスはルートを作成してパブリック信頼アンカーと同レベルでセキュリティを確保します。一方で社内認証局は発行プロセスの詳細な管理が可能ですが、ソフトウェア、ハードウェア、ライセンス、トレーニングといった経費が必要となります。それぞれの認証局タイプのメリットとデメリット、それぞれの平均コストについては後で詳しく説明します。

ここでは、PKIの社内管理に、社内の時間、経費、人員を投資するだけの価値があるかどうかが問題です。インハウス型のPKIシステムの管理にはメリットもありますが、隠れたコストが存在しています。気を付けなければならないのは、財務的に実行可能な計画として立ち上げても、まもなく多大な財務上の問題となる場合があることです。ハードウェアの費用だけでも、例えばハードウェアセキュリティモジュール（HSM）といったデバイスは総投資額に500万円追加でかかることになります。

エンジニアは多くの場合、商用認証局はパブリックPKI専用であると思い込み、プライベートPKI向けの費用対効果に優れた柔軟なソリューションは提供されないと誤解されています。

クラウド型（ホスト型）プライベートCAのよくある誤解

ネットワークエンジニアリングチームは、よくある誤解から、ホスト型の認証局を採用しない場合があります。多くの場合、商用CAはパブリックPKI専用であると思い込み、プライベートPKI向けの費用対効果に優れた柔軟なソリューションは提供されないと誤解されています。

エンジニアによるクラウド型（ホスト型）認証局の誤解の例：

- プライベート認証局にもパブリック認証局と同じ価格を請求する
- 証明書プロセスを自動化する柔軟性が提供されない
- 特定の証明書プロファイルに制限される

コスト。パブリックSSL/TLSサーバ証明書を購入するためだけに商用認証局を利用して来たかもしれません。この経験をもとに、プライベート証明書にはパブリック証明書と同等の費用がかかると思う方もいますが、実はそうではありません。商用認証局のクラウド型（ホスト型）ソリューションからプライベート証明書を発行するのは、通常、同じ商用認証局でパブリック証明書を発行する費用の数分の1に過ぎません。

柔軟性。多くの人の思い違いの1つは、インハウス型CAでできることを、ホスト型ソリューションでは達成できないという誤解です。たとえば、ホスト型ソリューションでは証明書の発行を自動化できるかどうか疑問に思うかもしれません。多くの商用認証局は、証明書の管理を自動化するRESTful APIなどのツールが備わっています。商用認証局を選択する際には、そのプラットフォーム、ツール、実装を十分に検討してください。

証明書プロファイル。多くの人が、ホスト型認証局では特定の証明書プロファイルに制限されると考えます。CA/ブラウザ フォーラムにより承認される証明書プロファイルのみが取得可能と誤解しています。しかし、これらはプライベート証明書なので、大部分の認証局は必要とする証明書プロファイルをすべて提供できます。一般的にSSL証明書プロファイルでなくとも、X.509でなくとも問題はありません。

インハウス型CAを構築する場合

最初に検討すべきことは規模です。PKIの規模を決める時にエンジニアが犯すよくある間違いは、現状のPKIプロジェクトに基づいてインハウス型認証局を構築することです。数年後には十分ではないことがわかります。注意しないと、貴重なリソースをインハウス型CAの構築に費やしたのに、会社の発展に合わせて拡張できず、プロジェクトを放棄せざるをえなくなってしまいます。

例えば、現在必要としているのがノートPCと携帯端末にワイヤレスネットワークに対する認証証明書を発行するCAだとします。低価格に抑えてインハウス型CAを構築できます。しかし、後ほど大規模なプロジェクトが出現すると、インハウス型CAの拡張が財務的負担になる場合があります。

現状のPKIプロジェクトの範囲に惑わされずに、長期的に考えてください。

半年後には、イントラネットのサーバー全てに対して証明書を発行する必要性が現れるかもしれません。また、APIを通じて証明書を自動的にすべてのサーバーに発行したくなる可能性もあります。そこで、APIインターフェイスを作成するというプロジェクトが1つ増えます。最初は小さなプロジェクトだったものがリソースを集中的に必要とする膨大なプロジェクトに膨れ上がります。

現状のPKIプロジェクトの範囲に惑わされずに、長期的に考えてください。5年後、10年後のことを想定するのは困難ですが、商用CAがこの役に立ちます。商用CAは広範囲にわたる企業との豊富な経験を持っているため、PKIが数年間にどのように拡張されているのか十分に理解しています。

また、インハウス型CA構築の負担を軽減できるような既存リソースの有無も検討してください。例えば、Microsoft Serverライセンスを所有している場合、認証局サーバーの経費はライセンス料金に含まれているので除外することができます。また、隔離されたネットワーク、ファイアウォール、専用ラックスペース、十分な知識を持ったエンジニアなど、現在利用可能なリソースがあるかどうかチームで確認することができます。既にそれらが全て備わっている場合、クラウド型よりもインハウス型の構築のほうが合理的かもしれません。インハウス型CAのコストの詳細については、後で示します。リストを見る際には、上記の検討事項を念頭に置いてください。

テクノロジーの財務費用とエンジニアの業務時間の機会費用をどちらも検討した上で、インハウス型認証局の構築に投資を開始すべきです。十分な予算と時間があること、インハウス型CAが実現するコントロールとカスタマイズが本当に必要であることを確認したら、インハウス型CAを構築します。ただし、ホスト型ソリューションは、往々にして数分の1のコストで同様のメリットを提供できることに留意してください。

digicert®

ホスト型CAを購入する場合

商用認証局は、ハードウェア、ソフトウェア、人員、トレーニング、証明書ポリシー、監査、脆弱性テストに膨大なリソースを注ぎ込んでいます。多くの場合、自社独自のCA構築に時間とお金を費やすよりも、商用認証局の構築済みインフラストラクチャを活用することで時間とリソースを大幅に節約できます。予算が限られている小規模のチームでは、ホスト型プライベートPKIソリューションの採用が合理的な場合があります。インハウス型の構築にかかる費用をほとんどかけずに、メリットの多くを実現できるからです。

自社で構築するよりホスト型の購入する方が良いと判断したら、会社で必要としている機能を商用CAが提供可能がどうか確認します。信頼性、導入の容易さ、機能性、サポート、コストなどを検討してください。

信頼性。商用認証局の経営が安定しているか。採用した認証局との作業に多大な時間とリソースを費やすことになるので、PKIが突然停止する状況に陥らないように確認する必要があります。

導入の容易さ。商用認証局が証明書配布を自動化するAPIを提供しているか。認証局がセキュリティギャップなしにインフラストラクチャに証明書を配布できるかどうか。申請と発行の間に遅延があるか。ユーザーの職務遂行に影響を及ぼすか。商用CAを選定する前に、導入に関してこの全てを確認しておく必要があります。

サポート。商用認証局は年中無休24時間体制のサポートを提供するか。このリストで最も重要な検討事項の1つです。ネットワークエンジニアが作業に行き詰まった際に、認証局の協力が簡単に得られるか。エンジニアが本来の業務に戻れるように、問題解決に向けて迅速にサポートを提供してくれるか。

コスト。商用認証局での証明書発行にどれだけの費用が発生するか。商用認証局は通常、証明書ごと、有効期間ごとに料金を請求します。ほとんどの場合、セキュリティの状況に応じてさまざまなタイプの証明書が提供されます。高価なオプションのように思われるかもしれませんが、商用認証局は、パブリック証明書とプライベート証明書の両方を導入するために必要なインフラストラクチャの構築に、膨大な時間とリソースを費やしています。前述の通り、商用認証局は通常、パブリック証明書の数分の1の費用でプライベート証明書を提供しています。

コストの比較: ホスト型と インハウス型

インハウス型CAのコストは、プロジェクトの範囲、証明書の数、ならびにソフトウェア、ハードウェア、運用スタッフ、冗長性、証明書ポリシー、脆弱性テストの必要性に応じて大きく異なります。このような多様性があるため、インハウス型CAのコストに一定の金額を提示するのは困難です。

会社の個別のPKIに必要な各コストを予測することはできませんが、必要となる典型的リソースを列挙することができます。以下のリストでは、個々のリソースがあるかどうか、ない場合はどの程度の費用がかかるのかを確認できます。

コストは主に6つのカテゴリに分けられます。

1. ハードウェア、ソフトウェア、ライセンス
2. PKIの専門知識
3. トレーニング
4. 証明書ポリシー（CP）と認証局運用規定（CPS）
5. 証明書ポリシーに対する監査
6. 脆弱性テスト

インハウス型プライベートPKIのコスト

ソフトウェア、ハードウェア、ライセンス	• Microsoft証明書サービスに含まれる認証局サーバー（冗長性確保のために2台を推奨） • 冗長性、高可用性、高速応答のためのオンライン証明書ステータスプロトコル（OCSP）と証明書失効リスト（CRL）分散サービス • ファイアウォールと分離ネットワーク（ファイアウォール、スイッチ、専用ラックスペース） • オフラインルートの格納メカニズムとオフラインルートのバックアップ（HSMが必要） • HSM署名 - Gemalto Luna 5：4万ドル～6万ドル（冗長性確保のために2台を推奨）
PKIの専門知識	• PKI局と管理者（役割分担のため2名） • APIインターフェイスを作成する開発者（カスタマイズが必要な場合） 注：業界標準の給与：12万ドル～20万ドル/1人
トレーニング	• 最新のPKIの変更にスタッフが対応できるよう定期的なトレーニングの実施 • コース、認定、コンファレンス
証明書ポリシー（CP）と認証局運用規定（CPS）	• 詳細については最新リファレンスをご覧ください（RFC 3647）。https://tools.ietf.org/html/rfc3647（英語リンク） • CP/CPSの作成（PKI担当者にとって80時間以上の作業） • CP/CPSの保守（常に最新の内容を維持することが必要なライブドキュメント） • ソフトウェア、ポリシー、規則におけるCP/CPSの実施
証明書ポリシーに対する監査	• 監査用の証拠としてPKIの重要な部分の継続的なログ記録 • CP/CPSのポリシー遵守をチェックする年次監査
脆弱性テスト	• CAとサポートサービスの侵入テスト - 4万～6万ドル/1回（CPSで定義された頻度で定期実施を推奨） • 脆弱性コンプライアンス、ネットワークスキャン、脆弱性スキャンの監査

ホスト型プライベートPKIの利点

信頼できるホスト型プライベートPKIの採用により削減できるコスト

- 認証局の安全な管理に必要な訓練を受けた運用スタッフ
- ハードウェア、ソフトウェア、ライセンス
- 業界全体のサーバー、ブラウザ、ライブラリのアップデート
- 高可用性の失効インフラストラクチャ (OCSPおよびCRL)
- APIを介した証明書管理

digicert®

エンジニアは人件費を見落としがちです。インハウス型CAの構築と管理に追加で雇用する人員コストだけでなく、エンジニアリングチームの業務時間という機会費用がかかります。

エンジニアは人件費を見落としがちです。インハウス型CAの構築と管理に追加で雇用する人員コストだけでなく、エンジニアリングチームの業務時間という機会費用がかかります。エンジニアがインハウス型CAの構築に時間を費やせば、本来の業務から何時間も離れることになります。

エンジニアリングチームには、電子メールサーバー、ワイヤレス、侵入テスト、監査、リスクアセスメントなどのセキュリティとインフラストラクチャの保守以外にも多くの責任があります。

業界標準の変化と証明書の有効期限の短縮は、将来的には自動化が選択オプションではなく必須になることを示しています。

5. 証明書の配布の自動化

PKIを大規模かつスムーズに実行するには、証明書の配布を自動化する必要があります。業界標準の変化と証明書の有効期限の短縮は、将来的には自動化が選択オプションではなく必須になることを示しています。数百台～数千台のデバイスを管理することになるかもしれません。自動化の利用により、チームの効率性が向上し、人為ミスや証明書が原因の稼働停止を減らしてセキュリティの確保に役立ちます。

自動化の主な4つのオプション：

1. RESTful API
2. Simple Certificate Enrollment Protocol (SCEP)
3. Enrollment over Secure Transport (EST)
4. Microsoft AD Auto-Enrollment

RESTFUL API

前述したように、選択した商用認証局がプログラム可能なAPIを提供しているかどうかを確認しておくことが重要です。認証局では、チーム側のプログラミングの一部として、RESTful APIエンドポイントが使用可能になっていますか？

既にエンタープライズデバイス管理ソフトウェア（Venafi、AirWatch、Casper、Taniumなどのツール）を使用していますか？使用している場合は、デバイスの管理に既に使用しているソフトウェアソリューションと統合して証明書をデバイスに配布できる商用認証局を探してください。

SCEP

このルートではデバイス上にSCEPエージェントが必要で、エンタープライズデバイス管理ソフトウェアと連携して動作します。このソフトウェアはスクリプトをデバイスに送信し、証明書を取得してSCEPサービスにアクセスする設定情報を提供するように指示します。

そうするとSCEPサービスはデバイスで証明書を取得します。この利点は、SCEPをサポートするデバイス（Android、Microsoft Windows、Apple iOS、SCEPエージェントをサポートするその他のオペレーティングシステム）であれば、SCEPはすでに確立されているプロトコルなので概念実証から本番環境により速く移行できる点です。

SCEPの利点は、エージェントが証明書をデバイスに配布する方法を既に把握していることです。エージェントは自動的にオペレーティングシステムの鍵ストアに証明書を配置します。一部のエンタープライズデバイス管理システムにはこの機能がありますが、この点はソフトウェアプロバイダーに問い合わせる必要があります。ソフトウェアにこの機能がある場合、DigiCert RESTful APIなどをSCEPエージェントの代わりに使用できます。

EST

SCEPの後継であるESTは、ECC (Elliptic Curve Cryptography：楕円曲線暗号方式) をサポートする点を除いて、ほぼ同じです。ECCは、より高速かつコンパクトで効率的な暗号鍵を作成する暗号アルゴリズムです。

MICROSOFT AD AUTO-ENROLLMENT

これは、すべてのWindows PCおよびサーバー上でMicrosoft Key Storeへの証明書配布を自動化するために使用できます。既に他の目的でMicrosoft ADを使用している場合は、AD自動登録を使用して証明書の配布を自動化することが理にかなっています。

DigiCert Managed PKI

PKIをネットワークに組み込む明確な計画が立ったなら、DigiCertがパブリックPKIとプライベートPKIをどちらも備えたソリューションの実現をお手伝いすることができます。

クラウド認証局	
プライベートSSL	ブランディングされ、カスタムプロファイルに対応する専用の中間証明書を使用して、より強力な監視を実現。
パブリックSSL	DigiCert Cloud PKIサービスは、主要ブラウザ、デバイス、およびオペレーティングシステムすべてで信頼されている証明書の大量導入に対応。

社内認証局	
プライベートSSL	インハウス型プライベートPKIから社内で信頼された証明書を発行インハウス型プライベートPKIから社内で信頼された証明書を発行。
パブリックSSL	現在利用できません

プライベートPKI

DigiCertは、プライベートPKI向けのホスト型ソリューションとインハウス型ソリューションを共に提供しています。当社の熟練したPKIアーキテクトが個別の環境に合わせてソリューションのカスタマイズを支援します。ホスト型ソリューション使用の準備が整っている場合でも、まだ検討中の場合でも、DigiCertの熟練エンジニアは構築または購入の意思決定をサポートします。

digicert®

DigiCertクラウド型CA 当社のホスト型ソリューションは、メンテナンスの煩わしさを解消し、コントロールを維持できます。ルートを作成してパブリック信頼アンカーに見合ったレベルで保護し、中間証明書、プロパティ、発行可能な証明書の種類、およびそれらの証明書の名前を監視します。

利点：

- 認証局をセキュアに管理する訓練された運用スタッフ
- ハードウェア、ソフトウェア、ライセンシング
- 業界全体のサーバー、ブラウザ、ライブラリのアップデート
- 高可用性と失効インフラストラクチャ（OCSPおよびCRL）
- APIを介した証明書管理

DigiCert中間認証局。インハウス型プライベートPKIから会社に対して社内で信頼された証明書を発行します。

利点：

- 発行の完全なコントロール
- インターネットに依存しない
- スケジュールに合わせて設定/開発の変更を実行

DIGICERT RESTFUL APIを使用した自動化とカスタマイズ

前述のとおり、DigiCert RESTful APIは他のツールと統合して証明書配布を自動化することができます。証明書プロセスを自動化し、PKIワークフローを簡単にカスタマイズできます。サードパーティのツールやアプリケーション、モバイルデバイス管理（MDM）、エンタープライズデータ管理（EDM）、セキュリティ情報とイベント管理（SIEM）などと統合することもできます。

DIGICERT MANAGED PKIを選ぶ理由

簡素化された証明書管理。当社のクラウド型プライベートPKIはRESTful APIと統合されているため、無料ツールを使用して証明書管理を簡素化および自動化することができます。

カスタム証明書プロファイル。当社の熟練のエンジニアチームは、あなたの組織にとって、どのような証明書プロファイルが理想的であるかアドバイスします。

中間証明書の発行。DigiCertの証明書は、ダウンタイムやサーバーの稼働停止の脅威なしに、数秒以内に発行されます。

必要に応じて拡張可能

貴社のPKIニーズに特有のご質問がおありですか？当社までメール：JPN-DIV-MPKI@digicert.comでお問い合わせください。

Darin Andrew
シニアPKIアーキテクト
darin.andrew@digicert.com

DigiCertのシニアPKIアーキテクトのDarin Andrewは、公開鍵インフラストラクチャ（PKI）とDigiCertシステムに関する豊富な専門知識を活用して、企業における信頼性の高い大規模信頼システムの効果的な構成および最適化を支援しています。Darinは、DirectTrust、LXIコンソーシアム、自動車工学協会（SAE）など、セキュリティに焦点を当てた多くの専門的な作業グループに貢献してきました。規模の大小を問わずサイバーセキュリティのニーズに応じて、PKIアーキテクチャのコンサルティングを務めています。