拡張性に富んだ　　を構築するための　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

はじめに

. 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

の技術的な側面については、ステップ 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

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 、 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（ ）、社内の - 、 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。

digicert®

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。

. 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　の構築かクラウド型（ホスト型）　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、　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、　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（　）といったデバイスは総投資額に　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　専用であると思い込み、プライベート　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、商用はパブリック　専用であると思い込み、プライベート　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　/　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　に過ぎません。

柔軟性。多くの人の思い違いの つは、インハウス型 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 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。 /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 証明書プロファイルでなくとも、 . 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。 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 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 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 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 だとします。低価格に抑えてインハウス型 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 の拡張が財務的負担になる場合があります。

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、 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、 インターフェイスを作成するというプロジェクトが 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 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。 年後、 年後のことを想定するのは困難ですが、商用 がこの役に立ちます。商用 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、 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 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、 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、ム

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 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 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 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、 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 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 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 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 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 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 のコストは、プロジェクトの範囲、証明書の数、
弩キＶ礄嶁貂頑翆遅瘖楡楡檞甘屯￣護遵栐傅奭亻 8 ま分導入すウ涯＜酚黀皃鉗鬣

エンジニアは人件費を見落としがちです。インハウス型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

そうすると　　サービスはデバイスで証明書を取得します。この利点は、　　をサポートするデバイス（　　、　　、　　、　　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、　　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。

　　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、　　などを　　エージェントの代わりに使用できます。

EST

　　の後継である　　は、　　：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。　　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　　およびサーバー上で　　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　　を使用している場合は、　　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。

　をネットワークに組み込む明確な計画が立ったなら、　がパブリック　とプライベート　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	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	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	インハウス型プライベート　　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　　から社内で信頼された証明書を発行。
パブリック	現在利用できません

プライベートPKI

　　は、プライベート　　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

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（　　および　　）
  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　　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