digicert®

SSLサーバ証明書管理のベストプラクティスチェックリスト

昨年は、企業の60%が重要なビジネスアプリケーションに影響するような証明書関連の障害を経験しました[1]。今では、このような障害で評判と成長率が損なわれると、大企業の場合、平均で1分間で5,600ドル[2]を失うことになります。

企業の電子証明書の管理に役立つ妥協のない基準を設定し、維持することが、これまで以上に重要になっています。

そこで、次のようなガイドラインを作りました。業界のベストプラクティスを必要な手順に切り出すことで、知識不足や証明書の不十分な管理と取扱いによって生じる損害を伴う障害から、ビジネスを安全に保護することができます。

digicert®

識別

発行されたすべての証明書を把握する

利用中の証明書を網羅したリストがなければ、セキュリティのリスクに目を向けることはできません。そこで、認証局（CA）から発行されたすべての証明書のリストを作成することから始めるのが良いでしょう。独自の認証局からあらゆるネットワークデバイスまで、すべてを網羅できていることを確認するのは困難ですが、ネットワークスキャナを使用して、SSLサーバ証明書を検出するのが、最も簡単な解決方法です。

すべての証明書のインストール場所を特定する

発行された証明書を所有していることを認識することは、第一段階に過ぎません。不正な証明書がインストールされると、暗号化されたデータが通知もなく漏洩する可能性があります。すべての証明書の確認済みサーバの場所を特定し、証明書のリストに加えます。

すべての証明書とドメインの所有者を明確にする

予期せぬ有効期限切れは、証明書関連の障害が発生する大きな要因です。証明書の管理者の確認と、管理者が退職したときに所有権を更新するプロセスの両方を必ず確立してください。

WebサーバのOSとアプリケーションのバージョンを認識する

ハッカーは、オペレーティングシステムの特定の弱点につけ込みます。例えばHeartbleedは、インターネットから誰でもシステムにアクセスできるようにするOpenSSL暗号ライブラリの脆弱性です。そのため、証明書のリストにオペレーティングシステムとアプリの詳細を含めることが不可欠です。

Webサーバの暗号スイートとTLSバージョンを特定する

暗号スイートは、TLS暗号化と連動してネットワーク接続を保護するアルゴリズムの一式です。ハッカーは、旧バージョンのTLSや安全でない暗号スイートをターゲットにする傾向があるため、稼働中のバージョンを証明書のリストに含めることが重要になります。

[1] https://www.venafi.com/blog/majority-businesses-still-experience-outages-are-you-protecting-your-certificates

[2] https://www.venafi.com/blog/what-if-you-could-guarantee-eliminating-outages-your-organization

改善

脆弱な暗号鍵、暗号スイート、ハッシュを削除する

MD5やSHA-1のような古いハッシュアルゴリズムが内部Webサイトに残っている場合は、更新する必要があります。推奨されるTLSのバージョンは、TLS 1.2とTLS 1.3のみで、必ずAESなどの最新の暗号化を使用します。

ワイルドカード証明書の発行と配布を管理する

ワイルドカード証明書は、複数のサブドメインの管理を簡単にするためには便利ですが、秘密鍵が漏洩した場合、ハッカーはそのドメインスペース内のどのシステムでも操作できるようになり、複雑で費用の掛かる取り消しと再発行が必要になるため、注意が必要です。ただし、厳しい条件を満たせば、ワイルドカード証明書はセキュアで柔軟になります。

適切な証明書タイプを実装する

証明書に関しては、適材適所な活用が必要です。内部システムの場合、プライベートSSLサーバ証明書を使用できますが、公開Webサイトには、企業認証（OV）かEV（Extended Validation）のいずれかが必要です。基本的なドメイン認証（DV）証明書はWebサイトが本物であることを証明するものではないので、機密情報を転送する場合はお勧めできません。

すべてのベンダーデフォルト証明書を管理する

ベンダー証明書は、通常自己署名され、期限切れになることがあります。また、脆弱な暗号鍵を使用していて、生産ネットワークの外部での使用を意図していない事が多く、ブラウザから信頼されません。それでも、企業がこれを多数所有していることがよくあります。最先端の証明書管理プラットフォームで最新の自動化ツールを使用することでベンダー証明書の削除と交換を効率化できます。

すべてのWebサービスに必ず最新のパッチをインストールする

オペレーティングシステムとWebサーバを進化する最も悪質な攻撃者から保護するためには、最新のパッチで更新することが不可欠です。

保護

- [ ] **発行と更新のプロセスを標準化/自動化する**
TSL証明書の発行と更新の際に、自動化/標準化のプロトコルを利用することによって、ユーザーのエラーを削減し、時間を節約できます。これは、高品質の証明書管理プラットフォームで簡単になります。

- [ ] **すべての証明書のインストールと更新をタイミング良く行う**
証明書の更新は、ビジネスの時間的制約に合わせて調整することが重要です。更新は、一定の間隔で、証明書の更新から有効期限切れまでの間を少なくとも15日空けることをお勧めしますが、他の業務には最大90日必要な場合もあります。

- [ ] **証明書の更新時に秘密鍵が再利用されないことを確認する**
使用している証明書のタイプがDV、OV、EVのいずれであっても、秘密鍵の再利用は鍵の漏洩というリスクにつながります。更新プロセスでは、必ず新しい鍵ペアを作成します。

- [ ] **証明書と秘密鍵を安全な方法でインストールする**
秘密鍵を安全なコンピュータで作成し、電子メールを自動的に廃棄できるシステムで、必ず暗号化された電子メールによってのみ配布します。

- [ ] **証明書の取り消しプロセスを実施する**
システムの稼働を終わらせたり、耐用年数を迎えたり、所有者が変わる際には、証明書の削除/取り消しを管理する適切なプロセスが実施されていることを確認します。

監視

ネットワークの変更を検出する

証明書を手作業で管理することは、ますます困難になっています。ネットワークは絶えず変化していて、ほとんどの企業が所有する多数の証明書は、急速にその数を増しています。ネットワークスキャンツールを使用すると、問題が発生した時点で発見でき、迅速な対応と保守が可能になります。

CT（Certificate Transparency）ログで不正な証明書をチェックする

ログに記録されないパブリック証明書は、信頼できないことを顧客に対して警告することになります。信用情報のように、CTログモニタリングはこれらの不正な証明書を検出し、データや評判が損なわれる前に改善できるようになります。

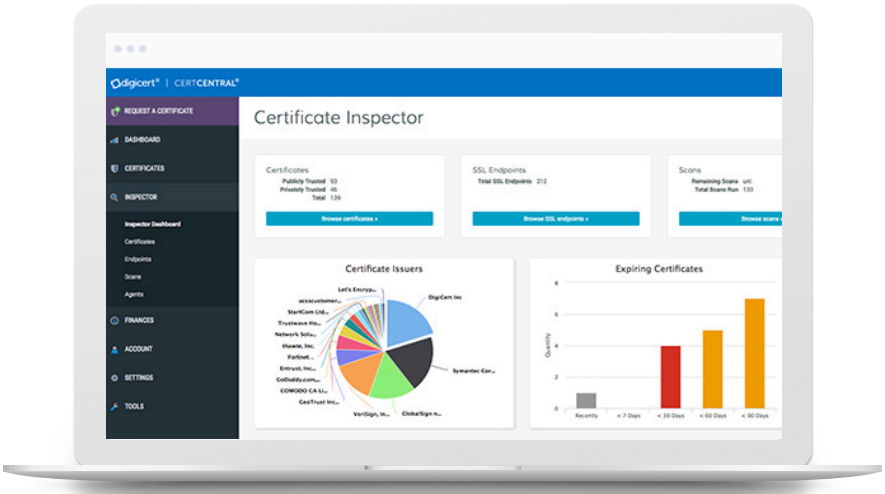
承認されていない証明書の申請をCAAで防止する

CAA（Certificate Authority Authorization）は、特定のドメインに対して証明書を発行できるCAを決定するDNSレコードです。CAAを使用することで、ご自身のドメインに証明書を発行できるCAを管理できるようになるため、承認されていない、不審なCAからの証明書発行を防止することができます。

まとめ

オンラインの企業を安全に保つための推奨事項をご確認いただきました。最後にお勧めのソリューションをご紹介します。

DigiCertのCertCentral



証明書管理を簡単に

DigiCert CertCentral®は、すべての証明書の識別、改善、保護、監視だけでなく、証明書の管理全体のカスタマイズや自動化に必要なツールと機能をすべて備えています。次のことができるようになります。

- ネットワークで新しいシステムと変更を検出する
- CTログで不正な証明書を監視する
- 承認されていない証明書の申請をCAAで検出/防止する

このすべてを単一画面で行えます。

詳細については、digicert.com/jp/certificate-managementをご覧ください。