PKI 自動化に関する現状

2021 レポート

PKI 自動化に関する現状レポート

PKI はテクノロジーのあらゆる側面における中核を成していると言っても過言ではありません。ユーザー、サーバー、デバイス、IoT、DevOps アプリケーション/サービス、電子文書のドキュメントサイニングなどで欠かせないものになっています。

しかし、PKI を手作業で管理することは急速にほぼ不可能な状況になりつつあります。最近の Ponemon 研究所の調査によれば、企業が管理する必要のある PKI 証明書の数は毎年 43% ずつ増加しています [1]。パブリック証明書の有効期限の短期化も進み、PKI 証明書の管理が企業の手に負えなくなるのはもはや時間の問題です。

企業がこの課題にどのように対処しているのか現状を詳細に把握するため、DigiCert ではテキサス州ダラスにある ReRez Research に依頼し、世界中の企業 400 社で PKI の管理を担当する IT マネージャーを対象に調査を実施しました。その結果、PKI 証明書を取り巻く混乱の全体像が浮き彫りになるとともに、優秀な組織が PKI 管理にどのように対処しているかについても明らかになりました。

企業が管理する必要のある
PKI 証明書数の増加率

43%

PKI 自動化とは

調査の回答者に対し、PKI 自動化の定義として次の要素が含まれるものとしました。

- 既存の電子証明書の検出
- 新規電子証明書の発行
- 有効期限が近づいた電子証明書の更新
- 必要に応じ電子証明書を失効
- コードサイニングの自動化
- クライアント証明書の登録申請プロセス
- ID 確認（ドキュメント署名用など）
- 拡張プロビジョニングアクティビティ（LDAP および Exchange への入力など）の自動化
- PKI 管理に関連するその他の組織内管理業務

1 2020 Global PKI and IoT Trends Study（Ponemon研究所）

PKI の急増がもたらす混乱

本調査の標準的な企業は現在、50,000 以上の証明書を管理しています。最も多い種類の証明書はユーザー証明書とサーバー証明書で、次にウェブサーバ、モバイルデバイス、E メールと続きます。企業が管理するパブリック証明書（パブリック認証局（CA）により発行された証明書）は、プライベート証明書（組織内のプライベート認証局によって発行された証明書）よりも 3 割程度多くなっています。

企業は現在、通常 **50,000** 以上の証明書を管理している。

これは前年と比べて急激な増加で、企業がワークロード管理に四苦八苦している十分な証拠があります。実際、予期せず期限切れになった証明書による停止を経験したことがある企業は 7 割近くにのぼります。この半年間だけでも、4 社に 1 社がそのような停止を 5、6 回程度経験していました。

なぜでしょうか。理由のひとつはワークロードの増加にあります。証明書の管理にかかる時間を非常に懸念している企業は 7 割近くにのぼります。しかし、可視化が十分でないという問題もあります。37% の企業が証明書の管理を 3 つ以上の部門で行っており、これが混乱を引き起こしています。調査によれば、一般的な企業では、実に 1,200 の証明書が実際に管理されていない野放しの状態になっており、半分近く（47%）が「不正な」証明書（IT 部門が知らぬ間に未管理で実装された証明書）がよく見つかると述べています。これらの問題を解決するためのソリューションが PKI 自動化であることは明らかです。そこで、企業における PKI 自動化の導入状況を調べました。

61% 証明書の管理にかかる時間を懸念している

47% 不正な証明書がよく見つかる

37% 証明書を管理している部門が 3 つ以上ある

この半年間に PKI 関連の停止を 5、6 回程度経験した

91% の企業が PKI 自動化を求めている

この調査結果によれば、ほとんどの企業 (91%) が PKI 自動化について少なくとも議論していることが分かりました。PKI 自動化についての議論がなく、議論する予定もないという回答した企業はわずか 9% です。企業の大多数 (70%) は 12 カ月以内の導入を見込んでいます。実際、25% の企業が既に実装中、もしくは実装が完了した段階にあります。しかし、それは簡単ではありません。企業が述べた課題には、自動化のコストが高い、複雑性、コンプライアンスの問題、スタッフや経営陣が変化を嫌うといったことがありました。

トレンド

企業が PKI 自動化を採用する主な理由は次のとおりです。

1. 不正な証明書
2. 耐量子コンピューティングへの対応
3. 証明書の有効期限の急速な短期化に伴い爆発的に増加しているワークロード
4. 管理する証明書数の急増
5. リモートワークのトレンド

問題点

企業を自動化に駆り立てるセキュリティの問題には次のようなものがあります。

1. 新しい証明書のプロビジョニングが遅い
2. 証明書の設定でミスしやすい
3. 担当者にかかる過度の負担
4. 不正な証明書の過度の増加
5. 証明書の有効期限切れ
6. 必要なときに証明書の失効に時間がかかるか、あるいは処理に失敗する

ペナルティー

PKI を自動化しないことによる負のコストは次のとおりです。

1. コンプライアンスの問題
2. セキュリティの問題
3. コスト
4. ダウンタイム
5. 怒った顧客や従業員

目標

PKI 自動化を導入する企業は次のことを目的としています。

1. セキュリティの向上
2. コンプライアンスの向上
3. 俊敏性の向上
4. 生産性の向上
5. ダウンタイムとコストの削減

最上位層と最下位層

多岐にわたる PKI メトリクスに対して各回答者がどの程度うまくいっているか（いないか）を判断するため、次のような質問をしました。

- 証明書の予期せぬ期限切れによるダウンタイムを回避
- 必要に応じ証明書をすぐに失効
- 電子証明書の効率的管理
- 不適切な証明書の管理によるセキュリティリスクの最小化
- 不適切な証明書の管理によるコンプライアンスの問題
- 不正な証明書を最小化
- PKI 関連の SLA を満たす
- PKI の発行および失効スピード

質問についての各回答を、達成度に基づいて、プラス～マイナスの点数を割り振り、スコアの合計値を算出しました。

回答者の対応状況の違いを明確にするため、回答者を 3 つのグループに分けました。

1 **先導グループ（リーダー）**

上記のさまざまなメトリクスを通して最高のスコアを出した組織です。

2 **ミッドレンジ**

上記のさまざまなメトリクスを通して中間のスコアを出した組織です。

3 **遅滞グループ（ラガード）**

上記のさまざまなメトリクスを通して最低のスコアを出した組織です。

次に、リーダーと遅滞グループを比較してその差を調べ、リーダーが実施している施策の違いを詳しく調査しました。

リーダーと遅滞

回答者は、各企業が直面している PKI 管理の問題について率直に述べてくれました。回答者は不正な証明書、予期せぬ証明書の期限切れによる停止など、多くの問題に直面しています。しかし、その問題の度合いは企業によって異なります。そこで、回答者を 3 つの層に分け、最上位層と最下位層を比べました。その違いは衝撃的なものでした。

率直に言って、リーダーのほうがうまくいっています。顕著なのは、3 割（33%）がそもそも PKI 自動化は重要と考えると述べていることです。リーダーのほうが以下の点について 2 ～ 3 倍うまくいっています。

- PKI のセキュリティリスクの最小化
- PKI ダウンタイムの回避
- 不正な証明書の最小化
- PKI の SLA の順守
- 電子証明書の管理
- 証明書の発行と失効
- コンプライアンス

一方、遅滞グループには PKI 証明書を管理するスキルがないために厳しいペナルティが課せられています。たとえば、次のようなことが挙げられます。

- コンプライアンスの問題
- セキュリティの問題
- 生産性の低下
- 遅延
- 過重労働
- 顧客の喪失
- 収益の損失

ではリーダーがリーダーたる所以は何でしょうか。私たちが PKI リーダーから学べることはあるのでしょうか。

PKI 自動化リーダーの特性

PKI リーダーは、PKI 証明書の管理にかかる時間について他の層の 2 倍懸念しています。だから PKI 管理に注力し続けるのです。また、不正な証明書についても他の層より懸念しています。さらに、PKI 自動化が組織の未来にとって重要だと考えています。おそらく、このことが既に PKI 自動化を実装済みと回答した企業が 6 倍である理由です。ここから学べることは何でしょうか。行動をどのように変えたらよいでしょうか。

無法地帯効果

データを深く掘り下げていったときに、興味深い問題点に気が付きました。理論上は PKI 証明書の管理をもっと余裕をもってこなせるはずのグループが、証明書の管理に四苦八苦していることが多いとわかったのです。

たとえば、管理する証明書の数が最も少ない企業のほうが、予期せぬ期限切れによる停止を経験する確率がずっと高い傾向にありました。また、こうした企業ではさまざまな PKI 管理項目について一様に低いスコアを出していました。

そのため、「少量」の PKI 証明書を扱うこれらの企業は、「大量」に扱っている企業よりも管理する証明書の数が桁外れに少ないのにもかかわらず、PKI の管理が非常に懸念されました。たとえば、PKI 証明書の管理にかかる時間を懸念していると回答したのは、「少量」を扱う企業のほうが 50% 近くも多いという結果でした。また、こうした企業が PKI 自動化プログラムで管理している証明書の割合は 2 倍近くにのぼります。

当初、これは矛盾しているように思えました。しかし、これらの「少量」を扱う企業の PKI 管理手法は実際には未成熟なものでした。100,000 を超える証明書を管理することも珍しくない、「大量」の PKI 証明書を扱っている企業では、その管理が極めて成熟しているのに対し、「少量」を扱う企業の状況は無法地帯のようなものです。何のルールもなく、誰もが勝手に証明書を管理しているのです。

証明書数が少ない企業の状況は無法地帯のようなもの。何のルールもなしに、誰もが勝手に証明書を管理している。

PKI 自動化リーダーの特性

PKI 管理のリーダーは、自社の証明書のインベントリを極めて責任をもって管理しているため、逆に、証明書についてあまり考えていない企業よりも辛口のスコアを付けるという結果になっていました。しかし、こうした組織では、証明書に関連するダウンタイムや、不正な証明書に関する報告が少なく、実際には彼らが想像するよりもうまく管理していることが分かりました。

自己評価のパラドックス

もうひとつの興味深い発見は、PKI 証明書の管理について最も懸念している企業間の差異です。懸念していると答えた企業は、客観的に見て他社より問題が少ないにもかかわらず、自社を低く評価していました。

たとえば、PKI の管理は難しいと述べる傾向が高い企業を見てみましょう。これらの企業は、新しい証明書の発行スピード、証明書の設定ミス、不正な証明書の発見、証明書のその他の問題を含むさまざまな分野について幾分、または極めて懸念していると答える傾向が他のグループより 3 ～ 5 倍ありました。

しかし、同時に実際の不正な証明書の件数は少なかったという結果が出ました (懸念していないと回答した企業のわずか 2/3)。さらに、証明書の予期せぬ期限切れによる停止を経験した回数も大幅に少なかったのです (懸念していないと回答した企業ではこの半年間に 3 ～ 5 回あったのに対し、たったの 1 回)。

セキュリティ関連の調査ではこのような現象がよく見られます。つまり、最も注意を払っている企業が自社の不十分な点や失策について最も強く意識しているため、意識していない企業と比べて自らを厳しく評価しがちなのです。しかし、そのように綿密な注意を払っているために、実際には、意識していない企業よりもずっと良好な結果を出しています。

PKI 証明書の管理を懸念している企業は、客観的に見て他社より問題が少ないにもかかわらず、自社を低く評価していました

推奨するステップ

PKI 証明書カタログを通じて広く自動化を利用すれば、組織全体として大きなメリットがあり、特に認証時間の短縮、暗号標準の進化、さまざまな業務プロセスでの電子証明書の採用促進といった変化を期待できます。では、自動化の取り組みに着手するとき、組織はどのような点を考慮すべきでしょうか。自動化によって証明書管理の目的をサポートする手順を、チェックリストとしてまとめてみました。

証明書管理

特定
証明書の全体像のインベントリを特定および作成します。

是正
企業ポリシーに従っていない鍵と証明書があれば是正します。

保護
発行と失効のベストプラクティスで保護します。登録申請、発行、更新を標準化および自動化します。

モニター監視
新しい変更があるかどうかモニターします。

証明書ワークフローの自動化

特定
管理されていない、または手動管理の証明書ワークフローを特定します。

実装
証明書ワークフローを一元的に管理するソフトウェアを使った自動化を実装します。

モニター
集中型の可視化と制御でモニターします。

一般的な証明書ワークフロー

- ウェブサーバー
- デバイス ID および管理
- コードサイニング
- 電子署名
- アイデンティティとアクセス

調査方法

テキサス州ダラスの ReRez Research は、北米、EMEA、アジア太平洋、中南米で 1,000 人の従業員を抱える 400 の企業の IT 専門家を対象に調査を実施しました。回答者は、IT 部門長、IT セキュリティマネージャー、IT 担当者に分類されます。特にユーザー、サーバー、モバイルデバイスの電子証明書の管理を担当する IT 専門家に焦点を当て、中小企業から大企業までを調査しました。

組織のニーズを評価し、カスタマイズされたソリューションについて相談するには、DigiCert PKI 自動化のエキスパートにお問い合わせください。PKI 実装の自動化を開始する方法はこちらをご覧下さい。