PKI 自動化に関する現状

2021 レポート

PKI×ˆ=t b”qÝ : 2021èÙ”Ä

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。

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

企業が管理する必要のある
PKI 証明書数の増加率

43%

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

PKI × ˆ = t　b ” q Ý　　: 2021è Ù ”Ä

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。

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

PKI×ˆ=t b”qÝ : 2021èÙ”Ä

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。

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

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

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

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。

PKI×ˆ=t　b”qÝ　　:2021èÙ”Ä

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。

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

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

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

保護

モニター監視

証明書ワークフローの自動化

特定

実装

モニター

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