digicert®

TLS/SSL証明書の管理
ベストプラクティスチェックリスト

TLS/SSL証明書の管理チェックリストです。
可視化を高め、人的エラーを減らし、不正な証明書を取り除きます。

1. 確認

- ☐ 発行した証明書を全てリストアップする
- ☐ 証明書のインストール先をすべて明らかにする
- ☐ すべての証明書とドメインについて、それらの担当者を明確にする
- ☐ WebサーバーのOSとアプリケーションのバージョンを確認する
- ☐ Webサーバーの暗号とTLS/SSLのバージョンを確認する

2. 改善

- ☐ 脆弱な鍵や暗号、ハッシュを取り除く
- ☐ ワイルドカード証明書の発行とインストール先を制限する
- ☐ 適切な種類の証明書をインストールする
- ☐ 通常ベンダーCAの証明書をすべて管理する
- ☐ Webサービスのすべてに最新のパッチを適用する

3. 防御

- ☐ 証明書の発行と更新のプロセスを標準化および自動化する
- ☐ 全ての証明書のインストールと更新を速やかに行う
- ☐ 証明書を更新するときに秘密鍵（と関連CSR）を再利用しないようにする
- ☐ 証明書と秘密鍵は安全な方法でインストールする
- ☐ 証明書の使用を停止する場合は、証明書を削除、失効させる

4. 監視

- ☐ 新たなシステム追加や変更の際にネットワークをスキャンする
- ☐ CT ログをチェックして、不正な証明書が存在しないか確認する
- ☐ 許可を得ずに証明書がリクエストされるのをCAAを利用して防ぐ