

PCI-DSSに準拠したシステムの内部ネットワークで信頼できるSSL証明書を利用していますか。

内部ネットワークのセキュリティ

PCI DSSでは内部ネットワークについても脆弱性監査とペネトレーションテストが規定されています。

しかしPCI準拠システムでも暗号化していない通信が原因でデータ漏えい事件も起きています。

内部ネットワークでも暗号化の必要性が明らかになってきています。

管理通信におけるPCI-DSS要件

2.3 すべてのコンソール以外の管理アクセスをSSH、VPN、またはSSL/TLSなどのテクノロジーで暗号化する。

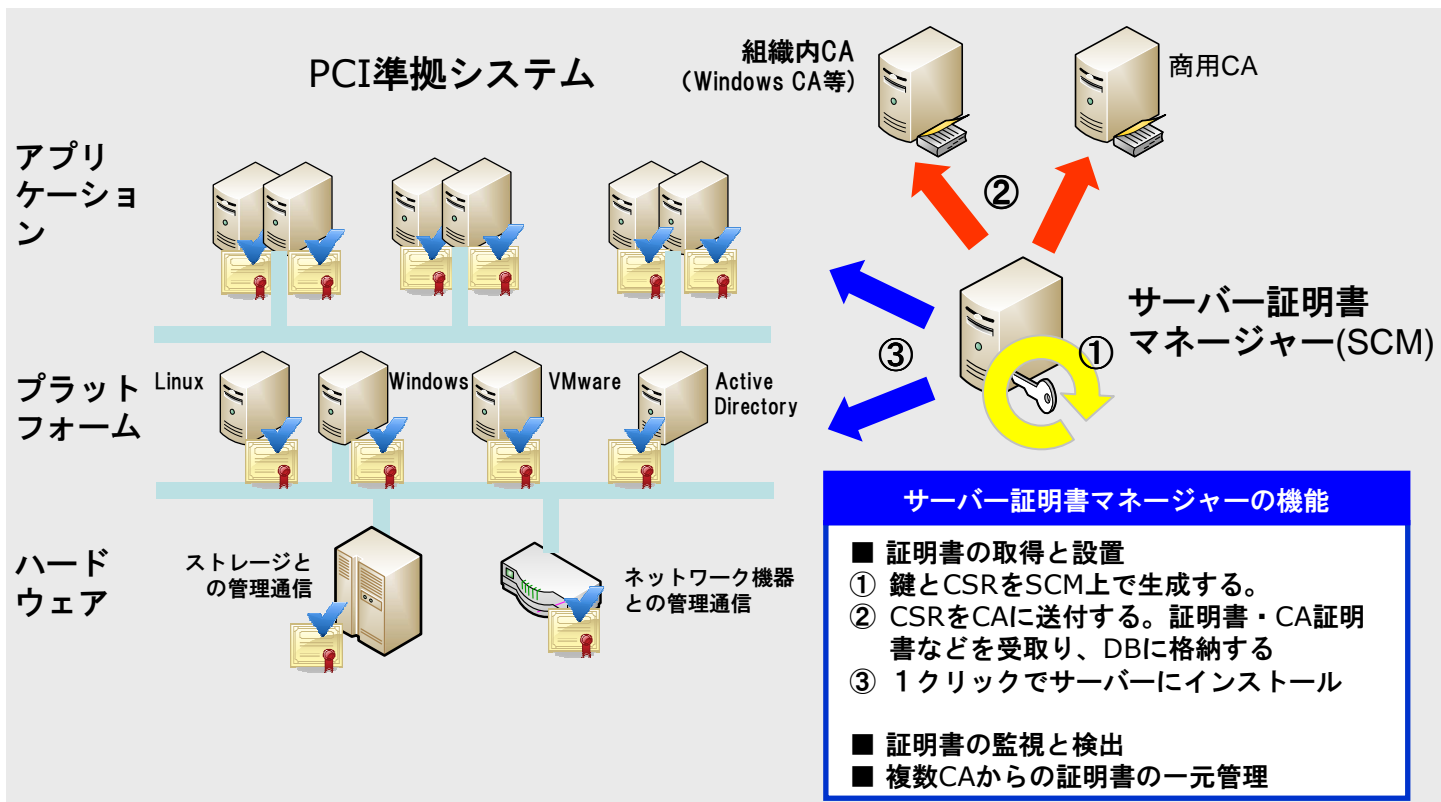
オープンネットワークにおけるPCI-DSS要件

4.1a 信頼できるSSL/TLS証明書のみを受け付ける。
4.1a 適切な強度の暗号化が実装されていること。
(SSL/TLSの場合128bit以上のAES,1024bit以上のRSAなど)



PCI準拠のためにITシステムの修正・監視・レポート、文書化、プロセス改善などを行いますが、重要なのはそれらを継続可能にすることです

Kousecサーバー証明書マネージャーは、ITシステムの全レイヤにおいて信頼できるSSL通信の運用の自動化を実現します。



記載されている会社名、製品名は、各社の登録商標または商標です。