FUJITSU
shaping tomorrow with you

FUJITSU Software Systemwalker PKI Manager V12.0.4 機能ご紹介

2013年10月
富士通株式会社

FUJITSU

PKI 概要

- PKIシステムの動向
- 目的に合った認証システムの構築

PKIシステムの動向

FUJITSU

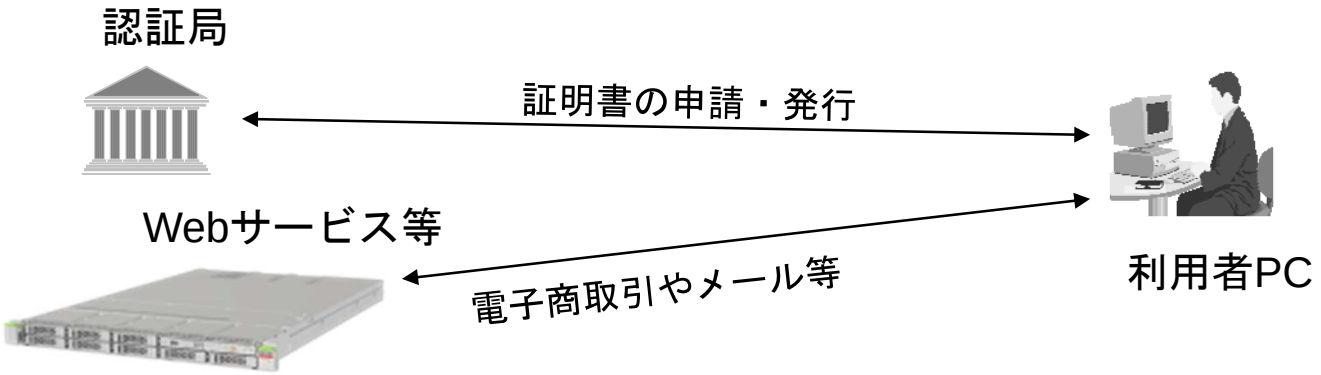
～背景～

■PKI(公開鍵基盤)は電子政府・電子署名の要

- ◆G to Gシステム
- ◆G to Bシステム
- ◆G to Cシステム
- ◆B to Bシステム
- ◆B to Cシステム

- ◆運用の効率化

高信頼認証局システムの必要性



目的に合った認証システムの構築

FUJITSU

～狙い～

■ 電子署名法対応システム

·電子署名法における特定認証業務の要件に対応

•電子署名法対応のPKIシステムが構築可能

■ 電子政府対応システム

•電子政府のGPKI要件に対応

•GPKIにおける政府側システム・民間側システムの構築が可能

■ 社内システム

•従業員証のICカード化による全従業員向け証明書の一括発行の運用に対応

•業務システムと連携した証明書の自動発行/失効

•携帯電話やスマートフォン向けの証明書発行

■ エンドユーザ向けシステム

•証明書発行サービスによる、申請に基づいた証明書の個別発行に対応

※ 電子署名法(正式名称:電子署名及び認証業務に関する法律)
2001年4月に施行された、認証業務の認定制度等を定めた法律。

FUJITSU

ご紹介

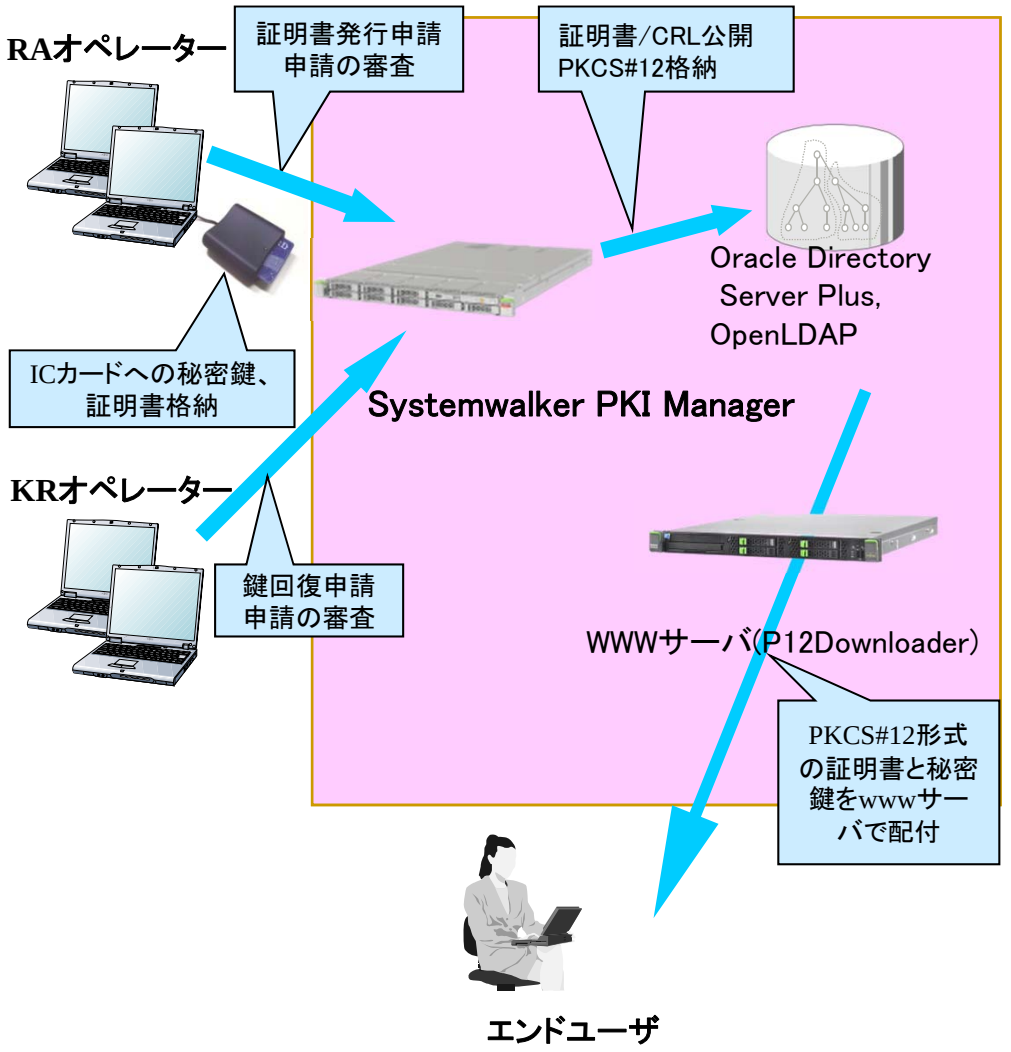
- 証明書の発行・失効
- 証明書の大量発行
- CA合議操作管理
- RAオペレータによる証明書申請
- RAOステータスチェック
- 構成例
- 認証局コンサル及び構築概要
- 製品体系

証明書の発行・失効

～証明書の発行・配付・失効・鍵回復～

証明書の発行・失効・鍵回復

- 証明書の発行
  - ーX.509 V3準拠の証明書の発行が可能
  - ーエンドエンティティで秘密鍵、公開鍵ペアを生成(PKCS#10)
    →エンドユーザに証明書(PKCS#7)を配付
  - ーRA内部で秘密鍵、公開鍵ペアを生成
    →エンドユーザに秘密鍵と証明書(PKCS#12)を配付
  - ーOracle Directory Server PlusやOpenLDAPと連携して、ディレクトリ経由で配付することも可能
- 証明書の失効
  - ー証明書を失効し、X.509 V2準拠のCRL(証明書失効リスト)の発行が可能
  - ーRAオペレーターが失効を申請
- 鍵回復
  - ーRAで秘密鍵/公開鍵ペアを生成した場合、紛失や破損時でも回復可能
  - ーKR(Key Recovery)オペレーターが鍵回復を申請/取得

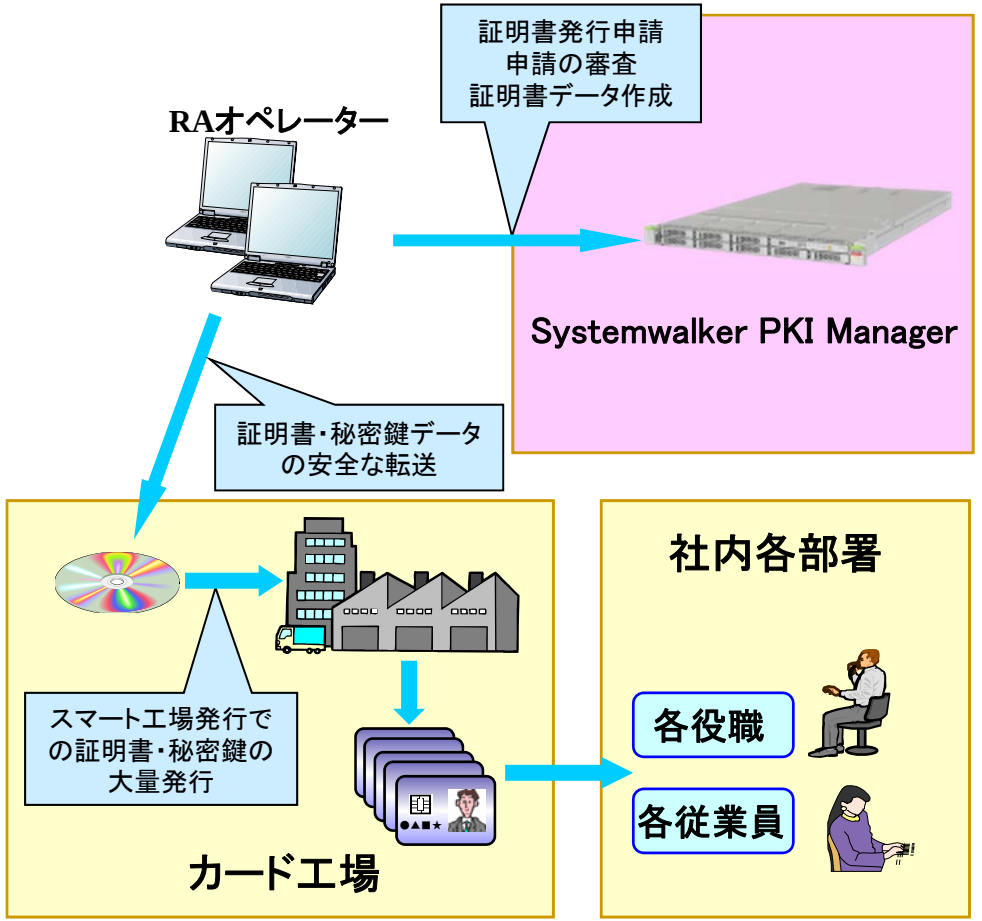


証明書の大量発行

～従業員カード発行など～

■ 一括発行対応

- 証明書の一括大量発行に対応
  - ー操作の容易性
- 作成方法は2種類
  - ーカード作成用データとして作成し、カード会社でカード化
    →従業員証のICカード化など
  - ーPKCS#12形式データとして作成し、ユーザに配付
    →WebブラウザやメールのPKI対応用データの一括発行など



CA合議操作管理

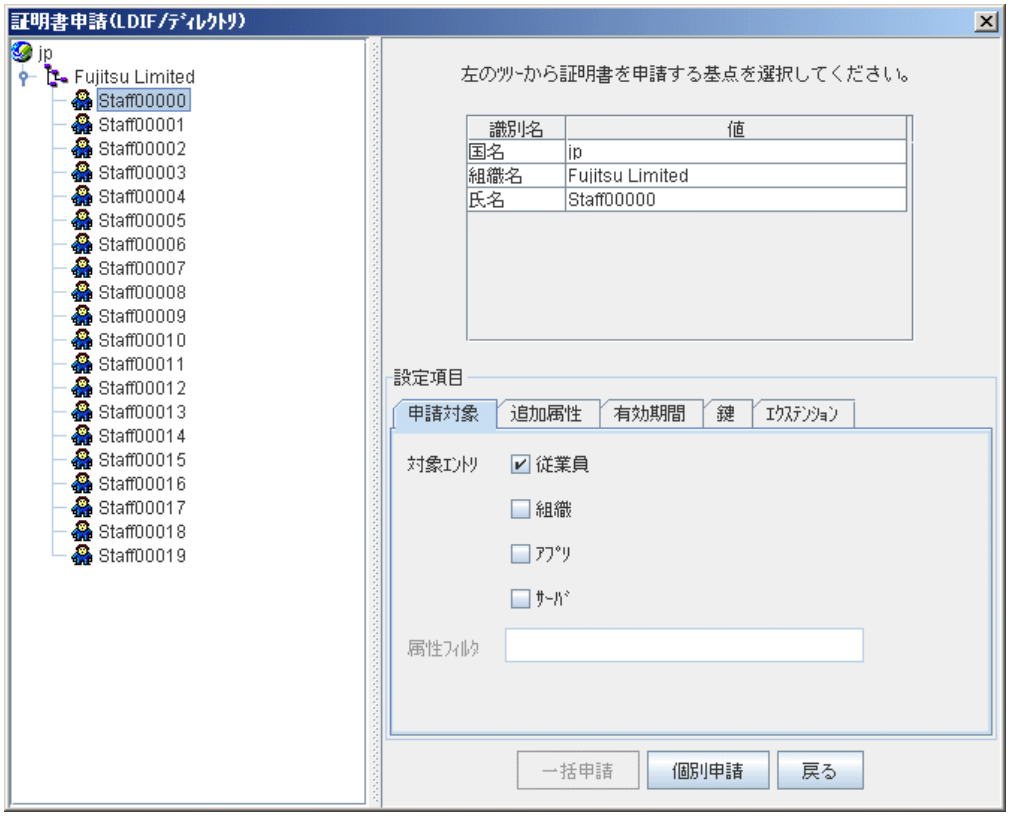
～画面例～

操作	最小合議者数	合議者	
		tarou	hanako
CA秘密鍵の生成	2	☑	☑
CAデーモンの起動	2	☑	☑
CAデーモンの停止	2	☑	☑
トークンの活性化	2	☑	☑
トークンの非活性化	2	☑	☑
鍵のバックアップ	2	☑	☑
鍵の復元	2	☑	☑
合議操作設定の変更	2	☑	☑
CA証明書の発行、登録	2	☑	☑
申請書の作成	2	☑	☑
CMPサーバ証明書の発行	2	☑	☑
環境設定	2	☑	☑
タイプ管理	2	☑	☑
相互認証証明書の発行、登録	2	☑	☑
鍵と証明書の作成	2	☑	☑
申請書から証明書の作成	2	☑	☑
証明書・CRLの登録	2	☑	☑
証明書の失効、削除	2	☑	☑
CRLの発行	2	☑	☑
CRLの削除	2	☑	☑

RAオペレータによる証明書申請

～画面例～

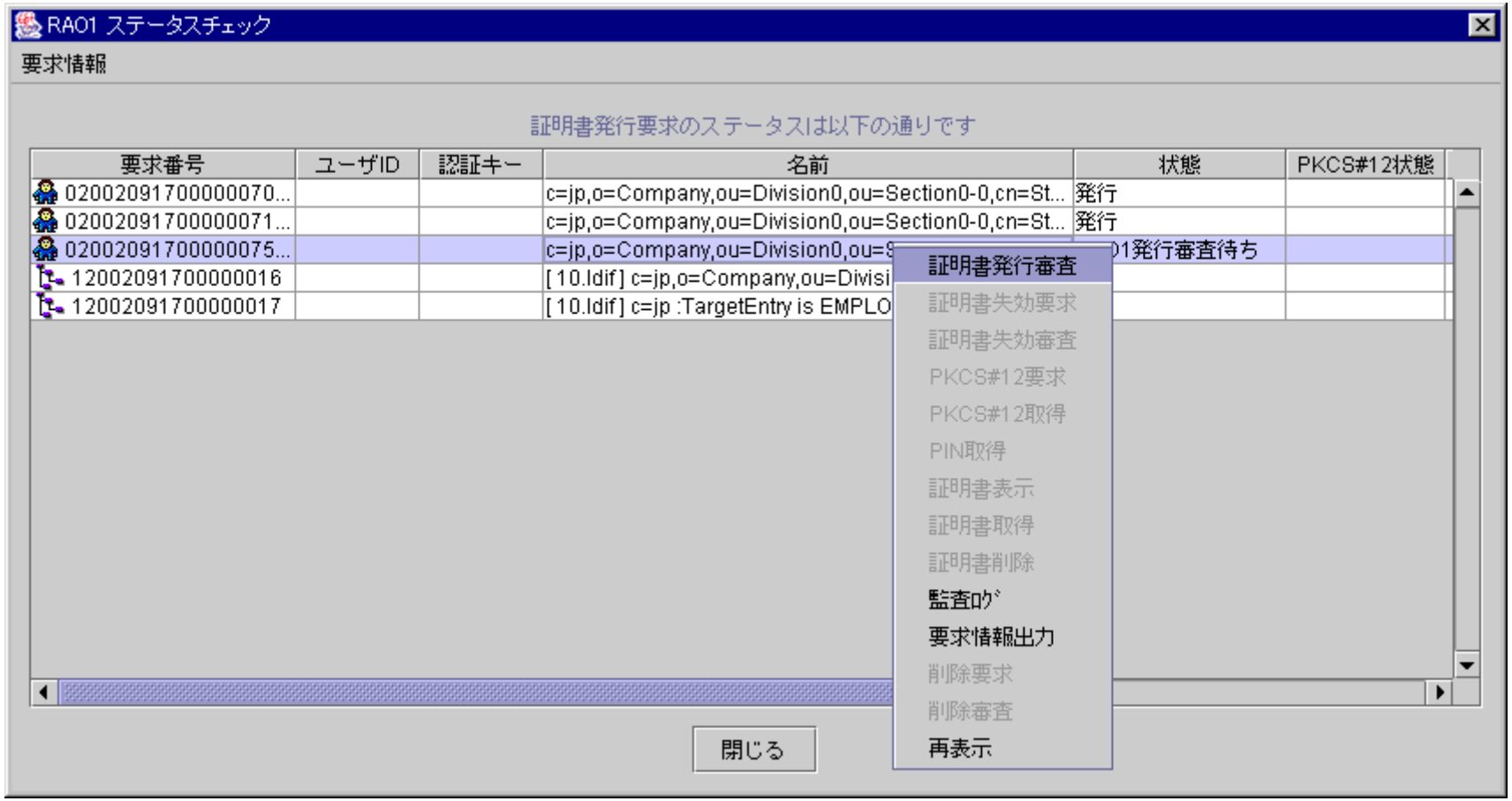
【PKCS#12方式の場合】



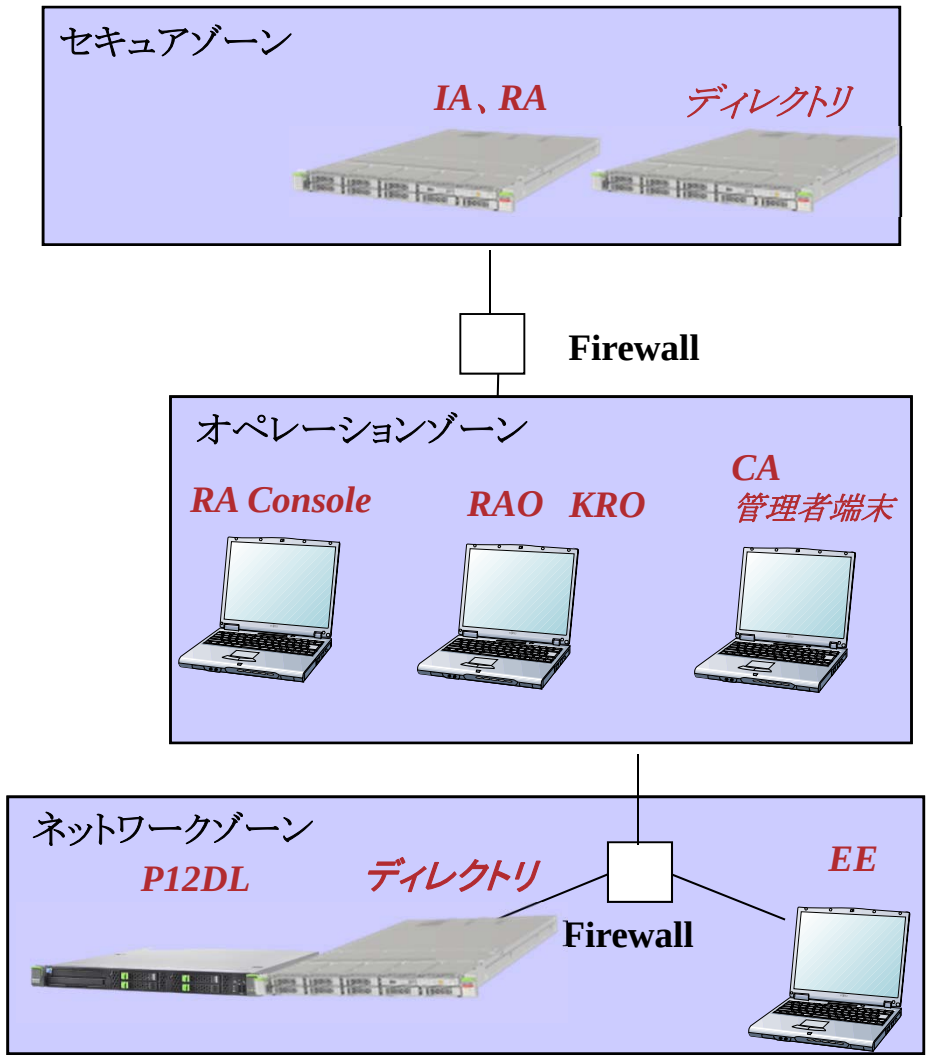
【PKCS#10/7方式の場合】

RAオペレータによるステータスチェック

～画面例～



構成例



■セキュアゾーン

認証局サーバ(IA,RA)の本体を設置する区画。PKI コンポーネントの心臓部で、最も高度なセキュリティが必要な部分です。通常は無人で運用し、ネットワーク設備も最小限に留めます。

・IA（Issuing Authority：発行局）
　証明書の発行/失効を行います

・RA（Registration Authority：登録局）
　EE を審査して証明書の発行申請や失効要求の是非を判断し、
　IA に証明書の発行や失効を依頼します。

■オペレーションゾーン

認証局操作用端末や登録局操作用端末を設置する区画。管理者が認証局や登録局を操作したり、エンドユーザに対する証明書発行承認・失効承認・鍵回復承認の操作などの日常の業務を行う区画です。

・認証局管理端末
　IA管理者端末(IAの管理)、RAコンソール(RAの管理)

・RAO（RA Operator） 証明書申請の一括・個別申請/審査/取得

・KRO (Key Recovery Operator) 鍵回復操作の申請/審査/取得

■ネットワークゾーン

EE が直接利用するサーバを配置する区画。イントラネット内のみのアクセスなら、イントラネットからのアクセスができる区画でかまいません。

・P12DL（PKCS#12 Downloader ）
　PKCS#12形式の証明書をﾃﾞｨﾚｸﾄﾘからのﾀﾞｳﾝﾛｰﾄﾞし証明書利用者に提供

・EE（End Entity：証明書利用者端末）

認証局コンサル及び構築概要

FUJITSU

設　計	構　築	運　用

Directory

・設計コンサルティング ・スキーマ設計 ・アクセス制御設計 ・サーバ連携設計　…etc	・Directory構築 ・スキーマ設定 ・アクセス制御設定 ・サーバ連携設定　…etc	・メンテナンス ・導入教育 ・Q&A

PKI

・ 認証局運用規程（CPS）作成支援 ・ 認証局ファシリティ構築コンサル ・ サービス約款の作成支援	・ 認証局ファシリティ構築 ・ 認証局構築 ・CAシステム構築 ・証明書発行ポリシー設定 ・Directory連携構築 ・カスタマイズ　…etc	・メンテナンス ・導入/運用教育 ・Q&A

スマートカード

・スマートカードデザイン作成サービス	・スマートカード二次発行サービス	・メンテナンス

ご提供サービス

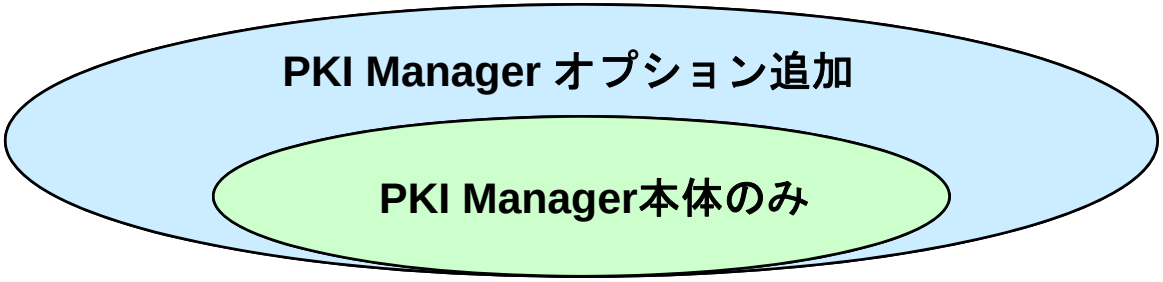
PKI PROPOSE，スマートカード発行・導入サービス

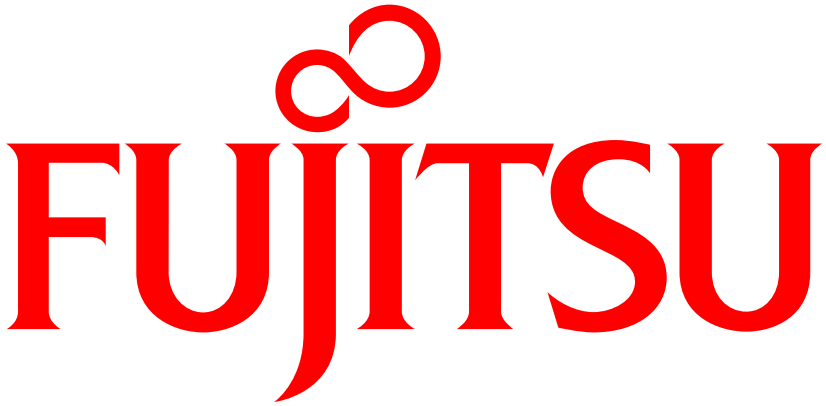
製品体系

FUJITSU

- **Systemwalker PKI Manager（本体のみ）**
  - ・基本モデル（100ユーザまで）

- **Systemwalker PKI Manager（オプション追加）**
  - ・ユーザ追加ライセンス
    500, 1000, 2000, 5000, 10000, 20000, 50000, 100000の８パターン





shaping tomorrow with you