本資料について

- 本資料は下記論文を基にして作成されたものです．
  文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．

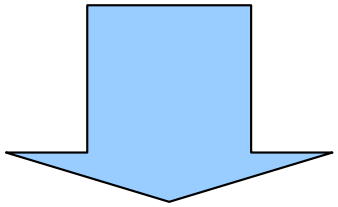
- 著者：高橋　成文，東川　淳紀，山本　修一郎，小尾　高史，谷内田　益善，大山　永昭
- 論文名：2階層PKIを用いたオンデマンドVPNシステム
- 出展：情報処理学会論文誌　Vol.46　No.5
- 発表日：2005年5月

2階層PKIを用いたオンデマンドVPNシステム

名城大学　理工学部
今村　圭佑

はじめに

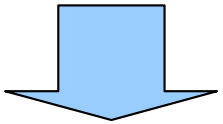
- 携帯電話やPDA等の小型端末の普及
- ホットスポットの増加
  - いつでもどこからでもインターネットに接続可能
- IPsec等の暗号化技術を用いたVPNの普及
  - セキュアな通信路を安価に構築可能



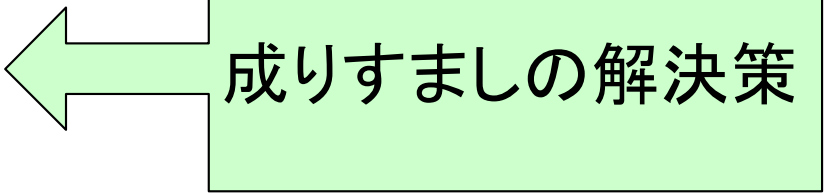
セキュアなユビキタス環境

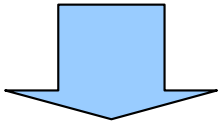
ユビキタス環境におけるVPNの課題

- 端末の小型化による盗難
  - 成りすまし脅威



公開鍵証明書による認証





公開鍵証明書が保存されている端末自体が盗難

成りすましの脅威は解決されていない

ユビキタス環境におけるVPNの課題

- VPN接続を行う為の必要な情報が特定できない
  - 接続元，接続先双方の暗号化アルゴリズムや鍵情報等を事前に設定しなければならない

従来は

自宅から会社へ接続するなど，必要な情報は，既知であることが前提であり，あまり問題にならなかった

ユビキタス環境では

VPN接続に必要な情報が事前に特定できるとは限らない

事前に必要な情報をVPN装置に設定出来ない

VPN接続に必要な情報を要求に応じて自動に生成

ユビキタス環境におけるVPNの課題

- 接続先，接続元の環境が動的に変化
  - IPアドレスやIDとパスワードによる認証のみでは不十分

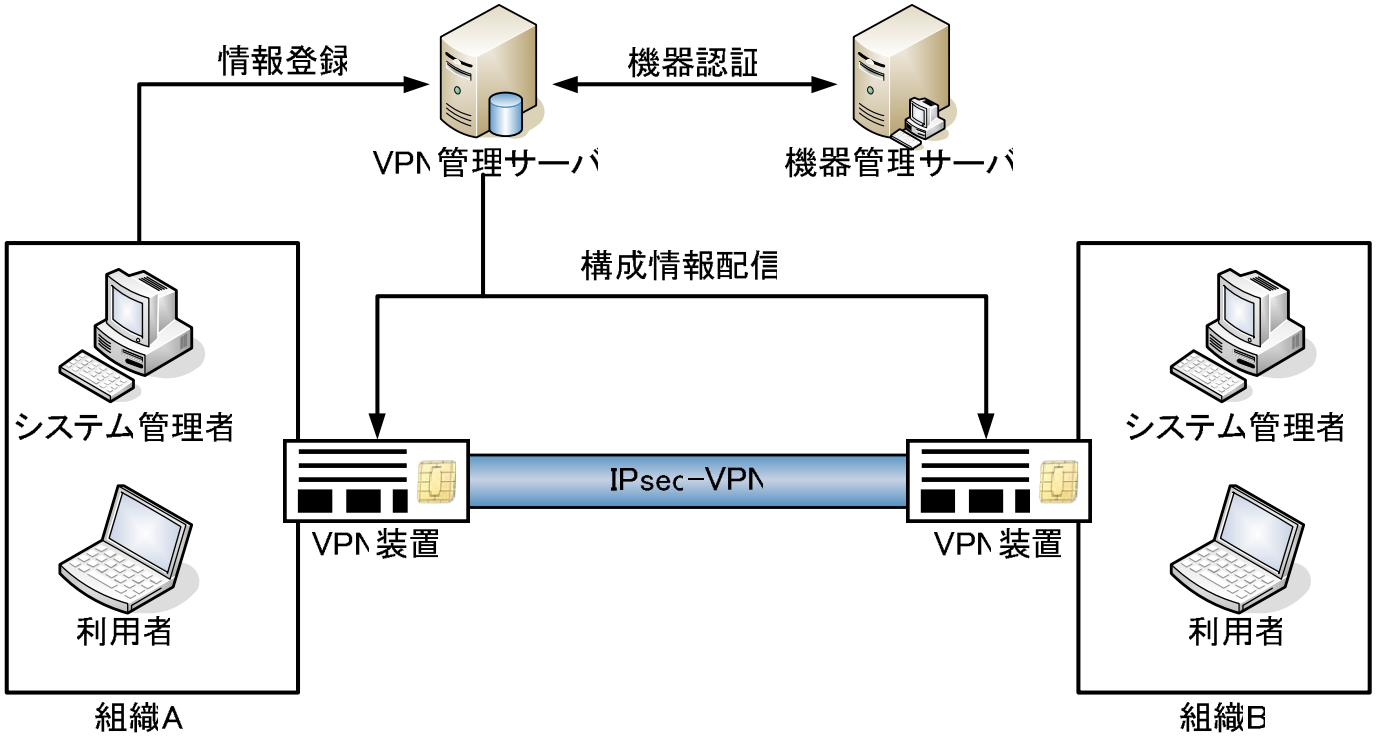
時間帯　位置情報　ユーザの属性情報　端末種別

柔軟にVPN接続の可否を制御可能であることが要求される

オンデマンドVPNでは3つの課題を解決

オンデマンドVPNシステム概要

- オンデマンドVPN構成要素
  - 機器管理サーバ（VPN機器の真正性を保障）
  - VPN管理サーバ（VPN接続を制御）
  - VPN機器（ICカード内臓のVPN機器）



オンデマンドVPNシステム概要

- VPN装置間はIPsec-VPNを使用
  - 鍵交換にIKE（Internet Key Exchange）を利用

  IKEを行うために必要となる情報をVPN装置に設定

設定情報の漏洩により，
機器の成りすまし，機密情報の漏洩

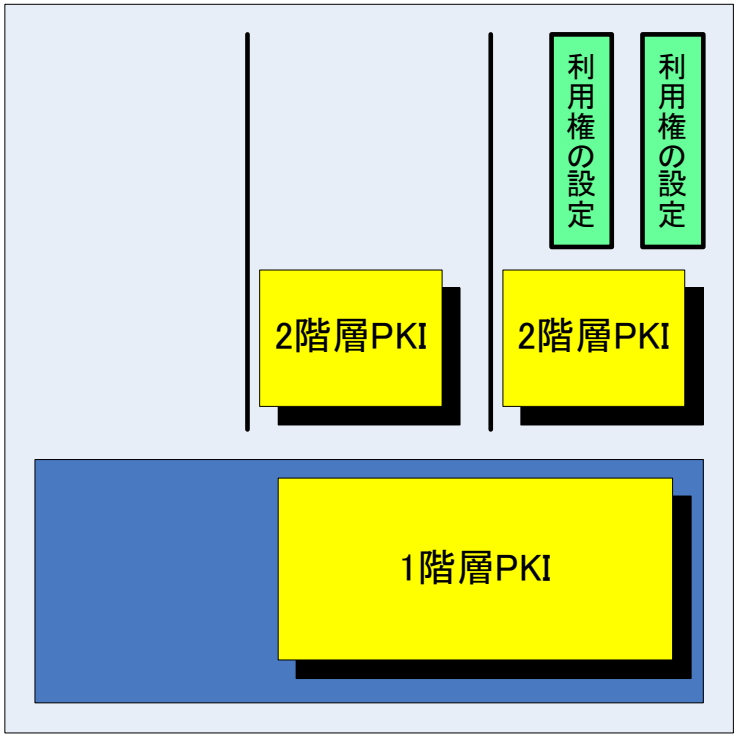
- オンデマンドVPNシステムでは・・・
  - VPN接続に必要な情報をVPN管理サーバで一元管理
  - 利用者の要求に応じてVPN装置に配信
  - 耐タンパ性e-Keyチップを VPN装置に組み込み，機器の成りすましを防止

オンデマンドVPNシステム概要

- オンデマンドVPNシステムを構成する技術
  - 2階層PKI技術に対応した耐タンパICチップ
    - 成りすましの問題を解決
  - IPsec構成情報生成技術
    - VPN装置の事前設定をなくし自動生成を行う
  - ポリシ制御技術
    - 柔軟にVPN接続の可否を行う

2階層PKI技術

- 第1レイヤー：チップの状態をコントロールするPKI
- 第2レイヤー：アプリケーション毎のPKI



2階層目のPKIに様々なアプリケーションを追加可能

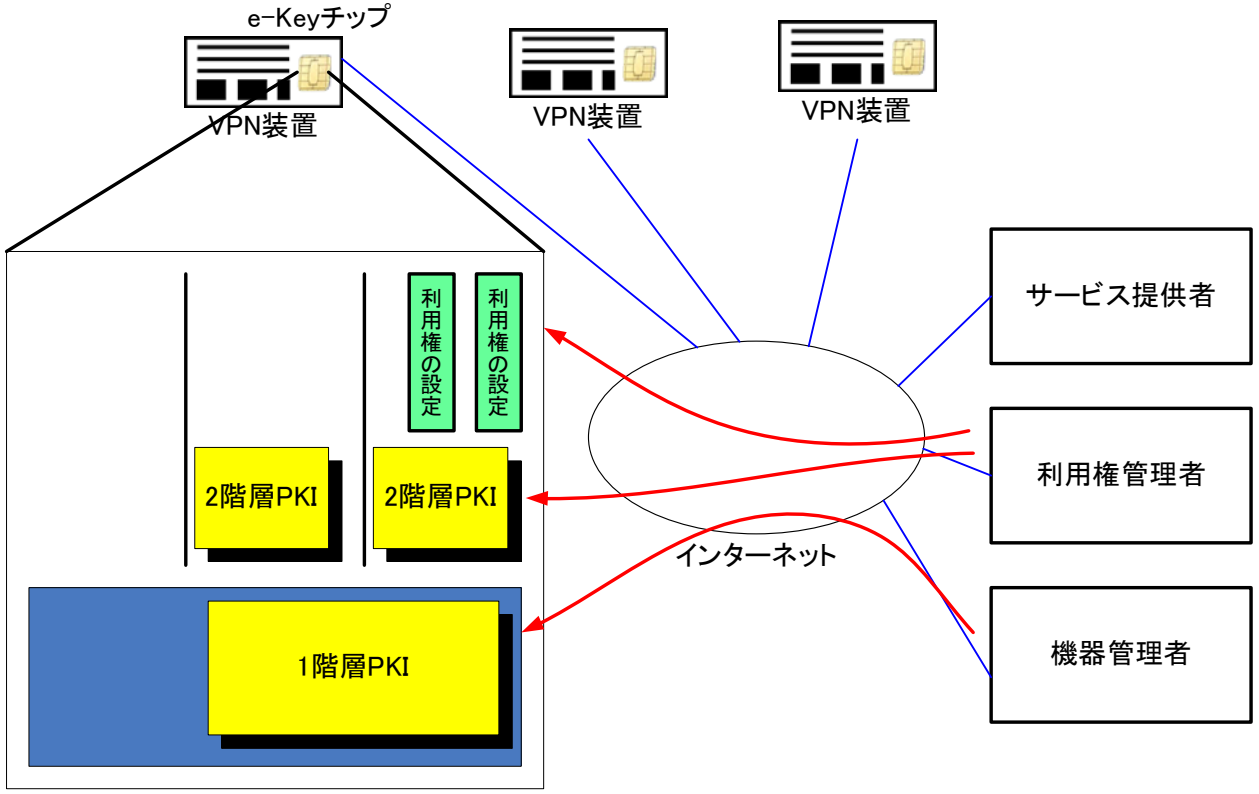
□1階層目のPKI情報をVPN装置認証に使用

□2階層目のPKI情報をVPNサービス利用権認証に使用

住民基本台帳ネットワークシステムに使用されており
すでに実用化されている

2階層PKI技術

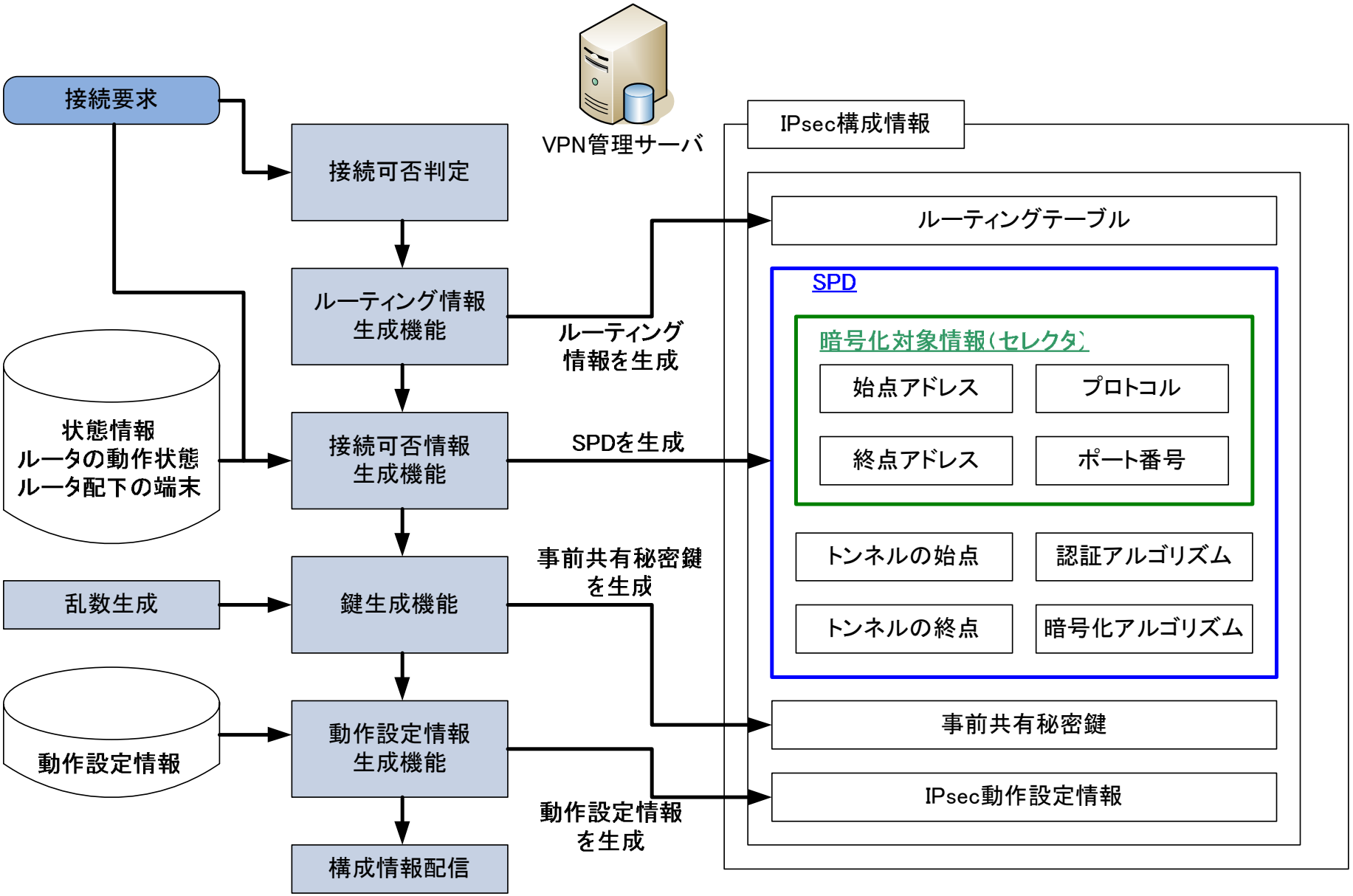
- e-Keyチップを搭載したVPN装置が機器管理者に認証される
- 1階層目のPKI情報が機器管理者によって設定
- 利用権管理者によってアプリケーションと2階層目のPKI情報を設定



IPsec構成情報生成技術

- VPN装置に配送するIPsec構成情報
  - セキュリティポリシーデータベース（SPD）
    - 暗号化処理対象パケットの選別するためのデータベース
    - 接続要求があったIPアドレスを元に生成・配信する
  - IPsec動作設定情報
    - VPN装置間のIPsec SAを生成するため情報
      - 認証方式や暗号化アルゴリズム，SAの有効期間など…
    - VPN管理サーバで管理し，接続要求と共にVPN装置に配信
  - 事前秘密共有鍵
    - IKEを行う前に事前共有秘密鍵認証方式を使用
    - VPN管理サーバで接続ごとに乱数を生成
    - VPN装置のe-Keyチップに書き込む
  - ルーティングテーブル
    - IPパケットの経路情報を記述したもの
    - VPN管理サーバがルーティングテーブルを生成・配信する

IPsec構成情報生成技術



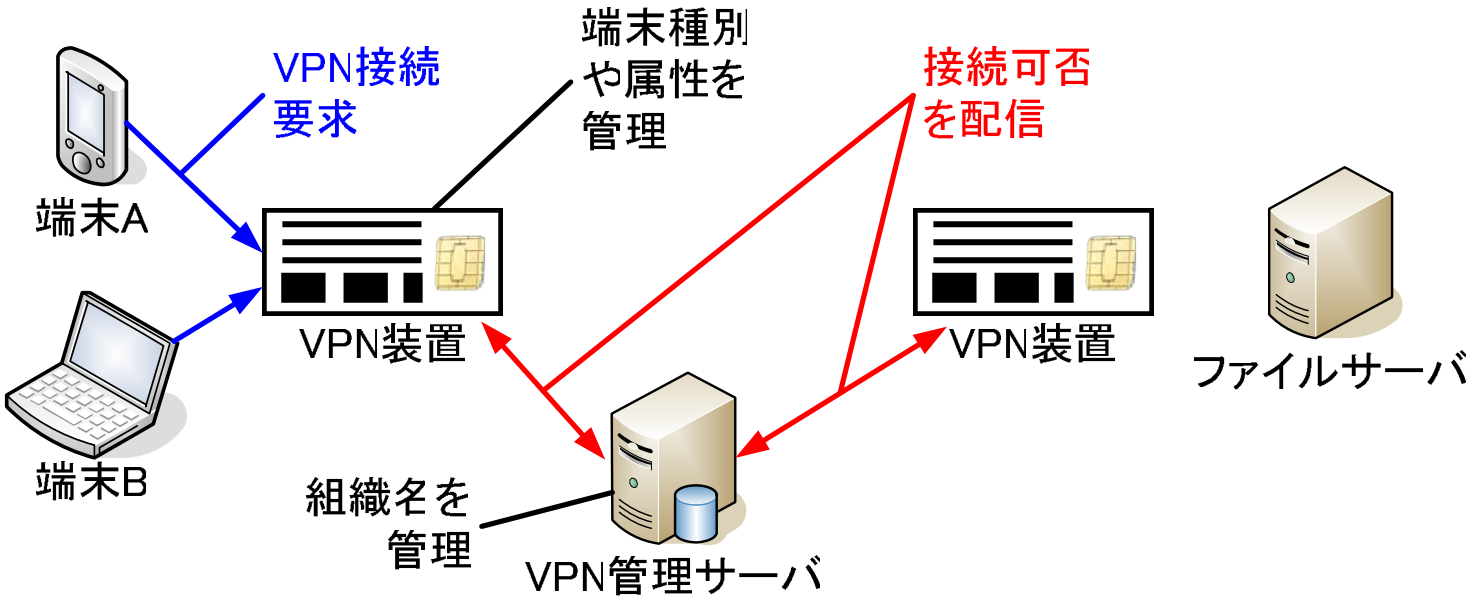
ポリシ制御技術

- 企業等がVPNを使用する場合
  - 企業の社員であることが前提
  - IPアドレスやID等の情報により個人を特定
  - SPDやRADIUS等の技術でセキュリティを保つことが出来た
- オンデマンドVPNシステムでは・・・
  - IPアドレスやID等の情報が事前に特定されていない
  - 相手の組織名や接続する端末の種別，時間帯，ユーザ属性といった単位でアクセス制御を実現

事前に静的に設定しておくおことは不可能

ポリシ制御技術

- VPN管理サーバ
  - VPN装置が利用されている組織名や設置されている場所を管理
- VPN装置
  - 端末の種別，ユーザ属性情報を管理



オンデマンドVPNシステムの動作概要

- 事前準備フェーズ
  - 機器登録
  - 利用権取得
  - 利用者登録
  - 接続ポリシ登録
  - 状態情報登録
- 利用フェーズ
  - 接続要求
  - 接続可否判定
  - 構成情報生成
  - 構成情報配信
  - 構築完了

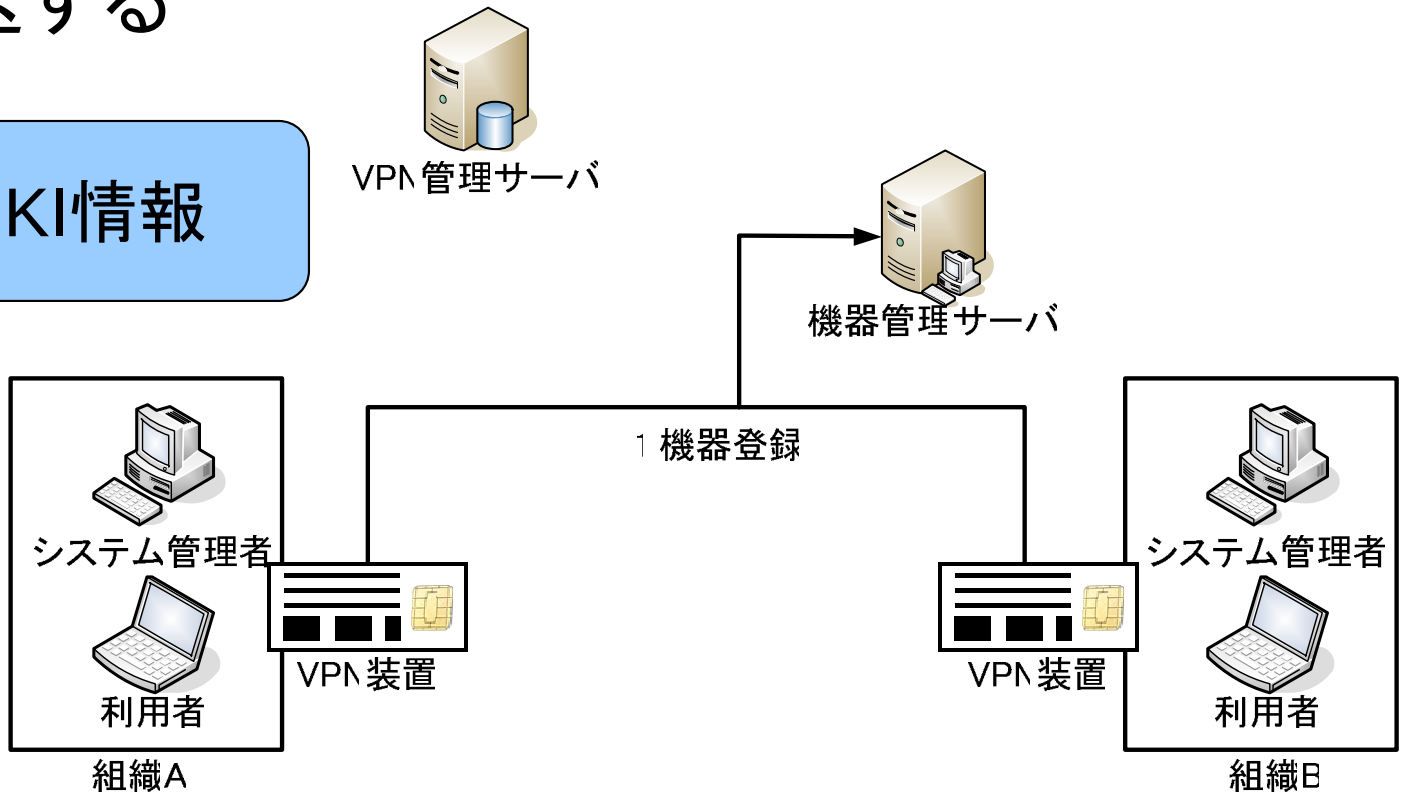
VPN装置やVPN利用者の登録，接続ポリシの設定

事前準備フェーズで登録された情報を元にVPNを構築

1.機器登録

- VPN装置のe-Keyチップ内に保存された仮の公開鍵証明書を用いてVPN装置の認証を行う
- 機器管理サーバで正式な公開鍵証明書・秘密鍵を生成し配送する

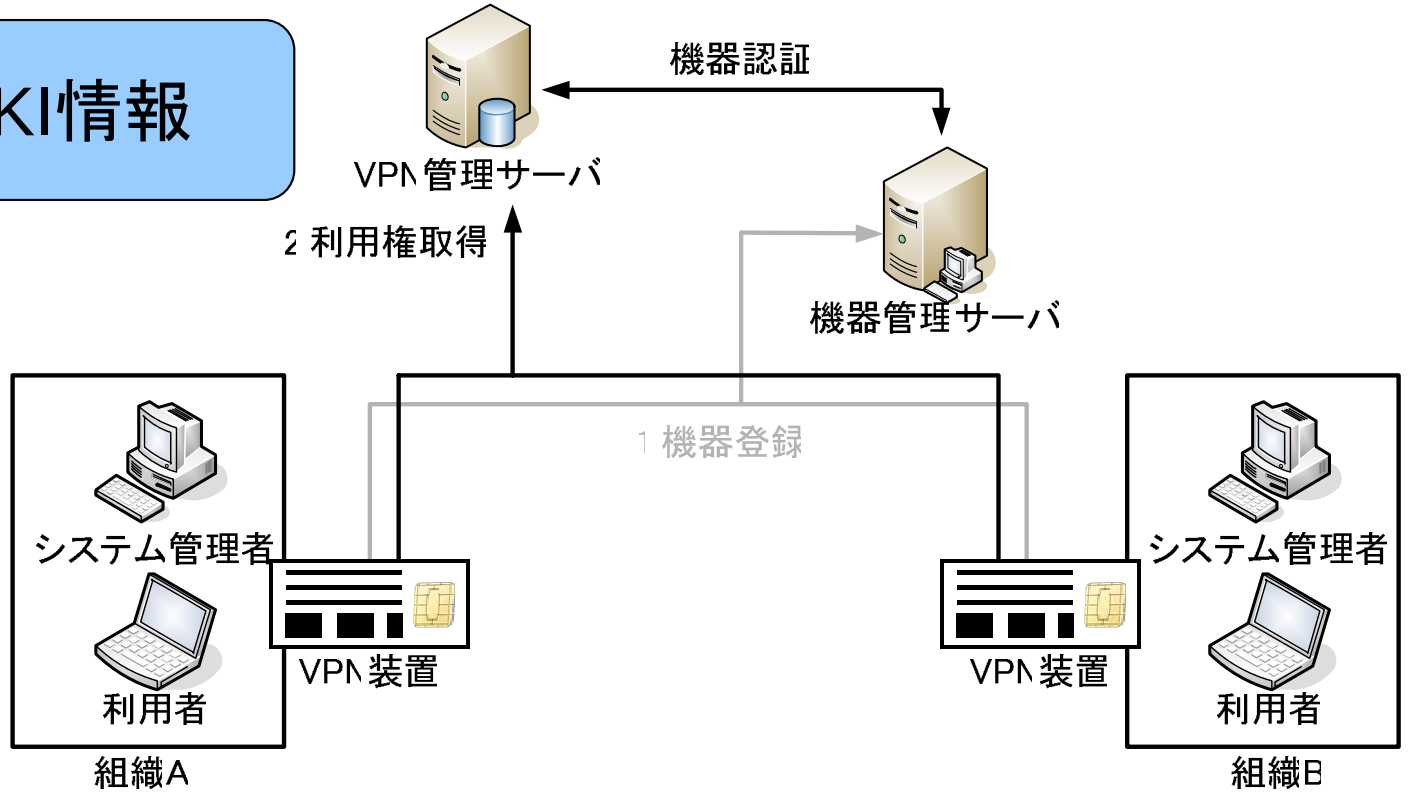
1階層目のPKI情報



2.利用権取得

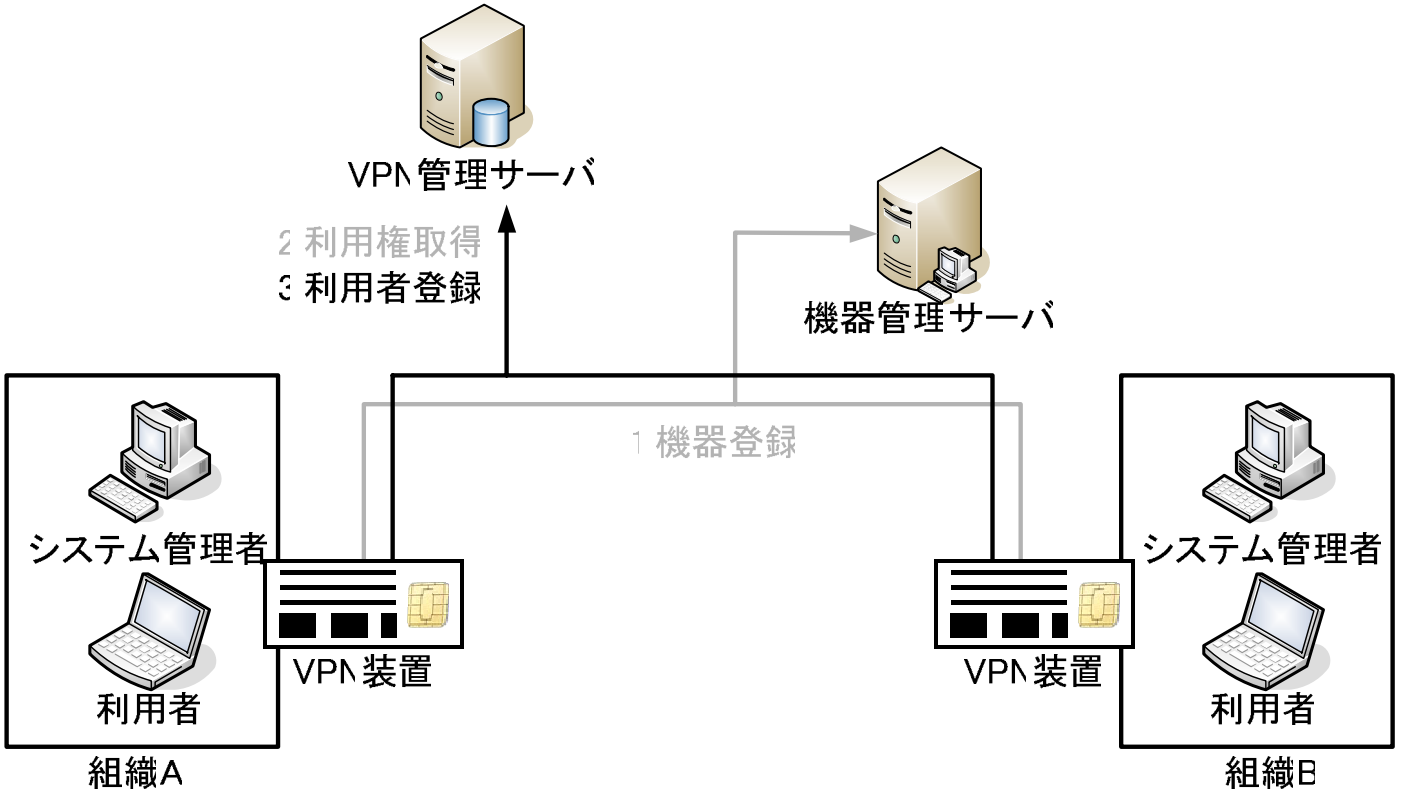
- システム管理者がVPNサービスの利用申請
- VPNサービス利用のためのチップアプリケーションをe-Keyチップにダウンロード

2階層目のPKI情報



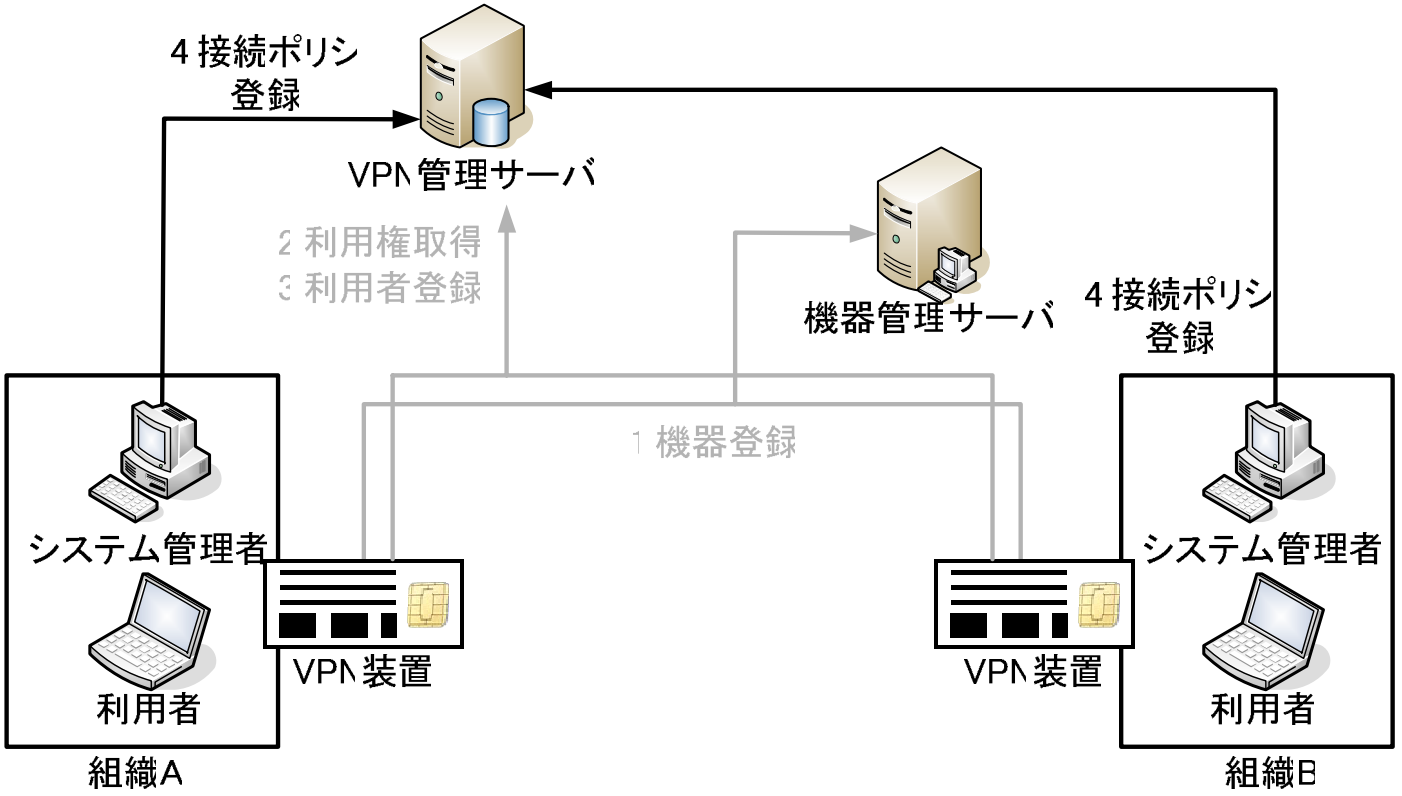
3.利用者登録

- VPN利用者情報をVPN管理サーバへ登録
- VPN管理サーバは1階層目のPKI情報を用いVPN装置を認証し，利用者ID，PWを登録



4.接続ポリシ登録

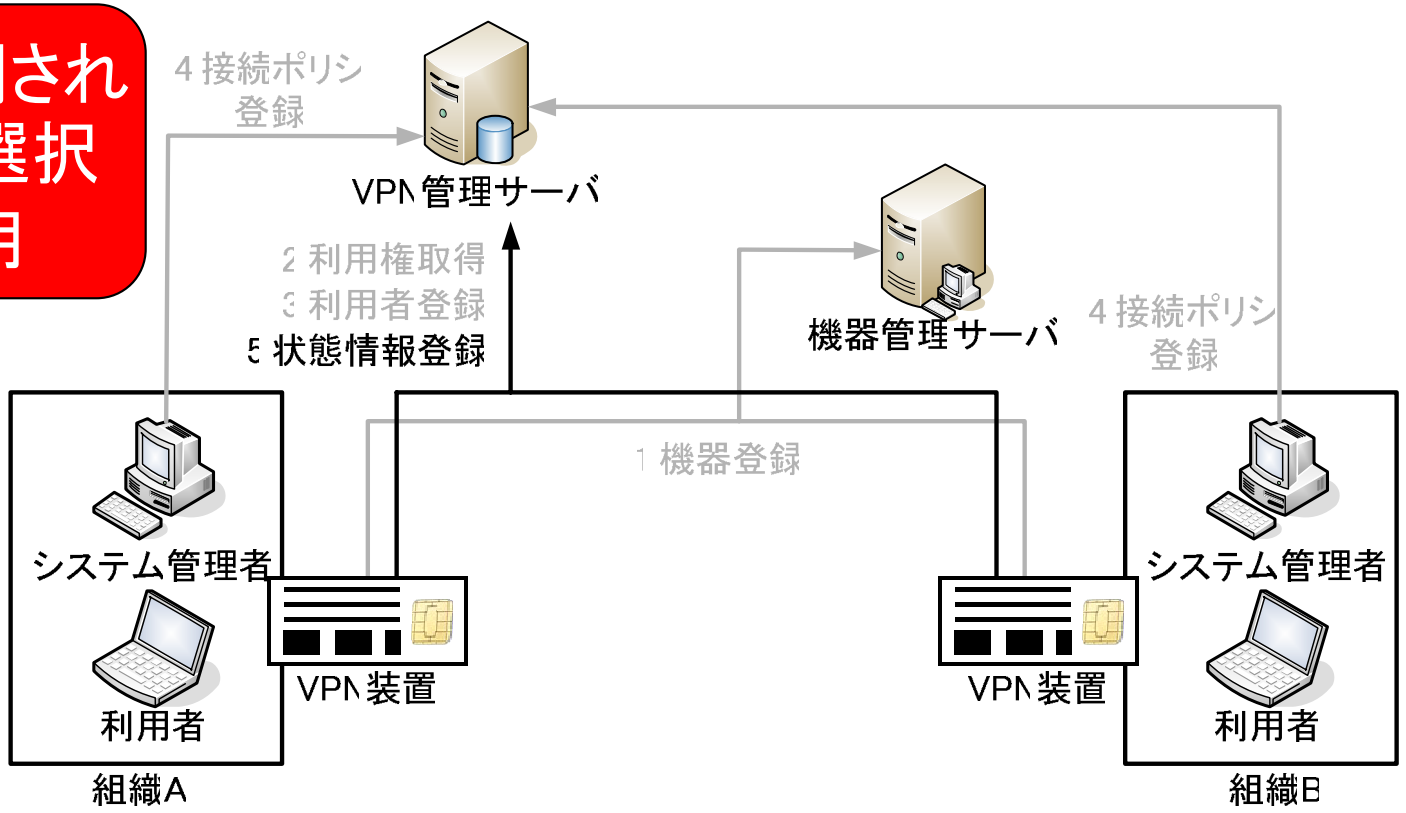
- VPN利用者がVPN接続を行うことを許可・禁止する相手先情報，自ネットワークへの接続を許可・禁止する相手先の情報を登録



5.状態情報登録

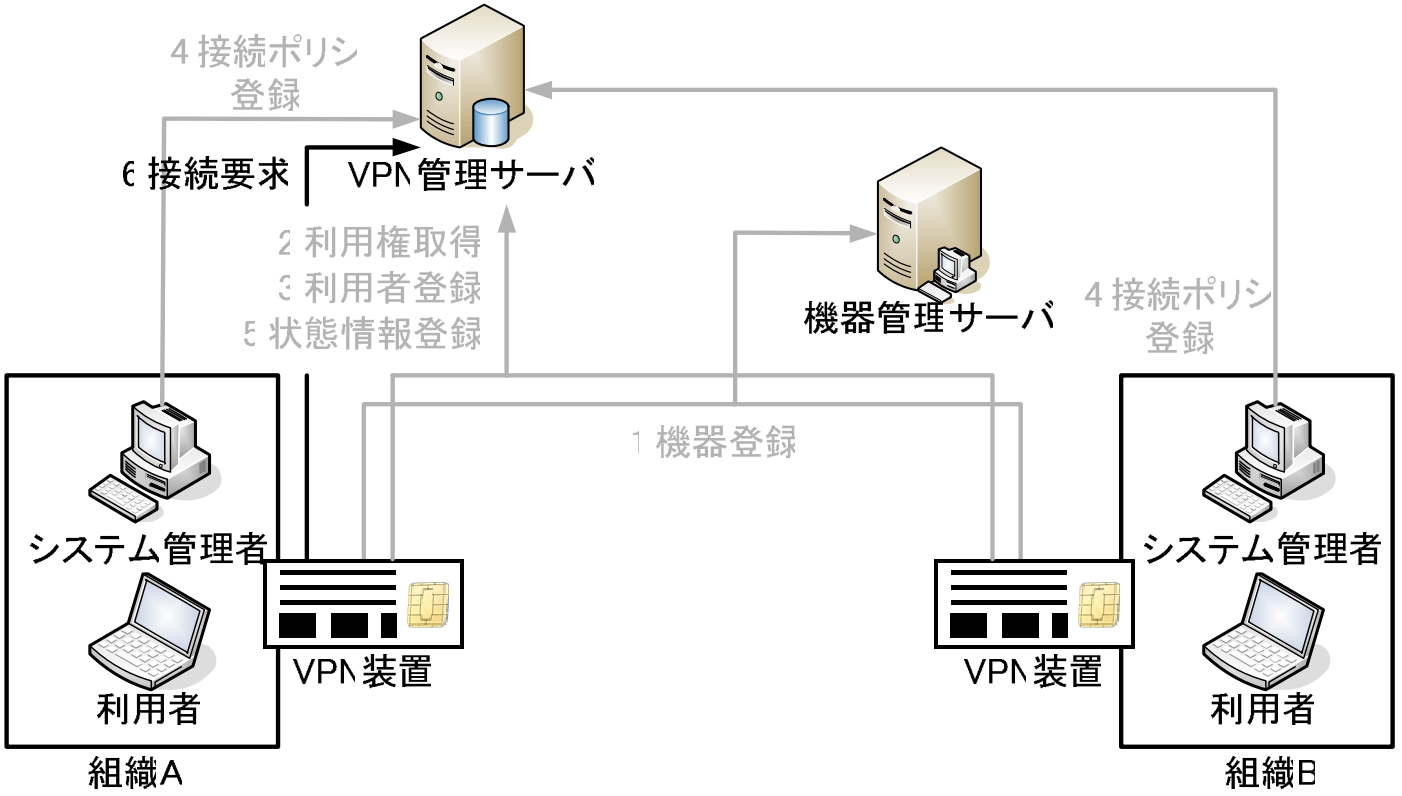
- VPN装置とその配下にいる端末のIPアドレスや端末種別等の状態情報をVPN管理サーバへ登録

登録情報は公開されVPN接続先を選択する際に利用



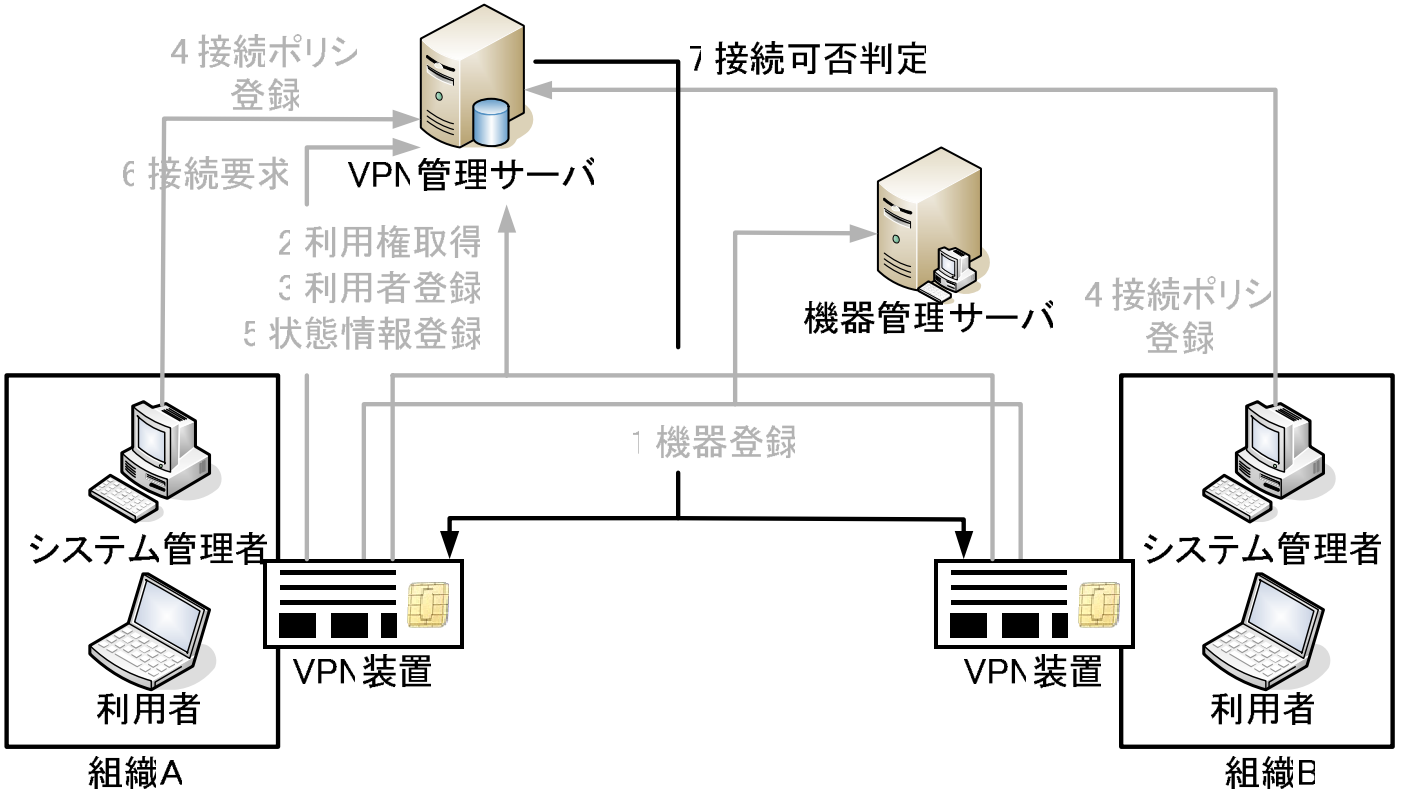
6.接続要求

- 利用者は接続したいVPN装置を選択
- VPN装置はVPN管理サーバへ接続し，2階層目のPKI情報による利用権認証を行う



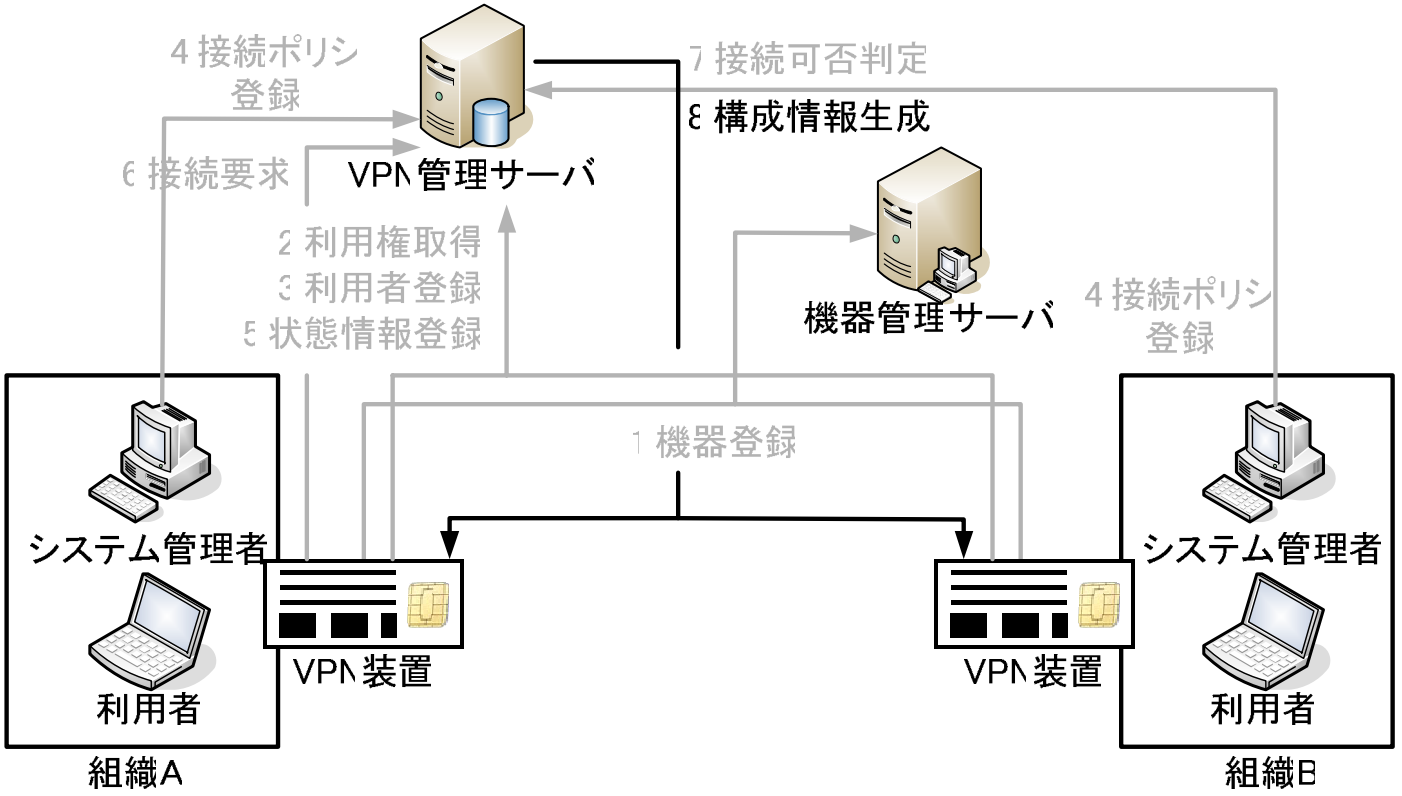
7.接続可否判定

- VPN管理サーバは，接続要求と接続ポリシを照合し，接続の可否を判定する



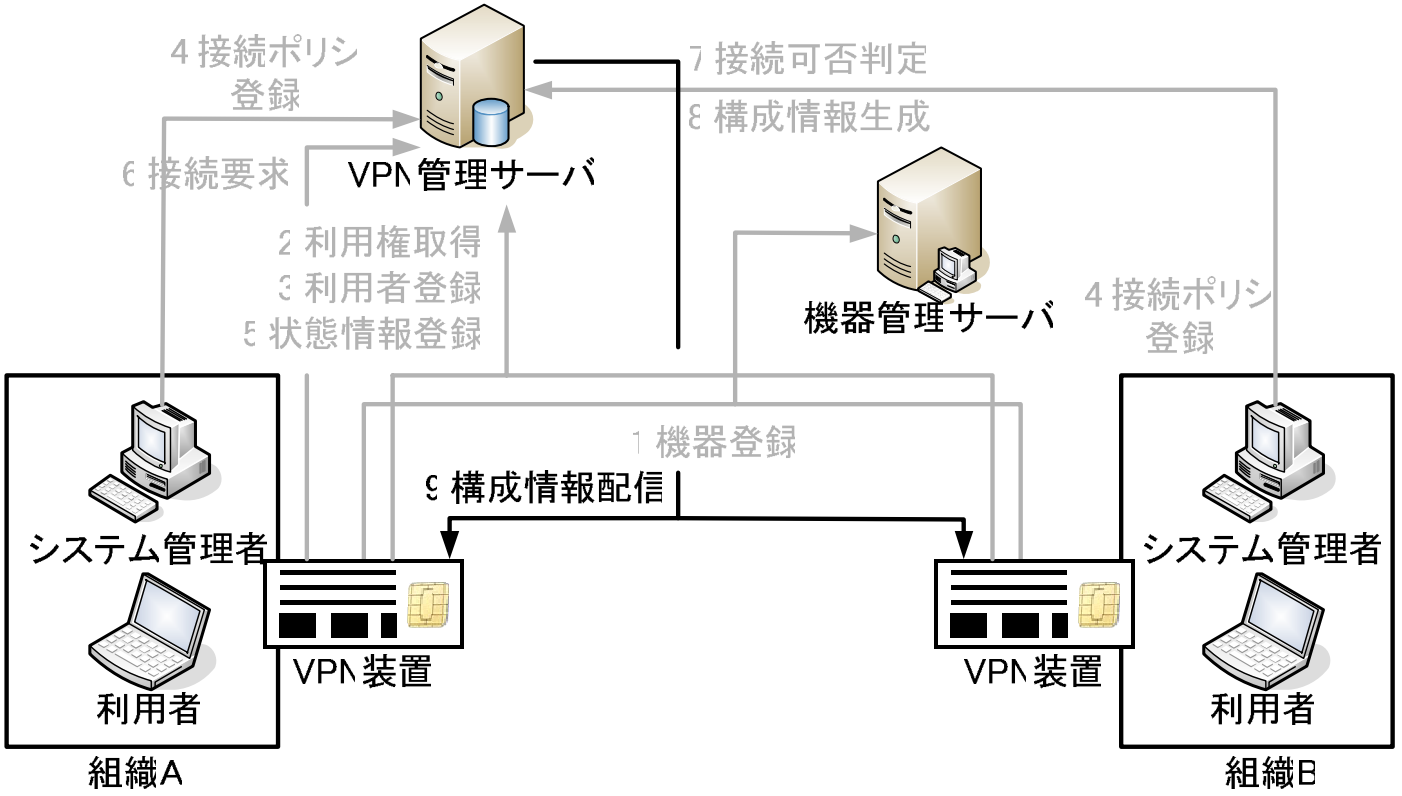
8.構成情報生成

- 状態情報と接続要求からVPN構成に必要となるIPsec構成情報とIKE用の事前共有秘密鍵を生成する



9.構成情報配信

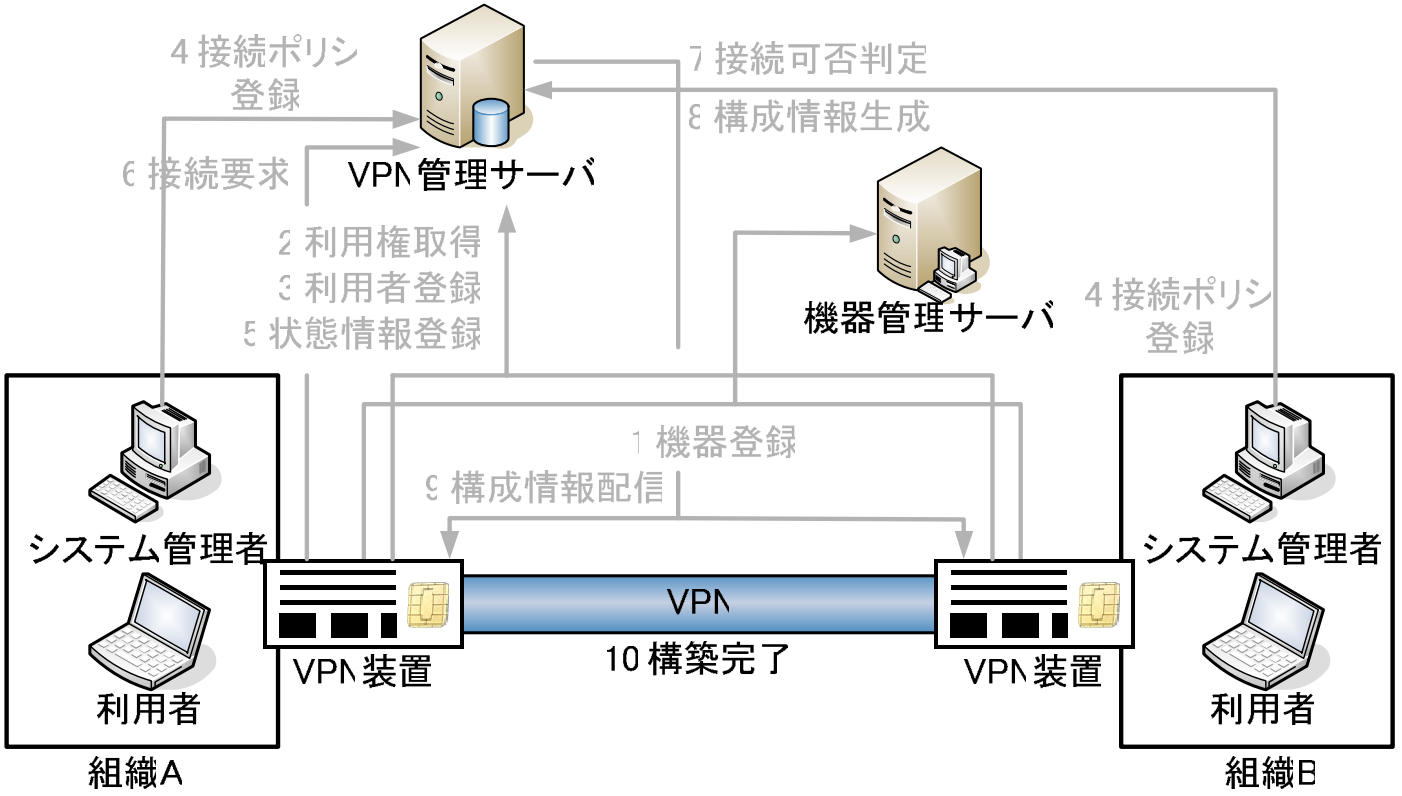
- VPN管理サーバから構成情報と事前共有秘密鍵を接続元，接続先のVPN装置に配信
- VPN装置に内蔵されているe-Keyチップに格納



10.構築完了

- 受信した構成情報と事前共有秘密鍵を用いてIKEを実行しVPNを構築

以降は通常のVPN通信が可能



オンデマンドVPNシステムの利点

- 2階層PKI技術
  - VPN装置の成りすましを解決
  - 設定情報の漏洩問題を改善
- IPsec構成情報生成技術
  - VPN接続先の情報がなくてもVPN構成情報を自動生成が可能
  - VPN装置に自動設定されるため設定の煩雑さがない
- ポリシ制御技術
  - 端末種別や属性情報，時間帯等でアクセス制御が可能

むすび

- オンデマンドVPNシステムは・・・
  - 2階層PKI技術をVPN装置に組み込み新たなVPN構築方法と認証技術
- 各端末にもICカードを導入し，リモートアクセス環境の構築やさらなるセキュリティ強化が期待できる

参考資料

- 著者：高橋　成文，東川　淳紀，山本　修一郎，小尾　高史，谷内田　益善，大山　永昭
- 論文名：2階層PKIを用いたオンデマンドVPNシステム
- 出展：情報処理学会論文誌　Vol.46　No.5
- 発表日：2005年5月

- 著者：鴨田　浩明，星川　知之，山岡　正輝，山本　修一郎
- 論文名：オンデマンドVPNシステムの実装と評価
- 出展：情報処理学会論文誌　Vol.47　No.8
- 発表日：2006年8月