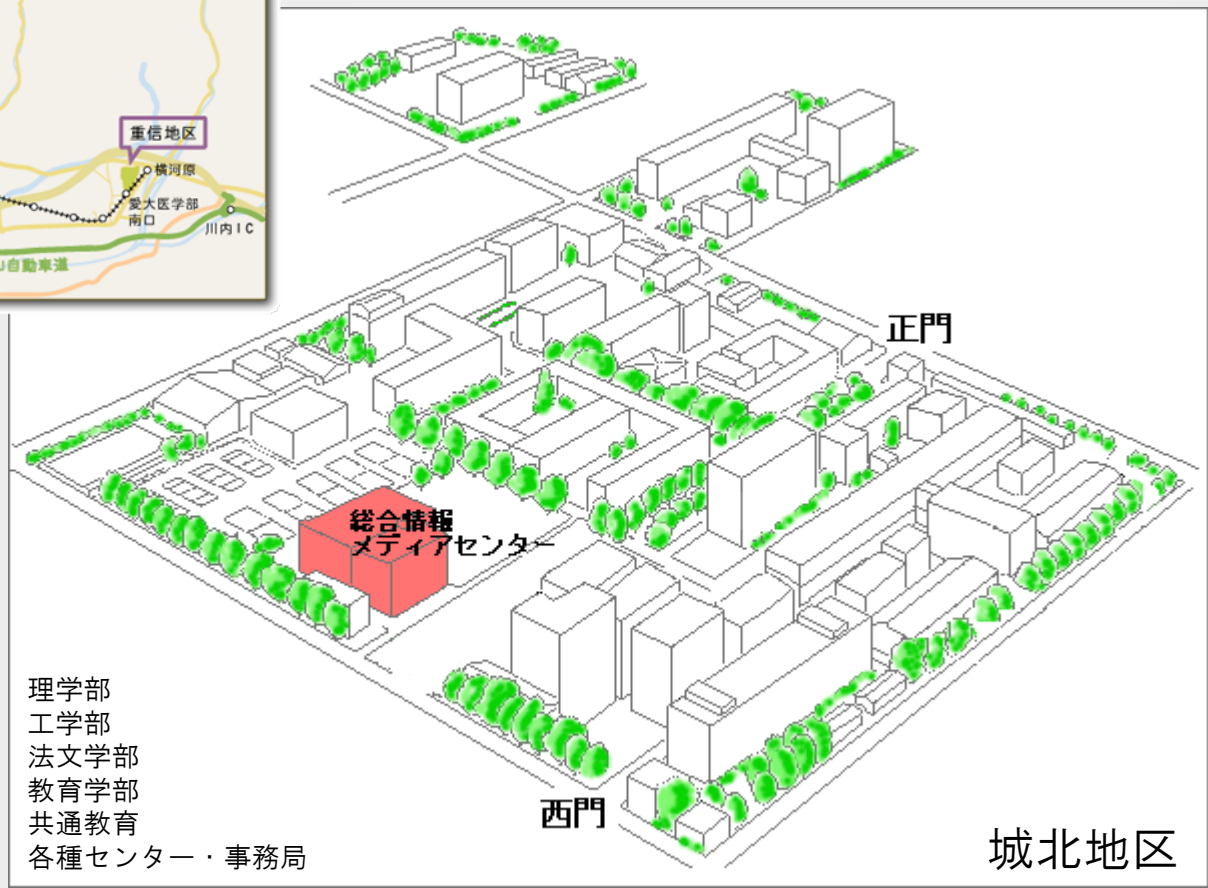
ネットワーク接続申請の簡略化

平成20年度情報処理軽井沢セミナー自由演習課題
於軽井沢国際高等セミナーハウス
2008年9月5日

愛媛大学　総合情報メディアセンター
宮内　譲嗣

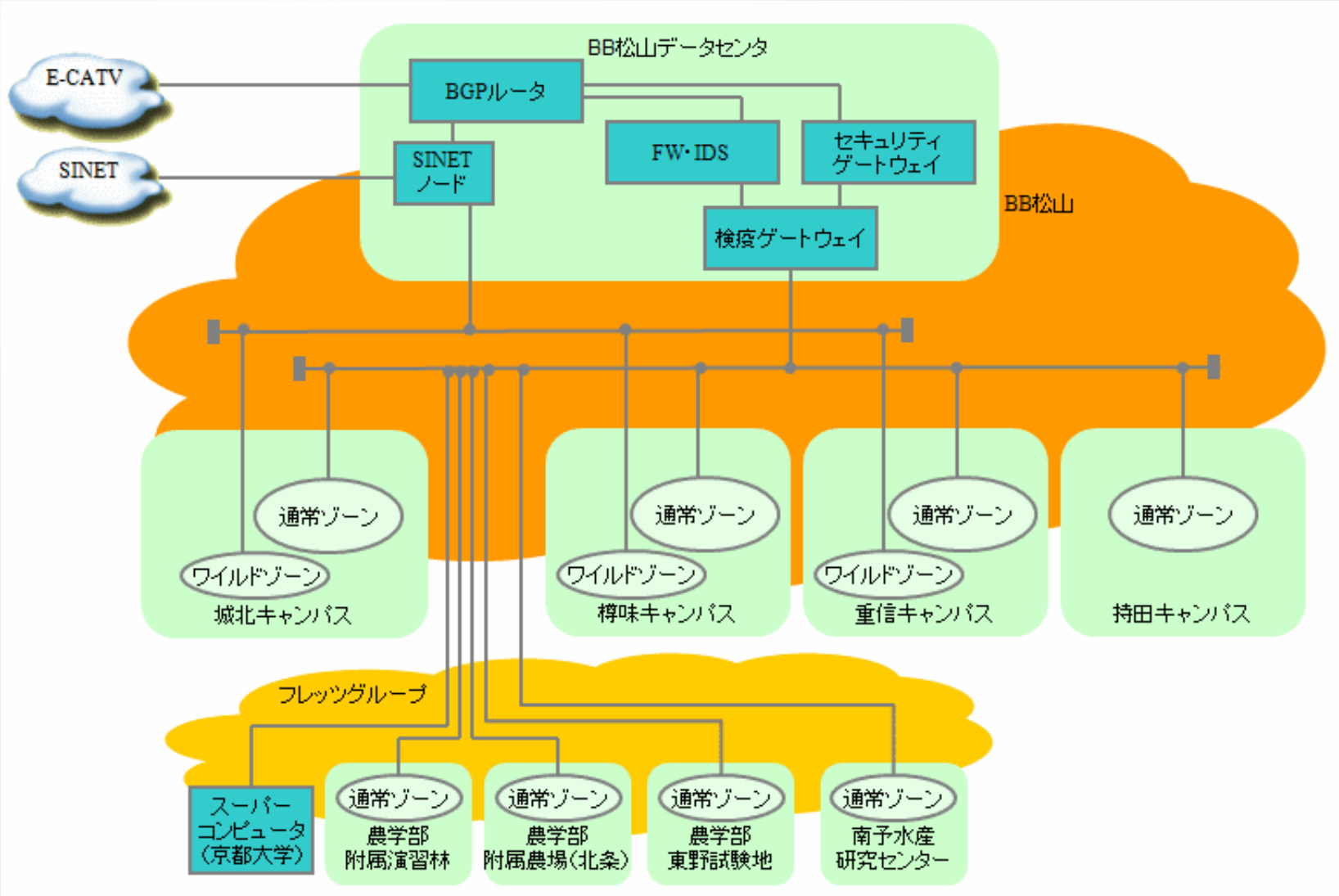
愛媛大学 -概略-

教職員数約1900名
学生約10000名

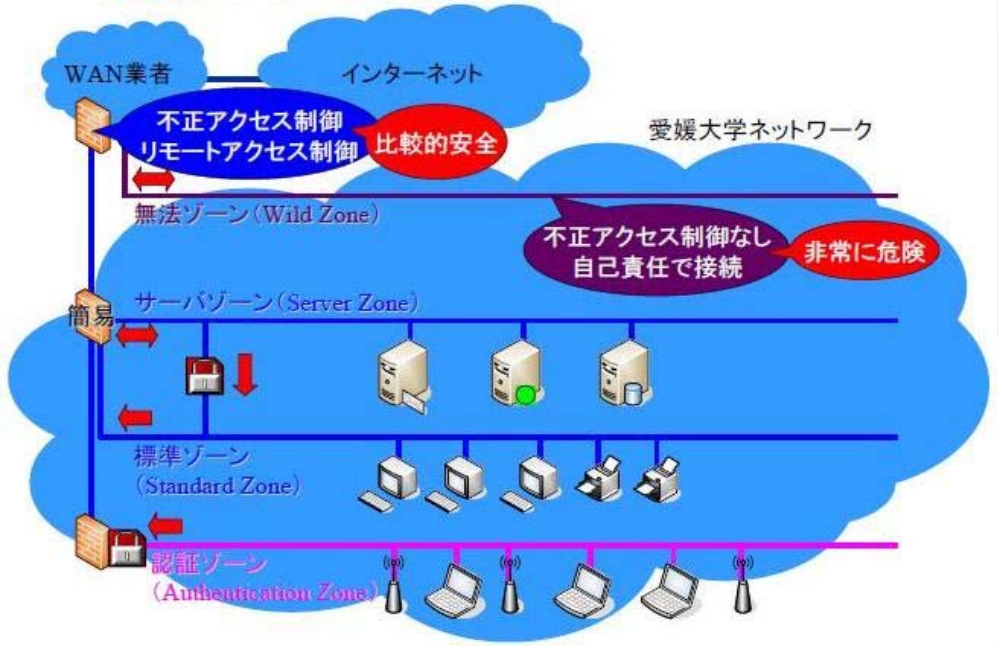


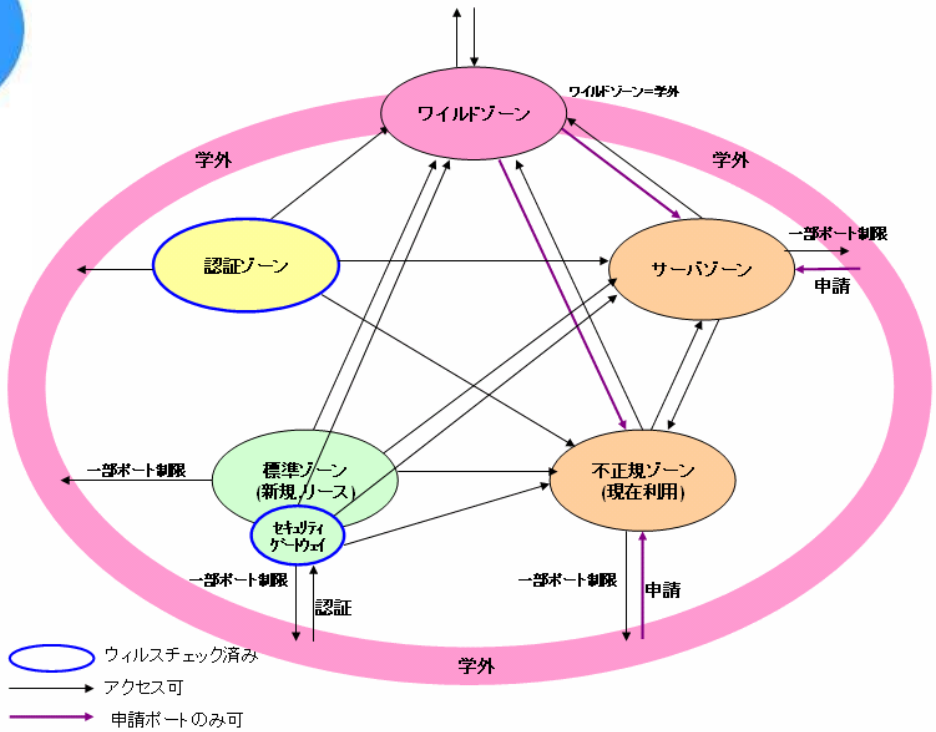
理学部
工学部
法文学部
教育学部
共通教育
各種センター・事務局

愛媛大学ネットワーク -概念図-



愛媛大学ネットワーク –ゾーンの概念–





ネットワーク利用の現状 –申請–

IPアドレス管理

- IPアドレスが重複せず、ユーザのネットワーク利用に支障をきたさない。

- 割当てたIPアドレスをもとに、インシデント発生時に、インシデントの渦中にある端末の所在を速やかに明らかにし、管理責任者へ連絡をとり、速やかな対策をとる

ネットワーク利用の現状 –申請–

- 申請書(紙)での申請

- 押印を要求
  ネットワーク接続だけでなく、ネットワーク利用についての責任の所在を明らかにするための書類。
  ↓
  「申請」という行為があればよいわけではない。

ネットワーク利用の現状 –申請–

- ネットワーク接続申請（≒IPアドレス利用申請）
  ネットワーク利用に必須

- IPアドレス使用数20000以上
  （クラスBのアドレス空間を管理）
  単一部署での管理は事実上無理

↓

建物や部局単位で、部局等ネットワーク管理者を設置し、建物や部局ごとアドレス管理を委任している。

ネットワーク利用の現状 -申請-

愛媛大学キャンパス情報ネットワーク利用内規

（IPアドレスの管理及び割当て）
第4 条基幹ネットワークを管理する者（ 以下「基幹ネットワーク管理者」という。）は，キャンパスネットワークのIPアドレスを管理し，部局等ネットワークを管理する者（ 以下「部局等ネットワーク管理者」という。）に割り当てる。
2 前項の規定によりIPアドレスの割当てを受けた部局等ネットワーク管理者は，部局等ネットワークに接続するコンピュータ，端末装置等の機器(以下「コンピュータ等」という。)にIPアドレスを割り当てる。
3 前二項の規定にかかわらず，基幹ネットワークに直接接続する機器については，基幹ネットワーク管理者がIPアドレスを割り当てる。
（ コンピュータ等の接続手続）
第5 条キャンパスネットワークにコンピュータ等を接続しようとする者は，接続しようとする部局等ネットワーク管理者にネットワーク接続申請書等を提出し，許可を受けなければならない。
2 部局等ネットワーク管理者は，部局等ネットワークの運用等に支障がないと認めたときは，前項の申請を行った者にネットワーク接続許可証等を交付する。
3 キャンパスネットワークにコンピュータ等の接続を許可された者(以下「ネットワーク利用責任者」という。）は，コンピュータ等の変更又は利用を取り止めるときは，部局等ネットワーク管理者に届け出なければならない。

ネットワーク利用の現状 -申請-

メディアセンター推奨の申請様式

ネットワーク接続申請書

（部局等ネットワーク管理者）殿

愛媛大学キャンパス情報ネットワーク利用内規第５条第１項の規定に基づき、下記のとおりコンピュータ等の接続を申請します。なお、愛媛大学キャンパス情報ネットワークの利用に当たっては、愛媛大学セキュリティポリシー，ガイドライン及び愛媛大学キャンパス情報ネットワーク利用内規を遵守します。

申請年月日	平成　　年　　月　　日	
申請区分	１．新規　２．変更*1　３．取消 (2, 3の場合は現在のIPアドレスを記入：133.71.　　)	
申請者の所属，氏名，連絡先電話及びメールアドレス	所属 氏名 印	
	e-mail	（内線）
	職員証番号	
主たる利用者（※大学院生，学生等申請者以外の場合は記入）	所属 氏名 印	
	e-mail	（内線）
コンピュータ等の種別	□学外公開サーバ*2　□学内公開サーバ □パソコン　□ネットワーク機器 □プリンタ　□その他（　　） □教育研究用システム　□事務用システム ※上記のシステムは構成図等を添付すること。	
コンピュータ名		
設置場所	館・棟　階　室（部屋番号）	
利用方法等		

*1）ＩＰアドレスを変更する場合は、各部局等ネットワーク管理者に「取消」申請と「新規」申請を提出してください。
*2）学外にサーバ等を公開する場合は，学外公開申請書を総合情報メディアセンターに提出すること。

ネットワーク接続許可証

平成　年　月　日

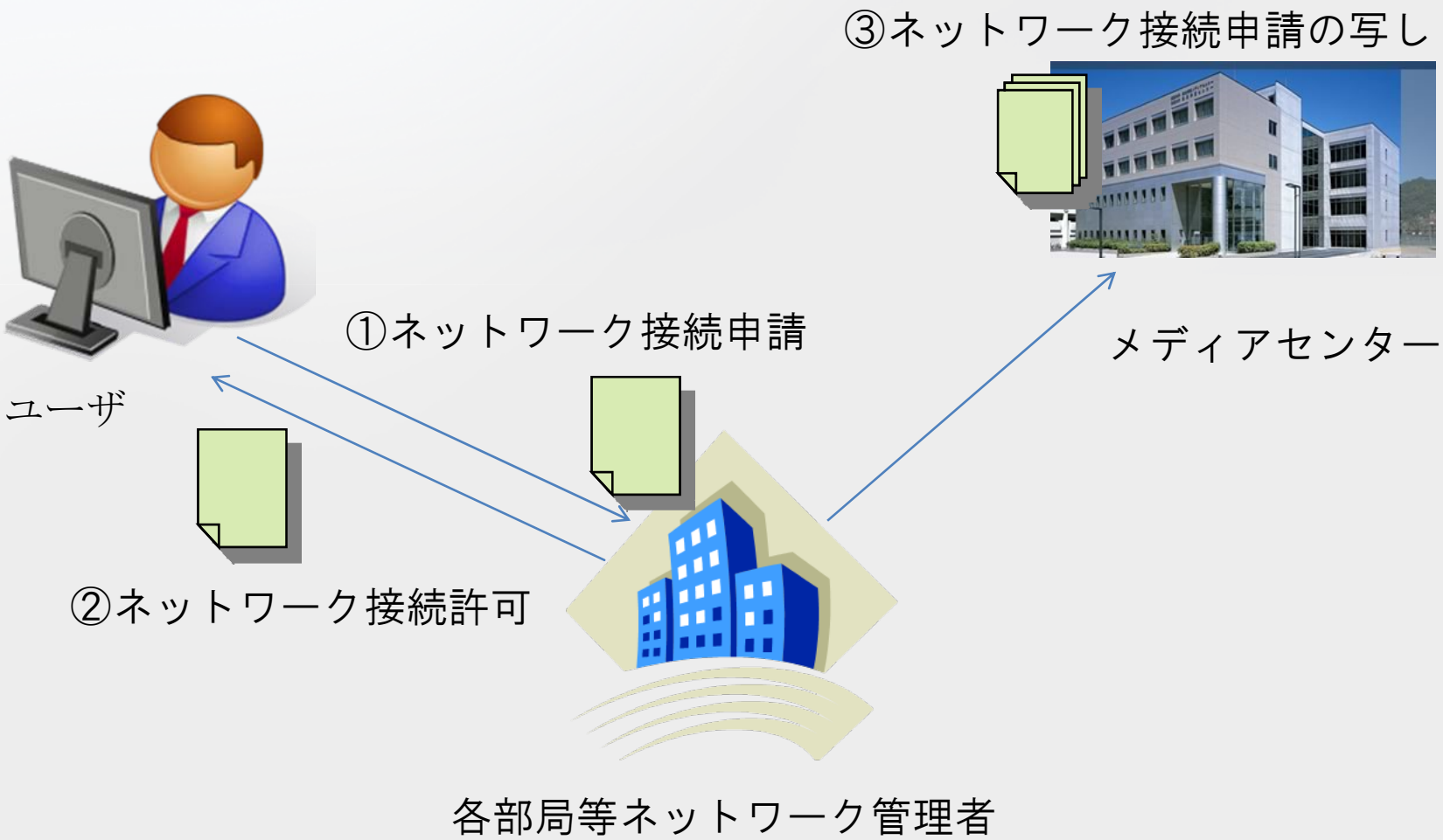
（申請者）殿

（部局等ネットワーク管理者）　印

上記申請を許可します。
なお、ＩＰアドレスについては、次のとおりです。

ＩＰアドレス	１３３．７１．

ネットワーク利用の現状 -申請-



ネットワーク利用の現状 -問題点-

- メディアセンターは申請書の写しをもらい、IPアドレスの割当て状況を把握することになる。IPアドレスの利用開始から、メディアセンターが把握するまでに、タイムラグがある。
- 申請方法は、メディアセンター推奨の様式はあるものの、部局独自様式で申請しているところもあり、利用状況があいまいな部分がある。

IPアドレスは
メディアセンターで一元管理したい！

IP一元管理にむけて　-予想される問題点-

1. 日常的・散発的に発生する申請に対応するだけの人的リソースが不足。

2. 実際の人を知らないため、申請書上の名前の記述と印章とを見て判断するしかない。本人性確認ができない。

3. 建物ごとに、施設の状況（セグメントの利用状況）が異なり、IPアドレスの適切な割当ができない。

IP一元管理にむけて　-解決策-

1. リソースが不足。
2. 本人性確認ができない。

↓

PKIを利用し本人確認をした上でWEB申請

3. IPアドレスの適切な割当ができない。

↓

DHCPサーバによるIPアドレス割当

IP一元管理にむけて　-・・・疑問-

本当にDHCPサーバによるIPアドレス割当をすれば

IPアドレスの適切な割当ができるだろうか・・・？

DHCPサーバでのIP管理 -問題点-

- DHCPサーバは、ネットワークに接続要求のあったクライアントを識別・認証しない。

  ↓

  アクセス権を持たない者（クライアント）から要求があった場合でも、ネットワークへの接続を許可してしまう可能性がある。
  インシデント発生時に責任者の特定ができない。

- MACアドレスをDHCPサーバに登録する方式

  ↓

  ユーザが利用できるクライアントが限定されるため、ユーザの利便性が悪くなってしまう。

- 認証スイッチを利用

  ↓

  全学への導入はコスト面で問題

DHCPサーバでのIP管理 -解決策-

ネットワーク接続申請と端末認証を

同時にできないだろうか？

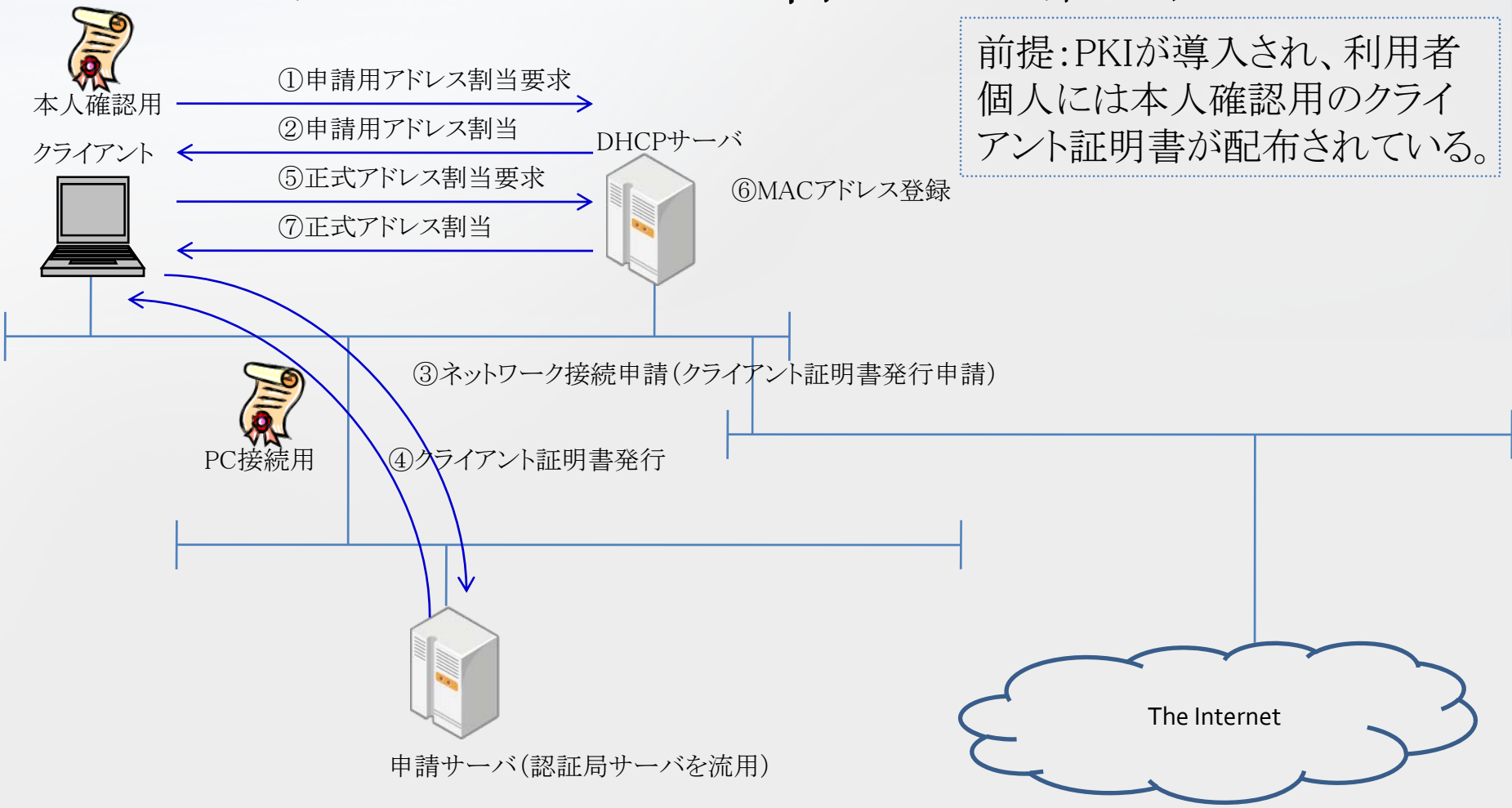
DHCPサーバでのIP管理 -解決策-

事前に本人確認用クライアント証明書を配布

本人確認用クライアント証明書をもとにPC接続用クライアント証明書を発行

DHCPサーバでのIP管理 -解決策-

前提：PKIが導入され、利用者個人には本人確認用のクライアント証明書が配布されている。



DHCPサーバでのIP管理 –メリット–

ユーザー

申請手続きが簡略化され、PCを接続したらすぐにネットワーク利用が可能になる。

メディアセンター

IPアドレスにとらわれず利用者管理がリアルタイムにでき、インシデントに即応できる。

ネットワーク接続申請の簡略化 –まとめ–

PKI認証局の構築・運用が何よりも必要

DHCPサーバへの認証機能の実装

ネットワーク接続申請の簡略化 –課題–

PKI認証局の構築・運用

DHCPサーバの認証機能について調査を要する

本人確認用のクライアント証明書の配布方法

プリンタ等のPC以外の機器の登録方法

そもそも本人確認用のクライアント証明書を利用して申請サーバにアクセスしたことが本人性確認になるのか

参考

発明名称：DHCP運用システム、DHCP運用方法および DHCPサーバ

【出願番号】特願２００５－３０３４９６（Ｐ２００５－３０３４９６）

http://www.j-tokkyo.com/2007/H04L/JP2007-116281.shtml