厚生労働省「シームレスな健康情報活用基盤実証事業」

認証認可システム

システム仕様書

改定欄
CHANGE

副番 REV	ページ PAGE 項目 ITEM	内　　容 C O N T E N T S	作成 DRAWN 日付 DATE ・　・	照査 CHECKED	検認 APPROVED

目　　次

1. 目的

能登北部「シームレスな健康情報活用基盤実証事業」で展開されるシステムの認証基盤の構築を行なう。

2. 関係者（ステークホルダー）

主なステークホルダーについては、「シームレスな健康情報活用基盤実証事業　システム仕様書」と同様とする。

3. 用語の定義

主な用語の定義については以下のとおり

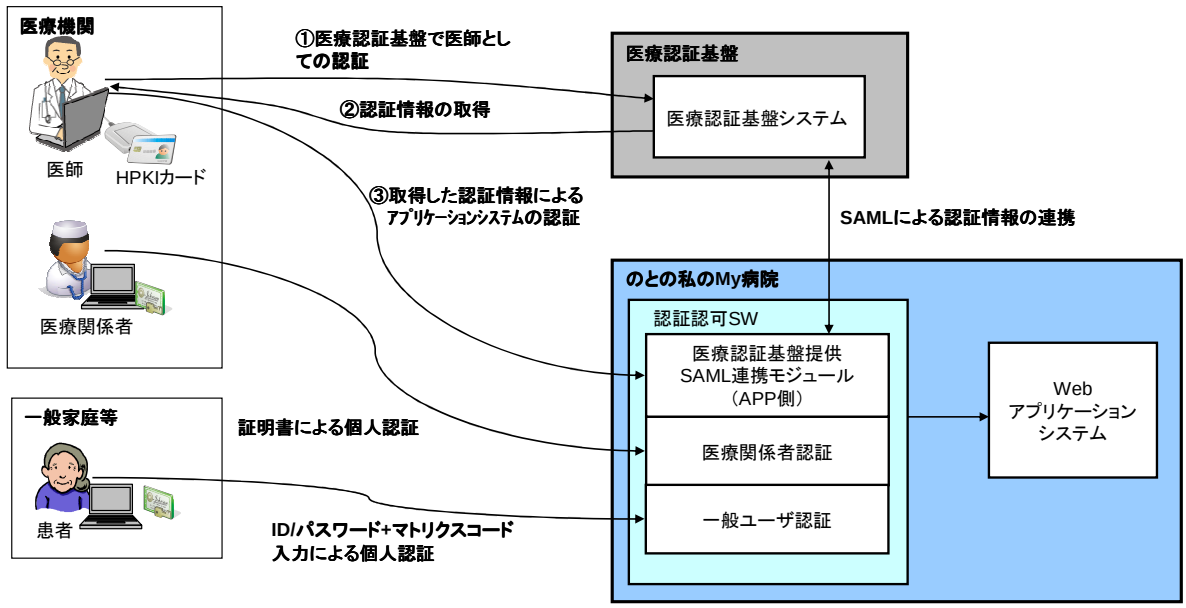
用語の定義

名称	説明
医療認証基盤	医療認証基盤整備において、HPKI カードによる個人認証を行なうためのシステム。医師向けの認証を医療認証基盤にて行なう。
OpenAM	Web シングルサインオンのオープンソースソフトウェア。OpenSSO の後継であり今回の認証基盤システムのベースのソフトウェアとなる。
認証 LDAP	LDAP は Lightweight Directory Access Protocol の略。OpenAM が使用する認証・認可情報などが格納される。
SAML	Security Assertion Markup Language の略。ドメインの異なるサービス間で認証を連携する方式。OASIS で標準化されている。SAML1.0、1.1、2.0 がある。 医療認証基盤との接続にて SAML を使用する。
HPKI	ISO17090(Health Informatics - Publibc Key Infrastructure で定義された保健医療福祉分野の医療従事者の資格をいれることのできる電子証明書
hcRole	healthcare role：医療従事者の資格

4. システムの概要

能登北部「シームレスな健康情報活用基盤実証事業」を利用するユーザの個人認証を行い、その認証情報を Web アプリケーションシステムに提供する。医師の認証に関しては日医認証局が発行した HPKI カードを利用し、医療認証基盤にて認証した情報を取得する。医療認証基盤で認証するために、医療認証基盤より提供された SAML 連携モジュールを組み込む必要がある。また、医師以外の利用者に関しては、別途証明書を発行し証明書による個人認証を行なう。また、患者は証明書認証ではなく、IDパスワードでも認証できる機能をもたせる。

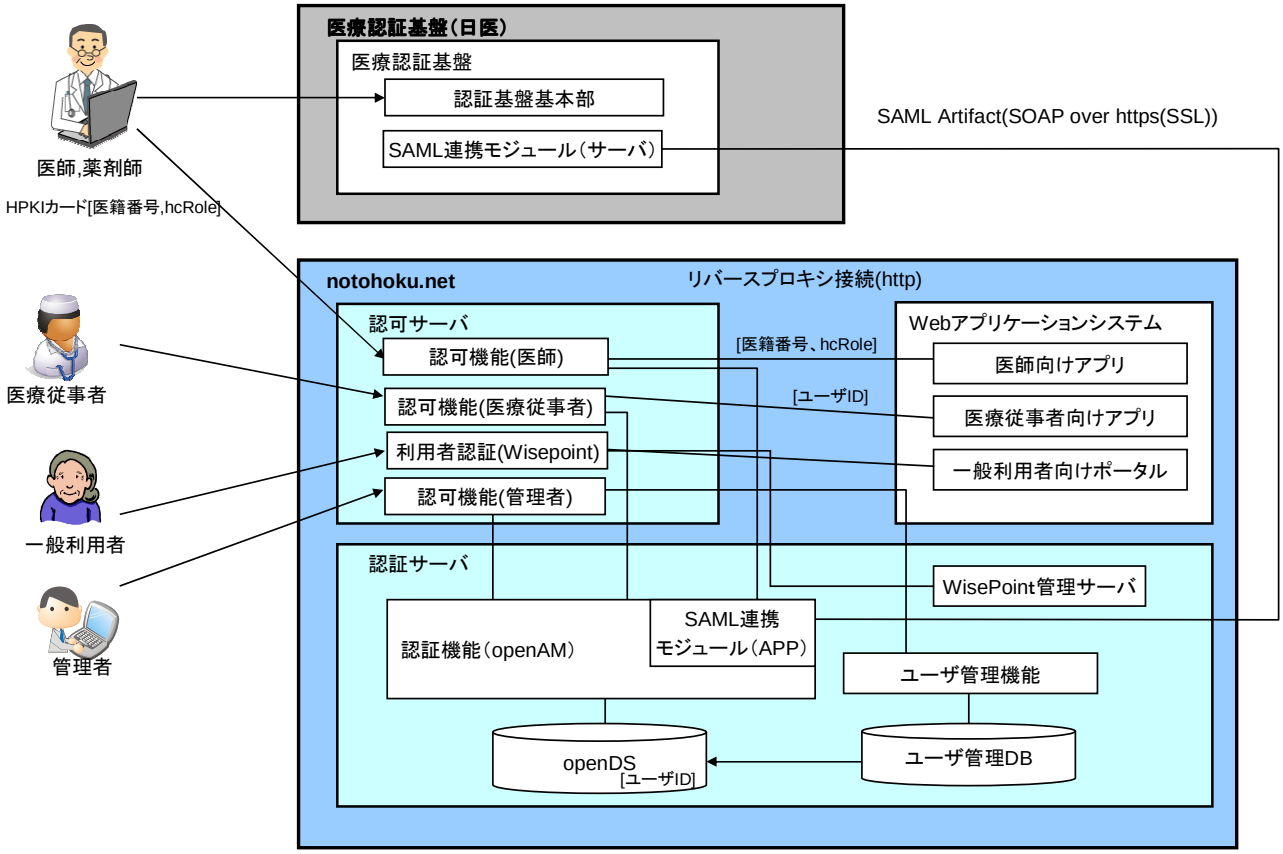
全体システム概要



5. システム構造

5.1　業務サブシステム構成図

システムを構成するサブシステムと、サブシステムの機能を業務サブシステム構成は以下のとおり



5.2 各処理機能およびインターフェース

5.2.1 認可機能

認可機能は利用者のネットワークから直接 http(https)リクエストを受け付け、認証されたユーザであるか確認して利用可能ユーザに対するサービスの提供を行なう。各役割の認証方法と、接続する Web アプリケーションは以下のとおり。

	認証先	認証方法	接続先アプリ
医師、薬剤師	https://hpki.notohoku.net /	医療認証基盤との SAML 連携	地域向けポータル 処方 ASP 画像サーバ ID 管理
医療従事者	https://pki.notohoku.net/	PKI	地域向けポータル 処方 ASP 画像サーバ ID 管理
利用者	https://idpwd.notohoku.net/	ID パスワード認証（マトリクス表を利用したワンタイムパスワード方式）	どこでも MY 病院
認証認可 SW 管理者	https://manage.notohoku.net/	PKI	認証認可 SW ユーザ管理機能

各 Web アプリケーションに提供する認証情報は、認証先の URL に応じて変更される。認証情報は HTTP ヘッダーまたは、Form データとして提供される。ヘッダー名または、Form データ項目名とその内容は以下のとおり

認証先	提供ヘッダー名	提供 Form データ項目	提供情報内容
https://hpki.notohoku.net	SSO_USER	-	医籍番号
	SSO_HCROLE	-	証明書に記載されている hcRole の項目 医師の場合「Medical Doctor」が入る 薬剤師の場合「Pharmacist」
	SSO_DEPT	-	組織情報（認証認可ユーザ情報ファイル 2.組織 ID の項目）
https://pki.notohoku.net	SSO_USER	-	ユーザ ID（認証認可ユーザ情報ファイル 8.証明書識別子の項目）
	SSO_HCROLE	-	証明書に記載されている hcRole の項目 （現在 hcRole が入る対象ユーザはない）
	SSO_DEPT	-	組織情報（認証認可ユーザ情報ファイル 2.組織 ID の項目）
	SSO_AUTH_TYPE	-	認証方式「PKI」が入る
https://idpwd.notohoku.net	-	userid	ユーザ ID（WisePoint ユーザデータ 1 ユーザ ID の項目）
		SSO_AUTH_TYPE	認証方式「PKI」が入る
https://mymanage.notohoku.net	SSO_USER SSO_DEPT SSO_GROUPS	-	認証認可 SW のユーザ管理機能用の情報

本システムでは運用業務の効率化を図るため､認証された全てのユーザに対して Web アプリケーションシステムへのアクセスを許可する。そのため、Web アプリケーションシステムでは、別途本機能から送信されるユーザ情報を Header より取得し、各機能にてアクセスを制御する機能の実装が必要となる。

認可機能では Web サービスとして SSL クライアント認証を実施する。SSL クライアント認証に関しては以下のものを使用する

SSL Version	SSL 3.0 または TLS1.0(SSL3.1)
暗号	AES(128bit/256bit)、Camellia(128bit/256bit) 3DES(168bit)
MAC	SHA-1

認可機能(利用者)および認可機能（管理者）では SSL クライアント認証要求として Japannet 発行の証明書または日本薬剤師会の証明書を要求する。認可機能（医師向け）では SSL クライアント認証要求は行なわず、SAML による医療認証基盤への認証要求を行う。

5.2.2 認証サーバ

認可機能に対して認証情報がないユーザがアクセスした場合、ユーザの認証を行なう機能をもつ。認証情報は認可機能（利用者）および認可機能（管理者）で SSL クライアント認証を実施したクライアント証明書を取得し、そこから認証に必要な情報を抜き取り LDAP に対してユーザが登録されているかを確認する。ユーザが登録されていない場合や証明書が失効されている等の場合には認証機能にてエラー画面を提供する。

登録されるユーザの種類と、その証明書情報は以下のとおり。

医師、薬剤師

issuer の DN	CN = HPKI-01-HPKI_J-forAuthentication-forIndividual OU = Regulated Healthcare Professional Union CA O = Japan Medical Association C = JP
ユーザ ID（個人の識別）	SubjectDN の SERIALNUMBER =で記載されている識別番号 ※薬剤師は識別番号に-jpa が付く

医療従事者

issuer の DN	CN = HPKI-01-MED-forAuthentication-forIndividual OU = Regulated Healthcare Professional Union CA O = Japan Medical Association C = JP
ユーザ ID（個人の識別）	SubjectDN の SERIALNUMBER =で記載されている識別番号 ※今回のユーザをあらわすために識別子を追加

※3 月までに登録した利用者や認証認可のユーザ管理者等は以下の証明書を使用する

issuer の DN	CN = Enterprise Premium CA O = Enterprise Premium Service C = JP
ユーザ ID（個人の識別）	SubjectDN の CN =で記載されている識別番号

5.2.3 SAML 連携機能（APP）

SAML 連携機能（APP）は医療認証基盤から提供される医師資格確認のためのモジュールである。このモジュールを組み込むことで、医師の個人認証および資格情報（hcRole）を取得する事が可能。そのため、SAML 連携モジュールを組み込み、医師の個人認証を医療認証基盤にて実施する。医療認証基盤で認証された情報として取得する医籍番号と hcRole をそのまま Web アプリケーションに提供する。
また、薬剤師も医療認証基盤での認証を実施する。

5.2.4 ユーザ管理機能

利用者(HPKI、PKI ユーザ)の登録・削除等の実施を行なう運用管理者用の機能。既存製品の機能をそのまま利用する。

5.2.5 マトリクス表を利用したワンタイムパスワード方式

一般利用者は、ID パスワードを使った認証を行うが、セキュリティ強化のため媒体に記載されるマトリクス表に従った追加コードを入力することで認証する機能を提供する。
マトリクス表を利用したワンタイムパスワード方式に関しては FalconSC 社製品「WisePoint」を利用する。

6. システム機能仕様

6.1 新業務フロー

6.1.1 ユーザ登録

認証認可 SW にユーザの登録作業が必要となる。医師の認証は医療認証基盤で実施されるが、認証認可 SW で利用者登録の確認を行なう必要があるため、医師自体のユーザ登録も必要となる。

ユーザの登録に関しては、ID 管理システムから CSV で出力されるものとする。

医師、薬剤師、医療関係者はその CSV ファイルを認証認可 SW のユーザ登録画面ににて登録する。

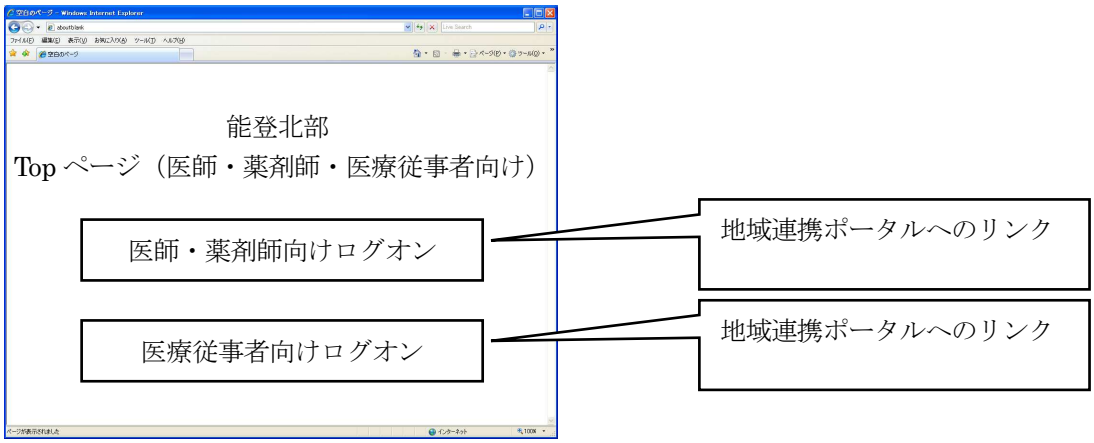
利用者（マトリクス表を利用したワンタイムパスワード方式を行うユーザ）は WisePoint の機能でユーザ登録を行う。また、登録したユーザは WisePoint の管理機能より認証文字情報を出力し、そのファイルを運用側に提供する。

7. ユーザインターフェース仕様

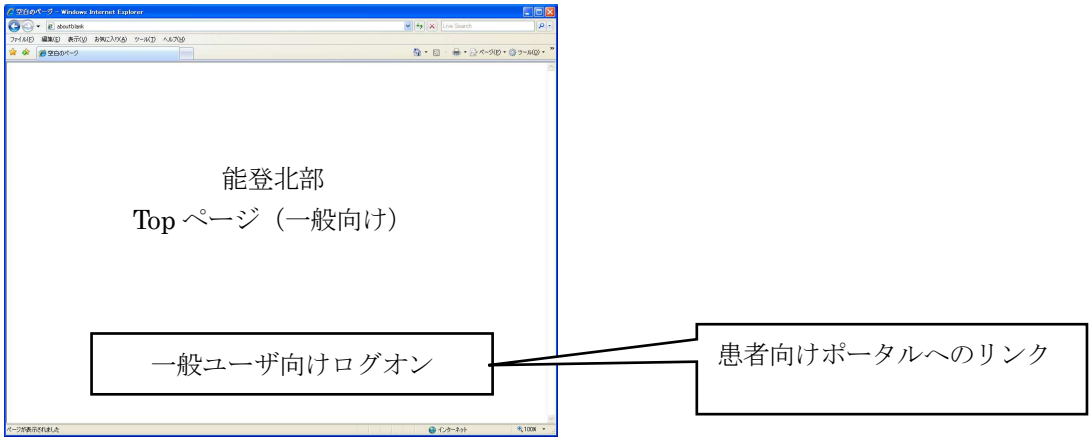
7.1 画面

認証認可 SW ではログオン前にシステム向けの TOP 画面を準備する。

地域ポータル向け Top 画面　http://hpki.notohoku.net/



どこでも MY 病院向け Top 画面 http://idpwd.notohoku.net/



システム管理者、運営管理者、認証認可 SW 管理者は Top 画面を用意しないため、直接アプリケーションの URL にアクセスする必要がある。

ログオン後は、各ユーザのポータルページに推移する。ポータルページは Web アプリケーション側にて準備する。

8. データファイル仕様

データファイルについて下記事項を記述する。

(1) 認証認可 SW データファイル一覧

ファイル名	認証認可ユーザ(医者、薬剤師、医療従事者)情報ファイル(CSV 形式)							
ファイル説明	認証基盤システムを利用するユーザ(医師)情報を一括で登録する。							
No.	項目名	タイプ	桁数	区分別必須				項目説明
				1	2	3	4	
1	区分	テキスト	2	○	○	○	○	ファイル登録区分 1:新規 2:ユーザ情報変更 3:ユーザ削除 4:組織削除(4 の組織削除は実施せず)
2	組織 ID	テキスト	20	○	○		○	ユーザが所属する組織。以下を指定。 医師:「Doctor」 薬剤師「Pharmacist」 看護師、ソーシャルワーカ等「Staff」 利用者「notohoku」
3	認証サービス ID	テキスト	41	○	○	○	○	SubjectDN の SERIALNUMBER=で記載されている識別番号 医師は番号のみ 薬剤師は番号＋-jpa 医療従事者は Notohoku+番号
4	氏名	テキスト	128 文字	○	○			PKI 認証ユーザ:氏名を指定 IDパスワード認証ユーザ:IDを指定(この項目をWebサービスに提供するため)
5	認証方式	テキスト	8	○				PKI
6	パスワード	テキスト	128 文字	△				不要
7	isuuer 区分	テキスト	2	△				電子証明書発行者情報 医師、薬剤師:3(日医認証用CA) 医療従事者:7(日医独自 CA) ※旧ユーザ(JN 証明書を利用しているユーザ)は以下で登録されている:6(Japannet Enterprise Premium CA)
8	証明書識別子	テキスト	4000 文字	△				証明書の中で個人を識別するための情報(IDパスワードユーザは不要) SubjectDN の SERIALNUMBER=で記載されている識別番号 認証サービス ID と同じ値 ※:6(Japannet Enterprise Premium CA)は SubjectDN の CN =で記載されている識別番号

※ 1 行目は説明用のため、処理はされない

※ 組織 ID はシステム構築時に設定する。事前に登録されていない組織 ID を指定するとユーザは登録できない。

※ △は認証形式(PKI、IDPWD)によって異なる

(2) WisePoint データファイル一覧

ユーザ登録時に下記 2 ファイルが必要

※WisePoint ユーザロールファイルは、コマンドラインツールを使用した登録時のみ必要。

ファイル名	WisePoint ユーザデータファイル				
ファイル説明	ユーザの基本情報				
No.	項目名	タイプ	桁数(最大)	必須	項目説明
1	ユーザＩＤ	ﾃｷｽﾄ	80 文字	○	ユーザのログイン ID
2	ユーザ名	ﾃｷｽﾄ	80 文字	○	ユーザ名
3	パスワード	ﾃｷｽﾄ	80 文字	○	ユーザのログインパスワード
4	有効期限	日付		-	パスワードの有効期限 yyyy-mm-dd hh:mm:ss
5	利用可能なログイン回数	数字	10 桁	-	ユーザが利用可能なログイン回数
6	ログイン回数	数字	10 桁	-	ユーザのログイン回数
7	**制御フラグ**	ﾃｷｽﾄ	1 桁	-	0:通常 1:利用停止 9:無効
8	**ポータル ID**	数字	10 桁	-	省略

ファイル名	WisePoint ユーザロールファイル				
ファイル説明	ユーザの基本情報				
No.	項目名	タイプ	桁数(最大)	必須	項目説明
1	**ロールID**	数字	10 桁	○	所属するロールの ID
2	**ユーザID**	文字列	80 文字	○	ユーザデータファイルで登録するユーザ ID
3	**ロールの優先順位**	数字	10 桁	-	1 で固定
4	**ロール管理者フラグ**	数字	1 桁	-	0:一般所属ユーザ 1:ロール管理者

カンマ文字区切りのテキストファイル形式で記述ください。

データ1件あたり1行で記述してください。

省略可能な項目は区切り文字を2つ続けることによって省略できます。

日付は 'yyyy-mm-dd hh:mm:ss' 形式で指定してください。

漢字コードは Linux の場合 EUC-JP、Windows®の場合 Shift_JIS をご利用ください。

改行コードは LF(0x0A)、CR(0x0d)+LF(0x0A) のどちらも使用できます。

データファイル中には空行（改行のみの行）も含め、フォーマットに準拠していない行は記述できません。

データファイル中にある、各データの最初のパラメータは空白にすることはできません。

ユーザー括登録ツールは直接データベースを操作します。そのため管理ツールほど入力データの正当性や整合性のチェックをしておりません。ご利用になる際にはデータの正当性、整合性にご注意下さい。

9. 性能・容量

本認証認可 SW では認証性能の要求はなく、実証レベルで実施するため、性能や容量を特に定めない。

10. システム構成

10.1 ハードウエア

認証基盤システムは認可サーバと認証サーバの 2 台の HW で構成される。コールドスタンバイ等の冗長構成は行わない。

認可サーバ

型名	DL360G7 XE E5620 1P4C 6G P410i/256
CPU	CPU XE5620 2.40GHz 1P/4C
メモリ	6GB（2GB×3 枚）
ディスク容量	600GB (RAID-5)

認証サーバ

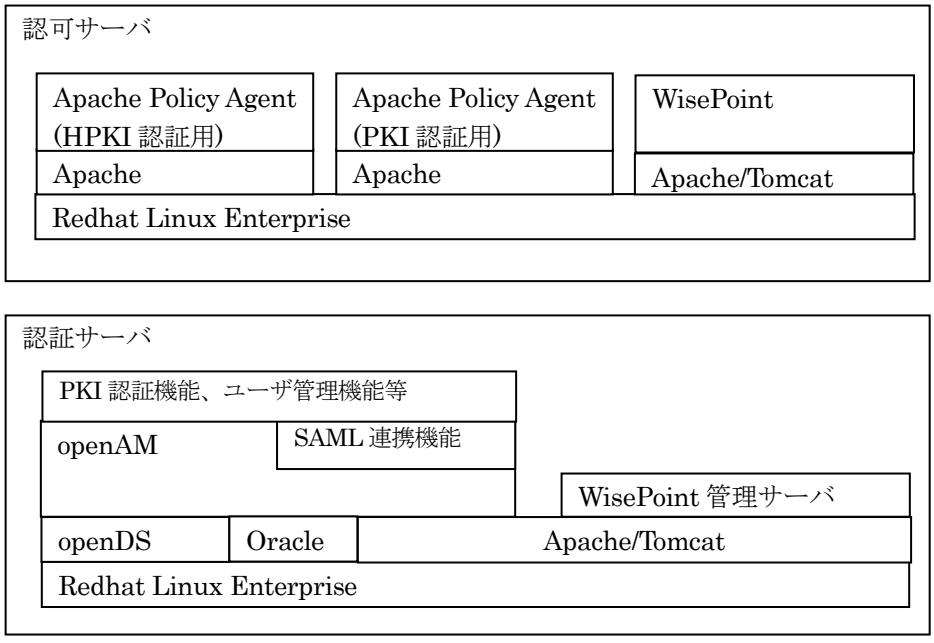
型名	DL360G7 XE E5620 1P4C 6G P410i/256
CPU	CPU XE5620 2.40GHz 1P/4C
メモリ	6GB（2GB×3 枚）
ディスク容量	600GB (RAID-5)

10.2 ネットワーク

認証基盤システムはデータセンター内に設置する

10.3 ソフトウエア

ソフトウエア構成は以下のとおり



①認可サーバ

OS	RedHat Linux Enterprise 5.7　64bit
JavaVM	JavaSE 6 JRE-6u33-linux-x64
Web サーバ	Apache HTTP Server 2.2.22 + mod_proxy モジュール + apache_v22_Linux_64_agent_304 + openssl-1.0.0g
Web アプリケーションサーバ	Tomcat 6.0.35
ウィルス対策	ServerProtect for Linux

②認証サーバ

OS	RedHat Linux Enterprise 5.7　64bit
JavaVM	JavaSE 6 JRE-6u33-linux-x64
Web サーバ	Apache HTTP Server 2.2.22 + ajp モジュール + openssl-1.0.0g
Web アプリケーションサーバ	Tomcat 6.0.35
Web アプリケーション	OpenAM 9.5.1(または opensso8.0) + 認証認可モジュール ユーザ管理アプリケーション
LDAP	OpenDS-2.2.1
データベース	Oracle11g
ウィルス対策	ServerProtect for Linux