長期運用を考慮した認証システムの設計と運用

平塚 紘一郎 [†]　大垣内 多徳 [‡,†]　田中 光也 [†]
福井大学 総合情報処理センター [†]　福井大学 医学部附属病院 医療情報部 [‡]

概 要

全学に供することを目的とした認証システムの設計構築を LDAP/PKI を用いて行った．長期にわたり電子的記録を行うシステムでの利用に対応するために，ランダム且つ一意に生成した cn を本学における籍の有無や身分等とは独立な，永久的な個人識別子として採用している．個人識別子と uid を独立に設定することで，管理の簡便性と利用者の利便性との両立を図った．また，本システムではログにデータ作成・変更者の記録をタイムスタンプを付加して保存することにより，問題等が生じたときの監査を可能にしている．本システムの報告とともに，導入や運用上の問題点や留意することがらについて報告する．

Design of an Authentication System which Considered Long-Term Use

Kouichirou HIRATSUKA[†]　Tatoku OGAITO[‡,†]　Mitsuya TANAKA[†]
Center for Computing and Network Services University of Fukui[†]
Department of Medical Informatics, University of Fukui Hospital[‡]

Abstract

An authentication system for a university was designed and constructed with LDAP/PKI system. In order to make an electronic data in the system is available over long time period, randomly and unuiqly generated 'cn', not 'uid' was adopted as unique personal identifier, where 'cn' was treated as a eternal identifier and 'uid' as a temporal one. Operation log was also recorded with the electric signatures of operators and timestamps. The separation of 'cn' from 'uid' provides convenience for both the system administrators and the users. The log with the signatures and timestamps make possible to audit the genuineness of the data.

1　はじめに

近年，コンピュータが広く普及し，様々な用途に用いられるようになった．これまで紙で作成されていた書類もコンピュータ上で作成されるようになり，電子化が進んできている．このような電子化された文書では，一般に紙に記載された文書と比較して偽造や改竄が容易であるとともに，作成者を特定することが困難である．これらの問題に対する解決策の一つとして，公開鍵暗号方式による電子署名が挙げられる．また，電子署名などを用いることで，電子的文書に法的効力などを持たせることができるようにした，e-文書法も施行された．このような背景から，今後は重要な文書などについても電子化が進むものと思われるため，公開鍵基盤等を整備していくことが非常に重要となる．

また，一般的なコンピュータシステムでは，利用者を確認するため，認証を必要とすることが多い．しかしながら，相互に関連しない複数のシステムが存在した場合，認証システムもそれぞれシステムごとに構築されることが多い．その結果，システム間で異なるアカウント名，パスワードが用いられることにつながり，利用者の利便性が損なわれている．さらに，利用者が記憶できないパスワードを書き留めることによるセキュリティ低下も問題となっている．このような事態を解消するため，最近になり，各システム間の認証システムを統一し，単一のアカウント名とパスワードで複数のシステムを利用できるようにする「統一認証システム」と呼ばれるものが様々な組織で導入されている．公開鍵基盤における個人識別子をこの統一認証システムにおける利用者 ID と統合することで，利用者に対して認証サービスの延長として公開鍵基盤における証明書を捉えさせることが可能である．しかし，一般的に認証システムにおいて，ある時点における個人の特定を目的としており，長期に渡って個人を特定できように

はなっていない．ある時点での認証結果をそのまま保存しただけでは，時間が経過した際に個人の特定が行えなくなる可能性が大きい．

このような問題を念頭に置いて，福井大学総合情報処理センターでは，学内に対する認証サービスを開始するうえで，長期にわたり個人特定ができることを，認証システム設計の重要な基本要件のひとつと位置づけた．これは，本認証サービスの想定される利用システムの中に，医学部附属病院や総合機器実験センター放射線同位元素実験部門等，電子文書の長期にわたる保存が法令により義務づけられているシステムが多数含まれているためである．以下では，長期運用を可能とするために考慮すべき点を述べ，それらに対する本認証システムにおける対応策を示す．その後，運用を開始するにあたっての初期データ作成時の問題点や運用上留意すべき点についての議論を行う．

2　考慮すべき問題点

長期にわたり，認証の結果と実在の人物を紐づけることが可能な認証システムを構築するためには，以下のような点について考慮する必要がある．

- 長期に渡る個人追跡の担保
- 組織構造からの独立
- 提供データの客観的正当性の提示

まず，長期に渡って個人を特定するためには，長期間変化しないような個人識別子を導入する必要がある．一般的に個人識別子としてはアカウント名が用いられることが多いが，利用者が直接意識するアカウント名は変更希望や，過去に使用されたアカウント名の再利用などを考慮すると，長期にわたり個人特定を行うには不適切であると思われる．一方，運用ルールとして，取得したアカウントの変更は認めないというシステムも可能ではある．しかし，改姓等によるアカウント名と姓名の解離や，システム運用から経過する時間が長くなった場合に，希望アカウント名が利用できないケースが増えるなど利用者の利便性を阻害するものと考えられる．

次に，長期にわたり運用する場合，組織構成に変化が起きる可能性を考慮するべきである．特に組織変更があった場合でも，個人識別子の変更を行う必要がないよう，配慮を行わなければならない．

最後に，登録されているデータが，いつ，どのような権限を持った人物によって登録されたのかを後から検証できるようにするべきである．認証システムへの登録から時間が経過した後，個人識別子に対する問い合わせが発生しても，客観的にその登録作業が適切であったことが説明できるようなシステムである必要がある．

3　システムの設計

近年，認証システムにおいては，登録情報の保存に LDAP （Lightweight Directory Access Protocol）が用いられていることが多い．本認証システムでも LDAP を用い，システムの設計および構築を行った．データ構造は RFC 4512，RFC 4514 に従い，利用する属性としては posixAccount（RFC 2307），person（RFC 4519），inetOrgPerson（RFC 2798）等に代表される標準的なものを基本的に用いる．その上で，長期運用に必要であるが，標準的なものが定義されていない必要最小限の項目について，IEEE より OID の割り当てを受けた上で，スキーマの拡張を行った．サーバとしては，LDAP の一実装であるサン・マイクロシステムズ社製の Sun Java System Directory Server（SJSDS）を採用している．

3.1　個人識別子の選定

長期にわたる個人特定のためには，個人識別子の選定が重要となる．まず，長期にわたって一意である必要があるため，表現できる文字列の種類が組織の人数に対して大きいのはもちろんのこと，ある程度の年数が経過した場合の人の出入りについても考慮しなくてはならない．さらに，個人識別子を変更または削除してしまうと，個人の特定が困難になるため，一度個人に割り振った個人識別子はシステム上に永続的に保存しておく必要がある．また，電子的文書に個人識別子を保存するにあたり，文字

の種類や文字列の長さにも配慮する必要がある．記号や特殊文字は使わないようにし，文字列長も短いものにしておく．様々なシステムに対応するためには，以上のような制限を設ける必要があると考えられる．

認証に用いる個人を特定するためのデータは，相対識別名（relative distinguish name: RDN）として，アカウント名（uid）が利用されることが多いと考えられるが，これは前節で述べたように長期保存を考えた場合には適切ではない．我々は，uid に代わる RDN として cn を利用することとした．cn は RFC 4519 において，対象に与えられた名称（“names of an object”）と定義されている．同定義の中で人に対するデータの場合，典型的な使い方としては「フルネーム」を用いる（“If the object corresponds to a person, it is typically the person’s full name.”）ともあるが，RFC 2798 において定義される displayName が利用可能であると考えたためである．普段の認証作業では利用者は uid を用いて認証を行うため，利用者が cn を意識する必要は無い．従って，覚えづらいものであっても問題無い．さらに，個人情報保護の意味で，他人に推測されない方が好ましいと思われる．以上の理由から，本システムでは cn をランダムに生成した．使用する文字は英字と数字（合わせて 36 文字）とし，文字列長は 8 桁とした．ただし，最初の文字は英文字とし，大文字と小文字の区別はつけないようにした．よって，$26 \times 36^7 \cong 2.0 \times 10^{12}$ 通りの文字列が生成できる．これは世界の人口（$\cong 6.6 \times 10^9$）と比べても十分大きく，長期にわたって個人識別子を割り振るにあたり，十分な大きさである．

以上のようなルールに従い，ランダムに生成した cn を，新規登録時に利用者へ割り当てる．

3.2 アカウント名の設計

一般の認証システムと同様，本認証システムにおいても uid をアカウント名とした．uid はログイン時のアカウント名や，メールアドレスの local part として用いられる．普段利用者が意識するため，選択権を与えることもサービスとして重要と考え，設計を行った．

本システムでは，アカウント名を個人に対する一属性とした．アカウント名で個人を特定するのでは無く，個人識別子によって個人を特定するため，アカウント名の変更が可能となっている．さらに，アカウント名はシステム上ある時刻において一意であればよく，離学などで無効となったアカウント名を再利用することも可能となっている．離学などによりアカウントが無効となる場合，そのアカウントが最後に使用されていた期間を保持しておき，同じアカウントの割り当て要求を受けた場合には情報を調べる．その結果，過去に使われていたアカウントであった場合は，移行期間などを考慮し，一定期間（本システムでは 2 年間を想定）経過していた場合，再使用を許可する．これにより，長期運用を行っても使用できるアカウント名が必要以上に減ることはなく，不自然なアカウント名を使用する頻度が低くなる．

なお，uid は英文字から始まる 2 文字以上，最大 8 文字の英数字とした．近年のシステムではアカウント名として扱える文字の種類や数は増えているが，様々なシステムでの利用を考え，このような制限を設けた．

初期登録時にはユーザからの希望を聞き，現在有効な uid と，過去に使用されていた uid でブロック期間が終了していないものの両方と重複しないように割り当てを行う．また，ユーザから正当な理由による変更申請があった場合は，変更を行う．なお，SPAM メールが大量に届いたりストーカーの被害にあったりするようなメールアドレスのみを変更したい場合には mailAlternateAddress を利用することも可能である．ただし，この属性に関しては標準化作業が中断し現状では draft も expire しているため，今後問題となる可能性が残る．

3.3 組織構造との関連

LDAP のデータ構造として構成員の所属情報を表す手法としては，個人を表現する DN 中に組織情報を含めるものと，従来の unix におけるグループ管理と同様，別空間として取り扱うものに大別できる．本システムでは，以下のような理由により個人を表現する DN には，所属部局の情報をいっさ

い含めず全ユーザを flat に登録するような設計を採用した．

- 所属部局の変更
  多くの組織では，定期的に人事異動が行われる．DN に組織情報を含めた場合，構成員の所属を変更することは不可能となり，データの再登録が必要となる．

- 組織構成の変更に対する対応
  一般に，組織はその存在を保つために常に内部構成を更新していくものであり，長期にわたり運用する認証システムを構築する場合，組織構造が変更される可能性を考慮にいれなければならない．個人を表すエントリの DN に組織情報を含めた場合，改組が発生した場合，所属部局が変更されたことと同様な問題に遭遇する．

- 複数の所属を持つ個人の表現
  組織において，すべての構成員の所属がただ一つに定まることは極めて稀である．多くの場合，複数の部局を兼任・併任している構成員が存在する．DN に，部局の情報を含めた場合，このような構成員の表現が不可能となり，所属部局を削ることによるデータ表現の完全性の欠如もしくは同一人物に複数の識別子を発行することによる追跡可能性の低下を招くものと考えられる．所属部局を，個人に対する一属性として捉えることで，このような問題に対応することは可能である．

3.4 データに関する説明責任の実現保証

最後に取り上げるのは，説明責任である．情報システムの運用部門と，組織構成員を把握しいる人事（学務）部門は異なっているのが一般的と考えられる．このような場合，情報システム運用部門によって運営されている認証システムが提供する認証データが，実際の組織構成員を反映しているかどうかを確認するのは非常に困難である．この問題に対応する一手法として，福井大学総合情報処理センター認証システムにおいては，データ登録時に正当な電子署名が施された入力のみを受けつけ，その記録に対してタイムスタンプを取得することで，「このデータをいつ，誰が登録した」のかを第三者により検証できる仕組みが実装されている．(DSM-47-2) 通常の認証システムのように比較的短い期間であれば，署名情報より登録者に関する情報が比較的得やすいため，この仕組みは有効に機能すると考えられる．

しかし，長期にわたる運用を考えた場合は，登録者が退職等により組織を離れることで登録者に関する情報が失われている可能性を考慮する必要が生じる．つまり登録されるデータの作製者を担保する事と，登録されるデータの内容について担保することは大きく異なるのである．この問題に対して，データ作製者の確認を行うとともに，データ作製者を実空間における，人事部門担当者に制限を行う機能を実装した．これにより，身分証明書の発行等に用いる人事関連の一次データと等価なもののみが，認証データベースに登録されるように運用を定めることが可能となり，実空間における身分証明書とほぼ同等の信頼性を確保できたものと考えている．

4 実際の運用と問題点

2007 年 4 月より，福井大学全学（工学部，教育学部，医学部，附属病院，事務局）を対象とした統一認証システムの運用を開始した．全教職員ならびに全学生合わせて 7000 人程度のデータを初期投入した．この統一認証システムは，本学総合情報処理センターの計算機や，メールアドレス（foo@u-fukui.ac.jp）のアカウントとして用いられている．ここでは実際の運用とその問題点について述べる．

4.1 初期データの作成

本学は，旧福井大学（工学部，教育学部）と旧福井医科大学（医学部，附属病院）が平成 15 年に統合されて新福井大学となった．その時点では，総合情報処理センターが管理する計算機システムにおいて旧両学のアカウントは統合されていなかったが，統一認証システムを導入するにあたって，アカウントの統合が行われた．

まず，複数のシステム上にあるアカウントを統合しなくてはならない．当然ながら，複数のシステムの同じアカウント名を別々の人が使用している可能性もあるので，調整する必要がある．調整にあたり，附属病院での現場の混乱を防ぐために，病院職員に対して優先してアカウントを割り振った．その後，残りの教職員に対し希望アカウントの調査（第 4 希望まで）を行ったが，重複は全体の 2% ほどであった．

次に，決定されたアカウントと人事データの突きあわせを行ったが，この作業は困難であった．まず，国立大学法人の場合，常勤職員と非常勤職員で異なる職員番号の番号体系となっており，同じ番号が複数の人に割り当てられることがある．また，非常勤職員の場合，雇用契約ごとに職員番号が発番されるため，同一人物が複数の職員番号を有する場合がある．さらに，外注職員などを含めると全ての職員を把握している部署は無く，各部局で独自の方法で人事を管理している場合もあった．これらの理由から，はっきりと個人を特定することができない事例が存在した．

現状では，氏名，生年月日と他の情報も含めて，個人を特定しているが，実際に対応がうまく取れておらず，修正を行った例もあった．

4.2 人と登録情報の対応

4.1 節でも述べたとおり，人と登録情報の対応を取るのは困難であったが，さらに実際に運用していくと異動などが生じる．このような，人がどう動いたかということを追跡するのは大変であることが分かった．例として，一度離学し，後に復学した場合の手続きを以下に示す．

1．紙媒体で過去の在籍の有無を確認

2．在籍していた場合，在籍期間および雇用形態を確認する

3．氏名と生年月日等から当時の雇用番号を調べる

4．雇用番号ををもとに，LDAP 上の登録データを調べる

以上のような手続きにより，人事部門は cn の特定を行う．上記手続きの 1 〜 3 は，人事部門システムで行われ，統一認証システムでは 4 の手続きのみを行う．そのため，統一認証システムにおいては，過去に割り当てられたすべての雇用番号を保存しておかなければならない．雇用番号を格納する属性としては RFC 2798 に employeeType が定義されているが，この属性は single-value であり，この目的には利用できない．そのため，スキーマ拡張を行い，複数の雇用番号を格納することが可能な別の属性を定義した．

5 まとめと今後の課題

長期にわたり個人特定が可能な認証システムの設計と構築を行った．

そのためには，システムだけではなく運用，特にデータの作成や変更などを適切に行う必要があり，明確な運用ルールを定めなければならない．人事異動などの際には，人事を担当している部局に署名付き LDIF の作成など，特殊な作業を行ってもらうこととなるため，どのようにすればうまく連携が取れるかなどについても考えていく必要がある．また，公開鍵基盤で証明書の発行を行う CA については，有効期限が設定されているため，これを満了した時点でどのように既存の情報を検証するか，今後検討を行う必要もある．

参考文献

[1] 電子署名及び認証業務に関する法律:
http://www.meti.go.jp/policy/netsecurity/digitalsign-law.htm

[2] e-文書法の施行について:
http://www.kantei.go.jp/jp/singi/it2/others/e-bunsyou.html

[3] RFC 2251: Lightweight Directory Access Protocol (v3)

[4] RFC 2307: An Approach for Using LDAP as a Network Information Service

[5] RFC 2798: Definition of the inetOrgPerson LDAP Object Class

[6] RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information ModelsLightweight Directory Access Protocol (v3)

[7] RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names Lightweight Directory Access Protocol (v3)

[8] RFC 4519: Lightweight Directory Access Protocol (LDAP): Schema for User Applications