サーバ証明書申請・発行システムの構築
－山口大学における UPKI 導入事例－

Construction of a System to Apply for and Issue Server Certificates
－ An Implementation of UPKI in Yamaguchi University －

永井好和† 王躍† 佐伯 徹郎† 久長穣†
多田村克己‡ 三池 秀敏‡
Yoshikazu NAGAI Yue WANG Tetsuro SAEKI Yutaka HISANAGA
Katsumi TADAMURA Hidetoshi MIIKE

† 山口大学大学情報機構メディア基盤センター
‡ 山口大学大学院理工学研究科
† Media and Information Technology Center, Organization for Academic Information, Yamaguchi Univ.
‡ Graduate School of Science and Engineering, Yamaguchi Univ.

（概要）

本論文では，国立情報学研究所が進める UPKI（University Public Key Infrastructure）の山口大学への適用に際して，登録局の一部機能を担当するために構築した，申請者の本人性や実在性等の確認方式を提案する．2004 年度から山口大学ではプライベート認証局の構築を進めたが，クライアント PC が使用するブラウザとの連携に新たな問題が生じてきたため，当初の予定通り普及するに至らなかった．この課題は，国立情報学研究所のプロジェクトに参画して，信頼性のあるサーバ証明書を用いることにより解決することができた．このプロジェクトにおいて，参加機関である山口大学は，申請者の本人性・実在性・管理責任およびドメインの実在性を確認する責務を負い，山口大学内ではメディア基盤センターがこの役割を担った．山口大学は主要３キャンパスに分散しており，各キャンパスで同じ対応が求められる．この環境の中，これまでに統一認証，教職員データベース，ホスト接続データベースを整備してきた．この利点を生かして，Web を介したサーバ証明書発行申請の手続きを簡略化する仕組みを構築した．本論文では，山口大学独自の仕組みを紹介し，学内サーバへの電子証明書インストールを促進した効果について報告する．

キーワード

UPKI，サーバ証明書，登録局，本人性確認，実在性確認

１．はじめに

山口大学（以下，本学）では，情報セキュリティ文化の向上を図るべく，さまざまの施策を進めている．情報セキュリティポリシーの策定をはじめとして，技術的セキュリティレベル向上のための学内ネットワークにおける統一認証や認証機能付き情報コンセントの普及，人的セキュリティレベル向上のための情報セキュリティ講習会，組織的セキュリティレベル向上のための ISMS（Information Security Management System）構築など多岐にわたる．一方，情報セキュリティの観点からは，学外からのアクセスに対する要望は多いにもかかわらず，多くのアプリケーションシステムが学内限定での利用にとどまっている．学外からのアクセスをより安全なものとするために，公開鍵基盤（PKI；Public Key Infrastructure）が有効である．本学では，早くから学

内における認証局の必要性を認識し，プライベート認証局の構築を進めてきた. しかし, 一般的に利用されるブラウザへの公開鍵のインストール作業の煩雑さから, プライベート認証局の普及が進まなかった. そのような状況の下, 2007 年 4 月より国立情報学研究所（以下，NII）における「大学間連携のための全国共同電子認証基盤（UPKI）構築事業」の一環として,「サーバ証明書発行・導入の啓発・評価研究プロジェクト」（以下，NII プロジェクト）が開始された[1]．全国の SINET 加入大学の参加により全国規模で共同の認証局を設置し，これによる認証基盤の運用ベースの評価をしようというものであった．参加大学に無料でサーバ証明書が提供されること，クライアントに新たなソフトのインストール作業が不要であることの２点が非常に魅力的であり，本学からはメディア基盤センター（以下，センター）が参加した.

他の NII プロジェクト参加大学の状況については, 東京大学からの報告がある[2]．東京大学では，本人確認などについては対面での確認を原則にしている. さらに部局の独立性を重要視して，大学全体のための登録局の他に部局登録局を設置する２重構造としている．本学では，教職員データベース，ホスト接続データベース等の仕組みが既にあり，学内ネットワークへのログインのための統一認証の仕組みが確立されている[3]．この環境の下で，大学における迷惑メール対応を統一的に実施している[4]. 本論文では，既存の仕組みを組み合わせて，人による作業プロセスを含めた申請者の本人性・実在性・管理責任およびドメインの実在性を確認するシステムの構築方法を提案する．提案システムは，分散キャンパスでの運用に通用するよう一部の確認事項を自動化するとともに，確認作業をルーチンワーク化することによって，PKI の知識を十分持たない教職員にも対応可能な仕組みである点に特徴をもつ.

本論文では，２章において本学におけるこれまでの認証局の取り組みと問題点について説明し，３章でその解決のための学内プロジェクト，４章で提案システムの詳細，５章でその運用状況・評価の順に説明した後，最後に６章で結論および今後の課題を述べる.

２．山口大学におけるこれまでの認証局の取り組みと問題点

2.1　山口大学プライベート認証局

センターでは，多数のサーバを維持管理し，学内に多様な情報サービスを提供している．本学では，以前より各サーバのために自己署名によるサーバ証明書を使用していたが，信頼に足るものではなかった．少なくとも学内において信頼できる認証局の構築が必要であるとの認識に立ち，サーバの実在性確認及び通信路の暗号化の必要性を認識して, 2004 年には学内プライベート認証局を構築した．この認証局により，センターの主要サーバを含む学内サーバに対してプライベートサーバ証明書の発行を行なってきた（なお，認証局サーバには，商用電子証明書を使用している）.

2.2　情報セキュリティ上の課題

プライベート認証局の場合，これらのサーバにアクセスするクライアント PC に, 対応する公開鍵をインストールする必要がある．プライベート認証局のサーバ証明書の場合, プライベート認証局の公開鍵がインストールされていないクライアント PC のブラウザでは必ず図１に示すような警告メッセージが表示される．これは，このクライアントがアクセスしているサーバの証明書の信頼性に疑問があることを示し，処理を続行するかどうかをユーザに問いかけるメッセージである．ユーザはサーバを信頼するか,（信頼しないで）処理を中止するかの選択をしなければならないが，従来は疑問を抱かず処理続行を選択することが常習化する傾向にあった．本当の警告の場合であっても無視することになるため，きわめて危険な運用をしていることとなる．これが第１の問題点である.

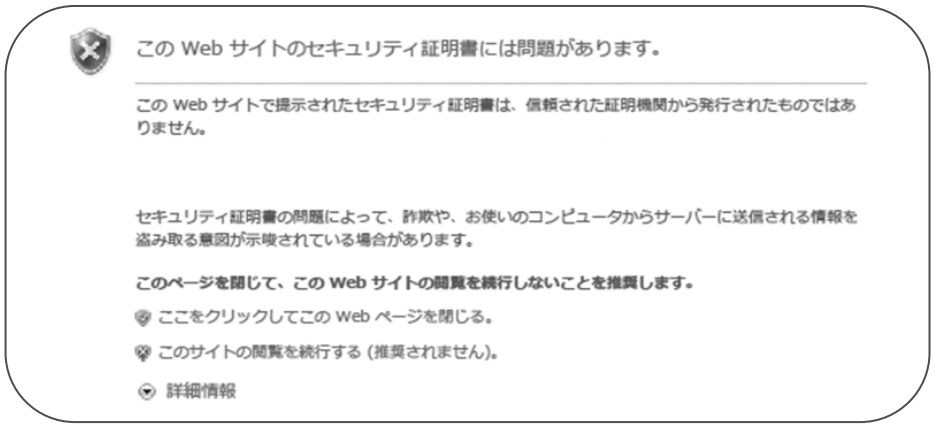

図１　サーバ証明書の信頼性警告画面（IE7 での例）

2.3　コスト上の問題

本学プライベート認証局の発行するサーバ証明書は無料であるが，商用電子証明書については，１件あたり年間約１万円の経費が必要であった．すべてのサーバについて商用電子証明書を利用する場合には, サーバごとに約１万円の年間経費が必要になる．これは，多数のサーバを維持管理する本学においては, 負担が大きすぎる. これが第２の問題点である．

３．UPKI試行プロジェクト

3.1　学内の NII プロジェクト参加体制

前章の第１と第２の問題点が解決されるためにNIIプロジェクトに参加したと言っても過言では無い．参加のためには，以下に示す第３と第４のさらなる問題を解決する必要があった．

NII プロジェクト[1]により，学内サーバ用電子証明書を無料で利用することができ，同時に学内の情報セキュリティレベルを向上させることができることが期待され，本学としても参加するべきプロジェクトであった．学内の対応組織として，教職員からなる UPKI 試行プロジェクト（以下，本学プロジェクト）を設置して，サーバがこの認証局を利用するよう学内の仕組みを整備する活動を開始した．公開鍵基盤（PKI ; Public Key Infrastructure）や電子認証に関する知識を十分持たない職員でも，サーバ証明書の申請者が本人であること等を正しく確認できる仕組み（体制）をつくり，センターの学内サービスの１つとして位置づけたうえで，次の２点の達成をめざした．

（１）　学内サーバの信頼性向上

（２）　サーバ証明書の維持管理コストの削減

プロジェクト参加条件のほとんどを満たしていることは確認できたが，「機関ごとに参加申し込みを行う」という条件により，センターがNIIのプロジェクトに参加するためには，センターが本学の窓口となることについて学内他部局の了承が必要であった. 同時に, 本学における認証基盤としてUPKIを採用することについて，学内の意思統一を図る必要があった．この点が，第３の問題点である．

センター内に本学プロジェクトを設置したことは, センターが本学におけるNIIとの窓口となること, およびNII提唱のUPKIを採用することをオーソライズする上でも役立った．

3.2　分散キャンパスでのセンターの役割

NII提唱のUPKIのサーバ証明書発行の諸手続の中で，次の項目の確認が本学の役割である．

(1)　申請者の本人性確認

学内のサーバ管理者（サーバ証明書発行申請者，NII のプロジェクトでは「加入者」）が実在し，間違いなく本人がサーバ証明書の発行を申請していることを確認すること．

(2)　申請者の実在性確認

申請者の所属が実際の所属と一致していること．

(3)　申請者のサーバの管理責任の確認

サーバが申請者所属の組織の所有または管理下にあること．サーバが参加機関の所有または管理下にあること．申請者がサーバの管

理者であること（申請者が，申請対象サーバを実務レベルで管理しており，サーバ証明書のインストールを含む操作と管理が可能であること）．

(4)　ドメインの実在性

申請対象サーバのドメインが実在すること．

これらの役割を，センター職員の増員なしで，しかも UPKI に関する専門的な知識のない職員で対応する新たな仕組みが求められた．しかも，本学は主要キャンパスが，山口市に１キャンパス，約４０ｋｍ離れた宇部市に２キャンパスある．そのため，各キャンパスにセンターの地区センターが設置されている．申請者が本人確認のために，キャンパス間を移動することは現実的ではなく，各キャンパスそれぞれにおいて申請者の本人確認が可能となる仕組みが求められた． これが第４の問題点である．この解決手段の詳細については次章で述べる．

3.3　プロジェクトの役割

サーバ証明書発行申請手続きの方法とともに，センターが無料のサーバ証明書発行の申請を受け付けることを学内に広報して，より多くの学内サーバにサーバ証明書を備え付けて各サーバの信頼性を向上し，UPKI を普及することを目指した．整理すると，次の２点が本学 UPKI 試行プロジェクトの役割であることを再確認して，構築を進めることとした．

(1)　サーバ証明書発行申請手続き

(2)　サーバ証明書発行の拡大・普及

４．サーバ証明書申請・発行システム構築

4.1　システム構築における基本的な考え方

サーバ証明書申請・発行システムは，事務処理を行う職員などの要員と，Webによる申請書受付を処理するコンピュータシステムである申請受付サーバとで構成される仕組みである．本学内のサーバ証明書申請の仕組みづくりのために，まず各種事務手続きを明確にし，その手続きを実施するための仕組み（Webページのデザインや申請受付サーバ）のあり方を検討した．

第４の問題点を解決するための課題は，次の２点にあった．

(1)　分散キャンパスでも，統一的に，申請者の本人性確認，実在性確認，サーバ管理責任の確認といったサーバ証明書申請手続きの一元管理ができること

(2)　PKIに関する知識の希薄な職員による作業ができること

本学プロジェクトでは，分散している各キャンパスどこからでも学内ネットワーク経由（Web経由）で申請書を提出できるアプリケーションシステムを開発した．申請受付サーバは，受け付けた申請書を一元的に蓄積し，サーバ証明書申請手続きの履歴を一元的に管理する仕組みとした．

人による手続きについては，本学におけるサーバ証明書申請手続きについて，関連規則，対応体制，具体的な担当者などを決めて，担当者の事務要項を作成した．申請者が勤務するキャンパスの地区センターそれぞれの登録担当者が対応することとし，各地区センター窓口職員が副登録担当者として事務処理を実施することとした．Webによるサーバ証明書発行申請の仕組みの検討に当たっては，新たな要員を求めることなく既存のセンター職員で対応可能とする点に留意した．属人性を排するために，センター職員の事務作業をルーチンワーク化して申請受付サーバと連携した仕組み（システム）を作り，PKI に関する知識の乏しい職員でも本学の役割を担える運用を可能とした．そのため，事務フローの見直しから始めてシステムを設計した．図２は，サーバ管理者によるサーバ証明書発行依頼から，メディア基盤センターでの確認・審査作業を経て，同センターがNIIプロジェクトにサーバ証明書発行を申請し，それを受けてサーバ証明書が発行されるまでの手続きの概略を示したものである．

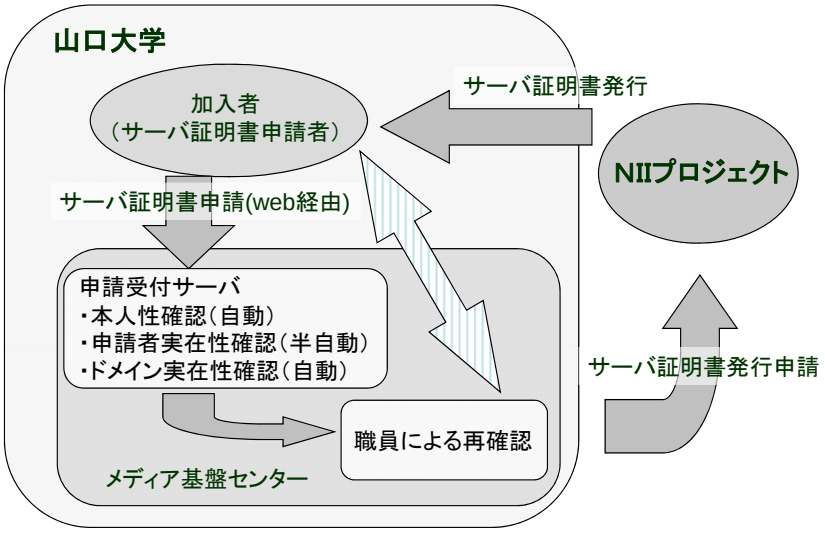

図２　　サーバ証明書申請・発行手続き概略

今回構築した提案システムの特徴は，学内における各手続きの中で，本学に既にある制度や仕組みを組み合わせるなどして，本学の役割を果たす仕組みを構築した点である．図に示す申請受付サーバを設置し，Web経由で次の４点の確認を自動的（または半自動的）に実施することにより，職員の作業項目を削減した．

(1)　申請者の本人性確認
　・統一認証（自動）
(2)　申請者の実在性確認
　・教職員データベースとの突き合せ（半自動）
(3)　申請者のサーバの管理責任の確認
　・ホスト接続データベースとの突き合わせ（半自動）
(4)　ドメインの実在性
　・DNS照合（自動）

なお，提案システム稼働当初しばらくは，申請者の本人性確認をより確実なものとするために，一度はセンター窓口に来訪頂いて名札（ICカード）による確認を併用している．

4.2　確認作業の実現方法

図３は，サーバ証明書の申請から発行までを事務手続きの流れに注目して示したものである(各手続きの詳細は付録参照)．ここでは，本学が担う役割にかかわる主な手続きについて説明する．

センターが主として４つの確認を行う役割を担うことは前述のとおりである．それぞれの確認事項が，図３記載の各手順のどこでどのように実現されているかを整理する．

まず，申請者の本人性確認の仕組みについて述べる．「確認１」（図中④）と「確認３」（図中⑩）の２回にわたって確認作業を行っている．前者は申請受付サーバが自動的に実施するものであり，本学の学内ネットワークの統一認証の仕組みを活用している．加入者が申請受付サーバにアクセスするためには，学内ネットワークにログインする必要がある．このときに使用するユーザ名/パスワードは本人しか知りえない情報であり，学内ネットワークにログイン出来たことを持って本人であると判断している．本学教職員は全員「公式メールアドレス」を付与され，センターが運営する共通のメールシステム（メールサーバ）を利用している．公式メールアドレスは教職員一人に１個与えられる．

「@yamaguchi-u.ac.jp」の前が本学内ネットワーク利用のためのユーザＩＤを兼ねている．申請書には申請者（加入者）のメールアドレスを記入欄があり，このメールアドレスが公式メールアドレスとして登録されているものであれば，教職員本人のものであると判断できる．

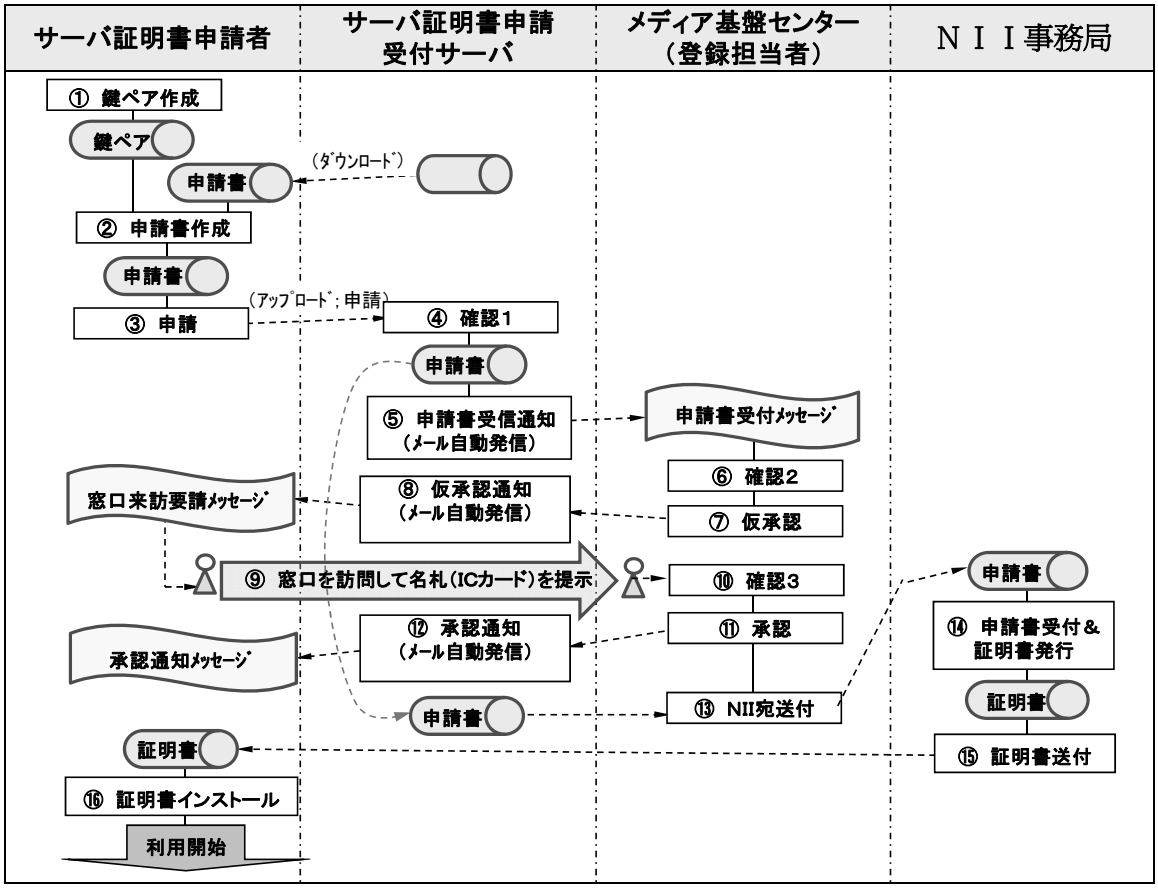

図 3　サーバ証明書申請・発行事務フロー（イメージ）

本学教職員は全員任用時に，人事課において撮影したデジタル写真画像を，氏名及びローマ字のイニシャルとともに IC カード表面に印刷した名札が貸与されている. 一般社会における自動車免許証同様，学内においては，この名札の保持者が印刷されている氏名の教職員本人であることを示す．ここでも，本人性確認のために本学の既存の仕組みを活用している．

次に，申請者の実在性確認について説明する．本学の教職員の公式メールアドレスは，学内でのみ参照可能な Web ページ「教職員アドレス一覧」に掲載される．この Web ページは人事課において管理されている教職員データベースをもとに作成されており，この一覧に掲載されている教職員が本学に在籍し，申請元である（申請者の）所属部署に所属していること，即ち実在していることを示している．

次に３つ目と４つ目の確認事項である申請者にサーバの管理責任があることの確認と，ドメインの実在性確認について説明する．本学においては，学内ネットワークにサーバや PC 等の機器を接続する場合には,「ホスト接続申請書」をセンターに提出して承認を取る必要がある．これは学内規則である「山口大学情報ネットワークシステム接続利用規則」に基づくものであり，ホスト接続データベースに登録され, センターにおける接続機器の IP アドレス管理（DNS 自動登録）の根拠にもなっている．ホスト接続データベースには次の項目等が登録されている．

・申請者（サーバ接続申請者）の所属・氏名
・運用（技術）担当者の所属・氏名
・FQDN 名
・設置場所（棟の名前，部屋名）

従って, サーバ証明書申請者とホスト接続申請者（または運用（技術）担当者）とが同じ教職員であれば，サーバの管理者自身がサーバ証明書発行を申請していると判断できる．もし両者の氏名が異なる場合，必要に応じて変更手続きなどを行う（例えば，ホスト接続申請時から管理者が交代しているが，変更手続きがなされていないケースなど）.

4.3　申請受付サーバの構築

既存のプライベート認証局の資産(ハードウェア，ソフトウェア）を活用して，新たな費用を発生させない方針で開発を進めた．特に注力したのは次の４点である．

(1)　操作性に十分配慮し，操作マニュアルは Web ページに書き込むなど，操作中に参照できること

(2)　申請書などの文書について Web ページを通じてやり取りできること

(3)　アクセスコントロールを通じて情報セキュリティに配慮すること

(4)　Web 上で，申請状況を管理できること

以上に配慮して，学内要員にて開発した．ハードウェアについても既存のサーバを転用することで，新たな経費の発生を抑えた．

５．サーバ証明書申請・発行システムの運用と評価および今後の取り組み

5.1　サーバ証明書発行状況

2008 年 3 月末日現在，25 台のサーバにおいて NII 発行のサーバ証明書を利用している．センターにおいて稼働させ維持管理しているサーバが大多数を占めるが，他部局のアプリケーションサーバにおける利用も始まっている．

5.2　運用状況

加入者は，前述のとおりセンターのホームページから随時申請書をアップロードできる．申請発生を通知するメールが自動的に登録担当者宛に届くため，登録担当者が気付かないまま受付案件が未処理になることはない．登録担当者においても，受付サーバが初期確認を自動的に実施し，確認動作が具体的な作業として明確になっていることから，ほとんど負担が増加していない．

5.3　評価

加入者にとっては，センターホームページの説明を読むことにより申請方法が判るとともに，初期確認が終わるまで（仮承認が終わるまで）センターに出向く必要がない．また，サーバ証明書がメールにより送付されるため，申請からサーバ証明書入手までの間で，各キャンパスのセンター窓口に出向くのは一度だけであり，非常に効率的であるといえる．各キャンパスの受付窓口担当者（登録担当者）においても，ルーチンワーク化された手順が確立されているため対応が容易であり，ほとんど手間のかからないサービス業務となっている．

5.4　サーバ証明書発行の拡大・普及への取り組み

提案システムの運用開始に合わせて，サーバ証明書利用促進のための広報活動として，センターは以下の広報活動を実施した．

(1) センターメールマガジン（不定期で全学教職員学生に向けて発信）にて，サーバ証明書発行申請受付開始を案内した．

(2) センターホームページから申請受付サーバへのアクセスを可能とした．

前述のように，センター以外に設置されているサーバにおけるサーバ証明書の利用は未だ低調であるため，全学対象の説明会の開催等による啓蒙活動を実施する予定である．

６．まとめ

本論文では，本学の既存の仕組みを組み合わせて，申請者の本人性・実在性・管理責任およびドメインの実在性を確認する，人による作業プロセスを含めたシステムの構築方法を提案した．提案システムは，分散キャンパスでの運用に通用するよう一部の確認事項を自動化するとともに，確認作業をルーチンワーク化することによって，PKI の知識を十分持たない教職員にも対応可能とすることができた．今回 NII プロジェクトに参加することにより，以下の２つの目的を達成できた．

(1)学内サーバの信頼性向上

(2)サーバ証明書の維持管理コストの削減

従来，学内の多くのアプリケーションにおいて，ブラウザが表示する警告メッセージを無視するか，あるいは無条件でサーバを信頼する傾向にあった．しかし，NII 発行のサーバ証明書の普及により，この警告メッセージを，注意を払うべき警告として受け止めるように変化してきた．警告メッセージは表示されないのが正常であるとの認識に立つ，本来の

姿になってきていることは，サーバの信頼性を向上させたことに他ならない．また，従来のプライベート認証局発行の証明書利用の場合に必須の作業であった，各クライアント PC のブラウザに対応する公開鍵をインストールする作業が不要であった．このインストール作業を不要とすることは，大学独自でプライベート認証局を構築・運営する場合には，ほぼ不可能なことと考えられ，実用面から見ても今回 NII プロジェクトに参加した意義は大きい．

また，商用サーバ証明書を利用する場合，1 件あたり年間約 1 万円が必要である．本学ではすでに 25 件のサーバ証明書を利用しており，年間約 25 万円の予算を削減できたことになる．まさに，サーバ証明書の維持管理コストを削減できたことになる．

今回の学内統一的なサーバ証明書申請・発行システムの構築は，本学における長年の情報基盤整備の延長線上で可能となるものであるが，本学と同規模の国立大学法人の参考になると考える．

一方，前述のように学内には未だ NII 発行のサーバ証明書を利用していない多数のサーバが稼働しており，サーバ証明書の普及に向けた活動が必要である．さらに，NII プロジェクトが期限付きのプロジェクトであることも継続運用上の不安材料である．無用の混乱を避けるためにも，プロジェクト終了後は NII 常設のサービスとして運用されることが強く望まれる[5]．さらに，NII で進められている UPKI 活用のプロジェクトの動向にも注目していく必要がある．本学としても，多方面の共通基盤を利用できる環境整備が必要である[6][7]．

参考文献

[1] 国立情報学研究所：“サーバ証明書の発行・導入における啓発・評価研究プロジェクト”, https://upki-portal.nii.ac.jp/cerpj.

[2] 西村健，佐藤周行：“東京大学におけるサーバ証明書発行体制の構築と課題”, 情報処理学会研究報告，2008-DSM-048，pp.79-84 (2008).

[3] 久長穣，刈谷丈治，三池秀敏ほか：“山口大学における統一認証の導入事例について”， 学術情報処理研究, Vol.10, pp.55-62 (2006).

[4] 久長穣，杉井学，三池秀敏：“大学における迷惑メール対応の在り方～利用者毎のオンデマンド対策の効果”，学術情報処理研究，Vol. 11，pp.5-13 (2007).

[5] 国立情報学研究所：“プロジェクトが発行するサーバ証明書の有効期限の延長について”, https://upki-portal.nii.ac.jp/item/inews/cerpj_updata_validity.

[6] 岡部寿男：“大学間連携のための全国共同電子認証基盤（UPKI）の構想”，http://www.jpgrid.org/event/2005/pdf/WS13_okabe.pdf.

[7] 島岡政基，谷本茂明，片岡俊幸ほか：“大学間連携のための全国共同電子認証基盤UPKIにおける認証連携方式の検討”，電子情報通信学会技術研究報告，IA-106-62, pp. 13-18 (2006).

付録　サーバ証明書申請・発行事務フロー詳細

図３の各手続きの詳細を説明する．（図３及び以下の説明では，登録担当者と副登録担当者を区別せずに登録担当者と記述している．）図３の各手続きの番号順に説明する．

① 鍵ペアの作成　･･･　申請者が申請に必要な鍵ペアとＣＳＲ（Certificate Signing Request）を作成する．NII からは openssl 等の利用を想定したマニュアルが配布されている．

② 申請書作成　･･･　申請者が申請書用紙（Excel ファイル）を申請受付サーバからダウンロードし，所属，氏名，E-Mail アドレス，申請対象のサーバの FQDN（Fully Qualified Domain Name）やＣＳＲ等の情報を記入（入力）する．

③ 申請　･･･　申請者が前項で作成した申請書を申請受付サーバにアップロードする．

④ 確認１　･･･　申請受付サーバは次の 2 点を確認し申請を受け付ける．

ａ）申請者の本人性；本人による申請であることを，ユーザ名/パスワードによる認証（4.2.節で説明）を必要とする学内限定 Web ページで申請書をアップロードしたことで，確認している．確認できない場合は，受け付けない．

b）ドメインの実在性；サーバが DNS サーバに登録されていることを，gethostbyname()関数を用いて，確認している．確認できない場合は，実在しないと判断し受け付けない．

⑤ 申請書受付通知　･･･　申請受付サーバは前項の確認事項２点の確認ができた場合，申請者と登録担当者宛に，申請がなされた旨のメールを自動発信する

⑥ 確認２　･･･　登録担当者が次の 2 点を確認したうえで，申請を仮承認する．

a）申請者の実在性；申請書の所属が実際の所属と一致していることを，学内限定の Web 上で公開されている教職員アドレス一覧（4.2. 節で説明）で確認する．確認できない場合は申請を却下する．

b）サーバの管理責任の確認；申請書の氏名がホスト接続申請書（4.2. 節で説明）の申請者（接続責任者）または運用（技術）担当者と一致していることを，ホスト接続申請書データベースで確認する．（申請者がサーバの管理者であることを，既にセンターにおいて確認済みであるとみなしている．）申請者がホスト接続申請書の申請者（接続責任者）や運用（技術）担当者と異なる場合は，申請者がサーバの管理者であることをホスト接続申請書で確認できるよう再提出してもらう．確認できない場合は，申請を却下する．

⑦ 仮承認　･･･　登録担当者は前項記載の確認ができると，申請受付サーバに仮承認を登録する．（Web ページ）

⑧ 仮承認通知　･･･　申請受付サーバは登録担当者の仮承認登録をきっかけとして，申請者と登録担当者にその旨を通知すると共に，申請者が名札を持ってセンターに来るようメールを発信する．

⑨ センター訪問　･･･　申請者本人が，センターに来訪する．

⑩ 確認３　･･･　申請者来訪時に，登録担当者が，次の 2 点を確認したうえで，申請を承認する．

a）申請者の本人性；窓口で申請者に本人の IC カードの提示を求め，IC カードの氏名が申請書の氏名と一致していることを確認する．さらに，IC カードの顔が申請者の顔と一致していることを，確認する．確認できない場合は，申請を却下する．

b）鍵管理の妥当性；鍵が外部に洩れないよう適切に管理を行っているか，申請者に確認する．確認できない場合は，鍵管理について再考してもらう．また申請書記載の内容で NII に申請してよいか，申請者に最終確認する．確認できない場合は，却下する．

⑪ 承認　･･･　登録担当者は前項記載の確認ができると，申請受付サーバに承認した旨登録する．（Web ページ）

⑫ 承認通知　･･･　申請受付サーバは登録担当者の承認登録をきっかけとして，申請者にその旨を通知する．

⑬ NII 宛送付　･･･　登録担当者は承認した申請書を NII 宛 E-Mail にて送付する．

⑭ NII が申請書受付＆証明書発行　･･･（省略）

⑮ NII が証明書送付　･･･（省略）

⑯ 申請者が証明書インストール　･･･　NII から直截申請者に送付されるサーバ証明書を，申請対象のサーバにインストールして利用を開始する．