UPKI イニシアティブ「サーバ証明書発行・導入における啓発・評価研究プロジェクト」と名古屋大学における事例

平 野　　靖　内 藤 久 資

Ⅰ．はじめに

情報発信・取得を Web 技術を使って行なう機会が多くなってきました。これによって直接窓口に出向かなくても，会議室の予約や書類の提出など，さまざまな申請を電子的に行なうことが可能になっています。このような申請を行なう際には，Web ページ（いわゆるホームページ）で提供される電子申請書に記入するために ID とパスワードを入力する必要があったり，きわめて機密性が高い情報の送受信を行なったりすることも少なくありません。もし通信内容が暗号化されずに Web サーバへ送信され，あるいは Web サーバから受信する場合には，誰かに通信内容を見られてしまう可能性があります。これが原因となって ID とパスワードが漏洩してシステムに不正侵入されてしまったり，個人情報が漏洩してしまったりという被害を引き起こしてしまう危険性があります。そのため，ID とパスワードを入力させたり，個人情報を扱ったりする Web ページでは，SSL（SecureSocketLayer）という技術を使って通信内容を暗号化し，より安全に Web 技術を使えるようにすることが必須となります。そして，このために必要なものが，サーバ証明書です。以下では，サーバ証明書とはどのようなものであるかを説明し，UPKI イニシアティブが行う「サーバ証明書発行・導入における啓発・評価研究プロジェクト」の概要と，名古屋大学での実例を説明します。名古屋大学以外の大学・機関の方で，本プロジェクトによるサーバ証明書の取得をしたい場合には，下記の URL の内容を示しつつ，ご所属の大学・機関のキャンパス情報基盤をつかさどる部局や情報担当理事などにご相談ください。

UPKI イニシアティブ「サーバ証明書発行・導入における啓発・評価研究プロジェクト」
https://upki-portal.nii.ac.jp/item/idata/odatao/cerpj/

Ⅱ．サーバ証明書とは

1．概要

サーバ証明書とはサーバが本物であることを証明したり，通信内容を暗号化したりするための電子的な証明書です。サーバ証明書を使うことによって，ユーザが不正なサーバに接続したり，個人情報が漏洩したりすることを予防できます。サーバ証明書を使っていない Web サーバのアドレスは Web ブラウザに“http:// ～”のように表示されますが，サーバ証明書を使っている場合には“https:// ～”のように表示されるとともに，多くの Web ブラウザでは，南京錠の鍵がかかっているアイコンが表示されます。

2．PKI 証明書の種類

本プロジェクトで発行する PKI 証明書は，パブリックなサーバ証明書であり，これによって学内に設置された Web サーバに，学内あるいは学外からアクセスする際に Web サーバの真正性と暗号化通信を実現します。PKI 証明書は 2 つの観点からそれぞれ 2 種類に分類することができます。以下，それらについて簡単に説明し，本プロジェクトで発行するサーバ証明書がどのようなものであるのかをご説明します。

2.1　サーバ証明書とクライアント証明書

SSL を実現する PKI 証明書には，サーバ証明書とクライアント証明書の 2 種類が存在します。前者はサーバの真正性をクライアントが確認するために用いられ，後者はクライアントの真正性をサーバが確認するために用いられます。Web サーバが不特定多数のクライアントに情報を提供する場合にはサーバ証明書が用いられ，特定のクライアントにのみ情報を提供する場合にはクライアント証明書が用いられることが多いようです。

2.2　パブリック証明書とプライベート証明書

前節と異なる観点で証明書を分類すると，サーバ証明書及びクライアント証明書のいずれにも，パブリックな証明書とプライベートな証明書の 2 種類が存在します。パブリックな証明書はサーバやクライアントとは関係ない機関（そのほとんどは民間機関）が発行し，第三者的な立場でサーバやクライアントの真正性を証明します。また，パブリックな証明書自体が本物であるか否かはインターネットに接続された環境であれば，どこにいても確認できます。一方，プライベートな証明書は特定の組織やグループ内だけで有効な証明書です。例えば，大学内に認証局を設置し，その認証局で発行された PKI 証明書は大学内でのみ，サーバやクライアントの真正性を確認できます。

3．必要性

サーバ証明書を使うことによって，盗聴，なりすまし，改ざんなどの不正行為を防止することが可能になります。したがって，不特定多数の人に対して公開している Web ページで，閲覧のみを許可する場合には，サーバ証明書を導入する必要性はほとんどありません。

以下，盗聴，なりすまし，改ざんについて，簡単に説明していきます。

盗聴　クライアントとサーバの間の通信路（ケーブル，ハブ，ルータなど）を通過する情報を盗み見ることを盗聴といいます。もし情報が暗号化されていない状態（平文）で通信路を通過すると，盗聴者は情報の内容を理解できてしまうため，ID やパスワード，個人情報などが漏洩する危険があります。一方，暗号化されている場合には，盗聴者は情報を見ることはできても，内容を理解することはできないため，漏洩の危険性が大幅に低下します。

なりすまし　目的とする Web サーバに接続していると思っていたら，実はまったく別の人が運

用している偽の Web サーバであったという事態（フィッシング詐欺など）が起こることがあります。これをなりすましといいます。このような事態が起こると，ID やパスワード，個人情報などを盗まれてしまう可能性があります。サーバ証明書を使うことによって，その Web サーバが本物であることを証明できますので，ユーザが安心して Web サーバを利用することができます。

改ざん　情報が平文で通信されたり，電子署名をされずに通信したりすると，通信路の途中で情報を書き換えられてしまう可能性があります。改ざんが行なわれると，ユーザ，あるいは Web サーバに不正に改変された情報が送られてしまい，主にユーザが不利益をこうむることがあります。

4．本人性・実在性確認

サーバ証明書は，サーバの本人性・実在性を証明するために重要な役割を果たします。逆に言えば，適正なサーバ証明書があれば，ユーザは「サーバが適切な管理者によって適切に運用されている」と思うでしょう。もし不適切な管理によって Web サーバが管理され，あるいは不適切に運用されている場合には，ID やパスワード，個人情報の漏洩につながりかねません。

そこで，サーバ証明書を発行する認証局は，サーバ管理者，及びサーバ自体について，本人性の確認と実在性の確認を行います。本人性の確認と実在性の確認は下記の内容を指します。

本人性の確認　なりすましや否認を防止するために，申請者及び申請対象の Web サーバが本人（本物）であることを確認する作業

実在性の確認　申請者及び申請対象の Web サーバが証明書に記載された部局に実在することを確認する作業

実際にサーバ証明書を発行する際に，認証局がどの厳密な確認を行うかは，それぞれの認証局の証明書ポリシによって決められています。

Ⅲ．国立情報学研究所「サーバ証明書発行・導入における啓発・評価研究プロジェクト」

1．概要

国立情報学研究所が中心となって運営する UPKI イニシアティブ[1]では，2007 年度から「サーバ証明書発行・導入における啓発・評価研究プロジェクト」を開始しました［2］。このプロジェクトの主な目的は，

- 大学等のサーバ証明書の普及を推進
- 認証局を用いた研究開発
- 学術機関の Web サーバ信頼性向上
- サーバ証明書の導入・運用ノウハウの共有
- 参加者のサーバに対してのサーバ証明書無償配布

などを通じて，Web サーバ運用責任者がサーバ証明書の使用を体験することによってサーバ証明書の必要性を理解すること，及び国立情報学研究所が認証局を運用することによる評価研究をすることです。本プロジェクトの実施期間中（2007 年 4 月 1 日～ 2009 年 3 月 31 日）は無料でサーバ証明書を取得することができます。なお，Web サーバの実在性や Web サーバ管理者の本人性の確認などを厳密に行なうことによって，商用サービスと同等の保証レベルを実現しますので，無料だからといって心配する必要はありません。

2．参加可能機関

本プロジェクトには機関（大学，大学共同利用機関など）として参加する必要があり，各機関からの参加申請はそれぞれ 1 つのみです。本プロジェクトに参加できる機関は，SINET 加入機関のうち，大学，短期大学，高等専門学校，大学共同利用機関，及びその他文部科学省の独立行政法人等です。

3．発行申請の作業分担

本プロジェクトでサーバ証明書を発行するに当たって，いくつかの異なる立場の人が分担して作業を行います。ここでは，それぞれの立場を説明します。参加申請手続きの流れを図 1 に，サーバ証明書の申請・発行の流れを図 2 に示します。

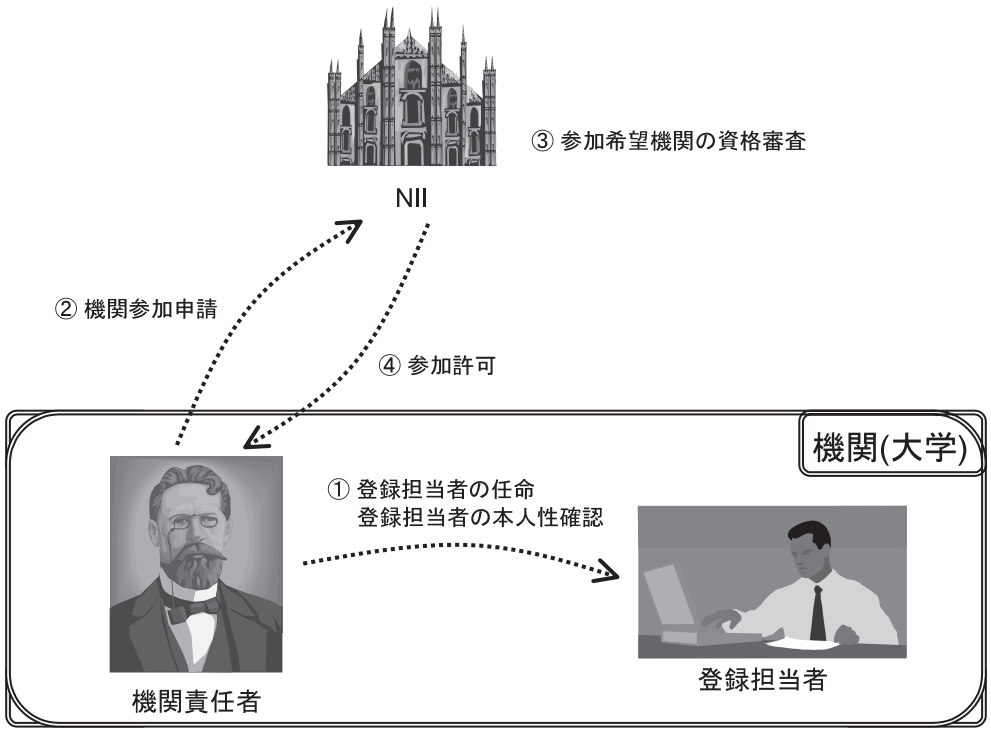


図 1　参加申請

3.1　機関責任者

機関責任者は本プロジェクトの参加機関での責任者であり，参加機関の課長以上，あるいは准教授以上の身分である必要があります。機関責任者は国立情報学研究所学術情報ネットワーク運営・連携本部認証作業部会（以下，部会と言います）との事務連絡を担当する登録担当者及び副登録担当者（以下，登録者と言います）を任命します。その際，機関責任者は，登録者の本人性の確認を行わなくてはなりません。

下記の URL をご参照の上，参加申請を行ってください。

https://upki-portal.nii.ac.jp/item/idata/odatao/entrySheets/

3.2　登録担当者，副登録担当者

加入者（Web サーバ運用責任者）からのサーバ証明書発行申請を受理・審査し，部会が定める S/MIME 証明書を用いてメールに署名を行った上で，申請書を部会に提出します。審査を行うにあたって，下記の事項を確認する必要があります。

加入者の本人性　発行申請書（加入者記入用）が，加入者本人によって申請されたことを確認する。

加入者の実在性　加入者が申請書に記載された参加機関に所属していることを確認する。

ドメインの実在性　加入者サーバの FQDN が，プロジェクトで申請したドメイン名を利用しており，存在する FQDN であることを確認する。

加入者サーバの実在性　加入者から申請されたサーバが申請書に記載された参加機関によって管理されていることを確認する。

実際に本プロジェクトに参加する場合には，これらの作業をどのように行うかを具体的に決定し，部会に申請する必要があります。本プロジェクトの Web ページに具体例がありますのでご参考にしてください。また，もし，電子認証用の全学的な ID 体系があり，学内の IP アドレスの管理者が確認できるのであれば，本稿の後半で述べる名古屋大学の例が参考になるかもしれません。

3.3　加入者（Web サーバ運用責任者）

基本的には，本プロジェクトに参加する機関に所属する正規職員の方で，Web サーバを管理していらっしゃる方であればどなたでも利用申請を行なうことができます。ただし，機関で独自の制限を行う場合もありえますので，機関責任者，あるいは登録担当者等にお問い合わせください。

サーバ証明書を使用しようとする加入者は，サーバ証明書発行に必要となる鍵ペアの作成及び証明書発行要求（CSR）の作成を行ってください。その際，証明書発行要求プロファイルは部会が別に定める方法に従って作成してください。

加入者が遵守すべき事項は下記のとおりです。

● Web サーバを適切に運用すること。
●秘密鍵が加入者（Web サーバ運営責任者）以外に知られないようにすること。
●秘密鍵が加入者（Web サーバ運営責任者）以外に知られるなど，Web サーバの運用に支障を来たす事態が生じた場合には，所属機関が定める窓口などに速やかに失効申請書を提出すること。
●国立情報学研究所，及び所属機関の求めに応じて，証明書利用状況や Web サーバのアクセス状況などを報告すること。

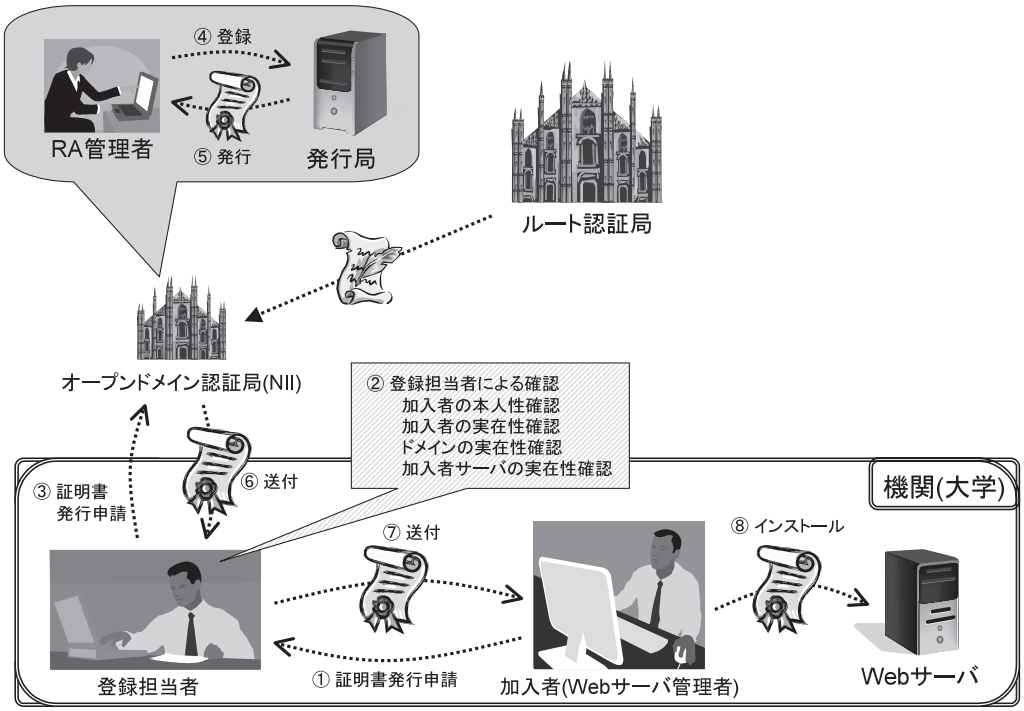


図２　サーバ証明書の申請と発行

3.4　国立情報学研究所学術情報ネットワーク運営・連携本部認証作業部会

部会は，登録者の申請に基づいて申請内容を確認し，本プロジェクトとの適合性を判断した後にサーバ証明書を発行します。サーバ証明書は，S/MIME 署名を利用したメールを用いて部会から加入者，及び登録者へ送付されます。

4．本プロジェクトにおけるサーバ証明書の発行対象となる Web サーバ

本プロジェクトでは，下記のすべての条件を満たす Web サーバに対してサーバ証明書を発行することができます。

●本プロジェクトに参加する機関が所有または管理する Web サーバであること

- https による暗号化通信，あるいは Web サーバの実在証明を必要とする Web サーバであること
- 本プロジェクトに参加する機関に割り当てられた DNS ドメイン以下の FQDN を持つ Web サーバであること
- 本プロジェクトに参加する機関に割り当てられた IP アドレスを持つ Web サーバであること
- Web サーバの利用者が特定少数ではないこと

5．推奨サーバ，推奨ブラウザ

本プロジェクトで発行されるサーバ証明書は下記のサーバ，及びブラウザで適切に認識されることを確認しています。サーバ証明書の利用申請を行なう前に，Web サーバとして用いるプログラム，及び対象とするユーザが使うことが予想される Web ブラウザをご確認ください。

- 推奨サーバ
  - Apache（mod_ssl）
  - Apache-SSL
  - MicrosoftInternetInformationServer5.0
  - MicrosoftInternetInformationServer6.0
  - IBMHTTPServer6.0.2 以上
  - JakartaTomcat
- 推奨ブラウザ
  - NetscapeCommunicator4.78 以上
  - NetscapeCommunicator7 以上
  - MicrosoftInternetExplorer5.5 以上
  - MicrosoftInternetExplorer5.2（MacOS）以上
  - Opera7.6 以上
  - FireFox1.0 以上
  - Safari1.2.2 以上

Ⅳ．名古屋大学 UPKI サーバ証明書発行プロジェクト

1．プロジェクトの概要

名古屋大学では，「名古屋大学ポータル」，「教務システム」をはじめとする種々のウェブサービスがあり，それらサービスの実在性及びセキュリティに対する懸念から，従来よりサーバ証明書を利用して SSL 通信及び実在性証明を行ってきました。また，一方では，情報連携基盤センターのサービスの一環として，「サーバ証明書取得代行サービス」が実施され，サーバ証明書の重要性に対する認識が徐々に深まっていました。

そこで，国立情報学研究所「サーバ証明書発行・導入における啓発・評価研究プロジェクト」

（以下「NII プロジェクト」）が始まるにあたって，名古屋大学としてプロジェクトに参加し，サーバ証明書の利用の重要性を，より一層広めるとともに，サーバ証明書の利用を容易にすべきと考え，情報連携統括本部が中心となって，「名古屋大学 UPKI サーバ証明書発行プロジェクト」（以下「名古屋大学プロジェクト」）を，2007 年 7 月にスタートしました。

名古屋大学プロジェクトのスタート時点での構成は，以下の通りとなっています。

機関責任者　情報連携統括本部長（CIO）
名古屋大学プロジェクト　情報連携統括本部・情報戦略室に設置。
（副）登録担当者　情報連携統括本部・情報サポート部で担当。

このように，名古屋大学では，情報連携統括本部がプロジェクトの責任を持ち，日常的な業務を情報サポート部に依頼しつつ，情報戦略室のプロジェクトとして運営しています。

2．名古屋大学の情報システム環境

以下では，名古屋大学でサーバ証明書の発行審査の方法とアプリケーション構築を解説しますが，それを解説するために，発行審査に関連する名古屋大学の情報システム環境を解説します。

名古屋大学 ID と CAS

名古屋大学では，名古屋大学 ID と呼ばれる統一認証環境を構築しています。この ID は，全構成員（教職員・学生）に配布されます。また，Web アプリケーションのためのシングルサインオン環境として，CAS を採用しています。CAS を利用した Web アプリケーションは，認証をパスしたユーザの属性情報を受け取ることが可能です。

IP アドレス発行責任者と IPDB

名古屋大学のネットワークは，建物ごとのサブネットに分割されています。ユーザが各サブネットで IP アドレスを利用する際には，サブネットごとに（さらに，それを利用する学部・学科単位で）IP アドレス発行責任者が割り当てられています。また，大学内で利用されているネットワーク機器は，すべて IPDB（IP アドレスデータベース）に登録することになっています。したがって，IP アドレス発行責任者は，各ユーザが，実際にサーバの管理をどのように行っているかを知ることができる最も身近な人間であると考えることができます。

3．発行審査の方法

プロジェクトに参加した各機関は，加入者からの発行申請に対して，NII プロジェクトの要請にしたがって，「加入者が正規の教職員であること」，「サーバが適切に管理されていること」及び「サーバが実在すること」を審査しなければなりません。そこで，名古屋大学での審査基準として以下を設定しました。

サーバの実在証明

- 申請されたサーバ証明書の FQDN から，名古屋大学プライマリ DNS サーバを利用して IP アドレスを検索することにより，サーバが実在することを確認します。
- さらに，その IP アドレスが名古屋大学のネットワークに属していることを確認することにより，サーバが名古屋大学内に設置されていることを確認します。

サーバの管理状況確認

サーバの管理状況が適切であることの確認，すなわち，サーバの管理者が責任を持って管理し，秘密鍵の漏洩に対して適切な対策を施していることを確認するために，以下の確認方法を採用しました。

- 申請されたサーバの IP アドレスの「IP アドレス発行責任者」に，「サーバが適切に管理されている」かどうかを問い合わせます。

一方，具体的な「サーバが適切に管理されていること」の内容としては，以下の項目を設定しました。

- 当該ホストの FQDN 及び IP アドレスが CSR に記述されている内容と一致すること。
- 当該ホストが，CSR に記述されている内容と一致するサーバ業務を行っていること。
- 当該ホストにおいて，サーバ証明書の秘密鍵が漏洩しないように対策を講じていること。
- 当該ホストのサーバ証明書を利用するサービスについて，サービス内容が不正に改変されることなく管理されていること。

4．発行審査のためのアプリケーションの構築

上記の発行審査の手続きを円滑に進めるため，名古屋大学では「サーバ証明書発行申請及び管理アプリケーション」を作成し，情報連携統括本部が管理するアプリケーションサーバ上に設置しました［4］。

このアプリケーションを通じて発行申請を行う際には，名古屋大学 ID を用いた認証にパスする必要があります。その時点で，加入者（サーバ証明書申請者）が正当な申請権限を持つユーザであることを審査することができます。

以下が，実際に発行申請を行う際の申請の流れとなります。（実際のウェブアプリケーションの画面は，図 3 ～図 6 参照）

1）発行申請者自身が, OpenSSL を利用し, 秘密鍵及び証明書発行要求書（CSR）を作成します。発行申請者が OpenSSL を利用できない環境の場合には，「情報連携統括本部 IT ヘルプデスク」に赴くことにより，秘密鍵及び CSR を生成することができます。

2）アプリケーションにアクセスし，CSR を投入すると同時に，申請者のメールアドレス及びサーバの IP アドレスを入力します。

3）アプリケーションは，以下の項目をチェックします。

- CSR が正当なものであるかどうかを確認します。
- CSR に記載された FQDN を DNS に問い合わせることにより，ホストが実在し，名古屋大学内に設置された機器であるかを確認します。
- 申請者が入力した IP アドレスと DNS で検索された IP アドレスが一致するかを確認します。

4）IPDB を利用して，該当の機器の IP アドレス発行責任者を検索します。

5）以上にパスした段階で，以下のメールを発信します。

- 申請者には「受理確認」のメールを発信。
- 該当する IP アドレス発行責任者に「サーバの管理状況を問い合わせる」メールを発信。
- 登録担当者に「申請があったことを連絡する」メールを発信。

以上で，申請者の申請の流れは終了します。

一方，IP アドレス発行責任者には，ホストの管理状況を問い合わせるメールが届きます。その中には，申請アプリケーションにアクセスする際の鍵（文字列）が記載されています。管理状況を確認した IP アドレス発行責任者は，アプリケーションにアクセスして，以下の流れにしたがってホストの管理状況を報告します。

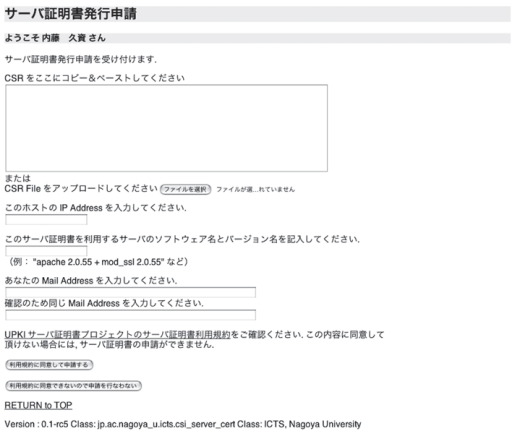
1）アプリケーションにアクセスして，メールに記載された鍵を入力する。

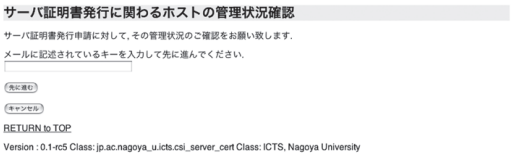
2）アプリケーションは入力された鍵を利用して，どの申請に対応する管理状況報告かを検索します。

3）IP アドレス発行責任者は，「管理が適切かどうか」を選択するボタンによって，管理状況が適切かどうかを報告します。

4）管理状況が適切と報告された場合には，以下のメールを発信します。

- 申請者には「管理状況が確認できた」旨のメールを発信。
- 該当する IP アドレス発行責任者に「サーバの管理状況が確認された」旨のメールを発信。
- 登録担当者に「管理状況が確認できたので，NII に対して発行申請を行う」要請のメー





ルを発信。ここには，NII への申請項目のすべてが記載されているため，このメールのみをもとに NII への申請が可能となっています。

また，アプリケーションには，「サーバ証明書の失効申請」を行う機能や，登録担当者が申請状況を把握するための管理ページ等も付属しています。

しかし，現時点では，アプリケーションにはいくつかの機能が不足していることが分かっています。具体的には，以下の機能が不足しています。

- 申請者自身または登録担当者が申請を取り消す，または，申請内容を変更する機能。
- IP アドレス発行責任者に対して，管理状況の確認願のメールを再送する機能。
- ホスト管理者の登録内容の変更機能。

今後の利用を通じて，不足する機能の追加を計画しています。

5．サーバ証明書の利用状況

名古屋大学では，2007 年 7 月にプロジェクトを開始し，当初の 1 ヶ月は試用期間と考え，情報連携統括本部の関係者のみに，プロジェクトを公開していました。2007 年 8 月からは，全学にプロジェクトをアナウンスし，全学で広くサーバ証明書を利用できる体制に移行しました。

その結果，2007 年 8 月末現在までに申請されたサーバ証明書の総数は 9 枚となっています。

付録

NII プロジェクトのサーバ証明書とその制限

NII プロジェクトが発行するサーバ証明書は以下に述べるプロファイルを持っています。

暗号化強度

署名アルゴリズム　SHA-1,RSA 暗号化

公開鍵暗号アルゴリズム　RSA 暗号化，512 ビット暗号化

通信暗号化アルゴリズム　AES-256

証明書チェイン

中間認証局 1

```
OU=NIIOpenDomainCA,
```

OU=UPKI,O=NationalInstituteofInfomatics,
L=Academia,
C=JP

中間認証局２

OU=SecurityCommunicationRootCA1,
O=SECOMTrust.net,
C=JP

ルート認証局

BulitinObjectToken;ValicertClass1VA,
http://www.valicert.com/

一般に，パブリックサーバ証明書が有効に機能するかどうかは，利用するブラウザにルート認証局の証明書が格納されているかどうかに依存しています。すなわち，NII プロジェクトのサーバ証明書が有効に機能するかどうかは，ルート認証局証明書 BulitinObjectToken;ValicertClass1VA がブラウザのルート認証局証明書のリストに格納されているかどうかによって決まるということです。

Ⅲ．5 節に記載されている推奨ブラウザは，このルート証明書をリスト内に持っていることが確認されています。一方，携帯電話の多くのブラウザでは，この証明書を持っていないため，NII プロジェクトのサーバ証明書を「正しいもの」と認識することができません。したがって，携帯電話のユーザも対象とするウェブサイトを運用する場合には，NII プロジェクトのサーバ証明書を利用することは適切とは言えません。その場合には，主要なベンダが販売しているサーバ証明書を利用することが望ましいと考えられます。

OpenSSL を利用した秘密鍵・CSR の作成手順

Ⅳ．4 節でも述べたとおり，サーバ証明書の発行申請のためには，秘密鍵と証明書発行要求（CSR）を生成する必要があります。ここでは，OpenSSL を利用した秘密鍵と CSR の生成方法について解説します。

秘密鍵の生成

サーバ証明書を利用する際には，証明書自身だけで利用することはできません。なぜなら，サーバ証明書を利用する通信において，クライアントに対してサーバ証明書を提示することになるため，サーバ証明書自身は誰もが可読となっています。したがって，サーバ証明書を利用する際には，それが真正なものであることを保証し，サーバ証明書の内容を復号化するための「鍵」を利用することとなります。それをサーバ証明書に対する秘密鍵と呼びます。秘密鍵は CSR を生成する際に必要とされ，CSR に基づいて発行されたサーバ証明書が真正なユーザによって利用される保証となります。

OpenSSL を用いて，RSA 暗号化による秘密鍵を作成するには以下の方法を取ります。

```
%openssl genrsa -out servername.key -des3
```

（この際，秘密鍵の復号化のためのパスフレーズの入力が求められます。）

これによって，DES3 暗号化された RSA 秘密鍵 servername.key が生成されます。

CSR の生成

秘密鍵を用いて CSR を作成するには以下の方法を取ります。

```
%openssl req -key servername.key -new -out servername.csr
```

この時，秘密鍵のパスフレーズの入力だけでなく，発行要求を行うサーバ証明書の CommonName の入力が求められます。NII プロジェクトのサーバ証明書は，CommonName として，C=JP,L=Academe であり，ST を持たないものと規定されているため，その規定どおりに入力を行います。

これによって，CSRservername.csr が生成されます。

秘密鍵パスフレーズの解除

ウェブサーバでサーバ証明書を利用する際には，ウェブサーバの起動時に，毎回秘密鍵パスフレーズの入力が求められます。実際の運用上は，パスフレーズの入力を毎回行うことは非現実的な側面があるため，秘密鍵のパスフレーズを解除して利用することがあります。

この運用を行う場合には，秘密鍵ファイルが漏洩しないように厳重に管理する必要があります。

```
%openssl rsa -in servername.key -out servername-without-ph.key
```

とすることで，パスフレーズが解除された秘密鍵 servername-without-ph.key を生成することも可能です。

参考文献

[1] https://upki-portal.nii.ac.jp/

[2] https://upki-portal.nii.ac.jp/cerpj

[3] https://repo1.secomtrust.net/sppca/NII/ODCA/NIIODCA-CP-V2.pdf

[4] https://app.icts.nagoya-u.ac.jp/csi_server_cert/

（ひらの　やすし：名古屋大学情報連携基盤センター大規模計算支援環境研究部門，
国立情報学研究所学術ネットワーク運営・連携本部（客員））

（ないとう　ひさし：名古屋大学大学院多元数理科学研究科，
名古屋大学情報連携統括本部・情報戦略室兼任）