政府関係機関事業紹介

UPKI電子証明書発行サービスのご案内

国立情報学研究所　学術認証推進室

1．はじめに

国立情報学研究所（以下、NII）が提供する事業のうち、オンライン認証に関わるものが３つあります。「学認」、「eduroam JP」、そして今回ご説明する「UPKI電子証明書発行サービス」（以下、本サービス）です。本サービスは、高等教育・研究機関に電子証明書を安価かつ迅速に提供することで、学術情報基盤のセキュリティ水準の向上をはかることを目的としております。本稿では、本サービスの概要についてお伝えいたします。

2．UPKI電子証明書発行サービスの概要

平成19（2007）年から平成27（2015）年まで実施した実証実験（以下、旧プロジェクト）で発行されたサーバ証明書は、多くの方々にご利用いただきました。NIIではこの後継となるサービスの提供を検討し、平成27年１月より「UPKI電子証明書発行サービス」の提供を開始しました。旧プロジェクトは実施期間を区切って提供しておりましたが、本サービスはNIIの事業として安定的に提供しています。

安定的に提供し、より安全かつ現状に即した利便性を提供するため、寄せられたニーズとフィードバックを参考にした次のような変更点があります。

有償での提供

旧プロジェクトは、その運営費をNIIの全額負担で提供していたのに対し、本サービスでは利用料という形で、利用機関に一部ご負担いただくことにしました。利用料は機関の規模（常勤の教員・研究者数の合計で決定します）に応じて設定します。また年間定額制を採用しているため、証明書を何枚発行しても、本サービスに登録したドメインに割り当てられたホストであれば追加料金は不要です。年間定額とすることによって、費用変動がなく予算計画が立てやすくなることと、証明書を費用増の心配なく必要な枚数発行できるという利点があります。

複数ドメインでの証明書発行申請

今日、高等教育・研究機関が保持・管理するドメインは、○○.ac.jp 以外にも多数あります。本サービスでは複数のドメインからの証明書発行申請にも対応できるよう、規程の整備を行いました。

発行可能な証明書を拡充

旧プロジェクトでは、サーバ証明書のみが発行可能でした。本サービスではこれに加えて、要望が多かったクライアント証明書とコード署名用証明書も発行可能です。

3．本サービスで発行できる証明書

本サービスで発行可能な証明書について、用途と利点をあわせてもう少し詳しくご説明いたします。

サーバ証明書

本サービスのサーバ証明書は、各ブラウザ提供元から信頼されたルート認証局の下位にある中間認証局から発行され、他の商用証明書と同等の信頼を得ています。よって、本サービスのサーバ証明書をインストールしたサーバは、高水準の安心が保証された証明書を用いたHTTPS通信が可能になります。その利点を列挙します。

- 認証：ブラウザは、正しいWebサイトを開いていて、悪意のあるサイトにリダイレクトされていないことを確認します。
- データ整合性：ウェブサイトとブラウザ間の通信改ざんを防ぎます。
- 秘密保護：悪意ある者がウェブサイトとユーザ間の通信を傍受できないよう保護します。

本サービスのサーバ証明書を利用すると、これらのメリットを享受できます。

また本サービスのサーバ証明書は、Organization Validation(OV)と呼ばれるもので、機関の名称が記

載されたものです。本サービスは、当該機関が実在し、証明書発行対象のドメインを保持・管理していることを審査・確認します。

クライアント証明書

本サービスのクライアント証明書は、大きく分けて２種類あります。まずは「認証と署名」に使える個人認証用証明書（便宜上個人としていますが、部や課などの組織も対象です）、そして「認証と署名」の機能に加え、証明書記載事項に利用者のメールアドレスを付与して発行されるS/MIME証明書です。その利点は下記のとおりです。

個人認証用証明書

- 証明書利用者の認証に使えます。パスワードに変わる、安全で強固な認証に利用できます。
- 証明書利用者の個人名や部課名とあわせて、電子ファイルに署名できます。なりすましと改ざんを防止できます。

S/MIME証明書

- 個人認証用証明書の利点に加えて、電子メールへの署名ができます。証明書利用者の個人名や部課名、メールアドレスを署名に含み、送信元を保証できます。なりすましと改ざんを防止できます。
- 電子メールを暗号化して送信できます（送信相手のS/MIME証明書が必要です）。悪意ある者に電子メールを傍受されても、暗号化されているため中身はわかりません。盗聴を防ぎ、情報漏洩などを防ぐことができます。

コード署名用証明書

コード署名用証明書は、プログラムやアプリケーション、スクリプトへの署名に用いる証明書です。これらの提供元を保証することができます。

本サービスの証明書には必ず機関名が含まれており、これで署名すると、確かにこのアプリケーションを提供しているのは○○大学だということが保証されます。学外に提供する場合のみならず、学内の業務で用いるアプリケーションでも署名を確認すること、確認できない場合はインストールしないことを徹底すれば、より安心・安全に業務を遂行できます。

4．証明書発行体制について

本サービスの特色の１つである、各機関での証明書発行体制構築について説明します。

通常、認証局を運用する電子証明書販売者から証明書を購入するときは、認証局において証明書発行申請の本人性・実在性の確認や審査が行われます。 本人性の確認とは、なりすましでないことの確認を言います。例えばAさんからサーバ証明書の申請があったとき、この申請を出しているのは本当にAさんか確認する必要があります。対面あるいは電子的な手段を用いてなりすましでないことを確認できなければなりません。また実在性の確認とは、Aさんが自組織の所属で間違いないか、実は組織と無関係な人が申請していないか、対象サーバが本当に存在するか、といった確認を言います。

本サービスでは、この確認と審査を、高等教育・研究機関それぞれで実施します。確認と審査を行う者を「登録担当者」と言い、機関ごとに複数名選任できます。登録担当者は、機関ごとに１名のみ設置する「機関責任者」によって任命されます。本サービスに利用申請するときは、必ず機関責任者と登録担当者をおき、証明書発行のための確認と審査体制を構築しなければなりません。

機関それぞれで証明書発行のための審査と確認が実施できるので、本サービスの窓口を通す必要はなく、迅速で効率的、かつ個々の機関の実情に即した厳密な審査が可能になります。さらに、発行処理は登録担当者だけが利用できる「電子証明書自動発行支援システム」を介して行うので、申請から発行までの所要時間はおおむね10分程度です。24時間いつでも証明書が取得できる点も、本サービスの特色と言えます。

5．おわりに

本稿では、NIIが行っているオンライン認証に関わる３つの事業のうち、UPKI電子証明書発行サービスをご紹介しました。サービスの概要と発行可能な証明書について述べ、サービスの特色と言える各機関での証明書発行体制構築についてもご説明しました。

本サービスは、機関内情報基盤のセキュリティ水準の向上に、安価かつ効率的に貢献できるものと考えております。もし関心をお持ちいただけたら、本サービスの利用をご検討いただければ幸いです。本稿で触れなかった詳細についてはWebサイト（https://certs.nii.ac.jp）をご参照いただき、不明点ございましたら、お気軽にサービス窓口 certs@nii.ac.jp までご連絡ください。