導入事例

ENTRUST

足立区の情報システム基盤「プライベート・クラウド型共通基盤」を支える公開鍵認証基盤にエントラスト製品を採用

足立区は「Entrust Authority」を初めとするPKIソリューションを導入し、すべてのシーンで証明書を使うことでクラウド・セキュリティを実現しました。

足　立　区

総人口: 666,540人
世帯数: 317,916
（2010年4月1日現在）

東京23区の北東部に位置する足立区は、運輸業の事業所数が都内で第1位であり、その数は2,400を数え、足立トラック・ターミナルを中心に東京に出入りする物流の一大中継基地を形成している。江戸時代には日光街道と奥州街道の第一宿「千住宿」があり、現在もその風情が残っている。同区は1963年から汎用コンピュータを導入するなど以前からIT投資に積極的で、現在も東京都の中では情報化はトップクラスである。

各業務部門が独自に構築し肥大化したシステム・ハードウェアの統合が課題

足立区は、「システム調達コストおよび総所有コスト（TCO）」の削減と「みえる化・統合化・標準化」をスローガンに、経営改革、業務改革およびシステム改革を進めている。従来のシステムでは、メインフレームをオープン化したものの、各部門で業務の数だけサーバーが存在し、業務端末や業務アプリケーションを個別に導入する状態だった。「当時は、各業務部門が業務システムを独自に構築していたため、SIベンダーもバラバラで、データベースの統合もできず、各システムの合計で100万件近いデータ量がありました。また、各業務システム（C/Sシステム）を構成する物理サーバーが約300台以上あり、区内に17箇所ある区民事務所では、複数業務の端末を利用する必要がありました。これらを何とか統合して経費の削減や場所の圧縮などを行いたい、という考えから、足立区では2008年から区民の視点に立った情報化を推進することを目的とした電子自治体推進計画を立て、共通基盤・ハードウェアの統合をすることにしました。」（政策経営部情報システム課課長 秦章雄氏）。共通基盤の構築にあたっては、足立区が主導的な役割を果たすことで、導入および運用コストの削減を図った。従来のシステム構築においては、ブラック・ボックス化が進みSIベンダーに頼らざるを得ない状況だったが、SIベンダーは、自治体業務に精通していないため、業務システムの都合に業務をあわせる結果となっていた。そのため「できあがった業務システムは職員が使いこなせず、ただ5年に一度のシステム更改をして、業務システムを使い続けていました。そのため、ノウハウの蓄積もできず、コストもかかっていました。また、システム構築の見積もりでは、SIベンダーの情報処理技術者（SE）の工数は人月制でスキルが高い人も低い人も関係なくまとめて人月請求されることや、設計ミスからくる構築期間の延期などにより、導入コストの高騰を招いていました。そこで、足立区では、使い勝手がよく、どのSIベンダーの業務アプリケーションでも動く共通基盤を低コストで構築するため、自治体自らがシステムを設計、詳細なシステム要件を提示して導入コストの削減を図り、業務プロセス管理を取り入れるなどの工夫をしました。」と、同課 システム最適化担当係長 保志野広氏は、コスト削減の取り組みについて語る。こうした経緯を経てプライベート・クラウド型共通基盤のシステム設計が始まったが、足立区では約67万人という膨大な区民の個人情報を扱っており、プライベート・クラウド型共通基盤のシステム構築にあたっては、情報セキュリティの堅牢性も求められている。民間では、低コストの外注先を見つけて業務を外部委託することも可能だが、区民の個人情報を扱う行政機関としては、個人情報保護条例により外出しすることはできないため、プライベート・クラウドをオンプレミスで構築することは必須だった。

PKI認証局を自前で設置

そこで、足立区では、区民生活の向上に役立つシステムを構築するため、内部業務系、学校教育系、住民情報系の3つの分野を載せる共通基盤で構成されるプライベート・クラウド型共通基盤「足立区プライベート・クラウド」の構築を2012年4月より開始した。構築にあたっては、クラウドによる情報セキュリティを担保するため、公開鍵認証基盤（PKI: Public Key Infrastructure）を利用した認証局を自前で作り、総務省の「オブジェクト識別子に係る推奨通信方式の規定に基づく、レベル4のオブジェクト識別子構成要素値（OID）」の認可を受けた。（無 線LAN（EAP-TLS）認証と電子メールの電子署名、使用のため）。「すべての業務サービスで双方向の認証技術を取り入れ信頼できる行政サービス環境を確

図1：クラウド環境セキュリティバリア

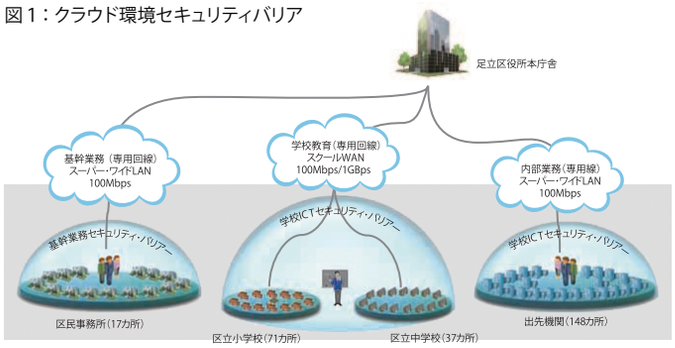
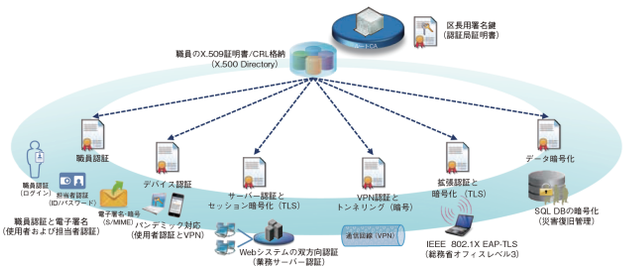


図2：プライベート・クラウドに不可欠な公開鍵認証基盤



立している。PKIによる認証局（CA: Certification Authority）を設置して証明書を発行し配布することで、職員以外の第三者による使用と侵入から業務システムを防ぐことができる。また、証明書に含まれている鍵を利用することで通信内容を暗号化でき、情報漏えいを防止することが可能だ。PKIを採用した経緯について、区のCIO補佐浦山清治氏は次のように語る。「足立区の3つの共通基盤（プライベート・クラウド）は、様々な場所から 教職員と 職員が利用しますが、それは区の施設のどこからでもアクセスできることを意味します。多数の使用者が存在する区のプライベート・クラウドにおいて権限を有している正当なアクセスのみを許可することで、様々なダーク・クラウド（外部）からのサイバー攻撃や内部の情報漏えいを未然に防ぎ、情報セキュリティを高めることができると確信していました。それには、ログインを始めとするすべてのセッションで職員と業務サーバー間での双方向の認証を必要とし Entrust® PKIが最適だったため、ワールドワードで信頼のある Entrust の PKIを採用しました」。PKIによる認証局を設置する場合には、発行する証明書のオブジェクト識別コードを取得する必要があるが、総務省からのオブジェクト識別コードの取得は、自治体初の試みだ。そのような認証局の開設は、手間をかけても情報セキュリティを高めようとする足立区の強い意思の現れだ、と言える。

足立区CIO補佐
飯田 勝吉 氏

政策経営部情報システム課
秦 章雄 氏

政策経営部情報システム課
システム最適化担当係長
保志野 広 氏

独自の認証局による相互認証とアクセス制御機能が充実しているEntrust製品を採用

PKI部分には「Entrust Authority」を初めとするPKIソリューションを採用し、職員認証、教職員認証、デバイス認証、SQL DBの暗号化など認証書を使って行い、やり取りするデータをすべて暗号化している。「個人情報を扱う以上、信頼性が高く実績があるPKI製品が必要でした。エントラスト社の製品は、海外の主要機関（米国連邦政府CIA、FBI、NSA、国際刑事警察機構（ICPO）；通称インターポールや主要銀行など各国の政府機関）にも多数採用されるなど信頼性も高く、大規模公共案件の実績があります。しかも、運用を考えた作りになっており、管理機能が充実しています。他社製品も調べたが、他社は、証明書の発行サービスが主で、対応技術者がいないことや、機能そのものが不足（暗号政策に未対応）しているなど、検討の俎上にのらなかった。独自に認証局を構築して区のクラウド環境のすべてのシーンで認証というセキュリティ・バリアで覆いたい、という我々の要望を満たすのは、日本では唯一エントラスト社のみでした。」と、浦山氏は、エントラスト製品を採用した理由を語る。また、基幹業務基盤システムでは、業務担当者のみが利用できるようにして、それ以外の者が目的外利用できないようにするアクセス制御と権限管理が必須だが、このアクセス制御の点でよい製品をもっているのがエントラスト社だったと、採用した理由を説明する。区内の小中学校108校で教職員3,800名が利用する足立区プライベートクラウドの学校教育基盤システムについては、既に2012年9月から仮想デスクトップで、Microsoft® Office 2010と校務支援システムが稼働しており、内部業務基盤システムもシステム更改順に稼働し始めている。

詳細はこちら：
entrust.com/ja

ENTRUST