

昭和 25 年 6 月 28 日 第二種郵便物認可

電波タイムズ

The Dempa Times

2014 年 (平成 26 年)

第 6367 号

11 月 28 日

金曜日

月 水 金 曜日発行
(祝日休刊)

発行所 株式会社 電波タイムズ社

〒105-0004 東京都港区新橋 5 丁目 20 番 1 号 電話 03(5473)5050 FAX (5473)5051
大阪支社/支局: 中部・静岡 <http://www.dempa-times.co.jp>

南波氏



辻井氏



仙石氏



平成 26 年 11 月 28 日 金曜日 「電波タイムズ」 掲載
(記事のホームページ掲載につきましては「株式会社電波タイムズ社」
の許可を頂いたおります。H26.12.11)

燕市役所で「組織暗号実証実験式」

中央コリドー情報通信研究所など



実験が行われた燕市役所



組織暗号実証実験の様相

新潟情報通信研究所理事長は「私も新ビシネスの創造などを進めているが、今回、辻井教授から依頼があった。燕市長さんにお話ししたところ、快諾をいただいた。NPO法人新潟情報通信研究所の下坂昇事務局長のご協力もあって、今回実験を行うことになった」と述べた。

中央大学研究開発機構は、平成25年度から3カ年計画で、独立行政法人情報通信研究機構（NICT）の委託を受けて、新たな暗号方式「組織暗号」の研究開発を推進している。NPO法人中央コリドー情報通信研究所は、設立以来、ICTによる情報化社会の発展を目的とし、このための大学の研究開発の支援および自治体等の成果の活用による地域の活性化を図る活動を推進。中央大学研究開発推進機構とは過

去に電子投票の研究およびその自治体での応用などで協力してきた。中央大学研究開発機構、中央コリドー情報通信研究所は、組織暗号がいくつかの自治体でその技術の紹介を行ってきたが、新潟県では、2団体とICT関連技術研究などで連携関係にある事業創造大学院大学、NPO法人新潟情報通信研究所が同様な活動を行っており、今回、協力依頼を行った。

近年、個人情報の保護強化が話題になる中、新潟県内の自治体で組織暗号の実証実験を行うこととなり、燕市の快諾を得たことから、市役所と4団体が連携して行ったもの。同市は、住民の個人情報保護と、個人情報の利活用による住民サービス向上の両立に意欲的に取り組んでいる。

従来型では特定の鍵で復号（平文に戻す）できる暗号化情報であるものを、組織暗号は復号することなく、任意の別の鍵で復号できる暗号化情報へ交換（再暗号化）できるもの。つまり、従来方式では、暗号化情報を別の鍵へ切り替えるたびに復号が行われ、個人情報漏えいのリスクが大きくなる。組織暗号は、平文に戻すことなく、暗号化情報を復号できる鍵を切り替えることができ、この暗号方式を組織間の通信に用いることで組織内外での個人情報の配信過程での情報漏えいが防止できる。

実験を行う前に「暗号情報セキュリティの技術と歴史」、組織暗号情報漏えいとマイ・ナンバー導入に備えて」と題して講演を行った辻井氏は同氏が著した「暗号情報セキュリティの技術と歴史」（講談社学術文庫）の内容を中心に説明した。

続いて「組織暗号—自治体での活用可能な業務例—」を近藤健NPO法人中央コリドー情報通信研究所事務局長が説明した。

続いて「組織暗号—燕市想定特定業務への適用案および実証実験の構成・内容紹介—」を才所敏明中央大学研究開発機構研究員が行った。

続いて「組織暗号—燕市想定業務例—」を沼田秀穂事業創造大学院大学学術担当副学長が説明した。

続いて「組織暗号—燕市想定特定業務への適用案および実証実験の構成・内容紹介—」を才所敏明中央大学研究開発機構研究員が行った。

実証実験に入って、実験システム動作説明を庄司陽彦中央大学研究開発機構研究員が行って、実験は成功した。デモシナリオは「保険年金課の管理者は、後期高齢者への医療通知を行うために、後期高齢者医療広域連合の後期高齢者医療担当部門へ医療通知書の提供を依頼したい。後期高齢者医療担当部門の管理者は、保険年金課の管理者より依頼を受けた、医療通知書の提供を行うが、閲覧する人は最小限にしておきたい。保険年金課の担当者は、担当地域の市民への通知業務を行うため、保険年金課の管理者より医療通知書を提供してもらいたい」。例えば、後期高齢者医療担当部門操作では、組織暗号で暗号化を行い、保険年金課の管理者に送る。後期高齢者医療担当部門の管理者は、データを閲覧する担当者を意識せずに暗号化が行えるものだ。また、保険年金課の管理者操作は、組織暗号で鍵の付け替えを行い、各文書を適切な担当者に送るものだ。保険年金課の担当者操作は、組織暗号で復号を行い、適切な担当者のみが復号するものだ。

4団体は今後、実証実験や意見交換を通じ、燕市などの自治体業務における個人情報の取り扱いの現状やマイナンバーへの対応に関する動向を把握、組織暗号の適切な利用に関し知見を深め、自治体での組織暗号の実用化に向け活動を展開する計画だ。

中央大学研究開発機構、事業創造大学院大学、NPO法人中央コリドー情報通信研究所、NPO法人新潟情報通信研究所は、11月21日に新潟県燕市役所で、組織暗号技術を活用した組織暗号実証実験式を開催した。同様の実験は10月に長野県大町市、箕輪町で行われ成功を収めた。燕市の実証実験はこの2市町での経験を踏まえて行われ、地方自治体などが今後、個人情報保護を扱う上で重要なものとしてい

挨拶した南波瑞夫燕市副市長は「わが国はユニキタス社会の実現を目指しているが、実際に情報を使う立場、持っている立場としては、セキュリティ面で個人情報を守るという課題であり、行政として個人情報を活用していかねければいけないが、制約もあってリスクもある。ユニキタス社会の実現において、暗号化技術は重要である。燕市は、情報化社会において、職員は全国どこへ

行っても携帯内蔵が使える、防災無線の整備、アマチュア無線局を持つていたり進んでいる。今回、実証実験に協力することは大変光栄なことである。安心して情報が使える社会に向けて本実験が成果を出せることを期待していること述べた。辻井重男中央大学研究開発機構教授、中央コリドー高速実験プロジェクト推進協議会会長が挨拶した。

仙石正和事業創造大学院大学学長、NPO法人研究開発推進機構とは過