平成１９年度 名古屋大学技術職員研修（情報処理コース）報告

玉置一雄
工学研究科・工学部技術部 電子・情報技術系

はじめに

本研修は，名古屋大学の技術職員に対して，その職務に必要な専門知識および技術を習得させ，技術職員の資質の向上と応用能力の開発および養成を図ることを目的とする. 本年度は 9 月 11 日から 13 日までの 3 日間，IB 電子情報館北館 10 階 創造工学センターオープンエリア東および全学技術センター会議室（共同教育研究施設 : 旧プラズマ研究所）で実施された．日程および講義内容は表 1 に示す.

Web サーバ認証と Ajax（Asynchronous JavaScript + Xml）入門

Web サーバのセキュリティ向上のためのサーバ証明書の必要性について理解を深めるとともに，実際の認証設定を行いサーバ認証およびクライアント認証等を体験した．Web アプリケーションの可能性について Ajax の概要や応用例を紹介して頂き，Ajax プログラミング技術の概要を習得した.

暗号化技術と PKI（Public Key Infrastructure）

「共通鍵暗号方式（DES, Triple-DES, IDEA, RC4, AES）: 暗号化する鍵と復号する鍵に同じ鍵を用いる暗号方式」,「公開鍵方式（RSA, DSS, ECC, DH）:暗号化する鍵と復号する鍵に異なる鍵を用いる暗号方式」,「ハッシュ関数（MD5, SHA-1）: 入力データから固定長のビット列を出力する関数」,「電子署名（Digital Signature）: メッセージを作成したのが本人であるか，内容が改ざんされていないかを検証する技術」,「X.509 証明書 : PKI で使用する公開鍵証明書の標準」,「SSL（Secure Sockets Layer）: 暗号化技術を使用してクライアントとサーバ間で安全な通信環境を提供するプロトコル」,「S/MIME（Secure/Multipurpose Internet Mail Extension）: 電子証明書を利用してメールの暗号化とデジタル署名の付与を実現する」,「PKI（Public Key Infrastructure）: 公開鍵暗号技術を用いた電子証明書を中心とした社会基盤のこと ; GPKI（政府認証基盤）; LGPKI（地方公共団体における組織認証基盤）; JPKI（公的個人認証サービス）; UPKI（大学間連携のための全国共同電子認証基盤)」 等の暗号化技術の基礎を習得した.

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

この目的は, 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料配布等を通じて，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，およ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ある. 名古屋大学におけるサーバ証明書発行申請作成手順について説明があり, 秘密鍵を利用して CSR（サーバ証明書発行リクエスト）を作成し，サーバ証明書の申請をした.

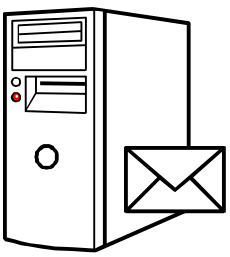

表１　情報処理コースの日程および講義内容

日　程		講　義　内　容
第1日目 9/11 (火)	午前	開講式，オリエンテーション 講義１「名古屋大学における技術支援」 （全学技術センター 山本進一 センター長） 講義２「技術職員向け知的財産の取扱方法」 （産学官連携推進本部 笠原久美雄 教授）
	午後	専門講義１「Ajax がもたらす Web アプリケーションの可能性」 （情報科学研究科 土田貴裕 講師） 専門講義２「PKI の基礎とその可能性」 （情報連携基盤センター 平野靖 准教授） 専門講義３「ネットワーク社会における電子証明書の重要性」 （大学院多元数理科学研究科 内藤久資 准教授） 実習１「研修用パソコン(各自持参)の環境設定」 （情報通信技術系 大川敏生 技術専門員ほか） 懇親会（花の木）
第2日目 9/12 (水)	午前	講義３「SSL について」　（情報通信技術系 大川敏生 技術専門員ほか） 実習２「Web サーバの設定」　（情報通信技術系 大川敏生 技術専門員ほか）
	午後	実習３「サーバ証明書の取得について」 （情報通信技術系 大川敏生 技術専門員ほか） 講義４「名大で行う UPKI について」 （情報連携基盤センター 川田良文 技術専門職員）
第3日目 9/13 (木)	午前	講義５「Ajax プログラミングについて」　（情報科学研究科 土田貴裕 講師） 実習４「体験 Ajax プログラミング」　（情報通信技術系 太田芳博 技術員ほか）
	午後	実習５「体験 Ajax プログラミング２」（情報通信技術系 太田芳博 技術員ほか） 記念写真撮影，閉講式

おわりに

本研修の講義を担当頂いた講師の先生方，企画・運営をして頂いた名古屋大学大学院 事務部・技術部の諸氏に感謝の意を表します.

参考文献

１．相戸浩志著「図解入門よくわかる最新情報セキュリティの基本と仕組み」秀和システム.
２．高橋登史朗著「入門 Ajax 増補改訂版」ソフトバンク クリエイティブ.
３．名古屋大学技術職員研修（情報処理コース）受講者資料.