情報セキュリティ基盤概論 Introduction to information security infrastructure

科目コード(Course Number) 10SMS03401
複合科学研究科 School of Multidisciplinary Sciences　複合科学研究科共通 Common Subjects of Multidisciplinary Sciences　複合科学研究科共通 Common Subjects of Multidisciplinary Sciences
学年(Recommended Grade) 1年　2年　3年　4年　5年
2単位(credit)　後学期 2nd semester
越前　功（ECHIZEN　Isao）　高倉　弘喜（TAKAKURA　Hiroki）　岡田　仁志（OKADA　Hitoshi）

〔授業の概要 Outline〕
情報通信サービスにおける情報セキュリティについて、技術、システム、法制度、経済性について概括する。

Information security technology, service, system, rule, and law give a fundamental framework for providing ICT (information and communication technology) systems and services. This course will introduce information security and give its explain in an ICT governance way.

〔到達目標 Learning objectives〕
情報セキュリティに関する基礎知識と情報セキュリティに関する課題解決の方法論を習得することにより、セキュリティを考慮した情報通信システム、サービスを提供することができるようになる。
Obtain the introductory part of secure ICT service by
(1) Understanding of related information security technology, system and service.
(2) Applying information security technologies to practical problems in providing ICT services.

〔成績評価方法 Grading policy〕
社会の中で必要となる基本知識の習得と課題に対する問題解決能力によって評価する。
Achievement of the aims (1) and (2) will be assessed by questions in the class and a report.

〔授業計画 Lecture plan〕
3名の専門分野の教員による講義と課題設定に対する報告とその評価、研究アドバイスを実施する。

1. ICTガバナンス概論、最新暗号技術、暗号システム設計と攻撃例（越前）
2. ICTサービスに関するセキュリティとプライバシー技術、メディアセキュリティ、デジタル著作権管理技術、Webコンテンツトラストシステム（岡田）
3. ICTアプリケーションセキュリティシステムとサービス、ルールと法律、サイバー攻撃検知と防止技術（高倉）

1. Introduction to ICT governance, modern cryptography and several examples of designing and attacking cryptosystems (Echizen)
2. ICT service-related security and privacy technologies, media security and digital rights management technologies, Web content trust system (Okada)
3. ICT application security systems and services, social rules and laws, Cyber attack detection and prevention technologies (Takakura)

〔実施場所 Location〕
国立情報学研究所(NII)：講義室1（12階1212号室）
NII: Lecture Room 1(12F, 1212)

〔使用言語 Language〕
日本語
English

〔教科書・参考図書 Textbooks and references〕
なし
None
現代暗号概論、公開鍵暗号基盤(PKI)、PKI安全性概念、コンテンツ配信、電子商取引、法と経済学、著作権法、個人情報保護法、電子署名法、情報セキュリティ統一基準、サイバー攻撃検知・防御技術など教科書を特定せずに教材を準備する。
Appropriate textbooks and articles are introduced at the lectures.

〔授業を担当する教員 Lecturers〕
越前功、高倉弘喜、岡田仁志

〔関連URL Related URL〕
URL:

〔上記URLの説明 Explanatory Note on above URL〕

〔備考・キーワード Others/Keyword〕
インターネット、Webサービスなど情報通信技術、情報通信サービスの基本知識を有すること。
Knowledge of ICT system and service is recommended.