セキュリティ技術

Security Technology

担当教員	満保雅浩，岡本健
専攻	リスク工学専攻
分野	リスク共通教育
授業形態	講義
標準履修年次	修士課程および博士後期課程
単位数	2
授業概要	目的：情報の漏えいや改ざん、なりすまし等、現在の情報化社会における種々の問題について、特に暗号・情報セキュリティ分野によって解決できるセキュリティ技術について解説する。 内容：ネットワークセキュリティ、暗号(データ守秘)、電子署名、認証技術
他科目との関連	本講義は「リスク学概論」と「セキュリティの基礎」から派生した内容となっており、これらの科目がセキュリティに対する概念や思想、用語について学ぶのに対し、本講義は実用的な原理や定理、運用などについて学ぶ。また、本講義と「リスク・セキュリティ管理」の学習によって、「リスクと現代社会」への橋渡しとなる役割をもつ。
授業の狙い	現在の情報化社会では、情報の漏えいや改ざん、なりすまし等、種々の事件が多発し、大きな社会問題になっている。現代社会が抱えるこれらの各種問題について理解すると供に、暗号・情報セキュリティによって解決できる各種のセキュリティ技術を学ぶ。
受講生に望む事	受講生は、現在の情報化社会がどのような脆弱性を有しているか、問題意識を持ち、積極的に学習してほしい。またこれらの問題を解決するため、どのような取り組みをすればよいか、受講生自身が考える機会を持ってほしい。

受講生の到達レベル　　暗号に関する安全性について、評価・解析手法を理解する。鍵配送と暗号技術について、体系的な知識を習得する。プライバシ保護技術の代表的な方式を理解する。認証系アルゴリズムが有する脆弱性について理解する。

授業計画　　授業は基本的に講述形式で行う。授業に対して理解度を高めるため、必要に応じて演習問題を提示する。授業は以下の課題からなる。

1.　暗号の危殆化（担当：岡本健）

インターネット社会の安全性を支えている公開鍵暗号系は、計算理論的な安全性に依存しているため、計算機能力の向上や解読アルゴリズムの効率化により、暗号システムの危殆化が発生する。本稿では、暗号解読における最新動向を考察することにより、長期利用に耐えうる暗号鍵の推奨サイズについて解説する。

2.　鍵配送と暗号技術（担当：満保雅浩）

複数の利用者間で暗号通信する場合、送信者・受信者の双方が暗号鍵を利用するため、鍵管理の負荷が大きくなる。この問題を解決する一手法として、木構造を用いた鍵管理方式について説明する。通信頻度情報を用いた効率の良いアルゴリズムについて解説する。

3.　プライバシ保護技術（担当：岡本健）

暗号・署名を用いたプライバシの保護技術について概説する。特に最近、実社会に有益な機能として注目されている匿名署名に関して、オブリビアス署名を例にして解説する。また、匿名性の強度について説明した後、情報理論的な安全性を有する匿名署名の構築手法について説明する。

4.　不正アクセス防止（担当：満保雅浩）

最初にインターネットにおける不正侵入の現状について説明する。次に Windows 系 OS と UNIX 系 OS が採用しているパスワード方式について説明し、不正侵入とパスワード認証との関連性について講述する。

教科書	教科書は特に指定しない。必要に応じてプリントを配布する。
参考書	1. 岡本栄司; 暗号理論入門(第 2 版), 共立出版, 2002 2. Menezes, P. Oorschot and S. Vanstone; Handbook of Applied Cryptogrpahy, CRC Press, 1996 その他の教材は、必要に応じて配布する。
成績評価	各課題に対するレポート(50%)、及びすべての講義の最後に行われる期末試験(50%)によって評価する。
関連情報	なし。
関連科目	リスク学概論 セキュリティの基礎 リスク・セキュリティ管理 リスクと現代社会