Information Security

Special Subjects
Elective 2 credit

MORI, Takuo

1. Course Description

Information security covers broad fields, from the cryptography to practice information networks or systems. In this course, we aim at systematically understanding the way to deal with security problems which may happen in practical information systems, from basic.

This course relates to the diploma policy 1 of the division of the integrated science and engineering, graduated school of Teikyo University.

2. Course Objectives

The goal of this course is that students master the following abilities;

Students can explain how to prevent from unauthorized accesses, and show basic countermeasures against unauthorized accesses.
Students can explain how to protect Web-applications, and show basic countermeasures against attack to the Web-applications.
Students can explain the operation principles of malware, and show basic countermeasures against malware.
Students can explain the operation principles of intrusion detection/protection systems(IDS/IPS) and, how to introduce IDS/IPS.
Students can show basic access control techniques and choose appropriate ones according to the situation.
Students can explain information security protocols.
Students can explain foundations of constructing/operating information systems.
Students can show outlines basics of Information Management Systems.
Students can explain new trends in information security technology.
Students can explain and write basic cyber-security programmings.

3. Grading Policy

Grading policy: Mid-term report(50%), Final-report(50%)

The way of feedback;
Answers for questions or feedback for the contents of class and reports will be given in a class, through LMS.

4. Textbook and Reference

Textbook
佐々木良一監修、電子情報通信学会編　現代電子情報通信選書「知識の森」ネットワークセキュリティ

<Comments>
訂正無し
　オーム社、ISBN-13: 978-4274215179
Reference
Justin Seitz著, 青木 一史 訳, 新井 悠 訳、一瀬 小夜訳、岩村 誠訳、川古谷 裕平訳、星澤 裕二訳　サイバーセキュリティプログラミング ―Pythonで学ぶハッカーの思考
　オライリージャパン、
ISBN-13: 978-4873117317

5. Requirements(Assignments)

Before each class, materials related to the class will be published through LMS. Students should download them to their own devices or print them to make it possible to refer to or to take notes.
Students should read these materials and grasp what they do not understand and they understand in an hour.
After each class, student should review the class through tests on the LMS in half an hour.

6. Note

In order to earn credits of this course, students must submit two reports.

Students should have basic (at least, undergraduate level) knowledge of the following source,
Mathematical logic, Algebraic systems, Elementary number theory, Complexity theory, Network technology, Programming language, Database theory.

After taking this course, students should take Quantum Information Science, and Advanced Information Security in the Doctor's Program.

7. Schedule

[1] A trends in network security
[2] Unauthorized access1 -Password Cracking-
[3] Unauthorized access2 -Basics of Web-application security-
[4] Unauthorized access 3 -Injection, XSS-

[5] Unauthorized access 4 -CSRF, Buffere-overflow, Drive-by-download-
[6] Malwares
[7] Intrusion detection/protection systems.
[8] Access control1 -An introduction to the access control-
[9] Access control2 -Identification, Fire wall-
[10] Information security protocols
[11] Construction/Operation of information security systems
[12] Information security management systems
[13] New Trends in network security1 -APT/IPv6-
[14] New Trends in network security2 -Threat to smart phones/tables-
[15] Cyber security programming