

科 目		必・選	担 当 教 員		学年・学科			単位数	授 業 形 態				
情報セキュリティ (Information Security)		選	村田 充利		5 年生 電気情報工学科			1	前期 週 2 時間				
授業概要		インターネットの爆発的な普及し利便性が向上した反面、ネットワーク上での種々のいたずら、情報漏洩、犯罪なども増加傾向にある。この授業では、ネットワークにおいてどういう脅威やリスクがあり、それらにどのように対処するかといったセキュリティの基本的な知識を学ぶ。											
到達目標		基本情報技術者試験および情報セキュリティスペシャリスト試験のセキュリティ関連問題を 6 0 % 解くことができる。											
評価方法		定期試験 6 0 %、課題・小テスト 4 0 % で評価する。											
教科書等		情報セキュリティ、情報セキュリティ標準テキスト編集委員会編、オーム社											
内 容										学習・教育目標			
第 1 週	オリエンテーション、情報セキュリティの基礎								C-2				
第 2 週	不正攻撃 (1)								C-2				
第 3 週	不正攻撃 (2)								C-2				
第 4 週	ウィルス (1)								C-2				
第 5 週	ウィルス (2)								C-2				
第 6 週	ファイアウォール (1)								C-2				
第 7 週	ファイアウォール (2)								C-2				
第 8 週	暗号 (1)								C-2				
第 9 週	暗号 (2)								C-2				
第 1 0 週	認証 (1)								C-2				
第 1 1 週	認証 (2)								C-2				
第 1 2 週	監査 (1)								C-2				
第 1 3 週	監査 (2)								C-2				
第 1 4 週	情報セキュリティポリシー (1)								C-2				
第 1 5 週	情報セキュリティポリシー (2)、国際標準・国内標準と関連法規								期末試験	C-2			
第 1 6 週													
第 1 7 週													
第 1 8 週													
第 1 9 週													
第 2 0 週													
第 2 1 週													
第 2 2 週													
第 2 3 週													
第 2 4 週													
第 2 5 週													
第 2 6 週													
第 2 7 週													
第 2 8 週													
第 2 9 週													
第 3 0 週													
(特記事項)			JABEE と の 関 連										
			JABEE	a	b	c	d1	d2a) d)	d2b) c)	e	f	g	h
			本校の学習 ・教育目標	A	A	C-1	C-1	C-2	B	B	D	C-3	B
								◎					

1. 合格ラインについて、特に記載の無いものは、60点以上を合格とします。

2. 定期試験について、特に記載の無いものは、評価配分を均等とします。(【例】年4回定期試験を実施した場合の各定期試験の評価配分は、特に記載の無いものは、25%ずつとなります。)

【第1週】オリエンテーション、情報セキュリティの基礎

ここでは、情報セキュリティの必要性やその対策の目的、機能および進め方など、情報セキュリティの全体について学習する。

【第2～3週】不正攻撃

不正攻撃とは、悪意をもって電子データや情報システムに、許可されていないアクセス（盗聴）、変更（改ざん）、破壊などを行う行為である。ここでは、不正攻撃の各種方法（ポートスキャン、トロイの木馬、バックドアなど）についての基礎知識や対策法について学習する。

【第4～5週】ウィルス

ウィルスは、自身単独のプログラムとしては存在せず、他のファイルの中に複製を埋め込み増殖するものである。昨今は、ネットワークを介して自動感染するワームタイプのものが増えている。ここでは、これらのウィルスに関する基礎知識を学習し、その対策法について考える。

【第6～7週】ファイアウォール

ファイアウォールは、学校などのLANと外部のインターネットの接続の間に設置し、外部からの不正アクセスやウィルスの侵入を防ぐ装置である。ここでは、ファイアウォールの仕組みや構成、運用方法について学習する。

【第8～9週】暗号

昨今、ネットワーク上を流れるデータ（メールなど）の盗聴や改竄、なりしませんが問題となっている。これを防ぐ方法として、データの暗号技術がある。暗号技術は、共通鍵暗号方式と公開鍵暗号方式の2つに大別される。ここでは、この暗号化技術について学習する。

【第10～11週】認証

認証とは、利用者が情報（データ）にアクセスする権限を有するかどうかを検証する技術（利用者認証）と、メールやサービスの内容が正当かどうかを証明する技術（デジタル署名、デジタル証明書など）である。ここでは、これらの認証技術について学習する。

【第12～13週】監査

監査とは、セキュリティ対策に問題がないかチェックし、不備が発見された際に対策を勧告する作業である。ここでは、監査の方法と対策ツールについて学習する。

【第14～15週】情報セキュリティポリシー

国際標準・国内標準と関連法規

情報セキュリティポリシーとは、情報を保護するために組織のメンバーが守るべき方針のことである。

ここでは、情報セキュリティポリシーの考え方や制定法について学習する。

情報セキュリティに関して、国際的あるいは国内的に色々の基準や法規が定められている。

ここでは、これらの基準や法規について学習する。

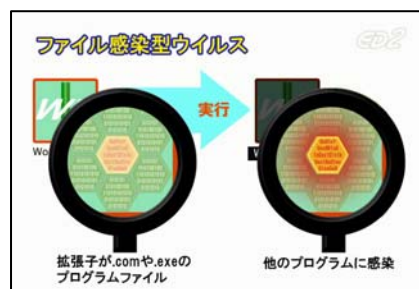


図1. ファイル感染型ウィルス

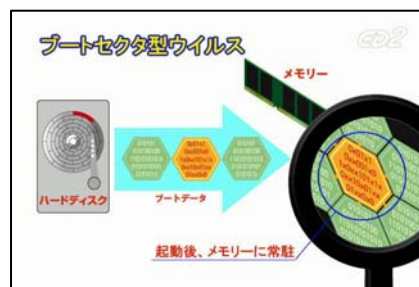


図2. ブートセクタ型ウィルス

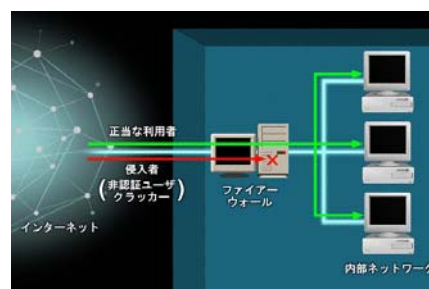


図3. ファイアウォール

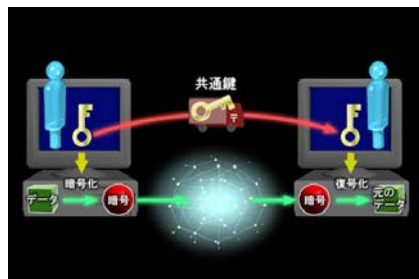


図4. 共通鍵暗号方式

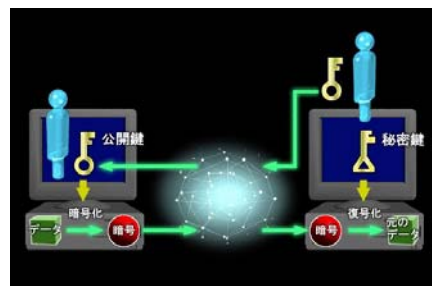


図5. 公開鍵暗号方式

【出典】

図1～2：「情報機器と情報社会のしくみ素材集」

<http://www.kayoo.info/jyohou-kiki/index.html>

図3～5：IPA「教育用画像素材集サイト」

<http://www2.edu.ipa.go.jp/gz/>