講義科目名称： 情報セキュリティ論　　科目コード： 51370

英文科目名称： Information Security Theory and Practice

開講期間	配当年	単位数	科目必選区分
1・2年前期	1・2	2	選択
担当教員			
大石　和臣			
添付ファイル			

講義概要	情報セキュリティは現代社会に不可欠である．本講義では情報セキュリティにおけるいくつかの技術を取り上げ，その理論と応用について輪講形式で学ぶ．候補技術は，暗号，暗号プロトコル，ソフトウェア保護，組込みシステムセキュリティ等であるが，これらに限定されるわけではない．
授業計画	1　イントロダクション 大学院のカリキュラムにおける本講義の位置づけを説明する．講義概要をシラバスを使って説明する．取り上げる技術について受講生と意見交換をしたうえで決定する．AL①．次回以降の準備を行う． 準備：取り上げたい技術について自分の意見をまとめてくる． 課題：次回の発表の準備をする（論文等を読み，理解し，プレゼン資料を作成する）． 2~5　トピック1 （例，公開鍵暗号） 公開鍵暗号の場合，特定の公開鍵暗号方式の理論を論文を読み進めながら理解する．次に，その方式を自分で実装する，あるいは実装されたソフトウェアライブラリ等を入手して，どのようにプログラミングされるのかを理解し，使い方を学習する．AL①，AL③． 準備：論文等を読み，理解し，プレゼン資料を作成する． 課題：次回の発表の準備をする（論文等を読み，理解し，プレゼン資料を作成する）． 6~10　トピック2 （例，ソフトウェア保護） ソフトウェア保護の場合，既存のソフトウェア保護方式を論文を読み進めながら理解する．次に，その方式を自分で実装する，あるいは実装されたソフトウェアライブラリ等を入手して，どのようにプログラミングされるのかを理解し，使い方を学習する．AL①，AL③． 準備：論文等を読み，理解し，プレゼン資料を作成する． 課題：次回の発表の準備をする（論文等を読み，理解し，プレゼン資料を作成する）． 11~15　トピック3 （例，組込みセキュリティ） 組込みセキュリティの場合，既存の組込みセキュリティに関する論文を読み進めながら理解し，どのような課題や解決方法があるのかを理解する．次に，解決方法が提案されているならば，その方法を理解し，実装する．解決方法が不十分な場合は，その改善について検討する．AL①，AL③． 準備：論文等を読み，理解し，プレゼン資料を作成する． 課題：次回の発表の準備をする（論文等を読み，理解し，プレゼン資料を作成する）． 15　課題レポートの出題 全15回の講義で学んだ内容について，それぞれのトピックを要約したレポートの提出を求める．
授業形態	講義，討論，演習（輪講形式のため，受講生は毎回発表を行い，内容について他の受講生および教員と意見交換をして，演習を行う）． アクティブラーニング：①:15回,②:0回,③:14回,④:0回,⑤:0回,⑥:0回
達成目標	1. 対象技術の理論を理解し，説明できる． 2. 対象技術の応用を理解し，説明できる． 3. 対象技術の位置づけを理解し，説明できる．
評価方法・フィードバック	毎回の発表の内容50%，課題レポート50%で評価する．授業中の質問に対する理解度を見てフィードバックする。
評価基準	秀：100~90 優：89~80 良：79~70 可：69~60 不可：59~0
教科書・参考書	教科書は指定しない．取り上げる内容に即した書籍，論文，プリントを指定・配布し，それを基に講義を進める．
履修条件	符号・暗号理論1，符号・暗号理論2，情報セキュリティCを全て履修済みであること（成績に条件はつけないが，良い成績であるほうが望ましい）．プログラミング言語Cのプログラミング経験およびアセンブリ言語の基礎知識を有すること．
履修上の注意	講義は輪講形式で進めるため，受講生は毎回発表，意見交換，演習を行う．その負荷は小さくないので，適切な負荷（各回における受講生1名の発表と質疑応答の時間が30分以内）となるように受講生数は少なくとも3名以上が望ましい．受講生数が2名以下の場合は受講者と事前に面談して講義内容を変更する必要があるため，第1回の講義より前に履修希望を担当教員に必ず伝えること．
準備学習と課題の内容	符号・暗号理論1，符号・暗号理論2，情報セキュリティCの内容を復習しておくこと．
ディプロマポリシーとの関連割合（必須）	知識・理解:40%,思考・判断:30%,関心･意欲:10%,態度:10%,技能・表現:10%