

2013年度 後期		リフレクションペーパー					
学科名	情報学科						
科目名	暗号とセキュリティの理論						
科目区分	専門科目	科目コード	4507	単位数	2	開講時期	2年次後期
必修・選択の別	必修科目(ネットワークコース)／選択科目(ソフトウェアコース)						
担当者	山崎重一郎						
授業の到達目標(シラバスから)	<ul style="list-style-type: none"> ・共通鍵暗号、公開鍵暗号、デジタル署名、認証プロトコルについて説明できる。 ・利用者認証技術と公開鍵暗号基盤を説明できる。 						
内容	9月21日 9月28日 10月 5日 10月12日 10月19日 10月26日 11月 9日 11月16日 11月30日 12月 7日 12月14日 12月21日 1月11日 1月18日 1月22日	第1回: 導入講義－学習教育目標、講義の進め方、評価方法の説明。 第2回: 共通鍵暗号－ブロック暗号 第3回: 共通鍵暗号－強度評価 第4回: 共通鍵暗号－ストリーム暗号 第5回: 公開鍵暗号とデジタル署名の基礎理論 第6回: 公開鍵暗号－公開鍵暗号の概要 第7回: 公開鍵暗号－素因数分解ベースの方式 第8回: デジタル署名の概要 第9回: ハッシュ関数 第10回: 公開鍵認証基盤、証明書の失効 第11回: IPSEC 第12回: TLSとS/MIME 第13回: プラインド署名と情報ハイディング 第14回: 定期試験 第15回: 定期試験の解答と講評					
成績評価基準	定期試験の成績(70%)と授業中に随時行う小テスト(30%)の成績を総計して評価点とする。						
授業到達目標の達成度	ほぼ達成できた						
反省点	理解できましたかの設問で、評価2が4%いたので、その学生を救う方法を考える。また、履修後の脱落者が減らしたい						
来年度の計画	今年も内容をかなり刷新したが、新しい内容を増やしたい						
授業評価アンケートに対するコメント	全体に良くなった						
履修登録者数	37名	定期試験 受験者数	25名	合格者数	24名	合格率	96%