2016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	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）	・共通鍵暗号、公開鍵暗号、ディジタル署名、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。				

日程と内容	
9月21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。
9月28日	第2回：共通鍵暗号－ブロック暗号
10月 5日	第3回：共通鍵暗号－強度評価
10月12日	第4回：共通鍵暗号－ストリーム暗号
10月19日	第5回：公開鍵暗号とディジタル署名の基礎理論
10月26日	第6回：公開鍵暗号－公開鍵暗号の概要
11月 9日	第7回：公開鍵暗号－素因数分解ベースの方式
11月16日	第8回：ディジタル署名の概要
11月30日	第9回：ハッシュ関数
12月 7日	第10回：公開鍵認証基盤、証明書の失効
12月14日	第11回：IPSEC
12月21日	第12回：TLSとS/MIME
1月11日	第13回：サイドチャンネル攻撃
1月18日	第14回：SSLの脆弱性
1月22日	第15回：マイナンバー制度と個人番号カード

成績評価基準				
定期試験	70%	実技		
臨時試験	30%	部外評価		
報告書・レポート		プレゼンテーション		
課題				
演習		計	100%	

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1名だけになった
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	8.1で概ね好評であった。

履修登録者数							
	31 名	定期試験受験者数	27 名	合格者数	24 名	合格率	89%