履修コード/科目名称	142521 / 情報セキュリティＢ		
開講年度・期	2020年 後期	開講曜日・時限	金曜日 3時限
単位数	2		
付記	◎予		
主担当教員氏名(カナ)	西村　和夫（ニシムラ　カズオ）		
副担当教員氏名(カナ)			

授業概要	情報セキュリティに関する法制度，アクセス制御および暗号の技術について理解します． (1) 不正アクセス禁止法，個人情報保護法，刑法，著作権法などの法律を学びます。 (2) アクセス制御の概念と方式を理解します（ファイル属性を変更する演習あり）． (3) 暗号によって達成可能な目標および暗号技術を理論的に理解します（推理小説“踊る人形”の暗号を解読する実習あり）．特に，公開鍵暗号の RSA 方式を理解します．そのうえで，ネットワーク上で情報セキュリティを実現する方法および認証局の必要性について理解します．いくつかの暗号プロトコルによる応用も学習します．
到達目標(ねらい)	情報セキュリティは新しい分野であり，ほとんどの受講者に基礎知識がないので，覚えるべき用語や内容が多くあります． ¶ 説明できるようになるべきこと： 主要な法規の概要，アクセス制御行列の概念，アクセス制御リストの方式と機能，アクセス制御の３手法，暗号系の基本的な用語，暗号解読における３段階の状況，共通鍵暗号系の概念，単換え字式暗号，転置式暗号，解読不可能な暗号，AES の外部仕様，公開鍵暗号系の概念，RSA 方式の概要，認証局の機能． ¶ 知るべきこと： OSS のライセンス方式についての基本的な事項，物理的なアクセス制御方式，ファイルパーミッション，世界の諜報機関の現状，暗号の定義，暗号解読の成功を秘匿した例，各種の古典的暗号の暗号化と復号のしかたおよび解読のしかた，ブロック暗号の利用モード，署名つきの暗号文の作り方，暗号技術を使ってできることの例，ハッシュ関数，　一方向性関数の概念，チャレンジ応答プロトコル，電子マネーの概要，TLS の概要，公開鍵基盤，量子暗号． ¶ その他： 各暗号方式の鍵の総数が示せる．公開鍵暗号系と公開鍵認証系で実現できることが示せる．秘匿と認証において誰のどの鍵を使うかが区別できる．

授業スケジュール				
第 1 回	授業の計画・内容	ガイダンス		
	準備学習（予習・復習等）	予習： シラバスの閲覧．★ YeStudy への登録 → 「成績評価の方法」の閲覧 → 授業用 Web ページの概観． 課題： ガイダンスの内容		60分
第 2 回	授業の計画・内容	法律による保護（情報セキュリティに関する国内法規）		
	準備学習（予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 法律による保護（1）		60分
第 3 回	授業の計画・内容	法律による保護（刑法，不正アクセス禁止法，個人情報保護法，著作権法）		
	準備学習（予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 法律による保護（2）		60分
第 4 回	授業の計画・内容	オープンソースソフトウェア（OSS）とライセンス，GFDL		
	準備学習（予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： オープンソースソフトウェア（OSS）のライセンス		60分
第 5 回	授業の計画・内容	アクセス制御（アクセス制御リスト，パーミッション），ファイル属性の変更（実習）		
	準備学習（予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： アクセス制御		60分
第 6 回	授業の計画・内容	暗号の概要と用語		
	準備学習	予習： 授業用 Web ページを閲覧し，到達目標を確認		

		（予習・復習等）	する． 演習： 暗号の概要と用語	60分
	第 7 回	授業の計画・内容	共通鍵暗号（転置式暗号，単換え字式暗号）	
		準備学習 （予習・復習等）	リポート（課題授業）： 共通鍵暗号	90分
	第 8 回	授業の計画・内容	“踊る人形”の解読（実演・実習），多表式暗号	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： “踊る人形”の解読	60分
	第 9 回	授業の計画・内容	暗号解読（鍵の総数，単換え字式暗号の文字頻度，多表式暗号の周期，転置式暗号の連接確率，解読不可能な暗号），暗号解読技術の応用	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 暗号解読	60分
	第 10 回	授業の計画・内容	ブロック暗号の利用モード，現代的な共通鍵暗号 AES	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： ブロック暗号	60分
	第 11 回	授業の計画・内容	公開鍵暗号（剰余演算）	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 剰余演算	60分
	第 12 回	授業の計画・内容	公開鍵暗号（RSA方式）	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 公開鍵暗号	60分
	第 13 回	授業の計画・内容	認証（電子署名，署名つきの暗号文），暗号技術を使ってできること	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 認証，暗号技術を使ってできること	60分
	第 14 回	授業の計画・内容	ハッシュ関数，一方向性関数	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： ハッシュ関数，一方向性関数	60分
	第 15 回	授業の計画・内容	暗号プロトコル（チャレンジ応答プロトコル，電子マネー，SSL/TLS），公開鍵基盤，認証局	
		準備学習 （予習・復習等）	予習： 授業用 Web ページを閲覧し，到達目標を確認する． 演習： 暗号プロトコル，公開鍵基盤，認証局	60分

履修上の留意点等	履修に際して予備的な知識は必要としません．反転授業を取り入れる予定です．	
成績評価の方法	51 %	試験
		レポート
	28 %	小テスト
	14 %	平常点
	3 %	課題（実習）
	4 %	課題授業
	毎回，YeStudy を通して何らかの演習や理解確認テストをしてもらいます．	
教科書/テキスト	[1] 授業用 Web ページ： https://www.komazawa-u.ac.jp/~kazov/Nis/lecture/security/index.html#B	

	[2] YeStudy (https://yestudy.komazawa-u.ac.jp/)
参考書 ▸ 図書館蔵書検索	[3] 情報処理推進機構 セキュリティセンター, 情報セキュリティ読本 五訂版 — IT時代の危機管理入門, 実教出版, 2018. (600円). ISBN 978-4-407-34775-3. [4] 結城浩, 暗号技術入門 — 秘密の国のアリス, 第3版, ソフトバンクパブリッシング, 2015. (3000円). ISBN 978-4-7973-8222-8.
学生による授業アンケート結果等による授業内容・方法の改善について	昨年度の授業も定刻どおりに行われ, 休講もありませんでした. アンケートによれば, 授業にはシラバスの内容が反映され (選択肢5+4で 92%), 受講を決める際に役に立っているそうです. 進度はほぼ適切であり (同 68%), 資料は授業内容を理解するうえで効果的だった (80%) ということです. 担当教員の熱意 (92%), 話し方 (96%), 板書やスクリーンの文字は良好 (84%) であり, 静粛な環境づくり (84%), 意見や質問への対応 (48%) は良好でした. 内容の理解 (56%) ・興味 (76%) ・達成 (72%) については, 興味も理解もほどほどという結果でした. 自由記述欄において, 良かった点には「授業用のサイトが整理されていて、どこを読むべきかわかりやすい。」などがありました. 悪かった点には, 「出席を早く取りすぎる」があったので, 途中から点呼の終了が授業開始４分後になるようにしました. 今年度は, 定期試験以外の配点をさらに増やします.
関連リンク	[過去の達成度] - 知識の増加量 (アンケートに基づく)
実務経験がある教員による授業科目	
アクティブラーニング型の授業科目	毎回 授業内容の確認テストを行い, それを評価します. 第５回には, ファイル属性の変更の実習をします. 各自の Web ページを簡便に作成し, それが他人から閲覧できるように, パーミッションの変更をします. 第８回には, 古典的な暗号の解読をします. 推理小説であるシャーロックホームズの“踊る人形”を科学的に解読して, 単換え字式暗号の解読が文字の出現頻度に基づき, 言語の特徴に依存することを体験します. この実習を通じて, 暗号文が解読できるのと, 鍵が判明するのとは異なるということを体験してもらいます.