付録1

CySec

国際化サイバーセキュリティ学　特別コース／シラバス

科目名	1　PF	2　CD	3　IN	4　DF	5　MG	6　DD
	基盤技術		インシデントレスポンス、人的、社会問題		情報システムと制度デザイン	
	サイバーセキュリティ基盤	サイバーディフェンス実践演習	セキュリティインテリジェンスと心理・倫理・法	デジタル・フォレンジック	情報セキュリティマネジメントとガバナンス	セキュアシステム設計・開発
項目＼担当者	岩井	八槇	安田	佐々木	安田	安田
科目概要	サイバーセキュリティを深く理解する前提として、アクセス制御・運用セキュリティ技術・暗号技術・OS仮想化技術・クラウド管理・ユビキタスセキュリティ・ハードウエアに関する脆弱性などの共通基盤技術に関して、知識と演習を通じて深い理解を得る必要がある。 本講義では、セキュリティ基盤技術を網羅的かつ系統的に学習すると伴に最新事例を演習を通じて実体験すし、セキュアな情報システム構築の知識と基礎力を養う。	ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、およびアクセスネットワークについての、セキュリティ技術について深く学ぶ。これら、ネットワークシステムへの攻撃手法やその脅威、およびそれらの対策について議論する。 また、それらの知識をもとに、セキュアなネットワークシステムを、デザインする手法を身につける。セキュリティ技術・攻撃対策・ネットワークデザインのそれぞれについて演習を実施し、セキュアな情報システムの設計・運用能力を養う。	セキュリティインシデントは、近年多岐にわたる知識により、その予防と発生後の対策が必要になって来ている。 本講義は、インシデントの犯罪心理学・行動学・最新の手法・ログや統計データの解析の概論を学ぶ。また関連する倫理規定や法を学び、インシデントレスポンスの手法を、グループワークにより実践的に、学習していく。	捜査や裁判（刑事・民事）に必要な情報（たとえばサーバへの侵入経路やメール発信者の真偽など）を、情報処理技術を用いて明らかにする技術や学問であるデジタルフォレンジックは、CIO補佐、あるいはCISO補佐にとって今後非常に重要な技術になっているが十分な講義が行われていない。 捜査や裁判（刑事・民事）に必要な情報を、情報処理技術を用いて何が行われたかを明らかにする、技術や学問であるデジタルフォレンジックの考え方や基本技術を習得するとともに、インシデント発生時に適切に対応できるようにする。	情報セキュリティの計画、設計・導入、運用・保守、見直しのPDCAサイクルを実施する方法論として、国際標準にもなっている情報セキュリティマネジメントシステム（ISMS）がある。 本科目では、企業の事業継続における情報セキュリティマネジメントとガバナンスについて、ISMSを中心としたケーススタディ（演習）で学ぶ。本科目の目標は、企業における情報セキュリティを統括する、CISOに必要な基本的な知識と能力を修得することにある。	脆弱なシステムに対する攻撃によって、社会的に大きな影響と被害が発生している。そのため、セキュアなシステム設計・開発、脆弱性検査とその対策は、重要性が増している。 本科目は、セキュアシステム設計・開発論について、演習を通して体得することを目指す。前半では、プログラム工程での脆弱性を作り込みで体験し、対策を学ぶ。その後、セキュリティのターゲットとなるものや、開発の前工程で脆弱性を作りこまないようにする、プロジェクトマネジメント手法を学ぶ。後半では、プロジェクト開始前の要求事項として何を要求すれば後工程で脆弱性が発生しないかを学び、コモンクライテリアを一例として一般としての手法を学ぶ。 最後に演習を行い、工程ごとのセキュリティ対策のディスカッションを行う。
修得できる能力	サイバーセキュリティ確保に関して必要となる各種技術の理解／ユビキタス技術に関する知識／サイバー攻撃そのものへの攻撃内容を理解し、対策を的確に選択・実施できる能力／セキュアな運用を可能とする幅広い基盤知識	通信ネットワークのセキュリティ確保に関して必要となる各種技術の理解／通信ネットワークを用いた、あるいは通信ネットワークそのものへの攻撃内容を理解し、対策を的確に選択・実施できる能力／セキュアな運用を可能とするネットワークシステムをデザインする能力	企業における情報セキュリティを統括するCISO（Chief Information Security Officer/最高情報セキュリティ責任者）として必要な基礎知識と能力／インシデントへの基本的な対応能力（上級セキュリティエンジニア）	デジタル・フォレンジックの考え方や基本技術を習得し、個人情報漏えいや不正侵入などのインシデント発生時に、応急対応をとれるようにするとともに、裁判に備えログを適切に収集、分析できるようにし、必要な資料を法的に問題ないように準備できるようにする。	企業における情報セキュリティを統括するCISO（Chief Information Security Officer/最高情報セキュリティ責任者）として必要な基礎知識と能力／ISMSの継続維持を可能とする社員教育の基本的能力／コンプライアンスならびに監査に関する基本的能力	セキュアシステム設計論の修得／コモンクライテリアに基づく保証と評価の実際について演習を通して体得する／Webアプリケーションの脆弱性検査手法とその基本的な対策の能力
1	4月10日（金） 18:10～ 暗号学／セキュリティアーキテクチャと設計／アクセス制御／通信とネットワークのセキュリティ／物理セキュリティ／運用セキュリティ／ユビキタスセ 岩井 将行／東京電機大学 セキュリティ入門基盤とCISSPイントロダクション　テクニカル　講義　演習	4月18日（土） 9:00～ 通信とネットワークのセキュリティ／アクセス制御／運用セキュリティ 奥村 恭弘／NTTコミュニケーションズ株式会社 総論：サイバーディフェンス実践　脅威の歴史から最新の脅威を踏まえながら　テクニカル　講義　演習	4月9日（木） 18:10～ 法、規則、コンプラ、捜査 安田 浩／東京電機大学 セキュリティインテリジェンス概論　マネジメント　講義　演習	9月18日（金） 18:10～ 法、規則、コンプラ、捜査 佐々木 良一／東京電機大学 デジタルフォレンジック入門　テクニカル　講義　演習	9月15日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 伊藤 潤／三井物産セキュアディレクション株式会社 CISSP講座 情報セキュリティマネジメントとガバナンス　マネジメント　講義　演習	9月26日（土） 9:00～ セキュリティアーキテクチャと設計／運用セキュリティ／ソフト開発 安田 浩／東京電機大学 柿崎 淑郎／東京電機大学 総論：セキュアシステム設計・開発　テクニカル　講義　演習
2	4月17日（金） 18:10～ 暗号学 齊藤 泰一／東京電機大学 CISSP講座 暗号技術の基礎 完全性・機密性・信頼性を確保するための暗号化の原則・手段及び方式／暗号技術の歴史／暗号方式・アルゴリズムの原則・特徴　テクニカル　講義　演習	4月18日（土） 10:40～ 運用セキュリティ 林 郁也／NTTコミュニケーションズ株式会社 インシデント情報の連携と報告書作成　テクニカル　講義　演習	4月16日（木） 18:10～ 法、規則、コンプラ、捜査／運用セキュリティ 杉浦 芳樹／NTTデータ先端技術株式会社 コミュニケーション力、コーチング、チームビルディング　マネジメント　講義　演習	9月25日（金） 18:10～ セキュリティアーキテクチャと設計／運用セキュリティ 上原 哲太郎／立命館大学 ハードディスクの構造，ファイルシステム　テクニカル　講義　演習	9月29日（火） 18:10～ 法、規則、コンプラ、捜査／情報セキュリティガバナンスとリスクマネジメント 中島 一樹／トヨタ自動車株式会社 企業戦略と社会的責任（CSR）　マネジメント　講義　演習	9月26日（土） 10:40～ ソフトウエア開発セキュリティ [redacted] セキュアプログラミング ネイティブアプリケーション①　テクニカル　講義　演習
3	4月24日（金） 18:10～ 暗号学 齊藤 泰一／東京電機大学 CISSP講座 暗号技術の基礎 ・シーザー、エニグマ ・ブロック暗号/ストリーム暗号 ・ハッシュ、乱数、鍵　テクニカル　講義　演習	4月18日（土） 13:10～ 通信とネットワークのセキュリティ／アクセス制御／運用セキュリティ 六宮 智悟／トレンドマイクロ株式会社 マルウエアの歴史/解析環境　テクニカル　講義　演習	4月23日（木） 18:10～ 法、規則、コンプラ、捜査／運用セキュリティ 角尾 幸保／日本電気株式会社 ソーシャルエンジニアリング技法　マネジメント　講義　演習	10月2日（金） 18:10～ セキュリティアーキテクチャと設計／運用／ソフト開発 上原 哲太郎／立命館大学 フォレンジックのための OS，Windows概論　テクニカル　講義　演習	10月6日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 伊藤 潤／三井物産セキュアディレクション株式会社 内部統制 及び IT統制　マネジメント　講義　演習	9月26日（土） 13:10～ ソフトウエア開発セキュリティ／セキュリティアーキテクチャと設計 [redacted] セキュアプログラミング ネイティブアプリケーション②　テクニカル　講義　演習
4	5月1日（金） 18:10～ 暗号学 大鐘 博子／株式会社NSD CISSP講座 暗号技術の応用 ・認証局/電子証明書/PKI ・SSL/TLS ・DRD，デジタル署名，他　テクニカル　講義　演習	5月9日（土） 10:40～ 通信とネットワークのセキュリティ／アクセス制御／運用セキュリティ 松木 晋祐／株式会社ベリサーブ 脆弱性検出技法（ファジング、リバースエンジニアリング）　テクニカル　講義　演習	4月30日（木） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 松浦 幹太／東京大学 セキュリティ経済学　マネジメント　講義　演習	10月9日（金） 18:10～ 法、規則、コンプライアンス、捜査／運用／ソフト開発 野崎 周作／株式会社UBIC フォレンジック作業の基礎　テクニカル　講義　演習	10月13日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 原田 要之助 ／情報セキュリティ大学院大学 国際標準にみる情報セキュリティ　マネジメント　講義　演習	10月17日（土） 9:00～ ソフトウエア開発セキュリティ／セキュリティアーキテクチャと設計 久保 正樹、戸田 洋三／一般社団法人JPCERT／ セキュアプログラミング Webアプリケーション①　テクニカル　講義　演習
5	5月15日（金） 18:10～ セキュリティアーキテクチャと設計 佳山 こうせつ／富士通株式会社 CISSP講座 セキュリティアーキテクチャ　テクニカル　講義　演習	5月9日（土） 10:40～ 通信とネットワークのセキュリティ／運用セキュリティ／アク[redacted] 木村 仁美／トレンドマイクロ株式会社 マルウエア解析演習① マルウェアの発見（検出手法）　テクニカル　講義　演習	5月7日（木） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 長谷川 長一／株式会社ラック CISSP講座 法・捜査・コンプライアンス　マネジメント　講義　演習	10月16日（金） 18:10～ 法、規則、コンプラ、捜査／運用／ソフト開発 野崎 周作／株式会社UBIC フォレンジック作業 データ保全　テクニカル　講義　演習	10月20日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 金児 茂／三井物産セキュアディレクション株式会 リスクマネジメントとリスク分析　マネジメント　講義　演習	10月17日（土） 10:40～ ソフトウエア開発セキュリティ／セキュリティアーキテクチャと設計 久保 正樹、戸田 洋三／一般社団法人JPCERT／ セキュアプログラミング Webアプリケーション②　テクニカル　講義　演習
6	5月22日（金） 18:10～ アクセス制御 河野 省二／株式会社ディアイティ CISSP講座 アクセス制御　テクニカル　講義　演習	5月9日（土） 13:10～ 通信とネットワークのセキュリティ／運用セキュリティ／アクセス制御 木村 仁美／トレンドマイクロ株式会社 マルウエア解析演習② 動的解析とヒューリスティック検知　テクニカル　講義　演習	5月14日（木） 18:10～ 法、規則、コンプラ、捜査 大河内 智秀／東京電機大学 セキュリティ倫理　マネジメント　講義　演習	10月23日（金） 18:10～ 法、規則、コンプラ、捜査／運用／ソフト開発 白濱 直哉／有限責任監査法人トーマツ フォレンジック作業 データ復元　テクニカル　講義　演習	10月27日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 金児 茂／三井物産セキュアディレクション株式会 リスクマネジメントとリスク分析　演習（ケーススタディ）　マネジメント　講義　演習	10月17日（土） 13:10～ ソフトウエア開発セキュリティ／セキュリティアーキテクチャと設計 寺田 真敏／株式会社日立製作所 セキュアインフラ構築（ネットワーク）　テクニカル　講義　演習
7	5月29日（金） 18:10～ アクセス制御 河野 省二／株式会社ディアイティ CISSP講座 ソフトウエアデベロップメント　テクニカル　講義　演習	5月30日（土） 9:00～ 通信とネットワークのセキュリティ／運用セキュリティ／アクセス制御 木村 仁美／トレンドマイクロ株式会社 マルウエア解析演習③-1 静的解析(アセンブリ)　テクニカル　講義　演習	5月21日（木） 18:10～ 情報セキュリティガバナンスとリスクマネジメント 大河内 智秀／東京電機大学 CSIRT（CSIRTの目的、意義、組織連携）　マネジメント　講義　演習	11月6日（金） 18:10～ 法、規則、コンプラ、捜査／運用／ソフト開発 白濱 直哉／有限責任監査法人トーマツ フォレンジック作業 データ解析①　テクニカル　講義　演習	11月10日（火） 18:10～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 北原 幸彦／NRIセキュアテクノロジーズ株式会社 情報セキュリティマネジメントの国際標準（ISO27000）とISMS　マネジメント　講義　演習	11月7日（土） 9:00～ 情報セキュリティガバナンスとリスクマネジメント／通信とネットワークのセキュリティ／ソフト開発 井上 吉隆／NTTスマートコネクト株式会社 セキュアインフラ構築（サーバ）　テクニカル　講義　演習

1

付録1

科目名	1 PF	2 CD	3 IN	4 DF	5 MG	6 DD
	サイバーセキュリティ基盤	サイバーディフェンス実践演習	セキュリティインテリジェンスと心理・倫理・法	デジタル・フォレンジック	情報セキュリティマネジメントとガバナンス	セキュアシステム設計・開発
8	6月5日（金）18:10～ 暗号学／セキュリティアーキテクチャと設計／アクセス制御／通信とネットワークのセキュリティ 金野 千里／独立行政法人 情報処理推進機構 制御システム、組み込み機器のセキュリティ テクニカル 講義 演習	5月30日（土）10:40～ 通信とネットワークのセキュリティ／運用セキュリティ／アクセス制御 木村 仁美／トレンドマイクロ株式会社 マルウエア解析演習③-2 静的解析 テクニカル 講義 演習	5月28日（木）18:10～ 法、規則、コンプラ、捜査 越智 啓太／法政大学 サイバー犯罪と心理学 マネジメント 講義 演習	11月13日（金）18:10～ 法、規則、コンプラ、捜査／運用／ソフト開発 野崎 周作／株式会社UBIC フォレンジック作業 データ解析② テクニカル 講義 演習	11月17日（火）18:10～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 北原 幸彦／NRIセキュアテクノロジーズ株式会社 ISMS演習 マネジメント 講義 演習	11月7日（土）10:40～ ソフトウエア開発セキュリティ／セキュリティアーキテクチャと設計 亀田 勇歩／SCSK株式会社 セキュリティ脅威分析 テクニカル 講義 演習
9	6月12日（金）18:10～ 通信とネットワークのセキュリティ 武智 洋／日本電気株式会社 CISSP講座 ネットワークセキュリティ テクニカル 講義 演習	5月30日（土）13:10～ 通信とネットワークのセキュリティ／アクセス制御／運用セ 草場 英仁／三井物産セキュアディレクション株式会社 エクスプロイトライティング テクニカル 講義 演習	6月4日（木）18:10～ 運用セキュリティ／法、規則、コンプラ、捜査 橋本 豪／西村あさひ法律事務所 企業の情報資産防衛と法制度・政策の交錯 ― 米国の例を参考に マネジメント 講義 演習	11月20日（金）18:10～ 法、規則、コンプラ、捜査／運用／ソフト開発 白濱 直哉／有限責任監査法人トーマツ 野崎 周作／株式会社UBIC フォレンジック作業 演習 テクニカル 講義 演習	11月24日（火）18:10～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 烏山 雄大／三井物産セキュアディレクション株式会社 情報セキュリティポリシー マネジメント 講義 演習	11月7日（土）13:10～ ソフトウエア開発セキュリティ／情報セキュリティガバナンスとリスクマネジメント／通信とネットワーク 亀田 勇歩／SCSK株式会社 セキュリティ脅威分析 演習 テクニカル 講義 演習
10	6月19日（金）18:10～ 物理（環境）セキュリティ 小熊 慶一郎／株式会社 KBIZ CISSP講座 物理セキュリティ テクニカル 講義 演習	6月20日（土）9:00～ 通信とネットワークのセキュリティ／アクセス制御／運用セキュリティ 草場 英仁／三井物産セキュアディレクション株式会社 エクスプロイトライティング 演習 テクニカル 講義 演習	6月11日（木）18:10～ 法、規則、コンプラ、捜査／運用セキュリティ 高取 芳宏／オリック東京法律事務所 データプロテクションと国際訴訟 マネジメント 講義 演習	11月27日（金）18:10～ 通信とネットワークのセキュリティ／ソフト開発 八槇 博史／東京電機大学 ネットワークフォレンジック（攻撃法，マルウェア，ログの取り方），Webの構造2 テクニカル 講義 演習	12月1日（火）18:10～ アクセス制御／セキュリティアーキテクチャと設計 大木 栄二郎／工学院大学 情報セキュリティ監査 マネジメント 講義 演習	11月28日（土）9:00～ 情報セキュリティガバナンスとリスクマネジメント／通信とネットワークのセキュリティ／ソフト開発 奥村 恭弘／NTTコミュニケーションズ株式会社 プロジェクト・マネジメント 演習 テクニカル 講義 演習
11	6月26日（金）18:10～ 運用セキュリティ 小林 浩史／日本電気株式会社 CISSP講座 運用セキュリティ テクニカル 講義 演習	6月20日（土）10:40～ 通信とネットワークのセキュリティ／アクセス制御／運用セキュリティ 国分 裕、小西 明紀／三井物産セキュアディレクション株式会社 脆弱検出方法（Webアプリケーション、スマートフォン） テクニカル 講義 演習	6月18日（木）18:10～ 法、規則、コンプラ、捜査／通信とネットワークのセキュリティ／運用セキュリティ 土屋 日路親／総務省 サイバーセキュリティと通信の秘密 マネジメント 講義 演習	12月4日（金）18:10～ 通信とネットワークのセキュリティ／ソフト開発 八槇 博史／東京電機大学 上記の演習 テクニカル 講義 演習	12月8日（火）18:10～ アクセス制御／セキュリティアーキテクチャと設計 大木 栄二郎／工学院大学 情報セキュリティ監査 演習 マネジメント 講義 演習	11月28日（土）10:40～ 情報セキュリティガバナンスとリスクマネジメント／セキュリティアーキテクチャと設計 大久保 隆夫／情報セキュリティ大学院大学 セキュリティ要求仕様と分析手法 テクニカル 講義 演習
12	7月3日（金）18:10～ 通信とネットワークのセキュリティ 岩井 将行／東京電機大学 ユビキタス技術とセキュリティ テクニカル 講義 演習	6月20日（土）13:10～ 通信とネットワークのセキュリティ／アクセス制御 国分 裕、小西 明紀／三井物産セキュアディレクション 脆弱検出技法（Webアプリケーション、スマートフォン）演習 テクニカル 講義 演習	6月25日（木）18:10～ 運用セキュリティ 伊藤 潤／三井物産セキュアディレクション株式会社 セキュリティコンサルティング概論とその技法（事例を踏まえたケーススタディー） マネジメント 講義 演習	12月11日（金）18:10～ 法、規則、コンプラ、捜査／ソフト開発 白濱 直哉／有限責任監査法人トーマツ 代表的な対象におけるDFの方法① テクニカル 講義 演習	12月15日（火）18:10～ 運用セキュリティ 林 郁也／NTTコミュニケーションズ株式会社 インシデントレスポンス演習① マネジメント 講義 演習	11月28日（土）13:10～ 情報セキュリティガバナンスとリスクマネジメント／ 大久保 隆夫／情報セキュリティ大学院大学 セキュリティ要求仕様と分析手法 演習 テクニカル 講義 演習
13	7月10日（金）18:10～ セキュリティアーキテクチャと設計 河野 健二／慶應義塾大学 Unix,LinuxOSのセキュリティアーキテクチャ（SELinux含む） テクニカル 講義 演習	7月11日（土）9:00～ 運用セキュリティ 中西 克彦／NECネクサソリューションズ株式会社 サイバーセキュリティ実践演習（CTF） テクニカル 講義 演習	7月2日（木）18:10～ 運用セキュリティ 満永 拓邦／一般社団法人JPCERT／CC インシデントハンドリングワークショップ① マネジメント 講義 演習	12月18日（金）18:10～ 法、規則、コンプラ、捜査／ソフト開発 野崎 周作／株式会社UBIC 代表的な対象におけるDFの方法② テクニカル 講義 演習	12月22日（火）18:10～ 運用セキュリティ 林 郁也／NTTコミュニケーションズ株式会社 インシデントレスポンス演習② マネジメント 講義 演習	12月19日（土）9:00～ セキュリティアーキテクチャと設計 宮坂 肇／NTTデータ先端技術株式会社 セキュリティ要求仕様と分析（ISO/IEC15408） テクニカル 講義 演習
14	7月17日（金）18:10～ セキュリティアーキテクチャと設計 松下 綾子／アルプスシステムインテグレーション株式会社 モバイルOSとセキュリティ テクニカル 講義 演習	7月11日（土）10:40～ 運用セキュリティ 中西 克彦／NECネクサソリューションズ株式会社 サイバーセキュリティ実践演習（CTF） テクニカル 講義 演習	7月9日（木）18:10～ 運用セキュリティ／法、規則、コンプラ、捜査 満永 拓邦／一般社団法人JPCERT／CC インシデントハンドリングワークショップ② マネジメント 講義 演習	12月25日（金）18:10～ 法、規則、コンプラ、捜査 桜庭 信之／西村あさひ法律事務所 法リテラシーと法廷対応 テクニカル 講義 演習	1月12日（火）18:10～ 事業継続と災害復旧の計画 小林 浩史／日本電気株式会社 CISSP講座 事業継続と災害復旧の計画 マネジメント 講義 演習	12月19日（土）10:40～ セキュリティアーキテクチャと設計 宮坂 肇／NTTデータ先端技術株式会社 開発手法 コモンクライテリアの評価方法論および演習（ケーススタディ） テクニカル 講義 演習
15	7月24日（金）18:10～ 暗号学／セキュリティアーキテクチャと設計／アク 岩井 将行／東京電機大学 セキュリティ基盤総合 テクニカル 講義 演習	7月11日（土）13:10～ 運用セキュリティ 正木 健介／NRIセキュアテクノロジーズ株式会社 攻撃の検知、解析（IDS/IPS/相関分析・SIEM） テクニカル 講義 演習	7月16日（木）18:10～ 運用セキュリティ／法、規則、コンプラ、捜査 安田 浩／東京電機大学 サイバーインテリジェンスvsセキュリティインテリジェンス総括発表会 マネジメント 講義 演習	1月8日（金）18:10～ 法、規則、コンプラ、捜査／通信とネットワーク 佐々木 良一／東京電機大学 デジタルフォレンジックの今後の展開 テクニカル 講義 演習	1月19日（火）18:10～ 情報セキュリティガバナンスとリスクマネジメント 佐々木 良一／東京電機大学 リスクコミュニケーション マネジメント 講義 演習	12月19日（土）13:10～ ソフトウエア開発セキュリティ／情報セキュリティガ 安田 浩／東京電機大学 柿崎 淑郎／東京電機大学 セキュアプログラミング 総合 セキュアな開発のライフサイクルと脆弱性を作りこまない開発 テクニカル 講義 演習
16	7月31日（金） 最終論述試験	7月25日（土） 総合演習試験	7月23日（木） 最終論述試験	1月22日（金） 学力考査と解説	1月26日（火） 最終論述試験	 総合演習
履修資格（前提）	ネットワーク、OS、セキュリティ関連技術に関する学部卒業レベルの知識を有すること	分散処理、コンピュータネットワーク、TCP/IPおよびセキュリティ関連技術に関する学部卒業レベルの知識を有すること UNIX系OSの操作に習熟していること プログラミング経験を有すること アセンブリ知識を有していること（x86）	1PF サイバーセキュリティ基盤の先修を推奨する. 5MG 情報セキュリティマネジメントとガバナンスの先修または同時履修を推奨する. 学部卒業程度の情報セキュリティに関する基礎知識を前提とする	1PF サイバーセキュリティ基盤の先修を推奨する. 学部卒業程度の情報セキュリティに関する基礎知識を前提とする	1PF サイバーセキュリティ基盤の先修を推奨する. 3IN セキュリティインテリジェンスと心理、倫理、法の先修または同時履修を推奨する. 学部卒業程度の情報セキュリティに関する基礎知識を前提とする	1PF サイバーセキュリティ基盤の先修を推奨する. 学部卒業程度の情報セキュリティに関する基礎知識を前提とする 基本的なプログラミング能力，基礎的なHTML/DBの知識を前提とする
成績評価方法・基準	・試験 50% ・講義中に実施する演習の成果とその報告 50%					

付録2

CySec

2015 年度（平成 27 年度）

文部科学省
「高度人材養成のための社会人学び直し大学院プログラム」
選定

東京電機大学
「国際化サイバーセキュリティ学特別コース」
募集要項

＜履修証明制度対応＞

TDU 東京電機大学

付録2

CySec

2015 年度（平成 27 年度）
文部科学省「高度人材養成のための社会人学び直し大学院プログラム」選定
東京電機大学「国際化サイバーセキュリティ学特別コース」募集要項
＜履修証明制度対応＞

東京電機大学では、「国際化サイバーセキュリティ学特別コース」として、6 科目（120 時間）を開講します。このコースは、履修証明制度に対応しています。

1. 教育目的

悪意ソフト攻撃は増加の一途であり、サイバーセキュリティ（以下CSと略す）のより一層の充実は、社会を安心・安全・豊かにするための喫緊の課題です。そのためには、社会活動に参加するすべての人々のCS意識を高める必要があります。

本プログラムは、社会構成員全員のCS意識の高揚を先導する、高度CS専門家を養成することを目的としています。

2. 教育課程

本プログラムでは、企業における情報セキュリティを統括する最高情報セキュリティ責任者（Chief Information Security Officer: CISO） や、セキュアな情報システムの開発において主導的役割を果たす上級セキュリティエンジニアを、育成すべき高度人材像としています。そのような人材を育成するため、企業等で活躍されている専門家を招聘し、事例紹介と事例に基づくワークショップ形式の演習と、座学ワークショップを合わせて実施します。

具体的には、法律・倫理など制度的枠組みに関する理解や、攻撃者の意図や行動に関する洞察、企業におけるコンプライアンスを実現するためのガバナンスなど、幅広くかつ高度な能力を育成するために、以下の6科目(演：演習中心3講座、講：講義・ワークショップ中心3講座)を開講します。

開講する科目は、大学院修士課程レベルの内容です。

①	サイバーセキュリティ基盤	(1PF)	(講)
②	サイバーディフェンス実践演習	(2CD)	(演)
③	セキュリティインテリジェンスと心理・倫理・法	(3IN)	(講)
④	デジタル・フォレンジック	(4DF)	(演)
⑤	情報セキュリティマネジメントとガバナンス	(5MG)	(講)
⑥	セキュアシステム設計・開発	(6DD)	(演)

※ 科目名に記載した英数字は科目記号です。

3. 履修証明書

学校教育法に基づく履修証明制度により、プログラム修了者には、「国際化サイバーセキュリティ学特別コース 履修証明書」を授与します。

【本プログラムにおける履修証明書交付要件】

開講される 6 科目（120 時間）を修得すること

【履修証明制度概要】

付録2

CySec

平成 19 年度の学校教育法の改正により、大学等における「履修証明制度」が創設されました。

これは、学生を対象とした学位プログラムの他に、社会人等を対象とした 120 時間以上の学習プログラム（履修証明プログラム）を提供し、修得した者に履修証明書を発行する制度です。履修証明制度には、以下の 3 点の特徴があります。

（1）大学の学位に比べ、より短期間に修得することが可能
（2）再就職やキャリアアップに役立つ社会人向けの教育プログラム
（3）プログラム修了者には、学校教育法に基づき履修証明書を交付

※履修証明制度に関する文部科学省 Web ページ
http://www.mext.go.jp/a_menu/koutou/shoumei/

4. 募集人員

国際化サイバーセキュリティ学特別コース　2015 年度　定員 20 名

5. 講座実施場所

東京電機大学　東京千住キャンパス

6. 開講期間・開講日時等

前期：　2015 年 4 月 6 日(月)～2015 年 7 月 29 日(水)
後期：　2015 年 9 月 14 日(月)～2016 年 1 月 27 日(水)
時間割は以下の通り。

科目名	配当期	曜日	時限
サイバーセキュリティ基盤 (1PF)	前期	金	6
サイバーディフェンス実践演習(2CD)	前期	土	1,2,3
セキュリティインテリジェンスと心理・倫理・法(3IN)	前期	木	6
デジタル・フォレンジック(4DF)	後期	金	6
情報セキュリティマネジメントとガバナンス(5MG)	後期	火	6
セキュアシステム設計・開発 (6DD)	後期	土	1,2,3

※　各科目のシラバスについては Web ページを参照
https://cysec.dendai.ac.jp/lecture/

受講にはノートPCが必要となります。推奨するスペック等については、Webページでお知らせする予定です。

7.　受講資格

本プログラムは、CISO、上級セキュリティエンジニア等を目指す、基本的な情報セキュリティの知識を有する者を対象に開講します。

次の各号の一つに該当する者（大学院修士課程入学レベル）

① 大学を卒業した者、及び本プログラム受講時までに卒業見込みの者
② 大学評価・学位授与機構から学士の学位を授与された者、及び本プログラム受講時までに授与される見込みの者
③ 外国において学校教育における 16 年の課程を修了した者、および本プログラム受講時までに修了見込みの者
④ 大学の 3 年次に在学し、当該大学（学部）で定める早期卒業基準を満たす者
⑤ 大学の 3 年次に在学し、または外国において学校教育における 15 年の課程を修了し、本大学院未来科学研究科委員会が、優れた成績で所定の単位を修得したものと認めた者
⑥ その他本大学院未来科学研究科委員会が、大学を卒業した者と同等以上の学力があると認めた者

開講される各科目を履修する際の前提条件は次の通りです。

(1PF) サイバーセキュリティ基盤
- ネットワーク、OS、セキュリティ関連技術に関する学部卒業レベルの知識を有すること。

(2CD) サイバーディフェンス実践演習
- 分散処理、コンピュータネットワーク、TCP/IP およびセキュリティ関連技術に関する学部卒業レベルの知識を有すること。
- UNIX 系OS の操作に習熟していること。
- プログラミング経験を有すること。
- アセンブリ知識を有していること（x86）

(3IN) セキュリティインテリジェンスと心理・倫理・法
- 1PF　サイバーセキュリティ基盤の先修を推奨する。
- 5MG　情報セキュリティマネジメントとガバナンスの先修または同時履修を推奨する。
- 学部卒業程度の情報セキュリティに関する基礎知識を前提とする。

(4DF) デジタル・フォレンジック
- 1PF　サイバーセキュリティ基盤の先修を推奨する。
- 学部卒業程度の情報セキュリティに関する基礎知識を前提とする。

(5MG) 情報セキュリティマネジメントとガバナンス
- 1PF　サイバーセキュリティ基盤の先修を推奨する。
- 3IN　セキュリティインテリジェンスと心理・倫理・法の先修または同時履修を推奨する。
- 学部卒業程度の情報セキュリティに関する基礎知識を前提とする。

(6DD) セキュアシステム設計・開発
- 1PF　サイバーセキュリティ基盤の先修を推奨する。
- 基本的なプログラミング能力、基礎的なHTML/DBの知識を前提とする
- 学部卒業程度の情報セキュリティに関する基礎知識を前提とする。

8. 出願手続き書類

以下の書類を、巻末に記載の送付先に郵送してください。

① 東京電機大学「国際化サイバーセキュリティ学特別コース」願書
写真 1 枚（脱帽上半身、背景なし、最近 3 ヶ月以内撮影、願書の所定欄に貼付

してください。）

② 最終出身学校の卒業証明書もしくは卒業見込証明書

③ 最終出身学校の成績証明書

「受講資格審査料」は、出願手続き期間内に、以下のとおり指定口座に振り込んでください。

振込先

銀行名:	三菱東京UFJ銀行(0005)
支店名:	神田支店(331)
種別:	普通
口座番号:	1186980
名義:	学校法人 東京電機大学 受講料口 理事長 加藤 康太郎
振込金額	10,000 円 （受講資格審査料）

※振込人名義の頭に 3000 と入れてください。
※振込手数料は振り込みされる方のご負担となります。

9. 出願手続き及び期間

【受付期間】 2015 年 2 月 13 日(金)～2015 年 3 月 4 日(水) 必着

【注意事項】

- 出願者は、出願書類一式（「8. 出願手続き書類」項目の①～③の書類）を、角形第 2 号封筒（240×332mm）に入れ、簡易書留・速達で郵送してください。郵送の際は、封筒の表面に出願書類在中と朱記してください。また封筒の裏面に出願者の住所、氏名を記載して下さい。
- 郵送された願書等は返送いたしません。

10. 受講資格審査

面接による受講資格審査を行います。

【受講資格審査日時】： 2015 年 3 月 7 日（土） 14 時 00 分～

【受講資格審査場所】： 東京千住キャンパス
〒120-8551
東京都足立区千住旭町 5 番
北千住駅東口（電大口）から徒歩 1 分
（JR 常磐線・東京メトロ（日比谷線・千代田線）・東武伊勢崎線・つくばエクスプレス）

※ 場所等詳細については 3 月 6 日（金）までにご連絡いたします。

11. 必要となる費用（受講資格審査料・受講費・教材費・施設利用費）

●出願時に必要な費用

【受講資格審査料】　10,000 円

●受講手続き時に必要な費用

【受講費】　16,000 円/科目　（6 科目で 96,000 円）
（本来は 32,000 円/科目　平成 27 年度は半額）

※　子育て世代女性の受講支援のため、一定の要件を満たした場合、上記とは別の受講費を設定しています。詳しくは巻末に記載のお問い合わせフォームにてご連絡ください。

【施設利用費】　10,000 円（半期）
（ID カード作成費、PC 等設備利用費、図書館利用費等）

【電子教材費】　実費
（$175～$220　$1 を 120 円で計算すると 21,000 円～26,400 円）

※　電子教材費は、受講人数と為替レートにより変動しますので、後日改めてご連絡します。

※　この電子教材費以外に教科書等の購入費がかかる場合があります。

12. 受講資格審査結果通知

下記の日程で発送いたします。

2015 年　3 月 10 日（火）発送予定

3 月 12 日（木）までに合否通知が届かない場合は、以下の Web ページの問い合わせフォームでお問い合わせください。

Web ページ：https://cysec.dendai.ac.jp/contact/

お問い合わせ内容の 1 行目に「CS 合否通知不着」と記載してください。2 行目以降に、氏名・電話番号・受験番号を記入してください。

13. 受講手続き等

合格者へは、合格通知とともに次の書類を送付いたします。所定の期間内に、受講費等の振込を含めた手続きを行ってください。詳細については、受講資格審査結果通知時に、改めてお知らせいたします。

① 「国際化サイバーセキュリティ学特別コース」履修申請書

② 受講費等の振込用紙

●受講手続き時に振り込む費用

【受講費】　16,000 円/科目
履修科目数に応じた受講費は次の通り。

1 科目	16,000 円	2 科目	32,000 円
3 科目	48,000 円	4 科目	64,000 円
5 科目	80,000 円	6 科目	96,000 円

【施設利用費】　10,000 円（半期）
（ID カード作成費、PC 等設備利用費、図書館利用費等）

付録2

CySec

【電子教材費】　　実費

（$175～$220　$1 を 120 円で計算すると 21,000 円～26,400 円）

※　受講手続きには健康診断書（指定項目（身長、体重、胸部 X 線所見、問診）の入ったもの）が必要になります。

※一度振り込まれた受講費等はいかなる理由があっても返金致しかねます。振込手数料は振り込みされる方のご負担となります。

手続締切日　　2015 年 4 月 8 日（水）　必着

【手続き書類の送付先】

〒120-8551　東京都足立区千住旭町5番

東京電機大学　1 号館 14 階　応用情報工学研究室内

国際化サイバーセキュリティ学特別コース事務局　行

【お問い合わせ先】

お問い合わせは Web のフォームからお願いします。

お問合せフォーム　　https://cysec.dendai.ac.jp /contact/

付録2

受験番号

2015年度（平成27年度）東京電機大学
「国際化サイバーセキュリティ学特別コース」願書

			記入日	2015 年 月 日	
ふりがな			性別	男 女	はがれないように枠内にしっかり貼付ける。 写真うら面には、氏名を記入する。
氏 名					
氏名ローマ字					
生年月日	西暦 年 月 日 生			歳	
ふりがな					
現住所 〒					
TEL	携帯		FAX		
E-Mail					

職場	企業・組織名	
	部署名	
	TEL	

	年	月	学 校 名
学歴			高等学校 卒業
			大学 学部 学科 卒業

	期間					勤務先名
	年	月	～	年	月	
職歴			～			
			～			
			～			
			～			

※1 申請いただいた方の情報は、「国際化サイバーセキュリティ学特別コース」の運用のため以外には使用いたしません。
※2 この写真を使用してIDカードを作成します。
※3 受講資格審査日時は、2015年3月7日（土） 14時00分 からを予定しています。詳細は追ってご連絡いたします。

付録3

CySec 国際化サイバーセキュリティ学特別コース　TDU 東京電機大学

■CySec オープニングシンポジウム講師紹介

谷脇康彦（たにわき・やすひこ）氏

内閣官房内閣審議官（内閣サイバーセキュリティセンター副センター長）。84年、郵政省（現総務 省）入省。郵政大臣秘書官、在米日本大使館 ICT 政策担当参事官、総務省総合通信基盤局料金サービス課長、同事業政策課長、情報通信国際戦略局情報通信政 策課長、大臣官房企画課長、大臣官房審議官（情報流通行政局担当）などを経て、13年7月より現職。著書に「ミッシングリンク～デジタル大国日本再生」（12年7月、東洋経済新報社刊）など。

Howard Schmidt 氏

Howard Schmidt serves as a partner in the strategic advisory firm, Ridge-Schmidt Cyber, an executive services firm that helps leaders in business and government navigate the increasing demands of cybersecurity. He serves in this position with Tom Ridge, the first secretary of the Department of Homeland Security. He also serves as executive director of The Software Assurance Forum for Excellence in Code (SAFECode).

Howard A. Schmidt brings together talents in business, defense, intelligence, law enforcement, privacy, academia and international relations, gained from a distinguished career spanning 40 years.

He served as Special Assistant to the President and the Cybersecurity Coordinator for the federal government. In this role Mr. Schmidt was responsible for coordinating interagency cybersecurity policy development and implementation and for coordinating engagement with federal, state, local, international, and private sector cybersecurity partners.

Previously, Mr. Schmidt was the President and CEO of the Information Security Forum (ISF). Before ISF, he served as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay Inc., and formerly operated as the Chief Security Officer for Microsoft Corp. He also served as Chief Security Strategist for the US-CERT Partners Program for the Department of Homeland Security.

Mr. Schmidt also brings to bear over 26 years of military service. Beginning active duty with the Air Force, he later joined the Arizona Air National Guard. With the AF he served in a number of military and civilian roles culminating as Supervisory Special Agent with the Office of Special Investigations (AFOSI). He finished his last 12 years as an Army Reserve Special Agent with Criminal Investigation Division's (CID) Computer Crime Unit, all while serving over a decade as police officer with the Chandler Police Department.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the University of Phoenix. He also holds an Honorary Doctorate degree in Humane Letters. Howard was an Adjunct Professor at GA Tech, GTISC, Professor of Research at Idaho State University and Adjunct Distinguished Fellow with Carnegie Mellon's CyLab and a Distinguished Fellow of the Ponemon Privacy Institute.

Howard is a Ham Radio operator (W7HAS), a private pilot, outdoorsman and an avid Harley-Davidson

rider. He is married to Raemarie J. Schmidt, a forensic scientist and researcher and instructor in the field of computer forensics. Together, they are proud parents, and happy grandparents.

Greg Thompson 氏

Vice President, Operational Governance, Scotiabank, Toronto, Canada Mr. Thompson is an IT Risk and Information Security professional with extensive industry experience in industries ranging from Telecommunications to the Financial Services Industry. He has held various senior level Information Security management positions including Head of Global IS Security and CISO for Manulife Financial Corporation (Toronto, Canada ? 2000–2003), VP Enterprise Security & Deputy CISO, Scotiabank (2008 – 2015), and VP Operational Governance, Scotiabank (2015–present).
As the Vice President of Operational Governance at Scotiabank Mr. Thompson oversees the growing IT Risk Management program which covers some 36 functional areas of IT service delivery, support, cyber security, strategic management, software development and governance.
Previous to his current role, Mr. Thompson spent nearly 7 years as the Vice President of Enterprise Security & Deputy CISO .He led a large multi–disciplinary team responsible for a broad range of IT Security services including; Cyber Security, Endpoint and Gateway Security, Security Governance, Regulatory Compliance, Vulnerability Management, Network & Forensics, Customer Authentication, and Business Continuity Management. Mr. Thompson is a Certified Information Systems Security Professional and is a graduate of the Richard Ivey School of Business, Executive Leadership Program. (University of Western Ontario).
In addition, Mr. Thompson spent three years serving on the Board of Directors for (ISC)2, [pronounced “ISC Squared”] a leading global not–for–profit organization which provides education and certification for Information Security professionals. Greg was an officer of the board, currently serving a Treasurer and was the co–chair of the Foundation committee where he worked with the organization to develop and implement strategies which strive to empower members, and the communities where we live through information security research, education and awareness.

Kevin Henry 氏

Kevin Henry is recognized as one of the Leaders in the field of Information Security worldwide. He has been involved in computers since 1976 when he was an operator on the largest minicomputer system in Canada at the time. He has since worked in many areas of Information Technology including Computer Programming, Systems Analysis and Information Technology Audit. Following 20 years in the telecommunications field, Kevin moved to a Senior Auditor position with the State of Oregon where he was a member of the Governor’ s IT Security Subcommittee and performed audits on courts and court–related IT systems. The co–chair of the CBK for the CISSP and several other certifications, as well as an author with published articles in over ten books and magazines, Kevin is the principal of KMHenry Management Inc. and served until recently as the Head of Education for (ISC)2 and Vice President of ITPG, responsible for all educational systems, products and instructors for training programs. Currently Kevin is an Authorized Instructor for (ISC)2, ISACA, and BCI.