INSTITUTE of INFORMATION SECURITY

2018 年度後期　サイバーセキュリティ企業向け集中コース

「CSIRT 構築に向け～CT-5：実践サイバーレンジ演習」

IISEC Cyber-Security Corporate Training Course 2018:

“Capacity Building for CSIRT”

！IISEC の正規課程在学生と OBOG は本コース(CT-5)を優待受講料でご利用いただけます！

サイバーセキュリティ企業向け集中コース「CSIRT 構築に向けて」は、CSIRT の基礎講座、および CSIRT 活動に必要な豊富な技術演習をセットで開講する企業研修コースです。

- CT-5：実践サイバーレンジ演習（3 days, 15 units, 定員 20 名）　　（1 unit は約 90 分）

２０１８年度後期の CT1 から CT4 演習は全て終了しました。ご受講ありがとうございます。
２０１９年度前期の開講スケジュールは、近日、ご案内予定です。

- CT-1：CSIRT 構築の手引きコース（2 days, 8 units, 定員 20 名）
- CT-2：ネットワークセキュリティ技術演習（2 days, 8 units, 定員 20 名）
- CT-3：Web アプリケーション検査演習（2 days, 8 units, 定員 20 名）
- CT-4：デジタルフォレンジック演習（3 days, 12 units, 定員 20 名）

サイバーセキュリティ企業向け集中コース「CSIRT 構築に向けて」では、今後、企業等の CSIRT でご活躍予定の方だけでなく、一般企業で IT を統括されている部門のマネージャの方、社内ネットワークの運用管理部門の方、企業 Web システムの運用管理部門の方、特に、システムやセキュリティサービスの調達を担当されている方にも相応しい講義と演習を予定しています。

情報セキュリティ大学院大学
セキュアシステム研究所
所長　　後藤　厚宏

SSLab

■CSIRT 実践講座

CT-5：実践サイバーレンジ演習（3 days, 15 units）

- コース内容：サイバー攻撃に対応可能な実践的スキルを修得するための講義およびハンズオン演習を行います。初日は、演習環境についての講義や防御ツール・調査・分析ツールの解説および演習を、2 日目と 3 日目はサイバーレンジ（TAME Range）を用いて、実例に基づく攻撃シナリオによるリアルな防御演習を行います。
  下記のいずれかに該当する方の受講を想定しています。
  - ✧ CT-1 から CT-4 のいずれかを受講済の方
  - ✧ 企業等においてサイバー攻撃の対応にあたられている技術者、あるいは、CSIRT (Computer Security Incident Response Team)構成メンバー
  - ✧ ファイアウォールや IDS 等の運用経験者、Web サーバ管理経験者、Windows や Linux など OS の管理ツール（コマンド）操作経験者、マルウェア解析経験者
- 講義と演習環境
  - ✧ イスラエル IAI 社の訓練システム TAME Range を用いて仮想コンピュータ上に実際のサイバー攻撃を再現することにより、より実践的なサイバー攻撃に対する防御スキルを身につけることができます。
  - ✧ 講義と演習に必要な環境は会場に完備されています。
- 講座日程

［CT-5 実践サイバーレンジ演習］

日 程		時 限	内 容
2 月 6 日	水	09:00～10:30	演習環境上の仮想企業ネットワークについて
		10:40～12:10	防御ツールについて（解説と演習）
		13:00～14:30	調査・分析について（解説と演習）
		14:40～16:10	演習環境上のインシデントレスポンス演習①
		16:20～17:50	
2 月 7 日	木	09:00～10:30	演習環境上のインシデントレスポンス演習②
		10:40～12:10	
		13:00～14:30	
		14:40～16:10	
		16:20～17:50	
2 月 8 日	金	09:00～10:30	演習環境上のインシデントレスポンス演習③
		10:40～12:10	
		13:00～14:30	
		14:40～16:10	
		16:20～17:50	

◆講座・演習の教室

本学の演習室・講義室を予定しています。
情報セキュリティ大学院大学（横浜市神奈川区鶴屋町 2-14-1）
[アクセス] http://www.iisec.ac.jp/access/

◆申し込み方法と受講料のお支払い

1．受講申し込み：添付のフォームにて、メール添付でお申し込みください。

2．受講料

CT-5：実践サイバーレンジ演習* (3 days, 15 units)

一般　400,000 円／人（税込 432,000 円／人）

IISEC 学生・OB・OG 優待受講料 200,000 円／人（税込 216,000 円／人）

※　実践サイバーレンジ演習は大日本印刷株式会社が提供するイスラエル IAI 社の訓練システム Tame Range を使用します.

3．受講前の手続き：

(ア) 本学より計算書をご送付しますので、社印のある注文書を申込み期限までにお送りください。

(イ) 注文書受領後、本学より、受講登録完了のメール(受講案内)と受講料のご請求書をお送りします。ご請求額を請求書記載の銀行口座あてにお振込みください。なお、振込手数料はお振込者様にてご負担願います。

4．受講申込みの際の注意事項等

・注文書受領後のキャンセルは承ることができません。また、コースを欠席なさった場合でも、一旦納入された受講料は原則として返金できませんので、予めご承知おきください。

・申込締切日(開講 2 週間前)時点で最少開講人数に達しない場合、開講を中止させていただくことがございます。その際は速やかに申込代表者の方にご連絡させていただきます。

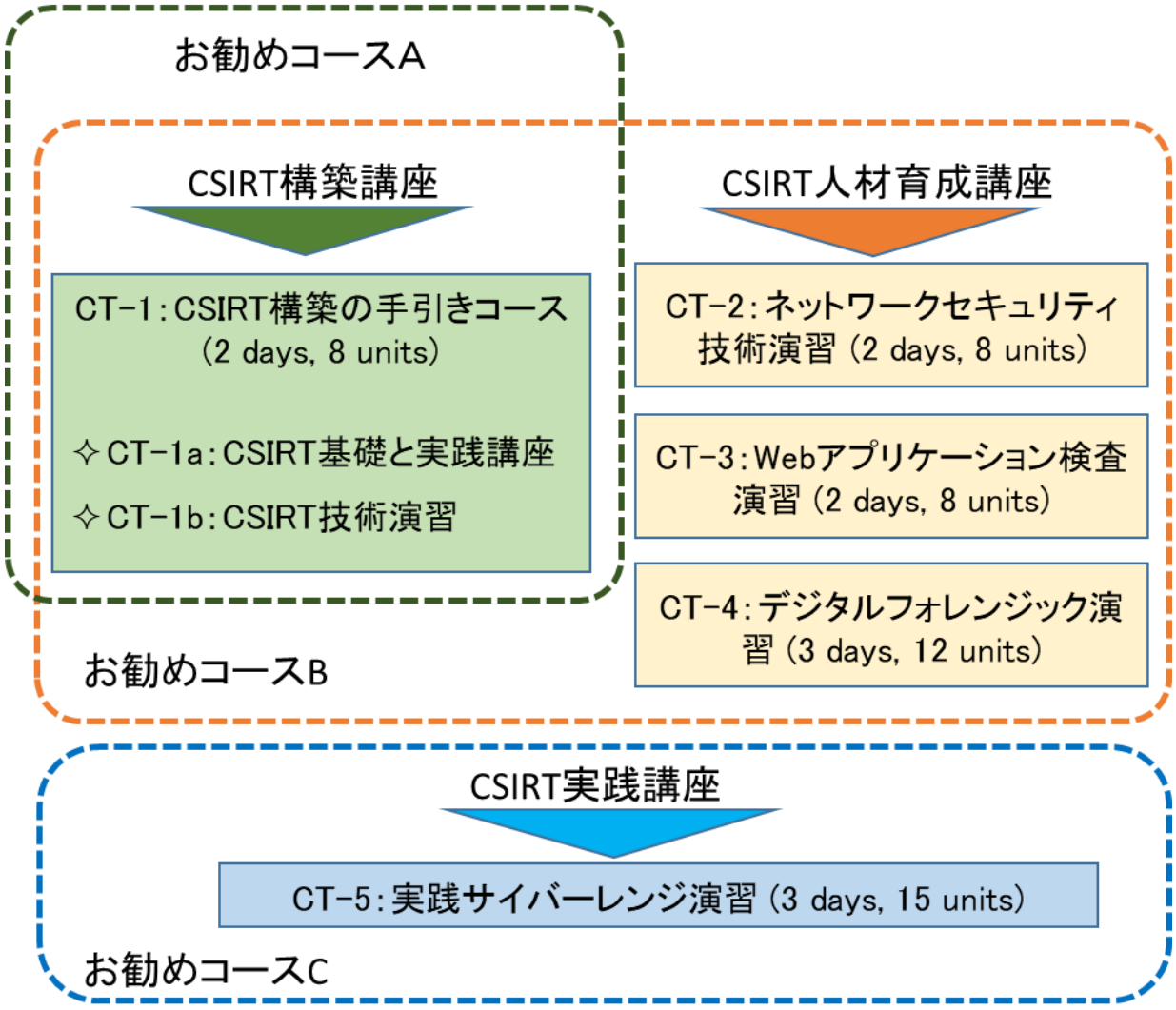
コース	申込締切日	開講日程	お支払期限
CT-5 (後期)	2019/1/26	2019/2/6, 2/7, 2/8	2019/3/末

【問い合わせ先】
情報セキュリティ大学院大学
セキュアシステム研究所
事務局
Email：ssl-info@iisec.ac.jp
Tel：045-410-0250

ご参考

◆コースの位置づけ

お勧めコースA: 社内CSIRT構築の企画担当の方
お勧めコースB: 社内CSIRTメンバを目指す方
お勧めコースC: CSIRTスキルの向上を目指す方



２０１８年度後期　終了コース

CT-1：CSIRT 構築の手引きコース（2 days, 8 units）　**２０１８年度後期　終了**

- コース内容：企業組織などでインシデント対応を担う企業内 CSIRT の基本的な役割と活動の考え方、企業を脅かす攻撃とその防御策について学ぶコースです。セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学びます。

CT-2：ネットワークセキュリティ技術演習（2 days, 8 units）　**２０１８年度後期　終了**

- コース内容： Web サーバ、メールサーバ等の設置・運用に際して必要となる基礎的なセキュリティ技術の習得を狙いとして、検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施します。

CT-3：Web アプリケーション検査演習（2 days, 8 units）　**２０１８年度後期　終了**

- コース内容： Web サーバの構築や運用に必要となる Web アプリケーションセキュリティ検査の知識および技術を習得し、独力で Web アプリケーションセキュリティ検査を実施し、その結果に応じて必要な対処を提案できる基礎スキルを身につけることを狙いとします。具体的には、脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施します。

CT-4：デジタルフォレンジック演習（3 days, 12 units）　**２０１８年度後期　終了**

- コース内容：インシデント発生後の対処に必要となるデジタルフォレンジック技術の基礎を習得することを狙いとします。具体的には、デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施します。