INSTITUTE of INFORMATION SECURITY

2021 年度前期 サイバーセキュリティ企業向け集中コース
「CSIRT 構築に向けて」

IISEC Cyber-Security Corporate Training Course 2021:
“Capacity Building for CSIRT”

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。
2021 年度前期は、Zoom を用いた遠隔オンライン開講といたします。

- **CT-1：CSIRT 構築の手引きコース** (2 days, 8 units)
  - ✧ CT-1a：CSIRT 基礎と実践講座　6 月 10 日(木)
  - ✧ CT-1b：CSIRT 技術演習　6 月 11 日(金)
- **CT-4：デジタルフォレンジック演習**　7 月 14 日(水)～7 月 16 日(金)　(3 days, 12 units)

(1 unit は約 90 分)

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。

なお、「ネットワークセキュリティ技術演習」(CT-2)と「Web アプリケーション検査演習」(CT-3)につきましては、企業様ごとの特別コースとして開講させていただきます。開講を希望される方は別途 SSL 事務局(E-mail：ssl-info@iisec.ac.jp)までご相談ください。

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 構築講座

CT-1：CSIRT 構築の手引きコース（2 days, 8 units）

● 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-1a：CSIRT 基礎と実践講座（4 units）

● 講義と演習環境

Zoom を使用して、オンラインで講義と演習を実施します。

● 主な講義・演習項目

- ✧ Unit 1: 企業におけるセキュリティリスクへの取組の基本、事故前提の活動、CSIRT の役割、CSIRT の活動例
- ✧ Unit 2: CSIRT ケーススタディ
- ✧ Unit 3: CSIRT インシデントハンドリングの基本
- ✧ Unit 4: CSIRT インシデントハンドリングの基礎演習

◇ CT-1b：CSIRT 技術演習（4 units）

● 講義と演習環境

Zoom を使用して、オンラインで講義と演習を実施します。なお、演習に必要な環境(演習用 VM イメージ)を事前に配布します。

● 主な講義・演習項目

- ✧ Unit 1：導入解説、攻撃手法のデモ（SQL インジェクション、クロスサイトスクリプティング）
- ✧ Unit 2：代表的な Web サーバ（Apache）のログの解説
  ログ解析演習 1（URL デコード）
  ログ解析演習 2（SQL インジェクション）と解説
- ✧ Unit 3：ログ解析演習 3（クロスサイトスクリプティング）と解説
  ログ解析演習 4（ディレクトリトラバーサル）と解説
- ✧ Unit 4：IDS/IPS 概説、セキュリティ診断概説、まとめ

■CSIRT 人材育成講座

CT-4：デジタルフォレンジック演習（3 days, 12 units）

● 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。

● 講義と演習環境

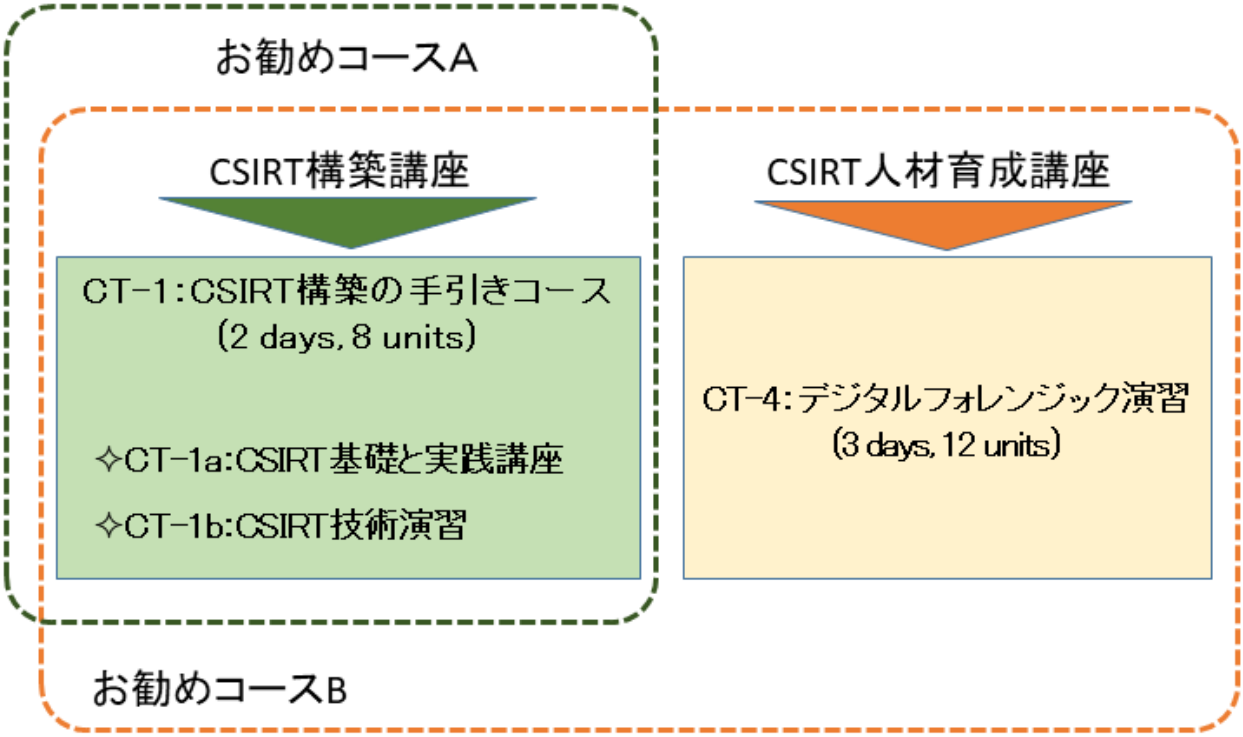
Zoom を使用して、オンラインで講義と演習を実施します。なお、演習に必要な環境(演習用 VM イメージ)を事前に配布します。本演習で解析対象とする端末 OS は Windows7 となります。

● 主な講義･演習項目

- ✧ デジタルフォレンジックに必要な知識と作業の流れ
- ✧ 各種オープンソース解析ツールの使い方
- ✧ 予備演習：Windows パソコン利用者が行った操作が明らかになっている状態で、その痕跡を調査
  - ファイルシステムのタイムスタンプ
  - レジストリ
  - イベントログ
  - Web アクセス履歴
  - USB デバイス接続履歴、等
- ✧ 解析演習：ある企業からの情報漏えいの原因、影響範囲等を解析
  - 情報漏えいの原因となった不正アクセス等の解析
  - 情報漏えい経路の解析
  - 不正アクセスに伴う影響範囲の解析、等
  - 解析結果報告書の作成
- ✧ まとめ

◆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



◆講座日程

[CT-1: CSIRT 構築の手引きコース]

日 程		時 限	内 容
6 月 10 日	木	◇CT-1a: CSIRT 基礎と実践講座	
		09:40～11:10	企業におけるセキュリティリスクへの取組の基本、事故前提の活動、CSIRT の役割、CSIRT の活動例
		11:20～12:50	ケーススタディ
		13:50～15:20	インシデントハンドリングの基本
		15:30～17:00	インシデントハンドリングの基礎演習
6 月 11 日	金	◇CT-1b: CSIRT 技術演習	
		09:40～11:10	導入解説、攻撃手法のデモ(SQL インジェクション、クロスサイトスクリプティング)
		11:20～12:50	代表的な Web サーバ(Apache)のログの解説 ログ解析演習 1 (URL デコード) ログ解析演習 2 (SQL インジェクション)と解説
		13:50～15:20	ログ解析演習 3 (クロスサイトスクリプティング)と解説 ログ解析演習 4 (ディレクトリトラバーサル)と解説
		15:30～17:00	IDS/IPS 概説、セキュリティ診断概説、まとめ

[CT-4: デジタルフォレンジック演習]

日 程		時 限	内 容
7 月 14 日	水	09:40～11:10	・デジタルフォレンジックに必要な知識と作業の流れ ・各種オープンソース解析ツールの使い方 ・予備演習: Windows パソコン利用者が行った操作が明らかになっている状態で、その痕跡を調査 – ファイルシステムのタイムスタンプ – レジストリ – イベントログ – Web アクセス履歴 – USB デバイス接続履歴、等 ・解析演習: ある企業からの情報漏えいの原因、影響範囲等を解析 – 情報漏えいの原因となった不正アクセス等の解析 – 情報漏えい経路の解析 – 不正アクセスに伴う影響範囲の解析、等 – 解析結果報告書の作成 ・まとめ
		11:20～12:50	
		13:50～15:20	
		15:30～17:00	
7 月 15 日	木	09:40～11:10	
		11:20～12:50	
		13:50～15:20	
		15:30～17:00	
7 月 16 日	金	09:40～11:10	
		11:20～12:50	
		13:50～15:20	
		15:30～17:00	

◆申し込み方法と受講料のお支払い

1. 受講申込みについて

添付のフォームにて、メール添付でお申込みください。
または以下、情報セキュリティ大学院大学 セキュアシステム研究所(SSL)の企業向け集中コースご案内ページより「受講申込書」をダウンロードし、必要事項をご入力の上、メール添付で SSL 事務局(Email:ssl-info@iisec.ac.jp)宛てにお送りください。

[企業向け集中コースご案内] https://www.iisec.ac.jp/sslab/courses.html

2. 受講料

CT-1：CSIRT 構築の手引きコース（2 days, 8 units) 66,000 円／人（税込）
CT-4：デジタルフォレンジック演習（3 days, 12 units) 99,000 円／人（税込）

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、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-1	2021/5/27	2021/6/10, 6/11	2021/7/末
CT-4	2021/6/30	2021/7/14, 7/15, 7/16	2021/8/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