2025 年 4 月

【東大用】

enPiT-Security “SecCap コース” 資料一覧

資料 1： enPiT-Security(SecCap コース)の概要

資料 2-1：2025 年度 SecCap 科目および実践演習モジュールリスト(情セ大開講分)

資料 2-2：2025 年度 SecCap 東京大学指定 基礎科目リスト

資料 3： SecCap 参加について

資料 4-1：2025 年度 SecCap 他連携大学開講科目リスト

資料 4-2：2025 年度 SecCap 他連携大学開講科目概要

資料 5： SecCap 参加登録申請書サンプル

(SecCap 参加登録申請)

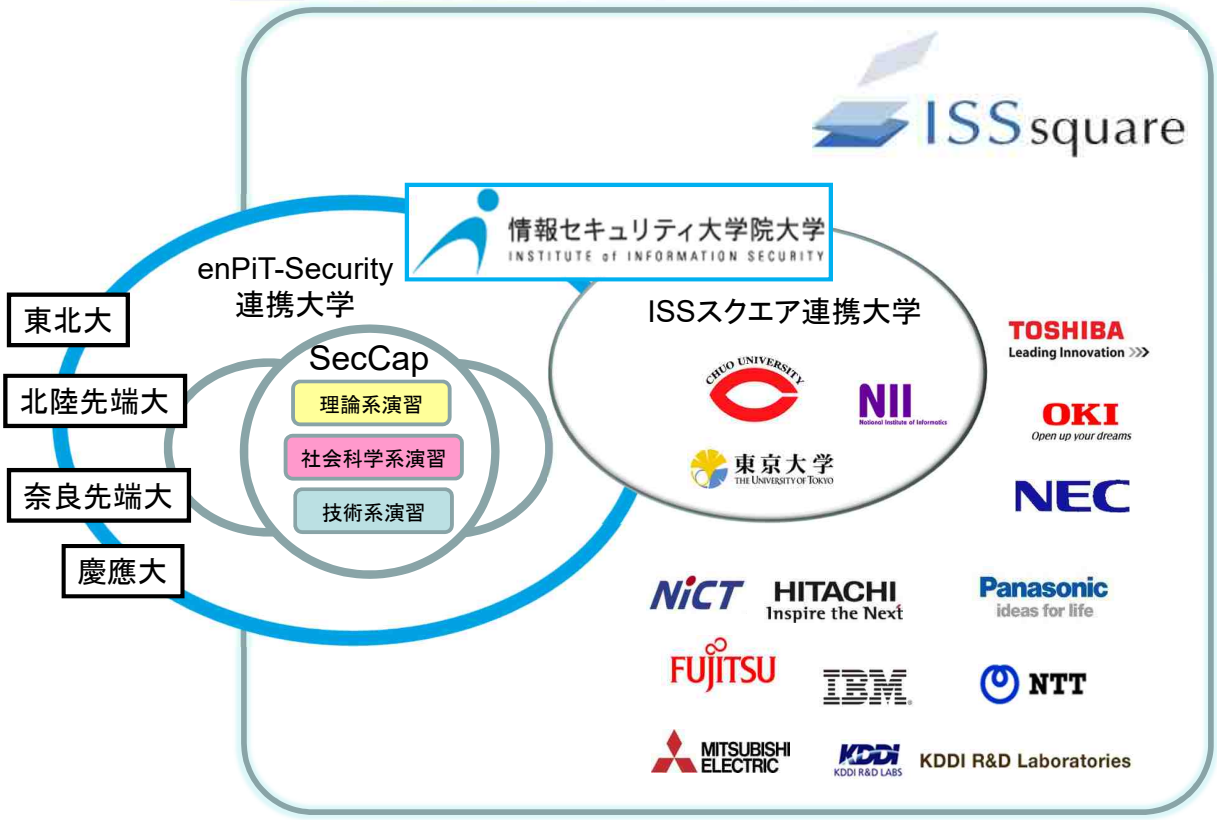
●SecCap 参加登録申請書

2025年度 SecCap資料

enPiT-Security（SecCapコース）の概要

情報セキュリティ大学院大学

ISSスクエアとenPiT-Security



実践セキュリティ人材プログラムenPiT-Security

SecCap

- 実践セキュリティ人材
  - 社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を，技術面・管理面で牽引できる実践リーダー
- enPiT-Security
  - 文科省 「情報技術人材育成のための実践教育ネットワーク形成事業: 分野・地域を越えた実践的情報教育協働NW」のセキュリティ分野の取組みとしてスタート（平成24年10月～平成29年3月）
- 平成29(2017)年度からは5連携大学の自主的な取組みとして継続

  情報セキュリティ大学院大学、東北大学

  北陸先端科学技術大学院大学、奈良先端科学技術大学院大学

  慶應義塾大学

enPiT-Security：SecCapコース

SecCap

- 実践力の育成：5つの連携大学が協力して開講する実践セキュリティ人材の育成コース（**SecCap**）によって，幅広いセキュリティ分野の最新技術や知識を具体的に体験を通して習得
- 幅のあるコース：技術的な知識，例えば，暗号をベースとする情報セキュリティ技術，Webサーバのセキュリティ技術，ネットワークセキュリティ技術から，法制度やリスク管理などの社会科学的な知識までをカバー
- キャリアデベロップメント：受講生は，技術系，理論系，社会科学系の講義や実践演習から，それぞれが目指すキャリアパスに沿った割合で，主体的・自主的に調合した学習プログラムを作って受講.

SecCapコースのカリキュラム（2025年度）

SecCap

基礎知識学習

共通科目（必修）：情報セキュリティ特別講義

基礎科目：所属大学指定科目

実践演習科目

（情セ大　開講）
- 特設実習（セキュリティ実践Ⅰ）
- 特設実習（セキュリティ実践Ⅱ）
  - I-01: NWとWebアプリのセキュリティ検査と対策演習
  - I-02: デジタルフォレンジック演習
  - I-03: Capture The Flag（CTF）入門と実践演習
  - I-04: インシデント対応とCSIRT基礎演習

（他連携大学で開講予定）
- 無線LANセキュリティ演習
- システム攻撃・防御演習
- インシデント対策基礎・応用
- リスクマネジメント演習
- ハードウェアセキュリティ演習
- IT危機管理演習
- モバイルアプリの脆弱性とその対策

先進科目

（情セ大　開講）
- 実践的IoTセキュリティ
- 特設講義（データ・サイエンスとアナリティクス）

（慶應大　開講）
- 情報セキュリティ技術特論1, 2

（東北大　開講）
- 情報セキュリティ法務経営論

その他の活動

企業インターンシップ

交流ワークショップ

enPiT-Security：SecCapの修了認定

SecCap

■ SecCap修了認定：大学院修士（単位認定）
- 共通科目：2単位
- 実践演習 and/or 先進科目：4単位
- 基礎科目：4単位（所属大学指定科目の中から選択）

SecCap6

■ SecCap10：“Security Specialist ”認定

SecCap受講生が1年間で、以下を取得できた場合は「SecCap10」を授与し、“Security Specialist”として認定する。
- 共通科目：2単位
- 実践演習 and/or 先進科目：8単位
- 基礎科目：4単位（所属大学指定科目の中から選択）

SecCap10

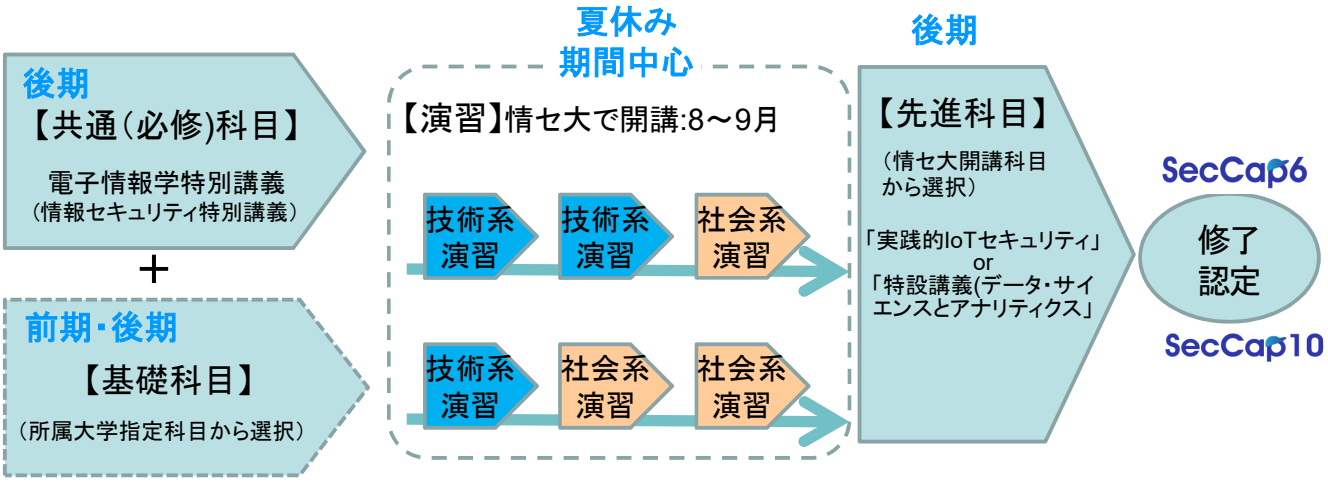
Security Specialist

SecCapコースの実践演習の選択

受講生が目指すキャリアパスに向けて，技術系，
社会科学系の実践演習を主体的に選択

共通(必修)科目（2単位）
& 基礎科目（4単位）
（基礎力）

実践演習科目 and/or 先進科目（4単位以上）
（実践力・応用力）



今後の予定

- 2025年4月16日(水): SecCap参加登録申請書提出期限
  【提出先】
  東京大学 学務課大学院チーム 情報理工担当(工学部8号館1階)

※ 情セ大にて参加登録申請書を受領後、SecCap演習の登録調整有り

※ 後期開講の先進科目「実践的IoTセキュリティ」は、演習機材数の制約により受入れ制限があり、10月半ばの情セ大後期履修登録期限後に他大学からの履修希望者の受入れ可否が決定することとなる。
SecCap修了認定を目指す学生は、本科目以外の演習・先進科目により、修了認定要件を満たせるよう登録申請することを勧める。

- 2025年5月中旬:SecCapコース登録内容確認票配布（予定）
- 2025年夏季:SecCap実践演習の実施
- 2026年3月:SecCap修了認定

（資料2-1）
2025.3.14版

【情セ大】2025年度 SecCap科目および実践演習モジュールリスト(予定)

種別	科目名	設置大学院	担当教員	単位数	時期	日程(予定)	時間帯	開講場所	他大学受け入れ可否(定員)	備考
共通必修	情報セキュリティ特別講義	情セ大	須崎・後藤	2	後期	10/1～ (15回)	水曜 5限 (18:20-19:50)	情セ大	○(ー)	連携大学の拠点に配信予定

種別	科目名	実践演習モジュール名	設置大学院	担当教員	単位数	時期	日程(予定)	時間帯	開講場所(※)	他大学受け入れ可否(定員)	備考
実践演習	特設実習(セキュリティ実践Ⅰ) (2単位) および 特設実習(セキュリティ実践Ⅱ) (2単位)	I-01 NWとWebアプリのセキュリティ検査と対策演習	情セ大	種茂　他	1相当	通年	8/16(土),17(日),18(月),19(火)	9:00-16:10	情セ大	○(10)	
		I-02 デジタルフォレンジック演習	情セ大	種茂　他	1相当		9/20(土),21(日),27(土),28(日)	9:00-16:10	情セ大	○(10)	
		I-03 Capture The Flag (CTF)入門と実践演習	情セ大	宮本	1相当		8/9(土) +実CTF競技会での実践	9:00-16:10	情セ大他	○(10)	
		I-04 インシデント対応とCSIRT基礎演習	情セ大	種茂　他	1相当		9/4(木),5(金),8(月),9(火)	9:00-16:10	情セ大他	○(10)	

(※)オンサイト開講を予定。社会情勢により変更の可能性あり。

種別	科目名	設置大学院	担当教員	単位数	時期	日程・時間帯(予定)		開講場所(※)	他大学受け入れ可否(定員)	備考
先進科目	実践的IoTセキュリティ	情セ大	須崎・荻野	2	後期	10/6～(15回)	月曜　5限 (18:20-19:50)	情セ大	受入制限あり。10月半ば以降受入可能数確定	
	特設講義(データ・サイエンスとアナリティクス)	情セ大	髙橋	2	後期	10/3～(15回)	金曜　6限 (20:00-21:30)	情セ大	○(10)	

(※)オンサイト開講を予定。社会情勢により変更の可能性あり。

種別	授業科目名	設置大学院	教員	単位	時期	曜日・時限(予定)	開講場所	他大学受け入れ可否(定員)	備考
基礎科目	ネットワーク設計とセキュリティ運用	情セ大	後藤・種茂	2	前期	月　6限	情セ大	ISSスクエア扱い	
	セキュリティシステム監査	情セ大	堀江・丸山	2	前期	土　2限	情セ大	ISSスクエア扱い	
	リスクマネジメントと情報セキュリティ	情セ大	後藤・桑名・藤澤	2	前期	木　5限	情セ大	ISSスクエア扱い	
	セキュアシステム構成論	情セ大	辻	2	後期	木　6限	情セ大	ISSスクエア扱い	
	暗号プロトコル	情セ大	土井	2	後期	火　2限	情セ大	ISSスクエア扱い	
	セキュア法制と情報倫理	情セ大	村上・小林(良)	2	後期	火　4限	情セ大	ISSスクエア扱い	
	セキュアプログラミングとセキュアOS	情セ大	柴山	2	後期	木　5限	情セ大	ISSスクエア扱い	
	サイバーセキュリティ技術論	情セ大	森井	2	後期	土(10/4～隔週)　3-4限	情セ大	ISSスクエア扱い	

【本件に関するお問合せ先】情セ大 SecCap担当(iisec@seccap.jp)

SecCap（東大用）

（資料2-2）
2025/3/14

■2025年度 SecCap 基礎科目リスト(東京大学指定科目)

2025年度 SecCapコース 東京大学開講 基礎科目(所属大学指定科目)

授業科目名	時期	曜日・時限	単位	担当教員	設置大学院
ネットワークアーキテクチャ（隔年開講）	S1S2	火3	2	瀬崎　薫	東大
アドバンスト・コンピュータアーキテクチャ（隔年開講）	S1S2	水4	2	入江　英嗣	東大
先端機械学習（隔年開講）	S1S2	月2	2	鈴村　豊太郎	東大
情報セキュリティ事例特論(隔年開講）	S1S2	木2	2	山口　利恵 越前　功	東大
ウェブ工学（隔年開講）	A1A2	月4	2	豊田　正史	東大
計算機言語システム論（隔年開講）	A1A2	火3	2	小林　直樹	東大
ワイヤレス通信工学(隔年開講）	A1A2	火3	2	杉浦　慎哉	東大
現代暗号理論（隔年開講）	A1A2	水2	2	高木　剛	東大
サイバーセキュリティ実践論（毎年開講）	A1A2	集中	2	関谷　勇司	東大
情報理工学連携講義II（毎年開講）	A2	金5	1	高橋　健太	東大

※以下、2025年度情報セキュリティ大学院大学開講の基礎科目からも選択可能。但し情セ大にて受講(遠隔配信はなし)

授業科目名	時期	曜日・時限	単位	担当教員	設置大学院
ネットワーク設計とセキュリティ運用	前	月　6限	2	後藤・種茂	情セ大
セキュリティシステム監査	前	土　2限	2	堀江・丸山	情セ大
リスクマネジメントと情報セキュリティ	前	木　5限	2	後藤・桑名・藤澤	情セ大
セキュアシステム構成論	後	木　6限	2	辻	情セ大
暗号プロトコル	後	火　2限	2	土井	情セ大
セキュア法制と情報倫理	後	火　4限	2	村上・小林(良)	情セ大
セキュアプログラミングとセキュアOS	後	木　5限	2	柴山	情セ大
サイバーセキュリティ技術論	後	土(10/4～隔週)　3-4限	2	森井	情セ大

（資料 3）

2025/4/1
IISEC

SecCap 参加について（補足説明）

1. 全体～共通要件・注意事項など～

A) “SecCap 修了認定”の要件

SecCap 受講生が 1 年間または 2 年間で所定の単位を取得できた場合は、年度末に SecCap 修了認定証を授与する。

1. 共通科目(必修)：2 単位
2. 実践演習科目 and/or 先進科目：計 4 単位
3. 基礎科目：4 単位（所属大学指定科目の中から選択）

B) SecCap10：“Security Specialist”認定の要件

SecCap 受講生が 1 年間で修了認定要件を満たし、かつ実践演習科目 and/or 先進科目で 8 単位以上を取得した場合は「SecCap10」を授与し、“Security Specialist”として認定する。

C) 履修申請時期について

- 通年科目(実践演習)、前期開講基礎科目、後期開講の共通科目、先進科目、および基礎科目ともに前期に履修申請（SecCap 参加登録申請書を提出）すること。

D) SecCap 提供科目を履修した場合の単位の扱い

- 情セ大及び他連携大学で開講される SecCap 提供科目を受講した場合、取得単位は SecCap 修了認定に反映される。
- SecCap プログラムにおける取得単位が、所属大学の課程修了所要単位として認められるかどうかについては所属大学(貴学 学務課大学院チーム 情報理工担当)に確認すること。

E) 実践演習の履修取止め

やむを得ず、履修できなくなった演習が生じた場合は、開講日の 1 週間前までに連絡すること。

連絡先：情セ大 SecCap 担当（iisec@seccap.jp）

F) やむを得ず、演習、先進科目を欠席する場合は、授業開始前までに連絡すること。

連絡先：情セ大 SecCap 担当（iisec@seccap.jp）

2. 情セ大開講の SecCap 実践演習科目の履修申請

A) 情セ大開講の SecCap 実践演習科目

- 特設実習（セキュリティ実践Ⅰ）、特設実習（セキュリティ実践Ⅱ）を開講する。ともに、情セ大開講の演習モジュールのみを対象とする。

B) 演習モジュール履修申請の際の注意

- I-01～I-04 の各演習モジュールは 1 単位相当である。よって、特設実習（セキュリティ実践Ⅰ）の 2 単位を取得するためには 2 モジュール、特設実習（セキュリティ実践Ⅰ）および特設実習（セキュリティ実践Ⅱ）の各 2 単位（計 4 単位）を取得するためには、4 モジュールの履修が必要となる。また 1 モジュールのみ履修することはできない。

C) 定員について

- 各演習モジュールには、機材の制約等から定員を設ける。希望者が定員を上回った場合は、選考を行う。選考の結果、受講できない演習または演習モジュールが生じた場合は、別途相談する。

D) 成績評価について

- 演習モジュール毎に成績を評価し、その成績を合算して成績とする。なお、3 モジュール以上の演習を受講した場合、その中で成績の上位から 2 つずつを合算する。
  - 特設実習（セキュリティ実践Ⅰ）の成績：成績上位 1 番目＋2 番目
  - 特設実習（セキュリティ実践Ⅱ）の成績：成績上位 3 番目＋4 番目

3. 他連携大学開講の SecCap 実践演習科目の履修申請

A) 演習科目毎に定められている受講条件、受講場所を確認して申請(SecCap 参加登録申請書を提出）すること。

B) 事前に貴学 学務課大学院チームを通して、情セ大 SecCap 担当宛てに参加申請について相談することを勧める。

以上

【本件に関するお問合せ先】情セ大 SecCap 担当(iisec@seccap.jp)

SecCap

（資料4-1）
2025/3/18

2025年度　他連携大学開講のSecCap実践演習モジュールリスト（情セ大学生が受講できるもの）※但し、人数制限あり

ID	科目名	実践演習モジュール名	設置大学院	担当教員	単位数	時期	日程（予定）	時間帯	受講場所
N-01	情報セキュリティ演習A	インシデント対策基礎・応用	NAIST	門林 他	1	集中	9/24～26		NAIST
N-02	情報セキュリティ演習B	ハードウェアセキュリティ演習	NAIST	林 他	1	集中	8/25～8/27		NAIST
N-03	情報セキュリティ演習C	IT危機管理演習	NAIST	藤川 他	1	集中	9/15～9/17（予定）		NAIST
K-01	セキュリティPBL演習 A	無線LANセキュリティ演習	慶應大	砂原	1	集中	夏季集中(予定)	9:00-18:00（予定）	慶應（日吉）
K-02	セキュリティPBL演習 B	システム攻撃・防御演習	慶應大	砂原	1	集中	夏季集中(予定)	9:00-18:00（予定）	慶應(日吉)
K-03	セキュリティPBL演習 C	リスクマネジメント演習	慶應大	砂原	1	集中	夏季集中(予定)	9:00-18:00（予定）	慶應(日吉),都内
K-04	セキュリティPBL演習 I	モバイルアプリの脆弱性検出とその対策	慶應大	砂原	1	集中	夏季集中(予定)	9:00-18:00（予定）	慶應(日吉)

2025年度　他連携大学開講のSecCap先進科目リスト（情セ大学生が受講できるもの）

ID	科目名	設置大学院	担当教員	単位数	時期	日程（予定）	時間帯	受講場所
K-1	情報セキュリティ技術特論1	慶應大	砂原 他	1	春学期	5/30、6/6、6/20、7/4(予定)	14:00-17:10	慶應（日吉）[遠隔あり]
K-2	情報セキュリティ技術特論2	慶應大	砂原 他	1	秋学期	調整中	金曜日 14:00-17:10	慶應（日吉）[遠隔あり]
(注意) K-1,K-2は片方のみの登録はできません。必ず前期に両方履修登録申請してください。								
TH	情報セキュリティ法務経営論	東北大	樋地・中村・高谷	2	後期	10/1～（15回）	16:20-17:50（予定）	オンライン受講（予定）

※ 情セ大以外の学生が上記科目の受講を希望する場合は、別途、各設置大学院との協定が必要です。

【本件に関するお問合せ先】情セ大 SecCap担当(iisec@seccap.jp)

SecCap

他連携大学開講のSecCap 実践演習・先進科目概要(情セ大学生が受講できる科目)

＜実践演習＞

ID	科目名	実践演習モジュール名	設置大学院	概　要
N-01	情報セキュリティ演習A	インシデント対策基礎・応用	NAIST	情報セキュリティ運用リテラシーIで得られた基本的な実践力をもとに、さらなる応用、適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバーで構成されたグループ内で議論を展開させ、理解を深める。 (内容) 〇インシデント対策基礎 セキュリティ対策が求められる具体的な組織を想定し、様々なインシデント発生とそれに付随するインシデント対応を模擬的に経験することにより、インシデント対応における具体的な役割分担、ならびに取りうるアクションについて体験的に学ぶ。 〇インシデント対策応用 セキュリティ管理策が欠けている具体的なネットワーク型情報システムを複数想定し、それぞれに対して考えうる様々な脅威の種類を演習ツールを用いて繰り返し検討することにより、脅威モデルの考え方、およびセキュリティ管理策の網羅性の検討方法について体験的に学ぶ。 〇インシデント対策まとめ ネットワーク型情報システムに対する標的型攻撃と、それに対するセキュリティ管理策の有効性を演習ツールを用いて繰り返し検討することにより、多様かつ多段にわたる標的型攻撃の性質、対策の考え方、ならびに個々の標的型攻撃に対するセキュリティ管理策の実効性について体験的に学ぶ。
N-02	情報セキュリティ演習B	ハードウェアセキュリティ演習	NAIST	情報通信機器などのハードウェアから情報漏えいが生じるメカニズムを学び、実験を通して物理的セキュリティに関する問題に対する理解を深め、ハードウェアセキュリティ対策の重要性を学ぶ。 (内容) 〇ハードウェアセキュリティ概要 ハードウェアセキュリティの概要を説明するとともに、コンピュータハードウェアとその動作原理を解説する。また、ハードウェア動作中に生じる消費電力や電放射磁波の計測の演習を行う。 〇公開鍵暗号に対するサイドチャネル攻撃とその対策 暗号アルゴリズムの基礎を解説するとともに、暗号アルゴリズムのハードウェア実装を行う。また、公開鍵暗号に対するサイドチャネル解析とその対策に関する演習を行う。 〇共通鍵暗号に対するサイドチャネル攻撃とその対策 共通鍵暗号に対するサイドチャネル解析とその対策に関する演習を行う。最後に、ハードウェアセキュリティに関する発表と議論を行う。
N-03	情報セキュリティ演習C	IT危機管理演習	NAIST	情報セキュリティ運用リテラシーIで得られた基本的な実践力をもとに、さらなる応用、適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバーで構成されたグループ内で議論を展開させ、理解を深める。また、習得した知識の理解度を評価するために、セキュリティコンテストあるいはCTF大会へ参加する場合もある。 *各回の授業内容は未定
K-01	セキュリティPBL演習A	無線LANセキュリティ演習	慶應大	無線LANにおけるセキュリティ対策の現状を把握し、より安全に無線LANを利用するための対策を検討する。具体的には、無線LANで使用されているプロトコルおよびセキュリティ技術について概観し、SSIDを公表せずWEP暗号化を行い、MACアドレスによる制限を行うアクセスポイントへの侵入やDoS攻撃を試みる。最終的に、実験結果をもとに安全な無線LANを運用するための方法についてグループごとに議論、考察する。
K-02	セキュリティPBL演習B	システム攻撃・防御演習	慶應大	脆弱性のあるシステムをインターネットに接続した場合、どのように攻撃されるのか、攻撃に対してどのように防御するのか等について理解する。具体的には、システムの攻撃によく利用される脆弱性や攻撃の原理、防御技術について概観し、実際の攻撃ツールを解析し、その原理を学ぶ。最終的に、実験結果をもとに安全なシステム運用の手法についてグループごとに議論、考察する。
K-03	セキュリティPBL演習C	リスクマネジメント演習	慶應大	情報セキュリティの現場において、予防対策や不正アクセス事故発覚時の対処(情報収集、関係各所との連携等)について実践に即して学ぶ。本演習で扱うウィルス検体は、サイバークリーンセンターデータセット(CCC Datasets)等を利用して行う。このため、x86機械語について理解している必要がある。また、情報セキュリティに関係する企業、組織見学会も併せて実施し、現場を実際に見ることで、セキュリティ問題意識を高める。
K-04	セキュリティPBL演習I	モバイルアプリの脆弱性検出とその対策	慶應大	モバイルアプリの開発が手軽に出来るようになった一方で脆弱性のあるモバイルアプリも散見される。本演習ではJavaのコードをツールを用いて解析し、モバイルアプリの脆弱性を見つけその対策について考察する。また、実際に対策を行ったアプリとそうでないアプリとの動作比較などを通してセキュアコーディング 手法などについて理解するとともにセキュリティに関する問題意識を高める。 本演習の受講はJavaについて理解している必要がある。

＜先進科目＞

設置大学院	科目名	概　要
慶應大	情報セキュリティ技術特論1	本科目は、SecCapコースに関連するインターネット、暗号、ポリシー、マネージメントなどの各分野の第一線で活躍する有識者をお招きし、最新事情について学ぶ。受講者は、個別に専門的な知識を習得するだけでなく、幅広い分野の情報を得ることで総合的に問題を考える能力を養う。 授業計画(予定)： 実際のインターネットの姿, 暗号技術の基礎, 位置情報とプライバシ, DNSとそのsecurity 等
	情報セキュリティ技術特論2	本科目は、SecCapコースに関連するインターネット、暗号、ポリシー、マネージメントなどの各分野の第一線で活躍する有識者をお招きし、最新事情について学ぶ。受講者は、個別に専門的な知識を習得するだけでなく、幅広い分野の情報を得ることで総合的に問題を考える能力を養う。 授業計画(予定):オープンソースライセンスの基礎と実務, 個人情報保護と匿名加工, プライバシー保護と匿名化, 内部統制とIT内部統制
東北大	情報セキュリティ法務経営論	変動著しい現代の情報社会において 情報セキュリティは、さまざまな面でますます重要になってきている。取り扱う情報の量の増加と質の多様化は情報セキュリティに技術的な広がりをもたらすと同時に、社会制度や法律との関係においても新たな問題を生じさせている。さらに、組織や社会に情報セキュリティを定着させるには、経済的合理性や組織マネジメントも不可欠である。本講義は、情報セキュリティ技術を組織の中で利用するために必要な社会的側面を説明できる能力の習得を目的とする。そのために本講義は、情報セキュリティを導入し定着させるために必要な経営上の意思決定方法について説明を行う。

【本件に関するお問合せ先】情セ大 SecCap担当(iisec@seccap.jp)