第7分科会

情報セキュリティ教育
―教養教育として、専門教育として―

報告者

桝田　秀夫　京都工芸繊維大学　情報工学・人間科学系／情報科学センター　教授

上原哲太郎　立命館大学　情報理工学部　教授

秋山　豊和　京都産業大学　コンピュータ理工学部　准教授

平山　敏弘　NPO日本ネットワークセキュリティ協会（JNSA）　教育部会　部会長

コーディネーター

藤田　和弘　龍谷大学　理工学部　教授

【参加者　28名】

教養教育としての情報セキュリティ教育について、15 年前から「情報セキュリティと情報倫理」を開講されている京都工芸繊維大学からご報告いただき、その後、専門教育としての情報セキュリティ教育に関して立命館大学および京都産業大学からご報告いただく。

また、社会が求める情報セキュリティ教育として JNSA からご講演いただく。講演の後、分科会への参加者を交えて、情報セキュリティ教育の学習・教育到達目標に関して議論を行う。

第7分科会

情報セキュリティ教育
―教養教育として、専門教育として―

龍谷大学　理工学部　教授　藤田　和弘

１．企画概要

毎日、仕事でパソコンやタブレットを使い、メールやSNSなどで情報をやりとりすることが当たり前となっています。また、一方で、情報漏えい、不正アクセス、そして、標的型攻撃メールなどの情報セキュリティに関する事件のニュースを目にしない日は無いといっていい状況となっています。

大学は高等教育機関として、学生を教育し社会へ送り出していますが、社会人となった学生が、職場、家庭、そして地域社会において情報機器を用いて情報処理や情報のやりとりをする上で、十分な情報セキュリティの知識を持っていることが重要です。Windows updateを知らない学生はさすがにいないとしても、某社が発行した証明書に対する、あるWebブラウザでの一部無効化などについてわかっている学生は少ないのではないかと思われます。情報系の専門教育を受けていない学生でも、一定の情報セキュリティの知識は必要であると考えています。

また、経済産業省「IT人材の最新動向と将来推計に関する調査結果」（平成28年６月10日）では、IT企業及びユーザ企業（産業界全体）で2020年には、情報セキュリティ人材が約19.3万人不足するという試算となっていることから、今後、情報セキュリティ人材の育成が重要であることがわかります。政府の政策的な取り組みとて、平成29（2017）年４月に、「情報処理安全確保支援士」制度が施行され、平成29（2017）年10月現在、6,994名が登録されています。このような社会的な状況で、IT企業及びユーザ企業において情報セキュリティ技術者の役割は重要であり、大学における専門教育として情報セキュリティ技術者を育成することは、重要であると考えています。

以上のような発想のもとに、この第７分科会では、大学における教養教育としての情報セキュリティ教育と専門教育としての情報セキュリティ教育について、意見交換をする場を提供したいと考えました。

教養教育としての情報セキュリティ教育に関して、京都工芸繊維大学情報科学センターの桝田秀夫教授にご講演をお願いしました。京都工芸繊維大学では、早くから全学的な教養教育としての情報セキュリティ教育に取り組んでおられます。具体的には、平成16（2004）年度より、情報科学センター設置に伴い配置された専任教員による全学の教養教育科目として「情報セキュリティと情報倫理」を開講されています。そこで、京都工芸繊維大学情報科学センターの桝田秀夫教授に、「情報セキュリティと情報倫理」の授業内容と授業運営についてご講演をお願いしました。同科目では、can do形式の12の学習目標を設定されています。

つぎに、専門教育としての情報セキュリティ教育として、おふたりにご講演をお願いしました。立命館大学情報理工学部では、コース制をとりいれられ、その中の「セキュリティ・ネットワークコース」を担当されている上原哲太郎教授に、専門教育としての情報セキュリティ教育について、ご講演をお願いしました。また、京都産業大学のコンピュータ理工学部は、平成30（2018）年４月に情報理工学部に改組され、コース制をとりいれられ、その中の「情報セキュリティコース」を担当される秋山豊和准教授にも、専門教育としての情報セキュリティ教育について、ご講演をお願いしました。



つぎに、社会が求める情報セキュリティ教育として、NPO日本ネットワークセキュリティ協会教育部会長の平山敏弘氏にご講演をお願いしました。ネットワークセキュリティ製品を提供しているベンダー、システムインテグレータ、インターネットプロバイダーなどネットワークセキュリティシステムに携わるベンダーが中心となりネットワークセキュリティの必要性を社会にアピールし、諸問題を解決するために、NPO日本ネットワークセキュリティ協会（JNSA）が2001年に設立されています。このJNSA

には教育部会があり、社会のニーズや時代の変化に適合したセキュリティ人材育成のために必要とされる知識・技能等の検討を行い、情報セキュリティ教育のコンテンツとして、シラバスや講義資料およびSecBoKを作成するとともに教育界・産業界への展開・使用を促進することで、情報セキュリティ人材の育成に貢献されています。

２．分科会当日のスケジュール

分科会の進め方としては、まず、コーディネーターからこの分科会の開催趣旨の説明をした後、講師にご講演いただき、その後、グループワークを行いました。

10：00-10：03　開催趣旨の説明
10：03-10：42　京都工芸繊維大学情報科学センター桝田秀夫教授のご講演
10：42-11：21　立命館大学情報理工学部上原哲太郎教授のご講演
11：21-12：00　京都産業大学コンピュータ理工学部秋山豊和准教授のご講演
12：00-13：30　昼休み
13：30-14：10　JNSA教育部会平山敏弘部会長のご講演
14：10-15：30　質疑応答およびグループワーク

３．分科会の概要

教養教育としての情報セキュリティ教育に関して、京都工芸繊維大学情報科学センターの桝田秀夫教授に、全学共通科目である「情報セキュリティと情報倫理」（１年次後期）についてご講演いただきました。この科目は、2004年度より開講されていて、2016年度まではサラ・バーズ著「IT社会の法と倫理」（桐原書店）および情報処理推進機構編著「情報セキュリティ読本 IT時代の危機管理入門」（実教出版）を参考書とし、2017年度からは山田恒夫編著「情報のセキュリティと倫理」（放送大学教育振興会）を参考書として、「情報社会への参画」、「情報とプライバシー」、「コンピュータの信頼性」、「コンピュータ犯罪」、「日本における法整備」、「ソフトウェアなどの知的財産保護」、「ネットワークセキュリティ技術」、「サイトセキュリティ技術」、「OS/言語処理系とセキュリティ技術」、「暗号技術と認証技術」、「ウィルスと不正アクセス技術」、「情報セキュリティマネージメント」、「専門家の倫理と責任」を扱っておられるとのことでした。あくまでも全学向けの授業であることを念頭に、前半が主に倫理的な話と技術の概論、後半が技術の詳細、最後が倫理の広範な話題としているとのことでした。授業展開としては、ほぼ毎回の授業でミニレポートの課題をだされたり、レポート課題を３回だされるなど、非常にていねいな授業展開をされているとのことでした。受講状況としては、最初の年度である2004年度が、入学定員に対し２割強の学生が受講し、最も受講率の高かったのが2011年度で８割を超えたそうですが、その後、受講率は減少し2017年度は２割程度であるとのことでした。今後は、受講率の向上を目指し、時間割の再調整を行いたいとのことでした。また、「KITスタンダード」に組み入れて必修化することも検討されているとのことでした。

専門教育としての情報セキュリティ教育に関して、立命館大学情報理工学部の上原哲太郎教授にご講演いただきました。教養教育としての情報セキュリティ教育は、情報セキュリティの概念、被害を受けないための教育としてのリテラシー教育、加害に加わらないための教育が重要であり、専門教育としての情報セキュリティ教育は、情報セキュリティ技術者・研究者育成のための基礎知識と教養が重要であるとのことでした。また、情報セキュリティに関する教科書10冊について、「暗号」、「認証」、「プロトコル」、「マルウェアとその対策」、「不正アクセスとその対策」、「WebとSSL/TLS・PKI」、「サイドチャネル攻撃」、「DoS攻撃」、「情報セキュリティマネジメント」、「個人情報保護・プライバシー」、「著作権保護·情報ハイディング」、「情報セキュリティ関連法」を扱っているかどうかを調査された結果、「暗号」、「認証」はほぼ全ての教科書で扱っているが、それ以外については扱っていたり扱っていなかったりバラバラであるとのことでした。「暗号」や「認証」が扱われる理由として、重要であることと変化が早くなく体系だっていて教えやすいということがあるのではないかとのことでした。情報セキュリティ教育は、専門教育としての難しさを有していて、その理由は、変化が早く外部要因が多い、教えるべき内容の多さと依然関係、学際的な要素が強い、

学生が想像しにくい世界がある点などが挙げられるとのことでした。そもそも守備範囲の広い情報セキュリティの分野で、どのような人材を育てるのかは難しく、セキュリティマインドを持つIT技術者の育成を基本とし、基礎が理解できていれば、早い変化にも耐えられるはずであり、好奇心が重要であるとのことでした。



専門教育としての情報セキュリティ教育に関して、京都産業大学コンピュータ理工学部の秋山豊和准教授に、平成30（2018）年４月にコンピュータ理工学部が改組して情報理工学部になった後の情報セキュリティコースにおけるセキュリティ教育についてご講演いただきました。セキュリティ教育として、「情報セキュリティ基礎」、「産業システムセキュリティ」、「情報セキュリティ特別講義」、「実践情報セキュリティ」という科目を設置されるとのことでした。特徴的な科目である「産業システムセキュリティ」では、情報システム（IT）だけでなく、制御システム（OT）の情報セキュリティを扱われるとのことでした。また、情報セキュリティ教育の課題として、倫理面で課題があり、ダークサイドへの人材の流出の危険性を挙げておられました。最後に、セキュリティを応用事例としたICT基礎教育の徹底が、必要とされる人材育成への第一歩であると言われていたのが印象的でした。

社会が求める情報セキュリティ教育として、NPO日本ネットワークセキュリティ協会（JNSA）教育部会の平山敏弘部会長にご講演いただきました。情報セキュリティ技術者が不足するという現状を説明した後、育成するべき情報セキュリティ技術者として、1)橋渡し人材からCISOを目指せる人材、2)セキュリティ技術の世界でトップを目指せる人材、3)現場実務を担う現場リーダー（特にユーザ企業）を挙げておられました。また、情報セキュリティ教育として何を学ぶべきかということで、JNSAでは情報セキュリティ知識体系（ SeCBoK2017, Security Body of Knowledge 2017）を作成しWeb公開されていることを示されていました。このSeCBoKでは、16の役割（ロール）と400弱のスキル項目が示されていて、セキュリティ人材育成に必要なスキルが明確化されているとのことでした。また、このSeCBoKを利用した教育プログラムの開発についても触れられていました。

講演の後、参加者からの質問をコーディネーターが整理したものをもとに、講演者に回答いただきました。

その後、講演者を中心に４つのグループに分かれて、立命館大学上原哲太郎教授がご講演されていた情報セキュリティの教科書で扱われている内容について、教養教育での情報セキュリティ教育として、また、専門教育としての情報セキュリティ教育として、グループワークで検討いただき、グループワーク終了後、ホワイドボードにて情報共有を行ったうえで、各グループに発表いただきました。

後日、ご参加いただいた方から、役に立ったというメイルをいただき、コーディネータとしてはうれしく思いました。

今回の分科会では、大学コンソーシアム京都の事務局には大変お世話になり、ありがとうございました。

最後に、お忙しい中、登壇いただきました先生方に感謝いたします。

第７分科会コーディネーター　藤田和弘（龍谷大学）

京都工芸繊維大学における情報セキュリティ教育「情報セキュリティと情報倫理」

京都工芸繊維大学　情報工学・人間科学系／情報科学センター　教授　桝田　秀夫

大学コンソーシアム京都 FD フォーラム

（分科会）情報セキュリティ教育
- 教養教育として、専門教育として -

京都工芸繊維大学における情報セキュリティ教育
「情報セキュリティと情報倫理」

京都工芸繊維大学
情報工学・人間科学系 / 情報科学センター

桝田 秀夫 (h-masuda@kit.ac.jp)

概要

- 京都工芸繊維大学における情報倫理教育
  - 科目「情報セキュリティと情報倫理」
  - 全学共通科目。一年次後期配当。(三大学連携科目)
- [京都工芸繊維大学の学部構成]
  - 工芸科学部
    - 生命物質科学域
      - 応用生物学課程
      - 生体分子応用化学課程
      - 高分子機能工学課程
      - 物質工学課程
    - 設計工学域
      - 電子システム工学課程
      - 情報工学課程
      - 機械工学課程
      - デザイン経営工学課程
    - 造形科学域
      - デザイン・建築学課程



科目：情報セキュリティと情報倫理

- 2004 年度より開講　（桝田は 2005 年度より担当。）
  - 全学共通科目→人間教養科目→ KIT 教養
  - 1 年次後学期 (2 単位)・選択・講義（座学）
- 「IT 社会の法と倫理」を参考書に指定
  - 2017 年度より、「情報のセキュリティと倫理」に変更
- Moodle システムを使って、毎回ミニレポートを課す

成績評価

- 毎回のミニレポート (50%) と 3 回の課題レポート (50%)
- 2012 年度より、課題レポートを減らして期末試験を導入
  - 毎回のミニレポート (20%)、課題レポート (30%)、および期末テスト（50%）

シラバス： 授業の目的・概要、学習目標

情報化が進展した社会において、情報機器と情報通信ネットワークを利用した情報のやりとりは、日常生活や仕事に必要不可欠なものである。そのような情報社会において、情報セキュリティ技術が果たしている役割とその機能について議論するとともに、各自が情報の受け手であると同時に送り手であることを認識し、情報を扱うときに生じる責任、適正な情報のやりとりをするために必要なルールや心構え、つまり、情報に関連した法規や情報モラルについて議論する。

学習目標

1. 情報化が進展した社会現代社会において、情報セキュリティと情報倫理が重要であることを自覚する。
2. 情報セキュリティ技術が果たしている役割とその機能について理解する。
3. 情報を扱うときに生じる責任、適正な情報のやりとりに必要なルールや心構え、情報に関連した法規や情報モラルを理解する。

シラバス： 授業計画項目 (1/3)

1　チュートリアル – 情報社会への参画　（1 章）
社会生活の中で情報や情報技術が果たしている役割や及ぼしている影響，情報モラルの必要性や情報に対する責任などについて議論する．

2　情報とプライバシー　（2章）
近年問題となっている個人情報漏洩などに関連して，個人情報の取扱いなど情報に対する責任に対して議論する．

3　コンピュータの信頼性　（4章）
情報社会において，さまざまなものがコンピュータ化されているが，そのコンピュータ自身の信頼性とその影響などについて議論する．

4　コンピュータ犯罪　（7章）
インターネットおよびコンピュータを利用した犯罪の実例とその防止について議論する．

5　日本における法整備　（総務省「国民の為の情報セキュリティサイト」）
刑法，不正アクセス行為の禁止に関する法律など，インターネット及びコンピュータを利用した犯罪に関連した法律に関して議論する．

6　ソフトウェアなどの知的財産保護　（5 章）
コンピュータでソフトウェアを利用する際に注意すべき著作権問題，およびインターネットを利用した情報のやりとりにおける著作権問題などについて議論する．

シラバス： 授業計画項目 (2/3)

7　ネットワークセキュリティ技術　（IPA「情報セキュリティ読本」）
TCP/IP プロトコルの基礎と，ファイアウォール，ネットワーク侵入検知システムなどについて議論する．

8　サイトセキュリティ技術　（IPA「情報セキュリティ読本」）
パスワードによるユーザ認証，ファイルアクセスなどに関するアクセス制御技術などについて議論する．

9　OS/ 言語処理系とセキュリティ技術　（独自）
バッファーオーバーフローなどによるインシデントの発生原因となる OS や言語処理系の 技術的な問題について議論する．

10　暗号技術と認証技術　（3章＋α）
暗号技術，PKI，および，バイオメトリクスなどによる認証技術などについて議論する．

11　ウィルスと不正アクセス技術　（独自）
コンピュータウィルスおよびコンピュータワームの実例とそれらが利用している技術，不正アクセスの実例とその技術について，議論する．

シラバス： 授業計画項目 (3/3)

12　情報セキュリティマネージメント
(IS テキスト「情報システムの運営」、JIPDEC)
情報セキュリティポリシーおよび ISMS (Information Security Management System) に基づく情報セキュリティマネージメントについて議論する.

13　専門家の倫理と責任　　(10 章)
情報処理技術者およびエンドユーザコンピューティングを推進する技術者としての情報社会における倫理と責任について議論する.

14　より広範な諸問題 - 総括　　(9章)
講義全般について総括した上で、情報セキュリティと情報倫理に関する今後の展望について議論する。

15　まとめ　　(独自)
講義全般について落ち穂拾い (リクエスト) 。

ミニレポートの例 (1/2)

課題 1: 身近なもので、「情報化されて便利になったもの」「今後、情報化されると便利になると思うもの」について、情報化される前と後でどう変わるかに重点をおいて (簡単に) 説明して下さい。

課題 2: 授業の中で触れた電子マネーについて、利用者に対するメリットと提供側のメリット (どのような情報として活用できる可能性があるのか) を、通常の現金と比較して、プライバシーの観点から (簡単に) 説明して下さい。

課題 3: 身近なコンピュータで、「壊れる (不具合が発生する) と想像したことのないもの」を挙げ、もし壊れた (不具合が発生した) 場合の自分を含む周りへの影響と、それが無かった場合の代替え手段を (簡単に) 説明して下さい。

課題 4:「コンピュータを使った犯罪にひっかからない為に心がけるべきこと」を自分の親 (または知合いのおじさん、おばさん) に説明するなら、どういう説明をするのが適切かを (簡単に) 説明して下さい。

課題 5: ウィルスソフトを「作成」した人は、可能性としてどのような法律違反をしたと見做されるかを、どの点で触れる可能性があるかを交えて (簡単に) 説明して下さい。

課題 6: ファイアウォールと IDS の違いを、実世界の生活になぞらえて説明するとすれば、どう説明するのが適切かを (簡単に) 説明してください。

課題 7: パスワード (暗証番号) の管理について、「これならコンピュータに詳しくない人でも、今までよりは良くなる」と思われる方法について、簡単に説明してください。

ミニレポートの例 (2/2)

課題 8: コンピュータの基本ソフト (OS) の脆弱性に対して、「利用者の立場」でできることは何かを考えてみて下さい。

課題 9: ソフトウェアおよびインターネットを利用するに当たって, 著作権の観点から注意すべきことについて, 各自の体験を基に述べて下さい.

課題 10: 暗号化により如何なる権力によっても「盗聴が全く出来なくなった場合」と、権限を持っていれば「すべてが盗聴できる場合」との得失を、身近な例を用いて説明し、その例ではどうなっているのが適切かを説明して下さい。

課題 11: ウィルスや不正アクセスを撲滅する為に必要となる対策方法について、「技術的な視点」もしくは「教育的な視点」から説明して下さい。

課題 12: 自分の自宅にある「情報資産」を洗い出し、分類とそのリスク分析したものを簡単に説明して下さい。

課題 13: 講義の中で出てきた以下に挙げる「事例」のうちの、講義中に説明をしなかったもののうちから一つ選び, 自分が直面した際に, 倫理的にどういう観点で考えて判断するのが適切か、また、実際に自分だったらどうするか (してしまうか) を説明して下さい。
1. 従業員のファイル複製　2. 不十分なプライバシー保護
3. リスクのあるシステム　4. 事実の公表
5. 個人情報の公表　6. 利害関係の申告
7. 著作権の侵害　8. 外国人プログラマの雇用

課題レポートの例

課題 1: 下記のいずれかの話題について、講義の内容をふまえた 15 分程度 (10 ～ 15 枚程度) のプレゼンテーションができるだけの発表資料と読み上げ資料を作成して下さい。

* 情報とプライバシー　* コンピュータの信頼性
* コンピュータ犯罪　* コンピュータ関連の法律

[想定する聴衆]

本講義を受講していない本学の学生向け

[提出方法]

基本的に、以下に挙げるプレゼンツールを使用して作成したファイルを、e-Learning システムにアップロードして下さい。

読み上げ資料は、プレゼンツールの「ノート」部分に書き込んで下さい。

課題レポートの例

課題 2: 下記のいずれかの話題について、講義の内容をふまえ、「達成度を確認できる試験問題」と「その解答」「その解説」を作成して下さい。

* ネットワークセキュリティ技術　* サイトセキュリティ技術
* OS/ 言語処理系とセキュリティ技術　* 暗号技術と認証技術
* ウィルスと不正アクセス技術　* ソフトウェアなどの知的財産保護

[想定する受験生]

本講義の受講学生

[試験問題作成の形式]

問題数: 10 問

問題形式:選択式 (最大 5 択) or 記述式 (混在して構わない)

課題レポートの例 (続き)

課題 3: 情報セキュリティと情報倫理に関する、重要性、役割と機能、技術、責任やルール、心構えについて、3 ページ程度のレポートを作成せよ。

[作成上の注意]

* Microsoft Word 形式、OpenDocument 形式、もしくは PDF 形式のいずれかで提出 (アップロード) すること。

* A4 縦方向、横書き、本文 11 ポイント (前後) で記述すること。

* 「タイトル」「学籍番号」「名前」「提出日付」を一ページ目の冒頭に明記すること。

注 : 2012 年度より、期末試験に切替。

教科書 / 参考書の変遷

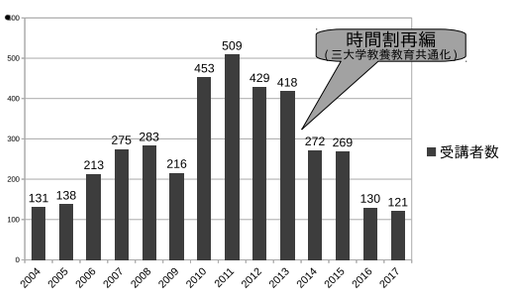
- 2005 年度～ 2016 年度
  - サラ・バーズ著「 IT 社会の法と倫理」(第 2 版)
  - IPA「情報セキュリティ読本 - IT 時代の危機管理入門 -」
- 2017 年度～
  - 山田恒夫著「情報のセキュリティと倫理」
    - 放送大学教材

授業計画の更新

講義回	2016 年度	2017 年度
1	チュートリアル - 情報社会への参画	1. 情報社会における光と影 2014
2	プライバシーと個人情報	9. 情報通信技術とプライバシー
3	コンピュータの信頼性	←
4	コンピュータ犯罪	3. サイバー犯罪の諸相と問題解決2：子供に対する視点から
5	日本における法整備	10. セキュリティと法
6	ソフトウェアなどの知的財産保護	⇑
7	ネットワークセキュリティ技術	4. サイバー犯罪の諸相と問題解決3：管理者の視点から
8	ホストセキュリティ技術	⇑
9	OS/ 言語処理系とセキュリティ技術	←
10	暗号技術と認証技術	5. 情報セキュリティの基盤技術1：暗号と認証の基礎
11	ウィルスと不正アクセス技術	2. サイバー犯罪の諸相と問題解決1：利用者の視点から
12	情報セキュリティマネジメント	8. 情報セキュリティマネジメント
13	専門家の倫理と責任	14. 技術者倫理と情報セキュリティ人材育成
14	より広範な諸問題	15. まとめと展望
15	総括	←

受講状況

定員 600 人 / 学年



まとめ

- 「情報セキュリティ」と「情報倫理」
- 前半が倫理 (非技術) 編、後半が技術編
  - 前半： 倫理的な話 + 技術の概論
  - 後半： 技術の (少し突っ込んだ) 詳細
  - 最後： 倫理の広範な話題
    - → あくまでも「全学部」向けの範囲で。
- 本学の取り組みは「広く浅く (薄く ?) 」

今後の課題

- 受講率の向上
  - 時間割の再調整
  - 必修化？
  - 「 KIT スタンダード」に組み入れる

専門教育としての情報セキュリティ教育

立命館大学　情報理工学部　教授　上原　哲太郎

R RITSUMEIKAN

専門教育としての
情報セキュリティ教育

立命館大学情報理工学部
セキュリティ・ネットワークコース
上原哲太郎　Twitter: @tetsutalow

R 大学における情報セキュリティ教育

- **一般教養教育として**
  - **情報セキュリティの概観（概念・世界観）**
  - **リテラシー教育≒被害を受けないための教育**
  - **情報倫理教育≒加害に加わらないための教育**
- **専門教育として**
  - **情報セキュリティ技術者・研究者育成のための基礎知識と教養**

Beyond Borders

R 情報セキュリティ教育に体系はあるか

- **教科書を見てみると？**



R 内容のばらつき

内容	A	B	C	D	E	F	G	H	I	J
暗号（共通・公開・ハッシュ）	●	●	●	●	●	●	●	●		●
認証（パスワード・生体）	●	●	●	●	●	●	●	●		●
プロトコル（認証・鍵交換）	●	●		●	●	●	●			●
マルウェアとその対策		●		●	●	●	●		●	
不正アクセスとその対策		●		●	●	●	●	●	●	
WebとSSL/TLS・PKI	●	●			●	●	●			●
サイドチャネル攻撃		●				●				
DoS攻撃						●	●		●	
情報セキュリティマネジメント		●		●	●		●	●		●
個人情報保護・プライバシー			●		●		●	●		●
著作権保護・情報ハイディング		●	●	●	●					●
情報セキュリティ関連法			●		●	●				●
その他	●	●	●	●	●	●	●	●	●	●

R コンセンサスはあるだろうか

- **暗号は多くの場合重要**
  - **共通鍵暗号／公開鍵暗号／ハッシュ**
  - **鍵共有や鍵管理**
  - **PKIとSSL/TLS**
- **認証も重要**
  - **パスワード認証**
  - **バイオメトリックスetc.**
- **でも他はかなり多様**

変化が遅い
体系立っており
教えやすい

Beyond Borders

R 特色ある内容

- **Buffer Overflow等の仕組み・強制MAC**
- **Webアプリケーションセキュリティ**
- **DNS Cache poisoning**
- **無線LANのセキュリティ**
- **ICカード**
- **情報倫理教育**
- **セキュリティ人材育成**
- **情報システム監査・セキュリティ監査**
- **Common Criteriaなどの認証制度**
- **インシデントレスポンス**
- **デジタル・フォレンジックス**

Beyond Borders

専門教育としての難しさ

- 変化が早く、しかも外部要因が多い
- 教えるべき内容の多さと依存関係
- 極めて学際的要素が強い
- 思わぬ知識が関係してくることがある
- 学生に想像しにくい世界観がある
- 倫理面やモラルに要配慮
- そもそも何を教えるべきかわからない
- 教えられる人がいるのかもわからない

Beyond Borders

変化が早い／外部要因で変化

- 例：SHA-1の危殆化
  - 1995年登場
  - 2005年　急速に危殆化
    その後少し鈍化したが2017年衝突見つかる
- 例：パスワードの常識
  - 複雑なパスワードを定期的に変更から
    単純でも長いパスワードを長期利用へ
  - 「パソコンで4桁暗証番号へ」
- Web開発環境の流行に脆弱性も左右

Beyond Borders

教えるべき内容の多さと依存関係

- 全てを教えることができるわけでは
  ないので取捨選択が必要
- 演習がないと消化不良だが時間が不足
- 他の教科との依存関係が複雑
  - 言語・コンパイラ・機械語→脆弱性
  - OSにおける保護モデル→不正アクセス
  - TCP 3Way Handshake→SYN Flooding
  - 法的リテラシなしに著作権や
    サイバー犯罪関係の刑法は教えられるか?

Beyond Borders

極めて学際的要素が強い

- 組織マネジメントとの強い関係
  - 特に情報セキュリティマネジメント
- いわゆる文系的学問との関係
  - 法学
  - 社会学
  - 経済学
  - 心理学

Beyond Borders

思わぬ知識が関係することが

- 例：サイドチャネル攻撃
  - 電力解析は素子の動作への理解が必要
  - 先日話題になったCPUの脆弱性は
    CPUの分岐予測機構／投機実行機能において
    アドレス計算を投機的に実行させることを
    うまく用いている
- 例：フィッシング
  - ラテン文字aに似たギリシャ文字α

Beyond Borders

学生に想像しにくい世界がある

- 大規模な情報システム
  - 身近な存在だが実感する機会が少ない
- 組織マネジメント
  - 情報セキュリティの基礎だが実感がない
- B2Cの世界
  - 顧客にルールを守ってもらうことの
    困難さが分かりにくい

Beyond Borders

倫理やモラルに配慮する必要

- 法的にグレーなまま実現されている技術に関する周知が必要
  - リバースエンジニアリング
  - 通信内容の解析
  - 個人に関する識別可能情報
- 悪用可能な技術を多く教えてしまう問題
  - 各種攻撃技法など

Beyond Borders

そもそもどういう人財を育てる？

- セキュリティの守備範囲はあまりに広い…
- 何でも知っている超人を育てることは不可能に近い
  - そもそも教える側のリソース



Beyond Borders

JNSA SECBoK2016より セキュリティ専門家といっても…

マルウェアアナリスト
侵入したマルウェアや使われたエクスプロイトを安全に解析し、攻撃手法の解明や対策手法の考案を行う。またシステム・ネットワーク上に残された痕跡から未知のマルウェアの検出も行える人物

フォレンジックアナリスト
インシデント時にシステム・ネットワーク上の証拠を発見、適切に証拠保全する人物

ペネトレーションテスター
最新の攻撃手法を熟知し、対策方法を提案する。必要に応じて、システム・ネットワークに脆弱性が検査を計画し適切に行える人物

インシデントハンドラー
インシデント時に素早く対応し、システム・ネットワーク運用者および管理者と連携して、対策を行い安全に復旧を行える人物

ネットワークアナリスト
システム・ネットワークの運用、管理を行う。インシデント時の初期対応も行える人物

プロフェッショナルセールス
組織に必要なセキュリティ対策を検討、提案する上で必要な基礎知識・スキルを持ち、ビジネス戦略的観点から最適なソリューションを提案できる人物

日本ネットワークセキュリティ協会 SecBok2016概要説明より抜粋

Beyond Borders

ITシステムを作る人たち

コンサルタント
顧客ニーズを把握し、提案。顧客満足度に責任を持つ人物

プロジェクトマネジャー
業務要件、IT要件を把握し要件を定義し、プロジェクトに責任を持つ人物

ITスペシャリスト
基盤システムの設計、構築、運用、保守する人物。

アプリケーションスペシャリスト
アプリケーションシステムの設計、構築、運用、保守する人物

日本ネットワークセキュリティ協会 SecBok2016概要説明より抜粋

Beyond Borders

ITシステムを使う人たち

インシデントマネージャー
インシデントハンドラー
インシデントの現場監督・ベンダとの連携・インシデントの処理

キュレーター・リサーチャー
インシデントの情報収集、運用しているセキュリティセンサ異常値の発見、影響分析

インベスティゲーター
外部からの犯罪、内部犯罪を捜査

リーガルアドバイザー
法律・法令に基づく支援

コマンダー・トリアージ
セキュリティ全体統括者

フォレンジックエンジニア
インシデントの原因究明や証拠発見などを行うための電子情報の分析

POC
外部との連絡窓口となり、情報連携 を行う。社内窓口として社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う

ノーティフィケーション
社内関連部署への連絡

セルフアセスメント・ソリューションアナリスト
リスクアセスメント、セキュリティ戦略の策定・推進

Copyright (c) 2016 NPO日本ネットワークセキュリティ協会

日本ネットワークセキュリティ協会 SecBok2016概要説明より抜粋

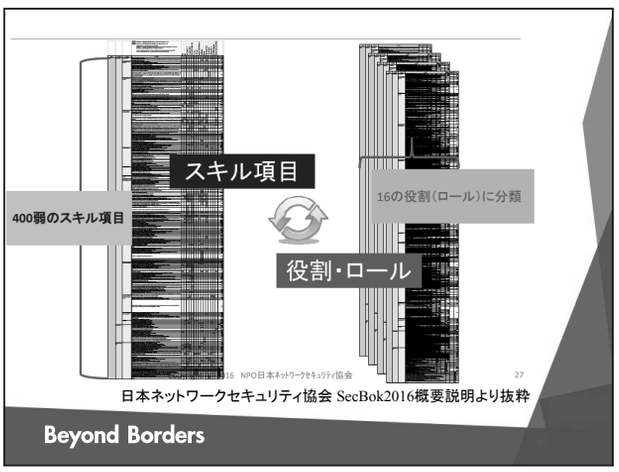
Beyond Borders

この人たちに必要なスキルは…

	NCAによるロール定義		NICEの専門分野	ユーザ企業職種	セキュリティベンダ職種
a	CISO	23	セキュリティプログラム管理（CISO）	（役員）	
b	POC		（なし）		
c	ノーティフィケーション		（なし）		
d	コマンダー	21	情報システムセキュリティ運用（ISSO）		
e	トリアージ	21	情報システムセキュリティ運用（ISSO）		
f	インシデント管理	15	インシデントレスポンス		インシデントハンドラー
g	インシデントハンドラー	15	インシデントレスポンス		インシデントハンドラー
h	キュレーター	14 15	計算機ネットワーク防御分析 情報保障コンプライアンス		SOCアナリスト
i	リサーチャー	14	計算機ネットワーク防御分析	ITセキュリティ部門	SOCアナリスト
j	ソリューションアナリスト	13	システムセキュリティ分析		マルウェアアナリスト/プロフェッショナルセールス
k	セルフアセスメント	13	システムセキュリティ分析		マルウェアアナリスト/コンサルタント
l	脆弱性診断	17	脆弱性アセスメントと管理		ペネトレーションテスター
m	教育・啓発	20	教育と訓練		（教育サービス）
n	フォレンジックス	18	デジタルフォレンジック		フォレンジックアナリスト
o	インベスティゲータ	19	捜査		フォレンジックアナリスト
p	（なし）	22	法的助言と弁護	（法務部門）	（弁護士）
q	（なし）	24	戦略策定とポリシー開発	（IT企画部門）	コンサルタント
r	（なし）	16	計算機ネットワーク防御インフラサポート	ITシステム部門	ネットワークアナリスト

日本ネットワークセキュリティ協会 SecBok2016概要説明より抜粋

Beyond Borders



日本ネットワークセキュリティ協会 SecBok2016概要説明より抜粋

Beyond Borders

立命館大学情報理工学部では…

- 2004年度開設
- 情報科学・情報工学の幅広い分野をカバー
- 情報系学部として日本最大級の規模
  - 多数の教員（約100名）
  - 多岐にわたる研究分野
- 国際化を意識した教育プロジェクト
  - HEDSPIプロジェクト
  - 「みらい塾」
  - 国際情報ソフトウェア学部





Beyond Borders

2017に改組（７コース）

専門領域を深く学ぶ６コース



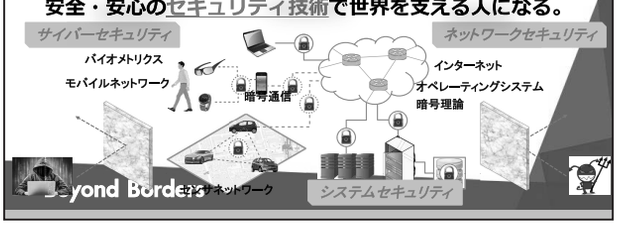
PBLで分野横断的に学ぶ英語コース

セキュリティ・ネットワークコース

コンピュータと情報ネットワークの基礎技術を学び、種々の攻撃から情報を護るセキュリティ技術を体系的に習得



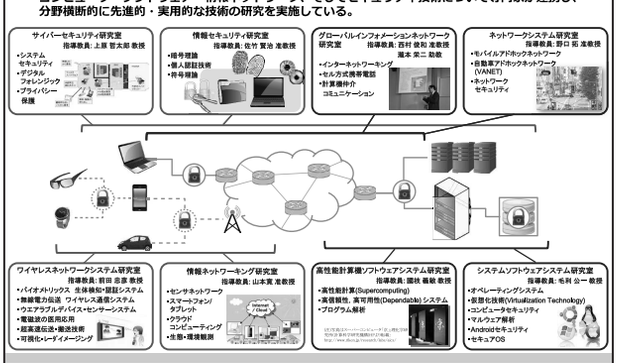
安全・安心のセキュリティ技術で世界を支える人になる。



Beyond Borders

セキュリティ・ネットワークコース

- コンピュータ・ソフトウェア・情報ネットワーク、そしてセキュリティ技術について専門家が連携し、分野横断的に先進的・実用的な技術の研究を実施している。



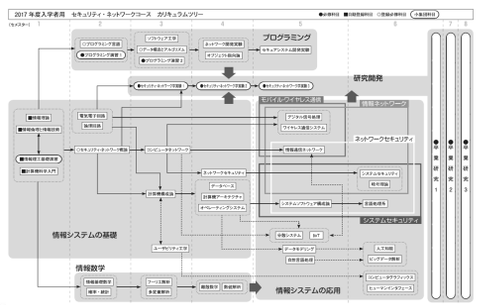
学生にアピールしている「学び」

- セキュリティ・暗号技術全般
- インターネット・ケータイの仕組み
- コンピューターの仕組みを基礎から

- ×ウィルス対策・ケータイアプリ
- ○基礎の技術・長く使える技術

Beyond Borders

実際のSNコースのカリキュラム



Beyond Borders

SNコースの学部教育の特色は…

- **かなり「伝統的」情報科学教育**
- **少し数学色が強め**
- **プログラミングはCで行う**
- **ネットワークはレイヤ低め中心**
- **セキュリティは**
  暗号＋システム構成と運用中心
- **マネジメントなどは卒研以降**

Beyond Borders

結論としては…

- **学部教育では専門教育で求められる**
  知識を全て詰め込まず大学院に回す
- **「セキュリティマインドを持つ**
  IT技術者」の育成を基本にする
- **基礎さえ出来ていれば**
  速い変化にも耐えられるはず
  あとは旺盛な好奇心が必要

Beyond Borders

デジタル・フォレンジック研究会 第359号コラムより

2015年4月27日 「情報セキュリティ人材が足りない、は本当か」
https://digitalforensic.jp/2015/04/27/column359/

- 我々は
  「現在圧倒的に不足しているのは
  【情報セキュリティ人材】ではなく、
  【情報セキュリティの基礎知識を
  有したＩＴ人材】である」という
  認識から出発するべきなのではないかと思います。

Beyond Borders

ICT教育とセキュリティ教育

京都産業大学　コンピュータ理工学部　准教授　秋山　豊和

第23回FDフォーラム 第7分科会
セキュリティ教育分科会
―教養教育として、専門教育として―
「ICT教育とセキュリティ教育」

京都産業大学 コンピュータ理工学部
秋山 豊和

自己紹介

- 大学研究室在籍時（～2000年）
  - 分散データシステムの研究開発（トランザクション処理）
- 大阪大学サイバーメディアセンター在籍時（2000年～2008年）
  - キャンパスネットワーク構築・運用（IP，BGP/OSPF）
  - 認証基盤システム構築・運用（PKI, SAML）
  - グリッドコンピューティングの研究開発
- 京都産業大学在籍時（2008年～現在に至る）
  - バス安全運転支援システムの構築（総務省SCOPE）
  - SmartCity実証実験プラットフォームの構築（日欧連携プロジェクトFESTIVAL：NICT委託研究）
  - IPA産業サイバーセキュリティセンター中核人材育成プログラム

セキュリティの専門家でない人がセキュリティ教育？

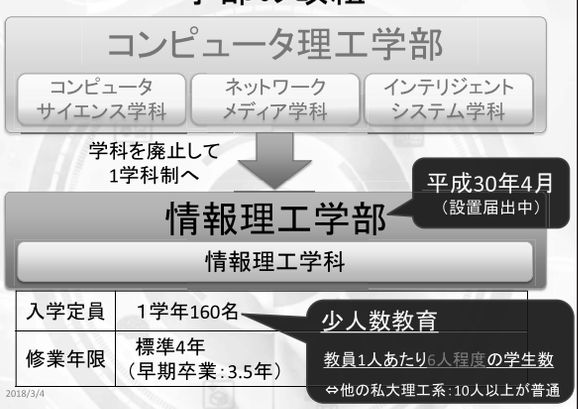
1

本日の内容

- 京都産業大学 情報理工学部（4月開設）と情報セキュリティコースについて
- セキュリティ分野の専門教育について
- セキュリティ教育における課題

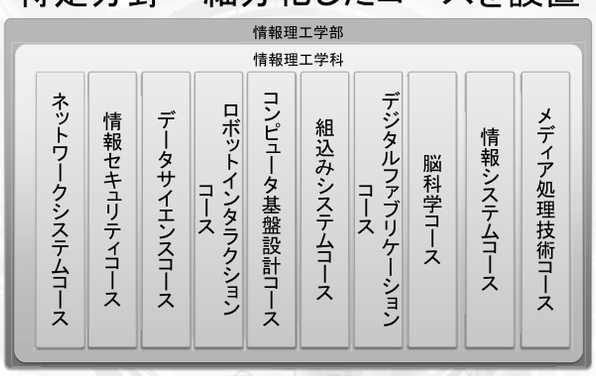
2018/3/4　2

学部の改組



2018/3/4

特定分野へ細分化したコースを設置



いずれのコースも「コンピュータ・プログラミング」は必須

情報理工学部について

コース制の骨子・位置付け

- 多数ある学部専門科目のうち、分野・領域に合う科目群をセットとして提供（コース）
  - 学生自らがコースを選択して該当科目を修得していく（学生はコースに所属するのではない）
  - 複数のコースを選択することも推奨（複数の方向性を兼ね備えた多様性ある人材育成）
- コース修了を卒業要件の一つとする
  - いずれか1つの「コース要件科目」すべて修得することを学部の卒業要件とする
  - コース毎に「コース要件科目」のセットが違う
  - 「コース推奨科目」も修得することで、よりコースに沿った学びの特徴が出る

5

情報理工学部について

複数コース選択について



情報理工学部について

情報セキュリティコース



- ICT教育におけるターゲット
  - 基礎技術の習得

基礎技術の応用がイメージできず，動機づけが弱い

- 応用（セキュリティ）にリンクした教育の確立
  - 情報技術：Information Technology (IT)
  - 制御技術： Operational Technology (OT)

産業システム

コース選択人数制限あり（30人まで）

産業システムを支える人材を育成する

情報セキュリティコース

セキュリティ教育

- 情報セキュリティ基礎
  - セキュリティリテラシ教育を行う
- 産業システムセキュリティ
  - IT/OTそれぞれについて技術的な内容を学ぶ
- 情報セキュリティ特別講義
  - セキュリティ分野の最新動向についてオムニバス形式で学ぶ
- 実践情報セキュリティ
  - IT/OTの技術について実習を通して理解を深める

情報セキュリティコース

セキュリティ教育

- 情報セキュリティ基礎
- 産業システムセキュリティ
- 情報セキュリティ特別講義
- 実践情報セキュリティ

ICT教育

- コンピュータ概論
- コンピュータネットワークI・II
- コンピュータ理工学実験
- コンピュータアーキテクチャI
- オペレーティングシステム
- 応用プログラミング（Web）
- 分散処理システム
- 情報理論
- 情報と職業（知的財産・コンプライアンスの基礎）
- 他

なぜ産業システム（IT + OT）か？（1/3）

- 社会への影響度の大きさ
  - 2014年 ドイツの製鋼所へのサイバー攻撃：溶鉱炉が被害
  - 2015, 2016年 ウクライナの変電所へのサイバー攻撃: 22万世帯に影響する停電



引用元: http://www.ibtimes.com/hackers-target-german-steel-mill-cyberwarfare-gets-physical-1777534



引用元: https://wired.jp/2017/01/14/hacking-ukraine-power/

なぜ産業システム（IT + OT）か？（2/3）

- IT分野とOT分野の違い

	制御システム（OT）	情報システム（IT）
セキュリティの優先順位	システムが継続して安全に稼動できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報
技術のサポート期間	10年～20年	3年～5年
求められる可用性	24時間365日の安定稼動（再起動は許容されないケースが多い）	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

引用元: https://www.ipa.go.jp/files/000044733.pdf

なぜ産業システム（IT + OT）か？（3/3）

- 現場の課題をそのまま教育に活用

DCS



一般に、DCSは、オペレータ（運転員）が制御・監視を行うためのHMI（Human Machine Interface）と、フィールドネットワークに接続して、HMI とコントローラを接続する制御ネットワークの3つの構成要素からなる。化学やガスプラントで利用。

PLC



PLC は、パソコンと監視・制御ソフトウェアの組み合わせによりプロセスの制御・監視を実行するものである。組立プラントやビル制御等で利用。

引用元：http://www.css-center.or.jp/pdf/about_CSSC.pdf

セキュリティ教育における課題

- 倫理面の課題
- セキュリティ人材の需要（採用）と供給（教育）
- ICT教育とセキュリティ教育について
  - 学部教育でのセキュリティ教育の課題

倫理面の課題

- 現場に適用可能な攻撃手法の共有
  - ダークサイドへの人材流出の危険性
- IPA産業サイバーセキュリティセンター中核人材育成プログラムでの例
  - 企業側がコスト負担した上で教育する人材を選出
  - 大学では同様な選出方法は採用できない
    - 低年次におけるセキュリティリテラシ教育の徹底が必要

セキュリティ人材の需要と供給

- セキュリティ人材とは？
  - 企業は攻撃技術や防御技術を習得した人材を集めたいのか？
    - 中途半端な人材の供給過多はダークサイドへの人材流出を招く
- 求められる人材とは？
  - 全てのレイヤを理解し，企業価値向上のためにICTシステムを活用し，かつ，安定運用できる人材
    - 考察）セキュリティの異常検知ができる人材と，IoTにおけるイベント検知ができる人材の違いとは？

ICT教育とセキュリティ教育

- セキュリティを応用事例としたICT基礎教育の徹底が必要とされる人材育成への第一歩
- 学部でのセキュリティ教育の課題
  - セキュリティの基礎は多岐にわたるため学部のみで必要な内容を習得するのは難しい面も
    - 例）セキュアプログラミング教育
      - 例外処理やテストなどは，開発においては重要な項目
      - 一方で，正常系の学習だけでも学部生には手一杯
        - » どのように取り入れていくかが課題

ICT教育とセキュリティ教育

- 学部でのセキュリティ教育の課題（つづき）
  - ICT教育の利点と難点
    - 利点：
      - 実際に触れながら学ぶことができる
    - 難点：
      - 毎年技術が進化する（教育内容の急速な陳腐化）
      - フレームワークなどの台頭によるブラックボックス化の進行ならびにインフラ技術との乖離
  - セキュリティ教育での例
    - Webアプリケーションのセッション管理
    - クロスサイトスクリプティング（XSS）の例

まとめ

- 京都産業大学 情報理工学部（4月開設）と情報セキュリティコースについて
- セキュリティ分野の専門教育について
  - 産業システムセキュリティ（IT/OTセキュリティ）
- セキュリティ教育における課題
  - 倫理面の課題
  - セキュリティ人材の需要（採用）と供給（教育）
  - ICT教育とセキュリティ教育について

2018/3/4 18

「なかなか進まぬセキュリティ人材育成」産業界における取り組みと学への要望について

NPO日本ネットワークセキュリティ協会（JNSA） 教育部会 部会長 平山 敏弘

JNSA NPO 日本ネットワークセキュリティ協会 Japan Network Security Association

『なかなか進まぬセキュリティ人材育成』

産業界における取り組みと学への要望について

2018 FDフォーラム 第7分科会

NPO日本ネットワークセキュリティ協会 教育部会 部会長
平山 敏弘

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 1

JNSA

1．不足する情報セキュリティ技術者

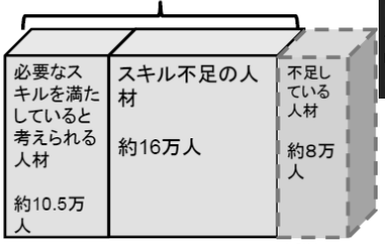
本当に足りないのは誰？ どう増やすの？

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 2

誰が足りない？ 何が足りない？

JNSA

国内のユーザー企業において情報セキュリティに従事する技術者 約26.5万人



IPAの試算によれば、国内のユーザ企業において、情報セキュリティ人材は大幅に不足（約8万人の不足）。

＜IPA試算「情報セキュリティ人材育成に関する基礎調査」の人材不足数に関する追加分析による。H24調査→H26追加分析。＞

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 3

では、どこで足りない？ どの業種で足りない？

JNSA

約8万人の業種別内訳

業種	（人）不足数
農林業・水産業・鉱業	256
建設・土木・工業	2,764
電子部品・デバイス・電子回路製造業	1,403
情報通信機械器具製造業	605
電気機械器具製造業	1,159
その他製造業	15,853
電気・ガス・熱供給・水道業	81
通信業	683
情報サービス業	1,885
その他の情報通信業	1,717
運輸・郵便業	2,710
卸売業・小売業	14,480
金融業・保険業	4,957
不動産業・物品賃貸業	1,547
学術研究・専門技術者	1,014
宿泊業・飲食サービス業	3,535
生活関連サービス業・娯楽業	3,301
教育・学習支援業	2,084
医療・福祉	8,473
複合サービス業	614
その他サービス業	8,462
計	81,590

特に情報関連以外の

・製造業
・卸売業・小売業
・医療・福祉

などのユーザ業種における人材不足が顕著

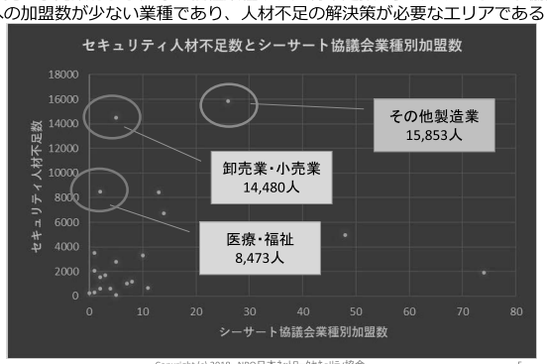
出典
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/it_jinzai_wg/pdf/002_03_00.pdf

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 4

セキュリティ人材不足数が多く、加盟数少の業種

JNSA

卸売・小売業および医療・福祉業種が、人材不足数が多く、シーサート協議会への加盟数が少ない業種であり、人材不足の解決策が必要なエリアである



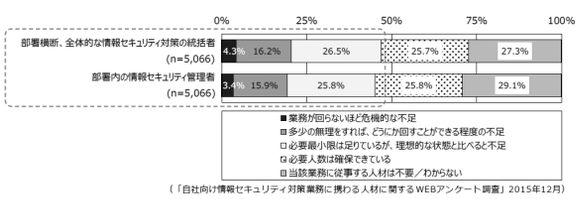
Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 5

本当に足りない？ ユーザ企業における、セキュリティ人材不足の現状

JNSA

ユーザ企業の約3-4%が、「業務が回らないほど危機的状況なセキュリティ人材不足」と現場責任者が回答している。

「自社向け」情報セキュリティ対策業務に携わる人材の不足感



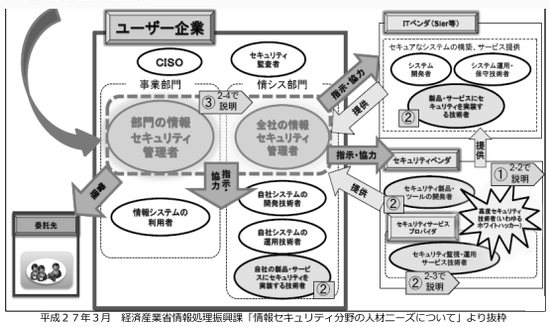
（「自社向け情報セキュリティ対策業務に携わる人材に関するWEBアンケート調査」2015年12月）

参照：経済産業省 IT人材の最新動向と将来推計に関する調査結果
http://www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会 6

今後必要となるセキュリティ人材像とは？

①ホワイトハッカーのような高度セキュリティ技術者
②安全な情報システムを作るために必要なセキュリティ技術を身につけた人材
③ユーザ企業において、社内セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材



平成２７年３月　経済産業省情報処理振興課「情報セキュリティ分野の人材ニーズについて」より抜粋

Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

育成すべきセキュリティ人材種別（9:1の法則）

橋渡し人材（CISO候補）　**トップガン人材**

1．橋渡し人材からCISOへ

2．ホワイトハッカーからトップガンへ

3．中堅レベル（現場リーダー）
（情報処理安全確保支援士レベル）
人材の育成
（数を増やす）

大別して3種類の人材育成が必要
1．橋渡し人材から、CISOを目指せる人材
2．セキュリティ技術の世界でトップを目指せる人材
3．現場実務を担う現場リーダー（特にユーザ企業での人材不足）

セキュリティ人材不足のうち約90%（約74,000人）

セキュリティ人材不足のうち約10%（約7,500人）

Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

スキル度と質量（スキル量）保存の法則の関係

山は土、タワーは鉄で構成されている

土ならば裾野を広く、鉄であればより固く

方法は違えども、600メートルに到達するには、
同じだけのスキル量が必要

硬い(深い)

質量保存の法則
「化学反応の前後で系の質量の総和は変わらない」
→　スキルの総和も変わらない（近道はない）

裾野が広い

Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

異なる技術者のスキルの幅と専門度

高尾山と東京スカイツリー
どちらも約600メートルの高さです

スキル到達点

高尾山と東京スカイツリー
どうやって同じ600メートルに到達できるのか

橋渡し人材（CISO候補）
（バーサタイリスト型人材）

トップガン人材
（スキル特化研究職型人材）

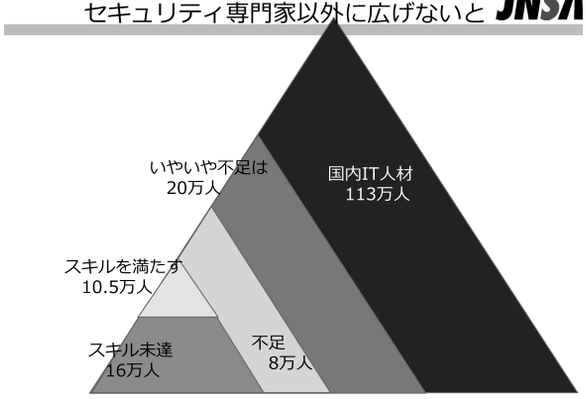
Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

野球に例えると
どう増やす　野球を知る人を入れて大人数



Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

人は増えない！
セキュリティ専門家以外に広げないと



Copyright (c) 2018　NPO日本ネットワークセキュリティ協会

2．何を学ぶのか？

情報セキュリティ知識分野
SecBoK（Security Body of Knowledge）
の登場

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK2017の公開



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

情報セキュリティ人材育成　取り組み経緯（1）

1）IPA様からの依頼で、2004年/2005年（修正版）と情報セキュリティスキルマップを作成

http://www.ipa.go.jp/security/fy15/reports/skillmap/documents/skillmap_2003.pdf
http://www.ipa.go.jp/security/fy16/reports/skillmap/documents/skillmap_2004.pdf



2）JNSAよりSecBoKとして名称変更し、経済産業省様受託事業のアウトプットとして公開

「情報セキュリティ教育の指導者向け手引書（２００７年版）知識分野がSecBoKそのもの(P.40-P67)

http://www.jnsa.org/result/2007/edu/materials/071111/tebiki2007.pdf



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

情報セキュリティ人材育成　取り組み経緯（2）

3）ISEPA より、「情報セキュリティ人財アーキテクチャガイドブック」を公開

ISEPA （情報セキュリティ教育事業者連絡会）より、2009年に人材育成ガイドを公開

http://www.jnsa.org/isepa/images/outputs/jinzai_arch_2009.pdf



4）SecBokを参考に、2009年に以下の「情報セキュリティプロフェッショナル教科書」

http://ascii.asciimw.jp/books/books/detail/978-4-04-867782-0.shtml



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK改訂活動

1）SecBoKの見直しおよびアップデート

現在のSecBok内容は、2004年に作成し、その後アップデートを重ねて2009年時点の内容が公開されているが、その後のアップデートが行われていない。
現在のユーザ企業における情報セキュリティ人材不足やクラウド時代などに対応できるようなアップデートが必要と考えて、2015年度に改訂活動を実施。

2）他協会および団体様に対してのSecBoK普及&利用促進活動

2009年よりアップデートが実施されていなかったのは、情報セキュリティ業界外への普及に問題があった点もあるため、今回のiコンピテンシ・ディクショナリ対応化に伴い、SecBokに関して、情報セキュリティ業界内にとどまらず、その他の外部協会および団体様への普及活動や情報共有活動を検討。

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

3．セキュリティ知識分野
（SecBoK）

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK改訂の方向性

分類	SecBoK改訂委員会での指摘事項および方針
職種	• ISEPAの32職種は多過ぎる。 ⇒セキュリティシステムにフォーカスした上で、どのような業務・プレイヤーがいるかに絞って整理すると少なくできるのではないか。 ⇒ビジネスモデルや業務内容に応じて、「ここにはこのような職種の人が必要」という形でまとめるとよい。
知識項目の分類	• 現行のスキルマップはベンダに偏り過ぎている。 ⇒新しい概念の取り込み（クラウド、仮想化、グリッド、SDNなど）が必要。 ⇒ユーザ向け、ベンダ向けという分類ではなく、職種やタスクをベースに整理することで、企業にとらわれずに整理することができる。
考慮点	• あまり細かいものは一般企業では受け入れてもらえない。 ⇒組織のミッションやビジョンを組織モデルに落とし込めるように。 ⇒平常時とインシデント発生時の区別。 ⇒自社で担当するか、外部委託するか、両方に対応できるようにする。
進め方	• 「ベンダと対話できる人材」など、現在不足している職種・人材像を明らかにした上で、そうした人材の育成に役立つ成果物を検討したい。

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK2017の特長

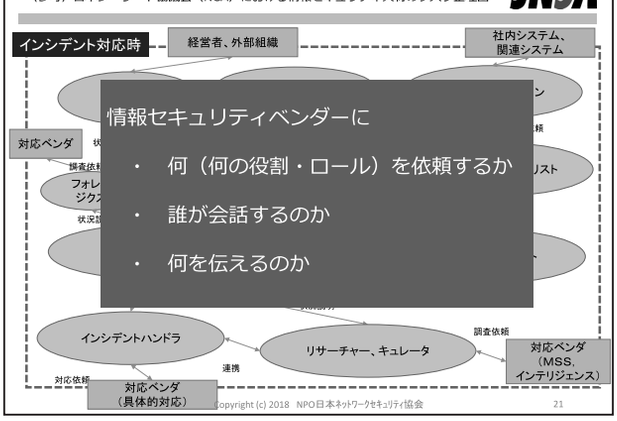
1．ユーザ企業での利活用対応
　日本国内において情報セキュリティ人材が大幅に不足していると指摘されているユーザ企業での活用に対応できるものにすべきである
　→　日本シーサート協議会で使用されている人材定義と連携、およびセキュリティベンダー職種とのマッピングを実施

2．世界基準への対応
　JNSAだけの認識ではなく、公に認知されているフレームワークを取り入れるべきである
　→　NISTのNICE Frameworkにおけるサイバーセキュリティに関する知識項目を取り込み

3．組織・ビジネスへの対応
　あまり細かくなり過ぎず、かつ実際の業務フローや組織モデルを想定できるものにするべきである
　→　従来のSecBoKにあった32職種を16職種に取り纏め、またIPA公開のiコンピテンシ・ディクショナリーやITSS+などのITスキル標準との連携を強化

Copyright (c) 2016 NPO日本ネットワークセキュリティ協会

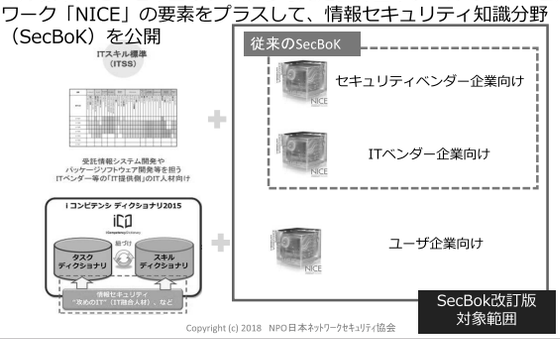
ユーザ企業内情報セキュリティ技術者の役割と関連部門
（参考）日本シーサート協議会（NCA）における情報セキュリティ人材のタスク整理図



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

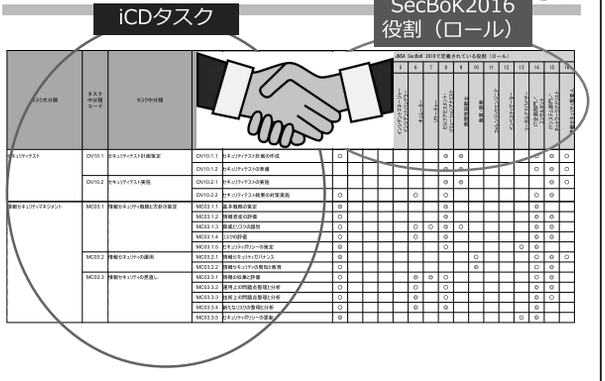
ユーザ企業も対象としたSecBoK

IT全般を対象にするiコンピテンシ・ディクショナリ2015（旧ITスキル標準）に、セキュリティから考えた世界基準レベルのフレームワーク「NICE」の要素をプラスして、情報セキュリティ知識分野（SecBoK）を公開



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBokとiCDとの連係強化



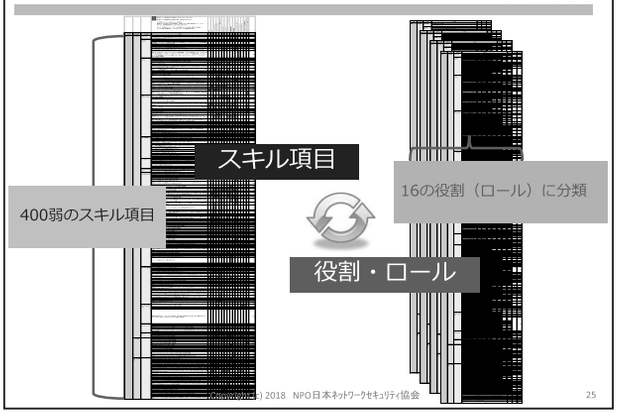
Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

各ロールとNICEフレームワークの対応づけ例

	NCAによるロール定義	NICEの専門分野		ユーザ企業職種	セキュリティベンダ職種
a	CISO	23	セキュリティプログラム管理（CISO）	（役員）	
b	POC		（なし）		
c	ノーティフィケーション		（なし）		
d	コマンダー	21	情報システムセキュリティ運用（ISSO）		
e	トリアージ	21	情報システムセキュリティ運用（ISSO）		
f	インシデント管理	15	インシデントレスポンス		インシデントハンドラー
g	インシデントハンドラー	15	インシデントレスポンス		インシデントハンドラー
h	キュレーター	14 15	計算機ネットワーク防御分析 情報保障コンプライアンス		SOCアナリスト
i	リサーチャー	14	計算機ネットワーク防御分析	ITセキュリティ部門	SOCアナリスト
j	ソリューションアナリスト	13	システムセキュリティ分析		マルウェアアナリスト/プロフェッショナルセールス
k	セルフアセスメント	13	システムセキュリティ分析		マルウェアアナリスト/コンサルタント
l	脆弱性診断	17	脆弱性アセスメントと管理		ペネトレーションテスター
m	教育・啓発	20	教育と訓練		（教育サービス）
n	フォレンジックス	18	デジタルフォレンジック		フォレンジックアナリスト
o	インベスティゲータ	19	捜査		フォレンジックアナリスト
p	（なし）	22	法的助言と弁護	（法務部門）	（弁護士）
q	（なし）	24	戦略策定とポリシー開発	（IT企画部門）	コンサルタント
r	（なし）	16	計算機ネットワーク防御インフラサポート	ITシステム部門	ネットワークアナリスト

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK改訂版構成（スキルと役割・ロール）



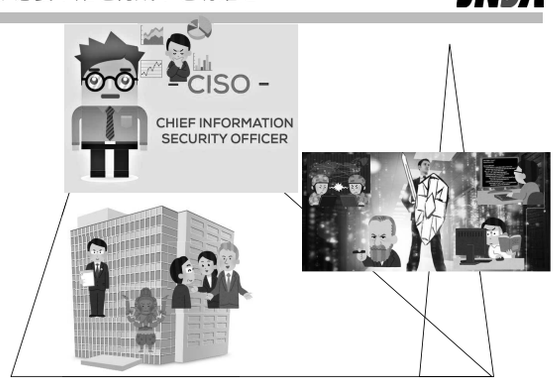
SecBoKロールとセキュリティ職種・ITSS+との連携

	役割（ロール）	役割定義（ユーザ企業における主な役割）	セキュリティベンダ職種	ITSS＋専門分野
1	CISO（最高情報セキュリティ責任者）	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。	（これらの役割は外部委託しないことを前提とする）	
2	POC（Point of Contact）	社内向けではJPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口、社内向けではIT部門関係担当社内の法務、渉外、IT部門、広報、各事業部との連絡窓口となり、それぞれ情報連携を行う。		CSIRTリエゾン
3	ノーティフィケーション	組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合には1部門と調整を行う。		
4	コマンダー トリアージ	自社で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関しては CISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。 事象に対する対応における優先順位を決定する。		CSIRTコマンド
5	インシデントマネージャー インシデントハンドラー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。 インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。社内はインシデントマネージャーに報告する。	インシデントハンドラー インシデントハンドラー	インシデントハンドリング
6	キュレーター	リサーチャーの収集した情報を分析し、その情報を自社に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）とすることが多い。	SOCアナリスト	CSIRTキュレーション
7	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。収集のみで分析はしない。	SOCアナリスト	
8	ソリューションアナリスト セルアセスメント	自社の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入された ソリューションの有効性を検証し、改善計画に反映させる。 中堅等ではリスクアセスメントを行う、インシデント対応時には脆弱性の分析、影響の調査等に対応する。	マルウェアアナリスト、プロフェッショナルセールス マルウェアアナリスト、コンサルタント	情報セキュリティアナリシス
9	脆弱性診断士	ネットワーク、OS、ミドルウェア、アプリケーションおよびセキュアプログラミングされているかどうかの検査および、是正効果の計画を行う。	脆弱性診断士（ベストレーションマスター）	脆弱性診断
10	教育・啓発	社内のリテラシーの向上、底上げのための教育及び啓発活動を行う。	（教育サービス）	
11	フォレンジックエンジニア	システム的な脆弱、構造検査、解析、報告を行う。悪意のある者は記録隠滅をすることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。	フォレンジックアナリスト	デジタルフォレンジクス
12	インベスティゲーター	外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の解明や証拠の確保、次に起こる事象の推測などを踏まえながら論理的に捜査対象を絞っていくことが要求される。	フォレンジックアナリスト	情報セキュリティインベスティゲーション
13	リーガルアドバイザー	システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する助言を行う。	（弁護士）	
14	IT企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。	コンサルタント	情報リスクストラテジ
15	ITシステム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。	ネットワークアナリスト	情報セキュリティアドミニストレーション
16	情報セキュリティ監査人	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。	情報セキュリティ監査人	情報セキュリティ監査

4．どの様に使うのか？

SecBoK利用例

誰が必要？誰を育成？を明確に



例えばキュレーター／リサーチャーを育成

分野	大項目	中項目	KSA-ID	小項目	CISO	POC	ノーティフィケーション	コマンダー・トリアージ	インシデントマネージャー	インシデントハンドラー	キュレーター	リサーチャー	ソリューションアナリスト	セルアセスメント	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	リーガルアドバイザー	コンサルタント	ネットワークアナリスト	ITシステム部門
セキュリティ基礎	知識		64	情報セキュリティシステム工学の運用に関する知識				習														
			67	機密性、完全性、可用性、盗聴及び改竄防止に関連する情報保証の基礎と組織要件に関する知識			習	習	習	習	習	習			習	習				習	習	習
			94	情報またはデータの利用、処理、蓄積及び移送に関連するリスクを管理するために用いられる情報保証の原理に関する知識			習	習	習	習	習	習			習	習				習	習	習
			95	情報技術のセキュリティ原理と手法（例：ファイアウォール、非武装地帯、暗号化）に関する知識			習	習	習	習	習	習			習	習				習	習	習
			96	ネットワーク通信、セキュリティ原理、観測、複製及び解析に関する原則の産業界の手法に関する知識			習	習	習	習	習	習	習	習	習	習	習			習	習	習
			326	サイバーセキュリティ問題に関する外部組織と学術機関に関する知識			習	習	習	習	習	習			習	習	習	習		習	習	習
			953	伝搬するセキュリティ問題、リスク及び脆弱性に関する知識			習	習	習	習	習	習			習	習	習	習		習	習	習
セキュリティガバナンス	知識		38	組織の企業情報セキュリティアーキテクチャシステムに関する知識				習	習	習			習	習								
			360	インデ/ジェンスの報告頻度、方針、手順を及び手段/報告書式、報告基準（例：要件と優先順位）、監視の実践および活動内容に関する知識				習														
			968	組織のリスク受容および/または リスク管理のアプローチに関する知識				習	習	習			習	習								

400弱のスキル項目からピックアップ

スキルマップ案　（キュレーター例）

分野	大項目	中項目	KSA-ID	小項目
基礎	ICT基礎	通信プロトコル・サービス	50	ネットワーク通信を提供するために、ネットワークサービスとプロトコルがどのように作用するかに関する知識
			81	ネットワークプロトコル（例：TCP/IP、DHCP）およびディレクトリサービス（例：DNS）に関する知識
		システム運用	28	データバックアップ、バックアップの種類（フル、インクリメンタル）及び復元コンセプトとツールに関する知識
		ビジネス基礎	897	損失評価の実施に関するスキル
セキュリティマネジメント	知識		984	計算機ネットワーク防御のポリシー、手続きおよび規制に関する知識
ネットワークセキュリティ	知識		892	ネットワーク通信のセキュアに関するスキル
			150	安全なネットワーク装置及び脆弱性の是正への理由を構成するために関する知識
			1072	ネットワーク・プロトコル、構成要素及び環境を含むネットワークセキュリティアーキテクチャのコンセプト（例：異種防御のアプリケーション）に関する知識
	トラフィック解析		17	ネットワークトラフィック解析手法に関する知識
			93	パケットレベル解析に関する知識
	侵入検知		66	侵入検知技術を適したホスト及びネットワークベースの侵入検知システムの導入検知手法と技術に関する知識
システムセキュリティ	知識		105	システムアクセスやシステムリソースとの脅威と脆弱性（例：バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQLやSQLインジェクション、競合状態、秘密の通信路、リプレイ、リターン指向攻撃、悪意のコード）に関する知識
セキュアシステム設計・構築	知識		1033	基本的なシステム管理、ネットワーク及びOSのハードニングに関する知識
セキュリティ運用	インシデント対応		60	インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識
			61	インシデントレスポンスとハンドリングの方法論に関する知識
	その他		923	セキュリティイベントの処理ツールに関する知識
サイバー攻撃手法	知識		1069	一般的な攻撃ステージ（例：フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、アクセス維持、情報収集、攻撃の実施）に関する知識
			895	脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル
	マルウェア		153	マルウェアの取扱いに関するスキル
			886	マルウェアからのネットワークの保護に関するスキル
			1028	マルウェア解析のコンセプトと手法に関する知識
	その他		941	攻撃クラスの検査（例：受動的、能動的、内部、近接、分散）に関する知識
			932	運用上の脅威環境の違い（例：第一世代（スクリプトキディ）、第二世代（非政府機関）による支援）、第三世代（政府機関）による支援）に関する知識
デジタルフォレンジック	知識		217	標準の運用手続きまたは国内標準に関する組織の完全性の維持に関するスキル

16の役割（ロール）から選別

資格試験と履修単位をSecBoKを利用してのマッピング

JNSA

前提スキル（職務遂行の前提として有しておくべきスキル）
必須スキル（職務遂行の実施に際して必要となるスキル）

分野	大項目	小項目No.	小項目	3	4	情報セキュリティマネジメント試験 出題範囲 項目No.	項目内容
1.セキュリティ基礎	総論	1-1	情報セキュリティシステム工学の原理に関する知識				
		1-2	機密性，完全性，可用性，認証及び否認防止に関連する情報保証の原理と組織要件に関する知識			1-1-1 1-1-2	情報セキュリティの目的と考え方 情報セキュリティのポイント
		1-3	情報またはデータの利用，処理，蓄積及び移送に関連するリスクを管理するために用いられる情報保証の原理に関する知識			1-1-1 1-1-2	情報セキュリティの目的と考え方 情報セキュリティのポイント
		1-4	情報技術のセキュリティ原理と手法（例：ファイアウォール，非武装地帯，暗号化）に関する知識			3-2-1 3-2-2 3-2-3	不正アクセス/クラッキング対策 マルウェア・不正プログラム対策 その他の技術的セキュリティ対策
		1-5	標準に基づいたコンセプトと能力を用いた，情報技術のセキュリティ評価，観測，検知及び改善のためのツール及び手続きの評価，実装及び普及に関する現在の産業界の手法に関する知識			2-4-3 2-6-1	改善 セキュリティ評価
		1-6	機密性，完全性及び可用性の原則の適用に関するスキル			1-1-1	情報セキュリティの目的と考え方
		1-7	サイバーセキュリティ問題に関する外部組織と学術機関に関する知識			2-4-4	コンプライアンス・組織/個人情報・情報収集
		1-8	出現するセキュリティ問題，リスク及び悪弱性に関するスキル				
2.セキュリティガバナンス	総論	2-1	組織の企業情報セキュリティアーキテクチャシステム				
		2-2	組織のリスク受容および/またはリスク管理のアプローチ				

キュレーター、リサーチャー履修単位表

NO	スキル分野	履修単位(SecBoKスキル小項目番号に対応)									
1	セキュリティ基礎	1-1	1-2	1-3	1-4	1-5	1-7				
2	セキュリティガバナンス										
3	セキュリティマネジメント	3-1	3-6	3-7	3-9	3-10					
4	ネットワークセキュリティ	4-6	4-15	4-16	4-17	4-23					
5	システムセキュリティ	5-1	5-3								
6	セキュアシステム設計構築										
7	セキュリティ運用	7-1	7-2	7-3	7-5	7-6	7-9	7-10			
8	暗号・認証・電子署名	8-1	8-2	8-3	8-4	8-5					
9	サイバー攻撃手法	9-1	9-2	9-3	9-4	9-5	9-12	9-13	9-14		
10	デジタルフォレンジック										
11	法・制度・標準	11-3	11-4								

情報セキュリティマネジメント試験シラバスと連携し、SecBoKスキル項目から履修単位にマッピングし教育体系を作成

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

モデル･コア・カリキュラムとの連携

JNSA

情報セキュリティ教育のモデル・コア・カリキュラムを3区分10種類に分け作成

区分		例示ごとの定義	育成しようとする情報セキュリティ人材像	対象者（凡例:◎） 専門人材	技術者	一般
区分1 学士課程4年間で卒業し社会に出ることを想定した区分	①	一般教養としての情報セキュリティに関する講義を対象とするもの	日常の社会生活を営む上で必要なセキュリティに関する知識を備えた人材	○	○	◎
	②	学士課程の卒業後就職を予定している広く理工系に近い学生を対象とするもの	情報セキュリティに関する基礎的な知識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	○
	③	情報セキュリティを専門とする学科等を対象とするもの	情報セキュリティに関する基礎的な知識・経験と意識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	△
区分2 学士課程4年間＋修士課程2年間の6年間の課程を経て社会に出ることを想定し、リサラシー教育が終了した学生（主に学部2年～修士1年）を想定した区分	④	修士課程に進学予定の情報系学士課程の学生を対象とするもの	情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材	◎	○	−
	⑤	情報セキュリティに関する単独の科目を対象とするもの	情報セキュリティに関する基本的な知識を備えた人材（セキュリティ分野への就職は前提としない）	△	○	○
	⑥	専門とは別に情報セキュリティを学ぶコース等を対象とするもの	習得した知識・実践的経験を自らの専門分野のセキュリティ対策に活かせる人材	△	◎	−
	⑦	情報セキュリティを専門とする専攻等を対象とするもの	情報セキュリティに関する専門的な知識と実践的な経験，及び意識を備えた人材（セキュリティの専門性をある程度兼揃できる環境への就職等を想定）	◎	○	−
区分3 情報セキュリティに関して体系的に学び直したいと考える現役IT技術者（就職後10～15年程度（30代中～後半）の技術者）を想定した区分	⑧	短期（2週間程度）集中コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	○
	⑨	中期（3～6ヶ月程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	△
	⑩	長期（1年程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	◎	△	⊢

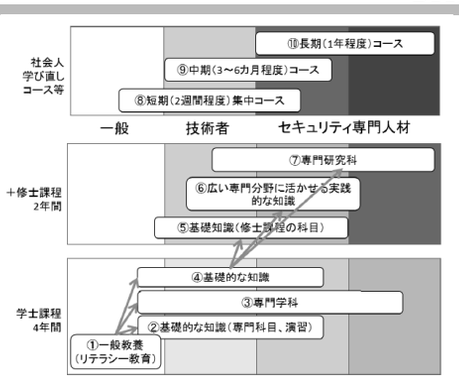
文部科学省
平成28年度理工系プロフェッショナル教育推進委託事業
「情報セキュリティ人材育成に関する調査研究　成果報告」より

http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/19/1386824_001.pdf

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

モデル･コア・カリキュラム　10例示の位置付け

JNSA



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

産業界で用いられている指標との対応　例示①

JNSA

記号凡例:
◎=演習を伴う実践的専門教育
○=座学中心の専門教育
◇=基礎的/入門的教育
★=状況に応じてケースバイケース
※=習得済が受講の前提

緑色は[産]及び[情]で求めているスキル
水色縦線は[産]のみで求めているスキル

SecBoK2016 知識項目		i コンピテンショナリディクショナリのスキル分類	メソドロジ				テクノロジ						
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	関連知識
基礎		工学基礎												
		ICT 基礎												
		ビジネス基礎												
		セキュリティ基礎									◇			
		セキュリティガバナンス												
セキュリティ専門分野		セキュリティマネジメント				◇	◇				★			
		ネットワークセキュリティ									◇			
		システムセキュリティ									◇			
		セキュアシステム設計・構築												
		セキュリティ運用				◇	◇				◇			
		暗号・認証・電子署名									◇			
		サイバー攻撃手法									★			
		デジタルフォレンジック												
		法・制度・標準				◇	◇				◇			

[産] 産業横断サイバーセキュリティ人材育成検討会「人材育成リファレンスに基づくスキルマッピング」が求めるスキル
[情] 情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

J17におけるCSとSecBoKスキル項目との連携

JNSA

J17の改訂に向けて各領域との連携を行なっている

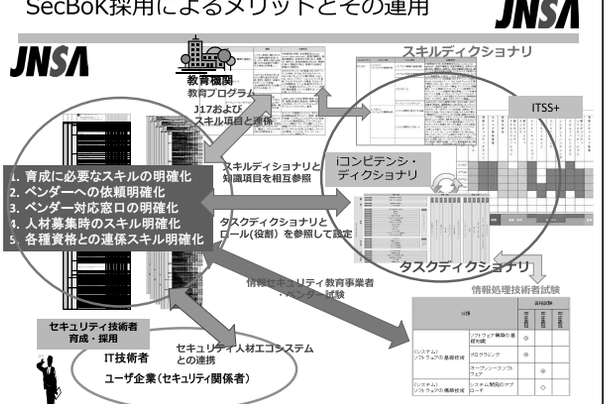
右は、CS(Computer Science)とSecBoKスキル項目との連携例である

CS	分野	大項目	中項目	小項目
●	基礎	ICT基礎	情報理論	情報理論に関する知識
				一般的なエンコード技術の識別（例：XOR, ASCII, Unicode, Base64, UUencode, URLエンコード）に関するスキル
●			計算機/ハードウェア	マイクロプロセッサに関する知識
				マンマシンインタラクションの原理に関する知識
				計算機アーキテクチャに適用される電子工学（回路ボード、プロセッサ、チップ及び関連する計算機/ハードウェア）に関する知識
				低外出ジッタ超コンピューティングのコンセプトに関する知識
				物理的及び仮想的ルータとストレージシティブの特性に関する知識
				パーソナルコンピューターの処理的分配に関するスキル
				多様な構成要素と周辺機器の機能を含む，基本的な物理的コンピュータの構成要素とアーキテクチャに関する知識
				電子デバイス（例：コンピュータシステム／構成要素，アクセス制御デバイス，デジタルカメラ，電子手帳，ハードドライブ，メモリカード，モデム，ネットワーク機器要素，プリンタ，リーダー/ライター，携帯電話，スキャナ，電話，コピー機，クレジットカードリスキマー，ファクシミリ，GPSなど）に関する知識
●			ネットワーキング	計算機ネットワークの基礎に関する知識
				組織のLAN/WANの役割に関する知識
				LAN/WANの原理（コンセプト）等地管理を含むに関する知識
				ネットワーク設計（アンコミセンティの目的，運用の目的及びハードオフに関する理解を含むに関する知識
				ネットワークハードウェアデバイスと機能に関する知識
				ネットワークインフラをサポートする通信手法，原理及びコンセプト（例：暗号化，デュアルハブ，時分割多重化）に関する知識
				ネットワークの設備の能力とアプリケーション（ハブ，ルータ，スイッチ，ブリッジ，サーバ，移送メディア及び関連するハードウェア等含む）に関する知識
				合理と要件に関する分析に関する知識
				回路解析に関する知識
				通信のコンセプトに関する知識
				既存ネットワークの範囲（例：PBX, LAN, WAN, Wi-Fi）に関する知識
				ネットワークトラフィックの能力とパフォーマンス特性の範囲に関するスキル
				ネットワークインフラの事業継続及び回復計画の作成，テスト及び実施に関するスキル
				LANのインストール，設定及びトラブルシューティングに関するスキル
				通信メディアの基本コンセプト，周波数及び範囲での適用（例：計算機/電話のネットワーク，衛星，ファイバ，無線）に関する知識
				ネットワークの通信の範囲とを理解（例：LAN, WAN, MAN, 無線LAN, 無線WAN）に関する知識
				GSMアーキテクチャに関する知識
				ネットワークシステム管理の原理，モデル，手法（例：エンドツーエンドのシステムパフォーマンスモニタリングおよびツールに関する知識
				通信方式（例：Bluetooth, RFID, 赤外線通信, Wi-Fi, ポケットベル，携帯電話，衛星等電アンテナ）及び/または，不正ないない情報の通信を可能とする，またはインストールされたシステムの正しい運用を妨げるジャミング技術に関する知識

Copyright (c) 2018 NPO日本ネットワークセキュリティ協会

SecBoK採用によるメリットとその運用

JNSA



Copyright (c) 2018 NPO日本ネットワークセキュリティ協会