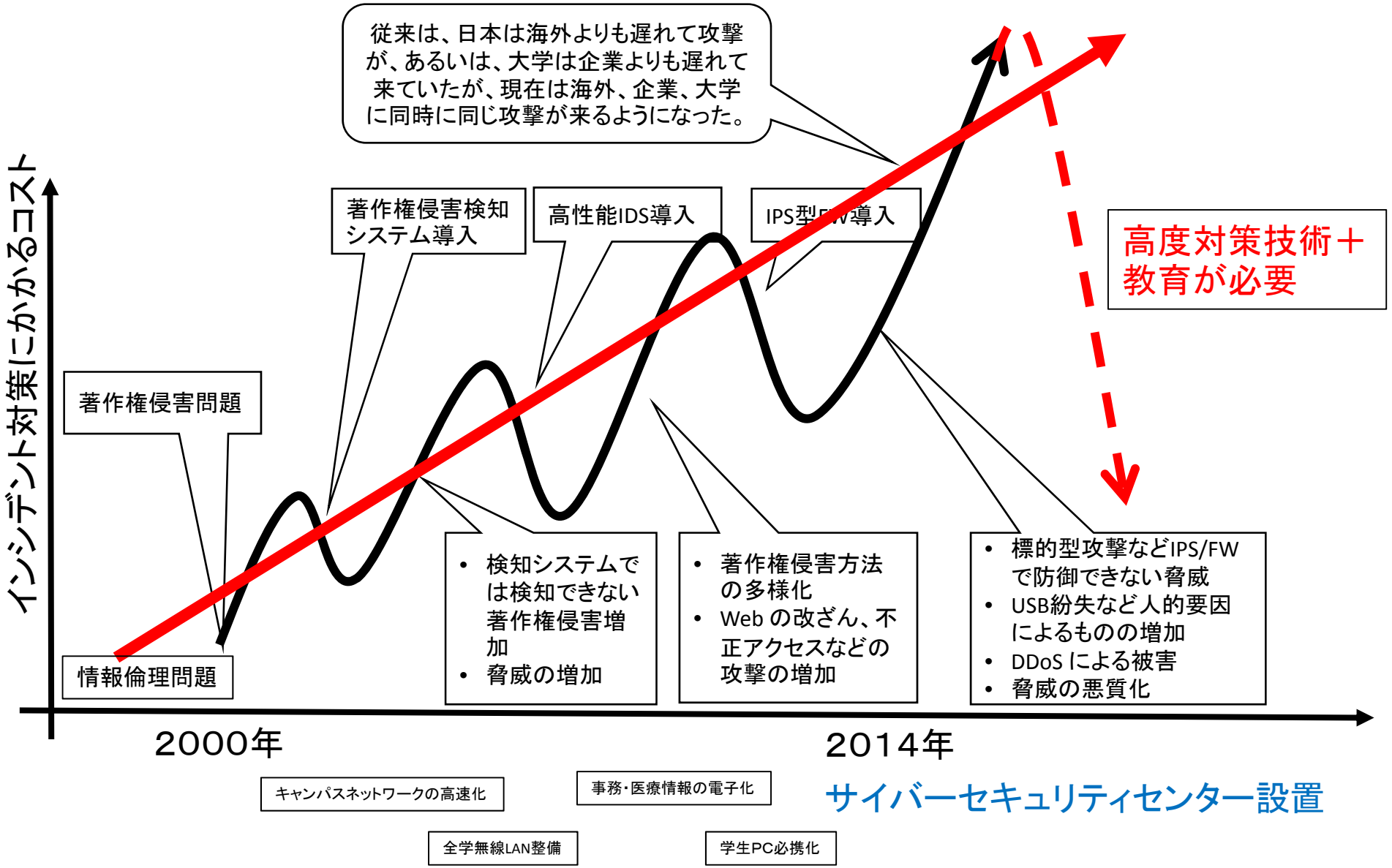
リテラシー教育としてのサイバーセキュリティ

岡村耕二
九州大学　サイバーセキュリティセンター

自己紹介

- 1990　　九州大学大学院修士課程修了
- 1990-92　民間企業
- 1993-95　奈良先端科学技術大学院大学助手
  - 教室系
- 1996-97　神戸大学総合情報処理センター
- 1998-99　九州大学情報処理教育センター
- 2000-　　九州大学情報基盤センター
- 2007-　　九州大学情報基盤研究開発センター
- 2014-　　九州大学サイバーセキュリティセンター

ICT 整備とインシデント、その傾向
現在のインシデント対策には新しいパラダイムが必要



九州大学におけるサイバーセキュリティの全学必須化について

- 2014年度　トップダウン的に開始
  - 減らない学生の著作権・倫理に関わるインシデント
  - 減らない教職員の情報倫理に関わるインシデント
    - 全学生に一律に現在教えるべきことを正しく教育する。
  - サイバーセキュリティセンターの設置
- 2014年度後期　選択科目で開講し、実績作り
- 2015年度
  - 教育企画委員会で審議
    - 2017年度から必須化にすることを全学決定
  - 基幹教育院で実施の協議
    - 科目増は不可能
    - 情報系科目の整理
      - 文系の選択的情報リテラシ教育
      - 理系の過剰なプログラミング系演習
      - 黎明期的な情報・ネットワークリテラシ教育の整理

~~本申請の概要~~

世界　サイバー脅威への対策は国家レベルの問題
(サイバー犯罪の損失額は全世界で年間59兆円、平成25年)

日本　サイバーセキュリティ基本法(平成26年)

八条：大学その他の教育研究機関の責務
- 自組織の自主的なサイバーセキュリティの確保
- サイバーセキュリティに係る**人材の育成**
- サイバーセキュリティに関する**研究**
- その成果の普及や国，地方公共団体への協力

九州大学

サイバーセキュリティの確保 ― 情報基盤センター(平成12年)・情報統括本部(平成19年)

人材教育
- 社会に送り出す卒業生・修了生のサイバーセキュリティの知識・能力を向上
- 世界水準の専門的知識を有する人材の育成

増え続けるサイバー攻撃への対処，全学ITシステムの安定的運用支援への還元できる実用的研究

研究
- 先進的、全学横断的、社会科学を取り入れたグローバルなサイバーセキュリティ研究の実施

サイバーセキュリティセンター(平成26年)

国内の機関

海外の機関

サイバーセキュリティセンターに
教授1、准教授 2、助教1の増員をお願いしたい

社会への還元

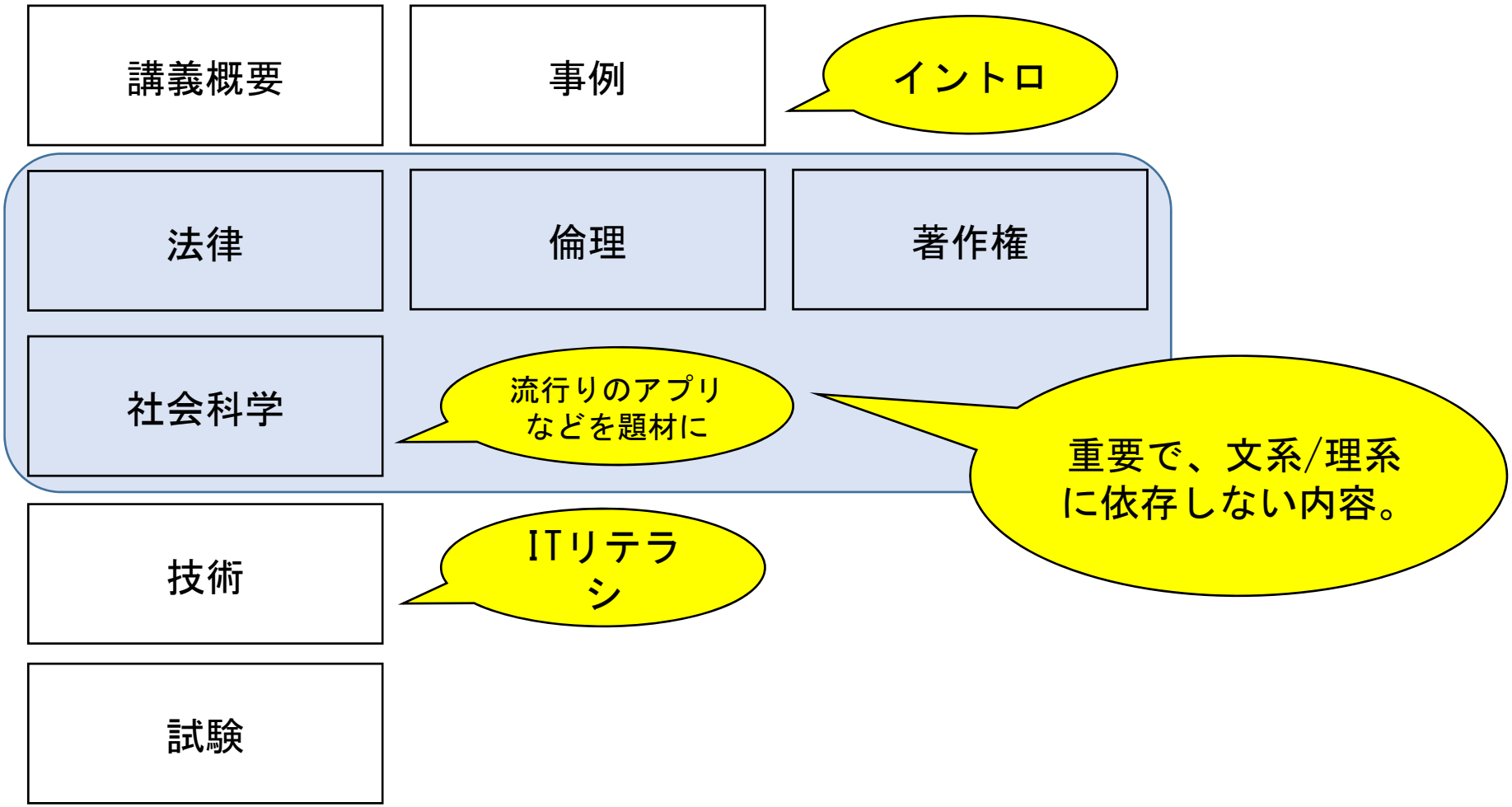
九大をこの分野のトップランナーへ

全ての学生がサイバーセキュリティを学ぶ理由

- サイバーセキュリティ基本法（2014年11月6日成立）
  - 教育研究機関の責務）第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
  - （国民の努力）第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

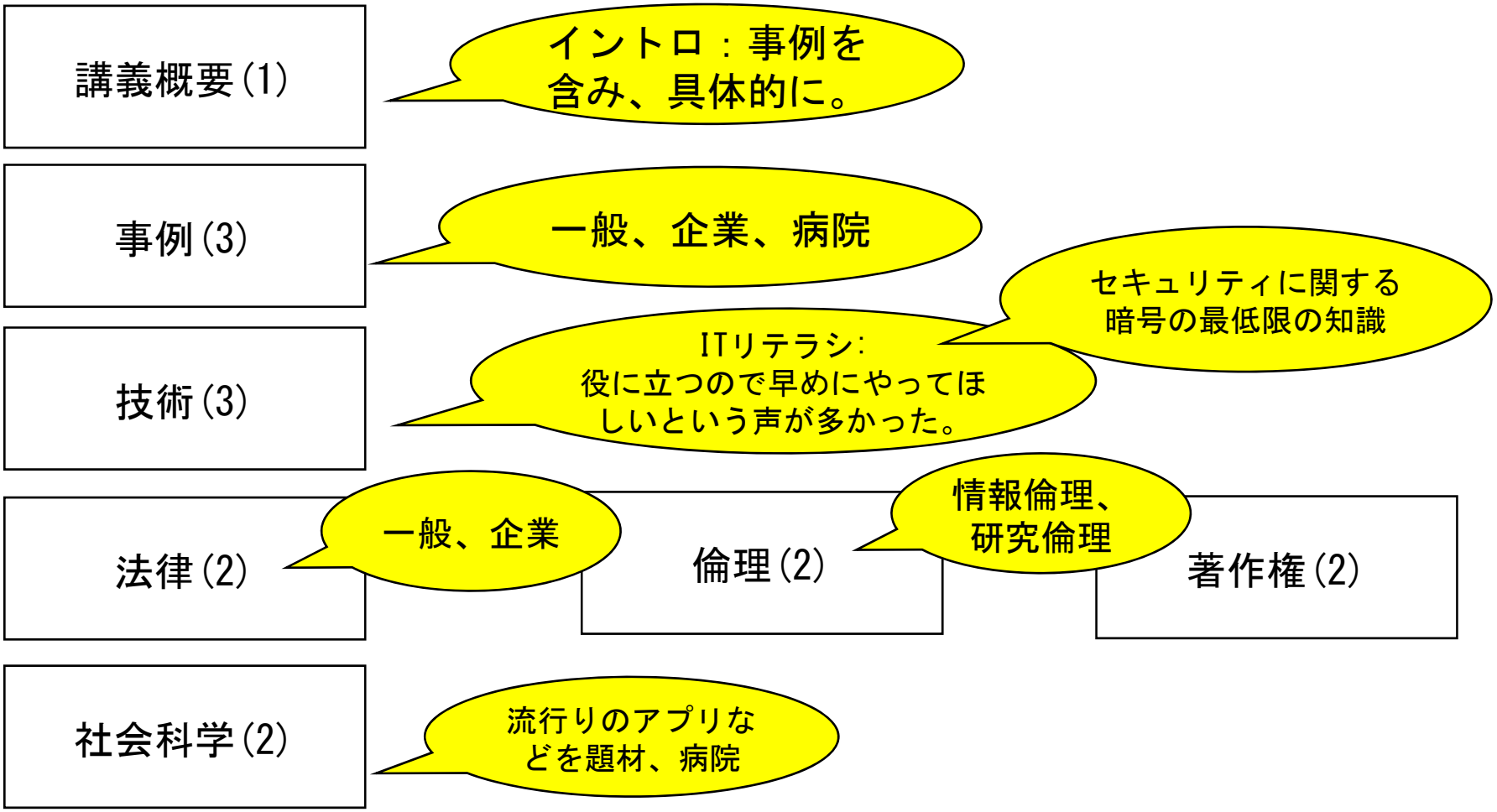
シラバス 2014年版（クォーター）

講義の目的
文系、理系区別なく、大学生がIT（サイバー空間）を利用する上で最低知っておくべきことを学ぶ。



シラバス 2016年版（セマスター）

講義の目的
文系、理系区別なく、大学生がIT(サイバー空間)を利用する上で最低知っておくべきことを学ぶ。



講義に対する感想
導入とサイバーセキュリティに関する最近の話題

- とても難しそうだなと思いましたが、知っておかなければならないことでもあるなと思いました。
- 初めて参加しました。今後役立つであろう情報を得ることが出来たので、非常に有意義な90分を過ごせたと思います。
- スパムメールに気をつけておけば、セキュリティは問題ないと考えていたので、マルバタイジング攻撃なるものの存在を知ってその無知さ加減を思い知らされた。これからセキュリティに対する知識を深めていきたいと思う。
- 思ったより面白そうな講義でよかったです。将来の生活に直接役立ちそうだと思いました。
- 今回の授業の中で初めて聞く言葉がたくさんありましたが、説明がわかりやすくて自分なりに理解できたと思います。
- 授業の内容はけっこう難しくて、理解するのが大変に感じたけど、自分が安全にパソコンやスマホを使っていくうえでとても役に立つ授業だと感じた。また、セキュリティ対策のことは自分でちゃんとわかっているつもりだったけど、知らないことが多くて、得るものの多い授業だったのでとてもおもしろかったです。
- 具体例よりも一般的な説明を優先したほうが理解しやすいかもしれません。
- 難しく感じます。
- 小テストの設問に対する答えをスライドや講話から探すのが困難だった。
- 小テストにだすことは、授業中に説明してほしいです。　標的型攻撃やフィッシング攻撃の説明はすごくわかりやすかったです。
- 小テストの内容は講義資料から見て分かるものにしてほしい。
- 小テストの要領がつかめない。
- よくわからない言葉が出てきて難しかった。
- 小テストの質問内容がくくりが大きく答えづらいものがある。関係性の説明は必ず入れなければならないキーワードなどがないとどの部分における関係性を答えればいいのかわからない。
- 問題が難しかったので三択問題がいいです。

講義資料

小テスト

1. 最近、サイバー犯罪が増えている理由について簡単に説明せよ。
2. 標的型攻撃とフィッシング攻撃の関係を説明せよ。
3. マルバタイジング攻撃のように避けられない攻撃にはどのように対応するのがよいと思いますか。
4. CTF とは何の略でしょうか。また、簡単に説明してください。
5. 講義に対する感想、要望を書いてください。（これは評点の対象にはなりません。）

ベネッセ個人情報流出事件

- 2014年7月9日に発覚したベネッセコーポレーション（ベネッセ）の大規模個人情報流出事件。
  - 内部犯行
  - データベースのあるサーバルームには、外部機器(PCや USB デバイス)の持ち込みは禁止されている。
  - エンジニアがデータベースサーバにスマートフォンを直接 USB 接続し、データを抜き取る。
    - サーバルームの監視カメラ
    - データベースサーバの記録
  - エンジニアは逮捕される。
    - 不正競争防止法違反（営業秘密の複製、開示）

講義資料

ベネッセ個人情報流出事件

- ベネッセのみに登録したはずの個人情報を使ったダイレクトメールが、別の通信教育を行う会社から届くようになり、個人情報が漏洩しているのではないかという問い合わせの急増により発覚
- 影響 (一部)
  - ベネッセのプライバシーマーク付与が取り消される。
  - 責任部署にいた二人の取締役が引責辞任
  - 顧客情報漏洩件数を3504万件と公表。個人情報漏洩被害者へ補償として金券500円を用意するとした。
    - 35,040,000 x 500 = ~~約17億円~~ 約175億円
      - 名簿計約7万5000件を計約60万円で購入
      - 8円/件

年金機構の事例
-年金管理システムサイバー攻撃問題-

- 外部の不正アクセスによって、日本年金機構の年金情報管理システムサーバから個人情報が流出した問題
  - コンピュータウイルスメールは5月8日から5月18日に、大量に届き、少なくとも2人の職員が開封していた。1回目の開封は5月8日に、職員が「『厚生年金基金制度の見直しについて（試案）』に関する意見」というタイトルの電子メールの添付ファイルを開けてしまった。
  - インターネットに接続出来るパーソナルコンピュータで、個人情報のサーバにもアクセスできるコンピュータネットワーク設計だった
  - 標的型メール

講義資料

技術とビジネス

- 必要に応じて技術が開発され、その技術に市場性があれば、ビジネス(金儲け)として発展します。
- ビジネスが発展すれば、技術開発が加速します。
- サイバーセキュリティ
  - 攻撃をする技術
    - 金儲けとして成功
      - さらに高度な攻撃技術の開発
  - 防御する技術開発・ビジネスの急増

講義資料

標的型攻撃

- APT（Advanced Persistent Threat）攻撃
- OS やブラウザーの既知の脆弱性を利用する。
- 巧みなフィッシングメールで、脆弱性を利用して外部アクセスを可能にするソフトウェア等が潜むコンテンツをもったサイトに誘導され、そのソフトをダウンロードさせられ、実行してしまう。
- 外部とそのソフトウェアが通信可能になり、外部からの操作で、情報漏洩などが行われる。
- 特定個人が狙い撃ちされる。
- ファイアウォール、アンチウイルス、イントラネット内でも被害にあう。対策は、脆弱性をふさぐ、または、フィッシングメールを見抜くしかないが、非常に困難

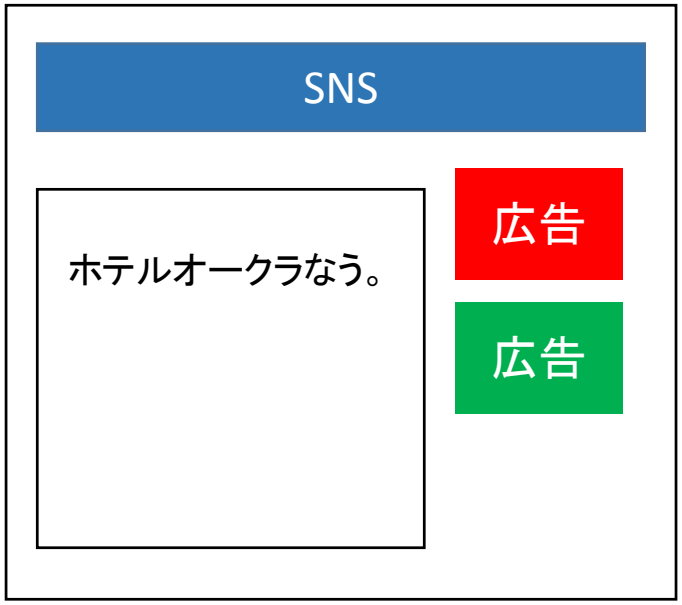
講義資料

避けられない脅威

フィッシング (Mail)
→ リテラシ

水飲み場型攻撃(Web)
→ Firewall

防御は不可能ではない。/確率が低い



- 広告に、Adobe フラッシュが用いられている。
- SNSを開けば、フラッシュファイルが自動にダウンロードされる。（避けられない）
- 広告は、だれでも出せる。支払いは匿名。
- SPAM でフィッシングメールを送るより、安く、確実。

ゼロデイ攻撃

開いただけで感染

情報漏洩、ランサムウェア

マルバタイジング攻撃

講義に対する感想
法律を知る

- 九州大学にもセキリュティポリシーと情報倫理規定があると初めて知った。法律や規定ができたのには、すべて背景があり、これを知っておくことは自分を守ることにもつながるので、今回の講義で学んだことを覚えておきたい。
- 最近になってやっと法律ができはじめていて、それ以前はほんとに無秩序だったことにとてもびっくりした。今でこそネットが世界を動かしているのだから、ネットに関する法律をもっと整備していくことが大切だと思う。
- 法律について全く知らなかったので、今回の授業はかなりためになった。特に、クラウドを使う際には気を付けようと思った。
- 知らない法律がたくさんあって少し怖いなと思いました。
- 不正アクセス行為に関する法律はごく最近に制定されたことに驚いた。自分たちが生まれたころにはすでに普及していたのであまり実感がない。
- クラウドなどのサービスを利用するときに、事前にどういうシステムなのか調査をし、身近な法律などを少しは目を通す必要があるなと思いました。
- 自分は法学部に在籍するため、法律と倫理の区別という問題はこれからの課題として考察していきたいと感じた
- 九州大学で利用しているIDやedunetにも規則がちゃんと存在しているのだと分かった。これからも取り扱いに気を付けていきたい。
- 今日の講義では、今まで知らなかった法律などを学ぶことができました。九州大学の情報倫理規定やセキュリティポリシのことも知らなかったので、家でじっくり読んでみたいです。
- 選択肢にしてもらえるとありがたいです。
- なにを言っているかわからなかった
- 問題を選択にしてほしい。
- 選択肢問題を希望します。なかなか記述だとどう書けばいいか悩みます。
- セキュリティポリシーの検索の説明がわかりにくく、問題の解答が困難だったのでせめてURLを講義資料に載せるなどしてほしかったです。
- 小テストの問題がスライドを見ても分からない。
- 口頭での説明のみだと聞き落としがちなのでスライドにも詳しく書いていただけると嬉しいです。
- 小テストの問題が難しいのでもう少し簡単にしてほしいです。
- 講義の内容と小テストの内容があまりリンクしていない気がします。
- 今回の授業は少しスライドがわかりつらかったと思います。もう少し、初心者用にやさしくしていただけると助かります。
- 問題が難しすぎる。スライドを見てもなにも参考になりそうなことが書いてない。先生の説明を聞き逃したら終わり。もう少しスライドを授業に沿ったものにしてほしい。セキュリティの非常に重要なのでしっかり理解しておきたい。

講義資料

小テスト

1. 不正アクセス行為の禁止等に関する法律が施行される以前は、不正アクセスが行なわれた場合どのような処置が取られていたでしょうか。
2. クラウドをビジネスで利用する時に特に法律的に注意しなければいけないのはどのような点についてでしょうか。
3. 九大生以外の友人に kitenet や edunet でインターネットに接続されたノートパソコンを使用させると、九州大学セキュリティポリシに反することになるでしょうか。理由をつけて解答して下さい。
4. 講義に対する感想、要望を書いてください。

刑法（けいほう、明治40年法律第45号）

- 犯罪に関する総則規定および個別の犯罪の成立要件やこれに対する刑罰を定める日本の法律。
- 明治40年（1907年）4月24日に公布、明治41年（1908年）10月1日に施行。
- 広義の「刑法」と区別するため、刑法典とも呼ばれる。
- 日本において、いわゆる六法を構成する法律の一つであり、基本的法令である。
- ただし、すべての刑罰法規が刑法において規定されているものではなく、刑事特別法ないし特別刑法において規定されている犯罪も多い。

講義資料

刑法（けいほう、明治40年法律第45号）

- 1987年の改正で、コンピュータ犯罪を防止するための3法が追加
  - 電子計算機損壊等業務妨害罪
  - 電磁的記録不正作出及び供用罪
  - 電子計算機使用詐欺罪

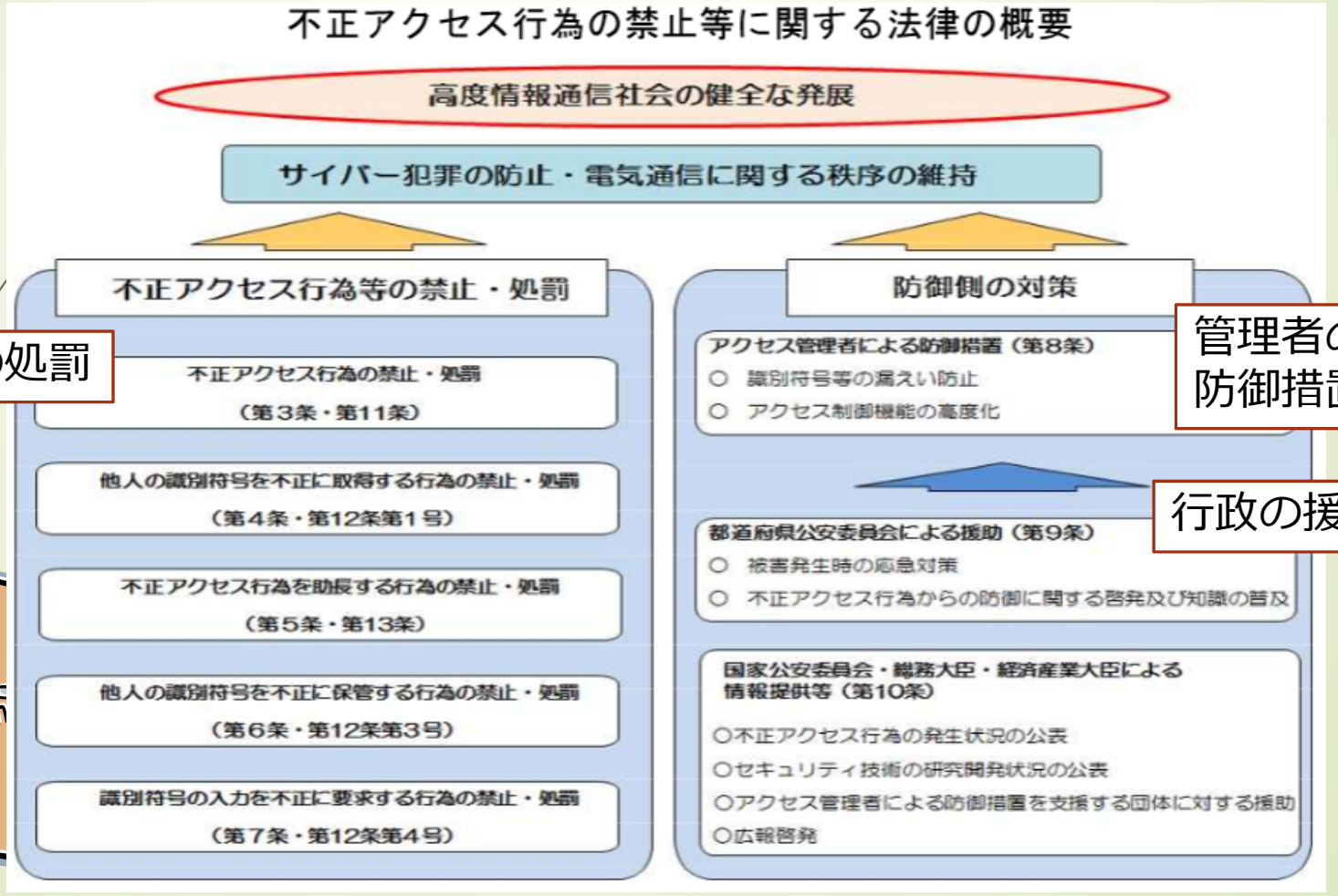
- コンピュータやデータの破壊や改ざんには刑事罰が科せられる

講義資料

不正アクセス行為の禁止等に関する法律（平成11年 (1999年) 8月13日法律128号）

https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf

行為者への処罰



管理者の防御措置

行政の援助

不正アクセス行為の禁止等に関する法律

講義資料

- 他人の識別符号を**不正に取得する行為**の禁止、処罰
  - 不正アクセス行為の用に供する目的で、他人の識別符号（パスワード等）を取得してはならない（4条）。
  - 違反者は1年以下の懲役又は50万円以下の罰金に処せられる（12条1号）。
  - 平成24年改正で新たに禁止された。
- **不正アクセス行為を助長する行為**の禁止、処罰
  - 何人も、業務その他正当な理由による場合を除いては、他人の識別符号（パスワード等）を、アクセス管理者及び利用権者以外の者に提供してはならない（5条）。違反者は1年以下の懲役又は50万円以下の罰金に処せられる（12条2号）。
  - 平成24年改正で、どの特定電子計算機の特定利用に係るものであるかが明らかでない識別符号を提供する行為も新たに禁止された。
- 他人の識別符号を**不正に保管する行為**の禁止、処罰
  - 何人も、不正アクセス行為の用に供する目的で、不正に取得された他人の識別符号を保管してはならない（6条）。違反者は1年以下の懲役又は50万円以下の罰金に処せられる（12条3号）。
  - 平成24年改正で新たに禁止された。

講義資料

クラウド利用と外国の法律
（経済産業省より）

http://www.publicpolicy.telefonica.com/blogs/blog/2011/05/19/cloud-computing-isn%E2%80%99t-just-a-buzzword-2/

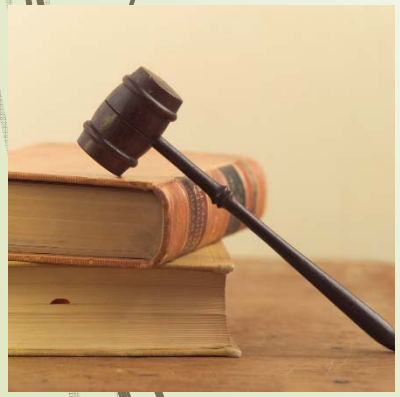
- データの物理的保存場所がわからない場合がある
  - 海外の大規模クラウド事業者が提供するサービスの場合、自分のデータが**どの国に設置されたサーバに保存されているかを特定できない場合がある**
  - 法規制上の制約（後述）や、司法の実効性を考えた場合、国内のサーバに保存することを確約する事業者を選択することも必要
- 米国愛国者法（USA Patriot Act）
  - 2001年9月11日に発生した同時多発テロ事件を受け、捜査機関の権限の拡大や国際マネーロンダリングの防止、国境警備、出入国管理、テロ被害者への救済などについて規定
  - テロリズムやコンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信や電子的通信を傍受する権限を明記
  - **捜査機関は金融機関やプロバイダの同意を得れば、裁判所の関与を求めることなく操作を行うことができる**ことを規定
    - 米国サーバにデータを保存する場合は、政府機関の捜査権限が大きいことに留意が必要
    - クラウドサービスを利用する場合、仮想的に分離された環境であっても、他ユーザと物理的に同一のサーバ機器などを共有している場合があるため、**他ユーザが捜査を受けることで、自社もシステム停止などの影響を受けるリスク**がある

講義資料

九州大学でのセキュリティに関する規定など

- 九州大学セキュリティポリシ
- 九州大学情報倫理規定

- 企業コンプライアンス（corporation compliance）
  - **コーポレートガバナンスの基本原理の一つ.** 企業が法律や内規などのごく基本的なルールに従って活動すること．ビジネスコンプライアンスという場合もある。
  - 「コンプライアンス」は「企業が法律に従うこと」に限られない「遵守」「応諾」「従順」などを意味する語だが，ここでは「法令順守」の意味で使用．**「社会規範，企業倫理」を含める**意見もある.



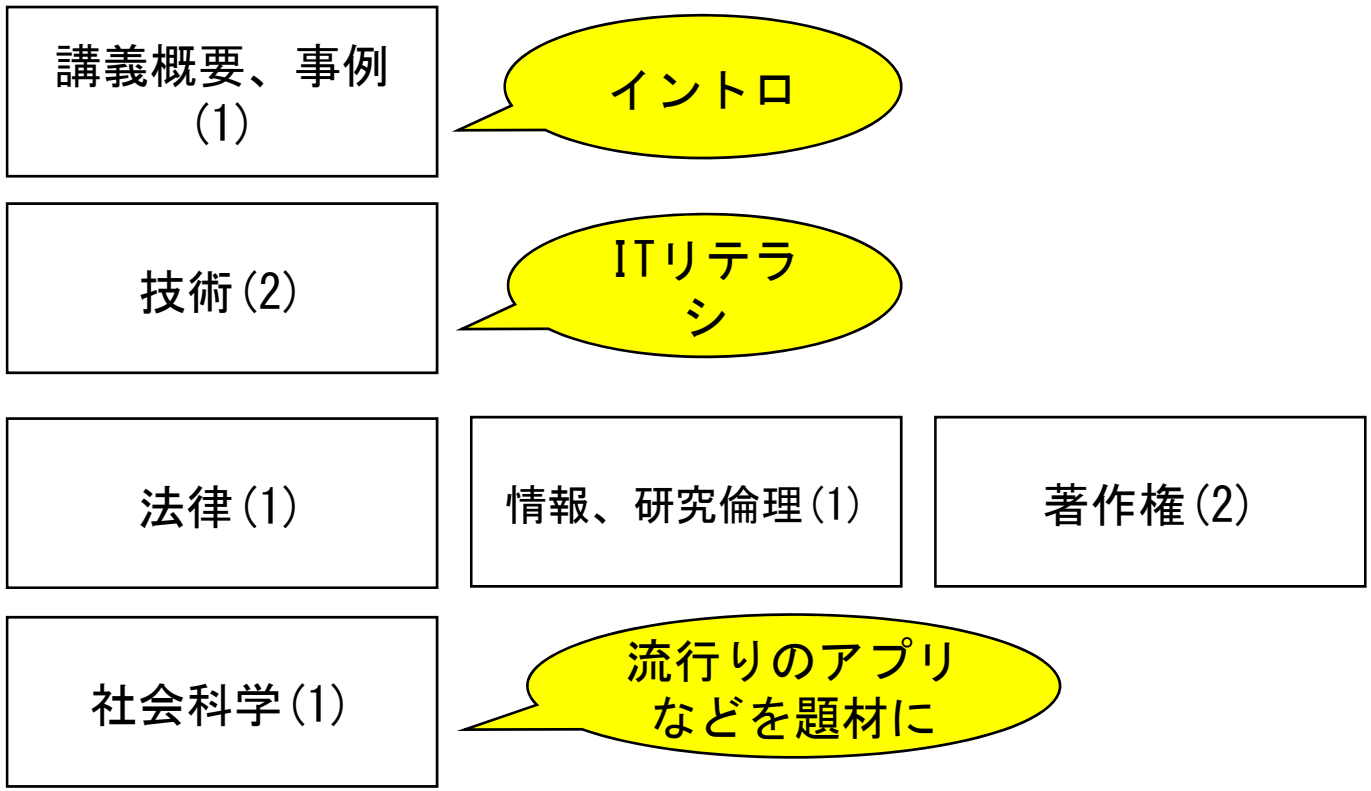
- 企業 = 九州大学

食品の偽装表示・不正会計・不正入札・クレームの隠蔽(いんぺい)・盗聴事件などの不祥事の頻発が背景

http://dictionary.sanseido-publ.co.jp/topic/10minnw/003compliance.html

シラバス 2017年～（クォーター）

講義の目的
文系、理系区別なく、大学生がIT(サイバー空間)を利用する上で最低知っておくべきことを学ぶ。



一般的なサイバーセキュリティ教育に用いる科目構成

応用数学は除く

暗号技術	電子署名と PKI	バイオメトリック認証	デジタル フォレンジック
情報 ハイディング	アクセス制御	不正 プログラム 対策	セキュリティ 評価
情報 セキュリティ ポリシー	プライバシー 保護	法制度	

IPA IT スキルとの対応

レベル7 Worldwide		
レベル6 日本ならどこでも活躍できる		
レベル5 組織のエース		
レベル4 人材育成・指導可能	高度情報処理技術者試験	(ST)(SA)(PM)(NW) (DB)(ES)(SC)(SM) (AU)
レベル3 自立して行動可能	応用情報技術者試験	(AP)
レベル2 命令遂行可能	基本情報技術者試験 情報セキュリティマネジメント試験	(FE)(SG)
レベル1 必要最低限の基礎知識	ITパスポート試験	(IP)

国家試験

2015年　ITパスポート 問題

問1　著作者の権利である著作権が発生するのはどの時点か。

ア　著作物を創作したとき　　イ　著作物を他人に譲渡したとき
ウ　著作物を複製したとき　　エ　著作物を文化庁に登録したとき

問24　個人情報保護法では個人情報取扱事業者に対して安全管理措置を講じることを求めている。経済産業分野のガイドラインでは，安全管理措置は技術的安全管理措置，組織的安全管理措置，人的安全管理措置，物理的安全管理措置に分類している。このうち，人的安全管理措置の具体例として，適切なものはどれか。

ア　安全管理に対する規程と従業員による体制の整備
イ　安全管理に対する従業員の役割及び責任についての周知や教育の実施
ウ　個人データを取り扱う情報システムへの従業員ごとのアクセス制御
エ　従業員の入退出管理や個人データを記録した媒体の施錠管理

問28　アクセス管理者は，不正アクセスからコンピュータを防御する役割を担う。不正アクセス禁止法において，アクセス管理者が実施するよう努力すべきこととして定められている行為はどれか。

ア　アクセス制御機能の有効性を検証する。
イ　アクセスログを定期的に監督官庁に提出する。
ウ　複数の人員でアクセス状況を常時監視する。
エ　利用者のパスワードを定期的に変更する。

問51　情報セキュリティの対策を，技術的セキュリティ対策，人的セキュリティ対策及び物理的セキュリティ対策の三つに分類するとき，物理的セキュリティ対策に該当するものはどれか。

ア　従業員と守秘義務契約を結ぶ。
イ　電子メール送信時にディジタル署名を付与する。
ウ　ノート PC を保管するときに施錠管理する。
エ　パスワードの変更を定期的に促す。

問56　無線LANのセキュリティを向上させるための対策はどれか。

ア　ESSID をステルス化する。
イ　アクセスポイントへの電源供給は LAN ケーブルを介して行う。
ウ　通信の暗号化方式を WPA2 から WEP に変更する。
エ　ローミングを行う。

問58　情報セキュリティの観点から，システムの可用性を高める施策の例として，最も適切なものはどれか。

ア　生体認証を採用する。　　イ　ディジタル署名を行う。
ウ　データを暗号化する。　　エ　ハードウェアを二重化する。

2015年　ITパスポート 問題・回答

問１　著作者の権利である著作権が発生するのはどの時点か。

ア　著作物を創作したとき
イ　著作物を他人に譲渡したとき
ウ　著作物を複製したとき
エ　著作物を文化庁に登録したとき

問24　個人情報保護法では個人情報取扱事業者に対して安全管理措置を講じることを求めている。経済産業分野のガイドラインでは，安全管理措置は技術的安全管理措置，組織的安全管理措置，人的安全管理措置，物理的安全管理措置に分類している。このうち，人的安全管理措置の具体例として，適切なものはどれか。

ア　安全管理に対する規程と従業員による体制の整備
イ　安全管理に対する従業員の役割及び責任についての周知や教育の実施
ウ　個人データを取り扱う情報システムへの従業員ごとのアクセス制御
エ　従業員の入退出管理や個人データを記録した媒体の施錠管理

問28　アクセス管理者は，不正アクセスからコンピュータを防御する役割を担う。不正アクセス禁止法において，アクセス管理者が実施するよう努力すべきこととして定められている行為はどれか。

ア　アクセス制御機能の有効性を検証する。
イ　アクセスログを定期的に監督官庁に提出する。
ウ　複数の人員でアクセス状況を常時監視する。
エ　利用者のパスワードを定期的に変更する。

問51　情報セキュリティの対策を，技術的セキュリティ対策，人的セキュリティ対策及び物理的セキュリティ対策の三つに分類するとき，物理的セキュリティ対策に該当するものはどれか。

ア　従業員と守秘義務契約を結ぶ。
イ　電子メール送信時にディジタル署名を付与する。
ウ　ノート PC を保管するときに施錠管理する。
エ　パスワードの変更を定期的に促す。

問56　無線LANのセキュリティを向上させるための対策はどれか。

ア　SSID をステルス化する。
イ　アクセスポイントへの電源供給は LAN ケーブルを介して行う。
ウ　通信の暗号化方式を WPA2 から WEP に変更する。
エ　ローミングを行う。

問58　情報セキュリティの観点から，システムの可用性を高める施策の例として，最も適切なものはどれか。

ア　生体認証を採用する。
イ　ディジタル署名を行う。
ウ　データを暗号化する。
エ　ハードウェアを二重化する。

サイバーセキュリティ基礎論：評価について。

- 2014年後期から基幹教育オープン科目で開講
  - 平成２６年度後期：３８名
  - 平成２７年度前期：５５名
  - 平成２７年度後期：１１５名
  - 平成２８年度前期：２２０名
- 2014年度
  - ペーパー試験(期末) + 演習(毎週)
- 2015年度
  - Moodle を使ったオンラインで試験(４択問題、期末) + 演習(毎週)
  - 出席をとっていないので、出席率が悪い。
- 2016年度
  - Moodle を使ったオンライン小テストを毎週実施
  - 期末試験は無し

- 工学部、医学部、経済学部、芸術工学部、法学部、理学部、教育学部、薬学部、農学部
- 歯学部以外

サイバーセキュリティ基礎論ルーブリック

		A	B	C	D	F
知識・理解 （３０点満点）	講義の内容について正しく理解している。 （３０点満点）	十分に理解できている。 （２７～３０点）	理解できている。 （２４～２６点）	ある程度理解できている。 （２１～２３点）	一部のみ理解できている。 （１８～２０点）	全く理解できていない。 （０～１７点）
専門的技能 （３０点満点）	サイバーセキュリティに関する専門的な知識について正しく理解している。 （３０点満点）	十分に理解できている。 （２７～３０点）	理解できている。 （２４～２６点）	ある程度理解できている。 （２１～２３点）	一部のみ理解できている。 （１８～２０点）	全く理解できていない。 （０～１７点）
汎用的技能 （３０点満点）	講義で得た知識を応用して自分の生活に役立たせることができる。 （３０点満点）	十分にできる。 （２７～３０点）	できる。 （２４～２６点）	ある程度理解できる。 （２１～２３点）	一部のみ理解できる。 （１８～２０点）	全くできない。 （０～１７点）
態度・志向性 （１０点満点）	講義スライド以外の事項を自ら調べて学習している。 （１０点満点）	十分に学習している。 （９～１０点）	学習している。 （８点）	ある程度学習している。 （７点）	一部のみ学習している。 （６点）	全く学習していない。 （０～５点）

課題・今後の展望

- 1学年 2,600名のため、150-180x 15 で計画。
- 200人クラスのため学生の管理が課題
  - 現在の200人超クラスで経験済み
  - 授業内容の理解の確認
    - 期末試験は行わず、授業ごとに小テストを実施する。
    - eラーニングシステムで。
      - 記述式 ×
      - 選択式 ○
  - 単位認定
    - 基本的には、各授業の小テストを総合的に評価
- 講義の評価
    - 九大生はセキュリティに強くなったか？
      - 定量的な証拠
- 英語授業