サイエンティフィック・システム研究会
Scientific Systems
ISSN 1883-5554

SS 研ニュースレター選集

vol.19

SS研ニュースレター選集 Vol.19 目次

「SS研ニュースレター選集」は、サイエンティフィック・システム研究会(SS研)の活動報告として、1年間の講演資料から代表的なものを選出して冊子としたものです。
毎年5月のSS研通常総会に合わせて発行しています。

(敬称略)

巻頭言

サイエンティフィック・システム研究会
会長　　松尾　裕一
(国立研究開発法人宇宙航空研究開発機構)

サイエンティフィック・システム研究会(SS 研)は、大学や研究所などの科学技術分野におけるコンピュータ利用機関を主体とした研究会として 1978 年に設立されました。以来 40 年間、会員間の相互利益を図ることを目的に、各種の分科会や WG などの活動を通じて、コンピュータのシステム技術、応用技術、利用技術に関する質の高い情報共有・情報交換の場、ユーザとベンダー間の高度な議論の場としての役割を果たしてきています。これらのうち、分科会活動の内容は『ニュースレター』で随時ご紹介しているところです。

この 1 年間の SS 研の活動を振り返ってみますと、本冊子の巻末の活動一覧にあります通り、分科会、WG、タスクフォースともいずれも時宜を得た企画であり、有益な講演やディスカッションを行うことができたと思います。その中でも特に会員の皆様のご参考となると思われる講演資料を、皆様からのアンケート結果を参考にしながら選び出したのが、この『ニュースレター選集』です。

全脳シミュレーションに向けた京による大脳皮質-視床-小脳の神経回路シミュレーションや HPCI を活用した FMO 創訳技薬技術の開発に関する科学技術計算の話題、大学における情報セキュリティの取組みや効率的かつ効果的な CSIRT の運営、NII-SOCS の運用から浮上してきたセキュリティ対策等のシステム技術に関する話題、アクティブラーニングの失敗事例、高等学校新学習指導要領におけるデータサイエンスの扱い等の教育環境に関する話題、日本発 空飛ぶクルマ 'SkyDrive' 開発への挑戦についての話題等々、正に旬なテーマを反映した選集になっているかと存じます。

19 年の長きに渡り『ニュースレター選集』を発刊できたこと、今号第 19 巻を、皆様にお届けできることは大きな慶びでございます。また、2018 年は SS 研設立 40 周年の記念すべき年でもあり、40 周年を皆様とともにお祝いできたことは至極の喜びであるとともに、これを機会に過去のニュースレター選集にも目を馳せていただき、コンピュータの世界にあって、40 年という時間の重み・移り変わりを改めて感じていただければと思う次第です。この『ニュースレター選集』は、2009 年発刊の第 9 巻からは、会員以外の方にも広くご覧頂けるようになりました。SS 研の活動成果を会員が活用されるのと同様に、会員外へも積極的に情報発信することによって広く社会に役立てるという方針の一環です。これもひとえに、活動に熱心にご参加頂いている会員の皆様および関係者の方々のご理解・ご協力によるものであります。ここに厚く感謝するとともに、この選集が広く活用されることを願って止みません。

2019 年 5 月

シ	ス	テ	ム	技	術	分	科	会		選	出
SS 研 ICT フォーラム 2018 より											

大学における情報セキュリティの取組み
～大学の情報セキュリティポリシー～

曽根 秀昭(東北大学)

大学における情報セキュリティの取組み
～大学の情報セキュリティポリシー～

2018. 8. 31

東北大学　サイバーサイエンスセンター／
国立情報学研究所　高等教育機関における情報セキュリティポリシー推進部会
曽根秀昭

情報セキュリティ対策
(2005)

セキュリティへの脅威

- 種類
  - 不正アクセス攻撃
  - ウィルス，わな
  - 通信妨害（傍受，改変）
- 対策・取組み
  - 防犯，秘密保持，監視
  - 何を何から守るか
  - どのように守るか
  - どのくらいまで守るか
  - 設備整備＋運用＝効果
    - ポリシー，ルール，テキスト

不正アクセス対策

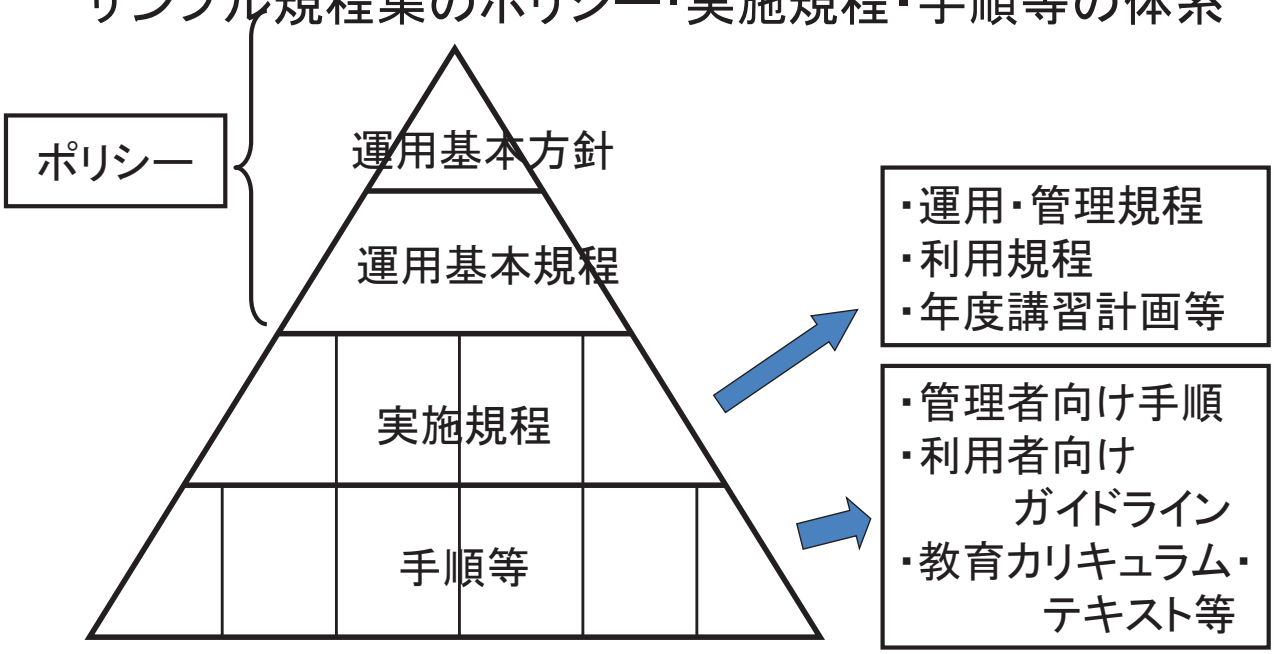
- アクセス制限の強化
  - ファイアウォール
  - パスワードの徹底
- セキュリティ対策
  - セキュリティホール，Update
  - セキュリティ管理
  - 暗号化通信
  - 不正アクセス検知
- 日常管理
  - トラブルの切り分け，対応
- 安全意識と正しい知識
- コンテンツの問題

コンテンツの問題

- 言論の自由の原則
- 他者危害の原則
- 他者の人格の尊重
- 法令，規程，規則の遵守
  - 知的財産権の侵害
    - （発明，考案，意匠，著作）
  - わいせつ罪，など
  - 違法行為の助長，誤認される行為
  - 目的外利用
  - 技術規程の遵守
- →利用の問題，情報安全･倫理の啓発

大学の情報セキュリティポリシー

サンプル規程集のポリシー・実施規程・手順等の体系



- 規程の条文サンプル＋解説
  - 規定している内容が理解しにくい項目や，各大学で修正すべき項目，他の選択や議論の余地があるものについて，策定の参考のために解説

7

大学で扱う情報

【構成員】
•役員， 各種の職員， 教員， 派遣職員， 受託業者， 各種の研究員
•学生 ←構成員なのか・顧客なのか（TA・RAは？）

【活動との関連】
•教育（学生へ）： 教務情報（履修，成績），教材・講義，eラーニング
•研究（学生とともに）： 研究情報（論文原稿，データ，技術・設備），発表論文
•運営： 経営（人事，財務，……），広報，
•（医療）

【情報セキュリティへの要請】
•情報システムの全体のセキュリティ（可用性・機密性・完全性）の維持・向上
•機密情報（入試・試験，未発表論文・特許技術，経営情報）
•社会や関係先へ対する責任
•個人情報保護，安全保障貿易管理（、医事）からの要請との関連
•（コンピュータソフトウェアの適正な管理）
•研究組織・研究者について，学問の自由との両立
•教育機関として，学生に対する情報セキュリティ教育

学内での情報セキュリティ対策を行う根拠規則

- 規則がないと対応したくても根拠がない
- 規則体系
  - 情報システム運用規則
  - 管理に関する規則
    - ◆システム管理、リスク管理、非常時行動計画、情報の格付け
  - 利用に関する規則
    - ◆利用、情報機器、メール利用、情報発信
  - 教育に関する規則
  - 監査に関する規則
  - 事務システムに関する規則

運用と管理に関する規則

- 情報システム運用規程
- 運用全般の根拠
  - 運用の組織： 役職の設定，権限の所在，指示系統
    - 下位規程で管理や利用等の規則を定める
- 情報システム管理規程
  - 管理に携わる者の遵守事項・項目別対策事項
- 情報の格付け
  - 機密性、可用性、完全性の観点から格付け
- 非常時行動計画
  - インシデント発生時の対応（非常時の組織）

11

利用に関する規則

- 情報システム利用規程
  - 情報システムの利用者の遵守事項
    - 利用にあたっての禁止事項、遵守事項
      - アカウント、情報機器の利用、メール、ウェブ、情報発信
- 情報機器取扱要領
  - PCやUSBメモリ等の利用時の遵守事項、注意事項
- メール利用要領
  - メールを利用するときの遵守事項、注意事項
    - HTMLメールの原則禁止、目的外使用の禁止、ToとCc等
- 情報発信要領
  - SNS等を利用するときの遵守事項、注意事項

12

クラウドサービスの導入と セキュリティ関連規則

13

サンプル規程集におけるクラウド対応

政府機関統一基準の対応に準拠

解説の追加

- 管理基準
  - 外部委託に外部設備を利用したサービスが含まれる
  - 外部設備を利用する場合にデータの所在に留意
  - IT部門を通さずにITに相当する外部委託発注を想定
- 技術基準
  - 通信回線の用語定義に仮想ネットワークを想定
  - サーバの共用を想定

- クラウド対応として新たな規則の作成はなし

14

学外へ出せる情報と出せない情報

- 情報の格付けから考える
- 学外に出せる（かもしれない）情報と情報システム
  - 学外からアクセスできる情報やシステム
    - ホームページのコンテンツとサーバ
    - 安否確認システム
    - 図書館システム
- 情報を本学情報システムに置く理由
    - 学外だとどこにあるかわからない不安
    - 学外だと情報にアクセスするまでに経由する機器数が増える
    - （データの保存場所に制約のある）学外との研究に関する情報
    - 機微な情報（人事情報，入試問題，学生の属性）

15

本学情報システムと約款による情報処理サービスの違い

- （サンプル規程集が対象とする）本学情報システム
  - 情報処理及び情報ネットワークに係わるシステム
    （本学情報ネットワークに接続する機器を含む）
    - 本学により、所有または管理されているもの
    - 本学との**契約**あるいは他の協定に従って提供されるもの
- 約款による情報処理サービス
  - 情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができる
  - 情報セキュリティに関する事項に条件選択の制限

16

外部委託における情報セキュリティ対策実施手順

- 必要な情報セキュリティ水準の確保（委託元としての責任者）
  - 可否の判断
    - ◆重要な情報を取り扱う情報処理業務は原則禁止
  - 調達：委託先の選定基準
    - ◆委託する情報処理業務に対する安定性
    - ◆求める情報セキュリティ対策等を遵守
      - ◆その範囲を定め，対策を調達仕様として周知
      - ◆侵害時の対処，履行状況の確認
  - 契約
    - ◆実施させる情報セキュリティ対策の明示＋確認書
  - 実施中
    - ◆取り扱う情報の秘密保持等
    - ◆情報セキュリティ対策の履行状況の確認
  - 納品・検収

17

「約款による情報処理サービス」の利用に際しての注意事項

- 処理された結果生じる著作権等の権利の放棄や移管が利用条件となっている場合
- 約款上データ消去等をサービス利用者側で直接実施できない場合
- 利用したデータの削除についてサービス 提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われる場合
- 留意事項（運用・管理）と，確認事項（C, I, A）
- 無償で利用を開始できる場合であっても、外部委託に該当する場合がある
  - 無償のメールサービス，アンケートサイト，オンラインストレージ

18

ソーシャルメディアによる情報発信

ソーシャルメディアの公式利用

- 公式広報，情報発信、研究成果公開，社会連携の効果
  - 迅速な情報発信 （ただし利用者限定もある）
  - 詳細なウェブサイトや紙媒体への補完としての併用
- 公式広報と，それ以外の情報発信の区別
  - 公式プレスリリースと，「中の人」（個人的意見を含む）
- 公式の広報・情報発信の注意点
  - ネットワークサービスのユーザとしての利用
  - 文書など従来の広報との使い分け（あるいは置き換え）
  - 組織としてのアカウント運用ポリシーの表明（公式，返信）
  - 情報の貧富，情報弱者への配慮

情報拡散の特性への配慮(1・2/4)
話題の選び方・閲覧者の想定

- 意図しないコミュニケーションが生じるおそれ。
- 話題の選び方、表現に注意する。
  - 公開メディアでは多くの人に見られることを意識
- 悪気のない投稿内容が他人を不快にしてしまう場合がある。
  - さまざまな地域、立場、文化的背景、価値観の読者
  - 他人への中傷をしない・誹謗にも注意

- 多様な閲覧者を想定して投稿する。
- 公開になる投稿は、想定外の閲覧者の目にも触れる。
  - 内輪のつもりの投稿も、公開・再掲載の可能
  - 想定外の他人に閲覧され，誤解・批判される可能性

21

情報拡散の特性への配慮（3・4/4)
匿名性は不確実・投稿の削除が困難

- 匿名にしていても、個人がわかることがある。
  - 後から閲覧者・投稿者がわかる可能性
    - 他の投稿やプロフィールを分析して特定
  - 実名・所属・住所などが暴露される可能性
- 個人を特定される可能性を想定しておく。
  - 実名がわかっても困らないように注意して行動
  - 想定外で実名が公開になることも想定

- 不用意な投稿を後で削除しても、ネット上から消えないことがある。
  - 連携サービスへの転送先では消えない可能性
  - 再掲載、アーカイブ、まとめに蓄積・保存されている可能性
- 将来まで責任をもてるかを考えて発言する。

22

情報発信・交流における留意点

- 相手を尊重し、不快にさせない
  - 過度な言い争い、反対意見主張、感情的発言
  - 友達以外への「友達申請」で当惑？
- 著作権・商標権
  - 著作物・商標の引用・転載に、許諾が必要
- 写真撮影時の肖像権
  - 撮影場所・対象について許可を得て撮影し掲載

23

トラブル発生時の対応

- 掲載内容による炎上（コンテンツインシデント）:
  - 想定外の批判、苦情、誹謗中傷の集中
  - 掲載内容が違法／不快／非常識； それぞれの対応
  - 公式／私的： それぞれの対応
    - 私的トラブルの場合に、所属先としての責任は？
    - 普段から安全とマナーの注意喚起は必要
- 公的アカウントの成りすまし（不正アクセス）
  - アカウント（パスワード）再設定
  - 掲載内容の一時閉鎖など

24

シ	ス	テ	ム	技	術	分	科	会		選	出
SS 研 ICT フォーラム 2018 より											

効率的かつ効果的な CSIRT 運営へ

松本 多恵(島根大学)

効率的かつ効果的なCSIRT運営へ

管理者,利用者ともに負担軽減を目指したCSIRT運営の可能性について

島根大学CSIRTメンバー
松本多恵

2018年8月31日

講習内容

1. 差止めなく進化していくサイバー攻撃
2. CSIRTの役割
3. CSIRTの課題（人間の弱点を狙う脅威）
4. CSIRTの課題（人材不足）
5. CSIRTの課題（予算面）
6. どうすれば利用者の利便性とセキュリティを担保できるのか
7. 情報セキュリティ教育
8. まとめ

2

差止めなく進化していくサイバー攻撃

昨日まで安全だったものが今日は危ない！

サイバーセキュリティ上の脅威の巧妙化・高度化

愉快犯
自己顕示,見せしめ,嫌がらせなどが目的

目立つ攻撃
すぐに攻撃に気づき,対策を講じることができる

攻撃手法の巧妙化

目立たない攻撃
攻撃の発覚が遅れるため,被害の拡大長期化

2000年

2000年1月24日科学技術庁（現・文部科学省）のホームページが不正に書換,総務省統計局のホームページで公開中の国勢調査などのデータが消去

不正アクセス禁止法施行（2000年2月13日）

2005年

2004年頃から個人情報やクレジットカード情報を狙ったサイバー攻撃
2005年データに不正アクセスを行い,個人情報を盗み出す

2008年コンフィッカーと呼ばれるUSBメモリ経由で観戦するコンピュータウイルス流行

2010年以降

2013年Webサイトの改ざん総件数7,726, 2014年3,664件,2015年3,335件,2016年3,274件と徐々に減少

サイバーセキュリティ基本法（2014年10月21日）

2017年5月世界で猛威を振るった「Wanna Cryptor」と呼ばれる身代金要求ランサムウェア

2017年
- ビジネスメール詐欺
- 仮想通貨の流出
- DDoS攻撃

4

情報セキュリティ対策とは

何を守るのか

何から守るのか

どのように守るのか

情報資産

情報セキュリティの脅威

外部脅威
内部脅威

技術的な対策
ウイルス対策ソフト
ファイアウォール

物理的な対策
バイトメトリクス認証
入退管理
災害対策

人的な対策
従業員、構成員の情報セキュリティ教育
CSIRTメンバーの教育

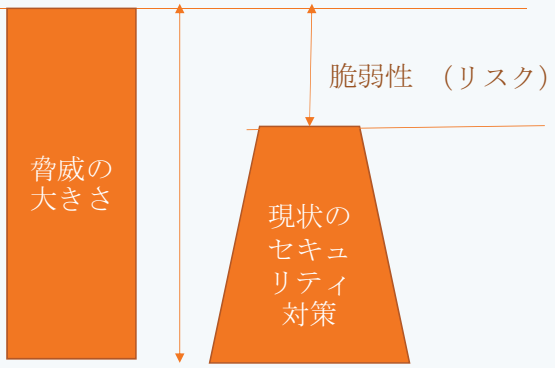
組織的な対策
情報セキュリティポリシーの策定
個人情報保護法
CSIRT等の構築

リスクの管理

脅威とは
システムまた組織に危害を与える,好ましくない偶発的事故の顕在的な原因

脅威基準値（脅威が発生すると）
（小）大きな問題にならないが，
今後の対策が重要になる可能性がある
（中）問題になる
（大）深刻な問題となる

脅威の種類	脅威の例
人（偶発的）	メール誤送信、ファイルの削除、書類の紛失，パソコンスマートフォンの破損，意図しないウイルス感染
人（意図的）	データ改ざん、ID等の不正取得　なりすまし
環境的	地震、津波、火災等の自然災害、サーバ等の経年劣化による不備　アップデート等の不備



脆弱性の基準値
（低）現状は，脅威に対しての対策が万全
（中）現状は，対策に改善の余地あり,安全性が中位
（高）大きなセキュリティ上の欠陥が存在し，安全性
が欠如する状況で早急な対策が必須

情報セキュリティ事故（個人情報漏えいなど）が組織に与える影響

個人情報，機密情報,知的財産，営業秘密,社内文書，社内システム情報,顧客情報，個人情報など重要な情報資産が脅かされる事故が多発

金銭的な被害

ブランドの失墜

責任者の進退問題

サービス・業務の停止

サイバーセキュリティ対策は,経営上の課題へ

① 技術の問題 ⇒ 組織の問題へ
② IT部門の課題 ⇒ 組織全体の課題へ

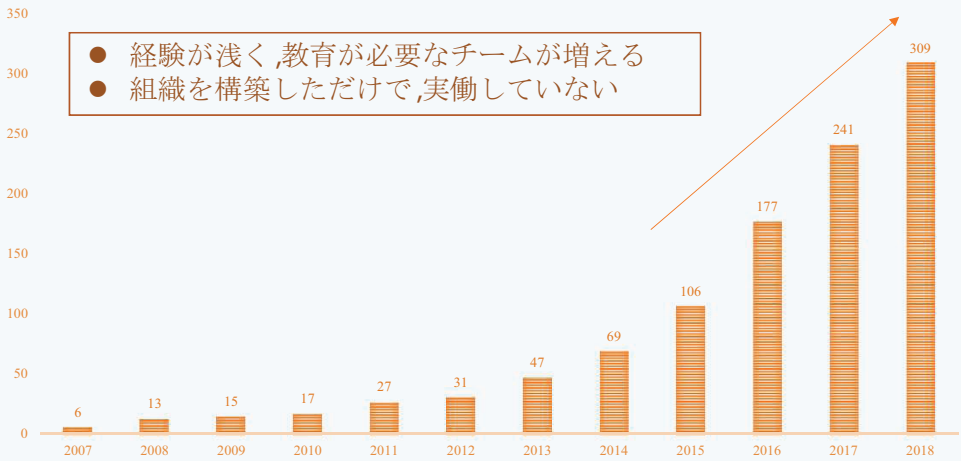
➡ CSIRTの設置

7

多くの組織が,サイバー攻撃,改ざん,窃取,破壊,強奪などの行為他のあらゆる干渉の被害を受けたホストやネットワークを迅速に対応し,被害を最小限に抑え,速やかに復旧させる「Computer Security Incident Response Team（CSIRT）」チームを整備

CSIRT構築ブーム

日本シーサート協議会加盟数の推移



出典：CSIRT構築から運用　著日本シーサート協議会をもとに作成
※241組織(2017年8月25日総会開催時点)
309組織（2018年8月6日現在　日本シーサート協議HPの会加盟数から引用）

8

CSIRTの役割

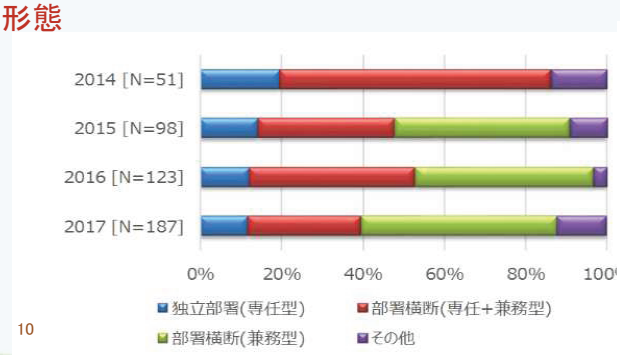
CSIRTの運営形態

CSIRTが完全に独立した部署として運用されているケースは少ない

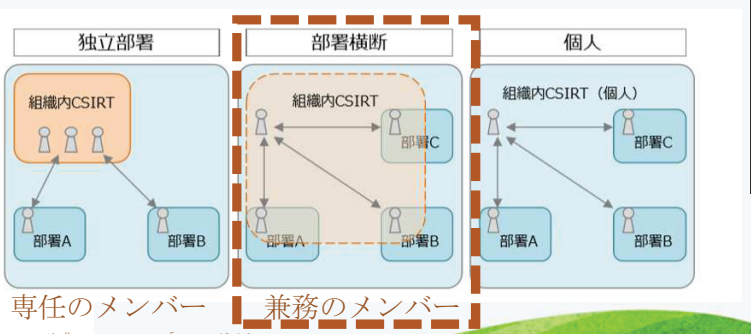
関連する部署にまたがった兼務のメンバーによって構成される

「仮想チーム」の形態をとるケースが多い

実装の形態



出典：日本シーサート協議会加盟組織一覧2017年版



出典：JPCERT/CC「CSIRTガイド」 http://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf

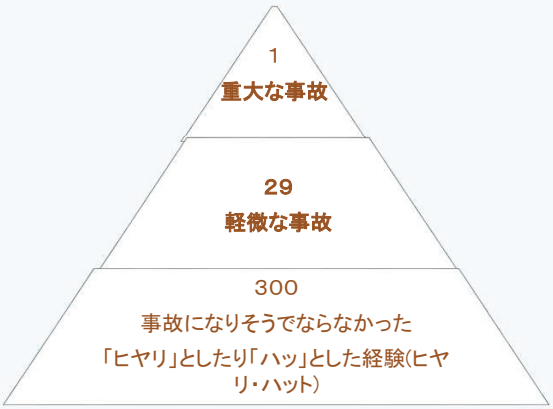
CSIRTの役割

組織内 CSIRT の基本的な役割

組織において発生したインシデントに対応する

（質問）
サンプル規定集での定義でインシデントの恐れがあるセキュリティイベントも含めて「インシデント」と定義されている一方で,上層部や構成員は「インシデント」というと重要な事態と捉えてしまい,説明に苦慮するのですが,どの様に理解を得るのがよいでしょうか

ハインリッヒの法則



11

効率的なインシデント対応のために

（質問）
インシデント対応に必要な情報はどのように収集しているか（すべきか）？また,日常的な活動の中で収集している（するべき）ならば,どのような方法がよいか

発生事象が「サイバー攻撃なのか、一時的な不具合なのか」などを的確に推測・判断する力が必要

- その時流行っているサイバー攻撃から推察する
- 組織内の脆弱性に関して事前に把握・整理する
- 攻撃者の目的を理解する
- 攻撃者に突破される可能性がある
- 対策を施す際, どのようにすれば侵入できるかの検討する（侵入されても大きな被害を出さない）

12

CSIRTの課題（人間の弱点を狙う脅威）

人的ミス事故を防止するには

ヒューマンエラーをはじめとした内部の人間に起因するセキュリティトラブル

ミスが起こる５つの原因
(1) 技能の問題
(2) 性格の問題
(3) 生理的な問題
(4) 感情の起伏の問題
(5) 環境の問題

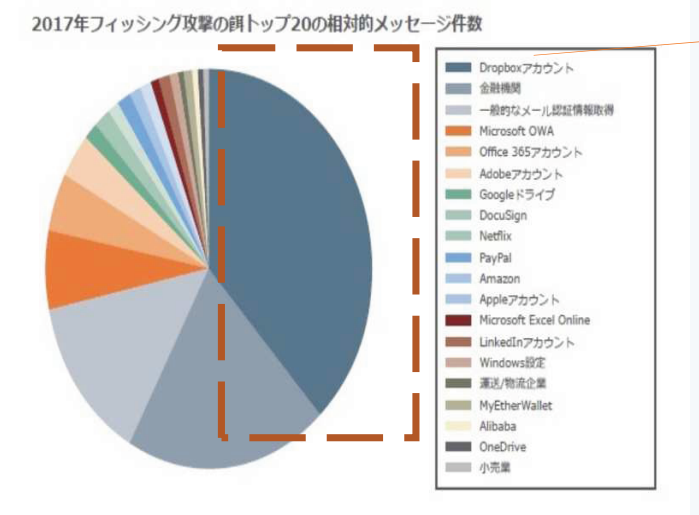
紛失・置き忘れ	盗難	メールの誤操作
誤操作によるデータ削除	内部犯罪・内部不正	規則違反

	漏えい原因比率				
	2013年	2014年	2015年	2016年	2017年
誤操作	34.90%	30.90%	25.80%	15.60%	25.10%
紛失・置忘れ	14.30%	12.60%	30.40%	13.00%	21.10%
不正アクセス	4.70%	2.40%	8.00%	14.50%	17.40%
管理ミス	32.30%	43.70%	18.80%	34.00%	13.00%
不正な情報の持ち出し	1.50%	2.80%	4.80%	6.80%	6.50%
盗難	5.50%	3.00%	5.50%	5.30%	6.50%
設定ミス	3.10%	2.10%	1.90%	4.70%	4.70%
内部犯行	1.00%	1.30%	2.10%	0.90%	2.10%
バグ・セキュリティホール	0.50%	0.30%	1.50%	1.70%	1.30%
ワーム　ウイルス	0.40%	0.30%	1.30%	1.10%	0.50%
その他	0.60%	0.40%	0.10%	1.90%	0.80%
不明	0.40%	0.20%	0.40%	ー	0.50%
目的外使用	0.70%	0.10%	0.30%	0.40%	ー

出典：特定非営利活動法人 日本ネットワークセキュリティ協会「情報セキュリティインシデントに関する調査報告書」から作成

14

フィッシング攻撃



出典：米Proofpoint「Human Factor 2018 Report」

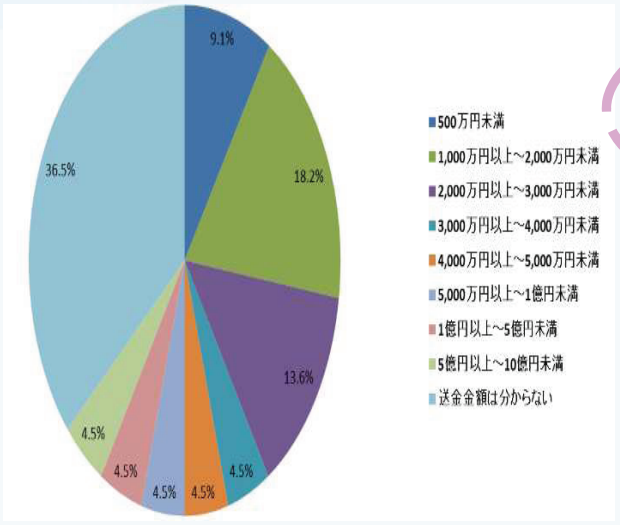
ファイル共有サービス「Dropbox」が増加

- クリック率が高いのは電子署名「DocuSing]を発信元と称するフィッシングの方がクリックされやすい
- メールが届いてかリックする時間
  1分以内11％
  5分以内4分の 1

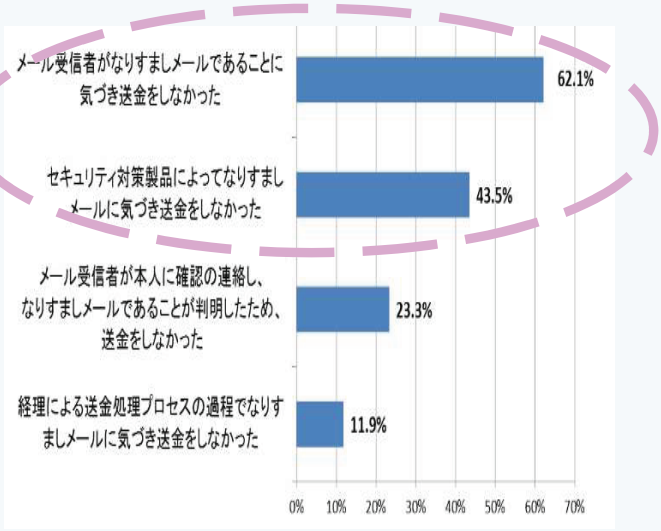
ソーシャリエンジニアリング
- 緊急性
- 信用あるブランドになりすます
- ビジネスメール詐欺（BEC）
- フェイチェーンを利用するメール詐欺
  「Re:」「Fwd:」

15

ビジネスメール詐欺



送金依頼メールに起因した送金金額内訳（N=22：単一回答）



送金を未然に防ぐことができた理由内訳（N=253：複数回答）

16

出典：トレンドマイクロビジネスメール詐欺に関する実態調査2018

CSIRTの課題（人材不足）

業務時間の定義（長期的な人材確保のために）

サービスの提供

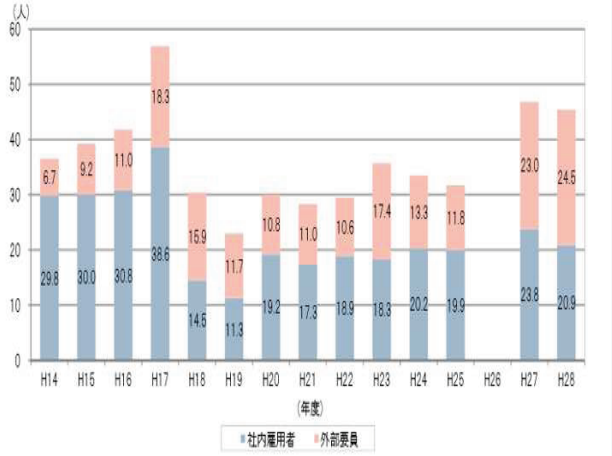
- 24時間,年中無休体制
- 交代制
- 業務時間内のみの対応
- 業務時間外の対応

◆ 連絡体制の構築
◆ 事象により連絡体制の変化

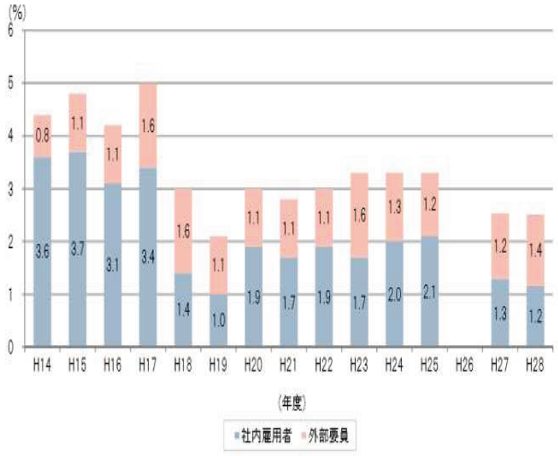
18

IT人材

一社平均 IT 要員数



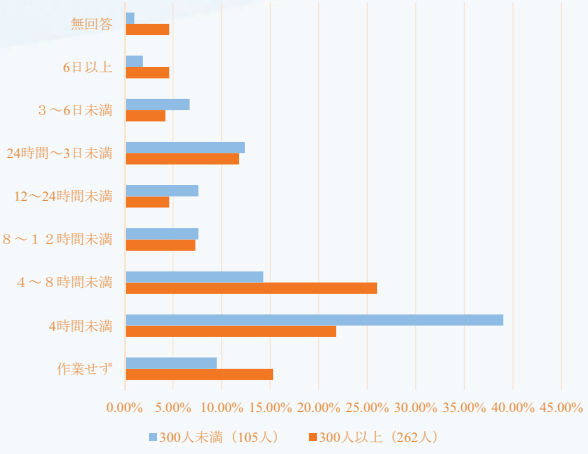
対総従業員数比



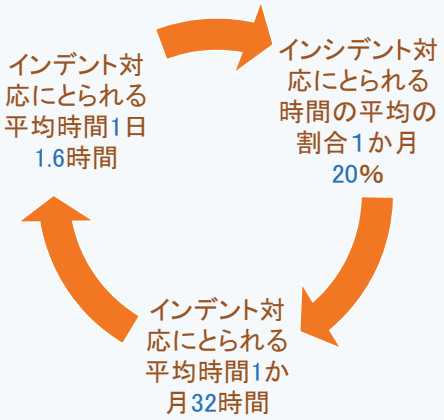
19

出典：経済産業省「情報処理実態調査」(2018)

ウイルス感染からの復旧作業延べ人日



出典：2014年度「情報セキュリティ事象被害状況調査　報告書」(IPA)から作成



出典：セキュリティ教育の実態調査エムオーテックス

20

CSIRTの課題（予算面）

CSIRTを運営する上での課題

最大の課題 「予算」

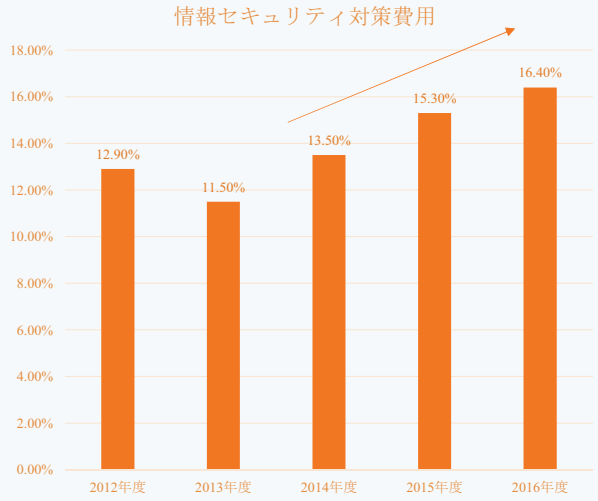
ROI（Return On Investment　投資利益率）＝1,425%

マルウェア攻撃への投資

ランサムウェア攻撃を仕掛ける場合に必要な準備や運用コストと,攻撃から得られる金額から算出された値

22

情報セキュリティ対策費用



出典：ITR「IT投資動向調査2017」

一社平均情報セキュリティ対策費用の推移

【中小企業】 (%)

	50万円未満	50～100万円	100～150万円	150～200万円	200～400万円	400～1,000万円	1,000万円以上	わからない	発生しなかった
平成22年	30.5	17.6	6.4	4.6	5.2	4.0	2.4	17.3	12.0
平成23年	30.2	16.1	6.8	4.7	5.9	3.6	1.7	18.4	12.6
平成24年	31.7	14.6	6.3	3.9	4.8	3.8	2.1	19.9	12.9
平成25年	35.2	16.9	6.0	3.1	4.9	4.0	2.0	18.0	9.8

【大企業】 (%)

	50万円未満	50～100万円	100～150万円	150～200万円	200～400万円	400～1,000万円	1,000万円以上	わからない	発生しなかった
平成22年	11.0	9.5	6.5	4.3	9.1	12.0	20.2	22.7	4.8
平成23年	10.2	10.0	5.5	5.2	10.2	11.9	18.5	23.4	5.0
平成24年	11.2	8.9	6.6	4.1	7.9	11.1	17.7	28.2	4.2
平成25年	12.7	9.1	5.3	5.1	8.5	12.1	19.5	23.5	3.8

出典　経済産業省「情報処理実態調査」

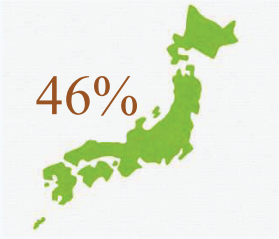
23

日本の企業は経済犯罪に関する事後対応費用が高額

直接的な被害額よりも事後対応費用の方が高いと答えた企業

世界全体

<



日本

不正が長期化

被害が全社的

出典：経済犯罪実態調査 2018 日本分析版をもとに作成

直接損失額＝逸失利益＋復旧に要するコスト＋事故対応に要するコスト＝（年間想定売上高÷365×業務停止日数）＋（復旧対応をおこなう人数×原価×復旧にかかる日数＋ハードウェア・ソフトウェア費用）＋（事故対応をおこなう人数×　原価　×　事故対応にかける日数）

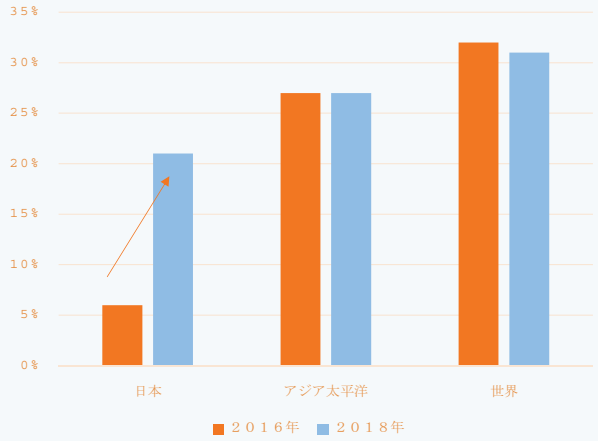
間接損失額　＝　補償・補填費用　＋　損害賠償費用　＋謝罪広告費用

ALE（年間損失予想額：Annualized Loss Exposure の頭文字）＝脅威の年間予想発生頻度×発生1回あたりの損失額

24

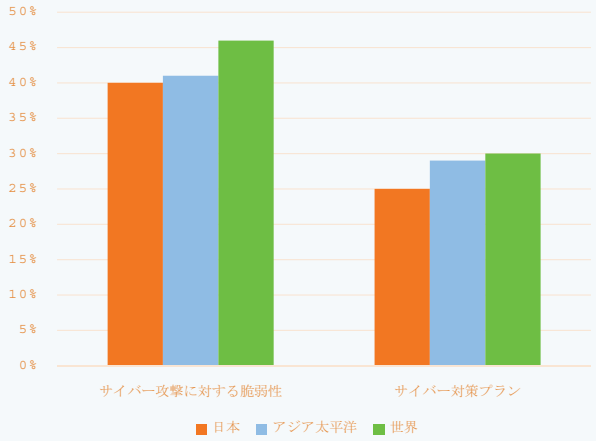
なぜ日本の企業は経済犯罪に関する事後対応費用が高額になるのか

過去2年間で被害にあったサイバー犯罪



出典：経済犯罪実態調査 2018 日本分析版をもとに作成

過去2 年間で実施したりクスアセスメント



出典：経済犯罪実態調査 2018 日本分析版をもとに作成

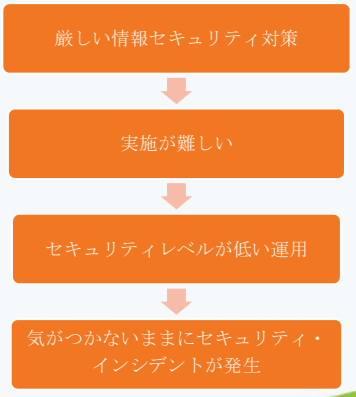
25

どうすれば利用者の利便性とセキュリティを担保できるのか

面倒な情報セキュリティ対策

情報セキュリティを万全にすればするほど,業務に支障や利用者の同意を得るのが難しい

（質問）
利用者として,手順が煩雑で不満を感じて「これで本当にセキュアになるのか？」という疑問を感じることがあると思うが,その場合に,どうやって利用者側の納得感を得るのか。工夫があれば教えて欲しい



聞き取り調査(電話,対面を含む)

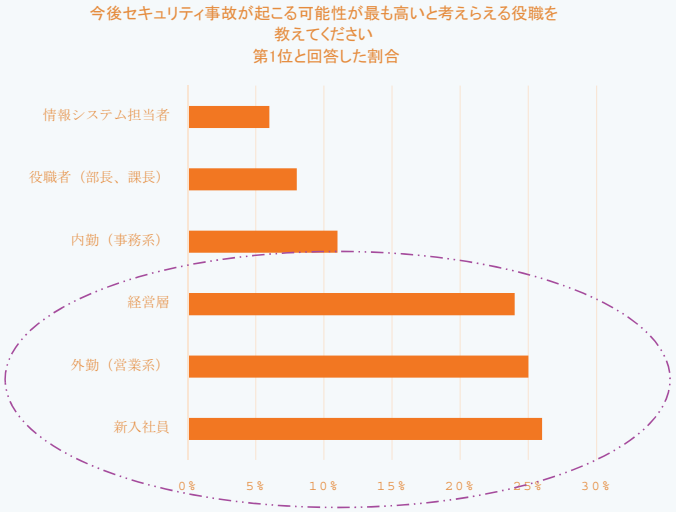
対象者:私立,公立,国立の教員に対して聞き取り調査期間　:2017年6月～8月
年齢　:30歳代～60歳代(男女)

質問項目
①貴大学における情報セキュリティ対策や運営に関して不満や良い点など

- 利用者の利便性とセキュリティはトレードオフだとわかるが,利用しずらい面がある
- 利用者はもちろん利便性がある方がいいが,安全面も協力したいと考えている
- 大学によって運営が異なりので,異動時は戸惑いを感じた
- セキュリティのe-learningに効果があるのか疑問である
- 注意喚起を個別に対応してほしい
- セキュリティが非常に面倒だと感じている

28

組織内の意識改革



出典：セキュリティ教育の実態調査エムオーテックスから作成

①情報セキュリティの基本をルール化して守る
②潜在的な事件や事故が顕在化したときに,人的なミスや事件・事故の誘引物や条件を取り除く（悪いことができない仕組みを作る）
③情報セキュリティに対する自覚の教育や専門教育を行う

懲罰性

個人情報の不適切な取扱いに係る懲戒処分等の状況一覧（教育職員）

（単位：人）

	平成23年度	平成24年度	平成25年度	平成26年度	平成27年度	平成28年度
免職	0	0	0	0	0	0
停職	1	1	0	1	2	0
減給	10	10	9	7	10	6
戒告	28	30	22	23	24	17

出典：「公立学校教職員の人事行政状況調査について」（文部科学省）をもとに作成

ルール強化（一例）

２０１３年４月２日から４月５日にかけて不正アクセスの被害にあったeBookJapan

ログイン成立分

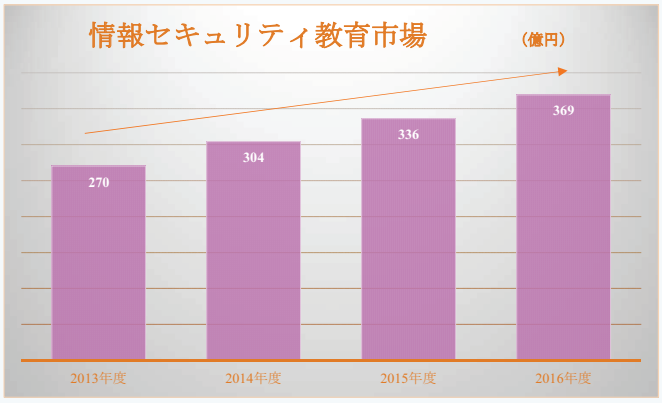
IDあたりPW試行回数	該当ID数
1	386
2	347
3	37
4	4
5	5

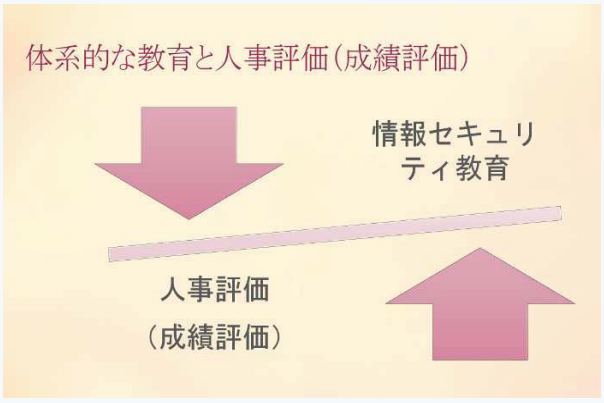
ログイン失敗分

IDあたりPW試行回数	該当ID数
1	1327
2	72
3	20
4	7
5	3
6	1
9	1

出典：eBookJapan 不正ログインに関する最終報告より

情報セキュリティ教育の導入

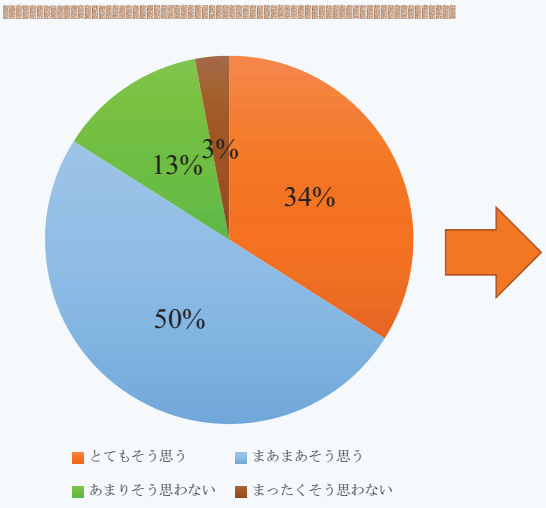




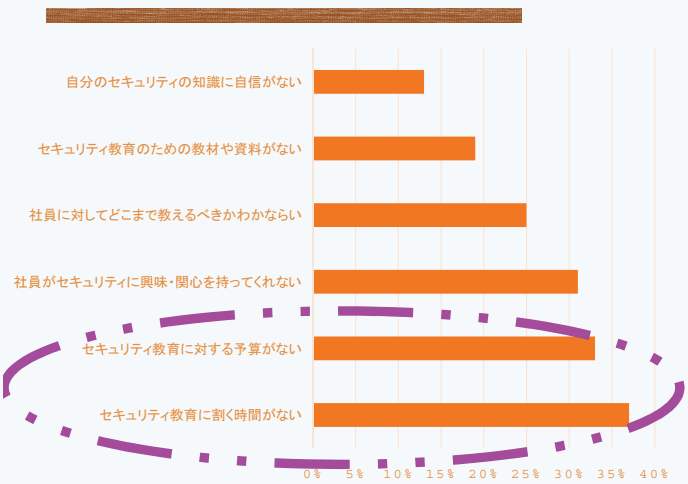
出典　2015年度 情報セキュリティ市場調査報告書

33

情報セキュリティ教育の問題点



出典：セキュリティ教育の実態調査（エムオーテックス）



出典：セキュリティ教育の実態調査（エムオーテックス）

34

情報セキュリティ教育（e-learning）

E-learningを活用した情報セキュリティ教育の問題点

- 毎年受講させないといけないのか
- 個々の情報リテラシーレベルに対応した内容のコンテンツが少ない
- テストで内容を確認する仕組みが多いが,本当に理解しているのか
- 情報セキュリティ教育の内容はあまり代り映えがしない
- 人事評価と連動する必要があるのか

作成側

- 毎年内容を見直しする必要がある

35

効率的かつ効果的なCSIRT運営には

効率的なインシデント対応を実施するには
- CSIRT運用の経験値を高める
- 予算の確保（中長期的）
- セキュリティ管理者の技術向上
- アウトソーシングの活用
- 長期的な人材確保
- 構成員のリテラシー向上（興味深い内容のもの）

シ	ス	テ	ム	技	術	分	科	会		選	出
システム技術分科会 2018 年度会合 より											

NII-SOCS の運用から浮上してきた セキュリティ対策の課題 ～高度化するサイバー攻撃にどう向き合うか～

高倉 弘喜(国立情報額研究所)

NII-SOCSの運用から浮上してきた セキュリティ対策の課題 ～高度化するサイバー攻撃にどう向き合うか～

高倉弘喜
国立情報学研究所

NII-Security Operation Collaboration Services(NII-SOCS)の経緯

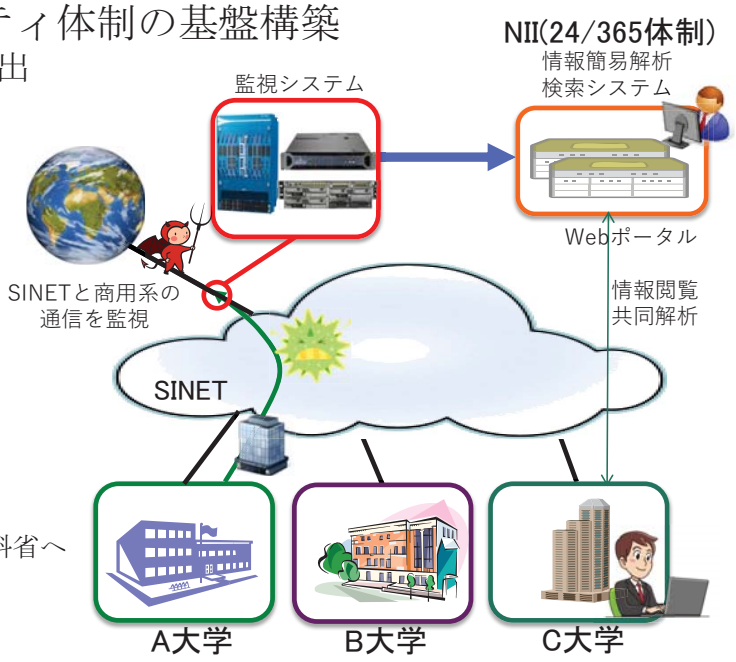
■サイバーセキュリティ基本法

- **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。
- **第三十二条**　本部は、その所掌事務を遂行するため必要があると認めるときは…国立大学法人の学長、大学共同利用機関法人の機構長…に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。

…と言われても…

NII-SOCSの構築と運用

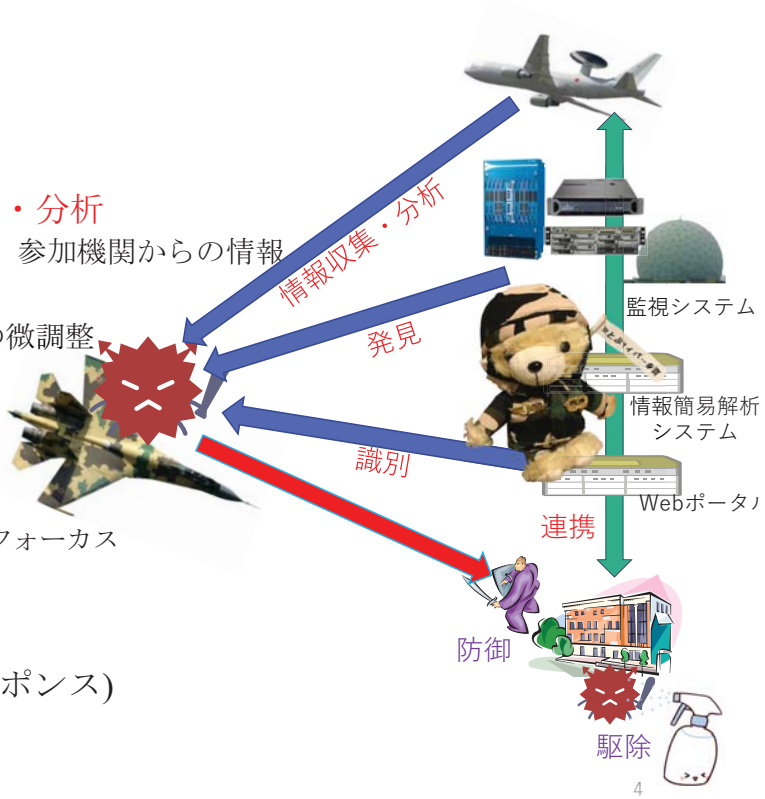
■ 大学間連携に基づく情報セキュリティ体制の基盤構築
- 国立大学法人等の運営費交付金から拠出
  - 7.8億(2016)、8億(2017)、8億(2018)
    - 2021までは継続の予定
- 3種類の監視システム
  - Sandbox搭載IDS (paloalto)
  - シグネチャベースIDS (Cisco FirePower)
  - DNSトラフィック監視 (Damballa CSP)
- 簡易解析システム＋Webポータル
  - 膨大な警報に緊急度・危険度の割付
- 外部セキュリティ機関との情報共有
  - 国内：NDAに基づく攻撃情報の提供
    - サイバー攻撃拠点のNIIへの事前通知
    - NIIは通信の有無のみを回答
      - セキュリティ機関：NISC経由で文科省へ
      - NII：大学に直接通知
  - 海外：MoUに基づく技術情報の共有



NII-SOCSの作業の流れ

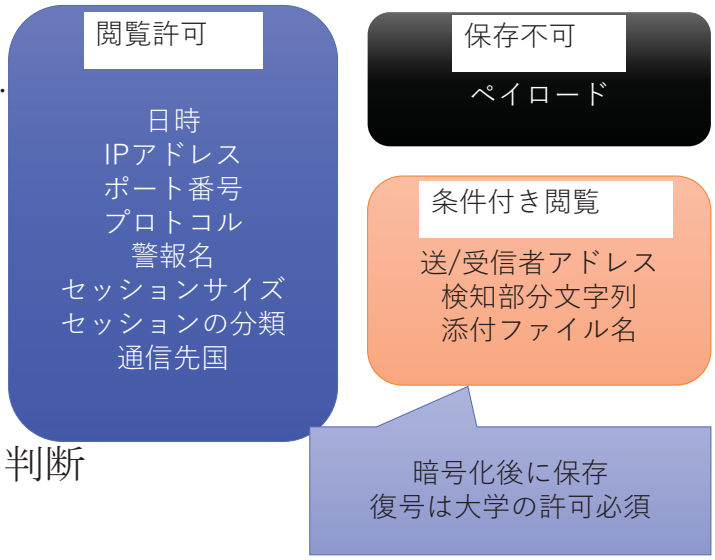
■ サイバー攻撃への初動対応
- 早期警戒情報(インディケータ)の収集・分析
  - 国内・国外のセキュリティ機関、民間、参加機関からの情報
- サイバー攻撃の発見
  - IDS、サンドボックス、ハニーポットの微調整
- サイバー攻撃の目標と脅威度の識別
  - 各種情報との照合
  - 攻撃先の分布状況や攻撃手法の解析
  - 被害推定
    - Zero Day攻撃など被害が大きいものにフォーカス
- 参加機関と連携

■ 参加機関
- 現場対応(予防措置/インシデントレスポンス)
  - 防御や駆除



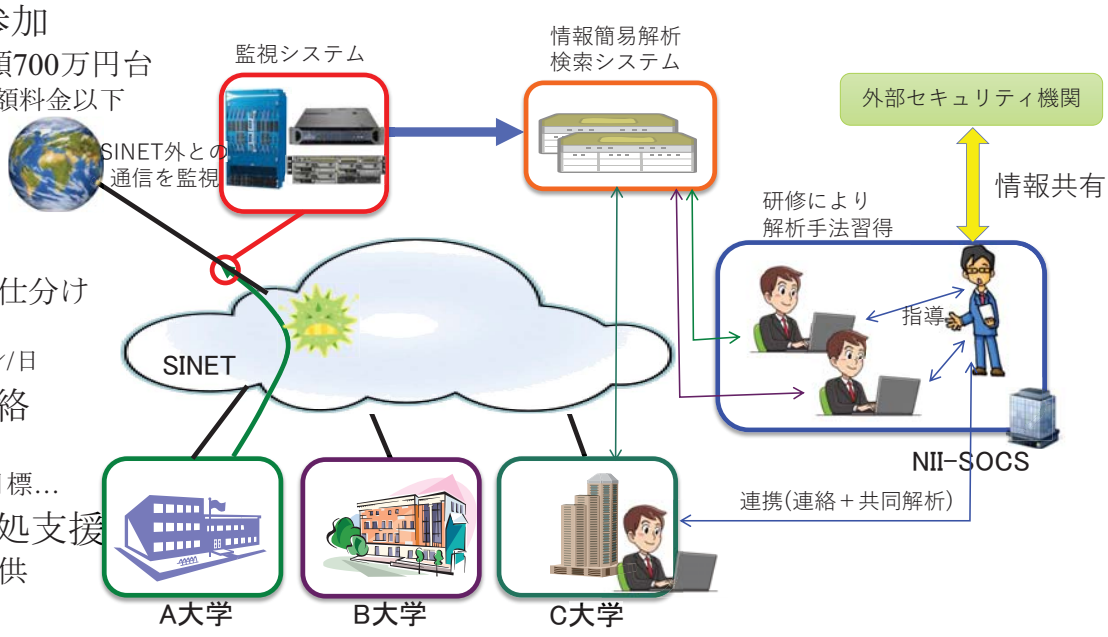
NII-SOCSの制限

- NIIは大学共同利用機関法人…国に準ずる独法
- 大学の構成員
  - 教職員…国立大学なら公務員に準ずる…
  - 学生・訪問研究者
  - 研究を覗き見るのは…
  - そもそも個人所有の情報端末
- 憲法遵守はmust
  - 通信の秘密
    - 通信の中身は覗けない
  - 財産権
    - 無断の脆弱性診断・コマンド実行不可
- 通信の内容を確認せずに攻撃成否を判断
  - 攻撃着弾後の挙動から推測
    - 誤判定の要因の一つ

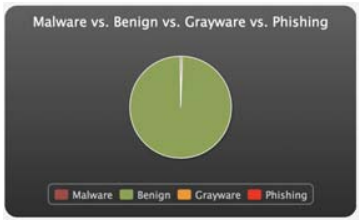


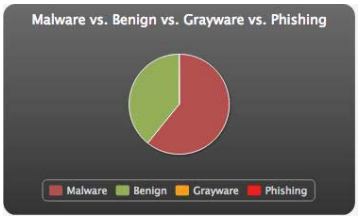
NII-SOCSの仕組み

- 100機関以上の参加
  - 1機関あたり年額700万円台
    - 大手SOCの月額料金以下
- 警報監視
  - 24/365体制
    - 平日日中4人
    - 夜間休日2名
  - 簡易解析結果の仕分け
    - 60万警報/日
    - 6億セッション/日
- インシデント連絡
  - 大学へ連絡
    - 週1件程度を目標…
- アクシデント対処支援
  - 必要な情報の提供



NII-SOCSの運用実績





- ■いかに絞り込むか?
  - ●膨大なデータ
    - ◆60万警報/日
    - ◆6億セッション/日
- ■概ね30分以内の通知
- ■9割を占める
  - ●マルウェア系
    - ◆半自動処理
- ■残り1割
  - ●絞り込み
  - ●目視による監視

中項目		累計 (2018/4/1~9月末)
通知件数		3617
	分類１：マルウェア感染の可能性	2760
	分類２：アプリケーションソフトの脆弱性によるもの	225
	分類３：C&Cサーバーとの実通信の可能性	480
	分類４：ブルートフォース攻撃の可能性	0
	分類５：辞書攻撃の可能性	0
	分類６：標的型サーバー攻撃に関与している可能性	0
	分類７：man-in-the-middle 攻撃	0
	分類８：DNS Amp 攻撃への参加	0
	分類９：その他	152
誤報件数		2

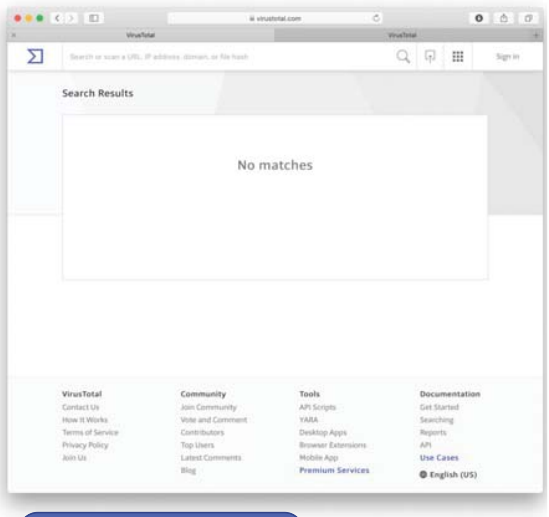
挙動の違いによる被害推定

- ■追加ダウンロードの可能性あり
  - ●関係機関へ通知

Date	Src IP	Dst IP	Src Port	Dst Port	Protocol	Sent(byte)	Rec. (byte)	Src Country	Dst Country
2018/5/○ 09:19:28	A.B.C.D	W.X.Y.Z	49940	80	tcp	2283	353460	Japan	Russian Federation
2018/5/○ 18:26:14	E.F.G.H	W.X.Y.Z	64464	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 19:07:37	E.F.G.H	W.X.Y.Z	50368	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 16:53:14	E.F.G.H	W.X.Y.Z	58072	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 17:45:15	E.F.G.H	W.X.Y.Z	61838	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 18:15:39	E.F.G.H	W.X.Y.Z	64279	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 19:59:12	E.F.G.H	W.X.Y.Z	53316	80	tcp	1154	23532	Japan	Russian Federation
2018/5/○ 16:41:48	E.F.G.H	W.X.Y.Z	57399	80	tcp	307	14466	Japan	Russian Federation
2018/5/○ 18:04:36	I.J.K.L	W.X.Y.Z	63829	80	tcp	307	14466	Japan	Russian Federation
2018/5/○ 19:37:44	I.J.K.L	W.X.Y.Z	52110	80	tcp	307	14466	Japan	Russian Federation

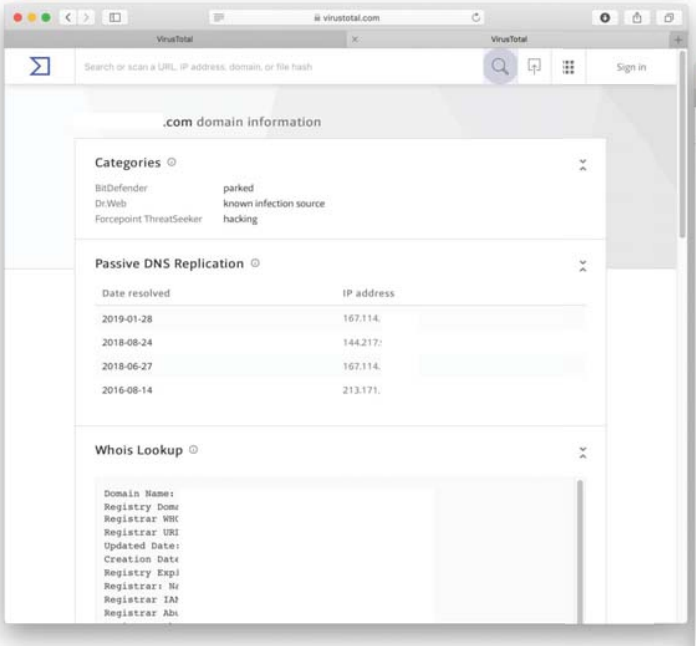
NII-SOCSの運用方針

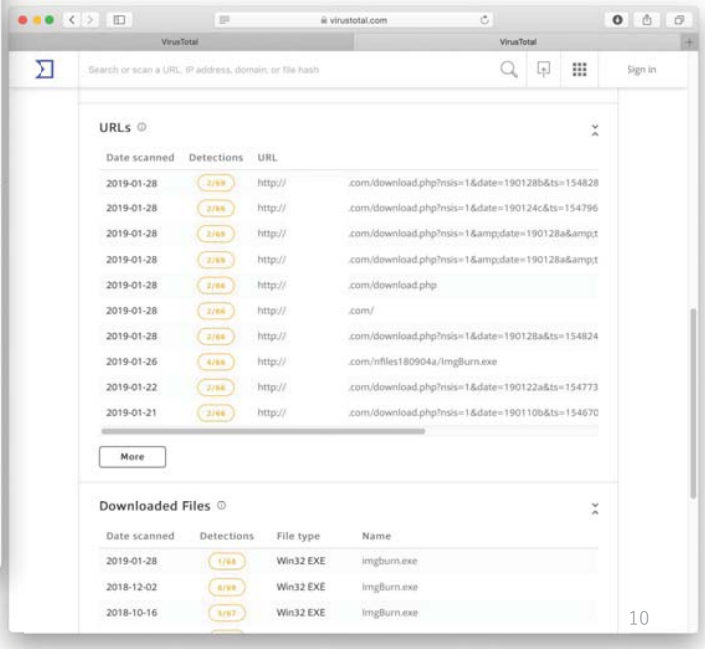
- 最近の攻撃のみ監視
  - 古い脆弱性を狙った攻撃
    - 情報収集目的での検知
      - 古い攻撃の大量発生→未知攻撃の可能性
- マルウェア
  - Sandboxによる検知
    - 通知は大手セキュリティソフト未検知のもののみ
      - 伝えられるのはハッシュ値のみ
      - 来年度からはマルウェア検体の提供も開始するが…
        - 懸念されるVirusTotalへの脊髄反射upload
- よくある誤対応
  - セキュリティソフトで検知されませんでした
    - それは当然
  - なので被害なしと判断します
    - それは大丈夫か？



一定期間経過観察
異常検知→再通知

配布元ドメインを調べれば疑わしいのは一目で分かるのに…





標的型攻撃への事例

- NII-SOCSで数名にのみ着弾確認
  - 月に数度は観測
- 採取時は未知マルウェア
  - 検知AV 0は当たり前
    - そもそもサンプルとして上がっていない
- 半日程度で検知が始まるが…
  - サンプルファイルを提供したのは誰か？
    - サンプルがなければ検知パターンが作れない
- 遅々として向上しない検知カバー率
  - 1件のみのサンプル提供
  - 各社サンドボックスからのアクセス回避
    - 緊急度と悪性度の判断しにくい

IT依存度が急速に高まる大学

- 見えない攻撃にどう対処するのか？
  - 重要なのはインシデント対応、それとも、事業継続？
- CIAからAICへ
  - 大学の事業が継続できること(Availability)
    - そもそもインシデントによるシステム停止と故障によるシステム停止の違いは？
    - 重要システムの故障でも事業継続… ダメージコントロール
  - 情報が得られることも重要(Integrity)
    - 異常データを吐く機器が特定可能
      - ➢ データ破棄 or 参考値として使える デグレーテッドオペレーションの可能性
        - NWは生きていることが分かる…も情報
  - 個々の機器のconfidentialityはそこそこでよい

レジリエントな情報システムの設計

CIAのために事前に立案する要領・手順

- 情報システム単体ではなく業務単位で事前に考えておく
  - アクシデントに至った状況下での適切な判断は困難
    - エリートパニックによる思考停止→全面遮断
- ダメージコントロールを想定した業務体制
  - ある温度センサーでマルウェア感染
  - コントローラでマルウェア感染
  - 認証システムへの不正アクセス

リスクレベルに応じた対応

- デグレーデッドオペレーション(縮退運転)を検討
  - 止められない
  - 止めたくない
  - 止めるしかない

停止による影響を考慮

止められない情報システム

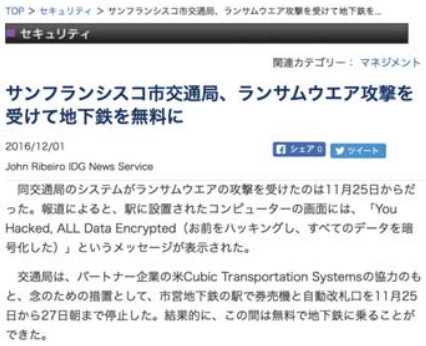
- 運用停止による影響が甚大
  - 人命に関わるもの(医療機器、危険物の管理)
    - 手動操作が困難
- ダメージコントロール
  - 運用継続による被害拡大防止
    - 防衛ラインの設定(Standalone運用は可能か)
- デグレーデッドオペレーション
  - サイバー攻撃による異常動作も想定
    - 担当者が張り付いてでも運用
    - 後で巻き戻し作業が入っても業務継続
    - 緊急停止機能の確認
    - 代替手段の確保

判断基準・手順のマニュアル化

止めたくない情報システム

- 運用停止による影響大
  - 顧客サービス
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 情報システム停止も想定
    - 手動による業務継続
      - 手書き出席票
    - 情報取得を諦めるのもアリ
      - 無料開放

利用者の不利益回避


TOP > セキュリティ > サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を...

セキュリティ

関連カテゴリー：マネジメント

サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を無料に

2016/12/01

John Ribeiro IDG News Service

同交通局のシステムがランサムウエアの攻撃を受けたのは11月25日からだった。報道によると、駅に設置されたコンピューターの画面には、「You Hacked, ALL Data Encrypted（お前をハッキングし、すべてのデータを暗号化した）」というメッセージが表示された。

交通局は、パートナー企業の米Cubic Transportation Systemsの協力のもと、念のための措置として、市営地下鉄の駅で券売機と自動改札口を11月25日から27日朝まで停止した。結果的に、この間は無料で地下鉄に乗ることができた。

http://www.dailymail.co.uk/news/article-2194960/United-Airlines-Computers-passengers-given-handwritten-boarding-passes.html
https://tech.nikkeibp.co.jp/it/atcl/idg/14/481709/120100278/?ST=cio-security&P=2

止めるしかない情報システム

- 代替手段がない
- 手動操作は不可能
  - Single Point of Failure(SPF)の存在を把握
    - 経営陣が知っていることが重要
    - 現場判断で停止させないことがベスト
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 多くの場合重要システムなので…

SPFは極力回避


JAL大量欠航を招いた「重量管理」のカラクリ

効率運用の負の側面が顕在化

次ページ ▸

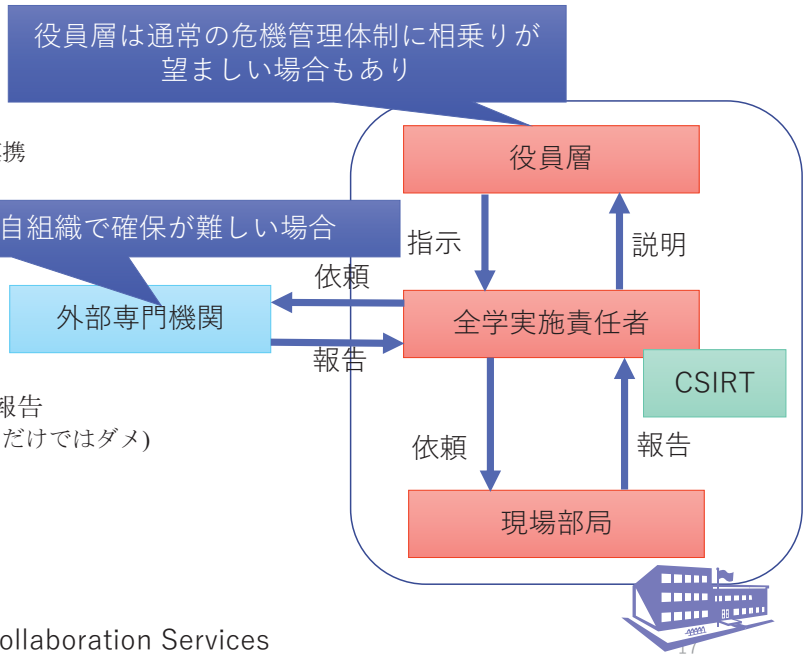
武政 秀明：東洋経済オンライン副編集長　2014/06/07 6:00

https://toyokeizai.net/articles/-/39544
https://ja.wikipedia.org/wiki/コンテナ#/media/File:Unloading_JAL_747.jpg

これからの大学に求められる能力

■ セキュリティマネージメント層
- 全学実施責任者
  - 指揮官役としての役割
    - インシデント発生時
      - 外部セキュリティ専門機関との連携
      - インシデント発生現場との連携
      - CSIRTとの調整
      - 役員層-他との意思疎通
    - アクシデント時の判断
      - 事業継続の判断
- CSIRT
  - 作戦参謀役としての役割
  - 技術だけでなく、組織運営への影響も報告
    - 他部門との連携必須(パソコンを見てるだけではダメ)

自組織での人材育成が必須
- 学内事情に詳しくなければ動けない
- キャリアパスで育成



NII Security Operation Collaboration Services

本当に欲しい人材は

■ おそらく技術だけのエンジニアは不要となる
- 今後数年間は…
  - SOCへの外注が進む…次期NII-SOCSの雲行きが…
  - セキュリティマネージメント層
    - ネットワークとセキュリティに詳しくなくてもよい
    - インシデント/アクシデントがBCPに及ぼす規模を想定できることが重要
- 急速に進むAI化&自動化
  - 雑魚はAIが片付けてくれる
  - 自己免疫機構
    - 攻撃検知と同時に検知パターンや暫定パッチを自動生成
- それでも残る人による判断
  - 自動対処はあくまでも人が判断する時間を確保するため
  - 暫定パッチ提供の可否・タイミング

パソコン触ったことがない人でも務まる…

教	育	環	境	分	科	会		選	出
SS 研教育環境フォーラム 2018 より									

アクティブラーニングの失敗事例
-教育現場が抱える問題とその解決に向けて-

亀倉 正彦(名古屋商科大学)

ＳＳ研教育環境フォーラム2018講演

アクティブラーニングの失敗事例

～教育現場が抱える問題とその解決に向けて～

２０１８．０９．０３
名古屋商科大学
地域活性化研究センター
商学部　教授　亀倉正彦

本講演の構成

自己紹介＆担当科目

↑ 「ＮＵＣＢフロンティア力育成講座」（GW企画実践）
「インターンシップ論」（GW・主体的発言・プレゼン）
「セミナー」（輪読→GW[グループワーク]）
「中部地域の都市計画」（講演・質疑・主体的発言）
↓ 「経営学入門」（講義　※変革中…苦労中…）

「教師からの一方通行」に近い授業から
「学生の発言や対話」によって構築される授業まで

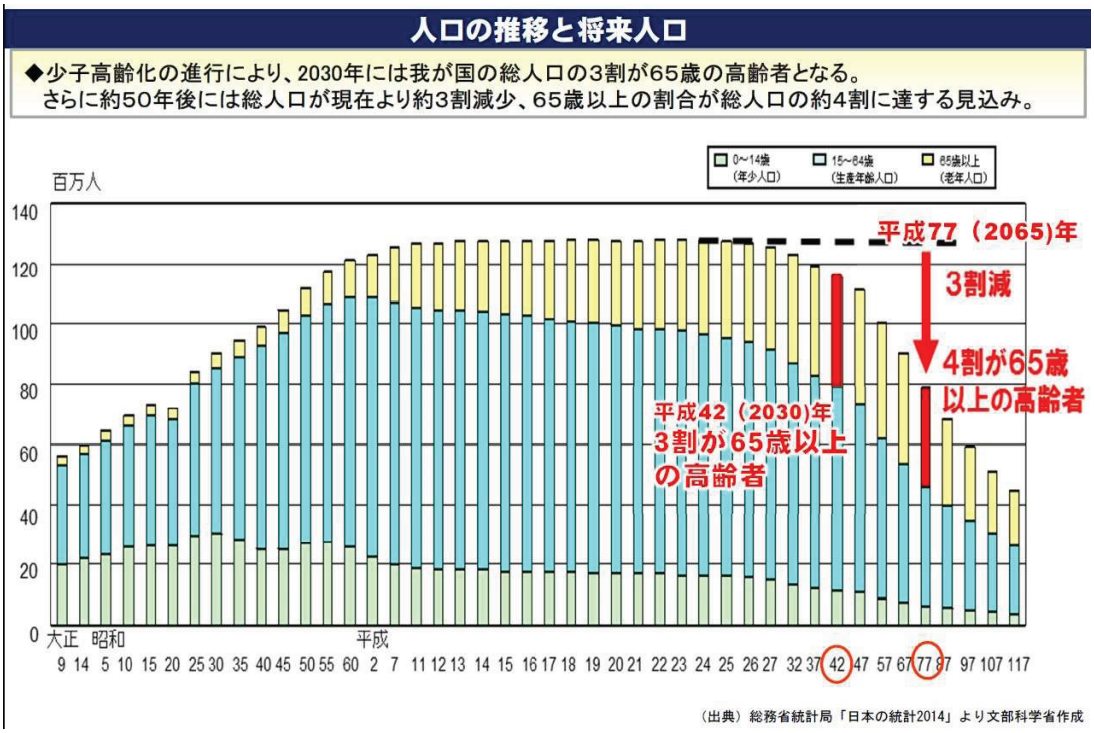
（主要）所属学会　委員会

◇教務委員会（前委員長）、（元ＦＤ推進委員会・幹事）
◇地域活性化研究センター
◇元「大学生の就業力育成支援事業」取組担当者
◇元「産業界のニーズに対応した教育改善・充実体制整備事業」
学内取組担当者　兼　中部圏副幹事校（ＡＬ担当）

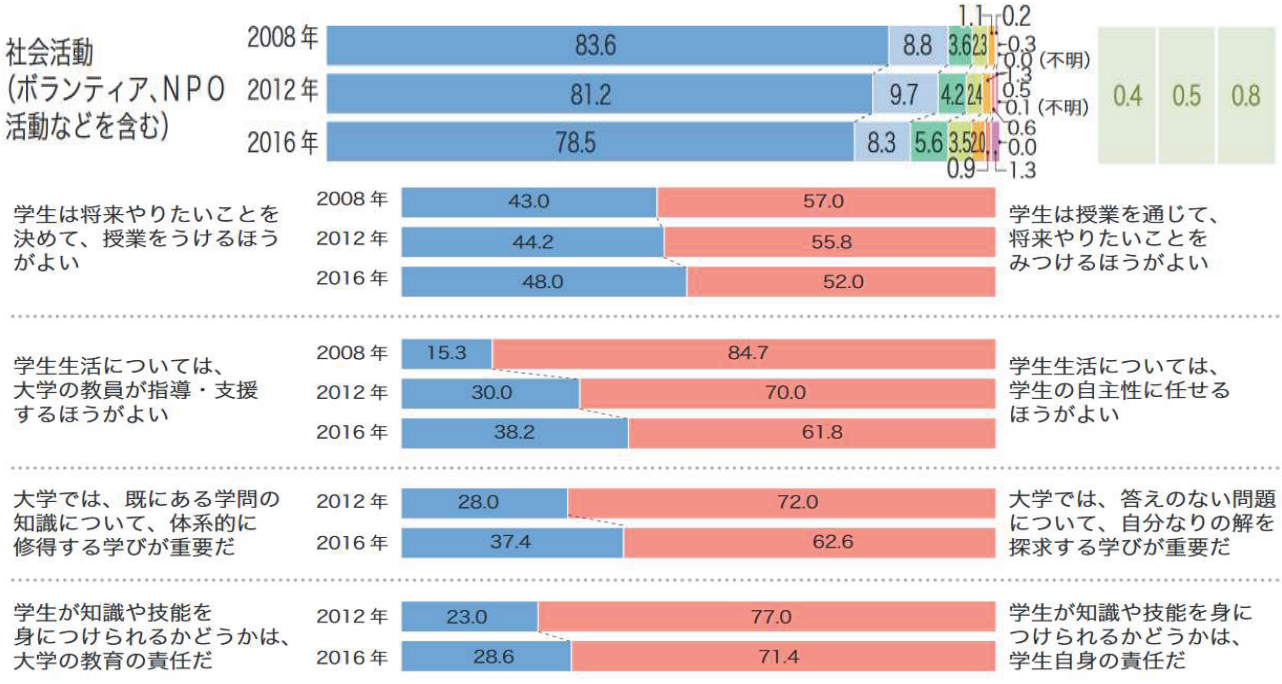
☆日本経営学会
☆組織学会
☆日本マネジメント学会（旧：経営教育学会）
☆大学教育学会
☆ＮＰＯ法人失敗学会、他

★総合戦略推進委員会（日進市）
★にっしん観光まちづくり委員会（委員長）　→　協会(2018.4)役員
★日進市道の駅整備検討委員会
★リニモ沿線地域づくり会議（愛知県）
★指定管理者審査委員会（日進市・委員長）、他

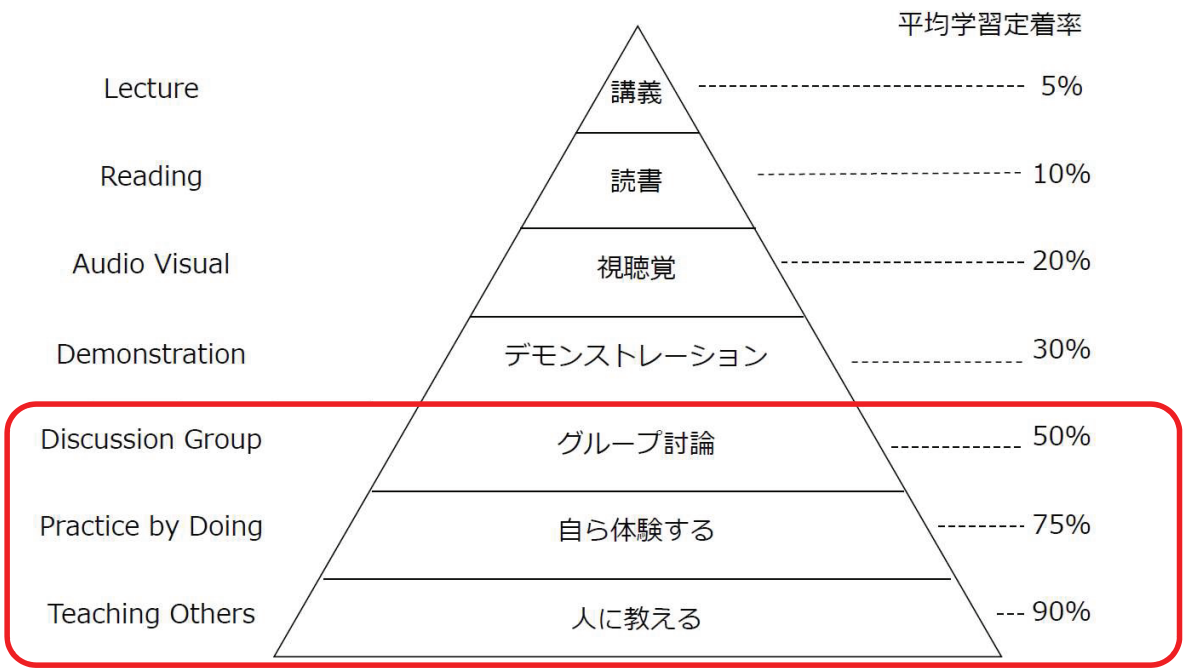
人口減少が意味するもの



データからみる大学生の学習・生活の変化
～ベネッセ「大学生の学習・生活実態調査報告書2016」より



The Learning Pyramid 学習ピラミッド
-National Training Laboratories USA



ＡＬ失敗の基本三事例

1．学びが「アクティブ(active)でない」こと
- 学びのアクティブって一体何だろうか…？？？

2．そもそも「学び(learning)がない」こと
- 科目目的は？　その活動の狙いは？
- 全学／学部の教育目標は？　位置づけは？

→「都市計画」（発言問題）

3．教員が「近視眼(myopia)」となること
- 専門性教育はもちろん大切。
- 但し、将来構想のない専門性教育は悪手。

（将来構想力＝imagination）

ACTIVE → 「主体的な」学生行動

Q．次のうち、アクティブラーニングの授業に該当すると思われるものはどれですか？（複数回答可）

①グループワーク、プレゼンテーション、討論

②教員による熱心で丁寧な講義

③予習復習、授業内小テスト、中間レポート

④どれも該当しない

A．

①

②

③

→

［官僚制の逆機能］ (by. Robert K. Merton)

①訓練された無能	(状況変化に対応できない)同調過剰。規則に固執することで、変化した状況に対応できなくなる。
②最低許容行動	(積極的に行動しない)処罰されない程度に規則に従い、積極的な言動をしなくなる。
③目標の転移	(本来の目的を見失う)目的と手段の関係が転倒し、規則の遵守自体が目的となってしまう。 成功の罠（成功経験が成功までのプロセスの全てを正当化してしまう）。
④革新の阻害	(変化に抵抗する)何か新しいことを取り入れて変革しようと試みると、 既得権益を保持しているメンバーからの抵抗を受ける。

「深い学びとは」

問題提起：
　Ａ語句→単純、　Ｂ語句と語句の関係→複雑

では、Ｂができたら「学びの深まり」と言えるか？
　→そのつながりを「丸暗記」したら深い学びなのか
　→理解と暗記をテストで区別できるのか
　※教員が「何を」「どのように」伝えたかによる。

①教員が措定した学びに到達するのか　ｏｒ
②学生が自分で何かに気づき、触発された学びを得るのか

「深さの系譜」との関わり(松下佳代,2015)

①深い学習　（＝講義内容との関連で正しく位置づけている）
　講義中心　知識技能の習得 論理や経験と関連させ繋げられる。
　→三本柱の論理構造を比較整理して位置づける。
　→理論を19c-20cのアメリカの経済実態と関連付ける。

②深い理解　（＝必要に応じて講義外の場面でも活用できる）
　ワーク中心　転移可能性や解釈応用やメタ認知的知識も含む。
　→現代ビジネスや日本的経営との関連を考える。
　→資格試験の発展的な問いに対して応用が利く。
　→学んだことを他の学問分野に結び付ける。

③深い関与　（＝前向きに積極的に取り組めているか）
　学生の関与　動機付け。
　→次スライドの次元３を参照。

適切な課題難易度の設計

[次元①．テーマ課題の解釈余地] ＝ 解決すべき課題は明確か

●作業課題はどの程度与えられているか。
●作業すべき内容をどの程度自分で見いだすのか。

[次元②．作業段取りのしやすさ]

＝ 作業の手続きや段取りは学生任せか懇切丁寧か

●作業のためのひな形はどの程度与えられているか。
●成果物の構造化をどの程度自分で考えて作るのか。
●作業へのヒント説明はどの程度与えられたか。

［次元③．解決必要性の自覚］

＝ 作業に取り組もうと感じるか=意欲の問題

●単位や成績評価とどのくらい紐付けされているか
●課題の狙いや目的などの趣旨説明はどの程度なされたか

Myopia → 適切なOwnership, Stewardship

Q．次のうちアクティブラーニングが上手くいかない原因として該当すると思われるものはどれですか？（複数回答可）

①研究をしっかりしているので問題ない
②努力する教員への適切なインセンティブ不足
③アクティブに学ばない／力のない学生の問題

A．
①
②
③

→

グループワークの効用とTips

◆一人では「言えない／言わない」意見が言いやすくなる。意見発言に二の足踏む恐れ。

◆学んだ知識を活用する場面では、正解／不正解でなく、個々の意見・考え方の多様性を認めることが大切である。

◆グループワークに参加する「全員」に役割と居場所があるように「場作り／環境作り」する。参加すれば自信につながることがある。

◆一部の強引な学生が押し切ったり、一部のやる気ない学生がフリーライダー化する形は、必要でない限り予防・回避する。

◆上手に活用すれば、クラス全員の意見を効果的に共有することが可能になる。

◆あまり長時間すると、単元の進度に遅れを来す恐れがあることに注意が必要。

社会人基礎力と教育改革力

社会人基礎力(学生)

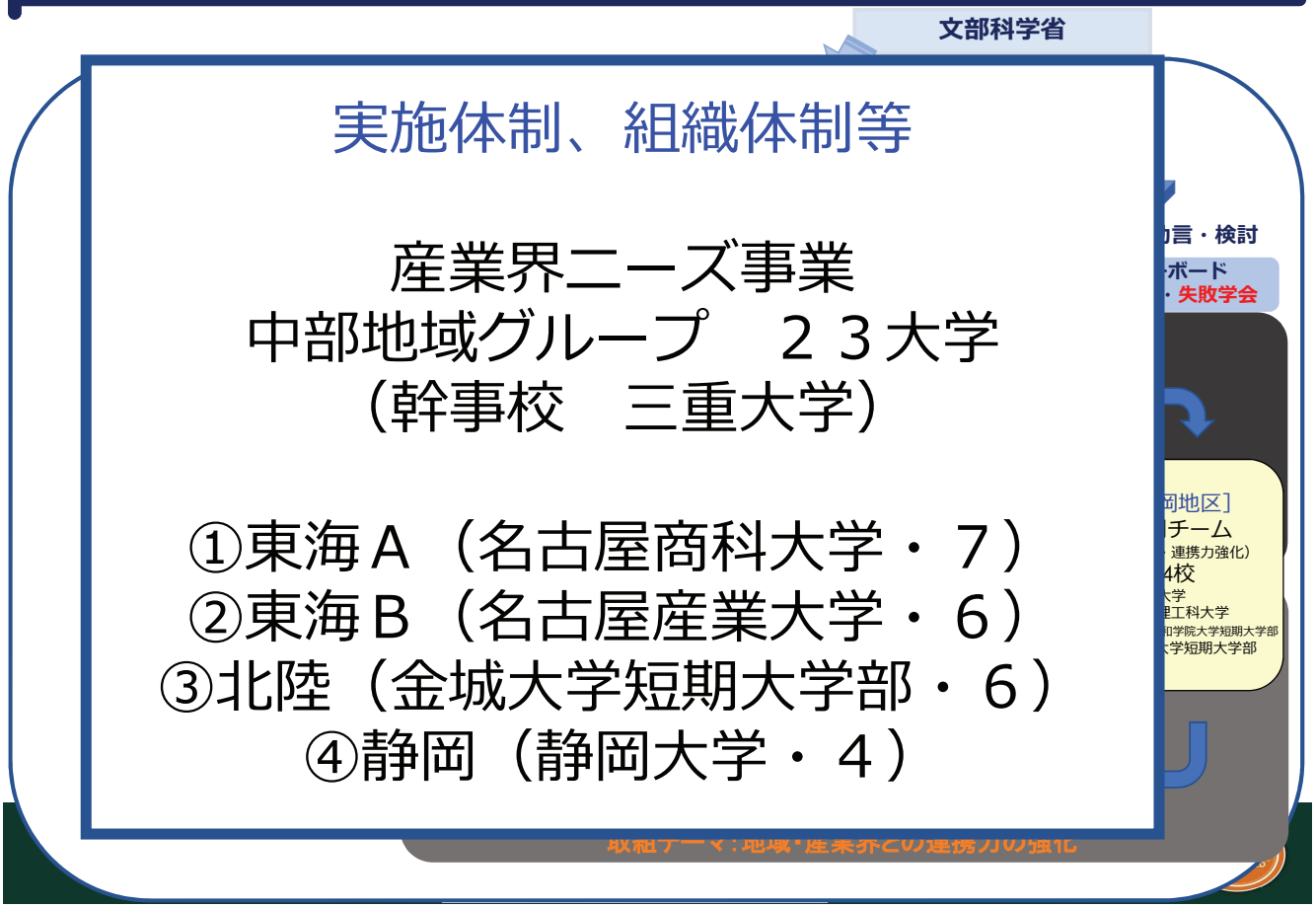
社会で働くために

1．前に踏み出す力
2．考え抜く力
3．チームで働く力

教育改革力(大学)

教育改革のために

1．前に踏み出す力
2．考え抜く力
3．チームで働く力



実施体制、組織体制等

テーマ設定の目的	**①アクティブラーニングを活用した教育力の強化** ・ 学生参加型授業、共同学習を取り入れた授業、課題解決型学習、ＰＢＬ、能動的な学習を授業に取り入れて、産業界のニーズに対応する。 ②地域・産業界との連携力強化 ・ 地域・産業界との連携によるインターンシップの高度化を図る。 ・ 地域・産業界との連携による授業の開講を行う。
産業界のニーズを把握する方法	①個別大学レベル 各大学は、それぞれの大学と関係する地域・産業界のニーズをアンケートや対話を通して把握する。 ②チームレベル 個々の大学が把握したニーズと大学での対応状況を、東海Ａチーム(７大学)、東海Ｂチーム(６大学)、北陸チーム(６大学)、静岡チーム(４大学)内の**連携ＦＤ**を通して検討する。 ③中部地域大学グループレベル ２３大学全体で、各大学の教育指針を把握したうえで、**中部圏産学連携会議**において、産業界側からのニーズに関する意見を得て、検討を行う。
期待される成果	①産業界にニーズに対応した人材育成体制の整備 ・産業界ニーズを取り入れたカリキュラムの改善 ・アクティブラーニング体制の整備 ・地域・産業界との連携体制の整備 ②中部圏教育改革ネットワークの構築 ・都道府県単位のネットワーク ・設立形態別大学ネットワーク ・目的別大学ネットワーク

とりまとめの経緯、目的
「失敗学」活用の背景

- 連携大学の多様性
  - 教育理念
  - 国立大学、県立大学、私立大学
  - ４年制大学、短期大学
  - 総合大学、文系大学、理系大学、福祉系大学
  - 学生数
  - 入学時の基礎学力

- 「成功」よりも「失敗」に共通性があるのでは
  - ノウハウがない、教職員からの協力が得られない、etc.

- 「失敗学」の理念
  - 同じ失敗を繰り返さないために失敗事例を分析

とりまとめの経緯、目的
失敗学の手法を活用

2013年5月　２３大学が手法を学ぶワークショップ
2013年8月　インターンシップ失敗事例ワークショップ
2014年5月　アクティブラーニング失敗事例ワークショップ
　　大学教育学会ラウンドテーブル
　　「失敗学から学ぶ教育改革」
2014年9月　『アクティブラーニング失敗事例ハンドブック』
2015年3月　『インターンシップ失敗事例ミニハンドブック』
2015年6月　アクティブラーニング失敗事例研究発表
　　大学教育学会自由発表
　　「教育改善における失敗学手法の可能性」
2016年3月　『失敗事例から学ぶ大学でのアクティブラーニング』
　　拙著・東信堂（溝上慎一・京都大学教授監修）
2016年6月　ＮＰＯ法人失敗学会・夏の大会　招待講演

とりまとめの経緯、目的
「失敗学」の方法論

1. 失敗事例の分析　⇒　直接原因と根幹原因の発見

2. 事例情報とそれから得られる『知識』の共有
　　⇒　同じ失敗を繰り返さないようにする

3. 原因、行動、結果を体系化する「まんだら」の作成
　　⇒　傾向と効果的対策の方向を見出す

4. 同じ失敗を繰り返さないための『仕組み』の構築

5. 先人の試行錯誤のデータベース化
　　⇒　最初の一歩を踏み出す勇気を与える

本講演の構成

1．はじめに
2．アクティブラーニング
　2－1．３つのポイント
　2－2．グループワーク
3．アクティブラーニング失敗マンダラ
　3－1．産業界ニーズ事業と失敗学
　3－2．アクティブラーニング失敗マンダラ
4．事例紹介
　4－1．特徴的な１０の失敗事例
　4－2．構造分析のススメ
5．まとめ

AL失敗事例HBの目次から

【はじめに】
- アクティブラーニング原因マンダラ
- アクティブラーニング結果マンダラ

【指導】
- 指導 1「課外活動における学生の怠慢な態度」
- 指導 2「商品開発後の販売の難しさ」
- 指導 3「グループワークでの学生の貢献度の差異」
- 指導 4「社会人基礎力の向上が認められない」
- 指導 5「プロジェクト活動における企業連携事業の進捗遅れ」
- 指導 6「リーダー不在のグループ活動に対する教員の支援」

⋮

【評価】
- 評価 1「アクティブラーニングの成果評価の困難さ」
- 評価 2「成果物への客観性の欠如」
- 評価 3「連携企業と教員の学生に対する評価の違い」
- 評価 4「学びのための成績評価（Assessment for Learning）」
- 評価 5「企業人の求める評価基準だけが正しいのか」

アクティブラーニング 失敗事例調査(H26.3実施)

◎産業界ニーズ事業・中部圏の東海Ａチーム（「ALを通じた教育改革力の強化」）
◎対象は「産業界ニーズ事業」中部圏２３大学（**回答２１大学**、**回収率９１．３%**）
　・産業界と連携して実施しているアクティブラーニング授業
　・科目担当者に回答を依頼
◎**回収された調査票の数**　合計**４５件**
◎**抽出された失敗事例数**　合計**６５事例**

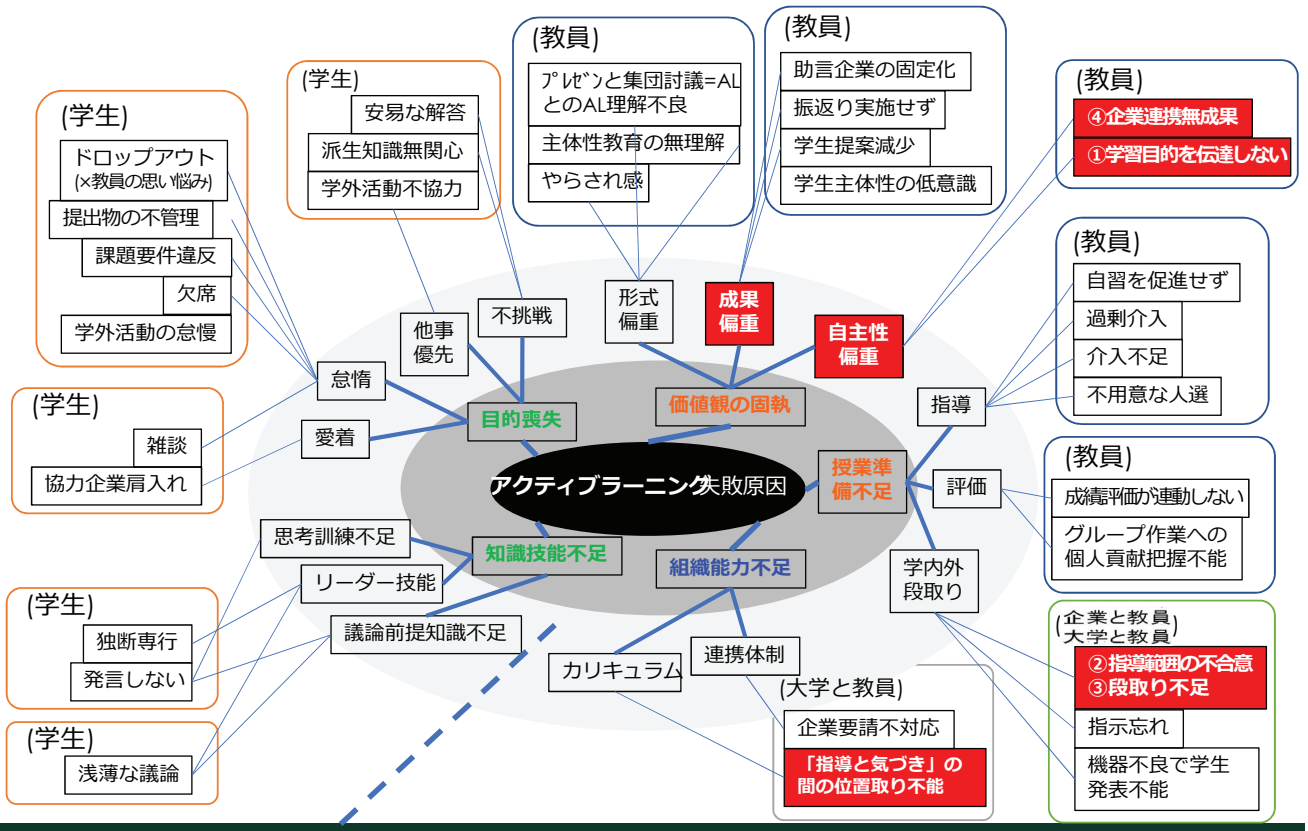
失敗結果（集計）

Grp作業無機能	成果物水準低下	教育負担増加	要件未完了	精神的苦痛	信用失墜
21	11	7	15	4	7
32.3%	16.9%	10.8%	23.1%	6.2%	10.8%

失敗原因（集計）

知識技能不足	目的喪失	価値観固定化	授業準備不足	組織能力不足
8	16	9	23	9
12.3%	24.6%	13.8%	35.4%	13.8%

(3) アクティブラーニング失敗原因マンダラ



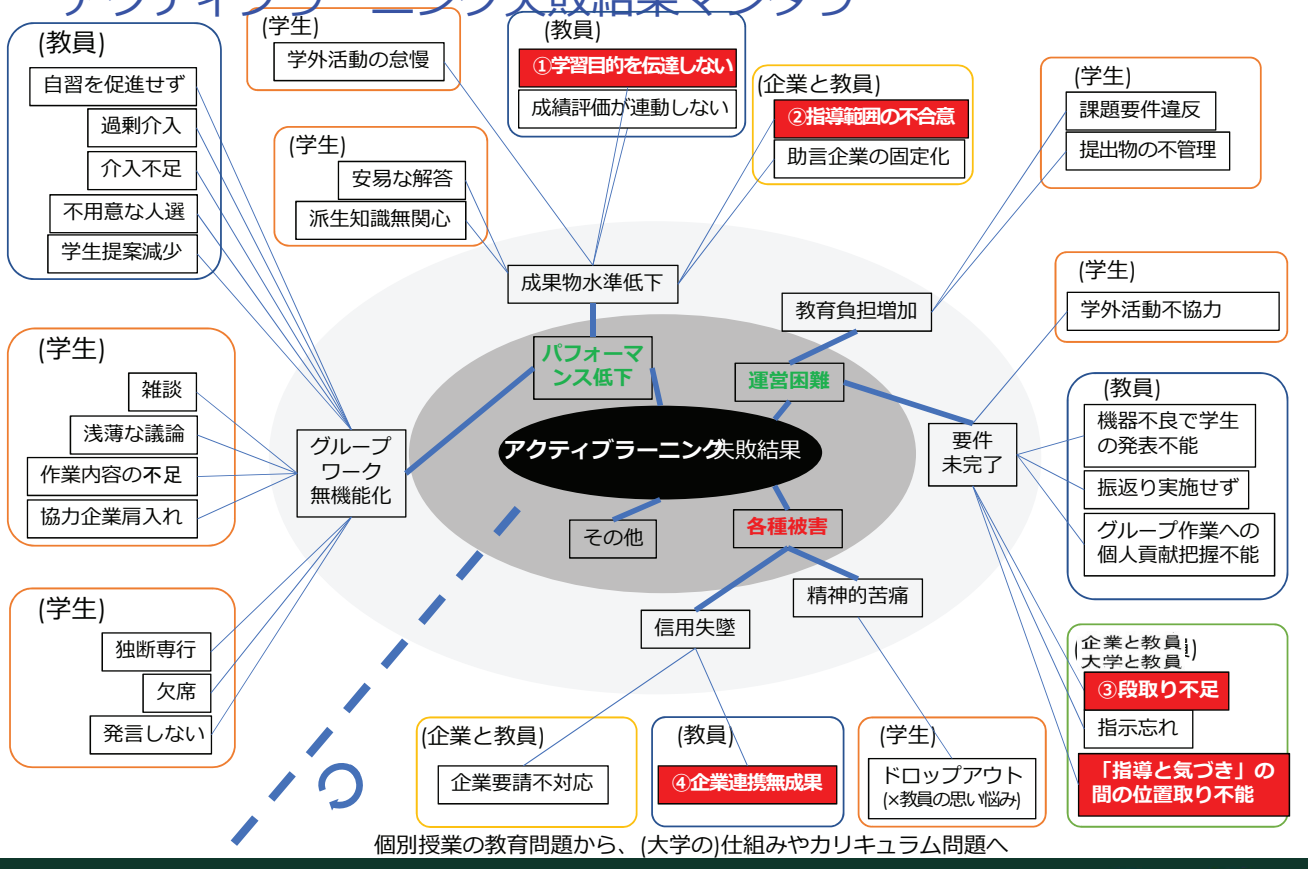
アクティブラーニング失敗原因マンダラ
注意すべきこと

■現実には複数の失敗原因は複合的に絡み合い失敗が起きる。

■研修で用いる場合には注意と配慮が必要。

…例えば、教員研修の場合、自己の反省点を棚上げし、学生や体制（学部学園）への批判に陥らせないように工夫する。

アクティブラーニング失敗結果マンダラ



個別授業の教育問題から、(大学の)仕組みやカリキュラム問題へ

アクティブラーニング失敗結果マンダラ
注意すべきこと

☆（インターンシップなどと異なり）その失敗が個別のクラス内の出来事としてとどまることが多い。つまり、教員個々の認識の問題になる。

↓

■何をもって失敗するのかが決めにくい。

■観察する人の主観によっても異なる。

■アクティブラーニング目的の二重性

①主体性、　②学習成果

→整理する必要

アクティブラーニング失敗原因マンダラ
AL失敗事例ハンドブックから

一例として、ALで話題になる「学びへの介入」について検討

↓

《介入が問題となる代表的な10のケース》

◆過少介入のケース(=自主性尊重)

…指導1(a),2(b),3(c),4(d),評価4(e),他5(f)

a学外マナー / b学習目的伝達 / c全員参加 / d学外講演 / e課題と成績評価の連動 / f学生の知識能力前提の考慮

◆過剰介入のケース(=成果尊重)

…指導7(g),評価2(h),3(i),他1(j)

g気づきの誘導 / h企業への愛着 / i壁越しの作業 / j過度な作業負担

↓

「介入不良」の観点でざっと　a～j　にキーワードを振った。

アクティブラーニング失敗原因マンダラ
論点. ファシリテートのあり方

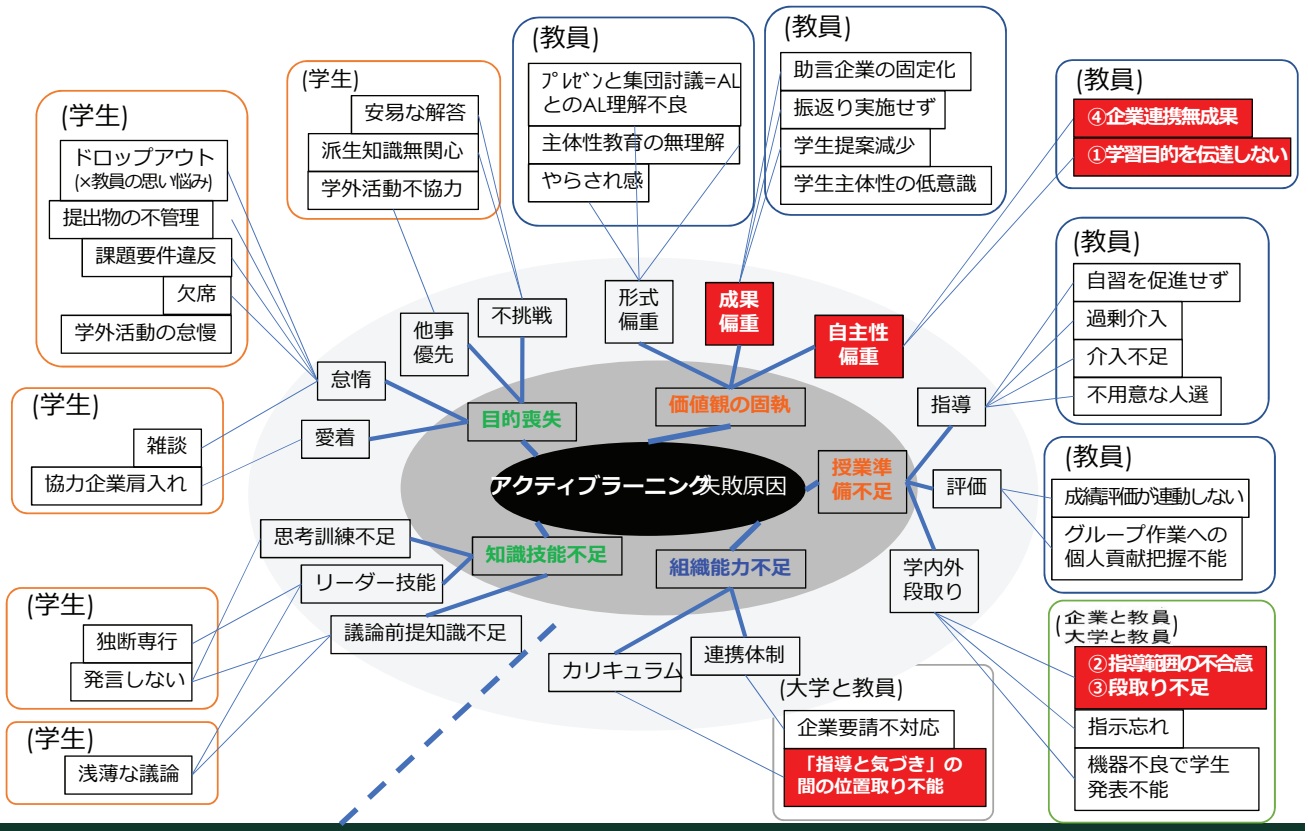
原因	行動	結果	キーワード
自主性偏重	**①学習目的を伝達しない**	成果物水準低下	**過少**介入
授業準備不足	**②指導範囲の不合意**	成果物水準低下	**過剰**介入
授業準備不足	**③段取り不足**	要件未完了	**過剰**介入
自主性偏重	**④企業連携無成果**	信用失墜	**過少**介入

自主性偏重（過少介入）　VS.　成果偏重（過剰介入）　の構図

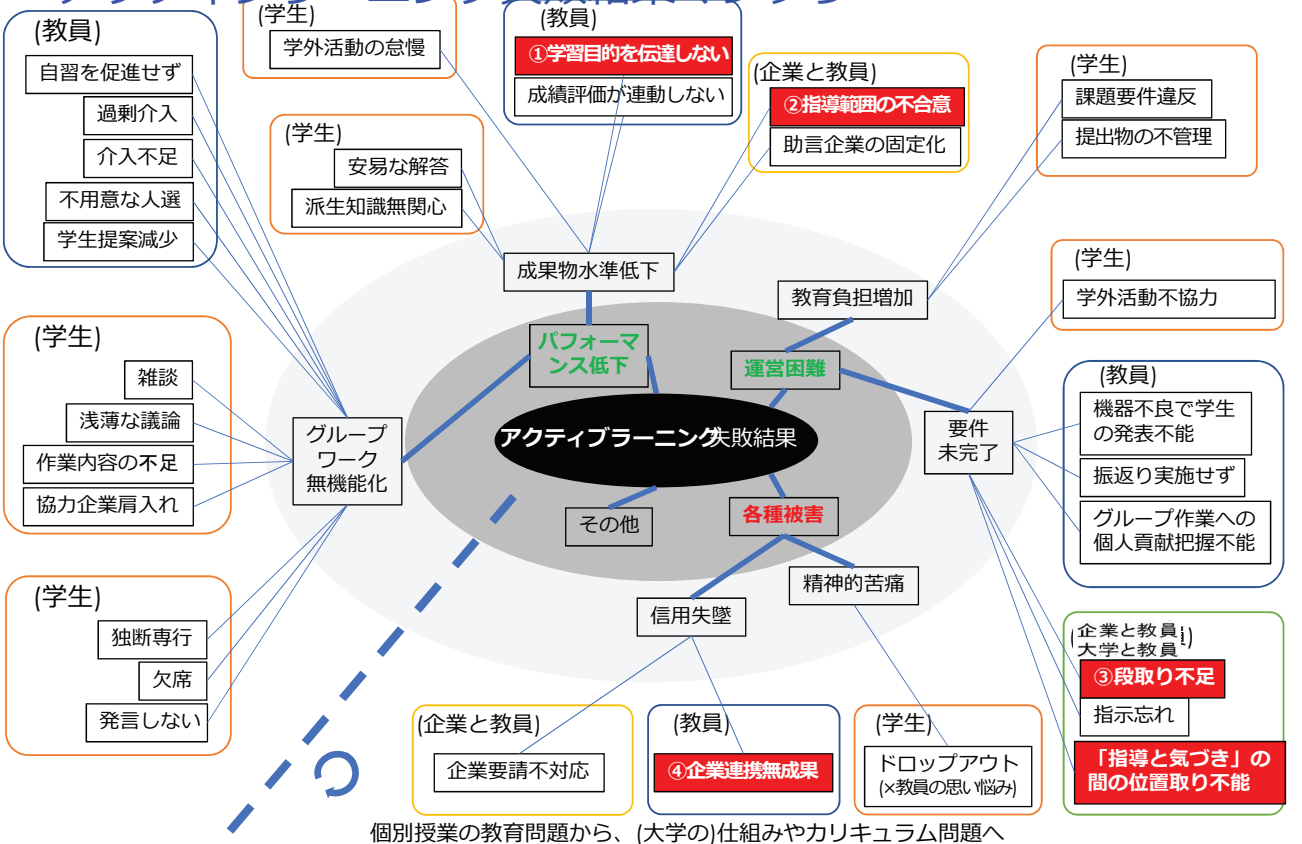
②と③	両方とも講師が「答え」を出したが、③はさらに重い失敗結果に至った →　**なぜこのような差が生じたのだろうか？**
①と④	同じ自主性偏重だが、④は信用失墜という重い失敗結果に至った →　**なぜこのような差が生じたのだろうか？**

Q１．「指導と気づき」の位置取りはどうすれば明確になるのか？
Q２．失敗はしてはならないのか？　しても良い失敗はあるのか？
Q３．なぜ成果を犠牲にしてでも自主性を尊重しなければならないのか？

(3) アクティブラーニング失敗原因マンダラ



アクティブラーニング失敗結果マンダラ

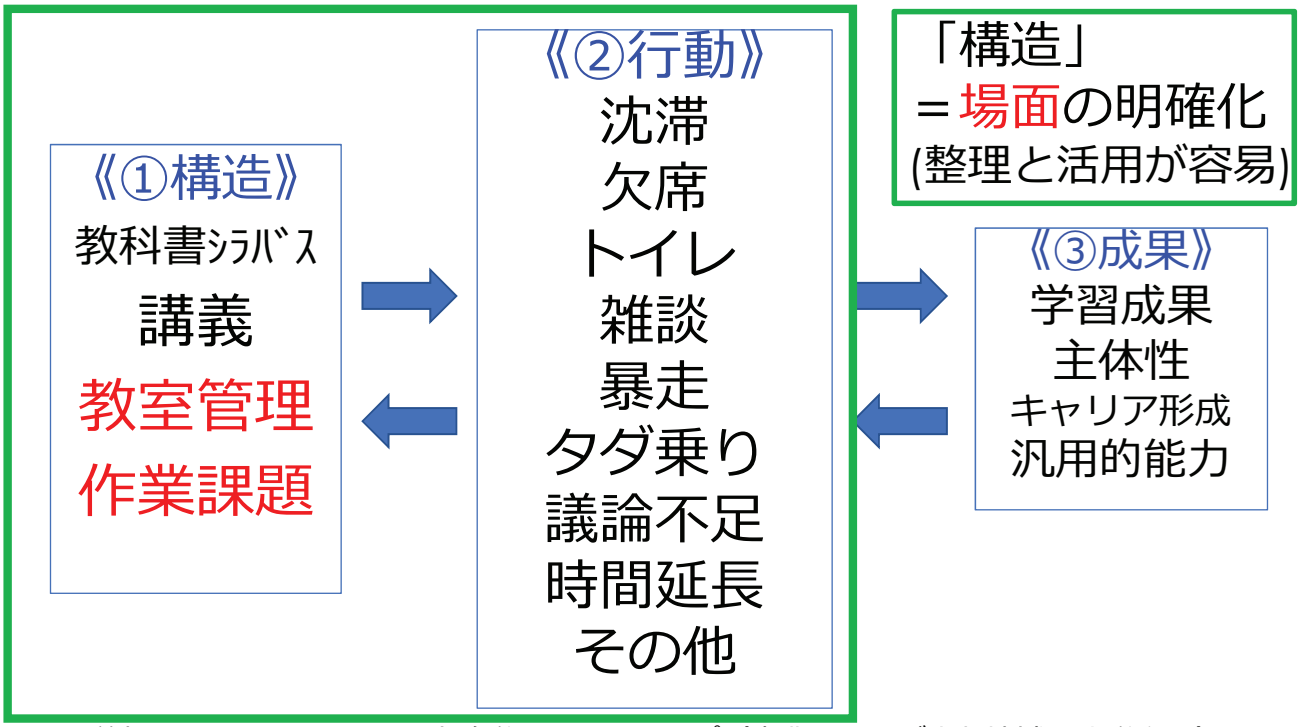


個別授業の教育問題から、(大学の)仕組みやカリキュラム問題へ

構造	行動	成果
前研修+事中監視	a学外マナーの悪さ	社会からの不信
学習目的伝達	b作業視野狭窄	挑戦課題発見不能
集団作業約束事	cタダ乗り行動	貢献学生の不満
原理専門バランス	d学外者講演に無関心	専門知識応用不能
学習動機外的内的	e課題と評価の不連動	学習意欲喪失
授業前提知識能力	f未熟なタスク管理	学習項目未消化
協力企業の要望	g気づきの誘導	学生企画機会喪失
現場直接体験	h企業への愛着	成果へのバイアス
指示伝達経路	i特定学生との二方通行	関係希薄指示待ち
作業(採点)時間	j毎回宿題＋ノート提出	消化不良精神疾患

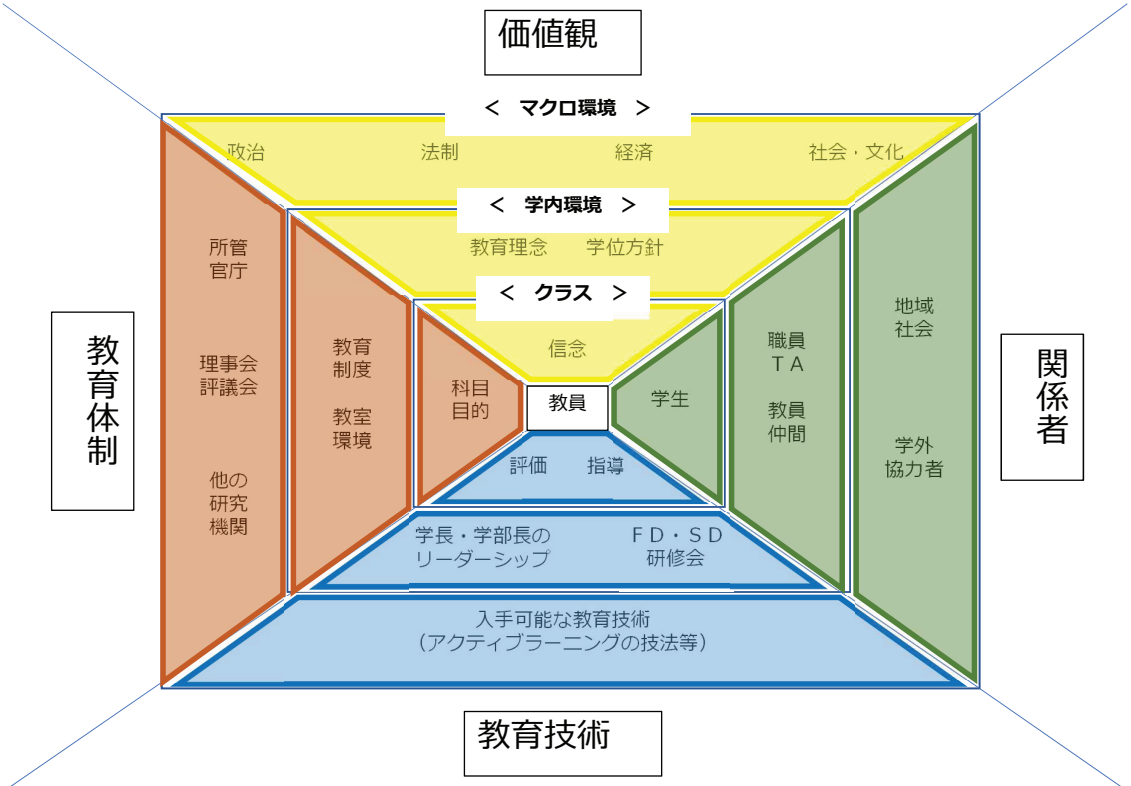
S-C-Pの発想　※産業組織論の知見の一部

【S-C-P発想】①構造Structure, ②行動Conduct, ③成果Performance



※着想のヒント　2013.5.18失敗学ワークショップ（産業界ニーズ中部地域23大学向け）
講師：飯野謙次（失敗学会・理事副会長 / SYDROSE LP 代表）

AL教育環境



①

Q．学生がアクティブラーニングをしたことをどのように確認することができるか？

Q. こちらが教えたことを受け止めて試験などで書き出せたとして、それで「アクティブ」と言い切れるのか？

［ヒドゥンゴール］

学生には伝えない何かの「隠されたゴール」を準備しておき、試験などでそれが学生自身で気付いたことの証として確認できるように準備しておく。

②

Q.
学外でのＰＢＬ授業、ケース授業、グループ活動を取り入れた授業、やりっぱなしになってないか？　学生の活動分だけ犠牲になる「知識の提供」の機会損失をどう説明するのか？

Q.
どこまでが大学で学ぶべき？　どこから卒業後の社会に出てから学ぶべき？

［経験の隔離］
コントロール不能な外部の諸要因（との接触）を意図的に日常的活動のルーティンから隔離すること。(Anthony Giddens 1991モダニティと自己アイデンティティ）

③

Q．reflection振返り　（※形成的評価 formative assessment）
中間試験は何のために実施しますか？　学生提出のレポートへのフィードバックは何のためですか？

Q. reflexivity再帰性
あなたの授業は何のためにあるのですか？　受講した学生は卒業後の社会で何ができるようになるのですか？　これを意識して定期的に授業のあり方を振り返りつつ修正していますか？

［reflexivity再帰性］
近代社会においては、社会制度(=教育もその一つ)そのものがこれまでの自らの経緯や経験を振り返りつつ修正されていくという再帰的なプロセスで営まれている。

④

◆アクティブラーニングの進展に伴い、学生の学び方が変化している。

◆初等・中等教育において、グループワークなどのアクティブラーニングの手法が広がっていくのに伴い、こうした学びを経験した生徒がやがて教員になる。

貴学の益々のご発展を心より祈念します。

ご静聴ありがとうございました。

亀倉正彦　名古屋商科大学
kamekura@nucba.ac.jp

教	育	環	境	分	科	会		選	出
教育環境分科会 2018 年度会合 より									

高等学校新学習指導要領における データサイエンスの扱いについて

大橋 真也
（千葉県立千葉中学校・千葉高等学校）

高等学校新学習指導要領におけるデータサイエンスの扱いについて

大橋　真也

千葉県立千葉中学校・千葉高等学校

はじめに

自己紹介

現学習指導要領

- 2013 年度より実施
- 数学科では，数学 I において,「データの分析」が必修化され話題になる。
- 情報科では，あまり明確には知られていないが，データサイエンスの一部が取り入れられている
- 教科間の連携はあまりなし

データの分析

- 四分位範囲，箱ひげ図，散布図，相関係数等
- 数学科の先生方があまり重視しない傾向に！
- 進学校では，進度の関係で教えていない学校も！
- 教えた経験がない，必要性の無理解
- いくつかの大学入試で採用し始める→徐々に対応が始まる

データの扱い

- データサイエンスとまでは行かない
- 教科書会社によっては，散布図，単回帰直線を掲載
- アナログとデジタルは学ぶが，連続データと離散データの扱いはあまり触れない
- サンプリングは教えているのですが...
- 量的データと質的データの扱いにも触れていない
- グラフの使い分けには触れているのに→ちょっとメチャクチャ
- 「情報の科学」の採択が 2 割程度 (選択必履修)，他は「社会と情報」

数学科と情報科の関連分野

- 集合 (集合演算，データベース，情報検索)
- アナログとデジタル
- n 進法 (2 進法の演算，基数変換，2 の補数表現)
- モデリング (数理モデリング，統計モデリング)
- シミュレーション (モンテカルロ法，待ち行列)
- 最短経路問題
- セル・オートマトン (ライフゲーム，渋滞)
- 暗号 (RSA 暗号等)
- 様々なグラフによる可視化
- 時系列データの扱い
- 回帰直線による予測