事業経営と情報セキュリティ

2013年7月22日

情報セキュリティ大学院大学　学長
日本生活問題研究所 CCW部会長

1. 現代という時代

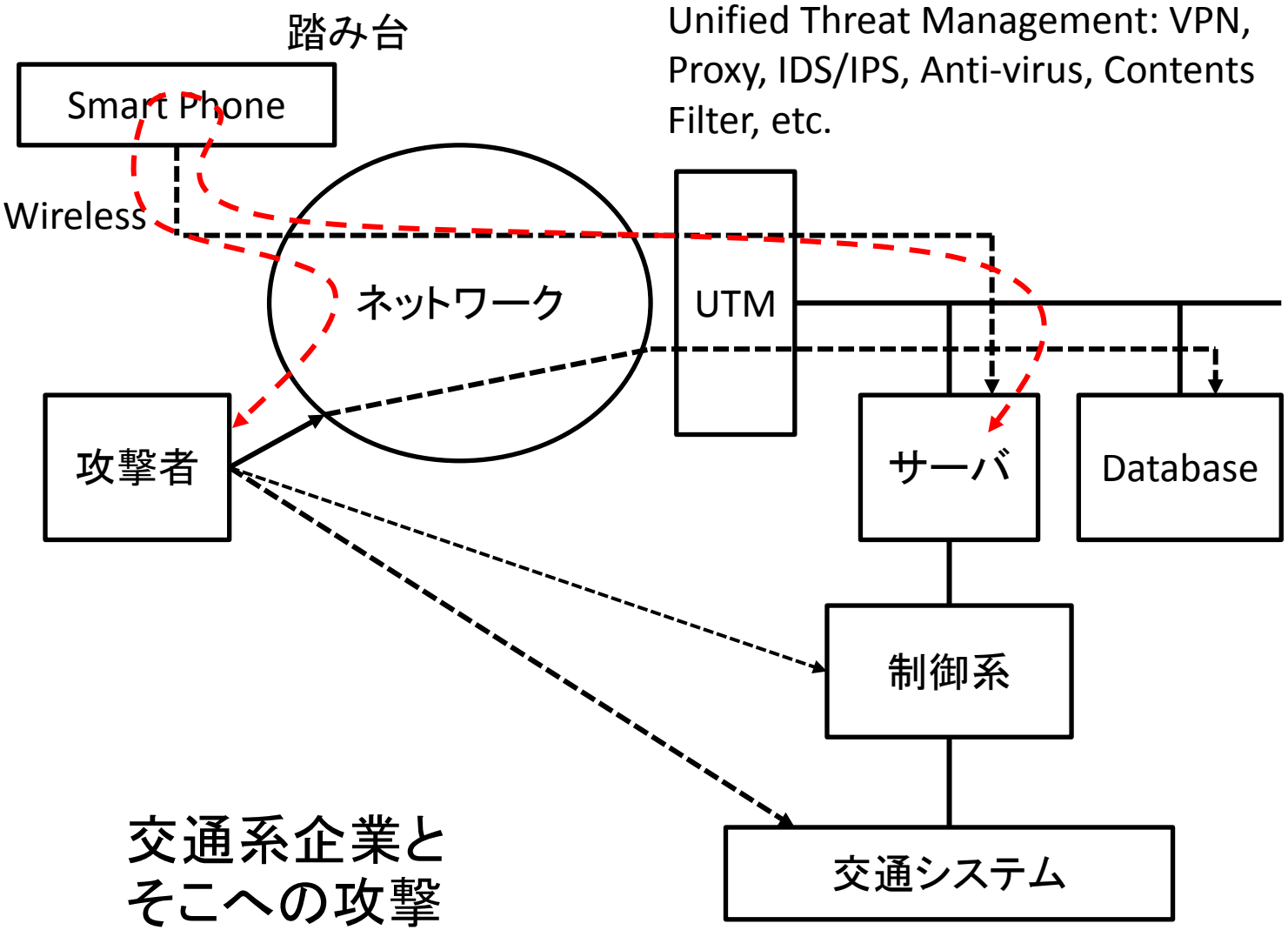
- 情報環境の変化
  - サーバクライアント + 企業内LAN + インターネット
  - スマートフォン+クラウド
- 情報セキュリティの変化
  - 愉快犯→　お金目的　→　政治信条、国家間
- 対応手法の変化
  - 企業出口対応FW + アウトソーシング
  - 経営層セキュリティ + 専門家

最近の攻撃

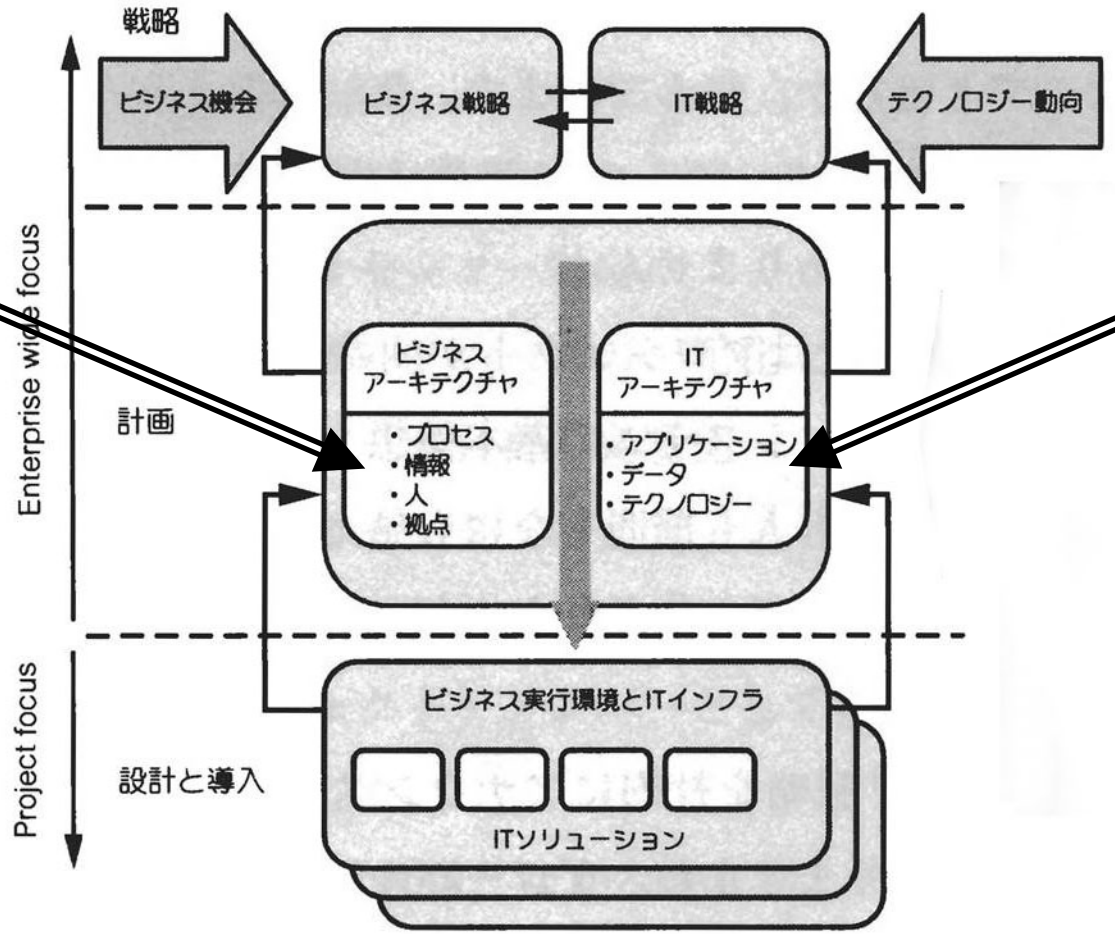
- 情報収集
  - Operation Aurora(2009): 米国企業知財流出（Google, Adobe, RSA他）
  - GhostNet(2009)　世界規模スパイネット
- 重要インフラ攻撃
  - Stuxnet(2010.9発生, 2012.6発表NY Times US+Israel), Saudi Aramco(2012.8)
  - 米電力会社発電施設マルウエア感染（2012末、USB)
- Wikileaks
  - 米国外交機密文書25万点全公開(2010.11より2011.9)
- 政府
  - 海上保安庁画像流出(2010.11,)国会議員のIDとパスワード漏洩(2011.8), 警視庁公安部外事第三課国際テロ情報の流出(2010.10), 警察庁誤認逮捕(2012.6-9), 農林水産省機密漏洩(2013.5)
- 金融機関預金の不正資金移動（2012, Operation High Roller, 世界$78M）
- 企業への攻撃/漏洩
  - AOL(2004), Yahoo(2004), KDDI(2006), 米PSN(2011.4), 米SonyOE(2011.5), ロッキード、米シティ(2011.5), Google(2011.6), 三菱重工(2011.8), IHI(2011春), YaHoo ID(2013.5)
- 韓国　放送局・金融機関(2013.3.20)
- 米DoD 中国軍部をサイバー攻撃で名指し批判(2013.5)
  - 2013.3 Mandian社　中国解放軍が機密入手目的でAPT攻撃を掛けたと報告

新しい事象と課題

- サイバー攻撃が増加：情報システムへの外部攻撃
  - 特定の標的への意図的組織的攻撃：Hactivism
  - 国家の関与：国家安全保障
- 攻撃対象が、制御系システムへ拡大
  - Stuxnet：イランのウラン濃縮設備へUSB経由の複合的マルウエアが侵入(2010)
  - Advanced Persistent Threat：特定の標的に対する持続的で高度なサイバー攻撃
- スマートフォン等増加に伴う新たな脅威の発生
  - スマホ、情報家電、センサー機器：PCと同じく世界共通のOSやソフトが利用されており、影響範囲大


踏み台
Smart Phone
Wireless
ネットワーク
UTM
Unified Threat Management: VPN, Proxy, IDS/IPS, Anti-virus, Contents Filter, etc.
攻撃者
サーバ
Database
制御系
交通システム
交通系企業と
そこへの攻撃

事業のニーズに合わせたEnterprise Architecture を備えたITシステムと脅威

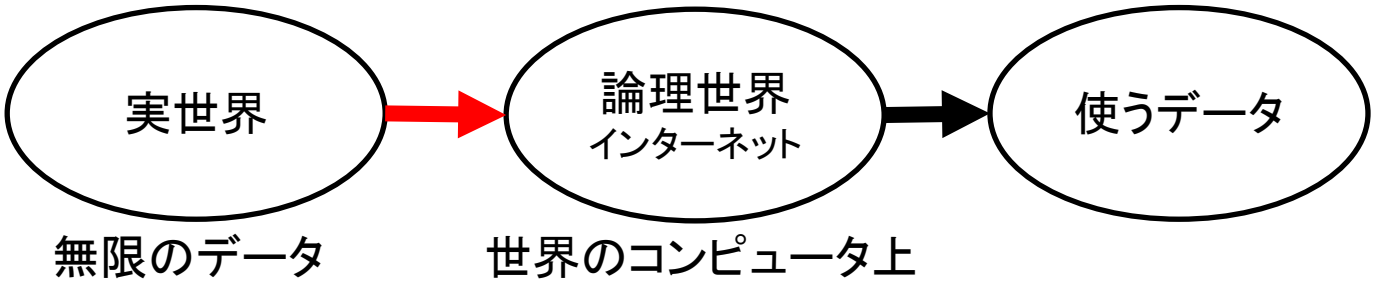


脅威：内部犯行、情報窃取、情報漏洩

脅威：インターネットからの侵入、システム情報窃取・破壊

Cyber Physical System 時代

- 膨大なセンサーがインターネットに接続される
  - 気象、スマートフォン、ビル管理、家庭内機器、自動車、交通
  - 膨大な実時間データの集積
- 膨大データ(Big Data)の解析
  - 快適な社会：現状把握、制御、予測
  - 裏側に潜む情報セキュリティ問題：データへのアクセス容易性、攻撃容易性・深刻度



我が国の情報セキュリティ対策

- 政府
  - サイバーセキュリティ戦略2013.5.21
  - 内閣官房情報セキュリティセンターNISCをサイバーセキュリティセンターに改組2015
  - 警察庁サイバー犯罪・攻撃への対策強化、防衛省サイバー防衛隊
- CSSC
  - 経済省：制御システムセキュリティ
- JPCERT, SOC, NICT, IPA

米国のサイバーセキュリティ

- サイバー攻撃
  - 政府機関、マスコミ、関係機関が標的ケース多発
  - 2012年末中国批判報道（NY Times, 等)後、新聞社へサイバー攻撃頻発、中国関与。SNS Twitter(2013.2)/Facebookへの攻撃
- 政府機関の取り組み
  - 連邦サイバーセキュリティ研究開発戦略計画(Trustworthy Cyber Space)
  - サイバセキュリティにおける国家連携の強化ISC
  - サイバーセキュリティ教育に関する国家計画NICE
  - サイバー司令部設置（増強　900→4,900)、防衛だけでなく攻撃目的編成
  - サイバー犯罪センター
  - 情報共有と安全性保護に向けた国家戦略
  - 2013.2Cybersecurity Framework官民連携制度策定中

対策に向けて

- リスクの認識
  - 侵入、機密漏洩、制御権窃取、社会影響
- リスク対策
  - 経営方針、管理運営、技術対策
- 経営方針
  - 対策組織（上意下達、下況上達）、インシデント対応（迅速）、機密情報の認識
  - IT技術：情報セキュリティはコア技術、技術は100%を保証できない。新規脅威の存在

対応手法の現状

- 技術の現状
  - 発生事象対応技術： UTM, Malware分析
  - 応用構成： 応用層内セキュリティ対応
  - SELinux： 権限の分割
  - ネットワーク： スイッチ構成の自由、基本機能(Dumb Network)
- 管理
  - フィッシング： 銀行・一般、10%(添付メール開封率)
  - ISMS：資産分析と基本構造提示、人間系の考慮
  - ベストプラクティス
- 法制
  - 自由と制限：インターネットの自由、信書の秘密
  - 情報系犯罪への対応は初期、規範未成熟

今後の方向と課題

- 技術
  - 基礎・基盤技術の再検討、OS強化
  - 新ネット： 管理強化、プロトコル制限
  - 旧機器（無対応機器）の整理： インターネット上、制御システム等
- 管理
  - 技術及び人間系・経営系との密連携
  - 技術補完とそれぞれに不完全性意識
- 法制
  - 情報対応ケースの蓄積
  - 情報社会規範の熟成と法制整備

2. 情報セキュリティ対策技術

① ネットワーク技術
- 認証、マルウエア分析、DMZ、FW、パケットフィルタリング、IDS/IPS、プロキシ、VPN、無線
- 新世代ネットワーク：モビリティ対処、セキュリティ対応

② システム技術
- セキュアOS、セキュアプログラミング、セキュア開発
- ログ、TPM、アクセス制御、thin client

③ 暗号と認証
- 共通鍵、公開鍵、アルゴリズム、ハッシュ
- 管理と運用の組み込み

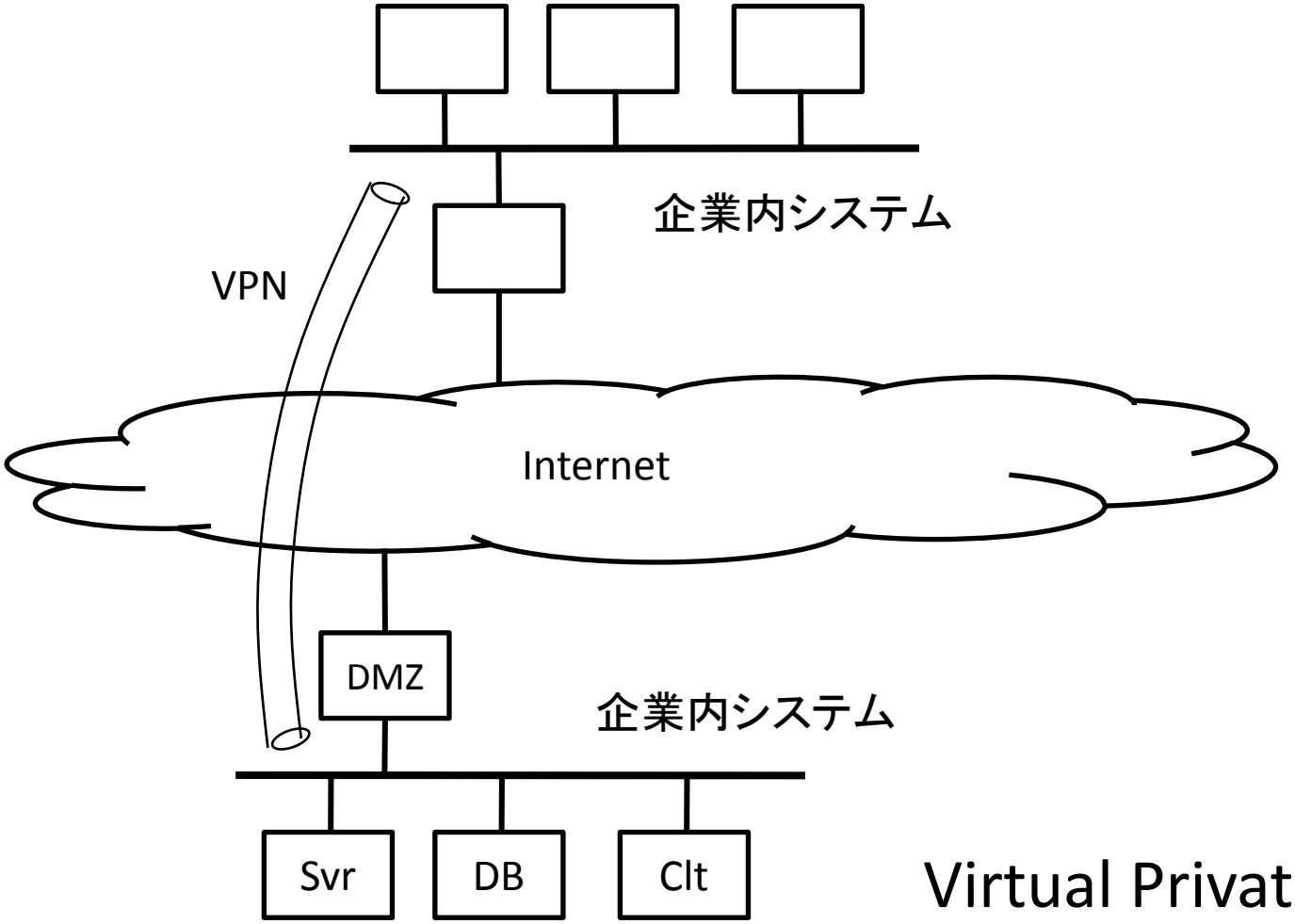
④ モバイル対策

⑤ 組込製品対策

⑥ SNSの利用

暗号の利用

- クラウドの利用増加
  - サーバコストの低減：管理、維持、高速度回線
  - 外部クラウドにも重要情報配置：　BCP対策
- 暗号の必要性
  - 暗号化して蓄積：クラウド管理者にも見せない
  - 暗号化したままの検索可能暗号
  - 機密分散の利用による確実化：　障害時用、冗長配置と兼ねる方式
    - カード利用による鍵管理の容易化
- 最近の暗号
  - 柔軟なアクセス条件設定、検索可能暗号



Virtual Private Network

組み込み製品へのセキュリティ対策

- 組み込みのリスク
  - 各段階での対策：企画、開発、運用、廃棄、漏洩や不正アクセス対策、修正の通知法、組織としての取り組み方針
  - ソフトパッケージ販売元のサポート体制事前確認、長期利用で危殆化
- 発生ケース
  - ATM/POS/航空チェックイン端末のウイルス感染とサービス停止
  - 無線LANにカーナビ接続（ガソリンスタンド無線LAN）の脅威
- 対策
  - リバースエンジニアリングし難い製品設計
  - 機密性、改竄からの完全性、可用性、利用ガイドにセキュリティ情報明記
- 今後
  - コンテンツセキュリティ、暗号化、ユーザ認証、IPv6等

モバイルマルウエアと対策

- 2004年6月： Cabirロシア、2008年：Symbian OS向けで400種
- 2011.12: Android で13,000種
  - スパイウエア67%、SMSトロイの木馬、iOSはAppleの情報提供無し
- 2013.6: 年間614%増加(28万件悪意アプリ)
  - Android(60%スマホ)が狙われる(92%)(スマホシェアは、Apple 19%, MS18%)。利用者が最新OSへ更新少ない
  - FakeInst等詐欺が62%/SMSゾンビ/NotCompatible/Android.Bmaster
- BYOD
  - Bring Your Own Device: 個人所有の端末を仕事でも利用する
  - セキュリティリスク；端末のなりすまし
  - MDM: Mobile Device Management, 2011より
- 対策
  - Mobile Security: 集中管理でスキャンや定義ファイル更新
  - 対策アプリLockout: 紛失・盗難対策：アドレス帳のクラウドへのバックアップ、端末の位置情報検索表示、遠隔操作で端末から警報音を鳴らす、操作した人の写真を取り持ち主に送付

サイバー攻撃インフラ

- Botnet: 遠隔C&Cサーバから Bot内マルウエアを操作して大規模攻撃
- Malnet: Malware Delivery Network 感染サーバ基盤攻撃。1,500種。Search Eng./Email/SNS/Mobileから
  - 多くのサーバを使い、マルウエア配信ネットインフラを作り、導いて感染させる。時々刻々変わる
- RAT: Remote Access Tool.
  - 遠隔操作を可能にするトロイの木馬。実行ファイルを直接メモリに読み込み、自身を復号化する。それがC外部からSSL通信を使ってファイルをダウンロードし、隠れたメモリ領域に読み込む等。

ソーシャルメディア

- Social Mediaの発達「公共財 SNS」
  - 人と人との間の繋がりの新たな構築：物理距離より、興味の距離、新たなリアル、興味の発信と共有
  - 新たな個人の出番（Netで発言する人）
  - 新たな知能：世界の知恵を借りる集合知が可能に
- 問題点
  - 社会悪の誘発、デマ
  - SNSのトラブル例：不用意なアルバイト発言、ソーシャルハラスメント、SNS疲れ（一貫自己像）、SNS体裁問題
  - SMの政府/自治体利用（広報+コメント）、機密保持と継続性、情報保存と廃棄
- 適切利用とリテラシー
  - 企業による利用と運用ガイドライン
  - 情報共有を企業内で実現できる企業内SNS: MS Yammer, Sale Chatter, 日本IBM IBM Connections, 縦割り組織の補足

3. 情報の特殊性と法制

情報技術の特殊性

- 距離を超え/壁を通過：迅速に世界と情報授受
- コピーが容易：　メモリ利用、情報窃盗は困難
- 目に見えない/物理サイズが無い
- どこにもある汎用情報処理機器
- 情報の法的禁止方式と法的保護方式
  - 禁止：負の財産型（事前）と不法行為型（事後）
  - 保護：知財型（パブリシティ含む）と秘密型（営業秘密）
- ソフトウエアの特性
  - かならずバグがあり、止まる可能性
  - 製造物責任法（PL法）の適用対象外

情報法制

- 諸問題
  - 電気通信事業法、信書のガイドライン
  - 通信内容、通信者情報（トレースバック）
  - 個人情報保護：実体との乖離、世帯単位と個人単位
- 国内対応
  - ウイルス作成罪(2011)、フィッシング罰則(2012)
  - 法制理念にコンシステントな1セットの体系化
  - 理念の対立に対する対応戦略：市場テストは米国（特区）
  - 海外クラウド対応は税制とDB規制
  - 専門家と政治家の役割分担：専門知識 vs 判断と責任
- 国際問題
  - 法制理念の相違 x 国際協調の必要性
  - 先に許可範囲を決めるか、試行後判例を積むか
  - 国際協調メカニズム形成、サイバーセキュリティに関する規範の整備、新国際秩序作りに戦略的に関わる

情報処理の高度化等に対処するための刑法等の一部を改正する法律

- 平成23年6月24日法律第74号
  - サイバー犯罪に対応するため、刑法ならびに関連法の改正を行う
  - コンピュータウイルスの作成や提供、保管をした場合不正指令電磁的記録に関する罪として犯罪化
  - メールサーバやリモートストレージサービスのサーバから捜査に関連するデータ（電子メールなど）のみを捜査機関が差押、押収することが可能
  - わいせつ画像等を電子メールなどで送信することは処罰対象
  - サイバー犯罪条約批准(日本は、2012.7)

4. セキュリティ経営とリスク

- リスク分析と対応
- セキュリティの考え方
- 標準化と統制
- 経営判断
- グローバル化
- BCPの課題
- 対応の原則
- 管理と運営

リスクの考え方

- リスクとは
  - 人的損失、財産損失、責任、投機、戦略、無形
  - 投機的リスク： チャンスの創生
- リスク対処：リスク最適化プロセス
  - 損失の発見と最小化
  - チャンスの発見と最大化
  - リスク情報の共有：リスクコミュニケーション
  - 企業価値：有形財と無形財（80%/2010)
- ソフトリスクの管理
  - 倫理観、企業理念、企業目標、企業文化、信用、透明性、社員の自発、社会化、モノ・カネからヒト・ココロ

リスクと情報セキュリティ

- 情報の位置
  - 公開し宣伝するべき情報
  - 秘密にしておくべき情報
  - この情報種別判断は経営判断そのもの
- この判断に基づいて行う作業

  ＝　情報セキュリティ対応・管理
  - 企業の強みを護るとともに、チャンスを作り現実のものとすべく行動する（リスクテーク）
  - リスク対象の多くが「情報」

情報セキュリティのレイヤ構造:企業における情報の役割

レイヤ	目的	守るべき情報
レイヤ4	情報処理システムとしての企業を守る	意志決定に必要な意味情報(インテリジェンス)
レイヤ3B	企業の信用・信頼に直結する情報を守る	契約約款・内部統制・コンプライアンス情報・風評
レイヤ3A	提供するサービスの品質を守る	サービス品質を表示するメタ情報
レイヤ2	情報資産のCIAを守る	管理している情報資産
レイヤ1	コンピュータとネットワークを守る	コンピュータとネットワーク

品質保証： JIS等の認証制度、格付け機関、資格、
見えないものの品質可視化： 情報セキュリティは代表例

情報漏洩の問題

情報の種類	秘密にするべきもの	漏洩の結果生じる問題
企業情報	製品/サービスの優位性の源、生産手法、運営手法、（分析結果）	製品/サービスの優位性消失
個人情報	利用者・顧客の情報、企業内従業員の情報： ビッグデータ	企業の信用・評判が失われる 守るべき注意義務を怠った しっかり管理していたが盗まれた

評判と対策

- 評判・信用
  - 企業として過去の積み上げによる大きな資産
  - 一旦失うと回復に長期間を要す
- 対策
  - 注意義務違反： 本質的に避けるべきもの
  - 管理したが盗まれた： 監査提示＋対策方針の即時公開（詳細不明でも）＋具体策策定
  - 危機管理：確率は低くとも、その評価とは独立して「あり得る事態を想定した準備」

セキュリティの考え方

- 経営の安定性
  - 企業業務の多くはICTに依存：システム等のセキュリティ対策でリスクに対応し、経営の安定性と信頼性を確保
- リスクに対する対応と責任
  - 回避努力、保険によるリスク移転、対策で低減、残りは受容
  - 過失責任の原則: 予測可能性と結果回避可能性を詰める、それでもリスクを取らざるを得ない場合がある
  - リスク原因者特定不可能な場合：大気汚染、社会で責任を負う
- 情報セキュリティのガバナンス
  - 情報管理の原則：Needs-to-Know原則に基づいた情報セキュリティ管理 vs 家族主義（社員全員経営）
  - 活用：市場機能、法・制度、自律的規律、技術・標準

セキュリティ対応と経営判断

- 対応策
  - 情報資産の管理＋破られたときの法的対抗手段＋第三者評価認証制度（例　ISMS)
- プロセスの統制
  - 資産を守ることでなく、プロセスの妥当性評価：　品質保証と品質マネジメントの区別
- 経営判断の原則：適法性とリスクテイク
- ベストミックス
  - 伝統はボトムアップ、情報セキュリティ施策はトップダウンが不可欠
  - 総合性人事 vs 情報セキュリティ専門性人事
  - セキュリティ：人間は弱い、それを極力防止する仕組み準備
- 経営陣との連携
  - ツールや部署任せでなく、事象発生時対応に備える
  - 情報管理は経営の一環、アウトソーシングで全対応は困難、経営における情報セキュリティ担当は必須

グローバル化と情報セキュリティ

- 文化的差異による問題発生
  - 生まれ育った文化環境と、企業文化
  - 集団主義的社会：同僚のミスをかばう問題点
- ホフステードの文化的次元
  - 権力・個人・男性的・不確実性・長期指標
  - 2国間の文化的スコアの差異 vs 問題発生確率
  - 男性と女性：機密を漏らすリスク、1.8倍
  - 宗教の影響：キリスト教、イスラム教、仏教、機密情報を共有するリスク（1:1.7:3倍）
- 海外会社における留意点
  - Needs-to-Knowの原則をしっかり教育すること
  - 職務上見に付くノウハウは営業秘密で管理必須、スキルは個人付帯

浅井：情報セキュリティ大学院
大学　学位論文2011

BCPの課題

- 事業継続
  - ICTへ高依存だと、事業継続と情報セキュリティは同一
  - 実行性あるBCPが取引上要求される：取引先を対象に
- 被害想定手法の課題
  - 原因からの分析（確率）でなく、起こり得る結果事象（原発の事故可能性）を想定し対応策を検討
  - 柔軟性と演習の重要性、リーダシップ
- 経営におけるBCPの位置付けの課題
  - 非シナリオ提示型訓練
- リスクコミュニケーション：企業間、行政、NPO、消費者
  - しなやかでしたたかな柔軟性と復元力

情報セキュリティ対応の原則

平時の基本認識4原則

1. 企業は、リスクの防止・保護のみならず、即応力・復元力を重視する
2. 企業活動はICTに依存し、そのリスク対策は経営者自ら最適化を図る
3. 対策は経営全体のガバナンスと責任のあり方と整合し、統制の取れたものである
4. 対策は企業文化等と不可分で、移殖では済まず、自ら生み出す

非常時の行動規範原則

林、田川、浅井著「セキュリティ経営」
勁草書房、2011年12月

管理・運営

- 管理問題: CIA, RASIS, PDCA（インシデント・レスポンス）
- 情報セキュリティ管理システム: 情報分類、リスク特定、評価、監査
- 情報セキュリティ予算(米)
  - 当初全IT予算の7-8% 落ち着くと3-5%、コンプライアンス対応で増加傾向
- 投資効果の評価基準
  - ROIで評価（米、日本では少）、直接売上に結びつかないが、信頼を高める企業価値生み出す効果あり
- 外部委託
  - 企業の40%は何らかの機能委託、全て委託は2%(米), ITリスクをコントロールできないと経営者責任を問われるので内部へ戻し続く
- 保険、企業の30%（米）が採用、8%(日本)
  - サイバーアタック保障保険、個人情報漏洩保険、IT事業者向け賠償保険、ネットワーク総合保険、e-リスク保険、eBANKセキュリティ保険など

5. 今後に向けて

- 社会科学の総合：法学・経営学・社会学
- セキュリティ対策
  - 資産、リスク、対応判断、残存リスク、コスト
  - 既存脆弱性は可だが、新規脆弱性は予測不可能
- リスクの定量評価
  - リスク＝損失＊攻撃成功率＊攻撃発生率
  - 観念論からの脱却：リスクを保険で扱い可能とし、経済活動に組み込む
- 我が国の情報セキュリティ体制のあり方
  - 個人、企業、政府、国防
  - 研究、教育

人材の要請

- セキュリティ専門人材の要請
  - 情報セキュリティ技術の研究・開発
  - セキュリティ対応実務者、システム運用者
  - 情報収集・分析と対応：専門企業、Forensics、国レベル、サイバー防衛
- 一般企業の人材
  - 情報システム担当のセキュリティ教育：基礎知識
  - 企業内情報管理者
- 管理経営人材
  - 対外情報戦略立案・実行者
  - CIO: 経営陣とセキュリティ部署との間を繋ぐ人材としての役割、完全外注はあり得ない
- 一般人リテラシ
  - 情報セキュリティ文化、若い時代からCTF

おわり

ISS square

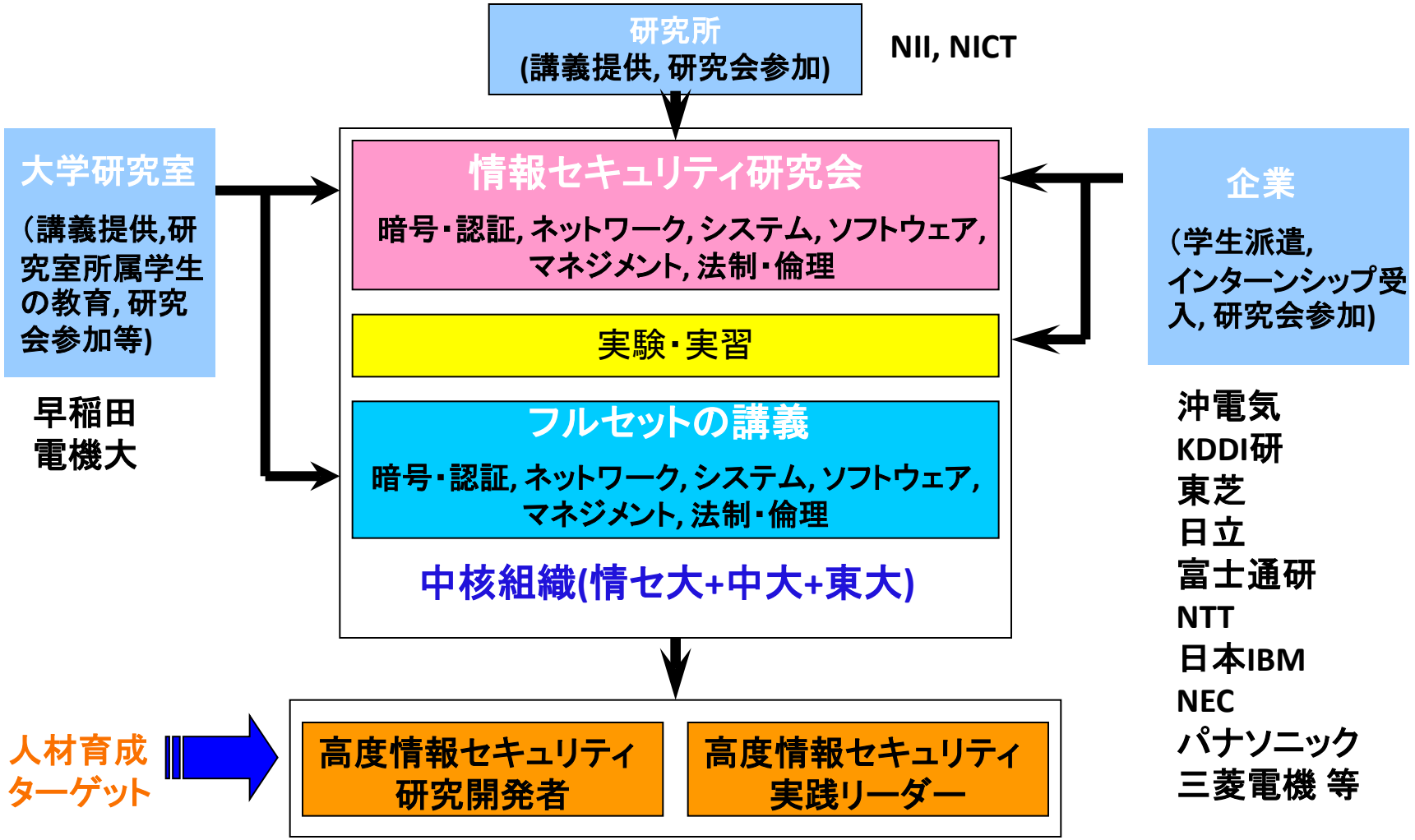
文部科学省平成19年度「先導的ITスペシャリスト育成推進プログラム」採択拠点

C. 研究と実務融合による
高度情報セキュリティ人材育成プログラム

Integrated Special Scheme for Information Security Specialist cultivation

情報セキュリティ大学院大学
プログラム代表　田中　英彦

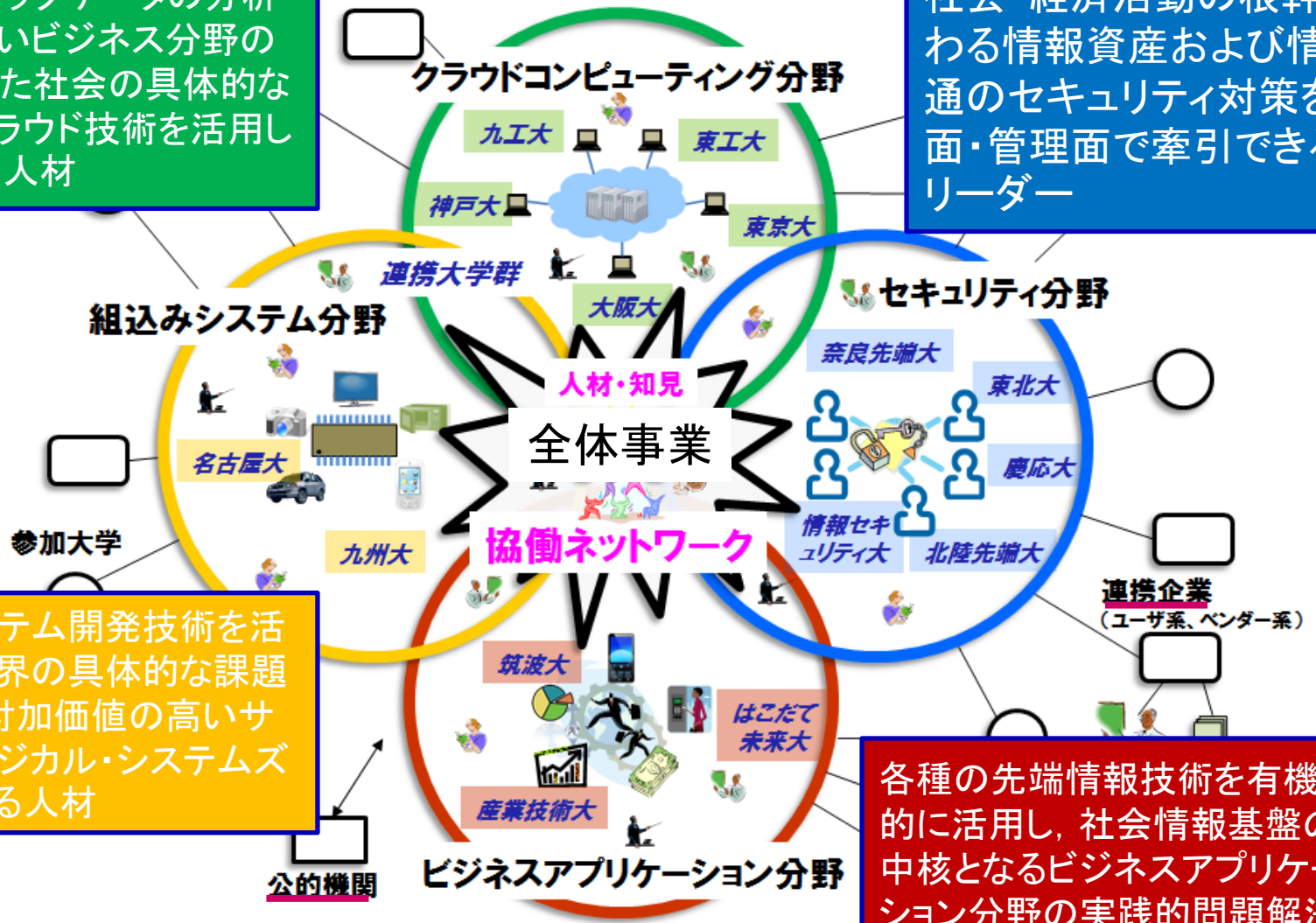
プログラムの全体構造


研究所
(講義提供, 研究会参加)
NII, NICT
大学研究室
(講義提供,研究室所属学生の教育, 研究会参加等)
早稲田
電機大
情報セキュリティ研究会
暗号・認証, ネットワーク, システム, ソフトウェア, マネジメント, 法制・倫理
実験・実習
フルセットの講義
暗号・認証, ネットワーク, システム, ソフトウェア, マネジメント, 法制・倫理
中核組織(情セ大+中大+東大)
企業
(学生派遣, インターンシップ受入, 研究会参加)
沖電気
KDDI研
東芝
日立
富士通研
NTT
日本IBM
NEC
パナソニック
三菱電機 等
人材育成
ターゲット
高度情報セキュリティ研究開発者
高度情報セキュリティ実践リーダー

文科省 「情報技術人材育成のための実践教育ネットワーク形成事業」

いわゆるビッグデータの分析手法，新しいビジネス分野の創出といった社会の具体的な課題を，クラウド技術を活用し解決できる人材

社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を，技術面・管理面で牽引できる実践リーダー



組込みシステム開発技術を活用して産業界の具体的な課題を解決し，付加価値の高いサイバー・フィジカル・システムズを構築できる人材

各種の先端情報技術を有機的に活用し，社会情報基盤の中核となるビジネスアプリケーション分野の実践的問題解決ができる人材

SecCapコースのカリキュラム

共通科目: 情報セキュリティ運用リテラシー Ⅰ Ⅱ

基礎科目: 所属大学指定科目

先進科目

理論系	•最新情報セキュリティ理論と応用
技術系	•情報セキュリティ技術特論 •先進ネットワークセキュリティ技術
社会科学系	•セキュア社会基盤論 •情報セキュリティ法務経営論

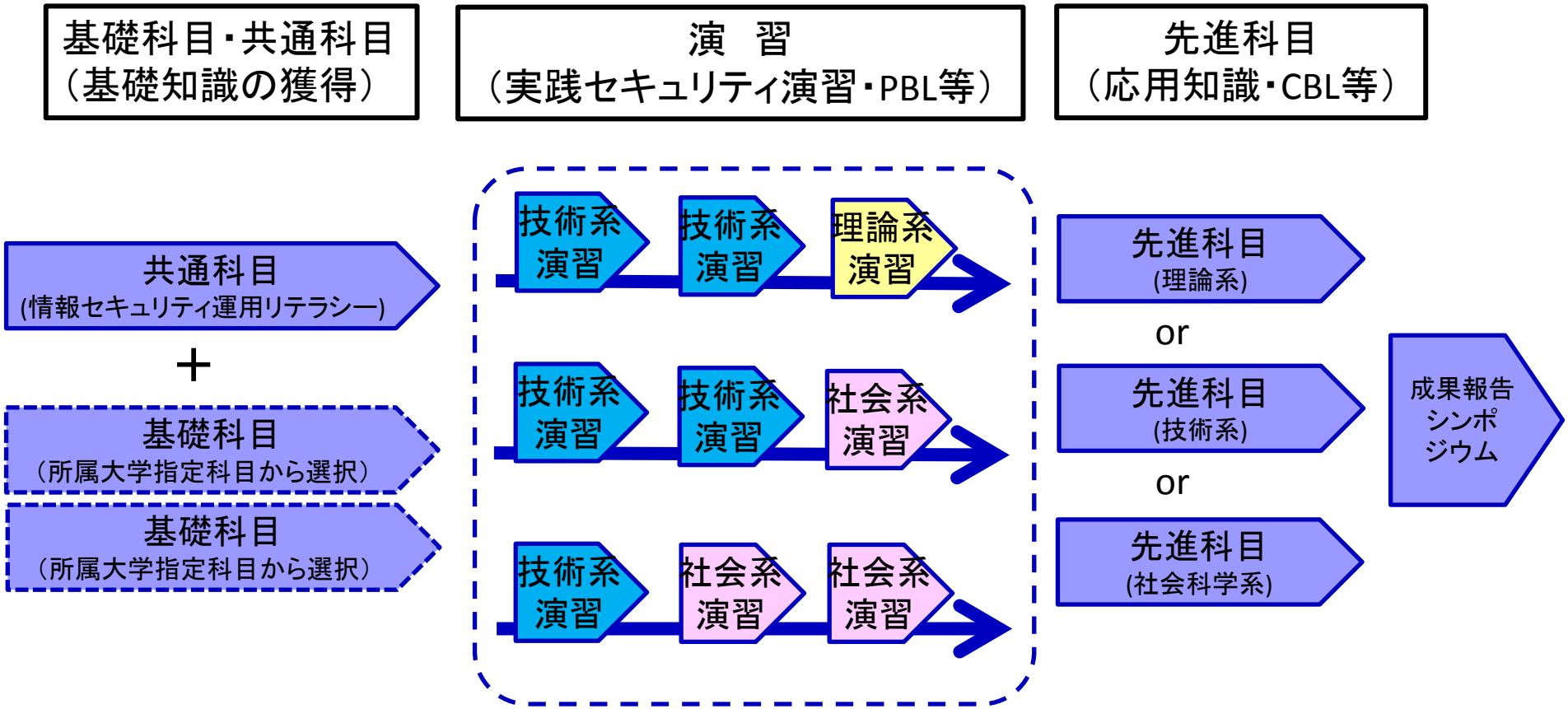
その他の活動

- セキュリティ分野シンポジウム
- 企業インターンシップ
- 交流ワークショップ

演習

理論系	•情報セキュリティ演習
技術系	•セキュリティ技術基礎演習 •ネットワークセキュリティ検査演習 •Webアプリケーションセキュリティ検査演習 •デジタルフォレンジック演習 •CTF演習 •無線LANセキュリティ演習 •システム攻撃、防御演習 •リスクマネジメント演習 •インシデント体験演習 •IT危機管理演習 •ネットワークセキュリティ実践 •ハードウェアセキュリティ演習
社会科学系	•セキュリティマネジメント演習 •インシデント対応マネジメント演習 •事業継続マネジメント演習

SecCapコースの実践演習の選択



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

PBL：Project Based Learning
CBL：Case-Based Learning

クラウドにおける
情報セキュリティリスク

1. ガバナンスの喪失
2. ロックイン
3. 隔離の失敗
4. コンプライアンスに関するリスク: チェックは可能か
5. 管理用インタフェースの悪用
6. データ保護
7. セキュリティ確保が不完全なデータ削除 : 機密性
8. 悪意ある内部関係者の存在
9. 司法権の違いから生ずるリスク
10. ネットワークの途絶や混乱

ENISA, 2009

表 1: 情報収集の脅威と対策

脅威	対策
ペイロード分析	暗号化 各アプリケーションの設定
ヘッダ分析	各端末の設定 Protocol Scrubber, Anti OS Fingerprinting System
挙動分析	IPsec (Traffic Flow Confidentiality Padding) Behavior Shaver

法　制

- 日本国憲法、刑法、他
  - -会社法、IT基本法、e文書法、電子署名法、著作権法、不正アクセス禁止法、電気通信事業法、電波法、プロバイダ責任制限法、携帯電話不正利用防止法
- 個人情報保護関連5法（2005年4月1日等）
- 金融商品取引法（2007年9月30日施行）
  - -財務報告の信頼性確保のための内部統制報告書の作成・提出等
- 特定商取引に関する法律：2008年改正
- 特定電子メールの送信の適正化等に関する法律：2008年12月1日施行
  - – OPT-OUT→OPTT-IN, 100万円→3000万円