情報共有に向けた情報セキュリティのあり方

2013年7月25日

情報セキュリティ大学院大学
田中英彦

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

最近の情報セキュリティ問題1

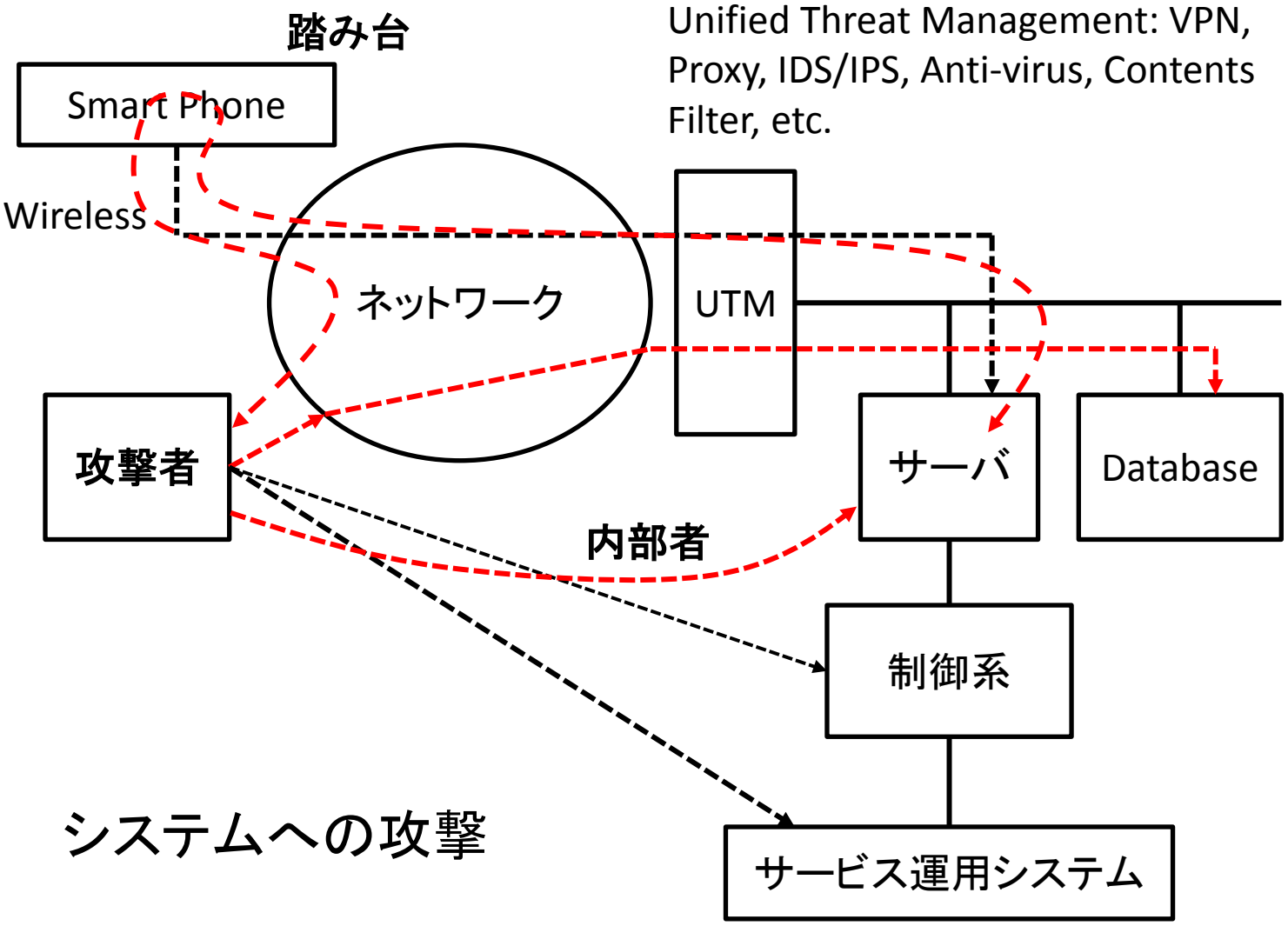
- 情報収集
  - Operation Aurora(2009): 米国企業知財流出（Google, Adobe, RSA他）
  - GhostNet(2009)　世界規模スパイネット
- 重要インフラ攻撃
  - Stuxnet(2010.9発生, 2012.6発表NY Times US+Israel), Saudi Aramco(2012.8)
  - 米電力会社発電施設マルウエア感染（2012末、USB)
- Wikileaks
  - 米国外交機密文書25万点全公開(2010.11より2011.9)
- 政府
  - 警視庁公安部外事第三課国際テロ情報の流出(2010.10), 海上保安庁画像流出(2010.11), 国会議員のIDとパスワード漏洩(2011.8)
  - 警察庁誤認逮捕(2012.6-9), 農林水産省機密漏洩(2013.5)

最近の情報セキュリティ問題2

- 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

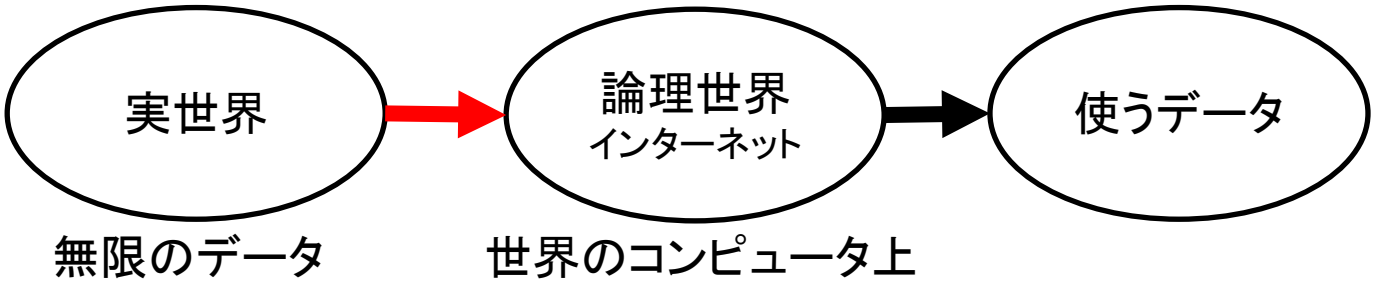
新しい事象と課題

- 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
内部者
制御系
サービス運用システム
システムへの攻撃

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



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。

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2013.6.10
    サイバー空間：強靭/活力/国際
  - 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
- 重要インフラ対策：統一基準
  - CSSC 経済省：制御システムセキュリティ
- JPCERT, SOC, NICT, IPA

対策に向けて

- リスクの認識
  - 盗聴・侵入・改竄・破壊・なりすまし、社会影響
- リスク対策
  - 経営方針、管理的対策、技術的対策
- 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
  - ネットレベル：UTM, Malware分析
  - ホスト・応用レベル：　ウイルス対策ソフト、脆弱性検査、Webプロキシ、SELinux
  - ファイルレベル：ユーザ認証、アクセス許可、ファイル暗号化
- 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
  - インシデント模擬訓練
- 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

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、UTM、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

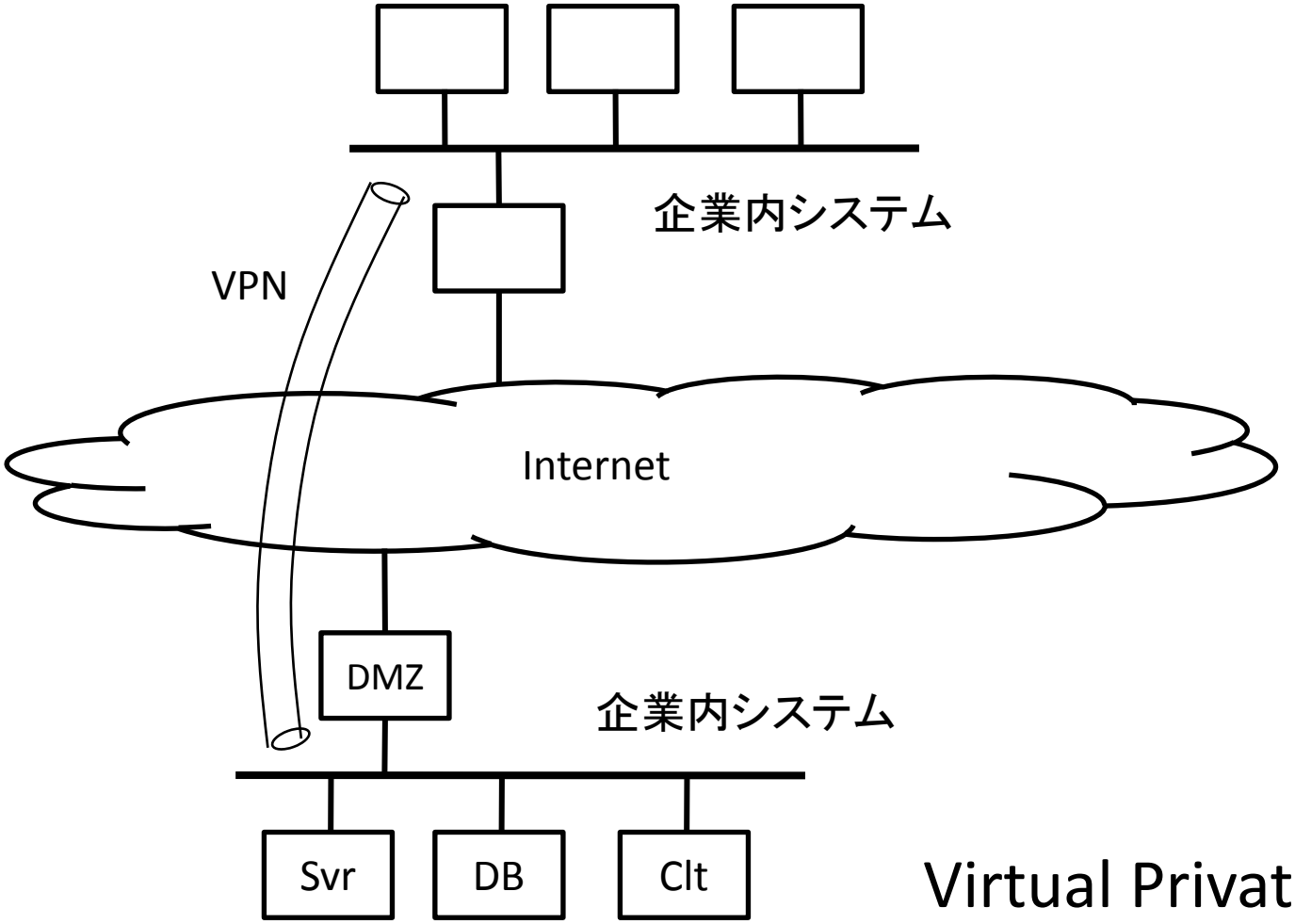
② システム技術
- セキュアOS、セキュアプログラミング、セキュア開発
- ログ、TPM、アクセス制御、thin client

③ 暗号と認証

④ モバイル対策

⑤ 組込製品対策

⑥ SNSの利用



Virtual Private Network

本人認証と暗号化

- ユーザ認証：例、ワンタイムパスワード
  - 時刻同期（タイムスタンプ）方式、トークン利用
  - チャレンジレスポンス方式：ランダム数値
- ファイル暗号化：例　MS EFS
  - ファイルを鍵で暗号化： AES256
  - 鍵をユーザ公開鍵で暗号化、更に退職や事故に備えて回復公開鍵による鍵の暗号化
  - NTFSファイルシステムのオプション機能

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

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、危殆化対策
- 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

モバイルマルウエアの対策

- 2013　年間614%増加(28万件悪意アプリ）
- BYOD：Bring Your Own Devices
  - 個人所有の端末を仕事で利用、端末のなりすまし問題
  - 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

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

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
- 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

- 情報の種類
  - 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	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

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、保険でリスク移転、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。リスク原因者特定不可能な場合
- 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
  - 活用：市場機能、法・制度、自律的規律、技術・標準

管理・運営

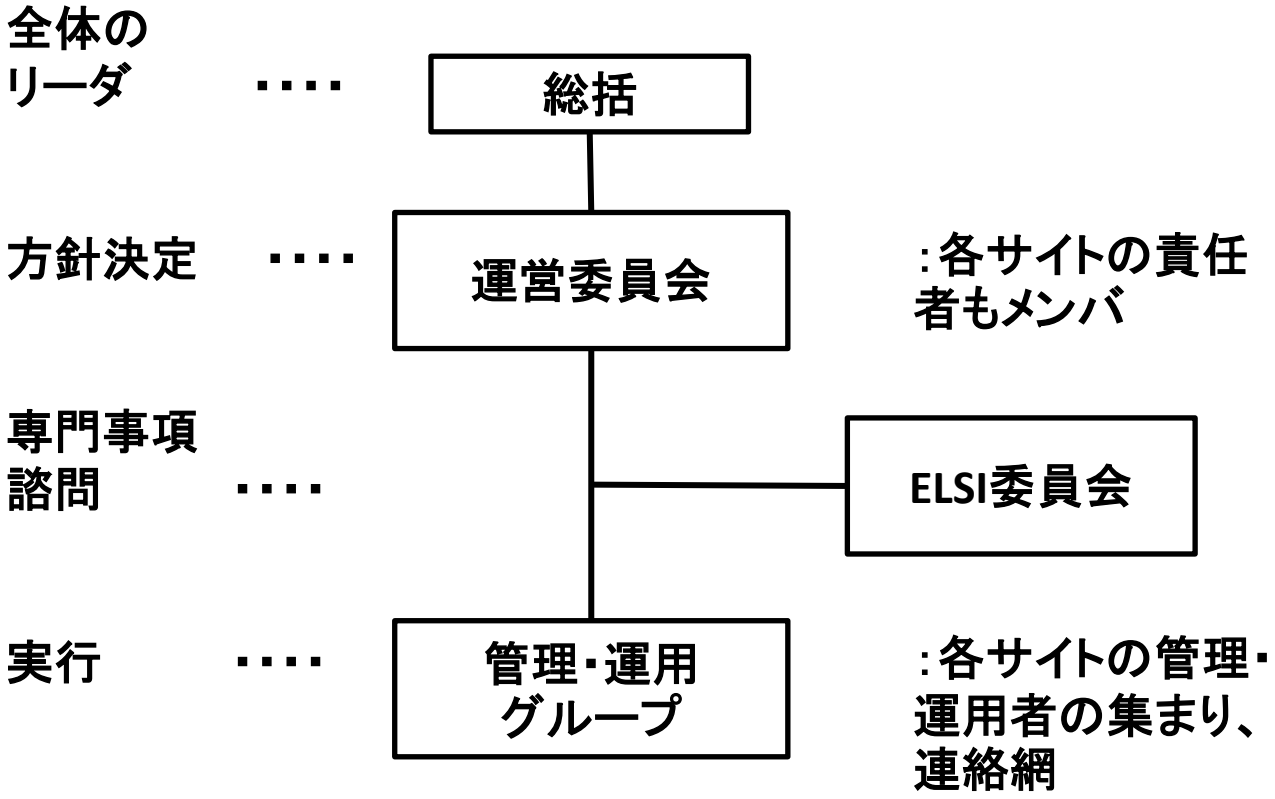
- 情報セキュリティ管理システム: 情報分類、リスク特定、評価、監査
- 情報セキュリティ予算(米)
  - 当初全IT予算の7-8% 落ち着くと3-5%、コンプライアンス対応で増加傾向
- 投資効果の評価基準
  - ROIで評価（米、日本では少）、直接売上に結びつかないが、信頼を高める企業価値生み出す効果あり
- 外部委託
  - 企業の40%は何らかの機能委託、全て委託は2%(米), ITリスクをコントロールできないと経営者責任を問われるので内部へ戻し続く
- 保険、企業の30%（米）が採用、8%(日本)
  - サイバーアタック保障保険、個人情報漏洩保険、IT事業者向け賠償保険、ネット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

5. 情報共有システム構築に向けて

- 必要な要素
  - 申し合わせ事項MOU: システム目的、関係者の定義、共有情報の定義、システム利用法、システム運用体制、管理体制、問題発生時対処法
  - システム設計書：機能設計、CIA（秘匿性/完全性/可用性)対応、標的型攻撃対応、外部インタフェース
  - システム利用マニュアル：情報投入、アクセス制御
  - システム運用マニュアル：連絡体制、障害対応、利用ログ取得と管理、証拠保全、問題提起と解決体制
  - システム管理マニュアル：責任体制、加入・退会

情報共有の意識合わせ

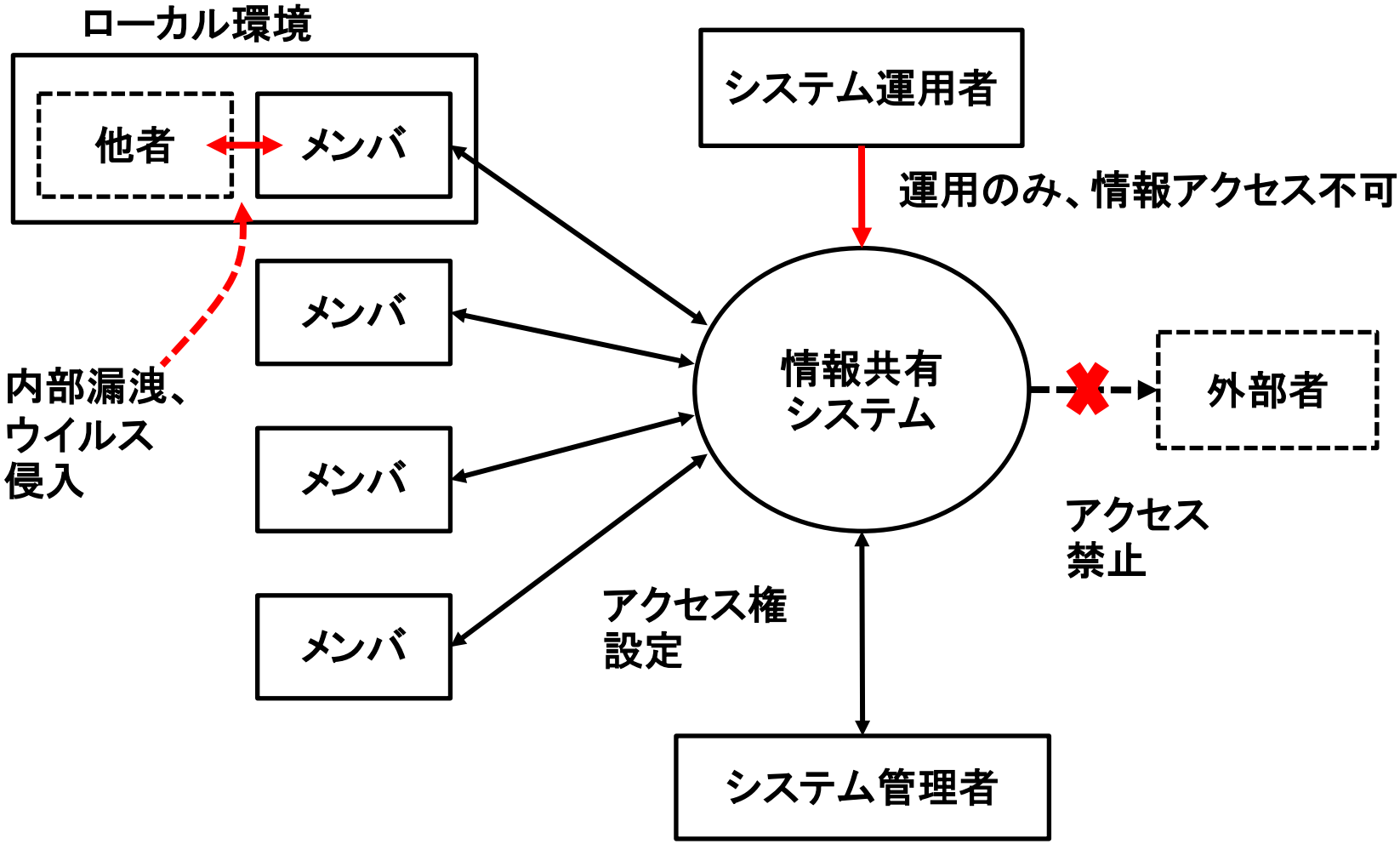
- 共有情報の提出
  - 作成者が提出決定権を持つ
  - 共有のメリットをMOUに明示：メリットパターン
  - 情報引き上げの考え方：コピー取れる状況では余り意味を持たないが、退会時に実行
  - 共有情報における患者データ等のプライバシ関係情報対応
- 共有情報の利用
  - 利用形態：読み/実行、書き/消去（権利者）
  - 利用後の成果発表への明示義務
  - アクセス権：個人毎の詳細アクセス権か全メンバ宛てのグローバルアクセス権か
  - 利用ログ取得：問題発生時の証拠、しっかりしたログ管理と保管、プライバシー対応



情報共有基盤運営組織図

信頼性・安全性対策

- 信頼性対策
  - システム障害、ネットワーク障害、自然災害想定
  - クラウドの利用時、業者への要求事項として災害対策、緊急モードの設定
  - 共有データはすべてローカルデータのコピーであることを前提とした利用
- 安全性
  - 情報漏洩対策（システム侵入対策、アクセス権、暗号化）、改竄対策（内容保証）
  - 処理結果を共有サイトに置くか否か



情報共有システムとそのステークホルダー

おわり

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ⅠⅡ

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

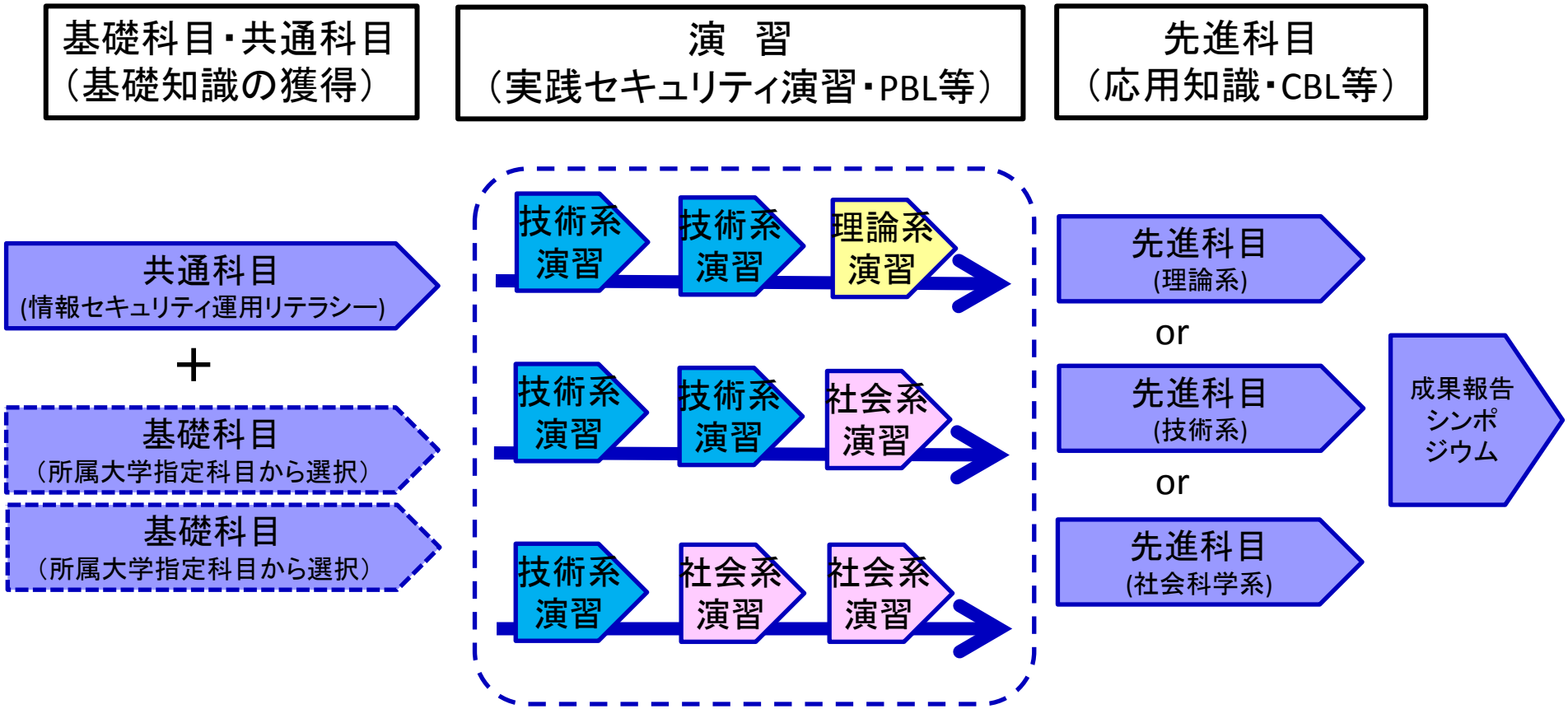
その他の活動

- 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

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