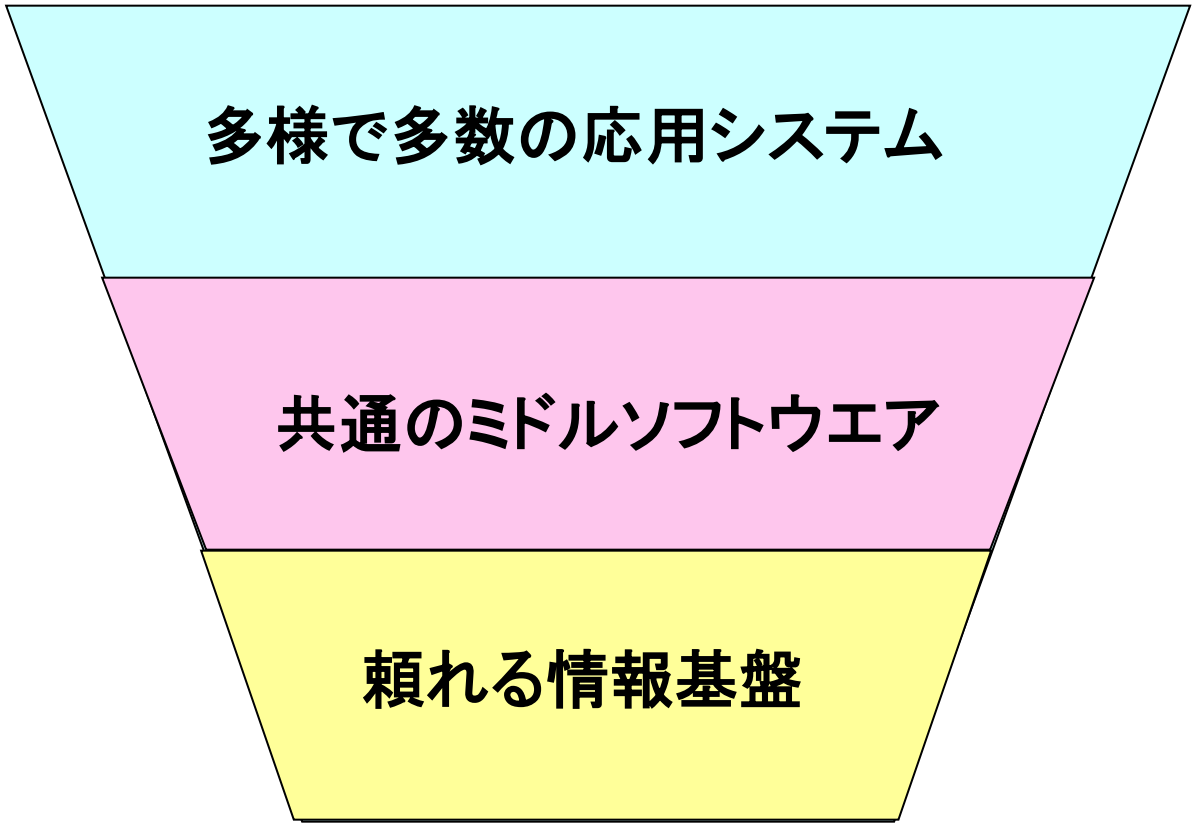
情報システムとセキュリティ

田中　英彦
情報セキュリティ大学院大学
2013年10月31日

目　次

1. 今後の情報システム
   - 生活基盤、経営と融合、組込、環境、CPS
2. 情報時代のセキュリティ
   - 最近の犯罪と動向、マルウエア
3. 情報セキュリティの対策
   - 技術、基本問題、モバイル、法制、リスク
4. 今後に向けて
   - 情報の役割、人材育成、期待

1.今後の 情報システム



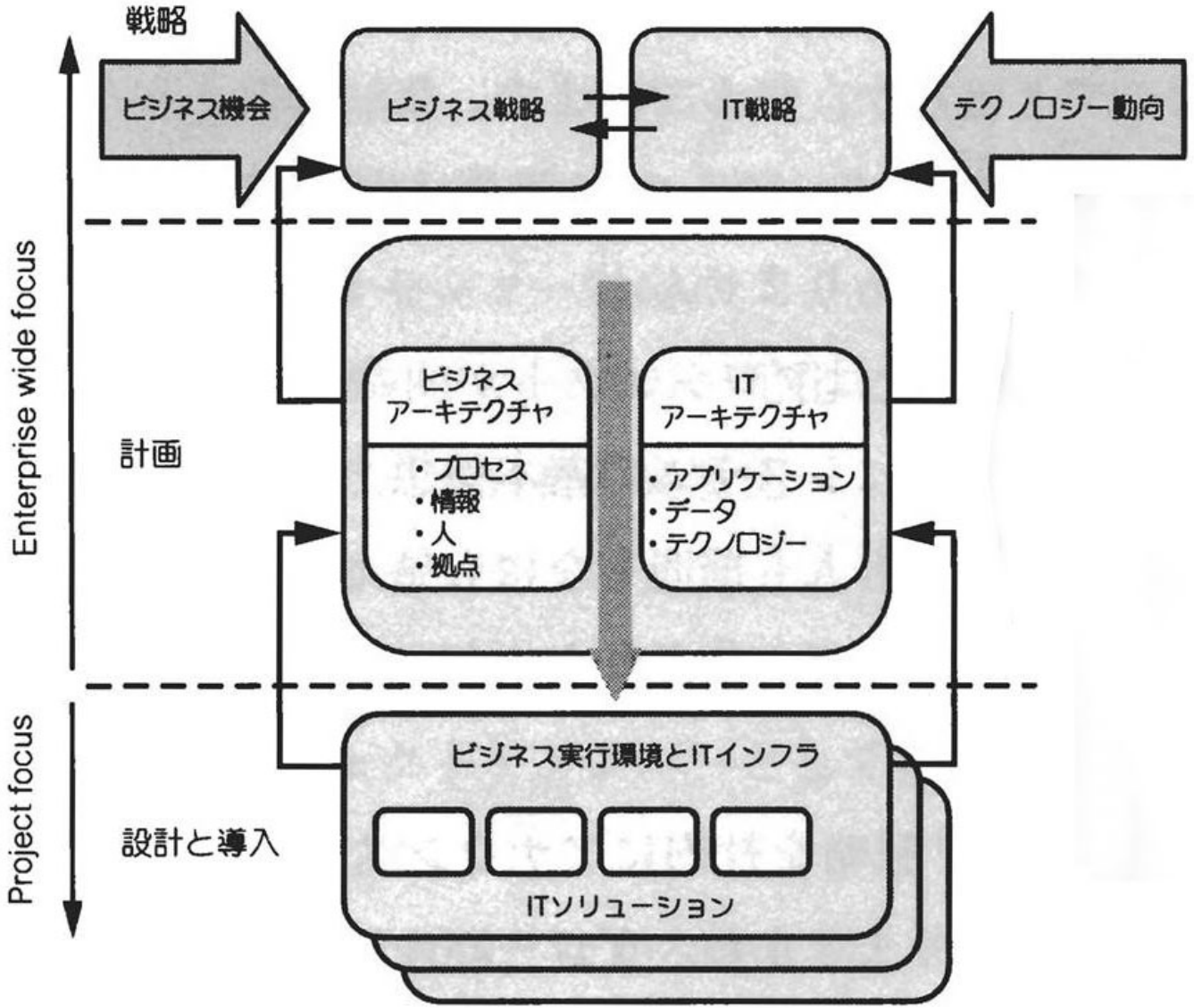
Amazon
Net-Banking
You-Tube

mail, Web
Business soft
XML

Server
Processor
OS
Internet

情報システムの3要素

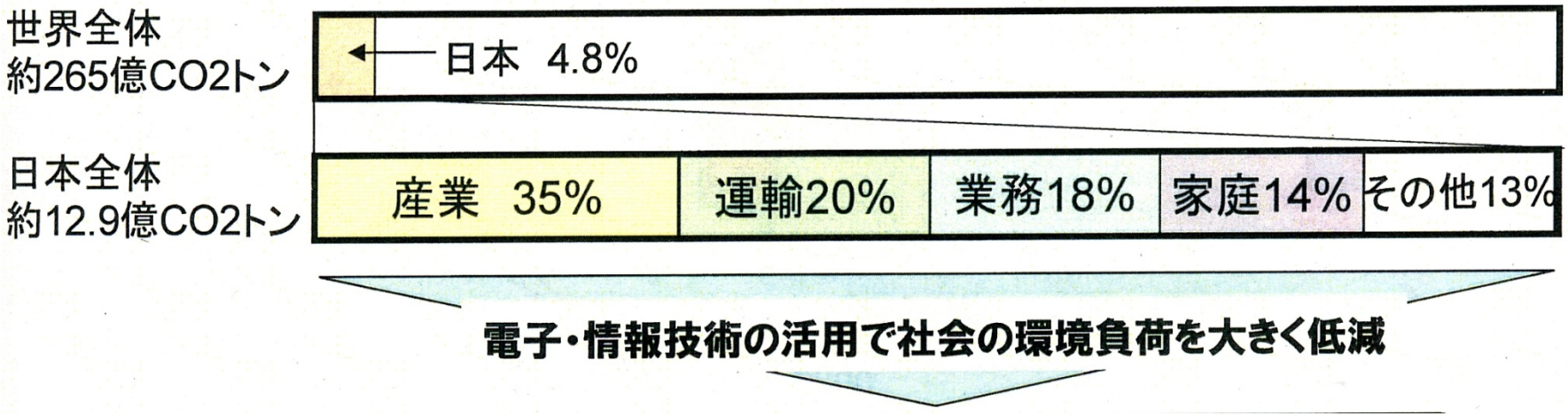
事業のニーズとITシステムの役割



組み込みシステムとソフトウエア開発費

- 携帯電話の組込ソフトウエア：500万行(1万人月）
- デジカメ：　300万行
- TV, DVD レコーダ：　100万行
- 自動車：　1000万行、電子部品コストは15%、
  40% 2015年
- カーナビ：　500万行
- 医療機器：　全研究開発費の60%
- 金融機関システム：　6500万行

ITの活用による環境負荷の低減

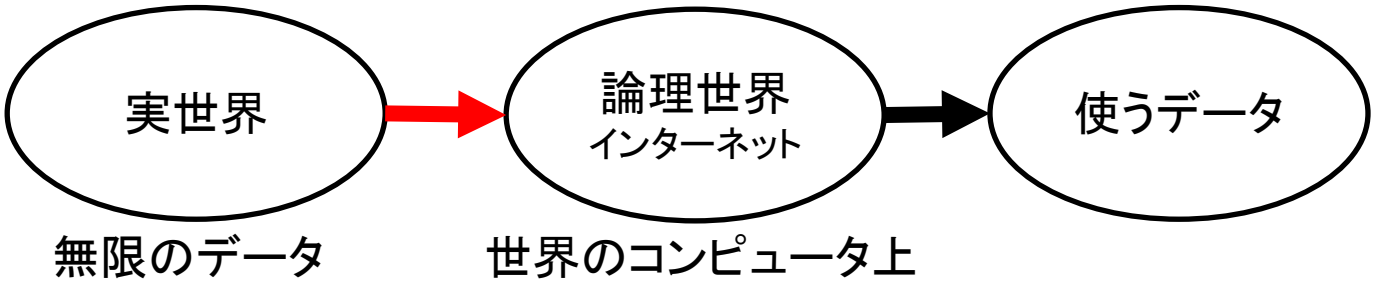


- 人・モノの移動を少なくする
- 生産・流通の効率化
- エネルギ利用効率の改善

IT普及で消費電力量拡大
2025年には、現在の
- 社会で扱う情報量200倍
- IT機器の消費電力　5倍
- 総発電量の20%

Cyber Physical System 時代

- 膨大なセンサーがインターネットに接続
  - 気象、スマートフォン、街角、コンビニ、ビル管理、家庭内機器、自動車、交通
  - 膨大実時間データ集積
- 膨大データ(Big Data)の解析
  - 快適な社会：現状把握、制御、予測



2. 情報時代のセキュリティ

- 道具の変化
  - 電話、手紙　→　インターネット、スマホ、クラウド
- 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→IP→政治信条・国家間
- 意識の変化
  - コピー、メール、ネット、無料、消えない

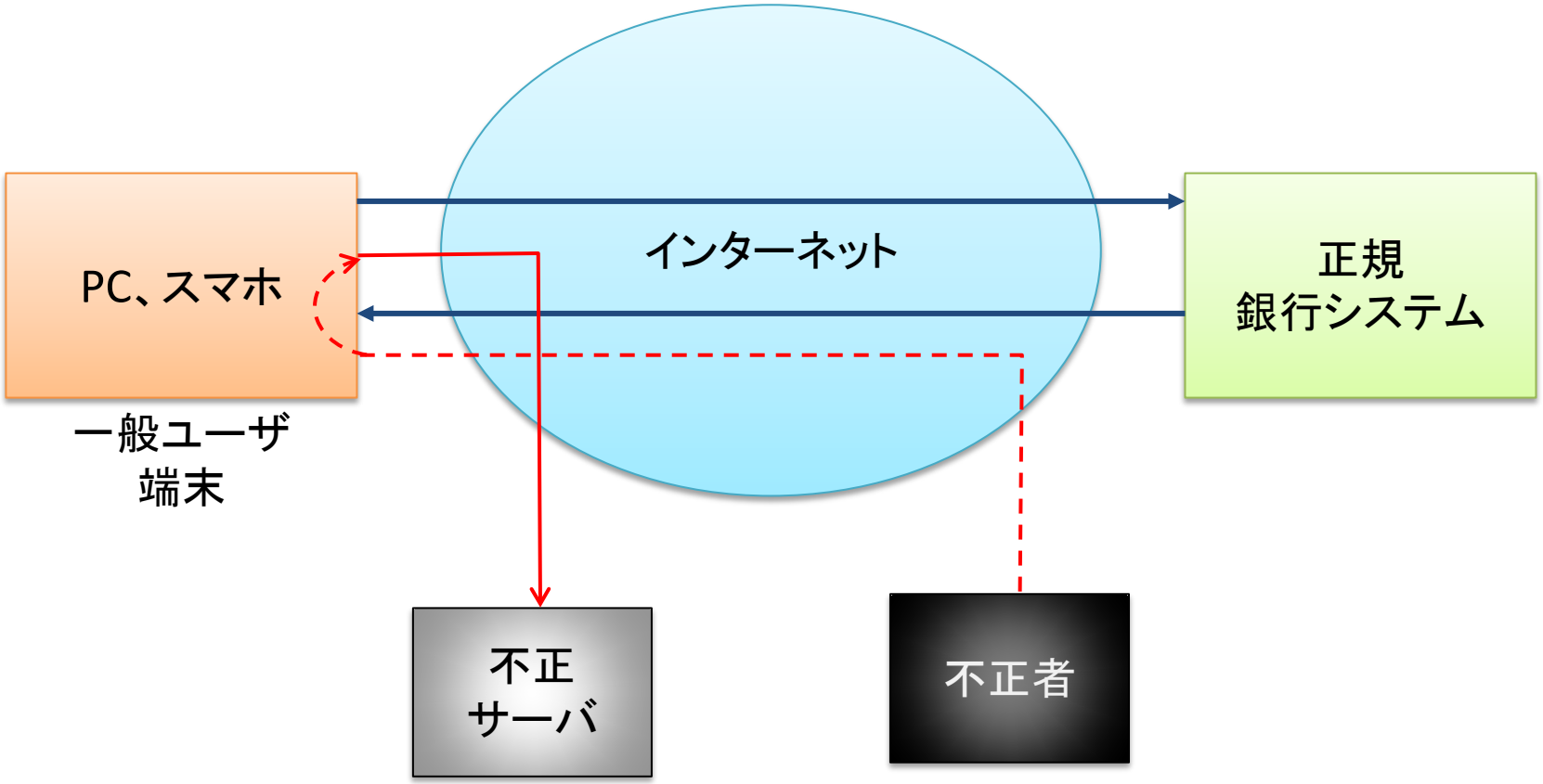
GRAND CHALLENGES FOR ENGINEERGING
-2008 National Academy of Sciences-

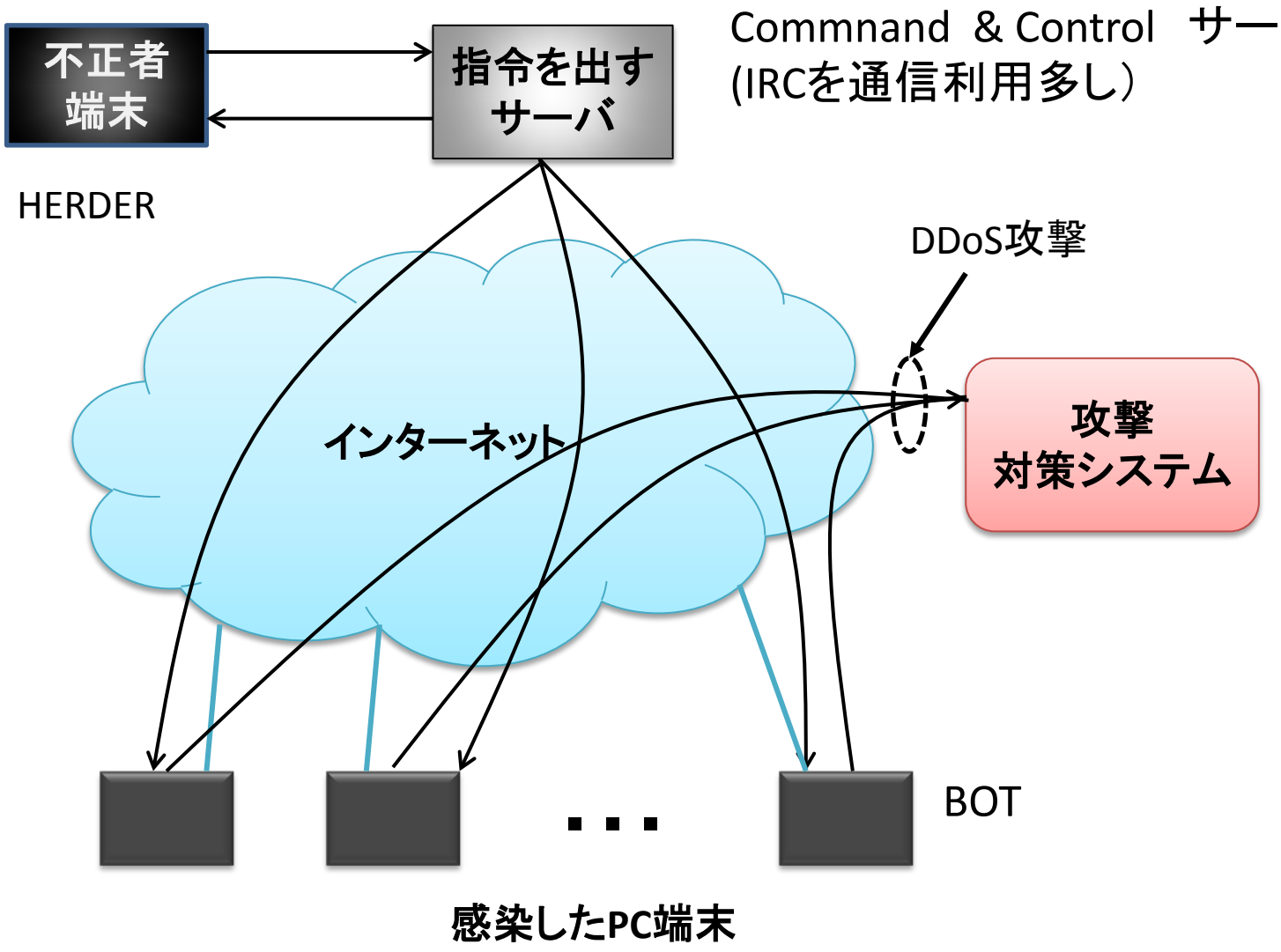
- Make solar energy economical 7
- Provide energy from fusion 10
- Develop carbon sequestration methods 13
- Manage the nitrogen cycle 16
- Provide access to clean water 19
- Restore and improve urban infrastructure 22
- Advance health informatics 25
- Engineer better medicines 30
- Reverse-engineer the brain 34
- Prevent nuclear terror 37
- Secure cyberspace 40
- Enhance virtual reality 42
- Advance personalized learning 45
- Engineer the tools of scientific discovery 48

最近の事件

- 情報収集　2009
  - Operation Aurora, GhostNet 世界規模スパイネット
- 重要インフラ攻撃 2010, 2012
  - Stuxnet, Saudi Aramco
- Wikileaks 2010-2011
  - 米国外交機密文書25万点全公開
- 日本政府 2010-2013
  - 海上保安庁,警視庁国際テロ情報,国会議員IDとパスワード、誤認逮捕, 農産省機密
- 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 2004-2013
  - AOL, Yahoo, KDDI, 米PSN, 米SonyOE, ロッキード、米シティ, Google, 三菱重工, IHI, YaHoo ID
- 国家間攻撃　2013 中国、米
  - 韓国　放送局・金融機関 2013.3.20

フィッシング（Phishing）
(DNSを書き換えるPharmingも)




不正者
端末
指令を出す
サーバ
Commnand & Control サーバ
(IRCを通信利用多し)
HERDER
DDoS攻撃
インターネット
攻撃
対策システム
BOT
感染したPC端末

新しい事象と課題

- サイバー攻撃増加：情報システムへ外部攻撃
  - 特定標的へ意図的組織的攻撃：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侵入(2010)
  - Advanced Persistent Threat：特定標的への持続的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発生
  - スマホ、情報家電、センサー機器：PCと同じ世界共通のOSやソフトが利用されており、影響範囲大

3. 情報セキュリティの対策

① ネットワーク技術
- 認証、マルウエア分析、FW、、IDS/IPS、プロキシ、VPN、無線
- 新世代ネットワーク：モビリティ及びセキュリティ対応

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

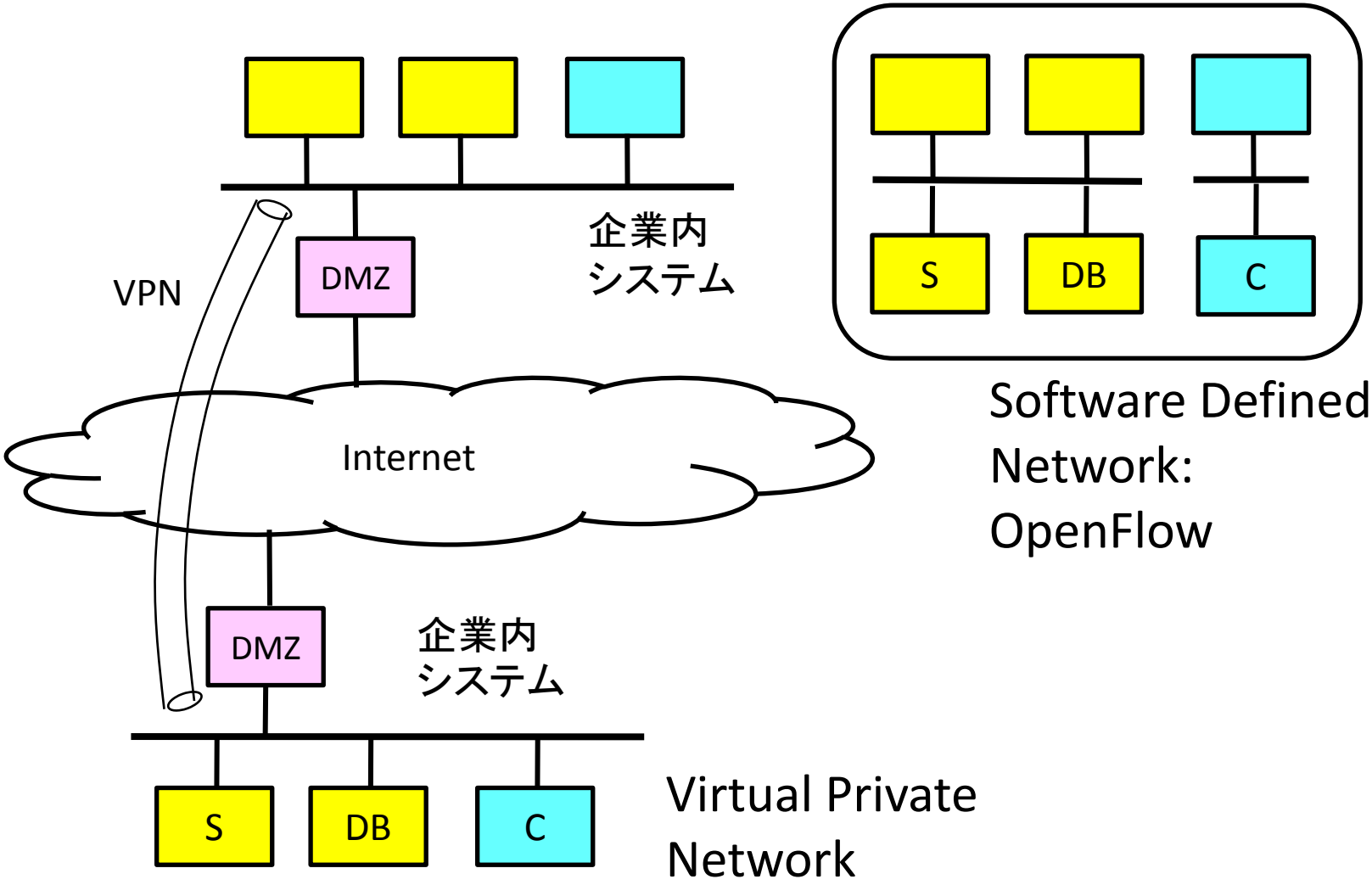
④ モバイル対策

⑤ 組込製品対策

⑥ SNSの利用対策

暗号の利用

- クラウドの利用増加
  - サーバコストの低減：管理コスト、高速度回線
  - 外部クラウドにも重要情報配置
- 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
  - 機密分散利用による確実化：障害用冗長配置
- 最近の暗号
  - 柔軟なアクセス条件設定、属性暗号

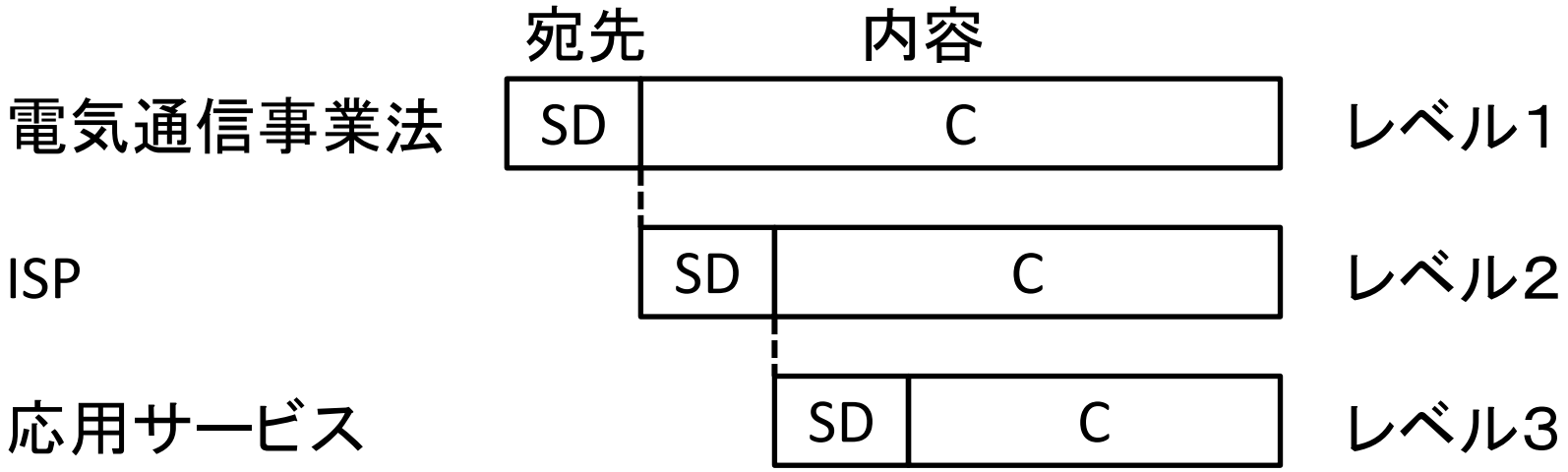

VPN
DMZ
企業内
システム
Internet
DMZ
企業内
システム
S
DB
C
Virtual Private
Network
S
DB
C
Software Defined
Network:
OpenFlow

情報共有における基本問題

- 情報収集における制約：収集は努力義務
  - 不正アクセス防止法、ログ取得、インシデント届出
  - 官の一般モニタリングは困難
- 信書の秘密からの制約：分析
  - アドレス情報のみ利用可能、内容利用禁止
- 個人情報保護範囲
  - 定義：個人の属性に関するすべての情報、暗号化等しておいても不可
- ビッグデータからの脅威問題
  - リンクで個人特定可能

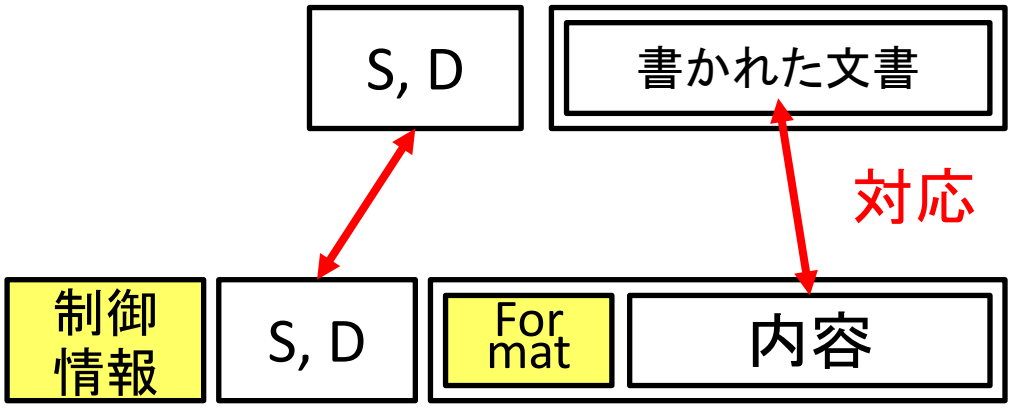
信書問題

- 従来：信書の秘密、SD+C の内SDはログ有
- 今後：通信の新たな枠組み、レベル構造



「信書の秘密」の情報時代に向けた再検討

手紙



メール

コピー
容易

新情報　　新情報　　:新判断要す

サイズ　　形式、サイズ

中継情報　　S’, D’

(wordなのに実行ファイル挿入)

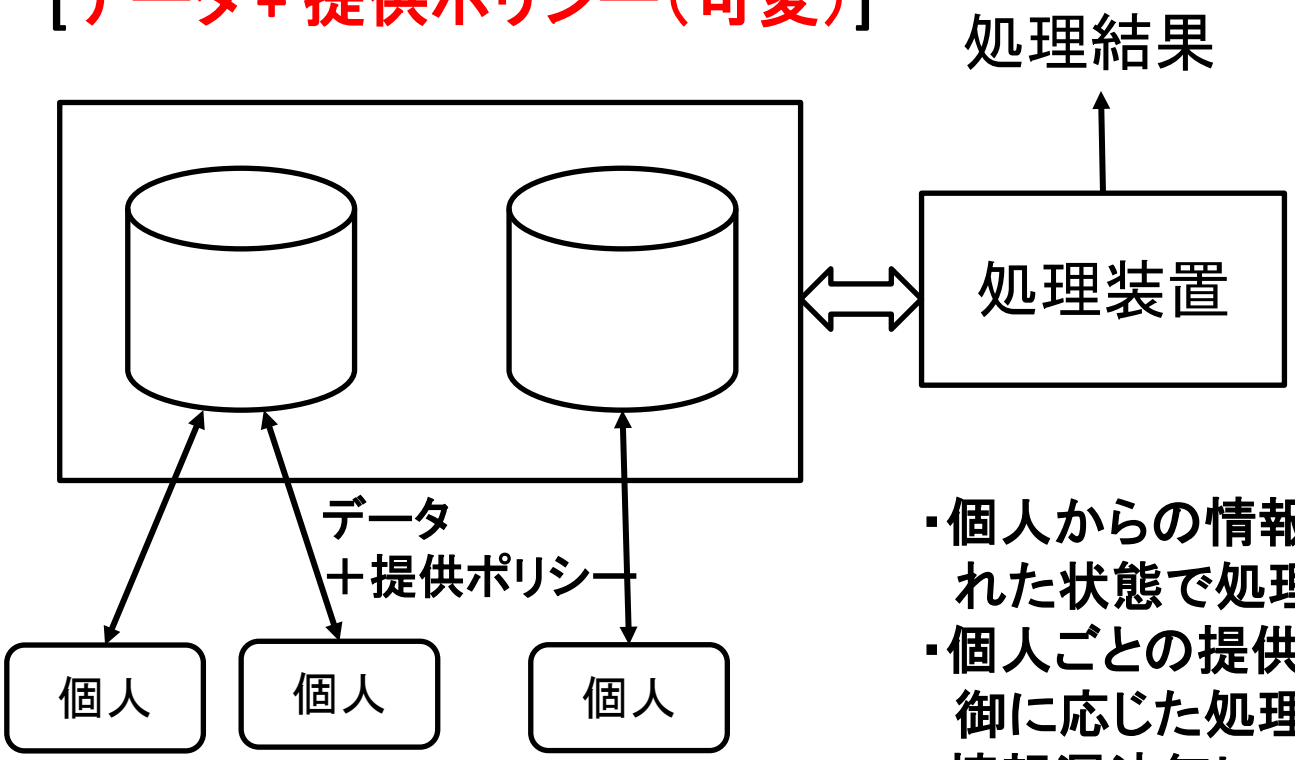
利用のメリット:追跡に有用　マルウエア判断に有用

内容とは無関係な犯罪情報(実行ファイル添付)

暗号化等秘匿化技術の考慮

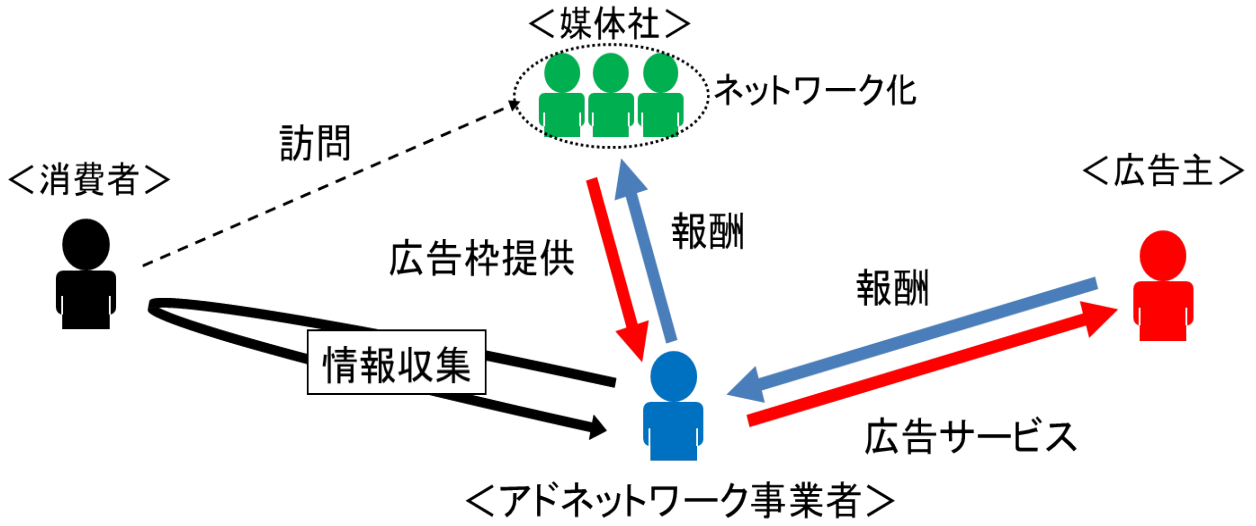
- 現状
  - 秘匿化されたものでも、他者に渉ると漏洩
- 変更の提言　cf. JNSA事故対応WG
  - 暗号等による高度な秘匿化と運用があれば情報漏洩事故とみなさない
- メリット
  - USB等による情報持ち出し可、通信による機微情報の送受が可能、活動が活性化
  - 無意味な情報漏洩事故が減り、実際的な管理対応が可

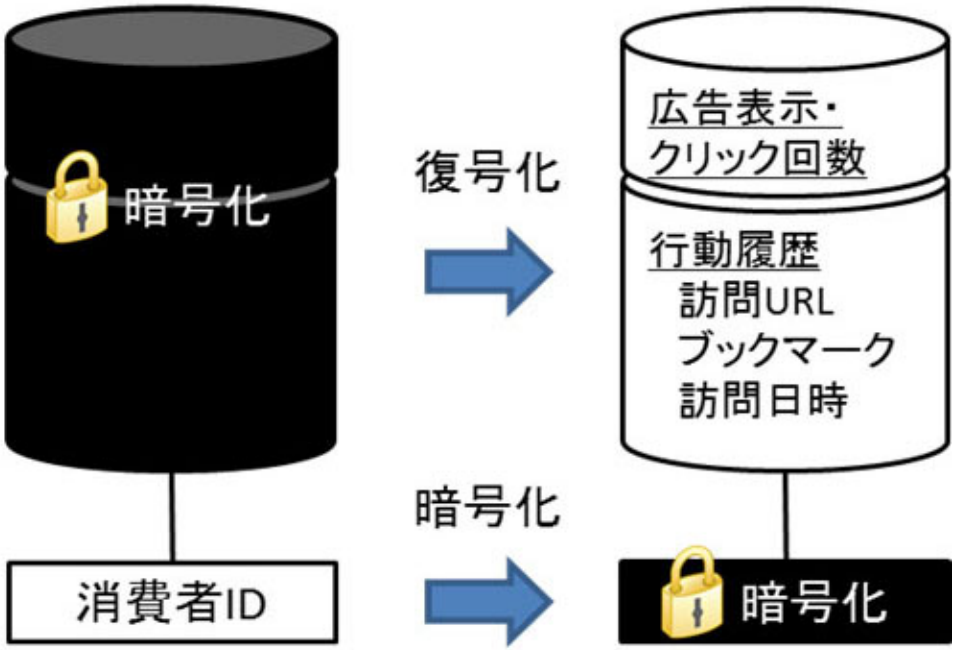
暗号化DBの集合:完全準同型暗号
[データ＋提供ポリシー（可変）]



- 個人からの情報を暗号化された状態で処理可能
- 個人ごとの提供ポリシー制御に応じた処理可能
- 情報漏洩無し
- 突合せ問題は、利用目的による制限で対応可能

解析性と制御性の両立

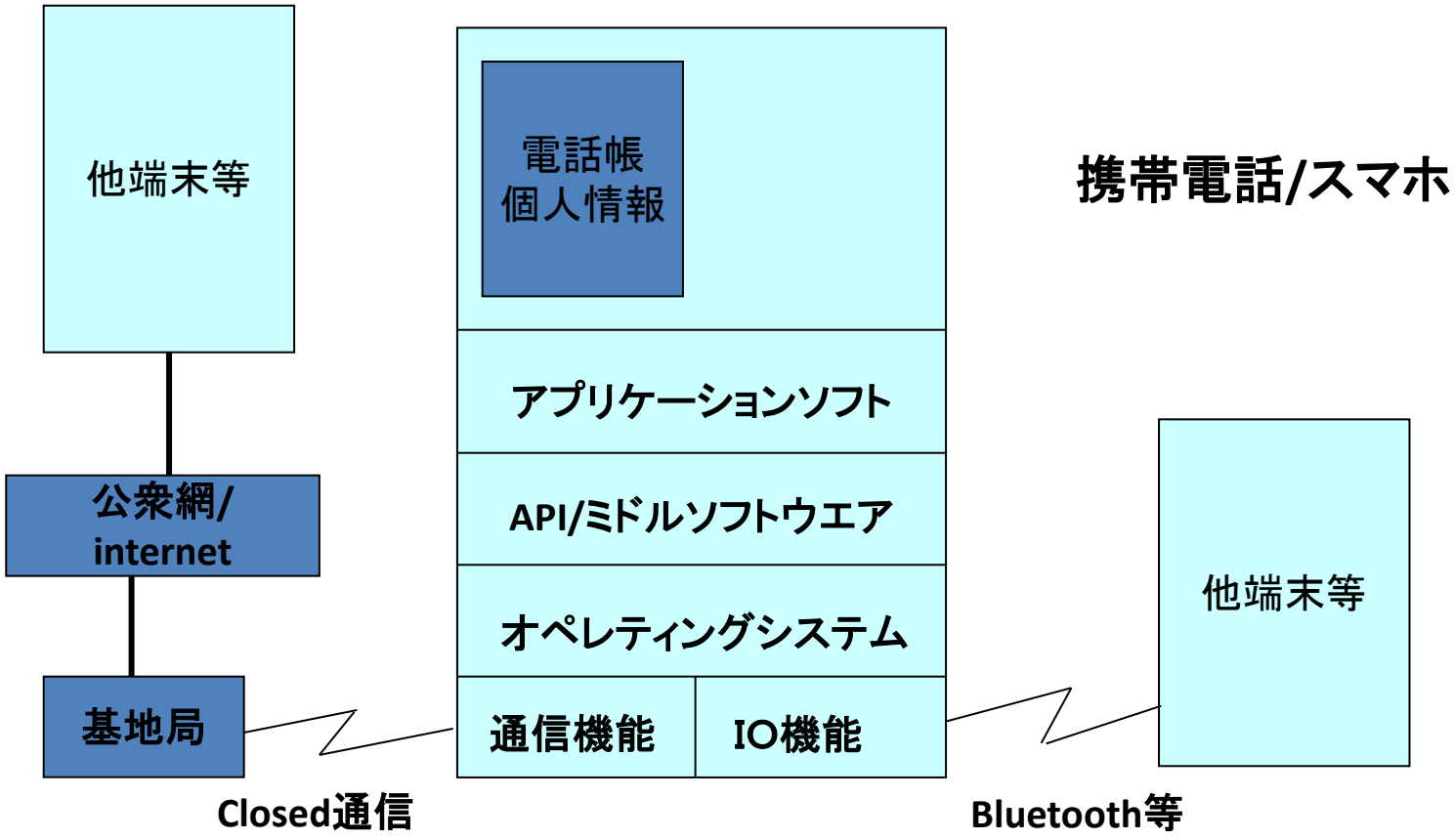




西村 俊介, 田中 英彦: “行動ターゲティング広告におけるプライバシー保護の実現方式の検討”, 第10情報科学技術フォーラム2011.

IDと内容の
関連性秘匿可能

携帯電話/スマホのセキュリティ



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%)
  - スマホ対策ソフト、iOS 255件、Android 110件 /2012年
  - FakeInst(コンテンツ利用課金の詐欺)が62%
- BYOD：Bring Your Own Device
  - 個人所有の端末を仕事でも利用、リスク；なりすまし
- 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

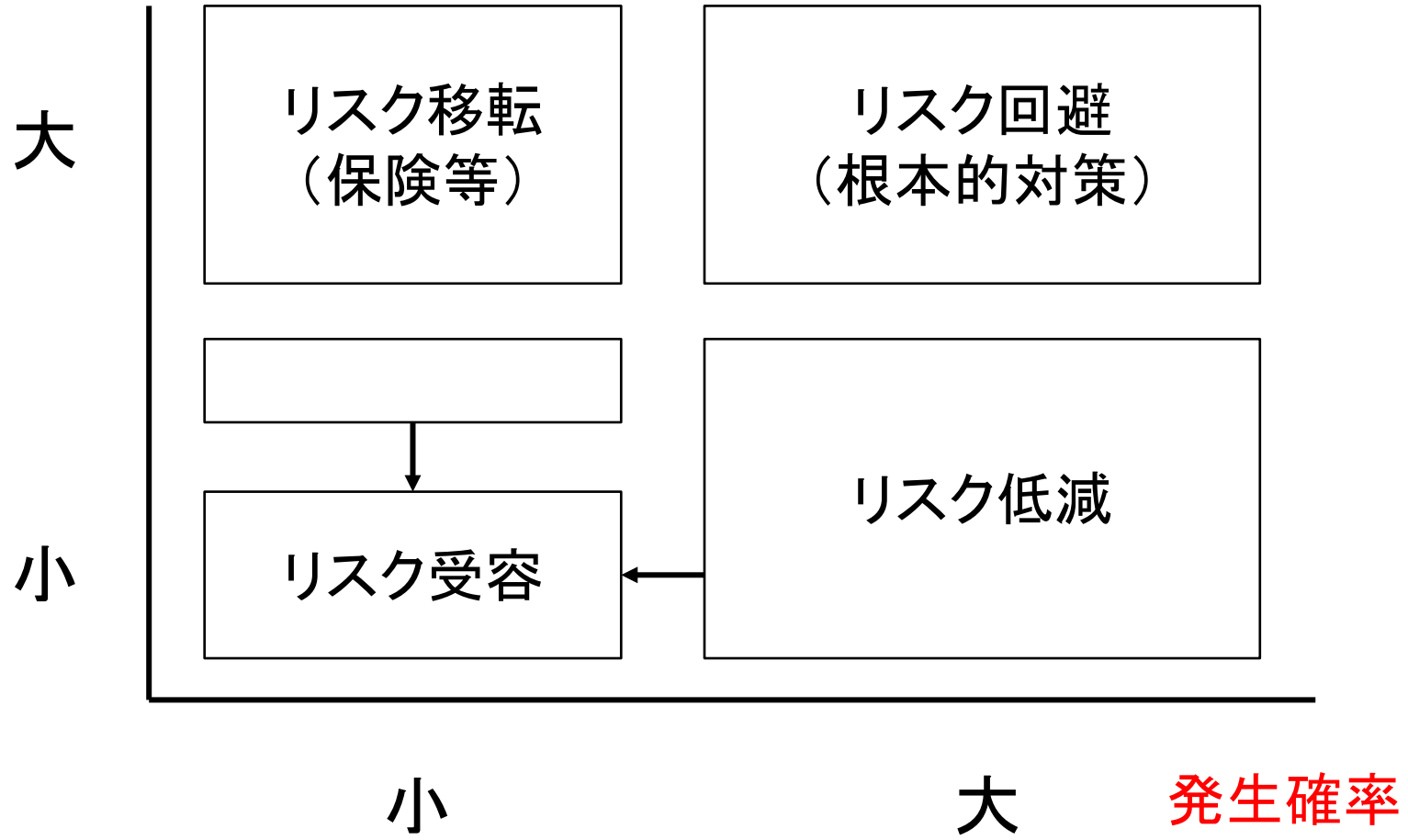
情報の特殊性と法制

- 情報技術の特殊性
  - 距離を超え、コピーが容易、サイズ、汎用機器
  - ソフトウエア：バグ、製造物責任法適用対象外
- 諸問題
  - 電気通信事業法、信書のガイドライン
  - 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)
  - 海外クラウド対応は税制とDB規制
- 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

リスクと情報セキュリティ

- リスク
  - 人的損失、財産損失、責任、投機、戦略、無形
- 情報の位置
  - 公開し宣伝するべき情報vs秘密にしておくべき情報
  - この情報種別判断　＝　経営判断
  - これに基づく作業：　情報セキュリティ対応・管理
  - 企業の強みを護り、チャンスを作り行動、リスクテーク
  - リスク対象の多くが「情報」

リスクマネージメント　JIS Q 2001



ソーシャルメディア

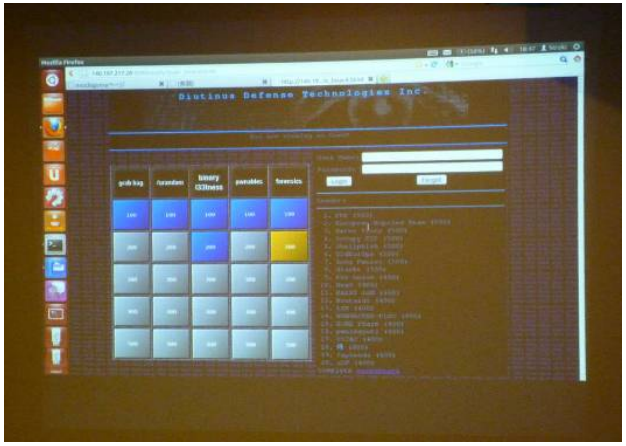
- Social Mediaの発達「公共財 SNS」
  - 人の繋がりの新たな構築：物理距離より、興味の距離、新たなリアル、興味の発信と共有
  - 新たな個人の出番（Netで発言）
  - 新たな知能：世界の知恵を借りる集合知
- 問題点
  - 社会悪の誘発、デマ、トラブル例：不用意なアルバイト発言、ソーシャルハラスメント、SNS疲れ
  - 機密保持と継続性、情報保存と廃棄
- 適切利用とリテラシー
  - 常識の醸成、使い分け(Twitter/Facebook/Line)

4. 今後に向けて

- 社会科学と情報科学の連携
- 社会における情報の役割とサポート
  - あらゆる活動のベース
  - それを支える情報技術：便利、信頼性
  - それを生かす情報セキュリティ対策：安全性
- 情報セキュリティの人材育成
  - 情報セキュリティ総合教育: IISEC
  - 実習活動：enPiT

情報セキュリティの高度人材の育成

- 約60%がセキュリティエキスパートを目指す現職の社会人
  （横浜駅　徒歩1分）
- 将来のCIOを育成する実務指向教育プログラム（ISS Square）

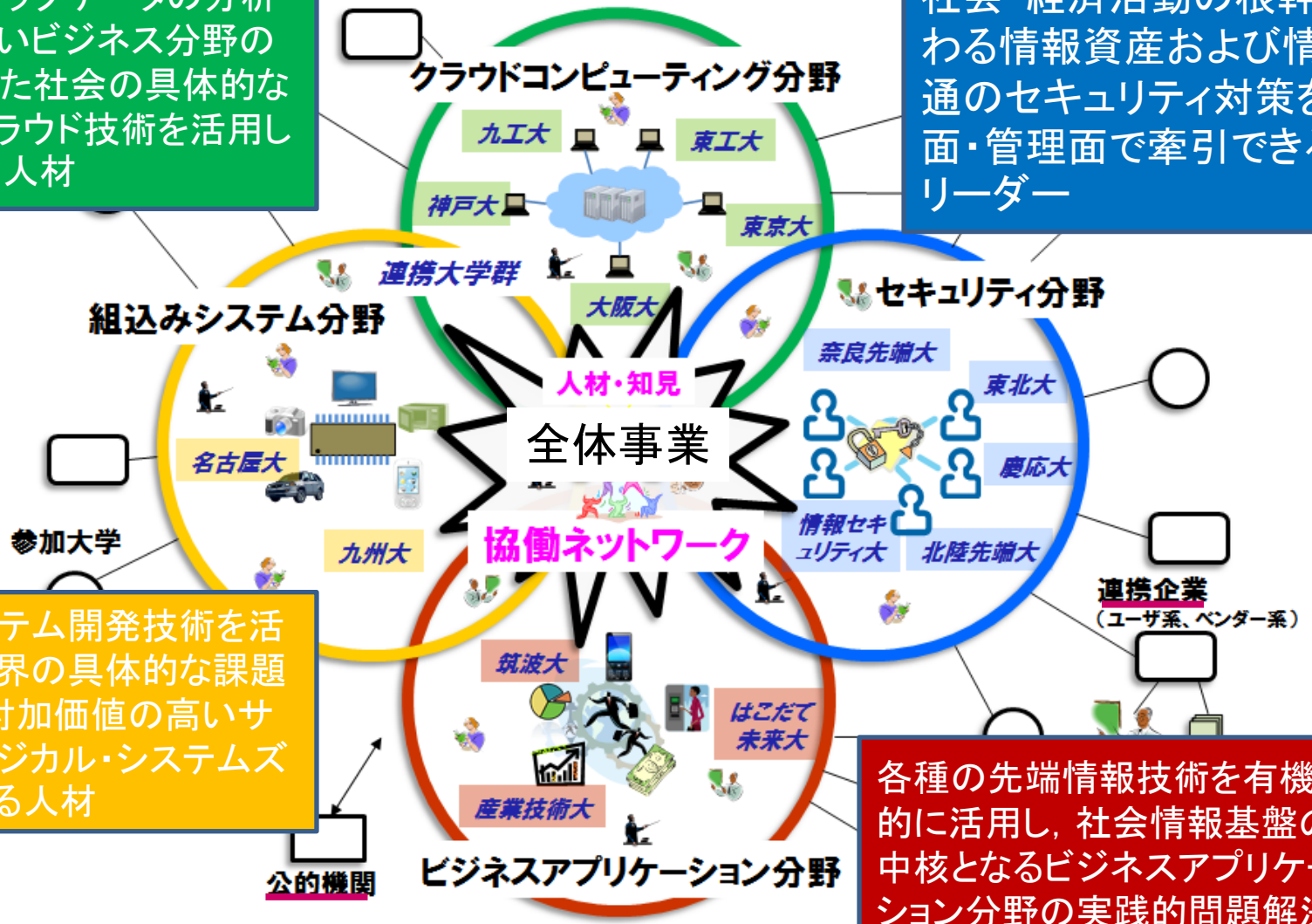


セキュリティコンテストDEFCON CTF（予選）参加スナップ

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

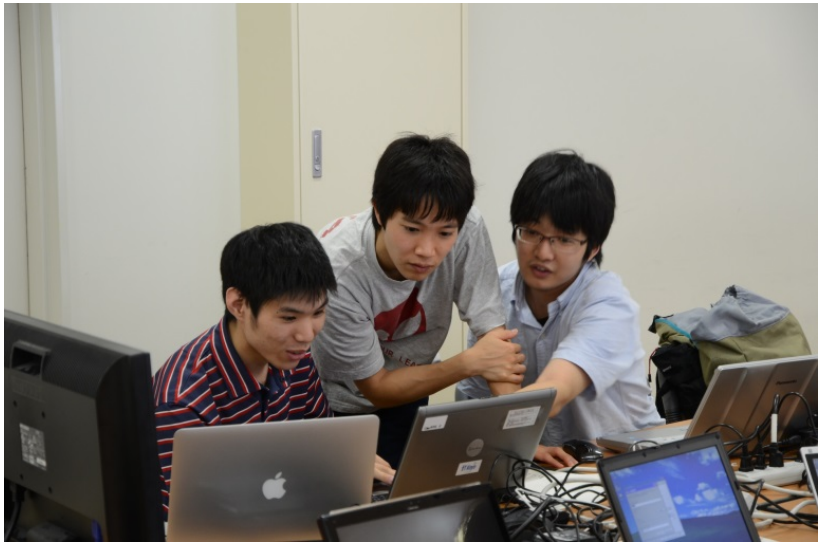
各種の先端情報技術を有機的に活用し，社会情報基盤の中核となるビジネスアプリケーション分野の実践的問題解決ができる人材

2013年度スケジュール

- 4月：SecCapコース講義開始

◆参加登録学生：90名

[連携大学] 情セ大：23名、東北大：13名
JAIST:6名、NAIST:5名、慶應大：21名
[参加大学] 東大：11名、中大：1名、
阪大：5名、 京大：5名



- 夏季：SecCap実践演習の実施
- 2014年1月30日(木)：enPiT全体シンポジウム＠横浜（日吉）
- 2014年3月4日(火)：セキュリティ分野シンポジウム及び修了生へのSecCap授与式

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

おわりに

- 未来は情報を生かす社会
  - それを実現するのは、皆様方
  - 情報分野は若い人々が力を発揮できる分野、のめり込む魅力、ハッカーの分野
  - 是非のめり込んで魅力発見を！
- 期待
  - 学術連携協定締結。情報＋セキュリティ連携
  - 皆様と、明るく信頼できる未来を創ろう
  - セキュリティは面白い。大学院の進学先活用人材需要大
  - 今後の皆様のご活躍に期待