繋がる世界における サイバーセキュリティ問題 とそれへの対応

2016年2月15日

田中　英彦

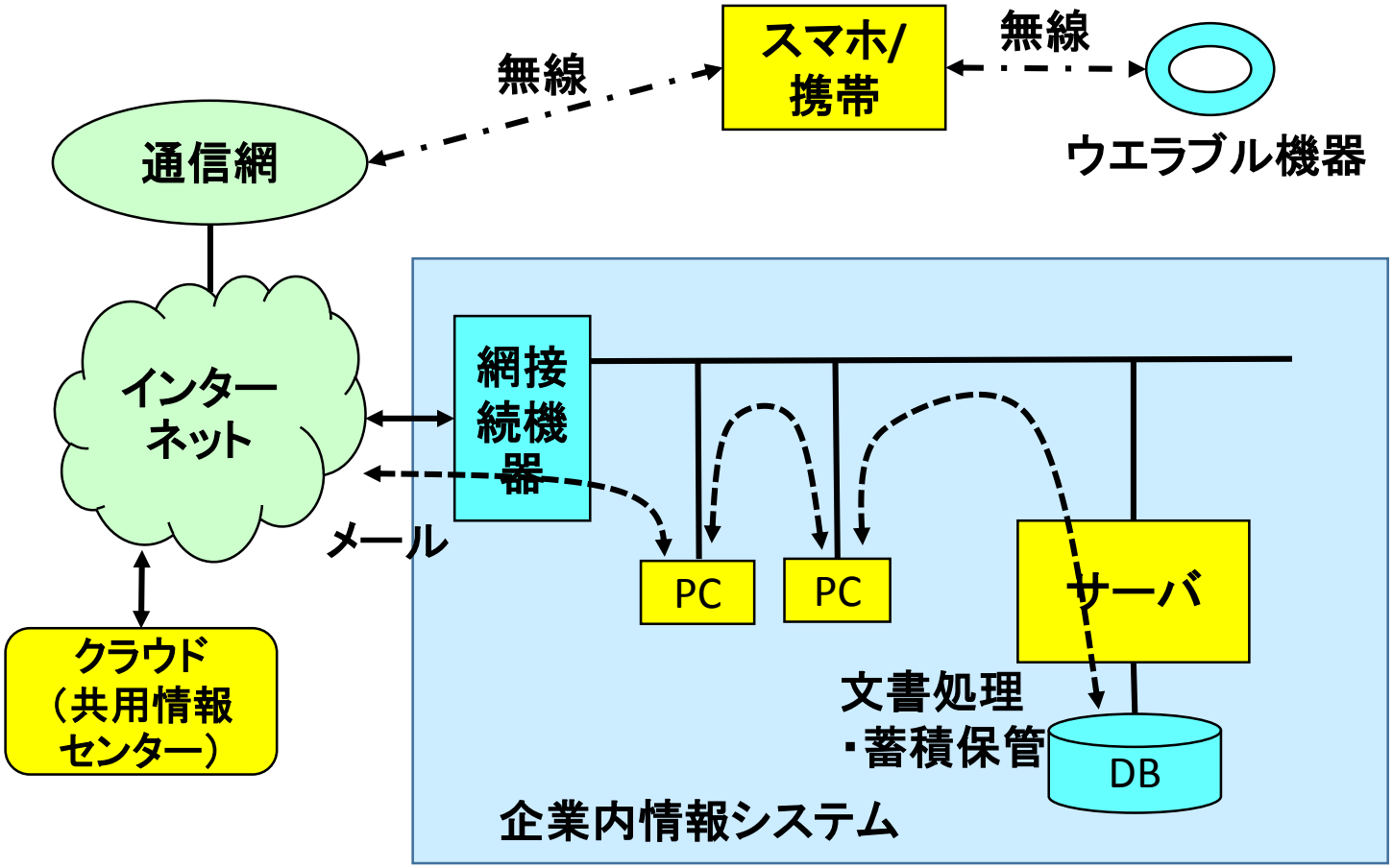
情報セキュリティ大学院大学

目　次

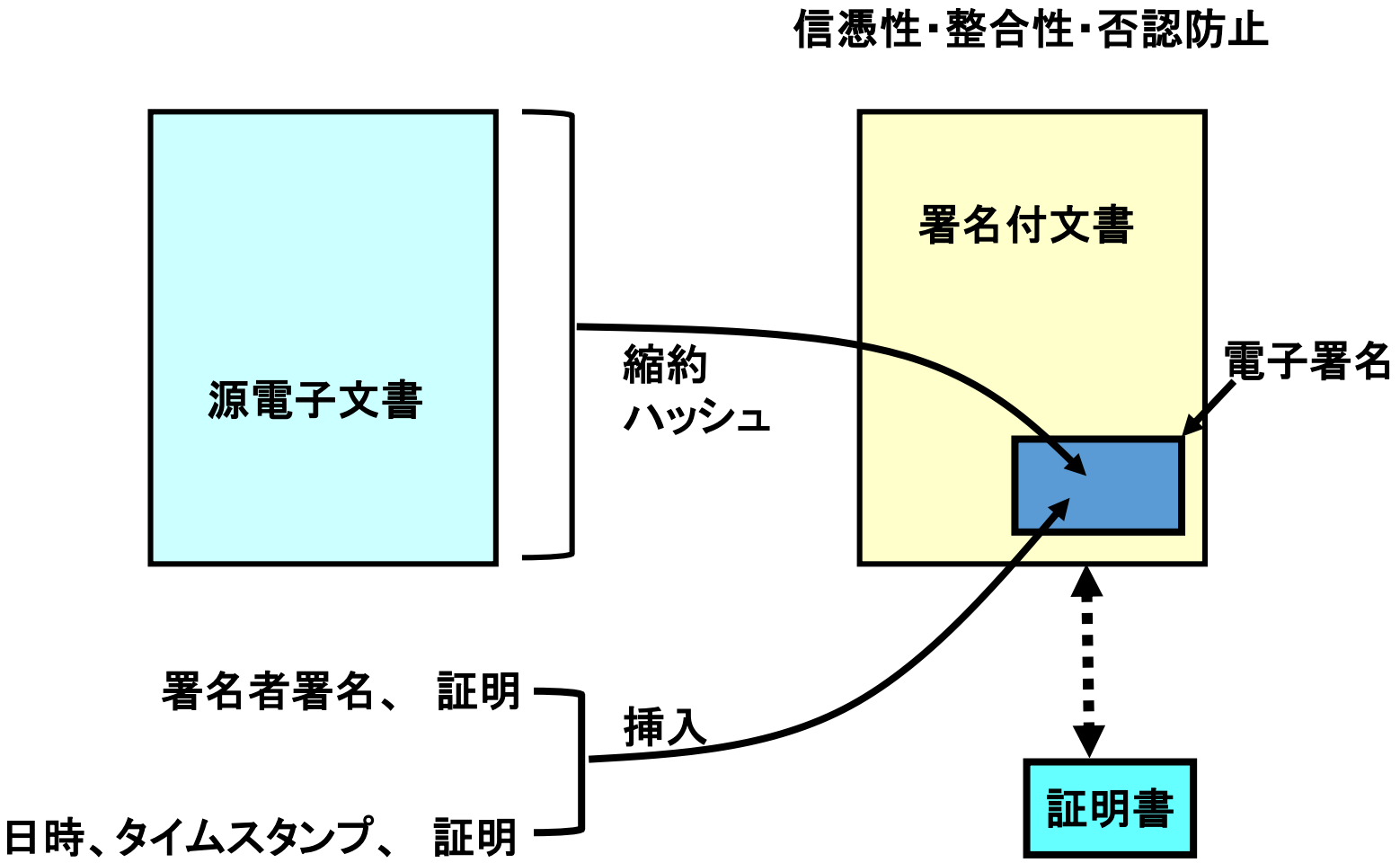
1. 情報社会
2. サイバーセキュリティ問題の現状
3. 情報社会の発展
4. IoTにおけるセキュリティ問題
5. セキュリティ対策と管理
6. 社会の変化と今後の課題

1. 情報社会

- 代表的領域における情報社会の現状
  - オフィス：email, FTP, 仮想デスクトップ
  - 製造工場: 3D printing(設計図=電子情報）
  - 物流：受け・倉庫・仕分け、QRコード利用
  - 家庭：写真、映像、音声、記録
  - 情報環境：モバイル、PC、クラウド、センサ、ウエラブル、インターネット
  - 電子媒体：e-文書法（文書の電子化保存を認める）
  - 取引時正当な相手の確認：従来方式（実印、印影、印鑑証明書）/PKI方式(秘密鍵、公開鍵、電子証明書)



情報機器の接続形態と利用


信憑性･整合性･否認防止
源電子文書
縮約
ハッシュ
署名付文書
電子署名
署名者署名、 証明
日時、タイムスタンプ、 証明
挿入
証明書

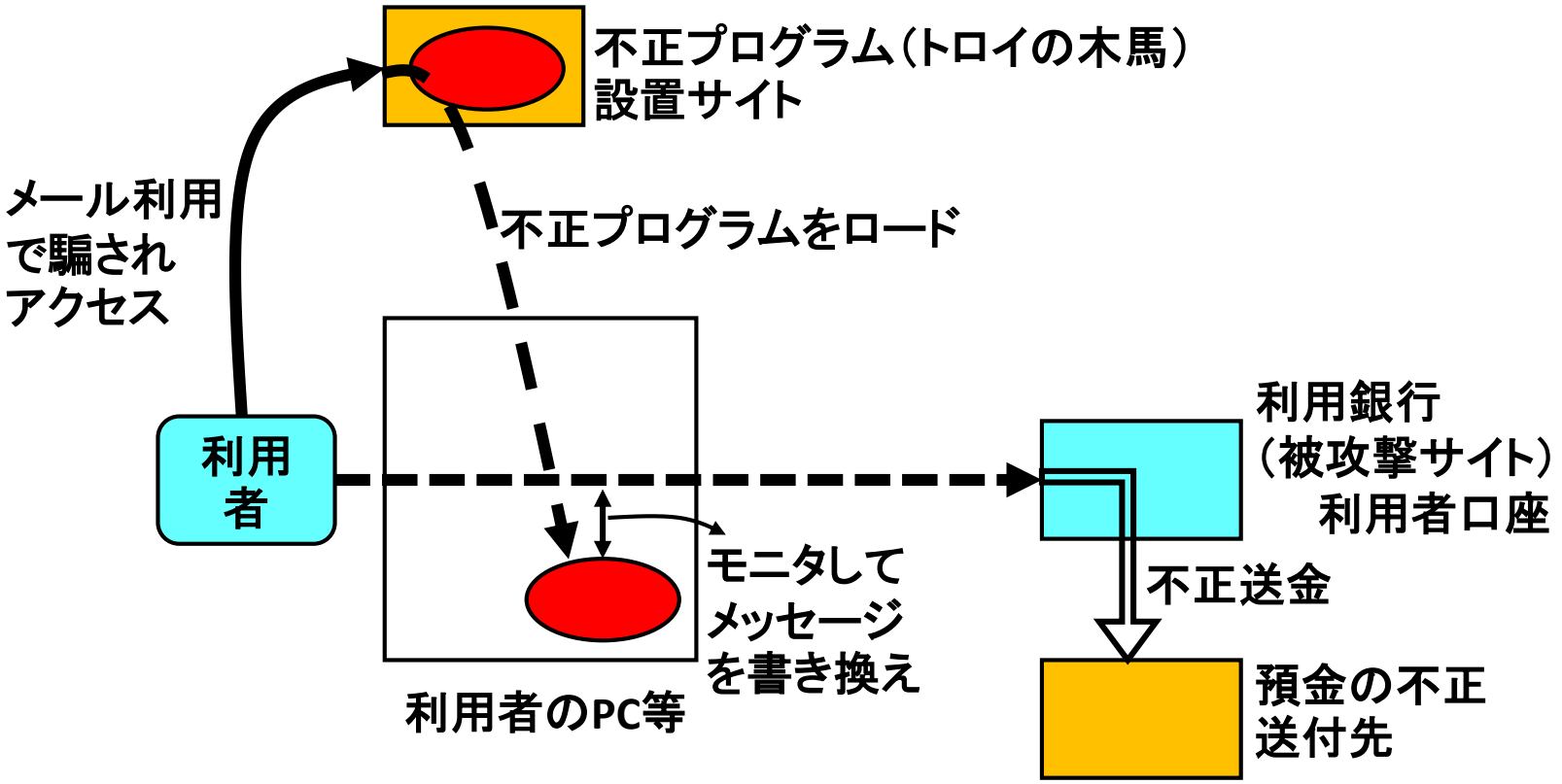
2. サイバーセキュリティの問題

- サイバー攻撃の変遷
- トロイの木馬
- 具体被害
- 漏洩コスト・件数
- 標的型攻撃
- Webサイト攻撃
- ランサムウエア

サイバー攻撃の変遷

年	攻撃名称/被害者等	内容
2004	AOL	大規模顧客情報流出　9300万件
2006	KDDI	大規模顧客情報漏洩　399万件
2007	エストニア	ソ連時代のブロンズ像移転に、ロシアからDDoS攻撃
2008	GhostNet	世界規模スパイネット ダライラマ事務所感染
2009	Operation Aurora	米国企業知財流出（Google, Adobe, RSA等）
2010	Stuxnet	イランにおける核施設攻撃で遠心分離機破壊
	Wikileakes	米国外交機密文書25万点全公開
	海上保安庁	尖閣諸島沖衝突事件画像情報流出
2011	日本国会議員	IDとパスワードが盗まれる
	PSN	大規模顧客情報流出　7700万件
	三菱重工	外部からシステム内侵入　情報漏洩可能性
2012	Operation High Roller	金融機関預金の不正資金移動　78Mドル
	Aramco	サウジアラビア企業が攻撃を受け、数万台PCダウン
	イスラエル	Anonymousが大規模攻撃　DDoS
	NPO Spamhaus	大規模はDDoS攻撃を受けた
2013	韓国	放送局、銀行など攻撃でシステム停止
2014	韓国	史上最大のクレジットカード情報流出　1億4000万件
	ベネッセ	通研ゼミ顧客情報、2070万件、DB管理会社派遣者
	OpenSSL	SSLソフトウエアの脆弱性問題、UNIX OS bash
2015	不正送金	諸銀行からの不正送金多発（29億円、倍増）
	年金機構	個人情報125万件流出、標的型攻撃

金融機関の預金を狙うトロイの木馬



具体被害

	被攻撃サイト	攻撃種類	被害
2013/3	通販サイト	Apache Struts2	個人情報漏洩
2013/5	レンタルサービス	SQLインジェクション	クレジットカード漏洩
2013/7	ポータルサイト	パスワードリスト	なりしまし個人情報
2014/1	オンライン銀行	フィッシング詐欺	ID. PSWD漏洩
2014/2	書籍購入サイト	ドライブバイダウンロード	ユーザがマルウエア感染

平均漏洩件数	604, 826	2012年シマンテック報告
損賠賠償額	7500万円	JNSA報告書
調査費用、再構築費用	5000万～1億円	IPA被害調査
ブランド毀損	売上額の5～40%	事例から

データ侵害の平均コスト：4.2億円、企業の9割は脅威侵入済み、7割は被害経験、侵入から発見まで242日

情報漏えいコスト2015年

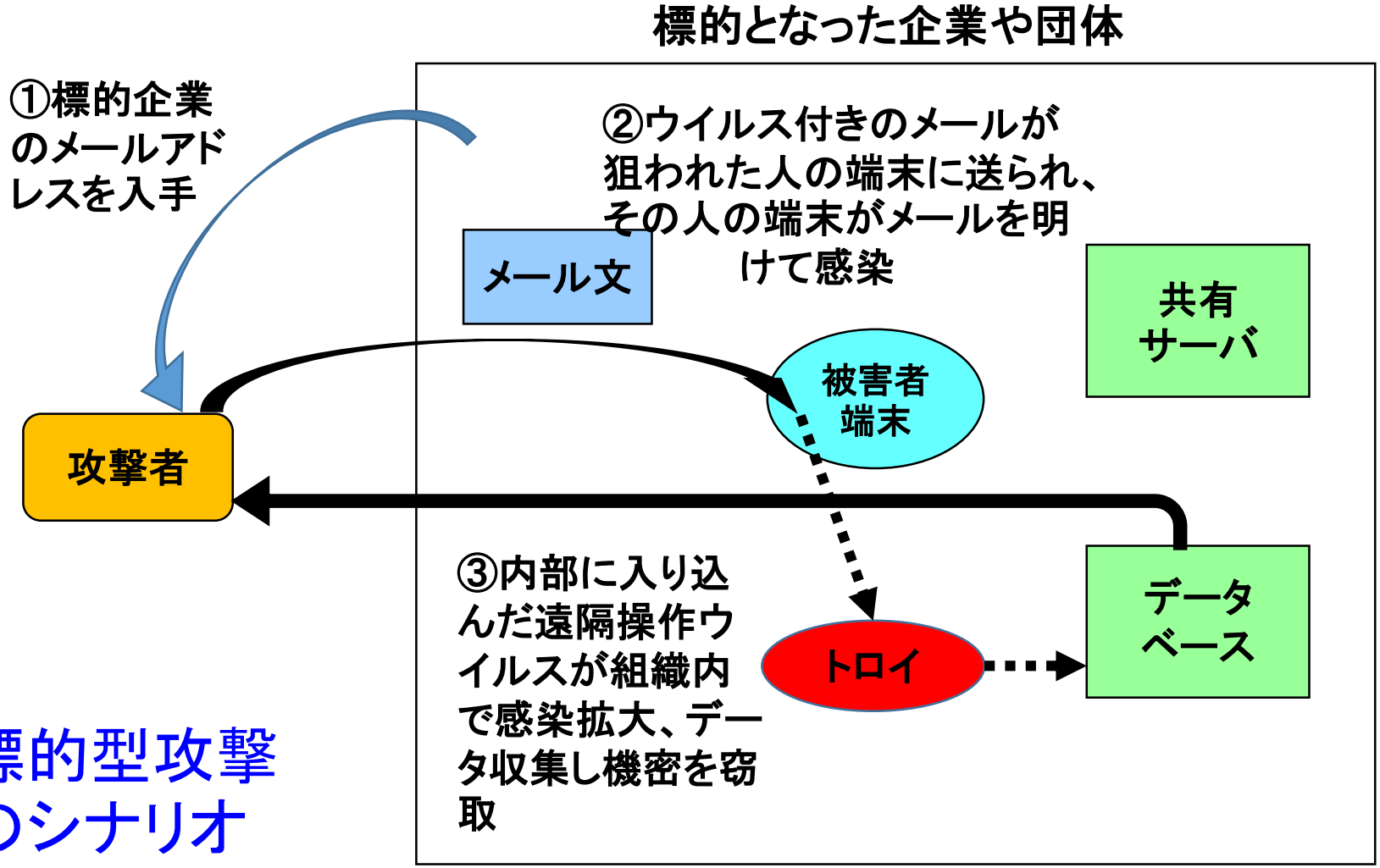
- 攻撃頻度と是正措置に必要なコスト増
- 結果：ビジネス機会の損失 157万ドル（133万ドル）
  - 異常な程の顧客離れ
  - 顧客開拓業務の負担増
  - 顧客からの評価の低下
  - 業務上の信用の失墜
- 対策コスト：99万ドル（76万ドル）
  - フォレンジック/調査活動、評価/監査業務、危機対応チームの管理、経営陣や取締役会との連絡
- 有効なインシデント対応には経営幹部関与が必要
  - 最高経営幹部の79%が認識（米、英）

情報漏えい件数

企業名	業務	漏洩件数
eBay	E-commerce	145,000,000
Hartland	Financial	130,000,000
T.J.Maxx/T.K.Maxx	Retail	94,000,000
AOL	Web	92,000,000
Anthem	Health care	80,000,000
Sony	Gaming	77,000,000
JPMorgan Chase	Financial	76,000,000
Target	Retail	70,000,000
Home Depot	Retail	56,000,000
Evernote	Web	50,000,000

標的型攻撃

- 60%が中小企業を対象とする
  - 中小企業は、対策に多くの資源投資が困難
  - 大企業の6社に5社が攻撃の標的
- 攻撃手法
  - メールに添付ファイル、その実行でマルウエアロード
  - 企業の使うソフトウエアを識別、その更新プログラム内部にマルウエアを隠し、ダウンロードを待つ
  - 未知の攻撃やSSL/TLS利用でチェック困難
- 対策: 完全防御は困難、事後策
  - 体制整備、情報収集と共有、実装(抑止策、被害拡大の防御策、被害発生検知策)、ダメージ制御と被害対処の備え、復旧手段確保、継続的対策に向けた実施評価と予算措置、人の教育


標的となった企業や団体
①標的企業のメールアドレスを入手
②ウイルス付きのメールが狙われた人の端末に送られ、その人の端末がメールを明けて感染
メール文
共有サーバ
被害者端末
攻撃者
③内部に入り込んだ遠隔操作ウイルスが組織内で感染拡大、データ収集し機密を窃取
トロイ
データベース

標的型攻撃のシナリオ

年月	報道された標的型攻撃
2009/11	世界のエネルギ関連企業や製薬会社
2010/1	Googleなど米国企業
2010/6	イラン核燃料施設
2011/4	ソニーへの攻撃で個人情報が流出
2011/9	三菱重工
2011/10	衆議院の議員のパスワード流出
2012/5	原子力安全基準機構で情報流出
2012/7	財務省で情報流出
2012/11	三菱重工でウイルス感染
2013/1	農林水産省からTPPなど機密情報流出
2013/2	外務省ネットから情報流出
2013/5	Yahoo JAPANから2200万件のIDや148万件のPSWDが流出可能性
2014/1	高速増殖炉もんじゅ、国立がんセンターで不正プログラム実行
2014/2	はとバスにIEのゼロデイ攻撃
2014/8	日本のISP, 大学などに水のみ場攻撃
2015/6	日本年金機構で125万件個人情報流出
2015.6	米国で政府職員情報2210万人分が流出、国家や産業の機密窃取

Webサイト攻撃

- Webアプリケーション脆弱性狙い
  - 2014年、78%のウエッブサイトは脆弱性を抱える
  - 内16%が重大脆弱性
- 各所にある脆弱性
  - Webサーバ、Webアプリ、DB、メール、net、遠隔アクセス、通信、OS、等
- 影響の大きな脆弱性（2015　3/4サイト未だ残存）
  - OpenSSL, GNU bash, SSL version3.0
- 水のみ場攻撃
  - 正規サイトを侵害、サイト訪問者を監視し標的企業だけを狙う

ランサムウエアの増加

- 裕福な国のユーザを対象とした身代金強要
  - ユーザは身代金を支払う傾向がある（欧米）
  - 日本でも急速に拡大中（2015.7)、届出件数(2015 111件、IPA)
- 詐欺メール
  - その国の言語で、その国の実在企業からのメールを装う。
  - 郵便局や電話会社から住所変更/確認、郵便物の再送先の入力を依頼する
- 強力なランサムウエアの出現
  - 仮想通貨の利用、Torネットの利用、モバイルへの移行（Androidのデータを暗号化するランサムウエア）、大規模ストレージへの攻撃
  - NASサーバのパッチ未使用の脆弱性を攻撃、強力暗号化でサーバ上全データ暗号化、楕円暗号利用
- 対策
  - データバックアップ、セキュリティ意識を高め、Torアプリをブロックする、スパム対策、一時フォルダから実行ファイルの実行を阻止

重要インフラや制御システムへの攻撃の急増

- 重要インフラ
  - 欧州電力会社、核施設破壊、石油パイプライン爆発、列車運行妨害、下水処理流出
- 製造業
  - US制御システムCERT報告2014: 重要機器製造業攻撃急増
- 状況
  - 攻撃が「無い」のではなく、「検出」していないので「発覚」なし
  - 古い機器の存在：脆弱性の存在、安定稼動の罠
  - USB経由
  - 今後接続されるIoT機器を「踏み台」にしての侵入
  - PLCを外部から制御するツールの公開：警視庁が警告 2015.12

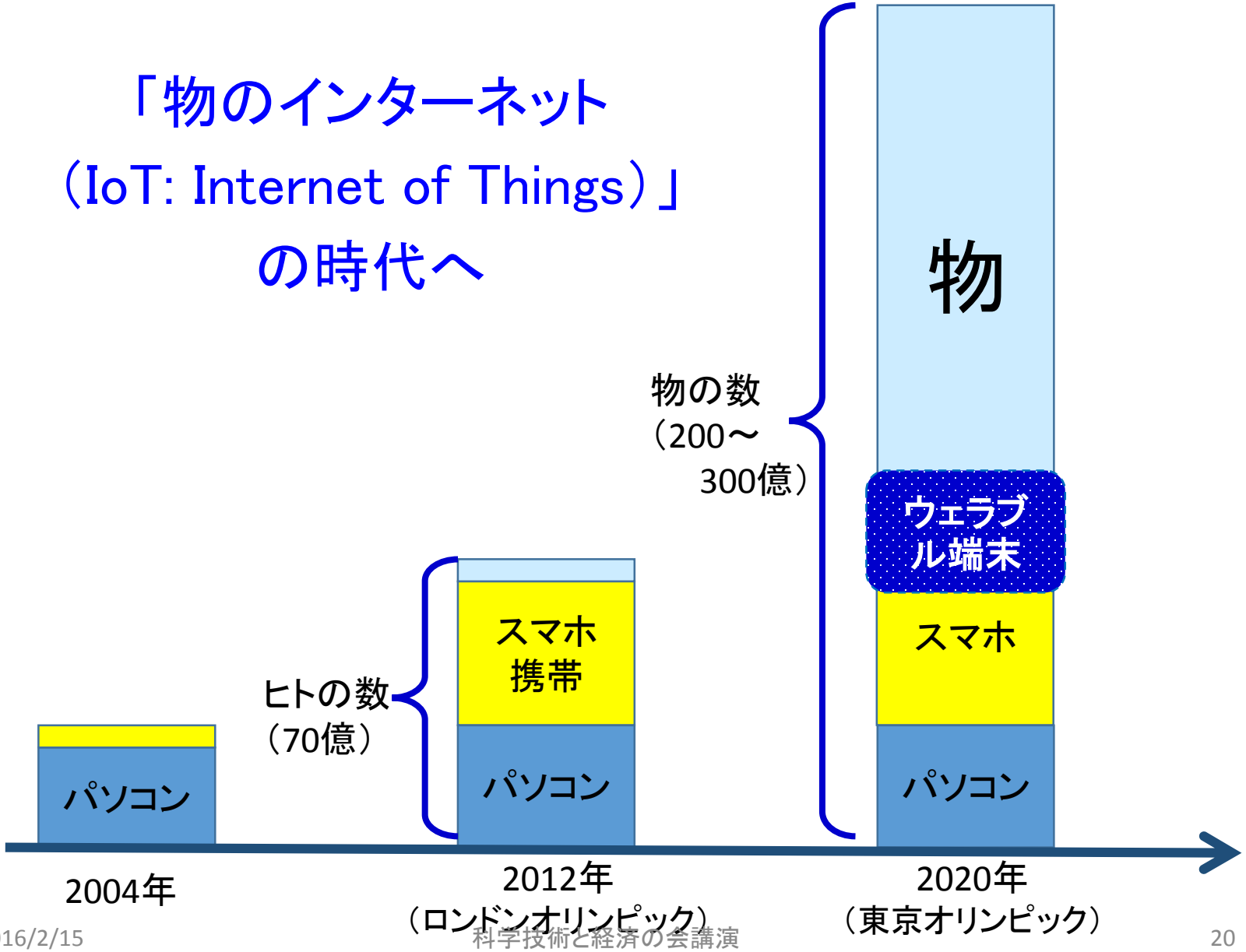
サイバー犯罪コスト調査2015

- 世界における企業毎のコスト
  - 日本　632万ドル、米　1542万ドル
- 組織規模との関連
  - 大規模組織より小規模組織の方が一人当たり費用は3倍
- 企業種別
  - 金融サービス・通信・ユティリティ・エネルギ・技術の分野は、小売・メディア・教育・研究分野より大幅に高い
- 損失の大きい犯罪に対するコスト：発生頻度加重
  - 内部不正5400万円、ウエブベース攻撃2000万円、サービス妨害2000万円
- 攻撃を解決する時間
  - 時間がかかるほど費用が高い：平均26日
- 情報損失が全費用の48%、次にビジネス中断30%
- 検出と復旧は最もコストがかかる内部活動(53%)

3. 情報社会の発展

- あらゆるモノが繋がる
  - IoT: 繋がるデバイス数、市・インフラ・ビル・交通・工場・医療福祉・生活
  - 機器が電子化されネット接続：サービス、更新、ウエラブル
- ビッグデータの活用
  - 効率化、マーケティング、便利、攻撃データの共用
- 人工知能の発達：deep learning
  - 画像認識、最適化
- 社会トレンド
  - 個中心、所有から利用へ、連携、物理と論理の融合

「物のインターネット（IoT: Internet of Things）」の時代へ



モノのインターネット

- 情報技術は製品に革命的変化を及ぼす
- スマート製品の力
  - スマート製品の能力：モニタリング、制御、最適化、自律性
  - 新機能、信頼性や稼働率の格段向上
  - 業界構造と競争のあり方を変え、企業を競争上の新機会と脅威にさらす。全く新しい産業を生む
  - 戦略面で新しい選択肢：価値創造、生み出す膨大データの活用・管理、販売チャネルの見直し
- モノの本質が変化する
  - 機能性は製品利用状況の膨大データ活用で実現
  - 生産過程で新業務が生まれ、バリューチェーンが変わり、ITを起爆剤とする変革は大規模へ

IoT に於けるビッグデータ利用

- センシング
  - 自動検針、ヘルスケア、バイオセンサ、五感センサ、構造物センサ、スマートハイウエイ、イメージセンサ
- 分析と知識抽出
  - 医療・ヘルスケア・環境・流通・物流・農業・社会インフラ
  - 人の行動：ユーザ行動・購買活動、ヘルスケア、フィットネス、医療、犯罪防止
  - 物の挙動：スマートシティ、設備稼働状況チェックによる予防保全・設計改良、スマートパーキング、環境モニタリング、インフラ稼動状況チェックでエネルギ管理・監視、気象情報から予測

IoTの世界

- 3要素
  - フロント：データを吸い上げる、センサとネット接続
  - クラウド：インフラ
  - プロバイダ：価値の高いサービスを提供する
- 特徴
  - 多い関連業種、ターゲット絞りが困難、市場拡大確実
  - 多様な業種と協業し経験と知見蓄積を力に：システムインテグレータ、ベンチャー企業と連携
- 新世界内のステークホールダ
  - Cloud/Crowd/Devices: 人と場所とモノのユニバース
  - 情報と経験を実時間で結びつけ、未経験問題でも解決
  - Collective Computing: 人の処理と計算機処理の区別曖昧化
  - 人の案内、ヘルス、教育、商業、実時間体験化

IoTのユースケース

- IoT
  - センサでモノが、モバイルで人が、繋がる。あらゆるモノが繋がり、新価値創造。2025までに3～6億ドル効果
- ４領域
  ① モノと人の繋がりを拡大
    - 個人ヘルスケア、健康情報蓄積予測で安心・安全社会支援
    - 生活データ収集、個別ニーズに応えるサービス提供
    - スマートスポーツ＆娯楽：スポーツ解析と連携
    - 店での顧客購買体験：機会ロスを減らし、情報共有
  ② 車：　安全運転支援、自動運転、車と地理情報を実時間解析し交通情報配信、個別サービス提供、保守改善
  ③ スマート製造：センサで故障予知、最適エネルギ管理、世界の工場・仕入先を実時間連携し最適な自律操作
  ④ 既存系：社会システムの裏側、鉄道、電化

ビッグデータ活用と変化

- データ源
  - 自然環境系：気温、地震計
  - 組み込み機器系：電力計、携帯のGPS
  - 社会活動系：Webやクレジットカード利用履歴、医療の薬剤・臨床データ
- 処理
  - フェーズ：センシングと転送、クレンジング、応用
- 利用目的の連携による変化
  - 自動車センサ: 保守点検→ 運転者の運転習性データ利用で保険料割引・割り増し
  - 目的に応じた匿名化で適応型セキュリティ対策
  - 情報の価値と特性が動的に変化：多様なステークホルダによる価値創造に柔軟に対応できるセキュリティ対策

ネットワーク家電

- 出来ること
  - 遠隔操作/遠隔視聴/メッセージ送信/機器・スマホとの連携
- リスク：従来ITと共通
  - 情報漏えい/不正な遠隔操作/機能停止/攻撃の踏み台/ポートスキャンで検索エンジンから検索可能となる
- 問題
  - FW/IDSは、家電では資源・価格面で困難
  - ルータ自体にも脆弱性
- 攻撃者に取って
  - 容易に機器を入手可能
  - シングルサインオン：認証情報漏洩でシステム全体に影響

コネクテッドカー

- 注目が集まる
  - CES2015: 国際家電見本市、主要自動車メーカ出展
  - CES2016: 重電見本市、自動運転車が座巻
- US市場形成プレイヤー
  - 車両情報把握伝送・車両情報活用・車両常時接続
  - Verizon LTEサービス：2014, 人工カバレッジ99%
  - 接続コネクタ：ODB2
- 国際競争
  - US: Google, Apple等IT系が主導、市場シェア高い
  - 日本：トヨタ等自動車産業が主導
- リスク顕在化と対策
  - Jeep 2015.7(140万台リコール）、Tesla 2015.8(ハイジャック）
  - 連邦取引委員会FTC: 2015.3 技術研究調査室、消費者保護

モバイル変革と期待

- モバイルとは
  - あらゆるモノが無線で繋がる機能：有線接続の限界打破
  - モバイルとは効果的な働きかたを実現すること
  - 効果的な方法は未だだが、モバイル変革は推進中
  - 期待：円滑コミュニケーション、実時間連携、生産性向上
- 利用
  - 接客のオンライン化による効率向上、体験付与
  - デジタルカタログ、動画マーケティング
  - 相互の居場所によらぬ会議：TV会議、資料交換
  - 存在場所によらぬ機器保守、遠隔操作：センサ
  - 仮想現実利用の遠隔操作精密手術、遠隔診断：ダビンチ
  - ウエラブル：物理人がネットに繋がる

医療現場にスマホ導入

- 慈恵医大　3200台iPhone ICTプロジェクト
  - PHSからスマホへ
  - 病棟内　企業との共同実証研究
- サービス開始　2016.1 オリンピックに向けて
  - PHSからスマホへ
  - ナースコールをスマホ対応
  - 病棟・外来棟　FreeWiFi設置、非常用WiFi電話、患者向け院内WiFi
  - スマホ診断券、院内呼び出し、院内ナビ、会計スマホ
  - ヘルスケアアプリ、翻訳システム開設

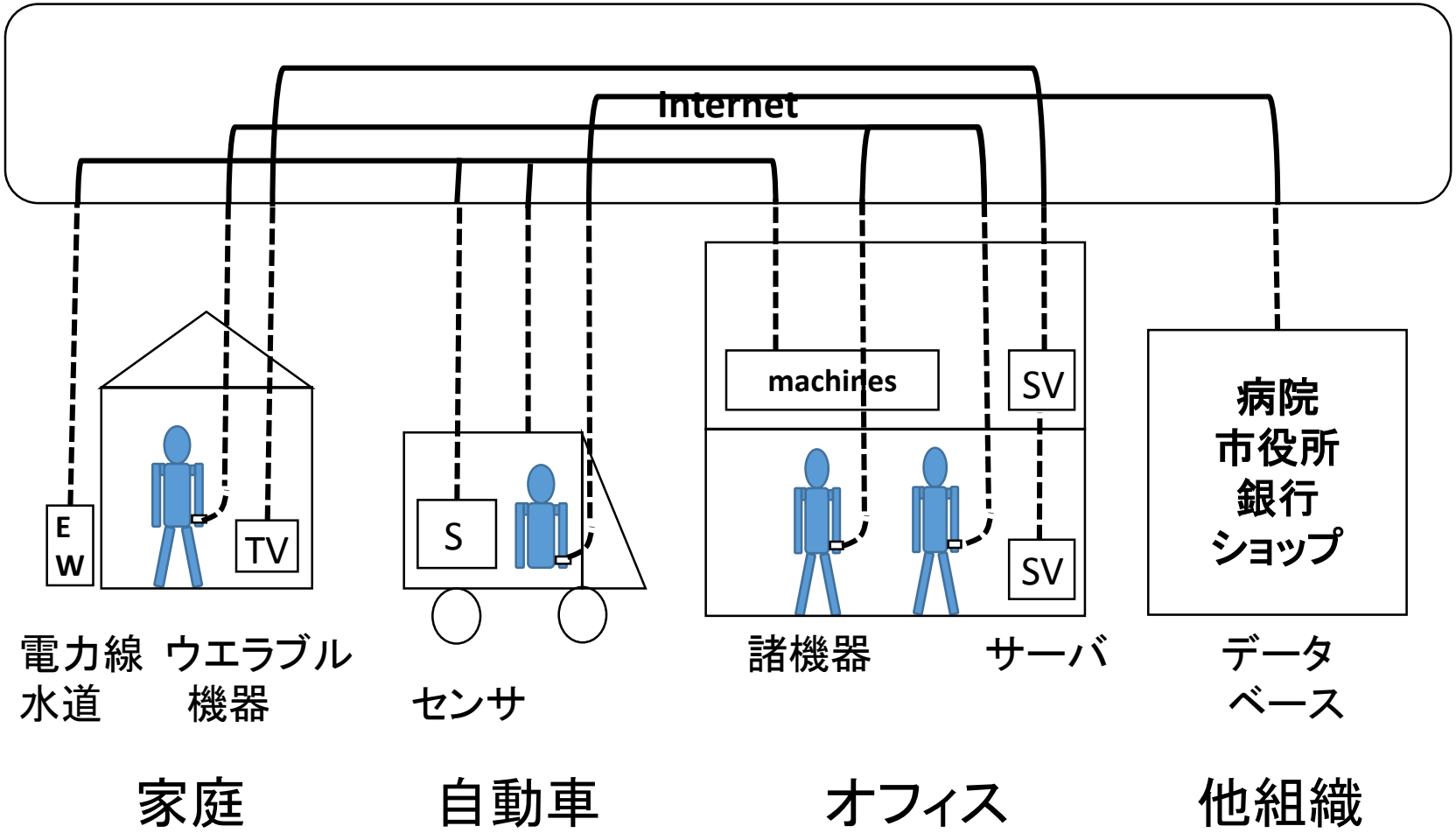
モバイルとクラウドの課題

- アクセス管理
  - 安全性と使い勝手を両立させるモバイルアクセス：きめ細かいユーザ/端末認証とアクセス制御、クラウドとオンプレミス混在環境でのアクセス管理
- アクセス認証に証明書利用
  - より厳格なクライアント認証：個人端末にクライアント証明書配布、既存ID管理とシームレスな連携
- クラウドアプリ認証
  - 境界線を越えるアプリ層間のフェデレーション認証が鍵
- 業務以外のWeb利用、マルウエア感染への対策
  - フォワードプロキシで望ましくないWebアクセスを止める

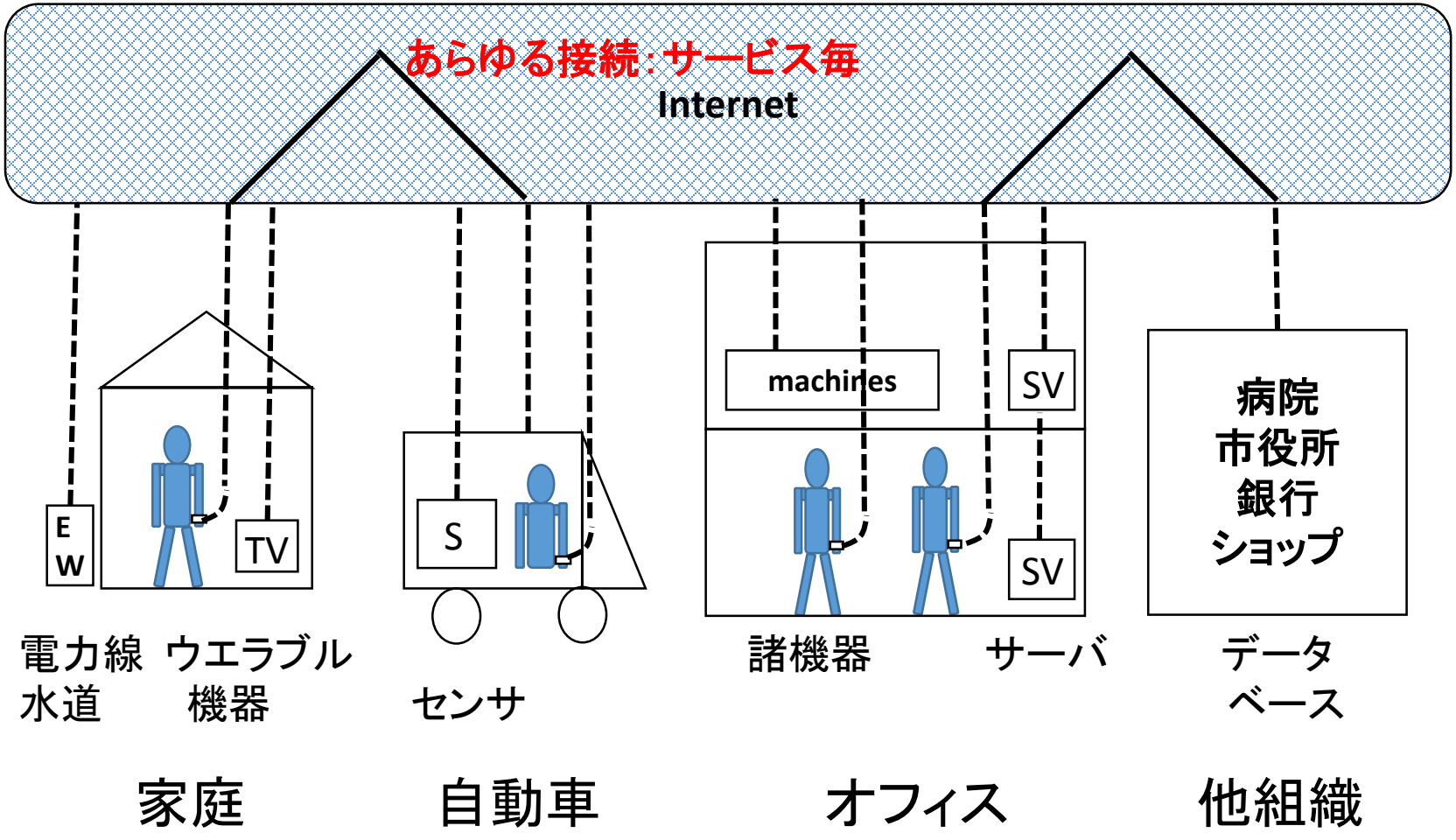
IoTによるシステムの変化

- センサ利用によるオンラインデータ収集と管理・制御・保守
  - スマート機器、遠隔最適保守、農業自動化
- サブシステム毎の情報化
  - 生産システム、保守システム、販売システム、気象予測システム、経営システム、市場情報システム
- サブシステム連携による複合システム
  - 生産と部品供給、販売・保守・部品供給、農業生産最適制御・気象・農業管理・農業機械・販売
- 複合システムの連携
  - 農業システムと穀物価格情報システム、健康システムと医療システム、スマートホーム（照明・空調・娯楽・セキュリティ）、EV共有システム、スマートシティ

繋がる社会イメージ：現状



繋がる社会イメージ：今後



IoTからの洞察とビジネス変革

- 主要な技術シフト
  - デバイスが生成するデータ量増大
  - ビジネスの成長を助けるクラウド
  - 企業と顧客間のよりスマートな連携：モバイル、ソーシャル
- IoTは物理世界とデジタル世界をつなぐ
  - 新ビジネスモデル、知的連携で最適化、製品の運用性能から製品開発改善、データ解析で業績改善
- ビジネス機会の誕生
  - 石油・ガスで探索・開発コスト減、エネルギ供給インフラ、車載システムの実時間監視、航空と防衛のコストダウン、スマート家電
- 今後は技術がビジネスモデルを定め駆動
  - ビジネス実現を可能にするICTは過去
  - 新プレイヤーが突然出現し既存産業構造を変える

グローバルIoT経済的インパクト

- グローバル経済効果
  - McKinsey&Company 2013 : $2.7 – 6.2 Trillion/year by 2025
  - Gartner 2013 : $1.9 Trillion/year in 2020
  - Cisco 2013 : $19 Trillion in next 10years
- 工業のみの経済効果
  - GE 2012 industrial internet : $10 – 15 Trillion in 20years
    産業機器からデータ採取、データ分析、最適化
    分野（航空、電力、鉄道、ヘルスケア、オイル・ガスで、
    システム効率向上（燃費、航路））

参考

1 T dollars = $ 10E12 ≒ ¥ 10E14 = 100兆円

4．IoTにおけるセキュリティ問題

- 新しい事象と課題
- 新リスク
- 課題の広がり
- OWASP TOP10問題
- IoTセキュリティリスク状況
- 脆弱性

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、情報システムから制御系システムへ拡大、電力網攻撃は21世紀の最大脅威（米）
  - 重要インフラを狙う攻撃：標的型攻撃の主要目標
- 接続機器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、影響範囲大
- セキュリティ/モバイル/クラウド　対応

新しいリスクへの対応

- スマート xx の脆弱性: ビル、自宅、グリッド、車
- 医療: データへの攻撃
- 安心 : 高齢化社会、デジタルデバイドの存在
- サイバーセキュリティリスク開示の現状
  - 有価証券報告書、開示が少ない
  - US(連邦規則、開示ガイダンス), EU(開示検討）、認識
- e-ディスカバリ : 電子的情報開示
  - 電子データを文書管理や訴訟対応のために保存するための準備 :
    メール保管対策　50%企業が未実施
- 特定個人情報保護評価 : Privacy Impact Assessment
  - 実施側 : 扱う必要性を理解してもらう。行政機関・地方公共団体
  - 国民側 : 扱いの透明性担保

課題の拡がり

- 多くの課題
  - 無線接続の安全性問題
  - 企業ネットとIoT応用の非両立性
  - ハードウエアの多様化
  - あらゆるモノにユニークなタグを付ける危険性
  - データを第三者に売るプライバシ問題
- セキュリティ脅威の広がり
  - 漏洩、大規模な破壊
  - 既存攻撃に加え、IoTの新規攻撃手段が出現
- IoT Top 10 Project 2014: OWASP
  - IoTの全様相を調べ、重要な10問題を抽出

OWASP IoT Top 10
-Open Web Application Security Project-

I1: 安全でないWebインタフェース
I2: 不十分な認証/認可
I3: 完全ではないネットワークサービス
I4: 暗号化されていない通信
I5: プライバシーの懸念
I6: 安全ではないクラウドインタフェース
I7: 安全ではないモバイルインタフェース
I8: 安全ではないソフト/ファームウエア
I9: 不十分なセキュリティ設定
I10: 物理的なセキュリティ問題

事例

- JEEPハッキング：BlackHat2015
  - ブレーキ、ギア、ステアリング等制御
  - リコール140万台
- 衛星利用サービスの攻撃
  - 拡散スペクトルシステムDSSSは認証無く、なりすまし
- 制御システムへの攻撃
  - ネット経由でPLCにマルウエア注入
- モバイル決済端末への攻撃
  - SQUARE社、カードリーダ、暗号化無いモデル
- Wi-Fiハッキング
  - APIが無認証で、コアシステム関数にアクセス化
- 心臓ペースメーカ不正操作
  - US GAO経由の警告

IoTのセキュリティリスク状況

- 端末当たり平均25の脆弱性
  - 暗号化しない通信
  - デバイスが単純なパスワードで利用可能
  - デバイスのユーザインタフェースに、クロスサイトスクリプティング、セッション管理の脆弱性
- あらゆるものが攻撃対象
  - 埋め込み型医療機器、アイロンからスパム攻撃チップ
  - ネットカメラの脆弱性で盗撮、道路信号システムの脆弱性
  - ATSC規格の脆弱性ですべての対応スマートTVに問題
  - GAOは航空機が不正アクセスを受けて制御される可能性警告2015
  - スマホを使ってBMW車のドアロックやエアコン操作
- 技術領域が多岐にわたりセキュリティ担保が困難
  - 必要な/実装されている　セキュリティレベルが異なる
  - リスク低減には、セキュリティベースラインを検討し、技術領域が多岐の問題をツールやサービス利用でノウハウ習得
- IoTは急速に進展

IoTデバイスの脆弱性現状

- IoTデバイス当たり平均25件
- プライバシ：80%、名前、メールアドレス、住所、CD番号、問題
- 認可：80%、不十分なパスワード
- 暗号化：70%、暗号化無しネット通信、50%モバイルは暗号化無し通信
- Webインタフェース：60%で、インタフェースにXSSやセッション管理脆弱性、認証情報を平文送信
- ソフトウエア： 60%で、ソフトウエアアップデート時に暗号化未使用
- 古い脆弱性がよく使われる
  - Heartbleed, Shellshock, POODLE、以前からある脆弱性の利用
- POSデバイス：攻撃の大幅増加と進化

5. セキュリティ対策と管理

- 企業における問題：経営からの視点
- 個別対策：データ保護/次世代対策
- 管理：ISMS, CSIRT, 意識改革、委託、保険
- 法制：情報法、サイバー空間
- 連携
- 対策のまとめ

企業における問題

- サイバーセキュリティは経営問題
  - 社会問題化のリスク
- マルウエア問題
  - 攻撃の侵入経路の大半はクライアントPC
  - 既存の不正プログラム検知だけでは不十分
  - 不正送金：法人口座（中小企業）が狙われる
- 仕事上の課題
  - 企業内に閉じたシステムを想定できない
  - 外部利用：契約後は先方に任せることになる、現地従業員のセキュリティ意識に不安
  - PCにマルウエアをダウンロード後は、セキュリティ無し
  - 情報が流出したら、回収できない

企業経営からの視点

- 組織目的の確認と改善
  - 判断に必要な情報の確認
- 迅速意思決定
- 組織体制構築：全体、担当、CSIRT組織化
- 社員意識改革・教育
- セキュリティ監視・現状分析・リスク認識
- 事故に備えた演習

個別対策例：データ保護

- 情報の存在場所に関わらず、多種多様な情報の保存、アクセス、共有を可能としビジネス活動を制限しない漏洩対策
  - 社内外の経路（デザリング、公衆無線LAN)やデバイス(スマホ、USB、Bluetooth）を総合管理
  - 必要な情報は暗号化して持ち出す、社外者には参照以外の操作を禁止した閲覧制御
  - 中央サイトで認証をかけてチェック、問題時即失効
- データ侵害平均総コスト
  - 379万ドル：2015 Ponemon Institute調査
  - 信頼やブランドが損なわれる

次世代対策

- 従来
  - 標的型攻撃でGateWay セキュリティ：入口・出口対策、IPS, FW, Proxy, 統合脅威管理UTM
  - 紛失による漏洩対策、モラル、シグネチャによる検知
- 対策
  - SIEM高度化：ビッグデータ解析との統合
  - SSL/TLS: SSL Visibility: 復号化/暗号化利用＋ポリシ
  - インシデントレスポンス対策：CSIRTとSOC
  - 迅速なマルウエア感染予防や感染後対処：運用負荷軽減。リモート操作でパッチ適用・状態確認・修復作業等

管理・運営

- 管理問題
  - PDCA、IT資産、インシデント・レスポンス、内部不正
- ISMSとCSIRT（消防団）組織
  - 情報分類、リスク特定、リスク評価、監査
  - CSIRT構築：大企業の4割以上構築済み（19→42% 2014)
  - 担当者個人では対応困難：同業と情報共有・連携
- 意識改革：リテラシ（ネット時代の常識）/信頼の輪
- 外部委託の限界
  - ITリスクを制御できないと経営者責任
- 最期の砦：保険
  - サイバーアタック保障保険、個人情報漏洩保障保険、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

情報法制

- サイバー空間における法律の限界
  - 国境を越え、匿名性が高く、法律施行が困難
  - 国家間規律：ソフトロー、国際ルール作り
- 国内対応
  - 電気通信事業法、信書のガイドライン
  - 個人情報保護：第二版2015(防御から利用へ）
  - ウイルス作成罪(2011)、フィッシング罰則(2012)
  - 特定電子メール送信：2008年: 事後拒否→事前承諾, 100万円→3000万円
- サイバーセキュリティ基本法(2015施行)
  - 内閣に戦略本部設置：戦略案作成、指揮監督の意見具申、各省庁に義務を課す権限
  - 改正案：2月、衆院提出、監視対象拡大

組織関連携

官民、民民など様々なレベルでの組織間連携、情報共有体制・協力体制の確立：諸分野におけるISACを作る
　　ー諸領域での設立が望まれる

- Telecom/Financial ISAC Japan
- CEPTOAR：情報共有・分析機能
- IPA
  - J-CSIP：重要インフラ向け
  - JVN:脆弱性DB
- JPCERT/CC
- GSOC（政府）
- SPREAD：サポータ育成
- JNSA-CERC
- 日本CSIRT協議会
- ISOG-J：オペレーション事業者
- JC3: サイバー犯罪対策
- LGWAN(地方公共団体）

組織・企業における対策と管理
ーまとめればー

- 対策
  - 強固な基礎：最新更新されたソフトの利用
  - 信頼できるマルウエア対策の利用
  - 安全なインターネット利用と、社内ITポリシーの設定・利用
  - ID管理、暗号化、強固な認証:基本要素
  - ガイドライン等への対応：自己判断から第三者
- 管理
  - 当事者意識：最悪自体想定、脅威の理解
  - 経営者参画：最良の対策検討から選択
  - 説明責任を果たせる環境
  - 標的型攻撃対応：攻撃を受ける可能性の認識
  - 定期的チェックと改善

6.社会の変化と今後の課題

- 世界の動きとわが国の計画
- 社会の変化
- 攻撃側の世界
- 研究開発の強化
- 対応組織の強化
- セキュリティ経営
- 人材育成

日本と世界

- 世界の時価総額トップ
  - Apple, Google, Microsoft, Exxon
  - 世界最大の小売業： AmazonがWalmartを抜いて1位
- 日本のベスト10
  - 自動車、銀行、通信インフラ、JT
- 比較
  - 革新的機能を持つモノの製造？：ICT企業は1社もない
  - 生活が仮想化、グローバル化
  - 消費者に訴求力？：スピーディで柔軟な情報サービス

世界の動き

- 3つの波:　global/digital/social
  - 複合的に重なり発展
- 情報化による影響
  - 国家を超えた統治機構のニーズ：環境破壊、ウイルス蔓延、サイバーテロなどの課題
  - ビジネス過程が電子化され、不可視化：知能を持った機械が実現する生産性向上
- 新生きがいの社会
  - 国のアイデンティティ消滅
  - ネット化された仲間と協働：賢さや楽しさの追及に生きがい、勤労価値の消失
  - AIの加速的発達による科学的知の発展

NIRA 研究報告書2015.10

第５期科学技術基本計画

- 総合科学技術会議・イノベーション会議
  - 新５ヵ年計画(2016-2020)：2015.12会議で答申案了承
  - 世界に先駆けて超スマート社会の実現
- 超スマート社会の実現Society 5.0
  - モノ作り(Industry 4.0)だけでなく、諸分野に広げ変革へ
  - サイバー空間と物理空間の高度融合：Society 5.0

•超スマート社会サービスプラットフォーム構築:

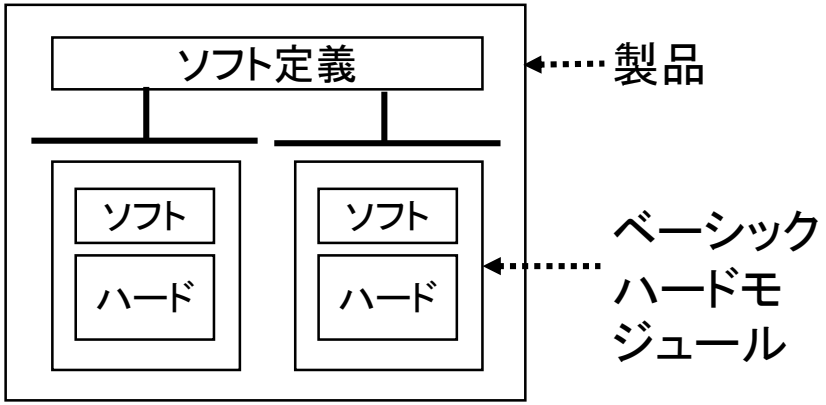
  - サービスや事業のシステム化、システム高度化、システム間連携
- 基盤技術の強化
  - プラットフォーム構築技術：サイバーセキュリティ、IoTシステム構築、ビッグデータ解析、AI、デバイス
  - 新価値創造のコア技術：ロボット、センサ、バイオ、素材・ナノテク、光・量子
- イノベーション創出の人・知・資金の好循環システム

Industry 4.0/Society 5.0

- 最新IT技術を駆使し生産効率高いスマート工場を実現
  - 単独の工場だけでなく、受け入れる部品、出荷製品、物流行程、販売ネット、顧客などをネットで繋ぎ、人の関与無く、機械が相互に通信し、生産・物流・顧客対応やサービスの全体を最適化
- 製造業だけでなく、サービス/社会の視点
  - Society 5.0
- 情報化の多面性
  - 製品を作るプロセスから買った製品を消費するプロセスまでメディア化。知のゲームとして普及
  - AIからの挑戦と適応:人類の存亡への挑戦と同時に、それに適切に対処するための事前適応（仲間として協働）

社会の変化

- 情報化から知能化へ
  - 物理空間と情報空間の融合：機械との共創社会、Cyber Physical Computing
  - ソフトウエア定義製品
  - ソフトウエアビジネスモデル：Airbnb/Apple/Uber
  - ネットビジネス：サービス事業者→ SNS → IoT



製品例：現在
SDN: Network
SDS: Storage
SDP: Software Defined Productsへ
繋いで、サービス再発見

攻撃側の世界

- 攻撃活動の市場化
  - 市場、請負、仕込み、攻撃活動
  - 侵入を見せての顧客獲得, 公開攻撃キット
  - Web 攻撃kit $数100/w, DDoS $10-1000/day, Card情報$10
- 攻撃活動の高度化
  - 対策を掻い潜る工夫が高度化：クリプトウエアは45倍増で、写真、重要契約書、請求書のファイルを暗号化し身代金要求。Tor, Bitcoin利用
  - 人（攻撃者）と人（防御者）のゲーム
- 攻撃側有利な世界
  - 一つでも穴があればよい vs すべてを防ぐ
- グローバル化
  - 世界に広がる攻撃者・Bot、捕捉の限界

セキュリティ研究開発機能の強化

- 情報セキュリティ技術は、輸入依存
- 情報セキュリティコア技術/情報は、わが国の必須アイテム
  - 国際間インテリジェンスにおける交換条件
  - 技術の研究強化、もぐら叩きからの脱却
- 研究内容と体制
  - 基礎研究：システムの複雑化対応
  - 強みの再確認
  - サイバーセキュリティ解析コア技術・設備
  - 研究向け共有情報の拡大と実効的利用体制

システムの複雑化問題

- 現在のサイバーセキュリティ対策
  - 脆弱性：脆弱サブシステム、個別対応
  - 対応：専門知識を持った専門家依存
- IoTの時代が来ている
  - 膨大な接続：センサ、車、システムなど
  - 設計原理の差異：異なるサブシステムが繋がる
- 重要課題：複雑性への対処
  - サブシステム・インタフェースの明確定義問題
  - 不明なサブシステム間接続はカオス
  - グローバル・システムの全体イメージ像把握

対応組織の強化

- 政府関係・公的組織：強化
  - NISC, 省庁、警察、GSOC, IPA, JPCERT、NICT, JC3, CSSC
  - 情報収集・分析・配信の機能強化
  - 共通脆弱性評価システムCVSS: ソフトの脆弱性深刻度を数値化
- 国際連携に向けた政策対話
  - サイバー空間の国際規範作り: ハーグ会議2015.4
  - 重要インフラ防護ベストプラクティス共有：MERIDIAN
  - サイバー空間の脆弱性、脅威、攻撃に関する国際的取り組み: IWWW
- 民間：連携形成
  - ISAC形成: 重要インフラ、諸分野
- 試行と修正という回し方：新時代の要件
  - 前もってすべての問題点を把握不可能
  - 法律と現実のギャップを埋める仕組み

サイバーセキュリティ経営ガイドライン

- 2015.12.28　METI・IPA発表　v.1
  - 企業戦略として、ITやセキュリティ投資に関する判断必要
  - 経営者が認識する3原則、担当に指示すべき重要10項目
  - サイバーセキュリティ経営チェックシート
- 3原則
  - 経営者は、IT活用推進中で、サイバーセキュリティを認識し、リーダシップで対策をすすめること
  - 自社のみならず、系列やサプライチェーン、IT委託先を含めたセキュリティ対策であること
  - 平時・緊急時に、サイバーセキュリティリスクや対策、対応に係る情報の開示など適切なコミュニケーションが必要

サイバーセキュリティ経営10項目

1. リーダシップの表明と体制の構築
   - ① リスクの認識、組織全体での対応の策定
   - ② リスク管理体制の構築
2. サイバーセキュリティリスク管理の枠組み決定
   - ③ リスク把握と実現セキュリティレベルを踏まえた目標と計画の策定
   - ④ 対策フレームワーク構築PDCAと対策の開示
   - ⑤ 系列やサプライチェーンを含めた対策の実施と状況把握
3. リスクを踏まえた攻撃を防ぐための事前対策
   - ⑥ 対策のための予算・人材確保
   - ⑦ ITシステム管理の外部委託範囲特定と委託先のセキュリティ確保
   - ⑧ 情報共有活動への参加を通し、攻撃情報の入手とその有効利用のための環境整備
4. 攻撃を受けた場合に備えた準備
   - ⑨ 緊急時の対応体制整備、定期的・実践的演習の実施
   - ⑩ 被害発生後の通知先や開示が必要な情報の把握、経営者による説明のための準備

ポリシ・サンプル、他参考

- 情報セキュリティポリシーサンプル改定　1.0版
  - JNSA: 2016.4予定、中小企業向け改定作業中
  - 対策実践手引き・ポリシーサンプル・状況チェックシート
- Framework for Improving Critical Infrastructure Cybersecurity V 1.0
  - US NIST 2014.2.24: Identify/Protect/Detect/Respond/Recover
  - Level: 1 Partial/2 Risk Informed/3 Repeatable/4 Adaptive
- Critical Security Controls for Effective Cyber Defense
  - Center for Internet Security作成：October 15, 2015. version 6
  - セキュリティ・プラクティスのセット：　20項目
  - https://www.cisecurity.org/

情報セキュリティ人材

- 人材の種類
  - 組織内オペレーション
    - 経営者/セキュリティ責任者/セキュリティ担当者/CSIRT
  - 組織間オペレーション
    - JPCERT/CC, SOC, GSOC, Telecom ISAC, IPA
    - グローバル：FIRST(信頼化されたCIRTの国際組織で、問題対応を効率化、メンバ間のTrusted連絡)
  - セキュリティ専門企業・組織：アウトソーシング受託
  - 研究開発：大学、NICT, 産総研、IPA, 企業
- 人材育成の必要性と機会
  - 大学：例　情報セキュリティ大学院大学
  - 専門企業
  - 社員全体のリテラシ＋対応組織専門知識

明日の信頼を創る情報セキュリティ人材を育成します

学長　田中英彦

- 本学は2004年に開学し、新しい学問の体系化と専門家の育成を旗印とする情報セキュリティ専門の独立大学院。
- 2015年10月までに、修士271名、博士29名の修了生。各所属組織において情報セキュリティに関する中核的業務を担う。
- 本学は、様々な分野の意欲的な学生を受け入れ、「明日の信頼を創る」高度な情報セキュリティ専門人材の育成に努める。

本学の特色

- **情報セキュリティ専門の大学院大学：　修士（情報学）　博士（情報学）**
- **技術・管理・法制、セキュリティ総合教育のカリキュラム**
- **将来のCIO/CISOを育成する実務指向教育と深い専門研究成果の蓄積**
- **横浜市神奈川区鶴屋町2-14-1（横浜駅きた西口徒歩1分）**

おわり