サイバー攻撃による脅威の現状と課題

2016年2月8日

田中　英彦

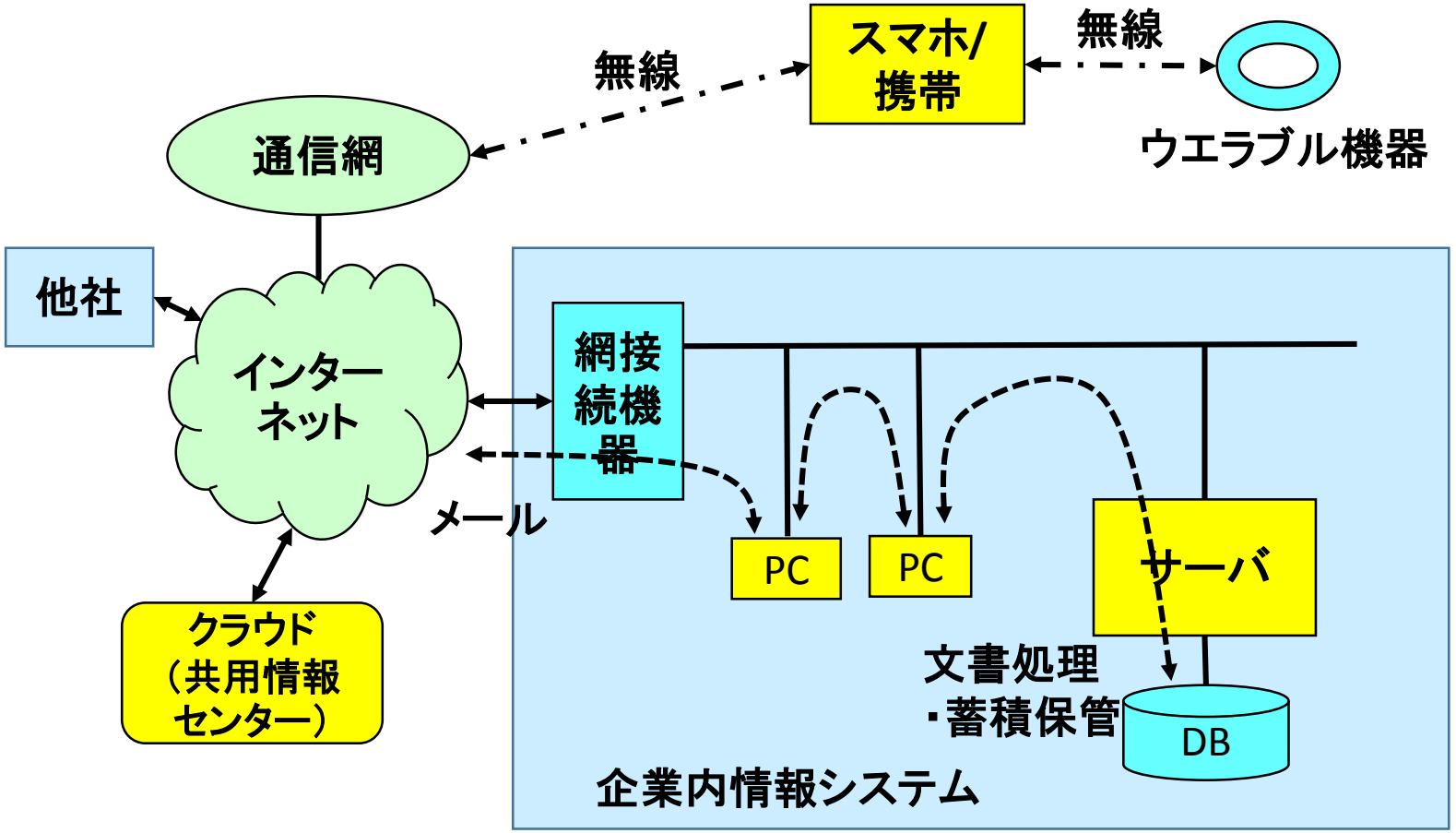
情報セキュリティ大学院大学

発表内容

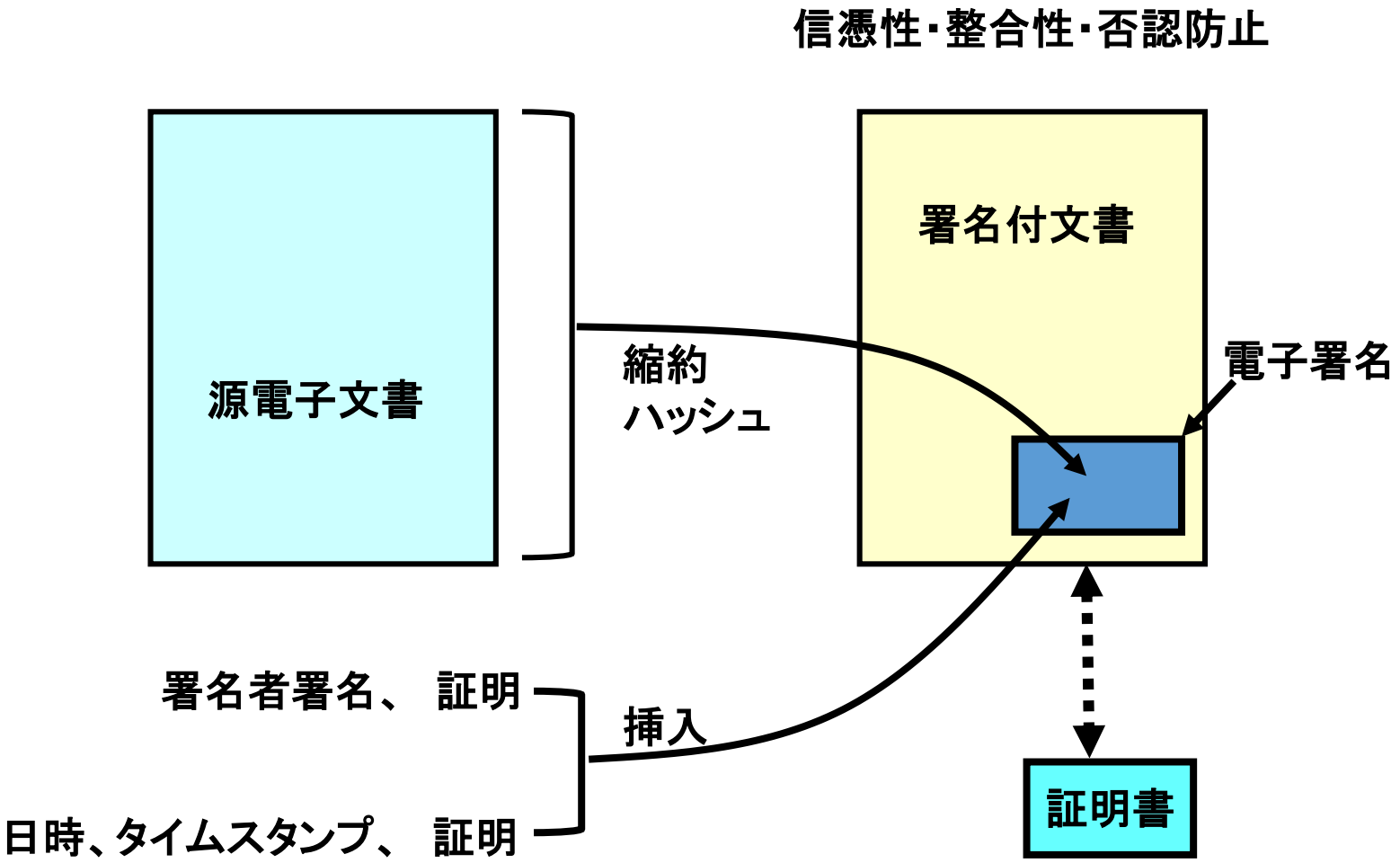
- サイバーセキュリティ問題の現状認識と課題把握
- 目次
  1. 情報社会
  2. サイバーセキュリティ問題
  3. 情報社会の発展
  4. 対策
  5. 交通システム
  6. 今後に向けて

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: 設計資料=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： PC、モバイル、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

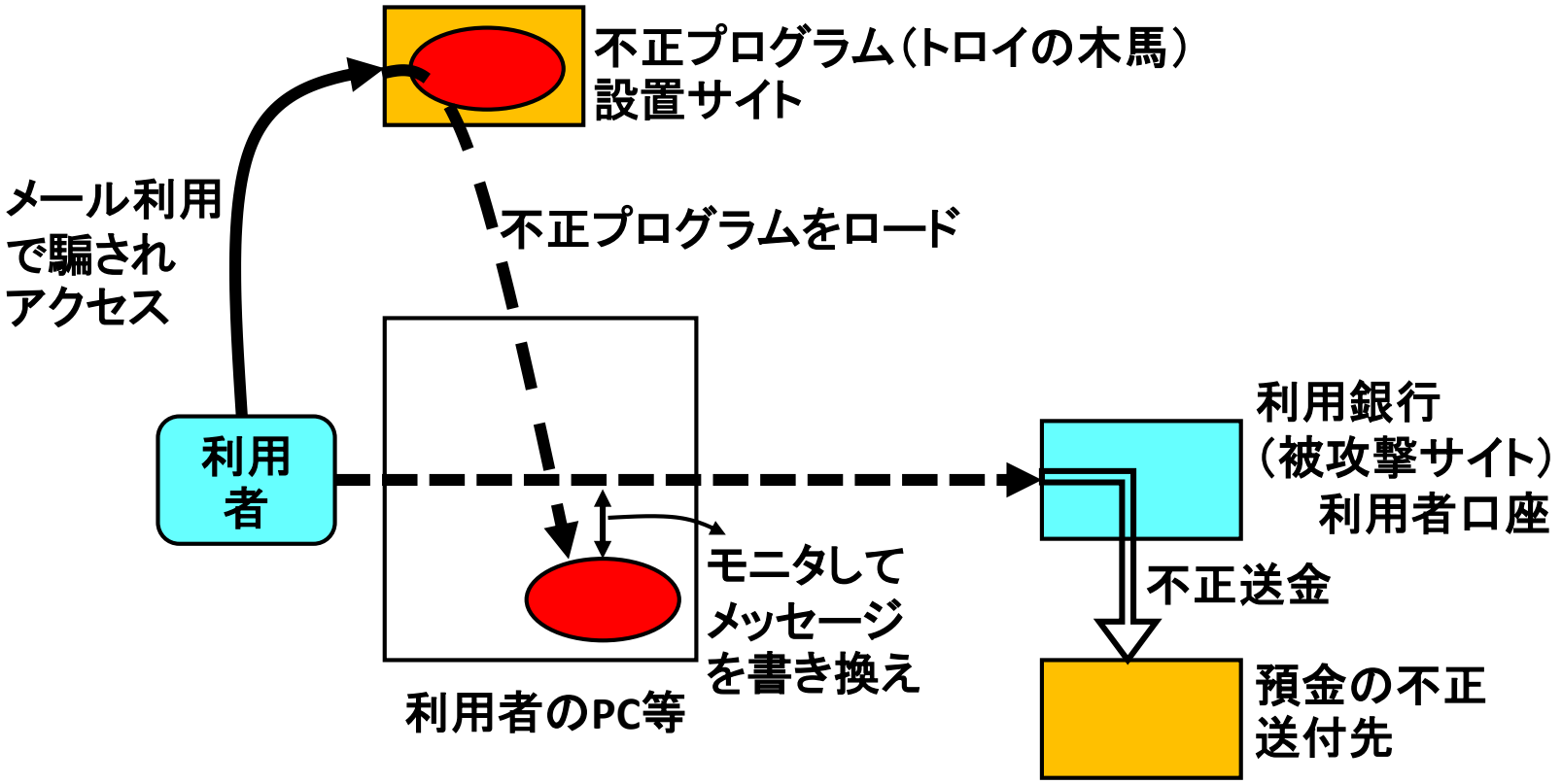
2. サイバーセキュリティ問題

- 情報窃取：知財盗難、機密窃取・暴露
- 情報破壊：誤謬注入、財産破壊
- サービス停止：DoS
- システム破壊：制御ソフトウエア破壊、重要インフラ機能停止
- Webサイト：脆弱性78%
- 資金窃取：なりすまし詐欺、不正送金
- スパムと正規メール数：2対1
- 放置された脆弱なホームルータが犯罪の温床

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

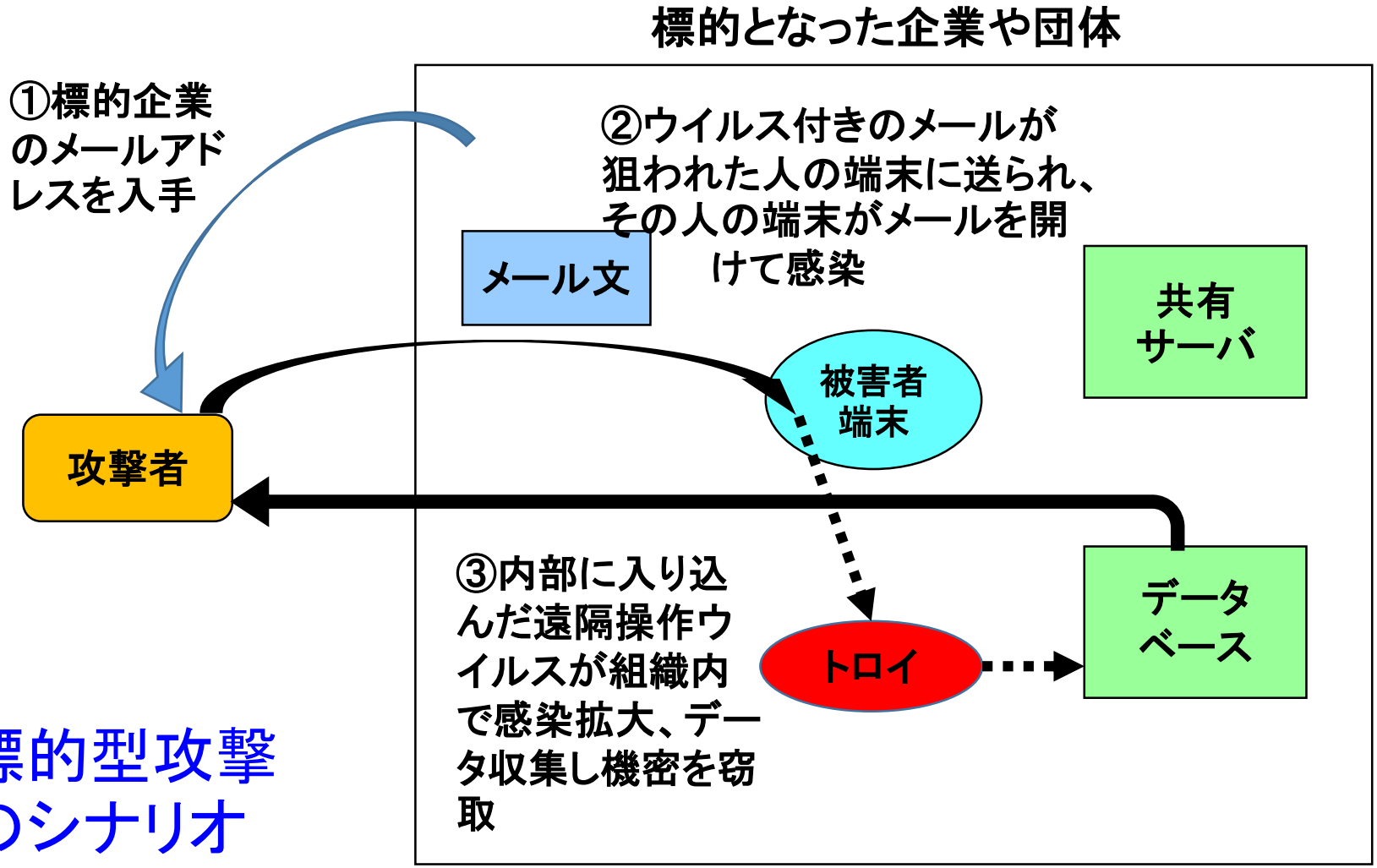
- 攻撃頻度と是正措置に必要なコスト増
- 結果：ビジネス機会の損失 157万ドル（133万ドル）
  - 異常な程の顧客離れ
  - 顧客開拓業務の負担増
  - 顧客からの評価の低下
  - 業務上の信用の失墜
- 対策コスト：99万ドル（76万ドル）
  - フォレンジック/調査活動、評価/監査業務、危機対応チームの管理、経営陣や取締役会との連絡
- 有効なインシデント対応には経営幹部関与が必要
  - 最高経営幹部の79%が認識（米、英）

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し、その更新プログラム内部にマルウエアを隠し、ダウンロードすることを待つ
- 対策: 完全防御は困難、事後策
  - 推進体制整備、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の対処への備え、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開けて感染
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

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)、相談１１１件(IPA 2015.12)
- 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

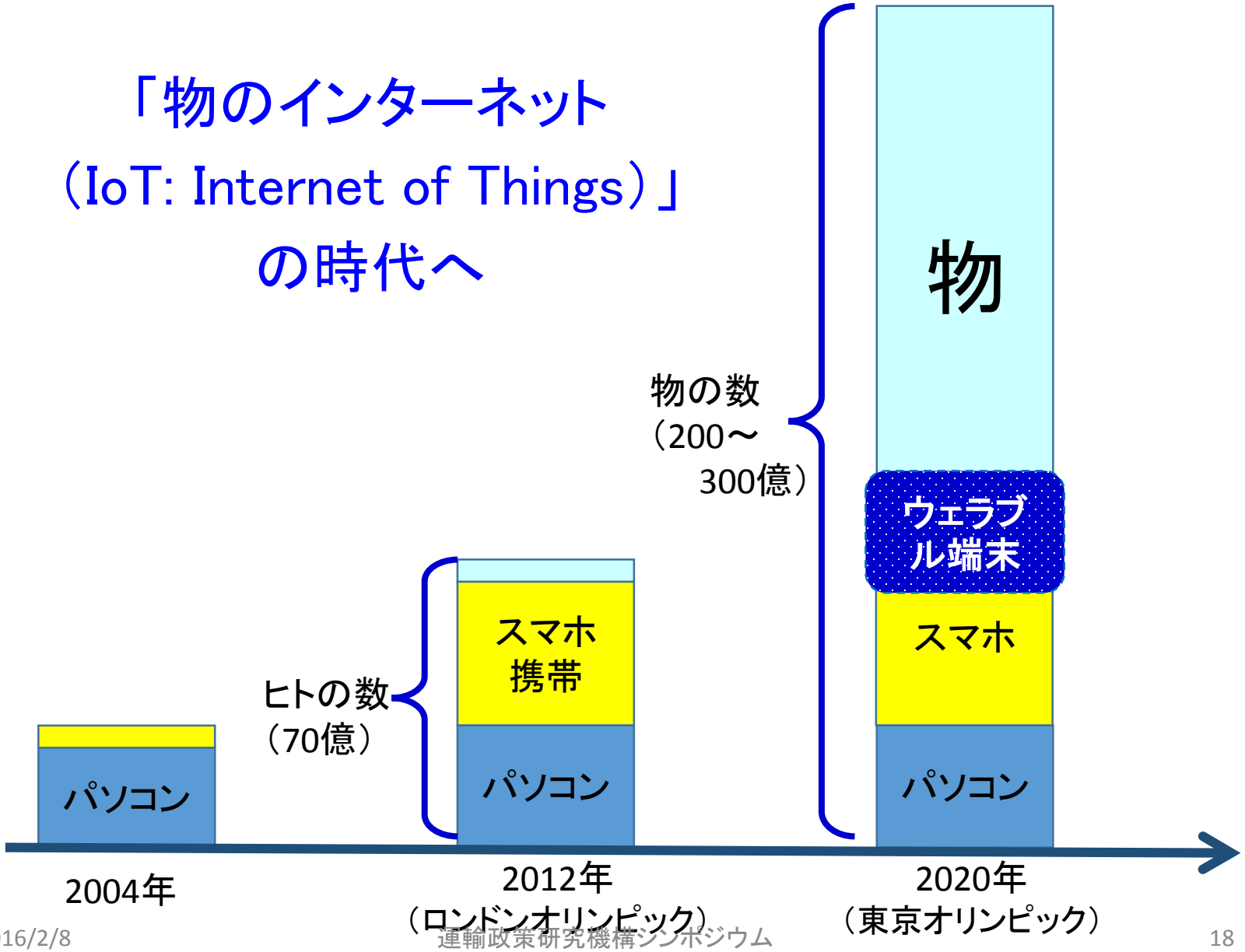
重要インフラや制御システムへの攻撃の急増

- 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

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



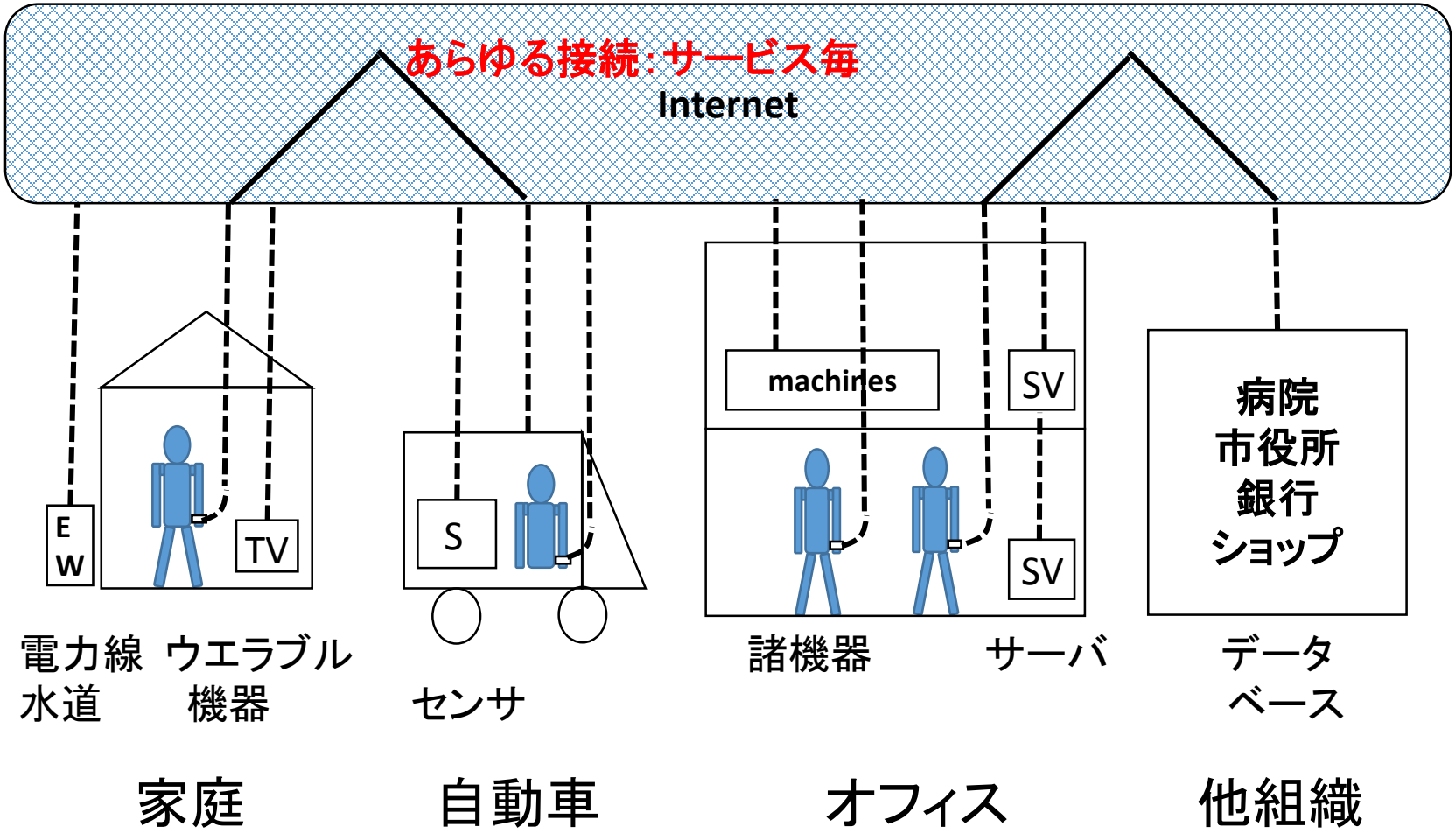
モノのインターネット

- 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

繋がる社会イメージ：今後



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

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

4. 対策

- 企業における問題
- 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、リスク
- 法制：情報法、サイバー空間
- 連携

企業における問題

- 情報セキュリティは経営問題
- 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
  - IT予算に占めるセキュリティ対策費：10-12%
  - 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しかない
  - 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

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
  - CIA（機密・完全・可用性）、PDCA、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)
- 人の意識改革:リテラシ(ネット時代の常識)
- 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、等

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

－担当者個人では対応困難：同業と情報共有・連携

- 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）

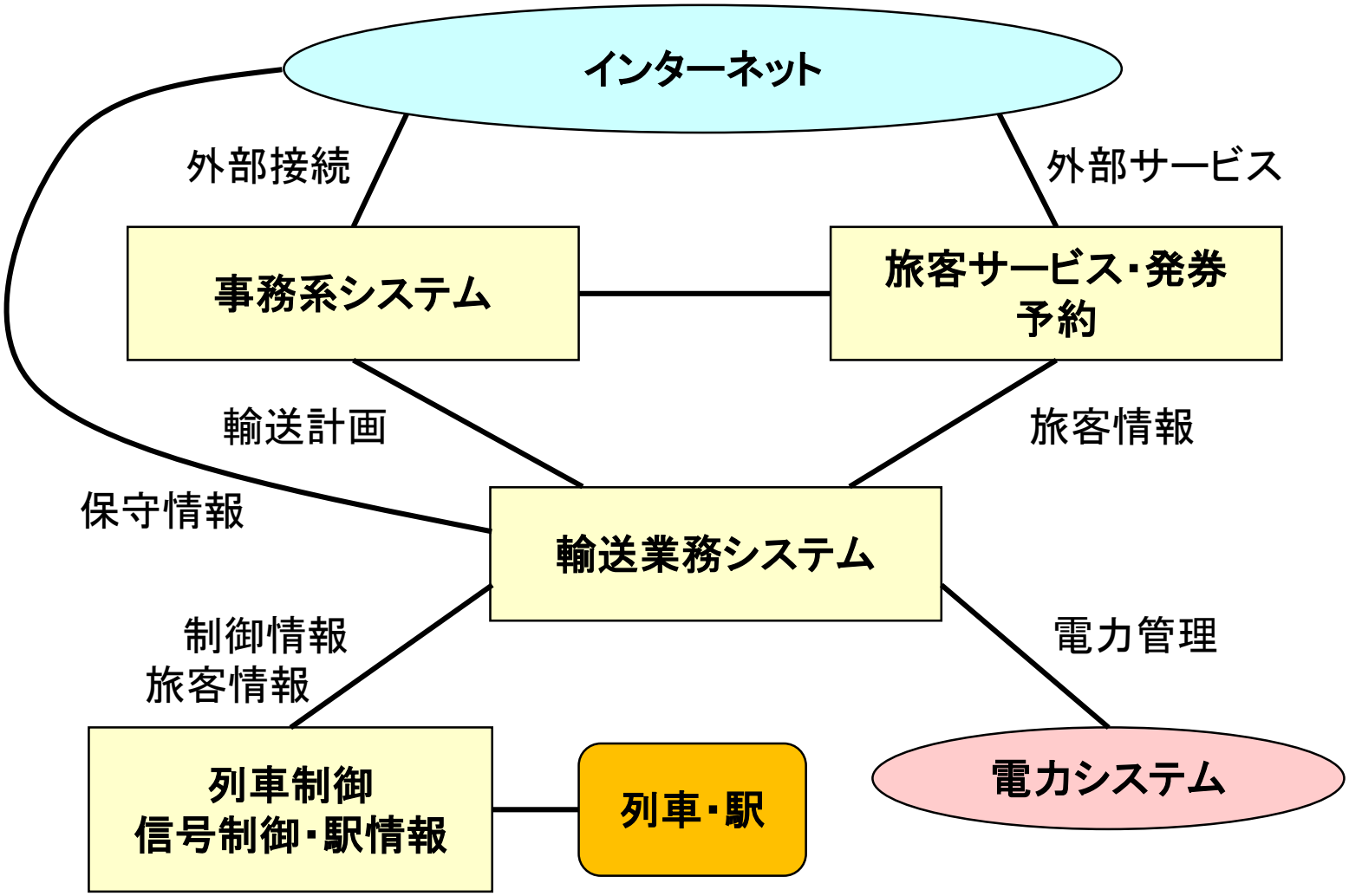
組織・企業における対策と管理

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、リテラシ
  - 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

5. 交通システム

A) 鉄道システム
   A) システム構成、特有技術、脆弱可能性
B) 航空システム
   A) システム構成、脅威可能性、管制、分析



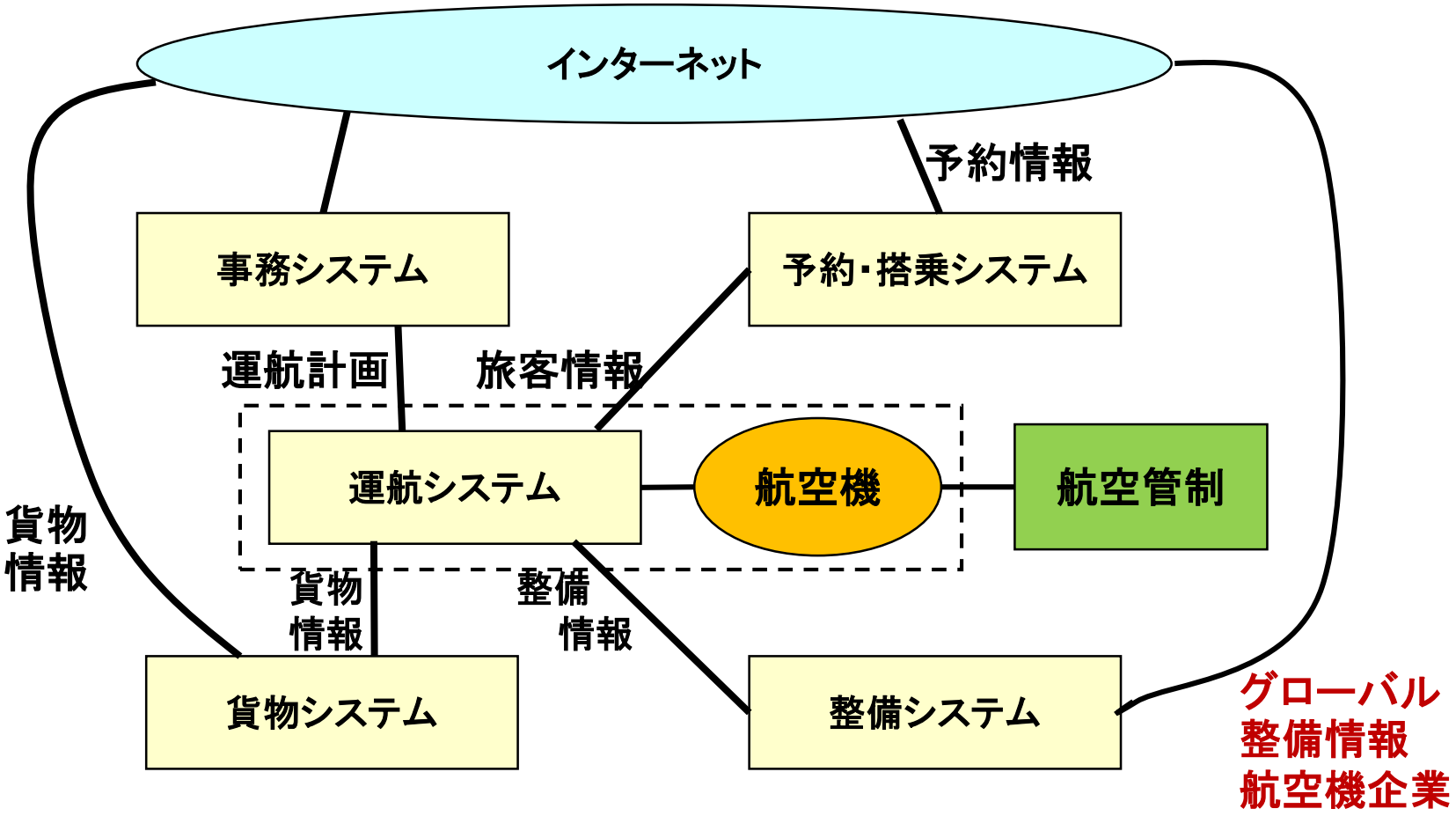
A) 列車事業の概要とシステム間情報接続

特有のアシュアランス技術

- 連動装置：列車存在による転轍機のロック
  - 物理的確実性の確保
- アシュアランス技術
  - 異種性：ダイヤや旅客案内等の情報系と列車の制御系の混在、長期的導入に伴う新と旧システムの共存性
  - 適応性：改修・変更・移行等、状況変化にシステムが対応する能力、システム稼働中にテスト可能
- 情報系と制御系のインタフェース
  - 表示系で終端し、人経由で制御+自動制動機構
  - 優れた構造だが、複雑化と新サービスへの対応は今後
  - 情報系・物理系攻撃によるサービス低下・混乱対応

鉄道事業システムの脆弱可能性

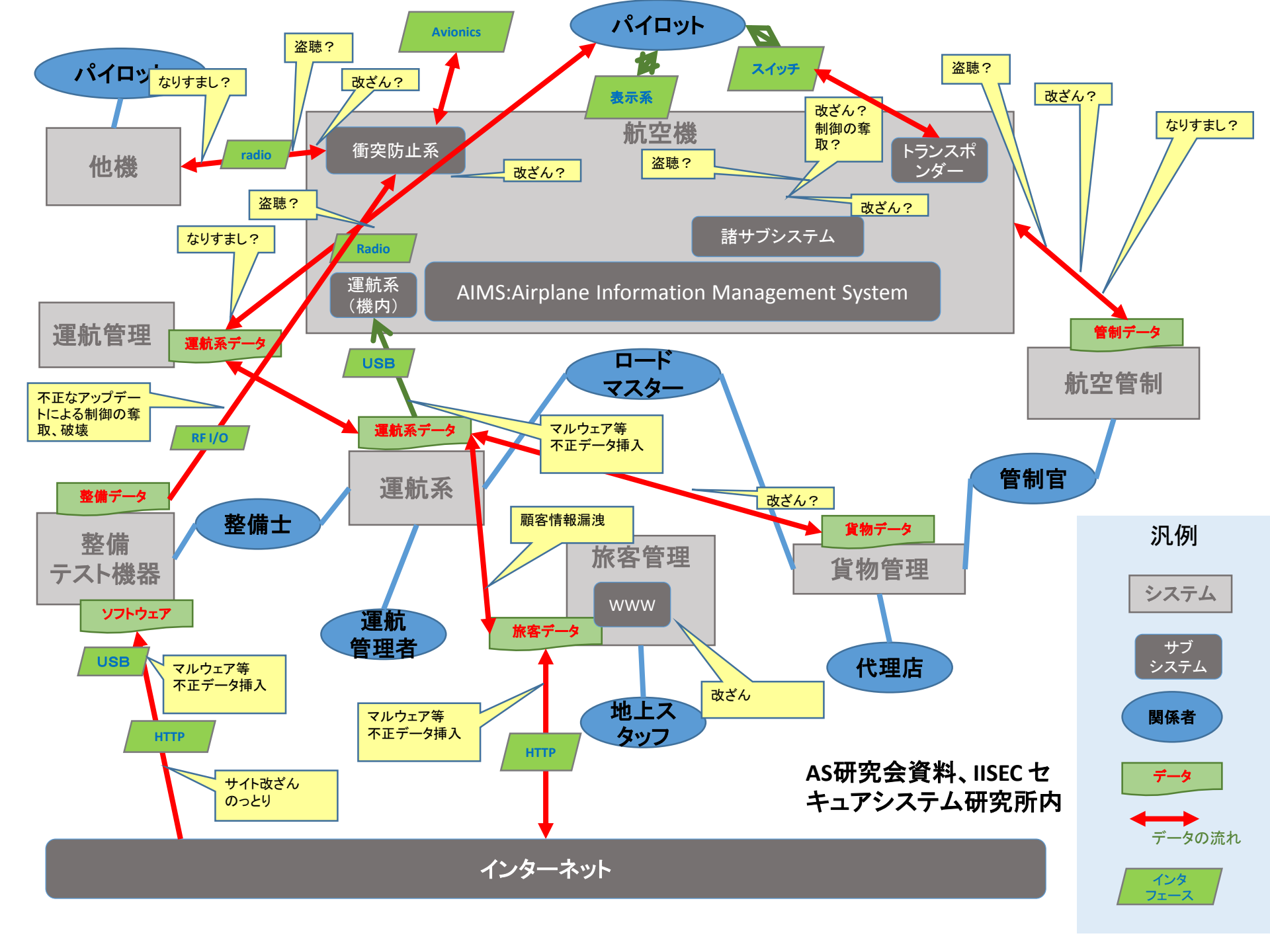
- 要素システムの脆弱性
  - 列車制御・運行システム
  - 事務系統システム
  - 旅客システム：切符、座席情報
- 脅威
  - クローズドシステムに対する内部犯行：信号制御、列車制御、運行計画擾乱、電力系攻撃
  - 旅客サービス攻撃による混乱
  - USB経由の攻撃
  - オープン系システム利用と外部接続：長期利用による脆弱性の内在潜伏
  - 事務系統への攻撃からの間接影響



B) 航空事業のシステム構成と情報接続

航空システムの脅威可能性

- パイロット、関係者の内部犯行
- 整備系への攻撃：インターネット経由、不正データ挿入、サイト改竄・乗っ取り、不正アップデート
- 旅客管理への攻撃：インターネット経由
- 運航系への不正データ挿入
- 航空管制への攻撃：ADS-Bの脆弱性、なりすまし、改竄、GAO報告
- 事務系への攻撃で間接的影響：欠航ポーランド


パイロット
パイロット
Avionics
盗聴？
なりすまし？
改ざん？
表示系
スイッチ
盗聴？
改ざん？
なりすまし？
他機
radio
衝突防止系
航空機
改ざん？
制御の奪取？
トランスポンダー
盗聴？
改ざん？
盗聴？
諸サブシステム
なりすまし？
Radio
運航系（機内）
AIMS:Airplane Information Management System
運航管理
運航系データ
管制データ
航空管制
USB
ロードマスター
不正なアップデートによる制御の奪取、破壊
RF I/O
運航系データ
マルウェア等不正データ挿入
運航系
整備データ
整備士
改ざん？
管制官
顧客情報漏洩
貨物データ
整備テスト機器
旅客管理
貨物管理
www
ソフトウェア
運航管理者
旅客データ
代理店
USB
マルウェア等不正データ挿入
マルウェア等不正データ挿入
改ざん
地上スタッフ
HTTP
HTTP
サイト改ざんのっとり
インターネット
AS研究会資料、IISEC セキュアシステム研究所内
汎例
システム
サブシステム
関係者
データ
データの流れ
インタフェース

GAO Report January 2015

- US Government Accountability Office
  - INFORMATION SECURITY: FAA Needs to Address Weaknesses in Air Traffic Control Systems
  - http://www.gao.gov/assets/670/668169.pdf
- 対象：NAS(National Airspace System：米国の航空交通管制を担うシステム)全般
- 4点の脆弱性

  1)高/低セキュリティシステム間境界の保護が貧弱
  2)一貫性のない利用者識別認証
  3)機微情報の暗号化対策の欠如
  4)貧弱なパッチ管理
  5)監査、監視活動の欠如

6. 今後に向けて

- 攻撃側の世界
- サイバーセキュリティ人材
- 推奨対策の参考資料
- まとめ

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
  - 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

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, GSOC, Telecom ISAC, IPA
    - グローバル：FIRST(信頼化されたCIRTの国際組織、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

推奨対策の参考資料

- サイバーセキュリティ経営ガイドライン　V1.0
  - 経済産業省、IPA: 2015.12.28
  - サイバーセキュリティ経営3原則:
    - リスク認識・全関係企業対策・適切コミュニケーション
  - サイバーセキュリティ経営の重要10項目 : 幹部指示
  - サイバーセキュリティ経営チェックシート
- 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

まとめ

- サイバーセキュリティの現状
  - 歴史、攻撃パタン、防げない、閉じた網はあり得ない
- 交通分野における現状と問題
  - ITシステムとの差異（制御系とのリンク、長期システム）
- 経営に関わる重要問題
  - リスクの認識、他に放り投げ不可、事故発生時、会社が責任を負う。管理範囲外は理由にならない
- 今後のセキュリティ
  - 交通分野ISACの設立、問題の共有の重要さ（自社に閉じるセキュリティは過去のモード）
- 協力して対抗

おわり