サイバーセキュリティ問題と私たちの生活

2015年11月19日

田中　英彦

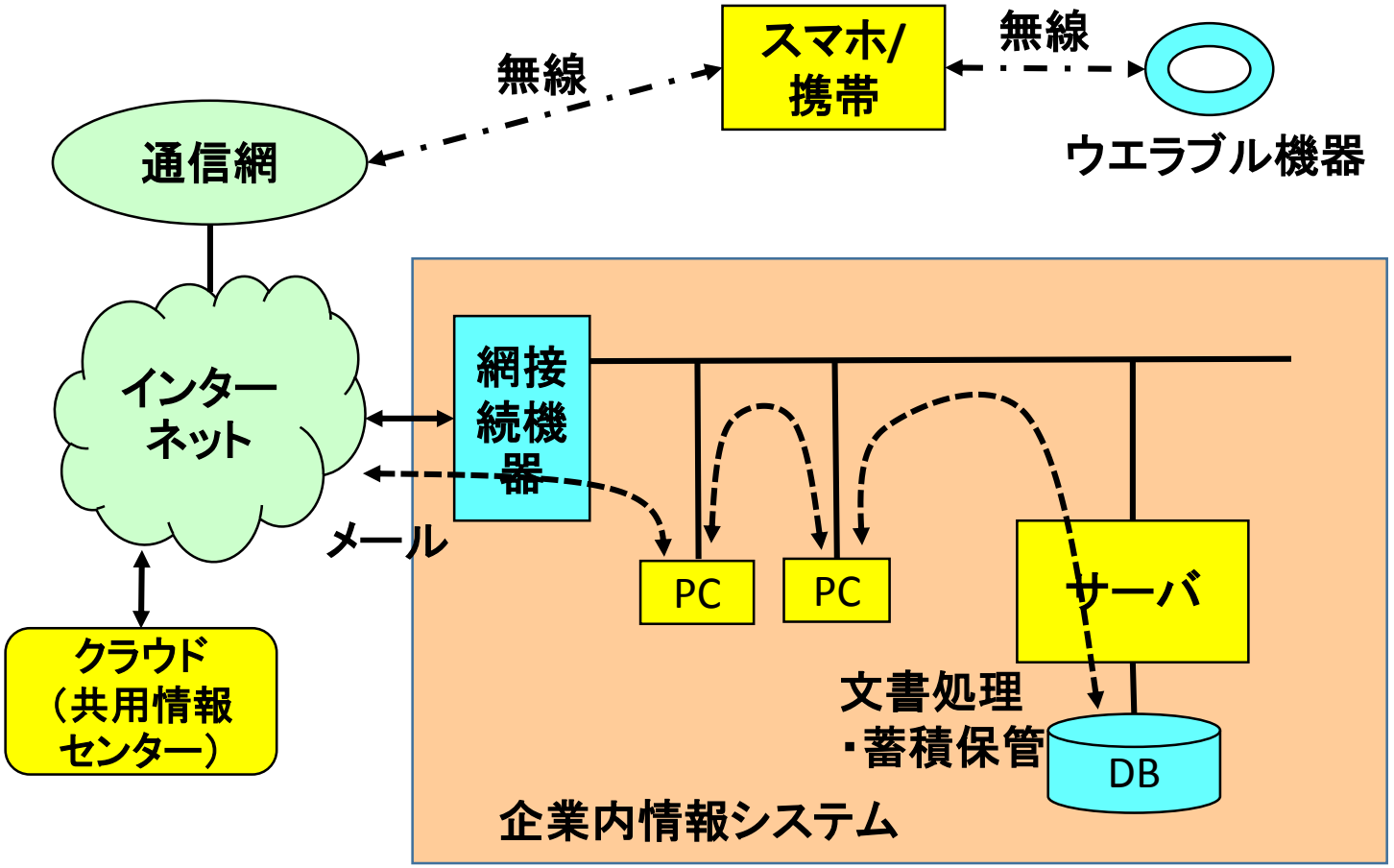
情報セキュリティ大学院大学

目　次

1. 情報社会
2. サイバーセキュリティ問題
3. 情報社会の発展
4. 社会を護る仕組み
5. 安全・安心な社会を目指して

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: 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

e文書法：電磁的記録

- 2004.11 制定、2005.4施行：商法や税法で保管義務のある文書の電子化保存。紙保存前提を、電子的作成した文書の、電子データによる保存を許容
  - 領収書や契約書のうち、額面が3万円未満のみスキャナ保存可能。税務署長の承認要す。入力者の電子署名が必要。タイムスタンプが必要。カラー画像での保存が必要
- 2015.3改正、2015.9施行：元々紙文書で作成した書類をスキャナで読み取ることで電子データに変換し、それを保存することも認められる
  - 金額基準廃止。承認不要。入力者の情報保存でよく電子署名は不要。タイムスタンプは必要。カラーもしくはグレースケールでよい。

実印から電子証明書へ

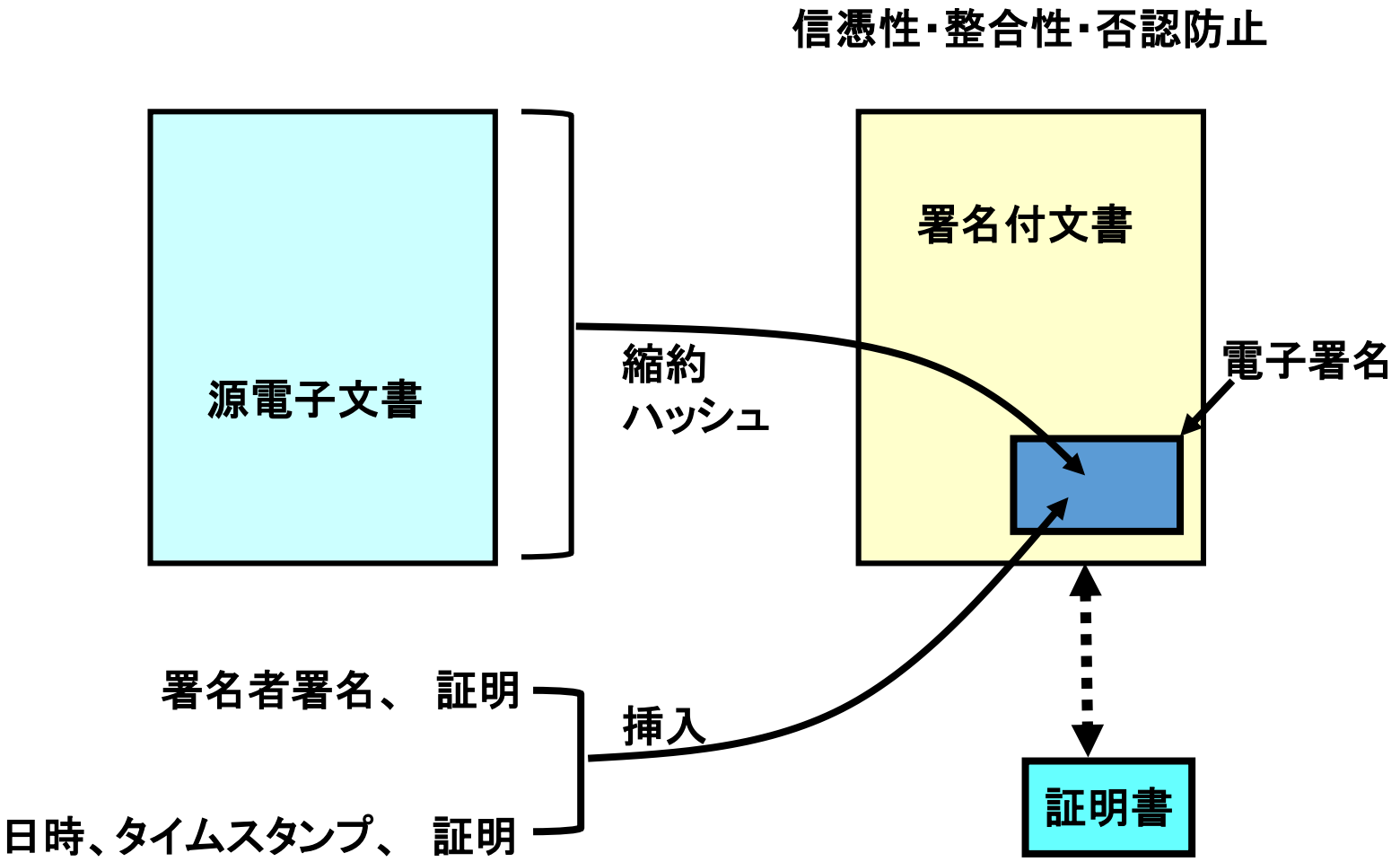
- 実印
  - 実印の保持と登録、契約書等に押印
  - 印影の提示、印鑑証明書提示
  - 正当な相手であることを証明
- 電子証明書方式
  - 電子証明書の登録（公的機関やサービス提供者へ）、秘密鍵の保持（ICカード内等）、電子署名の利用
  - 公開鍵の提示、電子証明書提示
  - 正当な人であることを証明
  - PKI: public key infrastructure　公開鍵基盤、送信者が秘密鍵で通信文に電子署名をおこなうと、受信側は利用者の公開鍵で署名を確認できる

電子署名の利用

- 電子化文書利用推進でビジネス活性化
  - そのための電子署名関連技術の採用
- 国際的共通利用に向けて
  - 米国：訴訟における電子証拠（デジタルエビデンス）ベース
  - EU・日本：電子署名
- 電子文書形式と長期署名化
  - PDFファイル用の標準化、Adobe Reader/Acrobatへの採用
  - Word/Excel、Open XML/Open Documentなどへ
- トラストを創る
  - 電子文書やデータの信頼性は電子署名で
  - 時刻の信頼性はタイムスタンプで
  - 信頼点の信頼性はトラスト・リストで
  - クラウドの信頼性は電子認証で

タイムスタンプ

- 証明内容
  - ある時刻にその文書が存在していた(存在)
  - その文書は改竄されていない(完全性)
- 利用目的
  - 約款、実験データ、契約書、議事録、監査記録など
  - 電子申請、電子申告
- 技術: 標準化、タイムスタンプ局が発行
  - デジタル署名、ハッシュ関数、分散TSA
- 否認防止
  - 文書への署名を否認することを防止可能
- 歴史は浅いが技術的には成熟:今後の利用期待
- 証明書の期限切れ後、署名の正当性を長期に渉り確保:長期署名


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

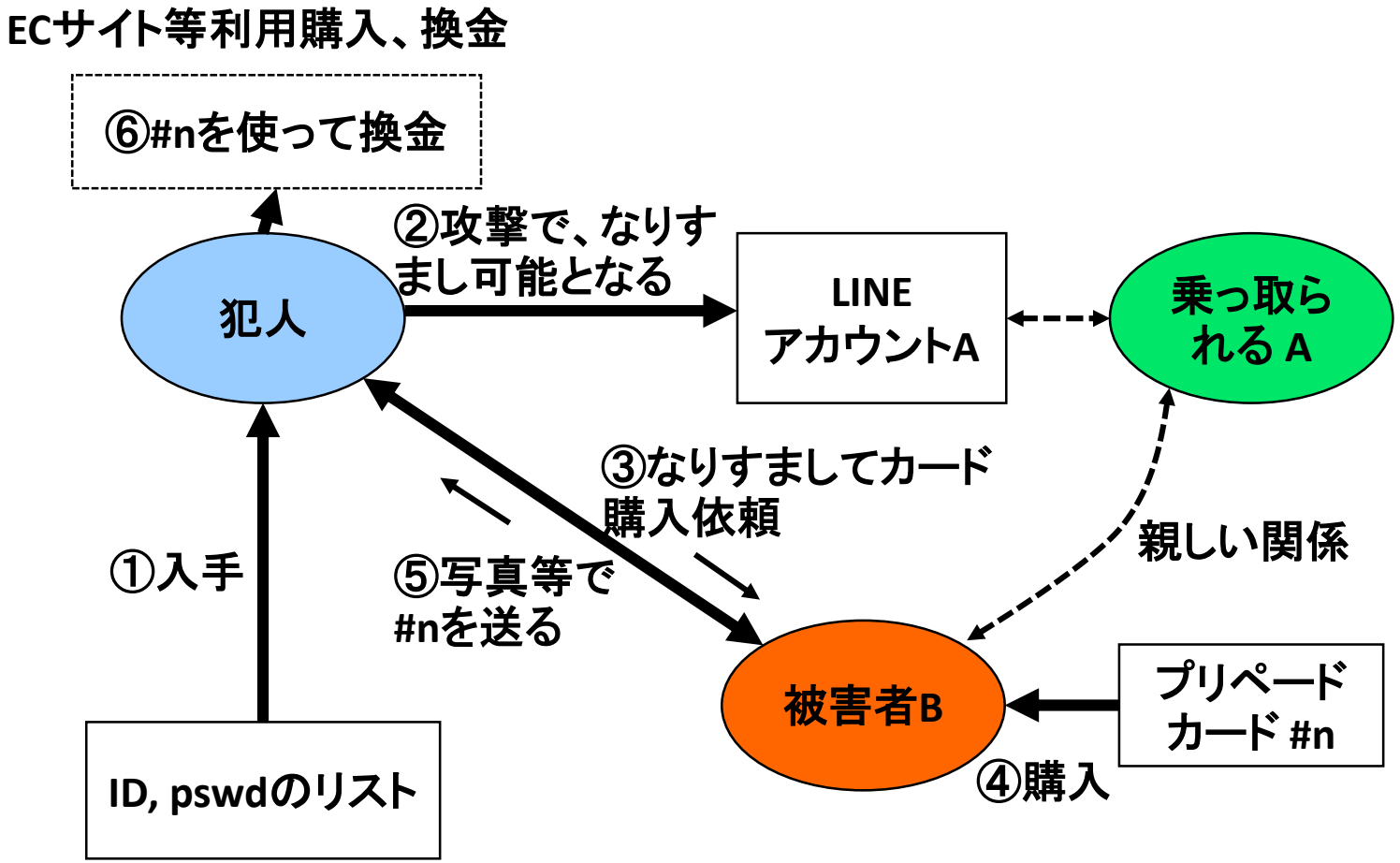
2. サイバーセキュリティ問題

- 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
- 資金窃取：なりすまし詐欺
- スパムと正規メール数：2対1

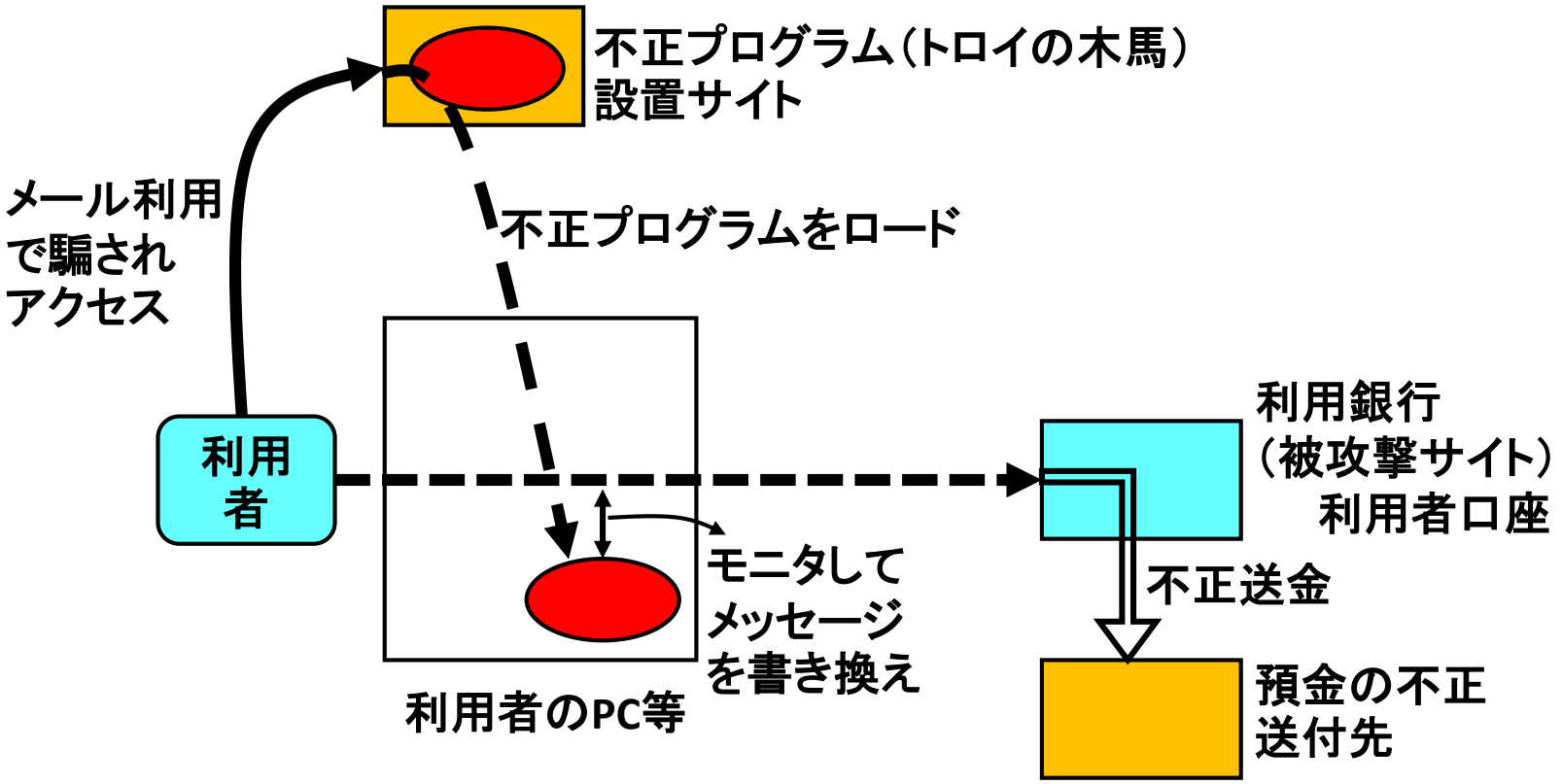
サイバー攻撃の変遷

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

LINE等乗っ取り


ECサイト等利用購入、換金
⑥#nを使って換金
②攻撃で、なりすまし可能となる
犯人
LINE
アカウントA
乗っ取られる A
③なりすましてカード購入依頼
⑤写真等で#nを送る
①入手
親しい関係
被害者B
プリペードカード #n
④購入
ID, pswdのリスト

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

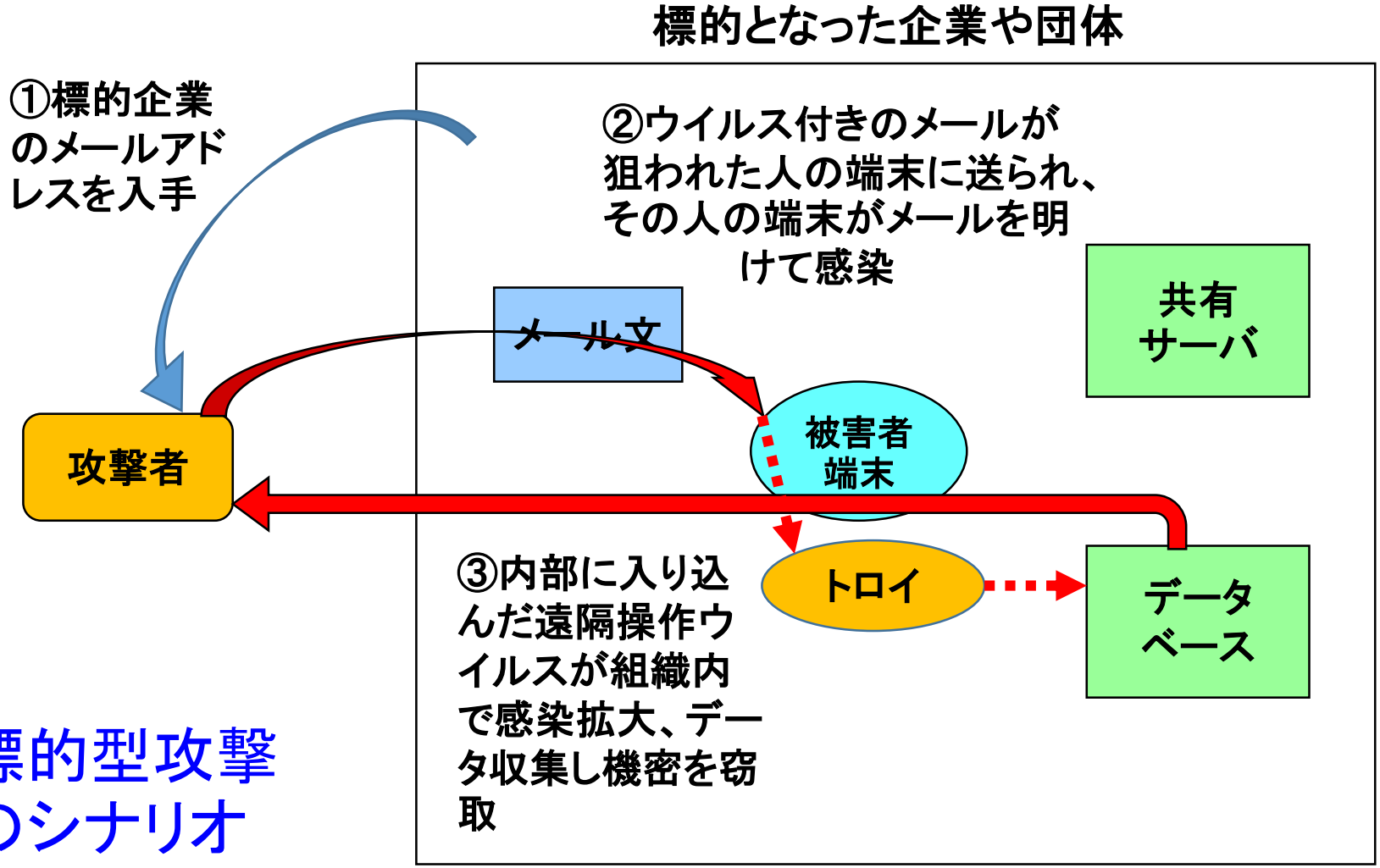
- 攻撃頻度と是正措置に必要なコスト増
- 結果：ビジネス機会の損失 157万ドル（133万ドル）
  - 異常な程の顧客離れ
  - 顧客開拓業務の負担増
  - 顧客からの評価の低下
  - 業務上の信用の失墜
- 対策コスト：99万ドル（76万ドル）
  - フォレンジック/調査活動、評価/監査業務、危機対応チームの管理、経営陣や取締役会との連絡
- 有効なインシデント対応には経営幹部関与が必要
  - 最高経営幹部の79%が認識（米、英）

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明けて感染
メール文
共有サーバ
攻撃者
被害者端末
トロイ
データベース
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

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

リスト型攻撃への対処

- リスト型攻撃
  - ID/PSWDの対が盗まれ市場に出回る。使いまわしが多いので攻撃が有効になる
- 対処
  - 予測：幅広いインテリジェンス
  - 防御：現実の脅威を意識したアセスメントと二要素認証やログモニタリングの実装
  - 検知：監視と分析
  - 対応：インシデント・レスポンス、初動トリアージ（状況確認と証拠保全）、フォレンジック解析、インシデント対応練習

Webサイトの防御

- 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：Webサーバ、Webアプリ、DB、メール、net、遠隔アクセス、通信、OS、等
  - OpenSSL, GNU bash, SSL version3.0
  - 正規のサイトを侵害し、サイト訪問者を監視し標的企業だけを狙う（水のみ場攻撃）
- 対処
  - ウエッブサイトの健康診断と対策：Check/Act/Plan/Do
  - Check(ログ調査、マルウエア診断、脆弱性診断）
  - OWASP(Open Web App. Security Project)の要件書利用等
  - 改善: 改竄検知システム、セキュアコーディング、WAF、定期診断ツール

オンラインサイトの電子証明書

- オンラインショッピング：150兆円/年
  - オンラインにおける信頼の基盤：デジタル証明書
  - サイバー犯罪被害額：13兆円/年（急増+50%）
  - 被害者数：3億8千万人
- 証明書の問題
  - 受信者が信頼できる場合に安全：証明書を欺く方法の存在
  - 認証局が証明を与える：ドメイン認証DV, 企業実在性認証OV, 拡張認証EVの3種
  - DVは、ドメイン名の使用権を示すのみで即発行。身元証明が無い。不正WebサイトSSLの78%がDV
  - ブラウザはDV/OVの区別をしないが、httpsの鍵マーククリックで判明
  - 業界団体がEVを開発：合法的企業であり、所在地が明らかである等、身元確認と、ブラウザに検証結果を視覚的に提供（緑色のアドレスバー）

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)
- 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

代表的な問題事案

- 偽メールへのウイルス添付
- 企業内システムへの侵入と情報窃取
- Webサイトアクセス時にウイルス感染
- 銀行アクセス時に偽サイトへ誘導
- 電力網攻撃で大規模停電
- 交通機関攻撃で列車停止、航空機墜落
- 国の機密情報窃取
- SNSでの誹謗中傷
- 家庭内空調・調理器具・鍵・自動車が攻撃対象
- 放置された脆弱なホームルータが犯罪の温床

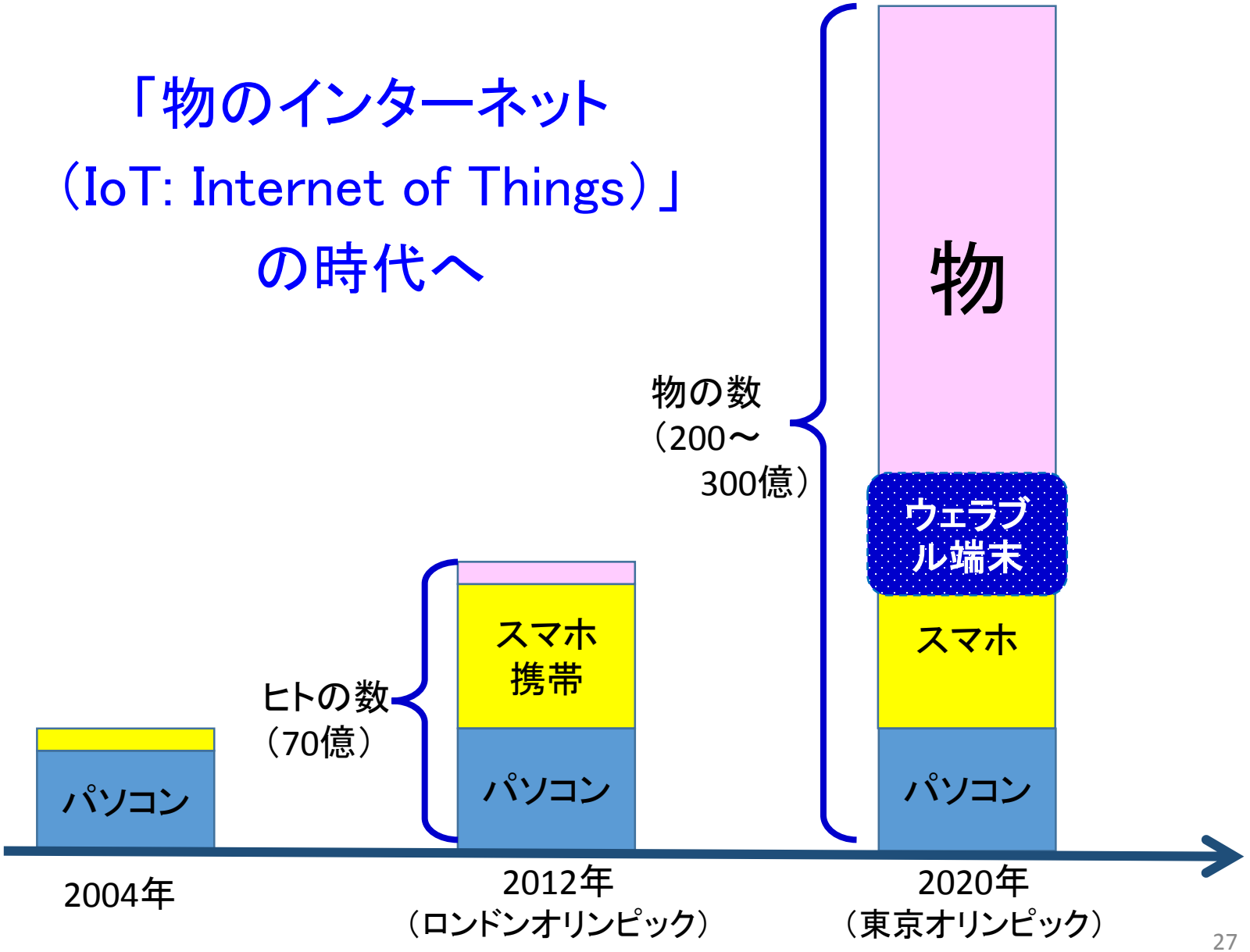
3. 情報社会の発展

- 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
  - 攻撃検知、対応に利用
- 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

組み込みシステムの発展と ソフトウエア開発費の増大

- 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

「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はセキュリティがキー

- 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

モバイル管理と対策

- 仕事/活動の変化
  - モバイルルータ、テザリングで、諸端末を場所や機種に依らず使う
- 必要機能
  - 多デバイス上互換性アプリと、通知による同期
  - 端末管理MDM：多様性への対応
- ソーシャルメディアSMSへの攻撃
  - Androidアプリ(100万)の17%が偽装したマルウエア、36%が迷惑なグレイウエア、モバイルマルウエアは7M個、四半期毎1M個増加、世界の感染率7%
- 対策
  - 社外からの安全なPC/タブレット利用環境
  - Wi-Fi 制御：アクセスポイントの限定
  - 社外ではVPN利用で、サーバのみと接続
  - アプリとコンテンツ管理の強化
  - 製品例：日立/FortiNET/CISCO/MobileIron社

クラウドの利用とセキュリティ対策

- クラウドによる生産性向上と問題
  - MS 365, Google Apps: サービス提供形態に影響
  - メールが脅威の開始手段：メールの25%にマルウエアへのリンクあり、漏洩（15%増、平均コスト$3.5M、顧客失う　医療・金融)
- クラウドをしっかり構築：2割が被害
  - クラウド上既存対策の限界:ウイルス/不正アクセス
  - 利用者による対策も必要不可欠：匿名化、秘密分散、次世代FW
  - 利用形態に応じたデータの使用許可、来歴調査
  - 機密やセンシティブデータの透明な活用：ポリシー明示で、あらゆるモノを強固に保存の一辺倒からの開放

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）
  - 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し遠心分離機破壊2010
  - 重要インフラを狙う攻撃：標的型攻撃の主要目標
- 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、影響範囲大

新しいリスクへの対応

- スマートxx の脆弱性
  - ビル管理、自宅、グリッド、自動車
- 自動車へのサイバー攻撃
- 医療機器への攻撃
- スマートホームへの攻撃
- リスク低減への考え方：
  - アセス・設計段階から考慮・運用、多層防御
- リスク管理手法
- 安心：高齢化社会、デジタルデバイド
- サイバーセキュリティリスク開示：有価証券報告書
  - US(連邦規則、開示ガイダンス), EU(開示検討）

リスク管理手法

- リスク要因：自然災害/パンでミック/情報セキュリティ
- ポイント：抽出し、3つの観点から抑える
  - 自社にとって重要なリスク（何を・何から・どう守る）抽出
  - 情報セキュリティ、事業継続、内部統制
- 情報セキュリティ
  - 機密性、可用性、完全性
  - セキュリティポリシー設定（取引先や契約者の機密情報、信用、情報資産の特定）
  - 責任と役割明確化
- 事業継続
  - リスクに優先順位で対応：経営者による判断
  - BCPの策定/訓練/回復と、継続的改善
- 内部統制

4. 社会を護る仕組み

- 技術
- 法制
- 管理
- 体制
- 脆弱性を長期に渉り保守可能とするエコシステムの確立
- 人の意識：リテラシ(ネット時代の常識)/信頼の輪

情報セキュリティ対策技術

① ネットワーク技術
- FW、IDS/IPS、プロキシ、VPN、無線LAN、UTM

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

③ 暗号：機密性、完全性、否認防止

④ 認証

⑤ 対策内容とシステム
- 入口対策、出口対策、内部活動分析
- WAF(Web対策）、イベントログ管理と実時間検知

企業における問題

- 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
  - 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にダウンロードした後は、セキュリティ無しになる
  - 情報が流出したら、回収できない

情報漏えいの防止機能

- ビジネス活動を制限せず漏洩を防ぐ仕組み
  - 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）を総合的管理し、漏洩を防ぐ
- 漏洩防止対策
  - 暗号化したファイルのみUSB/DVDにコピーできるように強制し、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のみの制御とする
  - 中央サイトで認証をかけ、それ無しに文書を開けない
  - 情報を社外と共有するが、必要な時点で閲覧の権利を失効させる。流出時、即失効できる
  - 流出の可能性がある操作を検知すると、システムが管理者へ報告を挙げる

セキュリティ情報イベント管理 SIEMと今後の適応型対策

- ネットワーク活動情報を収集・監視する
  - 高度解析手法、データ収集範囲と規模拡大により不自然な動きを実時間で検出
  - 他に必要な道具：可視化と、実施可能対応策の提供ツール
- 統合型セキュリティフレームワーク
  - 脅威の動向を広範囲で捉え、変化に素早く対応し柔軟な統合型対策
  - 完全防御に代えて、攻撃侵入の容認：攻撃の素早い検知と確実な対応を図る。復旧コストや社会的信用失墜等を阻止
  - 変化への柔軟な適応能力：アーキテクチャは迅速で柔軟に変更可能、全体は緊密に統合。内外から情報を収集・集約し、脅威の全容を把握する。攻撃を予測し事前対応体制

管理・運営

- 管理問題
  - CIA, RASIS, PDCA（インシデント・レスポンス）、内部不正
- ISMSとCSIRT組織
  - 情報分類、リスク特定、リスク評価、監査、CSIRT構築
- 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

企業内における緊急対策グループ（消防団）の設定

- CSIRT: Computer Security Incident Response Team
  - 攻撃検知、問題発生時に緊急対応、社内のセキュリティ指示系統監視組織、社外には統一した窓口
  - 他社のCSIRTとの連携、企業代表組織なのでセンシティブ情報を他社と共有が可能
  - 対応フローの事前整備、組織のセキュリティ対策と従業員のセキュリティ意識向上
- 状況
  - 大企業の4割以上は構築済み（19→42% 2014)
  - サイバー攻撃にセキュリティ担当者個人では対応困難
  - NCA(日本CSIRT協議会）に参加し、情報共有・連携

情報法制

- 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
- 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：実体との乖離、世帯単位と個人単位
  - ウイルス作成罪(2011)、フィッシング罰則(2012)
  - 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（事後拒否）→OPTT-IN（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
  - サイバーセキュリティの定義は狭い：警察と安全保障の線引きは今後詳細化

サイバー空間と法

- サイバー空間における法律の限界
  - サイバー空間は国境を越え、サイバー犯罪は匿名性が高く、法律の施行が困難
- 国家間におけるサイバー空間を規律する法体系
  - ICTを国家主権の発動として防衛に使えるか
  - 国家の強制執行であるハード・ローより、実質的法的規範となるソフト・ローや倫理教育の役割：民間資格、第三者または国際標準優位
  - 国際的ルール作り：インターネットで自由vs規制
  - 誤謬前提のリスク概念の受け入れ
- セキュリティは非常に広い問題を含む
  - 経済・産業政策、基本的人権、生命、標準のガバナンス、重要インフラ防御、サイバー戦争と防衛

5. 安全安心な社会を目指して

- 情報セキュリティは総合対策
- わが国の情報セキュリティの対応組織
- 組織間連携
- 組織内対策
- マイナンバー制度
- 結論的に言えば

情報セキュリティは総合対策：経営問題

- ネットワーク環境：設計・構築
- サービス環境：マシンの設計・設定
- 業務アプリケーションの設計・開発
- 運用・管理・保守・オペレーション
- トラブルシューティング
- 法制度、法律問題の準備・チェック・対応
- サーバルームの入退出管理、作業管理
- 権限許可、監視、記録管理
- 企業経営・事業継続・インシデント対策

わが国の情報セキュリティ対応組織

- 政府
  - 内閣サイバーセキュリティセンターNISC
  - 警察庁、防衛省、総務省、経済省
- 分析機関・対応・広報
  - JPCERT/CC, Security Operation Center, 専門企業
  - IPA, Telecom ISAC, ACTIVE, J-SCIP, JVN, JNSA, 制御システムセキュリティセンター, CSIRT, 日生研（CCW)
  - 国際組織：FIRST, Trusted Teamsの連携組織
- 研究・教育
  - 研究：NICT, 産総研, 大学
  - 教育：情報セキュリティ大学院大学、enPiT-Security

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

- Telecom/Financial ISAC Japan
- CEPTOAR
- J-CSIP
- IPA
- JPCERT/CC
- GSOC（政府）
- SPREAD
- JNSA-CERC
- 日本CSIRT協議会
- ISOG-J
- JC3
- LGWAN(地方公共団体）

組織・企業における対策

- 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
- ガイドライン等への対応：自己判断から第三者
- 政府等統一基準、IPAシステム設計ガイド、自治体向けポリシーガイド、Top 20 CSC、OWASP要件書2.0
- マイナンバー対応
- 定期的チェックと改善

組織とデータを護るベース

- 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
- 評価/レビュー/監査：組織の活動と関係他社、顧客関係をみながら
- クラウド利用時は信頼できる業者

マイナンバー制度

- 3分野で制度運用開始
  - 社会保障、税、災害対策の行政手続き
  - 利用開始後、民間事業者は税や社会保障の手続きで、マイナンバを記載する（個人12桁、法人（自由）13桁）
- スケジュール
  - 2015年10月半ば、マイナンバー通知
  - 2016年1月運用開始
- 義務
  - 手続き電子化対応：政府・自治体、税務・年金・健康保険・雇用保険に関し、人事・労務・経理・ICT業務
  - マイナンバー記載された書類は特定個人情報
  - 委託先監督義務：委託者と同等の方針・取扱規程
  - 安全管理措置：機密保護、データベースの管理、電子署名・電子認証の利用

マイナンバー制度の必要性

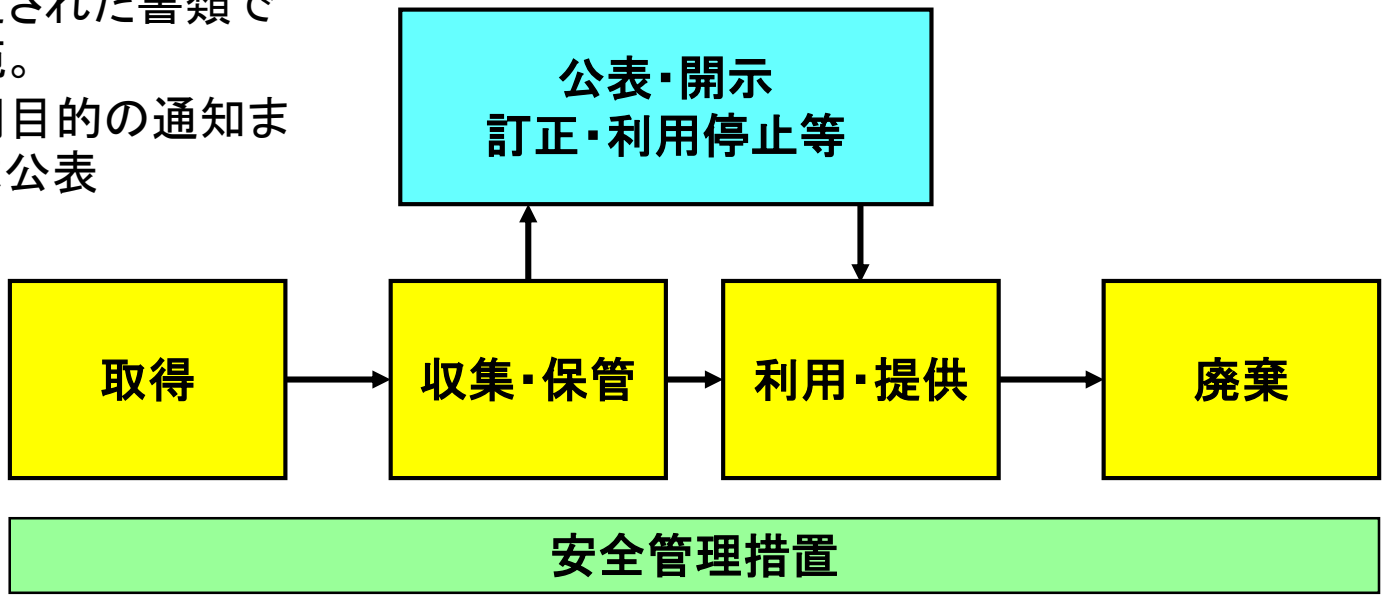
- 情報社会の基盤
  - 人を正しく社会の中で位置づける
  - 活動を効率的に認証する(紐付ける)
  - 税・社会保障・住民基本台帳、利便性
  - 強いセキュリティ維持:分散管理、セキュリティ技術
- 過去の紙ベースシステムの問題
  - オフラインのみで迅速性・機械処理が不可能
  - コピーされて悪用されると追跡不能
  - 実印の認証は困難:偽造できる
  - 紙の安全神話からの脱却:新社会
  - 人処理ベースでコスト膨大

マイナンバー対応に向けて

- 企業のセキュリティ対策
  - 技術対策、既存IT資産管理
  - マイナンバー情報（特定個人情報）の厳重管理：不正利用に重い罰則、信用失墜、社員への責任問題
- IT資産管理
  - 重要情報の識別と管理、管理コストの増大
  - IT端末管理
  - 管理機能のクラウド化：物理サーバ廃止、管理負荷・コスト削減、一元管理可能
  - マイナンバーファイル：証跡管理用ログ管理（アクセス履歴、利用履歴管理）

厳格な本人確認:
なりすまし防止、
番号取得時に番号確認と身元確認を規定された書類で実施。
利用目的の通知または公表

従業員家族のマイナンバー取得:扶養控除申告書、家族の本人確認を行って事業主へ提出義務
マイナンバーを扱うルール整備
保管:法で規定された事務に使う目的のみ



例:個人番号カード、通知カードと運転免許証、代理人の場合も

必要無くなり、法令の保存期間経過後は、速やかに廃棄

マイナンバー取り扱いの各フェーズ

安心安全な社会を築こう

- 今後の社会は情報ベース：距離・時間を越える
- 明るい未来はセキュアな情報システム・ネットがコア
- セキュリティ機器は問題を減少させる有効手段
- 完全は無い。問題発生対応の準備　保険の利用
- セキュリティ犯罪対応法制：情報の本格組込
- セキュリティ問題は時変、未知への対応
- セキュリティを若いときから常識化・重要な人材育成
- トラスト（信頼・信任・信用）の重要性
- 人の信頼の輪を形成：内部不正を減らす
  - 不正のトライアングル（機会・プレッシャ・正当化）
  - 疑う社会ではなく、信頼社会の再構築

おわり

ご清聴、ありがとうございました