サイバーセキュリティの現状と課題

2015年11月2日

田中　英彦
情報セキュリティ大学院大学
学術会議会員（19-21期）連携会員（22-23期）

目　次

1. 情報セキュリティの現状
2. 今後の社会：情報社会の発展
3. サイバーセキュリティ問題と課題
4. 安全安心な社会を目指して
5. 求められるセキュリティ人材と研究活動

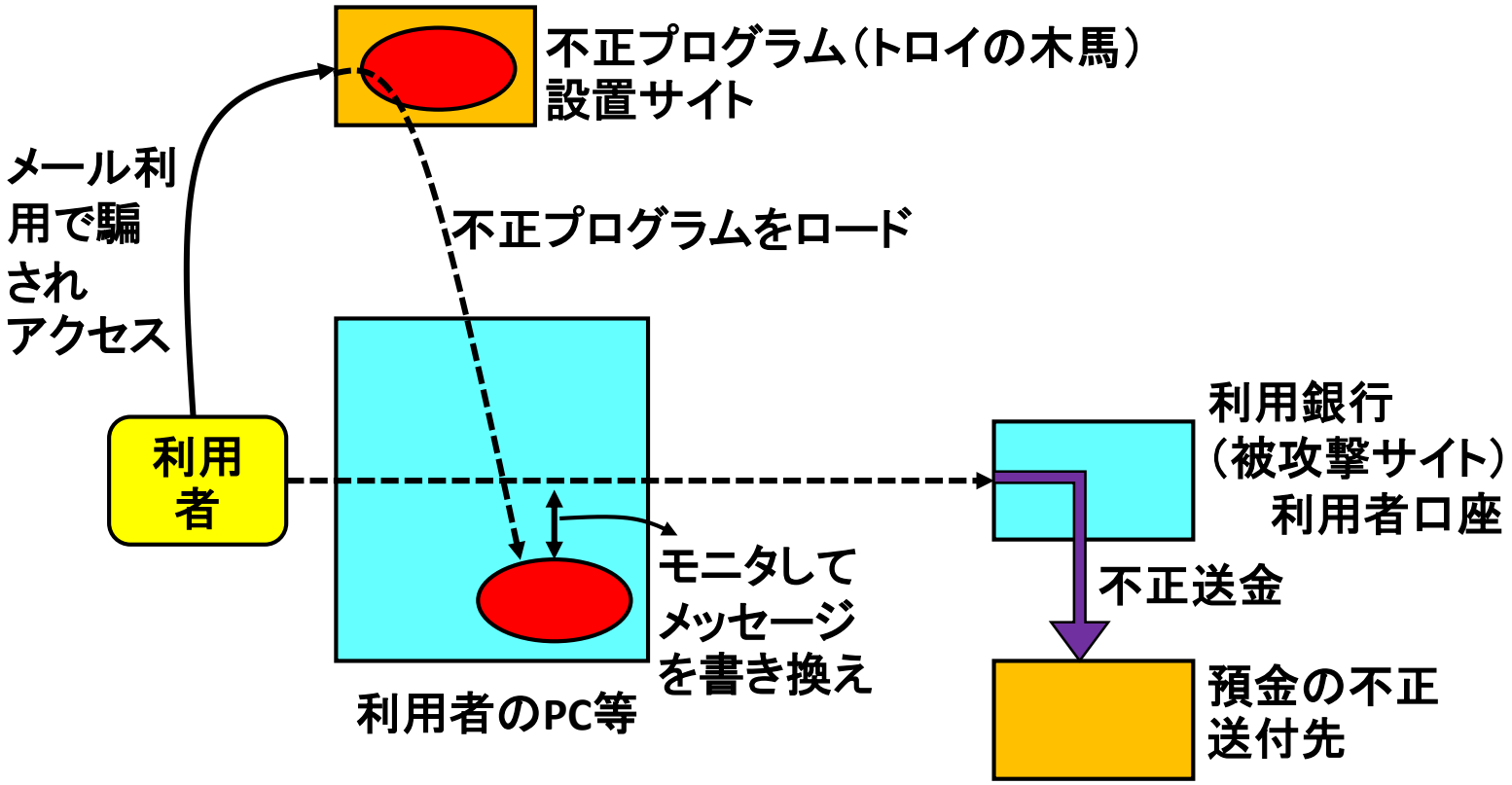
1. 情報セキュリティの現状

(1) サイバー攻撃の変遷
(2) 金融機関の預金を狙うトロイの木馬
(3) 世界の情報漏えい件数
(4) 標的型攻撃
(5) リスト型攻撃への対処
(6) Webサイトの防御
(7) ランサムウエアの増加

(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

(2) 金融機関の預金を狙うトロイの木馬



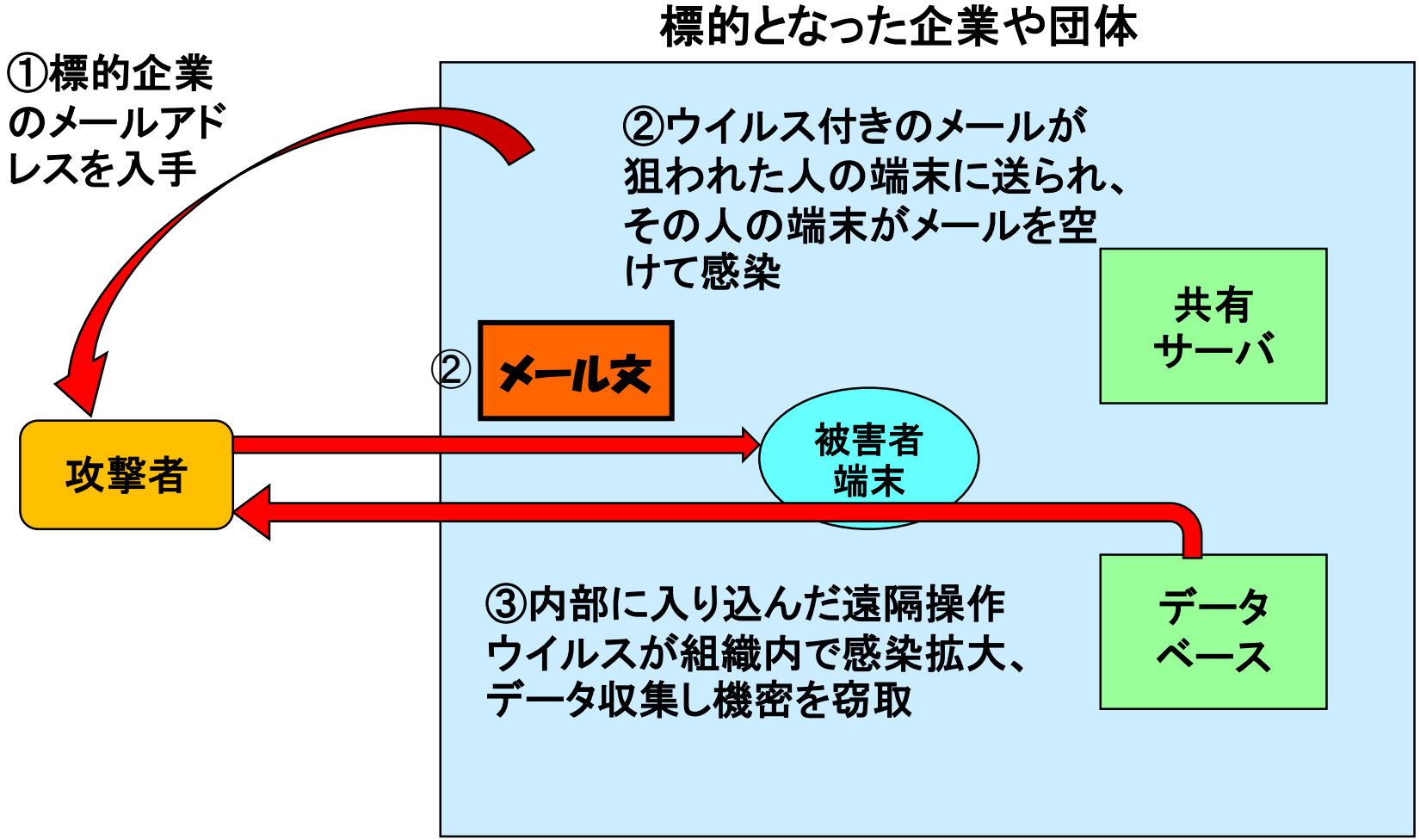
(3) 世界の情報漏えい件数

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

(4) 標的型攻撃

- 60%が中小企業を対象
  - 中小企業は、対策に多くの資源を投資することが困難
  - 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、ダウンロードを待つ
- 対策: 完全防御は不可能、侵入事後策
  - 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

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



標的型攻撃のシナリオ　280日継続

(5) リスト型攻撃への対処

- リスト型攻撃
  - ID/パスワード等が盗まれ市場に出回る。使いまわしが多く攻撃が有効
- 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（FW, IDS, anti-Virus, WAF)と分析(脆弱性、セキュリティイベント管理、ログ管理、SOC分析）
  - 対応：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、インシデント対応シミュレーション

(6) 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）
  - 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、標的にした企業だけを狙う（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）
  - 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
  - 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

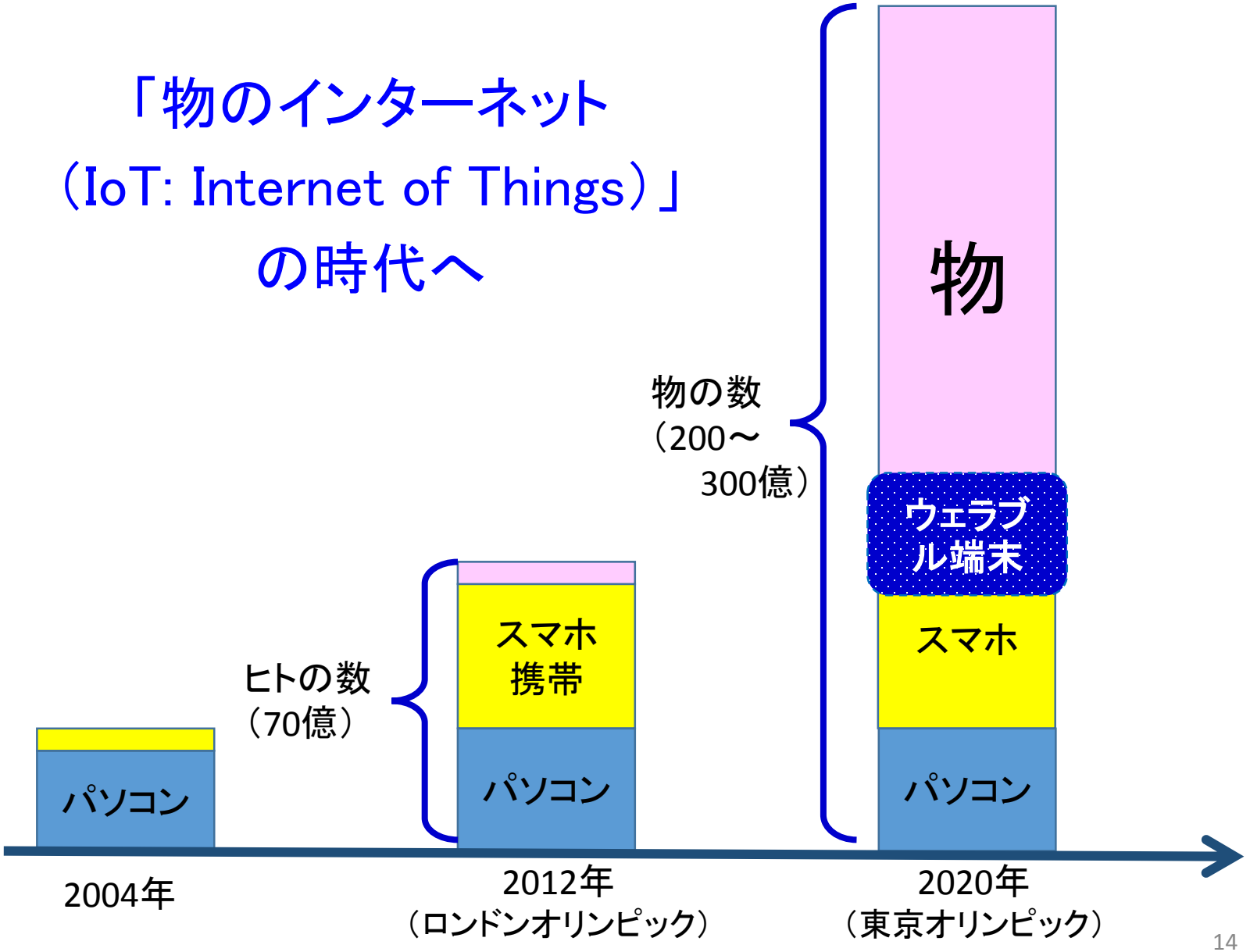
(7) ランサムウエアの増加

- 裕福な国のユーザを対象
  - これらの国の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デバイスのデータを暗号化するランサムウエア）、大規模ストレージ攻撃
  - NASサーバのパッチ未使用の脆弱性を攻撃、RSA 2048/256bit鍵使用でサーバ上全データ暗号化、楕円暗号利用も
- 対策
  - データバックアップ、セキュリティ意識を高めフィッシングに対抗する、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

2. 今後の社会：情報社会の発展

- あらゆるモノが繋がる
  - IoT: センサ、機器など、市・インフラ・ビル・交通・工場・医療福祉・生活に影響
  - 機器が電子化されネット接続：更新、ウエラブル、組み込み
- 新プラットフォーム
  - メインフレーム⇒LAN/Internet⇒クラウド
  - Mobile Devices：スマートフォン、タブレット
- クラウド, BigData, AI　の利用
  - コストと対応迅速：外部システム＋内部システム
  - 大規模公共データ公開、分析・利用で効率化
- 社会トレンドのキーワード
  - 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
  - 無線接続普及で接続機能を持つスマート製品
- スマート製品の力
  - 新機能、信頼性や稼働率の格段向上、製品間連携で高い機能性
  - 業界構造と競争のあり方を変え全く新しい産業を生成
  - 戦略面で新しい選択肢：価値創造確保、生み出す膨大データの活用・管理、販売チャネルの見直し、企業の役割変化
- モノの本質が変化
  - 競争新時代の到来：スマート製品増大と、それが生み出すデータ
  - IT: 機能性と性能向上は利用状況の膨大データから実現。生産過程では新業務、バリューチェーンが変わり、生産性向上の波

IoTにお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

OWASP IoT Top10

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

出展　OWASP Web応用の団体、
Internet of Things Top Ten Project

3. 今後のサイバーセキュリティ問題

(1) モバイル環境
(2) クラウドの利用
(3) 新たなリスクへの対応
(4) 重要インフラや国家への攻撃

(1) 安全なモバイル環境の設定

- 社外からの安全なPC/タブレット/スマホ利用環境
- Wi-Fi 制御
  - 企業：許可されたアクセスポイントのみの利用を、システムレベルで強制する。許可されていない他のAPを表示させない。3G, LTEでも同種運用
  - 公衆設備：各所の設備をセキュアに
- VPN利用
  - 社外では、VPNサーバ以外とのネットワーク接続を禁止し、社内ネットワーク経由のアクセスのみを許可
- 多くの製品

(2) 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
  - 利用の発展
  - 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
  - 集中によるデータの散在を防ぐ
  - セキュリティ維持：匿名化、秘密分散、グローバル新攻撃情報分析と利用（リンクスキャン、ポリシ設定）
  - 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することからの開放

(3) 新たなリスクへの対応

- 新機器 の脆弱性： ビル管理、グリッド
- 自動車・航空機へのサイバー攻撃
- 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： Security by Design
  - アセス・設計段階から考慮・運用、多層防御
- リスク管理手法の採用
- 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）
- 安心：高齢化社会、デジタルデバイド

(4) 重要インフラや国家への攻撃

- エネルギー部門
  - 標的型攻撃の主要な目標、世界各国の攻撃対象上位５部門
  - 新しいガス田地図、効率的な太陽光発電技術など価値ある情報の窃取、制御システムの混乱、評判を落とす
- 現状と今後
  - 無防備なシステム：オンラインとオフライン
  - 新しい攻撃経路：スマートグリッド
- 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

4. 安全安心な社会を目指して

(1) 情報セキュリティは総合対策
(2) 情報セキュリティの対応組織
(3) 適応型サイバーセキュリティ対策
(4) 管理と法制

(1) 情報セキュリティは総合対策

- 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

(2) 情報セキュリティ対応組織

- 政府
  - 基本法(2014.11公布・施行)、戦略本部設置(2015.1)、内閣サイバーセキュリティセンターNISCへ改組(2015.1)
  - 警察庁、防衛省、総務省、経済省、外務省
- 分析機関・対応・広報
  - JPCERT/CC, Security Operation Center, 専門企業
  - IPA, Telecom ISAC, ACTIVE, J-SCIP, JNSA, CSSC, JC3, 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：大学、enPiT-Security、専門企業

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、セキュリティ発生時に緊急対応、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などとの連携、企業代表組織なのでセンシティブ情報の他社との共有が可能
  - 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

(3) 適応型セキュリティ対策

- 旧来手法の限界
  - 発生状況の全体像把握困難
  - 脆弱性報告後4時間以内に、多くの攻撃発生
- 適応型セキュリティ・フレームワーク
  - 脅威の動向をグローバルチェック
  - 攻撃の素早い検知と確実な対応
  - 変化への柔軟な適応能力：攻撃予測で事前対応体制
- 対策の設置形態
  - 社内対応、外部委託

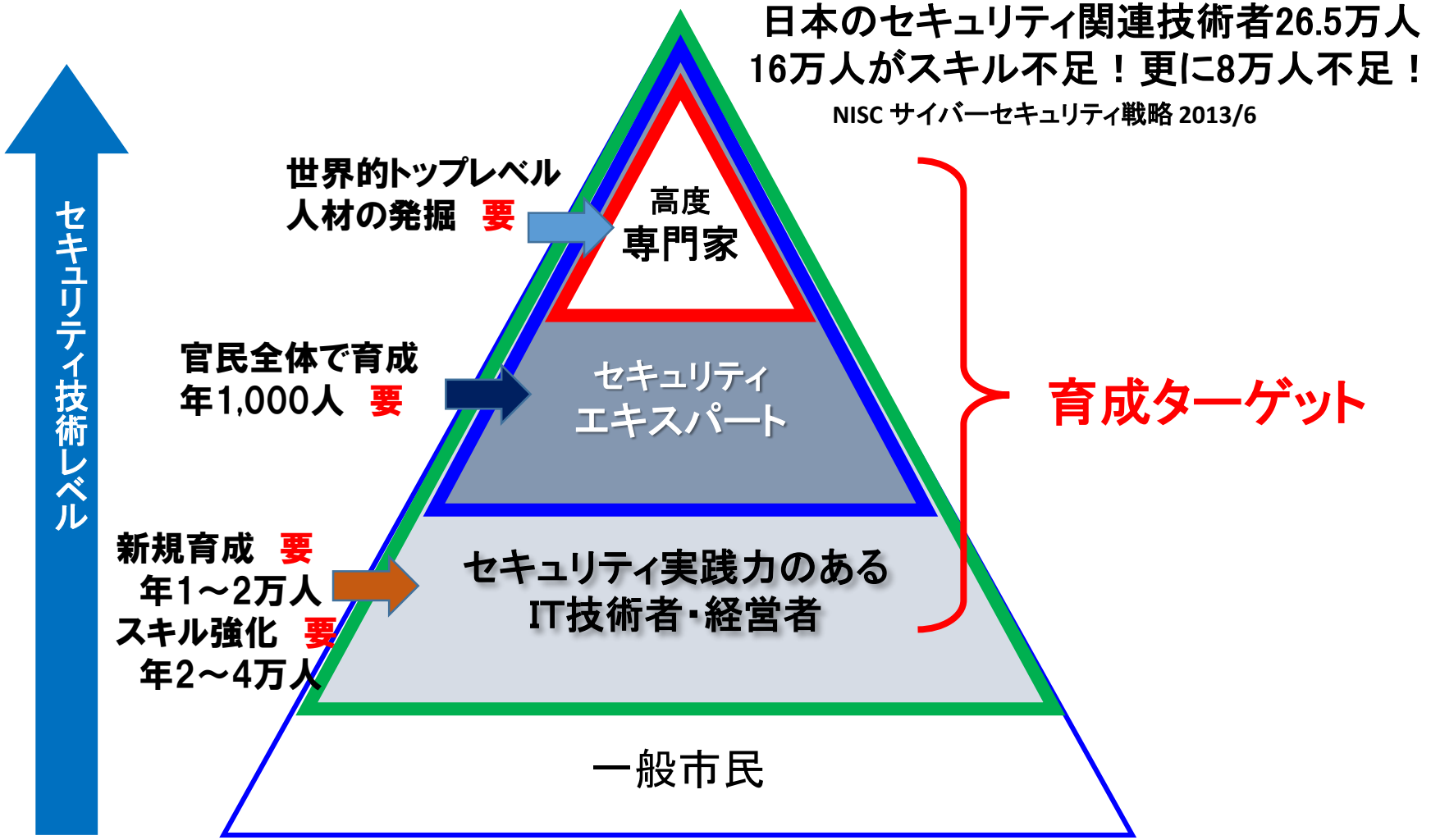
(4) 管理と法制

- 管理問題
  - CIA, PDCA、内部不正、ISMS、CSIRT構築、評価基準
- 外部委託の限界認識
  - ITリスクを制御するのは経営者の責任
- 最期の砦：保険
  - サイバー攻撃保障、個人情報漏洩保障、ネットワーク総合、e-リスク保険
- 情報技術の特殊性（物理と異なる）と製造物責任法（PL法）
- 国内対応
  - 電気通信事業法、信書のガイドライン
  - 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）
  - 個人情報保護改正、マイナンバー法（情報化の基盤）(2015)
- 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

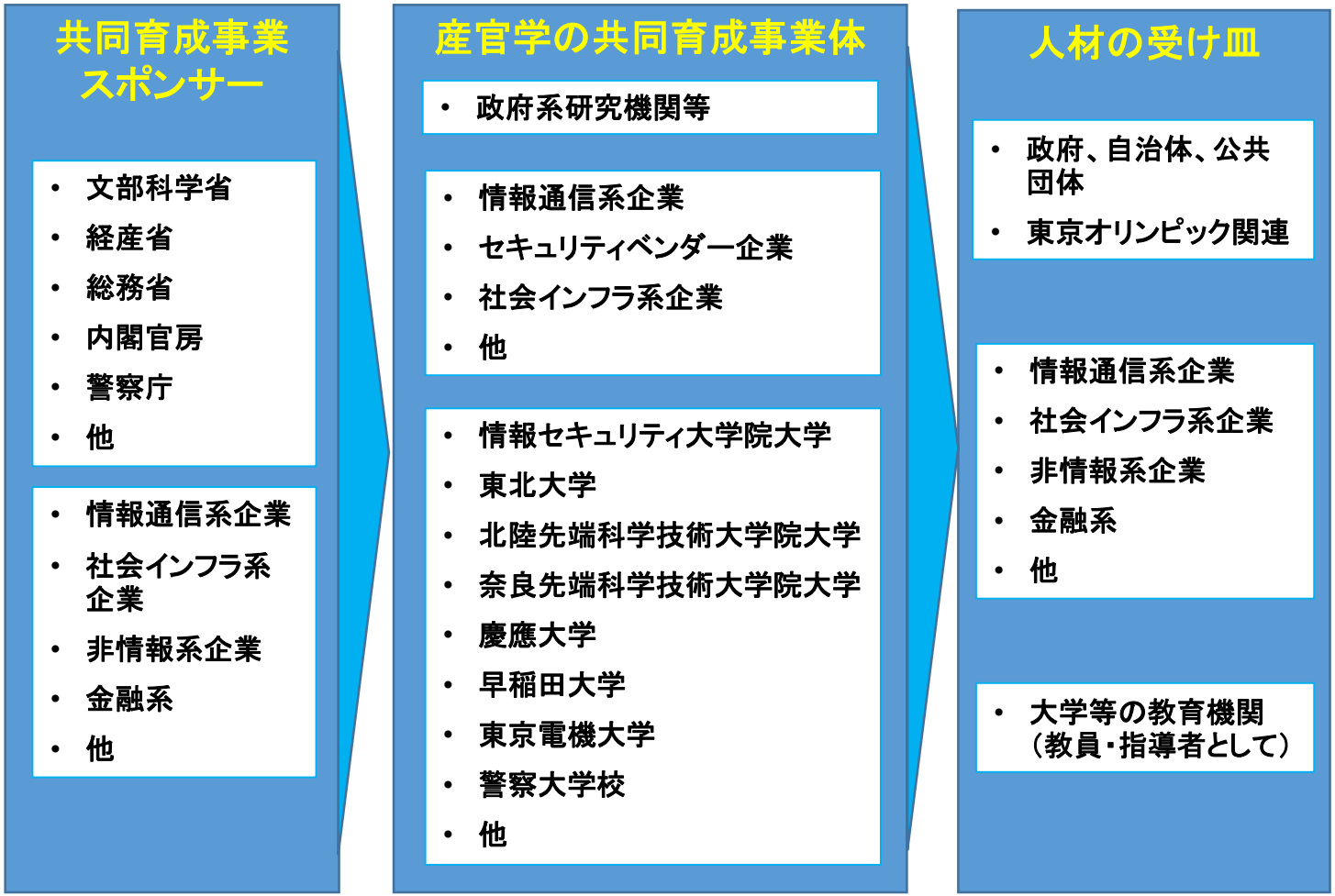
5. 求められる情報セキュリティ人材と研究活動

(1) 情報セキュリティ人材

- 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


日本のセキュリティ関連技術者26.5万人
16万人がスキル不足！更に8万人不足！
NISC サイバーセキュリティ戦略 2013/6
セキュリティ技術レベル
世界的トップレベル
人材の発掘 要
高度
専門家
官民全体で育成
年1,000人 要
セキュリティ
エキスパート
新規育成 要
年1～2万人
スキル強化 要
年2～4万人
セキュリティ実践力のある
IT技術者・経営者
一般市民
育成ターゲット

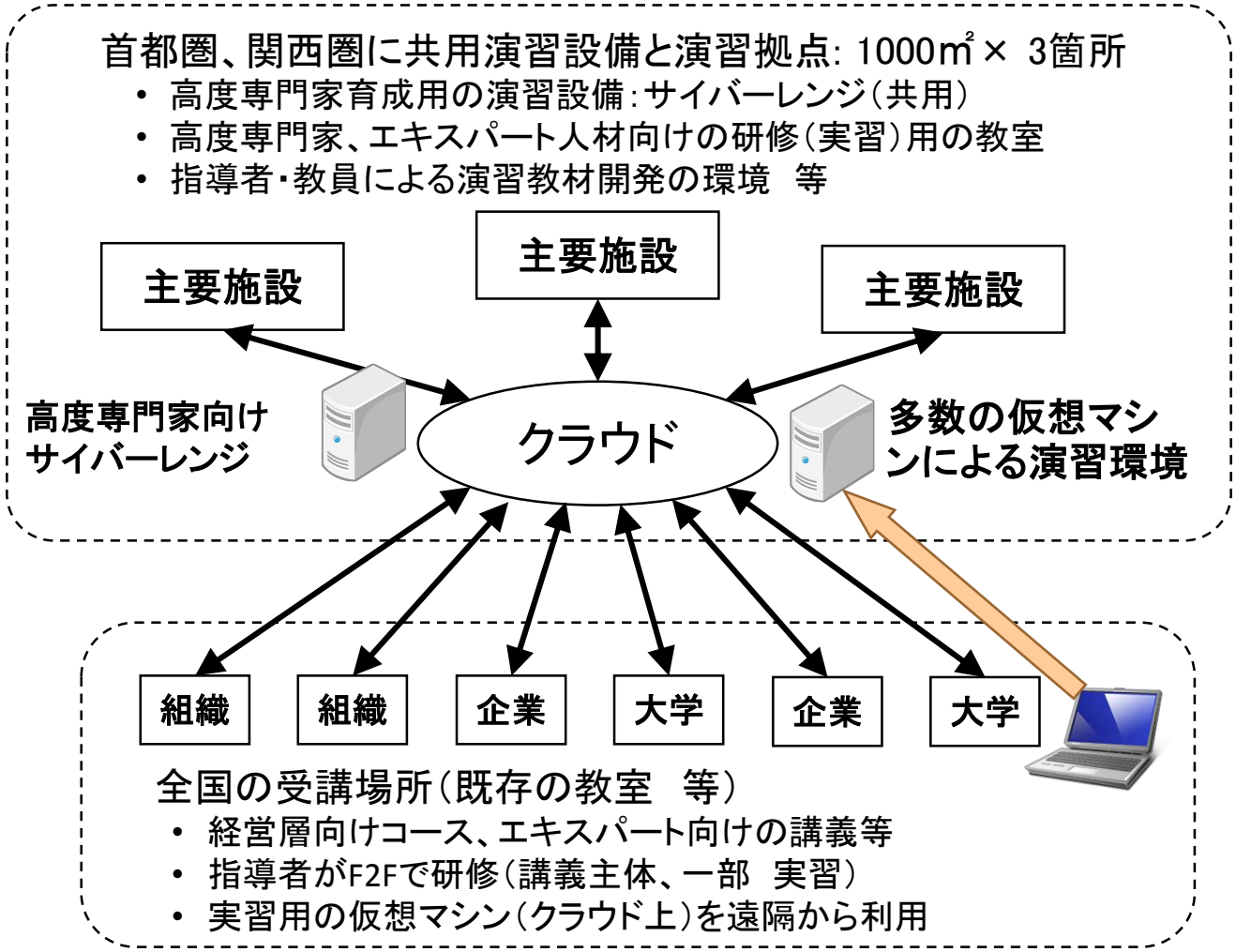
オールジャパン産官学の共同育成事業体



実効性のある人材育成活動

- 共同育成事業体: 集中専門人材の育成
- 指導者や教員の育成活動：企業・官庁・自治体等内での人材育成活動へ展開
- 経験と実績を活用：企業内研修、文科省プログラムenPiT-Secと教材など活用
- 経営層向けセキュリティ研修
- ベース人材育成
  - 基礎講義（MOOC含む）活用のセキュリティ基礎人材育成
  - 大学学部教養課程でのサイバーセキュリティ概論
  - 義務教育への情報教育とセキュリティリテラシ教育

構成例：先端的高度専門家や諸分野のサイバーセキュリティ人材育成のための共用設備と教材開発



産学官連携

- 産の役割
  - 人材の積極採用とキャリアパスの構築
  - 共用設備による専門家育成に向けた受講者の提供と、新教育ニーズの提示
  - 学と協力しての人材育成活動
  - インターン実務研修の場を提供
  - 共用設備の維持管理の費用分担
  - 現場データの提供
- 学の役割
  - 当初教材と講師の提供
  - 継続的全国レベルの大量サイバーセキュリティ人材育成活動
  - 継続的な講師人材の育成
  - 教材の継続的機能向上開発（研究主体の大学院と連携）
  - 現場データを用いた研究開発
- 官の役割
  - 事業の初期投資による事業の立ち上げ
  - 共用設備導入と、続く数年の維持費提供
  - 中央官庁や自治体からの受講者派遣と新規採用
  - 現場データの共有環境構築支援

(2) 研究開発機能の強化

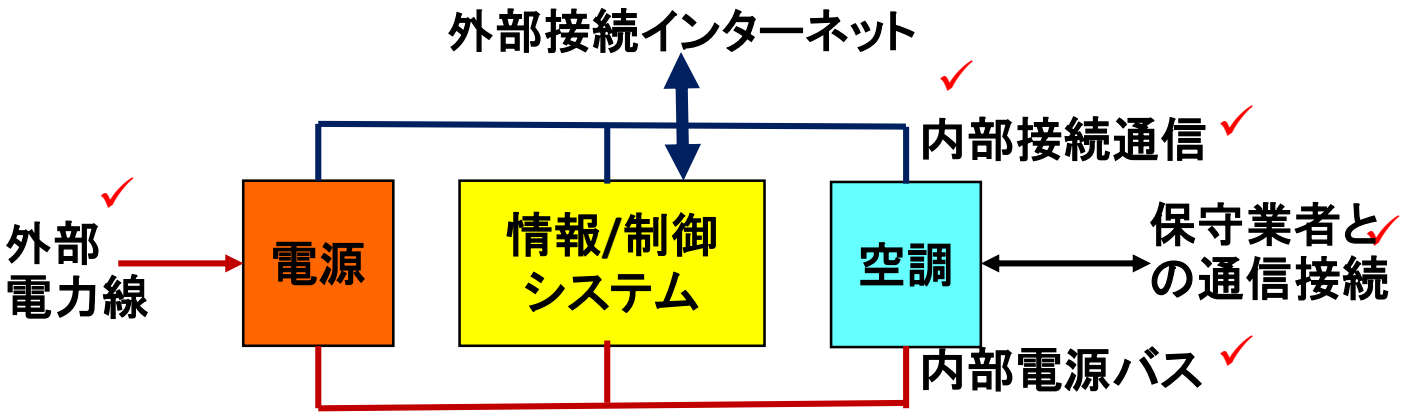
- 情報セキュリティ技術は、輸入依存
- 情報セキュリティコア技術/情報は、わが国の必須アイテム
  - 国際間インテリジェンスにおける交換条件
  - 技術の研究強化、もぐら叩きからの脱却
- 研究内容と体制
  - 基礎研究：システムの複雑化対応
  - サイバーセキュリティ解析コア技術・設備
  - 研究向け共有情報の拡大と実効的利用体制

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

異なる設計原理への対応

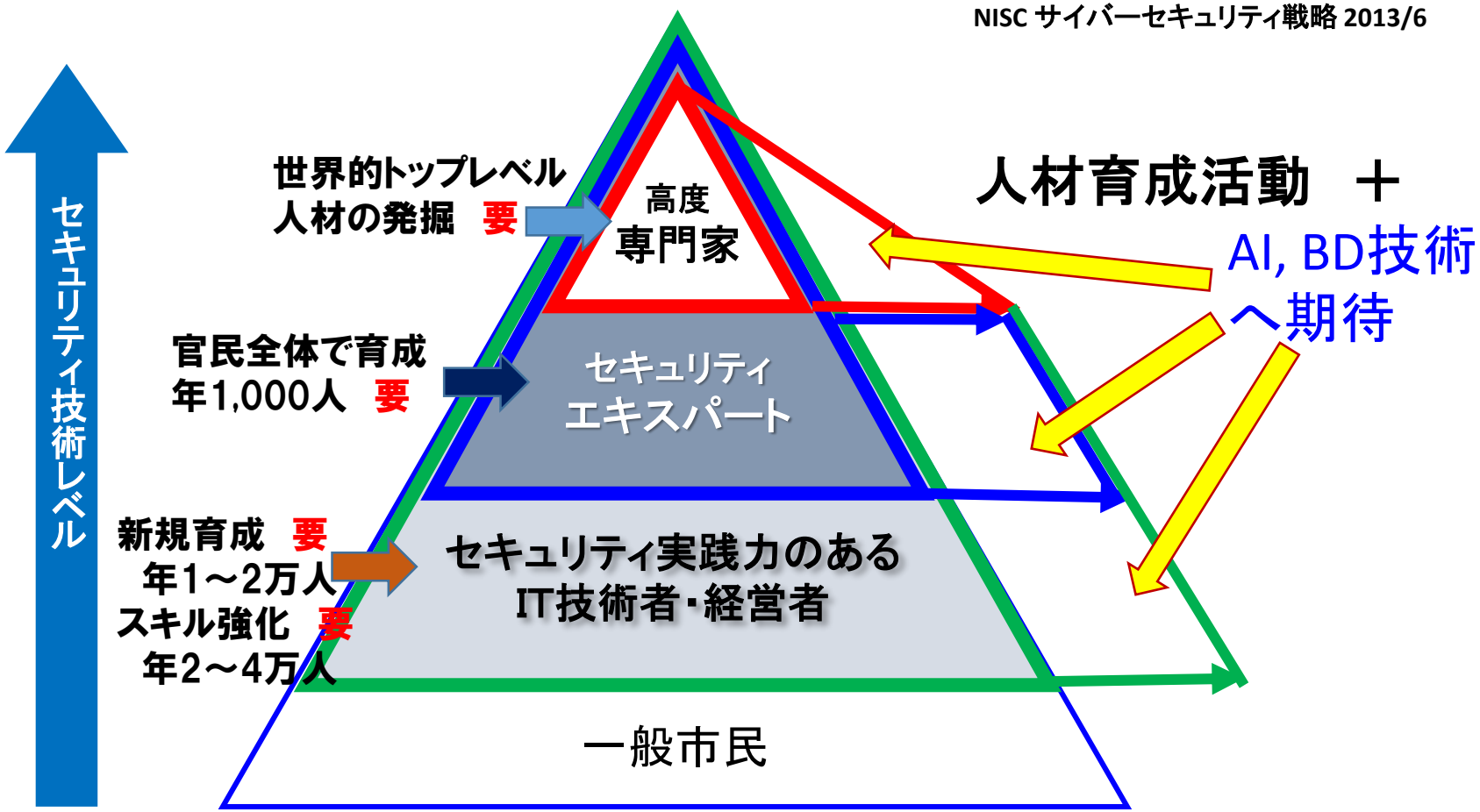
- 従来の諸システム設計原理
  - 自然発生由来の故障→　故障対応の２重化
  - 設計誤り/抜け→　テストで極少化
- サイバーセキュリティ設計原理
  - 悪意（裏に人）由来の攻撃→　時代で変化、検出
  - 脆弱性→　完全事前対応は困難、発見時パッチ



研究開発テーマ例

- システム設計フレームワーク
  - 異原理システム間接続方式：原則に戻っての対応
- 次世代高セキュア・コアシステム：チップ、装置
- セキュリティ要素技術
  - OS、暗号、形式的開発、脆弱性発見、認証システム
- システム内分析と攻撃の自動検出
  - 攻撃分析による知的進入防御システム
- 人・機械・法制の役割分担と明確化
  - 法制のあり方と、線引きへの実利用からの反映
- 次世代サイバーセキュリティ対応技術の研究開発
  - 人ベース→ IT高度支援（ビッグデータ解析、知的処理、学習機能）
- 現場データの利用推進
  - 大学研究者から遠い現場データ

日本のセキュリティ関連技術者26.5万人
16万人がスキル不足！更に8万人不足！
NISC サイバーセキュリティ戦略 2013/6



おわり

サイバーセキュリティ人材育成連絡会

http://www.cybersecurity-edu.org/