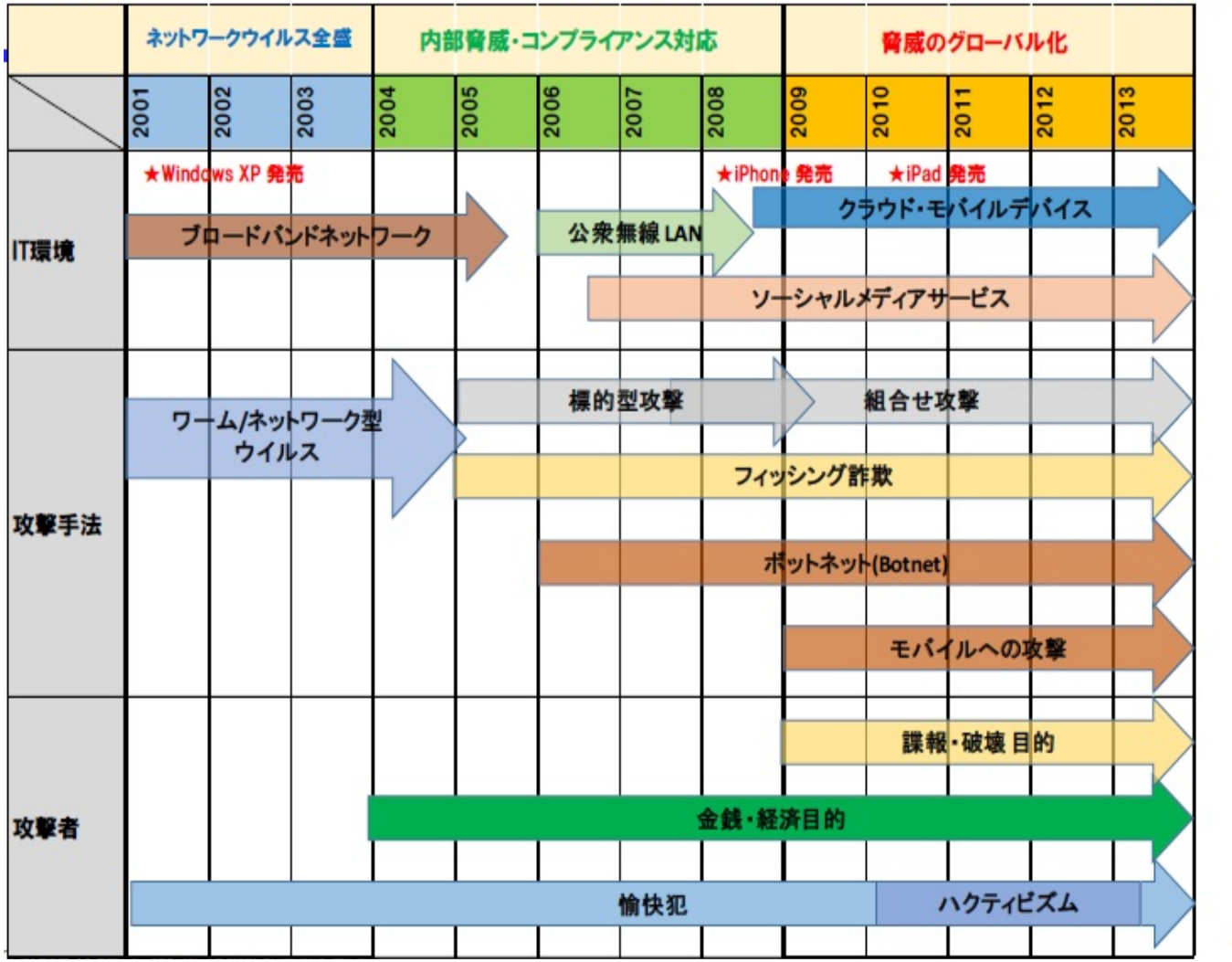
サイバーセキュリティ月間　キックオフシンポジウム

サイバーセキュリティ基本法とこれからの日本

2015年2月2日

林　紘一郎
情報セキュリティ大学院大学教授
情報セキュリティ政策会議構成員
Board Director Training Institute理事

情報セキュリティの変遷（IPA資料）



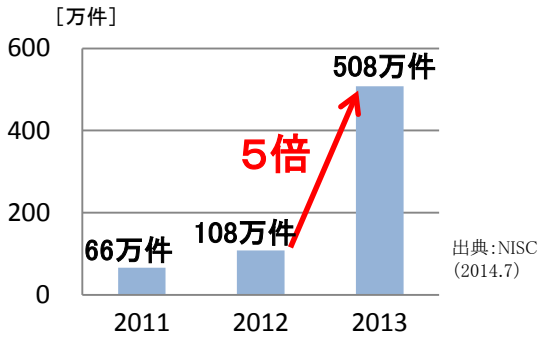
https://www.ipa.go.jp/files/000037684.pdf

サイバー脅威の深刻化

政府機関等への攻撃激化

⇒ 6秒に1回攻撃が発生

センサー監視等による脅威件数

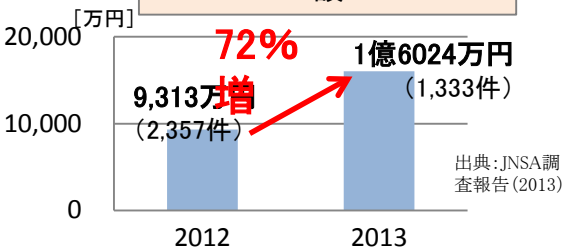


強化① 機関の防護・対処能力の強化

攻撃対象の拡大・深刻化

⇒情報漏えい事案の被害額が増加

1件あたりの想定損害賠償額



⇒重要インフラ（情報通信、鉄道等）への攻撃件数が増加

出典：NISCへの通報件数

76件（2012年度） → 133件（2013年度）

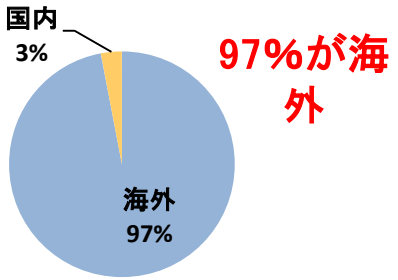
約2倍

強化② 官民連携の強化

サイバー攻撃のグローバル化

⇒攻撃のほとんどが国境を越える

不正プログラムの接続先（2013）



出典：警察庁（2014.2）

強化③ グローバルな連携強化

政府戦略

以下の各戦略において、サイバーセキュリティ推進体制の強化の必要性が規定。

- 国家安全保障戦略（H25.12.17 閣議決定）
- サイバーセキュリティ戦略（H25.6.10 情報セキュリティ政策会議決定）
- 「日本再興戦略」改訂 2014（H26.6.24 閣議決定）

サイバーセキュリティに係る国家戦略を策定・推進する

司令塔機能の強化や体制整備が急務

東京五輪へ向けた準備

2012年のオリンピック・パラリンピックロンドン大会では、開催期間中、約2億件のサイバー攻撃が発生。英国政府は、6年前からサイバー攻撃対策を準備。

サイバー攻撃の実例

時期	対象・攻撃者	被害内容	新規性
1990年	イラク防空システム・米軍	プリンターにマルウエアを仕込むも、ミサイルでの破壊が先行	最初の事例
1999年	セルビア防空システム・米軍	データの改ざんによる機能低下	セルビア側はハッカー集団が応戦
2007年	エストニア全域・ソ連の関与？	銀行システム等に対するDDoS攻撃やウエブ改ざん	第1次Web大戦？
2007年	シリア核施設・イスラエル軍	可能性：①データの改ざん、②ディスプレイ画面の改ざん、③敵・味方識別機能の無力化	成果が顕著
2008年	グルジア全域・ソ連のハッカー集団	南グルジア独立紛争に呼応して、あらゆるサイバー攻撃	サイバー・パルチザン（民間人の参加）
2010年	イラン核施設・米＋イスラエル軍？	閉域網である制御システムに、USBを介してウイルス感染させる	史上初のサイバー兵器？

（出典）伊東寛 [2012]『第5の戦場：サイバー戦の脅威』祥伝社

サイバーセキュリティ基本法の概要①

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒ 「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靭な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、
教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

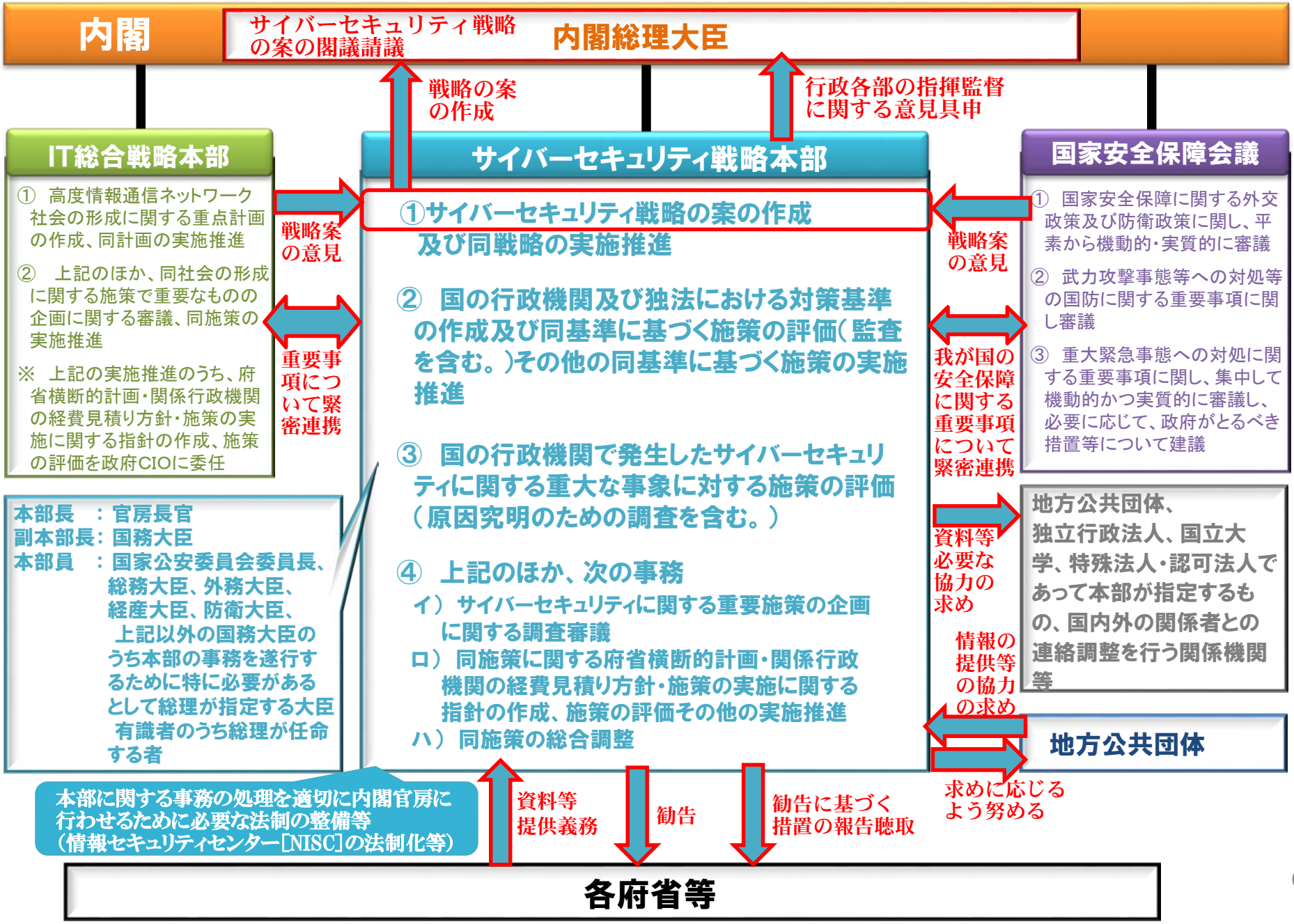
■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

サイバーセキュリティ戦略本部の機能・権限（イメージ）



政府におけるサイバーセキュリティ確保のための機能強化

サイバーセキュリティ基本法

［(衆)内閣委員長提案により186回通常国会へ提出。第187回臨時国会で成立］

内閣官房組織令の一部改正等

〔同年12月16日に政令改正を閣議決定。〕

IT総合戦略本部 ⇔ 緊密連携

サイバーセキュリティ戦略本部
（本部長：内閣官房長官）

- サイバーセキュリティ戦略本部の所掌事務
  - ① サイバーセキュリティ戦略案の作成
  - ② 政府機関等の防御施策評価（監査を含む）
  - ③ 重大事象の施策評価（原因究明調査を含む）
  - ④ 各府省の施策の総合調整（経費見積り方針の作成等を含む）
- サイバーセキュリティ戦略本部に関する事務は、内閣官房副長官補が掌理

緊密連携 ⇔ NSC（国家安全保障会議）

資料等提供義務 ↑　勧告 ↓　勧告に基づく措置の報告聴取 ↓

各府省等

事務局 ←

政府において本部に関する事務を内閣官房で行わせる等のために必要な*法制*を整備（基本法附則第２条）

内閣サイバーセキュリティセンター（NISC）（注）

- 内閣サイバーセキュリティセンターの所掌事務を規定
  - GSOCに関する事務
  - 原因究明調査に関する事務
  - 監査等に関する事務
  - サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

＋

戦略本部の事務の稼働状況、東京オリンピック・パラリンピック大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、

法制の追加的な整備について引き続き検討

（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

2015年（平成27年）から本格稼働（基本法・政令改正の施行日は平成27年１月９日）

サイバー・インシデントの特性

① 実行者の特定困難性：匿名化手段（TOR＝The Onion Router ） やボット化・踏み台化（パソコンやサーバが乗っ取られ、指令サーバに支配される）などにより、誰が本当の実行者かの特定が難しい

② 被害の潜在性（ステルス性）：ウイルス感染や、不正アクセスなどによる情報の窃取あるいは乗っ取りにも、痕跡を残さないので、被害者も気づかない

③ インシデントから攻撃までの連続性・越境性：偶発的インシデント、いたずら、営利目的、攻撃、テロ、武力攻撃の準備（インテリジェンス）までが、連続的に展開され区分が難しい上、容易に国境を越えてしまう

防御を難しくする6つの非対称

以下のいずれにおいても、攻撃側が優位

(1) 一点突破 対 全面防御、

(2) 違法覚悟 対 合法の範囲内、

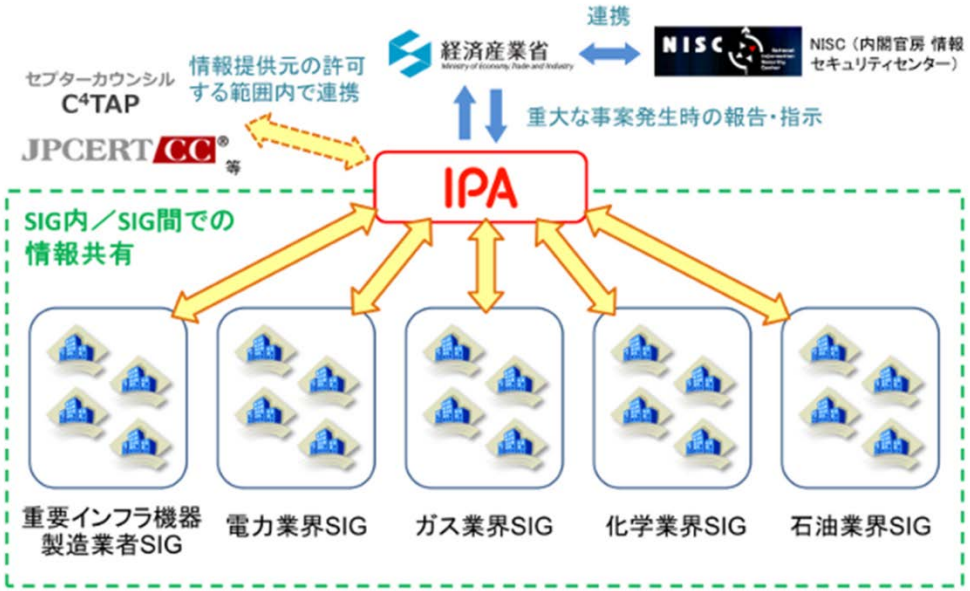
(3) ゲリラ軍 対 正規軍（しかもタテ割り）、

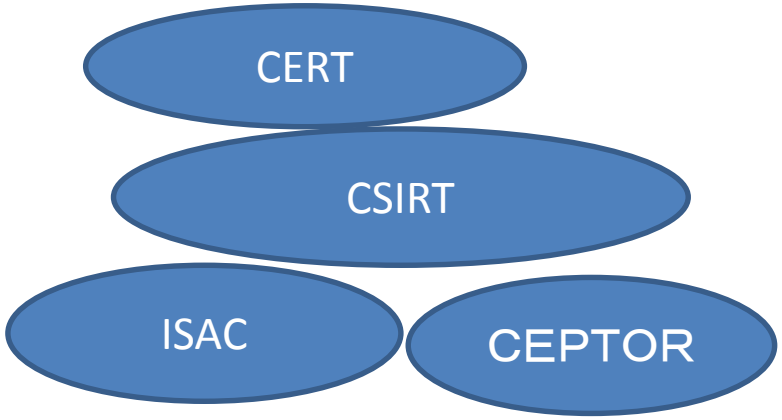
(4) 緩やかな国際連携 対 国内組織、

(5) 多数の予備軍 対 少数精鋭、

(6) （一部国家の）暗黙の援助 対 国際秩序遵守

防御側の情報共有





INTERNET Watch ニュース
日本版NCFTA、産官学共同の「日本サイバー犯罪対策センター（JC3）」業務開始
（2014/11/14 12:02）
　日本版NCFTAとしてサイバー空間の脅威に対処するための非営利団体「一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）」が13日、業務を開始した。

わが国経済を取り巻く環境

以下は日本に特有のことではないが、わが国が他に先駆けて経験する

- 少子・高齢化：国内市場の縮小と変化、女性の活用や国際展開が必須（外へのグローバル化）
- グローバル化：市場と雇用のグローバル化、経営におけるダイバーシティ、経営と監督の分離（内なるグローバル化）
- モノから情報へ：物余り、差異化、情報的価値、所有から利用へ
- 時間資本主義（松岡真宏 [2014]『時間資本主義の到来』草思社）:時間が最も希少な資源

環境変化への適応力

- A型（情報で統合し人事は分散）とJ型（人事で統合し情報は分散）（青木昌彦 [1989]『日本企業の組織と情報』東洋経済）：ハイブリッドはあり得るか？
- これを情報セキュリティの面から見ると、もう1つのA型とJ型の問題になる（林・田川・淺井 [2011]『セキュリティ経営』勁草書房）：これまたハイブリッドはあり得るか？
- ここで決め手になるのが、情報を主体にして、企業を「巨大な情報処理システム」と見ることであるが、わが国の経営者も経営学者も、このような発想に乏しい
- 同様に情報を主体にして、誰がアクセス可能か、どの範囲で共有可能か、という視点であるが、わが国では、この仕訳も徹底していない。
- 最後に紹介する resilience とも関連

Need-to-Know の原則

- 業務上必要な人だけに知らせて（あるいは、アクセスを許可し）、不要な人には知らせない（アクセスを禁ずる）という原則
- Job description が明確なアメリカ型企業には向いているが、「日本的経営」の伝統とは相容れない面がある（例、隣の社員の電話を取らない）
- しかし、インターネットの普及に伴って、各自がアドレスを持つようになり、個人を基礎にした経営管理方式が普及しつつある（共通のアドレスが不自然になった）
- 若者が「上司との飲み会」を嫌うように、次第に個人ベースの社会になるのだろうか？
- 震災の反省として、自助・共助・公助の3本の矢が必要とされたが、共助が一番「どっちつかず」になりそう（わがマンションでの災害時初期対応演習の経験から）

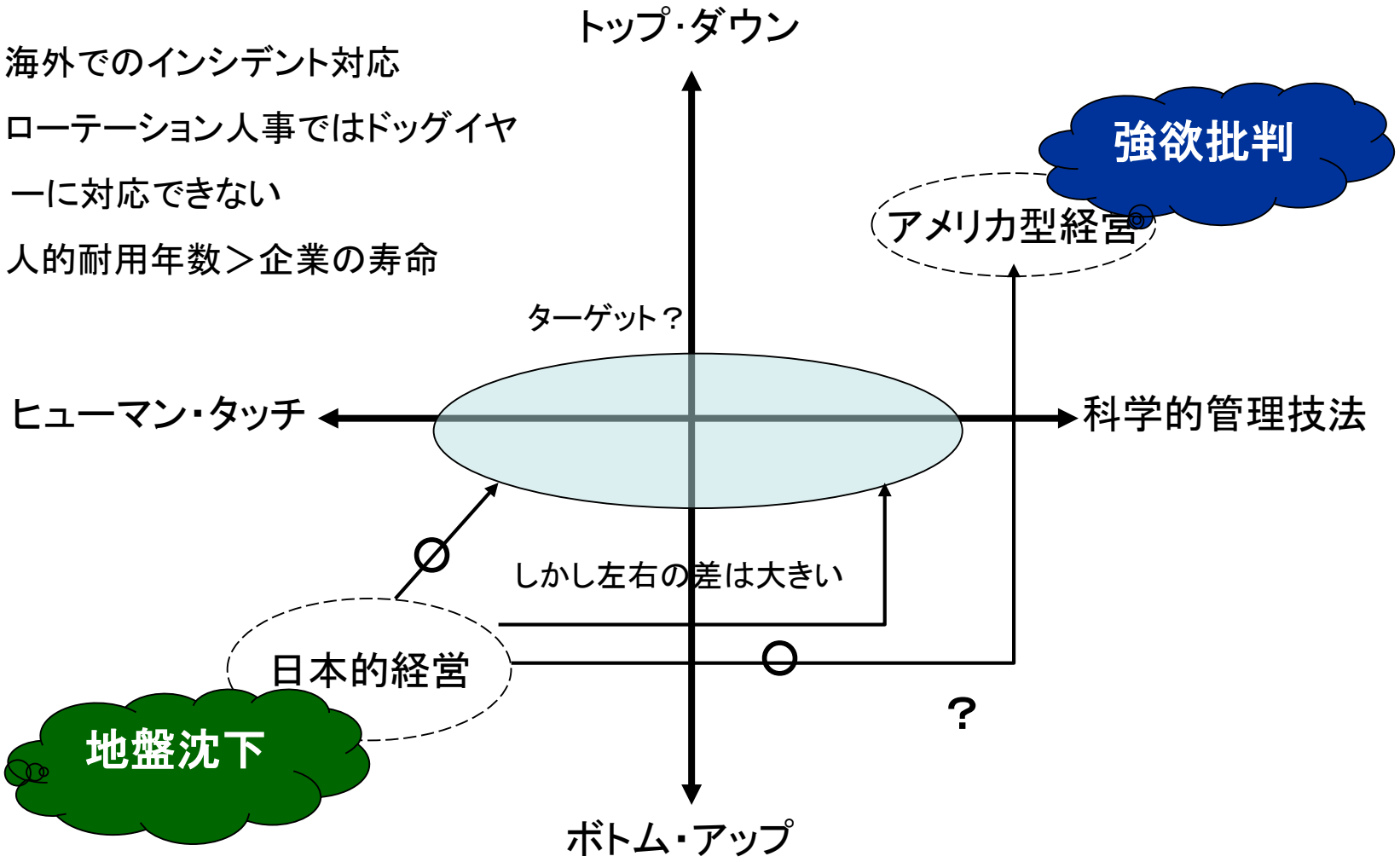
Need-to-Share の要請と限界

- アメリカのインテリジェンス・コミュニティでは、9.11で多くの予兆を感知しながら事件の発生を抑止できなかった反省から、部門や組織を超えた情報共有の仕組み（Information Sharing Environment = ISE)が求められた
- 同時に、自治体や民間企業においても、情報共有の意義を説く主張が強くなった
- しかし Wikileaks や Snowden 事件を機に、need-to-know を原則としつつ、それに share の要請をどう付け加えるべきか、という現実論が復活している

・海外でのインシデント対応

・ローテーション人事ではドッグイヤーに対応できない

・人的耐用年数＞企業の寿命



出典：林紘一郎・田川義博・淺井達雄［2011］『セキュリティ経営』勁草書房

特定秘密保護法の意義

- （立法者は意識していないようだが）「秘密の法的保護」という一般論を提起し、量刑についてバランスを取った
- 従来欠落していた「国家の秘密」という概念を明確化し、指定や解除の方法など「セキュリティ・マネジメント」の面にも踏み込んだ
- 特別管理秘密という「法的な根拠薄弱な存在」を解消し、明示的・限定的に保護することとした
- 秘密の3要件（営業秘密についての ① 非公知、② 有益（実質秘）、③ 秘密管理性）を再確認した
- 秘密を扱う者の資格条件（セキュリティ・クリアランス）を明確化した
- ただし、「知る権利」など比較考量すべき価値との調和については、具体的な手続きの整備が十分か、運用の実態がどうなるかなど、なお議論を残している

差異化としての品質と管理システム

アレンとヤーゴの『金融は人類に何をもたらしたか』（東洋経済、2014年）における藤野の監訳者解説（p.348 ）から

- トヨタのJITは、世界標準と認められるほどの価値があるが、これを形式知化した教科書や、訓練コースの設計に努力しなかった。
- この間アメリカは、これを徹底的にビジネススクールで教えるとともに、APICS（American Production and Inventory Control Society）が資格制度を作り、今では日本人がそれを受けている。
- 日本人に欠けているのは、こうした広い視野をもたらす教養である。
- 今後この種の応用が必要なのは、いずれも制御理論に基づく、金融イノベーションと、サプライチェーン・マネジメントである。

私は、この藤野のコメントに、以下を追加したい。

- 「セキュリティ・マネジメント」も、この種の応用が必要だし、未だ日本が追い付ける分野である。

費用と投資の考え方

- 会計的理解：費用は単年度・収益に直接寄与しない、投資は長期的・収益につながり償却対象資産になる
- 財務的理解：費用は年度決算になり cash flow として全額が資金の支出、投資はROI (Return On Investment) の対象で cash flow としては原価償却費分が償却期間中利用できる
- 経営的理解：義務的・消極的支出が費用、意図的・積極的支出が投資
- Redundancy:効率性の観点からは「冗長度」だが、セキュリティの観点からは「安全係数」（林雄二郎 [1969] 復刻版は[2007]『情報化社会ハードな社会からソフトな社会へ』講談社）

セキュリティは費用か投資か

- ITサービス企業にとっては、セキュリティはかつては「おまけ」だったが、今日では「それ自体が商品」としての価値を持ちつつある（アンバンドルして値付けすることも可能）。
- IT利用企業にとっても、セキュリティは「サービス品質」を担保するものとして、意識され始めたのではないか
- 利用者にとっても、「セキュリティが担保されないサービスは、危なくて使えない」という認識が生まれているのではないか
- 遅れているのは、むしろ供給サイドのトップで、前ページのように「利益を生ませる」意識が必要か
- オリンピックを控え、イベントにはセキュリティが不可欠との理解が進めば、「利益の一部はセキュリティのおかげ」との理解が進むはず
- 他のプレゼンターが実例を示してくれることに期待したい

Resilience という発想

- インターネットは、そもそも resilience を実現する手段として考案された。だから、従来の概念としての（守りの）セキュリティの発想は希薄
- 3.11を機に、2つの P から2つの R へ:

  Prevention + Protection ---> Response + Resilience

  （林・田川・淺井 [2011]『セキュリティ経営』勁草書房）
- 国土強靭化にも、そのような発想が含まれている

  http://www.cas.go.jp/jp/seisaku/resilience/
- だとすれば、resilience の中に「費用から投資へ」という発想が暗示されているのではないか？