我が国における
サイバーセキュリティの状況

2015年2月2日

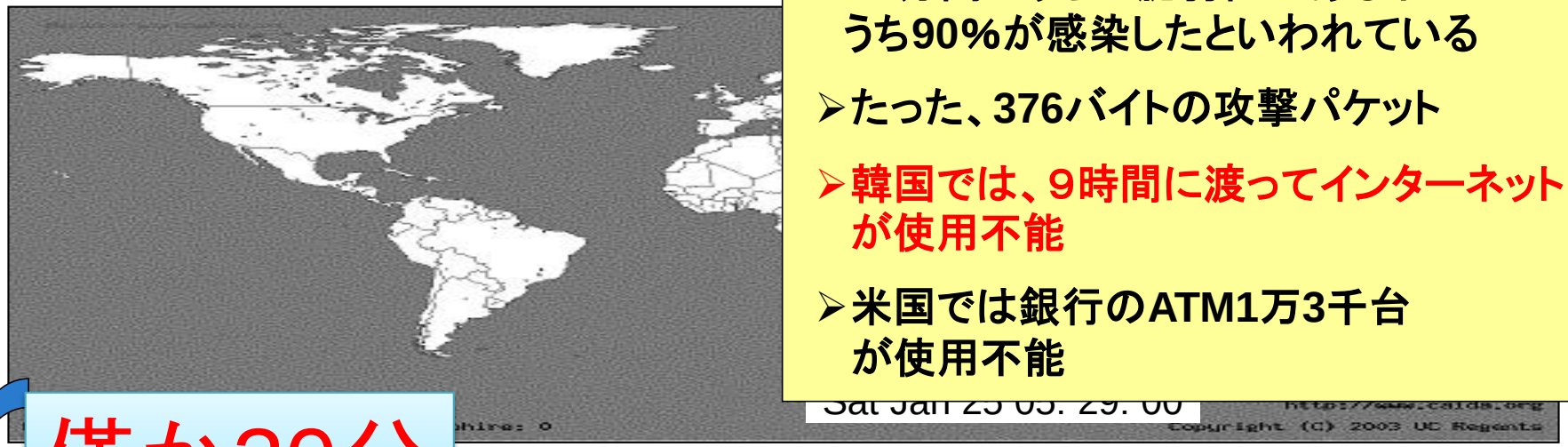
東京工科大学
手塚　悟

目次

1．サイバー空間における攻めと守りの状況

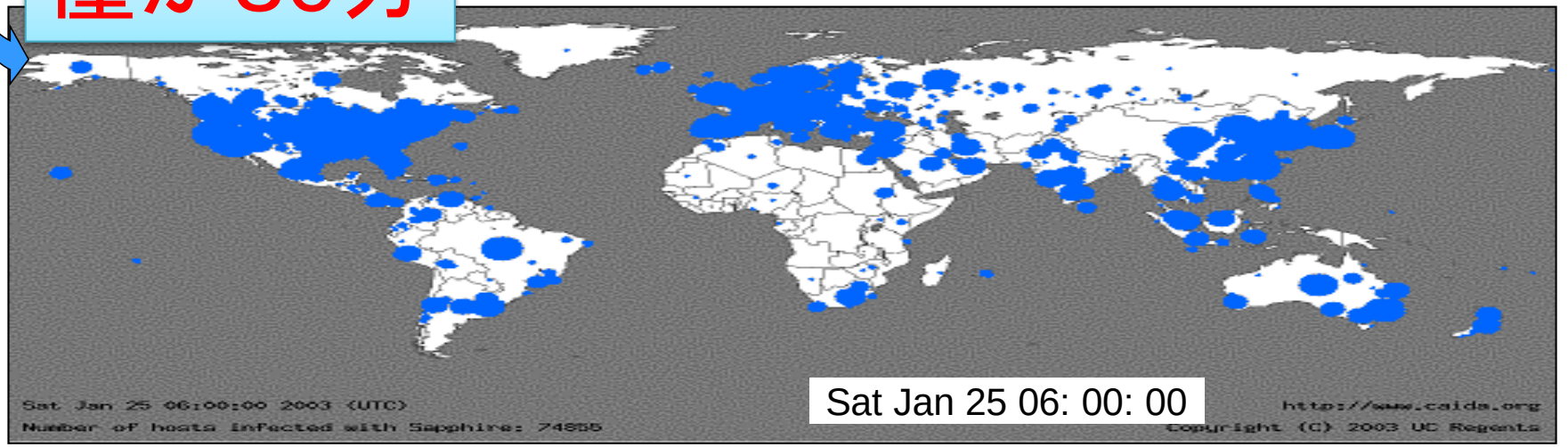
●Slammer: 感染動作自体がインターネットをDoS状態に陥れる

2003年01月25日　　Slammer ワーム発生



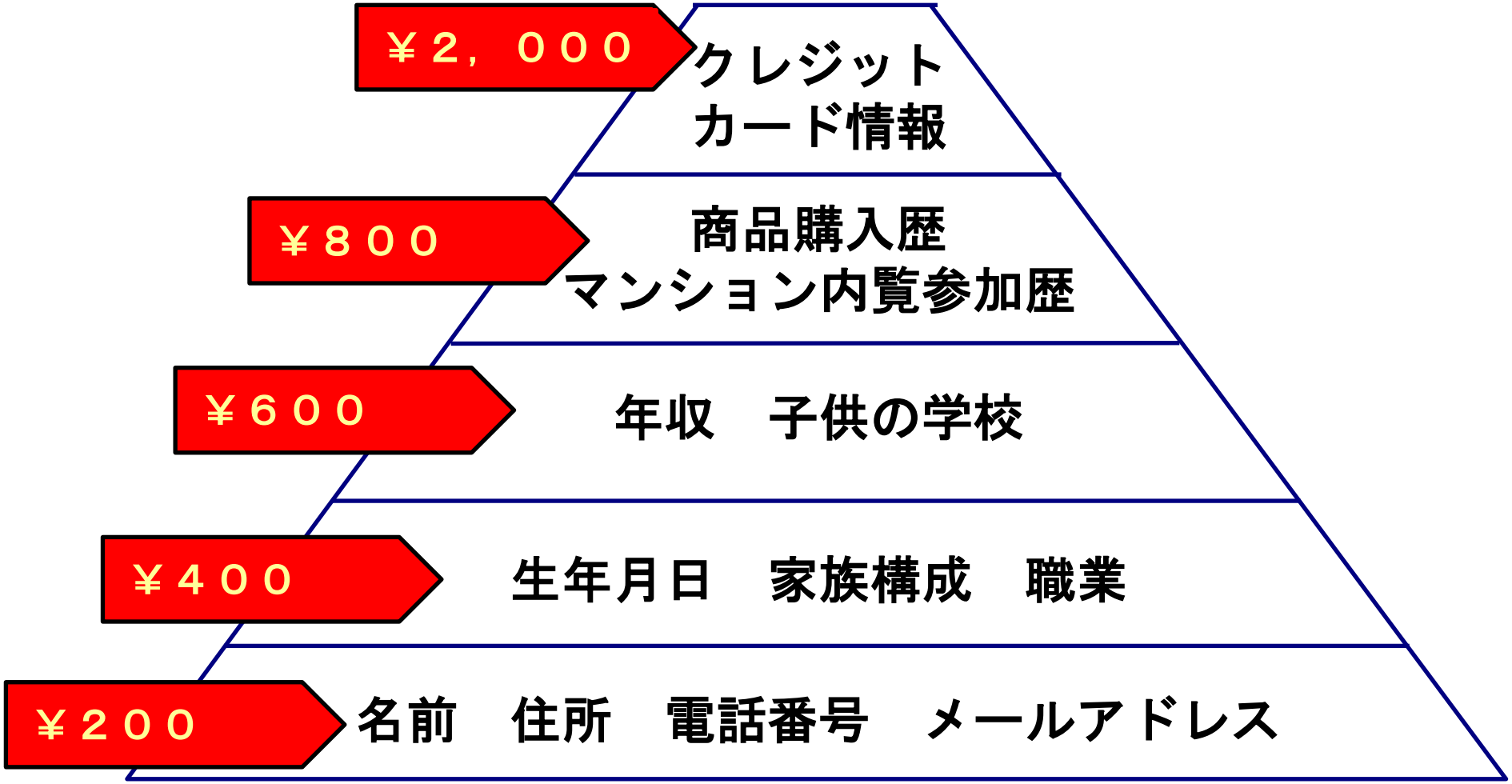
- 10分間のうちに脆弱性のあるホストのうち90%が感染したといわれている
- たった、376バイトの攻撃パケット
- 韓国では、9時間に渡ってインターネットが使用不能
- 米国では銀行のATM1万3千台が使用不能

僅か30分



１．サイバー空間における攻めと守りの状況

- 情報の値段は
  例）



1．サイバー空間における攻めと守りの状況

- 攻撃種類
  - 国家機密情報等を狙った攻撃
  - 企業秘密情報等を狙った攻撃
  - 個人情報等を狙った攻撃
  - 金銭等を狙った攻撃
  - 愉快犯としての攻撃　　等

1．サイバー空間における攻めと守りの状況

サイバー攻撃の特徴（例）

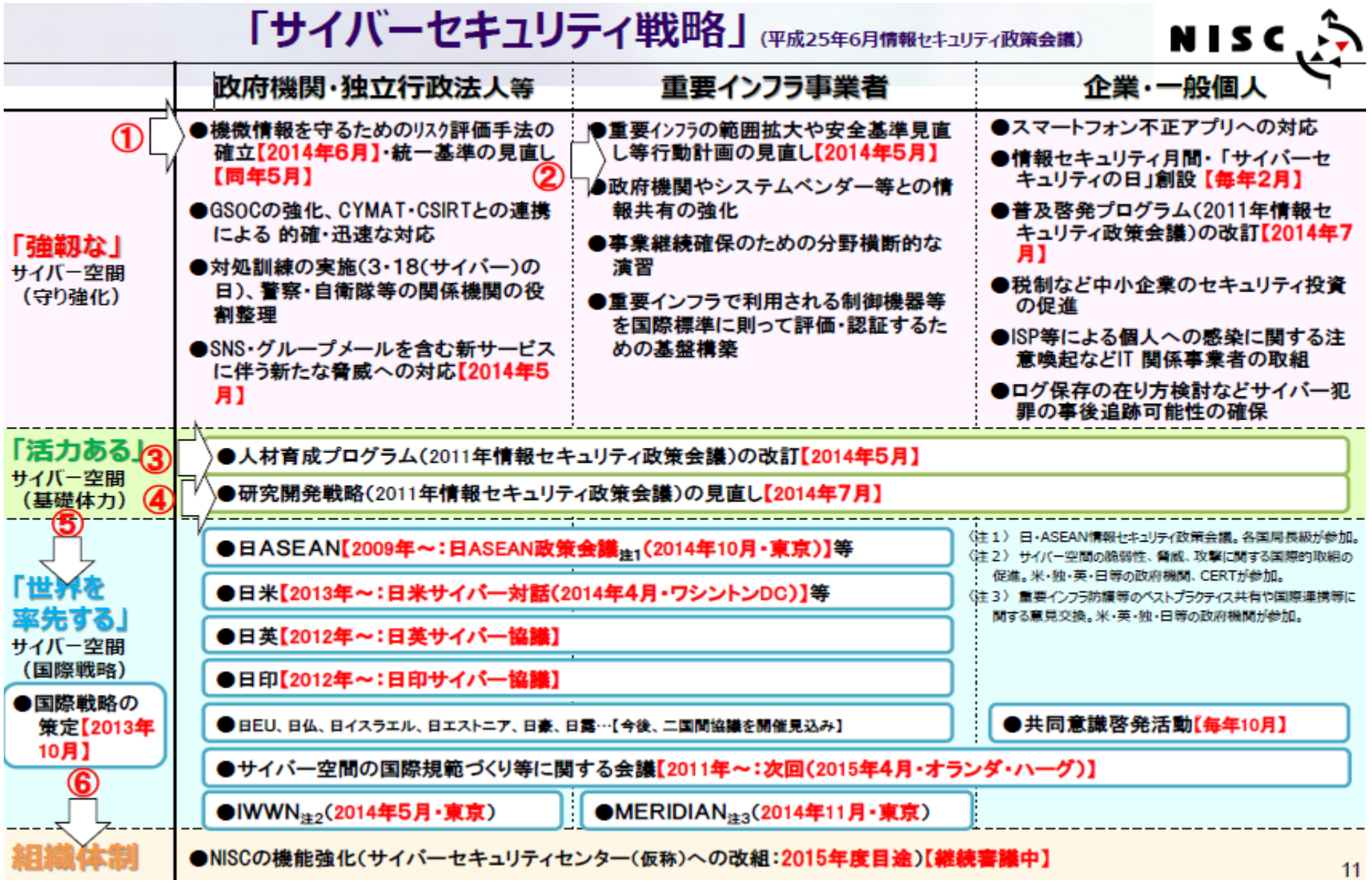
- 非対称性（高価な兵器を必要とせず、費用がかからない）
- 攻撃側の優位性（インターネットは拡張性があり、新技術の導入も容易）
- 従来の抑止モデルが適用されず（攻撃者の特定が困難かつ時間を要する）
- ソフトウェア及びハードウェア自体が脅威を内在（サプライチェーンリスク）
- 予測の困難性（国家及び非国家主体の両方が実行者になり得る）

6

1．サイバー空間における攻めと守りの状況

- 守備範囲
  - 政府機関（各府省庁）
  - 独立行政法人
  - 地方公共団体
  - 重要インフラ事業者
  - 大企業
  - 中小企業
  - 個人　　等

1．サイバー空間における攻めと守りの状況



1．サイバー空間における攻めと守りの状況

世界が直面するグローバルリスク
～一層深刻な状況へ～

NISC

本年に入り、世界経済フォーラム（WEF）は、**今後10年間で全世界及び全産業界に重大な悪影響を及ぼす可能性が高いリスク**として、**サイバー攻撃及び重要情報インフラの故障**を位置づけ。

インターネット依存が高まり、それに繋がるデバイスの規模も極めて大きくなったことで、**2014年には構造的破綻のリスクがこれまでで最大規模に達し、システムばかりでなく社会までも破壊**できるほどになると指摘。

備考：全世界及び全産業界に対して重大な悪影響を及ぼす可能性のあるものとして抽出した31のリスクに関する今後10年間の展望について、世界各地の700名以上の専門家に対する調査結果をとりまとめたもの。「1」は「発生する可能性がないもの」又は「影響がないと思われるもの」、「7」は「大いに発生する可能性があるもの」、又は「甚大かつ破壊的な影響があると思われるもの」を示している。

＜出典：WEF「グローバルリスク報告書2014年版」(2014年1月16日)＞ 4

目次

1. サイバー空間における攻めと守りの状況
2. サイバーセキュリティの政策
3. サイバーセキュリティのガバナンスと産業化
4. 次世代を担うCISOの育成
5. 官民連携の在り方
6. 今後のサイバー空間の安心安全

2．サイバーセキュリティの政策

● 米国サイバー･セキュリティ法制定までの背景

- 2012年4月26日、米国上院議会は Cyber Intelligence Sharing and Protection Act (CISPA) を否決
- 2013年2月12日、オバマ大統領は Improving Critical Infrastructure Cybersecurity の行政命令を発令
- 2014年8月27日、JPMorgan Chaseはじめとした10以上の金融機関がハッキングを受けたこと発覚
- 2014年11月6日、日本のサイバーセキュリティ基本法可決成立
- 2014年11月24日、米国ハリウッドにて、ソニー・ピクチャーズ・エンタテインメントへのハッキングが電子メール、従業員の個人情報、未公開の映画本編のコピーなどの情報が流出
- 2014年12月18日、オバマ大統領のサインにより、5つのサイバーセキュリティ関連法が制定

2．サイバーセキュリティの政策

● 米国サイバーセキュリティ法は5つの法から構成

サイバー関連で2014年12月18日、オバマ大統領のサインにより、以下5つの法が同時に制定される。

1) サイバーセキュリティ強化法　S.*1353 Cybersecurity Enhancement Act (No: 113-274)

2) サイバーセキュリティ従業員評価法　H.R.**2952 Cybersecurity Workforce Assessment Act (No: 113-246)

3) 国土安全保障省・サイバーセキュリティ従業員評価法　S.1691 Homeland Security Cybersecurity Workforce Assessment Act　(Border Patrol Agent Pay Reform Actの一部、Section 4) (No: 113-277)

4) 国家サイバーセキュリティ保護法　S.2519 National Cybersecurity Protection Act of 2014 (No: 113-282)

5) 連邦政府情報セキュリティ近代化法　S.2521 Federal Information Security Modernization Act (No: 113-283)

*S. Senator 上院に提出された法案

**H.R. House of Representative
下院に提出された法案

２．サイバーセキュリティの政策

- 我が国の政策
  - サイバーセキュリティ基本法：2014年11月6日成立
  - 内閣官房内閣サイバーセキュリティセンター政策
  - 総務省情報セキュリティ政策
  - 経済産業省情報セキュリティ政策
  - 警察庁サイバー犯罪対策
  - 防衛省サイバー空間安全保障

＊内閣官房内閣サイバーセキュリティセンター：　NISC　(National center of Incident readiness and Strategy for Cybersecurity)

2．サイバーセキュリティの政策

サイバーセキュリティ基本法案の概要　資料1－2（参考）

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、強靱な体制の構築
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

2．サイバーセキュリティの政策

「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針（案）」の概要　資料1

1．機能強化の必要性

- あらゆる活動のサイバー空間への依存の高まりにより、リスクが深刻化（甚大化・拡散・グローバル化）
- 「世界最高水準のIT社会」をIT利活用においても実現することが成長戦略の柱の1つ
- 国際的な連携の強化が必要な諸外国においても、積極的な体制強化が実施
- 2020年東京オリンピック・パラリンピックに向けた対策の強化が必要

我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

2．機能強化に向けた方針

IT社会の形成を目的とし、民間の主導的役割等を基本理念とするIT基本法の基本的枠組みは今後も堅持することが適当

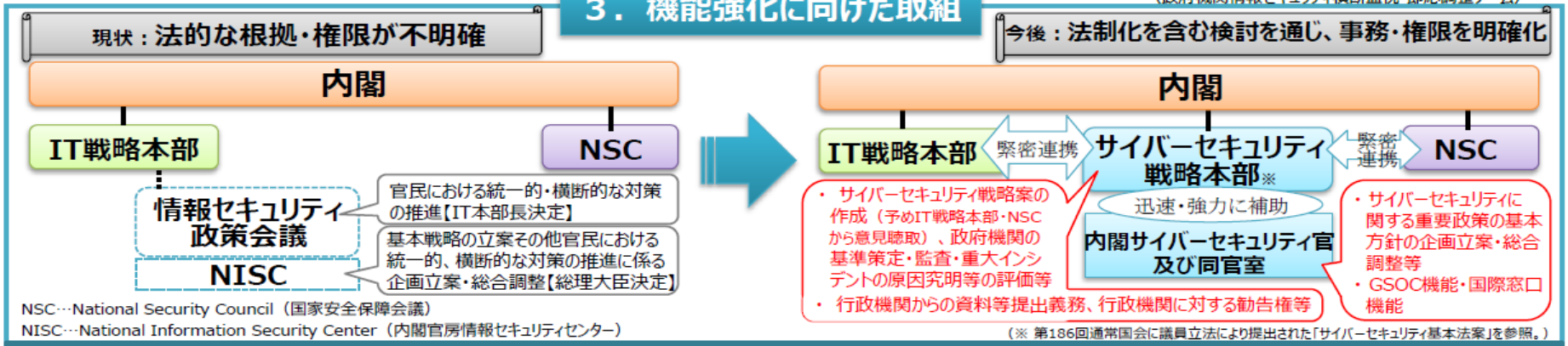
国家の安全保障・危機管理上、国の主導的役割を定め、マルチステークホルダーの相互連携によるサイバー空間の防護が必要

IT社会の形成及びサイバー空間の防護のための関係者の役割を明確化し、それが果たされるための国の基本的施策が必要

「サイバーセキュリティ」に関する施策を総合的かつ効果的に推進するための体制を整備することが必要

GSOC…Government Security Operation Coordination team（政府機関情報セキュリティ横断監視・即応調整チーム）

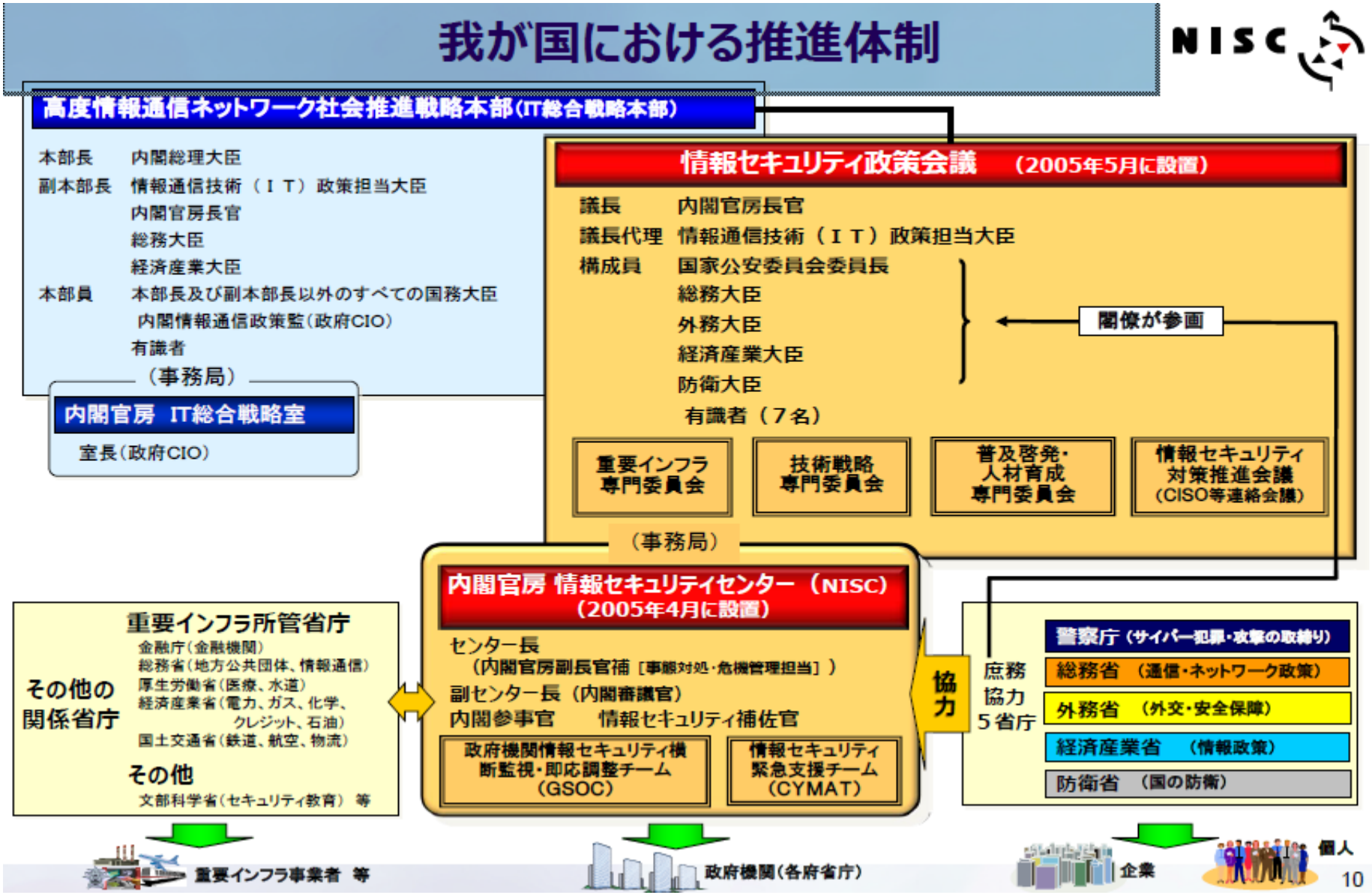
3．機能強化に向けた取組



2015年度を目途に「サイバーセキュリティ戦略本部（仮称）」及び「内閣サイバーセキュリティ官（仮称）」へ強化

出典：内閣官房情報セキュリティセンター（NISC）資料より

2．サイバーセキュリティの政策



２．サイバーセキュリティの政策

● 関連組織

● 重要インフラ関連組織

- CEPTOAR : Capability for Engineering of Protection, Technical Operation, Analysis and Response

● 総務省関連組織

- NICT : National Institute of Information and Communications Technology

● 経済産業省関連組織

- IPA : Information-technology Promotion Agency, Japan
- JPCERT/CC : Japan Computer Emergency Response Team Coordination Center
- CSSC : Control System Security Center

● 警察庁関連組織

- IAjapan : Internet Association Japan

● 民間組織

- Telecom-ISAC : Telecom-Information Sharing and Analysis Center
- JNSA : Japan Network Security Association
- NCA : Nippon Computer Security Incident Response Team Assoiation　etc.

2．サイバーセキュリティの政策

（参考）セプター及びセプターカウンシル

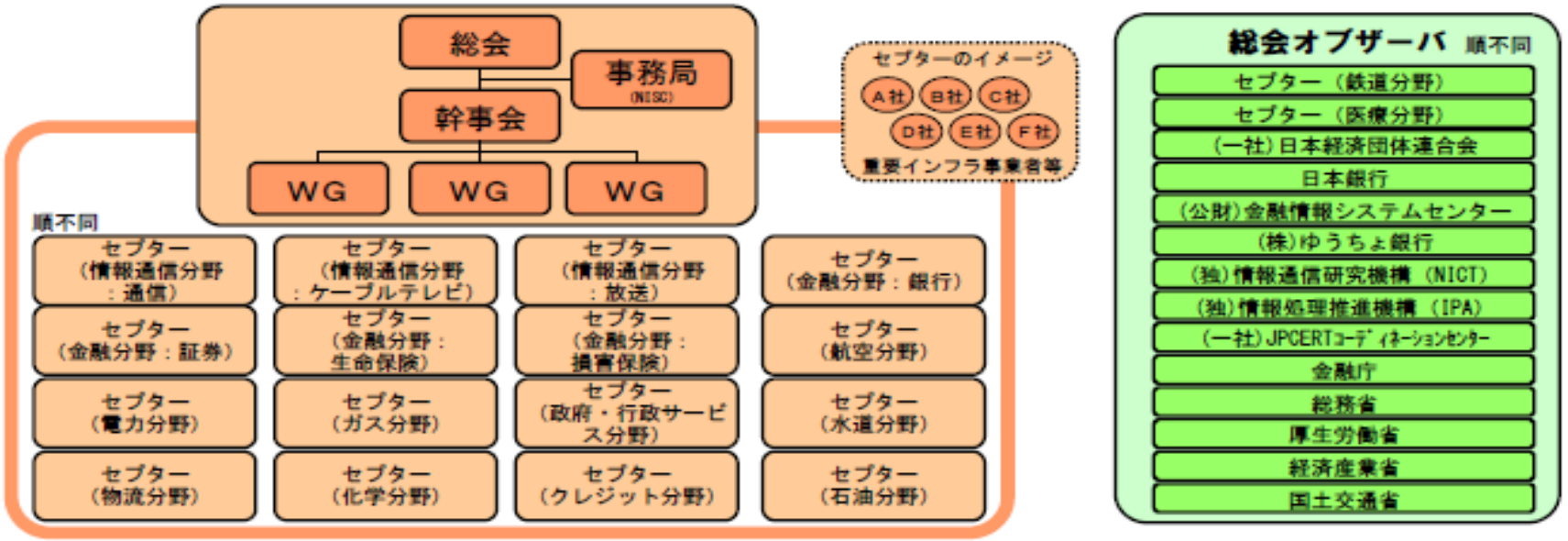
NISC

セプター（CEPTOAR） Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- IT障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

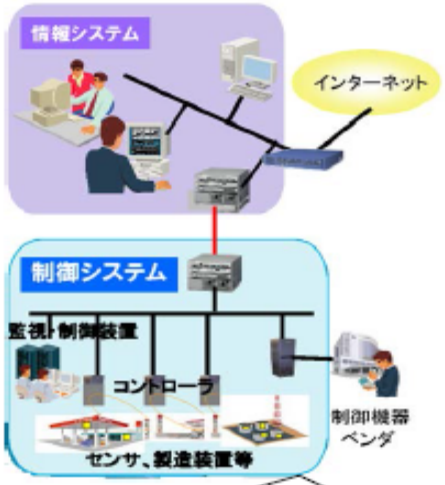
- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、2009年2月26日に創設。



出典：情報セキュリティ政策会議重要インフラ専門委員会第38回会合資料より

制御システムの普及

NISC



従来

制御システムは事業者毎に固有の仕様部分が多く、詳細な内部仕様等を把握できない限り、外部からの攻撃は難しいものであった。

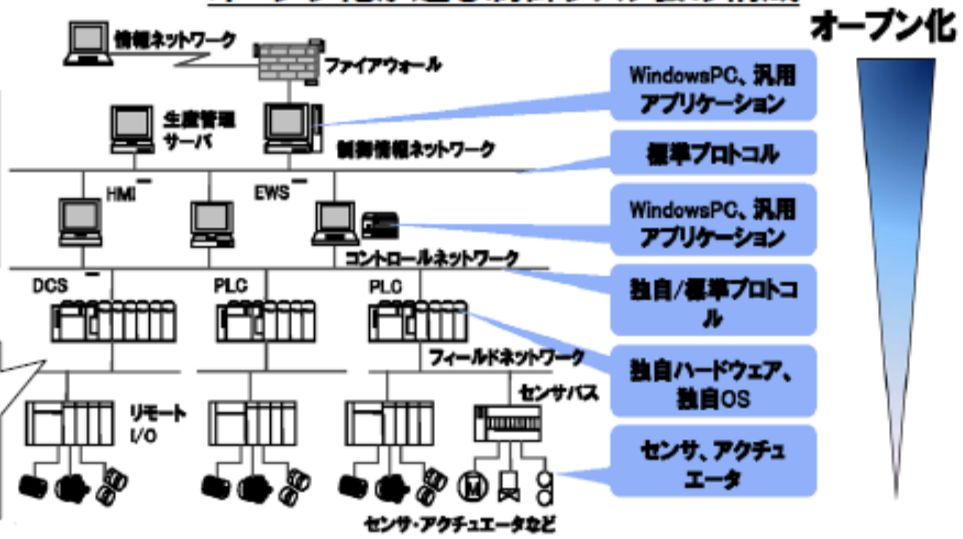
最近の状況

- ○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
- ○ 外部ネットワークにも接続されるようになっている。
- ○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。

- ○ 生産の自動化や、フィードバック制御による入力値の自動制御等、様々な用途で工数の軽減や正確性の向上を目的に利用。
- ○ 最近は、一般的な情報システムが接続するオフィスネットワークから、制御情報系ネットワーク、制御ネットワークを介して、制御システムのコントローラやセンサーまでを間接的に接続するような構成が多い。

- ○ アプリケーション等が動作する上層のレイヤではWindowsのパソコン等のクライアント端末や汎用アプリケーション、標準プロトコルを利用。
- ○ 実際の制御に関わる下層部分は独自のプロトコルやハードウェア、OSが利用される割合が高く、固有の仕様により構成。
- ○ オープン化が上層部から徐々に進行。

オープン化が進む制御システムの構成



【出典：独立行政法人情報処理推進機構「制御システムセキュリティ国際標準の現状と日本の取組み」（2011年11月18日）http://www.ipa.go.jp/files/000025094.pdf】

26

目次

1. サイバー空間における攻めと守りの状況
2. サイバーセキュリティの政策
3. サイバーセキュリティのガバナンスと産業化
4. 次世代を担うCISOの育成
5. 官民連携の在り方
6. 今後のサイバー空間の安心安全

３．サイバーセキュリティのガバナンスと産業化

● 重視するポイント

● 「予防体制の整備」と「事故発生時の迅速な対応」

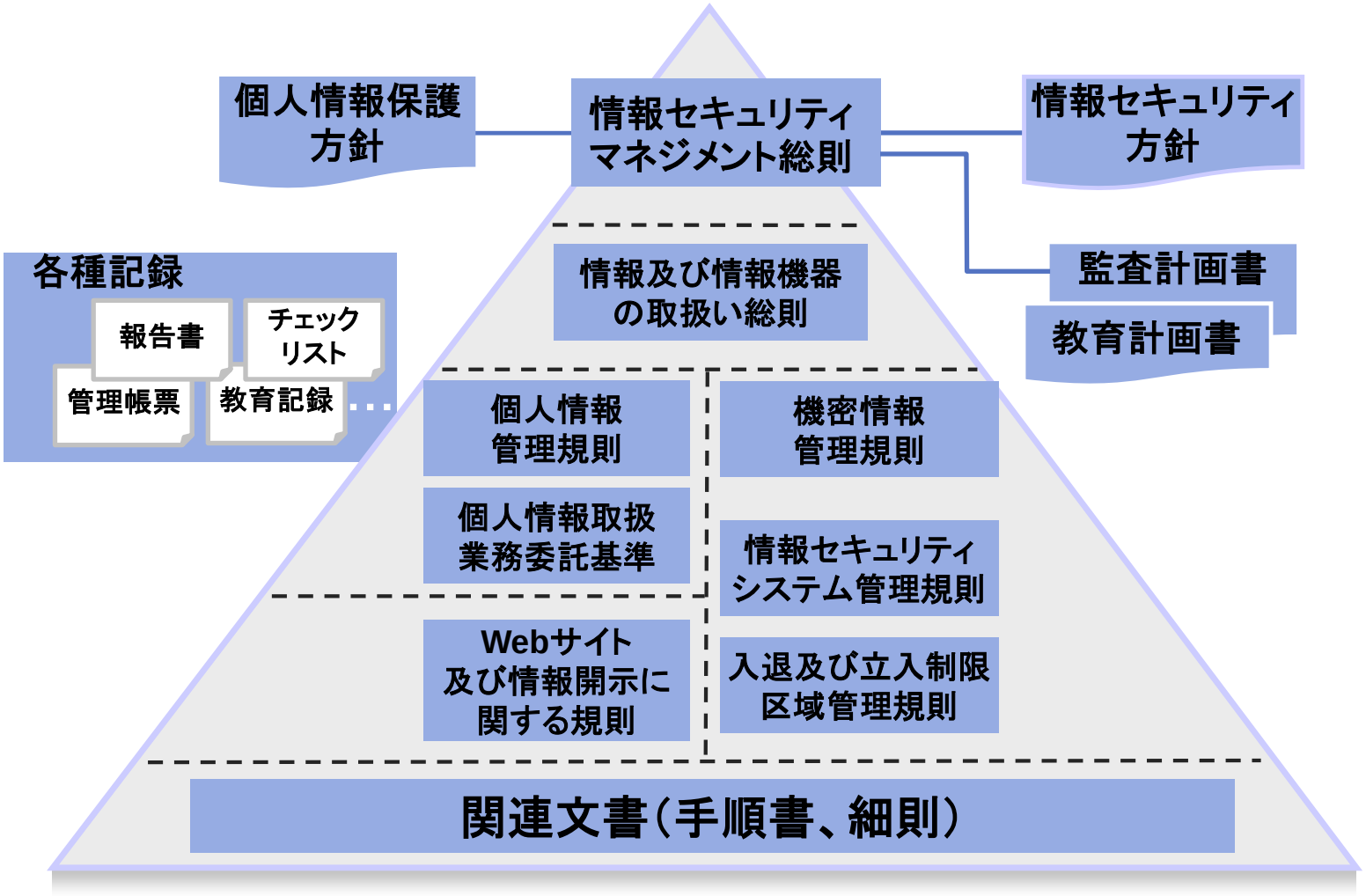
- 守るべき情報資産を明確にして、脆弱性評価とリスク分析結果に基づいたセキュリティ対策を実施
- 「事故は起きるかもしれない」という考え方から一歩進めて、「事故は必ず起こるもの」という前提に立った迅速な対応を実施

● 利用者のセキュリティ意識向上

- 情報セキュリティを継続して守っていくためには、一人ひとりが、日々の情報を取り扱う上で必要な知識を身につけ、高い意識を持つことが重要
- 階層別のカリキュラムを用意し、e-ラーニングによる全員教育などを通じて、倫理観とセキュリティ意識の向上を推進

3．サイバーセキュリティのガバナンスと産業化

● 情報セキュリティ関連規則・文書体系図



3．サイバーセキュリティのガバナンスと産業化

● 情報セキュリティ教育

対象者	形態	内容
情報資産管理者	・座学形式	各部署で情報資産の管理責任者として行動するために必要な知識教育
管理職教育	・座学形式	個人情報保護、情報セキュリティ、機密情報管理について管理職として必要な知識を身に着ける教育
新入社員教育	・座学形式	情報セキュリティ、機密情報管理について新入社員として必要な知識を身に着ける教育
全員教育	・Eラーニング	個人情報保護、情報漏えい防止、機密情報管理に関する基礎を身に着ける教育
全員教育	・演習形式	実例に基づいたケーススタディを用い、その原因、対策を考えることにより、情報の取扱いに関する実践的知識を身につける教育
情報セキュリティ担当者	・宿泊研修形式	個人情報保護、情報セキュリティ、機密情報管理に関する詳細な知識教育。事例を踏まえた実践演習
情報システム担当者	・座学形式 ・一部演習形式	ネットワークセキュリティ、セキュリティインシデント対応、Webアプリケーションセキュリティ、社外公開サーバセキュリティに関する情報システム担当者向けの教育

３．サイバーセキュリティのガバナンスと産業化

- 情報セキュリティ監査
  - 情報セキュリティ監査責任者の指揮のもとで、1回/年で実施
  - 情報セキュリティ監査での確認事項
    - 情報セキュリティ規則と情報資産の管理および情報セキュリティ対策の合致状況
    - 個人情報保護およびJIS Q 15001:2006と個人情報管理体制の合致状況
    - 個人情報保護マネジメントシステムとJIS Q 15001:2006の合致状況

● サイバーセキュリティのビジネス体制

● 職制

- 本体内に位置づく正式職制としての組織
  （独立あるいは同様な位置づけの組織の一部、見えることも重要）
- 組織としてしっかりした内部体制を持つ（上長、部下、査定権他）

● 予算

- コストセンタとして運営（人件費、調査他活動費、その他共通費）
- 財源：本社共通費

● 位置づけ

- セキュリティ関連の業界動向を把握
- セキュリティ関連の最新技術を把握・蓄積

● 構成

- 事業の分かる人員（幹部管理職候補）とセキュリティ状況のわかる人員（専門職候補）
- 名称、組織構成、委員会の設定、兼務者・出向元活動費負担等

３．サイバーセキュリティのガバナンスと産業化

● サイバーセキュリティのビジネス体制

● 評価・ポジション・キャリアパス（計画的に実施）

- 専門技能職：技能レベルに応じた評価・格付け・昇格（新たな体系の導入）
- 管理職：評価・格付け・昇格
- 管理職候補のローテーション

＊セキュリティと関係しない人材のポジションにはしない
（単なる管理職としてのポジション）

● ミッション

- セキュリティ関連の動向把握に基づく企画、調整（ガバナンス）
- セキュリティ関連能力の蓄積（人財散逸防止）、人財育成、専門サービスの提供

● その他

- グローバルな体制、人員確保（何処かを母体）、連携についても検討する必要有り
- 具体的なフィールドを持ち、設計、テスト、インシデント対応他に参加することで、常に実践的な技術力の向上を図る機能を持つ
（情報システムセキュリティ、先進システム環境のセキュリティ管理他）

3．サイバーセキュリティのガバナンスと産業化

1．現状認識と課題

1　現状認識

- 我が国の情報セキュリティ産業は一定の市場規模を有しているが、現状、ソフトウェア、ハードウェアいずれにおいても、世界市場を席巻するプラットフォーム製品やビジネスモデルを有していない。
- 他方、要素技術の研究開発においては、次世代暗号や制御システムに係るセキュリティ技術等においては世界をリードしており、その有効活用が課題。
- また、セキュリティ技術等を製品に実装する能力に優れている。

2　産業活性化に係る課題

- 要素技術に係る優れた研究開発を実用化につなげることが重要。
- 我が国が得意とする実装能力を有効活用し、例えば、自動車産業におけるセキュリティの組み込み等の、分野ごとのカスタマイズされたセキュリティ実装に積極的に取り組むことが有効。

1

2．課題解決に必要な取組

【具体策】

（1）研究開発の積極的実用化
- ・企業における積極的経営（選択と集中、個性化）
- ・研究開発戦略への実用化目標の掲載
- ・官による国産製品の積極的導入
- ・実用化支援施策の展開（資金供給、目利き等）

（2）市場拡大
- ・セキュリティ製品等導入支援（企業におけるリスク評価等支援）
- ・経営者に対する普及啓発

（3）要考慮事項
- ・安全保障に係る技術の国内産業化

2

3．サイバーセキュリティのガバナンスと産業化

参考1．情報セキュリティ産業の現状

■日本の情報セキュリティ産業の現状

2011年度の我が国の情報セキュリティ市場は約64．3億ドル/年であり、世界全体の市場規模が約539億ドル/年に対するシェアは12%程度。(※1)

2011年度の我が国の情報セキュリティ市場の成長率は+9.9%とされている。世界全体の成長率は13.1%とされており、世界全体に比べて、日本の産業成長率が低い傾向にある。(※1)

情報セキュリティ市場は、大きく情報セキュリティツール市場と情報セキュリティサービス市場に分けることができる。2011年度における両者の割合は、26%、74%である。(※1)

研究開発成果を直接活用するのはツール市場であり、その規模は、約14億ドル程度である。市場の内訳では、「個人向けセキュリティソフトウェア」「エンドポイントセキュリティ・プラットフォーム」が多く、合わせて54%を占めると報告されている。

補足：

JNSAによる報告書(※2)では、2011年度の我が国の情報セキュリティ市場は、約6483億円であり、上記とほぼ一致しているが、市場成長率は-2.4%としている。また、2011年度のツール市場とサービス市場の割合は、55%、44%となっている。ガートナーの調査との差異は、一般のインテグレーションやITマネジメントサービスを含めていないことが主因と考えられる。

※1：平成23年度企業・個人の情報セキュリティ対策促進事業(情報セキュリティの市場調査)調査報告書(平成24年3月　ガートナージャパン株式会社)
※2：2010－2011年度情報セキュリティ市場調査報告書V1．0(2012年1月　NPO日本ネットワークセキュリティ協会)

3

3．サイバーセキュリティのガバナンスと産業化

参考2. 研究開発の現状

■研究開発の水準

JSTによる報告書(※1)によると、セキュリティ・ディペンダビリティ分野における研究開発レベルは、「暗号・認証基盤および応用」「量子情報セキュリティ」が非常に進んでいる、「ネットワークセキュリティ」「コンピュータセキュリティ」について遅れているが、他の分野は進んでいる、という報告がなされている。

ただし、本報告書は専門家集団による主観評価によるものであり、「ネットワークセキュリティ」に関して、NICTで運用しているJGN-X(新世代通信網テストベッド)等の先進的な活動についての言及がなく、低めに評価されている可能性がある。

このことより、我が国の情報セキュリティに関する研究開発レベルは、一部を除き一定の先行レベルにあるといえる。

	ディペンダブル情報システム		管理・運用・評価認証		暗号・認証基盤および応用		ネットワークセキュリティ※1		コンピュータセキュリティ		仮想化		量子情報セキュリティ		ハードウェアセキュリティ		生体認証	
研究水準	○	→	○	→	◎	→	△	↗	△	→	○	→	◎	→	○	↗	○	→
技術開発水準	○	→	○	↗	◎	↘	△	→	○	→	○	→	◎	→	○	↗	◎	→
産業技術力	○	→	◎	↗	◎	↘	△	↗	○	→	○	→	○	→	○	↗	○	↘

凡例
「研究水準」:大学・公的研究機関の研究レベル
「技術開発水準」:企業における研究開発のレベル
「産業技術力」:企業における生産現場の技術力(注:製品と市場の両方の視点が含まれている)
左欄(現状):◎非常に進んでいる ○進んでいる △遅れている ×非常に遅れている
右欄(近年のトレンド): ↗上昇傾向 →現状維持 ↘下降傾向

出典:科学技術・研究の国際比較2011年版 電子情報通信分野(独立行政法人科学技術振興機構 研究開発センター)より
セキュリティ・ディペンダビリティ分野の該当部分を抜粋

4

3．サイバーセキュリティのガバナンスと産業化

参考3. 研究開発の現状（つづき）

■科学技術・研究の国際比較2011年版 電子情報通信分野（独立行政法人科学技術振興機構 研究開発センター）より
セキュリティ・ディペンダビリティ分野の該当部分を抜粋

		ディペンダブル情報システム		管理・運用・評価認証		暗号・認証基盤および応用		ネットワークセキュリティ		コンピュータセキュリティ		仮想化		量子情報セキュリティ		ハードウェアセキュリティ		生体認証	
日本	研究水準	○	→	○	→	◎	→	△	↑	△	→	○	→	◎	→	○	↑	○	→
	技術開発水準	○	→	○	↑	◎	↓	△	→	○	→	○	→	◎	→	○	↑	◎	→
	産業技術力	○	→	◎	↑	◎	↓	△	↑	○	→	○	→	○	→	○	↑	○	↓
米国	研究水準	◎	↑	◎	↑	◎	→	◎	→	◎	→	◎	→	◎	→	◎	→	◎	→
	技術開発水準	◎	↑	◎	↑	◎	→	○	→	◎	→	◎	→	◎	→	◎	→	◎	→
	産業技術力	○	↑	◎	→	◎	→	○	→	◎	→	◎	→	○	→	◎	→	◎	→
欧州	研究水準	◎	↑	◎	↑	◎	→	○	↑	○	→	○	→	◎	→	◎	→	◎	→
	技術開発水準	○	↑	◎	→	○	→	○	↑	○	→	○	→	◎	→	◎	→	◎	→
	産業技術力	○	→	◎	→	○	→	△	→	○	→	△	→	○	→	◎	→	◎	→

凡例
「研究水準」：大学・公的研究機関の研究レベル
「技術開発水準」：企業における研究開発のレベル
「産業技術力」：企業における生産現場の技術力（注：製品と市場の両方の視点が含まれている）

左欄（現状）：◎非常に進んでいる ○進んでいる △遅れている ×非常に遅れている
右欄（近年のトレンド）：↗上昇傾向 →現状維持 ↘下降傾向

5

目次

1. サイバー空間における攻めと守りの状況
2. サイバーセキュリティの政策
3. サイバーセキュリティのガバナンスと産業化
4. 次世代を担うCISOの育成
5. 官民連携の在り方
6. 今後のサイバー空間の安心安全

4．次世代を担うCISOの育成

- セキュリティ人財
  - 情報セキュリティ技術者（IPAによる）
    - 従事者：約23万人
    - 内訳：スキルあり　約9万人
    - 　　スキルなし　約14万人
    - 不足者：約8万人
  - 大学院、大学、高専、専門学校（IPAによる）
    - 受講可能学生：約2万人
    - 論文等執筆学生：約1000人
  - 求められるセキュリティ人財
    - サイバー攻撃技術に精通する人財
    - サイバー攻撃を分析する人財
    - インシデント対策する人財
    - システムの脆弱性を発見する人財
    - 欠陥のないシステムを開発する人財
  - 中長期的な育成/安定的な採用
    - 大学社会人コースへの派遣
    - ローテーションやポストの確保

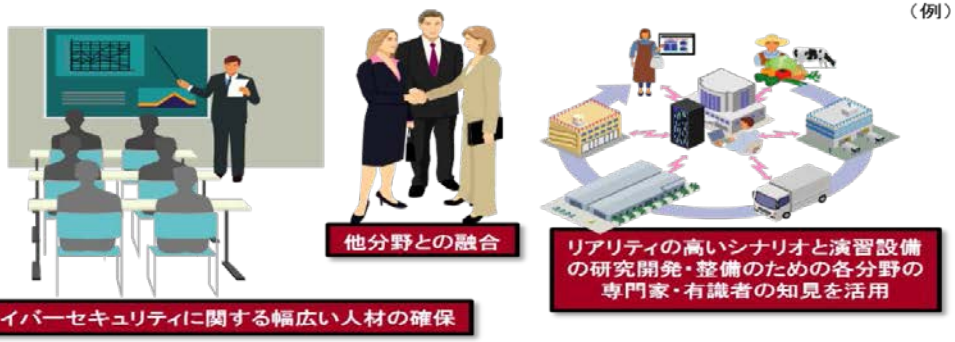
4．次世代を担うCISOの育成

- サイバーセキュリティ人材の育成等

IT 利用の拡大や高度化に伴い、2020 年頃及びそれ以降における日本のサイバーセキュリティを支えるための人材ニーズの想定等マイルストーンを示 しつつ、人材育成や新規産業に挑戦するベンチャー企業を指導・支援する専 門家、メンター等を確保し、裾野を拡大していく必要がある。

【実現のための取組例】

- 攻撃者側の攻撃手法等も熟知した技術者の育成
- サイバーセキュリティの技術教育のみでなく、組織経営、安全保障・ 危機管理、法学、心理学等といった他分野との融合を促進
- 各国が強みを有する技術を有機的に組み合わせ、発展させることによる高度な技術開発や、ASEAN諸国等との人的関係強化のため、海外からの優秀な人材の獲得、共同研究などの支援の充実を含め、国際連携 による研究開発を推進。その際、相手国のセキュリティに係る技術水準 等に応じた関係を構築。
- セキュリティ人材不足解消のために学生・社会人を対象に教育コースの充実を図ると共に経営層・現場管理者・オペレータ等のレイヤごとに 普及啓発を行いつつ、連携を意識したプログラムを開発し、全体の底上げを図る。特に経営層に対する取組はサイバーセキュリティ人材の需要 喚起の点から重視。
- 経営層へのセキュリティ意識の浸透のため、大学等教育機関における 経営学分野等のセキュリティ教育を充実
- 事案対処能力を向上するためには、大規模自然災害、オリンピック開催に不可欠なインフラの運用停止、設備の盗難破壊といった多種多様なシナリオにサイバーセキュリティに関するコンポーネントを加えた総合的なアプローチが必要。そのため、産学官が国内外と協力し、演習・訓練環境の整備及びシナリオ作りに早急に着手。
- 公的研究機関とベンチャー企業との共同研究や研究開発成果を活用したベンチャー企業の育成
- ベンチャー企業育成の一環として、産学官が連携し、起業志向の学生 に対する意識付けを促進



※ オリンピック・パラリンピック東京大会に関する取組も重要な契機。

（例）

● 米国Emergency Management Institute
国家的な危機管理訓練、演習、教育を牽引する組織

● 英国Emergency Planning College
首相府直属の緊急事態計画大学
事例研究等を通じた実践的な内容を提供

出典：NISC「IT利活用セキュリティにおける総合的かつ戦略的政策推進に係る提言」資料より

4．次世代を担うCISOの育成

●CISOの有無

- CISO（Chief Information Security Officer：最高情報セキュリティ責任者）
  - 「CISOはいない」： 57.7%
  - 「兼務者がいる」： 37.6%
  - 「選任者がいる」： 3.4%

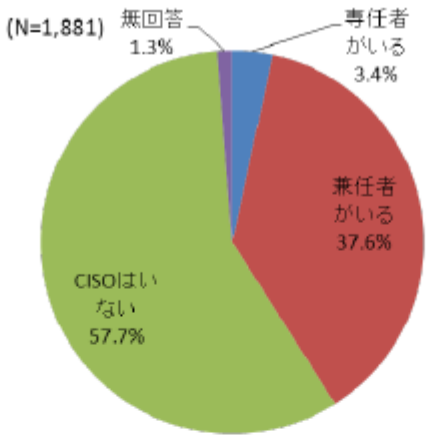


図 3.2-3 CISO の有無

- 「300人以上企業」
  - 「CISOはいない」： 48.9%
  - 「兼務者がいる」： 3.4%
- 「300人以下企業」
  - 「CISOはいない」： 65.8%
  - 「兼務者がいる」： 30.4%

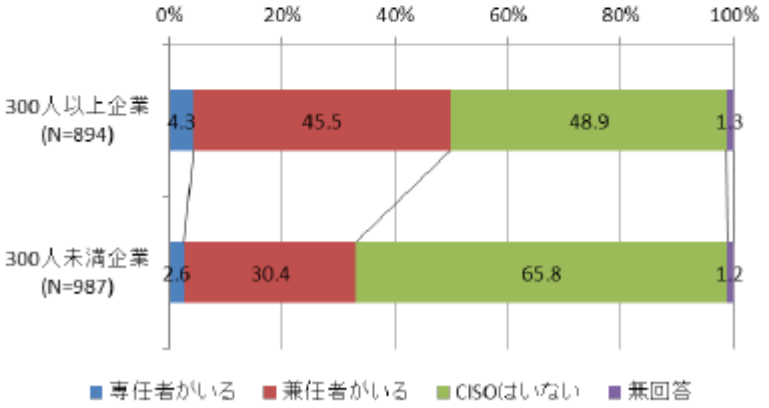


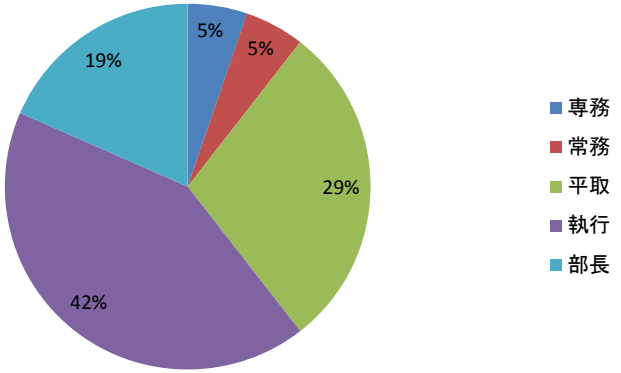
図 3.2-4 CISO の有無（従業員規模別）

4．次世代を担うCISOの育成

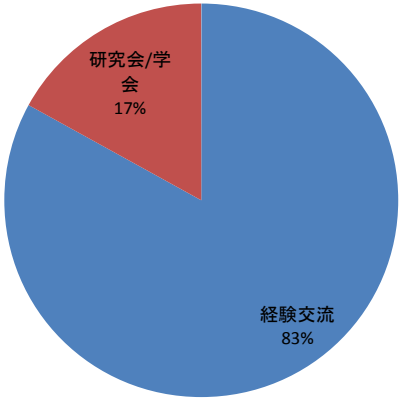
●参照型アプローチの限界

- CIO/CISOは根本的な課題に取り組むための組織的な地位に不足はない
- CIOやCISOは経験交流に熱心で、お互いに体験談や成功例の共有に努めている
- 課題の本質を見抜くのは難しく、参照型アプローチになりがち
- 現実に発生している様々な問題の背景には、このような参照型アプローチの限界があると思われる

CIOの職位



CIOの参加する情報収集先



日経情報ストラテジー「CIO登場」に出ている38人のCIOの実態から
http://itpro.nikkeibp.co.jp/article/COLUMN/20090803/335057/ 2011/02/02アクセス

4．次世代を担うCISOの育成

● 組織における学位取得者の日米比較

- CISOは技術に加えて、経営・組織・人事・法律等の高度で専門領域横断的な専門知識が必要とされる
- わが国では、マネジメントに関わる組織的な地位にある幹部に学位取得者の割合が高いとはいえない
- 就職後もっぱら組織内教育により人材育成を図ることが中心となっている
- アメリカにおいては企業幹部のMBAやJD(Juris Doctor)以上の学位取得がある程度常識となってきており、連邦政府職員や軍幹部においても学位取得者の割合は高い

出典：日本セキュリティ・マネジメント学会第25回全国大会資料より

4．次世代を担うCISOの育成

● 企業の人材育成の課題

- 日本企業は、企業文化を人材育成プログラムの中に取り込み、これを中心に据えて、その企業でのみ使われる仕事のノウハウを教育する傾向がある
- 企業に対する忠誠心とその企業特有の仕事のやり方によって効率化を実現する
- セキュリティのマネジメントにおいて、理論的な最適解は探求されるにしても、企業内の価値観に基づいて意思決定が行われる傾向がある
- このような風土においては、理論的な最適手法に長けた人材はむしろ出る釘(杭)として排除されやすく、客観的・普遍的価値観に基づいて様々な課題に対応できる「目利き」が育ちにくい環境にある
- 国際競争力を考えた場合に、我が国においては汎用性を持った総合力を備えた人材を育てることはなかなか難しい

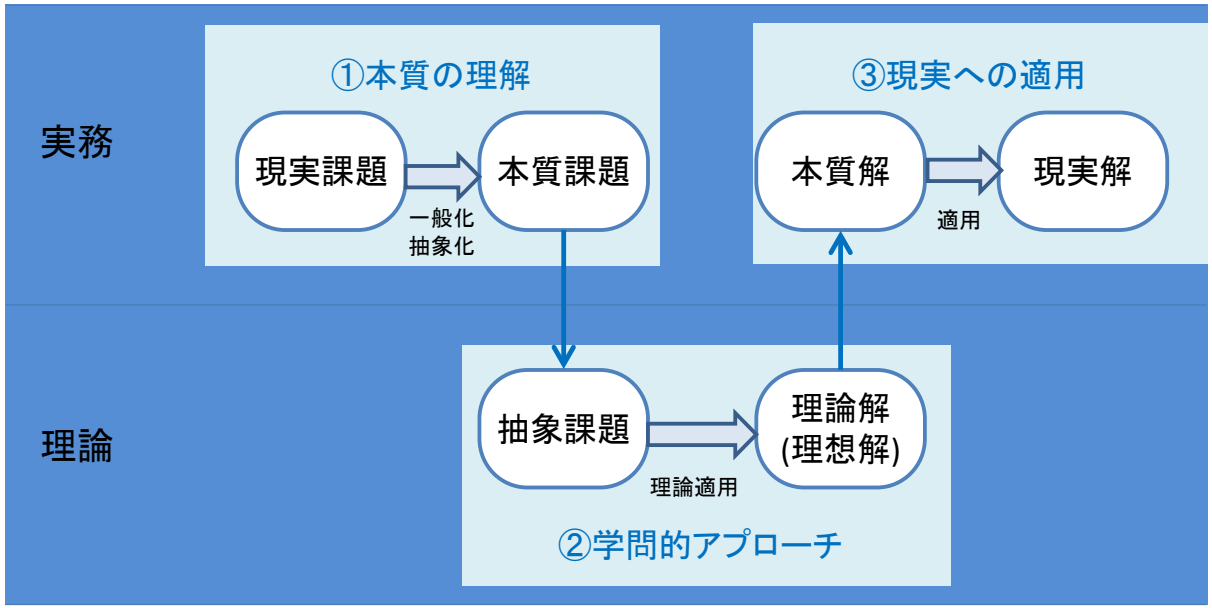
出典：日本セキュリティ・マネジメント学会第25回全国大会資料より

4．次世代を担うCISOの育成

● 産学連携の共同作業

- セキュリティのマネジメントを総合科学として発展させるためには、理論と実務を統合したアプローチが不可欠である

- 産の実務に基づく本質的な課題設定と、学の抽象課題から理論解を見つける普遍的方法論とを、本質課題を通して連結することが、産学連携の一つの重要な解決の糸口になる



- 理論解を本質解に解釈しなおす力が求められる

- CISOが、自らの課題を抱えて、学のアプローチの習得に取り組むのがベスト

4．次世代を担うCISOの育成

● 産の取り組み

- 企業活動の中核にセキュリティマネジメント思想をしっかりと植えつけることが肝要

- セキュリティリスクの認識をトリガーとした客観的普遍的価値観を取り込むべき

- 経営方針に取り込むとともに、人材育成にも工夫を盛り込むべき
  - 実務の本質がわかる人材の育成
  - 実務の本質的な問題選定ができる人材の育成
  - 学の力を借りて問題解決を的確にできる人材の育成

- 専門性と汎用性の両方を備えたT型人材さらにはΠ型人材をいかに育てるのかが、今後の我が国の産業競争力を高めるための重要な点である

目次

1. サイバー空間における攻めと守りの状況
2. サイバーセキュリティの政策
3. サイバーセキュリティのガバナンスと産業化
4. 次世代を担うCISOの育成
5. 官民連携の在り方
6. 今後のサイバー空間の安心安全

５．官民連携の在り方

● 官民連携

- 政府としてとるべき方策、特に調達先企業に求める情報セキュリティ要件

> ●一般の調達等において、国の安全に関する重要な情報を扱う契約を締結する際には、情報セキュリティ上必要な事項を遵守するよう求める。

- 政府と企業等との連絡・連携の在り方

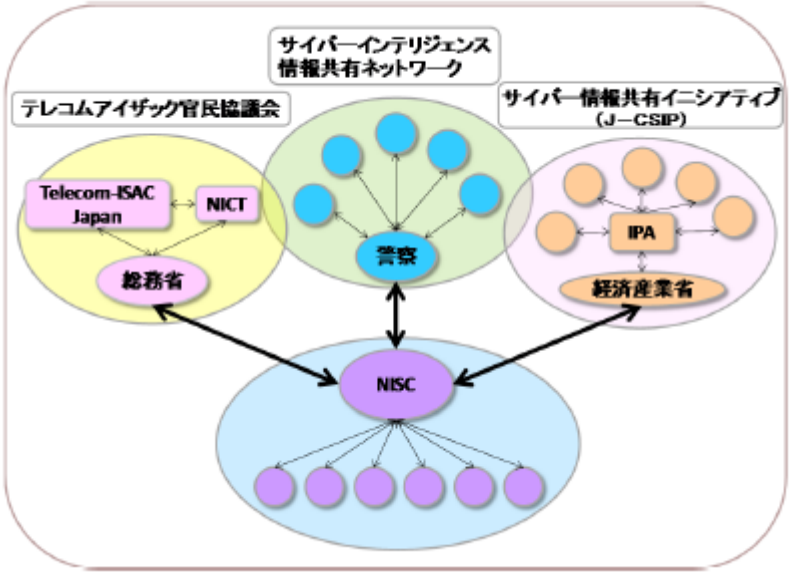
> ●CSIRT の横断組織である日本シーサート協議会や JPCERT コーディネーションセンター、情報セキュリティ事業者（SOC(Security Operation Center)事業者）、(独)情報処理推進機構と政府の調整役 CSIRT である内閣官房情報セキュリティセンターとの連携、情報交換の緊密化を図る。

5．官民連携の在り方

● 官民連携

● 政府と企業等との連絡･連携の在り方（続き）

●NISC は、警察庁のサイバーインテリジェンス情報共有ネットワーク、経済産業省のサイバー情報共有イニシアティブ(J-CSIP)、総務省のテレコムアイザック官民協議会等と NISC が運用する府省庁間のインシデント情報共有ネットワークとの情報連携の結節点の役割を果たす。



出典：情報セキュリティ対策推進会議官民連携の強化のための分科会資料より

５．官民連携の在り方

● 官民連携

- 産業界の取組に対する政府の協力、情報提供の在り方

●SOC 事業者において、高度な対応を可能とするため、顧客の情報の一部を連携する諸機関と共有できるような標準的な契約、ひな形約款の策定に向けた検討を行う。

- 企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等

●企業等における組織内 CSIRT 等の整備、情報セキュリティ人材の育成、標的型攻撃等の最近の情報セキュリティに関する状況等について広く官民で意見交換を行うためのシンポジウム等を開催する。

5．官民連携の在り方

情報共有体制の強化

行動計画-III.2（p15～）

NISC

多様な脅威に対応するため、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策に加え、分野内、分野間あるいは官民間の情報共有を一層強化する。

行動計画期間当初の課題

- 情報共有頻度の分野間格差の解消
- 「脅威の類型」の細分化
- 大規模IT障害対応時の情報共有体制の構築
- 新たな関係主体との連携の在り方の整理　　等

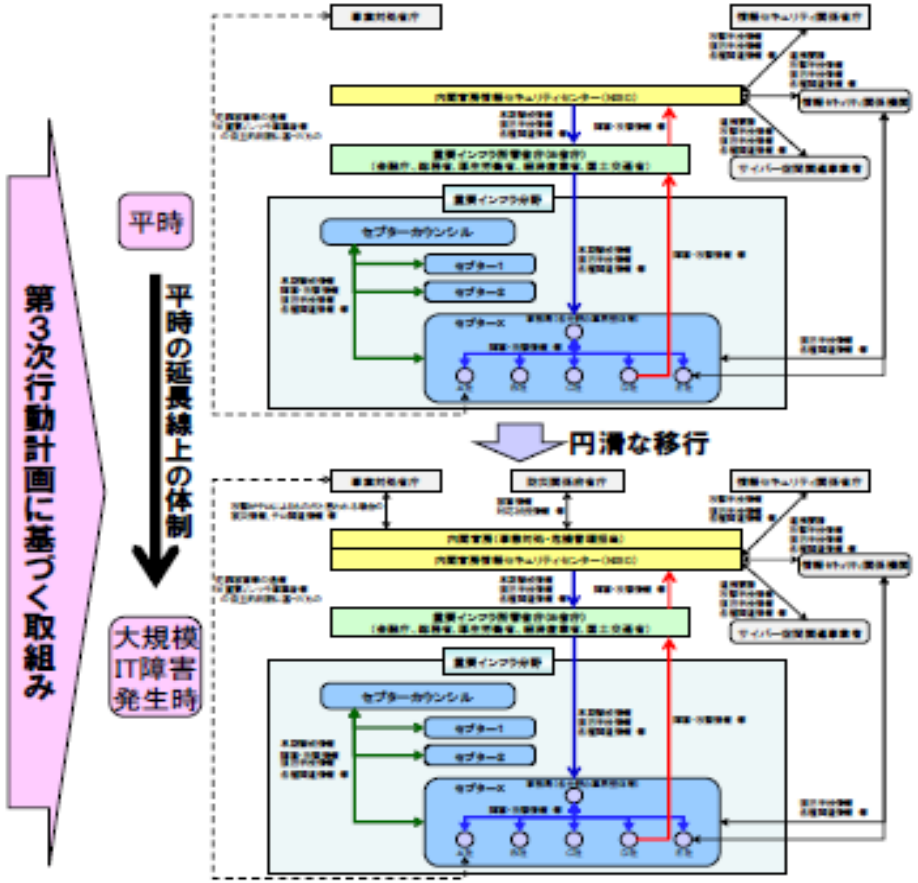
行動計画期間中の施策

（1） 情報共有体制の発展
- 新たな関係主体※の追加
  ※防災関係府省庁、サイバー空間関連事業者
- 平時とその延長線上の大規模IT障害対応体制の構築

（2） 情報共有の更なる促進
- 迅速・正確な状況把握のための情報連絡・提供時の詳細項目の見直し
- セプターカウンシルを始めとするセプター間の情報共有の更なる充実

（3） 関係主体の役割の明確化
- 多様な関係主体の役割を平時・大規模IT障害発生時に分類して明確化

第3次行動計画に基づく取組み



8

目次

1. サイバー空間における攻めと守りの状況
2. サイバーセキュリティの政策
3. サイバーセキュリティのガバナンスと産業化
4. 次世代を担うCISOの育成
5. 官民連携の在り方
6. 今後のサイバー空間の安心安全

６．今後のサイバー空間の安心安全

●情報セキュリティとは

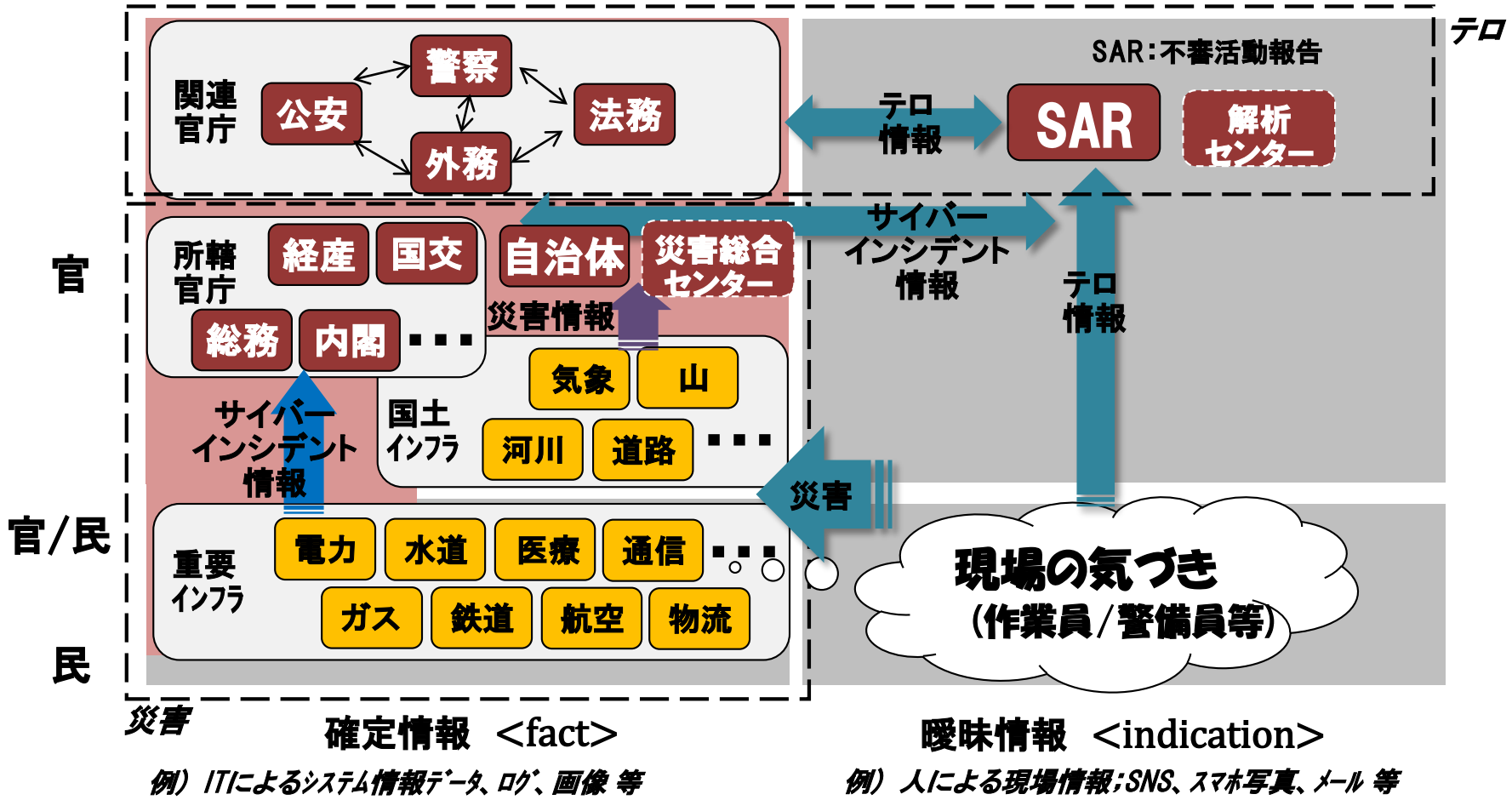
組織にとって価値ある情報資産を、
機密性、完全性、可用性の観点において維持するもの

●通称「セキュリティのCIA」と呼ぶ

機密性 Confidentiality	アクセス許可されたものだけが情報にアクセスできることを確実にすること
完全性 Integrity	情報及び処理方法が、正確であること及び完全であることを保護すること
可用性 Availability	許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること

６．今後のサイバー空間の安心安全

- 緊急対応を踏まえた「平時における」情報共有の在り方
- 災害、テロ対策を代表例として情報共有をシミュレート

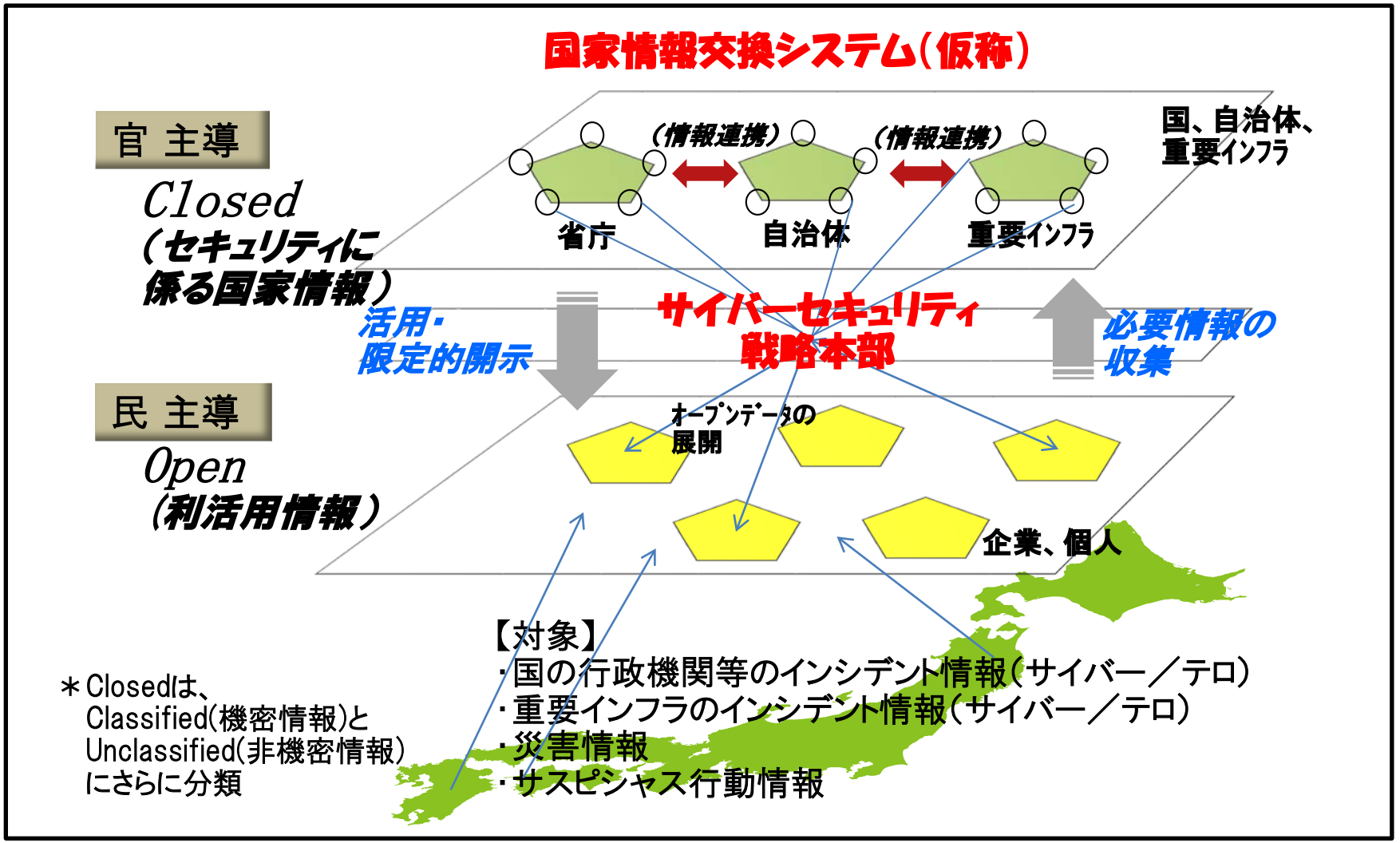


「現場の動き」を定常情報で裏付けし、予兆を検知し、現場へ指示

SAR：Suspicious Activity Report

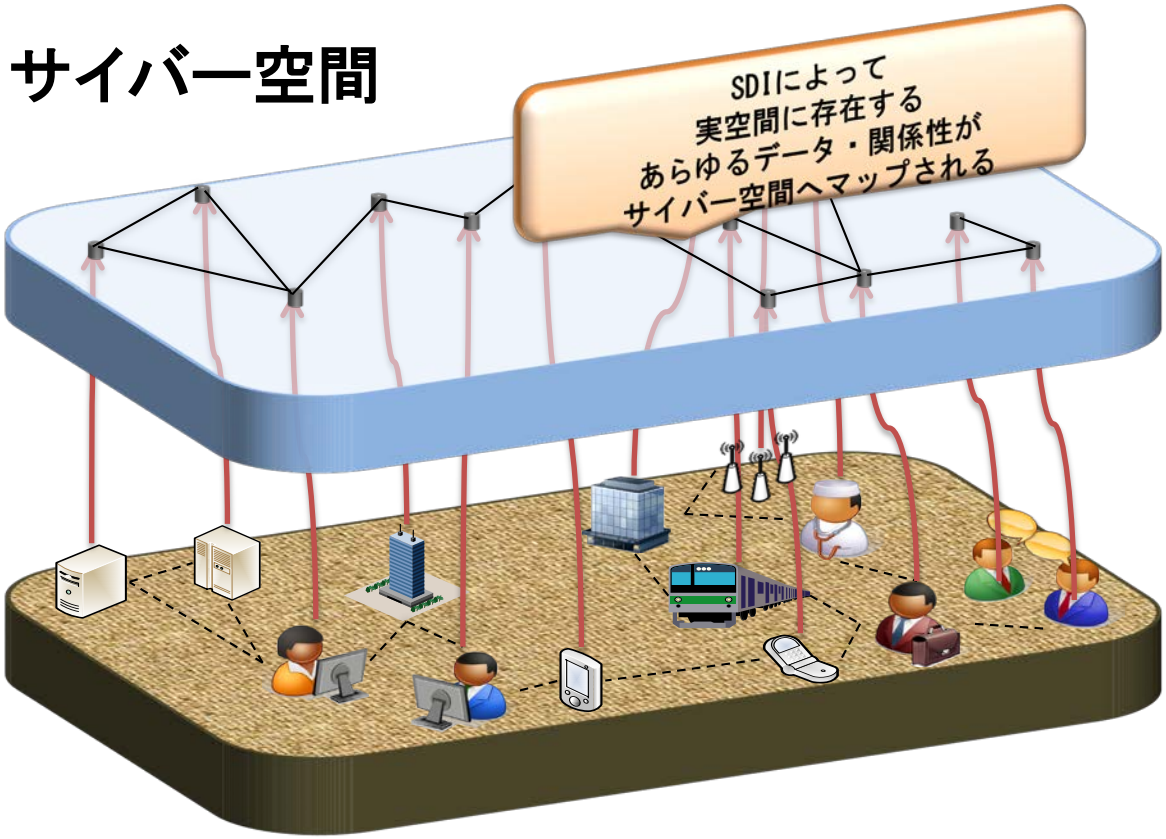
６．今後のサイバー空間の安心安全

「サイバーセキュリティ基本法」における重要施策の一つとして
国家における緊急情報の共有化を図るものとする



６．今後のサイバー空間の安心安全

- TSDI(Trusted Social Data Infrastructure)： ビッグデータ
- TSPI(Trusted Social Process Infrastructure)：ビッグプロセス



ビッグデータ

ビッグプロセス

IoT: Internet of Things