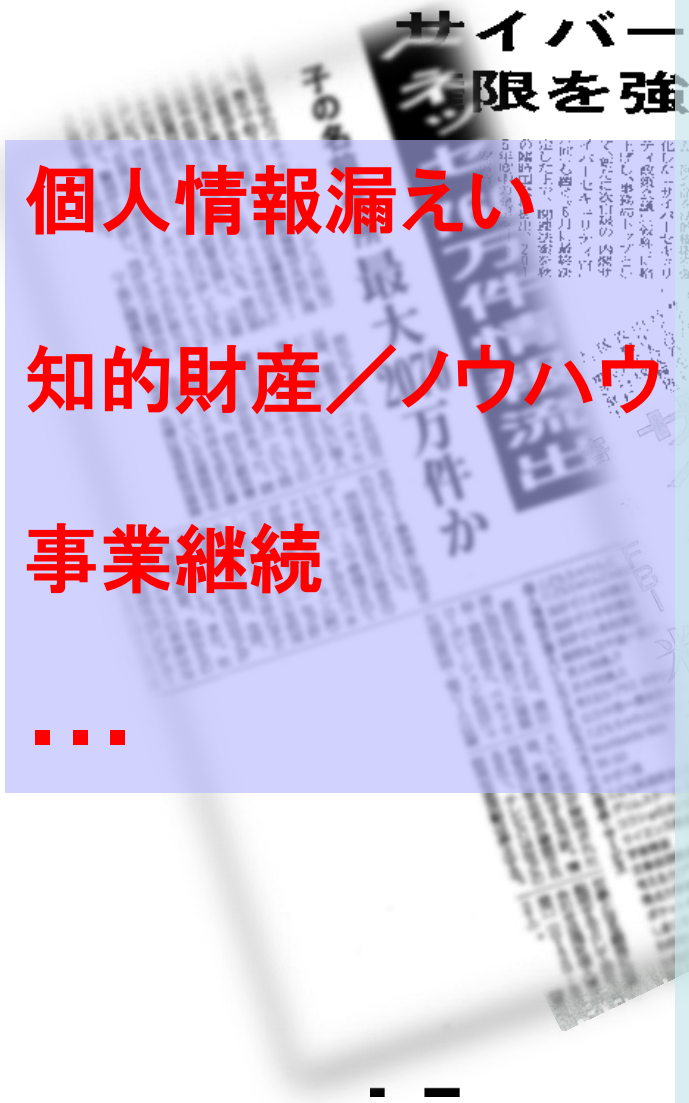
NISC

National center of Incident readiness and Strategy for Cybersecurity

我が国のサイバーセキュリティ政策について

平成28年9月
内閣サイバーセキュリティセンター（NISC）
内閣審議官　三角　育生

紙面を賑わす「サイバー」



個人情報漏えい

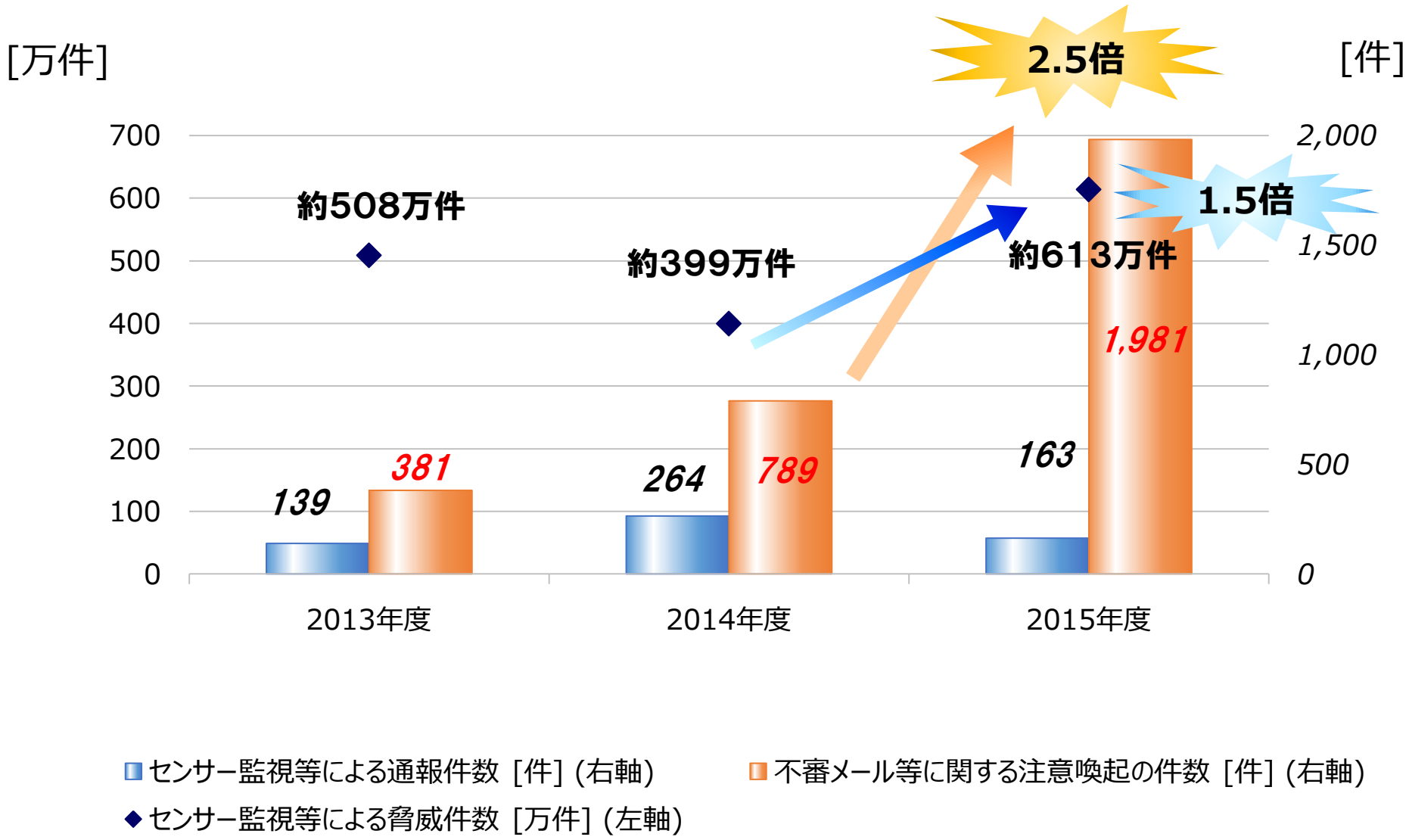
知的財産／ノウハウ

事業継続

・・・

- エストニアへの大規模サイバー攻撃（2007年5月）
- ジョージアへの大規模サイバー攻撃(2008年8月）
- 重工業・国会へのサイバー攻撃(2011年秋）
- 韓国重要インフラへのサイバー攻撃(2013年4月）
- 米国映画会社へのサイバー攻撃（2014年12月）
- フランスTV5モンド(2015年4月上旬）
- 日本年金機構(2015年6月上旬）
- 米国人事管理局(2015年6月上旬）
- ウクライナ電力網への攻撃(2015年12月）
- 旅行会社への攻撃(2016年6月）

リスクの深刻化 （政府機関等の状況）



※GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）におけるGSOCセンサー等による監視活動において、不審な通信やWeb サイトの障害等（疑いを含む）を検知し、当該政府機関へ通報した件数。

新たな「サイバーセキュリティ戦略」について（全体構成）

平成27年9月4日閣議決定

1 サイバー空間に係る認識

- サイバー空間：「**無限の価値を産むフロンティア**」である人工空間　経済社会の活動基盤
- 「**連接融合情報社会（連融情報社会）**」が到来
  サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

「自由、公正かつ安全なサイバー空間」を創出・発展➡**「経済社会の活力の向上及び持続的発展」**、**「国民が安全で安心して暮らせる社会の実現」**、**「国際社会の平和・安定及び我が国の安全保障」**に寄与

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ／②受動から**主導**へ／③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

費用から投資へ

- **安全なIoTシステムの創出**
- **セキュリティマインドを持った企業経営の推進**
- **セキュリティに係るビジネス環境の整備**

国民が安全で安心して暮らせる社会の実現

2020年・その後に向けた基盤形成

- **国民・社会を守るための取組**
- **重要インフラを守るための取組**
- **政府機関を守るための取組**

国際社会の平和・安定 我が国の安全保障

サイバー空間における積極的平和主義

- **我が国の安全の確保**
- **国際社会の平和・安定**
- **世界各国との協力・連携**

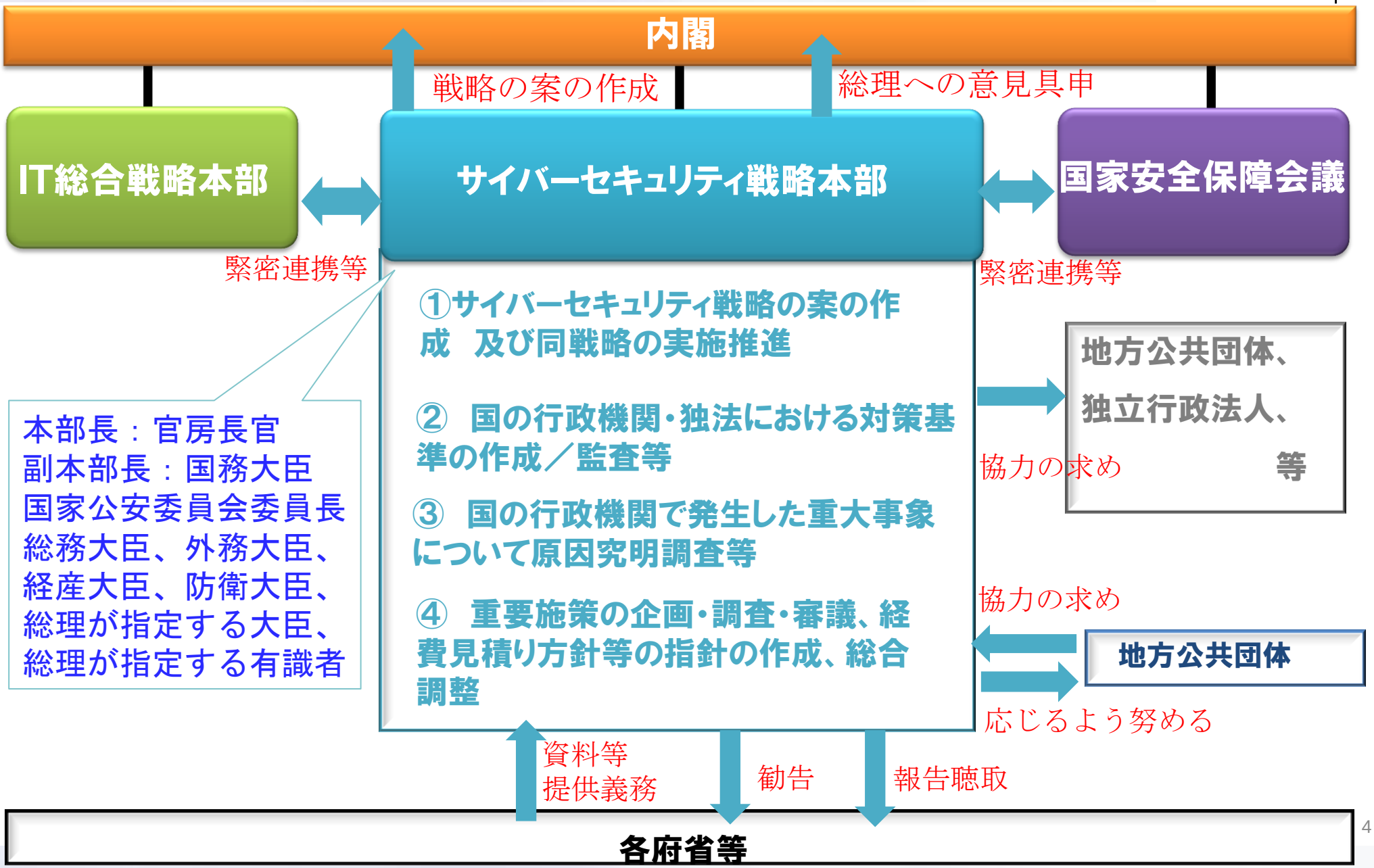
横断的施策

- **研究開発の推進**
- **人材の育成・確保**

5 推進体制

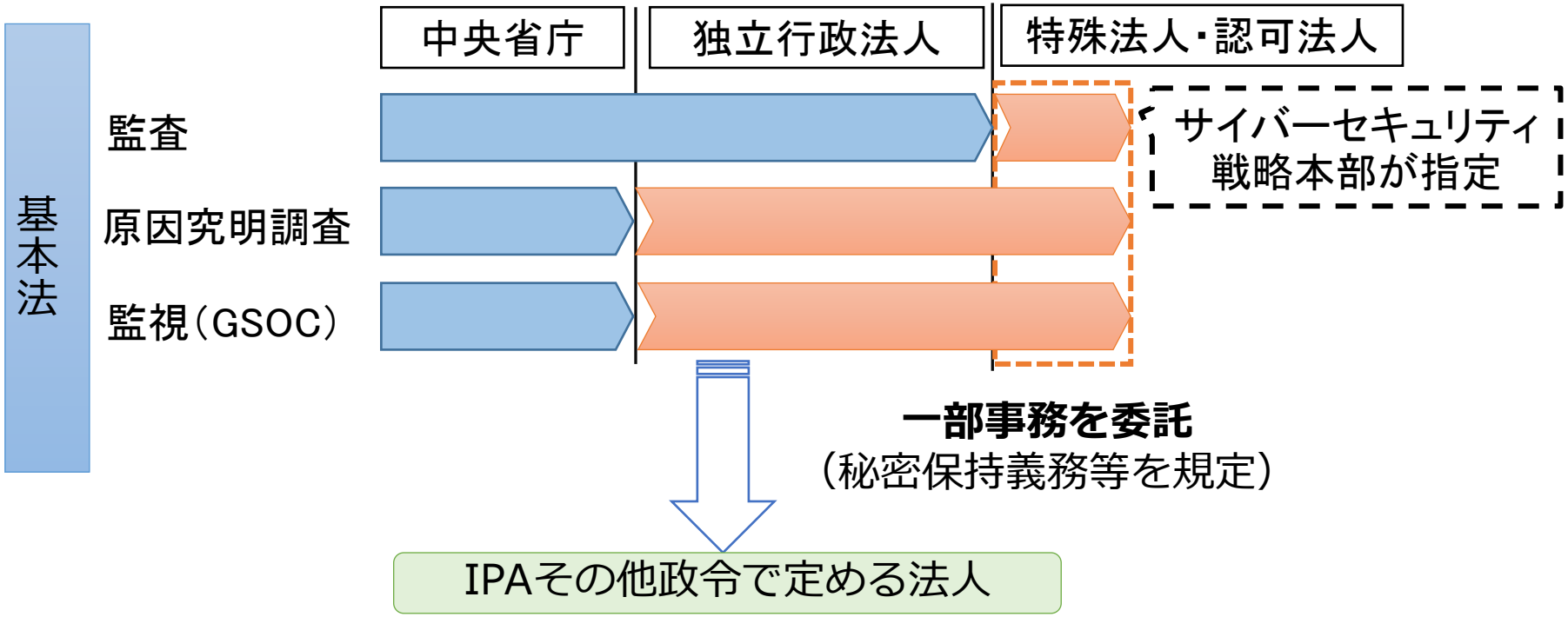
官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

サイバーセキュリティ戦略本部の機能・権限（イメージ）

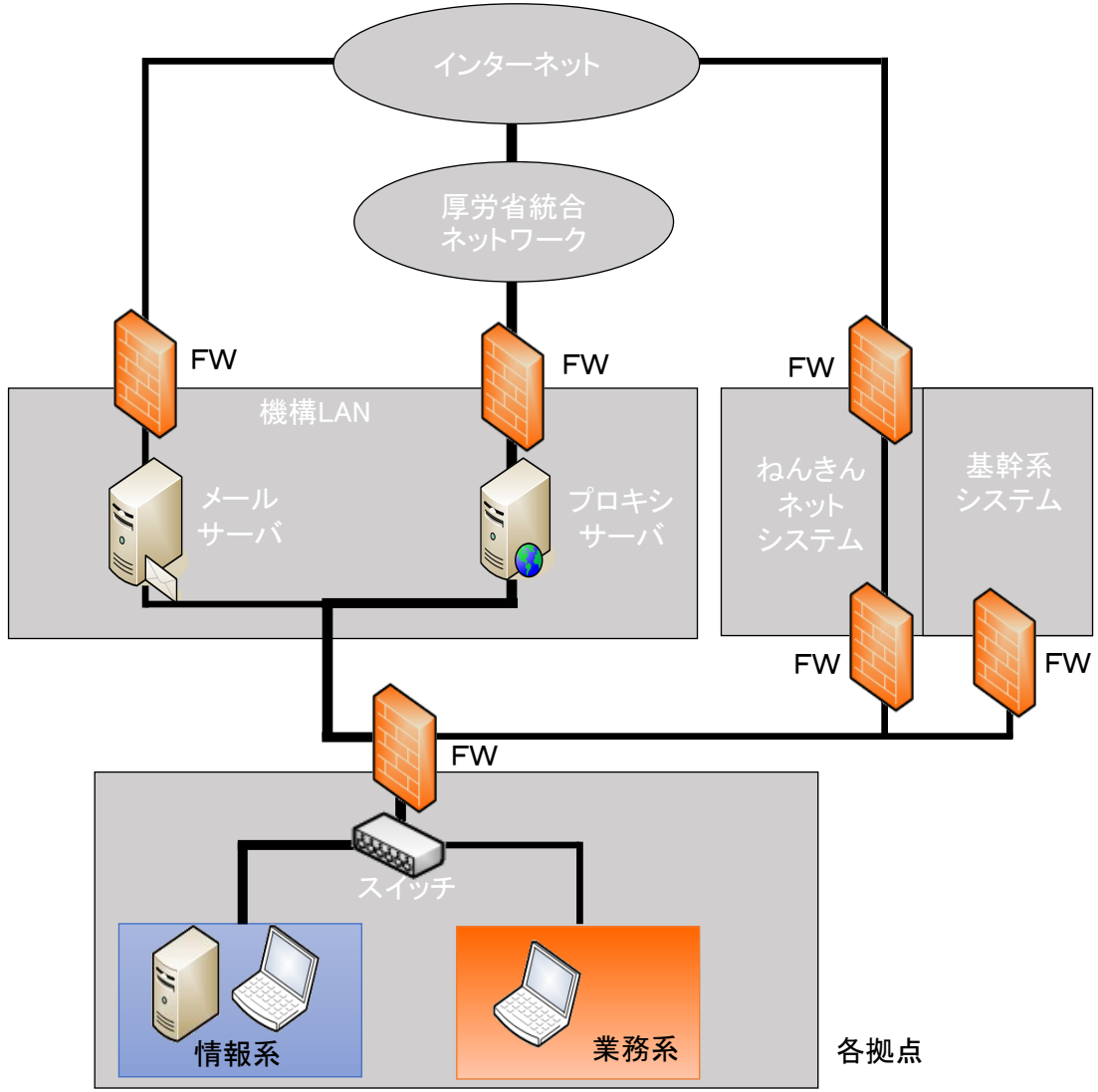


サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の概要（H28.4.22公布）

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）等に委託



年金機構の事例


インターネット
厚労省統合
ネットワーク
FW
FW
FW
機構LAN
メール
サーバ
プロキシ
サーバ
ねんきん
ネット
システム
基幹系
システム
FW
FW
FW
スイッチ
情報系
業務系
各拠点

標的型攻撃の特徴と対策

□ 標的型攻撃の特徴

○ **メール開封を前提**とした対策が必要
○ 初期段階での認知・対処、**侵入範囲を拡大させない**ための**システム設計・構築・運用**が重要

□ 標的型攻撃に対する情報システム防御策等の考え方

［検討対策例］

◆ システム防御策

- メールに添付された**実行形式のファイルを取り込まない・起動できないようにシステム設定**
- 既知の**脆弱性を放置しない**(アップデート、脆弱性診断等)
- **ウェブブラウザの拡張機能の必要最小限の使用**
- 侵入範囲が**拡大しにくいよう**に設定・運用
- 重要な情報に攻撃が到達しないよう、**システム分離**
  (各システムで扱える情報・できない情報につきルール化し、職員に徹底)
- **ローカル管理者権限**のパスワードを共通とする範囲の**最小限化**
- **不要な管理アカウント**の確実な**消去**
- 内部ネットワークにおける**異常を検知**する仕組みの整備

◆ インシデント対策に係る対策

- 不審メールの受信につき攻撃者が繰り返して攻撃を試みるものとして**継続的に対応**
- システム構築・運用事業者とは独立した専門性の高い事業者への依頼等、**平素からの準備**
- CISO等**権限を有する者の下**でのインシデント対応

(出典)サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」(2015年8月)

政府統一基準の改定

事案発生に備えた対処体制（CSIRT）、対処・連絡手順等の整備に係る規定の強化

- ◆ 事案対処に必要な知識・能力を有する**対処体制（CSIRT）の構築等**
- ◆ 発生した事案の対処に係る**意思決定手法や判断基準、対処方法等の事前準備**

不正プログラム感染の発生を前提とする情報システムの防御策の強化

- ◆ **情報システムの重要な情報を扱う部分のインターネットからの分離**
- ◆ **インターネット接続口の集約**
- ◆ **実行プログラム形式ファイルが添付された電子メール受信時のシステム措置**

情報及び情報システムへの不正アクセスの防止等を目的とする対策の見直し・強化

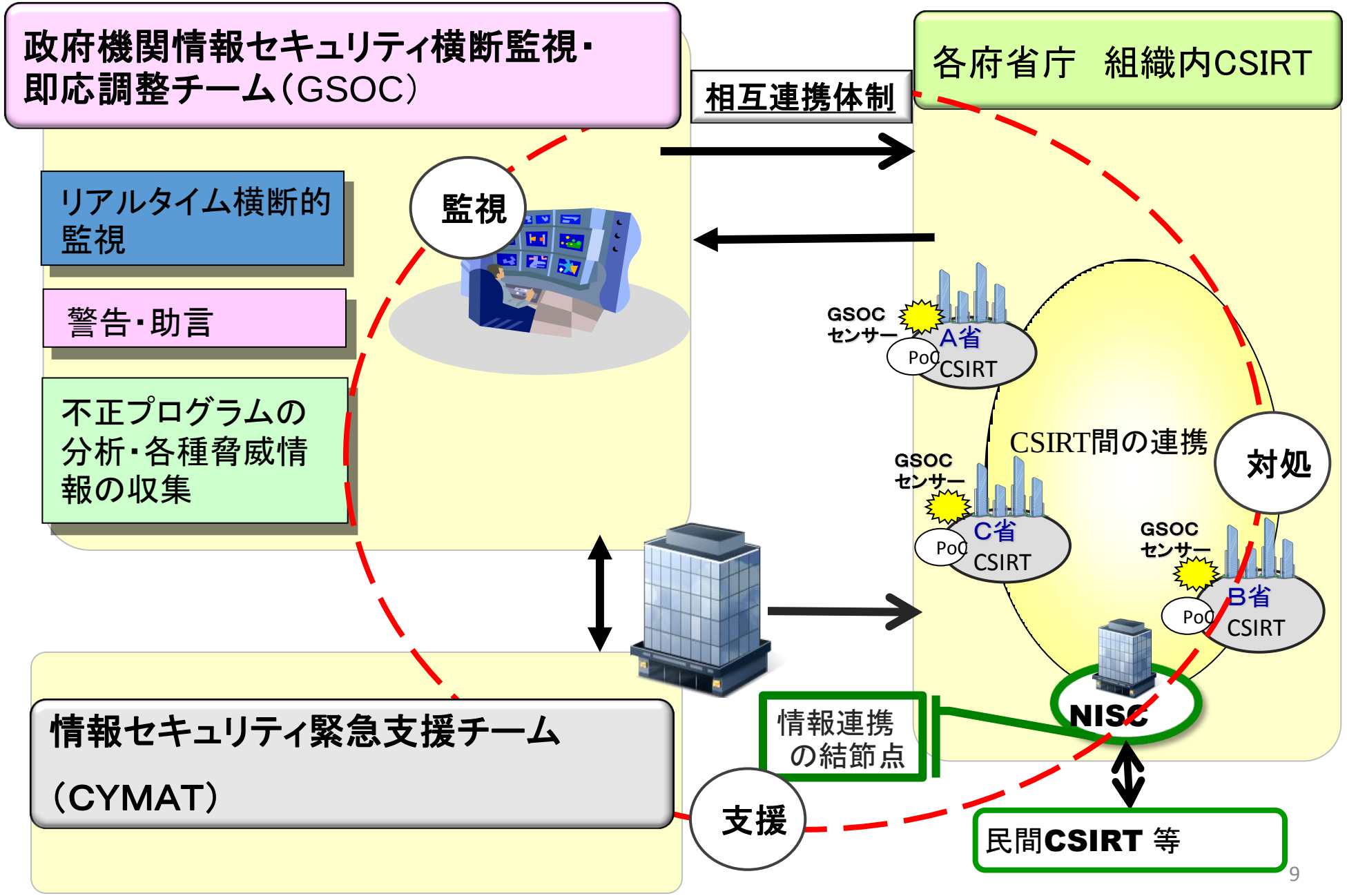
- ◆ 機密性・完全性の高い情報を大規模かつ体系的に管理する**データベースに対する対策**

新たなIT製品・サービスの普及等に伴う対策事項の明確化

- ◆ 外部事業者に委ねる際のリスク評価に基づく**クラウドサービス※利用可否の判断**
- ◆ **委託事業の実施場所（クラウド構成機器の所在地等）、準拠法・裁判管轄の指定**
- ◆ **クラウドサービス及び提供事業者の信頼性の確認**

※ 外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

政府機関における情報集約・支援体制の枠組み



重要インフラ事業者に係る取組み

重要インフラの情報セキュリティ対策に係る第３次行動計画

１．安全基準等の整備及び浸透
対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求

２．情報共有体制の強化
平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化

３．障害対応体制の強化
関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化

４．リスクマネジメント
重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援

５．防護基盤の強化
関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　　等

◆重要インフラ分野**13**分野（電力、通信、金融、航空、鉄道、医療、石油等）
◆「経営層に期待する在り方」
◆**PDCA**サイクル
◆客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施

第3次行動計画の見直しに向けたロードマップ

行動計画見直しに当たっての基本方針

◆「機能保証」の考え方に基づく取組を含める。

◆行動計画の見直しについて、平成29年3月末を目途に結論。早急に対処すべき事項については、行動計画の見直しを待たずに対処。

考慮すべき環境変化

(1)ＩｏＴの浸透に伴う制御技術と情報通信技術の相互依存性の高まり

(2)面的防護に向けた情報共有等の連携体制強化の必要性等

(3)諸外国における重要インフラへの取組の加速化

強化すべき取組の方向性

サイバー攻撃に対する体制強化

- 経営層における取組の強化の推進
- 情報共有の強化
- 内部統制の強化の推進
- マイナンバー制度の運用に係るセキュリティの確保に関する取組
- 東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化

防護範囲の見直し

- 情報共有範囲の拡大
- 分野横断的な情報共有の強化
- 国の安全等の確保の観点からの取組

多様な関係者間の連携強化

- 国際連携
- 人材育成

「サイバーセキュリティ人材育成総合強化方針」

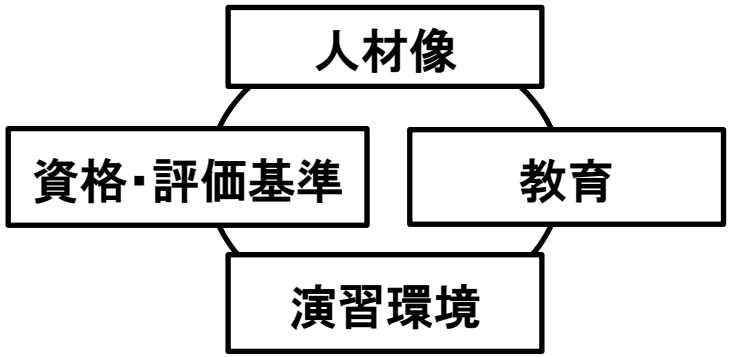
○人材の需要と供給の好循環の形成

【人材の需要(雇用)】
適切な認識の下で雇用・キャリアパスを確保
－経営戦略上の「投資」
－サイバー攻撃への対処の必要性

経営層 ⇔ 橋渡し人材層 ⇔ 実務者層

好循環

【人材の供給(教育)】
人材育成の循環システム
－確かな知識と実践力の下に、様々な業務経験を経て、人材が育成



企業経営のためのサイバーセキュリティの考え方

グローバルな変化

- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合により、チャンスとリスクが一層増大

サイバーセキュリティは、やむを得ない「費用」でなく、積極的な経営における**「投資」の対象**

二つの基本的認識

＜①**挑戦**＞
新たな製品・サービスの価値（**「セキュリティ品質」**）を創造

＜②**責任**＞
全てがつながる社会において、**社会的な要求・要請**

三つの留意事項

①**情報発信**により社会的評価を向上

②提供する機能やサービスを全うする観点からの**リスク対策**

③**サプライチェーン**全体でのサイバーセキュリティの確保

企業タイプ別の取組み手法例

積極的にITで革新する企業
・IoTガイドライン
・ブランドとして情報発信

基盤としてIT活用する企業
・経営ガイドライン
・コンプライアンスと説明

リソース制約ある中小企業等
・安全なクラウド
・アドバイザー

戦略的イノベーション創造プログラム（SIP）

“重要インフラ等におけるサイバーセキュリティの確保”（2015～19年度の5年間を予定）

達成目標

- 悪意のある機能を“持ち込ませない”、悪意のある動作を“いち早く発見する” システムの実現
- 国産セキュリティ技術を確立。重要インフラ産業の競争力強化、安全な社会基盤実現に貢献

⇒ 2020年五輪大会の安心安全な開催

研究開発計画案概要

古い機器、セキュリティが弱い機器は「信頼」できる機器で囲いこんで防御

②システム起動時、運用時にもセキュリティを確認

①「信頼の起点」を機器に作り込み、認証制度設計

③動作監視・解析
「信頼」できる機器での分析により迅速対処

:「信頼の起点 ☆ 」が入るチップ

④重要インフラ間の情報共有プラットフォームとセキュリティ運用のための人材育成

SIP

安全なIoTシステムのセキュリティに関する一般的枠組

① IoTシステムについて、範囲、対象を含めた定義、リスクを踏まえたシステムの特性に基づく分類、その結果を踏まえた適切な対応の明確化

② IoTシステムに係る情報の機密性、完全性及び可用性の確保、モノの動作に係る利用者等に対する安全確保に必要な必須要件を明確化

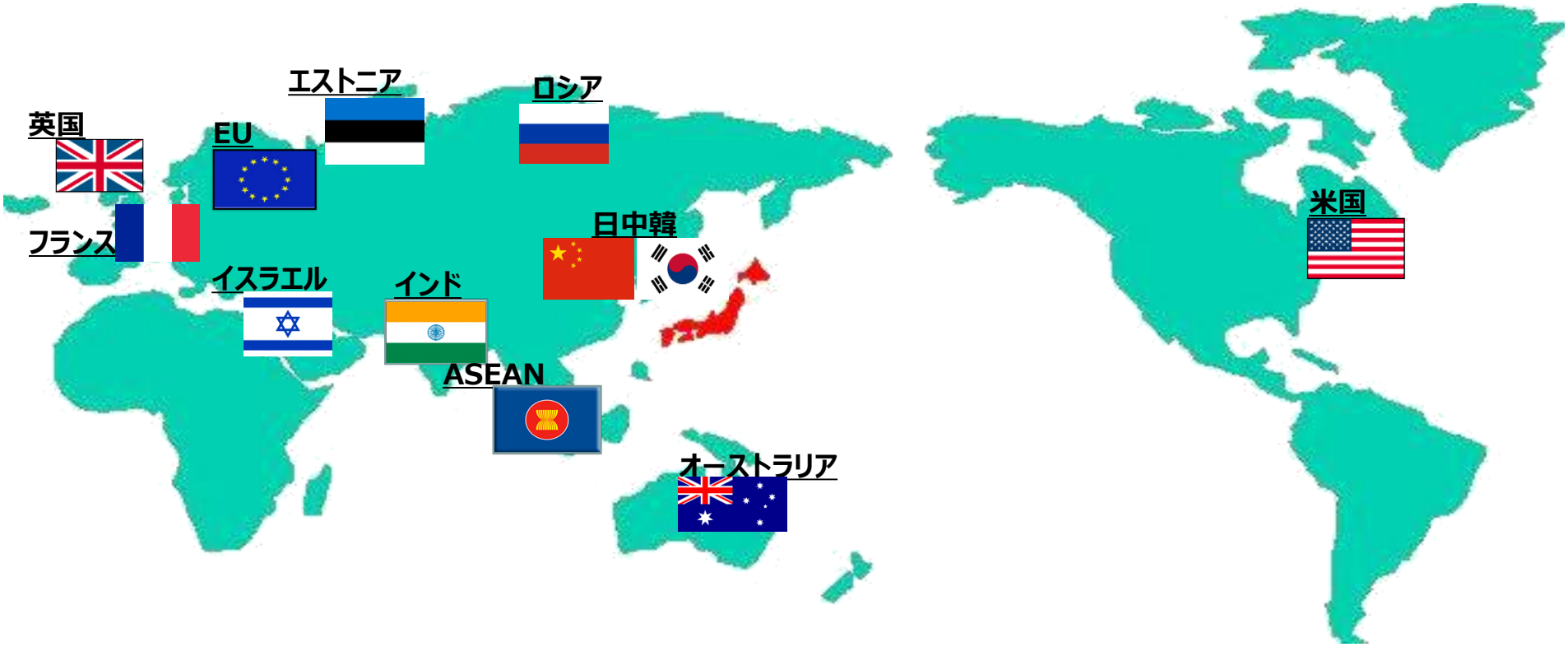
③ 確実な動作の確保、障害発生時の迅速なサービス回復に必要な必須要件を明確化

④ 接続されるモノ及び使用するネットワークに求められる安全確保水準(法令要求、慣習要求)を明確化

⑤ 接続されるモノ及びネットワークの故障、サイバー攻撃等発生時の機密・完全・可用性、安全の確保、迅速なサービス復旧の明確化

⑥ IoTシステムに関する責任分界点、情報の所有権に関する議論を含めたデータの取扱いの在り方の明確化

国際連携に向けた政策対話の推進



多国間・マルチステークホルダーの取組み

サイバー空間の国際規範づくり等に関する会議

MERIDIAN

IWWN

普及啓発（サイバーセキュリティ月間等）

知る・守る・続ける

普及啓発プログラム

- 国民一人一人がどうしたらよいか　⇒　相談、助言等
- 地域での取組促進
- 協議会方式で
- 学ぶ機会のある人、ない人等向けの施策

詳しい資料はこちら

NISCのホームページ ― http://www.nisc.go.jp/index.html

サイバーセキュリティ戦略（H27年9月4日閣議決定）
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf

政府機関の情報セキュリティ対策のための統一基準
（H28年8月31日本部決定）　http://www.nisc.go.jp/active/general/pdf/kijun28.pdf

サイバーセキュリティ政策に係る年次報告（2015年度）（H28年6月13日本部決定）
http://www.nisc.go.jp/active/kihon/pdf/jseval_2015.pdf

日本年金機構における個人情報流出事案に関する原因究明調査結果（H27年8月20日本部決定）
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

政府統一基準関連、重要インフラの第3次行動計画、人材育成プログラム、研究開発戦略等についてはサイバーセキュリティ戦略本部等のページ　http://www.nisc.go.jp/conference/index.html