NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティに関する動向と政策

内閣官房　内閣サイバーセキュリティセンター(NISC)
三角育生

平成２８年１月

目次

- サイバー攻撃の現状
- サイバーセキュリティの推進体制（基本法とNISC）
- サイバーセキュリティ戦略
- 重要インフラに関する施策（第３次行動計画）
- 政府機関、国民への対応
- サイバーセキュリティの将来について考える

- **サイバー攻撃の現状**

何のために
何を守るのか

個人情報

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）
- 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）　・・・・・・

サイバー脅威の深刻化

IT依存度の高まり

ＰＣ

多くの職場・家庭に普及し、インターネットに接続
（2014年末：PC普及率 78.0%、インターネット普及率 82.8%）
※2015年版情報通信白書（総務省）

スマートフォン

世帯保有率が６.6倍に急増
（2010年末：9.7%→2014年末：64.2%）
※2015年版情報通信白書（総務省）

自動車

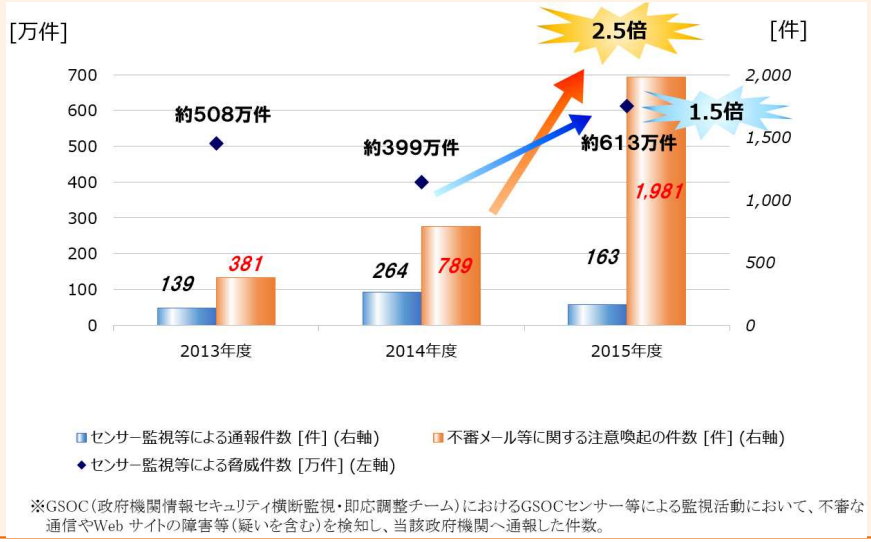
一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの取組みガイド（2013.8 IPA）

スマートメーター（次世代電力量計）

電力会社による開発・導入の開始
［主な予定］・東京：2020年度までに2700万台の導入完了
・関西：2022年度までに1300万台の導入完了

サイバー攻撃の増加

【政府機関への脅威件数等】



※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。

国家関与の疑われる攻撃

韓国（2013年4月）

重要ｲﾝﾌﾗ（金融・放送等）に対する大規模サイバー攻撃が発生。韓国当局は北朝鮮の所業と発表。

米国（2014年12月）

ｿﾆｰ・ﾋﾟｸﾁｬｰｽﾞ・ｴﾝﾀｰﾃｲﾝﾒﾝﾄ社に対するサイバー攻撃が発生。 米国政府は北朝鮮に責任ありとし、国家安全保障上の問題として対応。

2020年東京オリンピック・パラリンピック競技大会へ向けた準備

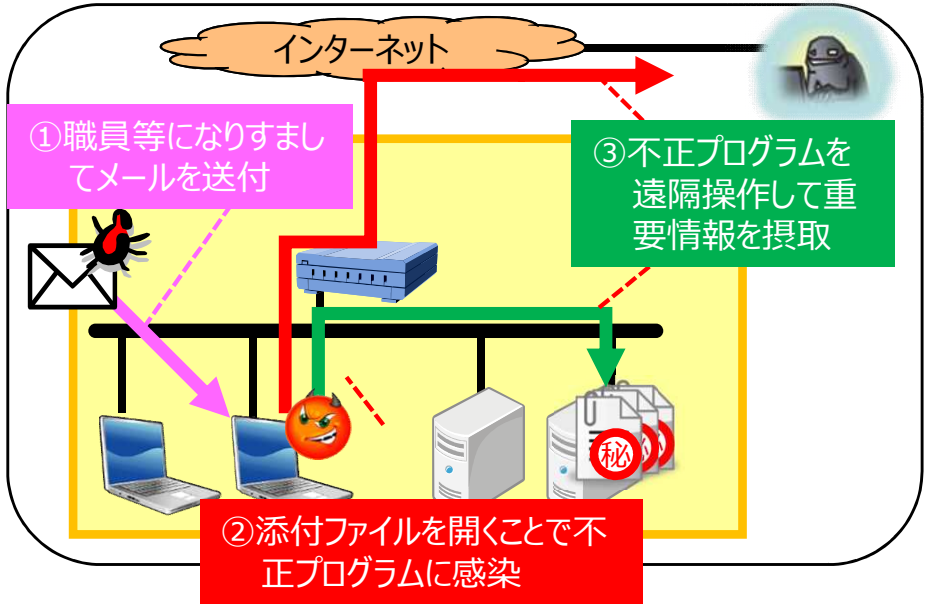
- 世界の注目を集める祭典。「ダウンタイム」は許されない。
- 2012年のロンドン大会では、開催期間中、約２億件のサイバー攻撃が発生。
- 英国政府は、6年前からサイバー攻撃対策を準備。

最近の脅威　①標的型メール攻撃

脅威の概要

- 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

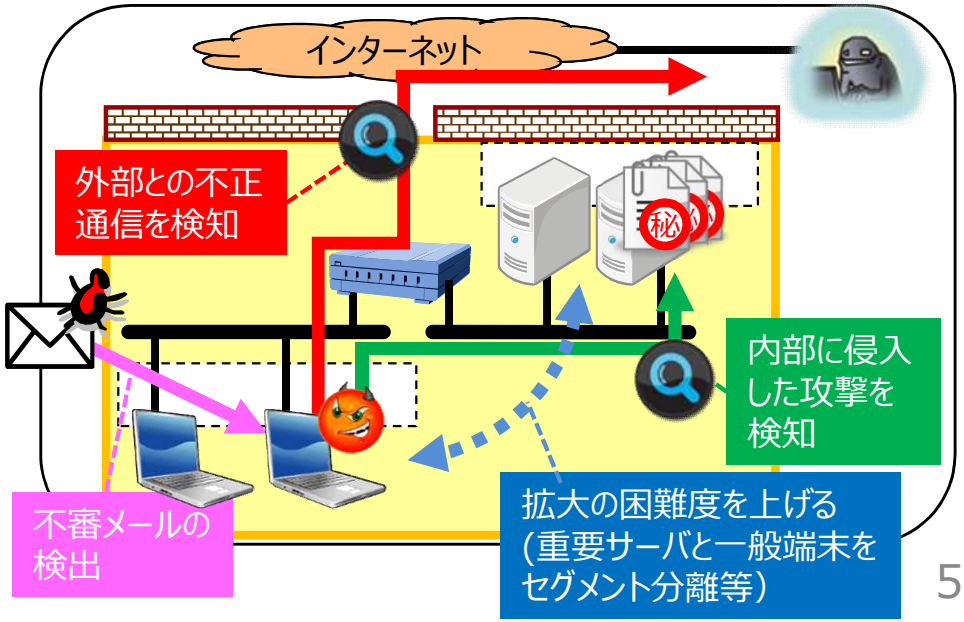
標的型メール攻撃のイメージ



主な対策

- 不審なメールを検出する仕組みの整備、対応能力を向上する（SPFの検証、教育・訓練、等）。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

対策の概要(例)



標的型攻撃メールの例

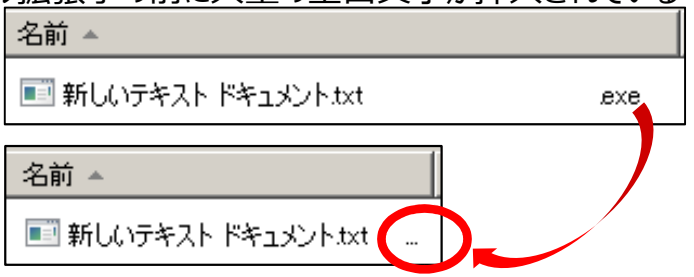
メールのテーマ

- 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容
  - ✓ 新聞社や出版社からの取材申込や講演依頼
  - ✓ 就職活動に関する問い合わせや履歴書送付
  - ✓ 製品やサービスに関する問い合わせ、クレーム
  - ✓ アンケート調査
- 心当たりのないメールだが、興味をそそられる内容
  - ✓ 議事録、演説原稿などの内部文書送付
  - ✓ VIP 訪問に関する情報
- これまで届いたことがない公的機関からのお知らせ
  - ✓ 情報セキュリティに関する注意喚起
  - ✓ インフルエンザ等の感染症流行情報
  - ✓ 災害情報
- 組織全体への案内
  - ✓ 人事情報
  - ✓ 新年度の事業方針
  - ✓ 資料の再送、差替え
- 心当たりのない、決裁や配送通知 (英文の場合が多い)
  - ✓ 航空券の予約確認
  - ✓ 荷物の配達通知
- IDやパスワードなどの入力を要求するメール
  - ✓ メールボックスの容量オーバーの警告
  - ✓ 銀行からの登録情報確認

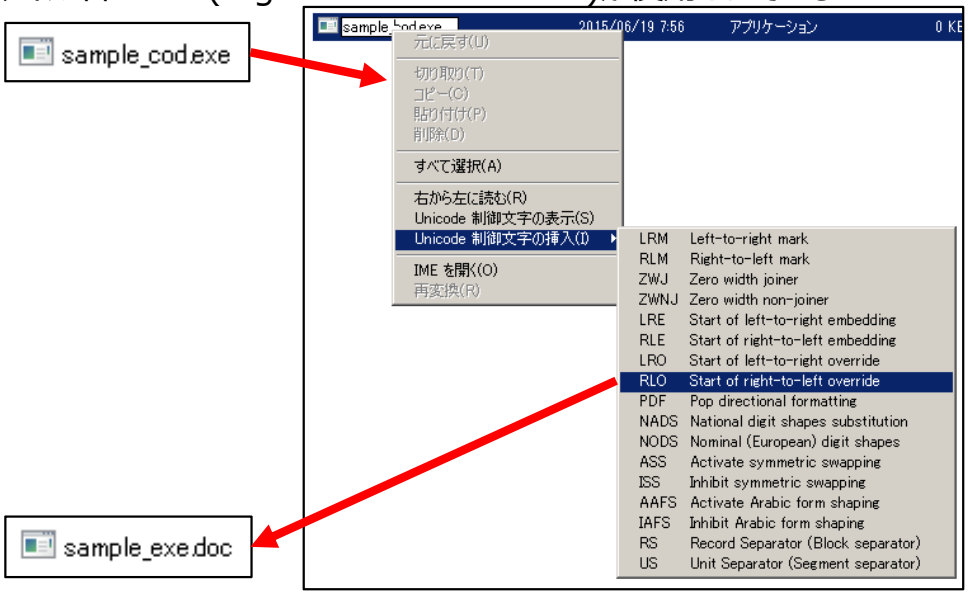
出典：IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」より

添付ファイルなど

- アイコンが偽装されている
  - ✓ 実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
- ファイル拡張子が偽装されている
  - ✓ 二重拡張子となっている
  - ✓ ファイル拡張子の前に大量の空白文字が挿入されている



  - ✓ ファイル名にRLO(Right to Left Override)が使用されている



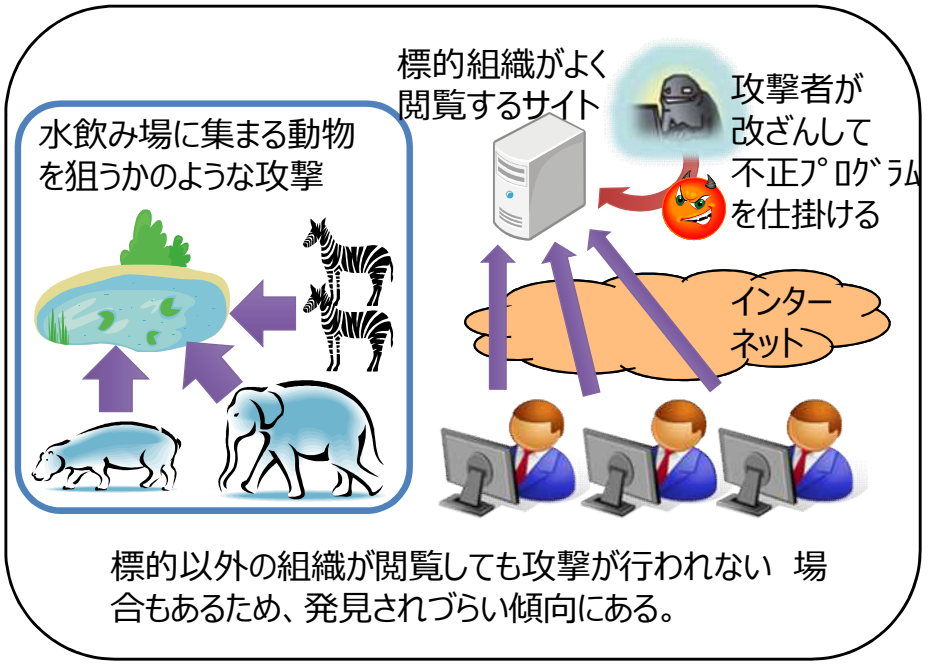
- 表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる（HTMLメールの場合）

最近の脅威　②水飲み場型攻撃

脅威の概要

- 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ブラウザの未知の脆弱性を悪用した攻撃（ゼロデイ攻撃）の場合もあり、未然防止は困難。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

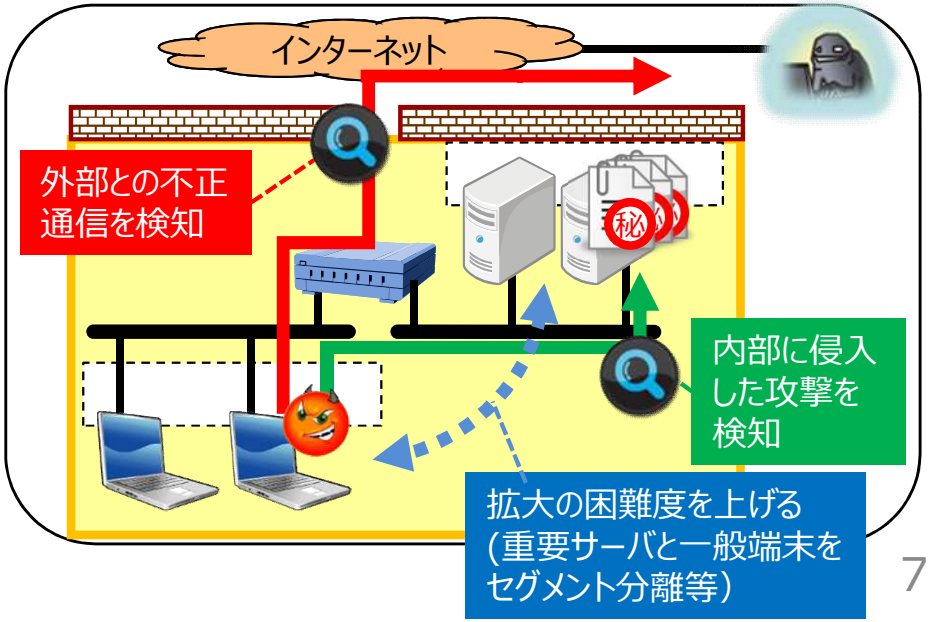
水飲み場型攻撃（イメージ）



主な対策

- 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
- 内部対策としては、以下が挙げられる。
  - 内部に侵入した攻撃を早期検知して対処
  - 侵入範囲の拡大の困難度を上げる
  - 外部との不正通信を検知して対処

対策の概要(例)

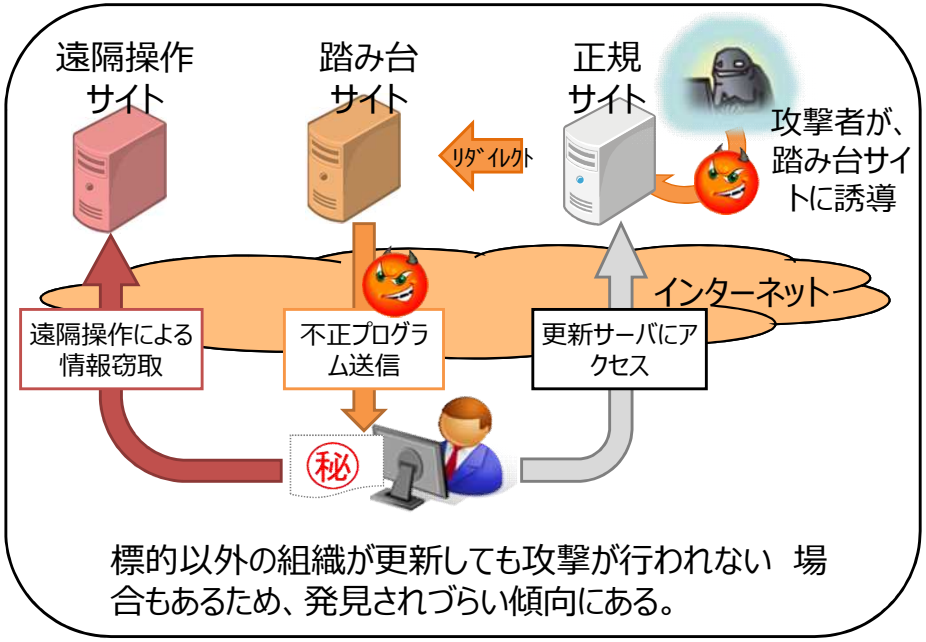


最近の脅威　③ソフトウェアの更新プログラムを悪用した攻撃

脅威の概要

- 広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行った端末を不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

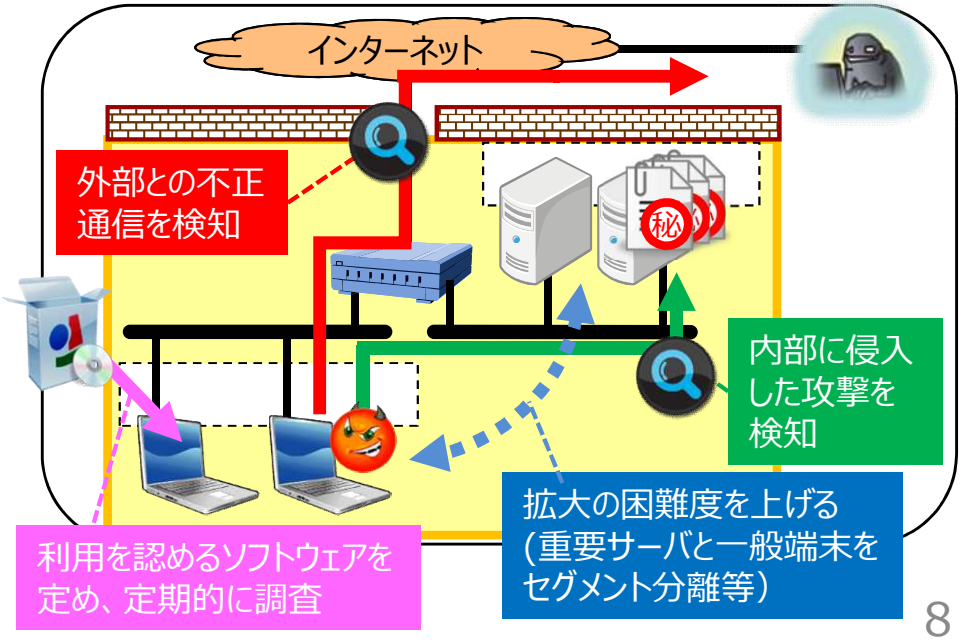
ソフトウェアの更新プログラムを悪用した攻撃（イメージ）



必要な対策

- 端末で利用を認めるソフトウェアを定め、利用されているソフトウェアの状態を定期的に調査する。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

対策の概要(例)



標的型メール攻撃の攻撃プロセス

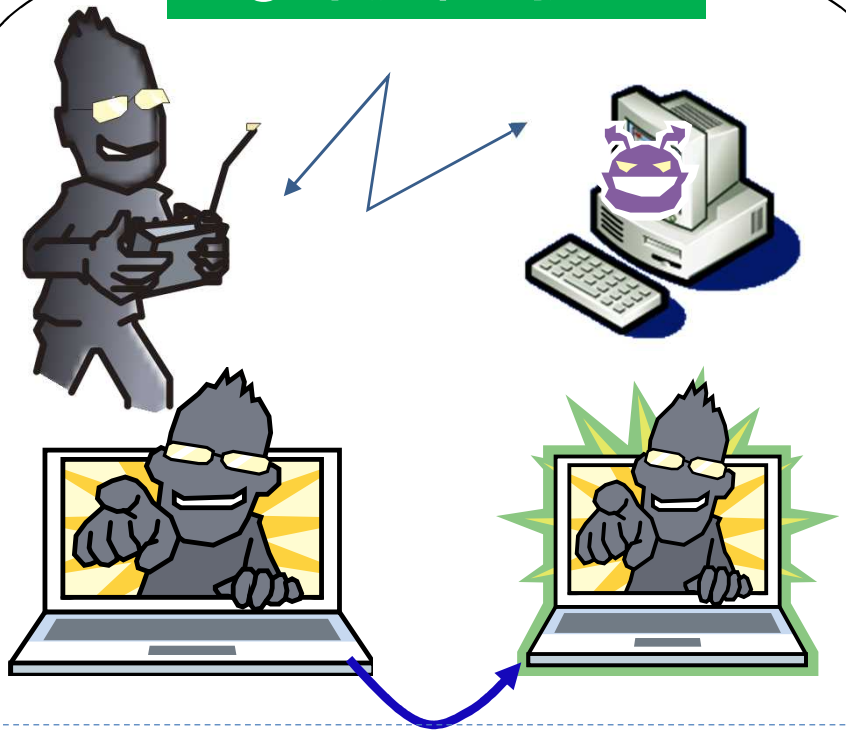
時間をかけて執拗に狙う！

① 初期潜入

ウィルス
対策ソフトが
検知しない！

最初はメールの
添付ファイルや
リンクを開くだけ

② 侵入範囲拡大



遠隔操作により、
システムの内部に侵入し、
乗っ取りを拡大

③ 目的達成

重要情報の窃取や
システム破壊も

標的型攻撃でのマルウェアがなぜ防ぎにくいのか

非対称性

- 防御側は全てをどんな時でも完全に防ぐ必要　←→　攻撃者はいつかどこかで穴を見つければよい

アンチウィルスソフトで検知できない

- マルウェア作成や難読化を容易にするソフトウェア　→　亜種増大によるパターンマッチの限界（全部は無理）
- 攻撃者は遠隔操作で最新版にアップデート可能　→　複数を常に侵入させ１つでも残っていれば勝利
- 攻撃者は既存のアンチウイルスソフトで検知できないことを確認してから使用

ゼロデイ脆弱性が狙われる

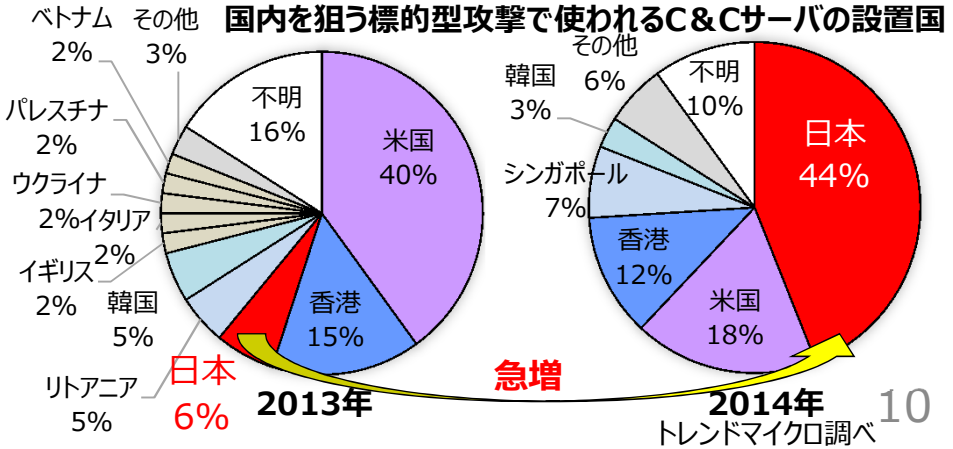
- 闇市場でゼロデイ脆弱性が取引　→　バグ発見はよいお金に（バグ発見報酬制度の進展が必要。。。）
- 攻撃側の体制変化；単独愉快犯から組織的・経済的行動　→　高い技術力と資金力
- パッチ公開後も短時間(数時間～数日)でマルウェア作成　→　企業のパッチ当ては、検証に数日～数週間

カスタマイズされた攻撃

- 対象を研究してから攻撃　→　メールのやりとりを把握して返信メールにマルウェアを仕込む等
- 特定業界しか見ないようなWebサイトが改ざんされ、特定IPだけにマルウェア埋め込み　→　発見されにくい

正常に見せかけた通信や挙動による検知逃れ

- 通常通信に紛れて遠隔操作 → http(80番)やSSL(443番)
- 攻撃指令(C&C)サーバは国内が主流 → .jpも安心できない
- OS標準コマンドを使用して感染拡大
- 解析環境（サンドボックス等）では反応しないよう細工
- メモリのみに存在するプログラム、自身が残したログの消去



日本年金機構における個人情報流出事案：事案概要

- 平成27年5月8日から20日にかけて4種類の不審メールが日本年金機構へ送付され、23日までに**31台の端末がマルウェアに感染**し、23件の不審な通信先への通信が発生
- 6月1日、機構は、外部から送付された不審メールに起因する不正アクセスにより、機構が保有している**個人情報の一部（約125万件）が外部に流出**したことが5月28日に判明したとして、報道発表
- 23件中1件の通信先への通信が約125万件の個人情報の流出に関する通信であったことが警察庁からNISCへの情報提供により判明

- サイバーセキュリティ戦略本部が、サイバーセキュリティ基本法第25条第1項第3号に規定された「国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）」に基づき原因究明調査を実施
- 6月1日、NISCに原因究明調査チームを設置
- 8月20日にNISCにて原因究明調査結果を公表
  http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

日本年金機構における個人情報流出事案：事案の状況と本部及びNISCの対応

- **5月8日(金)(検知・通知1)**
  - NISCは、厚生労働省(以下「厚労省」という。) ネットワークにおいて不審な通信を検知し、厚労省政策統括官付情報政策担当参事官室 (以下「情参室」という。) に対してその旨を通知した。
  - NISCは、厚労省情参室から不審な通信をした端末を特定し、LANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。(以降、厚労省情参室に対し、随時、助言等を実施。)
- **5月15日(金)(解析結果提供A)**
  - NISCは、厚労省情参室から5月8日に受信した不審メールⅠに関する不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。
- **5月19日(火)(解析結果提供B)**
  - NISCは、厚労省情参室から5月18日に受信した２種類の不審メール（不審メールⅡ、不審メールⅢ）及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。
- **5月21日(木)(解析結果提供C)**
  - NISCは、厚労省情参室から5月20日に受信した不審メールⅣ及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。
- **5月22日(金)(検知・通知2)**
  - NISCは、厚労省ネットワークにおいて不審な通信を検知し、厚労省情参室に対してその旨通知した。
  - NISCは、厚労省情参室から、機構において、不審な通信をした端末のLANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。
- **5月29日(金)**
  - NISCは、厚労省から、5月8日以降の経緯について5月19日に機構が警察へ相談したこと及び機構において情報流出が生じた旨の説明を受け、サイバーセキュリティ戦略本部長(官房長官)(以下「本部長」という。) に報告した。
  - 本部長は、NISCから報告を受け、即時に「特定重大事象」[注1]であるとの判断を行った。
  - NISCは、厚労省の要請を受けて、厚労省と機構が行う対応を支援するため、CYMAT[注2] を派遣した。
- **6月1日(月)**
  - NISCは、客観的・専門的立場から原因究明を実施するため、原因究明調査チームを設置した。
  - 本部長は、サイバーセキュリティ基本法第30条第2項の規定に基づき、機構を監督する立場にある厚生労働大臣に対して、厚労省が機構に対して行ってきたサイバーセキュリティに関する監督に関する資料、情報の提供を要請した 。
  - 内閣官房副長官(事務)を議長とするサイバーセキュリティ対策推進会議を開催し、全府省庁に対して、システム点検と個人情報の適正管理を指示した。

注1：「 サイバーセキュリティ戦略本部重大事象施策評価規則 」(平成27年2月サイバーセキュリティ戦略本部決定)において、①国の行政機関が運用する情報システムにおける障害を伴う事象であって、行政事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの、② 情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの等の事象をいう。
注2：情報セキュリティ緊急支援チーム(通称CYMAT：CYber Incident Mobile Assistance Team)

日本年金機構における個人情報流出事案：事案に関する技術的検討①

□ 原因究明調査により判明した事項①(ネットワーク構成の確認等)

◆ 機構のネットワークは、情報系からプロキシサーバを経由しての外部通信以外の外部通信が遮断される設定。
したがって、攻撃者による外部との不審な通信については、プロキシサーバにその履歴が残る（プロキシログの解析結果は次頁参照）。

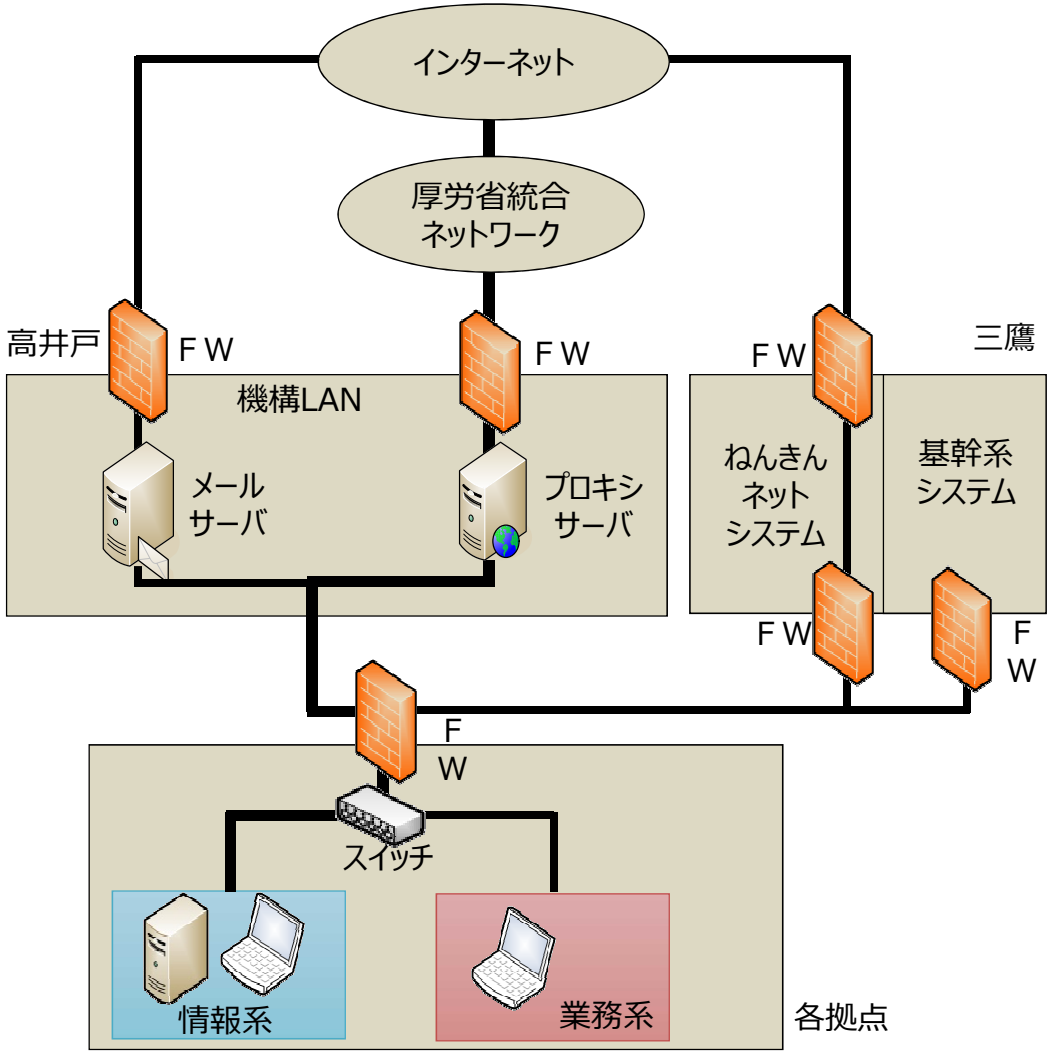
・業務系端末からの外部通信について

業務系端末から厚労省統合ネットワーク経由の外部通信は、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、ＮＩＳＣ職員が説明どおりの設定となっていることを直接確認。

プロキシサーバに、業務系端末からの外部通信に関する履歴なし。

・メール用回線等を通じた外部通信について

メール用回線及びねんきんネットシステム経由のWebアクセスは、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、ＮＩＳＣ職員が説明どおりの設定となっていることを直接確認。



日本年金機構における個人情報流出事案：事案に関する技術的検討②

□ 原因究明調査により判明した事項②(プロキシログの解析、不審メールとの突合等)

◆ プロキシログの解析により、不審な通信先２３件、不審な通信を行った端末３１台を特定、不審メールと突合。

不審メールの番号	受信日	不審メールの概要	発生した不審な通信
Ⅰ	5月8日(金)	件名：「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先：公開メールアドレス(2) リンク：商用オンラインストレージ	端末１台が不正プログラムに感染、不審な通信が発生。約４時間後に端末の通信ケーブルを抜線、その後は不審な通信なし。
Ⅱ	5月18日(月)	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス(98) 添付ファイル：給付研究委員会オープンセミナーのご案内.lzh	端末３台が不正プログラムに感染、不審な通信が発生するも接続先への通信は失敗。
Ⅲ	5月18日(月) ～ 5月19日(火)	件名：厚生年金徴収関係研修資料 宛先：非公開の個人メールアドレス(20) 添付ファイル：厚生年金徴収関係研修資料（150331厚生年金徴収支援G）.lzh (16) リンク：商用オンラインストレージ(4)	不審な通信は発生せず。
Ⅳ	5月20日(水)	件名：【医療費通知】 宛先：公開メールアドレス(3) 添付ファイル：医療費通知のお知らせ.lzh	20日午後、端末１台が不正プログラムに感染、不審な通信が発生。数時間以内に、他の6台の端末からも不審な通信が発生。 21日から23日にかけて、合計21台の端末から国内のサーバ(接続先Ｘ)への多数の通信。

◆ NISCでは、不審メールⅡ及び不審メールⅢに関する解析結果を5月19日夜に、不審メールⅣに関する解析結果を5月21日夕刻に、それぞれ厚労省情参室に提供しているが、これらの解析結果には不正プログラムの接続先に関する情報が含まれていた。

◆ 5月22日にNISCにおいて不審な通信を検知し厚労省に通知した後、機構による調査の過程で接続先Ｘへの多数の通信が判明した。

日本年金機構における個人情報流出事案：ＣＳＩＲＴの運用等に関する検討

	ＮＩＳＣ	厚労省	年金機構
インシデント対処	● 政府統一基準(注1)では、インシデントを認知したときに、CISO(注2) やNISCに報告することを定めている。 ● 統一基準では、インシデント発生時に、CISOやNISC等への連絡のため、各府省庁において報告窓口を含む報告・対処手順を整備することとしている。	● 厚労省の情報セキュリティポリシーでは、インシデントを認知したときに、CISOやNISCに報告する旨定めている。 ● 厚労省は、報告・対処手順を整備しているが、今回のインシデントにおいて、GSOC (注3) から連絡を受けた担当窓口から、厚労省の責任者（CISO、課長等の幹部）に報告が上がっていなかった。	● 機構のセキュリティポリシーにおいて、インシデント対処の必要性を規定し、その具体化はリスク管理一般の規程等に委ねている。 ● 当該規程において、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、サイバー攻撃を想定した具体的な対応が明確化されていない。
CSIRT (注4) 体制	● 政府統一基準では、CSIRTに属する職員については、「専門的な知識又は適性を有すると認められる者を選任すること」と定めている。 ● CSIRTに属する職員の選任は、各府省庁が統一基準の規定に従うこととされている。	● 厚労省のポリシーでは、CSIRTに属する職員について、「CISO、情報政策担当参事官、当該事案に係る部局の総括的な課長及び担当課室長等、CISOアドバイザを充てる」と定めている。 ● CSIRTの構成員が課室長等以上であり、実働要員（課長補佐以下の職員）が選任・指名されていなかった。	● 特殊法人である機構は、政府統一基準の直接の適用対象ではない。 ● CSIRT体制は定めておらず、セキュリティポリシーや諸規程にもその定めはない。（機構によると、平成27年7月10日からCSIRT体制の構築の検討を開始。）
個人情報を取り扱うシステムの整備等	● 「ガイドライン」(注5) において、標的型攻撃に対する多重防御の取組は、外交・安全保障等に加え「個人にもたらされる被害」も対象としている。	● 厚労省統合ネットワークにおける標的型攻撃に対する多重防御の取組を進めていたが、機構の情報系ネットワークは、「ガイドライン」の取組の対象としておらず、標的型攻撃に対する多重防御の取組が十分でなかった。	● インターネットに接続していない業務系からインターネットに接続をしている情報系に個人情報を移して取り扱っていた。

(注1)「政府機関の情報セキュリティ対策のための統一基準」(平成26年5月　情報セキュリティ政策会議決定)
(注2) Chief Information Security Officer :最高情報セキュリティ責任者
(注3) 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
(注4) Computer Security Incident Response Team:コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織
(注5)「高度サイバー攻撃対処のためのリスク評価等のガイドライン」　（平成26年6月25日　情報セキュリティ対策推進会議）

日本年金機構における個人情報流出事案：今回のサイバー攻撃の特徴と対策

◘ 標的型攻撃の特徴

- 標的型攻撃は巧妙化しており、使われるメールも見分けが困難。
  →メール開封を前提とした対策が必要。
- 攻撃者は乗っ取った端末を足掛かりとして、侵入を拡大させる。
  →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

自組織の情報・システム・業務を守る目的・対策について考え、職務・職責に応じて実施することが求められる。

［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ようにアップデート等を行う。脆弱性診断を実施。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。
- 業務・情報の性質等に応じて重要な情報に攻撃が到達しないよう、システム分離。
- システム分離したときに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。　　等

◆ インシデント対策に係る対策

- 不審メールの受信（不正プログラム動作の可能性）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。

日本年金機構における個人情報流出事案：本部・NISCがとるべき再発防止対策

□各府省庁への情報提供が有効に機能するための対策

- ◆ NISCは、不審な通信検知後、速やかに分析を行い、インシデントの疑いのあるものは当該省庁に対して通知等を行っているが、通知や提供する不正プログラムの解析結果の重要性を当該省庁が理解し、迅速に適切な措置が取られることを前提としている。
- ◆ 今回の事案の教訓を踏まえれば、今後は、平素から各府省庁に対して、標的型攻撃を含むサイバー攻撃の本質と影響、NISCからの検知通知や不審メール等の解析結果の活用方法、対処方法等について研修や演習の機会を提供していく必要がある。
- ◆ 研修や演習の対象は、情報システム部局のみならず、独立行政法人、特殊法人等を所管する部局の幹部も対象として含めねばならない。本部は、その実施状況を年次報告等において評価し国民に説明していくことが重要である。

□インシデントに備えた体制の強化

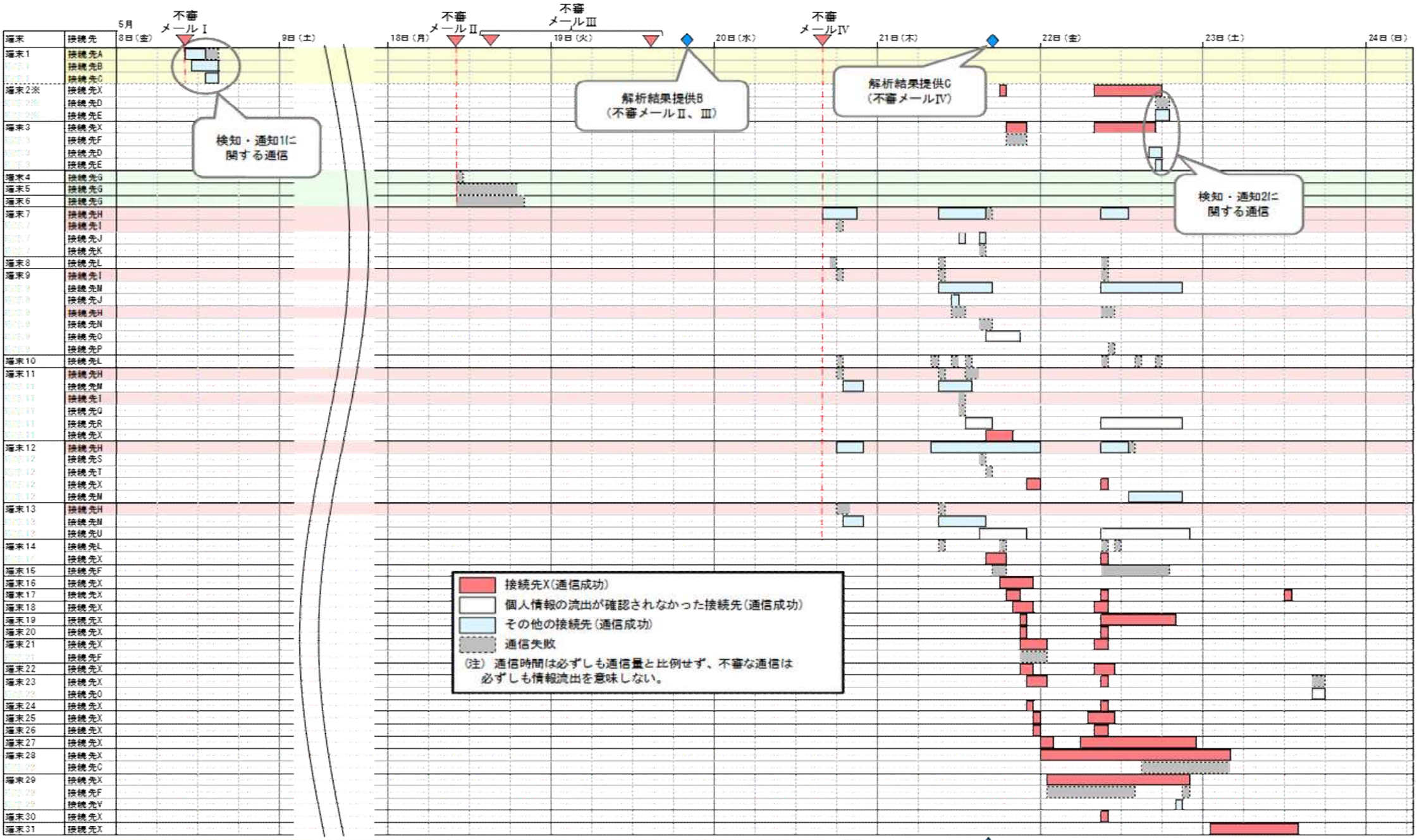
- ◆ 各府省庁においては、政府統一基準等に従って、CISOの指示の下、専門的な知識又は適正を有すると認められる者を選任したCSIRTを整備し、平素から要員の事案対処能力、経験の向上を図り、実践できるようにしておくことが求められている。
- ◆ NISCは、各府省庁のCSIRTが、事案発生時に実働する体制が整備・強化されるよう、事案の対応についての演習・訓練等の機会を設け、また、本部は、各府省庁において適切に体制整備がされ、実践のための必要な取組がなされているか等についても監査の対象とするなど、PDCAサイクルに基づく着実な取組を確保していく。
- ◆ 本部及びNISCは、政府統一基準等の見直しを行い、サイバーセキュリティ対策の向上を図る。

□標的型攻撃のリスクを踏まえたシステムの構築、維持、運用の強化対策

- ◆ 本部及びNISCは、標的型攻撃への対処について、政府統一基準の他、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を取りまとめ、その実施を推進してきたが、その適用範囲は、国の行政機関としている。
- ◆ 今後は、大量の個人情報を取り扱うリスクの高いシステムにおいても、サイバー攻撃のリスクを踏まえたシステムの構築、維持、運用がなされるよう、各府省庁に対し多重防御の取組を加速化すべく次のような取組を促すよう対策を講じていく。
  - リスクを考慮したシステム構築を行うための基準の改善（適用範囲の拡大を含む。）
  - システムの維持運用を確実にする監査の強化
  - 特に技術的な事項について、外部から起用するCIO補佐官、CISOアドバイザーの積極的な活用
- ◆ 併せて、GSOC機能について、攻撃の手法が時々刻々巧妙化していることを踏まえ、不断の見直しを行っていく必要がある。

本文書は、NISCの対処能力を推知しうる情報が含まれるが、発生した事案の重大性に鑑み、可能な限り実態解明のための情報開示を行い、説明責任を果たす観点から取りまとめたものである。

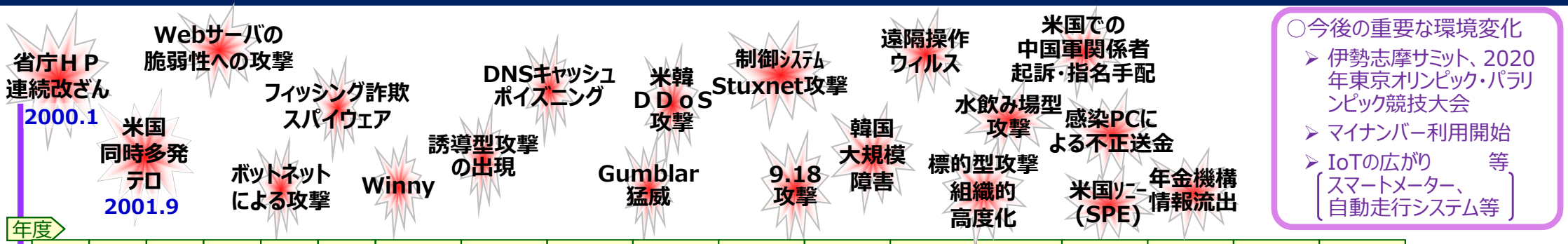
年金機構事案：感染端末と不審な通信



(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)

- **サイバーセキュリティの推進体制（基本法とNISC）**
  - **事案の発生と政策・推進体制の変遷**
  - **基本法の制定による体制整備**

サイバーセキュリティ政策の経緯



年度

2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017

試行錯誤 → DoS攻撃、コンピュータウイルス対策 → リスクゼロ社会 → 「事故前提社会」でのリスクベース対策 → 国家安全保障・危機管理としてのサイバーセキュリティ　高度なサイバー脅威に対し、積極的な対処が求められる時代に

e-Japan 戦略 (2001.1.22) → e-Japan 戦略Ⅱ (2003.7.2) → IT新改革戦略 (2006.1.19 IT戦略本部決定) → i-Japan 戦略2015 (2009.7.6) → 新たな情報通信技術戦略 (2010.5.11 IT戦略本部決定) → 世界最先端ＩＴ国家創造宣言 (2013.6.14 閣議決定, 2014.6.24 改定, 2015.6.30 改定)

参考：IT利活用

情報セキュリティ局長等会議
(1999.9設置)
ハッカー対策等の基盤整備に係る行動計画
(2000.1策定　HP改ざんの直前)

基本戦略

- 第１次 情報セキュリティ基本計画 (2006.2.2 政策会議決定)
- 第２次 情報セキュリティ基本計画 (2009.2.3 政策会議決定)
- 国民を守る情報セキュリティ戦略 (2010.5.11 政策会議決定)
- サイバーセキュリティ基本法公布 (2014.11.12)
- サイバーセキュリティ戦略 (2013.6.10 政策会議決定)
- サイバーセキュリティ戦略 (2015.9.4 閣議決定)

年次計画

SJ2006 → SJ2007 → SJ2008 → SJ2009 → JS2010 → JS2011 → JS2012 → CS2013 → CS2014 → CS2015

SJ：セキュアジャパン　JS：情報セキュリティ　CS：サイバーセキュリティ

政府機関対策

- 情報セキュリティポリシーに関するガイドライン (2000.7 情報セキュリティ対策推進会議決定)
- 政府機関の情報セキュリティ対策のための統一基準
  - 第1版 (2005.12.13 政策会議決定) 第2版 (2007.6.14 政策会議決定) 第3版 (2008.2.4 政策会議決定)
  - 第4版 (2009.2.3 政策会議決定) 平成23年度版 (2011.5.11 政策会議決定) 平成24年度版 (2012.4.21 政策会議決定)
  - 平成26年度版 (2014.5.19 政策会議決定)

重要インフラ対策

- 重要インフラのサイバーテロ対策に係る特別行動計画 (2000.12 情報セキュリティ対策推進会議決定)
- 重要インフラの情報セキュリティ対策に係る行動計画 (2005.12.13 政策会議決定)
- 重要インフラの情報セキュリティ対策に係る第2次行動計画 (2009.2.3 政策会議決定)
- 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 (2014.5.19 政策会議決定, 2015.5.25 戦略本部改訂)

組織体制

- 内閣官房 情報セキュリティ対策推進室 (2000.2設置)
- 内閣官房情報セキュリティセンター (2005.4 設置)
- 情報セキュリティ政策会議 (2005.5 設置)
- GSOC (2008.4 運用開始)
- CYMAT (2012.6 設置)
- 内閣官房内閣サイバーセキュリティセンター (2015.1設置)
- サイバーセキュリティ戦略本部 (2015.1設置)

サイバーセキュリティ基本法の概要

平成26年11月12日　公布（法律第104号）
平成27年１月９日　全面施行

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）**

■**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36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

罰則

■**罰則（第３７条）**
⇒ 30条2項（事務の委託関連の守秘義務）違反

附則

■**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基本法～目的（法第１条）

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、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し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

背景

- インターネット等の整備
- ITの活用の進展

⇒ 世界規模でのサイバーセキュリティに対する脅威の深刻化等内外の諸情勢の変化

喫緊の課題：情報の自由な流通の確保　＆　サイバーセキュリティの確保

対応：サイバーセキュリティに関する施策を総合的に推進

- 基本理念を定め
- 国・地方公共団体の責務等を明らかにし
- サイバーセキュリティ戦略の策定等施策の基本となる事項を定め
- サイバーセキュリティ戦略本部を設置

＆ 高度情報通信ネットワーク社会形成基本法（IT基本法）

目的

- 経済社会の活力の向上と持続的発展
- 国民が安心して暮らせる社会の実現
- 国際社会の平和・安定の確保、我が国の安全保障に寄与

サイバーセキュリティ基本法～定義（法第２条）

第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

「サイバーセキュリティ」

電磁的方式により｛記録され／発信され／伝送され／受信され｝る情報の｛漏えい／滅失／毀損｝の防止

例：その他の当該情報の安全管理のために必要な措置

&

｛情報システム／情報通信ネットワーク｝の｛安全性／信頼性｝の確保のために必要な措置

含む：｛情報通信ネットワーク／電磁的記録媒体｝を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置

が講じられ、
その状態が適切に
維持管理されていること

※電磁的方式…電子的方式、磁気的方式その他人の知覚によっては認識することができない方式

サイバーセキュリティ基本法～国の責務

国の責務

（**国の責務**）

第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する**総合的な施策を策定**し、及び**実施**する**責務を有する**。

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）

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法　（平成十一年法律第百三号）第二条第一項 に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法　（平成十一年法律第九十一号）第四条第十五号 の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、**国の行政機関**、**独立行政法人及び指定法人**（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十二条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生じる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する**統一的な基準の策定**、**国の行政機関**における**情報システムの共同化**、情報通信ネットワーク又は電磁的記録媒体を通じた**国の行政機関、独立行政法人又は指定法人**の**情報システムに対する不正な活動の監視及び分析**、**国の行政機関、独立行政法人及び指定法人**におけるサイバーセキュリティに関する**演習及び訓練**並びに**国内外の関係機関との連携及び連絡調整**によるサイバーセキュリティに対する**脅威への対応**、**国の行政機関**、**独立行政法人**及び**特殊法人**等の間におけるサイバーセキュリティに関する**情報の共有**その他の必要な施策を講ずるものとする。

サイバーセキュリティ基本法～重要インフラ関係部分

重要インフラの定義

法第３条及び第12条第２項第３号

重要社会基盤事業者　**国民生活及び経済活動の基盤**であって、その**機能が停止し、又は低下**した場合に国民生活又は経済活動に**多大な影響を及ぼす**おそれが生ずるものに関する事業を行う者

重要社会基盤事業者等　**重要社会基盤事業者**及びその**組織する団体**並びに**地方公共団体**

重要インフラの責務

（地方公共団体の責務）

第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する**自主的な施策を策定**し、及び**実施**する責務を有する。

（重要社会基盤事業者の責務）

第六条　重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力するよう努める**ものとする。

施策

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条　**国は**、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の**自主的な取組の促進**その他の**必要な施策**を**講ずるものとする。**

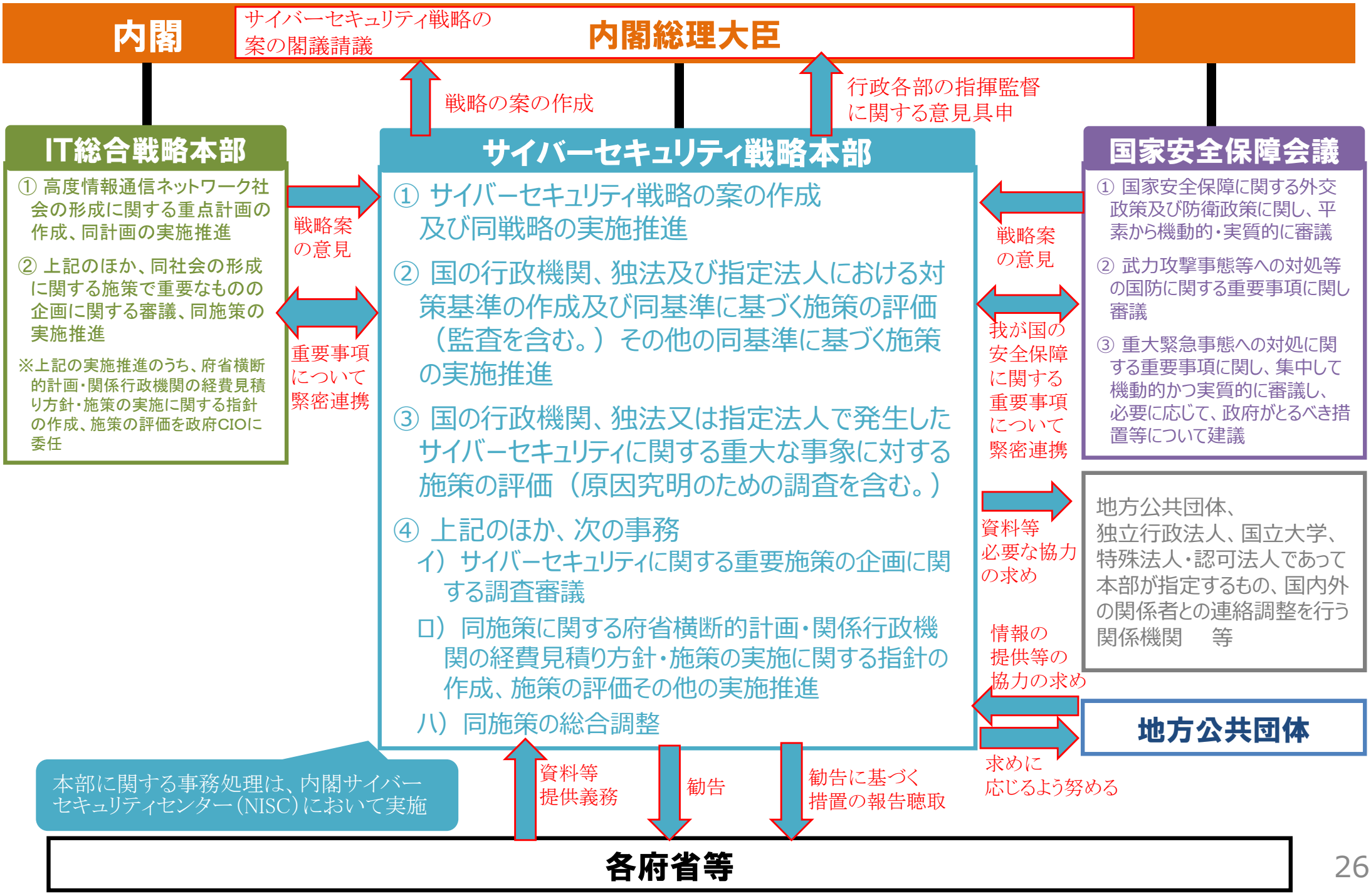
（サイバー関連事業者その他の事業者の責務）

第七条　**サイバー関連事業者**（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）**その他の事業者**は、基本理念にのっとり、その事業活動に関し、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力するよう努める**ものとする。

（国民の努力）

第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に**必要な注意を払うよう努める**ものとする。

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～戦略本部

（設置）

第二十四条　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、内閣に、**サイバーセキュリティ戦略本部（以下「本部」という。）を置く**。

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

一　**サイバーセキュリティ戦略の案の作成及び実施の推進**に関すること。

二　**国の行政機関、独立行政法人及び指定法人**におけるサイバーセキュリティに関する**対策の基準の作成**及び当該基準に基づく**施策の評価（監査を含む。）**その他の当該基準に基づく**施策の実施の推進**に関すること。

三　**国の行政機関、独立行政法人又は指定法人**で発生したサイバーセキュリティに関する**重大な事象に対する施策の評価**（原因究明のための調査を含む。）に関すること。

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策で**重要なものの企画に関する調査審議**、**府省横断的な計画**、**関係行政機関の経費の見積り**の方針及び**施策の実施に関する指針の作成**並びに**施策の評価**その他の**当該施策の実施の推進**並びに**総合調整**に関すること。

２　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。

３　本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。

４　本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

（組織）

第二十六条　本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

サイバーセキュリティ基本法～勧告

（サイバーセキュリティ戦略本部長）

第二十七条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。

2　本部長は、本部の事務を総括し、所部の職員を指揮監督する。

3　本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一条の規定により提供された資料、情報等に基づき、必要があると認めるときは、**関係行政機関の長に対し、勧告することができる。**

4　本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、**その勧告に基づいてとった措置について報告を求めることができる。**

5　本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、**内閣総理大臣に対し**、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう**意見を具申することができる。**

内閣法

第六条　内閣総理大臣は、閣議にかけて決定した方針に基いて、行政各部を指揮監督する。

事務の委任

（事務の委任）

第三十条　本部は、第二十五条第一項第二号に掲げる事務（独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準に基づく監査に係るものに限る。）又は同項第三号に掲げる事務（独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事業の原因究明のための調査に係るものに限る。）の一部を、独立行政法人情報処理推進機構その他のサイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人に**委託**することができる。

２　前項の規定により事務の委託を受けた法人の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を洩らし、又は東洋してはならない。

３　第一項の規定により事務の委託を受けた法人の役員又は職員であって当該委託に係る事務に従事するものは、刑法（明治四十年法律第四十五号）その他の罰則の適用については、法令により公務に従事する職員とみなす。

（罰則）

第三十七条　第三十条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

サイバーセキュリティ基本法～資料提供

（資料提供等）

第三十一条　**関係行政機関の長**は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する**資料又は情報**であって、本部の所掌事務の遂行に資するものを、**適時に提供**しなければならない。

２　前項に定めるもののほか、**関係行政機関の長**は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する**資料又は情報の提供**及び**説明**その他**必要な協力**を**行わなければならない。**

（資料の提出その他の協力）

第三十二条　本部は、その所掌事務を遂行するため必要があると認めるときは、**地方公共団体**及び**独立行政法人**の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の理事長、**特殊法人**及び**認可法人**であって本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な**資料の提出**、**意見の開陳**、**説明**その他の**協力**を**求めることができる。**

２　本部は、その所掌事務を遂行するため**特に必要があると認めるとき**は、前項に**規定する者以外の者**に対しても、**同項の協力を依頼することができる。**

地方公共団体以外の
重要インフラ事業者等もこちら

我が国におけるサイバーセキュリティ政策推進体制

内閣

内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　東京オリンピック競技大会・パラリンピック競技大会担当大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術(IT)政策担当大臣
有識者（７名；10名以下）

閣僚が参画

遠藤　信博　日本電気株式会社代表取役執行役員社長
小野寺　正　ＫＤＤＩ株式会社取締役会長
中谷　和弘　東京大学大学院法学政治学研究科教授
野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎　情報セキュリティ大学院大学教授
前田　雅英　日本大学大学院法務研究科教授
村井　純　慶應義塾大学教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
サイバーセキュリティ補佐官

政府機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

＜重要インフラ所管省庁＞

金融庁　（金融機関）
総務省　（地方公共団体、情報通信）
厚生労働省　（医療、水道）
経済産業省　（電力、ガス、化学、クレジット、石油）
国土交通省　（鉄道、航空、物流）

＜その他関係省庁＞

文部科学省（セキュリティ教育）等

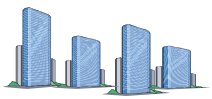
協力

協力

閣僚本部員５省庁

警察庁（サイバー犯罪・攻撃の取締り）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）

重要インフラ事業者等



政府機関（各府省庁）

企業

個人

基本法第13条の規定に基づき戦略本部が指定する法人（指定法人）について

■ 特殊法人・認可法人は、その行う業務や保有する情報も様々であることから、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動に及ぼす影響を勘案して、サイバーセキュリティ戦略本部が指定。

①から④の要件に該当するかを検討

①国の業務との一体性	②保有情報の機微性、業務の国民生活・経済活動へ与える影響	③法人の自主的な対策のみに委ねることの適切性	④NISCの知見・能力の活用可能性
		※ 自主的な対策に委ねた場合に必要な対策が講じられず、重大かつ深刻な事象を発生させた、又は発生させるおそれがあること	※ （NISCが行ってきた）インターネット接続口にセンサーを設置した監視による実効性あるセキュリティ対策が図られること）

以下の法人を指定

■ 公的年金関係
- 日本年金機構
- 地方公務員共済組合連合会
- 地方職員共済組合
- 都職員共済組合
- 全国市町村職員共済組合連合会
- 国家公務員共済組合連合会
- 日本私立学校振興・共済事業団
- 公立学校共済組合

■ マイナンバー関係
- 地方公共団体情報システム機構

ＮＩＳＣと関係機関との協力（パートナーシップ）について

サイバーセキュリティ対策を推進するため、ＮＩＳＣは関係機関との協力関係を強化。

一般社団法人ＪＰＣＥＲＴコーディネーションセンター（JPCERT/CC）

【協力内容】 **国際連携活動及び情報共有等**に関するパートナーシップを新たに締結。（参考：「サイバーセキュリティ基本法」（平成26年法律第104号）による、インシデント発生時に国内外の連絡調整を行う関係機関への協力要請。）

独立行政法人情報処理推進機構（ＩＰＡ）

【協力内容】 **脆弱性対応**、**民間事業者や独立行政法人等との情報共有**、政府機関の**システム調達等に関するセキュリティ認証**、**国民・企業等に対する普及啓発**等の幅広い分野でのパートナーシップを新たに締結。

国立研究開発法人情報通信研究機構（NICT）

【協力内容】 **情報通信関連のセキュリティ技術情報の共有**、**研究開発戦略の推進に関する協力**、**2020年オリンピック・パラリンピック東京大会等に向けたサイバーセキュリティ技術に関する協力**等に関するパートナーシップを締結。

国立研究開発法人産業技術総合研究所（AIST）

【協力内容】 **脆弱性等に関する情報共有**、研究開発の推進等に関する協力、ITやサイバーセキュリティに関する**科学技術的な専門的知見の共有、プライバシー保護に関する専門的知見の共有、サイバーセキュリティに関する企業等との橋渡しに関する協力**等に関するパートナーシップを締結。

・サイバーセキュリティ戦略

新たな「サイバーセキュリティ戦略」について（全体構成） （2015.9.4閣議決定）

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
  同時に、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・発展させ、もって「**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**」に寄与する。

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**
安全なIoT活用による新産業創出

■ **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備

■ **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

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**
事業者の取組促進、普及啓発、サイバー犯罪対策

■ **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化

■ **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定 及び 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**
警察・自衛隊等のサイバー対処能力強化

■ **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進

■ **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的施策

■ **研究開発の推進**
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ **人材の育成・確保**
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

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

新たな「サイバーセキュリティ戦略」について（総論）

1.サイバー空間に係る認識　　2.目的　　3.基本原則

- 本戦略は、2020年東京オリンピック・パラリンピック競技大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示すもの。

1　サイバー空間に係る認識

- サイバー空間は「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間で、経済社会の活動基盤である。
- 実空間のモノやヒトが、サイバー空間により物理的制約を超えて連接することで、実空間とサイバー空間の融合が高度に深化した「連接融合情報社会(連融情報社会)」が到来しつつある。
- 一方、国民生活・経済社会活動への重大な被害や我が国の安全保障に対するサイバー脅威も高まっている。今後、こうした脅威が更に深刻化することが予想される。

2　目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって**「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」**に寄与する。

3　基本原則

本戦略の目的達成のための施策の立案及び実施に当たり、以下に示す基本原則に従う。

① 情報の自由な流通の確保：サイバー空間発展の基盤として、情報の自由な流通が保証された空間を維持

② 法の支配：実空間と同様にサイバー空間に対しても「ルールや規範」の適用を徹底

③ 開放性：常に参加を求める者に開かれ、新たな価値を生み出す空間として保持

④ 自律性：各者の主体的な行動により、悪意ある行動を抑止する自律的メカニズムを推進

⑤ 多様な主体の連携：様々な主体の適切な連携関係構築とダイナミックな対処策実現

我が国は、上記の５つの基本原則に従うとともに、国民の安全・権利の保障のため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として保持する。

新たな「サイバーセキュリティ戦略」について（各論①）

4.目的達成のための施策

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

- 企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(SBD)の考え方に基づき、安全なIoT(モノのインターネット)システムを活用した事業を振興
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を整合的に実施するための体制等を整備
- エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドライン等を整備
- IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築(経営ガイドライン等の発信含む)
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民民間・官民間における脅威・インシデント情報の共有網の拡充

■セキュリティに係るビジネス環境の整備

- 政府系ファンドの活用等により、サイバーセキュリティ関連産業を振興(ベンチャー企業の育成等を含む)
- 中小企業等のクラウドサービス活用に有効なセキュリティ監査の普及促進
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステムのセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備

▲自動運転車の実証実験

サイバーセキュリティ経営ガイドライン

- **サイバー攻撃対策は、ＩＴを利活用する限り避けて通れない経営課題。**
- **企業経営者を対象に、対策を推進するためのリーダーシップのとり方について、ガイドラインを策定。（平成27年12月）**

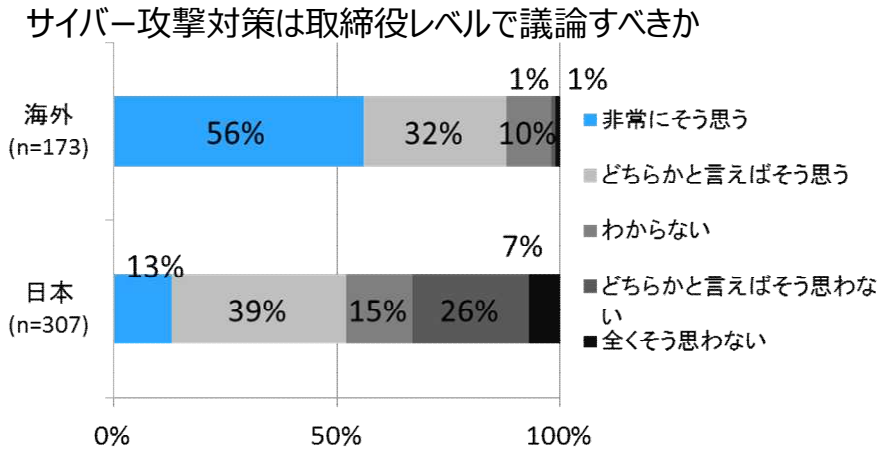
【サイバー攻撃リスクは経営課題】

○Web サーバーに対する不正アクセスにより個人情報が流出した懸念が発生。

○結果として４半期純利益を大幅に下方修正した事例あり。

【サイバー攻撃対策が経営問題として考えられていない】

○海外の企業と比べ、サイバー攻撃対策について取締役レベルの問題と考える我が国企業は少ない



（出典）KPMGジャパン「KPMG Insight 日本におけるサイバー攻撃の状況と課題ーセキュリティサーベイ2013からー」より経済産業省作成

【サイバーセキュリティ経営ガイドラインの概要】

１．サイバーセキュリティ経営の３原則

（１）経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

（２）自社のみならず、ビジネスパートナーを含めた対策が必要

（３）平時及び緊急時のいずれにおいても、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

２．サイバーセキュリティ経営の重要１０項目の概要

（１）リーダーシップの表明と体制の構築

（サイバーセキュリティリスクを認識し、体制構築を指示）

（２）サイバーセキュリティリスク管理の枠組み決定

（ＰＤＣＡの仕組を作らせ、経営者も適時状況を把握）

（３）リスクを踏まえた攻撃を防ぐための事前対策

（対策に必要な資源（予算、人材等）の確保）

（４）サイバー攻撃を受けた場合に備えた準備

（緊急時の対応体制の整備と演習の実施、経営者の説明準備）

サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

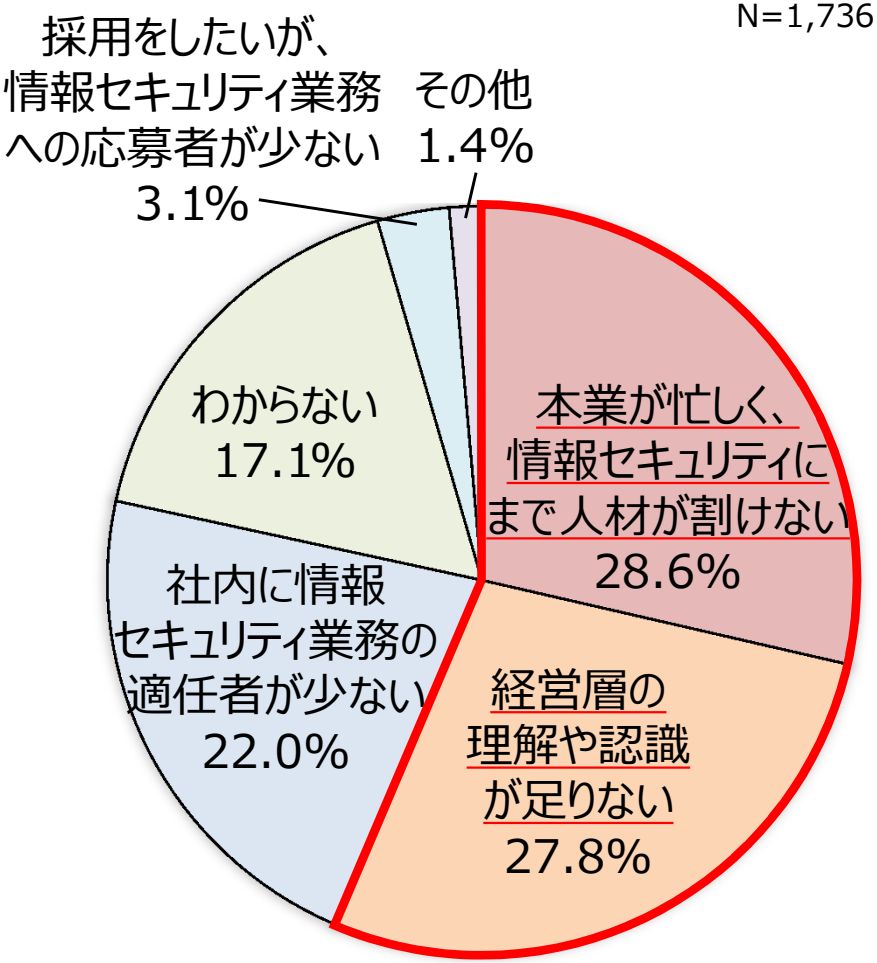
企業等における情報セキュリティ対策の現状

○企業では**情報セキュリティに関する業務に従事する人員が不足**。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。

○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が６割程度。

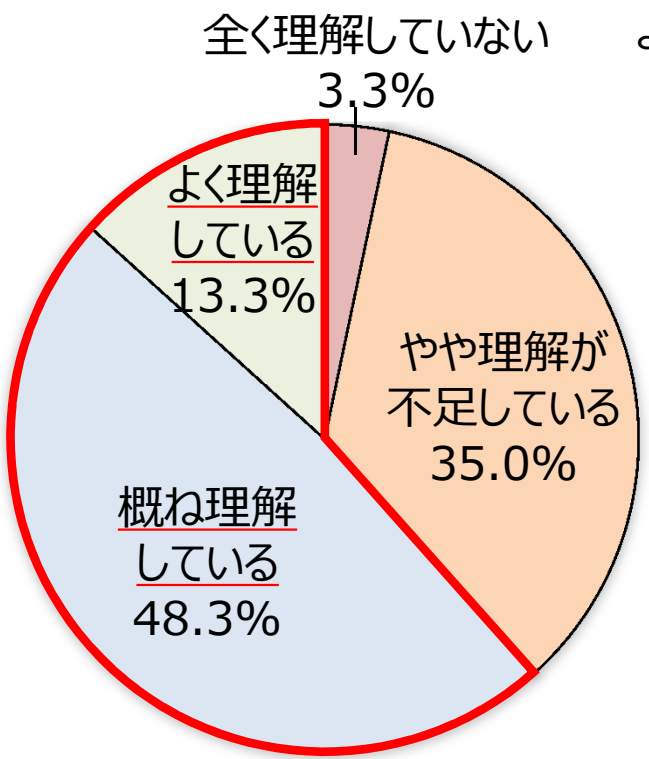
人員不足の原因（社内向け業務）

N=1,736

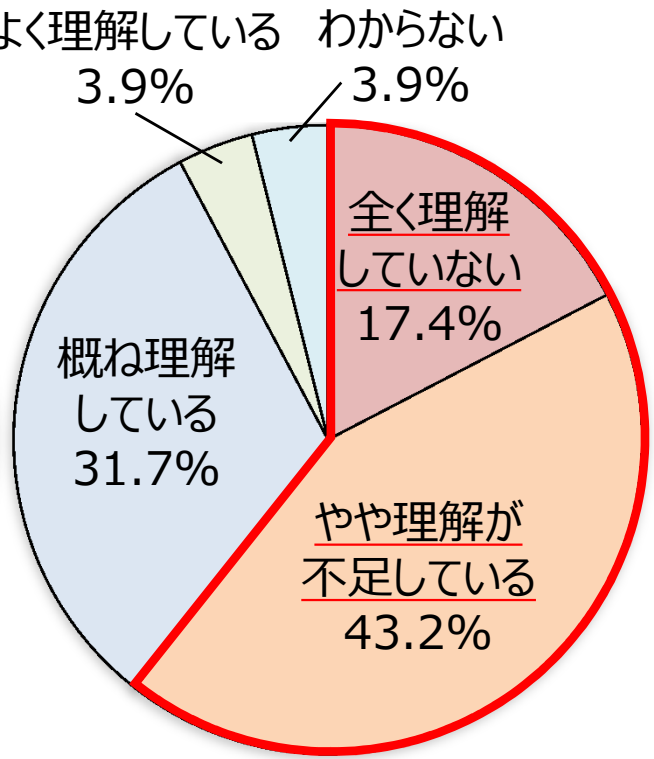


経営層の認識・理解度

経営層自身 N=180
（６割が理解して**いる**と回答）



経営層以外N=2,731
（６割が理解して**いない**と回答）



出典：独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2014年7月　より作成

サイバーセキュリティに関するリスク開示（有価証券報告書）

上場企業225社（日経225）の平成21～25年度の5年間を対象
「事業等のリスク」へのサイバーセキュリティリスクの記載状況の調査・分析

- 開示企業数は、平成21年度の52%（116社）から**平成25年度の60%（136社）**へと増加。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の**14業種が100%（合計51社）**。
- 繊維、パルプ・紙、鉄鋼等の**4業種は0%（合計14社）**。
- 素材産業全体（64社）では開示割合が32.8%と低く、**原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低い**と考えられる。
- サイバーセキュリティリスクの**記載文書が5年間同一の企業（65社）には、その記載の仕方が包括的で意味が広く捉えられる（想定インシデント・被害が具体的でない）もの**が多かった。
- 自社で発生したサイバーセキュリティインシデントを記載している企業は**調査対象企業中4社**と少なかった。

平成25年度 日経225社-業種別サイバーセキュリティ情報開示状況

日経業種分類				開示企業数	開示企業%	
大分野	（社数）	中分野	（社数）		中分類	大分類
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	**100.0%**	
B 金融	21	**06 銀行**	11	11	**100.0%**	100.0%
		07 その他金融	1	1	**100.0%**	
		08 証券	3	3	**100.0%**	
		09 保険	6	6	**100.0%**	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	**100.0%**	
		13 サービス	7	5	71.4%	
D 素材	64	14 鉱業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	**100.0%**	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	**100.0%**	
		27 その他製造	3	3	**100.0%**	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	**100.0%**	
		31 海運	3	1	33.3%	
		32 空運	1	1	**100.0%**	
		33 倉庫	1	1	**100.0%**	
		34 電力	3	3	**100.0%**	
		35 ガス	2	2	**100.0%**	
合計	225		225	136		

新たな「サイバーセキュリティ戦略」について（各論②）

4.目的達成のための施策

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

- ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化の推進
- 攻撃を受けた端末の利用者に対する注意喚起等の推進
- 整備が進む公衆無線LAN等のセキュリティ確保のための対策検討
- 地域における普及啓発活動の促進、中小企業や地方公共団体への啓発・支援
- サイバー犯罪への対処能力・捜査能力の向上に向けた取組の強化
  （通信履歴の保存の在り方についての関係事業者における適切な取組の推進を含む）

▲双方向型の普及啓発セミナー（サイバーセキュリティカフェ）

■ 重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制を整備
- スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進


▲サイバー攻撃等に対する対応能力向上のための演習
（重要インフラ分野横断的演習）

■ 政府機関を守るための取組

- ペネトレーションテスト等を通じたセキュリティ対策を徹底、サプライチェーン・リスクへの対応、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能強化、 標的型攻撃に対する多重防御の取組加速等による防御力の強化
- マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化
- 新たなIT製品・サービスの特性を踏まえた政府統一的なセキュリティ対策の策定・推進
- 独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等への監視・監査・原因究明調査の実施等による総合的な対策強化

（参考）インシデント対応体制～意義

- ITシステムの複雑化　→原因特定や復旧がより困難に／IT部門と利用部門の乖離
- ITシステムの汎用化　→被害が広範囲かつ短期に拡大しやすい
- 攻撃の高度化・複雑化　→対策・対応に高い専門性が必要で部門ごとの確保が困難

組織的な対応が必要

求められれる機能とは、

組織内の情報共有及び連携

- ✓ インシデント報告を集める窓口の一本化
- ✓ 組織内のインシデントの一元管理と部署間調整

外部組織との調整

- ✓ 外部に起因するインシデント（DDoS、高度サイバー攻撃(APT:Advanced Persistent Threat)による攻撃など）を解決するため、他組織に対する適切な依頼
- ✓ 外部からのインシデント関連情報を受け取る窓口の一本化
- ✓ 組織間連携しなければならないインシデント対応のため、外部組織との強い信頼関係構築

インシデント発生後に、その対応方法を考え始め対応体制をとるのは、被害を拡大させる一因となる

→できるだけ**事前にインシデント対応計画を策定し、対応体制等を整えておく**必要

JPCERT/CC資料より作成

（参考）インシデント対応体制～有用性

組織内CSIRTについて

- ✓ Computer Security Incident Response Team の略、「シーサート」と発音される
- ✓ 組織内でコンピュータセキュリティインシデント対応に関する業務を専門に担当するチーム
- ✓ 組織によっては、他の関連業務と兼務することによって、組織内にCSIRT の機能を実装している場合もある

組織の内部に対する主な機能

- ✓ 組織内で発生したインシデントの報告を受けるための、一本化された窓口を提供する
- ✓ 発生したインシデントに対応する、または、発生したインシデントへの対応に必要な技術的支援やノウハウを提供する
- ✓ インシデント対応における組織としての意思決定を支援する
- ✓ 組織横断的に発生するインシデントにおいて、組織内の調整役として活動する
- ✓ 組織の情報システム管理者、ユーザ、その他の従業員に対し、セキュリティ教育と意識啓発を行う

組織の外部に対する主な機能

- ✓ 外部のインシデント対応組織との連絡調整を行う
- ✓ セキュリティインシデントの事例や動向、インシデント対応手法や技術に関する情報を外部から収集し、組織内に展開する
- ✓ 従業員・メディア・国民へ適切な情報を提供する

JPCERT/CC資料より作成

新たな「サイバーセキュリティ戦略」について（各論③）

4.目的達成のための施策

国際社会の平和・安定及び我が国の安全保障　～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

- 警察や自衛隊を始めとする対処機関の能力の質的・量的な向上
- 安全保障上重要な先端技術(宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等)に係るサイバーセキュリティの確保
- 政府機関や重要インフラ事業者等によるサービスの持続的提供のための情報の共有・分析・対応に向けた官民連携の一層の強化

▲日ASEAN情報セキュリティ政策会議

■国際社会の平和・安定

- 国連等におけるサイバー空間に係る国際的なルール等の形成に向けた積極的な貢献
- サイバー空間を悪用する国際テロ組織に対する国際社会と連携した対処
- 各国の能力構築(キャパシティビルディング)への積極的な協力の推進

▲我が国で開催したサイバーセキュリティに関する国際カンファレンス（Meridian Conference 2014）

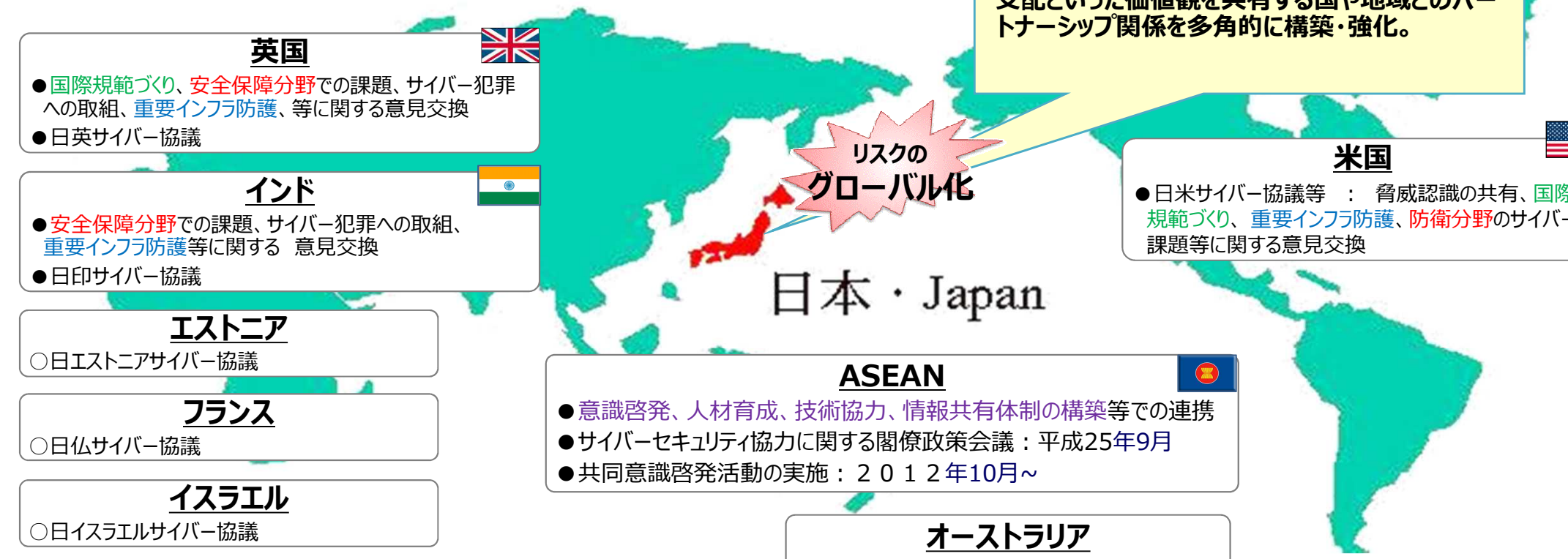
■世界各国との協力・連携

- アジア大洋州　：　日・ASEAN間の協力関係の更なる深化・拡大並びに地域の戦略的パートナーとの協力・連携の強化
- 北米　：　同盟国たる米国とあらゆるレベルでの緊密な連携・対応(日米サイバー対話、インターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ等)
- 欧州・中南米・中東アフリカ　：　基本的価値観を共有する国々とのパートナーシップの構築・強化

国際連携に向けた政策対話の推進

基本的な考え方

「情報の自由な流通の確保」という基本的な考え方の下、民主主義、基本的人権の尊重及び法の支配といった価値観を共有する国や地域とのパートナーシップ関係を多角的に構築・強化。



EU
- 重要インフラ防護や官民の情報共有等の取組の共有、意識啓発や政策動向の意見交換

ロシア
- ○日露サイバー協議

英国
- 国際規範づくり、安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護、等に関する意見交換
- 日英サイバー協議

インド
- 安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護等に関する　意見交換
- 日印サイバー協議

エストニア
- ○日エストニアサイバー協議

フランス
- ○日仏サイバー協議

イスラエル
- ○日イスラエルサイバー協議

米国
- 日米サイバー協議等　：　脅威認識の共有、国際規範づくり、重要インフラ防護、防衛分野のサイバー課題等に関する意見交換

ASEAN
- 意識啓発、人材育成、技術協力、情報共有体制の構築等での連携
- サイバーセキュリティ協力に関する閣僚政策会議：平成25年9月
- 共同意識啓発活動の実施：２０１２年10月～

オーストラリア
- ○日豪サイバー協議

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
- サイバー空間における自由と安全保障の両立、開放性や透明性、マルチステークホルダーの重要性、サイバー空間における**国際行動規範づくり**，サイバー犯罪条約，キャパシティ・ビルディング、サイバー空間における従来の**国際法や国家間関係を規律する伝統的規範の適用**、信頼醸成措置等に関する対話。
- 60ヵ国の政府機関，国際機関，民間セクター，NGO等が参加。
- ハーグ会議：20１５年4月　～

MERIDIAN
- **重要インフラ防護**等のベストプラクティスの共有や国際連携方策等に関する意見交換。
- 米・英・独・日等の重要インフラ防護担当者が参加。

IWWN
- サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。
- 米・独・英・日等の政府機関、CERTが参加。

新たな「サイバーセキュリティ戦略」について（各論④・推進体制）

4.目的達成のための施策　　5.推進体制

横断的施策

■研究開発の推進

- 関係者間の情報・データの共有等によるサイバー攻撃の検知・防御能力の一層の向上
- 融合領域の研究促進、及び安全保障のためのコア技術(暗号技術等)の保持
- 各国が強みを有する技術を有機的に組み合わせた国際連携による研究開発の推進

▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ

■人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 初等中等教育段階からの教育の充実
  (論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実)
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進

▲ 58ヶ国が参加したセキュリティコンテスト(2014年度)

5　推進体制

- NISC対処能力の一層の強化や産学官及び関係省庁間の連携強化によるサイバー攻撃の検知・分析・判断・対処の機能強化
- 国家の関与が疑われる高度な攻撃に対し、戦略本部とNSC(安全保障)・重大テロ対策本部(危機管理)と緊密に連携
- 東京オリンピック・パラリンピック競技大会等に向け、リスクの明確化、組織・施設・協力関係の構築・維持、十分な訓練を実施

- 戦略本部は、各年度の年次計画及び年次報告を作成するとともに、経費見積り方針を策定する。

情報セキュリティ研究開発戦略（改定版）（14年７月、情報セキュリティ政策会議決定）

サイバーセキュリティ戦略（2013年6月策定） において示された
○ サイバー攻撃の検知・防御能力の向上
○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発 等

を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1．サイバー攻撃の検知・防御能力の向上
・分散しているサイバー攻撃情報等の共有のための組織等の連携強化
・研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討

2．社会システム等を防護するためのセキュリティ技術の強化
・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進

3．産業活性化につながる新サービス等におけるセキュリティ研究開発
・今後発展が期待されるIT利用分野で上流工程からセキュリティ品質の組込を推進

4．情報セキュリティのコア技術の保持
・暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化

5．国際連携による研究開発の強化
・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

研究開発の効果・成果を高めるための方策等

1．研究成果の社会還元の推進
2．必要な研究開発リソースの確保と柔軟性確保
3．情報セキュリティ技術と社会科学など他分野との融合

情報セキュリティ研究開発における重要分野
（※ 左記の観点を踏まえ、重要分野を整理）

(1) 情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク 等
(2) ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保 等
(3) 個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用 等
(4) 研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術 等
(5) 発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続 等

SIP新課題：重要インフラ等におけるサイバーセキュリティの確保

H27（2015）年度～H31（2019）年度（予定）、H27年度予算：5億円

経緯

6月18日（第10回CSTI）	新課題候補「重要インフラ等におけるサイバーセキュリティの確保」の承認
8月6日	情報セキュリティ大学院大学・後藤厚宏教授の内閣府政策参与への任命
9月15日～10月5日	研究開発計画案パブリックコメントの実施
10月15日	ガバニングボードでの事前評価
11月10日（第12回CSTI：持ち回り）	実施方針の決定

PD

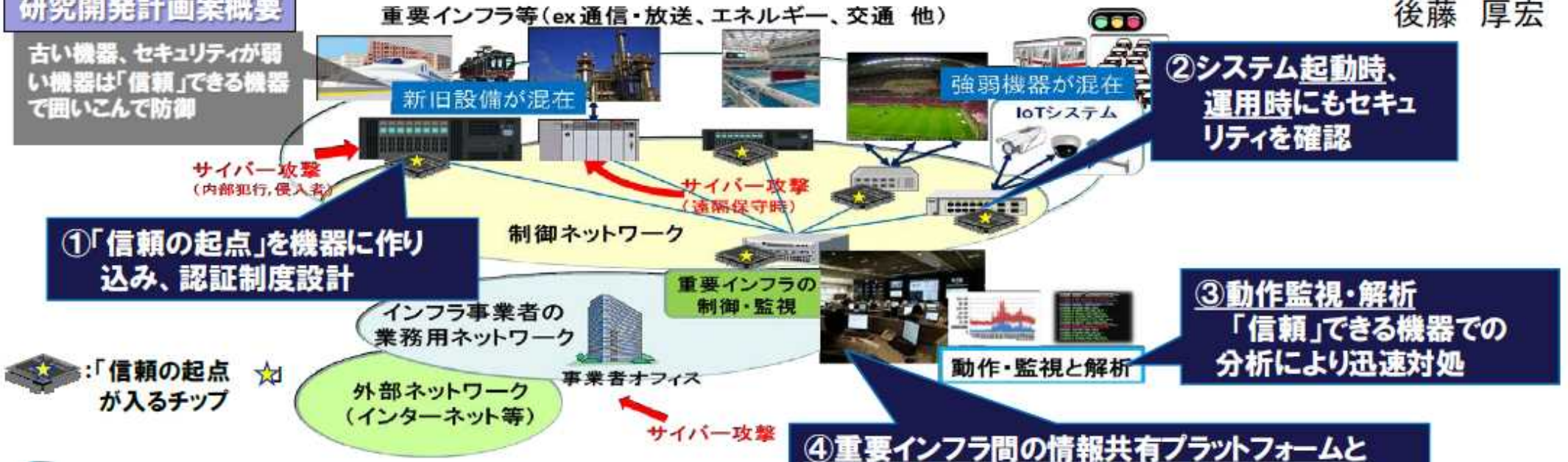
情報セキュリティ大学院大学教授
後藤　厚宏

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

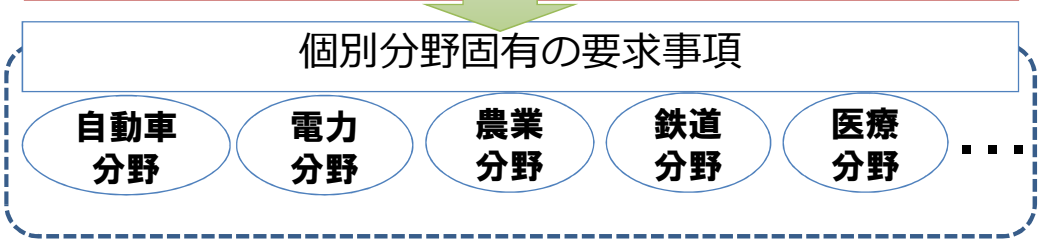


安全なIoTシステムのためのセキュリティに関する一般的枠組について（概要）　（H27.8）

目的

- IoT(Internet of Things)システムは、従来の情報セキュリティの確保に加え、新たに**安全確保が重要**
- **セキュリティ・バイ・デザイン**の思想で設計・構築・運用されることが不可欠
- 安全なIoTシステムが具備すべき**一般要求事項としてのセキュリティ要件の基本的要素**を明らかにしたもの

安全なIoTシステムのためのセキュリティに関する一般的枠組み（個別分野の標準の**"テンプレート"**）



検討の視点

- 一つのIoTシステムリスクが他のIoTシステムに波及する可能性→**System of Systems**としての捉え方
- **機密性、完全性、可用性に加え、安全性**の要件確保

基本原則

- 関係者間の相互理解及び相互信頼の下、ネットワーク側とモノ側が、一体となり**システム全体としてセキュリティ確保**を図ることが必要。
- **セキュリティ・バイ・デザイン**を基本原則とし、**システム稼働前に確認・検証できる仕組**が必要。
- その際、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の**各段階の要件定義**が必要であり、以下の項目の明確化が必要。
  - ✓ 定義・範囲
  - ✓ 安全性・機密性・完全性・可用性
  - ✓ 確実な動作に必須事項、障害発生時の回復に必要な要件
  - ✓ 法律等からの要求事項
  - ✓ サイバー攻撃時の機能確保と迅速な復旧
  - ✓ 責任分界点、データの扱い方

取組方針

- **法令等の要求事項の明確化**
- IoTシステムの構成を**適切にモデル化**し、モデルを参照しながらセキュリティ要件を議論
- リスクアセスメントを活用した**セキュリティ対策や実装方法等の明確化**。ただし、リスクに応じた**柔軟な対応が必要**。
- 普遍的な**性能要求**とその時点での有効な手段の具体的方法を示す**仕様要求**の適切な適用
- 技術革新を前提とした**段階的・継続的アプローチ**
- IoTシステムに関連する者の**役割分担**（連携・協調によるセキュリティ確保の在り方や責任分界点の明確化を含む）
- データの利活用と個人情報保護の仕組み、機器認証の在り方などの**運用ルールの明確化**

新・情報セキュリティ人材育成プログラム（１４年５月、情報セキュリティ政策会議決定）

サイバーセキュリティ戦略で示された課題

情報セキュリティに係るリスクの深刻化に対応するためには、
○人材の量的不足の解消に向け 積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題。
○そのためには、社会全体で育成し活用するための仕組みが必要。

人材の量的・質的不足

情報セキュリティ従事者 約**26.5万人**
うち質的不足 **約16万人**
さらに量的不足 **約8万人**
⇒これら人材の雇用の受け皿も不可欠

ＩＴ人材１０６万人（ＳＥ８０万人）*IPA調べ

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○組織の経営層
・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。
・製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

○実務者層のリーダー層
・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

【供給】人材の「量的拡大」と「質的向上」

○ＩＴ技術者等に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。

○高度な専門性及び突出した能力を有する人材の発掘・育成を推進するとともに、実社会での活躍を促進。

○グローバル水準の人材の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。

○政府機関は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。

○教育機関（初等中等教育機関含む）の実践的なＩＴ教育を充実させるとともに、情報セキュリティに関する教員養成を推進。

「サイバーセキュリティ人材育成総合強化方針」概要①　（H27.3本部決定）

策定の趣旨

「「日本再興戦略」改訂2015」（平成27年６月閣議決定）、「サイバーセキュリティ戦略」（平成27年９月閣議決定）等を踏まえ、サイバーセキュリティ分野の人材育成の具体的な強化方針を示す。

参考１「日本再興戦略」改訂2015 抜粋
・人材育成に係る施策を総合的に推進するため、本年度中に「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。

参考２　サイバーセキュリティ戦略抜粋
・人材育成に係る施策を総合的かつ強力に推進するための方針を策定する。

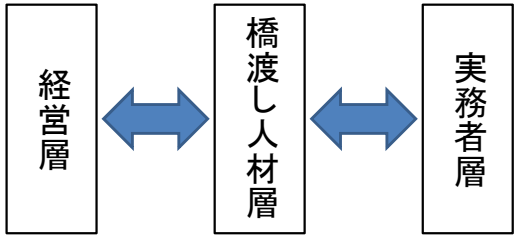
全体構成

第１章　社会で活躍できる人材の育成
第２章　政府機関における人材の育成
第３章　今後の検討の枠組み

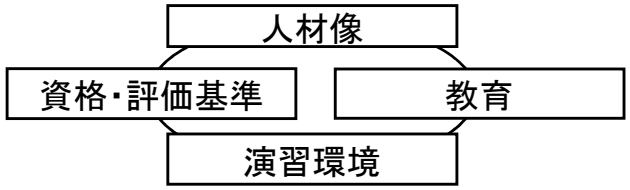
基本的考え方

○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

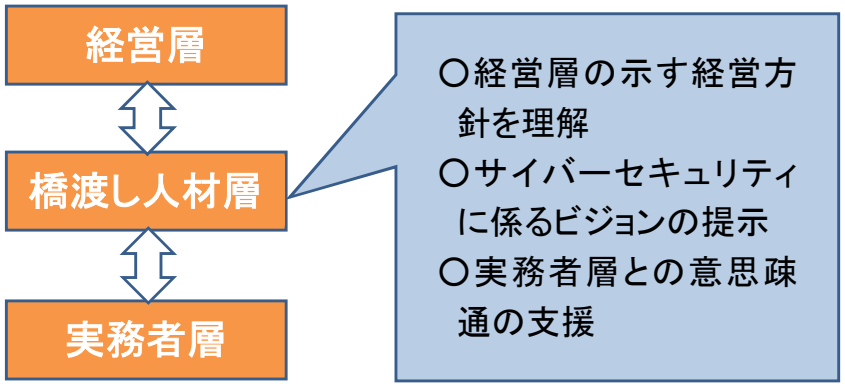


【人材の供給（教育）】
人材育成の循環システム
－確かな知識と実践力の下に、
　様々な業務経験を経て、人材が育成



社会で活躍できる人材の育成　（強化方針②）

人材の需要面



（1）経営層の意識改革

- 「サイバーセキュリティ経営ガイドライン」（平成27年12月）の普及促進
- 企業等のセキュリティ対策に係る情報発信の方策の検討（平成28年6月を目途）

（2）「橋渡し人材層」の育成（→経営層への働きかけ）

- 経営層への説明用コンテンツの作成（平成28年6月を目途）
- マネジメント能力向上のための演習の実施（平成28年度以降）
- セキュリティと他分野の専門性を併せ持つ教育の推進（社会人向け、継続）

人材の供給面

人材像の提示
- 産業界で求められる人材像の明確化（平成28年度中）

教育の充実
- enPiT等の大学教育の充実（平成28年度から大学学部にも拡大）
- 高専における演習環境の整備等（平成28年度から実施）
- 「職業実践力育成プログラム」制度等の活用による社会人の学び直し促進（継続）

演習環境の整備
- NICTにおける実践的なサイバー防御演習（CYDER）の拡充（法制度の整備を含む）
- 制御システムのセキュリティ演習の実施（継続）
- 国立情報学研究所における実践的演習環境の整備（国立大学法人等向けに平成28年度から実施）

能力の可視化
- 情報処理安全確保支援士制度の創設（法改正、平成28年度中に具体的な制度設計、国内外の企業等で行っている演習等も活用し、平成32年までに3万人超の有資格者の確保）

enPiT：「成長分野を支える情報技術人材の育成拠点の形成」事業　Education Network for Practical Information Technologiesの略称（「エンピット」と読む）
NICT：国立研究開発法人情報通信研究機構　National Institute of Information and Communications Technologyの略称
CYDER：実践的なサイバー防御演習　CYber Defense Exercise with Recurrenceの略称

（注）上述に加え、突出人材の発掘・育成を推進（人材発掘の場づくり（継続）に加え、平成28年度から演習基盤の整備等を推進）

政府機関における人材の育成　（強化方針③）

【課題】
- ○ セキュリティに係る人材の圧倒的不足
- ○ 一般職員の情報リテラシーが不十分
- ○ システム管理や業務改革の知識・経験を有する人材の不足
- ○ 自組織におけるセキュリティ対策等の司令塔機能が弱体

政府一体となって、政府機関においてセキュリティ・IT人材を本格的に確保・育成する第一歩として、以下の取組を実施

1. 各府省庁における司令塔機能の抜本的強化

- ○ 平成28年度から「サイバーセキュリティ・情報化審議官」の新設等により司令塔機能を抜本的に強化
- ○ 「セキュリティ・IT人材確保・育成計画（仮称）」を作成し、これらの審議官等で構成する会議で共有・フォローアップ
- ○ サイバーセキュリティ対策推進会議（CISO等連絡会議）、各府省庁情報化統括責任者（CIO）連絡会議、次官連絡会議においても共有

（CISO:最高情報セキュリティ責任者Chief Information Security Officerの略称、CIO:情報化統括責任者Chief Information Officerの略称）

2. 橋渡し人材（部内育成の専門人材）の確保・育成

（1）体制の整備・人材の拡充
- ✦ 各府省庁の統括部局・一定のシステム所管部局の体制の整備及び人材の拡充

（2）有為な人材の確保
- ✦ 積極的な広報のほか、大学等での出張講義、インターンシップ等を検討　✦ 各府省庁において有為な人材を確保

（3）一定の専門性を有する人材の育成
- ✦ 「セキュリティ・IT人材育成支援プログラム(仮称)」の作成(研修受講、内閣サイバーセキュリティセンター（NISC）等への出向、大学院・民間企業への派遣等を通じた人材育成)　✦ 将来的に一部人材の総務省行政管理局等での採用・一括管理の枠組みの検討

（4）研修体系の抜本的整理
- ✦ 新たに役職段階別に研修体系を抜本的整理（橋渡し人材の受講者数を4年で1千人超規模を目指す）、修了者へのスキル認定の枠組み構築等
- ✦ 管理職向けの実践的演習等　✦ CSIRT要員研修等の活用　（CSIRT：情報セキュリティ緊急対応体制　Computer Security Incident Response Teamの略称）

（5）適切な処遇の確保
- ✦ 業務の専門性・特殊性等を踏まえ手当等を新たに支給することによる一定の給与上の評価　✦ 高位ポストまで見据えた人事ルート例（イメージ）の設定

3. 外部人材（即戦力の高度専門人材）の確保

- ○ NISC等において高度セキュリティ人材を採用し監査等で各府省庁に派遣　○情報通信技術（IT）総合戦略室における政府CIO補佐官の積極的活用
- ○ 産学官連携によるセキュリティ・IT人材の育成

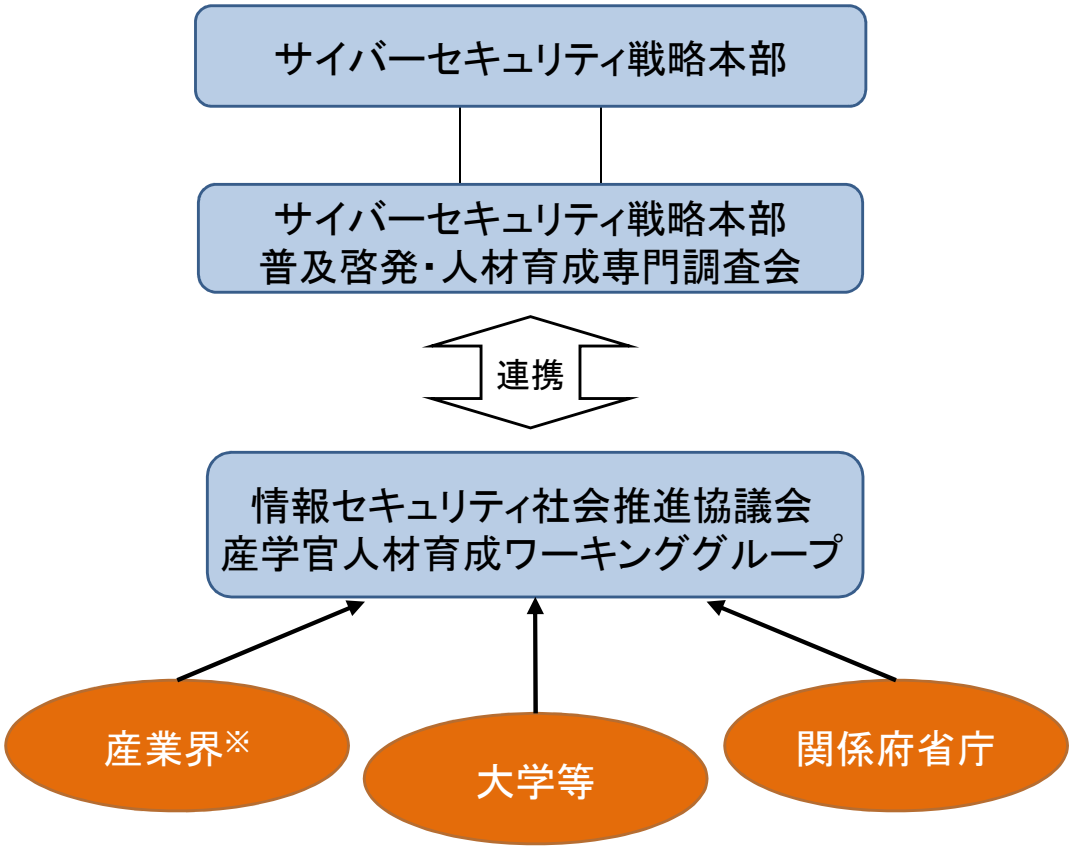
4. 一般職員の情報リテラシー向上

- ○ 各府省庁の新人研修等でのセキュリティ・IT研修実施　○ 新任管理職研修でのセキュリティ・ITの基礎的知識の習得機会提供
- ○ 人事評価マニュアルを改訂し、セキュリティ等に係る行動の評価の着眼点を明示等

今後の検討の枠組み　（強化方針④）

【社会で活躍できる人材の育成】

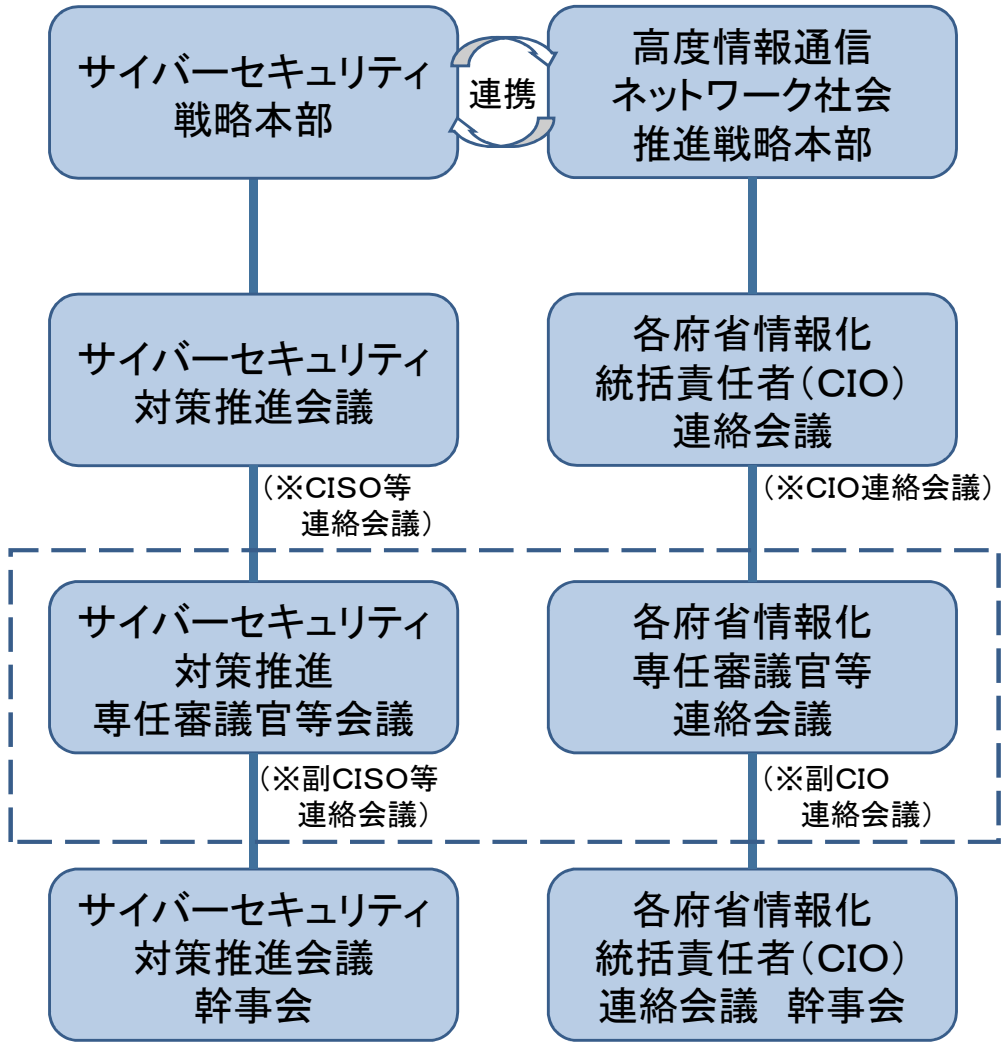
・「産学官の情報共有の場」として情報セキュリティ社会推進協議会 産学官人材育成ワーキンググループで情報共有する。
・次期人材育成プログラムを策定・公表する。（平成28年度中）



※「産業横断サイバーセキュリティ人材育成検討会」との連携を含む。

【政府機関におけるセキュリティ・IT人材の育成】

・平成28年度よりサイバーセキュリティ対策推進専任審議官等会議及び各府省情報化専任審議官等連絡会議を設置する。
・各府省庁において「セキュリティ・IT人材確保・育成計画（仮称）」を作成する。



（CISO:最高情報セキュリティ責任者　Chief Information Security Officerの略称
CIO:情報化統括責任者　Chief Information Officerの略称）

（参考）政府機関等のサイバーセキュリティ対策の抜本的強化①

※日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、2015年に示した対策強化策であって、すでに、所要の法改正を行ったとともに、抜本的な強化を図っているところ。

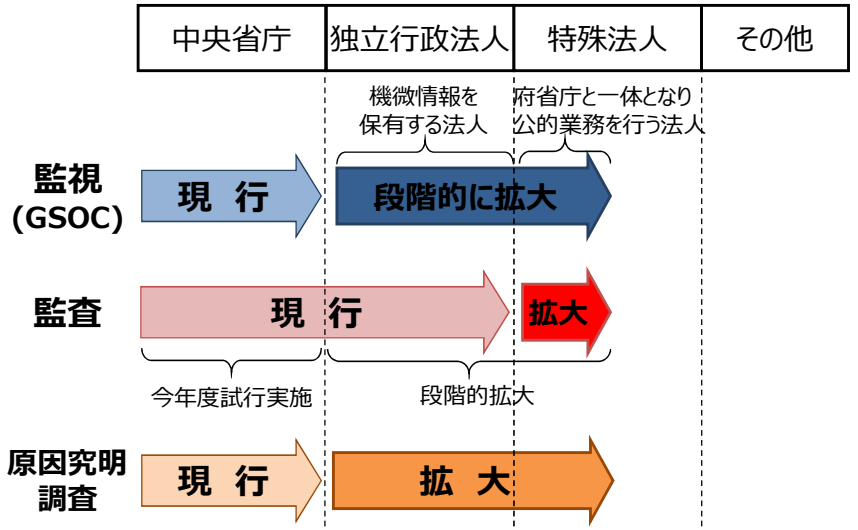
1．NISCの機能強化

■ GSOCの大幅な機能強化

- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化

■ 業務対象の拡大等

- 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大



■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携

■ NISCの要員強化

- 高度セキュリティ人材の民間登用等による対処能力の一層の強化

（参考）政府機関等のサイバーセキュリティ対策の抜本的強化②

２．政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対処に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

（参考）政府機関等のサイバーセキュリティ対策の抜本的強化③

３．その他の重要課題への取組強化

■ 重要インフラに関する取組強化

- 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
- 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善

■ セキュリティ人材の育成のための演習環境の整備（本年度中に人材育成総合強化方針(仮称)を策定）

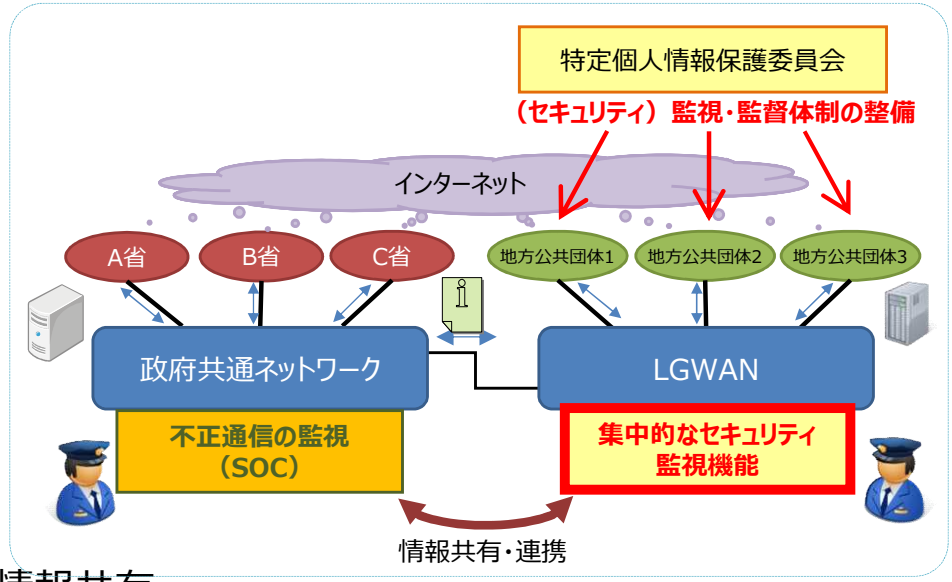
- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 即応予備チームの体制整備

- 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備
  （法改正について速やかに検討）

■ マイナンバー制度の円滑な導入に向けた対策の強化

- 特定個人情報保護委員会において、関係機関と連携して
  監視・監督体制を整備（本年度中を目途）
- 総合行政ネットワーク（LGWAN）について集中監視機能を
  設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知
  体制を整備
- 官民連携を実現する認証連携のための枠組みの取組方針を策定



■ 事案対処に関する取組強化

- サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
- 対処機関における能力の質的・量的向上

・重要インフラに関する施策（行動計画とその見直し）

重要インフラの情報セキュリティに係る第３次行動計画

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、
自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、
ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する

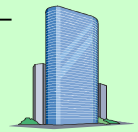
重要インフラ（１３分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

ＮＩＳＣによる調整・連携

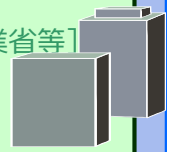
重要インフラ所管省庁（５省庁）

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、鉄道、物流］



関係機関等

- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］



重要インフラの情報セキュリティに係る第３次行動計画

H26.5.19 情報ｾｷｭﾘﾃｨ政策会議 策定
H27.5.25 ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略本部改訂

安全基準等の整備・浸透

重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化

ＩＴ障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施・演習・訓練間の連携によるＩＴ障害対応体制の総合的な強化

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評価を含む包括的なマネジメントの支援

防護基盤の強化

広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

第３次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおける**サービスの持続的な提供**を行い、**自然災害やサイバー攻撃等に起因するＩＴ障害**が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を**可能な限り減らす**とともにＩＴ障害発生時の**迅速な復旧を図る**ことで重要インフラを防護する。

「基本的な考え方」

情報セキュリティ対策は、**一義的には重要インフラ事業者等が自らの責任において実施**するものである。
また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- **政府機関は**、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して**必要な支援を行う**。
- 取組に当たっては、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のみでは多様な脅威への対応に限界があることから、**他の関係主体との連携をも充実させる**。

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- **自らの状況を正しく認識**し、**活動目標を主体的に策定**するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、**相互に自主的に協力**する。
- ＩＴ障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、ＩＴ障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とする**リスク源の認識**。
- 上記のリスク源の評価及びそれに基づく**優先順位を含む方針の策定**。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営**資源の継続的な確保**。
- システムの運用状況の把握等を通じた当該方針の**実行の有無の検証**。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の**検証及び改善策の有無の検証**。

第３次行動計画 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的に、PDCAサイクルの下、「指針」及び「安全基準等」の相互的・継続的改善を目指す。

※安全基準等・・・業法、業界標準／ガイドライン、内規等の総称
※指針・・・・・・安全基準等の策定・改訂に資するため、分野横断的に必要度の高い対策項目を収録したもの

行動計画期間当初の課題

- 優先順位付けされた指針の提示要望（事業者等から）
- 事業者等のPDCAサイクルに沿った指針の見直し

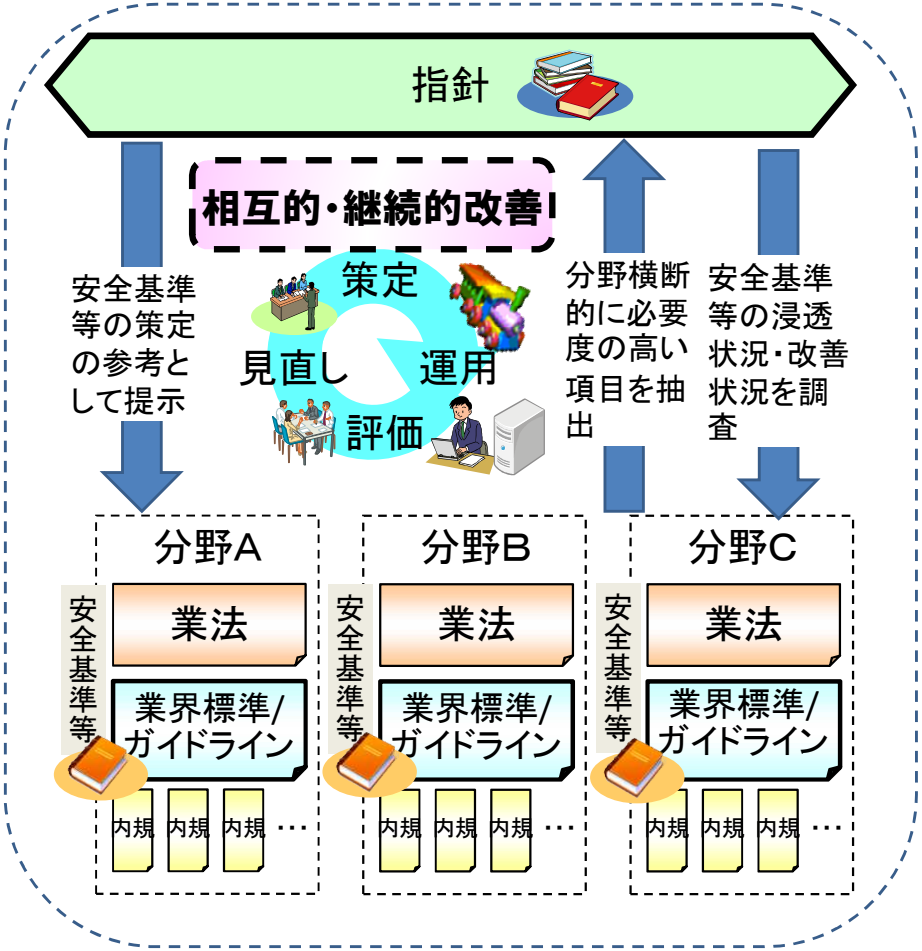
行動計画期間中の施策

（１） 指針の継続的改善
- 指針本編・対策編のPDCAサイクルに沿った見直し
- セキュリティ対策の優先順位付け等（成長モデル）の考え方の例示

（２） 安全基準等の継続的改善
- 各分野の安全基準等を対策等から得た知見を基に改善

（３） 安全基準等の浸透
- 毎年の調査（重要インフラ事業者等への往訪を含む）により、対策状況を客観的に把握
- 中小規模事業者等調査対象の拡大と対策プロセスに沿った項目整理により、強化対象等を明確化

第３次行動計画に基づく取組



『重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定指針』について

指針策定の背景

目指す方向

重要インフラにおけるサービスの持続的な提供

課題

IT障害の極小化／IT障害の迅速な復旧と再発防止

一義的には重要インフラ事業者等による適切かつ継続的な実施・改善が必要

～自らの情報セキュリティ対策の水準や不足を知るために、照らす規範等（安全基準等）が必要～

課題解決に向けて

国の施策として、情報セキュリティ対策の水準の維持・向上に資するガイドラインの提示

～分野ガイドラインや事業者等の内規等の策定・改訂に資する指針の提示～

＊第3次行動計画を受けた指針（第4版）を2015年度に提示

指針（第4版）の概要

指針の体系（以下3冊にて構成）	記載内容	
指針_本編 （概念）	Ⅰ．目的及び位置付け Ⅱ．「安全基準等」で規定が望まれる項目	「策定の目的」、「対象範囲」、「対象とする原因」、「役割」、「公開」、「対策項目（PDCAベース）」に係る解説 ※（解説例）：「情報セキュリティ対策（技術）に係る設計・実装・保守」 情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。
↓ 具体的に何をすればよいか		
指針_対策編 （具現化例）	Ⅰ．対策編の位置付け Ⅱ．具体的な情報セキュリティ対策項目の例示	対策項目（PDCAベース）毎の取組や成果等の例示 ※（対策項目例）：「情報セキュリティ対策（技術）に係る設計・実装・保守」 〇セキュリティ要件の実装に付随するネットワークに係る対応 －外部ネットワークとの接続制限（プロキシ経由等） －内部と外部のネットワークの分離 －不要なポートの閉塞 －公開するサーバー上に保存する情報の制限 －ルーターによるDoS攻撃対策　　等
↓ どの対策から行うか		
指針_手引書 （優先順位付け等の考え方）	Ⅰ．目的及び位置付け Ⅱ．情報セキュリティ対策の優先順位付け及び対応策決定のプロセス	各プロセスを解説しつつ、「どのような対策をどの程度で行うか」を各事業者等が自ら定めることを推奨

第３次行動計画 施策②：情報共有体制の強化

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

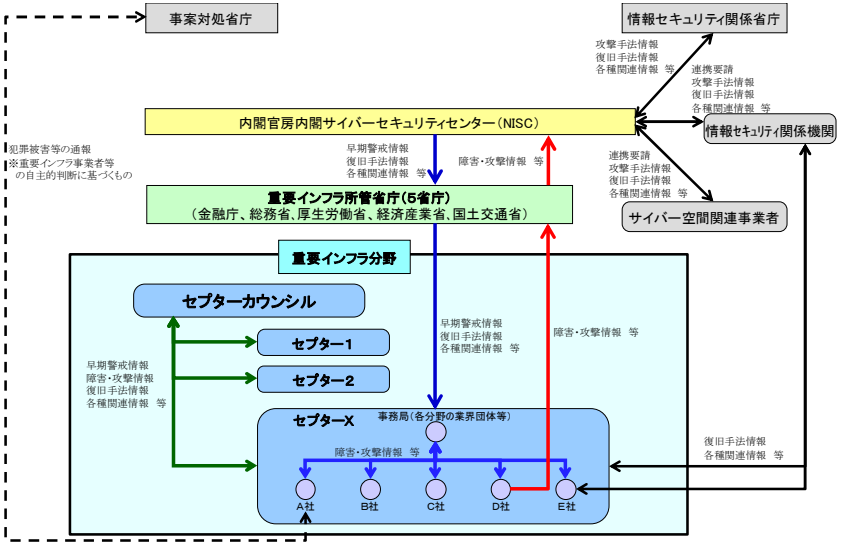
- 多様な関係主体の役割を平時・大規模IT障害発生時に分類して明確化

第３次行動計画に基づく取組

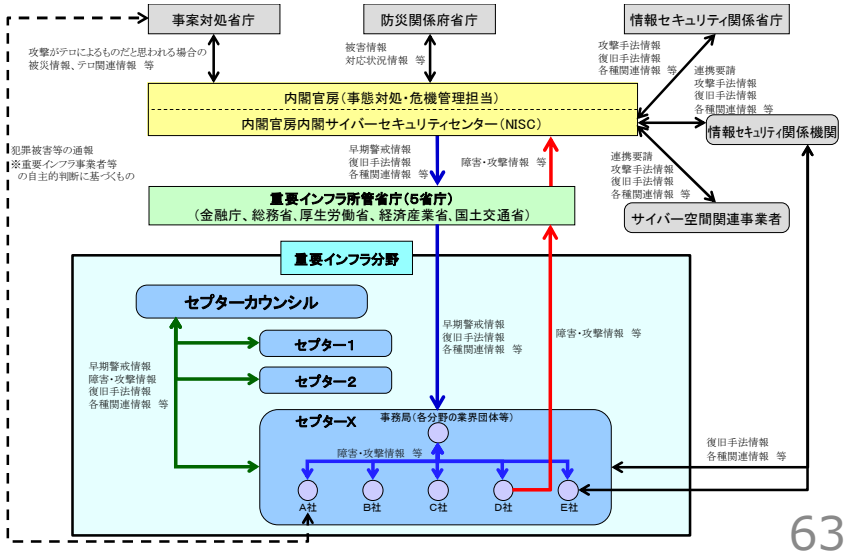
平時

平時の延長線上の体制

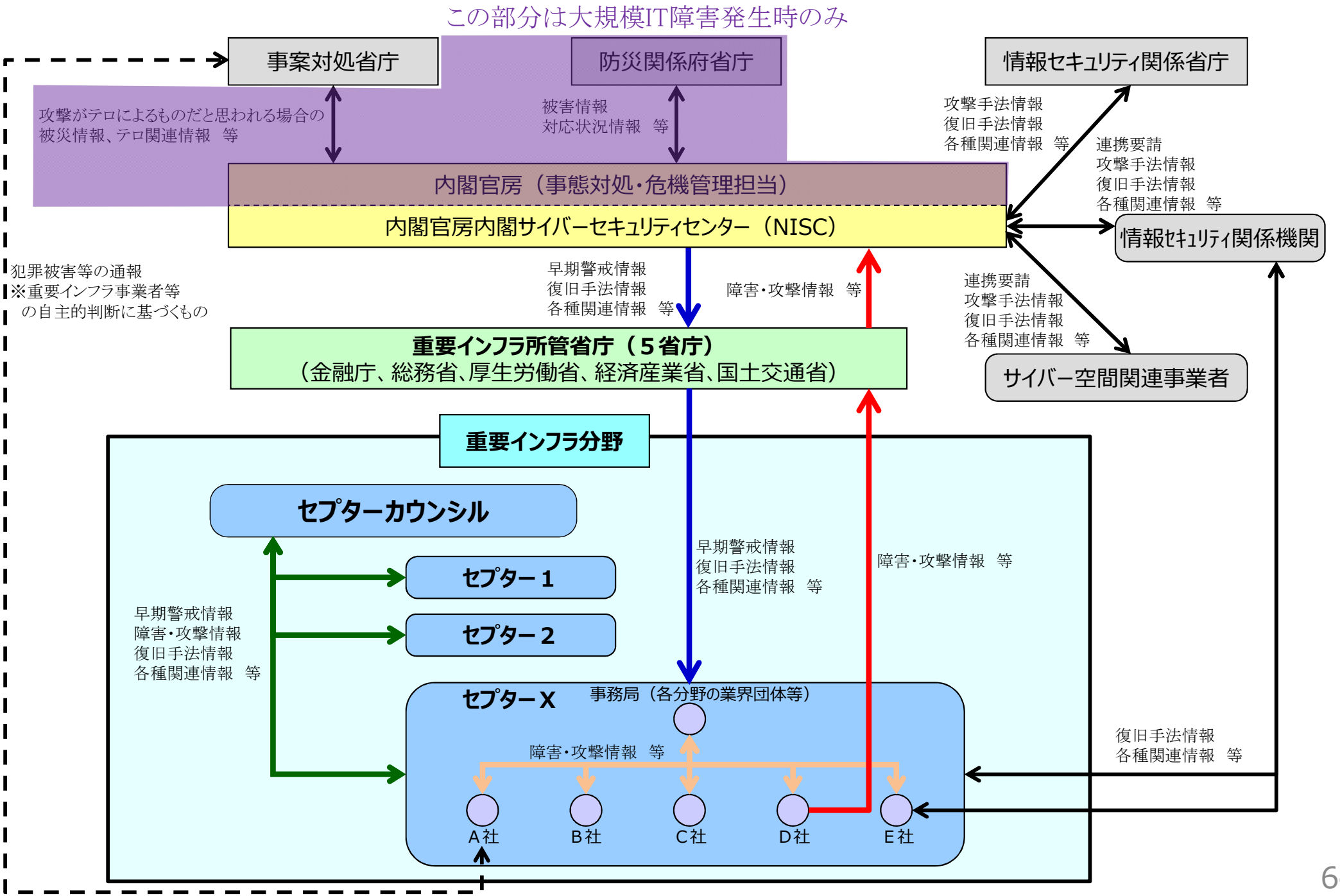
大規模IT障害発生時



円滑な移行



（参考）情報共有体制


この部分は大規模IT障害発生時のみ
事案対処省庁
防災関係府省庁
攻撃がテロによるものだと思われる場合の
被災情報、テロ関連情報　等
被害情報
対応状況情報　等
内閣官房（事態対処・危機管理担当）
内閣官房内閣サイバーセキュリティセンター（NISC）
情報セキュリティ関係省庁
攻撃手法情報
復旧手法情報
各種関連情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
情報セキュリティ関係機関
犯罪被害等の通報
※重要インフラ事業者等
の自主的判断に基づくもの
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
サイバー空間関連事業者
重要インフラ所管省庁（５省庁）
（金融庁、総務省、厚生労働省、経済産業省、国土交通省）
重要インフラ分野
セプターカウンシル
セプター１
セプター２
早期警戒情報
障害・攻撃情報
復旧手法情報
各種関連情報　等
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報　等
セプターX
事務局（各分野の業界団体等）
障害・攻撃情報　等
A社
B社
C社
D社
E社
復旧手法情報
各種関連情報　等

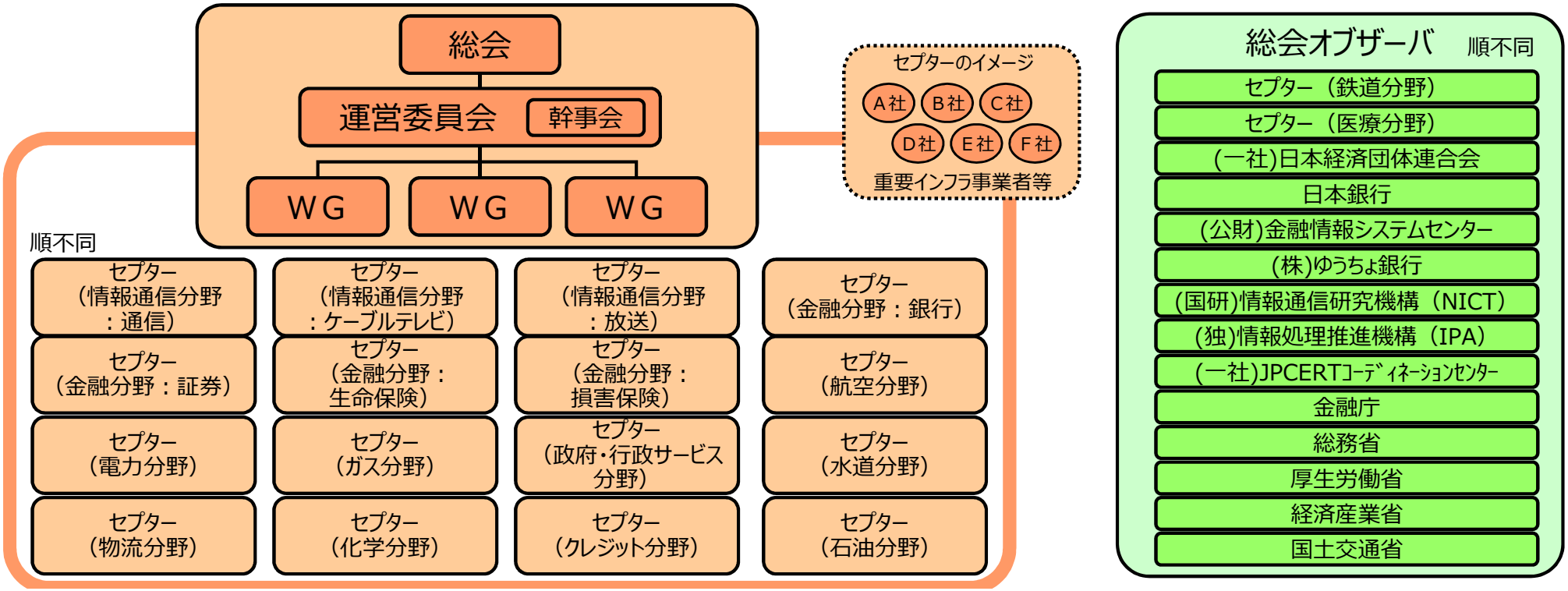
（参考）セプターとセプターカウンシル

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。



（参考）セプター特性把握マップ

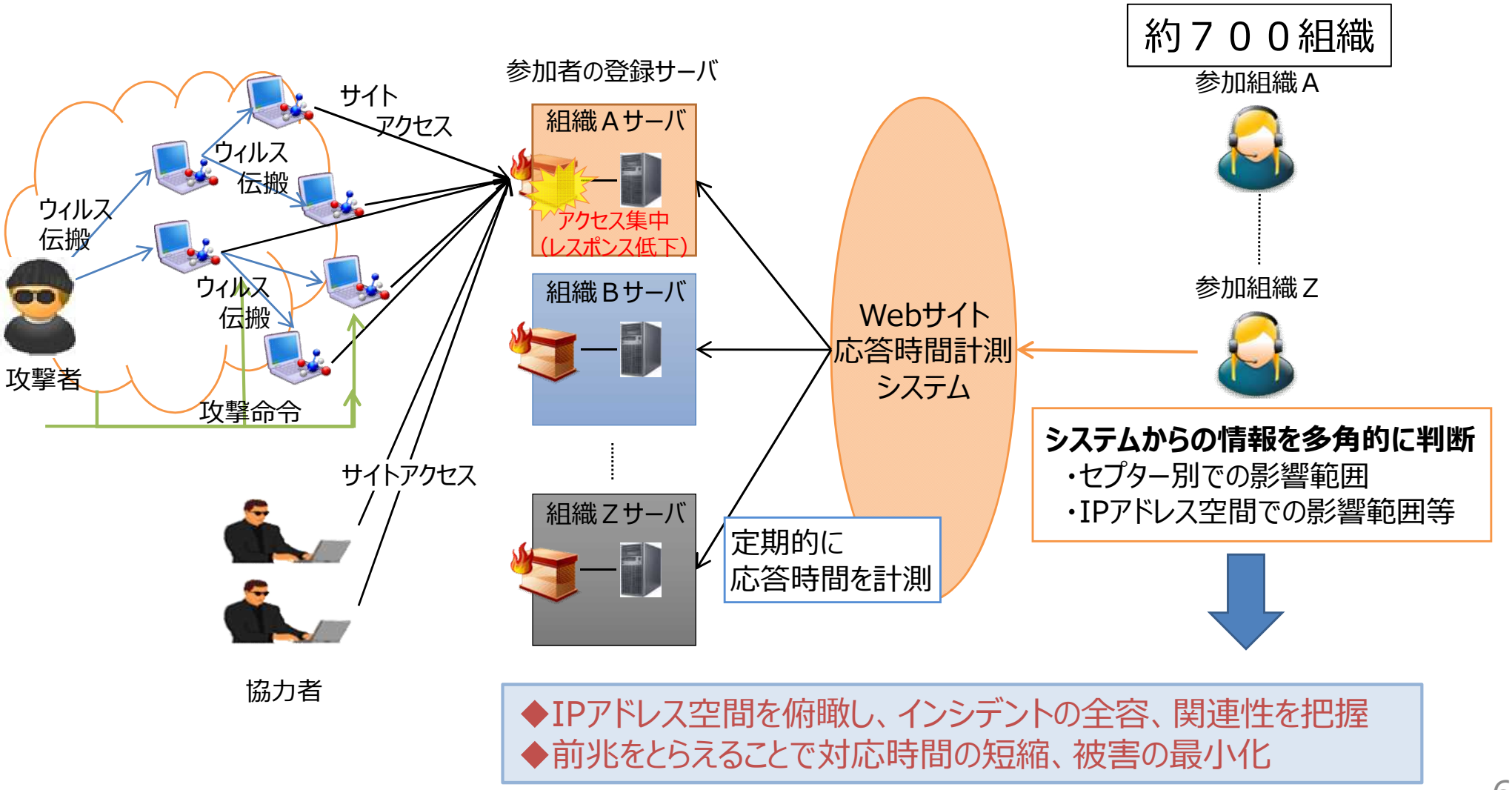
2016年9月末日現在

重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会				航空分野におけるCEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR											
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務・決裁システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 ＩＴ推進部品質グループ	定期航空協会	(一財)日本鉄道電気技術協会	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（内訳）	24社・団体 （固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等）	332社 ((一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	194社 1団体 （日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟）	1,433社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	260社 7機関 （金融商品取引業者、取引所等証券関係機関）	41社 ((一社)生命保険協会の定款に定める社員および特別会員）	29社 （オブザーバ3社含む） ((一社)日本損害保険協会 情報システム委員会参加会社）	14社 1団体 （航空運送事業者、定期航空協会）	22社 1団体 （鉄道事業者22社、1団体）	12社 2機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	10社 （主要な一般ガス事業者10社）	47 都道府県 1,741 市区町村	1グループ 6機関 （医療機関、(公社)日本医師会、四病院団体協議会((一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会）、保健医療福祉情報システム工業会）	8水道事業体 （会員水道事業体のうち会長都市並びに地方支部長都市） [補足]障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,361事業体)へ情報を提供	6団体 16社 （日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社）	13社 （主要な石油化学事業者）	27社 （主要なクレジットカード会社等）	14社 ・グループ （主要な石油精製・元売会社）
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年４月制定	2014年１２月制定
連絡手段	メール	メール 電話	メール 電話	メール WEB	メール WEB	メール 電話 FAX 携帯電話 WEB	メール WEB	メール	メール	メール 携帯電話	メール	メール	メール 電話 FAX	メール 電話 FAX 携帯電話 衛星電話	メール 電話 FAX 携帯電話	メール 電話 携帯電話 FAX	メール	メール 電話

（注）　本マップは、各セプターの自主的な整備状況を把握し、マップとして取り纏めたもの。

（参考）Webサイト応答時間計測システム

重要インフラ事業者が登録するＷｅｂサイトの応答時間を定期的に計測することで、サイトの動作状況を統計的に監視し、動作異常や外部からの大量のトラフィック等を検知し、複数の観測を複合的に見ることで、異常の早期発見・事実の確認、原因推測をより正確に行い、重要インフラサービス等の被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組み

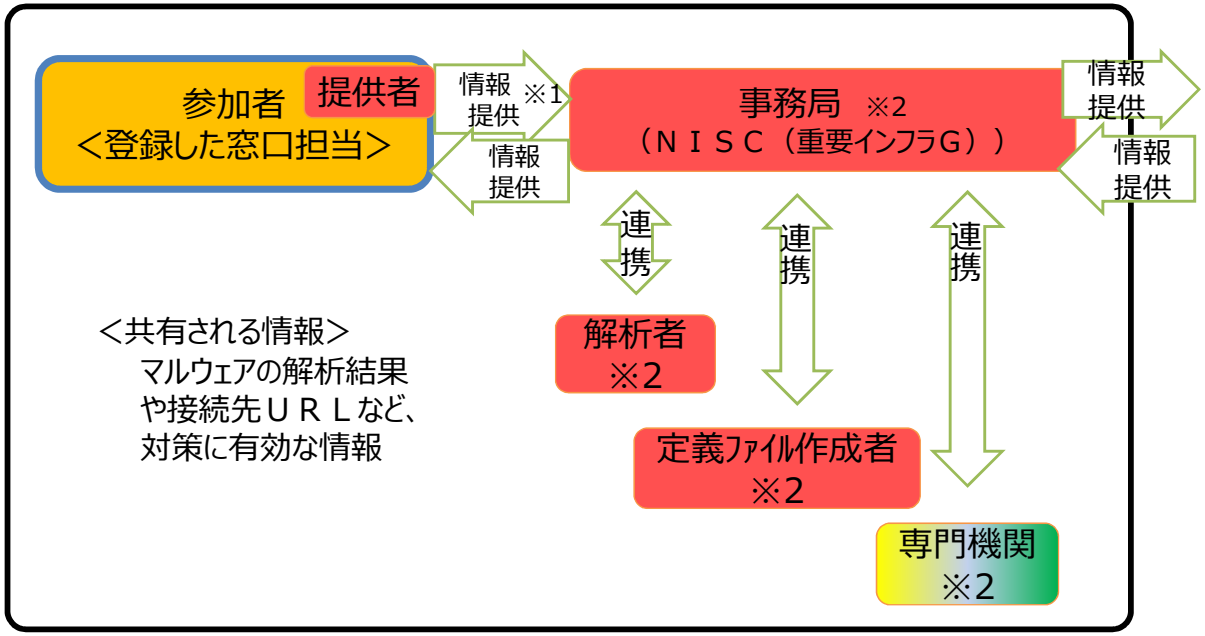


（参考）標的型攻撃に関する情報共有体制（C⁴TAP）

C⁴TAP: **C**eptoar **C**ouncils **C**apability for **C**yber **T**argeted **A**ttack **P**rotection

重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有することで、より多くの標的型攻撃に関する情報を収集・共有し、重要インフラサービスへの標的型攻撃の未然防止、もしくは被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組み

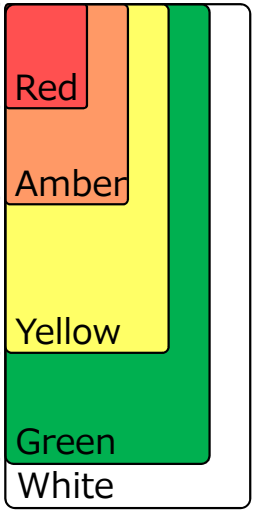
＜情報共有体制図＞



※1　情報を扱う者（参加者、解析者等）は、本体制の運用規程を合意し、登録された者
※2　情報提供者が、上記類型から、情報の種類毎に、情報共有範囲を指定

＜情報共有範囲の類型＞

Red	情報提供者、事務局及び解析者限り
Amber	Red＋参加者（セプターカウンシル構成員）
Yellow	Amber＋規程に合意し遵守することを表明したオブザーバ等
Green	Yellow＋未参加のカウンシル関係者等
White	公開可能



参加者：約３５０組織（運用開始時）

第３次行動計画 施策③：障害対応体制の強化

分野横断的演習の更なる充実に加え、IT障害対応に関する他の演習・訓練との連携・役割分担を行うことで、重要インフラ事業者等のIT障害対応能力を高める。

行動計画期間当初の課題

- 横断的演習の成果の重要インフラ全体への普及・浸透
- IT障害発生時の対応を踏まえた関係主体の在り方
- 重要インフラ所管省庁等による演習・訓練との連携　　等

行動計画期間中の施策

（１）　分野横断的演習の改善

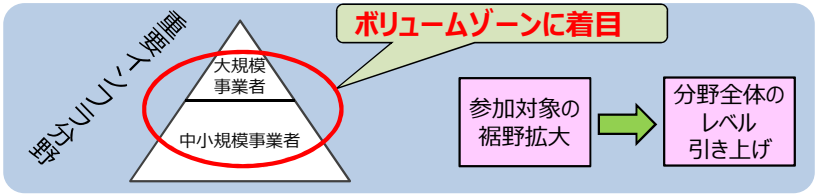
- 他施策等との連携強化による横断的演習自身の改善
  ※他施策で得られた知見、最新動向のシナリオへの反映
  ※演習成果の他施策への反映
- 成果の浸透
- 参加対象の裾野拡大

（２）　関係演習・訓練との連携による相乗効果

- セプター訓練・重要インフラ所管省庁による他演習・訓練と相互に連携・補完

第３次行動計画に基づく取組

分野横断的演習の参加者拡大



ＰＤＣＡによる改善プロセス例

重要インフラ事業者

Plan(準備)	Do(実働)	Check(確認)	Act(是正)
参加個社における IT-BCP等関係規程の整備・見直し	平時における システム運用 平時における 情報連絡・情報提供 規程に基づく 自主訓練等の実施（含、セプター訓練）	参加個社における 規程類・体制の 実効性検証 官民間/民民間の情報 共有体制の実効性検証	分野横断的演習から得た改善点の抽出・分析
○演習から得た改善点に基づくIT-BCP等関係規定の整備・見直し 例：指揮命令系統の明確化 権限委譲、代行順位 広報、利用者への対応　等	○整備・見直しをした関係規定に基づくシステム運用、情報連絡・情報提供、自主訓練等の実施	<規程類・体制の実効性検証> ○IT-BCP本体の実効性検証 ○IT-BCP発動の際の連絡・対応体制等の検証 <官民間/民民間情報共有体制の検証> ○セプター内の体制の検証 ○セプター間の体制の検証	○実効性検証を踏まえた改善点の抽出・分析
演習の事前準備		演習当日	演習後の振返り等

国

Plan(準備)	Do(実働)	Check(確認)	Act(是正)
分野横断的演習の企画 行動計画の 各施策群への反映	セプター訓練 事業者による IT-BCPの見直しの促進 情報共有体制による 情報提供の実施 安全基準等の改善の促進	分野横断的演習の実施 （目的に照らした 各項目のチェック（各施策群）	分野横断的演習から得た改善点の抽出・分析 行動計画の 各施策群における 改善点の抽出・分析（フィードバック）
<演習の企画> ○前回演習から得た改善点を踏まえた今回演習の企画 <各施策群への反映> ○前回演習から得た改善点に基づく情報共有体制の見直し ○前回演習から得た改善点に基づく指針の改訂	<セプター訓練> ○分野横断的演習のベースである官民間の情報伝達体制の機能確認 <IT-BCPの見直しの促進> ○前回演習から得た各事業者のIT-BCPの改善点の見直しの促進 <情報提供> ○見直した情報共有体制による情報提供の実施 <安全基準等の改善の促進> ○改訂した指針を参考にした各分野の安全基準等の改善の促進	<演習の実施> ○演習シナリオに沿う中での、あるべき姿と実態の乖離状況のチェック －障害対応体制 どの程度機能しているのか 何が不足しているのか －情報共有体制 障害対応体制の観点から、何が不足しているのか －指針 障害対応体制の観点から、何が不足しているのか	<演習の改善点> ○今回演習で得た次回演習での改善点の抽出・分析 <フィードバック> ○今回演習で得た情報共有体制の改善点の抽出・分析 ○今回の演習で得た指針の改善点の抽出・分析

（参考）２０１６年度分野横断的演習　開催概要 ～2006年度より実施～

＜事前説明会＞
日　程　：２０１６年１０月２８日（金）、１１月１日（火）、２日（水）
場　所　：東京会場、地方会場（説明会の模様について、演習当日まで動画配信）
内　容　：①重要インフラ防護施策の概要説明（第３次行動計画、情報共有体制）
②分野横断的演習の事前説明
③最新動向等についての有識者講演　等

規程類の事前確認、個別検証課題の確認・調整

＜演習当日＞
日　時　：２０１６年１２月７日（水）１２：１５～１７：００
場　所　：東京会場、地方会場、自職場
参 加 者　：５０５組織２，０８４名（うち、１５３組織３７８名が地方会場、
１０９組織９８９名が自職場より参加。）
【重要インフラ事業者等：１３分野　合計４４６機関】
【セプター：１３分野１８セプター】
【関係機関、分野横断的演習検討会有識者、政府機関　等】


演習の模様


丸川大臣による視察

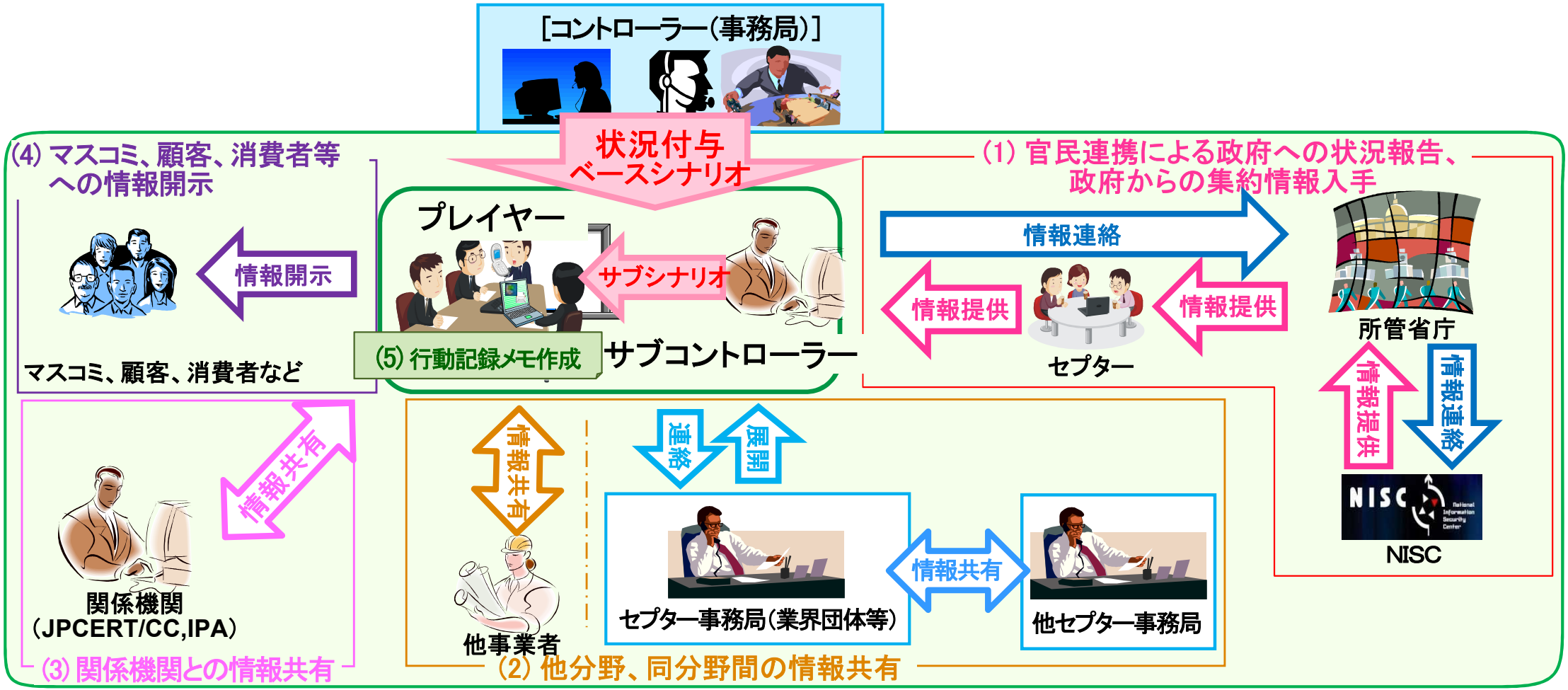
演習内容　：
○第１部　各分野においてサービスへの影響が小さいＩＴ障害が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証。（ランサムウェア）
○第２部　サービスへ影響が生じるＩＴ障害が発生し、事業継続が脅かされる事態を想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。（ＤＤｏＳ攻撃、ＯＳ脆弱性、制御システム）

演習を通じた内規・体制等の課題抽出

＜事後の意見交換会＞
日時（予定）：２０１７年１月２４日（火）１４：００～１７：３０
場　所　：東京会場、大阪会場
内　容　：①分野をまたいだ事業者等間での情報共有（グループディスカッション）
②最新動向等についての有識者講演　等

他事業者等との情報共有を通じた改善の促進

（参考）２０１６年度分野横断的演習　演習の流れ



[プレイヤーの対応内容]

1. コントローラー(事務局)から、演習ツールで状況付与(ベースシナリオ)が投入される。
2. 各プレイヤーは、上記(1)～(5)の各種対応を行い、IT-BCP等に関する検証を行う。
   (1) 官民連携: 所管省庁を介して、NISCへ自社サービス状況や対応内容等の連絡を行う(情報連絡)。 また、NISCから他分野の状況を集約した情報を入手(情報提供)し、自社対応に役立てる。
   (2),(3) 情報共有: セプター事務局(業界団体等)、他事業者、関係機関との情報共有(問合せ、回答、情報交換など)や、連携(応援要請、復旧支援・協調など)を行う。
   (4) 情報開示: マスコミや顧客などへ自社サービスの障害状況、復旧状況・見込みなどを開示する。
   (5) 行動記録: 振り返りを行うため、演習での対応内容(電話連絡、想定される社内対応等も含む)を行動記録メモに記録する。
3. 各プレイヤーは、行動記録メモを基に、検証課題ごとに振り返りの観点を記載した振り返りシートに照らして、自組織内で振り返りを行う。

（参考）２０１６年度分野横断的演習　シナリオ

【第１部】ランサムウェアによる攻撃
情報共有体制、インシデント初動対応を重点とする。
（CSIRTや社内情報共有も意識）

JPCERT/CCによる早期警戒情報

↓

不審メールの受信及びメールの開封報告
外部への不信通信検知

↓

端末に不審な画面が表示され業務支障が起きていることを確認

↓

経営層からCSIRTを中心に社内横断的な情報収集を行うように指示

↓

システム保守ベンダーからの対応提案

↓

NISCからの情報提供

１シナリオ７５分
状況付与は
概ね５分置き

【第２部】ＤＤＯＳ攻撃／ＯＳ脆弱性／制御システム
障害対応体制、内部的な判断、意志決定、インシデントの本格対応を重点とする。（他分野との情報共有も意識）

2-a）
DDOS攻撃による重要インフラサービス障害発生

2-b）
OS等における脆弱性を突いた攻撃による重要インフラサービス障害発生

2-c）
制御システムのマルウェア感染による重要インフラサービス障害発生

↓

IT-BCP等発動等の判断時に発動権限者と連絡が取れない状況の発生

↓

同業他社のサービス障害について速報が報道される

↓

JPCERT/CC 及び IPAからの早期警戒情報

↓

経営層からCSIRTを中心に社内横断的な情報収集を行うように指示

↓

NISCからの情報提供

↓

経営層から自分野・他分野の状況について報告するよう指示

第３次行動計画 施策④：リスクマネジメント

重要インフラ事業者等がその事業目的であるサービスの持続的提供を実現するために実施するリスクマネジメントを支援する。

行動計画期間当初の課題

- 重要インフラ事業者等において、事業目標達成に向け必要なリスクマネジネントの訴求
- 環境変化等に応じて生じ得るリスク源、多大な影響が生じうる環境変化の中長期的な調査

行動計画期間中の施策

（１） リスクマネジメントの標準的な考え方

- リスクマネジメントは自らの状況把握をし、各重要インフラ事業者等がそれぞれにおいて主体的に実施
- 防護基盤強化のため作成する手引書等の利活用
  ※国際標準への準拠を求めるものではなく、自組織のリスクマネジメントの更なる最適化等が目的。

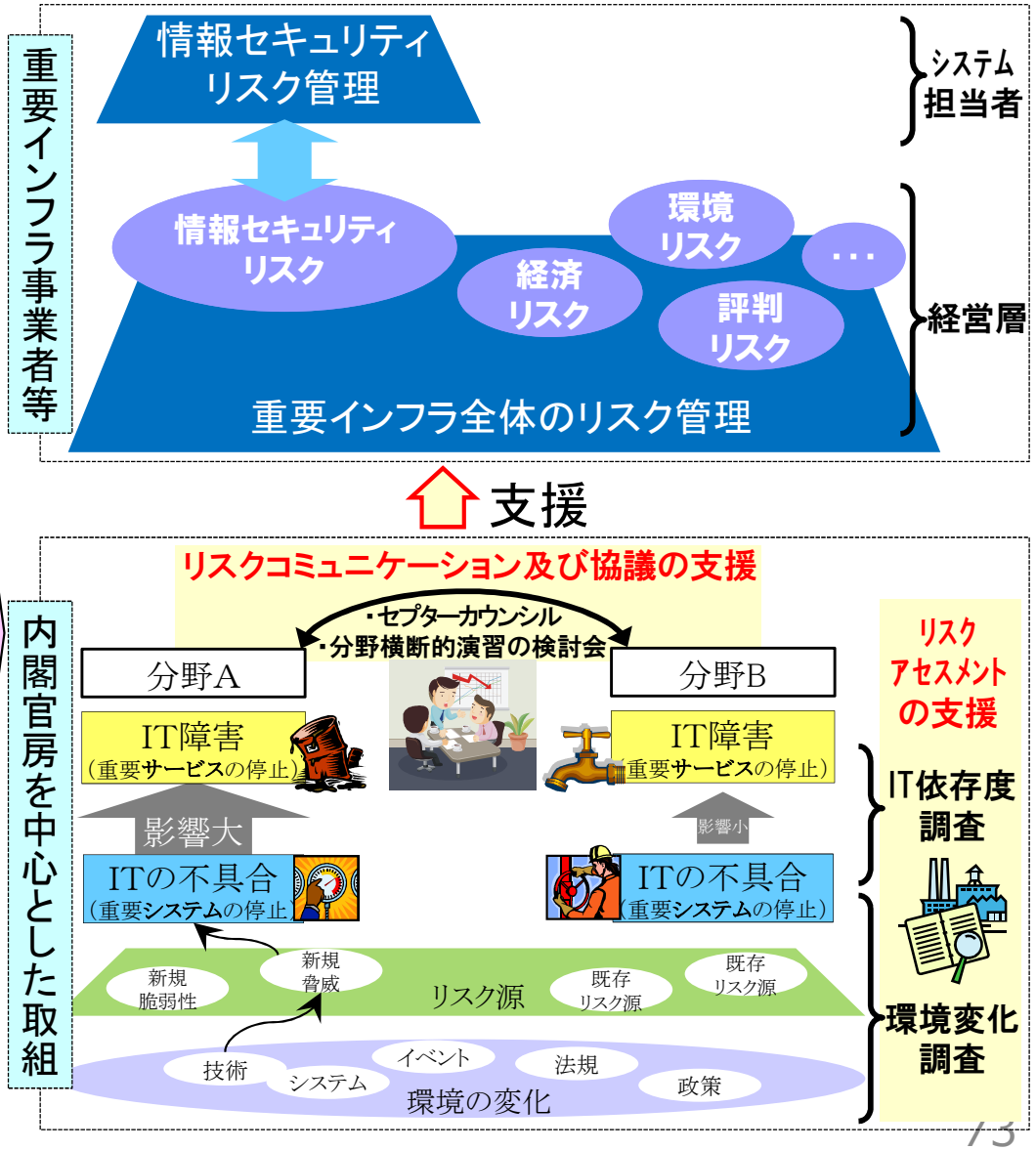
（２） リスクマネジメントの内閣官房による支援

- リスクアセスメントの支援
  - ・環境変化調査
  - ・相互依存性解析（ＩＴ依存度調査含む）
- リスクコミュニケーション及び協議の支援

（３） 他施策との相互反映プロセスの確立

- 環境変化調査、相互依存性解析の結果 ⇒ 他施策
- 他施策で顕在化したリスク等 ⇒ 調査・解析対象

第３次行動計画に基づく取組



リスク評価手順の全体像

コンセプト

○事業者の活動目標を阻害しうる不確かさの影響をリスクと捉える。

○活動目標に照らして守るべき対象を特定し、防ぐべき結果からリスクを特定・分析・評価する。

リスクアセスメントの対象を特定するフェーズ

1 リスクアセスメントの目的の確認

事業者の活動目標を設定し、事業者のリスク評価の目的を確認する。

2 重要サービスの特定

事業者の活動目的を踏まえ、重要なサービスを特定する。

3 重要サービスの影響分析

重要サービスについて、最低限許容されるサービスの範囲・水準を分析し、サービスが阻害された際の影響を分析する。

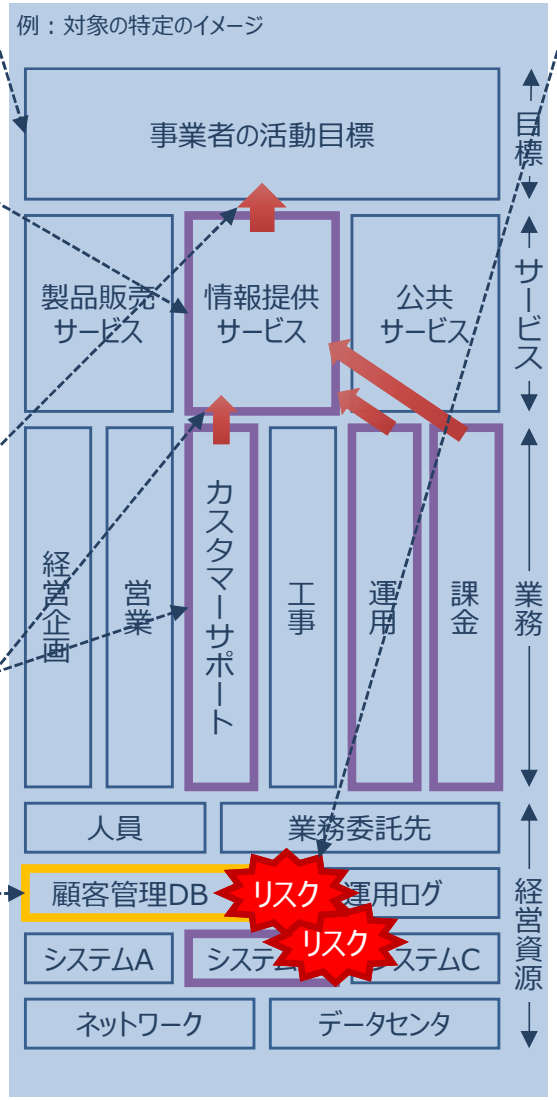
4 重要サービスを支える業務の特定及び当該業務の影響度分析

重要サービスの提供に必要な業務を洗い出し、当該業務について、最低限許容される水準を分析し、業務が阻害された際の影響を分析する。

5 業務を支える経営資源の特定

重要サービスの提供に必要な業務について、事態発生時に最低限満たすべき業務水準を維持するために必要な経営資源を特定する。

例：対象の特定のイメージ



リスクアセスメントを実施するフェーズ

6 リスクアセスメント及びリスク対応方針の決定

リスクの特定

業務を維持するために必要な経営資源について、業務の阻害につながる結果、それ生じる事象、事象を引き起こす原因（リスク源）を特定する。

リスクの分析

業務の阻害につながる結果が重要サービスの提供に必要な業務に与える影響の度合い、業務を阻害する結果を生じる事象の発生頻度等について分析する。

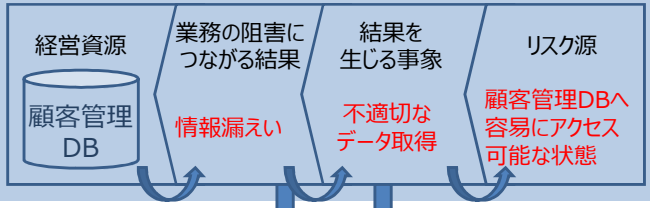
リスクの評価

リスクの分析結果（影響度、予想発生頻度等）を勘案し、当該リスクへの対応の要否を決定する。

リスク対応方針の選定

リスク対応を実施するうえでの対応方針（低減・回避・移転・保有）を選定する。

例：顧客管理DBを経営資源とした際の作業イメージ



例：分析に用いる基準の例

影響度	
5	業務の復旧が不能
4	MTPD内の復旧が困難
3	MTPD内の復旧が可能
2	業務に軽度な影響
1	業務への影響なし

発生頻度	
5	頻発
4	1年に一回程度発生
3	数年に一回程度発生
2	10年に一回程度発生
1	50年に一回程度発生

例：リスクマップを用いた評価の例

※右記はリスクマップを用い、影響度と発生頻度を掛け合わせた値から判定する例。具体的な方法は基準及び判定方法は組織の状況に応じて選択が必要

影響度＼発生頻度	5	4	3	2	1
5	25	20	15	10	5
4	20	16	12	8	4
3	15	12	9	6	3
2	10	8	6	4	2
1	5	4	3	2	1

例：リスク対応方針の選定の例

	対策方針※1	具体的な対策の例※2
	低減※3	顧客管理DBの運用ルールを見直す
	回避	顧客管理DBを用いない
	移転	顧客管理DBの運用を外部に委託する
	保有	リスクを関係主体で認識する

※1 検知・回復については具体的な対策を検討する際に考慮する
※2 具体的な対策の検討は本手順には含まれない
※3 対策実施しリスクを許容できるレベルまで低減することを指す

第３次行動計画 施策⑤：防護基盤の強化

広報公聴、国際連携、関係規程類、国際基準等の手引書作成等、重要インフラ防護の全体を支える共通基盤的な取組を強化する。

行動計画期間当初の課題

- 広報公聴の一層の充実
- 二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携の強化
- 参照すべき規程類の整備・活用　　等

行動計画期間中の施策

（１）　広報公聴
- 行動計画及びその取組について、広く認識・理解を得るための公報広聴活動の充実

（２）　国際連携
- 欧米、ＡＳＥＡＮ、Meridian等二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携

（３）　規程類の整備
- 重要インフラ防護に係る関連規程集の発行
- 国際基準等の適用の際の手引書等の整備
- 情報セキュリティに関する評価・認証制度の拡充の支援

第３次行動計画に基づく取組

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

共通基盤の強化

知見と成果の反映

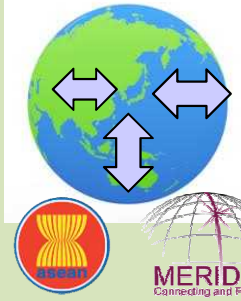
防護基盤の強化

広報公聴

Web等による広報

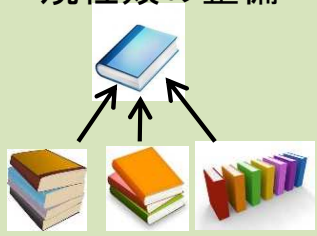
講演

国際連携



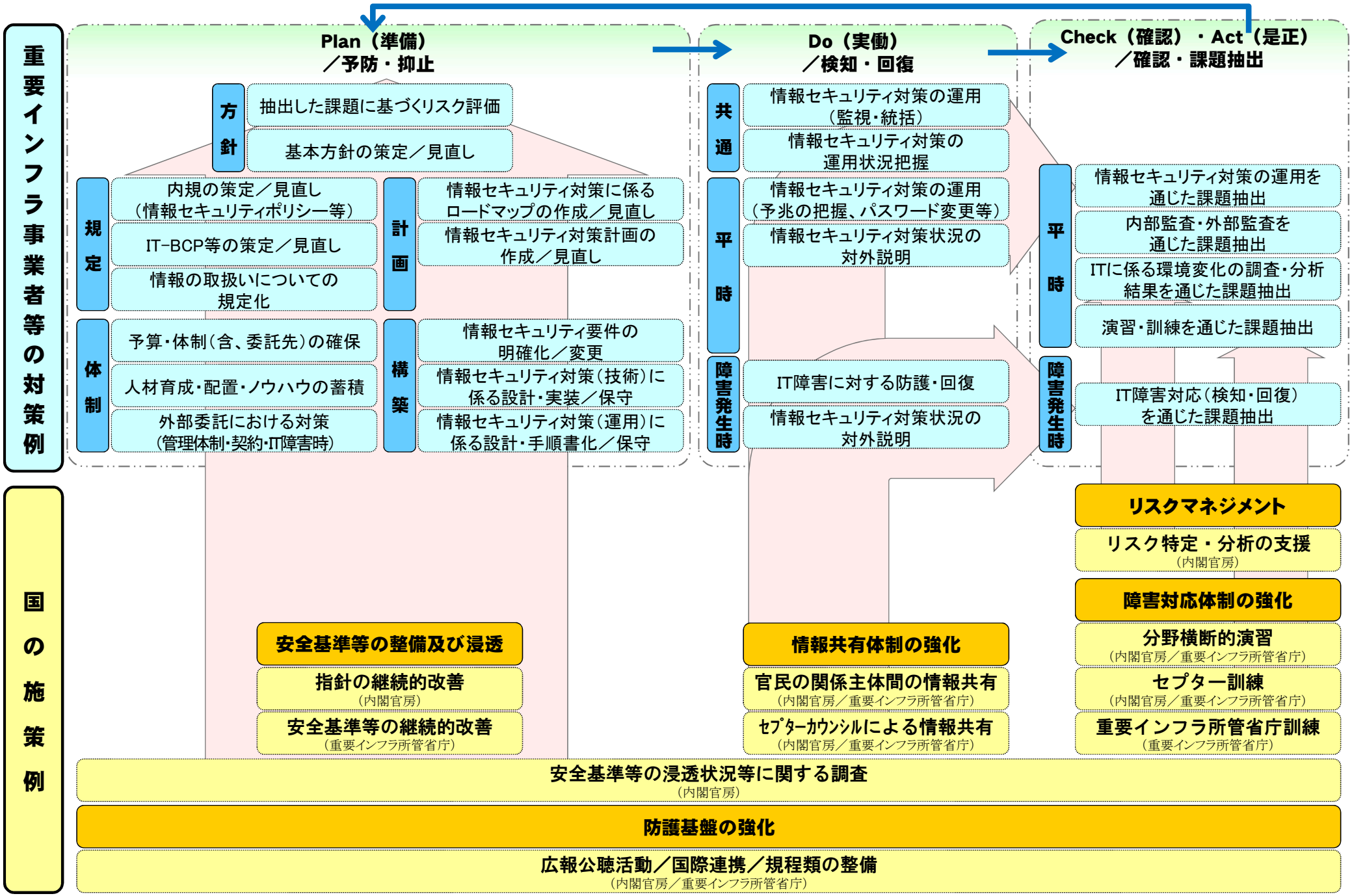
二国間、地域間
多国間の連携

規程類の整備



関連規程類を俯瞰可能な手引書

「重要インフラ事業者等による対策例」と各対策に関連する「国の施策例」



第3次行動計画の見直しのポイント

１．行動計画の目的

重要インフラサービスは、安全かつ持続的に提供（機能保証）することが求められることから、自然災害やサイバー攻撃等に起因するＩＴ障害とそれによるサービス障害の発生を可能な限り減らすとともに、発生時の迅速な復旧が可能となるよう、関係主体において経営層の積極的な関与の下、情報セキュリティに関する取組を推進する。また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図っていく。

２．重要インフラを取り巻く現状と課題

◆ 行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ サービスの安全かつ持続的な提供のため、情報系(ＩＴ)だけではなく、制御系(ＯＴ)を含めた情報共有の質・量の改善等が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

「**IT障害**」については、制御系（OT）に起因した障害も含むことを明確化するため、「**重要インフラサービス障害**」とする方向で検討中

３．行動計画の見直しの３つの重点

次の3つを重点として行動計画に基づく5つの施策群の取組の深化を図る。

①　先導的取組の推進(クラス分け)

重要インフラ分野が依存し、短時間のＩＴ障害でも影響が大きくなるおそれがある分野(例：電力、通信、金融)において、一部事業者による先導的な取組を進めるとともに、他の事業者、さらには他の分野にも波及させることにより、重要インフラ全体の機能保証の確保を図る。

②　オリパラ大会を見据えた情報共有体制の強化

連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大等により、情報共有を促進するとともに、重要インフラ内外の共有範囲の拡充、制御系を意識した情報共有等を図る。また、演習等の継続・改善等により、障害対応体制の強化を図る。

③　リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスの安全・継続的な提供のため、重要インフラ事業者等へのリスクマネジメントの更なる浸透や、CSIRTやコンティンジェンシープランの整備等を含む対処態勢の整備の推進図る。

行動計画に基づく５つの施策群

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

４．行動計画の見直しに向けた今後のスケジュール

➢　平成28年中に行動計画の見直し（案）を策定・公表、平成29年3月までに結論を得る。

①重要インフラ事業者の先導的取組の推進（相互依存性等を踏まえたクラス分け）

重要インフラ事業者の情報セキュリティ対策における先導的取組を推進するとともに、重要インフラ事業者以外の事業者についても情報セキュリティ対策レベルの向上を図る。

重要インフラ事業者

先導的取組を行う事業者

電力分野
- 一般送配電事業者　等

情報通信分野
- 主要電気通信事業者　等

金融分野
- 主要都市銀行　等

✓ 他の重要インフラ事業者からの依存が大きい
✓ 比較的短時間のIT障害であってもその影響が大きい

その他の事業者

電力分野
- 左記以外の電気事業者

情報通信分野
- 左記以外の情報通信事業者

金融分野
- 左記以外の金融機関

- 他の重要インフラ分野の事業者

依存関係

重要インフラ事業者以外

- 重要インフラ事業者の主要関係先や外部委託先
- 先端技術等の知的財産や営業秘密を保持する企業、研究機関、大学等
- 安全保障上重要な企業

◆ 行動計画に基づく取組

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

◆ 個々の事業者において情報セキュリティ対策を実施

今後の取組

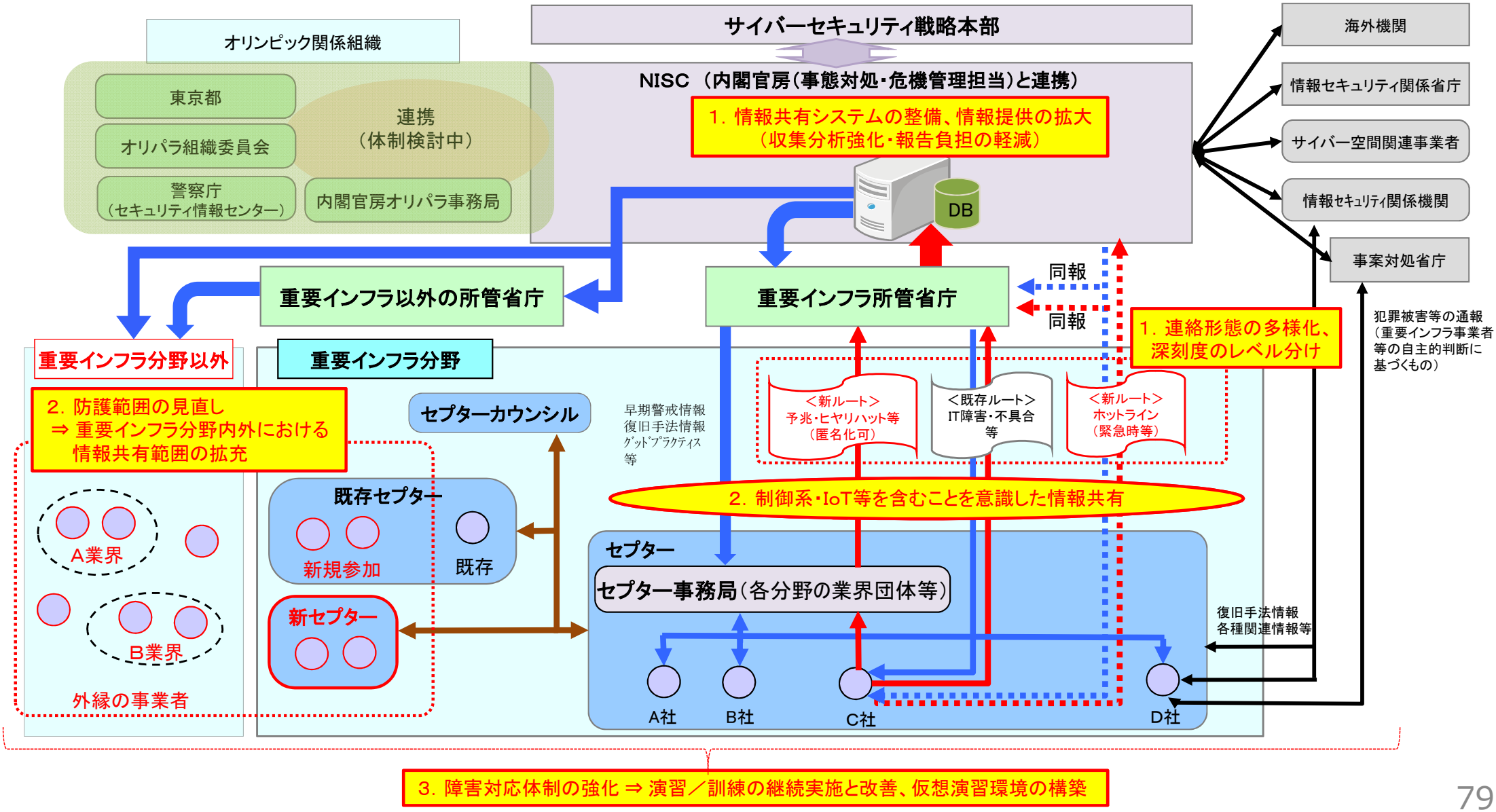
➢ 先導的取組の実施(例)
- ◆ISACの設立・加盟
- ◆侵入テストの実施
- ◆リスクマネジメントの重点化
- ◆NISCとのホットライン構築
- ◆浸透状況調査結果を踏まえた対策の深化

➢ 先導的取組を実施していくための体制づくり

➢ NISC又は所管省庁からの情報提供を開始
➢ NISC又は所管省庁への情報連絡、その他の情報セキュリティに係る取組について、組織内の体制が確実なものとなった後に開始

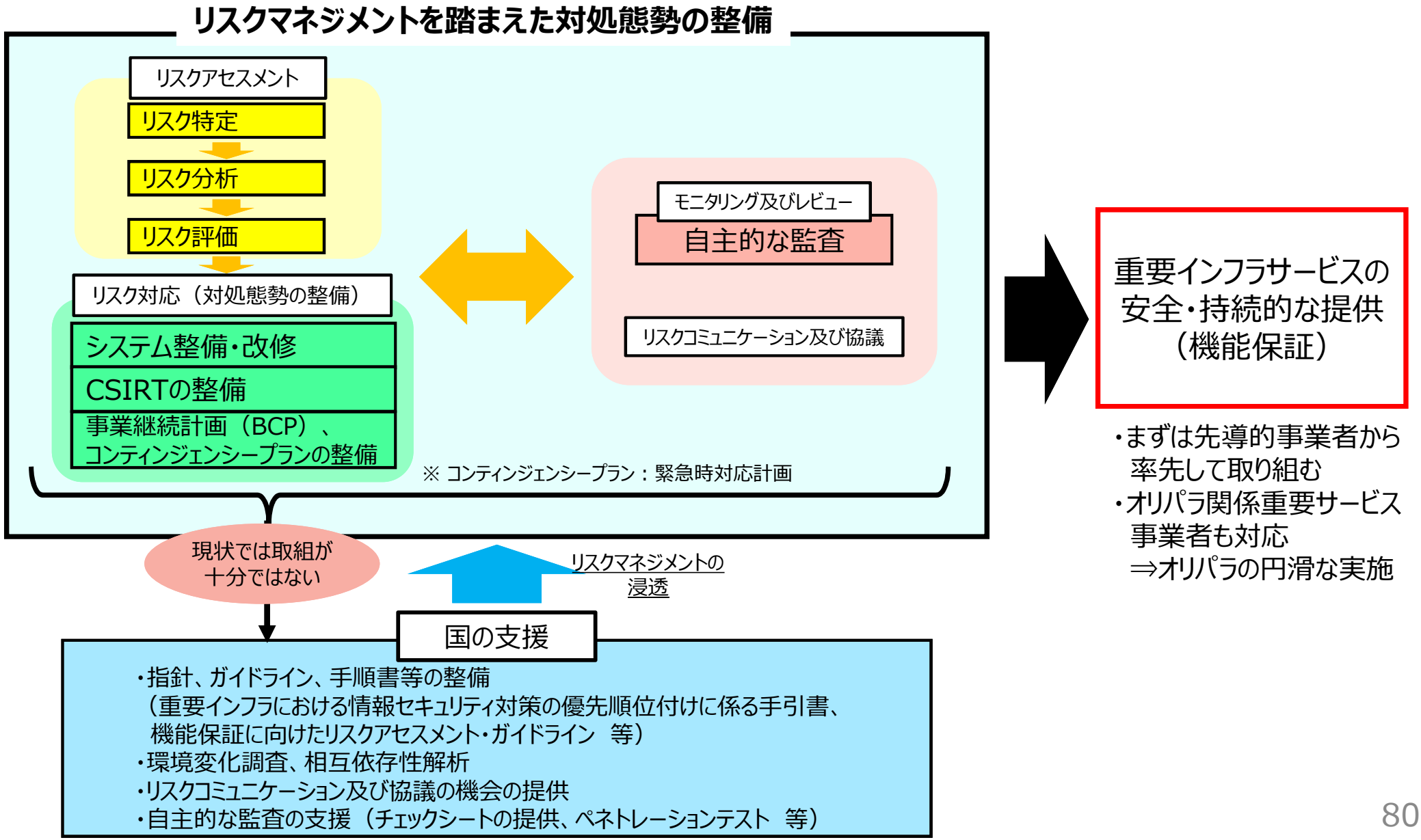
②オリパラ大会を見据えた情報共有体制の強化

1．情報共有の更なる促進 ⇒ 連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大
2．防護範囲の見直し　　⇒ 重要インフラ分野内外における情報共有範囲の拡充、制御系・ＩｏＴ等を含むことを意識した情報共有
3．障害対応体制の強化　⇒ 演習／訓練の継続実施と改善、仮想演習環境の構築



③リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスを安全・持続的に提供できるよう、重要インフラ事業者等によるリスクマネジメントを踏まえた対処態勢整備を推進する。



④第３次行動計画の施策群の主な見直し事項

第3次行動計画の目標（理想とする将来像）と評価

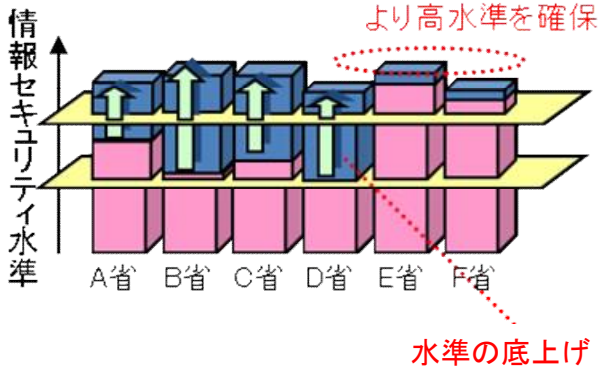
- ◆ 重要インフラ事業者等が自主的に見直しの必要性を判断し改善を図るサイクルが浸透しつつあるが、ＰＤＣＡのうちＣＡについてはいまだ十分とは言えない状況。
- ◆ 官民、民民間の情報共有が着実に進展。演習等により防護能力が向上。脅威の深刻化を踏まえ、情報共有の質・量の改善、ＩＴ障害対応経験等を将来に活かす取組が必要。
- ◆ 国民への取組内容の発信を実施。しかし、国民の不安感はぬぐい切れていない。引き続き、国内外の多様な主体との連携、情報収集・分析、国民への適切な発信の継続が必要。
- ◆ 2000年以降、行動計画として策定・公表、定期的な評価・見直しが行われている。これに基づく継続的取組により対策が着実に進展。同計画の基本的枠組みの維持が妥当。
- ◆ 重要インフラ防護の目的に照らし、機能保証の観点から取組を進めることが重要。また、一部で先導的な取組も進められており、これを適宜展開していく。

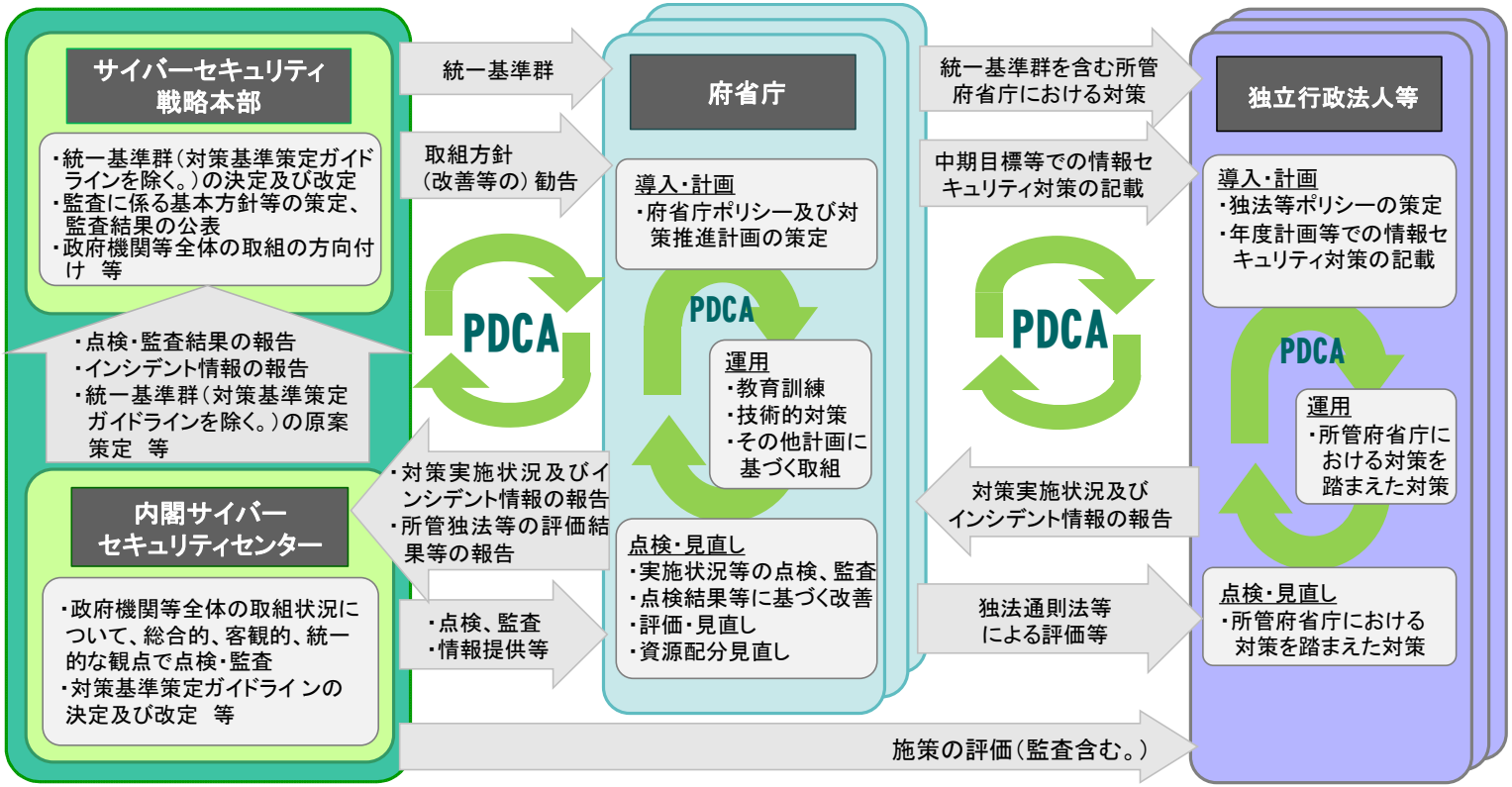
第３次行動計画の施策群	見直しの方向性（案）	具体化に向け検討すべき事項
①安全基準等の整備及び浸透	○経営層に期待される認識・行動、内部統制の強化、ＯＴを視野に入れた人材育成等について追記し、指針を充実 ○情報セキュリティへの取組を業法における保安規制に位置づける等、制度的な枠組みの検討・整備 ○安全基準等の浸透状況調査を通じた重要インフラ事業者の情報セキュリティ対策レベルの底上げ	○経営層に期待される認識・行動を受けた重要インフラ事業者による内規見直しの進め方 ○現状の制度的枠組みの再確認、課題整理
②情報共有体制の強化	○情報共有の更なる促進 ・連絡形態の多様化（セプター事務局経由の省庁報告ルート（匿名化）） ・事案の深刻度のレベル分け ・迅速な共有プラットフォーム整備（ホットライン含む） ・制御系・ＩｏＴ等を含むことを意識した情報共有 ・情報提供の拡大　等	○その他の情報共有の促進方策
③障害対応体制の強化	○重要インフラ事業者の実用性を重視した分野横断的演習及びセプター訓練の継続実施・改善	○重要インフラ事業者等が検証できるような仮想演習環境の構築
④リスクマネジメント	○施策のスコープを拡大し、機能保証の観点から、リスクアセスメント結果を踏まえた対処態勢の整備支援に係る取組（オリパラも見据えた取組を含む。）を追加	○リスクアセスメント結果を適切に経営意思決定に反映させるための内部統制の強化（自主的な監査の強化等）に対する支援の在り方
⑤防護基盤の強化	○重要インフラ分野内外の情報共有等を行う範囲の見直し ○情報セキュリティ対策への経営層の関与の推進 ○国際会議等で得た情報の関係主体への積極的な提供 ○人材育成の支援（IT、OT両方に対応できるハイブリッド人材を含む。）	○拡充を図る重要インフラ分野内外の情報共有先（外縁等）

- **政府機関、国民への対応**
  - 政府自身のセキュリティへの取組
  - 国民全体への取組
  - 2020年に向けた取組

政府機関等の情報セキュリティ対策のための統一基準群

- 政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）は、政府機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組み。
- 統一基準群では、府省庁及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
- 統一基準群の運用により、個々の組織のPDCAサイクルや政府機関等全体のPDCAサイクルを適切に回し、政府機関等全体としての情報セキュリティを確保する。

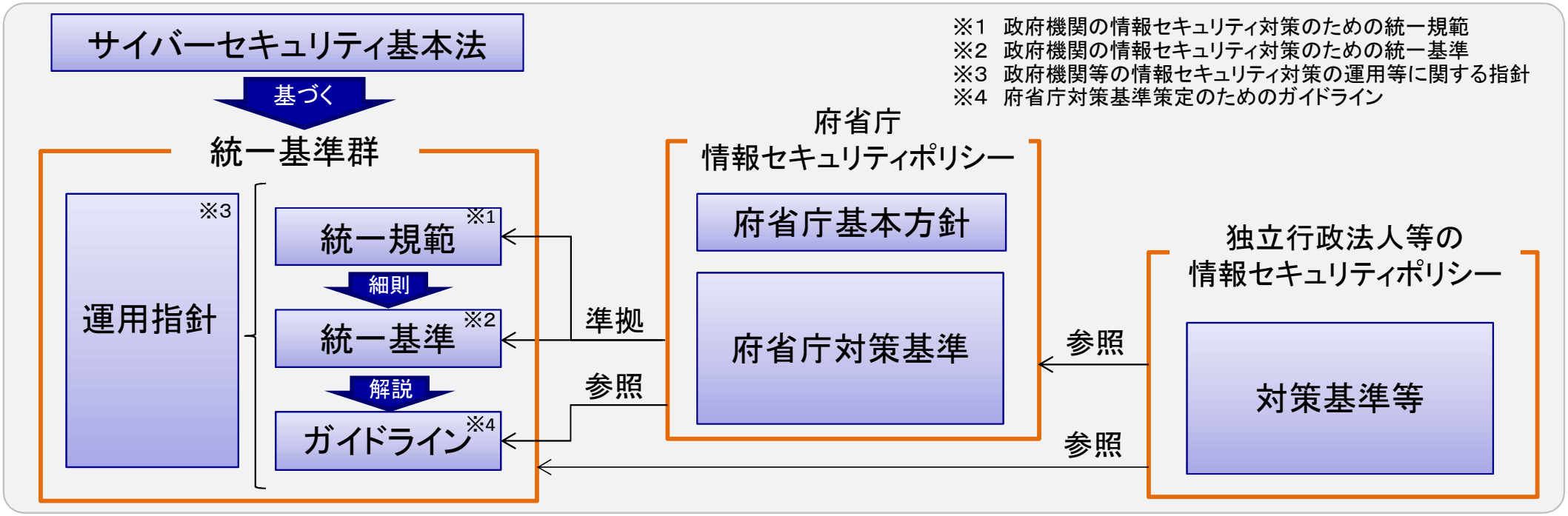




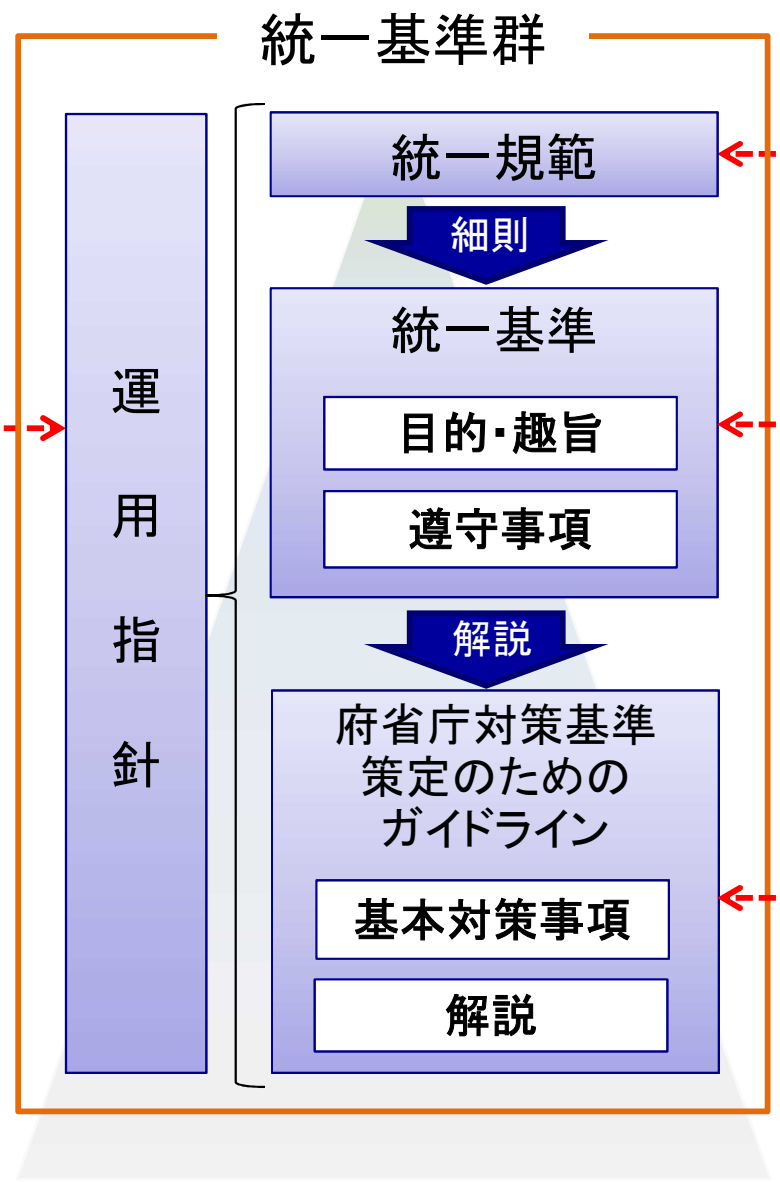
統一基準群と各府省庁・各法人の情報セキュリティポリシーの関係

- 平成28年度版の改定により、統一基準群を、サイバーセキュリティ基本法に基づく政府機関及び独立行政法人等におけるサイバーセキュリティに関する対策の基準と位置づける。
- 府省庁は、統一規範及びその細則である統一基準に準拠するとともに、ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて各府省庁のポリシーを策定する。
- 独立行政法人等は、運用指針に基づき、府省庁のポリシーを踏まえて、組織及び取り扱う情報の特性等を踏まえた独法等ポリシーを策定する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。



統一基準群の構成（平成28年度版）



政府機関等の情報セキュリティ対策の運用等に関する指針

政府機関及び独立行政法人等の情報セキュリティ対策の策定の考え方や、その運用方法等について定めたもの

政府機関の情報セキュリティ対策のための統一規範

政府機関の取るべき対策の統一的な枠組みを定めたもの

政府機関の情報セキュリティ対策のための統一基準

各府省庁が情報セキュリティ確保のために採るべき対策及びその水準をさらに高めるための対策の基準を定めたもの

府省庁対策基準策定のためのガイドライン

統一基準に準拠して府省庁対策基準を策定する際に参照可能な基本対策事項を定めたもの
併せて、府省庁対策基準の策定手順や統一基準の遵守事項を満たすために採られるべき基本的な対策事項の例示、考え方等を解説

サイバーセキュリティ対策を強化するための監査に係る基本方針

1　監査の目的

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、対策強化のための自律的かつ継続的な改善機構であるＰＤＣＡサイクルが継続的かつ有効に機能するよう助言し、対策の効果的な強化を図る。

2　監査の対象

国の行政機関、独立行政法人及び指定法人※

3　監査の基本的な方向性

(1) 助言型監査
- 有益な助言を行う。
- グッドプラクティスを共有。

(2) 第三者的視点からの監査
- 内部監査とは独立した監査を実施。

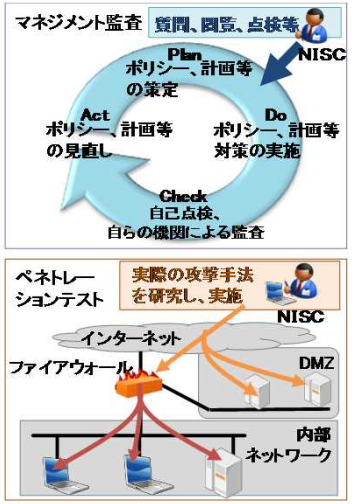
(3) 各機関の状況を踏まえた監査
- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定
- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

4　監査の実施内容

(1) マネジメント監査
- 国際規格において基本的な考え方である組織全体としてのＰＤＣＡサイクルが有効に機能しているかとの観点から検証する。
- 対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。

(2) ペネトレーションテスト
- 疑似的な攻撃を実施することによって、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。



5　監査の進め方

(1) 監査方針の策定
- 年度ごとの監査の基本的な考え方を含む年度監査方針を、年次計画の一部として策定。

(2) 監査の実施
- 必要に応じて外部専門家が協力。
- 過年度の監査実施結果のうち重要な事項については、改善状況を継続的にフォローアップ。

(3) 個別の監査実施結果の通知
- 監査実施結果を、各機関の最高情報セキュリティ責任者（ＣＩＳＯ）へ通知。
- 各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は計画を報告。

(4) 監査実施結果の取りまとめ・報告
- サイバーセキュリティの特性を踏まえ、攻撃者を利することのないよう配慮しつつ、当該年度に実施した監査の結果を取りまとめ。
- サイバーセキュリティ戦略本部に報告。

※サイバーセキュリティ基本法第13条に基づき、サイバーセキュリティ戦略本部が指定する法人

政府機関等における体制

政府機関・情報セキュリティ横断監視・即応調整チーム（GSOC）

2007年度　GSOCの整備を開始
2008年度　整備完了、本格運用を開始
2009年度　本格運用

リアルタイム横断的監視（24時間対応）
分析力の向上

警告・助言
的確・迅速な情報共有による各府省庁の対応力向上

不正プログラムの分析・各種脅威情報の収集

監視

相互連携

相互連携体制

検知情報等の提供

発生事案等の報告

各府省庁　組織内CSIRT
CYMAT要員
ＧＳＯＣ担当　等

2013年３月　整備完了

各組織において情報セキュリティに関する障害・事故等が発生した際、被害拡大防止や早期復旧等を円滑に行うための体制

①インシデント情報の集約・分析、緊急対処の方針決定・指示
②責任者等への報告・連絡
③要員等への教育・訓練
④関係機関等との情報連携

ＧＳＯＣセンサー
PoC
A省 CSIRT

CSIRT間の連携

ＧＳＯＣセンサー
PoC
C省 CSIRT

対処

ＧＳＯＣセンサー
PoC
B省 CSIRT

情報セキュリティ緊急支援チーム（ＣＹＭＡＴ）
2012年６月29日　設置

技術的な支援・助言

要員：各府省庁から派遣される情報セキュリティに関する技能・知見を有する職員で構成
活動事象：サイバー攻撃等により支援対象機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象

①発生事象の正確な把握
②被害拡大防止、復旧、再発防止のための技術的な支援及び助言
③対処能力の向上に向けた平時の取組（研修、訓練等の実施）

支援

情報連携の結節点

NISC

連携・情報交換

民間CSIRT 等

オリンピック・パラリンピックにおけるサイバーセキュリティの重要性について

サイバーセキュリティの現状

ＩＴ依存度の高まり

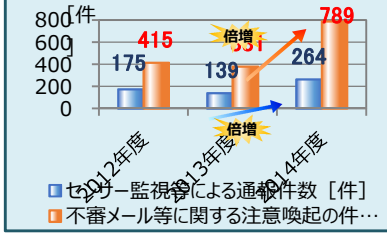
ＰＣ　多くの職場・家庭に普及インターネットに接続

スマホ　携帯電話の50%以上がスマホに置き換わり

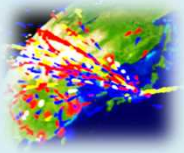
ｽﾏｰﾄｶｰ　１台に100個以上のコンピュータを搭載

ｽﾏｰﾄﾒｰﾀｰ　2020年までに2700万台が普及（東電管内）

標的型攻撃の脅威の深刻化



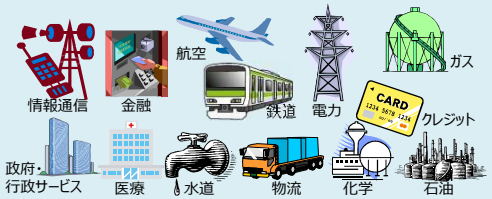
以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、標的型メールによる脅威が一層深刻化。



日本に向けたサイバー攻撃は世界中から飛来

重要インフラに対する脅威の深刻化

- 金融・交通・情報通信など重要インフラへのサイバー攻撃も増加
- オリンピック・パラリンピックの運営に重要インフラの防護が必要



東京大会における要検討事項

- サイバー攻撃は近年急激に増加し、対象が重要インフラ全体にも拡大
- 大会期間中に障害が発生すれば、日本の威信が損なわれる懸念
- ロンドン大会の経験を踏まえ、物理（テロ）面とともに、サイバー面からも、十分な準備期間をかけた慎重な対策が必要
- 新たな施設整備に当たっては当初からサイバーセキュリティの考慮が必要

ロンドン大会でのサイバーセキュリティとサイバー攻撃

＜構築システム＞

- 約47億回のホームページ閲覧、約１億回のオンライン動画リクエスト数に耐えうるシステム
- メイン会場に観客向けの公衆無線LANアクセスポイントを約1,500箇所設置

＜事前準備＞

- テスト・リハーサルを繰り返し実施

＜体制構築＞

- 組織委の技術チームがテクノロジー・オペレーション・センターを設置
- 技術スタッフ約600名が24時間稼働（セキュリティ関連スタッフを含む）
- 政府側のセキュリティ体制・関係機関とも緊密な連携

＜発生したサイバーセキュリティ事案＞

- 組織委NWに係るセキュリティに関する警告：約２３億件
- 公式HPに対する悪意ある接続要求（不正アクセス）：約２億件
- 開会式直前にスタジアムの電力供給制御システムへの攻撃情報を入手　→手動切替体制を急遽確保
  切替時間の30秒（＝停電）で開催国の威信が損なわれる（Reputation Risk への対応も必要）

2020年東京オリンピック・パラリンピック競技大会に向けた取組

2020年東京オリンピック・パラリンピック競技大会（以降、大会）を成功へと導くためには、大会の開催・運営を支える重要サービスにおけるサイバーセキュリティを確保し、安定したサービスを供給することが不可欠との認識の下、関係機関と連携し取組を検討。

【検討体制】

東京オリンピック競技大会・東京パラリンピック競技大会推進本部
（本部長：安倍総理）

2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議
（議長：杉田副長官）

セキュリティ幹事会

座長	– 内閣危機管理監
座長代理	– 内閣官房オリパラ事務局長、内閣官房副長官補（内政）、内閣官房副長官補（事態対処・危機管理）、警察庁次長
構成員	– 関係省庁の局長級
オブザーバー	– 東京都、組織委、警視庁、東京消防庁の幹部
事務局	– 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房（内政・事態・NISC）において処理

テロ対策ＷＴ

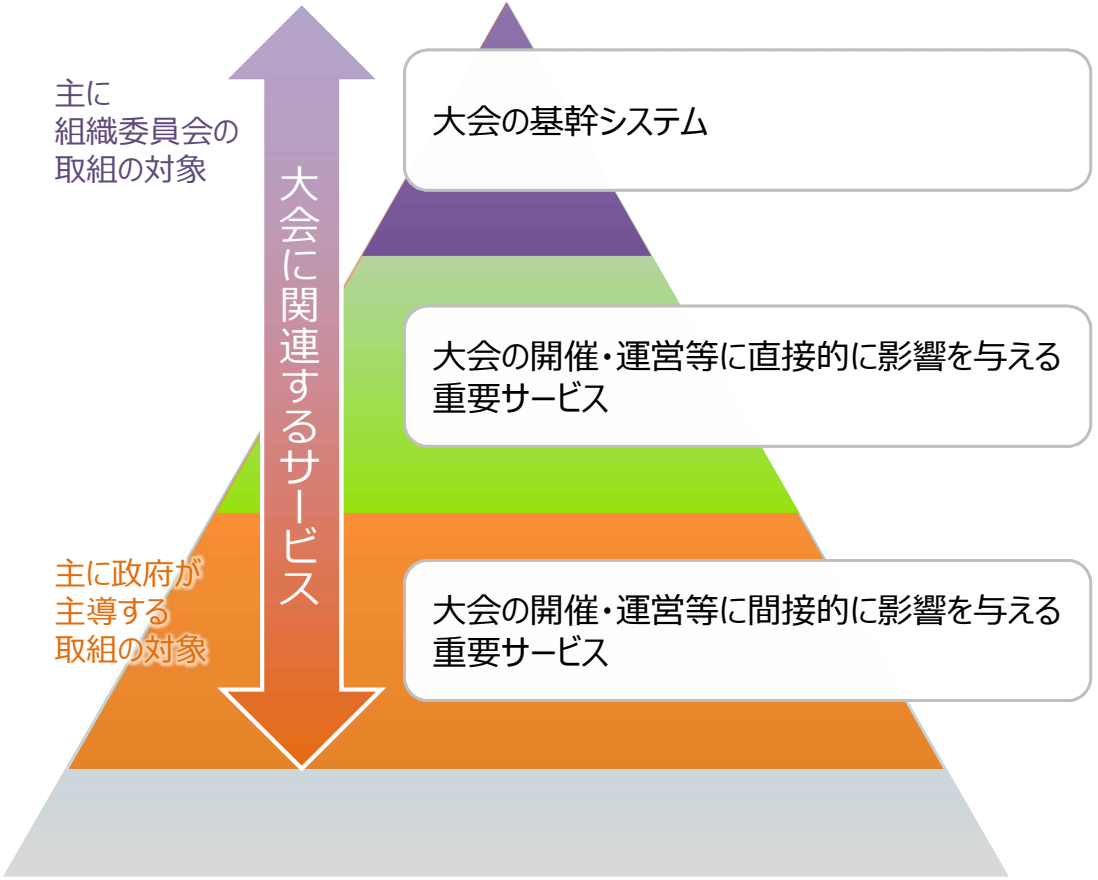
座長	– 内閣審議官（事態・内政）
座長代理	– 内閣審議官（オリパラ事務局） 警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 警察庁、国交省、防衛省の協力を得て内閣官房（事態・内政）において処理

サイバーセキュリティＷＴ

座長	– 内閣審議官（NISC副センター長）
座長代理	– 内閣審議官（オリパラ事務局） 警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房（NISC）において処理

2020年東京オリンピック・パラリンピック競技大会における
サイバーセキュリティ体制に関する検討会

【大会の開催・運営を支える重要サービスのイメージ】



サイバーセキュリティ確保のための取組

大会の運営に大きな影響を及ぼし得る重要システム・サービスを対象としたリスクアセスメントに基づく対策の促進や、大会組織委員会を含めた関係組織との情報共有の中核的組織としての対処体制（オリンピック・パラリンピックCSIRT）の整備に向けて検討を実施。

東京オリンピック・パラリンピック競技大会に向けた取組

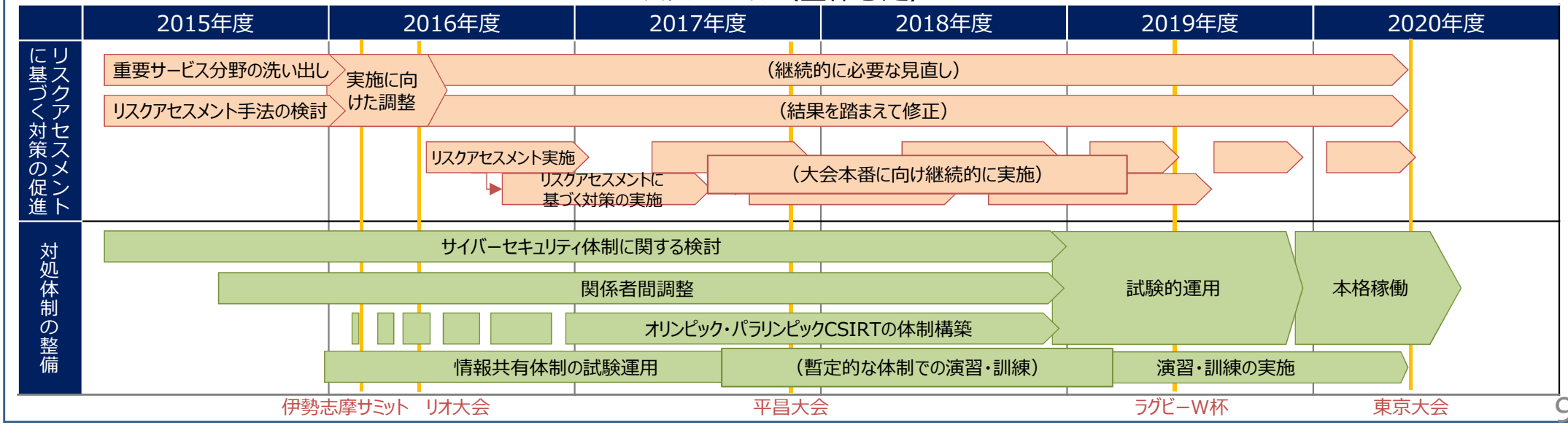
リスクアセスメントに基づく対策の促進
（事前対応のための取組）

- ○ 大会の開催・運営に影響を与える重要サービス事業者等を選定し、リスクアセスメントの実施を依頼。各事業者等は、10～12月の期間でリスクアセスメントを実施中。
- ○ 事業者等が実施するリスクアセスメントの手順書をNISCにおいて作成。現在、NISCでは事業者等からの手順に関する問合せへの対応を実施。

対処体制の整備
（事案発生時の迅速かつ的確な対処のための取組）

- ○ 関係組織に対して対処のための的確な情報共有を担う中核的組織としての対処体制（オリンピック・パラリンピックCSIRT）の構築に向け、2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する体制検討会において、具体的な体制を検討。
- ○ G7伊勢志摩サミット及びリオ大会において、現地に連携要員を派遣。情報共有手段として同検討会メンバーを中心とした体制の試験運用を実施。

スケジュール（全体想定）



2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組①

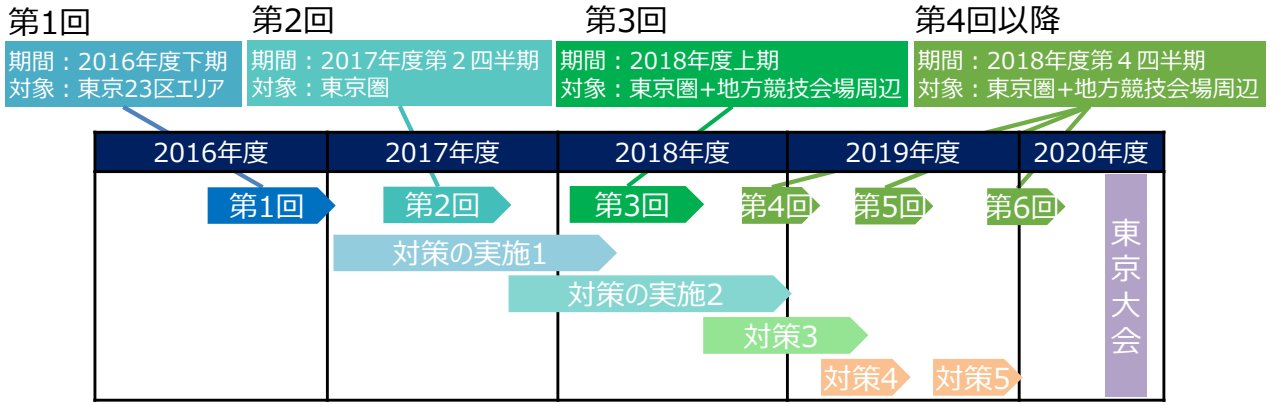
- ロンドン大会の事例を参考に、東京大会の開催に必要なサービスの安全かつ継続的な提供のため、リスクマネジメントの実施を促進。
- ９月に説明会を開催し、大会の開催・運営に影響を与えうる重要サービスを提供する事業者等に自主的な取組の実施を依頼。

大会に向けたリスクアセスメントの取組概要

○ リスクマネジメントの促進のため、セキュリティリスクを特定・分析・評価する手順をNISCで作成。

○ 大会の開催・運営に影響に与えうる重要サービス分野を、関連する所管省庁と調整の上で選定し、実施を依頼。

○ 大会に向けて、継続的に複数回実施することを想定。
- 対象となる事業者等の拡大
- 手順や例示するリスクシナリオの継続的な充実



東京大会に向けたリスクアセスメントの取組スケジュール

第１回（2016年度）の取組概要

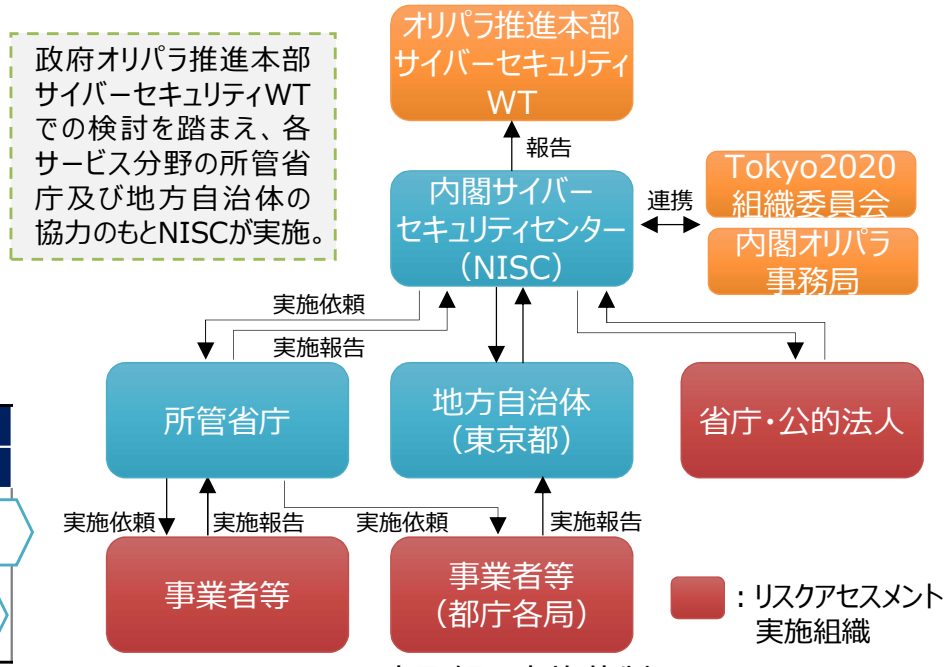
○ 第１回（2016年度）は東京23区エリアの事業者等が対象。

○ ９月に事業者等の担当者を招き、説明会を開催済み。
各事業者等は、10～12月の期間でリスクアセスメントを実施予定。
NISCは事業者等からレポートを受領し、３月を目途に結果をとりまとめる。

○ 明らかになったリスクについては、事業者等による自主的な対策を依頼。

第１回目（2016年度）の実施スケジュール

	2016年度			
	第１四半期	第２四半期	第３四半期	第４四半期
内容	重要サービス分野、事業者等の調整（NISC、所管省庁） リスクアセスメント手法の検討（NISC）	説明会	リスクアセスメント実施（各事業者等）	対策の実施（各事業者等） 結果とりまとめ、次回に向けた見直し（NISC）



本取組の実施体制

2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組②

対象とするリスク

情報、情報システム、制御システム等の情報資産に係る事象の結果（自然災害やサイバー攻撃等に起因するIT障害）から認識されるリスク

基本的な考え方

全世界からの注目を集める2020年東京オリンピック・パラリンピック競技大会を直接的・間接的に支える重要なサービスを提供する事業者等には、そのサービスを安全かつ継続的に提供することが期待される。

そのために必要な措置を事業者等が自身で講じられるようにするためには、リスクを特定・分析・評価することが必要。

＜イメージ＞

2020年東京オリンピック・パラリンピック競技大会の成功

成功のためには…

（要件）大会開催に必要なサービスが安全かつ継続的に提供されること

⇒ 大会開催に向けた各関係主体の活動目的

機能を保証するためには…

活動目的に対する不確実さ（＝リスク）を特定・分析・評価し、必要な対処につなげることが重要

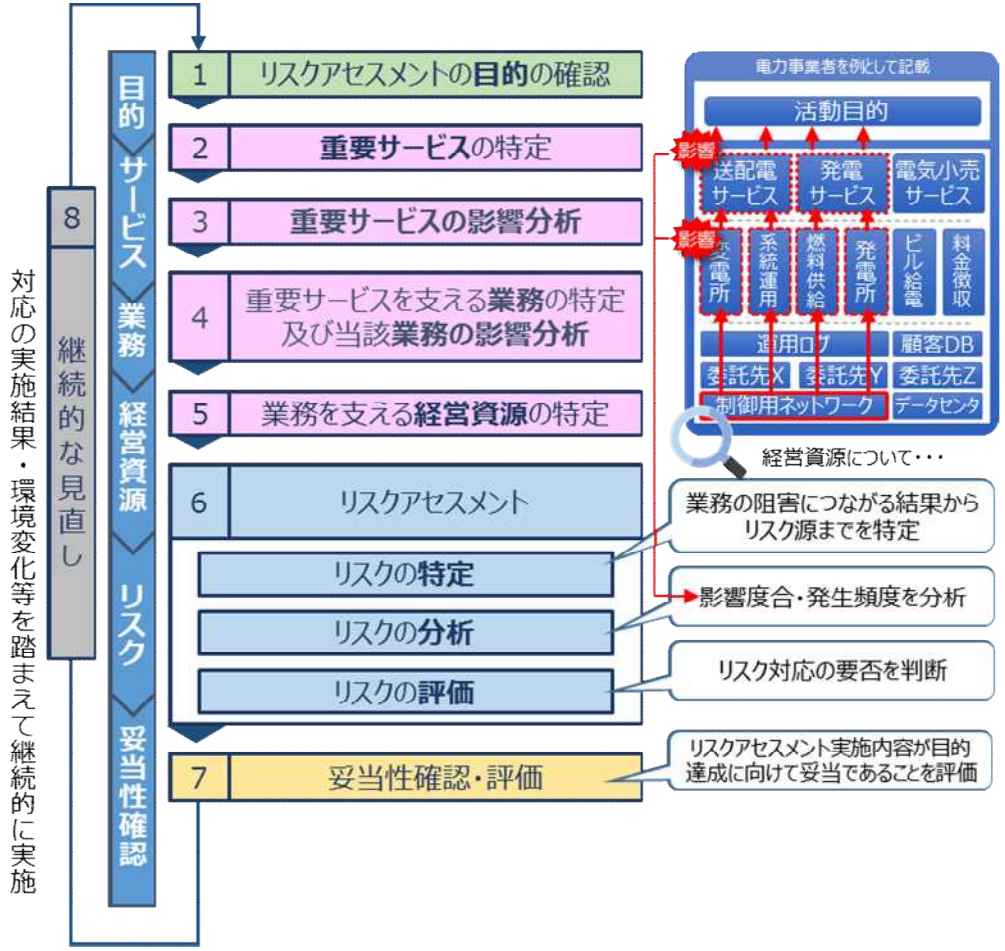
各関係主体が、

① 大会開催を支える重要なサービス及び必要なサービスレベルを特定し、

② そのサービス提供を全うすることに対するリスクを特定・分析・評価することが重要（機能保証のためのリスクアセスメント）

機能保証のためのリスクアセスメントの枠組み

「機能保証の観点から、事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定」し、その「サービス提供の維持・継続に必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを分析」していく。



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

★毎年２月～３月１８日をサイバーセキュリティ月間

- **サイバーセキュリティの将来について考える**
  - 民間との連携
  - IoTシステムの指数学的普及
  - ブロックチェーン、AI、ロボット等、既存の枠組みを変える可能性