NISC
National center of Incident readiness and Strategy for Cybersecurity

2020年に向けた 政府のサイバーセキュリティの取組

２０１５年１２月１４日
内閣サイバーセキュリティセンター（NISC）
企画官　伊貝　耕
http://www.nisc.go.jp/

我が国における危機①
～リスクの甚大化～

NISC

機微な情報に対する巧妙な攻撃

【最近の主な事例】　氷山の一角

2011.9～	[三菱重工業、衆議院等] 標的型攻撃によるウイルス感染発覚
2012.5	[原子力安全基盤機構] 過去数か月間の情報流出の可能性確認
2013.1	[農林水産省] TPP情報流出に関するサイバー攻撃事案報道
2013.4	[宇宙航空研究開発機構] サーバに対する外部からの不正アクセス発覚
2013秋頃	[政府機関等] 特定者がウェブ閲覧により感染するゼロデイ攻撃※発覚
2014.1	[原子力研究開発機構] ウイルス感染による情報の流出の可能性発覚

24時間365日（約8秒に１回）

【政府機関への脅威件数等】

	2012年度	2013年度	2014年度
センサー監視等による脅威件数 ※※	約108万	約508万	約399万
センサー監視等による通報件数	175	139	264
不審メールに関する注意喚起の件数	415	381	789

※ 「ゼロデイ攻撃」とは、ソフトウェアにおける未修正・未発表のセキュリティ上の脆弱性を悪用した攻撃

※※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

重要インフラに対する攻撃

【重要インフラへの攻撃件数等】　危機の高まり

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡※件数	15	76	133

	2012年度	2013年度
標的型攻撃メール等の情報提供※※件数	246	385

＜内訳＞
不正アクセス、DoS攻撃　121
ウイルスへの感染　7
その他の意図的要因　5

【重要インフラ分野】　保護対象の多様化

① 情報通信　② 金融　③ 航空　④ 鉄道　⑤ 電力
⑥ ガス　⑦ 政府・行政サービス　⑧ 医療　⑨ 水道　⑩ 物流
○ 化学　○ クレジット　○ 石油　※※※

［参考］米国の状況　電力、水道及び交通分野等の重要インフラに対する攻撃が、**2011年以降、17倍に増加**　（2013年6月デンプシー統合参謀本部議長講演）

※ NISCへの情報連絡件数のうちサイバー攻撃（意図的要因）に関するもの。　※※重要インフラ機器製造、電力、ガス、化学、石油の5業界からIPAへ情報提供されたもの
※※※　「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年5月19日情報セキュリティ政策会議決定）において追加

我が国における危機②
～リスクの拡散・グローバル化～

NISC

攻撃の対象範囲の拡散

国民1人1人へ

いつでもどこでも何でも

【スマートフォンの普及等】

スマートフォン
世帯保有率が**6倍**に急増※
（2010年末：約10%→**2013年末：約63%**）
携帯端末を標的とする不正サイトが**20倍**に急増※※
（2011年度末：約3千→**2013年度末：約5万7千**）

スマートカー
1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**※※※

スマートメーター（次世代電力量計）
各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

【我が国社会全体への浸透】

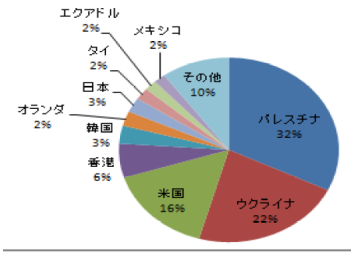
※　総務省「平成25年版情報通信白書」
※※　トレンドマイクロ㈱調べ（2014年4月）
※※※　（独）情報処理推進機構（IPA）「自動車の情報セキュリティへの取組みガイド」（2013年8月）
※※※※　経済産業省「第14回スマートメーター制度検討会」資料（2014年3月）

世界中からの多様な主体による攻撃

グローバル化

国家関与の可能性

【海外からの我が国への攻撃状況※】



【最近の主な事例】

2011.3	［韓国］政府機関等の40のウェブサーバへのDDoS攻撃発生 ***→ 日本の家庭用PCが踏み台となり攻撃指令サーバ化***
2013.3	［韓国］重要インフラに対する大規模サイバー攻撃発生 ***→ 使用された不正プログラムが我が国でも同時期に確認***
（備考）	
2014.12	［米国］SPE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**。

※　警察庁（2014年2月）

海外のサイバー攻撃事案（2014年8月～、報道ベース）

NISC

○ JPモルガン・チェース（2014年8月中旬）
2014年8月、サイバー攻撃が行われ、顧客の名前、住所、電話番号、電子メールアドレス及びユーザー関連の内部情報が流出したことが明らかとなった。サイバー攻撃は、ウクライナをめぐる西側諸国によるロシアへの金融制裁に対する報復としてロシア政府の関与した可能性もあるとのFBI捜査官の見解もある。

○ ソニー・ピクチャーズ・エンターテイメント（2014年11月下旬）
2014年11月、「平和の守護者（Guardians of Peace）」を名乗る組織が、システムに侵入し、同社の数千に及ぶ社内文書や未公開の4作品を含む5作品の同社映画全編の違法コピーがオンライン上に流出。米国政府は、12月19日、当該サイバー攻撃を北朝鮮政府による犯行とし、翌月2日、大統領令を発出し追加的な経済制裁を実施。

○ 保険会社アンセム（2015年2月上旬）
2015年2月、同社に対するサイバー攻撃により、8,000万人分に及ぶ新旧加入者や従業員の個人情報が盗まれた。氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えいしたが、クレジットカードや医療記録などの情報は流出した形跡はないとしている。なお、攻撃者は米国人事管理局（OPM）（後述）へのサイバー攻撃を行った中国人民解放軍ハッカー部隊であるとの可能性も指摘されている。

○ イラン石油省（2015年3月下旬）
本年5月26日、イラン国営放送は、イラン石油省が同年3月21日から24日の4日間の休日に米国によるサイバー攻撃を受けており、これを撃退したとの発表を報じた。イラン政府は米国政府に対して書簡を送付するとともに、国際司法命令を準備中であるとしている。なお、イラン政府高官は、本年2月イランの科学施設や工業施設に対して複数回のサイバー攻撃が行われていることを明らかにしている。

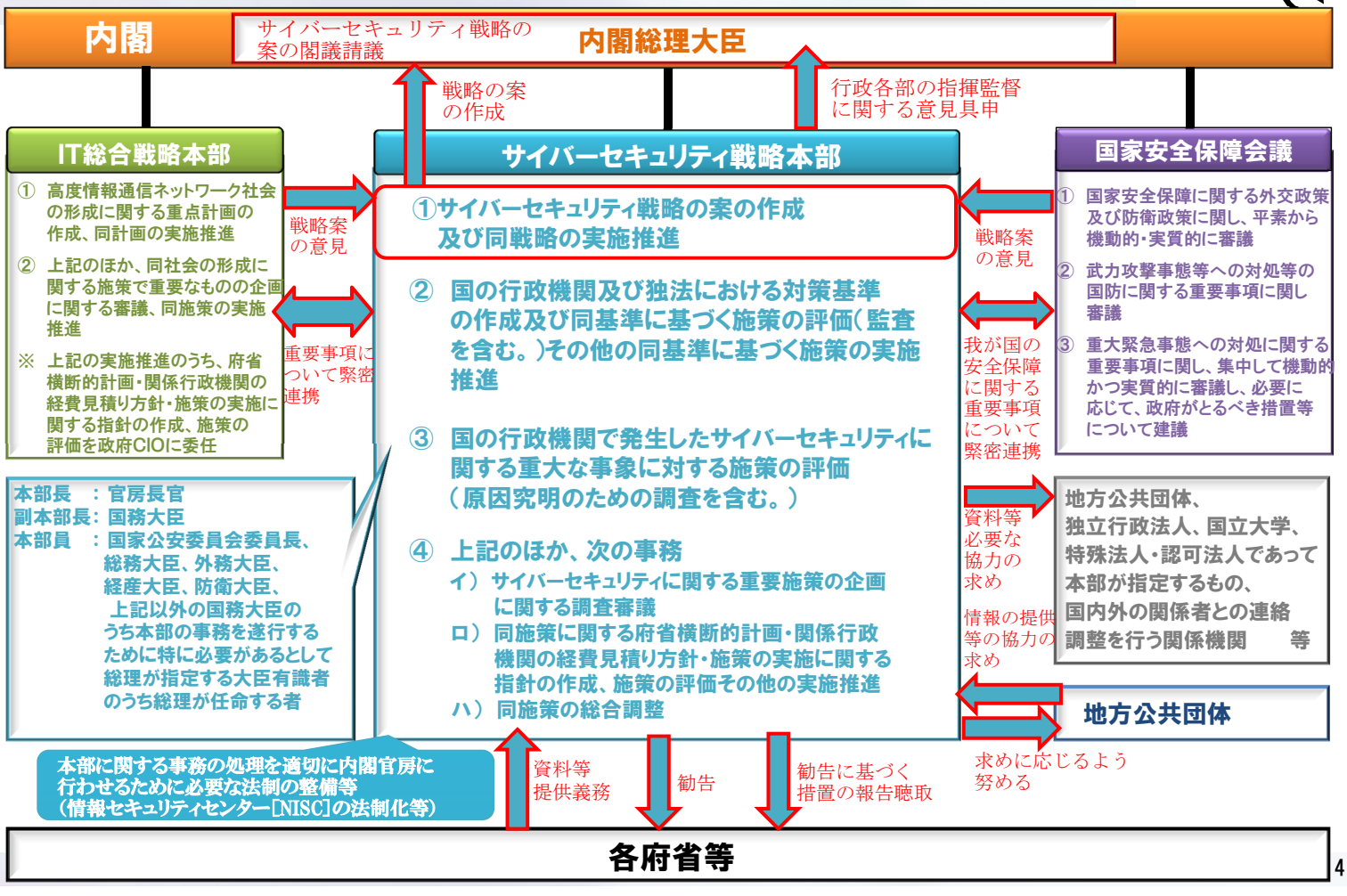
○ フランスTV5モンド（2015年4月上旬）
2015年4月8～9日、フランス国営テレビTV5モンドは、イスラム国に所属すると主張するグループ「Cybercalophate」によってTVチャンネル、Web、FaceBookが乗っ取られ、イスラム国の犯行を主張するメッセージが表示されていた。4月10日、フランス国防省は、調査の結果、軍の機密情報が漏えいすることはなかったと発表した。

○ ドイツ連邦委議会（2015年5月上旬）
2015年5月15日、ドイツ連邦議会（下院）のサーバにサイバー攻撃を受け、約2万台のパソコンが外部から自由に操作できる状態となった。メルケル首相の下院事務局のパソコンも感染。情報機関のトップは、手法が極めて巧妙であることからロシアの関与を示唆している。少なくとも5人の議員のパソコンからデータ流出が確認されており、それ以外の情報も流出するおそれがあるとしている。

○ イラン核問題6か国協議会場（2015年5月中旬）
2015年5月12日、スイス当局はイランの核問題をめぐる6か国協議がジュネーブのホテルで行われた際、サイバー攻撃が行われた可能性があり、それに関連するホテルの家宅捜査及びITシステムやソフトウェアの差し押さえを行ったと報道されている 。イスラエルの関与が疑われているが、イスラエルは根拠のないものであると否定している 。

○ 米国人事管理局（2015年6月上旬）
2015年6月4日、米国人事管理局は、システムが侵入され、400万件の職員及び元職員の個人情報が流出したと発表 。さらに、7月9日には、2150万人の情報が盗まれていたことを明らかにした専門家の見解では、中国人民解放軍のハッカー部隊である「ディープ・パンダ」と呼ばれる組織が今回の攻撃及び保険会社アンセムへの攻撃を実施したとされている。

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戦略本部（2015年2月10日）

安倍総理

●サイバー空間は、経済成長やイノベーションを推進するために必要な場。サイバーセキュリティは**成長戦略を実現するためにも必要不可欠**な基盤。

●他方、サイバー空間における脅威はますます深刻化。サイバー攻撃への対応は、まさに**国家の安全保障・危機管理上の重要な課題**。

●**サイバーセキュリティ戦略本部は、名実ともに、我が国のサイバーセキュリティ分野の司令塔**となるべき存在。まずは、**サイバーセキュリティ施策の基本的方針について、新たな「サイバーセキュリティ戦略」を策定**。

●**オリンピック・パラリンピック東京大会の成功にはサイバーセキュリティの確保が必要不可欠**。こうした点も見据え、我が国のサイバーセキュリティに万全を期して参りたい。

新たな「サイバーセキュリティ戦略」について（全体構成）

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
- あらゆるモノがインターネットに連接され、サイバー空間と実空間との融合が高度に深化した**「連接融合情報社会」**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**
  経営者の意識改革、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

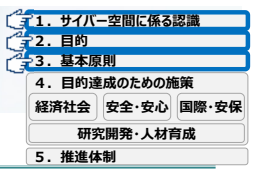
横断的施策

- **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、オリンピック・パラリンピック東京大会に向けた対応

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年オリンピック・パラリンピック東京大会の開催、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」が到来しつつある。
- 一方、社会経済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、国民生活への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、下記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・演習等実施の推進

■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システム等のセキュリティに係る国際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

IoTと成長戦略

IoTは成長戦略のkeyの１つ

○成長戦略進化のための今後の検討方針　（平成27年１月29日産業競争力会議決定）
（略）「ロボット革命」の実現に加え、ビッグデータ、人工知能やモノのインターネット（IoT）等の急速な発展により生産・流通・販売、交通、健康・医療、公共サービス等の幅広い分野で想定される産業構造の変革に対応するため、今後のビジネスモデルの在り方を見据えた産業横断的な課題及び対応策の検討を進めるとともに、人材育成やセキュリティ対策、グローバル市場を念頭に置いた国際標準化対応などの環境整備を加速化する。

背　景

- ハードウェアデバイスの進化
  （センサー等の小型化・低価格化が進展）
- 低廉・高速なインターネットの普及
- ビッグデータ解析技術の進歩

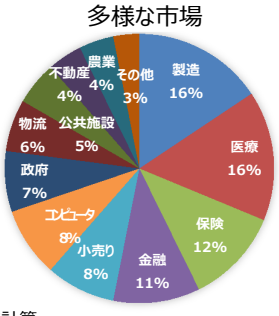
- あらゆるモノがネットワークでつながり、リアルタイムでのデータ化・自動制御が進展。あらゆる産業でデータの利活用、高度な判断サービスや自動制御が可能に。

市場規模・対象範囲の拡大

- 創出する経済価値：**1.9兆ドル（約228兆円）**
- 全体のサービス投資：**2630億ドル（約32兆円）**
- 対応製品は約250億台
  （PC、スマートフォン、タブレット以外の端末が過半数）

※ 数字は2020年時点の予測、1ドル＝120円で計算

多様な市場



Source: 全てGartner

諸外国も国家レベルで推進

ドイツ政府は、2011年、独製造業の競争力強化のための構想**"Industry4.0"** を提示し、IoTによるさらなる効率化を国全体で強化。
メルケル首相の強力なリーダーシップにより推進。

米国政府は、2012年、ビッグデータを活用し、国家の喫緊の課題解決を図るため**"BigData R&D Initiative"** を発表。民間では、GEが、「インダストリアル・インターネット」を提唱。60社以上でコンソーシアムを形成。

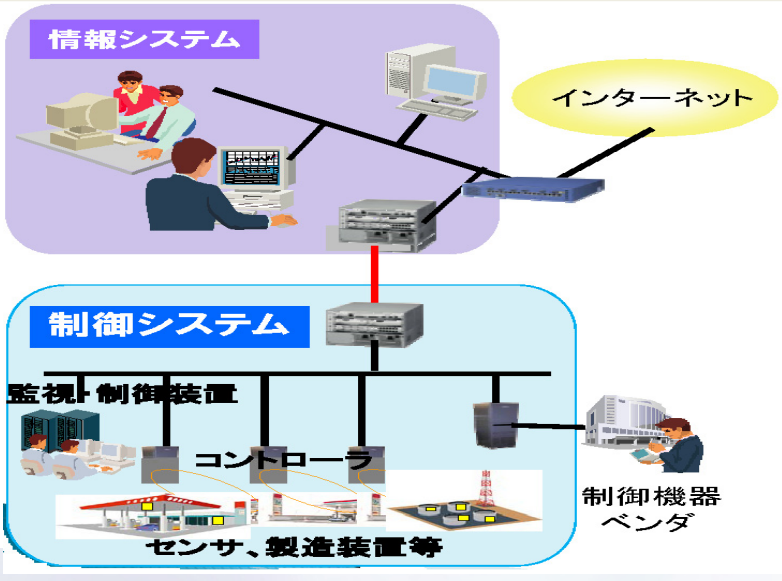
制御システムの汎用化の進展

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

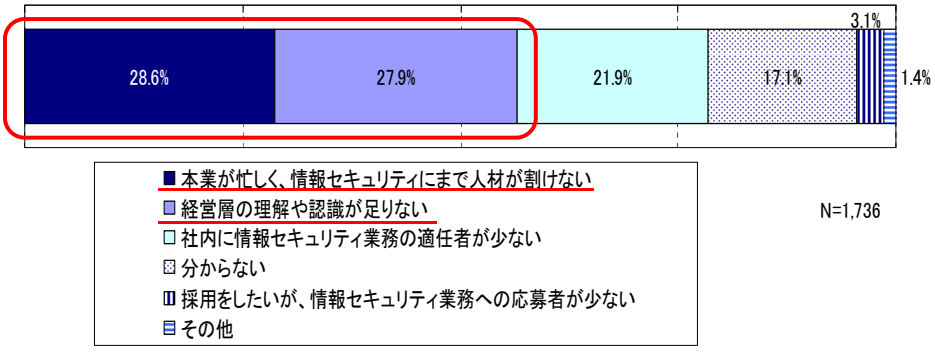
○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
○ 外部ネットワークにも接続されるようになっている。
○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。



企業等における情報セキュリティ対策の現状

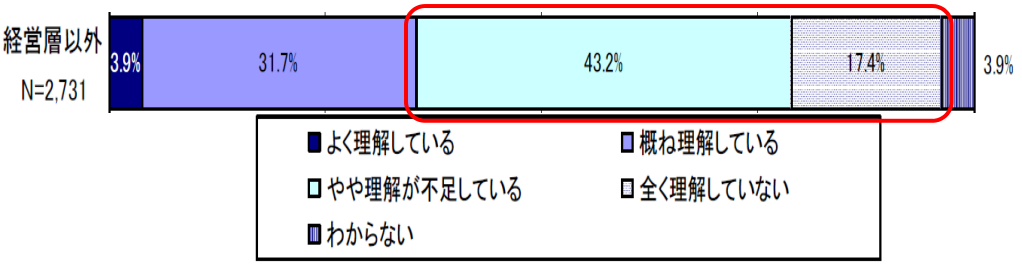
○企業では**情報セキュリティに関する業務に従事する人員が不足**。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

人材不足の原因（社内向け業務）



企業経営層の情報セキュリティに対する理解度

（経営層以外からの回答）



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」2012年4月

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）

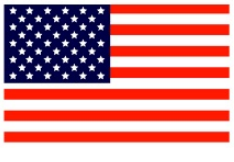
- 開示企業数は、平成21年度の52%（116社）から平成25年度の60%（136社）へと増加。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の14業種が100%（合計51社）。
- 繊維、パルプ・紙、鉄鋼等の4業種は0%（合計14社）。
- 素材産業全体（64社）では開示割合が32.8%と低く、原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低いと考えられる。
- サイバーセキュリティリスクの記載文書が5年間同一の企業（65社）には、その記載の仕方が包括的で意味が広く捉えられる（想定インシデント・被害が具体的でない）ものが多かった。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

米国におけるサイバーセキュリティに係るリスク開示

- 米国企業のForm 10-Kに記載するリスク要因については連邦規則（Regulation S-K Item503 (c)）にて規定されており、どの企業にもあてはまるような一般的な記述ではなく、当該企業特有の内容について、具体的に分かり易く説明するよう要求されている。



- また、サイバーセキュリティリスク開示に関するガイダンスとしては、米国証券取引委員会（SEC）企業財務局から2011年10月に発行された「CF Disclosure Guidance: Topic No. 2 Cybersecurity」（CFDG: Topic No.2）がある。
  同文書は、上場企業がサイバーセキュリティについて、自社特有の事実と状況を考慮しつつ、どのような場合に何を開示すべきかを判断する助けとなるガイダンスである。
- 上記に基づき、米国企業においては、サイバーセキュリティに関する自社特有の事実・状況に照らしたリスクや想定被害について詳しく開示している傾向があり、被害事例を開示する企業も見られる。
- なお、証券法は、詳細な開示によって当該企業がサイバーセキュリティ上の危険に晒されるような場合にまで開示を求めるものではないとしている。

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～

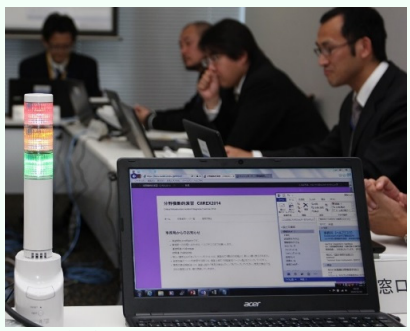
■国民・社会を守るための取組

- 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、ネットワーク基盤の安全確保の推進
- 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
- 自治体や中小企業等の取組に対する積極的な啓発・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
- 情報提供によって不利益が生じない環境の構築、より効果的かつ迅速な官民の情報共有（ホットライン構築、情報共有の様式・手順の改良、処理の自動化等）、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー導入等の環境変化も見据え、地方公共団体に対し、政府として必要な支援を実施
- 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、監視・即応機能を中心とした機能強化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

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年5月、情報セキュリティ政策会議決定）

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
- 事案対処省庁
- 防災関係府省庁
- 情報セキュリティ関係機関
- サイバー空間関連事業者

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

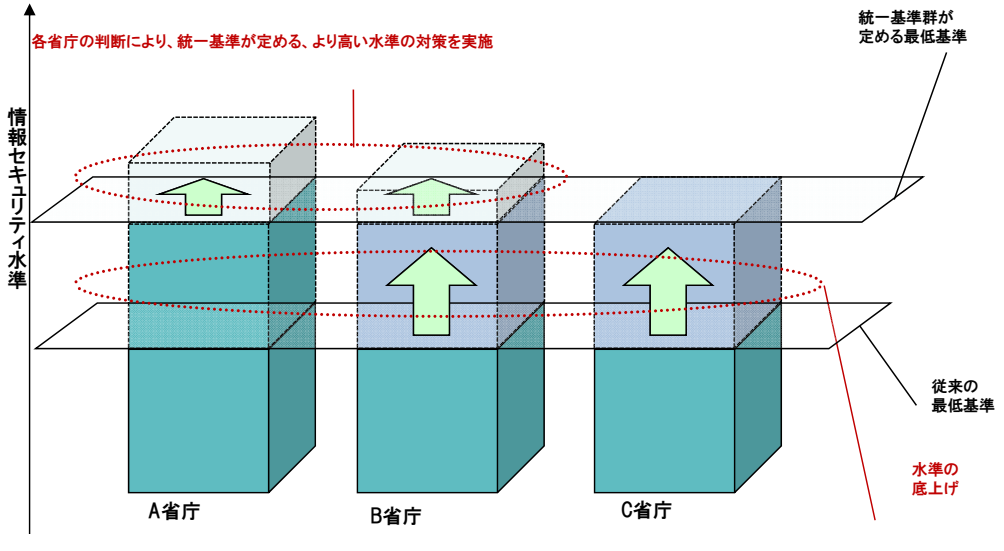
安全基準等の整備・浸透	情報共有体制の強化	障害対応体制の強化	リスクマネジメント	防護基盤の強化
重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進	IT障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化	官民が連携して行う演習等の実施・演習・訓練間の連携によるIT障害対応体制の総合的な強化	重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援	広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

統一基準群（政府機関セキュリティポリシーのベースライン）

○政府機関が実施すべき対策の統一的な枠組みを構築

○政府機関全体の情報セキュリティ水準の底上げに寄与

＜統一基準群の効果（イメージ）＞



統一基準群の改定（14年5月、情報セキュリティ政策会議決定）

◆ 標的型攻撃への対策

➢ 標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずる。

標的型攻撃のイメージ

・特定の組織の情報に狙い
・従来の外壁防護を無効化

内部対策の強化が重要

◆ サプライチェーンリスクへの対策

➢ 情報システムの構築等の外部委託の際、委託先における不正機能の混入防止のため、厳正な管理を要求。

サイバーセキュリティ対策を強化するための監査の基本方針

（15年5月　サイバーセキュリティ戦略本部決定）

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　※独立行政法人については、当面、特に必要があると認める場合に監査の対象とする。

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。

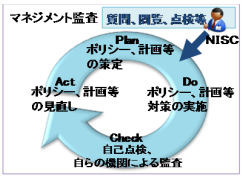
(3) 各機関の状況を踏まえた監査
- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

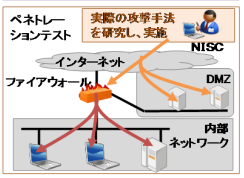
(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定
- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

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　※監査事務については、内閣サイバーセキュリティセンターが実施する。

(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。

政府機関等のサイバーセキュリティ対策の抜本的強化（1/3）

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、所要の法改正を含め、抜本的な強化を図る。

（注）「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に盛り込み、積極的かつ総合的に推進する。

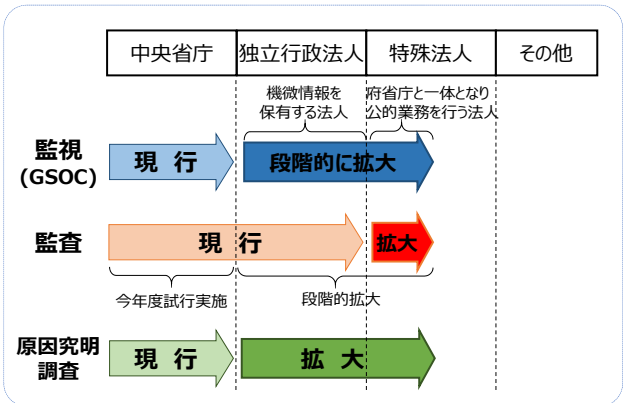
1．NISCの機能強化

■ 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（所要の法改正について速やかに検討）



■ 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（所要の法改正について速やかに検討）

■ 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

政府機関等のサイバーセキュリティ対策の抜本的強化（2/3）

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）

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）

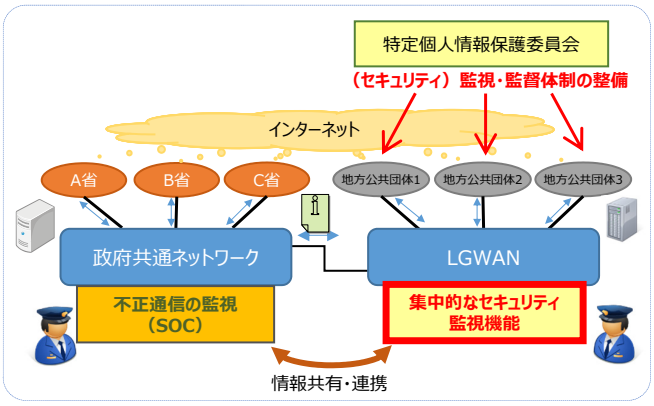
3．その他の重要課題への取組強化

■ 重要インフラに関する取組強化（本年中を目途に具体策を決定）
- 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（本年中を目途）



■ 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

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 ： 日米安保体制を基軸とす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

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
- 第2回日EU・ICTｾｷｭﾘﾃｨﾜｰｸｼｮｯﾌﾟ：2013年12月
- 第1回日EUサイバー協議：2014年10月

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
- 第２回日英サイバー協議：2014年11月

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
- 第1回日印サイバー協議：2012年11月

エストニア
○日エストニアサイバー協議(2014年12月)

フランス
○日仏サイバー協議(2014年12月)

イスラエル
○日イスラエルサイバー協議（2014年11月）

ロシア
○日露サイバー協議（2015年3月）

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。

リスクのグローバル化

国際連携取組方針
（１３年１０月）
●多角的なパートナシップの強化や技術の国際展開等の加速化

米国
- 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
- 第2回日米サイバー対話：2014年4月@ワシントン

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：2015年2月

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。

ASEANとの国際連携の成果（2013～2014年）

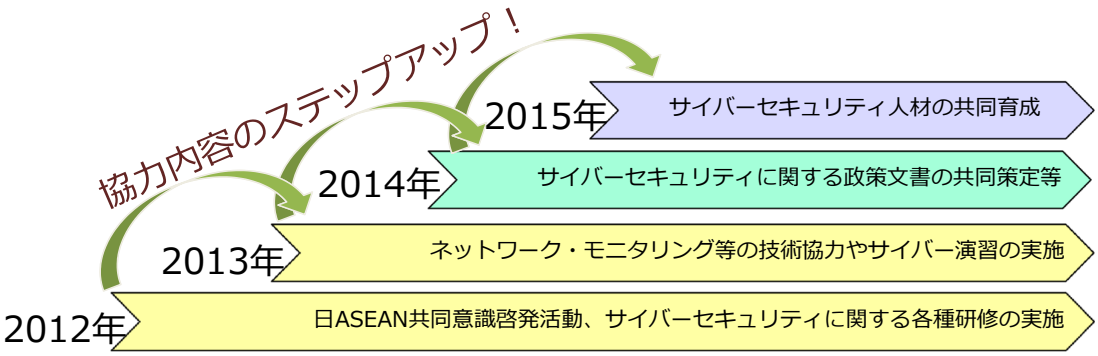
NISC

- ASEAN各国との国際会議*を主催、協力内容をステップアップ

2013年以前からの取組である日ASEAN共同意識啓発活動や各種研修、技術協力、サイバー演習等について、内容を充実・高度化させつつ継続

2014年の重点的取組として、「日ASEANにおける重要インフラ防護に関するガイドライン」を共同策定。また、サイバー犯罪対策対話によって法執行分野の能力構築支援を開始

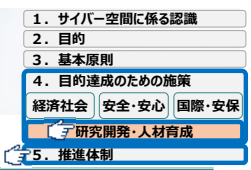
2015年の重点的取組として、高度なスキルを有するサイバーセキュリティ人材の共同育成に向けた検討を開始



ASEAN・JAPAN

*第7回 日ASEAN情報セキュリティ政策会議(局長級）及び第3回日ASEANシンポジウム（2014年10月7日～9日・東京）
第6回 日ASEAN政府ネットワークセキュリティワークショップ（課長級）(2014年8月27日～28日・シンガポール）
重要インフラ専門家パネル（2014年1月・東京、2月・クアラルンプール、5月・タイ）
第1回 日ASEANサイバー犯罪対策対話（2014年５月・シンガポール）

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）



NISC

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
- 産学連携による実践的な演習の機会の充実
- 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)
- 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
- 実践的能力を評価する仕組みや資格制度の充実、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

- 官民及び関係省庁間の連携強化により、サイバー攻撃の検知・分析・判断・対処の機能を強化
- 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
- オリンピック・パラリンピック東京大会に向け、リスクの明確化、実践的対処体制の構築、十分な演習・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、経費見積もり方針を策定する。

「サイバーセキュリティ2015」の概要について

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

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

- IoTに係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】
- M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】
- エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】
- 経営ガイドラインの策定【経済産業省】
- 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】
- ISACを活用した情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 政府系ファンド等の活用検討【経済産業省】
- 著作権法におけるリバースエンジニアリングに関する適法性を明確化【文部科学省】
- 制御システムセキュリティ認証の拡大【経済産業省】

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

- マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】
- 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】
- 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】

■重要インフラを守るための取組

- 東京オリンピック・パラリンピック競技大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】
- マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】

■政府機関を守るための取組

- 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】
- 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【内閣官房】

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

- 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】
- カウンターインテリジェンスに係る取組の推進【内閣官房】
- サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】
- 部外インフラ等、関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 二国間協議や多国間協議に参画し、国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映【内閣官房及び外務省】
- 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】
- 各国における能力構築を支援【内閣官房 他】

■世界各国との協力連携

- ASEAN諸国との連携を強化【内閣官房 他】
- インターネットエコノミーに関する日米政策協力対話にて一致した、米国との情報共有を強化【総務省】
- 包括的な日米サイバー防衛の連携【防衛省】

横断的施策

■研究開発の推進

- 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】
- 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】

■人材の育成・確保

- 高度なITの知識と経営などその他の領域における専門知識を併せもつ人材の育成【文部科学省及び経済産業省】
- 初等中等教育に携わる教員等を対象とした研修、情報交換【文部科学省】
- 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】
- サイバー防御演習を通じた実践的セキュリティ人材の育成【総務省】

推進体制

- 伊勢志摩サミットにおけるサイバーセキュリティの確保や東京オリンピック・パラリンピック競技大会に向けた対策の検討【内閣官房】

2020年オリパラ東京大会に向けたセキュリティ対策検討体制

【概要】
○閣僚会議においてセキュリティ対策の進捗管理を行うことをIOCに対して明確化するとともに、関係府省庁によるセキュリティ幹事会、テロ対策WT及びサイバーセキュリティWTを平成26年10月に設置。今後の課題や緊密な連携についての確認とあわせ、計画・運営段階において関係機関を主導するシニア・セキュリティ・コマンダーとして警察庁次長を登録。

【体制】

オリパラ推進本部（本部長：安倍総理）

←IOCが設置を求める**TOGC**（Tokyo Olympic Games Council）**に相当**

オリパラ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（シニア・セキュリティ・コマンダー）

構成員 – 内閣官房（内政・オリパラ事務局・事態・内調・ＮＩＳＣ）、内閣府（防災担当）、警察庁、金融庁、総務省、消防庁、法務省、公安調査庁、外務省、財務省、文科省、厚労省、経産省、国交省、海上保安庁、原子力規制庁、防衛省の局長級

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

＊平成26年10月のセキュリティ幹事会設置当時は「オリパラ閣僚会議」

サイバーセキュリティ戦略（2015年９月閣議決定）抜粋

＜6．推進体制＞

（略）

さらに、2020年の東京オリンピック・パラリンピック競技大会を始めとする国際的なビッグイベントにおけるサイバーセキュリティの十全な確保が必要である。とりわけ東京オリンピック・パラリンピック競技大会については、同大会に係るサイバーセキュリティ上のリスクを明確にした上で、大会運営及びこれに関係する諸機関や、関連する重要インフラが提供するサービスへのサイバー攻撃に対して、予防、検知を的確に行い、関係主体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オリンピック・パラリンピックCSIRTの整備を加速化する。また、そのために必要となる組織・施設・協力関係の構築及び維持、専門家の確保、事前の十分な訓練について、2016年の伊勢志摩サミット及び2019年に我が国で開催されるラグビーワールドカップにおける取組を踏まえ、段階的かつ着実に推進する。こうした取組によって培った対処能力については、持続的なサイバーセキュリティの強化のため、大会後においても活用していく。

（略）

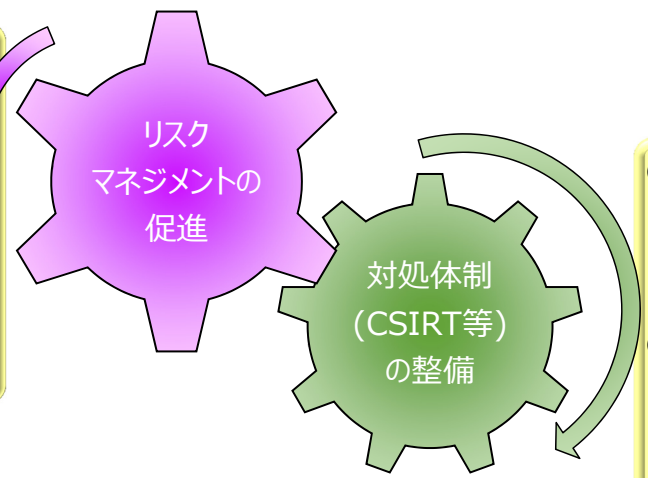
リスクマネジメントの促進と対処体制（CSIRT）の整備

○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、大会運営を支える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重要。

○これを実現するには、大会の開催・運営に影響を与えるサービスを提供する事業者において、サイバーセキュリティ上のリスクを把握し、リスクに応じた必要な対策を施すこと、また、事案が発生した際に関係組織間で迅速に必要な情報共有を行い、的確に対処するための体制の構築及び強化が必要。

○大会の開催・運営に影響を与える重要なサービスを提供する事業者を選定。

○サイバーセキュリティ上のリスクを特定・分析・評価するための手順をとりまとめ、選定された事業者を中心としてリスクマネジメントの実施を促進。

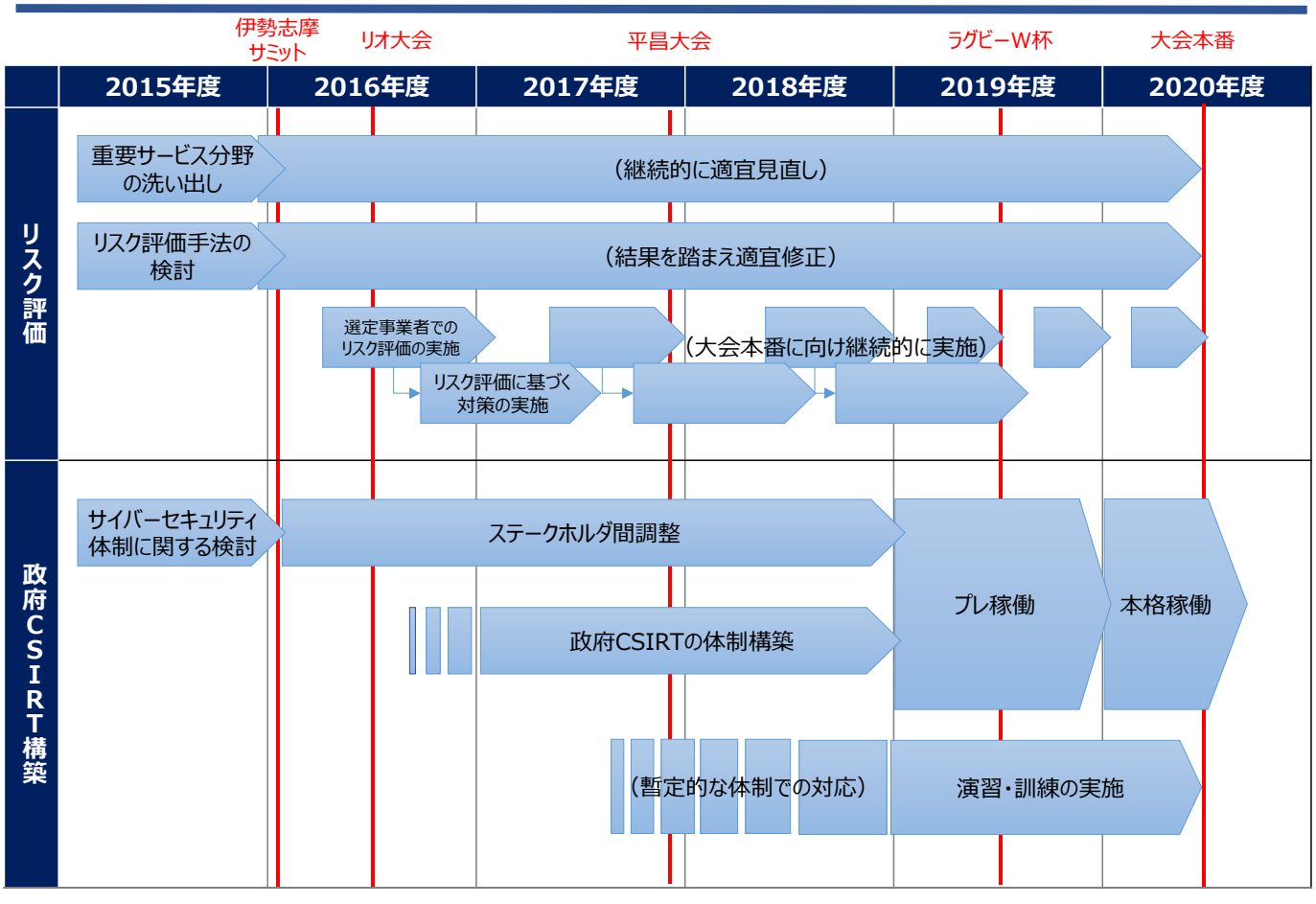


○関係組織に対して対処のための的確な情報共有を担う中核的組織としてのオリンピック・パラリンピックCSIRTを整備。

○整備にあたっては、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（以降、検討会）を通じ、政府/関連組織の役割を整理し、具体的な体制を検討。

各取組を並行して実施し、補完し合いながら推進

2020年オリパラ東京大会に向けた作業スケジュール



NISC

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