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

「東京オリンピック・パラリンピック競技大会のためのサイバーセキュリティ政策」

内閣官房　内閣サイバーセキュリティセンター(NISC)
東京オリパラチーム　企画官
雲田　陽一

サイバーセキュリティ政策の経緯

○今後の重要な環境変化
- 2020年東京オリンピック・パラリンピック競技大会
- マイナンバー利用開始
- スマートメーター、自動走行システム等

省庁ＨＰ連続改ざん 2000.1
Webサーバの脆弱性への攻撃
偽サイト誘導詐欺 スパイウェア
米国同時多発テロ 2001.9
Winny
誘導型攻撃の出現
米韓への大規模攻撃
イラン核施設への攻撃
9.18攻撃
韓国大規模障害
遠隔操作ウィルス
水飲み場型攻撃
標的型攻撃 組織的高度化
米国での中国軍関係者起訴・指名手配
感染PCによる不正送金
米国ソニーピクチャーズへの攻撃
年金機構情報流出
世界規模の身代金要求型攻撃

年度: 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018

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

参考：IT利活用
- 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, 2016.5.20 改定)
- 世界最先端ＩＴ国家創造宣言 官民データ活用推進基本計画 (2017.5.30 閣議決定,)

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)
- ｻｲﾊﾞ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基本法改正公布 (2016.4.22)
- **ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2015.9.4 閣議決定)**

年次計画
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
SJ2006 | SJ2007 | SJ2008 | SJ2009 | JS2010 | JS2011 | JS2012 | CS2013 | CS2014 | CS2015 | CS2016 | CS2017

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)
  - 平成28年度版 (2016.8.31 戦略本部決定)

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)
- 重要インフラの情報ｾｷｭﾘﾃｨ対策に係る第４次行動計画 (2017.4.18 戦略本部決定)

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)
- 内閣官房内閣ｻｲﾊﾞ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)

2014.9 山口大臣 → 2015.6 遠藤大臣 → 2016.8 丸川大臣 → 2017.8 鈴木大臣

サイバーセキュリティをめぐる状況の変化

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
（2016年末：PC普及率 73.0%、インターネット普及率 83.5%）
※2017年版情報通信白書（総務省）

スマートフォン 

世帯保有率が7.4倍に急増
（2010年末：9.7%→2016年末：71.8%）
※2017年版情報通信白書（総務省）

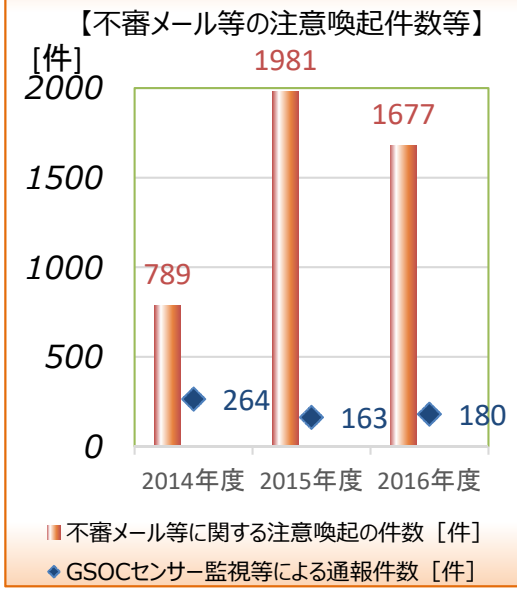
自動車 

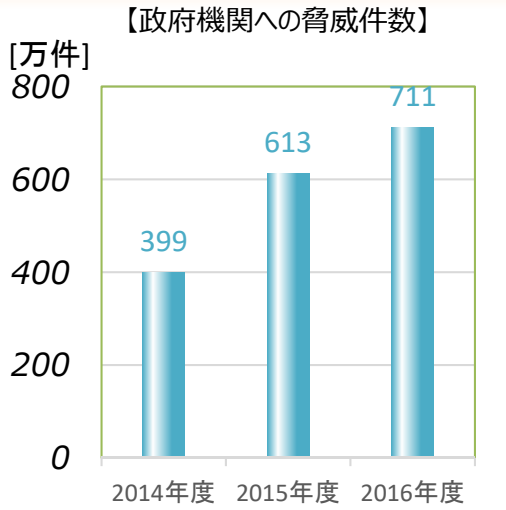
一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの取組みガイド（2013.8 IPA）

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





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。

東京五輪へ向けた準備

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

サイバー脅威に対応し、サイバーセキュリティを強化するため、サイバーセキュリティ基本法が成立、施行。
（平成26年11月12日公布。平成27年１月９日全面施行）

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）

協力

＜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＞

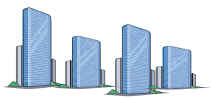
文部科学省（セキュリティ教育）等

協力

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

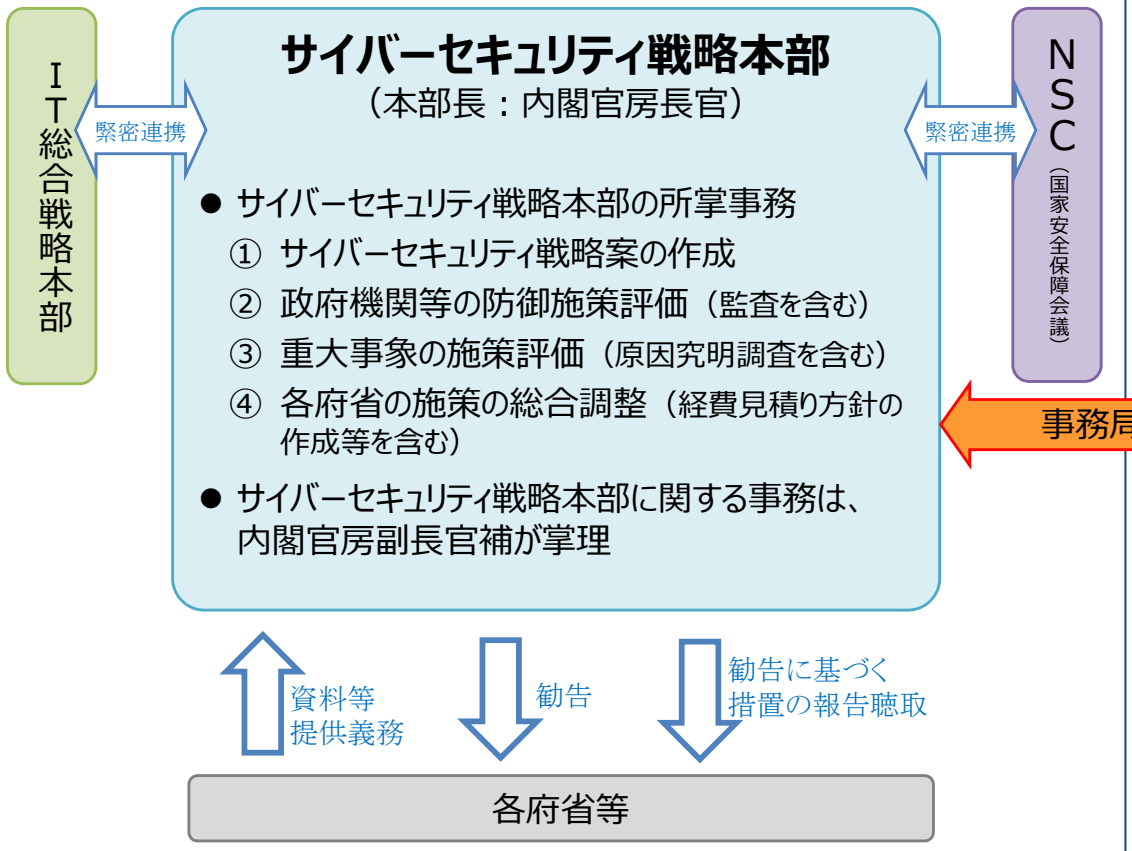
「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」概要

1　機能強化の必要性

以下の観点から、我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

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

2　サイバーセキュリティ基本法の制定



3　我が国の推進体制の機能強化に向けた取組

（１）　情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。

（２）　内閣官房情報セキュリティセンター（ＮＩＳＣ）を以下の組織に法制化（内閣官房組織令）する。

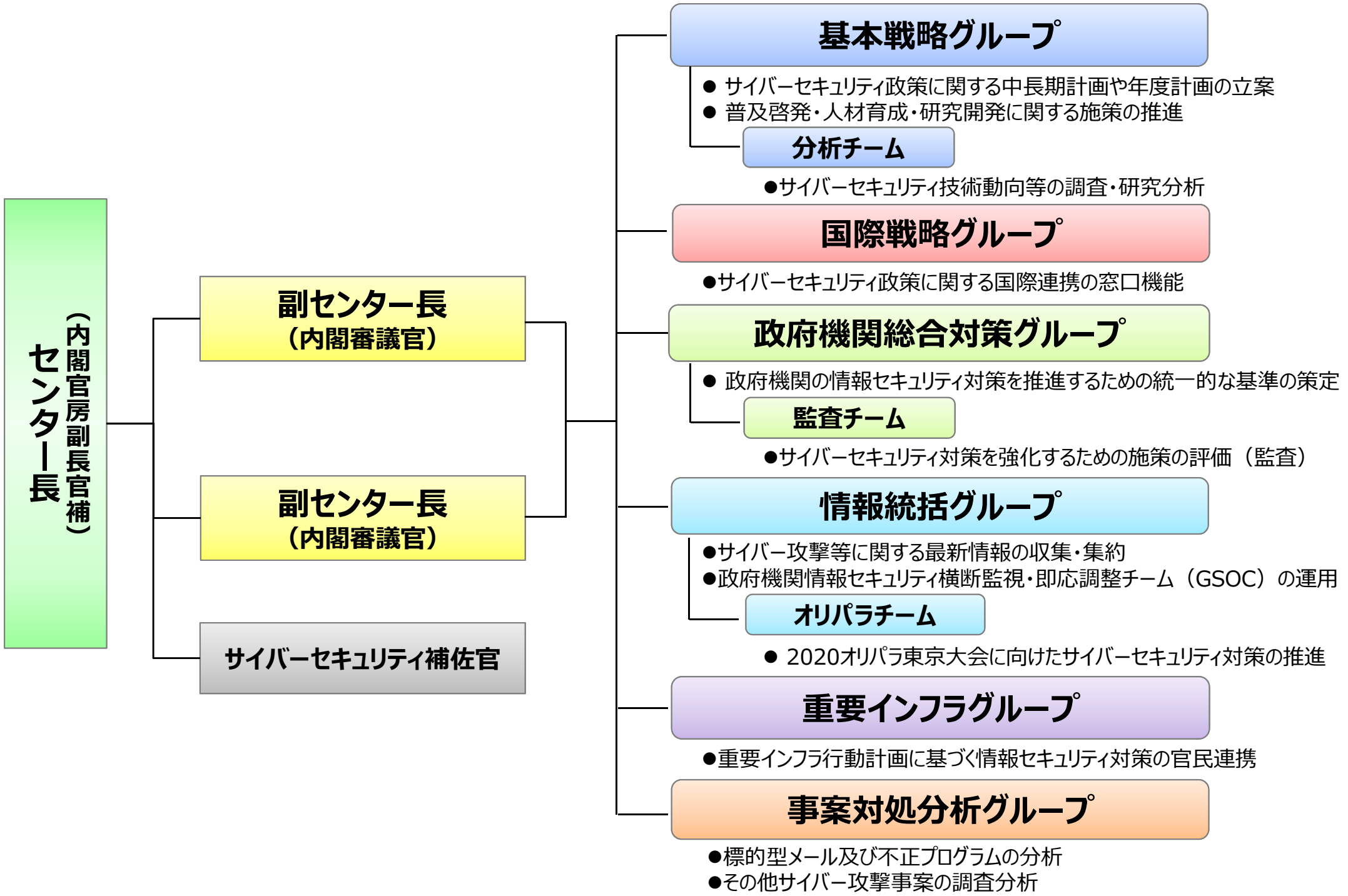
内閣サイバーセキュリティセンター（注）

- 内閣サイバーセキュリティセンターの所掌事務
  - ① ＧＳＯＣに関する事務
  - ② 原因究明調査に関する事務
  - ③ 監査等に関する事務
  - ④ サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

（３）今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

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

内閣サイバーセキュリティセンター（NISC）の組織体制



「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

2020年及びその後を見据えたサイバーセキュリティの在り方について
－サイバーセキュリティ戦略中間レビュー（平成29年７月13日）－

(必要な制度面の見直しも含め)可能な施策から段階的に実施（1年以内）

脅威等の変化

IoT機器を踏み台にしたサイバー攻撃の顕在化

省庁・分野を越えた情報共有の必要性

2020年に向けた抜本的対策を見据えた取組の必要性

ボット撲滅の推進

情報共有・連携ネットワーク（仮称）の構築・運用

オリパラ大会に向けた体制の整備

経済社会の活力の向上及び持続的発展

- 安全なIoTシステムの創出による国際競争力の強化（国際標準化）
- セキュリティに係るビジネス環境の整備

国民が安全で安心して暮らせる社会の実現

- 深刻度判断基準
- 政府機関等の効率的・効果的防護
- 地方公共団体、大学等における対策の向上
- サイバー犯罪対策等の強化
- 普及啓発・情報発信

国際社会の平和・安定及び我が国の安全保障

- 我が国の安全の確保
- 国立研究開発法人の策の強化
- 海外の多様な主体との多層的な連携
- サイバー犯罪等対策の国際的な連携

- 経営層の意識改革や、橋渡し人材等幅広い階層における人材育成・確保の継続的な促進
- 研究開発等の推進

重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

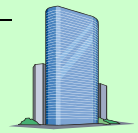
重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

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

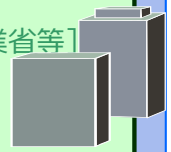
ＮＩＳＣによる調整・連携

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対策に係る第４次行動計画

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

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

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重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

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】

オリパラ推進本部
（本部長：安倍総理）

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、NISCセンター長）、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）、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、スポーツ庁、厚労省、農水省、経産省、国交省、気象庁、海上保安庁、環境省、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において処理

テロ等警備対策ＷＴ

座長	－ 内閣審議官（事態、オリパラ事務局）
座長代理	－ 内閣審議官（内政）、内閣府審議官（防災）、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	－ 関係行政機関の協力を得て内閣官房において処理

サイバーセキュリティＷＴ

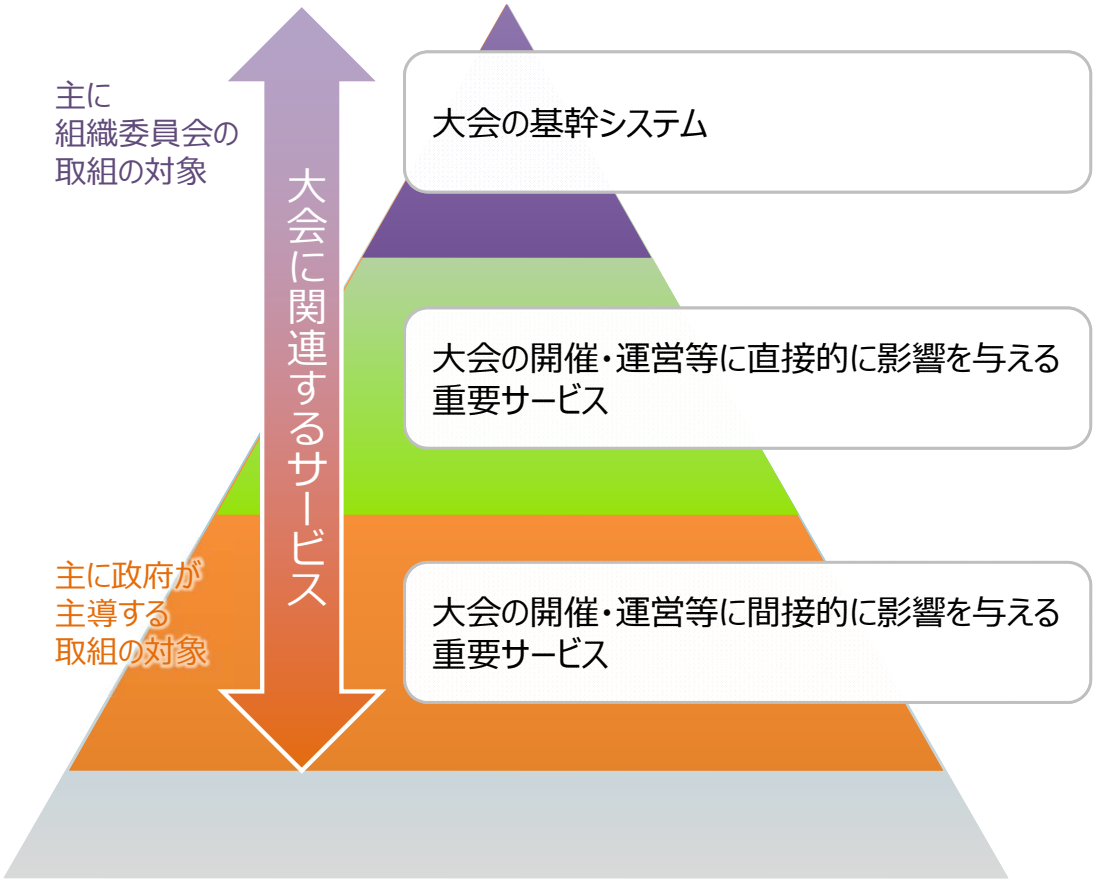
座長	－ 内閣審議官（NISC副センター長）
座長代理	－ 内閣審議官（オリパラ事務局）、警察庁審議官
構成員	－ 関係省庁の課長級
オブザーバー	－ 関係機関の幹部
事務局	－ 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房において処理

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

セキュリティ情報センター

- 平成29年7月24日、警察庁に設置
- 大会の安全に関する情報を集約
- 関係機関等と協力し、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対し必要な情報を随時提供

【大会の開催・運営を支える重要サービスのイメージ】



2016年リオデジャネイロオリンピック・パラリンピック競技大会における状況

関連するWebサイト等への複数のサイバー攻撃が認知されたものの、**大会運営に支障をきたすような事象は発生しなかった**

期間中の取組

リオデジャネイロオリンピック・パラリンピック競技大会組織委員会（以下「リオ組織委」という。）技術運用センターにNISC職員２名を連携要員として派遣。
情報セキュリティ責任者（CISO）との緊密な連携により状況を把握するとともに、
NISC、情報セキュリティ関係組織等において認知した関連脅威情報を提供。

リオ組織委における状況

✓ 公式及び多くの関連Webサイトに対する多くのDDoS攻撃やWebアプリケーションへの攻撃試行を認知。一部のWebサイトからの情報窃取等が発生。
- 開会当初は大会関連Webサイトを標的とした攻撃が多く確認されたが、徐々に攻撃の対象が周辺のWebサイトへと移行。
- 認知した攻撃の多くは、SNS等にて攻撃の予告や実施の書き込みが確認された。
- オリンピック開会直後に攻撃のピークを迎えたが、事前の対策、演習等の備えにより迅速に対処し大きな問題は発生しなかった。

＜大会開会後の攻撃対象の遷移＞

✓ 大会公式Webサイト
✓ ブラジルオリンピック委員会・
ブラジルパラリンピック委員会のWebサイト　等

✓ 連邦政府の大会特設Webサイト
✓ 連邦スポーツ省、リオ州・リオ市のWebサイト　等

✓ オリンピック会場の建設事業者のWebサイト　等

＜リオ組織委　技術運用センター内の様子＞

本取組及び今後のブラジル政府からの聴取による知見は
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確保のための取組に反映・応用

リオ大会における状況

関連するサイト等への複数のサイバー攻撃は認知されたものの、
<u>大会運営に支障をきたすような事象は発生しなかった</u>

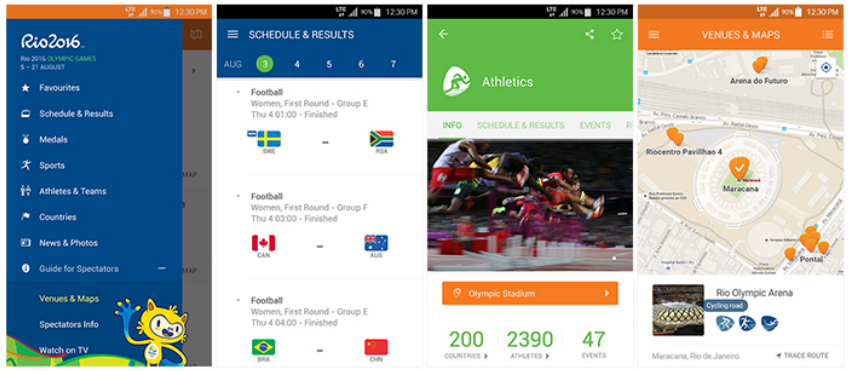
期間中における事案対応等

○事前に想定したサイバーセキュリティ上の
- ✓「OpOlympicHacking」を中心とするハッカー集団
- ✓ サイバー空間におけるリアルテロ等の予告行為
- ✓ ボットネット（多数のマルウェア感染端末）による攻撃

○大会期間中の状況
- ✓ 公式アプリ利用者の想定外のアクセス集中
- ✓ ブラジル国内のハッカー集団の活発な活動。複数の国のグループからも支持表明
- ✓ 選手、プレス等の契約業者向けのWi-Fi等へのマルウェア感染端末の持ち込み

○発生した主な事案
- ✓大会公式Webサイトに対する脆弱性探索や攻撃
- ✓ブラジル連邦、リオ州等の政府機関に対する攻撃及びWebサイトからの情報漏洩
- ✓関連団体のWebサイトに対する攻撃
- ✓OBS（Olympic Broadcasting Services）の Webサイトからの情報漏洩
- ✓公式Webサイトによく似たフィッシングサイト

ハッカー集団による活動



Rio2016公式アプリ

リオ大会における状況

事象① Webサイトへの攻撃

オリンピック・パラリンピック期間中、スポーツ関連のWebサイトに対する攻撃予告や、DDoS攻撃が原因とみられる閲覧不可事象が発生。一部のWebサイトからはデータベース情報等が流出。

攻撃予定時刻の
カウントダウンWebサイト

ハッカー集団によって配布されたDDoS攻撃ツール

国際オリンピック委員会
国際パラリンピック委員会
ブラジルオリンピック委員会
ブラジルパラリンピック委員会
ブラジルスポーツ省
世界反ドーピング機関
スポーツ仲裁裁判所

国際陸上競技連盟
国際ウエイトリフティング連盟
ブラジルサッカー連盟
ブラジルハンドボール連盟
ブラジル近代五種競技連盟
ブラジルボクシング連盟

マイケル・フェルプス公式サイト

攻撃予告や被害があった
スポーツ関連Webサイトの一部

事象② 個人情報の情報漏えい

2016/8/13　世界反ドーピング機関（WADA）が、ロシアの組織的なドーピングを内部告発した選手の個人アカウントが、何者かによってハッキングされていたことを公表。パスワードを入手した第三者が、選手のアカウントを不正に利用していたことを明かした。

2016/9/13　WADAから情報漏えいした、選手の医療情報がインターネット上で公開された。WADAは公式に流出を認めた。後日、日本人選手の情報も公開された。

ハッカー集団が公開したWebサイト

リスクマネジメントの促進のための取組概要

サイバー攻撃等による2020年東京オリンピック・パラリンピック競技大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。
第２回は対象を１都３県に拡大するとともに、横断的リスク評価を実施するために必要な情報について報告いただく。

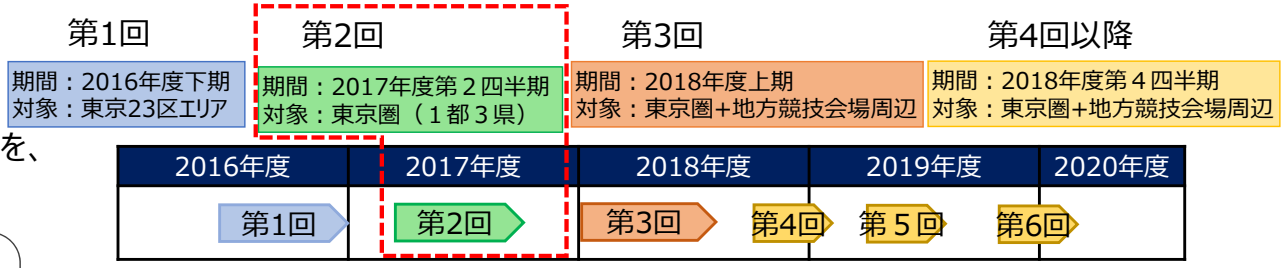
○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成。

○ 東京大会の開催・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。

（通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給　計19分野）

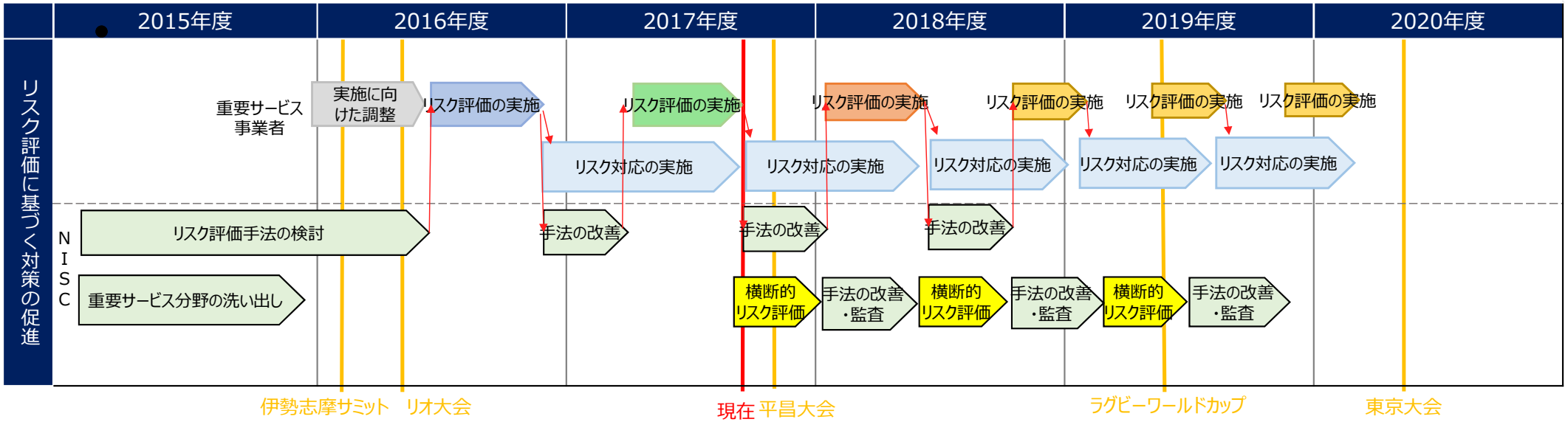
○ 東京大会に向けて、継続的に複数回実施。PDCAサイクルを繰り返す。

○ NISCによる大会全般にわたる横断的リスク評価の実施に向けて、必要な情報の特定や方法の検討を実施。



【横断的リスク評価】

サービスの継続的な確保が滞った場合に、大会への影響が重大なサービスを分野を横断して抽出するとともに、それらのサービスに対して、事業者等が自組織におけるリスク評価で設定した満たすべきサービス水準が妥当であるかを検証。検証結果は、事業者等におけるリスク評価結果の妥当性確認や、大会に向けた訓練等に活用。



リスクアセスメントの全体像

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、

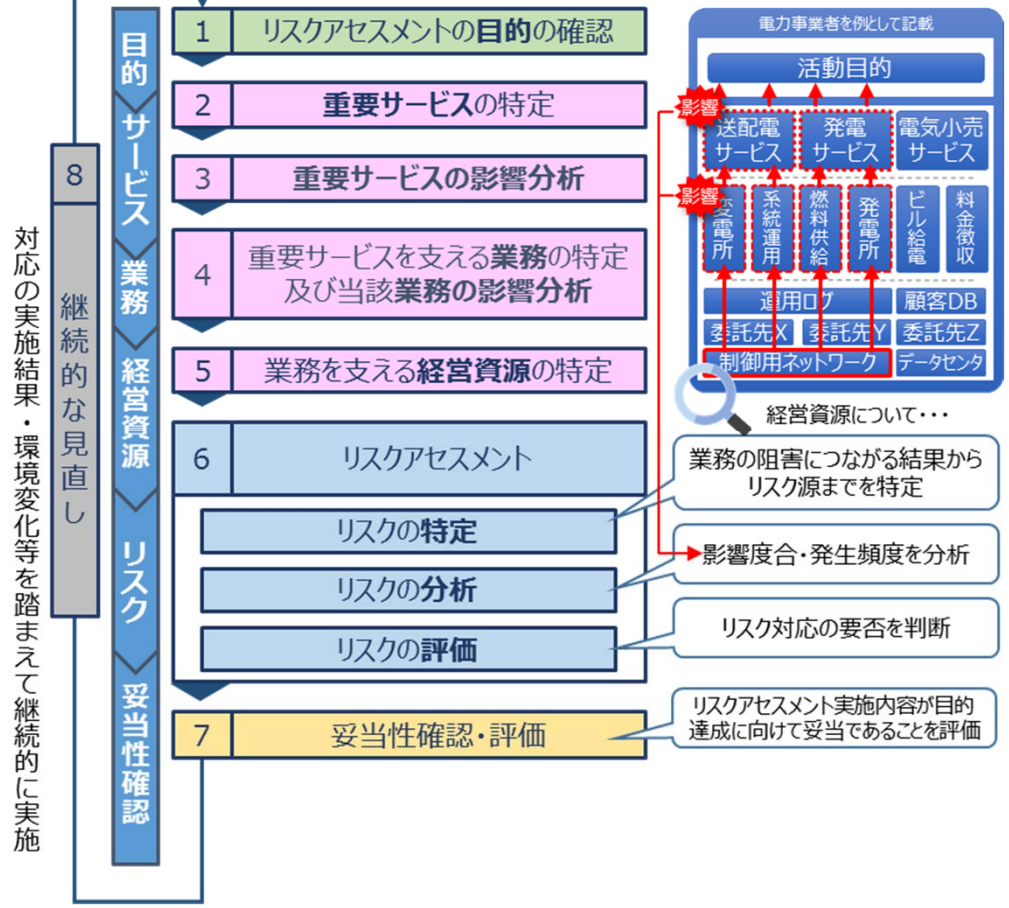
① 大会開催を支える重要なサービス及び必要なサービスレベルを特定し、

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。



2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティ確保に向けたリスク評価への取組状況

◆ 2016年度は、東京23区内の重要サービス事業者等を対象に第１回のリスク評価の取組を実施。
◆ ７月から実施する第２回に向けて、事業者等の拡大および手順・報告事項の見直しを実施。
◆ 今後、横断的な戦略的リスク評価を行い、これに基づくマネジメントを強力に推進。

第１回の取組

＜取組概要＞
○ サイバーセキュリティリスクを特定・分析・評価するための手順書（※）をNISCが作成。
○ 大会の開催・運営に影響を与えうる重要サービス分野を選定し、事業者等にリスク評価の実施を依頼。
※ 手順書をNISCのWebサイトで公開（http://www.nisc.go.jp/active/infra/files/riskhyoka.ZIP）

＜重要サービス事業者等におけるリスク評価の実施状況＞
○ 74組織から実施結果のレポートを受領。
- 多くの事業者等において、前向きな対応がなされたことを確認。
- 各事業者等で部署横断的な取組により実施。
- 大多数の事業者等が、すべての手順の実施を完了。
- 初めてサイバーセキュリティのリスク評価を実施した組織から、「現状と課題を明らかにできた」との回答。

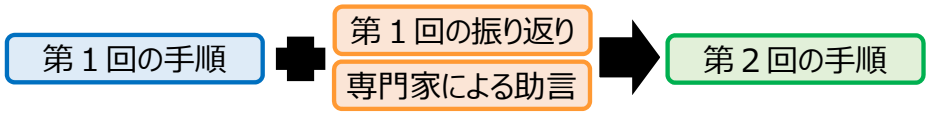
○ 情報交換会等を開催し、事業者等の担当者間の交流を促進。

第１回の実施結果レポートの主な傾向

主な傾向	今後に向けた対応方針
経営層(CISO等)の関与のある組織では、リスク評価の内容が充実。	経営層(CISO等)を含め、組織や関係者を幅広く巻き込むことを促進。
リスク源の選定にばらつき。	より多様な観点から検討できるように、各様式の記入例、業務の阻害につながる事象の結果の例、結果を生じうる事象（脅威）の例を充実化。

第２回の取組

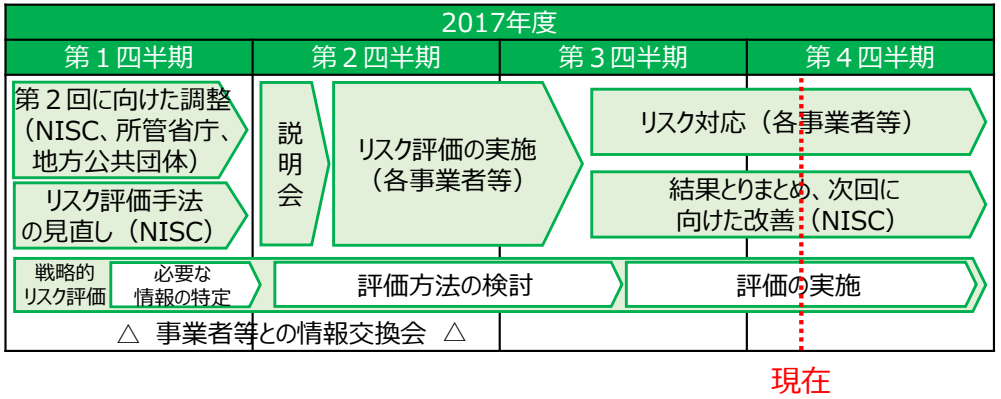
○ 第１回の振り返り、専門家による助言等を踏まえ、リスク評価の手順を充実化。
- 2012年ロンドン大会のサイバーセキュリティ責任者らの助言をもとに、過去大会の知見を反映。



○ 大会全般にわたる横断的な戦略的リスク評価の実施に向けて、必要な情報の特定や評価手法の検討を国として実施。
○ 継続的に事業者等の担当者間の情報交換を促進する機会を設定。

＜重要サービス事業者等におけるリスク評価の実施状況＞
○ 130組織から実施結果のレポートを受領
・現在、実施結果を取りまとめ中

第２回の実施スケジュール



重要サービス事業者等を対象とした情報交換会

情報交換会の概要

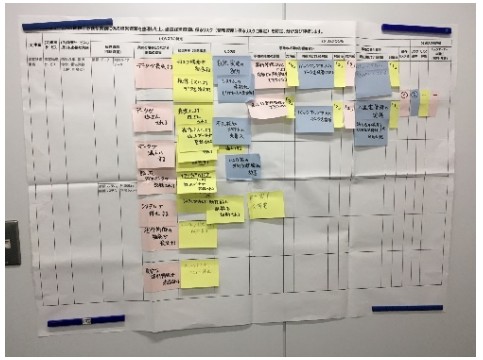
今年度より新たにリスクアセスメントに加わった組織・事業者を含めて、第2回アセスメントの効率的・効果的な実施の促進とそのための必要な情報提供をするともに、同業分野との交流の場を提供し、意見交換の促進を図ることを目的として、重要サービス事業者等を対象とした情報交換会を実施。

日時：平成29年９月19日
主な内容：
- **輸送運営計画に関する講演**
  （東京オリンピック・パラリンピック競技大会組織委員会）
- **ワークショップ**（内閣サイバーセキュリティセンター）

参加実績：重要サービス事業者：38組織（61名）

ワークショップの概要

目的：リスクアセスメントにおいて重要サービス事業者等間のディスカッションを通じて、
①リスクアセスメントの手順に対する理解を深める
②同業分野の事業者間の人的ネットワークの構築・醸成する
方法：グループごとにリスクの特定、分析、評価に取り組んでいただく。（**グループワーク**）
題材：**鉄道業の模擬事業者についてリスクアセスメント**を行う。
内容：
- 概要説明
- グループワーク
  ・リスクの特定①　（業務の阻害につながる事象の結果の検討）
  ・リスクの特定②　（結果を生じ得る事象、リスク源の検討）
  ・リスクの分析
  ・リスクの評価
- グループ内で認識した主要リスクの全体共有
- 解説


グループワークの結果

リオデジャネイロオリンピック・パラリンピック競技大会における日本政府の取組

● 大会準備期間

ブラジル連邦政府機関、ブラジル国内のサイバーセキュリティ関連機関、リオ大会組織委員会、大会に関連するサイバーセキュリティ関連企業等の**リオ大会関係者を複数回にわたって訪問**。

リオ大会に関連するサイバーセキュリティ対策全般、大会期間中の対処体制の準備、事前の訓練等の状況について詳細に**ヒアリングを実施**するとともに**信頼関係を醸成**。

● 大会開催期間中

リオ大会組織委員会との合意に基づき、組織委内のセキュリティオペレーションセンターに**リエゾン２名を派遣**し、**日本からの情報提供を実施**するなど、**大会全日程期間のオペレーションに参画**。

併せて、セキュリティオペレーションセンター内において**大会関連サイバーセキュリティ関連企業と緊密な情報交換**を実施。

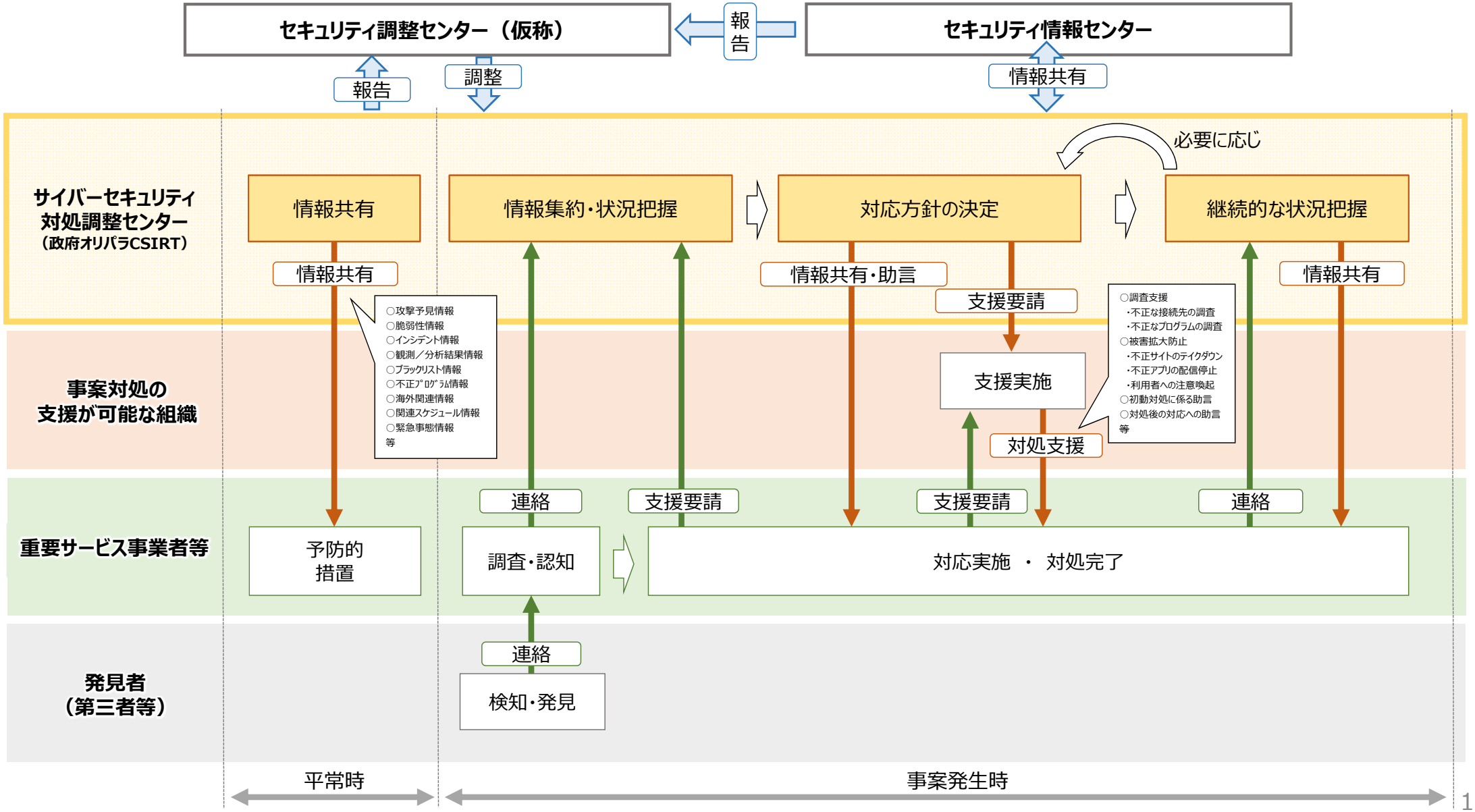
● 大会閉会後

リオ大会期間中の状況の整理のため、**大会関連サイバーセキュリティ関連企業等と緊密な情報交換**を実施。

また、ブラジル連邦政府機関、ブラジル国内のサイバーセキュリティ関連機関、リオ大会組織委員会、大会に関連するサイバーセキュリティ関連企業等の**リオ大会関係者を 訪問し、大会終了後の教訓事項のヒアリングを実施**。

サイバーセキュリティ対処調整センター（政府オリパラCSIRT）のイメージ

◆ セキュリティ調整センター（仮称）等との緊密な連携の下、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織。
- ➢ 関係組織の攻撃予見情報・脆弱性情報・事案情報等を情報共有システムを通じて集約し、迅速に共有。
- ➢ 事案対処のための支援が必要な組織に対して、適切かつ円滑に対処を調整。



ご清聴ありがとうございました。

内閣官房　内閣サイバーセキュリティセンター(NISC)
東京オリパラチーム　企画官
雲田　陽一