資料安信作3－6

重要インフラのサイバーセキュリティについて

総務省　サイバーセキュリティ統括官室

サイバーセキュリティ政策の推進体制

1

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　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
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
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 ※1
有識者※2（８名；10名以下）

閣僚が参画

遠藤　信博　日本電気株式会社取締役会長
小野寺　正　ＫＤＤＩ株式会社相談役
後藤　厚宏　情報セキュリティ大学院大学学長
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
前田　雅英　日本大学大学院法務研究科教授
宮澤　栄一　株式会社デジタルハーツホールディングス取締役会長
村井　純　慶應義塾大学環境情報学部教授

※1 平成27年７月22日付け内閣総理大臣決定により本部員に指定
※2 令和元年6月25日現在

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 | ｻｲﾊﾞｰｾｷｭﾘﾃｨ対策推進会議（CISO等連絡会議）

（事務局）

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

橋本大臣

連携

サイバーセキュリティ協議会
官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

＜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、空港）

＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

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）
上席サイバーセキュリティ分析官
サイバーセキュリティ参与
政府関係機関・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

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）

「サイバーセキュリティ基本法」の概要

（平成26年11月、第187回国会（臨時会）において成立。平成28年、平成30年改正後）

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、強靭な体制の構築

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）

■サイバーセキュリティ協議会を組織（第17条）

■犯罪の取締り及び被害の拡大の防止（第18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19条）

■産業の振興及び国際競争力の強化　（第20条）

■研究開発の推進等（第21条）

■人材の確保等（第22条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第23条）

■国際協力の推進等（第24条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置（第25条）

■所掌事務等（第26条）
⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査等の実施

■組織等（第27条～第30条）
⇒内閣官房長官を本部長として、副本部長（国務大臣）、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、総理が指定する国務大臣、有識者本部員で構成

■事務の委託（第31条）
⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

■資料提供等（第32条～第37条）

第Ⅴ章．罰則

■罰則（第38条）
⇒戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

「サイバーセキュリティ基本法」における位置づけ

（基本理念）

第三条　サイバーセキュリティに関する施策の推進は、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による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、**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をいう。**以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

（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。

（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。

「サイバーセキュリティ戦略」（平成30年7月27日 閣議決定）の全体概要

中長期的

戦略期間（2018～2021年（3年間））

1 策定の趣旨・背景

1．1． サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

1．2． 2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2 サイバー空間に係る認識

2．1． サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。様々な分野で当然に利用され、人々に豊かさをもたらしている。

※：Internet of Thingsの略

2．2． サイバー空間における脅威の深刻化

・技術等を制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3 本戦略の目的

3．1． 基本的な立場の堅持

（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3．2． 目指すサイバーセキュリティの基本的な在り方

（1）目指す姿（持続的発展のためのサイバーセキュリティ（「サイバーセキュリティエコシステム」）の推進）（2）主な観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）

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

1．新たな価値創出を支えるサイバーセキュリティの推進

<施策例> 経営層の意識改革の促進（「費用」から「投資」へ）

・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）

・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

2．多様なつながりから価値を生み出すサプライチェーンの実現

<施策例> 中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定

3．安全なIoTシステムの構築

<施策例> IoTシステムにおけるセキュリティの体系の整備と国際標準化

・IoT機器の脆弱性対策モデルの構築・国際発信

等

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組

<施策例> ・脅威に対する事前の防御（積極的サイバー防御）策の構築

・サイバー犯罪への対策

2．官民一体となった重要インフラの防護

<施策例> ・安全基準等の改善・浸透（サイバーセキュリティ対策の関係法令等における保安規制としての位置付け）

・地方公共団体のセキュリティ強化・充実

3．政府機関等におけるセキュリティ強化・充実

<施策例> ・情報システムの状態のリアルタイム管理の強化

・先端技術の活用による先取的対応への挑戦

4．大学等における安全・安心な教育・研究環境の確保

<施策例> ・大学等の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組

<施策例> ・サイバーセキュリティ対処調整センターの構築の推進

・成果のレガシーとしての活用

6．従来の枠を超えた情報共有・連携体制の構築

<施策例> ・多様な主体の情報共有・連携の推進

7．大規模サイバー攻撃事態等への対処態勢の強化

<施策例> ・サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化

等

国際社会の平和・安定及び我が国の安全保障への寄与

1．自由、公正かつ安全なサイバー空間の堅持

<施策例> ・自由、公正かつ安全なサイバー空間の理念の発信

・サイバー空間における法の支配の推進

2．我が国の防御力・抑止力・状況把握力の強化

<施策例> ・国家の強靭性の確保（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）

・サイバー攻撃に対する抑止力の向上（①実効的な抑止のための対応、②信頼醸成措置）

・サイバー空間の状況把握の強化（①関係機関の能力向上、②脅威情報連携）

3．国際協力・連携

<施策例> ・知見の共有・政策調整

・事故対応等に係る国際連携の強化

・能力構築支援

等

横断的施策

人材育成・確保 <施策例> 戦略マネジメント層の育成・定着、実務者層・技術者層の育成（高度人材含む）、人材育成基盤の整備、政府人材の確保・育成の強化、国際連携の推進

研究開発の推進 <施策例> 実践的な研究開発の推進（検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備）、AI等中長期的な技術・社会の進化を視野に入れた対応

全員参加による協働 <施策例> サイバーセキュリティの普及啓発に向けたアクションプランの策定、国民への情報発信（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5 推進体制 本戦略の実現に向け、サイバーセキュリティ戦略本部の下、内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。施策が着実かつ効果的に実施されるよう必要な予算の確保と執行を図る。 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」（H29.4.18決定 H30.7.25改定）の概要①

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、サイバー攻撃や自然災害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（１４分野）

- 情報通信
- 金融
- 航空
- 空港
- 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、空港、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

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

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推進

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

出典：内閣官房内閣サイバーセキュリティセンター作成資料

「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」（H29.4.18決定 H30.7.25改定）の概要②

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、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し、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ 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る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次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。

◆ 機能保証のため、情報系（ＩＴ）に限らず、制御系（ＯＴ）を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 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。

３．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

① 先導的取組の推進(クラス分け)

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

② オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③ リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

４．本行動計画の期間

➢ 第４次行動計画はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

出典：内閣官房内閣サイバーセキュリティセンター作成資料

重要インフラ セプター一覧（14分野・19セプター）

2019年3月末日現在

重要インフラ分野	情報通信			金融				航空	空港	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	空港	鉄道	電力	ガス	政府・地方公共団体	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 銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空CEPTOAR	空港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
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 日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部経営企画・法務グループ	(一社)日本損害保険協会 ＩＴ推進部 品質管理グループ	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術ユニット	地方公共団体情報システム機構 情報化支援戦略部	(公社)日本医師会 情報システム課	(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（のべ数）	23社 1団体	335社 1団体	197社・団体	1,386社	269社 7機関	41社	46社	14社 1団体	8社	22社 1団体	14社 3機関	10社・団体	47 都道府県 1,741 市区町村	1グループ 18機関	8水道事業体	6団体 17社	13社	51社	12社
NISCからの情報の展開先（構成員以外）	407社・団体	411社	12社	3社・団体	—	—	—	—	—	—	14社・機関	182社・団体	—	379社	内容に応じ1,343事業体へ展開	—	—	—	—
その他（核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等（内容に応じ展開先を選定））																			

■ その他	
既存事業領域を越える連携等	情報通信（ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟）、金融（金融ISACにおいて、加盟金融機関間で情報共有・活動連携）、電力（電力ISACにおいて、加入する電気事業者間で情報共有・活動連携）、化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者への拡張）、制御システム（JPCERT/CCが提供するConPaS等）、J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報CISTA（JPCERT/CC：セキュリティ情報全般）

出典：内閣官房内閣サイバーセキュリティセンター作成資料

＜サイバー攻撃の事例１＞ サイバー攻撃によるウクライナ停電

■ サイバー攻撃によりエネルギー供給が停止した初の事例
2015年12月23日　変電所の遮断機切断で最大6時間の停電発生（ウクライナ）
2016年12月17日　変電所の遮断機切断で1時間15分の停電発生（ウクライナ）

2015年
【概　要】
①標的型メール攻撃（ＩＴ系への攻撃）
　マルウエアを含む添付ファイルをメールで送付
→マルウエアに感染させ、長期間の偵察活動で情報を収集
②ＤＯＳ攻撃で電話システムに支障発生（ＩＴ系への攻撃）
→復旧活動を妨害
③遠隔操作で変電所の遮断機を切断（OT系への攻撃）
→最大6時間の停電発生（２２万５千世帯）
※ＵＰＳ（Uninterruptible Power Supply;非常時電源）が動作しないように設定

【被害】 攻撃者は、制御システムを遠隔から手動操作して停電を発生させた

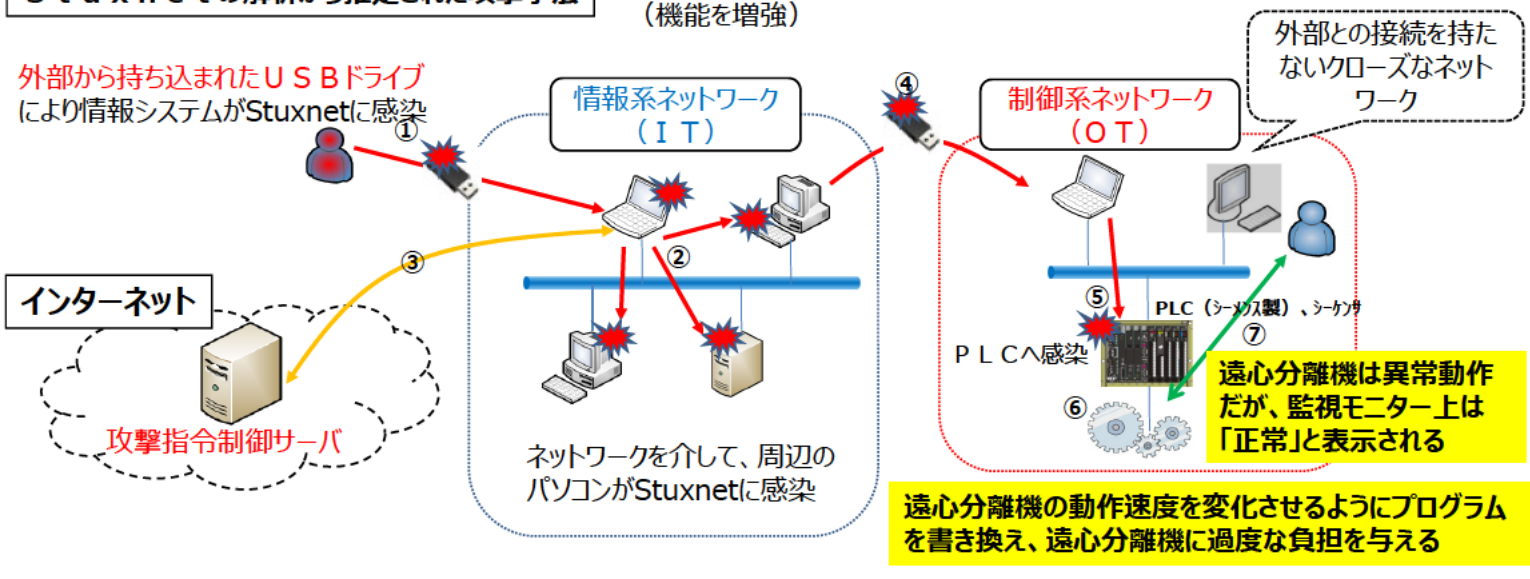
2016年
2015年とほぼ同じ手法だが、ＰＣに感染したマルウェアが発送電設備を直接操作し、
1時間15分の停電発生

＜サイバー攻撃の事例２＞ イラン原子力関係施設への攻撃

■ 2010年7月イランのブシェール原子力発電所及び同年11月イランのウラン濃縮施設がStuxnet（スタックスネット）と呼ばれるコンピュータウイルスによってサイバー攻撃を受けた。
→ 遠心分離機の相当数が稼働不能となり、プロジェクトの大幅遅延となった。

Ｓｔｕｘｎｅｔの解析から推定された攻撃手法

感染したパソコンは、攻撃指令制御サーバと通信を行いStuxnetをアップデート（機能を増強）



クローズドなシステムだからといって、100%安心とは言い切れない

<サイバー攻撃の事例３> 大規模サイバー攻撃　WannaCry

■ 2017年5月12日頃より、ランサムウェア（WannaCry)による被害が世界中で多数発生。

【感染時の画面イメージ】

【ドイツ鉄道】
行先表示装置がWannaCryに感染
→行先案内表示装置を故障扱い

【被害を受けた国】

【概　要】 150か国30万台以上（国内：600カ所以上2000端末以上）のコンピューターに感染、データを暗号化し、使用不能にする。身代金としてビットコインを要求
【攻撃形態】 不審メール開封による感染や、インターネットに接続している端末が感染するなど、Windowsの脆弱性を利用した攻撃
【被害状況】 ルノー（フランス）,Telefonica（スペイン）,FedEx(アメリカ),ドイツ鉄道(ドイツ)など

【対策】
マイクロソフトが3月15日に出したセキュリティ更新プログラム（MS17-010)を適用
セキュリティパッチを適時使用　/　重要データはバックアップ

2020年東京大会に向けた取組状況について

■ サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、大会の運営に大きな影響を及ぼし得る重要サービス事業者 等を対象とした**リスクマネジメントの促進**や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、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としてのサイバーセキュリティ対処調整センターの構築等、**対処態勢の整備**を推進中。

リスクマネジメントの促進

○**取組状況**
手順書を作成するとともに、東京大会において開催・運営に影響を与える重要サービス事業者等を選定し、リスクの低減と最新のリスクへの対応のため、**リスクアセスメント**の実施を依頼。2016年度から2020年６月末まで計６回を予定。第3回目においては、対象の事業者を全国へ拡大、実施結果について横断的に分析し各事業者等にフィードバック。
また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況をNISCが検証する**横断的リスク評価**を実施。2020年３月末までに計３回を予定。第1回目においては、電力、通信、水道、鉄道、放送等から5者を対象に実地検証、全重要サービス事業者等から20者を対象に書面検証を実施。

○**今後の取組**
リスクアセスメントの取組については、重要サービス事業者等のリスクアセスメントにおいて、情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、残存リスクが顕在化した場合の対応体制の強化を促進。
横断的リスク評価の取組については、引き続き、重要サービス事業者等（競技会場(レガシー部分)を含む。）を対象として検証を実施するとともに、競技会場のオーバーレイ部分の対策の整備状況及び監督状況について東京大会組織委員会を対象として検証を実施。

対処態勢の整備（サイバーセキュリティ対処調整センターの構築等）

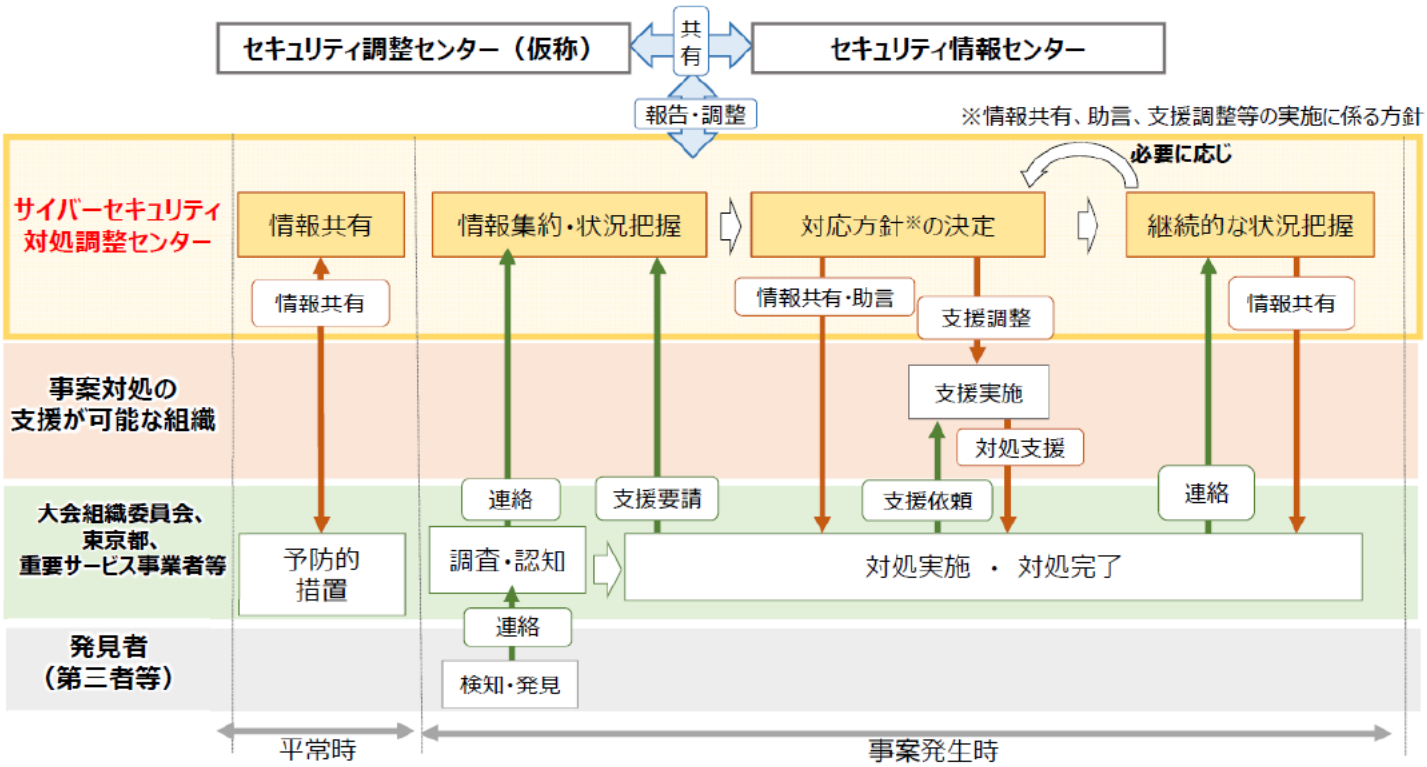
○**取組状況**
情報共有・事案発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議し、**運用方針等を決定**した。また、サイバー脅威情報の提供について４社から協力を受けることを決定するとともに、大会組織委員会、東京都等を交えた机上演習を実施した。
情報共有システムの構築が完了し、2019年４月に**サイバーセキュリティ対処調整センター**を設置した。

○**今後の取組**
サイバーセキュリティ対処調整センターは、大会関係組織と情報共有システムを介した**情報共有**の促進及び**インシデント発生時の対処支援調整**を実施。また、重要サービス事業者等も参加する情報共有及びインシデント発生時の対処支援調整等の**訓練・演習**を実施し、大会関係組織間で緊密に連絡調整を図るための態勢を整備。さらに、大会までの大規模イベント（G20大阪サミット、ラグビーワールドカップ等）において情報共有及びインシデント発生時の対処に係る試験運用を実施。
これらの取組を通じて、大会に向けて万全の対処態勢の整備を目指す。

出典：内閣官房内閣サイバーセキュリティセンター作成資料

サイバーセキュリティ対処調整センターについて

■ 2020年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のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する対処支援調整を実施。



出典：内閣官房内閣サイバーセキュリティセンター作成資料