NISC National center of Incident readiness and Strategy for Cybersecurity

日本のサイバーセキュリティ戦略

～　現状と課題　～

2019年7月4日

内閣サイバーセキュリティセンター
副センター長
山内　智生

日本のサイバーセキュリティ政策の枠組みとNISC

- サイバーセキュリティ基本法
  - 「サイバーセキュリティ」の法的定義
  - サイバーセキュリティ戦略の位置付け
  - サイバーセキュリティ戦略本部（以下「戦略本部」）の権限と任務
    戦略本部は関係大臣と有識者から構成
- NISC（内閣官房に所属）は、戦略本部の事務局として、次のような任務を実施
  - 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
    - **サイバーセキュリティ戦略の案の作成と実施の推進**
    - 重要インフラ防護のための政策
    - 政府機関等の情報システムについての統一基準群の作成と監査
    - サイバーセキュリティに関する人材育成に関する戦略
    - サイバーセキュリティに関する研究開発に関する戦略　　等
  - 政府CSIRTとして、政府機関に対するサイバー攻撃を常時、監視、分析、対処
  - CYMATを通じて、重大な事象が生じた場合の政府機関への支援

サイバーセキュリティ政策の推進体制

NISC

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※
有識者（8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締役会長
- 小野寺　正　ＫＤＤＩ株式会社取締役相談役
- 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

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）

（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

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、空港）

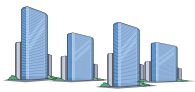
＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

- 警察庁（サイバー犯罪・攻撃の取締
- 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

目指す姿（持続的な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」の実現）

○　新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（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）から、官民のサイバーセキュリティに関する取組を推進していく。

※　狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（未来投資戦略2017より）

＜サイバーセキュリティの基本的な在り方のイメージ＞

サイバーセキュリティ戦略(2018年７月27日閣議決定)

NISC

- ◆ サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの
- ◆ サイバーセキュリティ2018は、同戦略に基づく初めての年次計画であり、各府省庁はこれに基づき、施策を着実に実施

＜全体構成＞

1　策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- 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

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービス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・社会的損失が生ずる可能性は指数関数的に拡大

3　本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な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。３つの観点（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）からの取組を推進

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

～新たな価値創出を支えるサイバーセキュリティの推進～

- ■ 新たな価値創出を支えるサイバーセキュリティの推進
- ■ 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
- ■ 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- ■ 国民・社会を守るための取組
- ■ 官民一体となった重要インフラの防護
- ■ 政府機関等におけるセキュリティ強化・充実
- ■ 大学等における安全・安心な教育・研究環境の確保
- ■ 2020年東京大会とその後を見据えた取組
- ■ 従来の枠を超えた情報共有・連携体制の構築
- ■ 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- ■ 自由、公正かつ安全なサイバー空間の堅持
- ■ 我が国の防御力・抑止力・状況把握力の強化
- ■ 国際協力・連携

横断的施策

- ■ 人材育成・確保
- ■ 研究開発の推進
- ■ 全員参加による協働

5　推進体制　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、同センターが調整・連携の主導的役割を担う。

サイバーセキュリティ協議会

サイバーセキュリティ基本法の一部を改正する法律が成立

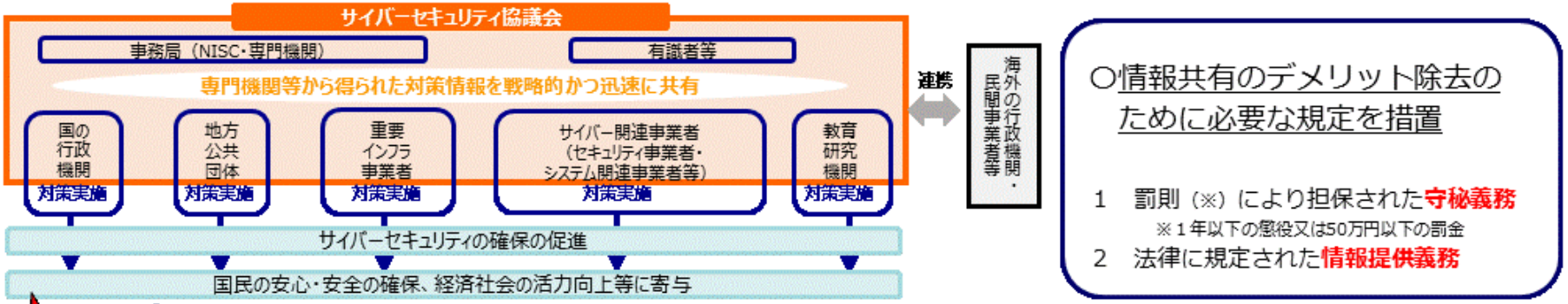
～民間企業等が情報共有をためらう要因となっているデメリットを、法律上の措置によって除去～

※ 平成31年（2019年）4月1日施行

概要

・官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための**協議会を創設**※

・**構成員に対して守秘義務及び情報提供義務を適用する**等の措置を講ずる。　※サイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣が組織



○情報共有のデメリット除去のために必要な規定を措置

1　罰則（※）により担保された**守秘義務**
※１年以下の懲役又は50万円以下の罰金

2　法律に規定された**情報提供義務**

サイバーセキュリティ協議会の運用ルール案　～デメリットの除去に加え、協議会の運用ルールにより情報提供を行うメリットを付加～

背景	**デメリット除去を法改正によって措置することは不可欠**だが、それだけでは情報提供を促進する**インセンティブにならない**ため、情報提供を行う**メリットを増加させることも重要**
解決策（運用ルール案）	提供者の**モチベーション**と提供される**情報の質**を維持するため、積極的な情報提供に**能力**と**意欲**を有する者を、一般の構成員と別に、**タスクフォース**としてグループ化
タスクフォースのメリット	○ 提供した未確定の情報に対して**相互にフィードバックを行う**ことで、**提供した情報の確度を高めることができる**。 ○ 各主体がフィードバックだけでなく、自らも積極的に情報を提供する**ギブアンドテイクの原則を徹底**することで、**タスクフォースのみに共有される情報を得ることができる**。

サイバーセキュリティ協議会　※改正法中、「協議会の組織及び運営に関し必要な事項は協議会が定める」としており、協議会の運用ルール（規約）を整備。

構成員の役割

タスクフォース
未確定の情報を相互にフィードバックを行い、速やかに対策情報等を作出する
※専門機関、セキュリティベンダ等

対策情報等の情報提供

一般の構成員
基本的に、作出された対策情報等を受領し、自らの組織の対策に役立てる
※国の行政機関、地方公共団体、重要社会基盤事業者等

2019年４月１日、サイバーセキュリティ協議会が組織され、同日から10日にかけて、構成員の募集を行い、**５月17日、構成員を決定**

政府機関における情報集約・支援体制の枠組み

NISC

政府機関
情報セキュリティ横断監視・即応調整チーム（第一GSOC）

2008年４月　GSOCの運用を開始
2009年１月　２４時間対応開始
2017年４月　第３期GSOC運用開始

第一GSOC
（NISC）

リアルタイムの横断的な監視

的確かつ迅速な警告・助言による情報共有

不正プログラムの分析・各種脅威情報の収集

第二GSOC
（IPA）

2017年４月　第二GSOC運用開始

独立行政法人等
情報セキュリティ横断監視・即応調整チーム（第二GSOC）

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

独立行政法人等　組織内CSIRT
第二GSOC担当　等

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
A省 CSIRT
B省 CSIRT
D指定法人 CSIRT
C独法 CSIRT

対処

NISC/IPA

情報連携の結節点

連携・情報交換

民間CSIRT 等

出動要請

技術的な支援・助言

相互連携

支援

情報セキュリティ緊急支援チーム（CYMAT）
2012年６月29日　設置

要員：各府省庁から派出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）

*CYMAT : CYber incident Mobile Assistance Team

*CSIRT : Computer Security Incident Response Team

IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ等について

■ サプライチェーン・リスクとは

- 情報通信機器等の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念。
- さらに、納入後においても、情報システムの特徴として、事後的な運用・保守作業により、製造業者等が修正プログラムを適用する等、調達機関が意図しない、不正な変更が行われる可能性。

■ サプライチェーン・リスク対策の重要性

- 「サイバーセキュリティ戦略」において、サプライチェーン・リスク対策の重要性について言及。
- 「政府統一基準群」において、サプライチェーン・リスク対策に係る考え方を記載。

～ 政府機関等の対策基準策定のためのガイドラインの解説（遵守事項5.1.2(1)(a)”「不正な変更が加えられない」について”に係る解説）から抜粋 ～

「開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。」

■ 「サプライチェーン・リスク対策」のより具体的な方策として全省庁による「申合せ」を決定。

（平成３０年１２月１０日　サイバーセキュリティ対策推進会議（第16回）各府省情報化統括責任者連絡会議（第81回）合同会議）

１．適用対象
国家安全保障・治安関係業務を行うシステム等、重要性の観点から５類型を提示。

２．適用時期
平成31年度予算に基づき平成31年４月１日以降に調達手続（公告等）が開始されるもの。

３．調達手続の流れ
- 「総合評価落札方式」や「企画競争」等を用い、RFIやRFPといった事前の情報取得や、審査の過程において、必要な情報を入手し評価することにより、サプライチェーン・リスク対策を実施。
- 必要に応じて、情報通信技術（ＩＴ）総合戦略室及び内閣サイバーセキュリティセンターから、講ずべき必要な措置について助言を実施。

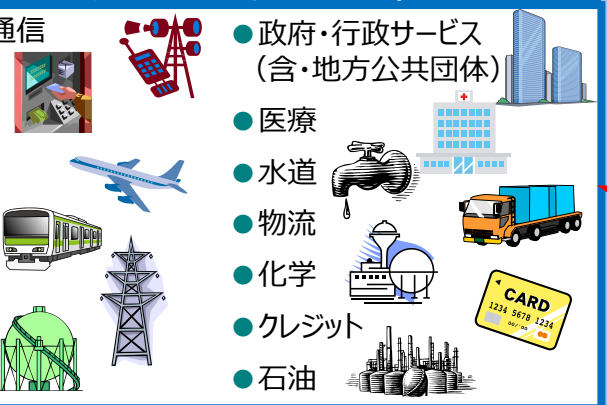
重要インフラの情報セキュリティ対策に係る第４次行動計画

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、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