NISC National center of Incident readiness and Strategy for Cybersecurity

草の根活動に期待すること

平成31年３月14日

内閣官房　内閣サイバーセキュリティセンター（ＮＩＳＣ）
参事官　吉田 恭子

サイバーセキュリティ戦略の概要

平成30年７月27日
閣 議 決 定

◆ 新たなサイバーセキュリティ戦略(2018年７月)は、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

＜新戦略(2018年戦略)（平成30年7月27日閣議決定）の全体構成＞

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。

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＞

①サービス提供者の任務保証
- 業務・サービスの着実な遂行 -
Mission Assurance

- 自らが遂行すべき業務やサービスを「任務」と捉え、これを着実に遂行するために必要となる能力及び資産(*)の確保
- 一部の専門家に依存するのではなく、「任務」の遂行の観点から、その責任を有する者が主体的にサイバーセキュリティ確保に取り組む

＊：人材、装備、施設、ネットワーク、情報システム、インフラ、サプライチェーンを含む

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–
Cybersecurity Ecosystem

全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を、持続的に発展していく一種の生態系にたとえて、「サイバーセキュリティエコシステム」と呼称する。

②リスクマネジメント
- 不確実性の評価と適切な対応 -
Risk Management

- 組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応

③参加・連携・協働
- 個人・組織による平時からの対策 -
New　Cyber Hygiene

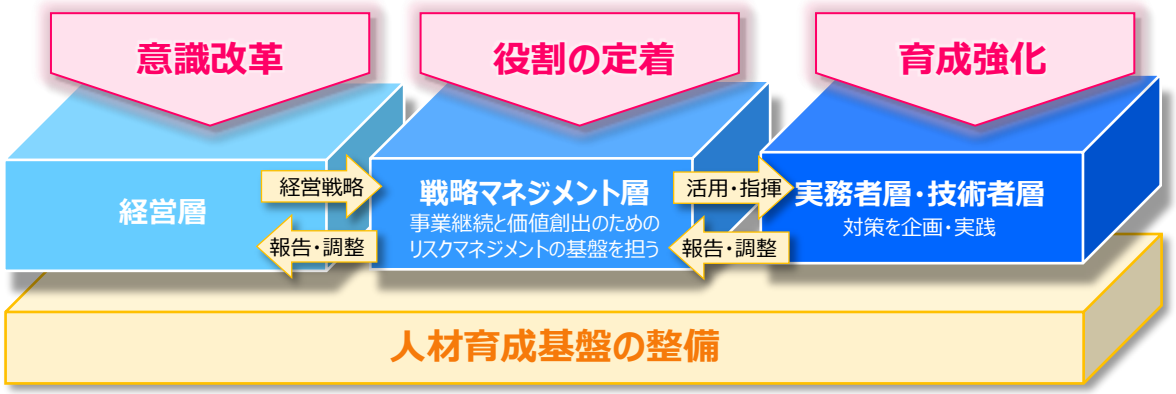
- サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が平時から講じる基本的な取組
- 平時・事案発生時の、各々の努力だけでない、情報共有、個人と組織間の相互連携・協働を新たな「公衆衛生活動」と捉える

サイバーセキュリティに関する共通基盤的な取組の推進

サイバーセキュリティを支える基盤的取組として、横断的・中長期的な視点で、人材育成・確保や研究開発に取り組むとともに、
サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組むような全員参加による協働を推進

１．人材育成・確保

- 「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
- 人材育成基盤の整備、国際連携の推進
- 各府省庁のセキュリティ人材の確保・育成強化

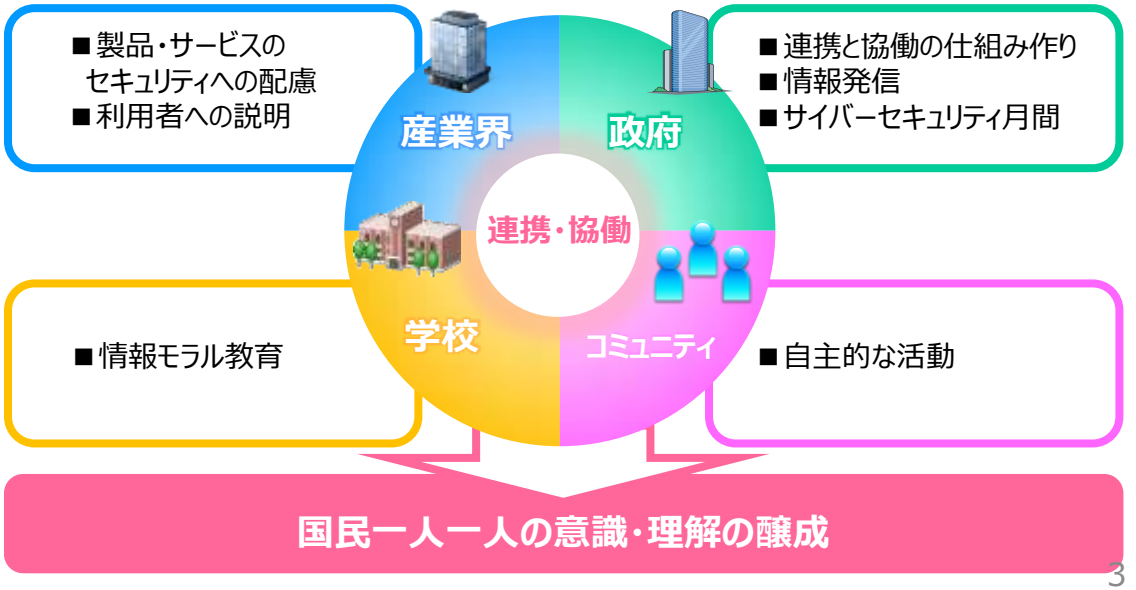


２．研究開発の推進

- 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等）
- 中長期的な技術・社会の進化を視野に入れた対応

３．全員参加による協働

- 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とそれに基づく連携・協働
- 「サイバーセキュリティ月間」などを通じた情報発信



「サイバーセキュリティ意識・行動強化プログラム」（概要）

2019年（平成31年）１月24日
サイバーセキュリティ戦略本部決定

1　はじめに

「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、普及啓発について、2020年東京オリンピック・パラリンピック競技大会を見据えつつ、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、本プログラムを策定。

2　現状

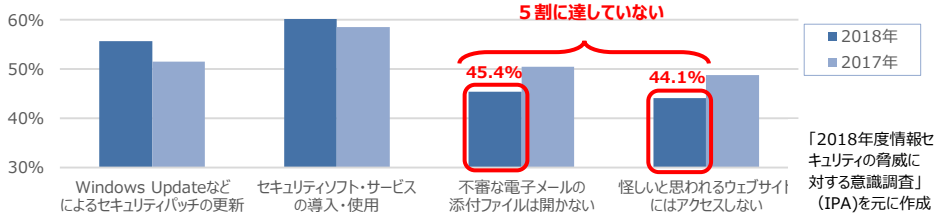
①個人：**AIやIoTの「生活」への浸透**に伴い、インターネット利用への**不安感が拡大。**一方、**具体的な対策の実施に十分に結びついていない。**

②企業：**中小企業では、特に規模の小さい企業ほど**担当者が置かれない場合も多いなど、**取組が遅れている。**

＜インターネットの利用に関連するトラブルへの不安感＞

(出典)インターネットの安全・安心に関する世論調査（内閣府、2018年11月）

＜セキュリティ対策の実施状況＞



「2018年度情報セキュリティの脅威に対する意識調査」（IPA)を元に作成

3　今後の取組の基本的な考え方

・対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、いわば「**サイバーセキュリティのラストワンマイル**」の状況。

・「３つの視点」から取組を推進：①**継続的な実施**、②対象に合わせた**適切なツール・コンテンツの提供**、③**関係者間の連携**の促進

4　具体的取組の推進

(1) 基本的な対策の徹底

・個人や企業が**取組の必要性を自覚し、当たり前のこととして取組を講じる**状態を目指し、**必要な対策を継続的に伝える**

（取組の一例）
「インターネットを安全に利用するための情報セキュリティ対策９か条」（2015年2月 NISC・IPA）の各種取組への浸透

(2) 重点的な対象とその内容

・**様々な対象に幅広く実施することを前提**としつつ、以下の対象について、**重点的に取組を実施**

①**中小企業**　中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、「SECURITY ACTION」活用の促進、中小企業支援ネットワークによる啓発等

②**若年層**　無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、先端的人材育成施策の推進

③**地域における取組の支援**　産学官連携型の取組の活性化、高専学生によるボランティア活動等

高専学生によるボランティア活動（提供：警察庁）

(3) 情報発信・相談窓口の充実

・**最新の脅威の情報・対策の適時かつ迅速な発信**や**相談できる窓口の確保**等、自ら取り組むための環境を整備

（取組の一例）NISCにおけるSNSによる情報発信

5　連携体制の強化

・**NISCをはじめとした関係機関が連携**し、ラストワンマイルに情報が行き着くよう配慮しつつ取組を推進
①**ポータルサイトによる取組の見える化・連携推進**　②ツール・コンテンツの共有　③サイバーセキュリティ月間の推進　④国際的連携の強化、⑤**ＰＤＣＡによる継続的改善**

・**官民の様々な取組を集約するポータルサイト**を構築し、**対象となる層や伝達手法の見える化及び連携を推進**

・個別施策の実施状況に加え、**個人や企業の対策の実施状況**等を分析し、本プログラムの**内容・効果の定期的な評価、見直しを実施**

（参考）官民の取組状況 （１/２）

- 現在、官民の様々な主体が各世代・各組織に向けて幅広く普及啓発の取組を実施。
- これらを大きく「セミナー・イベント」、「ツール・コンテンツの提供」、「タイムリーな情報発信」に分類すると、主に以下のような取組が実施されている。

民間における取組

公的機関における取組

対象 / 手法	個人			組織				
	若年層	就労世代	高齢者	小規模企業者	中小企業	大企業	教育機関	地方自治体
セミナー、イベント等	サイバーセキュリティ月間イベント（NISC）							
	各地におけるイベント等（警察庁、都道府県警察）							
	サイバーセキュリティセミナー等の開催（総務省等）							
	電子署名及びトラストサービスに関する普及啓発（総務省、法務省、経済産業省）							
	ネットモラルキャラバン隊の実施（文部科学省）			中小企業支援機関向け講師派遣（経済産業省、IPA）				
	ひろげよう情報モラル・セキュリティコンクール（経産省、IPA）	情報モラル教育の推進（指導者セミナー開催）（文部科学省）		講習能力養成セミナー（経済産業省、IPA）				
		学校教育の情報化指導者養成研修（NITS、文部科学省）			JPCERT/CCによる情報共有会（経済産業省）		インターネット安全教室（経済産業省、IPA、JNSA）	
	インターネット安全教室（経済産業省、IPA）				フィッシング対策セミナー（経済産業省、フィッシング対策協議会、JPCERT/CC）			
	e-ネットキャラバン（FMMC、総務省、文部科学省）			関西におけるサイバーセキュリティ人材育成、意識醸成（近畿経済産業局、近畿総合通信局、関西情報センター）				
	標語募集（FMMC、総務省、文部科学省）			セミナー、研修、勉強会、演習の開催（JASA）				
	情報セキュリティサポーター・マイスターの育成、ミーティング（SPREAD）				JC3フォーラム（JC3）			JC3フォーラム（JC3）
		全国大会（Grafsec）				経営トップセミナー、経営宣言（経団連）		
	地域の各団体によるイベントや勉強会の開催（Grafsec助成事業）					トップ層会合（CRIC CSF）		
	セミナーやイベント、コンテスト開催（JNSA）							
	学生向けセミナー（CRIC CSF）			制御システムセキュリティカンファレンス（JPCERT/CC）				

※情報セキュリティ社会推進協議会に参画している一財、一社、NPO等を中心に記載

（参考）官民の取組状況（2/2）