NISC National center of Incident readiness and Strategy for Cybersecurity

その１

新たなサイバーセキュリティ戦略について

平成30年8月21日

内閣官房　内閣サイバーセキュリティセンター（NISC）
内閣審議官　三角 育生

サイバーセキュリティ基本法※の概要（平成28年改正後）

※平成26年11月12日公布。平成27年１月９日全面施行

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、強靱な体制の構築
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）**

■**犯罪の取締り及び被害の拡大の防止（第17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18条）**

■**産業の振興及び国際競争力の強化（第19条）**

■**研究開発の推進等（第20条）**

■**人材の確保等（第21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22条）**

■**国際協力の推進等（第23条）**

第Ⅳ章．サイバーセキュリティ戦略本部

■**設置（第24条）**

■**所掌事務等（第25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26条～第29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30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31条～第36条）**

第Ⅴ章．罰則

■**罰則（第37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

新たなサイバーセキュリティ戦略

（平成30年７月27日閣議決定）

サイバーセキュリティ戦略・サイバーセキュリティ2018の概要

- ◆ 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。

現状認識と将来像（サイバー空間と実空間の一体化に伴う脅威の深刻化）

中長期

策定の趣旨・背景

【（2015年戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～

一体化

【サイバー空間と実空間の一体化、活動空間の拡張】

サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR 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**、経済社会活動・国民生活の既存構造に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている**。
・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。
・**IoT機器で得られるデータ**を利用した新たなビジネスやサービスが創出されつつある。

サイバー空間における脅威の深刻化

・サイバー空間における技術・サービスを**制御できなくなるおそれは常に内在しており、多大な経済的・社会的な損失が生じ得る。**
・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性
・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

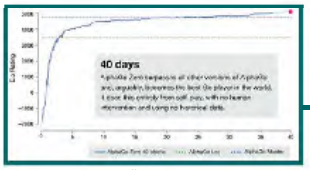
（参考①）AIの進化の経緯

人工知能は、1956年～1960年頃の第一次ブーム、1980年代の第二次ブームを経て、現在、機械学習の一種である深層学習（ディープラーニング）が画像認識において高い能力を見せ始めたことが発端となって期待が高まっている。

考えるのが早い人工知能 → **ものしりな人工知能** → **データから学習する人工知能**


出典：Google Official Blog


出典：GIGAZINE



出典：ZDNet

・**レイ・カーツワイル氏(Google技術責任者)は、2045年にシンギュラリティ(AIが人類の知性を上回る)の実現を予測**

・**棋譜なしに人間を超える能力を持つ囲碁ソフト「AlphaGo Zero」の実現（2017年）**

・**囲碁ソフト「AlphaGo」が韓国トッププロ棋士に勝利（2016年）**

・**ディープラーニング技術を活用しAIが「猫」を認識（2012年）**

・ワトソンがクイズ番組で勝利（2011年）

・Deep Blueがチェスで勝利（1997年）

【第３次AIブーム】
ウェブとビッグデータの発展
計算機の能力向上
（2013年~）

・福島邦彦氏による脳科学研究に基づくネオコグニトロン（※）の発表（1979年）
※視覚パターン認識に関する階層型神経回路モデル。畳み込みニューラルネットワーク（CNN）の原型。

・ダートマスワークショップ（※）（1956）
人工知能（Artificial Intelligence）という言葉が決まる
※人工知能という学術分野を確立した会議

【第２次AIブーム】
「エキスパートシステム」の出現
（1980年代）

冬の時代

【第１次AIブーム】
人工知能（AI）の原型が生まれる
（1956年~1960年代）

冬の時代

・**言語の意味理解：Generating Images(2015.12-)**


A stop sign flying in blue skies.

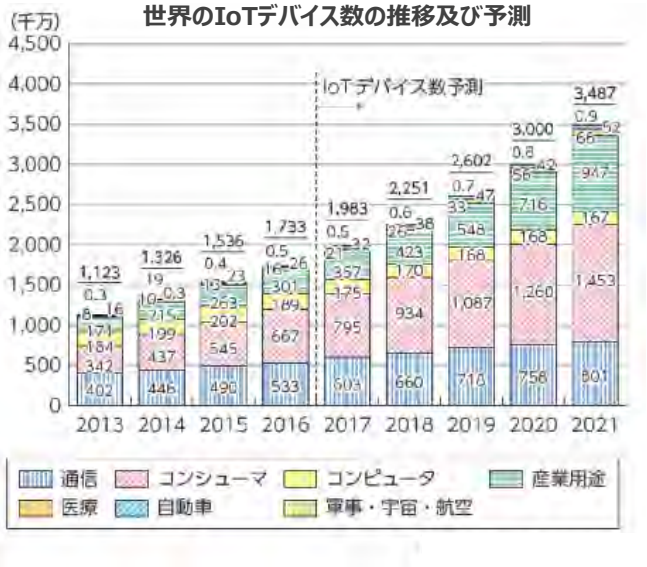
・**（1947年）アランチューリングによって「人工知能の概念」提唱**

出典：Elman Mansimov et. al: “Generating Images from Captions with Attention”, Reasoning, Attention, Memory (RAM) NIPS Workshop 2015, 2015
参考：総務省 情報通信審議会 総会（第37回）「新たな情報通信技術戦略の在り方」第二次中間答申（案）
東京大学　松尾豊氏　人工知能の未来-ディープラーニングの可能性とサイバーセキュリティに対する影響-（サイバーセキュリティ戦略本部　研究開発専門調査会第6回会合発表資料）

（参考②）サイバー空間におけるイノベーションの進展

爆発的に増加するIoT機器

- 2016年時点でインターネットにつながるモノの数は173億個であり、2015年時点の154億個から12.8%の増加と堅調に拡大
- 2020年は約300億と現状の数量の2倍に拡大する見通し



(出典)平成29年版情報通信白書（総務省）（データはIHS Technology作成）

革新的な金融サービスの登場

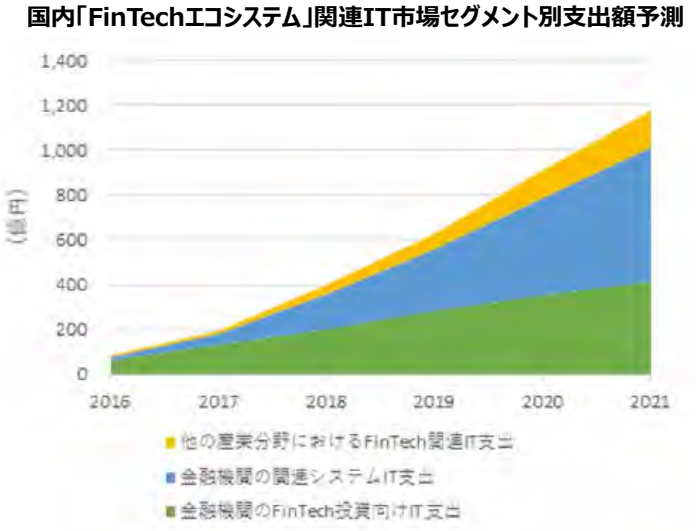
・融資：Web上で貸し手と借り手を募り、Rating等を実施して融資を実現

・決済：ブロックチェーンの技術を活用した決済サービスも登場

・送金：国際送金やP2P送金等のモバイル送金サービス

・資本性資金調達：ベンチャー企業と個人投資家をマッチングさせ資本を調達するサービス

・個人資産管理：アカウントアグリゲーション等により顧客の資産を分かり易く管理



(出典)：2017年国内の金融分野における第３プラットフォーム需要動向調査（IDCジャパン）

【１．策定の趣旨・背景】及び【２．サイバー空間に係る認識】のポイント

サイバー空間における脅威の深刻化に関する事例（国内外のサイバー攻撃等の事案）

【国内】

○民間企業を標的としたOSインジェクション攻撃（2016年4月）

2016年4月20日から同28日にかけて、ソフトウェアの脆弱性を突いたOSインジェクション攻撃により、 民間企業4社（日本テレビ、J-WAVE、栄光ゼミナール、エイベックス）から合計**142万人分の個人情報が流出**する事案が発生した。

○ダークウェブによるクレジットカード情報の取引（2017年4月）

発信元の特定が困難な**「ダークウェブ」と呼ばれるインターネット上のサイトで、日本のクレジットカード会社の利用者約10万人分の個人情報が売買**されていることが海外のセキュリティー会社の調査で分かった。サイバー攻撃を受けた企業などから流出したとみられる。

○金融機関を標的としたDDoS攻撃（2017年9月）

外国為替証拠金取引事業者など**金融事業者を狙ったDDoS攻撃**が継続。一部の事業者では攻撃による被害と障害復旧を公表した。

○仮想通貨の窃取を狙った攻撃（2018年１月）

登録申請中のみなし仮想通貨交換業者が保有していた仮想通貨（NEM）が不正に外部に送信され、**顧客からの預かり資産5億2,300XEM（約580億円）が流出**した。

【海外】

○バングラデシュ銀行（2016年2月）

2016年2月5日、バングラディシュ中央銀行がハッキングを受け、**約8,100万ドル（約91億円）が不正送金**された。ニューヨーク連邦準備銀行のバングラディシュ中央銀行の口座情報が流出し、その口座から他の銀行の口座に送金された模様であり、犯行は銀行が営業していない日に行われた。米国のセキュリティ会社は、攻撃手法は過去に北朝鮮の関与が断定された手法と同様だったと明らかにした。

○ドイツ原子力発電所（2016年4月）

2016年4月、ドイツの原子力発電所で、**燃料棒監視システムにてマルウェアが発見された**。マルウェアとしては、リモートアクセスを行うトロイの木馬と、ファイルを盗み取るマルウェアの2種類が存在していたが、同システムがインターネットに接続されていなかったことから、実質的な被害は出ていないようである。なお、感染対象としては、燃料棒監視システムとUSBメモリ18個

○Miraiによる大規模DDoS攻撃（2016年9月）

IoT機器に感染し史上最大規模のDDoS攻撃を仕掛ける新型マルウェア（いわゆる“Mirai”）が登場した。2016年9月、米セキュリティサイトKrebs on Securityが、ピーク時665GbpsのDDoS攻撃によって一時的にサイト閉鎖に追い込まれ、同22日には、フランスのインターネットサービスプロバイダーであるOVH社が、1.1Tbpsに達する大規模なDDoS攻撃を受けた。

○米Yahoo（2016年12月）

2013年8月に**10億件以上のアカウント情報が窃取**されていた。

○ウクライナ電力供給会社（2016年12月）

2016年12月17日深夜、ウクライナの国営電力会社Ukrenergoの**変電所がサイバー攻撃を受け**、キエフ北部及び周辺地域で**約1時間の停電が発生**

○英国の病院、仏ルノー等（2017年5月）

ランサムウェア**「WannaCry」の感染により、英国の国民保険サービス（NHS）関連システムが停止し、多数の病院で医療サービスが中断するなどの被害が続出。**また、仏ルノーでは車両の生産ラインの稼働が停止。その他にも、スペインのテレフォニカ、独のドイツ鉄道、米国のFedEx等、**世界各国で被害あり**。

2017年12月に、**米国は、このサイバー攻撃が北朝鮮によるものであるとして、北朝鮮を非難する旨発表**。同日、我が国も米国を支持し、北朝鮮を非難

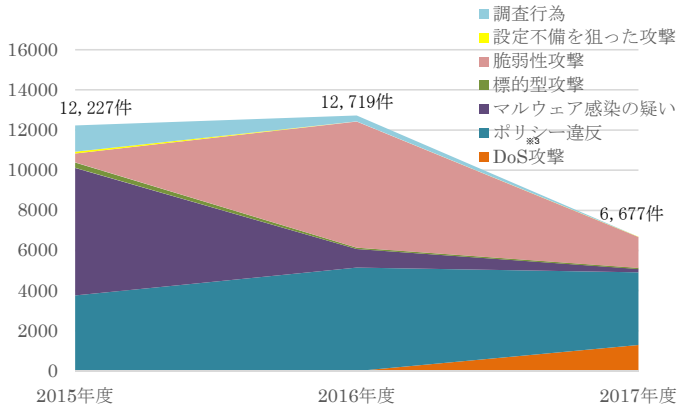
（参考）政府機関等に対するサイバー攻撃等の傾向

政府機関等における情勢

- ウェブアプリケーションの脆弱性を悪用した攻撃等、依然として政府機関等を対象とした攻撃が頻発しているが、政府機関等の対策により、サイバー攻撃に係る件数は減少傾向。ただし、攻撃は巧妙化が図られるなど、予断を許さない状況。
- 2017年４月から、国による監視、監査、原因究明調査等の範囲を政府機関に加え、独立行政法人等へ拡大。

【第一GSOC※1における確認を要するイベント検知件数※2】

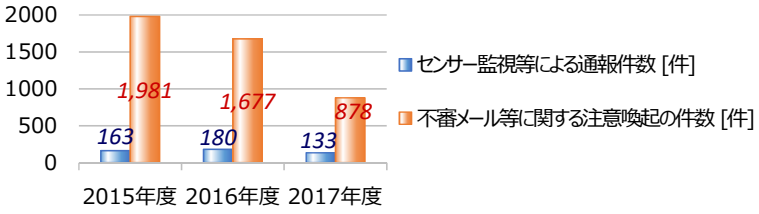
センサー監視等によるイベント検知件数のうち、対処の要否について確認を要するものの件数は昨年度より減少している。なお、既知の脆弱性に対する攻撃等が減少する一方、脆弱性が短時間のうちに攻撃に悪用されるなど攻撃の種類は昨年度より増加している。



※1 政府機関に対する情報セキュリティ横断監視・即応調整チーム
※2 既に攻撃手法に対応済みであるため攻撃としては失敗した通信、攻撃の前段階で行われる調査のための行為にとどまり明らかに対応不要と判断できる通信等を分析しノイズとして除去した上で、なお対処の要否について確認を要する事象の件数
※3 Denial of Serviceの略。サービス不能攻撃

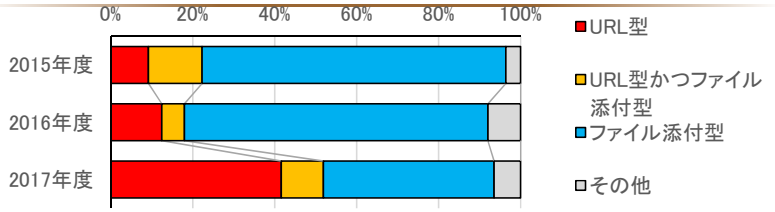
【政府機関に対する攻撃の傾向】

センサー監視等による通報件数は133件、不審メール等の注意喚起件数は878件となり、どちらも2016年度から減少しているものの、脆弱性情報の公開直後の攻撃の増加、不審メールの巧妙化が確認されており、引き続き注意が必要。



【政府機関等に対する不審メールの傾向】

2017年度は、不審なファイルが添付されたメール（ファイル添付型）の比率が減少し、不審なURLが記載されたメール（URL型）の比率が増加。



（出典）：サイバーセキュリティに係る年次報告（2017年度）（平成30年７月25日サイバーセキュリティ戦略本部決定）

（参考）サイバーセキュリティに係る諸外国の政策動向

米国

2017年５月、連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令（EO13800）に署名。同大統領令に基づき、関係機関は以下の事項について報告書を発表

- 連邦政府のサイバーセキュリティ、IT近代化
- 重要インフラ防護
- ボットネット対策
- 抑止、国際協力
- 人材育成　等

英国

2016年11月に国家サイバーセキュリティ戦略を改訂

- 「防御」、「抑止」、「開発」を目的とすること
- 「積極的サイバー防御」の推進
- 「攻撃的サイバー能力」の保有・強化

等に言及

EU

- 「ネットワーク情報セキュリティ指令」（NIS指令）を発行（2016年7月）、2018年５月までに加盟国において国内法化義務付け
- 「サイバー外交ツールボックス」の公表（2017年6月）
- サイバーセキュリティ強化に向けた政策パッケージの公表、サイバーセキュリティ法案（2017年9月）
- 一般データ保護規則（GDPR）が成立（2018年5月より施行）

中国

2017年６月、「サイバーセキュリティ法」を施行し、同法に基づく以下関連規制を発行

- ネットワーク製品及びサービスの安全審査弁法
- 個人情報及び重要データの越境安全評価法
- 重要情報インフラ保護弁法　等

【３．本戦略の目的（目指すサイバーセキュリティの基本的な在り方等）】のポイント
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＞

【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」に係る諸施策の目標及び実施方針のポイント
新たな価値創出を支えるサイバーセキュリティの推進

・全ての産業分野において、企業が事業継続を確固なものとしていくとともに、新たな価値を創出していくための動きを支えるための基盤として、一体的にサイバーセキュリティの確保に取り組む
・その際には、サイバーセキュリティ対策をリスクマネジメントの一環として捉え、取り組むことが重要

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
- 経営層の意識改革の促進（「費用」から「投資」へ）
- 企業のサイバーセキュリティ対策に関する積極的な情報発信・開示の促進
- 官民が連携してサイバーセキュリティ保険の活用を推進
- セキュリティビジネス強化に向けたガイドライン策定、リスク分析、研究開発等

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
- 脅威を明確化し、運用レベルでの対策を実現する業種横断的指針の作成
- 産業分野ごとの具体的対応策の提示
- 中小企業の取組の推進

３．安全なIoTシステムの構築
- IoTシステムに関するサイバーセキュリティの体系整備と国際標準化
- IoT機器の脆弱性対策モデルの構築・国際発信

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：取組の例

経営層におけるサイバーセキュリティに取り組む必要があるとの認識を広げて必要な対策の検討・導入を促すとともに、市場がその取組を企業価値向上につながるものとして評価し、サイバーセキュリティに対する投資へのインセンティブが生まれるという好循環の形成を目指す。

経営層の意識改革

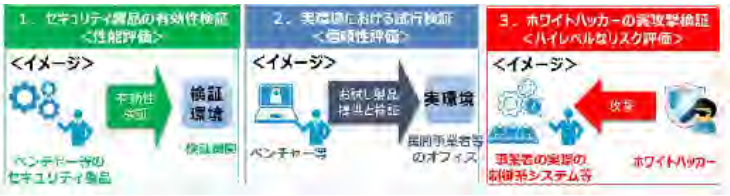
＜内閣官房＞
・官民の連携による、経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催

＜経済産業省＞
・取締役会の関与の促進や投資家への啓発の観点から、サイバーセキュリティへの経営層の関与を、上場企業で行われている「取締役会の実効性評価」の評価項目へ組み込むことを促進
・コーポレート・ガバナンス・システムに関する議論の中で、「守り」のリスク管理の一環として、サイバーセキュリティ対策を位置付けることを検討

先端技術を利用したイノベーションを支えるサイバーセキュリティビジネスの強化

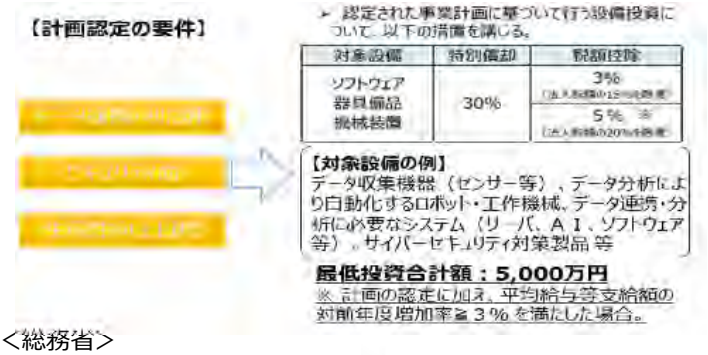
＜経済産業省＞
・サイバーセキュリティ対策のニーズ明確化・具体化、シーズ発掘、ビジネスマッチングのための「コラボレーション・プラットフォーム」の設置（2018年6月より活動開始）
・日本のセキュリティニーズに応じたサイバーセキュリティ製品の有効性や、IoT機器等の脆弱性等を実機を通じて検証する仕組みの構築

＜実戦的サイバーセキュリティ検証基盤の全体像＞



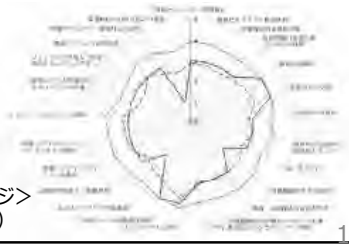
サイバーセキュリティに対する投資の促進

＜総務省・経済産業省＞
・サイバーセキュリティ対策が講じられたデータ連携により生産性を向上させる取組に関するシステム・製品の導入に対して税額控除等を措置する「コネクテッド・インダストリーズ税制」により、事業者のセキュリティ対策の強化と生産性向上を同時に促進



＜総務省＞
・ベストプラクティスも盛り込んだ「セキュリティ対策情報開示ガイドライン」（仮称）を策定、公表

＜経済産業省＞
・「サイバーセキュリティ経営ガイドライン」の活用促進に向け、「対策事例集」と自社の状況（成熟度）を把握するための「可視化ツール」の整備・活用を推進



＜可視化ツールのイメージ＞
（米国ＮＰＯとも協力）

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：取組の例

サイバー空間と実空間の一体化が加速的に進展する中、「Society 5.0」の実現に向け、サプライチェーン全体を俯瞰した取組を推進する。

サイバーセキュリティ対策指針の策定

＜経済産業省＞
・サプライチェーンにおける脅威を明確化し、運用レベルでの対策が実施できるような業種横断的な指針として、「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定
・産業分野ごとに守るべきものやリスクに違いも存在するため、産業分野ごとにセキュリティ水準の検討を進めるとともに、その上で、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進める。

サイバー空間におけるつながり
【第３層】
- サービスを創造するためのデータの信頼を確保

フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写”する機能の信頼を確保

企業間のつながり（従来型サプライチェーン）
【第１層】
- 適切なマネジメントを基盤に各主体の信頼を確保

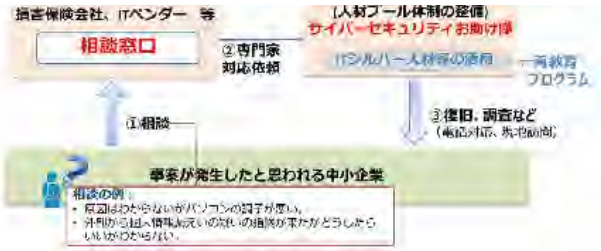
中小企業の取組の促進

＜経済産業省＞
・中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」への登録を促す。

■2018年7月現在で、自己宣言企業は13,000社弱

■中小企業庁と連携して、宣言企業数を大幅に加速させることが急務

・24時間相談窓口などの体制を持つ損保会社等と連携して、中小企業のサイバーセキュリティに関する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」を創設するとともに、ITに従事してきたシルバー人材の再教育などを通じて人的リソースを確保



＜サイバーセキュリティ保険等と連携した「サイバーセキュリティお助け隊」のイメージ＞

3． 安全なIoTシステムの構築：取組の例

経済社会の発展に不可欠なインフラとしてのサイバー空間に悪影響を及ぼし得る脆弱なモノのサイバーセキュリティ対策が喫緊の課題。
官民が連携し、安全なIoTシステムの構築に取り組む。

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

＜内閣官房＞
・各主体の間での共通認識の醸成と、役割や機能の明確化を図った上で、協働した取組を推進

自律的なIoTシステムに係る関係省庁の取組を推進するとともに、各主体が協働できるよう情報共有等の取組を推進する。

脆弱性対策に係る体制の整備

＜総務省＞
パスワード設定に不備のある機器の調査・特定を行い、利用者への注意喚起を円滑に行えるような所要の制度整備を推進

パスワード設定に不備のある機器の調査を行い、電気通信事業者の協力の下、当該機器の利用者を特定し、設定変更を促す取組を行う。

【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」に係る諸施策の目標及び実施方針のポイント

国民・社会を守る任務を保証

国民が安全で安心して暮らせる社会を実現するためには、政府機関、地方公共団体、サイバー関連事業者、重要インフラ事業者等、教育研究機関、そして国民一人一人に至るまで、多様な関係者が連携して多層的なサイバーセキュリティを確保することが重要であり、これらの業務やサービスが安全かつ持続的に提供されるよう「任務保証」の考え方に基づく取組を推進していく。

1． 国民・社会を守るための取組
- 「積極的サイバー防御」の構築
  （脅威情報の共有・活用の促進、脆弱性情報の提供等）
- 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
- 重要インフラ行動計画に基づく取組の推進
- 地方公共団体の取組強化

3． 政府機関等におけるセキュリティ強化・充実
- 情報システムの状態のリアルタイム管理の強化（新たな統一基準群に基づく取組等）

4． 大学等の多様性を踏まえた対策の推進
- 各層別研修及び実践的な訓練・演習の実施

5． 2020年東京大会とその後を見据えた取組
- サイバーセキュリティ対処調整センターの構築

6． 従来の枠を超えた情報共有・連携体制の構築
- 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強化
- サイバー攻撃と実空間の双方の危機管理に挑むための対処態勢の強化

1． 国民・社会を守るための取組：取組の例

サイバー空間の脅威の深刻化に伴い、社会全体におけるサイバーセキュリティへの危機意識が高まっている状況を踏まえ、全ての主体が、自主的にセキュリティの意識を向上させ、主体的に取り組むとともに、連携して多層的にサイバーセキュリティを確保する状況を作り出していく

安全・安心なサイバー空間の利用環境の確保

「積極的サイバー防御」の推進

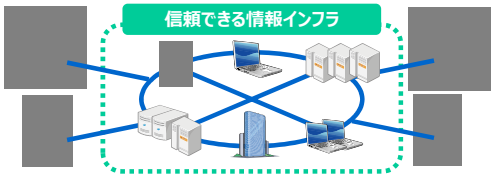
サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じる「積極的サイバー防御」を推進

＜総務省＞
・先行的防御を可能にするための脅威情報の共有・活用の促進

＜経済産業省＞
・IoT機器を含むソフトウェア等の脆弱性対策情報ポータルサイト（JVN）において対策情報の公表、対策ツールの提供等を通じ、利用者の対策を推進
・フィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組

信頼できる情報インフラの整備の促進

＜内閣官房、総務省、経済産業省＞
・情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等について調査を実施



仮想通貨、自動運転車等に関する対策の推進

＜金融庁＞
・仮想通貨交換業者におけるサイバーセキュリティの強化に向け、実効性のある自主規制機能の確立を促す

＜国土交通省＞
・国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論を主導

サイバー犯罪への対策

サイバー犯罪の実態把握・取締りの推進

＜警察庁、法務省＞
・取締り・捜査に必要な専門的知識・技能の習得のための各種研修の実施

＜総務省＞
・能動的・網羅的なサイバー攻撃観測技術の開発

官民が連携したサイバー犯罪対策の推進

＜警察庁、総務省、経済産業省＞
・被害防止のための広報啓発活動や最新の手口・被害実態等の情報共有の推進

＜警察庁＞
・民間事業者等の知見を活用した人材育成

＜警察庁、総務省＞
・事後追跡可能性の確保

2～4． 重要インフラ、政府機関、大学等におけるセキュリティ対策の推進：取組の例

官民一体となった重要インフラの防護

重要インフラの防護については、「任務保証」の考え方を踏まえ、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ため、「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」に基づいた取組を推進

第４次行動計画に基づく主な取組

＜内閣官房、重要インフラ所管省庁＞
・リスクマネジメントの活動全体が継続的かつ有効に機能するよう取組を推進
・安全基準等を策定するための指針を浸透させ、業務内容や組織の規模等を考慮した安全基準等を継続的に改善
・サイバー攻撃による重要インフラサービス障害等に係る深刻度評価基準を策定
・官民の枠を超えた様々な規模の主体の間での訓練・演習を実施
・制御系システムに関する人材育成、脅威情報の情報共有等を推進

地方公共団体のセキュリティ強化・充実

＜総務省＞
・セキュリティポリシーに関するガイドラインを随時更新
・地方公共団体職員を対象とした集合研修・eラーニングを実施
・緊急時対応訓練の支援及びCSIRTの連携組織の設立

政府機関等におけるセキュリティ強化・充実

新たな技術を活用し、情報システムのセキュリティ水準の向上を進めるとともに、その確認を通じて、従来の攻撃側優位の状況を改善する。併せて、組織的な対応能力の充実を行う

＜内閣官房、関係府省庁＞
・情報システムの防御能力の向上と状態のリアルタイムでの把握
・政府機関等における横断的な連携の高度化

大学等における安全・安心な教育・研究環境の確保

大学等において自律的にサイバーセキュリティ対策を行うとともに、大学等の連携協力によるサイバー攻撃への対応体制の構築や情報共有等を国が積極的に支援

＜文部科学省＞
・大学等の多様性を踏まえた対策を推進
・大学等の連携協力による取組を推進