資料１

次期サイバーセキュリティ戦略の検討について

資料１－１　次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の概要

資料１－２　次期サイバーセキュリティ戦略に関する検討事項等について

資料１－３　次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の概要

資料１－１

【背景】

サイバー空間におけるイノベーションの進展

AI、IoT等、サイバー空間を前提とする技術やサービスの利用が社会的に受容され、既存構造を覆すイノベーションを牽引。これにより、サイバー空間と実空間の一体化が急速に進展

・AIの劇的進化

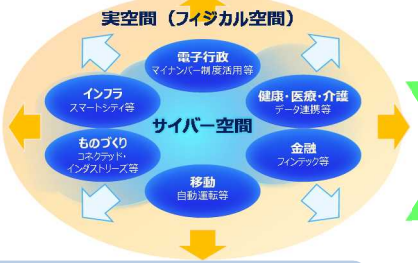
深層学習によりAIが「猫」を認識（※1）

囲碁ソフトがトッププロ棋士に勝利（※2）

・フィンテックの進展

国内「FinTechエコシステム」関連IT市場セグメント別支出額予測（※3）

・サイバー空間と実空間の一体化の進展



サイバー空間の脅威の深刻化・巧妙化

IoTや重要インフラを狙った攻撃等により、サイバー空間の脅威は深刻化・巧妙化。サイバー空間と実空間の一体化の進展に伴い、実空間における経済的・社会的損失のリスクが指数的に拡大するおそれ

・IoTを狙った攻撃が急増

・重要インフラを狙った攻撃の深刻化

－ウクライナ電力供給会社への攻撃(2016)

－身代金攻撃（WannaCryの感染）による英国医療サービス停止（2017）

諸外国の政策動向

サイバーセキュリティをめぐり、諸外国においても戦略的取組を強化

米国

・連邦政府、重要インフラ強化に関する大統領令（2017）

・オープンでセキュアなインターネットを推進

英国

・国家サイバーセキュリティ戦略（2016）

・防御、抑止、開発

中国

・国家サイバー空間セキュリティ戦略（2016）

・サイバー空間主権確保

2020年東京オリンピック・パラリンピック競技大会の開催

次期戦略の期間中に開催される同大会に向けた体制整備及び取組の強化を推進

グローバル化、サービス経済化、人材不足を見据えた取組の強化

サイバーセキュリティに係る国際競争力強化、人材育成、国民全体のセキュリティマインドの醸成、推進体制の強化等の必要

検討事項

第一　サイバー空間の将来像と新たな脅威の予測

・経済活動、国民生活への変化・影響

・脅威の状況の予測

・諸外国の動向

等について、把握・分析・予測

第二　2020年東京オリパラ競技大会とその後を見据えた体制整備

・2020年オリパラ大会に向けた体制整備

・同大会で得た経験・知見に基づき、大会後の持続的なサイバーセキュリティ強化

第三　新たに取り組む課題と対策の速やかな実施

・次期戦略において新たに取り組むべき課題の明確化と対策の速やかな実施を推進

サイバー空間の将来像を視野に入れ、サイバーセキュリティの基本的な在り方を明確化し、次期戦略を策定

（※１）出典：Google Official Blog　（※２）出典：GIGAZINE

（※３）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）

次期サイバーセキュリティ戦略策定までの主要スケジュール（案）

時期		H29年度(2017年度)			H30年度(2018年度)			
		1	2	3	4	5	6	7
新戦略関係	閣議							★ 閣議 (新戦略決定)
	サイバーセキュリティ戦略本部	☆ 本部⑯ (基本的考え方等) (1/17)		☆ 本部⑰ (骨子案等)		☆ 本部⑱ (パブコメ案)	☆ 本部⑲ (新戦略案等)	☆ 本部⑳ (年次計画決定等)
	その他 (有識者本部員等の関係者からの意見聴取等を随時実施)	→	→	→	→	→	→	

IT総合戦略本部及び国家安全保障会議からの意見聴取

パブリックコメント実施

資料１－２

次期サイバーセキュリティ戦略に関する検討事項等について

主な検討事項

【サイバー空間の将来像と新たな脅威の予測】

・ＡＩをはじめ、IoT、Fintech、ロボティクスなど、サイバー空間を前提とする様々な技術やサービスが社会的に受容され、**あらゆる産業領域において当然に利用される**ようになるなど、**経済社会の大きな変化について、現状及び将来の見通しをどのように考えるか。**

・経済社会の変化に伴い実空間（フィジカル空間）との一体化が進むサイバー空間を踏まえ、サプライチェーンにおけるリスクの増大や国家の関与が疑われる事案も含め、**急速に深刻化・巧妙化する脅威について、現状及び将来の見通し、さらにはその対策をどのように考えるか。**

・米国、英国、ＥＵに加え、中国、ロシアなどの**諸外国の動向をどのようにとらえるか。また、その動向は我が国にどのような影響を及ぼすか。**

【2020年東京オリンピック・パラリンピック競技大会とその後を見据えた体制等の整備】

・安全、安心な東京大会の実現のためのサイバーセキュリティ対策の取組について、**さらに充実・強化すべき点や、大会後においても持続的なサイバーセキュリティの強化につながるようにするために留意すべき点**にはどのようなことがあるか。

【次期戦略において新たに取り組むべき課題の明確化と対策の速やかな実施】

・現行戦略に基づく施策の実施状況をどのように評価するか。とりわけ、サイバーセキュリティに係る**国際競争力強化、人材育成、国民全体のセキュリティマインドの醸成、推進体制の強化**等の観点から、新たな課題や対策を強化すべき課題はあるか。

以上を踏まえ、**あらゆる主体が参加し、実空間（フィジカル空間）との一体化が加速的に進展するグローバルなサイバー空間とそれを支えるサイバーセキュリティの基本的な在り方**について、どのように考えるか。

サイバー空間の認識に関する変化のイメージ

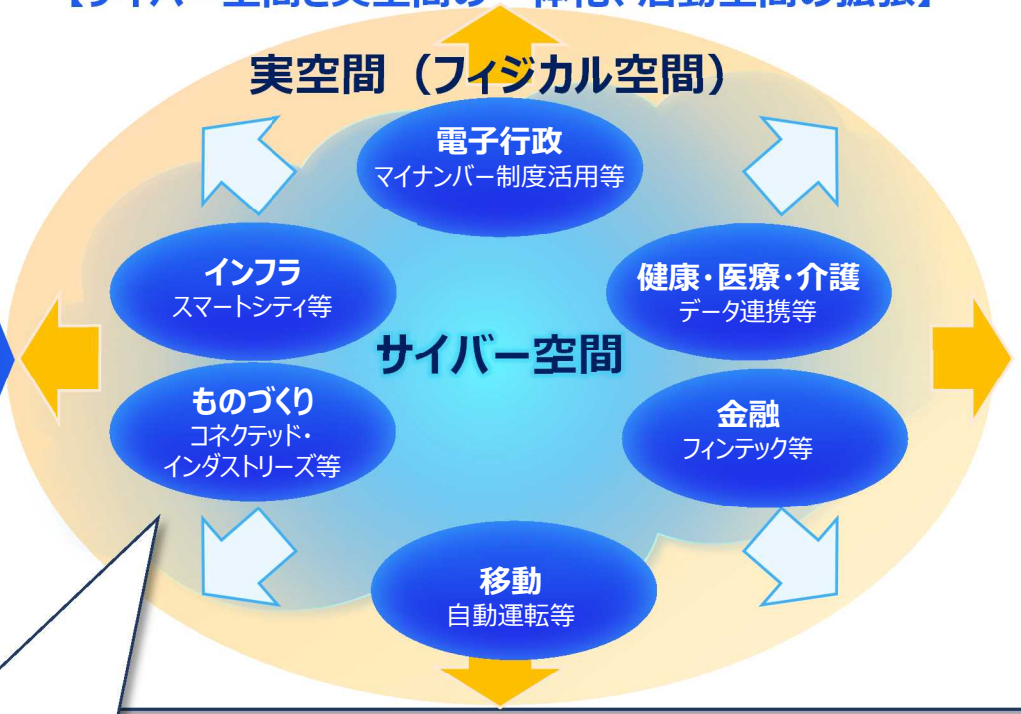
中長期

現行戦略策定時（2015年9月）から現在における変化

【（現行戦略策定時）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】



サイバー空間がもたらす恩恵

- 技術革新（AI、IoT、Fintech等）やサービスの利用拡大に支えられ、**経済社会活動・国民生活の**様々な分野で、既存社会の構造を根底から覆すような**イノベーションを牽引**。
- これにより、**サイバー空間と実空間の一体化が進展し、必須インフラ化**。
- **人間社会全体の活動空間自体も急速に拡張**。この恩恵を最大限享受できるようにすべき。

サイバー空間がもたらす脅威

- サイバー空間における**脅威は深刻化・巧妙化**（例：ゼロディ攻撃、ダークウェブ、AI活用）。
- サイバー空間と実空間の一体化の進展に伴い、**実空間での経済的・社会的損失のリスクが指数的に拡大するおそれ**。
- こうした影響拡大の可能性も踏まえて、国家の関与が疑われる事案が増加し、**被害の深刻化が懸念される。**
- **もはや特定の主体による対策だけではサイバーセキュリティは守れず**、イノベーションに支障が生ずるおそれ。

＜参考資料＞

○ 現行サイバーセキュリティ戦略の概要（平成27年９月４日閣議決定）・・・・・・・・・・・・・・・・・・・ 4P
○ サイバーセキュリティ戦略の位置付け ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 5P
○ サイバーセキュリティ政策の経緯 ・・ 6P
○ サイバー空間におけるイノベーションの進展 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 7P
○ AIの進化の経緯・・・ 9P
○ サイバー攻撃の脅威 ・・・ 10P
○ 国内外のサイバー攻撃事案 ・・ 11P
○ 現行戦略に基づく施策の実施状況と評価のまとめ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 12P

現行サイバーセキュリティ戦略　平成27年９月４日閣議決定

1 サイバー空間に係る認識

- サイバー空間：**「無限の価値を産むフロンティア」**である人工空間経済社会の活動基盤
- **「連接融合情報社会（連融情報社会）」**が到来
  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➡**「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

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**
- **セキュリティマインドを持った企業経営の推進**
- **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

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**
- **重要インフラを守るための取組**
- **政府機関を守るための取組**

国際社会の平和・安定 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**
- **国際社会の平和・安定**
- **世界各国との協力・連携**

横断的施策

- **研究開発の推進**
- **人材の育成・確保**

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

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基本法（平成26年法律第104号）（抄）

第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。

２　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。

一　サイバーセキュリティに関する施策についての基本的な方針

二　国の行政機関等におけるサイバーセキュリティの確保に関する事項

三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項

四　前三号に掲げるもののほか、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するために必要な事項

３　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。

４　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。

５・６　（略）

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

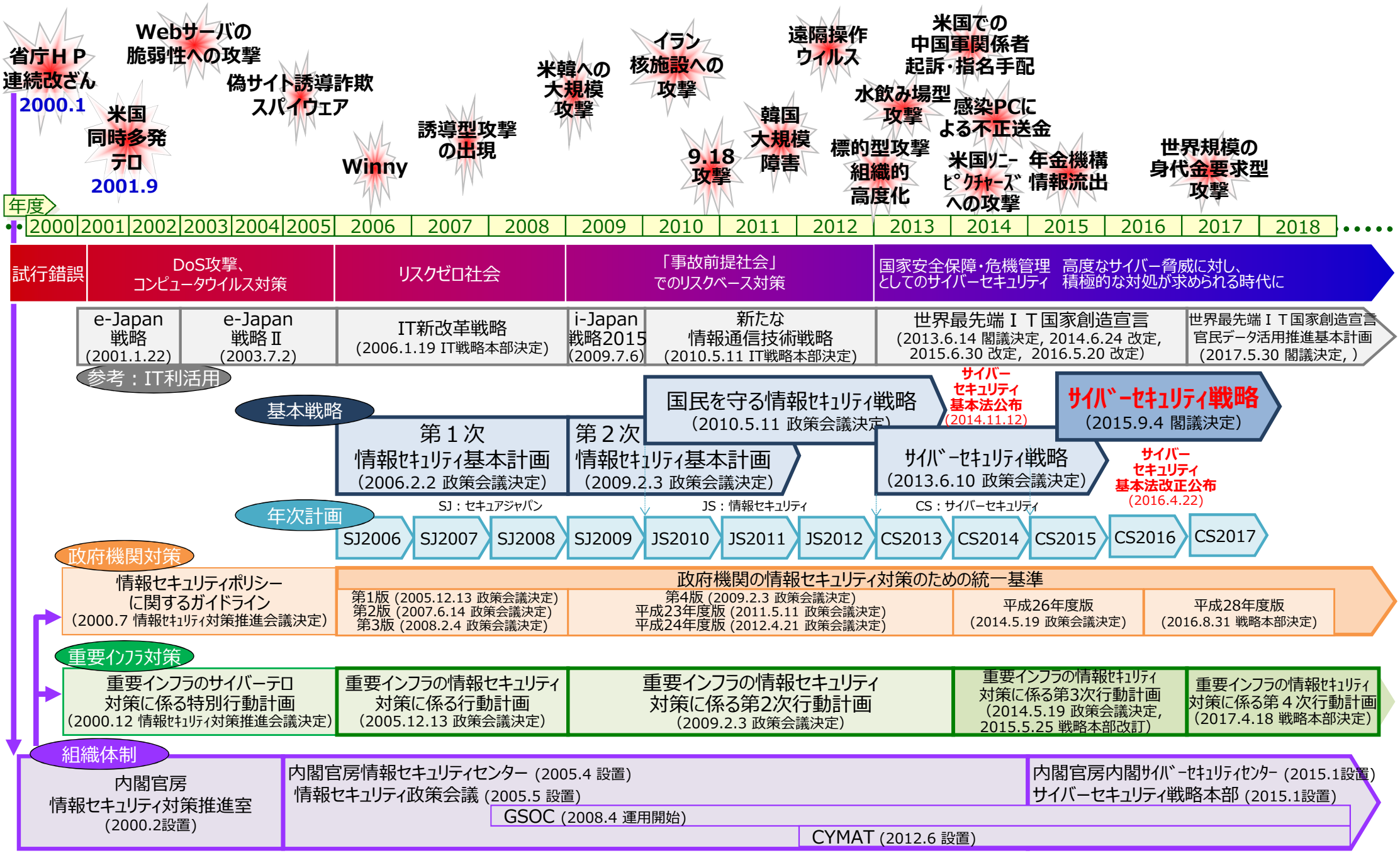
一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二～四　（略）

２　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。

３・４　（略）

サイバーセキュリティ政策の経緯

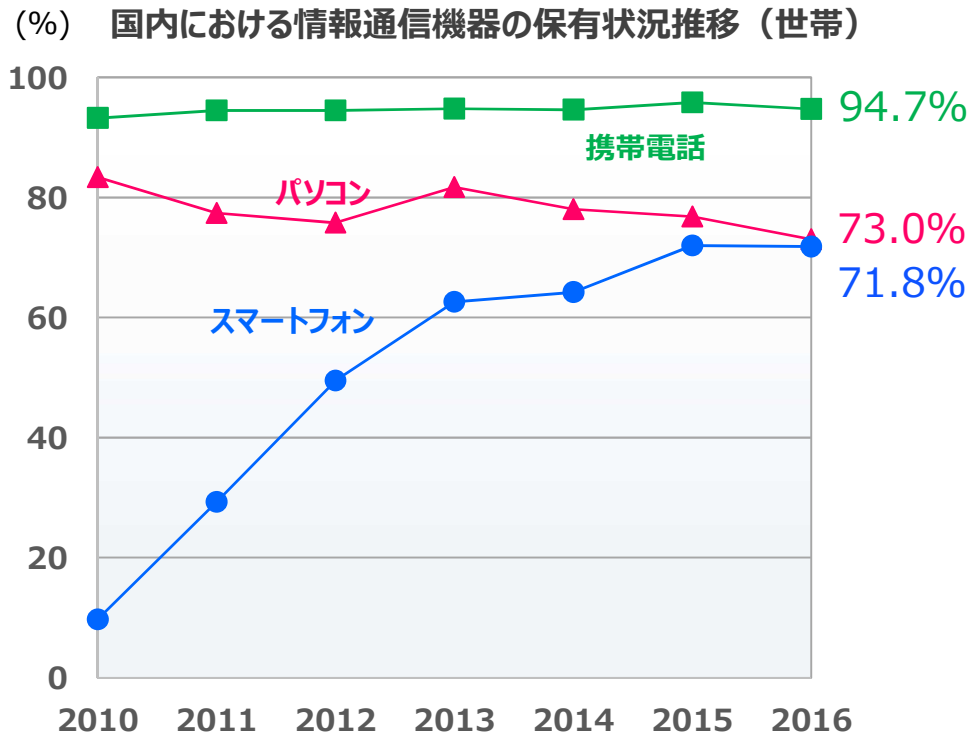


サイバー空間におけるイノベーションの進展

生活の中心となりつつあるスマートフォン

- スマートフォンの普及が進み、世帯保有率は7.4倍に急増(2010年末：9.7%→2016年末：71.8%)
- パソコンからの主役交代が加速しており、2016年におけるインターネットに接続する端末の利用状況は、スマートフォン５８％(増加傾向)、パソコン59%(横ばい傾向)

(引用)平成29年版情報通信白書（総務省）

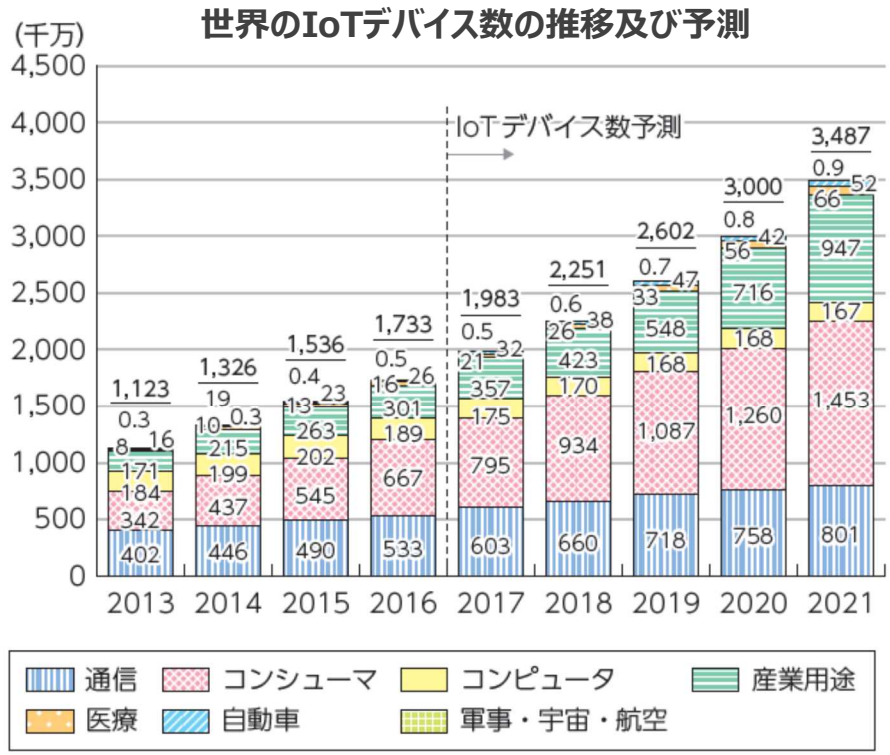


※携帯電話にはスマートフォンを内数とし含めている

(参考)平成29年版情報通信白書（総務省）

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）

サイバー空間におけるイノベーションの進展（続き）

AIの劇的な進化

・2011年：「ワトソン」が米国のクイズ番組でクイズ王に勝利

・2012年：ディープラーニングによりAI自らが猫の特徴を識別する機能を飛躍的に向上

・2016年：囲碁ソフト「AlphaGo」が 韓国トッププロ棋士に勝利

・2017年：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

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

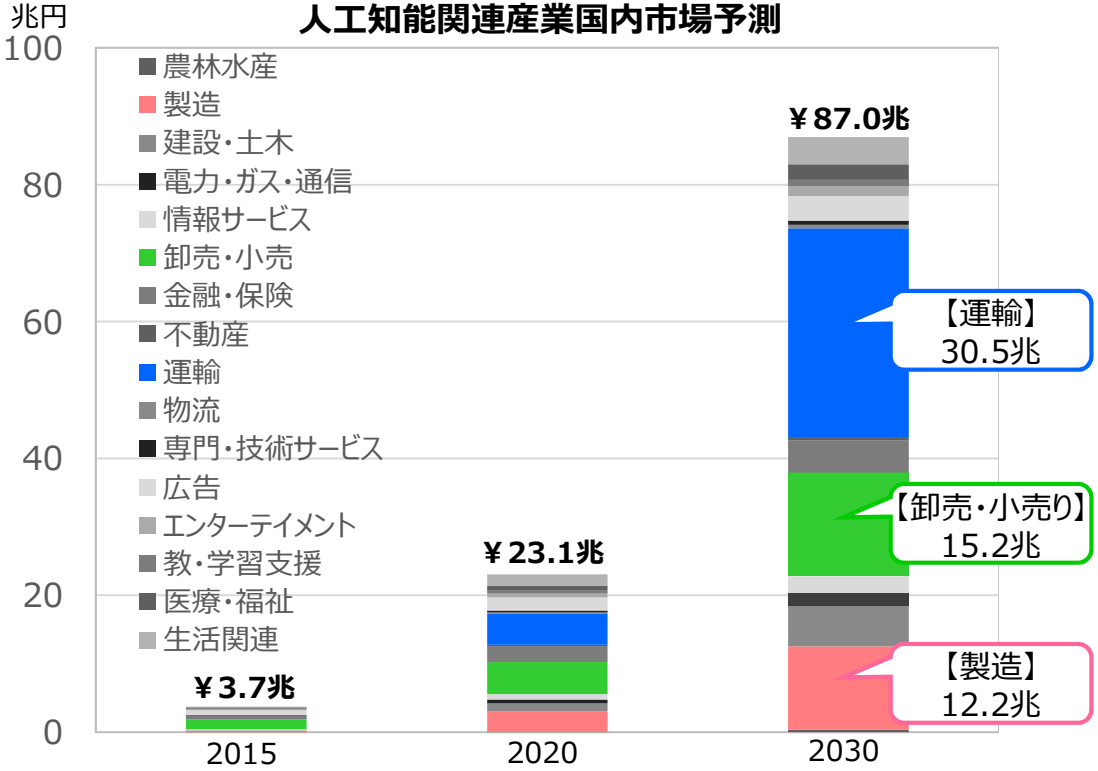
・決済：ブロックチェーンの技術を活用した決済サービスも登場

・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

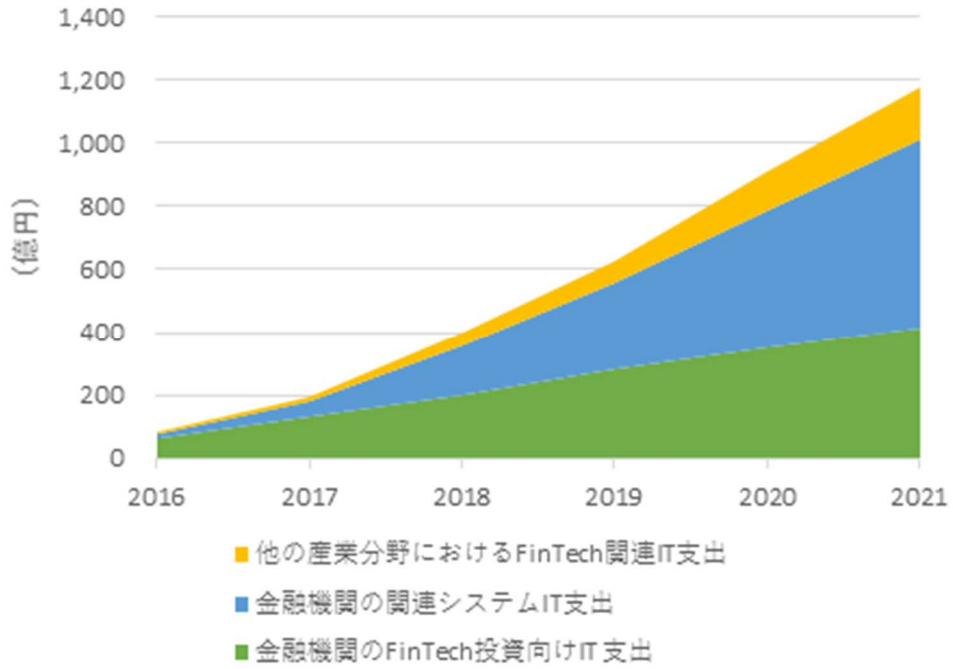
・個人資産管理：アカウントアグリゲーション等により顧客の資産を分かり易く管理

人工知能関連産業国内市場予測



（出典）：人口知能関連産業国内市場予測（EY総合研究所2015）

国内「FinTechエコシステム」関連IT市場セグメント別支出額予測



（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）

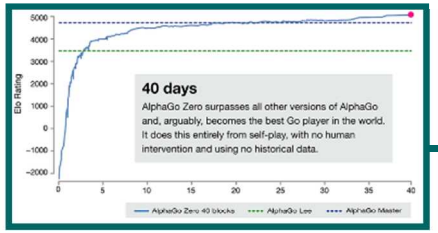
AIの進化の経緯

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）

サイバー攻撃の脅威

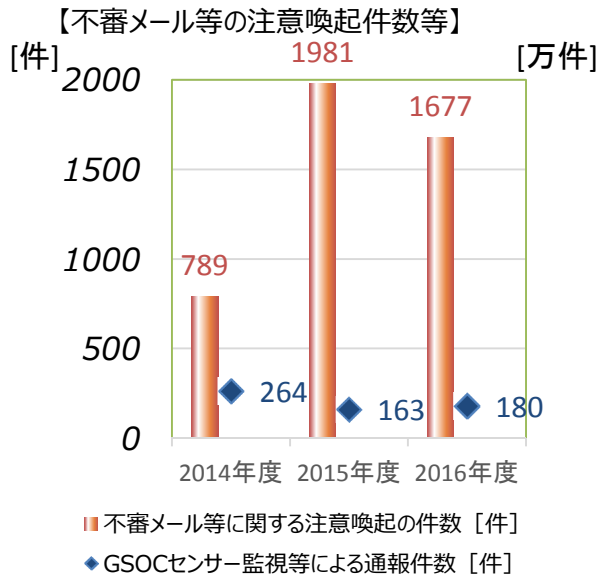
- **サイバー攻撃の様態は、深刻化・巧妙化。また、IoTの進展に伴い、IoT機器を狙った攻撃も急増。**
- **サイバー空間と実空間の一体化の加速的進展に伴い、実空間における経済的・社会的損失のリスクが指数的に拡大するおそれ。**

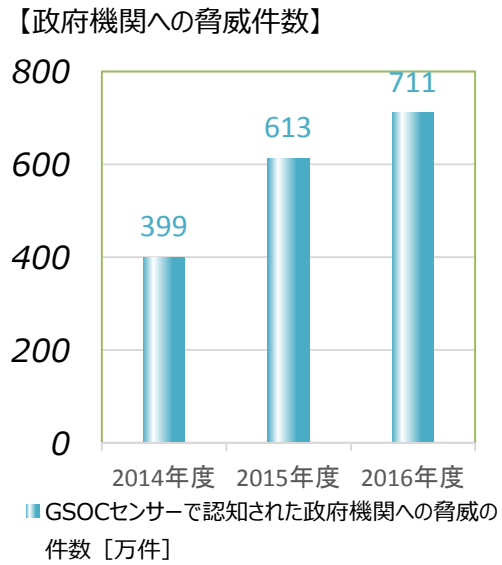
順位	組織における10大脅威	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	7位
3位	ウェブサービスからの個人情報の窃取	3位
4位	サービス妨害攻撃によるサービス停止	4位
5位	内部不正による情報漏えいとそれに伴う業務停止	2位
6位	ウェブサイトの改ざん	5位
7位	ウェブサービスへの不正ログイン	9位
8位	IoT機器の脆弱性の顕在化	圏外
9位	攻撃のビジネス化（アンダーグラウンドサービス）	圏外
10位	インターネットバンキングやクレジットカード情報の不正利用	8位

2016年に発生し、社会的影響が大きかった
セキュリティ上の脅威として発表した「情報セキュリティ10大脅威2017」
（情報処理推進機構発表）

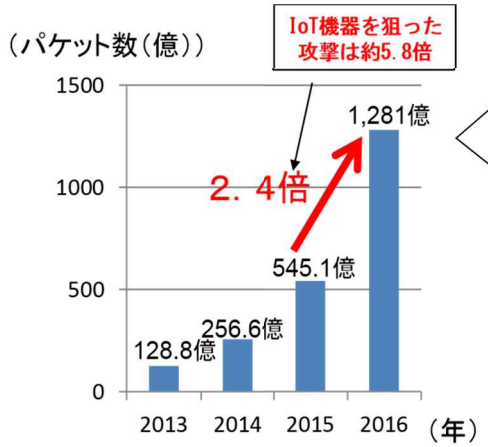
※出典：IPAウェブサイト https://www.ipa.go.jp/security/vuln/10threats2017.html

○政府機関等を対象とした攻撃が頻発





○IoT機器を狙った攻撃が急増

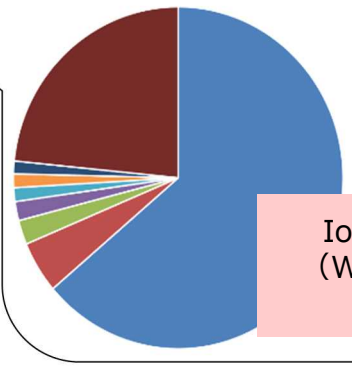


1年間で観測されたサイバー攻撃のパケット数

観測された全サイバー攻撃
1,281億パケットのうち、

$\frac{2}{3}$

がIoT機器を狙っている！



IoT機器を狙った攻撃
（Webカメラ、ルータ等）
64%

出展：総務省サイバーセキュリティタスクフォース（第１回）資料1－2中の図を最新化

国内外のサイバー攻撃事案

【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。

【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**。
平成29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。

現行戦略に基づく施策の実施状況と評価のまとめ

1　経済社会の活力の向上及び持続的発展

	サイバーセキュリティ政策に係る年次報告（2015年度・2016年度）より		
	(1)安全なIoTシステムの創出	(2)セキュリティマインドを持った企業経営の推進	(3)セキュリティに係るビジネス環境の整備
主な実績	• 「IoTセキュリティガイドライン」の策定 • スマートメーターセキュリティガイドライン等、各分野のガイドラインについても検討を推進 • 「安全なIoTシステムのためのセキュリティに関する一般的枠組」を策定	• 「サイバーセキュリティ経営ガイドライン」の策定 • サイバー攻撃への対処能力向上のための演習の実施 • 「企業経営のためのサイバーセキュリティの考え方」を公表 • 「中小企業の情報セキュリティ対策ガイドライン」を公表	• セキュリティ技術研究のための先進的な研究開発を進めるための支援事業を開始 • 我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進 • 我が国企業のセキュリティ確保及び国際競争強化の基盤となるビジネス環境の整備の取組
課題	• IoTに対する総合的なセキュリティ対策を**関係省庁が連携して実施**していくことが必要 • **国際標準化等に取り組む**ことにより、安全、高品質を訴求できるIoTシステムを実現し、世界的な市場シェアの獲得を目指すことが必要	• 経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、**実務者層との間のコミュニケーションの支援を行う「橋渡し人材層」の育成**が重要 • 経営層の認識、情報発信の状況や関連する制度面の課題等の把握に努め、**経営層の認識を高めていくための推進方策等について検討**していくことが必要	• サイバーセキュリティに係る投資を促進することで、サイバーセキュリティ関連産業における**継続的な需要喚起を促すことが必要** • 引き続き先進的な研究開発を行っているベンチャー企業に対する支援事業を実施させるとともに、国際会合等に参加し、積極的に**我が国の意向を国際標準等に盛り込むことが必要**

現行戦略に基づく施策の実施状況と評価のまとめ

2　国民が安全で安心して暮らせる社会の実現

	サイバーセキュリティ政策に係る年次報告（2015年度・2016年度）より		
	(1)国民・社会を守るための取組	(2)重要インフラを守るための取組	(3)政府機関を守るための取組
主な実績	• 「サイバーセキュリティ月間」では、ソーシャルメディアの活用や国民に親しみやすいメディアの活用など新たな取組を実施するなど、普及啓発活動を推進 • サイバー犯罪への対策についても警察庁を中心に強化	• 「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」における各施策を着実に推進 • 第３次行動計画の成果と課題をとりまとめ、機能保証の考え方を踏まえた「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」を策定	• 政府機関におけるセキュリティ・IT人材の育成についての施策を「サイバーセキュリティ人材育成総合強化方針」に記載 • 統一基準群の改定、政府機関への監査を実施
課題	• 各地で実施されている草の根的な活動に対し、積極的に支援等を行うことが必要 • サイバー犯罪の捜査や未然防止に向け、官民の人事交流などの官民連携の強化が必要 • インターネットの利用に関し、年齢層や所属等が異なる多様な国民のニーズにきめ細やかに対応していけるよう、**着実に普及啓発活動を推進していく**ことが必要	• 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、各関係主体において、「**安全基準**等の整備及び浸透」、「**情報共有体制**の強化」、「障害対応体制の強化」、「**リスクマネジメント**及び対処態勢の整備」及び「防護基盤の強化」の各施策を推進することが必要	• 司令塔機能の抜本的強化やセキュリティ・IT人材(部内育成の専門人材)の確保・育成等、**政府機関におけるセキュリティ・IT人材の育成を推進**することが必要 • 独立行政法人及び指定法人に対する監査及び監視を実施するなど、引き続き、政府機関、**独立行政法人及び指定法人におけるサイバーセキュリティ確保のための取組を総合的に強化**することが必要

現行戦略に基づく施策の実施状況と評価のまとめ

3　国際社会の平和・安定及び我が国の安全保障

	サイバーセキュリティ政策に係る年次報告（2015年度・2016年度）より		
	(1)我が国の安全の確保	(2)国際社会の平和・安定	(3)世界各国との協力・連携
主な実績	• 各対処機関は、サイバー空間に係る情報を収集・分析し、それに対処する体制整備の取組を継続的に実施 • 防衛装備品に代表される安全保障上重要な先端技術のサイバーセキュリティの確保に向けて、官民協力のもと取組を推進	• G7伊勢志摩サミット、国連政府専門家会合等を通じ、法の支配の確立に積極的に寄与し、法執行面の各国との連携強化を推進 • 「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」を策定し、政府全体の取組としてキャパシティビルディングに積極的に協力	• アジア大洋州、北米、欧州、中南米、中東アフリカの各地域において、各国政府や地域の主体との間での連携強化が着実に進行
課題	• 関係機関の防護能力の強化とサイバー空間に係る情報収集・分析能力のさらなる強化が必要であり、そのため、**海外関係機関との情報共有等の連携が必須** • **我が国の安全保障上重要な先端技術の防護**のため、関係する事業者におけるサイバーセキュリティの強化を一層徹底することが必要	• サイバー空間における法の支配の確立に向けて、各国との連携のもと、サイバー空間における**国際法の適用や国際規範について、より具体的に議論を進める**ことが必要 • キャパシティビルディングは、対象国の現地ニーズのきめ細かな把握と状況に応じた効果的な支援のため、政府一体で戦略的に対応することが必要	• **アジア大洋州においては、日ASEAN情報セキュリティ政策会議による取組を継続・強化しつつ、各国の状況に応じた連携・協力の強化を図ること**が必要 • 米国とは、日米安保体制を基軸に、経済面や安全保障面を含むあらゆる協力を拡大・深化させることが必要 • 欧州とは、二国間協議等を通じた連携や国際場裡での協力強化を進めることが必要 • その他、共通の価値観を持つ国々との連携を着実に進めることが必要

現行戦略に基づく施策の実施状況と評価のまとめ

4　横断的施策　／　5　推進体制

	サイバーセキュリティ政策に係る年次報告（2015年度・2016年度）より		
	4　横断的施策		5　推進体制
	(1)研究開発の推進	(2)人材の育成・確保	
主な実績	• 「サイバーセキュリティ研究開発戦略」の策定 • 内閣府（総合科学技術・イノベーション会議）では、SIPに「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加し、産学官が連携した総合的な研究開発を推進	• 「サイバーセキュリティ人材育成総合強化方針」を策定 • 「サイバーセキュリティ人材育成プログラム」を策定 • 資格制度の整備や演習環境の強化等、セキュリティ人材の育成・確保に関する施策を推進	• サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の施行により、監視・監査・原因究明調査の対象を、独立行政法人及び一部の特殊法人・認可法人（指定法人）へ拡大 • 東京都２３区内のオリパラの重要サービス事業者等を特定し、第１回目のリスク評価を実施
課題	• 実空間とサイバー空間の融合が高度に深化し、新しい価値が創出されていく中で、単に情報システムへの脅威に対応するだけでなく、**「人間」や「人間が安心して暮らすことのできる社会システム」を守り、強くしていく方策**の検討が必要 • SIPにおける「重要インフラ等におけるサイバーセキュリティの確保」についても着実に取組を進めていくことが必要	• 経営層、橋渡し人材層、実務者層等、**それぞれの人材層を対象にした施策間の連携**等により、より効果的な人材育成の実施を図る必要 • 「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律」の成立を踏まえ、情報処理安全確保支援士制度の実施に向けて取り組むことが必要	• **リスク評価**について、対象組織の地域的、業種的な**拡大を図っていくこと**が必要 • **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）**の整備において、情報共有・対処支援の詳細な実施要領を策定し、演習や訓練等を通じて最適化するとともに、人員体制の検討・調整等を具体的に実施していくことが必要

資料１－３

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）

平成　　年　　月　　日
サイバーセキュリティ戦略本部決定

現行のサイバーセキュリティ戦略（平成 27 年９月４日閣議決定。以下「現行戦略」という。）において、「今後３年間に執るべき諸施策の目標や実施方針を示す」とされており、平成 30 年に計画期間を終えるため、次期のサイバーセキュリティ戦略（以下「次期戦略」という。）の策定に向けた検討を行う必要がある。

次期戦略の策定に当たっては、サイバーセキュリティ基本法（平成 26 年法律第 104 号）が定める「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」及び「国際社会の平和・安定及び我が国の安全保障」に寄与するものとなるよう、以下の事項を十分に踏まえることが重要である。

第一　サイバー空間の将来像と新たな脅威の予測

サイバー空間における科学的知見の進展や技術革新、全産業領域を通じたサービス利用の拡大が我が国の経済活動や国民生活にもたらす変化や影響、国家の関与が疑われる事案も含めて急速に深刻化・巧妙化する脅威の状況、サイバーセキュリティをめぐる諸外国の動向等について、把握・分析し、将来を見据えたものとすること

第二　2020 年東京オリンピック・パラリンピック競技大会とその後を見据えた体制等の整備

次期戦略の期間中に開催される 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体制整備及び取組の強化を図り、サイバーセキュリティ対策に万全を期するものとすること。さらに、同大会で得た経験や知見等に基づき、大会後においても持続的なサイバーセキュリティの強化につながるものとすること

第三　次期戦略において新たに取り組むべき課題の明確化と対策の速やかな実施

「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 日サイバーセキュリティ戦略本部決定）に記載されている施策の取組状況を含め、現行戦略の実施状況等を踏まえつつ、新たに取り組むべき課題を明らかにし、速やかに対策を実施すること

そのうえで、政府においては、あらゆる主体が参加し、実空間（フィジカル空間）との一体化が加速的に進展するグローバルなサイバー空間の将来像を視野に入れつつ、それを支えるサイバーセキュリティの基本的な在り方を明確にし、次期戦略の策定に係る検討を開始する。