資料２

サイバーセキュリティ研究・技術開発の動向及び検討の方向性について

平成31年1月30日

サイバーセキュリティ戦略本部　研究開発戦略専門調査会
内閣サイバーセキュリティセンター（NISC）

1．サイバーセキュリティを取り巻く環境
（ICTの進展、脅威傾向、市場・技術動向など）

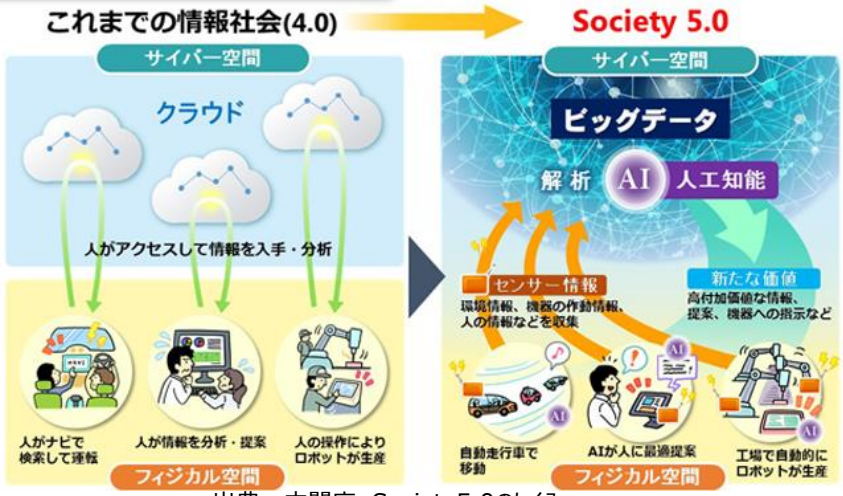
2．研究・技術開発に関する日本と各国の政策

3．本調査会における検討事項とスケジュール

今後のICTの進展

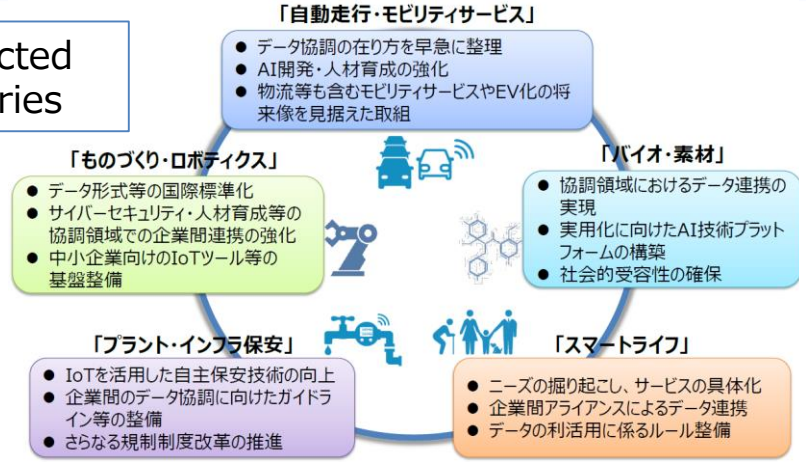
- 5GやAI，IoT等のテクノロジーの進化により、Society5.0が進展し、自動運転やスマートライフ等の新たなサービスが実現されるなど、サイバー空間と実空間の一体化がより一層進むと想定される。

Society5.0の進展



出典：内閣府　Society5.0のしくみ

Connected Industries



出典：経済産業省　Connected Industries

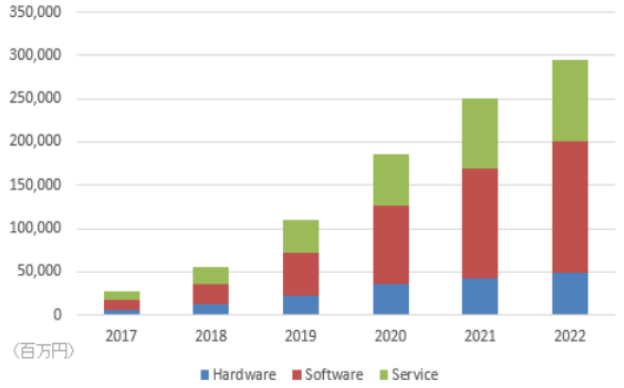
5G本格展開

出典：総務省　第5世代移動通信システムの技術的条件

AIの進化

- ・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
- ・2018年：ディベートシステム「Project Debater」がイスラエルのディベートチャンピオンに勝利

AIシステム市場 ユーザ支出額予測（セグメント別）



(出典) IDC Japan プレスリリース「国内コグニティブ／AIシステム市場予測を発表」

近年のサイバー攻撃の脅威傾向と将来予測

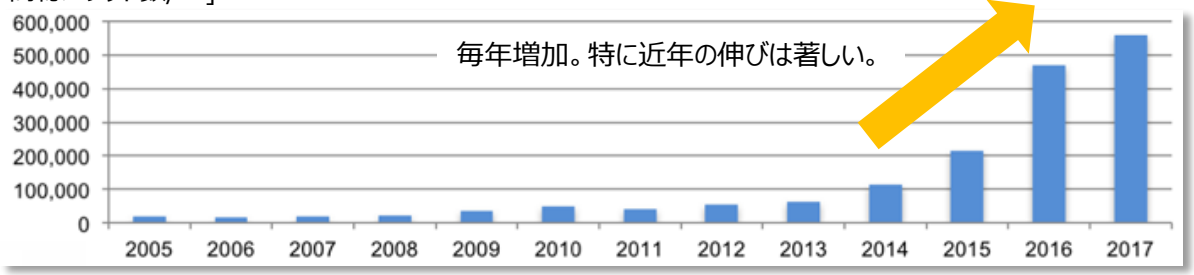
- ここ数年、観測されるサイバー攻撃の数（疑い含む）は増加傾向にあり、新種のマルウェアも毎年一定数発生。
- また、新たな脅威の発生（AI, IoT, 5G等の新技術やサプライチェーンをターゲットにした攻撃等）や攻撃者優位の拡大（新技術の悪用による攻撃の巧妙化・大規模化等）が予測されており、今後もその脅威は増大すると想定される。

近年の脅威傾向

IPアドレスあたりの年間総観測パケット数

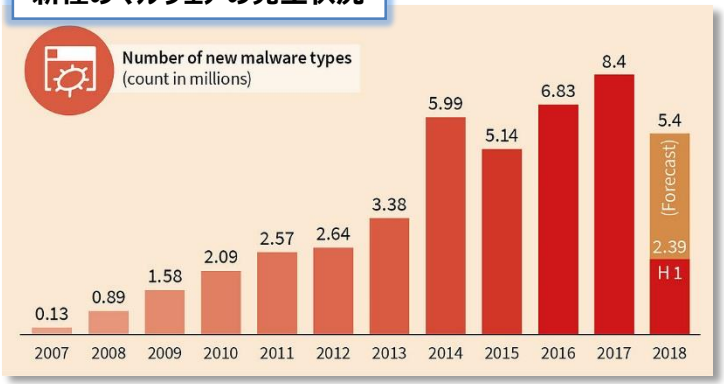
NICTの観測システム(Nicter)に届いたパケットの個数。マルウェアに感染した機器からのパケットやDoS攻撃を受けているサーバのパケットなど、サイバー攻撃の疑いの高いパケットが観測される。

[年間総パケット数/IP]



（出典）：Nicter観測レポート2017

新種のマルウェアの発生状況



（出典）：G DATA Security Blog：https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web

将来の脅威予測

シマンテックの予測

- 攻撃者は、人工知能（AI）システムに侵入し、攻撃にも AI 支援を利用する
- 防御側も、脆弱性を見極め反撃するために AI への依存度を強める
- 5G の配備と導入が進み、攻撃の範囲が拡大する
- IoT ベースの普及で、大規模 DDoS 攻撃を超えた新しく危険な攻撃が出現する
- サプライチェーンを悪用する攻撃が、質量ともに増大する

（出典）：シマンテック公式ブログ https://www.symantec.com/connect/ja/blogs/2019

McAfeeの予測

- 将来の回避技術における人工知能（AI）の更なる活用
- 音声認識機能を活用したIoTデバイスへの攻撃が次なる標的に

（出典）：McAfee公式ブログ https://blogs.mcafee.jp/mcafee-labs-2019-threats-predictions

トレンドマイクロの予測

- AI技術を利用した高度な標的型攻撃が確認される
- サイバー犯罪者同士によりIoTをめぐる「ワーム戦争」が勃発する

（出典）：トレンドマイクロ：2019年セキュリティ脅威予測 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181213-01.html

国内外のサイバー攻撃等の事案

【重要インフラ等の業務・機能・サービス障害】

○…国内　□…海外

□ 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。

□ 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**

【情報（個人情報・知的財産等）の毀損及び漏えい】

○ 日本年金機構への不正アクセス（2015年5月）

日本年金機構において、外部からの標的型メールに添付されたウイルスに感染したことにより、不正アクセスが行われ、**個人情報約125万件が外部に流出**した。

□ 米Facebook（2018年9月）

2018年9月、Facebook社はハッキングの被害を受け、**約5,000万件の利用者情報が流出したおそれ**があると発表

□ 米マリオット（2018年11月）

2018年11月30日、ホテルの予約データベースに不正なアクセスがあり、最大で**約５億人の利用客情報が流出したおそれ**があると発表。

2018年12月12日、**米国務長官は、このサイバー攻撃に中国が関与していると指摘**

○□ 中国を拠点とするAPT10の活動（2018年12月）

中国を含むG20メンバー国は、知的財産の窃取等の禁止に合意している中、中国を拠点とするAPT10といわれるグループからの日本の**民間企業、学術機関等を対象とした長期にわたる広範な攻撃を確認**。

12月20日から21日にかけて、**英国・米国等からAPT10に関して声明文が発表。12月21日、我が国もこれらの国を支持し、外務報道官談話を発出**

【金銭の窃取・詐取】

○ 国内大手航空会社ビジネスメール詐欺（2017年12月）

国内大手航空会社が、**偽の請求書メール**により、航空機リース料等の支払要求に応じ、**３億円を超える詐欺被害**に遭った。

○ 仮想通貨が不正に送信されたとみられる事案（2018年１月）

国内仮想通貨交換業者から**約580億円相当**の仮想通貨（NEM）が**不正に送信**されたとみられる事案が発生した。

○ 仮想通貨が不正に送信されたとみられる事案（2018年９月）

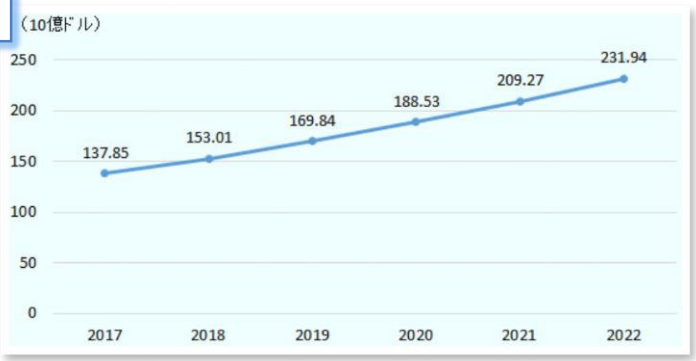
国内仮想通貨交換業者から合計**約70億円相当**の仮想通貨（Bitcoin, Monacoin, Bitcoin Cash）が**不正に送信**されたとみられる事案が発生した。

世界のサイバーセキュリティ市場予測と日本の状況

- サイバー攻撃の脅威の高まりとともに、サイバーセキュリティ製品・サービスの需要も高まっており、世界のサイバーセキュリティ市場は2018年に1,530億ドルに達し、2022年には2,300億ドルに至ると予測されている。同様に日本のサイバーセキュリティ市場も年々伸びている。
- 一方で、世界における我が国のセキュリティ製品シェアは低く、米国や欧州との差が大きい状況。また、日本市場への外資系企業の参入も相次いでいる。

世界と日本のサイバーセキュリティ市場予測

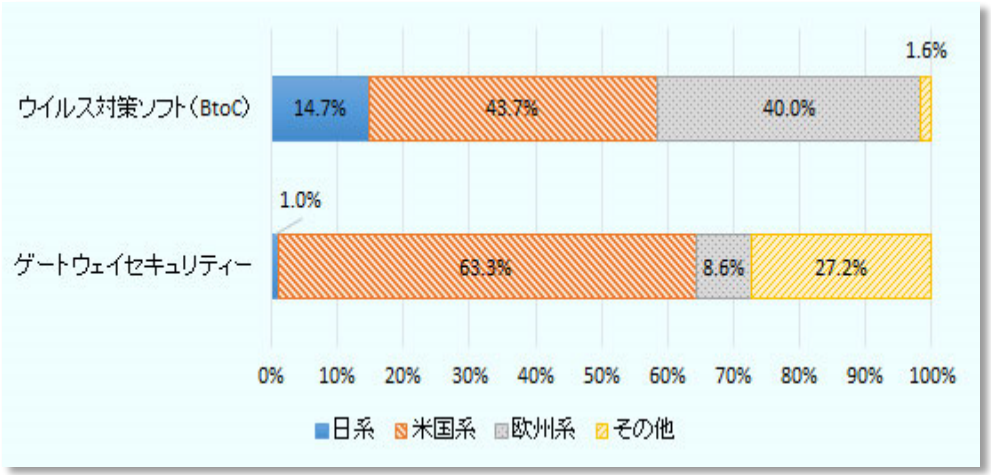
世界



日本

（出典）拡大するサイバーセキュリティ市場（JETRO）
https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html

セキュリティ関連製品の地域別市場シェア（2016年）

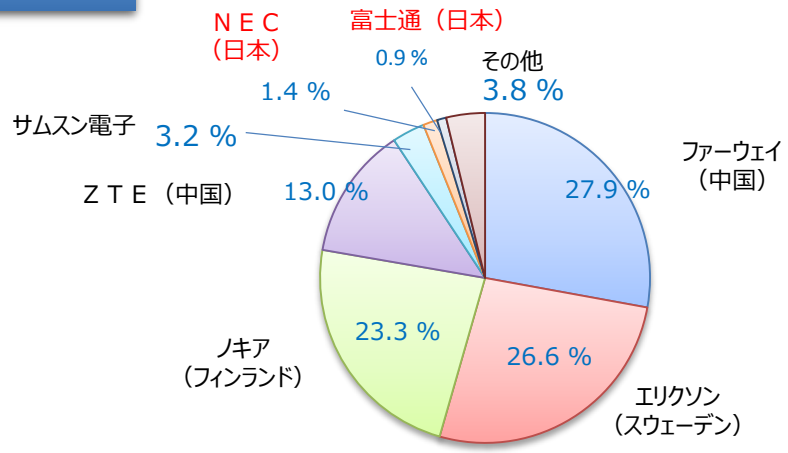


（出典）拡大するサイバーセキュリティ市場（JETRO）
https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html

ICT製品の市場シェアの状況

● サイバー攻撃から守る対象となる各種ICT製品についても、欧米や中国のシェアが高く、日本のシェアは低い状況。

基地局



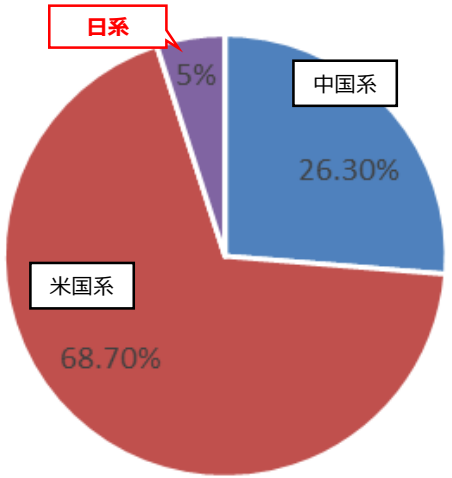
（出典）：IHS Markit 2017年

サーバ製品

サーバ製品シェア

会社	3Q18シェア
1. Dell Inc.	17.5%
2. HPE/New H3C Group	16.3%
3. Inspur/Inspur Power Systems	7.3%
4. Lenovo	6.2%
5. IBM	5.1%
5. Huawei	4.5%
5. Cisco	4.5%

（出典）IDC Worldwide Quarterly Server TrackerよりNISC作成



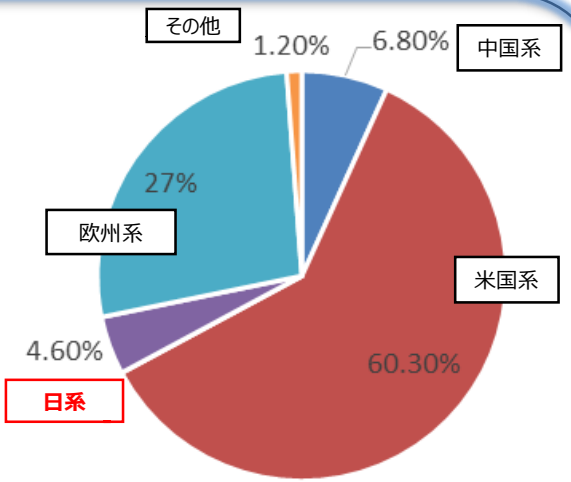
（出典）NEDO 平成29年度サービス・ソフトウェアの国際競争ポジションに関する情報収集

ルータ製品

ルータ製品シェア

会社	3Q18シェア
1. CISCO	42.7%
2. Huawei	23.5%
3. JUNIPER	13.4%

（出典）IDC記事よりよりNISC作成
https://www.idc.com/getdoc.jsp?containerId=prUS44527718



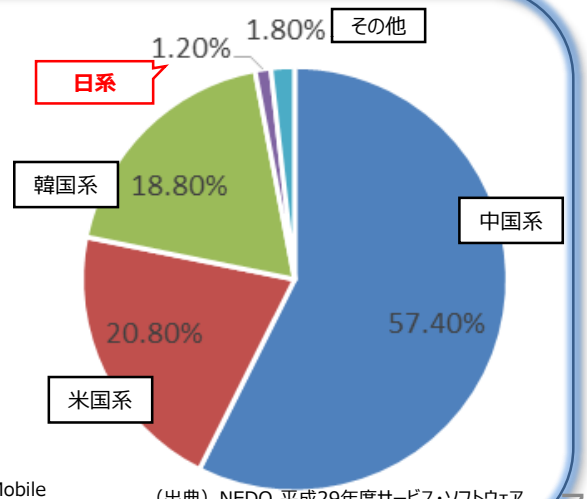
（出典）NEDO 平成29年度サービス・ソフトウェアの国際競争ポジションに関する情報収集

スマートフォン

スマートフォンシェア

Vendor	2Q18 Market Share
1. Samsung	20.9%
2. Huawei	15.8%
3. Apple	12.1%
4. Xiaomi	9.3%
5. OPPO	8.6%

（出典）IDC Worldwide Quarterly Mobile Phone TrackerよりNISC作成



（出典）NEDO 平成29年度サービス・ソフトウェアの国際競争ポジションに関する情報収集

グローバル企業と日本企業の研究開発投資額の比較

- 研究開発投資額のランキングを見ると、Amazon, Alphabet(Google親会社)等の世界で活躍しているICT企業が上位にラインクイン。両社とも売上高に占める研究開発投資額が10%を越えている。また、中国ICT大手企業の研究開発投資額も伸びている。
- 一方、日本企業は、ヘルスケア分野を除き10%未満の状況であり、総じて低い。

研究開発投資額グローバルランキング

順位(2018)	順位(2017)	順位の変化	社名	本社所在地	業種	R&D支出(10億ドル)	売上高(10億ドル)	対売上高R&D支出比率(%)
1	1	0	アマゾン	北米	ソフトウエア・インターネット	22.6	177.9	12.7%
2	2	0	アルファベット	北米	ソフトウエア・インターネット	16.2	110.9	14.6%
3	5	↑ +2	フォルクスワーゲン	欧州	自動車	15.8	277.0	5.7%
4	4	0	サムスン	その他	コンピュータ・エレクトロニクス	15.3	224.3	6.8%
5	3	↓ -2	インテル	北米	コンピュータ・エレクトロニクス	13.1	62.8	20.9%
6	6	NA	マイクロソフト	北米	ソフトウエア・インターネット	12.3	90.0	13.7%
7	9	↑ +2	アップル	北米	コンピュータ・エレクトロニクス	11.6	229.2	5.1%
8	7	↓ -1	ロシュ	欧州	ヘルスケア	10.8	57.2	18.9%
9	12	↑ +3	ジョンソン・エンド・ジョンソン	北米	ヘルスケア	10.6	76.5	13.8%
10	8	↓ -2	メルク・アンド・カンパニー	北米	ヘルスケア	10.2	40.1	25.4%
11	11	0	トヨタ自動車	日本	自動車	10.0	259.9	3.9%
12	10	↓ -2	ノバルティス	欧州	ヘルスケア	8.5	50.1	17.0%
13	15	↑ +2	フォード	北米	自動車	8.0	156.8	5.1%
14	20	↑ +6	フェイスブック	北米	ソフトウエア・インターネット	7.8	40.7	19.1%
15	14	↓ -1	ファイザー	北米	ヘルスケア	7.7	52.6	14.6%

（出典） PWC Strategy& 2018年グローバル・イノベーション1000調査結果概要
（ただし中国企業は除く）

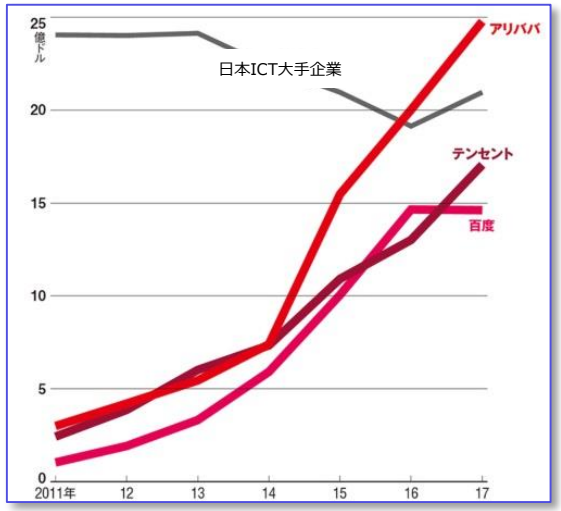
日本ランキング

順位(2018)	順位(2017)	グローバル順位(2018)	社名	業種	R&D 支出(10億ドル)	売上高(10億ドル)	対売上高R&D支出比率(%)
1	1	11	トヨタ自動車	自動車	10.0	259.9	3.9%
2	2	18	本田技研工業	自動車	7.1	131.8	5.4%
3	3	37	日産自動車	自動車	4.6	110.4	4.2%
4	4	38	ソニー	コンピュータ・エレクトロニクス	4.3	71.6	6.0%
5	5	39	パナソニック	コンピュータ・エレクトロニクス	4.2	69.2	6.1%
6	6	40	デンソー	自動車	4.2	42.6	9.9%
7	↑ 8	51	日立製作所	コンピュータ・エレクトロニクス	3.1	86.3	3.6%
8	↑ 9	53	武田薬品工業	ヘルスケア	3.1	16.3	18.8%
9	↑ 10	54	キャノン	コンピュータ・エレクトロニクス	2.9	36.2	8.1%
10	↓ 7	55	東芝	工業製品	2.8	46.2	6.0%

（出典） PWC Strategy& 2018年グローバル・イノベーション1000調査結果概要

中国ICT大手の研究開発投資額の推移

アリババ、テンセント、百度は2013年頃から売上高の10%前後を研究開発に投資



（出典） 米PWC調査をもとに
NISC作成

参考：グローバルICT企業のセキュリティへの投資例

Amazonの例

AWSのセキュリティ強化のため、暗号技術者を多数採用。

Amazon is quietly doubling down on cryptographic security

Ingrid Lunden @ingridlunden / 5 months ago

Now it appears that one of the leading companies in cloud services is looking for more ways to double down and fight the latter. Amazon's AWS has been working on a range of new cryptographic and AI-based tools to help manage the security around cloud-based enterprise services, and it currently has over 130 vacancies for engineers with cryptography skills to help build and run it all.

（出典） techcrunch:https://techcrunch.com/2018/08/30/amazon-aws-cryptography-security/

アリババの例

ネットワークセキュリティを含む研究開発費を２倍超に。

アリババ、研究開発費を２倍超に拡大－ＡＩなどに３年で１兆6900億円

中国の電子商取引会社アリババ・グループ・ホールディングは研究開発費を２倍余りに増やし、向こう３年で150億ドル（約１兆6900億円）とする。次世代技術を開発し、業界を一変させる可能性のあるムーンショット（困難だが実現すれば大きな影響をもたらし得る挑戦）プロジェクトを探る。

アリババは世界各地に研究所を７カ所設立し、研究員を100人採用すると電子メールを通じて発表した。人工知能（ＡＩ）やインターネット・オブ・シングス（ＩｏＴ）、量子コンピューティングの研究に従事し、特定分野では機械学習やビジュアルコンピューティング、ネットワークセキュリティーなどを含むとしている。

（出典）Bloomberg: https://www.bloomberg.co.jp/news/articles/2017-10-11/OXN1C56S972901

Alphabetの例

先端的なサイバーセキュリティ技術にフォーカスした企業の立ち上げ。

AlphabetがXムーンショット生まれのサイバーセキュリティ企業Chronicleを立ち上げ

2018年1月25日 by Frederic Lardinois

あなたが、まだ間違って"Google"と呼んでるかもしれないAlphabetが今日（米国時間1/24）、新しいサイバーセキュリティ企業Chronicleの立ち上げを発表した。それは、企業のハッカー検出と撃退能力を高めることがねらいだ。ChronicleはAlphabetのXムーンショットグループから巣立ち、今ではGoogleなどと同じく、Alphabet傘下の単独企業だ。

（出典）techcrunch:https://jp.techcrunch.com/2018/01/25/2018-01-24-alphabet-launches-new-cybersecurity-company-chronicle-out-of-its-x-moonshot-factory/

テンセントの例

ブロックチェーンに注力し、高い評価。広い分野で積極に応用。

テンセントのブロックチェーン技術、信用審査で高い評価

中国ネットサービスの騰訊控股（テンセント）は10月に中国政府系機関が開催したブロックチェーンのカンファレンスで、ブロックチェーンの信用における審査および評価で優勝した。同社のブロックチェーン技術は電子インボイスやゲーム、金融、医療といった分野での応用を実現しており、今後もより広い分野で積極的に応用領域を拡大していく。

（出典） nikkeibp: https://trend.nikkeibp.co.jp/atcl/contents/technology/00004/00064/

スタートアップを取り巻く環境と日本のプレゼンス

- 高度化・巧妙化するサイバー攻撃に対抗すべく、世界的に先端技術を開発する新興企業が多数生まれているが、米国やイスラエルが中心。
- サイバーセキュリティ分野で活躍している企業のランキング調査等においても、日本企業は上位にランクインしていない。また、スタートアップの成長しやすい拠点ランキングでも同様の結果が出ている。
- 一方で、日本でもスタートアップを支援する施策によりサイバーセキュリティ関連のスタートアップ企業も出てきている。

サイバーセキュリティ トップ500

Cybersecurity 500

Meet the world's hottest and most innovative cybersecurity companies to watch in 2018. Press Release

Cybersecurity 500 By The Numbers: Breakdown By Region

search by keyword　search

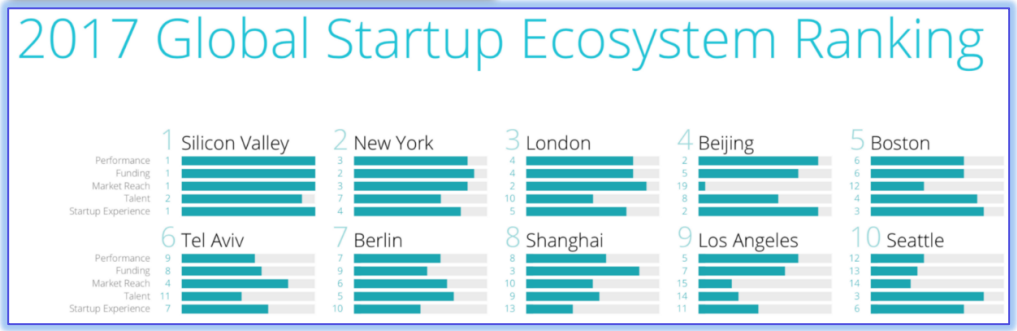
Showing 1-100 of 500　100 per page　Page 1 of 5

#	Company	Cybersecurity Sector	Corporate HQ
1	Herjavec Group	Information Security Services	Toronto, Canada
2	KnowBe4	Security Awareness Training	Clearwater FL
3	CyberArk	Privileged Access Security	Petach-Tikva, Israel
4	Raytheon Cyber	Cyber Security Services	Waltham MA
5	Cisco	Threat Protection & Network Security	San Jose CA
6	IBM Security	Enterprise IT Security Solutions	Waltham MA
7	Microsoft	Datacenter to Endpoint Protection	Redmond WA
8	Amazon Web Services	Cloud-Powered Security	Seattle WA
9	FireEye	Advanced Threat Protection	Milpitas CA
10	Lockheed Martin	Cybersecurity Solutions & Services	Bethesda MD
11	Check Point Software	Unified Threat Management	Tel Aviv, Israel
12	RSA	Intelligence Driven Security	Bedford MA
13	Symantec	Endpoint, Cloud & Mobile Security	Mountain View CA

500社中、日本は3社のみ。上位へのランクインはない。

（出典）CYBERSECURITY VENTURES Cybersecurity 500

スタートアップの成長しやすい拠点



（出典）Startup Genome：Global Startup Ecosystem Report 2017

上記はICT全体のランキング。サイバーセキュリティ分野では、ニューヨーク、ボストン、シリコンバレー、フェニックス、トロント・ウォータールー、オタワ、ハーグ、フランクフルト、ベルリン、プラハ、テルアビブ、ベエルシェバが主要拠点とされている。

日本のスタートアップ支援プログラム

J-Startup

- 世界で戦い、勝てるスタートアップ企業を生み出し革新的な技術やビジネスモデルで世界に新しい価値を提供するスタートアップ企業の育成支援プログラム。
- プリファードネットワークス社（深層学習フレームワークの開発・提供等）やカウリス社（法人向け不正アクセス検知サービスの提供）が参画。

国内外のセキュリティ学会における日本の状況

- 国内のセキュリティ学会では、暗号・認証等の基盤技術のほか、IoT・AI等の動向を踏まえた応用技術に関する研究発表が広く行われている。
- 暗号については、海外のセキュリティ学会でも一定数の論文が採択されており、強みを有している分野である。

国内のセキュリティ学会の研究発表テーマ

コンピュータセキュリティシンポジウム2018
主催：情報処理学会コンピュータセキュリティ協会

01.暗号要素技術・評価
02.署名・暗号プロトコル
03.視覚的・物理的暗号技術
04.情報ハイディング
05.ネットワーク監視・追跡
06.マルウェア検知・解析
07.Web・クラウド・メールセキュリティ
08.アクセス制御
09.認証・バイオメトリクス
10.システムセキュリティ・設計・実装
11.OS・仮想化
12.ハードウェア・組み込み・制御システム
13.IoT機器・ユビキタスセキュリティ
14.電子商取引・暗号通貨
15.コンテンツ保護
16.ソフトウェア保護
17.AI・機械学習とセキュリティ
18.リスク管理・セキュリティポリシー
19.インシデント対策・管理
20.CSIRT
21.セキュリティ評価・監査
22.プライバシー保護・匿名化
23.デジタルフォレンジック
24.セキュリティ教育・法律
25.心理学とトラスト
26.その他

海外のセキュリティ学会における論文採択状況

会議名	論文総数	日本の採択数 ＊日本の組織が著者の一人である論文数	著者の所属
Crypto 2018	79	6 ＊暗号	NTT, 産総研, NICT, 横浜国大など
NDSS 2019	89	1 ＊攻撃検知	NICT
ACMCCS 2018	134	2 ＊秘密計算、攻撃予測	NEC, KDDI

SCIS2019
主催：電子情報通信学会

暗号関連（暗号理論，情報理論的安全性，公開鍵暗号，楕円・超楕円曲線暗号，格子暗号，秘密計算，高機能暗号，共通鍵暗号，ブロック暗号，ストリーム暗号，ハッシュ関数，署名，認証など）耐量子暗号，量子暗号・量子計算，ハードウェアセキュリティ，PUF，サイドチャネル攻撃，ネットワークセキュリティ，ネットワーク攻撃検知・対策，マルウェア対策，ウェブセキュリティ，クラウドセキュリティ，モバイルセキュリティ，組み込みセキュリティ，制御システムセキュリティ，自動車セキュリティ，フィンテック，ブロックチェーン，電子透かし，コンテンツ保護，ソフトウェア保護，プライバシー保護，生体認証・バイオメトリクス，教育・心理学，セキュリティ評価・モデル，IoTセキュリティ

1．サイバーセキュリティを取り巻く環境

（ICTの進展、脅威傾向、市場・技術動向など）

2．研究・技術開発に関する日本と各国の政策

3．本調査会における検討事項とスケジュール

サイバーセキュリティ研究開発戦略（概要）

平成29年7月13日サイバーセキュリティ戦略本部決定

NISC

【趣旨】

○情報通信技術（ＩＴ）の進化や、人間と情報の関わり方が変化していることを踏まえつつ、将来的（近い将来、中長期）なサイバーセキュリティ研究開発の方向性についてビジョンを提示

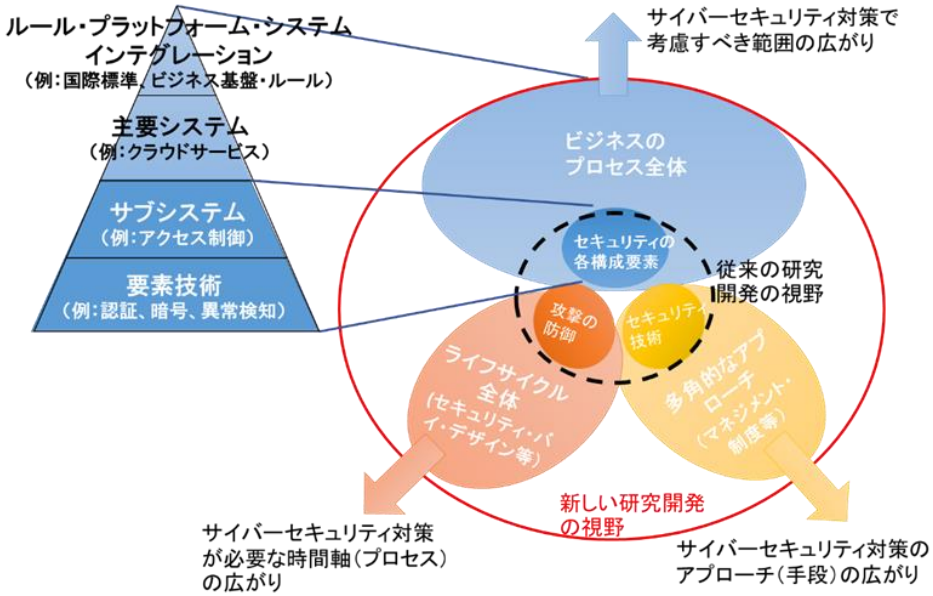
【近い将来】

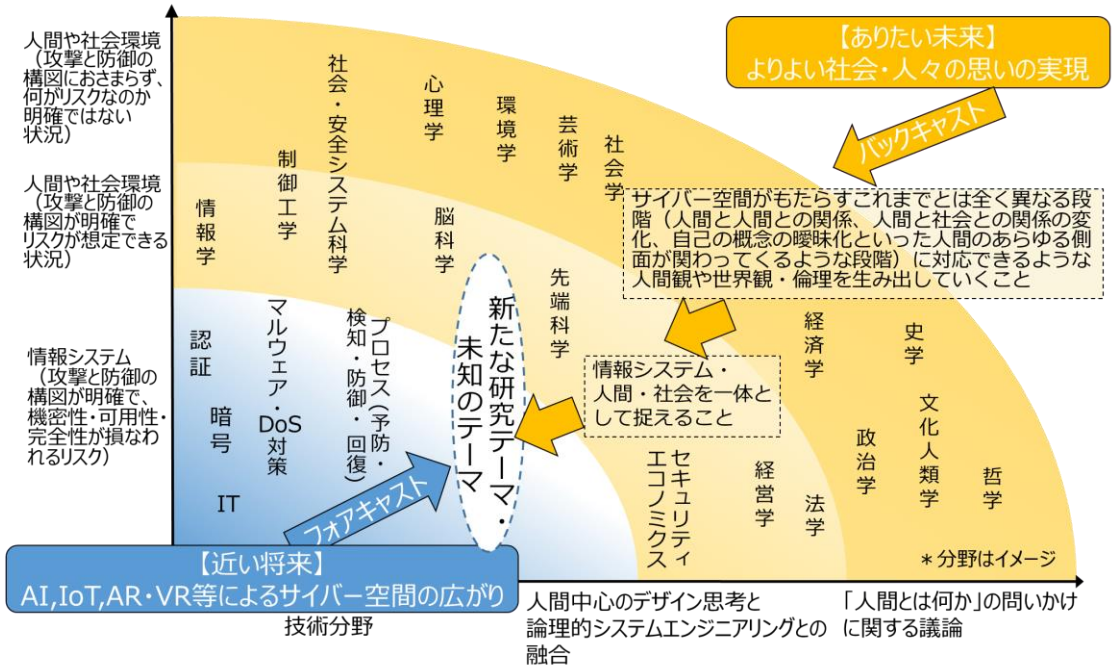
情報システムの進化（つながる（IoT）、知能化する（AI）、広がる(ネットワーク技術)）**を見据え、研究開発の視野を広げることが必要**

IoT、AI、AR・VR等
ITのさらなる進化

【中長期】

サイバーセキュリティの考え方の再定義：情報システムだけでなく、社会や人間を一体として捉えることが必要





【今後の取組】

○人文社会科学分野を含め、本戦略を発信し、具体的な研究分野やテーマについて検討を行うなど、具体化に取り組む。

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。

諸外国のサイバーセキュリティ研究開発に関する取組

米国 (参考1)

- 研究開発に特化した戦略「2016 Federal Cybersecurity Research and Development Strategic Plan 」を策定。 4つのサイバーセキュリティ対策のカテゴリ（阻止、防御、検知、適用）を定義し、それぞれについて、短期・中期・長期の研究開発の取組を規定。
- 毎年度、実行計画「Implementation Roadmap」を策定し、NIST, NSF, NSA, DARPA, DHS, DoD等を中心に産学官が連携して研究開発を推進。
- 2019年度要求で7.4億ドルの予算を計上。

英国 (参考2)

- 全体戦略の「NATIONAL CYBER SECURITY STRATEGY 2016-2021」において、①DEFEND（防御）, ②DETER（阻止）, ③DEVELOP（開発）を柱に掲げ、特に③の部分で研究開発を位置付け。
- 「cyber security science & technology strategy」において重点分野（IoTとスマートシティ, データと情報保護, 自動化、機械学習とAI等）を特定。
- 政府主導の下、ACE (Academic Centre of Excellence)と呼ばれる枠組みの下、認定基準をクリアした大学が中心となって研究開発を推進。

イスラエル (参考3)

- 全体戦略の「ISRAEL CYBER SECURITY STRATEGY」にて、①ロバストネス（頑健性）②レジリエンス（強靭性）、③ディフェンス（防御）の3つの柱を掲げ、これらに必要な能力構築の一環として研究開発を位置付け。
- ベングリオン大学、テルアビブ大学等の６つの大学において、政策や技術等の異なる分野に焦点を当てたサイバーセキュリティ研究センターを設置。
- 政府主導プロジェクトとして、南部ベルシェバに産・官・学・軍が同居する「サイバースパーク」を設置。サイバー分野でのエコシステムを生み出し、イノベーション活性化を狙う。

シンガポール (参考4)

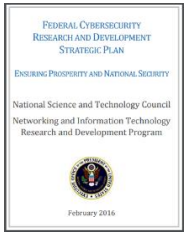
- 全体戦略の「Singapore Cybersecurity Strategy 2016」において、①弾力性のあるインフラ構築、②より安全なサイバー空間の維持、③活気あるサイバーエコシステムの開発、④国際パートナーシップの強化の４つの柱を掲げ、特に③の部分で研究開発を位置付け。
- 実行計画である「National Cybersecurity R&D Programme(NCR)」において、2020年までのR&D実行計画を策定。
- 産・学・官の連携組織として、シンガポールサイバーセキュリティコンソーシアムを設立。

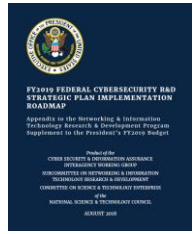
参考1:米国の連邦サイバーセキュリティ研究開発戦略プラン

○　国家科学技術会議（NSTC）が主導して策定した「2016年連邦サイバーセキュリティ研究開発戦略プラン」に基づいて具体的な注力分野を特定。
○　研究開発の実行計画を年度ごとに策定し、産学官において推進。

✓ 4つのサイバーセキュリティ対策のカテゴリ（Deter：阻止, Protect：防御, Detect：検知, Adapt：適用）を定義し、短期、中期、長期の取組を規定。
加えて、上記を活かす先端的技術として、以下の分野の研究開発に注力。

①サイバーフィジカルシステム, IoT　　④自律システム
②クラウドコンピューティング　　⑤モバイル機器
③高性能計算





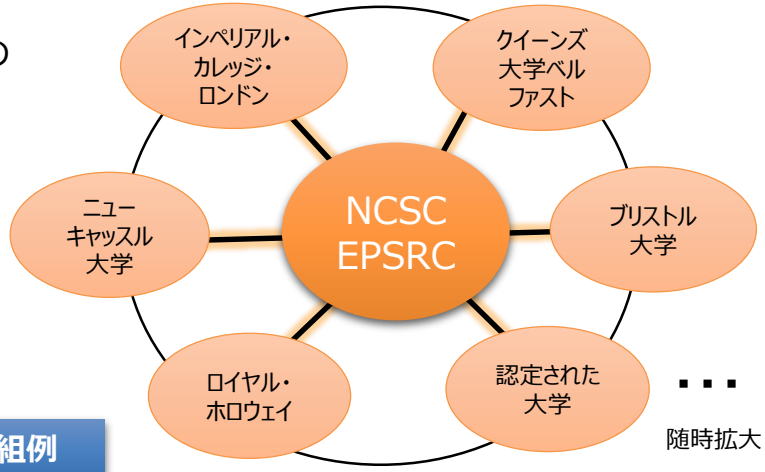
✓ NIST, NSF, NSA, DARPA, DHS, DoD等が、本戦略に基づく実行計画を年度ごとに策定し、産・学と連携しながら研究開発を推進。2019年度要求で7.4億ドルの予算を計上(プライバシー分野も含む)。

	Deter（阻止）	Protect（防御）	Detect（検知）	Adapt（適用）
短期	• 攻撃レベルの測定基準 • 攻撃抑止と犯罪・経済制裁の関係性評価	• セキュアなアップデートメカニズムの開発 • エビデンスベースのアセスメント技術 • 軽量暗号、プライベートデータベース、耐量子計算機暗号	• ネットワークをマップするための自動化ツール • セキュリティオペレーションツールのUI改善	• 攻撃が発生しても、重要な資産の利用継続が可能となる技術
中期	• リアルタイムのアトリビューション	• 脆弱性を減らす静的・動的解析ツール • セキュリティポリシー導出自動化ツール • 98%の確率でSWとHWの真正性を検証するツールと技術	• 悪意のあるサイバー活動の特定（フォルスポジティブ率、フォルスネガティブ率の低減）	• 相互依存システムの機能のタイムリーな回復
長期	• 正確かつ効率的な攻撃者の特定	• 10万行のコードあたり1つの欠陥を持つソフトウェアの開発をサポートするツール • 10年間で2桁のオーダーでセキュリティ制御の有効性と効率を向上	• 自動サイバー脅威予測ツール	• 適応的で効果的な集団防御

参考2:英国のACE (Academic Centre of Excellence)の概要

○　英国サイバーセキュリティセンター（NCSC）と工学・物理科学研究評議会（EPSRC）による認定基準をクリアした大学により構成されるACE(Academic Centre of Excellence)の枠組みを中心に、サイバーセキュリティの研究開発を推進。

- ✓ 2001年に、「英国のサイバー攻撃に対するレジリエンス向上」のための産学官連携を目的としてEPSRCとGCHQによりACEの枠組みを立上げ（その後、GCHQの役割をNCSCが継承）。
- ✓ 2019年1月時点で17の大学が認定を受けて参加。
- ✓ 認定された大学に対して、毎年約20,000ポンドの助成金を付与。



参加大学が注力している研究分野

- 暗号、鍵管理および関連プロトコル
- 情報リスクマネジメント
- システムエンジニアリングとセキュリティ解析
- 情報保証の方法論
- 運用保証技術
- 戦略技術と製品の安全性に関する研究
- サイバーセキュリティと人的要因の科学
- 信頼性と信頼性の高いシステムの構築

ACE 認定大学の取組例

大学名	専門分野
インペリアル・カレッジ・ロンドン	以下を含むセキュアかつレジリエントなソフトウェアシステム工学 ・運用システムと情報アシュアランス ・セキュリティ分析とシステム検証
ニューキャッスル大学	・ソーシャル技術を用いたサイバー犯罪 ・インフラのセキュリティアシュアランス ・サイバーセキュリティ科学
クイーンズ大学ベルファスト	・サイバーフィジカルシステムセキュリティ ・リアルタイムネットワーク分析と仮想化 ・高機能/省電力暗号アーキテクチャ
ロイヤル・ホロウェイ	・理論的かつ実践的な暗号アプリケーション ・サイバーセキュリティの社会的、技術的、組織的観点 ・RFIDタグやスマートタグ、組込機器の情報アシュアランス

参考3:イスラエルのサイバーセキュリティエコシステム

○　軍・産・官・学が連携したサイバーセキュリティエコシステムが特徴。サイバーセキュリティ研究センターを中心とした学術エコシステムとスタートアップを多数輩出するサイバースパークが存在。

✓ 安全保障分野を端緒とした学術エコシステム

- ベングリオン大学、テルアビブ大学等の６つの大学に、政策や技術等の異なる分野に焦点を当てたサイバーセキュリティ研究センターを設置。学術エコシステムとして機能している。
- 国防分野におけるサイバーセキュリティへの投資がエコシステムの原動力。
- 人材育成においては、中等教育と兵役期間中の専門教育の影響大。高校からサイバー分野の教育を実施し、サイバー分野の適性のある者は、高校卒業後の兵役期間中にサイバー関連部署に配属されて専門能力を習得。兵役終了後、大学や民間で活躍。

✓ サイバースパークの設立

- ネタニヤフ首相及び国家サイバー局のイニシアチブにより、南部都市ベルシェバに2014年に設置。サイバー分野のエコシステム活性化を狙う地理的な産・官・学・軍のクラスター。
- 企業では、ドイチェテレコム、EMC、ロッキードマーティン、オラクル、IBMなどの多国籍企業やJVPなどのベンチャーキャピタルが入居しており、多数のスタートアップが活動中。

参考4:シンガポールの国立サイバーセキュリティ研究開発プログラム

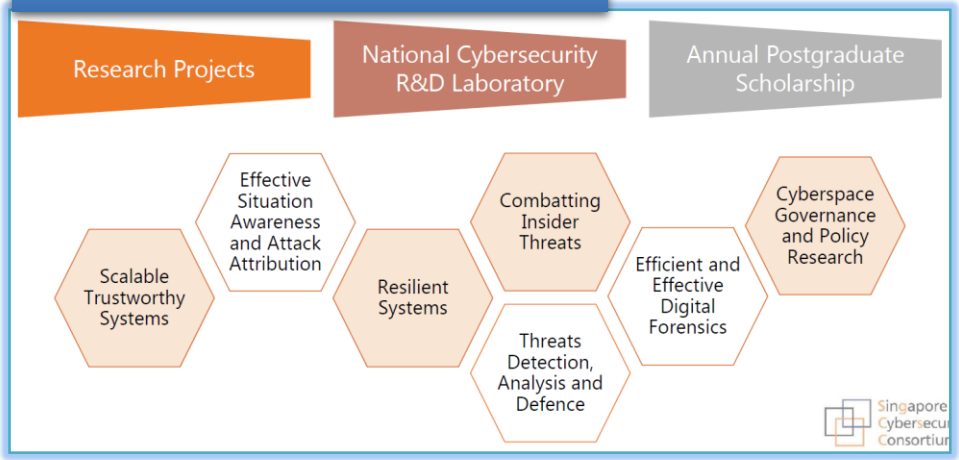
○ 2013年に策定した「サイバーセキュリティ研究開発プログラム」に基づき、シンガポール国立大学、国立研究財団（NRF）が中心となり、サイバーセキュリティに係る研究開発を推進。
○ また、産学官連携組織としてシンガポールサイバーセキュリティコンソーシアムを設立。

✓ 研究開発の注力分野として以下の6つテーマを挙げ、シンガポール国立大学、国立研究財団（NRF）が中心となって研究開発を推進。2020年までに総額1.9億ドルを予算として計上。

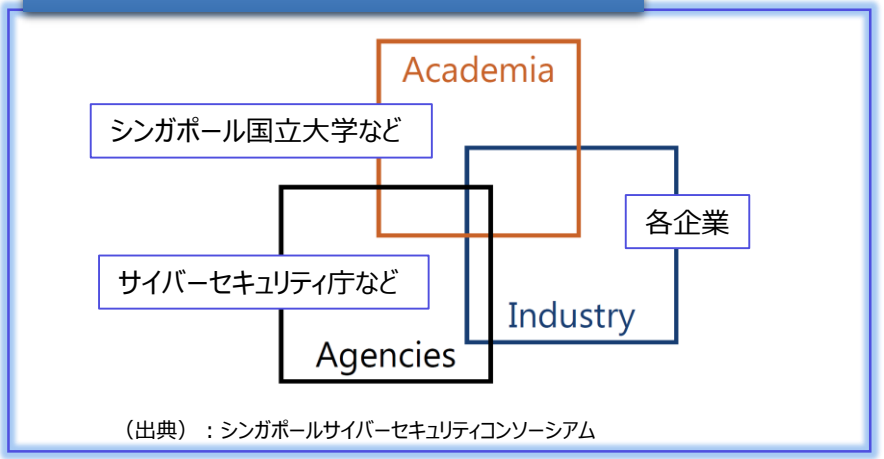
①拡張性のあるトラスト確保システム（Scalable Trustworthy Systems）
②レジリエントシステム（Resilient Systems）
③効果的な啓発と攻撃の特定（Effective Situation Awareness and Attack Attribution）
④内部犯行（Combatting Insider Threats）
⑤脅威検出、分析、防御（Threats Detection, Analysis and Defence）
⑥効率的かつ効果的なデジタルフォレンジック（Efficient and Effective Digital Forensics）

✓ また、2016年にサイバーセキュリティにおける研究、人材育成、啓発を目的とした産学官連携組織としてシンガポールサイバーセキュリティコンソーシアムを設立。

国立サイバーセキュリティ研究開発プログラム



シンガポールサイバーセキュリティコンソーシアム



（出典）：シンガポールサイバーセキュリティコンソーシアム

1．サイバーセキュリティを取り巻く環境

（ICTの進展、脅威傾向、市場・技術動向など）

2．研究・技術開発に関する日本と各国の政策

3．本調査会における検討事項とスケジュール

主な検討事項（１／２）

- 新たなサイバーセキュリティ戦略等を前提としつつ、サイバー空間における脅威の状況や、AI、IoT、５G等の活用拡大を踏まえ、**サイバーセキュリティの研究・技術開発の推進方策について、具体的に検討していく**ことが必要。
- この点に関して、諸外国においては、それぞれの国の特性を活かした仕組み・エコシステムが構築されている。
- 本調査会においては、**国産技術の育成も視野**に入れつつ、**「注力すべき分野の特定」、「必要となる技術の育成」、「ビジネスへの展開」**といった流れで検討を進めるべきではないか。

１．注力すべき分野の特定

○現状把握
・我が国では、サイバーセキュリティの研究・技術開発について、**どのような分野を中心に取組が進められているか**。
・諸外国とも比較した際、それぞれ**どのような水準**にあると考えられるか。

○分野の特定
・今後、サイバー空間における脅威の増大やサプライチェーンリスクの高まり、AI、IoT、5Gの活用の一層の拡大に鑑み、**どのような分野の研究・技術開発に注力していくことが必要と考えられるか**。
【注力すべきと考えられる分野の例】
・サプライチェーンリスクへの対応強化等に向けた、**トラストの証明に関する取組**
・AI等も活用したリアルタイムでの**攻撃把握の分析と、それを活用したセキュリティ対策の開発**
・IoT機器の増大や量子計算機の実現等に関連する、**暗号技術に関する新たな課題を見据えた研究開発**
・その他、どのような課題が考えられるか。

主な検討事項（２／２）

２．必要となる技術の育成

○重点課題の推進
- **重点的に取り組むべき課題**（例として、トラスト確保、攻撃把握・分析・共有、暗号のための技術等）について、**ロードマップを策定して関係機関が連携して取り組む**ことが必要ではないか。その際には、**国産技術の育成の観点**からの検討も必要ではないか。
- **サイバー攻撃に関するデータ**については、研究・技術開発のベースとしての重要性に鑑み、より活用しやすくなる方策が必要ではないか。

○環境整備
- **我が国のサイバーセキュリティの研究・技術開発を担う人材**を、どのように育成していくべきか。
- 諸外国において、**大学間の協力や、国際的な連携**も見られる中、産学官の連携をどのように進めていくべきか。
- 国産技術の育成と併せて、既製の製品・サービスの**セキュリティの検証のための技術**も必要ではないか。
- その他、制度上の課題など、検討が必要な課題はあるか。

３．ビジネスへの展開

○製品・サービスの開発支援や、マーケティング支援
- **日本発のサイバーセキュリティの製品・サービスのシェアが低い状況の要因**は、どのような点にあるか。例えば、通信設備自体のシェアが低いことが、セキュリティ製品・サービスの導入においての障害の一因となっているのではないか。
- サイバーセキュリティに関する**技術のビジネス化**や、市場獲得のための**マーケティング活動**への支援について、どのような施策を講じていくべきか。

○スタートアップ企業の育成支援
- **スタートアップ企業の育成**は、国産製品・サービスを生み出していく上で重要であるが、諸外国と比較し必ずしも活発ではない状況。どういった点が不足しているか、また、どのような支援が求められるか。

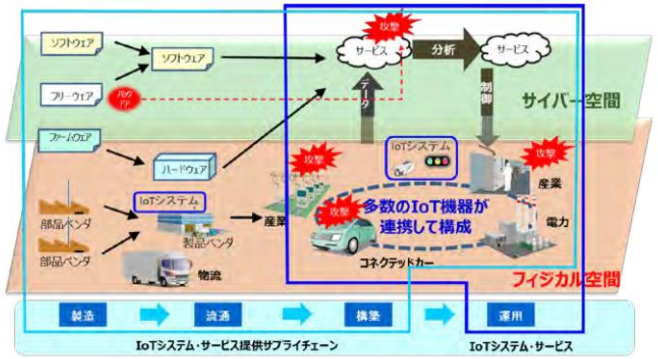
重点分野の課題例①：トラスト確保のための取組

- Society5.0の進展とともにサイバー空間と実空間の一体化が進む等、サプライチェーンの複雑化が想定される。また、世界的にもサプライチェーンリスクへの対応強化を求める枠組みの整備等が進んでいる。
- これらを受け、製品のトラストの証明（例：脆弱性、トロイ等の不正機能への適切な対応等）、利用するICT機器・サービス等のトラストを確保するための先端研究、技術的検証体制の整備等が重要な課題となっている。

＜課題例＞
- トラスト確保のための総合的対策の策定、対策を支える先端研究の促進（ハードウェアトロイの検出等）
- 技術的検証を行うための産学官の体制整備

サプライチェーンの複雑化

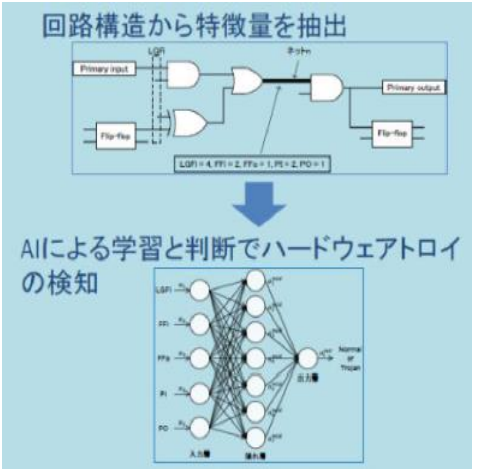
Society5.0の世界では、多様な要素（人、組織、製品、システム、サービス、データ等）が相互に連携・融合して構成されることから、一企業として取組むセキュリティ対策だけでは限界



（出典）戦略的イノベーションプログラム　IoT社会に対応したサイバー・フィジカル・セキュリティ　研究開発計画

ハードウェアトロイの検出

IoT機器などのハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を実施。未知のハードウェアトロイを誤りなく検知することが目標



(出典)：未知なる脅威、ハードウェア・トロイに挑む
https://www.waseda.jp/top/news/55572

サプライチェーンに関連するグローバル規格等の動向

【米国】
- NIST SP800-171
  政府機関の情報システム等における非CUI保護を目的としたサイバーセキュリティ対策の要件を規定
- Cybersecurity Framework
  サプライチェーンのリスク管理項目を追加

【欧州】
- NIS Directive
  重要インフラに対し、最新のサイバーセキュリティ対策の実装を要求
- サイバーセキュリティ認証フレームワーク導入検討
  ネットワークに接続する機器のセキュリティに関して、認証・確認するための自主的フレームワークを整備

重点分野の課題例②：攻撃把握・分析・共有

- AIやIoT等の進展により、新たな脅威の増加も想定される中、リアルタイムでの攻撃把握、予兆の検知、攻撃挙動の分析等がますます重要となる。
- また、サイバー防御に係る技術開発の推進や深層学習（Deep Learning）のような新技術の活用にあたっても、サイバー攻撃に関するデータの必要性・重要性が増しており、関係のデータを把握し、関係者で共有できるような仕組み作りが必要とされている。

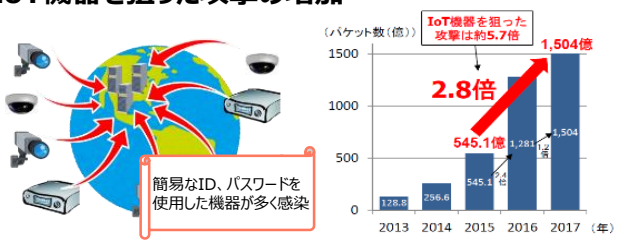
＜課題例＞

- 我が国における攻撃観測連携基盤の構築
- 観測された攻撃データとDeep Learningによる深層解析
- 攻撃データ共有のための仕組み作り

新たな脅威の増加

IoTの普及、SNS・ネットショッピングの利用拡大等が人々の生活に様々な恩恵をもたらす一方で、IoT機器を狙った攻撃が増加したり、ランサムウェアの被害が発生。

IoT機器を狙った攻撃の増加



出典：総務省　IoTセキュリティ総合対策プログレスレポート2018

ランサムウェアの脅威

・2018年度も昨年度に引き続き、被害が発生

・手動で感染を広げることで高度な攻撃を行うもの等、感染手口が高度化

サイバーセキュリティ関連情報の共有

サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とするサイバーセキュリティ・ユニバーサル・リポジトリを構築

（出典）NICT
http://www.nict.go.jp/cyber/index.html

データの必要性

AIとセキュリティ 佐々木 良一

セキュリティ対策のためにＡＩを実際に利用するにあたっては、以下のような問題を解決することが望ましい。しかし、これらをどのように解決したか言及しているものは少ない。

（１）ＡＩシステムは適切に分類された大規模なデータセットを得ることが望ましいが、この分野でこのようなデータセットを入手するのは一般に困難である。特に、サイバー攻撃は時間とともに特性が変化することが多く、それぞれの期間における大量のデータの入手が必要となるが困難なことが多い。

（出典）デジタル・フォレンジック研究会 第５３１号コラム

Is Big Data Enough for Machine Learning in Cybersecurity?

Data and machine learning in cybersecurity

機械学習やサイバー攻撃への即時対応にデータが必要

Fundamentally, machine learning requires data to be operational. Threat data is necessary to combat cyberattacks at zero-time, as in the case of far-reaching ransomware attacks that swept the globe last year and continue to affect organizations around the world.

（出典）https://www.trendmicro.com/vinfo/us/security/news/security-technology/is-big-data-big-enough-for-machine-learning-in-cybersecurity

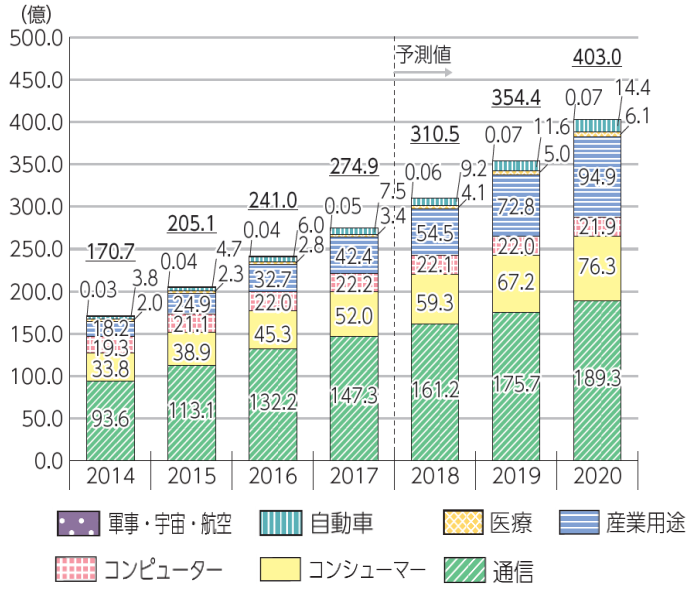
重点分野の課題例③：暗号

現状、暗号分野については、Crypto等のトップカンファレンスにおいて、日本は一定の論文採択数を誇る等、世界的に強みがある。一方、IoT機器の増大や量子計算機の実現見込み等、暗号技術に関する新たな課題が出てきており、これらを見据えた研究開発が必要とされている。

＜課題例＞
- IoT機器の爆発的な増加に備え、リソースの限られた機器でも活用可能な暗号技術の研究開発（軽量暗号等）
- 2030年頃の量子計算機の実現見込みを見据えた暗号技術の研究開発（量子暗号、耐量子計算機暗号等）

爆発的に増加するIoT機器

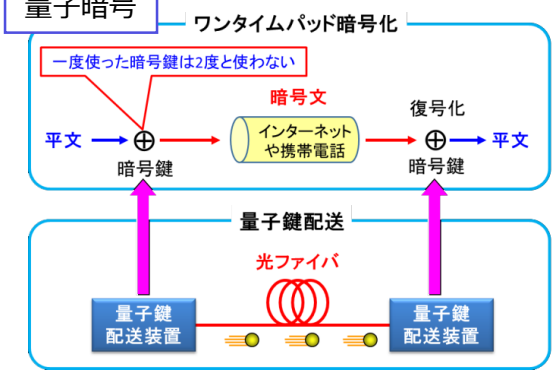
- 2017年時点でインターネットにつながるモノの数は275億個であり、2016年時点の241億個から14.1%の増加と堅調に拡大
- 2020年は約400億と現状の数量の1.5倍に拡大する見通し



(出典)平成30年版情報通信白書（総務省）（データはIHS Technology作成）

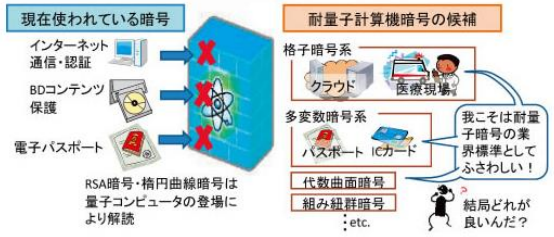
量子暗号、耐量子計算機暗号

量子暗号



(出典)：https://www.nict.go.jp/press/2014/10/24-2.html

耐量子計算機暗号



(出典)：https://www.nict.go.jp/publication/NICT-News/1303/02.html

量子計算機の実現見込み

2030年頃、既存暗号解読可能な量子計算機の実現が見込まれている

- M. Mosca:
  [Oxford] 1996: “20 qubits in 20 years”
  [NIST April 2015, ISACA September 2015]:“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”
  [London, September 2017]:”1/6 chance within 10 years”
- Microsoft Research:
  [October 2015]: Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade.
- Simon Benjamin
  [London, September 2017]:
  Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 years”

今後のスケジュール（案）

時期	2018年	2019年				
	6月	1月	2月	3月	4月	5月
研究開発戦略 専門調査会						

第８回
専門調査会
（6月11日）

○議題
・有識者からの
プレゼンテーション
①戸川委員
(ハードウェアトロイ)
②後藤PD
(SIP第2期)
・意見交換

第９回
専門調査会
（1月30日）

○議題
・我が国のサイバーセキュリティに関する研究・技術開発における課題について
・有識者からのプレゼンテーション
・意見交換

第10回
専門調査会
（2月下旬~3月上旬）

○議題案
・有識者からのプレゼンテーション
・意見交換

第11回
専門調査会
（4月中旬）

○議題案
・「我が国のサイバーセキュリティ研究・技術開発の取組方針（仮称）」案の提示

「我が国のサイバーセキュリティ研究・技術開発の取組方針（仮称）」決定（5月中）