資料３

次期年次報告・計画の策定に向けた進め方等について

資料３－１　次期年次報告・計画の策定に向けた進め方等について

資料３－２　次期年次報告・計画の策定に向けた背景と主な課題

次期年次報告・計画の策定に向けた進め方等について

資料３－１

方向性（案）

○新戦略に掲げた抽象的な概念（「サイバーセキュリティエコシステム」等）について国内外の関係者の理解・浸透を図るために、経済社会の動向を捉えつつ、**適切なトピックを選んだうえで、章を新設**し、記載

○前年度の実績を次年度に反映する等、関連性の明確化のため、年次報告と年次計画の**冊子を一本化**

○記載の根拠となる**データについて**、関係省庁等の協力を得て**充実化**

新設する章でとりあげる内容（案）

サイバー空間に係る動向とリスク

サイバーセキュリティ戦略
[2018年7月27日閣議決定]

国外の動き

■ **先端技術の利用拡大に伴うリスクの高まり**

■ **サイバー空間利用の裾野拡大に伴うリスクの高まり**

■ **国際的なイベントに伴うリスクの高まり**

主な課題（年次報告・計画で詳細に記載）

○サイバーセキュリティ戦略に掲げた概念の具体化
- ・目指す姿
  - -サイバーセキュリティエコシステム
- ・諸施策の実施方針
  - -経営層の意識改革の促進（「費用」から「投資」へ）
  - -脅威に対する事前の防御（積極的サイバー防御）策の構築

等

○サイバー空間と実空間の一体化に伴う脅威への対応
- ・サプライチェーン・リスク対策

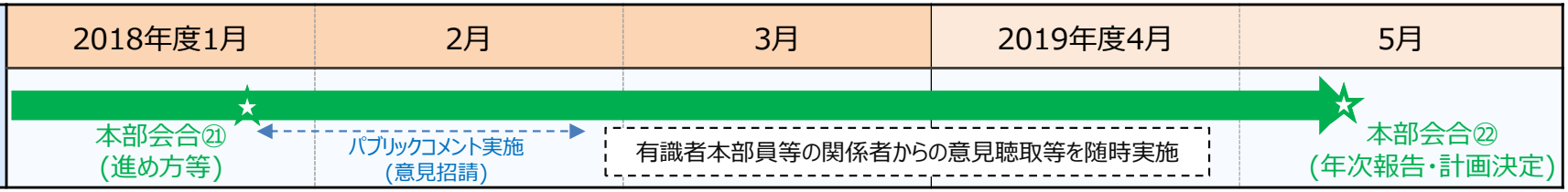
○国際イベントを見据えた取組や情報共有・連携体制
- ・サイバーセキュリティ対処調整センター
- ・サイバーセキュリティ協議会

○全員参加による協働
- ・サイバーセキュリティ意識・行動強化プログラム

等

進め方

次期年次報告・計画策定スケジュール



資料３－２

次期年次報告・計画の策定に向けた背景と主な課題

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。

サイバー空間に係る動向とリスク

サイバーセキュリティ戦略

[2018年7月27日閣議決定]

目指す姿

サイバー空間が持続的に発展し、人々に豊かさをもたらす社会(Society 5.0)の実現

①基本的な立場の堅持

自由、公正かつ安全なサイバー空間

②全ての主体が自律的に取り組む「サイバーセキュリティエコシステム」の推進

(主な観点)

- サービス提供者の任務保障
- リスクマネジメント
- 参加・連携・協働

国外の動き

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

- 新たな国家サイバー戦略（2018/9）
- 連邦政府・重要インフラの保護、安全・信頼のインターネット維持等

EU

- サイバーセキュリティ法成立（2018/12）
- 欧州ネットワーク・情報セキュリティ機関(ENISA)の権限拡大等

英国

- 国家サイバーセキュリティ戦略（2016）
- 「防御」、「抑止」、「開発」を目的

中国

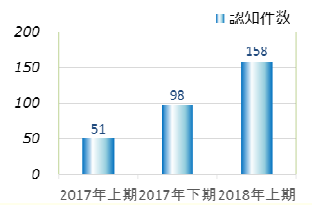
- 国家サイバー空間セキュリティ戦略（2016）
- サイバー空間主権確保

■先端技術・サービスの利用拡大に伴うリスクの高まり

仮想通貨に係る被害が増加。今後、AI、Fintech、自動運転車、ドローン等の先端技術・サービスの利用拡大が予想され、AI等に係るリスクが生じるおそれ

仮想通貨の不正流出被害の増加

【仮想通貨交換業者等への不正アクセス等による不正送信事犯の認知件数】



[直近の事例]

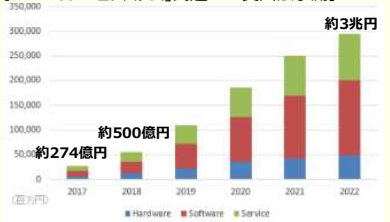
2018/1　コインチェックで約580億円相当の被害

2018/9　テックビューロで約70億円相当の被害

出典：「警察庁 平成30年上半期におけるサイバー空間をめぐる脅威の情勢等について」の数字をグラフ化

AI市場の拡大

【国内「FinTechエコシステム」関連ＩＴ支出額予測】

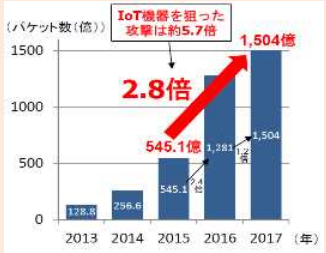


出典：IDC Japan プレスリリース「国内コグニティブ／AIシステム市場予測を発表」（2018年5月14日）

■サイバー空間利用の裾野拡大に伴うリスクの高まり

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(身代金攻撃)の被害が発生。今後も、意識が高くない個人や企業が狙われるおそれ

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 参考資料９

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

■国際的なイベントに伴うリスクの高まり

G20やオリンピック・パラリンピック等の国際イベントは、最高度の注目を集めるため、サイバー攻撃が生じており、今後も、攻撃のターゲットとなるおそれ

2012年ロンドン大会の状況

LONDON 2012

- 大会公式Webに約2億件の悪意ある接続要求
- 開会式前にスタジアム電源系への攻撃情報を入手し、必要な対処を実施

2018年平昌大会の状況

PyeongChang 2018

- 準備期間中に約6億件、大会中に約550万件のサイバー攻撃
- 開会式でサイバー攻撃に起因して一部のサービスが利用不可

記載にあたっての観点･方向性（案）

【サイバー空間に係る動向とリスクについて】

・新戦略で示した状況（サイバー空間と実空間の**一体化に伴う脅威の深刻化）に何か変化はあるか。**米国、英国、EU、中国など**諸外国の動向**をどのように捉えるか。

・一体化に伴う脅威の深刻化に関して次のような具体的な観点が考えられるが、考慮すべきことは何か。

- 先端技術・サービスの利用拡大に伴うリスク
  AI、Fintech、自動運転車、ドローン等の先端技術・サービスの利用の拡大に伴って、**脆弱性が生じるリスク**
- サイバー空間利用の裾野拡大に伴うリスク
  サイバー空間におけるサービスの社会への定着が進み、利用の裾野が拡大するとともに、多様な主体間のつながりが広がり、**人々の生活に様々な恩恵をもたらす一方で**、必ずしも**意識が高くない個人や企業が狙われるリスク**
- 国際的なイベントに伴うリスク
  G20やオリンピック・パラリンピック等、世界の注目を集める**国際的なイベントを狙ったサイバー攻撃**のリスク

【主な課題（年次報告・計画で詳細に記載）】

○サイバーセキュリティ戦略に掲げた概念の具体化

・「サイバーセキュリティエコシステム」「経営層の意識改革」「積極的サイバー防御」等について

○国際イベントを見据えた取組や情報共有・連携体制について

・平成31年４月に創設予定の「**サイバーセキュリティ協議会**」の運用について留意すべき点はあるか。

・G20大阪サミットや2020年東京大会に向けて、平成31年３月末を目途に構築予定の「**サイバーセキュリティ対処調整センター**」の運用について留意すべき点はあるか。

○サプライチェーン・リスク対策について

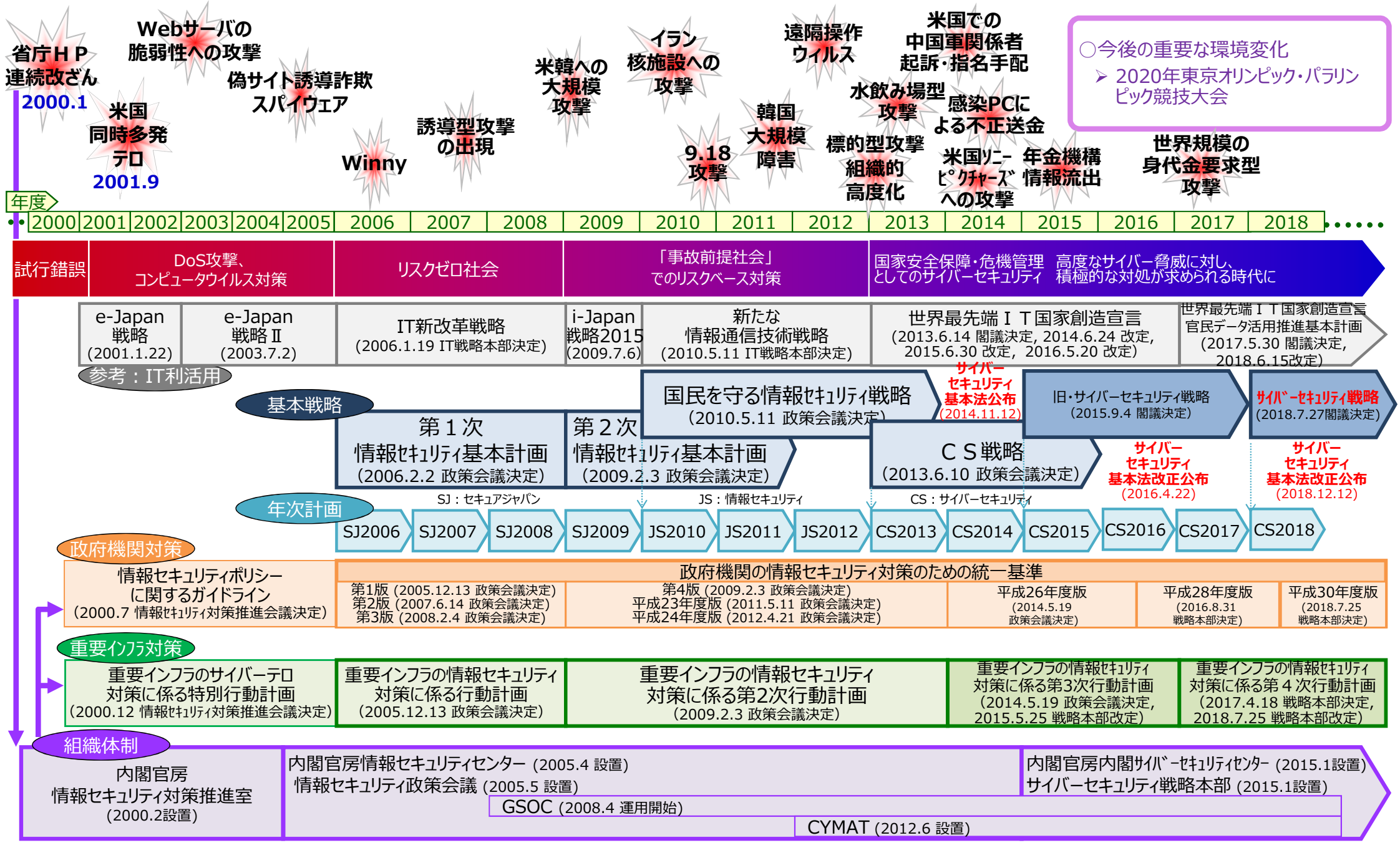
・「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」の運用について

○全員参加による協働について

・**サイバーセキュリティ意識・行動強化プログラム(案)**や今後の進め方について、どのように考えるか。

＜参考資料＞

サイバーセキュリティ政策の経緯



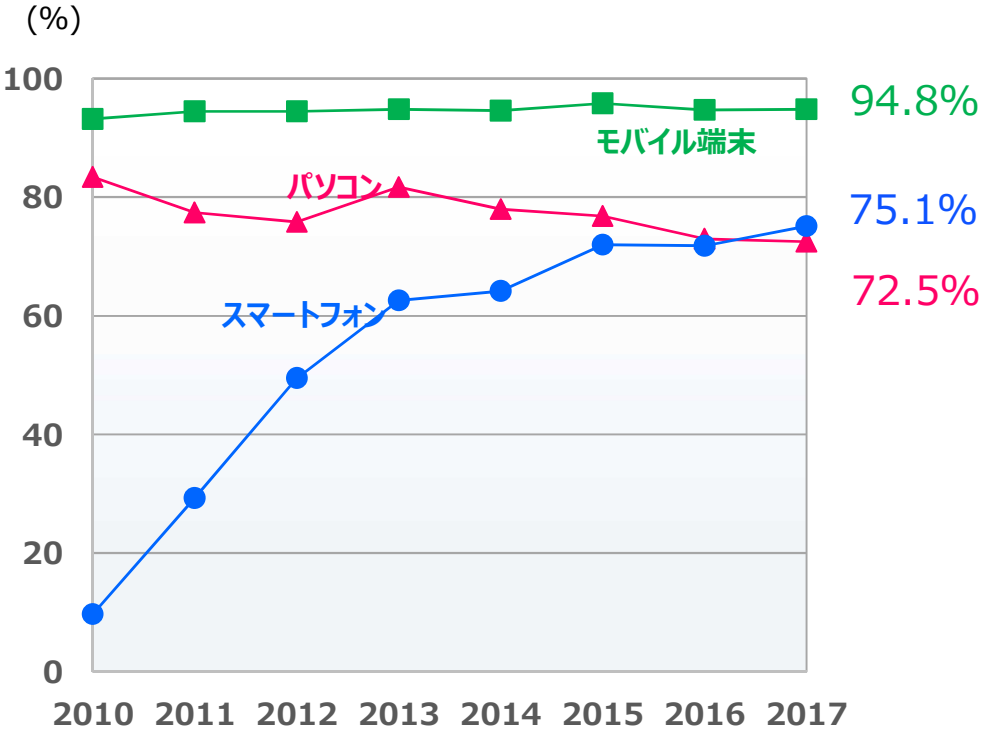
サイバー空間におけるイノベーションの進展

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7.5倍に急増
  (2010年：9.7%→2017年：75.1%)

  ※個人保有率は60.9%（2017年）

国内における情報通信機器の保有状況推移（世帯）



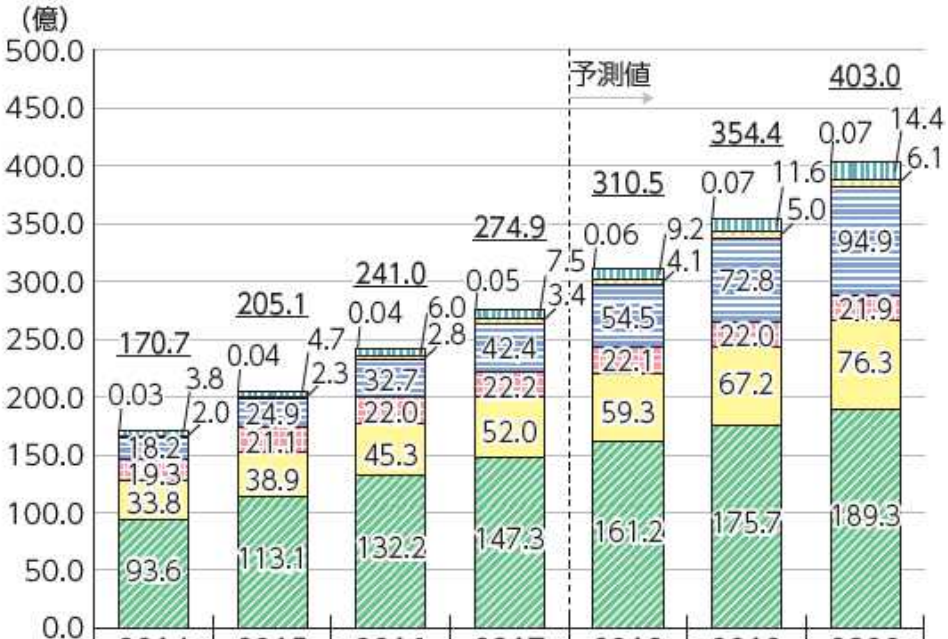
※モバイル端末にはスマートフォンを内数とし含めている

(参考)平成30年版情報通信白書（総務省）

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

世界のIoTデバイス数の推移及び予測



	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

(出典)平成30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

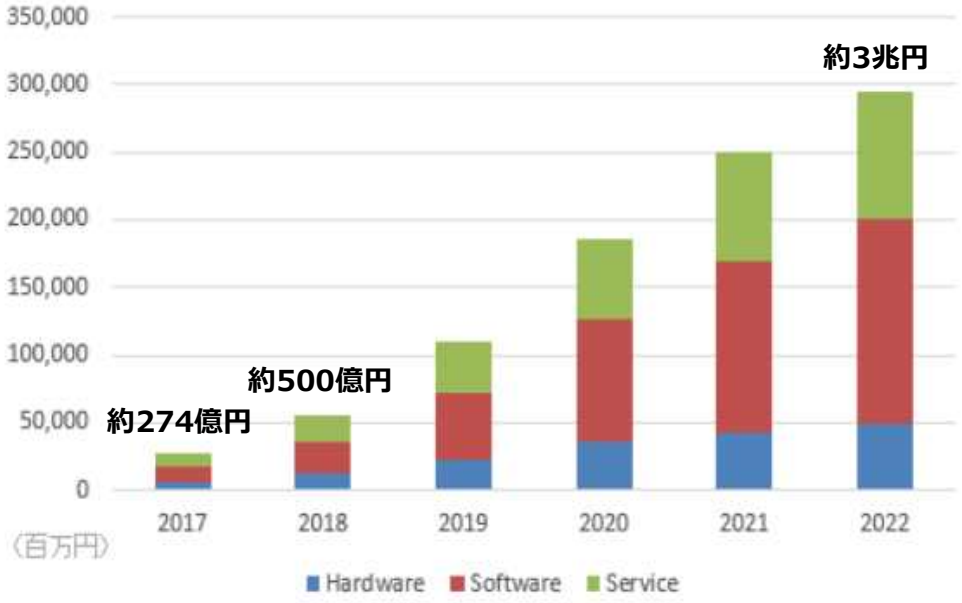
・2012年：ディープラーニングによりAI自らが猫の特徴を識別する機能を飛躍的に向上

・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

・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）※1



※1：(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」（2018年5月14日）

革新的な金融サービスの登場

【代表的なFinTechサービスの例】※2

・預金・資産管理：PFM(Personal Financial Management)、バーチャルバンク

・融資　　：P2P融資、ソーシャルレンディング、クラウドファンディング

・決済　　：モバイル決済、オンライン決済、モバイルPOS、自動支払

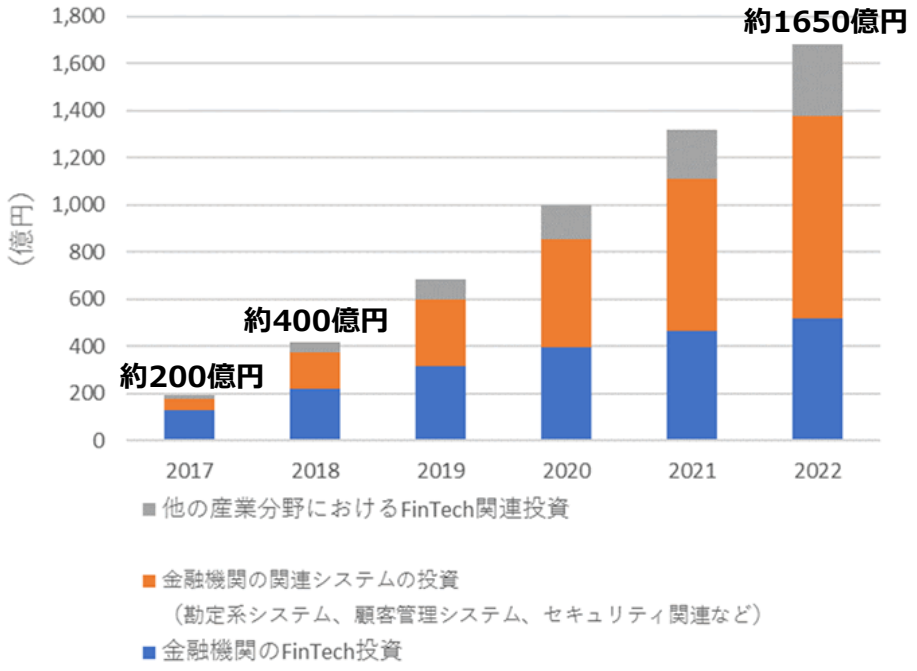
・送金　　：オンライン送金、P2P送金

・投資・資産運用：ロボアドバイザー、オンライン証券・FP(Financial Planner)

・通貨・決済NW　：仮想通貨決済・取引所、非中央集権型取引（ブロックチェーン）

※2：(出典)平成30年版情報通信白書（総務省）より作成

国内「FinTechエコシステム」関連ＩＴ支出額予測 2017年～2022年※3



※3：(出典) IDC Japan プレスリリース「国内における「FinTech」のIT支出への波及効果に関する調査結果を発表」（2018年10月2日）

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。**

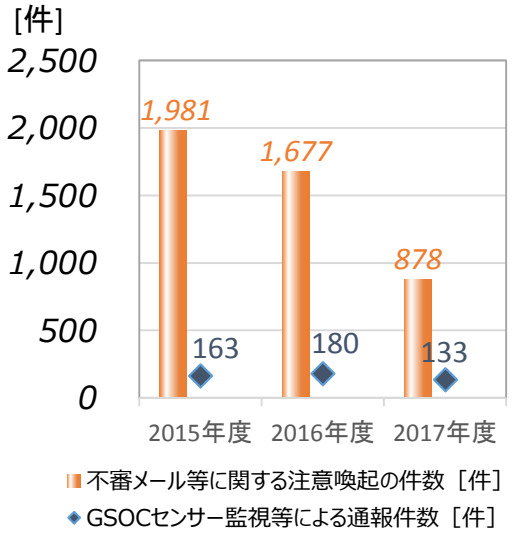
順位	組織における10大脅威	昨年順位
1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺による被害	ランク外
4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービスの停止	4位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

2017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2018」（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/10threats2018.html

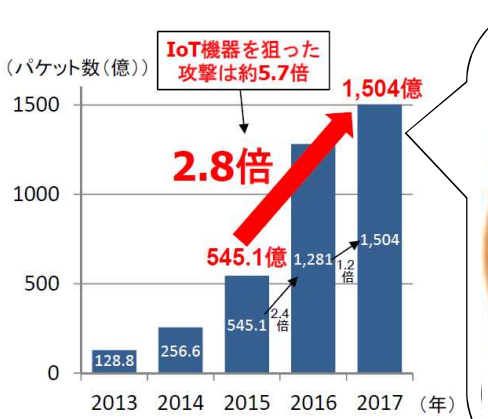
○政府機関等の対策により、サイバー攻撃に係る件数は減少傾向。ただし、標的型等攻撃は巧妙化が図られるなど、予断を許さない状況

【不審メール等の注意喚起件数等】

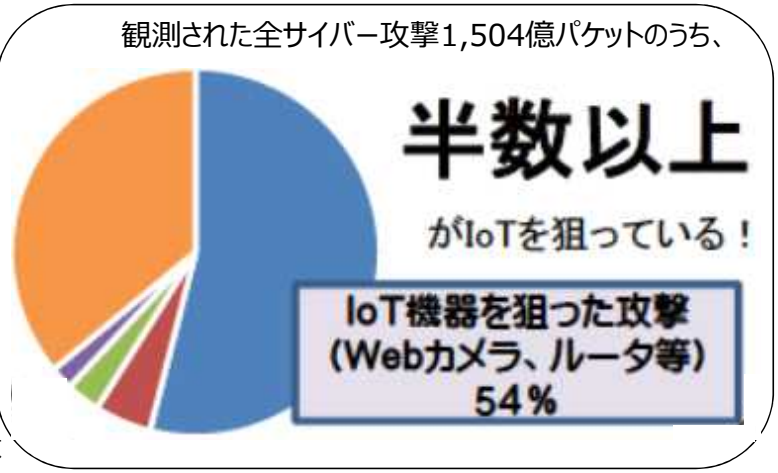


【確認を要するイベント検知件数の推移】

○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

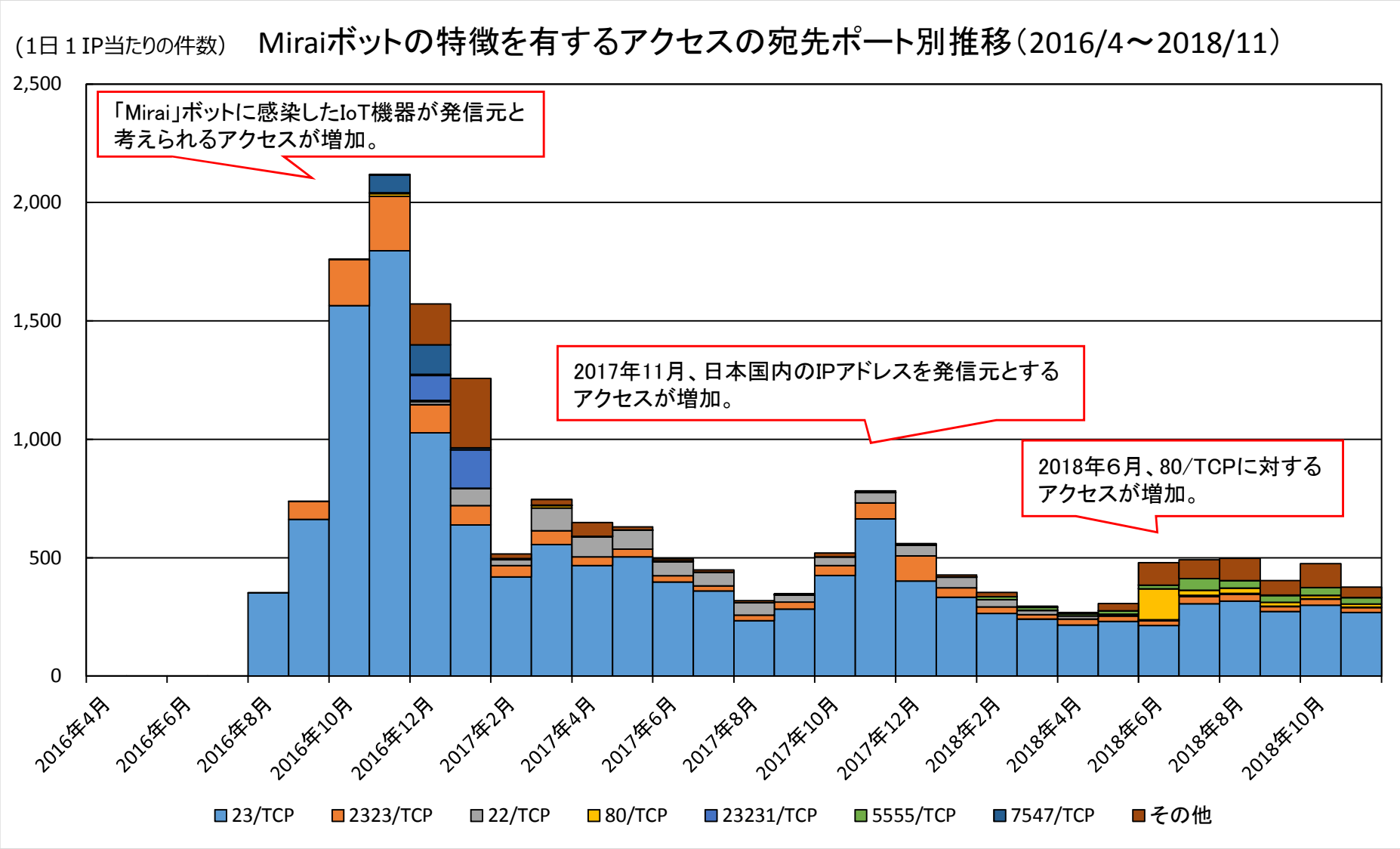


出典：総務省 IoTセキュリティ総合対策プログレスレポート2018 参考資料９

ボットネットに関するアクセス

- **2016年に登場したMiraiボットの特徴を有するアクセスが、引き続き、国内において観測されている。**

○Miraiボットの特徴を有するアクセスの推移



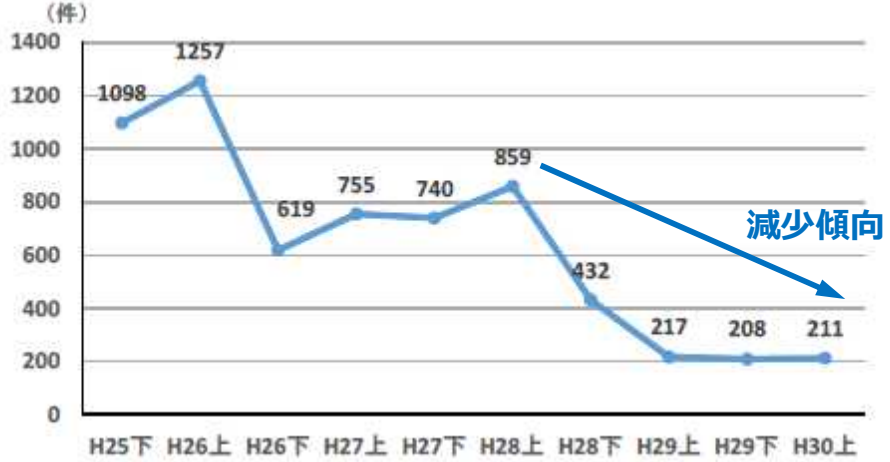
資料提供：警察庁 情報技術解析課　サイバーフォースセンター

インターネットバンキング・仮想通貨をめぐる脅威

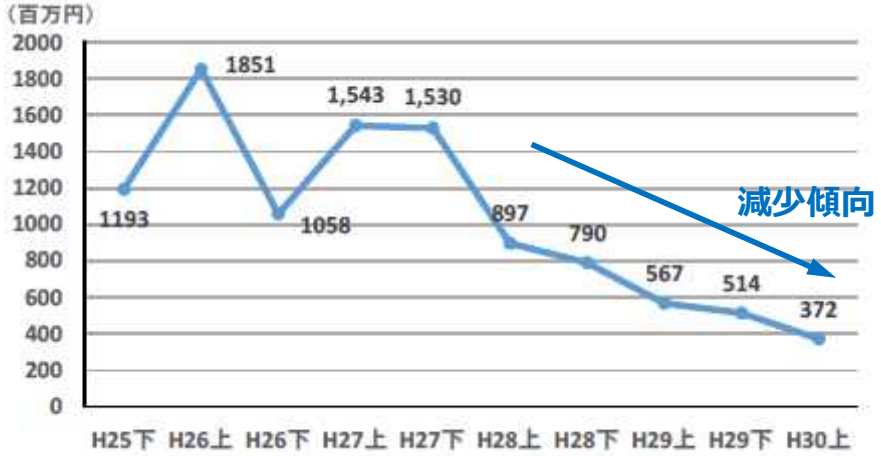
- **インターネットバンキングに係る不正送金事犯による被害は、モニタリングの強化等の対策により減少傾向。**
- **一方、仮想通貨交換業者等への不正アクセス等による不正送信事犯は、認知件数・被害額ともに急増。**

○インターネットバンキングに係る不正送金事犯は減少傾向

【インターネットバンキングに係る不正送金事犯の発生件数】



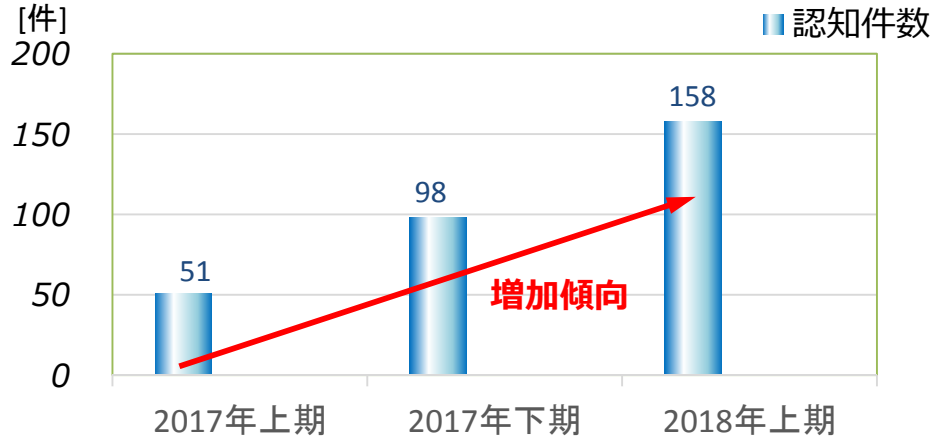
【インターネットバンキングに係る不正送金事犯の被害額



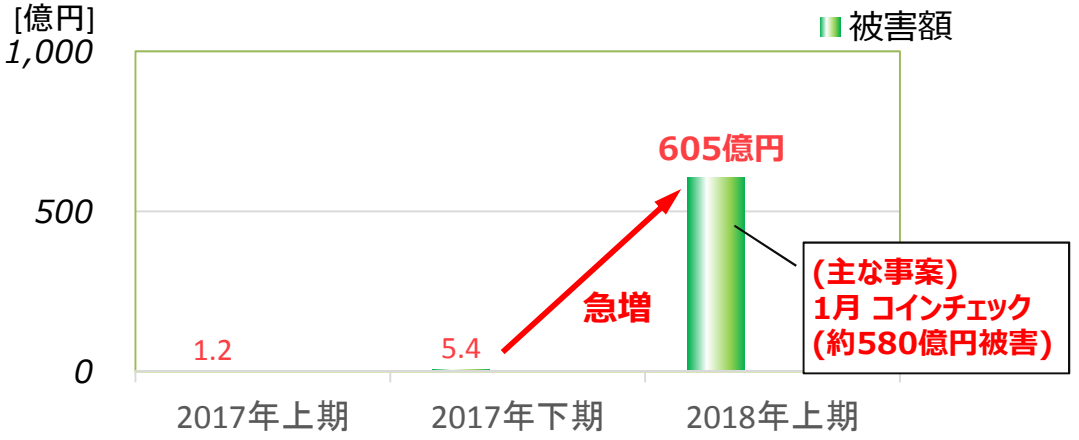
出典：警察庁 平成30年上半期におけるサイバー空間をめぐる脅威の情勢等について

○仮想通貨の不正送信事犯が急増

【仮想通貨交換業者等への不正アクセス等による不正送信事犯の認知件数】



【仮想通貨交換業者等への不正アクセス等による不正送信事犯の被害額】



出典：「警察庁 平成30年上半期におけるサイバー空間をめぐる脅威の情勢等について」の数字をグラフ化

＜その他 直近の事例＞
- 2018年6月　韓国　ビットサムで約35億円相当の被害
- 2018年9月　国内　テックビューロで約70億円相当の被害

ランサムウェアの脅威

- **昨年度に引き続き、ランサムウェアによる被害が発生**。
- WannaCryのような自己伝染機能を持つものの他、SamSamやKeyPassのように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**。

【ランサムウェアによる被害の例】

報道日時(2018年)	感染組織/地域等	ランサムウェアの種類	概要	出典
7月14日	多摩都市モノレール	未公表	7月6日、多摩都市モノレールの**一般業務系で利用するファイルサーバやバックアップサーバがマルウェアに感染**し、サーバ上で保存されているファイルにアクセスできない状態となった。	日本経済新聞
7月17日	LabCorp	SamSam	米国ノースカロライナ州に本社を置く、**診断、医薬品開発、技術的ソリューションを提供する企業LabCorp社**は、ランサムウェアへの感染が判明した後、システムの一部をネットワークから切断したと明らかにした。	LabCorp HP
7月31日	米国、カナダ、英国、中東	SamSam	SamSamランサムウェアの感染による**身代金支払いの総額が、600万ドルを超えている**とセキュリティ会社のSophos社が調査結果を公表した。	Sophos社プレスリリース
8月7日	TSMC	WannaCry	8月3日、Apple社のiPhone等の半導体チップを製造する世界最大の半導体製造ファウンダリであるTSMCが、同社の複数の工場においてランサムウェアの被害にあい、**生産が一時停止**したことを公表した。	日本経済新聞
8月12日	全米プロゴルフ協会	Bitpaymer	8月7日、全米プロゴルフ協会のサーバがランサムウェアの被害にあった。同協会や開催する大会に関連するイベント告知用の素材や大会の**ロゴ等のデジタルデータや関連ファイルが侵害され、身代金の要求がされている**と報道された。	Forbes JAPAN
8月13日	ブラジル、ベトナム等	KeyPass ランサムウェア	Kaspersky Labの研究者が、新種のKeyPassランサムウェアが一部の地域で拡散していると発表した。**KeyPassランサムウェアは攻撃者が手動による高度な攻撃を行う能力がある**としている。	Kaspersky HP
9月27日	サンディエゴ港	不明	9月25日、**サンディエゴ港のITシステムがランサムウェアによるサイバー攻撃を受けた**ことを公表。連邦捜査局(FBI)及び米国国土安全保障省(DHS)が捜査を開始した。犯人はビットコイン(BTC)で身代金を要求したとのことだが、その金額は明らかにされていない。	PORT of SAN DIEGO HP

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・米国等がAPT10に関する声明文を発表。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。