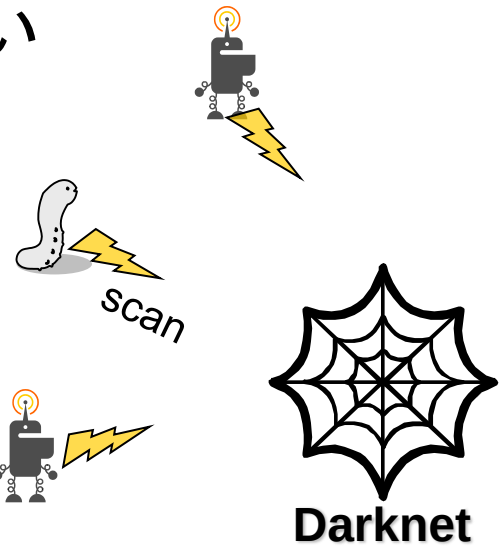
我が国におけるサイバーセキュリティ研究開発戦略、および具体的な関連施策

２０１８年3月7日

横浜国立大学　先端科学高等研究院　IAS客員教授
情報通信研究機構　主管研究員
内閣サイバーセキュリティ補佐官
中尾康二

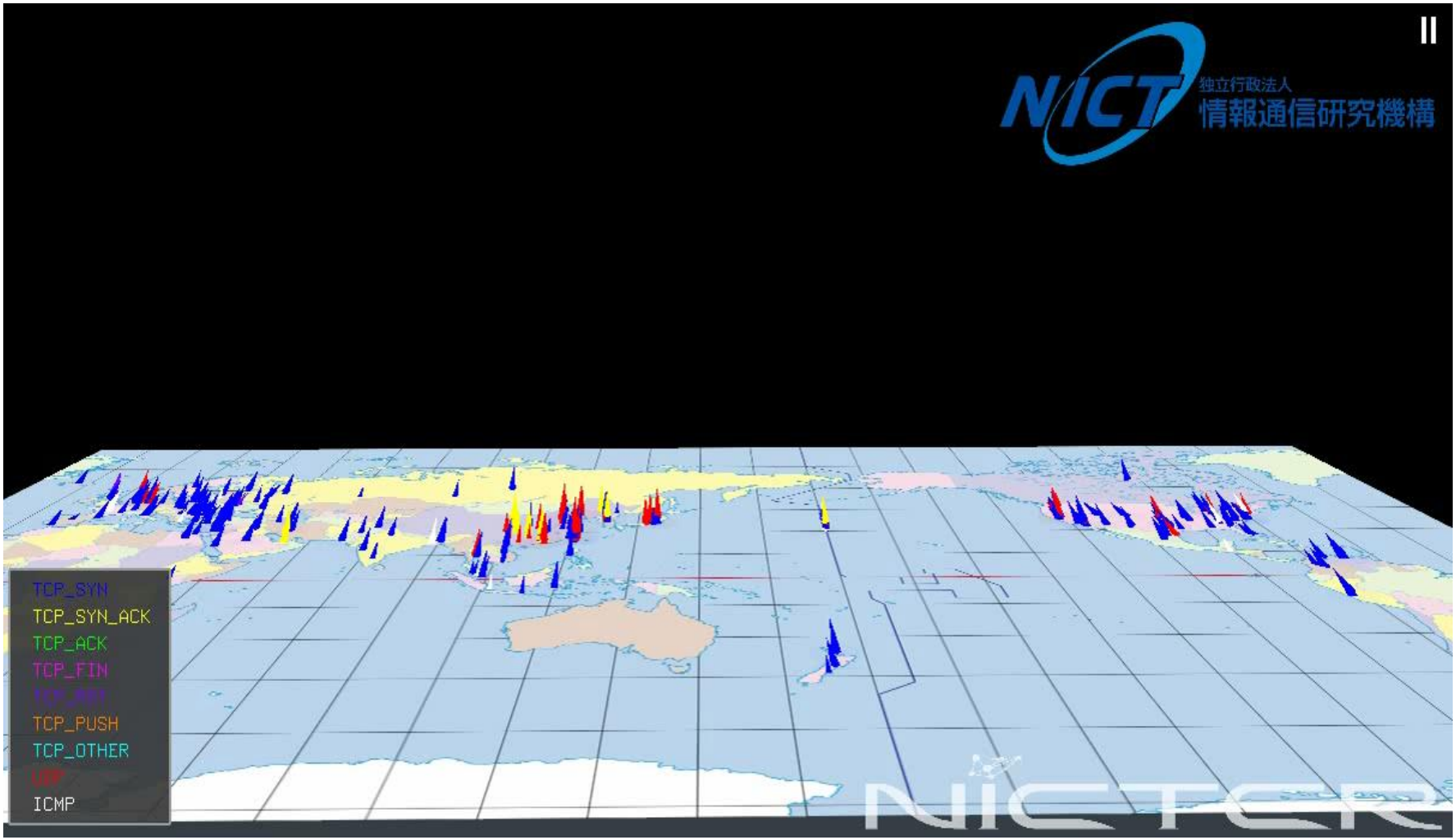
ダークネットを用いて攻撃確認！

- **ダークネット = 未使用IPアドレスブロック**
  - ✓パケットが飛んでくること自体おかしい



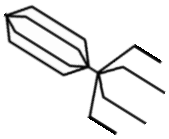
- **ダークネットで見えるもの**
  - ✓**インターネット上で何かを探す行為**
    - ワーム型マルウェアによるスキャン
    - DRDoSのリフレクタ探索（DNS Open Resolver、NTP etc.）
    - セキュリティ関連組織等による調査
  - ✓**DoS攻撃の跳ね返り**
    - DDoSバックスキャッタ
      ※送信元IPアドレス偽装されたSYN Floodへの応答
    - DNS水責め攻撃のバックスキャッタ
      ※送信元IPアドレス偽装されたランダムサブドメイン攻撃
  - ✓設定ミス

ダークネットにおける攻撃状況



マルウェア関連用語
～ マルウェアの感染形態に着目した分類～

- **ウイルス（狭義のウイルス）**
  - ✓ 単体動作せず，自分自身を他のファイルやプログラムに寄生
  - ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
  - ✓ ファイル感染型：実行可能ファイルを主な感染対象

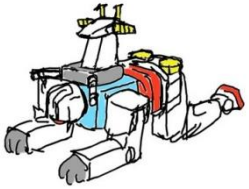


ウイルス

- **ワーム**
  - ✓ 単体で動作し自己増殖を行う
  - ✓ ウイルスに比べ高い感染力を有し，大規模感染を引き起こす
  - ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
  - ✓ Windowsのファイル共有やメッセージング機能を利用するもの
  - ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用いるもの

ワーム

- **トロイの木馬**
  - ✓ 有用なプログラムやファイルに偽装
  - ✓ ユーザ自身によるシステムへのインストールや起動を誘う
  - ✓ 感染機能を持たないものが多い

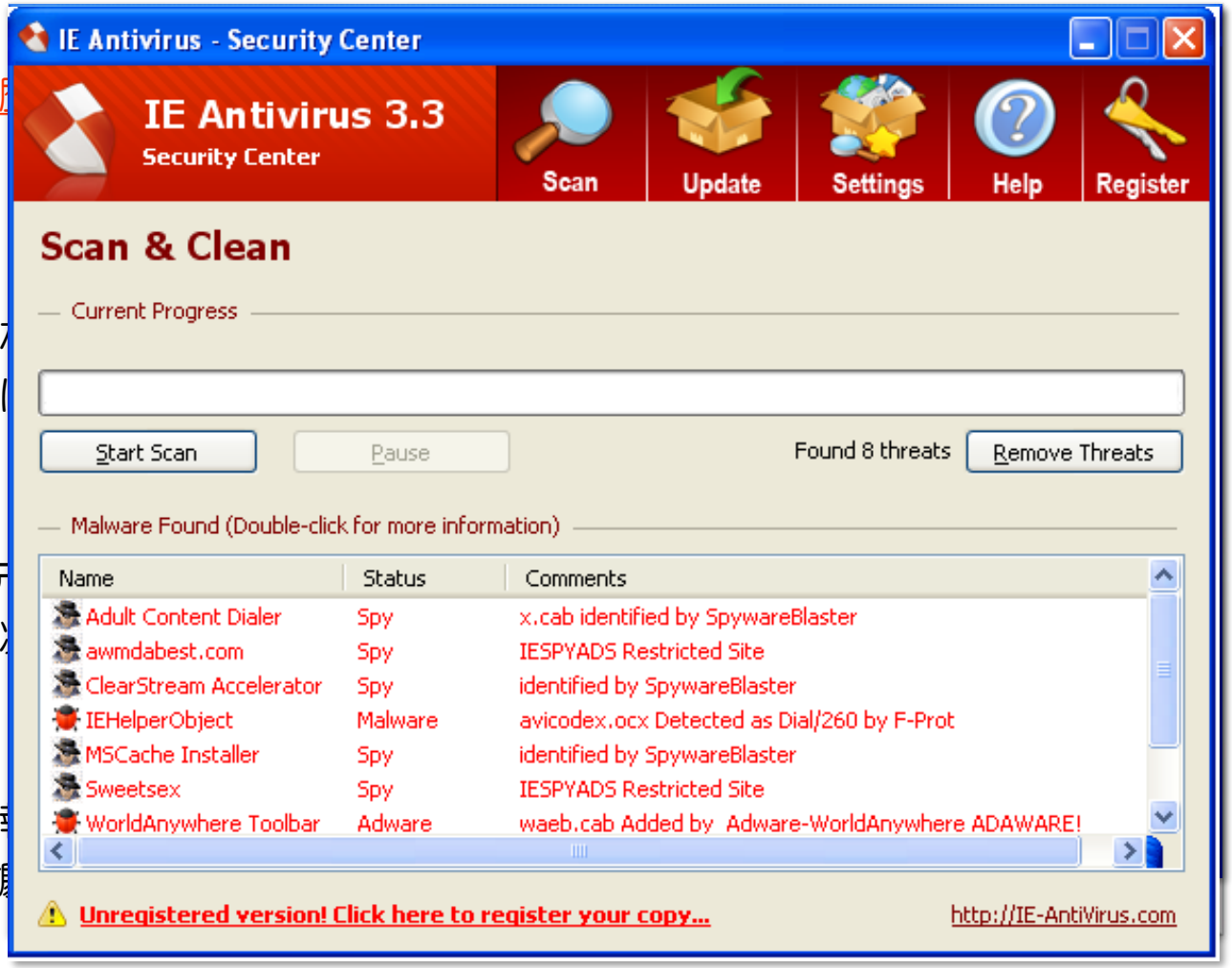


トロイの木馬

出典：GIZMODE Japan

マルウェア関連用語
～ マルウェアの目的に着目した分類～

- スパイウェア
  - ✓ 個人情報や行動履
  - ✓ ユーザのキーボー
- アドウェア
  - ✓ ユーザに企業広告
  - ✓ ユーザの同意なし
- ランサムウェア
  - ✓ ユーザのPC上のテ
  - ✓ データの復号や解
- スケアウェア
  - ✓ ユーザに虚偽の情
  - ✓ 不安（scare）を煽

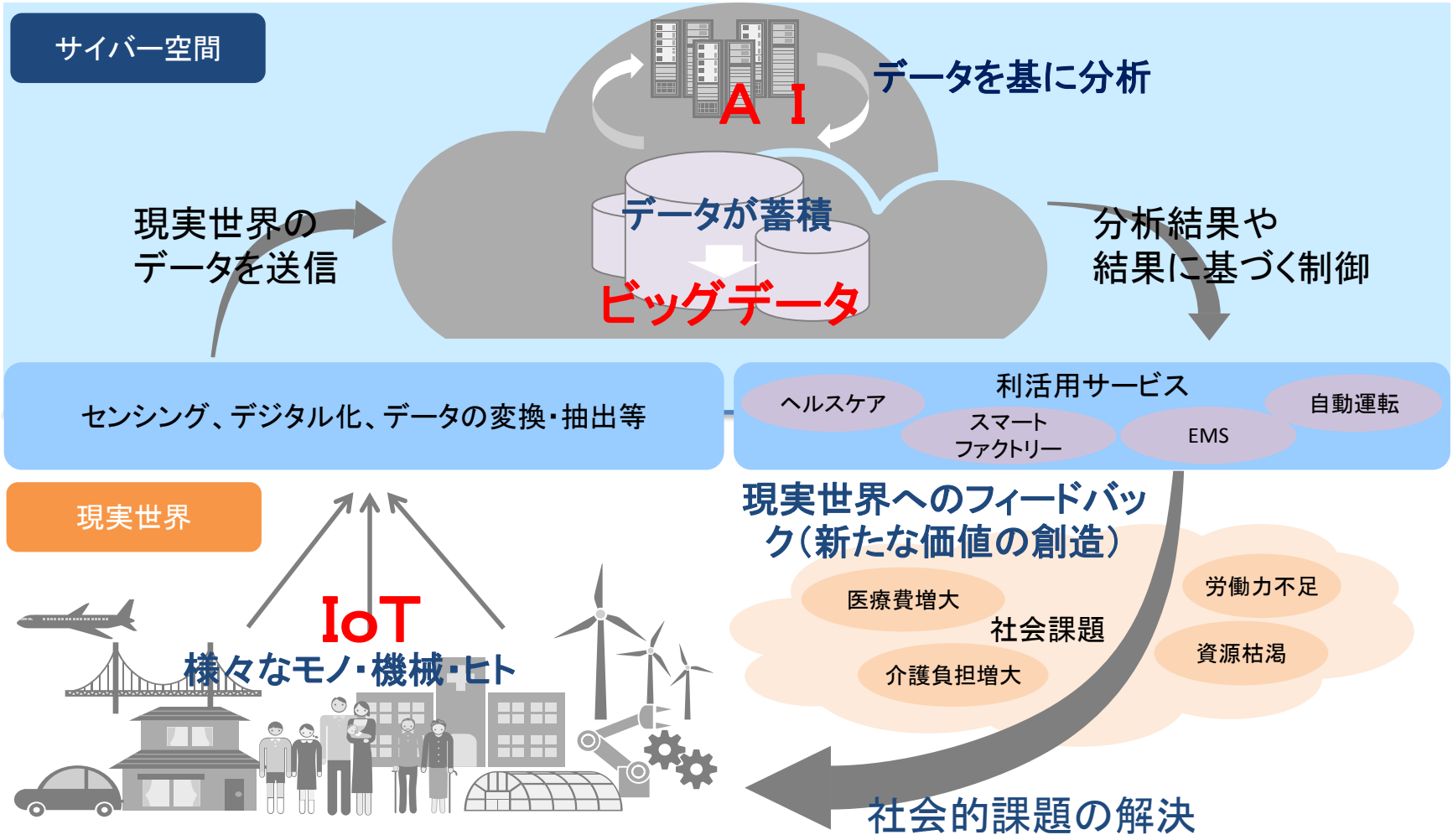


ランサムウェアについて

2014年に流行した「CryptoLocker」、2015年に流行した「TeslaCrypt」、2016年に流行した「Locky」、さらに、2017年に登場した「WannaCry」

WannaCryが感染した時の画面

データ主導社会



総務省　谷脇氏「データ主導社会とサイバーセキュリティ」より抜粋

未来投資戦略2017（17年6月）

Ⅰ. Society 5.0に向けた戦略分野

1. 健康寿命の延伸
- **データ利活用基盤の構築**
- 保険者・経営者による「個人の行動変容の本格化」
- 遠隔診療、AI開発・実用化
- 自立支援に向けた科学的介護の実現
- 革新的な再生医療等製品等の創出促進、医療・介護の国際展開の推進

2. 移動革命の実現
- 世界に先駆けた実証
- データの戦略的収集・活用、協調的領域の拡大
- 国際的な制度間競争を見据えた制度整備

3. サプライチェーンの次世代化
- データ連携の制度整備
- データ連携の先進事例創出・展開

4. 快適なインフラ・まちづくり
- インフラ整備・維持管理の生産性向上

5. FinTech

Ⅱ. Society 5.0に向けた横割課題

価値の源泉の創出

1. データ利活用基盤・制度構築
- 公共データのオープン化
- 社会のデータ流通促進、知財・標準の強化

2. 教育・人材力の抜本強化
- 世界に先駆けた実証
- データの戦略的収集・活用、協調的領域の拡大
- 国際的な制度間競争を見据えた制度整備

3. イノベーション・ベンチャーを生み出す好循環システム

価値の最大化を後押しする仕組み

1. 規制の「サンドボックス」の創設
2. 規制改革・行政手続簡素化・IT化の一体的推進
3. 「稼ぐ力」の強化
4. 公的サービス・資産の民間開放
5. 国家戦略特区の加速的推進
6. サイバーセキュリティ
7. シェアリングエコノミー

Ⅲ. 地域経済好循環システムの構築

Ⅳ. 海外の成長市場の取り組み

総務省　谷脇氏「データ主導社会とサイバーセキュリティ」より抜粋

リスクのグローバル化

（注）海外のサイバー攻撃事案（報道ベース）

○ ソニー・ピクチャーズ・エンターテイメント（2014年11月下旬）

2014年11月、「平和の守護者（Guardians of Peace）」を名乗る組織が、システムに侵入し、同社の数千に及ぶ社内文書や未公開の4作品を含む5作品の同社映画全編の違法コピーがオンライン上に流出。米国政府は、12月19日、当該サイバー攻撃を北朝鮮政府による犯行とし、翌月2日、大統領令を発出し追加的な経済制裁を実施。

○ 保険会社アンセム（2015年2月上旬）

2015年2月、同社に対するサイバー攻撃により、8,000万人分に及ぶ新旧加入者や従業員の個人情報が盗まれた。氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えいしたが、クレジットカードや医療記録などの情報は流出した形跡はないとしている。なお、攻撃者は米国人事管理局（OPM）（後述）へのサイバー攻撃を行った中国人民解放軍ハッカー部隊であるとの可能性も指摘されている。

○ フランスTV5モンド（2015年4月上旬）

2015年4月8～9日、フランス国営テレビTV5モンドは、イスラム国に所属すると主張するグループ「Cybercalophate」によってTVチャンネル、Web、FaceBookが乗っ取られ、イスラム国の犯行を主張するメッセージが表示されていた。4月10日、フランス国防省は、調査の結果、軍の機密情報が漏えいすることはなかったと発表した。

○ ドイツ連邦委議会（2015年5月上旬）

2015年5月15日、ドイツ連邦議会（下院）のサーバにサイバー攻撃を受け、約2万台のパソコンが外部から自由に操作できる状態となった。メルケル首相の下院事務局のパソコンも感染。情報機関のトップは、手法が極めて巧妙であることからロシアの関与を示唆している。少なくとも5人の議員のパソコンからデータ流出が確認されており、それ以外の情報も流出するおそれがあるとしている。

○ 米国人事管理局（2015年6月上旬）

2015年6月4日、米国人事管理局は、システムが侵入され、2，210万件の職員及び元職員の個人情報が流出したと発表 。同局は、情報流出による影響を調べているが、人事管理局や内務省だけでなく、ほぼすべての連邦政府機関に及ぶとされる。さらに数百万人の職員の情報が流出していた可能性もあるとしている。専門家の見解では、中国人民解放軍のハッカー部隊である「ディープ・パンダ」と呼ばれる組織が今回の攻撃及び保険会社アンセムへの攻撃を実施したとされている。

○ オーストラリア気象局（2015年12月上旬）

2015年12月2日、オーストラリア気象局が保有する同国最大のスーパーコンピュータが大規模なサイバー攻撃を受けた。同コンピュータは国防省のネットワークとつながっており、政府のシステムが危険にさらされたとされるが、被害の詳細は不明である。オーストラリア政府関係者は、中国の関与を示唆しているが、中国外務省はサイバー攻撃への関与を否定した。なお、同気象局は、公式発表において、「セキュリティに関する問題にコメントしない」としている。

○ ウクライナ電力供給会社（2015年12月下旬）

2015年12月23日、ウクライナ西部のイヴァーノ＝フランキーウシク地域で、変電所の遮断により、約6時間の停電が発生した。電力供給会社でマルウェアが発見されているが、マルウェアが停電につながったとする因果関係は確認されていない。ウクライナ保安庁は、ロシアの関与を示唆しているが、ロシア政府は反論している。

○ イスラエル電力公社（2016年1月下旬）

2016年1月26日、イスラエル電力公社が過去最大規模のサイバー攻撃を受けた。このサイバー攻撃で電力供給に支障が生じてはいなかったとされている。後日、攻撃は、ランサムウェアを用いた金銭目的であることが濃厚であると報じられた。

総務省　谷脇氏「データ主導社会とサイバーセキュリティ」より抜粋

サイバーセキュリティ戦略（１５年９月閣議決定）

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	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 我が国の安全保障
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	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	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

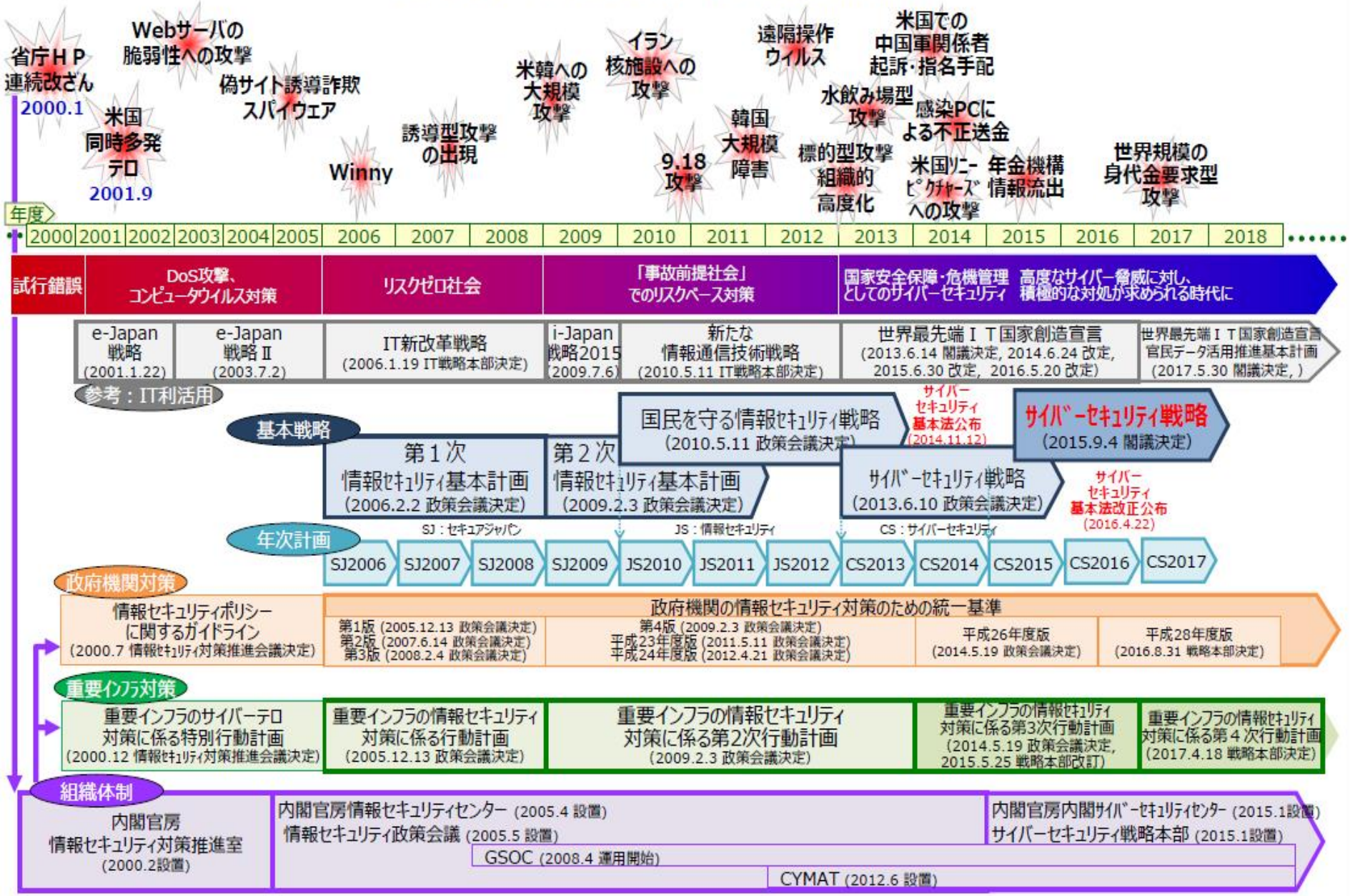
横断的施策

■ 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



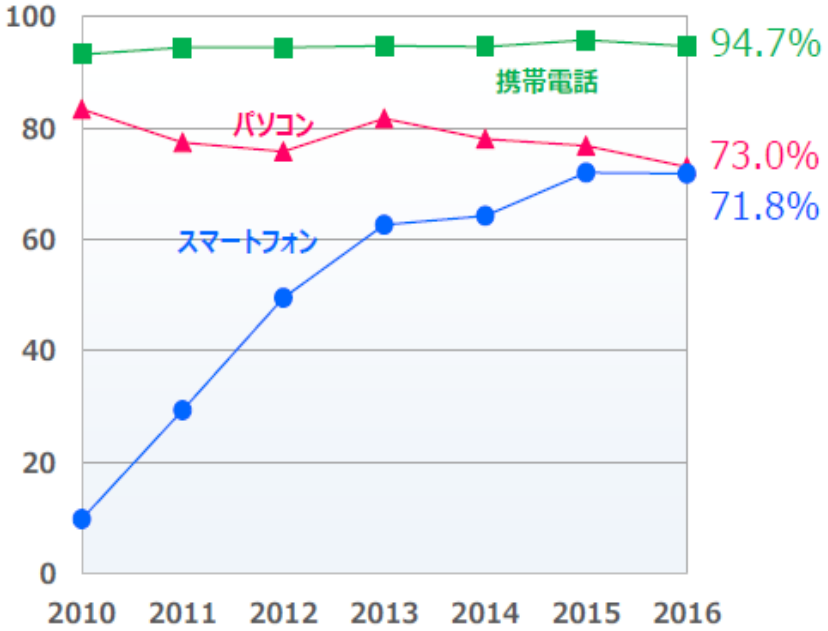
サイバー空間におけるイノベーションの進展

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）

(%)　国内における情報通信機器の保有状況推移（世帯）



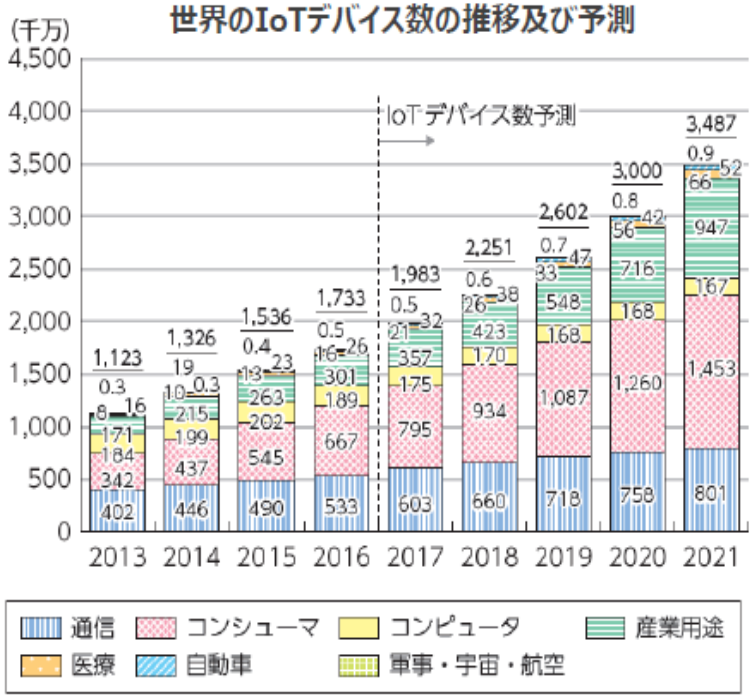
※携帯電話にはスマートフォンを内数とし含めている

(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

世界のIoTデバイス数の推移及び予測



(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

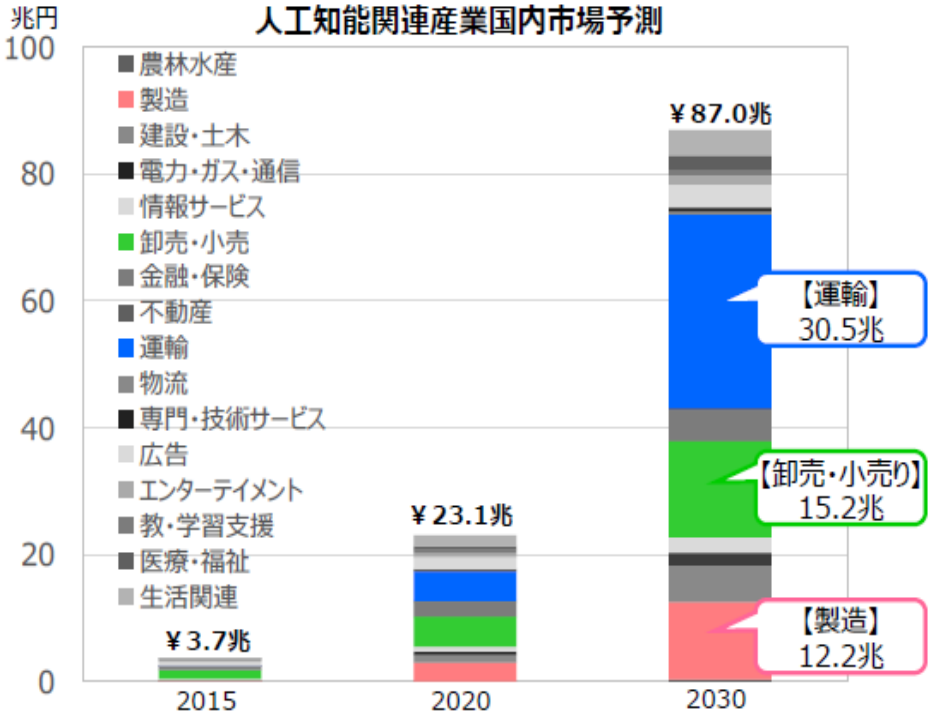
・融資：Web上で貸し手と借り手を募り、Rating等を実施して融資を実現

・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

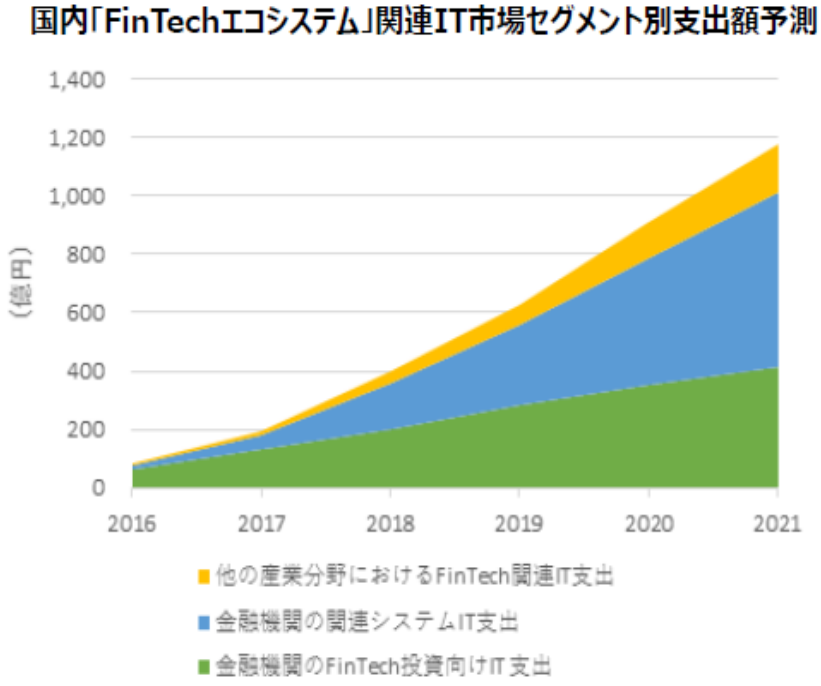
・送金：国際送金やP2P送金等のモバイル送金サービス

・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



（出典）：人口知能関連産業国内市場予測（EY総合研究所2015）



（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）

NISCにおける「研究開発戦略」（2017年）

サイバーセキュリティ研究開発戦略（概要）

【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

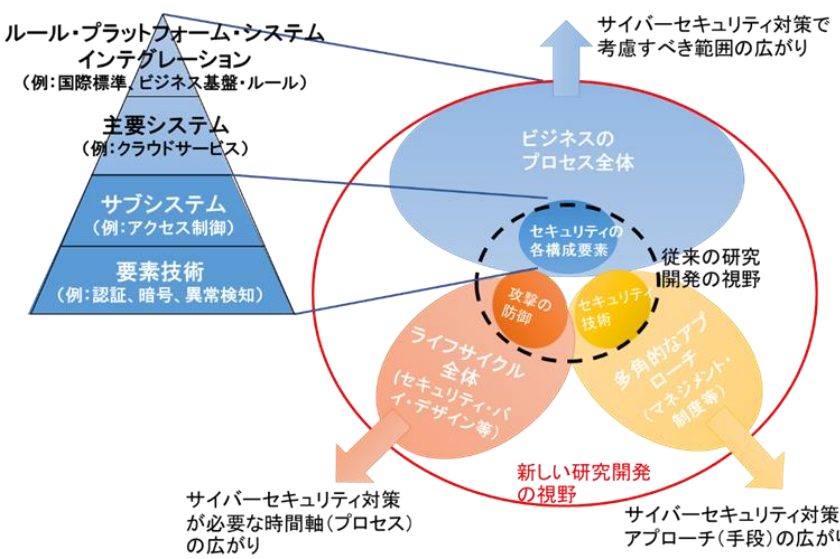
【近い将来】

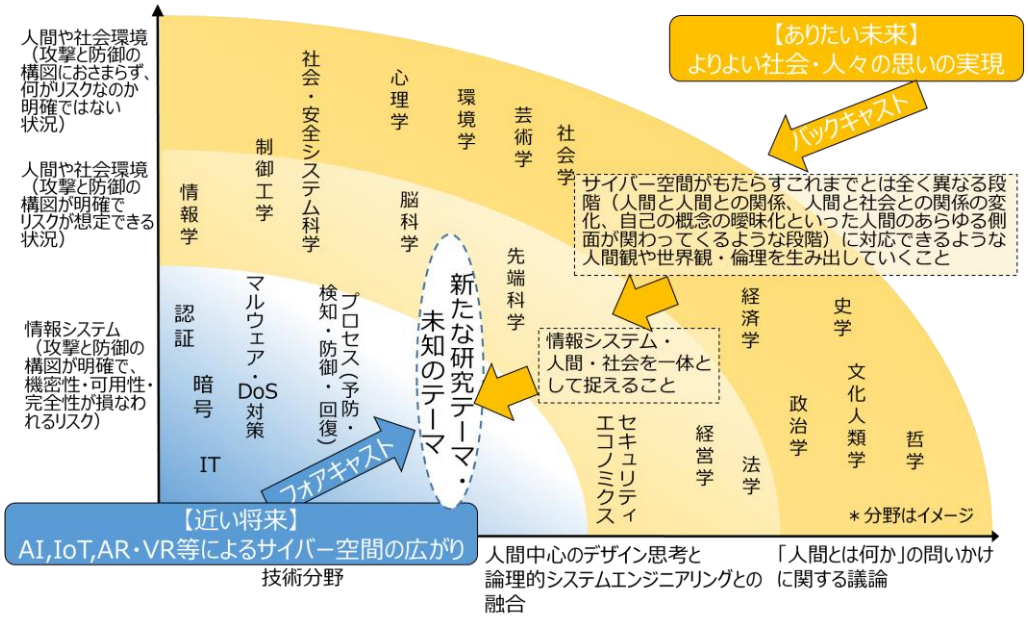
情報システムの進化（つながる（IoT）、知能化する（AI）、広がる(ネットワーク技術)）**を見据え、研究開発の視野を広げることが必要**

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。

(参考)サイバーセキュリティ研究開発戦略

【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

○研究開発の目的として、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、研究開発を通じて国際競争力を強化すること、研究開発で得られた知見により新産業を創出すること、我が国として必要な技術力を獲得・保持すること、を意識。

【近い将来】

○基本的考え方：多層防御のサイバーセキュリティだけでは対処が困難な可能性。視野を広げてサイバーセキュリティ対策を捉え、研究開発に取り組んでいくことが期待される。

・セキュリティの各構成要素だけでなく、ｼｽﾃﾑｲﾝﾃｸﾞﾚｰｼｮﾝなどをビジネスプロセス全体を視野に入れることが重要
・サイバー攻撃の防御技術だけでなく、設計・運用・評価分析・廃棄といったライフサイクルの各段階での技術も重要
・セキュリティ技術だけでなく、マネジメントやリスクコミュニケーションといった多角的なアプローチも重要

○テーマ：近い将来のＩＴの利活用の変化の流れ（つながる（IoT）、知能化する（AI）、広がる（ネットワーク関連技術））を見据えた研究開発が必要。

○方法論：研究開発の課題に対応した方法論（産学連携、ｵｰﾌﾟﾝ・ｸﾛｰｽﾞ戦略等）も、視野に入れることが必要。

【中長期】

○超高齢化社会と人口減少社会といった課題に直面する中、サイバー空間においては、ＩｏＴやＡＩ、ＡＲ・ＶＲ等により、人間の能力は拡張し、実空間とサイバー空間の融合が高度に深化していく。これにより、これまでの労働を代替するにとどまらず、新たな価値を創造し、より良い社会や人々の思いの実現につながっていく可能性がある。

○一方、こうした情報通信技術（IT）は、経済社会の変化をもたらし、現在の経済社会を前提とした将来の技術進歩の外挿（フォアキャスト）によるアプローチのみでは、限界がある可能性。このため、サイバーセキュリティの考え方を再定義（「情報システム」だけでなく、「人間」や「社会」を一体として捉えたセキュリティ）し、ありたい未来から現在すべきことを考えるバックキャストのアプローチも必要。

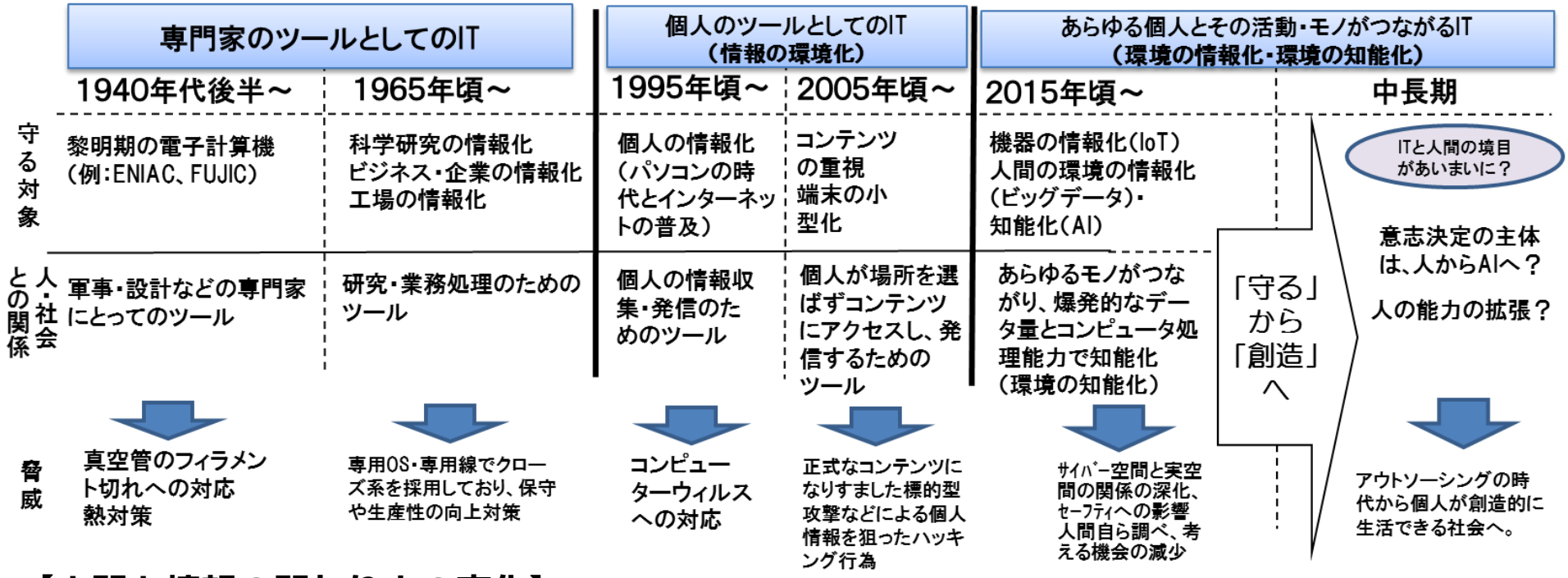
○人文社会科学や情報通信技術（IT）に関連する様々な分野との協業により、「人間」や「社会」を一体で捉えることで、新たなサイバーセキュリティ研究の発見につながる。その際、人間中心のデザイン思考と論理的なシステムエンジニアリングとを融合させるアプローチが有効な可能性。こうしたサイバーセキュリティ研究は、創造的なものであり、人類社会の持続可能性という課題を解決することにつながるもの。

【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。

（参考）情報通信技術（ＩＴ）の進化/人間と情報の関わり方の変化

【情報通信技術（ＩＴ）の進化】



【人間と情報の関わり方の変化】

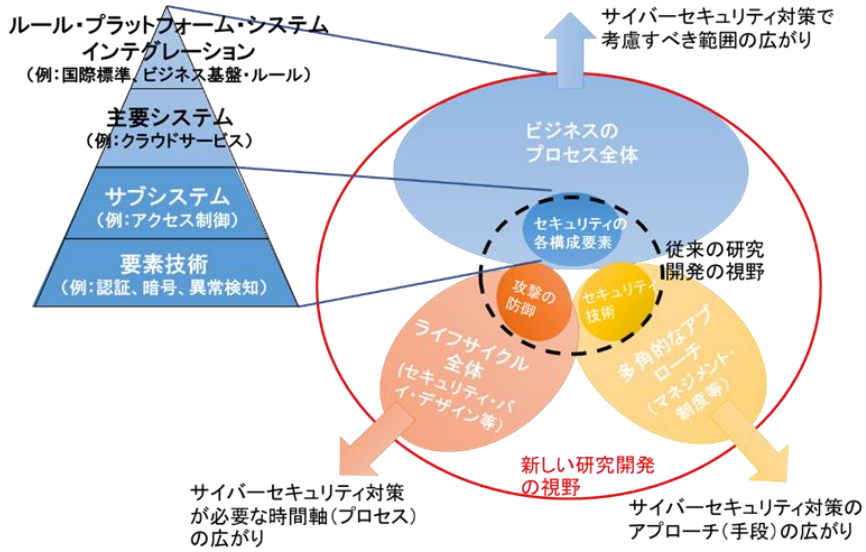
①情報の環境化（インターネットの普及により、多くの情報が身の回りにあふれること）

②環境の情報化（IoTにより、ITが実世界と結びつき、センサーが実世界から収集したデータを基に実世界を変えることができること）

③環境の知能化（実世界から収集したデータがビッグデータとして蓄積され、そこから有用な情報を取り出すために人工知能が活用されること）

（参考）近い将来のＩＴの利活用を想定した研究開発戦略

【研究開発の視野の広がり】



【セキュリティ研究開発における課題に対応した方法論（例）】

- 産学官の連携と企業経営層のリーダーシップによる研究開発
- 脅威に関する情報やユーザー等のニーズを踏まえた実践的な研究開発
- サイバーセキュリティの研究開発に係る制度の検討（海外も視野に入れた対応）
- オープン・クローズ戦略の推進と情報発信
- イノベーションの「シーズ」としての研究開発の推進

【近い将来のITの利活用の進化(例)】

つながる －サイバー空間と物理空間の融合(IoT)－	知能化する －AIの高度化・ビッグデータの活用－	広がる －ネットワーク技術の高度化－
• IoTシステムは、安全性の要求等従来型の情報システムと異なる特性を持つ。 • 我が国の強み・弱みを捉え、想定されるビジネス自体の目的や戦略に照らし、ビジネスの品質を決定する一要素としてIoTシステムのセキュリティの考え方の整理を前提にした、研究開発が必要。	• AIの普及により、その悪用が公共利益の損失につながる可能性があることから、ガイドラインや倫理指針等を踏まえた対応が必要 • サイバーセキュリティ分野におけるAIの活用（攻撃者の持つ技術の高度化への対応）	• 新しいネットワーク関連技術（ＳＤＮ、ブロックチェーン等）の発展を踏まえた対応が必要。 • 既存の仕組を根本的に変えるような技術の発展の影響に関する社会学的研究も必要。

（参考）中長期を見据えた研究開発戦略

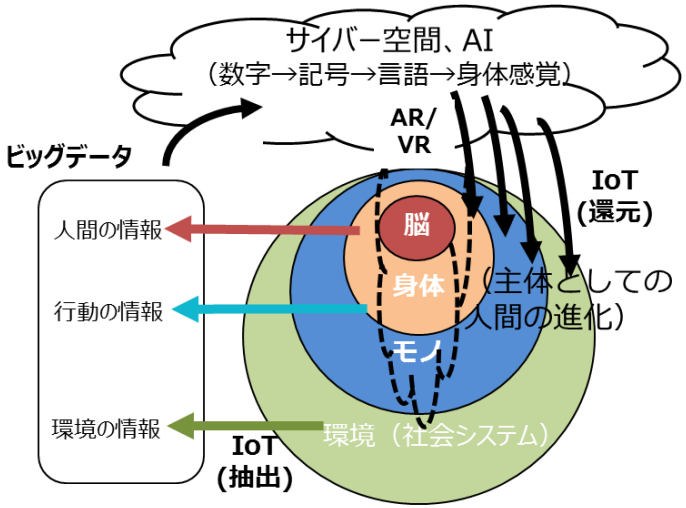
【サイバー空間の広がり】

多様な価値観を承認し、人々の物理的欲求のみならず、精神的な欲求をも満たし、より良い社会を形成する基盤

①ＡＩ（人工知能）
ディープラーニングにより「目を持った機械（認識や運動の上達ができる機械・ロボット）」が誕生

②ＡＲ・ＶＲ（拡張・仮想現実）
VRは、身体を介した一人称の体験をパブリッシュ（本人が知覚可能な体験として、コピー・伝送・再生）することが可能なシステム。

（サイバー空間と人間の関係）



サイバー空間は、書類や画像・音声等を電子化した情報が共有されるだけでなく、脳や身体（人間）、身の回りにあるモノ、さらには環境（社会システム）とつながり、人間の能力が拡張するとともに、モノや環境が知能化するなど、実空間に多大な影響を及ぼしうるのではないか。

出典：株式会社NTTデータ経営研究所 Info-Future No.52のレポートを参考にNISC作成

【サイバーセキュリティの考え方の再定義】

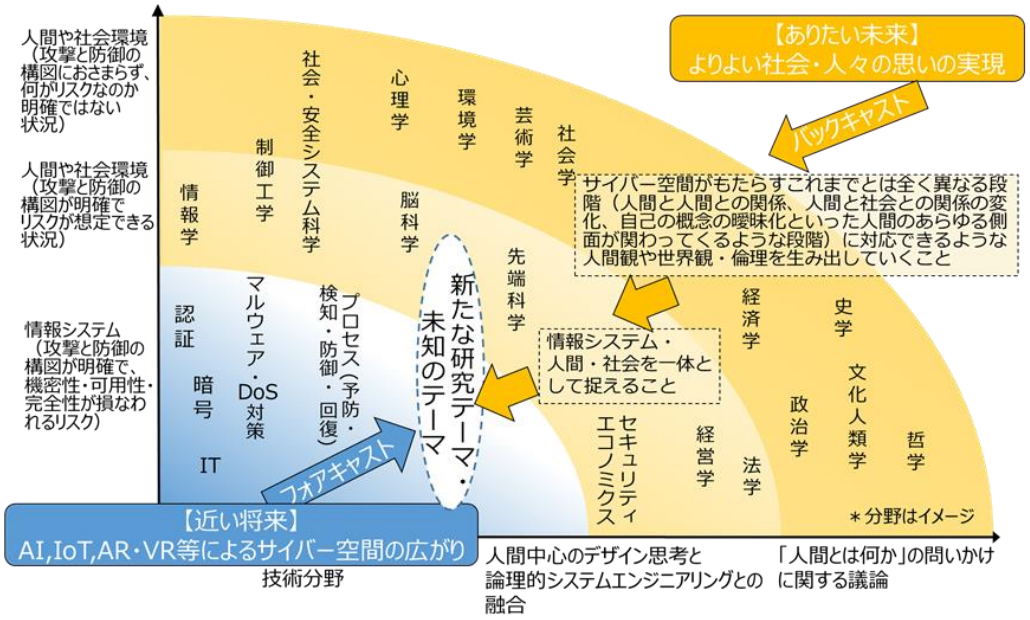
サイバー空間の広がりによって経済社会の前提が変化する中、現在の経済社会を前提とした将来の技術進歩の外挿（フォアキャスト）によるアプローチのみでは、限界がある可能性

↓

「情報システム」だけでなく、「人間」や「社会」を一体として捉えたサイバーセキュリティ（あ［illegible］たい未来からのバックキャスト）

人文社会科学や情報通信技術（ＩＴ）に関連する様々な分野との協業を図りつつ、人間中心のデザイン思考と論理的なシステムエンジニアリングとを融合させるアプローチによって、人類社会の持続可能性という課題を解決できる可能性。

（サイバーセキュリティ研究の広がり）



日本（特に政府）における「具体的な関連施策」の紹介

Society5.0の実現へ向けた社会の変化に伴うサイバー攻撃の脅威

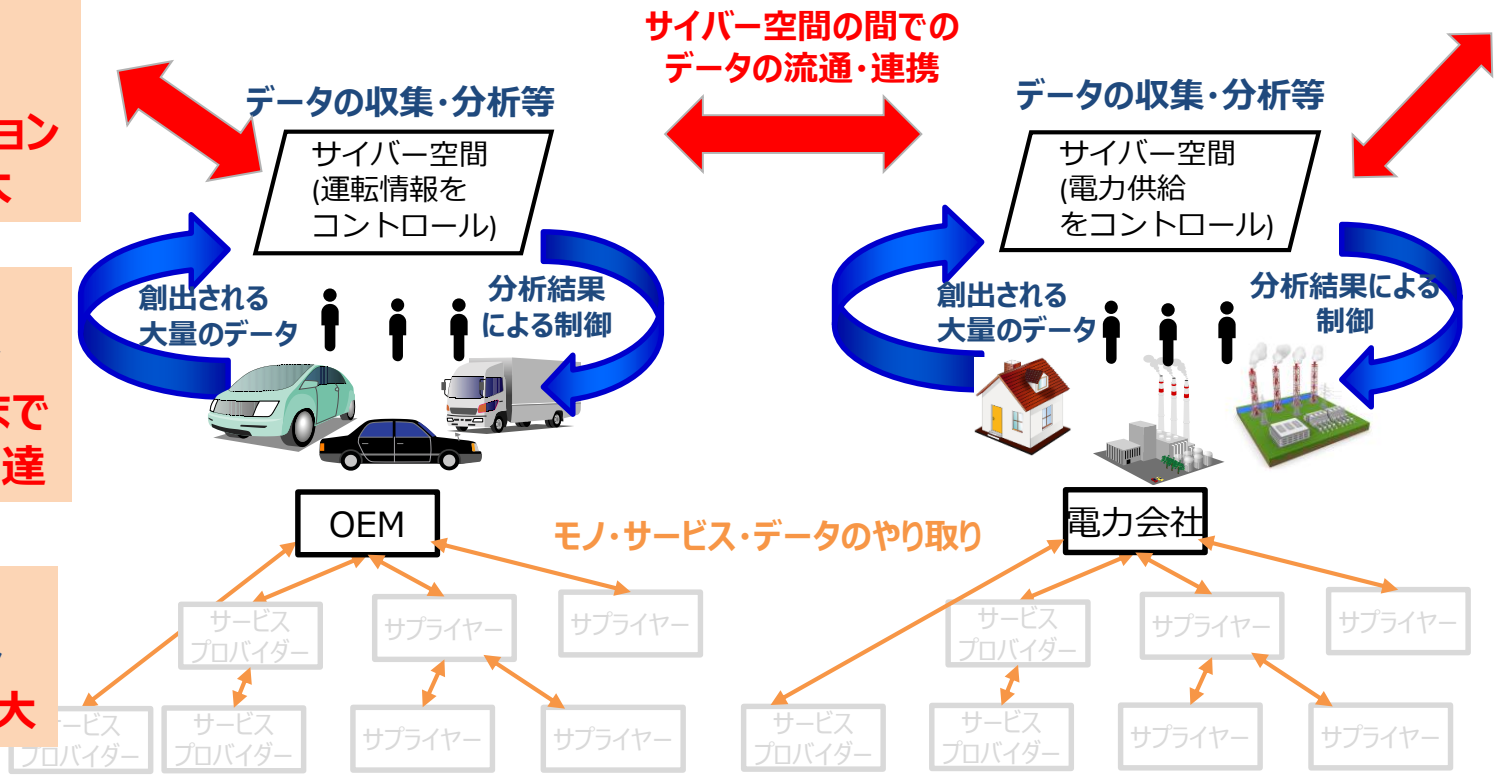
- IoTで全てのヒトとモノがつながるsociety5.0の社会では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

Society5.0の社会におけるモノ・データ等の繋がりのイメージ

大量のデータの流通・連携 ⇒データプロテクションの重要性が増大

フィジカルとサイバーの融合 ⇒フィジカル空間までサイバー攻撃が到達

複雑につながるサプライチェーン ⇒影響範囲が拡大



『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定へ向けて

- Society5.0、Connected Industries の実現へ向けて、**産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応することが必要**。
- **このため、産業に求められるセキュリティ対策の全体像を整理**し、**産業界が活用できる『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**することを目指す。

１．各事業者が本フレームワークを活用することで期待される効果

- **Society5.0、Connected Industries の実現に求められるセキュリティの確保**
- **製品・サービスのセキュリティ品質を差別化要因(価値)にまで高めることで競争力を強化**

２．サイバー・フィジカル・セキュリティ対策フレームワークに必要な要件

① 各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる。
- 社会として目指すべき概念だけではなく、各事業者が実際にセキュリティ対策を実施するうえで活用できる内容にする。

② セキュリティ対策の必要性とコストの関係を把握できる。
- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるようなものにする。
- リスク・シナリオ・ベースの考え方も考慮する。

③ グローバルハーモナイゼーションを実現する。
- グローバルサプライチェーンの中で、日本における製品・サービスのセキュリティ対策が海外からも認められるよう、グローバルの動きをよく取り入れ、米欧などの主要な認証制度との相互承認を確保する。

『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ①

WG1において検討を進め、年度内に大枠を整理することを目指す

来年度以降SWGにおいて具体を検討

3つの切り口	脅威が守るべきものへ与える影響(リスク分析) **守るべきもの**	**脅威**	**具体的な対応策(構成要素ごとに整理)**
企業と企業の繋がり	・仕様通りの製品、サービス ・情報の秘密保持 ・安全な取引	■マルウェアの混入 ■不正な機器の混入(調達段階)	**セキュアなサプライチェーン構築のために取引先に確認すべき項目** ■納入されるモノのセキュリティ確保 ■取引先のセキュリティ状況の確認 ■取引先とのやり取りのセキュリティ確保
フィジカル空間とサイバー空間の繋がり	・実現したい機能 ・レジリエンス ・セキュリティ ・セーフティー　等	■不正な機器の混入(設置段階) ■計測データの改ざん ■制御機能への攻撃	**セキュアなCPS構築に向けて必要な対策の項目** ■安全なIoTシステムの導入 ■CPS/IoTの構築と運用 ■組織文化の醸成　等
サイバー空間とサイバー空間の繋がり	・セキュアなデータ流通 ・サイバー上でのサービス利用	■データベースに格納されるデータの信ぴょう性 ■データプラットフォームへの攻撃 ■ネットワーク上での攻撃	**セキュアなデータ連携・活用に必要な対策の項目** ■データプラットフォームのセキュリティ ■データ品質の確認 ■データプラットフォームに参加する企業のセキュリティの確認　等

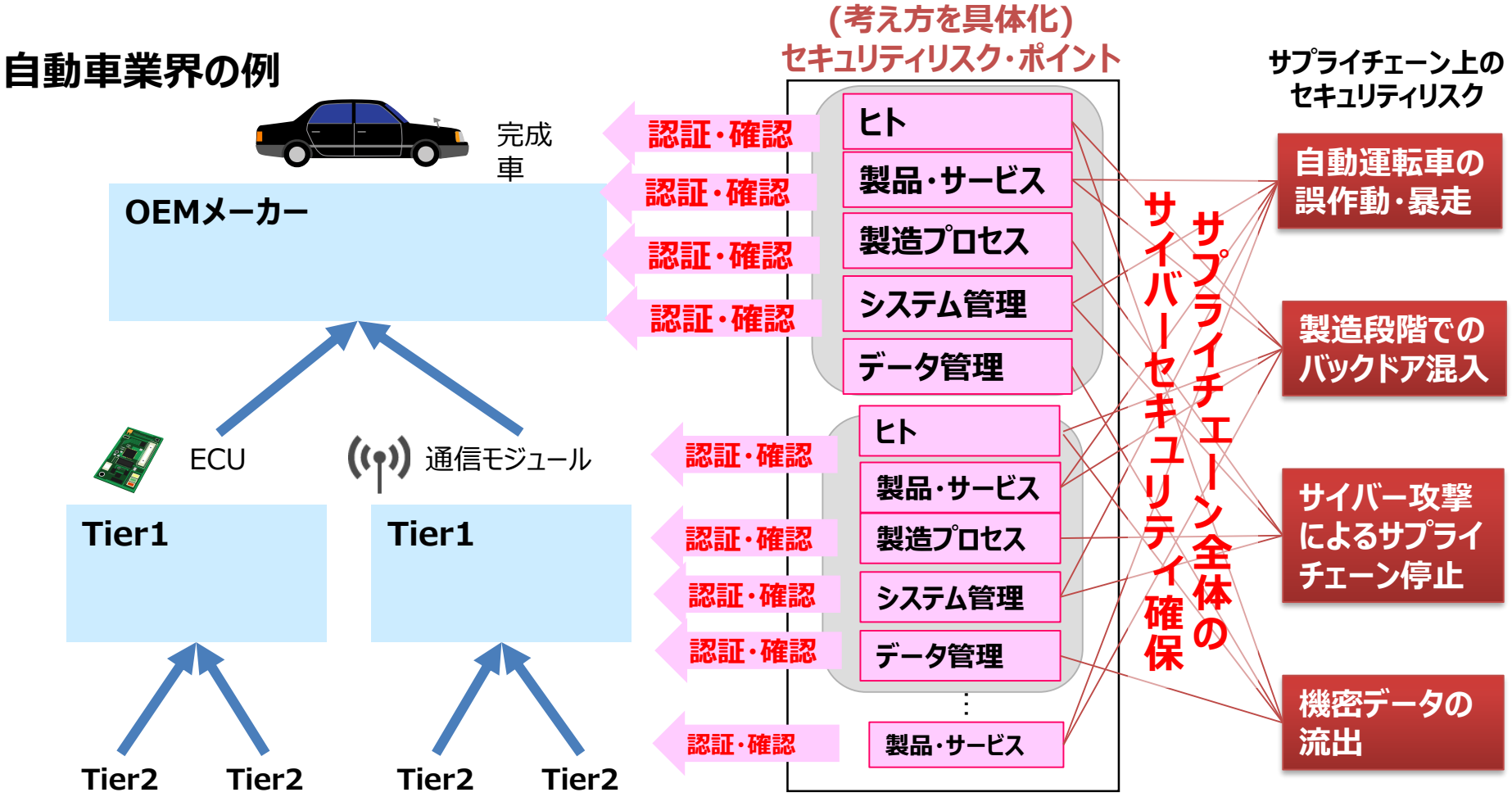
互いに関係

互いに関係

各分野のライフサイクルや求められる機能を踏まえたセキュリティ対策ガイドライン

『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ②

- サプライチェーン全体のサイバーセキュリティを担保するには、**取引先やモノが信頼できることを各リスクポイントにおいて確認することが必要**。



リスク評価及び制御システムのセキュリティリスク分析ガイドについて

- 東京オリンピック・パラリンピックの開催に影響を与える重要なインフラ事業者については、侵入テストを含む徹底的なリスク評価と対策立案を実施
- 評価結果等をもとに、ＩＰＡが制御システムのセキュリティリスク分析のガイドを策定・公表

リスク評価・対策立案

- 重要インフラ事業者によるサイバーセキュリティ対策を確認し、防御力の確認や改善計画策定等を行う事業を平成28年度から実施（４分野）
- 今年度、当省所管の重要インフラの2分野について実施

リスク評価結果等をもとに作成

制御システムのセキュリティリスク分析ガイド

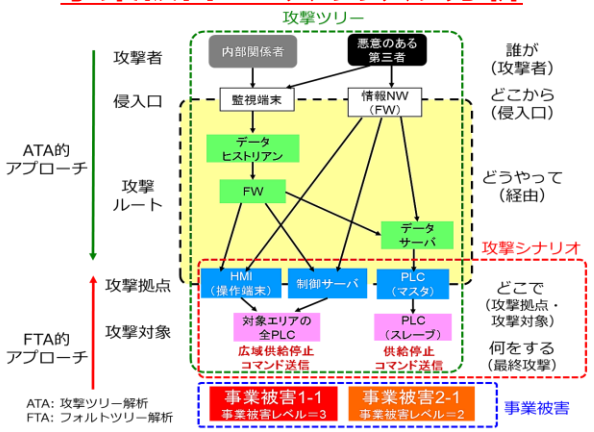
【ガイド本編】

【別冊】

- リスク分析の全体像の理解向上と取組促進

リスク評価の手順や手引きの提示

- 資産ベースのリスク分析
- **事業被害ベースのリスク分析**



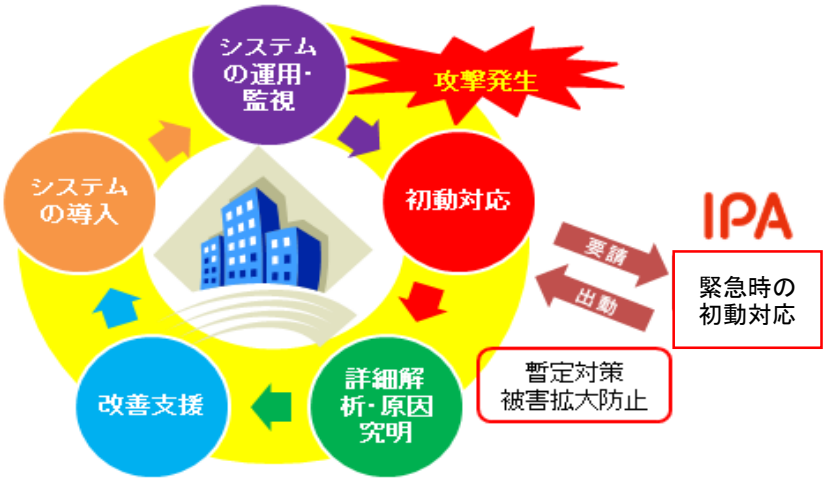
【事業被害、攻撃シナリオ、攻撃ツリーの関係】

高度標的型サイバー攻撃を受けた組織への初動対応支援

●平成26年7月、IPAに、個々の組織の能力では対処困難な、高度標的型サイバー攻撃を受けた組織に対する初動対応を行う「サイバーレスキュー隊（J-CRAT）」を立ち上げ。

●最初の標的となり、対応遅延が社会や産業に重大な影響を及ぼすと判断される組織（主として、重要インフラ事業者、業界団体・独法等）に対して、初動対応支援を実施。

【サイバーレスキュー隊の活動】



重要インフラ、業界団体等

経済社会に被害が拡大するおそれが強く、一組織で対処が困難な深刻なサイバー攻撃の発生

・初動時の緊急処置の助言
・被害状況の理解促進
・対応体制の早急な立ち上げの支援

IPA 独立行政法人 情報処理推進機構 Information-technology Promotion Agency, Japan

サイバーレスキュー隊

インシデント情報の収集・共有によるサイバーセキュリティ対策の強化

- IPAは、重要インフラ事業者に対するサイバー攻撃情報共有体制　（J-CSIP（ジェイシップ）：Initiative for Cyber Security Information sharing Partnership of Japan、11業種、227組織が参加）を構築
- 公的機関としての信頼性を基に、秘密保持等契約を結び、企業から情報を収集、解析、秘匿化し、迅速に共有することにより被害拡大を防止
- さらに、分野ごとの情報共有体制を強化（J-CSIPの対象拡大）していく方針

【J-CSIPの仕組み】

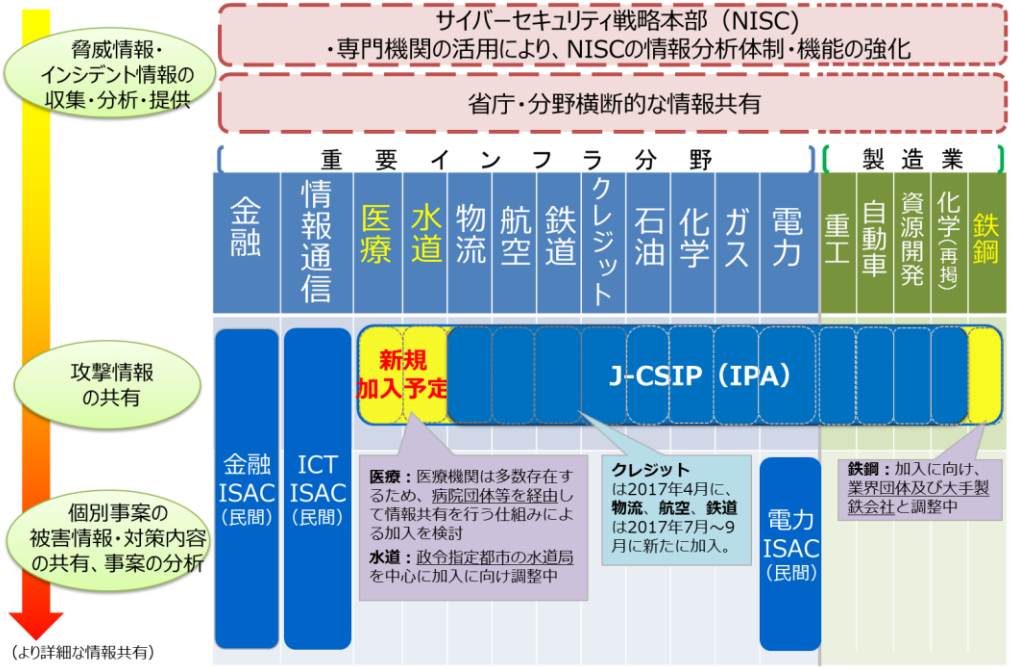
IPA

サイバー攻撃情報の収集

攻撃手法を解析し、情報提供者の営業秘密等保護のための匿名化を行った上で共有。

共有件数
（800件以上）
（2012年5月からの累計）

重要インフラ等企業
（重工、電気、ガス、化学、石油、資源開発、自動車、クレジット、物流、航空、鉄道：11業種227組織）



IoTセキュリティ総合対策（2017年10月）

脆弱性対策に係る体制の整備

- IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。
- 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等における セキュリティ対策の促進

- 民間企業等のサイバーセキュリティに係る投資を促進。
- サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

- 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

- 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証（関係府省と連携）

IoTセキュリティ総合対策の推進

○ IoTサービスの普及に伴い、インターネットに接続されているIoT機器の種類・台数は年々増加している。昨年10月には、IoT機器を踏み台にした世界規模のサイバー攻撃が発生するなど、サイバー攻撃の脅威は今後も増大すると予測されており、セキュリティ対策の強化が急務。

○ 関係省庁、研究機関、業界団体等と連携しつつ下記の取組を実施し、IoT機器に関する脆弱性対策を推進。

ＩｏＴ機器に関する脆弱性対策の概要

① 脆弱なIoT機器の実態調査、所有者等への注意喚起

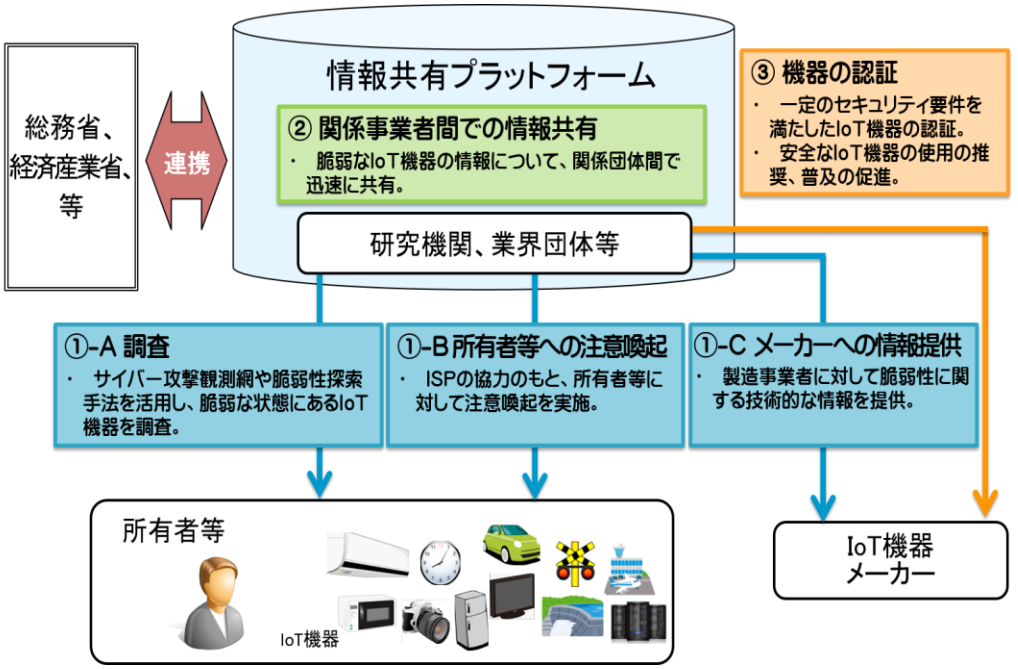
広域ネットワーク探索手法、サイバー攻撃観測網等を活用し、インターネットに接続されているIoT機器の調査を実施。脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を行う。

② IoT機器の脆弱性情報の関係事業者間での共有

①の取組等により収集した脆弱なIoT機器の情報について、関係事業者間で共有する仕組みを構築し、IoT機器の製造事業者等が脆弱性に迅速に対応することを可能とする。

③ 一定のセキュリティを確保したIoT機器の認証

一定のセキュリティ要件を満たしたIoT機器を認証し、安全なIoT機器の使用の推奨、普及を促進する。



期間　平成30年度～平成34年度

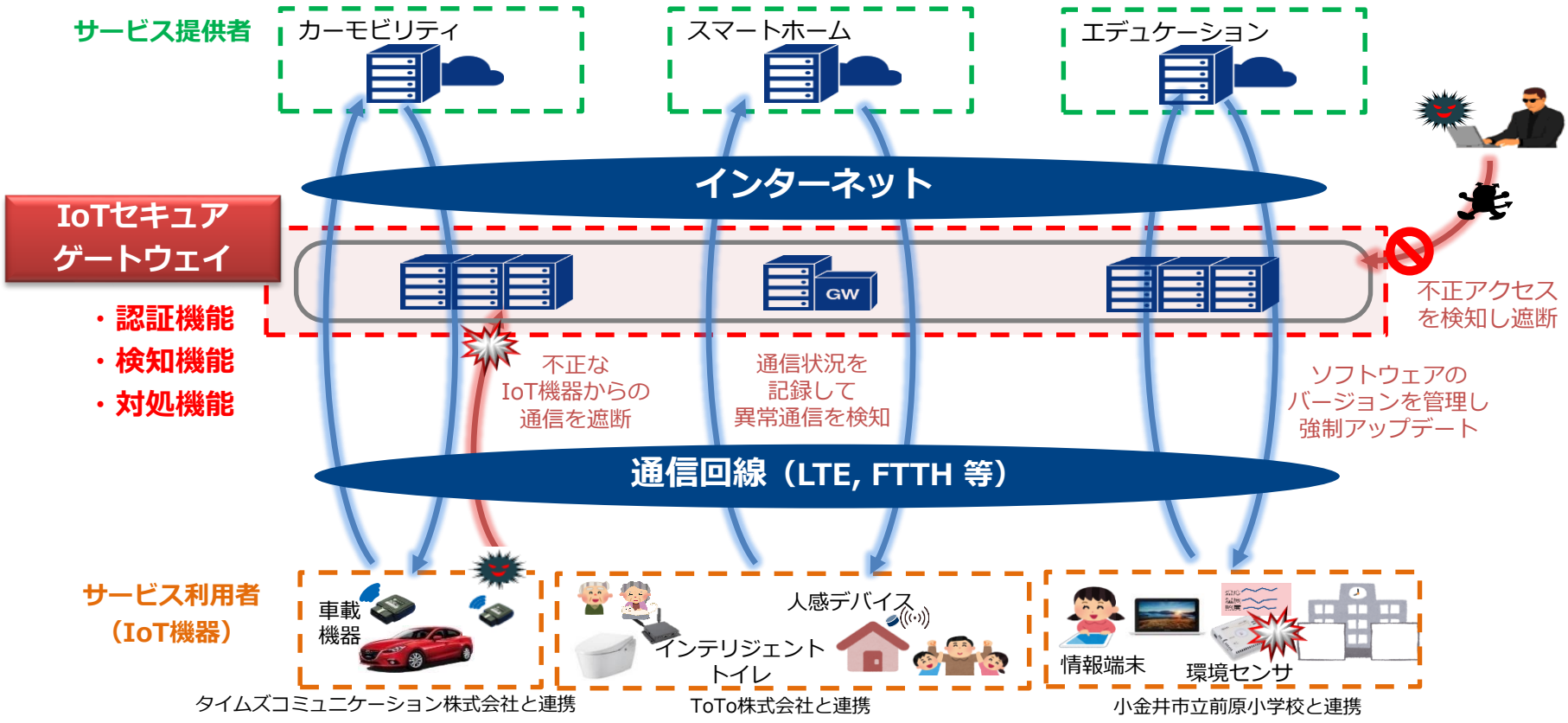
平成30年度政府予算案　6億円（5年間の総額では18億円を想定）

IoTセキュアゲートウェイの実証実験

○　IoT機器とインターネットの境界にIoTセキュアゲートウェイを設置し、その有用性に関する実証実験を実施。

○ 様々なセキュリティ脅威に対して、認証、検知、対処といった一連のセキュリティ対策ができるかを試行。

実証実験のイメージ



IoTセキュリティガイドライン

- 本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの（平成28年7月5日公開）。
- 各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	**IoTの性質を考慮した基本方針を定める**	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	**IoTのリスクを認識する**	• 守るべきものを特定する • つながることによるリスクを想定する
設計	**守るべきものを守る設計を考える**	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	**ネットワーク上での対策を考える**	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	**安全安心な状態を維持し、情報発信・共有を行う**	• 出荷・リリース後も安全安心な状態を維持する • 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す

IoTセキュリティ総合対策：研究開発の推進

■基礎的・基盤的な研究開発等の推進

新たに出現する未知の標的型攻撃の挙動を早い段階で明らかにするとともに、分析結果をセキュリティ対策機関等と連携して情報共有を図ることが可能な、高度で効率的なサイバー攻撃誘引基盤（STARDUST）を構築。

■広域ネットワークスキャンの軽量化

膨大なIoT機器に対する広域的なネットワークスキャンを効率的に実施するため、その軽量化などの必要な技術開発を推進。

■ハードウェア脆弱性への対応

ビッグデータやAIを活用しつつ、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推進。

■スマートシティのセキュリティ対策の強化

スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を　　国際的な標準化プロセスに提案する等の取組を一体的に推進。

■衛星通信におけるセキュリティ技術の研究開発

安全性を備えた衛星通信を実現するために、量子暗号技術の研究開発や高秘匿衛星光通信技術の実証を行うとともに、衛星のバックアップや高高度での中継を行うための航空機等による移動体光通信技術の研究開発を実施。

■AIを活用したサイバー攻撃検知・解析技術の研究開発

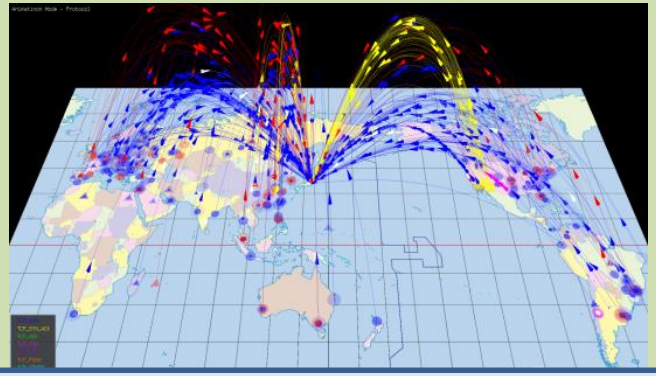
サイバー攻撃の検知・解析を自動化するような、AIを活用したサイバー攻撃検知・解析技術の研究開発を推進。

情報通信研究開発機構（NICT）におけるサイバーセキュリティ技術

■　国立研究開発法人　情報通信研究機構（NICT）では、研究開発の一環として、サイバーセキュリティ技術の成果展開を実施。無差別攻撃型（マルウェア）対策技術については、多くの自治体に導入が進むとともに、年金機構に対しても使用された標的型攻撃対策についても、早期導入に向けた取り組みを推進。

◆NICTER（ニクター）【無差別型攻撃対策】

- ダークネット（未使用IPアドレス）への通信をセンサーで観測することで、サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化。
- 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、マルウェアに感染した自治体へアラートを提供。



602自治体に導入済み（平成28年10月時点）

◆NIRVANA改（ニルヴァーナ・カイ）【標的型攻撃対策】

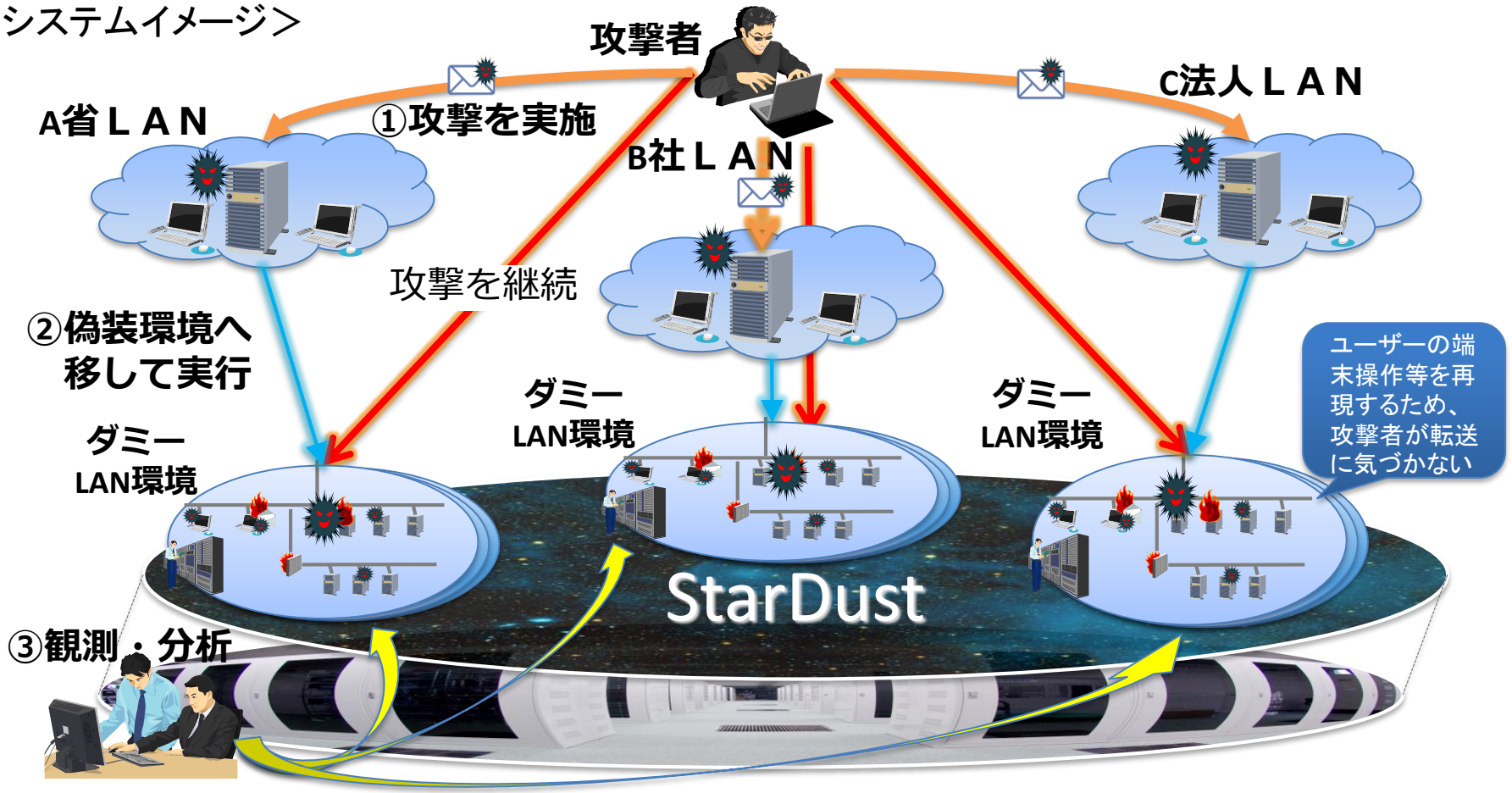
- NICTERの技術を応用し、組織内にセンサーを設置して組織内の通信状況をリアルタイムに可視化するとともに、本技術について2015年6月から技術移転開始。
- さらに、本技術と組み合わせ、ネットワーク内での異常検知時に通信を自動遮断する技術等を開発中。

技術移転を開始（平成27年6月）

サイバー攻撃誘引基盤（STARDUST）

■ NICTでは、標的型サイバー攻撃の詳細な手法を把握するため、①攻撃者が標的型メールを特定組織に送信した場合に、②不正な添付ファイル等を「あらかじめ構築した偽装環境」で実行し、③偽装環境で具体的な攻撃手段（入力コマンド等）の観測・分析が可能なシステム（StarDust）を研究開発している。

＜システムイメージ＞

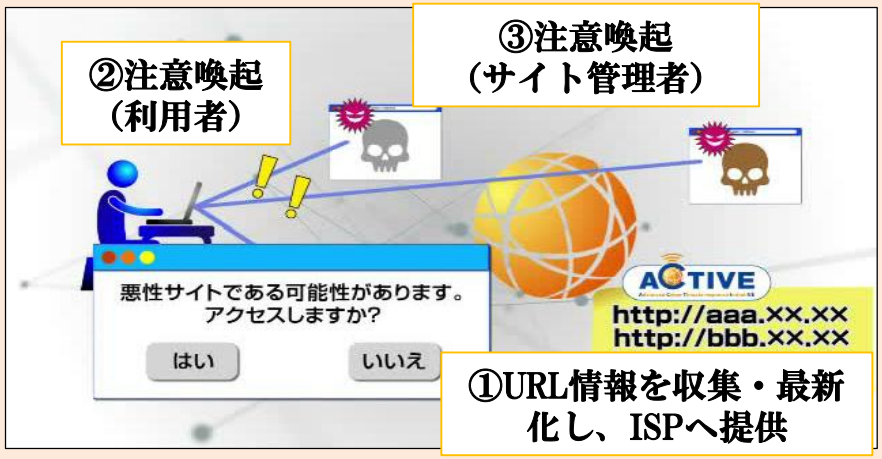


ウィルス感染被害予防対策“ACTIVE”

平成25年11月からインターネットサービスプロバイダ（ISP）等との協力により、インターネット利用者を対象に、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト（ACTIVE）を実施。

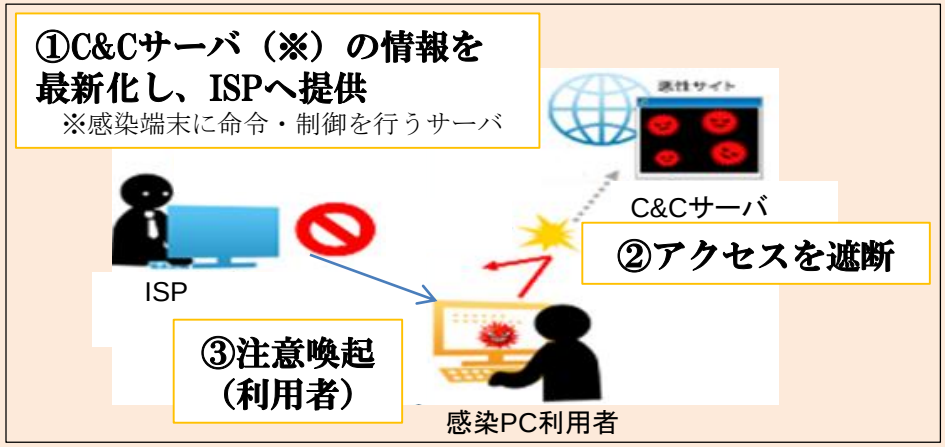
ACTIVE（Advanced Cyber Threats response InitiatiVE）の取組

（１）マルウェア感染防止の取組



①マルウェア配布サイトのURL情報を最新化し、ISPへ提供。
②マルウェア配布サイトにアクセスしようとする利用者にISPから注意喚起。
③マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

（２）マルウェア被害未然防止の取組



① C&Cサーバの情報を最新化し、ISPへ提供。
② 感染PC利用者からのC&Cサーバへのアクセスを遮断する。
（2016年2月から2017年10月までに約2億5,728万件の遮断実績）
③ 感染PC利用者に注意喚起。

○ 実施期間：平成25～29年度

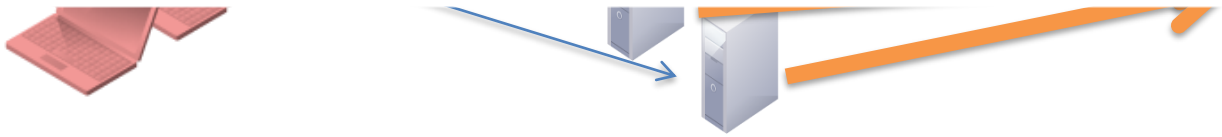
PRACTICE（研究）プロジェクトの紹介
-DR-DoS 攻撃に対する早期警報について-

DRDoS 攻撃とは

1. ボットが多量は問い合わせをレフレクター（Reflectors)
2. 答
3.

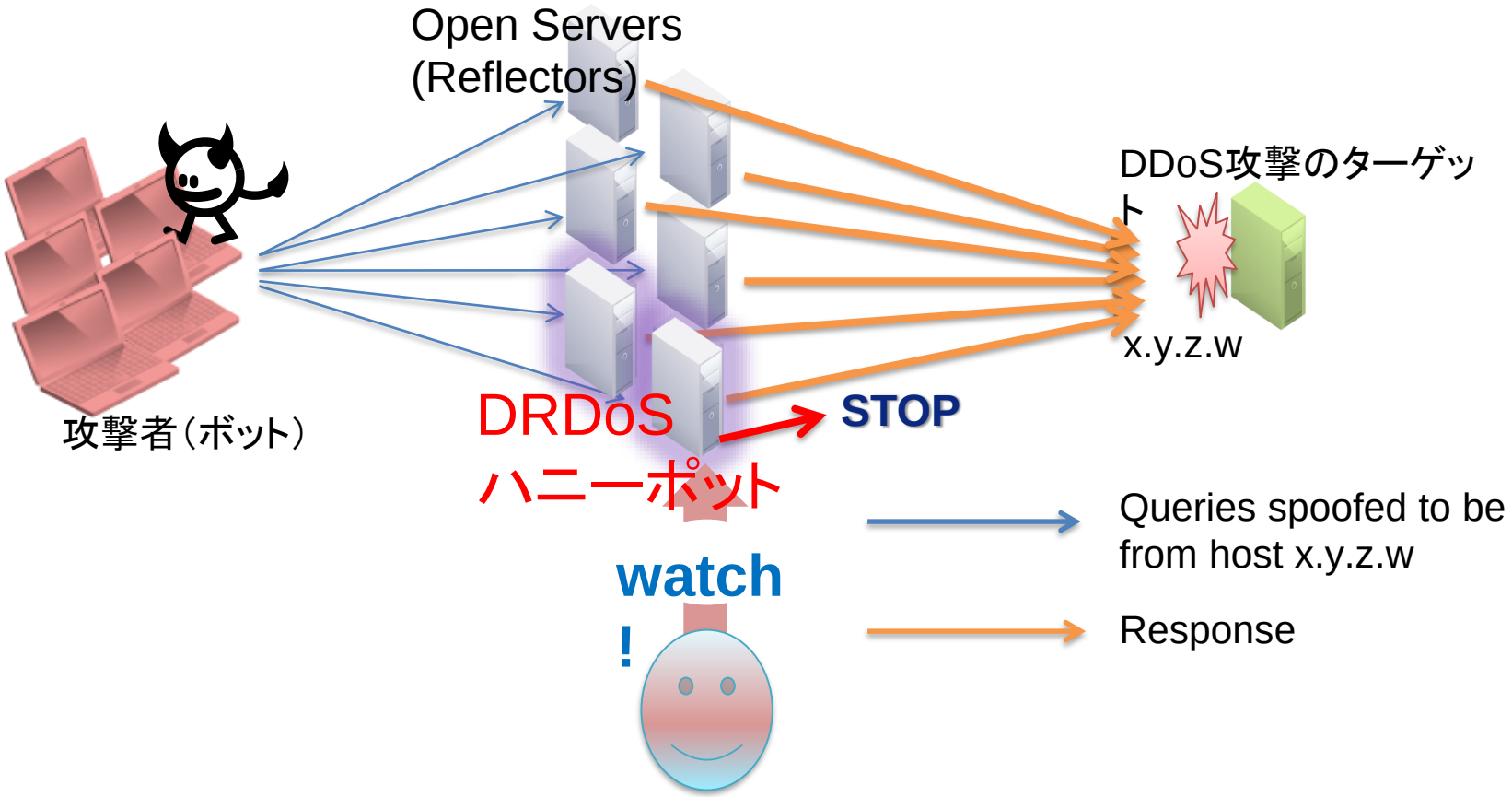
Cat	Protocol	Port(s)	Description
Network Svc	SNMP v2	161	Monitoring network-attached devices
	NTP	123	Time synchronization
	DNS	53	(Primarily) Domain name resolution
	NetBios	137	Name service protocol of NetBios API
	SSDP	1900	Discovery of UPnP-enabled hosts
Leg.	CharGen	19	Legacy character generation protocol
	QOTD	17	Legacy "Quote-of-the-day" protocol
P2P	BitTorrent	any	BitTorrent's Kademlia DHT impl.
	Kad	any	eMule's Kademlia DHT impl.
Gam	Quake 3	27960	Games using the Quake 3 engine
	Steam	27015	Games using the Steam protocol
Bots	ZAv2	164XY	P2P-based rootkit
	Sality	any	P2P-based malware dropper
	Gameover	any	P2P-based banking trojan

urce
oofed
se



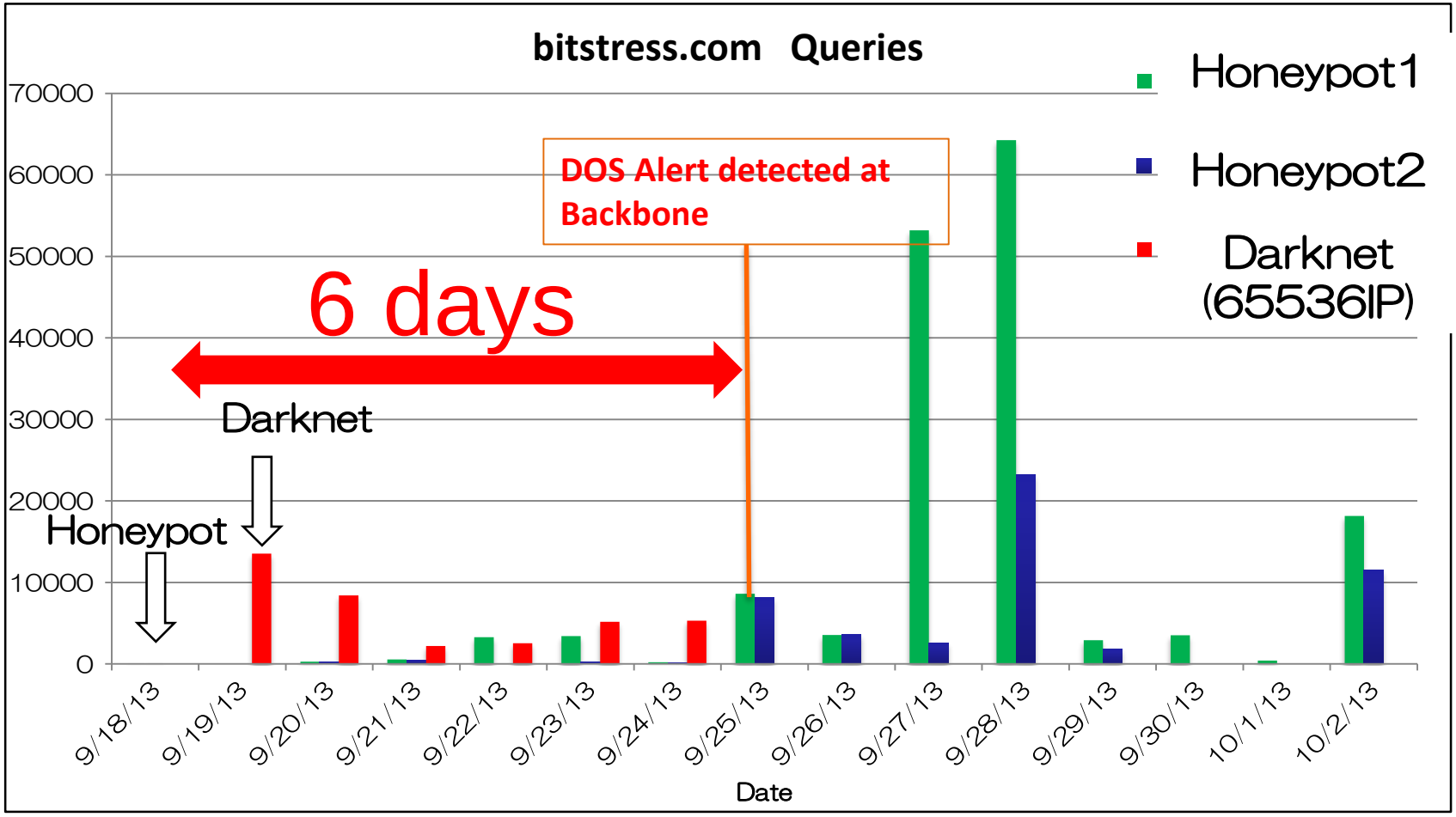
DR-DoS ハニーポット

PRACTICEプロジェクトは、DR-DoS攻撃をモニターするためのハニーポットを設置し、攻撃を捕捉した。



DR-DoSで狙われたドメインの早期検知(DNS)

実際、ISPのバックボーンで新たなDR-DoSの出現を検知する前にハニーポットやダークネットで該DR-DoSを検知している。



平均すると、どのくらい前に検知する？

本調査（統計）では、50％以上の場合に、2日以上前にDR-DoSを検知している。（DNSが使われた場合の例）

Days prior to attacks	#domains
0 day	4 (12.1%)
within 1 day	5 (15.2%)
2～7 days	7 (21.2%)
8～30 days	6 (18.2%)
31～ days	4 (12.1%)
After the attacks	3 (9.1%)
Not detected	4 (12.1%)

早期警戒アラートメール（例）

アラートメールの例：攻撃開始通知

攻撃対象IPの情報
（1アラートで1ホストのみ記載）

XXXX網宛DRDoS攻撃を観測しましたので、お知らせします。

攻撃観測センサ（DRDoS Honeypot）に対して閾値を超える攻撃パケットが初めて到達した時刻

[攻撃対象IP]
YYY.YYY.YYY.YYY

[検知時刻]
2015-ZZ-ZZ ZZ:ZZ:ZZ

攻撃の種類
dns: DNS Amp攻撃
ntp: NTP Amp 攻撃
chg: CHARGEN(port 19) Amp攻撃
qotd:QOTD(port 17) Amp攻撃
SNMP:SNMP(port 161) Amp攻撃
SSDP:SSDP(port 1900) Amp攻撃

[プロトコル]
NTP : port 123

[DRDoS Honeypot 詳細データ]
AS番号 : "AS???? XXXX"
country : "Japan"
pps(最大) : 2.183333333333333
pps(平均) : 1.1583333333333334

ハニーポットに対して攻撃パケットが連続して観測された期間内に検知された瞬間最大pps,最小ppsの数値

[ドメイン]

DNS Amp攻撃に該当する場合、攻撃に使用されたドメイン名、クエリタイプ、観測された総クエリ数

(end)

アラートメールの例：攻撃終了通知

XXXX網宛DRDoS攻撃観測結果について、以下の通りお知らせします。

攻撃開始時刻と攻撃終了時刻（攻撃開始後、被害IP宛に攻撃パケットが1分間以上観測されなかった時点の時刻）の両者を記載

[攻撃対象IP]
YYY.YYY.YYY.YYY

[検知時刻/終了時刻]
2015-ZZ-ZZ ZZ:ZZ:ZZ/2015-ZZ-ZZ zz:zz:zz

[プロトコル]
NTP : port 123

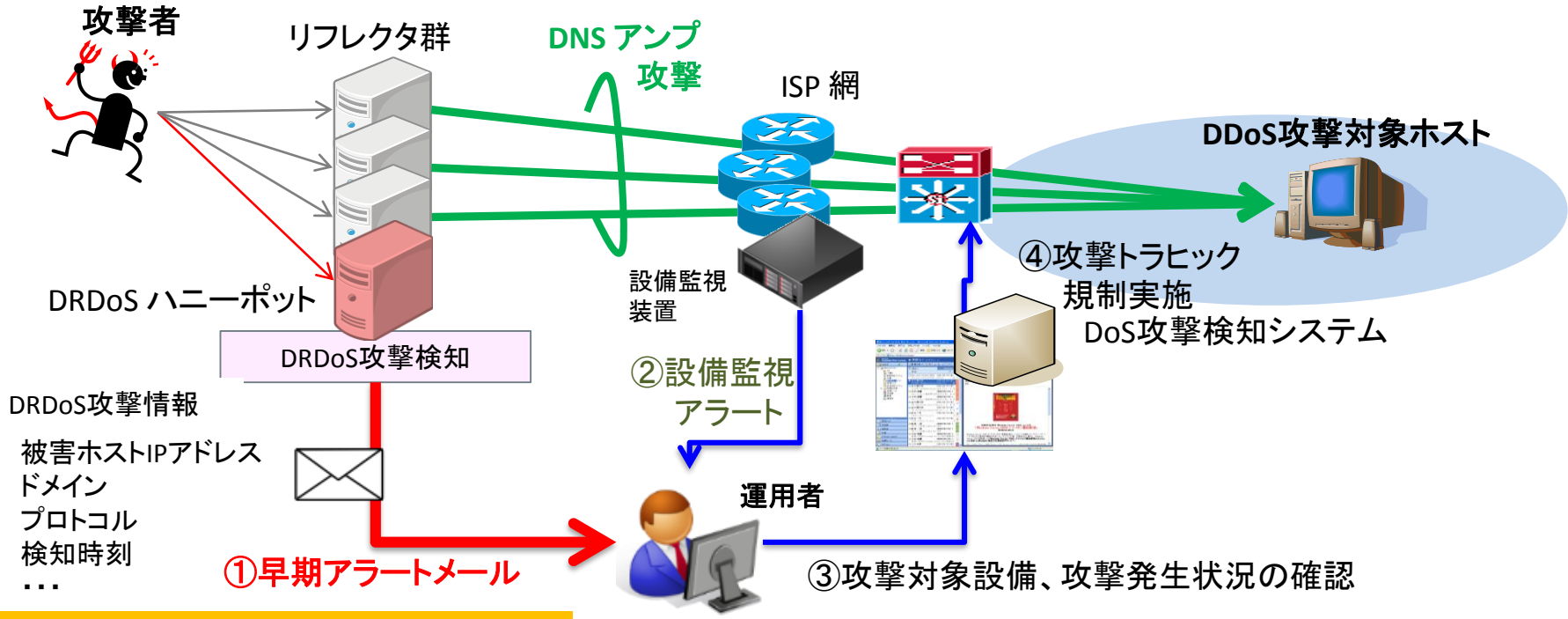
[DRDoS Honeypot 詳細データ]
AS番号 : "AS???? XXXX"
country : "Japan"
pps(最大) : 71.68333333333334
pps(平均) : 58.96875
総パケット数 : 28305

[ドメイン]

(end)

早期警戒アラートの利活用

■ 昨年度より実施している国内ISP向けに「DRDoS ハニーポット」を活用したリアルタイムアラート情報の配信を継続し、既存のDoS攻撃対策システムとの連携等の導入により以下の通り更なる攻撃対応の早期化へ取り組んだ。



早期警戒アラート利活用の評価結果

2015/4/1～11/30の間で対応を行った大量通信に対するアラート活用の評価状況は以下の通り。

1) 発生検知までの時間： 設備アラート発生の「3分3秒」前に本アラートを運用者へ配信
2) アラート配信時の対応時間：アラート非配信時と比較してDoS攻撃対応時間が「34秒」短縮
3) 精度（大量通信の検知精度）：「89.8%」（948件の本アラートの内、851件が大量通信と合致）

リスクマネジメントの促進のための取組概要

取組の目的

サイバー攻撃等による2020年東京オリンピック・パラリンピック競技大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。
第２回は対象を１都３県に拡大するとともに、横断的リスク評価を実施するために必要な情報について報告いただいた。

リスク評価の取組概要

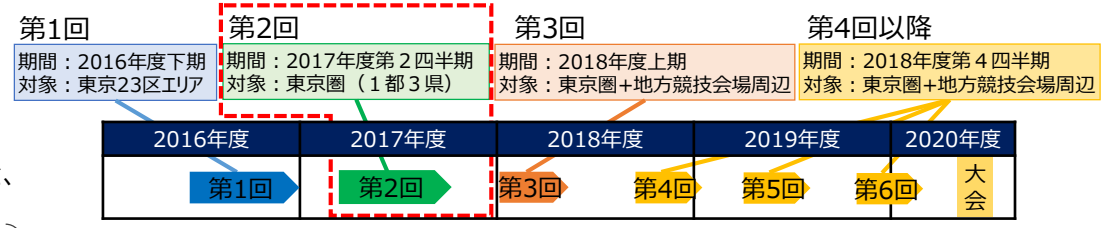
○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成。

○ 東京大会の開催・運営に影響に与えうる重要サービス分野を、関連する所管省庁と調整の上で選定。

通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給、バス　計20分野
第 2 回で選定した重要サービス分野

○ 東京大会に向けて、継続的に複数回実施。PDCAサイクルを繰り返す。

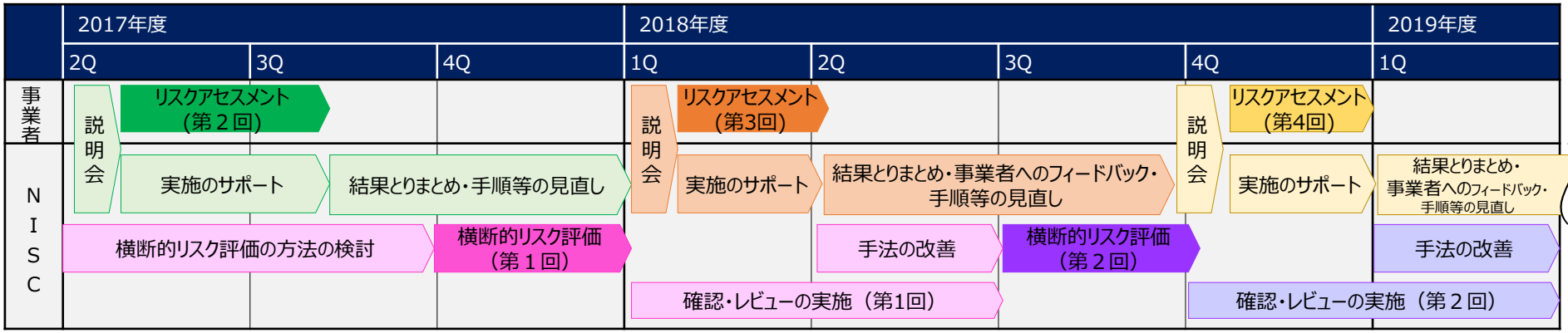
○ NISCによる大会全般にわたる横断的リスク評価の実施に向けて、必要な情報の特定や方法の検討を実施。



東京大会に向けたリスクアセスメントの取組スケジュール

【横断的リスク評価】

サービスの継続的な確保が滞った場合に、大会への影響が重大なサービスを分野を横断して抽出するとともに、それらのサービスに対して、事業者等が自組織におけるリスクアセスメントで設定した満たすべきサービス水準が妥当であるかを検証。検証結果は、事業者等におけるリスクアセスメント結果の妥当性確認や、大会に向けた訓練等に活用。



2019年度第１四半期までのスケジュール（予定）

「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」の概要

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系(ＩＴ)に限らず、制御系(ＯＴ)を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

３．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

①　先導的取組の推進(クラス分け)

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

②　オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③　リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

４．本行動計画の期間

➢　第４次行動計画はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

重要インフラサービス障害等に係る深刻度判断基準（素案）

○ 概要

重要インフラサービス障害の深刻度や当該障害に関する情報の重要度に応じて影響範囲や対処行動等が異なってくることも踏まえ、関係主体間で認識の共有を図り、迅速な対応要否等の判断に資するため、下表のとおり、重要インフラサービス障害に係る深刻度の判断基準の例を設け、具体化に向けた検討を進める。（第4次行動計画別添抜粋）

○ 目的

①可視化された深刻度により、発生した事象について関係主体間で共通の理解を助ける（客観性、国際的整合性に留意）

②深刻度レベルを政府の対応を判断する基準とする

③事象に関する情報共有の体制や方法の基準とする

表1　重要インフラサービス障害に係る深刻度判断基準（例）

深刻度	定　義
レベル5（危機）	複数の重要インフラサービスに著しい影響を与えるおそれが切迫している事象
レベル4（重大）	重要インフラサービスに著しい影響を与えるおそれが高い事象
レベル3（高）	重要インフラサービスに一定の影響を与えるおそれが高い事象
レベル2（中）	重要インフラサービスに影響を与えるおそれがある事象
レベル1（低）	重要インフラサービスに影響を与えるおそれが小さい事象

（第4次行動計画別添抜粋）

具体化

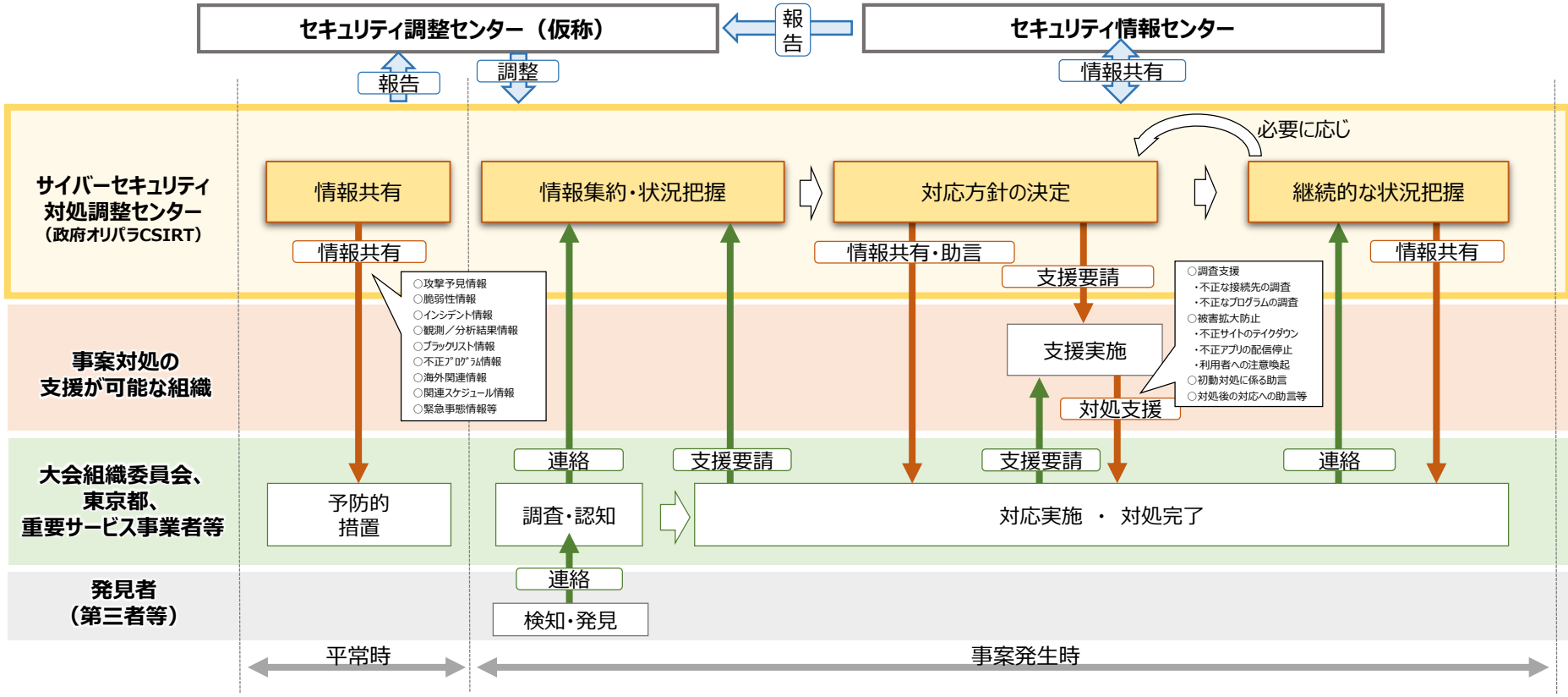
表2　検討のための素案

深刻度	国民・社会への影響	システムへの影響	
		非常用系	常用系
レベル5（危機）	国民生活等に広範かつ著しい影響を与えるおそれが切迫		
レベル4（重大）	国民生活等に著しい影響を与える可能性が高い	重要インフラサービスの安全性・持続性への影響により評価	
レベル3（高）	国民生活等に明らかな影響を与える可能性が高い		重要インフラサービスの提供への影響により評価
レベル2（中）	国民生活等に何らかの影響を与える可能性がある		
レベル1（低）	国民生活等に影響を与える可能性は低い		
レベル0（なし）	国民生活等に影響を与える可能性はない		

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）の構築等について

◆「サイバーセキュリティ対処調整センター」の構築時期・役割等をセキュリティ幹事会において決定（平成29年12月）

- サイバーセキュリティ対処調整センターを平成30年度末を目途に構築する。
- センターの構築及び運用は、オリパラ推進本部の下で、オリパラ事務局と緊密に連携し、内閣サイバーセキュリティセンターが中心となって行う。（センターの運用前については、NISCがその業務を担う。）
- センターは、大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供するとともに、必要があるときには関係機関等のインシデント対処に対する対処調整を行う。
- オリパラ特措法第８条第１項の規定を踏まえ、センターは、必要があると認めるときは、大会組織委員会等に対して、サイバーセキュリティに係る情報の提供、説明その他必要な協力を求める。



サイバーセキュリティ分野における国際連携

サイバー空間に関するグローバルな議論

- サイバー空間の国際的なルールの形成と普遍化、最先端の知見の共有、信頼醸成、情報共有等を目的として、国連サイバー政府専門家会合、重要インフラ防護に関するMeridian会議（※１）、先進各国によるIWWN（※２）、産学官の関係者が一堂に会する「サイバー空間に関する国際会議（ロンドン・プロセス）」等に参加。

※１　重要インフラ防護に関する国際連携を推進する場として2005年に英国で始まった会合。我が国の他、欧米やアジアの各国の政府職員が参加し、重要インフラ防護に関するベストプラクティスの交換や国際連携の方策等について議論。

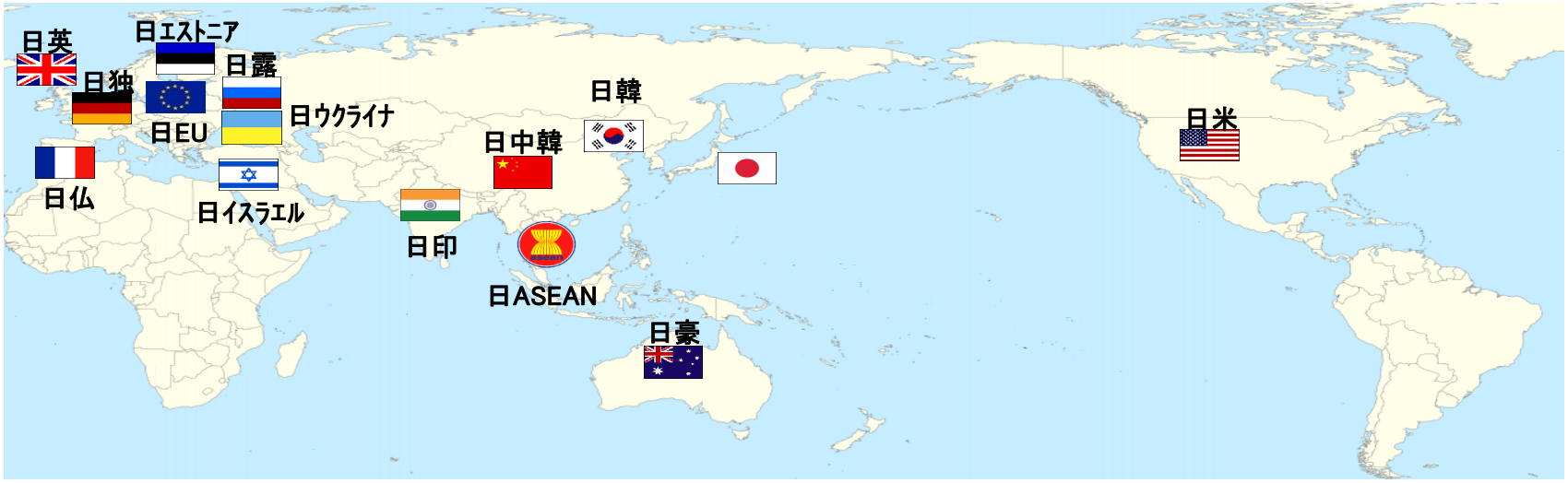
※２　2004年に米国土安全保障省と独連邦内務省の主導により創設された枠組。サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組みを促進することを目的とする。先進各国のサイバーセキュリティ担当機関及び国を代表するCSIRT（インシデント対処を行う部門）が参加。

二国間協議

- 2012年の英国及びインドを皮切りに、米国、EU、中韓、イスラエル、仏、エストニア、豪州、ロシア、独、韓及びウクライナとの間でサイバー協議を実施。各国との間で年1回程度の頻度でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論。

地域連携・セキュリティレベル底上げ

- セキュリティマネジメント体制の確立、維持、改善などを目的として日ASEAN情報セキュリティ政策会議等を実施。



米国との国際連携

- 近年、サイバー攻撃の態様は、より一層複雑化・巧妙化・高度化。また、国境を越えるサイバー空間の脅威に対しては、国際的に連携して対処していく必要。
- サイバー攻撃は、自衛隊や米軍の任務遂行の場面において大きな阻害要因等となり得ることから、今後日米防衛協力を一層推進していく上で、サイバー空間の安定的かつ効果的な利用の確保は重要。

日米サイバー協力の主要枠組み

- 日米サイバー対話（政府間の包括的な協議）
- 日米サイバー防衛政策ワーキンググループ（防衛当局間の政策協議）
- 日米ITフォーラム（防衛当局間の情報通信分野に関する協議）
- 日米情報保証実務者定期協議（統幕、在日米軍間の協議）

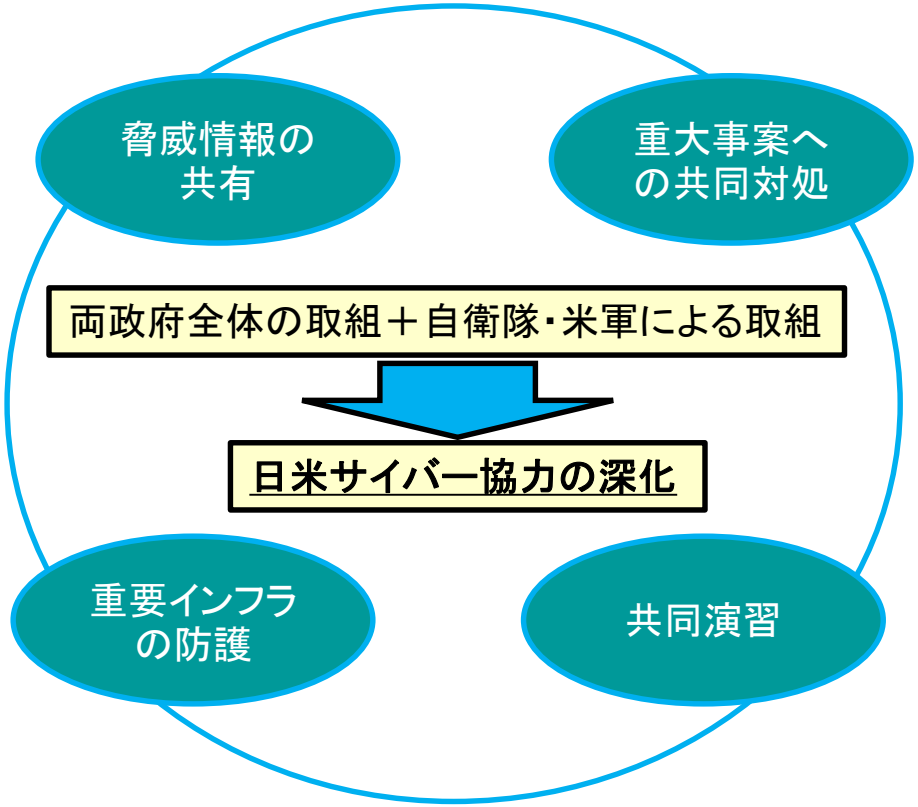
日米サイバー防衛協力の主要成果

日米防衛協力のための指針（平成27年4月）

- サイバー空間に関する協力の項を新たに設け、情報共有等、今後の日米のサイバー協力に関する方向性を記述

日米ｻｲﾊﾞｰ防衛政策ﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ共同声明（平成27年5月）

- サイバーに係る脅威認識を共有した上で、重大なサイバー事案への対処、役割・任務、情報共有、重要インフラ防護等、防衛省＝国防省間における具体的な協力分野を記述。

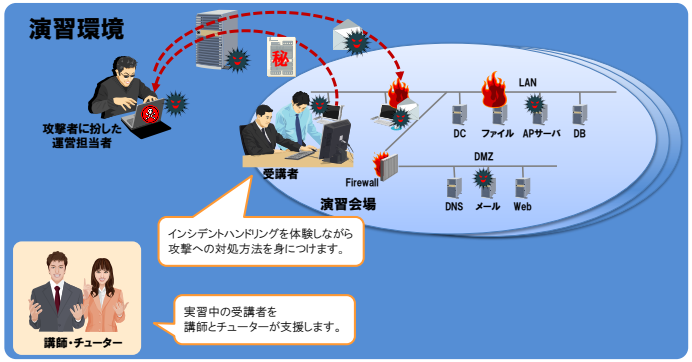


この他、シンガポール、ベトナムとの防衛当局間でITフォーラムを実施するとともに、英国、NATO、エストニア、豪等との間で、防衛当局間によるサイバー協議を設け、脅威認識やそれぞれの取組に関する意見交換を実施。

国際連携の推進

■ASEAN各国との連携

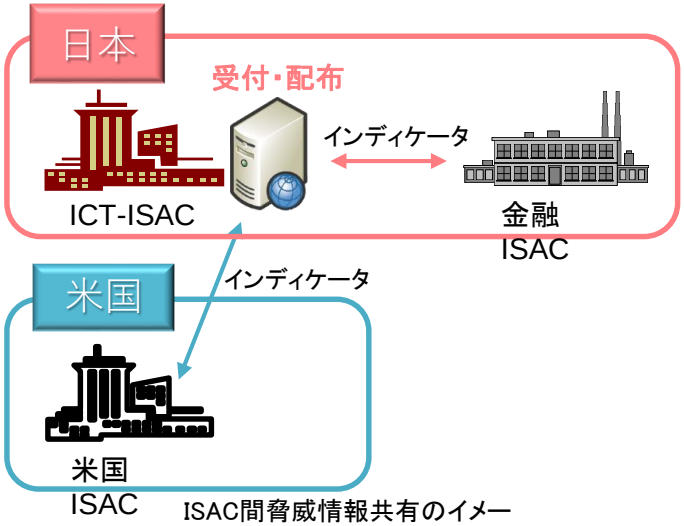
実践的サイバー防御演習「CYDER」等の海外展開を通じたセキュリティ人材の育成支援（日ASEANサイバーセキュリティ能力構築センター等）を推進するとともに、各種会議等を通じて、我が国及びASEANにおけるサイバーセキュリティの脅威をめぐる状況やIoTセキュリティ対策に関する情報交換を行うほか、ASEAN側のニーズを踏まえつつ、ASEANにおけるIoTセキュリティ強化に向けた施策の導入・促進のための協力を推進。
（平成29年～平成33年の5年間で800人を目標）。



実践的サイバー防御演習のイメージ

■国際的なISAC間連携

国際連携ワークショップの開催等を通じて、日本のICT-ISACと米国のICT分野のISACとの連携を強化し、通信事業者、IoT機器ベンダー、セキュリティベンダー等が、AIS（Automated Indicator Sharing）等を介して脅威情報を自動的に共有し、サイバーセキュリティ対策への活用を促進。



ISAC間脅威情報共有のイメージ

■国際標準化の推進

ISO/IEC（国際標準化機構/国際電気標準会議）及びITU-T（国際電気通信連合電気通信標準化部門）における、IoTシステムのセキュリティに係る国際標準化に関する活動に積極的に貢献。

■サイバー空間における国際ルールを巡る議論への積極的参画

様々なチャネルを通じて進められている、サイバー空間における国際ルール等に関する議論へ積極的に参画。

サイバーセキュリティに関する研究開発

達成目標

戦略的ｲﾉﾍﾞｰｼｮﾝ創造ﾌﾟﾛｸﾞﾗﾑ（SIP）「重要インフラ等におけるサイバーセキュリティの確保」
H27（2015）年度～H31（2019）年度（予定）、H27年度予算：5億円、2016年度：25.5億円、2017年度：27.1億円

- **悪意のある機能を“持ち込ませない”、悪意のある動作を“いち早く発見する” システムの実現**
- **国産セキュリティ技術を確立。重要インフラ産業の競争力強化、安全な社会基盤実現に貢献**

⇒ **2020年五輪大会の安心安全な開催**

PD

情報セキュリティ大学院大学学長
後藤　厚宏

研究開発計画案概要

アウトプット目標①　（コア技術）

機器・ソフトウェアの改ざんを検知する真贋判定技術およびＩｏＴ向け暗号実装技術

（システム構築時～運用時）

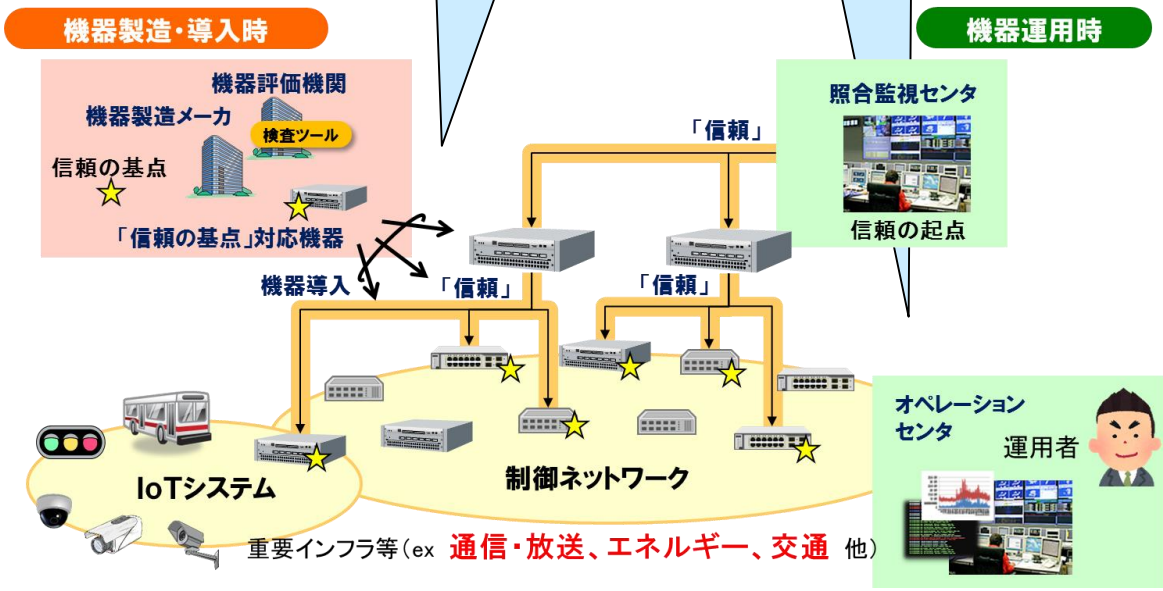
アウトプット目標②　（コア技術）

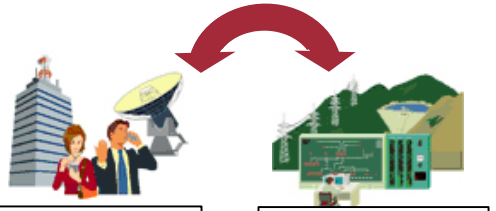
制御ネットワークシステムの異常動作を早期に検知し防御する動作監視・解析・防御技術

（運用時）

アウトプット目標③　（社会実装技術）

- 適合性確認のあり方と仕組み
- 重要インフラの環境下での評価検証技術
- 重要インフラ分野内・分野間の情報共有基盤
- システム運用者のセキュリティ対応能力を継続的に向上できる環境整備
- ＩｏＴ技術の活用ニーズの急速な高まりを踏まえたＩｏＴセキュリティ社会実装技術





通信放送分野　エネルギー分野　交通分野

- **また、安全なIoT機器やIoTシステムを利用するビジネス等の普及、我が国製品の海外展開を念頭に置いたセキュリティの国際標準化等の活動を進める**

今後の日本のサイバーセキュリティ研究開発？（私見1）

- 近年　攻撃者と防御者の力の差がさらに大きくなっている
- ハイレベルの攻撃者には、潤沢な予算が付いており、ほぼ多くのセキュリティ施策の調査、検証を実施している
- 防御側としては、多くの分析知見を横連携する連携共有力、連携分析力を強化するしかない
- さらに、これらの分析などの知見においては、学術系（大学系）をきちんと入れ実施することが重要
- 最近のハイレベルではない、アベレージ(以下）のハッカーは、「ばら撒き」型APTを多く出しており、多くが「お金」目当て。その場合、メールからマルウェアInjectし、攻撃者（人間）が重要なファイル（売れるファイル）があるかを探し、なければ、そのPC/システムが「ボットに使える環境か」を確認し、もしボットに使えない場合は、ランサムをしかけてお金をとる・・ような動作がほとんど。
- ただ、ハイレベルのハッカーはお金にはそんなに執着しない（すでにお金持ち）

今後の日本のサイバーセキュリティ研究開発？（私見2）

- 遠い先の状況を見ることが非常に難しい状況になっている。
- まずは、近傍の世界に視点をおきたい。

- サイバー攻撃は、研究者の環境で具体的に把握することは難しい。組織、国の運用の現場で起こっている。
- そのためには、総合的な観測力強化、分析力強化、共有力強化を多くの関係組織と連携して実施する体制、実現力が必要。すなわち、「連携力の強化」を促進する必要あり。
- その際、どのように学術系から寄与、関与できるのか
  - ✓ 新しい観測手法の考案　（実データが重要）
  - ✓ AIなど活用の分析・解析手法の考案　（実解析が重要）
  - ✓ 耐性強化のための研究開発
  - ✓ アカデミアと実運用系との橋渡しが重要、結果を活用できる環境つくり
- 基盤系セキュリティ（暗号などの基礎技術）の研究開発は平行して進めるべき。

Thank you for your attention

Toward success of Tokyo 2020!!