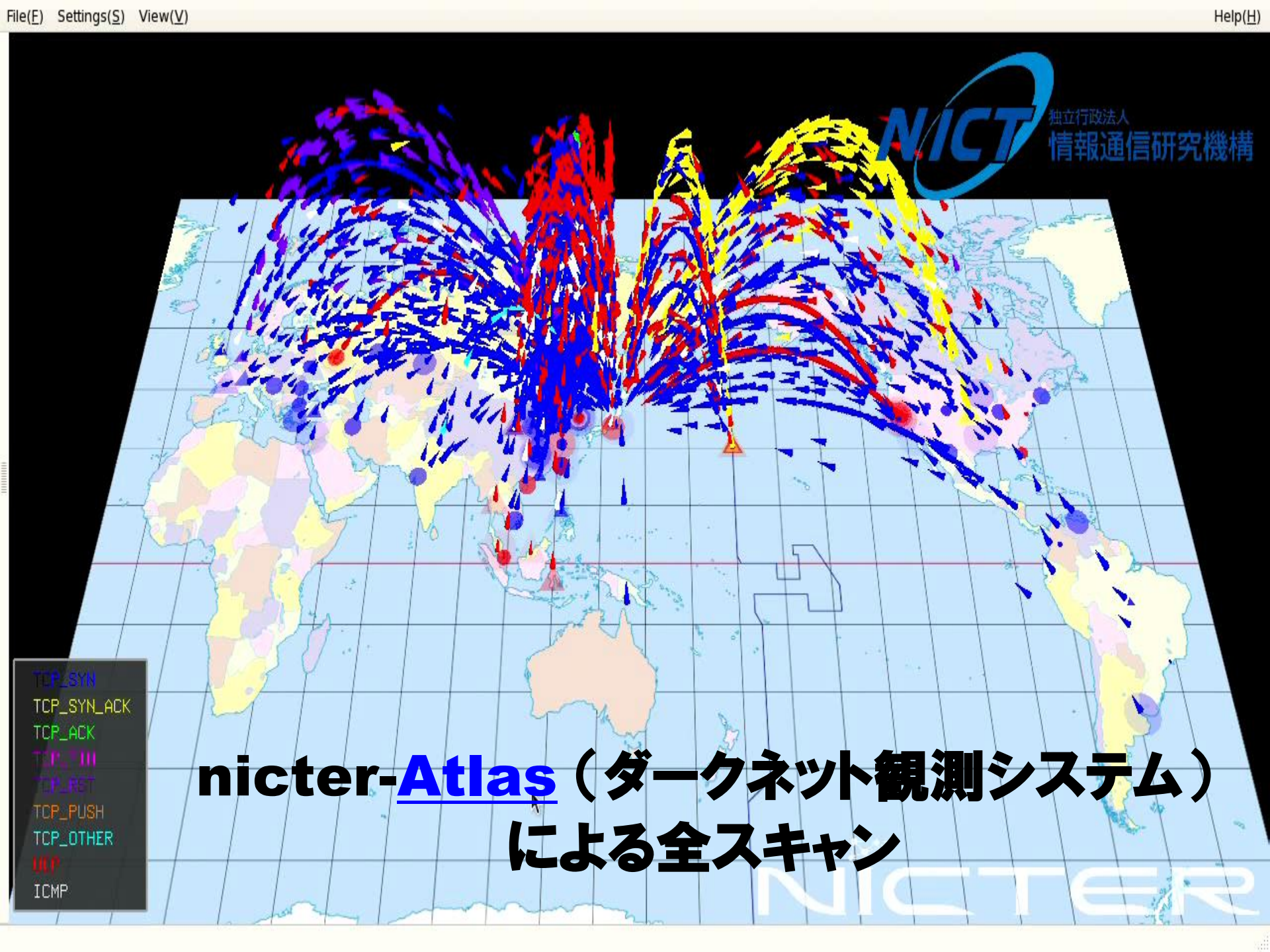
サイバーセキュリティ研究開発における今後の展望

中尾康二

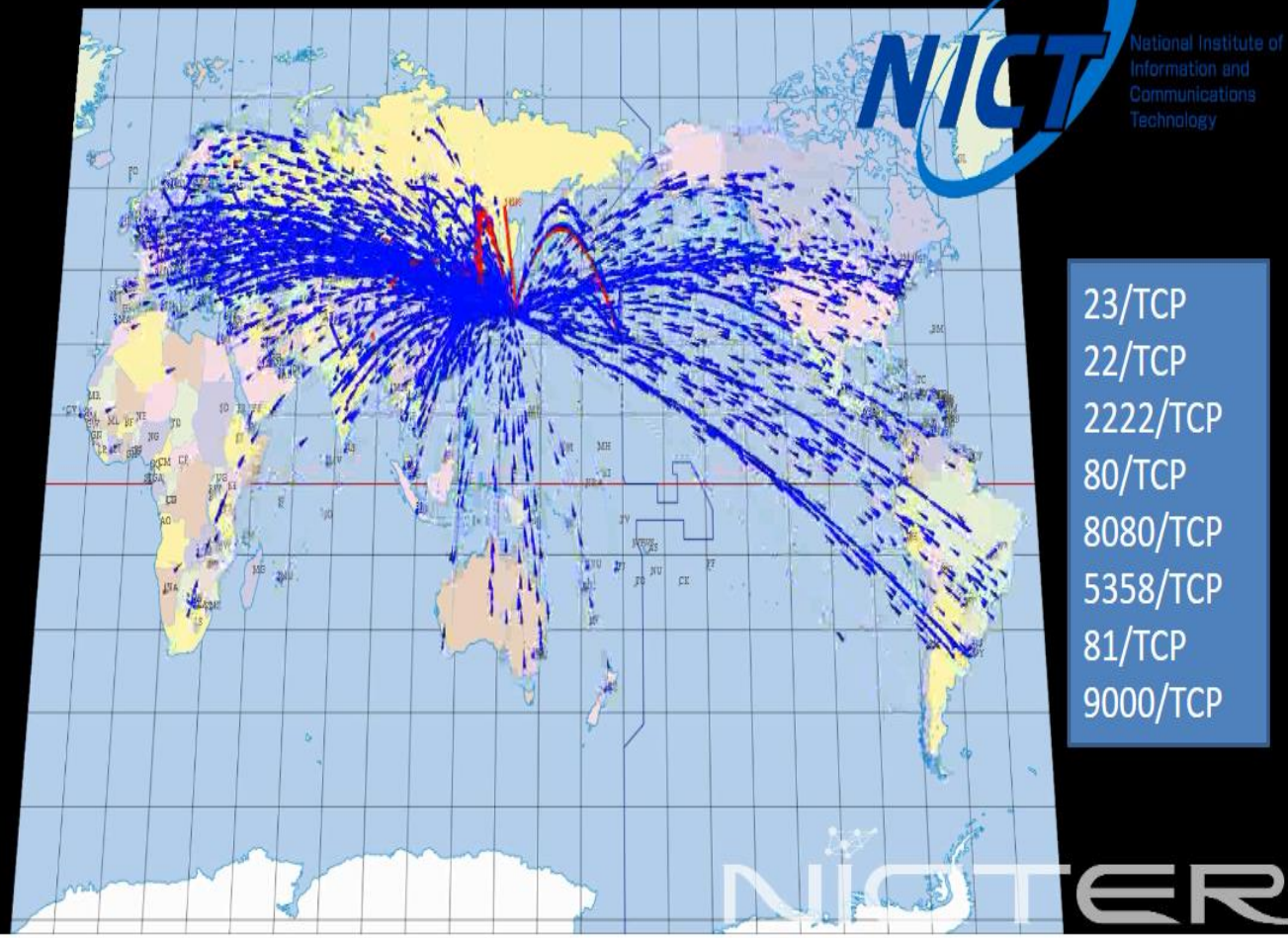
NICT サイバーセキュリティ研究所　主管研究員

サイバー攻撃の現状

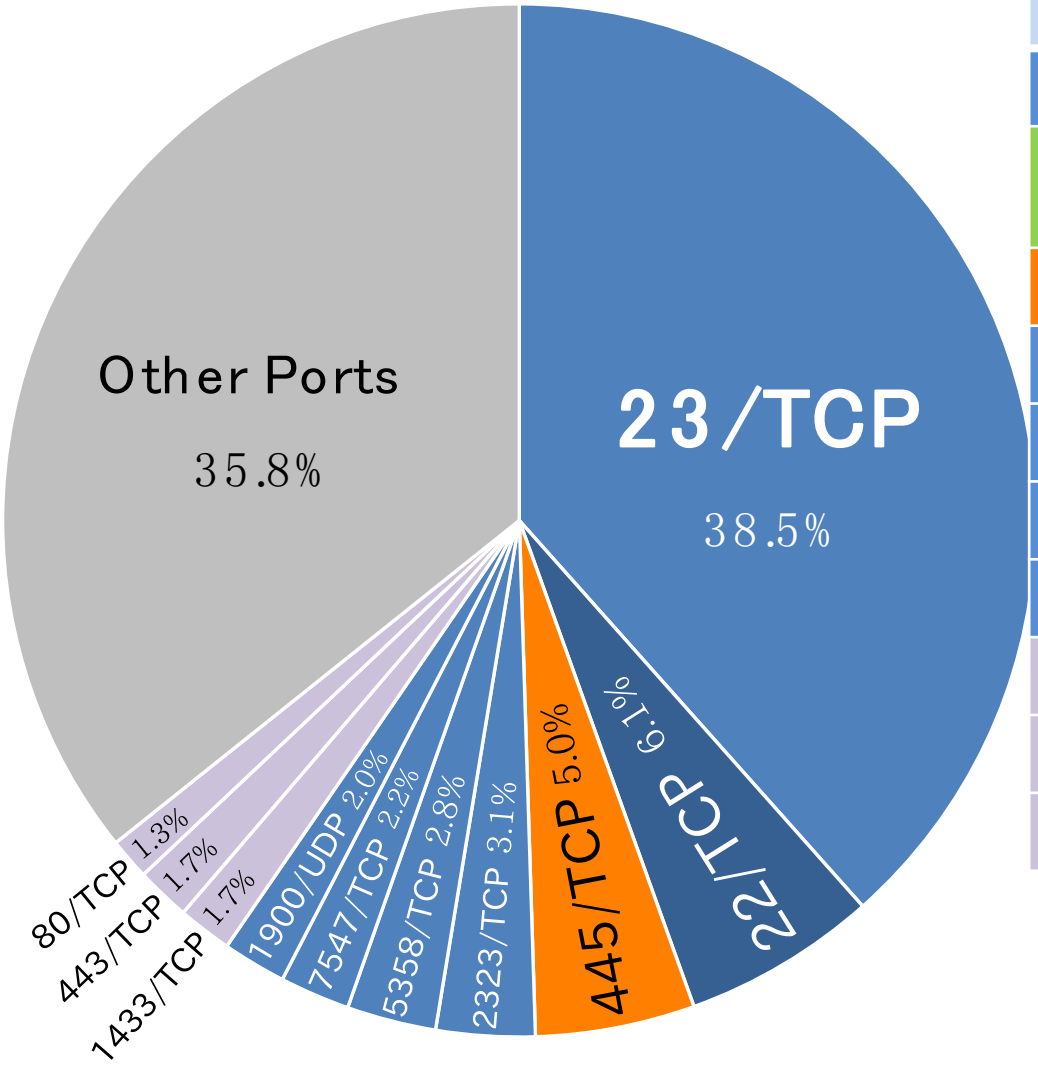
- NICTによるサイバー攻撃観測：1500億回スキャン/2017年、5300スキャン/秒（スキャン：攻撃の予備活動として、標的を調査する活動）
- マルウェア発生の頻度：2017年：1億２千万/年、36万/日（以前と比較：９千/日：2007年、40/日：1997年）、実際のハッキング数（約2000件/日（2017年））
- 100以上の高度に洗練された攻撃グループが世界中に存在（標的：金融機関、重要インフラ（制御系システムを含む）、製造業、運輸業などへと拡大化（多くが金銭目的））
- テロリズム（妨害活動）による被害：ドイツ（製鋼所）：2014、ウクライナ（送電網）：2015-2016、英国/ドイツ等（病院等）：2017、韓国（冬季オリンピック）：2018などで多発
- セキュリティ対応費用の増大等：ランサムウェア（暗号化し金銭をとるマルウェア）/80億ドル（世界）、50％費用増加（日本）、内部犯行事例の増加（攻撃全体の約20％に）
- 最近の急増するビジネス環境による脆弱点の多様化：クラウド、ビックデータ、IoT、サプライチェーン、5G（第5世代ワイヤーレス通信）等への変化


File(F) Settings(S) View(V)
Help(H)
独立行政法人
情報通信研究機構
TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
UDP
ICMP
nicter-Atlas（ダークネット観測システム）
による全スキャン
NICTER

IoT攻撃に関連するポート群へのスキャン
（ポート23へのスキャンを含む）



スキャン攻撃で使われているポートの分散（2017年）



Port	Target Service
23/TCP	IoT (Web Camera, etc.)
22/TCP	IoT (Mobile Router, etc.) SSH
445/TCP	Windows (Server Service)
2323/TCP	IoT (Web Camera, etc.)
5358/TCP	IoT (Web Camera, etc.)
7547/TCP	IoT (Web Camera, etc.)
1900/UDP	IoT (Home Router, etc.)
1433/TCP	SQL
443/TCP	SSL/TLS
80/TCP	HTTP

５４％以上がIoT関係

NISC National center of Incident readiness and Strategy for Cybersecurity

参考資料５－２

H29年策定のNISC　研究開発戦略

サイバーセキュリティ研究開発戦略 骨子について

平成29年 3月 3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．策定方針

平成26年７月に、今後３年程度を見据えた基本的な研究開発の方針として、「情報セキュリティ研究開発戦略（改訂版）」を策定した。「サイバーセキュリティ基本法」及び「サイバーセキュリティ戦略」（平成27年9月策定）を踏まえ、「サイバーセキュリティ研究開発戦略」を策定する。

（１）研究開発の目的

①研究開発を通じて国際競争力を強化すること
②研究開発で得られた知見により経済成長につながる新産業を創出すること
③我が国として必要な技術力を獲得・保持すること

（２）対象

- 政府や公的研究機関等のみならず、大学、企業等の取組についても視野に入れる。

（３）時間軸と内容

- 「近い将来」だけでなく「中長期」な社会・経済とITの利活用の進化を視野に入れる。
- 個々の技術的な課題を深掘りするのではなく、将来的なサイバーセキュリティの考え方を踏まえた研究開発の方向性について、ビジョンを示す。

2．状況認識と課題

（1）視点

・ITの進歩は極めて急速であり、数年後の予測は困難。このため、長い人類の歴史を見据えた上で、現在を位置付け、未来に向けたサイバーセキュリティの研究開発を考えていくことが必要

（2）現代の認識

・人類の知的活動に関わる欲求について、これまで「知の継承」（文字と紙の発明）、「知の流通」（活版印刷の発明）、さらには「場所や時間の制約にとらわれない知の共有・活用」（コンピュータとインターネットの発明）を実現

・経済成長のために必要な新しい価値を生むフロンティアの発見が必要

・近代（工業化社会）の終わりとしての情報・知の時代をむかえており、万人が自己の思いやより良い社会の実現をできる転換期に差しかかっているのではないか。

（3）ITの進化と人・社会のかかわり

・専門家のツールとしてのITから、個人のツールとしてのIT、そしてあらゆる個人とその活動・モノがつながるITに変遷。その中で、近年、人と情報の関わり方も大きく変化。

①**「情報の環境化（空気のような存在）」**：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時代

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

今後の課題

サイバー空間の広がりや脅威の深刻化を踏まえ、近い将来のIT利活用に必要なサーバーセキュリティに関する研究開発を促進するとともに、サイバーセキュリティの考え方の変化も含め、中長期を見据えた独自性の高い研究開発を推進

3．サイバー空間の脅威の深刻化への対応
～近い将来のITの利活用に必要なサイバーセキュリティ技術の開発～

近い将来（５～１０年後）想定されるITの利活用の進化と、セキュリティ研究開発における課題に対応するための取組を推進する。その際、脅威に対する後追いではなく、近い将来の脅威を見越した研究開発を行うことが重要である。

■基本的な考え方

- システム全体（情報システムだけでなく、それを取り巻く環境）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社会学的なアプローチも重要

■近い将来のITの利活用の進化(例)

サイバー空間と物理空間の融合(IoT)	AIの高度化・ビッグデータの活用	ネットワーク技術の高度化
• セキュリティの範囲が広がるため、セキュリティ技術のみならず、幅広い技術の知見を統合した研究開発。 • これまで物理空間特有の問題であった安全管理を視野に入れたセキュリティの研究開発。	• ビッグデータの信頼性を確保して活用する技術やプライバシー保護の研究開発。 • AIの脆弱性に対する攻撃対応。 • サイバー攻撃のAI化への対応（防御のAI化）。	• 新しいネットワーク技術におけるセキュリティ・バイ・デザインが必要。 • 暗号の高速化・高度化が必要。 （例：暗号化したまま高速に検索ができる技術の確立など）

■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
- 攻撃の実データを活かし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・クローズド戦略と海外への発信

4．サイバーセキュリティの考え方の再定義
～中長期を見据えた独自性の高い研究開発～

- 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、サイバー空間を介して人間の能力は拡張し、これまでの生活や労働を代替するにとどまらず、新たな価値を創造していくと考えられる。そして、人々の思いやより良い社会の実現につながっていく可能性がある。
- このように実空間とサイバー空間の融合が高度に深化していく中で、「自由、公正かつ安全なサイバー空間」を創出・発展させるためには、サイバーセキュリティの考え方として、サイバー空間を構成する情報システムへの脅威への対応のみならず、「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、強くすることに注目すべき。（サイバーセキュリティの考え方の再定義）

■人間や社会システムを守る視点での研究開発（例）

（人間の脳を守る）

・AIやAR/VR技術により、サイバー空間を介して人間の判断や行動に影響を及ぼすことへの対応が必要ではないか？

（人間の身体を守る）

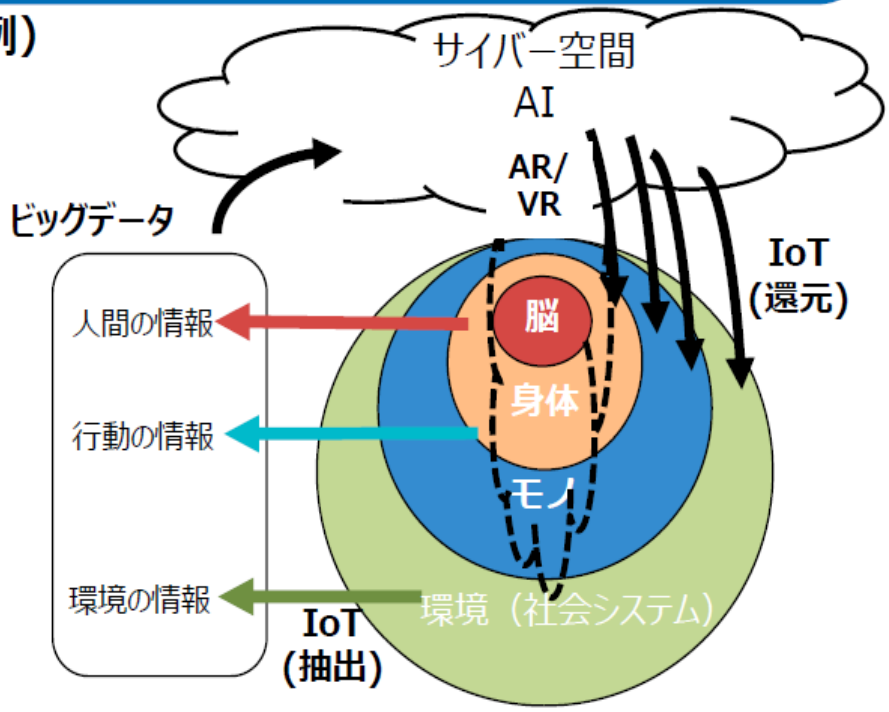
・自動運転やロボットといったIoT技術が身近になるため、サイバー空間からのいかなる影響に対しても、人間の安全を確保することが必要ではないか？

（人間を取り巻く環境（社会システム）を守る）

・「機能保証」の考え方を基本とした研究開発の再構築が必要ではないか？

■システム全体を強くするための方法論（例）

- 異分野（心理学や安全工学だけでなく、脳科学、政治学や社会学などの社会科学、文化人類学など）と連携したアプローチの検討
  - 予測困難な変化に強い仕組とするため、人の生活や社会の許容度など多要素の知見を集積して全体として適切なシステムを構築



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

日本におけるサイバーセキュリティの研究
（CSS-2018を例にとり）

基盤系の研究開発（１）

- 2A1: 個人認証 （座長：大木　哲史）
  - 2A1-1: 覗き見耐性を持つマウス操作と数字盤を組み合わせた個人認証方式の提案と評価
  - 2A1-2: スマートフォンとウェアラブル端末の加速度センサを用いたスマートロックにおける歩行認証
  - 2A1-3: DPA対策マスクの変換アルゴリズムの改良と認証方式への適用
  - 2A1-4: ワンタイム図形生成に基づく特定の認証キーのない認証手法
- 2A2: 暗号解析・安全性評価（１） （座長：白勢　政明）
  - 2A2-1: 軽量ブロック暗号PiccoloのMILP手法を用いたDivision Propertyの検証
  - 2A2-2: Type-1一般化Feistel暗号に対する量子識別攻撃の改良
  - 2A2-3: Sliding window法からの漏洩情報を用いた秘密鍵復元攻撃の改良
  - 2A2-4: A Continuous Genetic Algorithm for Optimizing Pruning Function for Lattice Enumeration
- 2A3: 暗号解析・安全性評価（２） （座長：安田　貴徳）
  - 2A3-1: KSS曲線を用いた効率的なペアリング暗号のための18次拡大体構成法の評価
  - 2A3-2: Estimating Secure Parameters for the Multivariate Encryption Scheme EFCp-
  - 2A3-3: Tame Automorphism Decomposition Problemに関する一考察
  - 2A3-4: 有限体上楕円曲線の新しい演算に基づくDLPとECDLPの関係
  - 2A3-5: 奇標数体上で生成される幾何系列の自己相関
- 2D4: 秘密計算 （座長：吉浦　裕）
  - 2D4-1: マルチパーティ計算を利用した秘匿情報統合分析に対するゲーム理論の適用
  - 2D4-2: ラウンド効率のよい2者間秘匿計算とその秘匿畳み込みニューラルネットワークへの応用
  - 2D4-3: Towards Practical Secure Automatic Speech Recognition
  - 2D4-4: Oblivious RAMを利用したセキュアな決定木の実装評価
- 4A2: 秘匿計算 （座長：大畑　幸矢）
  - 4A2-1: 僕たちは一番大切なものに気づいていなかった-秘密外部結合プロトコルの設計と実装-
  - 4A2-2: 高精度かつ高効率な秘密ロジスティック回帰の設計と実装
  - 4A2-3: 準巡回シンドローム復号問題に基づく線形関数秘匿計算

基盤系の研究開発（２）

- 3A2: 高機能暗号（１）（座長：藤岡　淳）
  - 3A2-1: レベル2準同型暗号の平文バイナリ制約を与えるコンパクトな非対話ゼロ知識証明
  - 3A2-2: BundleされたWitness SpacesにΣプロトコルによるWitness-Indistinguishable ArgumentsとそのグローバルIDへの適用
  - 3A2-3: CBDH仮定に基づく効率的な閾値公開鍵暗号
- 3D2: プライバシー技術理論（座長：清　雄一）
  - 3D2-1: 二分決定図による複数の線形モデルの出力値公開の安全性評価と疾患リスク予測値公開への適用
  - 3D2-2: 攻撃者の条件を緩和した推薦システムに対するModel Inversion攻撃
  - 3D2-3: Locally Private Continual Countingにおける1-Shot Reportingメカニズムの有用性解析
  - 3D2-4: 集計表セル秘匿問題の拡張によるデータ効用保持の有効性評価
- 3A3: 高機能暗号（２）（座長：光成　滋生）
  - 3A3-1: 鍵更新機能付き検索可能暗号：効率化に向けた一工夫
  - 3A3-2: 並列処理かつ動的データに向けた検索可能暗号の改良
  - 3A3-3: Identity/Attribute-Based Signature Resilient to Hard-to-Invert Leakage under Standard Assumptions
  - 3A3-4: IDベース暗号の強秘匿匿名性について

応用系の研究(１)

- 1E3: クラウド・仮想化（座長：須賀　祐治）
  - 1E3-1: Intel SGXを利用するコンテナのマイグレーション機構
  - 1E3-2: OverlayFSを用いたコンテナに対するサービス妨害攻撃の防止
  - 1E3-3: キャッシュのモニタリングによるキャッシュサイドチャネル攻撃の検知
  - 1E3-4: JavaScriptを用いたスマートフォン向けFIDO UAF Cloudの提案と評価
- 1A4: Webセキュリティ（座長：齋藤　孝道）
  - 1A4-1: プッシュ通知を用いたパスワードマネージャの提案と評価
  - 1A4-2: WordPressプラグインで発生するCSRF脆弱性とSelf-XSS脆弱性の組み合わせによるXSS脆弱性
  - 1A4-3: アクセスパターンに基づく攻撃対象Webアプリケーション発見手法の提案
  - 1A4-4: Webサイトのセキュリティ・センサス
- 1A5: Androidセキュリティ（座長：孫　博）
  - 1A5-1: ソーシャルネットワークで共有されるAndroidアプリケーションの実態調査
  - 1A5-2: Androidにおけるランタイムパーミッションのクラス別適用手法
  - 1A5-3: Androidアプリケーションのコンポーネント間通信による脅威分析の効率化と高度化
  - 1A5-4: AndroidにおけるWebViewのWebアクセス観測機構を利用した悪性Webサイトの脅威分析と対策の提案
- 2E3: ユーザインタフェースが変えるセキュリティ（座長：五味　秀仁）
  - 2E3-1: 視覚障害者の暗証番号入力時におけるのぞき見防止方法の検討
  - 2E3-2: 言語圏ごとのパスワード生成・管理の傾向比較
  - 2E3-3: パスワード非開示によるパスワード強度測定方式
  - 2E3-4: スマートフォンにおける音声とタッチスクリーンから取得した耳介を用いた個人認証
- 3B3: ブロックチェーン（座長：長谷川　佳祐）
  - 3B3-1: ブロックチェーンを用いた認証・認可システムの設計と実装
  - 3B3-2: プライバシーを考慮したブロックチェーンの取引者間事前合意プロトコル
  - 3B3-3: ブロックチェーンを利用したセキュアな分散処理を実現するフレームワークの提案
  - 3B3-4: Ethereumブロックチェーン上に潜むマルウェアなどの定量的リスク分析
  - 3B3-5: 暗号通貨（ビットコイン）・ブロックチェーンの高信頼化へ向けてのMELT-UP活動（II）-運用と倫理-

応用系の研究(２)

- 4B2: IoTセキュリティ（座長：磯原　隆将）
  - 4B2-1: クロスデバイストラッキング技術に関する調査：2018年版
  - 4B2-2: クロスアプリケーションフィンガープリンティング-同一端末上のアプリケーション間の紐付け-
- 4B1: 自動車セキュリティ（座長：吉田　琢也）
  - 4B1-1: CANのイベントメッセージに対する侵入検知手法の提案
  - 4B1-2: CAN通信における汎用的な攻撃検出を目的とした時系列データ解析
  - 4B1-3: 車載インフォテインメントシステムにおけるホワイトリストと遅延付加によるCANバス上のDoS攻撃緩和手法
- 4C1: Drive-by-Download攻撃（座長：羽田　大樹）
  - 4C1-1: Drive-by-Download攻撃時の通信データの関連性分析
  - 4C1-2: ドメインを用いないWebアクセスに着目した悪性サイト検知手法の提案
  - 4C1-3: ソースコードの類似度に基づく悪性JavaScriptの検知
  - 4C1-4: ユーザ環境観測によるRIG Exploit Kitの長期観測と時間変化に対して頑強な攻撃検知

侵入、マルウェア分析系の研究(１)

- 1B5: データセット （座長：大野　一広）
  - 1B5-1: 研究用データセット「動的活動観測2018」
  - 1B5-2: マルウェアデータセットに関する調査
  - 1B5-3: ネットワーク型侵入検知システム評価用セッション型データセットに関する一考察
  - 1B5-4: 【ディスカッション】MWSデータセットの提供者，利用者にこれだけは言っておきたい！
- 2B3: ログ分析・侵入検知 （座長：橋本　正樹）
  - 2B3-1: リモート型シェルコードのエミュレーションによる攻撃成否判定手法
  - 2B3-2: 行動表現文法*ELL*を用いた攻撃シナリオ再構築技術
  - 2B3-3: 不正侵入検知におけるセキュリティアラートのシグネチャ別発生量に着目した誤検知削減手法
  - 2B3-4: IoT機器に特化したアノマリ型侵入検知システムの提案
  - 2B3-5: 車載ネットワークCANにおけるバスオフカウンター攻撃の改善
- 2D3: 追跡技術と現実 （座長：小栗　秀暢）
  - 2D3-1: ライフスタイル認証におけるIPアドレス情報の利用について
  - 2D3-2: Webトラッキング技術に関する対策技術の検証及び考察
  - 2D3-3: 可視画像からの指静脈認証のなりすまし可能性の検討とその対策手法
  - 2D3-4: Androidアプリがサードパーティに送信する情報の調査: JDIを用いた動的解析機構
  - 2D3-5: JavaScriptによるクライアントPC操作の法律問題
- 2C4: 検知回避と誤検知 （座長：中津留 勇）
  - 2C4-1: アンチウイルスによる誤検知の調査と対策の提案
  - 2C4-2: 特定環境で動作するマルウェアへのセキュリティアプライアンスの耐性評価
  - 2C4-3: Windowsにおけるプロセッサレベルの特徴量に注目した亜種マルウェアの検知
  - 2C4-4: Linuxにおけるファイルレスマルウェア対策
- 3C2: 表層解析とプログラム解析 （座長：岩本　一樹）
  - 3C2-1: マルウェアによるRDTSC命令の利用方法についての分析
  - 3C2-2: シンボリック実行を利用したIOC変換
  - 3C2-3: シンボリック実行を活用したマルウェア解析環境検知機能の回避条件自動抽出の研究
  - 3C2-4: Concept DriftとScale-freeの性質を持つデータセットに対する検知の自動化手法

侵入、マルウェア分析系の研究(２)

- 3B1: マルウェア・ネットワーク分析 （座長：藤田　彬）
  - 3B1-1: 準パススルー型ハイパーバイザによるストレージアクセスパターンの収集システムの提案
  - 3B1-2: AlkanetにおけるMeltdown対策済Windowsのシステムコールトレース手法
  - 3B1-3: PTRレコードの連続的設定を加味した動的IPアドレスブロックおよびクラウド領域検出
  - 3B1-4: IoTマルウェアと通信可能な悪性サーバの探索
- 3C1: ダークネットとDDoS攻撃 （座長：牧田　大佑）
  - 3C1-1: 宛先アドレス順序とペイロードに着目したネットワーク走査活動の分析
  - 3C1-2: 宛先変化数を用いた協調型走査活動を行なうホスト群抽出手法の提案
  - 3C1-3: Darknet及びハニーポットの比較分析に基づくマルチベクタ型DDoS攻撃の検知方法の検討
  - 3C1-4: ユーザの行動履歴を考慮したDDoS攻撃加担対策手法の検討
- 3C3: 攻撃検知 （座長：瀧本　栄二）
  - 3C3-1: RISC-Vにおけるプロセッサ情報を用いた動的なアノマリ検知機構
  - 3C3-2: システムログ書式の構造に着目したシステム異常検出手法の検討
  - 3C3-3: 類似メールを利用したばらまき型メールの検出
  - 3C3-4: XSS攻撃検知のためのテストベースホワイトリスト自動生成手法に関する検討
- 4D2: サイバー攻撃 （座長：松中　隆志）
  - 4D2-1: サイバー攻撃観測用センサーの静的特性に関する考察
  - 4D2-2: 長期間観測した通信データを用いたサイバー攻撃活動と推定されるプログラムの分類による攻撃者像の一考察
  - 4D2-3: 「サイバーセキュリティ能力成熟度モデル」を一部改良して使用した国レベルの能力測定の提案
  - 4D2-4: エコシステムで構成するサイバー攻撃と防御演習システムCyExecの提案
- 3B4: 動的解析 （座長：折田　彰）
  - 3B4-1: MITB攻撃においてコンテンツ改ざんを行う不正JavaScriptの解析手法
  - 3B4-2: スクリプト実行環境に対する解析機能の自動付与手法
  - 3B4-3: 動的解析においてログが取得できないマルウェアの実態調査
  - 3B4-4: 動的な関数アドレス解決APIの呼び出しログを用いたマルウェア分類
- 4D1: 攻撃分析 （座長：白石　善明）
  - 4D1-1: サイバー攻撃に対する能動的観測による収集データのモデル化と正規化手法
  - 4D1-2: 標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の改良
  - 4D1-3: On Automation and Orchestration of an Initial Computer Security Incident Response Using Centralized Incident Tracking System
  - 4D1-4: マルウェアによる感染活動の目的推定に向けた動的解析ログに基づく分析

ネットワーク系の研究

- 2C1: 悪性ドメイン名 （座長：岡田　雅之）
  - 2C1-1: Combosquattingドメインネームの生成モデルとその評価
  - 2C1-2: OCRを利用したホモグラフIDNの検知法
  - 2C1-3: Active LearningとEnsemble Learningを用いた悪性ドメイン名検知システム
  - 2C1-4: IDNホモグラフ攻撃の大規模実態調査：傾向と対策
- 2B2: ネットワークセキュリティ （座長：森　達哉）
  - 2B2-1: Torネットワークへの攻撃に対するサーバ発ランダム画像挿入による防御手法の検討
  - 2B2-2: 画像分類を用いるIoT マルウェアの検知手法についての提案
  - 2B2-3: Rig Exploit Kitを利用したDrive by Download攻撃における分類評価
  - 2B2-4: アグリゲート署名を用いたBGPsec AS_PATH検証手法の提案と実装評価
- 3C4: 通信データ分析 （座長：小出　駿）
  - 3C4-1: ペイロードの特徴量に注目した未知のネットワーク異常検出
  - 3C4-2: マルウェアの通信特徴に基づくSSL/TLSを利用したC&C通信検出手法
  - 3C4-3: Cutwail通信プロトコルの解析

機械学習系の研究

- 2C2: 機械学習（1）（座長：市野　将嗣）
  - 2C2-1: DCGANを用いたネットワークトラフィックの異常検出
  - 2C2-2: Adversarial trainingを用いた未知ファミリ検知手法
  - 2C2-3: マルウェア感染端末の分類精度改善に向けたラベルなしネットワークログの活用法
  - 2C2-4: 侵入検知モデル構築における能動学習と無作為選択を用いたラベリングコスト削減手法の検討
- 2C3: 自然言語処理の活用（座長：芦野　佑樹）
  - 2C3-1: 出現頻度の高い可読文字列を用いた未知のマルウェアの検知手法
  - 2C3-2: 異常検知器を用いた未知の悪性マクロの検知手法
  - 2C3-3: 静的データに基づくマルウェア検知に適した特徴空間の分析
  - 2C3-4: fastTextを用いたマルウェア亜種判別
  - 2C3-5: 話題誘導するトピックモデルを用いたセキュリティレポート分類
- 4C2: 機械学習（2）（座長：嶋田　創）
  - 4C2-1: コード断片からのコンパイラ推定手法
  - 4C2-2: API呼び出しとそれに伴う経過時間とシステム負荷を用いた重み付けスコアに基づくマルウェア検知手法
  - 4C2-3: ヘッダ情報解析と深層学習手法を用いた電子メールによるゼロディ攻撃検出に関する研究
  - 4C2-4: 機械学習を用いたマルウェア検出システムの提案
- 2B1: 敵対的学習（座長：高橋　健志）
  - 2B1-1: 機械学習システムの脆弱性と対応策にかかる研究動向について
  - 2B1-2: 画像分類深層学習器に対するModel Extraction 攻撃の検証
  - 2B1-3: 深層学習における高い非認識性を持つ電子透かしの疎構造に対する埋め込み
  - 2B1-4: 実世界でも攻撃可能なAudio Adversarial Example

その他(１)

- 1A3: 認証・個人識別（座長：毛利　公一）
  - 1A3-1: 歩容データのDTW距離に基づく個人識別における複数部位のフュージョン手法
  - 1A3-2: 体臭によるプライバシーの侵害度合いの調査
  - 1A3-3: 超音波の分離放射による音声認識機器への攻撃:ユーザスタディ評価と対策技術の提案
  - 1A3-4: 車載ネットワークセキュリティ演習プログラムの報告
- 1E4: 情報基盤（座長：渡邊　裕治）
  - 1E4-1: 未知語を考慮した固有表現認識によるセキュリティインテリジェンスの構造化手法
  - 1E4-2: Generating Security Intelligence through Social Network Sentiment Analysis
  - 1E4-3: STIX2.0/TAXII2.0を用いたインディケータの自動収集と攻撃検知の自動化
  - 1E4-4: 脅威情報の共有に向けたグラフ記述のための軽量マークアップ言語の提案
- 2A4: 暗号実装評価（座長：国井　裕樹）
  - 2A4-1: システムを改変しない攻撃者とOS機能を信頼の基点とする暗号処理の安全性に関する一考察
  - 2A4-2: 実環境を想定したWPA2に対するKRACKsの評価実験
  - 2A4-3: IoT機器への適用に向けたTLS1.3の性能評価
- 3A1: 暗号構成手法（座長：松崎　なつめ）
  - 3A1-1: マンハッタン距離を用いた幾何学的グループ鍵共有法に関する検討
  - 3A1-2: 相関のある情報を用いたMultiple Access Wiretap Channelにおける秘匿通信について
  - 3A1-3: 深層学習の分類によるステガノグラフィの方法
- 3D3: 加工（座長：井口　誠）
  - 3D3-1: 特許出願からみた匿名化関連技術の技術動向ー平成29年度特許出願技術動向調査よりー
  - 3D3-2: 属性推定攻撃を抑止可能なプログラム送付型匿名化方式の提案
  - 3D3-3: 自己情報コントロールと権限分散を両立するパーソナルデータ流通方式の提案
  - 3D3-4: 匿名データの安全性指標としての再識別率とその活用方式の提案
  - 3D3-5: PWS Cup 2018: 匿名加工再識別コンテストの設計～履歴データの一般化・再識別～

その他（２）

- 2E4: ソーシャルエンジニアリングとインテリジェンス（座長：宮本　大輔）
  - 2E4-1: 仏教の視点から考えるソーシャルエンジニアリング対策（その1）
  - 2E4-2: OSINTと人間の心理を利用した標的型メール攻撃に対するインテリジェンスを活用した防御に関する基礎検討
  - 2E4-3: インテリジェンスを利用する標的型メールと標的型メールに対するインテリジェンスを利用した防御に関する検討
- 3E3: OWS：OSSセキュリティ（座長：面　和毅）
  - 3E3-1: TrustZone Technologyを利用したアクセス制御ポリシーの保護手法
  - 3E3-2: TOMOYO Linuxによる強制アクセス制御効果の可視化
  - 3E3-3: ログ出力の抑制によるSELinuxの不要なポリシ削減手法
  - 3E3-4: 権限昇格攻撃防止手法における権限の格納位置のランダム化
  - 3E3-5: 独自のカーネル用仮想記憶空間を用いたカーネルモジュール監視手法
- 3A4: 偽造防止技術（座長：宇根　正志）
  - 3A4-1: マルチモーダル人工物メトリクスのための機能性材料の開発（色相と発光強度の違いをもたらすアップコンバージョンガラス蛍光体）
  - 3A4-2: 偽装QRコードの構成とその効果，およびその対策について
  - 3A4-3: SeQR: ショルダーハック耐性を持つQRコード生成方法
  - 3A4-4: バーコードの多段二重符号化による情報付加と偽造防止
- 3E4: 実行監視・脆弱性分析（座長：山内　利宏）
  - 3E4-1: ヒープ領域に対するソースコード不要のIntel MPX命令適用手法
  - 3E4-2: プロセス内処理に対する遠隔認証手法の提案と実装
  - 3E4-3: TEE搭載デバイスにおける閲覧画面の偽装検出技術の提案
  - 3E4-4: Linuxディストリビューション間でのELFバイナリにおけるセキュリティ対策機構の適用状況の比較
- 4A1: 物理・視覚化暗号（座長：小川　一人）
  - 4A1-1: 不可視インクを用いた効率的なカードベース暗号プロトコル
  - 4A1-2: プレゼント交換に適したシンプルなカードベース置換生成
  - 4A1-3: 情報セキュリティアンプラグド～計算機を用いない情報セキュリティ教育～
  - 4A1-4: メッセージングアプリの普及に基づく簡単で公平なコイントス
- 4E1: リスク分析・プライバシー（座長：高橋　雄志）
  - 4E1-1: 矛盾-無関心を考慮したトラスト値の遷移について
  - 4E1-2: 業務プロセスの信頼性の改善手法
  - 4E1-3: テレワークにおけるプライバシーの課題に関する調査
  - 4E1-4: 海事サイバーセキュリティの現状と課題

その他(３)

- 2E1: 利用者を知り，セキュリティを造る（座長：金岡　晃）
  - 2E1-1: 小学校高学年を対象としたSNS教育ゲームの開発
  - 2E1-2: 警備システムの構築と顧客の合意形成を支援するシステムの研究
  - 2E1-3: 環境情報を用いた脆弱性検出のチャットボット
  - 2E1-4: 「かわいい」はセキュリティ警告の効果を改善しうるか？（第２報）～心理効果による安全行動誘引の試み～
- 2E2: セキュリティ技術の普及に向けて（座長：坂本一仁）
  - 2E2-1: セキュアなUIの実現を目指して?USBモデルの提唱?
  - 2E2-2: 経営マネジメント状況による情報漏洩インシデント削減効果の評価(2)
  - 2E2-3: 開発者向けユーザブルセキュリティ・プライバシー研究の現状調査

海外の動向（NISC資料を参照）

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

1）サイバーフィジカルシステム、IoT
2）クラウド
3）高性能計算
4）自立システム
5）モバイル機器

✓ NIST, NS…連携しながら研究開発を推進。201…

	D…			pt（適用）
短期	・ ・			撃が発生しても、重要な資産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)

○　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。

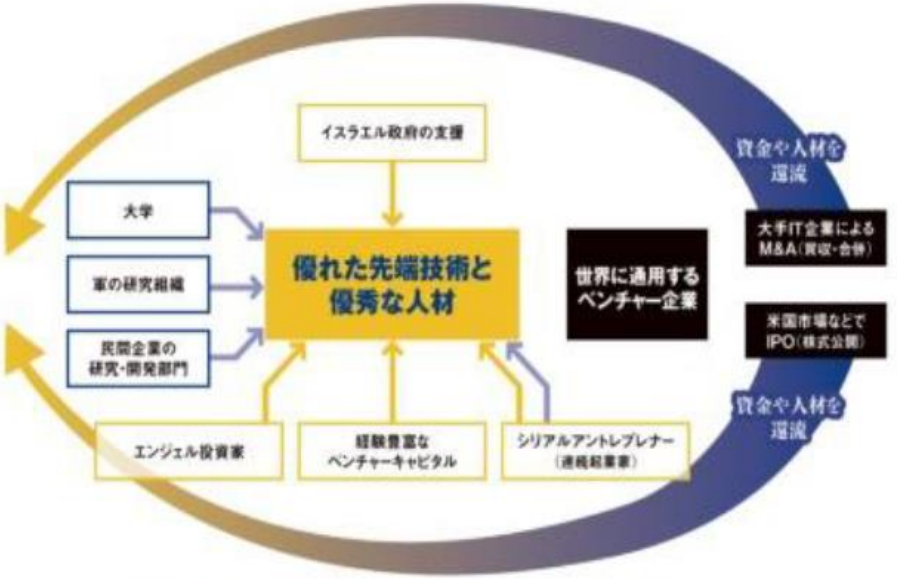
1）暗号・鍵管理、プロトコル
2）情報リスクマネジメント
3）システムエンジニアリング
4）情報保証の方法論
5）運用保証技術
6）戦略技術と製品の安全性の研究
7）サイバーセキュリティ人的要因の科学
8）高信頼性システムの構築

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。



（出典）：日経XTECH イスラエルのエコシステム、破壊的ベンチャー生み出す
https://tech.nikkeibp.co.jp/it/atcl/column/14/092900078/093000001/

✓ 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。

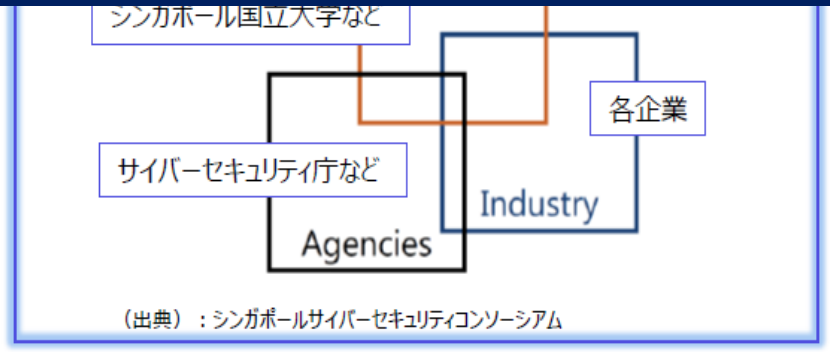
参考4:シンガポールの国立サイバーセキュリティ研究開発プログラム

○ 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）

1）スケーラブルなTrustworthyシステム
2）レジリアントなシステム
3）効果的な攻撃状況の把握、攻撃アトリビューション
4）内部犯行対策
5）脅威検出、分析、対応（保護）
6）効果的、効率的なデジタルフォレンジック



（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

（例）日仏サイバーセキュリティ連携研究

研究連携項目：WG構成

- **WG1: <Formal Methods>**

Cryptographic Protocol Verification/Privacy by Formal Methods

- **WG2 <Cryptography>**

Lattice-based cryptography / Post-quantum cryptography

- **WG3 <Events and Malware Analysis >**

Events collection by sensor technologies and exchange for joint analysis of attack events with malware analysis

- **WG4 <System Security and IoT security>**

Countermeasure against Side Channel Attacks (using Polymorphic Code)

- **WG5 <Privacy>**

Technologies on Sanitization, Generalization and Data Mining for privacy preserving (to be applicable for specific applications)

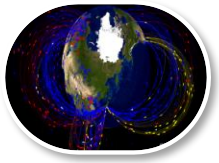
- **WG6 <ICS/ITS Security>**

Automotive Security, CIIP

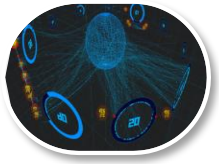
- **WG7 <Network, network security, measurement>**

Virtualization, SDN security, including measurement of security performance and effectiveness…　(including 5G security)

NICTサイバーセキュリティ研究室 研究マップ



インシデント分析センタ（ニクター）
NICTER



対サイバー攻撃アラートシステム（ダイダロス）
DAEDALUS

サイバー攻撃統合分析プラットフォーム（ニルヴァーナ・カイ）
NIRVANA改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）
NIRVANA改弐

受 Passive

Global(無差別型攻撃対策)

(標的型攻撃対策)Local

全

局

能 Active

From Security Big Data

To Security Intelligence

CURE
Cybersecurity Universal Repository

Dark net
Live net
DNS DB
Proxy Log
Honey pot
Amp Pot
IoT PoT
SPAM
Web Crawl
DBD
C&C URL
Mal ware (exe)
Mal ware (result)
Events
Alerts
Vulnera bility
Asset Info
News
Blogs

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

今後の展望（サイバーセキュリティのための課題）

1. 実時間での攻撃の把握／攻撃予兆の把握（早期に攻撃を理解）
   - 世界規模での攻撃観測連携基盤の構築 → 予兆分析に繋げる
2. 攻撃の複雑化、多様化、進化／変化に向けた挙動の高度分析（適切・迅速な対応へ）
   - 上記の観測攻撃データに基づくDL（Deep Learning）による深層解析技術
3. セキュリティ対策自動化（新ビジネス環境やネットワーク環境などに対応した）
   - 新たな環境における脅威分析の実施、そのためのセキュリティ対策の自動化の研究
4. 基盤的セキュリティ技術の見直し（量子計算機対応等）
   - 量子計算機、新世代NWなどの新たな環境に向けた基盤技術の見直し、新規研究
5. 重要インフラなどに対するTrust（Trustworthiness）の確保

   「安全・安心」の確保 → 「Trust（信頼）の確保」が喫緊の課題
   - 「Trust（信頼）の確保」のための総合的対策の導出、先端研究の促進、技術的検証を行うための体制整備
6. 安全・安心システムにおけるIoT活用、システム間の相互運用性確保
   - 応用の研究、相互運用性確保に向けた認証や脆弱性対策の推進

例えば、 ハニーポットと予兆分析

PRACTICE

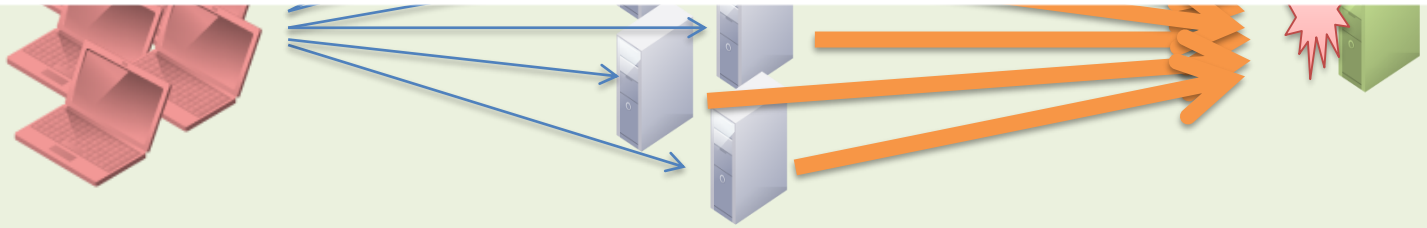
（総務省プロジェクトの一部）

DR-DoS 攻撃の早期検知

DRDoS 攻撃

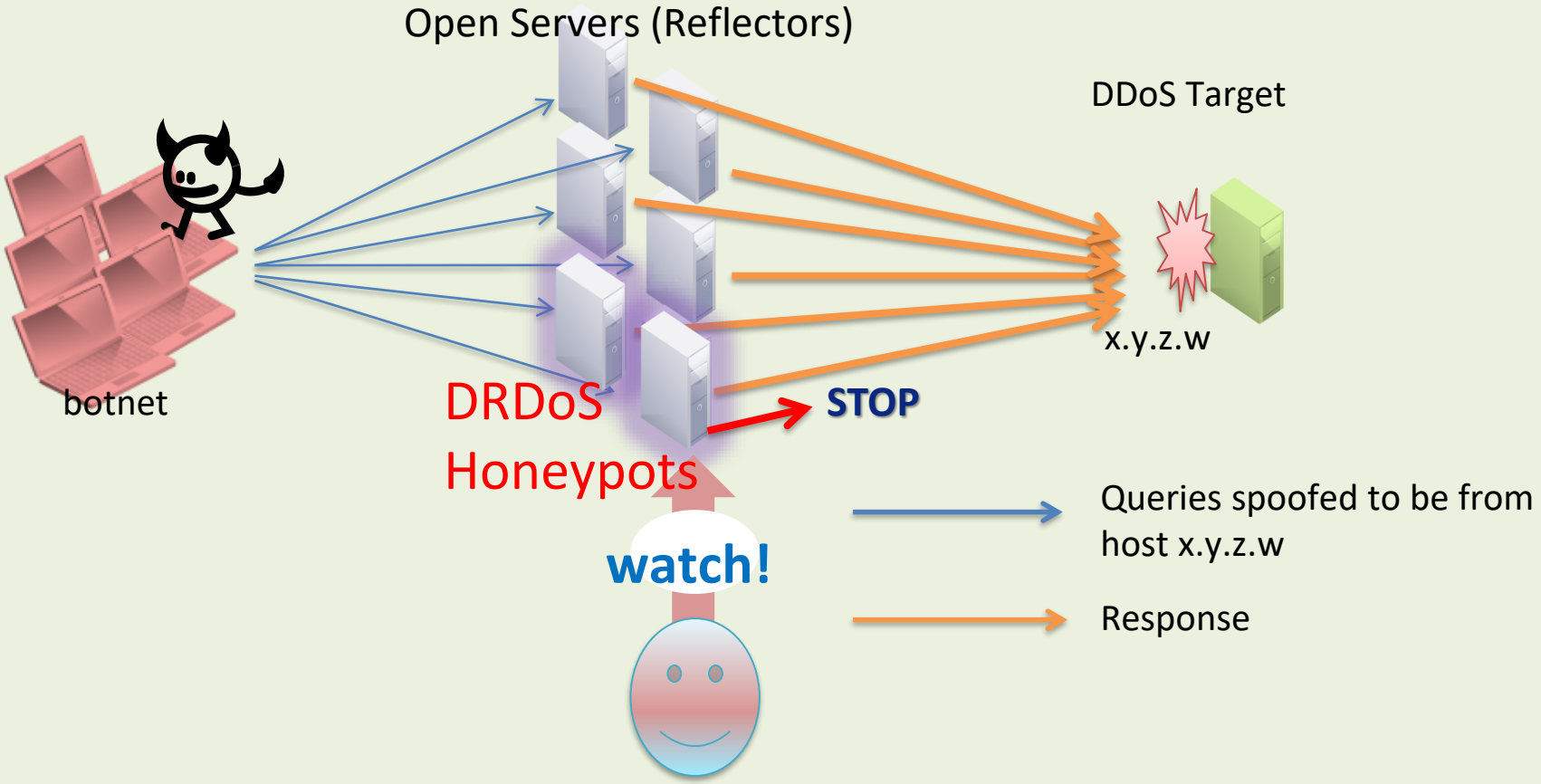
1. ボットがソースIPアドレスを標的システムへ詐称してリフ
2.
3.

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



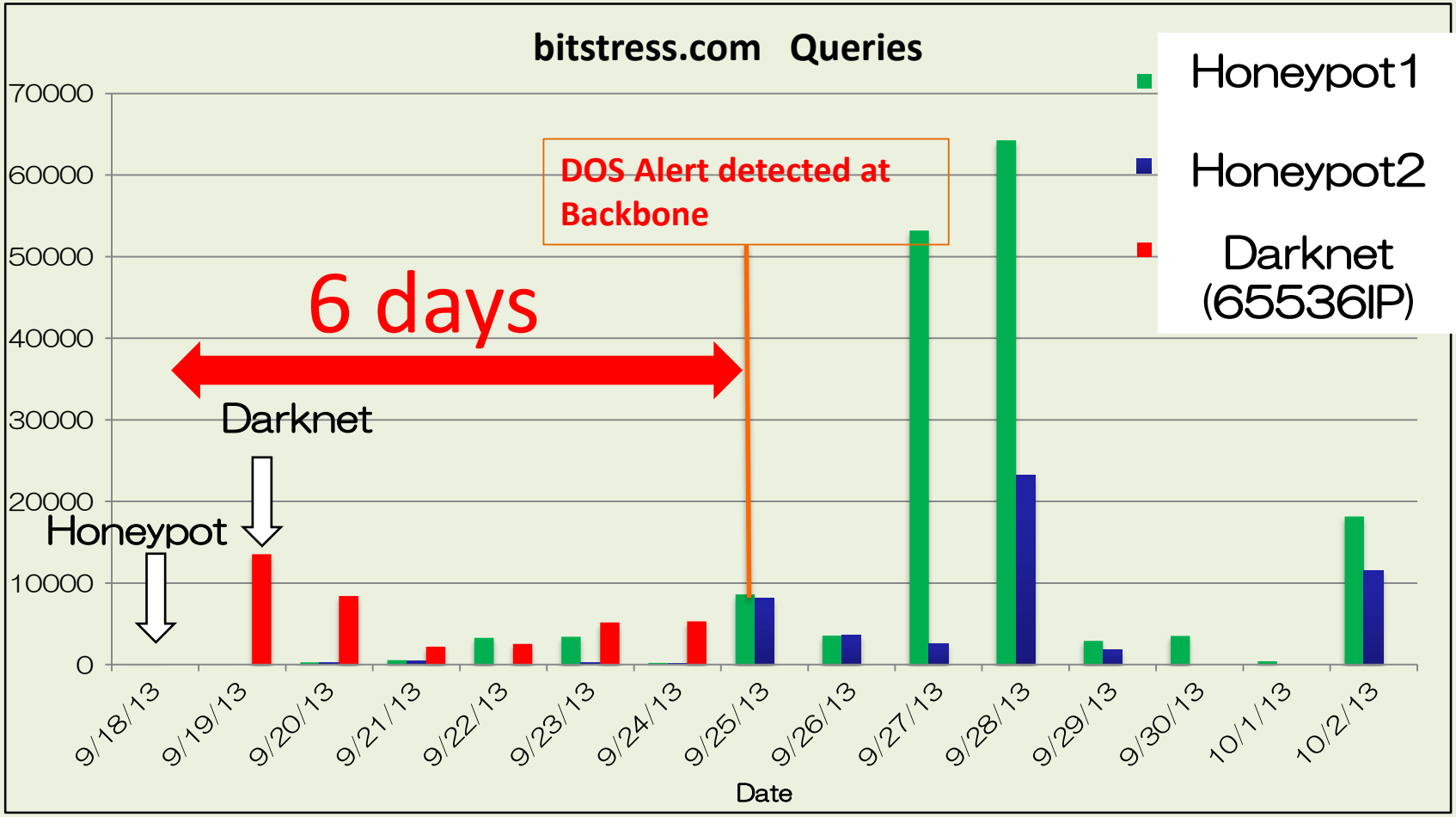
DR-DoS ハニーポット

PRACTICEプロジェクトでは、DR-DoSを検知するためのサーバー（ハニーポット）を設置した。（標的は攻撃しない）



早期のDRDoS攻撃の検知が可能

実際の大量はDoS攻撃の前に、不正なあるレベルの大量な攻撃を検知した。
攻撃者は、実際の攻撃の前に試験的にテスト攻撃をしたり、徐々に攻撃が増えていく傾向にある様子。



どの程度、事前に大量攻撃が検知できるか？

５０％以上のDNSを用いたDRDoS攻撃の場合は、平均２日以上前に、大量攻撃になることを検知している。

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%)

DR-DoS alert メールの活用

- DR-DoS alert sample (e-mail)

START of DR-DoS attack

[Target IP]
XXX.XXX.XXX.XXX

[Detection time]
2014-11-13 23:57:37

[Protocl]
DNS : port 53

[DRDoS Honeypot detail datea]
AS num : "AS2516 KDDI KDDI CORPORATION"
country : "Japan"
pps(MAX) : 2.2
pps(AVG) : 1.1416666666666666

[Domain]
"wradish.com ANY IN":137

END of DR-DoS attack

[Target IP]
XXX.XXX.XXX.XXX

[Detection time]
2014-11-13 23:57:37

[Protocol]
DNS : port 53

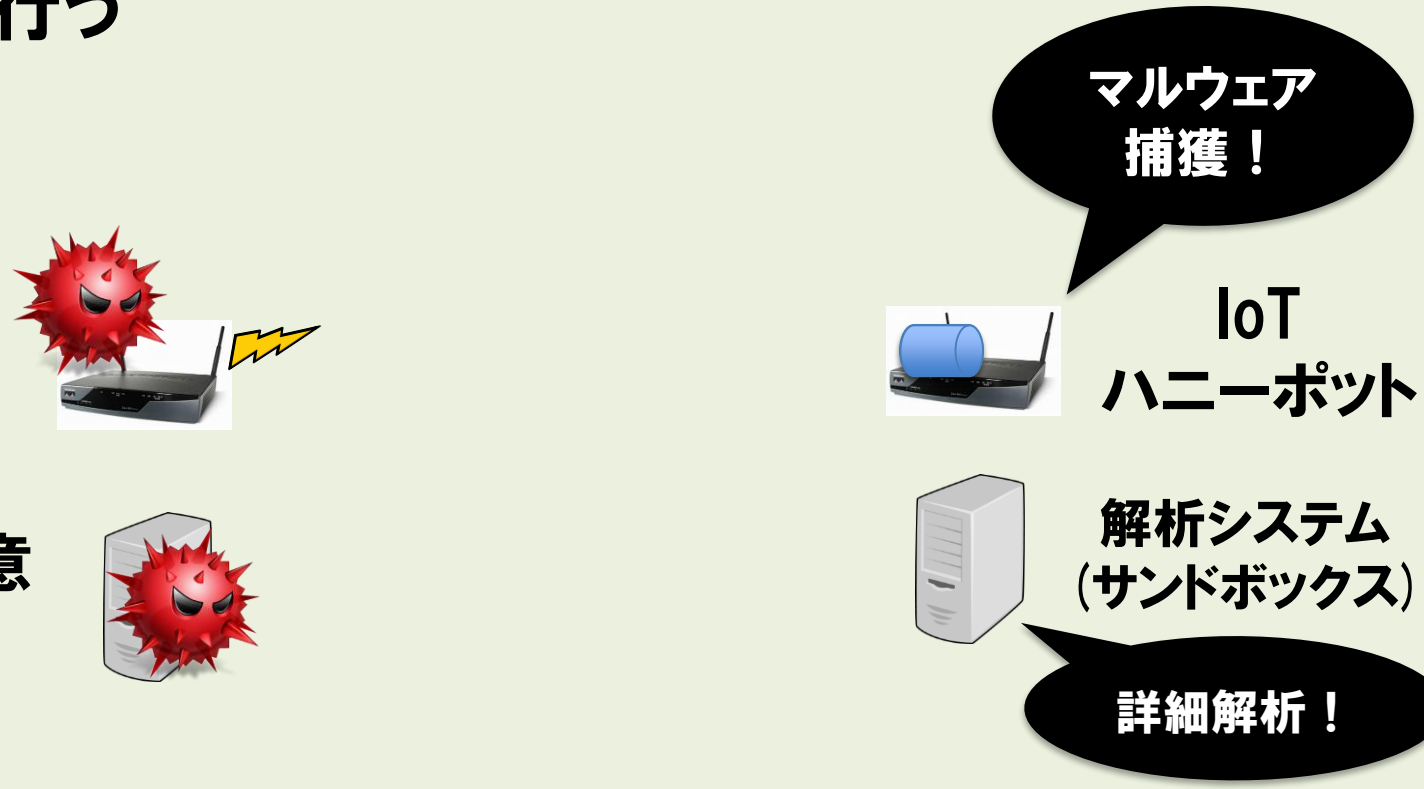
[DRDoS Honeypot detail data]
AS num : "AS2516 KDDI KDDI CORPORATION"
country : "Japan"
pps(MAX) : 2.2
pps(AVG) : 1.1416666666666666

[Domain]
"wradish.com ANY IN":137

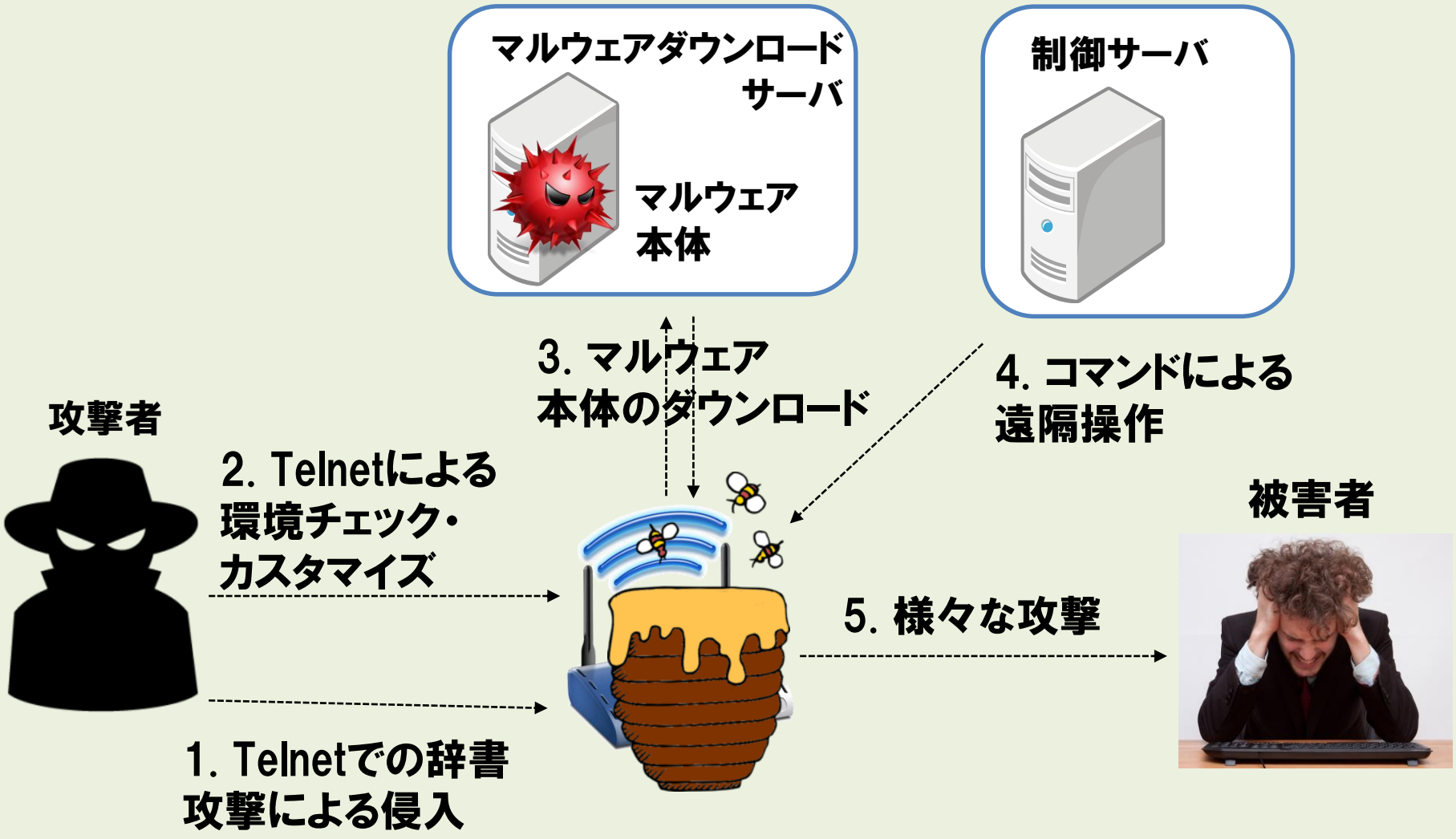
例えば、 IoTハニーポット/ダークネット

ハニーポットによる攻撃の観測とマルウェアの捕獲・詳細分析

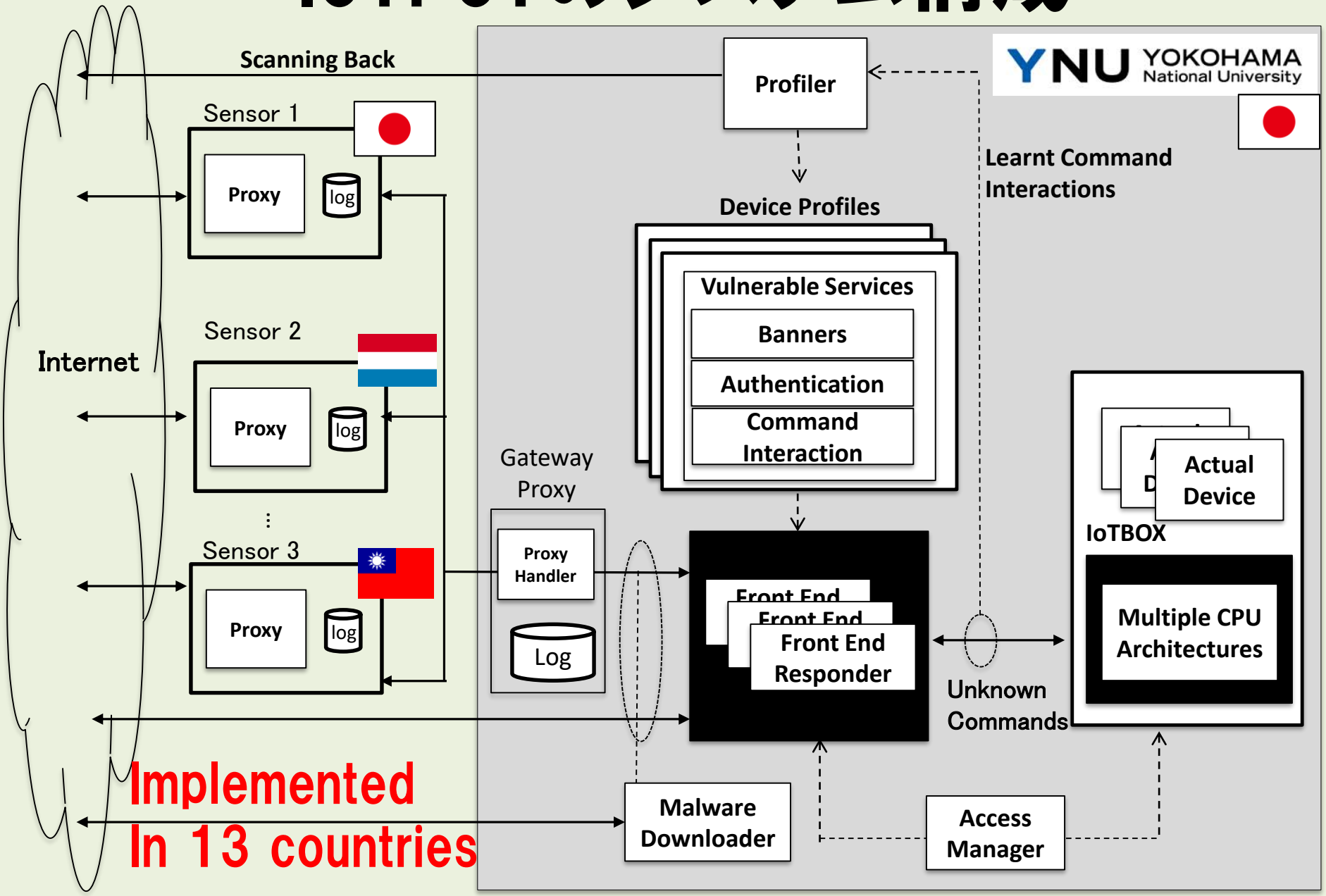
脆弱な機器を模擬した**囮システム（ハニーポット）**により攻撃元と通信を行い、攻撃の観測・マルウェア捕獲し、詳細解析を行う



Telnetベースのマルウェア感染の流れ

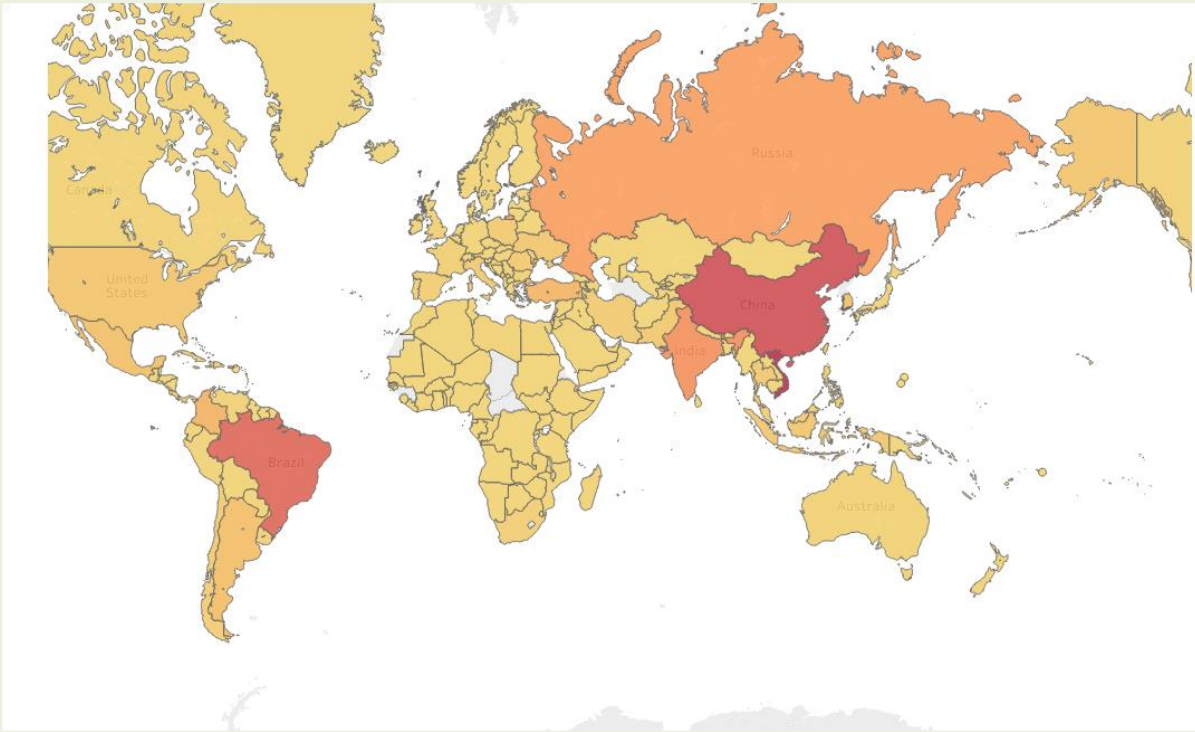


IoTPoTのシステム構成



世界的な感染状況

- 218カ国(または地域)からの観測
- 特に、アジア諸国からが多い



攻撃ホストはIoT 機器（横国調べ）

LED display control system

Solid Stage Recorder

Data Acquisition Server

Wireless Router

TV Receiver

GSM Router

IP Phone

Parking Management System

VoIP Telephony System

Fire Alarm

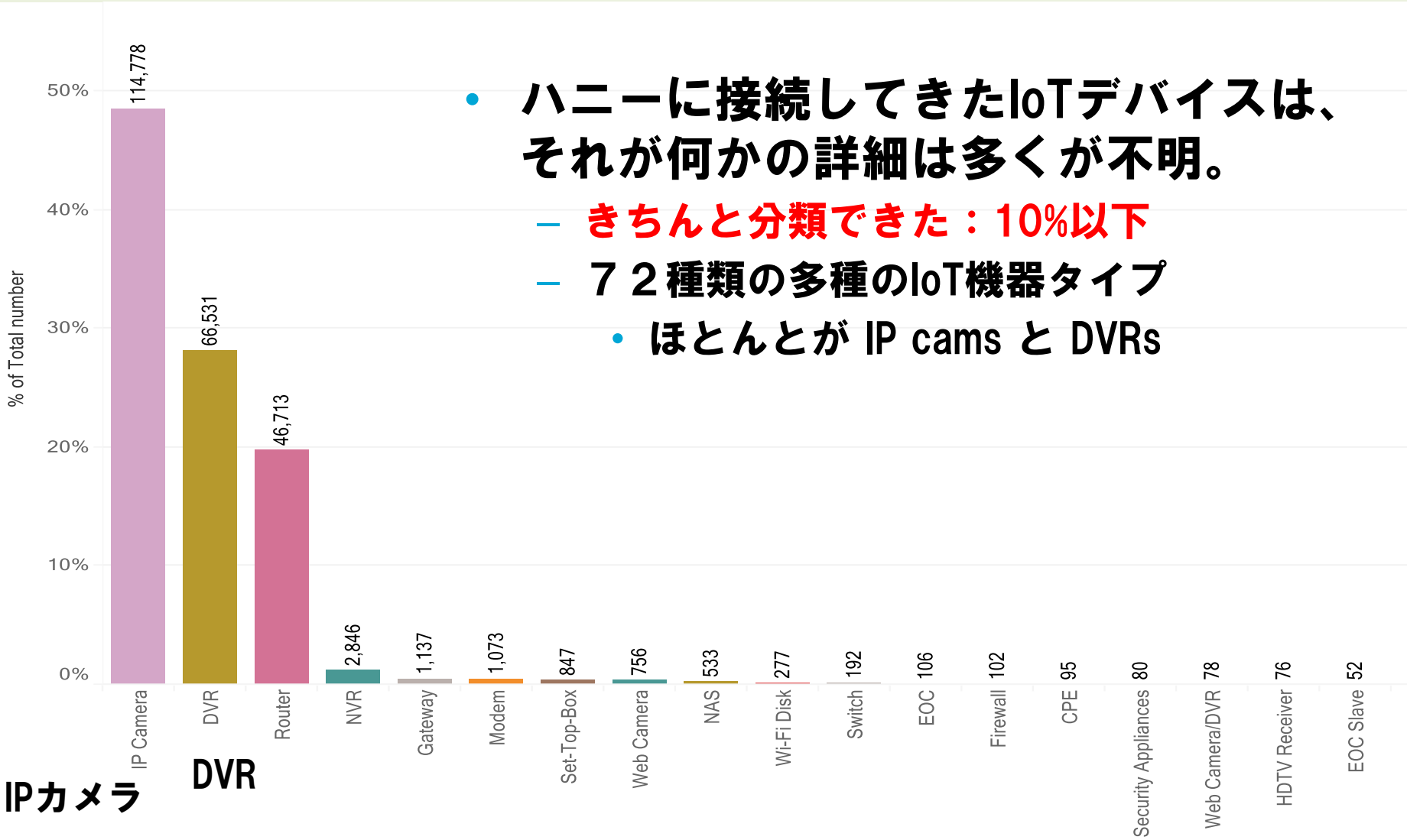
Security Appliance

Internet Communication Module

Video Broadcaster

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, “IoTPOT: Analysing the Rise of IoT Compromises,” 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015).

感染IoT機器の種別

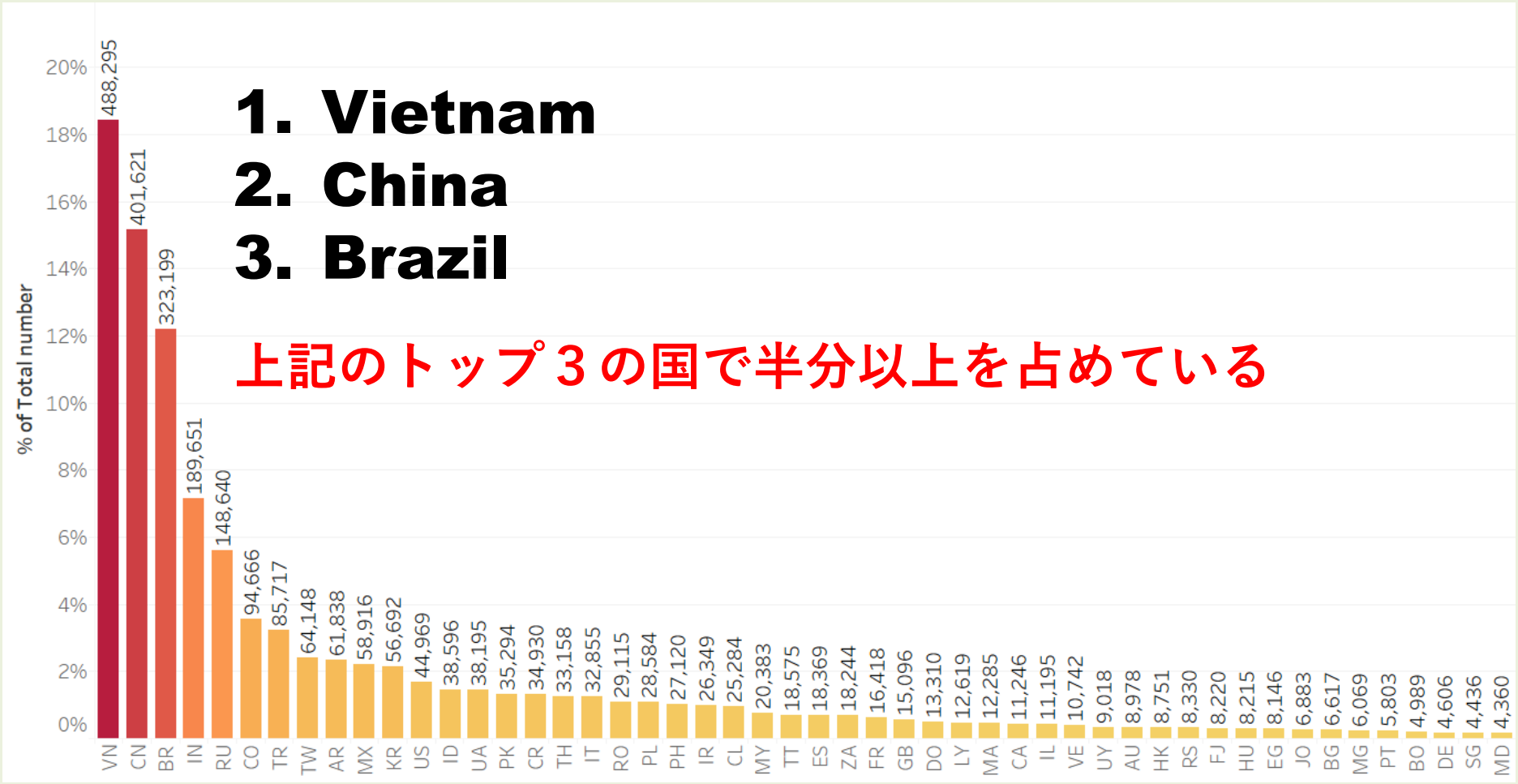


- ハニーに接続してきたIoTデバイスは、それが何かの詳細は多くが不明。
  - きちんと分類できた：10%以下
  - ７２種類の多種のIoT機器タイプ
    - ほとんとが IP cams と DVRs

IPカメラ

DVR

IPアドレス数の観点から、感染国の状況

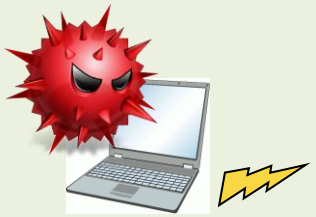


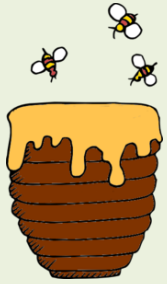
攻撃の観測のための2つのアプローチ

» （これまでの）受動（passive）型：
観測用ネットワークで攻撃が来るのを待つ
- ダークネットモニタリング
- ハニーポット

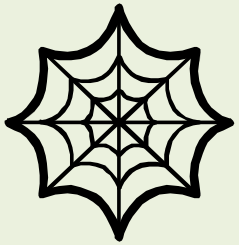
» 能動（active）型：
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

攻撃元機器の判定





ハニーポット

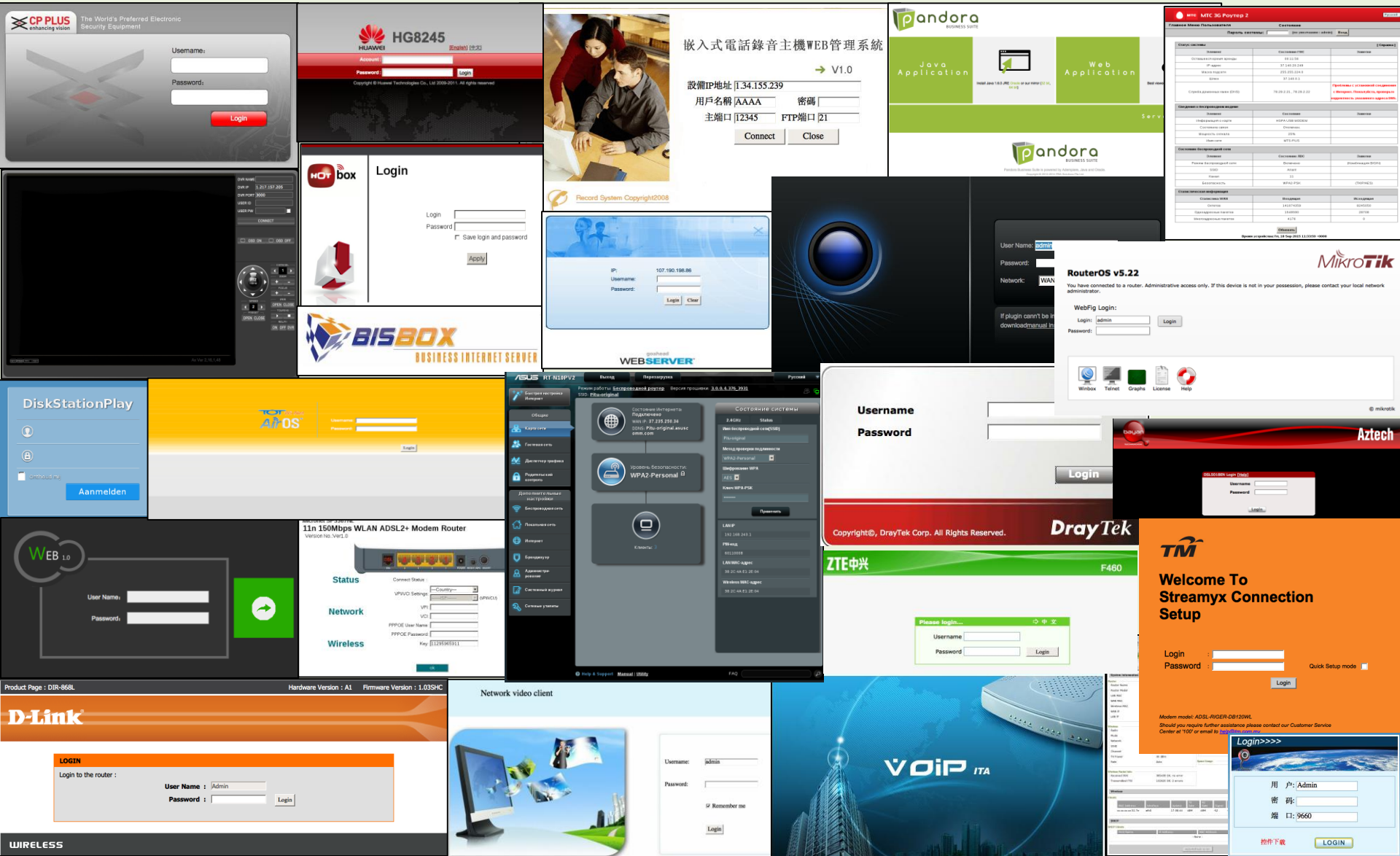


ダークネット

Web、Telnetサービスへの接続による機器判定

→IoT機器であることを確認

攻撃元(感染)機器のWebインターフェイスの例



感染機器の種別（事例）

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - 電話
  - アナログ電話アダプタ
- インフラ
  - 駐車管理システム
  - LEDディスプレイ制御システム








デバイスはWebおよびTelnetの応答から判断しています.

- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - セットトップボックス・アンテナ
- その他
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 医療機器（MRI）
  - 指紋スキャナ






国内メーカの機器の感染事例も複数確認

感染機器情報はJPCERT/CC，内閣サイバーセキュリティセンターに情報提供、または、メーカに直接情報提供を実施中

今後の展望（サイバーセキュリティのための課題）

1.
- 攻撃・攻撃予兆の把握のための研究開発

2.
- 攻撃挙動の高度分析のための研究開発
  - -AI等の活用

3.
- セキュリティ対策自動化のための研究開発
  - -AI等の活用

4.
- 暗号・認証などの基盤技術のための研究開発
  - -PQC等の研究も含む

5.
- Trustシステム構築（サプライチェーン等）のための研究開発

的検証を行うための体制整備

6.
- 今後のICT応用（IoT、ビックデータ、クラウド、5G、重要インフラ等）のためのセキュリティ研究開発

さらに

オフェンシブ　セキュリティ

- 攻撃者が有利な状況を打破するアプローチをしたい。「オフェンシブセキュリティ」(offensive security) は、攻撃者の視点に立ってセキュリティの問題を考えてみること。(我々が攻撃者に対してカウンターアタック(反撃)をしかけるということではない)。
- 攻撃者の考えや思考過程をシミュレートし、攻撃者にとって旨味のある方法は何か、それを実現するために必要な技術は何かを先回りして考えること。それを「セキュリティ・バイ・デザイン」(security by design) に生かす。

研究のためのセキュリティ情報の円滑・有効な共有

- 攻撃者の仲間は、多くの攻撃情報、対策情報などを共有そいている。少なくとも、セキュリティ研究開発では、データセットの共有化、解析結果の迅速な共有などを推進するべき。(e.g. Stardustの活用)
- 共有した(共有する)データの活用・利用の方法についても、円滑な共有化が必要。利用については、人間工学的な利活用についても研究を進めるべき。

セキュリティ人材育成の推進(体系的なアプローチ)

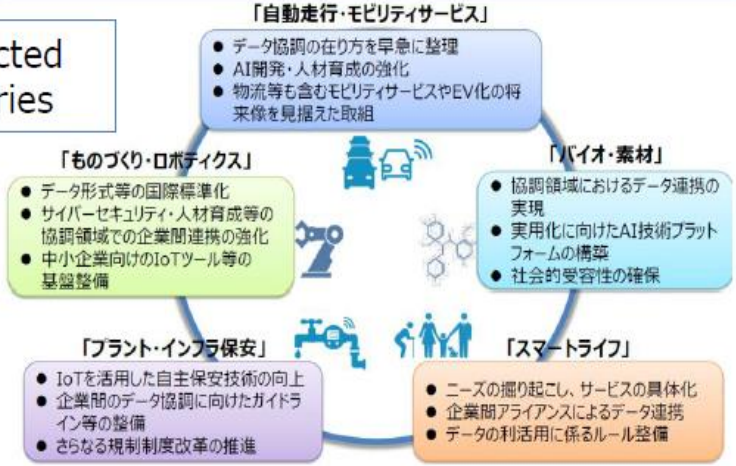
今後のICTの進展

- 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

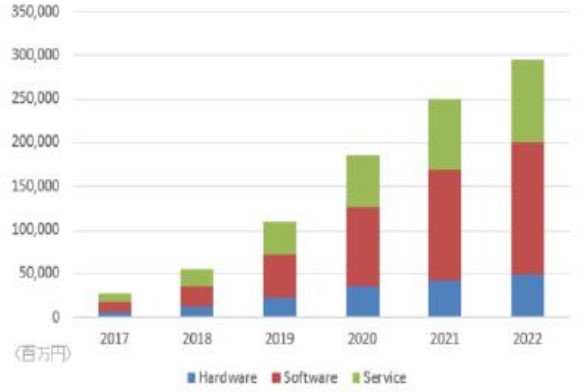
AIシステム市場 ユーザ支出額予測（セグメント別）

・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



(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」

Tokyo2020では、多様なIoT機器、クラウドを含めたバックエンドシステムの活用が期待（Super-Smart+Connected City）

Smart+Connected City Parking	Smart+Connected City Traffic	Smart+Connected City Safety & Security	Smart+Connected City Location Services	Smart+Connected City Lighting
				
Give citizens live parking availability information to reduce circling and congestion	Monitor and manage traffic incidents to reduce congestion and improve livability	Automatically detect security incidents, shorten response time, and analyze data to reduce crime	Provide view of people flow data to aid planning and leverage location data for contextual content and advertising	Manage street lighting to reduce energy and maintenance costs

今後、増えていく新しい脅威に立ち向かうため、多岐に渡る先進的、連携的な対策で対抗することが肝要

Thank you for your attention

Toward success of Tokyo 2020!!