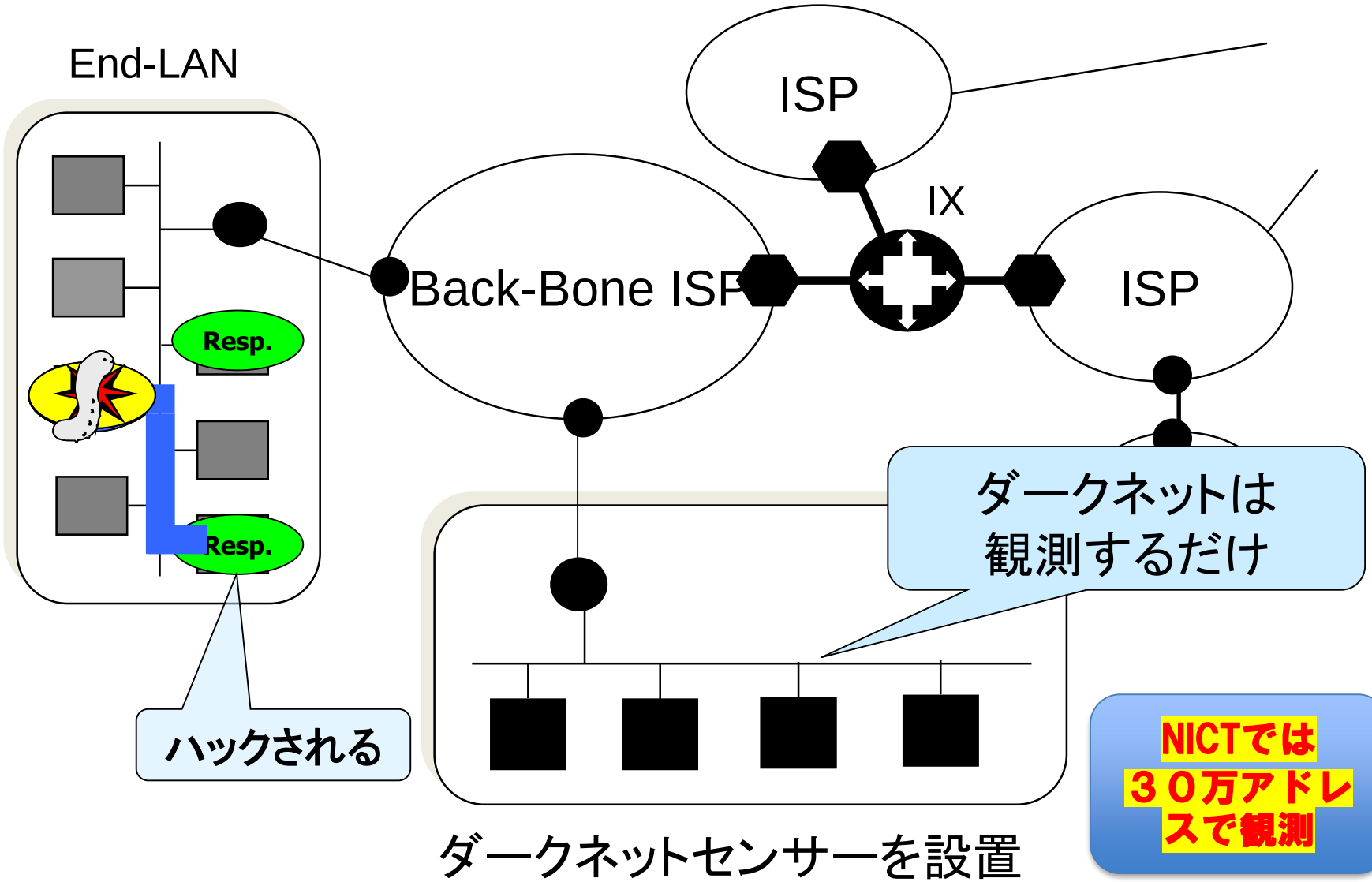
資料２

サイバーセキュリティ研究開発における今後の展望

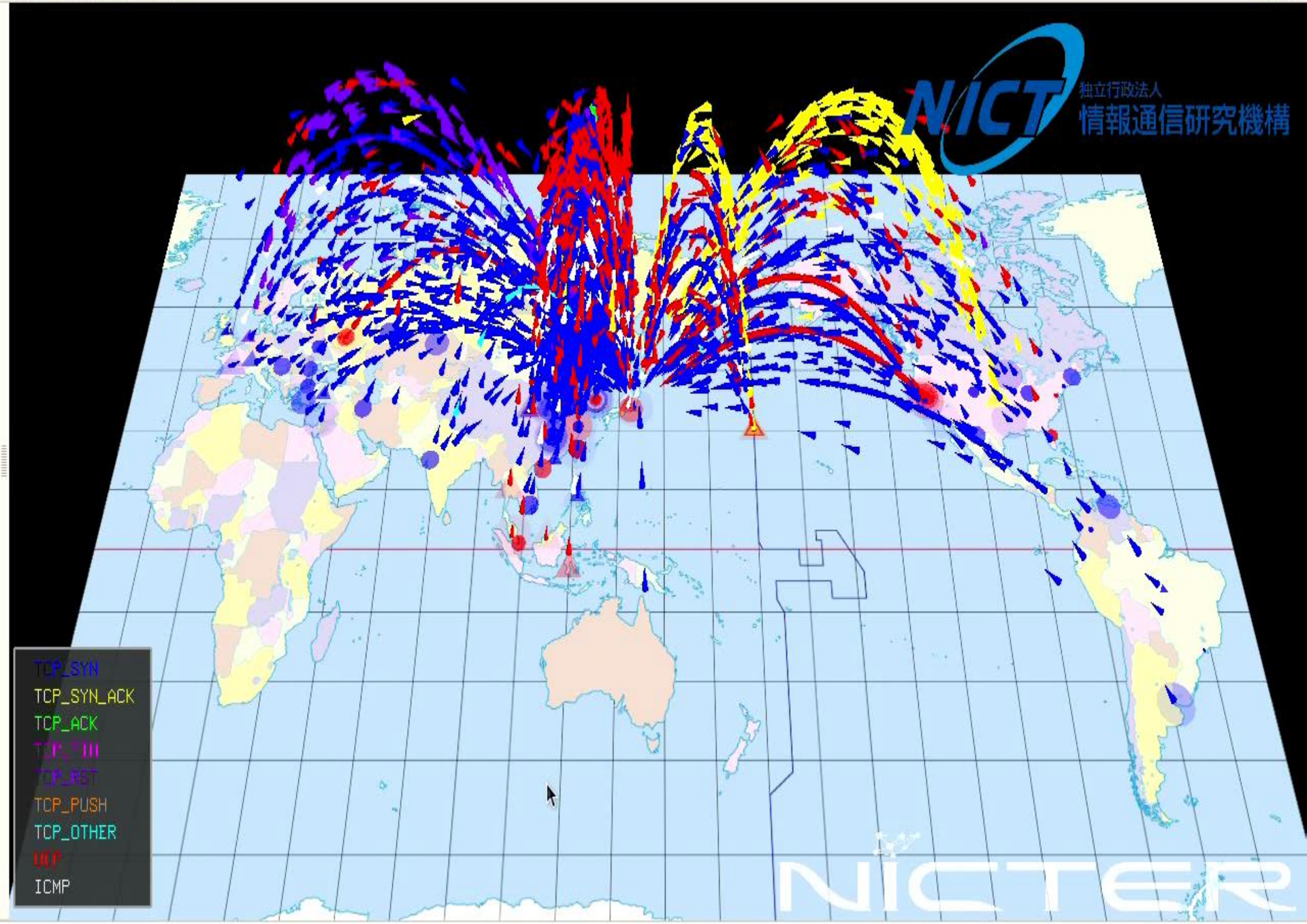
中尾康二

NICT サイバーセキュリティ研究所　主管研究員

ダークネットを用いてサイバー脅威の検証

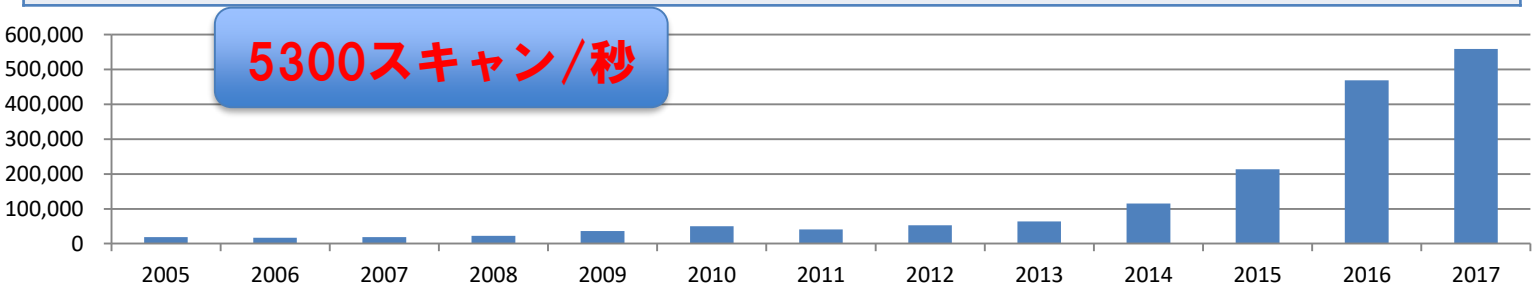


File(F) Settings(S) View(V) Help(H)



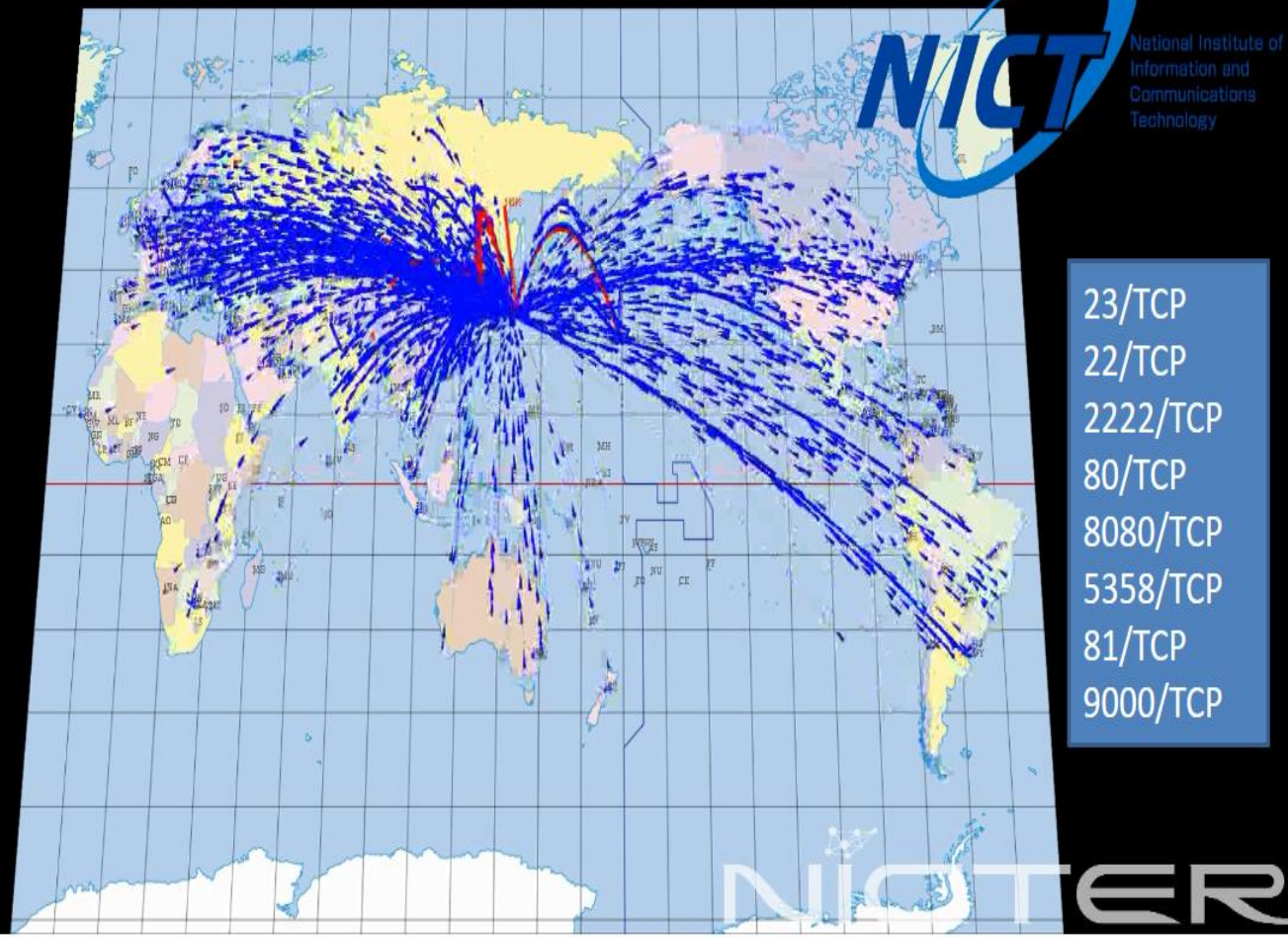
年毎のダークネット観測データの統計

Year	Number of packets par year	Number of IP address For darknet	Number of packets par 1 IP address per year
2005	0.31 billion	16 thousands	19,066
2006	0.81 billion	100 thousands	17,231
2007	1.99 billion	100 thousands	19,118
2008	2.29 billion	120 thousands	22,710
2009	3.57 billion	120 thousands	36,190
2010	5.65 billion	120 thousands	50,128
2011	4.54 billion	120 thousands	40,654
2012	7.79 billion	190 thousands	53,085
2013	12.9 billion	210 thousands	63,655
2014	25.7 billion	240 thousands	115,323
2015	54.5 billion	280 thousands	213,523
2016	128 billion	300 thousands	469,104
2017	**150 billion**	300 thousands	**559,125**

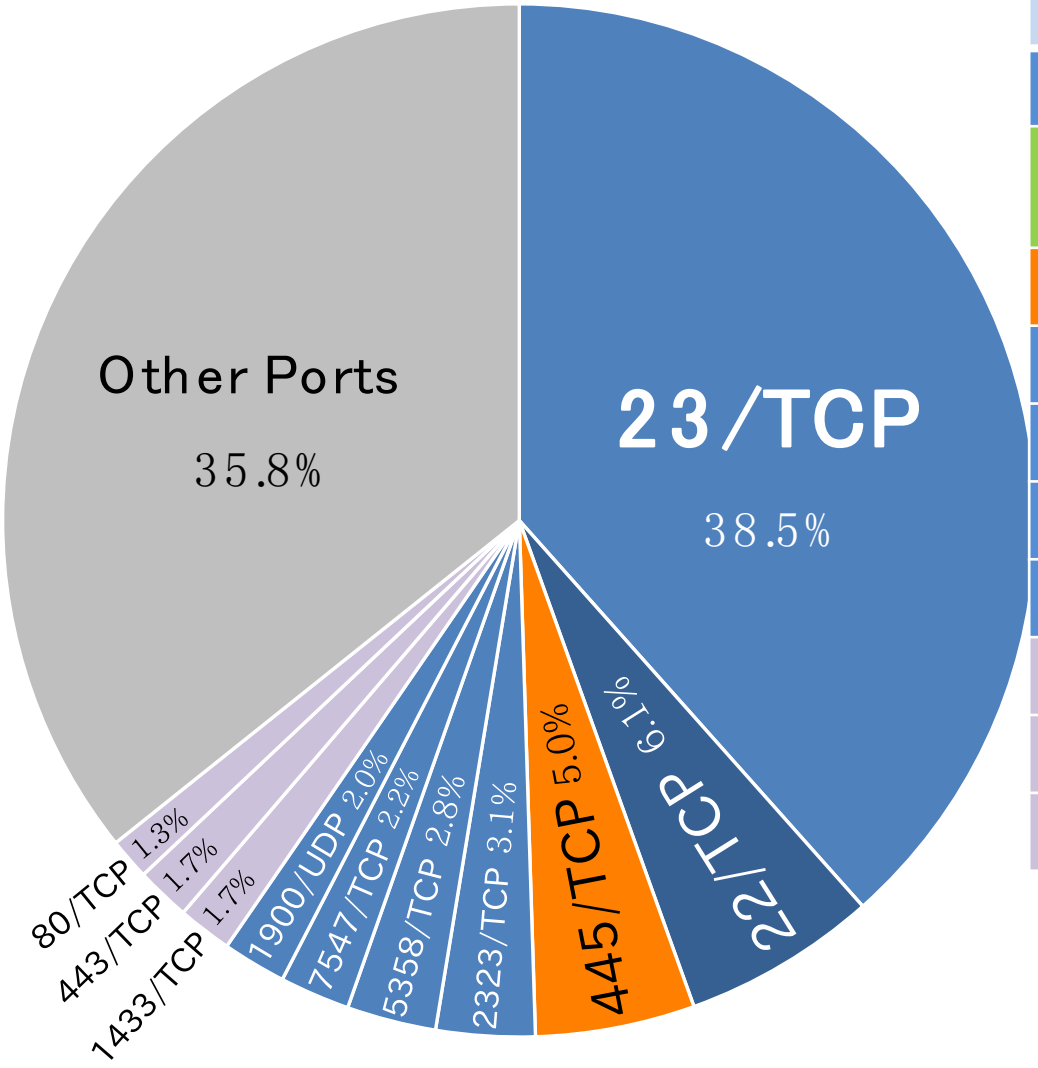


Number of packets par 1 IP address per year

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）



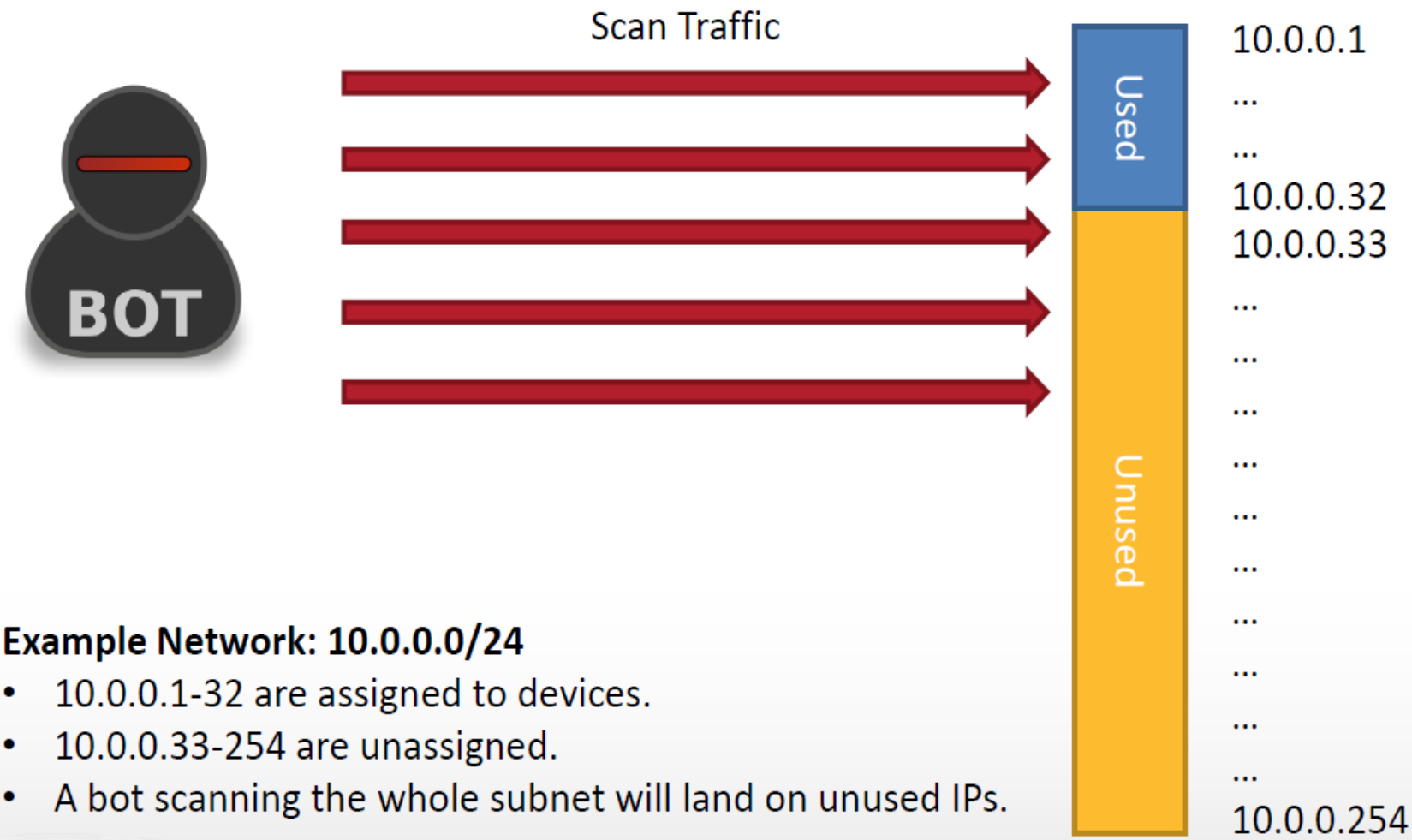
スキャン攻撃で使われているポートの分散（2017年）



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

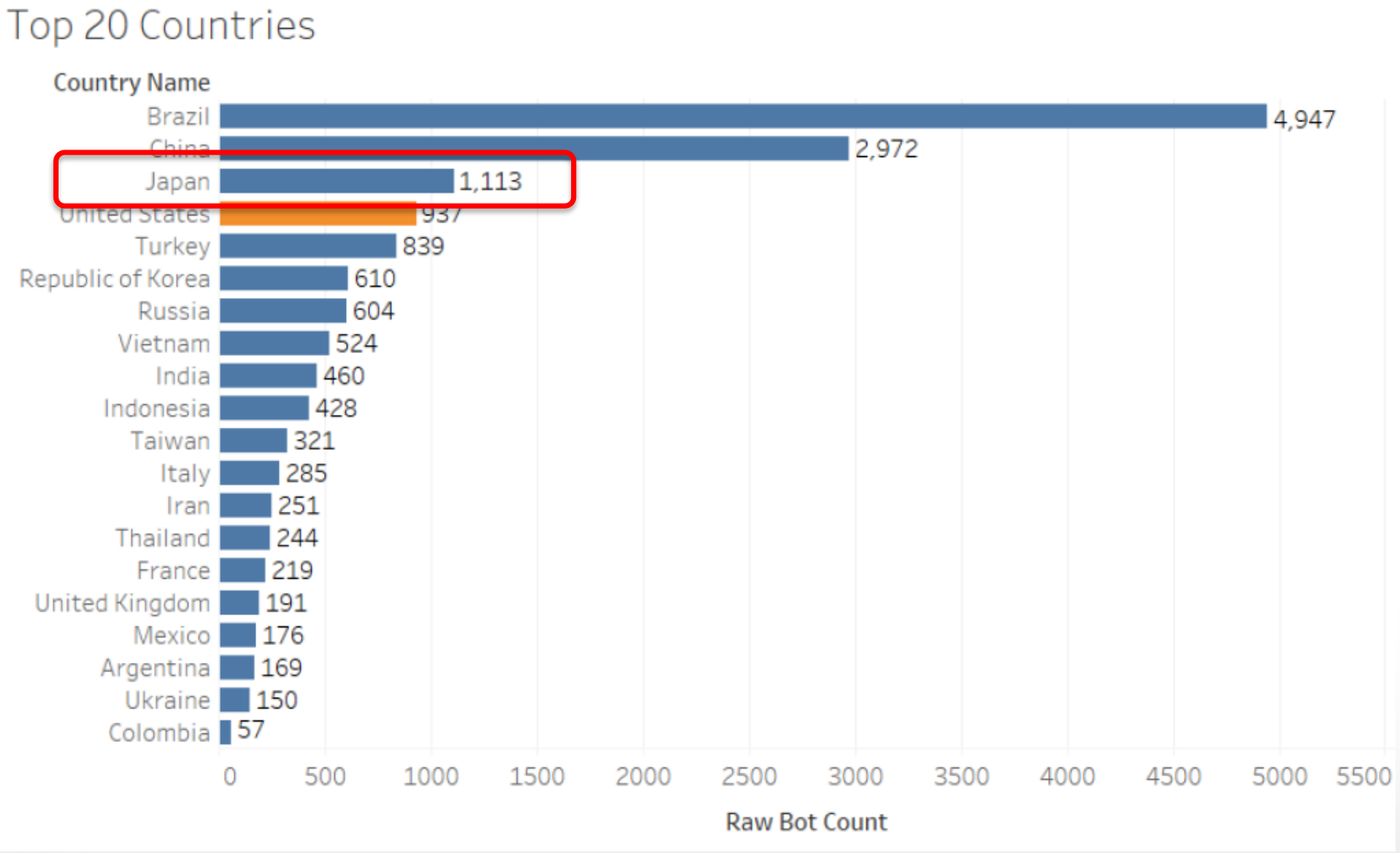
What is a darknet?



Example Network: 10.0.0.0/24

- 10.0.0.1-32 are assigned to devices.
- 10.0.0.33-254 are unassigned.
- A bot scanning the whole subnet will land on unused IPs.

Top 20 countries – raw numbers



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

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

- 2A1: 個人認証
- 2A2: 暗号解析・安全性評価（１）
- 2A3: 暗号解析・安全性評価（２）
- 2D4: 秘密計算
- 4A2: 秘匿計算
- 3A2: 高機能暗号（１）
- 3D2: プライバシー技術理論
- 3A3: 高機能暗号（２）

応用系の研究

- 1E3: クラウド・仮想化
- 1A4: Webセキュリティ
- 1A5: Androidセキュリティ
- 2E3: ユーザインタフェースが変えるセキュリティ
- 3B3: ブロックチェーン
- 4B2: IoTセキュリティ
- 4B1: 自動車セキュリティ
- 4C1: Drive-by-Download攻撃

侵入、マルウェア分析系の研究

- 1B5: データセット
- 2B3: ログ分析・侵入検知
- 2D3: 追跡技術と現実
- 2C4: 検知回避と誤検知
- 3C2: 表層解析とプログラム解析
- 3B1: マルウェア・ネットワーク分析
- 3C3: 攻撃検知
- 4D2: サイバー攻撃
- 3B4: 動的解析
- 4D1: 攻撃分析

ネットワーク系の研究

- 2C1: 悪性ドメイン名
- 2B2: ネットワークセキュリティ
- 3C4: 通信データ分析

機械学習系の研究

- 2C2: 機械学習（1）
- 2C3: 自然言語処理の活用
- 4C2: 機械学習（2）
- 2B1: 敵対的学習

その他

- 1A3: 認証・個人識別
- 1E4: 情報基盤
- 2A4: 暗号実装評価
- 3A1: 暗号構成手法
- 3D3: 加工
- 2E4: ソーシャルエンジニアリングとインテリジェンス
- 3E3: OWS：OSSセキュリティ
- 3A4: 偽造防止技術
- 3E4: 実行監視・脆弱性分析
- 4A1: 物理・視覚化暗号
- 4E1: リスク分析・プライバシー

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。

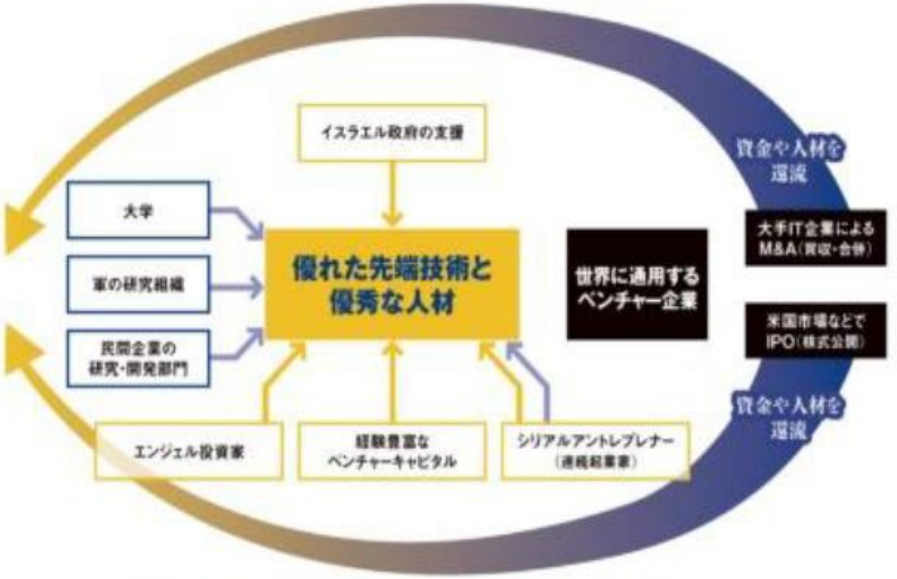
1）暗号・鍵管理、プロトコル
2）情報リスクマネジメント
3）システムエンジニアリング
4）情報保証の方法論
5）運用保証技術
6）戦略技術と製品の安全性の研究
7）サイバーセキュリティ人的要因の科学
8）高信頼性システムの構築

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

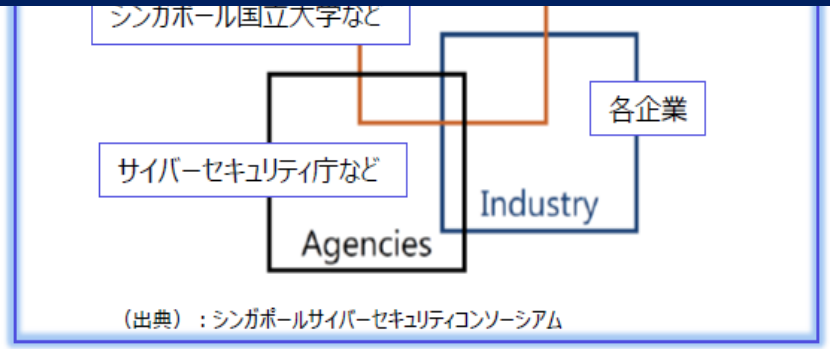
○ 2013年に策定した「サイバーセキュリティ研究開発プログラム」に基づき、シンガポール国立大学、国立研究財団（NRF）が中心となり、サイバーセキュリティに係る研究開発を推進。
○ また、産学官連携組織としてシンガポールサイバーセキュリティコンソーシアムを設立。

✓ 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）

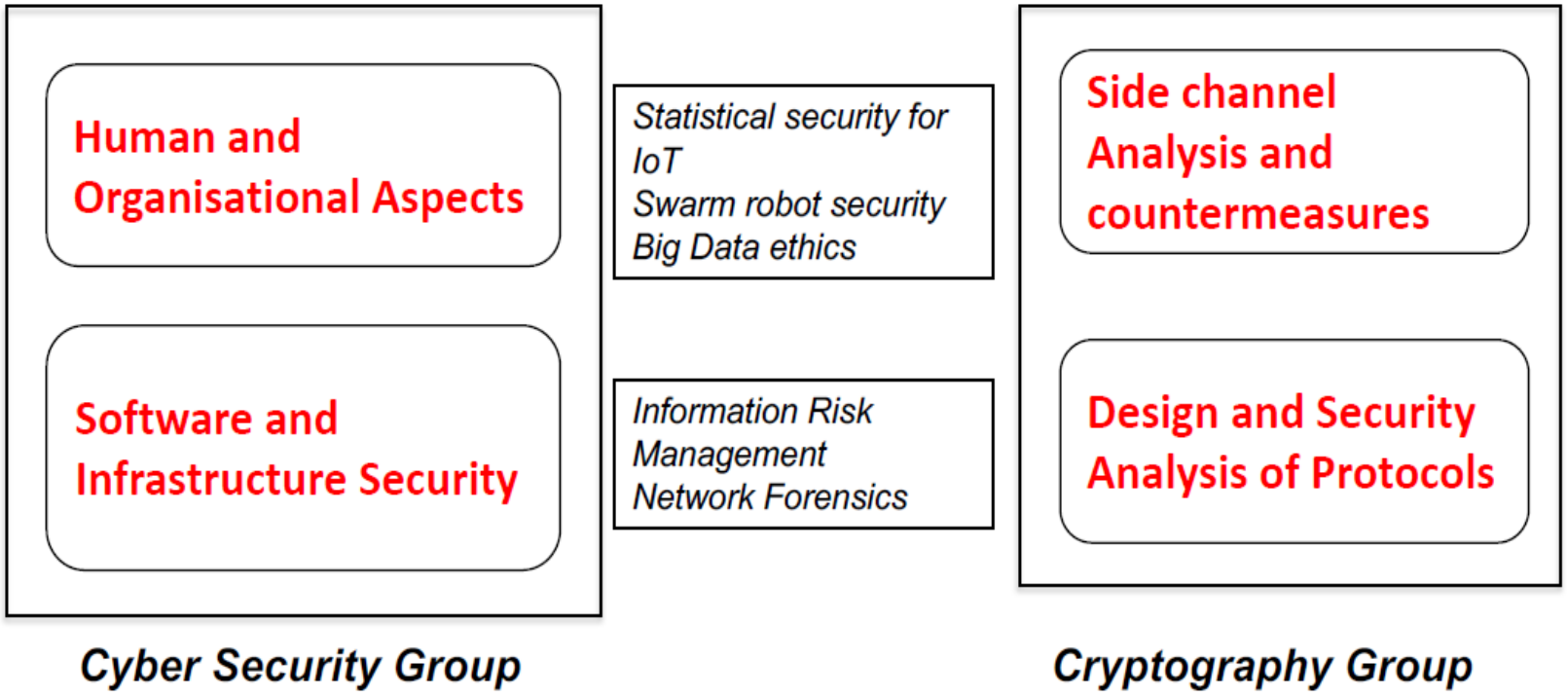
1）スケーラブルなTrustworthyシステム
2）レジリアントなシステム
3）効果的な攻撃状況の把握、攻撃アトリビューション
4）内部犯行対策
5）脅威検出、分析、対応（保護）
6）効果的、効率的なデジタルフォレンジック

✓ ま
セ

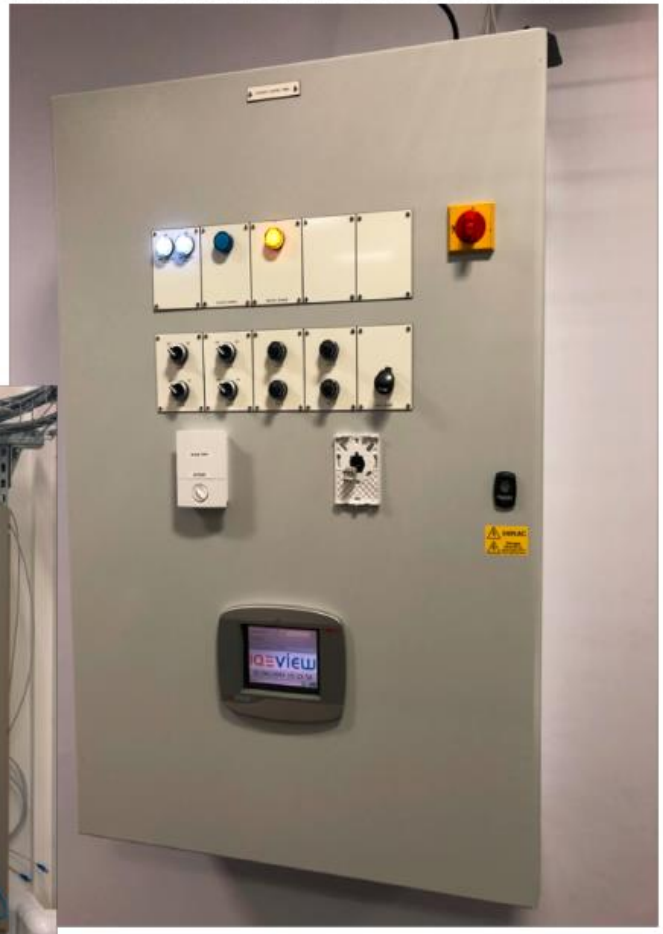


（出典）：シンガポールサイバーセキュリティコンソーシアム

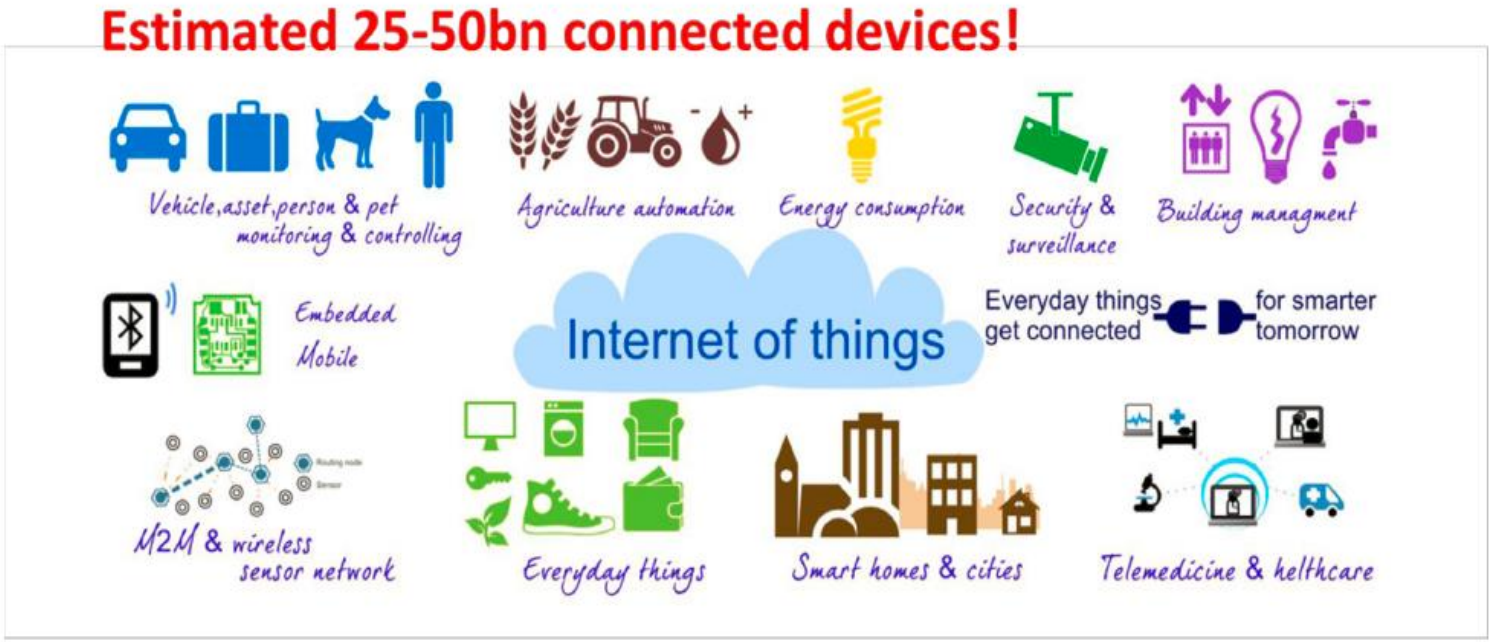
Bristol大学(英国)における
サイバーセキュリティ研究紹介



Current Research grants: > £15M
40 Researchers

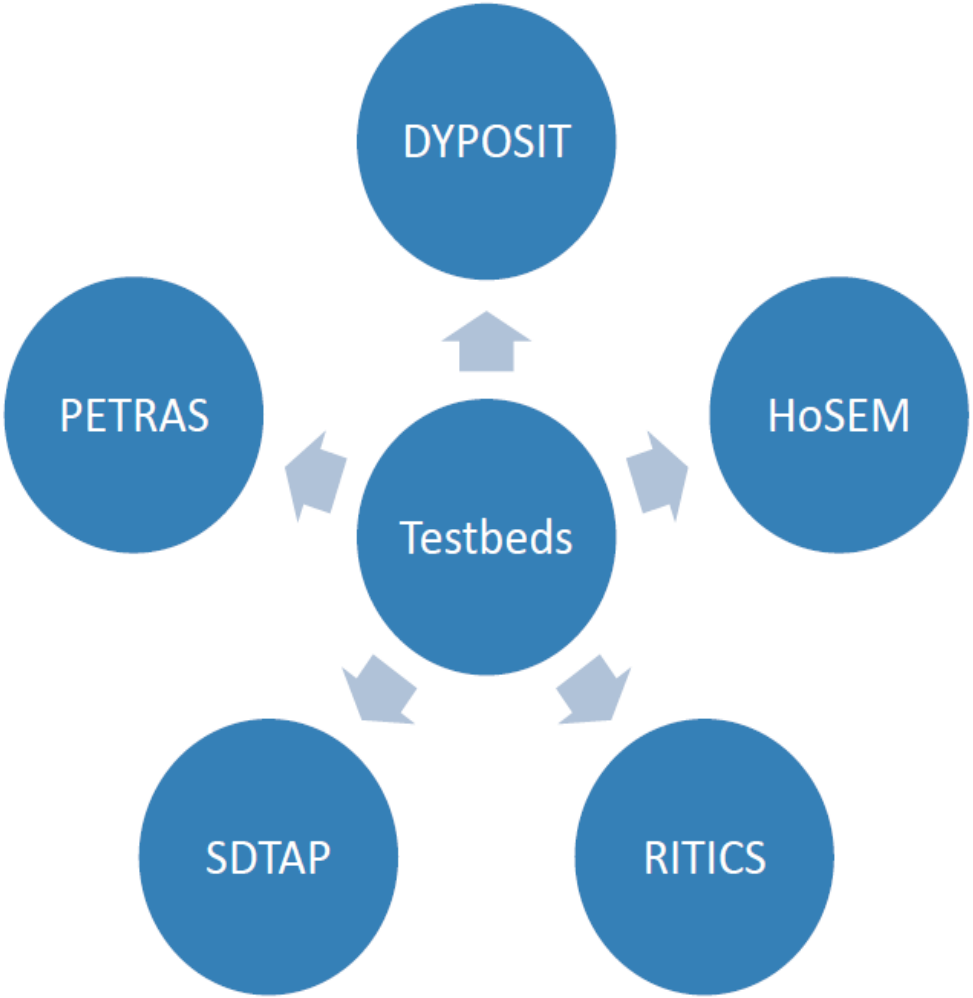


Centre for Doctoral Training on Trust, Identity, Privacy and Security in Large-scale Infrastructures

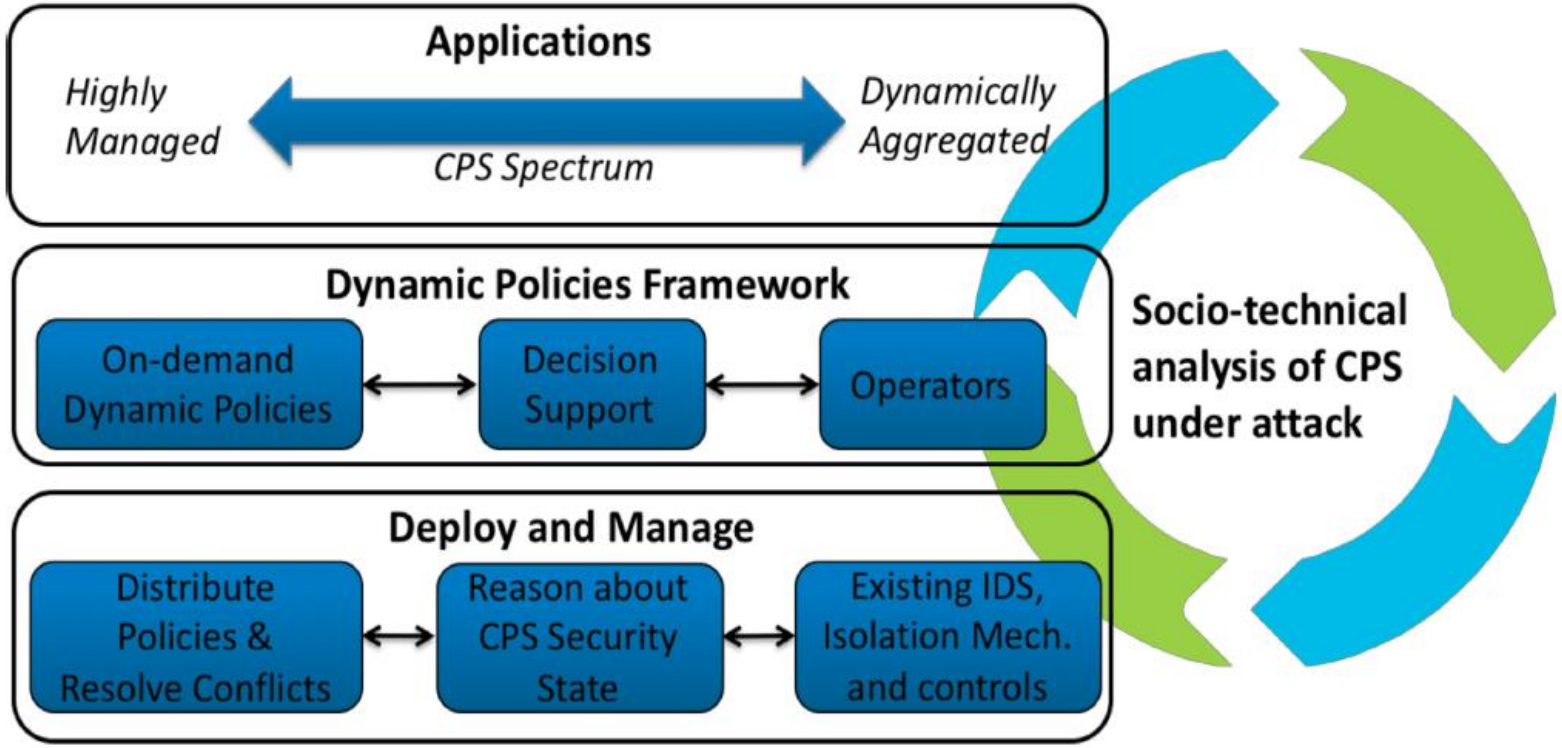


Centre for Doctoral Training on Trust, Identity, Privacy and Security in Large-scale Infrastructures

Estimated 35 zeta-bytes (35 x 10^{21}) of digital records!


DYPOSIT
PETRAS
HoSEM
Testbeds
SDTAP
RITICS

DYPOSIT: Dynamic Policies for Cyber-Physical Infrastructures under Attack



- Attack analysis
  - How and why security vulnerabilities are introduced into cyber-physical systems
  - Analysis of attack scenarios and their implementation for studying system and operator behaviours under attack

- Attack detection
  - Specialised vulnerability scanners and intrusion detection systems for cyber-physical infrastructures

- Dynamic policy models
  - Model for dynamic change in an ICS configuration

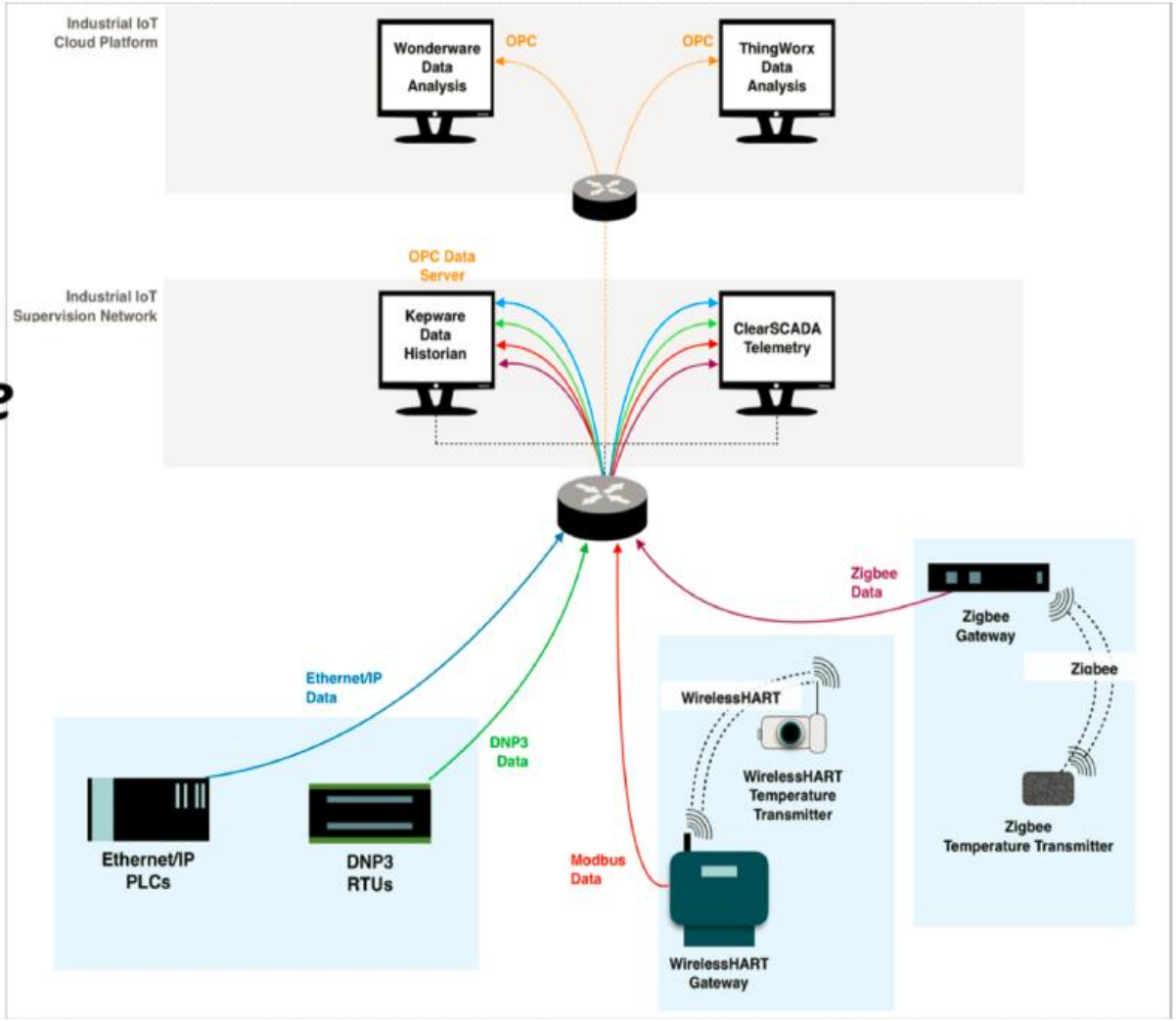
- Platforms to support dynamic policies
  - A CPS Operating System that supports secure loading of third- party application micro-services, strong application isolation, confidentiality of application data and contractually limited access to device resources.

PETRAS: Cyber Security of Internet of Things

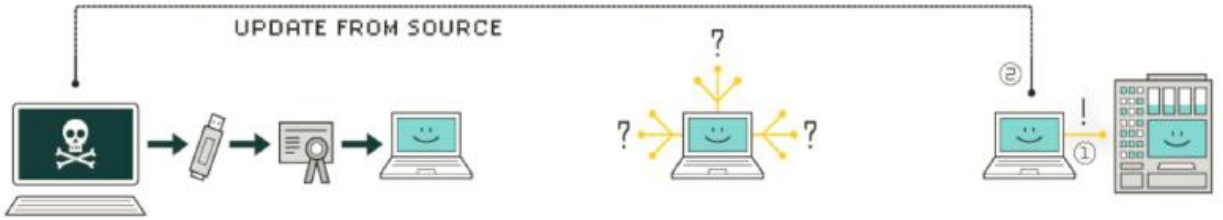
Security and Safety of life, infrastructure and environment

Resilience

The Convergence of IoT and OT



Anatomy of Attacks



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

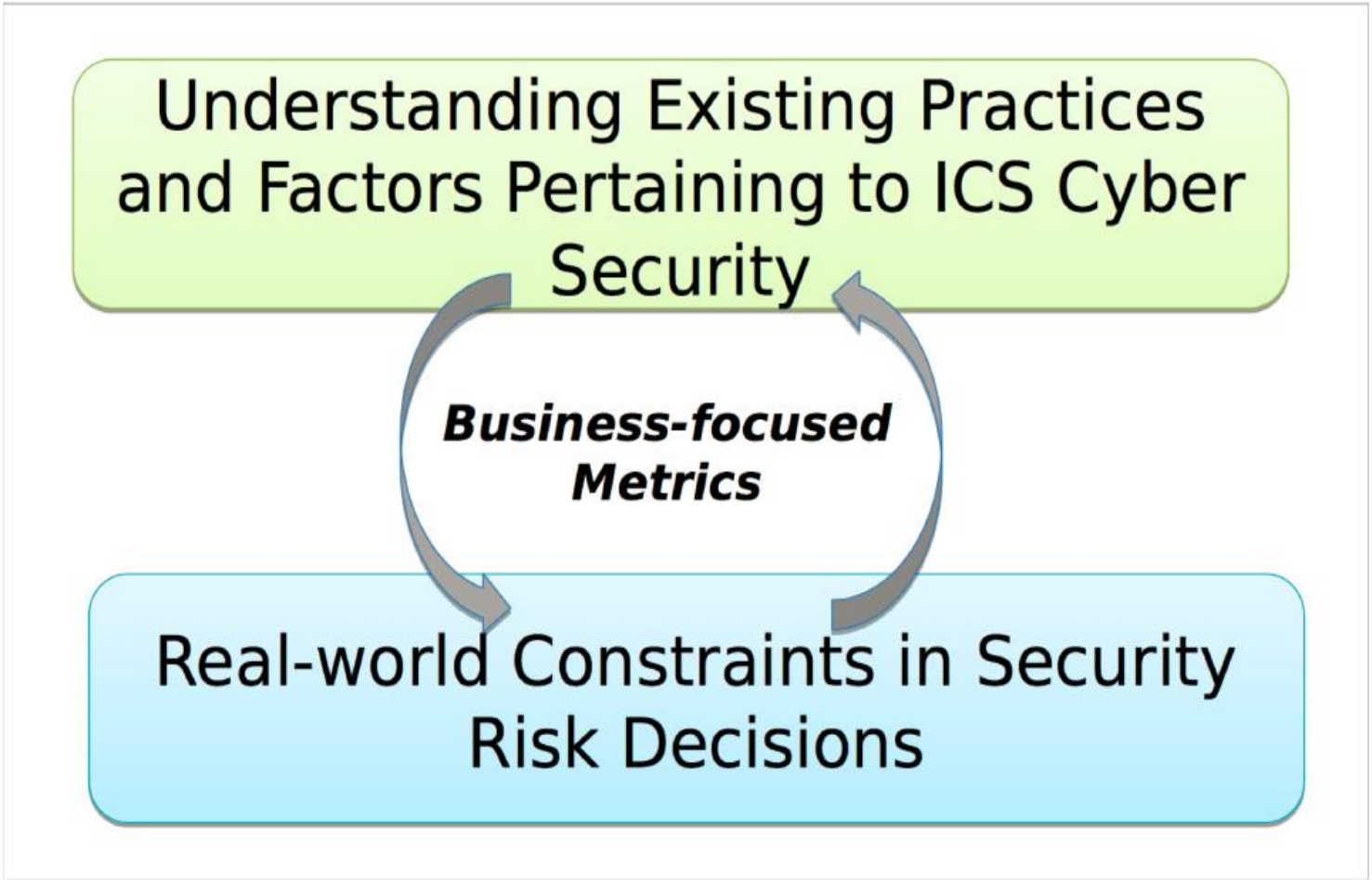
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

RITICS: Risk management in cyber-physical systems

- **Mumba:** Systematic and rigorous metrics for security risk decision-making
- **NIS:** Organisational and sectoral differences in compliance


Understanding Existing Practices and Factors Pertaining to ICS Cyber Security
Business-focused Metrics
Real-world Constraints in Security Risk Decisions

Case Studies

Latent Design Conditions

Game play

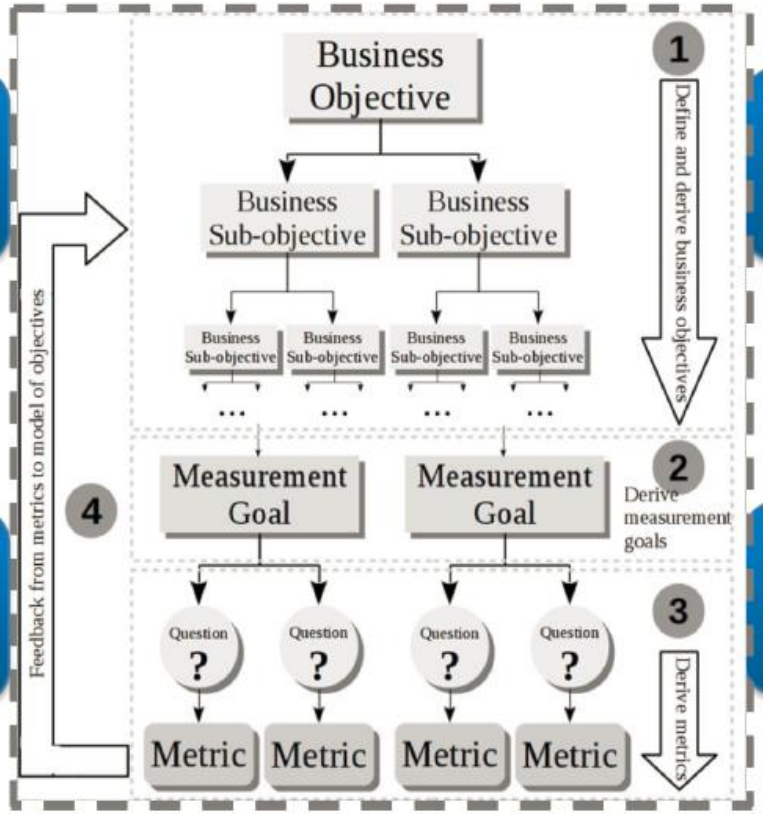
Decision Patterns and Risk Thinking

Fieldwork

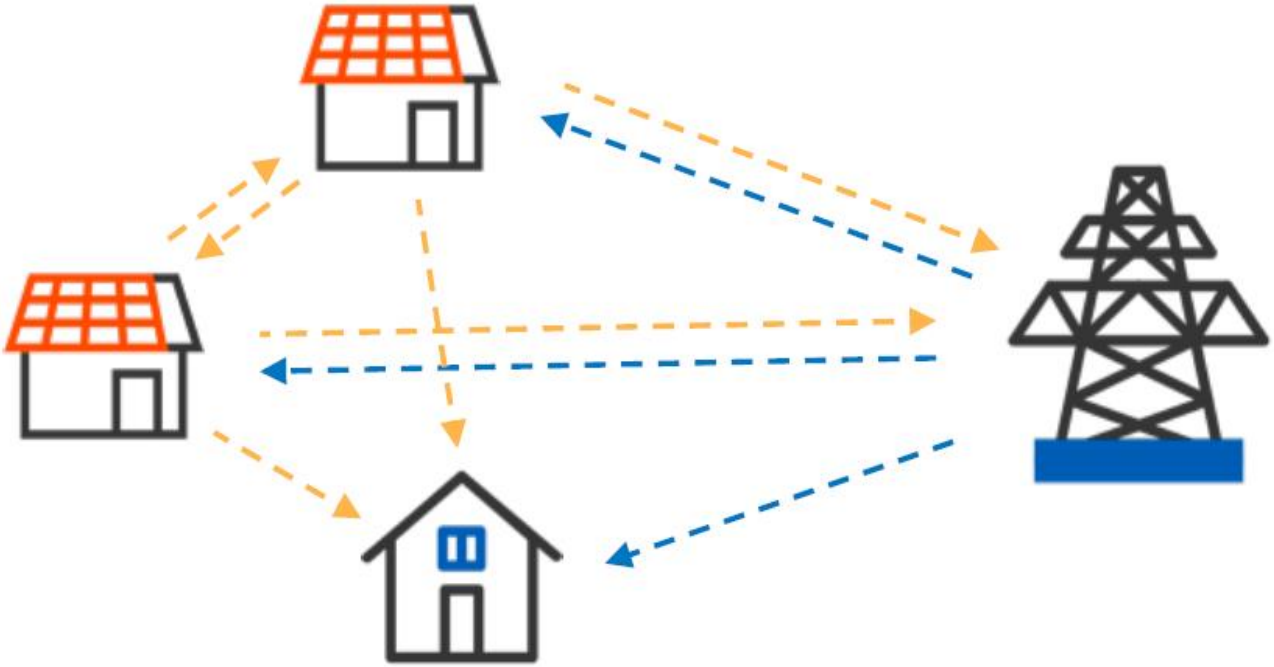
Grey Area and Limbo Design

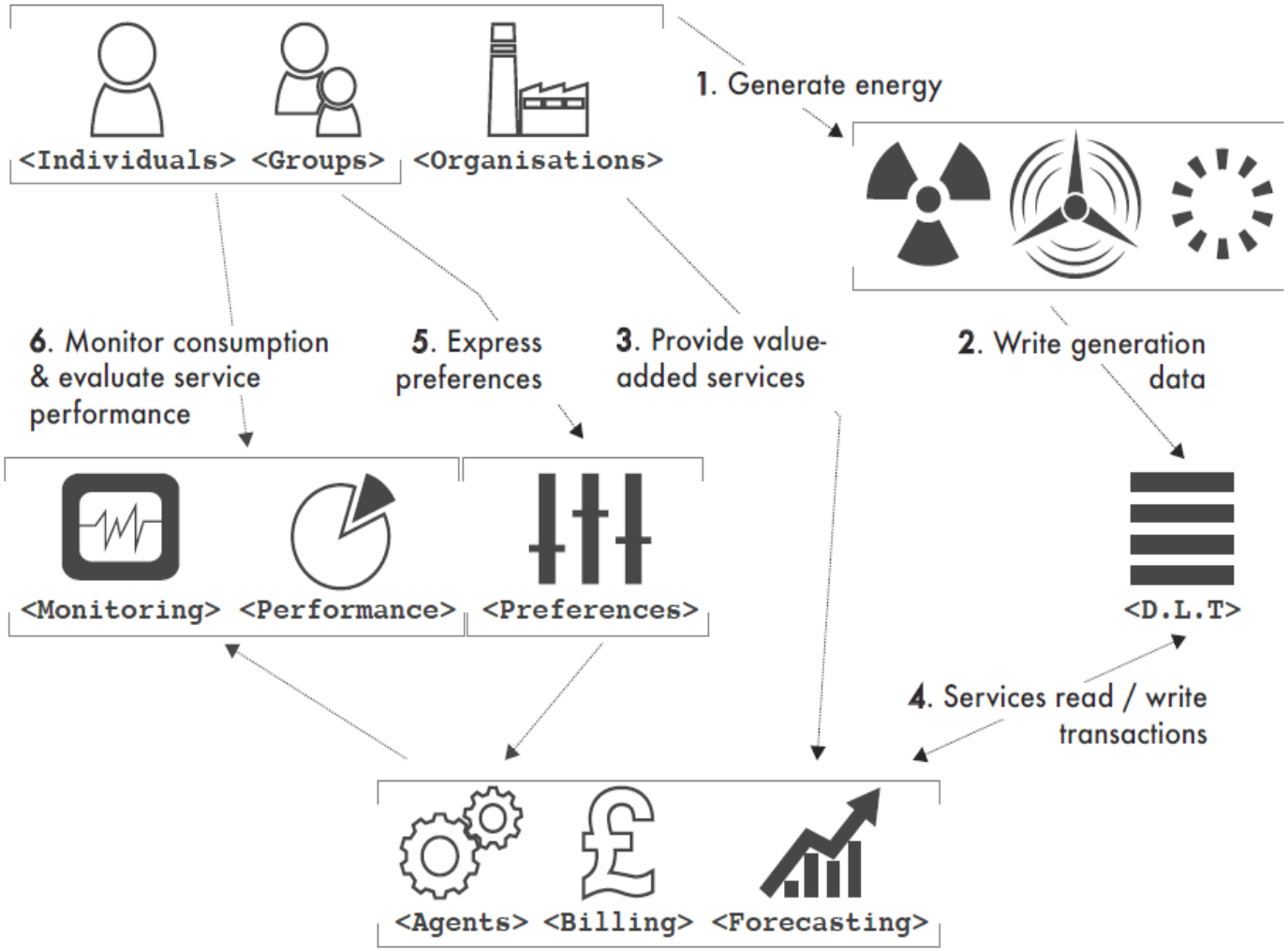
Testbed

Technological Factors



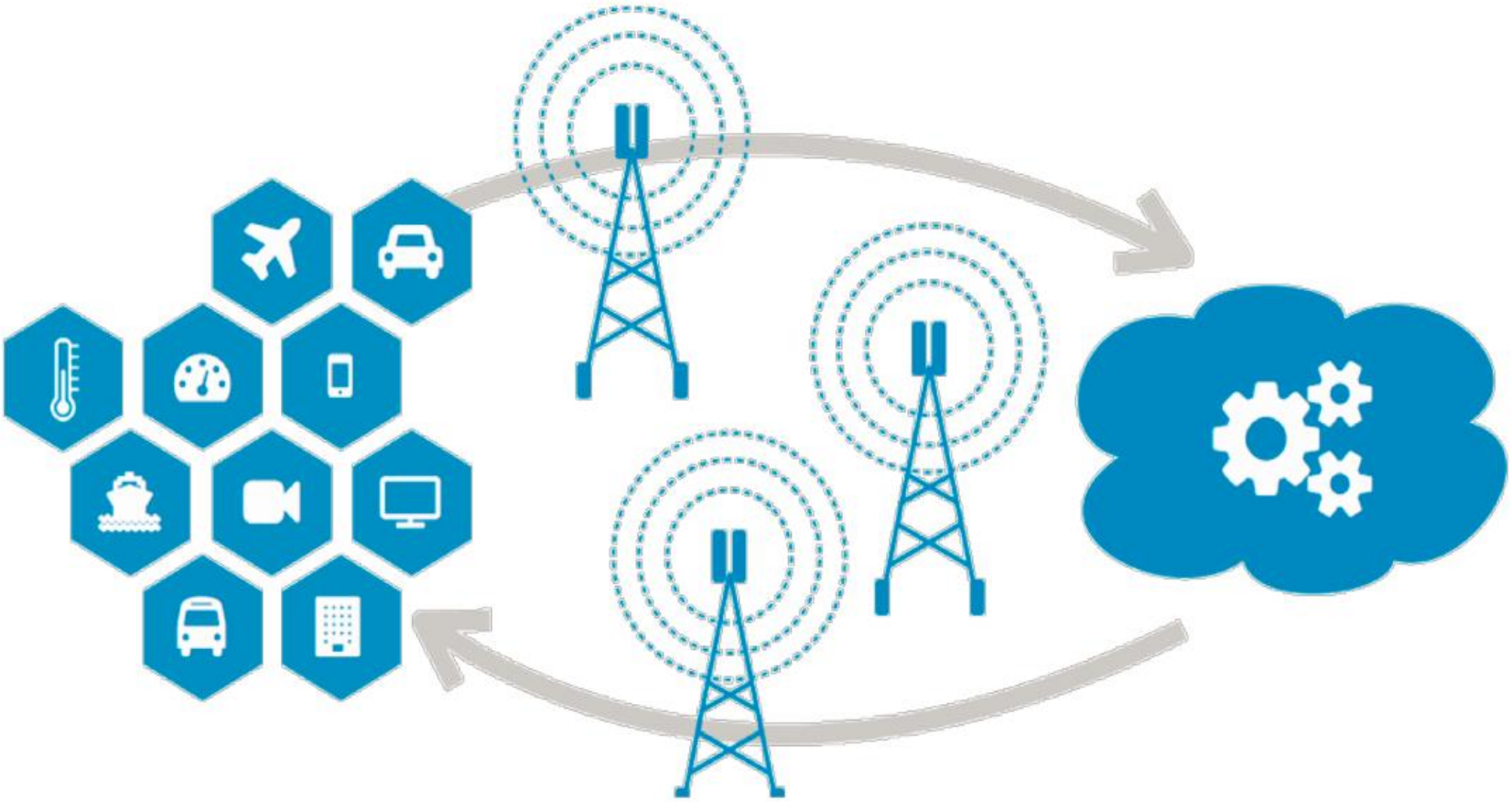
HoSEM: Household Supplier Energy Market




<Individuals> <Groups> <Organisations>
1. Generate energy
6. Monitor consumption & evaluate service performance
5. Express preferences
3. Provide value-added services
2. Write generation data
<Monitoring> <Performance>
<Preferences>
<D.L.T>
4. Services read / write transactions
<Agents> <Billing> <Forecasting>

University of BRISTOL
Bristol Cyber Security Group

SDTAP: Security of Devices and Technologies at the Periphery（周辺）



- At least 10 PhD students starting per year
- Four major areas of focus:
  1. Socio-technical challenges to security and privacy at-scale
  2. Resilient Infrastructures in Partially-Trusted Environments
  3. Empirically grounded assurances for security and privacy at-scale
  4. Responsible innovation

AIRBUS

altran


babcock
trusted to deliver™


Google


National Cyber
Security Centre
a part of GCHQ


THALES


Vodafone


IBM


Lloyd's Register
Foundation


CORNELL
TECH


UF
UNIVERSITY of
FLORIDA


TECHNISCHE
UNIVERSITÄT
DARMSTADT


KU LEUVEN


THE UNIVERSITY
of ADELAIDE


NICT


CYSEC

Queens大学(英国)における
サイバーセキュリティ研究紹介


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
SECURING OUR
DIGITAL TOMORROW
QUEEN'S
UNIVERSITY
BELFAST
ESTP1845

Research Strategy

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Securing Connected Systems

Building on our cores areas of expertise:

- Secure Connected Devices
- Networked Security Systems
- Industrial Control Systems (ICS) Security
- Security Intelligence

Secure Connected Devices

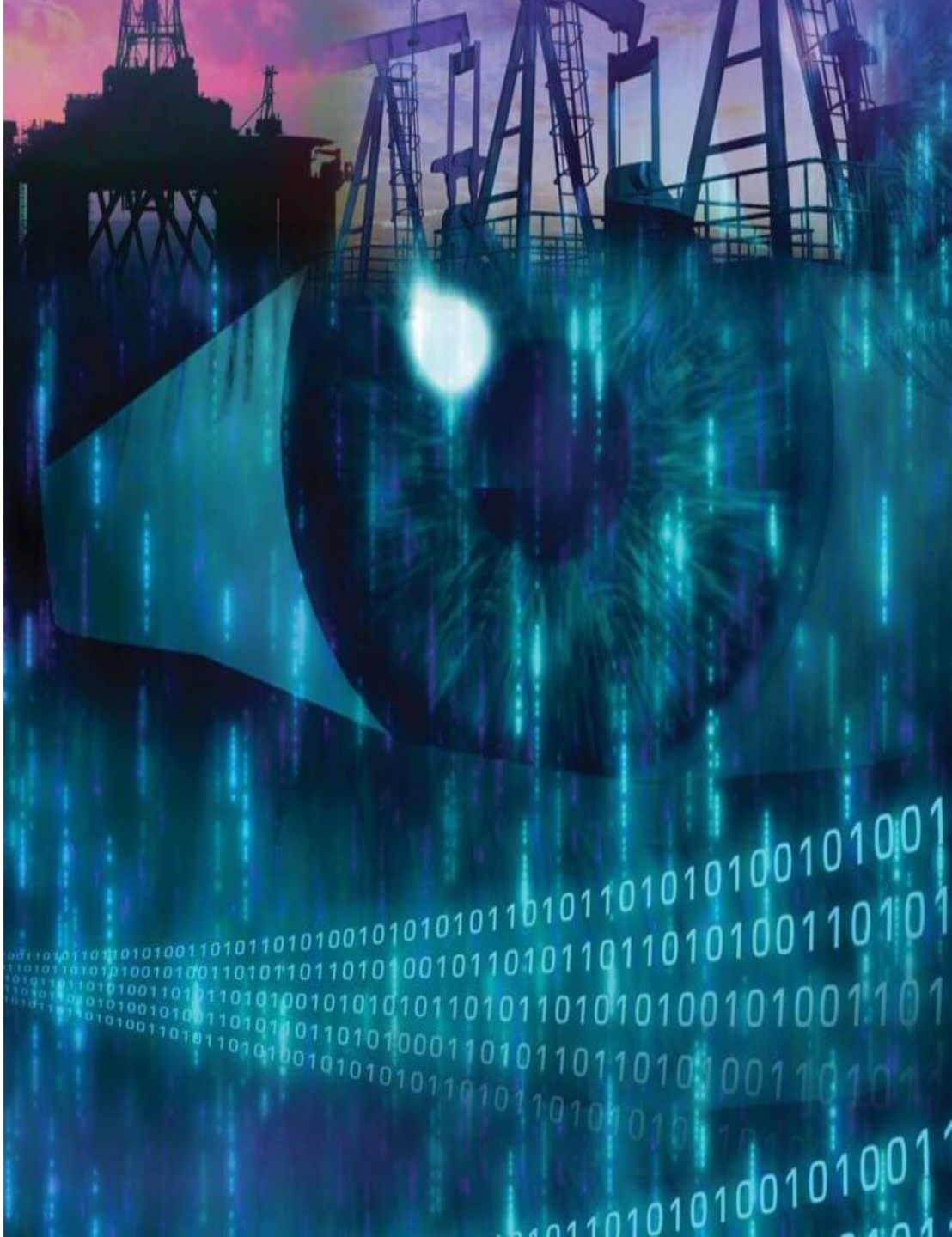
- Trusted Hardware
- Hardware-based Security Services

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Networked Systems Security

- Network Security
- SDNFV Security
- Malware Analytics
- Cloud Security
- Mobile & IoT Security

Industrial Control Systems (ICS) Security



CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security Intelligence

Securing cyber-physical systems through the development and application of novel AI technologies

CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
Secure Connected
Devices
PROFESSOR MÁIRE O'NEILL
JANUARY 2019

Insecure Connected Devices

Tech Republic's list of the 1 *least secure* connected devices - Feb 2018





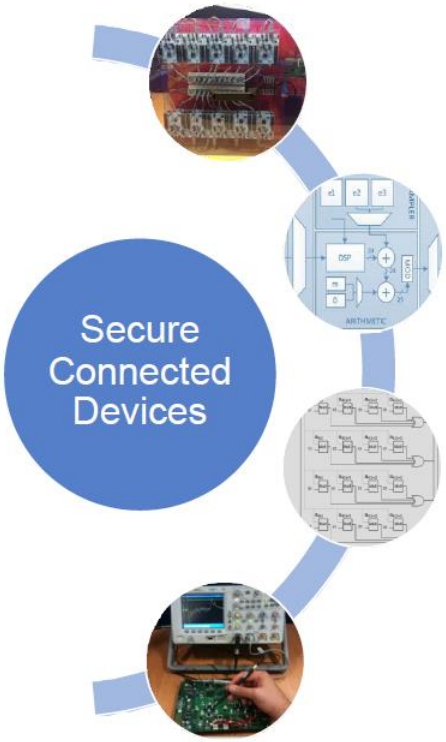





Adapted from https://www.techrepublic.com/pictures/photos-the-11-least-secure-connected-devices/

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Secure Connected Devices



Trusted Hardware

- Cryptographic Hardware & Software Architectures
- Physical Unclonable Functions (PUFs)
- Side Channel Analysis (SCA)
- Hardware Trojan Detection

Hardware-based Security Services

- Practical Post-quantum cryptography
- Advanced Cryptographic Architectures

EPSRC

in association with National Cyber Security Centre

SAFE crypto

sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS

Centre for Defence Enterprise

BAE SYSTEMS

intel
Sponsors of Tomorrow.

KeyHAS – Hide and Take Keys

uniserver

riscure

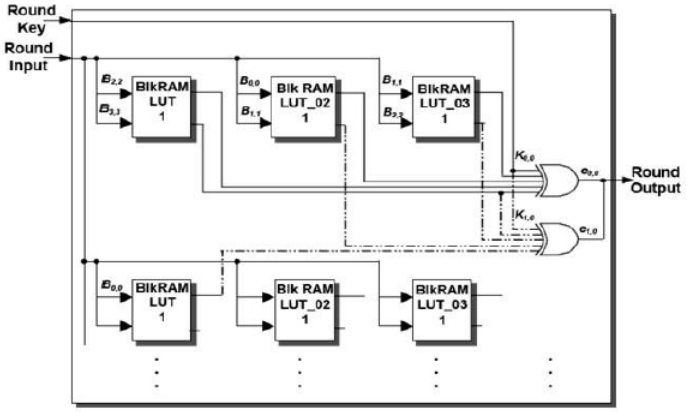
Rambus
Cryptography Research

Cryptographic Hardware Architectures

CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

High Speed AES

- Very high-speed Advanced Encryption Standard (AES) Hardware Architectures
- Novel algorithmic & architectural optimisations
- Successfully commercialised by Amphion Semiconductors (acquired by Trident Microsystems, 2010)

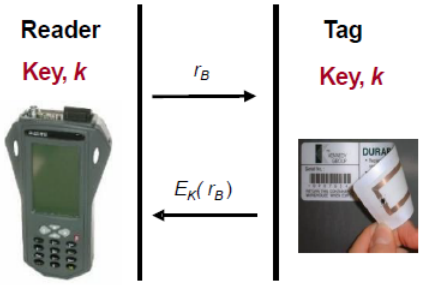


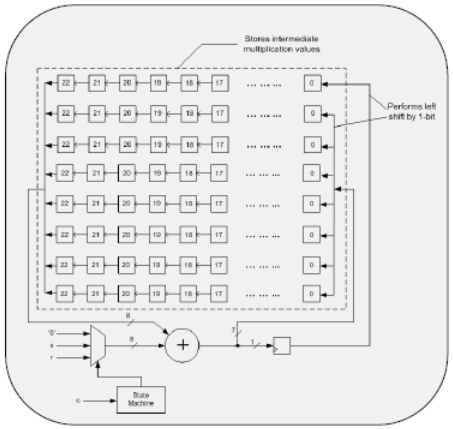
AMPHION

ENTROPIC

Lightweight Security

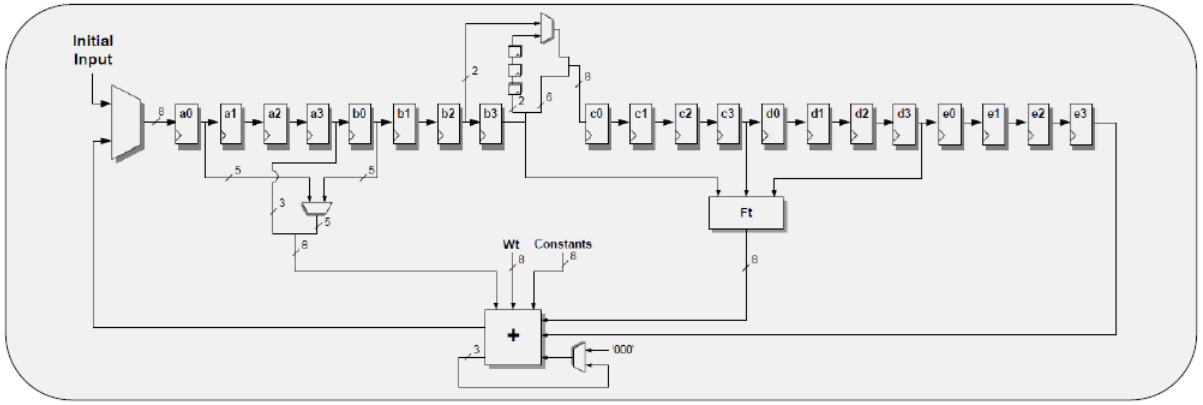
- *First to show* that a public key algorithm, the **GPS Identification Scheme**, could be deployed on passive RFID tags (2007) – in collaboration with Matt Robshaw, Orange Labs, France
  (180nm CMOS, 900 gates, 5uA at 500 kHz, 68 cycles)





Lightweight Security

- Lightweight **SHA-256** Hash Function Designs optimised for RFID (2011)
  - *smallest & lowest power designs to date*
  (130nm CMOS, 5358 gates, 2.86uW@100 kHz)
- Proposed use of SHA-1 and GPS ID algorithm (2010) to provide the **lowest cost Digital Signature design** to date for RFID (130 nm CMOS, 7500 gates)



Fully Homomorphic Encryption

CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

High-speed FHE over the integers

Coron et al., Public Key Compression and Modulus Switching for FHE over the Integers, EUROCRYPT 2012

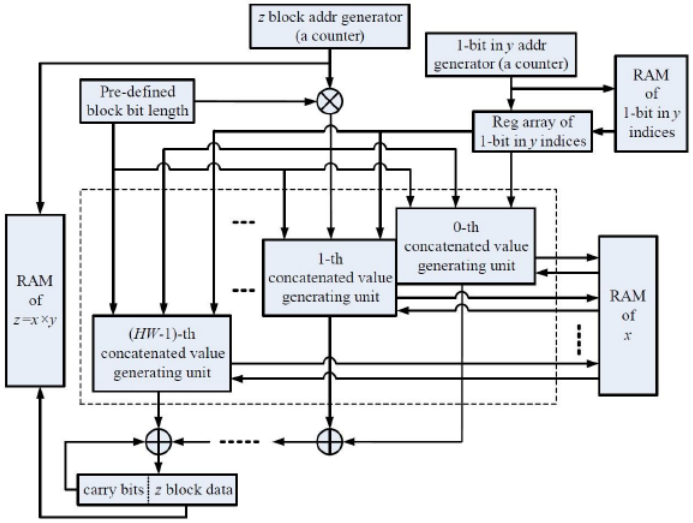
THALES

$$C = m + 2r + 2 \sum_{i=1}^{\theta} b_i x_i \bmod x_0$$

Parameter sizes	Bit-length of b_i	Bit-length of x_i or x_0	θ
Toy	936	150,000	158
Small	1476	830,000	572
Medium	2016	4,200,000	2110
Large	2556	19,350,000	7659

b_i can be taken to be a Low Hamming Weight (LHW) integer with max HW of 15

Proposed LHW Multiplier Architecture



Quantum-Safe Cryptography

CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

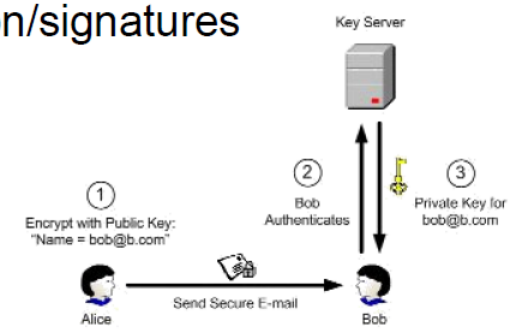
Quantum-Safe Cryptography

Lattice-based Cryptography (LBC) emerging as a very promising PQ candidate

- LBC encryption and digital signatures already practical & efficient
  - NTRUEncrypt exists since 1996 with no significant attacks to date
  - Recent LBC signatures schemes shown to outperform RSA sig schemes

- Underlying operations can be implemented efficiently

- Allows for other constructions/applications beyond encryption/signatures
  - Identity based encryption (IBE)
  - Attribute-based encryption (ABE)
  - Fully homomorphic encryption (FHE)



Side Channel Analysis

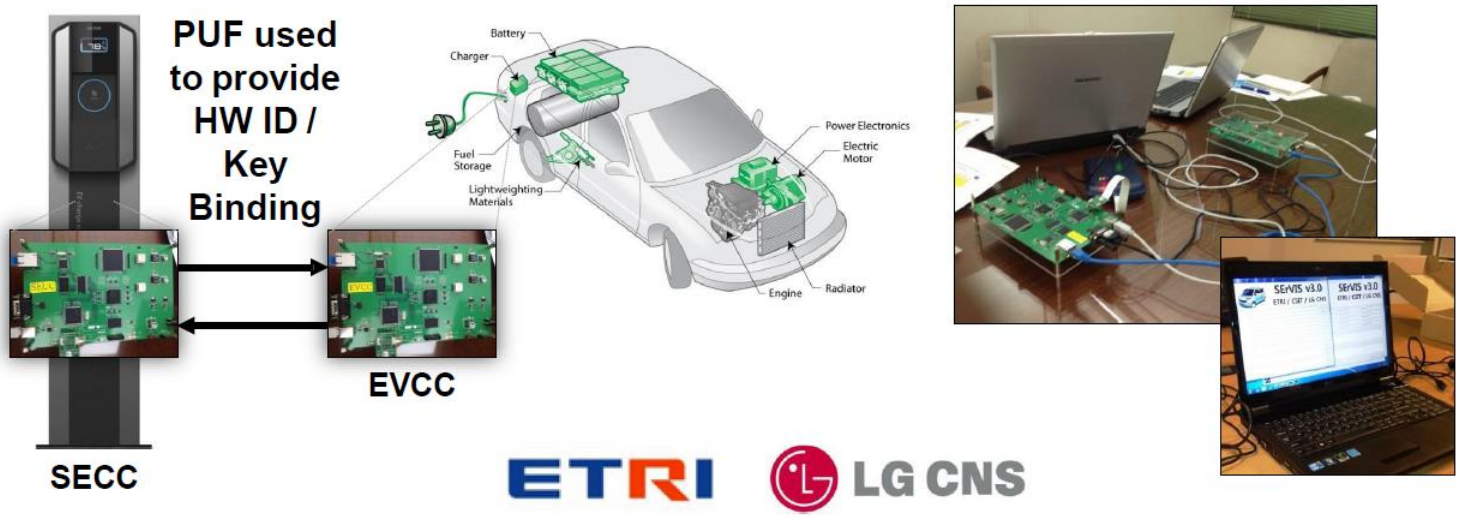
CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Physical Unclonable Functions

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

PUF for Connected Devices

Integrated PUF into Vehicle to Grid (V2G) Communication Interface for use in an Electric Vehicle (EV) charging system



ETRI LG CNS

（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)

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

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
   - を理解）
2. 攻撃挙動の高度分析のための研究開発
   -AI等の活用
   - 度分析
   - 解析技術
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
   - 境などに
   - 策の自動化
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
   -

攻撃・攻撃予兆の把握のための研究開発

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）

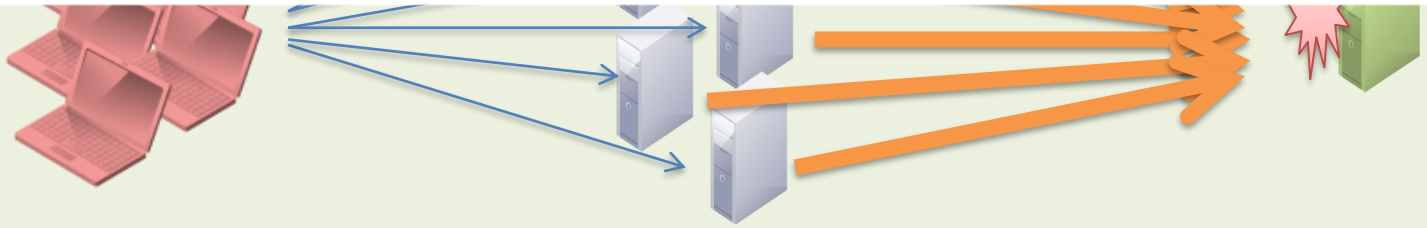
DR-DoS 攻撃の早期検知

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. れ

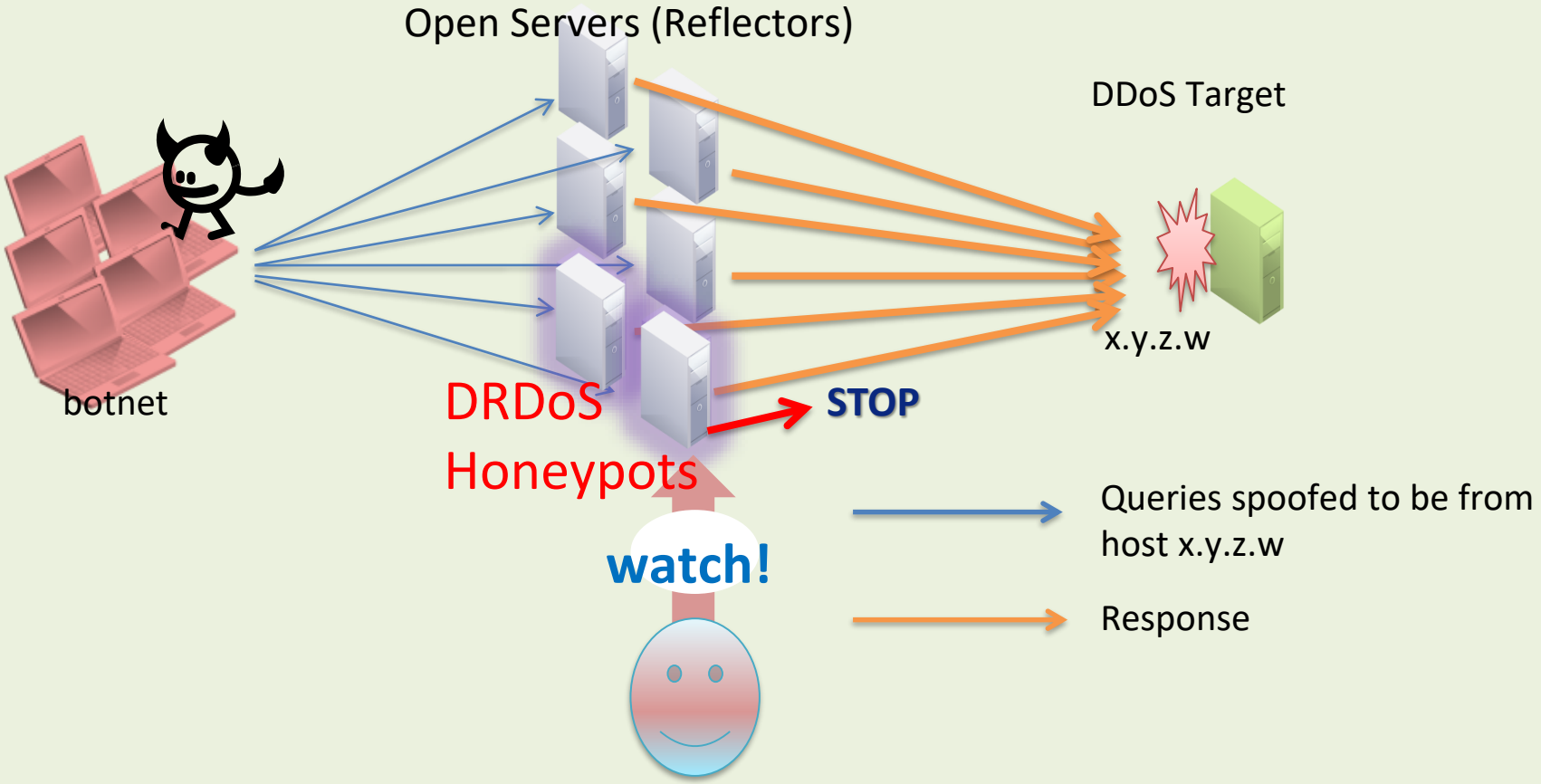
Cat	Protocol	Port(s)	Description
Network Svc	SNMP v2	161	Monitoring network-attached devices
	NTP	123	Time synchronization
	DNS	53	(Primarily) Domain name resolution
	NetBios	137	Name service protocol of NetBios API
	SSDP	1900	Discovery of UPnP-enabled hosts
Leg.	CharGen	19	Legacy character generation 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

e IP



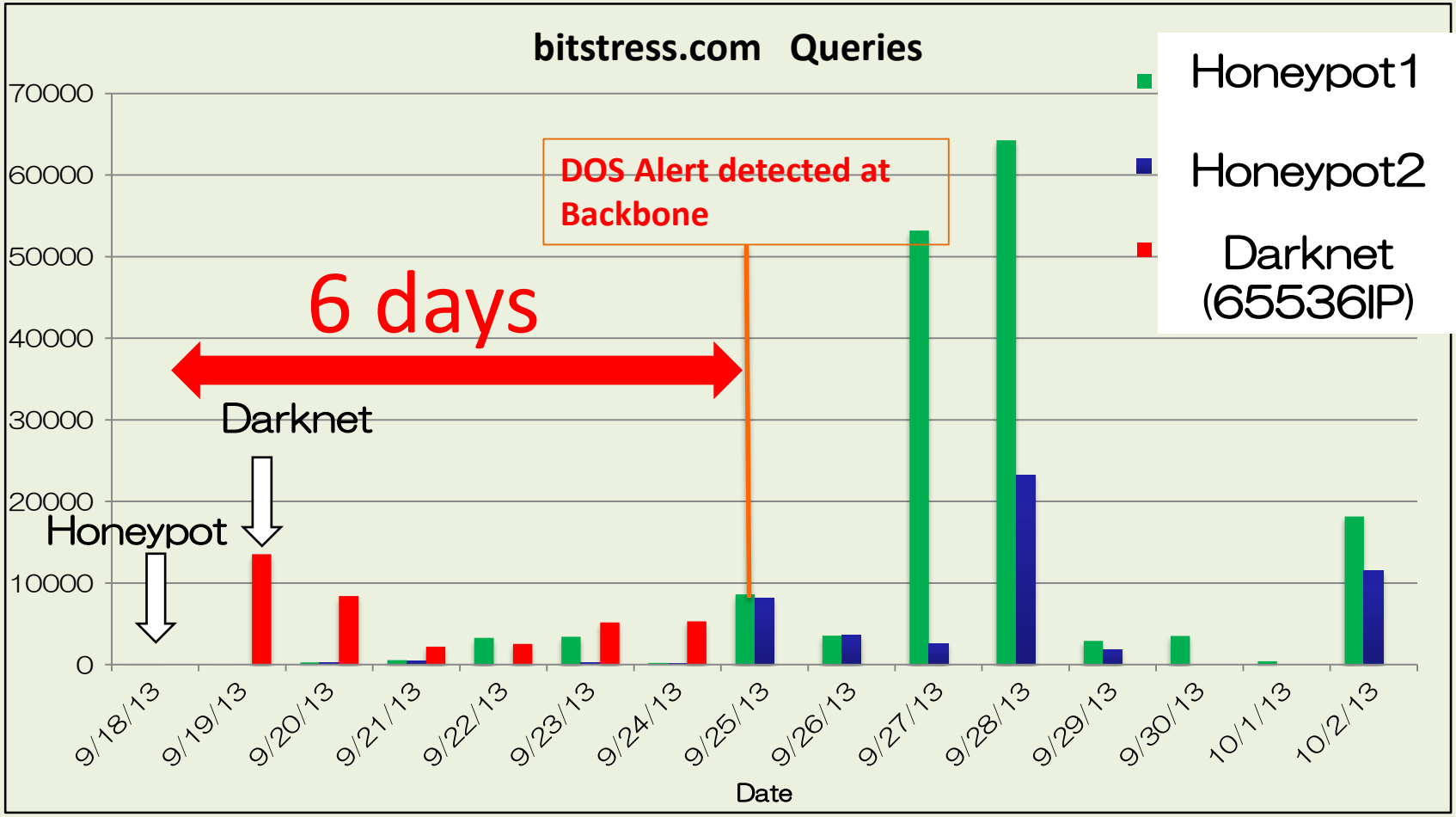
DR-DoS ハニーポット

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

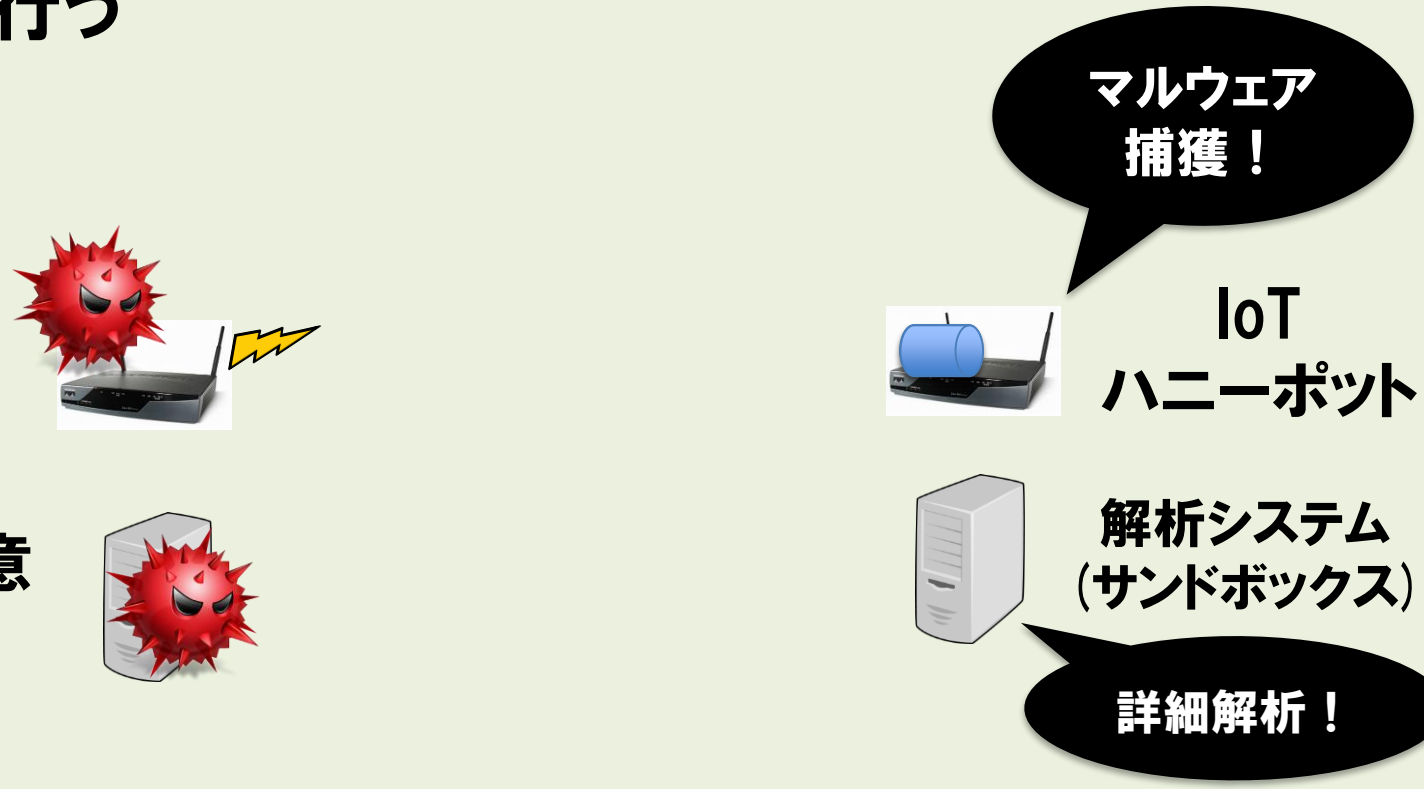
[DRDoS Honeypot detail data]
AS num : "AS2516 KDDI KDDI CORPORATION"
country : "Japan"
pps(MAX) : 2.2
pps(AVG) : 1.1416666666666666

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

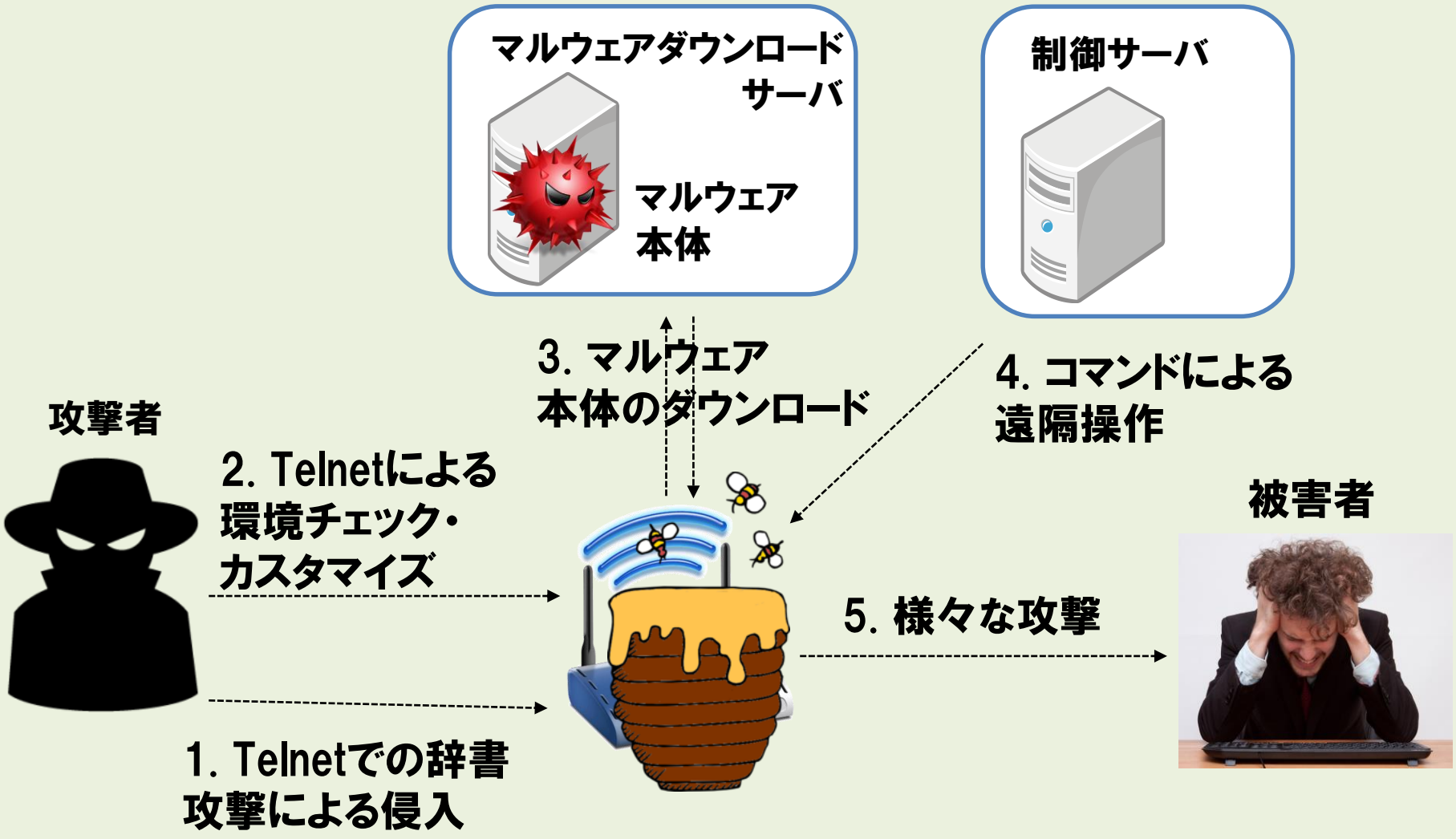
例えば、 IoTハニーポット/ダークネット

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

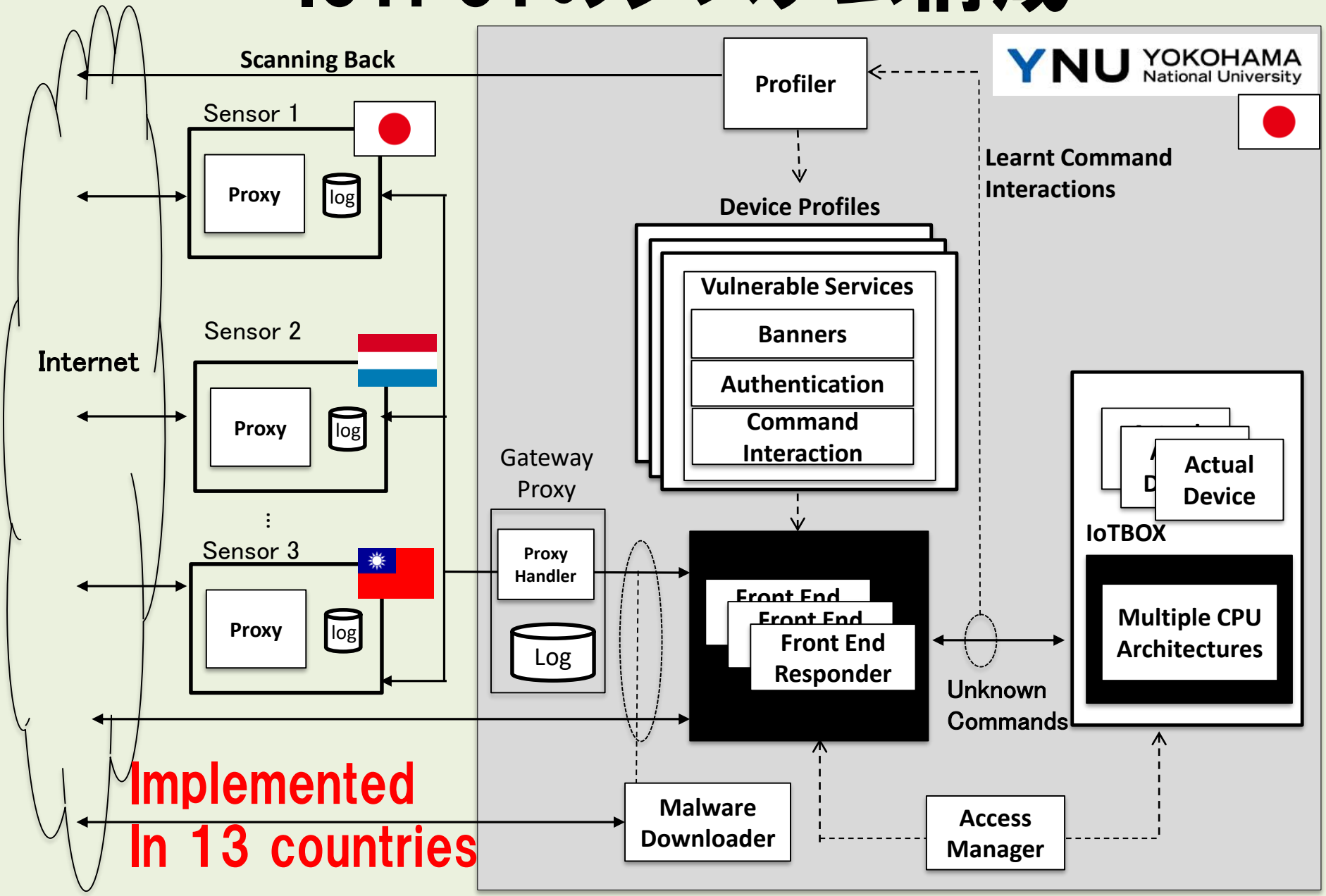
脆弱な機器を模擬した**囮システム（ハニーポット）**により攻撃元と通信を行い、攻撃の観測・マルウェア捕獲し、詳細解析を行う



Telnetベースのマルウェア感染の流れ

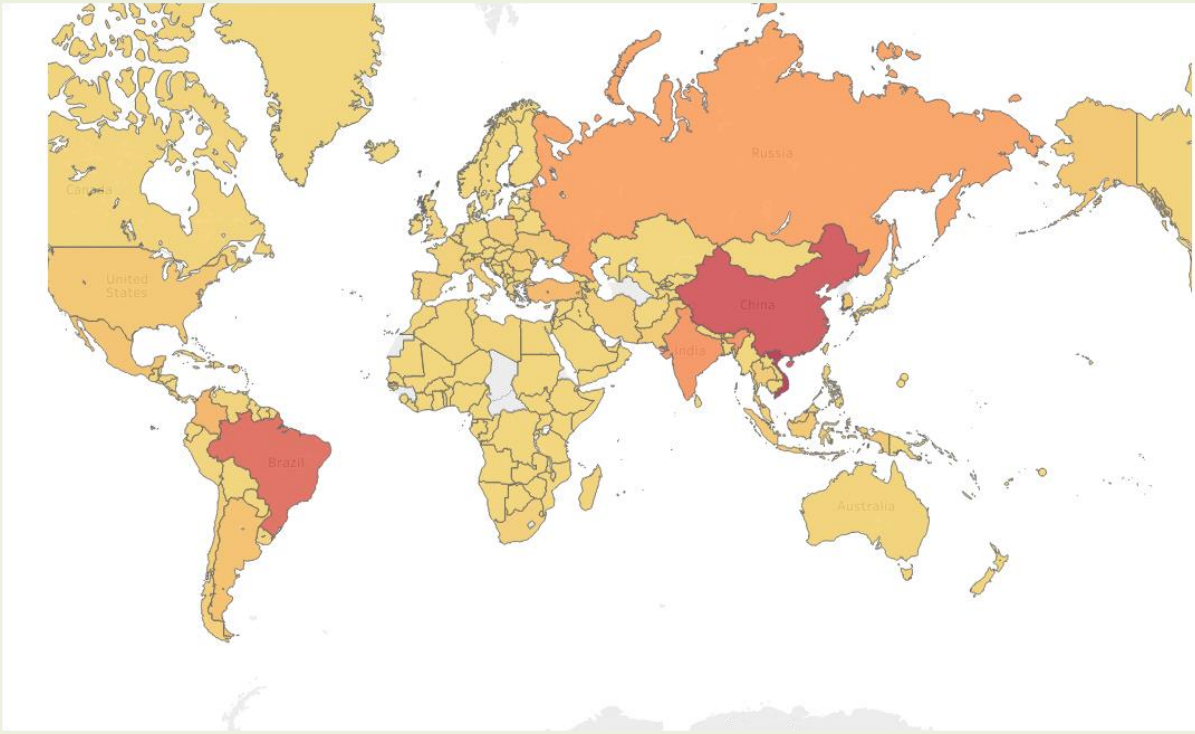


IoTPoTのシステム構成



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

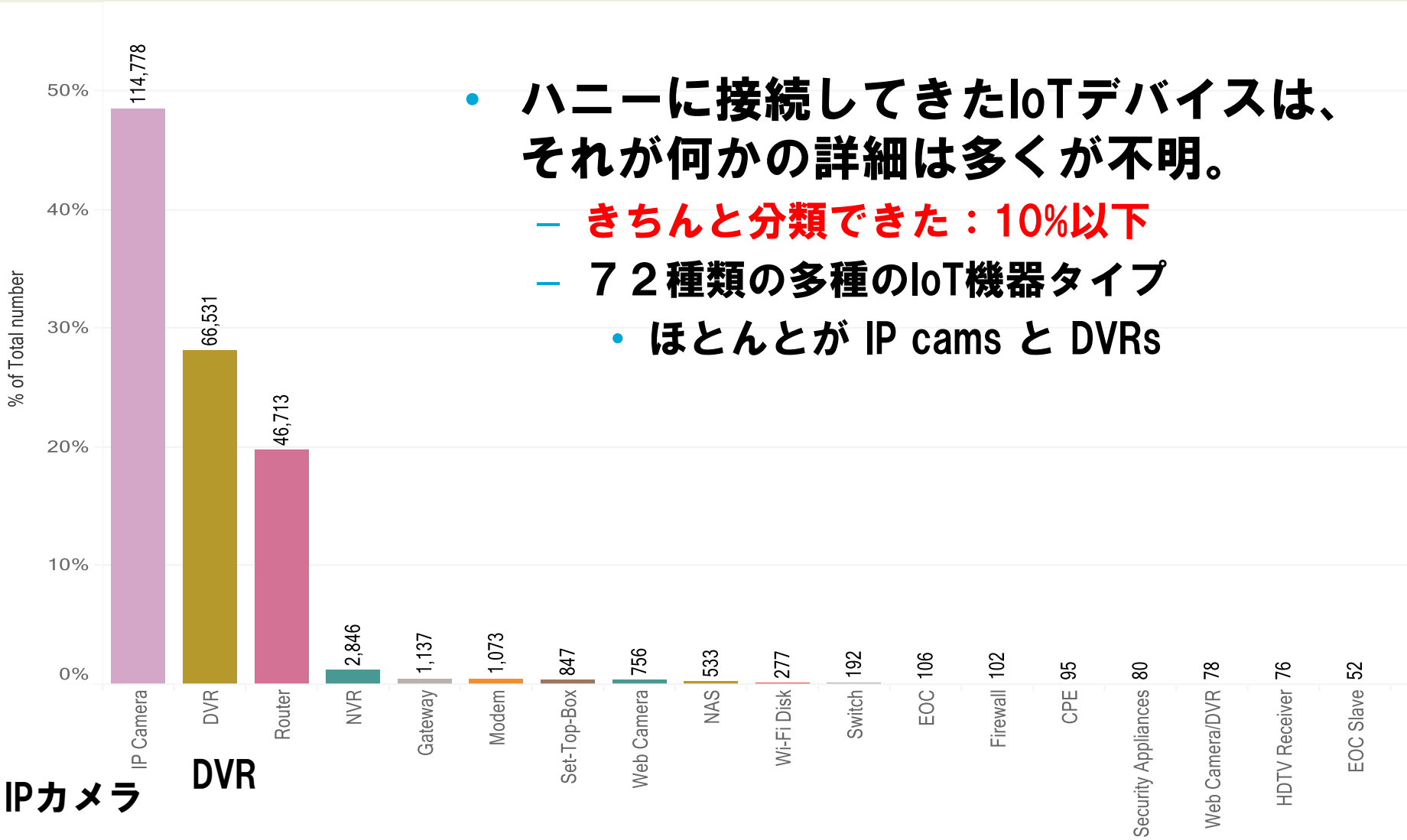
Security Appliance

Internet Communication Module

Video Broadcaster

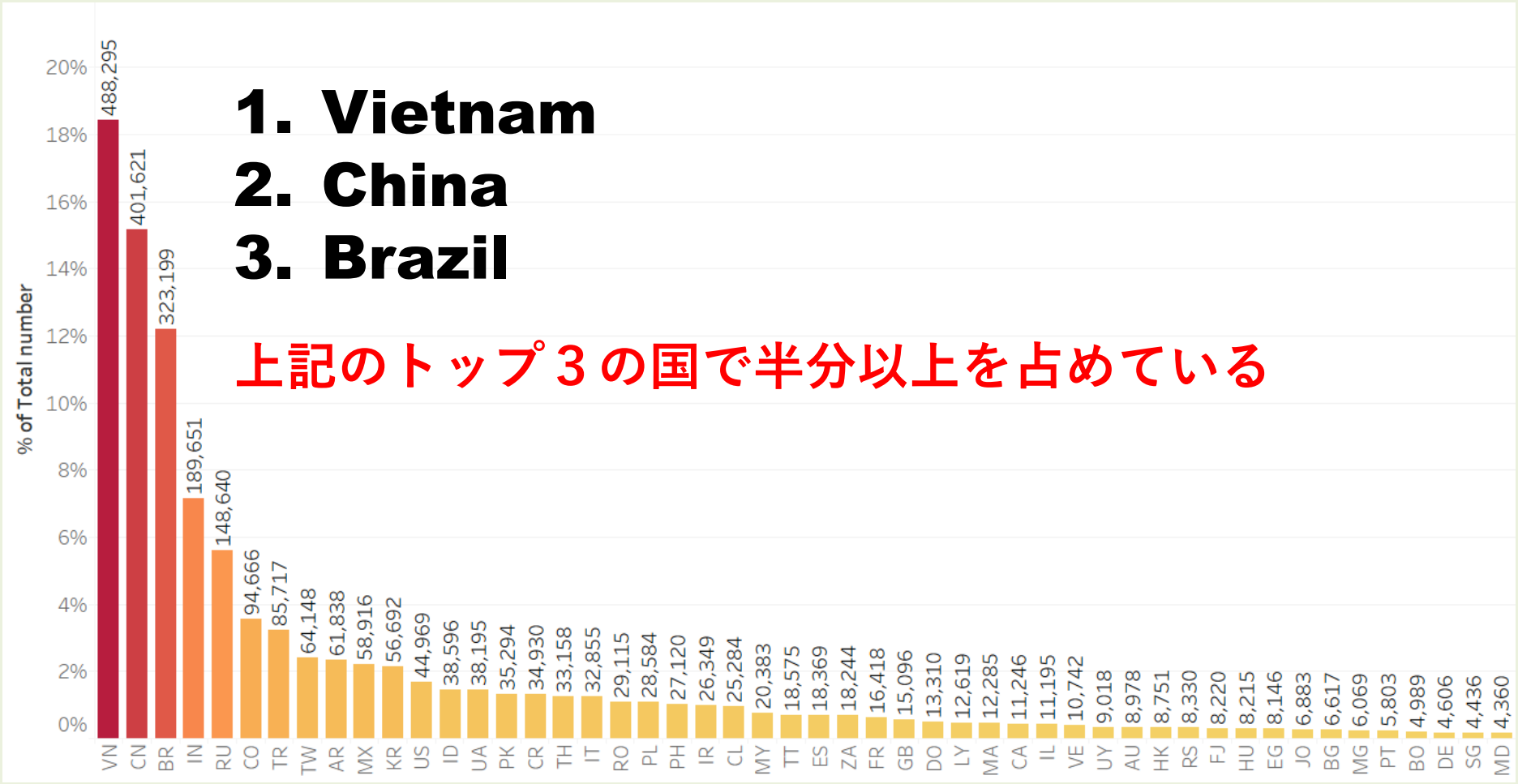
Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, “IoTPOT: Analysing the Rise of IoT Compromises,” 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015).

感染IoT機器の種別



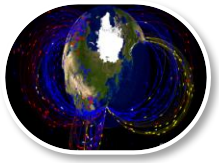
- ハニーに接続してきたIoTデバイスは、それが何かの詳細は多くが不明。
  - きちんと分類できた：10%以下
  - ７２種類の多種のIoT機器タイプ
    - ほとんとが IP cams と DVRs

IPアドレス数の観点から、感染国の状況

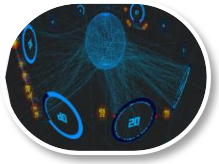


攻撃挙動の高度分析のための研究開発
-AI等の活用

事例：高度分析のためのデータ収集（NICT）



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

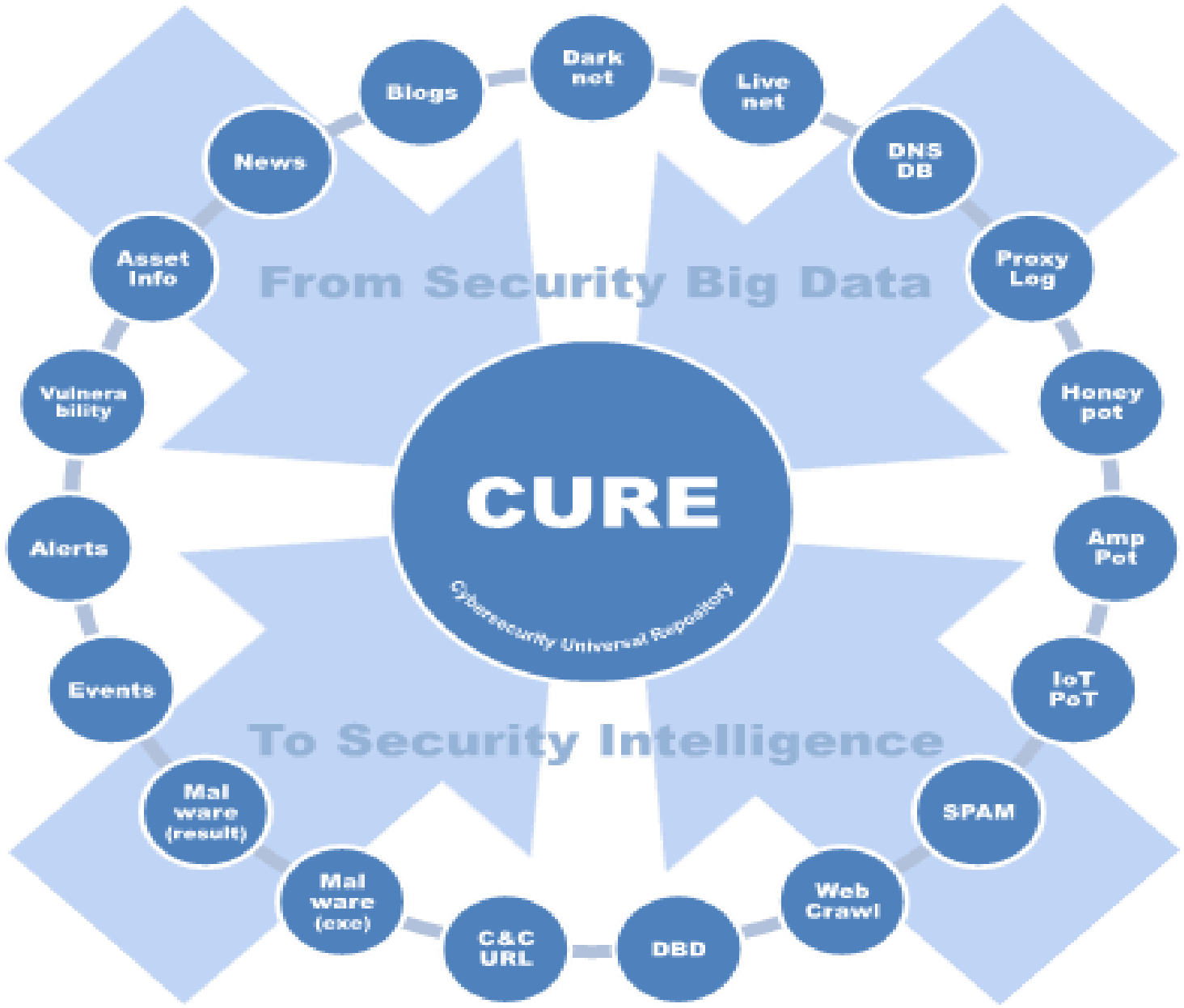
From Security Big Data

To Security Intelligence

CURE
Cybersecurity Universal Repository

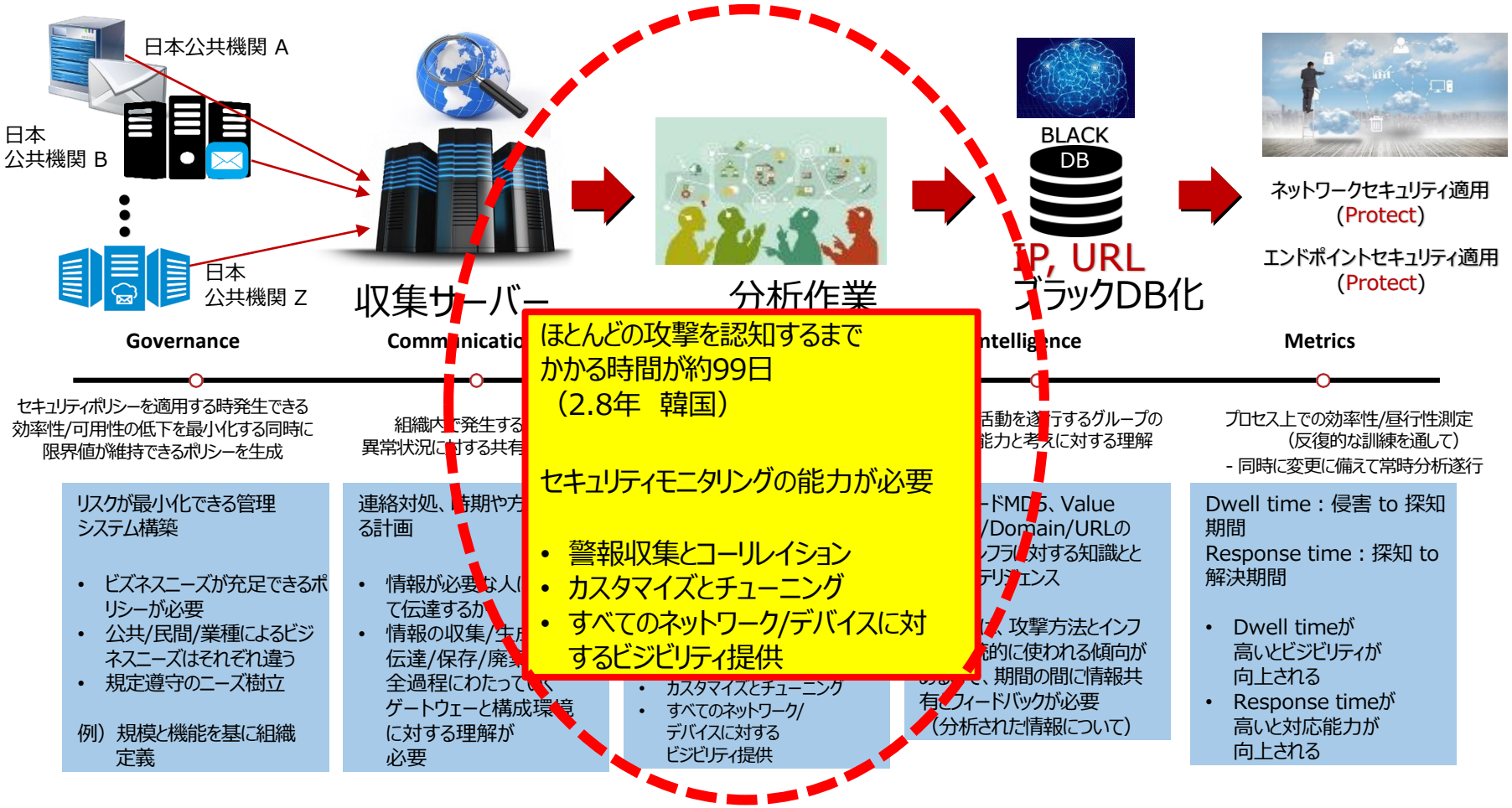
Dark net
Live net
DNS DB
Proxy Log
Honey pot
Amp Pot
IoT PoT
SPAM
Web Crawl
DBD
C&C URL
Mal ware (exe)
Mal ware (result)
Events
Alerts
Vulnera bility
Asset Info
News
Blogs

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE


From Security Big Data
CURE
Cybersecurity Universal Repository
To Security Intelligence
Dark net
Live net
Blogs
News
DNS DB
Asset Info
Proxy Log
Vulnera bility
Honey pot
Alerts
Amp Pot
Events
IoT PoT
Mal ware (result)
SPAM
Mal ware (exe)
Web Crawl
C&C URL
DBD

（例）Deepプロファイリング ＋ 常時分析と訓練実施（Response Architecture）

❖ メール基盤の悪性コードとAPT分析（Black IP & URL DB化）



追及すべき新たな研究開発の方向性

分析対象となるデータプラットフォームの構築：

- NICT　CURE（ダーク、ハニー、サンドボックス等）
- ICT-ISAC　AIS+ISACデータ
  （C2サーバ, DLサーバ、Domain,　マルウェアハッシュ、その他のオープン情報等）
- JPCERT/CC, IPA
- 海外の同様なシステムとの結合等

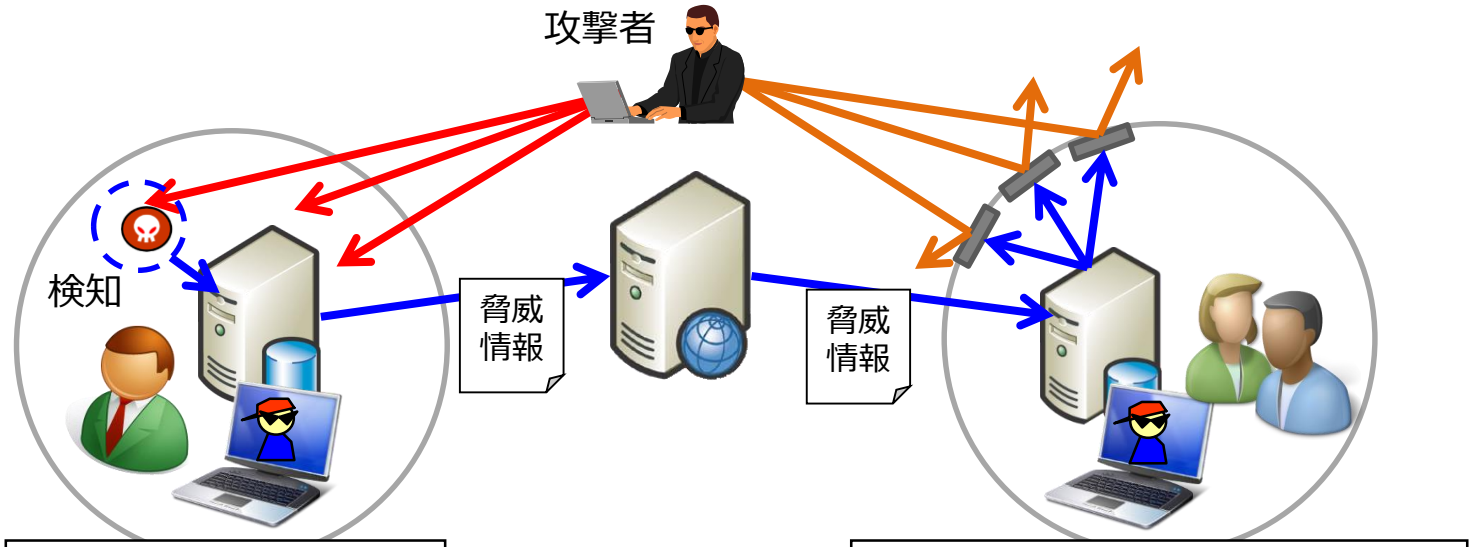
統合データに基づく高度分析の目指すもの：

- これまでの攻撃パターン・手法の把握と分類
- 新しい攻撃パターングループの検知
- 攻撃グループの全体像を把握
- 新規攻撃に対する深層データの提供

高度な情報共有化の視点で

多層防御としての(情報活用＋対策)

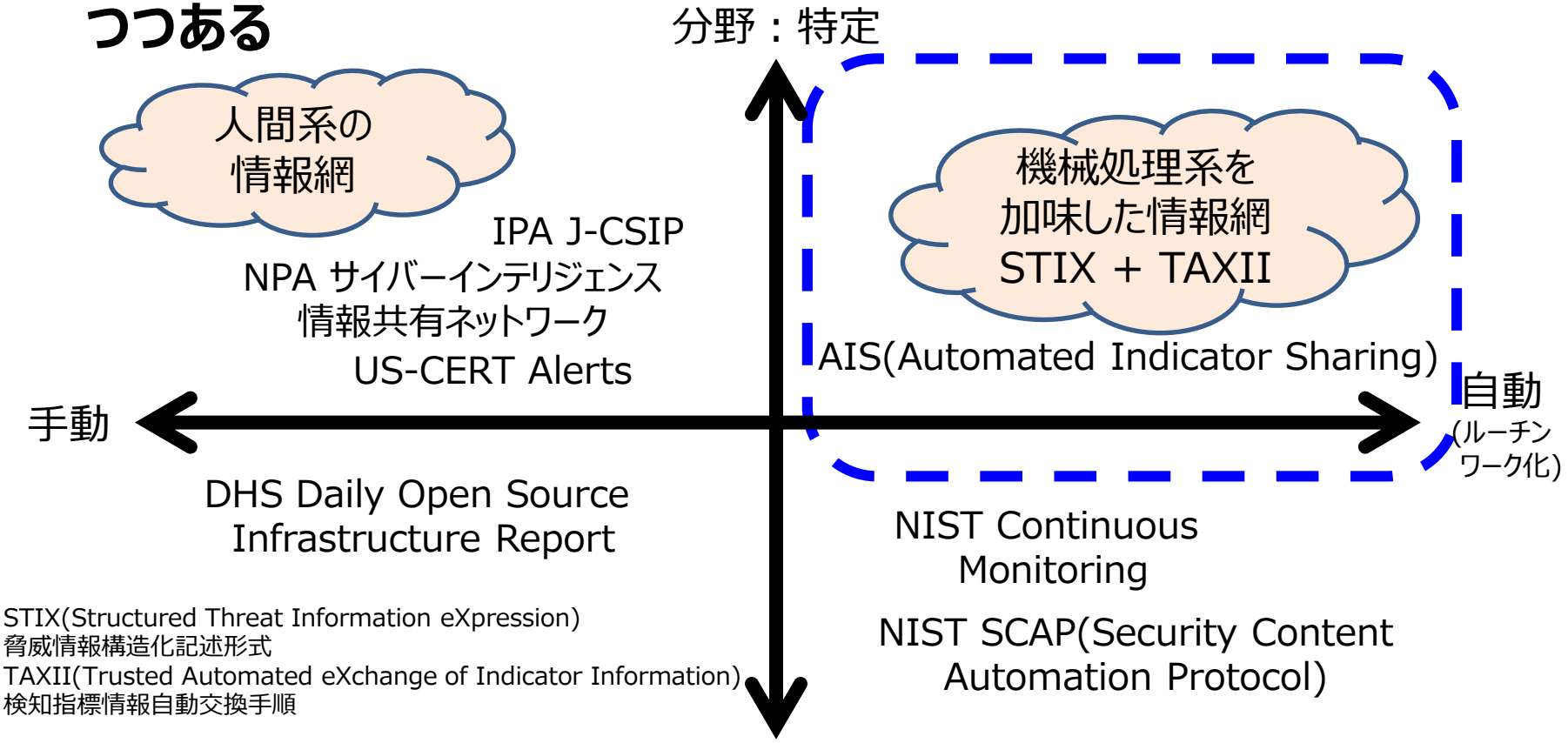
- **集団防御のための連携**
  - ✓ 事前措置：組織にサイバー攻撃が行われる前に(入手タイミング)、組織にない情報を利用して(カバー率)、サイバー攻撃対策につなげる。
  - ✓ 事後措置：組織にない情報を利用してサイバー攻撃による影響有無を特定する。



情報共有と機械化の潮流

米国での取り組みと情報共有の分類

- **機械利用を想定した大量の脅威情報が流通する仕組みが整いつつある**



STIX(Structured Threat Information eXpression)
脅威情報構造化記述形式
TAXII(Trusted Automated eXchange of Indicator Information)
検知指標情報自動交換手順

米国での取り組みと情報共有の分類

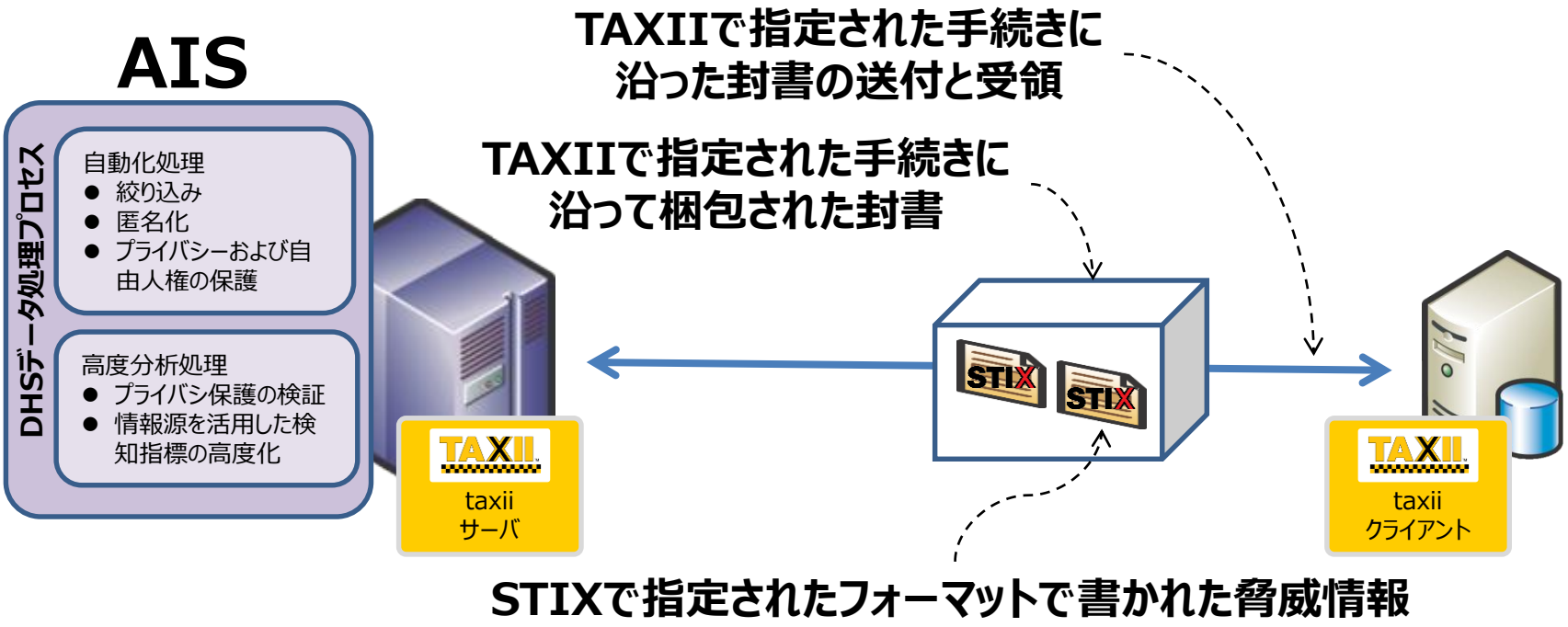
- **人手を介した連携vsシステムを介した連携**
  - 人手を介した連携(人間系の情報網、human readable)：高度な分析は可能ではあるが、情報を持っていても、即時的な対処につなげられない。
  - システムを介した連携(機械処理系を加味した情報網、machine readable)：高度な分析はできないが、情報があれば、即時的な対処につなげられる。人手で処理する場合、その人の技量によってしまう。ゆえに、技量によって左右されないシステム化は有用である。

	地震の場合	サイバー対策の場合
機械処理系を加味した情報網 machine readable	電子メールで配信される地震速報	STIX/TAXIIなどを用いたシステム化
人間系の情報網 human readable	気象庁が発表する会見	メール、SNSなどを用いた連携

情報共有と機械化の潮流

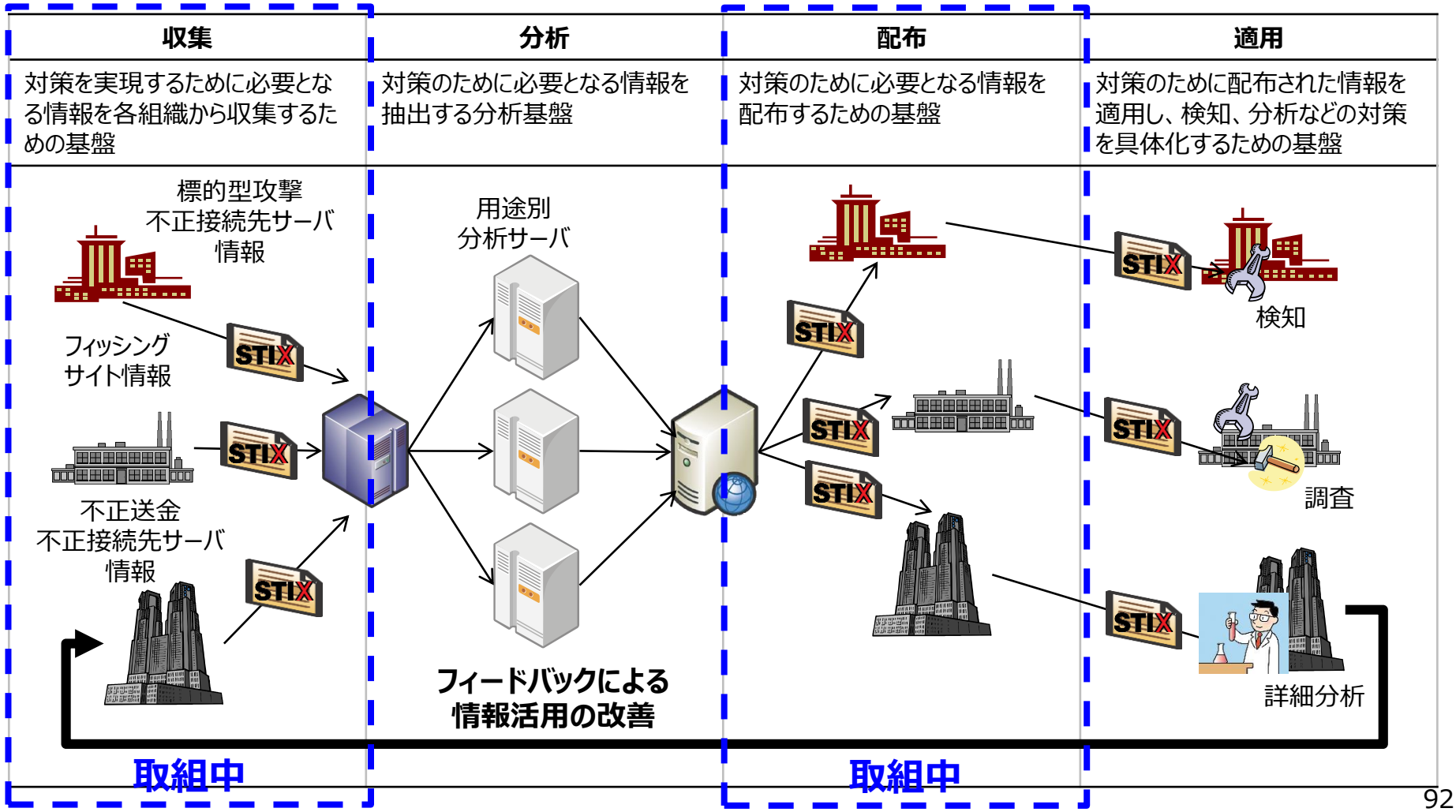
米国AIS(Automated Indicator Sharing)

- **米国政府が提供する官民連携の情報共有基盤**
  - 2015年サイバーセキュリティ法に基づき、2016年3月からDHSの下で活動を開始、攻撃指令サーバのドメインやIPアドレス、マルウェアのハッシュ値などの脅威情報を配信



ICT-ISACでの取り組み（例）

目標とする情報活用基盤



情報活用基盤

サイト taxii.ict-isac.jp

- システムを介した連携基盤(攻撃活動スピードへの追従)の整備
  - 2016年9月、情報活用基盤試行のため構築

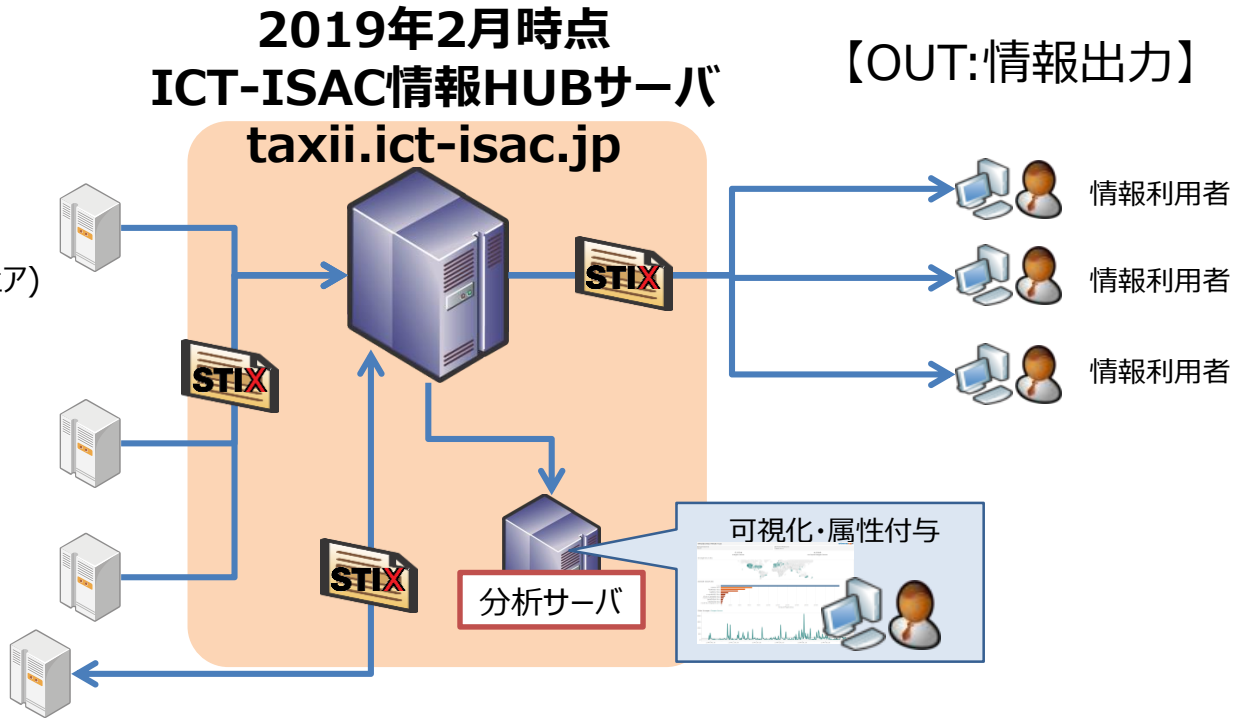
【IN:情報入力】

用途別-ISAC間
①情報通信事業者 検知情報
②金融事業者 検知情報
③ブロックリスト
④セキュリティベンダ(バンキングマルウェア)
⑤接続先解析システム

用途別-ISAC内
⑥ACTIVE(ICT-ISAC)
⑦PRACTICE(ICT-ISAC)

提供元別
⑧AIS(米)

用途別-ISAC間
⑨分散型不正接続先監視システム



【OUT:情報出力】

情報利用者
情報利用者
情報利用者

情報活用基盤

サイト taxii.ict-isac.jp

- システムを介した連携基盤(攻撃活動スピードへの追従)の整備
  - 2016年11月より、データ投稿を開始

種別		グループ [*]	内容
用途別	ISAC間	C2 (①、②)	taxii.ict-isac.jpを利用している組織が保有する動的解析装置が検知した不正接続先(ここで、C2は、ダウンローダサイトを含む広義のC２情報)
		BLOCKLIST (③)	組織で適用している不正接続先遮断リスト交換
		BKMW_* [バンキングマルウェア] (④)	セキュリティベンダ(動的解析装置が検知したデータ)から提供されたバンキングマルウェアに関する情報(マルウェアの設定ファイル配布サイト/攻撃対象金融機関サイト/マニュピレーションサーバ)
		VCITY (⑤)	**接続先解析システム(動的解析装置)が抽出した不正接続先**
		C2M_DL/UL (⑨)	**分散型不正接続先監視システム**
	ISAC内	PRACTICE (⑥)	DoS攻撃即応WGで取り扱う情報
		ACTIVE (⑦)	ACTIVE業務推進WGで取り扱う情報
提供元別		AIS (⑧)	AISから提供されている情報の一部を投稿
		FROM_JE-ISAC	電力ISACからの情報を受信する(試行用)
		TO_JE-ISAC	電力ISACに情報を通知する(試行用)

[*] 2019年2月時点で用意しているグループ(グループのことをフィード(Feed)と呼んでいる)

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
   - を理解）

2. 攻撃挙動の高度分析のための研究開発
   -AI等の活用
   - 度分析
   - 解析技術

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
   - 境などに
   - 策の自動化

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)

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!!