資料2-3

サイバーセキュリティに関する総務省の取組

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第15回

令和２年11月
総務省

NICTにおけるサイバーセキュリティ分野の研究マップ

- 急増するサイバー攻撃から社会システム等を守るサイバーセキュリティ分野の技術の高度化が不可欠となっていることを踏まえ、 NICTにおいて研究開発を推進。
- 受動的/積極的な観測技術、標的型攻撃対策（Local）、無差別攻撃対策（Global）など、技術の種類を問わず、研究開発に取り組む。
- 更なる高度化を図るため、各研究分野においてAIを積極的に活用。

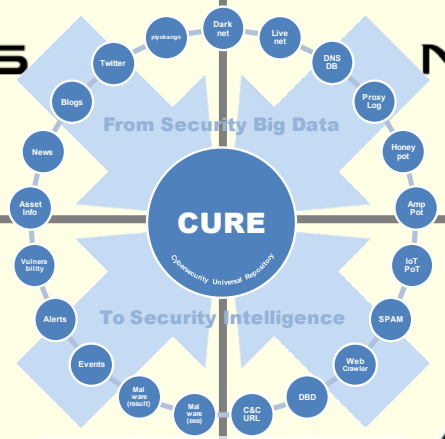
インシデント分析センター（ニクター）
NICTER

対サイバー攻撃アラートシステム（ダイダロス）
DAEDALUS

Passive

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



Global

Local

リフレクション攻撃専用ハニーポット
AmpPOT※1

IoTマルウェア専用ハニーポット
IoTPOT※1

※1 横浜国立大学/独Saarland大との共同研究

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE ※2

Active

※2 サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする技術

AIを活用したサイバーセキュリティの高度化

STARDUST

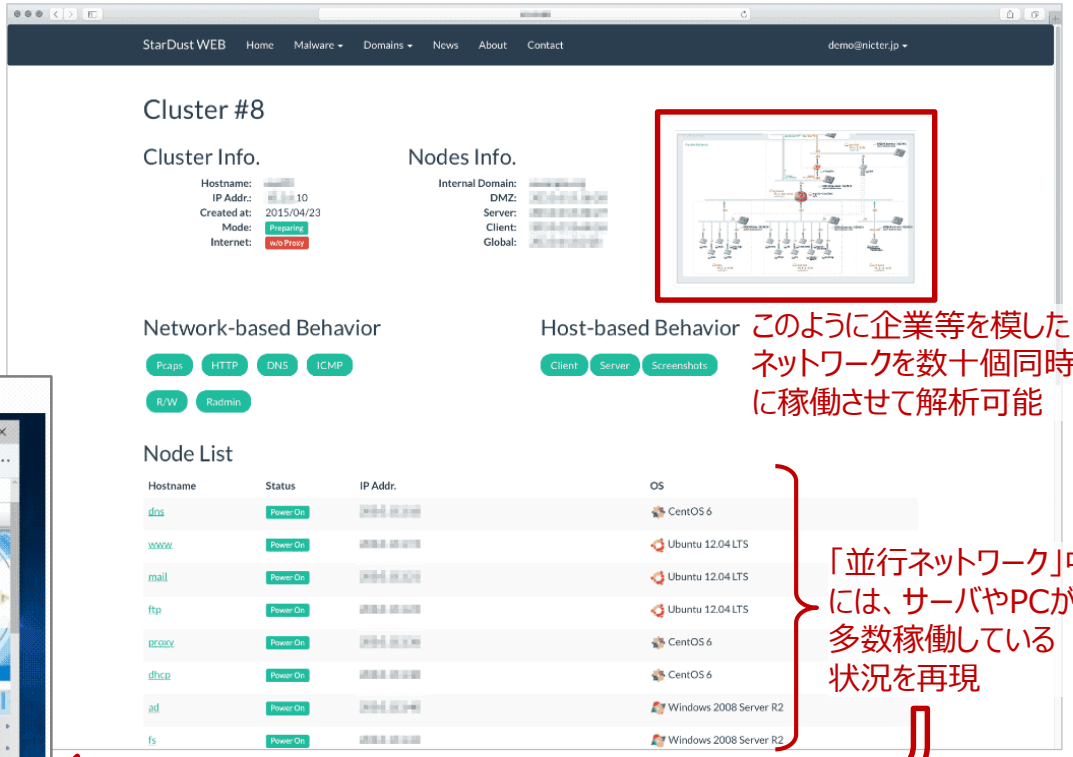
- 組織を精巧に模擬した「並行ネットワーク」を高速・柔軟に自動生成し、標的型攻撃等の攻撃者を誘い込むサイバー攻撃誘引基盤。
- マルウェアに感染させた後の攻撃者の挙動も含めて、攻撃者に気づかれず、リアルタイムに観測・分析可能。

＜並行ネットワーク＞

攻撃者に標的先と誤認させ、攻撃を誘因するためのいわゆる「社内LAN」環境を構築。

- ✓ 政府や企業等を精巧に模した模擬環境
- ✓ 各種サーバやPCが数十台～数百台稼働
- ✓ 数十の並行ネットワークを同時稼働可能

並行ネットワークの画面イメージ



このように企業等を模したネットワークを数十個同時に稼働させて解析可能

「並行ネットワーク」中には、サーバやPCが多数稼働している状況を再現

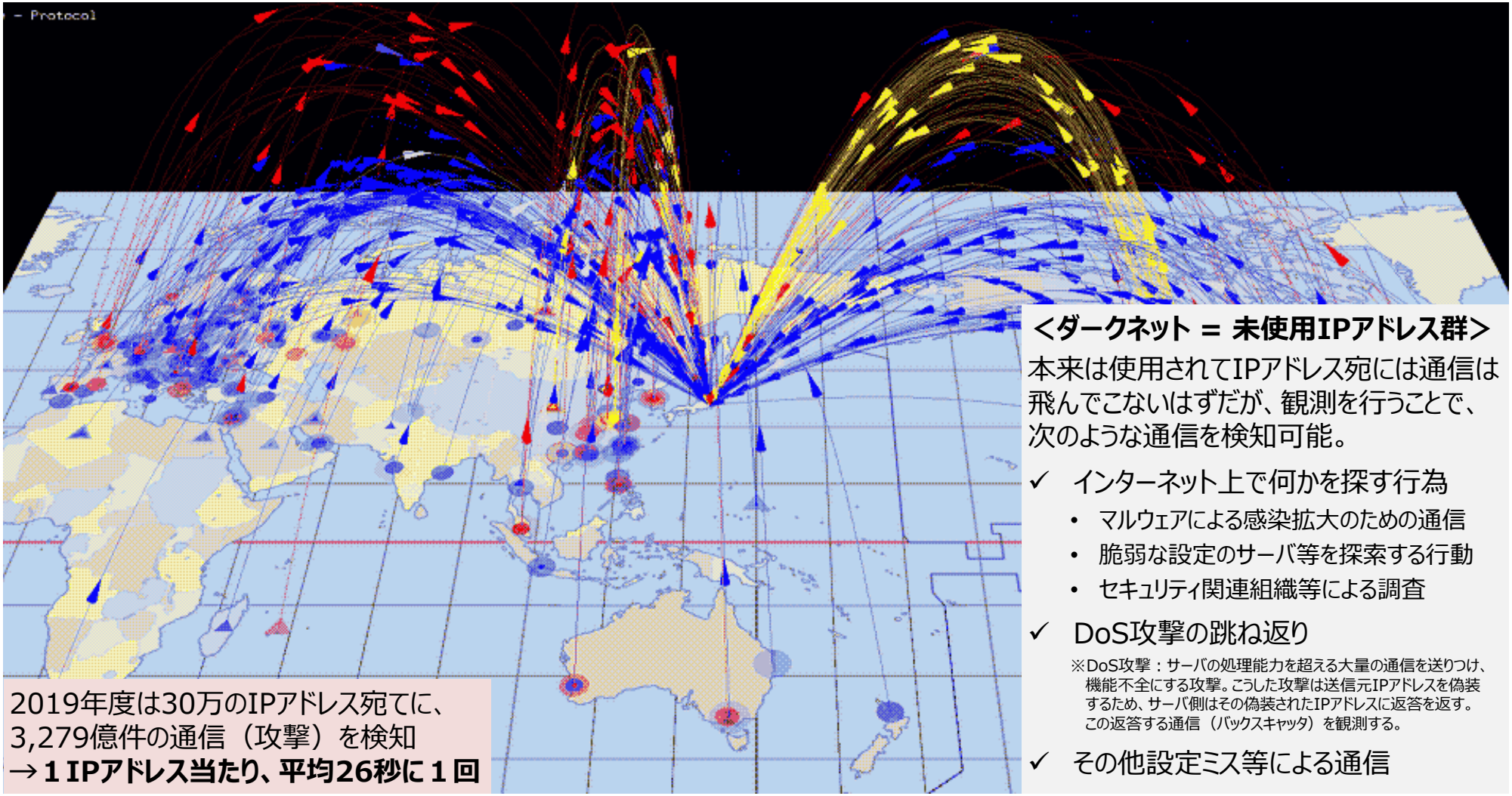
並行ネットワーク内で稼働するPC等のイメージ

組織における情報資産を模した模擬情報（重要に見えるファイル等）を配置し、さも利用者が使っているかのような状況を再現。攻撃者の挙動をステルスに観測。

NICTER

Network Incident analysis Center for Tactical Emergency Response

- 無差別型サイバー攻撃を、リアルタイムかつ大規模に観測・分析するシステム。
- 国内外の30万の未使用IPアドレスからなる「ダークネット」により攻撃を観測。



2019年度は30万のIPアドレス宛てに、
3,279億件の通信（攻撃）を検知
→１IPアドレス当たり、平均26秒に１回

＜ダークネット = 未使用IPアドレス群＞

本来は使用されてIPアドレス宛には通信は飛んでこないはずだが、観測を行うことで、次のような通信を検知可能。

- ✓ インターネット上で何かを探す行為
  - マルウェアによる感染拡大のための通信
  - 脆弱な設定のサーバ等を探索する行動
  - セキュリティ関連組織等による調査
- ✓ DoS攻撃の跳ね返り

※DoS攻撃：サーバの処理能力を超える大量の通信を送りつけ、機能不全にする攻撃。こうした攻撃は送信元IPアドレスを偽装するため、サーバ側はその偽装されたIPアドレスに返答を返す。この返答する通信（バックスキャッタ）を観測する。

- ✓ その他設定ミス等による通信

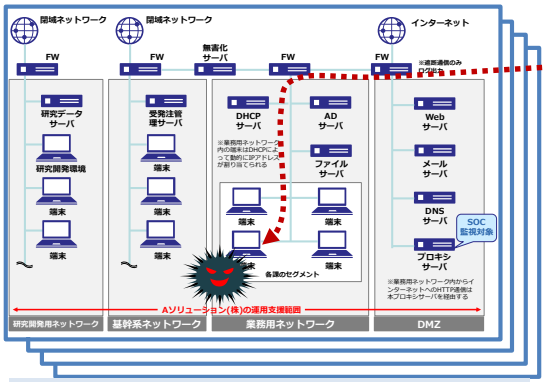
実践的サイバー防御演習（CYDER）

CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材・データを使用して**本番同様の作業**を実施

インシデント（事案）対処能力の向上

令和２年度の実施計画

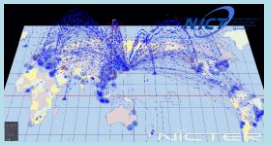
※このほか、令和３年１月頃から未受講の地方公共団体を対象としたオンライン演習を導入予定

コース	受講対象組織	対象者	開催地	開催回数	実施時期
Aコース（初級）	全組織共通	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	７１回	８月～翌年２月
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	２０回	10月～翌年２月
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋・福岡	１５回	１月～翌年２月

サイバーセキュリティ統合知的・人材育成基盤

➢ サイバーセキュリティ情報を**国内で収集・蓄積・分析・提供**するとともに、**社会全体でサイバーセキュリティ人材を育成する**ための共通基盤をNICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。

STARDUST
サイバー攻撃誘因基盤

NICTER

サイバー攻撃観測網

各種外部情報


CYDER
実践的サイバー防御演習

サイバーコロッセオ
オリパラ関係者向けサイバー演習

民間が有する各種演習教材

成果展開

成果展開

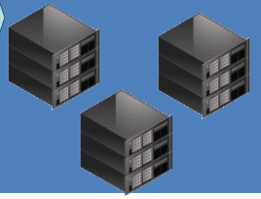
教材変換インタフェースの開発・標準化

サイバー攻撃分析環境


情報

大規模集約データベース


情報

セキュリティ機器テスト環境


最新の攻撃情報（演習教材に反映）

相互補完

受講者の挙動（攻撃分析に活用）

演習教材提供環境


演習用大規模計算機環境
受講者挙動DB


AIを駆使した大規模横断分析＋付加価値の付与

根拠・背景等が
説明可能な国産セキュリティ情報

提供

政府機関・セキュリティ機関等

- マルウェア情報
- 指令サーバ情報
- 攻撃元IPアドレス情報
- 攻撃者/攻撃手法情報 等

コミュニティ形成による連携

人材育成事業者 | 教育機関 | ICTベンダ

安全な無線通信サービスのための新世代暗号技術に関する研究開発

➢ 5G等の高度化において、大規模量子コンピュータ等に解読されないよう、①ＬＴＥと同等の安全性を確保しつつ、超高速・大容量に対応した共通鍵暗号方式、②5G等の特性を損なわないよう、5G等のユースケースに応じた耐量子計算機暗号（PQC）への機能付加技術等を確立することで、無線通信リソースの効率的な利用環境を提供することにより、無線リソースのひっ迫を抑止し電波の有効利用を図る。

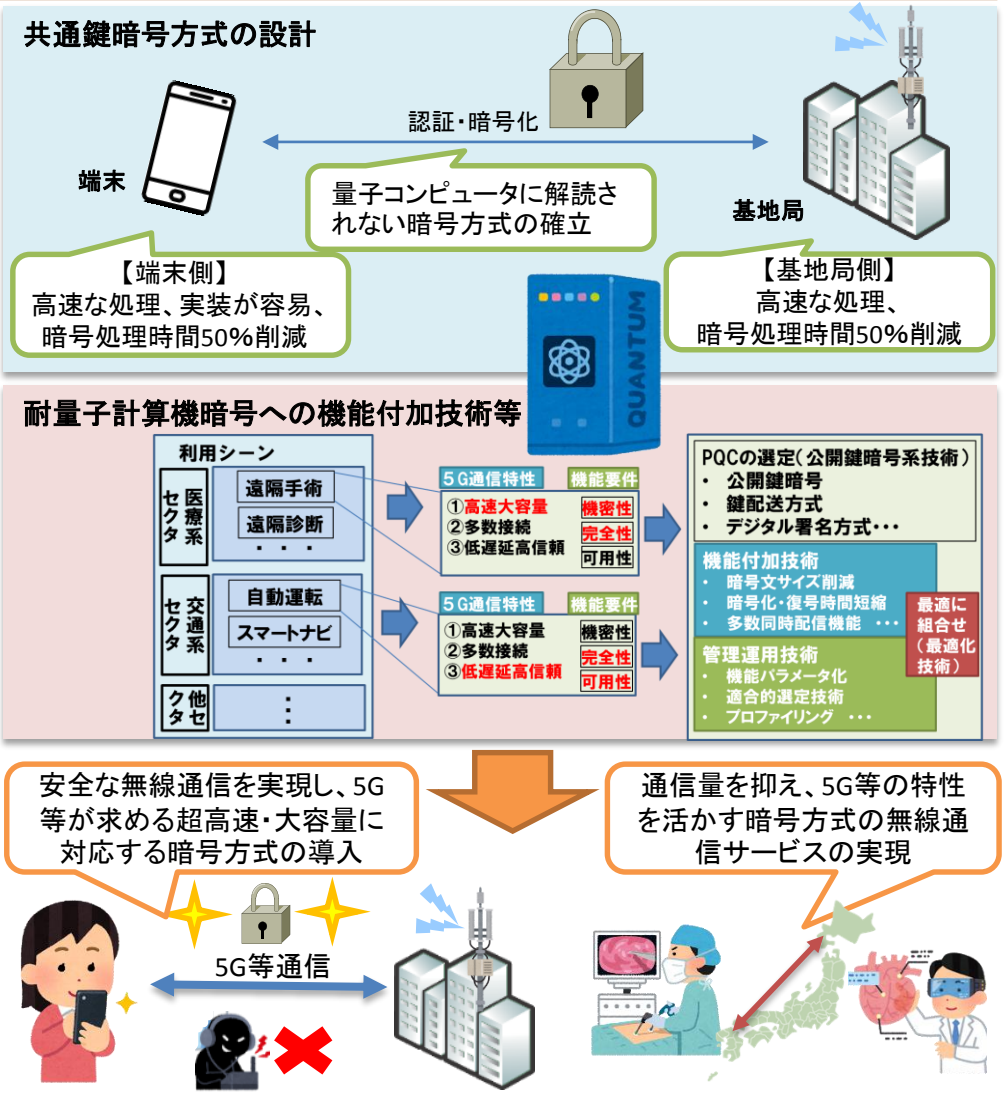
【背景・課題】

・大規模量子コンピュータ等が実用化されると、共通鍵暗号方式においては、ＬＴＥと同等の安全性を確保するためには鍵長を増加する必要があるが、スマートフォン等の限られた情報処理能力の中で5G等が求める高速・大容量に対応した暗号方式の設計が課題である。

・また、公開鍵暗号方式においては、高速な解読が可能となるため、PQCへの移行が必要である。今後、複数の暗号方式が採用される予定であるが、5G等のユースケースに応じて最適化し、スマートフォン等の計算資源や通信量を抑えるようにPQCへの機能付加等が必要である。

【実施内容】

大規模量子コンピュータ等に解読されないよう、①ＬＴＥと同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応できる共通鍵暗号方式、②5G等のユースケースに応じ、通信データ量を抑え、PQCへの機能付加技術等を確立し、無線通信の効率的な利用環境を提供することにより、電波の有効利用を図る。



５Ｇネットワークの脆弱性対策

➢ IoTシステムの基盤技術である５Ｇネットワークにおいて、ハードウェア上に故意に組み込まれた不正なチップは、国民の安心・安全を阻害する深刻な脅威となることから、チップの設計・製造における脆弱性を検知する手法を整備し、５Ｇを活用する重要インフラ事業者やチップ製造ベンダ等への周知・啓発を図る。

【背景・課題】

○ 電子機器のハードウェア上に故意に組み込まれた脆弱性（ハードウェアトロイ）のリスクが増大している。

○ ５Ｇネットワークを構成するハードウェア上に組み込まれた不正なチップは、製品出荷後に交換・修正することが難しく、その影響は極めて深刻なものとなりうる。

○ 通信事業者等５Ｇを活用する重要インフラ事業者や、チップ製造ベンダ等が、設計・製造におけるチップの脆弱性を検出し、必要な対策を実施できる体制の整備が急務となっている。

【実施内容】

① 電子機器を構成するチップについて、不正に改変された回路の検知技術及び対応策の検証を実施。

② 回路情報が入手できないチップについて、電子機器の外部から観測される情報により不正動作を検知する技術及び対応策の検証を実施。

③ 不正検知AIに対する攻撃（敵対的サンプル）を想定した検証を実施。

④ ５Ｇネットワーク上での運用面の手順等について検討。

＜不正なチップの脅威と検知技術のイメージ＞