サイバーセキュリティ対策の高度化
AIを活用したサイバー攻撃対策技術の開発

官民研究開発投資拡大プログラム（PRISM）

AI技術領域

令和元年度成果

令和２年７月

総務省

設計・製造における
チップの脆弱性検知手法の研究開発

資料1　「設計・製造におけるチップの脆弱性検知手法の研究開発」の概要

アドオン額：200,000千円（総務省）
元施策・無 / PRISM事業・新規

課題と目標

- IoT機器に搭載されたソフトウェアだけでなく、ハードウェアのセキュリティを含めたサプライチェーン全体のセキュリティの確保が課題。
- ハードウェアチップの設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での運用技術を確立するとともに、当該技術の社会実装を加速する。

「設計・製造におけるチップの脆弱性検知手法の研究開発」の概要

- PRISMで実施する理由：
  電子機器の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になる可能性があることから、サプライチェーン上の脅威となっている。また、チップに仕込まれた不正な回路や部品を検出する技術は確立しておらず、産学官で連携して研究開発を加速し、社会実装を進めることが急務となっていることから、PRISMにより研究開発を前倒しで開始した。
- テーマの全体像：
  統合イノベーション戦略推進会議において2019年６月に決定した「ＡＩ戦略2019　～人・産業・地域・政府全てにＡＩ～」に基づき、サプライチェーンでチップ脆弱性を検知、安全性を保証するしくみの実用化・事業化を目指し、本研究開発を実施した。また、不正回路・機械学習エンジンデータベースの構築と国内外の他の機関など外部連携の拡大、国際的ハブの形成等を通じて、民間研究開発投資誘発に貢献する。

出口戦略

- ハードウェアチップの設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での運用技術を確立するとともに、当該技術の社会実装を加速する。
- 技術確立・普及段階：Web サイトや国際的ハブなどの活動を通じて、開発する技術の必要性とこれらの技術を組み込んだ社会システムの構成についての普及啓発を行う。
- 実用化・事業化段階：本技術のパテント・コンソーシアムの構築、または、ライセンシング枠組みの構築を行う。また、ハードウェアトロイの監査・認証スキームの事業化や他の監査・認証団体への当該スキームの委託・ライセンス提供を行う。

民間研究開発投資誘発効果等

- 本研究開発成果によりハードウェアチップの安全性が向上し、海外からの信頼性・需要が高まり、日本でのセキュアなチップ設計やシステム設計に関する民間投資の促進が見込まれる。
- 民間からの貢献額：令和元年度末時点では、各研究開発機関において、人件費、機器の提供等、計約1.1億円の貢献見込み
  ・内訳：（人件費）70百万円、（機器費等）40百万円

資料2　「設計・製造におけるチップの脆弱性検知手法の研究開発」の概要

施策全体像

n 技術開発

① 外部から調達した設計ツールや設計部品を用いたチップ設計全体の安全性を担保するために、回路情報の中に不正に改変された回路が含まれるか、機械学習等のAIを活用して検知する技術を開発。

② 市販の組込みマイコン等の安全性を担保するために、不正回路が組み込まれたチップにより構成される電子機器に対し、電力波形の特定部分の電力量や継続時間等、電子機器の外部から観測される情報を用いて、不正動作を機械学習等のAIを活用して検知する技術を開発。

n 社会実装

サプライチェーンの起点となるハードウェアチップの設計・製造における脆弱性検知手法を確立し、90%以上の精度で不正有無の判定を行う検知システムを実装する。通信事業者や各種半導体メーカ・回路開発ベンダと連携し、システムを利用して開発した安全性の高いチップを実用化し、流通を促進する。

n 関係するSIP施策

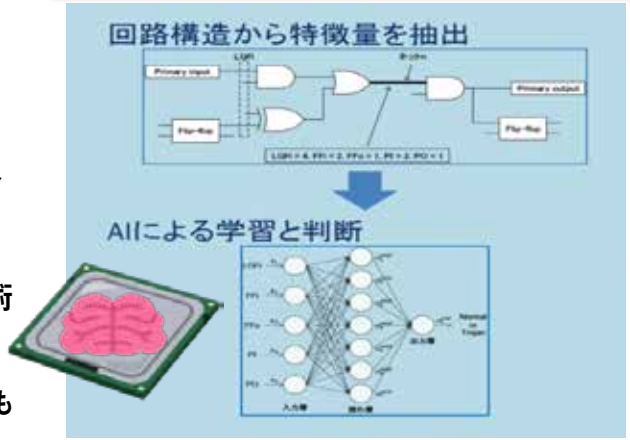
SIP第２期　IoT社会に対応したサイバーフィジカルセキュリティ：「IoTサプライチェーンの信頼の創出技術基盤の研究開発」

SIPによる技術と相互補完し、SIPが目指す、サプライチェーン全体を通じたセキュリティの確保に資する。

・SIP：ゴールデンチップ（正常と確認された回路）あるいはその設計図面がある前提で、そこから逸脱するものを検知する。

・PRISM：不正な回路を検知する（ゴールデンチップは必要としない）

AIにより，既知・未知の不正回路を検知する技術開発が急務



スケジュール

（最終目標）不正でない回路を不正と判定する誤検知率が5%以下という条件のもと、不正回路を見逃す見逃し確率10%以下

	実施項目	令和元年度	令和2年度	令和3年度	令和4年度
課題Ⅰ	ア）不正回路を識別するための特徴量抽出技術	標準ベンチマークを対象	実回路等、対象を拡大		
	イ）AI/機械学習に基づく不正回路検知技術	FPGA開発ボードを対象	FPGA搭載電子機器等、対象を拡大		
課題Ⅱ	ア）外部情報を取得する電子機器の動作のモデル化技術		単一チップによる動作モデル化	複数チップによる動作モデル化と実回路適用	
	イ）AI/機械学習に基づく不正動作検知技術		単一チップによる不正動作検知	複数チップ・実回路による不正動作検知	

（最終目標）正常動作を不正動作と判定する誤検知率が5%以下という条件のもと、不正動作を見逃す見逃し確率10%以下

資料3　「設計・製造におけるチップの脆弱性検知手法の研究開発」の目標達成状況

- 回路情報を用いて不正回路を検知する技術（不正回路検知技術）及び電子機器の外部から観測される情報を用いて不正動作を検知する技術（不正動作検知技術）を確立することを最終目標とする。
- 令和元年度において、不正回路検知技術では、標準ベンチマーク回路をもとに見逃し確率20%以下、誤検知率5%以下の特徴量抽出技術の開発を完了した。また、不正動作検知技術では、単独の組込みマイコンから構成される比較的簡易な電子機器の動作をモデル化し、不正動作を検知するアルゴリズムの開発を完了するとともに、高精度アナログ計測モジュールの設計・実装を完了した。

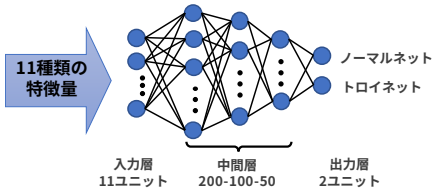
	研究内容	令和元年度目標	目標の達成状況
課題Ⅰ不正回路検知技術	ア）不正回路を識別するための特徴量抽出技術	回路設計に標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路と不正でない回路を識別するための特徴量を抽出する技術を開発する。	• 11種類の不正回路の特徴量を抽出。Trust-HUBベンチマーク回路（大規模ベンチマークを含む）に対して、多層ニューラルネットワークを用いることで、TPR85%程度、TNR95%以上の識別成果（見逃し確率15%程度、誤検知率5%以下、すでに実用レベル） • ハードウェアトロイの機能ごとに、サプライチェーン上の影響の分析を実施。情報の機密性及び安全性を脅かす機能について、サプライチェーン上流のメーカに法的責任が生じ得るため、実用化・社会実装において対応すべきことを確認。
	イ）AI/機械学習に基づく不正回路検知技術	ベンチマーク回路等を用いて、AIにより回路情報から不正回路を検知する技術を開発する。	• 課題Ⅰア）と連携して、回路情報から不正回路を検知する技術を開発。 • 不正回路の動作・有効化方法等の体系化を完了。 • IoT開発ボード、FPGA開発ボード、FPGA搭載ネットワークカードを対象とした計12種類の不正回路のサンプル実装を完了。 • 亜種の不正回路の回路情報を自動生成する亜種生成ツールを開発。
課題Ⅱ不正動作検知技術	ア）外部情報を取得する電子機器の動作のモデル化技術	単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するような電子機器の外部情報の特徴量を抽出する技術を開発する。	• 組込みマイコンの動作をモデル化し、不正動作検知アルゴリズムを構築。 • 同モデル上で、複数の組込みマイコンについて不正動作検知に成功し、目標達成。
	イ）AI/機械学習に基づく不正動作検知技術	単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するように、AIにより外部情報から不正動作を検知する技術の基本検討を行う。	• 電子機器の電力波形計測に必要となる、計測精度0.1mW刻み、サンプリング精度1kHzの高精度アナログ計測モジュールのプロトタイプの設計・実装を完了。計測精度の目標達成。 • HDL（Hardware Description Language）開発効率化を目的とした高位合成ツールの導入完了。利用するゲートアレイの検討等、研究開発環境の導入完了。 • 不正ハードウェアならびに不正ソフトウェアについて、実際の市場においてどのような事例が存在するかについて実態調査完了。

資料4　「設計・製造におけるチップの脆弱性検知手法の研究開発」の成果

課題Ⅰ－ア）①不正回路を識別するための特徴量抽出技術に関する要素技術開発

- ベンチマーク回路を使い、11種類の特徴量を用いることで、ニューラルネットワーク識別器によるトロイ信号線を識別（識別した信号線数は合計で数十万以上のデータ）

多層ニューラルネットワークを用いた識別結果
TPR（True Positive Rate） 84%以上、TNR（True Negative Rate） 95%以上（見逃し確率16%以下、誤検知率5%以下）



課題Ⅰ－ア）②設計・製造におけるチップの脆弱性検知手法に関する動向調査

- ハードウェアトロイの機能ごとに、サプライチェーン上の影響の分析を実施し、研究開発の実用化に反映
- Ø 情報の機密性及び安全性を脅かす機能はサプライチェーン上流のメーカに法的責任が生じ得るため、対処が必要
- Ø 今後の実用化・社会実装に向け、機密性を損なう回路／派生回路および安全性を損なう回路／派生回路を検知する技術を確立する

課題Ⅰ－イ）AI/機械学習に基づく不正回路検知技術

(1) 不正回路の体系化を完了
・Trust-HUBから取得した88個のサンプルを詳細に分析し、分類

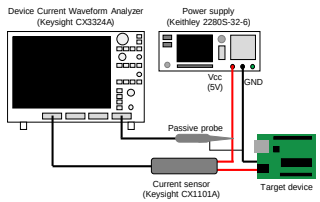
(2) 不正回路の新規サンプル(12種類)の実装を完了
・IoT開発ボード向け6種類、FPGA開発ボード向け3種類、FPGA搭載ネットワークボード向け3種類を実装



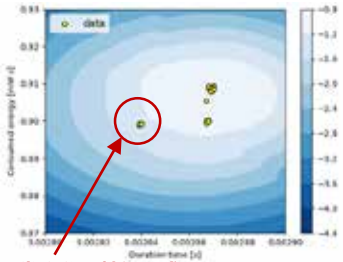
(3) 亜種生成ツールを開発
・不正回路の回路情報（ゲートレベル記述のVerilog-HDL）から、亜種の回路情報を自動生成するツールを開発。

課題Ⅱ－ア）外部情報を取得する電子機器の動作のモデル化技術

(1) 単一組込みマイコンの動作モデル化
(2) 消費電力を利用した異常動作の検知手法の確立
(3) 複数の組込みマイコンを用いた異常動作検知の実証



動作モデルのもと、組込みマイコンの異常動作検知に成功



異常動作の検知に成功

課題Ⅱ－イ）AI/機械学習に基づく不正動作検知技術に関する研究開発

(1) 高精度アナログモジュールの実装
(2) AI実現のための事前調査の実施
(3) 分野横断的な電子機器の調査と不正プログラムの動向調査の実施

高精度アナログモジュールの実装
目標：サンプリング1kHz, 電力測定誤差±0.1mWに対して
サンプリング5kHz, 電力測定誤差±0.01mWまで実現。外部に接続した電子機器の電力の特徴量を計測可能。5kHzになった場合においても電子機器の電力特徴量を捉える事は可能。

AI実現のための事前調査の実施
AI機能についてニューラルネットワークをFPGAに対して現実的な数となるか検討。事前研究結果からFPGAのLUT数の要求数を検討したところ、15,000個のLUTを用意する事で可能。

電子機器に利用されるICチップの調査と不正プログラムの動向調査の実施
不正プログラムは複数アーキテクチャにおいて1000個の不正ソフトウエアの収集を行った。電子機器に利用されるICチップの調査にてICチップそのものを不正にコピーして流通させることが行われている事から、不正回路の実在を裏付ける脅威として捉える

資料5　「設計・製造におけるチップの脆弱性検知手法の研究開発」の民間からの貢献及び出口の実績

n 民間からの貢献額は、1年で計約1.1億円相当。詳細については以下のとおり。
①人件費
- 本研究開発に関わる技術調査等の自己負担分（15名程度、70百万円相当）

②機器費等
- 本研究開発で使用する機器のうち、PC、サーバ、計測機器、FPGAボード等については、一部自己負担で用意（40百万円相当）

令和元年度当初見込み	令和元年度実績
①人件費・・・・本研究開発に関わる技術調査等を自己負担する（70百万円程度）	①人件費・・・・本研究開発に関わる技術調査等の自己負担分 内訳：常勤14名、非常勤1名など 合計：70百万円相当
②機器費等・・・・本研究開発で使用する機器の一部を自己負担で用意する（40百万円程度）	②機器費等・・・・本研究開発で使用する機器の自己負担分 内訳：PC4台、サーバ1台、計測機器2台、FPGAボード14台など 合計：40百万円相当

n 出口戦略
- ハードウェアチップの設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での運用技術を確立するとともに、当該技術の社会実装を加速する。
- また、安全なハードウェアチップの設計・製造に関する特許取得、業界標準化、国際標準化を通じて、同分野における我が国の国際競争力を図る。
- 目標の達成に向け、①設計・製造におけるチップの脆弱性検知手法の確立（数値目標）、②サプライチェーン上での運用技術の確立と社会実装の加速技術、③特許取得・業界標準化等を通じた我が国の国際競争力強化のアウトカム目標を設定した。

令和元年度当初見込み	令和元年度実績
①設計・製造におけるチップの脆弱性検知手法の確立（数値目標）・・・・標準ベンチマーク回路を元に、不正でない回路を不正と判定する誤検知率が5%以下（=TNR95%以上）という条件のもと、不正回路を見逃す見逃し確率20%以下（=TPR80%以上）を実現する特徴量抽出技術を確立し、AIにより回路情報から不正回路を検知する技術を開発する。また、単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するような電子機器の外部情報の特徴量を抽出する技術を開発し、AIにより外部情報から不正動作を検知する技術の基本検討を行う。 ②サプライチェーン上での運用技術の確立と社会実装の加速・・・・研究開発運営委員会等を通じて、ハードウェアトロイ検知に関する取り組みを調査し、検知技術の開発及びサプライチェーンでチップ脆弱性を検知、安全性を保証するしくみの方向性を検討する。 ③特許取得・業界標準化等を通じた我が国の国際競争力強化・・・・研究開発運営委員会等を通じて、標準化の方向性を検討する。	① いずれの数値目標についても達成。ハードウェア脆弱性の検証を実運用している半導体設計メーカと意見交換を行い、令和元年度に達成した数値目標（TNR95%以上、TPR85%程度）であっても、ハードウェアトロイ特定に実用レベルで利用可能性がある旨確認した。 ② ハードウェアトロイのサプライチェーンセキュリティを確保するための既存の仕組み（標準や認証）に関して調査を行うとともに、ハードウェアトロイに着目した場合に、チップのサプライチェーン上での安全性確保のため、どういった脅威を対象とするべきか調査を行った。諸外国の法制度等を調査した結果、(1)情報の機密性に関するものと(2)機能の変更・妨害を行うものを対象と特定し、これらの脅威に基づく研究開発実施のため、フィードバックを行った。 ③ ISO/IEC JTC 1/SC 27/WG3への寄書のドラフトを作成し、ISO/IEC SC27会合(2020年4月)にて、本プロジェクトの成果を紹介した。また、同WG3で検討されているハードウェアセキュリティに関するSPの共同ラポーターに就任した。

サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発

資料1　「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の概要

アドオン額：200,000千円（総務省）
元施策・無 / PRISM事業・新規

課題と目標

- マルウェアの感染は世界的な社会問題となっており、政府、重要インフラなどの組織に対する脅威は増加の一途をたどっている状況であるが、マルウェア感染挙動の早期把握や、それらの情報を関連組織間で効果的に共有化できていない。
- 多くの手段により収集したデータに基づき、AI技術を駆使することにより、マルウェアの攻撃挙動の解析を自動化し、重大なインシデントになる前に挙動解析を完了し、早期警戒情報を導出する。また、ISAC組織等との情報共有・連携を進め、マルウェアによる被害の低減に資する。

「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の概要

- PRISMで実施する理由
  マルウェアによる攻撃活動の観測・収集は多くの手段で行われているが、それらを有機的に分析し、攻撃の初期挙動を捉えて関係者と的確に共有することはできていない。大量のIoT機器に感染したマルウェアによる大規模な攻撃が発生しており、攻撃の初期挙動を的確に把握し、早期警戒情報として関係者に共有することは喫緊の課題であることから、PRISMにより研究開発を前倒しで開始した。
- テーマの全体像
  統合イノベーション戦略推進会議において2019年６月に決定した「ＡＩ戦略2019　～人・産業・地域・政府全てにＡＩ～」に基づき、本研究開発を推進。SIPの技術により構築した強靭なセキュリティ基盤に対して、外部からの攻撃に対する早期警戒情報を通知することでさらに安全性を高めることが期待できる。また早期警戒情報は民間でも有効に活用できるものであることから、セキュリティ対策の新たな民間投資の促進が期待される。

出口戦略

- セキュリティオペレーションセンタやインシデント対応組織などにおいて、本施策が開発するハイブリッド高速分析プラットフォームにおいて導出される早期警戒情報等を用い、マルウェアに起因する攻撃被害の低減、精度の高いマルウェア解析、攻撃への対処優先度判断支援が行われるような仕組みを構築する。
- その際、内閣サイバーセキュリティセンターやJPCERT/CC、及び各重要インフラにおいて活動している、情報共有のためのISAC組織（ICT-ISAC，金融ISAC、電力ISAC等）とも連携し、効果的な活用を行う。

民間研究開発投資誘発効果等

- 早期警戒情報の提供先組織（上記出口戦略に例示する組織等）の状況に応じて、下記の項目について順次投資の促進が期待される。
  - 早期警戒情報を効果的に受信・処理するためのシステムへの投資
  - 早期警戒情報に加え、他組織からのセキュリティ情報も購読し、それらを一元管理・活用するためのシステムへの投資
  - その他のセキュリティ情報への投資
  - サイバー攻撃分析技術を効果的に活用すべく、必要なデータを収集するための大規模ストレージを含むシステムへの投資
  - 各組織の中に存在するアンチウィルスやSIEM等のシステムを含む、統合セキュリティ管理システムへの投資

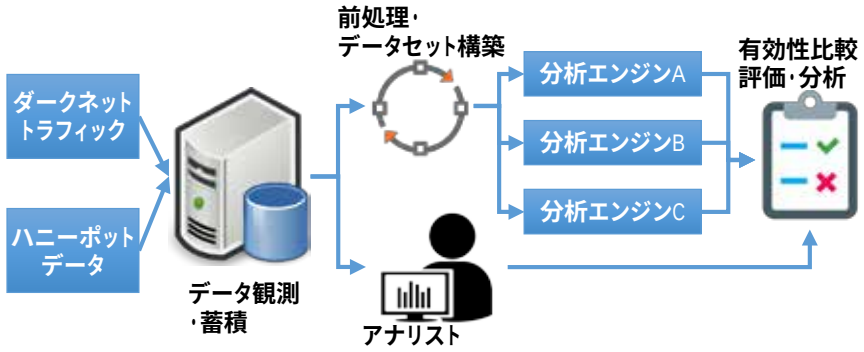
資料2　「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の概要

施策全体像

n **技術開発**

① 多種多様な観測手段から得られるサイバー攻撃情報（マルウェア、脅威情報、トラフィック）に対し、各種機械学習のエンジンを用いて、多角的なマルウェア挙動に関連する特徴量を抽出する技術を開発。

② 抽出された多角的なマルウェア挙動に関連する特徴量を用いて、サイバー攻撃の初期挙動の検出及び影響度分析を行い、早期警戒情報を導出する技術を開発。



n **社会実装**

既存の観測手段による攻撃挙動を用いた特徴情報の抽出や機械学習による攻撃挙動解析のための評価システムを構築する。当該システムにサイバー攻撃の初期挙動や影響度分析の結果を入力し、その有効性、効果を検証し、早期警戒情報を提供する環境の構築を行う。

n **関係するSIP施策**

SIP第２期　IoT社会に対応したサイバーフィジカルセキュリティ　「信頼チェーンの維持技術の研究開発」

SIPの真贋判定技術等によりサイバー攻撃に対して強靭な基盤を構築できるが、外からの攻撃が届く前段階で攻撃の初期挙動を検知することはできない。サイバー攻撃発生時の対処実施に当たり、本研究成果の早期警戒情報をリアルタイムに活用することで、被害の未然防止や最小化に資することができる。

スケジュール

		R1年度	R2年度	R3年度	R4年度
各要素技術の研究開発	マルウェア分析		初期評価	ダークネット分析技術の実証・改良 マルウェアサンプル分析技術の実証・改良	ハイブリッド高速分析プラットフォームの実証
	脅威情報分析		初期評価	構造化情報分析技術の実証・改良 非構造化情報分析技術の実証・改良	
	ライブネット分析		初期評価	セキュリティアラート分析技術の実証・改良 囮文書の分析技術の実証・改良	
ハイブリッド高速分析プラットフォーム構築			プラットフォームの概念設計	概念実装 プラットフォームのプロトタイプ開発 実証の準備（協力依頼等）	

資料3　「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の目標達成状況

- 多種多様な観測手段により収集したサイバー攻撃データに基づき機械学習を駆使することによる、マルウェアの攻撃挙動解析の自動化技術を確立するとともに、大きなインシデントに発展する前の早期のタイミングでマルウェアの攻撃挙動解析を完了し、早期警戒情報を導出する技術を確立する。
- 令和元年度においては、ダークネットやハニーポットによって取得した攻撃挙動から特徴情報を抽出し、機械学習を活用してマルウェア活動の早期発見やその機能分析を実現する技術の開発、及び脆弱性情報およびセキュリティアラート情報の分析を効率化・自動化する技術を開発した。

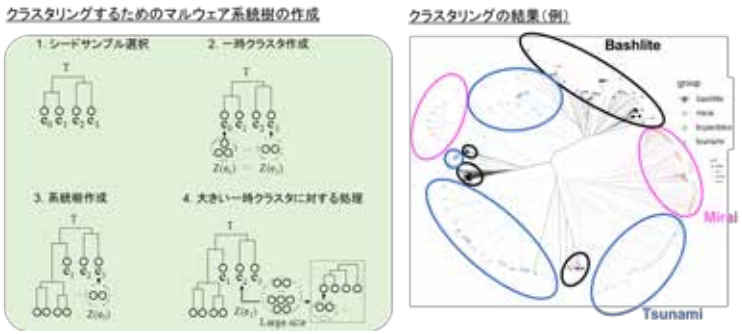
研究内容		令和元年度目標	成果・達成状況
各要素技術の研究開発	マルウェア分析技術の開発	[ダークネット分析技術] マルウェアの感染活動の発生をリアルタイムに検知する技術を開発する。	マルウェアの感染活動の発生をリアルタイムに検知する技術を開発し，実験によりそのフィージビリティ（検知精度91.2%）を確認。
		[マルウェアサンプル分析技術] 大量のマルウェアを高速かつスケーラブルに分析する技術を開発する。	従来、現実的な処理時間で分類が実現できなかった大量のマルウェアサンプルを高速に分類する技術（マルウェアサンプル分析技術）を開発。
	脅威情報分析技術の開発	[構造化情報の分析技術] 脆弱性の種別を自動的に判別する技術を開発する。	CVE（Common Vulnerabilities and Exposures）などの構造化された脆弱性情報を収集し、脆弱性分類番号を自動付与する脅威情報分析技術を開発し、限られたデータセットにおいて、95%の精度を実現。
		[非構造化情報の分析技術] 脅威情報の自動分類および脅威トレンドの抽出のための技術を開発する。	セキュリティレポートから脅威に関連するトピック群を自動生成し、その各トピックに含まれるキーワードを自動抽出できる技術を開発。初期的評価実験の結果、各グループがセキュリティ脅威情報の視点でのトピックになっていることを選択されたキーワードにより確認。
	ライブネット分析（トラフィック分析）技術の開発	[セキュリティアラートの分析技術] 機械学習を用いて、セキュリティアラートの中で重要度の低いものを自動的に除外する技術を開発する。	教師無し学習アルゴリズム（Isolation Forest）を用い、特定のセキュリティアプライアンスがあげるアラートのうち、重要度の低いアラートを87%除外することに成功。その際に、重要度の高いアラートが除外されることなく100%維持されていることを確認。
		[標的型攻撃の分析技術] 囮文書を分析するためのシステムフレームワークを構築し、重要度別分類技術の評価を行う。	標的型攻撃などに利用される囮文書を、その文書のトピックなどを特徴量として用いることにより、重要度別に分類する技術を開発。その初期検証実験では、200個の囮文書を97.5%の精度にて分類できることを確認。
ハイブリッド高速分析プラットフォーム構築		開発した要素技術を用いて、ハイブリッド分析プラットフォームを概念レベルにて設計する。	ダークネット分析技術とマルウェアサンプル分析技術を組み合わせることにより実現するハイブリッド分析プラットフォームを概念レベルにて設計。具体的には、各要素技術から提供されるデータがどのように本プラットフォーム上にて活かされるべきかを特定の事例に絞って検討し、そのフィージビリティを検証。

資料4　「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の成果

○マルウェア分析技術の開発

- **マルウェア活動の早期検知**
  ダークネット空間に到着するパケットの送信元の同期性を教師なし機械学習により分析。

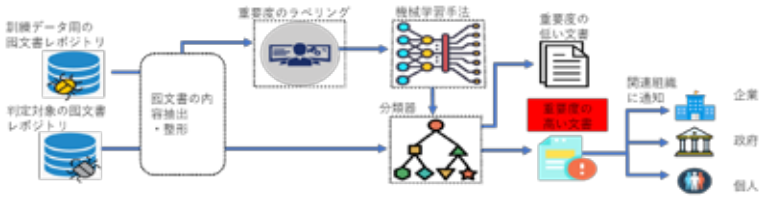
- **マルウェアクラスタリング**
  インターネット上で発生したマルウェアを捕獲するためにハニーポットを開発。マルウェア検体の一時クラスタを作成してから、一時クラスタ内の間について類似度を計算。



○ライブネット分析技術の開発

- **セキュリティアラートのスクリーニング**
  教師なし学習方である「Isolation Forest」（以下IF）を利用して、大量である通常アラート（誤検知）から異常アラート（インシデント）を検出。

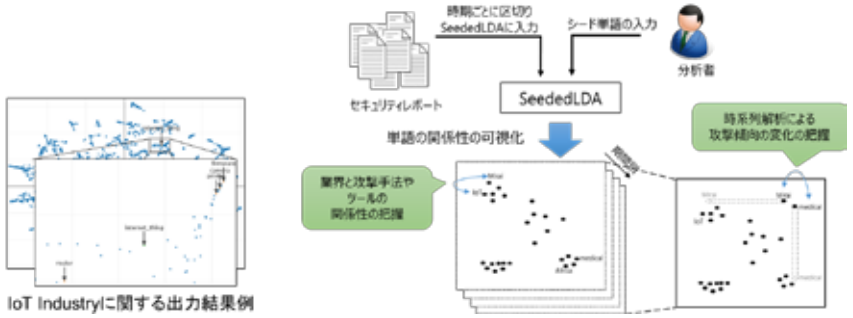
- **囮文書のトピック推定および分類**
  囮文書のなかに特定の個人や組織を狙った攻撃の可能性を示唆する特徴がないか調査し、その特徴をもとにAI/機械学習法により重要な囮文書を自動判定。



○脅威情報分析技術の開発

- **脆弱性の深刻度判定及び分類**
  脆弱性情報の説明文を特徴とし、Boruta手法で有効な特徴を選択した後に、最適な分類モデルを構築するために様々な機械学習アルゴリズムを試行。

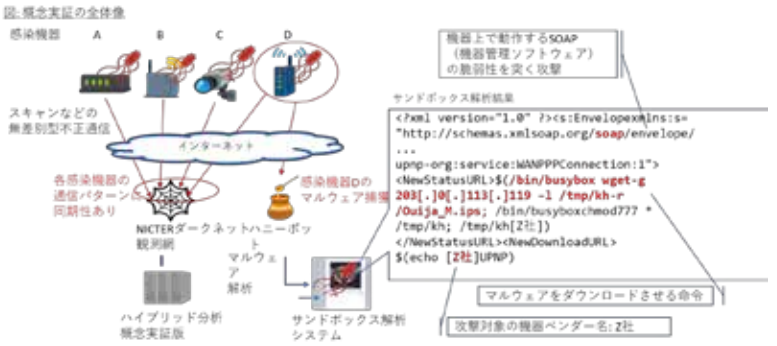
- **脅威情報の自動分類および脅威トレンドの抽出**
  話題誘導するトピックモデル（SeededLDA）によりセキュリティレポートを学習。及び単語の関係性の可視化から攻撃手法や攻撃傾向を分析。



○ハイブリッド高速分析プラットフォーム構築のための概念実証

1.複数の感染機器（下図ではA～D）からの通信に対して同期性検知アラートがあがった（ダークネット分析の成果）
2.ある機器（下図ではD）からマルウェアサンプルの捕獲に成功し、解析を実施（マルウェアサンプル分析技術等の成果）
　§ サンドボックス解析の結果:Z社の機器を狙い、機器上の管理ソフトの脆弱性を突いてマルウェアをダウンロードさせる命令を内包
　§ マルウェアからの不正通信トラフィックを収集し、（C2等との）通信パターンなどの特徴抽出に成功
3.同期性があった他の感染機器（図ではA～C）もZ社の機器を狙い、同じマルウェア感染の疑いが濃厚

→個別の分析技術を効果的に突合することにより、単独では見えなかった多くの解析情報を得ることに成功



資料5 「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の民間からの貢献及び出口の実績

n 民間からの貢献額： 1 年で 1 億円相当
①人件費　本研究開発の人件費自己負担分（13名、50百万円相当）
②機器費等　本研究開発で使用する機器のうち、サーバ、ストレージシステム、セキュリティアプライアンス等については、一部自己負担で用意（50百万円相当）

令和元年度当初見込み	令和元年度実績
①研究職員 常勤研究員 7名、招聘研究員3名、リサーチアシスタント3名	①研究職員 常勤研究員 7名、招聘研究員3名、リサーチアシスタント3名
②・高性能 GPU サーバ 1台 ・CPU サーバ / ストレージサーバ 2台 ・機械学習用ワークステーション 2台 ・Laptop PC 6台 ・機械学習を用いたダークネット解析エンジンの汎用データ処理システム 1式 ・セキュリティ機器からのアラート情報の初期スクリーニング自動化ツール 1式 ・ライブネットトラフィック知能解析フレームワーク 1式	②・高性能 GPU サーバ 1台 ・CPU サーバ / ストレージサーバ 2台 ・機械学習用ワークステーション 2台 ・Laptop PC 6台 ・機械学習を用いたダークネット解析エンジンの汎用データ処理システム 1式 ・セキュリティ機器からのアラート情報の初期スクリーニング自動化ツール 1式 ・ライブネットトラフィック知能解析フレームワーク 1式

n **出口戦略**
ü **本施策において、導出される攻撃予兆情報や早期警戒情報に関し、以下のような効果、社会的な有効性を達成する。**
- **マルウェアに起因する攻撃の初期段階の活動を導出し、インシデントが大規模化する前に攻撃を捕捉し、被害を低減する。**
- **攻撃挙動の共通性、類似性から同種のマルウェアファミリーやグループを特定し、マルウェア挙動解析を実施する組織へ情報提供を迅速に行い、精度の高い、マルウェア解析に資する。**
- **攻撃によって想定されるインパクトの自動分析を行うことにより、組織がインパクトの大きい攻撃への対策を優先的に実施できるよう支援する。**

ü **早期警戒情報により、上記のような効果が、セキュリティオペレーションセンタやインシデント対応組織などにおいて期待される。**
ü **また、内閣サイバーセキュリティセンターやJPCERT/CC、及び各重要インフラにおいて活動している、情報共有のためのISAC組織（ICT-ISAC，金融ISAC、電力ISAC等）において効果的に活用されることが期待される。**
ü **さらに、国際的な攻撃情報分析組織（米国のISACなど）との連携を行い、国際レベルで解析力の強化を行うことも可能となる。**

令和元年度当初見込み	令和元年度実績
出口戦略で、各種機関に提供することとしている早期警戒情報等に関し、それらを導出するための技術の開発に取り組む。各要素技術の取組見込みについては、以下のとおり。 ①マルウェアの感染活動の発生をリアルタイムに検知する技術を開発し、そのフィージビリティを検証する。 ②脆弱性の分類ラベルの階層性に着目した判別方法の検討とシステムの試作を行う。 ③Web上に存在する情報からインテリジェンス情報を自動生成する技術の基本設計と試作を行う。 ④インテリジェンス情報からマルウェア分析に有用な情報を生成する技術のための調査検討を行う。 ⑤セキュリティアラートのうち、重要度の低いものを除外する技術を開発し、そのフィージビリティを検証する。	①マルウェアの感染活動の発生をリアルタイムに検知する技術を開発し，実験によりそのフィージビリティ（検知精度91.2%）を確認。その成果を国際会議TrustCom'19にて発表 ②脆弱性の種類を自動で付与する手法の設計と試作を行い、既存研究に比べて多数のラベル(31種)の判別に対して80%以上の精度を達成した。 ③セキュリティレポートから脅威に関連するキーワードを抽出するクラスタリングに基づく手法の基本設計と試作を行い、875件の文書に対して適用した。 ④脆弱性・脅威情報からの特徴的な単語の抽出手法、およびセキュリティインシデントとの関連付け手法の設計のための調査を行った。 ⑤セキュリティアラートのうち、87.4%の重要性の低いアラートを安全に除外する技術を開発することに成功し、内部トラフィックを用いた評価を実施。その成果を国際学会ICONIP'19にて発表