資料1-1

作業途上のものであり取扱注意

研究領域の具体例の検討

第6回WG（10月中旬）に向け、WGの集合知として複数の具体例を挙げるため、委員より構想・提案のあった研究領域の具体例のアイディアを単純にリストにしたもの。

通し番号は事務局にて便宜的に付しており、また、大まかに「現状の強み分析のための研究領域の整理」の順番に機械的に並べている。

No.	研究領域（仮称）	研究領域における研究内容及び目標の概要
1	信頼ある分散型データガバナンスを実現する革新的セキュリティ技術の開発(Security for DFFT)	本研究領域では、個人や法人がデータでのアクセスをコントロールし価値をマネージできる仕組みをWeb上に構築することを目的に、分散・非中央集権型のモデルにおいて、ID管理、ユーザ認証、アクセス制御、データ保護と利活用の両立を実現する新たなセキュリティ技術を開発する。具体的には以下の開発を目標とする。 1) 分散ID/自己主権ID: 要素として認証(生体認証、ID連携など含む)、暗号(高機能暗号、秘密計算等)、ブロックチェーン 2) AI for Security: AIによる個人へのデータコントロールのサポート、Fake dataの検知技術など 3) トレーサビリティ: Blockchainなどを活用したTrust of Dataの確保・証明技術 4) 分散/P2Pセキュリティ: 分散・非中央集権的に存在するデータへのアクセス制御や、処理の正しさの証明・確認 5) エッジセキュリティ: 上記技術をエッジ側で分散し効率的に処理する技術
2	プライバシーを保護したサイバー攻撃観測データの共有・分析基盤	サイバー攻撃の全容を把握するためには多角的かつ多地点での観測データを統合的に集約して分析する必要がある。これまで、組織横断的に観測データを共有するMWSを代表とするコミュニティ活動が推進されてきたが、センシティブな情報が含まれない限定的な観測データに限って共有されてきた。しかしながら、以下の観点でサイバー攻撃観測データの情報共有を阻害する要因が存在する。 A. 観測データに含まれるプライバシー情報の保護（組織内・顧客のプライバシー情報が含まれる場合、他組織との情報共有ができない） B. 情報提供者の匿名性（情報提供はしたいが、提供元は明かしたくない） C. 情報提供者と情報受給者の間でのインセンティブのアンバランスさ（情報提供者は提供するだけではメリットがない。情報受給者に徹した場合、労せずとも情報が手に入る。） よってこの阻害要因を解決するため、テーマ１「プライバシーを保護したサイバー攻撃観測情報を共有する基盤技術」（Aの解決）、テーマ２「プライバシーを保護したサイバー攻撃観測情報を分析する基盤技術」（Bの解決）、および、テーマ３「情報提供の量に応じてバランスの取れた情報受給を実現するプライシング機能」（Cの解決）の実現を目指す。
3	持続可能な社会のためのシステムセキュリティ技術（グループ型）	多様なアプリケーション・サービスが実現される社会において量と質（機能性・耐タンパー性など）の両面において増加するセキュリティ処理のコストを削減・維持し、持続可能とするための革新的なシステムセキュリティ技術を開発する。AIシステム、IoTシステム、ブロックチェーンシステム、量子システムといったキーテクノロジｘシステムの基幹的セキュリティ技術から自動運転システムや高度化医療システムなどのアプリケーションｘシステムの応用的セキュリティ技術の研究開発を対象として、同システムで将来的に予想されるセキュリティ処理の質的・量的な劇的な増加の問題を解決する（例えば10年でセキュリティコストを100分の1とする等の）技術革新に国際的研究グループにより取り組む。
4	持続可能な社会のためのシステムｘセキュリティ技術（個人型）	多様なアプリケーション・サービスが実現される社会において量と質（機能性・耐タンパー性など）の両面において増加するセキュリティ処理のコストを削減・維持し、持続可能とするための革新的なシステムセキュリティ技術を開発する。AIシステム、IoTシステム、ブロックチェーンシステム、量子システムといったキーテクノロジｘシステムの基幹的セキュリティ技術から自動運転システムや高度化医療システムなどのアプリケーションｘシステムの応用的セキュリティ技術の先端的な研究開発を個人もしくは少数の研究グループが（可能なら国際連携により）行う。
5	人工知能セキュリティ	機械学習（ML）とセキュリティは異なる分野で独立に発展してきた技術であるが、各技術の有用性と社会的重要性が高まるにつれ、両者を融合したクロスオーバーの領域が盛んに研究されるようになった。それらの研究は（A）「MLを用いた防御技術」、（B）「MLを用いた攻撃技術」、（C）「MLに対する攻撃」、（D）「MLに対する攻撃への防御技術」の4つのサブテーマに大別することができる。本研究領域は、これらのサブテーマを理論から応用まで、包括的に実施することを狙いとする。いずれのサブテーマもMLの理論を専門とする研究者とのコラボレーションを期待できる。
6	自動運転セキュリティ	ドライバ不在で動作するレベル4以上の自動運転技術を対象とし、自己位置推定、環境認識、経路計画、経路追従、ハンドル操作、アクセル/ブレーキ操作を実現するソフトウェアが具備すべきセキュリティメカニズムを明らかにする。また、そのようなメカニズムの PoC 実装、ならびにフィールド実験評価を行う。 サブ領域は以下の通り (A) 自動運転における機械学習アルゴリズムのセキュリティ評価 (B) 自動運転における環境認識（センサー）のセキュリティ評価 (C) (A)(B) の実装評価（フィールド実験）
7	Connected Car セキュリティ	Connected Car のセキュリティは、今後の交通インフラを支える重要技術である。CANには様々なデバイスが接続されており、センサーや車両制御装置が無線通信デバイスや車々間通信装置を介して外部と繋がった場合の攻撃リスクは、重大な事故に繋がる可能性があり、とても大きい。クラッキングされた自動車が移動しながらマルウェアをバラ撒くような事態も想定される。商用車においては運行管理システムなど、日本の物流を支えるシステムも関わってくるほか、コストの重要性が大きくなる。本研究では、従来型の、乗員の安全を守るセーフティの一貫としてのセキュリティだけでなく、このような外部との連携・接続やエコシステムを前提としたConnected Carセキュリティシステムの研究開発・標準化をおこなう。
8	自動車のサイバーセキュリティエコシステムにおけるプレゼンス強化	今後、コネクテッドカーへのサイバー攻撃がより一般的になると、利用者、OEM、サプライヤ、サービス提供者、システム運用者、セキュリティ企業、行政等を巻き込む、自動車のサイバーセキュリティエコシステムが生まれることが想定される。この時、どこでだれがサイバー攻撃情報、脅威情報を収集し、対策を立案、実施することが効果的なのか、技術的、制度的、産業構造的な観点から必要な準備を検討し、産業界、学術界の役割を明確化しつつ、先行的な取り組みを実施する。例えば、自動車サイバーセキュリティに関する特区を設定し、各種の実験、検証、攻撃観測などを行う。個々の攻撃の検知や対策だけでなく、脅威情報がどのように収集、流通、管理され、対策が検討、導入されるかというサイバーセキュリティエコシステムにおいてどのように効率的かつ効果的に対策を行うかという観点で検討を行い、当該分野での我が国のプレゼンスを高めることを目的とする。
9	Society 5.0を実現するシステムにおけるサプライチェーンセキュリティ基盤技術	Society 5.0を実現するためには、ITシステム、IoTシステム、サイバーフィジカルシステムなどが高度に連携したシステムが実現され、広く利用されることが想定される。一方で、これらのシステムがサイバー攻撃に対して、強靭な耐性を持ち、信頼性できるシステムであることが必要不可欠である。 また、これらのシステムは、様々なサプライヤーの協力の下に、一つのシステムとして構築されるため、構築されたシステムの健全性の検証や、動作中のシステムの健全性や完全性を検証するコンピュータサイエンスやシステムセキュリティ技術を基盤とする新しい基盤技術が必要不可欠である。 さらに、これらのシステムを構成する個々の機器についても、サプライチェーン上での製造物として安全性や信頼性が担保されており、最終製造物についても、その構成要素となる個々の製造物の中に、不正なプログラムやハードウェアなどが混入しておらず、信頼できるものであるか検証できることが必要である。これに加え、機器の利用中に、ファイルシステムやメモリ上の実行中のプログラムが、不正なものに改ざんされたり、正常な機能を提供できない状態になったりすることを防止し、検知できる要素技術を継続して研究し、高度化することが重要である。 第2期SIPでは、実稼働するサプライチェーンに組み込み実用できるセキュリティ対策基盤を実現するものの、実現した基盤で利用される個々の要素技術の高度化や、課題解決のための新たな要素技術の研究開発を、学術的な観点を踏まえて行う必要がある。これにより、従来から行われていた経験則や発見的手法で導き出された手法ではなく、学術的観点で検証され、定量的に評価可能な手法で構築された手法をベースとする対策基盤の実現を目指す。 これらの要素技術を研究開発し、さらにSIPのシステムに融合することで、Society 5.0を実現するセキュアで信頼性のあるコンピューティング基盤を実現する。
10	身近なものを用いたレクリエーション暗号と教材展開	カードベースプロトコルはトランプカードを利用し、お互いの入力を秘匿したままANDやXORなどの演算を行うマルチパーティ計算である。トランプカードを様々な方法でシャッフルするなどの手順を繰り返すことで目の前で所望の結果を得ることができるため、暗号技術を身近に感じることができるとされている。 カードベースプロトコルを皮切りに、お菓子のPEZやコイン、ボールなどの玩具を用いるなど様々な方式に拡張されている。これらの方式は大学のオープンキャンパスなどで催されることがあり、日頃硬い研究を行っている研究室においては、研究の楽しみを理解してもらう導入として効果が高いと考えられている。同じような方式としてはスキュタレー暗号（棒状に紐を巻き付けることで暗号文を復号する方式）や視覚型復号秘密分散（複数の透明性のある画像を重ね合わせることで隠された画像を復元する方式）などがあり同様に紹介されてきた。 これらの方式はすでに産学官において幅広く研究が進められている。今回これらの結果をベースに、高校より若い世代に対して効果をもたらす教材開発も視野に入れたレクリエーション暗号方式の検討を行って頂くことを考えた。