資料2-1

注）具体例のとりまとめに向けた作業途上であり取扱注意

＜認証システムの安全性に関する評価手法の確立＞

概略

共同研究先: インターネット企業、ユーザー企業
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
○○Payなどの電子決済サービスの利用が普及しているが、これらのサービスを経由した金銭の窃盗事件も顕在化している。不正なアクセスやアカウント作成の防止のため、より安全な認証システムの構築が行われているが、各社コンサル等を活用しつつも手探りで構築している状態であり、構築した認証システムの安全性を客観的に証明し、利用者に分かりやすく説明することは難しい状況にある。また、利便性と安全性のバランスは難しく、安全性を重視して手続きがなると顧客獲得の障害につながりかねないため、実現方法のバランスが難しい。電子決壊サービスは安全性も重要であり、かつ、利用者の利便性も両立させなければ、事業は立ち行かなくなるため、客観的評価手法による安全性の証明および利便性も考慮した認証手法の確立は電子決済サービス事業者および金融機関の関心が高いと想定される。

概要

共同研究により期待される成果：
大学による科学的基礎に基づくアプローチにより認証システムを含むサービスの安全性の評価手法の確立し、客観的にシステムの安全性を証明できるようにする。（認証機能単体ではなく、本人確認を伴うアカウント作成やカード情報の登録、利用、各社のサービス間の連携までも含む、提供サービス全体としての評価であることに留意）また、システム全体としてのユーザー利便性（わかりやすさ）と安全性の両立を考慮した新たな手法の検討・提案をする。

共同研究の概要:
- **＜認証プロセスの評価手法検討に資する具体な取り組みや研究はないか＞**で培われた理論、原理に基づく、認証のプロセスのモデル化やスコアリングによる評価手法の確立するとともに、様々な認証システムに対する利用におけるステップ数や実行容易性といったわかりやすさと安全性の評価
- **＜新規の認証プロセス検討に資する具体な取り組みや研究はないか＞**で培われたプロセス検討能力により、新たな利便性と安全性を両立した認証システムの提案とプロトタイピングの実装

共同研究の形態:企業からは、研究費を提供し、大学にて研究員を雇用して研究を実施する
共同研究に想定する期間および規模: 年、万円/年、 名
想定される研究分野: セキュリティ評価・リスク評価、アイデンティティ管理及び認証

＜サイバー攻撃観測網等を活用したエンドユーザへのセキュリティ侵害インジケータ(IOC)等提供サービス＞

概略

共同研究先: インターネット企業
実現の方向性: 企業にとっての付加価値向上となるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト: （例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
高いシェアをもつSNSは実質的に情報通信基盤としての役割を担っており、例えば、「新型コロナ対策のための全国調査」なども行われている。マルウェア感染情報やセキュリティリスク情報をユーザに提供する活動は、 、情報通信基盤としての役割を担うSNSプロバイダの社会貢献度向上につながるという観点で潜在的なニーズがあると考えられる。

概要

共同研究により期待される成果：
SNSプロバイダとの連携により、広く国民に「セキュリティチェック」の実施を促すメッセージを配信することで、エンドユーザが自身のネットワーク環境(自宅やオフィスなど)の健全性を確認し、マルウェア感染やセキュリティリスクを把握することができる。これまで研究機関によるサイバー攻撃観測結果を直接的に一般のエンドユーザに提供し活用することは困難であったが、エンドユーザとのコミュニケーションチャネルとしてSNSと連携することで国産IOC（indicator of compromise：セキュリティ侵害インジケータ）の活用にもつながる。サイバー攻撃観測、広域スキャンに基づく注意喚起の有効性向上は当該分野のホットトピックであるが、SNSを活用した全国規模のサイバーセキュリティ注意喚起はこれまで例がなく、その効果検証・向上に関して学術研究成果も期待される。サイバーセキュリティ対策を重視する各種政策との整合性も高い。

共同研究の概要:
- 国内に構築されたサイバー攻撃観測網(ダークネットやハニーポット)、広域スキャンシステムの観測情報に基づき、エンドユーザへのセキュリティ侵害インジケータ(IOC)等を、国内で高いシェアを誇るSNSプロバイダとの連携により広く国民に配信・提供する。
- ダークネットやハニーポットによるサイバー攻撃観測の研究や広域スキャンプロジェクトで蓄積されたサイバー攻撃やIoT機器の脆弱性に関する情報を活用し、国民のセキュリティ向上につなげる。
- サイバー攻撃や脆弱性の改善状況を観測することで、大学・研究所にてセキュリティ注意喚起の頻度や内容が、注意喚起の効果や効率にどのような影響を与えるかを検証する。

共同研究の形態:企業からは、エンドユーザへの情報配信基盤(及び資金)を提供し、大学・研究所は研究員と観測情報等の研究成果を提供
共同研究に想定する期間および規模: ２年、万円/年、２～３名
想定される研究分野: ネットワーク攻撃検知, 検知(観測)に基づく研究, IoTセキュリティ

注）具体例のとりまとめに向けた作業途上であり取扱注意

＜商用ソフトウェアの脆弱性対策と堅牢化手法の有効性研究＞

概略

共同研究先: ITベンダー企業（ソフトウェア開発会社（特にセキュリティソフトの開発を行う会社））
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
ウイルス対策ソフトや資産管理ソフトなど、日本ローカルの商用ソフトウェアにおいても脆弱性がサイバー攻撃者によって悪用されている。商用ソフトウェアベンダー自身もコストをかけて脆弱性対策をしてるが、より高度な攻撃対策を実装することで、製品の価値向上に繋がりうる。特に任務保証が求められる重要インフラにおいては、導入するソフトウェアの堅牢性や万が一の侵害時の悪用検知は重要視される傾向にあり、重要インフラ市場でも有効性が認められる対策であれば、非機能要件の強化であっても、製品の売り上げにつながると想定される。

概要

共同研究により期待される成果：
ソフトウェアの脆弱性調査や対策の研究を行っている大学研究者との共同研究により、通常の市場サービスでは見つからないソフトウェアの脆弱性（ソフトウェアの動作等に係るもので例えば認証の不備で成立してしまう悪用など）を洗い出し、対策手法を検討。プロトタイピングにより実装への道筋を得、製品の堅牢性を高めることに資する。さらに、攻撃者による製品機能の悪用検知や攻撃検知といった、よりプロアクティブな対策手法も検討する。なお、実施した脆弱性対策や悪用検知対策等に関する研究発表を可能とすることで大学側へのインセンティブを与えることも考えられる。（ただし、攻撃者に有益となる防御の工夫等、機微な部分については秘匿）。

共同研究の概要:
- 大学等においてマルウェアの動作特性の解析とそれを活用した対策の研究で培われた攻撃手法の分析能力と対策手法を使って、ダミーファイルを利用した悪用検知などのプロアクティブな対策手法を発案しプロトタイプ実装を試みる。
  （可能な限り実環境にて、攻撃研究を行っている研究者に攻撃演習を実施し、有効性を評価する。）
- 大学等においてファイルシステムやOSの仕組みに深くかかわる攻撃や対策といったハードニングにつながる技術研究で培われた知見を活かして、マルウェア等によるソフトウェアの悪用を監視したり、悪用から保護する対策機能（プロセスの保護、設定ファイル含めた関連ファイルの保護強化など）のプロトタイプ実装を試みる。

共同研究の形態:企業からは、資金および共同研究要員を提供し、大学の研究員と合同で研究を実施する
共同研究に想定する期間および規模: 3年、万円/年、2~3名
想定される研究分野: ソフトウェア脆弱性、攻撃手法、マルウェア

注）具体例のとりまとめに向けた作業途上であり取扱注意

＜端末側での利用者のセキュリティリスク低減に向けた分析・把握に係る研究＞

概略

共同研究先: セキュリティベンダー企業
実現の方向性: 企業保有のデータを共有して学理に基づく分析を行うもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト: （例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
COVID-19を受け、テレワークの普及とともにクラウドサービス利用が増え、端末におけるセキュリティ対策が重要視されるとともに、端末の利用状況の把握・分析の需要が高まっている。セキュリテイベンダー企業が提供しているソフトウェア製品の機能強化により、上記需要に応える。具体的には、ソフトウェア製品によるPCの証跡ログを活用することで、端末側でのセキュリティリスクの高い行動や、端末を操作する者が心理的にリスクの高い状況にあることを分析・把握できるようにし、顧客に提供する。これにより、ソフトウェア製品の機能強化による差別化や新規サービス提供の機会に繋がりうると想定される。

概要

共同研究により期待される成果：
セキュリティベンダーより実際の環境にある各端末から収取したPCの証跡ログを提供し、セキュリティ心理学的知見を有する大学にてセキュリティリスクの高い行動や、メンタルヘルス的にリスクの高い状況を検知する条件を調査し、証跡ログの分析手法を確立する。プロトタイピングにより製品の機能強化に繋がる実装への道筋を得るとともに、試行に協力してくれるユーザをセキュリティベンダーと共に獲得し、実環境での検証を行うことで精度を向上する。

共同研究の概要:
- 大学等において取り組まれているサイバーセキュリティ状況認識の研究で培われた行動分析的知見を使って、PC端末の証跡ログからセキュリティリスクの高い行動に繋がると判断できる分析手法を発案しプロトタイプ実装と検証を試みる。
- 大学等において取り組まれているメンタル負荷などの研究で培われた心理学的知見を使って、PC端末の証跡ログから心理的にリスクの高い状況と判断できる分析手法を発案しプロトタイプ実装と検証を試みる。

共同研究の形態:企業からは、研究費およびデータを提供し、大学にて研究員を雇用して研究を実施する
共同研究に想定する期間および規模: 2年、万円/年、 2名　**想定される研究分野:**　セキュリティ心理学、OSセキュリティ

＜自動運転技術のトラスト確立＞

概略

共同研究先: ユーザ企業（自動運転ソフトウェア開発会社）
実現の方向性: 新たに技術・システムを作る際にセキュリティを同時に作り込むもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
自動運転技術の安全性評価をする際には、従来の安全性評価（事故回避等）に加え、サイバー（フィジカル）セキュリティに特有な悪意がある入力や環境が用意されたケースを想定しておくことが必要である。そこで、自動運転技術を実現するソフトウェアを開発する企業と連携し、自動運転ソフトウェアのセキュリティを保証する技術の研究に取り組む。セキュリティに強い点付加価値向上とすることで、他社に対する差別化ポイントとなりえる。
連携先としてはTier-3/4 相当のサプライヤとの連携が想定される。

概要

共同研究により期待される成果：
自動運転ソフトウェアで実装される、環境認識、信号検知、信号認識、経路計画、障害物回避、駐車計画、経路追従などの機能を実現するアルゴリズムに対し、悪意のあるデータが意図的に入力された際の挙動を明らかにし、得られた知見を実機を用いたハードウェア上で再現、評価する。これにより、自動運転技術に固有なセキュリティ脅威に対する対策にセキュリティ・バイ・デザインで取り組めるようになる。

共同研究の概要:
- 大学として機械学習セキュリティの応用的研究の基礎と実装評価、ハードウェア評価のノウハウを有する大学が分担して攻撃の分析と再現を行い、企業は自社製品で培ったノウハウやデータを元に、特にセキュリティ脅威が高いと考えられる機能を同定する。
- **＜他に産学連携の事例となりうるものはないか。＞**

共同研究の形態:企業に研究費を出してもらい「人」の雇用は大学側で行う形態
共同研究に想定する期間および規模: 3年、万円/年、 PI 3名、RA 6名　**想定される研究分野:** AIセキュリティ、自動車セキュリティ
一定の資金が必要となるため、原資は国プロの利用を想定（大学と企業が連名で申請）