別紙２

アクセス制御機能に関する技術の研究開発の状況

１　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関してとりまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下の４件であり、その研究開発の概要は、別添１のとおりである。

- サイバーセキュリティ技術の研究開発
- Ｗｅｂ媒介型攻撃対策技術の実用化に向けた研究開発
- 欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
- サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発

２　民間企業等で研究を実施したもの

(1)　公募

警察庁、総務省及び経済産業省が令和元年12月9日から令和2年1月24日までの間にアクセス制御機能に関する技術の研究開発状況の募集を行ったが、その結果、提案はなかった。

(2)　調査

警察庁が令和元年９月に実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア　大学（13大学、18件）

東京理科大学（２件）
福山大学
島根大学
名古屋大学
城西大学
佐賀大学（３件）
東京電機大学
崇城大学
立命館
お茶の水女子大学
北九州市立大学
広島大学（３件）
東北工業大学

イ　企業（３社、４件）

トビラシステムズ株式会社（２件）
株式会社FFRI
株式会社アズジェント

また、それぞれの研究開発の概要は別添２のとおりである。

なお、別添２の内容は、アンケート調査の回答内容を原則としてそのまま掲載している。

アンケート調査は、以下の条件に該当する大学及び企業の中から、調査対象として無作為抽出した大学314校、企業1,336社の計1,650団体を対象に実施した。

・大学

国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

・企業

市販のデータベース（四季報）に掲載された企業であって、業種分類が「情報・通信」「サービス」「電気機器」「金融」であるもの

（別添１）

対象技術　インシデント分析技術

テーマ名　サイバーセキュリティ技術の研究開発

開発年度　平成18年度～

実施主体　国立研究開発法人情報通信研究機構
法人番号　7012405000492

背景、目的

サイバー攻撃の急増と被害の深刻化によりサイバーセキュリティ技術の高度化が不可 欠となっていることから、ネットワークを介したサイバー攻撃やマルウェア等の活動を大局的に把握・対応するための各種観測技術、分析技術、可視化等の研究開発を行う。

研究開発状況（概要）

これまでに研究開発・整備したサイバー攻撃観測機構や、マルウェアの収集・分析機構に関して、世界規模の観測網確立に向けた観測規模の更なる拡充、より高度な観測・分析機構の開発等を行った。観測・分析結果については、Webサイト等で広く公開するとともに、アラートシステム等の外部への技術移転を行った。また、地方自治体へのアラート提供を拡大する等、研究開発成果の社会展開を推進した。

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　サイバーセキュリティ研究室　042-327-6225

将来の方向性

上記の研究開発を通じて、将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

対象技術　インシデント分析技術

テーマ名　Web媒介型攻撃対策技術の実用化に向けた研究開発

開発年度　平成28年度～平成32年度

実施主体　株式会社KDDI総合研究所、国立大学法人横浜国立大学他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　5030001055903（KDDI総合研究所）、6020005004971（横浜国立大学）

背景、目的

Webを媒体としたサイバー攻撃は拡大の一途を辿っており、情報処理推進機構（IPA）が公表している「情報セキュリティ 10大脅威2015」においても、Web系の脅威が約半数を占め、国民の関心は高い。平成27年6月に公表された日本年金機構からの年金情報流出においては、不正なWebサイトへの誘導も行われたと報道されており、Web系の脅威とその対策は依然、重要課題である。

また、従来からあるWebの改ざんや「ドライブ・バイ・ダウンロード攻撃」に加え、標的型攻撃にWebサーバを利用する「水飲み場攻撃（watering hole attack）」や、オンラインバンキングユーザを狙ってWebブラウザ経由で情報を窃取する「バンキングマルウェア」、検索エンジン経由で不正なWebサイトに誘導する「SEO（Search Engine Optimization）ポイゾニング」など、攻撃手法が多様化・複雑化してきている。さらに、攻撃対象がWindows OSのみならず、Mac OSやAndroid等のモバイル端末、IoT機器（linux組込み系機器）にまで広がってきており、重大な社会問題となっている。

そこで、これまで機構が委託研究として取り組んできた「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」（平成24年度～平成27年度）を実用化に向けてさらに発展させ、観測対象をWindows OSのみならず、Mac OSやモバイル端末、IoT機器等に拡大するとともに、Webを媒体とした新たなサイバー攻撃への抜本的な対策に資する観測・分析・対策技術を確立する。

研究開発状況（概要）

平成28年度から以下の研究開発を開始。平成30年度に行った中間評価の結果、平成32年度までの延長を決定。

（１）新型ブラウザセンサの研究開発
（２）新型観測機構の研究開発
（３）新型攻撃情報分析基盤の研究開発
（４）Web媒介型攻撃対策技術大規模・長期実証実験

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_190.html）
電話 042－327－6011

将来の方向性

上記セキュリティ対策技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術　侵入検知・防御技術、ぜい弱性対策技術

テーマ名　欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発

開発年度　平成30年度～平成33年度

実施主体　東日本電信電話株式会社、学校法人慶應義塾他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　8011101028104(東日本電信電話株式会社)、4010405001654（学校法人慶應義塾）他

背景、目的

本研究開発は、欧州との連携により研究開発の促進が期待できる領域について、欧州委員会（EC: European Commission）と連携して共同で実施するプログラム。

ハイパーコネクテッド社会の実現に向けて、実践的なサイバーセキュリティ技術の研究開発は不可欠である。そのため、セキュリティ、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を通じ、世界規模で有効かつ実効性のあるサイバーセキュリティ基盤技術の構築を目指す。

研究開発状況（概要）

平成30年度から研究開発を開始。

具体的には、「新たな脅威への機敏な対応」、「脆弱性自動検出/自動修復」、「セキュリティツールのオープンソース化」、「IoTセキュリティ」、「クラウドセキュリティ」、「データセキュリティ」、「プライバシー保護」、「データ匿名化」、「IoT／クラウドに関するブロックチェーン」、「重要インフラ保護」、「クロスボーダ・アプリケーション」に関わる研究開発及び実証を行う。

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_195.html）
電話 042－327－6011

将来の方向性

国際標準化を睨んだ研究開発力の強化や国際実証環境の構築を軸とした共同研究開発に取り組むことにより、情報通信基盤の共通化を通じた豊かな社会への貢献に資する。

対象技術　インシデント分析技術

テーマ名　サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発

開発年度　令和元年度～令和 2 年度

実施主体　国立大学法人九州大学、学校法人早稲田大学 他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　3290005003743（国立大学法人九州大学）、5011105000953（学校法人早稲田大学）他

背景、目的

マルウェアへの感染は世界的な問題であり、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辿っている状況であるが、感染活動の早期把握やそのマルウェアに関する情報の関連組織間での共有ができていない。

この問題の解決には、セキュリティインシデント発生の可能性をより早く検知し、それを分析するための関連情報を自動的に生成し、関連付け、そのインシデントのもととなったマルウェアや脆弱性を分析する必要がある。これらのタスクは大量のデータを分析することが求められるため、人手による分析は非現実的である一方で、コンピュータによる自動処理の効果が大きく期待できる領域である。また、これらの分析は単一の分析にて完結するものではなく、例えばライブネットトラフィック分析やダークネットトラフィック分析、マルウェア分析、脆弱性分析、Web 情報分析など、様々な分析結果を総合的に判断するハイブリッド分析が求められる。そこで本研究では、国立研究開発法人情報通信研究機構が開発中のマルウェア活動の活性化を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す。

研究開発状況（概要）

令和元年度から以下の研究開発を開始。

(1) サイバー攻撃インフラ情報の収集と分析、(2) 実時間で実現可能な大規模かつ構造的なマルウェア分析、(3) インテリジェンス情報の生成と分析について

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_21601.html）
電話 042－327－6011

将来の方向性

感染活動を自動的に検知し、マルウェアに関する情報と共に自動的に警告を提供可能となる。安心・安全な国際的なサイバー社会の構築・運営に大きく貢献する。

（別添２）

ア　大学

企業・大学名	東京理科大学理工学部
代表者名	井手本康
所在地	〒278-8510 千葉県野田市山崎2641
窓口部署名	理工学事務課
電話番号	04-7122-9728
ホームページのURL	https://st.tus.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ホームページ掲載内容改ざん検知及び自動修正システム 開発元(メーカー名等)： シスコ・ネットワーキング・アカデミー 開発国： 日本 価格： シスコネットワーキングアカデミー会員限定無償配布です。 発売時期： 平成25年4月1日～ 出荷数：	ホームページで公開される内容が改ざんされることで一番危険なことは、「改ざんされた情報が一般大衆の視線にさらされてしまうこと」です。本システムは不正侵入を即時検知すると同時に、不正改ざんされた情報をすぐに自動修正することで、誤った情報の流布を阻止することを目的としています。現在、新潟大学理学部のホームページにおいて、私の作製した本システムが実用化されています。(但し、もう、新潟大のHPが外部サービスに委託された可能性もあります。)

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	○
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	東京理科大学理工学部
代表者名	井手本康
所在地	〒278-8510 千葉県野田市山崎2641
窓口部署名	理工学事務課
電話番号	04-7122-9728
関連部門名	理工学部情報科学科・東京理科大学CCNA講座
ホームページのURL	https://st.tus.ac.jp
研究説明のURL	シスコシステムズ及びシスコネットワーキングアカデミーの担当者達による守秘義務が求められています
対象技術	研究開発状況
研究開発名称： クラウド化されたハニーポットシステム 研究開発国： 日本 研究開発時期： 平成31年4月1日～	・サイバー犯罪対策は大きく「防御」と「犯人特定」の2種類に大別されます。しかし、現在のセキュリティ対策は防御のみが中心で、消極的対策である感じが致します。 ・東京オリンピック2020では、全てのネットワークシステムを、シスコシステムズが管理することを総務省が決定しており、現在、前回のリオデジャネイロオリンピックにおけるサイバー攻撃のデータを分析し、東京オリンピックにおける防御ガイドラインを作成しています。 ・本システムは、通常、単体でおとり捜査目的で設定されるハニーポットをネットワークレベルで実装することで、仮想化技術と並用し、クラウドレベルでの犯罪者検知及び犯罪者が用いた技術の抜きとりに使用されています。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	○
高度認証技術	
インシデント分析技術	○
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	福山大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福山大学工学部情報工学科
ホームページのURL	
研究説明のURL	http://www.yama-lab.org/~yamanoue/wiki/index.php?BotCapturingNet
対象技術	研究開発状況
研究開発名称： 遠隔操作ウィルス包囲網 研究開発国： 日本 研究開発時期： 平成24年4月～	○　Gameover Zeus のようなウィルスを想定し、その通信をまねたプログラムを作成し、そのプログラムの検知をある程度できることを示している。スピードが遅いため、その部分の改良を行っている。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	○
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	国立大学法人島根大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	学術研究院理工学系
ホームページのURL	
研究説明のURL	https://www.staffsearch.shimane-u.ac.jp/kenkyu/search/f9744d5cdf8b80135d91ac82c25fb108/detail?page=research
対象技術	研究開発状況
研究開発名称： 耐量子計算機暗号の多項式数理における安全性評価手法の確立 研究開発国： 日本 研究開発時期： 平成31年4月1日～令和5年3月31日	

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	国立大学法人名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報基盤センター 情報基盤ネットワーク部門
ホームページのURL	
研究説明のURL	https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	研究開発状況
研究開発名称： （特になし） 研究開発国： 日本 研究開発時期： 継続的	

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	○
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	学校法人城西大学
代表者名	上原明
所在地	〒102-0094 東京都千代田区紀尾井町3番26号
窓口部署名	城西大学理学部事務室
電話番号	049-271-7728
関連部門名	とくに無し(現段階では個人による研究)。
ホームページのURL	http://www.josai.ac.jp
研究説明のURL	とくに無し。
対象技術	研究開発状況
研究開発名称： AIと情報セキュリティに関する研究 研究開発国： 日本 研究開発時期： とくに決めていない。	AI とりわけ深層学習理論と情報セキュリティの融合領域に焦点を当て研究している。まだ研究の初期段階であり、様々な知見を蓄積して、取り組むべき重要な問題(テーマ)を絞り込んでいる。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	○
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： IoT機器向き軽量暗号・認証方式 研究開発国： 日本 研究開発時期： 平成28年4月1日～	認証方式を開発した。仕様は論文として発表している。暗号方式への拡張を行っている。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： IoT機器のためのハニーポット 研究開発国： 研究開発時期： 平成29年8月1日～	現在、IoT機器向けハニーポットを開発している。プロトタイプは作成できている。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： ブロックチェーンを用いたログ保存システム 研究開発国： 日本 研究開発時期： 平成30年10月1日～	ブロックチェーンを用いてログを保存する要素技術を開発している。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	○
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	東京電機大学 総合研究所 サイバー・セキュリティ研究所
代表者名	
所在地	〒120-8551 東京都足立区千住旭町5番
窓口部署名	
電話番号	
関連部門名	東京電機大学 総合研究所 サイバー・セキュリティ研究所
ホームページのURL	http://www.dendai.ac.jp/crc/
研究説明のURL	http://www.lab.ine.aj.dendai.ac.jp/wordpress/
対象技術	研究開発状況
研究開発名称： セキュアー電子メール、秘密映像伝送、クラウドデータ保管 研究開発国： 日本 研究開発時期： 平成19年3月6日～令和2年12月31日	秘密電子メール、秘密映像伝送技術ならびにクラウドを活用したデータの安全分散保管技術に関しては、プロトタイプソフトウェアを試作し、技術展示が出来るレベルに達している。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	崇城大学
代表者名	理事長・学長 中山峰男
所在地	〒860-0082 熊本県熊本市西区池田4-22-1
窓口部署名	総合企画課
電話番号	096-326-3791
関連部門名	崇城大学 情報学部 情報学科
ホームページのURL	https://www.sojo-u.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 軽量カオス暗号の開発 研究開発国： 日本 研究開発時期： 平成27年4月1日～	カオスに基づく暗号用非線形変換関数を設計中である。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	学校法人立命館
代表者名	森島朋三
所在地	〒604-8520 京都市中京区西ノ京栂尾町8番地
窓口部署名	
電話番号	
関連部門名	情報理工学部
ホームページのURL	www.ritsumei.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 標的型攻撃における攻撃者特定 研究開発国： JP 研究開発時期： 平成30年4月1日～	方式検討を終了し、プロトタイプ実装中。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	○
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	国立大学法人お茶の水女子大学
代表者名	学長 室伏きみ子
所在地	〒112-8610 東京都文京区大塚2-1-1
窓口部署名	研究協力課
電話番号	03-5978-5503
関連部門名	お茶の水女子大学 小口研究室
ホームページのURL	http://www.ocha.ac.jp/
研究説明のURL	https://www.yama.info.waseda.ac.jp/crest/
対象技術	研究開発状況
研究開発名称： JST CREST ビッグデータ統合利用のためのセキュアなコンテンツ共有・流通基盤の構築 研究開発国： 日本 研究開発時期： 平成27年10月1日～令和3年3月31日	

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	○
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	北九州市立大学国際環境工学部
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	北九州市立大学国際環境工学部情報システム工学科
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 携帯端末を対象とした生体認証の信頼性に関する研究 研究開発国： 日本 研究開発時期： 平成28年4月1日～令和2年3月31日	本研究開発は,スマートフォンやタブレットPCなどの携帯端末において，個人の身体的特徴あるいは行動的特徴に基づき本人確認を行う生体認証システムの信頼性対策技術を確立することを目的とし,利用環境の変化に対する高い頑健性,生体情報の保護機能の具備,リソースに制約のある環境でのユーザの利便性やシステムの信頼性の維持の三点を柱とする従来にはない携帯端末に適した生体認証システムの実現を目指している.これまでの研究開発において，①認証システム自身がその場に適した認証方式を適応的に選択するという新たなコンセプトに基づくコンテキストアウェアネスなマルチファクタ認証システムの提案，②生体情報を保護するテンプレート保護技術に必要不可欠となる携帯端末から取得可能な筆記情報と音声を用いた生体ビット列生成アルゴリズムの提案，③プロセッサの性能やバッテリ,メモリの容量など使用可能なリソースに制約のある携帯端末での利用を想定した利便性・安全性・リソースのバランスを考慮したユーザ認証アルゴリズムの提案をそれぞれ行い,実際の利用場面を想定したシミュレーション実験に基づき提案方式の有効性を明らかにしている.今後は,開発した生体認証システムの携帯端末への実装に向けて,評価環境を実験室からフィールドに移し,実際の利用環境に近い条件下で当該システムの性能評価を実施する予定である.

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	http://www.pu-hiroshima.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 複数のセキュリティソフトウェアをオールインワン方式で組み込んだ教育用マイクロサーバの開発 研究開発国： 日本 研究開発時期： 平成22年4月～	大学および大学院の演習で利用することを想定し、オープンソースのセキュリティソフトウェアを複数組み合わせ、マイクロサーバ上で様々な機能を適宜切り替えて利用できるようなシステムを構築している。サーバ起動時に簡単に「ルータとして動作」、「ファイアウォール(IPS)として動作」といった切り替えができるようなシステムになっている

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	http://www.pu-hiroshima.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： コンテンツ指向型ネットワークにおけるキャッシュ改ざん対策 研究開発国： 日本 研究開発時期： 平成29年4月～	現在のIPネットワークとは異なるアーキテクチャである「コンテンツ指向型ネットワーク」において通信を阻害するために行われる攻撃であるキャッシュ改ざんを検知し、拡散を抑止する手法について検討・提案を行っている

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	http://www.pu-hiroshima.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 無線APの帯域不正占有対策 研究開発国： 日本 研究開発時期： 平成27年4月～	公共無線LANのAPの利用において、不正に帯域を専有しようとする行為である「inflated ACK-NAV」に対する対策手法の検討・提案を行っている

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	学校法人東北工業大学
代表者名	樋口龍雄
所在地	〒982-8577 宮城県仙台市太白区八木山香澄町35番1号
窓口部署名	情報サービスセンター
電話番号	022-305-3896
関連部門名	工学部 情報通信工学科 角田研究室
ホームページのURL	https://www.tohtech.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 人間社会のセキュリティ構造を模倣したIoT向け運用モデルの開発 研究開発国： 日本 研究開発時期： 平成27年4月～	基本要素のモデル化と基本要件の分析が完了し、インターネット標準のネットワーク管理技術を活用した概念実証のためのプロトタイプ実装を通じて提案の基本的実現性を確認している。現在は、プロトタイプ実装の改良による通信効率の改善などを図るとともに、様々なネットワーク管理技術を活用したプロトタイプ実装を開発し実用性に関する検討を進めている。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

イ　企業

企業・大学名	トビラシステムズ株式会社
代表者名	明田篤
所在地	〒460-0003 愛知県名古屋市中区錦2丁目5-12 パシフィックスクエア名古屋錦3F
窓口部署名	
電話番号	050-5533-3720
ホームページのURL	http://tobila.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 迷惑電話フィルタ 開発元(メーカー名等)： トビラシステムズ株式会社 開発国： 日本 価格： 発売時期： 平成23年6月～ 出荷数：	契約者の利用情報、警察・自治体からの提供情報、自社で独自に収集した情報を元に独自のアルゴリズムを利用して作成された迷惑電話番号情報を用いて、迷惑な電話をフィルタリングします。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	トビラシステムズ株式会社
代表者名	明田篤
所在地	〒460-0003 愛知県名古屋市中区錦2丁目5-12 パシフィックスクエア名古屋錦3F
窓口部署名	
電話番号	050-5533-3720
ホームページのURL	http://tobila.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 迷惑メッセージフィルタ 開発元(メーカー名等)： トビラシステムズ株式会社 開発国： 日本 価格： 発売時期： 平成29年9月21日～ 出荷数：	当社独自のアルゴリズムにより収集・分析した迷惑メールデータベースを活用し、詐欺につながるテキスト情報を含むメールやSMSをフィルタするサービス。迷惑メールデータベースは、利用者に届くメールやSMS情報を収集・分析し、迷惑URLとして出現頻度の高いURLや、迷惑メールとしての特徴を持つ本文情報から、独自のアルゴリズムにより危険な疑いのあるURL情報等をパタン抽出し、それらの情報について社内調査を行った上で構築している。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	株式会社FFRI
代表者名	鵜飼裕司
所在地	〒150-0013 東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4F
窓口部署名	総務部
電話番号	03-6277-1811
ホームページのURL	https://www.ffri.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： FFRI yarai 開発元(メーカー名等)： 株式会社FFRI 開発国： 日本 価格： 3～9,000円(ボリュームライセンス) 発売時期： 平成21年5月～ 出荷数： 2019年6月時点で約74万3千件の契約あり※サブスクリプション契約のため出荷数がありません	旧来のセキュリティ対策では防御できない標的型攻撃など、未知の脅威に対しても効果を発揮する次世代エンドポイントセキュリティ。 ＜特徴＞ ・θ-day攻撃や未知のマルウェアなど、未知の脅威にも効果を発揮 ・パターンファイルに依存しない独自の5つの検知エンジンを搭載 ・純国産技術による日本発の次世代エンドポイントセキュリティ ・「防御」を重視し、被害発生・事後対応コストを最小化 ・他社製品と同時使用が可能で、多重防御環境を実現 ・豊富な防御実績と導入実績の一部を公開 ・侵入した脅威の調査・レポーティング・除去を行うEDR機能も追加費用無しで利用可能

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	○
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	株式会社アズジェント
代表者名	杉本隆洋(代表取締役社長)
所在地	〒104-0044 東京都中央区明石町6番4号 ニチレイ明石ビル
窓口部署名	セキュリティ・プラス ラボ
電話番号	03-6853-7406
関連部門名	セキュリティ・プラス本部
ホームページのURL	https://www.asgent.co.jp/
研究説明のURL	https://www.asgent.co.jp/press/releases/2014/20140117-000373.html
対象技術	研究開発状況
研究開発名称： 不正アクセスの経路及び手法に関する調査研究 研究開発国： 日本 研究開発時期： 平成26年4月1日～継続中	セキュリティプラスラボ設立以来、世界中で横行する脅威の実態やその攻撃手法、またそれらの脅威からクラウド環境やモバイルデバイスを含めた情報資源を守るための対策技術の研究はもとより、国内外の有識者や組織との積極的な連携を図ることにより、技術だけでは守ることのできない「ソーシャルエンジニアリング」のような領域まで踏み込んだ広義での「セキュリティ」に関する調査、研究を継続して行っています。また、その調査・研究成果は講演活動、レポート、トレーニング等を通じて市場に発信しています。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	