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５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
- サイバーフィジカルセキュリティ技術の研究開発

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３年12月６日から令和４年1月21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ところ、次のとおり１者から計１件の提案があった。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の内容は当該企業から応募のあった内容を原則としてそのまま掲載している。

パスロジ株式会社

(2)　調査

警察庁が令和３年８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（14大学、23件）

東京理科大学（２件）
京都大学（３件）
岩手大学
東北工業大学
神奈川工科大学
東京電機大学
創価大学
中央大学（３件）
日本大学（４件）
金沢大学
中京大学
名古屋大学（２件）
立命館大学
福岡大学

イ　企業（５社、９件）

ソースネクスト株式会社
キャノン株式会社（４件）
富士電機株式会社（２件）
株式会社ネクストジェン
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３のとおりである。

なお、別添３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248校、企業1,595社の計1,843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～令和2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、令和2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～令和3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。

対象技術　その他アクセス制御機能に関する技術、高度認証技術
テーマ名　サイバーフィジカルセキュリティ技術の研究開発
開発年度　平成17年度～
実施主体　国立研究開発法人 産業技術総合研究所 **法人番号**　7010005005425
背景、目的 サイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合した社会では、サイバー空間、フィジカル空間、両者の境界における攻撃、それらを組み合わせた攻撃が存在する。これらの攻撃を防ぐアクセス制御技術として、高い安全性と効率性（速度、メモリ等）を両立する暗号技術の研究開発を行う。
研究開発状況（概要） 複雑なアクセス制御を柔軟に実現する高機能暗号技術や、暗号化した状態で検索や計算を行う技術（秘匿データベースについては企業との連携で実用化）、匿名認証技術、さらにはIoT機器との通信のセキュリティを高める軽量暗号技術等の提案を行っている。
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 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター TEL：03-3599-8001（代表） URL:https://www.cpsec.aist.go.jp/
将来の方向性 データの授受に関わるハードウェア、ソフトウェアのセキュリティ対策技術と組み合わせることで、サイバーフィジカルシステム全体のセキュリティ測定、強化、保証する技術を確立していく。

（別添２）

企業名（及び略称）　パスロジ株式会社 法人番号　8010001091039	
代表者氏名　小川 秀治	
所在地（郵便番号及び住所）東京都千代田区神田神保町一丁目６番地１　タキイ東京ビル７階	
関連部署名及び電話番号　ログインプロテクト担当窓口 03-5283-2263	
ＵＲＬ　https://www.passlogy.com/	
対象技術	技術開発状況
高度認証技術（ログインプロテクト） 平成26年度から研究開発を開始	インターネット上サービスなどへのログイン可能な時間を極限まで減らすことで、認証のセキュリティ強度を高める技術を開発。 これまでの認証の仕組みとの最大の相違は「認証を受け付けない状態が標準状態」であり、その状態においては、ログインフォームに対していかなるパラメータ（たとえ正解であっても）を送信してもシャットアウトすること。 正規の利用者がログインする際には、スマートフォンアプリをワンタップし、「これからログインする」という合図をサービスに送信し、サービス側は、合図を受け取ってから1分間だけ、ログインを待ち受ける状態になる。 この間に利用者はいつも通りのログイン操作で安全な認証を経て、ログイン可能となるので、不正アクセス及びアカウントロック攻撃 の被害に遭うリスクを低減することができる。 **本技術情報の詳細**：https://www.passlogy.com/pdf/loginprotect_202201.pdf

（別添３）

ア　大学

企業・大学名	東京理科大学
代表者名	本間　芳和
所在地	162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
ホームページのURL	https://www.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: クリプトボックス 開発元(メーカー名等): 株式会社クリプト・ベーシック 開発国: 日本 価格: 50万円 発売時期: 2012年4月1日～ 出荷数: 2	独自の鍵共有プロトコルと共通鍵暗号方式により従来と比較して10倍以上の鍵長を持つ暗号通信をもとに，強力なVPNを構築できる.

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	東京理科大学
代表者名	本間　芳和
所在地	〒162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
関連部門名	認証技術
ホームページのURL	https://www.tus.ac.jp
研究説明のURL	https://wakasapo.nedo.go.jp/seeds/seeds-0246/
対象技術	技術の概要・特徴など
研究開発名称： PDI認証 研究開発国： 日本 研究開発時期： 2016年4月1日～	理論及び研究実装，POC用プロトタイプが完成している． 現在，サービス開始を目指し，サーバー安定稼働，API整備を進めている．

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	

企業・大学名	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-u.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: eduroam JP 開発元(メーカー名等): 国立情報学研究所 開発国: 日本（欧州と共同開発） 価格: 無料 発売時期: 2006年8月～ 出荷数: 国内310機関	教育、研究機関で提供されるキャンパス無線LANを相互に安全にローミングで利用できるようにする国際的な認証連携のしくみ　www.eduroam.jp

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	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-u.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: 学術認証フェデレーション GakuNin 開発元(メーカー名等): 国立情報学研究所 開発国: 日本 価格: 無料 発売時期: 2009年4月～ 出荷数: 大学等258機関、サービス提供機関188	学術eリソースを利用する大学等と学術eリソースを提供する出社等が相互に認証連携を行うための国際的なしくみ www.gakunin.jp

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	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	〒606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
関連部門名	ネットワーク研究部門
ホームページのURL	https://www.media.kyoto-u.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 対話的に通信制御が可能なマルウェア解析システム 研究開発国： 日本 研究開発時期： 2020年4月～	マルウェア解析のためのサンドボックス上での通信制御の仕組みとして、対話的に制御が可能なシステムを開発している。

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	国立大学法人岩手大学
代表者名	学長　小川　智
所在地	〒020-8550 岩手県盛岡市上田三丁目１８番８号
窓口部署名	理工学部事務部
電話番号	019-621-6305
関連部門名	理工学部システム創成工学科知能・メディア情報コース
ホームページのURL	https://www.iwate-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： ウイルスの検出・分類に関する研究 研究開発国： 日本 研究開発時期： 2016年4月～	ウイルスの表層あるいは動的解析結果を利用した，機械学習による検出・分類手法の研究を行っている．

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	技術の概要・特徴など
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： 2015年4月～	基本要素のモデル化と基本要件の分析が完了しており，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プロタイプ実装を開発して，提案の概念実証と基本的実現性を確認している． 現在は，開発したプロトタイプ実装をベースとして実装の改良を進めるとともに，実用性に関する検討のため様々な IoT デバイスを対象とした実験を進めようとしている

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	神奈川工科大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学部
ホームページのURL	
研究説明のURL	https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=208504&item_no=1 https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=211007&item_no=1&page_id=13&block_id=8
対象技術	技術の概要・特徴など
研究開発名称： IoTマルウェアの解析技術の研究開発 研究開発国： 日本 研究開発時期： 2019年10月1日～2022年3月1日	IoTマルウェアの解析の要となるライブラリ関数の特定が完了した。今後はライブラリ関数の情報を活用して、関数のトレースによる動的解析技術やIoTマルウェアの検知・亜種分類の研究開発を行う予定である。

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	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	https://www.dendai.ac.jp/crc/
研究説明のURL	http://www.lab.ine.aj.dendai.ac.jp/wordpress/
対象技術	技術の概要・特徴など
研究開発名称： セキュア・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： 2007年3月6日～2021年12月31日	秘密電子メール、秘密映像伝達技術並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、技術展開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	創価大学　理工学部　情報システム工学科
代表者名	
所在地	〒192-0003 東京都八王子市丹木町1-236
窓口部署名	理工学部事務室
電話番号	042-691-9400
関連部門名	創価大学　理工学部　情報システム工学科
ホームページのURL	www.soka.ac.jp/science/infosys/
研究説明のURL	www.soka.ac.jp/science/infosys
対象技術	技術の概要・特徴など
研究開発名称： サイバーフィジカルシステムの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： 2017年4月1日～2023年3月31日	大学の研究室内での研究であり、実用等商品化は考えていない

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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	国際情報学部
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： SDNにおける文脈型動的セキュリティプロトコル 研究開発国： 日本 研究開発時期：	

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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	国際情報学部
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	http://www.iperc.uec.ac.jp/datafile/annualreport/iPERC2019HP.pdf
対象技術	技術の概要・特徴など
研究開発名称： 産業用インターネットオブシングス（Industrial Internet of Things: IIoT)機器・システムに対する遠隔セキュリティ検証手法 研究開発国： 日本 研究開発時期： 2019年4月1日～	制御システムの模擬プラントにおいて評価を進める中で、実用化する上での課題に対処している。

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	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報化学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： 生体から得られる電磁気情報を用いた個人認証システム 研究開発国： 日本 研究開発時期： 2016年12月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： ブロックチェーン技術を用いた単一医療機関向け診療記録システム 研究開発国： 日本 研究開発時期： 2017年12月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： 標的型メール対策訓練支援システム 研究開発国： 日本 研究開発時期： 2017年12月15日～	実験用のシステムを構築し、有効性の検証を行っている。

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	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： デジタルフォレンジック技術の学習支援システム 研究開発国： 日本 研究開発時期： 2018年9月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	国立大学法人金沢大学
代表者名	学長　　山崎　光悦
所在地	〒〒920－1192 石川県金沢市角間町
窓口部署名	研究・社会共創推進部研究推進課研究推進総務係
電話番号	076-264-5230
関連部門名	学術メディア創成センター
ホームページのURL	https://www.kanazawa-u.ac.jp/
研究説明のURL	ホームページでは公開しない
対象技術	技術の概要・特徴など
研究開発名称： Raspberry Gate 研究開発国： 日本 研究開発時期： 2011年4月1日～	組み込み機器のセキュリティ研究の一環としてアクセス制御の技術開発も行っている

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	中京大学
代表者名	
所在地	〒466-8666 名古屋市昭和区八事本町１０１－２
窓口部署名	学園経営戦略部
電話番号	052-835-7138
関連部門名	中京大学工学部
ホームページのURL	https://www.chukyo-u.ac.jp/
研究説明のURL	http://www.e-ontap.com/blog/?date=20210331
対象技術	技術の概要・特徴など
研究開発名称： 隠れオープンリゾルバスキャナ 研究開発国： 日本 研究開発時期： 2021年3月1日～	試験運用中。すでに数千の脆弱なネットワークを発見し、JPCERT/CC へ報告している。商用化の計画は無し。研究発表は 1,2 年中に計画。

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	国立大学法人東海国立大学機構名古屋大学
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研究部門 基盤ネットワーク研究G
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_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	技術の概要・特徴など
研究開発名称： （特に名称をつけていない） 研究開発国： 日本 研究開発時期：	大学における継続的な研究であり、特に期間を区切って研究開発しているわけではない。

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	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
ホームページのURL	
研究説明のURL	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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（立命館大学）
代表者名	森島朋三
所在地	〒604-8418 京都府京都市中京区西ノ京東栂尾町８番地
窓口部署名	BKCリサーチオフィス
電話番号	077-561-2802
関連部門名	情報理工学部
ホームページのURL	http://www.ritsumei.ac.jp/
研究説明のURL	https://www.asl.cs.ritsumei.ac.jp/研究プロジェクト:salvia
対象技術	技術の概要・特徴など
研究開発名称： 情報漏洩を防止するオペレーティングシステム 研究開発国： 日本 研究開発時期： 2003年4月1日～	情報漏洩を防止する基盤ソフトウェアというコンセプトに基づき，オーバヘッド，実現可能性，機能的限界などの各視点から，複数の実現手法について検討・開発を進めている．

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	○

企業・大学名	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福岡大学情報基盤センター中國研究室
ホームページのURL	
研究説明のURL	なし
対象技術	技術の概要・特徴など
研究開発名称： キーボード入力のタイミングを用いた生体認証 研究開発国： 日本 研究開発時期： 2016年9月1日～2022年3月31日	現段階では少数の被験者の協力による認証精度を確認している。 極めて高い認証精度を確認しており、近日中に多くの被験者を用いて、認認証精度を検証する計画である。 現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することを協議しており、同メーカーから日本国内に向けて販売することを目指す。

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	

イ　企業

企業・大学名	ソースネクスト株式会社
代表者名	代表取締役社長 兼 COO 小嶋智彰
所在地	105-7133 東京都港区東新橋1-5-2　汐留シティセンター33階
窓口部署名	
電話番号	
ホームページのURL	https://sourcenext.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: ZERO ウイルスセキュリティ 開発元(メーカー名等): K7 Computing Pvt Ltd. 開発国: インド 価格: 1,980円・税込（1台用） 発売時期: 2003年11月14日～ 出荷数: 累計1000万台以上	「ZERO ウイルスセキュリティ」は、2006年より更新料0円で発売している製品。 「ウイルスセキュリティ」そのものは2003年の発売です。 「ウイルスセキュリティ」のエントリー数はのべ1000万台を突破しています。

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	

企業・大学名	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
ホームページのURL	https://global.canon
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: imageRUNNER ADVANCE/DX シリーズ 開発元(メーカー名等): キヤノン株式会社 開発国: 日本 価格: 本体標準価格 67万円～500万円 発売時期: 2016年1月1日～ 出荷数:	弊社製品はオフィスにおけるネットワーク事務機器であり、顧客のオフィスネットワークインフラに接続され顧客情報が流通する為、セキュリティ脅威として、悪意や誤用による情報漏洩、他の情報機器へ攻撃踏み台としての悪用などの可能性に対して、高度な暗号化による盗聴防止、 ユーザ認証機能による権限のある情報参照への認可、 ファームウェアの改ざん防止・検知など、セキュリティに対して万全の備えを有している。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 改ざん検知・復旧技術開発 研究開発国： 日本 研究開発時期： 2017年5月～2022年1月	改ざん検知、復旧の順に開発を進めております。改ざん検知については商用化済みでして、復旧について商用化を目指して開発を進めている状況です。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 無線LANセキュリティ技術開発 研究開発国： 日本 研究開発時期： 2020年6月～2022年6月	無線LANセキュリティ技術開発として、1年以内の商用化を目指して、ハードウェアおよびソフトウェアの開発を進めております。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： Canon ID(コンシューマ向け認証認可基盤) 研究開発国： 日本 研究開発時期： 2015年1月～2022年12月	コンシューマ向け認証認可基盤として開発を進めております。Canon IDとして商用化済みでして、現在は、Canon IDに対して多要素認証の導入などセキュリティを向上する機能を提供するべく開発を進めている状況です。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	https://www.fujielectric.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: IoTプラットフォーム 開発元(メーカー名等): 富士電機株式会社 開発国: 日本 価格: 発売時期: 2018年9月1日～ 出荷数:	当社顧客サイトに設置されるエッジコントローラと、エッジコントローラにより収集したデータに基づきサービスを提供するクラウドから構成される。 提供サービスにはエネルギーマネジメント、稼働監視などが含まれる。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	技術開発本部　デジタルイノベーション研究所
ホームページのURL	https://www.fujielectric.co.jp/
研究説明のURL	https://www.fujielectric.co.jp/about/technology/fundamental/embedded_equipment.html
対象技術	技術の概要・特徴など
研究開発名称： 組込機器のセキュリティ技術 研究開発国： 日本 研究開発時期： 2019年4月1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	株式会社ネクストジェン
代表者名	大西　新二
所在地	108-0072 東京都港区白金1-27-6　白金高輪ステーションビル6F
窓口部署名	
電話番号	03-5793-3230
ホームページのURL	https://www.nextgen.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: VOIPセキュリティ診断サービス 開発元(メーカー名等): 株式会社ネクストジェン 開発国: 日本 価格: 実施内容による 発売時期: 2007年～ 出荷数: 200機器程度の診断実績	VIOP音声網に対するセキュリティ診断サービスです。新たな攻撃ツールや手法について継続的な調査を行っており、診断サービスでは、これらをもとに机上検討及び模擬攻撃を実施し、なりすましや改ざん、盗聴といった音声網へのリスクを可視化します。固定電話やモバイルなど通信事業者や、クラウドPBXサービス事業者、またはこれらに設備を導入するベンダが主な顧客です。国内の大手通信事業者が主な顧客ですが、詳細は当社HP（下記）をご覧ください。 https://www.nextgen.co.jp/solution/voip/service/sipvoip.html

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6-4　ニチレイ明石町ビル
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	技術の概要・特徴など
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： 2014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へ発信しています。

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	