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２年12月７日から令和３年1月22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２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　企業（４社、６件）

株式会社アイオーデータ機器（３件）
正栄食品工業株式会社
株式会社オロ
兼松株式会社

イ　大学（15大学、16件）

神奈川工科大学
上智大学
崇城大学
東京情報大学
北海道科学大学
佐賀大学
名古屋大学
東京電機科学大学
石巻専修大学
八戸工業大学
お茶の水女子大学
中央大学
福岡大学
金沢大学（２件）
東北工業大学

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222校、企業1,600社の計1,822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。

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、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）

ア　企業

企業・大学名	（株）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-SV4 開発元（メーカー名等）： アイオーデータ機器 開発国： 価格： ¥9,200～￥32,200 （容量による） 発売時期： 平成26年6月～ 出荷数：	パスワードロックとアンチウイルス機能を備えたＵＳＢメモリー

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）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-HB3 開発元(メーカー名等)： アイオーデータ機器 開発国： 価格： オープン 発売時期： 令和元年6月～ 出荷数：	パスワードボタン付きＵＳＢメモリー

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）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-FP 開発元(メーカー名等)： アイオーデータ機器 開発国： 価格： オープン 発売時期： 令和元年6月～ 出荷数：	指紋認証によるログイン機能を備えたＵＳＢメモリー

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	正栄食品工業株式会社
代表者名	本多市郎
所在地	〒110-8723 東京都台東区秋葉原5番7号
窓口部署名	総務部総務課
電話番号	03-3253-1211
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： トレンドマイクロ　ウィルスバスター 開発元(メーカー名等)： トレンドマイクロ 開発国： 日本 価格： 発売時期： 出荷数：	

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	株式会社オロ
代表者名	川田　篤
所在地	〒153-0063 東京都目黒区目黒3-9-1　目黒須田ビル
窓口部署名	コーポレート本部
電話番号	03-5724-7001
ホームページのURL	https://www.oro.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ＺＡＣ／ＲｅｆｏｒｍａＰＳＡ 開発元(メーカー名等)： アイオーデータ機器 開発国： 株式会社オロ 価格： 約3,200,000円 （ソフトウエア価格） 発売時期： 平成18年～ 出荷数： 1,000	Ｗｅｂブラウザから弊社サーバ（クラウド）にアクセスし、ＥＲＰ各種機能を利用。ＨＴＴＰＳ通信により、通信を暗号化。ログイン時は、ユーザ名・パスワードにより認証。アカウントロックの条件は、利用各社がマスタで設定。別途オプションとして、ＧｏｏｇｌｅアカウントＳＡＭＬ方式によるサインイン連携を提供。

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	兼松株式会社
代表者名	谷川　薫
所在地	〒105-8005 東京都港区芝浦1-2-1　シーバンスＮ館
窓口部署名	
電話番号	03-5440-8111
ホームページのURL	https://www.kanematsu.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Ａｃｃｏｕｎｔ＠Ａｄａｐｔｅｒ 開発元(メーカー名等)： 日立ソリューションズ株式会社 開発国： 日本 価格： オープン 発売時期： 出荷数： 不明	・ＭＡＣアドレス認証により、予め登録されたＰＣ端末以外の社内ネットワーク接続を防止する製品。 ・制御機能によるネットワーク遅延が発生しない仕様。

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 大学

企業・大学名	神奈川工科大学
代表者名	
所在地	〒243-0292 厚木市下荻野1030
窓口部署名	
電話番号	
関連部門名	セキュリティ研究センター
ホームページのURL	
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： 安全なＩｏＴサービスを実現するための総合セキュリティ対策技術 研究開発国： 研究開発時期： 令和2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	学校法人　上智学院
代表者名	佐久間　勤
所在地	〒102-8554 千代田区紀尾井町7-1
窓口部署名	上智大学　総務局　広報グループ
電話番号	03-3238-3179
関連部門名	暗号
ホームページのURL	www.sophia.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： 名称　特になし 研究開発国： 日本 研究開発時期： 平成30年4月～	秘密分散法のデータサイズに関する理論的研究。・シェアの生成法。・シェアサイズの見積り）に関する基礎研究を行なっている。

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	学校法人君が淵学園（崇城大学）
代表者名	理事長　中山峰男
所在地	〒860-0082 熊本市西区池田4-22-1
窓口部署名	地域共創センター
電話番号	096-326-3418
関連部門名	崇城大学情報学部
ホームページのURL	https://www.sojo-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： カオス暗号の研究 研究開発国： 日本 研究開発時期： 平成24年4月1日～	簡単な規則に基づくカオスを応用したＩｏＴ向け暗号を設計中である。

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	東京情報大学
代表者名	学長　鈴木　昌治
所在地	〒265-8501 千葉市若葉区御成台4-1
窓口部署名	総務課
電話番号	043-236-4603
関連部門名	ネットワークシステム研究室
ホームページのURL	http://www.tuis.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： ネットワークセキュリティ、情報ネットワーク技術に関する研究 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　北海道科学大学
代表者名	北海道科学大学　学長　渡辺泰裕
所在地	〒006-8585 北海道札幌市手稲区前田7条15丁目4-1
窓口部署名	入試　地域連携部研究推進課
電話番号	011-688-2241
関連部門名	北海道科学大学
ホームページのURL	https://www.hus.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： 多要素認証技術 研究開発国： 日本 研究開発時期： 平成28年4月～令和2年9月	基礎的な技術の実現可能性に対する初期検討段階

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　豊田　一彦
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	技術の概要・特徴など
研究開発名称： 耐量子計算機暗号プロトコル 研究開発国： 日本 研究開発時期： 平成31年4月1日～	量子コンピュータの解読に耐性のある暗号プロトコルを開発した。仕様は論文として発表している。計算量、通信量の評価を行っている

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
ホームページのURL	
研究説明のURL	https://www.net.nagoya-u.ac.jp/menber/shimada./
対象技術	技術の概要・特徴など
研究開発名称： （名前なし） 研究開発国： 日本 研究開発時期： 平成25年4月1日～	ＵＲＬから概要や発表文献を見て下さい。

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	東京電機科学大学総合研究所 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	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： 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	石巻専修大学
代表者名	学長　尾池　守
所在地	〒986-8580 宮城県石巻市南境新水戸1
窓口部署名	事務部　事務課（学務担当）研究支援係
電話番号	0225-22-7716
関連部門名	理工学部情報電子工学科
ホームページのURL	https://www.senshu-u.ac.jp/ishinomaki/
研究説明のURL	https://astesj.cam/v05/i05/p09
対象技術	技術の概要・特徴など
研究開発名称： ストリーム暗号 研究開発国： 日本 研究開発時期： 平成28年4月1日～	主にストリーム暗号に関する研究を行っている。カオス・ニューラルネットワークを用いた乱数発生器を様々な組込みシステムへの応用を試み、通信データの暗号化・複合化の高速化を目指す。最近では車載ネットワークCAN向けのストリーム暗号を提案した。詳細は「研究内容の説明がされているURL」の論文をご参照してください。

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	八戸工業大学
代表者名	学長　坂本　禎智
所在地	〒031-8501 青森県八戸市大字妙字大開88-1
窓口部署名	事務部　学事課
電話番号	0178-25-8111
関連部門名	ネットワークセキュリティ
ホームページのURL	syomu@hi-tech.ac.jp
研究説明のURL	https://www.hi-tech.ac.jp/profile/database.cgi?cmd=dp&num=18
対象技術	技術の概要・特徴など
研究開発名称： 遠隔健康支援システム 研究開発国： 日本 研究開発時期： 令和2年7月1日～ 令和3年1月29日	◎遠隔システム：在宅勤務者、および高齢者の方と遠隔でコミュニケーション（ビデオ会会議機能／チャット機能／録音・録画機能）を取るシステム（アプリ）をおいて、クラウドネットワークのセキュリティ構築方法を研究している。施設のケアスタッフは、呼出しがあった時、端末に発信者情報が自動でポップアップ表示され、発信者を確認出来る。また、発信者の蓄積データを選択して閲覧し、健康状態を推察できるように構築する。 ◎医療情報連携機能：バイタル機器と端末が連携しバイタル情報の収集・グラフ化を行い、サーバに通知する事で蓄積データを作成する。施設では、発信者情報を基に、各種蓄積データを閲覧する。 ◎研究開発状況：遠隔システム機能との連携で、サーバおよび端末の最新セキュアOSに対応したサーバの多層防御を想定し、不正プログラム対策・Webレピュテーション・IPS／IDSが可能な既存の製品を選択し、テストを行っている。サーバ保護に必要な複数の機能がオールインワンのSaaS型総合サーバセキュリティ機能を組み込むために、既存システムの改修部分を特定し、テストを実施する段階である。

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	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・産学連携課
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	技術の概要・特徴など
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3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	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事務室
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： 遠隔通信ロバストネステスト 研究開発国： 日本 研究開発時期： 平成31年4月1日～	技術研究組合 制御システムセキュリティセンター との共同研究により実施している。ネットワークにつながる系統連系保護装置やスマート保安を実現する機器の設置時や更改時に遠隔からセキュリティ試験を実施できるようにする。試験実施手順の煩雑さと誤判定率の高さを課題として、現在研究開発を進めている。試験対象が遠隔地に多数存在するため、試験の遠隔・自動化を進め、試験実施の負担を軽減することを目的としてる。今後のスマート保安におけるセキュリティ評価のあり方を具体的に検討する際に、実用化段階にあることを目指す。

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	

企業・大学名	福岡大学
代表者名	貫 正義（理事長）
所在地	〒814-0180 福岡県福岡市城南区七隈八丁目19-1
窓口部署名	情報基盤センター事務部 情報戦略室
電話番号	092-871-6631
関連部門名	福岡大学情報基盤センター研究開発室（中國研究室）
ホームページのURL	https://www.fukuoka-u.ac.jp/
研究説明のURL	https://passpath.net/ （現在は福岡大学内からのみアクセス可能）
対象技術	技術の概要・特徴など
研究開発名称： パスワード共有システム 研究開発国： 日本 研究開発時期： 令和元年12月1日～ 令和2年11月30日	研究開発はほぼ完了し、実装もほぼ完了している状況である。 研究開発成果をサービスとして学内外に無償で提供する計画である （本学の研究推進部などと協議中）。

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	総合メディア基盤センター
ホームページのURL	https://www.kanazawa-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： Raspberry Gate 研究開発国： 日本 研究開発時期： 平成27年4月1日～	Raspberry Gate は、IoTデバイスの集合体が構成する、小規模なローカルネットワークの対外接続点に設置するセキュリティゲートウェイであある。現在は、IPv4に対する実装と性能評価を終え、IPv6対応を進めている。

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	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	理工研究域電子情報通信学系
ホームページのURL	https://www.kanazawa-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： Privacy-preserving smart contracts on blockchains 研究開発国： 日本 研究開発時期： 令和2年4月1日～ 令和5年3月31日	We aim to design, build, and analyze a complete system that allows smart contracts on a blockchain to handle private data stored off-chain without compromising the privacy of the data. The main idea is to use a combination of cryptographic commitment schemes and zero-knowledge proof techniques, which have been tested and validated in several academic papers. A major challenge for realizing a general-purpose system that supports privacy-preserving smart contracts is its efficiency, both in terms of contract development and execution costs. Thus, we are now in the process of designing and developing domain-specific languages tailored for privacy-preserving smart contracts, as well as their optimizing compilers that produce smaller, more efficient zero-knowledge proofs to reduce the execution cost.

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： 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	○