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２件であり、その研究開発の概要は、別添１のとおりである。

Ｗｅｂ媒介型攻撃対策技術の実用化に向けた研究開発
HTTP相互認証プロトコル

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平成29年12月８日から平成30年１月26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。

甲賀電子株式会社

(2)　調査

警察庁が平成29年10月から11月にかけて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（６大学）

国士舘大学
関西大学
佐賀大学（３件）
日本大学
長崎大学（３件）
名古屋大学

イ　企業（２社）

株式会社ラック
ジャパンシステム株式会社

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330校、企業1,270社の計1,600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　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年度より以下の研究開発を開始、平成30年度に実施予定の実証実験に向けて研究開発は予定通り進捗中。平成32年度に終了予定だが、平成30年度に中間評価を行い、平成31年度以降の契約延長の可否を判定する。

（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の実証実験

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
（http://www.nict.go.jp/collabo/commission/itaku_kadai_h28.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　高度認証技術

テーマ名　HTTP相互認証プロトコル

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

HTTP相互認証プロトコルは、Webシステムでのフィッシング攻撃を防止するための新しい認証プロトコルです。

この認証プロトコルはPAKEと呼ばれる暗号・認証技術に新たな手法で改良を加え、Webの標準プロトコルであるHTTP及びHTTPSに適用したもので、ユーザがパスワードでサイトの真偽性を確認できる仕組みを提供することによって、フィッシングの防止を実現します。

研究開発状況（概要）

HTTP および HTTPS 上でのこれまでの標準認証技術である BASIC、DIGEST 認証法のフレームワークを拡張した形で、サーバがユーザを認証し、ユーザ側ではブラウザがサーバを自動的に認証するという、相互認証プロトコルを開発しました。これら認証は、ユーザのパスワードに関する情報が正しいサーバには登録されていて、偽サーバには無いことを利用して行われています。

開発したプロトコルの仕様が、インターネット技術の標準化を行っている IETF から3つの標準文書として発行されました(RFC 8053: HTTP Authentication Extensions for Interactive Clients, RFC 8120: Mutual Authentication Protocol for HTTP, RFC 8121: Mutual Authentication Protocol for HTTP: Cryptographic Algorithms Based on the Key Agreement Mechanism 3 (KAM3))。また技術を体験してもらうためのサーバ実装、Firefox、Chromium ベースのブラウザ（クライアント）の試験実装を公開しています。

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人産業技術総合研究所　情報技術研究部門
TEL: 029-862-6600
URL:https://www.itri.aist.go.jp/

将来の方向性

IETFで標準化されたHTTP相互認証プロトコルの仕様の普及を図り、開発技術がブラウザの標準機能として搭載されることを目指します。これにより、認証機能を個々のWebアプリケーションで作りこまなくても安全に実現することが可能になることから、偽サーバによる情報詐取被害の防止に貢献していきます。

（別添２）

企業名（及び略称）：甲賀電子株式会社 法人番号：9160001005362	
代表者氏名：代表取締役　中沼　忠司	
所在地（郵便番号及び住所）：〒520-3047　滋賀県栗東市手原5-8-10	
関連部署名及び電話番号：営業技術課　077-552-5123	
ＵＲＬ：http://www.koga.co.jp	
対象技術	技術開発状況
（注１） ・侵入検知・防衛技術 ・ぜい弱性対策技術 ・高度認証技術 開発年：2013年～2017年	【技術概要】 成り済ましによる侵入を防ぐ技術の提案です。 現状のインターネットの網機能（TCP/IP）は変更せず、ルーター・ホスト等の端末側のプロトコルを変更する軽微なソフト修正により実現します。 既存のIoTシステムには、通信回線と通信端末の間に本技術を実行するセキュリティ･ゲートウェイを設置することで､サイバー攻撃から保護します。 接続を許容するIPアドレスを予め登録しておき､正しい送信元の通信回線とは相互に回線認証して接続し､IPアドレスを偽証する発信者の通信回線とは１バイトのデータも授受せずに切断して侵入を防ぎ､不正アクセスを排除します。 【開発状況】 試作機を完成させ、本技術が有効に機能することを確認済み。 【工業所有権】 国際特許を出願済み、日本は特許査定。以後各国の特許を取得する予定。

（別添３）

ア　大学

企業・大学名	国士舘大学　理工学部
代表者名	理工学部長　二川　佳央
所在地	東京都世田谷区世田谷4-28-1
窓口部署名	
電話番号	03-5481-3251
関連部門名	国士舘大学　理工学部
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： 特になし 研究開発国： 日本 研究開発時期： 平成28年4月1日～平成29年7月31日	学内の論文誌（紀要）にて発刊予定のレベル。

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	学校法人関西大学
代表者名	池内　啓三
所在地	大阪府吹田市山手町3-3-35
窓口部署名	高槻事務局高槻キャンパス事務グループ
電話番号	06-6368-1121
関連部門名	関西大学　総合情報学部
ホームページのURL	www.kansai-u.ac.jp
研究説明のURL	http://www.firefly.kutc.kansai-u.ac.jp/
対象技術	技術の概要・特徴など
研究開発名称： スマートフォンのモーションセンサーを利用した個人認証 研究開発国： 日本 研究開発時期： 平成23年～	スマートフォンを動かす動作、つまりスマートフォンの移動情報を表す加速度・角速度センサーからの得られる情報が個人ごとに異なる特徴を持っていることに着目し、様々な動作で本人を確認できるセンサー情報の活用技術の開発を行っている。比較的低い本人拒否率を実現できているが、単純すぎる動作では他人受入率が高くなるため、動作にはある程度の複雑さが必要であること、認証アプリケーションの動作の制約でスマートフォンの画面を触りながら認証動作を行わなければならない、といった問題点が明らかになっている。現在のスマートフォン等のデバイスを利用開始する段階では、ロック解除する動作が必要であるが、ロック解除のための認証動作を行わずとも、そのデバイスの保持者の動作履歴を元に、所有者本人かどうかの確認を行うための技術開発を行なっているところである。

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	佐賀大学大学院工学系研究科
代表者名	工学系研究科長　渡　孝則
所在地	佐賀県佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学大学院工学系研究科知能情報システム学専攻廣友研究室
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： IoT機器のためのハニーポット 研究開発国： 日本 研究開発時期： 平成29年8月1日～	現在、ハニーポット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	佐賀大学大学院工学系研究科
代表者名	工学系研究科長　渡　孝則
所在地	佐賀県佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学大学院工学系研究科知能情報システム学専攻廣友研究室
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： IoT機器向き軽量認証方式 研究開発国： 日本 研究開発時期： 平成28年4月1日～	認証アルゴリズムの基本部分はできている。計算量評価、セキュリティレベル評価などの理論的評価はできている。プログラムを実装し、実験的評価を行っている段階である。IoT機器向けに機能の高度化、拡張を今後行う予定である

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	佐賀大学大学院工学系研究科
代表者名	工学系研究科長　渡　孝則
所在地	佐賀県佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学大学院工学系研究科知能情報システム学専攻廣友研究室
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： 悪性Webサイトのマルチ環境解析システム 研究開発国： 日本 研究開発時期： 平成27年4月1日～	悪性Webサイトの分析手法と分析プログラムの基本部分はできている。悪性Webサイトの分析妨害技術が日々進化しているので、それに対応できるように機能を拡張している。

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	学校法人日本大学
代表者名	
所在地	東京都千代田区九段南4-8-24（日本大学本部）
窓口部署名	
電話番号	
関連部門名	日本大学工学部情報工学科
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： 無線マルチホップネットワークコミュニティの参加管理 研究開発国： 日本 研究開発時期： 平成29年4月3日～平成32年3月25日	方式検討中

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	長崎大学　工学部　情報工学コース
代表者名	喜安　千弥
所在地	長崎県長崎市文教町1-14
窓口部署名	長崎大学工学部情報工学コース事務室
電話番号	095-819-2574
関連部門名	長崎大学工学部情報工学コース
ホームページのURL	http://www.cis.nagasaki-u.ac.jp/program/
研究説明のURL	http://www.cis.nagasaki-u.ac.jp/
対象技術	技術の概要・特徴など
研究開発名称： 計算機を用いた暗号プロトコルの安全性に関する研究 研究開発国： 日本 研究開発時期： 平成26年4月1日～平成29年12月1日	計算機を用いた暗号プロトコルの安全性評価として、暗号プロトコルの安全性自動検証ツールProVerifを用いた暗号プロトコル（各種ワンタムパスワード認証方式、TLS1.3など）の安全性評価を実施。

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	長崎大学　工学部　情報工学コース
代表者名	喜安　千弥
所在地	長崎県長崎市文教町1-14
窓口部署名	長崎大学工学部情報工学コース事務室
電話番号	095-819-2574
関連部門名	長崎大学工学部情報工学コース
ホームページのURL	http://www.cis.nagasaki-u.ac.jp/program/
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： 通信品質保証技術における未解決問題への挑戦 研究開発国： 日本 研究開発時期： 平成18年4月1日～平成29年11月13日	通信品質保証技術のうち、鍵となる理論についての研究を行っている。この理論は、渋滞の事前予測を可能にする。現状では、精度が悪かったために、空いているのに満車表示をしてしまう状況であったが、それを改善することができそうだというところまできている。※通信品質保証技術が完成すると、認証技術と合わせて、インターネットが元々持っているDDoSに対する脆弱性を克服できると言われている。

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	長崎大学　工学部　情報工学コース
代表者名	喜安　千弥
所在地	長崎県長崎市文教町1-14
窓口部署名	長崎大学工学部情報工学コース事務室
電話番号	095-819-2574
関連部門名	長崎大学工学部情報工学コース
ホームページのURL	http://www.cis.nagasaki-u.ac.jp/program/
研究説明のURL	www.cis.nagasaki-u.ac.jp/program
対象技術	技術の概要・特徴など
研究開発名称： 有限代数系の演算と暗号分野への応用 研究開発国： 日本 研究開発時期： 平成10年4月1日～平成29年11月（継続中）日	有限代数系に基づく暗号技術（RSA暗号／署名、ElGamal暗号／署名、楕円曲線暗号／署名など）に関する理論的研究（処理の高速化や安全性考察など）を行っている。これまでの研究成果として、代数曲線に付随するペアリングの計算手法の構築や、格子を用いた素因数分解手法の構築が挙げられる。

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	名古屋大学　情報学部
代表者名	情報学部長　村瀬　洋
所在地	愛知県名古屋市千種区不老町
窓口部署名	情報学部・情報学研究科　庶務係
電話番号	052-789-4716
関連部門名	名古屋大学　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	https://i.nagoya-u.ac.jp
研究説明のURL	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： 安全かつ便利な次世代ネットワーク 研究開発国： 日本 研究開発時期：	近年の標的型攻撃は高度化しており、マルウェア等の組織内への侵入を完全に防ぐことは難しくなっている。組織へのマルウェア侵入の疑いがある時には、組織内ネットワークを完全停止してマルウェア感染端末の炙り出しがしばしば行われるが、この方法は組織の業務を大幅に滞らせるという問題がある。もし、攻撃者が業務妨害を目的としているならば、その時点で攻撃者の目的は達成されてしまう。そこで、事前に組織内ネットワークをVLAN 等で分離しVLAN間の通信をネットワークスイッチ等で制御可能な形に設計すると同時に、業務フローのデータベースを記述し、マルウェア等による攻撃の発生時に継続可能な業務を最大限取りつつ、通信制御による攻撃封じ込めを試みるネットワーク管理者補助システムの研究を実施した。また、マルウェアやその活動検出および分類に関する研究として、マルウェア活動以外の一般のプログラムはネットワーク通信を学習し、そこから外れた物をマルウェア活動とする、アノマリ型のマルウェア活動検知の研究を実施した。主要な成果として、ネットワーク通信の間隔をもととして未知攻撃検知を行うもの、プロセスのAPI コールログからプロセスのマルウェアらしさを評価するもの、一般的なHTTP 通信に偽装して行うマルウェア通信をホストペア分割をもととした分類によって検出するものが挙げられる。

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	

イ　企業

企業・大学名	株式会社ラック
代表者名	代表取締役社長　西本　逸郎
所在地	東京都千代田区平河町2-16-1
窓口部署名	サイバー・グリッド・ジャパン　次世代技術開発センター
電話番号	03-6757-0100
ホームページのURL	https://www.lac.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： LAC Sparrow 開発元(メーカー名等)： 株式会社ラック 開発国： 日本 価格： 現状製品化はしているが、販売はしていない（当社サービスの中での活用 発売時期： 出荷数：	以下「CYBER GRID JOURNAL Vol.1」で公開しているP16,17で紹介してい記事をご確認ください。 https://www.lac.co.jp/lacwatch/pdf/20160901_cgjournal_vol1_s001t.f

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	ジャパンシステム株式会社
代表者名	井上　修
所在地	東京都渋谷区代々木1-22-1　代々木一丁目ビル3F
窓口部署名	セキュリティ事業本部　第一ソリューション部
電話番号	03-5309-0279
ホームページのURL	http://www.japan-systems.co.jp/index.html
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ARCACLAVIS Ways 開発元(メーカー名等)： ジャパンシステム株式会社 開発国： 日本 価格： 100ユーザ利用で80万円～ 発売時期： 平成10年4月 出荷数： 120万クライアントライセンス	ICカード、生体（顔、静脈、指紋など）などの認証デバイスを用いPCやシステムへのログオン時に二要素認証を実現するサーバ、クライアントシステム。企業、団体などでの運用、管理を行えるよう管理者向けの管理画面を用意。マルチテナント型であり、複数の企業や組織体で利用可能。官公庁、自治体などの公共分野で多数の実績あり。国産自社開発、保守体制で18年超のプロダクトである。

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	