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
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
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28年12月９日から平成29年１月27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４者から計４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。

イーロックジャパン株式会社
株式会社ギデオン
サイエンスパーク株式会社
フューチャーアーキテクト株式会社

(2)　調査

警察庁が平成28年８月から９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）

秋田大学
大阪府立大学
佐賀大学
東京情報大学
徳島大学
名城大学

イ　企業（２社）

アラクサラネットワークス株式会社
株式会社東京商工リサーチ（３件）

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325校、企業1,286社の計1,611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、IT総覧等）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　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

開発年度　平成24年度～平成27年度

実施主体　株式会社KDDI研究所、株式会社セキュアブレイン
（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研究所）、3010001090029（セキュアブレイン）

背景、目的

近年、攻撃者の改竄によって多くのWeb サイトに悪性サイトへのリダイレクト命令を埋め込まれ、それらサイトにアクセスしたユーザが悪性サイトへ誘導されてマルウェアに感染するといった被害が拡大している。これは、ブラウザやプラグインの脆弱性を悪用し、強制的にマルウェアをダウンロード・実行させるドライブ・バイ・ダウンロード攻撃（Drive-by-Download attack：以下DBD 攻撃）が原因である。

このDBD 攻撃は従来のリモートエクスプロイト攻撃とは異なり、ユーザのWeb アクセスを攻撃の起点とするため、ダークネット観測のような従来の受動的な攻撃観測手法ではその脅威を捉えられない。一方、能動的にWeb サイトをクローリングし検査を行うクライアントハニーポットのようなシステムを用いて、検知した悪性サイトのURL をブラックリストとして提供することで攻撃を防止する対策手法も存在する。しかし膨大な数のWeb サイトが存在し、なおかつ悪性サイトはそのURL を短期間で遷移させているという状況において、効果的な対策とするためには、シード（クローリングの起点）をどこに設定するかという問題点と、如何に検査したURL の鮮度を保つか（再検査までの期間を短くするか）という問題点が存在するなど、セキュリティ分野で未だ決定打となる対策が打ち出せていない状況が続いている。

本研究開発では、機構が検討してきた基本アーキテクチャ及びプロトタイプを踏まえた上で、DBD 攻撃についてその脅威を解明し、安心・安全なネットワーク社会の実現に向け、DBD 攻撃対策フレームワークの確立に資することを目指す。

研究開発状況（概要）

平成24年度より以下の研究開発を開始し平成27年度に終了。

（１）DBD攻撃大規模観測網構築技術
（２）DBD攻撃分析・対策技術
（３）DBD攻撃対策フレームワーク実証実験

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_h27.html）
電話 042－327－6011

将来の方向性

上記セキュリティ技術を確立し、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　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し、平成32年度に終了予定。但し、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。

これまでプロトコルを3つの文書で記述し、インターネット技術の標準化を行っている IETF での標準化提案を行いました。現在 HTTPAUTH WG で標準化の議論が行われており、議論の結果に基づき、サーバ実装、Firefox、Chromium ベースのブラウザ（クライアント）実装を改良してきました。平成29年1月に、標準化案3つのうちの1つで、提案プロトコルで必要となるパラメータ等を規定する文書が、RFC 8053 HTTP Authentication Extensions for Interactive Clientsとして標準化されました。

詳細の入手方法（関連部署名及びその連絡先）

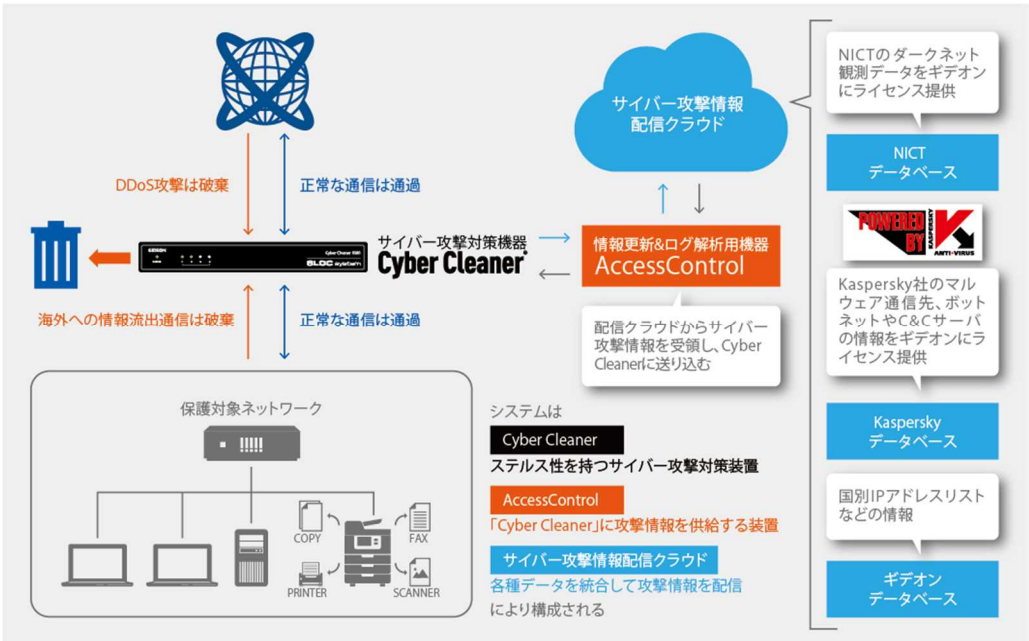
独立行政法人産業技術総合研究所　情報技術研究部門
TEL:029-861-5284
URL:http://www.itri.aist.go.jp/

将来の方向性

IETFで引き続き残りの2つの文書を標準化し、HTTP相互認証プロトコルが標準機能としてブラウザに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）：イーロックジャパン株式会社 法人番号：9010001131875	
代表者氏名：秦　基嘉	
所在地（郵便番号及び住所）：〒102-0083　東京都千代田区麹町3-12-7	
関連部署名及び電話番号：セキュリティコンサルタント事業部　03-3265-1169	
ＵＲＬ：http://www.elock.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 ・その他アクセス制御機能に関する技術 WebALARM:2000年、The GRID Beacon：2011年	（注２） ■WebALARM 不正侵入、改竄等防御対策として開発されたセキュリティ対策ソフトウェアです。Server上のあらゆる静的ファイルをリアルタイムに監視し、万一不正に改竄された場合でも検知後瞬時に自動復旧を行い、管理者への警告、証拠保全するリカバリーツールです。データアップデートに関しても監視を止めず自動更新可能です。また、PCIDSS要件10.5.5、11.5にも対応しております。 ■The GRID Beacon フィッシング手法、ＤＮＳ改竄による別サイトへの誘導やMITM、 MITB等あらゆる危険を完全に排除する2経路/2要素認証システムです。スマートフォンを強力なアウトオブバンド・マルチファクタ認証装置として利用することで、OTP専用機器やマトリクス表等といった複雑な認証要素は不要となり、低コストで老若男女を問わず利便性のよい強固なセキュリティを実現します。 また追加機能として、顔認証、声紋パターン認証等生体認証にも対応します。

企業名（及び略称）株式会社ギデオン 法人番号　2020001019903	
代表者氏名 代表取締役　西尾　高幸	
所在地（郵便番号及び住所）〒223-0056 神奈川県横浜市港北区新吉田町3448-4	
関連部署名及び電話番号 総務部 電話番号:045-590-1216	
ＵＲＬ http://www.gideon.co.jp/	
対象技術	技術開発状況
・侵入検知・防御技術 ・ぜい弱性対策技術 ・インシデント分析技術 ・その他アクセス制御機能に関する技術 開発年: 平成２６年度～ 平成２７年度	(1)Cyber Cleaner(製品名) はゲートウェイ（もしくはルータ）の上位に設置し通信(PPPoE通信上)を判定し、攻撃(有害)通信を遮断することで下位のネットワークを保護する。このことで外部からの攻撃(DDoS攻撃などによる)及び内部からの情報流出(マルウエア感染などによる)を防ぐ。 (2)サイバー攻撃情報(NICTからライセンスされた情報、Kaspersky社からライセンスされた情報、及びギデオン社から提供する国別、ISP別情報など)は、最新情報としてギデオン社から毎時配信され、Cyber Cleanerに反映され最新のサイバー攻撃に即応する。 (3)Cyber CleanerはIPアドレスをもたないため、機器自体が攻撃を受けることがなく、また攻撃により停止しない。 (4)PPPoE通信及びVPN通信の経路上に導入設置できる唯一のサイバー攻撃対策機器*。 (5)TCPヘッダ解析で判定するため、どのような通信環境にでも対応可能で、かつ処理が高速に行える。 ＊20170106現在 

企業名（及び略称）サイエンスパーク株式会社
法人番号　8021001026306

代表者氏名　小路　幸市郎

所在地（郵便番号及び住所）神奈川県座間市入谷3-1649-2

関連部署名及び電話番号　開発部SDK開発課　046-255-2544

ＵＲＬ　http://www.sciencepark.co.jp/

対象技術	技術開発状況
・その他アクセス制御機能に関する技術 平成13年～	「Driverwareセキュリティ SDK」は、エンドポイント向けの情報セキュリティシステムを開発する際に利用できるソフトウェア開発キットである。情報セキュリティ製品に必要な機能をOSの処理に近いカーネル層にて実現することで、情報流出経路の変化に対応する。近年はPCから各種スマートフォンへのデータ持ち出しを禁止する機能や、無許可のWi-Fi通信を禁止する等、新しいデバイスへの対応を行った。現在、Bluetooth通信の制御を開発中であり、今後も新しい情報流出経路への対応に取り組んでいく。 主要な機能は以下の通り。

ネットワーク制御	IPアドレス、ポート単位でのTCP/UDP通信制御、ログ収集、Wi-Fi通信の制御
ファイル制御	ファイルの読み込みと書込みの許可・禁止を制御
ファイルログ収集	ファイルアクセスのログ収集
ファイルの持ち出し承認機能	第三者による許可、禁止指示による、ファイルの持ち出しフロー
ライティング制御	CD、DVD、Blu-rayへの書き込み許可・禁止を制御、ログ収集
印刷制御	印刷の許可・禁止を制御、ログ収集
外部デバイス制御	iPhone、Android端末など、USB接続による携帯端末へのファイル持ち出し制御
暗号化制御	ファイル単位でのリアルタイム暗号化・復号
通信制御	シリアルや赤外通信などCOMポートの通信を制御します。
その他	キーボード等のHID（Human Interface Device）の入出力制御

＜＜製品概要＞＞
http://www.sciencepark.co.jp/information_security/sdk/summary.html

企業名（及び略称）フューチャーアーキテクト株式会社 法人番号　2010701032272	
代表者氏名　東 裕二	
所在地（郵便番号及び住所）〒141-0032 東京都品川区大崎1-2-2 ｱｰﾄｳﾞｨﾚｯｼﾞ大崎ｾﾝﾄﾗﾙﾀﾜｰ	
関連部署名及び電話番号　Technology Innovation Group / 03-5740-5723	
ＵＲＬ　http://www.future.co.jp/	
対象技術	技術開発状況
ぜい弱性対策技術 開発年： 平成28年度-平成29年度	国内のサイバー攻撃（標的型攻撃）による被害件数は年々増加しており、ソフトウェアやウェブアプリケーションの脆弱性への対応の遅れや漏れによるリスクは急速に高まっています。一方で新着の脆弱性情報は届け出のあるものだけで年間に約6000件を超え、それらをシステム管理者が手動で管理する負荷は高く、数百から数千のシステムを管理する場合にはとくに困難でした。 この課題を解決するために、当社はシステムが抱える保安上の欠陥に関する情報の収集と検知を全自動化した脆弱性スキャンツール「Vuls（VULnerability Scanner）」を開発し、2016年4月1日にオープンソース（*1）として無償で「GitHub」（*2）に公開いたしました。 「Vuls」は、オンプレミス環境とクラウド環境のどちらにも対応し、広範なソフトウェアの脆弱性をスキャンして日々発見される脆弱性がどのサーバに該当するかまで特定します。これにより管理者は脆弱性をリアルタイムに検知できるようになり、サイバー攻撃によるリスクを低減できます。また、内容や深刻度をひと目で把握できる日本語のレポートが発行され、システム管理者の負荷を大きく低減させます。 尚、「Vuls」は公開直後から世界中で話題となり、2016/10/1にGitHubスター獲得ランキング全言語第1位に入りました。またSlack（*3）コミュニティへの参加者も300名を超え、日々増加しています。 今後は、より広範なセキュリティ脅威に対応できるよう機能のブラッシュアップと拡張を図り、脆弱性スキャンツールのデファクトスタンダードを目指すとともに、エンタープライズ用途にも対応するサービスメニューとしての展開を目指します。 ＊1　オープンソースとは、ソースコードを広く一般に公開し、誰にでも無償で自由に扱えるようにしたソフトウェアのことを指します。 ＊2　「GitHub」はソフトウェア世界中の開発者のためのソースコード管理・共有を目的としたWebサービスです。 ＊3　「Slack」はチーム内でのコミュニケーションをとるためのチャットサービスです。 ※　「Vuls™」は、当社の親会社であるフューチャー株式会社が商標登録出願中です。 ■Vuls公開リポジトリ：　https://github.com/future-architect/vuls

（別添３）

ア　大学

企業・大学名	秋田大学理工学部
代表者名	村岡　幹夫
所在地	〒010－8502　秋田県秋田市手形学園町１－１
窓口部署名	総務担当
電話番号	018-889-2305
関連部門名	秋田大学　理工学部　数理・電気電子情報学科　人間情報工学コース
ホームページのURL	http://www.riko.akita-u.ac.jp/
研究説明のURL	http:www.ie.akita-u.ac.jp/
対象技術	技術の概要・特徴など
研究開発名称： 口唇の動き特徴を用いた個人認証 研究開発国： 日本 研究開発時期： 平成22年4月1日～平成31年3月31日	口唇の動き特徴から研究室レベル（20人程度）の個人認証が可能である

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	大阪府立大学　大学院　工学研究科
代表者名	辰巳砂　昌弘
所在地	〒599－8531　大阪府堺市中区学園町１－１
窓口部署名	共同研究，受託研究等に関するお問い合わせ研究連携推進課
電話番号	072-254-9107
関連部門名	電子透かし
ホームページのURL	http://www.eng.osakafu-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： 電子透かしを用いた改ざん検出と復元 研究開発国： 日本 研究開発時期：	あらかじめ，電子透かし技術を利用して画像に透かしを埋め込み，透かし入り画像を作成しておく．透かし入り画像に改ざんが施されたとしても，埋め込まれている透かしがどのように破壊されているかを確認することによって，どの領域が改ざんされたかを検出できる．その上，改ざんされる前の状態を，低解像度ではあるものの，復元可能である．

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 佐賀大学
代表者名	
所在地	〒840－8502
窓口部署名	
電話番号	
ホームページのURL	http://www.saga-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： Opengate, OpengateM 開発元(メーカー名等)： 佐賀大学 開発国： 日本 価格： オープンソース 発売時期： 出荷数：	無線LANや情報コンセントを利用する際に利用者を認証するためのシステムであり、Webによる平易なインターフェイスを持ち、特別なソフトウェアを導入することなく、利用可能です。利用者の認証終了後、ネットワークを利用することができ、利用終了後は即座に閉鎖します。IPv4のみだけでなく、IPv6にも対応しています。様々な認証方式に対応し、Shibbolethによるシングルサインオンにも対応しているのが特長です。また、Webによる認証と連携して、利用者のデバイスをMACアドレスで認証することも可能です。このACアドレス認証のためのデバイスの登録管理機能も有しています。Opengate　http://www.cc.saga-u.ac.jp/opengate/

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・セキュリティコース
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	徳島大学理工学部
代表者名	河村　保彦
所在地	〒770－8506 徳島県徳島市南常三島町２丁目１番地
窓口部署名	常三島事務部理工学部事務課総務係
電話番号	088-656-7304
関連部門名	知能情報系・ネットワークシステム制御研究室
ホームページのURL	http://www.tokushima-u.ac.jp/st/
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： M2M/IoTネットワークにおけるアクセス制御 研究開発国： 日本 研究開発時期： 平成28年4月1日～	構想段階

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	名城大学理工学部情報工学科　鈴木秀和研究室
代表者名	鈴木　秀和
所在地	〒　468－8502　名古屋市天白区塩釜口一丁目501番地
窓口部署名	理工学部事務室
電話番号	052-832-1151
関連部門名	理工学部
ホームページのURL	http://www.meijo-u.ac.jp/
研究説明のURL	http://www.ucl.meijo-u.ac.jp, http://www.ntmobile.net/
対象技術	技術の概要・特徴など
研究開発名称： NTMobile（Network Traversal with Mobility） 研究開発国： 日本 研究開発時期： 平成22年6月～	NTMobileとは，IPv4/IPv6混在ネットワークにおいて通信開始時に端末（PC，サーバ，スマートフォンのモバイル端末など）間で暗号鍵の交換および暗号化通信路を動的かつできる限りエンドツーエンドで構築する技術である．これまでに暗号化通信機能，通信相手認証機能，暗号鍵管理機能などの技術仕様を決定し，一部の機能についてはLinux，Android，iOSアプリとして実装が完了している．現在は企業と共同研究開発を進めており，研究開発成果をライブラリやサービスとして構築し，アプリケーション開発者などへ提供することを検討している．

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	

イ　企業

企業・大学名	アラクサラネットワークス株式会社
代表者名	南川育穂
所在地	〒212－0058　川崎市幸区鹿島田１－１－２　新川崎三井ビル　西棟
窓口部署名	
電話番号	
ホームページのURL	http://www.alaxala.com/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： AXシリーズ（スイッチ、ルータ） 開発元(メーカー名等)： アラクサラネットワークス株式会社 開発国： 日本 価格： ¥81,000（AX620R-2105）～ 発売時期： 平成16年10月1日 出荷数： 累計　167,600台（2015年9月30日時点）	AXシリーズは、VLANによるネットワーク分離やACL(Access Control List)による通信制御といった基本的なセキュリティ機能に加え、アクセス制御に関わる以下の特徴的な機能で安心なネットワークを提供します。1. ホワイトリスト機能 ネットワーク上の通信を学習し、自動で許可リストを作成。運用中は、ネットワークに上の全ての通信を監視。許可リストにない不正な通信を全てシャットアウトすることで、様々な攻撃からネットワークを効果的に守る。 対象モデル： AX2500S、AX260A2. トリプル認証IEEE802.1X認証/Web認証/MAC認証） 様々な端末が混在した環境でも、端末に応じた認証を利用可能。また、複数端末を集線するハブ経由でも認証が可能なため、コストパフォーマンスの高いネットワークを構築可能。対象モデル：AX8600S、AX8300S、AX8600R、AX620Rを除く全モデル3. セキュア仮想ネットワーク単一の物理機器上でネットワークを仮想的に分離する。ネットワーク上のトラフィックを分けることが可能なため、物理構成に囚われないセキュリティの確保が可能。また、機器の集約が可能なため、コスト低減も可能。対象モデル：AX2500S、AX2200S、AX1200S、AX260A、AX620Rを除く全モデル

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	株式会社　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ウイルスバスター 開発元(メーカー名等)： トレンドマイクロ株式会社 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　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： IBM Aliss 開発元(メーカー名等)： 日本アイ・ビー・エム株式会社 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　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： CISCO VPN-GW, Micorsoft Active Directory IIJ GIOリモートアクセス 開発元(メーカー名等)： シスコシステムズ合同会社, 日本マイクロソフト株式会社 株式会社インターネットイニシアチブ 開発国： 米国、米国、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	○