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７件であり、その研究開発の概要は、別添１のとおりである。

ネットワークセキュリティ技術の研究開発
セキュリティ知識ベースを用いたネットワークリスク評価と対策提示
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
HTTP相互認証プロトコル
漏洩に強い認証/鍵管理基盤 LR-AKE
ホワイトリスト制御技術
ハイパーバイザーによるシステムコール手順確認ツール

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27年12月11日から平成28年１月29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２者から計２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
サイエンスパーク株式会社

(2)　調査

警察庁が平成27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（２１大学）

秋田大学
岩手大学（２件）
岩手県立大学（５件）
宇都宮大学
大阪府立大学
九州大学（２件）
京都工芸繊維大学
熊本大学（２件）
高知大学
埼玉工業大学
佐賀大学（２件）
静岡大学（２件）

芝浦工業大学
信州大学
崇城大学
千葉工業大学
東海大学（２件）
東京理科大学
東北学院大学
日本文理大学（２件）
八戸工業大学

イ　企業（３社）

キャノンITソリューションズ株式会社（３件）
京セラコミュニケーションシステム株式会社（４件）
株式会社バッファロー

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1,080社の計1,405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　ネットワーク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

ネットワーク上におけるサイバー攻撃・不正通信等に耐えるとともに、それらを検知・排除するため、イベント（スキャン、侵入等）の収集・測定及びこれに基づく傾向分析・脅威分析を実時間で行い予兆分析を含めた対策手法の迅速な導出を行うインシデント対策技術の研究開発を行う。

研究開発状況（概要）

これまでに研究開発・整備した広域に設置された観測点からのセキュリティログの分析手法、マルウエアの収集機構・収集したマルウエアの分析機構に関して、日本全国規模の観測網構築に向けた観測対象ネットワークの更なる拡充、より高度な観測アーキテクチャ・攻撃検出機構の開発、マルウエアの分析精度の高度化を行った。この結果をこれまでに構築したインシデント分析システムに反映し、観測結果をWeb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始めるなど、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　ネットワーク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　ぜい弱性対策技術

テーマ名　セキュリティ知識ベースを用いたネットワークリスク評価と対策提示

開発年度　平成23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

ネットワークに対する攻撃、ネットワークを通じた攻撃は、プロトコルの設計や製品の実装などにおける誤りに起因する脆弱性を利用して仕掛けられる。また、複数の脆弱性を組み合わせて利用する攻撃も脅威となっている。そのため、ネットワーク利用における脆弱性の存在を把握し、その脆弱性を利用した攻撃に基づくリスクをあらかじめ認知するとともに、その脆弱性の対策法を利用者に提示できる仕組みが必要であり、そのための技術開発が求められている。

研究開発状況（概要）

脆弱性を含むネットワーク機器や、脆弱性を含むプロトコルの情報をセキュリティ知識ベースとして蓄え、当該知識ベースを活用してネットワーク利用者がサービスを利用する際に発生しうるリスクを導出して可視化するとともに、リスクを低減する対策技術を提示するプラットフォームの研究開発を行っている。これまでに、セキュリティ知識ベースを活用することにより、スマートフォンアプリを利用する際に被るリスクを可視化して提示するシステム、および企業内ネットワークに接続される情報機器に残存する脆弱性を自動的に検知してその対策方法を提示するシステムを開発した。

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　ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室　042-327-6858

将来の方向性

セキュリティ知識ベースを活用して、あらゆるネットワーク利用におけるリスク対策法の提示を実現する研究開発を行う。

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

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年度に終了予定。

（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 産学連携部門 委託研究推進室
（http://itaku-kenkyu.nict.go.jp/index.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　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

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。

これまでにプロトコルの標準化案を公開し、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っています。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。

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　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 でプロトコルを標準化し、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。

対象技術　高度認証技術

テーマ名　漏洩に強い認証/鍵管理基盤 LR-AKE

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

パスワードは現在最も広く使われているセキュリティ要素の一つであるが、フィッシング詐欺や、サーバからのパスワードハッシュの漏えい、クライアント端末からのパスワード暗号化ファイルの漏えいなどに弱いという問題点の他、複数のパスワードを管理しなければならず、それらを覚えきれないという問題点があった。そこで、これらの問題点を解決するための新たなパスワード認証方式 LR-AKE/AugPAKE およびそれらを応用したパスワードや鍵の遠隔分散管理方式、ID 連携手法などの研究開発を行った。

研究開発状況（概要）

LR-AKE はクライアント／サーバいずれからの記録情報の漏えいにも耐性のある次世代の２要素認証技術である。２要素認証に加えて鍵やパスワードなどの重要情報の遠隔分散管理機能、ID 連携機能などを有する。産総研技術移転ベンチャーにより製品化され、利用時のサポートも提供されている。また、LR-AKE の初期設定時に短いパスワードのみを用いて行われる相互認証プロトコルは IETF において RFC6628 として承認され、現在、その参照実装とその改良を行っている。

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　情報技術研究部門
TEL:029-862-6600
URL:http://www.itri.aist.go.jp/

将来の方向性

本技術は既に実用化され、技術移転可能な状態にある。また、産総研技術移転ベンチャー企業 BURSEC(株) などからシステム導入時や利用時のサポートを受けることも可能である。

対象技術　侵入検知・防御技術

テーマ名　ホワイトリスト制御技術

開発年度　平成 24 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

制御システムなどでは経済性の観点から汎用の OS を利用するが､特定のアプリケーションのみが特定の計算資源（ファイル、デバイス、IP アドレス、ポート）のみを使って動作するものが多い。このような環境では他の計算資源は使わないために、それらを制限することで攻撃を困難にするホワイトリスト制御技術を開発する。

研究開発状況（概要）

アプリケーションの実行順番や利用する計算資源（ファイル、デバイス、IP アドレス、ポート）を規定し、それ以外の利用方法は禁止するホワイトリスト制御技術を作成した。Windows7 32bit と Windows XP Embedded のドライバとしては利用可能になっている。現在はプロセスに対する攻撃である DLL インジェクション、スクリプトインジェクションに対応する拡張を行っている。

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　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

WindowsXP のように OS のサポートが終わっても特定アプリケーションを動かしたい要求は多い。そのような環境では他の計算資源は不要なため、作成しているホワイトリスト制御を提供することで、他の計算資源の脆弱性に関連する攻撃を抑制する技術として展開していく予定である。

対象技術　侵入検知・防御技術

テーマ名　ハイパーバイザーによるシステムコール手順確認ツール

開発年度　平成 24 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

多くの攻撃はアプリケーションの脆弱性を突いて、作成者の意図しない動作手順を起すことで、情報取得や破壊行為を行う。アプリケーションが作成者の意図した通りに動作していることを第三者的に確認することで、侵入検知を行う。

OS やアプリケーションに変更を加えることなく侵入検知を行うために、OS とハードウェアの間に入るハイパーバイザーを作成し、アプリケーションから OS に処理を依頼するシステムコールを監視する。システムコールの呼び出し順番がアプリケーションの定義と異なれば攻撃として検知する。

研究開発状況（概要）

Windows とハードウェアの間に挿入され、Windows のシステムコールをトレースするハイパーバイザーを開発している。アプリケーションが発行するシステムコールの呼び出し手順を予め登録しておき、それから反した呼び出しがあった場合にマルウェアとして認識する技術を開発している。現在は Windows 7 32bit のシステムコールログ取得ができるプロトタイプを開発し、詳細な呼び出し手順確認の拡張を行っている。

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　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

アプリケーションから発行されるシステムコールは複雑であり、状態遷移が爆発する。一つ一つ状態遷移を確認する手法は動作が少ないアプリケーションに限られるため、今後は機械学習等による多量データ解析と併用して、複雑なアプリケーションに対する攻撃にも対処できるようにする。また、多くのテストベッドを用意して、システムコールのログを大量に取得し、挙動が環境に依存するマルウェアの検出も行う予定である。

（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
・侵入検知・防御技術 ・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	１）「WebALARM」は、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。また、PCIDSS要件10.5.5、11.5にも対応しております。 ２）「The GRID Beacon」は、不正アクセスやMITM、MITB等の攻撃を防ぐ2要素/2経路認証システムです。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。

<table>
<tr><td colspan="2">企業名（及び略称）サイエンスパーク株式会社
法人番号　8021001026306</td></tr>
<tr><td colspan="2">代表者氏名　小路　幸市郎</td></tr>
<tr><td colspan="2">所在地（郵便番号及び住所）神奈川県座間市入谷3-1649-2</td></tr>
<tr><td colspan="2">関連部署名及び電話番号　開発部SDK開発課　０４６-２５５-２５４４</td></tr>
<tr><td colspan="2">ＵＲＬ　http://sciencepark.co.jp/</td></tr>
<tr><td>対象技術</td><td>技術開発状況</td></tr>
<tr><td>・その他アクセス制御機能に関する技術
平成１３年～</td><td>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開発キット『Driverwareセキュリティ SDK』を開発した。PCからファイルの持ち出しを禁止する機能や、ファイル操作等のログを収集する機能、ファイルを暗号化する機能等の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している。
年々変化する情報流出経路に対応するため、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順次行った。現在も継続して、新デバイスへの対応に取り組んでいる。

実現している機能は以下の通り。
<table>
<tr><th>機能</th><th>概要</th></tr>
<tr><td>ネットワーク制御</td><td>IP アドレス、ポート単位でのTCP/UDP 通信制御、ログ収集</td></tr>
<tr><td>ファイル制御</td><td>ファイルの読込みと書込みの許可・禁止を制御</td></tr>
<tr><td>ファイルログ収集</td><td>ファイルアクセスのログ収集</td></tr>
<tr><td>持ち出し認証機能</td><td>第3 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</td></tr>
<tr><td>ライティング制御</td><td>CD、DVD、Blu-ray への書込み許可・禁止、ログ収集</td></tr>
<tr><td>印刷制御</td><td>印刷の許可・禁止、ログ収集</td></tr>
<tr><td>外部デバイス制御</td><td>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</td></tr>
<tr><td>暗号化制御</td><td>ファイル単位でのリアルタイム暗号・復号</td></tr>
<tr><td>その他</td><td>キーボード等のHID (Human Interface Device)の入出力制御</td></tr>
</table>
<<製品概要>>
http://www.sciencepark.co.jp/information_security/sdk/summary.html</td></tr>
</table>

（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番1号
窓口部署名／電話番号	総務担当／018-889-2305
関連部門名	秋田大学理工学部
ホームページのＵＲＬ	http://www.riko.akita-u.ac.jp/index.html
研究説明のＵＲＬ	
対象技術	研究開発状況
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 研究開発期間： 2010年4月1日～ 2018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	岩手大学教育学部吉田研究室
代表者名	吉田等明
所在地	〒020-8550 岩手県盛岡市上田3丁目18番33号
窓口部署名／電話番号	019-621-6534
ホームページのＵＲＬ	
製品説明のＵＲＬ	http://www.cpi-tec.jp/adtek/seihin/J-crypt/index.html
対象技術	技術の概要・特徴など
製品名： 情報セキュリティシステム J-crypt 開発元： （株）エマージングテクノロジー （株）アドテックシステムサイエンス 開発国： 日本 価格： 25万円程度 発売時期： 2006年9月1日 出荷数： 10	暗号・復号にはUSB接続されるキーを用いたもの。 （株)アドテックシステムサイエンスの破産に伴い，現在は販売は行っていない。

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	岩手大学教育学部吉田研究室
代表者名	吉田等明
所在地	〒020-8550 岩手県盛岡市上田3丁目18番33号
窓口部署名／電話番号	019-621-6534
関連部門名	吉田研究室
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： カオス暗号の実用化等に関する研究 研究開発国： 日本 研究開発期間： 2000年～	乱数生成の高速化と堅牢性の向上に関する研究

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	岩手県立大学ソフトウェア情報学部高田研究室
代表者名	高田　豊雄
所在地	〒020-0693 岩手県滝沢市滝沢152-52
窓口部署名／電話番号	019-694-2500
関連部門名	岩手県立大学ソフトウェア情報学部高田研究室
ホームページのＵＲＬ	http://callisto.comlab.soft.iwate-pu.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： スマートフォンのキーストロークダイナミクスを用いた個人認証 研究開発国： 日本 研究開発期間： 平成24年～平成27年	最近のスマートフォンは加速度センサ、感圧センサ等の様々なセンサをもち、また、トグル入力やフリック入力等、スマートフォン特有のキー入力方式を有する。本研究は以上のような特性をもつスマートフォン向けのキーストローク入力に基づく個人認証方式を提案している。提案方式は歩行中や自動車の乗車中でも優れた等エラー率を有する。

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	岩手県立大学ソフトウェア情報学部高田研究室
代表者名	高田　豊雄
所在地	〒020-0693 岩手県滝沢市滝沢152-52
窓口部署名／電話番号	019-694-2500
関連部門名	岩手県立大学ソフトウェア情報学部高田研究室
ホームページのＵＲＬ	http://callisto.comlab.soft.iwate-pu.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： ライフログ情報を用いた個人認証 研究開発国： 日本 研究開発期間： 平成25年～平成26年	近年、twitter、facebookといったSNSが日常生活に密着する形（以下、ライフログ）で盛んに利用されている。一方、従来のパスワード認証は安全性（推測困難性）と記憶容易性の高いトレードオフを図ることは困難であった。本研究ではライフログの内容がユーザ本人にとって記憶の想起が容易であることを利用したパスワード作成補助方式と認証方式を提案している。

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	岩手県立大学ソフトウェア情報学部高田研究室
代表者名	高田　豊雄
所在地	〒020-0693 岩手県滝沢市滝沢152-52
窓口部署名／電話番号	019-694-2500
関連部門名	岩手県立大学ソフトウェア情報学部高田研究室
ホームページのＵＲＬ	http://callisto.comlab.soft.iwate-pu.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： パスワードリスト攻撃を考慮したパスワード管理方式 研究開発国： 日本 研究開発期間： 平成27年～	近年、個人ユーザは複数のインターネットサービスを利用することが一般的であり、多くのサービスではパスワード認証が用いられている。パスワードリスト攻撃は、攻撃者が何らかの方法で入手した、あるサービスのパスワードリストを他のサービスの不正ログインに用いる手法である。多くのユーザは複数のサービスで同一あるいは類似のパスワードを用いる傾向がありパスワードリスト攻撃を蔓延させる結果となっている。本研究では、各サービス（あるいはサービス実施ホスト）の特徴抽出と分類からユーザのパスワード作成と使い分けを補助する方式を提案する。

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	岩手県立大学ソフトウェア情報学部高田研究室
代表者名	高田　豊雄
所在地	〒020-0693 岩手県滝沢市滝沢152-52
窓口部署名／電話番号	019-694-2500
関連部門名	岩手県立大学ソフトウェア情報学部高田研究室
ホームページのＵＲＬ	http://callisto.comlab.soft.iwate-pu.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： インターネット観測システムの観測点保護方式 研究開発国： 日本 研究開発期間： 平成24年～	インターネットにおいて脆弱性やその他攻撃の傾向をいち早く把握・周知するシステムとしてインターネット観測システムがあり、わが国でも情報通信研究機構のnicterや警察庁の@police等が知られている。このシステムでは観測点の配置が攻撃者に知られると観測点を迂回されたり観測点がDoS攻撃に遭う可能性があり、観測点配置は秘匿される必要がある。本研究では様々な観測点検出攻撃に対する対処方式を提案している。

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	岩手県立大学ソフトウェア情報学部高田研究室
代表者名	高田　豊雄
所在地	〒020-0693 岩手県滝沢市滝沢152-52
窓口部署名／電話番号	019-694-2500
関連部門名	岩手県立大学ソフトウェア情報学部高田研究室
ホームページのＵＲＬ	http://callisto.comlab.soft.iwate-pu.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： ライフログ記載情報を用いた個人認証 研究開発国： 日本 研究開発期間： 平成25年～平成26年	近年、twitter、facebookといったSNSが日常生活に密着する形（以下、ライフログ）で盛んに利用されている。一方、従来のパスワード認証は安全性（推測困難性）と記憶容易性の高いトレードオフを図ることは困難であった。本研究ではライフログの内容がユーザ本人にとって記憶の想起が容易であることを利用したパスワード作成補助方式と認証方式を提案している。

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	宇都宮大学オプティクス教育研究センター
代表者名	谷田貝　豊彦
所在地	〒321-8585 栃木県宇都宮市陽東7-1-2
窓口部署名／電話番号	オプティクス教育研究センター事務室／ 028-689-7074
関連部門名	情報フォトニクス
ホームページのＵＲＬ	http://www.opt.utsunomiya-u.ac.jp
研究説明のＵＲＬ	www.yamamotolab.science/
対象技術	研究開発状況
研究開発名称： セキュアディスプレイ 研究開発国： 日本 研究開発期間： 2014年4月1日～	情報表示画面の覗き込み、映像信号の盗聴を防止するために、光学的に復号される暗号を用いて、映像信号の暗号化と観察位置の3次元的な限定を行なう情報表示のセキュリティ技術（セキュアディスプレイ）を提案し、プロトタイプを開発している。

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	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／電話番号	共同研究、受託研究等に関するお問合せ 研究連携推進課／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	研究開発状況
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 研究開発期間：	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、改ざんされる前がどのようであったのかを、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	九州大学　システムＬＳＩ研究センター
代表者名	福田　晃
所在地	〒819-0395 福岡市西区元岡744
窓口部署名／電話番号	システムＬＳＩ研究センター
ホームページのＵＲＬ	http://www.kyushu-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： VRICS (Value and Right Circulation control System) 開発元： 九州大学 開発国： 日本 価格： 発売時期： 出荷数：	セクトラルモデルを実現したID管理と，ICカードなどの認証デバイスを用いた個人認証を特長とした情報基盤。 サービス毎に異なるIDを用いてサービスを提供し，他の同様のIDとの間に隠された関係性を有する、個人にユニークに付番したIDを秘匿としたHidden relationship ID Accessモデルを実現している。

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	九州大学　システムＬＳＩ研究センター
代表者名	福田　晃
所在地	〒819-0395 福岡市西区元岡744
窓口部署名／電話番号	システムＬＳＩ研究センター
関連部門名	九州大学
ホームページのＵＲＬ	http://www.kyushu-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： 未定（ＶＲＩＣＳ） 研究開発国： 日本 研究開発期間：	実証実験中、機能拡張検討中。

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	京都工芸繊維大学 情報工学・人間科学系 情報セキュリティ研
代表者名	稲葉 宏幸
所在地	〒606-8585 京都市左京区松ヶ崎橋上町1
窓口部署名／電話番号	075-724-7499
関連部門名	情報工学・人間科学系　情報セキュリティ研究室
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： HW法によるIDSログ分析システム 研究開発国： 日本 研究開発期間： 2013年4月1日～	近年、ネットワークを介した情報システムが広く利用されている。 しかし、サイバー攻撃による情報漏洩等の被害が多数報告されており、ネットワークセキュリティの確保は重要な問題のひとつである。 対策技術のひとつである侵入検知システム(IDS) は、一般に膨大な量の検知アラートが発生するため、その情報を有効に利用し組織のセキュリティ向上に役立てることは必ずしも容易ではない。 本システムは、この問題に対し、Holt-Winters (HW) 法を用い、IDS の警告イベント数を予測するシステムであり、不定期に大量の検知が発生するようなイベントであっても高い予測精度を保つことができる。

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	国立大学法人熊本大学工学部
代表者名	工学部長　村山伸樹
所在地	〒860-8555 熊本県熊本市中央区黒髪2丁目39-1
窓口部署名／電話番号	国立大学法人熊本大学教育研究推進部自然科学系事務ユニット総務担当／096-342-3514
関連部門名	
ホームページのＵＲＬ	http://www.kumamoto-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： ロケーションプライバシー保護 研究開発国： 日本 研究開発期間： 2013年～2015年	k-anonymityに基づくローケーションのクローキング手法の実現可能性を確認した。

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	国立大学法人熊本大学工学部
代表者名	工学部長　村山伸樹
所在地	〒860-8555 熊本県熊本市中央区黒髪2丁目39-1
窓口部署名／電話番号	国立大学法人熊本大学教育研究推進部自然科学系事務ユニット総務担当／096-342-3514
関連部門名	
ホームページのＵＲＬ	http://www.kumamoto-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： クラウドコンピューティング環境のセキュリティ 研究開発国： 日本 研究開発期間： 2014年～2015年	問題があるかを検討中。（まだ問題がはっきりと見つかっていない。）

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	高知大学 教育研究部自然科学系理学部門 鈴木一弘研究室
代表者名	鈴木一弘
所在地	〒780-8520 高知県高知市曙町二丁目5-1
窓口部署名／電話番号	
関連部門名	
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： 推論による情報漏えい防止のためのリスク評価アルゴリズムの研究 研究開発国： 日本 研究開発期間：	SNS上で「地震だ」とつぶやくと、つぶやいた時刻と、気象庁の地震情報を基にしてそのユーザの居所がある程度絞り込まれてしまう。このようなタイプの情報漏えいを推論による情報漏えいと呼ぶ。本研究では推論による情報漏えいを防ぐために、グラフモデル（情報同士の推論関係をネットワークモデル化したもの）上でのシミュレーションや漏えいリスク評価をするアルゴリズムを研究開発する。現在の研究開発状況はまだ初期段階である。

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	埼玉工業大学
代表者名	内山俊一（学長）
所在地	〒369-0293 埼玉県深谷市普済寺1690
窓口部署名／電話番号	情報基盤センター／048-585-6823
関連部門名	
ホームページのＵＲＬ	http://www.sit.ac.jp/
研究説明のＵＲＬ	http://www.sit.ac.jp/user/watabe/
対象技術	研究開発状況
研究開発名称： 研究開発国： 研究開発期間： 2003年4月1日～	防犯カメラ画像中の耳介画像から容疑者候補を挙げるシステムの作成を目指し、耳介認証の研究をしています。耳介正面による認証ならRank1認証率99.5%、等誤差率は0.5%程度にできます。しかし耳介は撮影角度の変化による形状の違いが大きいので3D統計モデルを利用した認証が必要になります。研究の結果、特徴点周辺に限定した3D統計モデル（モデル法線）の作成に成功し、20° 撮影角度が違う場合、 Rank 1認証率が78.4%から97.6%に、 30° 違う場合、56.1%から80.0%に向上できることがわかりました（渡部他、映情学誌、65,7,1016-1023,(2011)、科研費研究課題番号 22700219）。この手法の適用範囲の調査、改良を試みています (科研費研究課題番号 24500260,15K00191)。 最近ではスマートフォンの画面解除に耳介認証が利用されるようになり注目されています。 http://ascii.jp/elem/000/001/003/1003803/ http://www.forbes.com/sites/amitchowdhry/2015/06/17/amazon-patents-a-system-that-unlocks-your-smartphone-with-your-ear/当研究室でもそのような研究も進めています。

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	佐賀大学総合情報基盤センター
代表者名	松前　進
所在地	〒840-8502 佐賀県佐賀市本庄町1
窓口部署名／電話番号	0952-28-8592
ホームページのＵＲＬ	http://www.cc.saga-u.ac.jp
製品説明のＵＲＬ	www.cc.saga-u.ac.jp/opengate/
対象技術	技術の概要・特徴など
製品名： Opengate,OpengateM 開発元： 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MAC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。

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	佐賀大学総合情報基盤センター
代表者名	松前　進
所在地	〒840-8502 佐賀県佐賀市本庄町1
窓口部署名／電話番号	0952-28-8592
関連部門名	総合情報基盤センター、工学系研究科知能情報システム学専攻
ホームページのＵＲＬ	http://www.cc.saga-u.ac.jp
研究説明のＵＲＬ	www.cc.saga-u.ac.jp/opengate/
対象技術	研究開発状況
研究開発名称： Opengate,OpengateMの改良 研究開発国： 日本 研究開発期間：	実用化を行っているOpengateおよびOpengateMの改良・機能追加を目指す研究である。

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	静岡大学情報学部
代表者名	酒井三四郎（学部長）
所在地	〒432-8011 浜松市中区情報3-5-1
窓口部署名／電話番号	総務係／053-478-1501
関連部門名	静岡大学情報学部情報科学科西垣研究室
ホームページのＵＲＬ	http://www.inf.shizuoka.ac.jp/
研究説明のＵＲＬ	http://minamigaki.cs.inf.shizuoka.ac.jp/work/2015/HCII2015Fujita.pdf
対象技術	研究開発状況
研究開発名称： CAPTCHA 研究開発国： 日本 研究開発期間： 2009年1月1日～	WEBサービス提供サイトに対し、自動プログラム（マルウェア）を使って、大量に不正なサービス利用要求を行う攻撃が日常的に発生している。このため、人間と機械を識別するチューリングテスト（CAPTCHA）の有用性が益々高まっている。 現在、文字画像判読型のCAPTCHAが広く利用されているが、OCR（自動文字読取装置）や機械学習の機能を備えたマルウェアによって突破されてしまっている。このため、人間のより高度な認知能力をCAPTCHAに適用することで、正規ユーザ（人間）に対してはCAPTCHAの解答容易性を確保しつつ（要件1）、不正者（マルウェア）に対するCAPTCHAの攻撃耐性の向上が求められている（要件2）。 また、CAPTCHAには、問題の自動生成に関する要求も存在する（要件3）。そもそもCAPTCHAは、機械（マルウェア）には理解できない問題をその題材として用いるわけであるので、機械（CAPTCHAシステム）がそれを認識して適切な問題を自動生成することは根本的に不可能なタスクである。 このため、当研究室では、上記の要件1～3を満たすCAPTCHA技術の研究開発に多方面からトライしている。

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	静岡大学情報学部
代表者名	酒井三四郎（学部長）
所在地	〒432-8011 浜松市中区情報3-5-1
窓口部署名／電話番号	総務係／053-478-1501
関連部門名	静岡大学情報学部情報科学科西垣研究室
ホームページのＵＲＬ	http://www.inf.shizuoka.ac.jp/
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： マイクロ生体認証 研究開発国： 日本 研究開発期間： 2013年4月1日～	生体情報は基本的に生涯不変である性質を持つため、漏洩した場合のリスクは非常に大きいものとなる。このため、使用する生体部位を比較的短期間で変更するショートターム型の生体認証が強く望まれる。また、その際、偽装生体の作成が難しく、かつ、生体情報から抽出されるユーザ本人に関する個人情報が小さくなければならない。 これらの要件を満たすために、当研究室では、生体部位の微細パターンを利用したマイクロ生体認証方式に関する研究開発にトライしている。

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	芝浦工業大学工学部情報工学科
代表者名	平川豊
所在地	〒135-8548 東京都江東区豊洲3-7-5
窓口部署名／電話番号	情報ネットワーク研究室／03-5859-8509
関連部門名	情報セキュリティ
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： 覗き見に耐性を持つパスワード認証方式 研究開発国： 日本 研究開発期間： 2015年6月27日～ 2016年3月31日	既存の覗き見耐性を持つパスワード認証方式の耐性向上をめざして研究開発に着手

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	信州大学工学部
代表者名	学部長　半田志郎
所在地	〒380-8553 長野市若里4-17-1
窓口部署名／電話番号	総務グループ（庶務）　米山　綾／026-269-5005
関連部門名	マルウェア解析
ホームページのＵＲＬ	http://www.shinshu-u.ac.jp/faculty/engineering/
研究説明のＵＲＬ	http://id.nii.ac.jp/1001/00122964/
対象技術	研究開発状況
研究開発名称： 文書型マルウェアに対するエントロピーとエミュレーションを用いたシェルコード特定方法 研究開発国： 日本 研究開発期間： 3年	アプリケーションの脆弱性を攻撃する文書型マルウェアを動的に解析するためには、該当する脆弱性をもつアプリケーションを準備する必要がある。しかし脆弱性の種類を特定することは困難な場合があり、またアプリケーションが入手できない可能性もある。一方、脆弱性を攻撃した後に動作する不正なプログラム(シェルコード)は脆弱性やアプリケーションに関係なく独立して動作することが多い。そこで本研究では脆弱性の種類を特定することなく、またアプリケーションが無くても文書型マルウェアの動的解析が行えるようにするために、文書型マルウェアに含まれるシェルコードを特定して実行する方法を提案する。提案手法では文書ファイルのエントロピーから算出したシェルコードの候補の優先順位に基づいて、文書ファイル内のバイト列をエミュレータで実行し、シェルコードの特徴を観測することで特定を行う。我々が作成したシステムに 88 種類の文書型マルウェアを投入した結果、74 種類でシェルコードを特定できた。また 74 種類のシェルコードを動的解析したところ、51 種類でマルウェアとしての動作を確認できた。

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	吉岡大三郎
所在地	〒860-0082 熊本県熊本市西区池田４－２２－１
窓口部署名／電話番号	
関連部門名	崇城大学情報学部
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： 研究開発国： 日本 研究開発期間： 2012年～	軽量カオス暗号の設計に取り組んでいる

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	千葉工業大学　工学部　電気電子情報工学科　菅原研究室
代表者名	菅原 真司
所在地	〒275-0016 千葉県習志野市津田沼２－１７－１
窓口部署名／電話番号	047-478-0393
関連部門名	
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： クラウドコンピューティングを用いたディジタルコンテンツの効率的共有 研究開発国： 日本 研究開発期間： 2010年4月～	アルゴリズムの考案と、その効率に関する計算機シミュレーションを用いた検証を行っている段階。 アクセス制御を行う側面は確かにあるが、研究の方向として、必ずしもコンピュータやネットワークに対する所謂セキュリティに重点を置いた研究ではありません。

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	東海大学 情報通信学部
代表者名	
所在地	〒108-8619 東京都港区高輪2-3-23
窓口部署名／電話番号	03-3441-1171
関連部門名	東海大学 情報通信学部 通信ネットワーク工学科
ホームページのＵＲＬ	http://www.u-tokai.ac.jp/academics/undergraduate/information_and_telecommu/
研究説明のＵＲＬ	http://www.ieice.org/ken/paper/20150303ZBxM/
対象技術	研究開発状況
研究開発名称： フローネットワークにおけるフロースクリーニング制御方式 研究開発国： 日本 研究開発期間： 2013年9月1日～ 2016年3月31日	企業カスタマへの不正侵入防止技術としてIPSが注目されている。しかし、各企業カスタマに専用IPSを割り当てるとコストが増加し、全ての企業カスタマ間に共用IPSを割り当てると各企業カスタマあたりの通信スループットが低下する。このため、IPS経由の経路で転送されるフローの安全性を検査し、安全なフローについては、IPSを経由しないカットスルー経路へオフロードさせる方式を提案している。これにより、セキュリティと経済性の両立を目指す。

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	東海大学 情報通信学部
代表者名	
所在地	〒108-8619 東京都港区高輪2-3-23
窓口部署名／電話番号	03-3441-1171
関連部門名	東海大学 情報通信学部 通信ネットワーク工学科
ホームページのＵＲＬ	http://www.u-tokai.ac.jp/academics/undergraduate/information_and_telecommu/
研究説明のＵＲＬ	http://www.ieice.org/ken/paper/20150303EBxR/
対象技術	研究開発状況
研究開発名称： 情報漏洩防止のための高速ログトレース方式 研究開発国： 日本 研究開発期間： 2013年9月1日～ 2016年3月31日	企業情報ネットワークで、機密ファイルをゲートウェイ経由で漏洩させる標的型攻撃が多発している。従来の対策では、ファイルがゲートウェイを通過する時に、複数サーバのログを逐次的にトレースし、長い時間をかけて、該当ファイルが機密ファイルかどうかを判定していた。そこで、予めブラックリストを作成し、機密判定を短時間で行う方式を提案している。これにより、リアルタイム的に利用される通信アプリケーションでも、セキュリティを強化することを目指す。

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	

企業・大学名	東京理科大学
代表者名	理事長　中根滋
所在地	〒125-8585 東京都葛飾区新宿６－３－１
窓口部署名／電話番号	
関連部門名	
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： 共通鍵暗号アルゴリズムの安全性の理論的・実験的解析評価 研究開発国： 研究開発期間：	これまでに共通鍵暗号アルゴリズムであるMISTY, CLEFIA, PRESENT, HIGHT, SNOW 3G, LED, HyRAL, Enocoro, MUGI, Trivium, PRINCE等の安全性を理論的・実験的解析により、定量的に評価してきました。その成果は学会発表により公開してきました。

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	東北学院大学
代表者名	学長　松本　宣郎
所在地	〒980-8511 宮城県仙台市青葉区土樋1-3-1
窓口部署名／電話番号	学長室事務課／022-264-6424
関連部門名	東北学院大学教養学部情報科学科　武田研究室
ホームページのＵＲＬ	http://www.tohoku-gakuin.ac.jp/
研究説明のＵＲＬ	takeda.cs.tohoku-gakuin.ac.jp/ja/research/paper
対象技術	研究開発状況
研究開発名称： 分散環境における P2P認証技術 研究開発国： 日本 研究開発期間： 平成19年3月1日～	平成19年度の委託研究「ダイナミックネットワーク技術に関する研究開発　課題キ　オーバーレイネットワークのセキュリティに関する技術」より、分散環境において認証システムを提供する技術である「セキュアオーバーレイネットワーク」の研究開発を行っている。委託研究は平成22年度に終了しているが、その後の当該技術の研究開発も継続して行っている。現在は、P2Pネットワークの運用技術の研究開発に注力しており、認証技術の開発に関する特別な進捗はない。運用技術の研究開発の終了後に、P2Pネットワークを対象として認証技術の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	日本文理大学
代表者名	平居　孝之
所在地	〒870-0397 大分県大分市一木１７２７
窓口部署名／電話番号	大学総務／097-592-1600
関連部門名	情報メディア学科
ホームページのＵＲＬ	www.nbu.ac.jp
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： 話者識別技術 研究開発国： 日本 研究開発期間： 2000年4月1日～	基礎理論の検証が完了し、試作システムでの有用性が確認された状況。経年変化および適用範囲の検証を実施している状況。

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	日本文理大学
代表者名	平居　孝之
所在地	〒870-0397 大分県大分市一木１７２７
窓口部署名／電話番号	大学総務／097-592-1600
関連部門名	情報メディア学科
ホームページのＵＲＬ	www.nbu.ac.jp
研究説明のＵＲＬ	
対象技術	研究開発状況
研究開発名称： 生体情報の符号化技術 研究開発国： 日本 研究開発期間： 2005年4月1日～	生体情報のうち、音声、歩き方等のモーション、生活パターン、骨格、について符号化に成功し、統合した本人基本情報化に取り掛かっている。現在、顔画像の高度情報化および顔凹凸等の立体情報の符号化に取り掛かっている。

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	八戸工業大学
代表者名	学長　藤田　成隆
所在地	〒031-8501 青森県八戸市妙字大開88-1
窓口部署名／電話番号	事務部　学事課／0178-25-8111
関連部門名	情報セキュリティ
ホームページのＵＲＬ	http:www.hi-tech.ac.jp/
研究説明のＵＲＬ	http://www.hi-tech.ac.jp/profile/database.cgi?cmd=dp&num=18
対象技術	研究開発状況
研究開発名称： 情報オブザーバーを用いた状態推定に基づくカオス同期系構築 研究開発国： 研究開発期間： 平成27年4月1日～ 平成28年3月31日	カオス同期系を用いた秘匿通信が提案されている。送信側・受信側の二つのサブ系において、暗号鍵の生成を担う両側の同期部は、情報セキュリティ上、送受信される同期化信号自体可能な限り次元数の小さいものを担う方が理想的である。しかし、実際は全ての同期部内部状態ベクトルを、ごく短期間ではあるが、同期部間の通信路に送信する。一方、状態オブザーバ（状態観測器）を用いたシステムの入出力測定から、内部状態を推定できる。オブザーバを用いて同期信号（低次元）から同期部（高次元）を再構築できる様に、先ずオブザーバを用いたカオス制御を研究した。現在はカオス同期部の状態推定および非線形状態フィードバック同期化制御則を研究している。

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ITソリューションズ株式会社
代表者名	内田　憲宏
所在地	〒140-8526 東京都品川区東品川2-4-11
窓口部署名／電話番号	セキュリティ商品企画課／03-6701-3437
ホームページのＵＲＬ	http://canon-its.jp/
製品説明のＵＲＬ	http://canon-its.jp/product/eset/index.html
対象技術	技術の概要・特徴など
製品名： ESET SMART SECURITY 開発元： ESET 開発国： スロバキア共和国 価格： ESETパーソナルセキュリティ 1年版新規購入ダウンロード版 3,200円（税抜き）～ 発売時期： 2003年 出荷数： 法人22万8千社、 1271万ライセンス 個人445万ユーザー （2015.3.31現在）	ESET（イーセット）セキュリティソフトウェアシリーズは、「高いウイルス検出率」と「軽快な動作」を両立。マルチデバイスに対応し、高度化・悪質化するマルウェアの脅威からあなたのインターネット生活を守ります。

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ITソリューションズ株式会社
代表者名	内田　憲宏
所在地	〒140-8526 東京都品川区東品川2-4-11
窓口部署名／電話番号	セキュリティ商品企画課／03-6701-3437
ホームページのＵＲＬ	http://canon-its.jp/
製品説明のＵＲＬ	http://canon-its.jp/guardian/
対象技術	技術の概要・特徴など
製品名： GUARDIANWALL／ WEBGUARDIAN 開発元： キヤノンITソリューションズ株式会社 開発国： 日本 価格： GUARDIANWALLフィルタリングモデル50ユーザ　新規価格¥261000（契約期間1年の希望小売価格（税別）） 発売時期： 1999年 出荷数： 2000社以上	GUARDIANWALL　メール誤送信対策・情報漏えい対策、アーカイブをワンシステムで実現する統合メールセキュリティソリューション。　GUARDIANWALLオプション　・強固なAES256bit方式による暗号化・タイムスタンプサービス。　GUARDIANWALL Cloud Edition　サービス事業者さまのニーズを反映した、マルチテナントやスケールアウトなどのクラウド環境に求められる機能を搭載した、メールフィルタリング・アーカイブソフト。　WEBGUARDIAN　適切なWebサイトアクセスと情報漏えい対策を同時に実現するWebセキュリティソリューション。

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ITソリューションズ株式会社
代表者名	内田　憲宏
所在地	〒140-8526 東京都品川区東品川2-4-11
窓口部署名／電話番号	セキュリティ商品企画課／03-6701-3437
ホームページのＵＲＬ	http://canon-its.jp/
製品説明のＵＲＬ	canon-its.jp/product/frt/
対象技術	技術の概要・特徴など
製品名： FortiGate 開発元： Fortinet 開発国： アメリカ合衆国 価格： オープン 発売時期： 2005年 出荷数： 30000台以上	FortiGateは、ウイルス/スパイウェア対策、スパム対策、アプリケーション可視化と制御、Webフィルタリングから無線LANコントローラーや仮想UTMまで、フルラインのセキュリティ機能とネットワーク機能をすべて1台の製品に統合しています。ハードウェア、ソフトウェア、サービスすべてをFortinet社が自社開発・提供し、操作性に優れた日本語GUIで導入も管理も容易。また、シンプルな価格体系によって導入後に利用する機能を順次増やすことができます。

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	京セラコミュニケーションシステム株式会社
代表者名	佐々木　節夫
所在地	〒612-8450 京都府京都市伏見区竹田鳥羽殿町6
窓口部署名／電話番号	075-623-0311
ホームページのＵＲＬ	http://www.kccs.co.jp
製品説明のＵＲＬ	http://www.kccs.co.jp/ict/security-tripwire/
対象技術	技術の概要・特徴など
製品名： Tripwire Enterprise 開発元： Tripwire 開発国： 米国 価格： 管理サーバライセンス：￥1,850,000、エージェントラインセンス（FS FIM）：￥178,000、いずれも税別。 発売時期： 2006年8月 出荷数：	「Tripwire」 は、企業システムのデータの整合性を常に監視し、外部のみならず、内部からの不正な操作やオペレーションミスによる変更を検知し早期復旧をサポートする、セキュリティ可視化ソリューションです。

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	京セラコミュニケーションシステム株式会社
代表者名	佐々木　節夫
所在地	〒612-8450 京都府京都市伏見区竹田鳥羽殿町6
窓口部署名／電話番号	075-623-0311
ホームページのＵＲＬ	http://www.kccs.co.jp
製品説明のＵＲＬ	http://www.kccs.co.jp/ict/security-tm_deep_security/index.html
対象技術	技術の概要・特徴など
製品名： Deep Security 開発元： Trend Micro 開発国： 価格： ¥1,067,500(Advance:最低購入5サーバでの価格) 発売時期： 2011年11月 出荷数：	Trend Micro Deep Security（Deep Security）は、サーバのセキュリティに求められる多様な機能（脆弱性対策、ファイアウォール、ファイルやレジストリなどの変更監視、セキュリティログ監視、ウイルス対策）を実装し、エージェントとバーチャルアプライアンスで、物理サーバはもちろん、仮想サーバにも適切なセキュリティ対策を施す統合型サーバセキュリティソリューションです。

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	京セラコミュニケーションシステム株式会社
代表者名	佐々木　節夫
所在地	〒612-8450 京都府京都市伏見区竹田鳥羽殿町6
窓口部署名／電話番号	075-623-0311
ホームページのＵＲＬ	http://www.kccs.co.jp
製品説明のＵＲＬ	http://www.kccs.co.jp/ict/security-network_assess/index.html http://www.kccs.co.jp/ict/security-web_application_assess/index.html http://www.kccs.co.jp/ict/security-smartphone/index.html
対象技術	技術の概要・特徴など
製品名： 脆弱性診断(セキュリティ診断) 開発元： 開発国： 価格： 発売時期： 2005年 出荷数：	ネットワーク脆弱性診断サービス、セキュアなWebアプリケーションのための脆弱性診断サービス、スマートフォンに関連するセキュリティ対策支援サービスなど、各種診断サービスを提供しております。

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	京セラコミュニケーションシステム株式会社
代表者名	佐々木　節夫
所在地	〒612-8450 京都府京都市伏見区竹田鳥羽殿町6
窓口部署名／電話番号	075-623-0311
ホームページのＵＲＬ	http://www.kccs.co.jp
製品説明のＵＲＬ	http://www.kccs.co.jp/ict/mobile-netbureau/
対象技術	技術の概要・特徴など
製品名： BizWalkers+シリーズ 開発元： 開発国： 日本 価格： 初期費用10万円から、月額費用2万1,000円から､いずれも税別。※基本サービスの場合（基本環境構築、ユーザID（30ID）まで、コンテンツ登録(3コンテンツまで）、管理者Web設定） 発売時期： 2014年5月 出荷数：	昨今、スマートフォンやタブレットなどスマートデバイスの普及が加速する中、ビジネス活用やワークスタイル変革への期待が高まっています。しかし、一方で、情報漏えいや不正アクセスなどへのセキュリティ対策はもちろんのこと、利用用途に応じた最適なモバイル環境をスピーディーに構築することが重要になっています。KCCSでは、企業のスタイルに合わせて、スマートデバイス、出張先や自宅のPCなどさまざまなデバイスから利用できる、柔軟性の高いセキュアなモバイルワークプレイスをご提供します。

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	株式会社バッファロー
代表者名	斉木　邦明
所在地	〒460-8315 愛知県名古屋市中区大須三丁目30番20号 赤門通ビル
窓口部署名／電話番号	社長室／050-5830-8865
ホームページのＵＲＬ	http://buffalo.jp/
製品説明のＵＲＬ	http://buffalo.jp/product/wireless-lan/ap/wxr_1900dhp/
対象技術	技術の概要・特徴など
製品名： エアステーション（無線LANルータ） 開発元： 株式会社バッファロー 開発国： 日本（一部製品／機能は海外より導入） 価格： ￥24300- （WXR-1900DHP、平成27年9月現在） 発売時期： 平成26年10月 出荷数： 非公表	本製品はPC、スマートフォンやタブレットなど、無線LANに対応した端末を家庭内機器に接続、あるいは有線アクセスサービスを通してインターネットへ接続するための機器（無線LANルータ）となります。無線LANルータはInternetからの攻撃、あるいは無線到達距離内の悪意のある攻撃者からの脅威にさらされており、これらから家庭内ネットワークを防御するためのさまざまな機能を搭載しております。※セキュリティに関連する機能のみ示しております①無線LAN経路を暗号化し、第三者の傍受・改善を防ぐ（AES-CCM）②無線LAN接続を行う共有鍵を端末へ安全に設定する（AOSS/WPS/QR Setup）③ネットワーク外部からの通信を判別し、意図せぬ通信を防ぐ（SPI）④配下ネットワーク端末からのマルウェアなどから本製品を保護する（CSRF/XSSプロテクション）⑤遠隔ネットワークの端末との通信を暗号化する（L2TP/IPsec）⑥端末のアクセスするサーバが危険かどうか判断し、通信を遮断する機能（コンテンツフィルタ）⑦隣接する端末同士の通信を遮断しウイルス感染等を防ぐ（プライバシーセパレータ）⑧旧式の暗号化（WEPなど）とLAN内の通信を分離しアクセスを制限する機能（WEP隔離機能）

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	