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８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
アクセス制御用ハードウェア:セキュリティバリアデバイス（SBD）

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26年12月12日から平成27年１月30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５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
株式会社ネクストジェン
バンクガード株式会社
岡本健稔（個人）

(2)　調査

警察庁が平成26年11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）

会津大学
大阪工業大学（２件）
九州工業大学（３件）
京都産業大学
神戸大学
崇城大学
東北工業大学
南山大学

八戸工業大学
弘前大学
広島大学
福井工業大学
法政大学
宮崎大学

イ　企業（３社）

株式会社インフィニテック
デジタルアーツ株式会社（２件）
日本電気株式会社（４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168校、企業1,282社の計1,450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　独立行政法人情報通信研究機構
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） 独立行政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　独立行政法人情報通信研究機構

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、製品における実装などにおける誤りに起因する脆弱性を利用して行われる。また、複数の脆弱性の利用を組み合わせて、攻撃を行うことが通常である。

一方で、ネットワーク利用者にとっては、利用するネットワークにおけるリスク（被害の可能性）を常に把握して、リスクの高いネットワーク環境の利用を避ける必要がある。そのため、ネットワーク上の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把握し､即座に利用者に提示できることが必要である。

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、当該知識ベースを元に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算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。平成 27 年度までにスマートフォンに関係するネットワーク利用リスクについての可視化と対策提示を行う仕組みを開発する。

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　042-327-5782

将来の方向性

スマートフォン、企業ネットワークを対象にしたリスク評価と対策提示から開発を行い、将来的にはインターネットにおけるリスク評価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
（(独)情報通信研究機構が実施する委託研究の委託先）

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（観測用センサ、大規模センタの開発など）
（２）DBD 攻撃分析・対策技術（静的・動的解析、リンク構造解析など）
（３）DBD 攻撃対策フレームワーク実証実験（一般ユーザの参加を想定）

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　独立行政法人　産業技術総合研究所

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）

独立行政法人産業技術総合研究所　セキュアシステム研究部門
TEL:029-861-5284
URL:http://www.risec.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　独立行政法人　産業技術総合研究所

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）

独立行政法人産業技術総合研究所　セキュアシステム研究部門
TEL:029-861-5284
URL:http://www.risec.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　独立行政法人　産業技術総合研究所

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）

独立行政法人産業技術総合研究所　セキュアシステム研究部門
TEL:029-861-5284
URL:http://www.risec.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　独立行政法人　産業技術総合研究所

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）

独立行政法人産業技術総合研究所　セキュアシステム研究部門
TEL:029-861-5284
URL:http://www.risec.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。

対象技術　侵入検知・防御技術、ぜい弱性対策技術

テーマ名　アクセス制御用ハードウェア:セキュリティバリアデバイス（SBD）

開発年度　平成２４年度～

実施主体　独立行政法人　産業技術総合研究所

背景、目的

制御システムでは、ハードウェアに余裕がなかったり、動作の保証や検証の観点から、OS の更新やパッチの適用が困難なケースがある。また、これらが可能な汎用の IT システムにおいても、複雑化した OS やアプリケーションのセキュリティホールを完全にふさぐことは困難であり、未発見の脆弱性を突くゼロデイ攻撃の頻度は増加傾向にある。セキュリティバリアデバイス(SBD)は、これら根絶しきれない脆弱性を持つソフトウェアをカバーし、SATA 等の各種 I/O ポートを中継する後付けハードウェアでセキュリティを保証することを目的としている。

研究開発状況（概要）

マザーボードとディスクの間に SATA ポートを中継するハードウェア装置 SBD を挿入することで、指定したファイル（現在 NTFS のみ）や領域の Read/Write アクセス制御が可能となる。マルウェアによる感染や情報漏洩の抑制効果が期待出来る。ディスク関連のキャッシュ群をもつ Windows OS などに対しても、再起動の際、書き込み禁止ファイルを復活させることで OS の動作と整合させる手法を確立した。SBD 上で行えるよう、現在プログラム移植を行っている。

詳細の入手方法（関連部署名及びその連絡先）

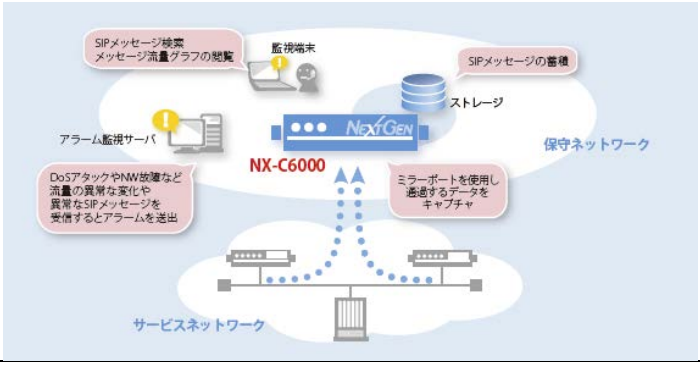
独立行政法人産業技術総合研究所　セキュアシステム研究部門
TEL:029-861-5284
URL:http://www.risec.aist.go.jp/

将来の方向性

指定したファイルを防御することに加え、SATA ポートの I/O からファイルに対するアクセスログを取得する手法を開発し、それを警告やファイル防御などセキュリティ向上に活用する予定である。また、USB など他のポートについても中継機能を開発し、多種ポートを連携させることで更にセキュリティ機能の向上を行いたい。

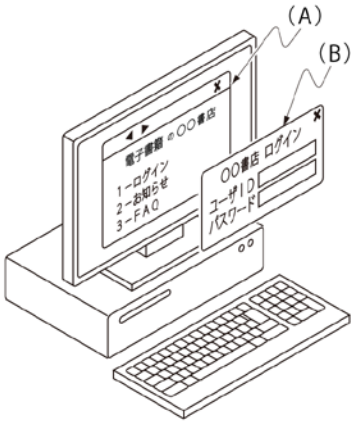
（別添２）

企業名（及び略称）：イーロックジャパン株式会社	
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/index.php	
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	１）「WebALARM」は、不正侵入、改竄等防御対策として開発されたコンテンツ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。 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。スマートフォンやタブレット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、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、低コストで利便性のよい強固なセキュリティを実現します。

企業名（及び略称）株式会社ネクストジェン	
代表者氏名　大西 新二	
所在地（郵便番号及び住所）〒108-0072 東京都港区白金1-27-6	
関連部署名及び電話番号　ネットワークセキュリティ事業本部/03-5793-3230	
ＵＲＬ　http://www.nextgen.co.jp/index.html	
対象技術	技術開発状況
侵入検知・防御技術 開発年： 平成21年度-平成26年度	近年、悪意ある第三者が企業のIP-PBX(構内交換機)や個人宅内機器に不正にアクセスして、その制御機能を奪い、なりすましによる国際電話発信によって、正規ユーザが高額な料金を請求される被害が発生しています。また、インターネット上ではSIP(Session Initiation Protocol)で使用されているポート(5060/udp)に対してのパケット流量が非常に多く観測されており(参考：（独）情報通信研究機構のnicter）、これらのほとんどは正規の通信ではなく、脆弱なシステムを見つけ出し、不正に侵入を試みるものと考えられています。 このようなVoIP(Voice over IP)、IMS(IP multimedia subsystem)に関する脅威を解決するシステムとして、株式会社ネクストジェンでは、SIP、Diameterに対応したネットワークフォレンジック技術、および侵入検知技術を提供しています。SIPメッセージのヘッダ・パラメータを詳細解析し、攻撃に使用されるツールを特定・検知する他、SIPやDiameterのメッセージ流量を監視し、IP電話システムの運用上の課題を解決するために必要な情報を提供します。また、本システムを用いてハニーポットを監視し、攻撃パケットの収集、および攻撃手法の研究に役立てております。本技術とネットワーク防御装置との連携により、健全なIP電話環境を社会に広めていくことに寄与できるものと考えます。 http://www.nextgen.co.jp/solution/voip/system/nx-c6000_nx-c6500.html（製品概要） 

企業名（及び略称）株式会社ネクストジェン	
代表者氏名　大西 新二	
所在地（郵便番号及び住所）〒108-0072 東京都港区白金1-27-6	
関連部署名及び電話番号　ネットワークセキュリティ事業本部/03-5793-3230	
ＵＲＬ　http://www.nextgen.co.jp/index.html	
対象技術	技術開発状況
ぜい弱性対策技術 開発年： 平成21年度-平成26年度	＜概要＞ 近年、VoIP(Voice over IP)分野における攻撃は種類・数共に増加傾向にあります。特にスマートフォンの普及とVoLTE（高速通信方式であるLTE 上で音声サービスを行うもの）の導入に伴って、携帯通信事業者のサービスに関連した分野での攻撃への対策が必要になってきています。 このような背景のもと、株式会社ネクストジェンではVoIPセキュリティ対策技術を提供できる国内唯一の存在として、VoIP脆弱性対策技術の研究開発を実施しております。 本対策技術では、SIP(Session Initiation Protocol)やIMS(IP multimedia subsystem) を使用したVoIPシステムやVoLTEシステムに対し、脆弱性の洗い出しとリスク分析を実施し、対象システムの信頼性、および品質向上に貢献します。 ＜特徴＞ 実利用環境に即した疑似攻撃を通信キャリアや企業のVoIPシステム、VoLTEシステムに対して実施し、盗聴、発信者番号詐称などのセキュリティリスクや、DoS攻撃などによるサービス停止に繋がる脆弱性を洗い出します。脆弱性検出作業は自動診断ツールを開発することにより、問題検出の高度化、およびスピードアップを図っております。また、診断結果のリスク評価をCVSS(Common Vulnerability Scoring System)を用いて可視化し、運用におけるセキュリティポリシー策定をサポートします。 http://www.nextgen.co.jp/solution/voip/service/sipvoip_1.html

企業名（及び略称）バンクガード株式会社	
代表者氏名　藤井健治	
所在地（郵便番号及び住所）　東京都武蔵野市吉祥寺本町2-15-15	
関連部署名及び電話番号　050-5532-3771	
ＵＲＬ www.bkguard.com	
対象技術	技術開発状況
高度認証技術 その他アクセス制御機能に関する技術 開発年: 平成25年度～ 平成26年度	【製品名称】スーパー乱数表 【概要】キャッシュカードの裏などに印字できる乱数表で、中間者攻撃（MITM/MITB）、乗っ取り、フィッシング攻撃等を防御 【従来の課題】従来技術は①一部の利用者しか防御できない（ハード、OSが限定される、②一部の攻撃しか防御できない(中間者攻撃等)、③高価(トークンの製造費・電池切れ対応費等）、④利便性の低さ等の課題があった 【利用方法】ネットバンクで送金先指定時、送金先口座番号の下2桁を乱数表を用いて指定する。画面に「送金先の最後の桁の数字に該当する画像を、E列から選択してください」と表示し、その下にE列の画像がランダムな順番で表示する。利用者なら正しい画像をクリックし送金を実行できるが、マルウェア/ハッカーは乱数表を保有していないので、ハッカーの口座番号に該当する画像を指定できず不正送金を阻止できる。また不正ポップアップ画面等で全乱数入力が求められても、利用者は画像なので騙されて入力できない 【現状】在京銀行でトライアル決定（平成27年1月30日現在） 【応用】住民基本台帳ICカードは読取装置が必要なため普及しなかった。スーパー乱数表を住基カードの裏面に印字し、通常の乱数表の様に本人認証に利用すれば、上記課題を解決。その他、学生証の裏に印字し遠隔授業に、社員証の裏に印字し在宅勤務に、保険証の裏に印字しクラウドカルテや電子お薬手帳に、企業ポイントカードの裏に印字し不正アクセス防止可能。 

企業名（及び略称）	
代表者氏名　岡本　健稔　（個人）	
所在地（郵便番号及び住所）〒713-8102 岡山県倉敷市玉島1187番地 メゾングレース102	
関連部署名及び電話番号　086-525-3720	
ＵＲＬ	
対象技術	技術開発状況
高度認証技術 開発年： 平成24年	【課題】 いわゆる「偽画面」を使った攻撃を防止します。具体的には、ネットワークから受信したメールやＷｅｂページなどの表示オブジェクトに行われた電子署名の検証結果の偽装を防止します。 【背景】 ソフトウェアのアップデートを促す偽のポップアップ、パスワード入力を求めるネットバンキングの偽画面、関係者であるかのように装ったメールで機密情報を窃取する標的型メールなど、偽の表示オブジェクトを使った攻撃が氾濫しています。このような偽物と真正な表示オブジェクトとを容易に判別できる仕組みが求められています。 【概要】 この技術を実施したイメージの図を下に記載しました。この図はパーソナルコンピュータを使って電子書籍を扱うＷｅｂサイトにログインする様子を示しています。図の（Ａ）は「電子書籍の〇〇書店」のメニュー画面です。利用者は、ログインするための項目を選択します。すると（Ｂ）のログインのためのダイアログボックスが表示されます。このダイアログボックスには真正であることを示す電子署名が行われています。そして、その電子署名の検証が成功したので、このダイアログボックスは利用者から見て手前に飛び出した位置に表示されます。利用者は手前に飛び出した位置に表示された表示オブジェクトを信頼することができます。  【詳細】 手前に飛び出した位置に表示オブジェクトを表示する仕組みなどの詳細な情報は、特許電子図書館(URL:http://www.ipdl.inpit.go.jp/homepg.ipdl)にて特許第4910076号又は特許公開2012-109960の公報をご参照ください。 【実施について】 実施可能な企業様に１回の契約で完全な権利譲渡の用意があります。

（別添３）

ア　大学

企業・大学名	公立大学法人会津大学
代表者名	理事長　岡　隆一
所在地	福島県会津若松市一箕町鶴賀上居合90
関連部署／電話番号	企画連携課／(0242)37-2511
関連部門名	
ホームページのURL	http://www.u-aizu.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： セキュリティマネジメント支援 研究開発国： 日本 研究開発期間： 平成16年5月～	基本部分については開発が完了している。今後はISO/IECの標準の変化や、認証に関する動向の変化に対応できる仕組みの検討と、システムの運用方法の検討を行う予定である。

不正アクセスからの防御対策	
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	大阪工業大学
代表者名	学長　井上　正崇
所在地	大阪府大阪市旭区大宮5丁目16番1号
関連部署／電話番号	企画課／(06)6954-4097
関連部門名	情報科学部情報ネットワーク学科
ホームページのURL	http://www.oit.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 属性証明書に基づくアクセス制御方式 研究開発国： 日本 研究開発期間： 平成19年4月1日～ 平成28年3月31日	アクセス権限は個人に対し付与するものではなく、個人の所属や肩書などの属性に対し付与すべきであるとの考えに基づき、利用者登録を必要とせず、利用者属性に基づきアクセス条件を規定し、利用者が提示した属性に基づきサービス使用可否を判断する方式、およびそれに基づくシステムの研究試作を実施している。 利用者の属性を証明する手段として、ITU-T/ISO標準のX.509属性証明書を使用する。属性証明書の所有者であることの証明は、X.509属性証明書と対応付けされるX.509公開鍵証明書により行う。これらより、全体のシステムは、公開鍵証明書を発行する電子認証局（CA）、属性証明書を発行する電子認証局（AA）、サービスを提供するアクセス制御システムから構成される。CAやAAを試作すると共に、アクセス制御の例として、電子的な学生証や職員証に基づき大学Webページの閲覧可否を判断するシステム、および属性証明書の所有者確認をネットショップサーバとは独立させ、別組織で発行された電子的な社員証に基づきネットショップ匿名優待サービスを行うシステムを試作している。

不正アクセスからの防御対策	
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	大阪工業大学
代表者名	学長　井上　正崇
所在地	大阪府大阪市旭区大宮5丁目16番1号
関連部署／電話番号	企画課／(06)6954-4097
関連部門名	情報科学部情報ネットワーク学科
ホームページのURL	http://www.oit.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： Webサーバセキュリティ 研究開発国： 日本 研究開発期間： 平成22年4月1日～ 平成28年3月31日	Webサーバセキュリティとして、SQLインジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリに対する対策を研究試作している。 SQLインジェクションに関しては、SQL文で特別の意味を持つ特殊文字を検出し、その効果をなくすように行う文字の置換処理（サニタイジング）とSQL文のひな型の解析処理を事前に済ませておき、ひな型の変動箇所に、実際の値を割り当て実行する機能（バインド機構）の2手段を試作している。クロスサイトスクリプティングに関しては、スクリプトにおける特別な意味を持つ文字を別の文字に置き換えるエスケープ処理を試作しており、クロスサイトリクエストフォージェリに関しては、乱数をクライアントに送信するトークンとして使用し、トークンの確認により正常な利用者からの送信か否かを判断する方式を試作している。 今後もWebサーバに対するその他の攻撃に対する対策を研究していく予定である。

不正アクセスからの防御対策	
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	九州工業大学 ネットワークデザイン研究センター
代表者名	
所在地	
関連部署／電話番号	
関連部門名	
ホームページのURL	http://www.ndrc.kyutech.ac.jp
研究説明のURL	http://www.ndrc.kyutech.ac.jp
対象技術	研究開発状況
研究開発名称： ネットワークセキュリティに関する研究開発 研究開発国： 日本 研究開発期間： 平成22年4月1日～	外部ネットワークからの攻撃の早期検出を可能にする技術および，異常検出後の対処方法について研究開発を実施しており，現在は，実ネットワーク環境におけるデータの取得および取得したデータの分析を進めている。

不正アクセスからの防御対策	
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	九州工業大学
代表者名	松永守央
所在地	福岡県飯塚市川津680-4
関連部署／電話番号	大学院　情報工学研究院/0948-29-7654
関連部門名	大学院　情報工学研究院
ホームページのURL	http://www.kyutech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 擬似乱数生成器に関する研究 研究開発国： 日本 研究開発期間： 平成18年～	暗号器を用いた一般的な構成とは異なる擬似乱数生成器の開発を目指している。カオス的に振る舞うロジスティック写像に着目し、計算器上に実装された写像の性質を調査している。擬似乱数生成器に求められるいくつかの設計上の指針を明らかにした。

不正アクセスからの防御対策	
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	九州工業大学
代表者名	松永守央
所在地	福岡県飯塚市川津680-4
関連部署／電話番号	大学院　情報工学研究院/0948-29-7654
関連部門名	大学院　情報工学研究院
ホームページのURL	http://www.kyutech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： クラウドストレージに適した暗号技術 研究開発国： 日本 研究開発期間： 平成26年11月～	アイディアの着想段階。状況設定と初歩的なプロトコルの考案が終了したところ。

不正アクセスからの防御対策	
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	京都産業大学
代表者名	学長　大城光正
所在地	京都府京都市北区上賀茂本山
関連部署／電話番号	コンピュータ理工学部/075-705-1531
関連部門名	コンピュータ理工学部
ホームページのURL	http://www.kyoto-su.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： Webブラウザのための簡易PKI利用機能の実装 研究開発国： 日本 研究開発期間： 平成26年4月1日～ 平成27年3月31日	WebRic技術などブラウザ間がP2Pで通信する事例が発生するなど、Webブラウザでの新たな通信形態における認証、暗号化等の要求が発生している。本研究ではWeb Cryptography APIなどの提案に伴い、検討が進められているWebアプリケーションでのPKI利用において、P2Pで用いられる簡易なPKI利用をサポートするために必要な機能拡張の調査ならびに実装を行う。成果はオープンソースとし製品化は検討していない。

不正アクセスからの防御対策	
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	神戸大学大学院　工学研究科　電気電子工学専攻　森井研究室
代表者名	森井　昌克
所在地	兵庫県神戸市灘区六甲台町1-1
関連部署／電話番号	神戸大学大学院　工学研究科／(078)803-6088
関連部門名	
ホームページのURL	http://srv.prof-morii.net/~morii/ http://bylines.news.yahoo.co.jp/moriimasakatsu/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 通信記録の分析によるウイルス感染PCの検出 研究開発国： 日本 研究開発期間： 平成24年4月1日～	HTTP通信など学内で収集している通信記録を総合的に分析してウイルス等に感染して遠隔操作される可能性があるPCなどの検出を行う。

不正アクセスからの防御対策	
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	君が淵学園　崇城大学
代表者名	吉岡　大三郎
所在地	熊本県熊本市西区池田4-22-1
関連部署／電話番号	情報学部/096-326-3111
関連部門名	崇城大学情報学部
ホームページのURL	http://www.sojo-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： 軽量カオス暗号の研究 研究開発国： 日本 研究開発期間： 平成24年4月1日～	これまで、ディジタルカオスに基づき暗号の主要部である非線形変換関数S-boxを設計した。今後、128bitのブロック暗号を設計する予定である。

不正アクセスからの防御対策	
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	東北工業大学工学部情報通信工学科松田研究室
代表者名	松田　勝敬
所在地	宮城県仙台市太白区八木山香澄町35-1
関連部署／電話番号	松田研究室／(022)305-3424
関連部門名	工学部情報通信工学科松田研究室
ホームページのURL	http://www.ice.tohtech.ac.jp/jp-ug/labs/matsuda.html
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 分散型ネットワークセキュリティ装置 研究開発国： 日本 研究開発期間： 平成22年4月1日～	基本構成要素の開発、試験を実施中。

不正アクセスからの防御対策	
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	南山大学
代表者名	学長　ミカエル・カルマノ
所在地	愛知県名古屋市昭和区山里町18
関連部署／電話番号	総務部総務課／(052)832-3112
関連部門名	理工学部
ホームページのURL	http://www.nanzan-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： IPV6における侵入検知 研究開発国： 日本 研究開発期間： 平成24年4月～	IPV6固有の侵入検知のための統計的手法を確立するために、リースIPアドレスを偽ったパケットを多数送信する疑似攻撃プログラムを開発してきた。ベイズ推定に基づく統計的分析もある程度進めてきたが、本格的な実験には至っていない。

不正アクセスからの防御対策	
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	清水　能理
所在地	青森県八戸市大字妙字大開88-1
関連部署／電話番号	工学部システム情報工学科／(0178)25-8135
関連部門名	秘匿通信
ホームページのURL	http://www.hi-tech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： カオスを用いた暗号鍵の生成 研究開発国： 日本 研究開発期間： 平成26年4月1日～ 平成29年3月31日	自然界のカオス現象（振動）から人工的なカオス発振回路（モデリング）を構築し、得られるカオス信号と情報信号から暗号文を生成します。また、カオス発振回路は暗号化鍵（ワンタイムパスワードとして）の生成にも応用します。

不正アクセスからの防御対策	
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	弘前大学総合情報処理センター
代表者名	葛西　真寿
所在地	青森県弘前市文京町3番地
関連部署／電話番号	弘前大学研究推進部社会連携課／(0172)39-3726
関連部門名	弘前大学総合情報処理センター
ホームページのURL	http://www.cc.hirosaki-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： ハードウェアベースIPSの研究 研究開発国： 日本、タイ王国 研究開発期間： 平成14年4月1日～	モバイル機器向けのIPS用のFPGAの開発を中心に行っている。

不正アクセスからの防御対策	
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	広島大学情報メディア教育研究センター
代表者名	相原　玲二
所在地	広島県東広島市鏡山1-4-2
関連部署／電話番号	ユーザサービス部門／(082)424-6252
関連部門名	広島大学情報メディア教育研究センター
ホームページのURL	http://www.media.hiroshima-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： ファイル名／ディレクトリ名を秘匿可能なクラウド向けファイル共有システム 研究開発国： 日本 研究開発期間： 平成26年4月1日～ 平成27年3月31日	属性ベース暗号を用いたシステムの試作および評価を行っている。科学研究費補助金による研究であり、未発表の内容も含まれているため詳細は記載しない。

不正アクセスからの防御対策	
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	福井工業大学情報システムセンター
代表者名	情報システムセンター長　池田　岳史
所在地	福井県福井市学園3丁目6番1号
関連部署／電話番号	情報システムセンター／(0776)29-7873
関連部門名	電子情報通信学会
ホームページのURL	http://www.fukui-ut.ac.jp
研究説明のURL	http://futredb.fukui-ut.ac.jp/html/100000242_ja.html?k=信川
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：	我々はこれまでに、カオス性をもったニューラルネットワークにおける創発現象について解析を行ってきた。特に、カオス共鳴やカオス同期などについては、通信や認証技術への応用が期待できた。例えば、カオスにおける初期値鋭微性を利用し、共通パラメーターを鍵として設定した暗号化通信や認証技術などである。今後、ニューラルネットワークでの研究成果と知見に基づき、アクセス制御機能に関する分野に参入していく予定である。

不正アクセスからの防御対策	
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	法政大学情報科学部
代表者名	理事長　田中　優子、学部長　雪田　修一
所在地	東京都小金井市梶野町3-7-2
関連部署／電話番号	小金井事務部学務課情報科学部担当／(042)387-6023
関連部門名	法政大学情報科学部
ホームページのURL	http://cis.k.hosei.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 不正防止可能秘密分散技術 研究開発国： 日本 研究開発期間： 平成18年4月1日～ 平成30年3月31日	保護対象となるデータを複数の部分情報に分けて複数のサーバで管理し、次の3つの安全性を保証する。 1.予め決められたグループのサーバが協力すると部分情報からデータが復元される 2.それ以外のグループが部分情報を持ちよってもデータに関する1ビットの情報も得られない 3.部分情報を改ざんしても高い確率で検知する 上記の性質を有する方式の開発を行い、世界最小の部分情報サイズを実現する方式を学会で発表。

不正アクセスからの防御対策	
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	宮崎大学情報基盤センター
代表者名	廿日出　勇
所在地	宮崎県宮崎市学園木花台西1丁目1番地
関連部署／電話番号	情報図書部／(0985)58-2867
関連部門名	情報基盤センター利用者支援部門
ホームページのURL	http://www.miyazaki-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： ICカード等を用いた多要素web認証 研究開発国： 日本 研究開発期間： 平成26年4月～	テストシステムを用いて実証実験を実行中

不正アクセスからの防御対策	
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	株式会社インフィニテック
代表者名	芳賀　紳
所在地	東京都品川区西五反田2-12-19　五反田NNビル3F
関連部署／電話番号	技術部／(03)5759-6810
ホームページのURL	http://www.infinitec.co.jp/
製品説明のURL	http://w3.infinitec.co.jp/modules/products/?page=category&cid=31
対象技術	技術の概要・特徴など
製品名： A-Locky.net 開発元： 株式会社インフィニテック 開発国： 日本 価格： 発売時期： 平成19年 出荷数：	A-LOCKY.netの基本機能 ●アクセス制御 ・USB認証キーが無いと、サーバの重要データ（情報金庫）にアクセスすることができません。 ・USB認証キーに権限をつけることで、利用できる重要情報を区別することができます。 ●暗号化 ・サーバ内の重要情報（情報金庫）は暗号化されていますので、万一、サーバ本体が盗難にあったとしても、サーバ内部の情報を閲覧することはできません。 ・サーバ内の暗号化された重要情報を閲覧するには、USB認証キーが必要です。 ●ログ管理 ・USB認証キーを利用している間の行動記録（ファイルの暗号化、複合化、印刷など）を取得し、サーバに一括管理します。 ・取得した記録から、必要に応じた（検索、抽出）記録を閲覧、印刷することができます。

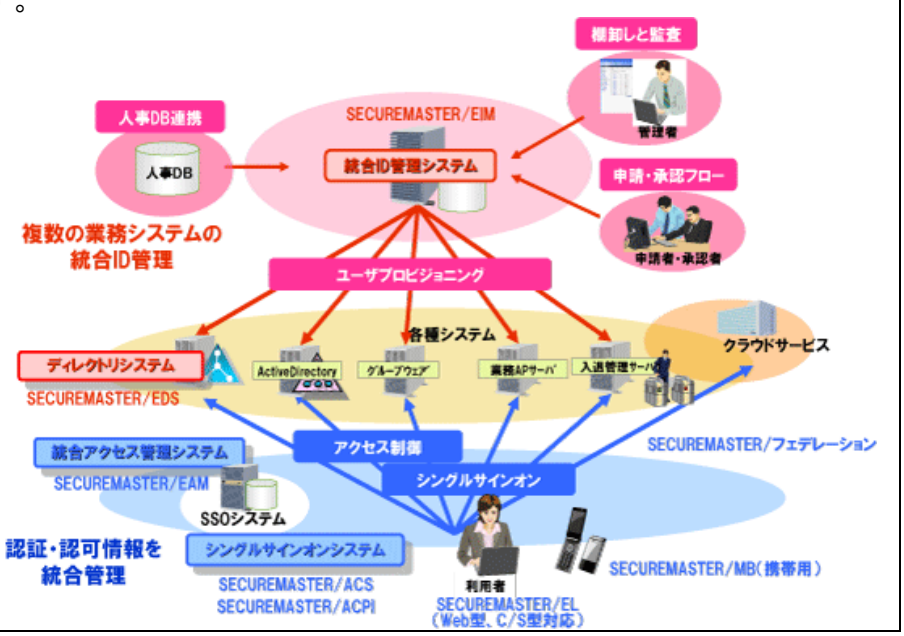
不正アクセスからの防御対策	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	デジタルアーツ株式会社
代表者名	道具　登志夫
所在地	東京都千代田区大手町1-5-1　大手町ファーストスクエア　ウエストタワー14F
関連部署／電話番号	開発部／(03)5220-1110
ホームページのURL	http://www.daj.jp/
製品説明のURL	http://www.finalcode.com/jp/
対象技術	技術の概要・特徴など
製品名： FinalCode 開発元： デジタルアーツ株式会社 開発国： 日本 価格： 10Lic 25万円から 発売時期： 平成22年6月～ 出荷数： 非公開	ファイルを自動的あるいは指定して暗号化すると共に、アクセス権をクラウドにて管理。いざとなったら、送ったファイルを後から削除することができるソリューション。 社外にファイルを送付した後も、ファイルの所在確認や、閲覧の許可・禁止、コピーや印刷の許可・禁止、閲覧期間制限、アクセス履歴のトラッキングが行える。 暗号化キーは利用者のハードウエアに紐付けられて自動的に生成され、クラウドで管理されるため、利用者はパスワードを意識することなく、通常のファイルと同様に扱うことができる。 この機能により、パスワード漏洩による情報漏洩の危険性から開放される。特に海外等の取引先に従来通りのパスワード保護したファイルを送付する際には、常にパスワード漏洩による情報漏洩がつきまとうが、そのような利用状況においても安全にファイルをやりとりできる。 また、サイバー攻撃など、マルウェアを利用した情報窃盗が行われた場合にも、明示的なパスワードが無いために、情報が漏洩することが無い。更には、ファイルの所在を確認することができるとともに、いざというときはリモートでファイルを削除することができる。

不正アクセスからの防御対策	
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	デジタルアーツ株式会社
代表者名	道具　登志夫
所在地	東京都千代田区大手町1-5-1　大手町ファーストスクエア　ウエストタワー14F
関連部署／電話番号	開発部／(03)5220-1110
関連部門名	開発部　開発５課
ホームページのURL	http://www.daj.jp/
研究説明のURL	現時点ではなし
対象技術	研究開発状況
研究開発名称： Kソリューションズ（仮称） 研究開発国： 日本 研究開発期間： 平成25年5月1日～ 平成27年年3月31日	主要な機能は研究開発が完了し、ユーザー・エクスペリエンスを高めるよう試験運用および、持続的なインテグレーションを実施中。製品化のための、マニュアル等を含む製品付属品については、今後製作予定。

不正アクセスからの防御対策	
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	日本電気株式会社
代表者名	遠藤 信博
所在地	東京都港区芝五丁目7番1号
関連部署／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/websam/securemaster
対象技術	技術の概要・特徴など
製品名： WebSAM SECUREMASTER 開発元： 日本電気株式会社 開発国： 日本 価格： ID管理　150万円～ アクセス管理・SSO 140万円～ 発売時期： 平成11年 出荷数： 約1,100システム	ID管理とアクセス管理を統合し、コスト削減と統制強化を図るとともに、情報の機密性を守ります。 ・ディレクトリから、ID管理、アクセス管理、シングルサインオン（SSO）まで、統合認証基盤構築に必要な製品を揃えたスイート製品です。共通的なインタフェースをご提供します。 ・GUIによる連携先システムの追加やアクセス制御ポリシ設定、お客さま固有の要件に対するAPIや開発言語による拡張など、種々の業務システムと柔軟に連携可能です。 ・自社製品で、国内にてソースコードを保有しているため、カスタマイズ要望、障害対応時なども迅速かつ柔軟なサポートが可能です。 

不正アクセスからの防御対策	
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	日本電気株式会社
代表者名	遠藤 信博
所在地	東京都港区芝五丁目7番1号
関連部署／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/infocage/
対象技術	技術の概要・特徴など
製品名： InfoCage 開発元： 日本電気株式会社 開発国： 日本 価格： 発売時期： 平成14年12月24日 出荷数：	・電子ファイルにセキュリティ情報を持たせ暗号化し、情報漏えいを防止。 ・ファイル/HDD暗号、媒体制御、認証によりPCの統合セキュリティを実現。 ・webアプリケーションに渡されるデータをチェック。攻撃とみなしたアクセスをブロックすることで、通常のファイアウォールやIDS/IPSでは防ぎきれないWEBアプリケーション層への攻撃を防止。 ・社内ネットワークから持ち込みPCを排除し情報漏洩やウイルス感染のリスクを低減。 ・セキュリティ対策が不十分なPCを、業務ネットワークから隔離し、ウイルス感染などの危険性を低減。 ・ネットワーク内のPCのセキュリティ対策状況を把握し、効率的にセキュリティレベルを維持。

不正アクセスからの防御対策	
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	日本電気株式会社
代表者名	遠藤 信博
所在地	東京都港区芝五丁目7番1号
関連部署／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/sg/
対象技術	技術の概要・特徴など
製品名： SG3600シリーズ 開発元： 日本電気株式会社 開発国： 日本 価格： 85万円～ 発売時期： 平成15年7月 出荷数： 約1000台	概要：NEC独自エンジンを搭載したファイアウォール製品 特徴：・VPN機能（IPSec、SSL-VPN、IPSec）の標準搭載により公衆のネットワーク上でも改ざんや盗聴から守られたセキュアな通信を実現。 ・メール、DNS、プロキシ、NTP、DHCPといった各種サーバ機能を標準搭載しているため、別途サーバ導入が不要。 ・動的ルーティングをサポートしており、ネットワーク構成の変更にも柔軟に対応可能。 ・冗長化機能により、万が一の場合でも待機系に自動切り替え可能。

不正アクセスからの防御対策	
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	日本電気株式会社　クラウドシステム研究所
代表者名	宮内　幸司
所在地	神奈川県川崎市中原区下沼部1753
関連部署／電話番号	044-431-7686
関連部門名	クラウドシステム研究所
ホームページのURL	http://jpn.nec.com/rd/crl/code/research/otr_jp.html
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 認証暗号 研究開発国： 日本 研究開発期間：	特徴 ・暗号化レート１（1ブロックにつき1回のブロック暗号） ・オンライン処理可能、さらに並列処理可能 ・ブロック暗号の暗号化関数のみを利用し、復号関数を必要としない ・ブロック暗号の標準的な安全性をベースとした証明可能安全性保証

不正アクセスからの防御対策	
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	○