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９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
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
漏洩に強い認証/鍵管理基盤 LR-AKE
高度電磁波解析技術によるLSIのセキュリティ対策に関する研究開発
プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究

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25年12月12日から平成26年１月14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、応募者は次のとおり３社であった。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。

アルプスシステムインテグレーション株式会社
日本アイ・ビー・エム株式会社
株式会社ニーモニックセキュリティ

(2)　調査

警察庁が平成25年12月から平成26年２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（３大学）

情報セキュリティ大学院大学
拓殖大学
広島大学

イ　企業（12社）

株式会社網屋（２件）

アルプスシステムインテグレーション株式会社（２件）
株式会社NTTデータ（２件）
西鉄情報システム株式会社
株式会社日立情報制御ソリューションズ
株式会社日立ソリューションズ
株式会社日立ソリューションズ東日本（２件）
株式会社富士通アドバンストエンジニアリング
株式会社富士通エフサス
株式会社富士通鹿児島インフォネット
三菱スペース・ソフトウェア株式会社（２件）
モジュレ株式会社

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199校、企業1,272社の計1,471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。
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います。また Apache ベースのサーバ実装、Firefox、Chromium ベースのクライアント実装を行ってきました。

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　03-5501-0900

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　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。現在、Windows7 32bit のドライバとしては完成しており、Windows XP Embedded へ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　03-5501-0900

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 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ホワイトリスト制御技術を開発している。現在、プロトタイプを済みで、今年度中にリアルタイムにトレースできる性能向上を予定している。

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　03-5501-0900

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　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～

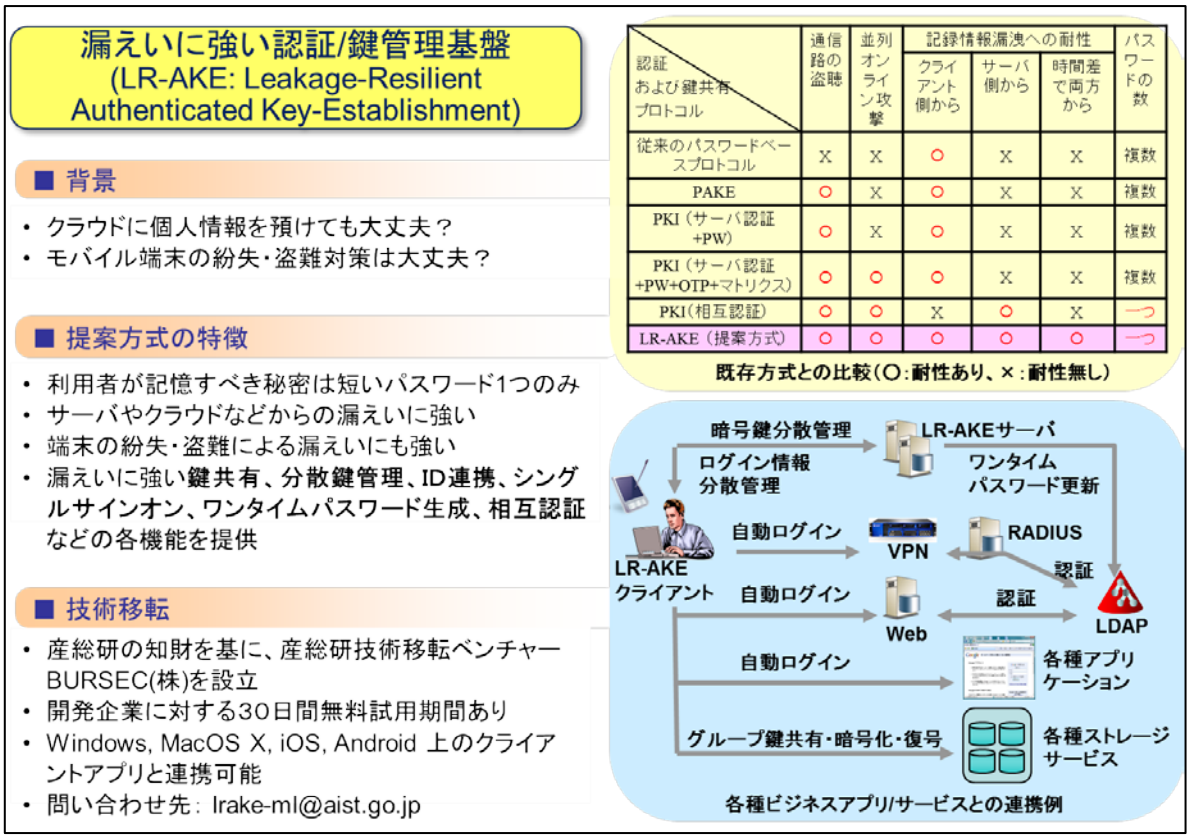
実施主体　独立行政法人　産業技術総合研究所

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、サーバー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／サーバー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が、本開発ではこの２要素認証機能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、短いパスワードを使って２要素認証へ移行する機能、ID 連携機能などの開発も行い、様々な用途に応用できるようにした。



認証および鍵共有プロトコル	通信路の盗聴	並列オンライン攻撃	記録情報漏洩への耐性			パスワードの数
			クライアント側から	サーバ側から	時間差で両方から	
従来のパスワードベースプロトコル	×	×	○	×	×	複数
PAKE	○	×	○	×	×	複数
PKI（サーバ認証+PW）	○	×	○	×	×	複数
PKI（サーバ認証+PW+OTP+マトリクス）	○	○	○	×	×	複数
PKI(相互認証)	○	○	×	○	×	一つ
LR-AKE（提案方式）	○	○	○	○	○	一つ

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　lrake-ml@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　高度電磁波解析技術によるLSIのセキュリティ対策に関する研究開発

開発年度　平成22年度～平成24年度

実施主体　東京大学（経済産業省からの委託）

背景、目的

本研究の目的は、あらゆる情報家電の安全性と信頼性の確保に対して重要となる、LSIの偽造、改ざん、情報漏えいなど、様々な脅威への対策として、高度化された電磁波計測技術を確立することにある。

このため、電磁波解析攻撃耐性評価技術の高度化、不正に挿入された回路の検出、異常動作の検出、偽造LSIの非破壊検査を通じて、LSIの放射電磁波を高精度で取得する装置及び解析手法を開発する。

研究開発状況（概要）

本研究では、高度電磁界計測・解析技術の開発・研究を進め、それを応用し、事業目的を達成するための電磁界解析システムを構築した。

具体的には、サイドチャネル攻撃を中心とする電磁波解析実験を通じて、電磁波中の情報取得に特化したマクロ磁界プローブの開発、磁界プローブをLSI上で移動しながら磁界計測を行う高精度スキャナの開発、高性能磁界プローブを実装した高精度スキャナの有効性を検証する評価実験用セキュリティ回路の開発、高精度磁界スキャナによって計測したデータを解析するツールの開発及び評価実験用セキュリティ回路による有効性の検証等を実施した。

詳細の入手方法（関連部署名及びその連絡先）

東京大学大規模集積システム設計教育研究センター
（http://www.vdec.u-tokyo.ac.jp/）
センター長　　浅田　邦博　（電話：03-5841-8901）

将来の方向性

本事業の成果の直接的な利用先は、ICカードの安全性評価である。新規の電磁波解析攻撃手法と高性能プローブを用いた局所磁解析手法は、ICカードの安全性評価において高いアドバンテージを有する日本の技術であり、海外のICカードツールベンダーとも協議を行って事業化につなげていく予定。

また、上記の実用化に向けて、開発した解析装置や技術のさらなる品質の向上、ユーザインタフェースの改良、コスト削減も重要な課題として事業終了後も引き続き検討を重ねていく予定。

対象技術　その他アクセス制御機能に関する技術

テーマ名　プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究

開発年度　平成 22 年度～平成 24 年度

実施主体　中央大学（経済産業省からの委託）

背景、目的

情報セキュリティに深く関わる価値観としては、自由、安心・安全、プライバシー保護の三者が重要であるが、この三者は、互いに矛盾・相克する場合が多い。管理経営、倫理、法制度、技術、即ち Management, Ethics, Law and Technology（MELT）を密結合・強連結させ、融合（MELT）させて、自由、安心・安全、プライバシー保護という相克しがちな三者の関係を止揚することが要請されている。

本研究開発は、クラウドに個人情報や機密情報が暗号化されて保管・預託される環境が増える中で、効率性、安全性の面から、暗号化した状態のままで、加算・乗算を含む統計処理や、サーバー管理者に知られることなく個人情報や機密情報の検索を行いたいという要請に応える。

研究開発状況（概要）

「個人情報を秘匿化したまま収集、処理、活用する医療・介護連携ネットワーク」を実現するため、個人情報の保護技術と個人情報の活用技術として、プライバシーを保護した個人情報の統計処理方式の研究開発、匿名アンケート方式の研究開発、プライベート情報検索方式の研究開発、次世代暗号による情報アクセス権限制御方式の研究開発を実施した。

具体的には、医療機関が保管する医療や介護における患者の記録などの機微な個人情報について、秘匿性を保ったまま、有効活用するために、必要なプライバシー保護方式及び情報処理方式等の開発、オンラインで患者等から医療、介護等の機微な情報に関するアンケートを行う際に、回答者の匿名性を担保し、アンケート回答に対する心理的な障壁を低減するとともに、有効な統計情報を抽出して活用するために必要な暗号方式の開発及び性能評価を実施した。また、医療・介護に関する情報について、患者や患者の家族が、関連する情報を検索する際に、当該検索者の個人情報及びその検索内容について秘匿したまま、必要な情報を取得できるシステムを構築するために必要な暗号方式、暗号プロトコル等の研究開発を行い、暗号プロトコル全体のセキュリティと性能を評価し、全体の評価を行った。さらに、患者の個人情報を適切に保護したまま、アクセス権限を持つ者のみが当該情報を有効に活用できることを目指すため、一括して暗号化した個人の様々な医療情報について、職能権限や資格ごとに複数の復号鍵を設定でき、アクセス権限がある情報のみを選択的に復号できる次世代の暗号方式を開発した。

詳細の入手方法（関連部署名及びその連絡先）

中央大学研究開発機構（http://www.chuo-u.ac.jp/research/industry_ag/rdi/）
機構教授　辻井　重男　（電話：03- 3817-1600）

将来の方向性

乱数付加による統計処理秘密分散方式は、他の暗号化状態処理方式に比較して、数桁以上の高速性を有する実用性の高い方式であり、国際会議及び有識者からの高い評価の下に、現在、IT 企業・クラウド事業者等と実用化へ向けて検討を進めている。

また、マイナンバー制導入後の電子医療・行政の進展に向けた本成果の活用に向け、暗号の有効性に対する社会の認識・信頼感を高めるためのフォーラムを立ち上げ、活動を開始した。その中で、間隔抽出方式や組織対応暗号等、本プロジェクトで得られた成果の導入を図る予定である。

（別添２）

企業名（及び略称）	アルプスシステムインテグレーション株式会社
代表者氏名	麻地 徳男
所在地（郵便番号及び住所）	〒145-0067　東京都大田区雪谷大塚町1-7
関連部署名及び電話番号	セキュリティ営業部　TEL 03-5499-8045
ＵＲＬ	http://www.alsi.co.jp/

対象技術	技術開発状況
（注１） その他アクセス制御機能に関する技術 開発平成24年～平成25年	（注２） ■ファイルの自動暗号化・アクセス制御、プログラムからの復号化 予め設定したアプリケーションにおいて、平文ファイル（暗号化されていないファイル）を開いたり、保存した際にファイルを自動的に暗号化およびアクセス権を付与します。 アクセス権は、文書レベル（例：極秘・社外秘・一般など）とユーザ（ログインID）が所属する職位（例：役員・職制・社員・パートナーなど）により、閲覧・編集・暗号解除などの権限を設定可能です。 暗号化されたファイルは、予め設定したアプリケーションのみで閲覧/編集可能ですが、メモリー上に展開する際に復号化を行っているため、ウィルス対策プログラムやファイル検索ツールなどでも、暗号化を維持した状態でのウィルス検知やファイル内検索が可能です。

企業名（及び略称）日本アイ・ビー・エム株式会社	
代表者氏名 マーティン・イェッター	
所在地（郵便番号及び住所）103-8510　東京都中央区日本橋箱崎町19-21	
関連部署名及び電話番号 ソフトウェア事業 080-5915-5217	
ＵＲＬ http://ibm.com/security/jp	
対象技術	技術開発状況
侵入検知・防御技術	IBM Security Network Protection XGS シリーズ は、2013 年に発表され、次のような侵入防御技術を実現しています。 - プロトコル分析に基づく侵入防御 - Secure Sockets Layer（暗号化通信）の検査 - ボットネットのコマンド＆コントロール（C&C）通信の検出 -Facebook、２ちゃんねる などの著名な、SNS、Web アプリケーションの検知や各Web サイトに対するユーザー・アクション(閲覧、書き込みなど)の制御 - URL フィルタリング - インジェクション検知ロジックによる SQL インジェクションからの保護 - シェル・コード・ヒューリスティック・エンジンにより、攻撃コードからの防御 - 最大 5Gbps 通信を処理可能

企業名（及び略称）株式会社ニーモニックセキュリティ	
代表者氏名　國米　仁	
所在地（郵便番号及び住所）　大阪市住吉区南住吉4-12-32	
関連部署名及び電話番号　本社　06-6608-6765	
ＵＲＬ　http//www.mneme.co.jp	
対象技術	技術開発状況
高度認証技術 開発年 ２０１２～ ２０１３	〈既存パスワード認証システムの安全利用〉 一般に文字パスワードは、平均3組ほどしか覚えていられないとされている。これは意思の欠如や精神力の弛緩によるものではなく、認知心理学でいう「記憶の干渉」が起こるための生理的な自然現象である。 干渉は情報量が少ないほど記憶刺激の類似性が高くなり起こりやすい(混乱混同が起こりやすい）。ところが、文字と画像の間、画像と画像の間では干渉は起こりにくくなる。特に自伝的画像記憶は情報量が膨大で相互の類似性が極めて小さいため、干渉は特に起こりにくい。４桁数字は情報量が少ないが故に混同が起こりやすく最も利用者泣かせな認証データだと言える。 カード上にユーザが選んだ既知画像と囮の画像を印刷し、画像のすべてに文字列を付与した画像カードを作成すると、カード上の既知画像の視認からランダムで強固なパスワード/暗証番号を抽出でき、既存の文字パスワード/暗証番号認証システムを安全に利用できるようになる。  （既知画像と囮の画像を並べ各画像に文字列を付与した「暗証画像カード」の例） 上例のように、手元のスマートフォンに内蔵されたカメラで撮影した小物類の中から利用者の懐かしい思い出が詰まった4点を古い順に見つけていくと、12組のそれぞれ異なる4桁の数字列が抽出される。上段の赤を追うとＡ銀行、右辺の緑を追うとＢカードといった具合である。勿論、１枚のカードに数字列１組のみを割り当てることも出来る。 この4桁の数字はランダムで無意味なので、カードを不正取得した第三者は0～9の数字が割り振られた20個の画像をいくら見つめても、何らかの情報を抽出するのは至難の業である。同時に不正取得される可能性のある免許証や手帳などから得られる利用者の個人情報は手掛かりにならず、語呂合わせ破りも無益な試みになる。1桁の数字の代わりに数桁の文字を使い、正解画像も囮画像もさらに増やせば極めて強固なランダム文字パスワードを抽出

	できる。 　こうしたカードのイメージは、印刷できるだけでなく携帯電話やスマートフォンに配信しておき適宜画面に表示して閲覧できる。同一のカードイメージをサービス提供事業者側で保管して利用者がアクセスできるようにしておくことも考えられる。カードの盗難に耐えられることに加えて、カードや携帯端末の紛失や災害などによる喪失にも対応できるので、可用性と利便性はさらに高まる。 　このように本技術は、既存の暗証番号／パスワード認証システムに一切の改変を加えなくても、暗証番号やパスワードの安全性を向上させる方策である。オンライン／オフラインを問わず、暗証システムやパスワード認証システムの利用者と運用事業者のすべてが受益者になる。利用者においては「脆弱な暗証番号／パスワードは使わない。メモしない。使いまわさない」の要求を容易に満たせ、運用事業者においては暗証番号／パスワードの盗用や流出から生じる事業の不安定性を大きく軽減できるようになる。 ＊以下、画像をパスワードに活用する方策についての参考資料。 日本セキュリティ・マネジメント学会（ＪＳＳＭ）　社会への提言 http://www.jssm.net/jssm/anniver25_03.pdf ＪＩＰＤＥＣ画像活用型本人認証システム・製品ユーザ向け説明ガイド http://www.jipdec.or.jp/dupc/project/ImageAuthentication/UGuide_ImageAuthentication.pdf ＪＩＰＤＥＣ画像活用型本人認証システム・製品事業者向けガイドライン検討報告書 http://www.jipdec.or.jp/dupc/project/ImageAuthentication/EGuide_ImageAuthentication.pdf 崩壊の危機に瀕する「パスワード問題」 http://it.impressbm.co.jp/e/2013/10/28/5179

（別添３）

ア　大学

企業・大学名	情報セキュリティ大学院大学情報セキュリティ研究科
代表者名	田中　英彦
所在地	神奈川県横浜市神奈川区鶴屋町2-14-1
関連部署／電話番号	情報セキュリティ大学院大学事務局/045-311-7784
関連部門名	情報セキュリティ大学院大学情報セキュリティ研究科
ホームページのURL	http://www.iisec.ac.jp
研究説明のURL	http://kaken.nii.ac.jp/d/p/24300009.ja.html
対象技術	研究開発状況
研究開発名称： 次世代情報セキュリティ基盤を実現するOS強化に向けた資源アクセス制御方式 研究開発国： 日本 研究開発期間： 平成24年4月1日～平成27年3月31日	本研究では、厳密且つ安全なアクセス制御機構を応用と基盤の協調により現し、情報システムに階層的防御網を適用する新たなOS技術を提案する。その中核は、応用の実行状況等を考慮して動的に最小のアクセス権限を与える機構の提案と、その強固な実現手段、及びこれらを実用的なものとする明快・簡便なポリシー記述・管理系の提案がその内容である。また、これをLinux上に実装し、分散トランザクション処理やクラウド環境への適用と有効性を示す。本研究の特徴は、従来OSでは粗すぎるアクセス制御により攻撃遅延・被害局所化が機能しない問題と、SELinuxに代表されるセキュアOSの細粒度アクセス制御は複雑すぎて実利用に耐えない問題の、両方を解決できることにある。研究では、厳密な階層的防御網を実現する実用的な細粒度アクセス制御機能について、まず単一システムに閉じた環境で作り上げる。中心となるテーマは、ポリシーの理解容易性・管理の簡便さ、制御対象の細粒度化で、論理言語によるポリシー記述と柔軟なポリシー管理機能により、人間にとって扱い易く強力なアクセス制御システムを実現する。次に、この方式を拡張し分散型の細粒度アクセス制御アーキテクチャを設計する。分散系への対応としては、主体や客体の状態を考慮するアクセス制御モデルを設計し、状態同定手法や、競合するアクセス権の調停等を実現する推論エンジンを検討しながら、国際標準モデルへの適合も計る。その後は、従来方式からの移行融合方式、クラウド環境への適用手法などを検討した上で、Linuxによる実験システムに実装し、各種評価と改善を行う。

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	拓殖大学工学部
代表者名	学部長　木嶋　彰
所在地	東京都八王子市館町815-1
関連部署／電話番号	学務部八王子学務課（工学部）/042-665-1447
関連部門名	工学部情報工学科
ホームページのURL	http://www.takushoku-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： モバイルアドホックネットワークにおけるワームホール攻撃検出 研究開発国： 日本 研究開発期間： 平成25年4月1日～ 平成29年3月31日	本研究では、AODVアルゴリズムをベースとした経路探索処理に位置情報を付加することで、経路の異常の検出を行う。ここで攻撃ノードによる位置情報の改竄を検出するために複数の独立した経路による情報伝達を行う。また、位置測定コスト低減のために測定ノードおよび測定頻度を減少させたときに位置情報の精度が劣化することを考慮して攻撃検出率について検討している。ワームホール攻撃の検出率についての確率的な評価については、全ノードがそれぞれ時間間隔をおいて位置測定を行うという状況について、ワームホールを介して通信を行ったノードが最後に位置測定を行った地点の確率分布を求め、さらにノード間の距離の分布と通信可能距離の関係から検出率を求めることができている。一方、シミュレーションによる評価については、これまでに開発したステルス型のワームホール攻撃のシミュレーション環境上に検出手法をインプリメントし動作確認および検出率の評価を行っている段階である。

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	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	
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25年4月1日～ 平成26年3月31日	属性ベース暗号を用いたシステムの試作及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、未発表が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	○

イ　企業

企業・大学名	株式会社網屋
代表者名	伊藤 整一
所在地	東京都中央区新川1-10-14
関連部署／電話番号	事業推進本部/03-3552-1331
関連部門名	amigram事業部
ホームページのURL	http://www.amiya.co.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： amigram 研究開発国： 日本 研究開発期間： 平成21年6月1日～	・基本機能を弊社Veronaサービスとして提供中 ・認証機構（証明書発行・管理含む）実装済み ・デバイス管理機構実装済み ・暗号化については他方式を検討 ・プロトコル開発中

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	株式会社網屋
代表者名	伊藤 整一
所在地	東京都中央区新川1-10-14
関連部署／電話番号	事業推進本部/03-3552-1331
ホームページのURL	http://www.amiya.co.jp/
製品説明のURL	http://www.amiya.co.jp/solutions/verona
対象技術	技術の概要・特徴など
製品名： Verona （ヴェローナ） 開発元： 株式会社網屋 開発国： 日本 価格： ルータ1台2万円／月～ （レンタルサービス） 発売時期： 平成22年11月1日～ 出荷数： 2,000台	＜概要＞ ・インターネットを利用し、安心安全なビジネスネットワークを提供する。これまで構築が難しく、コスト高になっていたVPNを、フルマネージドサービスとして提供する。 ＜特徴＞ ・３者認証機構をベースに、ルータやリモートアクセス端末接続時の安全性を確保する。 ・ルータは、インターネット上のサーバから自分自身の構成情報を取得し、自立的に動作する。 ・ファイアウォール機能として、通信ポート（TCP、UDP）を動的に開放する機能を有する。

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	アルプス システム インテグレーション株式会社
代表者名	麻地　徳男
所在地	東京都大田区雪谷大塚町1-7
関連部署／電話番号	管理部/03-5499-8181
ホームページのURL	http://www.alsi.co.jp/
製品説明のURL	http://www.alsi.co.jp/security/ilp/
対象技術	技術の概要・特徴など
製品名： InterSafe ILP 開発元： アルプス システム インテグレーション株式会社 開発国： 日本 価格： Webサイトを参照してください 発売時期： 平成22年12月～ 出荷数： 44万ライセンス	InterSafe ILPは「重要情報を保護」「外部デバイスで不正に持ち出しさせない」「持ち出し後のファイルを安全に活用する」「送信データの情報漏洩を防止」がオールインワンで可能な情報漏洩防止対策製品です。

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	アルプス システム インテグレーション株式会社
代表者名	麻地　徳男
所在地	東京都大田区雪谷大塚町1-7
関連部署／電話番号	管理部/03-5499-8181
ホームページのURL	http://www.alsi.co.jp/
製品説明のURL	http://www.alsi.co.jp/security/is/
対象技術	技術の概要・特徴など
製品名： InterSafe Webfilter 開発元： アルプス システム インテグレーション株式会社 開発国： 日本 価格： Webサイトを参照してください 発売時期： 平成12年9月～ 出荷数： 1,200万端末以上	InterSafe Webfilterは、URLデータベースに基づいてクライアントPCのWebアクセスをコントロールするゲートウェイ型のWebフィルタリングソフトです。不正サイトへのアクセスや書き込みを禁止し、情報漏洩・ウイルス感染防止や私的利用防止による業務効率向上を実現します。また、アクセスログの活用、保管により内部統制も支援します。

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	株式会社NTTデータ
代表者名	岩本　敏男
所在地	東京都江東区豊洲3-3-3豊洲センタービル
関連部署／電話番号	基盤システム事業本部セキュリティビジネス推進室/050-5546-9012
関連部門名	基盤システム事業本部セキュリティビジネス推進室
ホームページのURL	http://www.nttdata.com/
研究説明のURL	http://www.nttdata.com/jp/merm
対象技術	研究開発状況
研究開発名称： 次世代モバイル活用基盤（仮称） 研究開発国： 日本・イタリア 研究開発期間： 平成24年 ～平成26年	詳細は、「http://www.nttdata.com/jp/ja/merm/」を参照してください。 この他、 「http://itpro.nikkeibp.co.jp/article/COLUMN/20131022/512887/」に詳細な解説があります。

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	株式会社NTTデータ
代表者名	岩本　敏男
所在地	東京都江東区豊洲3-3-3豊洲センタービル
関連部署／電話番号	基盤システム事業本部セキュリティビジネス推進室/050-5546-9012
ホームページのURL	http://www.nttdata.com/
製品説明のURL	http://nws.jp.nttdata.com/vim
対象技術	技術の概要・特徴など
製品名： VANADIS Identity Manager／VANADIS SSO 開発元： 株式会社NTTデータ 開発国： 日本 価格： パッケージ単体で 50万円～ 発売時期： 平成13年4月～ 出荷数： 非公表	企業内で管理されるIDを総合的に管理し、それに基づく認証、SSO認可を提供する。

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	西鉄情報システム株式会社
代表者名	村田　秀明
所在地	福岡県福岡市博多区千代4-1-33　西鉄千代県庁口ビル
関連部署／電話番号	管理本部　技術推進グループ/092-645-2534
ホームページのURL	http://www.nishitetsu.ne.jp/nis/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Webアプリケーションぜい弱性診断サービス 開発元： McAfee, 三菱電機情報ネットワーク 開発国： 日本 価格： 9万円～ 発売時期： 平成26年2月1日頃～ 出荷数：	（概要）最新のぜい弱性データベースを用いて検査を実施し、Webアプリケーションが抱えるぜい弱性を発見・検出する。また、発見されたぜい弱性の深刻度・影響等の診断結果をご報告。診断結果に基づいて対策を行うことにより、侵入、改ざん、漏洩などのインシデント被害を未然に防ぐことが可能となる。 （特徴）最新のぜい弱性データベースに基づいて検査を実施することにより新種の攻撃やぜい弱性にいち早く対応。

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	株式会社日立情報制御ソリューションズ
代表者名	新　吉高
所在地	茨城県日立市大みか町5-1-26
関連部署／電話番号	研究開発センタ/0294-53-6624
ホームページのURL	http://www.hitachi-ics.co.jp/
製品説明のURL	http://www.hitachi-ics.co.jp/product/virsecur/scbox/scb/htm
対象技術	技術の概要・特徴など
製品名： 不正持込PC検知＆強制排除システム「S. COATBOX」 開発元： 株式会社日立情報制御ソリューションズ 開発国： 日本 価格： 225,000円／台 発売時期： 平成18年6月～ 出荷数： 約940台 （2014年1月末現在）	【概要】パソコン持ち込みが原因の企業内ネットワーク不正侵入を、既設ネットワークへの接続を通して監視。不正持込みパソコンを検出した場合は、ネットワークから排除し情報漏洩を防止。 【主な機能】 ●不正接続したPCの強制排除 ●接続PCの接続状況の管理 ●制御・管理ソフト（別売り）を利用することで複数台のS.COATBOXと連携し、広域でのネットワーク監視を一元管理することが可能 【導入効果】 ●機密情報の保全・ウイルス感染の防止 ●ネットワーク管理者の負担低減

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	株式会社日立ソリューションズ
代表者名	佐久間　嘉一郎
所在地	東京都品川区東品川4-12-7
関連部署／電話番号	広報・宣伝部/03-5479-5013
ホームページのURL	http://www.hitachi-solutions.co.jp
製品説明のURL	http://www.hitachi-solutions.co.jp/hibun/
対象技術	技術の概要・特徴など
製品名： 秘文シリーズ 開発元： 株式会社日立ソリューションズ 開発国： 日本 価格： サーバ：30万円～ クライアント（１クライアント）：1万円～ 発売時期： 平成11年12月～ 出荷数： 680万ライセンス	詳細は、上記ＵＲＬを参照してください。 （参考イメージ図） ～エンドポイントからメール、Web、スマートデバイスまで対応～ 

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	株式会社日立ソリューションズ東日本
代表者名	森　悦郎
所在地	宮城県仙台市青葉区本町二丁目16番10号
関連部署／電話番号	
関連部門名	研究開発部
ホームページのURL	http://www.hitachi-solutions-east.co.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： セキュアなクラウドサービスマッシュアップ技術 研究開発国： 日本 研究開発期間： 平成25年4月1日～ 平成27年3月31日	非公開情報となります。

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	株式会社日立ソリューションズ東日本
代表者名	森　悦郎
所在地	宮城県仙台市青葉区本町二丁目16番10号
関連部署／電話番号	
ホームページのURL	http://www.hitachi-solutions-east.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Custom Browser for Android™ 開発元： 株式会社日立ｿﾘｭｰｼｮﾝｽﾞ東日本 開発国： 日本 価格： 発売時期： 平成24年9月1日頃 ～ 出荷数： 20	Androidタブレットを対象としたセキュアブラウザ （1）認証デバイスとの連携による利用認証により、正しい利用者のみが操作可能 （2）ホワイトリスト方式によるアクセス制御で、業務サイトに限定した安全な利用が可能 （3）ファイルのダウンロード制限による、情報漏えい防止 （4）豊富なカスタマイズメニュー

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	株式会社富士通アドバンストエンジニアリング
代表者名	小原　恒明
所在地	東京都新宿区西新宿3-7-1　（新宿パークタワー）
関連部署／電話番号	03-5324-1500
ホームページのURL	http://jp.fujitsu.com/group/fae/
製品説明のURL	http://jp.fujitsu.com/group/fae/
対象技術	技術の概要・特徴など
製品名： Info Barrier （インフォ バリア） 開発元： 株式会社富士通アドバンストエンジニアリング 開発国： 日本 価格： 7,900円（税抜き）／1ライセンス～ 発売時期： 平成12年10月～ 出荷数： 約700,000ライセンス	パソコン上の「ユーザの操作を制限」することで、内部者による情報漏洩を防止及び監視する。

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	株式会社富士通エフサス
代表者名	今井　幸隆
所在地	神奈川県川崎市中原区中丸子13番地2 野村不動産武蔵小杉ビル N棟
関連部署／電話番号	
ホームページのURL	http://jp.fujitsu.com/group/fsas
製品説明のURL	http://jp.fujitsu.com/group/fsas/services/network/detection/
対象技術	技術の概要・特徴など
製品名： ウイルスふるまい検知サービス 開発元： 株式会社富士通エフサス 開発国： 日本 価格： 50万円～ 発売時期： 平成25年2月～ 出荷数： 10ユーザ程度	昨今のサイバー攻撃は巧妙化が進み、管理者が気づかないうちに情報が搾取されている事例も相次いでいます。 本サービスは、従来のパターンマッチングでは捉えられない未知の脅威が引き起こす、不正通信の”早期探知”から”対応支援”まで、一連の対応をトータルで提供するサービスです。 （特徴） ・お客様のセキュリティ要件に合わせて、日々のネットワーク監視から以上の早期検知、トラブル対処までの各種メニューを組み合わせて提供 ・ログの解析や異常の原因切り分けなど、高度なスキルを要する作業をセキュリティエキスパートが支援 ・24時間体制のセンター監視と全国規模でのオンサイト作業の対応

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	株式会社富士通鹿児島インフォネット
代表者名	髙榎　勝義
所在地	鹿児島県鹿児島市鴨池新町5-1鴨池ＡＣアネックス
関連部署／電話番号	事業推進統括部/099-250-3511
関連部門名	IDCサービス部
ホームページのURL	http://jp.fujitsu.com/kfn/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 発行センターを介したワンタイムパスワード認証システム 研究開発国： 日本 研究開発期間：	1 SCISZ014における論文発表及び技術展示 2 プロトタイプ構築及び技術検証

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	

企業・大学名	三菱スペース・ソフトウェア株式会社
代表者名	
所在地	東京都港区浜松町2丁目4番1号　世界貿易センタービル32階
関連部署／電話番号	
ホームページのURL	http://www.mss.co.jp/
製品説明のURL	http://www.mss.co.jp/businesfield/security/sumizumi/index.html
対象技術	技術の概要・特徴など
製品名： すみずみ君 開発元： 三菱スペース・ソフトウェア株式会社 開発国： 日本 価格： 発売時期： 出荷数：	・機能概要 すみずみ君は、個人情報・機密情報の管理ツールとしてクライアントPC／共有サーバ内のすみずみまで個人情報・機密情報に該当するファイルを「簡単」「高速」「高精度」に検出するツールです。ファイル名を検出するのみではなく、そのファイル内の「どこに個人情報・機密情報があるか」も簡単にチェック出来ます。 ・付属ユーティリティ 住所、電話番号、電子メールアドレス、生年月日、苗字、クレジットカード番号、銀行口座番号の7種の標準搭載辞書の他、固定文言や特定文字パターンなどの検査条件を柔軟に設定できる辞書ユーティリティ。 ＩＴ資産管理ツールなど、他のソフトと連携して情報漏洩を実現するリネーム・ユーティリティを標準搭載しています。

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	三菱スペース・ソフトウェア株式会社
代表者名	
所在地	東京都港区浜松町2丁目4番1号　世界貿易センタービル32階
関連部署／電話番号	
ホームページのURL	http://www.mss.co.jp/
製品説明のURL	http://www.mss.co.jp/businesfield/security/MSIESER/index.html
対象技術	技術の概要・特徴など
製品名： Dynamic MSIESER 開発元： 三菱スペース・ソフトウェア株式会社 開発国： 日本 価格： 発売時期： 出荷数：	「ネットワーク・フォレンジック製品」として2002年10月発売開始以来バージョンアップを重ね、情報漏洩対策システム機能として2011年には「送信ファイル検査機能」、2012年には「標的型サイバー攻撃対策用付加装置PACKENCHER」を追加。 （製品モデル） Dynamic MSIESERを構成する製品モデル体系を以下に示します。 （１）Dynamic MSIESER　360G8 ・エントリーモデル ・パケット処理性能：標準モード　20ＧＢ～40ＧＢ/日 （２）Dynamic MSIESER 380G8 ・高性能モデル ・パケット処理性能：標準モード 100GB/日、高速モード500GB/日 （３）Dynamic MSIESER 350G8 ・高性能・LTOドライブ内臓モデル （４）PACKENCHER ・標的型サイバー攻撃対策用付加装置

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	モジュレ株式会社
代表者名	代表取締役 木原　礼子
所在地	東京都港区芝5-25-11　ヒューリック三田ビル2階
関連部署／電話番号	メンバー＆オフィスサービス/03-3454-2061
ホームページのURL	http://www.modulat.com/
製品説明のURL	http://www.modulat.com/b_service/smartphone.html
対象技術	技術の概要・特徴など
製品名： パスジェネ 開発元： モジュレ株式会社 開発国： 日本 価格： ０円 （フリーソフト） 発売時期： 平成23年8月4日頃 ～ 出荷数： 不明	「パスジェネ」は、企業の情報システム部・システム管理者が定期的に変更するパスワードやテスト用のワンタイムパスワードの作成と管理を行うためのアプリです。パスワードの文字数や種類を選んで、パスワードを簡単に自動作成する事が出来ます。 パスワードを作成する場合、いかに連想されづらいパスワードを作成するかが重要です。「パスジェネ」は、英字/数字/記号を含めた複雑なパスワードを簡単に作成する事が出来ます。 【主な機能】 ・パスワードの文字を「英字」、「数字」、「記号」より選択してパスワード作成（複数選択可） ・パスワードの文字数を「4」、「6」、「8」、「10」、「12」を選択してパスワードを作成 ・作成されたパスワードの編集も可能 ・任意のパスワードを入力する事も可能（文字数を「0」にして下さい） ・簡易なＩＤ管理機能（作成したＩＤ、パスワードはサファリ等他のアプリへの連携には対応しておりません。コピーはできます。）

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	○