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取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。

実施テーマは次のとおりであり、その研究開発の概要は、別添１のとおりである。

マルウェア配布等危害サイト回避システム
ネットワークセキュリティ技術の研究開発
マルウェア対策ユーザサポートシステムの研究開発
情報家電など、非PC端末における未知脆弱性の自動検出技術に関する研究開発

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23年12月２日から12月26日までの間にアクセス制御技術に関する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そのまま掲載している。

株式会社ネクストジェン
株式会社ICTストラテジー総合研究所
株式会社富士通ソーシアルサイエンスラボラトリ
エヌ・ティ・ティ・コミュニケーションズ株式会社
日本CA株式会社
情報セキュリティ大学院大学

(2)　調査

警察庁が平成23年10月から11月にかけて実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア　大学

国立大学法人九州工業大学
東京情報大学

イ　企業

株式会社エヌ・ティ・データ
株式会社ソリトンシステムズ
ヌリテレコム株式会社
株式会社シー・エス・イー

ファインアートテクノロジー
シスメックスＲＡ株式会社
ウォッチガード・テクノロジー・ジャパン株式会社
株式会社ＣＩＪ
日本信号株式会社
日本無線株式会社
富士通株式会社

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（研究開発のうち実用化しているもののみ）をそのまま掲載している。

アンケート調査は、次の条件により抽出した1,300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」又は「金融」であるもの

(別添1)

対象技術　その他アクセス制御に関する技術
テーマ名　マルウェア配布等危害サイト回避システムの実証実験
開発年度　平成21年度～平成23年度
実施主体　エヌ・ティ・ティ・コミュニケーションズ株式会社（総務省からの委託）
背景、目的 近年、一般に広く利用される有名Webサイト改ざんによりWeb感染型マルウェアを埋め込まれることにより、多くの国民がマルウェア感染の脅威にさらされるようになった。 こうしたマルウェアへの対策として、ユーザは、セキュリティベンダから提供されるウイルス対策ソフトの導入及びアップデート、OSやアプリケーションのアップデートを行うことが有効であるが、インターネット利用ユーザの意識やスキルの不足により徹底されていないのが現状である。 社会全体としての情報セキュリティの向上を実現するためには、電気通信事業者によるネットワーク側での対策を行うことが効果的であり、マルウェアを配布するサイト等にアクセスすることによる感染を未然に防止するためのマルウェア配布等危害サイト回避システムが有効である。 本事業では、危害サイトへのユーザアクセスに対して、注意喚起を行うことにより、ユーザのマルウェア感染を未然に防ぐマルウェア配布等危害サイト回避システムの実証実験を行い、主に危害サイト評価情報データベースの構築とISPへの情報提供方法について検討する。
研究開発状況（概要） マルウェア配布等危害サイト回避システムは、危害サイト評価情報を基に、ISPの顧客である一般ユーザが危害サイトにアクセスするのを防止するものであり、危害サイト評価情報提供システム、トラヒック解析システム及び危害サイト注意喚起システムから構成される。 （１）危害サイト評価情報提供システム 正確性の高い危害サイト評価情報データベースを作成し、ISPに危害サイト評価情報を提供するシステムであり、以下のサブシステムから構成 ①　クローラシステム ②　マルウェア動的解析システム ③　サイト解析システム ④　スコアリング分析評価システム ⑤　危害サイト公開システム （２）トラヒック解析システム ISPのネットワークの一部のトラヒックをモニタリングし、シードリストを生成するシステム （３）危害サイト注意喚起システム 危害サイト評価情報提供システムから、危害サイト評価情報を受け取り、その情報を元に一般ユーザの危害サイトへのアクセス時に注意喚起を行うシステム

詳細の入手方法（関連部署名及びその連絡先）

総務省情報流通行政局情報流通振興課情報セキュリティ対策室

電話　03-5253-5749

将来の方向性

本事業を通じて、マルウェア配布等危害サイト回避システムに関する技術を確立し、実運用に向けての法律等の制度面の検討を行う。

対象技術　侵入検知技術

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。

　また，対策手法の導出に当たって，再現ネットワークの活用による検証、発信元追跡技術の研究開発を行う。さらに DoS(サービス不能)攻撃によるネットワーク障害への耐性を高めるための研究開発を行う。

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､マルウェアの収集機構･収集したマルウェ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、マルウェ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プロトタイプに反映し、実運用に向け開発を進めた。

　また、異なる機関に属する複数の観測点で収集したログから、その組織が有する情報を互いに開示することなく､共通の攻撃を解析する技術について更に高速化が可能なアルゴリズムを開発し、その有効性を検証した。本アルゴリズムを正規のユーザのプライバシーを保護しつつ発信元を追跡する技術に拡張した。攻撃ベクタの捕捉能力と解析能力の向上のため､仮想マシンモニタを用いて不正アクセス発生時点のメモリ、ディスク内容を捕捉する技術を開発し、逐次解析器による再現フローの自動化とデータ蓄積を実施した。また海外研究機関と連携し、ネットワークを流れるパケットの内容を自動分類し､パケットに含まれる攻撃ベクタを高精度で捕捉できる機械学習アルゴリズムの開発を進めた。

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企画室
042-327-5774

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　不正プログラム対策技術

テーマ名　マルウェア対策ユーザサポートシステムの研究開発

開発年度　平成21年度～平成23年度

実施主体　株式会社日立製作所、KDDI株式会社
（情報通信研究機構（NICT）が実施する委託研究の委託先）

背景、目的

本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析をnicter等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出及び自動駆除の仕組みを実現することを目的とする。

ユーザにおけるマルウェア対策として一般的なものは、セキュリティベンダ等が提供しているシグネチャ（マルウェア検査パターン）に基づくアンチウィルスソフトである。

アンチウィルスソフトでは、シグネチャを採用しているため、既知のマルウェアに対しては十分対応できるが、未知のマルウェアや、一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードに対しては、現状十分に対応できていない。

また、新しいマルウェアが現出した場合、セキュリティベンダ等が対応するパターンファイルを更新するまでに一定の時間を要するため、ユーザが必要なときに、必要なものをタイムリーに入手できるところまでには至っていない。

コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展する中で、上述のように未知のマルウェアや一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードのように、アンチウィルスソフトによる対応では十分カバーし切れない領域が存在している。

セキュリティベンダ等による取組を補完しつつ、そのような未知のマルウェアも対応できるように、検体の解析に基づくマルウェア判定をベースとした駆除ツールを、実時間に近い形でユーザに提供していくことが必要になってきている。

研究開発状況（概要）

・平成21年度より以下の研究開発を実施中である。

（１）ユーザパソコンへの負荷をかけず、ホワイトリスト化等を用いた高能率探索手法を駆使し、実行コードがマルウェアかどうかをユーザサポートセンターで解析するとともに、マルウェアを駆除するツールを自動的に提供するフレームワーク

（２）ユーザのパソコン上で検査プログラムを実行してから、ユーザに対して駆除ツールが提供されるまでの一連の手続きが10分程度で完了するシステム

（３）上記のマルウェア検出から駆除までを実環境で有効に機能させるための実証実験

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://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）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　脆弱性対策技術

テーマ名　情報家電等、非PC端末における未知脆弱性の自動検出技術に関する研究開発

開発年度　平成22年度～平成24年度

実施主体　株式会社フォティーンフォティ技術研究所（経済産業省からの委託）

背景、目的

現在、情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を実施することを目指す。

本事業では、今後のインターネットにおいて重要な役割を占めることが予想される非PC端末において、外部脅威を誘発する主要因である「セキュリティぜい弱性」を自動検出するための技術を研究開発する。本技術により、製品出荷前に未知のセキュリティぜい弱性を効率的に検出・対処するスキームを開発現場で簡単に構築する事ができる。

研究開発状況（概要）

本事業により、開発する検査ツールにおいては、予測不能なデータを入力することで、セキュリティのぜい弱性を検査するファジングの手法を用いる。具体的な開発状況については、次のとおりである。

（１）ファジングベース開発（平成22年度実施）

①ファジング定義言語開発（平成22年度実施）

セキュリティ検査ツールで用いるファジング定義言語の設計を行った。

（２）ファジング開発・実装

①基本エンジン開発（平成22年度実施）

②エンジン群　追加開発（平成23・24年度実施予定）

①および②で未知ぜい弱性を検出するファジングエンジンの開発を行った。平成24年度も追加開発を行う。

（３）ファジングルール追加実装

①ベースルール開発（平成22年度実施）

②情報家電、モバイル端末、スマートメーター専用ルール開発（平成23・24年度実施予定）

ファジングルールを開発し対応プロトコルを追加した。平成23年度も追加開発を行う。

詳細の入手方法（関連部署名及びその連絡先）

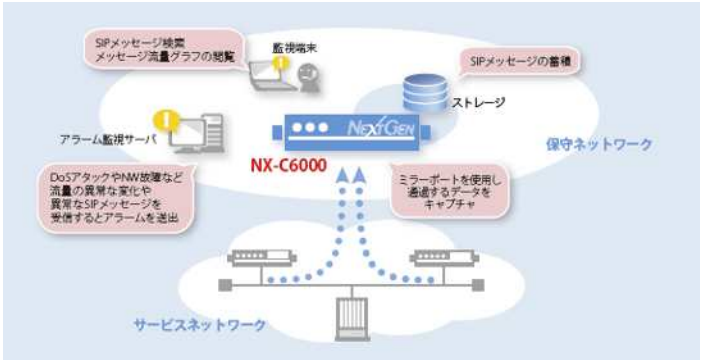
株式会社フォティーンフォティ技術研究所（http://www.fourteenforty.jp/）

鵜飼 裕司（Tel:03-6413-5177）

将来の方向性

　未知のセキュリティぜい弱性を発見する技術は世界的にも研究途上であり、主にセキュリティ研究者の一部が保持する特殊な技術となっているが、これら技術をツール化する事で、一般の開発現場で手軽にぜい弱性を発見する事が可能となる。

(別添2)

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） 東京都千代田区麹町3-3-4 KDXビル9F	
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/03-3234-6855	
ＵＲＬ http://www.nextgen.co.jp/solution/security/	
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23年度	近年、悪意ある第三者が企業のIP-PBX(構内交換機)や個人宅内機器を乗っ取り、なりすましによる国際電話発信によって、高額な料金を請求される被害が発生しています。また、警察庁サイバーフォースのインターネット定点観測においてもシグネチャを用いた不正侵入などの検知では平成22年７月９日に「VoIP(Voice over IP)」が急増し、その後減少するも平成22年12月頃よりほぼ横ばいの推移を続けています。 このようなVoIP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(Session Initiation Protocol)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、規定に準拠しているか判断する他、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集約します。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/products/security/nx-c6000.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 新ニ	
所在地（郵便番号及び住所） 東京都千代田区麹町3-3-4 KDXビル9F	
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/03-3234-6855	
ＵＲＬ http://www.nextgen.co.jp/solution/security/	
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23年度	＜概要＞ SIP(Session Initiation Protocol)を使用したVoIP(Voice over IP)システムに対し、ぜい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及び品質向上に貢献します。 ＜特徴＞ 実使用環境に即した疑似攻撃をVoIPシステムに対して実施し、盗聴、発着番号詐称などのセキュリティリスクや、DoS攻撃等によるシステムの停止に繋がるぜい弱性を洗い出します。擬似攻撃には、SIPプロトコルに特化した250万以上のメッセージを自動で生成し、容易かつ短期間にぜい弱性の問題を発見します。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。

企業名（及び略称）　株式会社ICTストラテジー総合研究所	
代表者氏名　代表取締役　久保哲男	
所在地（郵便番号及び住所）　〒100-0005　東京都千代田区丸の内1-8-3	
関連部署名及び電話番号　本社　03-4530-0565	
ＵＲＬ　http://www.is-ri.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 開発年： 平成22年度～ 平成23年度	・ネットショップやネットバンク等への初期登録や、毎回のログイン時に、予め登録してある固定電話・携帯電話から認証サーバに電話し発信者番号を通知することにより本人認証を行う技術 ・ＰＣやスマートフォンでの本人確認に対応 ・ＩＤ、パスワードを盗まれたとしても、電話端末を物理的に盗まれない限り、不正アクセスが不可能 ・ＰＣに特別なソフトを別途インストールする必要がなく、また全ての電話会社の全ての機種の電話端末で利用可能 ・ワンタイム・パスワードのようにトークンの配布・管理コスト不要 ・発信者番号は総務省令等にて、全電話会社が対策済

企業名（及び略称）：株式会社富士通ソーシアルサイエンスラボラトリ（富士通SSL）	
代表者氏名　　：花岡　和彦	
所在地（郵便番号及び住所）：211-0063　神奈川県川崎市中原区小杉町1-403 武蔵小杉タワープレイス	
関連部署名及び電話番号：セキュリティソリューション本部 ネットワークサーバセキュリティ部	
ＵＲＬ　http://www.ssl.fujitsu.com/	
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 ・不正プログラム対策技術 ・その他アクセス制御機能に関する技術 開発年：平成15年	富士通SSLが開発した「SHieldWARE」は、サーバのアクセス制御を実現するソフトウェア製品です。 汎用ＯＳでシステム管理者が利用する「特権ＩＤ」の権限を最小化できます。管理者も含めた全てのユーザに対して強制アクセス制御を実施し、情報漏えいなどのリスクを低減できます。 また、サーバ上の操作ログをＯＳコマンドレベルまで詳細に記録でき、不正侵入の履歴からサーバアクセスログまで、ＩＴ全般統制に不可欠な監査証跡を確実に収集･管理することが可能です。

企業名（及び略称）　エヌ・ティ・ティ・コミュニケーションズ株式会社	
代表者氏名　代表取締役社長　有馬　彰	
所在地（郵便番号及び住所）　〒100-8019　東京都千代田区内幸町１丁目１番６号	
関連部署名及び電話番号　先端IPアーキテクチャセンタ　050-3812-4969	
ＵＲＬ　http://www.ntt.net/service/traffic.html	
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 開発年：平成19年	1) 大規模ネットワークのトラフィックをxFLOWを使い、統括的に解析し、IPアドレス、アプリケーション別に可視化 2) トラフィックパターンシグネチャおよび通常トラフィック波形からの乖離レベルチェックによりDDoS攻撃等の異常トラフィックを検知 3) DDoS攻撃検知時に、ネットワーク機器を制御し、DDoS攻撃を効率的に軽減する技術開発

企業名（及び略称）日本CA株式会社	
代表者氏名	
所在地（郵便番号及び住所）東京都千代田区平河町2-7-9 JA共済ビル	
関連部署名及び電話番号　セキュリティ＆VSAソリューション事業部	
ＵＲＬ http://www.ca.com/jp/	
対象技術	技術開発状況
・高度認証技術	証明書技術を応用したソフトウェアトークンによる２要素認証を提供します。米国特許クリプトグラフィック・カモフラージュ技術＊1(US Patent No. 6,170,058)により、証明書で問題となるオフラインの総当たり攻撃による秘密鍵の解読を事実上不可能とする事が可能となり、従来ハードウェアで物理的に保護していた証明書をソフトウェアで安全に保護することができ、「証明書を持っている」および、秘密鍵を解くための「パスワードを知っている」の２要素認証を実現可能です。現在この技術を利用した製品を商用化済みで、さらに様々な認証形態に対応するための研究開発を進めている。 ＊1 クリプトグラフィック・カモフラージュ技術 通常の証明書におけるオフラインによる総当たり攻撃では、パスワードで保護されている証明書内の秘密鍵の特徴である「１で始まり１で終わる」（例：1E459FC479C3B41）という書式からパスワードおよび秘密鍵をクラッキングする。この技術は上記のように判読されるのを防ぐため、間違ったパスワードを利用しても１で始まり１で終わるように結果を偽装する。また利用したパスワードが正しいか否かは、サーバに問合せが必要となり、数回間違えるとロックされ、総当たり攻撃が不可能となる。

企業名（及び略称）　情報セキュリティ大学院大学	
代表者氏名　田中英彦 研究科長・教授	
所在地（郵便番号及び住所）　〒221-0835　神奈川県横浜市神奈川区鶴屋町2-14-1	
関連部署名及び電話番号　情報セキュリティ大学院大学事務局　045-311-7784	
ＵＲＬ　http://www.iisec.ac.jp/	
対象技術	技術開発状況
・侵入検知・防御技術 ・不正プログラム対策技術 ・その他アクセス制御機能に関する技術	1) TOMOYO Linux の研究開発 本研究では、アプリケーションが実行される状況に基づき、各アプリケーションが行おうとしている処理の内容を考慮することができるアクセス制御方式について検討している。提案方式は、TOMOYO LinuxとしてLinux上に実装され、公開されている。 2) アクセス制御ポリシー記述・管理方式の研究開発 本研究では、論理プログラムとしてアクセス制御規則を記述し、細粒度アクセス制御の課題であるポリシーの可読性や保守性を向上しながら、複数領域のポリシーを矛盾なく統合可能することで、情報システム全体のセキュリティを厳密なアクセス制御により強化するものである。本研究の成果に対しては、認可判定の妥当性と表現力の評価により、記述言語の有用性を実証済で現在1)を含む実際のＯＳへ実装中である。

（別添3）

【大学】

大学名	国立大学法人九州工業大学情報工学部飯塚キャンパス
所在地	〒820-8502 福岡県飯塚市川津680-4
関連部署／電話番号	0948-29-7500
ホームページのURL	http://www.iizuka.kyutech.ac.jp/
対象技術	技術の概要・特徴など
・その他アクセス制御に関する技術	高速パケット分類回路では、通常TCAMを使用している。しかし、TCAMは高価であり、消費電力も大きい。本製品は、汎用メモリと小型のFPGAのみを使用しているので、安価で低消費電力である。 本製品は、一般の消費者には販売せず、セキュリティ製品のベンダーに回路IPとして、提供する予定である。本研究は、文部科学省、地域イノベーション戦略支援プログラムの支援を受けている。

大学名	東京情報大学
所在地	〒265‐8501 千葉県千葉市若葉区御成台4‐1
関連部署／電話番号	庶務課／ 043-236-4603
ホームページのURL	http://www.tuis.ac.jp/
対象技術	技術の概要・特徴など
不正プログラム対策技術	現在のウイルスに対する対抗策は、各個人が所有するコンピュータ（以下「ノード」という。）に対し免疫を与えウイルスのまんえんを抑制している。これはネットワークの中からランダムにノードを選び免疫を与えている事になる（ランダム型）。バラバシ＝アルバートモデル（BAモデル）を用いたシミュレーションでは、この免疫配置手法ではネットワーク内部の８割ものノードに対し免疫を与えなければならないことが過去の研究から分かっている。 そのため平成14年にCohen らは、ネットワークの中からランダムにノードを選び、そのノードに隣接しているノード1つに免疫を与える手法（Cohen型）を提案し、２割程度の免疫数でウイルスのまんえんを抑制できることを実証した。 そこで、Cohen型を改良した手法の提案と、ASネットワーク（企業や学校などの団体を１ノードとした現実ネットワークデータ）を用いたシミュレーションでの効果の違い、またASに対する各免疫配置手法の効果の違いについての原因の解明を行った。 Cohen型では免疫を与えたノードのリンク数（ノード同士のつながり）がランダム型よりも多い特徴がある。これによりウイルスの拡散を最小限に留めることができ、ランダム型よりも効果的にウイルスのまんえんを抑制できる。これを応用し、Cohen型の改良として、ネットワークからある一つのノードを選び、そのノードに隣接している最もリンク数の高いノードに免疫を与える手法（Cohen改良型）でシミュレーションを行った。この結果、Cohen型よりもリンク数の多いノードに対し免疫を与えることができ、BAモデル、AS共にCohen型よりもCohen改良型のほうが効果的にウイルスのまんえんを抑制できた。

【企業】

企業名	株式会社エヌ・ティ・ティ・データ（略称NTTデータ）NTT DATA CORPORATION
所在地	〒135-6033 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	TEL.03-5546-8202（代表）
ホームページのURL	http://www.nttdata.co.jp/index.html
対象技術	技術の概要・特徴など
・侵入検知・防御技術 ・ぜい弱性対策技術	■使いこなせるOSセキュリティ強化カーネル TOMOYO(R) Linux ＜商品概要＞ ・Linuxサーバ向けのセキュリティ強化カーネルであり、アクセス制御機能を強化することで、システムへの不正侵入を防止します。アクセス許可の学習機能により、セキュリティポリシー作成の労力を大幅に削減します。直感的なアクセス許可の指定が可能な構文により、使いこなせるセキュアなＯＳを実現します。 ＜用途・適用業務＞ ・アプリケーションレベルでのアクセス制御を行うシステム（Webサーバ、APサーバ、DBサーバ等）に存在する未知のセキュリティホールを攻撃してシステムに侵入されるという脅威に対する保険として利用します。 ＜メリット・効果＞ ・システム管理者が作成したポリシーに基づきファイルの読み書きやプログラムの実行を制限することで、セキュリティホールに起因する不正侵入に対する耐性を大幅に高めます。また、セキュリティ修正プログラムの適用頻度を減らすことができるようになるため、動作確認試験のための稼動を大幅に削減できます。 ・ポリシーを最初から作成できるため、管理者が許可したいことだけを許可できます。また、ポリシーの作成を支援する機能があり、管理者が許可したいことを実行するだけでポリシーを作成できます。ポリシーの構文は単純で誰でも理解して使いこなせます。必要に応じてログイン認証の強化や管理者業務の分担も実現できます。 ＜特徴＞ ・理解して使いこなせることを念頭に開発されているので、誰でも簡単に導入及び運用ができます。 　実際のシステムの振る舞いに沿ってポリシーを作成するため、自然な記述ができます。そして、ポリシーの内容は誰にでも理解できるため、不要なアクセス許可を確実に検出することができます。 　TOMOYO Linuxは学習機能によりポリシーを作成することができるため、Linuxディストリビュータが関与できない独自アプリケーションに対応することが得意です。

企業名	株式会社ソリトンシステムズ（Soliton Systems K.K.）
所在地	東京都新宿区新宿2-4-3
関連部署／電話番号	本社　03-5360-3811
ホームページのURL	http://www.soliton.co.jp/
対象技術	技術の概要・特徴など
・高度認証技術	■有線/無線LANはもちろん、VPN、ダイヤルアップも安全にLANは、企業に蓄積されたあらゆる情報への出入口です。誰もが無秩序に接続できる状態ではなく、決められた人、決められたPCだけが接続できるように鍵をかけておく必要があります。 NetAttest EPSにはLANへの接続時にユーザやPCを特定する認証サーバとしてIEEE802.1X等ネットワーク認証に必要な機能が詰め込まれています。LAN接続時に認証を行えば、正規のユーザの利便性を損ねずに不正なユーザやPCをシャットアウトできます。もちろんLANへの直接接続だけではなく、VPNやリモートアクセス接続など、ネットワークの入り口を1台で守る統合認証サーバとして活躍します。 ■利用可能なユーザ情報データベース ・ローカル NetAttest EPSに内蔵されたデータベースです。 ・Active Directory Active Directory に登録されたユーザを参照できます。主にMS-PEAP 認証で利用します。 ・LDAP X.500準拠のLDAPサーバに登録されたユーザ情報を参照し認証できます。主にPAPで利用します。 ・RADIUS RADIUSプロキシ機能により、受信した認証要求を他のRADIUSに転送し、認証できます。 ■本格的なプライベートCA 証明書の発行や運用に必要な各種機能を搭載しています。証明書の要求から、承認、発行、配付、更新などの一連のワークフローを提供し、証明書の運用・管理負荷を大幅に軽減します。 ■ワンタイム・パスワード 認証のたびに毎回違うパスワードを利用するワンタイム・パスワードが利用可能です。別途サーバを用意することなく、手軽に利用開始できます。PCでもスマートフォンでも端末を問わず高いセキュリティを確保します。VPN接続の認証に最適です。

企業名	ヌリテレコム株式会社
所在地	東京都千代田区麹町3-2-4
関連部署／電話番号	03-3512-2882
ホームページのURL	http://www.nuritelecom.co.jp/index.html
対象技術	技術の概要・特徴など
・不正プログラム対策技術	・USBストレージ、CD/DVD、SDメモリカード、FDの使用を禁止します。 ・社内で使用する外部記憶媒体を管理し、個人所有の外部記憶媒体の使用を禁止することができます。 ・一時的に使用可能にした後、自動的に使用禁止に戻すことができます。 ・管理者のための機能が充実しています。 ・各PCの設定変更や一括変更、一覧表示が行えます。 ・PCをグルーピングして管理することができます。 ・禁止対象外のユーザを設定することができます。 ・禁止設定を行っているPCでも、緊急時に管理者がデバイスを使用することができます。 ・アプリケーションの起動には管理者パスワードが必要です。コンソールの操作履歴が採取できます。 ・アンインストールやサービスの停止、使用禁止設定変更のためには管理者パスワードが必須です。

企業名	株式会社シー・エス・イー
所在地	〒150-0044東京都渋谷区円山町23-2 アレトゥーサ渋谷ビル
関連部署／電話番号	03-3463-5631 （代表）
ホームページのURL	http://www.cseltd.co.jp/
対象技術	技術の概要・特徴など
・高度認証技術	SECUREMATRIX（セキュアマトリクス）は、株式会社シー・エス・イーが開発した、認証デバイスを一切使わない本人認証システムです。人が頭の中に思い描くイメージからワンタイム・パスワードを生成する「マトリクス認証」方式を採用し、セキュリティ及び利便性の向上、コスト削減の全てを同時に実現します。 ＜マトリクス認証の仕組み＞ 「マトリクス認証」は、ユーザがあらかじめ設定した「位置」と「順番」（＝パスワードイメージ）を使って、マトリクス表（アクセスするたびにランダムに表示が変わる乱数表）から、その位置と順番に当てはまる数字を抜き出してワンタイム・パスワードとして認識させる認証方式です。パスワードは「ワンタイム（使い捨て） 」になるため、強固な認証を実現できます。

企業名	ファインアートテクノロジー
所在地	〒30072 台湾新竹市埔頂路18号8F
関連部署／電話番号	886-3-577-2211（代表）
ホームページのURL	http://www.fineart.com.tw/jp/
対象技術	技術の概要・特徴など
・不正プログラム対策技術	■X-FORT主要機能 ・コンピュータ周辺機器経由の情報漏えい防止 UFD、モバイルハードディスク、メモリカード等各種外部メモリデバイス及びCD/DVD-ROMドライブ、プリンタ、赤外線、Bluetooth等の書き出しルートを制御することができます。またハードプロテクションメカニズムを提供、ディスクによる起動やハードディスク接続によるデータの持ち出しを防止します。特に外部メモリデバイスに対し、禁止・リードオンリー・自動暗号化・管理者承認等多種のアクセスパターンを提供、情報セキュリティとユーザビリティを兼備した柔軟なツールです。 ・ネットワーク経由の情報漏えい防止 マイネットワークの利用を厳格に制御、電子メール、IMソフトウェア、P2Pソフトウェア、FTP、Webアップロード等の方法によるファイル転送、3G／3.5Gネットワークカード、無線ネットワークカード、ダイヤルアップネットワーク接続等行為等、完璧にネットワークルートの流出を制御します。 ・トータルなコンピュータ管理ツール 具有ソフトセキュリティ、リモートコントロール、ファイル転送、コンピュータ資産管理、Windows Update及びWSUS・Hotfix等コンピュータ管理機能を統合、また豊富な分析レポートを提供、コンピュータの状況を完全に把握することができます。 健全なシステム構成：データベース及びエクスポートログの定期バックアップカスタマイズが可能、事後調査のよりどころとすることができます。さらに自動バックアップ及びロードバランス機能を備えたclient-server構成、複数拠点を擁する大型企業に対しサーバ間の同期及び暗号ローミングメカニズム等多様なサーバ集中管理機能を提供します。 ・システムのセルフディフェンスメカニズム 作為的なデータの破壊や削除行為を回避します。クライアントへのサイレントインストールはユーザの操作にまったく影響を及ぼしません。

企業名	シスメックスＲＡ株式会社
所在地	本社　〒399-0702 長野県塩尻市広丘野村1850-3
関連部署／電話番号	TEL．0263-54-2251（代）
ホームページのURL	http://www.sysmex-ra.co.jp/
対象技術	技術の概要・特徴など
・ぜい弱性対策技術 ・高度認証技術	■IPsecによる強固なセキュリティ機能 　強力な暗号化と認証機能を持ったIPsecにてプロトコルやアプリケーションに関係なく転送される通信データ（TCP/UDPパケット）のセキュリティ機能を高めることができます。 ■簡単接続 　イーサネットインターフェースを2ポート装備し、通信機器とLANケーブルの間に中継器として挟み込むだけで通過する通信データは自動的に暗号化され送信先へと転送されます。 また、通信機器へは設定変更や特殊なアプリケーションをインストールする必要はなく、既存システムへの導入が迅速に行うことができます。 ■柔軟設定 　設定はPC上から専用ツール（NSSetup）にて行います。 認証キーの設定のみで完了する基本的な対向通信から、詳細なセキュリティポリシーの設定による経路別の動作指定といった応用的な用途まで幅広く柔軟に対応できます。 ■高速・安定動作 　専用ASICによるハードウェア処理により、最高90Mbps（AES、512byte/pkt双方向通信時のSmartbit値）の高速で安定した動作を実現しています。 ■NAT対応 　NAT-Traversal/UDP-Encapsulation によるNAT越えを実現できます。

企業名	ウォッチガード・テクノロジー・ジャパン株式会社
所在地	〒150-8512 東京都渋谷区桜丘町26-1 セルリアンタワー15階(本社は米国)
関連部署／電話番号	03-5456-7880
ホームページのURL	http://www.watchguard.co.jp/
対象技術	技術の概要・特徴など
・侵入検知・防御技術	■ XTM多機能ファイアウォール WatchGuard XTMネットワーク・セキュリティ・アプライアンスは、新しいクラスのパフォーマンス・ソリューションです。 高速スループットを大量のトラフィックに対応できる先進的なネットワーク機能と組み合わせ、手頃な価格で提供できます。 標準で柔軟な管理ツールがバンドルされているので、IT管理者は中央のコンソール、コマンドラインインタフェース、またはWebUIから一元的にセキュリティ管理を行うことが可能です。 WatchGuard XTMは、全部で16モデルです。 ・50ユーザから10,000ユーザ以上の環境まで、幅広いビジネスに対応しています。 ・Firewall、UTM機能をベースにレイヤ7のアプリケーション制御を実施できます。

企業名	株式会社ＣＩＪ
所在地	横浜市西区平沼1-2-24 横浜ＮＴビル
関連部署／電話番号	045-411-2571（市場開拓推進事業部市場開拓企画部）
ホームページのURL	http://bunshokanri.jp/
対象技術	技術の概要・特徴など
・その他アクセス制御に関する技術	Ofigoは文書管理システムと契約書管理システムをラインナップしたシリーズ製品 ■Ofigo文書管理 　Ofigo文書管理サーバへは、使いなれたブラウザでアクセスでき、登録も簡単な操作でドラッグ＆ドロップできるため「使いやすく、分かりやすい」４階層構造となっています。 その他 ・アクセス権限の設定で、重要ファイルへのアクセスを制限 ・Ofigo文書管理サーバへの全操作ログを保管 ・データは自動で暗号化。万が一の場合も情報漏えい防止 ・「確定署名」でファイルを改ざんから守る ことができます。 ■Ofigo契約書管理 　締結されている契約書の内容など都度総務に電話して聞かなくても、この契約書管理ソフトをインストールすれば自席のパソコンより確認ができます。 締結先、契約名、担当者など、各種の属性で検索できるので大量の契約書から該当する契約があるか？その内容は？などすぐさま確認することができます。 　契約の更新・メンテナンスなどに便利な、期限通知ができます。 　通知日と通知先を設定しておくことで、自動でメール通知が行われます。また、この設定は何個でも設定することが可能です。

企業名	日本信号株式会社（THE NIPPON SIGNAL CO.,LTD）
所在地	〒100-6513 東京都千代田区丸の内1-5-1 新丸の内ビルディング
関連部署／電話番号	03-3217-7200
ホームページのURL	http://www.signal.co.jp/
対象技術	技術の概要・特徴など
・侵入検知・防御技術	■目的 入室管理と連携し、物理資産の閲覧・貸出しの管理を行う。 ■機能概要 ・書類検知（常時） ・書類位置検索、表示 ・書類アクセス検知 ・書類持ち出し／貸出し管理 ・返却管理 ・不正アクセス管理 ■システム利用例 ・物理資産に積層ICタグを貼り付け、登録用リーダでサーバに登録する。 ・積層ICタグを貼り付けた物理資産を各書庫に設置し、積層ファイルリーダにより常時監視を行う。 ・書庫から書類を取り出す際には、各書庫の上に設置された認証用リーダに物理資産をかざし持ち出す。 ・認証せずに物理媒体を持ち出す等の不正があったときには警報装置が作動する。 ■システム構成及び導入規模の例 ・積層ICタグ１万5000枚 ・積層ファイルリーダ ・積層トレイリーダ ・管理サーバ ・情報端末必要数 ・警報装置必要数 ・入室管理システム別途用意

企業名	日本信号株式会社（THE NIPPON SIGNAL CO.,LTD）
所在地	〒100-6513 東京都千代田区丸の内1-5-1 新丸の内ビルディング
関連部署／電話番号	03-3217-7200
ホームページのURL	http://www.signal.co.jp/
対象技術	技術の概要・特徴など
その他アクセス制御に関する技術	■目的 交通ICカードシステムの内部統制を実現するために、交通ICカード利用における一件明細の完全性保障と不正行為を防止する。 ■機能概要 ・接続するネットワークの正当性検証 ・運用者及び保守員の識別・認証 ・権限に応じたアクセス制御 ・データ保護 ・監査ログ取得 ■アクセス制御機能を実装した装置の例 ・自動券売機 ・自動精算機 ・自動改札機 ・駅係員端末 ・チャージ機

企業名	日本無線株式会社
所在地	〒167-8540東京都杉並区荻窪4-30-16藤澤ビルディング
関連部署／電話番号	03-6832-1721（代表）経営企画室／0422-45-9774
ホームページのURL	http://www.jrc.co.jp/jp/index.html
対象技術	技術の概要・特徴など
ぜい弱性対策技術	NDC-1434は、異なるイントラネットワーク間で、TCP/IPにより情報交換を行う場合のIPアドレス変換やセキュリティ問題を解決するゲートウェイ装置です。 ◆８組のクライアントーサーバ間のTCPコネクションデータを中継することが可能です。 ◆ネットワーク間の分離が可能となり、インターネットワーク間のセキュリティ機能を実現します。 ◆イントラネットワーク間のIPアドレス体系を完全に分離できます。

企業名	富士通株式会社
所在地	本店住所: 〒211-8588 神奈川県川崎市中原区上小田中4-1-1
関連部署／電話番号	044-777-1111
ホームページのURL	http://jp.fujitsu.com/
対象技術	技術の概要・特徴など
その他アクセス制御に関する技術	Interstage Application Server （インターステージアプリケーションサーバ）は、変化するビジネス環境を継続的に支える高信頼・高性能なアプリケーション実行基盤です。 富士通独自のスマートソフトウェアテクノロジー（注）と互換性保証及び標準技術への対応により、業務システムの安定稼動や、素早いシステム構築や柔軟なサーバ集約を実現します。