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５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
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
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
効率的な鍵管理機能を持つクラウド向け暗号化データ共有システムの研究開発

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24年12月6日から平成25年１月10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10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そのまま掲載している。

株式会社神戸デジタル・ラボ
日本コントロールシステム株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社日立システムズ
ニクサン株式会社
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
株式会社ネクストジェン
株式会社フォティーンフォティ技術研究所
株式会社シマンテック

(2)　調査

警察庁が平成24年11月から平成24年12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（７大学）

神奈川工科大学
熊本大学
玉川大学
東洋大学
北海道情報大学

立命館大学
琉球大学

イ　企業（６社）
沖電気工業株式会社
キーウェアソリューションズ株式会社
ソースネクスト株式会社
日本電気株式会社
富士通株式会社
１ｓｔホールディングス株式会社

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289校、企業1,111社の計1,400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）

テーマ名　ネットワークセキュリティ技術の研究開発
対象技術　インシデント分析技術
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、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、その有効性を活用するための、可視化エンジンを開発した。
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 電話　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。

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
対象技術　インシデント分析技術
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)情報通信研究機構からの委託）
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） 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。

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
対象技術　不正プログラム対策技術
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（(独)情報通信研究機構からの委託）
背景、目的 近年、マルウェア（不正プログラム）に関して、実行コード（ここではスクリプトまたはプログラムのソースコードを指す。）を意図的に読みにくくする“難読化”や、実行コードが意図的に動的に変更される“自己変貌化”等の手法の開発が進んできている。このような既知のものではないマルウェアに対しては、シグネチャ(マルウェア検査パターン)等の既存技術による検出や駆除だけで対応することには自ずと限界がある。 このようなマルウェアに関しては、感染行動等の挙動を把握することが重要となる。しかしながら、感染しても正規の実行コードを装い、それに気付かせないようにするものや、外部の指令サーバからの攻撃命令を待ち受けるなど、挙動を示すまでに一定の時間を要するものが存在する。このため、ユーザのパソコン内で稼動・常駐しているプログラムがマルウェアであるかどうかを判別するためには、当該プログラムの実行コードを詳細に解析することが有用である。 しかしながら、ユーザのパソコン内で稼動・常駐している多種多様なプログラムのうち、大多数は正規の実行コードであることから、そのようなプログラムの中からマルウェアの疑いのある怪しい実行コードのみを的確に選別することは難しい状況である。 また、ユーザのパソコン上で、実行コードを詳細に解析するにあたっては、処理が重く、パソコンのリソースへの負荷が大きくなることが懸念される。 他方、アンチウイルスソフトを提供するセキュリティベンダーにおいても、このような新しいマルウェアが現出するたびに、詳細な解析を行い、パターンファイルの更新や提供を行ってきているが、ビジネス面の制約などもあり、ユーザが必要なときに、必要なものをタイムリーに提供するところまでには至っていない。
研究開発状況（概要） ・平成21年度より以下の研究開発を開始し平成23年度に終了した。 （１）検査プログラムに関する研究開発 （２）マルウェア駆除ツールの自動生成・最適化・高速検証手法に関する研究開発 （３）ユーザサポートプロトコルに関する研究開発 （４）課題ア～ウ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://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。

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

対象技術　ぜい弱性対策技術

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

近年インターネットに接続するデバイスの多様化が進んでおり、情報家電や制御システムなど様々なデバイスがインターネットに接続するようになってきている。しかし、情報家電等はオープンなネットワークに接続して利用されてこなかったことからセキュリティ対策が不十分であり、対策が急務となっている。

これに対して、セキュリティ脆弱性を自動検出するための技術を研究開発する。未知のセキュリティ脆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、研究成果をツール化することにより、一般の開発現場で手軽に脆弱性を発見することが可能となる。

研究開発状況（概要）

平成22年度、23年度に実施した情報家電等、非PC端末に対するファジング技術開発・実装の継続に加えて、平成24年度では、制御システム向けのファジング技術として、EDSA（Embedded Device Security Assesment）認証に適合可能なファジングツールの研究開発を実施している。EDSA認証はISASecureにより策定されたもので、制御システム機器、及びその評価ツールの満たすべき要件を定めたものである。

EDSAに規定された要件に適合するツールの開発を実施し、認証の取得を行うべくISASecureへの認証申請を実施している。

また、23年度より継続して以下に関する技術開発を継続している。

①Fuzzingエンジン群追加開発

（１）ミューテーションファジングの研究及び開発

23年度の研究結果を基に、ブロックソート方式、統計に基づくデータ生成方式、オートマトン方式、バイナリツリー方式のミューテーションアルゴリズムを研究開発する。

（２）モバイルOS脆弱性発見手法調査

23年度は、Android OSを対象にアーキテクチャ、セキュリティモデル、考えられる脅威の分析を行った。本年度は、対象をAndroid以外のOSまで広げ、今後普及することが想定されるモバイルOS全般について同様の調査を実施する。本年度はAndroid以外のOSとしてWindows Phone 7に関する調査を行い、BlackHat USA 2012にて講演を実施している。

http://www.blackhat.com/usa/bh-us-12-briefings.html#Oi

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　（電話：03-6277-1811）

将来の方向性

平成 22 年度から 3 年をかけてファジングエンジンの研究開発や EDSA 認証に適合可能なツールの研究開発を行った。今後、対応プロトコルの拡充、新規のファジングアルゴリズムの研究開発を行い、情報家電に限らず幅広い分野で利用可能なツールとしていく。

テーマ名　効率的な鍵管理機能を持つクラウド向け暗号化データ共有システムの研究開発

対象技術　その他アクセス制御機能に関する技術

開発年度　平成 22 年度～平成 24 年度

実施主体　株式会社神戸デジタル・ラボ（KDL）（経済産業省からの委託）

背景、目的

理論の分野では、属性ベース暗号、格子暗号、インテリジェント暗号等、次世代に向けた様々な方式が提案されている。一方で、実際のサービスとして提供されているのは Voltage Security Inc.の ID ベース暗号など、数少ない。

近年、脚光を浴びているクラウドコンピューティングに適すると言われる属性ベース暗号方式に着目し、サービスとして提供できるレベルに引き上げるための研究開発を行い、サービスモデルの構築・評価を行い、サービス化を目指す。

研究開発状況（概要）

本研究開発事業では、クラウド環境を利用する際に企業が求めている高度なプライバシー保護機能を持った暗号化データ共有システムの研究開発を行い、クラウドコンピューティングのセキュリティに対する不安を解消する安全・安心なクラウドコンピューティングサービスを提供する基盤を構築した。

具体的には、クラウド内のデータを暗号化する方式として、属性ベース暗号方式を採用した暗号モジュールの実装を行い、実運用に耐えられるように鍵失効機能を追加したデータ共有システムの基盤を構築した。

さらに実用に耐えうるか性能評価を実施し、また有識者からの意見を募り有用性を評価した。

本研究の成果は大手機械メーカーに採用され、実際のサービスへの実装に向けて活動中である。

詳細の入手方法（関連部署名及びその連絡先）

株式会社神戸デジタル・ラボ（KDL）（http://www.kdl.co.jp/）
セキュリティソリューション事業部　近藤伸明　（電話：078-327-2280）

将来の方向性

現在サービス実装を行っている案件を拡張し、企業内の属性ベース暗号基盤を構築・販売するモデルを確立し、営業展開を行う。

並行して、複数の企業を一括して１つの属性ベース暗号基盤で賄える仕組みを開発し、中小企業にも普及できる廉価モデルの構築を目指す。

上記サービスを展開することにより、企業が利用する高度情報通信ネットワークに係る安全性・信頼性の確保に貢献する。

（別添２）

企業名（及び略称） 株式会社神戸デジタル・ラボ（KDL）	
代表者氏名：永吉一郎	
所在地（郵便番号及び住所）〒650-0033 兵庫県神戸市中央区江戸町93番栄光ビル5F	
関連部署名及び電話番号 セキュリティソリューション事業部　近藤伸明　078-327-2280	
ＵＲＬ http://proactivedefence.jp/	
対象技術	技術開発状況
ぜい弱性対策技術 研究開発時期： 平成24年度	「Androidアプリケーションの脆弱性診断技法の研究開発」 対策技術本研究開発では、Androidアプリケーションを提供／開発／運用する企業が脆弱性のない安全なAndroidアプリケーションであることを確認研究開発時期するために実施するAndroidアプリケーションの脆弱性診断について、効率よく網羅的に診断できる手法の研究開発を行った。 これまでもマルウェア等の不正アプリケーションからスマートフォンを守る為の対策は実施することはできた。また、JSSECC日本スマートフォンセキュリティ協会）により「Androidアプリのセキュア設計・セキュアコーディングガイド」が平成24年11月に公開され、これによる対策は実施できたが、Androidアプリケーションの脆弱性診断の観点からは不十分であった。 具体的には、「使用されるSSL証明書が不正であるか否かをチェックするロジックが欠落していないか」「WebView等の機能を持つ場合に不正なJavaScriptが実行されないか」等の脆弱性について、運用者や利用者の目線による脆弱性だけではなく、アプリ開発者やハッカー目線での脆弱性を研究成果として追加し、自動診断ツールの開発を行った。 研究成果については、自社のAndroid診断のサービスとして平成24年12月より提供を開始すると伴に、JSSECにて診断項目の標準化の一環として共有していく予定である。

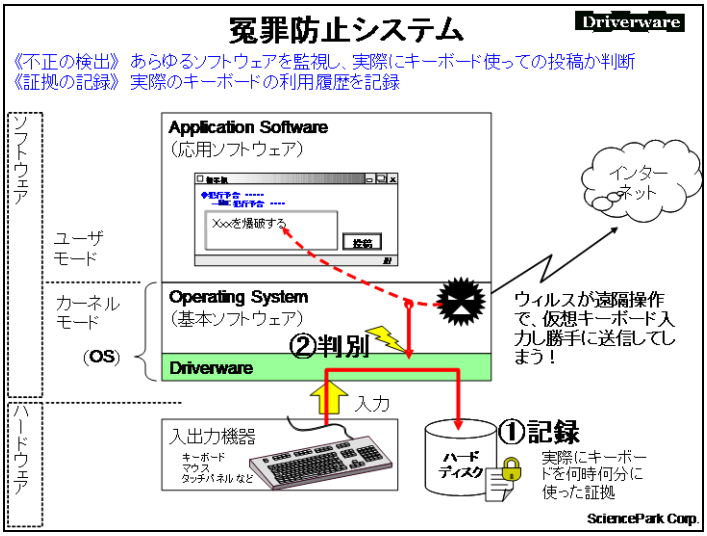
企業名（及び略称） 日本コントロールシステム株式会社（NCS）	
代表者氏名　　堀内 伸泰	
所在地（郵便番号及び住所）〒150-0013 東京都渋谷区恵比寿1-19-15 ウノサワ東急ビル7階	
関連部署名及び電話番号 NEPPIOユニット 045-477-5800	
ＵＲＬ http://www.nippon-control-system.co.jp/	
対象技術	技術開発状況
侵入検知・防御技術 開発年： 平成21年度～ 平成24年度	CFCA(Communications Fraud Control Association)の報告書(2011 Global Fraud Loss Survey)によると、現在世界で起こっている通信サービスを利用した様々な攻撃の中で、国際電話を不正に利用した「なりすまし電話」による被害額は40億ドルに上る（2011年）。これは、IDやクレジットカードの不正利用によるものを上回り最多の額となっている。 このような状況に対し、VoIPサービスを利用した「なりすまし電話」のような脅威からの防御に有効な以下の技術開発を行った。 ・ネットワークを流れるメッセージのリアルタイム解析をプロトコル定義書レベルで行う。これにより悪意のあるメッセージを検出する。 ・管理画面から編集可能なプロトコル定義書から解析ルーティンを自動生成する。これによりサービス稼働中に解析ルーティンを変更し、即時に新しい攻撃へ対処することが可能となる。 ・メッセージ内の任意の情報で統計情報を作成する。例えば、「先週、先々週の同時刻と比較して150%を上回る国番号への発呼があった場合、アラームを上げる」など、統計情報との比較条件も柔軟に設定可能。

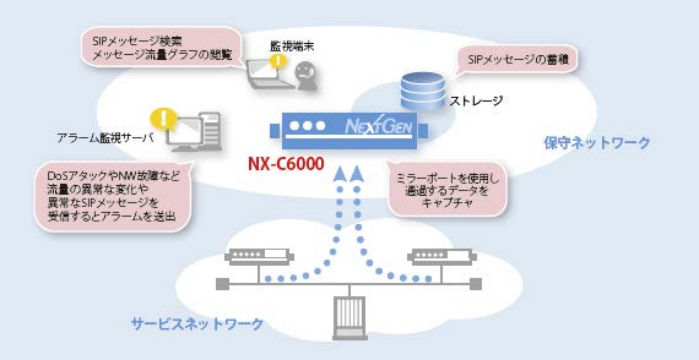
企業名（及び略称）エヌ・ティ・ティ・コミュニケーションズ株式会社	
代表者氏名　有馬 彰	
所在地（郵便番号及び住所）　〒100-8019 東京都千代田区内幸町１丁目１番６号	
関連部署名及び電話番号　先端IPアーキテクチャセンタ 050-3812-4697	
ＵＲＬ　http://www.ntt.net/service/traffic.html	
対象技術	技術開発状況
その他アクセス制御機能に関する技術	1) ネットワーク機器の情報を収集することで、大規模ネットワークの利用状況を可視化。 ネットワーク機器が吐き出す xFlow 情報を収集、統計化したものを WebUI で分析することで、 IP アドレス、アプリケーション毎のトラフィックを分析することが可能。 2) トラフィックパターンの解析によりDDoS攻撃等の異常トラフィックを検知。 類型化したシグネチャとのマッチング、週平均、曜日平均等の通常トラフィック波形からの乖離レベルチェック等により、異常の発生を検知。 3) DDoS 攻撃発生時に制御機器と連携して攻撃元からのアクセスを遮断するためのコード出力。 検知されたDDoS攻撃のアクセス元インタフェースに対し､ネットワーク機器を制御して攻撃トラフィックを遮断･ブラックホール装置へ誘導するための制御コードを出力｡通知情報とあわせて制御機器と連携してDDoS攻撃を効率的に軽減するために利用可能。

企業名（及び略称）　株式会社日立システムズ	
代表者氏名　高橋　直也	
所在地（郵便番号及び住所）　141-8672 東京都品川区大崎１－２－１	
関連部署名及び電話番号　03-5435-7777（代表）	
ＵＲＬ　http://www.hitachi-systems.com/	
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	日立システムズが開発したセキュリティプロダクト「SSCom（エス・エス・コム）」はクライアント・サーバ間のオンライン認証、暗号通信、アクセス制御などのセキュリティ機能を電子証明書を使用して実現するソフトウエア製品です。 SSComがサポートする各機能は電子証明書のX.509規格、認証と暗号通信のSSLなどの国際標準または業界標準の基盤技術と、独自開発によるアクセス制御の応用技術から構成されます。 研究・開発した応用技術 ＜グループアクセス制御＞ グループアクセス制御とは一般的な用語ではなく、株式会社日立製作所殿の研究成果を当社が製品化した技術です。ユーザやアクセス対象をグループとして定義することにより、例えば企業での人事異動などにも容易に対応できるシステムを構築可能とする技術です。 特徴を以下に示します。 ・アクセス対象ごとに接続を許可するユーザやグループを指定できる ・グループは、「開発プロジェクト」のように部署を横断する名称を指定でき、「所属＝本社」のような所属を意識した条件式でも指定できる ・グループにも他のグループや条件式を指定できる ＜モバイル接続への対応方式＞ アクセス制御情報に「アクセスした場所」という情報を指定でき、同一ユーザに対してアクセスする場所の違いによるアクセス権限を設定できます。 ＜大規模構成への対応方式＞ アクセス制御情報は一元的に管理できますが、システムが大規模になりすぎると特定の管理者の負荷が大きい。このため、SSComでは多段認証機能によりアクセス権限（定義）の分散管理を実現しています。

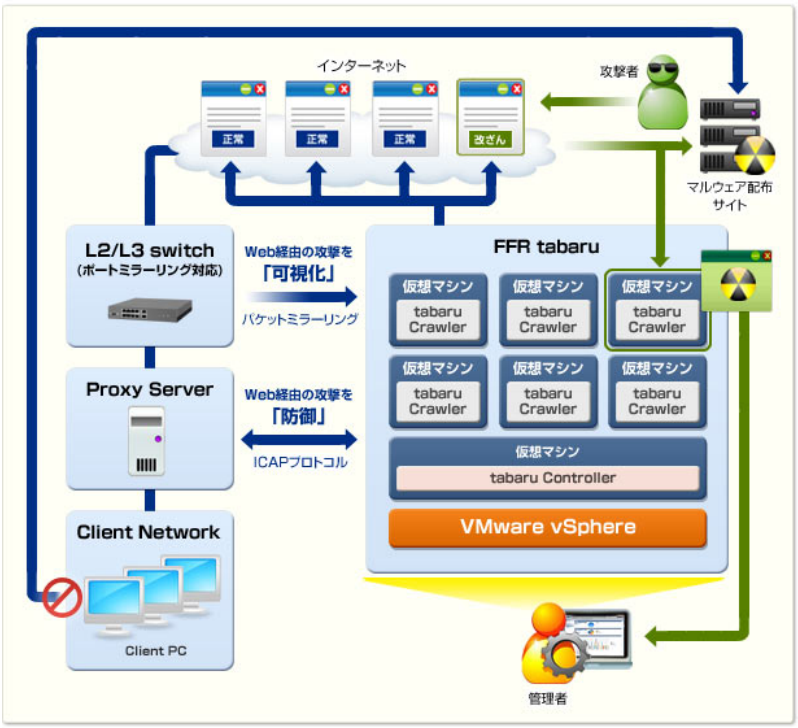
企業名（及び略称） ニクサン株式会社	
代表者氏名：伊藤一彦	
所在地（郵便番号及び住所）〒103-0023東京都中央区日本橋本町3-3-6ワカ末ビル7階	
関連部署名及び電話番号 営業部　03-6202-7454	
ＵＲＬ http://www.niksun.co.jp	
対象技術	技術開発状況
インシデント分析技術 平成１２年 侵入検知技術 平成１７年	NIKSUN社（米国プリンストン市） が開発したインシデント分析技術は NetDetector （アプライアンス装置名）に下記機能を実装しました。 すべてのパケットを取得 NetDetector は、ネットワークを通過するすべてのパケットを収集し、関連付けを行って独自のデータベースへ保存を同時に行うことができる唯一のセキュリティ監視アブライアンスです。取得した各パケットにタイムスタンプを付与して結合し、インデックス化します。これによりネットワークのセキュリティ監視カメラのように詳細な情報を提供します。 詳細なフォレンジック分析 NetDetectorは、ネットワークパケットから様々のコンテンツを抽出することができる最も高度なフォレンジック製品です。音声、映像、ウェブ、IM、FTP、Eメール、画像などの広範囲に渡るコンテンツを詳細で高速に検索し、再現します。これによりセキュリティに関するインシデントを迅速に認識し、根本原因の修正を行うことができます。 統合性のある可視化 今日のサイバー攻撃において、効果的な検知は資産を守るために必要不可欠な手段です。NetDetectorは、異常やシグネチャに基づいた侵入をプロアクティブに検知します。これらは、ラインレートのスピードでネットワークトラフィックを分析して、即座に攻撃対象となったシステム、ゼロデイ攻撃、マルウェアなどを検知します。

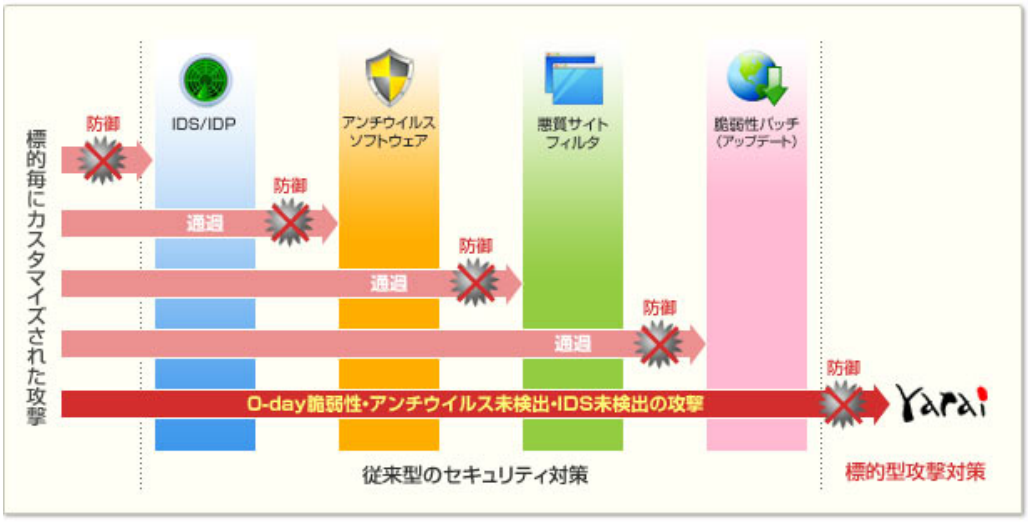
企業名（及び略称） イーロックジャパン株式会社	
代表者氏名：秦　基嘉	
所在地（郵便番号及び住所）東京都千代田区麹町3-12-7	
関連部署名及び電話番号 セキュリティ事業部　03-3265-1169	
ＵＲＬ http://www.elock.co.jp/webalarm/index.html http://www.gridelock.com/gridv2/demo.htm	
対象技術	技術開発状況
・侵入検知・防御対策 ・脆弱性対策技術 ・高度認証技術 ・その他アクセス制御機能に関する技術 開発年：平成11年	１）「WebALARM」は、不正侵入や人為ミス等の対策として開発されたコンテンツセキュリティ対策ソフトウェア製品です。 WebALARMは、サーバ上のあらゆる静的ファイルをリアルタイムに監視するとともに、万一不正に改ざんされた場合でも自動修復し、証拠を保全するリカバリーツールです。WebALARMは、不正改ざんを検出後、いち早く管理者に警告を出し、自動的に元のコンテンツに復旧します。 ２）不正アクセスを防ぐ２要素認証システム 「The GRID」は、安全性と利便性を実現する多要素認証システムです。普段ご利用のパソコン等を鍵として使う、またスマートフォンでアカウントをロックするという２段構えで簡便で安全性の高いセキュリティを提供いたします。そのため、ユーザー様は、従来の複雑な第２認証要素から解放され（専用デバイス、マトリクス表やソフトウェア等が不要）、強固なセキュリティを実現します。

企業名（及び略称）　サイエンスパーク株式会社	
代表者氏名　代表取締役社長　小路 幸市郎	
所在地（郵便番号及び住所）　〒252-0024 神奈川県座間市入谷3-1649-2	
関連部署名及び電話番号　ドライバウェア事業本部　046-255-2544	
ＵＲＬ　http://www.sciencepark.co.jp/information%5Fsecurity/	
対象技術	技術開発状況
不正プログラム対策技術	【概要】 冤罪防止のために、物理キーボード入力履歴と遠隔操作によるキーボード入力履歴とを区別する技術を活用する。 【特徴】 最近問題になっている、なりすましによる掲示板投稿の犯人誤認の原因は、サーバ側に記録される投稿者のパソコンのＩＰアドレスを重視していたことに起因する。従来の対策は、投稿者のパソコン内に潜む遠隔操作するウイルス感染の履歴を調査することで、遠隔操作か否かを区別することであった。しかし、高度化するウイルスの機能で、実行後にウイルスが自身を削除し履歴を復元できなくする手法により、分析に多大な時間とコストを要している。 本技術は、パソコンに接続されたキーボード（物理キーボード）からの入力履歴を記録する機能を持つデバイスドライバで構成される。このような独自機能を持つデバイスドラバ群をパソコンＯＳ内の各周辺機器の制御ルートに配置し、周辺機器を横断的に制御する、Driverware（ドライバウェア）という技術を利用する。物理キーボードの入力履歴を記録することで、なりすましの分析を容易にし、また遠隔操作されていると判断した場合にはネットワークなどの外部通信を遮断することで、なりすましによるパソコン利用を防ぐ。  冤罪防止ソフトウェアの概要図

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/index.html	
対象技術	技術開発状況
侵入検知技術 開発年： 平成21年度-平成24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、インターネット上ではSIPで使用されているポート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ないものと考えられています。 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、攻撃に使用されるツールのフットプリントを特定、検知する他、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。また、本システムをハニーポットとして利用し、攻撃パケットの収集及び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/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/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24年度	＜概要＞ SIP(Session Initiation Protocol)を使用したVoIP(Voice over IP)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攻撃などによるシステムの停止に繋がる脆弱性を洗い出します。今年度には、それまで手作業で行っていた脆弱性検出作業を自動化するツールを開発、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）　株式会社フォティーンフォティ技術研究所	
代表者氏名　鵜飼裕司	
所在地（郵便番号及び住所） 〒150-0013 東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4階	
関連部署名及び電話番号　技術戦略室/03-6277-1811	
ＵＲＬ　http://www.fourteenforty.jp/	
対象技術	技術開発状況
侵入検知・防御技術 開発年： 平成 22 年度～ 平成 24 年度	【背景】 標的型攻撃ではメールの添付ファイルとしてマルウェアを送り付けるだけでなく、メール文面にWebリンクを記載して不正サイトに誘導し、ドライブバイダウンロードの手法を用いてWebを閲覧するだけでマルウェアを侵入・感染させる手口が問題となっています。 【概要】 フォティーンフォティ技術研究所が開発した「FFR tabaru」は、ゲートウェイ型標的型攻撃対策製品として開発されたセキュリティソリューションです。基本的な仕組みは、ネットワーク上に仮想化技術を使ってエンドポイント環境を再現し、NWスイッチやProxyから受け取ったURLを巡回します。仮想環境には標的型攻撃の検出に特化した「FFR yarai」のヒューリスティックエンジンが搭載されており、Web経由の標的型攻撃を高精度に検知します。 【製品概要】 http://www.fourteenforty.jp/products/tabaru/index.htm 【システム概念図】 図解 FFR tabaru システム概念図 

ぜい弱性対策技術 開発年： 平成 20 年度 ～ 平成 22 年度	【背景】 既存のウイルス対策製品では、近年のマルウェアが悪用するセキュリティ脆弱性攻撃の検知機能が実装されておらず、効果的に機能しているとは言えない状況です。また、既存のウイルス対策製品は、マルウェアの個体を特定するパターン情報の配信が完了するまで対策が十分に行えない状況にあり、ファイアウォール、IDS/IDP、アンチウイルス、ソフトウェアアップデートといった複合的な対策でも防御困難なケースが増加しています。 【概要】 フォティーンフォティ技術研究所が開発した「FFR yarai」及び「FFR yarai 脆弱性攻撃防御機能」は、「ヒューリスティックエンジン」検出機能を搭載することにより、マルウェアが感染活動で使用する、ほぼ全ての脆弱性攻撃を防御可能です。 また、昨今のマルウェアに実装されているコード実行型のセキュリティ脆弱性攻撃に対し、パターン情報に依存することなく汎用的な仕組みで確実に検知します。 【製品概要】 http://www.fourteenforty.jp/products/yarai/index.htm http://www.fourteenforty.jp/products/yaraizdp/index.htm 【従来型対策との違い】 図解 従来型の対策とFFR yarai(標的型攻撃対策)の違い 

インシデント分析技術 開発年： 平成 23 年度	【背景】 国家や企業をターゲットとした標的型攻撃は、巧妙な攻撃手法を取り入れており、ターゲット組織のセキュリティ対策を潜り抜けることを目的としたマルウェアを作成、ソーシャルエンジニアリングを駆使したメールやSNS等でターゲット組織内にマルウェアを送り込みます。 セキュリティ脆弱性を悪用したマルウェアも急増しており、近年では未修正(0-day)の脆弱性を悪用するケースも多発しています。このため、近年の新しいマルウェアの多くは、既存の仕組みで検知できない状況が続いています。 【概要】 フォティーンフォティ技術研究所が開発した「FFR yarai analyzer」はインシデント発生時に、既存の仕組みでは検出が困難となってきている新しいタイプのマルウェアによる脅威を可視化し、対抗するための製品です。プログラムファイルや文書ファイル、各種データファイルを自動的に解析し、マルウェア判定だけでなく、どのようなリスクが想定されるかを把握するための概要解析結果をレポートとして出力します。 【製品概要】 http://www.fourteenforty.jp/products/yarai_analyzer/index.htm

不正プログラム対策技術 開発年： 平成 24 年度	【背景】 昨今オンライン・バンキングにおける振込操作や、オンライン・ショッピングサイトにおけるクレジットカード等による電子決済がWebブラウザ上で行われています。こうした取引がWebブラウザ上で行われることが定着してきたことにより、Webブラウザを取り巻くセキュリティ脅威は深刻化してきています。 【概要】 フォティーンフォティ技術研究所が開発した「FFRI Limosa」はオンライン・バンキングを提供する金融機関やEC事業者、SNSなどのWebサービス事業者などが管理するWebサーバーへ設置することで、サービス利用者がログイン時に自動的にWebブラウザへ適用され、従来型脅威であるID/パスワードの搾取を防御するだけでなく、新しい脅威であるユーザー端末上に不正プログラムとして感染したマルウェアによるMITB攻撃からもWebブラウザを守ります。 【製品概要】 http://www.fourteenforty.jp/products/limosa/index.htm 【対策概要図】 図解 FFRI Limosaによるブラウザの保護 

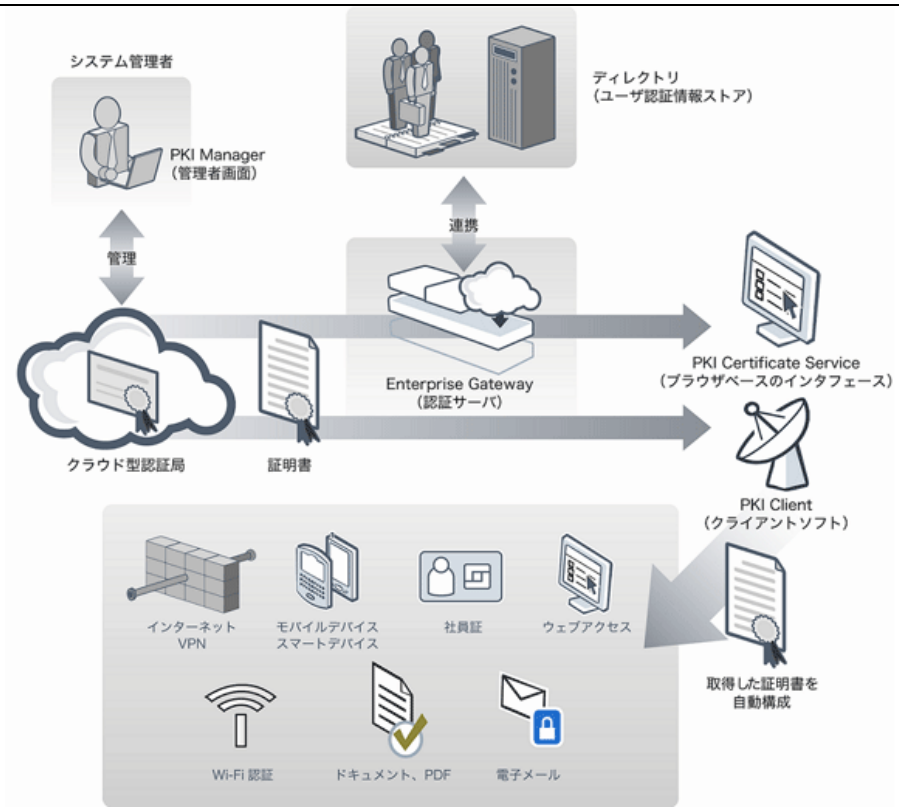
企業名（及び略称）：株式会社シマンテック（シマンテック）	
代表者氏名：河村浩明	
所在地（郵便番号及び住所）：〒107-0052 東京都港区赤坂1-11-44	
関連部署名及び電話番号：	
ＵＲＬ：http://www.symantec.co.jp	
対象技術	技術開発状況
侵入検知・防御技術(平成21年)	Symantec Critical System Protectionとして製品化 Symantec Critical System Protectionは、ホスト上のプロセスおよびユーザに対してホワイトリスト化された動作のみを許可することで不正な操作を防止します。 主要な機能は下記の通りです。 - ファイル改ざんの監視: 変更を行ったユーザーやファイル内の変更箇所など、ファイルへの変更をリアルタイムで識別。 - 設定の監視: ポリシー違反、不審な管理者、および侵入者の活動をリアルタイムで識別。 - 対象を絞った防止ポリシー: すぐにカスタマイズできる強化ポリシーにより、サーバーへの侵入やサーバーの危殆化に速やかに対応。 - きめ細かい侵入防止ポリシー: アクセス制御機能によって未承認プロセスの実行の禁止し、承認されたアプリケーションのプロセスであったも所定の動作に制限して未知の脅威の実行を阻止。 - ファイル、システム、および管理者のロック: 物理サーバーと仮想サーバーを要塞化してシステムの稼働時間を最大化し、レガシー OS のサポートコストを低減。 - 幅広い物理プラットフォームへの対応: Windows ベースおよび Solaris、Linux、AIX、HP-UX などの 非 Windows ベースのプラットフォームを監視して保護。また、Virtual Agents を活用し、非対応のプラットフォームや一般的でないプラットフォームに対応。 - vSphere の保護と監視: 最新の vSphere 強化ガイドラインに基づいて作

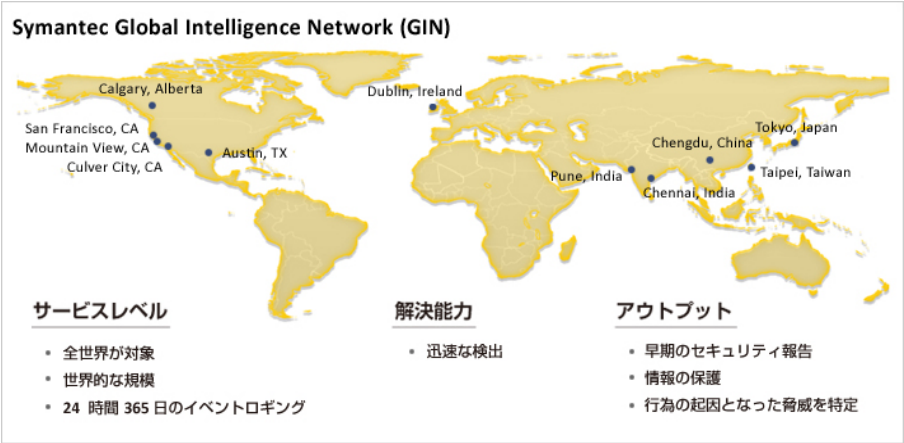
	成されたすぐに使えるポリシーを利用して、管理サーバー、ハイパーバイザ、ゲストにおいて環境を総合的に保護。 - 集中管理: イベントのリアルタイム表示およびグラフィカルなレポート機能により、ヘテロジニアスなシステムの管理を簡素化。 参照URL: http://www.symantec.com/ja/jp/critical-system-protection
侵入検知・防御技術(平成21年)	Symantec Web Gatewayとして製品化 Symantec Web Gateway は、仮想アプライアンスまたは物理ハードウェアによって提供され、ウェブによって運ばれる複数のタイプのマルウェアから組織を保護します。 製品の特徴は下記の通りです。 - Web コンテンツフィルタリングソフトウェアは、リアルタイムで更新されるシマンテックのグローバルインテリジェンスネットワークにより、強力な保護機能を提供 - シマンテックの数々の賞に輝くウイルス対策エンジンを統合 - 未知の脅威、標的型の脅威、または変異し続ける脅威をプロアクティブに防止するシマンテック インサイトを搭載 参照URL: http://www.symantec.com/ja/jp/web-gateway
侵入検知・防御技術(平成22年)	Symantec Messaging Gateway powered by Brightmailとして製品化 Symantec Messaging Gateway powered by Brightmail は、効果的で正確なリアルタイムのスパム対策とウイルス対策、先進のコンテンツフィルタリング、情報漏えい対策を統合することによって、メッセージの送受信を保護します。 製品の特徴は下記の通りです。 - メッセージや添付ファイルに含まれる企業データにフィンガープリントを付与し識別する機能によって重要な顧客データや企業の機密情報を保護 - Symantec Messaging Gateway に組み込まれた先進のスパムフィルタリング機能のほか、情報漏えい防止ポリシーを活用し、情報漏えい対策製品やメールの暗号化製品との効果的な連携が可能 - ダッシュボード、エグゼクティブサマリー、詳細かつ包

	括的なレポート機能によって、脅威の傾向や潜在的なコンプライアンスの問題をプロアクティブに突き止め、スパム対策ゲートウェイの効果と効力を立証 - 複数コンソールの管理、多様なポリシー設定、ログおよびレポートの矛盾による複雑さをなくすことで、メッセージセキュリティの効果と効力を立証し、管理コストを削減 - 仮想化環境のリソースを有効利用し、突発的なメール量の増大にも柔軟に対応できる、Symantec Messaging Gateway Virtual Edition は、 VMware ハイパーバイザ上で動作可能 参照URL：http://www.symantec.com/ja/jp/messaging-gateway
ぜい弱性対策技術（平成21年）	Endpoint Management powered by Altirisとして製品化 Endpoint Managementは、エンドポイントとシステムのすべての管理操作を最適化して、迅速にコスト削減と組織の効率化を実現します。コンピューティングインフラ全体とスマートフォン、タブレット、ノート PC、デスクトップ PC を含むクライアントデバイスのすべてを、シマンテックの統一されたエンドポイント管理およびセキュリティポートフォリオによって標準化するとともに、すべての導入、有効化、管理を一カ所で実現します。 参照URL： http://www.symantec.com/ja/jp/products-solutions/families/?fid=endpoint-management
ぜい弱性対策技術（平成21年）	Control Compliance Suiteとして製品化 Symantec Control Compliance Suite は、IT ガバナンス、リスク、コンプライアンス（GRC）プログラムを構築する強固なフレームワークを提供することによって、今日の複雑な IT リスクやコンプライアンスの課題に対処します。 Control Compliance Suite により、ビジネスに関連した表現で IT リスクを知らせ、総合的なリスク分析に基づいて修正作業に優先順位を付け、セキュリティとコンプライアンスに関する総合的な態勢を改善するための評価プロセスを自動化することができます。 Control Compliance Suite は、以下に示す 4 段階のプロセスで IT リスクと IT コンプライアンスの管理の面における課題に対処します。 計画：ビジネス面および IT セキュリティ面での目標を定義

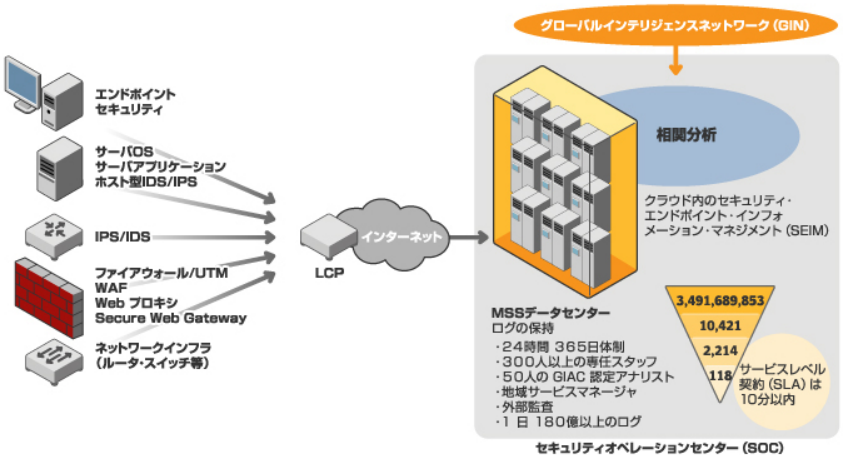
	します。外部の規制およびベストプラクティスの枠組みを順守するポリシーを作成します。余分な作業を回避するために、複数の要件に関連する制御にポリシーをマップします。 評価：目的とする基準や制御に照らして、効果を評価します。ポリシー違反と脆弱性を特定します。ポリシーがどの程度順守されているかを評価します。より詳細な全体像を得るために、シマンテックの他のソリューションやシマンテック以外のソリューションのデータを取り込みます。IT リスクの「総合的な分析」を可能にするために、データを一元的に管理します。 レポート：Web ベースのダッシュボードとレポート機能により、アクションと説明責任を促進します。経営幹部、各部門のリーダー、監査部門、IT 運用部門と、対象ユーザーに合わせてダッシュボードをカスタマイズします。ビジネスに関連した表現で IT リスクを可視化し、計画されている修正作業の影響を経時的にモデル化します。 修正：技術的な重大度ではなく、ビジネスにおける重要度に基づいて、修正作業に優先順位を付けます。IT に関する緊急性の最も高い問題に迅速に対処できるよう、Symantec Workflow を利用して、修正チケットの発行を自動化します。 参照URL： http://www.symantec.com/ja/jp/control-compliance-suite
高度認証技術 （平成23年）	Symantec O3として製品・サービス化 クラウドサービス使用に際して接続者および接続先、そして、接続内容を監視・管理するゲートウェイサービスです。 ゲートウェイは仮想サーバもしくはクラウドベースのサービスとして提供され、利用者は自組織の環境に合わせたサービス形態を選択できます。また、Active DirectoryやLDAPサーバとの連携機能も備え、組織のセキュリティポリシーに合わせた運用を容易にしております。 参照URL：http://www.symantec.com/symantec-o3

高度認証技術 （平成24年）	Symantec Validation & ID Protection（VIP）としてサービス化 Symantec Validation & ID Protection（VIP）は、クラウド型の認証サービスです。ワンタイムパスワードトークンにより生成される一回限り有効な使い捨てパスワードを使用するワンタイムパスワード認証、および、使用しているデバイスや行動プロファイルに基づいたリスク分析をバックグランドで実行して世紀のユーザか否かを判別するリスクベース認証の2通りの認証方式を備え、コスト・利便性・セキュリティのバランスに応じた最適な認証方式を提供します。 サービスの概要は下記の図を参照ください。  参照URL：https://www.verisign.co.jp/vip/
高度認証技術 （平成24年）	Symantec Managed PKI Serviceとしてサービス化 Symantec Managed PKI Serviceは、クラウドタイプの認証局構築サービスです。幅広い構築と運用実績を持つSymantecの発行局から、お客様独自のブランドまたはSymantecブランドの電子証明書を発行します。 サービスの概要は下記の図を参照ください。

<table>
<tr>
<td></td>
<td> 

参照URL：https://www.verisign.co.jp/mpki8/</td>
</tr>
<tr>
<td>インシデント分析技術（平成21年）</td>
<td>Global Intelligence Networkとして運用
Global Intelligence Networkでは、世界の200カ国を超える24万以上のセンサーから、5-10分間隔で情報を収集して分析することで、脆弱性や攻撃の情報をリアルタイムに把握して顧客の被害を最小限に留めます。情報の分析には、日本を含む世界11か所のセキュリティレスポンスセンターが従事し、24時間365日体制で従事しております。
セキュリティレスポンスセンターの配置は下記の通り。
 

参照URL：</td>
</tr>
</table>

	http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_4ste
インシデント分析技術（平成22年）	Managed Security Serviceとしてサービス化 Managed Security Serviceにおいては、受託元のシステムを24時間体制で監視してインシデント発生時に即時で分析します。平成24年末現在で、全世界5か所のセキュリティオペレーションセンターより1200社以上の顧客の合計70万台以上のデバイスを監視しております。また、解析するログは1日180億行以上に上ります。 サービスの仕組みは下記の通りです。  参考URL： http://www.symantec.com/ja/jp/theme.jsp?themeid=TokyoSOC_mss
不正プログラム対策技術（平成23年）	Symantec Protection Engineとして製品化 Symantec Protection Engineは、製品やサービスに組み込み可能な不正プログラム検出・除去機能モジュールです。 主要な機能は下記の通りです。 - ウイルス、マルウェア、スパイウェア、ワーム、トロイの木馬を検出する高性能スキャン機能を提供。 - ICAP でサードパーティ製の NAS デバイスと統合。 - HTML での参照や CSV 形式へのエクスポートが可能な統計レポートおよび詳細アクティビティレポートを作成。 - リソースの使用状況がわかる消費レポートを作成。 - アラート機能が向上し、一定数のイベントが発生した場合に電子メールまたは SNMP アラートでイベントトリガを送信。 - 集中検疫機能によって、管理者は、潜在的な脅威を集中

	管理サーバーの安全な領域に移行。 - ログ機能でイベントの詳細をキャプチャ。 参考URL: http://www.symantec.com/ja/jp/protection-engine-network-attached-storage
不正プログラム対策技術（平成22年）	Symantec Endpoint Protectionとして製品化 Symantec Endpoint Protection は、Symantec Insightと SONARという新世代の検出テクノロジを搭載。Symantec Insightは、ソフトウェアの作成者やインターネット上の普及状況などの要素からソフトウェアの安全性を評価し、SONARは約1400のプロセスの挙動を分析してマルウェアを検知します。 仮想環境では、VMware vShield Endpoint に対応し、物理マシン以上のパフォーマンスを発揮できます。 参考URL： http://www.symantec.com/ja/jp/endpoint-protection

（別添３）

ア　大学

企業・大学名	神奈川工科大学　岡本学研究室
代表者名	岡本　学
所在地	〒243-0292　神奈川県厚木市下荻野1030　Ｎ科ＫＩ-901
関連部署／電話番号	(046)291-3133
関連部門名	神奈川工科大学
ホームページのURL	http://nmana.kanagawa-it.ac.jp
研究説明のURL	nmana.kanagawa-it.ac.jp/about/about_lab.html
対象技術	研究開発状況
研究開発名称： 　足あと方式によるフィッシング防止 研究開発国： 　日本 研究開発期間： 　平成23年4月1日 ～	ＳＣＩＳ２０１２(日本の学会)にて「足跡共有サイトによるフィッシング防止」を発表。Ｓｏｕｐｓ２０１２(国際会議、アメリカ、査定あり)「Ａｎｔｉ－ｐｈｉｓｈｉｎｇ　ｓｙｓｔｅｍ　ｕｓｉｎｇ　ｆｏｏｔｐｒｉｎｔ－ｓｈａｒｉｎｇ　ｗｅｂｓｉｔｅ」を発表。今後、より実サービスに近い方式を提案する。

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	熊本大学総合情報基盤センター　武藏研究室
代表者名	武藏　泰雄
所在地	〒860-8555　熊本市中央区黒髪2-39-1
関連部署／電話番号	総合情報基盤センター／(096)342-3824
ホームページのURL	http://www.cc.kumamoto-u.ac.jp
製品説明のURL	www.cc.kumamoto-u.ac.jp/~musashi/
対象技術	技術の概要・特徴など
製品名： 　ＳＳＨ辞書攻撃検知プログラム 開発元： 　熊本大学総合情報基盤センター　武藏研究室 開発国： 　日本 価格： 発売時期： 出荷数： 	ＳＳＨサーバに対する辞書攻撃を検知することができるシステムである。検知モデルは以下のとおりである。 ・ＳＳＨサーバから発信される逆引きドメイン名名前解決通信量を監視する。 ・一定の期間の通信量が閾値を越えた時点で検知候補リストに入れる。 ・クエリキーワードに含まれるＩＰアドレスのユークリッド距離を測定し、０であれば検知とする。ここで検知されたクエリＩＰがＳＳＨ攻撃元のＩＰアドレスとなる。 ・また、攻撃先も同時に得られる。 ・組織内のＳＳＨサーバがどのように攻撃されるか時系列的に判る。

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	熊本大学総合情報基盤センター　武藏研究室
代表者名	武藏　泰雄
所在地	〒860-8555　熊本市中央区黒髪2-39-1
関連部署／電話番号	総合情報基盤センター／(096)342-3824
関連部門名	熊本大学総合情報基盤センター　武藏研究室
ホームページのURL	http://www.cc.kumamoto-u.ac.jp
研究説明のURL	www.cc.kumamoto-u.ac.jp/~musashi/
対象技術	研究開発状況
研究開発名称： ＤＮＳサーバに対するＡＰＴ攻撃検知システム 研究開発国： 日本 研究開発期間： 平成20年4月1日 ～平成25年3月31日	ＤＮＳ通信量とＤＮＳクエリに含まれるクエリキーワードを監視し、ネットワークに対する事業調査活動やＤＮＳサーバに対するＤｏＳ攻撃を検知して阻止するシステムである。既存ＩＰＳと連携して攻撃を阻止できるシステムを開発中である。

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	玉川大学　工学部
代表者名	小野　道照
所在地	〒194-8610　東京都町田市玉川学園6-1-1
関連部署／電話番号	工学部事務室／(042)739-8861
関連部門名	
ホームページのURL	http://www.tamagawa.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 量子暗号鍵配送の実用化に関する研究 研究開発国： 日本 研究開発期間： 平成17年8月1日 ～	コヒーレントパルス一変調方式を用いた光通信量子暗号の具体的な信号形式およびその信号の発生装置を提案した。さらに、提案した信号系の基本的な性質を調査した。研究成果は、国際会議(ＮＣＳＰ2010、ＮＣＳＰ2011)および学術論文誌(Ｊｏｕｒｎａｌ　ｏｆ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｉｎｇ、2011)で報告した。量子暗号鍵配送で共有した乱数系列(暗号鍵の種)に含まれる誤りを訂正する手法にＣａｓｃａｄｅと呼ばれる対話型プロトコルがある。Ｃａｓｃａｄｅ　プロトコルは公開する情報が少ないという長所を有するが通信回数が多く、系列の長さとともに処理時間が増加する問題を国際会議(ＱＣＭＣ2006)で指摘した。その問題を解決するためにパラレル処理を導入することで通信回数を大幅に削減し、系列長が増加しても通信回数がほとんど影響を受けない方式を提案し、計算機シミュレーション結果を国内学会(2011電子情報通信学会総合大会)で報告している。

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	東洋大学
代表者名	理工学部長　吉田　泰彦
所在地	埼玉県川越市鯨井2100
関連部署／電話番号	教学課　担当大野／(049)239-1769
関連部門名	東洋大学　理工学部
ホームページのURL	http://www.toyo.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 　パケットキャプチャ解析、分析技術 研究開発国： 　日本 研究開発期間： 　平成22年4月1日 ～平成27年3月31日	パケットキャプチャ解析を中心に情報通信ネットワーク、及び、無線ＬＡＮ等を流れる情報を分析する技術開発を中心とする

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	北海道情報大学
代表者名	中島　潤
所在地	〒069-8585　北海道江別市西野幌59番2
関連部署／電話番号	中島研究室／(011)385-4411
関連部門名	
ホームページのURL	http://www.do-johodai.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 超高速ＮＷ向けネットワークフォレンジックシステムの開発 研究開発国： 日本 研究開発期間： 平成21年4月～	40Ｇｉｇａｂｉｔあるいは100Ｇｉｇａｂｉｔ級の超高速ネットワークで通信されるトラフィックを補足・記録し、セキュリティインシデント発生時に、その状況や手口等を事後追跡可能なネットワーク・フォレンジック・システムを、民間記号との共同研究により開発中である。

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	立命館大学理工学部　電子情報工学科
代表者名	(藤野　毅)
所在地	〒525-8577　滋賀県草津市野路東1-1-1
関連部署／電話番号	
関連部門名	耐タンパ暗号ＬＳＩ及び偽造防止認証技術
ホームページのURL	
研究説明のURL	www.dvlsi.jst.go.jp/list/h21-03.html
対象技術	研究開発状況
研究開発名称： ＪＳＴ(ＣＲＥＳＴ)のデイペンタブルＶＬＳＩシステムの基盤技術で開発 研究開発国： 研究開発期間： 平成21年9月～平成27年3月	耐タンパ暗号回路：試作チップ動作検証確認　偽造防止ＬＳＩ：試作チップ動作検証確認＋デモシステム開発完了

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	国立大学法人　琉球大学工学部
代表者名	工学部長　高良　富夫
所在地	〒903-0213　沖縄県中頭郡西原町字千原1番地
関連部署／電話番号	琉球大学工学部　総務係／(098)895-8589
関連部門名	工学部情報工学科　長田研究室
ホームページのURL	http://www.tec.u-ryukyu.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 　トラストフレームワークモデルによるＩＤ関連の信頼性向上(他) 研究開発国： 　日本 研究開発期間： 　平成20年4月～平成24年12月(継続中)	トラストフレームワークモデルをＯｐｅｎＩＤに通用するための技術は、特許出願中(特願2012-101684)である。現在、関連技術としてＩＤ連携において、多様な属性情報を利用した柔軟な認証(許可)技術を検討中である。特許出願中の技術を含めて、２社ほど問い合わせがあり、実用化に向けたアプリケーション(応用)についても検討中である。

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	○

イ　企業

企業・大学名	沖電気工業株式会社　研究開発センタ
代表者名	
所在地	〒335-8510　埼玉県蕨市中央1丁目16-8
関連部署／電話番号	(048)420-7070
関連部門名	
ホームページのURL	www.oki.com/jp/
研究説明のURL	www.oki.com/jp/press/2012/12/z12106_3.pdf
対象技術	研究開発状況
研究開発名称： 省電力マルチホップＮＷ向け暗号通信路確立代行技術 研究開発国： 日本 研究開発期間： 平成23年7月1日～現在	センサ機器とインターネット上の任意の装置間で暗号通信路を確立するもの。通信監理サーバが処理を代行することにより無線マルチホップネットワークを流れる通信量を削減する。Ｉｐｖ６対応９２０ＭＨｚ帯省電力無線機２０台、ゲートウェイ装置１台の構成で実証実験を実施。実験結果から通信量を30～40%に削減し、省電力効果を得られることを確認した。

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	沖電気工業株式会社　研究開発センタ
代表者名	
所在地	〒335-8510　埼玉県蕨市中央1丁目16-8
関連部署／電話番号	(048)420-7070
関連部門名	
ホームページのURL	www.oki.com/jp/
研究説明のURL	www.oki.com/jp/press/2012/02/z11104.html
対象技術	研究開発状況
研究開発名称： 　量子暗号システム 研究開発国： 　日本 研究開発期間： 　平成23年4月1日～(実施中)	量子暗号発生に必要な光源の基盤技術を開発。これまでの光源に比べ、小形、低電力、常温動作可能なことを実証。

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	キーウェアソリューションズ株式会社
代表者名	三田　昌弘
所在地	〒156-8588　東京都世田谷区上北沢5-37-18
関連部署／電話番号	経営企画室　ＩＲ部／(03)3290-1111
ホームページのURL	www.keyware.co.jp
製品説明のURL	www.keyware.co.jp/info/press/press121210.html
対象技術	技術の概要・特徴など
製品名： 　セキュアカーテン 開発元： 　キーウェアソリューションズ株式会社 開発国： 　日本 価格： 発売時期： 　平成24年12月10日 出荷数：	スマートフォン情報漏えい防止 ・不正Ｗｉ－Ｆｉ接続防止 ・のぞき見防止 ・画面情報流出防止

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	ソースネクスト株式会社
代表者名	松田　憲幸
所在地	〒105-0001　東京都港区虎ノ門3-8-21　虎ノ門33森ビル6F
関連部署／電話番号	
ホームページのURL	http://www.sourcenext.com
製品説明のURL	www.sourcenext.com/product/bd/home
対象技術	技術の概要・特徴など
製品名： スーパーセキュリティＺＥＲＯ 開発元： Ｂｉｔｄｅｆｅｎｄｅｒ 開発国： ルーマニア 価格： 3970円 発売時期： 平成23年12月22日 出荷数： 17万本	ＡＶ－ＴＥＳＴで「Ｎｏ．１ウイルス対策エンジン」と認証されたビットディフェンダーのエンジン※の最新版を使用したＷｉｎｄｏｗｓパソコン向けの総合セキュリティ対策製品。マルウェア検知ではシグネチャマッチングに加え、仮想環境でのふるまい検査(Ｂ－Ｈａｖｅエンジン)、実環境でのふるまい監視(ＡＶＣエンジン)など複数技術を組み合わせて高い検知率を持っている。　その他、中間者攻撃・ＭＩＴＢ攻撃・フィッシングなど決済を狙った攻撃をクライアントサイドで防ぐ「決済ブラウザ」や、ウイルスサイトからの被害を防止する「仮想ブラウザ」、Ｆａｃｅｂｏｏｋ保護機能などを搭載している。

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	日本電気株式会社　中央研究所
代表者名	
所在地	〒211-8660　川崎市中原区下沼部1753
関連部署／電話番号	http://www.nec.co.jp/rd/
ホームページのURL	www.nec.co.jp/soft/sg/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 　ＳＧ3600シリーズ 開発元： 　ＮＥＣ 開発国： 　日本 価格： 　85万円～ 発売時期： 　平成15年7月 出荷数： 　約600台	(概要)ＮＥＣ独自のエンジンを搭載したファイアウォール製品。 (特徴)・ファイアウォール機能と連携したＶＰＮ機能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、別途サーバによる導入が不要　・二重化機能により、万が一の場合、待機系のファイアウォールに自動的に切り換えるため、止まらないファイアウォールシステムを提供。

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　中央研究所
代表者名	
所在地	〒211-8660　川崎市中原区下沼部1753
関連部署／電話番号	
ホームページのURL	http://www.nec.co.jp/rd/
製品説明のURL	www.nec.co.jp/cced/infocage
対象技術	技術の概要・特徴など
製品名： 　ＩｎｆｏＣａｇｅ 開発元： 　ＮＥＣ 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、情報漏洩を防止。・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し、攻撃とみなしたアクセスをブロックし、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、情報漏洩やウィ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、ウィ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　中央研究所
代表者名	
所在地	〒211-8660　川崎市中原区下沼部1753
関連部署／電話番号	
ホームページのURL	http://www.nec.co.jp/rd/
製品説明のURL	www.nec.co.jp/cced/GUARDIANWALL/
対象技術	技術の概要・特徴など
製品名： ＧＵＡＲＤＩＡＮＷＡＬＬ 開発元： キャノンＩＴソリューションズ株式会社 開発国： 日本 価格： ライセンス：９６万円～　保守：１４．４万円/年～ 発売時期： 平成12年6月 出荷数： 2000社	「ＧＵＡＲＤＩＡＮＷＡＬＬ」は、個人情報や機密情報の漏えいを防ぐメールフィルタリングソフトです。　ＧＵＡＲＤＩＡＮＷＡＬＬは下記のような課題を解決します。・個人情報を含むメールを禁止したい・決められたドメインやメールアドレス以外へのメール送信を禁止したい。・誤送信しないよう送信者に再確認させたい。・「社外秘」や「機密情報」といった言葉を含むメールは必ず上司にＣＣしたい。・部下のメールは上司がチェックしてから送信したい。・もしものときのために添付ファイルは暗号化しておきたい。

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	日本電気株式会社　中央研究所
代表者名	
所在地	〒211-8660　川崎市中原区下沼部1753
関連部署／電話番号	
ホームページのURL	http://www.nec.co.jp/rd/
製品説明のURL	www.nec.co.jp/middle/WebSAM/products/secmaster/index.html
対象技術	技術の概要・特徴など
製品名： 　ＳＥＣＵＲＥＭＡＳＴＥＲ 開発元： 　日本電気株式会社 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11年 出荷数： 　約１０００システム	(概要)ＷｅｂＳＡＭ　ＳＥＣＵＲＥＭＡＳＴＥＲ(ウェブサム　セキュアマスター)は、複数の業務システムのＩＤ情報や認証・認可情報の統合管理、および企業内システムやクラウドサービスへのシングルサインオンを実現する製品です。　ＳＥＣＵＲＥＭＡＳＴＥＲ導入により、ユーザ情報の管理コストを削減し、セキュアなＩＤ・権限管理を実現します。また、シングルサインオンにより利用者の利便性を向上し、業務効率を改善します。

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	日本電気株式会社　中央研究所
代表者名	
所在地	〒211-8660　川崎市中原区下沼部1753
関連部署／電話番号	
関連部門名	
ホームページのURL	http://www.nec.co.jp/rd/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 　総合アクセス制御 研究開発国： 　日本 研究開発期間： 　平成19年4月1日 ～平成25年3月31日	仮想化されたＩＴサーバ、クライアントＰＣ端末内のアクセス制御機能を、単一のアクセスポリシーをベースに一括自動制御する技術の開発を2010年度に開発完了。アクセス制御対象をネットワークに拡大し、ＯｐｅｎＦｌｏｗを活用した自動制御技術の開発を2012年度に完了予定。

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	富士通株式会社
代表者名	
所在地	
関連部署／電話番号	
ホームページのURL	http://.jp.fujitsu.com/
製品説明のURL	fenics.fujutsu.com/products/ipcom/products/lineup/ipcom_es_sc.html
対象技術	技術の概要・特徴など
製品名： ＩＰＣＯＭ　ＥＸ　ＳＣシリーズ 開発元： 富士通株式会社 開発国： 日本 価格： ５８万円～ 発売時期： 平成18年10月 出荷数：	・様々な脅威に対処し、システムを保護 ステートフル・インスペクションや、アプリケーションレベルのフィルタリング、アノマリ型のＩＰＳ、シグネチャに基づくアンチウイルス、Ｗｅｂコンテンツフィルタリングなどの機能を搭載しています。ＤｏＳ/ＤＤｏＳ攻撃、ウイルス、Ｐ２Ｐアプリケーションなどのさまざまな脅威に対応できるため、強固なセキュリティを実現します。 ・安全なリモートアクセスを実現 ＶＰＮ機能により、インターネットを利用した場合でも秘匿性の高い安全な通信が可能です。更に、アンチウイルス機能との組み合わせにより、ＶＰＮ通信でのウイルス対策が可能です。ＩＰＣＯＭＥＸシリーズはＩＰｓｅｃ－ＶＰＮとＳＳＬ－ＶＰＮ、Ｌ２ＴＰ/ＩＰｓｅｃに対応しているため、事業間アクセスにはＩＰｓｅｃ－ＶＰＮ、リモートアクセスにはＳＳＬ－ＶＰＮ、またはＬ２ＴＰ/ＩＰｓｅｃといった使い分けも可能です。 ・次世代ファイアーウォール アプリケーション辞書を使ったアプリケーション通信の制御で、幅広い脅威に対するネットワークセキュリティの強化を実現。

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	１ｓｔホールディングス株式会社
代表者名	内野　弘幸
所在地	〒150-0031　東京都渋谷区桜丘町20-1渋谷インフォスタワー14Ｆ
関連部署／電話番号	情報システム部／(03)5962-7400
ホームページのURL	http://www.1st-hd.com
製品説明のURL	http://www.variosecure.net/service/mns.html
対象技術	技術の概要・特徴など
製品名： 　マネージドセキュリティサービスゲートウェイセキュリティ 開発元： 　バリオ　セキュア・ネットワークス株式会社 開発国： 　日本 価格： 　オプション設定によってことなります 発売時期： 　平成14年5月 出荷数： 　3400	独自開発したルータをお客様の社内に設置し、各種ネットワーク関連のセキュリティポリシーを設定することで、社内システムを外部の脅威から統合的に管理する。リモート監視と保守がセットになっている。（上記製品説明のＵＲＬを参照）。

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	