

平成25年3月28日
国家公安委員会
総務大臣
経済産業大臣

不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況

1 趣旨

不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）第10条第1項の規定に基づき、国家公安委員会、総務大臣及び経済産業大臣は、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表する。

参考：不正アクセス禁止法（抜粋）

第10条 国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。

3 前2項に定めるもののほか、国は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

2 公表内容

不正アクセス行為の発生状況

平成24年1月1日から12月31日までの不正アクセス行為の発生状況を公表する。

アクセス制御機能に関する技術の研究開発の状況

国家公安委員会、総務省又は経済産業省のいずれかに係るアクセス制御機能の研究開発の状況、募集・調査した民間企業等におけるアクセス制御機能の研究開発の状況をそれぞれ公表する。

3 掲載先

国家公安委員会ホームページ <http://www.npsc.go.jp/>

総務省ホームページ http://www.soumu.go.jp/joho_tsusin/security/security.html

経済産業省ホームページ <http://www.meti.go.jp/policy/netsecurity/index.html>

不正アクセス行為の発生状況

第1 平成24年中の不正アクセス禁止法違反事件の認知・検挙状況等について

平成24年中に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

1 不正アクセス行為の認知状況

(1) 認知件数

平成24年中の不正アクセス行為の認知件数^{注1}は1,251件で、前年と比べ、362件増加した。

表1 - 1 不正アクセス行為の認知件数の推移

区分	年次	平成20年	平成21年	平成22年	平成23年	平成24年
認知件数		2,289	2,795	1,885	889	1,251
	海外からのアクセス	214	40	57	110	122
	国内からのアクセス	1,993	2,673	1,755	678	987
	アクセス元不明	82	82	73	101	142

(参考)「連続自動入力プログラムによる不正ログイン攻撃^{注2}」による不正アクセス行為
不正アクセス行為については、表1 - 1の記載とは別に、一部の事業者から都道府県警察が新たに提供を受けることとした資料により、平成24年5月以降、114,013件の「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為が報告された。

注1 ここでいう認知件数とは、不正アクセス被害の届出を受理した場合のほか、余罪として確認した場合、報道を踏まえて確認した場合、援助の申出を受理した場合、その他関係資料により不正アクセス行為の事実確認ができた場合において、被疑者が行った構成要件に該当する行為の数をいう。なお、本文「(参考)」として記載の連続自動入力プログラムによる不正ログイン攻撃については、ID・パスワードの正規利用者に対する確認を行っていないことから、従来の認知件数と同様の不正アクセス行為の事実確認ができた場合とまではいえず、別に記載した。

注2 連続自動入力プログラムによる不正ログイン攻撃とは、インターネット利用者の多くが複数サイトで同一のID・パスワードを使い回している状況に目を付け、不正取得した他人のID・パスワードのリストを悪用して、連続自動入力プログラムを用いてID・パスワードを入力し、不正アクセス行為を敢行する手口の攻撃をいう。

- (2) 被害に係る特定電子計算機のアクセス管理者^{注3}
 被害に係る特定電子計算機のアクセス管理者をみると、一般企業が最も多く（1,163件）次いで行政機関（52件）となっている。

表1 - 2 被害を受けた特定電子計算機のアクセス管理者の推移

区分 \ 年次	平成 20年	平成 21年	平成 22年	平成 23年	平成 24年
一般企業	685	466	457	762	1,163
プロバイダ	1,589	2,321	1,405	115	22
大学、研究機関等	5	4	2	1	12
その他	10	4	21	11	54
うち行政機関	6	3	13	6	52
不明	0	0	0	0	0
計	2,289	2,795	1,885	889	1,251

「プロバイダ」とは、インターネットに接続する機能を提供する電気通信事業者をいう。

「大学、研究機関等」には、高等学校等の学校機関を含む。

「その他」の「うち行政機関」には、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。

- (3) 認知の端緒

認知の端緒としては、利用権者^{注4}からの届出によるものが最も多く（892件）次いで警察職員による被疑者の取調べ等の警察活動によるもの（270件）被害を受けた特定電子計算機のアクセス管理者からの届出によるもの（80件）発見者からの通報によるもの（5件）の順となっている。

表1 - 3 認知の端緒の推移

区分 \ 年次	平成 20年	平成 21年	平成 22年	平成 23年	平成 24年
利用権者からの届出	656	487	314	680	892
警察活動	1,567	2,277	1,488	75	270
アクセス管理者からの届出	60	21	66	121	80
発見者からの通報	4	7	9	7	5
その他	2	3	8	6	4
計	2,289	2,795	1,885	889	1,251

注3 特定電子計算機とは、ネットワークに接続されたコンピュータをいい、アクセス管理者とは、特定電子計算機を誰に利用させるかを決定する者をいう。例えば、インターネットへの接続や電子メールの受信についてはプロバイダが、インターネットショッピング用のホームページの閲覧についてはその経営者が、それぞれアクセス管理者となる。

注4 利用権者とは、特定電子計算機をネットワークを通じて利用することについて、当該特定電子計算機のアクセス管理者の許諾を得た者をいう。例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や企業からLANを利用することを認められた社員が該当する。

(4) 不正アクセス行為後の行為

不正アクセス行為後の行為としては、オンラインゲーム、コミュニティサイトの不正操作（他人のアイテムの不正取得等）が最も多く（662件）、次いでインターネットショッピングの不正購入（223件）、情報の不正入手（99件）、インターネットバンキングの不正送金（95件）、ホームページの改ざん・消去（42件）、インターネット・オークションの不正操作（他人になりすましての出品・落札）（29件）、不正ファイルの蔵置（1件）の順となっている。

表1 - 4 不正アクセス行為後の行為の内訳

区分	年次	平成23年	平成24年
オンラインゲーム、コミュニティサイトの不正操作		358	662
インターネットショッピングの不正購入		172	223
情報の不正入手		74	99
インターネットバンキングの不正送金		188	95
ホームページの改ざん・消去		28	42
インターネット・オークションの不正操作		22	29
不正ファイルの蔵置		4	1
その他		43	100

2 不正アクセス禁止法違反事件の検挙状況

(1) 検挙件数等

平成24年中における不正アクセス禁止法違反の検挙件数は543件、検挙人員は154人と、前年と比べ、検挙件数は295件増加し、検挙人員は40人増加した。その内訳をみると、不正アクセス行為に係るものがそれぞれ533件、151人、識別符号提供行為^{注5}に係るものがそれぞれ4件、4人であったほか、平成24年5月1日に施行された不正アクセス行為の禁止等に関する法律の一部を改正する法律（平成24年法律第12号）により新設された罪については、識別符号の取得行為^{注6}が2件、2人、識別符号の保管行為^{注7}が2件、2人、フィッシング行為^{注8}が2件、1人であった。

表 2 - 1 検挙件数等の推移

区分		年次	平成 20年	平成 21年	平成 22年	平成 23年	平成 24年
不正アクセス 行為	検挙件数		1,737	2,532	1,598	242	533
	検挙事件数 ^{注9}		101	95	103	101	133
	検挙人員		135	114	123	110	151
識別符号 提供（助長）行為	検挙件数		3	2	3	6	4
	検挙事件数		3	1	3	6	4
	検挙人員		3	1	4	6	4
識別符号 取得行為	検挙件数						2
	検挙事件数						2
	検挙人員						2
識別符号 保管行為	検挙件数						2
	検挙事件数						2
	検挙人員						2
フィッシング 行為	検挙件数						2
	検挙事件数						1
	検挙人員						1
計	検挙件数 （件）		1,740	2,534	1,601	248	543
	検挙事件数 （事件）		101 （重複3）	95 （重複1）	104 （重複2）	103 （重複4）	136 （重複6）
	検挙人員 （人）		137 （重複1）	114 （重複1）	125 （重複2）	114 （重複2）	154 （重複6）

（重複）とは、各行為の重複を示す。

注5 他人の識別符号をアクセス管理者や利用権者に無断で第三者に提供する行為をいう。

注6 不正アクセスの目的で他人の識別符号を取得する行為をいう。

注7 不正アクセスの目的で他人の識別符号を保管する行為をいう。

注8 アクセス管理者になりすまし、当該アクセス制御機能にかかる識別符号の入力を求める行為をいう。いわゆるフィッシングサイトを公衆が閲覧できる状態に置く行為等。

注9 事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は1事件と数える。

(2) 不正アクセス行為の態様

検挙件数を不正アクセス行為の態様別にみると、識別符号窃用型^{注10}が532件であり、セキュリティ・ホール攻撃型^{注11}は1件であった。

表 2 - 2 不正アクセス行為の態様の推移

区分		年次				
		平成 20年	平成 21年	平成 22年	平成 23年	平成 24年
識別符号窃用型	検挙件数	1,736	2,529	1,597	241	532
	検挙事件数	100	94	102	100	133
セキュリティ・ ホール攻撃型	検挙件数	1	3	1	1	1
	検挙事件数	1	1	1	1	1
計	検挙件数 (件)	1,737	2,532	1,598	242	533
	検挙事件数 (事件)	101	95	103	101	133 (重複1)

3 検挙事件の特徴

(1) 不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る不正アクセス行為の手口についてみると、言葉巧みに利用権者から聞き出した又はのぞき見たものが最も多く(229件)、次いで利用権者のパスワードの設定・管理の甘さにつけ込んだもの(122件)となっている。また、識別符号を知り得る立場にあった元従業員や知人等によるもの(101件)、スパイウェア等のプログラムを使用して識別符号を入手したもの(29件)、共犯者等から入手したもの(22件)、フィッシングサイトにより入手したもの(18件)等も依然として発生している。

注10 アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為(不正アクセス禁止法第2条第4項第1号に該当する行為)をいう。

注11 アクセス制御されているサーバに、ネットワークを通じて情報(他人の識別符号を入力する場合を除く。)や指令を入力して不正に利用する行為(不正アクセス禁止法第2条第4項第2号又は第3号に該当する行為)をいう。例えば、セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

表3 - 1 不正アクセス行為に係る犯行の手口の内訳

区分	年次	平成23年	平成24年
識別符号窃用型		241	532
	言葉巧みに利用権者から聞き出した又はのぞき見たもの	29	229
	利用権者のパスワードの設定・管理の甘さにつけ込んだもの	59	122
	識別符号を知り得る立場にあった元従業員や知人等によるもの	52	101
	スパイウェア ^{注12} 等のプログラムを使用して識別符号を入手したもの	1	29
	共犯者等から入手したもの	38	22
	フィッシングサイトにより入手したもの	59	18
	他人から購入したもの	0	0
	ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したもの	0	0
	その他	3	11
セキュリティ・ホール攻撃型		1	1

(2) 被疑者

不正アクセス禁止法違反に係る被疑者と識別符号を窃用された利用権者の関係についてみると、元交際相手や元従業員等の顔見知りの者によるものが最も多く（75人）、次いで交友関係のない他人によるもの（60人）、ネットワーク上の知り合いによるもの（19人）となっている。

また、被疑者の年齢についてみると、10歳代（64人）が最も多く、20歳代（34人）、40歳代（28人）、30歳代（21人）、50歳代（6人）及び60歳代（1人）の順となっている。

なお、最年少の者は14歳、最年長の者は65歳であった。

表3 - 2 年代別被疑者数の推移

区分 \ 年次	平成20年	平成21年	平成22年	平成23年	平成24年
10歳代 (人)	48	31	29	51	64
20歳代	42	33	39	30	34
30歳代	35	35	35	19	21
40歳代	11	13	17	10	28
50歳代	1	2	5	2	6
60歳代	0	0	0	2	1
計	137	114	125	114	154

注12 パソコン内のファイル又はキーボードの入力情報、表示画面の情報等を取り出して、漏えいさせる機能を持つプログラムをいう。

(3) 不正アクセス行為の動機

不正アクセス行為の動機としては、オンラインゲームやコミュニティサイトで不正操作を行うための最も多く（219件）、次いで嫌がらせや仕返しのため（100件）、好奇心を満たすため（85件）、不正に経済的利益を得るため（79件）の順となっている。

表3 - 3 不正アクセス行為の動機の内訳

区分	年次	平成23年	平成24年
オンラインゲームやコミュニティサイトで不正操作を行うため		39	219
嫌がらせや仕返しのため		58	100
好奇心を満たすため		32	85
不正に経済的利益を得るため		97	79
顧客データの収集等情報を不正に入手するため		15	38
料金の請求を免れるため		0	10
その他		1	2
計		242	533

(4) 利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（532件）について、当該識別符号を入力することにより利用されたサービスをみると、オンラインゲーム、コミュニティサイトが最も多く（318件）、次いで会員専用・社員用内部サイト（98件）、電子メール（44件）、インターネットバンキング（31件）、インターネットショッピング（28件）、ホームページ公開サービス（8件）、インターネット・オークション（5件）の順となっている。

表3 - 4 利用されたサービスの内訳

区分	年次	平成23年	平成24年
識別符号窃用型（件）		241	532
オンラインゲーム、コミュニティサイト		83	318
会員専用・社員用内部サイト		16	98
電子メール		23	44
インターネットバンキング		14	31
インターネットショッピング		87	28
ホームページ公開サービス		5	8
インターネット・オークション		4	5
その他		9	0

4 都道府県公安委員会による援助措置

平成24年中、不正アクセス禁止法第9条の規定に基づき、都道府県公安委員会がアクセス管理者に対して行った助言・指導はなかった。

表4-1 都道府県公安委員会の援助措置実施件数の推移

区分 \ 年次	平成20年	平成21年	平成22年	平成23年	平成24年
援助措置	1	0	0	0	0

5 防御上の留意事項

(1) 利用権者の講ずべき措置

ア フィッシングに対する注意

電子メールにより、本物のウェブサイトに酷似したフィッシングサイトに誘導したり、添付されたファイルを開かせたりして、ID・パスワードやクレジットカード情報を不正に取得する事案が多発していることから、発信元に心当たりのない電子メールに注意する。また、金融機関等が電子メールで口座番号や暗証番号、個人情報を問い合わせることはなく、これらの情報の入力を求める電子メールはフィッシングメールであると考えられることから、情報を入力しない。

イ パスワードの適切な設定・管理

言葉巧みに聞き出したID・パスワードによる不正アクセス行為、利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為が発生していることから、パスワードを設定する場合には、IDと全く同じパスワードやIDの一部を使ったパスワード等、パスワードの推測が容易なものは避ける、複数のサイトで同じパスワードを使用しないなどの対策を講じる。また、パスワードを他人に教えない、パスワードを定期的に変更するなど自己のパスワードを適切に管理する。

ウ 不正プログラムに対する注意

コンピュータに不正プログラムを感染させ、他人のID・パスワードを不正に取得する事案が発生していることから、信頼できない電子メールに添付されたファイルを不用意に開いたり、信頼できないウェブサイト上に蔵置されたファイルをダウンロードしたりしない。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、コンピュータ・ウイルス対策等の不正プログラム対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。

(2) アクセス管理者等の講ずべき措置

ア フィッシング等への対策

フィッシング等により不正に取得したID・パスワードを使用した不正アクセス行為が多発していることから、インターネットショッピング、オンラインゲーム、インターネットバンキング等のサービスを提供する事業者にとっては、ワンタイムパスワード^{注13}等により個人認証を強化するなどの対策を講ずる。

注13 インターネット銀行等における認証用のパスワードであって、認証の度にそれを構成する文字列が変わるものをいう。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

イ パスワードの適切な設定・運用体制の構築

利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為が多発していることから、アクセス管理者は、容易に推測されるパスワードを設定できないようにする、定期的にパスワードの変更を促す仕組みを構築する、複数のサイトで同じパスワードを使用することの危険性を周知するなどの措置を講ずる。

ウ ID・パスワードの適切な管理

ID・パスワードを知り得る立場にあった元従業員による不正アクセス行為も引き続き発生していることから、従業員が退職した時や特定電子計算機を利用する立場でなくなった時には、当該従業員に割り当てていたIDを削除したり、パスワードを変更したりするなど識別符号の適切な管理を徹底する。

エ セキュリティ・ホール攻撃への対応

セキュリティ・ホール攻撃の一つであるSQLインジェクション攻撃^{注14}を受け、クレジットカード番号等の個人情報が流出する事案や、Webサーバの脆弱性に対する攻撃を受け、ホームページが改ざんされる事案が発生していることから、アクセス管理者は、プログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するための侵入検知システム等を導入し、セキュリティ・ホール攻撃に対する監視体制を強化する。

6 検挙事例

1	サーバのセキュリティ・ホールを攻撃して不正アクセスを行い、記録されていた複数のID・パスワードを入手するとともに、これらをインターネット上の掲示板に投稿して他人に提供した不正アクセス禁止法違反事件
---	--

無職の少年（15）は、平成24年5月、無料ホームページサービスを提供するサーバのセキュリティ・ホールを攻撃して不正アクセスし、同サーバ内に記録されていた複数の会員のID・パスワードを不正に入手した上で、これらをハッカー仲間らが使用する掲示板に投稿して他人に提供した。平成24年6月、不正アクセス禁止法違反で検挙した（京都）。

2	他人が契約した無線LANを無断利用してインターネットに接続し、他人になりすましてメールサーバに不正アクセスした上で、嫌がらせメールを送信した不正アクセス禁止法違反事件
---	---

高校生の少年（17）は、平成23年10月、通学路付近の複数の無線LAN電波を無断利用してインターネットに接続のうえ、同級生が使用するメールアカウント用のID・パスワードを使用してメールサーバに不正アクセスした上で、同人に嫌がらせメールを送信した。平成24年7月、不正アクセス禁止法違反等で検挙した（警視庁）。

3	大手チケット販売サイトに他人のID・パスワードを使用して不正アクセスを行い、大量の観劇チケット等を不正に購入して換金した不正アクセス禁止法違反及び電子計算機使用詐欺事件
---	--

注14 SQLというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

無職の男（42）らは、平成24年1月から9月までの間、他人のIDからそのパスワードを推測して大手チケット販売サイトに不正アクセスを行い、利用権者があらかじめ登録していたクレジットカード情報を使用して観劇チケット等を大量に不正購入した上、チケットショップでこれを換金した。平成24年10月、不正アクセス禁止法違反及び電子計算機使用詐欺で検挙した（広島）。

4	大手コミュニティサイトのフィッシングサイトを海外サーバ上に構築し、複数の利用権者からID・パスワードを不正に取得した不正アクセス禁止法違反事件
---	--

中学生の少年（14）は、平成24年5月、大手コミュニティサイトのログイン画面に酷似したフィッシングサイトを海外のサーバに開設した上、自己が開設するブログに同フィッシングサイトに誘引する書き込みを投稿して、他人のID・パスワードを不正に要求した。平成24年12月、不正アクセス禁止法違反で検挙した（熊本）。

5	元勤務先のサーバに不正アクセスを行い、同サーバ内のブログデータを消去して同社の業務を妨害した不正アクセス禁止法違反及び電子計算機損壊等業務妨害事件
---	--

風俗店従業員の男（22）は、平成24年3月、元勤務先のホームページ管理用サーバに管理者用のID・パスワードを入力して不正アクセスを行い、同サーバに記憶・蔵置されていたブログデータを消去し、同社の業務を妨害した。平成24年6月、不正アクセス禁止法違反及び電子計算機損壊等業務妨害で検挙した（愛知）。

(参考) 不正アクセス関連行為の関係団体への届出状況について

独立行政法人情報処理推進機構 (IPA) に届出のあったコンピュータ不正アクセスの届出状況について

IPA では、不正アクセス被害の実態を把握し、その防止に関する啓発を行うため、情報産業、企業の情報部門、個人ユーザ等から、広くコンピュータ不正アクセスの被害情報の届出を受け付け、その被害状況、防止策を定期的に公表している。

1. 不正アクセスに関する届け出状況

(平成24年中にIPAに届出のあったコンピュータ不正アクセス(注1)が対象)

平成24年中のコンピュータ不正アクセスに関する届出件数は121件(平成23年:103件)であった。(注2)

平成24年は同23年と比べて、18件(約17%)増加した。

届出のうち実際に被害があったケースにおける被害内容の分類では、「侵入」及び「なりすまし」による被害届出が多く寄せられた。

以下に、種々の切り口で分類した結果を示す。

個々の件数には未遂(実際の被害はなかったもの)も含まれる。

また、1件の届出にて複数の項目に該当するものがあるため、それぞれの分類での総計件数はこの数字に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。総計は255件(平成23年:180件)あった。

1件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず

ア 不正アクセスによる侵入行為

侵入行為に係る攻撃等の届出は201件(平成23年:145件)あった。

(ア) 侵入の事前調査行為

システム情報の調査、稼働サービスの調査、アカウント名の調査等である。

6件の届出があり、ポートやセキュリティホールを探索するものであった。

(イ) 権限取得行為(侵入行為)

パスワード推測やソフトウェアのバグ等いわゆるセキュリティホールを利用した攻撃やシステムの設定内容を利用した攻撃等侵入のための行為である。

99 件の届出があり、これらのうち実際に侵入につながったものは 47 件である。

【主な内容】

ソフトウェアのぜい弱性やバグを利用した攻撃：14 件

パスワード推測：11 件

(ウ) 不正行為の実行及び目的達成後の行為

侵入その他、何らかの原因により不正行為を実行されたことについては 96 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：41 件

プログラムの作成・設置(インストール)、トロイの木馬等の埋め込み等：21 件

裏口(バックドア)の作成：10 件

踏み台とされて他のサイトへのアクセスに利用された：9 件

資源利用(ファイル、CPU 使用)：3 件

証拠の隠滅(ログの消去等)：3 件

イ サービス妨害攻撃

過負荷を与えたり、例外処理を利用してサービスを不可若しくは低下させたりする攻撃である。10 件(平成 23 年：7 件)の届出があった。

ウ その他

その他にはメール不正中継やメールアドレス詐称、正規ユーザになりすましてのサービスの不正利用、ソーシャルエンジニアリング等が含まれ、44 件(平成 23 年：28 件)の届出があった。

【主な内容】

正規ユーザへのなりすまし：41 件

メールの不正中継：1 件

ディレクトリ・トラバーサル：1 件

(2) 原因別分類

不正アクセスを許した問題点/弱点による分類である。

121 件の届出中、実際に被害に遭った計 105 件(平成 23 年：75 件)を分類

すると次のようになる。

被害原因として「ID、パスワード管理不備」や「古いバージョン使用、パッチ未導入等」が多くなっているなど、基本的なセキュリティ対策がなされていないサイトが狙われていると推測される。また、原因が不明なケースがますます多くなっており、手口が巧妙化するとともに原因究明が困難な事例が多いことが推測される。

【主な要因】

ID、パスワード管理の不備によると思われるもの：18件

古いバージョンの利用や、パッチ・必要なプラグイン等の未導入によるもの：15件

DoS 攻撃・その他によるもの：9件

設定の不備（セキュリティ上問題のあるデフォルト設定を含む。）によるもの：7件

原因不明：56件

(3) 電算機分類

不正アクセス行為の対象となった機器による分類である（被害の有無は問わない。）

【主な対象】

WWW サーバ：64件

メールサーバ：14件

クライアント：5件

その他のサーバ：5件

不明：26件

1件の届出で複数の項目に該当するものがある。

(4) 被害内容分類

121件の届出を被害内容で分類した133件中、実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は117件（昨年：81件）である。

なお、対処に係る工数やサービスの一時停止、代替機の準備等に関する被害は除外している。

【主な被害内容】

ホームページ改ざん：38件

踏み台として悪用：25件

オンラインサービスの不正利用：20件

サービス低下：13件

データの窃取や盗み見：8件

1件の届出で複数の項目に該当するものがある。

2. 対策情報

平成23年はCMS(Content Management System)のぜい弱性を悪用したウェブサイト改ざんの届出が増加したが、平成24年はそれに加えてサーバ管理ツールのぜい弱性を悪用したウェブサイト改ざんが多かったといえる。また、被害原因の多くが不明であったことから、こうした改ざんを行うための攻撃手口の巧妙化がうかがえる。その他では、なりすましによってオンラインゲーム等のサービスを勝手に使われて金銭被害が出たケースや、メールアカウントを窃取されて迷惑メール送信に悪用されていた被害も目立っていたといえる。主に原因不明なケースが多く見受けられたが、基本的なセキュリティ対策を実施していれば、被害を免れていたと思われるケースが多く見受けられる。システム管理者は次の点を確認して総合的に対策を行うことが望まれる。

- ・ ID やパスワードの厳重な管理及び設定
- ・ ぜい弱性の解消(修正プログラム適用不可の場合は、運用による回避策も含む。)
- ・ ルータやファイアウォール等の設定やアクセス制御設定
- ・ こまめなログのチェック

また、個人ユーザにおいても同様に次の点に注意することが望まれる。

- ・ Windows Update や Office Update 等、OS やアプリケーションソフトのアップデート
- ・ パスワードの設定と管理(複雑化、定期的に変更、安易に他人に教えない等)
- ・ ルータやパーソナルファイアウォールの活用
- ・ 無線 LAN の暗号化設定確認(WEP は使用せず、できる限り WPA2 を使用する。)

(参照)

【システム管理者向け】

「icat」サイバーセキュリティ注意喚起サービス

<http://www.ipa.go.jp/security/vuln/icat.html>

「情報セキュリティに関する啓発資料」

<http://www.ipa.go.jp/security/fy18/reports/contents/>

「脆弱性対策のチェックポイント」

http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

「安全なウェブサイトの作り方 改訂第6版」

<http://www.ipa.go.jp/security/vuln/websecurity.html>

「JVN (Japan Vulnerability Notes)」 脆弱性対策情報ポータルサイト

<http://jvn.jp/>

「SQL インジェクション攻撃に関する注意喚起」

http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLInjection.html

「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」

http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html

「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」

<http://www.ipa.go.jp/security/topics/20091224.html>

「IPA メールニュース」

<http://www.ipa.go.jp/about/mail/>

【個人ユーザ向け】

「ここからセキュリティ」情報セキュリティ・ポータルサイト

<http://www.ipa.go.jp/security/kokokara/>

「IPA セキュリティセンター・個人ユーザ向けページ」

<http://www.ipa.go.jp/security/personal/>

「Microsoft セキュリティセンター」(日本マイクロソフト社)

<http://www.microsoft.com/ja-jp/security/default.aspx>

「MyJVN」(セキュリティ設定チェッカ、バージョンチェッカ)

<http://jvndb.jvn.jp/apis/myjvn/>

「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」

<http://www.ipa.go.jp/security/topics/alert20110803.html>

ウイルス対策を含むセキュリティ関係の情報・対策等については、下記ページを参照。

「IPA セキュリティセンタートップページ」

<http://www.ipa.go.jp/security/>

注1 コンピュータ不正アクセス

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。

注2 ここに挙げた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではない。

一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）に報告（調整対応依頼）があった不正アクセス関連行為の状況について

JPCERT/CC は、国内の情報セキュリティインシデントの被害低減を目的として、広く一般から不正アクセス関連行為を含むコンピュータセキュリティインシデントに関する調整対応依頼を受け付けている。

1. 不正アクセス関連行為の特徴および件数

（平成 24 年中に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象）

報告（調整対応依頼）のあった不正アクセス関連行為(注 1)に係わる報告件数(注 2)は 17,265 件であった。この報告を元にしたインシデント件数（注 3）は 16,926 件であり、インシデントをカテゴリ別に分類すると以下の通りである。

（ 1 ） プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ/サービス/弱点の探査を意図したアクセス等、システムのアクセス権において特に問題のなかったもの(影響を生じないか又は無視できるアクセス)について 10,289 件の報告があった。
[1/1-3/31: 1,823 件、4/1-6/30:2,281 件、7/1-9/30:3,391 件、10/1-12/31: 2,794 件]

（ 2 ） システムへの侵入

管理者権限の盗用が認められる場合やワーム等を含め、システムへの侵入について 1,814 件の報告があった。
[1/1-3/31: 142 件、4/1-6/30: 139 件、7/1-9/30:796 件、10/1-12/31: 737 件]

（ 3 ） マルウェアサイト

閲覧することで PC がマルウェアに感染してしまう攻撃用サイトや攻撃に使用するマルウェアを公開しているサイトについて 786 件の報告があった。
[1/1-3/31: 162 件、4/1-6/30: 209 件、7/1-9/30:202 件、10/1-12/31: 213 件]

（ 4 ） ネットワークやコンピュータの運用を妨害しようとする攻撃

大量のパケットや予期しないデータの送信によって、サイトのネットワークやホストのサービス運用を妨害しようとするアクセスについて 36 件の報告があった。
[1/1-3/31:7 件、4/1-6/30:11 件、7/1-9/30:12 件、10/1-12/31:6 件]

(5) Web 偽装事案(phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 1,324 件の報告があった。

[1/1-3/31: 324 件、4/1-6/30: 367 件、7/1-9/30: 273 件、10/1-12/31:360 件]

(6) その他

コンピュータウイルス、SPAM メールを受信等について 2,677 件の報告があった。

[1/1-3/31:77 件、4/1-6/30:825 件、7/1-9/30:592 件、10/1-12/31:1,183 件]

2 . 防御に関する啓発および対策措置の普及

JPCERT/CC は、日本国内のインターネット利用者に対して、不正アクセス関連行為を防止するための予防措置や、発生した場合の緊急措置などに関する情報を提供し、不正アクセス関連行為への認識の向上や適切な対策を促進するため、以下の文書を公開している(詳細は <http://www.jpCERT.or.jp/>参照。)

(1) 注意喚起

[新規]

2012 年 1 月	Microsoft .NET Framework の複数の脆弱性に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 2012 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2012 年 2 月	PHP 5.3.9 の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起 2012 年 2 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2012 年 3 月	Adobe Flash Player の脆弱性に関する注意喚起 DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起 2012 年 3 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 2012 年 2 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起

2012年4月	Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 2012年4月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起
2012年5月	Adobe Flash Player の脆弱性 (APSB12-09) に関する注意喚起 2012年5月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起 PHP の脆弱性に関する注意喚起 ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起
2012年6月	ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性 (APSB12-14) に関する注意喚起 2012年6月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起 2012年6月 Java SE の脆弱性を狙う攻撃に関する注意喚起
2012年7月	2012年7月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起
2012年8月	2012年8月 Microsoft セキュリティ情報 (緊急 5件含) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB12-18) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性 (APSB12-16) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB12-19) に関する注意喚起 MS-CHAP v2 の認証情報漏えいの問題に関する注意喚起
2012年9月	2012年8月 Java SE の脆弱性に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2012-4244) に関する注意喚起 2012年9月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2012年10月	Adobe Flash Player の脆弱性 (APSB12-22) に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2012-5166) に関する注意喚起 2012年10月 Microsoft セキュリティ情報 (緊急 1件含) に関する注意喚起
2012年11月	Adobe Flash Player の脆弱性 (APSB12-24) に関する注意喚起 2012年11月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起 2012年10月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起

2012年12月	2012年12月 Microsoft セキュリティ情報 (緊急 5件含) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB12-27) に関する注意喚起
----------	---

(2) 活動概要 (報告状況等の公表)

発行日 : 2013-01-17 [2012年10月1日 ~ 2012年12月31日]

発行日 : 2012-10-10 [2012年7月1日 ~ 2012年9月30日]

発行日 : 2012-07-12 [2012年4月1日 ~ 2012年6月30日]

発行日 : 2012-04-12 [2012年1月1日 ~ 2012年3月31日]

(3) JPCERT/CC レポート

[発行件数] 50件

[取り扱ったセキュリティ関連情報数] 276件

注1 不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的)に発生する全ての事象が対象になる。

注2 ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

注3 「インシデント件数」は、各報告に含まれるインシデント件数の合計を示す。ただし、1つのインシデントに関して複数件の報告がよせられた場合は、1件のインシデントとして扱う。

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	<p>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。</p>
研究開発状況（概要）	<p>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。</p> <p>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。</p>
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	<p>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。</p>

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	<p>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。</p> <p>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 サイトをクロール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 を短時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 (クロールの起点) 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。</p> <p>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旨とする。</p>
研究開発状況 (概要)	<p>・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。</p> <p>(1) DBD 攻撃大規模観測網構築技術</p> <p>(2) DBD 攻撃分析・対策技術</p> <p>(3) DBD 攻撃対策フレームワーク実証実験</p>
詳細の入手方法 (関連部署名及びその連絡先)	<p>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</p> <p>(http://itaku-kenkyu.nict.go.jp/index.html)</p> <p>電話 042 - 327 - 6011</p>
将来の方向性	<p>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。</p>

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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
研究開発状況（概要）	<p>・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。</p> <p>（１）検査プログラムに関する研究開発</p> <p>（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</p> <p>（３）ユーザサポートプロトコルに関する研究開発</p> <p>（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</p>
詳細の入手方法（関連部署名及びその連絡先）	<p>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</p>
将来の方向性	<p>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。</p>

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	<p>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。</p> <p>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。</p>
研究開発状況（概要）	<p>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 Assessment）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。</p> <p>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。</p> <p>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。</p> <p>Fuzzingエンジン群追加開発</p> <p>（1）ミューテーションファジングの研究及び開発</p> <p>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。</p> <p>（2）モバイルOS脆弱性発見手法調査</p> <p>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。</p> <p>http://www.blackhat.com/usa/bh-us-12-briefings.html#0i</p>
詳細の入手方法（関連部署名及びその連絡先）	<p>株式会社フォティーンフォティ技術研究所（http://www.fourteenforty.jp/）</p> <p>鷓飼 裕司（電話：03-6277-1811）</p>
将来の方向性	<p>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。</p>

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	<p>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。</p> <p>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。</p>
研究開発状況 (概要)	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
詳細の入手方法 (関連部署名及びその連絡先)	<p>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)</p>
将来の方向性	<p>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。</p> <p>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。</p> <p>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。</p>

(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	<p>「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。</p> <p>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。</p> <p>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。</p> <p>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共に、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。</p>

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 NEPP10ユニット 045-477-5800	
U R L http://www.nippon-control-system.co.jp/	
対象技術	技術開発状況
<p>侵入検知・防御技術</p> <p>開発年： 平成21年度～ 平成24年度</p>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> ・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	
U R L 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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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 攻撃を効果的に軽減するために利用可能。</p>

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）	
U R L 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	<p>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ェア製品です。</p> <p>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。</p> <p>研究・開発した応用技術</p> <p><グループアクセス制御></p> <p>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。</p> <p>特徴を以下に示します。</p> <ul style="list-style-type: none"> ・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 <p><モバイル接続への対応方式></p> <p>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。</p> <p><大規模構成への対応方式></p> <p>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。</p>

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） 千103-0023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	
U R L 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	<p>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。</p> <p><u>すべてのパケットを取得</u></p> <p>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プライアンスです。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。</p> <p><u>詳細なフォレンジック分析</u></p> <p>NetDetectorは、ネットワークパケットから様々な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。</p>
侵入検知技術 平成17年	<p><u>統合性のある可視化</u></p> <p>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。</p>

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	
U R L http://www.elock.co.jp/webalarm/index.html http://www.gridlock.com/gridv2/demo.htm	
対象技術	技術開発状況
<ul style="list-style-type: none"> ・ 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 	<p>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。</p> <p>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。</p> <p>2) 不正アクセスを防ぐ2要素認証システム</p> <p>「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段階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。</p>
開発年：平成11年	

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
U R L	http://www.sciencepark.co.jp/information%5Fsecurity/

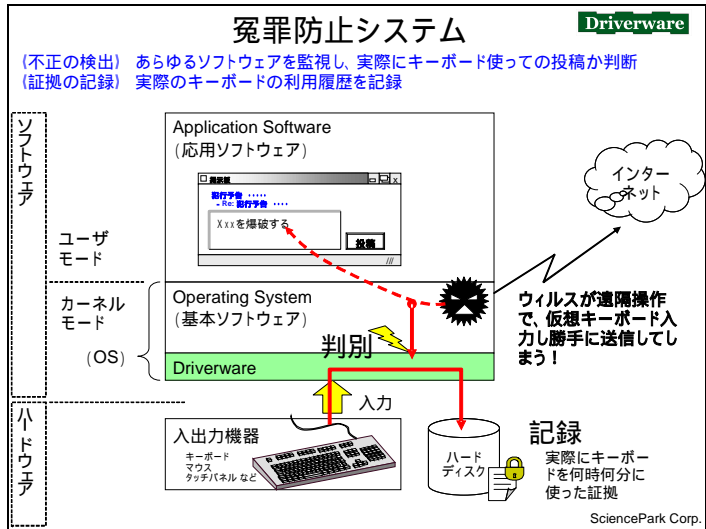
対象技術	技術開発状況
------	--------

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イバ群をパソコン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。

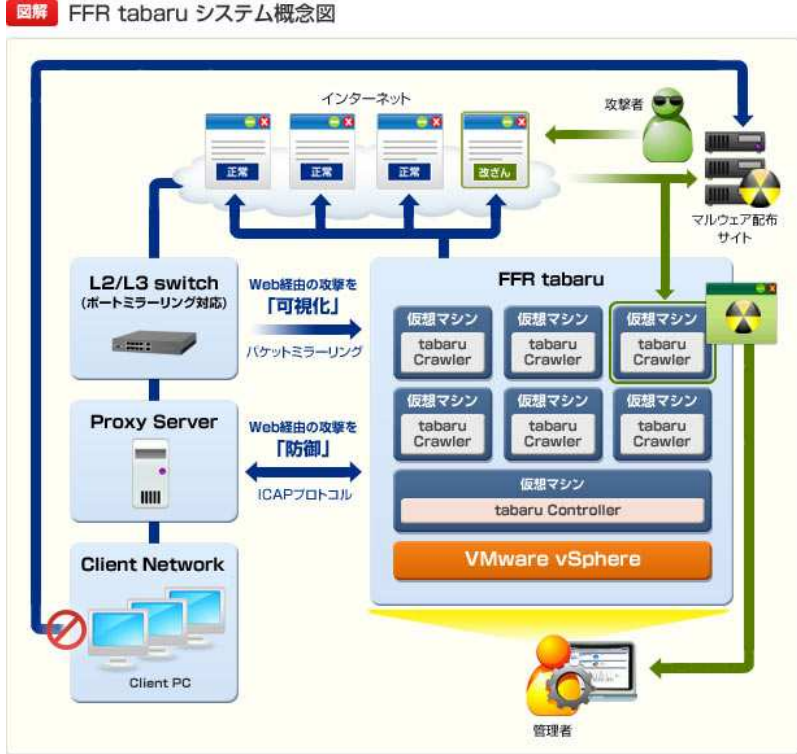


冤罪防止ソフトウェアの概要図

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	
U R L http://www.nextgen.co.jp/index.html	
対象技術	技術開発状況
<p>侵入検知技術 開発年： 平成21年度-平成24年度</p>	<p>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 packets 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。</p> <p>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。</p> <p>http://www.nextgen.co.jp/products/security/nx-c6000.html(製品概要)</p>

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	
U R L 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	<p>< 概要 ></p> <p>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。</p> <p>< 特徴 ></p> <p>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。</p> <p>http://www.nextgen.co.jp/solution/voip/service/sipvoip_1.html</p>

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	鷓飼裕司
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
<p>侵入検知・防御技術</p> <p>開発年： 平成 22 年度～ 平成 24 年度</p>	<p>【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。</p> <p>【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。</p> <p>【製品概要】 http://www.fourteenforty.jp/products/tabaru/index.htm</p> <p>【システム概念図】  </p>

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。

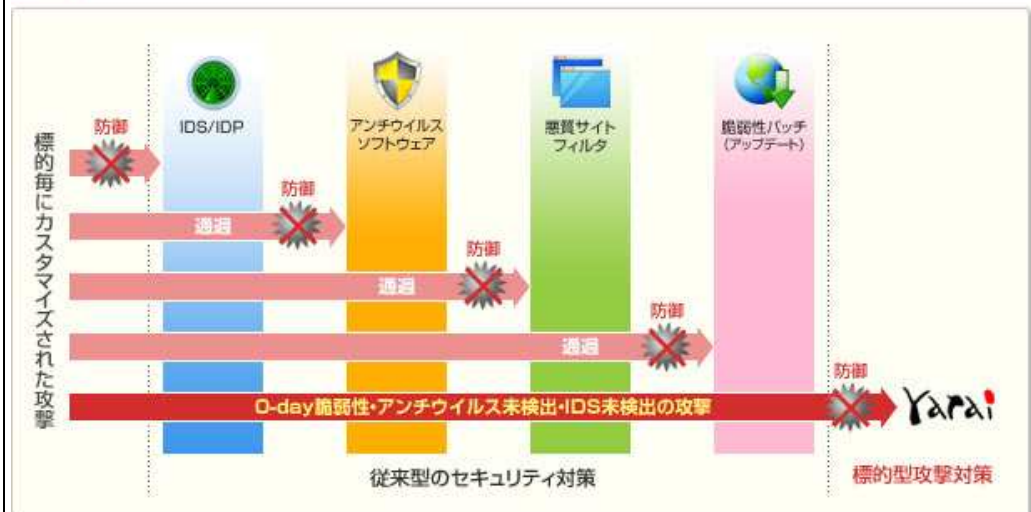
【製品概要】

<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	<p>【背景】</p> <p>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。</p> <p>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。</p> <p>【概要】</p> <p>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た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。</p> <p>【製品概要】</p> <p>http://www.fourteenforty.jp/products/yarai_analyzer/index.htm</p>
------------	---

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




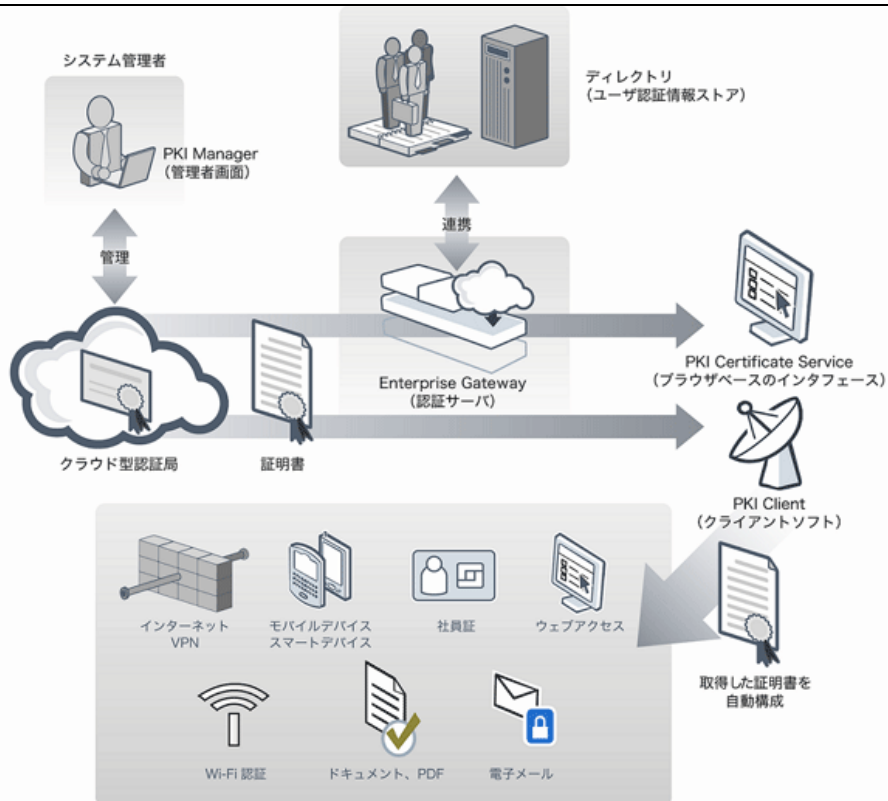
企業名（及び略称）：株式会社シマンテック（シマンテック）	
代表者氏名：河村浩明	
所在地（郵便番号及び住所）：〒107-0052 東京都港区赤坂1-11-44	
関連部署名及び電話番号：	
U R L：http://www.symantec.co.jp	
対象技術	技術開発状況
侵入検知・防御技術(平成21年)	<p>Symantec Critical System Protectionとして製品化</p> <p>Symantec Critical System Protectionは、ホスト上のプロセスおよびユーザに対してホワイトリスト化された動作のみを許可することで不正な操作を防止します。</p> <p>主要な機能は下記の通りです。</p> <ul style="list-style-type: none"> ・ ファイル改ざんの監視： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 最新の vSphere 強化ガイドラインに基づいて作

	<p>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。</p> <ul style="list-style-type: none"> ・ 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。 <p>参照URL： http://www.symantec.com/ja/jp/critical-system-protection</p>
<p>侵入検知・防御技術(平成21年)</p>	<p>Symantec Web Gatewayとして製品化</p> <p>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。</p> <p>製品の特徴は下記の通りです。</p> <ul style="list-style-type: none"> ・ 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 <p>参照URL：http://www.symantec.com/ja/jp/web-gateway</p>
<p>侵入検知・防御技術(平成22年)</p>	<p>Symantec Messaging Gateway powered by Brightmailとして製品化</p> <p>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。</p> <p>製品の特徴は下記の通りです。</p> <ul style="list-style-type: none"> ・ 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

	<p>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</p> <ul style="list-style-type: none"> ・ 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 <p>参照URL : http://www.symantec.com/ja/jp/messaging-gateway</p>
<p>ぜい弱性対策技術（平成21年）</p>	<p>Endpoint Management powered by Altirisとして製品化</p> <p>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。</p> <p>参照URL : http://www.symantec.com/ja/jp/products-solutions/families/?fid=endpoint-management</p>
<p>ぜい弱性対策技術（平成21年）</p>	<p>Control Compliance Suiteとして製品化</p> <p>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。</p> <p>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。</p> <p>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</p>

	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>参照URL： http://www.symantec.com/ja/jp/control-compliance-suite</p>
<p>高度認証技術 (平成23年)</p>	<p>Symantec 03として製品・サービス化</p> <p>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。</p> <p>参照URL：http://www.symantec.com/symantec-03</p>

<p>高度認証技術 (平成24年)</p>	<p>Symantec Validation & ID Protection (VIP) としてサービス化</p> <p>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ウ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。</p> <p>サービスの概要は下記の図を参照ください。</p>  <p>参照URL : https://www.verisign.co.jp/vip/</p>
<p>高度認証技術 (平成24年)</p>	<p>Symantec Managed PKI Serviceとしてサービス化</p> <p>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。</p> <p>サービスの概要は下記の図を参照ください。</p>



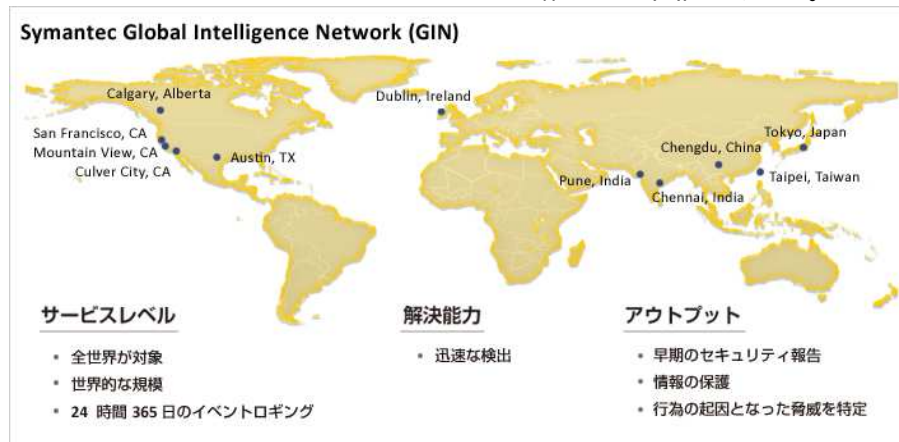
参照URL : <https://www.verisign.co.jp/mpki8/>

インシデント分析技術（平成21年）

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 :

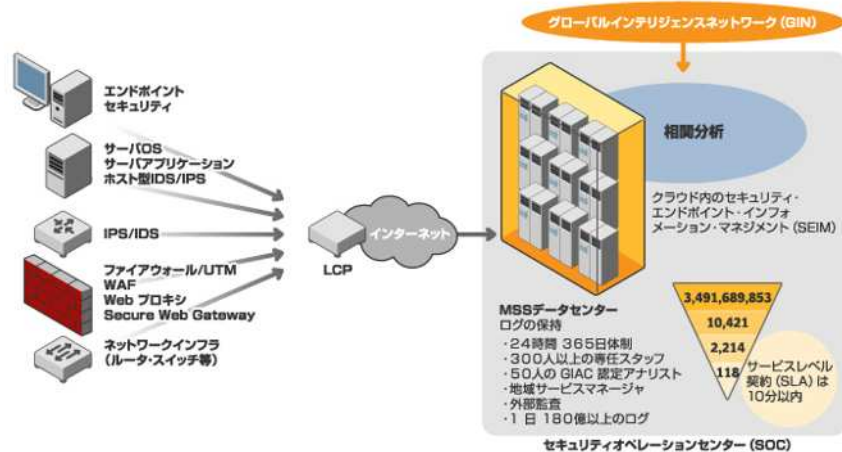
http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_4st

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。

	<p>参考URL： http://www.symantec.com/ja/jp/protection-engine-network-attached-storage</p>
不正プログラム対策技術（平成22年）	<p>Symantec Endpoint Protectionとして製品化</p> <p>Symantec Endpoint Protection は、Symantec Insightと SONAR という新世代の検出テクノロジーを搭載。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。</p> <p>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。</p> <p>参考URL： http://www.symantec.com/ja/jp/endpoint-protection</p>

(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K I -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」を公表。Soups2012(国際会議、アメリカ、査定あり)「Anti-phishing system using footprint-sharing website」を公表。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 武蔵研究室
代表者名	武蔵 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 蔵研究室 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。 <ul style="list-style-type: none"> ・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 武蔵研究室
代表者名	武蔵 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 武蔵研究室
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等を通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～	40G i g a b i tあるいは100G i g a b i t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 L S I 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： J S T (C R E S T) の デイペンタブル V L S I システムの 基盤技術で開発	耐タンパ暗号回路：試作チップ動作検証確認 偽造防止 L S I：試 作チップ動作検証確認 + デモシステム開発完了
研究開発国：	
研究開発期間： 平成21年9月～平 成27年3月	

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	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。
研究開発国： 日本	
研究開発期間： 平成23年4月1日 ～(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	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 I R 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	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
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：	

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	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。
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	

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	<p>(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。</p>
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	

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： I n f o C a g e 開発元： N E C 開発国： 日本 価格： 発売時期： 平成14年12月24 日 出荷数：	<p>・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。</p>

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	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。
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	

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.fujitsu.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： I P C O M E X S C シリーズ 開発元： 富士通株式会社 開発国： 日本 価格： 5 8 万円～ 発売時期： 平成18年10月 出荷数：	<p>・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。</p> <p>・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。I P C O M E X シリーズはI P s e c - V P N と S S L - V P N、L 2 T P / I P s e c に対応しているため、事業間アクセスにはI P s e c - V P N、リモートアクセスにはS S L - V P N、またはL 2 T P / I P s e c といった使い分けも可能です。</p> <p>・次世代ファイアウォール 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。</p>

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	