平成１４年２月７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

平成１１年８月に成立した「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７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７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。
２　前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１３年１月１日から平成１３年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

警察庁、総務省又は経済産業省のいずれかの予算で実施しているアクセス制御機能の研究開発の状況及び昨年末に募集した民間企業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/
○　経済産業省ホームページ　http://www.meti.go.jp/policy/netsecurity/

不正アクセス行為の発生状況

第１　平成13年中の不正アクセス禁止法違反事件の検挙状況等について

平成13年中に警察庁に報告のあった不正アクセス行為（以下「期間中の不正アクセス行為」という。）が対象である。

１　不正アクセス行為の発生状況及びその特徴

期間中の不正アクセス行為は1,253件で、前年の不正アクセス行為（不正アクセス禁止法の施行日である平成12年２月13日から平成12年12月31日までの間をいう。以下同じ。）の件数と比較して、約12倍となった。このうち、海外から不正アクセス行為が行われたことが判明しているものは448件で、前年の約18倍となった。

		平成13年	平成12年	増　減
認知件数		1,253	106	1,147
	海外からのアクセス	448	25	423
	国内からのアクセス	258	73	185
	不明	547	8	539

不正アクセス行為の大幅な増加の要因としては、

○　ホームページ書換えプログラムによるホームページ書換え事案（以下「書換えプログラムによる事案」という。）（813件）

○　自己増殖型不正プログラムによる事案（94件）

○　攻撃予告に関連すると思われるセキュリティ・ホール攻撃型（不正アクセス禁止法第３条第２項第２号及び第３号のアクセス制御機能による特定利用の制限を免れる情報又は指令を入力する行為をいう。）の不正アクセス行為の連続発生事案（以下「攻撃予告に絡む事案」という。）（55件）

○　自己増殖型DoS攻撃プログラム及び自己増殖型バックドア作成プログラムによる事案（28件）

の発生が挙げられる。（下表参照。また、これらの事案の特徴については、参考１から７を参照。）。

なお、これらの不正アクセス行為の原因としては、既知のセキュリティ・ホールが解消されていなかったことが挙げられる。

	海外からのアクセス	国内からのアクセス	不明	計
書換えプログラムによる事案	387	145	281	813
自己増殖型不正プログラムによる事案	3	0	91	94
攻撃予告に絡む事案	22	0	33	55
自己増殖型DoS攻撃プログラム及び自己増殖型バックドア作成プログラムによる事案	2	1	25	28
総　数	414	146	430	990

これらの被害に係る特定電子計算機のアクセス管理者別に見ると、確認できた中では一般企業が429件と最も多く、次いでプロバイダが182件の順となっている。

また、認知の端緒としては、警察職員によるいわゆるサイバーパトロールや被疑者の取調べ等の警察活動が930件と最も多く、次いで警察等への届出等が286件（アクセス管理者からの届出が168件、利用権者からの届出が118件）の順となっている。

なお、不正アクセス行為後の行為として、ホームページの改ざん、消去を伴うものが935件、DDoS攻撃ツールやバックドア・ツール等のプログラムを仕掛けられていたものが178件あった。

被害に係る特定電子計算機のアクセス管理者別	平成13年	平成12年
プロバイダ	182	59
大学、研究機関等	101	8
一般企業	429	25
その他	139	14
不明	402	—
計	1,253	106

認知の端緒別	平成13年	平成12年
アクセス管理者からの届出	168	30
利用権者からの届出	118	23
警察活動	930	35
発見者からの通報	21	7
その他	16	11
計	1,253	106

2　不正アクセス禁止法違反事件の検挙状況

平成13年中の不正アクセス禁止法違反の検挙件数は35事件（67件）、検挙人員は51人で、前年に比べ検挙事件数は４事件増加し（検挙件数は変わらず）、検挙人員は14人増加した。その内訳は、不正アクセス行為が35事件(66件)、51人であり、不正アクセス助長行為が１事件(１件)、１人であった。

不正アクセス行為の態様については、33事件（52件）が識別符号窃用型（不正アクセス禁止法第３条第２項第１号の他人の識別符号を無断で入力する行為をいう。）であり、３事件（14件）がセキュリティ・ホール攻撃型であった。

なお、検挙人員51人中49人が成人であり、２人が少年であった。

事犯別		平成13年	平成12年
不正アクセス行為	検挙事件数	35	30
	検挙件数	66	62
	検挙人員	51	34
不正アクセス助長行為	検挙事件数	1	4
	検挙件数	1	5
	検挙人員	1	5
計	検挙事件数	35（重複１）	31(重複３)
	検挙件数	67	67
	検挙人員	51（重複１）	37(重複２)

3　不正アクセス行為の検挙事例

嫌がらせの目的で元交際相手の識別符号を窃用した不正アクセス禁止法違反及び名誉毀損事件

無職の男(21)が、嫌がらせの目的で、無料電子メール・サービスのリマインダ機能を悪用してアクセス管理者から入手した元交際相手のＩＤ・パスワードを使用して不正に無料電子メール・サービス等を利用し、同人のプロフィールを掲示するホームページの内容をわいせつな内容等に書き換え、掲示して同人の名誉を毀損した。13年１月、不正アクセス禁止法違反及び名誉毀損罪で検挙した（広島)。

なりすまし目的で他人の識別符号を窃用した不正アクセス禁止法違反及び詐欺未遂事件

無職の男(22)が、他人になりすまして詐欺を行う目的で、インターネット・オークションの格付けの高い利用権者から個人情報を聞き出し、同人になりすましてアクセス管理者からパスワードを入手し、インターネット・カフェ等に設置されたクライアントコンピュータを用いて同人のＩＤ・パスワードを使用して不正にインターネット・オークションを利用するとともに、同人になりすまして同インターネット・オークション上に虚偽の情報を掲載して出品し、応募してきた相手に代金を郵送させてだまし取ろうとしたが、その目的を遂げなかった。13年５月、不正アクセス禁止法違反及び詐欺未遂罪で検挙した(愛知)。

ハッキング手法を試す目的で他人の識別符号を窃用した不正アクセス禁止法違反事件

大学生の男(18)が、雑誌等で知り得たハッキング手法を試す目的で、ｉモード電話機を利用し、無料ホームページ・サービス提供事業者のアクセス管理者になりすまして「あなたのセキュリティに異常があります。ログイン名及びパスワードを送信してください。」等の虚偽メッセージを送信することにより利用権者から直接入手したＩＤ・パスワードを使用して不正にウェブ・サーバに侵入し、同パスワードを変更した。13年５月、不正アクセス禁止法違反で検挙した(警視庁)。

嫌がらせの目的で元勤務先の識別符号を窃用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

無職の男(48)が、解雇された腹いせに、勤務当時知り得た元勤務先の会社のＩＤ・パスワードを使用して同社がホームページを開設しているプロバイダのウェブ・サーバに不正に侵入し、元勤務先に無断で同社のホームページ契約を解約することにより同社のホームページのデータを消去した。13年５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罪で検挙した(新潟)。

嫌がらせの目的で元勤務先の識別符号を窃用した不正アクセス禁止法違反、電子計算機損壊等業務妨害、名誉毀損及びわいせつ図画公然陳列事件

会社員の男(33)が、退職金の未払い等に対する腹いせに、勤務当時知り得た元勤務先の学習塾のＩＤ・パスワードを使用して、同塾がホームページを開設しているプロバイダのＦＴＰサーバに不正に侵入し、同ホームページにわいせつな画像を張り付けて同塾関係者の名誉を毀損した。13年７月、不正アクセス禁止法違反、電子計算機損壊等業務妨害罪、名誉毀損罪及びわいせつ図画公然陳列罪で検挙した（警視庁）。

いたずら目的でウェブ・サーバのセキュリティ・ホールを突いた不正アクセス禁止法違反事件

大学生の男(22)が、いたずらの目的で、クラッキング・ツールを使用して財団法人のウェブ・サーバのセキュリティ・ホールを突いて不正に同サーバに侵入した。13年７月、不正アクセス禁止法違反事件で検挙した（千葉）。

嫌がらせの目的で他人の識別符号を窃用して同人の電子メールを盗み見た不正アクセス禁止法違反及び電気通信事業法違反事件

会社員の女(30)が、嫌がらせの目的で、無料電子メール・サービスのリマインダ機能を悪用してアクセス管理者からパスワードの送付を受けるなどの方法により入手した同僚の女性のＩＤ・パスワードを使用して不正に無料電子メール・サービス等提供事業者の電子メール・サーバに侵入し、同女あての電子メールを盗み見るなどした。13年７月、不正アクセス禁止法違反及び電気通信事業法違反で検挙した（警視庁）。

嫌がらせの目的でｉモード電話機用ホームページの識別符号を窃用してホームページを改ざん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

無職の女(26)らが共謀の上、嫌がらせの目的で、利用権者が応援する歌手の名前から推知したパスワードを使用して不正にｉモード電話機用の無料ホームページ・サービス提供事業者のウェブ・サーバに侵入し、当該ホームページを改ざんするなどした。13年８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罪で検挙した（熊本）。

インターネット・オークションに係る識別符号を窃用した多数人による広域にわたる不正アクセス禁止法違反事件

会社員の男(26)らは、嫌がらせ、いたずら等の目的で自己又は何者かが推知した利用権者のインターネット・オークション用のＩＤ・パスワードを使用して不正にインターネット・オークションを利用し、さらにこのうちの会社員(23)がＩＤ・パスワードをインターネット上の掲示板サイトに掲載したため、それを見た会社員(20)その他の数十名の者らが、当該ＩＤ・パスワードを使用してそれぞれ不正に同インターネット・オークションを利用した。13年10月から12月までに、不正アクセス禁止法違反で13人を検挙した。（警視庁、茨城、愛知）

なりすまし目的で友人等の識別符号を窃用した不正アクセス禁止法違反及び著作権法違反事件

会社員の男(28)が、他人になりすまして海賊版ソフトウェアを販売する目的で、ホームページ作成を手伝った際に知り得た友人等のＩＤ・パスワードを使用して不正に当該友人等がホームページを開設等しているプロバイダのＦＴＰサーバに侵入し、同人になりすましてホームページ上で海賊版ソフトウェアを販売するなどした。13年10月、著作権法違反で、11月、不正アクセス禁止法違反で検挙した（兵庫）。

なりすまし目的で、クラッキング・ツールにより入手した他人の識別符号を窃用した不正アクセス禁止法違反及び詐欺事件

無職の男(27)らが、共謀の上、他人になりすまして詐欺を行う目的で、キーボード操作状況を記録するクラッキング・ツールをインターネット・カフェのクライアントコンピュータに仕掛けて入手した他人のＩＤ・パスワードを使用して不正にインターネット・オークションを利用し、同人になりすまして同インターネット・オークション上に虚偽の情報を掲載してハイウェイカードの出品を仮装し、応募してきた相手に代金を他人名義の銀行口座に振り込ませてだまし取った。13年11月及び12月、不正アクセス禁止法違反及び詐欺罪で検挙した（警視庁）。

４　検挙事件の特徴

(1) 犯行の手口

不正アクセス行為で検挙した35事件（66件）の手口としては、利用権者のパスワード管理の甘さにつけ込んだＩＤ・パスワードの入手が18事件（29件）と最も多く、次いでアクセス管理者又は利用権者になりすました利用権者又はアクセス管理者からのＩＤ・パスワードの直接入手が６事件（８件)、推知が６事件(９件)の順となっており、特に高度なコンピュータ技術及び電気通信技術を有していない者でも行える形態が目立った。

このほか、クラッキング・ツールによるＩＤ・パスワードの入手等が３事件(６件)あった。

(2) 被疑者の特徴

元交際相手や元社員等の利用権者と顔見知りの者による犯行が35事件中28事件(45件)と目立った。

また、検挙した被疑者の年齢は、20代が28人と最も多く、次いで40代が16人、30代が５人、10代が２人の順となっている。最年長の者は48歳であり、最年少の者は14歳であった。

(3) 犯行の動機

不正アクセス行為の動機としては、元交際相手や元勤務先の会社等に対する嫌がらせや仕返しが13事件（17件）と最も多く、次いで利用料金の請求を免れるためが５事件（８件)、メールの盗み見が４事件（６件）の順となっている。

(4) その他

不正アクセス行為が別の犯罪の手段として利用されていた事案は、12事件(23件)であった（電子計算機損壊等業務妨害事件（５事件（12件))、電気通信事業法違反事件（２事件（４件))、詐欺・詐欺未遂事件（２事件（３件))、名誉毀損事件（２事件（２件))、著作権法違反事件（１事件（２件))、私電磁的記録不正作出事件（１事件（１件)、わいせつ図画公然陳列事件（１事件（１件))（重複計上))。

5　都道府県公安委員会による援助措置

都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第６条の援助規定に基づくアクセス管理者に対する助言・指導を、平成13年中に21件（北海道、旭川２件、東京、愛知、三重、滋賀３件、京都、大阪２件、鳥取２件、愛媛、長崎、熊本３件、宮崎、沖縄）実施している。

	平成13年	平成12年
都道府県公安委員会による援助措置	21	6

6　防御上の留意事項

(1) サーバの適切な管理

サーバの管理者等は、インターネット上などで常にセキュリティ情報を確認し、使用しているオペレーティングシステム又はアプリケーション・プログラムにセキュリティ・ホールが発見されたことを知ったときは速やかに修正プログラムをインストールする等セキュリティ・ホールを解消するための措置を講ずる。

(2) 識別符号の適切な管理

検挙した35事件（67件）中20事件（33件）が元社員や元交際相手等の顔見知りからパスワードを知り得た者の犯行であり、不正アクセス行為が行われた原因としては、パスワードの定期的な変更を行っていなかったことが挙げられる。利用権者においても、パスワードを定期的に変更するなど識別符号を適切に管理する。

(3) その他

ＩＤ・パスワード入手の手口としては、管理者を名乗ったり、偽のホームページを立ち上げたりするなどしてアクセス管理者になりすまし、利用権者からＩＤ・パスワードを直接入手するものが目立った。利用権者においては、アクセス管理者から利用権者に対してパスワードの入力や回答を求めることは通常あり得ないことに留意し、不用意にパスワードを開示しないようにする。また、無料電子メール・サービスのリマインダ機能を悪用して、アクセス管理者から利用権者のパスワードを入手する手口も目立ったことから、リマインダ機能の悪用の可能性に留意して、インターネット上における各種サービスを利用しなければならない。

アクセス管理者は、警察がハイテク犯罪相談窓口、ホームページ等を通じて提供している不正アクセス事案に関する対策も参考にし、利用権者に対する注意喚起を行うなどの自主防衛措置を講ずるよう努めなければならない。

（参考）

1　攻撃予告に絡む事案について

13年２月から３月までの間、海外のサイトに我が国のサイトに対する攻撃を予告する内容が掲載されたことに関係すると思われる日本企業等に対するホームページ書き換え事案が連続的に発生した。

(1) 特徴

ア　攻撃の予告及び犯行声明が中国語で当該サイト上に掲載されていたこと

イ　書き換えの内容は日本政府を非難するものであること

等が挙げられる。

(2) 本事案の原因となったシステムの管理・設定上の主な問題点（対策）

ア　特定のオペレーティングシステム（WindowsNT,Windows2000）で動作するセキュリティ・ホールを有するウェブ・サーバ用プログラム（IIS）の修正プログラムをインストールせず使用していること（修正プログラムのインストール）

イ　特定のオペレーティングシステム（WindowsNT,Windows2000）で動作するホームページ作成・管理プログラム（Front Page Server Extentions）の設定ミス（設定

の再確認又は不必要な場合当該プログラムの削除）
ウ　セキュリティ・ホールを有するＤＮＳサーバ用プログラム（Bind）の修正プログラムをインストールせず使用していること（修正プログラムのインストール）

2　書換えプログラムによる事案について

13年５月、ホームページ書換えプログラムによる地方公共団体、民間企業、大学等のホームページ書換え事案が連続的に発生した。

(1) 特徴

ア　自己を不正に他の特定のサーバに複写・蔵置することを繰り返す自動的な機能及び特定のサーバに対するセキュリティ・ホール攻撃機能を有する不正プログラムを用いて自動的に攻撃を行っていること

イ　ホームページの書換え内容が米国政府等を非難する内容であること

等が挙げられる。

(2) 本事案の原因となったシステムの管理・設定上の主な問題点（対策）

ア　特定のオペレーティングシステム（Solaris）で動作するセキュリティ・ホールを有するシステム管理用プログラム（sadmind）の修正プログラムをインストールせず使用していること（修正プログラムのインストール）

イ　特定のオペレーティングシステム（WindowsNT,Windows2000）で動作するセキュリティ・ホールを有するウェブ・サーバ用プログラム（IIS）の修正プログラムをインストールせず使用していること（修正プログラムのインストール）

3　自己増殖型DoS(Denial of Service)攻撃プログラムによる事案について

13年７月から８月にかけて、ある特定の日時以降に特定のサーバに対してDoS攻撃（標的となるサーバに過剰な負荷をかけるなどして当該サーバのサービスを妨害する攻撃）を行う機能を有するプログラムが、国内の多数のサーバに感染する事案が連続的に発生した。

(1) 特徴

２(1)アのほか、一定期間の感染活動の後、特定の日時に、アメリカ合衆国ホワイトハウスのホームページ用IPアドレスに対してDoS攻撃を仕掛けるものであること等が挙げられる。

(2) 本事案の原因となったシステムの管理・設定上の主な問題点（対策）

２(2)イに同じ。

4　自己増殖型バックドア作成プログラムによる事案について

13年８月、自己増殖型DoS攻撃プログラムと同様の感染機能により、他のサーバに感染した上、バックドアを作成するプログラムが、国内の多数のサーバに感染する事案が連続的に発生した。

(1) 特徴

２(1)アのほか、次のことなどが挙げられる。

ア　サーバのシステムファイル保護機能を無効とすること

イ　特定のドライブ及びフォルダをネットワーク上に公開すること

(2) 本事案の原因となったシステムの管理・設定上の主な問題点（対策）

２(2)イに同じ。

5　自己増殖型不正プログラムによる事案について

13年９月、サーバ及びクライアントコンピュータを攻撃・感染対象とした不正プログラムが、短期間で国内の多数のサーバ及びクライアントコンピュータに感染する事案が発生した。

(1) 特徴

２(1)アのほか、次のことなどが挙げられる。

ア　ウェブ・サーバのトップページを改ざんし、クライアントコンピュータから閲覧がなされただけで、当該クライアントコンピュータに感染すること

イ　クライアントコンピュータからは、電子メールによる感染メールの配信、共有化されているネットワーク上の他のクライアントコンピュータへのファイル転送等がなされることにより感染すること

(2) 本事案の原因となったシステムの管理・設定上の主な問題点（対策）

２(2)イのほか、次のことが挙げられる。

ア　Windowsが動作するクライアントコンピュータにおける特定のブラウザソフトウェア（Internet Explorer）の修正プログラムをインストールせず使用していること（修正プログラムのインストール）

イ　共有フォルダ等にパスワードの設定が行われていないこと（フォルダのプロパティ設定から共有時のパスワード設定を行う）

6　DDoS(Distributed Denial of Service)攻撃ツールについて

DDoS攻撃とは、インターネット上の複数のコンピュータにDoS攻撃用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉にDoS攻撃を行い、標的となるサーバのサービスを妨害するものである。

DDoS攻撃ツールが仕掛けられていた場合は、オペレーティングシステムの再インストールにより攻撃用ツールを削除するとともに、オペレーティングシステム及びアプリケーション・プログラムのバージョンアップ並びに定期的点検等により再発に注意しなければならない。

7　バックドアについて

バックドアとは、部外からネットワークを通じて不正にサーバに侵入するための裏口のことである。クラッカー等は、一度侵入に成功したサーバにバックドアを設置することにより、当該バックドアを通じて次回以降の侵入を容易に行うことが可能となる。バックドアの設置方法は巧妙化してきており、当該サーバのアクセス管理者が存在に気付かない場合があるほか、削除しても再起動後に自動的にバックドアが設置されるツールが当該サーバに組み込まれている場合もある。バックドアが設置されたサーバから確実に当該バックドアを駆除するためには、オペレーティングシステムの再インストール及び修正プログラムのインストールを行うことが望ましい。

8　リマインダ機能について

リマインダ機能とは、利用権者がパスワードを忘れてしまった時に、アクセス管理者が何らかの方法で本人確認を行った上でパスワードを再発行する機能である。本人確認の方法としては、ＩＤ・パスワードの発行時に本人しか知り得ない情報を登録しておき、再発行時にその情報を利用権者に入力させるものなどがある。

（注１）　不正アクセス行為の認知の考え方

認知とは、被害届出の受理をした場合のほか、余罪として発覚した場合、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とすることとしている。

（注２）　不正アクセス行為の件数の計上について

・　一のアクセス制御機能に対する一の手口による侵害行為を１件とする。ただし、被疑者が異なる場合（共犯を除く。）はそれぞれ１件として計上し、短期間に一のアクセス制御機能に対して同一手口による侵害が継続的に行われた場合は包括して１件と

する。
・　不正アクセス行為と他の罪とが併合罪又は観念的競合の関係にある場合、これを別件として扱い、１件計上する。

第２　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

１　情報処理振興事業協会（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

平成１３年１月１日から１２月３１日の間にIPAに届出のあったコンピュータ不正アクセス（注１）が対象である。

コンピュータ不正アクセス被害届出件数は550件（昨年：143件）であった（注２）。平成１３年は、Sadmind/IIS、CodeRed、Nimdaなどの既知の脆弱性を狙ったワームの出現により、ワーム感染及びワーム形跡（未感染）に関する届出が全体の約46%（550件中255件）あり、不正アクセスの新たな脅威として捉える事が必要である。

以下に、種々の切り口で分類した結果を示す。各々の件数には未遂(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分類に該当するものがあるため、それぞれの項目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。重複があるため、届出件数とは異なり総計は333件（昨年：147件）となる。なお、この件数には、ワームに関する届出は含まれていない。

(ｱ) 侵入行為に関して

侵入行為に係わる攻撃等の届出は193件（昨年：67件）あった。

ａ　侵入の事前調査行為

システム情報の調査、稼動サービスの調査、アカウント名の調査等である。29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。
そのなかで実際に侵入の被害を受けたのは4件であった。

ｂ　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、システムの設定内容を利用した攻撃など、侵入のための行為である。193件の届出があり、これらのうち実際に侵入を受けたものは97件である。
パスワード推測：4件
ソフトウェアのバグを利用した攻撃：52件
システムの設定内容を利用した攻撃：21件

ｃ　不正行為の実行及び目的達成後の行為

実際に侵入を受けた97件について、その後行われた種々の行為である。１件の侵入で種々の行為が行われているため重複がある。
ファイル等の改ざん、破壊等：65件
プログラムの作成(インストール)、システムファイルの改ざん、トロイの木馬などの埋め込み等：12件
資源利用（ファイル、CPU使用）：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：20件
裏口の作成：3件
証拠の隠滅：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もしくは低下させる攻撃である。11件（昨年：６件）の届出があった。
過負荷を与える攻撃：4件

例外処理を利用した攻撃：1件
SPAMメール：6件

(ｳ) その他

その他には、ソーシャルエンジニアリングや、サービスの外部からの利用が含まれ、94件（昨年：74件）の届出があった。2001年の被害で特徴的な攻撃(嫌がらせであると思われる)は、メールアドレス詐称である。前年から蔓延している模様で、39件（昨年：26件）の届出があった。メール中継に利用されたケースの中にも、当該メールがアドレス詐称のものであると思われるものが多くなっている。

メール中継に関するもの：26件
そのうちメール中継に実際に利用されたもの：25件
オープンプロキシの利用：1件
メールアドレス(ドメイン)の詐称：39件
その他：28件

(2) ワーム別の分類

ワームの種類による分類である。ワームに関する届出は、実際にワームに感染した届出184件、ワームには感染しなかった届出71件、合計255件であった。主なワームの届出件数は以下の通りである。

Sadmind/IIS：132件（うち感染：132件）
CodeRed：77件（うち感染：29件）
Nimda：41件（うち感染：18件）
その他（Linux/Lionなど）：5件（うち感染：5件）

(3) 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。

実際に侵入を受けた97件（昨年：42件)、ワームに感染した184件、メール中継に係わる問題(弱点)のあった25件（昨年：41件)、オープンプロキシ利用の1件（昨年：2件)などの計307件（昨年：88件）を分類すると以下のようになる。

ID、パスワード管理の不備によると思われるもの：4件
古いバージョンの利用やパッチ・必要なプラグインなどの未導入によるもの：232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：42件
不明：29件

(4) 電算機分類

攻撃や被害の対象となった機器による分類である。

WWWサーバ：259件
メールサーバ：67件
DNSサーバ：23件
FTPサーバ：14件
ファイアウォール：8件
ルータ：3件
Proxyサーバ：1件
その他のサーバ：26件
クライアント：159件

(5) 被害内容分類

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届出件数は375件（昨年：93件）である。対処に係わ

る工数やサービスの一時停止、代替機の準備などに関する被害は除外している。

メール中継に利用された：25件
サーバダウン：12件
不正アカウント作成：4件
WWW書き換え：177件
パスワードファイル盗用：4件
サービス低下：20件
オープンプロキシ：1件
ファイルの書き換え：39件
その他：106件

(6) 対策情報

(2)の被害原因分類にもあるように、基本的な(既知の)対策をとっていなかったために被害にあってしまったものが多くなっている。下記ページなどを参照し、今一度状況確認・対処されたい。

「セキュリティ対策セルフチェックシート」
http://www.ipa.go.jp/security/ciadr/checksheet.html
「コンピュータ不正アクセス被害防止対策集」
http://www.ipa.go.jp/security/ciadr/cm01.html
ウイルス対策を含むセキュリティ関係の情報・対策などについては、下記ページを参照のこと。
「IPAセキュリティセンタートップページ」
http://www.ipa.go.jp/security/index.html

（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）ここにあげた件数は、コンピュータ不正アクセスの届出をIPAが受理した件数であり、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。

２　コンピュータ緊急対応センター（JPCERT/CC）に届出があった不正アクセス関連行為の状況について

平成１３年１月１日から１２月３１日の間にJPCERT/CCに届出のあったコンピュータ不正アクセスが対象である。

(1) 不正アクセス関連行為の特徴および件数

届出のあった不正アクセス関連行為（注 1）に係わる報告件数は 2,853件（昨年：2,232件）であった。

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、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 2,272件の報告があった。
[1/1-3/31: 557件、4/1-6/30: 870件、7/1-9/30: 452件、10/1-12/31: 393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を含め、システムへの侵入について 103 件の報告があった。

[1/1-3/31: 38件、4/1-6/30: 28件、7/1-9/30: 26件、10/1-12/31: 11件]

③ 電子メールの送信ヘッダを詐称したメールの配送

電子メールの送信ヘッダを詐称した電子メールの配送について 70件の報告があった。

[1/1-3/31: 39件、4/1-6/30: 20件、7/1-9/30: 2件、10/1-12/31: 9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 66件の報告があった。

[1/1-3/31: 19件、4/1-6/30: 18件、7/1-9/30: 20件、10/1-12/31: 9件]

⑤ 電子メール配送プログラムへのアクセス

電子メール配送プログラムへの、電子メールの中継を目的としたアクセスについて 43件の報告があった。

[1/1-3/31: 22件、4/1-6/30: 14件、7/1-9/30: 4件、10/1-12/31: 3件]

⑥ その他

インターネットを介して伝播するワーム、トロイの木馬、コンピュータウィルス、IP アドレスを詐称したパケットの偽造、Web ページの改竄等について 311件の報告があった。

[1/1-3/31: 96件、4/1-6/30: 103件、7/1-9/30: 67件、10/1-12/31: 45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]

CDE ToolTalk に含まれる脆弱性に関する注意喚起
80番ポート (HTTP) へのスキャンの増加に関する注意喚起
BSD 系 OS の lpd に含まれる脆弱性に関する注意喚起
Linux の telnetd に含まれる脆弱性に関する注意喚起
"Code Red" Worm の変種に関する注意喚起
"Code Red" Worm の伝播活動再開に関する注意喚起
telnetd に含まれる脆弱性に関する注意喚起
SSH のパスワード認証の脆弱性に関する注意喚起
Microsoft IIS の脆弱性を利用し伝播する Worm 関する注意喚起
Solaris の NIS プログラム ypbind に含まれる脆弱性に関する注意喚起
Solaris のプリンタデーモンに含まれる脆弱性に関する注意喚起
Microsoft IIS Index Server に含まれる脆弱性に関する注意喚起

Solaris に感染し Microsoft IIS を攻撃するワームに関する注意喚起
DDoS の踏台およびBINDなどのセキュリティ上の弱点に関する注意喚起
Web ページ改ざんに関する注意喚起

[更新]

BIND のセキュリティ上の弱点に関する注意喚起(続報)

② 緊急報告

[新規]

Microsoft IIS の脆弱性を使って伝播するワーム "Code Red II"
Microsoft IIS の脆弱性を使って伝播するワーム
Solaris に侵入し Microsoft IIS を攻撃するワーム
Microsoft IIS バージョン5.0 のセキュリティ上の問題について
Linux Worm に関する緊急報告

[更新]

Microsoft IIS の脆弱性を使って伝播するワーム "Code Red II" (更新)
Microsoft IIS の脆弱性を使って伝播するワーム (更新)
Microsoft IIS の脆弱性を使って伝播するワーム (更新)
Microsoft IIS バージョン5.0 のセキュリティ上の問題について (URL の訂正)
Microsoft IIS バージョン5.0 のセキュリティ上の問題について (更新)

③ 技術メモ

[更新]

Web ページの改竄に対する防衛 (Version 4)
サービス運用妨害攻撃に対する防衛 (Version 3)
コンピュータセキュリティインシデントへの対応 (Version 3)
関係サイトとの情報交換 (Version 3)
sendmail バージョンアップマニュアル (Version 11)
電子メール配送プログラムの不正利用 (予期しない中継) - (Version 5)

④ 活動概要（届出状況等の公表）

発行日: 2002-01-23 [2001年10月1日 ～ 2001年12月31日]
発行日: 2001-10-23 [2001年7月1日 ～ 2001年9月30日]
発行日: 2001-07-26 [2001年4月1日 ～ 2001年6月30日]
発行日: 2001-04-26 [2001年1月1日 ～ 2001年3月31日]

⑤ JPCERT/CC レポート

[発行件数] 31件
[取り扱ったセキュリティ関連情報数] 106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。

アクセス制御機能に関する技術の研究開発の状況

不正アクセス行為の禁止等に関する法律（平成１１法律第１２８号）第７条の規定に基づき、アクセス制御機能に関する技術の研究開発の状況を次のとおり公表する。

１．国の予算で実施しているもの

警察庁、総務省又は経済産業省のいずれかの予算で実施している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る。具体的には、国立研究所で実施している研究、国からの委託研究、国からの補助事業により実施している研究等である。

実施テーマは以下のとおりであり、その研究開発の概要は、別添１のとおりである。

インターネットアプリケーションのセキュリティ脆弱性に関する研究
ネットワーク侵入検出システム IDA(Intrusion Detection Agent System)の研究開発
情報通信危機管理基盤技術の研究開発
暗号アプリケーションプログラムインターフェース技術基盤の研究開発
出所不明のパケット流出を許さないセキュアな情報通信ネットワークの研究開発
次世代証拠基盤に関する研究開発
情報セキュリティ高度化のためのデータ保護技術に関する研究開発
相互接続時のセキュリティポリシの管理技術に関する研究開発
属性認証を用いたサービスの相互接続技術に関する研究開発
不正アクセス発信源追跡技術に関する研究開発

２．民間企業で研究を実施したもの

平成１３年１１月１９日から１２月１４日までの間に、アクセス制御技術に関する研究開発状況を募集した。その間の応募者は以下のとおりであり、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申告のあった内容をそのまま掲載している。

ＲＳＡセキュリティ（株）
エヌサイファー・コーポレーション
エヌ・ティ・ティ　アイティ（株）
エヌ・ティ・ティ・コミュニケーションズ（株）
エヌ・ティ・ティ・ソフトウェア（株）
（株）データコントロール
（株）東芝
（株）ドリームウェア
日本オラクル（株）
（株）日本システムディベロップメント
ベリマトリックス・ジャパン（株）
（株）山武
（株）山田洋行
（株）ランデック
（株）ローレルインテリジェントシステムズ

対象技術　その他の認証技術

テーマ名　インターネットアプリケーションのセキュリティ脆弱性に関する研究

開発年度　平成１２年度から

実施主体　独立行政法人　産業技術総合研究所　情報処理研究部門

背景、目的

近年、インターネット向けのサービスが、Web アプリケーションで運用されることが多くなってきた。それらは各サイトで個別に製作されているため、そのアクセス制御の安全性はサイト任せとなっている。そこには実効的な安全基準は存在せず、個人情報を漏洩したり、成り済ましアクセスを許してしまう欠陥のあるサイトが現実に多数存在している。こうした個別の欠陥の問題は、新技術の開発というアプローチで回避できるものではなく、開発および検収に携わる現場の技術者がアクセス制御方式について正しい知識を持つ以外に解決の道はない。この研究は、実在した欠陥の原因を分析し、対策のための技術情報を広く公表することで、同じ欠陥が再生産される事態を防止することを目的とする。

研究開発状況（概要）

平成 12 年度の成果：

国内 18 ヶ所の Web メールサービスのうち 7 ヶ所に、URL に含まれるセッション ID が漏洩することが原因で、メールの内容を盗み見られる欠陥があることを指摘した。「REFERER 問題」として広く知られることとなり、他のいくつかのサービスにおいても同様の欠陥が自発的に修正された。

平成 13 年度の成果：

クロスサイトスクリプティング脆弱性について調査し、国内の著名なサイト 8 ヶ所において、この脆弱性が原因で、個人情報（住所、電話番号、誕生日等）が漏洩するほか、3 サイトではクレジットカード番号が盗まれ得る状態であることを確認した。また、オンラインマーク、プライバシーマーク取得事業者から無作為に抽出した 50 サイト、銀行、証券 23 サイトを対象に調査したところ、その約 8 割に同脆弱性が残存していることを確認した。10 月には、経済産業省から、この問題について周知徹底を図るよう、関係団体に要請する通知がなされた。

現在の研究状況：

アクセス制御の欠陥には他にも様々の形態のものがあり、現在も調査を継続中である。

詳細の入手方法

これまでに公開された論文、資料等は下記の URL より入手可能。

http://SecurIT.etl.go.jp/

将来の方向性

アクセス制御方式の欠陥を機械的に検出する診断ソフトウェアの研究開発。システム評価のための実効的な安全基準の策定。

対象技術　侵入検知技術

テーマ名　「ネットワーク侵入検出システム IDA（Intrusion Detection Agent system）の研究開発」

開発年度　平成９年度～平成１０年度

実施主体　情報処理振興事業協会技術センター（研究協力機関：早稲田大学、日本総合研究所、SRA、上越教育大学）

背景、目的

インターネットの普及に伴い、不正アクセス行為も増加している。不正アクセス行為は他人のシステムに不正に侵入し、ファイルの改ざん、サービスの妨害等を行う行為であり、ネットワークに繋がっているどのサイトでも起りうる可能性がある。こうした不正侵入に対処するため、どのサイトにも導入可能な、独自の侵入検出システム IDA を研究開発する。

IDA は、ホストベースのネットワーク侵入検出を目的としたシステムであり、従来の侵入検出システム(IDS)のように、ネットワーク上に分散したホストのログをサーバに集中させたり、頻繁なアップデート等を行うことなく、モバイルエージェントによって必要な情報のみ収集することにより、それを解析してシステムに重要な被害を与える攻撃を重点的に検出するシステムである。

また、複数のサイトを踏み台としてシステムに侵入する不正アクセスも増加していることから、不正アクセスの起点を追跡する機能についても併せて開発を行う。

研究開発状況（概要）

(1) リモートアタック検出機能

軽量でかつ未知のリモートアタック（システム上になんら権限を持っていない状況からの侵入）を検出可能な手法を研究開発し、侵入検出システム IDA 上に実装する。軽量化のために、「痕跡」という侵入に付随して発生する事象からの検出から侵入解析を始める。痕跡検出後の侵入判定手法として、多変量解析の一分野である判別分析を用いている。これにより未知のリモートアタックも検出可能になる。

(2) インターネット上の侵入追跡機能

踏み台の起点を追跡するための、情報公開サーバシステムの開発を行う。LAN 内の接続情報を分散処理し、踏み台を追跡するために必要な情報のみ Web サーバ上で公開する方式を開発する。公開情報をもとに、踏み台を追跡することが可能になる。

(3) IDS 保護のための機能

侵入検出システムそのものが攻撃対象になった場合の防御メカニズムを研究開発する。すなわち侵入判定に係わるプロセスや、ログファイル等の保護を行う。これはカーネルレベルでのアクセス制御を行うことによって実現する。この保護機能は IDA だけでなく、Linux ベースのホストベース IDS で実装可能である。

詳細の入手方法

これまでに公開された論文等は下記の URL より入手可能。また開発ソフトおよびマニュアルについても、同様の URL にて入手可能。

Http://www.ipa.go.jp/STC/IDA/jp/

将来の方向性

本研究で得られた「痕跡」に基づく検出手法および多変量解析による判定手法は、他の IDS ネットワークベース IDS も含む。

対象技術　侵入検知技術
テーマ名　情報通信危機管理基盤技術の研究開発
開発年度　平成１２年度～
実施主体　独立行政法人通信総合研究所
背景、目的 　我が国の電子政府構想の根幹を揺るがし、我が国経済の将来を背負う電子商取引などを危機的状況に陥れる不正アクセスやサイバーテロに対処するため、ネットワーク上に生じた異変を的確に検出・分析し、対策を提示する先端的要素技術を研究開発する。
研究開発状況（概要） 　今後極めて大きな市場が見込める電子商取引等のＩＴ市場の発展を阻害する恐れのある不正アクセスやサイバーテロを未然に防止するため、平成１２年度に、総務省通信総合研究所に、不正アクセス模擬実験装置等を備えたネットワークセキュリティ施設、危機管理用安全対策施設、検証実験用テストフィールド、の３つからなる情報通信危機管理研究施設を整備し、不正アクセス行為やサイバーテロを検証・再現し、対策を講じるための研究開発を開始した。平成１３年度にはこれらの施設を拡充し、不正アクセスに関する各種事例を記録し検証する方法の開発、およびサービス不能攻撃への対処方法の検討、等を進めている。また、不正アクセス模擬実験装置を実ネットワークに接続し検証する方法の研究開発、および電磁波漏洩対策に関する研究開発、等に着手する。
詳細の入手方法（関連部署名及びその連絡先） 　独立行政法人通信総合研究所　情報通信部門　非常時通信グループ　大野浩之 　電話　０４２－３２７－５５４２
将来の方向性 　ナショナルセキュリティや国民経済・生活に対する大きな脅威となってきている「サイバーテロ」や大規模不正アクセスに対抗する国家レベルのネットワーク危機管理技術の研究、標準化等を行い、現実のサイバーテロや情報戦争に対応できる技術の獲得を目指す。

対象技術　その他の認証技術
テーマ名　暗号アプリケーションプログラムインターフェース技術基盤の研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　日本電気株式会社（通信・放送機構(TAO)からの委託）
背景、目的 　政府・自治体、各企業における申請業務、調達・購買業務の電子化が数年内に本格化する動きにあり、電子文書の真正性や機密性を確保する電子署名技術、暗号化技術の重要性は日々増している。電子政府や電子商取引などのアプリケーションには、プラットフォームフリーの JAVA が採用され始めており、電子文書交換のための標準フォーマットについても XML が定着しつつある。 　しかしながら、アプリケーションの観点から見ると、プラットフォームフリーといえども署名・暗号化ライブラリとのインターフェース（暗号 API）は未だ標準化に至らず、各々のアプリケーションが個別に対応しているため、互換性を損なっているのが現状である。また、XML 文書に対して暗号化を施した文書の格納フォーマット（以下、XML 暗号文書フォーマットという）も、アプリケーション毎に個別に定義しているため、XML 暗号文書の相互運用性も確保できない。 　そこで、電子政府システムや電子商取引システムなどへの適用を想定して XML 暗号文書フォーマットを策定し、JAVA 実行環境における電子署名、暗号化処理を実現するアーキテクチャに関する技術開発を実施する。
研究開発状況（概要） ・今年度から以下の研究開発を実施中。 (1)XML 文書に対する署名・暗号インターフェース (2)Web クライアントのブリッジ機能 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先） 通信・放送機構（http://www.shiba.tao.go.jp）
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　その他の認証技術
テーマ名　出所不明のパケット流出を許さないセキュアな情報通信ネットワークの 研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　株式会社東芝（通信・放送機構(TAO)からの委託）
背景、目的 電子投票など、サーバに多数のコネクションが集中するケースでは、DoS(Denial of Service)攻撃等のサイバー攻撃によって、サービスが致命的なダメージを受ける危険性がある。そのため、サーバ自体にコネクションを張る前の段階で、不正な通信を排除することが求められる。 また、不正な通信と正しい通信を判別するためには、利用者認証と機器認証を組み合わせるなどの方法によって、より厳密な認証を実現することが望まれる。 これらの技術の実現によって、不正な通信をより早期に発見・遮断し、ネットワークの不正利用防止と重要システムの保護を可能とする研究開発を実施する。
研究開発状況（概要） ・今年度から以下の研究開発を実施中。 (1)ネットワーク層における段階的な利用者・機器認証を行うプロトコルの研究　開発 (2)上記プロトコルを用いたポリシベースの各種管理技術 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先） 通信・放送機構（http://www.shiba.tao.go.jp）
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　その他の認証技術
テーマ名　次世代証拠基盤に関する研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　株式会社日立製作所（通信・放送機構(TAO)からの委託）
背景、目的 　電子政府の実現には、電子文書の証拠性が必須であるが、電子文書の証拠性確保は電子署名などの暗号技術に依存しており、20～30 年以上の期間にわたって証拠性を確保しない限り、これらの電子文書は補助的にしか扱うことはできない。また、電子文書の保存のみならずネットワーク上の様々な行為などの証拠性の確保も、電子文書の証拠性を長期間維持する基盤技術の実現の研究として実施する必要がある。本研究では、以上に対応する技術開発を実施する。
研究開発状況（概要） ・平成 13 年度から以下の研究開発を実施中。 (1)電子文書の証拠性を長期にわたって維持する技術 (2)証拠保存構築技術の正確な実行を保証する基盤技術 (3)証拠情報に対するアクセス制御に関する研究開発 (4)証拠性保証システムにおけるネットワークモデルの研究開発 (5)ヒューマンインターフェイスの研究開発 ・平成 15 年度末までに上記研究開発完了
詳細の入手方法（関連部署名及びその連絡先） 　通信・放送機構（http://www.shiba.tao.go.jp）
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　侵入検知技術
テーマ名　情報セキュリティ高度化のためのデータ保護技術に関する研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　三菱電機株式会社、株式会社富士総合研究所、リコーシステム開発株式会社、東京工業大学、エヌ・ティ・ティ・コミュニケーションズ株式会社、　日本電気株式会社（通信・放送機構(TAO)からの委託）
背景、目的 ネットワーク上の資源は、ネットワーク機器やサーバ・クライアント装置などのハードウェア、ハードウェア上で様々なサービスをネットワーク利用者に提供するアプリケーションなどのソフトウェア、そして利用者のユーザデータに大別できる。ハードウェアとソフトウェアは、サイバー攻撃により破壊を受けても入れ替えることで修復することが可能であるが、人間の知的生産の結果であり各ユーザにとって最も重要な資産であるユーザデータは、バックアップがない限り再生することは不可能である。 さらに、次世代インターネットプロトコルである IPv6 では、ユーザは特別の知識なしに情報機器等をネットワークに接続し、その利便性を享受できる反面、グローバルネットワークアドレスの使用により、LAN 内に置かれたユーザデータに対するサイバー攻撃の危険性が増加すると考えられる。 以上のように、ネットワーク上に存在するユーザデータをどのように守るかが重要な課題となりつつあることから、サイバー攻撃に対して耐性を持つネットワークとして、保存装置等の周辺機器が OS の管理から独立して動作することで、データに対する不正アクセスの防止、データの保存、復旧を図るためのアーキテクチャを研究・開発し、さらにこのアーキテクチャを保存装置以外の周辺機器に応用し、セキュリティ面で高機能な外部装置を開発することを目的とする。
研究開発状況（概要） ・平成 13 年度から以下の研究開発を実施中。 (1)データ保護機能を有する電子保存技術 (2)データ保護機能を有する分散環境自動構築技術 ・平成 15 年度末までに上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先） 通信・放送機構（http://www.shiba.tao.go.jp）
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　その他の認証技術
テーマ名　相互接続時のセキュリティポリシの管理技術に関する研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　富士通株式会社、九州大学、株式会社富士通プライムソフトテクノロジ　（通信・放送機構(TAO)からの委託）
背景、目的 電子政府や電子商取引など、異なるネットワークのインターネット相互接続ニーズが高まる中、相互接続時のセキュリティレベルの一貫性の確保が大きな問題として認識されている。この問題への対応として、特定のサイトで集中的にセキュリティ管理を行う方法があるが、このような方法は非常に大きな負荷の集中を招きやすく、スケーラビリティの問題が指摘されている。 また、将来的には、パソコンだけでなく全ての携帯電話や PDA(Personal Digital Assistants)などが P2P(Peer to Peer)型のネットワークを構成する可能性もある。 このような莫大な数のネットワークの相互接続と将来的な分散ネットワーク環境を念頭に、集中管理型ではなく自律分散型でネットワーク相互間のアクセス制御を実現し、セキュリティレベルの一貫性を確保するセキュリティシステムの開発を実施する。
研究開発状況（概要） ・平成 13 年度から以下の研究開発を実施中。 (1)相互接続時のセキュリティポリシ管理技術に関する研究開発 (2)標準化活動と普及促進に向けた各種研究開発 ・平成 15 年度末までに上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先） 通信・放送機構（http://www.shiba.tao.go.jp）
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　その他の認証技術
テーマ名　属性認証を用いたサービスの相互接続技術に関する研究開発
開発年度　平成 13 年度～平成 15 年度
実施主体　株式会社日立製作所（通信・放送機構(TAO)からの委託）
背景、目的 　電子政府、商行為、組織内業務など、将来的には非常に多くの分野で各種の電子申請、取引行為が実施されるものと思われる。このとき、特定の資格を持った人の申請機能や特定の会員・組織に属する人に限ったアクセス制御機能が必要になるが、本研究では、単独のサービス内に閉じた申請ではなく、複数の独立したサービスが連携することによって新たなサービスを提供するという、サービスの相互接続を前提とした電子申請に対応した技術開発を実施する。
研究開発状況（概要） ・今年度から以下の研究開発を実施中。 (1)資格証明機能の拡張技術 (2)アプリケーション利用時の制御技術 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先） 通信・放送機構（http://www.shiba.tao.go.jp）
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	侵入検知技術
テーマ名	不正アクセス発信源追跡技術に関する研究開発
開発年度	平成１１年度～平成１３年度
委託先	株式会社エヌ・ティ・ティ・データ 東日本電信電話株式会社　　（通信・放送機構（TAO）からの委託）

背景、目的

・　インターネットを活用した電子商取引等の高度なアプリケーションの発展のためには、その基盤インフラであるインターネットが、不正アクセスの侵害的行為の脅威から守られ、安全性が確保されていることが重要であり、不正アクセスそのものを抑止するような研究開発が求められている。

・　そこで、個々のネットワークに監視ツールを導入する等、不正アクセスを監視する技術、及び、監視情報をもとに不正アクセス発信源の追跡を可能とするような技術に関する研究開発を行い、インターネットの安全・信頼性の向上に寄与することを目的とする。

研究開発状況（概要）

・　平成１１年度より以下の研究開発を実施中。

（１）　パケット発信源追跡に関する研究開発

（２）　次世代不正アクセス検知技術の研究開発

（３）　発信源追跡技術の不正利用防止技術の研究開発

・　平成１３年度末に開発終了予定。

詳細の入手方法（関連部署名及びその連絡先）

・　通信・放送機構　（http://www.shiba.tao.go.jp/）

・　総務省総合通信基盤局データ通信課　（０３－５２５３－５８５４）

将来の方向性

・　不正アクセスを抑止し、セキュリティの高いインターネットを実現するため、当該技術の標準化を目指す。

企業名（及び略称）RSAセキュリティ株式会社	
代表者氏名　山野　修	
所在地（郵便番号及び住所）〒100-0005 東京都千代田区丸の内1-3-1　東京銀行協会ビルヂング13F	
関連部署名及び電話番号　マーケティング統括本部　　（03）5222-5240	
ＵＲＬ　http://www.rsasecurity.co.jp	
対象技術	技術開発状況
時刻によって変化するパスワードを生成するアルゴリズムとその認証方法 1985 年	一定間隔(通常一分)で変化する乱数を、その時点での時刻と秘匿されている番号から一定のアルゴリズムで生成し表示するカード型のデバイスを、認証を希望する利用者側に配備し、利用者は認証希望時にその時表示されている乱数をパスワードとして認証側に送付する。認証側、例えば一般のアプリケーションは送付されたパスワードを別途設置された認証装置に転送して認証の代行を依頼し、その回答により認証の可否を決定する。認証装置は、パスワード受信時の時刻と予め登録されている当該利用者の秘密番号から利用者デバイスと同じアルゴリズムで乱数を生成し、送付されたパスワードの妥当性（一致）を検証し結果を回答する。利用者デバイスと認証装置間の時計の差を補償するため、認証装置では、前回認証時までの累積時間差を記憶し乱数生成時に時刻を調整したり、許容できる範囲の複数の時刻について乱数を生成し、いずれかとの一致を確認して認証を許可するなどの処理を行う。

企業名（及び略称）nCipher Corporation Ltd (エヌサイファー・コーポレーション)	
代表者氏名　Alex van Someren (アレックス・ヴァン・ソマレン)	
所在地（郵便番号及び住所）Jupiter House, Station Road, Cambridge, CB12JD, UK	
関連部署名及び電話番号　英国本社　　+44-122-372-3602, 日本代表事務所　　03-5456-5486	
ＵＲＬ http://www.ncipher.com	
対象技術	技術開発状況
その他認証技術 １９９６年 （1及び2） ２０００年 （3）	以下の１)～３)を組合せてファイアウォールの内外からの不正アクセス行為を阻む環境を構築する。(FIPS 140-1 Level3 認定取得済) １）　ハードウェア（HSM:Hardware Security Module）により階層化された秘密鍵情報を管理をするため、ネットワーク上やサーバーのメモリー　にさえ秘密鍵情報が残ることがない。 ２）　複数のスマートカードと HSM にファームウェアとして内蔵されたロジックにより、鍵管理ポリシーや鍵のバックアップとリカバリーを効率的に可能にする。 ３）　アプリケーションまたはコンテンツの一部をセキュリティ・コードとしてHSMに内蔵することによるアプリケーションまたはコンテンツへの直接のアタックを不可能にする。

企業名（及び略称）　エヌ・ティ・ティ　アイティ株式会社（NTT-IT）	
代表者氏名　　橋田　幸雄	
所在地（郵便番号及び住所）〒231-0032 横浜市中区不老町2-9-1　関内ワイズビル	
関連部署名及び電話番号 ITソリューション事業部　045-651-7514	
ＵＲＬ http://www.ntt-it.co.jp/	
対象技術	技術開発状況
その他の認証技術	ワンタイムパスワード認証技術技術－PERM認証－ 毎回の認証の度に、パスワードを変更することにより、ネットワーク途中でのパスワードの盗聴に対してセキュリティ耐性の強い認証方法としてワンタイムパスワード認証方式がある。ワンタイムパスワード認証は、サーバとの間で時間同期する方式（例えば一定時間毎にパスワードをサーバとクライアントで特定演算により更新）とチャレンジレスポンス方式（サーバから与えられたチャレンジコードに対してクライアント側で特定演算した結果を返送）があるが、PERM認証は、後者の方式を採用しており、かつ、ソフトウェアで簡易に実現でき安全性が高い方式として技術開発した。 本PERM認証を用いた応用例として、暗号転送メールPop-up MAILを技術開発している。Pop-up MAILは、会社に届いたメールを一旦、暗号した後、ファイアウォールの外にあるPop-upメールサーバに転送して、事前に登録した利用者は、社外からその転送サーバにアクセスして本人あてのメールを確認したり返信したりできる。社外からファイアウォールに穴をあけずに、社外からメールを確認でき、かつ、暗号化されているため他人に見られる心配のない転送メールである。転送サーバにアクセスする際、本人確認のためにPERM認証方式を適用している。 関連ホームページ： http://www.ntt-it.co.jp/goods/1ji/int/popup/index.html

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　　鈴木　正誠	
所在地（郵便番号及び住所）〒100-8019　東京都千代田区内幸町一丁目１番６号	
関連部署名及び電話番号：ソリューション事業部ｅ-ガバメント営業部　03-6700-7305 ソリューション事業部プラットフォーム技術開発推進部　03-6700-9977	
ＵＲＬ　http://www.ntt.com/	
対象技術	技術開発状況
侵入検知技術（H11.7開発）	以下の１）～５）を組合せて不正侵入を体系的に防止する技術。 １）セキュリティポリシ／スタンダード／マニュアル等の規定作成技術：ポリシーの規定の他、具体的な保護策を記述するスタンダード、利用規定を考慮したマニュアル等を体系的に作成する技術。 ２）セキュリティ要件を満たしたＳＩ技術：必要なセキュリティ要件を洗い出し、セキュリティ要件を満たした設計、構築を行なう技術 ３）セキュリティホール調査技術：CERT、CIACの報告だけでなく、独自のデータベースによる方法で500種類以上の擬似攻撃を準備し、弱点を明確にする技術。 ４）運用者向けのトレーニング：運用システム部門担当者を対象としたセキュリティ基礎教育を体系的に行なう技術。 ５）ログ解析／モニタリング：200種類以上の項目を網羅したFWログ解析、300種類以上の監視項目に対応した24時間対応不正アクセス監視を行なう技術。
その他の認証技術（H12.8開発）	e-Security ASP：インターネットを使った情報提供やＷｅｂ業務アプリケーションといったＷｅｂベースのプライベートネットワーク構築に欠かせない認証／認可（シングル・サイン・オン）や暗号化通信を実現するアプリケーションを複数ユーザで利用するＡＳＰ。（関連HP　http://www.ntt.com/managed/）

企業名（及び略称） エヌ・ティ・ティ ソフトウェア株式会社	
代表者氏名 鶴保 征城	
所在地（郵便番号及び住所）〒231-8554 横浜市中区山下町233-1	
関連部署名及び電話番号 eエンタープライズ事業部 ／ 03-5782-7261	
ＵＲＬ http://www.ntts.co.jp/	
対象技術	技術開発状況
（注２） その他の認証技術	（注３） シングルサインオン認証と統合アカウント管理に関する技術 1.シングルサイン：クライアントから様々なＯＳ、アプリケーションへのログオンを自動化、実アカウント／パスワードを隠蔽化 2.アクセスコントロール：Ｗｅｂコンテンツに対して、ディレクトリ単位でのユーザアクセス制御 3.ユーザ認証：クライアント利用者を特定し、認められたユーザ以外のログオンを否認 4.アカウント集中管理：各種ＯＳ、アプリケーションのアカウント情報の一元管理（作成、変更、削除） 5.ポリシーベースの統合ユーザ管理：ディレクトリ技術を用いて、組織と個人、権限を効率的に管理 6.ログの収集：各ＯＳ、アプリケーションへのアクセス状況（ログオン成功、失敗など）のログの収集

企業名（及び略称）株式会社データコントロール	
代表者氏名　原　健人	
所在地（郵便番号及び住所）〒106-0032 東京都港区六本木 2-2-8 ケルビンビル 5 階	
関連部署名及び電話番号　部署名：営業本部 営業部　電話：03-3582-2110	
ＵＲＬ　http://www.datacontrol.co.jp/	
対象技術	技術開発状況
ファイアウォール技術	弊社は米国 WatchGuard 社（本社：ワシントン州シアトル市）からインターネット接続用ルータと社内ネットワークの間に設置するだけで、簡単にインストールする事ができるプラグアンドプレイのファイアウォール専用ハードウェアセキュリティ製品、WatchGuard FireboxIII シリーズを輸入し、販売をおこなっています。機能としてはパケットフィルタリングや、アプリケーションプロキシ等のファイアウォール機能に加え、スタティック/ダイナミック NAT（IP マスカレード）のネットワークアドレス変換、NT PDC、RADIUS、内部認証等のユーザ認証、CyberPatrol による Web アクセス制御が有ります。 販売にあたって、弊社では販売後のインストールサービス（システムインテグレーション含む）やダイレクトサポートサービスがあり、万一、故障が生じたときの修理サポートもご用意しています。（参照：米国 WatchGuard ホームページ http://www.watchguard.com）

企業名　　株式会社　東芝	
代表者氏名　　取締役社長　岡村　正	
所在地　　〒105-8001　東京都港区芝浦一丁目１番１号	
関連部署名及び電話番号　　ｅ－ソリューション社　渉外担当　03-3457-2652	
ＵＲＬ　www.toshiba.co.jp	
対象技術	技術開発状況
１．ファイアウォール技術	・CheckPoint 社のパケットフィルタリングベースのソフトウェアファイアウォールを当社ハードウェアと一体化し運用を容易にしたファイアウォール技術（2000 年開発）
２．侵入検知技術	・Web サーバに対するリクエストを既知不正アクセスのパターンと比較し、不正アクセスには即座にそのセッションを遮断することによって Web サーバの安全性を高める侵入検知・防御技術（2000 年開発） ・Internet Security Systems 社のセキュリティ監視ツールを利用してセキュリティ監視システムを構築するサービス技術（2000 年開発） ・Web サーバの通信状態や負荷状態を監視することにより、Web サーバに過剰な負荷をかけ、Web サーバ機能をダウンさせる DoS 攻撃や DDoS 攻撃を検出・防御する技術（2001 年開発）
３．その他認証技術	・インターネット標準の公開鍵基盤（PKI）認証を実現する認証局システムを VeriSign 社製品などを利用して構築するサービス技術（1999 年開発） ・Web サーバにおける公開鍵認証や S/MIME 対応の IC カードシステム技術（2000 年開発）

企業名（及び略称）	株式会社ドリームウェア
代表者氏名	稲山光一
所在地（郵便番号及び住所）〒160-0023	東京都新宿区西新宿8-14-24 西新宿KFビル7F
関連部署名及び電話番号	03-5337-3301
ＵＲＬ	http://www.logsaver.jp/　http://www.dreamware.jp/

対象技術	技術開発状況
ファイアウォール技術 2000年開発	Logsaverは、独自で開発したCD-Rへの保存技術を導入する事により、サーバ上で発生するログデータをCD-Rにリアルタイム保存することが可能です。 例えば、ハッカーによってハードディスク上のログファイルを改ざんされたとしても、Logsaverによって保存されたCD-Rのデータには改ざん前のデータを残すことができます。 CD-Rに保存する為、根本的に改ざん・削除することが不可能です。 また、独自の圧縮技術を使用して保存するので、1枚のCD-Rに3～5GBのデータを保存することが可能です。 対応OS：　SUN Solaris　Linux IBM AIX　WindowsNT4.0 HP-UX　Windows2000 Tru64Unix　等

企業名（及び略称）	日本オラクル株式会社
代表者氏名	新宅　正明
所在地（郵便番号及び住所）	〒102-0094 東京都千代田区紀尾井町 4-1 ﾆｭｰｵｰﾀﾆｶﾞｰﾃﾞﾝｺｰﾄ
関連部署名及び電話番号	システム製品マーケティング部　03-5213-6666（代表）
ＵＲＬ　http://www.oracle.co.jp/	

対象技術	技術開発状況
侵入検知技術 開発年：H13 年	■以下の２つの技術を組み合わせることで、不正侵入を検知する。 １）機密データに対するアクセスのみの監査を行うことで、システムへの侵入と機密データの窃取を検知する技術。 ２）機密データに対するアクセスがあった場合に、任意のトリガー（ロジック）を起動する技術。
その他認証技術 開発年：H12 年	■大規模ウェブアプリケーションの構築に不可欠なシングルサインオンを実現する技術。 ■大規模クライアントサーバーアプリケーションの構築に不可欠なシングルサインオンを実現する技術。 ■生体的特長を利用してデータベースに認証を行う技術。 ■IC カード等を利用してデータベースに認証を行う技術。 （関連 URL http://www.oracle.co.jp/9i/index.html）

企業名（及び略称）	株式会社日本システムディベロップメント（ＮＳＤ）
代表者氏名	取締役会長兼社長　内久保晋一郎
所在地（郵便番号及び住所）	〒163-0777 東京都新宿区西新宿 2-7-1 新宿第一生命ビル
関連部署名及び電話番号	東京システム営業９部　03-3342-0457
ＵＲＬ　http://www.nsd.co.jp/dst	

対象技術	技術開発状況
その他認証技術 （HTML ページに対するアクセス制御） （開発年 2000 年）	PKI 技術を用いた X.509 の電子証明書によるクライアント認証技術を用いて、Web サーバのコンテンツ（HTML ページ）に対するアクセス制御を実現します。 WEB サーバ側で、どのコンテンツにどの電子証明書がアクセス可能なのかをデータとして保持し、クライアントからのアクセス毎に、その情報をチェックして、アクセスの制御を行います。 複製不可能な、電子証明書を用いて、よりセキュリティレベルの高いアクセス制御が可能です。 サーバ側のソフトウェアは、Web アプリケーションに依存せず、その上位で動作するため、より強固なアクセスコントロールを実現することが可能です。

企業名(及び略称)	ベリマトリックス・ジャパン株式会社
代表者氏名	代表取締役社長　森　勉
所在地(郵便番号及び住所)	〒150-0014　東京都港区芝2-13-4 JBP芝ビル15F
関連部署名及び電話番号	営業本部　コンテンツ営業部　03-5730-3117
ＵＲＬ	http://www.verimatrix.co.jp

対象技術	技術開発状況
その他認証技術 開発年：2001年	■ 著作権/著作隣接権など財産権を管理する企業向けコンテンツ認証技術 著作権のあるオリジナルコンテンツに認証を行うための電子透かし技術、電子ファイルを暗号化してデータベースに保存する電子認証システム、配信事業者向けに販売権の許諾を行なうシステムを含むコンポーネントを提供。 （CopyCert Manager for Right Ownersの製品情報を参照 ） ■ 許諾コンテンツを消費者向けに配信/販売する事業者向け配信システム 権利者からの電子ファイルの許諾申請や電子証明書の発行/管理を行なえるGUI、許諾コンテンツに販売時の認証を行なうための電子透かし技術、WEBシステムとの連動サポートを行なうシステムを含むコンポーネントを提供。 （CopyCert Manager for Distributorsの製品情報参照 ） ■ 会社のドメインに対して不正アクセス調査をする技術 会社等のドメインに対して不正アクセス調査をするサービスで、許可された軍事技術を民間転用したものを応用しています。これはお客様との一定のご契約のもと、社内システムに認証システムを設置し、様々な不正アクセスの有無を調査/監視を続けるサービスです。違法性のあるコンテンツを送受信した端末のIPアドレスやそのコンテンツ自体の違法性を証明するレポートなどをご契約いただいた企業経営者様にご提供いたします。基本的には社内システムには一切手を加えずに調査を実施し、監視を続けます。社内の機密文書など登録された重要書類等を外部へのメール添付での送付や許可されていない印刷またはフロッピーディスクへのコピーなどを禁止または記録することサービスも提供しています。（ DomainWatchのサービス情報を参照 ）

企業名（及び略称）	株式会社　山　武
代表者氏名	佐　内　大　司
所在地（郵便番号及び住所）	〒251-8522　藤沢市川名１－１２－２
関連部署名及び電話番号	SecurityFriday　0466-20-2430
ＵＲＬ	http://www.securityfriday.com

対象技術	技術開発状況
侵入検知技術 （2000 年）	ローカルネットワーク上の電子計算機に侵入、または不正利用し、ネットワーク上のパケットを不正に収集しているネットワーク盗聴ノード（プロミスキャスモードにあるノード）を、ARP パケットを用いてリモートから検出する技術を開発した。 この技術の使用により、稼動中のネットワークに影響を与えることなく、ローカルネットワーク上のネットワーク盗聴ノードを検出することができる。

企業名（及び略称）株式会社　山田洋行	
代表者氏名　山田　正志	
所在地（郵便番号及び住所）〒150-0002　渋谷区渋谷２－１０－６	
関連部署名及び電話番号　情報通信システム部　03-3475-1557	
ＵＲＬ http://www.fs-support.yamada.co.jp/	
対象技術	技術開発状況
ファイアウォール技術 (2001 年開発済)	F-Secure 社が開発した技術で、個々のクライアントマシンにインストールして、不正アクセスから保護します。集中管理機能を持つ F-Secure Policy Manager から、インストール／アップグレード／設定変更／アラート情報収集が可能なファイアウォール技術です。 サポートしているＯＳ　Win95/98/Me/NT4.0/2000
侵入検知技術 (2001 年開発済)	OmniSecure 社が開発した技術で、重要なデータが記憶されているファイルサーバーから、不正に情報が漏洩する事、情報が改ざん、破壊されることを VPDisk というソフトウェアをサーバーにインストールする事により防止出来ます。認定されたユーザーのみが、この重要なデータをアクセス出来ます。重要なデータは、リアルタイムに暗号化されてディスクに記憶される為に、このデータが外部に持ち出されても安全です。 サポートしているＯＳ　Solaris,Linux

企業名（及び略称）株式会社ランデック	
代表者氏名　代表取締役　鬼頭　行夫	
所在地（郵便番号及び住所）〒456-0032 名古屋市熱田区三本松町１５-１３	
関連部署名及び電話番号　システム営業部　052-889-1472	
ＵＲＬ　www.landec.co.jp　mail@landec.co.jp	
対象技術	技術開発状況
ファイアウォール技術	変動グローバルアドレスを Web-Server の IP フィルタリングを行う技術。 《用途》 ADSL・ケーブル TV などのインフラはグローバルアドレスが変動する。 固定アドレスのあるインフラであれば、インターネット経由であっても Web-Sever 側に IP をフィルタリングする機能（機構）を持たせれば、初期段階のファイアウォールゲートウェイが可能になる。ADSL などの変動するアドレスのファイアウォールゲートウェイを今回開発した。 《詳細技術》 コンピュータには世界に 1 個しか無いアドレスがある。その内のひとつ MAC アドレスを FTP によりインターネット送信する。受信先は、前もって登録された MAC アドレスを照合し、確認した変動アドレスを通過する仕組みのプログラムである。（暗号化送信+ID+パスワードも照合する）

企業名（及び略称）株式会社ローレルインテリジェントシステムズ	
代表者氏名　長谷川　福重	
所在地（郵便番号及び住所）〒225-0002　神奈川県横浜市青葉区美しが丘 5 丁目 35 番 2 号	
関連部署名及び電話番号　　東京営業部　　03-5510-3010	
ＵＲＬ http://www.lis-fss.co.jp/index.html	
対象技術	技術開発状況
その他認証技術 本人認証技術 平成 10 年 9 月 開発完了	名称「(1) IC カードによる本人認証および（2）ネットワーク認証」 （1）IC カード（CPU 付）を利用し本カード内で、本人認証を行う。また、パスワード 6 回不正で IC カード自体が使用不可になるので、パスワードアタックおよびハッキングは困難。 （2）ICカードと認証サーバーによるチャレンジ/レスポンス方式（暗号/復号）を用いた自動ネットワーク認証を行う。 アクセスを希望する被認証側（クライアント）に認証側（認証サーバー）から暗号コード（チャレンジコード）を伝送し、クライアントにおいて、復号した演算結果を認証サーバーに伝送、サーバー側の演算結果と一致する場合のみアクセスを許容する。 暗号アルゴリズムは、当社開発の「SXAL/MBAL」（共通鍵方式）を使用している。