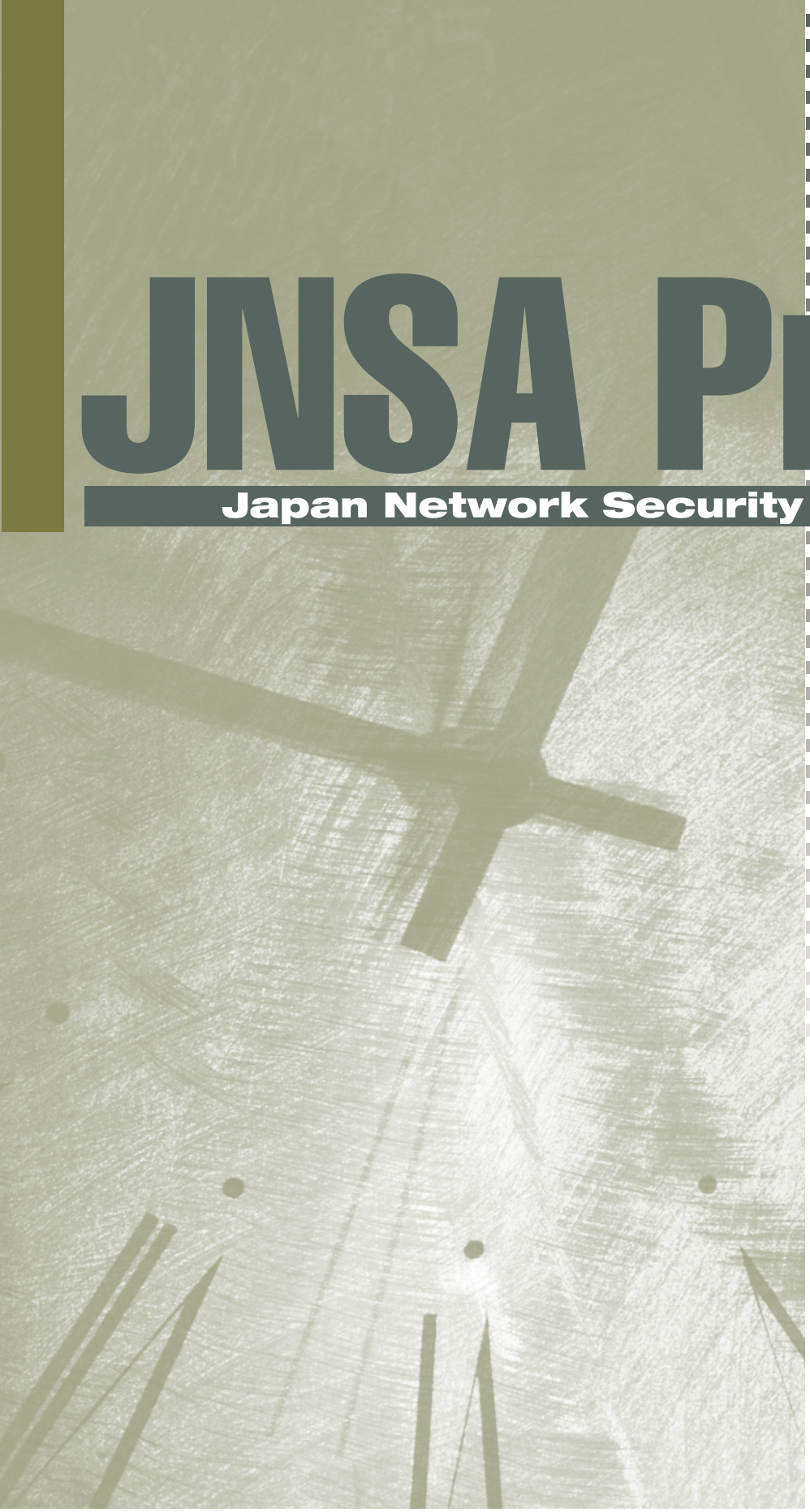


JNSA Press

Japan Network Security Association

Vol.11
August 2004

CONTENTS

特定非営利活動法人 日本ネットワークセキュリティ協会
NPO Japan Network Security Association

セキュアなネットワークのもたらす変革

シスコシステムズ株式会社 執行役員CTO / JNSA副会長
大和　敏彦

ネットワーク・セキュリティの重要性が益々高まっている。セキュリティ脅威の増大が一つの要因であるが、IPネットワークの広がりがもう一つの要因である。IPネットワークは、IP電話のように音声も統合し、ビジネスや生活を変革し続けている。

クリティカルなネットワーク応用例として、病院のネットワークが目指す変革をご紹介したい。先進病院ネットワークの狙いは、「患者中心で、安心で安全な医療」である。

核となるのが、電子カルテで、あらゆる診療情報を一元管理することによって、情報共有による高度で適切な医療の実現、患者とのコミュニケーションの向上、および医療の質の向上のためのトレーサビリティ、が実現されようとしている。医者の診断、検査、使用した薬等、あらゆる情報がリアルタイムでインプットされ、ネットワークを通じて統合される。容量が1Gバイトを越えるコンピューター断層撮影(CT)や磁気共鳴映像法(MRI)等の医療画像も、高速のネットワークで迅速にやり取りされる。ネットワークは、診療室、検査室、ナースステーションや事務室だけでなく、ベッドサイドまで広がる。高速ネットワークに接続されたベッドサイドのPCを使って、医者と患者が電子カルテを使って診療を進められる。ベッドサイドのインフラは、医者と患者の双方向コミュニケーション・ツールとして使われるだけでなく、患者への連絡や案内の提供、ビデオ放送等の娯楽に使うことができ、患者の満足度向上に役立てることが出来る。医療ネットワークの広がりは、さらに、遠隔地との音声、リアルタイム・ビデオを使った遠隔診断、遠隔医療支援へと応用分野を広げようとしている。これらのネットワークは、医療のあり方、仕組みを大きく変えていくものと考えられている。

このような応用で使われるネットワークには、情報漏洩への対策、ネットワーク・セキュリティの対策が、なくてはならないものであるし、またネットワークが止まることも許されない。止まらない、セキュリティ等の問題があってもすぐに回復する、かつ問題に対して自動的に対処できるようなネットワークが必要とされているのである。

新分野での活用は、まだまだ広がり、新しいネットワークの価値を生み出すものと思われる。その中で、JNSAがセキュアなネットワーク実現という形で、貢献していく事を期待したい。

法律家から見た個人情報漏洩問題

弁護士
尾崎　孝良

かつては、インターネットセキュリティ関連のインシデントといえば、ウイルス、不正アクセス・侵入、ハッキング・クラッキングというのが定番であった。しかし、昨今のセキュリティのインシデントといえば、個人情報の流出事故であり、しかも朝日新聞がまとめた「企業の個人情報の主な流出・紛失例」をみると

時期		企業名	規模
03年	6月	ローソン	56万人
	8月	アプラス	8万人
	10月	ファミリーマート	18万人
04年	1月	三洋信販	116万人
	2月	ソフトバンクBB	451万人
		シティバンク	12万人
	3月	ジャパネットたかた	30万人
		アッカ･ネットワークス	30万人
		東武鉄道	13万2000人
		サントリー	7万5000人
	4月	コスモ石油	92万人
		日本信販	10万人
	5月	三菱マテリアル	1000人
		ツノダ	3000人
	6月	阪急交通社	62万人
		良品計画	1124人
		Bs-i･P&G	1万人

（出典：http://www.asahi.com/special/privacy/index.html）

2004年前半だけですでに十数件の事故が発生し、各事件で数千人～数百万人までの個人情報が流出している。

中でも、500万人近く（最近の報道では実は660万人分だったともされている）の情報を流失してしまったYahoo! BB事件が最も深刻である。

■Yahoo! BB事件---470万件流出

本年2月24日ころ報道各紙に「Yahoo! BBから470万人分の個人情報が流出」との見出しが踊った。

当初、ソフトバンク側は「それら（470万件）がYahoo! BBユーザーのデータであるかどうかは確認していない」（宮内副社長）と述べ、同月25日から照合作業を開始した。

そして、同月27日、ソフトバンクは、警察から提供を受けたデータの照合結果について発表、451万7千件の個人情報が流出していたことを明らかにした。同社の孫正義社長は陳謝するとともに、Yahoo!BBのすべてのユーザに対し、500円相当の金券などを送るとした。

3月18日には、管理諮問委員会名で、報告書が発表された。その内容は以下のとおり。

・「正規アクセス権者からパスワードを漏らされた者」の侵入ではなく「正規アクセス正規パスワードによる犯罪目的利用」ではないかと結論づけた（なお、この点について、後に退職した者がパスワードを漏洩したことが判明）。

・データベースへアクセスするには、ID・パスワードを使う仕組みとなっており、ID・パスワードは、情報管理の担当者が、現場担当者からの請求に応じて、必要に応じる形で発行していた。2003年7月以降のパスワードは、4箇所のデータベースのいずれかにアクセスできるという意味でのアカウントを総計した場合に、135件発行されていた事実が報告され、内数件はグループ・アカウントとして発行されていたとのことであった。

・パスワードの管理方法については、セキュリティに関する注意規定が作成、公表されており、特にその中に「IDとパスワードの管理について」との文書が作成されており、管理教育が行われており、通常のパスワード管理体制は確立されており、ずさんな管理を行っていたとまではいえないと結論づけた。

・以上を前提に、顧客に対する500円のお詫び料の支払については、「相当な範囲にある」とした。

■ずさんな管理体制

ところが、5月30日ころになって、情報を漏洩した者とその協力者が判明。過去にソフトバンクBBで業務委託者としてシステム関連の業務に従事していた者（協力者）が、ソフトバンクBB株式会社のリモートメンテナンスサーバへアクセスするためのアカウントとパスワードを容疑者らに伝え、容疑者らは同サーバを経由して顧客データベースへ不正にアクセスし、顧客情報を持ち出したことが判明した。

協力者は2002年5月から2003年2月まで、ソフトバンクBB株式会社サービスオペレーション本部にて業務委託者として、ネットワークメンテナンスやサーバ構築業務に従事してた、という。協力者は業務における必要性から、リモートメンテナンスサーバへのアクセス権限を保有していた。また、顧客データベースへのアクセス権保有者170名（135アカウント）の中の1名。

つまり、既に退職していたにもかかわらず、IDパスをそのまま放置していた実態が明らかになったのだ。

さらに、6月18日なると、「（同容疑者が）同社のIP電話「BBフォン」の通話記録も引き出していたことが警視庁の調べでわかった。また、同容疑者が引き出したヤフーBBの顧客情報は、今年1月時点の登録者全員にあたる約660万人だったという。同社の情報管理のずさんさが改めて浮き彫りになった」（朝日新聞）と報道された。

以上のように、Yahoo! BB事件は、セキュリティ意識の甘い企業体質が通信記録といった極めてプライバシー性の高い情報を流出するという事態にまで発展してしまった事例である。

■個人情報保護法の概説

このような大事件が発生する中で法律の仕組みははどのようになっているのか。まず、最近各所で話題の個人情報保護法の内容についてみてみよう。

個人情報保護法は、昨年5月に成立し、来年4月の本格施行に向けて、関係省庁がガイドラインなどを策定しているところである。

この法律の目的は、「個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」（第1条）としている。

なお、インターネットではよく「この法律は、個人情報利用の有用性に配慮しつつも、個人のプライバシーに関する権利を保護していくことを目的にしている」との表現をみかけるが、誤りである。プライバシーと個人情報は（密接に関連するが）概念が異なる。

この法律における「個人情報」とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（2条1項）をいう。特定の個人を識別することができれば、公開情報であっても個人情報となる。たとえば名刺に記載されているような事項は（プライバシー情報とはなり得ないが）個人情報だ。

そして、「個人情報を含む情報の集合物」であって「電子計算機を用いて検索することができるように体系的に構成したもの」等を「個人情報データベース等」という（同条2項）

この「個人情報データベース等」を事業の用に供している者が、個人情報取扱事業者であり、主として個人情報取扱事業者がこの法律の各種規制を受けることになる。なお、「個人情報データベース等」を事業の用に供している者であっても、国の機関や公共団体は対象にならないし、また、「その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者」も除外されることになる。

これを受けて、政令2条で「法第二条第三項第四号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定

の個人の数の合計が過去6か月以内のいずれの日においても五千を超えない者」と規定した。したがって、過去6か月のうち、1日でもDB上の個人情報が5000件を超えてしまったら、個人情報取扱事業者となってしまうので注意が必要だ。

なお、法律相談や講演会の質疑でよく聞かれるのだが、①上記施行令2条の内容と、②法2条5項（その具体的内容は施行令4条で規定）で規定される「6か月以内に消去すれば同法上の保有個人データに該当しない」との例外規定とを混乱している方が多いようなのでここで注意を喚起しておく。すなわち、個人データを6か月以内に消去したとしても、ある1日のデータ量が5000件を超えていれば、個人情報取扱事業者となる（ただし、規制の多くは、「保有個人データ」を客体とするので、データを全部6か月以内に消去していれば法的規制をほとんど受けないといえる。上記法令を勘違いして、5000件を若干上回るデータを有している企業が、6か月以内にわずかな数を消して5000件を超えないようしても、当該企業は個人情報取扱事業者であり、その企業の保有する個人データについては個人情報保護法の規制対象となる）。

限られた企業のみとしか取引しない零細子会社以外、ほとんどの企業が規制対象となると考えてよい。

■個人情報取扱事業者の責務（OECD 8 原則に照らして）

個人情報を取得した個人情報取扱事業者は、取得・利用・管理のすべてのプロセスにおいて責任を負うことになる。

情報主体である個人の許可なしに、表示した目的以外の使用や、第三者への提供をしてはならない。また、個人情報取扱事業者は、管理体制を整備し、実施することが求められる。

個人情報取扱事業者に課せられる、主な義務をまとめてみよう。

個人情報保護の基本原則として、OECD（経済協力開発機構）が1980年9月23日「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（Recommendation of the Council concerning Governing the Protection of Privacy and Transborder Flows of Personal Data）としてまとめた、OECD 8 原則

①収集制限の原則（Collection Limitation Principle）
②データ内容の原則（Data Quality Principle）
③目的明確化の原則（purpose Specification Principle）
④利用制限の原則（Use Limitation Principle）
⑤安全保護の原則（Security Safeguards Principle）
⑥公開の原則（Openness Principle）
⑦個人参加の原則（Individual Participation Principle）
⑧責任の原則（Accountability Principle）

が国際的な基本原則となっている。個人情報保護法の政府の提案趣旨もこのOECD 8 原則に対応する形式で整理されているので、以下、趣旨説明資料（第156回国会）から引用しよう。

○ 目的明確化の原則
収集目的を明確にし、データ利用は収集目的に合致するべき

○ 利用制限の原則
データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない

- 利用目的をできる限り特定しなければならない。（第15 条）
- 利用目的の達成に必要な範囲を超えて取り扱ってはならない。（第16 条）
- 本人の同意を得ずに第三者に提供してはならない。（第23 条）

○ 収集制限の原則
適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき

- 偽りその他不正の手段により取得してはならない。（第17 条）

○ データ内容の原則
利用目的に沿ったもので、かつ、正確、完全、最新であるべき

・ 正確かつ最新の内容に保つよう努めなければならない。（第19 条）

○ 安全保護の原則

合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき

・ 安全管理のために必要な措置を講じなければならない。（第20 条）
・ 従業者・委託先に対し必要な監督を行わなければならない。（第21 、22 条）

○ 公開の原則

データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき

○ 個人参加の原則

自己に関するデータの所在及び内容を確認させ、又は意義申立を保証するべき

・ 取得したときは利用目的を通知又は公表しなければならない。（第18 条）
・ 利用目的等を本人の知り得る状態に置かなければならない。（第24 条）
・ 本人の求めに応じて保有個人データを開示しなければならない。（第25 条）
・ 本人の求めに応じて訂正等を行わなければならない。（第26 条）
・ 本人の求めに応じて利用停止等を行わなければならない。（第27 条）

○ 責任の原則

管理者は諸原則実施の責任を有する

・ 苦情の適切かつ迅速な処理に努めなければならない。（第31 条）

■罰則と行政指導法の限界

個人情報保護法の罰則についてみると、個人情報取扱事業者の違反行為には、最終的には、罰金などの罰則が科されることになる。違法行為是正の仕組みは以下のとおりだ。

まず、個人情報取扱事業者が上記各条の規定に違反した場合には、個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を、主務大臣が「勧告」することができる（34条1項）。

そして、この勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべく「命令」を発することになる（同条2項）。なお、緊急の場合は、1項の勧告をせずに命令を先行できる（同条3項）。

そしてこれらの「命令（34条2項又は3項）」に違反した者は、6か月以下の懲役又は30万円以下の罰金が科せられる（56条）。法人の役員や従業員が違反した場合は、両罰規定により法人にも罰金が科せられる（58条1項）

■情報漏洩に関する刑事法制

以上みたとおり、個人情報保護法というのは、法律の規定する「個人情報」（これは必ずしも知られたくないプライバシー情報とは限らない）を事業者が管理すべく、監督官庁が指導する行政指導法であって、この法律に基づいて企業が個人に損害賠償責任を負うことはない。

もちろん、法律の「理念」は、前述のとおり、OECDの8原則に準拠した妥当な内容となっているのだが、あくまで行政指導法であって、各個人に個人情報事業者に対する新たな権利を付与したものではない。

また、勧告→命令という手続きを経て悪質な命令違反がある場合には刑罰が科されることになるが、通常はそこまでいく前に、監督官庁の指導に服するだろう。

では、個人情報が流出したり、不正に利用された場合、それらの行為に対する罰則はあるのだろうか？

他人の情報を無断で盗み見ることは悪いことだというのは常識だろう。特に、他人に知られたくないプライバシー情報を勝手に入手してはいけない、誰もがそう思う

だろう。

しかし、社会常識とか道徳に照らして「悪いこと」がすべて「犯罪」として処罰されるかというとそうではない。

情報を勝手に「盗む」のだから単純に泥棒（窃盗罪）なのでは？と考える方も多いのだが、そう簡単ではない。

刑法235条窃盗罪の構成要件は、他人の占有する「財物」を不法領得の意図をもって自己の占有に移すことである。

ここで「財物」というのは有体物（形あるもの）のことをいう。唯一の例外は、電気エネルギーだ（刑法245条）。したがって、「情報」のような無体物は「財物」でない。情報窃盗は窃盗罪ではないのである。

話はそれるが、利益（債権）も財物ではないから、利益の窃盗も犯罪ではない。たとえば、レストランで最初はお金を払うつもりで注文し（最初から食い逃げするつもりだと詐欺罪になる）、レジのとこまで行ったらサイフが無いのに気づいて走って逃げた、という事案は、典型的な「利益窃盗」で刑法上の窃盗罪には該当しない（警察は、窃盗容疑で逮捕することはできない）。むろん、道義的には許されることではないので、決しておすすめはしないが。

企業内の情報が盗まれた場合、フロッピーやCD-R、印字した紙が企業の占有物であった場合、盗まれた財物に注目して窃盗罪として立件するのが実務的な運用である。情報を盗むこと自体は犯罪事実ではなく、企業の占有下にあるフロッピーとか紙という「財物」（ずいぶん安い「財物」ではあるが）を自己（犯人）の占有に移した事実をもって窃盗罪としている。そのフロッピーに重要な情報が入っていたというのは、情状（罪の重さを決める事情）となる。

したがって、メールやファイル転送を利用して情報を漏洩した場合、刑法犯にはなり難い。極端な話、情報を丸暗記して持ち出してしまえば、それがどんなに重要な情報であろうと犯罪扱いされることはない。

これだけ、情報が大きな価値を持つ時代になってしまったのに、法律が時代に追いついていないともいえる。

このようなコンテクストから、「新しくできた個人情報保護法というのは情報窃盗を取り締まる法規である」と勘違いする向きもあるようだ。このような解説をインターネット上での掲示板などで散見する。しかし、個人情報保護法は、後述するとおり、「個人情報取扱事業者」に課せられる事業者規制法である。刑法の窃盗犯の特別法ではない。おそらく、「情報の窃盗は取り締まることができない」という立法背景を読み違えた理解と思われる。

それでは、「刑法を改正して、情報も財物とすれば良いではないか」と考える方もいると思うが、事はそう簡単ではない。安易に情報窃盗を窃盗罪にすると、本屋の立ち読みなども該当してしまう。日常生活で無償で情報をもらう場面は意外と多いのだ。また、財物と異なり「占有」の認定が難しいので、いつ窃取したのかの認定も困難だ。

カメラ付き携帯電話の普及で、本屋で必要な情報を撮影するのが法的にどのように評価されるのか（刑法の立法論のほかに著作権法上の問題もある）、まだまだ議論の尽きないところであり、立法化は容易でない。

■贈収賄罪等の可能性

窃盗罪に該当しなくとも、他の罪に問われることがある。よくある類型は贈収賄だ。国家公務員やNTTなどの特殊法人が業務データを提供する見返りとして、金銭を受け取った場合収賄罪になる（金銭を渡した側は贈賄罪）。

ただし、民間企業同士ならどんなリベートを渡そうが贈収賄にはならない。

また、地方自治体では、個人情報保護条例を定めているところもある。後述の宇治市事件では、市の「電算組織に係る個人情報の保護に関する条例」に違反するとして、データを持ち出した外部委託業者を刑事犯として告訴した（ただし、特殊事情により不起訴処分となった。後述）。

要するに（NTTのような特殊法人を除く）民間企業から個人情報が漏洩しても刑事事件として立件することは

難しい。結果として、情報を漏らした者に対する制裁が十分できない。告訴すらできないという事態も考えられる。管理の甘かった企業に対する社会的な批判が集中する。その企業は、何ら事後対策をすることもできず信用を失うということになってしまうのが実態だ。

■不正競争防止法

以上のとおり、一般の企業や個人が秘密を漏洩しても何ら罰則規定も存しなかったのであるが、平成１６年１月から改正不正競争防止法が施行された。

改正法では、営業秘密の侵害に対する刑事罰の導入などが盛り込まれている。

例えば、同法14条１項３号では、詐欺等行為や管理侵害行為（営業秘密が記載され、又は記録された書面又は記録媒体の窃取、営業秘密が管理されている施設への侵入、不正アクセス行為その他の保有者の管理を害する行為）により取得した営業秘密を、不正の競争の目的で、使用し、又は開示した者は、３年以下の懲役又は300万円以下の罰金が科されると規定している。

これによって、従来不可罰であった「情報窃盗」の一部が、営業秘密に限り罰せられる可能性が出てきた。

■情報窃盗罪立法化の危険

本年５月12日に日経新聞が「産業構造審議会（経産相の諮問機関）の情報セキュリティ部会が11日の部会で提言をまとめた。管理者の許可なく個人情報を電子的に読み取った場合も、物を盗んだ場合と同様に処罰できるようにする」と報じた。関係資料については（同部会の議事要旨を除き）公開されていない模様である。

有体物の窃盗はともかく、情報の窃盗を安易に刑罰の対象とするのは、構成要件が不明確になるし、罪刑法定主義の観点からも望ましくない。前述のとおり、書店での立ち読みとか電車の中で他人が読んでいる新聞をのぞき込んだだけで「窃盗」となるのは常識に反するだろう。

官僚の側からすると「どこまで取り締まるのサジ加減は我々官僚が決める」という論理になるのだろうが、非常に危険である。官僚の暴走を抑えるためにも、情報窃盗の立法化についてはよく監視しておく必要があろう。

■不法行為法

以上のとおり、情報を漏洩した者に対して刑事責任を問うことは極めて難しい。

そこで、民事訴訟において個人情報を漏洩されてしまった個人が企業・官庁等を訴える場合は、民法709条等の不法行為法に基づき、故意又は過失と発生した損害に対する因果関係を立証して、損害額を請求することになる。

事例としては、宇治市事件（2002年７月最高裁決定）がその先例とされる。

事件が明らかになってから第１審判決（2001年）までの情報は、毎日新聞臺宏士記者の綿密な取材による、記事「個人情報の大量流失事件から2年、京都府宇治市の苦悩」(注1)に詳しい。以下この情報を下に事例分析しよう。

1998年４月ころ、宇治市は、乳幼児検診システムの開発を計画し、外部の民間企業に開発を委託した。市役所内での作業は、就労時間の制約があるので、開発を担当した元大学院生の男性アルバイトは、市の許可を得て、同システムに利用する住民基本台帳と外国人登録名簿の元データ計21万7617件分を持ち帰って作業を行うことになった。

この大学院生は、大阪府の名簿屋に電子メールで購入を打診し、光磁気ディスクに21万人分をコピーして郵送し、５月13日に口座に代金25万8000円が振り込まれたという事件である。事件の起きた98年当時は誰も気づかなかった。問題が判明したのは丸１年後のことである。

翌年1999年５月にインターネットで宇治市の住民票データが販売されていることが判明、市は名簿業者を通じて名簿を回収。６月３日には「完全回収宣言」を市議会総務委員会に報告した。

(注1) 旧リンクはhttp://www.mainichi.co.jp/digital/netfile/archive/200107/17-4.htmlであった。
現在ドメインの変更があったためリンク切れの模様。

また、宇治市は6月10日に宇治署に刑事告発、宇治署はアルバイト男性を「宇治市電子計算機組織に係る個人情報の保護に関する条例」違反で京都地検に書類送検した。

しかし、京都地検は1999年12月、「刑の廃止」を理由に不起訴処分とした。

新条例には、罰則についての旧条例の経過措置に関する明文規定がなかったためだ(一般に、罪刑法定主義により罰則は遡及できない。もっとも、旧条例にも罰則規定はあったのだから単なる立法ミス(経過措置の書き忘れ)ともいえる)。

一方で、宇治市議を含む市民3人が「プライバシーを侵害され、精神的苦痛を受けた」として、同市と大阪市北区の情報処理会社を相手取り、慰謝料など計約200万円の支払いを求めた訴訟を起こした。これ以降、本件は、民事事件として処理されることになる。2001年2月23日、京都地裁の八木良一裁判長は原告側の主張を全面的に認め、被告両者に慰謝料と弁護士費用各1万5000円、計9万円を支払うよう命じた。宇治市は直ちに控訴した。

2001年12月25日大阪高裁(岩井俊裁判長)は、1人につき1万5000円の慰謝料支払いを命じた1審・京都地裁判決を支持し、市の控訴を棄却した。市は最高裁に上告。

そして、2002年7月11日最高裁第一小法廷(藤井正雄裁判長)は、市の上告を棄却する決定を出した。大阪高裁判決が確定した。

■損害賠償額に関する考察など

この事案は、いくつかの点で興味深い。

まず、明らかに情報窃盗して横流しをした者に対して刑事責任を追及できなかったことである。前述のとおり、条例の経過措置立法ミスもあったが、根本的な問題として情報窃盗に対して罪を問うことの難しさがある。

また、一人あたりの損害賠償額が1万5000円とされたことである。これを高いとみるか安いとみるかだが、情報が誰でも閲覧できる基本4情報(氏名、性別、生年月日、住所)くらいであったことからすると、法曹界では妥当な額とされている。この点、前述のYahoo! BB事件では、独自の見解に基づき500円分の金券の配布で済まそうとしたところ、後になって通話記録まで流出したということが報道された事案であり、慰謝の措置として十分といえるのか、批判の強いところでもある。毎日新聞によると被害者の中で一人10万円の慰謝料を求めて大阪地裁に提訴したグループも出てきており
(http://www.mainichi-msn.co.jp/shakai/jiken/news/20040517k0000e040061000c.html)
今後の動向が注目される。

情報漏洩をしてしまった場合、一人あたり1万円以上の損害賠償責任がかかるという通説的な考えをとった場合、1万人分のデータが流出すれば、住基情報程度の簡易な情報でも、「損害賠償額は億のオーダになる」のである。個人情報管理には十分な対策が必要な所以だ。

尾崎孝良氏の紹介

昭和35年生まれ。東京大学理学部数学科卒・英国ケンブリッジ大学Diploma of Computer Science修了という経歴の理系出身の異色弁護士。医事法務のほか、デジタル著作権や情報セキュリティに造詣が深く、各方面で積極的に発言している。最近ではGPL読書会やハッカーのための法律講座などの活動も行っている。情報セキュリティ大学院では、セキュリティの法律実務について教えている。著書に「デジタル著作権」(ソフトバンクパブリッシング)がある。

2003年 情報セキュリティインシデントに関する調査報告書の概説
～ウイルス被害、個人情報漏洩被害の考察～

セキュリティ被害調査WG
株式会社ディアイティ　山田　英史

情報セキュリティワーキンググループでは、2001年から世の中の情報セキュリティインシデントの被害調査を実施している。2003年度は、2002年度の調査と同様に2部構成で調査結果をまとめた。

＜第1部＞
情報セキュリティのインシデントに関する調査および被害額算出モデル
＜第2部＞
情報漏洩による被害想定と考察（賠償額および株価影響額）
以下に2003年度報告書について解説する。

なお、解説は報告書の中で特徴的なところを部分的に取り上げたものであり、また紙面の構成上図表も縮小するため、是非あらためて『2003年度 情報セキュリティインシデントに関する調査報告書（PDF）』をダウンロードし参照いただきたい。

報告書URL
http://www.jnsa.org/active2003_1a.html

1. 調査の目的

個人情報漏洩事故は連日マスコミに取り上げられ、コンピュータウイルスもテレビのニュースに上がるほど情報セキュリティ被害は身近な問題となっている。マスコミに取り上げられる場合、「情報セキュリティ事故を起こす＝組織に欠陥がある」という論調で語られることが多い。その影響もあり、企業や公共機関の情報セキュリティ対策に対する要求は高まるばかりである。

ユーザが求めるセキュリティレベルを実現するために、企業や公共機関など組織は、どのような対策をどのような内容・規模で実施すれば良いのか、また、それはどの程度のコストを要するものなのか、何らかの目安があれば検討の助けになるだろう。しかし、その性質上、インシデントの実態は積極的に公表されることがほとんど無く、被害そのものの定義も明確となっていないため、被害発生の結果として把握されるべき被害金額などが算定できない状況にある。本ワーキンググループでは、「情報漏洩事故」における「損害賠償の可能性」や「株価への影響」について、今後の議論の題材になることや、企業経営者が考えるべき情報セキュリティのリスク量の把握や、行うべき投資判断の一助となることを目的として、検討および提案を行う。

2.『第1部 情報セキュリティのインシデントに関する調査および被害額算出モデル』の概要

＜第1部＞では、アンケートやヒアリングによって、国内の情報セキュリティインシデントに関する現状を把握するための情報収集とその結果を取りまとめた。2003年度は、独立行政法人 科学技術振興機構 社会技術研究システム（以下RISTEXとする）との共同調査を実施し、2002年度を大きく上回る規模のアンケートが実施できた。この情報から得られる結果と、

被害額算出モデルによって得られた結果により、情報セキュリティマネジメントにおける「リスクの大きさ(被害規模)」と「対策規模」の把握、および効果の計測などについての考察を行った。

2.1　調査対象

- JNSAメンバー企業を中心とするIT関連企業。
  （一部に非ＩＴ企業を含む）
  JNSAセキュリティ被害調査ワーキンググループメンバーにて調査を実施。
- 東証１部上場企業より無作為に抽出した1,000社。
  RISTEXにより調査を実施。

2003年度はRISTEXの協力もあり、全業種が網羅され、かなり実社会に近いアンケート集計となった。（報告書 ＜第1部＞ 7ページ 質問A-1）

2.2　調査方法

- 対象企業に対して、アンケート及びヒアリングにより調査を行う。
- 2003年1月から12月の1年間に実施した対策および情報セキュリティインシデント被害について回答を頂いた。
- アンケートは、2002年度の調査用紙をより簡便かつ詳細な回答ができるように修正したアンケート用紙を使用した。
- JNSAメンバー企業を中心とする企業へのアンケートは、JNSA事務局長の依頼文書と共に送付し、回答記入後、事務局へ返送いただき、集計を行った。
- RISTEXにて抽出した対象企業1000社については、RISTEXより情報セキュリティご担当者宛に送付し、回収後RISTEX事務局で集計を行った。
- また、回答の中で面談可能とのご連絡をいただいた企業に対して、当ワーキンググループメンバーが直接訪問し、具体的な内容について、ヒアリングを実施した。

2.3　アンケート回収率とヒアリング引受率

JNSAメンバー企業のアンケート回収率は2002年度が37%であったのに対し2003年度は25%と下がったものの、RISTEX回収分により回答件数は2002年度の約3倍の214件になった。

ヒアリング承諾件数は、2002年度が18件であったのに対して2003年度は15件となった。

	アンケート		
	送付	回答	回答率
JNSA	190	47	24.74％
RISTEX	1,000	167	16.70％
合計	1,190	214	17.98％

2.4　調査結果の分析と特徴

2.4.1　対象企業の平均年間売上および従業員数

アンケート回答企業214件の平均年間売上と平均従業員数は以下の通り。

平均年間売上：31,895,663万円
平均従業員数：4,084名

年間売上高の最小値は150万円、最大値は約5兆2千億円、従業員数は最小3人、最大14万人とかなり幅が出た。

2.4.2　情報セキュリティ管理担当者の人数

情報セキュリティの運用にたずさわる人員数は以下の通り。

専任者の平均人数：2名
兼任者の平均人数：22名

ヒアリング調査の際に、兼任者の情報セキュリティに関わる負担を確認したところ、日常業務の内10～30%をその対応にあてているという回答を数社から得た。

2.4.3　情報セキュリティ予算

情報セキュリティ予算について、回答者の70%が「情報システム関連予算の一部として計上」としている。各社の情報セキュリティ予算の平均は以下の通り。

・情報システム関連予算の平均金額：5,573万円
・情報システム予算に対する割合　：6.1%

2.4.4　情報セキュリティを確保するために導入しているシステム

情報セキュリティのために導入しているシステムは、2002年度と同様の結果となった。ファイアウォールやウイルスチェックなど基本的なシステムはすでに十分普及しているため、今後の調査でも変化は無いと想像できる。

ファイアウォール導入割合：92.1%
全クライアントPCにウイルスチェックソフトを導入：92.1%
侵入検知システム（IDS）：29.4%

ヒアリング調査によると、基本システムは導入が一通り完了したため、次はPC単位での対策に重点を置き始めているという回答がいくつか見られた。具体的には、各クライアントPCに監査ツール（資産管理ツールとしても利用）を実装し、パッチの適用状況やウイルス定義ファイルの更新状況を一元管理するという管理面の強化である。2003年に猛威を振るったMSBlasterが、社外でウイルス感染したPCを社内に持込み被害を拡大したという経験が生かされているものと考えられる。パッチの適用やウイルス定義ファイルの更新をポリシーとして義務付けても、実際の実施を社員まかせているため徹底できず、MSBlasterでその問題が露呈した企業が多かったようだ。

2.4.5　情報セキュリティに関する規程

「規程がない（19.2%）」と「分からない（0.9%）」という回答から逆算すると、79.9%の企業が何らかのかたちで情報セキュリティに関する規程を持っていることになる。規定のレベルは様々で、情報セキュリティポリシーとして明確に規定している以外に、就業規則やその他の規程の一部として策定しているユーザも多い。

2.4.6　監査の実施

情報セキュリティを維持するため監査を実施することが推奨されているが、RISTEXのアンケートでは以下のような結果が得られた。

外部監査機関によるセキュリティ監査の実施：21%
社内による情報セキュリティ内部監査の実施：35%

前述のポリシーの策定状況と比べると、監査の実施は低い水準に止まっている。監査制度の普及が望まれる。

2.4.7　情報セキュリティ教育

RISTEXのアンケートでは、「情報セキュリティに関する全社員向け教育」は34%が実施しているという結果が得られた。

この結果もやはりポリシーの策定状況と比べると、実施は低い水準に止まっている。教育はポリシーの実施において基本的な対策であり、効果も望めるため、もっと重視されて良いだろう。さらに教育の必要性をアピールしていく必要があると感じる。

2.4.8　被害が発生したときの対応計画の対象

この質問はJNSAメンバー企業のみを対象にした。被害状況の確認事項の設定や確認責任者の設定、社内連絡体制などについて、「定めていない（10.6%）」「分からない（4.3%）」から逆算すると85.1%が何らかの対応計画を持っていることになる。事業継続においてインシデント対応計画は重要であり、計画は策定するだけでなく訓練も推奨する。

2.5　被害状況の概要

2003年度のアンケートでは、113件のインシデントが集まった。被害の種類別では、やはりMSBlasterが69件と最も多く、全体の60%を占めた。

2.5.1　被害額算出モデル

2001年度に提示した被害額算出モデルは2002年度に改定したが、2003年度は改定を加えなかった。

インシデント被害額
＝表面化被害＋潜在化被害
＝直接被害＋間接被害＋潜在化被害
＝逸失利益（直接的な被害）
　＋復旧に要したコスト（ハードウエア、ソフトウエア、工数）
　＋営業継続費用＋喪失情報資産＋機会損失
　＋補償、補填、損害賠償など（間接的な被害）
　＋（固定費（人件費）×インシデントによる影響を受けた人数
　　×IT感応度（業務依存度）×停止時間）
　＋業務外の潜在化被害（ブランド価値の低下など）

2.5.2　インシデント毎の被害額の検証

集まった113件のインシデントを前述の被害額算出モデルに当てはめて被害額を算出した。詳細は、報告書 ＜第1部＞ 43ページ　被害状況（インシデント毎の被害額）を参照いただくとして、ここでは合計のみを記す。

a. 直接被害計　　：約6億88万円
b. 間接被害計　　：約300万円
c. 潜在化被害計　：約5億8286万円
合計（a＋b＋c）　：約11億8674万円

なお、上記試算の際、被害額算出モデル中の「IT感応度」は便宜上0.2を使用した。0.2という値は、2001年度の調査の際、実際に実施された被害復旧作業の分析により得られた数値である。本来は個別の組織によりITに依存する度合いが異なるため一律ということはない。（詳細は、報告書 ＜第1部＞ 79ページ IT感応度を参照）

2.5.3　日本全体におけるウイルス総被害額の推計

2003年度のアンケート結果から日本全体でのウィスル被害額を推計した。（詳細は、報告書 ＜第1部＞ 49ページ 日本全体におけるウイルス総被害額の推計を参照）

被害額の集計は、「会社企業数」「総事業所数」「総従業員数」の3パターンで推計してみた。それぞれ異なった結果が得られたため、どの方法が適切なのか、あるいは別の集計方法を検討すべきなのか、今後の課題であるが、もっとも妥当性があると思われる「総従業員数」からの推計によると、日本全体でのウィスル被害額は861億円という値が得られた。

2.5.4　被害にあったグループとあわなかったグループの比較

アンケート結果を「情報セキュリティインシデントにより被害にあった企業のグループ」と「被害にあわなかった企業のグループ」に分け、両者の比較を行った。

結果的には、導入セキュリティシステム、運用状況、予算の面では両者に大きな差が見られなかった。逆に多くの面で「被害にあった企業のグループ」の方が良い結果が得られた。

参考に、両者の従業員1人当たりの情報セキュリティ予算を上げる。

被害にあったグループ　　：13,910円/人
被害にあわなかったグループ：5,647円/人

サンプル数が非常に小さいなど、統計学的な問題も多く、今後の課題と考えている。

ただし、被害にあった企業が被害を契機に「確認事項」「確認責任者」「社内連絡体制」「連絡体制の規定」「各部門に担当者を設置」を強化したという回答は大いに参考になるだろう。

2.6　望まれる対策レベル

アンケートとヒアリングの結果から導き出される対策レベルを示す。

対応レベル	対　策	具体例	対応レベル
対応レベル1	技術的対策	ファイアウォール	レベル1
		ウイルス対策	
		IDS	
		メール監視ソフト	
		認証デバイス	
		PCセキュリティ（ウイルスチェック、パッチ適用、データ暗号化	レベル2
対応レベル2	運用的対策	入退室管理	
		セキュリティ責任者の設置	
		情報セキュリティ規定の策定	
		セキュリティ事故対応マニュアルの策定	レベル3（推奨レベル）
対応レベル3（推奨レベル）	実施度の向上	情報セキュリティ教育・啓発	
		罰則規定の整備	
		監査機能の強化	
		事故発生時の連絡体制の整備	
		事故発生を想定した訓練	レベル4
対応レベル4	第三者認証の向上	ISMS・BS7799認証	
		プライバシーマーク取得	
		情報セキュリティ監査の実施	

実際に被害を経験した企業が、事後対応計画を重視した対策を取っていることから、レベル 3 を推奨レベルとした。

3.『第2部 情報漏洩による被害想定と考察（賠償額および株価影響額）』の概要

＜第 2 部＞では、社会的な反響があり、関連者も多数に上るセキュリティインシデントの種類の一つとして、「情報漏洩」を取り上げた。本ワーキンググループでは、情報漏洩事件を「損害賠償の可能性」と「株価への影響」の2つの側面から分析した。

3.1　調査方法

2003年1月から12月の1年間にインターネット上に公開された情報漏洩事件・事故を対象に、以下の集計を行った。

・漏洩情報組織の業種
・漏洩の原因と経路
・漏洩情報の内容と量
・被害者人数
・漏洩後の組織の対応

当ワーキンググループにて考案した「損害賠償額算出モデル」に上記集計結果を当てはめ、各事例における想定賠償額を求めた。併せて漏洩組織と業務委託先の、漏洩後の株価の変動を求めた。

3.2　個人情報保護法との関連

本報告書で述べる個人情報漏洩による損害賠償額は、個人情報保護法の罰則に定められている罰金（または懲役）とは大きく異なることを理解して欲しい。

個人情報保護法違反は漏洩組織に対する制裁であり、損害賠償請求は被害者の救済という側面を持つ。

当ワーキンググループでは、すぐに被害に結びつき易いと思われる、損害賠償や信用失墜を調査・分析の対象とした。

3.3 国内の情報漏洩の分析

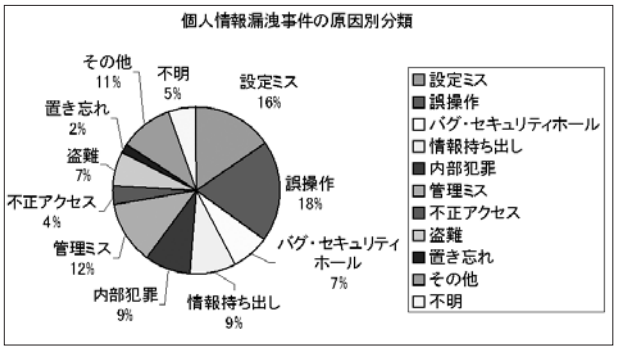
2003年1年間に公表された情報漏洩事件は57件で、被害者の合計人数は、155万4,592人 (一件平均30,482人)であった。詳細は、報告書 ＜第2部＞ 9ページ 表 4-1：2003年 個人情報漏洩事件 一欄表を参照いただきたい。

3.3.1 漏洩情報の分析

それぞれの漏洩情報の項目が、各調査対象の事件に含まれていた確率を出現確率とする。2003年の事例では、氏名・住所・生年月日・性別・電話番号・職業・Emailアドレスといった、いわゆる基本情報が出現確率の上位をしめた。他に件数は少ないものの、クレジットカード番号・信用情報・病名・感染症検査の結果など機微な情報も含まれる事例もあった。（詳細は、報告書 ＜第2部＞ 10ページ 4.1.2 漏洩情報の分析を参照）

3.3.2 情報漏洩の原因

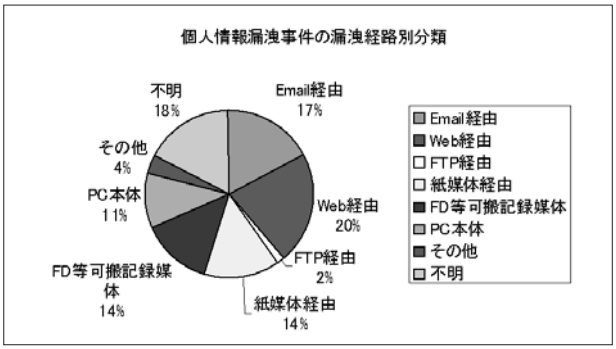
2003年の個人情報漏洩事件の原因別分類は下図の通り。



2002年度は設定ミスや誤操作といった技術的人為ミスの比率が全体の88%を占めていたのに比較して、2003年度は情報持ち出しや内部犯罪など非技術的犯罪の比率が上がったことが特徴である。

3.3.3 情報漏洩経路

情報漏洩経路の分類は以下の通り。



情報漏洩経路においても昨年度と異なった結果が見られる。

2002年度の漏洩経路においては、インターネットを介したWeb経由・Email経由・FTP経由が98%を占めていた。2003年度は、先の3つの経路の合計が39%という結果にとどまり、紙媒体・FD等可搬記録媒体・PC本体の盗難・置き忘れ等が大幅に増加している。

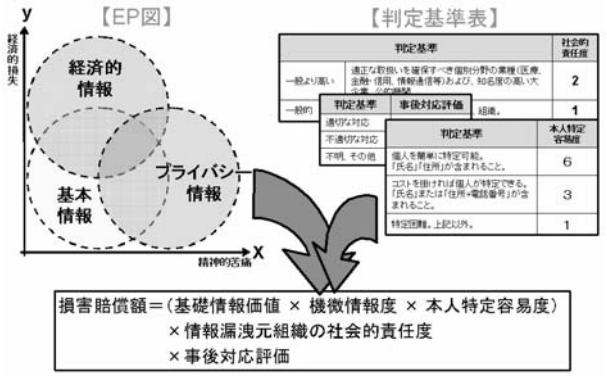
3.4 個人情報漏洩による損害賠償額

2003年度も損害賠償の予想計算式を独自に提案した。2002年度版は漏洩情報の量に基づき情報価値を算定したのに対し、2003年度版では漏洩情報のプライバシー度や経済的価値という内容に着目して価値を決めるなど、大きく改良を加えた。

3.4.1 損害賠償の予想計算式の解説

2003年の損害賠償金想定額の算出式の特徴は、EP図（Economic-Privacy Map）を用いて、個人情報が持つ「経済的損失」と「精神的苦痛」の2つのリス

クを分析し、個人情報の価値を定量化した点である。他にも、判定基準表を用いて算出式の各項の数値を求めやすくする改良を実施した。



3.4.1.1　個人情報価値の算出式とEP図の解説

個人情報価値は以下の算定式で求める。

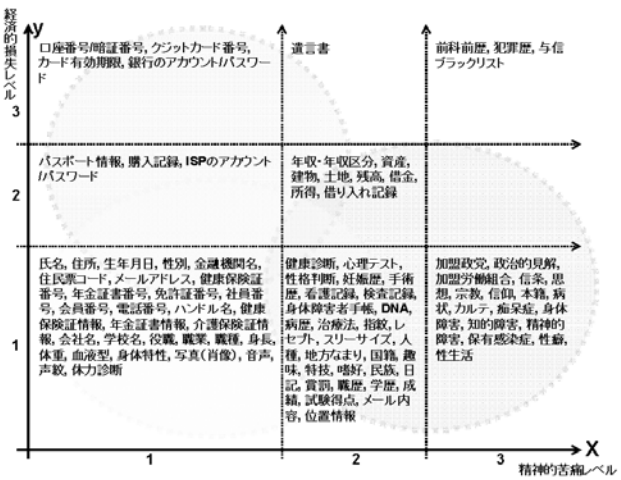
漏洩個人情報価値＝基礎情報×機微情報×本人特定容易度

（1）基礎情報は一律500ポイントとする。

（2）機微情報は、下記算定式で求める。

機微情報＝$(10^{x-1} + 5^{y-1})$

xおよびyに入る値はSimple-EP図から求める。漏洩情報に重み付けをするためにEP図のx軸・y軸を3段階に分割し、各エリアに漏洩情報をプロットしなおしたのがSimple-EP図である。x軸は右に行くほど精神的苦痛レベルが高くなり、y軸は上に行くほど経済的損失レベルが上がる。



Simple-EP図

漏洩情報が複数種類ある場合は、全情報の内最も大きなxの値と最も大きなyの値を採用する。

（3）本人特定容易度は、漏洩した個人情報からの本人の特定し易さを表すもので、以下の判定基準を使用する。

判定規準	本人特定容易度
個人を簡単に特定可能。 「氏名」「住所」が含まれること。	6
コストをかければ個人が特定できる。 「氏名」または「住所＋電話番号」が含まれること。	3
特定困難。上記以外。	1

詳細は、報告書 ＜第2部＞ 26ページ 5.1.3 損害値の計算方法を参照いただきたい。

3.4.1.2　社会的責任度の解説

社会的責任度は下表に示すように、「一般より高い」と「一般的」の2つから選択する。社会的責任度が一般より高い企業、組織は、「個人情報の保護に関する基本方針（平成16年4月2日 閣議決定）」に「適正な取扱いを確保すべき個別分野」として挙げら

れている業種を基準とし、そこへ政府機関など公的機関と知名度の高い大企業を含めることにした。

判定規準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融、信用、情報通信等）および知名度の高い大企業、公的機関	2
一般的	その他一般的な企業および団体、組織。	1

3.4.1.3　事後対応評価

過去の情報漏洩事件における事後対応行動から、適切な対応と不適切な対応を分類した。（事後対応行動については、報告書 ＜第2部＞ 29ページ 5.1.5 事後対応評価を参照）

この基準に当てはめて、事後対応の適切／不適切さを判断する。「事後対応評価」の値は下表から選択する。

判定規準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

3.4.2　2003年度 個人情報漏洩による損害賠償額

前述した損害賠償金想定額の算出式を、2003年度の情報漏洩事件57件に当てはめた結果は、最後の「4. 2003年度の統括」の後に置いた表になる。被害者全員が損害賠償訴訟を起こすことは考えにくいが、仮に起こした場合を想定している。当算定式は潜在的な情報価値を把握することにも役立つと考えるので、是非自社の情報に適用して算定を試みていただきたい。

3.5　情報漏洩による企業価値影響の算出

2002年度と同様に、情報漏洩により生じた企業の信頼失墜、ブランドイメージ低下の大きさを株価変動からの把握を試みた。調査対象57件の内上場企業18社を対象に分析した。

3.5.1　株価変動の把握方法

情報漏洩第一報公表日から起算して当初14日間における1日あたりの企業価値影響額(短期影響額)を見た。

基準レシオ＝事件発生前1週間の（当該企業株価/日経平均株価）の平均値

n日レシオ＝事件発生後のn日目の（当該企業株価/日経平均株価）

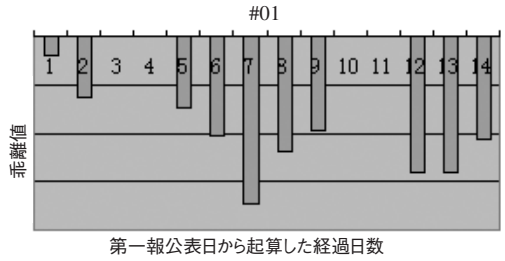
n日乖離値＝（基準レシオ－n日レシオ）×n日の日経平均株価

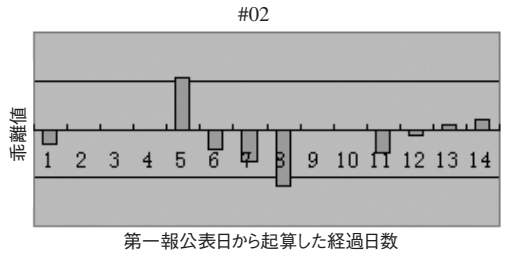
平均乖離値＝（1～14日目までの乖離値）の平均値

短期株式影響額＝平均乖離値×発行済株式数　←（企業価値影響額）

3.5.2　事件報道後の乖離値の経時変化

2003年の分析結果からは、情報漏洩事件と株価変動との顕著な相関関係を見出すことはできなかった。分析結果の一部を以下に示す。





3.5.3　情報漏洩による企業価値影響の考察

情報漏洩事件後、7割の企業で株価が低下した。

18件中12件がマイナス変動（66.7%）

結論としては、今年度の調査でも、情報漏洩事件

と株価との間の相関性を解明するまでには至っていない。

しかし、情報漏洩という不祥事は企業にとってはマイナス要素であり、企業価値を減ずる要因になりうることは何人も否定できないだろう。マイナス要因を明示的にするためにも、株価への影響を追究することの意義は大きいと考える。実際の株価の動きには様々な要因があり、その中から情報漏洩事件に起因する株価変動分を抽出・計測することは難しいものの、継続的なアプローチにより、その手掛かりを掴みたい。

4. 2003年度の統括

2003年はMSBlasterが大きなインシデントとしてクローズアップされた。その後もコンピュータウイルスによる被害は繰返し発生している。また、被害の件数が少ないため統計には表れないが、P2Pソフトによる情報漏洩など新しいIT技術に伴うインシデントも発生している。現時点で効果があるセキュリティ対策でもいずれはそれを回避する脅威が発生することは予想できる。2003年度の調査においても、インシデント被害を経験した企業が被害を契機に事後対応を強化しているように、事故前提の体制作りが今後重要になるだろう。

現実の企業では何が実施され、どのような問題点を抱えているのかを知ることは、今後の情報セキュリティを考える場合に大変役に立つ。現場の声を集める作業は重要で、そのための手段としてアンケートとヒアリングは有効であると考える。

また、個人情報漏洩については社会に与える影響と世間の注目度を考えると、啓発の意味も込め引き続き実態調査を実施していく必要があるだろう。

2003年度
個人情報漏洩による損害賠償額

想定損害賠償総額：
280億6936万円（平均 5億5038万円）
合計被害者人数：
155万4592人（平均 30,482人）

No	業種名	被害人数	精神的苦痛レベル(x)	経済的損失レベル(y)	機微情報度	社会的責任度	事後対応評価	本人特定容易度	1人あたり損害賠償額	損害賠償総額（千円）	No
1	金融・保険業	1,000人	2	1	11	2	2	3	66千円	66,000千円	1
2	教育、学習支援業	不明	2	1	11	1	1	1	6千円	不明	2
3	情報通信業	202人	1	1	2	2	1	3	6千円	1,212千円	3
4	その他	不明	1	1	2	1	1	3	3千円	不明	4
5	運輸業	190人	1	1	2	1	1	1	1千円	190千円	5
6	教育、学習支援業	220人	2	1	11	1	1	6	33千円	7,260千円	6
7	サービス業（他に分類されないもの）	443人	1	1	2	1	1	1	1千円	443千円	7
8	教育、学習支援業	7,381人	2	1	11	1	1	3	17千円	121,787千円	8
9	情報通信業	1,500人	1	1	2	2	1	6	12千円	18,000千円	9
10	サービス業（他に分類されないもの）	450,000人	1	1	2	1	1	6	6千円	2,700,000千円	10
11	公務（他に分類されないもの）	92人	1	1	2	2	1	1	2千円	184千円	11
12	公務（他に分類されないもの）	574人	1	2	6	2	1	6	36千円	20,664千円	12
13	情報通信業	不明	2	1	11	2	1	3	33千円	不明	13
14	金融・保険業	15,000人	2	3	35	2	1	6	210千円	3,150,000千円	14
15	その他サービス	2人	1	1	2	2	1	1	2千円	4千円	15
16	医療・福祉	1,300人	3	1	101	2	1	6	606千円	787,800千円	16
17	教育、学習支援業	950人	1	1	2	1	1	3	3千円	2,850千円	17
18	金融・保険業	2,800人	1	1	2	2	1	1	2千円	5,600千円	18
19	金融・保険業	98人	3	1	101	2	1	6	606千円	59,388千円	19
20	公務（他に分類されないもの）	100人	2	2	15	2	1	3	45千円	4,500千円	20
21	金融・保険業	800人	2	2	15	2	1	6	90千円	72,000千円	21
22	サービス業（他に分類されないもの）	170人	1	1	2	1	1	1	1千円	170千円	22
23	教育、学習支援業	23,000人	1	1	2	1	1	1	1千円	23,000千円	23
24	サービス業（他に分類されないもの）	210人	1	1	2	2	1	6	12千円	2,520千円	24
25	卸売・小売業	560,000人	1	1	2	1	1	6	6千円	3,360,000千円	25
26	公務（他に分類されないもの）	1,300人	3	1	101	2	1	6	606千円	787,800千円	26
27	公務（他に分類されないもの）	761人	1	3	26	2	1	6	156千円	118,716千円	27
28	金融・保険業	325人	1	2	6	2	1	6	36千円	11,700千円	28
29	製造業	573人	1	1	2	2	1	1	2千円	1,146千円	29
30	製造業	不明	3	1	101	1	1	6	303千円	不明	30
31	金融・保険業	74人	1	2	6	2	1	6	36千円	2,664千円	31
32	公務（他に分類されないもの）	128人	1	1	2	2	1	6	12千円	1,536千円	32
33	情報通信業	480人	1	1	2	2	1	1	2千円	960千円	33
34	金融・保険業	126人	1	3	26	2	1	6	156千円	19,656千円	34
35	金融・保険業	1,453人	1	3	26	2	1	6	156千円	226,668千円	35
36	卸売・小売業	182,780人	1	1	2	1	1	6	6千円	1,096,680千円	36
37	情報通信業	不明	1	1	2	2	1	6	12千円	不明	37
38	医療、福祉	240人	3	1	101	2	1	3	303千円	72,720千円	38
39	情報通信業	173人	1	1	2	2	1	1	2千円	346千円	39
40	卸売・小売業	6,000人	2	1	11	1	1	6	33千円	198,000千円	40
41	金融・保険業	79,110人	2	2	15	2	1	6	90千円	7,119,900千円	41
42	金融・保険業	75人	2	2	15	2	1	6	90千円	6,750千円	42
43	情報・通信	1,370人	1	1	2	2	1	3	6千円	8,220千円	43
44	情報通信業	3,974人	1	2	6	2	1	3	18千円	71,532千円	44
45	情報通信業	58,515人	1	1	2	2	1	6	12千円	702,180千円	45
46	公務（他に分類されないもの）	872人	2	1	11	2	1	6	66千円	57,552千円	46
47	卸売・小売業	1,912人	1	1	2	1	1	6	6千円	11,472千円	47
48	運輸業	10人	2	2	15	2	1	6	90千円	900千円	48
49	教育、学習支援業	197人	2	1	11	1	1	6	33千円	6,501千円	49
50	サービス業（他に分類されないもの）	1,200人	2	1	11	2	1	6	66千円	79,200千円	50
51	サービス業（他に分類されないもの）	不明	2	2	15	1	1	6	45千円	不明	51
52	金融・保険業	280人	2	3	35	2	1	6	210千円	58,800千円	52
53	情報通信業	4,312人	2	2	15	2	1	6	90千円	388,080千円	53
54	運輸業	131,742人	1	1	2	1	1	6	6千円	790,452千円	54
55	卸売・小売業	9人	1	1	2	1	1	3	3千円	27千円	55
56	情報通信業	985人	1	2	6	2	1	3	18千円	17,730千円	56
57	公務（他に分類されないもの）	9,584人	2	1	101	2	1	6	606千円	5,807,904千円	57
	合計	1,554,592人								28,069,364千円	
	1件あたりの平均（不明を除く）	30,482.2人								550,380千円	

JNSA ワーキンググループ紹介

Webセキュリティ調査・検証WG

Ｗｅｂセキュリティ調査・検証WGリーダー
株式会社アークン
斉藤　純平

■はじめに

ここ数年、企業のビジネスを左右する情報や機密性の高いデータなどが、Internet上に公開されたWebサーバおよびデータベースサーバに格納されています。しかし、「サイバーテロやインターネットセキュリティ侵犯の75%は、インターネットアプリケーションによって発生する」(2002年：Gartnerレポート)といわれるように、現在Webが、重要なIT資産の情報漏えい、改ざん、不正利用といった脅威にさらされています。また、攻撃手法もこれらの状況の変化により変わってきています。以下一例を示しますが、これらの攻撃はブラウザ経由で行われるためファイアウォールでは防ぐことが出来ない特徴があります。

- **SQLインジェクション攻撃**
  Webの作り方によっては、ブラウザ経由でバックグラウンドで動作するDataBaseからDataを抜き出すことが出来る。
- **クッキー改ざん攻撃**
  ECサイトで商品購入情報を保存しているクッキーを改ざんすることにより割引価格で購入可能。
- **パラメータ改ざん攻撃**
  会員専用サイトなどで簡単なセッションIDを使用していると一旦正会員としてサインイン後URLのセッションIDを変更することにより他の会員になりすまし、他の会員の情報を閲覧可能。

■活動目的

本年度より活動を開始するWebセキュリティ調査・検証WGでは、組織にとって近年益々重要な基盤となっているWeb環境に特化した攻撃手法やその対策を調査・研究します。

本年度の活動はWebの脆弱性・Webに特化した攻撃手法の調査、および具体的な対策の調査を行います。また、攻撃検知・防御ソリューションによる対策については検証環境を構築した上で検証を行います。

■今後の予定

現在、Web開発の立場、Webの脆弱性を診断する立場、Web診断ツール・Webアプリケーションファイアウォールベンダーの立場の方々を中心に33名がWGに参加いただいております。

本年度は、診断チーム、開発チーム、WAFW(Web Application Firewall)チームの3つに分かれ以下の成果物を目標に活動を行うこととなりました。

- **診断チーム**　「Webセキュリティ診断ガイドライン」
- **開発チーム**　「セキュアWebアプリ開発ガイドライン」
- **WAFWチーム**「Web Application Firewall製品選定のガイドライン」
- **全体**　「脆弱性分類表」、「WG活動報告書」

また、実際の検証に際してはどこまで本年度中に出来るか解りませんが以下を予定しています。

- 脆弱版Webアプリケーション VS 診断チーム
- セキュア版WebアプリVS診断チーム
- Web Application Firewall(デフォルト)VS診断チーム
- Web Application Firewall(チューニング済)VS診断チーム

今後ますます重要になってくるWebアプリケーションセキュリティに関し、JNSAならではの成果物を出すべく活動を行っていければと考えています。

マーケットリサーチ WG

マーケットリサーチWGリーダー
株式会社IDGジャパン
玉井　節朗

■ はじめに

一口にITセキュリティ市場といっても多岐にわたるIT製品分野に存在している。企業では、事業規模、予算、機密保持の重要性、その他もろもろの事情に合った、ハードウェア、ソフトウェア、ITサービスのセキュリティ機能を利用してシステムを構築し運用を行っている。このような理由からITセキュリティ市場動向や導入状況を統括して調査することは難しく、公的な信頼できる調査資料は存在しないのが現状である。

JNSAではその活動目的である、セキュリティの重要性の啓蒙活動、普及の障害となっている問題の分析、を推進するため、ITセキュリティ市場の現状把握が不可欠であると考え自ら市場調査を実施することとした。

原案では、ハードウェア、ソフトウェア、ITサービスの各分野でセキュリティ製品についての出荷状況、企業のセキュリティ投資規模、導入状況の調査を行い、その結果に基づき導入に関する問題点の分析、国内の市場規模の実績値と予測値を推定する予定であった。しかし、定量的な市場分析を行うためにはセキュリティ製品を製造・出荷している企業の調査協力が必須であるが、実際には業績をオープンにして企業に協力をしていただくのは困難、という理由で市場規模の実績値と予測値の推定は今後の課題とすることとした。

このため、企業におけるITセキュリティ製品導入状況及び導入後の問題点の把握を主目的として調査を実施することとした。

■ 調査目的

目標：国内の情報セキュリティ市場規模を調査し今後の市場予測を行なう

★企業のセキュリティシステム普及状況を確認し，強化すべきポイントを把握する

★国内のセキュリティ産業の動向を把握し、事業企画の材料として会員企業に提供する

★将来のセキュリティ普及の方向性を検討する材料とする

■ 具体的な活動・成果

1. 初回の調査では情報セキュリティの導入状況と満足調査を中心に行なうこととする

★セキュリティ製品の利用状況の調査である

★ベンダーにもエンドユーザーとして調査に参加してもらう（会員への送付も含める）

★ユーザからサービスやセキュリティ製品に対しての満足度を収集する

※出荷・導入状況まで聞いてもおそらく答えてもらえないだろう

★市場規模は、導入している製品がわかればある程度推測できるので今回は敢えて数値化する質問にしない

2. 具体的なアンケート項目内容を3つの製品別サブワーキンググループ編成（ハード、ソフト、サービス）し作成する（敬称略）

ハード	サブリーダー	：郷間
	メンバー	：能地、中村、渡部、坂本
ソフト	サブリーダー	：番野
	メンバー	：野村、米澤、依田、山田、飯島、浜武
サービス	サブリーダー	：勝見
	メンバー	：荒川、中津、斉藤、岡本

3. 調査先ユーザリスト、送付先データに付いては今後の会議でまとめる。

ユーザ団体であるJUASとの共同調査についても今後内容を確認し協力お願いすることにしている。更に今後の調査分析、発表も会議の決定を以って随時報告する。

★目標送付数は約3,000件、回収目標は約200件
★回収率を上げる為成るべく選択式で答えやすく且つ項目数を絞り、30項目以内を目標としている

4. 調査報告、発表時期 （目標予定）

★Network Security Forum 2004
（会期：10月28日、29日　会場：青山TEPIA）
★Web サイトにて結果報告
★JNSA Pressにて紹介・結果報告

■ 今後の展開・スケジュール（予定）

7月中旬	アンケート項目内容確認、発送先リスト確認
8月末	アンケート発送（配信）
9月中旬	アンケート回収（収集）、分析開始
9月末	アンケート結果分析会議
10月中旬	結果資料確認会議
10月末	NSF2004にて発表、資料配布、WEBアップ

■ WGメンバー　19名　（順不同）

玉井　節朗（IDGジャパン）
塚本　卓郎（IDCジャパン）
郷間　佳市郎（京セラコミュニケーションシステム）
能地　將博（マカフィー）
中村　亨（松下電工）
渡部　真江（アークン）
坂本　健太郎（コンピュータ・アソシエイツ）
番野　邦彦（キヤノンシステムソリューションズ）
野村　智子（トリップワイヤ・ジャパン）
米澤　一樹（セキュアコンピューティングジャパン）
依田　真一（コンピュータ・アソシエイツ）
山田　勝志（クオリティ）
飯島　邦夫（クオリティ）
浜武　千恵（アークン）
勝見　勉（シマンテック）
荒川　弘（ITサービス）
中津　有美（ジェイエムシー）
斉藤　麻衣子（トレンドマイクロ）
岡本　真知（シーフォーテクノロジー）

★コメント★
限られた予算内で皆様の必要な情報・成果がこのアンケート等でどこまで達成、満足していただけるのか多少疑問を持ちながら進めております。ただ今年は初回ということもありさまざまなカテゴリでの満足度調査を中心としており、各企業の出荷台数、投資規模等の実態調査を当初より避けた内容となっておりますので皆様のご理解の程お願いしたいと思います。

プライバシー保護実装研究 WG

プライバシー保護実装研究WGリーダー
日本アイ・ビー・エム　システムズ・エンジニアリング株式会社
久波　健二

■ はじめに

個人情報漏えい事件が各メディアで取り上げられる中、来年の個人情報保護法の完全施行に向けて、企業は対応を迫られています。プライバシー保護や法制対応の観点から様々な情報が各方面から発信されているにも関わらず、情報システム部の担当者から何をすれば良いのか分からないという声が聞かれます。現場では、より具体的な対策方針が求められているといえます。本WGは昨年活動致しましたプライバシー保護ガイドライン作成WGの検討結果をもとに、さらにIT分野での実装内容を検討し、その成果により少しでも現場の担当者の疑問に答えるべく発足致しました。

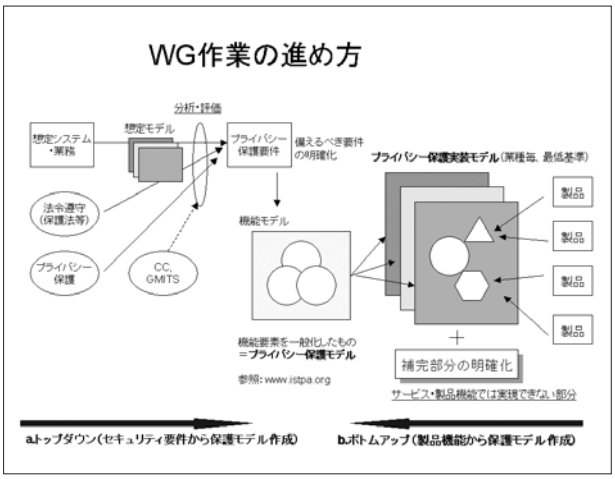
■ 活動の目的

本WGではプライバシー保護、特に個人情報保護法対応のために、IT技術はどこまで対策可能かを調査・研究致します。昨年、個人情報保護ガイドライン作成WGにてマネージメントの観点を中心に研究致しましたが、今回はIT技術の検討に注力し、IT技術で可能な部分の抽出と、それにより組織・運用で実施する部分との明確化を目指します。具体的には2つのアプローチを実施しています。一つ目はトップダウン手法を用い、幾つかの想定企業をモデル化し、そのモデルを分析・評価することでプライバシー保護に関するIT機能要件を導出します。2つ目はボトムアップ手法を用い、現在、各社で提供されているサービスや製品をカテゴリー分類することにより実現可能なIT機能を整理致します。以上の2つのアプローチの成果から、成果物としてプライバシー保護に必要な機能をモデル化したプライバシー機能モデル作成と、想定企業に適合させたプラバシー保護実装モデルを作成し、さらに組織・運用にて補完すべき機能の明確化を実施致します。

■ 現在までの進捗状況と今後の予定

本WGは本年3月末に発足し、ほぼ隔週で会合を実施し研究を行っております。コンサルタント、システムエンジニア、会計士等、各々の分野におけるスペシャリストの皆様のご参画により様々な観点での検討を実施しています。現時点はトップダウン手法によるプライバシー要件の洗い出しと、ボトムアップ手法によるカテゴリー分類を実施済みです。9月末のベータ版公開に向けて、成果物作成を開始しております。

本WGの活動については先日の成果報告会で発表しておりますので、そちらをご覧下さい。
http://www.jnsa.org/seminar_20040518.html



■ おわりに

本WGはセキュリティ管理サイクルのPDCAの中で、プライバシー保護対策に関するP（Plan：計画）とD（Do：実施）の観点で研究を行っております。いち早く具体的対策を公開することにより、企業の円滑な対策計画と実施を促進できれば幸いです。また、今後必要となるC（Check：監視）とA（Action：改善）の観点から個人情報保護法運用指針WG（仮称）との連携を深めて、研究成果がより実のあるものとなることを目指しています。

これだけは知っておきたい

インターネット安全教室2004

～ウイルス感染、詐欺行為、プライバシー侵害などの被害にあわないために～

誰でも手軽にインターネットに接続できるようになった今日、ウィルス感染、詐欺行為、プライバシーの侵害など、情報犯罪の被害にあう危険性がますます高くなってきています。そこで、経済産業省とNPO日本ネットワークセキュリティ協会（JNSA）は、警察庁の後援をえて、全国各地で「インターネット安全教室」を開催することになりました。ぜひこの機会にセミナーに参加し、インターネットを安全快適に活用するにはどうしたらいいか、被害にあったときにはどうしたらいいかといった情報セキュリティの基礎知識を身につけてください。

[主　催]　経済産業省、NPO日本ネットワークセキュリティ協会（JNSA）

[後　援]　警察庁、その他

[開催地]　（8月10日現在）

日程	県名	共催者	開催場所
10月7日（水）	島根県	財団法人しまね産業振興財団	くにびきメッセ
10月16日（土）	東京都	足立区立扇中学校PTA、 足立区立奥本小学校PTA	足立区立奥本小学校 体育館
10月日程未定	兵庫県	兵庫ニューメディア推進協議会	会場未定
11月2日（水）	神奈川県	横須賀市	横須賀市役所正庁
11月6日（土）	愛知県	NPO東海インターネット協議会	名古屋市公会堂
11月17日（水）	岐阜県	岐阜県，財団法人岐阜ソフトピア ジャパン	ソフトピアジャパン
11月19日（金）	和歌山県	NPO情報セキュリティ研究所	わかやま館
12月10日（金）	青森県	財団法人八戸地域高度技術振興 センター	八戸インテリジェント プラザ
2月26日（土）	熊本県	NPO熊本県次世代情報通信推進機構	熊本市総合女性センター

※お近くで開催の際には、ぜひご参加ください。

その他、昨年開催地方（新潟、神奈川、福井、奈良、大阪、岡山、徳島、大分、沖縄）でも開催予定。

開催地の詳細は、JNSAホームページをご覧ください。　**http://www.jnsa.org/caravan.html**

第59回IETFミーティング参加報告

JNSA研究員　安田　直義

2004年2月29日～3月5日に韓国 ソウル Lotte Hotelにて開催された第59回IETF(Internet Engineering Task Force: http://www.ietf.org/)に、ChallengePKI活動の一環として参加した。IETFは、インターネット上のプロトコルをはじめとする技術標準について議論し決める団体だが、JNSAのChallengePKIでは、2002年7月の横浜で開催された第54回IETF以来参加している。
今回の第59回IETFへの参加は次のような目的を持っていた。

1. 日本より提案しているInternet-Draftである Multi Domain PKI(セコムトラストネット 島岡氏著)の扱いを調整
2. 証明書のUTF8Stringに関しての議論に参加

セコム株式会社 IS研究所
松本　泰、　石垣　陽

セコムトラストネット株式会社
島岡　政基

富士ゼロックス株式会社
稲田　龍、横田　智文、益井　隆徳

NPO 日本ネットワークセキュリティ協会
安田　直義

ソウル Lotte Hotel

概観

IETFでは活動を8つのエリアに分け、各々のエリアにArea Directorを設け、Area Directorの統括の元にWGでの標準化活動を行っている。通常の標準化活動はメールベースで行われるが、年に3回、実際に顔をあわせるオフラインの会議が行われている。この会議は、2回は米国内、1回は米国外で行われる習慣となっているが、今回の韓国での開催は、2002年の第54回横浜に続きアジアでの2回目の開催になる。

今回のIETFのホストにはKorea TelecomとSamsungがなり、協賛としてTIA、ANF、ETRI、KIPA、KISA(Korean Information Security Agency)、KISTI、KRNIC、NCAOSIAなど韓国の官民両サイドでのバックアップがなされていた。また今回、初めての試みとして、IETFに併設してIPv6 Demonstrationが行われていた。

第59回IETFミーティングの参加者は、32カ国から総勢1,545人だった。今回は、韓国での初めての開催のせいか、やはり韓国人の参加が目立ち、参加国別の統計は事務局によると第一位 韓国人 45%、第二位 米国人 22%、第三位 日本人 10%とのことだった。

JNSAが中心となったChallengePKIの活動を中心にIETFを概観してみよう。

セキュリティ関連の活動

ここ数年、セキュリティの確保はインターネットにとり大きな課題となっており、各社は種々の対策/提案を行なってきた。IETFは、標準化を行なう立場で活動を行なっており、多くのプロトコルに関してセキュリティ面での強化を行なってきている。

ここ数年にわたり初日にはSecurity Tutorialが開催され、インターネット・プロトコルに対して必要とされるセキュリティ要件に関しての講義が行われている(後述)。Internet-Draft/RFCに関しては“Security Consideration”の項目が必須となるなどインターネットの標準化に関してセキュリティは必須の要件となっている。

JNSAのChallengePKIのグループも、月曜日の夜に、

PKIX-WGのChairであるSteve Kent氏、Jim Schaard氏と供にRussell Housley氏、Steven Bellovin氏と食事をし、PKIのモデルを今後どうIETFで扱うかに関してディスカッションをした。

PKI関係の活動

Steve Kent氏、Jim Schaard氏、Russell Housley氏、Steven Bellovin氏とのディスカッション

現在、ChallengePKIで作業しているGPKI/PKI関連の活動において、現行のIETFにおけるPKIの利用に関しての標準文書であるRFC 3280では十分ではない事が判明している。特に、PKIのドメインが複数あり、互いに相互認証する場合のモデルに関してきちんとした文書の整備が必要である事がわかっている。

この問題に関して、ChallengePKIグループではセコムトラストネットの島岡氏を中心にしてInternet-Draftsを作成しているが、これの扱いに関して前記のメンバおよびIPA 宮川氏、セコム株式会社 IS研究所 松本氏、JNSA 安田などを交えてディスカッションを行った。

当初、59th IETF開催前にPKIX-WG ChairであるNISTのTim Polk氏（今回は脊椎捻挫のため欠席）およびBBNのSteve Kent氏にInternetにおけるPKIのモデルの話であるのでPKIX-WGのWork Itemとして活動を行なえないかと打診をしてみた。両氏からは、PKIX-WGのミッションは標準化を行なうことであること、IESGよりPKIX-WGは、新たなWork Itemの追加を許されていない事を理由にPKIX-WGでの活動にすることは難しいとのコメントがあり、Security AreaのADであるRussell Housley/Steven Bellovinの両氏に相談すべきと助言された。Russell Housley/Steven Bellovin の両氏は、PKIのモデルに関する記述の不足を認め、Security Areaの新たなWGとして活動を行なう事を提案された。

Stephen Kent氏(左)、Steven Bellovin氏(中央)、Russell Housley氏(右)

左から稲田氏、Jim Schaard 氏、島岡氏、宮川氏(右)

WGの作成は、正道でありIETFにおいて標準化を行う際には必要となることである。IETFのルールでは、まず、BOFを最大3回おこない必要性が認められたらWGとすることになっている。最大3回のBOFにおいて必要性が認められない場合、そのアイテムはIETFで扱うべきものではないと認定されることになる。

ChallengePKIで、IETFの新しいWGを目指して活動するかどうか議論を行なったが、現時点では新たなWGを作ることは地理的、言語的にも荷が重く、できれば中心になって旗を振ってもらえる方がいないか検討して欲しいという希望を伝えるとともに、何らかの方法で個人的なI-DをRFCにすることはできないかを相談した。Russell Housley/Steven Bellovinの両氏は、個人としてRFCを発行することは可能であるが、IESGが認める事が必要であり、そのためにはきちんとした識者によるレビュが必須であるという要件が示され、レビュアとして適切な人間を数名上げていただいた。今回のIETFで行なわれた、OPSECも同様の立場にあるとのことだが、ChallengePKIとしては、この提案を受け、新たなWGを

作らず、識者によるレビュを受けてIESGにBCPとしてRFC化を目指す方針とした。

今後、2004年末にRFC化を目指して下記のような作業を行う予定である。

1. I-Dの改訂
2. PKIX-WGその他関係あるMLに対してアナウンス
3. 議論用のMLの立ち上げとアーカイブの開始
4. 平行して識者へのレビュ依頼
5. 60th IETFにおいてBOFの開催

Public-Key Infrastructure WG

3月1日に行われたPKIX-WGは、Co-Chairであるの NISTのTim Polk氏が脊椎捻挫のためBBNのStephen Kent氏により仕切られ、参加者は約50名程度だった。

WGのミーティングは通常通りにドキュメントステータスより始まり、粛々と議題をこなしていく進行で、議論としては若干低調ではあったが、内容としてはQualified CertificateのRFC化が進み、Proxy CertificateはRFC化が決まるなど多くの面で進展が見られた。それらの中からひとつだけ紹介しておこう。

Subject Identification Methodに関する問題

韓国のKISAのJongwook Park氏と米国NIST Tim Polk氏の連名での報告があった。韓国では既に国民に対して証明書を発行しており、米国も計画があるが、その際に証明書内に格納するプライバシー情報（住所、生年月日、性別、氏名など）をどう証明書内に表現するかが問題になっている。

韓国や米国はこの問題を重要なものとして捉え、特定の方式で暗号化した情報を記載することにより、適切な権限を持った利用者のみに情報が開示される方式を提案している。日本で展開されている公的個人認証サービスに関しても同様な問題を抱えており、日本の場合は、公的個人認証サービスの証明書を利用するのは官側のみと規定し問題がないとしているが、実際には民間でも広く使われそうなので、もっとよく考えなければならないだろう。広く官民で利用できるようにするためには証明書に記載されるプライバシー情報などを適切に扱える仕組みが必要なので、このアプローチは注目される。今回は、現在のI-Dのステータスの報告と、更なる修正が必要との報告が行なわれていた。

その他のセッション

New Comer's Training

2月29日の13:00-14:00に開催された、初めて参加する聴衆のためのガイダンス講座で、今回は初めての試みとして通常の英語でのセッションのほか、韓国語でのセッションも開催されていた。

英語でのセッションは、約120名が参加しIETFの概要と標準化の流れと基本的な考え方として“Rough consensus and running code”が説明された。一言で言えば、「細かなことは気にせず、動くものを（追認して）標準化する」ということであり、ITU-T/ISOなどとは異なる標準化ポリシーの元に「標準化」が進められていることが説明されている。IETFのこのスタンスが、インターネットの急速な発展とdog yearといわれる急速な変化に何とか追従している理由ともなっている。

Editor's Training

2月29日13:00-15:00に開催され、参加者は40名ほどであった。

Editor's Trainingは、Internet-Drafts/RFCを書く人に対してのセッションであり、RFC Editorがどのような観点で「編集」を行いIETFでの標準化文書が作られるかの過程の説明を行う。Editorとしての心得や、どのタイミングでRFC Editorに送るべきかなどが説明された。

Internet-Drafts/RFCを作成する面で役に立つツール類の紹介もあった。Internet-Drafts/RFCは、基本はnroffで作成されているが、XMLにも対応できており、それらのTipsなどの説明があった。

セッションは、多くの質問が寄せられ、当然とはいえ、Internet-Drafts/RFCを書くことがセッション参加者の

主な興味対象であることが感じられた。

紹介されたツール類は、以下のようなものである

1. Text Formatting Tools / http://www.rfc-editor.org/formatting.html
2. xml2rfc / http://www.ietf.org/rfc/rfc2629.txt
3. nroff(groff)
4. Microsoft word template / http://ftp.rfc-editor.org/in-notes/rfc-editor/2-Word.template.rtf
5. LaTeX
6. MIB reference and compilers

Security Tutorial

2/29の15:00-17:00に開催された。参加者は300名程度。満席であり、SUNのRedia Perlman女史が説明した。Redia女史は、ARPの開発者としても知られている人物で、IETFの長老の一人である。

インターネットでなぜ、Securityが重要であるかに関しての説明を、技術的なコンセプト、守るための個別の技術などを平易に、解説しており、特に暗号技術に関しても多くの説明を行っていた。暗号に関しては、「勝手に暗号を作るべきではなく、きちんとレビュを受けたものを使うのが望ましい」というコメントを残していた。セキュリティプロトコルは大変難しいので、全部自分でやるのではなく、複数の人間が共同して行うことが重要とも言っていた。

セッション終了後、Redia女史に「大変有効なセッションなのでスライドをもらえないか」と聞いたところ、後日連絡することを快諾された。その後、このドキュメントはIPAと共同で翻訳され、Webページから公開されている。

Redia Perlman女史(中央)と稲田氏(左)

Security Tutoriaruの会場

http://www.ipa.go.jp/security/ietf/ietfsectut-ja-20040608.pdf

WG Chair Training

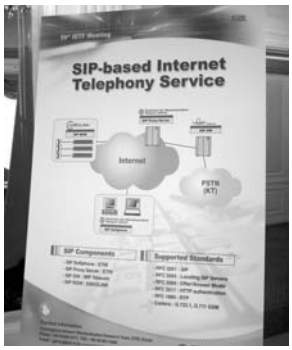
2月29日13:00-15:00に開催。Mararet Wassermanが説明した。

WG Chairになった人、またはこれからなろうとしている人向けに、WG Chairの役割と責任の範囲が解説された。また、WGを公正かつオープンかつ生産的に運用するためのノウハウが紹介された。このセッションはIETF参加者全員が聞くことが出来、特にWGのChairとして指名されていなくても聞くことが可能である。

参加者は、10数名程度と少数であったが、WG運営に必要な作業や情報の紹介は、WGを運営しようとする人々だけでなく、WGに参加して具体的な活動をしていく(例えばI-Dを執筆したりする人々)にとっても非常に有益なセッションだった。

オープン性と公正性を保つための工夫として、オフラインミーティングに参加できない人々に配慮して必ずMLでの確認を求めたり、言語や文化の異なる人々のために、オフラインミーティングでも口頭でのコミュニケーションに頼らず文書を記録として残せるよう注意を促すなど、IETFの本質的な運営ノウハウが非常に興味深かった。

WG Chairとなるべき人々に対して、IETFの基本思想である“Rough Consensus, Running code”を改めて説明するあたり、基本思想の維持徹底を心がける努力を欠かしてないことも窺えた。



SIP利用IPv6電話の説明


SIP利用IPv6電話のデモ

IPv6 Demoについて

今回のIETFは、初めての試みとしてIPv6の製品群のデモンストレーションが同じ会場ホテルの別室で行われた。これはホストである韓国 Korea Telecomの思惑とIETFの思惑が一致したために実現したようである。デモ会場には、SIPを利用したIP電話が置かれ、国際電話を無料でサービスしていた(通話料はKorea Telecom持ちのようである)。デモンストレーションを見る限り、特にIPv4/IPv6の違いを意識せずにアプリケーションを利用できるようである。日本へテスト的に電話をしてみたが、SIP応用のIP電話は、十分に実用に耐える品質を持っているようだ。

現時点ではSIPのパケットに関しては暗号化・電子署名といった伝送路中での盗聴・改竄対策はなされていないが、IETFのSIP関連のWGでは、SIPパケットに対して暗号化・電子署名を行うための議論が進められている。


KEIS6デモの一部

SIPパケットをPKIベースのCMS(Cryptographic Message Syntax)で暗号化·電子署名を行うことが提案されており、比較的早期に暗号化·電子署名が導入されると思われる。

韓国は、国策としてIPv6を推進しており、Seoul市内に大規模なIPv6デモンストレーション場(KEIS6、IETF会場より見学ツアーあり)を用意するなどIPv6の普及を図っている。日本においても国策としてIPv6の発展・普及は行われているが、韓国に比べると迫力に欠ける感じがするのは何故だろうか。

以上、ソウルで開催された第59回IETFのほんのさわりをご紹介した。IETFはやはり一度は行って話を聞いてみる価値があるだろう。一度だけではすまないかもしれない。自分の問題意識を持って、実際に起こった問題や提案を持っていけば、多少言葉が通じなくても歓迎されるのは間違いないだろう。さまざまな問題点を議論し、より良いRFCを作り上げ、世界の多くの開発者や、ひいてはそれを使うユーザが幸せになることが、共通の目的意識だろう。JNSAのChallengePKIプロジェクトも、11月のI-DのRFC化へ向け、更に磨きをかけて行きたい。

より詳しい報告は、別途JNSAのWebページでも掲載する予定なので、そちらも参照していただければ幸いである。

会員企業ご紹介⑪

株式会社インフォセック
(http://www.infosec.co.jp)

インフォセックは、情報セキュリティが高度情報化社会のさらなる発展の原動力になると考え、2001年7月に、情報セキュリティの専門会社として三菱商事株式会社によって設立されました。米国最先端企業の、SAIC社、Symantec社と技術提携しており、最先端の情報セキュリティ技術をリーズナブルなコストでお客様にご提供しております。日本側技術者も充実しておりますので、日本の風土・特質に合致した、きめ細かなサービスをご利用いただけます。

■ インフォセックの特徴 ■

- 情報セキュリティ専門会社
- 米国最先端企業との技術提携
- 日本の風土に合ったサービス提供
- マネジメント系とシステム系の統合
- ベンダーフリー

■ コンサルティング ■

• マネジメント系とシステム系の統合

マネジメント系と、システム系・技術系を組み合わせた、効率的な対処方法をアドバイス致します。

• 多彩なサービス

・個人情報保護法対策支援
・ISMS、Pマーク認証取得支援
・セキュリティポリシー作成支援
・セキュリティ監査
・ネットワーク／ウェブ脆弱性診断
・アーキテクチャーレビュー
・研修・トレーニング

• 豊富な実績

官公庁、金融機関、放送局、電力会社、
家電メーカー、通信会社、製薬会社、
鉄道会社、広告会社、医療法人、総合商社

• 多数の資格保有者

ISMS主任審査員、システム監査技術者、
BS7799リードオーディタ、CISM、
CISSP、MCSE、CCNA、CNE、MCNE、
情報セキュリティアドミニストレータ

■ セキュリティ監視サービス ■

• 常時監視

24時間、365日、年中無休でお客様のシステムログを監視致します。

•大量のログからイベントを検出

高度な監視システムによって大量のログの中から、セキュリティ・イベントを探し出します。専門分析員が過剰検出を排除し、お客様の負担を軽減します。

•最大シェア

世界および日本国内において、お客様から最大のご支持をいただいております。

お問い合わせ先
株式会社インフォセック
〒105-0001 東京都 港区 虎ノ門4-1-17
城山MTビル
TEL: 03-5425-3460 FAX: 03-5425-3461
E-Mail: information@infosec.co.jp

オムロン フィールドエンジニアリング株式会社

(http://www.omron-fe.co.jp/)

OMRON

オムロン フィールドエンジニアリング株式会社(OFE)は、オムロンの社会産業システム機器の設置工事や保守サービスを目的に1970年に創業しました。
オムロンの社会産業システムは、自動改札機や券売機などの駅務システム、都市交通や高速道路の渋滞を緩和する交通管制システム、ATMなどの店舗端末を中心とする金融系システム、工場のラインの自動制御などインダストリアルシステムなど、極めて公益性・公共性が高く可用性・保全性が要求され、短時間に復旧ができないと社会的インパクトが大きいシステムが多いのが特徴です。このため24時間365日のソーシャルセキュリティ・ニーズにお答えすることが、OFEの創業時来のDNAとなっています。たとえば、条件の厳しい首都圏の金融系システムでは30分以内到着の保守サービスを提供、またコンビニエンスストアATMに対しては深夜を含めた24時間365日のオンサイト保守サービスを提供しています。
一方、近年では、外資系大手PCメーカーやルータ・スイッチ通信機器などの設置、監視、保守やウイルス発生時のオンサイト駆除なども行っており(オムロン外の顧客比率は50%程度)、社会産業システム保守で鍛えられた作業品質で高い評価を頂いております。
OFEのサービスの特徴をまとめますと：
○迅速かつ均質な保守サービス　○全国150サービス拠点　○365日24時間対応　○誠実・元気・３K厭わず
となります。

オンサイト・ソリューションとサービスの見える化

弊社では、お客様の現場におけるさまざまなニーズに柔軟にお答えすることを「オンサイト・ソリューション」というコンセプトに集約し、このキーワードの元で保守サービスの質的・量的な劇的向上に努め、保守サービスのビジネスプロセス全般の仕組みをレベルアップすることにより、お客様の顧客満足度(CS)向上に日々努力を重ねています。
このようなオンサイト･ソリューションのＣＳ向上の具体策が「サービスの見える化」です。弊社では、コールセンタを中心に、

①お客様の障害の早期復旧
②障害復旧のための、オンサイト作業が必要な場合、お客様の契約にそった部材の配送(緊急・翌日)・CE(カスタマエンジニア)の派遣
③オンサイト作業の進捗報告

といった一連の保守サービス･プロセスをご提供しておりますが、オンサイト対応を行うCEはi-mode携帯を活用しており、お客様にサービスプロセスの進捗状況を逐次Webで公開しています(可視化)。

他の「サービスの見える化」の代表例は下記の通りです。

・対お客様：Web上での障害復旧用動画マニュアルの提供
　オンサイト保守の、Webでの公開(お客様との契約による)
・対ＣＥ　i-modeでCEに対して、障害対応を行う装置の、障害履歴
　アクセスの最短経路提示・故障コード検索、
　部材の到着時刻確認　等

なお、コールセンタを中心とした一連の「サービスの見える化」によるビジネスプロセス改革で、(社)日本オフィスオートメーション協会様の IT総合賞、リックテレコム社様のコールセンタ・アワード2004 マネジメント部門 金賞、などを受賞いたしました

最後に

弊社はJNSA参加企業では珍しい事業を行っています。しかしながら、ソーシャルセキュリティの最後の砦はオンサイトサポートであると考えています。24時間いつでもどこでも、迅速にお客様に駆け付けるサービスを提供させていただくのがOFE。オンサイトサービスでお困りの場合にはOFEに是非相談ください。

お問い合わせ先
オムロン　フィールドエンジニアリング株式会社
システム営業本部　ITインフラ営業部
03-3448-8128　it_sales@ofe.omron.co.jp

株式会社コネクタス
(http://www.connectous.co.jp/)

CONNECTOUS
株式会社コネクタス

3つの事業がCONNECTOUSを支える柱です。

セキュリティ製品開発、IT教育、ネットワークシステムコンサルティング、この3つがコネクタスを支える柱です。コネクタスは、それぞれを別個に事業展開するのではなく、相互に密接に連携させ、相乗効果を生み出すことで、より優れた確かなサービスの提供を目指しています。セキュリティ製品開発過程に得た技術や知識を各業務に反映させ、コンサルティング業務を行う上で経験した事例や問題を教育部門や研究開発部門にフィードバックし、IT教育の質の向上と新たなるソリューションや製品の開発につなげていきます。

低価格・低運用コストのメール監査アプライアンス「メールタンク」発売中

電子メールというツールは便利な反面、社内の重要情報を簡単に社外に持ち出せてしまうという大変危険な面も持っています。また昨今では電子メールで重要な商談を進めてしまう例も散見されますが、機器故障などによる電子メールの紛失の備えができていない例も多いようです。メール監視技術を提供する製品の必要性は高まっていますが、既存製品の多くは、導入コストや管理コストの面で中小規模の事業者の方が導入することが難しいという問題点があります。コネクタスでは、これらの問題点をクリアしたメール監視アプライアンスを開発、2004年7月より販売を開始しました。

■製品の特長

1．低価格

メールの監視に特化したことでフォレンジック機器としては圧倒的な低価格を実現しました。メールのみに特化して保存するため、一般のフォレンジック機器よりも少ないハードディスク容量で効果的なデータフォレンジックを行うことが出来ます。

2．簡単設置＆低管理コスト

メールサーバとLANの間にメールタンクを設置するだけで簡単に監査を開始できます。特殊なハブの購入等、他の機器の必要はありません。設定項目も少なく、ブロードバンドルータ感覚で設置が可能です。また、メンテナンスフリーのアプライアンスですので、専門知識を持った管理者を置く必要がありません。最初に簡単な設定を行うだけで、メールの監査を開始出来ます。

3．簡単監査

メールの監査を行うべき立場にある方は、機器の管理者と同じではないはずです。メールタンクは、この認識に基づいて、機器の管理とメールの監査を別々の方が行うことができるよう設計されています。また、監査は普段利用するブラウザやメールソフトから可能なように設計されています。監査担当者が難解な専用ソフトの操作方法を覚える必要はありません。

Security Solution 2004 出展のお知らせ

2004年10月20日（水）～22日（金）の期間、東京ビッグサイトで開催される「Security Solution 2004」（日経ＢＰ社主催）に出展いたします。弊社出展では、弊社製品「メールタンク」を展示にてご紹介させていただく予定です。

ご多忙のことと存じますが、是非ご来場下さいますようご案内申し上げます。

お問い合わせ先
株式会社コネクタス
〒108-0023東京都港区芝浦４丁目16番25号
第３安全ビル ３Ｆ
TEL:03-5730-4851 FAX:03-5730-4853
e-mail:info-jnsa@connectous.co.jp

株式会社ステラクラフト

(http://www.stellar.co.jp/)

STELLAR CRAFT

ネットワークに対して“確かに自分であること”を伝えられるなら、
もっと可能性が拡がるはず。

それぞれの個人が、また企業の中のスタッフが、ネットワークをもっと安心して活用できる、そして権限を与えられる仕組みを、実際に使えるカタチにして、世の中に送り出していきます。
“ユーザ認証”の可能性を追求し続けるエンジニア集団、それが ステラクラフト です。

■ RADIUS認証サーバ「Enterpras」シリーズ

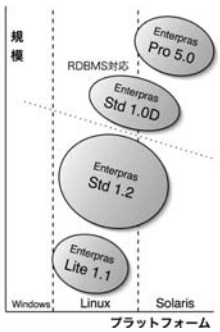
ステラクラフトがスクラッチから開発し機能向上を続けているIETF標準準拠のRADIUS認証サーバ群です。変革を続けるネットワーク環境に対して、常に最新のユーザ認証の仕組みを取り入れて、高性能で信頼性の高いAuthentication, AuthorizationとAccountingの各機能を提供します。

Enterpras Pro 5.0

通信事業者、大企業向け
オプションが充実(EAP、IPv6、Proxy、各種OTPほか)
Oracle、DB2対応
カスタマイズ対応

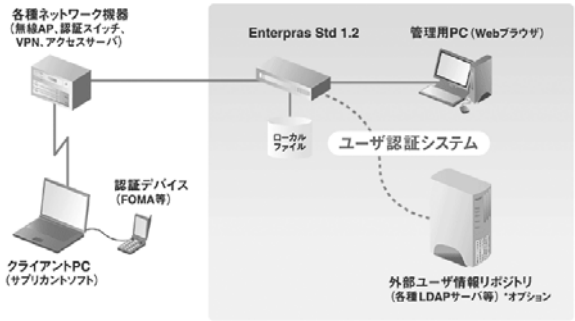
Enterpras Std 1.2

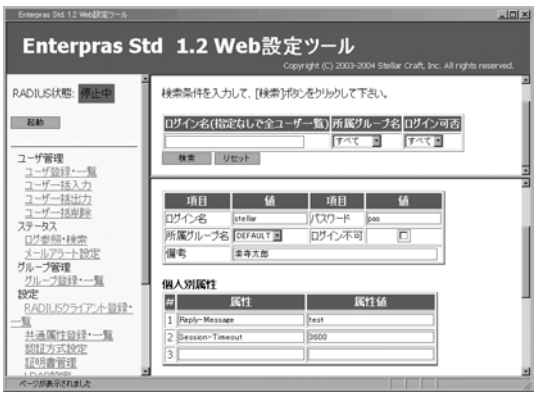
中規模エンタープライズ向け
EAP標準サポート
ローカルファイル,LDAP, UNIXアカウント,Windowsドメイン



◆ Enterpras Std 1.2

ミッションクリティカルな大規模組織に多数導入済みのEnterpras Proをベースに、一般企業／学校のネットワークアクセスに必要な機能を抜粋、信頼性の高いユーザ認証基盤をリーズナブルな価格で提供します。
多彩なユーザ情報リポジトリにも対応し、構築の容易なスタンドアロン構成から、既存システムとのLDAP連携まで、柔軟なユーザ情報管理の仕組みを、使いやすい管理ツールとともに実現しました。

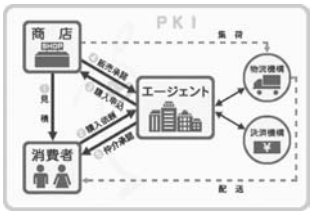




ユーザ毎、所属グループ毎に異なる返信アトリビュートが設定でき、任意のユーザを一時的にログイン不可とする制御や特定のログ出力を検出して通知するアラート機能も完備していますので、管理初心者にも簡単にきめ細かい認証制御が可能です。

■ プライバシー保護 EC システム「Patease」

しっかりしたユーザ認証を基盤として、ネットワークの新しい信頼モデルを構築するというステラクラフト独自のコンセプトを実装したECの先進的システムです。
PKI技術を活用して個人情報を保護することにより、気軽で安心できる電子商取引を可能としています。



お問い合わせ先
株式会社ステラクラフト 企画営業部
本社：
〒530-0002 大阪市北区曽根崎新地1-4-20 桜橋IMビル
Phone: 06-4799-3333 / Fax.: 06-4799-3330
東京事業所：
〒105-0021 東京都港区東新橋1-1-17 大鉄ビル
Phone: 03-5537-5890 / Fax.: 03-5537-5895
E-mail: sales@stellar.co.jp

寿限無株式会社
(http://www.jugamu.jp/)

寿限無株式会社は、企業や自治体などでセキュリティポリシー／コントロールの立案から実施運用に様々な立場で関わってきたコンサルタント/エンジニアが集まり、2003年9月に設立されました。
寿限無株式会社は今後ますます高まる情報セキュリティシステム構築の要求に、コンサルテーション、システム開発、導入、運用において高い技術力とサポート体制でお応えします。
私たち寿限無が常に大切にしたいと考えていることは、ネットワークシステムの先にあるユーザの利益も意識することです。単なる技術者としての視点ではなく、各スタッフの経験と人間性に裏付けされたアプローチがクライアントから支持される理由であると考えています。

■サービスメニュー

寿限無株式会社では情報セキュリティシステム構築に向けて豊富なサービスメニューを提供しています。寿限無のメンバーはインターネット創世記からISPやコンピュータメーカ、大手SI社への技術サポートの経験を通じて情報システム構築技術には高い技術を有しています。特にIPネットワークやUNIXシステムでは数多くの大規模システム構築とサポートを経験しています。そうした経験から、セキュアな情報システム構築にはシステム構築技術だけでなく、適切なポリシー作成、スケジューリング、システム監査などシステム全体のマネージメントが不可欠と考えます。また、システム管理者だけでなくエンドユーザの教育もシステムを安定してかつセキュアに保つためには不可欠な要素です。

寿限無ではこうした企業姿勢のもと、特にセキュリティポリシーコンサルティングとトレーニングに注力していきたいと考えています。

・セキュリティポリシー作成/コンサルティング
・システム/セキュリティ監査
・セキュリティトレーニング
・セキュリティ関連認証取得支援
・セキュアドネットワーク構築/コンサルティング

■おすすめのサービス

寿限無では様々なサービスの中でも現在特に注力しているのが以下のサービスです。

・セキュリティトレーニング
・認証取得後コンサルティング

昨今の個人情報流出事件を見るまでもなく、情報セキュリティ事件の過半数は組織に関係した内部犯行です。また情報取扱者の認識不足、知識不足による不注意での情報漏洩も後を絶ちません。こうした事態には従来の技術的アプローチだけでは力不足です。情報システム利用者の教育トレーニングが不可欠です。

従来からシステム管理者への教育、知識啓蒙は多く行われてきましたが、情報セキュリティについてはシステムに関わる全員の意識レベル向上を目的とした教育トレーニングが不可欠です。寿限無ではコンピュータメーカー公認トレーナーや、教育機関での講師経験が豊富なトレーナーがお客様の組織業種に合わせてトレーニング教材の作成から、トレーニングの実施、トレーナー育成までお手伝いいたします。

人員教育とともに最重要と考えているのが認証取得後のコンサルティングです。ISMSや情報セキュリティ監査制度、プライバシーマークなど、公的な情報セキュリティ認証監査制度が充実してきました。しかしながら、いまだ認証取得が目的となっていて、認証取得後のシステム改善、維持更新には手がまわらないという声が聞かれます。寿限無では認証取得後のシステム改善計画策定や情報セキュリティ対策実施手順策定のお手伝いなど、実務のサポートをご提供いたします。主要な情報セキュリティ機器の対策実施手順についてはテンプレートを用意し、短時間に対策手順書作成が可能な体制を整えています。

情報セキュリティ対策でお困りな点はぜひ寿限無までご相談ください。

お問い合わせ先
寿限無株式会社
〒488-0853　尾張旭市旭前町広久手4902-1
TEL 0561-52-3503　FAX 0561-55-0172
E-Mail info@jugame.jp
http://www.jugame.jp/

東日本電信電話株式会社

(http://www.ntt-east.co.jp/tms/category/security.html)

NTT東日本の提供するトータルセキュリティソリューションSeCIO：

NTT東日本では、これまでネットワークとＮＴＴグループの研究開発力を強みにしたセキュリティソリューションSeCIOを提供してまいりました。

今年度は、頻発する情報漏洩事件への対応、企業内のウィルスの大規模感染の防止、個人情報保護法への対応をテーマにしたソリューションを強化し、「情報漏洩対策ソリューション」、「デスクトップ管理ソリューション」、「セキュリティプラットフォームソリューション」、「セキュリティコンサルティング」の４つのメニューを用意しました。

1）情報漏洩対策ソリューション

◆情報漏洩評価サービス：

最近の情報漏洩事例を考慮し、ネットワーク、端末管理、業務管理、作業環境、組織環境、コンプライアンスの６つの側面から社内を総点検し情報漏洩の危険性について総合的に評価します。

◆PC盗難・紛失対策：

ハードディスクの暗号化などにより、万が一のPCの紛失、盗難、廃棄パソコンからの内部情報流出を防ぎます。

◆機密文書漏洩対策：

ファイルのアクセス制限やファイルの暗号化による機密文書の不正な流出を防止します。

◆ログ収集・分析：

ログ収集、分析によりセキュリティ事故を追跡可能にします。また普段からログを記録することにより情報漏洩を抑止します。

◆サーバセキュア化：

Webサーバ要塞化／メール暗号化／DBサーバ暗号化などにより各種サーバのセキュア化をします。

2）デスクトップ管理ソリューション

◆ウィルス対策：

セキュリティパッチおよびウィルスパターンファイルの更新を一元管理することにより、社内ネットワークにおけるウィルスの大規模感染を防ぎます。

◆IT資産管理：

社内のIT資産情報を迅速に把握し、社内資産の有効活用、不正ライセンスの排除によるコンプライアンス対策に効果を発揮します。

◆デスクトップ管理導入コンサルティング：

端末管理システムを導入したものの、導入が進まない、パフォーマンスが出ないというお客様にコンサルティングを行い、効果的な導入支援をお手伝いいたします。

3）セキュリティプラットフォームソリューション

◆サーバ更改をトリガーとしたＡＤ導入：

WindowsNTのサポート切れに伴うサーバ更改を契機に、グループ・ポリシーを一括管理できるActiveDirectoryの導入を推進し、セキュリティの強化を実現します。

◆ネットワーク更改をトリガーとした検疫ネットワーク導入：

ネットワークの更改を契機に、不正端末をネットワークからシャットアウトする検疫ネットワークの導入を推進し、セキュリティの強化を実現します。

◆シングルサインオン導入：

ユーザ認証管理を一元化することで、セキュリティ強化と利便性の向上の両立を実現します。

◆センタセキュリティ対策：

外部からの不正アクセスに対し、データセンタレベルの高信頼なファイアウォール、侵入検知システムの導入を支援します。

4）セキュリティコンサルティング

◆セキュリティポリシー策定：

現状での情報資産の管理状況や業務におけるセキュリティ管理の実態を調査し、お客様の現状に即した“セキュリティポリシー”の策定をお手伝いします。

◆認定取得支援サービス（Pマーク、ISMS）：

企業の情報セキュリティ対策に関する認証制度（ISMS，プライバシマーク）の取得に向けて、セキュリティ専門家が的確なコンサルティングを行い、ISMS、Pマークの取得のお手伝いをします。

◆セキュリティ教育：

eラーニング方式により、従業員皆様の情報セキュリティに関するリテラシーを短期間で向上させるためのお手伝いをします。

お問い合わせ先

NTT東日本　ビジネスユーザ事業推進本部
ビジネスソリューション営業部
第二システムグループ　セキュリティ担当
〒112-0004　東京都文京区後楽2-5-1
TEL：03-3830-5934　FAX:03-3830-3547
e-mail secio@ml.bch.east.ntt.co.jp

マカフィー株式会社
(http://www.mcafee.com/jp/)

マカフィー株式会社は、ネットワークの不正侵入を阻止し、次世代の複合型攻撃、脅威からコンピュータシステムを保護する、業界で最も包括的なコンピュータ セキュリティ ソリューションを日本のネットワーク社会に提供しています。マカフィーは、大企業、官公庁・自治体、中小企業および個人ユーザのセキュアなネットワーク環境をサポートしています。

Protection-in-Depth™ストラテジー

今日のビジネスが、ワイヤレスデバイスやスマートフォンに依存する度合いが増すにつれ、ネットワークは、“穴だらけ”の状態になり、その結果、脆弱になってしまいます。そのため従来のファイアウォールや不正侵入検知システムでは、十分安全とは言えません。また、IT管理者は、脆弱点パッチの対応のため、いつも慌ててネットワーク上の処理に追われることになります。McAfee® Protection-in-Depthストラテジーは、コンピュータやアプリケーションサーバ、ウェブサービスエンジンのセキュリティを包括的にセキュアなものにするために、企業や一般ユーザ、政府機関をサポートしています。

McAfee System Protection

McAfee VirusScan® Enterprise 8.0i

マカフィーが提供する最新のウイルス対策、McAfee VirusScan Enterprise 8.0i。このMcAfeeソリューションは、ウイルス対策にMcAfee Entercept®の不正侵入防止技術とファイアウォール技術を統合した、PCおよびファイルサーバー用のワンストップソリューション、次世代のウイルス対策です。この強力な統合ソリューションは、バッファオーバーフローや複合型など、今日発生している新しいタイプの攻撃からプロアクティブにネットワークを防御します。さらに先進の危機管理機能を備えていますので、攻撃による損害や経費の削減を実現します。

McAfee IPSはゼロ・デイアタックにも対応

ATTACK	McAfee Anti-Virus	McAfee IntruShield
Sasser		Block
Bugbear.b	Block	Block
Nachi		Block
Lovsan		Block

McAfee ePolicy Orchestrator®

最大25万台までのクライアントPCをカバーできる高いスケーラビリティを誇るウイルス対策統合管理ソリューションです。

McAfee WebShield® Appliance

ハイエンド製品McAfee WebShield e1000は、毎時16万通のメールスキャニングを実現するハイスループット製品。SMTP、HTTP、FTP、POP3のスキャンに対応しています。

McAfee VirusScan ASaP

国内7000社、50万台超のユーザベースをもつ、全自動アップデート、つまり管理者不要を実現した、企業向けASP型クライアントウイルス対策サービスです。

McAfee Network Protection

McAfee IntruShield®

McAfee IntruShieldは、特許技術を集積・統合することで、たとえ複雑なネットワークであっても、既知、未知の攻撃やDoS攻撃から防御し、従来の不正侵入検知製品につきものの誤検知（False Positive）の問題を解消します。この技術を利用すれば、ネットワークの周縁だけでなく、データセンターなどネットワークのコア、また遠隔の支店までを含むすべての範囲が防御できます。今日の巧妙な攻撃から確実にネットワークを防御する、それがMcAfeeのIntrushieldです。

お問い合わせ先
マカフィー株式会社
コーポレートコミュニケーション部
〒150-0043 東京都渋谷区道玄坂1-12-1
渋谷マークシティウエスト20階
TEL：03-5428-1100　FAX：03-5428-1480
marcom_japan@mcafee.com

菱洋エレクトロ株式会社

(http://www.ryoyo.co.jp)

弊社は、1961年に半導体商社の草分けとして設立し、国内外の半導体ビジネスを中心に激変する社会の中で、お客様のニーズを的確に捉えて、事業を拡大してまいりました。一方、エレクトロニクス総合商社としての位置付けの基に情報機器ビジネスにも力を入れ、HP、Sun、インテル、MS、エプソン、京セラミタ、三菱、NMV製品を主とした、ソリューションビジネスを積極的に展開しています。また、新規取扱い製品を増やし、ストレージ、セキュリティに関連する高機能商品を取り揃え、コンサルティングから導入、インストール、運用管理、保守、常駐に至るきめ細かなサポートを行います。

情報漏洩対策フォレンジック製品『MSIESER』(エムシーサー)のご紹介

『MSIESER』の特徴

『MSIESER』は通信パケットを記録し電子メール、Webアクセス、FTP転送の内容を解析して表示する機能を、HP Proliantに搭載して提供するアプライアンス製品です。

情報漏洩、不正アクセスを正確に記録/復元！

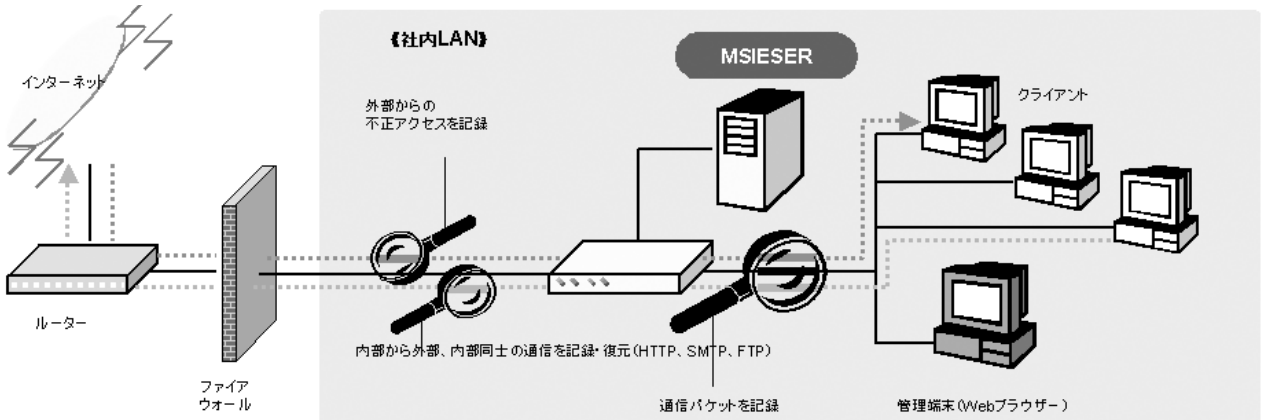
電子メールの送受信者、そして内容や添付ファイルを記録/復元できるほか、WebアクセスのURLや掲示板への書き込み内容をユーザーごとに確認することもでき、内部情報の流出や不正行為の証拠を示すことができます。

簡単、迅速な操作性を追及！

膨大に記録されるデータの中からキーワードやURLで電子メールやWebアクセス履歴を抽出する検索機能、アクセスの頻度を視覚的に確認できるグラフ解析など、ネットワークの利用状況や不正利用者の追跡を支援する機能も充実しています。操作は全てWebブラウザーから簡単に行えますので、特別な知識がなくても導入、運用することができます。

『フォレンジックサーバー』とは？

法廷に持ち込めるほど確かな方法でデータを取得、保管するシステムです。
情報事故に対する捜査や法廷論争におけるシステムへの不正アクセス、情報漏洩に対し、迅速な捜査と正確な証拠を示すフォレンジック・サーバーが重要になっています。



弊社はMSIESER（エムシーサー）と各種のセキュリティ製品を組み合わせて、お客様にご満足いただけるセキュリティソリューションをご提案させて頂いております。

お問い合わせ先
菱洋エレクトロ株式会社
システム情報機器営業第2本部　営業推進部
担当：　武石　野嶋
TEL：　03-5565-1635　FAX：03-3546-6377
e-mail：solution@ryoyo.co.jp

JNSA会員企業情報

JNSA会員企業のサービス・製品・イベント情報です。

■製品情報■

○eTrust Secure Content Manager v1.1 日本語版

情報漏えい、eメールに起因する法的責任、迷惑メール、ウイルス、悪意あるプログラム、不快なコンテンツなど、様々な脅威からビジネスを保護する統合コンテンツセキュリティソリューションです。下記2製品を2004年8月末からリリース予定。完全日本語版。
(1) eTrust SCM Gateway: ゲートウェイ製品。
　価格: ￥240,000（50ライセンス）～
(2) eTrust SCM Suite: クライアント、サーバ、グループウェアのウイルス対策製品も含めた包括的な製品。
　価格: ￥390,000（50ライセンス）～
http://www.caj.co.jp/etrust/scm/

◆お問い合わせ先◆
コンピュータ・アソシエイツ株式会社
CAジャパン・ダイレクト（0120-704-600）

○情報漏洩対策及び個人情報保護へのセキュリティ・ソリューション「pointsec」のご紹介

pointsecの特徴としては、「ＨＤＤ丸ごと暗号化」によるデータセキュリティ，「ＩＤ＆パスワード認証」による認証セキュリティ，クライアントへの「ポリシー強制管理」によるセキュリティポリシー機能を融合したソリューションです。
pointsecは、国内では官公庁，金融，医薬をはじめとして、多くの企業に導入していただいております。
http://www.tokyo.metro.co.jp/security/pointsec/index.html

◆お問い合わせ先◆
株式会社メトロ 情報通信営業部
TEL 03-5789-1022
E-MAIL：sales@tokyo.metro.co.jp
URL：http://www.metro.co.jp

○Sidewinder G2 Security Appliance

難攻不落のファイアウォールとして、発売以来、侵入実績ゼロを誇るSidewinderファイアウォールに、アンチ・スパム、アンチ・ウィルスを始めとする様々な機能を追加し、かつ、導入がスムーズなアプライアンスにパッケージングした究極のゲートウェイ セキュリティ ソリューションです。開発当初から、「ファイアウォールで防げない攻撃」を防ぐことを実証し続けてきた、アプリケーション・プロキシ群も、さらに機能強化が図られています。
http://www.securecomputing.co.jp

◆お問い合わせ先◆
セキュアコンピューティングジャパン株式会社
TEL：03-5114-8224
E-MAIL：japan_info@securecomputing.com

■サービス情報■

○「個人情報漏えい対策のためのコンサルティング」

ネットマークスでは、相次いで発生する企業の情報漏えい防止のため、特別のコンサルティングチーム「Netmarks Secure Excellent Partners（NSEP）」を結成、企業における情報セキュリティについて、経営的な観点から現状の把握、対策方法の策定や実装まで、常に全体最適から顧客のことを考え、信頼できるパートナとしてお客様をサポートします。
http://www.netmarks.co.jp

◆お問い合わせ先◆
株式会社ネットマークス
セキュリティビジネスソリューション部
TEL：03-3423-5926
E-Mail：info@netmarks.co.jp

○セキュリティ教育

SEA/J情報セキュリティ技術認定　開講日程
基礎　□東京会場　9月14日15日
　　10月12日13日
　　□大阪会場　9月16日17日
　　10月20日21日
応用マネジメント編　9月16日17日
　　10月14日15日
応用テクニカル編　9月29日30日10月1日
　　10月20日21日22日

--新サービスをリリース致しました--
●個人情報保護法対応した規定策定支援ツール
　「Privacy Policy Implement Kit」
●脆弱性の管理対策「脆弱性マネジメントサービス」
http://www.hucom.co.jp/

◆お問い合わせ先◆
株式会社ヒューコム
SMS事業本部
TEL：03-5306-7339
E-MAIL：sms@hucom.co.jp

■イベント情報■

○「Trustedソリューションセミナー」
　～最強の情報漏洩対策～

最強の情報漏洩対策として注目を浴びている「セキュアOS」及び関連したソリューションをご紹介いたします。
まだセキュアOSを理解されていない方にもご理解いただけるよう仕組み（概念）を整理してご説明させていただくとともに、具体的なソリューション事例をご紹介して自社やお客様への

具体的な適用方法をご理解いただけるようなプログラムにしております。
http://www.jtsl.co.jp/japanese/event/20040806.html

◆お問い合わせ先◆
日本高信頼システム株式会社
セミナー事務局
E-MAIL：sales@jtsl.co.jp

○４月まで間に合う個人情報保護を目的とした
認証取得セミナ

開催日時：8月25日(水)　13：00より受付開始
開催場所：ホテルニューオオタニ（紀尾井町）

個人情報保護対策の観点から注目すべき法律や規格を再確認すると同時に要点を解説します。
具体的な対策方法として、マネジメントシステムの導入が有効です。
本セミナでは、「プライバシーマーク認証」や「ISMS認証」取得を想定した組織のための実践的な手法を考えていきます。
http://www.dit.co.jp/

◆お問い合わせ先◆
株式会社ディアイティ　セキュリティビジネス推進室
TEL：03-5634-7651
E-MAIL：sbd-info@dit.co.jp

情報セキュリティ対策を推進する「セキュリティ対策推進協議会」が設立

近年、コンピュータウイルス/ワームの被害の拡大、情報セキュリティに関連する事件の発生等により、情報通信基盤におけるそれらの影響を懸念する声が高まっており、IT関連団体相互の密接な連携による的確かつ迅速な対策が強く望まれています。そのような背景を受け、JNSAを含む以下のIT関連企業・団体の賛同のもと、本年初頭より設立準備会を開催し、このたび「セキュリティ対策推進協議会（SPREAD: Security Promotion Realizing sEcurity meAsures Distribution）が設立されました。

設立団体/企業

Telecom-ISAC Japan (Telecom Information Sharing and Analysis Center Japan)
NPO 日本ネットワークセキュリティ協会（JNSA）
その他22社（予定）

「わかりやすく」「迅速に」「確実に」

一般に、各種のセキュリティ情報は一般ユーザにとって、難解になりがちで、ユーザにおける対策が不十分なケースが多く見られます。SPREADでは、公開された脆弱性情報や対策情報などのセキュリティ関連情報を「わかりやすく」「迅速に」「確実に」インターネット利用者に流通させることを推進していきます。

SPREADでは、その目的を達成するため、JNSA及びTelecom-ISAC Japan を中心に、各種メーカー、ISP、システムインテグレータ、量販店、メディア、各種コミュニティや政府関連機関など、コンピュータ、インターネットに関係する様々な業界の団体と密接に連携を図っていきます。

「セキュリティ対策推進協議会」の活動内容

SPREADでは情報セキュリティ対策を推進するために、次の活動を行っていきます。

- セキュリティ関連情報を、「わかりやすく」整理、編集し、一般のインターネット利用者向けに提供する。
- 各種ウイルス、ワームなどが発生した際はもちろん、発生する前の段階から、適切な情報を「迅速に」、インターネット利用者へ「確実に」発信する体制を整え運営する。
- セキュリティ啓発イベントを開催し、インターネット利用者に積極的なセキュリティ対策推進活動を実施する。

本協議会では9月より順次情報発信のサービスを開始し、秋には全国的啓発イベント「情報セキュリティ強化週間（仮称）」の実施を計画しています。

2003年度JNSA WG成果報告会レポート

JNSAの各WGの活動成果報告会が下記の要領で開催されました。
2004年5月18日（火）10:00～15:30
会場： 大手町サンケイプラザ
会場いっぱいの盛況で、関心の高さを物語っていました。簡単に内容をご紹介しておきます。

303号室
教育部会　10:00～12:00
10:00～10:30　「情報セキュリティ教育の動向とJNSA」 教育部会長　東京電機大学教授　佐々木良一先生 10:30～11:10　スキルマップ作成WG （株）富士総合研究所　佐久間敦氏
11:10～11:20　休憩
11:20～12:00　ITSS実証実験評価WG （株）ヒューコム　松田剛氏
12:00～13:00　昼休み
政策部会　13:00～15:30
13:10～13:50　個人情報保護ガイドライン作成WG （株）大塚商会　佐藤憲一氏 13:50～14:10　プライバシー保護実装研究WG 日本IBMシステムズ・エンジニアリング（株）　久波健二氏
14:10～14:20　休憩
14:20～15:00　セキュリティ被害調査WG 損保ジャパン・リスクマネジメント（株）　山本匡氏 15:00～15:30　情報流通検討委員会 横河電機（株）　武智洋氏

1. 教育部会

教育部会長の佐々木先生から、情報セキュリティ教育の動向についてのお話がありました。技術者教育とともにリテラシー教育の重要性についても指摘され、特にJNSAのインシデント調査のデータを利用して、社内教育の有無とセキュリティに関する被害の有無との関連があることをあげられました。

この後、スキルマップ作成WGの報告書の紹介と、ITSS実証実験の内容について報告されました。

2. 政策部会

最初に政策部会長の下村氏から挨拶があり、個人情報保護ガイドライン作成WGの報告が行われました。WGでは「個人情報保護法対策　セキュリティ実践マニュアル」を執筆しており、この情報も紹介されました。

次に新しくできたプライバシー保護実装研究WGが紹介され、プライバシ保護のために必要なセキュリティ機能のリスト作成や実際に実現するための要件調査などの活動予定について報告がされました。

休憩を挟んで、セキュリティ被害調査WGから、3回目となる報告書について説明があり、2003年度の試みとして、情報漏洩があった場合の損害賠償額の予想計算式について解説されました。

最後に情報流通検討委員会について状況報告がありました。6月30日のN+I 2004Tokyoのコンファレンスの場で「セキュリティ対策推進協議会」の設立について発表されましたが、今後は協議会としてセキュリティー対策情報の円滑な伝達を実現して行くことが紹介されました。

3. 技術部会

教育部会、政策部会の隣の部屋で、別トラックとして技術部会の報告会が開催されました。技術部会は丸1日の発表が行われ、活発な活動を印象付けていました。

セキュリティポリシーWGは、ポリシーから脅威・脆弱性および残存脅威を導いた考え方について説明しました。また、2004年度の活動として、ISMSやJIS X5080との適合性や、サンプルの全面見直しを行う予定であることが示されました。

暗号使用ポリシーテンプレート作成WGは、データ暗号化（情報の機密性）のための暗号使用ポリシーテンプレートを作成したことが報告されました。

情報セキュリティ標準調査WGは、情報セキュリティに関係する標準、認定制度などには多くの規格があり、相互関係が整理されていないとの認識で、ISO15408, 17799, ISMS, SSE-CMM等の関連をまとめて一覧表を作り公開したことが説明されました。

セキュアOSとその活用方法研究WGは、各社のTrustedOSまたはSecureOSと呼ばれているものの勉強会を行い、日本国内におけるセキュアOS市場の動向を歴史にそってまとめました。

不正プログラム調査WGは、不正プログラムの定義、分類、構造、対策などについて調査分析を行い、報告書が作成されました。

Webセキュリティ調査・検証WGは、Web環境に特化した攻撃手法やその対策を調査・研究することを目標にし、Webの脆弱性・Webに特化した攻撃手法の調査、および具体的な対策の調査、攻撃検知・防御ソリューションによる対策実証実験を行います。

ここで昼休みを挟み、午後からはPKI相互運用技術WGから報告されました。ChallengePKIの活動を中心に、2003年度は「セキュリティAPI」や「タイムスタンプ」といったより具体的で詳細な内容に踏み込んでいます。IETFに対する国際標準にもインターネットドラフトを提案するなど、国際的な役割が認識されてきています。2004年の11月にはRFCとして提案することを予定しています。

電子署名検討WGは、電子署名活用モデルの提案を目標に設立されました。まず、「阻害要因の分析」を行い、公的個人認証サービスに関する意見・情報の交換を行って、電子署名を取りまく環境の再確認を行いました。2004年度は活用モデルについて考察する予定でしたが、ひとまずS/MIMEにおける電子署名の使われ方という具体的なテーマで実証実験などを行う予定となっています。

データストレージ＆セキュリティWGは、JNSAとJDSF(日本データストレージフォーラム)が合同で設置したWGで、セキュリティを重視したデータマネジメントのあり方について検討しています。

インターネットVPN-WGは、インターネットVPNを導入する際の注意点、安全なVPNを実現するための運用方法などについて考察することを目的としています。色々なVPN方式について比較検討しています。

コンテントセキュリティWGは、コンテントセキュリティの新たな定義を提案し、コンテンツの不正流通を監視することなどにも視点を置いています。

ハニーポットWGは、実際に複数のハニーポットを構築して使い方や、どのような利用方法が適しているのかを考え、更にデータ(LOG)の利用の仕方、また、収集した情報に含まれるプライベート情報の取り扱い方などについても調査・考察することを目指しています。

以上、簡単に昨年度の活動をご紹介しましたが、JNSAのWebページに更に詳しい内容が掲載されていますので、ぜひご参照ください。また、各WGの活動内容については、実際にWGにご出席いただくのが一番正確な情報が得られます。一度事務局までご相談いただければ、調整いたしますので、ぜひご連絡ください。

304号室
技術部会　10:00～15:30
10:05～10:35　セキュリティポリシーWG **（株）NTTデータ　土屋茂樹氏** **10:35～10:55　暗号使用ポリシーテンプレート作成WG** **（株）アークン　板倉行男氏**
10:55～11:05　休憩
11:05～11:15　情報セキュリティ標準調査WG **セコム（株）IS研究所　渡並智氏** **11:15～11:25　セキュアOSとその活用方法研究WG** **日本高信頼システム（株）　澤田栄浩氏** **11:25～11:45　不正プログラム調査WG** **（株）アークン　渡部章氏** **11:45～12:00　Webセキュリティ調査・検証WG** **（株）アークン　斉藤純平氏**
12:00～13:00　昼休み
13:00～13:30　PKI相互運用技術WG **セコム（株）IS研究所　松本泰氏** **13:30～14:00　電子署名検討WG** **NTTコムウェア（株）　磐城洋介氏**
14:00～14:10　休憩
14:10～14:30　データストレージ＆セキュリティWG **（株）ネットマークス　内田昌宏氏** **14:30～14:50　インターネットVPN-WG** **セコムトラストネット（株）　若林進二郎氏** **14:50～15:10　コンテントセキュリティWG** **（株）ネットアーク　松本直人氏** **15:10～15:30　ハニーポットWG** **園田道夫氏**

JNSA「セキュリティ・スタジアムセミナー第二弾」

「情報漏洩の傾向と対策」開催される

セキュリティ・スタジアム企画運営WG
根津　研介

2004年5月28日(金)、人事労務会館（品川区大崎）にて、「情報漏洩の傾向と対策」と題したセミナーが開催されました。盛夏を思わせるような晴天に恵まれ、81名の方が参加される中、活況なセミナーとなりました。

情報漏洩のケーススタディ

まずは、2004年に入って急に頻発しはじめた情報漏洩の様々なケースについて、分類や傾向、影響、原因などについて、IPA非常勤研究員/JNSA研究員の園田道夫氏が講演されました。特に、2002年、2003年と年間20件程度であった企業の情報漏洩事例が、2004年に入ってたかだか半年程度の間に、既に倍の40件以上も出ている状況に危機感を訴えられていました。

また、ほとんどの事例において、流出経路不明のものか内部犯行によるものが大多数であり、「本来の手順の確率と遵守、それを支える技術的なサポート」が最も重要であることを強調されていました。

私自身、春先の信販系の情報漏洩の被害（不正請求ハガキや、週に2, 3回勧誘系の電話が会社に急に来るようになった）と思しき状況になったことを考えると、とても人ごととは思えず、「明日は自分も被害者」というぐらいの気構えで、事に当たる必要があることを痛感しました。

ログは何でも知っている

続いて、伊原秀明氏がコンピュータが保存する様々なログの可能性と限界について講演されました。通常、記録されるログとコンピュータフォレンジックでそれぞれ追跡できる範囲、限界から、人の操作（キーボード、マウス、画面）の記録（ログ）の重要性と取り方についての解説、プライバシーへの配慮、削除されてしまったファイルの追跡や復活方法などについて解説されていました。

また、これらの電子的な記録について、訴訟等の際に証拠となり得るための方法についても触れられていました。

会社は何をすればいいのか？

続いてのプログラムでは、園田氏が、2005年に一般企業でも施行される個人情報保護法を念頭に置き、企業のIT部門のマネジャーが、経営陣や、現場に対して「どのようなアプローチ」で「何を行っていく必要がある」のかについて講演されました。具体的な対策だけでなく、セキュリティ投資の費用対効果、という項目についても少しだけ述べられていました。

IT予算については、例えば売上の10%など、ごく大雑把な目安が語られているだけでしたが、例えば各対策の費用対効果や、全体への波及効果など、もっと突っ込んだ話をしていくべき時期にきている、と感じました。

パネルディスカッション

最後に、園田氏、伊原氏に加え、弁護士の尾崎孝良氏を迎えてパネルディスカッションが行われました。特に、尾崎氏からは、企業が社員の社内でのコンピュータを使った行動の記録（ログ）を取ることとプライバシー権との関係の論拠になる判例の紹介など、情報漏洩に関連する判例や論拠について、非常に興味深いお話がありました。

次回はセキュリティスタジアム

セミナー参加者のみなさんのご協力もあり、次回のセキュリティスタジアムWGの活動は、本番である「セキュリティスタジアム」の開催となります。開催日程や参加要項等はまだ未決ですが、11月頃に開催を予定していますので、こぞってご参加ください。詳細は、決定次第、事務局よりお知らせさせていただきます。

事務局お知らせ

JNSA ANNOUNCE

1. 主催セミナーのお知らせ

●「Network Security Forum 2004」

■日　　時：2004年10月28日（木）·29日（金）

■会　　場：青山TEPIAホール（４F）
　　＆エクジビションホール（３F）

■形　式：コンファレンス（聴講無料）＆デモ展示

■運　営：IDGジャパン株式会社

今年のNSFでは、JNSA5周年の節目として、参加無料のコンファレンスとセキュリティセミナーの併催で行います。プログラム詳細はNSF2004ホームページをご覧ください。
http://www.idg.co.jp/expo/nsf/index.html

2. 後援イベントのお知らせ

1.「ネットワーク・セキュリティ・ワークショップ in越後湯沢 2004」

会　期：2004年10月７日（木）～９日（土）
主　催：ＮＰＯ新潟情報セキュリティ協会
会　場：湯沢町公民館（新潟県）
　　http://www.yuzawaonsen.gr.jp/conf/

2.「AVAR2004 in Tokyo」

会　期：2004年11月4日（木）～5日（金）
主　催：AVAR Association of anti Virus Asia Researchers
会　場：シェラトングランデ東京ベイ
http://www.avar.org

3.「電子自治体フェアTOKYO 2004」

会　期：2004年11月16日（火）～17日（水）
主　催：社団法人日本経営協会
会　場：池袋サンシャインシティ
http://www.noma.or.jp/show/densi_tokyo/2004/index.html

4.「マルチメディア＆ＶＲメッセぎふ2004」

会　期：2004年11月17日（水）～18日（木）
主　催：マルチメディア＆ＶＲメッセぎふ実行委員会
会　場：ソフトピアジャパン（岐阜県大垣市加賀野4-1-7）
　　http://www.softopia.or.jp/mvm

3. JNSA部会・WG 2004年度活動

1. 政策部会

（部会長：下村正洋/ディアイティ）

政策部会では、様々な基準・ガイドラインの策定や、他団体との連携などを検討している。

【セキュリティ被害調査WG（情報セキュリティインシデント被害調査プロジェクト）】

（リーダー：山田英史氏/ディアイティ）

2001年から継続して被害調査を行い、被害額算定モデル等を提案してきた。今年度は、これらのモデルのレベルアップをさらに図りたい。

主な活動内容としては、下記の通り。

- 前年度調査の課題への対応と再調査実施。
- 簡易算出方法、各種指標のさらなる拡大および整理・精緻化
- 被害発生時の緊急ヒヤリング体制整備、事故情報の収集
- 公開された事故情報による被害額の算出対象事故の検討

【セキュリティベンダーとしての管理基準策定WG】

（リーダー：丸山司郎氏/ラック）

JNSA行動指針の運用方法検討を行なう。既存会員への周知と既存会員組織内での遵守状況確認から、広報活動やアンケートの実施、運用マニュアルの作成等を検討していく予定である。

また、JNSA所属会員にとって、有益な運用スキームの構築、行動指針の遵守状況を対外的なアピールに利用可能なものとする。

【セキュリティ監査WG】

（リーダー：大溝裕則氏/ジェイエムシー）

情報セキュリティ監査制度の運用開始に伴い求められている、業界別、業態別の監査（管理）基準および監査人の質の向上について研究を行なう。

【マーケットリサーチWG】

（リーダー：玉井節朗氏/IDGジャパン）

国内のセキュリティ市場規模、セキュリティ製品の導入状況を調査し、今後の市場予測を行なう。この結果から以下の目的を達成する。

1　企業のセキュリティシステム普及状況を確認し，強化すべきポイントを把握する。
2.　国内のセキュリティ産業の動向を把握し、自供企画

の材料として会員企業に提供する。
3. 将来のセキュリティ普及の方向性を検討する材料とする。

【プライバシー保護実装研究WG】
（リーダー：久波健二氏/
日本IBMシステムズ･エンジニアリング）
プライバシー保護のために、IT技術はどこまで可能かの調査・研究をする。各社製品技術でどこまで対応可能かを調査し、製品だけでは満足できない要件をどうすればITで補完できるかの検討、ITで可能な部分と組織・運用で可能な部分の明確化などを行なう。
予定成果物は、プライバシー保護に必要な機能をまとめた『プライバシー保護モデル』と、実際の設計・構築を意識した実装モデル。

【セキュリティ会計ガイドライン検討WG】
（リーダー：佐野智己氏/凸版印刷）
企業における情報セキュリティ確保への取り組みを会計的視点から認識･評価･伝達（ディスクロージャー）する仕組みとして、『環境会計』に倣い、『セキュリティ会計』を定義し、その基本的な考え方を取りまとめる。
予定成果物は『ガイドライン』の上程。

---

2. 技術部会

（部会長：佐藤友治氏/インターネット総合研究所）
技術部会では、今年度も成果物を作成するワーキンググループと勉強目的のワーキンググループに分かれて活動を行なう。その他、予算を得た活動は、プロジェクトとして活動を進める。主なワーキンググループ活動予定は、以下の通り。

【セキュリティポリシーWG】
（リーダー：小杉聖一氏/NECソフト）
セキュリティポリシーは現在セキュリティマネジメントを実施するために必須のものであり、導入が進められている。実際に策定する場合、規格、標準、法令などを知り、何を決めればいいのか？　何を注意しなければならないのか？　を知っている必要がある。本WGでは、セキュリティポリシー策定のポイントをISMS認証基準などを参考にし、リスク分析や規程書（ドキュメント）作成のポイントや実際の実装方法を議論しながら成果を公開していく。

【コンテントセキュリティWG】
（リーダー：松本直人氏/ネットアーク）
コンテントセキュリティに関するガイドラインドキュメントを作成。広く一般的に定義が無いコンテントセキュリティの定義と具体的なカテゴリー分けと手法を分類整理する。主な活動予定は、上記をふまえた勉強会およびドキュメント作成など。

【不正プログラム調査WG】
（リーダー：渡部章氏/アークン）
トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加している。また、ウイルス、ワームも同様に近年では不正アクセスを目的としたものも少なくない。実際の不正アクセス技術ではこれらのツールを組み合わせて利用するケースが多く、不正プログラムとその対策の調査研究を実施し、その成果を普及させる。

【ハニーポットWG】
（リーダー：園田道夫氏/JNSA研究員）
2004年度は、2003年度に準備を整えたハニーポットサイトの運営を実際に行いつつ、そこからどのようなデータが得られるのか解析していく。その後はハニーポットサイトをさまざまに展開し、ネットワーク上の場所によって得られるものが違うか？とか、公開形態やサーバーによって異なるか？などのテーマを設定しながらデータを収集し解析していく。
また、ハニーポットだけにとどまらず、トラフィック解析などのテーマも追いかけていく予定。

【データストレージ＆セキュリティWG】
（リーダー：立身俊雄氏/ジェイエムシー）
企業がデータの運用および保存を行う際の指標の検討を行なう。世の中の基準やユーザアンケート等による調査・分析に基づく、マネジメントポリシの作成などを予定。なお、本WGは、JDSF（Japan Data Storage Forum）殿と協調して活動する。

【暗号使用ポリシーテンプレート作成WG】
（リーダー：板倉行男氏/アークン）
セキュリティ管理策として暗号製品を使用する場合、ISMSなどのセキュリティポリシー認証基準では暗号使用ポリシーの策定を推奨している。また暗号技術を使用する場合、暗号に使用する鍵管理のルールを明確にし、それが守られなくてはならない。そのため、暗号使用ポリシーのテンプレートを作成する。今年度はPKI、電子署

名の管理策をとる場合の暗号使用ポリシーを検討する。

【S/MIME検討WG】
（リーダー：磐城洋介氏/NTTコムウェア）
電子署名アプリケーションの普及と調査を目的として昨年発足した「電子署名検討WG」の活動を引き継ぎ、今年は電子署名・特に利用イメージで最も身近にPKI・電子署名を体験できる「S/MIME」について、各種メーラの調査・検証や利用のノウハウなど、関連情報の共有を行うことを目的とする。予定成果物は、「S/MIMEメーラ実装状況レポート（仮題）」。

【Webセキュリティ調査･検証WG】
（リーダー：斉藤純平氏/アークン）
Web環境に特化した攻撃手法やその対策を調査・研究し、また、この分野は実環境を使用しての攻撃実験や検知・防御ソリューションの検証が困難であるため、貸し出し可能な検証環境を構築する。予定成果物は、「Webセキュリティ調査・検証報告書」。

【PKI相互運用技術WG】
（リーダー：松本泰氏/セコム）
安全、安心な社会を構築する上でPKIの必要性を社会にアピールし、ネックとなるPKI相互運用性の問題などを自ら解決していく。
主な活動予定は、IETFの参加（年3回）、JESAPなどの他団体との連携、IETFのRFCなどの提案等。

【ChallengePKIプロジェクト】
（リーダー：松本泰氏/セコム）
2003年は、タイムスタンプの調査と開発環境をテストスィートに組み込むと共に、セキュリティAPIのあり方の調査とCriptAPIとJavaでのサンプルコードを公開した。
ChallengePKIで得た知見は、国際標準を検討しているIETFの場で議論を重ね、各方面のキーマンのレビューを受けRFCとして公開するための準備を行っている。

---

3. マーケティング部会
（部会長：古川勝也氏/マイクロソフト）
JNSA自身の認知度向上と、ネットワークセキュリティに関する普及・啓発活動を行う。

【セキュリティ啓発WG】
（リーダー：古川勝也氏/マイクロソフト）
昨年度経済産業省の委託事業として行なった「インターネット安全教室」を拡張して今年度も行なう予定である。その企画・運営協力を行なう。

【セキュリティスタジアムWG】
（リーダー：園田道夫氏/JNSA研究員）
不正アクセス手法の攻防の一大実験場「セキュリティスタジアム」の企画と運営を行なう。
2004年度はセミナーとスタジアム本大会をさらにシステマチックに開催できる仕組みを整えていく予定。セキュリティトピックのセミナーの企画や本大会企画準備、技術教育講座の企画なども検討していく。

---

4. 教育部会
（部会長：佐々木良一氏/東京電機大学教授）
ネットワーク・セキュリティ技術者の育成のために、産学協同プロジェクトを進め、大学や企業で行うべき教育のカリキュラムの検討やユーザー教育の在り方についての調査・検討などを行なう。

【スキルマップ作成WG】
（リーダー：佐久間敦氏/富士総合研究所）
ネットワークセキュリティ技術者に求められる知識やスキルを整理、体系化した「スキルマップ」を整備し、ネットワークセキュリティ技術者を育成に向けた各種施策の検討を行うことを目的とする。

---

5. 西日本支部
（支部長：井上陽一氏/ヒューコム）
JNSA西日本支部は関西に拠点を置くメンバー企業の協賛の下、西日本におけるネットワーク社会のセキュリティレベルの維持･向上並びに、日々高まる情報セキュリティへのニーズに応えるべく、先進性を追及すると共に、質の高いサービスを提供する事を目的として活動致している。
今年度は、関西方面でのセキュリティ啓発セミナーを中心として活動を行なっていく。

【セミナー運営WG】
（リーダー：中台芳夫氏/西日本電信電話）
西日本支部主催セキュリティセミナーのコンテンツの企画検討と運営を行なう。

4. JNSA役員一覧

会　長　石田　晴久
多摩美術大学教授・東京大学名誉教授

副会長　長尾　多一郎
株式会社ネットマークス 代表取締役社長

副会長　東　貴彦
マイクロソフト株式会社 業務執行役員

副会長　大和　敏彦
シスコシステムズ株式会社 執行役員CTO

理　事(50音順)

株式会社アイアイジェイテクノロジー
在賀　良助

株式会社ヒューコム
井上　陽一

株式会社大塚商会
宇佐美　慎治

三菱電機株式会社　情報技術総合研究所
後沢　忍

株式会社フォーバルクリエーティブ
浦野　義朗

浦山　清治

シムデスク･テクノロジーズ
岡村　靖

新日鉄ソリューションズ株式会社
甲斐　龍一郎

株式会社シマンテック
勝見　勉

セコムトラストネット株式会社
川上　博康

トレンドマイクロ株式会社
小屋　晋吾

株式会社ディアイティ
下村　正洋

株式会社ネットマークス
鷲見　晴美

ELNISテクノロジーズ株式会社
鈴木　伸秀

セコム株式会社
鈴木　優一

横河電機株式会社
武智　洋

マカフィー株式会社
田中　辰夫

株式会社IDGジャパン
玉井　節朗

NTTアドバンステクノロジ株式会社
辻　久雄

システムニーズ株式会社
中山　恵介

株式会社ＮＴＴデータ
西尾　秀一

株式会社ラック
西本　逸郎

大日本印刷株式会社
野久保　秀紀

東芝ソリューション株式会社
坂内　明

マイクロソフト株式会社
古川　勝也

NTTコミュニケーションズ株式会社
松尾　直樹

RSAセキュリティ株式会社
山野　修

古河電気工業株式会社
吉澤　昭男

グローバルセキュリティエキスパート株式会社
若井　順一

東京海上火災保険株式会社
綿引　宏行

監　事

清友監査法人　公認会計士
土井　充

顧　問

東京大学　教授
今井　秀樹

新東京法律事務所　弁護士
北沢　義博

東京電機大学　教授
佐々木　良一

慶応義塾大学　教授
武藤　佳恭

早稲田大学　客員教授
前川　徹

早稲田大学　教授
村岡　洋一

奈良先端科学技術大学院大学　教授
山口　英

東京大学　教授
吉田　眞

事務局長

株式会社ディアイティ
下村　正洋

5. 会員企業一覧

2004年7月30日現在　176社　50音順

【あ】
（株）アークン
RSAセキュリティ（株）
（株）アイアイジェイ テクノロジー New
（株）アイ・ソリューションズ New
（株）ITサービス
（株）アイ・ティ・フロンティア
（株）IDGジャパン
（株）アイネス
アイネット・システムズ（株）
アイマトリックス（株） New
（株）アクセンス・テクノロジー
あずさ監査法人
（株）網屋
アライドテレシス（株）
（株）アルゴ21
（株）アルテミス
（株）アンラボ
イーディーコントライブ（株）
伊藤忠テクノサイエンス（株）
学校法人 岩崎学園
インターネット セキュリティ システムズ（株）
（株）インターネット総合研究所
ｲﾝﾃｯｸ・ｳｪﾌﾞ・ｱﾝﾄﾞ・ｹﾞﾉﾑ・ｲﾝﾌｫﾏﾃｨｸｽ（株）
（株）インテリジェントウェイブ
インフォコム（株）
（株）インフォセック
（株）インプレス
ウッドランド（株）
AT＆Tグローバル・サービス（株）
（株）エス・アイ・ディ・シー
エス・アンド・アイ（株） New
（株）エス・エス・アイ・ジェイ
SSH コミュニケーションズ・セキュリティ（株）
（株）エス・シー・ラボ
NRIセキュアテクノロジーズ（株）
NRIデータサービス（株）
NECソフト（株）
NECネクサソリューションズ（株）
NTTアドバンステクノロジ（株）
NTTコミュニケーションズ（株）
エヌ・ティ・ティ・コムウェア（株）
（株）NTTデータ
（株）エネルギア・コミュニケーションズ
エムオーテックス（株）
エリアビイジャパン（株）
ELNISテクノロジーズ（株）
（株）大塚商会
オムロンフィールドエンジニアリング（株）

【か】
韓国電子通信研究院 New
キヤノンシステムソリューションズ（株）
キヤノン・スーパーコンピューティング・エスアイ（株）
京セラコミュニケーションシステム（株）
（株）ギガプライズ
（株）クインランド
クオリティ（株）
（株）グローバルエース
グローバルセキュリティエキスパート（株）
クロス・ヘッド（株）
（株）コシダテック
（株）コネクタス
コンピュータ・アソシエイツ（株）

【さ】
サイバーソリューション（株）
サン・マイクロシステムズ（株）
（株）シー・エス・イー
（株）シーフォーテクノロジー
（株）ジェイエムシー
ジェイズ・コミュニケーション（株）
（株）CRCソリューションズ
シスコシステムズ（株）
システムニーズ（株）
（株）シマンテック
シムデスク・テクノロジーズ New
寿限無（株）
（株）翔泳社
（株）情報数理研究所
新日鉄ソリューションズ(株)
図研ネットウエイブ（株）
（株）ステラクラフト
ストーンソフト・ジャパン（株）
住商エレクトロニクス（株）
住生コンピューターサービス（株）
セイコープレシジョン（株）
セキュアコンピューティングジャパン（株）
（株）セキュアソフト
セコム（株）
セコムトラストネット（株）
（株）セゾン情報システムズ
（株）セタ
セントラル・コンピュータ・サービス（株）
ソニー（株）
ソフトバンクBB（株）
ソラン（株）
（株）ソリトンシステムズ
（株）損保ジャパン・リスクマネジメント

【た】
大興電子通信（株）
大日本印刷（株）
ダイヤモンドコンピューターサービス（株）
（株）タクマ New
中央青山監査法人
（株）ディアイティ
TIS（株）
テクマトリックス（株）
デジタルアーツ（株）
デジボックス（株）
学校法人電子学園　日本電子専門学校
（株）電通国際情報サービス
監査法人トーマツ
東京海上火災保険（株）
東芝ソリューション（株）
東芝情報システム（株）
東洋通信機（株）　トヨコムネットワークシステムズ
（株）東陽テクニカ
凸版印刷（株）
トップレイヤーネットワークスジャパン（株）
トリップワイヤ・ジャパン（株）
トレンドマイクロ（株）

【な】
（株）ニコンシステム
西日本電信電話（株）
日本アイ・ビー・エム（株）
日本アイ・ビー・エム　システムズエンジニアリング（株）
日本オラクル（株）
日本高信頼システム（株）
日本コムシス（株）
（株）日本システムディベロップメント
日本セーフネット（株）
日本電気（株） New
日本電気エンジニアリング（株）
日本電気システム建設（株）
日本電信電話（株）　情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
ネクストコム（株）
（株）ネットアーク
（株）ネット・タイム
（株）ネットマークス
（株）ネットワークセキュリティテクノロジージャパン
ネットワンシステムズ（株）
ノベル（株）

【は】
（株）ハイエレコン
東日本電信電話（株）
（株）日立システムアンドサービス
（株）日立製作所
日立ソフトウェアエンジニアリング（株）
（株）ヒューコム
（株）ビー・エス・ピー
（株）PFU
ファルコンシステムコンサルティング（株）
（株）フォーバル クリエーティブ
富士ゼロックス（株）
富士ゼロックス情報システム（株）
（株）富士総合研究所
富士通（株）
富士通エフ・アイ・ピー（株）
富士通関西中部ネットテック（株） New
富士通サポートアンドサービス（株） New
（株）富士通ソーシアルサイエンスラボラトリ
（株）富士通ビジネスシステム
扶桑電通（株） New
（株）フューチャーイン
（株）プラーナ
（株）ブリッジ・メタウェア New
古河電気工業（株）
（株）プロティビティ

【ま】
マイクロソフト（株）
マカフィー（株）
松下電工（株）
（株）三菱総合研究所
三菱電機（株）情報技術総合研究所
三菱電機情報ネットワーク（株）
（株）メトロ

【や】
横河電機（株）

【ら】
（株）ラック
菱洋エレクトロ（株）
（有）ロボック New

【特別会員】
社団法人日本インターネットプロバイダー協会
特定非営利法人　アイタック
ジャパン データ ストレージ フォーラム

6. JNSA年間活動（2004年度）

4月	4月7日	第1回政策部会
	4月8日	第1回幹事会
	4月9日	第1回マーケティング部会
	4月10日	第1回教育部会
	4月24日	2004年度理事会
	4月27日	IETF参加報告会
5月	5月11日	2004年度技術部会
	5月12日	ITセキュリティ評価・認証制度勉強会
	5月18日	2003年度WG成果報告会（大手町サンケイプラザ）
	5月18日	JNSA総会（大手町サンケイプラザ）
	5月20-22日	コンピュータ犯罪に関する白浜シンポジウム後援
	5月28日	セキュリティスタジアムセミナー（人事労務会館）
6月	6月8日	第2回幹事会
	6月17日	第2回政策部会
	6月23日	臨時幹事会
	6月25日	第1回西日本支部会合
	6月28日-7月2日	Net World+Interop 2003 Tokyo後援
	6月29日	JASA情報セキュリティフォーラム後援
7月	7月12-16日	日韓ベンチャープラザ2004後援
	7月13日	個人情報保護法説明会開催
	7月19日	第2回西日本支部会合
	7月21-23日	ワイヤレスジャパン2004後援
	7月27日	第1回技術部会リーダー会
	7月28日	セキュリティ・マネジメント・フォーラム協賛
	7月30日	第3回幹事会
8月	8月3日	第3回政策部会
	8月27日	セキュリティAPIセミナー（セコムホール）
9月		
10月	10月7-9日	ネットワーク・セキュリティワークショップin越後湯沢2004協力
	10月28-29日	Network Security Form 2004（青山TEPIAホール）
11月		
12月	12月1日	Internet Week 2004開催
1月		
2月		

2003年10月～2004年2月「インターネット安全教室」開催

★JNSA活動スケジュールは、http://www.jnsa.org/active6.htmlに掲載しています。
★JNSA部会、WGの会合議事録は会員情報のページは、http://www.jnsa.org/member/member1.htmlに掲載しています。（JNSA会員限定です）

7. JNSAについて

■会員の特典

1. 各種部会、ワーキンググループ・勉強会への参加
2. セキュリティセミナーへの会員料金での参加および主催カンファレンスへの招待
3. 発行書籍・冊子の配布
4. JNSA会報の配布（年3回予定）
5. メーリングリスト及びWebでの情報提供
6. 活動成果の配布
7. イベント出展の際のパンフレット配付
8. 人的ネットワーク拡大の機会提供
9. 調査研究プロジェクトへの参画

入会方法
　Webの入会申込フォームにてWebからお申し込み、または、書面の入会申込書をFAX・郵送にてお送り下さい。折り返し事務局より入会に関する御連絡をいたします。

8. お問い合せ

特定非営利活動法人
日本ネットワークセキュリティ協会 事務局
〒136-0075　東京都江東区新砂1-6-35
T.T.ランディック東陽町ビル
TEL：　03-5633-6061
FAX：　03-5633-6062
E-Mail：sec@jnsa.org
URL：　http://www.jnsa.org/

西日本支部
〒530-0047　大阪府大阪市北区西天満2-3-14
西宝西天満ビル4F（株）ヒューコム内
TEL：　06-6362-2666

JNSA Press vol.11

2004年8月31日発行

発行所　特定非営利活動法人
日本ネットワークセキュリティ協会（JNSA）
〒136-0075
東京都江東区新砂1-6-35　T.T.ランディック東陽町ビル
TEL: 03-5633-6061　FAX: 03-5633-6062
E-Mail: sec@jnsa.org　URL: http://www.jnsa.org/

印刷　プリンテックス株式会社

ネットワークセキュリティフォーラム 2004

http://www.idg.co.jp/expo/nsf/index.html

会　期　：　2004年10月28日（木）・29日（金）
会　場　：　青山TEPIAホール
4F　セキュリティコンファレンス（定員200名）
3F　展示会
主　催　：　特定非営利活動法人日本ネットワークセキュリティ協会
料　金　：　参加無料

2005年4月より「個人情報保護法」が施行され、個人情報の取り扱いに対して企業は定格な対応をしなければなりません。個人情報保護に関する国際的な基準を十分踏まえた上で、制度面や技術面及び運用管理など、あらゆる角度からの十分な対策が求められます。コンピュータウィルス·不正アクセスの被害が増えている中、企業全体のネットワークセキュリティ対策が経営者にとっての最重要課題と考えられています。

2004年度は、昨年までのコンファレンス中心の構成から一新して、経営戦略面と技術管理面の双方の視点から構成するコンファレンスプログラムと、JNSA会員企業によるIT資産を守るためのセキュリティ製品やソリューションの展示会との両面で展開し、ITセキュリティ担当者の知識向上を主眼に置いて展開します。皆様のご来場を心よりお待ち申し上げます。

28日予定プログラム	「個人情報保護ガイドラインの概要と政府のセキュリティ政策の最新動向」 「ISMS認定/Pマークを早く安く取得するポイント」 「Identety Based Securityのプロジェクト」 「岐阜市情報セキュリティポリシーの策定と導入」 「個人情報保護対策　総点検　仮題と緊急対策」
29日予定プログラム	「コンポーネントからプロファイルへ　～セキュリティ技術開発から浸透への転換～」 「増大するネットワーク驚異の傾向と対策」 「これからのWebセキュリティを考える」 「ネットワークの自己防衛」

展示会出展社募集中

●スポンサーシップ　￥1,000,000－（税別）
オープンシアターセミナー1Day（10：00～17：00）、デモ展示ブース2小間提供(奥行き2m×幅2m＝1小間)、オフィシャルWebサイトでのロゴ掲載とリンク設定、ガイドブックでの貴社情報掲載、各種プロモーション資料・場内看板でのロゴ掲載、来場者向けダイレクトメール希望数提供

●デモブース出展　￥250,000－（税別）
デモ展示ブース1小間提供(奥行き2m×幅2m＝1小間)、ガイドブックでの貴社情報掲載、来場者向けダイレクトメール希望数提供

お問合せ

特定非営利活動法人 日本ネットワークセキュリティ協会事務局
〒136-0075　東京都江東区新砂1-6-35　T.T.ランディック東陽町ビル
TEL：03-5633-6061 / FAX：03-5633-6062 / E-Mail：sec@jnsa.org
NSF2004運営事務局　株式会社IDGジャパン内　nsf@idg.co.jp

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

〒136-0075 東京都江東区新砂1-6-35 T.T.ランディック東陽町ビル1階
TEL 03-5633-6061　FAX 03-5633-6062
E-mail: sec@jnsa.org　URL: http://www.jnsa.org/

西日本支部
〒530-0047 大阪府大阪市北区西天満2-3-14 西宝西天満ビル4F　(株)ヒューコム 内
TEL 06-6362-2666