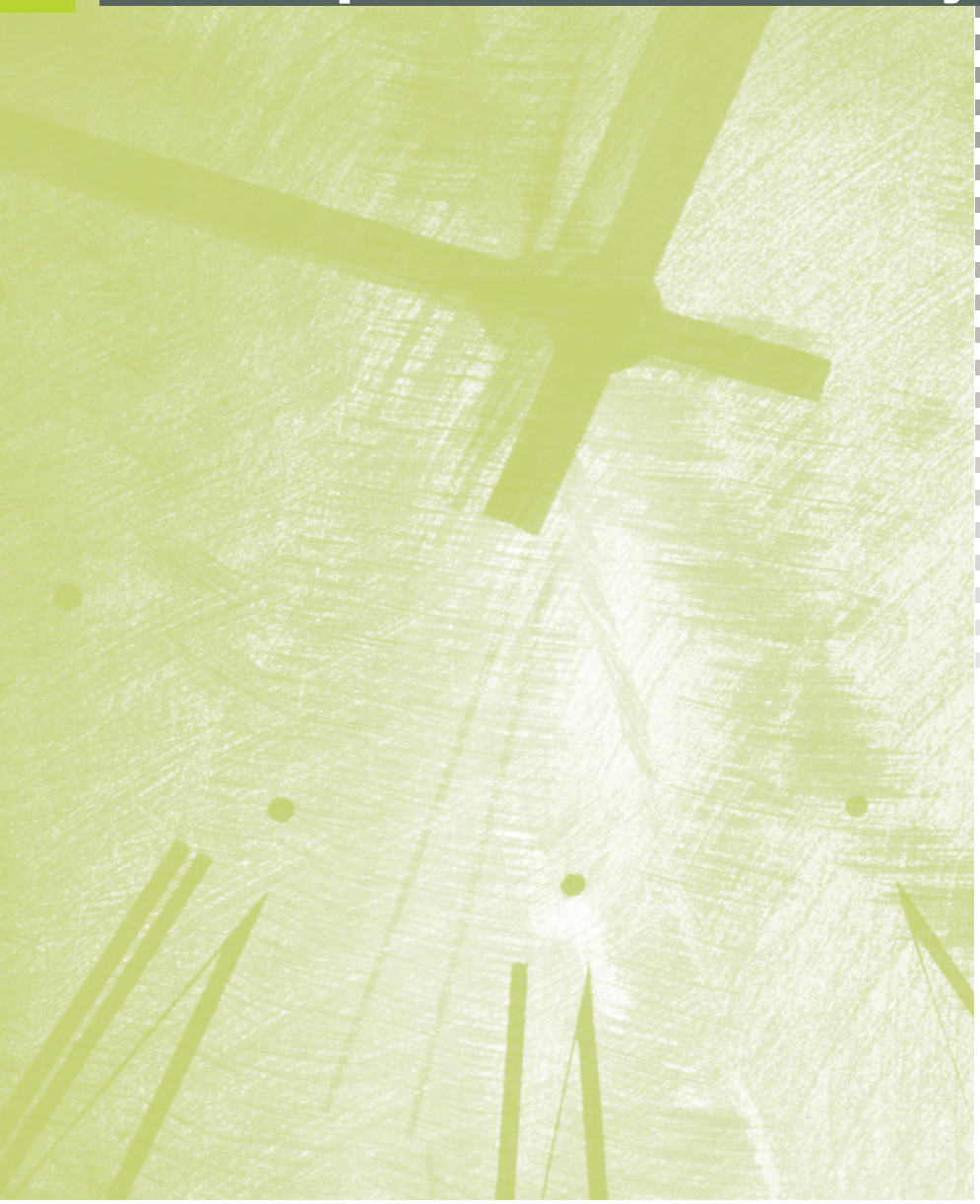
JNSA Press

Japan Network Security Association



Vol.8
September 2003

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

PKI Lovers

東京電機大学
佐々木　良一

公開鍵暗号とデジタル署名の概念が、DiffieとHellmanによって、米国のIEEEという学会の論文誌に招待論文として発表されたのは、1976年のことである。公開鍵暗号とそれを利用したデジタル署名の技術があったからこそ、インターネットでできることが飛躍的に広がったという意味で、これらの技術は20世紀の応用数学分野における最大の発明の1つといって良いだろう。

私が、日立製作所で、デジタル署名の応用システムの研究および研究管理に最初に携わってからでも15年以上になるが、今でも公開鍵暗号やデジタル署名、そしてそれらをベースとするPKI（Public Key Infrastructure）の仕組みは美しいと思う。そして、何とか、これらが、社会の中でさらに大きな位置を占めるようになってほしいと考えている。米国にもこういうように考える人はいて、弁護士のR.Merrill氏によるとそれらの人々をPKI Loversと呼ぶのだそうだ。そう言う意味では、私も立派なPKI Loversの一人だろう。

電子署名法が成立したにもかかわらず、PKIの普及はあまり進んでいないという声も強い。この分野についてビジネスとして否定的な見方をする人も増えてきている。

ビジネスがどう動いていくかの予測は本当に難しい。セキュリティという当たらない研究をずっと続けてきた人間としてはなおさらである。セキュリティの研究を始めたときにはISDNの立ち上がりとともにセキュリティシステムが普及すると考えていたのだが実際は、インターネット時代になってからであった。しかし、時代は動くべき方向に動き、そして動くときには、技術者の予想をはるかにこえて激しく動くのだと思っている。

わたしは、15年前の段階で認証機関の必要性を認識し、そのサービスの実現を損害保険会社などに勧めつつ、自分でそのビジネスを立ち上げようなどとは全く考えていなかった。1990年代中盤になって、ベリサインなど新興の企業がサービスをはじめるのを見て、米国のベンチャー精神のすごさを痛感するとともに、時代はやはり動くべき方向に動くのだと思った。そして、その後、暗号やデジタル署名などの技術を核としたシステムの受注が日立としても急速に増大し、私たちの研究成果が、特許の活用とともにビジネスに直接的に結びつく時代となっていった。

今後、認証機関はいろいろに機能を拡大していくだろうと考えている。従来は狭義の認証機関が中心だったが、今後は、時刻や取引内容そのものを公証する機関や、取引主体の信頼を証明するブランド認証機関も出現してくると考えられる。そして、それらがアプリケーションと結合して大きなビジネスになっていくだろう。この予想があたってほしいというのが、PKI Loversとしての私の願いである。

2002年度情報セキュリティ被害調査報告について

株式会社損保ジャパン・リスクマネジメント
山本　匡
株式会社NTTデータ
大谷　尚通

情報セキュリティ被害調査ワーキンググループでは、前年に引き続き、情報セキュリティインシデントの被害調査をプロジェクトとして行った。
今年は、昨年の調査及び被害モデルのみならず、情報漏洩事故による被害の影響についての考察を加え、２部構成とした。各部の概要は「2.目的」の通りである。(なお、本報告では、紙面の構成上、第一および二部をまとめて報告する。)

1. 目　的

サイバーテロや重要インフラセキュリティに対する関心は、益々高まり、今まで以上に重要インフラである情報システムにおけるセキュリティインシデントに関する過去の事例や現状についても関心が高まっている。

しかし、これらセキュリティインシデントに関する具体的な事例や被害額についてのまとまった情報は殆ど無い。インシデントの性質上、一般に公表されることが稀であるということに加え、そもそも被害の定義が曖昧であることも、情報が得られない大きな原因となっている。

また、同様なことは、対策の面でも生じており、対策定義の曖昧さにより、対策コストの情報は、まだ不足している。

そこで＜第１部＞では、昨年同様にアンケートやヒアリングによって、国内におけるサイバーテロや重要インフラ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を行った。この情報から得られる結果を基に、昨年度提案したセキュリティインシデントの被害額や情報セキュリティの対策投資額を推計するモデルに対し、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」の把握と効果の計測、効率的なマネジメントの実現において、更に精緻なモデルとするため検討を加え、2002年度モデルとして提案する。

また、＜第２部＞では、社会的な反響があり、関連者も非常に多数に上る事故種類の一つとして、今回「情報漏洩」を取り上げた。この「情報漏洩事故」は、どの企業にも共通の脅威であり、個人情報保護法案の進捗を踏まえると、経営者としては当然認知すべきリスクの一つである。

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った。

1 第1部の概要

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算出モデルについて、下記の内容をまとめている。

(1)「情報セキュリティインシデントに係る被害額・対策の投資費用に関する調査」

アンケートやヒアリングにて調査すべき項目を設定し、実際の企業においてインシデント発生や発生で要した費用(被害額)を調査した。

また、情報セキュリティインシデントの対策として実施されている取り組みへの投資額についても調査した。

(2)「被害額算出モデルの提案」

前年作成した情報セキュリティインシデントに関する被害額の算出モデルについて、更なる検討を加えたモデルを作成した。

具体的には、システム対応者の労務費用だけでなく、損害賠償に要した費用、復旧等に要した人件費、ハードウェア等物理的被害、イメージダウンによる被害、業務の停止による逸失利益などを想定し、被害額を算出するモデルの再検討と提案を行った。

(3)「情報セキュリティインシデント対策の標準モデルと対策費用」

前年調査との対比を交えた現時点で考えられる被害抑制のための標準的なモデルや望まれる対策レベルや予算規模などの提案を行った。

2 第2部について

情報漏洩による被害想定と考察について、当ワーキンググループの一案として、下記内容をまとめている。

(1)「情報漏洩による損害賠償被害額の想定」
2002年に発生した、情報漏洩事件について調査を実施し、そのインシデント内容を分析した。本分析結果を元に、当ワーキンググループとして、個人情報の価値およびその情報が漏洩した際における賠償金額等について、いくつかの仮定に基づいて被害額を算出した。
(2)「情報漏洩による企業価値への影響(株価面での考察)」
情報漏洩による企業価値低下の一端を探るため、2002年に情報漏洩事件を生じた企業について、情報漏洩の事故発生と当該企業の株価の動きについて、どの様な関係があるのかを調査し、本結果を元に、当ワーキンググループとして影響額を算出した。

2. 調査の概要 (以降、第1部について記述)

1 調査対象
・セキュリティ被害調査WGメンバーにて調査を依頼し、了解頂いた日本のインフラや基幹産業を構成する企業や組織。
・JNSAメンバー企業を中心とするIT関連企業。(一部に非IT企業含む)

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。
・アンケートは、昨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大幅に修正したアンケート用紙を使用。
・JNSAメンバーへのアンケートは、JNSA事務局長の依頼文章と共に送付し、記入後、事務局へ返送、集計を行った。
・JNSAメンバー以外へのアンケートは、ヒヤリング担当者より先方へ個別依頼にて収集。

3 調査の結果
3.1 ヒヤリング調査の結果
(詳細は報告書参照)
3.2 アンケート調査の結果(集計表)
(詳細は報告書参照)
3.3 アンケート回収率とヒアリング引受率
アンケートの回答率37%(昨年比▲6%)であるが、回答件数は12件増加している。ヒアリング承諾18件、承諾率50%程度は、ほぼ昨年同レベルである。
3.4 アンケート拒否の主な理由
自社の情報セキュリティに対する取り組み方の詳細を答えることがポリシーに反する場合や、セキュリティ内容の回答に対する抵抗があげられる。

4 調査結果の分析と特徴
今回の調査内容について、情報セキュリティに関連が大きい部分を中心に分析を行うとともに、昨年の調査結果との比較も行った。
4.1 本年調査の調査結果と考察
詳細は報告書参照。概要は下記の通り。
・業種:JNSA会員企業中心であり、情報系が多い。
・対策状況:基本対策はほとんど実施済み。
4.2 前年度調査結果と今年度調査結果の比較
詳細は報告書参照。概要は以下の通り。
・規定の制定が10%増加。
・取引契約における対策の強化が増加。
・パッチ適用の増加。
・教育関連の予算増加。
・ウイルスチェックは、95%以上普及。

5 被害状況の概要
前年2001年度の被害報告は調査対象55件中33件(61%)あったが、本年2002年度は同66件中11件(17%)と前年の約1/4に大きく減少した。また、被害範囲も低く留まり、被害金額は12万円程度と低い。
一定水準のセキュリティ対策は実施されているため、被害の拡大をもたらすのは外部要因ではなく、故障など不可抗力的なものや運用手順上の問題に起因する場合に限定された結果となった。

6 調査結果の分析と特徴(総括)
今回のアンケートによると各社のセキュリティ対策については、ファイアウォールやコンピュータウイルス対策

は約100%が配備し、侵入検知システム（IDS）も43.9%が導入しているという結果となった。また、パッチの適用も100%が実施している。

ファイアウォール、ウイルスチェック、IDSなどの導入により、不正侵入・コンピュータウイルスへの技術的対策は定着してきたが、昨今問題になっている情報漏洩については設定ミスや関係者による不正といった人的要素が高く、技術的対策よりも管理・運用面の対策が求められる傾向にある。

運用面については、ポリシー等規定を設定している企業は87.9%になり、連絡体制の整備、教育の実施も高い比率で実施している。このように、技術面・運用面の整備が進んだことが今回の調査で被害額が低く抑えられる結果に結びついたと考えられる。

しかし反面、被害を受けたと回答した企業も同様に技術的対策やポリシーの策定は実施しており、教育の徹底やチェック機能の強化に再考の余地があることを明らかにした。利便性とのバランスを考慮しながらも、罰則規定など強制力を伴う運用ルールや管理体制の強化が企業にとって今後の課題となるだろう。

予算面に関しては、65.2%の企業が情報セキュリティに割り当てる予算を情報システム関連予算の一部として計上しており、また、売上高に占めるセキュリティ予算の割合も非常に低く、企業活動の中でセキュリティ対策が優先順位の低い位置にあることを示唆している。

セキュリティ対策は効果が見えにくいというのも予算が確保できない理由のひとつと考えられるが、今後のアンケートおよびヒアリング内容については、導入しているセキュリティ技術がインシデント発生率にどのような影響を与えているのか、また、連絡体制などの対策が被害発生後の対応にどれだけ効果を発揮しているのかを、定量的にまたコスト的に把握するような質問項目を検討していく必要があるだろう。

3. 情報セキュリティインシデント対策の標準モデルと対策費用

1 被害発生を抑止している情報セキュリティインシデント対策の状況

本年度の「情報セキュリティインシデントが発生した企業のグループ」と「被害にあわなかった企業のグループ」について、「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」項目のアンケート結果をもとに対策などの差異を把握するために分析を行った。

しかしながら、ファイアウォールやウイルスチェックソフトなどのセキュリティ対策システムの導入比率との相関関係は、残念ながら特に見出せなかった。

ただし、情報セキュリティインシデント被害を受けた後に、すぐにシステム的な対策を実施したことも考えられるため一概に無関係とは結論付けられない。

2 抑止モデルの情報セキュリティ関連予算の実際

本年度の調査で、情報セキュリティインシデントが「発生した企業」と「発生しなかった企業」を二つのグループに分けて、その中で「情報セキュリティ関連予算」について、アンケート回答のある企業のみを取り出し、傾向を分析したところ、インシデント被害の「発生した企業」と「発生しなかった企業」の各グループの従業員数とセキュリティ予算を合計して「一人あたりのセキュリティ予算」を比較すると、「被害にあわなかったグループ」の一人あたりの情報セキュリティ予算が15,991円に対し「被害にあったグループ」の予算は5,327円と3倍の差が出た。

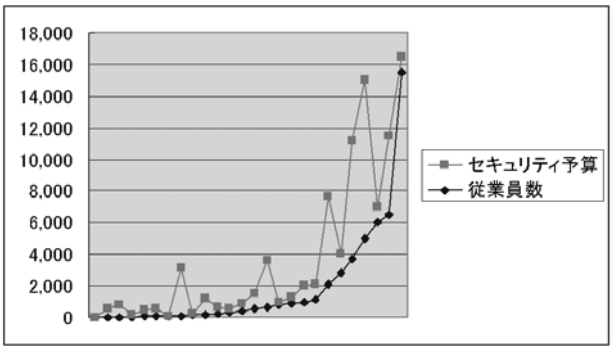
「情報セキュリティ予算」は、企業規模が大きくなれば一人あたりの金額は少ない傾向があり、情報セキュリティ予算の定義が明確ではない点を考慮すると、今回表れた「3倍の差」を単純に判断できないが、来年度以降の調査においても継続的に傾向を分析していきたい結果となった。

3 望まれる対策レベルと予算規模の提案

ハード面での対策はほぼ完了している企業も多かった。しかし、運用面を要因とする事故は多く、人的部分の教育までが、被害拡大を防止するための対策に含むべきとの結論となった。

対策レベル		具体例
対策レベル１	技術的対策	アンチウイルスソフト
		メール監視ソフト
		ファイアウォール
		IDS
		認証デバイス
対策レベル２	運用上対策	入退室管理
		セキュリティ管理責任者の任命
		情報セキュリティに関する規程作成
		セキュリティ事故対応マニュアル
対策レベル３（推奨レベル）	情報セキュリティ教育・啓発	コンピュータウィルス教育
		パスワード管理教育
		機密情報保護教育
対策レベル４	セキュリティ監査・第三者認証	ISMS ・ BS7799
		Ｐマーク

今回のアンケートでは、情報システム予算における情報セキュリティ関連予算の割合は、最大65%（従業員数140名）から最小0.1%（従業員数15,470名）まで多岐にわたり、平均で14.5%になった。



4. 2002年度情報セキュリティインシデント被害額算出モデルに関する検討

昨年度モデルをもとに、今年度の情報セキュリティインシデントに関する被害額の算出モデルを作成した。

昨年との変更点は、営業継続費用や喪失情報資産、機会損失などの追加や文言の修正を中心としており、詳細は報告書を参照願いたい。

また、これらの項目をアンケートの調査票としてまとめており、今後の被害調査時の記入表として活用いただければと考える。

D－1事故状況

1	被害コード→			
	＜事故状況＞			
2	発生日時	年　月　日（　：　）		
3	被害システムについて	事故時の対策について		
4	被害システムの種類について（該当システムの右欄に○をお付け下さい。）			
	(1) インターネット（DMZを含む）		(4) 社内専用ネットワーク	
	(2) イントラネット		(5) E C (B to B)	
	(3) エクストラネット		(6) E C (B to C)	
5	停止時間			時間
6	影響を受けた従業員の人数			人
7	システム停止時の業務処理量の低下割合			%
8	システムの年間売り上げ（EC関連の場合）			円
9	システムの年間収益（EC関連の場合）			円
10	被害を受けたサーバーの数			台
11	被害や影響を受けたクライアントの数			台
12	営業継続費（代替システム設置、人手の処理など）			円
	代替手段 ＜対応方法をご記入下さい＞			
13	逸失利益（システム売上×停止時間、確実な利益の逸失分等）			円
14	喪失した情報資産			円
15	機会損失（見込み利益で逸失分、売上増分の逸失など）			円
16	賠償・補償金額			円
17	その他関連出費（ブランド価値の維持費用について）			
	(1) お詫び広告			円
	(2) 謝罪出状			円
	(3) お詫び行脚			日人工
18	復旧作業量（システム部門他）			日人工
19	復旧費用（業者等への支払額）			円
20	貴社従業員の一日当たりの人件費			円／日

5. モデルおよび調査の今後の課題

1 モデルの課題

1.1 情報セキュリティインシデント被害額算出モデルの課題

モデルについては、昨年から課題となっている「IT感応度」については、今年度の見直しで十分な材料が無く、前回提案と特に大きな進歩を遂げることができなかった。今後は、企業毎に大きく異なるシステムの導入状況や業種などの情報で、ある程度数値化できる仕組みが本モデルの幅広い利用のために必要と考える。

また、対策の標準モデルについては、被害の有無を中心に考えたが、大きな差は無かった。しかし、事故の発生時期とアンケート時期のタイムラグにより、事故発生と対策の相関を掴むためには、対策の導入時期までも踏まえたものにする必要も考えられる。

2 調査の課題

2.1 アンケートの課題

今回の調査では、昨年の冗長なアンケート項目を見直し、十分な議論を重ねてポイントを絞ったアンケートの作成を行った。

しかしながら、今年のアンケートにおいても、記入のし易さなどの課題は残っている。

2.2 ヒアリングの課題

今回のヒアリング調査先も全般的に協力的であった。しかしながら、ヒアリング作業には人手が必要であり、件数増加を行う場合には、大きな課題となる。

6. 情報漏洩による損害賠償被害額の想定（以降、第2部について記述）

2002年は、個人情報保護法案と住民基本台帳ネットワーク(住基ネット)の運用開始に代表されるように、個人情報漏洩に注目された年(注：報告書の執筆時点では、個人情報保護法案は成立前だった)である。そこで本章では、不正アクセス等による情報漏洩事件について調査を実施し、そのインシデント内容を分析した。本分析結果を元に、個人情報の価値およびその情報の漏洩による賠償金額等について、いくつかの仮定のもとに被害額を算出した。

1 国内の情報漏洩

2002年1月から12月の間に発生した、ネットワーク経由での不正アクセス等による情報漏洩事件は、当ワーキンググループの調査結果によると、インターネット上で公に報道されたものだけでも計63件にものぼり、被害者の合計人数は、41万8,716人（1件平均 6,646人）であった。そのほとんどが、個人情報（メールアドレスのみの場合も含む）の漏洩である。

1.1 漏洩情報の分析

表1に情報漏洩事件の漏洩情報を分析した結果を示す。出現確率は、それぞれの漏洩情報の項目が、各調査対象の情報漏洩事件に含まれていた割合を示す。「氏名」は、情報漏洩事件うちの86％に含まれており、最も流出する可能性が高い情報である。さらに「氏名」、「住所」、「メールアドレス」、「電話番号」までの上位4つの情報が、他の情報に比べて高い確率で漏洩している。これは、これらの情報がホームページ上のアンケート、会員情報の記入などにおいて、ひとまとめの情報として頻繁に収集されているためと考えられる。

表1において、出現頻度が少ないため「その他」に分類した情報は、スリーサイズ、顔写真、趣味、年収、学歴、企業名、部署名、クレジットカード番号、プリペイドカード番号など、より個人の私的な情報が含まれている。これら情報は、漏洩する確率が高い上位4種類の情報よりも、より個人的な情報を含んでおり、情報漏洩による被害が大きく、深刻である。

表1：情報種別毎の漏洩件数と出現確率

漏洩情報名称	件数 (出現確率)
氏名	54件 (86%)
住所	38件 (60%)
メールアドレス	29件 (46%)
電話番号	28件 (44%)
生年月日	10件 (16%)
職業	6件 (10%)
性別	5件 (8%)
ユーザID	4件 (6%)
パスワード	2件 (3%)
アンケート関連	11件 (17%)
その他	21件 (33%)

2 情報漏洩元の分析

情報漏洩元の組織は、企業が約8割を占める。これは、企業が公共機関や教育機関に比べて、インターネットを利用したメーリングリストやアンケート募集、顧客への付加サービスを活発に行っているからであり、想定された結果である。今後は、e-Japan計画に代表されるように、政府、自治体がインターネット上におけるサービス提供を進めるため、情報漏洩事件に占める公共機関の割合が増加することが懸念される。図2に示す情報漏洩原因のうち、「設定ミス」、「誤操作」、「管理ミス」といった人為的なミスに由来した原因は、あわせて67％である。情報漏洩原因の「バグ・セキュリティホール」「不正アクセス」は、人為的なミスに直接関係していないが、最新のパッチを適用したり、Webシステムをより強固な構造へ変更したりすることにより、回避可能であったと思われる。つまり、人的要因に対する対処不足によって発生

した情報漏洩は、前述の2つの原因らを合わせて、全体の88%にもおよぶ。

情報の漏洩経路は、Web経由が84%、Email経由が13%であり、この2つで漏洩経路の大半を占める。どちらも、現在のインターネットの利用において、最も普及し、利用されているサービスである。

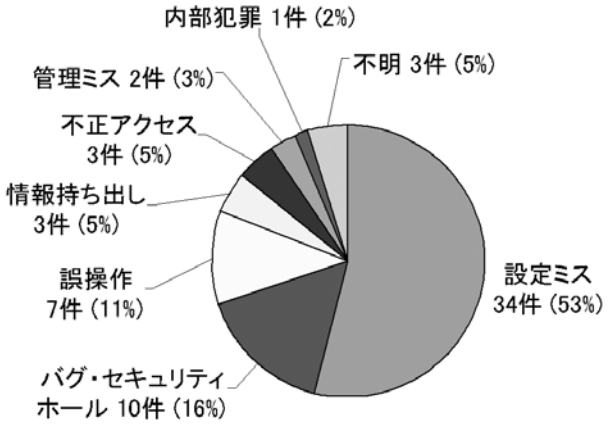


図2：情報漏洩原因

2.1 情報漏洩の原因

「Web経由」「Email経由」「FTP経由」が代表的な情報漏洩経路である。その中でも「設定ミス」が原因となって「Web経由」において情報漏洩に至るケースがもっとも多い。事件発生時の情報から、このWeb経由による情報漏洩の原因は、以下のような「設定ミス」、「バグ・セキュリティホール」とその他要因が、重なったことによって発生したと考えられる。

- web serverの設定ミス。ディレクトリ・リスト表示の許可設定ミスなど。
- ファイルパーミッションの設定ミス
- cgi等プログラムの設計ミス
- 推測しやすいファイル/ディレクトリ名の利用

（これらの複合要因の場合が多い）

Web(HTTP)は、CG/SSI、JavaScript/PHP、JPS/ASPなど双方向性サービスの手段として発達した。Webは、システム構築が容易で、便利なインタラクティブ・サービスを提供できる反面、システムの複雑化によりセキュリティホールを含みやすい。その結果、不正アクセスや設定ミスなどによる情報漏洩に結びつきやすいと想定される。

3 情報の種類と賠償額

3.1 宇治市住民基本台帳データ大量漏洩事件

漏洩した情報の価値をもとに、情報漏洩事件に対する賠償額が算出できると考える。そこで、宇治市住民基本台帳データ大量漏洩事件の控訴審判決より、漏洩した情報と損害賠償額との関係を参考とした。

表2：宇治市情報漏洩件数

情報名	漏洩件数
住民記録	18万5800件
外国人登録関係	3297件
法人関係	2万8520件
合計	21万7617件

・賠償額

被害者（住民）らに対し、慰謝料として1人当たり1万円、弁護士費用は、被害者（住民）1人当たり5000円。よって、1人当たりの賠償額は、1万5000円。

参考文献：http://www.law.co.jp/cases/uji2.htm

宇治市住民基本台帳データ大量漏洩事件で漏洩した個人情報は、「氏名」、「住所」、「性別」、「生年月日」の一般的な個人情報に加え、「世帯主名」、「世帯主との続柄」といったプライバシー度の高い情報が含まれていたという特徴がある。これに加えて、個人情報の情報源は、宇治市(自治体)の管理する住民基本台帳であることから、情報として最も信頼性・正確性が高い。上記の内容と、事件発生後にデータ回収、市民に対する説明、防止策の実施などの真摯的な対応姿勢が見られたことなどを考慮した結果から、慰謝料として被害者(住民)1人当たり1万5000円が言い渡された。もし、情報漏洩件数の約22万件より約22万人が訴訟をおこした場合、損害賠償額の合計は、約33億円となる。

式1：宇治市裁判における損害賠償額

15,000円×217,617件=32億6,425万5,000円

3.2 情報漏洩事件における損害賠償額の算出式

個人情報漏洩事件における損害賠償の実例はまだ少なく、賠償金額の基準が明らかになるには、今後発生する訴訟判決の事例の積み重ねが必要である。しかしながら、多発している情報漏洩事故を考えると、賠償金額に対する何らかの指標や想定モデルが必要と考えられる。本ワーキンググループでは、前述の判例や弁護士先生の意見

などを考慮し、あくまでも今後の議論の題材とするため、式2の算出式を設定した。
算定対象の情報漏洩事件について、式2の各項目に当てはまるポイントを表3から選択し、評価ポイントを算出する。表4の対応表を用いて、評価ポイントから漏洩情報1件当たりのおおよその損害賠償額を算定する。

式2：情報漏洩元組織の損害賠償額の算出式

情報漏洩元組織の損害賠償額 (評価ポイント)
= 漏洩情報の内容に基づく慰謝料 →表3:①の和
× 個人情報提供の同意の有無 →表3:②から選択
× 情報提供者との関係 →表3:③から選択
× 情報漏洩元組織の社会的信頼度 →表3:④から選択
× 事件後の対応姿勢 →表3:⑤から選択

表3：評価ポイント表

算式項目	状況別ポイント
①被害者に対する慰謝料(複数選択可)	基本的な個人情報 = 100
	特徴的な個人情報(3種類以下) = 500
	特徴的な個人情報(それ以上) = 1000
	メールアドレスのみ = 10
	個人を特定するID,パスワード関係 = 300
②個人情報提供の同意の有無	同意有り = 2.0
	同意無し = 1.0
③情報提供者との関係	顧客 = 2.0
	アンケート、プレゼント応募者 = 1.0
④情報漏洩元組織の社会的信頼度	一般より高い = 1.5
	一般的 = 1.0
⑤事件後の対応姿勢	良い = 1.0
	普通 = 2.0
	悪い = 4.0

表4：評価ポイントと想定慰謝料の対応表

1件当たりの評価ポイント	想定慰謝料
1000ポイント未満	0～5,000円
1000～2000ポイント未満	～10,000円
2000～5000ポイント未満	～50,000円
5000ポイント以上	50,000円以上

4 情報漏洩による損害賠償被害額想定

2002年の情報漏洩事件一覧および算出式(式2)を用いて算出した損害賠償額を表5、表6(次ページ)に示す。

2002年の国内におけるインターネット上の情報漏洩による損害賠償額は、推定の結果、以下のようになった。

表5：2002年 情報漏洩 総損害賠償額(推定)

総損害賠償額(推定)：
151億4,270万円(418,716人)

1件当たりの平均損害賠償額(推定)：
2億4,036万円(1件平均：6,646人)

図6に算出式(式2)で求めた2002年情報漏洩事件の評価ポイントの分布を示す。情報漏洩事件全体に対して、漏洩情報が基本的な個人情報やメールアドレスのみの情報漏洩事件が多いため、1件当たりの想定慰謝料が5000円以下(評価ポイントが1000ポイント未満)の漏洩事件が、全体の約70%を占めた。宇治市裁判例の損害賠償額(3600ポイント相当)以上にあてはまる情報漏洩事件は、10件(16%)であった。いずれも特徴的な個人情報が漏洩した事件であった。

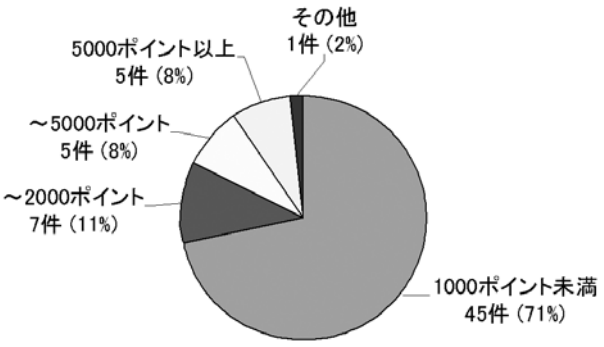


図6：情報漏洩事件の評価ポイント分布

情報漏洩の被害者全員が、損害賠償訴訟を起こすとは限らないが、損害賠償金額および、情報漏洩事件によるブランドイメージの低下等による売上への影響などを含めれば、情報漏洩による損害は、コンピュータウィルス等によるインシデント被害同様、その損害額は大きい。個人情報を収集・管理している場合は、情報漏洩によるリスクを平均損害賠償額(表5)ではなく、収集・管理している情報の内容と件数から算出式(式2)を用いて推定可能である。よって、アンケートや顧客サービスを実施するにあたり、その情報内容と件数から、情報漏洩リスクとして損害賠償額を算定し、セキュリティ投資額の参考とすることが可能である。

表6：2002年 情報漏洩事件一覧

企業・団体 No.	区分	漏洩情報 基本情報	特徴情報	メールアドレス	パスワード	評価ポイント	想定慰謝料	被害人数（人）	想定損害賠償総額（万円）
A	企業			○		200	5,000	1,900	950
B	企業	○				200	5,000	10,000	5,000
C	企業	○				600	5,000	1,388	694
D	企業	○				400	5,000	2,972	1,486
E	企業	○			○	800	5,000	68,471	34,236
F	企業	○				1,200	10,000	900	900
G	企業	○				400	5,000	22	11
H	企業	○				800	5,000	370	185
I	企業			○		100	5,000	1,462	731
J	企業			○		200	5,000	不明	不明
K	企業	○				1,200	10,000	4,300	4,300
L	企業	○				600	5,000	730	365
M	企業	○				200	5,000	4,000	2,000
N	企業	○				800	5,000	4,000	2,000
O	企業	○				400	5,000	10,000	5,000
P	企業	○				400	5,000	368	184
Q	企業	○				800	5,000	60	30
R	企業	○				400	5,000	1,303	652
S	企業	○			○	1,600	10,000	不明	不明
T	企業	○				600	5,000	800	400
U	企業	○				400	5,000	350	175
V	企業	○				400	5,000	1,000	500
W	教育機関	○				400	5,000	1,800	900
X	企業	○	◎			4,400	50,000	37,000	185,000
Y	企業	○				400	5,000	45,000	22,500
Z	企業	○				200	5,000	1,500	750
AA	企業	○				800	5,000	340	170
AB	企業	○				400	5,000	4,700	2,350
AC	その他	○				400	5,000	14,000	7,000
AD	企業	○				400	5,000	242	121
AE	企業	○				800	5,000	2,000	1,000
AF	企業	○				800	5,000	700	350
AG	企業	○				400	5,000	280	140
AH	公共機関	○				1,200	10,000	6,541	6,541
AI	企業	○				400	5,000	不明	不明
AJ	企業	○				400	5,000	1,100	550
AK	企業	○				800	5,000	5,000	2,500
AL	企業	○				1,600	10,000	1,600	1,600
AM	企業	○				400	5,000	1,200	600
AN	企業	○				400	5,000	2,093	1,047
AO	企業	○				400	5,000	不明	不明
AP	企業	○	◎			8,800	100,000	100,000	1,000,000
AQ	企業	○				1,600	10,000	不明	不明
AR	企業					算出不能	5,000	不明	不明
AS	企業	○				800	5,000	1,700	850
AT	教育機関	○	○			4,800	50,000	304	1,520
AU	企業	○	○		○	7,200	100,000	17,000	170,000
AV	公共機関			○		600	5,000	350	175
AW	企業	○				400	5,000	398	199
AX	企業	○				400	5,000	3,244	1,622
AY	企業	○			○	6,400	100,000	235	2,350
AZ	企業	○				200	5,000	1,200	600
BA	企業	○				400	5,000	50,000	25,000
BB	企業	○	○			2,400	50,000	400	2,000
BC	企業	○				400	5,000	335	168
BD	公共機関			○		600	5,000	59	30
BE	その他	○	○		○	7,200	100,000	不明	不明
BF	公共機関	○				1,200	10,000	483	483
BG	企業	○	○			7,200	100,000	65	650
BH	公共機関	○				600	5,000	154	77
BI	公共機関	○				600	5,000	190	95
BJ	教育機関	○	○			4,800	50,000	3,107	15,535
BK	企業				○	4,800	50,000	不明	不明
合計	63						合計	418,716	1,514,270
							平均	6,646	24,036

7. 情報漏洩事故による企業価値への影響(株価面での考察)

企業は、広報活動やＩＲ活動を行い企業価値の創造を行っている。これに対し、情報漏洩事故の発生は、信頼感の失墜および企業価値の低下を招く事故の一つと考えられる。

しかしながら、企業価値の指標が数多くあるのと同様に、情報漏洩などの不祥事によって、「どれくらい企業価値が低下したか？」を把握することは非常に難しい。

この点について、情報漏洩による企業価値低下の一端を垣間見るため、情報漏洩の事故発生と当該企業の株価の動きについて、どの様な関係があるのかを調査した。

1 情報漏洩事故発生後の株価変動の把握方法について

情報漏洩事故が発生した株式上場企業(もしくは密接な関連上場企業)について、事故発生後の短期及び中期における株価の動きを検討した。

株価の動きは、株式相場全体との連動性もあり、単純に金額を比較せず、株式相場全体＝日経平均とし、「事故発生の前日(前月末)」における「日経平均値と当該企業株価」との割合を基準とし、「事故発生後の日経平均と値と当該企業株価」割合の変化について、＜短期＞と＜中期＞に分けて調査した。

2 実例による株価変動の調査

2.1 短期影響額

企業毎に影響の有無や大小があるものの、「全社集計」においては、わずか8社の合計額で約150億円を示している。そして、企業によっては、1社のみで100億を超える数値も見られる。

8社の短期影響額の合計＝150億円

2.2 中期影響額

短期と比較し、より大きな影響が出ている。企業毎に影響の有無や大小があるものの、「全社集計」においては、わずか8社の合計額で約220億円を示している。そして、企業によっては、1社のみで250億を超える数値も見られる。

8社の中期影響額の合計＝220億円

3 企業における情報漏洩事故の株価への影響想定とその利用

企業経営者のリスク管理の一つとして、情報漏洩事故を想定し、自社株価への影響を考える場合への利用が考えられる。具体的には、下記の様な算式による影響額の試算が考えられる。

① 各社の「前日株価に対する差額割合」である「0～9％程度」数値の利用の場合

影響額＝自社株価×（0～9％）×発行株数

② 全社集計の「一株当たり差額」である「6～9円程度」の利用の場合

影響額＝6～9円×発行株数

これらの数値や算式を用い、情報漏洩事故の株価への影響額を事前想定することは、経営者における予防的なリスク管理として重要と考える。

今回の結果による影響の大きさを考えると、「情報セキュリティ対策費用」を単なる「システムコスト」ではなく、「企業価値の低下を防ぐためのＩＲ費用の一つ」として、積極的に捉え直すことも必要である。

4 算出基準値の課題

今回は、算出の基準値として「日経平均」を利用したが、株価の動きには業種毎のトレンドがあり、「日経平均」と「業種平均」が乖離する事は日常的に起こっている。

企業経営者の立場としては、同業他社との優劣も重要であり、今後は影響の把握をより精緻にするため、算出の基準値に「業種平均」を取り入れることも検討すべきである。

8. 最後に

今回2部構成で報告書を作成した。第2部においては、今後の各方面での議論の題材とするため、公表された情報漏洩事故について検討を加え、賠償による被害額の想定や企業価値の一端を示す株価への影響について、本ワーキンググループとして数値を示した。これは、メンバー内での討議・検討の結果であり、法律問題など我々の専門分野以外の要素が多く、現時点ではトライアル的な数値であることは否めない。

しかしながら、これらの被害の数値算出および算出課程を明示したことで、専門家を巻き込んだ今後の議論の題材を示すことができた。

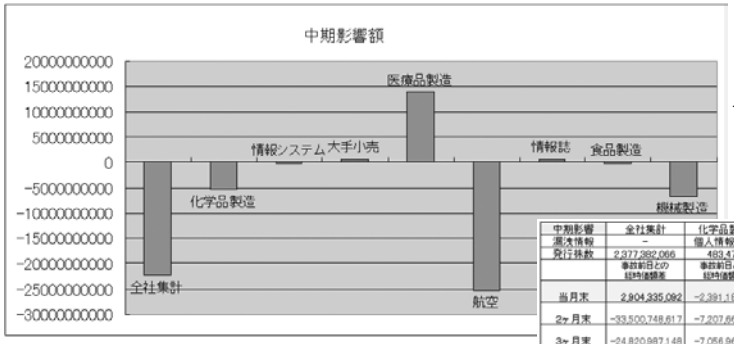
各異分野の専門家における共通の話題として取り上げられ、情報システムのリスクアセスメントで必要な「リスク量の把握」における把握モデルの構築が前進し、安全な情報化社会の形成に役立つことを期待したい。

報告掲載URL

http://www.jnsa.org/active1a.html

9. 2003年度の活動

誰もが興味のある被害について調査を行っているが、これらの事故情報収集は、容易ではない。しかしながら、本ワーキンググループならではの自由な発想による被害算出を、アンケートやヒアリングと共に今年度も引き続き行っていく予定である。



←中期影響額のグラフ

↓影響状況一覧

中期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	－	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,085	21,076,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当月末	2,904,335,092	-2,391,186,437	385,046,116	228,968,428	35,552,585,519	-30,089,363,254	992,471,666	361,720,517	-2,135,907,464
2ヶ月末	-33,500,748,617	-7,207,661,195	34,112,062	733,372,351	17,875,262,835	-40,587,241,253	383,916,817	-46,604,046	-4,685,906,189
3ヶ月末	-24,820,887,148	-7,056,943,701	53,223,297	1,000,553,392	568,067,968	-5,931,163,173	148,204,325	-163,011,541	-13,439,897,715
4ヶ月末	-33,659,566,285	-4,798,506,294	-925,642,464	540,858,539	1,623,993,216	-24,069,485,182	1,025,077,127	-1,072,899,642	-6,082,961,582
4ヶ月間累積	-89,076,966,959	-21,454,317,627	-353,260,990	2,503,752,711	55,619,909,539	-100,677,252,861	2,549,669,936	-920,794,712	-26,344,672,954
1ヶ月当り	-22,269,241,740	-5,363,579,407	-88,315,247	625,938,178	13,904,977,385	-25,169,313,215	637,417,484	-230,198,678	-6,586,168,239
一株当り差額	-9.4	-11.1	-14.5	81.2	65.9	-16.4	11.1	-12.1	-116.5
前月株価に対する金額割合	－	-4.40%	-1.29%	9.44%	3.97%	-4.50%	5.40%	-1.66%	-14.26%

情報セキュリティ監査について

セキュリティ監査WG前リーダー
朝賀　康義

2002年9月経済産業省が、「情報セキュリティ監査研究会（以下、「研究会」という。）」が発足し、JNSA下村事務局長が委員として選任されました。JNSA政策部会では、研究会の各種実作業を行うためにセキュリティ監査WGを発足し、「情報セキュリティ管理基準」、「情報セキュリティ監査人スキルマップ」などを作成してまいりました。そして、本年度から「情報セキュリティ監査制度」の運用が始まり、特に初期においては地方自治体からのセキュリティ監査のニーズが多いことを想定し、「電子自治体のためのセキュリティ管理基準」を策定しています。なお、監査WGでは、この基準を使って実際に監査を受けていただける地方自治体を募集しています。
ここでは、情報セキュリティ監査制度とセキュリティ監査WGの活動についてご紹介いたします。

1. セキュリティ監査制度の必要性

情報システムを構成するハードウェアやソフトウェアの高度化や、ブロードバンドの普及、さらには電子政府／電子自治体の進展などもあいまって、情報システムは年々利便性が高いものになっています。一方、複雑化した情報システムにひそむ弱点をついたサイバー攻撃や、個人情報の漏えい、さらにはITを利用した詐欺事件などが多発しています。こうした状況において、企業、政府、自治体の情報セキュリティに関する関心は高まりつつあります。特に政府、自治体においては、今年度は総合行政ネットワーク（LGWAN）への接続や、8月からの住民基本台帳ネットワークの本格稼動があり、情報セキュリティに関する関心は否が応でも高まっています。また民間企業においても相次ぐ個人情報漏えい事件や個人情報保護法の成立を受け、急速に情報セキュリティへの関心が高まっています。

しかし、ウイルス対策ソフトやファイアウォールの導入など、個別的な対策はしているものの、人的・物理的・技術的なセキュリティを総合的に対策している組織体は多くはないようです。またポリシーをつくっていても、その運用状況をきちんと管理し、適切な情報セキュリティ管理をしている組織体は極めて少ないのが現状です。

表1　情報セキュリティ監査の実施状況

	実施している	実施していない	無回答
大企業(N=541)	20.0%	79.7%	0.4%
中小企業（N=951）	7.2%	91.7%	1.2%
地方公共団体（N=172）	4.7%	95.3%	0.0%
病院（N=109）	4.6%	95.4%	0.0%
大学（N=175）	9.1%	90.3%	0.6%
その他学術/研究機関 (N=70)	11.4%	88.6%	0.0%

（資料：総務省「情報セキュリティ対策の実施状況調査結果」）

情報セキュリティは、人的・物理的・技術的対策の最も脆弱な点から破れるものです。また攻撃の手法は日々高度化しています。したがって本来ならば、総合的な情報セキュリティ監査を定期的に実施／受ける必要があるはずですが、実際には、

・監査主体としては、「情報セキュリティ監査とは何か」という指針が無いため、監査の正当性を信じてもらえない
・被監査主体においては、どのような効果があるかわからない、誰に頼めばよいかわからない

といった課題があり、情報セキュリティ監査が普及していなかったようです。

そこで経済産業省情報セキュリティ監査研究会では、

①「情報セキュリティ監査」を考える上での基本的な視点を整理し
②「情報セキュリティ監査」の標準的な基準を策定し
③「情報セキュリティ監査」を行う主体のあり方を提示する

ことにしました。

加えて経済産業省では、この成果を受け、適正な「情

報セキュリティ監査」を受ける主体が増えることにより、日本全体の情報セキュリティのレベルが向上すること、また、「情報セキュリティ監査」の市場が適切に成長していくことを期待しています。

2. セキュリティ監査制度の概要

(1) 基本的な視点

①システムではなく情報資産を監査する

従来からある「システム監査」においてもセキュリティに関する視点はありましたが、あくまでも情報システムとしてのセキュリティの視点でした。現実世界では、システムの弱点だけでなく人の運用上の問題や悪意により情報セキュリティが破れることも多くなっています。そこで「情報セキュリティ監査」では、守るべきものは情報システムではなく情報資産であると考えています。

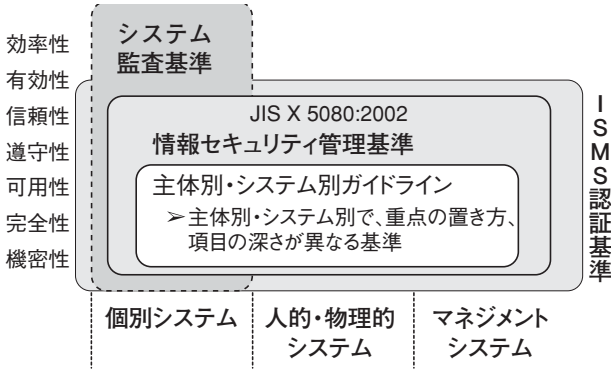
②セキュリティの強度ではなく情報資産に対するマネジメントを監査する

情報セキュリティを脅かすリスクは日々変化・高度化しています。ある時点におけるセキュリティ対策が明日も有効であるという保証はありません。そこで「情報セキュリティ監査」においては、ある時点における「情報セキュリティの強度」ではなく、その組織において情報資産に対するリスクのマネジメントが効果的に実施されているかどうかを監査すべきと考えています。

③マネジメントサイクルの視点

情報セキュリティリスクをマネジメントするには、情報資産に対するリスクアセスメント(評価)を行い、その評価を基に適切な管理策(コントロール)を割り当て、その管理策が適切に実施されているかどうか、そもそもリスクアセスメントが適切であったかどうかを評価する必要があります。情報セキュリティ監査では、このような評価を行い、情報セキュリティ対策を改善するのに役立つものになります。

図1　情報セキュリティ監査の対象



(2) 多種多様な監査ニーズに対応した監査制度

①保証型と助言型の選択制

監査には、監査結果を被監査主体の外部に対する“お墨付き”とする保証型監査と、改善課題を内部的に利用したり、責任の限界を外部に示すための改善提案型監査の二つがあります。

保証型監査では、監査人は、基準に照らして適合しているか否かについて意見を表明します。保証型監査の代表例は会計監査です。不適切な監査意見を表明したりすると賠償責任を問われたり資格を剥奪されるなどします。ただし(会計監査を含め)保証型監査といえども絶対の安全を保証するものではなく、監査人が見た範囲についての“合理的な保証”となっています。

改善提案型監査では、基準に対する適合性を○か×かで意見表明するのではなく、基準とのギャップを指摘したり、改善の方向性を示すことを目的としています。改善提案型の監査の代表例として、システム監査が挙げられます。

「情報セキュリティ監査」では、被監査主体のニーズにより、保証型監査でも改善提案型監査でも、どちらでも選択できるようにしています。これは、被監査主体としては、“お墨付き”を得たいというニーズがある一方、そのような第三者に対して保証を提供できる独立性や責任能力のある監査組織が少ないこと、またそもそも“お墨付き”が得られるほどの情報セキュリティ管理体制ができている組織が少ない現状において、“不適合意見”を得るために監査を受ける組織は無いであろうことから、「情報セキュリティ監査」を広めていくために、両方のタイプの

監査を選択できるようにしています。

②全部と一部の選択性

「情報セキュリティ監査」では、監査の対象範囲も自由に選択できます。もちろん、組織の全ての領域と全ての情報資産を対象とした方が望ましいのですが、対策ができた(あるいはできていない)部門から監査を受けるとか、ネットワークを使った外部からの攻撃への対策だけ先行して監査を受けるなど組織や情報資産の一部だけについて監査を受けることも可能とされています。

さらには、前述の保証型監査と改善提案型監査を組み合わせることもできるとされています。例えば、オフィスエリアの人的セキュリティについては改善提案型監査を受けて、ネットワークセキュリティについては保証型の監査を受けるといった混合型監査も認められています。

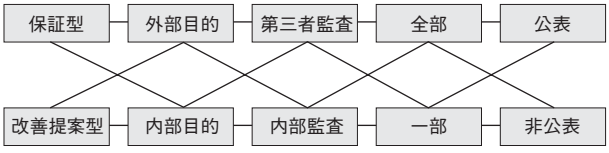
③多様な監査企業

「情報セキュリティ監査」には、経営、人的オペレーション、建築、ネットワークセキュリティ、法律など、幅広い領域の知識や経験が必要とされます。この全ての領域をひとりでカバーできているような人はもちろん、企業としても少ないのが現状です。「情報セキュリティ監査」を普及するためには、一握りの専門家や専門企業を監査主体として認めるのではなく、部分的でも一定の知識･経験を持つ主体を監査主体として取り込むことで、監査サービスの向上、被監査主体の満足が得られると考えられています。そこで、セキュリティソリューションベンダーのみならず、システム監査企業、監査法人、その他様々な業種の参入を認めています。

とはいえ、何の制限もない中では被監査主体が監査主体の選定に戸惑ったり、監査サービスの質の向上が期待できないことから、「情報セキュリティ監査企業台帳」に過去の実績などを公開することを最低条件とし、被監査主体が監査主体を選べるようにしています。

また今後、NPO日本セキュリティ監査協会(JASA、設立準備中)において、監査人として必要な資質や受けるべき研修などの基準を明らかにしていくことになるでしょう。

図2　情報セキュリティ監査は組み合わせ自由自在



3. 管理基準と監査基準

研究会では、半年間の活動の成果物として

①「情報セキュリティ管理基準」

②「情報セキュリティ監査基準」

を発表しました。

「情報セキュリティ管理基準」は、各組織が自らの情報セキュリティポリシー策定やセキュリティ対策を検討する際の拠り所であり、監査をする際のチェック項目ともなるものです。

また「情報セキュリティ監査基準」は、監査を行う際に監査主体が従うべき規範を定めたものです。

(1)「情報セキュリティ管理基準」

研究会では、「情報セキュリティ監査」制度におけるチェック項目である管理基準について、そのベースとして、JIS X 5080:2002を選びました。これは、

・情報システムではなく情報資産を対象とする

・リスクマネジメントの有効性を評価する

・国際的な整合性

の観点から、ISO/IEC 17799:2000をローカライズしたJIS X 5080:2002が最適と考えたためです。

情報セキュリティ管理基準は、JIS X 5080:2002をベースにしていますが、これをチェックリストとしてより使いやすくするために以下のような方法で体系化しています。

① 目的

② コントロール

「JIS X 5080:2002 の管理策(コントロール)」において、管理すべき内容が複数ある場合はそれを細分化する。

③ サブコントロール

「JIS X 5080:2002 の管理策(コントロール)のガイダンス」の内容を項目化し、内容に応じて上記のコントロールごとに振り分けする。

(2) 情報セキュリティ管理基準の使い方

情報セキュリティ管理基準を使って監査を実際に行う場合には、

・「コントロール」を判断尺度として使う

・組織の事業内容や規模により、「コントロール」を取捨

選択したり、追加したり、あるいはその業界の用語に読み替える

などの注意が必要です。

管理基準を見ると、一見「サブコントロール」がチェックすべき項目のように思えてしまいますが、そうではありません。「サブコントロール」は、統制目標である「コントロール」を達成するための手段の例示であり、その全てを実行することが求められているわけではありません。

また、取り扱っている情報資産の内容や業界特有の表現や規制にも配慮して運用することが必要です。例えば、個人情報取扱事業者においては、個人情報保護法に対応するために、管理基準で求められている以上の対策が必要な場合もあるでしょうし、自治体など行政機関では、“従業員”を“職員”に読み替えたり、“経営陣”をその組織の実態に合わせて読み替える必要があるでしょう。

【ISMS制度との関係】

情報セキュリティ監査制度の兄貴分にあたる制度として、「ISMS適合性評価制度」があります。情報セキュリティ管理基準がベースとするJIS X 5080は、元々は英国規格BS7799のベストプラクティス集であるpart1をベースにしているのに対し、ISMS適合性評価基準は、BS7799の認証基準であるpart2をベースにしています。したがって2つの基準は、個別システムではなく情報資産を組織としてトータルに保護するためのマネジメント体制を評価するという基本的な視点において整合性が取れています。制度として異なる点は、ISMS制度は認証するかしないか(マークを与えるか否か)の審査をするのに対し、情報セキュリティ監査制度は、前述のように「保証－改善提案」、「全部監査－一部監査」などを被監査主体が選択できるようにしている点です。

現時点においては、対外的なブランディングのためにはISMS制度、段階的な改善のためには情報セキュリティ監査制度を利用するなど、目的によって制度を使い分けることができるかもしれません。

4. JNSAセキュリティ監査WGの活動

【JNSAセキュリティ監査WGの活動】

JNSA政策部会では、情報セキュリティ監査研究会の発足を受けて、昨年9月にセキュリティ監査WGを発足しました。昨年度は、サブWGを2つつくり、監査基準サブWGでは、JIS X 5080ベースのセキュリティ管理基準の作成を支援し、セキュリティ監査人スキルマップ・サブWGでは、セキュリティ監査人に必要と考えられるスキルを洗い出しました。そして今年度は、電子自治体のためのセキュリティ管理基準モデルを策定し、パブリックコメントを募集いたしました。

セキュリティ管理基準は、経済産業省に正式に採用され、WEBでも公開されていますので、ここでは「セキュリティ監査人スキルマップ」と「電子自治体のセキュリティ管理基準(JNSA案)」をご紹介します。

(1) セキュリティ監査人スキルマップ

研究会の報告書でも指摘されている通り、監査人の質の確保が、「情報セキュリティ監査」制度が普及するかどうかを左右すると考えられます。そこでJNSA監査WGでは、セキュリティ監査人に要求されるスキル要件を洗い出すことにしました。この洗い出し作業には、ISMS認証取得コンサルティングの経験を持つコンサルタントを中心に、リスクアセスメントや内部監査など、ISMS構築の現場経験を踏まえて検討しました。

検討に当たっては、

- 日本情報処理開発協会　ISMS審査員研修コース基準2.2履修目標
- 日本情報処理開発協会　JITEC 情報処理技術者スキル標準～システム監査技術者

に示されるISMS審査員およびシステム監査技術者としてのスキル要件との比較をすることにより、情報セキュリティ監査人としてのスキル要件を浮彫りにしました。

またJNSA教育部会スキルマップWGの成果物「セキュリティ技術者スキルマップα.1版」も参考にしました。

この検討を通じて明らかになったのは、

- マネジメントシステム、技術的セキュリティ、人的セキュリティ、物理的セキュリティ、監査技術はそれぞれ独立した高度な知識である
- ISMS審査員およびシステム監査技術者のスキル要件では、技術的セキュリティ、人的セキュリティ、物理的セキュリティ、に関する要求が不十分である
- 特に技術的セキュリティについてのカバーが不十分である

ということでした。

特に、従来IT関連の監査の主流であった情報セキュリティ監査技術者の資格要件にセキュリティ技術に関する要件が少ないこと、またISMS審査員の研修基準においても（また実際の研修においても）セキュリティ技術に関する要件が少ないことから、今後「情報セキュリティ管理基準」を理解し、監査現場で技術的な確認をするには、追加の研修等が必要となることが予想されます。

ＷＧでは、こうした課題を解決するために「セキュリティ監査人スキルマップ案」とともに、以下の提言を経済産業省に提出しました。

- 独立した高度な知識を幅広く一人の人間が保有することは困難であるため、大組織に対する監査においては、複数の専門家による監査チームを編成することが望ましい
- 地方公共団体や中小企業など、監査予算規模が小さいが対象数が膨大な組織のために、必要要素を網羅した人材を育成する専門教育プログラムの開発が必要である
- 開発される専門教育プログラムは、カバーすべき範囲が広範であるため、受講者の既存資格や経験を考慮し、不足している領域のみを効率的に提供できるようにモジュール化することが望ましい

JNSA情報セキュリティ監査人SkillMAp α.1版
領域：技術的セキュリティ

情報セキュリティ監査人スキルマップ	
中分類	小分類
ファイアーウォール	ネットワークポリシー設計
	DMZ等構成の設計
	NAT (StaticNAT / DynamicNAT / IPマスカレード)
	ファイアーウォールのルーティング
	アクセスコントロール技術（PacketFilterling / Circuit Level Gateway / Application Level Gateway）
	ファイアーウォールの基礎的役割
侵入検知システム	IDS負荷分散
	HoneyPot
	IDSの弱点（FalsePositive ・ FalseNegative ・ 暗号環境での未検出 ・ Stick攻撃 ・ 取りこぼし）
	管理者への通知方法
	防御機能（TCPリセット/ルータ・ファイアウォールでの遮断）
	検知アルゴニズム（不正検出・異常検出）
	侵入検知システムの分類（NetworkIDS/Host IDS/ハイブリッドIDS）
	侵入検知システムの基礎的役割（ファイアウォール防御技術との違い）
ウィルス対策	防御システムの構築(ウイルスからの防御システム構造)
	対応ポリシー（感染時）
	設定ポリシー
	ウィルス対策個所の設計
	スキャン方式と検出方法
	感染媒体の種類と感染方法
	ウィルスの分類および定義の理解
	定義ファイルのアップデート
OSセキュリティ	アカウントの管理（ユーザ、パスワード）
	アクセス権の管理（ネットワーク、ディレクトリ・ファイル）
	ファイルシステム
	耐タンパー

情報セキュリティ監査人スキルマップ	
中分類	小分類
ネットワーク技術	ルーティング制御
	プロトコル制御
	アクセスコントール制御
	端末認証
	暗号化方式（SSL、IPSecなど）
	NAT
	運用管理（ログ、ＳＮＭＰ、設定ツール）
	無線ＬＡＮ
	ネットワーク基本知識
	ネットワーク設計技術(セキュア)
暗号	暗号アルゴリズム
	共通鍵暗号方式
	公開鍵暗号方式
	ハイブリッド方式
	暗号アルゴリズムの種類(ブロック暗号、ストリーム暗号)
署名	メッセージダイジェスト
	デジタル署名の仕組み
	デジタル署名の利点
認証	ワンタイムパスワード
	認証トークン(ICカード等)
	バイオメトリクス
	チャレンジ&レスポンス
	ID ・パスワード
攻撃手法	TCPスキャン
	UDP スキャン
	その他偵察行為
	Sniffing,盗聴行為
	パスワードクラック
	DoS攻撃
	DDoS攻撃
	バッファオーバーフロー
	Format String Bug
	トロイの木馬

Trusted OS	工事中
PKI(認証局の構築と運用)	認証局の運用形態
	認証局の構築
	秘密鍵管理(HSMN、アクセラレータ)
	認証局運用規程(CPS)
	証明書ポリシー(CP)
(PKIの定義)	認証機関
	証明書リポジトリ
	証明書失効
	鍵のバックアップと回復
	自動鍵更新
	鍵履歴
	相互認証
	否認防止のサポート
	タイムスタンプ
(PKIが提供するサービス)	認証
	データの完全性(否認防止)
	データの秘匿性
サーバーセキュリティ (Web)	一般的なWebシステム構成
	基本認証
	PAM認証
	SSL
	http通信・webサーバ・ブラウザの基本機能
	HTTP通信で利用される言語(html/XML)
	Webサーバの設定により脆弱になってしまう個所
	Webサーバ上でのファイルのパーミッション(wrxの付け方、umask
	サーバプログラム実行権限
	Chroot
	クライアントアプリケーション(プラグイン、ヘルパー、ActiveX)
	ログ管理
	ロジック爆弾
	メール爆弾
	Spyware
	バックドア
	不正アクセスの隠蔽(ログ改ざん等)
	古典的不正アクセス技法(サラミ)
	クロスサイトスクリプティング
	最新不正アクセス手法
	情報収集
	偵察行為
	攻撃後処理
その他	最新の攻撃手法・脆弱性情報の入手方法に関する知識

(参考) システム監査人コア知識・スキル	
中分類	小分類
情報技術一般	ソフトウェアに関する知識
	ハードウェアに関する知識
	ネットワークに関する知識
	コンピュータ設備に関する知識
情報技術の動向	Web技術(インターネット、イントラネット、エクストラネット)
	認証局(CA)、認証技術(PKIなど)
	暗号
	VPN(バーチャルプライベートネットワーク)

(2) 電子自治体のセキュリティ管理基準(JNSA案)

監査WGでは、「情報セキュリティ監査制度」に対応した地方自治体向けのセキュリティ監査における監査項目(セキュリティ管理基準モデル)を作成いたしました。

情報セキュリティ監査制度では、情報セキュリティ管理基準をもとに、被監査組織・業界ごとに実態に合った項目・表現に修正した管理基準を作成し、運用することを求めています。そこでJNSA監査WGでは、まず初めに電子自治体の推進、特に住基ネットの本格稼動を控え、情報セキュリティ対策の確立を強く求められている地方自治体向けの管理基準モデルを作成し、提案することにいたしました。

作業にあたっては、以下の自治体向けの情報セキュリティ関連のガイドラインを参考にしました。

A：地方公共団体における情報セキュリティ対策に関する調査研究報告書(H14.2)
http://www.soumu.go.jp/singi/security.pdf

B：情報セキュリティティポリシーに関するガイドライン(H14.11.28一部改定)
http://www.bits.go.jp/sisaku/2002_1128/ISP_Guideline_20021128.html

C：住民基本台帳ネットワークシステム及びそれに接続される既設ネットワークに関する調査表
http://www.soumu.go.jp/c-gyousei/daityo/021107_1.html

監査WGでは、これらのガイドラインを参考にしつつ、

検討メンバーの現場経験を通じた自治体の現状や個人情報に関する機密性の要求度合いを考慮して、管理基準について下記のようにチェックしました。

●判定基準の定義

記号	ガイドラインなどで求めている	JNSAとして必要と考えるか
○	求めている	必要
□	求めていない	必要
△	求めている	不要
×	求めていない	不要

目的	コントロール		サブコントロール	管理基準	JNSA提案
7.3 利用者の責任					
認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	○	11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言すること	7.3.1.11	□
	2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	○	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスから特別な保護をすること	7.3.2.1	□
			2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	7.3.2.2	□
			3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること	7.3.2.3	×
			4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	7.3.2.4	×
			5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	7.3.2.5	□
7.4　ネットワークのアクセス制御					
ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	○	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	7.4.1.1	○
			2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	7.4.1.2	○
			3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	7.4.1.3	□
			4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	7.4.1.4	□
			5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	7.4.1.5	□
ネットワークを介したサービスの保護のため	2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること	○	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	7.4.2.1	○
			2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	7.4.2.2	△
			3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	7.4.2.3	○

情報セキュリティ監査について

今回作成した電子自治体情報セキュリティ管理基準（JNSA案）は、情報セキュリティ管理基準の中で電子自治体において必要と考えられる監査項目の抽出のみをしており、管理基準の詳細項目（サブコントロール）の表現を自治体向けの表現に置き換えるなどはしておりません。従いまして、本管理基準案をご覧いただくにあたり、従業員_職員、経営陣_首長／幹部などと読み替えていただく必要があります。

今後に残された課題としては、

・自治体向けの表現に置き換える（特に個人情報の保護を重視した表現への置き換えや、コントロールの追加を検討する）
・インタビューや資料の確認だけでなく、技術的なチェックを加えるべき項目を洗い出す

さらには、

・実際に自治体の監査で使ってみる

等が必要と考えています。

特に、自治体の監査における試行を通じて、基準の読み替えや技術的チェック項目や方法の標準パターンを作っていくことが重要と考えます。

現在、JNSAのホームページにて、この「電子自治体情報セキュリティ管理基準（JNSA案）VER.0.8」についてパブリックコメントを募集し、また実際に本管理基準での監査にご協力いただける自治体を募集しています。ご協力いただける自治体の方、自治体をご紹介いただける方は、是非JNSA事務局までご連絡ください。

【参考サイト】

経済産業省　情報セキュリティ政策、署名認証のページ
http://www.meti.go.jp/policy/netsecurity/index.html
経済産業省　「情報セキュリティ監査企業台帳」申告についてのおしらせ
http://www.meti.go.jp/policy/netsecurity/audit_register.start.html
JNSAスキルマップWG「情報セキュリティプロフェッショナル育成に関する調査研究」
http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html
JNSA監査WG　電子自治体情報セキュリティ管理基準（JNSA案）VER.0.8
http://www.jnsa.org/active7_030715.html

JNSAワーキンググループ紹介

電子署名検討ワーキンググループ

NTTコムウェア株式会社
電子署名検討WG　リーダー
磐城　洋介

電子署名検討ＷＧは、「e-Japan」構想による電子政府の構築にともない注目を集めつつある「電子署名」をキーワードに各種課題の検討を行います。健全な電子社会に貢献をするため官民問わず電子署名利用の阻害となっている技術・法律上の問題を調査報告し、利用者に対する啓発となる適正な利用モデルをガイドラインとしてまとめるために結成しました。

■ 電子署名の課題

このWGで検討するのは電子署名法で規定されたセキュリティ機能を有する「電子署名」を対象とします。「電子署名」は技術的な方式を規定する用語ではありませんが、本WGでは特定認証業務で定められたＰＫＩ（公開鍵基盤）による「デジタル署名」にターゲットを当てて下記の観点で課題を抽出していきます。

・ 技術的に未解決な課題
・ 運用・運営に関する課題
・ 法律・社会規範に関する課題
・ 導入コストなど経済的な課題

■ WGの方向性

電子署名の利用は欧州で活発に検討されており、EESSI（イージー）と呼ばれる欧州各国の政府機関により結成された標準化団体においては、利用時の問題・課題をクリアするためのフレームワーク（技術検討の結果を受けた利用モデルおよびそれと連携した法律などのガイドライン）の整理が進んでいます（図1）。

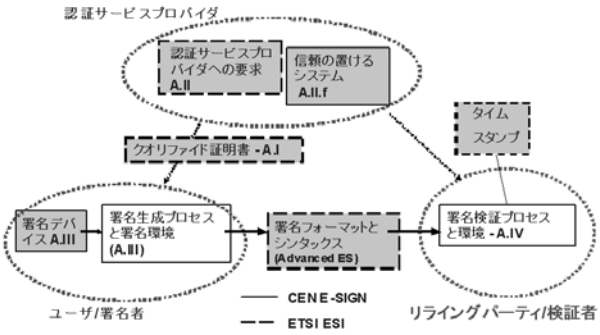


図1．EESSIの認証フレームワーク

本ＷＧにおいては、これら動向を踏まえ日本国内の認証フレームワークをターゲットとして、各種ガイドラインの策定に有用な情報の収集や技術検証を行っていく予定です。

■ 今後の活動

本ＷＧには電子政府で利用される認証基盤（GPKI）や、それと連携するシステムを開発した経験を持つエンジニアがメンバーにいるため、電子政府構想に対して実装面における様々な課題・難題に直面した際の意見（生の声！）が活発に飛び交っています。本ＷＧの当面の活動は、電子署名に関する様々な課題を整理するために、現状把握と前項に挙げた課題の詳細化を行い、広く世間に対して電子署名の技術・方式への理解を深めるための働きかけを行います。

検討の具体的な一例を挙げると、とかく電子署名と比較されがちな「印鑑」との違いなどを例に取り、実社会における信頼モデルや印鑑などの利用の実態と合わせて現状の把握を行います。（図2）また技術的な課題の詳細化

活動の一環として、JNSAによる実験CAを立ち上げ本WGのメンバーやJNSAの希望者会員を対象に証明書の発行を行い、電子署名AP（Outlook　Expressを用いたS／MIMEなど）の利用を通じて技術的な側面での課題の明確化や実際に利用する際に生じる問題について検討していきます。

これら検討結果を受けて、モデルとして選んだ業界における電子契約や調達などのシステムにおける電子署名セキュリティのガイドラインを検討する予定です。

■ おわりに

今年度中には公的個人認証基盤による電子証明書の発行を受けられるようになり本格的に電子証明書の利用が始まる計画になっています。理論から利用の段階に入ったPKIにはまだまだ未解決な問題と様々な解決手段があることを明らかにすることで、利用者である国民が安全にシステムを利用できるための手助けをすることと、利用者のPKIに対する不安を取り除くことができれば良いかと考えています。

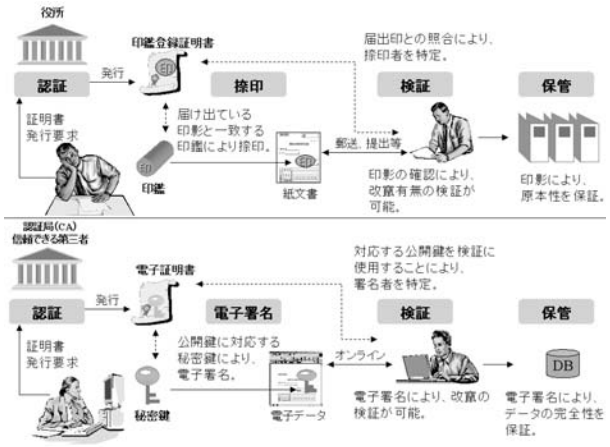


図2．印鑑利用と電子署名利用の類似点

JNSAワーキンググループ紹介

セキュリティ啓発ワーキンググループ

マイクロソフト株式会社
セキュリティ啓発WGリーダー
古川　勝也

セキュリティ啓発WGは、昨年のCD-ROM作成WG の活動をさらに強化した形で、今年の４月より活動を開始しました。全国各地でセキュリティ関連の啓発活動を実施し、JNSAの全国的な認知度の向上とセキュリティに対する理解の向上を目的として活動を予定しており、本年度は、経済産業省の委託により「インターネット安全教室」と題したセミナーを全国10ヶ所で開催いたします。今回の対象は、一般の家庭を対象としており、インターネット利用時のメリットとセキュリティ面での留意点を題材にしています。これらの活用を通じて安全なインターネットの利用が促進されることを切に願っています。

■セキュリティ啓発WGについて

全国の家庭に急速にブロードバンド環境が浸透し常時接続環境や家庭内での無線LAN環境が一般的になりつつある今日、ウイルス感染や詐欺行為、プライバシー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。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、情報犯罪を防ぐことはできません。こうした状況をふまえ、セキュリティ啓発WGでは、家庭や学校からインターネットにアクセスする人々を対象に、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を開催することにいたしました。この「インターネット安全教室」は、経済産業省の委託により実施するもので、各地の学校・自治体・団体・新聞社・商工会議所などの協力を得て、2003年10月～11月にかけて、全国10カ所で開催する予定です。

■「インターネット安全教室」参加対象者の検討と全体像について

「インターネット安全教室」では、今回のセミナーの対象を、「家庭や学校でパソコンを使う人」としました。生徒や教職員の方々、老若男女を問わず幅広いインターネットの利用者が対象となります。

インターネットを利用した情報の収集や、ショッピング、オークション、チャットといったコミュニケーションを、ネットワークインフラやテクノロジの進化により、非常に快適に行える環境が一般の家庭においても利用することができるようになりました。その反面、インターネット上のセキュリティ問題に対しての理解や、対策についてはまだまだ認知されていない現状があります。

そこで、今回は全国でのセミナーを展開し、インターネットを利用する上での最低限のセキュリティ対策の認知を高めることにいたしました。

全体のトーンとしては、非IT関連の方々も対象としているので、簡単な表現を行うこと、映像や画像を利用して直感的にイメージさせることを配慮して作製することにしました。そこで、実際のWGメンバーの体験や、周囲の動向を踏まえた、身近に発生しうる内容を具体的な例としてとりあげることにしました。また、メッセージの１つとして、インターネットの危険性だけではなく、インターネットの利便性についても強調しています。インターネットを利用することにより、生活が豊かに楽しくなる

というメリットについても等しく認知してもらうことが目的だからです。また、より理解度を高めるために、前回職場向けに作成したものと同様に、15分程度の映像を家庭向けに作成し教材として利用する予定で、副教材として参加者にCD-ROMの形式で配布を予定しています。
セミナーの基本的な構成は、全体の時間として120分を予定しており、今回作成した家庭向け映像の上映、内容の解説、実機を利用した体験学習、パネルディスカッションの４つの要素で構成されます。

■家庭向け映像コンテンツの選定

ＷＧメンバーによるブレインストーミングにより、非常に多くのセキュリティ上の留意点が挙げられました。そして、作成にあたっての前提として、１）インターネットを快適に利用するために必要なマナーや一般常識を含めて理解をしてもらう、２）今現在、実際に発生している問題点をとりあげ対応策を盛り込むこと、の２点を盛り込み、一般家庭の日常にあてはめた場合のインターネット利用の中に潜むセキュリティ上の留意点を洗い出し取捨選択を行い以下の６項目に絞りました。

Part1　危険なメール

電子メールはコミュニケーション手段として、非常に便利なツールとして広く利用されていますが、留意すべき点として、メールに添付されてくるウイルスの脅威や、金銭の払い込みを指示するような詐欺メールなどがあります。

Part2　個人情報の漏洩

Web上では、資料の送付や、プレゼント、懸賞への応募といったサイトで、氏名や住所などの個人情報の入力が必要となる場面があります。個人情報を入力するにあたり他の用途で利用されないような注意が必要となります。

Part 3　しのびよる詐欺行為

インターネットを介した商取引やオークションといったやり取りが一般化しています。取引先が信頼できる相手なのか、入力してよい情報の判断についての注意が必要となります。

Part 4　掲示板・チャットのマナー

ネット上で複数の人々と意見を交わしたり、情報のやり取りをおこなうことのできる掲示板やチャットは有用な情報を入手したり、新たなコミュニティの形成など非常に有用な反面、不確実な情報やコミュニケーションミスによるトラブルも発生する場合があるので注意が必要です。

Part 5　「盗聴」される無線LAN

配線が不要なため、家庭内での利用が急速に進む無線LANの環境ですが、設定を誤ると情報が外部に漏れてしまうことがあるので注意が必要です。

Part 6　ホームページの落とし穴

情報を発信するのに有効なのがホームページの立ち上げですが、記載すべきでない情報が含まれていないか、著作権に対しての配慮がなされているかといった確認も必要になります。

CD-ROM撮影風景

■今後の予定

実際のセミナー実施は10月以降となり、現在実施に向けての作業が進んでいます。この記事が掲載される頃には、開催場所等の詳細についても確定していると思われますので、JNSAのサイトでスケジュールをご確認のうえ、皆様もぜひ本イベントへの参加をスケジュールしていただければ幸いです。

http://www.jnsa.org/caravan.html

第56回IETFミーティング参加報告書

富士ゼロックス株式会社
稲田　龍

セコムトラストネット
島岡　政基

NPO 日本ネットワークセキュリティ協会
安田　直義

富士ゼロックス情報システム株式会社
増田　健作

2003/3/17-21に米国サンフランシスコのSan Francisco HILTONにて開催された第56回IETF(Internet Engineering Task Force: http://www.ietf.org/)ミーティング にNPO　日本ネットワークセキュリティ協会(略称: JNSA http://www.jnsa.org/)が2002年度に情報処理振興事業協会セキュリティセンター(略称: IPA/ISEC http://www.ipa.go.jp/security/)より委託を受けた事業であるJNSA Challenge PKI 2002プロジェクトの報告とその成果物である“Multi Domain PKI Test Suite”のデモンストレーションをPKIX-WGにて行う目的でJNSA安田直義氏、セコムトラストネット島岡政基氏およびFXIS増田健作氏と共に参加したので報告する。

第56回IETFミーティングの参加者は34カ国から325の組織で、総勢1,640人であった。アトランタの第55回IETFミーティングの参加者は34カ国から334の組織で、総勢1,706人であった。横浜の第54回IETFが2,064人、第53回のミネアポリスのIETFが1,756人であった。同時テロ以前のロンドンで行われた第51回IETFが2,457人であったことを考えるとテロの影響と米国におけるITバブルの崩壊の影響と思われる。

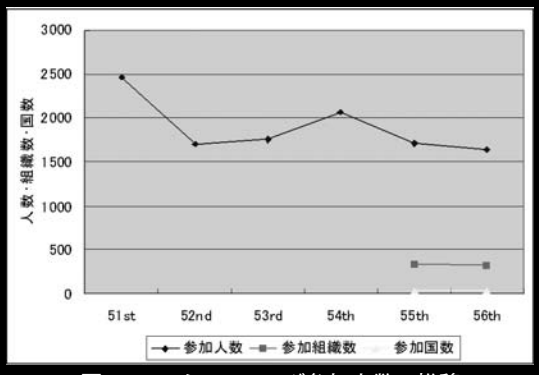


図1 IETFミーティング参加人数の推移

■報告者のPKIX-WGでの発表に関して

報告者である稲田は、アトランタで行われた第55回IETFに引き続きJNSAと共同で行っている「JNSA Challenge PKI 2002」の報告とその成果物である“Multi Domain PKI Test Suite”のデモンストレーションをPKIX-WGで報告した。

写真1 PKI-WGミーティングで報告している稲田(右)

「JNSA Challenge PKI 2002」プロジェクトおよび“Multi Domain PKI Test Suite”は、IPA/ISECの平成14年度「情報セキュリティ関連の調査・開発に関する公募」に対してJNSAが応募し採択された「電子政府情報セキュリティ相互運用支援技術の開発」によるものである。発表内容は、「JNSA Challenge PKI 2002」の概要(図2)と成果物である“Multi Domain PKI Test Suite”のコンセプトと機能概略（図 3)の説明および今後、Multi Domain PKI環境を定義し、テスト環境を作るためのInternet-Draftsを書く事を報告した。

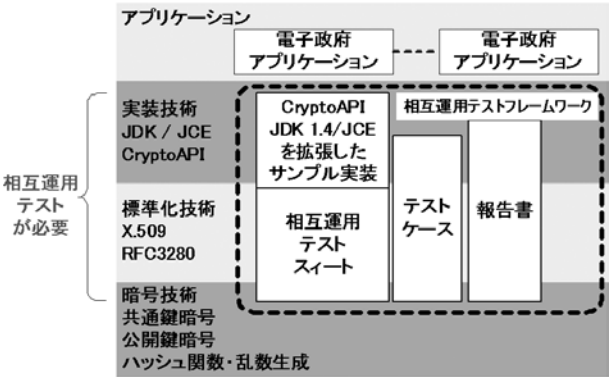


図 2 JNSA Challenge PKI 2002の概要

日本政府は、行政手続きの効率化と国民負担の軽減を目標に、国民と行政機関の間の申請・届出・通知などといった手続きを電子化する「電子政府」の構築を目指している。

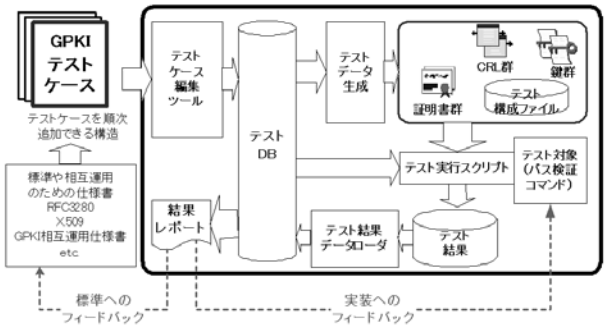


図 3 “Multi Domain PKI Test Suite”の概要

情報流通の基盤として構築されている政府認証基盤(GPKI)では、ブリッジCAモデルと呼ばれる信頼モデルが使用されている。ブリッジCAモデルは、主体者が異なるマルチドメインPKIを実現する手段として柔軟性のあるモデルであるが、その反面、ドメイン間での相互運用性を確保するために高度な技術を要する。

その状況下で、適正なPKIアプリケーションの開発を行うために証明書の失効確認/パス検証を行うテスト環境として“Multi Domain PKI Test Suite”とテストケースを開発した。“Multi Domain PKI Test Suite”はGPKIに限らず、汎用なPKIテスト環境を提供する。

現在、インターネット上ではPKIのアプリケーションが使われているが、複雑なPKIドメインを適用している例は少ない。また、PKIXが出したRFC 3280では、複雑なPKIドメインを使うことも考慮されてはいるが実際に試せる環境は少ない。NISTなどでRFC 3280の相互接続実験は行われているが、テスト環境の構築が難しく手軽にテストすることは難しい。

今回の“Multi Domain PKI Test Suite”は、スタンドアロンで動作し手軽にテスト環境を構築/運用できるようにしたものであり、他に類がない。「JNSA Challenge PKI 2002」の報告書を英訳および“Multi Domain PKI Test Suite”の公開を6月に公開する事を発表した。

写真 2 質問をするSteve Hanna氏

また、この“Multi Domain PKI Test Suite”を作るにあたってMulti Domain PKIの定義がIETFでは文書化されていない事が明らかになった。Multi Domain PKI環境でのテストケースを適正に作成維持していくためには「Multi Domain PKIの定義」を文書化し共通の認識で作成していく必要性を実感したため、「Multi Domain PKIの定義」のInternet-Drafts化を行うことと、テストケースを交換しやすくするためにテストケースデータベースのスキーマの定義をするInternet-Draftsを作成するつもりであると報告した。

発表後のQ&Aでは、Sun Microsystems社のSteve Hanna氏(JAVA JDKのPKI検証ライブラリの作成者)から、発表に使用したスライドがいつ公開されるかという質問があった(スライドはPKIX-WGのチェアには送付済みで、後日、Proceedingsとして公開される予定)。

写真 3 Tim Polk氏と

ミーティング終了後、台湾のPanasonic Taiwan Laboratoriesの周立平氏/陳柏飛氏がコンタクトして来た。彼らもMulti Domain PKI環境でのテストを行うことに苦慮しており、公開の時期と彼らの環境で動くかどうかを気にしていた。

ミーティングの終了後、Tim Polk氏と今後の活動に関しての議論を行った。作成を意図している2つのInternet-Draftsは、WGドキュメントにするかJNSAのパーソナルドキュメントではじめるかに関わらず7月のPKIX-WGでの議論対象にすることも可能であることを確認した。

また、発表後にGlenn Mansfield Keeni氏(Extended Incident Handling(INCH)の主要メンバー)より以下の共同で行える事がないかという趣旨のメールをもらった。

Subject: Todays PKIX Presentation
From: Glenn Mansfield Keeni <glenn@cysols.com>
To: Ryu Inada <Ryu.Inada@fujixerox.co.jp>
Dear Inada-san,
That was good and important work ! What are the plans from now. Let me know if I can help in any way.
We are looking forward to the presentation in Vienna.
Cheers
Glenn

■IETFにおけるPKIの応用

前回のアトランタで行われた第55回IETFミーティングでも、話題として上げられていたが、PKIをS/MIMEやSSL/TLS以外のアプリケーション/プロトコルでも利用する動きがある。

実際、AAA-WGで決まったDiameterにおいてはデータの交換形式としてCMS(Cryptographic Message Syntax)を用いて暗号化/電子署名が実現されている。
今回のS/MIME-WGのミーティングにおいてもSIPのパケットフォーマットにCMSを使うという動きがある。

PKIの利用範囲が広まりつつある反面、なかなか配備が進まない、技術的に難解であると言う不満が出ている。これらの状況は、ようやくPKIが「インターネットで使える技術」として認知されたということである。

また、今回の「IESG Open Plenary」で正式に発表されたが、Security AreaのDirectorとして長年貢献したMITのJeffrey I. Schiller氏に代わり、元RSA Laboratories(現Virgil Security社)のRussell Housley氏が就任した。Housley氏はRFC 2459/3280の著者の一人でありPKIの第一人者である。この交代は、3年近くPKIX-WGの活動を通じ、PKIの展開を進めていたが、この展開が遅々として進まない反面、OASIS/W3C/EESIなどから続々とPKIに対しての標準の提案とIETFに対しての協調の要請が出ている状況をIESGとしては看破できず、PKIに対してのてこ入れがなされたと報告者は受け取った。前節にも述べたとおり、PKIが「インターネットで使える技術」として認知こともあり、今後の展開が期待される。

■IETFの在り様の変化

IETFは、インターネットの標準の策定を行っているが、昨今、活動範囲が多岐にわたり他組織との間の協調の必要性が高くなっており、IETFが独自に規約/標準を決められなくなりつつある。これは、インターネットが複雑化し多くの団体がその価値を認め利用を始めていることの証明である。

また、IETFの内部にも問題を抱えている。

第一に、IETFの運営資金をどうするかが問題となり

つつある。IETFは、いくつかの資金源を持っているが、多くは年3回のIETFオフラインミーティングの会費で賄っている。ここ数回のオフラインミーティングの参加者が落ち込んでいる状況を考えると楽観は出来ない。実際、過去からの繰越金で運営されている状態であり3年後には資金が枯渇するとの報告があった。また従来、IETFのオフラインミーティングには、スポンサーが付くが(第54回の横浜のIETFでは、富士通がスポンサーとなった)、今回のオフラインミーティングでは初めての試みとしてスポンサーなしでオフラインミーティングが行われた。これは、米国でのIT業界の不況のためスポンサーのなり手がなかったのではないかとも、また、特定のスポンサーの利害にIETFが左右されるのを嫌ったとも考えられる。

第二に、IETFが標準化を行う領域が広く、また細分されておりIETFに参加しているメンバーのレビューが出来なくなりつつある。具体的には、各WGから提出されるInternet-Draftsのレビュー率が低くなり(平均10%程度)、Internet-DraftsとしてIESGが承認できない状況が増えている事が報告されている。これはInternet-Draftsの内容が高度に専門化されてしまい、多くのメンバーは何が書いてあるかが理解できていない状況であるといえる。

■IETFにおけるセキュリティに対する意識

IETFにおいても、セキュリティは大きな問題として取り上げられており、「セキュリティ」はひとつのキーワードとなっている。

具体的には、RFC/Internet-DraftにはSecurity Considerationというセクションが設けられておりRFCの発行に関してArea Director/IESG(Internet Engineering Steering Group)から「セキュリティに関しての考察が甘い」といったコメントがある場合が多い。

IETFの初日である17日には、Security Tutorialが開かれ、Security AreaのArea DirectorであるJeffrey Schiller 氏/Steven Bellovin氏よりProtocolを安全に設計するためのチュートリアルが開かれた。このSecurity Tutorialは昨今のIETFでは毎回開催されている。

また、IETFの会期の終わり近くに「Open Security Area Directorate」があり、IETFおよびインターネットにおけるセキュリティのあり方の議論と現状の報告が行われる。

今回の「Open Security Area Directorate」では、PKIが話題となっていた。PKIは、3年にわたって展開を行おうとしているが、うまく展開できていないのはなぜであるかが話題となっている。

IETFミーティングではターミナルルームと無線LANでのネットワークコネクティビティを提供しており、すべてのコンファレンスルームでインターネットへ自由に接続できる。前回のIETFミーティングでは、IETF主催者側より「無線LANにおいてパケットの盗聴の可能性があるのでSSL/SSH/IPsecなど暗号化を行うこと」という注意が流れている。今回のIETFでは、IETFのWeb上(http://www.ietf.org/meetings/netinfo.html)に以下の注意が載せてある。

> Security Warning
>
> Please note that using 802.11 without additional encryption is not private. In particular, do not use protocols with cleartext passwords, such as telnet or non-APOP POP3. Instead, use encrypted protocols such as SSH, SSL or IPsec. It is well-known that people may be sniffing packets on the network. There should be no expectation of privacy when using unencrypted protocols on the IETF-56 network.

EAPで無線LANの認証とセキュリティに関しての議論がなされている一方で、この様にある意味では無防備なネットワーク環境が用意されているところにIETFのひとつの側面が現れている。インターネットは、自由なネットワークアクセス環境を提供する。その上で自己を守るための枠組みを作り、それを利用するか否かは利用者が決めるべきであるという考えである。

■IETFのネットワーク環境とターミナルルーム

IETFでは、インターネットの利用を行うためターミナルルームが用意されているが、ここ数回のIETFにおいて通例となっている無線LAN(IEEE 802.11b)によるネッ

写真 4 ターミナルルーム 左側: 入り口/右側: 全景

トワークアクセスが提供されており、会場およびその周辺では自由にネットワークアクセスを行うことが出来た。そのためか、今回のターミナルルームはいつものターミナルルームに比べ狭く感じた(写真 4右)。
会場となったホテルのロビーおよびバーにおいてもこの無線LANを使うことが出来たためロビーのそこかしこでノートPCを持った参加メンバーがインターネットに接続していた。また、ロビー/バーで食事を取りながら打ち合わせをする姿も多く見られた。(写真5)

写真 5 ホテルのロビーにて

ターミナルルームはSUN Microsystemsが運営をしており、SUN RAYを持ち込んでいた。SUN RAYを使うために、SMART CARDが配られており、このCARDには固有のUIDが書き込まれており、ユーザ毎のSUN RAYの設定情報を呼び出すのに使われているとの事であった。(写真6)

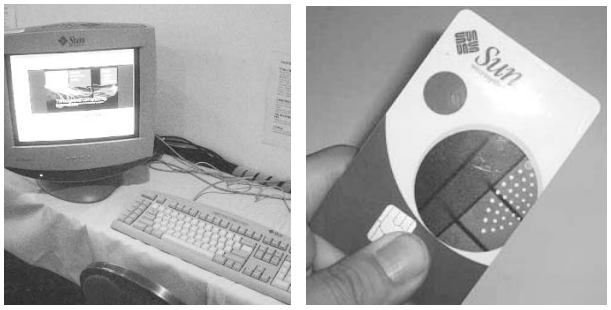


写真 6 SUNRAY(上)とSMART CARD(下)

IETFも転換期を迎えているのかもしれないが、次に引き受ける組織もまだ見えていない。ただ、参加しているメンバーは組織が変わっても相変わらず一緒に作業するチームになることは間違いないだろう。このような意味では、組織ではなく、知識の集約であることが理解できる。このような「場」にきちんと参加し、実体のあるデータや意見を出し、ディスカッションを行うことが重要であろう。日本でこのような活動ができるようになってきたのは喜ばしいことであるし、JNSAが協力できていることはすばらしいことだと思う。今後とも各位のご協力を賜れば幸いである。

会員企業ご紹介❽

ELNISテクノロジーズ株式会社

(http://www.elnis.com)

ELNISテクノロジーズは、2003年1月に日新電機株式会社情報通信開発事業部より分社独立したネットワークセキュリティの専門会社です。日新電機時代の1995年よりネットワークセキュリティの重要性に着目し、海外から高機能、最新技術を誇る製品をいち早く導入・評価し、国内向けのローカライズや販売を続けてきました。これまで培ってきた多くの実績やノウハウを活用し、セキュリティのプロとして皆様のセキュリティ対策に最適なプランをご用意し、ご提案いたします。

■最先端のセキュリティ製品

弊社では、常に最新の市場動向に着目し、海外より最先端の技術や製品を発掘し、より多くの国内ユーザ様にご利用いただけるよう、サポートやサービス等を含めてご提供いたしております。CyberGuard社のファイアウォール、Symantec社のポリシー監査や侵入検知、Zone Labs社のZone Labs Integrityなどです。

■自社開発のセキュリティソリューション

さらに、日新電機時代に培ったメーカとしての経験を活かし、ウィルス対策、ハイアベイラビリティ・ファイアウォールなどのアプライアンス製品を開発。ハードウェアの24時間365日の障害復旧対応サービスも含めたソリューションとして提供しております。

●注目製品●

安全性の高いファイアウォール CyberGuard Firewall

専用のセキュアOS上で動作する強固なアプライアンス型ファイアウォールCyberGuard Firewall。専用OSは、米国NCSCやヨーロッパITSEC、オーストラリアDSDなど、公的機関で高いセキュリティ基準に認定されています。

クライアントPCのポリシー管理 Zone Labs Integrity

集中管理が可能なエンドポイントファイアウォールZone Labs Integrity。エンドポイントPCのウィルス定義ファイルが最新でなければネットワークに接続させなかったり、許可しない通信アプリケーションを使用させないことで、最新のワームやウィルスの自動実行・拡散を防止します。加えて、全エンドポイントPCを一箇所で集中管理できるため、セキュリティポリシーを組織レベルで統一することができます。

情報漏えい抑止ソリューション ELNIS Security Detector

2003年7月には、内部情報漏えい抑止ソリューションELNIS Security Detectorを新発売。SMBパケットを解析し、Windows環境での共有のディレクトリやファイルに、誰が、いつ、どのようなアクションを起こしたのかを把握し、不審なアクセスに対して警告を発することができる画期的なソリューションです。本製品はNETWORLD+INTEROP 2003 TOKYOにてBest of Show Awardを受賞するなど高い評価を受けています。

■多様なサービス

セキュリティの専門家の立場から、お客様からのご相談に応じて、様々なサービスをご提供しています。

■セキュリティ検査/対策支援レポートサービス
■BS7799/ISMS適合性評価認定制度認定取得コンサルティングサービス
■セキュリティ教育サービス　　等

お問い合わせ先
ELNISテクノロジーズ株式会社　営業部
〒101-0024東京都千代田区神田和泉町1
神田和泉町ビル
TEL03-5821-5914　FAX03-5821-5884
http://www.elnis.com　webinfo@elnis.nissin.co.jp

コンピュータ・アソシエイツ株式会社

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

企業が受けるセキュリティ被害の損害の大部分は、外部からの侵入よりも、内部からのアクセスによるものと言われています。実際、日本国内においてもこのようなケースにより情報が漏洩し、当該企業がその情報の対象である顧客などから訴訟を受けるケースも目に見えて増加してきています。
コンピュータ・アソシエイツ(CA)は、企業の“内部セキュリティ”の必要性を訴えています。この領域を対象とするソフトウェア製品「eTrust Access Control」をご紹介させていただきます。

4つのコントロールを行う OS セキュリティ強化ソフト【 eTrust Access Control 】

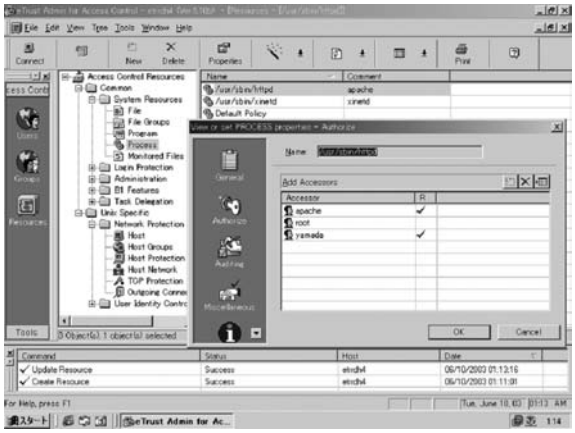
「eTrust Access Control(以下、eAC)」はUNIX系、Linux系、Windows系OSのセキュリティ強化製品です。

1. rootアカウントのコントロール

特権ユーザであるroot(Administrator)アカウントは、全てのファイル・プロセスに対し完全なアクセス権を持っています。この権限は、ウェブページ改竄や誤作動によるウェブサービスの停止なども引き起こします。また社内外の不正行為・システムの脆弱性を利用した攻撃をする際の標的となり得ます。
eACは、rootアカウントを一般ユーザのように扱うことによって、root権限をコントロールします。つまり、root依存の集中管理から脱却し、権限を分散させることで、これらの問題を根本的に防ぎ、各ユーザの責任の明確化を実現します。

2. システムリソースのコントロール

ファイル／ディレクトリ、ログイン、TCPサービス、特定ホスト、改竄検知、プロセス、suコマンドといった様々なリソースへのアクセスをコントロールします。
eACでは、アクセス権の制限をかける前に、ユーザに警告を通知するワーニングモードでテスト稼働を実行できます。これにより、アクセス権限設定の妥当性を検証した後、本稼働に移行するという段階的な運用が実現されます。



3. アクセスログのコントロール

アクセスログの取得とその保存は企業におけるセキュリティ管理にとって重要な要素です。eACはOSの標準機能よりも詳細なアクセスログを取得できます。例えば、UNIX系のOSでは、suコマンドによりユーザが切り替わった場合でも、もとのユーザとして記録されます。アクセスログはeACにより保護することで改竄を防ぎ確実な保存を可能にします。
また、異なるOSでも同じ形式でアクセスログを取得できるため、セキュリティ管理に必要なレポートを一元的に作成できます。

4. 異種多様サーバのコントロール

eACでは、複数台の異なるOS間で、リソースの設定やユーザ情報を一括更新する事ができます。図のようなGUIを用い、管理者の端末から遠隔操作を行います。アクセスログに関しても、転送機能を使用して、一つの端末で一元的に集中管理することができます。その結果、管理者の運用能率が上がり、管理コストの削減を実現します。

対応OS
管理サーバ：Solaris, HP-UX, AIX,
Red Hat Linux,
Windows NT/2000
管理ソフト：Windows NT/2000

製品名：eTrust Access Control
価 格：52万4,000円より
問い合わせ：
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 : 0120－702－600

大興電子通信株式会社
(http://www.daikodenshi.jp)

DAiKO

DAiKOは、日本がまだコンピュータの黎明期であった1953年の創業以来、IT（情報技術）のプロフェッショナルとして、企業経営および技術分野で多数の問題の解決に携わってまいりました。おかげさまで、約6,000社のお客様に支えられて、今年50周年を迎えさせていただきます。
私たちは、製造業、流通・サービス業、金融業、公共などの業種別のソリューションを軸に、セキュリティソリューション、ネットワークソリューションなどを最適に組み合わせることで、お客様の経営課題のトータルな解決に全力を尽くしております。

◆ DAiKOセキュリティソリューションサービスの内容

（1）構築導入サービス

① ファイアウォール構築サービス
- ファイアウォールのポリシー設計、構築、テスト
- VPN環境の設計、構築、接続テスト

② セキュアインターネットサーバ構築サービス
- サーバ公開前に、セキュリティパッチや各種設定の変更を実施することでセキュアなサーバとして提供

③ VPN、暗号化システム構築サービス
- サーバ～クライアントに対しツールの導入作業を実施

④ 認証システム（ワンタイムパスワード）構築サービス
- RSAセキュリティ社の「SecurID」及び認証サーバである「ACE/Server」の導入

⑤ ウィルス対策システム構築サービス
- インターネットゲートウェイからクライアントまで、各メーカのウィルス対策ツールの導入、Mailサーバやファイアウォールの設定変更

⑥ セキュリティ監査・監視システム構築サービス
- インターネットセキュリティシステムズ社の「Internet Scanner」「System Scanner」「Database Scanner」「RealSecure」の導入支援

⑦ メールコンテンツ管理システム構築サービス
- クリアスイフト社の「MIME Sweeper」によるメール管理システムの導入支援

⑧ サーバルーム入退室管理システム構築サービス
- ICカード、磁気カード、指紋認証等を利用したシステム構築

⑨ サーババックアップシステム構築サービス
- コンピュータ・アソシエイツ社の「ARCserve」等によるサーバ・バックアップシステムの構築

（2）運用支援サービス

① セキュリティ診断サービス
- インターネットセキュリティシステムズ社「Internet Scanner」「System Scanner」等によるネットワーク、各種サーバの脆弱性の検査、セキュリティレベルの調査、および対策の提示
- 自社開発ツールによるファイアウォールの負荷テスト、Mailサーバの第三者中継チェック
- ペストパトロール社の「Pest Patrol」によるスパイウェア、トロイの木馬の検出、除去

② セキュリティ監視サービス
- ネットワークや公開サーバに不正アクセス監視のためのセンサーを設置し、24時間365日リアルタイム監視

③ RealSecureログ解析サービス
- 「RealSecure」のログを解析し、対処方法を提示

④ ファイアウォールログ解析サービス
- ファイアウォールのログ解析による被害の未然防止

⑤ ウィルス監視サービス
- ウィルスの発生状況からウィルス対策ソフトのバージョン、パターンファイルの更新状況までをセンター監視

（3）コンサルティング

① セキュリティポリシー策定
- 最適なセキュリティポリシー策定を支援

② ISMS認証取得
- ISMS適合性評価制度に基づくISMS認証取得支援

③ プライバシーマーク取得
- プライバシーポリシーの策定から申請まで、プライバシーマーク取得支援

④ セキュアインターネットインフラ構築
- ファイアウォール、インターネットサーバ、IDS、ウィルス対策ソフト等、インターネットインフラ構築時のトータルセキュリティ対策を企画、提案

お問い合わせ先
大興電子通信株式会社
営業推進部
TEL:03-3266-8171 FAX:03-3266-8109
E-mail:planner@daikodenshi.co.jo

株式会社日本高信頼システム研究所
(http://www.jtsl.co.jp)

株式会社日本高信頼システム研究所（略称：JTSL）は、2002年2月にセキュリティエンジニア数名が出資しアジア域においてコンピュータ環境の信頼性（特にセキュリティ面）を向上させることを目的として立ち上がった中立系のセキュリティソリューション専門企業です。
弊社が最も得意とするTrustedOSを用いた高信頼システムソリューション。ほんの一握りの企業がソリューション提供していたTrustedOSは昨年から中央官庁の本格的な動きが始まったことを受けてようやく日本でも本格的に目覚める時期がやってきました。
最近、新聞紙面や雑誌に掲載されることが多くなってきたTrustedOSや機能を簡略化したセキュアOSを始めとする信頼できるセキュリティソリューションはセキュリシステム全体の大幅なコストダウンを実現する一方で、比類なきセキュリティ強度をお客様に提供いたします。

主な事業内容

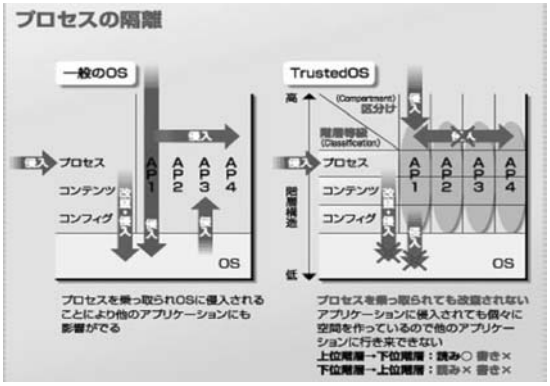
◆高信頼システムソリューション
TrustedOS、セキュアOSを用いたセキュリティ対策のご提案～導入、サポートまで
・サーバ構築（ポリシー設計、アプリケーション動作確認含）
・運用支援（一部、オンサイトや24H対応が可能です）
・教育（日本語環境ににて実施）

＜取扱い製品名＞
・PitBull.comPack
・PitBull LX
・Trusted Soalris
・SELinux

◆セキュリティソリューション
お客様の環境に合わせたセキュリティ対策のご提案～導入、サポートまで
・FireWall
・IDS
・VPN
・ウィルス対策
・認証（OTP全般、バイオ認証）
・コンサルテーション（ISMS、BS7799-2）

TrustedOSとは、
米国国防総省が定めたセキュリティ基準を満たした製品。「米国国防総省は，1985年に高信頼コンピュータ・システムの評価基準書であるTCSEC(Trusted Computer System Evaluation Criteria)を策定しました。これはコンピュータのセキュリティ強度をランクづけした規約です。TCSECではセキュリティ強度が高い順にA，B，C，Dの4つのDivisionを定めており、さらにそれぞれを細かくクラス分けしてあります。このうちTrustedOSと呼ばれるものは通常、B-Division以上の要求仕様を満たした製品です。

PitBullの概要



■主な機能
・強制アクセス制御、セキュリティゲートウェイやSecurity Communication Enforcerによる通信の制御など
・メモリプロセス、ファイル、パケット、デバイス等の隔離

■導入効果
・高度なセキュリティの実現によるリスクの低減
・セキュリティ対策製品の整理(必要最小限で良い)
・運用/維持コストの大幅な削減

■これまでの国内導入実績（PitBull）
・中央省庁（GPKIなど）
・大手SI企業（公開Webサーバ）、
・特殊法人（公開系全サーバ）
・大手流通企業（エクストラネットサーバ）
・他多数

お問い合わせ先
株式会社日本高信頼システム研究所
システム営業本部　ソリューション営業部
TEL : 03-3868-8921
E-Mail : sales@jtsl.co.jp

株式会社ネット・タイム
(http://www.nettime.co.jp)

株式会社ネット・タイム

今お使いのID・Passwordは大丈夫ですか?

"e" style with "S".

社内不正の約60%がID・Passwordの管理不備、他人からの入手によるものです。(警視庁資料による)

ネット・タイムでは、ICカード(非接触とのハイブリットカード含む)をはじめとしたセキュリティインテグレーションツール「ARCACLAVIS」を中心に様々な"e"styleに対応したセキュリティソリューションを開発・製品化してまいりました。また、セキュリティインテグレーターとして、パートナー各社が持つセキュリティ技術を組み合わせて、お客様の"e"styleに求められるトータルな製品・サービスを提供しています。

■セキュリティインテグレーションツール …ARCACLAVIS

IT革命を生き抜き、勝ち残る。今、企業に求められる経営戦略。それがARCACLAVISなのです。

企業にとって生産性、競争力を向上させるためコンピュータネットワークの活用は不可欠です。反面、e-business、e-commerceが拡大するネットワーク社会においては、社外からのシステムへの不正侵入、社内情報の社外への漏洩等、従来の企業経営では想定できなかったリスクを抱えています。ARCACLAVISは、ICカードによるユーザ認証、重要データの暗号化など、ネットワーク社会に不可欠なセキュリティアプリケーションを提供し、企業の積極的な経営をサポートします。

第三者の不正アクセスから企業システムをガード。情報社会のライフラインに安心と信頼を提供します。

情報社会においてコンピュータシステム、ネットワークは企業の生命線です。コンピュータ犯罪による情報システムの停止、破壊は企業にとって致命傷となりかねません。ARCACLAVISは、ICカードによるアクセスコントロールにより、第三者のコンピュータシステムの不正使用を防ぎます。

■非接触対応…ARCACLAVIS

「ARCACLAVIS」が、FeliCa技術に対応。オフィス環境では、入退室管理の"物理的なセキュリティ"から、PC起動制御、社内ネットワークシステムへのアクセス管理、自宅やモバイル環境では、RAS接続時のアクセス認証等の"情報セキュリティ"といったマルチアプリケーソン環境を、利便性の高い非接触ICカード1枚に統合して、セキュアにご提供します。

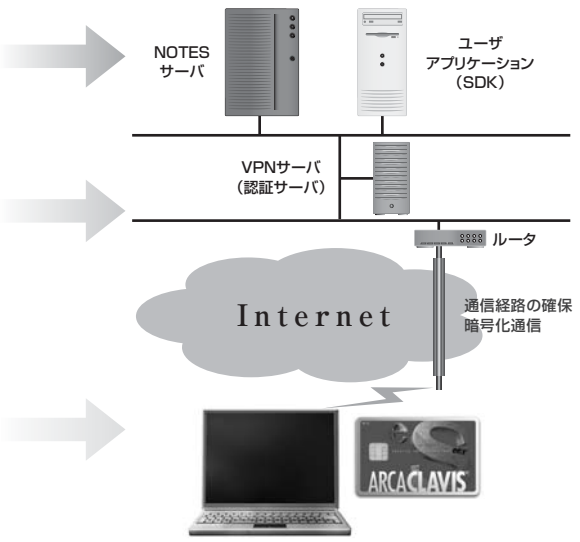
お問合せ先

株式会社ネット・タイム

営業本部 〒160-0022
東京都新宿区新宿1-34-5 御苑直田ビル
TEL.03-5360-7761 FAX.03-5360-7717
e-mail : info-arca@nettime.co.jp

ARCACLAVISアプリケーション

NOTES	本人認証、セットアップの簡略化、ユーザ環境の切り替え。
SDK (別売)	個別開発により、お客様のアプリケーションや他のベンダーから提供された認証情報をICカードに格納。
VPN	自動接続から通信経路の保護、アクセス制御、ログ収集。
RAS	ICカード内にRAS接続情報を格納。
OTP [Powered by SecurID]	パスワード生成の素となるシードをICカードに格納。SecurID(RSA社)認定。
ENCRY Pro	ファイル暗号、復号をリアルタイムに実現。
LOGIN	Windowsログイン制御。
LOCK	PCの起動制御。
AutoLogin	アプリケーションへの自動認証機能。



株式会社ヒューコム
(http://www.hucom.co.jp)

株式会社ヒューコムは、1986年に産声を上げました。以来、時代の先進性を絶えず追求しつつ、インターネットを基盤とした情報技術の進化と共に発展を続け、現在では“セキュアネットワーク分野のトータルソリューションプロバイダ”として、ネットワークシステムの設計、構築、ポリシに則った運用・管理、監視、更にはセキュリティ教育まで、一貫したソリューションの提供をOne Stop、One To Oneで実現できる企業として、事業を展開しております。
本稿では、特に、2002年８月の住民基本台帳ネットワーク稼動と同時に、システムへの不正侵入、機密情報（個人情報）漏洩等のセキュリティ事故の未然防御、更には適切なセキュリティマネジメントの継続的向上を目的として組織化しましたLG－SAT（地方自治体セキュリティ監査チーム）が提供するHUCOM情報セキュリティ監査サービスを以下に紹介致します。本年４月に施行されました経済産業省の情報セキュリティ監査制度に準拠したものであり、独立且つ高い専門性・倫理性を持って客観的に評価し得るセキュリティ監査サービスであります。

【サービス概要】

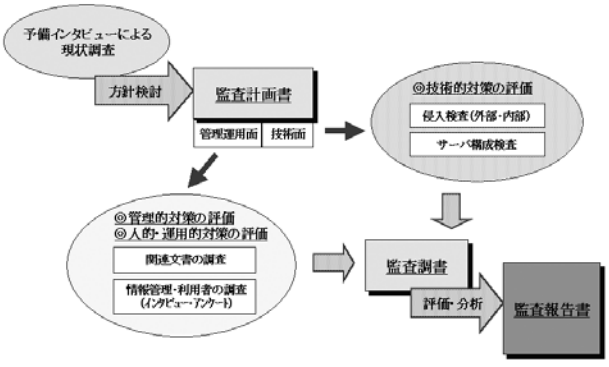
経済産業省「情報セキュリティ監査基準」に準拠し、ポリシーレベルの管理的対策から、人的・運用的対策、技術的対策までを総合的に評価します。

1. セキュリティポリシーや各種管理規程の調査、情報セキュリティ管理部門へのインタビューにより、セキュリティ基本方針やセキュリティ組織、各種法的要求事項への遵法性などについて評価します。
2. 情報管理・利用部門へのインタビューや現場調査により、人的要因による情報漏洩リスクに対する管理的対策の有効性を検証します。
3. システム文書の精査により、システム設計や技術的対策の適切性を検証、また運用管理が正しく行われているかを評価します。技術的対策に関しては、脆弱性検査によりその有効性を検証します。
4. 監査結果報告では、現状のセキュリティ対策の客観的な評価と共に、改善すべき事項と改善の方向性を具体的に提案します。

【HUCOM監査サービスの特徴】

1. 技術的対策における脆弱性検査は、セキュリティサービスプロバイダとしてのノウハウ及び中央省庁、地方自治体等の豊富な実績に基づき、対策の実効性を検証します。
2. 上記脆弱性検査は、クラッキング手法に基づくペネトレーションテストを外部・内部ネットワーク両面よりスキャニングを実施。更に最近の事例で多く見られるXSSに代表されるWebアプリケーションの脆弱性を調査します。
3. 監査報告を受けて対策を実施した後に、それが有効かを確認するフォローアップ監査を実施いたします。
4. オプションとして、システム管理者向けのセキュリティ技術者トレーニング、一般職員・全社員対象のセキュリティ意識向上教育の提供が可能です。

【サービスフロー】



◆お問合せ先◆
株式会社ヒューコム　SMS事業本部
〒166-8521 東京都杉並区梅里1-7-7
新高円寺ツインビル
TEL：03-5306-7339　FAX：03-5306-7334
E-mail sms@hucom.co.jp
URL　http://www.hucom.co.jp

松下電工株式会社
(http://www.nais-netcocoon.com)

■■■　ネットワークセキュリティ製品のご紹介　■■■

松下電工は、既存事業に加えて、新しい市場・商品・サービスの創造に積極的に取り組んでいます。
今回は、IT関連新事業であるネットワークセキュリティを実現する「NetCocoonシリーズ」の商品をご紹介いたします。

『VPN通信のトラブルシュート・ツール「NetCocoon Emulator」新発売』

◆新商品「NetCocoon Emulator」は、松下電工(株)が新たに開発したMan-in-the-Middle技術を応用したVPNブリッジ機能により、Pre-Shared KeyまたはPKCS #12によるIPsecの復号を可能にし、さらにSSLの復号にも対応した、VPNのトラブルシュートに最適必須のプロトコル・アナライザです。

◆IPsecの暗号化鍵(SKEYID_e, KEYMAT)を出力しないVPN装置にも対応できますので、VPN装置の開発から、VPNの構築、運用まで、より多くのシーンで活用いただけます。

◆また、暗号通信の復号以外にも、トラフィックをさまざまな切り口で視覚化する各種ビュー、対象パケットをすばやく分類、抽出するフィルタ機能、通信トラブルの原因究明に便利なパケットの編集・リプレイ機能など、充実した機能でネットワークの検証を強力にサポートします。

『ユビキタス時代の最先端通信インフラ、モバイルVPNソフト「Viatores Ver4.3」発売』

ユビキタス時代のワークスタイルは、「どこでもオフィス」。これをViatoresが実現します！

◆「最新技術の採用商品」：このViatoresは、移動先でもアドレス変更が不要なMobile IP技術(使い易い！)、高いセキュリティレベルの通信を可能にしたIPSec技術(安全通信！)を採用しています。

◆「どこからでもイントラネットにアクセスできます」：営業拠点、ホットスポット、自宅、ホテル、海外など、インターネットに接続できる環境さえあれば、国内外を問わず、幅広くイントラネットにアクセス可能です。ブロードバンド接続のレスポンスは、そのまま体感できるので、快適です。勿論ダイヤルアップにも対応できます。

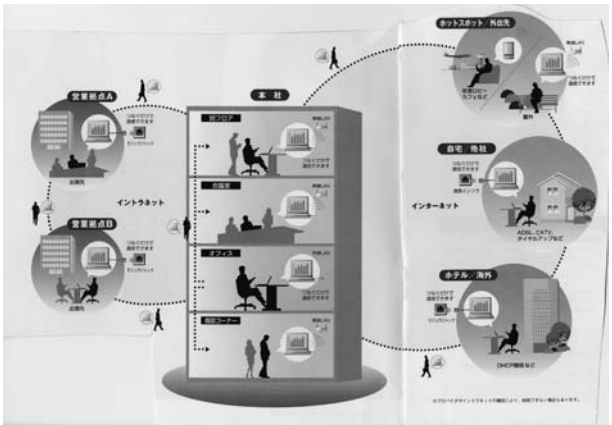
◆「ランニングコストの削減」：固定低価格である常時接続環境の利用により、通信コストを削減できます。

◆現在の接続環境を自動認識してシームレス・ローミングを実現します。有線LANから無線LANへの切替も自動で行うため、通信が途絶えません。

◆ICカードなどを用いた個人認証システムと連携することで、ICカードを持った個人だけがViatoresを使用でき、その履歴を記録・管理できます。個人情報管理が求められる自治体などへ有効です。

◆「マネージメント機能の充実」：ネットワークポリシー設定後、自動的に各コンポーネントのキーファイルなどを生成します。ユーザーを作成することで、自動的にホームアドレスを割り振ります。

◆主な導入実績：自治体、大学、メーカー企業、製薬会社研究・営業部門、海外営業関連部門　ほか



商品の詳しい説明は、ホームページをご覧ください。⇒
http://www.nais-netcocoon.com

◆お問合せ先◆
松下電工株式会社
新事業推進部　ネットワークセキュリティチーム
〒571-8686 門真市大字門真1048番地
TEL：06-6906-6384
E-Mail security@trc.mew.co.jp

JNSA会員企業のサービス・製品・イベント情報です。

■製品情報■

○セキュリティポリシー対応暗号システム「データクレシス」

セキュリティポリシー対応暗号システム「データクレシス」はISMSやBS7799などのセキュリティポリシー認証基準の下で運用できる暗号システムです。情報資産の機密性の区分（極秘、関係者秘、社外秘など）に応じて暗号化する事により、復号できる権限者が決定される。セキュリティ監査資料の出力や暗号使用ポリシー・基準書の作成支援機能がある。セキュリティポリシーと暗号化による情報漏洩対策として有効です。
http://www.ahkun.jp

◆お問い合わせ先◆
株式会社アークン
E-mail: dc@ahkun.jp

○企業のための個人情報保護法対策決定版！！「情報セキュリティと個人情報保護　完全対策」価格：9,500円＋税

個人情報保護法が施行され、企業や自治体はどんな対応が必要になるのでしょうか。もし個人情報が漏洩すれば、企業のイメージがダウンするだけにとどまりません。訴訟に発展すれば、多大な費用が発生する可能性すらあります。
　本書は、そうした個人情報の保護に関する課題と対策を解説。漏洩するケースや企業内における個人情報の取り扱い方、情報資産を保護するための情報セキュリティポリシーの策定などから構成しております。
http://coin.nikkeibp.co.jp/coin/kj

◆お問い合わせ先◆
グローバルセキュリティエキスパート株式会社　管理部
TEL:フリーダイヤル 0120-210546（年中無休6:00～22:00）
携帯・PHSから 03-5696-6000

○「家庭」のインターネットセキュリティに関する意識調査報告書

（株）富士総合研究所は（株）イオンビスティーと共同で、消費者のインターネットセキュリティに対する意識および実態の把握のため、「『家庭』のインターネットセキュリティに関する意識調査」を行いました（有効回答数8,428件）。「家庭のセキュリティ対策の実態」「インターネットセキュリティに対する意識」「使用しているセキュリティ製品」「個人情報保護に対する意識」など、消費者の生の声についてまとめています。

http://www.fuji-ric.co.jp/newsrelease/netresearch030731.html

◆お問い合わせ先◆
株式会社 富士総合研究所 情報セキュリティ評価研究室
E-mail: secenq@cyg.fuji-ric.co.jp
TEL: 03-5281-5292

○英国nCipher社CodeSafe SSL

CodeSafe SSLは選択したSSLセッションを耐タンパHSM内部でのターミネートを可能とし、SSLセッションを顧客ブラウザからHSMへダイレクトに繋げ、WEBサーバ上からの情報漏洩を防止します。
また、PIN認証やセキュアな再暗号化・復号化処理、データベース暗号、タイムスタンプのようなアプリケーションをHSM内へ格納可能。
http://www.marubun.co.jp
http://www.ncipher.com

◆お問い合わせ先◆
丸文株式会社　情報機器部　営業第2課　廣瀬　智康
TEL　03-3639-9881　FAX 03-5644-7627
E-mail : hirose@marubun.co.jp

■サービス■

○iSafeセキュリティ監査・アセスメント

トータルシステムのセキュリティを確保することを目指すiSafeセキュリティ事業として、情報セキュリティ監査およびセキュリティプロセスアセスメント を基本としたサービスを提供します。情報セキュリティ監査業務では、経済産業省の提示している管理基準を合理的に解釈し直した汎用基準を産業・企業特性に合わせたテイラリングにより助言型の監査を行うほか、国際規格ISO／IEC21827に基づく成熟度評価も行います。
http://www.imslab.co.jp/

◆お問い合わせ先◆
株式会社　情報数理研究所
E-mail: precbk@imslab.co.jp

○情報セキュリティ対策支援トレーニング& SEA/J情報セキュリティ技術者認定コース

・情報セキュリティ対策支援トレーニング
『WEBセキュリティ管理(1日)』 9月10日、9月17日
『セキュアプログラミング技法(1日)』 9月11日、9月18日
【概要】セキュアなWEBサーバ構築とWEBプログラミングの技術習得
【対象】構築系技術者、開発系技術者
・ＳＥＡ／Ｊ情報セキュリティ技術者認定コース
『基礎コース(2日)』 9月24～25日、10月22日～23日
【概要】スキルマップの項目に対応した体系的な知識教育
【対象】情報セキュリティ全体の基礎知識を習得されたい方
http://www.hucom.co.jp/service/education.html

◆お問い合わせ先◆
株式会社ヒューコム　広報担当
E-mail: pr@hucom.co.jp
TEL: 03-5306-7378

■イベント紹介■

○CISSP紹介セミナー

国際的に権威のある情報セキュリティ専門家資格試験CISSPがさらに本格的に導入されます。この試験は高度なものですが、昨年のわが国導入以来すでに多くの方がチャレンジしています。CISSPおよびその公式教育CBKセミナーに関する本年度2回目の紹介ミニセミナー(日本語)を行います。
日時：11月18日(火)(予定)
日程は変更の可能性がありますので弊社ホームページでご確認ください。
http://www.imslab.co.jp/

◆お問い合わせ先◆
株式会社　情報数理研究所
E-mail: precbk@imslab.co.jp

○ウイルス対策管理セミナーのご案内

本セミナーでは、管理者の方々のニーズに合わせ、「ウイルス対策管理に全く手間をかけたくない方」、「ウイルス対策管理は大変だけれど、やはり自分で一元管理しなければならない方」それぞれのケースについて、最適なソリューションをご紹介致します。また、インターネットからのウイルス感染を防護し、より強力なウイルス対策を実現したいお客様向けに、ゲートウェイにおける効果的なウイルス対策についてもご説明させていただきます。
http://www.nai.com/japan/seminar/systemmanagement.asp

◆お問い合わせ先◆
日本ネットワークアソシエイツ株式会社

イベント開催の報告

NSF2003 spring開催の御報告

今年から、JNSAでは、NSF（Network Security Forum）を年2回開催し、春は前年の活動報告として活動内容をご紹介し、秋はシンポジウムとして更に広い視点で議論もできる場にしていこうと考えています。本年度は6月3～4日の2日間「RSA Conference 2003」と併催で行いました。

■ **会期：** 2003年6月3日（火）～4日（水）
■ **会場：** 東京国際フォーラム
　　地下2階　セミナー室
■ **主催：** JNSA
■ **同時開催：** RSA Conference 2003 Japan
■ **協力：** キースリーメディア・イベント株式会社

プログラムは、2日間で10のWGの活動報告が行われるという、濃い内容となりました。プログラムは下記のURLをご覧になっていただければと思いますが、発表されたWGとタイトルだけを挙げてみます。

http://www.jnsa.org/nsf2003spring/

●不正プログラム調査WG活動報告
「メモリ感染型ネットワーク・ワームの脅威とその対策」
●コンテントセキュリティWG活動報告
「コンテンツビジネスへの脅威とその可能性」
●セキュリティ被害調査WG活動報告
「2002年度被害調査結果と国内被害額の推計」
●セキュリティ監査WG活動報告
「情報セキュリティ監査制度を利用した、情報セキュリティ管理策定」
●スキルマップ作成WG活動報告
「知の尺度「Skillmap」の考え方～セキュリティ技術者育成に向けて」

●セキュリティポリシーWG活動報告
「ポリシーサンプルの解釈と応用」
●相互接続WG活動報告
「802.1Xを使った無線LANのセキュリティと相互接続実験」
●インターネットVPN-WG活動報告
「公衆無線LANをビジネスで使用するときの課題」
●Challenge PKI 2002 活動報告
「PKIアプリケーションの相互運用を促進するChallenge PKI 2002」
●Challenge PKI 2002 活動報告
「IETFでのPKI関連技術動向」

現在JNSAで活動しているWGは約20に上りますので、今回ご紹介できたのはまだ半分程度でしかないことになります。JNSAの活力の基はWGそのものだといってよいでしょう。

◆◆◆ WGを支えるモチベーション ◆◆◆

JNSAのWGを支える力は、どこからくるのでしょうか？ひとつの仮定や現状は、次のようなものです。

- WGは原則的にはボランティアベースで活動している。
- WG活動は、メンバーの自主性を尊重し、事務局などは側面支援を行っている。
- WG参加メンバーが問題意識を持っているテーマを選択し議論している。
- 成果物はJNSAから原則公開とする。（原著作権は執筆者個人に帰属する。）
- 外部から受託する予算もWG活動と連動している。

このように、問題意識が共有されているテーマについて、必要性を感じて参加していることが、最大の効果を挙げているように思えます。

実はこのような形態で活動できている団体は、案外少ないと思います。今後の課題は、このようなモチベーションやパワーを維持し、更に高めて有用なコンテンツを公開し続けていくことでしょう。

発表資料は下記のURLで公開しています。

http://www.jnsa.org/nsf2003spring/program.html

事務局お知らせ
JNSA ANNOUNCE

1. セミナーのお知らせ

● JNSA、日経インターネットソリューション主催「セキュリティ・スタジアム」セミナー

テーマ：「コンピュータ・フォレンジック」

「コンピュータ・フォレンジックとは何か？」
講師：伊原秀明氏・渡辺勝弘氏
「不正アクセスの脅威」
講師：渡辺勝弘氏
「不正アクセス調査」
講師：伊原秀明氏
「コンピュータ・フォレンジックの法的側面」
講師：牧野法律事務所
弁護士／牧野二郎氏

■日　　時：2003年9月10日（水）
午後1時～午後5時半　開場12時半

■会　　場：工学院大学新宿校舎
新宿区西新宿1-24-2

■定　　員：120名

■参加料金：
JNSA会員　9,000円　　非会員 10,000円
＊当日現金でのお支払いとなります

■お申込み：JNSAホームページのセミナー申込みフォームよりお申込み下さい。
http://www.jnsa.org/seminar_20030910.html

● Network Security Forum 2003 (NSF 2003)

開催趣旨：セキュリティの現実に鋭く切り込む目が放せない3日間！！

■会　　期：2003年10月22日（水）～24日（金）
13：00～17：30

■会　　場：東京ビッグサイト　会議棟

■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（JNSA）

■協　　力：日経ＢＰ社

■併　　催：Security Solution 2003（日経ＢＰ社）

■同時開催：セキュリティ論文審査発表（22日）

■参加料金：（22日は無料）
1日券　　JNSA会員　7,000円　　非会員　8,000円
2日間共通券　JNSA会員 12,000円　　非会員 15,000円

■お申込み：JNSAホームページよりお申込み下さい
http://www.jnsa.org/nsf2003/

■予定セッション：
22日 セキュリティ論文発表ならびに表彰式
（参加費無料）
23日・パネルディスカッション
「日本のインシデント対応体制」
モデレータ　山口　英 氏
・「米国政府関連情報セキュリティ最新動向」
～2003年7月米国視察団報告～
・パネルディスカッション
「セキュリティホールに関する法制化の諸外国状況報告と日本における提言」
情報ネットワーク法学会
24日・「講演内容未定」　高木浩光 氏
・「世界的なPKIの相互運用を目指すChallenge PKIプロジェクト」
松本　泰 氏、稲田　龍 氏
・「ネットワーク監視技術としてのハニーポットについて」
濱本　常義 氏
・「WindowsとUNIX/Linuxのセキュリティ：2003」
小島　肇 氏

JNSA全国情報セキュリティ啓発キャラバン

これだけは知っておきたい

インターネット安全教室

～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、ウイルス感染、詐欺行為、プライバシー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。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、情報犯罪を防ぐことはできません。こうした状況をふまえ、NPO 日本ネットワークセキュリティ協会（JNSA）では、家庭や学校からインターネットにアクセスする人々を対象に、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を開催することにいたしました。この「インターネット安全教室」は、経済産業省の委託により実施するもので、各地の放送局・新聞社・青年会議所・自治体・教育機関などの協力を得て、2003年10月～11月にかけて、全国10カ所で開催する予定です。

[開催時期]
2003年10月～11月
[開催場所]（　　）は共同開催
奈良（なら情報セキュリティ研究会）、福井（福井県高度情報化推進協議会事務局）、岡山（岡山市）、
神奈川（学校法人岩崎学園）、福岡（学校法人麻生塾）、沖縄（浦添市）、大分（財団法人ハイパーネットワーク社会研究所）、
大阪（北大阪商工会議所）、新潟（財団法人にいがた産業創造機構・NPO新潟情報セキュリティ協会）、徳島、札幌
※詳細は別紙スケジュールを参照
[主　　催]
経済産業省
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）
[協　　力]
各地の放送局・新聞社・青年会議所・自治体・教育機関など
[開催目的]
■ウイルス感染、詐欺行為、プライバシー侵害などの情報犯罪に対する正しい理解を広め、初心者でも安全快適にインターネットを楽しめるように啓発する
■各地でネットワークセキュリティの啓発に関わる人々に「インターネット安全教室」セミナーのノウハウやツールを提供し、「インターネット安全教室」の活動を全国に広める
■各地でインターネット・ビジネスに関わる人々の振興に役立てる
■情報化月間の行事のひとつとして、情報化に対する正しい理解と認識を広める

【キャラバン概要】

■対象者
・家庭や学校からインターネットにアクセスする人々
・地域でネットワークセキュリティ啓発に関わる人々
・各地でインターネット・ビジネスに関わる人々
※1回あたり100名～300名の参加者を予定。
※全国10カ所で開催し、総計1,000名～3,000名の参加者を予定。

■開催地
各地の放送局・新聞社・青年会議所・自治体・教育機関などに協力を呼び掛け、会場の提供や参加者の募集、告知、取材、報道などの協力を得られる地域で開催する。

■構成（2時間）

「インターネット安全教室」CD-ROM（ビデオ）とテキストを用意し、インターネットのどこが危険か、どうすればインターネットを安全・快適に楽しむことができるかについて解説する。次に、参加者の中から数名に、実際に情報犯罪がどのようなものなのか、被害にあったときにはどうすればいいかといった体験学習をしてもらう。そして、当地でインターネット・ビジネスに関わる方とディスカッションを行い、インターネット・ショッピングを安全に楽しむ方法や、インターネット・コミュニティに参加する方法、公共サービスを活用する方法などを紹介する。最後に、記念に「インターネット安全教室」ステッカーなどのノベルティを配付し、インターネットにアクセスする際にどんな点に気をつければいいか、いつでもポイントを思い出せるようにしてもらう。

1.オープニング

2.セミナー

・「インターネット安全教室」CD-ROM（ビデオ）を上映
・「インターネット安全教室」テキストを解説
・体験学習
・現地でインターネット・ビジネスに関わる方とのディスカッションや質疑応答

3.エンディング

・「インターネット安全教室」ノベルティとCD-ROMを配付

■JNSAセキュリティ啓発キャラバン開催スケジュール（8/20日現在）

10月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
			(1)奈良県 帝塚山大学			
12	13	14	15	16	17	18
	体育の日					
19	20	21	22	23	24	25
				(2)福井県 福井県中小企業産業大学校		(3)岡山県 岡山市職員研修所
26	27	28	29	30	31	

11月

日	月	火	水	木	金	土
						1
						(4)神奈川県 岩崎学園
2	3	4	5	6	7	8
	文化の日				(5)福岡県 麻生塾	
9	10	11	12	13	14	15
				(6)沖縄県 浦添市民会館		(7)大分県 大分県立芸術文化短大
16	17	18	19	20	21	22
		(8)大阪府 北大阪商工会議所				
23	24	25	26	27	28	29
勤労感謝の日	振替休日					(9)新潟県 にいがた産業創造機構
30						

2. 後援イベントの知らせ

1.「電子署名・認証フォーラム」

会　期：2003年9/24（水）～25（木）
主　催：電子署名・認証利用パートナーシップ(JESAP)
　　財団法人日本情報処理開発協会(JIPDEC)
　　http://www.procom-i.co.jp/jesap/
会　場：工学院大学新宿校舎

2.「ネットワーク・セキュリティワークショップ in越後湯沢」

会　期：2003年10/2(木)～4(土)
主　催：ネットワーク・セキュリティワークショップ
　　in越後湯沢
会　場：新潟県南魚沼市湯沢町
　　http://www.yuzawaonsen.gr.jp/conf/

3.「Security Solution 2003」

会　期：2003年10/22(水)～24(金)
主　催：日経BP社
会　場：東京ビッグサイト
　　http://expo.nikkeibp.co.jp/secu-ex/

4.「Security Tech Update／Tokyo 2003」

会　期：2003年11/11(火)～12(水)
主　催：株式会社IDGジャパン
会　場：東京国際フォーラム
　　http://www.idg.co.jp/expo/nws/

3. JNSA年間活動（2003年度）

4月 3日	第1回政策部会
4月18日	第1回幹事会
4月23日	理事会（九段会館）
4月24日	第1回西日本支部主催セキュリティセミナー
5月 8日	技術部会
5月21日	定期総会（スクワール麹町）
5月21日	臨時理事会（スクワール麹町）
5月22-24日	白浜シンポジウム後援
5月17日	第2回政策部会
5月28日	第2回幹事会
6月2-3日	RSA Conference 2003後援
6月2-3日	NSF2003 spring開催（東京国際フォーラム）
6月 9日	第1回西日本支部会合
6月13-14日	セキュリティ監査WG合宿
	（晴海グランドホテル）
6月25日	第1回教育部会
7月2-4日	NetWorld+Interop 2003 Tokyo後援
7月 9日	第3回幹事会
7月16日	第3回政策部会
7月16-18日	Wireless Japan 2003 後援
8月20日	第2回西日本支部主催セキュリティセミナー
8月28日	第4回政策部会
8月28日	第4回幹事会
9月10日	セキュリティスタジアムセミナー（工学院）
9月24-25日	電子署名・認証フォーラム後援
10月22-24日	NSF2003開催（東京ビッグサイト）
10月～11月	全国情報セキュリティキャラバン実施
12月3日	Internet Week 2003参加

★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）

4. JNSA部会・WG　2003年度活動内容

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：山本匡氏/損保ジャパン・リスクマネジメント)

2001年、2002年と継続して、被害調査を行い、被害額算定モデルを提案してきた。

今年の活動においても、前年同様なアンケートやヒヤリングによる被害調査を行い、算出モデルの精緻化を行うと共に、これらの被害の定量化について手がかりを掴みたい。

主な活動内容としては、下記の通り。

・2002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

【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する。

【個人情報保護ガイドライン作成WG】

(リーダー：佐藤憲一氏/大塚商会)

JNSAで個人情報保護ガイドラインを作成し、会員企業はもとより、広く市場に公開・流布することにより、企業の個人情報の取扱いに関する意識向上、各種セキュリティ対策の実施を促す。

企業における個人情報の保護対策を実施、運用する場合の標準的ガイドラインを作成中で、2003年秋頃を目処に書籍を発行予定。

【セキュリティ監査WG】

(リーダー：朝賀康義氏/アイセス)

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。主な活動予定は下記の通り。

・地方自治体向け監査(管理)基準の策定
・監査人の質の向上のためのスキルマップ作成、教育内容の検討
・その他の業界向けの監査(管理)基準策定、研究

2. 技術部会

(部会長：佐藤友治氏/株式会社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：土屋茂樹氏/NTTデータ)

セキュリティポリシーの必要性は徐々に浸透しつつあるが、具体的に策定する場合、何を決めればよいのか、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議論しながら成果を公開していきたい。

過去3年間に作成したポリシーやスタンダードをベースにして、内容の精査、新たな情報の付加、ISMSv2との親和性を考慮しながら、より使いやすいサンプルを作成していく。

【LANセキュリティWG】

(リーダー：関義和氏/ディアイティ)

802.1Xセキュリティ技術を中心に無線LAN、認証スイッチなどLANレベルのセキュリティ普及させるための活動を行う

無線LANセキュリティの技術を追跡し新たな相互接続実験の企画を検討する認証スイッチ、認証VLANの接続実験の企画を検討する802.1Xのセキュリティ機構を構築するためのガイドラインやガイドブックの検討を行う。

【インターネットVPN-WG】

(リーダー：松島正明氏/新日鉄ソリューションズ)

Internet VPNを活用した、リモートアクセス環境の導入する際に検討すべき項目や、考慮点をまとめガイドラインを作成する。

Internet VPNで使用可能なプロトコルの調査の後、検証手順に基づき実機検証を実施、その結果をもとに企業ユーザー向けのInternet VPNを利用したリモートアクセス環境導入のガイドラインを作成する。

【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）
インターネット上に存在する様々なコンテントに関して、その流通と蓄積の方法は様々である。しかし、その流通・蓄積される過程において、コンテント自身が製作者、著作者の意図に反した用いられ方、取得のされ方が行われる場合がある。これに意図しないコンテントの流通および取得に関して、技術的な立場に立ち、現在どのようなことが可能であるかを把握する調査を行い、最終的にコンテンツセキュリティに関する技術動向レポートを作成したい。

【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。

【PKI相互運用技術WG】
（リーダー：松本泰氏/セコム）
PKIの相互運用技術の問題を解決することによりPKIのアプリケーションの開発、PKIを使用したSIなどを促進する
Challenge PKI 2001, Challenge PKI 2002などの成果を元にIETFのRFCを作成する。その他、PKI相互運用実験を検討中

【技術用語WG】
（リーダー：佐藤慶浩氏/日本ヒューレット・パッカード）
ネットワークセキュリティに関する用語の定義はあいまいな場合があり、用語の認識の違いにより、情報に誤解を生む可能性がある。本WGでは、用語の定義と解説を作成し、また、技術文書作成にあたっての英訳語集も作成することによって、用語による混乱を軽減させる。
2002年度の活動において目標が達成できていない項目を継続して実施し、用語集のWebでの公開を目指す。

【情報セキュリティ標準調査WG】
（リーダー：佐藤慶浩氏/日本ヒューレット・パッカード）
技術用語WGにて、各種標準での用語が不統一であることや、認定制度自体が不明瞭であることに問題意識を持ち、認定制度そのものに焦点を置いた調査を目的としたWGである。
調査対象：ISO15408, 17799, ISMS, SSE-CMM
前期に作成した標準一覧表を、外部向け成果物作成を前提とするかを決定する。また、表の項目や表現方法を改善する。その後、表に調査結果を記入して完成させ、標準一覧のWebで公開を目指す。

【ハニーポットWG】
（リーダー：園田道夫氏/アイ・ティ・フロンティア）
年度前半は攻撃観測の拠点を構築して、実際に観察し、年度後半には構築方法や観測運営方法、観測結果について報告する。

【データストレージ＆セキュリティWG】
（リーダー：内田昌宏氏/ネットマークス）
企業がデータの運用および保存を行う際に指標となるような管理ポリシーの作成を目指す。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）
暗号管理策として暗号使用ポリシーテンプレートの策定に向けた勉強会から、テンプレート作成までを行なう予定。

【電子署名検討WG】
（リーダー：磐城 洋介氏/NTTコムウェア）
電子署名法の施行以来、様々な電子署名システムが検討／構築されているが、現状では様々な問題／課題に直面しており方式やビジネスモデルの見直しなど利便性やコスト面におけるマイナスイメージが指摘される。これらの問題をもたらした原因を洗いだし、電子署名に関する世間の認知や正しい理解を促すと共に、申請・決済・稟議・契約などの適用モデル毎に必要とされる要素の検討及び最終的な実装モデルを「ガイドライン」として公開することで、健全な電子社会の発展に貢献することを目的とする。

●勉強会目的のWG

【IRT研究WG】
（リーダー：武智洋氏/横河電機）
IRTに関する日本国内外の情報交換を行い、今後考えるべき問題などについてざっくばらんな議論を行う。NIRTや企業内、業界内IRTなどを始め、国際連携など

についても、議論できる「場」を作る。WGでの議論を元に、一般への情報公開として、勉強会や報告会などを行うことも課題としたい。

【セキュアOSとその活用方法研究WG】
（リーダー：佐藤慶浩氏/日本ヒューレット・パッカード）
Trusted OSなどのOSのセキュリティ機能を強化したセキュアOSについての勉強と、それを活用するための方法を調査、啓発するためのWG。初期の2ヶ月程度で勉強をして、WG参加の初心者と経験者の足並みを揃え、その後、OSの活用方法や、そのためのミドルウエアの利用方法なども勉強した上で、それらを啓発する活動を行なう。

---

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）
10月～11月に行なう全国セキュリティ啓発キャラバンの企画検討を行なう。キャラバン開催地の選定や、使用するCD-ROMと冊子のコンテンツ作成、検討、実際の運営の協力など。

【セキュリティスタジアム企画運営WG】
（リーダー：園田道夫氏/アイ・ティ・フロンティア）
来春予定されている、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」の企画と運営のためのWGで、セキュリティスタジアムの準備、募集、調達等含めた設営と、ターゲットサーバー構築などを行なう予定。また、一連のセキュリティスタジアムセミナーの企画・運営を行なう。

---

4. 教育部会
（部会長：佐々木　良一氏）
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：松田　剛氏/ヒューコム）
ネットワークセキュリティ技術者を育成するために、関係するスキルのリストアップと、個々の職種・職務によって必要とされるスキルを対応させ、セキュリティ技術者が必要とするスキルの鳥瞰図を作ることを目的とする。
今年度は、経済産業省による「高度IT人材育成システム開発事業」の「ケースメソッドによるセキュリティスキルアップ教育」のプロジェクト実施が確定している。

【ITSS実証実験評価 WG】
ITSS実証実験の教育効果の測定評価を目的としていて、その成果を今後のセキュリティ技術者の評価基準策定にも利用できることを目指して発足。

---

5. 西日本支部
（支部長：井上陽一/ヒューコム）
JNSAでなくては提供できない質の高いサービスを一丸となって提供していく。
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。

5. 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 取締役
経営戦略担当

副会長　大和　敏彦
シスコシステムズ株式会社
CTOアライアンス＆テクノロジー本部長

理　事(50音順)

TIS株式会社
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

テクマトリックス株式会社
浦山　清治

ソフトバンクBB株式会社
岡村　靖

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

株式会社ネットマークス
亀井　陽一

トレンドマイクロ株式会社
小屋　晋吾

日本ヒューレット･パッカード株式会社
佐藤　慶浩

株式会社ディアイティ
下村　正洋

新日鉄ソリューションズ株式会社
杉田　寛治

ELNISテクノロジーズ株式会社
鈴木　伸秀

エントラストジャパン株式会社
鈴木　優一

横河電機株式会社
武智　洋

日本ネットワークアソシエイツ株式会社
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

株式会社NTTデータ
中村　逸一

システムニーズ株式会社
中山　恵介

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

株式会社東芝e－ソリューション社
坂内　明

株式会社フォーバルクリエーティブ
早水　潔

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

6. 会員企業一覧

(2003年7月9日現在　169社　50音順)

【あ】
(株)アークン
RSAセキュリティ(株)
(株)アイセス
(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
(株)アクセンス・テクノロジー
朝日監査法人
アマノ(株)
(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
(株)イーツ
伊藤忠テクノサイエンス(株)
学校法人 岩崎学園
(有)インターネット応用技術研究所
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)栄光
(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)
エントラストジャパン(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】
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S.I.(株)
(株)ギガプライズ
(株)クインランド
クオリティ(株) *New*
(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
コベルコシステム(株)
コンピュータ・アソシエイツ(株) *New*

【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
シーティーシーエスピー (株)
(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)
ジェイフォン(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
シャープシステムプロダクト(株)
Japan Cyber Security Institute
(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)
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) *New*
セコムトラストネット(株)
(株)セゾン情報システムズ
(株)セラク
セントラル・コンピュータ・サービス(株) *New*
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)
中央青山監査法人
(株)ディアイティ
TIS(株)
(株)TBCソリューションズ
テクマトリックス(株)
デジボックス(株)
(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)
(株)東芝　e-ソリューション社
東芝情報システム(株)
(株)東陽テクニカ
凸版印刷(株) New
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　ｼｽﾃﾑｽﾞｴﾝｼﾞﾆｱﾘﾝｸﾞ(株)
日本エフ・セキュア(株)
(株)日本高信頼システム研究所
日本コムシス(株)　IT事業本部
(株)日本システムディベロップメント
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
日本ネットワークアソシエイツ(株)
日本ビジネスコンピューター(株)
日本ヒューレット・パッカード(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)
ノキア・ジャパン(株)
ノベル(株)

【は】
(株)ハイエレコン
(株)ヒューコム
(株)ビー・エス・ピー
(株)PFU
(株)日立システムアンドサービス New
(株)日立製作所 New
日立ソフトウェアエンジニアリング(株)
東日本電信電話(株)
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)
(株)富士通ソーシアルサイエンスラボラトリ
富士通エフ・アイ・ピー(株)
(株)富士通ビジネスシステム
(株)フューチャーイン
(株)プラーナ
(株)ブライセン
古河電気工業(株)
(株)プロティビティ

【ま】
マイクロソフト(株)
松下電工(株)
丸文(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)
三菱電線工業(株)
(株)メトロ

【や】
ユーディテック・ジャパン(株)
横河電機(株)

【ら】
(株)ラック
レインボー・テクノロジーズ(株)

【わ】
ワイ・エー・ピー・ホールディングス(株)

【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 New

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

編集後記

長い長い梅雨が終わったと思ったら、いよいよ夏本番の到来、と思いきや今年は天候不順の夏の到来で、今年の寒い夏休みに「夏休みを返して！」と思っている人も多いことでしょう。

今回のJNSA Pressでは、新しくJNSA顧問になられた佐々木良一先生にご挨拶の文章をお願いし、また特集記事には活動報告を発表したばかりの２つのWGに執筆をお願いしました。

さらに、今年度の新たな活動も次々と始まっていて、事務局の方がJNSAの活動についていくのがやっとの状態です。

昨年の11月に事務局は従来の場所から隣のビルに移転して、独立の事務所を構えるようになりました。２年目からはずっと３名体制でやってきましたが、６月からはプロジェクトに伴い増員をし、現在は短期の出向者も含めて６名となっています。ところが、机はもともと４台しかなく、１台を増やし、それでも足りなくて、１人は決まった机が無く、空いている席で仕事をするというような悲しい状況になっています。

そんな中でも、私たちは仲良く和気あいあいと楽しく仕事をしています。（と思っています。。。）

10月には主催イベントNSF2003と、全国情報セキュリティ啓発キャラバンがいよいよ始まります。お近くでのキャラバン開催の折りには、ぜひともご参加ください。楽しいノベルティグッズとCD-ROMと共にお待ちしています。

（事務局）

NPO日本ネットワークセキュリティ協会会員 行動指針

NPO日本ネットワークセキュリティ協会は、ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術および情報セキュリティへの脅威に関する情報提供などを行うことで、情報化社会へ貢献することを目的としております。

そのため、以下の通り会員の行動指針を定め、規範とするよう努めます。

会員は、この指針の遵守に努め、会の目的を共有するにふさわしい姿を目指しま

1. 自ら情報セキュリティポリシーを定め、他の手本となるような運用に努めます。
2. お客様の情報などの重要情報に関して、その取扱い手続きを明確にし、管理するように努めます。
3. 自ら取り扱う製品およびサービスについて、その情報セキュリティレベルの維持・向上に努めます。
4. 自ら公開するインターネットサイトおよびメール等のサーバ類について、その情報セキュリティレベルの維持・向上に努めます。
5. 情報セキュリティに関連する法規・法令等を遵守します。
6. 自らの構成員に対して、情報セキュリティポリシー及びその実施手順について教育・訓練を繰返し実施することに努めます。
7. クラッキングなどの不正行為を許さず、その撲滅に努めます

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