JNSA Press

Japan Network Security Association

Vol.23
August 2008

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

セキュリティインシデント対応で考えること

株式会社ラック サイバーリスク総合研究所 取締役所長
JNSA 理事　西本 逸郎

2005年から被害が目立つようになった金銭目的の犯罪は、2008年に入りさらに増加している。起こってはならないことではあるが、ある面、増えているということはそれだけ実社会においてITの利用･活用が推進しているという証左だと思う。例として、ネット活用を徹底的に行い、事業を推進している通販関係のインシデント対応で感じたことを書いてみたい。

1．経営者次第

経営者の視点が重要だ。事態を軽く考えたい意識が働く方もいるが、多くの経営者は、利用者や取引先は大変重要な「財産」であり、それを守ることが第一義であり、生命線であると確信し、そのためにしっかりとした決断を下している。同時に、事業に対する思いやビジョンなどを熱く語る方も多い。苦しい中、さすがだと思う。一方、周りの支える方が、頭をたれてほとんど口を開かないことも、またよく見かける。これは、事件を起こしてしまったという責任感もあるのだろうが、そういう体質なのだろう。

2．がんばるシステム管理者

年商10億以上くらいになると、システムやセキュリティに関しても少しは手を打てると思うが、それ以下では正直辛い。大手の中でも「うまくプログラムを書ける」レベルの自社要員やソフトハウスなど頼っていることは多い。そういう人たちは経営者が推進したいビジネスを一所懸命プログラムで実現している。それだけ機動性も高くコストもかからないため、ビジネスモデルが良ければ、成功していく。素晴らしいと思う。しかし、残念なことにネットワーク、データベース、セキュリティといった基盤技術を持っていないか、あるいは知らないため、インシデントにつながっている。企業がある程度成長すると、継続成長の為にIT戦略とそれを支える基盤技術が必須となるが、そういった人材や機会にめぐり合えるのは経営者の運かもしれない。

結局、経営者のビジョンを支えるIT戦略立案と推進を図れる人材の確保が重要であるが、圧倒的に少ない。そのためには、セキュリティのプロを養成するだけではなく「うまくプログラムを書ける人」にセキュリティを理解してもらうことが、第一歩のように思う。

私たちが提供する、様々なセキュリティサービスやソリューションが本当に社会に根付いていくため、また、今後の高度IT依存社会を勝ち抜いていくためにも、経営者を支える「セキュリティが分かる人材」の確保が重要であり、費用対効果も高い策であると信じる。

JNSAの技術者集団でのボランティア（若しくは原価）ベースで、このような企業をインキュベーションしていく活動や、セキュリティ技術者以外にセキュリティ技術を導入していくような活動など、私たちが対応すべき課題はまだまだ多い。

情報セキュリティ市場調査結果の概要
～日本の情報セキュリティ市場の規模と姿を概観する～

市場調査WGリーダ 勝見　勉

はじめに

JNSA政策部会のセキュリティ市場調査ワーキンググループ(WG)では、この程2007年度の国内情報セキュリティ市場調査結果を取りまとめた。この調査は同年度の経済産業省委託事業の一環として実施したもので、2008年7月4日に経済産業省より公表された。
(経済産業省　商務情報政策局　情報セキュリティ政策室：「平成１９年度情報セキュリティ市場調査報告書の公表について」2008年７月４日 http://www.meti.go.jp/policy/netsecurity/h19fy_marketresearch.html)

当WGでは、2004年度以来、国内の情報セキュリティ市場について、その規模の算定と現状の概観のとりまとめを行っている。ここでは、過去の調査経緯にも触れながら、経済産業省発表の平成19年度報告書に基づき、その内容のポイントをピックアップしつつ、現状の日本における情報セキュリティ市場の実態の一端をご紹介したい。

1. 2006年度における国内情報セキュリティ市場規模

今回調査の基準年度とした2006年度の国内情報セキュリティ市場規模の推定実績値は、表1に示すように、「情報セキュリティツール」が2,875億円、「情報セキュリティサービス」が3,012億円(同9.5%)で、合計5,887億円となった。その前年の2005年度には各々が2,387億円、2,752億円で、合計5,139億円と推定される。2005年度に初めて5,000億円の大台に乗ったものと見られる市場は、2006年度には15%弱の高い伸びを示して、6,000億円に近い規模に達したと推測している。

ではこの市場規模は、IT全体の市場に対してどの程度の比率を占めるものなのか。社団法人電子情報技術産業協会(JEITA)の調査報告「2005年度ソフトウェア及びソリューションサービス市場規模調査結果」※1によれば、2005年度のソフトウェア及びサービスの売上高は5兆3,069億円(うちSI開発2兆5,663億円、ソフトウェア6,855億円、アウトソーシング・その他サービス2兆551億円)である。また、同報告が参考として示しているハードウェアの出荷額は、合計で2兆6,524億円(うちメインフレーム1,933億円、サーバ6,584億円、ワークステーション530億円、パソコン1兆7,477億円)となっており、合計すると7兆9,593億円に達する。

情報セキュリティの市場規模は、IT市場の中では「ソフトウェア」または「サーバ」の市場規模にほぼ匹敵し、パソコン市場の約３分の１に相当する規模となっていると言える。IT市場全体に対する比率という視点では、情報セキュリティの5,139億円は、ソフト・ハード・SI合計約8兆円の約6.5%に相当する。ここ数年行われている内外の各種調査から、一般にITセキュリティ投資はIT投資全体に対して数パーセント(調査により概ね1%から7%程度の範囲にばらつく)を占めるものと見られているが、本調査をJEITAの数字と比較する限りでは、この一般に言われている範囲の上端に近いところに該当するという結果となった。

※1 社団法人電子情報技術産業協会・ソリューションサービス事業委員会「2005年度ソフトウェアおよびソリューションサービス市場規模調査結果について」平成18年9月28日 http://it.jeita.or.jp/statistics/soft_sol/h17/index.html

表１　国内情報セキュリティ市場規模　実績と予測

（金額：百万円、成長率：対前年比増加率）

国内情報セキュリティ市場推計		平成17（2005）年度（推定実績）		平成18（2006）年度（推定実績）			平成19（2007）年度（実績見込）			平成20（2008）年度（予測）		
		金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
情報セキュリティ市場合計		513,899	100.0%	588,726	100.0%	14.6%	656,152	100.0%	11.5%	693,831	100.0%	5.7%
情報セキュリティツール合計		238,677	46.4%	287,503	48.8%	20.5%	323,315	49.3%	12.5%	345,299	49.8%	6.8%
	統合型アプライアンス	9,823	4.1%	14,479	5.0%	47.4%	18,590	5.7%	28.4%	20,713	6.0%	11.4%
	アクセス制御製品	44,967	18.8%	48,033	16.7%	6.8%	49,758	15.4%	3.6%	51,168	14.8%	2.8%
	セキュアコンテンツ管理製品	98,214	41.1%	114,657	39.9%	16.7%	123,905	38.3%	8.1%	126,651	36.7%	2.2%
	アクセス管理製品	39,022	16.3%	46,706	16.2%	19.7%	52,325	16.2%	12.0%	57,420	16.6%	9.7%
	システムセキュリティ管理製品	27,525	11.5%	38,375	13.3%	39.4%	45,259	14.0%	17.9%	49,827	14.4%	10.1%
	暗号製品	19,126	8.0%	25,254	8.8%	32.0%	33,479	10.4%	32.6%	39,521	11.4%	18.0%
	合計	238,677	100.0%	287,503	100.0%	20.5%	323,315	100.0%	12.5%	345,299	100.0%	6.8%
情報セキュリティサービス合計		275,212	53.6%	301,223	51.2%	9.5%	332,837	50.7%	10.5%	348,532	50.2%	4.7%
	セキュリティコンサルテーション	54,701	19.9%	63,485	21.1%	16.1%	72,218	21.7%	13.8%	77,413	22.2%	7.2%
	セキュアシステム構築サービス	143,494	52.1%	142,397	47.3%	-0.8%	145,394	43.7%	2.1%	140,781	40.42%	-3.2%
	セキュリティ運用・管理サービス	60,633	22.0%	71,946	23.9%	18.7%	86,267	25.9%	19.9%	96,800	27.8%	12.2%
	セキュリティ教育	12,374	4.5%	16,331	5.4%	32.0%	20,480	6.1%	25.4%	24,046	6.9%	17.4%
	情報セキュリティ保険	4,010	1.5%	7,064	2.3%	76.2%	8,477	2.5%	20.0%	9,491	2.7%	12.0%
	合計	275,212	100.0%	301,233	100.0%	9.5%	332,837	100.0%	10.5%	348,532	100.0%	4.7%

［出典：経済産業省「平成１９年度情報セキュリティ市場調査報告書」、以下図表全て同じ］

2. 市場の分類と、区分別の市場規模

当調査では、市場を大きく「情報セキュリティツール」と「情報セキュリティサービス」に区分し、各々を、主として機能の違いに着目して、更に大分類レベル、中分類レベルに区分している。各市場区分の定義は、表2のようになる。詳細は報告書を参照されたい。

表2　国内情報セキュリティ市場分類

セキュリティツール	統合型アプライアンス	FW、IDS、ウイルス対策等複数機能を持ったアプライアンス
	アクセス制御製品	FW、IDS/IPS、VPN、アプリケーションファイアウォール
	セキュアコンテンツ管理製品	アンチウイルス、URLフィルタ、メールフィルタ等
	アクセス管理製品	認証、ログオン管理・アクセス許可、PKI製品
	システムセキュリティ管理製品	セキュリティ情報統合管理、ポリシー・アクティビティ管理ツール、脆弱性検査ツール　等
	暗号製品	暗号化製品、暗号モジュール
セキュリティサービス	セキュリティコンサルテーション	ポリシー構築、監査・診断等セキュリティ管理全般コンサルティング　　企画認証取得支援サービス
	セキュアシステム構築サービス	ITセキュリティの設計、導入、製品選定等支援 等
	セキュリティ運用・管理サービス	ITセキュリティの監視、運用支援、脆弱性検査、事案対応支援等のサービス、電子認証サービス、情報提供サービス 等
	セキュリティ教育	教育実施、コンテンツ提供、教育ASP、資格認定　等
	情報セキュリティ保険	情報セキュリティおよびITセキュリティ保険

2-1. 情報セキュリティツール市場

図1に2006年度における国内情報セキュリティツール市場の区分別分布を示す。

全体の約4割を占める「セキュアコンテンツ管理」は比較的古くから導入の進んだウイルス対策製品中心の市場で、セキュリティ製品では唯一消費者市場での浸透も進み、大規模な市場を形成している。これに次ぐのがファイアウォールとIDS／IPSを中心とする「アクセス制御」であるが、普及度が高いことと「統合型アプライアンス」への移行とで市場は成熟している。その分、UTMとも呼ばれる「統合型アプライアンス」の成長が著しいが、価格低下も進行して市場規模は限定的である。

「アクセス管理」、「システムセキュリティ管理」ならびに「暗号製品」市場は成長率が高い。これは情報漏洩対策の本格化と、内部統制対応のために、データの保護のみならず、システムへのアクセス権管理やシステム上の利用態様管理を徹底させようとする動きの結果と見られる。

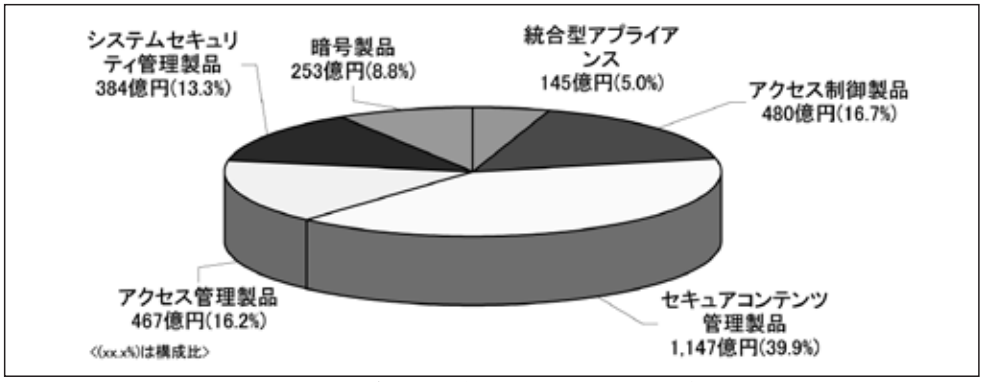


図1　2006年度の情報セキュリティツール市場

2-2. 情報セキュリティサービス市場

図2に2006年度における国内情報セキュリティサービス市場の区分別分布を示す。

全体の約半分を占める「セキュアシステム構築」はいわばセキュリティSIであり、システムにセキュリティを組み込む場合にほとんどのケースで必要になることから金額的には大規模である。しかし、SIにおけるセキュリティの「与件化」の結果、セキュリティ売上として数字が表に表れにくくなっており、市場の伸びは限定的となっている。従い、この市場に関しては、成長率の低さは必ずしも需要の停滞を意味しない。

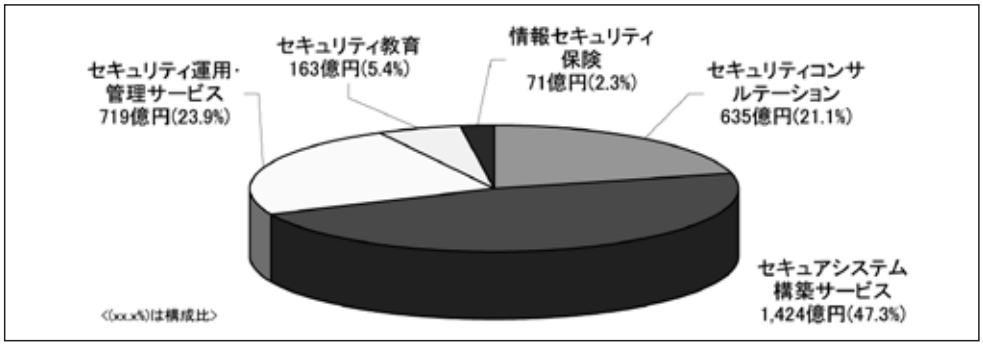


図2　2006年度の情報セキュリティサービス市場

これに次ぐ規模を持つのが「セキュリティ運用・管理サービス」であり、Webへの攻撃被害の増加に伴い脆弱性検査やインシデント対応サービスが伸びている。「セキュリティコンサルテーション」は個人情報保護対応や内部統制対応で伸びてきたが、2008年度は一服しそうである。市場規模は小さいが、「セキュリティ教育」は社員へのセキュリティ意識の徹底を目的とする需要が拡大している。

3. 国内情報セキュリティ市場の特性概要

上記で見てきた市場の特性の他に、全体を概観して次のようなことが指摘できる。

(1) 本調査期間の年平均成長率は10.5%と、最近の日本経済の成長率やIT産業出荷額の伸び率に比べても著しく高い伸び率を示しており、急速な拡大が続いている。

(2) 世界的にも市場の拡大速度は速いが、本調査対象期間のうち、海外と比較可能な2006年～2008年の間では、国内市場は世界全体、あるいは世界の各地域市場のどれよりも低い成長率を示すという結果になっている。

(3) アクセス制御製品やセキュアシステム構築サービス等の、市場規模も大きく普及度の高い製品やサービスが1桁台の成長に鈍化、またはマイナス成長となっている一方、システムセキュリティ管理製品、暗号製品、教育サービス等は2006年度には30%以上の極めて高い成長を見せており、カテゴリによって市場の成熟度と成長速度に大きな違いがある。

(4) 情報セキュリティ対策の重点が、ネットワークへの外部からの脅威に対する防衛から、内部からの情報漏洩･流出の未然防止や抑止にシフトしており、システムへのアクセスの管理やデータの暗号化、社員教育等への取組に力点が移っていると見られる。

(5) 情報漏洩対策やIT統制対応等組織内部に対する対策の需要が拡大するのに対応して、暗号製品、ログ取得や端末管理に関する製品分野では、国産ベンダの台頭が進んでいると見られる。ただし、市場の細分化とも関連して、市場セグメント毎の参入企業の数は必ずしも多くなく、個々の事業規模も限られていると見られる。

(6) このように、国内参入企業の事業基盤が万全でないことから、国内産業の存立基盤が十分とは言えず、産業育成策が課題となると思われる。特にITベンチャーからの参入に対しては、技術開発、市場開発、信用補完等の面での支援が必要と思われる。

[出典:前出資料より筆者抜粋･要約]

4. 世界の情報セキュリティ市場との比較

IDC社から提供を受けた世界市場のデータ(分類等で若干の差異あり)を用いて世界市場との比較を行った。図3に、アプライアンス、ソフトウェア、サービスの区分で集計した世界市場(IDC)と日本市場(JNSA)の市場推移グラフを示す。

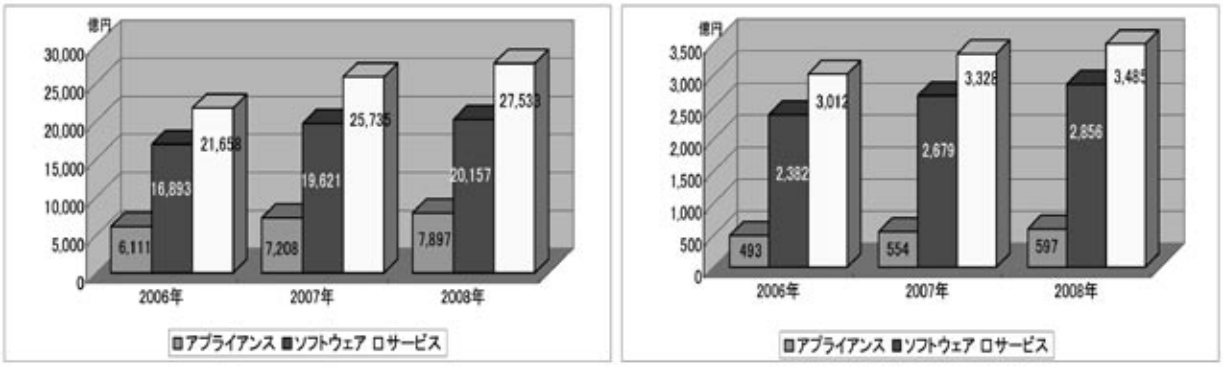


図3　世界と日本の情報セキュリティ市場推移

2006年度における日本市場の対世界シェアは、アプライアンス：8.1%・ソフトウェア：14.1%・サービス：13.9%・合計：13.2%であり、アプライアンスが極端に低い結果となっている。調査ベースの違いもあり一概に言えないが、日本は外部脅威より内部管理に重心が移ってきた結果かも知れない。

なお、参考までに2006年度における地域別のアプライアンス・ソフトウェア・サービスの構成比比較を図4に示す。北アメリカ市場が世界全体の構成比とほとんど同じ値を示す一方、日本市場が極端にアプライアンスの比率が低く、逆にアジア太平洋（日本を除く）は極端にアプライアンスの比率が高いという、興味ある対照を示している。

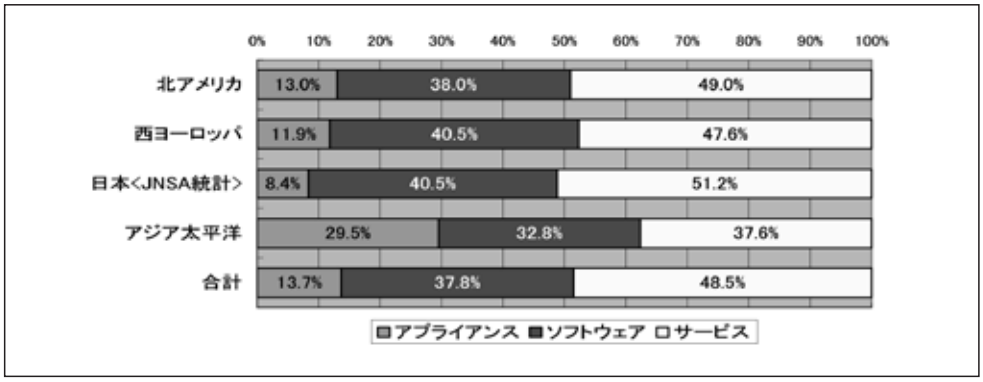


図4　2006年度地域別情報セキュリティ市場構成比

ちなみに、地域別市場規模金額は、北米：20,277億円、西欧：12,401億円、日本（当調査）：5,887億円、アジア太平洋：3,480億円である。

5. 市場のトピック

2007年度の市場調査では、市場金額の算出や市場区分ごとの動向、特徴点の抽出・分析の他に、市場の変化に影響を与えると考えられる様々な動きや事象を、各方面の研究成果も参照しつつ、トピックとして取り上げた。ここではその内容を紹介する紙数がないので項目のみをご紹介する。詳細は報告書本文を参照されたい。

(1) 外部からの攻撃の脅威
(2) 内部統制と情報セキュリティ
(3) 情報セキュリティ監査

(4) 情報セキュリティ対策におけるASP/SaaSの市場動向について
(5) 物理的セキュリティとの連携
(6) セキュリティ対策の実効性評価
(6)-1. PCI DSS
(6)-2. 情報セキュリティ格付け制度
(6)-3. ISO27004と日本ISMSユーザグループの活動
(6)-4. 情報処理推進機構の研究レポート
(6)-5. 電子商取引推進協議会によるセキュリティ対策評価モデル
(6)-6. 米国国立標準技術研究所(NIST)からのガイドライン(SP)

ポイントとしては、外部からの脅威が、「見えない化」「標的型攻撃」といった特徴を顕著にして悪質化すると同時に、経済的実被害を伴うことでより深刻度を増す一方、内部統制や情報セキュリティ監査といった管理面での対応が進化しだし、市場もそれを反映する変化を見せていること。セキュリティ対策の費用対効果や初期投資、また技術的専門性の点から今後ASP/SaaS型サービスが、特に中小企業での導入に際して有力な解となる期待があること。セキュリティ対策も構築・実装からその有効性・実効性評価にまで目が向いてきたこと、などを読み取っていただけると考える。

6. 今までの歴史と今後の展望

JNSAによる情報セキュリティ市場調査は、2004年度に自主企画としてユーザ実態調査を行い、同年度に経済産業省からの委託事業としてベンダ側の市場数値を推計算出する調査を実施した。2005年度にはベンダ側調査を前年度の外部委託から自力調査に切り替えて実施し、JNSAとしての方法論を確立することができた。
その後調査時期と対象年度の整合の見直し等もあり、2007年度には、「情報セキュリティガバナンス」の実施施策の一環として実施され、産業構造審議会における検討のための資料として活用される等、その位置づけは重みを増している。

2008年度も、前年度調査を踏襲した調査をJNSAで実施することが決定しており、今までの成果を踏まえてより充実した調査となるよう、ワーキンググループを挙げて取り組んで行きたいと思う。なお、WGメンバーは随時募集しているので、関心のある方は参加してご一緒に調査・分析に携わっていただければと思う。
本調査が、経済産業省の政策企画運営だけでなく、JNSA会員始め産学の各方面でも参考にされ活用いただければ幸いである。

最後に2007年度報告書の執筆メンバーを紹介して本項の締めくくりとしたい。(順不同、敬称略)

ワーキンググループリーダ	
勝見　勉(リコー・ヒューマン・クリエイツ株式会社)	
ワーキンググループメンバ(調査・執筆参加者)	
市川　順之(伊藤忠テクノソリューションズ株式会社)	塩見　友規(オー・エイ・エス株式会社)
花水　剛(キヤノンマーケティングジャパン株式会社)	風間　勇人(サイバーエリアリサーチ株式会社)
森田　弥生(新日本監査法人)	秋山　卓司(日本クロストラスト株式会社)
長谷川長一(株式会社ラック)	光野　元彦(パスロジ株式会社)
佐藤　友治(株式会社ブロードバンドセキュリティ)	
オブザーバ	
瀬田　陽介(国際マネジメントシステム認証機構株式会社)	

Challenge PKI プロジェクト発 PKI 相互運用の国際標準

セコム株式会社 IS 研究所　島岡 政基

1. Challenge PKI プロジェクト発 PKI 相互運用の国際標準

PKI相互運用技術WGのChallenge PKIプロジェクト（以下、本プロジェクト）[1]では、2001年からPKIの相互運用性確保に向けて様々な取り組みを行ってきた。これらの取り組みから得られた相互運用性確保に関連する知見を国際的にフィードバックするため、IETF（Internet Engineering Task Force）に対して「マルチドメインPKIの相互運用性に関するメモ」（以下、本提案）として提案を行い、2008年7月にRFC 5217 “Memorandum for Multi-Domain PKI Interoperability”[2]として公開された。今回は本プロジェクトがIETFでどのように標準化を進めてきたか、これまでの経緯を振り返りながら説明する。

2. Challenge PKI と IETF との関わり

2001年から活動を始めた本プロジェクトは、PKIの相互運用性確保に必要な様々な知見が、国際的に十分に共有されていないことを懸念してきた。特に、ポリシが異なるPKIドメイン同士が相互運用する場合は、技術仕様上の互換性だけではなく、例えばトラストアンカをどうするか、ドメイン同士で相互接続するのか、あるいはリライングパーティ毎に個々に他のPKIドメインを信頼するべきか、といった運用面での問題も合わせて解決していかなければならない。

本プロジェクトは初めに、こうした問題について2002年7月に横浜で開催された第54回IETF会合で、PKIX WGの有識者を交えて非公式BoF[3]を開催して議論を行った。その結果、こうしたマルチドメインPKIの相互運用性問題については国際的に知見を共有する必要があるという結論に至り、IETFに対して本プロジェクトから提案を行うことになった。

こうした経緯から、本プロジェクトでは、以降のIETF会合に継続的に参加して、1）PKI相互運用の動向について観察、2）標準化提案の進め方について調査・協議、3）標準化にあたっての支持者の獲得、4）実際の標準化提案、を行ってきた。

3. マルチドメイン PKI の相互運用問題

マルチドメインPKIの相互運用における最も重要な問題の一つとして、適切なマルチドメインPKIを設計するためのノウハウが十分に共有されていない、という問題が挙げられる。マルチドメインPKIを実現した例として、米国連邦政府のFederal PKIや、日本の電子政府認証基盤であるGPKIがあり、それぞれのフレームワークの中で相互運用性を確保する情報はある程度整備されているのだが、例えば誰かが大規模なPKIを設計する場合に、マルチドメインPKIで設計すべきかシングルドメインPKIで設計すべきか、またマルチドメインPKIだとしたらどのような信頼モデルを選ぶべきか、といった情報は世界的にもほとんど整備されていなかった。このため、今後出来上がるであろう様々なPKI、特に大規模PKIが十分な相互運用性を確保しないまま構築・運用される可能性が懸念されていた。

[1] http://www.jnsa.org/mpki/
[2] http://www.ietf.org/rfc/rfc5217.txt
[3] Birds of Feather の略。問題提起やブレインストーミングなど目的を厳密に定めない緩やかな会合を指す。

そこで、本提案では相互運用可能なマルチドメインPKIをできるだけ簡単に実現できるようにするために、以下の理解について世界中で共有すべく提案を行った。

表1　本提案の主な章構成

2. Public Key Infrastructure（PKI）Basics	
	PKIドメインの構成要素となる個々のPKIの関係について整理した。 特に信頼関係の観点から、認証局同士の信頼関係と、認証局と利用者（Relying-Party）との間の信頼関係は明確に分けて論述した。
3. PKI Domain	
	PKIドメインの定義と、PKIドメインを確立するための要件、PKIドメインモデル（PKIドメイン同士の信頼関係）について解説した。
4. Trust Models External to PKI Relationships	
	PKI同士の関係に依らない信頼モデルとして、認証局と利用者の信頼関係によって確立されるトラストリストモデルがある。これはPKIドメイン同士の信頼関係とは異なる性質のものであるため、あえて章を分けて記述した。 トラストリストの信頼モデルを分類するとともに、トラストリストによる信頼関係を築く際の考察を行った。

このように、マルチドメインPKIを設計するにあたって必要な知識を正しく共有し、マルチドメインPKIを構成する際の主な選択肢（PKIドメインモデル）を示すことによって、マルチドメインPKIの相互運用性を実現することを目指している。

4. IETF の標準化プロセス

IETFにおける標準化活動の多くは、IESG（Internet Engineering Steering Group）の下に設置された8つのArea（部会）と、各Areaの下の約120のWG[4]によって進められており、その標準化プロセスは図1のように定められている。各フェーズの左に示す期間は、各フェーズに要する期間の目安としてIESGが定めたもの[5]であり、実際にはこの他に各フェーズでの改訂作業期間や再レビューの期間などを考慮する必要がある。

提案者は、最初に提案内容をI-D（Internet-Draft）としてIETFに投稿し、標準化したい旨を適切なWGまたはAD（Area Director）に表明（Publication Request）する。この提案内容が、IETFのいずれかのWGの活動内容に合致する場合には、WG Draftとして当該WGの中で提案活動を進める。WG Draftは、WGレビューを受けて最終的にWG提案としての合意を得た（WG Last Call[6]を通過した）後、AD Evaluationのステップに進むことになる。

一方、いずれのWGの活動内容にも合致しない場合は、AD-Sponsored Draft（旧Individual Draft）つまりAD後援のもとでの個人提案として提案活動を進めていくことになる。Sponsoring ADは、提案内容に関連する有識者にExpert Reviewを依頼し、その結果を受けてAD Evaluationのステップに進むことになる。

その後IETF Last Call[7]を経て、IESG Evaluation（全ADによるレビューと投票）で承認されれば、あとはRFC-Editorによる編集上の校正と著者による最終確認（AUTH48[8]）を経て正式にRFCとして公開されることになる。なお、これらの標準化プロセスは、I-D Tracker[9]と呼ばれるWebサービスによって進捗管理されており、誰でも状況を確認することができる。

---

4 http://www.ietf.org/html.charters/wg-dir.html

5 http://www3.tools.ietf.org/group/iesg/trac/wiki/PublishPath

6 ○○ Last Call とは、○○における最終的なコメント受付期間を指す。ただし Last Call 期間中のコメント内容によっては期間を延長したり、コメントを受けて改訂した後に改めて再度 Last Call を行う場合もある。

7 基本的には WG Draft の場合は 2 週間、AD-Sponsored Draft の場合は 4 週間が Last Call 期間となる。

8 もともとは「著者による最終確認を 48 時間で済ませる」が語源だが、昨今ではしばしば延長されているのが実情である。

9 https://datatracker.ietf.org/idtracker/

表 2　IETFの8つのArea

Abbrev.	Area
APP	Application Area
INT	Internet Area
OPS	Operations & Management Area
RAI	Real-Time Applications & Infrastructure Area
RTG	Routing Area
SEC	Security Area
TSV	Transport Area
GEN	General Area

図 1　IETFの標準化プロセス

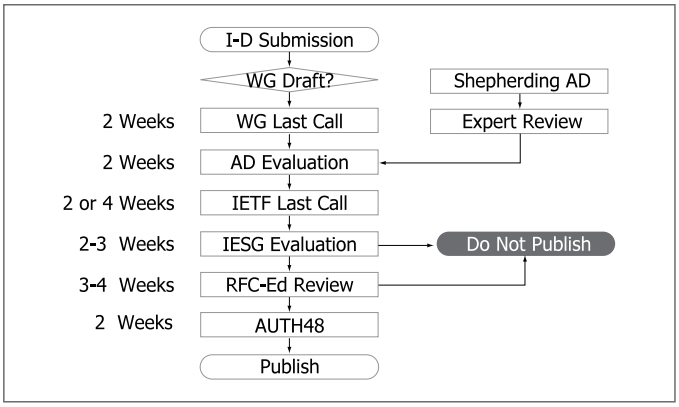
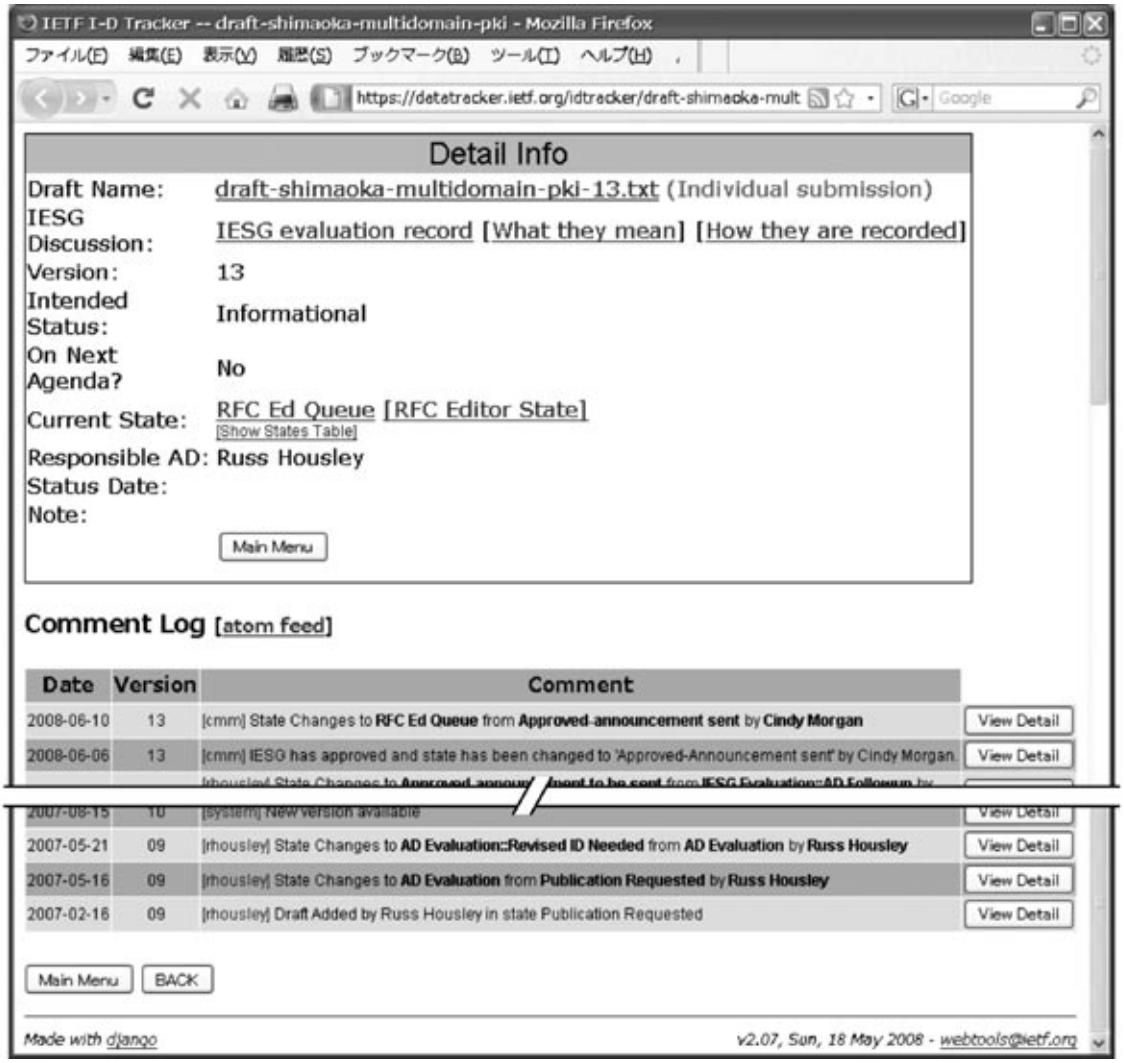


図 2　I-D Trackerによる進捗管理



5. NIST とのコラボレーション

PKIや暗号技術の分野において、米NIST（National Institute of Standards and Technology）/CSD（Computer Security Division）[10]は非常に大きな影響力を発揮してきた。NISTは、暗号鍵管理装置のセキュリティ要件を定めたFIPS140-2をはじめとする様々な米連邦政府の暗号製品調達基準の策定や、SHA-1やRSA1024bitの暗号アルゴリズムの移行指針を示したSP800-57をはじめとするSP800シリーズ文書の公開を行うとともに、実運用が行われている数少ないマルチドメインPKI環境である米Federal PKIの設計・構築に早くから携わっている。こうした経験や実績から、NISTはIETFにおいてもPKIX WGやS/MIME WGでの標準仕様策定で中心的役割を担っており、NISTのマルチドメインPKIに関する実績はIETFに限らず世界的にも広く認知されている。

そこで本プロジェクトがIETFでの提案を円滑に進めるにあたっては、NISTの支援を得ることが重要であると考え、キーパーソンとして当時PKIX WG co-chairを務めていたTim Polk氏（NIST）と、横浜のIETF会合以降も継続して提案の進め方について協議を重ねてきた。また、本プロジェクトを立ち上げ当初から支持いただいている宮川寧夫氏（IPAセキュリティセンター）の仲介により、Polk氏の同僚でありFederal PKIの設計にも携わってきたNelson Hastings氏（NIST）を、2004年9月から共著者として迎え入れることができた。更に2006年1月には、Hastings氏の紹介により、やはりFederal PKIやDoD PKIの設計に携わってきたRebecca Nielsen女史（Booz Allen Hamilton社）が共著者として名乗り出てくれたため、最終的には筆者を含めた3名で提案文書の執筆を進めることになった。

6. IETF における標準化

前述の第54回IETF会合での非公式BoFの結果を受けて、著者は本プロジェクトが持つ知見をまとめた内容をI-D初版として2003年7月にIETFへ投稿し、翌8月のオーストリア・ウィーンで開催された第57回IETF会合では、PKIX WGにて本提案の内容について発表を行った。当時PKIX WG co-chairのPolk氏は、当初このI-DをWG Draftとすることで合意してくれていたが、PKIX WGは当時WG Draftを非常に多く抱えており、WG Draft削減の見直しを図るようIESGに求められていたこと、またWGメンバから本提案が技術仕様の策定ではなく運用要件に主眼をおいたものであるというコメントを受けた経緯もあり、WG DraftではなくIndividual Draft（後にAD-Sponsored Draft）として提案を進めることになった。

その後、PKI相互運用技術WG内部でもレビューと改訂を重ねながら、2004年9月にHastings氏、2006年1月にはNielsen女史を共著者に加えたこともあり、2007年2月に、共著者らが従事してきたFederal PKIやDoD（米国防総省）PKIの知見を包括した大幅改訂を完了させた。

この間、並行してIETF会合ではPolk氏をはじめ、もう一人のPKIX WG co-chairであるStephen Kent氏（BBN社）や、当時のSecurity ADでありPKIX WGだけでも16本ものRFC文書を執筆したRuss Housley氏（Vigil Security社）、PKIX WGに限らずIETFの様々なAreaで幅広く活躍しているPaul Hoffman氏（VPN Consortium）らと標準化の進め方についても継続的に協議を進めてきた。実はこの頃のIETFはまだIndividual Draftの標準化プロセスにおいてAD Sponsoringの考え方が不明瞭だったため、筆者も具体的なアクションがわからずに迷走気味だった。偶然にも本I-Dの大幅改訂を終えた2007年春に、Individual Draftの標準化プロセスを明瞭にする2本の文書[11, 12]が発行された。これに伴い筆者は直ちに、Housley氏にSponsoring ADとなっ

[10] http://csrc.nist.gov/
[11] RFC 4858 “Document Shepherding from Working Group Last Call to Publication”
[12] IETF Operational Notes: “Guidance on Area Director Sponsoring of Documents”、http://www.ietf.org/IESG/content/ions/ion-ad-sponsoring.html

てもらうことを依頼し、これまでの経緯からすぐに快諾してもらうことができた。

その後は、Housley氏自身と氏が指名したPolk氏によるExpert Reviewを受け、IETF Last Call、IESG Evaluation、RFC Editor Reviewと順調に進んだわけだが、実はHousley氏にSponsoring ADを依頼した直後に、Security ADだったHousley氏がIETF Chairに昇任、Expert Reviewをする予定だったPolk氏もまたSecurity ADに昇任するという、筆者らにとってはまさにサプライズ人事があった。このため、本提案は光栄にもIETF Chair Sponsored（?）Draftとして、またSecurity ADによるExpert Reviewを伴って標準化を進めていくことができた。AD Sponsored Draftとなってから極めて順調にプロセスが進んだ背景には、こうしたIETFにおけるキーパーソンのポジションの変化が一つの要因としてあったようにも思える。また、PKIX WGの中心として活躍してきたHousley氏、Polk氏がIETFの中でステップアップしたという事実は、IETFの今後の流れがPKI技術をはじめとするセキュリティ技術へと少しずつ潮目が変わり始める兆しなのではないだろうか。

7. 標準化から学んだこと

こうしてIETFを通じて得られた様々な人脈や知見、特に一般的なWG Draftという形ではなく完全に個人の提案としてRFCを発信したことから得られた知見は実に貴重なものだが、今後IETFの標準技術に関わる方々に対して、またIETFに限らず国際標準化や世界的な合意形成を目指す方々にも有効と思われるいくつかの情報を述べておきたい。

7-1. RFCを読む全ての人たちへ

まず、標準化活動までは携わらないかもしれないが、IETFの標準技術を勉強したり調査したりする人たちにとって有益な情報を紹介する。

(1) RFC Reading Tools (http://tools.ietf.org/inventory/reading-tools)

本来テキストファイルであるRFCをタグ付き文書で読むことができるツールが提供されており、ページや章節、参考文献などがハイパーリンク化されている他、改訂版や旧版の有無、元のI-Dへのリンクや、各文書との差分表示など、非常に使い勝手がよい。

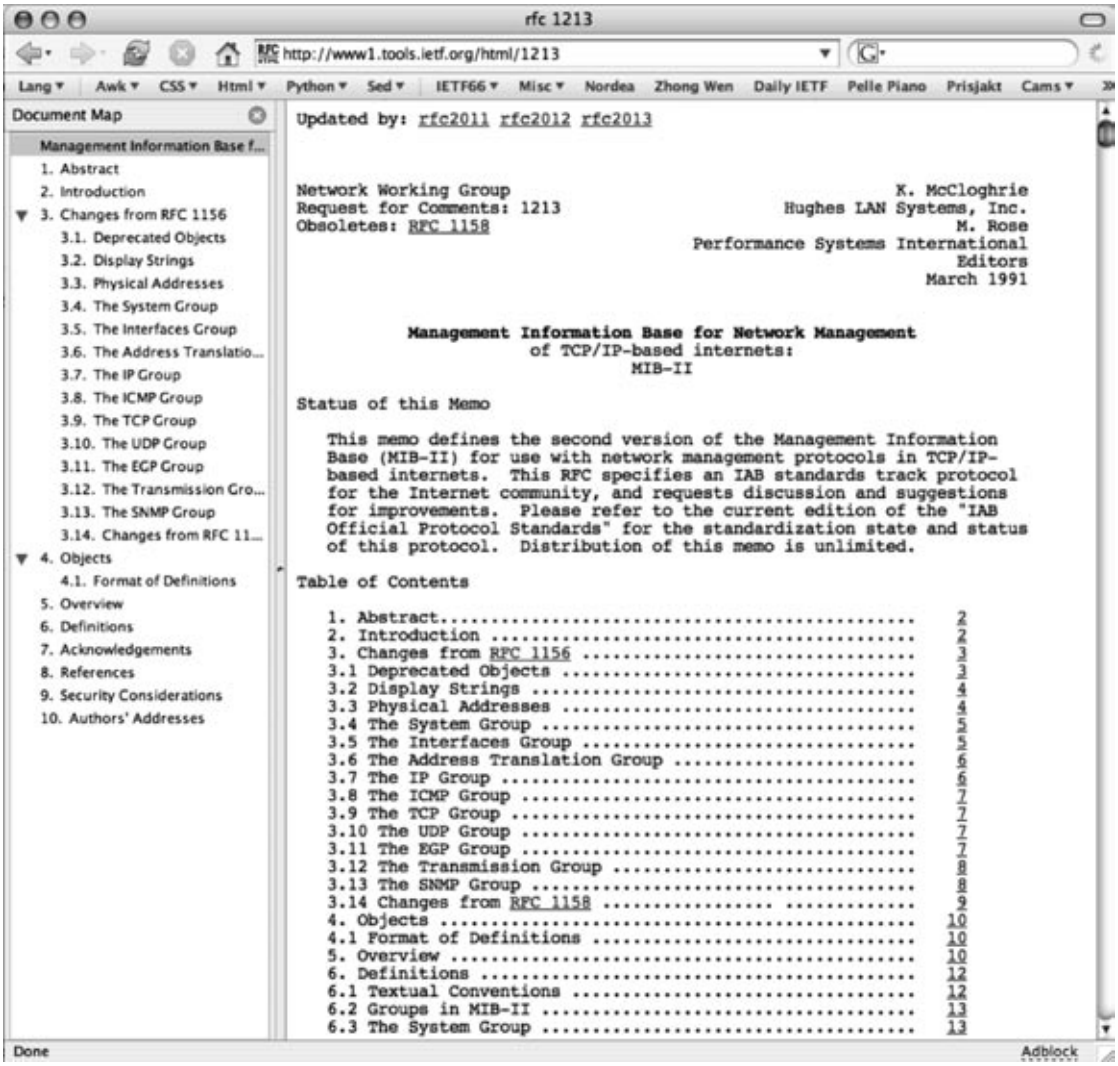
オンラインで利用するWebサービス[13]や、オフラインで利用可能なqRFCviewの他、Firefoxの拡張機能として利用可能なDocument Map[14]も提供されている。

その他、インターネット上に公開されているRFC文書を取得するコマンドラインツール(RFC util)も提供されている。こちらはキーワードや正規表現検索も可能なので、自分に必要なRFCを簡単に確認・取得することができる。

[13] http://tools.ietf.org/html/

[14] 本原稿執筆時点では、残念ながらまだ Firefox 3.0 には対応してなかった。

図3　HTMLized RFCs with Document Map



(2) Unofficial Repository (http://www.potaroo.net/ietf/)

公開されたRFCや最新のI-DはIETFリポジトリからも取得できるが、旧版のI-Dや期限切れI-D[15]はIETFリポジトリから取得することができない。この非公式サイトでは、過去のI-Dの履歴を(ほとんど)全てアーカイブしているだけでなく、前後の版との差分も表示してくれるので、各RFCが議論されてきた経緯や変遷などを調査する場合には非常に便利である。

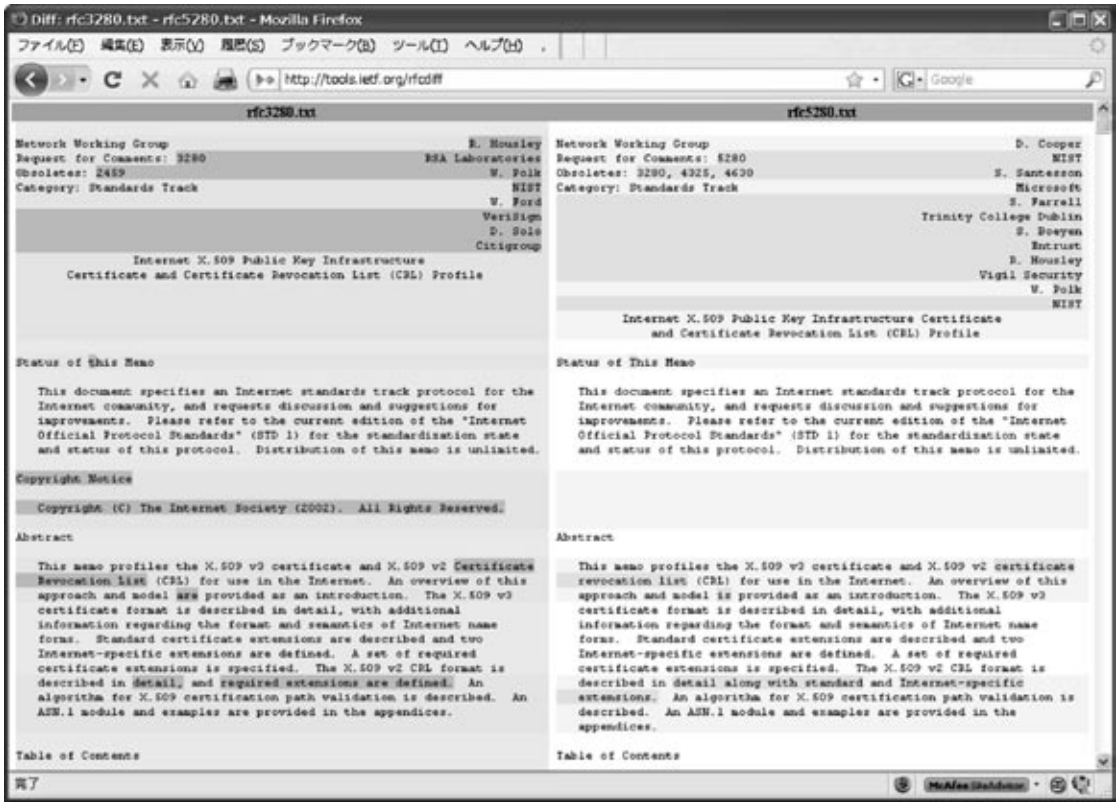
(3) Rfcdiff Tool (http://tools.ietf.org/tools/rfcdiff/)

前述のリポジトリでも使われている、RFC文書形式のテキストファイルの差分を表示するツールが提供され

[15] I-D の有効期間は原則として 6 カ月であり、期限内に更新されないと IETF リポジトリから削除される（厳密には「期限切れとなった」旨のメッセージで上書きされる）。

ている。コマンドラインから利用するものだけでなく、Webサービスとしても提供されているので、わざわざ比較文書をダウンロードしなくても確認できるのは非常にありがたい。差分表示の形式は何種類か定義されており、選択することができる。

図 4　RFCdiff Web Serviceの表示例（Side-by-side diff）



(4) Pre-formatted bibligraphic entries for RFCs　(ftp://ftp.rfc-editor.org/in-notes/rfc-ref.txt)

RFC文書のReferencesに記載されている形式のテキストデータが提供されている。RFC文書を参考文献として記述したい場合に便利である。

7-2. IETFで標準化活動に関わる人たちへ

次に、IETF中心ではあるものの、他の標準化団体も含めて国際標準化や世界的な合意形成を目指す方々に役立つであろう情報を紹介する。

(1) Educational Materials（http://tools.ietf.org/group/edu/）

ここには、IETFで標準化を進める上で有益となる様々な教材が公開されている。これらは主にIETF会合初日のトレーニングセッションで用いられる資料である。

① IETF Structure and Internet Standards Process
（http://www.ietf.org/proceedings/07dec/slides/newcomer-0/70newcomers.ppt）

IETFの組織概要や標準化プロセスの概説と、各組織が標準化においてどのような役割を持つのか、また知的財産権の扱いなどを解説している。

② RFC Editor Tutorial（ftp://ftp.rfc-editor.org/in-notes/rfc-editor/tutorial71.pdf）
RFCの種類や標準化プロセスの紹介、I-Dの書き方などを解説している。I-Dを書き始める人たち、あるいは既に書き始めた人でも是非一度はこれに目を通して欲しい。

③ Introduction to WG Leadership
（http://www.ietf.org/proceedings/07jul/slides/leadership-0.pdf）
WG設立の手順やWG運営に関する解説であり、一般には関係なさそうだが、WG chairがどのような方針に基づいて判断を行うのか、を理解しておくことはWG内での標準化を進める上で有益な情報源になると考えられる。

(2) xml2rfc（http://xml.resource.org/, http://tools.ietf.org/tools/templates/）

以前はI-Dはnroffというマクロ言語で書く必要があったが、最近はXMLベースが主流となってきている[16]。このページでは、XMLファイルからRFCフォーマットのテキストファイルを生成するxml2rfcというツールとその関連情報が公開されている。XMLファイルとすることで、nroffでは自動化できなかった参考文献や図表へのクロスリファレンス、目次などの自動生成もできるようになった。

xml2rfcでは、RFCフォーマット以外にも”ページ制御なしRFCフォーマット”（Wordなどへコピペする時に便利）や、HTML形式での出力もできる。

(3) IESG Additional Materials（http://www.ietf.org/IESG/content/index.html）

これもWG運営同様で、I-Dを最終承認するIESGがどのような方針で判断を行うのか、を理解しておくことは最終承認を円滑に進める上で有益な情報源になると考えられる。
具体的には、以下の情報が参考になると考えられる。

- WG Document Shepherd writeup questions and template
- Document Shepherd template for individual submissions via AD

8. 最後に

本プロジェクトおよび本提案にご理解ご支援をいただいたPKI相互運用技術WGはじめJNSAメンバの皆様に改めて御礼申し上げます。また、長年の上司でもありPKI相互運用技術WGリーダでもある松本泰氏、IETF会合でPolk氏らとの協議をいつもサポートしてくださった富士ゼロックスの稲田龍氏、JPNICの木村泰司氏、JNSA事務局の安田直義氏にも心から感謝の意を表します。

[16] I-D を XML 形式で記述することは RFC 2629 および下記の URL で規定されている。
http://xml.resource.org/authoring/draft-mrose-writing-rfcs.html

JNSA ワーキンググループ紹介

情報セキュリティ関連パブコメ検討 WG の紹介

WG リーダー
株式会社ディアイティ　河野　省二

■ 情報セキュリティ業界の一員として

従来から JNSA では情報セキュリティ業界の団体として、またその一員としてパブリックコメントへの対応を促進してきました。しかしながら、その対象は経済産業省、総務省、警察庁などの一部の官公庁の政策にとどまっており、昨今の情報セキュリティニーズの広がりに対応するのが難しくなってきたのも現状です。

そこで、情報セキュリティに関する政策をウォッチし、必要に応じて勉強会を開催するためのグループとして、パブコメ検討 WG を発足しました。

情報セキュリティ業界の一員として、政策に興味を示し意見をあげていくだけではなく、JNSA が業界のリーダーシップをとり続けていくことも本 WG 発足の目的の一つです。

■ パブコメ検討 WG の活動

1. 情報セキュリティ関連政策の選択と報告

パブリックコメントが求められている政策は電子政府のホームページに一覧が掲載されています（http://search.e-gov.go.jp/servlet/Public）。この中から情報セキュリティや情報技術に関連する政策を取り出し、JNSA 会員向けに告知をします。

2. 情報セキュリティ関連政策の勉強会の開催

パブリックコメントが求められている政策において、特に検討を要するものについては、勉強会を開催します。

3. パブリックコメントの提出

勉強会を開催したものについては、JNSA パブコメ検討 WG としてパブリックコメントを提出します。

■ 勉強会の開催

パブコメ検討 WG の第一回勉強会として、2008 年 7 月 11 日に「次期情報セキュリティ基本計画に向けた第 1 次提言」をテーマに開催しました。

内閣官房情報セキュリティセンターの関参事官をお招きして、情報セキュリティ基本計画の概要や委員会での検討事項などをお話しいただき、資料からは読み取れない部分についても十分に理解できるものとなりました。

30 名ほどの参加者からは活発な意見や質問、また技術的な提案などもあり、本政策に関する理解をさらに深めることができたのではないかと感じました。また、勉強会の後には、パブリックコメントを作成するための討議も行い、WG メンバー以外の方からも多くの意見をいただく事ができました。

このような勉強会を繰り返していく事で、JNSA 会員の皆様に、政策が発表される前からその内容を十分に理解していただき、自らのビジネスに活用していただきたいと考えています。

■ 今後の予定

パブコメ検討 WG では政策に関する勉強会を開催するだけではなく、政策に関する様々な資料を一元的にご覧いただけるように、アーカイブズ WG との連携をしながら、多くの方に情報セキュリティ関連政策をご覧いただき、理解していただけるような場を提供していきたいと考えています。

情報セキュリティに関連する政策の流れなどをご覧いただく事で、より深い理解を得られるのではないかと期待しています。

JNSA ワーキンググループ紹介

情報セキュリティ教科書執筆者 WG のご紹介

WG リーダー
オー・エイ・エス株式会社　塩見　友規

■ WG 活動の目的

情報セキュリティ教科書執筆者 WG は、情報セキュリティのプロフェッショナルを目指そうという ICT 技術者向けの「教科書」を作成する事を目的としています。作成する「教科書」は、「セキュリティ知識分野作成（SecBok）WG」の策定している「情報セキュリティスキルマップ（セキュリティ知識分野）」の最新版と連携し、専門家としての初学者に知ってもらいたい内容を出来るだけ網羅する内容とします。

■ 教科書作成の経緯

同様のコンセプトを持った書籍として、佐々木良一先生監修の元、JNSA 教育部会の「スキルマップ作成 WG」が編著者となり、2005 年 4 月に秀和システムより「情報セキュリティプロフェッショナル総合教科書」が出版されました。当時はネットワーク、サーバ、通信など個々の情報セキュリティ技術に関する書籍や、セキュリティマネジメントに関する書籍は数多く出版されていましたが、技術からマネジメント、法律までを体系的に学習出来る書籍は少なく、特に初級者から中級者向けの書籍は出版されておらず、広範囲に渡るセキュリティ技術・知識を包括して得る事が出来る場も少ない事などから、広範囲に渡る分野の知識を体系的に学習する事が出来るとして、出版後も高い評価を頂く事が出来ました。

しかし、技術の発展や情勢の変化に伴い、情報セキュリティ分野においても、マルウェアの複雑化や SQL インジェクションによる被害拡大、脅威の多様化や攻撃手法の複雑化・高度化による脅威の見えない化など、近年著しく脅威の傾向にも変化が生じて来ており、2005 年当時の情報のみでは現状にそぐわない状況になりつつあります。その為、最新の脅威の傾向及び対策を反映した新しい教科書を作成する事となりました。

■ 新版の作成に向けて

今回作成している「情報セキュリティのプロフェッショナル向け教科書」（書名未定）は、現在の情勢に合わせて新しい項目を追加するなど、内容については全面改訂に近いもので、書名等についても変更していく予定です。また、数多くの著名な執筆者の方々にご協力頂いている事もありますので、内容については社内教育や大学・専門学校などの公的機関での教育にも活用出来るよう充実したものを目指して参ります。情報セキュリティ技術者の人材育成に貢献出来るような書籍を皆様のお手元にお届け出来るように鋭意邁進する所存ですので、ご期待下さい。

■ 活動の予定

- '08/ 秋頃～「情報セキュリティのプロフェッショナル向け教科書」（書名未定）出版

会員企業ご紹介㉓

株式会社アルファシステムズ

http://www.alpha.co.jp/

株式会社アルファシステムズは、ソフトウェアの受託開発をコアビジネスとし、創業以来35年以上システム開発に関わってきました。特に基幹系通信システムでは多くの実績を上げており、お客様から高い評価を頂いています。

ソフトウェアの受託開発は、お客様のオフィスに常駐する場合が多々あります。そのほとんどが首都圏ですが、管理職については勤怠管理等の社内業務に関してその都度自社へ戻っており、かねてからその非効率性について指摘する声がありました。

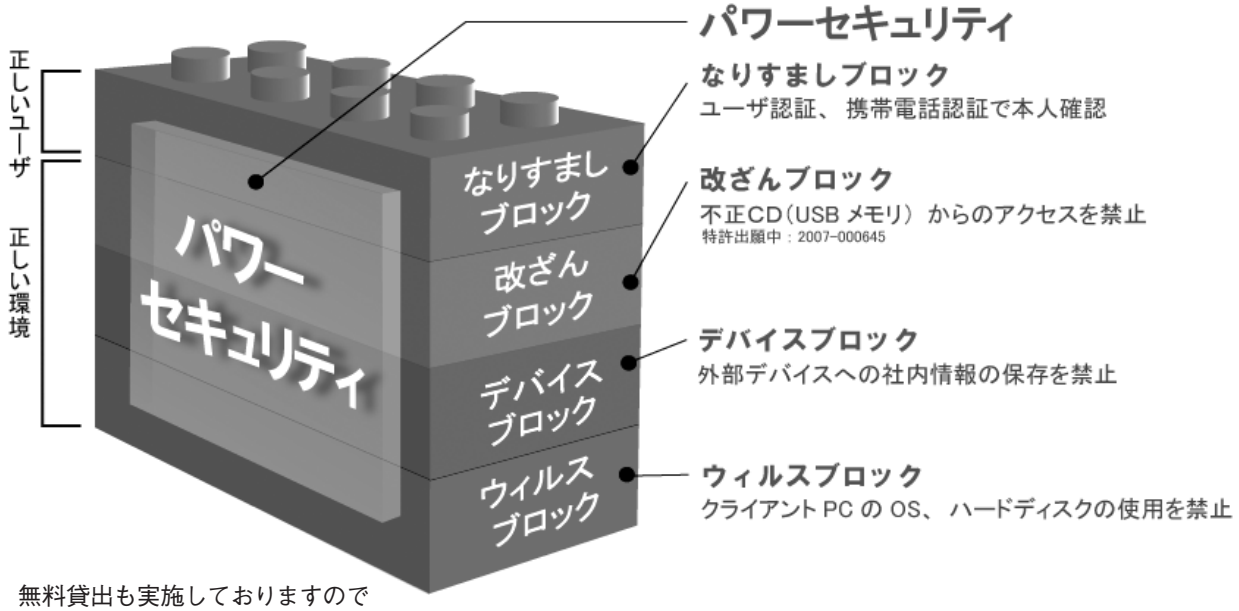
この問題を解消すべく、これまでのソフトウェア開発で培ってきたノウハウを活かし、研究開発部門・情報システム部門・情報セキュリティ部門が協力し、堅牢強固なリモートアクセスシステムの開発、およびテレワークの導入をすすめました。現在では、社内運用だけでなく、情報漏えい防止製品としてお客様へご提供しております。

■情報漏えい対策ならリモートアクセスソフトウェア「alpha Teleworker」！

alpha Teleworkerは、社外から「安全」「手軽」に社内ネットワークへ接続できるリモートアクセスソフトウェアです。

画面転送型のシンクライアント方式であるため、クライアントPCに社内の情報を一切保存できません。さらに、専用のCD（またはUSBメモリ）をPCで起動させるだけで接続環境が整うため、安全・手軽にリモートアクセス環境を実現することができます。

■強力なセキュリティ対策を実現 ～パワーセキュリティ～



無料貸出も実施しておりますのでお気軽にお問い合せください。

お問い合わせ先

http://www.alpha.co.jp/teleworker/

株式会社アルファシステムズ　製品販売本部 アルファテレワーカー係

〒150-0002 東京都渋谷区渋谷二丁目17番5号 シオノギ渋谷ビル12階

TEL：03-3498-5166　E-Mail：teleworker@alpha.co.jp

兼松エレクトロニクス株式会社

http://www.kel.co.jp/

KEL
KANEMATSU ELECTRONICS LTD.

兼松エレクトロニクスは、ストレージ、ネットワークなど、様々な環境においてお客様の情報セキュリティの維持管理のサービスレベル向上に取り組んでいます。個人情報保護法に続いて内部統制のためのJ-SOX法など、各企業では次々と新たな法規制への対応を迫られています。兼松エレクトロニクスは、これらのお客さま方のセキュリティ・レベルを強化するために、データ暗号化、システムのログ管理などの情報セキュリティのトータル・ソリューションをご提供します。

■ テープ暗号化アプライアンス“Eclipz”

Eclipzは、メインフレームに接続されているテープ装置の前に設置するだけで容易に、しかもメインフレームの負荷を意識することなくテープの暗号化を実現できます。現在使用されているほとんどのテープ装置には暗号化機能はないため、テープの暗号化を行うためには、システム環境を最新の環境にするとともに新たに暗号化機能を持ったテープ装置を導入するなど、多くの手間と費用が必要になります。Eclipzはこれらのユーザー負担を極力抑えて容易にテープ媒体のセキュリティを向上します。個人情報保護法の施行により、外部保管を行うデータには暗号化が望まれています。Eclipzは、現状のシステム資源を生かしたままで強固な暗号化を実現する唯一のソリューションです。

■ システム機器のパッチ対応をネットワークレベルで実現する仮想パッチソリューション“IBM Proventia Network IPS”

IBM Proventia Network IPSは、独自のVirtual Patch®技術によってシステム機器の脆弱部分に対する攻撃を即座に検知します。セキュリティ研究開発チーム“X-Force”からアップデートされるセキュリティシグニチャ“X-Press Update”が、サーバーやシステムに仮想的にパッチを適用した状態を作り出し、脆弱部分を防御してウィルスや不正アクセスなどをネットワーク上で阻止します。

重要なシステムほどすぐにパッチを適用できないのが現状ですが、IBM Proventia®がパッチマネージメントをより効率的に行い不正攻撃を防御します。セキュリティホールの発生や新種のウイルス、ワームに即座に対応し、セキュリティ作業の利便性を上げて低コスト化を実現します。

兼松エレクトロニクスでは、セキュリティ診断サービスから運用サービスまで、お客様のネットワークセキュリティを統合的に実現するトータルソリューションを提供します。

■ 企業のIT戦略に重要なシステム全体のログを有効活用する統合ログ管理アプライアンス“LogLogic”

LogLogicは、ネットワーク機器、サーバー、データベース、アプリケーションまでのログデータを集中管理、リアルタイム解析、高速検索、レポーティング、長期保存までのログライフサイクルマネージメントを行う統合ログ管理システムを、導入やメンテナンスが容易なアプライアンス製品として提供します。システム全体のログを有効活用することで、許可されていないアクティビティや不正トラフィックをリアルタイムに検出し、複雑で高度化しているサイバー攻撃検知等のセキュリティ対策や、個人情報保護法、業界で注目されているPCI-DSSへの対応、システム全体で記録されたログデータのモニタリング実施による監査対応、財務報告書の完全性を証明するといった内部統制対策を実現します。

お問い合わせ先
兼松エレクトロニクス株式会社
〒104-8338　東京都中央区京橋 2-17-5
http://www.kel.co.jp/

富士通関西中部ネットテック株式会社

http://jp.fijitsu.com./kcn/

FUJITSU
THE POSSIBILITIES ARE INFINITE

先端テクノロジーで、セキュアなユビキタス社会の未来を拓きます。

富士通関西中部ネットテック株式会社は、これまで培ってきた最先端の通信/IP/モバイルネットワークシステムおよび防災・安全・安心分野の開発ノウハウと、企業や官庁・自治体向けのソリューション業務の経験を活かし、あらゆるものが、いつでも、どこでも、誰とでも、安心してつながるセキュアなユビキタス社会の実現に向けて取り組んでいます。

ソリューション業務

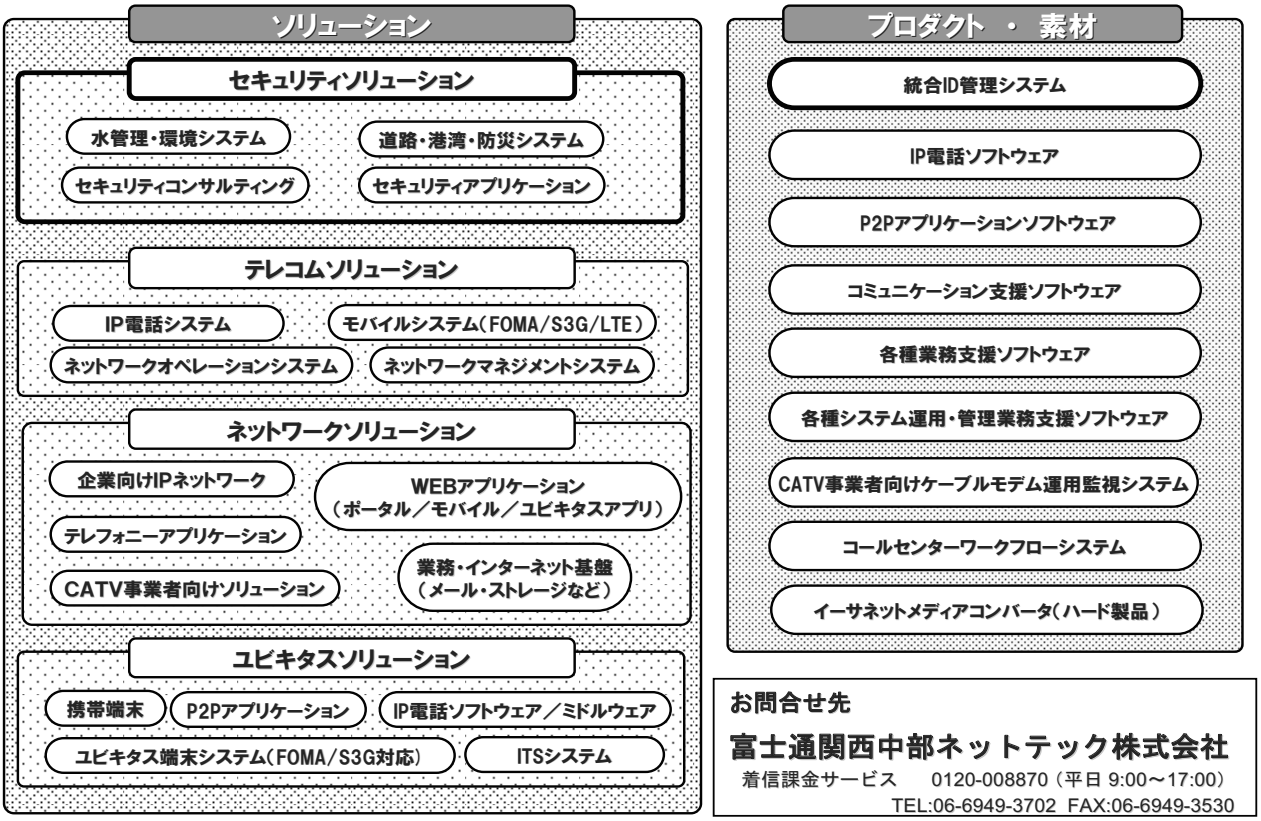
長年培った情報通信システムの開発技術をベースに、コンサルティングから設計、構築、運用、およびユーザアプリケーション開発を、セキュリティソリューションをはじめとして、お客様のニーズに応える様々なソリューションを提供しています。

IP電話サービスソフトウェア、アプリケーションシステム、およびミドルウェア開発

キャリアやISPでIP電話サービスを実現する高信頼サーバソフトウェア、パソコンやPDA搭載用IP電話ソフトウェアおよびネットワークの効率的な運用のためのネットワークマネジメントシステム、およびJavaアプリシステム等の効率的な開発を実現する通信用ミドルウェアの開発を進めています。

モバイル・ユビキタスネットワークシステム、アプライアンスの開発

W-CDMA(FOMA)方式および次世代モバイルネットワークシステム、ユビキタスネットワークシステムを構成する基幹系システムおよび各種アプライアンスのソフトウェア開発およびハードウェアの設計に取り組んでいます。



お問合せ先
富士通関西中部ネットテック株式会社
着信課金サービス　0120-008870（平日 9:00～17:00）
TEL:06-6949-3702 FAX:06-6949-3530

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■

○スパム対策のパイオニア『IronPort Cシリーズ』

ジェイズ・コミュニケーションが取り扱っているスパム対策アプライアンス『IronPort Cシリーズ』はIPレピュテーション、Domain Key、VOF（Virus Outbreak Filters：ウィルス拡散防止フィルター）、コンテンツフィルターなど、最新のテクノロジーを駆使し、企業の電子メールシステムを保護。不要なメールは事前にブロックします！

【製品情報詳細】
http://jscom.jp/products/ironport

◆お問い合わせ先◆
ジェイズ・コミュニケーション株式会社
担当：東日本営業部　吉岡
TEL: 03-6222-5858　FAX:03-6222-5855
E-mail: yoshioka@jscom.co.jp

○IP Geolocationデータベース「SURFPOINT v2.0」

IP Geolocationデータベースは、IPアドレスに位置情報や接続環境を結びつけたデータベースです。
2008年9月1日「SURFPOINT v2.0」が新登場！
日本国内利用の全IPアドレスを収録。市区町村の位置判定が可能に。
アクセスユーザの国内外判定、国内での位置判定によって
- ●ネットバンク等のアカウント作成/ログイン時の国内外チェックや不正検出
- ●デジタルコンテンツ配信における配信地域管理

などが可能に！

【製品情報詳細】
http://www.arearesearch.co.jp/ip/sp_v2.html

◆お問い合わせ先◆
サイバーエリアリサーチ株式会社　IP事業部　担当：中西
E-mail: info@arearesearch.co.jp
TEL: 03-3243-1070（東京支社）　055-991-5544（本社）

○InterSafe CATS(インターセーフキャッツ)

持ち出しPC、サテライトオフィスなど社内ネットワークに接続できない環境でもWebフィルタリングの一元管理を実現し、情報漏洩を防止します。
インターネット上で各種設定を行うため、サーバが不要でポリシーを自動的に反映することが可能で、導入・運用が簡単です。Winnyなど指定したプログラムの起動を制限する機能も装備。データベースは携帯電話5キャリアのフィルタリングに採用されるなど高い精度が評価されています。

【製品情報詳細】
http://www.alsi.co.jp/security/iscats/index.html

◆お問い合わせ先◆
アルプスシステムインテグレーション株式会社
TEL: 03-5499-1331
E-mail: ssg@alsi.co.jp

■サービス情報■

○マネージドセキュリティサービス

企業のネットワークセキュリティ対策を「初期費用」と「月額料金」で実現します。
ファイアウォール、IDS&ADS等の不正アクセス対策から、VPN、回線／機器の冗長化、サーバ負荷分散、ウィルス／Winny／迷惑メール対策、URLフィルタに至るまで、お客様の個別ニーズに合わせた機能をご選択頂けます。
対策に必要な、機器のレンタル、導入、運用・監視、24時間365日緊急対応等をサービスに含み、国内2,600以上の拠点へのサービス提供をしています。

【サービス情報詳細】
http://www.variosecure.net/service/index.html

◆お問い合わせ先◆
バリオセキュア・ネットワークス株式会社
TEL: 03-5733-6314
E-mail: sales@variosecure.net

JNSA 2007 年度ワーキンググループ活動報告会

JNSAの活動報告会は、今までも総会とあわせて開催してきましたが、今年は活動報告だけではなく、特に効果的な成果が出たワーキンググループの活動を中心にして、色々な課題や今後の方向性、他の活動との関連性などを探る内容としました。JNSAの活動を通して、情報セキュリティに関連する問題点を浮き彫りにし、これからの活動テーマについて情報共有を行いたいという意図がありました。この狙いは、ある程度成功したように思いますが、内容が盛りだくさんになってしまい、2部屋に渡って並行開催しましたが、休憩時間が合わなかったり、時間が押してお昼休みが短くなってしまうなどの課題もありました。各ワーキンググループの活動内容に基づいたセミナーやディスカッションは、別途独立して開催していきますので、併せてご参加いただければと思います。

■ 日時：2008年6月13日(金)9：30〜15：30
■ 場所：ベルサール八重洲 3 F

報告会は、25ページのプログラムのように2セッションパラレルで開催されました。

Room1では、JNSAの中に新しく設立された教育事業者連絡会(ISEPA)と教育部会、ユーザ部会のBoF、それと政策部会のBoFが開催されました。より広いRoom2+3では、政策部会と西日本支部のBoF、それとこの日に設立された日本セキュリティオペレーション事業者協議会(ISOG-J)、技術部会を主体とした報告と議論、そしてU40部会の報告がされました。

以下、部会ごとに各々で議論された内容をごく簡単にご紹介しておきます。

Room1

◆9:30−11:20 教育事業者連絡会(ISEPA)

「人材育成マップとキャリアパスの現状と今後について」と題し、(ISC)2の衣川氏がモデレータ役を勤めて、パネラー各氏のキャリアを中心に議論が進められました。キャリアパスの事例として各氏は文科系、理科系の転職経験者としての経験談が紹介され、議論が進められました。同じ会社でキャリアを積むには、スペシャリスト的な能力とジェネラリスト的な能力が求められると思われるのと、セキュリティについての専門家としての評価は現在もされていないし、成果物が見えにくいので今後も難しいのではないか、という議論がされました。

情報セキュリティについては、空気や水と同じで、あって当たり前、止まってしまうと責任を押し付けられ易いという点が大きな問題であり、先進性やチャレンジ性を評価できるようにしなくてはならないのではないかという意見が紹介されました。特に全体像や情報セキュリティの内容が見えていないのではないか、という議論がされていました。

◆11:20−12:00 教育部会

「教育部会の目指すもの」というテーマで、ITの教育を取り巻く状況や問題について問題提起とそれに対応した教育部会の活動内容と方向性が簡単に紹介されました。

2つ目に「情報セキュリティ教育の基礎情報と拡散への試行」というテーマで、SecBok-WGとセキュリティ講師スキル研究WGの過去からの活動を集大成し、新たなステップを実現するための企画が説明されました。T-1グランプリやスタープロジェクト等の内容と計画が解説され、参加者の協力をお願いしたい、という依頼がされていました。

3つ目にセキュリティリテラシーベンチマーク作成WGから、理解度チェックの2種のベンチマークとそこで最近追加された管理機能等について説明がされました。今年度からは経済産業省の委託が終了しJNSA独自で継続することになったので、名称やアイコンも変更し、更に柔軟な機能追加と運用を行

うことを考えていることが説明されました。

◆12:30－14:00　ユーザ部会BoF

企業内の非IT部門などのユーザを対象としたユーザ部会がいよいよ発足しました。どのような点に悩んでいるのか、どのようになれば良いのかなどを会場の参加者とディスカッションしながら、情報セキュリティモラルの向上などについて、今後の部会の歩む方向性を確認する議論が行われました。

◆14:00－15:30　政策部会BoF

JNSA会員限定で「情報セキュリティ対策の評価について」というテーマで、評価や監査の実際や手法についてのざっくばらんな議論が行われました。事故が起こった時の事前対策の評価なども話題として挙げられ、何らかのガイドラインが欲しいというような意見も出ていました。特に結論は出さず、これからもその時々の状況を共有するためのディスカッションを行いたいということでお開きになりました。

Room2+3

◆9:30－10:55　政策部会

3つのテーマで議論が行われました。最初は情報漏えいインシデントの調査結果を元にして、現実の対策の現状を探るものでした。情報漏えいの調査は引用件数がとても多い調査ですが、これからの調査の方向性の議論を行い、またこれまでの調査結果の編集データをCD－ROMで実費頒布しました。

2つ目は、経済産業省から委託されている情報セキュリティ分野の市場規模調査について、2005～2008年度の国内市場のデータを紹介すると共に、その海外市場との比較やトピックスが紹介されました。

3つ目は、新しい活動として動き出した、アイデンティティ管理や内部統制、J-SOX方関係の検討結果について議論されました。

◆11:00－12:30　西日本支部BoF

情報セキュリティについて、今までもアンケート調査などを行ってきていますが、自社の情報資産やリスク評価を行えばよいのか、JNSAが出来る貢献は何か、等々というテーマでディスカッションが行われました。

◆13:00－13:30　日本セキュリティオペレーション事業者協議会(ISOG-J)発足発表

この日(6/13)に発足が発表されたISOG-Jについて、その経緯や構成、活動内容について解説されました。

◆13:30-14:30　技術部会

技術部会からは2つのテーマで議論が行われました。JNSAのWebサーバをセキュアOSに変更した再のエピソードがパネル形式で紹介されました。実際の情報を公開することは、今まで躊躇していた人のハードルを下げることにもなり、JNSAとしての意義もあるだろうと言うことで、TOMOYO Linuxを適用したそうです。結果は、思った以上に簡単で、実稼働状況のサーバを移行する際の問題も直ぐ解決できたそうです。

2つ目は、「安全なWebサイトの構築・運用」についてWebアプリケーションセキュリティWGで作成したケーススタディ方式のコンテンツについて紹介されました。成果は、セキュリティ製品バイヤーズガイドの解説記事として活用されています。

◆14:30-15:00　U40部会

昨年から活動を始めたUnder40部会の活動から、勉強会や実験ネットワークの内容について紹介されました。実験ネットワーク（LaboNet）はほぼ準備が整い、夏くらいには実働できる状態になるだろうとのことでした。勉強会の後などに懇親会を行っていて、平均10名前後が参加しているそうです。幹事会へもオブザーバ参加し、徐々に幹事会への参加も進め、JNSAの次世代を担えるような意識を持って活動をしているとのことでした。

Room 1	
教育事業者連絡会（ISEPA）（9：30 ― 11：20）	
110 分	**人財育成マップとキャリアパスの現状と今後について** (ISC)2 JAPAN 衣川俊章 氏 **パネルディスカッション** 「情報セキュリティのキャリアパス～現状と未来～」
教育部会（11：20 ― 12：00）	
5分	**教育部会の目指すもの** サイバー大学・JNSA 安田 直 氏
15 分	**SecBok WG・セキュリティ講師スキル研究WG** 長谷川長一 氏
20 分	**セキュリティリテラシーベンチマーク作成 WG** JMC リスクソリューションズ 大溝裕則 氏
12：00 ― 12：30 **昼　休　み**	
ユーザ部会 BoF（12：30 ― 14：00）	
90 分	**企業内ユーザの情報セキュリティモラル向上への課題** モデレータ：大塚商会 佐藤憲一 氏
政策部会 BoF（14：00 ― 15：30）※ JNSA 会員限定	
90 分	**情報セキュリティ対策の評価について** モデレータ：ラック 西本逸郎 氏

Room 2＋Room 3	
政策部会（9：30 ― 10：55）	
45 分	**セキュリティ被害調査 WG** NTT データ 大谷尚通 氏
20 分	**セキュリティ市場調査WG** リコー・ヒューマン・クリエイツ 勝見 勉 氏
20 分	**内部統制におけるアイデンティティ管理WG** グローバルセキュリティエキスパート 宮川晃一 氏
西日本支部 BoF（11：00 ― 12：30）	
90 分	**何故進まない中小企業における情報セキュリティ対策** **モデレータ：** 富士通関西中部ネットテック 嶋倉文裕 氏 **パネリスト：** 経済産業省 下田裕和 氏 IPA セキュリティセンター 石井 茂 氏 JNSA 西日本支部長 井上陽一 氏
12：30 ― 13：00 **昼　休　み**	
日本セキュリティオペレーション事業者協議会（ISOG-J）発足発表（13：00 ― 13：30）	
30 分	**日本セキュリティオペレーション事業者協議会（ISOG-J）発足について** ラック 武智 洋 氏
技術部会（13：30 ― 14：30）	
50 分	**セキュア OS 普及促進WG** JTS 澤田栄浩 氏
10 分	**Web アプリケーションセキュリティWG** アイアイジェイテクノロジー 加藤雅彦 氏
U 40 部会（14：30 ― 15：00）	
30 分	**Under 40 部会活動報告** アイアイジェイテクノロジー 加藤雅彦 氏


政策部会発表の様子


ユーザ部会 BoF の様子

2008年度
「インターネット安全教室」のお知らせ

～パソコンや携帯電話で思わぬトラブルや犯罪にまきこまれないために～

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、これらの被害を防ぐことはできません。

こうした状況をふまえ、経済産業省と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2003年度より開催しています。

2007年度は全国で130回の「インターネット安全教室」を開催、6835名の方々にご参加いただきました。昨今の携帯電話などによるネット利用の低年齢化や学校等での開催などを考慮し、昨年は「親子で守って安全・安心10か条」というリーフレットを作成しました。会場毎の受講者層の違いに対応できるよう、今年も副教材を充実させていきたいと考えています。

2008年度も全国各地の共催団体の方々のご協力を得て、引き続き開催してまいります。なお、現時点での開催状況は次頁のとおりです。

【開催概要】

[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、その他各開催地大学・新聞社・県・県警等（以上予定）

[開催一覧]（次頁）一覧をご覧下さい。（2008年7月24日現在）

開催状況については、随時更新しています。「インターネット安全教室」ホームページをご確認ください。
http://www.jnsa.org/caravan/

◆「インターネット安全教室」共催団体募集について◆

「インターネット安全教室」は、以下の地域で活動している共催団体を募集しております。

岩手県・埼玉県・高知県・鳥取県・福岡県・佐賀県

- 一般市民向けの情報セキュリティセミナーを実施したいがコンテンツがない
- 教材を製作するにもコストも手間もかかるのでなかなかできない
- セミナー運営のノウハウがない
- しかし、情報セキュリティは大切。普及活動を行わないといけないと思っている

とお考えの団体等におかれましては、是非とも「インターネット安全教室」の共同開催をご検討下さい。また、そのような団体をご存知の方は是非事務局までご紹介下さい。
詳しくは下記のお問い合わせ先までご連絡下さい。

【お問い合わせ先】

■NPO 日本ネットワークセキュリティ協会（JNSA）事務局
E-Mail：caravan-sec@jnsa.org

2008年度「インターネット安全教室」開催一覧

（2008年7月24日現在）

日　程	開催地	共催団体	会　場
6月7日（土）	富山	株式会社富山県総合情報センター	富山市立鵜坂公民館　会議室
6月7日（土）	愛媛	愛媛県 IT 推進協会	アイテムえひめ 愛媛国際貿易センター
6月7日（土）	鹿児島	NPO 法人鹿児島インファーメーション	鹿児島市消費生活センター研修室
6月17日（火）	岐阜（新規）	高山市立国府中学校	国府中学校　体育館
6月21日（土）	北海道	国立大学法人北見工業大学	北見工業大学総合研究棟 2 階多目的講義室
6月24日（火）	鹿児島	NPO 法人鹿児島インファーメーション	鹿児島市消費生活センター研修室
6月30日（月）	富山	株式会社富山県総合情報センター	富山市総曲輪公民館
7月5日（土）	群馬	NPO おおた IT 市民ネットワーク	宝泉行政センター　多目的ホール
7月5日（土）	神奈川	NPO 情報セキュリティフォーラム（NPO-ISEF）	綾瀬市立中央公民館　3 階　講堂
7月7日（月）	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山南警察署
7月8日（火）	群馬	NPO 法人おおた IT 市民ネットワーク	錦打中学校　体育館
7月11日（金）	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山市立福南中学校
7月12日（土）	沖縄（新規）	NPO 法人フロム沖縄推進機構	沖縄コンベンションセンター　会議場 A1
7月12日（土）	神奈川	NPO 情報セキュリティフォーラム（NPO-ISEF）	アートフォーラムあさみ野　セミナールーム
7月17日（木）	大阪	NPO 法人きんきうぇぶ	河内長野市立小山田小学校
7月29日（火）	神奈川	NPO 情報セキュリティフォーラム（NPO-ISEF）	伊勢原市商工会館　4 階　中会議室
7月30日（水）	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山市立光南台中学校図書館
8月6日（水）	山形	山形大学学術情報基盤センター	山形大学小白川キャンパス学術基盤センター
8月20日（水）	大阪	GIS 総合研究所	堺女性大学
8月22日（金）	長野	上田市マルチメディア情報センター	上田市・東築地公民館
8月22日（金）	神奈川	NPO 情報セキュリティフォーラム	逗子市役所 5 階 第 7・8 会議室
8月25日（月）	鹿児島	NPO 法人鹿児島インファーメーション	奄美情報処理専門学校
8月27日（水）	東京	NPO 情報セキュリティフォーラム	中野区立武蔵台小学校 視聴覚教室
9月4日（木）	大阪	NPO 法人きんきうぇぶ	河内長野市南花台西小学校
9月18日（木）	神奈川	NPO 情報セキュリティフォーラム	鎌倉商工会議所 3F 会議室
9月25日（木）	大阪	NPO 法人きんきうぇぶ	河内長野市三日市公民館
10月3日（金）	東京	NPO 情報セキュリティフォーラム（NPO-ISEF）	中野区立新山小学校 図書室
10月10日（金）	大阪	NPO 法人きんきうぇぶ	河内長野市立楠小学校
10月12日（日）	福島	NPO 法人日本コンピュータ振興協会	公立大学法人会津大学
10月17日（金）	神奈川	NPO 情報セキュリティフォーラム	ウエルネスさがみはら A 館 7 階 視聴覚室
10月18日（土）	福島	NPO 法人日本コンピュータ振興協会	福島県文化センター 視聴覚室
10月24日（金）	鹿児島	NPO 情報セキュリティフォーラム	秦野市立西公民館 2 階 大会議室
11月8日（土）	大阪	NPO 法人きんきうぇぶ	河内長野市立長野小学校
11月8日（土）	徳島（新規）	財団法人 e- とくしま推進財団	アスティとくしま
11月12日（水）	青森	財団法人八戸地域高度技術振興センター	八戸市総合福祉会館　2 階多目的ホール
11月15日（土）	神奈川	NPO 情報セキュリティフォーラム	川東タウンセンター マロニエ 2 階 集会室 202
11月18日（火）	神奈川	NPO 情報セキュリティフォーラム	横須賀市役所 3 号館 5 階 正庁
11月18日（火）	大阪	NPO 法人きんきうぇぶ	河内長野市立高向小学校
11月27日（木）	神奈川	NPO 情報セキュリティフォーラム	フォーラム南太田 3 階 大会議室
11月29日（土）	神奈川	NPO 情報セキュリティフォーラム	川崎市多摩市民館 3 階 大会議室
11月（予定）	大阪	GIS総合研究所	追手門学院大学
1月29日（火）	大阪	NPO 法人きんきうぇぶ	河内長野市立南花台公民館

事務局お知らせ
JNSA ANNOUNCE

1. 主催セミナーのお知らせ

● Security Day 2008
会　期：2008年12月16日（火）
主　催：JPCERTコーディネーションセンター（JPCERT/CC）
日本インターネットプロバイダー協会（JAIPA）
日本データ通信協会（Telecom-ISAC Japan）
日本ネットワークセキュリティ協会（JNSA）
日本電子認証協議会（JCAF）
会　場：ベルサール八重洲

● JNSA主催イベント
会　期：2008年12月17日（水）～18日（木）
会　場：ベルサール八重洲
詳細については、JNSAホームページをご覧ください。

● 第1回全国情報セキュリティ啓発シンポジウム
やろっさ「インターネット安全教室」in ふくい
会　期：2008年10月31日（金）
主　催：経済産業省
日本ネットワークセキュリティ協会（JNSA）
共　催：NPOナレッジふくい、福井大学
会　場：福井県国際交流会館

2. 後援・協賛イベントのお知らせ

1．SCMフォーラム2008
会　期：2008年9月9日（火）～10日（水）
主　催：社団法人日本ロジスティクスシステム協会
会　場：東京ビッグサイト　会議棟6階
http://logistics.or.jp/fukyu/experience/convention/scmforum/scmforum2008.html

2．モノづくりフェア2008
会　期：2008年10月23日（木）～25日（土）
主　催：日刊工業新聞社
会　場：マリンメッセ福岡
http://www.nikkanseibu-eve.com/mono

3．Internet Week 2008
会　期：2008年11月25日（火）～28日（金）
主　催：社団法人日本ネットワークインフォメーションセンター
会　場：秋葉原コンベンションホール
http://internetweek.jp/

3. JNSA 部会・WG 2008 年度活動

1．政策部会
（部会長：西本逸郎 氏/ラック）
調査事業や様々な基準・ガイドラインの策定、他団体との連携などを行う。

成果物目的のワーキンググループ

【セキュリティ被害調査WG】
（リーダー：大谷尚通 氏/NTTデータ）
2008年 1年間に発生した情報漏えいによる情報セキュリティ被害の実態を調査し、情報漏洩インシデントの傾向、対策状況、組織に与えるインパクト等を定量的に分析し、報告書として公開する。また、情報漏洩以外の情報セキュリティインシデントについて、算定モデルを検討し、同じく組織に与えるインパクト等の定量化を目指す。
予定成果物は
「2006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（英訳版）」
「2007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（速報版、本編、英訳版）」
「2007年度 情報セキュリティインシデントに関する調査データCD-ROM」
「2008年度 情報セキュリティインシデントに関する調査速報」

【セキュリティ市場調査WG】
（リーダー：勝見　勉 氏/JNSA研究員）
情報セキュリティに関する市場の状況ならびに規模等を調査・分析し、WG参加者、JNSA、業界、行政の参考に供する。併せて参加者の勉強・研鑽の場として活用してもらい、業界知識の拡大、人脈の展開、調査分析スキルの向上に資する。
2007年度と同様の調査が実施されるなら、継続受注を目指して、調査を継続する。

【内部統制におけるアイデンティティ管理WG】
（リーダー：宮川晃一 氏/グローバルセキュリティエキスパート）
2008年度は、企業におけるアクセス権付与に関する考え方と、アイデンティティの企業間連携を成果物テーマとして、第2版の発行を目的とする。また、インターネットにおけるアイデンティティ（OpenID, Libety, SAMLなど）を勉強テーマとして活動する。
予定成果物は、内部統制におけるアイデンティティマネージメント解説書とセミナーの実施。

【情報セキュリティランキングWG】
（リーダー：佐野智己 氏/凸版印刷）
情報開示の充実度や取り組み姿勢、社会貢献活動などにも着目した、JNSA版情報セキュリティランキングを定期的に公表する。上位ランキング企業がどういう取り組みをしているかを把握するとともに、真摯に取り組む企業を讃える仕組みとして定着を目指す。
予定成果物は、ランキング結果。

【情報セキュリティ関連パブコメ検討WG】
（リーダー：河野省二 氏/ディアイティ）
毎年、各省庁から情報セキュリティ関連の政策が数多く提出されており、これらの多くにパブリックコメントが求められている。
これらの政策についてよく理解するための勉強会を開催し専門家としての知識を得ること、そして専門家としての意見を政策に反映するためのパブリックコメントを提出することを目的として活動する。

2. 技術部会

（部会長：二木真明氏/住商情報システム）
ネットワークセキュリティに関する調査･研究や、実証実験などを行なう。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。

成果物目的のワーキンググループ

【ハニーポットWG】
（リーダー：園田道夫 氏/JNSA研究員）
ネットを飛び交うマルウェアの実態を、ハニーポットやおとりサーバー、おとりのアカウントなどを用いて研究･解析する。
予定成果物は、マルウェア捕獲報告書。

【セキュアプログラミングWG】
（リーダー：伏見論 氏/情報数理研究所）
セキュアプログラミングの技術的課題の収集、および、アプリケーションセキュリティの国際規格の内容の検討とコメント作成を行う。
予定成果物は情報規格調査会に対するインプットコメント。

【セキュアＯＳ普及促進WG】
（リーダー：澤田栄浩 氏/JTS）
セキュアＯＳの有効性をアピールするために活動内容をWebに公表し、公表している情報を見てもらえるように各種雑誌にアピールしていく。また、インシデントとセキュアOSの関係を紐解いていく。

勉強会目的のワーキンググループ

【PKI相互運用技術WG】
（リーダー：松本泰 氏/セコム）
PKI相互運用技術の情報共有を行う。年間の活動としては、IETFの参加、PKI dayなどのセミナー開催など。予定成果物は、「暗号アルゴリズムの移行問題」について、何らかの報告書をまとめる可能性がある。

プロジェクト

【Challenge PKI】
（リーダー：松本泰 氏/セコム）
2008年度は、Multi-domain-PKIのRFC化の見通しが立っており、このRFC化を足掛かりとして、「暗号アルゴリズム移行問題」、「電子署名法に関連した相互運用技術の課題」など、幅広い問題の解決に取り組むことを検討している。

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。

【会員製品 PR 企画検討WG】
（リーダー：小屋晋吾　氏/トレンドマイクロ）
IDGジャパン社に運営移管した「セキュリティ製品バイヤーズガイド」へのコンテンツ提供や製品登録への協力などについて検討を行う。

【セキュリティ啓発WG】
（リーダー：平田敬 氏/ブリッジ･メタウェア）
2007年度同様、経済産業省の委託事業である「インターネット安全教室」の企画・運営を通してセキュリティ啓発活動を行う。

4. 教育部会

（部会長：安田直 氏/サイバー大学/JNSA主席研究員）
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。

【CISSP行政情報セキュリティCBK－WG】
（リーダー：大河内智秀 氏/NTTコミュニケーションズ）
2008年度は、CISSPに関する知名度向上に関する取組みを行う。

【セキュリティリテラシーベンチマーク作成WG】
（リーダー：大溝裕則氏/JMCリスクソリューションズ）
2008年2月に公開した組織管理者向け機能を追加した「情報セキュリティ理解度チェックサイト」のビジネスモデル案の検討を行うとともに、サイト全体の自主運営に向けた検討を行う。

【SecBok（セキュリティ知識分野作成）WG】
（リーダー: 長谷川長一 氏/ラック）
引き続き、セキュリティ知識の策定と活用に関わる検討を行う。また、活動の目的や内容がほとんど重複する情報セキュリティ教育事業者連絡会（ISEPA）との棲み分けを検討し、今年度以降の役割分担と連携関係を明確にする。予定成果物は、「セキュリティ知識分野2008年度版（仮）」、「セキュリティ知識分野活用ガイド（仮）」

【セキュリティ講師スキル研究WG】
（リーダー：長谷川長一 氏/ラック）
引き続き、セキュリティ講師に必要なスキルの調査研究および実証を行う。（情報セキュリティ教育事業者連絡会;ISEPAとの連携による活動も行う）
策定した「セキュリティ講師スキル（案）」をもとに更なる調査や実証実験を実施する。予定成果物は、「セキュリティ講師スキル研究調査報告書」

【情報セキュリティ教科書執筆者WG】
（リーダー：塩見友規 氏/オー・エイ・エス）
情報セキュリティのプロフェッショナルを目指そうというIT技術者向けの「教科書」を執筆することを目的とする。スキルマップなどの項目分類の更新情報等を参考にし、専門家としての初学者に知ってもらいたい内容をできるだけ網羅する。予定成果物は、情報セキュリティのプロフェッショナル向け教科書（書名未定）の出版。

【教育アーカイブズ検討WG(仮称) 】
（リーダー：河野省二 氏/ディアイティ）
JNSAメンバー始め非メンバーも、セミナーや研修用に色々なスライド等を持ち、大抵の場合再利用されずに埋もれている状態である。著作者本人が公開すれば権利関係の問題は無く、質の高い教育用資料を社会的に共有することができる。
教育用資料等の有効活用、歴史的なアーカイブを保管・検索できる「場」を作るということは意義があるだろうということから、具体的なアーカイブを作るための検討と試行をする予定である。
予定成果物は、試行用データの収集とデータベース化の試行報告書。

【岡山理科大学遠隔授業実施WG(仮称)】
（リーダー：未定）
今まで、情報セキュリティの教育者のスキルについて検討を行い、2006年度に「情報セキュリティ教育の指導者向け手引書」を公開した。これらの成果を実践に生かす形で、岡山理科大学で集中講義という形で遠隔授業を行ってみた。
2009年度からは2単位(15駒)の正式単位認定講義となるのに伴い、カリキュラムやシラバス、講義内容、講義形式等々の検討を行うため、WGとして活動することにした。
講師候補の方々を始め、実際の大学での遠隔授業に一家言ある方の参加も可能である。
予定成果物は、講義のシラバス、講義資料、定期試験、等々のコンテンツ類と報告書。

5. U40部会
（部会長：加藤雅彦 氏/アイアイジェイテクノロジー）
若年層を対象メンバーとして、技術習得向上のための研鑽の場、人脈作りの場を提供する。また、JNSA運営への積極的な関与、会員間の交流の強化、活動活性化のための情報流通強化、セキュリティ業界や社会への貢献などを目的とする。

【JNSAラボネットWG】
（リーダー：坂本 慶 氏/ディアイティ）
ワーキンググループの活動における、実環境を使った技術検証などが円滑に行えるように、検証環境の設計と構築を議論し、実際の環境構築を行う。またU40部会のWGとして、本活動を通して若手メンバーのスキル向上を図る。予定成果物は、検証環境の提供。

【勉強会企画検討WG】
（リーダー：嘉津義明 氏/シマンテック）
若年層の知識および技術向上のため、メンバー向けの勉強会を企画検討し、講師手配などを行なう。これにより外部との人脈作りおよび運営面についてのスキルアップも図る。また、良い企画があれば、JNSA会員向けのセミナーとして推薦する。

6. ユーザー部会　※新設

（部会長：未定）

JNSA参加企業は、ISMSやPマークを取得し、かつ情報セキュリティベンダーとして、セキュリティビジネスを行っている。しかしながら、自社の企業内ユーザー（例えば、営業、エンジニア、管理系部署）の情報セキュリティモラルが上がっていないことも事実である。

このため、今年度は、成功失敗の事例紹介、テーマ毎の研究会を行い、効果的な企業内ユーザーのモラル醸成方法、効率的な情報セキュリティ運用方法を模索していくような活動を行う予定である。

7. 西日本支部

（支部長：井上陽一 氏/JNSA顧問）

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する。今年度も引き続き関西方面でのセキュリティ啓発セミナーを中心に活動を行う。

【企画運営WG】

（リーダー：井上陽一 氏/JNSA顧問）

中小企業の情報セキュリティ水準の底上げ、中小企業の負担軽減に繋がる方策について、情報セキュリティチェックシートWGと共同して明示･PDCA定着化のための啓発を行うと共に、近畿経済産業局と協働して地域における産官共同の基盤づくりを行う。予定成果物として、情報セキュリティチェックシートWGと共同して、チェックシート作成･解析結果を報告書としてまとめる。

【情報セキュリティチェックシートWG】

（リーダー：嶋倉文裕 氏/富士通関西中部ネットテック）

情報セキュリティチェックシートを使用することにより、中堅・中小企業の経営者（経営層）が気付きを超えた企業価値向上の視点で、自社のセキュリティ対策の現状を認識し、対応して頂く上でのガイダンスとなるような情報セキュリティチェックシートの作成を目標として活動する。

予定成果物は、チェックシートおよびアンケート解析結果報告。

情報セキュリティ教育事業者連絡会(ISEPA)

（代表：与儀大輔 氏/ラック）

連絡会各会員団体の運営する資格の位置付け、キャリアパスに対する共通認識の提示、施策提案、さらには各種教育機関との連携によるコンテンツの共同利用など、情報セキュリティ人材育成に関する様々な情報を社会に広く提供し、人材育成の拡大に向けた様々な取り組みを推進する活動を行う。

【イベントWG】

（リーダー：杉本毅氏/ITプロフェッショナル･グループ）

ホームページ、各種イベント、あるいは各種の広報活動により、ISEPA情報セキュリティ教育事業者連絡会の活動や取り組みを、社会に広く紹介していく。

【スキルWG】

（リーダー：衣川俊章氏/ITプロフェッショナル･グループ）

各団体の資格試験の内容を体系的に整理し、各資格試験の相関図の作成やキャリアパスを提示し、情報セキュリティの分野で求められる人材像を具体的に示していく。

【相互認証WG】

（リーダー：関取嘉浩氏/NRIセキュアテクノロジーズ）

各事業者間の相互認証の可能性の検討を行なう。また、必要に応じてWGを開催し、相互認証の可能性について検討していく。認定資格取得者数の調査も行う予定。

日本セキュリティオペレーション事業者協議会(ISOG-J)

（代表：武智洋 氏/ラック）

セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進する事業を実施することにより、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に向けて寄与する目的として発足。JNSA下部組織として、ガイドラインの策定や技術向上に向けた検討、普及啓発活動を行う。

4. JNSA 役員一覧 2008 年 6 月 13 日現在

会　長　佐々木　良一
東京電機大学 教授

副会長　高橋　正和
マイクロソフト株式会社

副会長　大和　敏彦
ブロードバンドタワー株式会社

理　事（50 音順）

足立　修	株式会社シマンテック
池田　修一	NTT コミュニケーションズ株式会社
後沢　忍	三菱電機株式会社　情報技術総合研究所
遠藤　直樹	東芝ソリューション株式会社
大坪　武憲	新日鉄ソリューションズ株式会社
勝見　勉	リコー・ヒューマン・クリエイツ株式会社
川上　博康	セコムトラストシステムズ株式会社
後藤　和彦	株式会社大塚商会
小屋　晋吾	トレンドマイクロ株式会社
佐藤　邦光	大日本印刷株式会社
下村　正洋	株式会社ディアイティ
立石　和義	NTT アドバンステクノロジ株式会社
橘　　伸俊	株式会社ネットマークス
玉井　節朗	株式会社ＩＤＧジャパン
西尾　秀一	株式会社ＮＴＴデータ
西本　逸郎	株式会社ラック
野々下幸治	マカフィー株式会社
森田　次朗	株式会社フォーバルクリエーティブ
日暮　則武	東京海上日動火災保険株式会社
山野　修	ＲＳＡセキュリティ株式会社
吉原　勉	株式会社アイアイジェイテクノロジー

監　事

土井　充	公認会計士　土井充事務所

特別顧問

石田　晴久	サイバー大学 IT 総合学部 学部長

顧　問

井上　陽一	
今井　秀樹	中央大学　教授
北沢　義博	霞が関法律会計事務所　弁護士
武藤　佳恭	慶応義塾大学　教授
前川　徹	サイバー大学　教授
村岡　洋一	早稲田大学　教授
安田　浩	東京電機大学　教授
山口　英	奈良先端科学技術大学院大学　教授
吉田　眞	東京大学　教授

事務局長

下村　正洋	株式会社ディアイティ

5. 会員企業一覧（2008年7月28日現在　203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
アイエックス・ナレッジ(株)
(株)ITプロフェッショナル･グループ
(株)アイ・ティ・フロンティア
(株)ＩＤＧジャパン
(株)アイティーブレーン New
(株)アイテクノ New
アイネット･システムズ(株)
(株)アイ・ビー・イー・ネット・タイム
(株)ＩＰイノベーションズ
アイマトリックス(株)
(株)アクシオ
あずさ監査法人
(株)網屋
(株)アルテミス
(株)アルファシステムズ New
アルプスシステムインテグレーション(株)
(株)ＩＳＡＯ
伊藤忠テクノソリューションズ(株)
学校法人 岩崎学園
(株)インストラクション
(株)インターネットイニシアティブ New
(株)インテックシステム研究所
(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
Impreva JAPAN
ヴァイタル･インフォメーション(株)
ウェブセンス･ジャパン(株)
ウェブルート･ソフトウェア(株)
ＡＴ＆Ｔジャパン(株)
(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)
エヌアイシー･ネットシステム(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)
エヌ･ティ･ティ・コムチェオ(株)
ＮＴＴコムテクノロジー(株) New
(株)ＮＴＴデータ
(株)ＮＴＴデータＣＣＳ
(株)エネルギア・コミュニケーションズ
Ｆ５ネットワークスジャパン(株)
エムオーテックス(株)
オー･エイ･エス(株)
(株)オーク電子
(株)大塚商会
(株)オレンジソフト

【か】

(株)Kaspersky Labs Japan
兼松エレクトロニクス(株)
(株)ガルフネット
関電システムソリューションズ(株)
キヤノンＩＴソリューションズ(株)
キヤノンマーケティングジャパン(株)
九電ビジネスソリューションズ(株)
京セラコミュニケーションシステム(株)
クオリティ(株)
(株)グローバルエース
グローバルサイン(株)
グローバルセキュリティエキスパート(株)
(株)ケーケーシー情報システム
(株)コネクタス
コンピュータエンジニアリングサービス(株)

【さ】

サードネットワークス(株)
サイバーエリアリサーチ(株)
サイバーソリューション(株)
(株)サイロック
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)ＪＭＣリスクソリューションズ

ジェイズ・コミュニケーション(株)
(株)ＪＴＳ
ＪＰＣＥＲＴコーディネーションセンター
シスコシステムズ合同会社
システム･エンジニアリング･ハウス(株) New
(株)シマンテック
(株)ジャパンネット銀行
寿限無(株)
(株)情報数理研究所
新日鉄ソリューションズ(株)
新日本監査法人
Ｓｋｙ(株)
(株)ステラクラフト
住商情報システム(株)
住生コンピューターサービス(株)
セキュアコンピューティングジャパン(株)
(株)セキュアブレイン
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム(株)
セコムトラストシステムズ(株)
(株)セラク
セントラル短資オンライントレード(株) New
ソニー(株)
ソフォス(株)
ソフトバンク(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)
(株)大和総研
(株)タクマ
チェックポイントソフトウェアテクノロジーズ(株)
ＴＩＳ(株)
(株)ディアイティ
デジタルアーツ(株)
(株)電通国際情報サービス
監査法人トーマツ
東京エレクトロン デバイス(株)
東京海上日動火災保険(株)
東京日産コンピュータシステム(株)
東芝ITサービス(株)
東芝ソリューション(株)
ドコモ･システムズ(株)
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)
日信電子サービス(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ＳＧＩ(株)
日本オラクル(株)
日本クロストラスト(株)
日本ＣＡ(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)
日本電信電話(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)
ネッツエスアイ東洋(株)
(株)ネットマークス
ネットワンシステムズ(株)
(株)野村総合研究所

【は】

(株)ハイエレコン
パスロジ(株)
バリオセキュア・ネットワークス(株)
(株)ハンモック
(株)日立システムアンドサービス
(株)日立情報システムズ
(株)日立製作所
日立ソフトウェアエンジニアリング(株)
(株)ＰＦＵ
(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)
富士通(株)
富士通エフ・アイ・ピー(株)

(株)富士通エフサス
富士通関西中部ネットテック(株)
(株)富士通ソーシアルサイエンスラボラトリ(富士通ＳＳＬ)
(株)富士通ビジネスシステム
富士電機アドバンストテクノロジー(株)
扶桑電通(株)
フューチャーアーキテクト(株)
(株)フューチャーイン
(株)ブリッジ・メタウェア
(株)ブロードバンドセキュリティ
(株)ブロードバンドタワー
(株)プロティビティジャパン

【ま】

(株)マイクロ総合研究所
マイクロソフト(株)
マカフィー(株)
松下電工(株)
みずほ情報総研(株)
三井物産セキュアディレクション(株)
(株)三菱総合研究所
三菱総研ＤＣＳ(株)
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】

ユーテン・ネットワークス(株)
(株)ユービーセキュア

【ら】

(株)ラック
LANDesk Software(株)
リコー・ヒューマン・クリエイツ(株)
(有)ロボック

【わ】

(株)ワイ・イー・シー
(株)ワイズ

【特別会員】

特定非営利活動法人　アイタック
韓国電子通信研究院
社団法人　コンピュータソフトウェア協会
ジャパン　データ　ストレージ　フォーラム
財団法人　ソフトピアジャパン
データベース・セキュリティ・コンソーシアム
特定非営利活動法人デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院　工学系研究科
社団法人　日本インターネットプロバイダー協会
社団法人　日本コンピュータシステム販売店協会
特定非営利活動法人　日本セキュリティ監査協会
有限責任中間法人　日本電子認証協議会

6. JNSA 年間活動（2008 年度）

4 月		
	4 月 23 ～ 24 日	「RSA Conference Japan 2008」後援
5 月	5 月 1 日	第 1 回幹事会
	5 月 14 日	2008 年度理事会（虎ノ門パストラル）
	5 月 26 ～ 27 日	「CeCOS II Tokyo(Counter eCrime Operation Summit II in Tokyo)」後援
6 月	6 月 5 ～ 7 日	「第 12 回サイバー犯罪に関する白浜シンポジウム」後援
	6 月 9 ～ 13 日	「Interop Tokyo 2008」後援
	6 月 13 日	2007 年度 WG 活動報告会（ベルサール八重洲）
	6 月 13 日	2008 年度総会（ベルサール神田）
	6 月 18 日	「平成 20 年度情報モラル啓発セミナー」（兵庫会場）後援
7 月	7 月 1 ～ 2 日	「SANS Future Visions 2008 Tokyo 」後援
	7 月 3 日	「PKI Day 2008」セミナー（東京ウィメンズプラザ）
	7 月 4 ～ 5 日	「WASForum Conference2008」後援
	7 月 8 日	第 2 回幹事会
	7 月 9 日	「2008 年度　情報セキュリティ監査シンポジウム　in Tokyo」後援
	7 月 10 ～ 12 日	「沖縄 ICT フォーラム 2008」後援
	7 月 16 ～ 18 日	「自治体総合フェア 2008」協賛
	7 月 17 日	「平成 20 年度情報モラル啓発セミナー」（三重会場）後援
	7 月 22 ～ 24 日	「ワイヤレスジャパン 2008」後援
	7 月 24 日	リコー情報セキュリティ強化セミナー「今、再び考える『情報ｾｷｭﾘﾃｨ』」後援
8 月	8 月 13 ～ 17 日	「セキュリティ＆プログラミング・キャンプ 2008」後援
	8 月 22 日	「被害調査 WG・リテラジーベンチマーク作成 WG 合同セキュリティ対策セミナー」（メルパルク東京）
	8 月 25 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（札幌会場）後援
	8 月 26 日	第 3 回幹事会・臨時理事会
	8 月 29 日	「CompTIA Breakaway in Japan」後援
9 月	9 月 26 日	「平成 20 年度情報モラル啓発セミナー」（北海道会場）後援
	9 月 26 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（高松会場）後援
	9 月 9 ～ 10 日	「SCM フォーラム 2008」協賛
10 月	10 月 2 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（仙台会場）後援
	10 月 21 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（福岡会場）後援
	10 月 23 ～ 25 日	「モノづくりフェア 2008」協賛
	10 月 31 日	「第 1 回全国情報セキュリティ啓発シンポジウム やろっさ『インターネット安全教室』in ふくい」
11 月	11 月 11 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（大阪会場）後援
	11 月 25 ～ 28 日	「Internet Week 2008」後援
12 月	12 月 16 日	「Security Day 2008」セミナー（ベルサール八重洲）
	12 月 17 ～ 18 日	「JNSA 主催イベント（予定）」（ベルサール八重洲）
	12 月 19 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（名古屋会場）後援
1 月	1 月 23 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（広島会場）後援
2 月	2 月 13 日	「2008 年度　全国縦断情報セキュリティ監査セミナー」（富山会場）後援
3 月		

2008 年 6 月～ 2009 年 3 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/aboutus/schedule.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 http://www.jnsa.org/member/index.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

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
E-Mail：sec@jnsa.org
URL： http://www.jnsa.org/

西日本支部
〒 532-0011　大阪府大阪市淀川区西中島 5-14-10
カトキチ新大阪ビル（株）ディアイティ内
TEL： 06-6886-5540

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。

■ JNSA 事務局移転のお知らせ■

JNSA 事務局は、本年 9 月に下記住所に移転することとなりました。

新住所［ 9月8日(月) 業務開始予定 ］
〒 105-0003 東京都港区西新橋 1-22-12 JC ビル 3 F
Tel: 03-3519-6440　Fax: 03-3519-6441

JNSA Press vol.23

2008 年 8 月 25 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）
E-Mail: sec@jnsa.org　URL: http://www.jnsa.org/
印　刷
プリンテックス株式会社

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

E-mail: sec@jnsa.org URL: http://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島5-14-10 カトキチ新大阪ビル （株）ディアイティ内
TEL 06-6686-5540