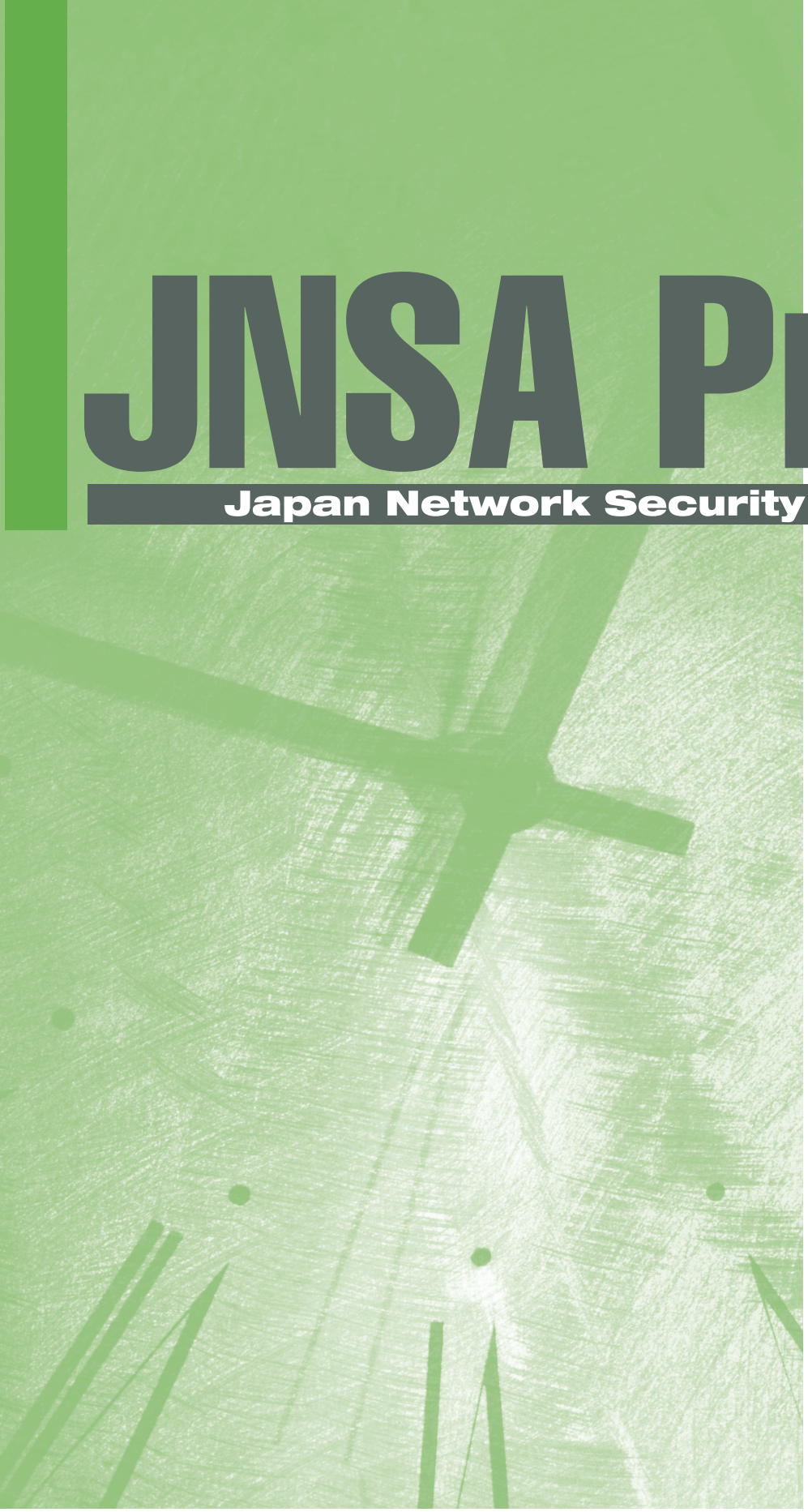
JNSA Press

Japan Network Security Association

Vol.17
August 2006



CONTENTS

ご挨拶
3番目のセキュリティ …… 1

特　集
- いま、米国企業でCSOが注目される理由‥ 3
- これからのオフィスセキュリティ強化対策のあり方を考える 7

JNSAワーキンググループ紹介
- セキュアプログラミングWG …… 11
- セキュリティリテラシーベンチマーク作成WG …… 13

会員企業ご紹介 …… 14

JNSA会員企業情報 …… 20

イベント開催の報告 …… 22

「インターネット安全教室」…… 34

事務局お知らせ …… 36

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

3番目のセキュリティ

有限責任中間法人 JPCERT コーディネーションセンター
常務理事 早貸　淳子

「セキュリティ」という言葉は、いろいろな意味で使われていますが、私が、業務上最初に触れた「セキュリティ」という言葉は、民事法上の「担保」を意味するものでした。「担保」の意味での“security”は、英米法辞典流に言えば、「権利の享受や実現を確保させるための物的又は債権的な保証のこと」ですが、平たく言えば、貸したお金等を将来回収できないかもしれないという不安に対して、回収が困難になったときに担保物を換価して相当額を得ることができるという安心を提供するものであるといえます。たとえば、“security deposit”といえば、敷金や保証金のことをいいます。

2番目に担当した「セキュリティ」は、「証券」（この場合には、“securities”と複数形で使うことが多いのですが。）でした。ここでいう「証券」とは、株式会社の「株式」等、企業に対する権利を証するものをいいます。この「証券」、すなわち、会社等に対して自分の権利を主張するための道具を得ておくことにより、投資をしたにもかかわらず会社側から権利を否認されてしまうようなことはない、という安心を得ることができます。

3番目に担当することになった「セキュリティ」が「情報セキュリティ」又は「コンピュータセキュリティ」です。「情報セキュリティ」とは、一般的には、情報資産の「機密性」、「完全性」および「可用性」を維持することであると説明されていますが、これは、上記の「担保」や「証券」としての“security”が、それを保有すること自体が安心を得るための道具になっているのとは異なっています。

保護を受けようとする債権や権利の内容に応じてどの程度の担保を取っておく必要があるかが決まってくるという点では、似通った部分もありますが、「担保」や「証券」は、法制度として創設されている仕組みであって、一定の法的要件を瑕疵なく満たせば有効なものとして成立し、想定された脅威に対する保護を得ることができるのに対し、情報セキュリティについては、想定される脅威に対してこれだけのことをしさえすれば情報資産を保護することができるという保証を得ることは困難といわざるを得ません。情報セキュリティについては、想定される脅威が技術の進歩と環境によって変化するという問題もあります。このような問題が、「情報セキュリティ対策にどこまで投資すればよいのか」、「投資した情報セキュリティ対策の有効性をどう評価するのか」という各組織内の担当者の悩みにつながっているわけです。

また、担保権や、証券に表象される権利の内容については、関係者間で法律や契約に基づいた観念が成立していれば十分なわけですが、情報セキュリティについては、仮に関係者間

で「ここまでやれば十分だよね」というコンセンサスが得られたとしても、実際に機密情報が漏洩したり、情報が継続的に利用できない事態が生じたりしてしまった場合には、「漏洩しなかったことにしよう」とか「事業が継続して行えていたことにしよう」と観念しても意味がないといわざるを得ませんので、安心を得るための対策のみならず、実際に事故が起きてしまった場合にどう対処（レスポンス）するかについてもあらかじめ検討しておくことが不可欠であるといえます。

JPCERT コーディネーションセンターは、企業等の組織が、自らが保有している情報資産に応じた情報セキュリティ対策を講じたり、最近顕著になってきているスピア型の攻撃に対する独自のインシデントレスポンス機能を備えたりすることができるよう、組織内 CSIRT の構築支援に一層の注力をしていきたいと考えているところであり、常日頃から上記の「情報セキュリティ対策にどこまで投資すればよいのか」、「投資した情報セキュリティ対策の有効性をどう評価するのか」等を始めとする企業その他の関係者の悩みに正面から取り組んでいらっしゃる JNSA の活動に高い関心をよせています。

JNSA の各 WG の活動の成果が広く利用されることにより、第 3 番目のセキュリティが「担保」や「証券」のような社会基盤として成熟･定着していくことを心より期待いたしております。

いま、米国企業でCSOが注目される理由
―CSOによる総合的な企業セキュリティ統括の重要性

株式会社ジュリアーニ・セキュリティ & セーフティ・アジア
代表取締役会長兼CEO　齋藤ウィリアム

セキュリティを統括するCSO

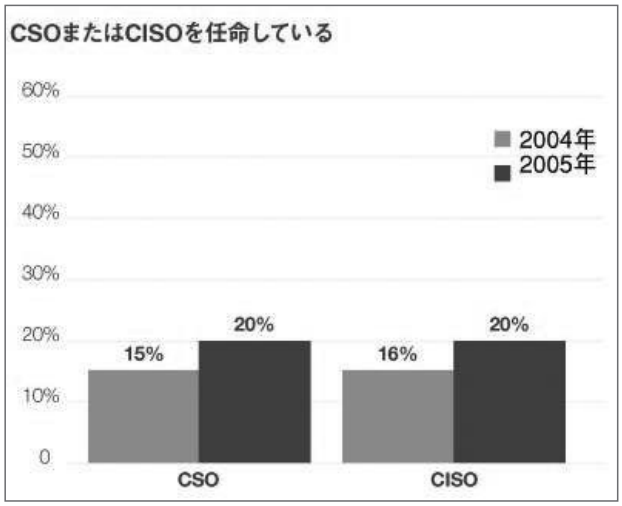
ここ数年、米国企業においてCSO（Chief Security Officer= 最高セキュリティ責任者）に対する認識が急速に高まっている。

日本でセキュリティ責任者といえばIT部門のセキュリティ担当者をイメージする場合が多いが、これはCISOであってCSOとは異なる。

CSOが担当するのは狭義のITセキュリティだけではない。物理セキュリティ、組織セキュリティまでふくめた総合的な企業セキュリティ、危機管理全般を統括する役職がCSOである。また、CSOは企業セキュリティ全般に対して単独で責任を持つ役職でもある。かりに企業がなんらかの災害(サイバーテロ、物理テロ、自然災害など）に見舞われて企業活動にダメージを受けた場合、予防策をふくめたすべての対策・事後処理など全プロセスに対して責任をとるのがCSOである。当然ながら米国企業でのCSOの地位は高く、CEOの元、CFOとならぶ役職と見なされるケースも少なくない。

● CSO任命企業の増加率

米国では、セキュリティ専門職を任命するケースが増加している



Source:CIO Magazine 米国版「情報セキュリティ動向調査 2005」

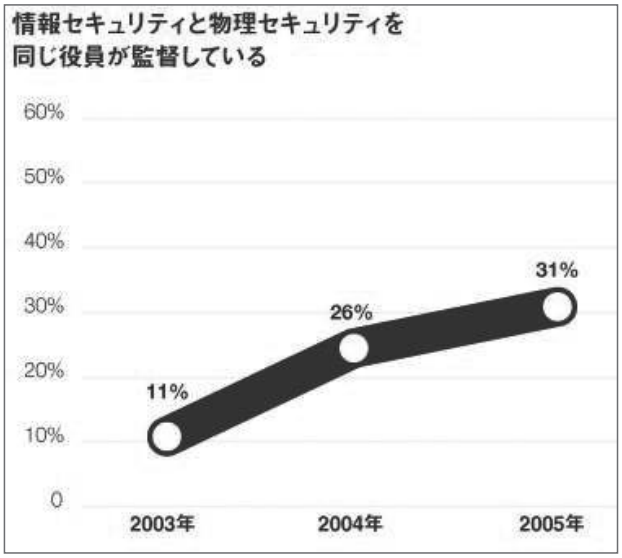
ではなぜCSOという役職が必要とされているのだろうか？

第一には「責任の所在を明確にする」という意識である。企業セキュリティには多くの部門が関係する。ところが、日常の対策や運用ルールについては個別部門ごとにボトムアップで決定されている場合がほとんどだ。たとえば、パスワード運用やノートPCの持ち出し規定についてはIT部門が決め、入退室カードの手配は総務が担当し、社員のセキュリティ教育については人事が受け持つ、といった具合。このような状況では、何か事件が起きたとしても誰も責任を取ることができない。

かりに退社した社員が、退社後、パスワードを悪用して企業の情報システムに侵入し重要な顧客データが流出したとする。このケースで責任を取るべきなのは誰だろう？IT部門の担当者？あるいは人事の担当者だろうか？予防策を講じるべきだったのはどの部門だろう？

●情報セキュリティと物理セキュリティの統合化率

米国ではここ数年、CSOが情報セキュリティと物理セキュリティ双方を監督する割合が増加している



Source:CIO Magazine 米国版「情報セキュリティ動向調査 2005」

「共同責任は無責任」という言い方があるが、これは企業のセキュリティ対策にもあてはまる。縦割りの各部門がボトムアップで連携するだけでは限界がある。企業が総合的なセキュリティを確保するためには、強力な権限を持つ CSO がすべての部門を鳥瞰し横断する形で統括する必要がある。

言うまでもなく現在では、データ流出などのセキュリティ侵犯事件が株価をはじめとした企業価値の下落に直結する。事故が起きてからでは遅い。米国企業で CSO の役割が重要視される背景には、企業自らが実効性あるセキュリティ対策を講じようとする意識の高まりがある。

BCP が企業を救う

前述したとおり CSO は、IT セキュリティだけでなく、物理セキュリティ、組織セキュリティもふくんだ総合的な企業セキュリティを統括する役職でもある。ここには近年注目されている BCM あるいは BCP への取り組みという意味合いも強く反映している。

BCM とは Business Continuity Management、BCP とは Business Continuity Plan の略語である。それぞれ「ビジネス継続マネジメント」「(実効性ある) ビジネス継続プラン」の意味を持つ。自然災害、人為的災害、環境災害、政治的災害、さらにはウイルス感染などの情報システム災害等が発生しても、企業の根幹となるビジネス機能を停止することなく、主要な企業活動を継続可能とすること。そのためのマネジメントが BCM であり、具体的対策や手順の取り決めが BCP である。

人為的災害であれ偶発的な災害によるものであれ、企業活動の停止や中断は、以後長期にわたって企業業績に大きな影響を与えてしまう。どのような災害に対しても、基幹部分の企業活動を継続できるよう対策を講じておくこと。これが BCM の基本的な考え方である。数回にわたって物理的なテロを経験した N.Y. の企業を中心にして、1990 年代後半からこの BCM の意識が非常に高くなっているのだ。

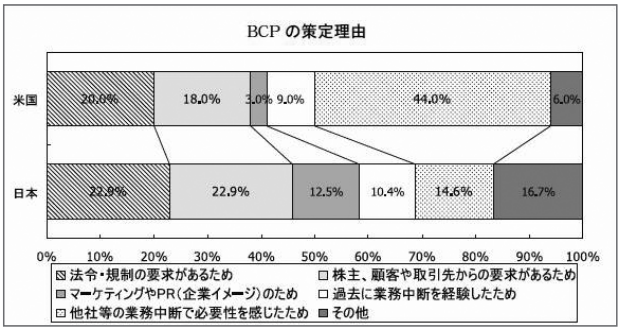
具体的な例をあげよう。

WTC（世界貿易センタービル）に本社を置いていたある薬品会社の例である。この薬品会社では 1993 年の爆弾テロの経験から、自主的に BCP の策定に着手した。1993 年 2 月の爆弾テロの際、本社機能が完全に停止し、世界中の支店をはじめとして社外社員からの連絡がまったく取れなくなってしまったのである。この企業では本社業務を一からすべて見直し、基幹業務については完全なバックアップサイトを構築した。このコストは何十億ドルとも言われ、一時は株主からも「本当に必要な対策なのか ?」と苦言を呈されたほどである。

しかし、この取り組みの有効性はすぐに証明されることになった。N.Y. では 1990 年代前半、2 回の大規模停電をはじめとして、大雪での交通ストップ、タクシー会社のストライキなどが頻発した。ところが BCP に取り組んでいたこの薬品会社では、まったく業務に影響を受けなかったのである。と同時に、BCP による予想外の効果も手にしている。業務の全面見直しによって無駄が削減され、日常的な業務の運用効率が改善されたのである。この企業で BCP に投資されたコストは、2 年以内にほぼ回収されたと言

● BCP 策定理由 : 日米比較

米国では44%もの企業が「過去の業務中断の経験」をBCP策定の動機にあげている。企業自身の切実な危機意識がBCPの取り組みにつながっている。



Source: KPMG ビジネスアシュアランス BCP サーベイ 2004/2005

われている。もちろん、9.11 テロに際しても本社機能を一切停止することなく、企業活動を続けることができた。

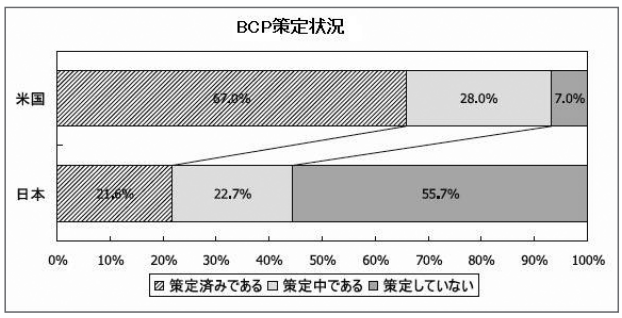
もう一例あげよう。NYSE（ニューヨーク証券取引所）は、9.11 テロに際して 3 日で業務を再開している。これは 1990 年代後半から CSO を任命して BCP に取り組んだ成果だと言われている。同じように、事前に BCP に投資して対策を講じていた証券会社は、テロ後もごく早期に業務を再開している。逆に BCP 投資を怠っていた証券会社は 3 か月以上も業務が停止し、以後、長期にわたって企業業績を大きく落ち込ませてしまった。

これらの例が示すのは次の 2 点である。BCP を背景とした総合的なセキュリティ対策の有無が、災害に際して企業存続のキーポイントとなること。

そして、実効性あるセキュリティ対策にかかるコストはけっして無意味な投資ではなく、災害時はもちろん、日常の業務においても副作用的なコストメリットを生じ得るものだということである。

● BCP 策定率 : 日米比較

策定済み・策定中を合計した割合では米国93%に対して、日本では約45%。対策の遅れが危惧される。



Source: KPMG ビジネスアシュアランス BCP サーベイ 2004/2005

JSOX 法はセキュリティ改革の好機

日本ではいまだに「セキュリティ対策はコスト高」という漠然とした印象が一般的である。

事実、企業の各部門が別個にセキュリティ対策に取り組んだ場合は、そうなる可能性が高い。総務、人事、情報システム部がそれぞれに企業部門のセキュリティポリシーを策定し、運用しているとすれば、重複した無駄なコストがかさむだけでなく、結果として実効性を伴わない形だけの対策になってしまう。これではまったくの無駄な出費である。

しかし、全体の業務の流れをセキュリティという観点から見直して分析し、有効な対策を講じていくことで、企業活動はセキュアにもなり、また日常的な業務のコストダウンにもなり得る。CSO 職の存在意義とは、セキュリティという観点からの業務見直し効果を企業にもたらすものでもある。

米国企業の CSO が統括するセキュリティの範囲は幅広い。IT 系の日常的なセキュリティポリシーはもちろん、採用社員のバックグラウンドチェック、退社時の手続き、災害時の業務システムの構築、移行の手順、またそれらについての社員教育、あるいは事件発生後の的確な情報公開の対応まで。情報システム、人事、総務、広報といった各部門を横断した、総合的な対策の策定と日々の運用に責任をもつのが CSO の役割である。

逆に言えば、CSO というポジションを置かなければ、こういった総合的なセキュリティ対策は難しい。CSO に適切な人材を割くことで、各部門はセキュリティの責任から解放され、企業全体としては真に実効性をもつ総合的なセキュリティ対策を手にすることができる。このような判断が、米国企業での CSO 職への注目につながっている。

日本では先の 6 月 7 日、参院本会議で「金融商品取引法（投資サービス法）」が成立した。メディアではインサイダー取引の罰則強化など金融系の話題ばかりがクローズアップされたが、この法案はもともと

準備段階から米国企業改革法（SOX 法 = サーベンス・オクスレー法）の日本版とされてきたものである。SOX 法は企業の内部統制ルールの強化を目的とした法案であり、BCP の策定とも強い関連性がある。BCP 策定を怠った経営者は、SOX 法の規定によって刑事罰が課せられる可能性すらある。かりに関東近辺での大地震によって本社業務が停止して株価が暴落した場合、BCP 策定をしていない経営者は内部統制違反に問われることも考えられる。

このため、今後は日本企業においても、BCP をも視野に入れた企業セキュリティポリシーの総合的な見直しが迫られることになるはずだ。

この機会を企業のセキュリティ対策の抜本的な改革期として前向きに対応するか、たんに面倒な規制として消極的に対応するか。企業は選択を迫られている。

本稿で述べたとおり、総合的なセキュリティ対策はけっして各部門の片手間で実現できるものではない。逆に、真に実効性をもつセキュリティを求めるならば、その結果として得られるメリットは予想以上に大きいものでもある。

企業を取り巻く環境が複雑さを増している現在、企業の安定的な発展と存続のためには、実効性あるリスクマネジメントが不可欠である。CSO 職によるトータルなセキュリティ対策。これこそが今後の災害多発時代の企業価値を決定する、ひとつの大きな要因となるはずである。

これからのオフィスセキュリティ強化対策のあり方を考える

大日本印刷株式会社 IPS 事業部
主席研究員　半田　富己男

個人情報保護法が 2005 年 4 月に施行された後にも、個人情報取扱事業者からの漏えい事案報告が続いています。内閣府が国民生活審議会個人情報保護部会へ提出した報告によると、平成 17 年度に個人情報取扱事業者が公表した個人情報の漏えい※1事案は、合計 1,556 件にのぼります。これらの個人情報漏えい事案のうち特段の情報保護措置を講じていなかった件数が全体の 51.7% を占めており、漏えい後の改善措置についてみると、全体の 96.5% の事業者が何らかの安全管理対策を講じています。事件が起きてからでないと、セキュリティ対策への投資の必要性が経営層に理解されにくいという、各企業の情報セキュリティ担当者の悩みは、この数字にも表れています。
こうした事案で、個人情報が漏えいしたとされる人数は、500 人以下の事案が全体の 71.6% と比較的小規模な事案が多くなっています。しかし、PC や記憶媒体の紛失・盗難による事案や、不正アクセスによる漏えい事案では、1 件あたりの漏えい人数が多くなり、重大な 2 次被害につながる恐れもあり、深刻な事態となることが多くなっています。大規模な個人情報漏えい事案を引き起こしてしまった企業は、損害賠償、社会的信用の失墜、顧客や取引先からの取引停止などという大きなダメージをこうむることにより、事業そのものを継続できないという重大な危機を迎えてしまいます。リスク管理の面から見ても、事件を起こしてしまってからの対応は難易度が高いばかりでなく、対応が完了する迄の期間のリスクを考慮すると、事前に適切な対応策をとっておくことが望ましいといえます。
本稿では、物理的セキュリティ対策と技術的セキュリティ対策の両面で効果的なキーデバイスとなる IC カードの使い方を軸にオフィスセキュリティ強化対策のあり方を考察します。

1. 物理的セキュリティ対策

個人情報保護法第20条は、個人情報取扱事業者に対して、その取り扱う個人データの漏えい、滅失又はき損の防止、その他の個人データの安全管理のために必要かつ、適切な措置を講じることを義務付けています。これを受けた経済産業省のガイドライン「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」では、組織的、人的、物理的及び技術的な安全管理措置を講じることを求めています。企業は利潤の追求にとどまらず、社会的責任(CSR)を果たすことが求められるようになり、法令遵守(コンプライアンス)と企業統治(コーポレート・ガバナンス)への関心が急速に高まっています。こうした背景から、今年に入って物理的セキュリティ対策に注目が集まり、オフィスセキュリティに特化した展示会(オフィスセキュリティ EXPO)が初めて開催されたり、オフィスの物理的セキュリティ対策を中心に第三者機関が評価・認証する制度(オフィスセキュリティマーク認証制度)が創設される等の動きが見られます。

(社)ニューオフィス推進協議会(NOPA)では、オフィスセキュリティマーク認証基準を定め、これに基づいたオフィスセキュリティマーク認証制度を2006年10月から開始しようとしています。この制度は、認証内容、取得費用及び期間等において、中堅・中小規模のSMB※2にとって比較的取得・継続しやすい認証制度となっています。ISMS適合性評価制度の認証基準JIS Q 27001でも、管理目的及び管理策として、セキュリティを保つべき領域を規定しています。こうした評価・認証制度では、機密性、完全性、可用性をバランス良く維持し改善していくためにPDCAサイクルを継続的に繰り返して、セキュリティ・レベルの維持・改善を図ることが要求されます。

※1「漏えい」の他、「滅失」、「き損」の事案を含む。　※2 Small and Medium Business

物理的セキュリティ対策の中でも、最初に着手されるのは、物理的セキュリティ境界のゾーニングと、それによって作られたセキュリティ領域への入退館(室)管理です。磁気カードやICカード等をセキュリティ領域のゲートに設置されたカードリーダにスキャンすることにより本人確認を行い、ゲートの電気錠を解錠する方法や、身体的特徴をセンサーで識別・認証して本人確認を行い、解錠する生体認証方式などが用いられています。

一方、従業員と来訪者を識別するために、氏名・顔写真入りのIDカードを貸与して着用させる方法が広く行われています。そのため､従業員識別用のIDカードと入退館(室)管理システム用カードを共通化しようと考えるのは自然な展開といえます。こうした用途のIDカードとして従来の社員証・職員証カードを新規に切り替える際には、磁気カードではなくICカードを採用する事例が増えています。ICカードは磁気カードより大きなメモリ容量を持ち、カード所持者を認証する機能や格納データに対するアクセス制御機能を持っているため、磁気カードに比べてセキュリティを向上させることが可能となります。ICカードには、リーダ・ライタとの通信方式により、接触型と非接触型がありますが、非接触型の場合、リーダ・ライタにカードを通す代わりに「かざす」だけでよいので入退館(室)管理での利用では、利便性の面から非接触型の人気が、最近特に高くなっています。

2. 技術的セキュリティ対策

技術的セキュリティ対策には、情報資産及びそれを取り扱う情報システムへの、アクセス制御、不正ソフトウェア対策、情報システムの監視等、情報資産に対するIT技術的な対策等があります。中でも、識別と認証は、情報システム利用者の身元を特定し、真正性を確認する技術で、情報システムへの不正アクセスを試みる者を入口で拒否する重要な防御機能です。認証技術を分類すると、パスワードなど利用者本人の記憶(知識)に基づく認証、ICカードや認証トークンなど本人のみが所持しているものに基づく認証、本人の身体的特徴に基づくバイオメトリクス認証の3種類があります。利用者IDとパスワードだけによる識別・認証では、利用者本人が覚えやすく簡単で短いパスワードを設定してしまうために、他人にパスワードを推測されてしまったり、逆に、長くて複雑なパスワードに設定したために利用者本人が覚えきれずに紙に書いてしまうところから他人にパスワードが漏えいしたりするなどの問題点があります。そこで、パスワードを知っていることと、ICカードを持っていることなど、複数の要素を組み合わせた多要素認証が注目を集めています。また、公開鍵基盤(PKI)のデジタル証明書等の暗号クレデンシャルを用いた認証でも、暗号クレデンシャルをセキュアに格納し、携帯性に優れた媒体として、ICカードが注目されています。これは、ICカードが耐タンパー性を持っていること、すなわち、ICカード自身がICカード内に格納された機密情報へのアクセスを制限し、機密情報の不正な読出し・複製を防ぐ機能を備えているからです。このため、ICカードを利用して、パソコンのログイン、起動制御、スクリーン・ロック等を実現するPCセキュリティ・ソフトウェアがさまざまなベンダーから提供されています。

PCセキュリティの分野だけでなく、最近では、プリンタ出力時に、プリンタキューにプリント・データを保持し、プリンタ出力命令をかけた者のICカードを認証した後に、印刷出力を開始するというセキュリティプリンタシステムも登場しています。一般に、オフィスでは共有プリンタが利用されているので、プリンタ出力の取り忘れや、印刷出力物を他人に持っていかれたりするといった経験は誰にでもあることでしょう。このように機密文書を共有プリンタに出力するオフィス環境では、セキュリティプリンタシステムが情報管理に非常に有効です。

3. IC カード化に際して

これまで見てきたように、物理的セキュリティ対策においても、技術的セキュリティ対策においてもICカードは重要な役割を果たしています。近年、ICカードはますます記憶容量が増加しつつあり、これら複数の機能を1枚のICカードに搭載することも可能になってきました。

ただし、複数の機能を1枚のICカードに搭載する場合には、ICカードを初期発行するまでに、あらかじめ、導入予定のICカード利用システムの各々について仕様を詰めておく必要があります。その理由は、ICカードを発行する際には、カード内のファイル・レイアウトを決めたうえで発行しなければならないからです。

企業の社員証・職員証カードといったIDカードは、一般に5年間程度の有効期間のカードとして発行されます。企業を取り巻く社会的要求・技術的環境が変化のスピードを、加速度的に速めている時代に、あらかじめ5年先までを見据えたセキュリティ・システム設計は困難です。結果的に、社員証ICカードを発行してから2年後には、セキュリティプリンタシステムの導入により、社員証とは別に、もう一枚のICカードを持たされることになったりしかねません。配付済の社員証ICカードを回収して破棄し、作り直しをすることは現実的ではないからです。同じ社内であっても、部門ごとに異なるベンダーのゲート管理システムが導入されることもあり、それぞれのゲート管理システム独自のカードを社員証ICカードとは別に持たなければならないケースも今後ますます生じることでしょう。

4. IC カードを核とした物理的セキュリティと技術的セキュリティの融合

このように、新たなセキュリティ・サービスを追加するたびにICカードを保有しなければならない枚数が増えてしまい、結果として利用者の利便性を損ねるという課題がありました。これを解決しようとして生まれた企業連合がSSFCアライアンス(Shared Security Formats Cooperation)です。SSFCアライアンスには入退館(室)管理システム、プリンタ・FAX・コピー機、オフィス什器、監視カメラ等、セキュリティ・システム各分野の主要ベンダーと、システム・インテグレータ等、合計100社以上が参加しています。SSFCアライアンスでは、これら複数のセキュリティ・システム分野のベンダーが共有できるICカード内のフォーマット仕様を策定し、ハードウェアベンダー系のメンバー企業は、このフォーマットに対応した機器を製品化します。

SSFC仕様に準拠したICカードとSSFC仕様アプライアンス製品機器の連携イメージの一例を述べましょう。SSFCカードを使ってゲートを通過すると、ゲートシステムはログを出力し、同時に監視カメラに対してゲートを通過した人物のSSFCカード内情報(ID番号など)を通知します。監視カメラは人物の画像をSSFCカード内情報(ID番号など)でインデックス化して録画します。ゲート内の執務室ではゲートを正しく通過した人物だけがパソコン、プリンタ、書類キャビネットを使うことができます。プリンタ等の各種機器は、ID番号付でログを出力しますので、セキュリティ管理者はインデックス化された画像から瞬時にID検索が可能となり、各機器から出力されるログ情報と合わせセキュリティ運用監視に目を光らせることが可能となります。

SSFC仕様の特長の一つに、カード所持者の所在場所情報を、ICカードを介してSSFC仕様セキュリティ機器に伝達する機能があります。SSFC仕様のゲートを通過したという情報がSSFCカードに記録されるので、この在室情報を利用すると、SSFCカード所持者に様々なセキュリティ・ソリューションを与えることが可能になります。

誰が、いつ、どこで、何をしたかを1枚のIDカードで、権限を与え、監査証跡を残すことが可能となります。

初期導入時に将来を見据えたセキュリティ・システムの設計が必要な従来のICカードと異なり、1枚のSSFCカードの導入運用から始めれば、SSFCアライアンスに参加する多数の有力ベンダーの製品群の中から、適切なタイミングで、適切な機器の導入が可能となります。

本稿で考察したセキュリティ・システムは、以下の点において優れています。

- セキュリティ対策への投資に対する経営層の理解が、得られやすい仕組みである
- 継続的なセキュリティ投資が可能な仕組みとなっている
- マルチベンダーでセキュリティ・システムを構築できるので、コストダウンが見込める
- 確実なログ情報が、ID番号付で収集できる
- 物理的セキュリティ対策と技術的セキュリティ対策を融合できる仕組みであるため、より高いセキュリティ効果を得ることが可能な仕組みとなっている

参　考

平成17年度 個人情報の保護に関する法律施行状況の概要、平成18年6月 内閣府
第20次 国民生活審議会 個人情報保護部会 第8回(平成18年6月30日) 資料6
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20bukai-index.html

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン、平成16年10月、経済産業省
http://www.meti.go.jp/feedback/data/i41013bj.html

セキュアプログラミング WG

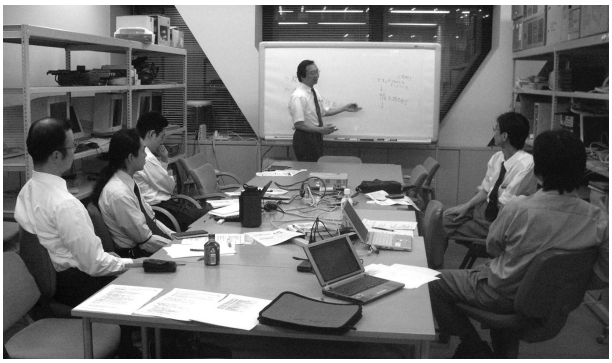
WG リーダー
株式会社 情報数理研究所　伏見　諭

■ いまなぜセキュアプログラミングか？

セキュアプログラミングは以前からある話題です。2、3年前に、e-Japanの重点項目の一つにひょっこり取り上げられて、脚光を浴びるかと思いきや、きっと課題があまりにも大きすぎたのでしょう、ある程度の普及を果たして後、マスコミ的な話題としてはすぐに下火になってしまいました。もっとも「アプリケーションセキュリティ」として見たときのWebのセキュリティは、さすがに一つの重点的な項目から外れることはありません。しかし、これも困難さはセキュアプログラミング全体と同様に大きなものです。

話題として派手になりえない要因は次のようなことが挙げられるかもしれません。

- 開発者のプロフェッショナルな課題だと思われるので、利用者サイドが自分の問題と思わない。
- 開発者は、そのような問題があるのは知っているが、日々の仕事の中でどうとりあつかえばよいか確信が持てない。
- 開発企業は、元来そのような問題を企業の問題でなく個別の開発者の能力の問題だと思っているので、組織的な取り組みをするところがごく少ない。
- 問題自体が大きすぎて、個々のエンジニアの手に負えるものではないので、いつの間にか実践的には忘れられる。
- 商業雑誌の編集者は、啓蒙的話題で読者の興味をあまり引かないと思うので、重点的には取り組まない。



しかし、これらの背後で問題は当然深く潜伏して、日々「セキュアでないプログラム、システム」が量産されています。もっとも、系統的ににソフトウェアを作成していくコミュニティ、企業では、セキュアプログラミングの重要性はいやでも認識されています。いろいろなオープンソフトコミュニティや、マイクロソフトのような企業はセキュアプログラミングの推進母体の一つとなろうとします。しかし、ソフトウェア、システム開発全体として見れば、対応も盛り上がり方も不十分なままです。

JNSAは、「ネットワークセキュリティ」という用語を名称として持っていて、このセキュアプログラミングの推進役としてはちょと畑が違うかなと思われる方もおられるかも知れません。しかし、それにかまうことはないでしょう。少し腰を落ち着けて、必要な技術テーマを知恵を出し合って深堀りしてみませんか。単純に頭の体操としても面白い話題がたくさん転がっています。また、それを実際の開発・運用業務につなげていくことも十分手ごたえがあるテーマだと思います。

■ スコープ

セキュアなシステム、ソフトウェアの実現を「開発者自身の話題」として、技術的に問題とすべきすべての領域。広く言えばこれにはWebセキュリティも含まれますが、そのタイトルのWGはすでにJNSAの中にありますので、Webの話題は比較的軽く、必要なら一つの話題として扱いましょう。

上流のアーキテクチャや分析・設計の話題、狭い意味のプログラミングの話題、テストの話題、運用の話題、セキュア機能コンポーネントなどを含みますが、このWGでは現場的な目で見ることを重点としていきたいと思います。

■ 想定成果物

今のところ決まっていません。しかし、せっかく活発な方が多く参加されていますので、単に勉強会に終わるのではなく、開かれた成果物につなげて行きたいと思っています。

■ 当面の活動

活動を立ち上げたばかりで、現在は参加者の問題意識を相互に提示しあうことで、問題領域を整理することを行っています。広めにJNSA内の問題の捉え方を調査するアンケートなどの提案、課題を研究・整理する活動の提案、基礎的脆弱性情報(個別の製品の脆弱性でなく)を整理蓄積する活動の提案、セキュアプログラミングルールの整理・提示の提案などが出されていますが、これらをどうするかは参加メンバーの皆さんの意向で決まります。

問題意識のある方はぜひ参加してみてください。

また、WGへの参加形態も、ミーティングのほかにML上での討議参加などいろいろな形が考えられると思います。これも今後具体的にしていきたいと思います。

セキュリティリテラシーベンチマーク作成 WG

WG リーダー
株式会社 JMC リスクマネジメント　大溝　裕則

当該WGは、経済産業省委託事業である「セキュリティリテラシーベンチマーク作成」を担うWGとして発足した。企業で働く一般社員、派遣社員などを対象とし、個人のセキュリティ知識やリテラシーの向上を目的としている。最終的には、各企業の社員のセキュリティ理解度チェックにも活用出来るようなものを目指したいと思っている。

1. WG の活動目的

昨今では、通常の生活のみならず企業における一般業務においてもメールやインターネットの利用は不可欠であるが、利用においての正しい知識が無ければ個人が被害を被るだけでなく、企業そのものが意図せずに加害者になってしまうような情報漏えい事故が頻繁に起きかねない。昨今のセキュリティ事故事例でも、管理者のミスや誤設定よりも利用者のセキュリティリテラシー不足から起きている事件事故が多くなっている傾向がある。利用者である一般社員や派遣社員に対しても、自己のセキュリティ知識レベルをきちんと把握でき、足りない知識を補うことができるようなしくみが必要と考え、その一つとして、Web上で簡単にチェックできるようなセキュリティリテラシーベンチマークを作成することとなった。

2. WG の年間活動予定

5月にWGを発足し、これまでに3回の会合を開催し、サンプルテスト問題の作成とテスト問題のカテゴリー決めを行った。現在は、テスト問題100問の作成を目標に、メンバーで問題作成を行っている。9月には問題を完成させると同時に、Webページの構築を進め、12月には完成、正式公開を目標としている。

それと同時に、来年度以降に向けてこのベンチマークを利用したビジネスモデルの検討も進めていく予定である。将来的には、ベンチマークを行った結果、足りない知識を補完できる教育とリンクできるようなしくみを作り、JNSA会員企業で教育ビジネスを行っている企業ともうまくリンクができるような方向でも検討をしている。

3. 予定成果物

セキュリティリテラシーベンチマーク

◆メンバーリスト（社名昇順）

株式会社インフォセック	山崎 貴子
エヌ･ティ･ティ･コムチェオ株式会社	吉川 昌吾
エヌ･ティ･ティ･コムチェオ株式会社	荒木 淳
株式会社 大塚商会	平井 健一
株式会社 大塚商会	持田 啓司
株式会社JMCリスクマネジメント	大溝 裕則
株式会社JMCリスクマネジメント	嘉代 賢嗣
セキュリティ･エデュケーション･アライアンス･ジャパン	小林 佑光
セキュリティ･エデュケーション･アライアンス･ジャパン	千原 遊子
株式会社ディアイティ	寺井 広貴
株式会社ディアイティ	藤井 雅展
日本ユニシス株式会社	長谷川 長一
富士ゼロックス株式会社	八巻 達也
株式会社ブリッジ･メタウェア	平田 敬
マカフィー株式会社	若林 勝広
リコー･ヒューマン･クリエイツ株式会社	勝見 勉
リコー･ヒューマン･クリエイツ株式会社	内田 茂

会員企業ご紹介⑰

アイネット・システムズ株式会社

http://www.ains.co.jp

AINET SYSTEMS Inc.

ネットワーク・フォレンジック
ー企業法令遵守の姿勢を育てるー

NetRAPTOR

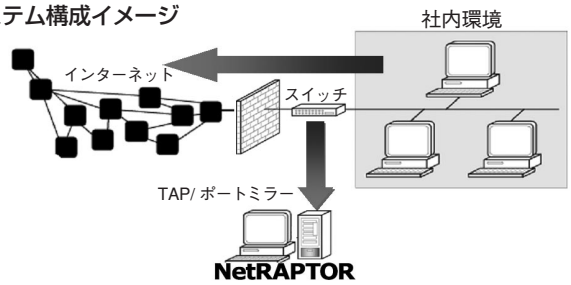
企業活動におけるIT利用の日常化に伴いネットを介した情報流出等､関係者を悩ませる問題は年々増加傾向にあります。また｢日本版SOX法｣施行が迫る中、いつ・だれが・どの情報を扱ったのか管理・記録することで企業としての責任を明確にしようとする‘内部統制重視’の姿勢は今後加速・浸透していくことが予想されます。

NetRAPTORは通信データの採取・保存をすることで情報を扱う社員の意識を向上させ企業法令遵守の姿勢を育てることを基本としながら、いざいうときは強力な検証機能をもって追跡調査を行い、企業としての責任を果たすことを支援する情報セキュリティ監査アプライアンスです。

■基本機能
- 通信データをすべて取得
- Web、メールデータの再現
- 強力検索
  ⇒キーワード･日時･プロトコル･IPアドレス･MACなど
  過去データを添付ファイル内まで詳細全文検索!
- リアルタイムアラート
  －不適切な通信には管理者へ報告

■特　徴
- 溜まったデータはバックアップ可能(NAS･SAN･テープ)
  ⇒ストレージへの直接検索可能!
- 一台構成でもデータ採取を止めることなく監査･バックアップ可能

システム構成イメージ



電子ファイル転送システム　*easyFiLEX*　そのファイル、メール添付で本当に安心ですか？

こんなことありませんか？

☆添付メールを送ろうとして...
- ●宛先アドレスを間違えた!
- ●容量が大きすぎて送れなかった!

☆無料ASPサイトならどうだろう...
- ●利用者が集中する時間になると使いにくい。
- ●不特定多数のユーザがアクセスするため
  安全性に不安がある。

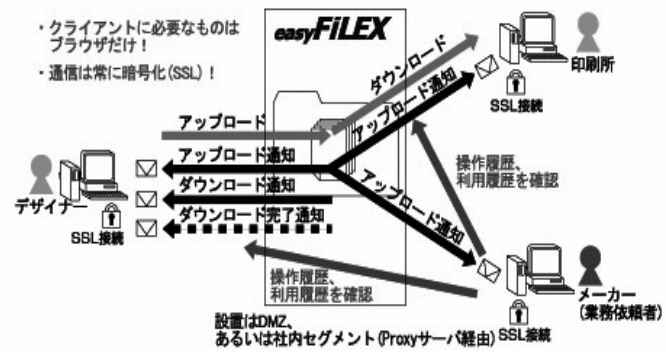
***easyFiLEX* なら…**

☆安全なデータ送信!
- ●暗号化通信を利用。
- ●利用ユーザを登録･管理。

☆送信ミスによる混乱を防ぐ!
- ●宛先アドレスの入力が不要。
- ●送信後でもファイルを削除することができる。

☆通信の混雑やサーバーの容量制限 の問題を解決!
- ●自社でサーバーを管理することにより、容量制限を
  自分で設定できる。
- ●データ送信･利用履歴を保存することができる。

■ご利用イメージ■



※製品に関するお問い合わせは・・・

アイネット・システムズ株式会社　ネットワーク事業部
〒542-0081 大阪市中央区南船場 2-9-8
シマノ住友生命ビル 3F
TEL: 06-6282-1760　FAX: 06-6282-1762
e-mail:net_sales@ains.co.jp
お気軽にご連絡下さい !!

NetRAPTOR 及び easyFiLEX は株式会社イージーネットの登録商標です。

株式会社ジュリアーニ・セキュリティ & セーフティ・アジア

http://www.gssa.jp

GIULIANI
SECURITY & SAFETY ASIA

NYCで実績をあげたセキュリティ・コンプライアンス策定、事業継続プランをあなたの企業にも。ジュリアーニ前NY市長ならびに当時のスタッフが最適なセキュリティ・コンサルティングをご提供致します。

ジュリアーニ・セキュリティ＆セーフティ・アジア(GSSA)は、ジュリアーニ前NY市長が設立したジュリアーニ・パートナーズの子会社、ジュリアーニ・セキュリティ＆セーフティの日本法人です。ニューヨーク市を実際に立て直したスタッフと連携し、IT、物理、組織セキュリティを統合したOneStop Full-Circle Securityのセキュリティ・コンプライアンスの確立と事業継続計画(BCP)策定をサポートします。

GSSA OneStop Full-Circle Security

ITセキュリティ
企業の通信システム、コンピュータ、ネットワーク、データが内部、外部、双方の発信源から受ける脅威

組織セキュリティ
不正行為を阻止するための適切な方針や手順が実施されない場合の脅威

物理セキュリティ
自然事象、人為的事象の双方によって脅かされる施設や機器に対する脅威

GSSA OneStop Full-Circle Securityの有効性

現状の問題点
- ITリスク、物理リスク、組織リスクにはかなりの重複部分と共存部分が存在
- 各セキュリティ問題の間には相関性があり、セキュリティに対するパッチワーク的アプローチは意味をなさない
- 各パッチに不安定なギャップが生じ､効率も悪化。セキュリティ投資が無駄になる場合も発生

解決策
- 完全に一体化した形で3つのリスクカテゴリー（ITリスク、物理リスク、組織リスク)のすべてに対処するために開発した独自のセキュリティ手法
- 「サークル」は連続的で、いずれのアプローチ・ポイントでも一貫した強度を発揮

このコンセプトを土台として、GSSAは各クライアントのニーズに合わせて、クライアントのセキュリティ環境のあらゆる側面を考慮しながらバランスの取れたセキュリティコンサルティングを提供します。

GSSA OneStop Full-Circle Securityは、国家、自治体、企業、個人の重要インフラの防御に従事した経験を持つ元公安官や元法執行官から成るチームの指揮の下で導入を実行します。

導入事例
- 国際空港
- 湾岸施設
- 大規模商用施設
- 大手プラント会社
- 大手警備会社　など

実績のあるセキュリティ・コンプライアンスの確立、事業継続計画なら

株式会社 ジュリアーニ・セキュリティ＆セーフティ・アジア
〒150-0001 東京都渋谷区神宮前5-52-2
青山オーバルビル14F
電話: 03-5485-7080 FAX:03-5485-2122
e-mail: info@gssa.jp

ソラン・コムセック コンサルティング株式会社

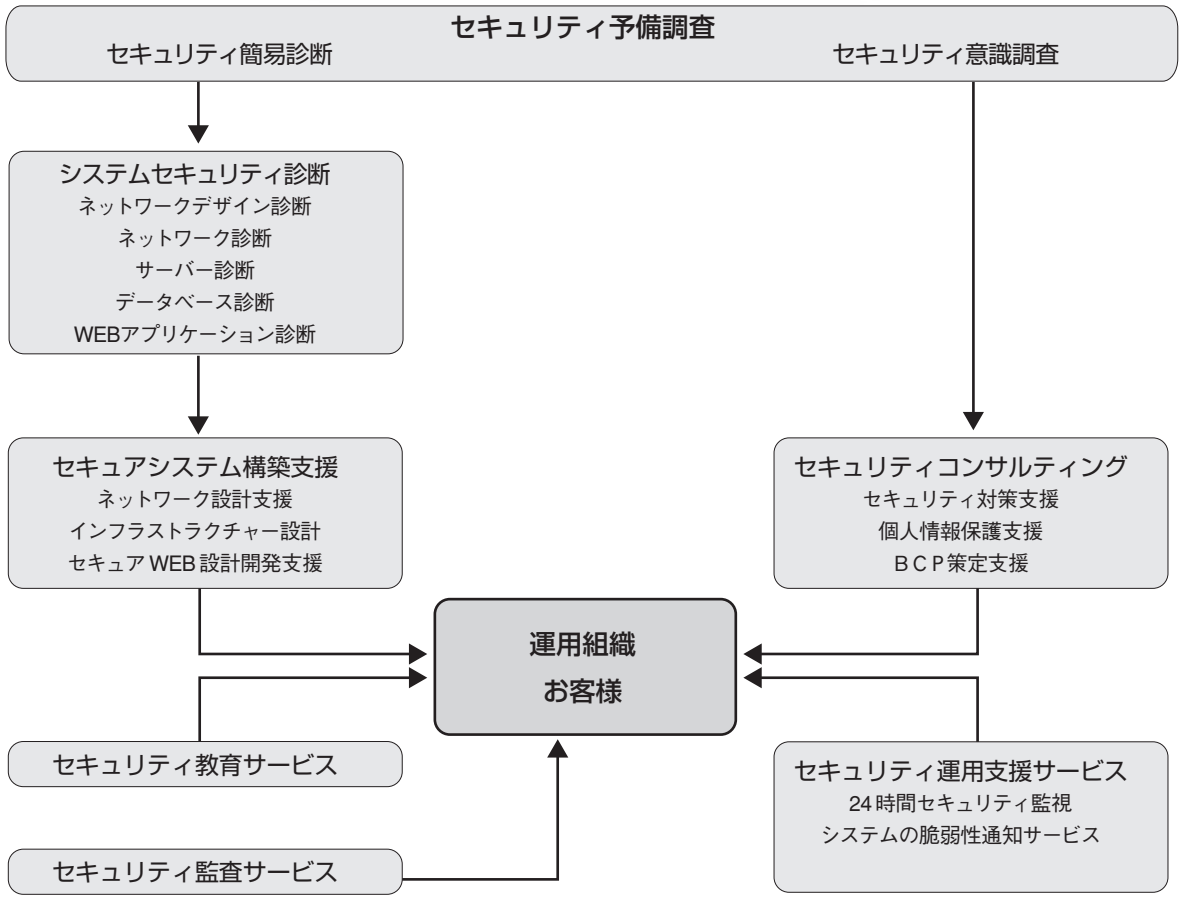
http://www.sorun-comsec.co.jp

SORUN-COMSEC CONSULTING

豊富なノウハウと経験を活かし多角的に情報セキュリティを支援

高度情報化社会では、情報セキュリティにかかわるさまざまなリスクが企業を取り巻いています。このリスクをいかに取り除くかということは、企業の経営戦略上、不可欠の課題です。当社では、企業の情報セキュリティをトータルにご支援するコンサルタントとして、お客様のビジネスをサポートします。
セキュリティ対策の立案(PLAN)から実施(DO)、点検·監査·監視(CHECK)、改善(ACTION)の4つの局面において、組織的、人的、物理的、技術的の4側面それぞれの対策を提供する事により、お客様の情報セキュリティをトータルにサポートいたします。

当社のコンサルティングフロー



お問い合わせ先

ソラン・コムセックコンサルティング株式会社

〒108-0073 東京都港区三田 3-12-16

TEL 03-5442-7901 FAX 03-5442-7860 e-mail:sec-info@sorun-comsec.co.jp

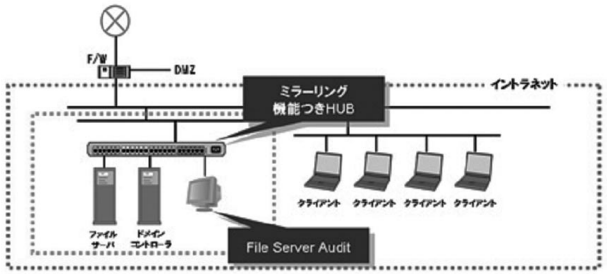
株式会社日本システムディベロップメント

http://www.nsd.co.jp/

株式会社日本システムディベロップメントは、1994年にMcAfee社の国内総代理店としてウィルス対策ソフトを販売開始しました。ウィルスの脅威がまだ企業で認識されていなかった頃からセキュリティへの取り組みをはじめた当社は、その後セキュリティ関連製品の開発や取り扱いを拡大してきました。近年では多様化するマーケットニーズに迅速かつきめ細かに対応するため、長年のシステム開発のノウハウと10年以上のセキュリティパッケージベンダとしてのノウハウを融合した、弊社独自のセキュリティパッケージを企画/開発/販売しています。
今後も製品販売のみならず、各種コンサルティングやサポートサービスを充実させ、セキュアなビジネスが展開できるシステム環境を提供して行きます。
今回は、弊社が独自に企画及び開発している二つのソリューションについてご紹介します。

クライアントPC、ファイルサーバにソフトの導入が不要のアクセスログ監査システム『File Server Audit』

『File Server Audit（ファイルサーバオーディット）』は、共有ファイルサーバで管理されるファイルに対する操作履歴を収集、解析する製品です。
共有ファイルサーバのファイルに対して、誰が、いつ、どのような操作を行ったのかが記録されますので、共有ファイルサーバに格納されている個人情報や機密情報が、適切に利用されているかどうかを容易に把握することができます。
個人情報保護法の施行、各省庁における情報セキュリティガイドライン策定などにより、ファイルの操作履歴を収集する必要性が高まり、数多くの操作履歴を管理する製品が発売されていますが、利用者のパソコン一台一台にソフトの組み込みが必要など、導入や運用に際し情報システム担当者に対する負担のかかる製品がほとんどです。
『File Server Audit』は、ネットワークを流れるデータを直接収集する方式を採用することにより、共有ファイルサーバや利用者のパソコンにソフトの組み込みが一切不要で、既存システムにほとんど影響を与えないソリューションを実現しました。更に、当社が独自に開発した仕組みにより収集結果を解析することで、利用者が実際に行った操作と一対一の操作履歴を出力することができるようになっています。



会社概要	
社名	株式会社日本システムディベロップメント （英名：NSD CO., LTD.）
設立	昭和 44 年 4 月 8 日
資本金	72 億 5 百万円 (平成 18 年 3 月 31 日現在)
従業員数	2,378 名 (平成 18 年 3 月 31 日現在)
事業内容	システム分析・設計の受託 / プログラム開発及び受託 / コンピュータ室運営管理 / ソフトウェアプロダクト

自動検疫チェックでウィルスパターン、セキュリティパッチの更新漏れゼロ『Secure Network Platform』

『Secure Network Platform（セキュアネットワークプラットフォーム）』は、社内ネットワークに接続しようとするPCに対し、

1）最新のセキュリティパッチ、ウイルスパターンが適用されているかチェック
2）企業ポリシーを満たしていないPCの社内ネットワークへの接続を拒否
3）隔離されたネットワークでセキュリティパッチ、ウイルスパターンを更新

の3つを行うことによって、セキュリティ対策済みのPCのみを社内ネットワークに接続可能とする、不正接続防止検疫ソリューションです。
従来の検疫ネットワーク製品では、検疫実行のために何らかのユーザ操作が必要でしたが、Secure Network Platformはネットワークに接続したタイミングで自動的に検疫を開始します。
セキュリティポリシーに合致しないPCは自動的に治癒まで行われる為、全社のPCのセキュリティレベルを一定に保つことができます。 また、ユーザ1人1人に対する検疫操作のユーザ教育も不要で、管理者に負担をかけません。

お問い合わせ先
株式会社日本システムディベロップメント
東京：〒 163-0777 東京都新宿区西新宿 2-7-1
新宿第一生命ビル
TEL : 03-3342-1369　FAX : 03-3342-0453
大阪：〒 541-0043 大阪市中央区高麗橋 3-3-7
NSD ビル
TEL : 06-7731-4607　FAX : 06-7731-0358
E-mail :『File Server Audit』fsa@nsd.co.jp
『Secure Network Platform』keneki@nsd.co.jp

株式会社ネットマークス

http://www.netmarks.co.jp

ネットマークス

ネットマークスは、メーカーにとらわれることなく時代に即したネットワーク構築というニーズの高まりを背景に、マルチベンダ環境でのネットワークインテグレータとして1997年に設立いたしました。
「We are here on customers' side」をスローガンに掲げ、お客様の立場で考えた最適なソリューションと誠実できめ細かなサービスの提供を目指しております。また、多くの導入実績により培った技術力とノウハウに基づき、付加価値の高いソリューションを提供しております。

<4つの基幹ビジネス>

当社は、IPテレフォニーなど企業内コミュニケーション基盤を統合するトータルVoiceソリューション、重要な情報を保全し、強固なネットワークセキュリティを実現するセキュリティシステム、情報をライフサイクルで管理し有効活用するためのストレージネットワークシステム、またシステムの運用・監視を行うアウトソーシングサービスの4つのソリューションを基幹ビジネスと位置付け、これらを融合させ、設計、構築、運用、監視、保守に至るまでトータルにお客様をサポートしております。
セキュリティソリューションについては、IT/セキュリティコンサルティングをベースに、最新の技術を取り入れたエンドポイントセキュリティ、マルチデバイス認証など幅広いセキュリティソリューションをご提供しております。また、お客様に代わりセキュリティシステムの運用・監視・保守を行うセキュリティアウトソーシングサービスも提供しております。

代表的なセキュリティソリューション

●IT/セキュリティコンサルティング

ITIL、COBITを活用した独自指標を用い、お客様のITシステムの現状分析やリスク分析を行い、対策方針や実装計画(IT実装策)のロードマップ案を提供します。

●フォレンジクスソリューション

クライアントPCの操作ログ収集による不正抑止から、異常検知、業務監査まで一貫したフォレンジック(監査証跡)基盤の構築をサポートします。万一の情報流出時にも原因を速やかに解明し被害拡大を防止します。

●マルチデバイス認証ソリューション

指紋、静脈等のバイオメトリクス認証やICカード、USBトークン、コールバック認証など多様なデバイス認証を利用環境に合わせて組み合わせることにより、強固で利便性の高い認証を実現します。
ネットマークス独自開発のマルチデバイス認証ソフトウェア「SecureSuiteXS」は、バイオメトリクス認証やICカード、USBトークンなど複数の認証方法を組み合わせて利用できるため、ネットワークやアプリケーションのログオン認証を強化します。また、Active Directoryに対応しているため、複雑なユーザ情報管理を容易に行うことが可能です。

(SecureSuiteXS ユーザ認証画面)

●アイデンティティ・アクセスマネージメント

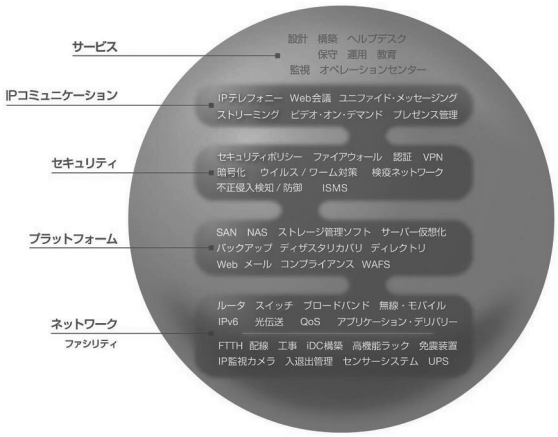
ユーザID(個人識別情報)やパスワード、アクセス権限の設定や管理を一元化します。複雑な企業内システムの統合管理を可能にすることで、業務の生産性向上、管理コストの削減に寄与します。

お問い合わせ先
株式会社ネットマークス　マーケットコミュニケーション部
〒107-0051 東京都港区元赤坂 1-3-12
TEL: 03-3423-5782　FAX: 03-3423-5902
E-MAIL: info@netmarks.co.jp　URL: http://www.netmarks.co.jp

ネットワンシステムズ株式会社
http://www.netone.co.jp

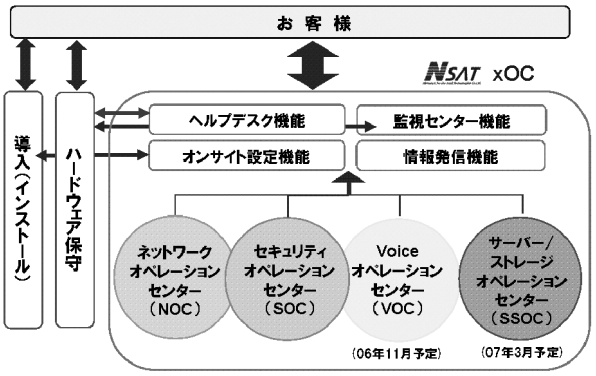
ネットワンシステムズのセキュリティサービス
～コンサルティングに始まりインテグレーション、運用サービスまで一環してご提供～

■ネットワンシステムズの事業領域
ネットワンシステムズは、従来からご提供しているCisco製品の販売・ネットワーク構築に加えて、現在では、サーバーやストレージの販売・構築を請け負うプラットフォーム事業、ネットワーク全般のセキュリティレベルを高めるセキュリティ事業、IP電話や会議システムの販売・構築を請け負うIPコミュニケーション事業、これらシステムの導入・保守・運用などのお手伝いをするサービス事業など、大きく5つの事業領域でお客様のご要望におこたえしております。



■セキュリティ事業の概要
ネットワンシステムズのセキュリティ事業は、お客様ネットワークのリスク分析から対応策のご提案まで総合的なサービス提供を行う「情報セキュリティ強化支援サービス」などコンサルティングサービスから始まり、お客様のネットワークに最適なセキュリティソリューションを導入するインテグレーションサービス、それらの運用を一括して請け負うエキスパートオペレーションセンター(以下、XOC)によるサービス、教育サービスという、4つのサービスをご用意しております。

■エキスパートオペレーションセンター
中でもXOCは、ネットワーク、サーバー/ストレージ、IP電話など、物理的な設置場所・形態・機能が異なるお客様の情報資産の運用とセキュリティの維持を、IPネットワークを利用して弊社のエキスパートが監視・管理・検査などを代行する、従来にない統合的かつ集約的な高付加価値運用サービスの拠点です。



お問い合わせ先
ネットワンシステムズ株式会社
〒140-8621
東京都品川区東品川2-2-8 スフィアタワー天王洲
ネットワンセキュリティセンター
TEL:03-5462-0833
E-mail : security@netone.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■

○『AntiMalware（アンチマルウェア）』

「アンチスパイウェア」と「アンチウイルス」のダブルエンジンを搭載した『AntiMalware』は、ワンクリックウェアを含むスパイウェア、キーロガー、ウイルス、ワームなどのマルウェア、およびWinny、WinMX、Shareなどのファイル交換ソフトに対応した法人向けマルウェア総合対策ソフトです。海外産に加え、国産のマルウェア対策を強化しインターネットに潜む様々な危険から企業のPCと情報を守ります。※ASPサービス版もございます。

【製品情報詳細】
http://www.ahkun.jp/product/am.html

◆お問い合わせ先◆
株式会社アークン
TEL: 03-5294-6065
E-mail: sales@ahkun.jp

○MSIESER（エムシーサー）

MSIESER（エムシーサー）はネットワーク上の通信を記録し、必要な時に解析･復元して
ネットワーク利用を監視する「フォレンジック･サーバー」です。
日本版SOX法や新会社法で要求されている「ITによる内部統制」や情報漏洩対策として
抑止･監査･証明･記録･証拠に威力を発揮します。
また、誰が･いつ･何を･どのように･何のために･･･を素早く解明します。
内･外部の不正利用者･痕跡を追跡、発見して解明する手段をご提供します。

【製品情報詳細】
http://www.ryoyo.co.jp/index.shtml

◆お問い合わせ先◆
菱洋エレクトロ株式会社
システム情報機器営業第2本部 MSIESERプロジェクト
TEL: 03-3546-5040
E-mail: msieser@ryoyo.co.jp

○EnCase Enterprise（エンケースエンタープライズ）

EnCaseはネットワーク越しに調査が可能なフォレンジック製品の決定版です。RAM上のデータやHDDをビットレベルで調査することが出来ます。また内部調査(eDiscovery)やインシデントレスポンスで時間とコストを大幅に削減できます。これらの調査結果は法廷証拠として全米で認められており多くの実績があります。COSOを基準とするSOX法にも有効利用できNIST（米国技術標準局)は2003年にEnCaseのForensicを正式認定しています。

【製品情報詳細】
http://www.encase.jp/

◆お問い合わせ先◆
株式会社ワイ･イー･シー
http://www.kk-yec.co.jp/inquiry/inquiry01.html

○HP OpenView Select Identity

Select Identityは、セキュリティポリシーに応じた、ユーザアカウントの登録、変更、削除といったIDライフサイクルに応じた設定をITシステムへ迅速に自動化する「IDプロビジョニング」をおこないます。
優位性として、業界No.1の使い勝手の良さ、簡単な配備ができることがあげられ、HP社全体で利用されています。
ユーザ管理やリソース利用にかかる作業を減らしコストを削減し、ITリソースへユーザを素早くアクセスさせることで生産性を向上させる利点があります。

【製品情報詳細】
http://www.hp.com/jp/openview/

◆お問い合わせ先◆
日本ヒューレット･パッカード株式会社
ソフトウェア･マーケティング部
E-mail: openview_jpn@hp.com

○ネットワークフォレンジック「NetRAPTOR」

NetRAPTORは通信データの採取･保存をすることで情報を扱う社員の意識を向上させ、いざというときには強力な検証機能をもって企業の説明責任を果たす支援をする情報セキュリティ監査アプライアンスです。
インターネットの私用閲覧、ネット掲示板への書き込み、Webメール、メール添付ファイルなどの通信を調査･再現し不適切な利用を発見します。

【製品情報詳細】
http://www.eni.co.jp/netraptor/index.html

◆お問い合わせ先◆
アイネット･システムズ株式会社
ネットワーク事業部
Tel:06-6282-1760　Fax:06-6282-1762
E-mail: net_sales@ains.co.jp

○「NOD32アンチウイルス V2.5」

「NOD32アンチウイルス V2.5」は、ウイルス定義ファイルにはない未知(新種)のウイルスを検出するウイルス対策ソフトです。独自のヒューリスティック機能を用いて、プログラムコードを素早く解析し、非常に高い確率でウイルス侵入を防ぎます。また、次世代のハイパフォーマンスな動作を可能にする

64ビットOS環境にもいち早く対応し、高速かつ軽快に、既知・未知のウイルスから守ります。

【製品情報詳細】
http://canon-sol.jp/product/nd/

◆お問い合わせ先◆
キヤノンシステムソリューションズ株式会社
E-mail: nod-info@canon-sol.co.jp

■ サービス情報 ■

○個人情報漏えい緊急対応サービス【個人情報119】

セキュリティインシデントに対して業界でも屈指の支援実績をもつ当社ラックがご提供する、個人情報漏えい事件のお助けサービス。
SQLインジェクションなど各種脆弱性をついた個人情報漏えい、Winnyによる情報流出事件などに際して、被害拡大の防止策、謝罪、関係機関への届出支援、メディアへの公表手続きに関するアドバイス、復旧支援に至るまで、一括してサポートします。
困ったとき、まずはご一報ください。

【サービス情報詳細】
http://www.lac.co.jp/p119/index.html

◆お問い合わせ先◆
株式会社ラック 個人情報119担当者
E-mail: p119@lac.co.jp

■ イベント情報 ■

○HP Software Forum Tokyo 2006

HPソフトウェアの年次イベントである「HP Software Forum Tokyo 2006」が来る9月中旬に開催されます。
【日　時】2006年9月19日(火)
10:00～18:30（受付開始 ： 9:30）
【会　場】東京コンファレンスセンター 品川

アクセス制御、パスワード管理、ユーザープロビジョニング、さらには連携アイデンティティに関して、海外講師による特別セッション『コンプライアンスからみた、ID管理の基礎~HP OpenViewソリューションと海外先進事例での考察~』が同日16:30から開催されます。
この他、ID管理最新製品デモも展示されます。

【イベント情報詳細】
http://www.hp.com/jp/swf2006/

◆お問い合わせ先◆
日本ヒューレット・パッカード株式会社
HPセミナー事務局
E-mail: call.hp@hp.com

○BCM(事業継続管理)実践トレーニング
－ワークショップ付3日間コース(同時通訳付)－

【日　時】平成18年9月11日(月)～9月13日(水)
10:00～17:00（開場9:30）
【会　場】全国農業共済会館3F テクノ研修センター

BSIとともに英国事業継続協会(BCI)がBCMの仕様として開発したPAS56、さらにBS25999へと進化しISO化が検討されているBCMに関する日本で初めてのBCI認定講座。
BCMで先進している英国において数多くのコンサルティング実績を持つ専門家が講師として、業務プロセスの重要性、相互依存性、継続のための要件、リスク、影響度分析などワークショップを交えた内容。

【イベント情報詳細】
http://www.itpg.co.jp/news.html

◆お問い合わせ先◆
株式会社ITプロフェショナル・グループ
E-mail: contact@itpg.co.jp
TEL 03 (3583) 8240　FAX 03 (3583) 8669

JNSA 西日本支部主催セキュリティセミナー

株式会社サイロック　松原　裕正

日本ネットワークセキュリティ協会西日本支部主催の第 8 回セキュリティセミナーが近畿経済産業局、大阪商工会議所、財団法人関西消費者協会、社団法人関西経済連合会の後援のもと、3 月 16 日（木）に大阪市北区にあるコンベンションルーム・アクスネッツにおいて開催されました。
当日は残念ながら雨天でしたが、約 100 人（～ 120 人）の方にご来場いただきました。
今回は「コーポレートガバナンス強化に直面する中小企業のセキュリティ対策について」をテーマとした、今後の中小企業における新たなセキュリティ対策の方向性が示されるセミナーとなりました。

初めに

まずJNSA西日本支部中台芳夫氏より、JNSAの各部会が行っている様々な調査活動や、ワーキンググループの活動内容のご紹介をいただきました。

アメリカではSOX法の導入によって、情報セキュリティ対策を核としたITガバナンスの見直しが進められています。そして日本でもアメリカと取引のある会社を中心に、セキュリティ対策の見直しが始まってきています。

それに対し中台氏は「この動きはひょっとすると2008年3月からの日本版SOX法の導入が予定されていることを考えますと、今後の企業活動に影響するというふうに考えられます。またこの5月施行が予定されている新会社法においても内部統制システムの構築に関する方向性が示されるということで、今後中小企業に対し大きな課題をもたらすものと考えられます」と語られました。そしてコーポレートガバナンス、SOX法の概要についてふれられました。

「今回のセミナーでは関西圏に多い中小企業において企業の内部統制強化がどのような影響をもたらすか、そしてどのようなセキュリティ対策が新たにクローズアップされるかを明らかにしていきます」と話されました。

講演 1

中小企業向け個人情報保護対策 WG 活動報告

最初は「中小企業向け個人情報保護対策WG活動報告」と題し、WGメンバー 嶋倉 文裕氏(富士通関西中部ネットテック株式会社)より、一年間の活動報告及び今後の課題に関してご発表いただきました。

嶋倉氏はまず、個人情報保護法施行後一年が経過した現在、関心が高まってきているにも関わらずファイル交換ソフト(Winny等)のソフトを介して情報漏えい事故が多発しており、中小企業の間で個人情報をめぐって混乱があるのではないかと指摘されました。

「個人情報保護対策法の施行で中小企業はどんな状態に陥るのか。大企業と比較してできる対策はあるのか」という疑問を追及することがWG発足のきっかけでした。2005年2月に発足後、6月からモニタ企

業による実地検証を開始し、10月に中間発表、そして12月に2社目のモニタ企業のコンサルティングを行い、そして本日の結果発表となりました。

環境や規模も違う、扱っている情報内容も違う、それぞれの中小企業が、「個人情報保護体制の構築(Plan)、安全管理の実装(Do)、監査(Check)、対策の見直し(Act)」の一連のPDCAの仕組みを自分たちで運営できるようなものを作成したいという思いのもと、モニタ企業へのコンサルティングを通じた実地検証や、JNSA提供の雛形も参考にした中小企業の運用に適した形のテンプレートを検討し、様々なフィードバックを通じてテンプレートの完成度をブラッシュアップしてまいりました。

また昨年10月に行われたJNSAセミナーのアンケート結果報告と分析が行われました。

個人情報の趣旨は「個人情報をうまく使う」為のものであったはずなのに、経済活動の足かせになっているのではないか?と言う指摘や、個人情報保護法の施行を逆風とせず、個人情報保護の意識を高める事によって顧客評価が上がったところもあるという結果がありました。個人情報は使う為に持っている資産でありながら、守る事に一生懸命になって、使いにくくしている、自分で自分の肩身を狭くしているのではないだろうか、そのためにどうすればいいのかを考える事が課題だろう、と語られました。

情報管理の対策が担当者任せになっていること、個人情報に対して過剰な反応をしたり、なんでも個人情報として一括りにしたり、個人情報保護の対策が解らないという現状もまた見えてきました。

中小企業の現状として、個人情報に対する意識はあるが、どこまですればよいのか分からない所がまだまだ多く、技術的･物理的対策は重視されているが、組織的・人的な対策が軽視されている状態であることが分かりました。

そこでWGは「自分たちの課題・問題点が把握できていないのは、技術ではなくマネジメントに問題がある為」と考え、組織的対策を各々に分類する等、セキュリティヒアリングシートを工夫しました。具体的事例として台帳作成を挙げながら、中小企業における対策推進方法として、目標時期と成果を具体的に盛り込み、セキュリティヒアリングシートを個人情報保護体制のチェックシートとして加工し利用する、そしてチェックシートそのものが規定集の原案も兼ねるようになる事を発表しました。

対策と今後の課題について、「現状を把握しましょう。目標として何をして言いか分からないという声もありましたが、問題を把握していないのに目標はたてられません。次に共通意識を持ちましょう。これは中小企業の強みです。人数が少ないからこそできる。どういうことをしないといけないのかが、はっきり分かる。そして対策を検討しましょう。セキュリティヒアリングシートをベースにして、それを個人情報保護体制のチェックシートに加工し、いつまでに何をするのか目標時期と成果をはっきり書いて、PDCAサイクルをスパイラルアップしていきましょう。」と話されました。

情報セキュリティを大きな変化として、個人情報保護法の次に「日本版SOX法」「不正競争防止法改正」等が今後の課題として控えています。

最後にコンプライアンスルールを守る事が中小企業だからこそ大切であり、企業価値を高める事になるのではないか、とまとめられました。

講演２

企業価値の向上に向けた情報セキュリティ対策：目に見えない資産の重要性と内部統制

「企業価値の向上に向けた情報セキュリティ対策:目に見えない資産の重要性と内部統制」と題し、東京大学大学院情報学環の田中 秀行氏よりご講演いただきました。田中氏は情報セキュリティに対し経済的、経済学的な側面に立って話をされました。

田中氏はまず、情報セキュリティ対策には、ITに

イベント開催の報告

直接関係するソフトウェアやハードウェアだけではなく､｢目に見えない資産｣が重要であると語られました。実際に実証分析を確認すると｢目に見えない資産｣にどれだけ取り組んでいるかが情報セキュリティの水準を上げるという事が確認できましたので報告いたしますと述べられました。

IT技術が上がっても必ずしも情報システムのセキュリティ水準は上がっていないこと、組織のあり方も含む経済的動機付けについて考える事が重要であることについてふれられました。｢目に見えない資産｣として、ビジネスプロセスや組織内での意思決定権、情報共有や組織文化、人と人との関係、人材を挙げ、これらが、IT投資成功の鍵と述べられました。

また、セキュリティ水準を定めるものは｢取り組みの総和であり、最も弱い所であり、最も強い所である｣と説明され、相互依存性があり様々な例と共に問題点を喚起しました。

企業価値とセキュリティ対策について、情報漏えい事件や不正アクセス事件の報道後、情報セキュリティ・インシデントがあると短期的な株価の下落につながる事を話されました。

情報セキュリティ対策は企業価値を下げない為の、ネガティブな努力になりがちですが、日本企業を対象にした実証分析からすると｢セキュリティ対策をすると、企業価値が高くなる。むしろポジティブな評価がもらえる面がある｣と言う話をされました。情報セキュリティは、相互依存性があり、自分だけではなく相手にも一緒にやってもらうのが情報セキュリティである事、目に見えない資産は投資家も評価していると語られました。

そして｢国内情報セキュリティ調査の別冊で平成16年情報処理実態調査を用いた情報セキュリティ対策の実証分析に関する調査研究｣(JNSA調査)の結果から内容の分析が行われました。

2004年3月末のデータで情報通信機械製造業は8割がセキュリティトラブルを経験しており、金融・保険業・医療業の企業4割とやや低いものの、全業種平均で6割以上の企業がなんらかのセキュリティトラブルを経験しており、ウィルス感染は半数以上の企業が経験しています。

セキュリティ対策の実態に関して、4分の3の企業は何らかのセキュリティ対策をしているが、残りの4分の1の企業が対策をしていない。単一の対策しか導入していない企業が1割以上であると言う実態がアンケートの結果より分かりました。

また、企業の規模に関わらず、情報セキュリティ対策を投資額で把握できているのは一部の企業に過ぎませんでした。情報セキュリティ対策の費用対効果についても把握できているかという現状が示されました。企業の情報システムの状態とセキュリティトラブル経験の関係においてシステムの使用範囲が広いほどトラブル経験率は高く、電子メールID数が多いほどトラブル経験率が多く、電子メールIDあたりのIT経費が多いほどトラブル経験率は低い可能性があるという､面白い結果が得られたと報告されました。

セキュリティへの認識度合いとトラブル経験率の関係においては、セキュリティ・トラブルを重要と認識する度合いが高ければ高いほど、トラブル経験率は低いと言うことがいえそうです。

さらに、ファイヤーウォールだけをセキュリティ対策にしている会社ほどトラブル経験率は高いと言う結果より､｢安易にファイヤーウォールに頼っている所にトラブルが多い｣と言う指摘をされました。防御措置を単一手段に頼らず、ファイヤーウォールと、何かを組み合わせたり、またインフォメーションセキュリティポリシー等のセキュリティ・マネジメントや責任・教育体制と組み合わせる事により安全性が高まり、セキュリティ対策の効果が現れる。セキュリティ管理者を置く時に全社での管理者ではなく、部門ごとにセキュリティ管理者を置く場合にトラブル経験率が低いと話されました。

そして、個人情報保護法が成立されてから残業が多くなり生産性が落ちるという現象が起こっていて、セキュリティ水準を上げながら生産性も上げる為には

技術力が不可欠である事、また効果的なセキュリティ対策はハードウェアやソフトウェアに頼るのではなく、マネジメントや人材教育のような「目に見えない資産」への対策と補完的に行う事が重要であります。

内部統制においてIT関連パッケージを導入する事にとらわれることなく、むしろビジネスプロセス、目に見えない資産の見直しをする事が重要であり、そうする事で、内部統制が有効的に機能しはじめ企業価値を高めると述べられました。

企業活動は従来の組織の境界を越えつつあり、組織が異なっても一つのプロセスとしてまとまりを持つ「プロセス・エンタープライズ」へ移行しています。サプライチェーンマネージメントがわかりやすい例ですが、組織を越えたつながりが一連のプロセスとして把握できるようなEAやSOAはその動きを加速しています。例として自治体の電子化構想を述べられ、組織の境界を越えた動きが加速していると述べられました。

内部統制は、非公開の中小企業であってもプロセス・エンタープライズを前提とすると、内部統制は組織の境界内にとどまらず密接に関係している可能性が高くなってきている為にSLAやSLMの対応が求められるようになる。内部統制の構築についても「目に見えない資産」に効果的投資が重要であり、IT投資を通じて業務を効率化できる面や生産性を上げる面もあるのではないか、「守り」の話になってしまいがちですが、ビジネス環境に応じて積極的なIT戦略は残されているのではないかと最後に話されました。

質疑応答部分で、目に見えない部分への投資はどれぐらい掛ければいいかについて、ハードウェア、ソフトウェア部分より教育部分をしっかり考えておくことと、しっかり最初に計画しておく事が重要で、資料としてセキュリティ対策設計段階での投資を1としてメンテナンス運用部分でのセキュリティ投資が60倍もコストが掛かるということが言われていると述べられ締めくくられました。

講演３

内部統制のためのITフレームワーク

最後に「内部統制のためのITフレームワーク」と題して、弁護士であり、また宇都宮大学工学部講師をされている高橋郁夫氏よりご講演をいただきました。高橋氏はアメリカのSOX法との比較等を通し、日本版SOX法の位置づけを行われました。そして内部統制のチェックリストを提示され、内部統制のあるべき姿、そしてITフレームワークの構築に関しての話をされました。

まず、日本の現状として、日本の政府がここ数年で取り組んできた会社法改正や改正監査基準などがあり、金融商品取引法に関しては全体像が見えてきたところです。「監査品質の向上」を実現するために内部統制の構築に関する企業努力をどのように評価するかが仮題です。

COSOフレームワークといわれているものは、資産保全等の観点から内部統制が考えられており、経営者はきちんと評価を行った上で外部に向けて報告をせねばならず、また公認会計士等が監査を行い、それを担保しなくてはなりません。これが金融商品取引法案の要旨として平成１８年3月１０日に閣議決定されました。これをマスコミは日本版SOX法と呼んでいます。

また日本とアメリカ版SOX法との比較では、訴訟制度が非常に違う点が指摘されました。日本版SOX法が施行されるにあたり、社会に対する影響は少ないのではないかと考えられますが、取引先との間で「信頼性を確保して、きちんと問題が起きないように、ビジネスも継続します、情報を預かっても守っていけます。」と宣言することが、内部統制を構築するということである、と問題提起されました。

業務プロセスの改善を前提としなければ、内部統制の構築が役に立つかどうかは微妙です。なぜならSOX法は新しい概念というわけではないからであり、日本版SOX法がどのレベルを要求するのかの合意はこれからの課題なので、早く対応することが目的ではないのではないかと考えられます。

実際にITが関わる部分を含む内部統制を考える場合、COSOキューブと呼ばれる、ビジネスの全般をコントロールするモデルがあります。一方、ITセキュリティで必要とされる要素はどのようなものがあるか、各要素に対する制御機能を考え、ビジネスの目的、IT資源等との情報をうまくリンクさせるための橋渡しが「COBIT」というモデルです。これはIT資源に関する色々な観点(計画と組織、調達と導入、サービス提供とサポート、モニタリング)からビジネス目標や到達目標など、いろいろな項目ごとのチェックを行うアーキテクチャーとなります。

リスクを減らして機会を増やしていく、そのために利益や効率を上げ、制御機能として内部統制を考えていくことが、企業文化を根付かせます。内部統制の基礎として重要なのは企業文化なのです。
内部統制をいろいろな業務ごとに構築し、IT化するとERPパッケージという形になります。ERPパッケージを導入しようとする時、元々のプロセスの見直しが重要であり、なかなかうまくいかない場合があります。この時は、ITを離れてコーポレートガバナンスを考え直す必要があります。

内部統制は不正を防ぐものとして、自分たちの企業の立脚点と、構成員で押し進めていこうとする文化、何が正しく何が間違っているということを理解していこうとする構成員全員の意思と共通の方向性が必要です。内部統制のキーワードはtransparency(透明性)を保持し、何か問題が起こったときに「自分たちはこうしていましたよ」というaccountability(説明責任)、監査証拠を示す考え方が非常に重要であると締めくくられました。

終わりに

個人情報保護法の施行後、個人情報の取り扱いに対する戸惑い、一種の空気のこわばりがあるようです。個人情報の価値が叫ばれているにもかかわらず、winnyなどのソフトを介して個人情報が漏えいしている事件が新聞に載ることは、もはや珍しくありません。

企業に対して、ITセキュリティ対策やコーポレートガバナンスの見直し等、内部統制に関する要求は日々高まっています。

今回のセミナーにおいては内部統制の構築、ITフレームワークという形で取れる対策について、経済学的な視点から、また法律的、学術的な視点からの分析が行われました。またアンケート結果を通して、現在の企業が直面している問題が見えてきたと考えられます。

「企業はどこまで内部統制を、セキュリティ対策を行うべきなのか?」という問いに対して、「それはそれぞれの企業によって違ってきます」という答えが返りました。

内部統制の構築がネガティブな努力ではなく、企業価値の向上につながるポジティブなものになりえるということが、中小企業のコーポレートガバナンスのひとつの指標となりえるのではないでしょうか。

JNSA 2005 年度 ワーキンググループ成果報告会

JNSA 主席研究員　安田　直義
JNSA 研究員　松田　剛

2006 年 5 月 30 日、大手町サンケイプラザに於いて、2005 年度日本ネットワークセキュリティ協会成果報告会と定時総会が開催されました。ここでは、成果報告会の内容についてご紹介します。尚、当日のプレゼン資料などは下記の URL で公開されていますので、合わせてご覧ください。

http://www.jnsa.org/2006/seminar/20060530.html

成果発表会は下記のプログラムのように、2 部屋に分かれて平行して報告されました。今年度は、昨年の両方聞きたかった、というご意見を参考にし、発表の長さを揃え、トラック間の休憩時間を合わせることで、相互に行き来できるように配慮してみました。

2 トラックの 1 トラック目は、教育部会と技術部会、2 トラック目は政策部会と西日本支部が担当しました。次に報告内容について順を追ってご紹介して行きましょう。

303 号室		304 号室	
教育部会（10:30-12:00）		政策部会（10:30-12:00）	
10:30-11:00	CISSP WG NTT コミュニケーションズ 大河内 智秀氏	10:30-11:00	セキュリティ会計ガイドライン検討 WG 凸版印刷 佐野 智己 氏
11:00-11:30	情報セキュリティ推奨教育検討 WG セキュリティ・エデュケーション・アライアンス・ジャパン 持田 啓司氏	11:00-11:30	スパイウェア対策啓発 WG アークン 蛭間 久季 氏
11:30-12:00	情報セキュリティ教育実証実験プロジェクト JNSA 研究員 松田 剛氏	11:30-12:00	セキュア・システム開発ガイドライン WG ラック 丸山 司郎 氏
12:00-13:00 昼休み			
技術部会（13:00-15:20）		政策部会（13:00-14:00）	
13:00-13:30	脆弱性定量化に向けての検討 WG セコム 金岡 晃 氏	13:00-13:30	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
13:30-14:00	PKI 相互運用技術 WG セコム 松本 泰 氏	13:30-14:00	セキュリティ被害調査 WG ディアイティ 山田 英史 氏
14:00-14:20 休憩			
14:20-14:50	WEB アプリケーションセキュリティ WG 住商情報システム 二木 真明 氏	西日本支部（14:20-14:50）	
		14:20-14:50	中小企業向け個人情報保護対策 WG 伊藤忠テクノサイエンス 市川 順之 氏
14:50-15:20	不正プログラム調査 WG アークン 渡部 章 氏		

トラック1（303号室）

教育部会

午前中は教育部会からの発表が3件ありました。

CISSP-WG

NTTコミュニケーションズの大河内智秀氏から、CISSPに関する活動の報告がされました。CISSP-WGは2006年度からISSJP-WGとして活動していますが、2005年度の活動として、CISSPの上位資格として日本の状況、特に地方自治体などを念頭に置いたISSJPのCBK（Common Body of Knowledge）作成や問題作成などの活動チーム、作業ドメインについて説明されました。ISSJPのドメインは、法ドメイン、制度・政策ドメイン、技術ドメイン、倫理その他ドメインの4つで構成されており、2007年より試験開始の予定だそうです。

CISSPは世界で5万名くらいが取得しているITセキュリティに関する代表的な資格ですが、日本でのセキュリティ意識の啓発のためにももっと普及させたいとのことでした。

情報セキュリティ推奨教育検討WG

セキュリティ・エデュケーション・アライアンス・ジャパン（SEA/J）の持田哲司氏から、情報セキュリティ推奨教育に関する活動報告がありました。教育の必要性はどの組織でも8割は認識しているが、実装は難しい。ともすると売れるという観点だけから教育プログラムを作ってしまう。組織の中で必要かどうかではなく、対症療法的な教育になりやすいという現状認識の下、どのような教育が実際に行われていて、またどのような教育を行えばよいのかを整理するという目標で活動され報告書がまとめられているそうです。

一例として、内部統制に関するITへの対応例を考えるとき、IT成熟度診断や、ERP、BPM系ツールが利用されることもあるが、これらでカバーしきれない部分の限界についての対策として、教育が重要な役割を持ち、これをIT担当者、全スタッフばかりではなく、経営者の教育も重要だとの指摘がありました。また、キャリアパス形成についてのロードマップについての考え方の説明があり、これらは報告書として公開される予定とのことでした。

情報セキュリティ教育実証実験プロジェクト

JNSA研究員の松田剛氏から、東京電機大学、工学院大学、岡山理科大学で行われた、ITセキュリティの専門家育成コースの実施について報告されました。高等教育機関でも、ITセキュリティに関するコースは解説されていますが、どちらかというと暗号教育などの理論研究に偏っている節があるので、もう少し実践的な教育内容があってよいのではないか、という即戦力への期待が発端となっています。

教えられる側、教える側の意識調査結果や、地方の問題として、対応できる講師がいないという事案に対する問題提起と解決の提案がされ、2006年度の活動として解決案の実践が予定されているとのことでした。

技術部会

午後は技術部会からの発表が4件ありました。

脆弱性定量化に向けての検討WG

WGメンバーのセコムの金岡晃氏に発表していただきました。本WGの目的は、サーバーマシンを運用管理する現場技術者がパッチ情報などを当てるに際して、どのくらいの重要度があるかを定量的に評価しようというところから始まっています。このために、攻撃が発生するメカニズムをモデル化するにあたって、CVSSやMSの脆弱性評価とは異なる検証可能なモデルを作るアプローチを採っています。

モデル化を考える際に検討したのは、脆弱性とは何か？のコンセンサスを取ることであり、脆弱性の構

成要素を整理し、攻撃が発生した時の主体(エンティティ)をオブジェクトとし、オブジェクト間の関連(リレーション)について、良い影響／悪い影響を評価する方法論を取っています。このように、攻撃発生のメカニズムの解析を基にした数式モデルを作成し、Excelシートで数値計算ツールを試作しているそうです。観測可能な属性値を適用して、メンバー内でレビュウを行っているそうです。2006年度活動として、引き続き数値化の確定やツールの公開、報告書の作成を行う予定とのことでした。

PKI相互運用技術WG

セコムの松本泰氏からハッシュアルゴリズムの危殆化等に関して、SHA-1問題の背景と現状について解説されました。最近話題になっているSHA-1というハッシュ関数が事実上解読可能となってしまったことを踏まえ、一番弱いところが狙われるのは必定なので、ある時点で下位互換性を断ち切る大きな転換が必要であることが説明されました。しかし、多くのアプリケーション等の実装は、暗号アルゴリズムに依存した仕様になっている場合が多く、移行が難しい問題点が指摘されました。タイムスタンプはSHA-1からSHA-2に移行できましたが、広く普及する前だったので移行ができた面と、移行できたのは文書のハッシュのみで、時刻証明のハッシュはSHA-1のままという問題点があります。

米国の政府調達基準を作っているNISTでは2010年までしかSHA-1を許しておらず、SuiteB基準ではSHA-1, RSAを認めていないのは重要な点であることが説明されました。

WEBアプリケーションセキュリティ WG

住商情報システムの二木真明氏から、Webアプリケーションのセキュリティを確保するための技術的な活動についての報告がありました。2005年度は、啓発コンテンツ、受発注ガイドライン、技術分科会に分かれて活動していました。

受発注ガイドライン分科会の奥原雅之氏(富士通)から、絶対人が死なない自動車です、というような契約内容が横行しているという点が上げられ、瑕疵だ、欠陥だ、仕様だ、などの水掛け論を避けるにはどうすればよいか、という問題提起がされ,「Webリスクモデルのツリーモデル」について説明がありました。

2005年度は、メンバーが技術系の中核を担っているため多忙で思うような成果が出せなかったという反省を踏まえて、2006年度はテーマを絞り込んで活動する予定だそうです。また、WGリーダーの二木氏が技術部会長になるのに伴い、新WGリーダーとしてIIJテクノロジーの加藤雅彦氏に交代し、技術的な背景を持った経営層に働きかけられるようなコンテンツを作成する方向で活動を予定しているとのことです。

不正プログラム調査WG

最後にアークンの渡部章氏から、不正プログラム全般に対しての対策ガイドラインの改定版について説明がありました。不正プログラムを分類化し、タイプ別、進入経路別に対策ソリューションをわかりやすくまとめたものになっています。不正プログラム対策の3要素である、予防、検出、復旧について、企業規模ごとに対策の考え方をイラストで説明されており、不正プログラム対策10か条や、具体的なチェックシートとともに解かりやすいガイドラインになっています。

(安田)

イベント開催の報告

トラック 2（304 号室）

2トラック目には、政策部会から5件、西日本支部から1件の発表をしていただきました。

政策部会

午前中と午後の前半は政策部会からの発表が5件ありました。

セキュリティ会計ガイドライン検討WG

凸版印刷の佐野智己氏に冒頭の発表をしていただきました。「セキュリティ会計」とはまだあまり聞きなれない言葉ですが、環境会計に倣って企業のセキュリティ確保における取組みを適切に把握、評価そして伝達する仕組みを示すもので、2004年度から研究に着手しました。情報セキュリティの確保や評価が難しいのは、定量化すなわち「費用対効果」が明確化できないといった問題は以前から指摘されていましたが、セキュリティ会計WGではこうしたセキュリティが抱える本質的な問題に正面から取り組んでいることから、筆者も注目するWGの一つです。

スパイウェア対策啓発WG

アークンの蛭間久季氏にご報告していただきました。一般的には 情報漏えいといえばWinny事件が注目されていますが、キーロガーやワンクリウェア（ワンクリック詐欺）などの危険性は十分に認識されているとは言えません。蛭間氏はスパイウェアを「利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム」と定義づけたうえで、一般のPC利用者にそうした危険性と対策方針を普及する取組みを紹介しました。スパイウェア問題に関する取組みはいまだ各国で統一した動きが見られず、今後は北米、欧州、中国、韓国などの事情を調査し、日本独自の対策方針を提言することを目標としています。

セキュア・システム開発ガイドラインWG

ラックの丸山司郎氏にご報告いただきました。セキュア・システム開発ガイドラインとは、「システムオーナー（ユーザ側企業）が、RFPに記載すべきセキュリティ要件」を整理したものを示します。その目的はユーザ側企業とITベンダー側のコミュニケーションギャップ解消を目指したものです。安全なシステムを作りたいというユーザ側とITベンダーの思いは共通なのに、方法論や成果物の評価をめぐって対立してしまう残念なケースも少なからず存在します。「リスク」という抽象概念を扱うことからこうした問題が発生するのだと思いますが、調達側と供給側双方の共通尺度が存在すれば実務的な効果は計り知れないでしょう。

セキュア・システム開発ガイドラインとは共通尺度、いうならばコミュニケーションツールのようなもので、パターン1：対策視点のRFP、パターン2：現象視点のRFP、パターン3：脅威視点のRFPといくつかの視点に分類して開発を目指しています。

セキュリティ市場調査WG

リコー・ヒューマン・クリエイツの勝見勉氏にご報告いただきました。セキュリティ市場調査WGは経済産業省の委託と支援を受け、国内の全情報セキュリティ事業者を対象に市場調査を行いました。報告のなかで興味深かったことは、「以前にこうした調査を行った際は事業者がセキュリティに特化した数値管理していたが、今日ではこれらはITシステムのなかの必要条件として組み込まれており、独立した数値

を有していないケースが多く、調査活動の難しさを再認識した」という点です。

こうした状況は調査ないしは統計的にはやっかいな側面があるかもしれませんが、安全意識がITシステムのなかにビルトインされつつあることを如実に示しており、セキュリティの面からは極めて歓迎できそうな傾向ではないでしょうか。

セキュリティ被害調査WG

政策部会の最後は、ディアイティの山田英史氏に発表していただきました。注目度の高いセキュリティ被害調査WGは、セキュリティ会計WGと同様にリスクの数値化・定量化を目的に設立され、主として情報漏えいに係わる損害賠償請求額を調査研究アプローチとして設定しています。様々な事件・事故の分析結果から山田氏は、「現在の企業・病院・学校などが施す個人情報保護対策は、情報の保護にナーバスな顧客や患者を基準に考えられており、普通の人にはむしろデメリットなのではないか。また本来であれば対策の目的は本人を守ることのはずなのに、どちらかと言うと企業側を守るために行っているような印象を受ける。法律の趣旨に従って、もっと本人の方を向いて考えるべき」との提言を行っていただきました。筆者も同法のもつ真の理念が社会に誤解されているという思いから、山田氏の提言には考えさせられるものを感じています。

西日本支部

中小企業向け個人情報保護対策WG

伊藤忠テクノサイエンスの市川順之氏に発表していただきました。西日本支部では、中小企業向け個人情報保護対策WGが精力的な活動を展開しています。このWGは、個人情報の保護やその対策手段の普及に力点を置いている点は他のWGと同様ですが、中小企業にターゲットを絞り込んでいるところがユニークです。2005年4月に同法が施行されたのちの中小企業の動向や大企業部門との比較などを通じて、課題を明確化していただきました。とくに中小企業部門では、技術対策の目標レベルを単独では決めにくい環境にあることを強く念頭におき対策ツールを策定、その紹介を行っていただきました。こうしたツールはこれまで大企業ユースを前提に作られているものが多く、中小企業部門のユーザ企業あるいはこのセグメントをマーケティング対象とするITベンダーの方には魅力的なものと思います。

（松田）

最後に

2005年度のJNSA活動報告会は多彩な内容でした。教育部会、技術部会、政策部会、西日本支部と、それぞれの内容も興味深いもので、多くの方々に参考となるものだったと思います。JNSAではこのほかにもマーケティング部会が中心になっている「インターネット安全教室」の活動もありますが、こちらは別稿でご紹介します。

JNSAの活動にご興味があれば、まずは参加してみてください。また、新しいテーマでの活動を起こされたい場合もぜひご相談ください。ご質問やご相談はご遠慮なく事務局までご連絡くださるようお願い申し上げます。

第２回 PKI Day －PKIの展開と最新技術動向

セコムIS研究所　新野　賢央

日本ネットワークセキュリティ協会PKI相互運用技術WGが主催する「PKI Day - PKIの展開と最新技術動向」が6月7日（水）に、南青山の東京ウィメンズプラザホールにおいて開催されました。「PKI Day」というタイトルを掲げてのセミナーは今回が2回目の開催となりますが、昨年10月に行われた第1回を上まわる250名以上の申し込みがあり、実際の参加者も190名という盛況でした。冒頭の主催者側挨拶の「ニッチなインフラ技術であるPKIが、確実に盛り上がりを見せている」という言葉も、にわかに実感できる雰囲気で始まりました。

まず午前の最初の講演では、セコムIS研究所の松本氏より「PKIの展開と最新技術動向」というタイトルでご講演いただきました。冒頭では、この相互運用技術WGのリーダーであるという立場から、現在までのChallenge PKI プロジェクトに関する経緯や活動報告を説明されました。続いて、電子署名法の改正議論、電子署名の展開という内容で、現行の電子署名法やPKIの展開に対する問題点を示しながら、今後どうなるべきかというビジョンを“松本キューブ”なる概念図を用いてわかりやすく解説されました。

続いての講演として、「わが国の保健医療福祉分野PKIの動向」というタイトルで、東京大学大学院・学際情報学府の山本氏にご講演いただきました。講演内容としては、行政の立場から医療情報がどう変革を遂げてきたのか、を示す年表に沿いながら、平成6年の医療画像の電子媒体への保存から始まり、最近の取り組みとしてIT新改革戦略におけるレセプトオンライン化、EHR-DB、HPKIの3点についてそれぞれ説明されました。

午前中最後の発表では、国立情報学研究所の島岡氏より、「大学間連携のための全国共同電子認証基盤UPKI構想と米国学術PKIの動向」というタイトルでご講演いただきました。講演内容としては、冒頭では簡単に米国学術PKIプロジェクトを紹介され、学術情報基盤UPKIの現状に関する話題を紹介されました。UPKIについては、3つのPKI、オープンPKI、キャンパスPKI、グリッドPKIをうまく連携させて機能させていくことが重要であると同時に、明確な保証レベルを定義してそれを共有して運用していくことが必要であると主張され、また、大学有志がUPKIに関してバーチャルに意見交換できるコミュニティ作りを進めていく予定であることも紹介されました。

午後最初の発表として、産業技術総合研究所グリッド研究センターの田中氏より「グリッドにおけるセキュリティの概要と動向」というタイトルでご講演いただきました。前半ではGSIというProxy証明書やDelegateを用いたグリッドセキュリティ技術を紹介され、これらの技術によりグリッドの普及面に関して大きく貢献した点、今後のビジネス展開にはセキュリティ上若干の問題があるProxy証明書に代替する技術が必要である点を示されました。また後半では、国をまたいでグリッドのポリシーや運用を調整するPAMと呼ばれる機関とその活動を紹介され、加えてIGTFと呼ばれるPAMを統括する上位機関が設立されたことについても紹介されました。

続いての発表として、三菱電機・情報技術総合研

究所の宮崎氏より「長期署名フォーマットとECOMにおける相互運用実証実験について」というタイトルでご講演いただきました。宮崎氏がWGリーダーを勤めるECOMの長期署名保存フォーマット普及SWGでは、前年度にECOMプロファイルに基づいた長期署名フォーマットの相互運用実験を行っており、今回はこの結果報告の内容を中心にお話いただきました。報告内容としては、この実験により参加企業数社内での相互運用性はある程度実証されたという反面、以前、不明確な仕様があり更なる議論が必要という部分も見つかったという報告もありました。また、現在直面している大きな問題として、推進すべき国際標準が実は国税要件の電子文書に対応しているとは言いがたい現状がある点をあげられました。

続いての発表としては、富士ゼロックス株式会社の稲田氏より「標準はどうのように実装されているのか?～OpenSSLにおけるSSL/TLSの実装に関して～」というタイトルでご講演いただきました。冒頭ではSSL/LTSに関する技術的概要や歴史などを、続くスライドでOpenSSLに関する生い立ちや特徴などを紹介されました。その中で、OpenSSLは事実上この分野におけるデファクトスタンダードツールとなっており、単純なSSL/TLSスタックとして利用するのに問題はないが、証明書の失効検証機能としては不十分な実装が見られるという点を説明されました。

最後の発表では、「Windows VistaのPKIとIE7」というタイトルでMicrosoftの渡辺氏よりご講演いただきました。冒頭では、今秋以降リリース予定である最新OS、Windows Vistaに新たに搭載される証明書の失効機能の紹介をされました。従来から悩みの種であった失効機能に対して、Vistaではデフォルトオンという設定を試みており、その背景にはどのような技術でもって数々の問題に対処してきたかという点について説明されました。また、発表後半ではVista搭載予定の最新セキュリティ機構である、

BitLocker、Microsoft Certificate Lifecycle Managerや、最新版IEであるバージョン7でのサイト認証の扱い方などについても示されました。

将来的にPKIはインフラとして私たちの生活に深くかかわってくる技術です。未来の生活には印鑑というものは古き時代の遺物となり、現実世界でもオンラインの世界でもICカードなどをかざして自分を他人に認証してもらう時代がすぐそこまで来ています。しかし、そこにはインフラとして備えるべき、相互運用性問題という大きな壁が存在しています。この大きな壁を乗り越えるには、まずはPKIを導入できるあらゆるドメインの人々が、「PKIはいかなる技術か」をしっかりと理解し、みなで議論しながら普及・啓発していくことが大切ではないでしょうか。こうした試みの一端を担うことを目的とし、今回のように有益なセミナーが多く開催され、多くの方々がPKIに興味を抱いてもらえることを期待するばかりです。

2006 年度
「インターネット安全教室」

～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 年度より開催してまいりました。2006 年度の開催状況は以下のとおりです。

【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

[開催一覧] 次の一覧をご覧下さい。(2006 年 8 月 20 日現在)

2006 年度「インターネット安全教室」開催一覧

日　程	開催地	共催団体	会　場
5月21日(日)	長野県	上田市マルチメディア情報センター	神科新屋生活改善センター
6月29日(木)	千葉県 (新規)	NPO法人松戸ITVネットワーク	松戸市民会館3F　301号室
7月6日(木)	長野県	上田市マルチメディア情報センター	市民プラザゆう
7月15日(土)	愛媛県	愛媛県IT推進協会	アイテムえひめ (愛媛県国際貿易センター) 4F会議室
7月27日(木)	奈良県	NPOなら情報セキュリティ総合研究所、 奈良県社会教育センター	奈良県社会教育センター
7月30日(日)	神奈川県	NPO情報セキュリティフォーラム	横浜市美しが丘西地区センター
8月4日(金)	鹿児島県	鹿児島大学学術情報基盤センター	鹿児島大学学術情報基盤センター 第1端末室・第2端末室
8月12日(土)	福岡県	北九州市、財団法人ハイパーネットワーク社会研究所	ウエルとばた2階多目的ホール
8月22日(火)	埼玉県	NPO情報セキュリティフォーラム	埼玉県生活科学センター 総合棟7階 研修室
8月22日(火)	愛媛県	愛媛県IT推進協会、伊方町情報推進協議会	西宇和郡伊方町立瀬戸中学校3F コンピュータ教室
8月23日(水)	神奈川県	NPO情報セキュリティフォーラム	足柄上合同庁舎 2階大会議室
8月23日(水)	神奈川県	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　集会室202
8月27日(日)	島根県	NPO法人プロジェクトゆうあい	松江市市民活動センター　201、202研修室
9月9日(土)	神奈川県	NPO情報セキュリティフォーラム	平塚合同庁舎 別館1階 大会議室
9月13日(水)	神奈川県	NPO情報セキュリティフォーラム	厚木合同庁舎 新館4階 大会議室
9月21日(木)	神奈川県	NPO情報セキュリティフォーラム	横須賀合同庁舎 5階 大会議室
9月25日(月)	神奈川県	NPO情報セキュリティフォーラム	相模原合同庁舎 3階 第一会議室
9月27日(水)	神奈川県	NPO情報セキュリティフォーラム	フォーラム南太田 3階 大研修室
9月29日(金)	兵庫県	財団法人ひょうご情報教育機構	三宮研修センター

日　程	開催地	共催団体	会　場
9月30日(土)	奈良県	NPOなら情報セキュリティ総合研究所	帝塚山大学学園前キャンパス 16号館6F・564教室
9月30日(土)	神奈川県	NPO情報セキュリティフォーラム	小田原合同庁舎 3階 E・F会議室
9月～11月 (予定)	島根県	NPO法人プロジェクトゆうあい	浜田市、隠岐郡(予定)
10月7日(土)	岡山県	岡山県インターネットセキュリティ対策連絡協議会	くらしき健康福祉プラザ(倉敷市笹沖)
10月14日(土)	大阪府	NPO GSI総合研究所	大阪工業大学 枚方キャンパス　情報科学部
10月22日(日)	宮崎県	福祉情報ボランティア宮崎、宮崎公立大学	宮崎公立大学
10月25日(水)	兵庫県	財団法人ひょうご情報教育機構	四季の森生涯学習センター
10月28日(土)	新潟県	NPO新潟情報セキュリティ協会	未定
10月28日(土)	広島県 (新規)	広島市情報政策課	広島市まちづくり市民交流プラザ マルチメディアスタジオ
10月28日(土)	滋賀県	NPO滋賀県情報基盤協議会	滋賀県立彦根工業高等学校
10月28日(土) (予定)	静岡県	静岡情報産業協会	「B-nest」静岡市産学交流センター
10月29日(日)	神奈川県	NPO情報セキュリティフォーラム	秦野市立本町公民館 2階 大会議室
11月7日(火)	茨城県	茨城県消費生活センター、龍ヶ崎市	龍ヶ崎市役所
11月8日(水)	兵庫県	財団法人ひょうご情報教育機構	淡路夢舞台国際会議場
11月10日(金)	秋田県 (新規)	NPO白神ねっと	能代市キャッスルホテル平安閣
11月14日(火)	神奈川県	NPO情報セキュリティフォーラム	藤沢市役所 防災センター 6階　会議室
11月15日(水)	神奈川県	川崎市、NPO情報セキュリティフォーラム	ラゾーナ川崎プラザソル 5階ホール
11月17日(金)	神奈川県	NPO情報セキュリティフォーラム	鎌倉生涯学習センター 4階　第6集会室
11月19日(日)	沖縄県 (新規)	石垣市、八重山支庁、竹富町、石垣市商工会	石垣市民会館中ホール(予定)
1月28日(日)	熊本県	NPO熊本県次世代情報通信推進機構	パレアホール(くまもと県民交流館パレア)
3月10日(土)	神奈川県	NPO情報セキュリティフォーラム	平塚合同庁舎 別館1階 大会議室
2007年3月 (予定)	千葉県	NPO法人幕張メディアアソシエイツ	ベイタウン・コミュニティコア(打瀬公民館)
※以下開催検討中			
	徳島県		
	鳥取県		

開催状況については、随時「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/

事務局お知らせ
JNSA ANNOUNCE

1. 主催セミナーのお知らせ

● Network Security Forum 2006 (NSF2006)

日　時： 2006年11月13日(月)～14日(火)
2日間　10:00 – 18:00
会　場： ベルサール神田
入場料： 無料
主　催： NPO日本ネットワークセキュリティ協会(JNSA)
運営事務局： IDGジャパン

NPO日本ネットワークセキュリティ協会では、上記の日程でNetwork Security Forum 2006を開催することとなりました。本年は､「内部統制を支えるITセキュリティ」を主軸テーマとし、JNSAのコンファレンスプログラム、スポンサー企業によるセッションに加え、展示会も併せて開催する予定です。

近年益々重要性を問われている内部統制について、様々なアプローチによるセッションを展開いたします。

皆様のご参加をお待ちしております。

詳細はホームページにてご確認ください。
http://www.idg.co.jp/expo/nsf/

● インターネット安全教室まつり

日　時： 2006年10月15日(日) 11:00～17:00
会　場： アクアアリーナ(アクアシティお台場 3F)
参加方法： 参加費無料･自由参加
主　催： NPO日本ネットワークセキュリティ協会(JNSA)
経済産業省
後　援： 警察庁
お問い合せ：「インターネット安全教室まつり」事務局
(caravan-sec@jnsa.org)
http://www.jnsa.org/caravan/

「インターネット安全教室まつり」は、JNSAと経済産業省が全国で展開している情報セキュリティの啓発セミナー「インターネット安全教室」をもとに、よりエンターテインメント性を高めた「おまつり」として開催します。子供から大人まで情報セキュリティについて楽しく学んでいただくとともに、全国各地で開催している「インターネット安全教室」の活動をさらに広め、できるだけ多くの皆さんに情報セキュリティの基礎知識を身につけていただくことを目的としています。ゲストにお笑いタレントはなわさんを迎えてのライブや安全教室クイズを行います。

情報セキュリティを楽しく学べるイベントですので、ぜひご参加下さい。

2. 後援イベントのお知らせ

1. SCMフォーラム

会期： 2006年9月13日(水) ～ 14日(木)
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　607、608会議室
http://logistics.or.jp/fukyu/experience/convention/scmforum.index.html

2. 平成18年度 情報モラル啓発セミナー

「今、企業に問われる情報モラルと社会的責任」
ー個人情報保護･情報セキュリティ対策の効果的な取り組みー
会期： 2006年9月15日(金)
主催： 中小企業庁、
財団法人ハイパーネットワーク社会研究所、
東北経済産業局
会場： コラッセふくしま(多目的ホール)
http://www.hyper.or.jp/moral2006/fukushima/

3. CPO (Chief Privacy Officer) Japan Summit 2006

会期： 2006年9月25日(月)
主催： 特定非営利活動法人 日本プライバシープロフェッショナル協会、日本CPO委員会
会場： 財団法人 日本青年館
http://www.ippa-npo.org/

4. 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： 2006年10月5日(木)～7日(土)
主催： 特定非営利活動法人新潟情報セキュリティ協会
ネットワーク･セキュリティワークショップin 越後湯沢実行委員会
会場： 新潟県南魚沼郡湯沢町
(湯沢町公民館、越後のお宿いなもと)
http://www.yuzawaonsen.gr.jp/conf

3. BUSINESS CONTINUITY MANAGEMENT 2006

“Compliance & IT 2006”
“Storage Management World 2006”
会期： 2006年11月21（火)～22日(水)
主催： BCM Conference実行委員会
会場： 新宿NSビル
http://www.idg.co.jp/expo/bcs/

3. JNSA 部会・WG 2006 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：山田英史 氏／ディアイティ）

例年通り、2006年1月～12月の1年間に発生する個人情報漏えい事件・事故を集計し分析する。本年度は、代表的な事例を掘り下げた分析にも取り組む予定。

予定成果物は、

1.「2006年 情報漏えい事件・事故集計速報」
2.「2006年 情報漏えいによる被害想定と考察」の予定。

【セキュリティ会計ガイドライン検討WG】

（リーダー：佐野智己 氏／凸版印刷）

企業における情報セキュリティ確保への取り組みを会計的視点から認識・評価・伝達(ディスクロージャー)する仕組みとして、『環境会計』に倣い、『情報セキュリティ会計』を定義し、その基本的な考え方を取りまとめる。

予定成果物は、成果報告書、雑誌コラム等の対外発表など。

【セキュア・システム開発ガイドラインWG】

（リーダー：丸山司郎 氏／ラック）

個人情報保護法施行を契機に、一般の情報システムへの管理責任が要求されるようになったが、そのレベルなどの明確な基準は存在しない。

開発システムのセキュリティ評価基準としてはISO15408が存在するが、どのレベルを選択すべきかが規定されていないことなどから、実装は難しい。

そこで、JNSAよりシステム開発に於けるセキュリティガイドラインを広く公開することにより、

1. 将来ISO15408等への国際標準への橋渡しをにらみながら、段階的に分かりやすく実施でき、
2. しかも、システムオーナもその妥当性(システムの社会的責任と費用対効果)を合理的に判断でき、
3. 利用者の財産などの保護対策内容を明示でき、
4. システム開発者や、運用者(SI/SO)の適切な発展と競争により、
5. IT社会の健全な発展への貢献をねらうものである。

予定成果物は、システムオーナが、RFPに記載すべきセキュリティ要件としてのセキュア・システム開発ガイドライン。

勉強会目的のワーキンググループ

【スパイウェア対策啓発WG】

（リーダー：野々下幸治 氏／ウェブルート・ソフトウェア）

現在の対策啓発Webの更新作業と関係省庁や他団体との勉強会及び啓発を行う。

プロジェクト

【セキュリティ市場調査WG】

（リーダー：勝見勉 氏／リコー・ヒューマン・クリエイツ）

活動テーマとして、次のものを候補として掲げ、現在WGで討議中

1.平成17年度市場調査結果の二次的・多角的分析
2.ユーザ実態調査(2004年度調査の2回目調査)
3.市場分類に関する詳細な定義の記述、シソーラス的なものの作成
4.平成18年度版市場調査(継続調査)の実施(経済産業省から受託獲得が前提)

予定成果物は、市場調査報告書など。

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

【不正プログラム調査WG】

（リーダー：渡部章 氏／アークン）

従来からのウイルスやワームなど感染を目的とした被害の他に、近年ではボットやスパイウェアなど、ハッキング、情報漏えい、詐欺などの実害を伴った不正プログラムが増加している。また、P2Pソフトによる著作権違反も問題となってきているため、マルウェア(不正プログラム全体)への対策が急務である。当WGではマルウェアとその対策の調査研究を実施し、その成果を普及させる。

予定成果物は、マルウェアの実証実験。

【ハニーポットWG】
（リーダー:園田道夫 氏/JNSA研究員）
2006年度は大規模ネットワークなどの情報解析技術の追求を行う予定。
予定成果物は、大規模ネットワークなどの情報解析技術の検討報告書など予定。

【WEBアプリケーションセキュリティ調査･検証WG】
（リーダー:加藤雅彦 氏/アイアイジェイテクノロジー）
昨年度、完成できていない成果物についての継続作業と、タイムリーな技術トピックなどについての検証イベントや勉強会などを行う予定。会合中心の作業から、オンラインの掲示板やメールを活用した活動へ移行していく形で検討したい。
予定成果物は、セミナー用コンテンツ一式･Webアプリケーションセキュリティ要件ガイドライン・攻撃手法研究レポート など。

【脆弱性定量化に向けての検討WG】
（リーダー:郷間佳市郎 氏/京セラコミュニケーションシステム）
これまでの成果を本年でまとめる予定。
成果物として脆弱性定量化に向けての検討レポートを作成する予定。

【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に関する話題と問題点の調査・討議･課題の整理、その他JNSAの活動として有益と思われる成果を出せるような活動を行う。7～9月は参加者の問題意識の相互のプレゼンテーションを行う。

勉強会目的のワーキンググループ

【暗号モジュール評価基準WG】
（リーダー:小川博久 氏/シーフォーテクノロジー）
下記の動向把握及び,ベンダーとしての取組み方を議論し,必要に応じて提言などを行う。
- 米国及び,カナダの暗号モジュールのセキュリティ要件及び,評価制度
- 同要件の国際標準化
- 日本国における同要件及び評価制度

【PKI相互運用技術WG】
（リーダー:松本泰 氏/セコム）
安全、安心な社会を構築する上でPKIの必要性を社会にアピールし、ネックとなるPKI相互運用性の問題などを自ら解決していく。主な活動予定は、WGの開催、IETFの参加、セミナー開催など。

プロジェクト

【IC･IDカードの相互運用可能性向上に係る基礎調査】
（リーダー:松本泰 氏/セコム）
IPA公募案件が採択された。オープンでセキュアで相互運用可能なIDカードを目指して、PKIから見たICカードの相互運用性を調査するとともに、公的な目的で利用されるIDカード等に関わる問題点を探るため、行政府等のヒアリングも予定している。

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。

【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）
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。今年度は独自開催の浸透に重点を置き、10月に普及啓発イベント「インターネット安全教室まつり」を実施予定である。

【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/JNSA研究員）
セキュリティスタジアムや技術セミナーを開催し、広くセキュリティ技術の啓発を行う。

【会員製品 PR 企画検討WG】
（リーダー:玉井節朗 氏/IDGジャパン）
会員企業の製品・企画PRの場をWEB上に設け（仮称：セキュリティ製品バイヤーズガイド）、広く一般企業に特に製品導入の為のガイドとして告知することを目的とする。
実質2ヶ月でサイト構築（開発・設計）を手がけ、コンテンツ･内容確認、企業情報収集･入力を10月上旬までに完成、アップデートした国内外の記事･特集を付加、10月末までに試験運用完了とする。
その他、サイト啓蒙の為のプランを作成し、10月末までに実行する。

初年度会員企業は、製品・企画等の登録、掲示、掲載を無料とする

予定成果物は、セキュリティ製品バイヤーズガイド。

4. 教育部会

(部会長:佐々木良一 氏/東京電機大学教授)

ネットワークセキュリティ技術者の育成のために、産学協同プロジェクトを進め、大学や企業で行うべき教育のカリキュラムの検討やユーザー教育の在り方についての調査･検討などを行なう。

【CISSP-WG】

(リーダー:大河内智秀 氏/NTTコミュニケーションズ)

CISSP-WGの活動を引き継ぎ、2006年度は、ISSJP試験開発活動を行う予定である。2007年1月に第一回目試験開催を予定している。

プロジェクト

【情報セキュリティ教育実証実験プロジェクト】

(リーダー:松田剛 氏/JNSA研究員)

昨年度事業の調査から、情報セキュリティ分野の人材育成を困難としている要因として、教える側(講師)の確保が難しいことが認識できた。特に地方の大学では講師の確保が極めて難しい状況で、東京との格差が大きい。

今年度はこうした格差を縮小するための方策として、JNSA会員企業で活躍している技術者を講師として依頼するとともに、遠隔受講、VoD(ビデオオンデマンド)などの手法の実証実験を行ってみる予定である。

【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リスクマネジメント)

インターネットの一般利用者を対象とした、情報セキュリティに関する知識やリテラシーの向上と、自己のセキュリティ脆弱性のセルフチェックのしくみづくりとして、ホームページ上で簡単に個人のセキュリティ知識度の自己チェックができる「セキュリティリテラシーベンチマーク」を作成する。

成果物は、Web上で公開する「セキュリティリテラシーベンチマーク」。

5. ユーザー部会(新設)

ベンダー企業とユーザー企業との橋渡し的ミッションを担う。氾濫するネットワークセキュリティに関する情報をユーザー企業へ的確に提供するとともに、各企業で生じる人材、ソリューション、情報などの課題について、ユーザー企業の支店から整理し、JNSAの各部会へ問題提起することで、部会の活性化やベンダー企業の製品・サービスの向上に寄与することを目的とする。

6. 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。

【セミナー運営WG】

(リーダー:井上陽一 氏/JNSA顧問)

西日本に拠点を持つ一般企業やユーザを対象に、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。また西日本支部会員企業間の知識共有、西日本にてインターネット普及活動を行うNPOとのネットワークセキュリティ啓発に向けた連携を行う。その他、勉強会･セミナーの開催を予定している。

【中小企業向け個人情報保護対策WG】

(リーダー:市川順之 氏/伊藤忠テクノサイエンス)

2005年4月の個人情報保護法完全施行後の中小企業の現状について調査し、中小企業に適した対策について研究する。

4. JNSA 役員一覧

会　長　石田　晴久
多摩美術大学教授・東京大学名誉教授
副会長　田中　芳夫
マイクロソフト株式会社
副会長　長尾　多一郎
株式会社ネットマークス
副会長　大和　敏彦
シスコシステムズ株式会社

理　事（50 音順）

足立　修	株式会社シマンテック
後沢　忍	三菱電機株式会社　情報技術総合研究所
内田　昌宏	株式会社ネットマークス
浦野　義朗	株式会社フォーバルクリエーティブ
甲斐　龍一郎	新日鉄ソリューションズ株式会社
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
下村　正洋	株式会社ディアイティ
武智　洋	横河電機株式会社
玉井　節朗	株式会社ＩＤＧジャパン
辻　久雄	ＮＴＴアドバンステクノロジ株式会社
西尾　秀一	株式会社ＮＴＴデータ
西本　逸郎	株式会社ラック
野久保　秀紀	大日本印刷株式会社
坂内　明	東芝ソリューション株式会社
日暮　則武	東京海上日動火災保険株式会社
古川　勝也	マイクロソフト株式会社
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
若井　順一	グローバルセキュリティエキスパート株式会社

監　事

土井　充	（公認会計士　土井充事務所）

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
佐々木良一	東京電機大学　教授
武藤　佳恭	慶応義塾大学　教授
前川　徹	早稲田大学　客員教授
村岡　洋一	早稲田大学　教授
安田　浩	東京大学　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（2006年8月21日現在 201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
(株)アイ・ソリューションズ
(株) ITサービス
(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
アイネット・システムズ(株)
(株) IPイノベーションズ
アイマトリックス(株)
(株)アクシオ
(株)アクセンス・テクノロジー
(株)網屋
アライドテレシス(株)
アラクサラネットワークス(株)
(株)アルゴ21
(株)アルテミス
伊藤忠テクノサイエンス(株)
学校法人 岩崎学園
(株)インストラクション New
インターネット セキュリティ システムズ(株)
インテック・ウェブ・アンド・ゲノム・インフォマティクス(株)
(株)インテリジェントウェイブ
インテリジェントディスク(株)
インフォコム(株)
(株)インフォセック
(株)インプレス
ヴァイタル・インフォメーション(株) New
ウインモバイル(株)
ウェブルート・ソフトウェア(株)
ウチダインフォメーションテクノロジー（株）
ウッドランド(株)
AT&Tグローバル・サービス(株)
(株)エス・アイ・ディ・シー
エス・アンド・アイ(株)
(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)
NECエンジニアリング(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)
(株) NTTデータ
(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)
エリアビイジャパン(株)
(株)大塚商会
オムロンフィールドエンジニアリング(株)
(株)オレンジソフト New

【か】

(株)ガルフネット
(株)ギガプライズ
キヤノンシステムソリューションズ(株)
キヤノン・スーパーコンピューティング・エスアイ(株)
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)
(株)クインランド
クオリティ(株)
KLabセキュリティ（株）
(株)クルウィット 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)
(株)コネクタス

【さ】

サードネットワークス(株)
サーフコントロール ジャパン
サイバーソリューション(株)
サイボウズ(株)
(株)サイロック

サン電子(株)
サン・マイクロシステムズ(株)
(株)シーエーシー
(株)シー・エス・イー
(株)シーフォーテクノロジー
(株) JMCリスクマネジメント
ジェイズ・コミュニケーション(株)
シスコシステムズ(株)
(株)シマンテック
寿限無(株)
(株)翔泳社
(株)ジュリアーニ・セキュリティ＆セーフティ・アジア New
(株)情報数理研究所
新日鉄ソリューションズ(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)セキュアスカイ・テクノロジー New
(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)
セントラル・コンピュータ・サービス(株)
ソニー（株）
ソフトバンクBB（株）
ソラン(株)
ソラン・コムセック コンサルティング(株)
(株)ソリトンシステムズ
ソレキア(株)
(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)タクマ
中央青山監査法人
TIS（株）
(株)ディアイティ
テクマトリックス(株)
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(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)
東芝ソリューション(株)
東洋ネットワークシステムズ(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)
日商エレクトロニクス(株)
日信電子サービス(株) New
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） New
日本オラクル(株)
日本高信頼システム(株)
日本コモド(株) New
日本CA（株）
日本ジオトラスト(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) 情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
日本ヒューレット・パッカード(株) New
日本ユニシス(株)
ネクストコム(株)
(株)ネット・タイム
(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 New

【は】
(株)ハイエレコン
バリオセキュア・ネットワークス(株) New
(株)ハンモック
東日本電信電話(株)
(株)日立システムアンドサービス
(株)日立製作所
日立ソフトウェアエンジニアリング(株)
(株) 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)
富士通関西中部ネットテック(株)
富士通サポートアンドサービス(株)
(株)富士通ソーシアルサイエンスラボラトリ
(株)富士通ビジネスシステム
富士電機アドバンストテクノロジー (株)
扶桑電通(株)
(株)フューチャーイン
(株)ぷららネットワークス
(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)プロティビティジャパン
ポイントセック(株) New

【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)
横河電機(株)

【ら】
(株)ラック
リコーテクノシステムズ(株)
リコー・ヒューマン・クリエイツ(株)
菱洋エレクトロ(株)
(株)ロックインターナショナル New
(有)ロボック

【わ】
(株)ワイ・イー・シー

【特別会員】
特定非営利法人 アイタック
アルゼンチン共和国情報セキュリティ協会 New
韓国電子通信研究院
ジャパン データ ストレージ フォーラム
特定非営利活動法人デジタル・フォレンジック研究会 New
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 日本パーソナルコンピュータソフトウェア協会
ブエノスアイレス州情報セキュリティ協会

6. JNSA 年間活動（2006 年度）

4月	4月11～12日	Lim Tec 2006後援
	4月12日	JSOX法勉強会（主婦会館プラザエフ）
	4月14～15日	拡大幹事会（熱海大観荘）
	4月19日	第1回幹事会
	4月20日	第1回西日本支部会合
	4月24日	2006年度理事会（八重洲富士屋ホテル）
	4月28日	第1回教育部会
5月	5月11日	セキュアプログラミングワークショップ
	5月11～12日	ソフトウェアテストシンポジウム2006大阪協賛
	5月15日	第1回政策部会
	5月16日	第3回迷惑メール対策カンファレンス後援
	5月18日	第1回技術部会リーダー会
	5月25～27日	第10回コンピュータ犯罪に関する白浜シンポジウム後援
	5月30日	2005年度WG成果報告会（大手町サンケイプラザ）
	5月30日	2006年度総会（大手町サンケイプラザ）
6月	6月5～9日	Interop Tokyo 2006 後援
	6月15日	第4回セキュアOSカンファレンス後援
	6月17日	ISACA大阪支部設立20周年記念講演会後援
	6月19日	第2回幹事会
	6月21日	第1回技術部会
	6月22日	第2回西日本支部会
	6月26日	内部統制におけるアイデンティティ・マネジメント研究にむけてのワークショップ
7月	7月6日	HOSTING-PRO 2006協賛
	7月6日	2006年度情報セキュリティ監査シンポジウム in 東京後援
	7月7日	セキュリティ対策についてのワークショップ
	7月12～14日	自治体総合フェア2006協賛
	7月19日	S/MIMEワークショップ
	7月19日	無線LANワークショップ
	7月19～21日	ワイヤレスジャパン2006/EXPO COMM WIRELESS JAPAN 2006後援
	7月21日	第9回西日本支部主催セキュリティセミナー（大阪国際会議場）
	7月26日	第3回幹事会
	7月28日	内部統制を見据えた、組織における情報セキュリティ人材育成セミナー後援
8月	8月2日	第2回政策部会
	8月8～12日	セキュリティキャンプ2006後援
9月	9月15日	平成18年度 情報モラル啓発セミナー福島 後援
10月	10月5～7日	ネットワーク・セキュリティワークショップin越後湯沢2006協力
	10月15日	インターネット安全教室まつり（お台場アクアシティ）
11月	11月13～14日	「Network Security Forum2006」主催
	11月21～22日	「BUSINESS CONTINUITY MANAGEMENT 2006」「Compliance & IT 2006」「Storage Management World 2006」後援
12月		

2006年6月～2007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/active/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/giji_2006/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
〒 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
〒 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 Press vol.17

2006 年 8 月 31 日発行
©2005 Japan Network Security Association
発行所
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
〒 136-0075 東京都江東区新砂 1-6-35　T.T. ランディック東陽町ビル
TEL: 03-5633-6061　　FAX: 03-5633-6062
E-Mail: sec@jnsa.org　　URL: http://www.jnsa.org/

印　刷
プリンテックス株式会社

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
〒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