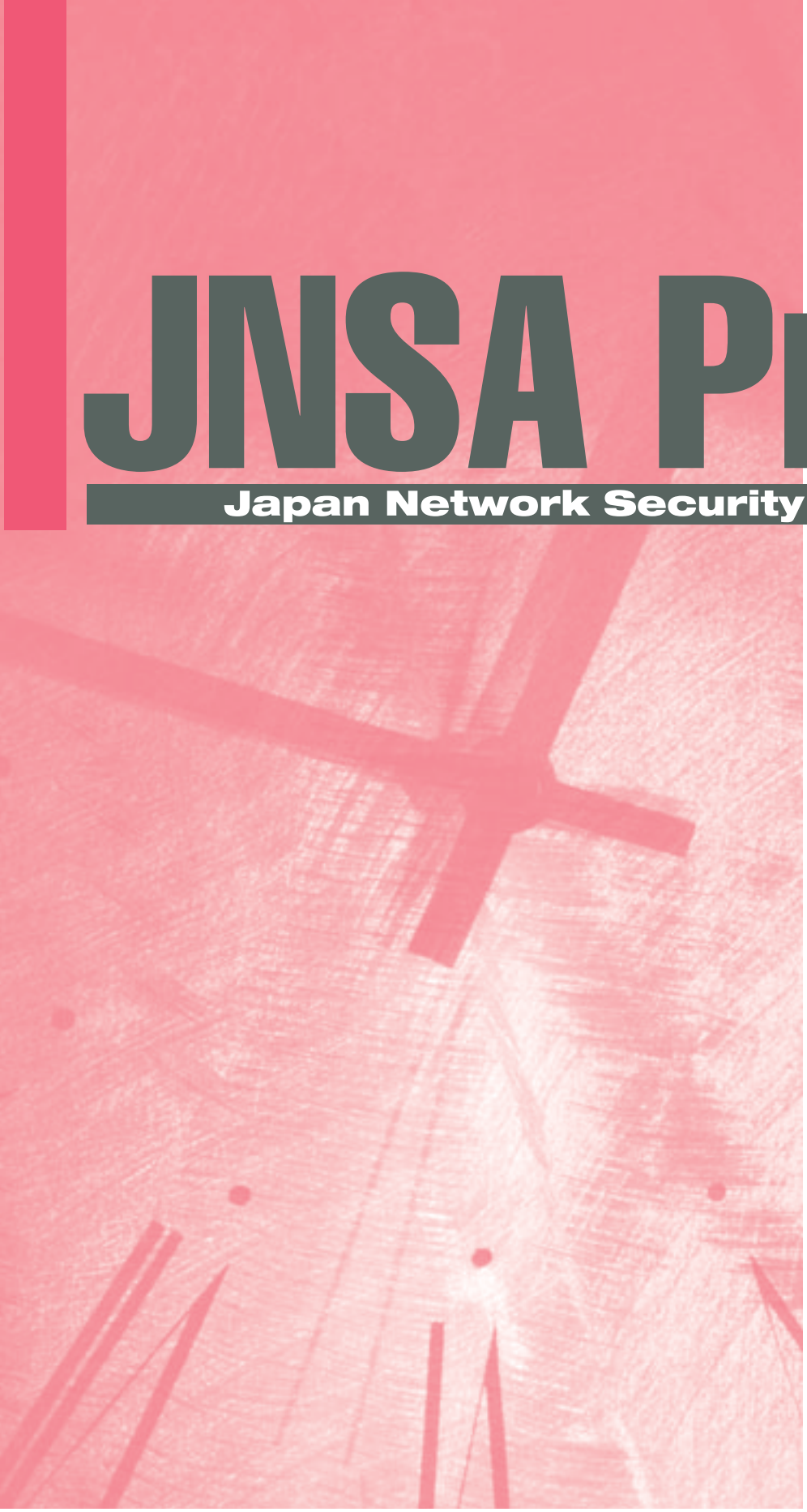


JNSA Press

Japan Network Security Association

Vol.19
March 2007

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

システム管理者から企業トップまで、
すべてのITワーカーにおくる、
セキュリティプロダクツのバイヤーズガイド

JNSA「セキュリティ製品バイヤーズガイド」が誕生!

―セキュリティ製品・サービスの情報収集ならおまかせ―

http://buyers.networkworld.jp

提供：株式会社IDGジャパン
協力：NPO 日本ネットワークセキュリティ協会（JNSA）
●お問い合わせ
株式会社IDGジャパン
JNSAセキュリティ製品バイヤーズガイド事務局
TEL：03-5800-4851　E-MAIL：jnsa_support@idg.co.jp

>>http://buyers.networkworld.jp

拡大する情報セキュリティのパラダイムと大学・学会の役割

日本セキュリティ・マネジメント学会（JSSM）会長
情報セキュリティ大学院大学 学長 辻井 重男

今年から、2月2日が情報セキュリティの日と定められた。その夜、総理大臣官邸で、ある催しがあり筆者も参列した。多くのテレビ局のカメラが並んでいたが、どの局も実際には何も放映しなかったし、どの新聞にもセキュリティのセの字も出なかったようである。視聴率などを優先するとそんなことになるのかと妙に納得したが、大学や学会としては、情報セキュリティに関する学術的研究・交流と社会啓発に意欲を燃やさねばと気を取り直している。

さて、2004年横浜駅近くに設立され、筆者が学長を努めている情報セキュリティ大学院大学では、つい先日、修士論文の発表会があり、夜間を中心に学んだ多くの社会人学生等から41件の論文が発表され、活発な討論が行われた。その内のいくつかの論文題目を下記に示す。これらを見てどう思われるだろうか。筆者が公開鍵暗号理論の研究を始めてから30年近い歳月が流れたが、情報セキュリティ＝暗号技術と言っても過言ではなかった往時を振り返ると隔世の感がある。

「Botnetの命令サーバドメインネームを用いたBot感染検出手法に関する研究」
「画像相関マッチングによる網膜認証方式」
「個人情報保護への過剰反応現象に関する研究」
「地方自治体の地理情報サービスにおける情報セキュリティ・フレームワークの適用に関する研究」
「2冪ねじれ点を用いた種数2の超楕円曲線の位数計算に関する研究」
「Webアプリケーションにおける言語ベースの動的情報フロー制御」
「輻輳型DoS攻撃を対象にした優先制御・帯域制御の研究」
「グループ署名を用いた利用履歴を秘匿できるコンテンツ配信・課金方式の研究」
「Social Engineeringの分析およびアクセス制御の提言」
「情報セキュリティインシデントにおける定量的費用分析に関する一考察」
「ステークホルダーの“リスク認知”に着目した情報セキュリティリスクアセスメント改善の研究」
「内部攻撃に対して安全なグループ鍵共有プロトコルの研究」
「ワンクリック詐欺対策手法の提案」
「問題構造化と事例分析による情報漏洩対策の改善モデルの研究」
「持駒方式を用いた多変数多項式型公開鍵暗号に関する考察」

さて、インターネットなどの普及浸透によって、人々の自在に動ける空間はリアル空間×サイバー空間へ飛躍的に拡大しているが、その一方で、例えば通信と放送に見られるように、様々な社会的組織や機能が連携・接近して、これまで、それぞれが異なる価値観の下に、あるいは無関係な利害の下に共存していた組織や機能の間で、価値観や利害の相克が深刻化している。筆者は、IT社会において、矛盾・対立する価値として、特に、自由、安全、プライ

バシーという3つに着目して、情報セキュリティを次のように概念規定している。自由の拡大のみを享受しようとすれば、安全性は低下し、プライバシー侵害を増大する。安全性向上のみを図れば自由は妨げられ、監視強化などによりプライバシー侵害が増える場面も多い。プライバシー保護のみに気を配れば、自由な情報流通は阻害され、匿名の下での悪事も増えて安全性が低下するケースも多発するだろう。安全性とプライバシー保護は必ずしも相反するとは限らないが、多くの場面で、自由の拡大、安全性の向上、プライバシーの保護は、互いに矛盾相克する。このような価値対立状況の下で、初めからバランスの問題と考えて安易に妥協するのではなく、できる限り高いレベルへ止揚して、高度均衡を図るのが情報セキュリティの役割であると筆者は考えている。

そこで、「情報セキュリティとは、技術、法制度、経営・管理、モラル・心理手法などを総動員して、それらの相乗効果により、自由の拡大、安全性の向上、プライバシーの保護を可能な限り同時に満たす基盤的システムである」と定義してはどうだろうか。これを学術の立場からいえば、情報セキュリティは学際的総合科学であるということになる。

情報セキュリティの日の行事の一つとして、2月25日の日曜日、日本セキュリティマネジメント学会では、「情報セキュリティと学会の役割」と題してシンンポジウムを開催した。筆者は、学会を、情報セキュリティ総合科学をダイナミックに構築するための学際的論文が積極的に発表されるような学術交流の場にしたいと訴えた。

また、情報セキュリティ大学院大学では、このような観点から、従来、暗号・認証コース、セキュアシステムコース、セキュリティ法制度と情報倫理コースを設けてきた。勿論、学生はどの科目も自由に選択できるようになっている。最近、特にヒューマンエラーなどの人間の心理や行動が情報セキュリティにおける大きな要因になってきたと思われる。上の修士論文題目にもこうした傾向が反映しているようである。暗黙知や信念・価値観など情報セキュリティを支える人間的基盤の中で、今後、情報セキュリティ心理学とでも呼ぶべき分野の構築が重要ではないかという議論を大学の中で日々闘わしている。

情報倫理の重要性は言うまでもない。明治時代、日本赤十字の創設者、佐野常民は、「真性の文明は道徳の進歩を伴わざるべからず」と述べている。道徳の進歩と言うあたりに、明治と言う時代の気分が見て取れるが、筆者はこの表現を真似て**「真正の情報文明は倫理観の変遷を伴わざるべからず」**と考えている。そのことを、つくづく考えさせられたのは、2005年末に起きたみずほ証券の「61万株1円」事件である。1株61万円の間違いだと知りつつ購入する行為に対する倫理的評価が大きく分かれ、筆者のアンケート調査結果では、約3割の人は市場原理で動いているのだから何等問題ないと考えていることが分った。18世紀のアダムスミスは国富論に先立って道徳感情論を書いている。スミスより38年早く生まれた石田梅岩は、商業が勃興した元禄期、武士の倫理に対して商人倫理のあり方を考えた。

インターネット資本主義とでも形容すべきグローバルな新資本主義を迎えた現在、我々は、先人に習い、最大多数の最大幸福と共に不幸な目にあう人の最小化のための新しい倫理を構築すべきときではないだろうか。

情報セキュリティと仕様のオープン性に関する課題
－「IC･ID カードの相互運用可能性の向上に係る基礎調査」から－

セコム(株) IS研究所
JNSA PKI 相互運用技術 WG リーダー　松本　泰

ICカードのセキュリティの高さの根拠として、よく耐タンパー性などが説明されます。しかし、耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等は、非常に重要な要素ではありますが、それらが評価されているからICカードは安全というのはかなり危ない発想です。それらにより何が保護されているか、どのように保護されているかといったことへの理解がより重要です。
ICカードを使った安全・安心なIT社会といったことがよく喧伝されていますが、その割にはICカードと、そのICカードを取り巻く技術は十分に知られておらず、情報セキュリティの専門家にも広く理解されているとは言いがたい面があります。
十分に知られていない理由のひとつに、ICカード自体や、ＩＣカードを利用する環境などに関して、セキュリティ上の理由として、その仕様が広く公開されていないことがあります。そもそも情報セキュリティの専門家にもあまり理解されていないものが、安全・安心なIT社会の基盤技術になるといったことがあり得るのでしょうか。
本稿では、IPAのサイトで公開された「IC・IDカードの相互運用可能性向上に係る基礎調査」に基づき、こうした問題の背景を探ってみることにします。

1. はじめに

独立行政法人 情報処理推進機構 セキュリティセンター（IPA/ISEC）の公募に、NPO JNSAの応募が採択された「IC・IDカードの相互運用可能性向上に係る基礎調査」の「調査報告書」が、2007年1月にIPAのサイトで公開されました。IPAのサイトでは、この調査を以下のように紹介しています。

> ICカードを利用し個人等を識別するIC・IDカードは、今後オンラインでの各種サービ等をセキュリティ面で支える社会インフラに成長する兆しを見せている。しかし、そのためには、クライアント環境や製造ベンダー等の違いによりサービス分野等をまたがっての利用に技術的な制約を受けない、相互運用可能性の確保が必要である。
> シーズ調査では相互運用可能性を実現する標準化動向や海外の取組みにおける技術体系の事例を、またニーズ調査では現在のIC･IDカードにおける相互運用可能性の実態と今後への展望を調査し、今後国内でIC･IDカードの相互運用可能性の向上に必要になる、国際標準を活用した関連技術の標準化やツール開発、普及方策の検討を行った

調査報告書のシーズ編においては、IC・IDカードの相互運用可能性(Interoperability)の課題を説明するため、フィンランドのFINIED、ベルギーのBELPIC、米国のPIVの3つのIC･IDカードの技術仕様を事例研究として取り上げています。これらの3つの事例を選択した理由は、技術仕様がオープンであることにつきます。FINEIDとBELPICは、日本の住基カードと公的個人認証サービス、米国のPIVは、国家公務員身分証明書ICカードに近いと考えられますが、公的個人認証サービスも国家公務員身分証明書ICカードも、調査報告書で説明しているレベルのIC･IDカードの技術仕様は、ほとんど何も公開されて

いません。従って、調査報告書で取り上げている3つの事例と同等レベルの技術的な説明を、これらのカードで行なうことはできません。

IC･IDカードに関して､｢仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る｣というアプローチと､｢仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する｣という一見相反するとも思えるふたつの考えが根底にあるように思えます。

何が正しいかはともかくとして、今後の情報セキュリティにおいて重要なコンポーネントとなる可能性があるIC・IDカードの技術やアーキテクチャは、正しく理解される必要があります。本稿は､｢国家公務員身分証明書ICカードと米国のPIVの比較｣､｢公的個人認証サービスとベルギーのBELPICの比較｣を説明することにより、以下の観点を考察して見ることにします。

(1) 情報セキュリティと仕様のオープン性
(2) 政府調達と民間の情報セキュリティビジネス
(3) カード内の鍵に関する仕様

2. 国家公務員身分証明書 IC カードと米国の PIV の比較

米国においては、政府機関全体を対象とするセキュアで信頼性のある身分証標準を規定する大統領指令(HSPD-12｢連邦政府職員と契約業者の共通識別基準のためのポリシー｣)が2004年8月に発効されています。このHSPD-12により、各政府機関は、米国国立標準技術研究所(NIST)が策定したFIPS-201(｢連邦政府職員及び契約業者の個人識別情報の検証｣)に準拠するカード(PIVカード)の発行が義務付けられることとなりました。各政府機関は、このPIVカードの発行を2006年10月27日までに開始しています。FIPS-201の準拠性は、このPIVカードだけではなく、関連する様々な周辺装置やサービスにも要求されます。

PIVカードについては、関連した大量の技術ドキュメントが公開されています。また､PIVカードアプリケーション、PIVミドルウェアの認定制度であるNPIVP(The NIST Personal Identity Verification Program)があり、これらは､｢調査報告書｣で詳しく説明しています。

米国PIVと国家公務員身分証明書ICカードを比較すると下の表のような感じになります。

PIVは、米国の安全保障を達成する上で｢仕様をオープンにすることで、安全･安心なIC･IDカードの普及を図る｣というアプローチを取っていると言えます。逆に日本の国家公務員身分証明書ICカードについては､｢仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する｣ため限定した範囲で使用するというアプローチに見えます。

比較項目	PIV	国家公務員身分証明書ICカード
配布対象	連邦政府職員と契約業者	国家公務員
配布枚数	2000万枚が予定されている	不明
プラットフォーム対応	規定なし	規定なし
IC･IDカードをサポートするミドルウェア	仕様、テスト仕様が公開されており認定制度がある ミドルウェアのレファレンス実装なども公開されている	不明
カードエッジI/F	NIST SP800-73	非公開 ※1
カード内のデータモデル	NIST SP800-73	非公開
格納されるEE（End Entity)証明書	認証用の証明書 署名用の証明書(Option) 暗号用の証明書(Option)	規定なし

※1 公的分野における連携ＩＣカード (http://www.kantei.go.jp/jp/singi/it2/others/iccard.html) の公的分野における連携ＩＣカード技術仕様（改定）に非常にアバウトなものがある。

3. 公的個人認証サービスとベルギーのBELPICの比較

BELPIC（Belgian Personal Identity Card）はベルギーの電子政府プロジェクトの一環として始まった国民IDカードのプロジェクトです。プロジェクトは2002年末より開始されており、パイロットプロジェクトを経て、2005年の9月からは新規に発行されるIDカードがすべてBELPICのカードとなっています。2009年末には12歳以上の全国民への配布を終える見込みを立てており、2006年10月の時点では400万枚を超えるカードが発行されています。ベルギーのBELPICと公的個人認証サービスを比較すると下の表ような感じになります。

比較項目	BELPIC	公的個人認証サービス
配布対象	12歳以上の全国民	15歳以上の希望者
配布枚数	400万枚（2006年11月現在）	18.3万枚（2006年10月末現在）
プラットフォーム対応	Windows,Mac,Linuxに対応	Windowsのみ Macの対応が一部なされている
ミドルウェアとユーティリティ	オープンソースが多く利用されており、専用ソフトのソースコードも数多く公開されている	バイナリコードを無償で配布
カードエッジI/F	カードエッジI/F	公開
7816-4,8に準拠		非公開
カード内のデータモデル	公開 PKCS#15に基づく	非公開
格納されるEE証明書	否認防止用の証明書 認証用の証明書	否認防止用の証明書のみ

BELPICで驚かされることのひとつに、政府が公認しているBELPICを利用するミドルウェアやアプリケーションの多くが、オープンソースとして公開されていることがあります。これは、BELPIC自体の仕様がオープンであることにも関係しています。BELPICは、「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」というアプローチだと言えます。公的個人認証サービスは、国家公務員身分証明書ICカードほどクローズドでないにせよ、「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」というアプローチに見えます。

4. 情報セキュリティと仕様のオープン性

BELPIC、PIVは、「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」というアプローチを取っているといえます。技術仕様をオープンにすることにより、相互運用可能性の問題等が広く技術者等に理解されれば、これらの相互運用可能なIC・IDカードを使った環境が整備されて行く結果となります。BELPIC、PIVは政府主導のプロジェクトですが、いずれ、民間ビジネスにも波及して行く可能性もあります。広く利用されればコストが下がり、それがまた利用を促進し、結果として、IC・IDカードを使った安全・安心なIT社会を構築するといったアプローチになります。

我が国において、公的個人認証サービスの普及が問題になっています。そもそも使い道がないから普及しないとか、そんなものいらないといった議論もあるかと思います。

公的個人認証サービスの普及について、技術的な問題ではないと言う意見が大半かと思います。しか

し、本質的には、技術的な不透明さも問題点のひとつではないでしょうか。技術的な不透明さは、論理的な理解の不足となり、何がベストプラクティスなのかという議論を困難にするだけでなく、プライバシー問題、セキュリティ問題に対して脅威を煽るだけの議論や、感情的な議論に終始してしまう結果となっているように思います。

調査報告書では、BELPIC、PIVの事例を説明していますが、これらは全て公開された情報に基づいて記述しています。少なくとも日本の公的個人認証サービス、国家公務員身分証明書ICカード等では、ここまでの情報は公開されていません。これらの仕様の入手などには機密保持契約の締結などが必要になります。これは「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」というアプローチです。こうしたアプローチの問題点は、技術が広く理解されないことにより、相互運用可能性の問題解決を阻害し、それが、安全、安心を提供するとされているIC・IDカードの普及の阻害要因となっているかもしれないという点にあります。次に説明する政府調達等においては、適正な競争を阻害するといった可能性もあります。

5. 政府調達と民間の情報セキュリティ

米国連邦政府におけるIT関係の調達は、民間のビジネスをドライブすることも念頭においているように思われます。これは、国家のIT戦略とも言えます。米国のPIVに関しても、幅広い技術仕様の公開、認定制度と、その認定製品の調達と言った調達のフレームワークを整備しており、民間のビジネスを育成する狙いも感じられます。それに対して、公的個人認証サービス（のICカードとしての仕様）、国家公務員身分証明書ICカード等では、その仕様のほとんどは公開されておらず、それぞれの用途に閉じています。行政関係の調達と言うビジネスがあっても、民間の情報セキュリティビジネスにとって規範となるようなものは提供していないと言えます。

PIVの仕様であるFIPS-201、SP800-73と言った技術文書は原案段階においても公開されているのですが、この原案に対して80を超える個人と組織から1900以上のパブリックコメントが寄せられています（http://csrc.nist.gov/piv-program/FIPS201-Public-Comments.html）。こうしたことは、PIVの相互運用可能性の課題を解決し、PIVが広く受け入れられる土壌を作っていると言えます。

HSPD-12「連邦政府職員と契約業者の共通識別基準のためのポリシー」と言う一見仰々しい大統領指令も民間のビジネスを大いに刺激しています。FIPS-201認定製品は、GSAのFIPS-201評価制度ウェブサイト（http://fips201ep.cio.gov/, http://fips201ep.cio.gov/apl.php）において、公開されていますが、2007年2月現在、195もの製品やサービスが公表されています。

PIV（PIVカードとPIVミドルウェア）に関しては、NPIVPという認定制度が立ち上がっています。NPIVPは、暗号製品の評価基準FIPS-140の評価認定制度であるCMVPに似た制度となっています。FIPS-140は、米国政府機関が暗号製品を調達する際の基準ですが、暗号製品の評価の難しさ故、客観的な評価がもとめられ、CMVPのような評価・認定制度が重要な意味を持つ様になりました。FIPS-140の基準のクリアーは、暗号製品ベンダーにとっては、高いハードルだったのですが、ハードル越えを米国政府が支援することにより、暗号製品ベンダーを育成した側面があります。そして米国連邦政府機関の調達等がドライブ役となり、米国企業の開発した暗号製品が世界の市場を席巻する大きな原動力となったと言えます。

同様に、IC・IDカードの相互運用可能性を確保した製品も非常に評価が難しい面があります。NPIVPのような評価・認定制度がデファクトの標準を作り出す可能性があるし、そうした狙いがある、また、民間企業はそれを求めているように感じられます。

6. カード内の鍵に関する仕様

ICカードの耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等が、保護すべき重要なものに、カード内の「鍵」があります。公開鍵暗号ベースのIC・IDカードの場合、プライベート鍵(Private Key)の扱いが重要だと言えます。IC・IDカードの技術仕様として、JavaカードやMULTOSカードといったものが仕様として重要と思われているかもしれません。しかし、例えば米国のPIVの場合、その実装として、JavaカードもMULTOSカードもネイティブOSカードも存在します。論理的な意味で重要な技術仕様としては、カード内のプライベート鍵や証明書に関する仕様があります。「カード内のプライベート鍵」の操作が、カード保有者の「署名」「認証」「暗号」にどう結び付くかが非常に重要なポイントです。下の表に、BELPICとPIVと公的個人認証サービスの「カード内の鍵や証明書の仕様の違い」を説明します。

IC・IDカード	カード保有者の証明書	証明書に対応した「プライベート鍵」の利用に関する説明
BELPICベルギー	認証用の証明書	認証(のための署名)に使用する 復号には使用できない(暗号には利用できない)
	否認防止の署名用証明書	署名操作のみ 署名操作毎にPINによるカード保有者の認証が必要。
PIV米国	認証用の証明書	認証(のための署名)に使用する。
	否認防止の署名用証明書 (オプション)	署名操作のみ 署名操作毎にPINによるカード保有者の認証が必要
	暗号用の証明書 (オプション)	発行者により「鍵」のバックアップがなされる
公的個人 認証サービス	否認防止の署名用証明書	署名操作のみ 否認防止用の証明書のみ発行される

BELPICのような欧州の電子身分証ICカードは、一般的にeIDと呼ばれていますが、このeIDは、IASすなわちIdentification、Authentication とelectronic Signature と言ったコンセプトで仕様が作成されています。eIDは、電子認証(Authentication)、電子署名(electronic Signature)、に利用できるものですが、その使い分けを明確にしています。例えば、BELPICでは、カードに格納される(否認防止の)署名用の証明書は、18歳以上に発行されています。BELPICは、2009年までに12歳以上の全国民に配布される予定ですが、責任能力の観点から18歳以下の国民には、IASの「S」を提供していません。否認防止の署名は「責任の所在」を示すので責任能力が必要な訳です。

BELPICの場合、認証用のプライベート鍵は、カード保有者がカードのPIN を入力し保有者認証を行なった以降は、カードに格納された認証用のプライベート鍵が認証要求の都度自動的に使われます(署名を行います)。こうしたことにより、シングルサインオン等、カード保有者に利便性を提供します。正当なカード保有者の認証(Authentication)時の認証用のプライベート鍵の利用は、カード保有者に不利益をもたらすことはありません。認証(Authentication)をするのはサービス提供者側であり、カード保有者が認証されるためにプライベート鍵を使うことにより責任が生じると言うことはない訳です。

これに対して否認防止の署名のプライベート鍵では、1回の否認防止の署名操作、つまりひとつの文書の否認防止の署名毎に「カード保有者の同意確認」(User Consent)のためのPIN の入力が必要な仕様になっています。これはカード自体が、「内容(文書など)

を理解せずに否認防止の署名してしまうこと」を防ぐ仕組みを有していると言えます。署名は、「カード保有者が行う」ものであり、この署名には、その署名文書等にはカード保有者の責任が生じるということを理解する必要があります。

日本の公的個人認証サービスでは、否認防止目的の証明書のみが発行されています。従って、公的個人認証サービスの発行する証明書を、認証（Authentication）として利用すべきではありません。否認防止目的のプライベート鍵を安易に責任の生じない認証（Authentication）として利用することは、責任が生じる署名に対するカード保有者のリテラシーの低下につながるからです。

7. おわりに

情報セキュリティ業界のビジネス上の難題に、その技術的な複雑さなどから、顧客にROI（費用対効果）や、ベストプラクティスを説明することが難しいことがあります。そのため、特に初期の頃は、必要以上に脅威を煽る傾向がありました。これは行き過ぎると長期的には、業界としての信頼を失う結果となるかと思います。

次に、情報セキュリティに関連した制度面の整備により、基準、規範などが整備され、今度は、コンプライアンスをビジネス上の武器にしている傾向があります。これは、もちろん間違いではありません。しかし、「情報セキュリティに関連した制度の整備」には、まだまだ、限界があり、実質的、現実的な情報セキュリティの問題点は、様々なところに存在します。制度面だけからの視点は、情報セキュリティの技術に対する正しい認識を歪めるようなところがあります。JNSA Press Vol.18の「現場まかせにしないセキュリティ設計、評価、実装のあり方について」の記事は、正に、そうした問題を指摘しています。

ICカード（ないしIC・IDカード）に関して言えば、耐タンパー性や暗号アルゴリズムの評価が、制度的にも整いつつありますが、情報セキュリティの専門家としては、これら以外にも解決すべき重要な課題があることを理解する必要があります。この理解の妨げになっているものにICカードの仕様の閉鎖性があります。確かに、リーズナブルなコストの範囲で、セキュリティを担保しようとすると、その仕様の公開範囲に妥協が必要な面はあります。しかし、仕様の閉鎖性は、ICカードの相互運用を阻害するなど、弊害が大きいことを理解する必要があります。

特に、行政の調達などにおいては、オープンシステムであってもセキュリティが保たれる仕様作りへの努力が必要でしょう。また、情報セキュリティの専門家としても、複雑さに負けず、あるべき姿を提案、提言していく必要があるでしょう。

IC・IDカードの技術やアーキテクチャが正しく理解されるために、本稿や「IC・IDカードの相互運用可能性向上に係る基礎調査」の「調査報告書」が少しでもお役に立てることがあれば幸いです。

参　考

IC・ID カードの相互運用可能性の向上に係る基礎調査
http://www.ipa.go.jp/security/fy18/reports/ICID/index.html

物理的セキュリティと情報セキュリティの融合

株式会社フォーバルクリエーティブ
上席テクニカルスペシャリスト　馬場　重通

1. 言葉の意味を整理する

ファイアウォールやウィルスワクチンは､「情報セキュリティ」と呼ばれるものであり、TCP/IPパケット通信を利用したバーチャルな論理的世界において、情報資産を様々な攻撃から防衛することを目的にしています。

それでは「物理的セキュリティ」とは、一体どのようなものなのでしょうか？

実はコンピュータネットワークは、バーチャルな論理的世界の中で動作しているとはいうものの、何も無い空間に存在しているわけではなく、数多くのサーバやクライアントパソコン上にソフトウェアをインストールし、それらをネットワークで結び合わせることで、初めてインターネットなどの巨大なバーチャル空間が形成されるのです。

コンピュータは、人間の心と体の関係に似ています。人間の心は、バーチャル空間で様々に想像を巡らすことが可能ですが、実はその想像は、体という物質的なものが土台となって成り立っています。体という物理的な実体がこの世に存在しなければ、魂も存在できないという意味です。

以上のように、バーチャルなコンピュータネットワークは、サーバやパソコン、ハブやルータなどの物理的実体がこの世に存在して、始めて存在することが可能となります。

物理的セキュリティとは、実体であるサーバやパソコン、ハブやルータなどの機器そのものを不審者から守ることを目的にしています。

2. 灯台下暗しになっていないか？

夜間に不審者が会社の中に侵入し、営業用のパソコンを持ち逃げされたという事件は毎日のように発生しています。

ファイアウォールや暗号技術などを駆使して、外部からの不正アクセスを完璧なまでに防衛することに熱心なシステム管理者は数多くおりますが、サーバルームやビルの建物の中に不正侵入されないように扉に鍵を取り付けたり、ICカード認証装置などの出入管理システムの導入を考える管理者は、ほとんどいないのです。よって上記のような事件が多発することとなり、いとも簡単に個人情報や機密情報が盗難に遭い、また情報システムが破壊されてしまうのです。

3. 先ずはルーピングが基本中の基本

物理的セキュリティは、部屋の扉に鍵を掛け、不審者や部外者が勝手に立ち入ることができないようにすることが基本です。

しかし近年のオフィスは、オープンフラットが好まれる傾向にあり、壁も柱も敷居も無い、だだっ広く見通しの良い環境が発達してきました。

このようなオープンフラットオフィスは、社員同士のコミュニケーションを深め、企業活動発展のために大きく貢献してきたと言えます。

しかしその反面、営業部や経理部、人事部や開発部、情報システム部などが何の敷居も無いままに1つのフロアに同居していることから、顧客や宅配の業者、ビル清掃の人間が、容易にサーバやパソコンなどの情報システムに触れることができる環境となってしまいました。

このようなオープンフラットなオフィス環境は、部外者からの攻撃だけでなく、社内の人間によるパソコンの窃盗や個人情報の盗難も容易にしています。

2005年4月1日の個人情報保護法本格施行以降、日本では、オープンフラットオフィスが急速に見直され、各部署を単位としてパーティションで壁を立て部屋を作り、扉に鍵を掛けて、社内の人間でも勝手に他の部署に立ち入ることができないように、オフィス環境の改良が進められています。

以上のように、部署単位やセキュリティレベルの必要強度単位毎にパーティションで部屋を作ること

をルーピングと呼んでおり、ルーピングされた各オフィスエリアのことをセキュリティエリアと呼んでいます。

これはファイアウォールのパケット通過ルールの設定に、多少似ているところがあります。

4. セキュリティエリアにはセキュリティレベル（セキュリティ強度）の設定が不可欠

壁と扉を設置してセキュリティエリアが出来上がったら、次にそれぞれのセキュリティエリア（部屋）の重要度がどのくらいあるのかを、4段階のセキュリティレベルで色分けします。

例えば、受付や商談コーナー、喫茶室などは、お客様や業者など、社外の人間が主に利用する場所ですので、扉は常に開放しておくべきであり、特別に厳重なセキュリティを施す必要はありません。

この逆に、サーバルームやマシンルームなど大量の個人情報や機密情報が管理され、情報システムの中枢を担うデータベースサーバが管理されている部屋などは、例えシステム管理者であっても、限られた数人の人間しか立ち入ることができないよう、厳重なセキュリティシステムを設置する必要があるのです。

以下にセキュリティレベルを設定するための一例を示します。

要度レベル	内　　容	対　　策
レベル4	**サーバルーム、金庫室など：** アプリケーションサーバやデータベースサーバなど、情報システムの中核を守る。特にデータベースに記録されている大量の個人情報を一度に持ち出されるのを阻止する。	内部犯罪対策
レベル3	**研究開発部、経理部、人事部など：** 未発表新製品、特許申請前技術、財務諸表、人事評価情報など、会社を維持して行く上で極めて重要な情報を守る。	内部犯罪対策
レベル2	**一般社員が働く職場：** 社外の人が侵入し、各部署が個人情報や業務書類が勝手に持ち出されないようにする。	外部犯罪対策
レベル1	**受付や商談コーナー、オープンスペースなど：** 社外の人間が侵入しても問題のないリア。	NON セキュリティ

次の図は、サーバルーム内において、サーバの種類や情報の重要性に応じ、さらに3つのセキュリティレベルを設定し、エリアを区分けした図面です。

エリアの重要度に応じて、扉の鍵を解錠するための個人認証装置は、

レベル3：指紋認証装置

レベル2：ＩＣカード認証装置

レベル1：パスワード認証装置

と3種類が用意されています。

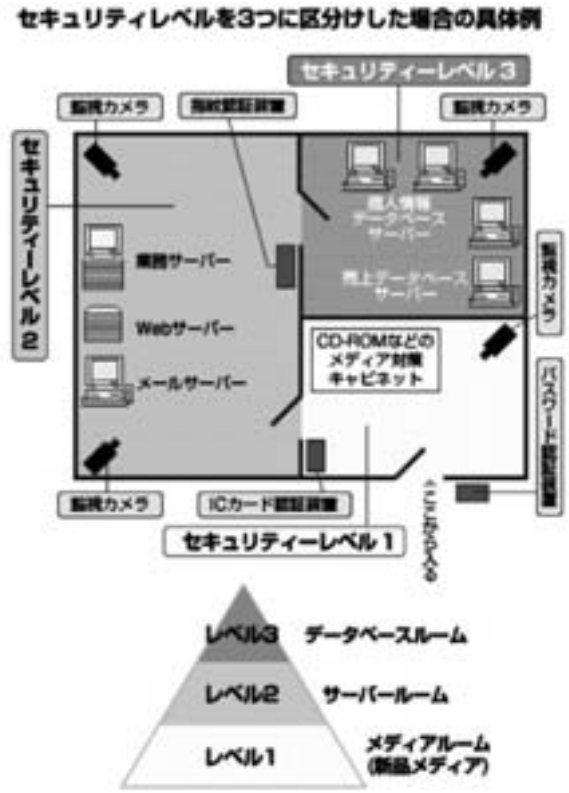
この図面で気をつけなければいけない点は、セキュリティレベルの重要度に応じて、エリアを入れ子状に設計するという点です。

例えばセキュリティレベル2エリアに進入する場合には、レベル1エリアからしか入ることができないように扉の位置を設計します。またレベル3エリアへ進入する場合には、レベル2エリアからしか入れないようにするのです。

このような入れ子状に建物を設計をすることにより、

レベル１の進入権限を持つもの：
パスワードを知っている。
レベル２の進入権限を持つもの：
パスワードを知っており、かつＩＣカードを所持している。
レベル３の侵入権限を持つもの：
パスワードを知っており、かつＩＣカードを所持している。なお且つ指紋を登録している。

となり、個人認証手段が積み上げられ、要求されるセキュリティレベルに応じたセキュリティ精度が確立されるのです。



5. 個人認証装置の選定方法

セキュリティエリアのレベルが上がれば上がるほど、成り済ましができない、本人を確実に確認できる最新な個人認証装置を導入する必要があります。個人認証装置の選定は、各セキュリティエリアの扉１つ１つに対して、入念に検討を進める必要があります。

各セキュリティエリアは入れ子状に設計し、セキュリティレベルが上がれば上がるほど、低位レベルエリア、中位レベルエリア、高位レベルエリア、最高位レベルエリアへと進入するように間取りの設計を行います。しかし、建物によっては、必ずしも前述のような理想的な間取りを設計できるとは限りません。低位レベルエリアからいきなり最高位レベルエリアへ進入する扉を設置しなければならないケースも多々あります。このような場合には、段々とレベルの高い個人認証装置を１台ずつ設置していく入れ子方式ではなくて、１枚の扉に対して複数の個人認証装置を設置する必要が出てきます。

それぞれのセキュリティレベルに応じて、どのような個人認証装置を設置したらよいか、以下に目安を示します。

セキュリティレベル	個人認証装置	扉の特徴	適用箇所
レベル 4	非接触 IC カード + 生体認証 （指紋認証など） + 二重扉	社内においては、最重要機密エリア。進入できる人間は極めて少人数に限られる。個人認証を確実に行う他に、扉を開けた隙に他の人間がなだれ込んでしまわないように、二重扉の導入を検討しましょう。	サーバルーム、 コンピュータールーム
レベル 3	非接触 IC カード + 生体認証 （指紋認証など）	全ての従業員が進入できるエリアではない。そのため、このエリアへの出入りは多くはないが、重要な個人情報などが格納されているので、少し時間が掛かっても個人認証は確実に行う必要がある。また入室の他、部屋から出るときにも個人認証を行い、退室履歴を取るようにしましょう。	ファイルや台帳、アンケート用紙や CD-ROM 等、個人情報が格納されている書籍庫など
レベル 2	非接触 IC カード	一般従業員の職場。ほとんどの従業員がこのアクセスクラスに属しており、出入りが頻繁に行われ、一度に多くの社員が出入りする扉である。そのため個人認証は非接触ＩＣカードでスムーズに行う必要がある。駅の改札のように。	一般従業員の職場など
レベル 1	NON または錠前と 鍵程度	昼間はフリースペースとして利用。夜間は施錠をするが、誰が開け閉めしたのかまでの履歴を取る必要はない。	受付や商談打合せコーナーなど

6. 監視カメラシステムとの連動

受付や商談コーナーなど、一般のお客様や宅配便業者が出入するスペースは、一般的に何の出入管理を行う必要もなく、営業時間内は、扉は開けっ放しにしておくケースが多いでしょう。

このようなエリアはＮＯＮセキュリティエリアと呼ばれており、オープンな企業イメージを損なわないためにも、夜間以外には鍵の施錠をしないのが一般的です。

とは言うものの、不正侵入者はこのようなＮＯＮセキュリティエリアから建物に侵入を試みますので、何のセキュリティも必要ないというわけではありません。

このような場合には、監視カメラを天井に設置して、画像を記録しておくことをお勧めいたします。

監視カメラはただ単に画像を録画し続けるだけですので、例え不審者が侵入したとしても、それを阻止することはできません。しかし実際に犯罪が発生した場合には、監視カメラで録画した映像を詳しく分析することで、犯人逮捕に役立てることができる唯一の方法となります。

また監視カメラを設置されていると、犯人は警戒をしますので、犯罪の抑止･予防にも繋がります。

監視カメラは、上記のような部外者への抑止効果以外にも、社内の人間の犯罪抑止にも繋がります。例えば個人認証をせずに共連れによって扉の中に進入するような内部の人間に対しては、扉の出入り部分に監視カメラを設置することで、共連れを抑止することが可能となります。

上記の場合、出入管理装置と監視カメラシステムを連動させ、扉が開いたタイミングで１０秒程度動画を録画します。それ以外のときは録画を中止すると

よいでしょう。不要な場面を撮影しないことにより、録画テープまたは録画記憶容量の節約に繋がる他、不正が起こった場合には、該当映像の検索をスムーズに行えるからです。

出入管理システムと監視カメラシステムを連動させることによりメリットが生じることとして、室内にいる人間が朝の最初の一人、または夜の最後の一人になった場合、室内の録画を行うという点です。

機密情報漏洩などの内部犯罪のほとんどは、他の社員がいない、一人の状態であるケースが多いという統計結果が出ています。

ですから、出入管理システムで部屋内の人数を常にカウントし、一人の状態を検知した場合には、監視カメラシステムに接点などで信号を出力し、室内の録画を開始するように指示を出すと良いでしょう。その後室内の人間がゼロになった際には、または２～１０名程度に増えた際には、録画を終了するように設定しましょう。

7. 生体認証装置を利用する場合は、個人情報保護法の遵守が必須

扉の鍵を解錠するための個人認証装置に生体認証装置を設置する場合には、従業員から指紋や静脈、虹彩(アイリス)パターンを採取し、認証装置内に登録しなければなりません。よって生体情報の利用目的を明示して、社員に承諾を得ることや、安全管理対策を実施して、生体情報が外部に漏れないように努めなければなりません。

認証装置内に登録される生体情報は、社員ＩＤや氏名と関連付けられて保管されますので、生体情報は完全なる個人情報に該当します。

ＩＣカード認証の場合には、個人情報保護法の遵守は必要ありません。なぜならば、ＩＣカードは企業サイドが従業員に対して発行するものですから、従業員個人から個人情報を取得する必要が無いからです。

8. 物理的セキュリティの未来像

論理的な情報資産であるデータベースサーバや、データベースサーバにアクセスするためのクライアントパソコンは、結局は１つの物理的なハードウェアから成り立っており、サーバルームや各職場の机の上に設置されています。ですから、情報資産は情報セキュリティで守るとともに、物理的セキュリティである出入管理システムでも守って行かなければなりません。

各クライアントパソコンからサーバへアクセスする際には、パスワードやICカード、指紋認証などの生体認証装置にてログオンを実施すると思います。

さてここで、出入管理システムは、各職場の部屋の中に存在する人間をリアルタイムに把握することが可能です。ですから、出入管理システムと情報セキュリティを融合させることにより、部屋の中に存在しない社員がクライアントパソコンからログオンしようとした場合には、明らかに成り済まし犯罪であることを検知することが可能となります。情報セキュリティ業界と物理的セキュリティ業界は、今まで会い交えることなく、それぞれに独立して製品開発を行い成長してきましたが、ここに来て両者のセキュリティシステムを融合させることにより、予想もしなかった大きな相乗効果が期待できることが分かって参りました。

例えばクライアントパソコンにログインをしたまま部屋の外に出た場合には、クライアントパソコンを自動でシャットアウトさせることも可能となるのです。

いままで物理的セキュリティは、目に見える物だけを守ればよいとされてきましたが、情報セキュリティシステムと融合させ統合することにより、より知的なトータルセキュリティプログラムを実現することが可能と見られていることから、今後は、物理的セキュリティと情報セキュリティの高度な融合をより一層推し進めて行くことにより、人間の犯罪心理や犯罪行動パターンに即したセキュリティプログラムが開発されることが期待されています。

境界セキュリティの限界とエンドツーエンドセキュリティの必要性

SSH コミュニケーションズ・セキュリティ株式会社
橋本　詩保

歴史から学ぶべきことがあるとすれば、それは最強の防衛でさえも突破され得るということです。中世の石造りの砦は、強力な包囲攻撃兵器により攻略され、またその後には火薬の発明によって制圧されました。19 世紀の南北戦争の巨大な要塞であったサムターおよびプラスキでさえも、より強力な銃器により陥落しました。これらの例やその他の数限りない例から、新たな技術およびこれまで以上に狡猾な敵によって、最も強靭と思われていた防衛線でさえも打破されてしまうことがわかります。

同じことが今日の企業 IT セキュリティにも当てはまります。多くの組織が、脅威は「最前線」で抑えられれば良いと考えています。このため、さまざまな外部の脅威から境界線内のイントラネットを保護すべく、情報セキュリティ製品に何百万ドルもの投資が行われています。これらの外部の脅威としては、ハッカー、電子メールウイルスおよび公共インターネットからもたらされるネットワークワームなどが挙げられます。これらの組織が選択するソリューションは主にファイアウォール、アンチウイルスソリューションおよび仮想プライベートネットワーク（VPN）ですが、信頼されていないインターネットから「信頼されている」イントラネットを保護することに重点が置かれています。

しかし現実には、境界線は繰り返し危険にさらされており、企業および政府機関は単に境界線のセキュリティソリューションに依存するだけでは全く不十分であることに気付き始めています。さらに、多くの組織では内部のセキュリティの脅威から身を守るための対策を怠っています。内部の脅威は、より重大かつ悪質な敵となる場合が少なくありません。

エンドツーエンドの通信セキュリティは、企業ネットワークの境界線保護のみに重点を置く今日の企業セキュリティアプローチの限界を打破する新たなアプローチです。エンドツーエンドのセキュリティは、データ通信の開始から終了までを保護し、アプリケーションと IT インフラストラクチャとの間で機能することにより、企業全体のセキュリティソフトウェアおよびセキュリティ ポリシーの双方について一元的な管理を提供し、内部および外部の双方のリスクに対するセキュリティを大幅に改善します。

1. 内なる敵

今日の境界線のセキュリティ防御に対抗するため、ハッカーはさらに巧妙な技術やアプローチを開発しています。代表例として、ポート80経由で内部ネットワークにアクセスすることが挙げられます。内部ネットワークに侵入すると、ハッカーは疑いを持たない内部関係者をだまして境界線の内部に「トロイの木馬」ソフトウェアを仕掛けるウェブサイトを訪問させます。このソフトウェアは機密データを収集してハッカーの元に送信する役割を果たします。また、悪意を持ったあるいは金銭を目的とした内部関係者が顧客情報を持ち出す事件が現実に起こっています。

しかし、これは氷山の一角に過ぎません。今日の真の課題は、内部に存在する IT セキュリティの脅威への対処です。古い時代に、偶然であれ意図的であれ、信頼された内部関係者によって緻密な防衛線内での防御が簡単に打ち破られたのと同様に、IT の防衛線内での防衛も会社の従業員によって打破されるということがあり得ます。

そしてその脅威は、ほとんどの人が考えているよりも大きいのです。Gartnerの調査によると、情報システムへの不正アクセスの70%が社員によるものであり、これらの内部セキュリティ侵害の95%以上が大規模な財務上の損失をもたらしています 。さらに、Computer Security InstituteおよびFBIの調査によると、大規模な組織に対する内部関係者の攻撃により平均270万ドルの損害が生じているのに対し、外部からの攻撃による損害額は平均してわずか5万7,000ドルにとどまっています 。また、金銭的な被害のみならず、顧客情報の漏洩によって企業としての信頼を失うリスクも伴います。

境界線のITセキュリティソリューションのみに依存していては十分ではないことは明白です。社員記録、顧客情報、パスワードやその他の機密データなど、組織に不可欠な情報の大部分は組織のイントラネット全域で無防備な状態で送信されています。多くの場合、悪意のない社員が不注意により組織の内部と外部の双方において同僚に機密情報を漏らしてしまっているケースもあります。機密データを収集するための使いやすいネットワーク・スニッフィング(データ傍受)プログラムは誰でも容易に入手できるため、その動機の如何にかかわらず、初心者でさえもこのような内部攻撃を実行できます。また、P2Pソフトウェアの不注意な使用により本人の気づかないうちに重大な機密情報が漏洩していることもあります。さらに悪いことには、TCP/IPネットワークは本質的に匿名での操作が可能なため、犯人を特定して最終的に捕らえることが極めて困難です。

企業の機密ITデータは内部関係者によってさまざまな形で外部に洩らされます。例えば、以下のような例が挙げられます

- 内部ネットワークへのセキュアでない無線アクセス(WLAN)を行っている際の近隣者による傍受
- 内部LANへの正規のアクセス権を持つ社員で、会社に対して不満を抱いている者や金銭を目的とした者
- 単純なパスワードを使用し、または不注意により機密情報を組織外の人物に漏らす、セキュリティに関する適切な研修を受けていない(悪意のない)社員
- 機密アプリケーションからのログアウトを忘れ、ワークステーションを権限を持たない人物が使用できる状態のままにするユーザ
- インターネットカフェなどの遠隔地からウェブベースのアプリケーションを使用して内部ネットワークにアクセスした後、Webのキャッシュを消去し忘れて、その後に使用するユーザに機密データへのアクセス権を与えてしまうユーザ
- WAP対応の携帯電話またはブルートゥース対応のラップトップ経由で接続された携帯電話を使用して内部ネットワークにアクセスするユーザ
- ウィルスに感染したP2Pソフトウェアによる顧客情報など機密情報の漏洩

新たな技術により、これらのセキュリティの脆弱性が記録的な数で悪用されています。例えば、パスワードの傍受およびIPパケットの隠蔽など、さまざまな攻撃方法を自動化して結合するネットワークワームが出現しており、これらのワームが無防備な内部ネットワークにアクセスできるようになると、相当な損失をもたらす可能性があります。

残念ながら、最近大きく取り上げられている多数のウイルス事件とは異なり、内部セキュリティの侵害はほぼ常に隠れたところで発生しており、一般に知られることはほとんどありません。多くの組織がこのような侵害を公表しない理由としては、不面目となる可能性、長期的な信用の失墜および広報上のマイナス効果などがあります。しかし、こうした事実が広く一般に知られていないために、情報セキュリティベンダおよび組織のIT予算担当者は境界線のセキュリティの強化のみを重視し続けています。

その結果、今日では多くの企業および政府機関において、内部アプリケーションおよびデータレポジトリに企業ネットワーク全体の機密性、データの整合性および強力な認証を提供する、完全なエンドツー

エンドの通信セキュリティソリューションを導入し、既存の境界線のセキュリティを補強するための強いニーズが生まれています。

2. 全体像

内部関係者によるリスク管理には、LANにおけるデータ保護および機密情報への電子的なアクセスの管理などだけではなく、そのほかにも沢山の注意が必要です。機密資料にアクセスするための最も簡単な方法の1つは、これまでと同様に、人をだまして必要な情報を入手することです。このため、すべてのリスクに対する包括的な保護を提供することは、情報セキュリティソリューションのみでは到底不可能です。それよりむしろ、組織におけるリスク管理に不可欠な部分として情報セキュリティを理解すべきです。利用可能な電子セキュリティ技術を組み込むことに加えて、セキュアな組織では人事プロセス、物理的なセキュリティ手法および一般的なセキュリティポリシーなどの分野について検討を行う必要があります。

エンタープライズ・リソース・プラニング(ERP)、顧客関係管理(CRM)および共同設計とワークフローのアプリケーションなど、組織全体で利用するアプリケーションの導入によって、内部ネットワークトラフィックの傍受は、組織の機密情報およびデータに違法にアクセスする上でこれまで以上に効率的な方法になります。その結果、多くの組織ではこれらのすき間を塞ぐためにITセキュリティにより多額の投資を行う必要が生じます。しかし、物理的セキュリティまたはセキュリティ認識に関する社員研修を犠牲にしたITセキュリティ投資は、また別の利己的な利用へとつながります。したがって組織の管理者は、セキュリティの検討にあたっては常に全体的なプロセスを見る必要があります。とは言うものの、全体図の一部としてITセキュリティの改善に重点を置く場合には、対処すべき数多くの重要な要件があります。

3. IT セキュリティ戦略

エンドツーエンドの通信セキュリティシステムが効果を上げるには、単にITの境界線から外の世界のみではなく、ユーザのワークステーションからアプリケーションサーバまでのパス全体でセキュアな通信を提供する必要があります。またこのシステムでは、イントラネット上のコンピュータからだけでなく遠隔地からもインターネット経由で組織ネットワークへのセキュアなアクセスが可能でなければなりません。

ほぼ全ての企業において、エンドツーエンドの通信セキュリティは、可能であればサーバアプリケーションと同じハードウェア上でアプリケーションとネットワークの間で稼動し、アプリケーション自体には何の変更も生じさせないものでなければなりません。この要件は、再プログラミングに多額の費用と時間がかかり、リスクを伴うレガシーアプリケーションにおいて特に重要です。ユーザの認証を行って通信を解読するには、ユーザのワークステーションのクライアントアプリケーションとネットワーク間に、エンドユーザの操作を必要としないクライアントを直接インストールします。互いに離れた場所にある多数のクライアントを管理下に置くには、システムの一元管理が可能である必要があります。

保護されていないアプリケーション通信からのリスクを管理するために技術的な対応策を導入する場合、検討すべき主要なセキュリティサービスは以下の通りです。

- FIPS-140-2認証暗号アルゴリズムを使用して機密情報の傍受を防ぐための通信の機密性保持/暗号化
- 転送中の情報の改ざんを防ぐためのデータ完全性
- アプリケーションへのアクセスを提供する前のユーザIDの確実な検証を容易にするための認証（Authentication）
- ユーザにアクセスを許可する情報を決定するための承認（Authorization）

これらの機能は相互に深く関連しています。例えば、通信が行われる前にユーザIDが検証されなければ、強力なデータ暗号化はほとんど価値がありません。また、通信プロセスの途中で誰でもデータを改ざんできるならば(データ完全性の欠如)、強力な認証は役に立ちません。同様に、ユーザが正しく認証されなければ、強力な承認手続きもほとんど価値がありません。

4. 今日の展望

一般的なIT環境は、サポートインフラストラクチャ(サーバハードウェア、オペレーティングシステム、データベースシステム、ネットワークハードウェアなど)および個別の組織アプリケーション(ERP、CRM、SCMなど)により構成されています。この環境においてセキュアな通信をどこでどのように導入するかに関する決定は、IT部門が効果的なエンドツーエンドの通信セキュリティを維持しながら、組織の主要な事業目標の達成に貢献できるかにも左右されます。

既存のセキュリティソリューションは多くの場合、ITインフラストラクチャまたは実際のビジネスアプリケーション自体が持つセキュリティ機能に基づいています。これらのアプローチのいずれも、実用的で費用効果の高いエンドツーエンドのアプリケーションまたはデータセキュリティの効果的な導入には適しておらず、しばしばその価値よりも多くの問題を引き起こします。

ITインフラストラクチャにセキュリティを統合するには、個々のサーバ専用のセキュリティハードウェアの配置など、複雑で費用のかかる技術的努力が必要となります。これらのアプローチはアプリケーションおよびデータを直接保護しないため、高価で柔軟性に欠ける傾向があり、悪意のある個人が悪用できる「バックドア」の脆弱性を残すことが少なくありません。

一方、既存の組織アプリケーションに暗号化および認証機能を埋め込むには、個々のアプリケーションでコードの修正が必要になります。専用の基幹アプリケーションに多額の投資を行っている大規模な組織では使用中のアプリケーションの数と種類が多いため、この選択肢はほとんど実行不可能です。予測される大きな問題としては、例えば、既存のアプリケーションコードの修正に要する多額の費用、エンドユーザに対する透過性の欠如、アプリケーションの相互運用性に関する課題およびアプリケーションパフォーマンスの低下が挙げられます。

5. 兵器庫の建設および管理

エンドツーエンドの通信セキュリティは、ネットワークおよびアプリケーションサーバ間の強力な認証および暗号化機能を備えたセキュリティソフトウェアの採用により、より優れたアプローチを提供します。アプリケーション自体を変更したり性能の低下をもたらすことなく、透過的にアプリケーションを保護するこのソフトウェアは、各基幹アプリケーションのフロントエンドとして機能し、ビジネスアプリケーションおよびデータへのクライアントのアクセスを制御します。ビジネスアプリケーションにアクセスする各ユーザ(または他のアプリケーション)は、サーバに対してクライアントを認証する小規模なセキュリティクライアントを持ち、メッセージやデータを相互にやり取りするためのセキュアなパイプラインを確立します。

このアプローチに使用されるセキュリティ技術は新しいものではありません。例えば、Secure Shellなどのポイントソリューションは、効果的で使いやすいクライアント/サーバセキュリティを提供し、内部および外部の包括的な保護のための理想的なソリューションとなり得ます。しかし課題となるのは、中規模から大規模な組織の場合はいずれも、何百ものアプリケーションサーバおよび何千、何万ものクライアントが存在する可能性があることです。これほど多数のセキュリティフロントエンドおよびセキュリティクライアントの管理は、物理的に不可能でないとしても、

短期間に極めて多額の費用が必要になります。

このため、大規模な組織が管理可能なセキュリティを実現するための鍵は、すべてのセキュリティサーバおよびクライアントを管理するセキュリティマネージャアプリケーションを加えることにあります。この方法により、ユーザ、ポリシーおよびソフトウェアの更新を一元管理し、組織全体に瞬時に適用することができます。

6. セキュリティの敵に対する戦いの遂行

2500年前、ヘラクレイトスは「万物は流転する」と言いました。この言葉は、絶え間なく変化が起こるセキュリティ業界にこそ最もよく当てはまります。

かつては、物理的なセキュリティのほかに必要とされるものはありませんでした。その後、組織が成功する上で情報の重要性が増すにつれて、セキュリティに関する社員教育が重要になりました。インターネットおよび汎用データ通信の出現により、主に境界線のセキュリティの形で電子的なセキュリティが前面に押し出されました。今日、大規模な組織の内部において共同作業の要件のためにより多くの人々が機密情報をこれまでより容易に利用できることから、私たちはセキュリティが組織の内部から危険にさらされるという不安に直面しており、それが最も大きな脅威となっています。今日の複雑な企業ITネットワークを保護するには、もはや境界線のセキュリティのみに頼ることはできません。

このため、組織はエンドツーエンドのアプリケーションおよびデータセキュリティをITインフラストラクチャに今すぐにも加える必要があります。エンドツーエンドの通信セキュリティは、内部および外部の双方のリスクに対するセキュリティを大幅に改善するだけでなく、エンドユーザにほとんど影響を及ぼすことなく既存の企業IT環境と容易かつシームレスに統合できます。このセキュリティは時の試練を経た技術に基づいており、導入、保守および構築が容易で、厳格な監視機能を提供します。これらの要素は、21世紀の企業がネットワークインフラストラクチャおよび貴重なデータを保護する上で必要となる基本的な要素です。

また、ITセキュリティマネージャがポリシーを容易に維持し、組織に関わる何百種類ものアプリケーションおよび何千人ものユーザに更新情報を素早く適用する上で役立つ一元管理機能を合わせて提供します。結局のところ、最高のセキュリティシステムでさえも、極めて順調に稼動している場合にのみ効果を上げるのです。

ハッカー、不満を抱いている社員、コンピュータ犯罪者およびテロリストが、企業、政府または消費者の機密データの強奪を引き続き企てることに疑いの余地はありません。しかし、境界線のセキュリティという焦点を越え、企業IT環境における重要な脆弱性のすき間を塞ぐことにより、エンドツーエンドの通信セキュリティは内部および外部の双方においてセキュリティの敵を打ち破るための強力な武器となります。

JNSA ワーキンググループ紹介

情報セキュリティランキングWG

WGリーダー
凸版印刷株式会社　佐野　智己

1. WGの発足にあたり

以前から考えていたことをJNSAでやってみようと思い、今年度、新たなチャレンジを始めました。

やりたいと思ったのは、ビジネス雑誌がしばしば特集で掲載している「××××大賞」や「○○○○ランキング」などの情報セキュリティ版です。情報セキュリティに真摯に取り組んでいる企業を褒め称え、情報セキュリティが企業評価に結び付く仕掛けが作れないか(よく言われる仕掛けが「格付け」や「社会的責任投資(SRI)」ですが、第3の仕掛けとして「ランキング」を昇華させたい!)、情報セキュリティに対する意識改革・啓発を促し、社会全体を巻き込んだムーヴメントを起こすことができないか。この命題に対して、今回はランキングという手法でアプローチすることにしました。

2. ランキングが伝えたいこと（私の想い）

どういう考え方のもとにランキングを算定するのかについては未だ議論の途上にありますが、ランキング上位に位置づけられた企業の取り組みを模範事例に、どこまでやればいいのか分からないと言われる情報セキュリティ課題に対して1つの解を提供したいと考えます。また、その時点でのトレンドをつかみたいとも思います。

もう1つ、対象企業の情報セキュリティの取り組み領域をここでは広く捉え、ステークホルダとのコミュニケーションや情報開示の充実度、社会貢献活動などにもスポットを当てたいと考えています。情報セキュリティ関連の製品・サービスを開発・提供している企業以外の企業や中小企業にも光が当たるようにしたいと思っています。

“企業が情報セキュリティに真摯に取り組み、かつステークホルダと適切なコミュニケーションをとることが企業価値の向上につながる!?”ということが定説化できるでしょうか。

3. WG活動（概況と予定）

2006年10月発足、これまでに4回のWGを開催しています(月1回程度の頻度でWG開催)。「情報セキュリティのランキングとは、何を測ったものなのか」「どういう企業が上位に来るべきなのか」「実際にどうやって測定するのか」など、情報セキュリティランキングの基本設計について議論を重ねているところです。これと並行して既存のランキングや調査レポートを参考に評価指標のプロトタイプの設計にも着手しました。今後は、種々の領域の方々との意見交換も行う予定です。

来年度、第1回JNSA版・情報セキュリティランキングが公表できることを目標にいまはじっくりと足元を固めているところです。

さいごに、情報セキュリティは、エコロジー同様、企業の社会的責任の重要なテーマの1つに挙げられます。そこで、エコロジーでの成功事例を情報セキュリティにも展開できないかと思いますが、実際はとても難しいことも感じています。社会全体を巻き込んだ「クールビズ」や「ウォームビズ」のような動きが情報セキュリティにも来るだろうか。「LOHAS(Lifestyles of Health and Sustainability)」のように、“セキュアなライフスタイルを楽しもう!”というウェーブが起きるだろうか。ランキングがそのきっかけを作ることができたらと願っています。

情報セキュリティチェックシート WG

富士通関西中部ネットテック株式会社
嶋倉　文裕

■ 概要

中小企業向け個人情報保護対策 WG として作成した「個人情報保護対策チェックシート」を情報セキュリティ全般を対象としたチェックシートに進化させ、中堅・中小企業の情報セキュリティ対策のガイドライン作成を目指します。

地域性・企業規模への視点での活動が支部に与えられた命題とも考えており、関係する本部の他の WG と連携しながら､整合性にも配意して推進します。

■ 目標

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情報セキュリティチェックシートの作成が目標です。

また、ユーザ側からの要請を認識することで、SI'er, ベンダーの RFP に活用して頂くことが可能なもの作成を目標とします。

■ 活動内容

月に一度の定例ミーティングを実施して各 WG メンバの活動報告や作成物の内容確認などを行います。

関係する本部の他の WG とも連携しアドバイスを頂くだけでなく、地域の特性による既存情報セキュリティ対策の限界、限界を補完する組織・人のオペレーショナルでの考察を行い、本部 WG に発信していくことも予定しています。

また、関西の中堅・中小企業を対象とした情報セキュリティチェックシートの作成、実態の把握を行うため、近畿経済産業局様、（財）関西情報・産業活性化センター様とも連携し活動します。

■ 予定

【第一フェーズ】

- 情報セキュリティチェックシート作成
  ～ 2007.6 末
- 現状調査／ヒアリング
  2007.7 ～ 2007.8
- 調査結果まとめ／解析
  2007.9 ～ 2007.10
- 冊子化
  2007.12 末

【第二フエーズ】

- リスク分析・リスク評価
  2008.1 以降

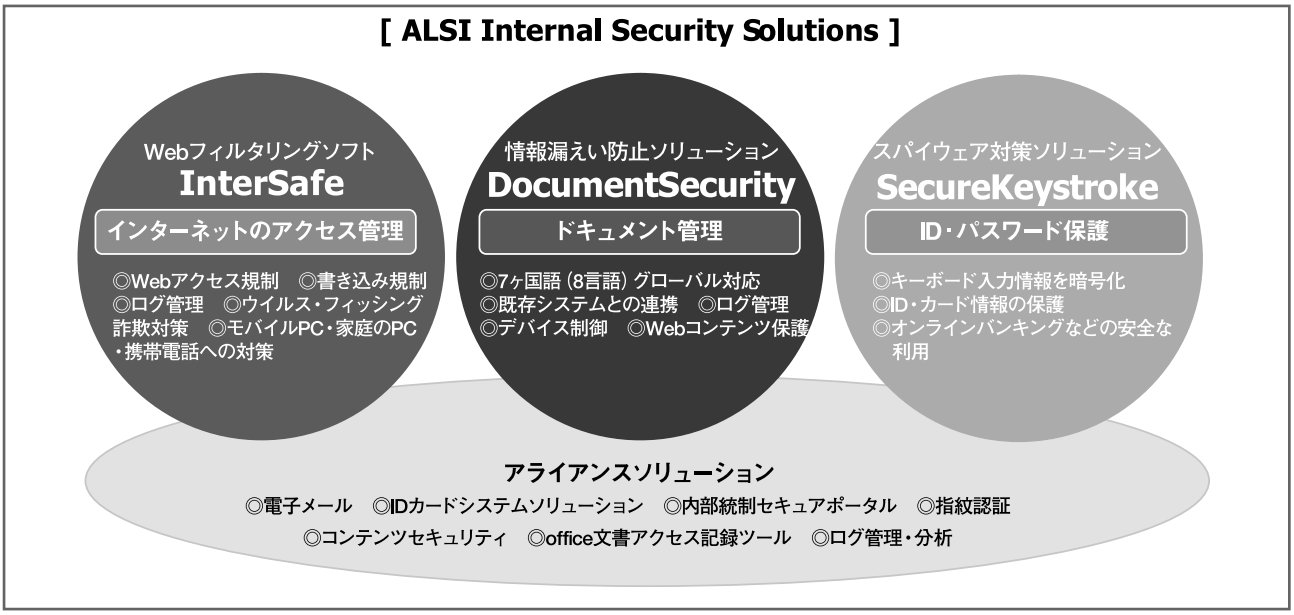
会員企業ご紹介⑲

アルプス システム インテグレーション株式会社

http://www.alsi.co.jp/

情報を守り、活用する。セキュリティの根幹はひとつ。
ほんとうに必要なものをトータルに。それがALSIのセキュリティソリューションです。

「J-SOXは本当に実現できるのか？」「内部統制には手間がかかりすぎる」「海外拠点も含めて一元管理したい」といった企業の声をよく耳にします。このような企業の複雑な課題に対しては、一般的なトータルソリューションの導入では解決できません。不要なものが多く、拘束が強くなるといった課題に突き当たるからです。でもALSIは違います。なによりも、情報のブラックボックス化をしない、つまり「情報は守りながら、活用する」というビジネスの観点に立った技術に裏打ちされているからです。明確なコンセプトで、本当に必要なものだけをより使いやすく。ALSIには真の意味でのトータルセキュリティを実現する力があります。



●「InterSafe」

3年連続でフィルタリング市場シェア1位を獲得（※1）

ALSIは1996年に日本で初めてフィルタリング事業を開始したパイオニア。2000年より発売を開始したWebフィルタリングソフト「Intersafe（インターセーフ）」は、3年連続で「フィルタリング市場」シェア1位を獲得するなど、企業や官公庁、教育現場などで最も導入されている製品です。

（※1）IDC Japan、富士キメラ総研、ミック経済研究所調べ

●「DocumentSecurity」

DRM市場シェア2位を獲得（※2）

情報漏えい防止ソリューション「DocumentSecurity（ドキュメントセキュリティ）」は、「ＤＲＭ(Digital Rights Management)/利用管理市場」で2位を獲得。ドキュメントの「作成･編集･保存･利用･破棄」というライフサイクル全般を、ドキュメントごとに、またユーザ／グループごとに柔軟に設定し、暗号化したファイルに使用制限をかけることで、企業内にある機密情報の流出の防止や、内部統制強化に利用することができます。

（※2）富士キメラ総研調べ

●「SecureKeystroke」

なりすましの被害を防ぐ新ソリューション

2006年11月より販売を開始した「SecureKeystroke（セキュアキーストローク）」は、キーボードの入力情報を暗号化し、キーロガーなどの被害を防止することができるソリューション。スクリーンショット型のスパイウエアにも対応し、オンラインバンキング、トレード、ショッピング、ゲームなどへの導入が着実に進んでいます。

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
セキュリティソリューション部
〒145-0066　東京都大田区南雪谷1-2-7
ニッセイ雪ヶ谷ビル5F
TEL:03-5499-1331　FAX:03-5499-0357
E-mail:ssg@alsi.co.jp　URL:http://www.alsi.co.jp/

株式会社イージーネット

http://www.eni.co.jp/

株式会社イージーネットは、1993年創業のオープンソース技術に基盤をおくシステム･インテグレータです。
長年養ってきたLinux、ネットワーク技術を基にセキュリティ対策製品を開発、販売しています。

ネットワーク・フォレンジック
NetRAPTOR（ネットラプター）
― 社外とのネットワーク通信を常時記録、監視し、
不適切な使用を検知、報告します！

・全ての通信データを採取、永続的に記録
・強力な検証機能でセキュリティ監査を支援
・同時に情報漏洩の抑止力として効果を発揮

- 通信パケット取りこぼしなし！
- キャプチャー性能ピーク時 930Mbps ！
- *2 秒以内の検索レスポンス！
  （ データ領域 3.6Tbyte 搭載時 ）
- リアルタイム解析 & 警告を管理者へ

* 検索条件により異なります

◆ 機能特徴 ◆

簡易検索･詳細検索

フォームを用いて簡単に検索条件を設定。また、論理式を直接記述することで、より詳細な条件指定も可能。

インテリジェント･ローテート機能

自動的にバックアップとローテートを実現。テープメディアの交換が必要になれば、管理者へ通知。1 台でキャプチャー 、解析、HDD 保存 、バックアップまで同時運用可能のため、バックアップ中にも検索が可能。

高速全文検索機能

BCC 送信メール 、Web メール 、添付ファイルの再現 (Web メール添付ファイルにも対応)。

リアルタイム解析･警告

アラート条件に設定した通信が行われると 、即座に管理者へ通知し 、内容の表示までリアルタイムに行うことが可能。

閲覧者管理機能

閲覧ログの表示･再現機能により閲覧者の監査が可能。また、閲覧可能範囲の限定も可能 (セグメント単位等)。

easyFiLEX- Ⅱ（イージーファイレックス）
― まだメールにファイルを添付しますか？
ファイル送受信に伴う様々なリスクを回避
安全で確実な新ビジネスツール

●メールへのファイル添付を廃止･禁止したい。
●ファイルを送るたびに暗号化するのは面倒だ。
● FTP の利用にセキュリティ上の問題を感じている。
●ファイル送信サービスの利用に不安を感じている。
などなど･･･**こんな問題をお持ちなら、**
easyFiLEX- Ⅱが解決します !!

※ 特許出願中（出願番号：2006-265837）

操作画面イメージ

◆ 機能概要 ◆

・SSL 暗号化通信
・利用者登録によるアカウント認証
・大容量ファイル対応、推奨取扱ファイル容量 2GB 程度
・利用者側で必要なのはブラウザのみ
・操作履歴の確認 (J-SOX、内部統制にも)
・利用者、管理担当者に対するメール一括送信
・管理区分を設け、各区分に管理担当者を置くことが可能
　また、1 区分に複数の担当者を設定できる
・ファイル取得期日、ファイル提出期日等の設定
・ファイル送受信の状況を即座に確認

お問い合わせは e-sales@eni.co.jp
株式会社イージーネット
大阪本社
〒 532-0003 大阪市淀川区宮原 4-6-18 新大阪和幸ビル 8F
TEL:06-6350-0850　FAX:06-6350-0845
東京営業所
〒 143-0016 東京都大田区大森北 1-2-3 大森御幸ビル 6F
TEL:03-3764-0568
URL:http://www.eni.co.jp/

クオリティ株式会社
http://www.quality.co.jp/

Quality Corporation

クオリティ株式会社は、東京を本社として、大阪･名古屋･上海･ソウル･シアトルに拠点をもつソフトウェア会社です。IT資産管理ツールのトップランナーとして、お客様と対話しながら、ニーズにあった製品やサービスを常に提供し、クライアントPCのセキュリティ対策、内部統制構築に役立つソリューションをお客様へご提案してまいります。

昨今、企業活動を支える情報システムは､「日本版SOX法」「会社法」「個人情報保護法」「不正競争防止法」などへ早急な対応が求められています。
クオリティでは、業務処理プロセスを支えるクライアントPC構成維持の仕組みの統制により「新会社法」「日本版SOX法」が求める内部統制の構築をサポートします｡「QAW/QND」を基盤とした『QAW/QND法制度対策ソリューション』は、現状把握から監査、利用制限、社員教育までの幅広い対策をご提供いたします。

IT資産管理ツールの決定版「QND Plus」は国内2,600社250万クライアントの導入実績、東証一部上場企業の6社に1社への導入実績があり、クライアントPCの現状把握から、台帳作成、自動インストール、脆弱性監査までをカバー。 管理工数を削減し、ウイルスや情報漏洩などのリスクから企業を守ります。
また、QND Plusの標準機能に、ソフトウェア起動制御や使用状況の把握などの追加機能を搭載し、クライアントPC構成の維持･管理に加え、管理ポリシに合わせたシステム利用制限が可能な「QAW」を中心に、クライアントPCのソフトウェアを、セキュリティポリシが定めるレベルに自動誘導し、それを維持するソフトウェア「eX LIC」、中小企業など専任のシステム管理者を配置できない企業で利用されているPCのセキュリティ対策に対し、インターネットを利用したサービスをASPで提供できるシステム「ISM(IT Security Manager)」、QAW/QNDが収集したパソコンのIPアドレスやMACアドレスを利用し、QAW/QNDで管理していない私物パソコンを特定、ネットワーク接続を遠隔で遮断するソフト「eX IPD」、QAW/QNDが収集したインベントリ情報とeX IPDが収集したネットワークの接続情報を元に、Winnyなどの社内で認めていないアプリケーションがインストールされているパソコンの利用者と接続場所をレイアウト図でビジュアル特定できる「eX IFM」、USBメモリなどの外部記憶媒体によるデータ持ち出しを制御する「eX WP」、クライアントPCの操作ログ収集ソフト「eX CLT」などのツールを組み合わせることにより、クライアントPCを基点とした企業リスクを低減します。
更に、ビジネス用PDF作成ソフト「DocuCom PDF Driver」と、ファイル単位で厳密なアクセスコントロールを可能にする「DKS Plus」を使用することにより、企業からの機密情報漏洩を防止します。

これらのツールを統合的組み合わせることで、大中小の規模を問わず、企業の強固な内部統制築をサポートいたします。

お問い合わせ先
クオリティ株式会社
〒102-0093 東京都千代田区平河町 1-4-5 平和第一ビル
TEL：03-5275-6124　FAX:03-5275-6130
E-mail：sales@quality.co.jp

TippingPoint 日本支社
http://www.tippingpoint.com/japan/

TippingPoint

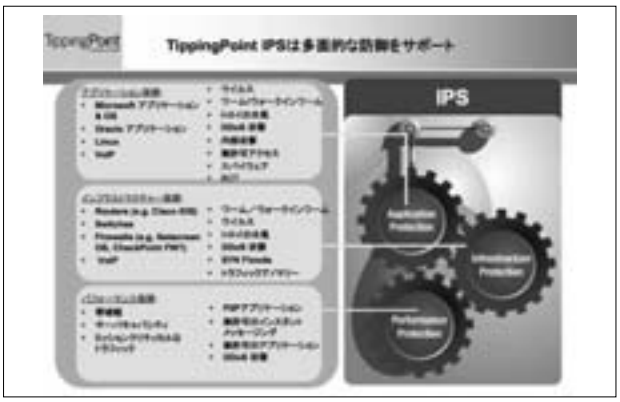
TippingPointは、IPS（Intrusion Prevention System：自動不正侵入防御システム）による統合セキュリティ管理ソリューションを提供しています。2002年に世界初のネットワークベースIPSを発表して以来、業界をリードしてきました。
IPS分野での世界マーケット・シェアでは、No.1（33%）の実績を誇り、世界で最も多くのアワードを受賞してます。
（2005年1月から12月の売上金額　Infonetics Research社調査）
日本では2006年4月に日本支社を設立し、日本市場に本格参入を開始いたしました。

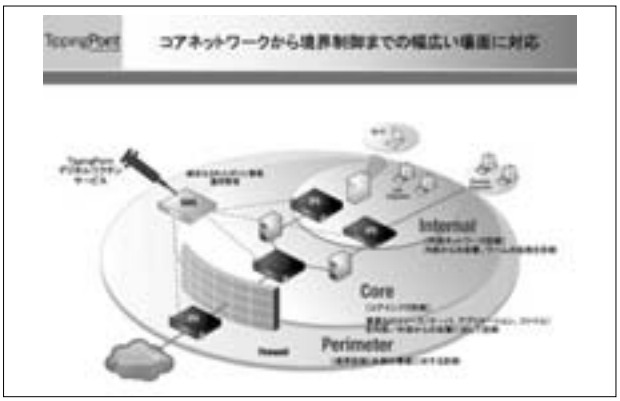
TippingPoint IPS統合セキュリティ管理ソリューションの特徴

1）ネットワーク性能
- ●高性能ASICアーキティチャによる高スループットと低い遅延
- 50Mbps-5Gbpsの拡張性と高可用性

2）不正侵入防御能力
- 実績のある高い検知精度
- コアネットワークから境界制御まで広範囲のネットワーク環境に対応
- Windows/Unix/Linux他主要なOS/DB等の脆弱性にいち早く対応（MS脆弱性に関しては12時間以内に対応）
- DDos攻撃対応

3）運用の容易性
- 実績のある推奨設定による簡単な導入設定
- 既存のネットワーク/アプリケーション環境に変更の必要なし
- デジタルワクチン自動更新による簡単な運用
- SMS(Security Management System：統合管理システム)による複数IPSの一元管理





お問い合わせ先
TippingPoint 日本支社
〒163-1030
東京都新宿区西新宿 3-7-1 新宿パークタワー N-30F
TEL: 03-5326-3063　E-mail: japan@tippingpoint.com

ポイントセック株式会社
http://www.pointsec.com

pointsec

ディスク丸ごと暗号化ソフト「Pointsec」で、情報漏えい対策を！

ノート PC、USB、またはPocket PCを紛失した場合、企業にとって実際の損失はどのくらいになるのでしょう。情報の量や企業規模を問わず、情報漏洩によってもたらされる損害は、目に見えるコストだけでは判断できません。顧客の信頼ダメージや、会社への評価。この数値化できない損害が、企業が最も恐れるべき損失です。統計によると、情報漏洩の原因は、60%がPCなどの機器の紛失と盗難です。ネットワークへの不正侵入による情報流出が25%であることに比べると、モバイル化が進んだ現在、従業員が使用するモバイル機器は、機密情報や個人情報の保護において潜在的な弱点となっていることがわかるでしょう。従業員が仕事をしやすくするために、優れたモバイル環境を提供し、一方で大切な情報を守る仕組み。それがPointsecを活用した“ディスクごと暗号化する”ソリューションなのです。
代表的なソリューションは、以下の通りです。

■ Pointsec for PC

クライアントPCにインストールするだけで、OSやシステムファイル領域を含め、ハードディスクを自動的に暗号化するセキュリティ製品です。

暗号化は強固なアルゴリズムを採用し、また暗号化/復号化を自動的に行うため、高い信頼性と簡単な操作性を実現しました。さらにパスワードハッキングを防ぐためにWindows起動前に認証を行うなど安全性も兼ね備えています。

■ Pointsec Media Encryption

リムーバブルメディア、ローカルフォルダを自動的に暗号化するセキュリティ製品です。

Pointsec Media Encryptionは、WindowsノートPC、デスクトップPC、CD-RW/DVDドライブ、および外付けハードディスク ドライブに対応しており、携帯用記憶媒体や、電子メールの添付ファイルなどのファイルやフォルダの暗号化も可能です。

■ Pointsec for Pocket PC

Pocket PCのシステム全体の暗号化とアクセス制御を実現するセキュリティ製品です。

Pointsec for Pocket PCは、システムを集中管理できるため、管理者がセキュリティポリシーを設定し、制御することができます。エンドユーザでは、変更することができません。

【製品詳細情報】
http://www.pointsec.com/products/

お問い合わせ先
ポイントセック株式会社
〒 107-0052
東京都港区赤坂 2-22-24 泉赤坂ビル 2 F
TEL: 03-3560-3177
E-mail: japansales@pointsec.com

ワンビ株式会社
http://www.onebe.co.jp

盗難・紛失したパソコンからの個人情報の流出防止を目指して
ワンビ株式会社は、企業、個人の個人情報流出を食い止めるために遠隔地からのデータ消去を実現する「トラストデリート」を中心にあらゆる個人情報漏洩防止を実現するために活動していきます。

遠隔データ消去製品「トラストデリート」

・携帯から消去命令を発行して、盗難・紛失したパソコンのデータを消去
・消去が完了した際には、消去証明書を発行します。

盗難・紛失したクレジットカードの利用停止のように、パソコンのデータを消去
年々ノートパソコンの紛失・盗難は増加する一方です。それに加え個人情報保護を求める声は高まっており、事故発生時の迅速な対応ソリューションが必要になります。
そこで、利用者の信頼された指示でインターネットを介した遠隔地からのデータ消去ソフトウェア「トラストデリート」で企業の情報を守ります。暗号化ソフトと併せて利用することで、さらにセキュリティの向上になります。

標準価格 6,279円（税込）

製品開発背景

個人情報保護法が条例化されてから、管理体制が義務付けられております。しかし、いままでのセキュリティで一時的に情報を保護することはできますが時間をかければ解析することも不可能でありません。また、利用者にとって運用が難しかったりすると、そのセキュリティをはずしてしまっているケースもあります。
普段のパソコンの利用方法のまま運用ができ、万が一パソコンの盗難・紛失にあった場合には、携帯などから、消去命令を出すだけでパソコンの重要データを消去してパソコンを利用できなくすることができるソリューションが必要だったのです。

会社概要

コンピュータの利用者のニーズを1つにまとめて、製品として成し遂げるために集まったプロダクトマネージメント集団です。日本では、製品化、サービス化させるためのマネージメント経験者が圧倒的に少ないために、埋もれているアイディアが数多くあります。それらの奇抜な発想や先進的な技術を、経験豊富な私たちプロダクトマネージメント集団が、製品化および市場に浸透させることを目的としております。

お問い合わせ先

〒151-0053
東京都渋谷区代々木2丁目16－15
新宿オークビル3階
TEL　03-6909-0305
eMail info_ml@onebe.co.jp

JNSA 会員企業情報

JNSA 会員企業のサービス・製品・イベント情報です。

■製品情報■

○BRODIAEA safeAttach（ブローディア セーフアタッチ）

BRODIAEA safeAttachは、電子メールの添付ファイルを自動で暗号化を行うサーバアプライアンス。暗号化により、メールの誤送信などによる情報漏洩のリスクを抑制する。また、サーバ側で暗号化を行うため、暗号し忘れなどの「うっかり」ミスも防止でき、作業効率の低下も防ぐことができる。

【製品情報詳細】
http://www.orangesoft.co.jp/safeAttach

◆お問い合わせ先◆
株式会社オレンジソフト 営業部
TEL: 03-5475-6451
E-mail: sales@orangesoft.co.jp

○NetRAPTOR

NetRAPTORは全ての通信データを記録保存し、万が一の際には迅速に検索、追跡調査を行えるネットワーク・フォレンジック製品です。わずかなパケットロスでも該当箇所の通信再生はできないことから、NetRAPTORは実用帯域でのパケット･キャプチャー100%を実現しました。またリアルタイム解析機能により、発生と同時に監査担当者へ告知し、キャプチャー･データの即時検索を実現。閲覧監査機能など実用に即した機能も実装しました。

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

◆お問い合わせ先◆
株式会社イージーネット
E-mail: e-sales@eni.co.jp

○NOD32アンチウイルス V2.7」

「NOD32アンチウイルス V2.7」は、ウイルス定義ファイルにはない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、最新OSのWindowsVistaに対応。検出することが困難とされてきたルートキットなどのステルス技術を利用したマルウェアも検出･駆除が可能です。

高速かつ軽快に、既知･新種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

○世界標準 暗号化ソリューション『PGP』

PGPは世界標準のメール暗号化ソフトとして世界中1000万を超えるユーザに愛用されています。暗号化強度、信頼性は世界トップレベルで様々な公共機関､企業にも導入されています。

メール暗号化機能のみならず、ファイル・フォルダの暗号化から、ハードディスク、共有フォルダなどさまざまな分野の暗号化を同一プラットフォーム上で実現しています。

【製品情報詳細】
http://www.nsd.co.jp/pgp/

◆お問い合わせ先◆
(株)日本システムディベロップメント 第8システム本部
E-mail: pgp@nsd.co.jp
TEL: 03-3342-1411　FAX 03-3342-0453

■サービス情報■

○P2Pチェック･削除プログラム「CS-F運用支援サービス」

暴露ウイルスによるファイル交換ソフトを介した情報漏洩事故が多発していますが、PCからファイル交換ソフトを検知･排除することが最も効果的な対応策です。
「CS-F運用支援サービス」で使用する「CS-F」は、業務や自宅で使用するPCにそれらのファイル交換ソフトがインストールされているかをチェックし削除するソフトで、管理者は環境に合わせた設定を個別に運用、管理することができ、情報流出の予防対策としてリスクの低減を支援します。

【サービス情報詳細】
http://www.dit.co.jp/security_service/cyberinfo/cs-f.html

◆お問い合わせ先◆
株式会社ディアイティ　セキュリティサービス事業部
TEL: 03-5634-7654
E-mail: info-ssd@dit.co.jp

○ホームページ情報漏えい診断サービス

暴露ウイルスによるファイル交換ソフトを介した情報漏洩事いまだに増え続けるホームページを悪用した情報漏えい事件。
2006年、弊社の診断サービスを導入していただいたお客様のうち、危険があるサイトと診断されたお客様は6割以上にものぼりました。
このような状況の中、貴社のサイトは「安全」といえますか？
ラックは「人の手」によるチェックを徹底し、積み上げた豊富な経験と実績を元に診断サービスを提供しております。

【サービス情報詳細】
http://www.lac.co.jp/business/sns/consulting/inspection/diagnosis.html

◆お問い合わせ先◆
株式会社ラック　SNS事業本部
TEL: 03-5537-2610
E-mail: sales@lac.co.jp【申込み】

JNSA 表彰のご報告

JNSAでは、情報セキュリティ向上のための活動を積極的に行い広く社会に貢献した、あるいはJNSAの知名度向上や活動の活性化等に寄与した個人、団体、JNSAワーキンググループを対象に「JNSA賞」と称する表彰を贈る制度を、2006年度に発足いたしました。

この賞は、情報セキュリティの向上に寄与された方々を広く紹介し、その活動を称え、更に積極的な活動をしていただけるよう、設置したものです。この賞が、広く社会に情報セキュリティが根付く発端となり、より良い社会を実現できる一助になればと考えています。

● JNSA賞発足の経緯

JNSAの活動の多くは、会員企業のボランティアに成り立っています。JNSAも発足から6年が経ち、今までJNSAの知名度向上や情報セキュリティの向上へ多大なる貢献をされた方々やワーキンググループを表彰し、さらなる活動への寄与や新しく活動へ参加される方々の目標となるように、という観点から、この度、「JNSA賞」という表彰制度を発足することといたしました。

● 受賞者決定まで

2006年8月に、過去にJNSAの知名度向上、活動の活性化、また広く社会の情報セキュリティの向上に貢献した個人、団体、JNSAワーキンググループの推薦(自薦、他薦は問わず)を募集し、9月の幹事会で第1次選考会を行い、10月の最終選考には過去と現在の部会長の皆様にお集まりいただき、2時間に渡る討論の末、受賞者を決定しました。

● 受賞者の発表

選考結果は11月13日(月)に主催カンファレンス「Network Security Forum 2006」の場で石田会長より発表を行い、翌年1月のJNSA賀詞交換会にて表彰式を行いました。

賀詞交歓会風景

● 表彰式

翌2007年1月23日に八重洲富士屋ホテルにおいて行われたJNSA新年賀詞交換会の場にて、JNSA賞受賞者の表彰式を行いました。

当日は、JNSA会員129名ならびに来賓37名の166名が見守る中、石田会長より、各受賞者への表彰状・表彰楯・金一封の授与を行いました。

2006年度のJNSA賞受賞者ならびにワーキンググループは以下の通りです。

全受賞者と石田会長

ワーキンググループ(WG)の部(3件)

○個人情報保護法ガイドラインWG

(WGリーダー:株式会社大塚商会 佐藤 憲一 氏)

2001～2005年の4年間で「個人情報保護法対策セキュリティ実践マニュアル」を2版執筆・出版し、JNSAの知名度向上と広く社会の情報セキュリティの向上に貢献。

○セキュリティ被害調査WG

(WGリーダー:株式会社ディアイティ 山田 英史氏)

2001年度より「情報セキュリティインシデント被害調査」を実施、中でも情報漏洩損害額の算出式の成果物は社会的注目を浴び、多数の引用・参照を受けながら毎年広く活用され、JNSAの知名度向上と広く社会の情報セキュリティの向上に貢献。

○PKI相互運用技術WG

(WGリーダー:セコム株式会社IS研究所 松本 泰 氏
サブリーダー:富士ゼロックス株式会社 稲田 龍 氏)

日本国内外における、PKIの技術に関する啓発活動を2000年より継続的に実施し、IETFで議論されるなど国際的にも注目を浴びた。中でも相互接続実験環境の構築では、PKIにおける複雑な認証環境の実現に貢献。

WG 部門の受賞 WG 代表者

個人の部(4件)

○大谷 尚通 氏

(株式会社NTTデータ／セキュリティ被害調査WG)

セキュリティ被害調査WGの「情報セキュリティインシデント調査」報告書作成において、情報収集・グラフ作成・報告書の推敲などを主に担当し、報告書の作成に陰ながら長年にわたり大きく貢献。

○土屋 茂樹 氏

(株式会社NTTデータ／セキュリティポリシー WG)

2002年度ならびに2003年度にセキュリティポリシーWGリーダーとして「情報セキュリティポリシー・サンプル0.92a版」等の成果物のとりまとめを行った。これらの成果物は、対外的にJNSAの認知度向上に大きく貢献し、その成果は今に至っても継続的に利用され続けている。

○山本 匡 氏

(株式会社損保ジャパンリスクマネジメント／セキュリティ被害調査WG)

2001年度から2003年度まで、セキュリティ被害調査WGリーダーとして、WGの運営・報告書の作成等を担当、現在各方面で利用されている損害賠償被害額の算出などの報告書作成の基礎を築く。

○松本 泰 氏

(セコム株式会社IS研究所／ PKI相互運用技術WG)

PKI相互運用技術WGのリーダーとして、日本におけるPKIの普及、具体化および啓発活動で主体的な活動を実施し、技術の促進とJNSAの知名度向上に大きく貢献。

個人部門の受賞者

特別賞(2件)

○山田 英史 氏

(株式会社ディアイティ／セキュリティ被害調査WG)

○渡部 章 氏

(株式会社アークン／不正プログラム調査WG)

情報セキュリティに関する普及啓発活動や各方面での貢献を評価され、経済産業省商務情報政策局長表彰を受賞。それによりJNSAの知名度向上に大きく貢献。

JNSAでは、今後も継続してこの表彰制度を実施していきたいと考えております。いずれは、JNSA会員内だけでなく非会員の方も表彰対象者としてこの表彰制度を世の中に拡げてくことも視野に入れて検討していく予定です。

(JNSA事務局)

イベント開催の報告

JNSA 西日本支部主催セキュリティセミナー
NSF2006 in Osaka『日本版ＳＯＸ法に求められる情報セキュリティの役割』

ＪＮＳＡ西日本支部　メンバー
富士通関西中部ネットテック株式会社　岡本　登

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 10 回セキュリティセミナー NSF2006 in Osaka『日本版 SOX 法に求められる情報セキュリティの役割』が、経済産業省、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、財団法人ひょうご情報教育機構、財団法人関西情報・産業活性化センター、NPO 滋賀県情報基盤協議会、NPO なら情報セキュリティ総合研究所、NPO 情報セキュリティ研究所、NPO GIS 総合研究所の後援のもと、10 月 26 日（木）に大阪市にある大阪国際会議場において開催されました。当日は、非会員の方 34 名を含め、63 名の方にご来場頂きました。
今回は、内部統制必須の時代を迎える中、情報セキュリティが自己防衛の目的だけはなく社会責任を全うする上でも重要な経営要素の一つになろうとしていることから、『日本版 SOX 法に求められる情報セキュリティの役割』をメインテーマとして取り上げ、講演では、政府の立場から、また学術的な観点から、さらには企業での実践事例に関してご講演を頂いたほか、JNSA 西日本支部の活動である中小企業における個人情報保護対策 WG からの成果報告もありました。本セミナーを通して、内部統制を効率よく、かつ実効力を持つものにするには、どのような観点で、どのようなセキュリティ対策を考えなければならないのか、またその課題と解決策とはどのようなものなのか、多少なりとも皆様のご参考にして頂けたものと確信しております。以下、当日のアンケート結果なども交えて簡単に内容をご紹介致します。

まずプログラムの最初に井上JNSA西日本支部長から、今回のセミナーに寄せる期待とご挨拶をさせていただき、引き続いて、基調講演として、「情報セキュリティを巡る状況と政府の対応について」と題して経済産業省　情報セキュリティ政策室 課長補佐 下田 裕和様からご講演を頂きました。


基調講演（経済産業省 下田裕和 氏）

時代の変化や事故の事例などの背景とともに、政府全体の取組みについて詳しくご説明を頂き、さらに情報セキュリティに対する経済産業省の具体的な取組みについてご紹介を頂きました。ご参加頂いた方々のアンケート回答を見ますと、政府や経済産業省の取組みについて豊富な内容で、大変勉強になったとのご意見を多数頂きました。安心･安全な情報経済社会の実現に向けた具体的な方向が示された貴重なご講演であったと思います。

2番目の講演は、「内部統制と情報セキュリティ　～グローバルエクセレンス企業を目指し～」と題し、松下電器産業株式会社 情報セキュリティ本部 本部長の金森 喜久男様からご講演を頂きました。

本ご講演では、実際に社内で実践された大変貴重な事例をご紹介頂き、これからの取組みにおいて、非常に参考になる内容であったかと思います。特に取組みに対する理念が明確であり、そこから発せら

れるメッセージには強い印象が残りました。「全社一丸となって取り組んでいる」などのアンケート回答からも参加された方々の受けられた印象が感じ取れます。

3番目の講演は、「日本版SOX法対応に向けた中堅・中小企業における内部統制とIT活用」と題し、NECネクサソリューションズ株式会社 コンサルティング部 部長の持田 敏之様からご講演を頂きました。

本ご講演では、コンサルタントのお立場から、内部統制をどのように構築していくかについてわかりやすく整理されたご説明を頂きました。どのように進めればいいのかという悩みをお持ちの参加者の方々には、ガイドラインとして活用できると感じて頂けたのではないでしょうか。アンケート回答でも「とても分かり易い説明でポイントが理解できた」とのご意見を頂いております。

続いて、「西日本支部中小企業向け個人情報保護対策WG活動報告」と題し、JNSA西日本支部のWGメンバーからこれまでの活動の状況を報告させて頂き、その成果物であるチェックシートを講演会場で実際に参加者の方々にチェックして頂くという初の試みをさせて頂きました。皆様のご協力により、貴重なデータが得られましたことを本紙面をお借りして改めて御礼申し上げます。また、アンケートでは、当日の方法等に付きましていくつかのご指摘も頂いておりますので、今後のご参考にさせて頂きます。なお、チェックシートの集計結果につきましては、JNSAのWEBページ（http://www.jnsa.org/result/index.html）にて公開させて頂きましたので、是非ご覧下さい。


中小企業向け個人情報保護対策 WG の発表

最後に、カーネギーメロン大学日本校 教授 武田圭史先生より「JSOX対応と情報セキュリティの見える化」と題しまして、ご講演を頂きました。

JSOX法、内部統制のポイントを踏まえた上で、情報セキュリティの見える化、脅威の見える化についてご説明を頂き、新たな側面から捉えた情報セキュリティの考え方を気付かせて頂いた良い機会になったと思います。アンケートでも「単なるアカデミックな分析以上に具体的であった」などのご意見も頂き、今後の武田先生の研究に注目して行きたいと思います。

おわりに

何からどのように取り組めばよいのかが悩ましいJ-SOX対応ですが、国内の動き、具体的な事例や方法論、また新しい視点での捉え方など、今後の対応に参考となる内容が盛りだくさんのセミナーだったのではないかと思います。J-SOXが適用される平成20年4月1日まで、もうあまり時間がありません。これまでは情報セキュリティが経営課題として取り上げ難い現状にありましたが、今後は中小企業をはじめとするあらゆる企業において、J-SOX対応に取り組む上で健全な情報セキュリティ対策こそが必須不可欠であるという認識を新たにしたセミナーになったと感じました。

NSF2006 概要報告

2006年11月13日（月）～14日（火）にベルサール神田でNetwork Security Forum 2006（NSF2006）が開催されました。今年も昨年に引き続き、コンファレンスに重点を置く形で実施され、事前申し込みも多くが満席となる盛況となりました。

＜来場者数＞

11月13日（月）天候／晴れ 730名
11月14日（火）天候／晴れ 337名
合計来場者数　1,067名

コンファレンスの構成

コンファレンスは、次ページのプログラムのように2日間に渡って開催され、1、2日目とも午前中の2つの基調講演と、午後のJNSAセッションとソリューションセッションで構成されています。プログラムの詳細については、JNSAのWebページからご覧ください。

基調講演は政府系の施策の話、学術系の技術や教育の動向解説、企業経営の視点からの企業統治やリスク管理などの話題と、最近の話題や興味を引くものでした。

JNSAセッションは、主に技術系と管理系の2セッションがパラレルに走り、さらにJNSA会員企業の製品サービスを中心とした紹介セミナーが2セッション用意され、4セッションが同時進行する形で進められました。沢山のセッションが用意され、あるいは聞きたいセッションが重なってしまった方もいらっしゃるかもしれませんが、それだけネットワークセキュリティの内容の裾野が広がり、専門性も高くなってきたのだと思います。

講演の資料は、JNSAのWebページから公開されていますので、内容についてはこちらをご覧になってください。かなり深い内容の講演が多く、聞き応え十分だったと思います。

基調講演の概要

1日目の基調講演の1番目として、内閣官房情報セキュリティセンター（NISC）情報セキュリティ補佐官 山口 英氏による「わが国の情報セキュリティ政策の方向性」が話されました。最初に補佐官としては、合意形成を作るのが主眼であり、情報セキュリティにおける基本的な将来像を作ることが重要だと話されました。このためにもパブリックコメントにいろいろな意見をインプットして欲しいとのことです。

2番目の基調講演は、東京電機大学の佐々木良一教授による「情報セキュリティ 2.0」が話されました。情報セキュリティの歴史や道筋について触れられ、攻撃もフィッシングからファーミングになり更にファクトリー（工業）になるのではないか、との問題提起がされました。最後に安全・安心を実現するためには広い観点からのアプローチが必須であると締めくくられました。

2日目の最初の基調講演は、経済産業省商務情報政策局情報セキュリティ政策室室長の頓宮裕貴氏による「経済産業省の情報セキュリティ政策について」というお話でした。2006年2月に策定された「第1次情報セキュリティ基本計画」等を踏まえて、企業等にお

基調講演（NISC 山口氏）

スポンサーセッション（ラック西本氏）

JNSA セッション（牧野弁護士）

ける制度的な情報セキュリティ対策を施策として実施する際の考え方や方向性について解説されました。

2番目は、ウッドランド株式会社代表取締役社長、財団法人国際IT財団副理事長の安延申氏から「内部統制と企業リスク管理」というテーマで話されました。いわゆるJ-SOX法の考え方や目的などについて解説され、企業の経営リスクと情報セキュリティの関係を、内部統制やリスク管理の観点から捉えることが重要であることが示されました。

さいごに

2006年のNSFは、インターネットや社内ネットワークだけでは無く、広く社会的な側面に対する技術的な問題点や現状について説明されました。また、J-SOXや情報セキュリティ報告書、フォレンジクスと、技術の背景を持った管理運用面の現状も大きなテーマになっていました。技術だけでは解決できない。だけど、技術の背景がないと施策もできないことが、ますます実証されてきた感じがします。

今後、NSFは形を変えてディスカッションと情報共有を行うことを考えて行きたいと計画しています。会員の皆様からのいろいろなアイディアを頂戴できれば幸いです

イベント開催の報告

プログラム概要

2006 年 11 月 13 日（月）		
	A会場	B会場
10:00 ｜ 10:50	【A-01】基調講演	
	わが国の情報セキュリティ政策の方向性 内閣官房情報セキュリティセンター（NISC）情報セキュリティ補佐官　山口 英	
11:00 ｜ 11:50	【A-02】基調講演	
	情報セキュリティ 2.0 東京電機大学教授　佐々木 良一	
13:00 ｜ 13:50	【A-03】	【B-03】
	ISO/IEC15408 評価及び認証制度について 独立行政法人情報処理推進機構（IPA） セキュリティセンター 情報セキュリティ認証室研究員 竹内 斎之郎	巧妙化するオンライン詐欺 株式会社セキュアブレイン プリンシパルセキュリティアナリスト 星澤 裕二
14:00 14:50	【A-04】	【B-04】
	地方公共団体の情報セキュリティ／埼玉県庁の事例 ～職員のセキュリティ意識向上に向けて～ 埼玉県総務部 IT 企画課 セキュリティ担当主査 小室 武晴	Forensics と Anti-Forensics の攻防 NSSL（National Security Strategy Lab.）[仮称] 主席研究員 永田 弘康
15:10 16:00	【A-05】	【B-05】
	情報セキュリティ報告書を公開して ～継続的な取組みへのチャレンジ～ 富士ゼロックス株式会社 情報セキュリティ部 部長 関 昭男	ボットネットに見る脅威の変化と今後の対応 JPCERT コーディネーションセンター 理事　真鍋 敬士
16:10 ｜ 17:00	【A-06】	【B-06】
	暗号モジュール試験及び認証制度について 独立行政法人情報処理推進機構（IPA） セキュリティセンター暗号グループ グループリーダー 山岸 篤弘	移動通信の安全と安心 株式会社 NTT ドコモ モバイルコンピューティング推進コンソーシアム 研究開発本部 サービス & ソリューション開発部 セキュリティ方式担当部長 本郷 節之

2006 年 11 月 14 日（火）		
	A会場	B会場
10:00 ｜ 10:50	【A-11】基調講演	
	経済産業省の情報セキュリティ政策について 経済産業省商務情報政策局情報セキュリティ政策室 室長　頓宮 裕貴	
11:00 ｜ 11:50	【A-12】基調講演	
	内部統制と企業リスク管理ー企業経営の視点から情報セキュリティを再考するー ウッドランド株式会社 代表取締役社長／財団法人国際 IT 財団 副理事長　安延 申	
13:00 ｜ 13:50	【A-13】	【B-13】
	内部統制監査を見据えた IT 統制への対応 日本大学商学部・大学院商学研究科 教授 商学博士　堀江 正之	暗号技術の最新動向 三菱電機情報技術総合研究所 情報セキュリティ技術部長 松井 充
14:00 ｜ 14:50	【A-14】	【B-14】
	デジタルフォレンジックと法的責任 牧野総合法律事務所 弁護士　牧野 二郎	東京工業大学の認証システムのご紹介： UPKI の実現に向けて 東京工業大学・学術国際情報センター 講師　飯田 勝吉
15:10 ｜ 16:00	【A-15】	【B-15】
	米国政府機関 FISMA コンプライアンスの動向と学ぶべきこと 株式会社 日立製作所 セキュリティ事業部 セキュリティソリューション推進本部 技師 JASA（日本セキュリティ監査協会）調査研究部会 WG1 サブリーダ 難波 電	Web (Attack) 2.0 - 新技術の表と裏 ～より便利に、より安全に使うためには～ 住商情報システム株式会社 ネットワーク・セキュリティソリューション事業部 営業統括部 担当部長 兼 情報システム部長付 CISSP JNSA 技術部会長 二木 真明
16:10 ｜ 17:00	【A-16】	【B-16】
	保証型情報セキュリティ監査のフレームワーク 工学院大学情報学部 教授 IBM ビジネスコンサルティングサービス株式会社 顧問 公認情報セキュリティ主席監査人 大木 栄二郎	標準はどう実装されているか？ ～ OpenSSL における SSL/TLS の実装に関して～ 富士ゼロックス株式会社 サービス技術開発部 マネジャー 稲田 龍

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 年度の開催状況は次ページのとおりです。

【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。（2007 年 2 月 28 日現在）

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/

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
4月12日(水)	福井県	(特)ナレッジふくい	福井県生活学習館　ユー・アイふくい
5月12日(水)	福井県	(特)ナレッジふくい	福井市フェニックスプラザ
5月21日(日)	長野県	上野が丘公民館　青少年育成懇談会	上田市神科新屋生活改善センター
5月27日(土)	石川県	石川県健康福祉部子ども政策課　児童育成グループ、 (特)ナレッジふくい	石川県青少年総合研修センター (ユースパルいしかわ)
6月25日(日)	福井県	福井県生涯学習館(ユー・アイふくい)、(特)ナレッジふくい	福井県生活学習館　ユー・アイふくい
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3F301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10日(月)	長野県	ひかり自治会、上田市マルチメディア情報センター	ひかり自治会館
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3日(木)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
8月4日(金)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
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8日(火)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
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25日(金)	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12日(火)	長野県	上田市マルチメディア情報センター	岩門公民館
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20日(水)	福井県	(特)ナレッジふくい	福井市映像文化センター　メディア実習室
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
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
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7日(土)	長野県	上田市マルチメディア情報センター	別所温泉センター
10月13日(金)	長野県	上田市マルチメディア情報センター	ささや
10月14日(土)	大阪府	大阪工業大学、NPO GIS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14日(土)	大分県	財団法人ハイパーネットワーク社会研究所	大分県立芸術文化短期大学　人文棟 大講義室
10月15日(日)	富山県	富山県総合情報センター	富山県ITセンター　情報工房施設
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)	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)	静岡県	しずおかITフェア実行委員会 (静岡県、静岡情報産業協会、(社)静岡県情報化推進協会)	「B-nest」静岡市産学交流センター
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	滋賀県立彦根工業高等学校
10月28日(土)	新潟県	NPO新潟情報セキュリティ協会	朱鷺メッセ　新潟コンベンションセンター 2階　中会議室　201

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
10月31日(火)	京都府	ITコンソーシアム京都	京都府消費生活科学センター
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11日(土)	北海道	NPOくるくるネット	室蘭市中小企業センター
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　第6集会室
11月17日(金)	福井県	(特)ナレッジふくい	福井県敦賀市西公民館
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
11月23日(木)	三重県	NPO東海インターネット協議会、 財団法人 人工知能研究振興財団	四日市市総合会館　7F　第1研修室
11月25日(土)	千葉県	NPO法人松戸ITVネットワーク	松戸市民劇場　第3会議室
11月26日(日)	鳥取県(新規)	NPO法人はっぴぃりんく、 鳥取県ジゲおこしインターネット協議会	保健福祉センターなわ
12月2日(土)	北海道(新規)	旭川情報産業事業協同組合	旭川市科学館
12月3日(日)	愛知県	NPO東海インターネット協議会、 財団法人 人工知能研究振興財団	今池ガスビル7階　B会議室
12月4日(月)	長野県	上田市マルチメディア情報センター	長小学校パソコン教室
12月6日(水)	山形県(新規)	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　127教室
12月8日(金)	青森県	財団法人 八戸地域高度技術振興センター	八戸インテリジェントプラザ アイピーホール
12月9日(土)	高知県	社団法人 高知県情報産業協会	高知県教育センター分館
12月23日(土)	石川県	NPO法人STAND	石川ハイテク交流センター
1月5日(金)	長野県	上田市マルチメディア情報センター	上田市マルチメディア情報センター
1月6日(土)	長野県	上田市マルチメディア情報センター	上田市マルチメディア情報センター
1月20日(土)	神奈川県	NPO情報セキュリティフォーラム	浦舟複合施設10階 みなみ市民活動センター研修室1・2
1月21日(日)	神奈川県	NPO情報セキュリティフォーラム	秦野市立南が丘公民館　2階　大会議室
1月26日(金)	和歌山県	NPO情報セキュリティ研究所	新宮市人権教育センター
1月27日(土)	福島県	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
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)
2月2日(金)	神奈川県	NPO情報セキュリティフォーラム	神奈川県民センター　2階　ホール
2月5日(月)	神奈川県	NPO情報セキュリティフォーラム	横浜市鶴見区役所　大会議室
2月9日(金)	神奈川県	NPO情報セキュリティフォーラム	葉山町立保育園・教育総合センター会議室
2月10日(土)	滋賀県	NPO滋賀県情報基盤協議会、滋賀県立瀬田工業高等学校	滋賀県立瀬田工業高等学校
2月15日(木)	大分県	別府市教育委員会、 財団法人ハイパーネットワーク社会研究所(協力)	別府市中央公民館
2月16日(金)	神奈川県	NPO情報セキュリティフォーラム	真鶴町民センター
2月17日(土)	長崎県	長崎県立大学、県立長崎シーボルト大学	長崎県立大学、県立長崎シーボルト大学 ※テレビ会議システムによる同時開催
2月17日(土)	島根県	サイエンスクラブ21、NPOプロジェクトゆうあい	エステック株式会社　4階
2月22日(日)	香川県	香川県情報サービス産業協議会、 香川県プロバイダ等防犯連絡協議会	e-とぴあ・かがわ「BBスクエア」
2月24日(土)	滋賀県	NPO滋賀県情報基盤協議会、滋賀県立八幡工業高等学校	滋賀県立八幡工業高等学校
2月26日(月)	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
3月2日(金)	神奈川県	NPO情報セキュリティフォーラム	厚木シティプラザ5階 厚木市ヤングコミュニティセンター
3月9日(金)	神奈川県	NPO情報セキュリティフォーラム	津久井合同庁舎　5階　会議室
3月10日(土)	北海道(新規)	公立はこだて未来大学	公立はこだて未来大学
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
3月10日(土)	島根県	NPO法人プロジェクトゆうあい、三隅情報センター、 島根県立西部情報化センター	ひゃこる情報ステーション研修室
3月18日(日)	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)
3月24日(土)	福井県	(特)ナレッジふくい	福井県生活学習館
3月30日(金)	福井県	(特)ナレッジふくい	丸岡中央会館(高椋公民館)

事務局お知らせ
JNSA ANNOUNCE

1. 主催セミナーのお知らせ

● 2006年度JNSA活動報告会(予定)

会　期: 2007年6月6日(水)
主　催: NPO日本ネットワークセキュリティ協会
会　場: ベルサール神田
参加費: 無料

詳細については、JNSAホームページをご覧下さい。

2. 後援･協賛イベントのお知らせ

1. RSA Conference Japan 2007

会期: 2007年4月25日(水) ～ 26日(木)
主催: RSA Conference Japan 2007実行委員会
会場: 東京プリンスホテル　パークタワー
※2007年4月1日以降「ザ・プリンスパークタワー東京」に名称変更予定
http://www.cmptech.jp/rsaconference/

2. 第11回サイバー犯罪に関する白浜シンポジウム

会期: 2007年6月7日(木) ～ 9日(土)
主催: サイバー犯罪に関する白浜シンポジウム実行委員会
会場: ホテル「コガノイベイ」
http://www.sccs-jp.org/

3.自治体総合フェア2007(社団法人日本経営協会)

会期: 2007年7月11日(水) ～ 13日(金)
主催: 社団法人日本経営協会
会場: 東京ビッグサイト
http://www.noma.or.jp/lgf/

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。

【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)
J-SOX法における「内部統制」の必要性が叫ばれている中で、ITの全般統制として、ITセキュリティに関する対応の必然性が求められている。
その中でも、アイデンティティ管理(アイデンティティ・マネージメント)分野については、 セキュリティポリシーを実装する上での共通基盤として注目されている分野である。
内部統制とアイデンティティ管理の関連をWG討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的とする。
予定成果物は、内部統制におけるアイデンティティ管理の定義とアイデンティティ管理システム設計ガイドライン

【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)
企業における情報セキュリティ確保に向けた取り組みを情報セキュリティガバナンスの構築状況やステークホルダとのコミュニケーション、情報開示の充実度、社会貢献活動などの観点からランキングを算定し、定期的に公表する。
このランキングにより、上位に位置づけられた企業の取り組みを模範事例として公開し、どこまでやればいいのか分からないと言われる情報セキュリティに1つの方向性/トレンドを示したい。

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。

【情報セキュリティ意識調査WG】
(リーダー:蛭間久季 氏/アークン)
総務省請負調査「情報セキュリティ関連サービス提供者から見た、利用者のセキュリティ意識や対策状況に関する現状調査」の実施を目的とする。
予定成果物は「情報セキュリティ関連サービス提供者から見た、利用者のセキュリティ意識や対策状況に関する現状調査」報告書。

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。
成果物は検討中。

【セキュアOS普及促進WG】
（リーダー：澤田栄浩 氏／日本高信頼システム）
各先進国で積極に取り組まれているセキュアOS開発が一段落を迎えようとする今、その利用について協議し、普及促進を図る段階を迎えようとしている。この流れの中で、日本でも様々なソリューションモデルを考案していく必要がある。
当WGでは、様々なタイプのセキュア基盤（OS）を利用したソリューションモデルの考案を行い、当該技術の普及促進を図り、産業界のインフラにまで発展したインターネットを、少しでも安全に利用できるよう社会貢献することを目的として活動していきたい。

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

【Challenge PKI】
（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：瀬川正博 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：瀬川正博 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15日に普及啓発イベント「インターネット安全教室まつり」を実施した。

【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：小屋晋吾　氏／トレンドマイクロ）
会員企業の製品・企画を独自の方法で整理、分類してエンドユーザーに情報提供するサイト「JNSAセキュリティ製品バイヤーズガイド」を設け、一般企業に特に製品導入の為のガイドとして利用していただくことを目的とする。
当該サイトは「ジャンル」と「使う（使いたい）側のニーズ」といった2つの角度から分類することで、ユーザーに高い検索性を提供する特徴を備える。また、ブログを活用した（ユーザー）コメント投稿機能も備えた、双方向メディアとして、活用可能。
この度、会員企業は製品・企画等の登録、掲示、掲載を無料として11月10日に公開の運びとなった。
URL: http://buyers.networkworld.jp/security/

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行政情報セキュリティ CBK－WG】
(旧ISSJP-WG)

(リーダー:大河内智秀 氏/NTTコミュニケーションズ)

CISSP資格認定者が更に日本のセキュリティ保全の価値を高めるための上級資格(ISSJP)を日本向けに作成する試験開発活動を行う。2007年1月に第一回目試験開催を予定している。

【SEA/Jカリキュラム改定作業WG】

(リーダー: 伊藤栄二 氏/ディアイティ)

情報セキュリティ教育のアライアンスベンダーであるSEA/Jより、教育カリキュラム改訂の一連作業(改訂内容検討、決定、教材、認定試験開発)の依頼があり、検討後受託しWG発足後作業を進めている。

カリキュラム検討にあたり、情報セキュリティ推奨教育検討WGでの資料等も参考にしている。

予定成果物は、認定テキストと認定試験。

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「知っておきたい情報セキュリティ理解度セルフチェック」を作成した。

この成果物は、現在JNSAのWeb上で公開している。

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。

【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)

中小企業向け個人情報保護対策WGとして作成した「個人情報保護対策チェックシート」を情報セキュリティ全般を対象としたチェックシートに進化させ、中堅･中小企業の情報セキュリティ対策へのガイドラインとする。

地域性･企業規模への視点での活動が支部に与えられた命題とも考えており、関係する本部の他のWGにも、西日本支部代表として参加しながら、整合性にも配慮して行きたい。

4. JNSA 役員一覧 2007 年 3 月 6 日現在

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（2007年3月6日現在　213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(株)
アライドテレシス
アラクサラネットワークス(株)
(株)アルゴ21
(株)アルテミス
アルプスシステムインテグレーション(株) New
(株)ＩＳＡＯ
(株)イージーネット
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
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Ｒ＆Ｄ
ヴァイタル･インフォメーション(株)
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

【か】

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) New
(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)
(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
(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
(株)ジャパンネット銀行
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
(株)情報数理研究所
新日鉄ソリューションズ(株)
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)セキュアスカイ・テクノロジー
(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 New
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
ＴＩＳ(株)
(株)ディアイティ
TippingPoint New
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 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)
東芝ソリューション(株)
東洋ネットワークシステムズ(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)
日商エレクトロニクス(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)
日本高信頼システム(株)
日本コモド(株)
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)
日本ユニシス(株)
ネクストコム(株)
(株)ネットシステム New
(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

【は】

(株)ハイエレコン
バリオセキュア・ネットワークス(株)

(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)

【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)
みすず監査法人
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
LANDesk Software（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
(有)ロボック

【わ】

(株)ワイ･イー･シー
ワンビ(株)

【特別会員】

特定非営利法人　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
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 New
特定非営利活動法人 日本セキュリティ監査協会 New

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
	8 月 25 日	第 3 回西日本支部会
9 月	9 月 13 日	「SCM フォーラム 2006」協賛
	9 月 15 日	平成 18 年度　情報モラル啓発セミナー福島 後援
	9 月 19 日	第 4 回西日本支部会
	9 月 20 日	第 4 回幹事会
	9 月 25 日	「CPO (Chief Privacy Officer) Japan Summit 2006」協力
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）
	10 月 23 日	平成 18 年度　情報モラル啓発セミナー松山　後援
	10 月 26 日	NSF2006 in Osaka（大阪国際会議場）
11 月	11 月 13 ～ 14 日	「Network Security Forum2006」主催
	11 月 15 日	「第 2 回プライバシーコンサルタントサミット 2006」協力
	11 月 18 日	「日本 IT ガバナンス協会設立記念カンファレンス 」後援
	11 月 21 日	第 5 回幹事会
	11 月 21 ～ 22 日	「BUSINESS CONTINUITY MANAGEMENT 2006」「Compliance & IT 2006」「Storage Management World 2006」後援
	11 月 29 ～ 30 日	「Tokyo International Security Conference 2006 」　後援
12 月	12 月 7 日	Security Day 2006 開催（Internet Week 2006 内）
	12 月 14 日	第 5 回西日本支部会
	12 月 15 日	平成 18 年度　情報モラル啓発セミナー名古屋　後援
	12 月 18 ～ 19 日	「デジタル･フォレンジックコミュニティ 2006 in Tokyo」後援
1 月	1 月 23 日	2007 年　JNSA 新年賀詞交歓会
	1 月 26 日	第 6 回幹事会
2 月	2 月 7 日～ 9 日	「NET&COM2007」　後援
	2 月 7 日～ 9 日	「PAGE2007」　後援
	2 月 16 日～ 17 日	拡大幹事会
	2 月 23 日	「インターネット安全教室」全国連絡会議
3 月	3 月 22 日	第 7 回幹事会
	3 月 28 日	「IC・ID カードの相互運用可能性」技術セミナー (メルパルク東京）

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
NOF 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.19

2007 年 3 月 31 日発行

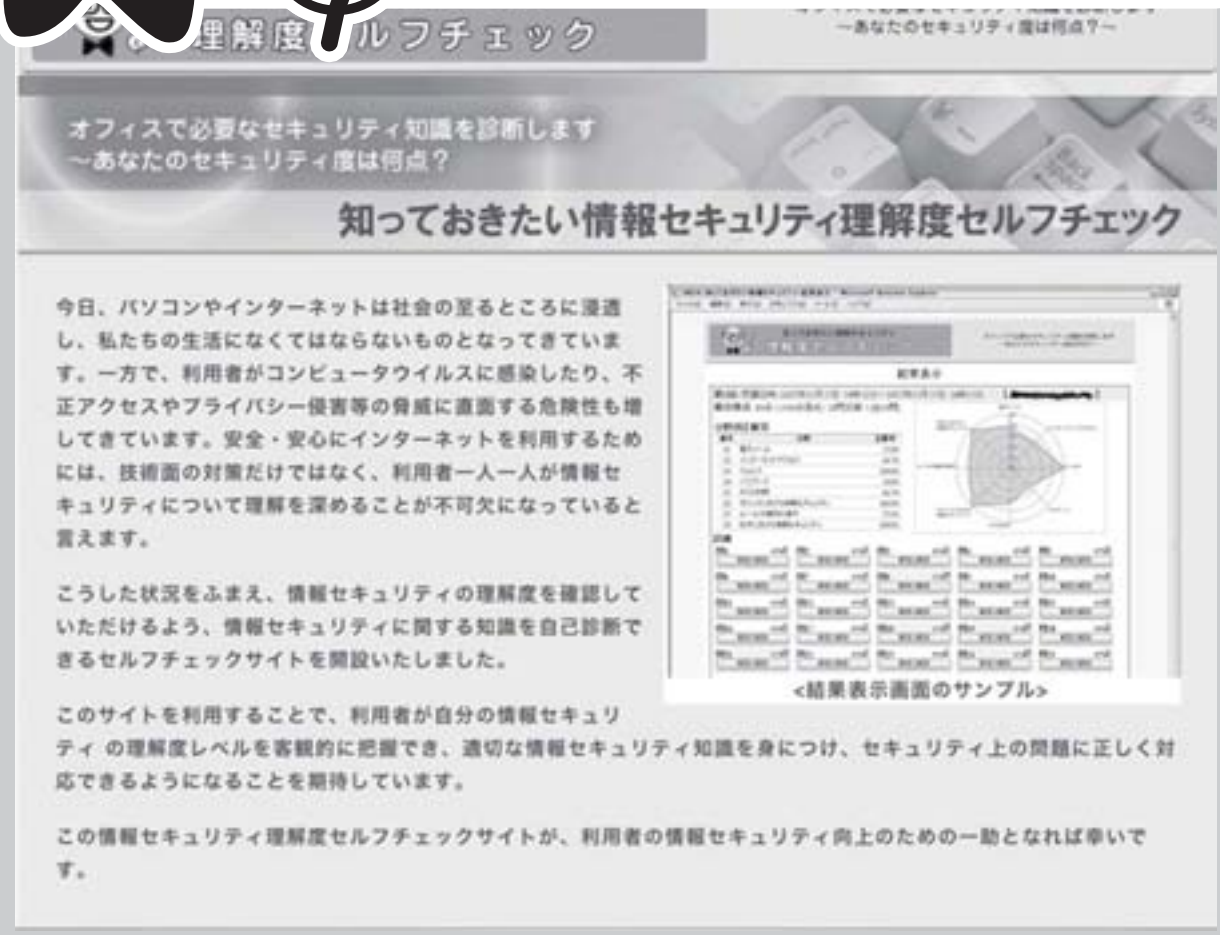
発行所
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
〒 136-0075 東京都江東区新砂 1-6-35　NOF 東陽町ビル
TEL: 03-5633-6061　　FAX: 03-5633-6062
E-Mail: sec@jnsa.org　　URL: http://www.jnsa.org/

印　刷
プリンテックス株式会社

知っておきたい情報セキュリティ
理解度セルフチェックサイト
http://slb.jnsa.org/slbm/

あなたのセキュリティ度は？

オフィスで必要な
セキュリティ知識を
診断します！



JNSA

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 NOF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