JNSA Press

Japan Network Security Association

Vol.12
December 2004

CONTENTS

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

「信頼できるコンピューティング」環境の実現に向けて

マイクロソフト株式会社 業務執行役員　最高セキュリティ責任者
／JNSA副会長
東　貴彦

セキュリティへの取組は、私どもの業界にとって、かつて経験したことのない大規模かつ重大な挑戦となりました。

過去20年間、テクノロジは驚くほどの進歩を遂げ、その成果は企業から一般消費者まで広く活用され、あらゆる人々の可能性を広げています。これに対し、わずかな犯罪的な人間の引き起こす行為はテクノロジとその利用環境への信頼感を損なうものであり、断じて容認することは出来ません。

今や社会に不可欠なインフラとなったコンピュータとネットワーク。その重要な構成要素の一つであるOSベンダーとして、セキュリティに対する取組みは単に脆弱性の継続的修正にとどまるものではありません。ウイルスやワームの発生を抑止するためにはソフトウエアの品質基準について全く新しい考え方が必要となってきました。ツールやプロセスの継続的な改善も必要です。また悪意あるコードや破壊的プログラムからシステムを守るために悪影響を封じ込めて抵抗力を強化する新しいセキュリティテクノロジの開発も求められています。

一方、インターネットを通じてほとんどのコンピュータが相互接続されている現在のネットワーク環境では、ユーザー側にもコンピュータの管理とセキュリティ対策への理解ならびに実施についての積極的な姿勢が強く期待されています。

このため今後のセキュリティ対策は、OSベンダーが自社製品とテクノロジのセキュリティ対策を最優先課題として取り組むと同時に、「技術」と「人」と「プロセス」の三要素が補完的・統合的に機能すること、そしてこれがあらゆるユーザーで実現することを目指して業界とユーザーが一致協力して推進するとことが不可欠と考えます。

JNSAは、「技術」的検証の促進、「人」に対する啓発やトレーニングの実施、「プロセス」の正しい運用の裏づけとしての調査活動、など多岐にわたる活動を行って市場全体として取組むセキュリティ対策の中で重要な役割を担います。

マイクロソフトはJNSAをベストパートナーとして協力し、「信頼できるコンピューティング」環境の実現に貢献したいと考えています。

e-文書法案のインパクトと今後の電子社会のあり方

セコム株式会社IS 研究所
JNSA PKI 相互運用技術WG リーダ
松本　泰

2005年4月の個人情報保護法施行を前に、「個人情報保護バブル」とも思える現象が起きていますが、もうひとつ来年の4月の施行を目指し、本年10月の臨時国会に提出された重要な法案があります。それがe-文書法案です。しかし、e-文書法案は、文書の電子化を促進する狙いがあるものの、その目的やインパクトは今ひとつ見えづらいものがあるのではないでしょうか。個人情報保護法とe-文書法案は正反対な性格を有すると考えられます。個人情報保護法は本格的なネットワーク社会、電子社会を迎えるに至ってこれまで法制度が後追いになり、ともすれば無法地帯化へ向かいそうなネットワーク化に対して、健全なネットワーク社会の発展を促すという元々の意図があったと考えられます。それに対してe-文書法案は全く逆で、これまでの法制度からの制約によりIT 化、ネットワーク化、電子化といったことが阻まれていた業界、業種に対して、これらを促進する狙いがあると思われます。現在のほとんど全ての法制度は、今日のITを想定していない書面に依存した業務を前提とした法制度であり、これらの法制度の規制の対象となる業務に従事する業界及び業種は非常に多いという現実があります。そうしたこともありe-文書法案の本来の意図が発揮されれば、その影響の大きさは計り知れないものがあります。そしてその影響が今後のあるべき社会に向かうよう議論がなされ、また、様々な努力がなされるべきだと考えられます。ここでは、e-文書法案の説明と動向、今後の方向性について説明します。

■e-文書法案の背景

企業内において業務の効率化と迅速化等のために、IT化やネットワーク化が推進されています。電子政府等の推進により、政府と民間の間で電子申請、電子入札等が可能になりつつあり、また、電子契約なども計画されています。そして、民間においても、B2Bなどの電子商取引が推進されています。こうした中、e-Japan戦略では、ブロードバンドの普及などIT基盤の整備が進んでいるとしながらも、そのIT基盤の利活用が進んでいないとしています。利活用が進んでいない理由のひとつと考えられているものに既存の法制度による制約があります。その典型的なものに、紙文書による保存義務を定めた多数の法令等があります。IT基盤を利活用しようにも、その対象となる文書が紙文書では利活用のやりようがないと言えます。法令により保存義務のある文書は、e-Japan戦略の成果とされている低価格なブロードバンドに実際に多く流れているSPAMメールやウィルス、違法コピーのコンテンツとは違い、社会活動、経済活動に大きな意味を持ちます。これらが紙文書から電子文書に移行できないことは、民間の経営活動や業務運営の効率化の阻害要因となっていると考えられます。

以上のようなことから、特に経済界から早期の解決策が求められてきました。2004年3月に日本経団連より発表された「税務書類の電子保存に関する報告書」では、紙文書の保管のために企業が費やしている保管費用は、年間約3,000億円にも上るとした調査結果をまとめています。報告書では、これまで認められていなかった契約書や領収書など、取引の相手方から紙で受け取る書類や手書きの帳簿等についてスキャナ等により電子化した電子文書での保存を認めるよう、要望を行なっています。以下にこれまでの一連の経緯を示します。

2003年7月　「e-Japan戦略Ⅱ」(IT戦略本部決定)
　　民間に保存が義務づけられている文書・帳票の電子的な保存を認める方向で検討
2004年2月　「e-Japan戦略Ⅱ加速化パッケージ」

（重点施策）
「IT規制改革の推進」：「e-文書イニシアティブ」
文書の電子保存を可能とする統一的な法律（e-文書法）

2004年3月　日本経団連の「税務書類の電子保存に関する報告書」

2004年6月　「e-Japan重点計画-2004」（2004年6月、IT戦略本部決定）
e-文書イニシアティブについて（e-文書法の立案方針）

2004年10月12日　e-文書法案の国会提出

2004年10月25日　経済産業省「文書の電磁的保存等に関する検討委員会」の発足

■e-文書法案の概要

e-文書法案は、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（通則法）」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律（整備法）」のふたつの法案から構成されています。前者は、電子保存容認に関する共通事項を定めており、後者は、通則法のみでは不十分な場合等の規定整備を定めています。法案（通則法）自体は極めてシンプルであり全9条で構成されています。

1条　目的電磁的方法により書面を保存、実際の書面の保存負担を軽減する。
2条　定義
3条　電磁的記録による保存主務省令で定める方法で電磁的記録を保存できる
4条　電磁的記録による作成主務省令で定める方法で電磁的記録を作成できる
5条　電磁的記録による縦覧等（注）
6条　電磁的記録による交付等
7条　条例等に基づく書面の保存等に係る情報通信の技術の利用推進等
8条　政令又は主務省令の制定改廃に伴う経過措置
9条　主務省令

附則

（注）内容を見るということを表現する場合、日本の法制度では「閲覧」と「縦覧」という用語が使用されることがあります。「閲覧」が、通常、申し出を待って、請求者に対して内容を調査する機会を与える場合に用いられるのに対し、「縦覧」とは、書類や名簿等について異議申立の機会を与える等の目的で広く一般に内容を見せる場合に多く用いられます。

通則法は、民間で保存が義務付けられた紙文書の電子化を容認する包括的な法律であり、通則法形式の採用により、個別に法改正せずに電子文書保存を容認される法律数は、250本あると言われています。また、技術要件など、具体的な方法は、各主務省令で定めるとするとされているところが重要なポイントです。

■電子保存のための技術要件

主務省令では、実際の電子文書保存の技術的な要件も定められると思われますが、現在、最も注目されているのは、日本経団連の報告書にあるような、紙文書をスキャナにより電子化したスキャン文書による電子文書保存の扱いです。この場合の技術要件としては、様々な意見があるようですが、以下のようなことが検討されているようです。

(1) 可読性（紙と同等の表現力の確保）

これは、一定値以上のスキャン性能、例えば300dpi以上であるとか、256階調（1677万色）以上といった技術要件です。

(2) ファイル形式と圧縮

どういったファイル形式で保存するか、例えばTIFF、PDFであるとかといったことのほか、可逆性のない圧縮

の扱いなど品質に対する影響をどこまで許容するかといった技術要件が検討されています。

(3) 検索性の確保

OCRによる索引の入力や、重要項目による検索機能の確保、例えば、税務書類関係の場合であれば、年月日、金額などの項目が必須になるかといったことが検討されています。

(4) 真正性

入力操作者の認証と電子署名などの要件です。スキャン文書の場合も、このスキャンを行う権限を有する者によって真正に電子化された旨をいかに証明するかといったことが技術要件になります。また、いつからその文書が存在し、それ以後改ざんされていないことを証明するタイムスタンプ(時刻署名)の付与が検討されています。

■税務書類の電子化

税務書類の電子保存は、e-文書法案に関連した最大の関心事のひとつです。それは、ほとんど全ての企業における共通の課題であり、税務に関連したIT化、効率化に対して最大のボトルネックになっていると考えられるからです。

税務書類の電子保存については、e-文書法案の前「電子帳簿保存法」(正式名「電子計算機を使用して作成する国税関係帳簿類の保存方法等の特例に関する法律」)のことを知る必要があります。電子帳簿保存法は、1998年(平成10年)に施行され、各企業、特に大企業においては基幹業務システムとして電子帳票システムが構築され、コスト削減が実現されていると思われます。電子帳簿保存法では、「自己が最初の記録段階から一貫して電子計算機を使用して作成する国税関係帳簿」であって、納税地等の所轄税務署長の承認を受けた場合に限り電子保存が認められています。しかし、紙媒体を電子化したデータの保存は、施行当時のIT技術では真実性及び可視性の保証に対する法的な対抗要件確保が困難との理由で一切認められていませんでした。紙媒体としては、法人税・消費税、源泉所得税、所得税・消費税、その他国税全て紙で受け取る証憑書類があるのですが、特にB2C(見積・契約・注文・領収)においては、電子化が困難なことになってしまいます。これが、今回のe-文書法案では、スキャン文書による電子文書保存を何らかの制約の元に認められる方向で検討されています。

現在、この税務書類の電子文書保存に関する主務省令を定める国税庁の方針が注目されています。日経コンピュータ2004年10月4日号の記事「期待はずれのe-文書法、コスト減は見込めず」では、国税庁の検討している内容では敷居が高すぎるため、e-文書法の恩恵を受ける企業は限られるのではないかといった指摘がなされています。

税務書類の電子保存について進んでいないのはスキャン文書による電子文書保存の是非の問題ではないという指摘もあります。税務書類の電子保存は、e-文書法案以前から「電子帳簿保存法」で認められていたわけですが、同法による恩恵を受けるのはごく一部の企業だけで普及していないという批判が以前からあったようです。電子帳簿保存法では、「自己が最初の記録段階から一貫して電子計算機を使用して作成する国税関係帳簿」に限り、電子保存が認められるとしているのですが、これが一番需要の多い「税法で民間に7年間の保存が義務づけられている帳簿書類」に適用されるわけです。これには「自己が一貫して電子計算機を使用」するシステムを7年間使い続けならなくなり、結果として「電子文書保存」ならぬ「電子システム保存」になってしまうという問題を発生させてしまっているという指摘があります。これについては最後にもう一度説明します。いずれにせよ税務書類の電子文書保存に関して様々な意見があるのはそのインパクトの大きさに起因します。これに関しては、様々な方面からの幅広い議論が期待されます。

■医療関係の動向

医療関係も、電子カルテなどの医療で使用する電子文書の保存が長らく求められていた分野です。そして、この医療に関連した電子文書の保存が、今後の医療のIT化にとっての促進策になるという認識がなされています。

e-Japan重点計画2004では、先導的にIT利活用を推進する先導的7分野のトップに医療が挙げられていますが、そこでは、「ITを活用した医療情報の連携活用」、「ITを活用した医療に関する情報の提供」、「電子カルテの普及促進」、「遠隔医療の普及促進」などの目標が掲げられています。これらの実現には文書の電子化および電子保存が大きな要件になっています。こうしたこともあり厚生労働省の「医療情報ネットワーク基盤検討会」においてこれらの要件が検討されてきました。この検討会の最終報告「今後の医療情報ネットワーク基盤のあり方について」が2004年9月に公表されており、この中で医療分野における電子文書の扱いについて検討した結果が記述されています。以下に電子文書保存に関連した部分の目次を示します。

Ⅲ. 医療に係る文書の電子化
Ⅳ. 医療に係る文書の電子保存
　1. 適切な電子保存の推進
　2. 診療録等の医療機関等以外の場所での電子保存
別紙
　法的に保存が義務づけられている医療関係の書類の電子的保存について
(e-文書法通則法案への対応など)

　この中で、e-文書法案については、電子保存の対象範囲、容認の要件等を整理して適切に対応し、紙媒体で作成された処方せん等は、一定の要件下でスキャナ読込みによる電子保存を容認するとされています。

■e-文書法対応の動向

　e-文書法案に対応したソリューションやサービスの確立に向け、いち早く取り組んでいる団体として画像情報マネジメント協会(JIIMA)があります。JIIMAでは、ずっと以前からJIIMA法務委員会を中心に、法律によって保存が義務づけられている書類を、紙以外の記録媒体で保存することが許容されるよう様々な活動を行っていたようです。具体的には、紙書類等をスキャナにより電子化したもの(電子化文書もしくはイメージデータと呼ぶ)や、マイクロフィルム等の画像情報の法的証拠能力をより確実なものとするための提案がなされていました。JIIMAでは、こうした活動に関連した標準としてJIS Z 6016「紙文書及びマイクロフィルム文書の電子化プロセス」の原案を作成しています。これに関しては、後述する「タイムスタンプ技術に関する調査報告書」にも、その活動が記載されています。

　e-文書法が、紙文書のスキャンを扱うということで、複写機、複合機(MFP)などの業界団体であるビジネス機械・情報システム産業協会(JBMIA)においても、様々な議論がなされているようです。こうした業界では、ネットワークに接続可能なコピー、プリンタ、スキャナ、ファクス機能などを統合したMFP(Multi Function Peripherals)といったものの開発が盛んに行なわれているのですが、このMFPを電子文書の標準的な入出力装置として確立させようと各社、熾烈な競争があるようです。MFPは、ネットワークに接続することを前提としているため、セキュリティに対する機能も必須として新たな応用も色々を検討されているようです。当然のことながらe-文書法の施行もビジネスチャンスと捉え様々な取り組みがなされているようです。MFPの機器自体に耐タンパ性を持った署名装置を組み込むことにより入出力の完全性を保証するといったことなども検討されているようですが、こうした取り組みは、これまでのドキュメントソリューションの考えかたを一変させてしまう可能性を秘めているのではないでしょうか。

　もうひとつは、非常に新しく、まだ業界自体が形成されているとは言い難いのですが、タイムスタンプ関係の業界があり、関連業界団体にタイムビジネス推進協議会があります。e-文書法の整備法が検討されている税務、医療といった分野では、技術要件としてスキャン文書に対してその存在証明を行なうタイムスタンプを施すことを必須とすることが検討されています。これには、このタイムスタンプを発行するタイムスタンプ局(TSA)の要件などが重要になります。総務省から2004年9月、「タイムビジ

ネスに係る指針（ネットワークの安心な利用と電子データの安全な長期保存のために）」といった文書が公表されたのは、こうした背景があります。現在注目されているのは、紙文書をスキャンする際に付与するタイムスタンプなのですが、そもそも、電子文書の保存には、スキャン文書に限らずタイムスタンプは重要な技術であり、その普及が期待されるところです。

■NPO JNSAにおける関連した取り組み

NPO JNSAでは、e-文書法案に関する直接的な取り組みはありませんが、文書の電子化に大いに関係がある電子署名、タイムスタンプといった分野においていくつかの活動がありました。そのうちのひとつに、昨年度のIPA（独立行政法人情報処理推進機構）の公募で採択された「タイムスタンプ・プロトコルに関する技術調査」と、その後追加発注となった「PKI相互運用テストスィートへの機能追加開発および関連調査」があります。以下に「タイムスタンプ・プロトコルに関する技術調査」の目次を示します。

1. はじめに
2. タイムスタンプ技術の概要
3. タイムスタンプ・プロトコル（RFC 3161）
4. タイムスタンプに関連した仕様と標準化動向
5. タイムスタンプに関連した実装
6. タイムスタンプ・プロトコルの相互運用
7. まとめ

参考文献

付録A

　各テストサイトにおけるTST のプロファイル比較

付録B

　PKIX TSP Interoperability Testing Draft

この「タイムスタンプ・プロトコルに関する技術調査」では、タイムスタンプ技術に関する動向を幅広く調査し紹介を行なっています。特にタイムスタンプ・プロトコルの標準であるRFC 3161（Internet X.509 Public Key Infrastructure Time-Stamp Protocol）を中心に、タイムスタンプや長期署名フォーマットなどの電子文書保存に大いに関係した標準化動向、実装上状況などが詳細に記述されています。タイムスタンプのクライアント、すなわちe-文書法などの対応した電子文書保存ソリューション側の視点からの記述が多く、e-文書法対応ソリューションなどの開発や、SI構築のためには非常に有用な資料だと思われます。

もうひとつの「PKI相互運用テストスィートへの機能追加開発および関連調査」では、「タイムスタンプ・プロトコルのテストスィート」、「テストケース」、「タイムスタンプ技術に関する調査報告書」が公開されています。このうちテストスィートとテストケースは、RFC3161の準拠性をテストするツールとテストケースであり、電子文書保存等に使用するタイムスタンプ・プロトコルのクライアントのテストが容易に行なえる環境を提供しています。「タイムスタンプ技術に関する調査報告書」は、技術だけではなく、むしろ現状の利用状況やタイムスタンプ技術に関連した法制度などへの提言といったことが中心の報告書となっており、技術者以外の読者も想定した記述となっています。以下に「タイムスタンプ技術に関する調査報告書」の目次を示します。

1 はじめに
2 タイムスタンプ・プロトコルの技術的可能性
3 民間企業におけるタイムスタンプの利用動向
4 省庁におけるタイムスタンプのニーズ調査
5 まとめ

この報告書の3章の「3.3.4社団法人日本画像情報マネジメント協会（JIIMA）」に先のJIIMAのe-文書法案に対する取り組みが記述されています。この報告書を作成した2004年3月時点におけるいくつかの官民の取り組みについてのヒアリング結果を記述していますが、官においてはタイムスタンプという言葉に対する認識はほとんどなく、民間のサービスもまだ始まったばかりといった印象で

した。しかし、その後のe-文書法フィーバーの中で、電子文書保存に関してのタイムスタンプの重要性は一気に認識が高まったように思われます。

■e-文書法案の課題と来るべき電子社会のあり方

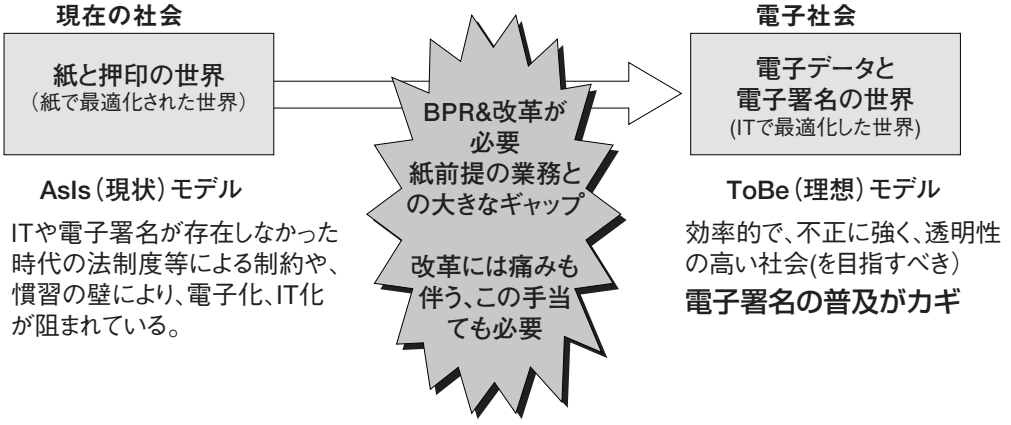
e-文書法案は、電子文書保存を容認する法律であり、電子文書保存を義務付ける法律ではありません。従って、紙による作成・保存から電子文書作成・保存に移行するかどうかという判断は各企業に委ねられています。日経コンピュータ誌「期待はずれのe-文書法、コスト減は見込めず」の記事中では、「企業の期待が大きい税務関連の書類/帳票に関して実際の運用ルールを定める国税庁が、適用対象をかなり限定する上に、電子保存のための技術に高いハードルを設定しようとしている」としています。そして、高いハードルには、スキャナの解像度、電子署名やタイムスタンプといった要件を挙げています。現在のところ、e-文書法案というITを促進するはずの法律が、こうした敷居の高さがアダになって税務関連の書類に関しては実際に利用されないと考える人は多いようです。これは、大変難しい問題をはらんでいます。現在の社会では、法制度で作成・保存が義務付けられた文書等に関しては、まだ、紙文書が中心であり、民間の取引などにおいても紙と押印が主流だと考えられます。それに対してITによる効率化を図るためには文書の電子化は避けて通れない課題であり、e-文書法案の大きな意図はここにあるはずです。一方、理想的な電子社会は、効率と共に不正に強く透明性の高い社会であるべきはずです。これには、やはり電子署名やタイムスタンプといった技術の普及と更なる研究開発が欠かせないと考えられます。

日経コンピュータの記事において国税庁の方が「真贋の判定は職人芸的な作業。現在でも改ざんの疑いのある書類/帳票は、ベテランの調査官が手触りで判別している」とし電子化すると改ざんの危険性が高まるのではないかということを指摘しています。そもそも、こうした不正防止のコストも含め、紙中心の世界での業務の最適化と、電子文書中心の世界での業務最適化には、大きなギャップがあります。長年の積み重ねにより紙文書の偽造の摘発が職人芸的な作業によって可能になったと考えられますが、電子文書には電子文書にふさわしいやり方があるはずで、それを追求し変革を促す必要があるのではないでしょうか。さもなければ、電子政府とかe-Japan戦略とかいった方針そのものが色あせたものになってしまいます。

平成12年に電子署名法（電子署名及び認証業務に関する法律）が施行されていますが、まだ、それほど大きなインパクトを与えていない印象がある理由のひとつは、税務書類の扱いに見られるような既存社会と電子社会の大きなギャップがあります。しかし、社会の基盤としての電子署名などの整備は着実に進んでおり、電子文書保存に関しては、電子署名、タイムスタンプの実用化以前と、現在では全く状況が異なります。電子帳簿保存法の「自己が最初の記録段階から一貫して電子計算機を使用して作成する国税関係帳簿」に限り電子保存が認められるというのは、電子署名法が施行され、電子署名、タイムスタンプが実用化された現在では、もう古い考えにしか過ぎません。電子署名とタイムスタンプが施された電子文書は、その電子文書のデータ自体が、誰の意思によって存在し、改ざん検出が可能で、何時の時点から存在しているかを証明します。こうしたことにより、電子文書は、「電子システム保存」の対象となった装置内に留まらず連携するために必要な電子文書として機能するはずです。e-Japan戦略の中でもIT基盤を利用した連携の必要性が至るところで説かれていますが、官民や利害関係者間などの連携を促進するためには、この電子署名とタイムスタンプが施された電子文書の重要性がもっと認識されるべきだと考えられます。

e-文書法案では、その目的として「国民の利便性の向上を図り、もって国民生活の向上及び国民経済の健全な発展に寄与する」といったことが記述されています。こうしたことを現実のものとするためには、単にこの法案の成立だけではなく、多方面にわたる議論と、技術開発などの更なる努力が望まれます。

※e-文書法は、本原稿執筆後の2004年11月19日に成立し2005年4月1日に施行となりました。



参考文献

(社）日本経済団体連合会「税務書類の電子保存に関する報告書」
http://www.keidanren.or.jp/japanese/policy/2004/018report.pdf

タイムスタンプ・プロトコルに関する技術調査
http://www.ipa.go.jp/security/fy15/reports/tsp/

PKI相互運用テストスィートへの機能追加開発および関連調査
http://www.ipa.go.jp/security/fy15/development/pki_interop/index.html

Challenge PKI 2003 タイムスタンププロトコル（TSP）相互運用テストスィート
http://www.jnsa.org/mpki/2003/index_j.html

日経コンピュータ「期待はずれのe-文書法、コスト減は見込めず」
http://itpro.nikkeibp.co.jp/free/NC/TOKU2/20040928/1/

今後の医療情報ネットワーク基盤のあり方について
医療情報ネットワーク基盤検討会最終報告　平成16年9月30日
http://www.mhlw.go.jp/shingi/2004/09/s0930-10a.html

民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律案
民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律案
http://www.cas.go.jp/jp/houan/index.html

文書の電磁的保存等に関する検討委員会の開催について
http://www.meti.go.jp/policy/it_policy/press/0005730/index.html

「文書の電磁的保存等に関する委員会」の連絡ページ
http://www.jipdec.jp/edoc/

インターネットの「P2P」を理解する

株式会社ネットアーク
代表取締役社長　松本　直人

昨今「P2P」もしくは「ファイル交換」という言葉が、インターネット上でブームとなっています。1999年にMP3ファイルが交換できるNAPSTARが世に出てから既に5年以上が経過しても、その熱は冷めることがありません。現在も問題として指摘されるのが、これらP2P上で交換されるコンテンツの著作権と、情報漏えいの流出先として無限に流通し続けるP2Pの特性について話題は多く、国内でも著作権管理団体などが主導して、P2P上の監視や警告を強めています。海外では、全米レコード協会などが個人を相手取った大規模な訴訟を行っているのも有名なお話です。
国内でも裁判所で係争中のP2Pに関連した事件がいくつかあり、今後も多くの問題整理が必要とされてきています。
インターネットに携わる企業にとって、これらP2Pに関連する問題や情報を正しく理解することは極めて重要です。ここでは、P2Pに関する国内動向や実態をみていきましょう。

1. P2Pの何が問題であるか？

P2Pは、Peer-to-Peer(ピアツーピア)の略称であり、末端のパソコン同士が通信によってデータ交換を行う仕組みを表したソフトウェア技術の総称です。末端のパソコン同士が自由にデータを交換できる反面、出来上がったP2Pネットワーク上で膨大な数の商用著作物が公開される形となり、大きな著作権侵害問題が表れるようになりました。その規模は全世界に及び、国内海外を問わずP2Pネットワークはインターネット上に広がりをみせています。

こうして大規模に出来たP2Pネットワーク上で問題視されるのは、前述の著作権侵害行為にあわせて最近では、情報漏えい問題、ウイルス感染などが挙げられます。オープンに末端のパソコン同士がデータ交換を行うため、どのようなデータでも流れることが出来るため、秘密としておきたかった情報が漏えいし流通し続けてしまうことや、P2Pネットワークから取得したファイルを媒介としたウイルス感染が懸念されています。

2. P2Pの問題点整理

P2Pの問題点を簡単に整理すると次のようになります。

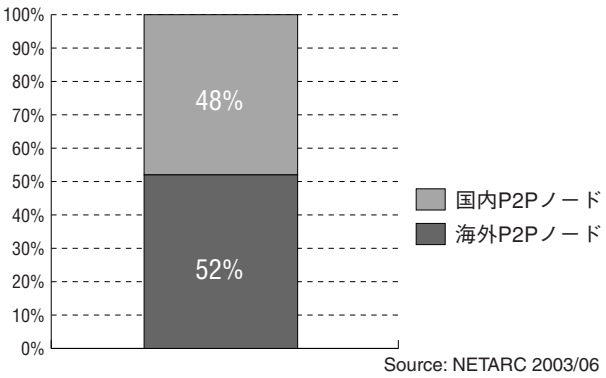
- P2Pの概念自体は優れた技術
- 著作権侵害行為と関連する法令順守への懸念
- 情報漏えいへの懸念
- ウイルス感染への懸念

P2Pネットワークは、無制限・無制御にオープンであるが故に、データ交換される内容によって、問題が複雑化していきます。これら今そこにある問題点を正しく理解しておくと良いでしょう。

3. P2Pの問題は国内だけのはない

P2Pネットワークは、無制限・無制御に全世界のインターネット上に広がっています。我々が調べたところ、P2Pファイル交換による問題は、日本固有の問題ではなく、世界的な問題でありさらに日本のコンテンツであってもP2Pネットワークを介して海外にも流通が進んでいます。

P2Pファイル交換ノードの国内・海外分布（N=143,669）



図：日本語キーワードによるP2Pファイル検索を行ったにも関わらず、国内のみならず海外にもファイル交換ネットワークが広がっていることが理解できます。

データ内容:　データは、2003年6月の1ヶ月間でP2Pノード探索システム P2P FINDERによって集計された累積P2Pノード数を元にしている。探索対象は、国内の利用が多いP2Pファイル交換ソフトウェア WinMX と Winny を対照とし、日本語圏を特定するために、日本語キーワードを用いP2Pファイル交換ネットワークでP2Pファイル検索を行いファイルを公開するP2Pノードを集計している。
集計方法は、過去一度発見されたP2Pノード（IPアドレス）は加算されず、新規に発見されたP2Pノードのみ加算されている。
日本国内を判断する基準としてAPNIC, RIPE, ARIN より報告されるIPアドレス割当地域情報を元にしている。
APNIC: http://www.apnic.net/
RIPE: http://www.ripe.net/
ARIN: http://www.arin.net/

4. P2Pネットワークは世界の国と地域で分布

P2Pネットワークは、日本という国境の概念がありません。インターネット上でコンテンツが交換・公開が繰り返されれば、容易に国境を越えて広がりをみせます。我々の調査結果としても、その数は膨大な国と地域にわたって存在していました。

P2Pファイル交換ノードが存在する国の分布
上位10カ国（N=143,669）

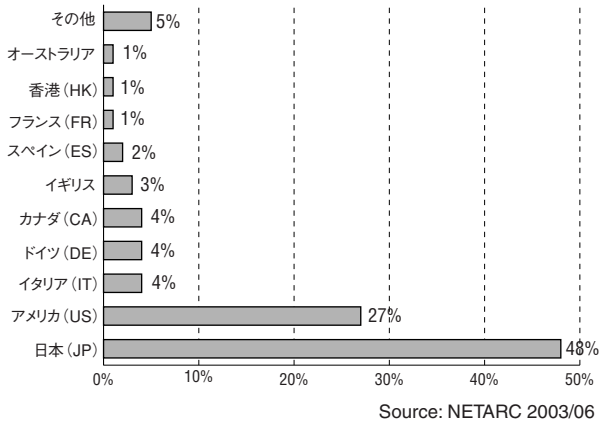


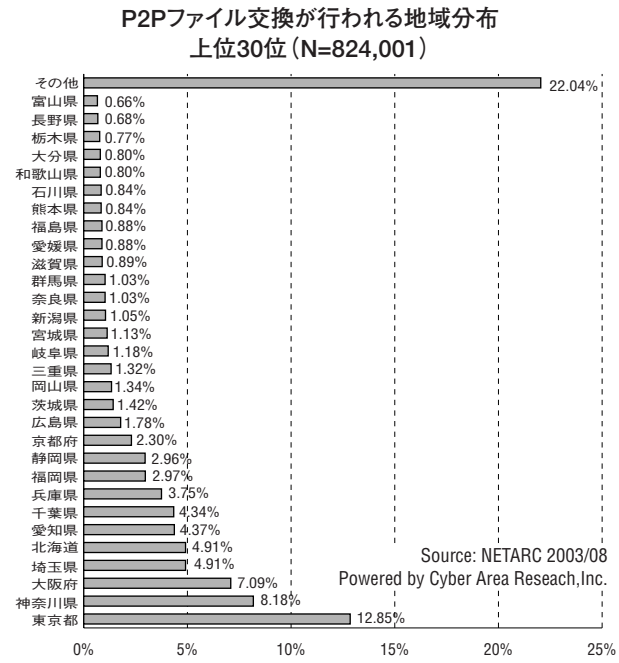
図:　P2Pファイル交換ネットワークは世界各国に存在している。日本とアメリカはもちろんインターネットが存在するほぼ全ての国に、P2Pファイル交換ネットワークが存在することが推測できます。

データ内容:　データは、2003年6月の1ヶ月間でP2Pノード探索システム P2P FINDERによって集計された累積P2Pノード数を元にしている。探索対象は、国内の利用が多いP2Pファイル交換

ソフトウェア WinMX と Winny を対照とし、日本語圏を特定するために、日本語キーワードを用いP2Pファイル交換ネットワークでP2Pファイル検索を行いファイルを公開するP2Pノードを集計している。
集計方法は、過去一度発見されたP2Pノード（IPアドレス）は加算されず、新規に発見されたP2Pノードのみ加算されている。
日本国内を判断する基準としてAPNIC, RIPE, ARINより報告されるIPアドレス割当地域情報を元にしている。
APNIC: http://www.apnic.net/
RIPE: http://www.ripe.net/
ARIN: http://www.arin.net/

5. P2Pは国内地域で分散している

我々の調査の結果から、国内P2Pネットワークは地域に極端な偏りがなく、分散していることがわかってきました。



図：P2Pファイル交換ネットワークは、東京だけではなく各都道府県にほぼ均等に分布しているのが推測できます。

データ内容: データは、2003年6月から8月までにP2Pノード探索システム P2P FINDERによって集計された累積P2Pノード数を元にしている。
探索対象は、国内の利用が多いP2Pファイル交換ソフトウェア WinMX と Winnyを対照とし、日本語圏を特定するために、日本語キーワードを用いP2Pファイル交換ネットワークでP2Pファイル検索を行いファイルを公開するP2Pノードを集計している。
集計方法は、過去一度発見されたP2Pノード（IPアドレス）は加算されず、新規に発見されたP2Pノードのみ加算されている。
日本国内を判断する基準としてAPNIC, RIPE, ARINより報告されるIPアドレス割当地域情報を元にしている。
APNIC: http://www.apnic.net/
RIPE: http://www.ripe.net/
ARIN: http://www.arin.net/
上記データは、サイバーエリアリサーチ株式会社様のご協力をいただき、IPアドレスと国籍、地域（都道府県・市外局番）、回線種別（ダイアルアップ・ADSL・CATV）、ISPなどを関連づけたIPアドレスデータベース を利用して解析を行った。

6. P2PはADSL回線に多く分布

我々の調査から、国内のP2Pネットワークの多くは、ADSL回線で繋がっていることがわかってきました。

国内P2Pファイル交換の回線利用分布（N=964,485）

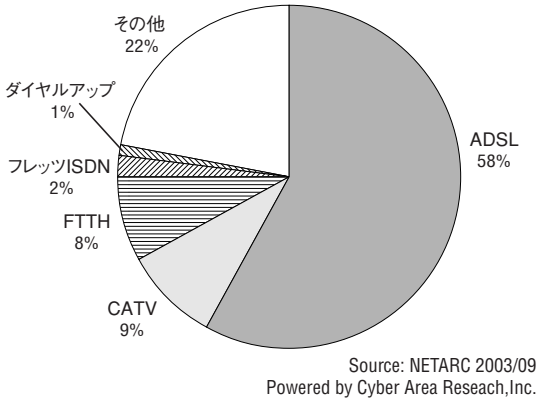


図:　ADSLの普及などを背景として、ブロードバンド化が進んでいます。

データ内容:　データは、2003年6月から9月までにP2Pノード探索システム P2P FINDERによって集計された累積P2Pノード数を元にしている。探索対象は、国内の利用が多いP2Pファイル交換ソフトウェアWinMXとWinnyを対照とし、日本語圏を特定するために、日本語キーワードを用いP2Pファイル交換ネットワークでP2Pファイル検索を行いファイルを公開するP2Pノードを集計している。
集計方法は、過去一度発見されたP2Pノード（IPアドレス）は加算されず、新規に発見されたP2Pノードのみ加算されている。

上記データは、サイバーエリアリサーチ株式会社 様のご協力をいただき、IPアドレスと国籍、地域（都道府県・市外局番）、回線種別（ダイアルアップ・ADSL・CATV）、ISPなどを関連づけた IPアドレスデータベース を利用して解析を行った。

7. まとめ

このようにP2Pネットワークは、P2Pソフトウェアの普及と数多くの人間によって、インターネット上に確固たるインフラを作り上げています。

P2Pに関するとある学説によると「P2Pは決してなくならないインフラとなる」というものがあります。一度普及し人間が媒介することによって増殖を繰り返すネットワークは、決してなくならないというものです。事実、国内においても事件が起こるたびに、P2Pファイル交換のユーザーが増減するという話題が出ますが、一向にゼロになることはありませんでした。

インターネットに携わる企業としては、これら無くならないP2Pネットワークを正しく理解し取り組んでいくことが、より重要になってくるでしょう。

JNSAワーキンググループ紹介

セキュリティ会計ガイドライン検討WG

セキュリティ会計ガイドライン検討WGリーダー
凸版印刷株式会社　佐野　智己

■はじめに

今年度より、政策部会内に『セキュリティ会計ガイドライン検討ワーキンググループ』(以下、本WG)を立ち上げ、活動を開始しました。

本WGの名称に使われている「セキュリティ会計」とは、「環境会計」からとった造語です。環境の世界では、既に「環境報告書」という形で企業における環境保全への取り組みを公表する仕組みが定着化しており、またその取り組みに対する意思決定のツールとして「環境会計」が多くの企業で導入されています。企業における情報セキュリティ確保および個人情報保護の取り組みは環境保全活動と似ている点が多いことから、先行する「環境会計」に倣い、「セキュリティ会計」という概念を提唱しました。

ところで、昨今の個人情報漏洩事件を受けて、情報セキュリティの確保や個人情報の適正な取り扱いがまさに“企業における社会的責任(CSR)”として捉えられるようになってきました。そして、CSRレポートの中で情報セキュリティや個人情報保護の取り組みを掲載する日本企業も出て来ました。しかし、その数はまだ少なく、あまり多くは語られていないのが現状です。個人情報保護法の全面施行が来春に迫り、実は身近なところで、社内・社外を問わず、情報セキュリティに対する説明責任が求められるようになって来ています。

本WGの活動が、IT社会の一員として、社会との有効なコミュニケーションの一助になれば幸いです。

■活動目的

企業における情報セキュリティ確保に向けた取り組みについて、適正に把握・評価・公表できる仕組みとして「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、発信していきたいと考えています。

以下にWG発足時に掲げた取り組み項目を挙げます。

1)「セキュリティ会計」の基本設計
2)環境会計などの既存モデルとの共通点・相違点の調査と適用の可否
3)情報セキュリティ確保に係るコストの分類と算定方法の提示
4)物量的／経済的効果の指標
5)情報セキュリティにおける有形・無形資産の価値評価
6)モニタリング　など

初年度にあたる2004年度は、環境省「環境会計ガイドライン」や情報セキュリティに係る諸規程などを参照しながら、『JNSA版セキュリティ会計ガイドライン(草案)』の策定を目指します。

また、JNSA内の他WGとの連携や関連団体との意見交換なども積極的に行っていく予定です。

■活動状況

月1～2回程度、WGを開催しています。

2004年度前半期は、8回、WGを開催しました。また、関連知識の習得のため、外部より講師をお招きし、勉強会を数回開催しました。

非常に“チャレンジングな”テーマではありますが、“JNSAらしい”解が出せたらと思います。

S/MIME検討WG

S/MIME検討WGリーダー
NTTコムウェア株式会社　磐城　洋介

■はじめに

電子署名法の施行以来、公的個人認証サービスの開始や、e文書法などPKIを利用したアプリケーションの普及が始まろうとしています。S/MIMEは、電子署名のアプリケーションとして古くから存在しますが、メールソフトの機能対応状況など一般的に利用するには様々な課題が未だ沢山あります。本WGは、これら課題の抽出のためS/MIMEを利用できる様々なメールソフト（MUA）の機能を検証し、S/MIME利用上の注意点を明確にするために活動しています。

■WG成立経緯

S/MIME検討WGは、昨年度活動した「電子署名検討WG」が母体となり、電子署名の普及というテーマに関してS/MIMEに着目した活動を行うことを目的とし成立しました。電子署名検討WGでは、PKIや電子署名について様々な課題・問題があることを意識し、解決を望む多くの仲間に期待されたのですが、課題の解決に向けた具体的で効果的なテーマや成果が得られませんでした。この教訓を踏まえ、地道な所から着手するため、古くから電子署名を実装した「S/MIME」に注目し活動を開始しました。

■現在までの進捗

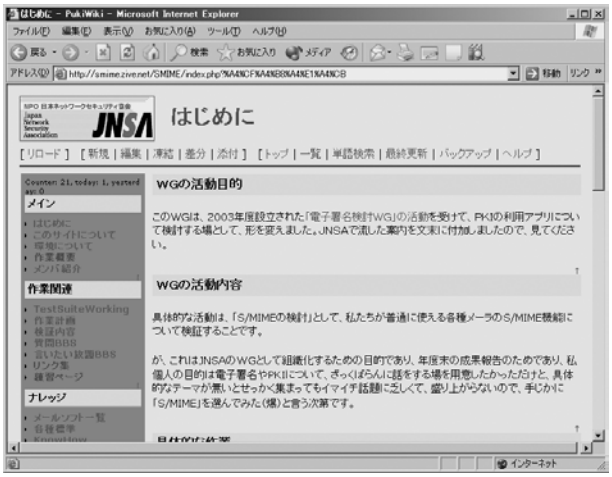
登録メンバは比較的多いのですが、皆多忙（特にリーダ（号泣））のため、会合は殆ど開催しておらずネット上で活動できるよう、WG専用サーバ（※1）上にコラボレーションツール（※2）を導入し、そこで活動を行っています。1/3くらいのメンバがこのサイトに情報提供を行い、掲示板などでディスカッションをしています。現在では、PKI相互運用技術WGの成果「PKI相互運用テストスイート」を用いた証明書検証の実験を行いつつあり、9種類のMUAについて実験を行っています。

■今後の予定

ターゲットMUAを増やしつつ、前項の実験テーマを来年3月まで行います。また、著名なMUAについては利用者支援のため、簡単な設定マニュアルなどの作成も検討しています。

※1
WG専用サーバは、メンバ限定のID/PWにより保護されている、WGリーダの自宅サーバ（Linux）です（笑）。
※2
PHPで作成された「PukiWuki（http://pukiwiki.org/）」を用いています。

「S/MIME検討WG活動支援Webページの一部」



個人情報保護法ガイドラインWG

個人情報保護法ガイドラインWGリーダー
株式会社大塚商会　佐藤　憲一

■ はじめに

昨年平成15年12月、政策部会　個人情報保護ガイドライン作成WGは、個人情報保護に対する社内の情報セキュリティマネジメント対策を中心とした『個人情報保護法対策　セキュリティ実践マニュアル』を作成、出版いたしました。今年６月には、経済産業省「個人情報保護法ガイドライン」の発表とともに、個人情報保護法に関連する多くの書物が発行されました。しかしながら、一般企業の経営者、情報システム管理者の方より、「保護法を遵守する為に、何をどの程度実施すれば、保護法対策といえるのか？」というご質問を多く受けました。

そこで、政策部会では、再度、個人情報保護法への具体的対策をより現実的に解説する目的で、個人情報保護法ガイドラインＷＧを急遽発足いたしました。現在、顧問弁護士　北沢先生を筆頭に、会員メンバー34名で活動を行っています。

■ 活動目的

本WGの活動目的は、一般企業が求める個人情報保護法を遵守するための具体的方法をガイドラインとして明文化し、広く流布することといたしました。また、活動成果物は、前回出版した『個人情報保護法対策　セキュリティ実践マニュアル』の第2弾として3月出版を計画しております。
以下、この出版物の特徴を列記いたします。

①読者の対象を中規模企業とし、200名程度の製造会社といたしました。また、このモデル企業を、経営者を中心とした全社共通組織、営業本部、マーケティング本部、サポート本部、工場、総務部（人事部含む）、お客様相談室、情報システム室の8部署を想定し、それぞれが、個人情報保護を推進するための方法を解説いたしました。
②各部署の解説方法は、経済産業省　個人情報保護法ガイドラインの精神に則り、個人情報の取得、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置、委託先の管理毎に解説することといたしました。
③個人情報保護法条文との分類表を作成し、解説した項目がどの条文と適合するかを一目で分かるようにいたしました。
④標準的規程、基準、手順書を数多く掲載するとともに、その解説を加え、より実践的に利用できるようにいたしました。
⑤安全なシステム構築するための具体的ソリューション例、各省庁のガイドライン、個人情報保護法の解説を加えました。

■ 最後に

12月7日現在、ドラフト版が完成し、年内ブラッシュアップ、そして3月出版に向けメンバー各位とも土日を潰しての執筆活動を行っております。会員の皆様も、第2版にどうぞご期待いただきたいと存じます。

NSF2004概要

JNSA研究員　安田　直義

2004年10月28日（木）～29日（金）に青山TEPIAでNetwork Security Forum 2004（NSF2004）が開催されました。今年は、コンファレンスに展示会を併設する形で実施され、特にコンファレンスは事前申し込みをお断りするほどの大盛況となりました。

＜来場者数＞

10月28日（木）天候／晴れ 624名
10月29日（金）天候／晴れ 413名
合計来場者数　1,037名

Network Security Forum 2004（NSF2004）会場受付

コンファレンス

コンファレンスは、18ページのプログラムのように2日間でテーマを分けて開催されました。1日目は、政策や運用、調査結果などの報告が中心になり、2日目は技術的な関連が主なテーマとなっています。各々について簡単に内容をご紹介しましょう。

1日目の基調講演として、「情報セキュリティ対策は企業価値を高められるか？－個人情報保護法に向けた準備と情報セキュリティ政策の最新動向－」と題して、経済産業省 商務情報政策局情報経済課 情報セキュリティ政策室 課長補佐の田辺雄史氏からご講演いただきました。


経済産業省の田辺氏

予防偏重社会から事故前提社会へ発想を変えて考えなければならない点を指摘され、そのために前提となる情報セキュリティを取り巻く環境の変化という観点から、政策や実施体制について解説されました。政府組織、重要インフラ、企業、個人を見据えたグランドデザインを描き、実現のスケジュールを作って進めていく構想が述べられました。e-文書法、個人情報保護法を始めとして、経済産業省としての政策が紹介され、特に「早期警戒」を重要課題として挙げられていました。情報セキュリティ早期警戒パートナーシップの一環としての定点観測網の整備や脆弱性情報の取り扱いについての状況などについても言及されていました。最後に組織的および技術的な情報セキュリティ対策について、セキュリティ監査の視点や、暗号アルゴリズム、ISO/IEC 15408の国際相互認証を行うCCRAなどについても言及されました。かなり内容の濃い盛りだくさんの内容でしたが、経済産業省がテーマとして持っている内容が一通り概説されたので、今後の日本の政策について更に多くの議論が行われることが期待されます。

続いて、「個人情報保護対策 総点検 課題と緊急対策－迫り来る個人情報保護法 全面施行にいかに対処すべきか？－」というテーマで、牧野総合法律事務所弁護士法人の牧野二郎弁護士からご講演いただきました。個人情報保護法の実施を目前に控え、企業として考えなければならない点を中心に、個人情報を扱う上での考え方や注意点を詳細に解説されました。対策プロジェクトの

ロードマップの例が示され、企業の守るべき情報の内容や、個人情報とセキュリティの関係など、頭の中を整理することが重要であると指摘されました。対策としての緊急課題や総点検項目などを取り上げ、客観的な判断ができることが大切であると結論されていました。

3番目には「情報漏えい被害の現状」と題して、株式会社損保ジャパン・リスクマネジメントの山本匡氏から、セキュリティ被害調査WGでの調査結果を基にした講演がされました。WGの報告書の第2部「情報漏洩による被害想定と考察」に含まれている「賠償額算出モデル」が注目されていましたが、リスク管理を行う上での情報資産の評価を行う目安として活用できるものなので、今後多方面での活用が期待されます。

4番目は、「ISMS認定/Pマークを早く安く取得するポイント」と題して、株式会社大塚商会の佐藤憲一氏が、セキュリティ関連の認定を取るに際して考えるべき点を整理して話されました。

5番目は、「Identity Based Security実装プロジェクト事例」というテーマでグローバル セキュリティ エキスパート株式会社の宮川晃一氏が、システムを利用するユーザ情報を一元集中管理する観点から解説されました。

2日目は、技術的な内容ではあるけれど、どちらかというとジェネラルな内容のセッションが中心に組み立てられました。

トップバッターは、「ネットワークの自己防衛－コンプライアンス確保のためのITインフラ－」と題して株式会社ネットマークスの正木淳雄氏が、インフラの現状が不完全であることを前提として、セキュアに利用するための検疫ネットワークという考え方を中心に解説されました。

次に昼休みの一部を使って、緊急特別調査報告として、JNSA政策部会マーケットリサーチWGが2004年8月に実施した「ITセキュリティ対策の導入状況と満足度に関する調査」の概要が報告されました。既に新聞などでも報道されていますが、正式な報告書が間もなく公開される予定です。

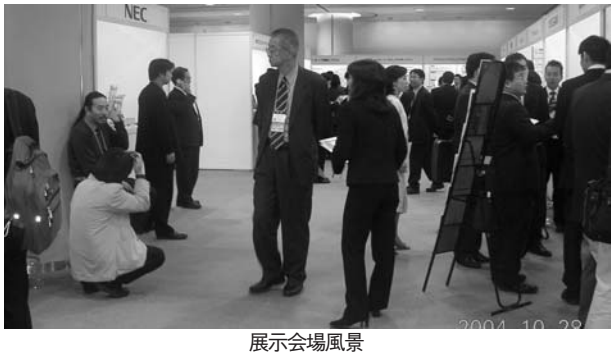
2番目に基調講演として、奈良先端科学技術大学院大学の門林雄基先生から「コンポーネントからプロファイルへ－セキュリティ技術開発から浸透への転換－」と言うテーマで、セキュアなシステムを開発する際に、今後考えた方が良いであろう方法論や状況を判りやすく解説されました。インターネットは恐ろしい場所だと脅してみても消費者の信頼を失ってしまうだけであり、技術者としては、マーケット担当者とは違う視点で技術を見るのが自然だし、その上でコミュニケーションが創られる必要があるだろうということが指摘されていました。

3番目のセッションは、「これからのWebセキュリティを考える－ビジネスの生命線を守るには・・・？」と題して、住商エレクトロニクス株式会社の二木真明氏から、これからのビジネスでの生命線となるWebシステムとそ

コンファレンス会場風景

	「コンファレンス」TEPIAホール（4F） A会場　※定員200名
10:30 ┆ 11:45	【A-1】 基調講演 満員御礼 「情報セキュリティ対策は企業価値を高められるか？―個人情報保護法に向けた準備と情報セキュリティ政策の最新動向―」 田辺 雄史（経済産業省 商務情報政策局 情報経済課 情報セキュリティ政策室 課長補佐）
13:00 ┆ 14:00	【A-2】 満員御礼 「個人情報保護対策 総点検 課題と緊急対策 -迫り来る個人情報保護法 全面施行にいかに対処すべきか？-」 牧野 二郎（牧野総合法律事務所弁護士法人 弁護士）
14:20 ┆ 15:20	【A-3】 満員御礼 「情報漏えい被害の現状」 山本 匡（株式会社損保ジャパン・リスクマネジメント ISOマネジメント事業部）
15:40 ┆ 16:40	【A-4】 満員御礼 「ISMS認定/Pマークを早く安く取得するポイント」 佐藤 憲一（株式会社大塚商会 S&S本部 テクニカルソリューションセンター部長代理）
17:00 ┆ 18:00	【A-5】 満員御礼 「Identity Based Security実装プロジェクト事例」 宮川 晃一（グローバル セキュリティ エキスパート株式会社 コンサルティング事業部）

コンファレンスプログラム　　↑1日目
2日目→



展示会場風景

	「コンファレンス」TEPIAホール（4F） A会場　※定員200名
10:30 ┆ 11:30	【A-11】 満員御礼 「ネットワークの自己防衛 -コンプライアンス確保のためのITインフラ-」 正木 淳雄（株式会社ネットマークス インターネットソリューション事業本部 マーケッティング部 部長）
13:30 ┆ 14:45	【A-12】 基調講演 満員御礼 「コンポーネントからプロファイルへ -セキュリティ技術開発から浸透への転換-」 門林 雄基（奈良先端科学技術大学院大学 情報科学研究科 助教授）
15:05 ┆ 16:05	【A-13】 満員御礼 「これからのWebセキュリティを考える -ビジネスの生命線を守るには・・・？-」 二木 真明（住商エレクトロニクス株式会社 ネットワークセキュリティ事業部 技術担当副事業部長）
16:25 ┆ 18:00	【A-14】 スペシャルパネルディスカッション 満員御礼 「増大するネットワーク脅威の傾向と対策」 ・日々進化するネットワーク脅威：その実態と傾向は？ ・複雑化・高度化する対策技術：何を選びどう使うか？ <ディスカッションパネラー> 西本 逸郎（株式会社ラック JSOC事業本部 取締役本部長） 園田 道夫（独立行政法人 情報処理推進機構（IPA）非常勤研究員、NPO 日本ネットワークセキュリティ協会（JNSA）研究員） 野々下 幸治（株式会社シマンテック 法人営業事業部 エグゼクティブシステムエンジニア） 能地 將博（マカフィー株式会社 マーケティング本部 マーケティング部 部長代理） 松島 正明（新日鉄ソリューションズ株式会社 基盤ソリューション事業部 マーケティング部 プロダクトマーケティンググループ シニアマネージャ）

のコンテンツを如何に守るか、という観点から、さまざまな注意点が紹介されました。

最後に、スペシャルパネルディスカッションとして、「増大するネットワーク脅威の傾向と対策」というテーマで、株式会社ラックの西本逸郎氏をモデレータとして、園田氏、野々下氏、能地氏、松島氏（所属等は18ページのプログラムを参照）の各パネラーの皆様で、日々進化するネットワーク脅威の実態と傾向、複雑化・高度化する対策技術について何を選びどう使うか？といったテーマでディスカッションが行われました。

今年のコンファレンスは、どちらかというとジェネラルな内容が中心になっていましたが、技術的に深い問題がなくなったわけではなく、最後は技術で裏打ちされなければ問題を解決できないのは、今も変わりありません。とはいえ、技術以外のことも考えなければならないことが多くなってきたということは、インターネットが社会インフラとして定着してきたということでもあるでしょう。社会生活になくてはならない仕掛けとして、どのようにしたら安全・安心・快適に使えるか、ということが今後ますます重要になってくることは確かです。

展示会

NSF2004では、久し振りに展示会が併設され、４つのゾーンに分かれて、全25社が参加しました。

- 情報漏洩対策・個人情報保護
- 情報セキュリティ・ネットワークセキュリティ
- セキュリティポリシー・その他
- ウイルス・ワーム・スパム対策

今回は最初の2つのゾーンが圧倒的に多く、世相を反映している感じがしました。また目的意識を持った来場者が多く、かなり実際的な商談も行われたようでした。

展示会場では、オープンシアターというセミナーコーナーが作られ、会員会社の中から製品や会社紹介などを中心としたミニセミナーが開催されていました。こちらもかなり盛況で、多くの聴講者を集めていました。

最後に

2004年のNSFは、セキュリティについて、インターネットや社内ネットワークのトラフィック制御やパケット監視、ウイルスや不正アクセスをはじめとするような技術面だけではなく、個人情報保護法やISMS、ISO15408などの管理運用面の関心も高まっていることが実感できました。技術だけではすまないけれど、技術がないと始まらないことが、ますます実証されてきた感じがします。

来年はまた新たな試みや状況がが出てくるかもしれません。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。

展示会場のオープンシアター

セミナーレポート

2004年度「インターネット安全教室」開催のお知らせ

～ウィルス感染、詐欺行為、プライバシーの侵害などの被害にあわないために～

●背景と目的

誰でも手軽にインターネットに接続できるようになった今日、ウイルス感染、詐欺行為、プライバシー侵害など情報犯罪の被害にあう危険性がますます高くなってきています。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、情報犯罪を防ぐことはできません。こうした状況をふまえ、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、警察庁の後援を得て、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」を全国各地で開催することと致しました。

●内容（約120分）

CD-ROM（ビデオ）の上映	20分
講師による解説	30分
県警による講話	20分
体験学習	20分
質疑応答	10分

・ウイルス感染、詐欺行為、プライバシー侵害などの情報犯罪に対する正しい理解を広め、初心者でも安全快適にインターネットを楽しめるようにする
・各地でネットワークセキュリティの啓発に関わる人々に「インターネット安全教室」セミナーのノウハウやツールを提供し、「インターネット安全教室」の活動を全国に広める
・セミナーコンテンツとして、冊子付きのセキュリティ啓発CD-ROMを作製し、セミナーで使用する。CD-ROMは開催地で配布するだけでなく、セミナー終了後は希望者へ広く配布し、セキュリティ啓発活動のツールとして役立てる

主催者挨拶：経済産業省 大崎氏


兵庫インターネット安全教室風景

●開催地

［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

日　程	県　名	共催者	開催場所
10月7日（水）	島根県	財団法人しまね産業振興財団	くにびきメッセ
10月16日（土）	東京都	足立区立扇中学校PTA・足立区立舎本小学校PTA	足立区立舎本小学校体育館
10月22日（金）	兵庫県	兵庫県・兵庫ニューメディア推進協議会	兵庫県私学会館
10月30日（土）	奈良県	なら情報セキュリティ研究会	帝塚山大学
11月2日（水）	神奈川県	横須賀市・横須賀市IT戦略会議	横須賀市役所正庁
11月6日（土）	愛知県	NPO東海インターネット協議会	名古屋市公会堂
11月6日（土）	神奈川県	厚木市・NPO情報セキュリティフォーラム	厚木市ヤングコミュニティセンター
11月7日（日）	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	大分県立芸術文化短期大学
11月9日（火）	福井県	福井県高度情報化推進協議会	小浜市働く婦人の家
11月17日（水）	岐阜県	岐阜県消費生活センター マルチメディア＆ＶＲメッセぎふ実行委員会	ソフトピアジャパン
11月19日（金）	和歌山県	NPO情報セキュリティ研究所	わかやま館
11月20日（土）	神奈川県	NPO情報セキュリティフォーラム	岩崎学園
11月20日（土）	大阪府	ヒューマンアカデミー	ヒューマンアカデミー大阪校
11月23日（火）	沖縄県	浦添市	浦添市社会福祉センター
11月27日（土）	岡山市	岡山市連合町内会IT専門委員会・岡山市電子町内会連絡協議会 岡山市・株式会社エス・シー・ラボ	ほっとプラザ大供
12月10日（金）	青森県	財団法人八戸地域高度技術振興センター	八戸インテリジェントプラザ
12月18日（土）	北海道	NPOくるくるネット	室蘭工業大学
12月18日（土）	新潟県	NPO新潟情報セキュリティ協会・財団法人にいがた産業創造機構	NICOプラザ
1月18日（火）	栃木県	栃木県・NPO栃木県シニアセンター	栃木県自治研修所
1月25日（火）	佐賀県	ＮｅｔＣｏｍさが推進協議会・佐賀県	アバンセホール
1月29日（土）	大分県	ひたインターネット協議会 財団法人ハイパーネットワーク社会研究所	日田市中央公民館ホール
2月4日（金）	神奈川県	藤沢市	藤沢市役所防災センター
2月8日（火）	高知県	社団法人高知県情報産業協会・高知県	高知県工業技術センター
2月19日（土）	神奈川県	小田原市・NPO情報セキュリティフォーラム	小田原市保健センター
2月22日（火）	大阪府	大阪市PTA協議会	中央区民センター
2月26日（土）	熊本県	NPO熊本県次世代情報通信推進機構	熊本市総合女性センター
3月6日（日）	千葉県	NPO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

「インターネット安全教室」は、参加費用は無料で、どなたでもご参加いただけます。
お近くで開催の際には、ぜひご参加ください。

セミナーレポート

JNSA西日本支部主催セキュリティセミナー NSF2004 in OSAKA

西日本支部　セミナー運営WGリーダー
西日本電信電話株式会社　中台　芳夫

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5回セキュリティセミナー「NSF2004 in OSAKA」が、大阪商工会議所、関西経済同友会、近畿経済産業局の後援のもと、11月11日(木)に大阪市にある新梅田研修センターにおいて開催されました。当日は雨天のため参加者の出足が心配されましたが、10月に都内で開催されたNSF2004の活況ぶりを反映した形で、約162名の方にご来場頂きました。

今回は一般企業にとっても関心の高い「個人情報保護」をテーマとして、行政、法曹、事業者、そして情報漏えい被害者の4つの立場から、個人情報・プライバシー権の保護の考え方、情報セキュリティへの取り組みに関する動向、および将来へ向けた課題等をご講演頂き、多数の参加者に改めて考えを深めて頂くセミナーとなりました。

プログラムは、最初に井上支部長から「JNSA設立五周年にあたり、NSF2004を東京で二日間開催し、約1000名のご来場者にお越し頂きました。個人情報保護法の完全施行まで5ヶ月を切り、いやがうえにも皆さんの興味が増している中、西日本でも同じテーマで、関西にゆかりのある方々を講師にお迎えし、本セミナーを開催致します。」とご挨拶を頂き、あわせて2003年度のJNSAの調査結果から、個人情報漏洩に伴う事業者の被害規模に関し、賠償額の算出モデルなどの要点をご紹介頂きました。

続いて基調講演として「情報セキュリティ政策の最新動向について　～個人情報保護法施行等を迎えて～」と題し、経済産業省・商務情報政策局・情報セキュリティ対策室課長補佐の田辺雄史様からご講演を頂きました。田辺様は「近年の電子商取引市場の急成長、企業のセキュリティ対策意識の低さ、脆弱性発見から攻撃までの期間短縮化を背景に、情報セキュリティに対する考え方は『予防偏重』型から『事故前提』型へ、経営全体にかかわる信頼性を勝ち取っていくインフラという見方へ変化しています」とお話され、政府としても3つの戦略と42の施策項目からなる「情報セキュリティ総合戦略」へ取り組んでいることを説明されました。田辺様はこの中から、文書の電子保存の認可によって企業経営の効率化に寄与するｅ－文書法（注：本セミナー後の11月19日に成立、2005年4月に施行予定）、および個人情報保護法と経済産業分野におけるガイドラインについて詳解されました。ガイドラインでは、個人情報保護法で安全管理措置の具体例が明記されていない分、参考事例を掲載し明確化を図った点、および従業員の個人情報の取り扱いについては厚生労働省と共同で作業した点などを説明され、ガイドラインの一部もご紹介頂きながら、広範囲に規範となるガイドラインになったことをお話頂きました。またご講演では、経済産業省における政策の柱として、IPA、JPCERT/CCを中心とした情報セキュリティ早期警戒パートナーシップ、コーポレートガバナンス（企業統治）のサブセットとして監査制度も含めた組織的な情報セキュリティ対策のあり方、技術的な情報セキュリティ対策の最新動向、そして電力分野等の重要インフラにおける情報セキュリティ対策についても言及され、経済産業分野における多方面な情報セキュリティ対策の展開についてご披露頂きました。

午後からは、法曹界の立場から「個人情報保護法と企業の対応」と題し、国立情報学研究所客員教授で弁護士の岡村久道様からご講演を頂きました。近畿大学法科大学院、奈良先端科学技術大学院、神戸大学法科大学院

でも教鞭を執っていらっしゃる岡村様は「民間部門での個人情報の取扱いルールを定めた法律はこれまでなかったのですが、４月の個人情報保護法の本施行に向けて、各企業とも来年２月頃の完了を目途に準備を進めています」と冒頭に挙げ、まさに各社とも切迫感に迫られている状況からお話頂きました。岡村様からは、法律の基本理念や構造、関連する法令の位置づけ、判例に学ぶ具体的な対策の考え方などの細部に至るまでを詳しく解説して頂きました。とりわけ個人情報保護法を遵守する上で陥穽になりがちな、利用目的の通知や公表の要・不要の考え方、データの正確性の確保の具体例、内部情報漏洩の主な原因と言われる従業者の監督、委託先の選任と委託契約において望まれつつある事項、委託先と第三者提供の違いとその留意点、情報主体への開示等の対応方法とクレーマー対策、個人情報保護方針(プライバシーポリシー)の策定の考え方や具体例、および不適正な個人情報の取り扱いに対する行政処分などについて、法律的な見地から留意すべき部分をお伝え頂きました。法律施行を前に、目的に沿った適正な取得、安全管理措置の実施、情報主体への対応といった、個人情報取扱事業者が法律に則って遵守すべき事項のほうがクローズアップされていますが、岡村様は「プライバシー権と個人情報保護法とは密接に関係しているが、別個独立の存在」と述べ、プライバシー権の考え方は引き続き存続し、今後企業が漏洩事故を生じた場合には二重の責任が問われるようになった点を明確にされ、一般企業の参加者にとってもどのようなポイントを抑えるべきかを明らかにした、有益なご講演を頂きました。

続いて、個人情報等を取り扱う事業者の立場から、「松下電器における情報セキュリティの推進」と題し、松下電器産業株式会社・情報セキュリティ本部参事の長野數利様からご講演頂きました。長野様は「松下電器グループは2003年度に連結子会社数372社、従業員数29万人(2004年度からは連結子会社数600社以上、従業員数約34万人)を抱える中、1999年からセキュリティに取り組み、2001年に社内の個人情報保護基本規定を制定しています。従来は規定が豊富にもかかわらず具体的な施策が不明確で、ドメイン・事業場毎のセキュリティ管理レベルのばらつきが大きく、また専任推進体制が未確立なために経営トップの意思が組織に浸透しにくいという課題を持っていました。このような背景のもと、全社的に統括する目的で、2004年4月1日から情報セキュリティ本部を発足しました。個人情報の保護、技術情報など営業秘密の守秘管理、セキュリティ機能を盛り込んだ安全・安心な製品の供給を３つの柱として取り組んでいます。」と紹介されました。個人情報だけでなく営業秘密も管理しなければならない事業者にとって、セキュリティマ

ネジメントサイクルに沿った全社的なセキュリティレベルの向上は必須課題です。松下電器グループでは、事業場単位の情報管理レベルを5段階の成熟度モデルで分類し、2005年2月までに国内全事業所で管理レベル3の達成を目標として掲げる、判りやすいマニュアル（情報セキュリティガイド）を全社員に配布する、あるいは情報セキュリティ事故についてA・B・Cの被害レベルを設定し、それぞれの被害レベルに対する対応アクションを策定するなど、全社的に理解しやすい形でセキュリティを実践し、レベルアップを図っている点に関してお話を頂きました。製品セキュリティに関しては、自らプロダクトを作り出すメーカーならではの取り組みですが、今後具体的な商品展開が大いに期待されるところです。

最後に、財団法人関西情報・産業活性化センターIDC事業部担当部長の木村修二様から「被害者の目で情報セキュリティを考える」と題した講演を頂きました。木村様は1999年に京都府宇治市で発生した約21万件もの住民情報データ流出事件において、情報管理課長として対処された方で、「セキュリティ業界が急躍進を遂げてきていますが、何故個人情報保護が必要になってきたか、その理念は何か、個人情報漏洩が発生した場合の本当の被害者は一体誰なのかを真剣に考え、過去の失敗を他山の石として学び、今後の失敗を防いで欲しいと思います。」と挨拶され、当時の貴重な経験を踏まえ、現在の個人情報保護およびプライバシー保護に関する課題や、個人情報を扱う現場の意識とセキュリティ業界側との意識のずれに警鐘を鳴らすお話を頂きました。ご講演の中で、「個人情報漏洩は社会システムの問題。需要があるから供給される。一方で漏洩を防衛しながら、もう一方で収集するような二律背反の個人情報対策を実施していないか」、「情報の取り扱いが簡単になった分、安全性が軽視され、事故の発生も容易になった」、「アプリケーションを作る人は個人情報保護条例を理解して欲しい」といった業界・ベンダへの問題提起、「個人情報漏洩は市民が被害者。事件には誠実に対応して被害者の救済が最優先」、「個人情報は市民からの預かりもの。情報セキュリティは生身の人間を護るものであって欲しい」、「個人情報を扱うサーバのログについて、市民や顧客へ開示できますか」等、現場への反省を込めた発言、そして「セキュリティを向上させれば、個人情報漏洩などの事故は減るのでしょうか？」と情報セキュリティの本質論に迫る木村様のお話を伺い、身につまされる思いがしました。セキュリティビジネスを推進する業界側にとって、個人情報を保護する現場の方々、そして個人情報主体である市民や顧客の立場に立って、意識すべき課題は未だに山積していることを改めて気づかされました。

法律施行を目前にし、個人情報保護への取り組みは企業にとっても避けられない問題とあって、今回のセミナーは熱気に満ちており、講演を通じて多数の方の関心が寄せられたました。一方で、法律の骨子やガイドラインを端的に理解し、目前の課題を理解したものの、自組織としてどう具体的に取り組んでいけば良いのか、未だに手探り状態にある企業や自治体も少なくないものと思われます。今回のセミナーをトリガーとして、お客様とセキュリティ業界が問題意識を一つにすべく歩み寄り、よりよい個人情報およびプライバシーの保護に向けて取り組むことが今後重要なことと感じられました。

セキュリティ・スタジアム2004盛況のうちに終了

セキュリティ・スタジアム実行運営委員会
根津　研介

2004年11月2日～4日まで、大田区産業プラザ（PIO）特別会議室でセキュリティ・スタジアム2004を粛々と開催いたしました。エントリされた参加者も多い日には30余名になりましたが、ちょうど、期間中に国民の祝日（文化の日）を挟んだために、参加者もセキュリティ技術を研鑽するのに、所属団体／企業の業務の一環として参加される方や、個人のスキル向上として参加される方など開催日によって傾向が見えて、セキュリティ技術者をとりまく社会的な環境の「いま」を表しているのではないかと思われました。

ここで、セキュリティ・スタジアムの内容について簡単にご説明したいと思います。

セキュリティ・スタジアムは、参加者が「攻撃」、「防御」、「監視／検知」のいずれか（複数エントリも可能）として参加します。「攻撃」に参加する人は、防御として参加した方が立てているサーバを攻撃し、どのような形で攻撃が成立するのかを実地を通して学び、公開されているツールや脆弱性そのものの有効性を検証します。「防御」で参加する人は、たとえば防御として設定すべき内容がどこまでなのかや、普段自分が設定している防御方法の有効性の検証、それから、攻撃を受けたときに十分にログがとれているのかや、どのようなログがでてくるのかを実地で検証し、確認します。

「監視／検知」で参加する人は、このような攻撃と防御のトラフィックの中から、有効な攻撃がどのように行われたのかをいかに効率よく摘出できるか等の監視ルールの有効性の確認や、監視ツールの有効な範囲、自動アラート機能がどのようなパケットパターンを誤検知するかの検証などを行います。また、攻撃パターンのパケットを大量に収集できるというメリットもあります。

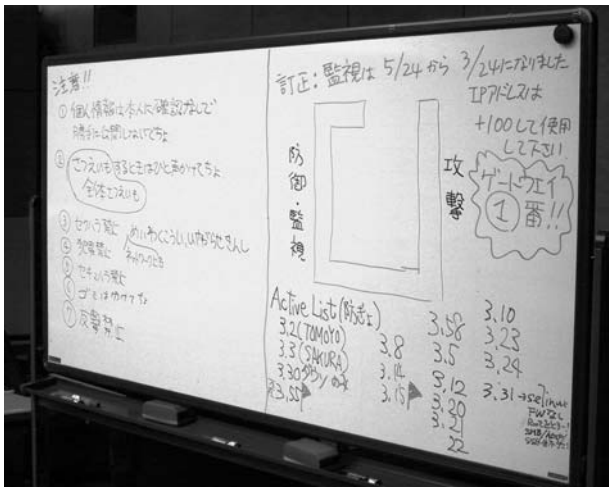
今回は、傾向として「攻撃」側として参加される参加者が多く、また、特徴としてセキュアOSワーキンググループからLinuxベースのセキュアOSであるTOMOYO Linuxと物理的に改ざんできない改造がなされているSAKURA Linuxが「防御」としてエントリしていただきました。この場を借りてお礼申し上げます。また、今回は特に「監査／検知」のエントリがほとんどありませんでしたが、今後、製品ラインアップをお持ちの企業の方の実証実験の場としても、ぜひ活用していっていただければと思います。

このような状況でしたので、若干防御側のマシンが不足したため主催者側が比較的防御レベルの低い防御マシンを数台用意して持ち込んでいました。この中には、実際に想定されるサーバの平均的な防御手段が講じられているものであったり、想定されうる限り弱いサーバなどがありました。つまり、インストールされただけのサーバもあり、また、SELinuxがオンになってはいるものの一切のパッケージアップデートが行われていないFedora Core 2などを防御側に持ち込んでいました。

また、先ほどとりあげたTOMOYO Linuxは、完全に設定されたものではまず攻略できないため、攻撃側の突くことのできる弱い部分を敢えて作り込んでおいていただき攻略のシナリオをいくつか用意していただきました。

三日間のセキュリティ・スタジアム競技を通して、いくつかの成果を得ることができました。主に、攻撃側の成果になりますが、まず、結果として、主催者側が用意した防御マシンはほぼ初日のうちに攻略されてしまいました。

また、TOMOYO Linuxは今回、参加者の注目の的であったため、多くの攻撃側参加者のターゲットになっていましたが、二日目になって、用意されていた脆弱性の



一つを通して攻略されました。今回、持ち込んでいただいたTOMOYO Linuxはファイルの実行権限やアクセス権が制限されており、apacheの構成ファイルやホームページは全て書き込み権限がないエリアに存在していたのですが、tomcatがインストールされていました。また、Sambaのバージョンが古くバッファオーバーフローの脆弱性が内在していました。これらに目をつけた参加者がSambaの脆弱性を利用してJavaプログラムをサーバー上にまんまと仕込み、apacheサーバを停止させることに成功すると、送り込んだJavaプログラムをtomcat経由で動作させてWebサービスを提供するようにしてしまったのです。これはネットワーク上からみると、まさしくホームページを書き換えたのと同じ結果を得ることができたことになります。

なお、主催者側が持ち込んだ防御側サーバの一つであるSELinuxがONのFedora Core 2ですが、宣伝不足のせいで三日間を通して攻略されることはありませんでした。「セキュアOS採用」という宣伝をすることによって、かえって攻撃者の心理に「なんとか落としてやろう」とする人間心理が垣間見えるような結果であったと言えるでしょう。

このように粛々と盛況な中でいくつかの成果も得ることができ、成功裏のうちにセキュリティ・スタジアム2004は無事、終了しました。今後、2005年の上半期中には今回の成果をふまえた上で、「セキュリティ・スタジアム2005」として、また、皆さんにご紹介できればと考えております。その際にはぜひ、より多くの方の参加とご協力のほどをお願いいたします。

会員企業ご紹介⑫

株式会社シーフォーテクノロジー
(http://c4t.jp)

株式会社シーフォーテクノロジーは、情報セキュリティ分野において、“核”となる技術（暗号化技術、秘密分散技術、電子透かし技術、ニューラルネットワーク技術）を独自開発し、事業展開しております。技術革新の速い分野において、常に先進技術を追求し、顧客へ最高のソリューションを提供することを目的に企業活動を行っています。
また、当社では、高まりゆく情報セキュリティのニーズに応えて、コアテクノロジーの製品及びライセンス提供を行うとともに、「アライアンスパートナー戦略」（CAP：C4 Security Alliance Partner Program）を中核とした販売展開を行っております。

当社は、共同開発パートナー、製造パートナー、販売パートナーという3領域のアライアンスパートナーと連携しております。それぞれの分野のアライアンスパートナーの強みを一体化させたシナジー効果により、幅広い市場ニーズに応えることが可能となり、多彩な事業機会を創出しております。
そのアライアンスパートナー戦略とともに「製品ラインアップ拡充戦略」で多様なユーザーの目的に応えることのできる幅広い製品を自社開発し、ラインアップを拡充していくことを基本戦略としております。

さらに、現在、CMVP（Cryptographic Module Validation Program：暗号モジュール評価プログラム）において、FIPS 140-2 適合認定取得中の当社暗号ライブラリ製品「C4CS（C4 Certified Suite）」の開発により培ったノウハウをもとに、米国のセキュリティコンサルティング企業や評価機関と連携しお客様に迅速・確実な認定取得支援サービスを提供しております。リスク分析からセキュリティシステム導入・構築、さらにシステム構築では最も重要である暗号実装まで広範囲に対応し、適切なコストで運用でき、確かな効果を得られるサービスをご提供致します。

情報開示・内部統制セミナーのご紹介

◆日　時：平成17年1月20日（木）、2月9日（水）、
2月22日（火）
13:00 ～ 16:40（受付開始 13:15）
◆会　場：東京国際フォーラム
1月20日（木）：G605
2月 9日（水）：G505
2月22日（火）：G604
◆参加料：無料

◆当日のプログラム：
13:30 ～ 13:40 開会
13:40 ～ 14:30 【第1部】
企業内容の開示を支える内部統制の構築
講師：東京北斗監査法人　南 成人
14:40 ～ 15:40 【第2部】
連結開示におけるコンプライアンス体制
講師：（株）スリー・シー・コンサルティング　児玉 厚
15:40 ～ 16:30 【第3部】
経営者のための情報セキュリティ
講師：（株）シーフォーテクノロジー　川本 武志
16:30 ～ 16:40 閉会

貴社名、ご所属、お名前、ご連絡先を明記の上、下記メールアドレス宛にお申し込みください。
E-mail：cap@c4t.jp

お問い合わせ先
株式会社シーフォーテクノロジー
セキュリティ事業本部
TEL: 03-5447-2253
E-mail: product@c4t.jp

株式会社セキュアソフト
(http://www.securesoft.co.jp)

セキュアソフトは、近年、深刻さを増すネットワーク上の脅威に対処するための最新セキュリティソリューションの開発・提供を行うとともに、新しい時代の情報セキュリティインフラを提案する企業です。
1996年韓国初の商用ファイアーウォールのリリース以降、韓国のセキュリティ市場をリードする役割を担ってきました。2002年に日本法人を立ち上げ、これまで日本の数多くの行政機関、教育機関、民間企業でセキュアソフトのセキュリティ機器が導入されております。ユーザに高品質で使い勝手のよいプロダクトを提供するとともに、常に時代が必要とするソリューションをお届けすることがセキュアソフトの使命です。

SecureSoft T-Series

統合セキュリティソリューションSecureSoft T-Seriesは、ネットワークのゲートウェイで必要とされる「Firewall」「IDS」「VPN」「AntiVirus」の機能をひとつにした一体型アプライアンス製品です。複数の機能を1台で提供することにより、導入コストの低減、管理・運用負担の軽減を実現します。
使い勝手の面において、管理画面、マニュアルが全て日本語化されており、本体に標準で提供しているログ管理ツール“SecureSoft Longserver”を使用することにより、手軽にログ集計・抽出・レポート作成が可能です。
また、全ての機能がモジュール化されており、用途に合わせた組み合わせ方が可能です。小規模オフィスから大企業、データセンターまで多様なラインナップを取り揃えており、機能、価格共にユーザのシステム環境に合わせてお選びいただけます。

＜SecureSoft T-1000＞

SecureSoft Absolute IPS

高性能ネットワーク侵入遮断システム SecureSoft Absolute IPSは、最大8 Gbpsのパフォーマンスを誇る業界最高水準の侵入検知防御システムです。既知・未知のワーム、DoS攻撃に対し、プロアクティブな検知・遮断を行います。
超高速Network Processorベースのアーキテクチャー採用により、あらゆるパケットに対するDeep Packet Inspection を高速で実現します。未知の攻撃への対処という点については、Self-Learningプロセスを通じたアノマリ検知機能により、トラフィックの異常兆候を判断し、プロアクティブな対応を可能にします。
さらに、Virtual Sensor、アプリケーションコントロール、IPF（インフラ保護）機能、など多様な機能をサポートし、ネットワークに対するセキュリティの強化に寄与します。
製品スペックでは、2Gbps、4Gbps、8Gbpsの帯域幅に対応し、精度の高い検知、リアルタイムでの防御を行います。

お問い合わせ先
株式会社セキュアソフト
セールスグループ
TEL: 03-5464-9966　FAX: 03-5464-9977
E-mail: info@securesoft.co.jp

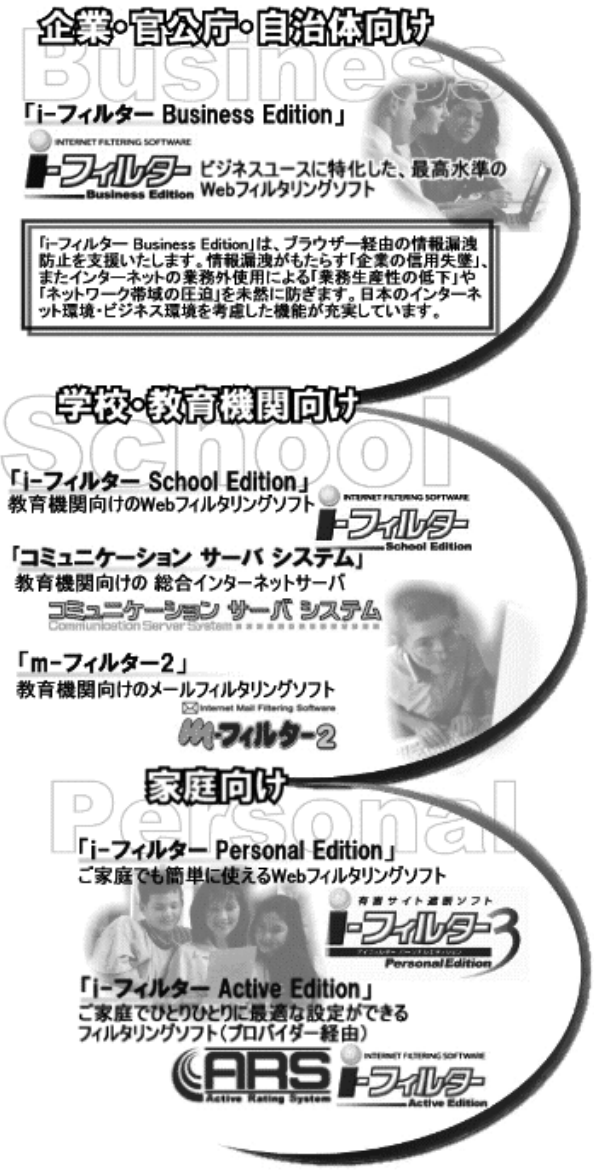
デジタルアーツ株式会社

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

Digital Arts Inc.

インターネットが日本において広がりを見せ始めた1995年、海外で誕生したインターネットを日本人にも使いやすいものにしようという思いを背景に、デジタルアーツ株式会社は設立されました。
デジタルアーツは創業以来このスタンスを忘れずに、お客様の視点で「より便利な、より快適な、より安全な」インターネット環境を作っていくことを目指し、パッケージソフト、ソリューション、サービスの企画・開発・販売を展開しております。

Webフィルタリング製品群



お問い合わせ先
デジタルアーツ株式会社
〒107-0061 東京都港区北青山3-6-16佐阿徳ビル
TEL: 03-5485-1347　FAX: 03-5485-1337
e-mail : ifilterb@daj.co.jp
www.daj.co.jp

主な事業内容

デジタルアーツは、インターネット社会の不安を取り除くソリューションの創出を目指し、インターネットアクセスに伴う危険を未然に防止する「Webフィルタリング」を中心とするセキュリティ事業をメインに事業展開をしています。
「Webフィルタリングソフト」の製品モジュールからデータベースまで、ソリューションの必要要素を1社で提供できる唯一のベンダーとして、企業・官公庁・自治体・学校・教育機関・家庭など、さまざまな市場で実績をあげています。

「i－フィルターBusiness Edition」製品紹介

- 掲示板などへの書き込み(POST)を制御するPOSTフィルター機能
- Webページを詳細に分類してアクセスをコントロール
- 部署ごと、支社ごとに異なったフィルタリングルールを適用可能
- HTTPのファイルアップロード規制や、アップロードしようとした内容の記録が可能

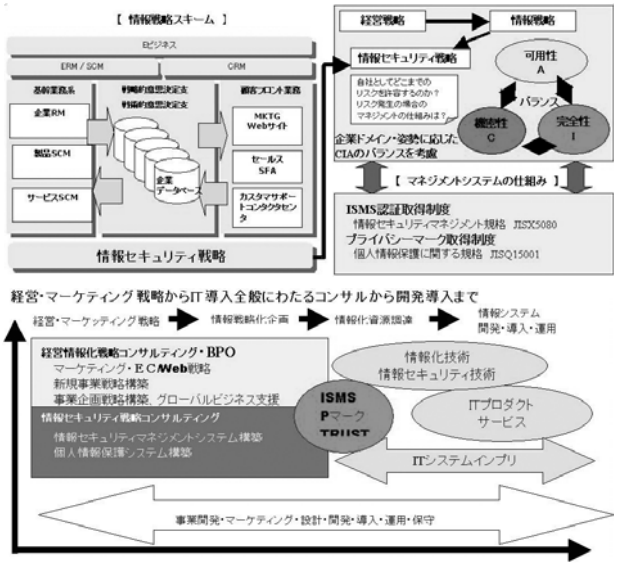
新しいフィルタリングマーケットの創造

デジタル社会の象徴であるインターネットはもはやパソコンだけにとどまらず、携帯端末や家電へ、そして企業、官公庁から学校、家庭へと、爆発的に拡大しています。
デジタルアーツは保有するフィルタリング技術を更に発展させ、迅速に市場に対して供給していく体制を構築し、時代に必要とされるソフトウェアをお客様の視点で作り続けていきます。

東京情報コンサルティング株式会社
(http://www.tokyoitc.jp)

経営・マーケティング戦略実現のための情報セキュリティ”コンセプトを日本初で実施致します。

情報セキュリティ戦略は、あくまで企業情報環境のインフラであり企業目的ではありません。その業界環境、企業文化、業種、業態に合わせた可用性、機密性、完全性のバランスが重要です。情報セキュリティを企業情報戦略の一環と捉え、経営・マーケティング戦略の実現のための情報セキュリティ戦略コンサルティングを行います。



コンサルティング・アウトソーシングサービス

当社は、お客様の幅広くかつ専門性が要求される高度な事業分野において、**各分野のプロフェッショナル集団**がプロジェクトチームで課題解決にあたります。また、社内に十分な要員が確保できない場合でも、企画・事業開発・戦略立案に係わる業務のアウトソーシングで対応いたします。

情報セキュリティ分野

情報セキュリティ戦略構築

経営情報戦略の一環として、いかにセキュリティ技術・人材をコントロールして実行性担保を図りながら、企業サプライチェーン活動から付加価値を生み出していくか、マーケティング戦略の視点を加えながら利益の極大化を目指すコンサルティングを致します。

1. 情報セキュリティマネジメント総合支援
2. 個人情報保護システム構築総合支援
3. 情報セキュリティ監査

大規模プロジェクト向けパッケージ
中堅・小規模企業向けS&Mパッケージ

個別サービス

・情報資産リスクアセス支援
　情報資産の特定からリスク分析・評価・対策
・個人情報リスクアセス支援
　個人情報業務フローの分析･評価･対策
・セキュリティ実装支援
　分析評価結果からセキュリティ実装支援、RFP作成
・マニュアル文書化支援
　ISMS文書テンプレート提供により管理文書作成
・内部監査員養成プログラム
　自社内での基本的なセキュリティ監査要員養成

4. 研修・トレーニング・セミナー

研修トレーニング
・情報セキュリティ研修(半日～1日)
・ISMS内部監査員養成研修(1日)
・個人情報内部監査員養成研修(1日)
・経営者・部門長クラス向け個人情報保護研修(半日コース)
・一般社員、パート、アルバイト向け個人情報対応企業研修(半日～1日)

講演・セミナー
・個人情報漏洩防止における企業対応（企業一般部門向け）
・個人情報漏洩クレームに対する企業対応（広報、顧客対応窓口向け）
・個人情報漏洩防止における具体的な企業対応策(現場社員、幹部社員向け)

教育ツール
個人情報保護法DVD・ビデオ
『よくわかる個人情報保護法』　上巻、下巻
(理解度確認テスト、解答用紙付)

お問い合わせ先
東京情報コンサルティング株式会社　(TokyoITC)
ＩＴビジネス事業部
東京都新宿区新宿1-30-16ルネ新宿御苑タワー９Ｆ
TEL 03-5368-4886　FAX 03-5368-4887
e-mail: info@tokyoitc.jp

日本高信頼システム株式会社

(htt@://www.jtsl.co.jp)

日本高信頼システム株式会社（略称：ＪＴＳ）は、2002年2月に株式会社日本高信頼システム研究所として立ち上がった中立系の企業で、今年5月に現社名へ変更し、高信頼システムソリューション専門のベンダーとして活動中です。単にセキュリティという切り口ではなく、信頼性というもう一段上の切り口でシステムを見て、多くの問題解決に挑んでいます。弊社では、高品質性・安全性・持続性の三要素にコストバランスを加味して、お客様ごとに最善と思われる「高信頼システムソリューション」をご提供していきます。

この秋に発表した二つの「高信頼システムソリューション」をご紹介いたします。

◆Windows環境における Trusted Thin Client Solution

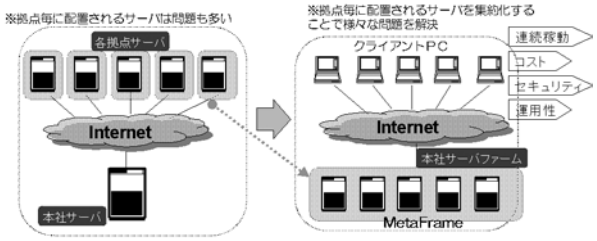
これまで数々のセキュリティ対策が必要だったクライアントPCをディスクレスにして、情報をサーバに集約させる事により、クライアント側からの情報漏えいを防止、情報の一元管理によるセキュリティポリシーの徹底と投資の集中化による極めて強度の高いセキュリティ対策が施せます。

サーバは、Windowsの「ターミナルサーバ」を使用、アクティブディレクトリとの連動によってドメインを統合しつつ、洗練されたグループセキュリティポリシーの適用によって、リファレンスモニタをも実現します。更にadministratorに権限を持たせたまま構成した時でも、事故が発生しないようにセキュアOS（PitBull）が無条件で付いています。

システム構成部分が大幅に減るため、システム構成によるシステム全体の信頼性向上を実現でき、あわせてセキュリティリスクの低減、運用コストの削減、業務効率の向上が実現されます。

Trusted Thin Client Solution　4つのキーワード

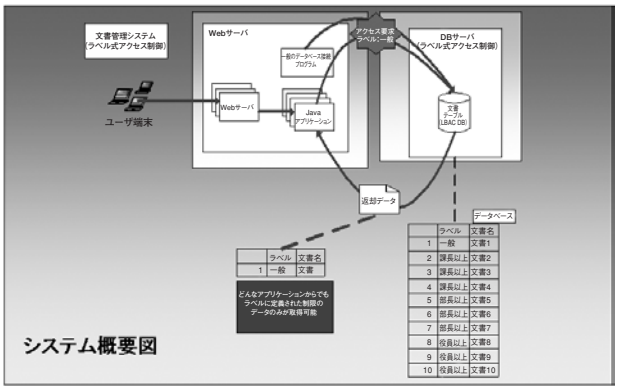
・構成の単純化（信頼性の向上）
・情報漏えい対策の強化（崩れないポリシー）
・業務システム効率化（一元管理の徹底）
・抜群の費用対効果（今までのような空振りは無い）



◆ラベル式アクセス制御を利用したデータベース保護 Trusted Database Solution

「Oracle9i Database」「Oracle Database 10g」のオプションであるラベル式アクセス制御機能を利用し、TrsutedOSで実現されている強制アクセス制御と同等の強力なアクセス制御をデータベース内部にまで実現します。本機能を利用すると、各レコード単位に機密区分情報を持てるため、今まで不可能であったレコード単位でのアクセス制御を実現できます。

本ソリューションは、Solaris8 + Oracle + PitBull FS + Oracleオプション製品で構成されます。



■H/W対策

ストレージの暗号化による媒体経由での漏えい防止

■運用・監視対策

アノーマリー検出と抱き合わせて自動アラートを実現

お問い合わせ先

日本高信頼システム株式会社　第1ソリューション部
TEL : 03-3868-8921　E-Mail : sales@jtsl.co.jp

日本ジオトラスト株式会社
(http://www.geotrust.co.jp/)

GeoTrust™ JAPAN
もっと信じられるインターネットを

日本ジオトラストは、電子証明書（サーバ証明書・企業認証・個人認証など）発行サービスを提供しており、証明書発行数の実績における世界シェア第二位のリーディングブランドです。
225,000枚（2004年12月現在）以上の発行実績があり、世界の140を超える国々でお客様に安心と信頼をご提供しています。

もっと信じられるインターネットを！

- 日本ジオトラストはWeb Trustの厳正な監査を毎年クリアしている米国の世界的な第三者認証局です。
- 日本ジオトラストでは、運営方法やプライバシーポリシーを含んだ非常に広範な監査範囲を有する事で知られるWebTrustが、毎年行う監査にその都度合格しており、そのガイドラインに基づいて運営しています。インターネットで暗号化を行う際、現在最もスタンダードとなっている技術基盤、公開鍵暗号基盤（以下PKI）と呼ばれる方式に必要な電子証明書を発行しています。
  ＊PKI方式とは、電子証明書を認識したウェブブラウザが通信先のサーバを認証し、秘密鍵と公開鍵を用いてSSL通信を行うというものです。この認証と通信の暗号化により、第三者の改ざん、盗聴、盗用、成りすましを防止することが可能になります。
- しかし、現在のサーバ証明書発行サービスでは、申し込みの際に登記簿謄本や、印鑑証明書の提出が必要で、さらに発行までには前述の書類を取得し、郵送した後2週間以上待ってやっとサービス開始にたどり着くというものでした。そのうえ、金額的にも実勢価格が10万円前後と非常に高価であったため、これらの要素が障壁となって、日本の総事業者数の90％以上を占める中小個人企業にはほとんど浸透していないというのが現状です。
- 日本ジオトラストでは従来統合されたサービスだったSSL通信用のサーバ証明書とウェブサイトの企業実在認証サービスを分割し、ユーザ側で選択できるようにしました。その為、面倒な書類手続きを廃し、かわりにドメイン管理者、サーバ管理者、SSL申請者が一致して初めて本人確認が成立したと想定し認証するシステムを採用しています。ジオトラストはクイックSSLプレミアムの開発、販売を通じて、すべての人に安心と信頼をお約束できるインターネットの実現に寄与してきました。
- 私達日本ジオトラストがご提案する128bitSSL暗号化技術、第三者認証サービスによる電子証明書は、今この瞬間にあなたとつながろうとしている誰かに、"今より、もっと"の安心を実現します。

■提供サービス

日本ジオトラスト

最大のサーバ証明書ソリューション

トゥルービジネスIDは、クイックSSLプレミアムの持つ、安全な128bit SSL暗号化通信能力とトゥルーサイトの持つ、企業の運営団体実在性認証能力を融合。天文学的なレベルの数字の羅列によるハイスペックな暗号化機能と、世界第2位のシェアを誇るジオトラストの実在性認証が、ユーザーに対する信頼度を高め、あなたのe-ビジネスのweb上でのステイタスを支えます。

お問い合わせ先
日本ジオトラスト株式会社
〒150-8512 東京都渋谷区桜丘町26-1
セルリアンタワー10階
TEL: 03-5728-1551（代）／FAX: 03-5728-1552
ウェブサイト: http://www.geotrust.co.jp/
お問合せメールアドレス: info@geotrust.co.jp

株式会社ヒューコム
(http://www.hucom.co.jp/)

株式会社ヒューコムは、“セキュアネットワーク分野のトータルソリューションプロバイダ”として、ネットワークシステムの設計、構築、ポリシに沿った運用･管理、監視、更にはセキュリティ教育まで、一貫したソリューションの提供をOne Stop、One To Oneで実現できる企業として事業を展開しております。
本稿では、来年4月の個人情報保護法完全施行へ向けた、個人情報保護態勢構築支援ツール「PPIK」のご紹介を致します。PPIKは個人情報保護態勢の構築を支援するツールで、社内の取り組み状況を分析し、どの部分が不十分かギャップを分析したうえで、不足個所への対策を具体的に提示することができるソフトウェアです。

PPIK（Privacy Policy Implement Kit）について

個人情報保護法の施行へ向けてどのような対策をすれば良いか、といった問いに対する的確なお答えを提示するのがこのPPIKです。
PPIKでは、個人情報保護法に照らし合わせて、現状どのような対策ができていますか、という質問項目を列挙してアンケートを取ります。アンケートの選択肢からお答えいただいた結果を分析し、コンプライアンスに照らし合わせて対策を示します。態勢を整えるためには、まずどこまで実施しているか具体的な現状把握が必要ですので、主に現場に近い人たちに答えてもらうことを想定しています。

PPIKの使用方法

パソコンにインストールし、PPIKを起動すると、質問項目が出てきます。それに答えていただくだけで、法律に対応できているかどうかと、その時点で取るべき対策が画面に表示されます。何が不足し、何をしなければいけないかが瞬時に分かります。

PPIKの特徴

◇簡単なインターフェース
アンケート形式の設問に回答をクリックで選択していくことで、各種法令への対応状況が確認できます。対応状況に不足がある場合には、とるべき対策内容が提示されます。
◇高レベルの対応とサポート
PPIKはさらに厳格な個人情報保護の規格である「JIS Q 15001:1999」のレベルも踏まえているため、高いレベルでの個人情報保護態勢を望む組織までもサポートします。
また、用語集による専門用語の解説や、履歴機能による過去の点検結果を参照することも可能です。
◇充実したライブラリ
本製品には基本規程から詳細規程まで、さまざまな場面に必要なサンプルドキュメントを含みます。社名を書き換えたり必要のない項目を削除することで、それぞれの組織に合った規程の策定が可能です。

■ソフトウェア要件

OS　：Windows2000、XP（日本語版）
ソフトウェア　：Microsoft Internet Explorer 6以上推奨
※付属の規定集を開くためには、Microsoft Office（Word、Exel)形式のファイルを開くことができるソフトが必要です。
HDD　：100Mbyte以上の空き容量が必要
画像解像度　：1024×768
販売価格　：200,000円

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

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■

○「脆弱性の窓」を防御するネットワークセキュリティアプライアンス『Vital Security Internet 1Box™』

新型/未知ウイルス、ワームなど、不正コード(MMC)のゼロデイアタックからネットワークをリアルタイムに防御する待望のFinjan Software社『Vital Security™』オールインワン アプライアンス版、ついに日本上陸！
「新種/未知ウイルス、および不正コード防御ソフト」、「アンチウイルス機能」、「Webフィルタリング機能」、「アンチスパム機能」などを1台に集約したゲートウェイ用コンテンツセキュリティ製品『Vital Security Internet 1Box™』
http://www.ahkun.jp/product/vs.html

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

○Policy Gurardian

セキュリティポリシーを策定しても上手く機能しない！そんな悩みをお持ちのご担当の皆様へ。「Policy Guardian」は今までにない新しいコンセプトで、情報セキュリティポリシーを確実に浸透させ、情報セキュリティの本当の意味を理解させるツールです。全てを規制して安心するのではなく、少しの抑止力を働かせながら繰り返し啓蒙教育を実施することで、確実にポリシーの意味を理解させていく運用をサポートします。
http://www.kcn.fujitsu.com/services/pro_policyG.html

◆お問い合わせ先◆
富士通関西中部ネットテック株式会社
フリーダイヤル　Tel：0120-008870（平日 9時から17時まで）
E-Mail：product@kcn.fujitsu.com
大 阪 本 社　Tel：06-6949-3702
中部事業所　Tel：052-745-2560

○アプリケーション　セキュリティ　ミドルウェア「SSH Tectiaソリューション」を発売

新しいエンタープライズ　セキュリティ　ソリューション「SSH Tectiaソリューション」を発売しました。
従来の「SSH Secure Shellシリーズ」の後継製品として、クライアント・サーバ型モデルに従って、2つのコンピュータ間のTCP/IP通信を保護します。企業内で利用されるビジネスアプリケーションを、最新のセキュリティで保護するためのセキュリティミドルウェアであり、既存のITインフラやアプリケーションの変更を行わずに導入することができます。企業内ネットワークにおいて、ビジネスアプリケーションが扱うデータを透過的に保護することで組織内通信のセキュリティを強化し、深刻化する企業内の情報漏洩を防ぐことが可能となります。環境のアップデート、設定の一元管理等を行い、管理者の運用管理コストを削減する統合管理ソフトウェア「SSH Tectia Manager」と、企業内エンドユーザがセキュリティを意識せず簡単に使用できる、無償提供のクライアントソフトウェア「SSH Tectia Connector」が新たに追加されました。

◆お問い合わせ先◆
SSHコミュニケーションズ・セキュリティ株式会社
Tel：03-3459-6830
E-Mail：sales.jp@ssh.com
URL：http://www.ssh.com/jp/

■サービス情報■

○Trustedシンクライアント・ソリューション

情報をサーバに集約させる事により、一元管理のしにくいクライアント側からの情報漏えいを防止、セキュリティポリシーの徹底と投資の集中化による極めて強度の高いセキュリティ対策が施せます(モバイルで遠隔地からも使用可能)。システム構成部品が大幅に減るため、システム全体の信頼性が向上、情報漏えいチャネル減少によるセキュリティリスクの低減、維持・運用コストの削減、業務効率の向上が実現されます。
http://www.jtsl.co.jp/japanese/newsolution/index.html

◆お問い合わせ先◆
日本高信頼システム株式会社
第1ソリューション部
Tel：03-3868-8921
E-Mail：sales@jtsl.co.jp

○SEA/J情報セキュリティ技術認定

セキュリティ全般の基礎知識を体系的に習得できるようIPA(情報処理推進機構)によって作成されたITスキルマップに対応しています。
開講日程
基　礎
□東京会場　12月 14日 15日
　2月 17日 18日
　3月 10日 11日
□大阪会場　12月 21日 22日
　2月 24日 25日
　3月 24日 25日
応　用
マネジメント編　12月 16日 17日
　3月 8日 9日
テクニカル編　12月 20日 21日 22日
　3月 16日 17日 18日
http://www.hucom.co.jp/

◆お問い合わせ先◆
株式会社ヒューコム　SMS事業本部
〒166-8521 東京都杉並区梅里1-7-7 新高円寺ツインビル
Tel：03-5306-7339　Fax：03-5306-7334
E-Mail：sms@hucom.co.jp

事務局お知らせ
JNSA ANNOUNCE

1. 主催セミナーのお知らせ

●「インターネット安全教室」

1月開催
18日　栃木県（栃木県自治研修所）
25日　佐賀県（アバンセホール）
29日　大分県（日田市中央公民館ホール）

2月開催
4日　神奈川県（藤沢市役所）
8日　高知県（高知県工業技術センター）
19日　神奈川県（小田原市保健センター）
26日　熊本県（熊本市総合女性センター）

3月開催
6日　千葉県（ベイタウン・コミュニティコア）

詳細は、こちらのURLをご覧下さい。
http://www.jnsa.org/caravan/index.html

2. 後援イベントのお知らせ

1．Security Tech Update/Tokyo 2005

会　期：2005年1月25日（火）～1月26日（水）
主　催：株式会IDGジャパン
会　場：新宿NSビル「NSイベントホール」
http://www.idg.co.jp/expo/nws/

2．PAGE 2005

会　期：2005年2月2日（水）～2月4日（金）
主　催：社団法人日本印刷技術協会
会　場：サンシャインシティコンベンションセンターTOKYO
http://www.jagat.or.jp/PAGE/index.htm

3．「NET & COM 2005」

会　期：2005年2月2日（水）～4日（金）
主　催：日経ＢＰ社
会　場：東京ビッグサイト
http://expo.nikkeibp.co.jp/netcom/

4．中小企業庁委託事業「平成16年度　情報モラル啓発セミナー」

会　期：2005年2月10日（木）
主　催：中小企業庁、
（財）ハイパーネットワーク社会研究所
会　場：沖縄コンベンションセンター
http://www.hyper.or.jp

3. JNSA部会・WG 2004年度活動

1. 政策部会

（部会長：下村正洋/ディアイティ）

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

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

（リーダー：山田英史氏/ディアイティ）

2001年から継続して被害調査を行い、被害額算定モデル等を提案してきた。今年度は、WGとして警察庁の調査案件「不正アクセス行為対策の実態調査ならびにアクセス制御機能に関する技術研究開発の状況等に関する調査」を受託、現在アンケート調査ならびに報告書作成作業を行っている。なお、昨年度からの独自調査も並行して行い、WGとして以下の内容を調査した報告書も作成する予定である。

【セキュリティベンダーとしての管理基準策定WG】

（リーダー：丸山司郎氏/ラック）

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

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

【セキュリティ監査WG】

（リーダー：大溝裕則氏/ジェイエムシー）

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

現在は、日経BP社の電子自治体ポータルサイトにて、WGメンバー有志でコラム「セキュリティ監査入門」を執筆中である。

http://premium.nikkeibp.co.jp/e-gov/column/2004/column9_18a.shtml

【マーケットリサーチWG】

（リーダー：玉井節朗氏/IDGジャパン）

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

1　企業のセキュリティシステム普及状況を確認し、強化すべきポイントを把握する。
2. 国内のセキュリティ産業の動向を把握し、自供企画の材料として会員企業に提供する。
3. 将来のセキュリティ普及の方向性を検討する材料とする。

9月に、「ITセキュリティの導入状況と満足度の調査」を行い、その中間発表を2004年11月に主催フォーラムNSF2004にて行った。最終報告書は12月中に公開予定である。

【プライバシー保護実装研究WG】

（リーダー：久波健二氏/日本IBMシステムズ･エンジニアリング）

プライバシー保護のために、IT技術はどこまで可能かの調査・研究をする。各社製品技術でどこまで対応可能かを調査し、製品だけでは満足できない要件をどうすればITで補完できるかの検討、ITで可能な部分と組織・運用で可能な部分の明確化などを行なう。

現在は11月で活動を終了し、「個人情報保護法ガイドラインWG」の情報システム部チーム担当として、WGを統合した。

【セキュリティ会計ガイドライン検討WG】

（リーダー：佐野智己氏/凸版印刷）

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

予定成果物は『ガイドライン』の上程。

【個人情報保護法ガイドラインWG】

（リーダー：佐藤憲一氏/大塚商会）

平成16年6月15日　経済産業省「個人情報保護法ガイドライン」が発表されたが、一般企業が切望することは、「保護法を遵守する何をどの程度実施すれば、保護法対策といえるのか？」である。そこで、企業が求める個人情報保護法を遵守するための具体的方法をガイドラインとして明文化し、広く流布することを目的とする

2005年3月にガイドライン書籍を発行予定で執筆活動中ある。

2. 技術部会

（部会長：佐藤友治氏/インターネット総合研究所）

技術部会では、今年度も成果物を作成するワーキンググループと勉強目的のワーキンググループに分かれて活動を行なう。その他、予算を得た活動は、プロジェクトとして活動を進める。主なワーキンググループ活動予定は、以下の通り。

【セキュリティポリシーWG】

（リーダー：小杉聖一氏/NECソフト）

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

【コンテントセキュリティWG】

（リーダー：松本直人氏/ネットアーク）

コンテントセキュリティに関するガイドラインドキュメントを作成。広く一般的に定義が無いコンテントセキュリティの定義と具体的なカテゴリー分けと手法を分類整理する。主な活動予定は、上記を踏まえた勉強会およびドキュメント作成など。

【不正プログラム調査WG】

（リーダー：渡部章氏/アークン）

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

【ハニーポットWG】

（リーダー：園田道夫氏/JNSA研究員）

2004年度は、2003年度に準備を整えたハニーポットサイトの運営を実際に行いつつ、そこからどのようなデータが得られるのか解析していく。その後はハニーポットサイトをさまざま展開し、ネットワーク上の場所によって得られるものが違うか？とか、公開形態やサーバーによって異なるか？などのテーマを設定しながらデータを収集し解析していく。

また、ハニーポットだけにとどまらず、トラフィック解析などのテーマも追いかけていく予定。

【データストレージ＆セキュリティWG】

（リーダー：立身俊雄氏/ディアイティ）

企業がデータの運用および保存を行う際の指標の検討を行なう。世の中の基準やユーザアンケート等による調査・分析に基づく、マネジメントポリシの作成などを予定。なお、本WGは、JDSF（Japan Data Storage Forum）殿と協調して活動する。

【暗号使用ポリシーテンプレート作成WG】

（リーダー：板倉行男氏/アークン）

セキュリティ管理策として暗号製品を使用する場合、ISMSなどのセキュリティポリシー認証基準では暗号使用ポリシーの策定を推奨している。また暗号技術を使用する場合、暗号に使用する鍵管理のルールを明確にし、それが守られなくてはならない。そのため、暗号使用ポリシーのテンプレートを作成する。今年度はPKI、電子署名の管理策をとる場合の暗号使用ポリシーを検討する。

【S/MIME検討WG】

（リーダー：磐城洋介氏/NTTコムウェア）

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

【Webセキュリティ調査･検証WG】

（リーダー：斉藤純平氏/アークン）

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

【PKI相互運用技術WG】

（リーダー：松本泰氏/セコム）

安全、安心な社会を構築する上でPKIの必要性を社会にアピールし、ネックとなるPKI相互運用性の問題などを自ら解決していく。

主な活動予定は、IETFの参加（年3回）、JESAPなどの他団体との連携、IETFのRFCなどの提案等。

【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）
脆弱性について、その危険度を定量化（数値化）する手法を検討する。
脆弱性の定量化については、すでにいくつかの方式がある。これらを検討した上で、実情に照らし合わせ、指標となりうる方式の検討を行っていく。

【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）
FIPS 140-2は今後暗号モジュールを実装する際の必須要件となりえ、CRYPTRECにおいても暗号モジュールのセキュリティ機能要求基準の0版とされている。しかし具体的には何をすれば良いのか？この用語はどの様な意味を持つのか？この定義は？と初見では理解し難い。
本WGはFIPS 140-2に対する疑問を解消し、啓発することを目的とする。

【ChallengePKIプロジェクト】
（リーダー：松本泰氏/セコム）
IPAの2004年度 情報セキュリティ関連の調査の「PKI における UTF8String問題に関する調査」に応募し採択された。現在、報告書は、作成中であるが、この報告書に付随する成果は、IETFに PKIX WGにフィードバックすることも検討している。

---

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

【セキュリティ啓発WG】
（リーダー：古川勝也氏/マイクロソフト）
昨年度経済産業省の委託事業として行なった「インターネット安全教室」を拡張して今年度は全国25ヶ所以上で行っている。その企画・運営協力を行なう。

【セキュリティスタジアムWG】
（リーダー：園田道夫氏/JNSA研究員）
不正アクセス手法の攻防の一大実験場「セキュリティスタジアム」の企画と運営を行なう。
2004年度はセミナーとスタジアム本大会をさらにシステマチックに開催できる仕組みを整えていく予定。セキュリティトピックのセミナーの企画や本大会企画準備、技術教育講座の企画なども検討していく。
2004年11月2日～4日に、「セキュリティ・スタジアム2004」を開催した。

---

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

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

---

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

【セミナー運営WG】
（リーダー：中台芳夫氏/西日本電信電話）
西日本支部主催セキュリティセミナーのコンテンツの企画検討と運営を行なう。
11月11日には、NSF2004 in OSAKAと題して、大阪市新梅田研修セミナーにてセミナーを開催した。

4. JNSA役員一覧

会　長　石田　晴久
多摩美術大学教授・東京大学名誉教授

副会長　長尾　多一郎
株式会社ネットマークス 代表取締役社長

副会長　東　貴彦
マイクロソフト株式会社 業務執行役員

副会長　大和　敏彦
シスコシステムズ株式会社 執行役員CTO

理　事(50音順)

株式会社アイアイジェイテクノロジー
在賀　良助

株式会社ヒューコム
井上　陽一

株式会社大塚商会
宇佐美　慎治

三菱電機株式会社　情報技術総合研究所
後沢　忍

株式会社フォーバルクリエーティブ
浦野　義朗

浦山　清治

シムデスク･テクノロジーズ
岡村　靖

新日鉄ソリューションズ株式会社
甲斐　龍一郎

勝見　勉

セコムトラストネット株式会社
川上　博康

トレンドマイクロ株式会社
小屋　晋吾

株式会社ディアイティ
下村　正洋

株式会社ネットマークス
鷲見　晴美

セコム株式会社
鈴木　優一

横河電機株式会社
武智　洋

マカフィー株式会社
田中　辰夫

株式会社IDGジャパン
玉井　節朗

NTTアドバンステクノロジ株式会社
辻　久雄

システムニーズ株式会社
中山　恵介

株式会社ＮＴＴデータ
西尾　秀一

株式会社ラック
西本　逸郎

大日本印刷株式会社
野久保　秀紀

東芝ソリューション株式会社
坂内　明

マイクロソフト株式会社
古川　勝也

NTTコミュニケーションズ株式会社
松尾　直樹

RSAセキュリティ株式会社
山野　修

古河電気工業株式会社
吉澤　昭男

グローバルセキュリティエキスパート株式会社
若井　順一

東京海上日動火災保険株式会社
綿引　宏行

監　事

清友監査法人　公認会計士
土井　充

顧　問

東京大学　教授
今井　秀樹

新東京法律事務所　弁護士
北沢　義博

東京電機大学　教授
佐々木　良一

慶応義塾大学　教授
武藤　佳恭

早稲田大学　客員教授
前川　徹

早稲田大学　教授
村岡　洋一

奈良先端科学技術大学院大学　教授
山口　英

東京大学　教授
吉田　眞

事務局長

株式会社ディアイティ
下村　正洋

5. 会員企業一覧

2004年11月24日現在　187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）アイ・ティ・フロンティア
（株）IDG ジャパン
（株）アイネス
アイネット・システムズ（株）
（株）IP イノベーションズ New
アイマトリックス（株）
（株）アクセンス・テクノロジー
あずさ監査法人
（株）網屋
アライドテレシス（株）
（株）アルゴ21
（株）アルテミス
（株）アンラボ
イーディーコントライブ（株）
（株）イオノス New
伊藤忠テクノサイエンス（株）
学校法人 岩崎学園
インターネット セキュリティ システムズ（株）
（株）インターネット総合研究所
インテック・ウェブ・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） New
インフォコム（株）
（株）インフォセック
（株）インプレス
ウッドランド（株）
AT＆T グローバル・サービス（株）
（株）エス・アイ・ディ・シー
エス・アンド・アイ（株） New
（株）エス・エス・アイ・ジェイ
SSH コミュニケーションズ・セキュリティ（株）
（株）エス・シー・ラボ
NRI セキュアテクノロジーズ（株）
NRI データサービス（株）
NEC ソフト（株）
NEC ネクサソリューションズ（株）
NTT アドバンステクノロジ（株）
NTT コミュニケーションズ（株）
エヌ・ティ・ティ・コムウェア（株）
（株）NTT データ
（株）エネルギア・コミュニケーションズ
エムオーテックス（株）
（株）エム・ファクトリー New
エリアビイジャパン（株）
ELNIS テクノロジーズ（株）
（株）大塚商会
オムロンフィールドエンジニアリング（株）

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

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

（株）損保ジャパン・リスクマネジメント

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

【な】
（株）ニコンシステム
西日本電信電話（株）
日商エレクトロニクス（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）
日本オラクル（株）
日本高信頼システム（株）
日本コムシス（株）
日本ジオトラスト（株） New
（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）
日本電気エンジニアリング（株）
日本電気システム建設（株）
日本電信電話（株）　情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
ネクストコム（株）
（株）ネットアーク
（株）ネット・タイム
（株）ネットマークス
（株）ネットワークセキュリティテクノロジージャパン
ネットワンシステムズ（株）
ノベル（株）

【は】
（株）ハイエレコン
東日本電信電話（株）
（株）日立システムアンドサービス
（株）日立製作所
日立ソフトウェアエンジニアリング（株）
（株）ヒューコム
（株）ビー・エス・ピー
（株）PFU
ファルコンシステムコンサルティング（株）
（株）フォーバル クリエーティブ
富士ゼロックス（株）
富士ゼロックス情報システム（株）
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
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 New
（株）ブリッジ・メタウェア
古河電気工業（株）
（株）プロティビティ

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

【や】
横河電機（株）

【ら】
（株）ラック
菱洋エレクトロ（株）
（有）ロボック

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

6. JNSA年間活動（2004年度）

4月	4月7日	第1回政策部会	
	4月8日	第1回幹事会	
	4月9日	第1回マーケティング部会	
	4月10日	第1回教育部会	
	4月24日	2004年度理事会	
	4月27日	IETF参加報告会	
5月	5月11日	2004年度技術部会	
	5月12日	ITセキュリティ評価・認証制度　勉強会開催	
	5月18日	2003年度WG成果報告会開催（大手町サンケイプラザ）	
	5月18日	JNSA総会（大手町サンケイプラザ）	
	5月20-22日	コンピュータ犯罪に関する白浜シンポジウム後援	
	5月28日	セキュリティスタジアムセミナー開催（人事労務会館）	
6月	6月8日	第2回幹事会	
	6月17日	第2回政策部会	
	6月17-18日	第5回電子署名・電子認証シンポジウム後援	
	6月23日	臨時幹事会	
	6月25日	第1回西日本支部会合	
	6月28日-7月2日	Net World+Interop 2003 Tokyo後援	
	6月29日	JASA情報セキュリティフォーラム後援	
7月	7月12-16日	日韓ベンチャープラザ2004後援	
	7月13日	個人情報保護法説明会開催	
	7月20日	第2回西日本支部会合	
	7月20日	脆弱性関連情報取り扱い説明会協賛	
	7月21日	日本UNIXユーザ会2004年度定期総会併設セミナー後援	
	7月21-23日	ワイヤレスジャパン2004後援	
	7月27日	第1回技術部会リーダー会	
	7月28日	セキュリティ・マネジメント・フォーラム協賛	
	7月30日	第3回幹事会	
8月	8月3日	第3回政策部会	
	8月26日	セキュリティAPIセミナー（セコムホール）	
	8月27日	第3回西日本支部会	
9月	9月15日	第4回政策部会	
	9月15日	第4回幹事会	
	9月30日	第2回教育部会	
10月	10月7-9日	ネットワーク・セキュリティワークショップin越後湯沢2004協力	2004年10月～2005年2月「インターネット安全教室」開催
	10月19日	第2回技術部会リーダー会	
	10月7-9日	平成16年度情報モラル啓発セミナー（仙台）後援	
	10月28-29日	Network Security Form 2004開催（青山TEPIAホール）	
11月	11月1日	JESAP電子署名・認証フォーラム後援	
	11月2-4日	セキュリティ・スタジアム2004開催	
	11月2-3日	スキルマップ作成WG合宿	
	11月11-12日	Pacsec.jp 2004後援	
	11月16-17日	電子自治体フェアTOKYO 2004後援	
	11月16-18日	Global IP Business Exchange後援	
	11月17-18日	マルチメディア&VRメッセぎふ2004後援	
	11月18-20日	セキュリティポリシーWG合宿	
	11月24日	第5回政策部会	
	11月24日	第5回幹事会	
12月	12月1日	Internet Week 2004開催（パシフィコ横浜）	
	12月6日	セキュアOSカンファレンス後援	
	12月9日	認証技術の動向セミナー開催（セコムホール）	
	12月13日	暗号モジュール評価基準カンファレンス開催	
	12月16日	平成16年度　情報モラル啓発セミナー（東京）後援	
	12月20-21日	デジタル・フォレンジック・コミュニティ2004後援	
1月	1月17日	賀詞交換会	
	1月26日	Security Tech Update/Tokyo 2005後援	
2月	2月2-4日	NET&COM 2005後援	
	2月2-4日	PAGE 2005後援	
	2月10日	平成16年度　情報モラル啓発セミナー(沖縄)後援	

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

7. JNSA について

■会員の特典

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

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

8. お問い合せ

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

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

JNSA Press vol.12

2004年12月27日発行

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

印刷　プリンテックス株式会社

NPO 日本ネットワークセキュリティ協会会員 行動指針

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

そのため、以下の通り会員の行動指針を定め、規範とするよう努めます。

会員は、この指針の遵守に努め、会の目的を共有するにふさわしい姿を目指します。

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

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

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

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