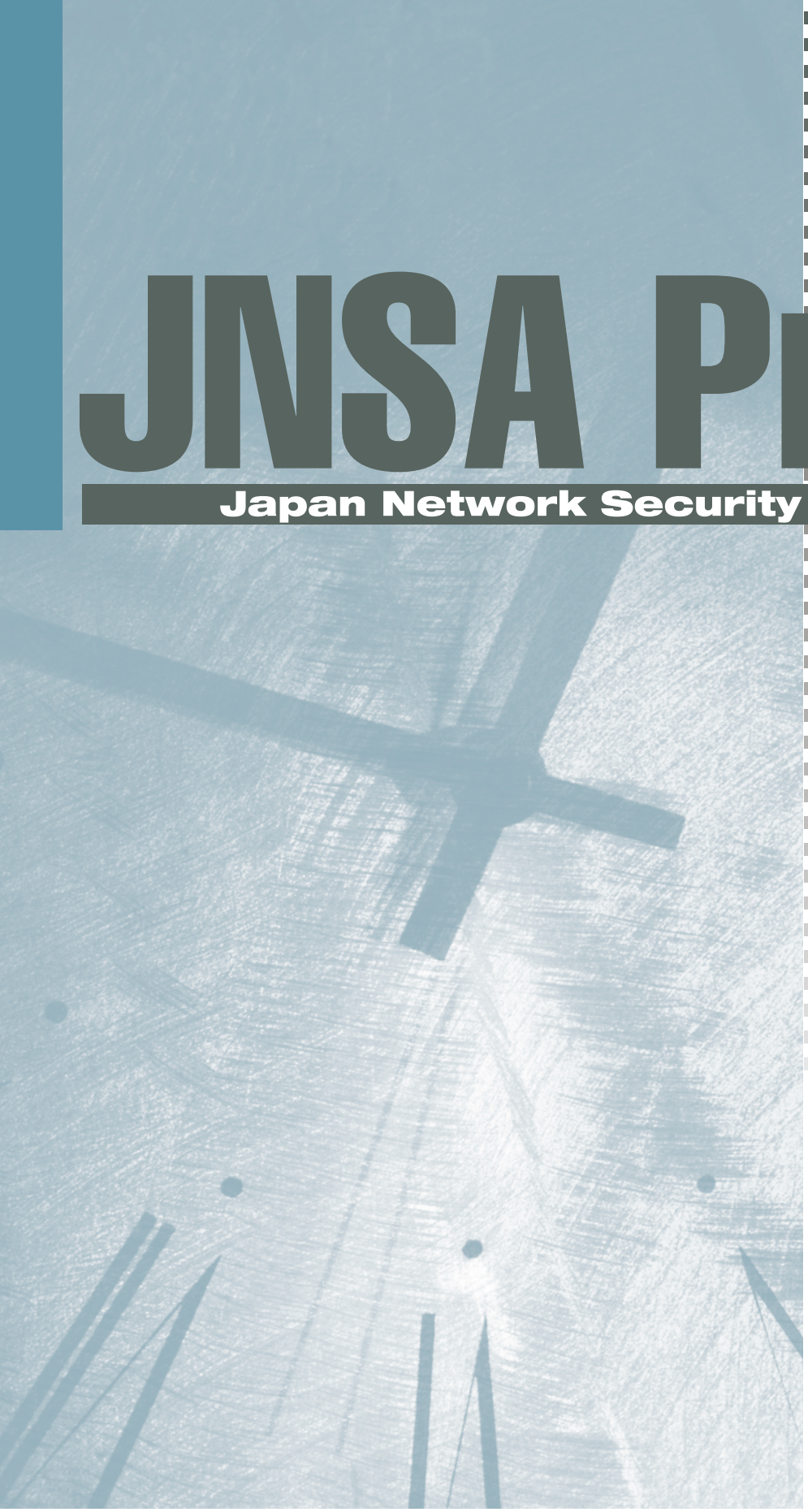


JNSA Press

Japan Network Security Association

Vol.9
January 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

暗号とネットワークセキュリティ

東京大学　生産技術研究所
教授　今井　秀樹

暗号技術がネットワークセキュリティの基盤の一つであることは、ネットワークセキュリティに関わる人なら誰でも理解していることでしょう。しかし、暗号だけで、ネットワークセキュリティが解決できるわけではないことも明らかです。では、ネットワークセキュリティ全体のなかで暗号はどのような地位を占めるのでしょうか。「今、暗号は使えるものがいくらでもある、適当に選んで使えばよい。暗号はただの道具の一つ。」という考え方が主流なのかも知れません。確かに、それも一理あります。ただし、暗号を選ぶ際には、CRYPTRECの電子政府推奨暗号リスト*などを利用して、安全なものを選ぶ必要があります。

しかし、暗号をブラックボックスとしてだけ扱うのは、余りにももったいないことです。暗号は、安全性を最も厳密に扱う科学であり技術です。情報セキュリティを考える際に、暗号の考え方がとても役に立つのです。ある著名な暗号技術者が「情報セキュリティを考える際、暗号を考えなくてよいことはない」と言っていましたが、その通りであると思います。どのような前提のもとで安全性をいかに定義し、それをどのようにして保証していくのかについて、最も論理的に扱っているのが暗号分野なのです。

暗号の考え方が有用であることを示すには、暗号研究者が暗号分野以外のセキュリティ分野でいかに活躍しているかを見れば十分でしょう。一流の暗号研究者は安全性についてあらゆる点から論理的に考える習慣が身についています。このため、システムの脆弱性に関し、鋭い洞察力を持っているのです。例えば、横浜国立大学の松本勉教授がほとんどの指紋センサーを欺ける偽造指紋をグミで作れることを示したことは、バイオメトリックス認証における重要な研究成果として世界的話題になりました。彼は筆者の弟子で暗号研究者に他なりません。このような例は他にも多くあります。

ただ、暗号理論で扱えるモデルが、非常に簡単なものに限られていることは事実です。現実の複雑なシステムにそのまま適用することはできません。しかし、最近、複雑なシステムでも簡単なモデルの合成で表せるなら、その安全性を要素モデルの安全性に基づいて議論するという研究も多くなされるようになってきました。将来は、かなり複雑なシステムでも、暗号的手法で厳密に安全性を議論できるようになるかも知れません。

もちろん、そうなったとしても、人を重要な要素として含む複雑な情報システムの安全性を、すべて理論的に厳密に扱えることはないでしょう。ただ、暗号技術や暗号的

な考え方がネットワークセキュリティ全般においても、次第に大きな部分を占めていかねばならないと考えています。それにより、簡単には崩せないセキュリティのコアの部分が拡がり、人が神経をすり減らさなくても安心して利用できるネットワークが実現していくと思えるからです。ネットワークセキュリティに携わる方々に、ここでもう一度、暗号の重要性を見直してして頂ければ、筆者として望外の幸せです。

* http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html
  http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

多様化するリスク管理の実際

ハニーポットWGリーダー
園田　道夫

1. 便利になりすぎた？PC

モバイルPC、ノートパソコンを見てみよう。ごく普通に無線LANが付いている。USBインタフェースも付いている。CDだけでなくDVDも読めるし書けるものまである。

もちろん従来からのethernetインタフェースはもはや標準だ。PCMCIAのスロットも同じ。56Kモデムもついているし、メモリスティックを食べてしまうものまである。

外部記憶を担うメディアも種類が増えた。USBメモリはギガ単位の容量になり、PCMCIA経由メモリカードがあったり、メモリスティックがあったり、もちろんCDやDVDがあったりもする。

そしてネットワーク。ethernetやモデムはもちろん、無線LANインタフェース内臓のものも珍しくないし、USBから無線LANにつないだりもできる。PCMPIAのアダプタとPHSカードからデジタルでダイヤルアップするのは、無線LAN利用よりも広がっているようだ。

高機能化は現在こんなに進んでいる。

裏を返せば、それだけリスクも多様化が進んでいるということでもある。

便利な機能はそれだけリスクもある。例えば、無線LANはいちいち線を用意しなくとも、電波が入る位置ならばどこででもネットワークに接続ができる。しかしこれは、電波が入る位置に居る人間ならば、誰でもネットワークに接続できる、ということでもある。そして問題は、電波が届く範囲を、今の技術とコストでは制御できない、ということである。つまり、リスクの程度としては、誰がいつ繋いでくるか分からない＝インターネットと同じ、ということになる。それをLAN（Local Area Network）などと言ってしまうから、安易に抜け道を作ってしまうわけだ。

外部記憶メディアが高機能で、かつ超小型化してきているのも厄介だ。例えばUSBメモリならば、たいていのものは余裕でおさまる容量である。それがどこにでも隠せるほどの大きさなのだ。

こういう時代に何をどう管理していかなければいけないのか？

2. 管理者、普通のユーザー、それぞれの言い分

リスクは確実に増えているのに、管理運用する側のリソースは増えていない。それどころか戦力はまっさきに削減されることすらある。

そうなると現場は目先の仕事をこなすことだけに追われることになる。目先の仕事の主なものは、多機能化したコンピュータの面倒を見ることだ。多機能化するということは、裏を返せばそれだけ不安定要素を抱え込むことでもある。流石に以前のようにいきなりブルースクリーンとか、いきなり起動しなくなるとか、そういうことは減っているが、動かない使えないという事象はそれほど減ってはいない。

いや、むしろ以前よりも依存度が高くなっているだけ、クレームやお助けのお願いの総量は増えているのではないだろうか。

減らされるリソースで増え続けるクレーム処理にあたりながら、さらに新しいリスクを管理する方法について考える余裕などあるわけがない。そんな過酷な状況で、いったいどうやってセキュリティを守ればいいのか？

管理者ではなく普通のユーザー側にも言い分がある。・・・だいたい会社でPCを全員使わないと仕事にならない仕組みなのに、そこまで不可欠に近いものになってきているはずなのに、なんでこんなによく止まったり、ウイルスだ何だとわけのわからない障害が起きたり、パッチとかサービスパックとか面倒な手間ばかりかかったりするのだろう？ウイルス対策ソフトウエアのパターンファイル（これがまたわけがわからん仕組みだが）を毎日更新しろとか、WindowsUpdateとかいう仕組みを使ってチェックしろとか、何か昔より確実にやることが増えて、折角PCを入れているのにいっこうに楽にならないし効率も上がらない。そんな

気がして仕方が無いのだがどうなのか？

そもそもなんでこう急いでいるときに限って動かなくなるのだ？

いや、それ以前に、長いパスワードをつけておぼえろとか、おぼえやすい単語は使うなとか、そればかりか3ヶ月に1回変えろとか、そんなことができると思っているのだろうか？急にある文書を印刷しなければならなくなったとき、いちいちPCを起動してファイルを探してとかやっていたら平気で10分とか15分とかかかってしまうし、つけっぱなしは止めろと言われても会議に資料が間に合わなくて怒られるのは自分だし、いちいち煩雑な手順など守っていられない。

無線LANなんて便利なシロモノを「危ないから使うな」と言われても全然納得できないし、だいたいどこが危ないのかよくわからない。外から繋いでくるやつが居たとして、ウチみたいに何もない会社から何を盗み出すっていうのか？ウチみたいなところに興味を抱くような悪者が居るとも思えないし。

まあでも、いろいろ大変なのはわかるので、せめてPCが止まったときにすぐ何とかなるような仕組み？連絡先？ヘルプ依頼先がはっきりしていて欲しいのだが、お助け連絡を入れても誰も出ないし、返事が遅いし、半日も1日もふらふらしなければならず「遊んでいるのか」とか言われてしまうし、そこだけでもなんとかして欲しいのだが。

こんな厄介なPCなんてシロモノ、いつまで使いつづけなければならないのだ？

3. 最も大きなリスク

結局のところ、現在最も大きなリスクとは「普通のユーザー」ではないだろうか。なぜなら、「普通のユーザー」は今のコンピュータが持つ機能とそのリスクを理解していないからだ。だがそれも無理は無い。「普通のユーザー」は専門家ではないからこそ「普通」なのだから。

「普通のユーザー」は便利さ、面白さは体感しているが、そのリスクがわからないし、そもそも何がどう危険なのかわかっていない。また、何でパッチだアップデートだが必要なのか、ウイルスってそもそも何でマズいのかも理解していないし、そもそもただでさえわけがわからないPCを言われたとおりに使うだけで精一杯だ。

そういう非専門家ユーザーのリテラシーを向上させるのは、いったいどうすればいいのだろうか？

ここで言うリテラシーの向上とはこういうことだ。「非専門家ユーザー」が、Windows系パッチ情報が出たらWindowsUpdateをきちっとチェックして必要ならば即導入し、ウイルス対策ソフトウエアのパターンファイルは1日1回は更新し、パスワードはランダム英数字8文字以上で辞書には載っていないものを用いて3ヶ月に1回は変更する。万が一怪しげなWebサイトに誘導されたとしても、そこが本当に「怪しい」かどうか様々な材料を見て判断し、怪しいとわかったら即回避する。お買い物サイトなどでも不要な個人情報を登録しないように気をつけて、目的のために止むを得ず登録した個人情報もちゃんと管理されているのかこれまた様々な材料を見て判断し、危ないようなら即回避する。そして、メールの添付ファイルはいきなりダブルクリックせず、ウイルスかどうか確認してから開けてみる。・・・リテラシーが十分に高いと言えるユーザーは、この程度のことは普通にできなければならない。

しかし、正直なところこのレベルにスタッフ全員が到達する、というのは無理だろう。

もちろん手順が決まっていることはできるだろう。だが残念ながらその手順が煩雑であることも多く、それでなくても仕事仕事で追われているのに手間も時間もかかると真面目なユーザーでもサボりたくなるのが人情だ。手順が決まっているものですらそうなのに、決まっていないとどうなるだろうか？専門家ですらそのお買い物サイトが危険なのかどうか判断できないこともあるのに、「非専門家ユーザー」には無理だ。

さらに追い討ちをかけるようだが、仕事のやり方そのものも多様化してきている。

今や仕事場だけが「仕事場」ではない。そこらじゅ

うに無線のアクセスポイントが存在するし、つなぎ放題でも安目のPHSカードも売れているし、常時接続は当たり前のように普及しているし、外出先でも家でも場所を選ばずに仕事ができるわけだ。そして例によってそうした便利さの裏にはリスクが有り、外出先でも家でもおかしなアクセスに晒されてしまう危険があるのだ。

現在、PCのユーザーが直面しているリスクには、ざっくり見てきただけでもこれだけの種類がある。厄介なことにこれだけのリスクのうちのどれかひとつを怠るだけで、ブラスターなどのワームを社内に呼び込んでしまうことになる。実際、IPA（情報処理振興事業協会）の「W32/MSBlaster及びW32/Welchiウイルス被害に関する企業アンケート調査」（2003年9月）によれば、ブラスターは持込PCから入り込んだ、というのが25％もある。やはり仕事のやり方が多様化してきていて、今までとは異なる経路でワームが持ち込まれているということが浮き彫りになっている。

また、BCN総研による「セキュリティ対策に関するアンケート調査」（2003年9月）という、企業だけではない一般ユーザーを対象とした調査では、「ブラスターをきっかけに何らかのセキュリティ対策を行ったか」という問いに対し、27.6％の人が「全く何もしていない」と回答している。ということはつまり、勤め人のユーザーのリテラシーを100％にしたところで、家庭やプライベートな活動の場などには未だに「何の対策もしていない」ユーザーが多数存在し、その脅威にさらされる、ということだ。常時接続ポイントがルーターでフィルタリングされていたとしても、子供が学校で感染してくるかも知れないし、親もプライベートサークルなどで感染してくるかも知れない。いったんそれが入り込んだらつねに感染する危険はあるわけだ。

切れ目無くどこでも仕事できるようになってしまった現在、ワームなどのリスクはまさしく、風邪などと一緒なのだ。そして、どんなに用心していても風邪は引くときは引いてしまうものだ。

とはいえ、何らかの対策を打たなければ、今までどおりワームが入り込むだろうし、今までどおり内部情報は漏洩するだろう。

4.「普通のユーザー」対策

もちろん、どの組織もただ手をこまねいていたわけではない。これまでにもさまざまなセキュリティ対策が講じられてきた。

しかし、そうした対策の中でも例えば「リテラシー教育による向上」「パッチ管理やパターン更新をユーザーに任せる方法」「PCの持ち出し、持込管理」「セキュリティポリシーの徹底」といった、「普通のユーザー（エンドユーザー）」にある意味依存するような対策はあまり効果が上がっていない。逆に、一定の成果を上げている対策には「ファイアウォールの導入」「サーバー、ゲイトウエイ型ウイルス対策」「IDSの導入」などが上げられるだろう。効果が上がっている対策は、「普通のユーザー（エンドユーザー）」に依存していないものが多いはずだ。

確かに情報システムに予算をかけにくいという状況はわかるが、結果として生じる事故などによって業務を大々的に停止されてしまうと、渋る予算をさらに上回って余りあるような損害を直接的に被ることになりかねない。そしてそういう機会はどんどん増えつづけている。

そろそろ「普通のユーザー」対策に本腰を入れていくべきではないだろうか。しかも「普通のユーザー」に依存しないで実施できる対策に。

対策をいくつか具体的に挙げてみよう。

（1）インベントリー管理

ここへ来て各ベンダーからエンドユーザーのインベントリー管理を行う製品が出始めている。これはエンドユーザーのPCのパッチやサービスパック状況を把握したり、エンドユーザーの行動をログに残したり、外部記憶装置（CD、DVD、USBメモリなど）の使用制限を行ったりするものもある。また、一時的に状

況を把握するだけでなく、例えばモバイル接続時にあらかじめ設定されたポリシーによるチェックを実施し、適合しないPCは繋がせない、などの管理を行えるものもある。

ちなみにマイクロソフト社からは、パッチの更新を行うための仕組みとしてSoftware Update Serviceが無償で提供されている。

さらには、保護すべきファイルに着目した、ファイル管理という手段もある。

(2)パーソナルファイアウォール

個々のPCのアクセスをフィルターするファイアウォールで、ウイルス対策ソフトウエアと同じパッケージになっていることも多い。個々のPCにそのまま入れておくだけでなく、統合的に管理する仕組みも製品として出てきている。上記インベントリー管理とセットになっていることもある。

(3)トラフィックモニター

ネットワークを飛び交う通信をモニターし、あるサーバーへのアクセス記録や相互通信の記録などを残しておく。情報漏洩時などの事後的な監査や追跡に役立てる目的である。

(4)部署ファイアウォール

例えば部署ごとにファイアウォールやルーターによるパケットフィルタリングの仕組みを導入する。いっせいに全社にワームが広がらないように、セグメントごとに防御するための仕組み。

現実的なものはこういうところだろうか。

(1)と(2)は、PCを持つユーザーすべてに導入、あるいはモバイルユーザーだけにでも導入するような対策である。従ってそれなりに個数も多くなるし、当然ながら初期投資もそれなりにかかるものだ。そうした投資を抑える方法はある。例えばフリーソフトウエアでの代用とか、集中管理をある程度あきらめる、などの機能制限を選択すれば、ベンダーが勧めるまんまのゴージャスな仕様のソリューションに大金をはたかないでも済むわけだ。決まったポリシーを適用しておくだけでも効果を上げることができる。

例えばパーソナルファイアウォールだ。もちろんすべてフリーのソフトウエアである必要は無いが、統合的に管理をするほどの柔軟性が必要なわけでもない。そのPCに対する外からのアクセスはすべて拒否し、内側から張られるTCPのセッションは許可、あとはDNS参照とftp、インターネットを使うときはそれだけで十分だろう。ファイル共有が必要ならば相手のサーバーを特定して該当するポートを許可すればいい。

これを実施するだけで、実はワームへの対策としては完璧とは言わないが十分だろう。ワームはその多くが「ファイル共有」と「OSに潜むセキュリティ上の弱点」を狙ってアクセスしてくる。そもそも仕事する上では必要が無いアクセスを解放してしまっているために、そうしたアクセスが脅威になるわけだ。不要なアクセスはさせないし、自らも行わない。これを実現するには個々のPCに入れるファイアウォールが現在のところは最適解である。個々のPCに入れておけば、モバイル環境であろうと外出先であろうと、危険な家庭内であろうと有効な防護策となる。

ファイアウォールをあまねく行き渡らせることが不可能であるならば(いろいろ事情もあるだろう)、部署ごとのファイアウォールでもう少し範囲を広めて通信制御する手もある。一般にファイアウォールというと運用管理にそれなりの手間がかかってしまうものだが、その組織に1つのファイアウォールなどの場合は、さまざまな要件を集約しなければならなかったり、通信量も多かったりで手間がかかるわけだ。しかしそれが例えば部署という軽い単位であれば、ポリシーもそんなに複雑なことをやらせなければ良いし、通信量もさほどではないだろうし、あまり気にかけず放置に近いくらいでも役には立ってくれる。また、情報漏洩対策として通信のログを取得することも容易だ。

もちろん通信のログをいくら取得したとしても、漏洩があったことを事後的にトレースできる、というこ

とでしかない。しかし、これを告知しておくことでの抑止効果は期待できるし、取得したデータをきちんと証明付きで保管しておけば、仮に民事での訴訟となった場合でも使える証拠となるはずだ。

通信の記録ということでは(3)のトラフィックモニターも同様である。ファイアウォールのログなどと異なり、こちらは使うツールや方法などによって取得するログの内容を加減できる。ただし、モニター対象となるネットワークのユーザーへの事前告知は必要だ。また、暗号化通信対策などは別途配慮しなければならないが、IPヘッダーレベルの情報だけでも取得できればいろいろと使えるだろう。

筆者のお勧めはこんな感じだ。

「ワーム対策」
①パーソナルファイアウォールの導入
②部署ファイアウォール
③インベントリー管理、もしくはパッチ管理（Software Update Serviceなど）

「情報漏洩対策」
①通信ログ管理
②インベントリー管理
③ファイル管理

数字はプライオリティで、2003年末現在のプライオリティだ。ファイル管理やメディア管理など、さらにリーズナブルで使えるソリューションが出現してきたら、このプライオリティは変動するものと思っていただきたい。

最後に1つ付け加えておきたいのは、「検疫」についてである。

PC個々にファイアウォールを行き渡らせることができない場合には、PCを外から持ち込むときに「検疫」させるのだ。ワームなどに感染しているPCには、大量のパケットを撒き散らすなどの特徴がある。その特徴が出ているかどうかを見極めて、もしクロだったら洗浄してから接続させるのだ。

例えばこれを、DHCPサーバーと連携して行うソリューションが出てきている。IPを付与する前にポリシーのチェック等を行うのだ。これはエージェントソフトウエアが必要となる。

他にはVPN接続時にポリシーベースでチェックするソリューションも存在する。ただしこれはVPN接続にしか今のところは対応していないようだ。

筆者は現実的な運用に耐える「検疫」は、もっと手軽でなければならないと考えている。今のところはまだ、十分に手軽なソリューションは存在せず、どこか重たいものばかりだ。LANスイッチなどのトラフィックを常に監視しているようなソリューションもあるが、理想的にはそれを自動化・軽量化したいところだ。

でなければ、疲弊した日本企業では導入してもらえないだろう。重たい仕組みを入れると現場が管理工数の増大で悲鳴を上げ、経営も予算を負い、ということになってしまう。

筆者はトラフィック解析の仕組みを突き詰めることで、重たい仕組みになることを打破できると考えている。だがその前に、予防策の方が重要であろう。しっかり対応できて十分に運用可能な、そういう予防策を選定するために、本稿が役に立つことを願っている。

JNSA ワーキンググループ紹介

データストレージ&セキュリティ WG

株式会社ネットマークス
データストレージ&セキュリティ WG リーダー
内田　昌宏

■ はじめに

それは、ヒューコム・井上社長（JNSA 理事）から頂いた一通のメールから始まった。『日本データストレージフォーラム（以下、JDSF[1]）から、JNSA への協力依頼があった。取りまとめしてほしい』と。
聞けば、JDSF では、データ・マネジメントの検討に際し、セキュリティは避けては通れない。データバックアップ認定制度なるものも規定され、益々、セキュリティに配意した活動の必要を感じているとの事。

考えてみれば、セキュリティ関係の国際標準やガイドラインの中でも、「事業継続」や「バックアップ」の項目は存在するものの、表現は「定期的にバックアップを実施すること」「復旧、回復の訓練を行うこと」などといった表現に留まっているケースが多い。

本 WG はこのような背景のもと、JDSF ／ JNSA 双方からメンバを募り、2003 年 6 月に共同 WG として活動を開始した。

■ 設立の趣旨／活動の目的

事業継続性の向上を図るため、企業内や IDC[2] でストレージネットワークの導入や活用が進んでいる。しかし、ストレージの導入が進むにつれて、「蓄積されたデータをどうやって不正アクセスや破壊から保護するか」ということが重要な課題になってきた。

このため本 WG では、企業がデータの運用および保存を行なう際に指標となるような管理ポリシ作成や推奨システムモデルの策定を目指す。この指標は、現状のストレージ技術やメディア特性を加味したものであり、データの種類や目的による法的な根拠も必要と考える。またデータの可用性や原本性の担保のためのセキュリティ技術や基準等も盛り込まれるべきであり、ストレージとセキュリティの技術的な側面だけでなく、人を含めた運用までを考慮する必要があると考える。可能であれば、業種・業態毎に必要な実装レベルについても検討していきたい。

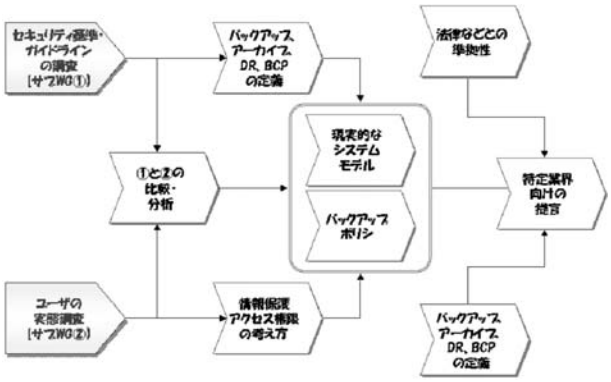
今のところ、本 WG の成果物は、

- データマネジメントポリシのサンプル
- 関連する法律・法令、ガイドラインの提示
- ストレージ技術とセキュリティ技術を活かしたシステムモデル

を考えている。

■ 活動方針と現在までの進捗

1 回目のキックオフミーティングに続いて、2 回目および 3 回目のミーティングでは、双方の理解を深めるため、ストレージおよびセキュリティの全体像／市場動向／トレンドなどについての勉強会を行なった。
具体的な活動を開始するにあたり、以下の 2 つのサブ WG にてスタート［下図参照］。



［図：当面の進め方］

□ **基準・ガイドライン調査サブ WG**

○ 目的：
バックアップ／アーカイブ／事業継続などの言葉の定義と、各々を実施する目的や意図を正確に理解するため、既存のセキュリティ基準やガイドラインから関連項目を調査する。

○ 調査：
経済産業省（ISMS、セキュリティ監査基準など）、金融庁（検査マニュアル、FISC ガイドラインなど）、厚生労働省（医療分野情報化のためのグランドデザインなど）、総務省（住基ネット、個人情報保

[1] http://www.jdsf.gr.jp
[2] Internet Data Center の略

護など)、警察庁関係など

□ **ユーザ現状調査サブWG**

○ 目的：
ユーザ企業でのバックアップの実態を理解することを目的に、システムの方式やバックアップポリシ有無などを調査する。

○ 調査：
JDSFおよびJNSA会員企業他にアンケート形式で依頼

各サブWGでのミーティングとワークの結果、現在、「基準・ガイドライン調査サブWG」では基準ガイドライン調査レポートを作成。「ユーザ現状調査サブWG」では、アンケート内容がほぼフィックスした。

■ 今後の予定

ユーザ現状調査アンケートを実施(2004年1月頃から)し、その結果と“基準ガイドライン調査レポート”を比較検討することで、現実的なバックアップポリシや、バックアップのためのシステムモデルを検討していく予定である。

なお平行して、「バックアップ」「アーカイブ」「ディザスタリカバリ」などの用語の定義も明確化していく予定である。

■ おわりに

外部団体とのコラボレーションWGは、JNSAにとってはじめての試みである。業界に留まらず広く外部と交流することで、より視野を広げていきたい。今回、共同作業を行なうJDSFは、ストレージ技術や運用技術を広く研究・発信しており、JNSAとJDSF双方の技術を共有し共同活動することで、今までにない成果が得られると確信する。

JNSA ワーキンググループ紹介

ハニーポットWG

ハニーポットWGリーダー
園田　道夫

■ はじめに

200年度に活動していた不正アクセス調査ワーキンググループが、追いかけるテーマが当初のものから離れてきたので、テーマを明確化する目的もあり活動を一度リセットし、ハニーポットワーキンググループとして2003年度に新装開店しました。2003年の9月には専用回線を準備、また専用マシンも購入しハニーポットをインストール、着々と準備を進めています。10月からは週に2回、メンバーが各々業務終了後に集まってはハニーポットをいじっています。

■ 活動の内容

文字通りハニーポットを中心にセキュリティ技術を調査学習しているワーキンググループです。しかし、それだけではなくハニーポットってそもそも売れるのか？みたいなことも議論しています。

ハニーポットに関わる技術というのは、これまでのセキュリティ技術のある意味集大成とも言えます。防衛技術、検知技術、そして攻撃技術について知見が無いと、構築し運用管理することは難しいものです。

このワーキンググループでは運用管理から、さらにその先にある情報公開についても検討をしています。

また、実際にハニーポットを構築もしています。構築している際に検討した論点や結果としてどういう実装になったかなどは、インターネットウィーク2003にて一端を紹介いたしましたが、正式なレポートは成果物として年度末にリリースする予定にしています。

現在構築中のハニーポットについて少し紹介しておきましょう。ハニーポットはご存知のとおり、囮とか罠とかいうニュアンスのサーバー、もしくはネットワークです。ネットワークのことはハニーネットと呼んだりもします。現在ワーキンググループにて構築中のものは小規模なハニーネットとでも言うべきもので、囮として使用されるサーバーは現在のところ3台（仮想的な意味で）あります。この3台はあるドメインを持ち、ごく一般的なサイトを構成しています。

サーバーソフトウエアはわざと旧型の穴があるものを用意しています。もちろん客寄せのためですが、回線が開通して機器を接続した途端に大量のワームのプローブアクセスに混じってお客さんらしきアクセスもあったりしましたので、もしかするとドメインもサーバーのコンテンツも全く必要無いのかも知れません。

他にサイト内にはIDSとパケットロガーも構築しています。何らかの怪しいアクセスが行われた場合、そのログを多角的に取得しておきたいという意味合いと、もう1つのテーマであるデータ解析の材料として実装しました。プロモーションがうまくいって、お客さんが多数いらっしゃるようだったら、今後検出精度等の比較も可能になると思います。

現在構築中のハニーポットはバージョン1ということになりますが、以降の計画としては、

- 現在の緩めのポリシーをキツイ方向に締めたらどういう反応があるか？
- 囮のタイプを変更してみるとどうなるか？

などを検討していくことになりますが、もしかすると多数のハニーポットを集中的に管理するような仕組みの導入と運用を実施していくかも知れません。この手の仕組みは単一のサイトのみでデータを取得・解析したところで限界は見えていますし、今後は相関解析という方法論の中に組み込んでいくことも考えていくべきだと思うからです。ある面dshield.org（incidents.org）の試みに近いようなことを、多くのサイト間で連携しないと、この技術がセキュリティ確保に役に立つのか、ひいては「売れる技術」たりえるのか、というところまで議論が行かないでしょう。実は「売れる技術」と「売れる製品」というのは違うと思いますが。

いずれにしてもこのハニーポットという、（今のところ）売れそうも無いが十分に魅力的な素材を追いかけて、技術や知識のみならずさまざまな方面での知見を深めていければ、と考えています。

みなさんもぜひ一度、活動に参加してみてください。

第57回IETF参加報告

富士ゼロックス株式会社
稲田　龍

NPO日本ネットワークセキュリティ協会(JNSA)では、PKI相互運用技術WGとChallenge PKIプロジェクトを中心にして、PKI関連の問題を取り上げ、実際に使えるものにするための試行として、問題点の指摘と改善案の提案や議論などを、大元のIETF(Internet Engineering Task Force: http://www.ietf.org/)のPKIX-WGに対して行ってきている。この活動は、Challenge PKI 2001で得られた知見や成果をIETFの場で議論するべく、横浜で2002年7月に開催された第54回IETFミーティングのPKIX-WGで始めてプレゼンを行い、プライベートBOFも開催したことが発端になっている。この後、Challenge PKI 2002の作業を通して、2002年11月のアトランタの第55回IETF、2003年3月のサンフランシスコの第56回IETFとPKIX-WGでの発表を重ねてきた。2003年7月のウィーンで開催された第57回IETFでは、Challenge PKI 2002の派生物として、個人提案の形ではあるがインターネットドラフトの提出を行い、非常に注目された。この報告では、第57回IETFの概要を簡単にご紹介する。
尚、2003年11月にミネアポリスで第58回IETFが開催されており、ここでも先のインターネットドラフトをRFCにするための準備として、主要なメンバーのレビューを行ってもらうことをお願いしたり、内容についてのディスカッションなども個別に進めることができるようになってきている。これらの成果は、2004年3月のソウルで開催される第59回IETFで発表する予定なので、今後のことについては改めてご報告したい。

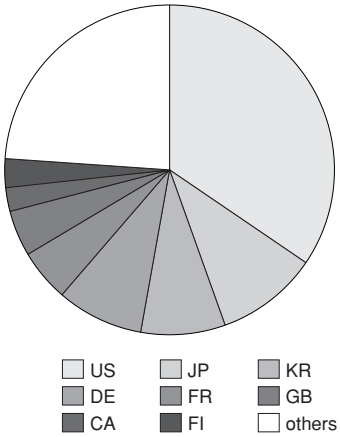
さて、2003年7月13～18日にオーストリアのウィーンのAustria Center Viennaにて開催された第57回IETFミーティングであるが、JNSAは2002年度に情報処理振興事業協会セキュリティセンター（略称：IPA/ISEC http://www.ipa.go.jp/security/）より委託を受けた事業であるChallenge PKI 2002プロジェクトの派生物であるInternet-Draft“Memorandum of Multi Domain PKI interoperability”（セコムトラストネット島岡政基氏著）に関しての島岡氏の発表と議論をPKIX-WGにて行う目的で、下記のメンバーで参加した。（敬称略、順不同）

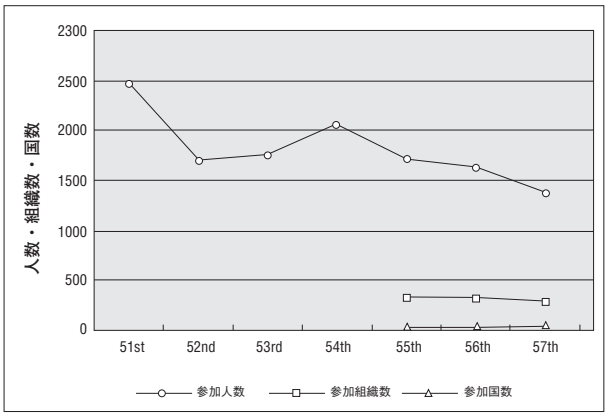
富士ゼロックス株式会社　稲田 龍、横田智文
セコム株式会社　松本 泰、漆島賢二
セコムトラストネット　島岡政基
ディアイティ(JNSA)　安田直義

■IETFの参加者

第57回IETFミーティングの参加者は48カ国から277の組織で、総勢1,331人であった。前回のサンフランシスコでの第56回が1,640名であり、アトランタの大55回が1,706名、横浜の大54回が2,064名、第53回のミネアポリスが1,756名であり、参加者数は減少傾向にある。日本と韓国、ドイツはほぼ同数だったが、米国からの参加者が大幅に減少している。同時テロ以前のロンドンで行われた第51回が2,457人であったことを考えると、米国でのITバブルの崩壊の影響は、いまだ強く残っている事が感じられた。

以下、第57回IETFで直接参加したPKIXでの議論と、関連するWGでのいくつかの議論を紹介する。少し専門的過ぎるかもしれないが、IETFの現場での議論を少しでもお伝えしたいので、いま少しお付き合いいただければ幸いである。





■ IETF/PKIX-WGの方向性

今回のIETFでは、WGチェアのSteve Kent/Time Polk両氏より「IESGの方針を受け、PKIX-WGはこれ以上新しいWorking Itemを増やさない」という方針が事前にアナウンスされた。また、この方針のため、今回のPKIX-WGのAgendaとして下記のような内容があげられている。

> 1.1 WG Focus and Direction [ADs]
>
> The working group has received direction from the IESG that will limit the types of new specifications accepted as PKIX work products.
>
> The ADs will present IESG's expectations for the PKIX WG along with the rationale. (15 min.)

これは、PKIX-WGが本来はインターネットにおけるX.509証明書を利用するための基盤技術を決めるためのWGであるにも限らず、ここ数年、PKIを利用したアプリケーションの必要性を受け、セキュリティエリアをはみ出した活動をしており、そのためにPKIの標準化および配備が遅々として進まない事を打開するためのIESGからの指示と受け取れる。

実際、IETFの他のWGにおいて認証およびセキュリティの仕組みとしてPKIを採用する例が増えておりそれらのWGでの議論とPKIX-WGでの議論が重複/対立を避けたと考えられる。

今回のPKIX-WGで、このAgendaをうけ、Security AreaのArea DirectorであるRuss Housley氏が上記の説明を行った。具体的にどういう活動を行うべきかに関してHousley氏は明言を避けたが、今後、PKIX-WGはこの方針を受けて活動を行うためPKIのインターネットにおける標準化活動は

1. PKIの利用に関しての基盤技術の確立（RFC3280の後継、証明書検証のための枠組み）
2. PKIを応用したプロトコル/アプリケーションの開発

の二つの流れにわかれ1をPKIX-WGが引き続き行い、2を他のWG/新設WGが行うモデルになると考えられる。

この状況は、数年前のIPv6 WGの状況に似ている。IPv6 WGもIPv6の基本プロトコルを制定後、運用、配備、ルーティングなど複数のWGを生み、IPv6の開発および配備を進めてきた。おそらくIESGの意図もIPv6と同様にPKIが基本部分の制定は終了し、今後、本格的な普及に向けた活動を行うことを意図したことと考えられる。

ミーティング終了後、チェアであるSteve Kent氏よりこの部分に関して以下の議事録がPKIX-WGのMLに投稿されている。

> WG Focus and Direction - Russ Housley
>
> The working group has received direction from the IESG that will limit the types of new specifications accepted as PKIX work products. Thus the WG is not accepting new work items.
>
> New WGs will be formed, as needed, to address PKI issues, or individual drafts can be submitted and subject to IETF-wide last call if the work described in them is mature and non-controversial. [no slides]

実際、現在のPKIX-WGでは、PKIの新たな利用に関してのInternet-Draftsも活発に投稿されており、これらの議論が活発になされれば新たなBOF/WGが形成されていく事は想像に難くない。次回、次々回のIETFにおいてPKIX-WGの活動および他のWG/BOFの動きをより注意深く観察し、今後のインターネットにおけるPKI利用の方向性を見定める事が重要と考えられる。

■ PKIX-WGでのInternet-Draftの発表

今回のIETF/PKIX-WGで、JNSAとIPA/ISECの名前で、セコムトラストネットの島岡政基氏がInternet-Draftの発表を行った。島岡氏は、JNSA Challenge PKI 2001/2002の中心人物の一人でありテストケース/テスト環境の設計、報告書の作成などを報告者と共に精力的に行ってきた。

JNSA Challenge PKI 2001/2002の活動を通じ、またアジアPKIフォーラムでの活動において島岡氏はいわゆるMulti Domain PKIに関しての定義が曖昧であり不要な誤解、理解の不足により相互接続性が阻害されていると感じた。そのため、いわゆるMulti Domain PKIに関しての状況を整理しまとめたInternet-Draft“Memorandum of Multi Domain PKI interoperability”を執筆した。
当初は、PKIX-WGのチェアであるSteve Kent氏（BBN Net）およびTim Polk氏（NIST）と相談の上、WG Draftとして公開する予定であったがIESGの方針によりPKIX-WGは、これ以上、Work Itemsを増やさない方針であるとのTim Polk氏の助言により島岡氏個人のPersonal Draftとして公開する事となった[1]。

Tim Polk氏との事前協議により、今回のPKIX-WGにて10分間の時間をもらい、島岡氏がこのInternet-draftを書く背景の説明と内容の説明を行い今後の予定などを発表した。

Title	: Memorandum for multi-domain PKI Interoperability
Author(s)	: M. Shimaoka
Filename	: draft-shimaoka-multidomain-pki-00.txt
Pages	: 16
Date	: June 2003

[1] PKI-WGの活動の方向性に関しては前節の「IETF/PKIX-WGの方向性」を参照のこと。

発表は、好意的に受け入れられた。特にTim Polk氏からは「非常によくまとまった発表であり、今後のRFC3280の後継のRFCに対しても反映したい」というコメントを付けていただいた。事実上、最大限の賛辞であり島岡氏のInternet-Draftが高く評価されたと感じた。おそらく、PKIX-WGがNo more New Work Itemの状態でなければ、文句なくWG DraftとしてPKIX-WGで（おそらくBCPもしくはInformational）RFCとして制定される道をとったものと思われる。

■ パス構築／パス検証に関して

PKIX-WGミーティング終了後、パス構築／パス検証に関してのInternet-Draftsを書いたMatt Cooper氏（Orion Security/draft-ietf-pkix-certpathbuild-00.txtの作者）と意見交換を行った。この意見交換ではMulti Domain PKIに関してのパス構築／パス検証に関しての扱い方と簡単な議論を行い、Matt Cooper氏と協力する事を約束した。後日、Matt Cooper氏と島岡氏でメールをやり取りし、より詳細なレビューを行っている。

■ IPv6アドレスの利用法に関して

IAB Open Plenaryにて、IPv6アドレスの利用に関して興味深い提言がなされた。

IPv6のアドレス体系は、IPv4アドレスでの反省の元に、以下の3つのアドレスを持っている。

1. Global Address
2. Site Local Address
3. Link Local Address

これらのアドレスはアドレススコープという概念の元にまとめられたものであり、各々、インターネット全体から見える、サイト(組織)内でのみ見える、ホスト内でのみ見えるというアドレス体系となっている。この「アドレススコープ」という概念は、IPv4に後付で取り入れられたいわゆるプライベートアドレス/グローバルアドレスの概念を整理/拡張したものである。

これらの「アドレススコープ」をどう使い分けていくべきであるかに関して、IABから以下のような提言がなされた。

1. Global Addressは、対外的なWeb Server/Mail Server/ルータ等全世界から見える必要があるサーバに割り当てる。
2. Site Local Addressは、組織内のデータ共有サーバやプリンタなど対外的に見せる必要はないが組織内では見える必要があるサーバに割り当てる。
3. Link Local Addressは、複数のインターフェイスを持つ場合で特定のインターフェイスに対してルーティングを行いたいなどといった場合に割り当てる。

IPv6対応の製品群は、家電などにも用いられるためセキュリティに対して種々の仕組みを持っており、このアドレススコープという概念もルーティング情報

の圧縮のためという側面と、「見せるべきもののみを見せる」という観点でセキュリティといえる(もちろん、この機能だけでは十二分でない事は明らかではある)。

稲田の所属する富士ゼロックスでも、コピー/プリンタのネットワーク接続を進めており、IPv6化も当然考えねばならない。そのときに、このアドレススコープに対しての対応と接続のために適したアドレススコープを選択できる機能は必須となる。

たとえば、SOHOオフィスなので使う場合は、SOHOオフィス内ではアドレスはSite Local Addressのみで運用されるかもしれない。その場合でもきちんと動作するコピー/プリンタが要求される。

また、単なるプリントエンジンとしてホストに接続する場合はLink Local Addressでの接続が要求されるであろう。等々、きちんとしたIPv6のアドレス体系/プロトコルの理解が要求される[2]。

■ NISTのS/MIME Test Suiteに関して

S/MIME WGのセッションにおいて、NISTのTim Polk氏がNISTで開発しているS/MIME Test Suiteに関して発表を行った。このTest Suiteは、特定のメールアドレスに対してS/MIMEメッセージを送るとそのS/MIMEメッセージの妥当性、正当性を評価しレポートするもののようである。

S/MIME WGの終了後、Tim Polk氏とNIST版S/MIME Test Suiteの構成と日本語に対するサポートの状況を問い合わせたところ、できる限りのサポートをしていただけることとのことであった。Tim Polk氏より、7/21の週にリマインダーとして具体的な依頼事項を記述したメールがほしいとのことであったので次のようなメールを送った。

問い合わせを行った内容は、

1. このTest Suiteのソースコードが公開される予定があるか?
2. 公開されるのなら、ソースコードを変更しChallenge PKI 2002の成果物であるGPKI Test Suiteに同梱して配布してかまわないか?

の2点である。

JNSAは第55回IETF、第56回IETFのPKIX-WGにてChallenge PKI 2001/2002の発表を行っており、Tim Polk氏にはその成果物としてGPKI Test Suiteを公開した事を報告してある。また http://www.jnsa.org/mpki/にてChallenge PKI Projectの成果物を公開している事を知らせてある。これらに関してもTim Polk氏は高く評価してくれている。

■ Challenge PKIへのお誘い

さて、紙数も尽きてきたので、まだまだお伝えしたいことはあるが、標準を作る話の常としてかなり専門的な議論となっているので、Challenge PKI Projectとしての第57回IETFでの議論はこのくらいで終えておこう。この後、2003年11月のミネアポリスでの第58回IETFでは、冒頭で述べたように更に中核人物との連携が実現できた。このような準備ができたので、2004年3月ソウルで開催される第59回IETFでは、Internet-DraftのRFC化を更に進める予定で準備している。

また、2003年11月末にIPA/ISECの課題として報告書を作成している、タイムスタンププロトコルに関する報告書と、アプリケーションAPIに関する報告書の成果を加えて、更にPKIの実運用環境で必要とされる技術標準を考えていきたいと考えている。もしご興味とアイデアをお持ちであれば、ぜひご連絡いただきたい。より広い知見を集められればより良いものになると思うので、ご指導ご協力を賜れるようお願いしたい。

[2] IPv6のアドレスは、通常はNeighbor Discovery Protocolと呼ばれるプロトコルでDHCPのようにアドレス情報を取得する。その際に、悪意のあるNeighborより妨害情報をもらわないようにするための枠組みもSEND(SEecurely Neighbor Discovery) WGで議論されPKI技術の導入も検討されている。

会員企業ご紹介⑨

株式会社網屋
(http://www.amiya.co.jp/)

AMIYA
IT Consulting
&
Project Management Services

株式会社網屋は、1996年12月にITConsulting & Project Management事業をキーワードに、お客様によりハイクオリティなビジネス環境をご提供することを目的とし設立致しました。
昨年に入りましてからリスクマネージメントの運用を急務とする日本のお客様のニーズに合致した、情報セキュリティ監査ツール『bv-control』の日本語対応版リリースに向けて開発を開始し、今年の7月に販売を開始致しました。既に大型案件の導入も行った経験上、単なる製品販売だけでなく以下のようなセキュリティ診断サービスもお客様にご提供することが可能になりました。

御社のWindows環境のセキュリティ状況を調査します
Windows Security Check Service

情報セキュリティ意識の高まりにより、サーバ・ネットワーク装置のセキュリティ対策は進みつつありますが、最も脆弱となりやすくチェックを必要とするのは従業員のデスクトップPCです。
従ってデスクトップPC内を調査し、効果的な対策を行うことで企業全体の脆弱性を無くすというセキュリティ対策こそが、今最も企業に必要とされる「デスクトップセキュリティマネージメント」という考え方です。
『Windows Security Check Service』は、マイクロソフトが推奨するセキュリティ基準を満たした状態になっているかを調査します。
『Windows Security Check Service』は、弊社が国内販売をおこなう米国BindView社の情報セキュリティポリシー監査ツール『bv-Control』を使用しています。

『Windows Security Check Service』の特徴

■アプリケーションをサーバやクライアントにインストールする必要が無いため、システムへのインパクトを心配することなく、すぐに調査が可能です。

■項目例

【OSの脆弱性によるセキュリティ事故を防ぐ】
・最新の Service Pack インストールの有無調査

【簡単に破られるパスワードを使わせない】
・極めて脆弱なパスワード利用ユーザの調査

【安定したディスク環境を保つ】
・ハードディスクの利用状況の調査

【情報漏洩のルートを減らす】
・リスクの高いアプリケーションのインストール状況の調査

お問い合わせ先
株式会社網屋
E-Mail：bv-info@amiya.co.jp
TEL：03-5643-1331　FAX：03-5643-1334
〒103-0014　東京都中央区日本橋茅場町1-2-3
ルート蛎殻町第二ビル

株式会社インテリジェント ウェイブ
(http://www.iwi.co.jp)

INTELLIGENT WAVE INC.

株式会社インテリジェント ウェイブは1984年の創業以来、金融関連に特化し銀行系カード会社や大手証券会社などをクライアントにもつ独立系ソフトウェア会社です。
自社開発パッケージによるクレジットネットワークシステムおよび集配信システムの提供では国内70％のシェアを占め、さらにカード不正検知システム等でセキュリティ分野へも積極的に展開しており、2003年11月には内部情報漏洩・内部犯罪監視システム「ＣＷＡＴ」の発売を開始しております。

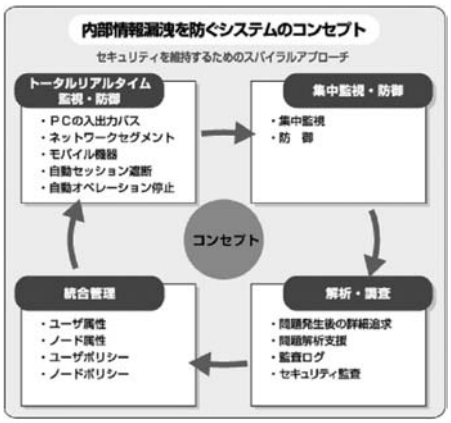
■ 主な事業内容
●カードビジネスのフロント業務　●ディーリング・トレーディング業務及びパッケージの製造・販売・技術支援
●カードビジネスのバック業務　●セキュリティシステム業務　●消費者向けパッケージ販売

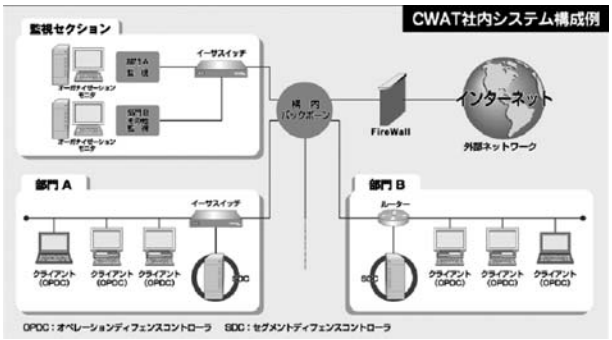
■内部犯罪を防ぐ統合監視システム「CWAT」
現在、多くの企業では外部からの犯罪に対して、FirewallやIDS（不正侵入検知システム）の導入で対応していますが、急激に増加しつつある内部情報漏洩・内部犯罪に対しては、ほとんどの企業が未対応な現状です。
最近の個人情報流出事件などの殆どは、内部情報漏洩・内部犯罪であり、緊急な対処を必要としています。
これまで、内部犯罪に対しては「本人認証機能」と「アクセス管理機能」が有効と考えられてきましたが、権限者が行う内部犯罪が増加するにつれ、これらの機能だけで内部情報の漏洩は防止出来なくなっています。
弊社の「CWAT」は、ネットワークと端末上操作の両方を不正挙動と特異挙動の観点から監視し、集中監視制御を実現することにより、内部犯罪を強固に防ぎます。

【CWATの特徴】
●特異挙動の監視
普段の行動を学習することで、通常と異なる行動を検知し、アクセス権限者であってもその操作を監視し不正利用の疑いがある場合は通知します。
●外部接続デバイス監視
ネットワーク上を流れる情報を監視するだけでなく、個々端末の使用状況や外部接続バスを監視し、不正利用を通知・禁止します。
●不正挙動の監視
ユーザやノードの属性情報も含めた細かなポリシー設定が可能で、ポリシー違反に対処することが可能です。
●モバイル機器の監視
モバイルPCに対応し、盗難や、持出し中の不正な操作など、様々な犯罪ケースに対応できます。

監視については、全ての監査ログに強固な暗号化を施された後に記録され、改竄等を防ぎます。又、ログのフィルタリング及びサンプリング機能を持っているため、リソースコストを抑えながら、柔軟に監査対応する事が可能です。全ての監視・防御については、統合管理コンソールよる集中管理が可能となっています。

【CWATのシステム構成】





お問い合わせ先
株式会社インテリジェント ウェイブ 営業本部
〒135-0042
東京都江東区木場5-12-8　木場グリーンパークビル
Tel:03-5620-1051 Fax:03-5620-1060
e-mail:cwatsales@iwi.co.jp

監査法人トーマツ エンタープライズリスクサービス部

(http://www.tohmatsu.co.jp/services/ers)

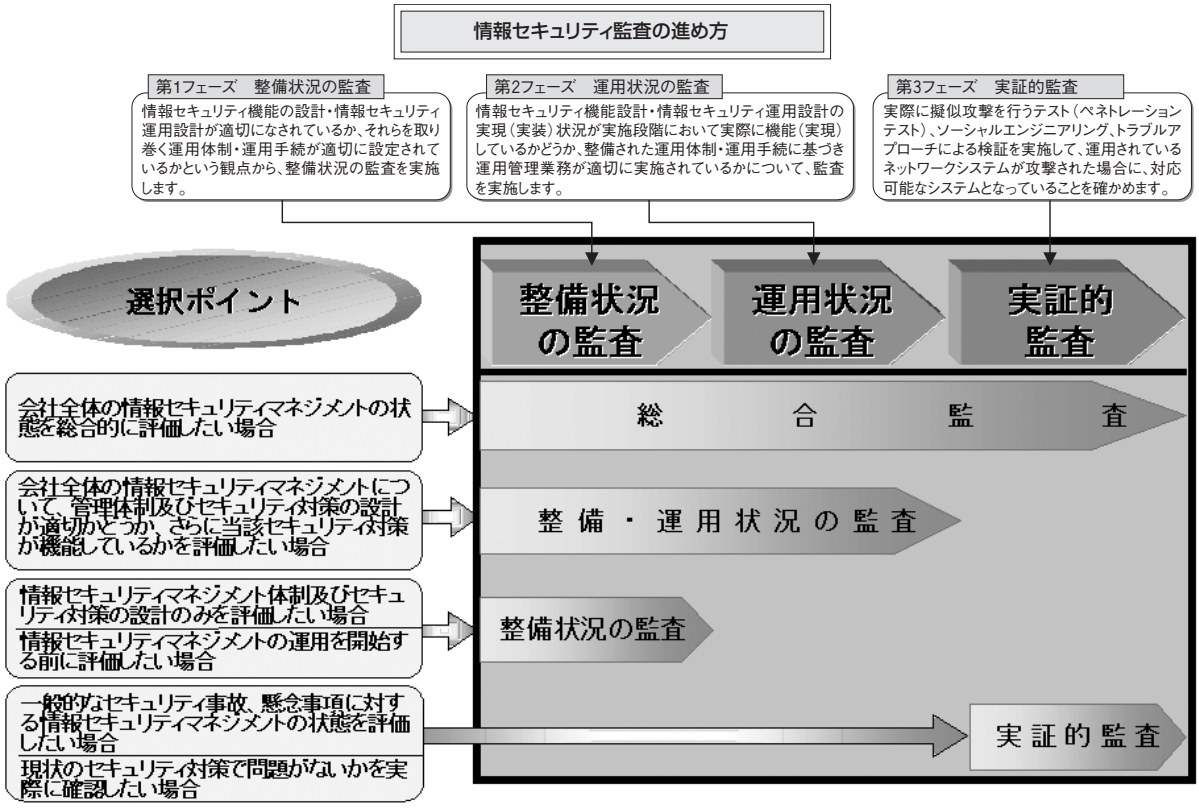
監査法人トーマツは、日本初の全国規模の監査法人として1968年に創立されました。以来、監査等の証明業務やアドバイザリー業務、税務、コンサルティングサービスを提供しています。エンタープライズリスクサービス部では、情報リスクマネジメントの観点から企業組織、情報、業務、テクノロジー、財務に関わるリスクを識別し、リスクとその管理に関わる総合的な監査やコンサルティングサービスを提供しています。

主なサービス内容

- 情報セキュリティ監査
- 情報セキュリティ方針・スタンダードの作成支援
- ＩＳＭＳ（ＢＳ７７９９を含む）の導入支援
- ＩＳＭＳ（ＢＳ７７９９を含む）の認証取得支援
- ネットワーク・セキュリティの評価・診断
- インターネット侵入によるセキュリティ検証
- プライバシーマーク取得支援
- WebTrustマーク取得支援
- 公開鍵インフラ（ＰＫＩ）の導入支援
- 電子認証局の監査 等

情報セキュリティに関するサービス

インターネットの普及によって、情報セキュリティリスクマネジメントが喫緊の課題となっています。情報セキュリティを確保し、ビジネス戦略を成功裡に推進しなければなりません。トーマツは、情報セキュリティ強化により貴社のeビジネスを成功に導きます。



お問い合わせ先

監査法人 トーマツ エンタープライズ リスク サービス（ERS）部

東京・本部　〒100-0005　東京都千代田区丸の内3-3-1　新東京ビル
TEL 03-6213-1112　FAX03-6213-1117

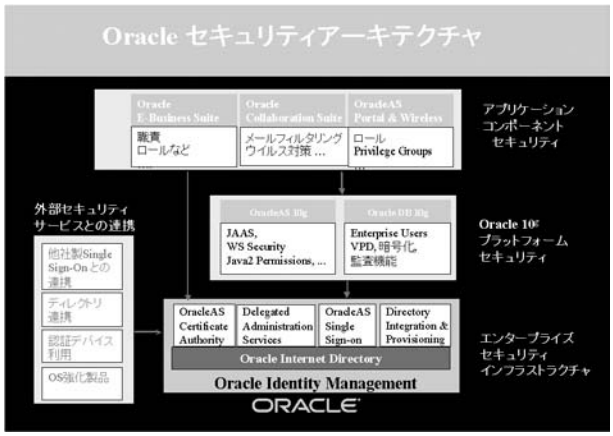
名古屋事務所　〒450-0002 名古屋市中村区名駅3-13-5
名古屋ダイヤビルディング3号館 TEL 052-565-5511

大阪事務所　〒541-0052 大阪市中央区安土町2-3-13　大阪国際ビルディング
TEL 06-6262-4558

福岡事務所　〒810-0001 福岡市中央区天神1-10-24　福岡三和ビル
TEL 092-751-0931

日本オラクル株式会社
(http://www.oracle.co.jp)

日本オラクル株式会社では2003年10月、Oracle Database 10g,、Oracle Application Server 10gを発表致しました。(2004年1月出荷予定)オラクルでは顧客が保有する最も価値の高い情報資産の多くはデータベースに格納されていることから、データベースでの情報保護対策が非常に重要であると考えています。またシステムと顧客規模が大きくなってくるとユーザ認証・アクセス制御・ユーザ管理が一元的かつ合理的に行われなければならなりません。オラクル製品にはさまざまな形でセキュリティ機能・オプション製品等が実装されており、情報保護のために利用できます。



1．データベースでのセキュリティ対策

(1)仮想プライベートデータベース

従来リレーショナル・データベースではオブジェクト(表・ビューなど)の単位でしかアクセス権限を制御できませんでしたが、オラクルでは仮想プライベートデータベース(VPD)を使うことにより行レベルでのアクセス制御を行うことが可能です。この機能はアプリケーション・コンテキストを利用することによって、オブジェクトを共有しているWebアプリケーションのユーザに対してもアクセス制御ができます。

(2)格納データの暗号化

データファイルの盗難などに備えて、機密性の高い情報については各表の列単位で暗号化を行い、更にハッシュ関数を使った改ざん検知などの仕組みを実装することができます。

(3)通信データの暗号化(Oracle Advanced Security)

データベースサーバとクライアント、またはアプリケーションサーバとの間の通信経路上における盗聴対策としてOracle Advanced Security(オプション)を使うことで通信データの暗号化が可能です。

(4)ファイングレイン監査

従来の監査機能に加えて、更に詳細な監査ポリシーを設定して監査を実施することができます。さらに監査動作を行った後、任意の動作(管理者にメール通知を行う等)をプログラムできます。

2．アプリケーションサーバを使ったユーザ認証とディレクトリ管理

(1)シングルサインオンとディレクトリ管理

Oracle Application Server 10gではそのコンポーネントとしてOracle Single Sign-on Server、Oracle Internet Directory、Oracle Certificate Authorityを実装し、配下のWebアプリケーションに対するシングルサインオンとアクセス制御を実施します。また従来のパスワード方式だけでなく、ディレクトリにデジタル証明書をインポートし、クライアント証明書を使ったSSLクライアント認証・シングルサインオンを実現することが可能です。これによりICカードなどの認証デバイスやPKIを使った認証基盤に対して高い親和性を発揮することができます。

(2)他社製品との連携動作

Oracle Single Sign-on Server、Oracle Internet Directoryはユーザの既存のシングルサインオンサーバ製品やディレクトリサーバとも相互に連携しながら導入を進めることが可能です。

3．セキュリティ評価・認証について

セキュリティに関する社会的関心の高まりとともに各種のセキュリティ関連国際標準が制定されています。オラクルではお客様にセキュリティ機能を安心して お使い頂けるようISO/IEC 15408(Common Criteria)EAL4、FIPS-140-1など合計17の各種国際標準のセキュリティ評価・認証を取得しています。

お問い合わせ先
日本オラクル株式会社
〒102-0094　東京都千代田区紀尾井町4-1
ニューオータニガーデンコート
Oracle Direct TEL：0120-155-096
URL：http://www.oracle.co.jp/contact/

株式会社ネットマークス
(http://www.netmarks.co.jp)

NETMARKS

株式会社ネットマークスは、メーカーにとらわれることなく時代に即したネットワーク構築というニーズの高まりを背景に、マルチベンダ環境でのネットワークシステムインテグレータとして1997年に設立いたしました。
ネットマークスでは、『We are here on customer's side.』をスローガン掲げ、お客様の立場で考えた最適なソリューションと誠実できめの細かいサービスを提供することを目指しております。

最新技術にも柔軟に対応するネットワークシステムの構築をベースに、重要な情報を確実に守るセキュリティシステム、データを安全に保管し最大限に有効活用するためのストレージネットワークシステム、また構築したシステムの運用・監視を行なうアウトソーシングサービスの4つのソリューションを基幹ビジネスと位置付け、これらを融合させ、設計、構築、運用・監視、保守にいたるまでトータルにお客様をサポートしております。
ネットワークセキュリティについては、最新の技術を取り入れたインターネットVPNシステムやエンドポイントセキュリティ、マルチデバイス認証など幅広いセキュリティソリューションをご提供しております。また、お客様におけるコストや人員を最小限に押さえるためのアウトソーシングサービスなども提供しております。
今後も、常にネットワークインテグレーション業界をリードし、グローバルな視野に立った企業を目指してまいります。

＜代表的なセキュリティソリューション＞

・高速ファイアウォールソリューション
インターネットの普及に伴うユーザ数や通信データ量の増加によりボトルネックとなりやすいファイアウォールの負荷分散を実現したソリューションです。アプリケーションレベルでの帯域制御やリアルタイムでのアクセスコントロール設定が可能なアプライアンスサーバの組み合わせで、強固なセキュリティを実現することが可能です。

・マルチデバイス認証ソリューション
アプリケーション、ネットワーク、OSへのログオン時などにおいて、指紋、虹彩等の生体情報とICカード、USBトークン等を組み合わせ、認証を行ないます。個々の認証デバイスの欠点を補完し、より強固で柔軟性のあるシステムを構築できます。

・セキュリティアウトソーシングサービス
『SecurePlanet』
セキュリティシステム構築後の運用や監視も非常に重要です。ネットマークスの提供する「SecurePlanet」は、運用・監視・保守とトータルにサポートを行い、高い信頼性・安定性・効率性を提供するセキュリティアウトソーシングサービスです。システムの認証代行、外部・内部からの不正アクセスやポリシー違反などの運用・監視をお客様に代わってセキュリティのエキスパートが24時間365日行い、トラブル発生時には迅速に対応します。


＜運用・監視センター＞

お問い合わせ先
株式株式会社ネットマークス　広報宣伝室
〒107-0051　東京都港区元赤坂1-3-12
TEL 03-3423-5782　FAX 03-3423-5902
E-Mail info@netmarks.co.jp

株式会社日立製作所
(http://www.hitachi.co.jp/secureplaza/)

日立のトータルセキュリティソリューション　―Secureplaza―

企業情報システムの進化が加速する一方、インターネットが企業の基幹ネットワークの役割を担う時代となってきました。こうしたなか、不正アクセスやコンピュータウィルス、情報漏えいなどのセキュリティトラブルが飛躍的に増加しています。日立は、グループ全体でトータルセキュリティソリューション「Secureplaza」において、多岐にわたるセキュリティ対策を、実際のシステムやサービスの広がりに即した９つのステップで提案する「ステップ別ソリューション」と、お客様の導入目的に合わせた製品／サービスをパッケージ化した「目的別ソリューション」という２つのソリューションでハイレベルなセキュリティ維持に貢献します。

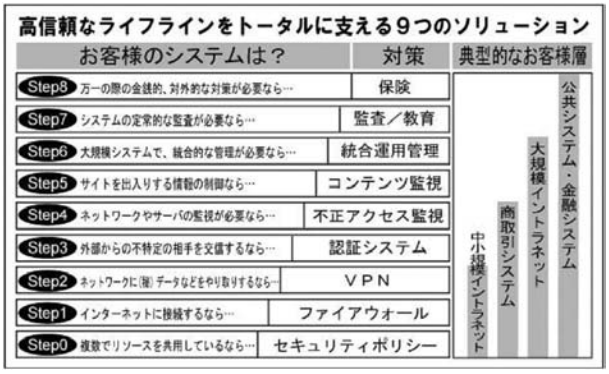
■セキュリティ対策を適切コストでスピーディに実現

セキュリティの脅威は、自社の損害だけでなく、企業としての信頼を著しく失墜させる危険性を秘めています。コーポレートガバナンスの観点からも、情報セキュリティが企業のビジネス資源となる時代、信頼度の高いビジネスを実現するには、確固たるセキュリティポリシーの策定と、外部からの攻撃を遮断し、内部の情報を確実に保護するトータルなセキュリティ対策が不可欠です。

日立の「Secureplaza」は、セキュリティの脅威からお客様のビジネスと信頼をプロテクトするため、豊富なソリューションメニューをご用意しています。

■ステップ別ソリューション

ステップ別ソリューションではシステムやサービスの広がりに即して考慮していくべきセキュリティ対策を、大別して９つのステップで構成しています。



Secureplaza ステップ別ソリューション

■目的別ソリューション

お客様の導入目的に合わせたソリューションをパッケージ化した目的別ソリューションをご紹介します。

◇Secureplaza/HS(Healthcare Service)

お客様のシステムをホームドクターのコンセプトで診断・管理します。セキュリティ状況を総合診断し、対策事項を的確にご提案すると同時に、システムの常時監視・運用、改善策の提言までお客様に代わってトータルにご支援します。

◇Secureplaza/IM(Identity Management)

PKI（公開鍵基盤）を実現する認証基盤システムをはじめ、署名法対応/GPKI相互認証対応、電子署名/タイムスタンプ、ヒステリシス署名、属性認証等最先端のソリューションを提供します。

◇Secureplaza/LG（Leak Guard）

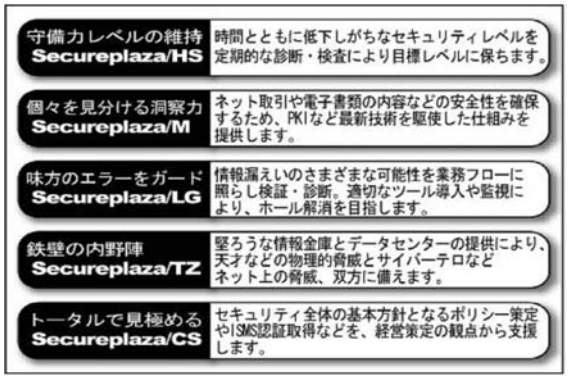
５W1Hの考え方で、「いつ・どこで・誰が・何の目的で・どうやって・何の情報が」漏えいするのかをトータルに診断・分析。情報漏えいルートやリスク分析結果に基づき、幅広いツール群の中から最適な情報漏洩防止ソリューションを提案します。

◇Secureplaza/TZ（Trusted Zone）

個人情報データ等、お客様の情報資産の中でも特に機密性の高いものを、物理的脅威、サイバーの脅威両面から保全します。また、外部からの不正PCの持込によるウィルス感染を防止するネットワークガードのソリューションも提供します。

◇Secureplaza/CS（Consultation Service）

セキュリティポリシーの策定からISMS認証取得、ISO15408対応セキュアシステム構築、個人情報保護法対応等幅広いコンサルティングメニューを提供します。



Secureplaza 目的別ソリューション

お問い合わせ先
株式会社日立製作所
情報・通信グループ
セキュリティソリューション推進本部
info-sec@system.hitachi.co.jp

JNSA会員企業情報

JNSA会員企業の製品・サービス・イベント情報です。

■製品情報■

○RADIUSサーバソフトウェア『fullflex EG』

企業・団体内でのユーザ認証に適した、多用途のRADIUSサーバソフトウェアが誕生しました。
操作ガイドつきのわかりやすいウェブGUIで、専門知識不足でも管理可能。IEEE802.1Xに対応し、ダイヤルアップの他、無線LANや認証VLAN等でもユーザ認証を行います。外部DBやワンタイムパスワードシステムとの連携も実現。
価格：25万円（50ユーザ）～150万円（3,000ユーザ×2）
http://accense.com/products/eg/

◆お問い合わせ先◆
株式会社アクセンス･テクノロジー
E-MAIL：sales@accense.com
TEL　：03-5206-7740

○「DataClasys」（データクレシス）

「DataClasys」（データクレシス）は極秘や社外秘などで管理をしている紙媒体の文書管理をデジタルファイル・データでも実現します。ISMSやBS7799などの情報セキュリティ認証基準にも対応できます。機密性の高いデジタルファイル・データを機密情報管理ポリシー策定、システム設定、監査までを一貫してサポートする初めてのデジタル文書管理・暗号システムです。
http://www.ahkun.jp/dataclasys/index.html

◆お問い合わせ先◆
株式会社アークン　プロダクト事業本部営業部
E-MAIL：info@ahkun.jp
TEL　：03-52946065

○秘密分散法応用の新製品
ＴＡＳ（Threshold Authentication Scheme）

東京大学との共同研究による認証スキームＴＡＳを12月より販売開始しました。
暗号鍵など秘匿情報をリスク分散して送付するシステム、従来難しかった再配布や追跡性の機能を持った電子チケットシステムの構築などに応用出来ます。情報家電や携帯電話などの各種ユビキタス環境で広くお使い頂くことが可能です。
http://c4t.jp

◆お問い合わせ先◆
株式会社シーフォーテクノロジー

○McAfee IntruShield

高精度IDS/IPS製品「McAfee IntruShield」は、ネットワークへの侵入をリアルタイムに検知、防御するアプライアンス製品。不正侵入やDDoSを検知するだけでなく「防御」も可能。シグネチャ分析とアノマリ分析を組み合わせた高精度検知ロジックや2ギガbpsの大量高速処理（最高機種の場合）、高い検知率などを誇り、数々の賞を受賞。価格は132万円から。
http://www.nai.com/Japan/products//intrushield.asp

◆お問い合わせ先◆
日本ネットワークアソシエイツ株式会社
TEL　：03-5428-1104

○Web認証ソフト WisePoint

日本語パスワードや乱数表を用いて本人認証を行う事でWebシステムの認証強化を実現。その他ポータル、アクセス制御、SSO機能も1パッケージで提供。既存のWebシステムを殆ど変更せず、低コスト・短期間で導入でき、企業合併や自治体統合時に既存リソースを用いて迅速に事業開始が可能。
本年9月、ＴＭＴマシナリー様にて事業統合時におけるIP–VPN網のセキュリティ確保に採用。
http://wisepoint.jp/

◆お問い合わせ先◆
ファルコンシステムコンサルティング株式会社 マーケティング本部
E-MAIL：sales@falconsc.com
TEL　：03-5452-0712

○HP Compartment Guard for Linux

Linux用に国産初の商用セキュアOSを提供しています。価格は1CPUにつき一律10万円です。機能の詳細は、下記Webをご覧ください。無償評価版もWebからダウンロードできます。
http://www.hp.com/jp/hpcg/

◆お問い合わせ先◆
日本ヒューレット・パッカード株式会社
E-MAIL：CGLX-INFO@security.jpn.hp.com

■サービス情報■

○御社のデスクトップセキュリティを診断！
『Windows Security Check Service』を開始

本サービスは御社のシステムにひそむ脆弱性や社員によるセキュリティ違反を洗い出し、どのような対策を取ればよいのかを考えるための指針となる情報を提供いたします。
●診断はマイクロソフトが提唱するセキュリティチェックリストに準拠
●調査時のシステム担当者への負荷や御社システムへのインパクトもほとんどなし
●そのまま経営者様や株主様に渡しても結果が理解できる、分かりやすい報告書をご提供

『Windows Security Check Service』の詳細はこちら
http://www.amiya.co.jp/service/wsc01.html

◆お問い合わせ先◆
株式会社網屋
お問い合わせフォーム：
http://www.amiya.co.jp/contact/inq01.html
E-MAIL：bv-info@amiya.co.jp
TEL　：03-5643-1331（担当：宮地）

○『不正PC検出サービス』

企業内ネットワークに接続されるクライアントPCを24時間365日体制でネットマークスの運用・監視センターから監視、無断でネットワークに接続される不正なクライアントPCを検出し、システム管理者に通知するアウトソーシングサービスです。これらのクライアントPC情報は資産管理データベースとして活用できるため、システム管理者が従業員に対して行なう調査や集計など、管理作業を軽減します。
http://www.netmarks.co.jp/prdct_srvc/prdct_info/service/index.html

◆お問い合わせ先◆
株式会社ネットマークス　マネージメントサービス事業部
E-MAIL：info@netmarks.co.jp
TEL　：03-3423-5941

○ソフトウエア開発のセキュリティなら「TRUSNET」

主なサービスとして、下記がございます。
⑴カスタムソフトウエアセキュリティ支援
・WEBアプリケーションの脆弱性を発見するスキャニング診断
・より根本的な脆弱性を発見するソースコード診断
・脆弱性を未然に防止する設計・開発コンサルテーション
⑵セキュアプログラミング　セミナー
http://www.trusnet.com/

◆お問い合わせ先◆
セントラル・コンピュータ・サービス株式会社
セキュリティソリューション部
TEL　：03-5626-7738
FAX　：03-5626-7763

○「Ultimate Hacking：ハッキング実践と対策スクール」

伊藤忠テクノサイエンス(株)は、アイ・ディフェンス・ジャパン社との協業により、過去3回開催し、大好評をいただいております、「Ultimate Hacking：ハッキング実践と対策スクール」の第4回目開催日程を2004年2月3日～6日に決定いたしました。
米国FoundStone社により世界各地で開催されている本コースでは、様々なハッキングや攻撃手法について、講義のみならず実習を通じて、実践的な防衛テクニックを学んで頂けます。
http://www.idefense.co.jp/service/ultimate/index.html

◆お問い合わせ先◆
伊藤忠テクノサイエンス株式会社
ネットワーク＆セキュリティ営業推進部　吉武(よしたけ)
E-MAIL：ctc-ns@ctc-g.co.jp
TEL　：03-5226-2652

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

SEA/J情報セキュリティ技術認定コース
『基礎コース(2日間)』　1月28日～29日、3月3日～4日
【概要】セキュリティのスキルマップ項目に対応した基礎知識を習得
情報セキュリティ対策支援トレーニング
『ネットワークセキュリティ総合コース(6日間)』
3月17日～19日、24日～26日
【概要】システム管理者に必要な専門的なセキュリティ知識を習得
http://www.hucom.co.jp/service/education.html#traning_hl

◆お問い合わせ先◆
株式会社ヒューコム　SMS事業本部
E-MAIL：sea-j@hucom.co.jp
TEL　：03-5306-7339

■イベント紹介■

『HPオラクル セキュリティ・センター』を、日本オラクル、日本ネッテグリティ、ネット・タイム、日本HPの4社で開設しました。ここではオラクルソフトウェア環境上でのセキュリティの検証や他のセキュリティ環境との相互運用や接続を検証します。このたび開設記念として、ICカード、アクセス制御、ディレクトリ、SSO、データベースまでの統合的なアイデンティティ・マネジメントのデモとセミナーを1月16日に開催します。
http://www.hp.com/jp/security

◆お問い合わせ先◆
日本ヒューレット・パッカード株式会社
E-MAIL：info@security.jpn.hp.com

NSF2003セミナー・レポート

2003年のNetwork Security Forum (NSF2003)は、10月22日から24日にかけて、東京ビッグサイトで開催され、延べ約300人の参加があった。プログラムは、22日にセキュリティー論文の審査と発表、23日は各界の有識者を集めたパネルを中心に据え、24日は主に技術的なテーマについてのセミナーを行った。次にこれらの内容を簡単にご紹介する。

22日『セキュリティー論文審査・表彰式』

今年初めての試みとして、日本セキュリティ・マネジメント学会(http://www.jssm.net/)との共催で、セキュリティ論文募集を行った。ネットワークセキュリティは、技術、管理・運用、法制度、モラル等を含めて対応する必要があり、今のような時期に、ネットワークセキュリティに関する研究を深め、いろいろな立場からの議論を行い、共通認識を形成していくことが重要であるとの考えから、論文審査を行うこととした。

A4で20ページとかなりまとまった分量の論文を募集したため、応募件数は11件と少なかったが、どれも力作ぞろいで高度な内容の論文が集まった。審査基準は、客観性を持ったテーマで、かつ下記のようなセキュリティ啓発に資する内容を持ったものとした。

- 斬新なアイディアをまとめたもの
- 技術的な標準化などに関する試案や提言
- 社会基盤に関する施策などに関する提言
- 技術者・ユーザ教育の普及啓発に関する実践や試行
- 技術と法律や運用などに関する相互関連
- その他、情報セキュリティに関するチャレンジ性

審査委員は、下記の先生方にお願いした。

- 辻井重男先生　(中央大学：JSSM会長)
- 石田晴久先生　(多摩美術大学：JNSA会長)
- 内田勝也先生　(中央大学)
- 佐々木良一先生　(東京電機大学)
- 塚本克治先生　(工学院大学)

厳正な審査を行い、下記の受賞論文が選考された。

1．最優秀賞　該当なし

2．優秀賞　2点(賞金各々10万円)

(1)プロセス実行履歴に基づくアクセスポリシー自動生成システム
　原田季栄氏／株式会社NTTデータ 技術開発本部

(2)日米欧の暗号技術標準化・評価プロジェクトを終えて
　神田雅透氏／NTT情報流通プラットホーム研究所

3．学生奨励賞(賞金5万円)

DRM機能を持つ決済システムについて
　天野光司氏／工学院大学(修士2年)

4．奨励賞(2点)

(1)大規模ネットワークセキュリティの確保に向けた研究開発
　福田尚弘氏／松下電工株式会社

(2)情報セキュリティ・マネジメントの制度設計
　田中秀幸氏／東京大学社会情報研究所
　松浦幹太／東京大学生産技術研究所 大学院情報学環

5．佳作(6点)

(1)IT利活用推進のための情報セキュリティマネジメントシステム構築および運用について
　大宮則彦氏／南山大学総務部事務システム課

(2) 情報セキュリティ分野における産学連携の状況
　江波戸謙氏／東京大学大学院情報学環・学際情報学府
　松浦幹太／東京大学生産技術研究所 大学院情報学環

(3)楕円曲線上の鍵分割構成による、同報暗号と鍵管理システムの検討
　扇裕和氏／株式会社メビウス

(4) セキュア社会実現へ向けての7つの提言
　ー安心と信頼に支えられたIT社会実現のためにー
　黒川信弘氏／松下電器産業株式会社

(5) 安心して暮らせる社会構築のためのセキュリティ戦略とドライバーウエアの提案
　武藤佳恭氏／慶應義塾大学環境情報学部

(6) デジタルデータの分散バックアップ方式の提案
　半田富己男氏／大日本印刷株式会社ビジネスフォーム事業部

更に、会員から下記のスポンサー賞をご提供いただいた。

- シスコシステムズ株式会社
  54M 802.11g　54Mブロードバンドルータ＋カード
- 株式会社ディアイティ

AP600G + ABGコンボカード
802.11a/b/g AP + カード
- マイクロソフト株式会社
  Windows 2003
- 株式会社大塚商会
  1 GB USBメモリー(USB2.0)8倍速、
  セキュリティソフト添付
- 日本ネットワークアソシエイツ株式会社
  ジバンシー高級ボールペン
- 株式会社シマンテック
  高級皮製システム手帳(3セット)
- サン・マイクロシステムズ株式会社
  Sun Developer Connection カバン

セキュリティー論文審査は、引き続き来年も実施することを計画している。今年出し損ねた方々も、来年は是非奮ってご応募いただければ幸いである。

23日 テーマ「e-Japan」

パネル1
「日本のインシデント対応体制」

社会インフラとしてのインターネットを強くする、と題して、政府、ISP、ベンダは何をすべきか、何をしてはならないか、という内容で、政府、ISP、セキュリティー組織、ITベンダー6人のIT関係者から報告するパネル・ディスカッションが行われた。冒頭、日本におけるインターネット・セキュリティーとインシデント対応体制の現状を、モデレーターの山口英氏(奈良先端科学技術大学院大学・情報科学研究科・教授)は「インターネットは生活に密着したインフラになっている」と指摘。セキュリティー強化には規制と法制、保険とリスク評価、司法機関と

警察、システム構築、オペレーターとISP、セキュリティー団体、エンド・ユーザー・システムといった多くの要素が関係するので、パネラー構成も多様になっていると説明した。

政府の立場からは、山崎琢矢氏(経済産業省・情報セキュリティー室・課長補佐)、BlasterやSobig-Fの攻撃を受けたISPとしてNTTコミュニケーションズの小山覚氏(IPインテグレーション事業部)、マイクロソフトアジアリミテッドの奥天陽司氏(セキュリティレスポンスチーム)、JPCERTコーディネーションセンター(JPCERT/CC)の山賀正人氏、産業技術総合研究所の高木浩光氏(グリッド研究センター・セキュアプログラミングチーム長)、それにISO/IEC 17799(セキュリティー・マネージメント)を審議中のパリからテレ・カンファレンスで参加した日本ヒューレット・パッカードの佐藤慶浩氏(セキュリティ・コンサルティング部・部長)によってディスカッションされた。

詳しくはJNSAのWebページを見ていただきたいが、締めくくりにあたって、山口英氏は「デベロッパーとユーザーの声が日本のインターネット・セキュリティーを高めていく原動力になるだろう」との総括を述べている。

パネル2
「セキュリティホールに関する法制化の諸外国状況報告と日本における提言」

このパネルは、情報ネットワーク法学会(http://www.in-law.jp/)の協力により実現した。経済産業省のセキュリティー脆弱性に関する6か国の法制度調査を行

った「経済産業省セキュリティホールに関する法律の諸外国調査委員会」のメンバーによる調査結果の解説が行われた。

当日配布された「『セキュリティホールに関する法律の諸外国調査』報告書」によれば、調査対象となったのはアメリカ、カナダ、イギリス、フランス、ドイツ、大韓民国の6か国。アメリカとイギリスはコモン・ロー(英米法)、フランスとドイツは大陸法の法体系になっているのが特長だ。調査は、質問事項を列挙したフォームを相手国法律事務所などに送付し、それに対する回答をまとめるという方法で行われている。

パネルで報告された内容はJNSAのWebページを見ていただきたいが、セッションの最後に、コーディネーターの高橋氏が調査委員会を代表して、日本での法整備について、画一的法規制よりも分野ごとの特別法が現実的であること、脅威にさらされた情報主体(消費者など)に対する通知を義務付ける必要があること、セキュリティー脆弱性情報の公開に関しては「責任ある開示」を正面から議論する時期に来ていることの三点の提言を行った。

2003年7月米国視察団報告「米国政府関連情報セキュリティ最新動向」

23日のセッションの最後は、JNSA事務局長の下村正洋氏による「米国視察団報告」が行われた。視察の目的は、本土安全保障省(DHS)の設立に代表される米国の情報セキュリティーに対する取り組みの調査などで、2003年7月28日から8月1日までの日程で土居範久氏(中央大学教授・慶應大学名誉教授)を団長とする35名が訪米し、おもに連邦政府機関での聞き取り調査を行っている。アメリカでは情報セキュリティーがグランド・デザインに基づく国家戦略として推進されていることが改めて確認されていた。

これも詳細はJNSAのWebをいていただければと思うが、視察の成果を、下村氏は「アメリカでは、DHSが中心になってグランド・デザインを策定し、その実現に基づいてさまざまな施策を実行していることが確認できた」とまとめている。日本においても、国益と国家安全保障を確保するためのグランド・デザインは一日も早く作るべき——。その思いを強くさせられたセッションであった。

24日 テーマ「技術セッション」

24日は、技術的な内容を中心としたセッションであり、セキュリティに関する最新の話題が解説された。これらも詳細なレポートはJNSAのWebページをご覧いただきたい。

「Webアプリの欠陥検査 実践編」

独立行政法人産業技術総合研究所　高木浩光氏

高木氏は、ログイン機能を持つWebアプリの欠陥検査を効率的に実践する手順を解説し、自身が開発に携わる「Webアプリの欠陥を自動検出する試作システム」を紹介した。これまで紹介された検査手続きを半自動化するも

のだ。完全な正規アクセスを保証する診断コースもあるので安心して利用できそうだ。

「世界的なPKIの相互運用を目指すChallenge PKIプロジェクト」
セコム株式会社IS研究所　松本泰氏
富士ゼロックス株式会社　稲田龍氏

最初に松本氏が過去2年間のChallenge PKIプロジェクトの経過を説明し、そこから導き出したPKI相互運用の課題を指摘した。

同プロジェクトは2001年、マルチドメイン、マルチベンダ環境でのPKI相互運用確立を目座してスタート。松本氏は「PKIの標準化と相互運用確立は同時進行で進むべきで、IETFとも積極的に連携していく必要がある。また、複雑な相互運用の問題を吸収するミドルウェアの開発も重要になるだろう」とまとめた。

次に稲田氏が講演に立ち、同プロジェクトのIETFへの働きかけを紹介した。詳細はJNSAのWebページ、および本誌の第57回IETF参加報告を見てもらいたいが、積極的にIETFの活動に加わっている様子がうかがえた。

「ネットワーク監視技術としてのハニーポットについて」
株式会社エネルギア・コミュニケーション　濱本常義氏

濱本氏は、不正アクセスの監視手段として注目されるハニーポットの運用実験の経過を報告。様々なツールを用いて侵入手口や侵入経路を探索していった様子をドキュメンタリータッチで語った。

濱本氏は運用実験で、かなり詳細に侵入者の手口を解析するのに成功している。その上で「ハニーポットの運用で気を付けるべき点は、ハニーポットが踏み台になって外部に迷惑をかけること。外向きのアクセス制御が必要になる」と指摘した。こうしたハニーポットの機能を本番システムに盛り込めば、不正アクセス監視や原因究明に役立つだろう。

「欠陥報告に見るWindowsとLinuxのセキュリティ」
龍谷大学理工学部　小島肇

小島氏は「WindowsよりLinuxの方が安全という見方もあるが、それは本当なのか」と問題提起し、2003年に報告された欠陥報告を振り返りながら、WindowsとLinuxのセキュリティを比較検証した。

「Linuxを利用すると、頻発するMs-Office向け攻撃は無視でき、再起動の必要も少なくなる。この利点は大きい。ただ逆に修正パッケージの適用頻度も多く、分かりやすいセキュリティ情報も少ない」という。今後、デスクトップ向けLinuxが普及してくれば、Linuxを対象とした攻撃が増えるのは避けられない。よりセキュアなOSと一般人にも理解できる情報提供が望まれているようだ。

以上、NSF2003も無事終了したが、反省点として、内容が濃いにもかかわらず、集客が伸び悩んだことがあげられる。来年からは実行委員会を組織して、JNSAとしてもっと内容について議論するとともに、告知と集客について会員の皆さまの衆知を集めたいと考えている。今後も会員の皆さまの更なるご協力をお願いする次第である。

全国情報セキュリティ啓発キャラバン

「インターネット安全教室」の御報告

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る。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ない。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）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よいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を開催した。この「インターネット安全教室」は、全国11カ所の自治体・学校法人・団体・商工会議所にご協力いただき、その他、警察庁、各地県警、放送局・新聞社・教育機関等の後援を得て、2003年10月～11月にかけて開催した。

期　間　2003年10月～11月

開催地　全国11カ所

主　催　経済産業省
NPO日本ネットワークセキュリティ協会

後　援　警察庁
その他、共催地毎の後援団体あり

共催並びに開催場所　下記の通り

日　程	県　名	共催地	開催場所
10月8日（水）	奈良県	なら情報セキュリティ研究会	帝塚山大学
10月23日（木）	福井県	福井県高度情報化推進協議会	福井県中小企業産業大学校
10月25日（土）	岡山県	岡山市情報政策課	岡山市職員研修所
10月27日（月）	徳島県	徳島県	徳島県立工業技術センター
11月1日（土）	神奈川県	学校法人岩崎学園	岩崎学園校舎
11月7日（金）	福岡県	学校法人麻生塾	麻生塾福岡校
11月13日（木）	沖縄県	浦添市	浦添市民会館
11月15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
11月18日（火）	大阪府	北大阪商工会議所	北大阪商工会議所
11月22日（土）	北海道	北海道情報大学	北海道情報大学
11月29日（土）	新潟県	にいがた産業創造機構 NPO新潟情報セキュリティ協会	にいがた産業創造機構

今回のインターネット安全教室は、主に、家庭や学校からインターネットにアクセスする人々や、セキュリティ啓発活動に携わる人々を対象としたセミナーである。個別のセキュリティ技術や政策などのセキュリティセミナーは首都圏では数多く開催されているが、このような一般の方々を対象にしたセキュリティ知識の底上げを目標としたセミナーは、あまり類をみないものであると言えるだろう。

各地毎に会場の規模が異なるが、集客に多大なるご尽力をいただいた共催者の方々のご尽力のお陰で、平均して100名～200名の方が参加され、沖縄では浦添市民会館にて700名が参加する大イベントとなり、11カ所全体では、2000名を超える方が参加したことになる。

[プログラム内容]

プログラムは2時間構成で、前半は今回のために新たに制作した映像CD-ROM「インターネット安全教室」(約20分)の上映とそれに関する講師解説、
後半は県警の方の解説「インターネット犯罪にあわないために」と実機4台を使った体験学習、質疑応答であった。参加者全員に、今回上映したCD-ROM(解説冊子付き)と、ノベルティとして紙製ボールペンとステッカー、紙扇子が渡された。

●CD-ROM映像

CD-ROM映像では、下記の6つのテーマに分けて作成した。できるだけ今年の事象も取り入れるよう配慮し、メールについてはウイルス感染メールだけでなく今問題になっている債権回収督促メールについても触れ、その他、無線LANを使用している際の傍受やインターネットショッピング・オークションを楽しむ場合の注意点などもわかりやすく映像で解説している。

1.危険なメールとホームページ
2.個人情報の漏えい
3.しのびよる詐欺行為
4.掲示板、チャットのマナー
5.侵入されるパソコン
6.ホームページ作成の落とし穴


奈良インターネット安全教室風景


神奈川インターネット安全教室風景

●体験学習

体験学習では、ウイルスメールへの感染を実際に模擬体験し、実際のウイルスを映像として画面で見ていただいた。(※ただし、現在のウイルスやワームは目で見てそれとわかるものが少ないため、ほとんどがかなり前のものである)その他、キーロガーを利用した、入力パスワードの漏洩の体験、メーラーやブラウザでのセキュリティ設定の方法などを解説した。

体験学習では、通常使っているブラウザやメーラーでも、その機能を熟知して利用している人は少ないようで、熱心にメモをとる方が多かった。また、ウイルスも実際に見る機会は大変少ないため、アンケートでも「ウイルスを見ることができて良かった」という意見が多かった。

●全体を通して

平日の実施が多かったため高齢者の方の参加が多かったが、参加者の方々は非常に熱心な様子であり、各地で

全国情報セキュリティ啓発キャラバン

北海道インターネット安全教室警察庁間仁田氏講演

新潟インターネット安全教室経済産業省大崎氏主催社挨拶

体験学習や質疑応答に手を挙げる人がいないのではと懸念していたが、結果的には体験学習にも積極的に手を挙げていただけた。また、高齢者を含めて申込の大半はメールであり、インターネットの普及率を感じさせた。誰もが手軽に使えるインターネットだが、セキュリティの知識をきちんと認識している人は、ネットワーク業務に携わるごく一部の人であり、実際に対策として何をすれば良いのか、自分のPCは本当に安全なのかをわかっている人は案外少ないと思える。今回のインターネット安全教室の当初の企画は、インターネットは車と同じように安全だが、車社会と同じように危険（個人情報の漏洩やウイルス感染など）も伴うものである。各学校などで行なわれている交通安全教室と同じように、インターネットの安全教室も定期的に行なわれるべきではないかという想いから始まった。インターネットを取り巻く環境は日々変わっていくので、このような教室も毎年定期的に繰り返されるべきではないかとの想いを強くした。アンケートの結果を見ても、大多数の方に満足して帰っていただけたことは、運営側としては大変に喜ばしいことであった。

徳島インターネット安全教室風景

今回参加者の方々に配布したCD-ROMを土台に、その方々が家庭であるいは職場でさらなるセキュリティ知識の向上に努めていただけることを切に願う。また、CD-ROMをツールとしてさらに多くの方にセキュリティの知識を学んでいただけると幸いである。

最後に、今回の開催には、集客と会場提供に多大なるご協力をいただいた各共催地のご担当者の方々、ご後援いただき各地の県警との連携をとっていただいた警察庁、CD-ROMコンテンツの内容検討に時間を割いていただいたJNSAセキュリティ啓発WGのメンバー、映像制作の池田事務所さま、村山監督、アドバイザーの木村氏等、多くの方々のご協力と連携の元に実施することができた。JNSA単独ではなかなか実現し得なかったことであろう。今後もこのようなネットワークを大切にし、さらなるセキュリティ啓発活動に繋げていきたいと切に願う。

事務局お知らせ
JNSA ANNOUNCE

1. 出展のお知らせ

● 情報処理振興事業協会（IPA）主催 「IPAX Winter 2004」～創造・安心・競争力～

■日　　時：2004年1月21日（水）
10:00～16:40

■会　　場：東京国際フォーラム
Bブロック7階　ホールB7

■主　　催：独立行政法人 情報処理推進機構
（現 情報処理振興事業協会）

■後　　援：経済産業省（予定）

■入 場 料：1,000円
但し、IPAホームページからの事前登録者は無料
http://www.ipa.go.jp/event/ipax/winter2004/

2. 後援イベントの知らせ

1.「ジェトロ国際テクノビジネスフォーラム」

会　期：2004年1月29日（木）～30日（金）
主　催：日本貿易振興機構（ジェトロ）
会　場：ジェトロ赤坂展示場
http://www.jetro.go.jp/tigergate/techno/japan/japan

2.「Developers Summit」

会　期：2004年1月29日（木）～30日（金）
会　場：東京コンファレンスセンター（品川）
主　催：（株）翔泳社
http://expo.seshop.com/event/dev/

3.「NET & COM 2004」

会　期：2004年2月4日（水）～6日（金）
主　催：日経BP社
会　場：日本コンベンションセンター
http://expo.nikkeibp.co.jp/netcom/

4.「活力自治体フェア '04」

会　期：2004年2月25日（水）～27日（金）
主　催：電子自治体推進フォーラム
日本工業新聞社，産經新聞社
会　場：パシフィコ横浜
http://www.jij.co.jp/event/jichi/

3. JNSA部会・WG今年度活動

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：山本匡氏/損保ジャパン・リスクマネジメント）

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

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

主な活動内容としては、下記の通り。

- 2002年度調査の課題への対応と再調査実施。
- 調査先の拡大。
- 簡易算出方法、各種指標のさらなる拡大および整理・精緻化。
- 被害発生時の緊急ヒヤリング体制整備、事故情報の収集。
- 公開された事故情報による被害額の算出対象事故の拡大。

【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。

【個人情報保護ガイドライン作成WG】

（リーダー：佐藤憲一氏/大塚商会）

昨年度より継続して個人情報保護ガイドラインの検討を進めており、2003年12月に企業側がどのような対策をとるべきかをわかりやすく解説したガイドライン「個人情報保護法対策　セキュリティ実践マニュアル」を発行した。企業における個人情報の扱い方と社内体制の構築方法、また対策が万全かどうかを調べるチェックシートや、契約書・誓約書の雛形など、企業の情報システム担当者から経営者まで、個人情報保護法に関わるすべての方を対象に具体的な対策を示す。

【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。

今年度は、8月に地方自治体向け監査（管理）基準を策定しホームページ上で公開している。

その他、日経BP社の電子自治体ポータルでメンバーによるコラムを執筆中である。

http://premium.nikkeibp.co.jp/e-gov/column/2003/column9_3a.shtml

---

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う。その他、予算を得た活動は、プロジェクトとして活動を進める。主なワーキンググループ活動予定は、以下の通り。

【セキュリティポリシーWG】

（リーダー：土屋茂樹氏/NTTデータ）

セキュリティポリシーの必要性は徐々に浸透しつつあるが、具体的に策定する場合、何を決めればよいのか、何を注意しなければならないのかを知っている必要がある。本WGでは、セキュリティポリシー策定のポイントを議論しながら成果を公開していきたい。

過去3年間に作成したポリシーやスタンダードをベースにして、そのような対策を実施する理由となる脅威および脆弱性を導き出し、さらに対策時における残存脅威についても明確にしていく。

【LANセキュリティWG】

（リーダー：関義和氏/ディアイティ）

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

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

【インターネットVPN-WG】
（リーダー：松島正明氏/新日鉄ソリューションズ）
Internet VPNを活用した、リモートアクセス環境を導入する際に検討すべき項目や、考慮点をまとめガイドラインを作成する。
Internet VPNで使用可能なプロトコルの調査の後、検証手順に基づき実機検証を実施、その結果をもとに企業ユーザー向けのInternet VPNを利用したリモートアクセス環境導入のガイドラインを作成する。

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

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

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

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

【情報セキュリティ標準調査WG】
（リーダー：佐藤慶浩氏/日本ヒューレット・パッカード）
技術用語WGにて、各種標準での用語が不統一であることや認定制度と標準の関係があまり解説されていないことに問題意識を持ち、標準等に焦点を置いた調査を目的としたWGである。
調査対象：ISO/IEC15408、17799、ISMS、SSE-CMMなど。前期に作成した標準一覧表を完成し、Webで公開中。後期では、標準や制度の相関を示した分類と年表を作成し公開の予定。

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

【データストレージ＆セキュリティWG】
（リーダー：内田昌宏氏/ネットマークス）
企業がデータの運用および保存を行う際に指標となるような管理ポリシーの作成を目指す。なお、本WGは、JDSF（Japan Data Storage Forum）殿と協調して活動する。

【暗号使用ポリシーテンプレート作成WG】
（リーダー：板倉行男氏/アークン）
暗号管理策として暗号使用ポリシーテンプレートの策定に向けた勉強会から、テンプレート作成までを行なう予定。

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

●勉強会目的のWG

【IRT研究WG】
（リーダー：武智洋氏/横河電機）
IRTに関する日本国内外の情報交換を行い、今後考えるべき問題などについてざっくばらんな議論を行う。NIRTや企業内、業界内IRTなどを始め、国際連携などについても、議論できる「場」を作る。WGでの議論を元に、一般への情報公開として、勉強会や報告会などを行うことも課題としたい。

【セキュアOSとその活用方法研究WG】
（リーダー：佐藤慶浩氏/日本ヒューレット・パッカード）
Trusted OSなどのOSのセキュリティ機能を強化したセキュアOSについての勉強をするためのWG。
WG参加の初心者と経験者の足並みを揃えるための勉強会を各ベンダーの協力を得て開催する。
合計4回の勉強会を開催し、10月30日に今年度の最終回を開催した。要望があれば、来年度の開催を検討する。

---

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

【セキュリティ啓発WG】
（リーダー：古川勝也氏/マイクロソフト）
経済産業省と共同で行なった全国セキュリティ啓発キャラバンの企画検討を行なうWGである。6月からキャラバンで使用するCD-ROMコンテンツの検討を行ない、10～11月に実施した「全国インターネット安全教室」ではスタッフとして運営に協力した。

【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/アイ・ティ・フロンティア）
来春予定されている、不正アクセス手法の攻防の一大実験場「セキュリティスタジアム」の企画と運営のためのWGで、セキュリティスタジアムの準備、募集、調達等含めた設営と、ターゲットサーバー構築などを行なう予定。9月には第1回セキュリティスタジアムセミナーを企画し、セミナー内容の企画と運営を日経BP社と協力して行なった。

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

【スキルマップ作成WG】
（リーダー：佐久間敦氏/富士総合研究所）
ネットワークセキュリティ技術者を育成するために、関係するスキルのリストアップと、個々の職種・職務によって必要とされるスキルを対応させ、セキュリティ技術者が必要とするスキルの鳥瞰図を作ることを目的とする。
今年度は、IPAからの委託事業により昨年に引き続きスキルマップを改訂し各項目についてのサンプル問題の作成まで取り組んだ。報告書は2004年にはIPAから公開される予定である。

【ITSS実証実験評価WG】
（リーダー：松田剛氏/ヒューコム）
ITSS実証実験の教育効果の測定評価を目的としていて、その成果を今後のセキュリティ技術者の評価基準策定にも利用できることを目指して発足したWG。
「高度IT人材育成システム開発事業」の委託事業として、ケースメソッドによるセキュリティスキルアップ教育を行なった。

---

5. 西日本支部
（支部長：井上陽一氏/ヒューコム）
西日本で、JNSAでなくては提供できない質の高いサービスを一丸となって提供していく。今年度は、関西方面でのセキュリティ啓発セミナーを中心として活動を行なっていく。

【セミナー運営委員会】
（リーダー：織田和子氏/シマンテック）
4月、8月、12月の大阪セミナーのコンテンツの企画検討と運営を行なった。

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 取締役
経営戦略担当

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

理　事（50音順）

TIS株式会社
在賀　良助

株式会社ヒューコム
井上　陽一

株式会社大塚商会
宇佐美　慎治

三菱電機株式会社　情報技術総合研究所
後沢　忍

テクマトリックス株式会社
浦山　清治

岡村　靖

株式会社シマンテック
勝見　勉

セコムトラストネット株式会社
川上　博康

株式会社ネットマークス
亀井　陽一

トレンドマイクロ株式会社
小屋　晋吾

日本ヒューレット･パッカード株式会社
佐藤　慶浩

株式会社ディアイティ
下村　正洋

新日鉄ソリューションズ株式会社
杉田　寛治

ELNISテクノロジーズ株式会社
鈴木　伸秀

エントラストジャパン株式会社
鈴木　優一

横河電機株式会社
武智　洋

日本ネットワークアソシエイツ株式会社
田中　辰夫

株式会社IDGジャパン
玉井　節朗

NTTアドバンステクノロジ株式会社
辻　久雄

株式会社NTTデータ
中村　逸一

システムニーズ株式会社
中山　恵介

株式会社ラック
西本　逸郎

大日本印刷株式会社
野久保　秀紀

東芝ソリューション株式会社
坂内　明

株式会社フォーバル クリエーティブ
早水　潔

マイクロソフト株式会社
古川　勝也

ＮＴＴコミュニケーションズ株式会社
松尾　直樹

RSAセキュリティ株式会社
山野　修

古河電気工業株式会社
吉澤　昭男

グローバルセキュリティエキスパート株式会社
若井　順一

東京海上火災保険株式会社
綿引　宏行

監　事

清友監査法人　公認会計士
土井　充

顧　問

東京大学　教授
今井　秀樹

新東京法律事務所　弁護士
北沢　義博

東京電機大学　教授
佐々木　良一

慶応義塾大学　教授
武藤　佳恭

早稲田大学　客員教授
前川　徹

早稲田大学　教授
村岡　洋一

奈良先端科学技術大学院大学　教授
山口　英

東京大学　教授
吉田　眞

事務局長

株式会社ディアイティ
下村　正洋

5. 会員企業一覧

(2003年11月26日現在　178社　50音順)

【あ】
(株)アークン
RSAセキュリティ(株)
(株)アイセス
(株)ITサービス
(株)アイ・ティ・フロンティア
(株)IDGジャパン
(株)アイネス
アイネット・システムズ(株) New
(株)アクセンス・テクノロジー
朝日監査法人
アマノ(株)
(株)網屋
アライドテレシス(株)
(株)アルゴ21
(株)アルテミス
(株)アンラボ
(株)イーツ
イーディーコントライブ(株) New
伊藤忠テクノサイエンス(株)
学校法人 岩崎学園
(有)インターネット応用技術研究所
インターネットセキュリティシステムズ(株)
(株)インターネット総合研究所
インテック・ウェブ・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
インフォコム(株)
(株)インフォセック
(株)インプレス
ウッドランド(株)
AT＆Tグローバル・サービス(株)
(株)栄光
(株)エス・アイ・ディ・シー 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データサービス(株)
NECソフト(株)
NECネクサソリューションズ(株)
NTTアドバンステクノロジ(株)
NTTコミュニケーションズ(株)
エヌ・ティ・ティ・コムウェア(株)
(株)NTTデータ
(株)エネルギア・コミュニケーションズ
エムオーテックス(株)
エリアビイジャパン(株)
ELNISテクノロジーズ(株)
エントラストジャパン(株)
(株)大塚商会
オムロンフィールドエンジニアリング(株)

【か】
キヤノンシステムソリューションズ(株)
キヤノン・スーパーコンピューティングS.I.(株)
京セラコミュニケーションシステム(株) New
(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 New
コベルコシステム(株)
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
シーティーシーエスピー(株)
(株)シーフォーテクノロジー
(株)ジェイエムシー
ジェイズ・コミュニケーション(株)
(株)CRCソリューションズ
シスコシステムズ(株)
システムニーズ(株)
(株)シマンテック
シャープシステムプロダクト(株)
Japan Cyber Security Institute
(株)翔泳社
(株)情報数理研究所
新日鉄ソリューションズ(株)
図研ネットウエイブ(株)
(株)ステラクラフト New
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)セラク
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)
(株)ソリトンシステムズ
(株)損保ジャパン・リスクマネジメント

【た】
大興電子通信(株)
大日本印刷(株)
ダイヤモンドコンピューターサービス(株)
中央青山監査法人
(株)ディアイティ
TIS(株)
(株)TBCソリューションズ
テクマトリックス(株)
デジタルアーツ(株) New
デジボックス(株)
学校法人電子学園　日本電子専門学校 New
(株)電通国際情報サービス
監査法人トーマツ
東京海上火災保険(株)
東芝ソリューション(株)
東芝情報システム(株)
(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)
日本アイ・ビー・エム(株) New
日本アイ・ビー・エム システムズエンジニアリング(株)
日本エフ・セキュア(株)
日本オラクル(株) New
(株)日本高信頼システム研究所
日本コムシス(株)
(株)日本システムディベロップメント
日本電気エンジニアリング(株)
日本電気システム建設(株)
日本電信電話(株)　情報流通プラットフォーム研究所
日本ネットワークアソシエイツ(株)
日本ビジネスコンピューター(株)
日本ヒューレット・パッカード(株)
ネクストコム(株)
(株)ネットアーク
(株)ネット・タイム
(株)ネットマークス
(株)ネットワークセキュリティテクノロジージャパン
ネットワンシステムズ(株)
ノベル(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)
(株)富士総合研究所
富士通(株)
(株)富士通ソーシアルサイエンスラボラトリ
富士通エフ・アイ・ピー(株)
(株)富士通ビジネスシステム
(株)フューチャーイン
(株)プラーナ
(株)ブライセン
古河電気工業(株)
(株)プロティビティ
ボーダフォン(株)

【ま】
マイクロソフト(株)
松下電工(株)
丸文(株)
(株)三菱総合研究所
三菱電機(株)情報技術総合研究所
三菱電機情報ネットワーク(株)
三菱電線工業(株)
(株)メトロ

【や】
ユーディテック・ジャパン(株)
横河電機(株)

【ら】
(株)ラック
レインボー・テクノロジーズ(株)

【わ】
ワイ・エー・ピー・ホールディングス(株)

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

6. JNSA年間活動（2003年度）

4月	4月3日	第1回政策部会
	4月18日	第1回幹事会
	4月23日	理事会（九段会館）
	4月24日	第1回西日本支部主催セキュリティセミナー
5月	5月8日	技術部会
	5月21日	定期総会（スクワール麹町）
	5月21日	臨時理事会（スクワール麹町）
	5月22-24日	白浜シンポジウム後援
	5月17日	第2回政策部会
	5月28日	第2回幹事会
6月	6月2-3日	RSA Conference 2003後援
	6月2-3日	NSF2003 spring開催(東京国際フォーラム)
	6月9日	第1回西日本支部会合
	6月13日	セキュリティ監査WGサブ合宿（晴海グランドホテル）
	6月25日	第1回教育部会
7月	7月2-4日	NetWorld+Interop 2003 Tokyo後援
	7月9日	第3回幹事会
	7月16日	3回政策部会
	7月16-18日	Wireless Japan 2003 後援
8月	8月20日	第2回西日本支部主催セキュリティセミナー
	8月26-27日	情報セキュリティシンポジュウム
	8月28日	第1回技術部会リーダー会
	8月28日	第4回政策部会
	8月28日	第4回幹事会
9月	9月17-20日	WPC EXPO 2003　主催者企画「何でも相談コーナー」後援
	9月10日	セキュリティスタジアムセミナー（工学院）
	9月24-25日	電子署名・認証フォーラム後援
10月	10月2-4日	ネットワーク・セキュリティワークショップ ｉｎ越後湯沢協力
	10月9日	第5回幹事会
	10月16日	第2回技術部会リーダー会
	10月17-18日	スキルマップ作成WG合宿（マホロバマインズ三浦）
	10月22-24日	NSF2003開催（東京ビッグサイト）
	10月29日	第5回政策部会／全国情報セキュリティキャラバン実施
11月	11月6-7日	Pacsec.jp後援
	11月12-14日	まちと人のセキュリティシンポジウム協賛
	11月19日	第3回技術部会リーダー会
	11月26日	第6回幹事会
	11月26日	日・韓セキュリティForum、商談会／全国情報セキュリティキャラバン実施
12月	12月3日	Internet Week 2003参加
	12月5日	第3回西日本支部主催セキュリティセミナー
	12月9日	第6回政策部会
	12月12-13日	セキュリティ標準調査WG合宿（初島）
1月	1月15日	第7回幹事会
	1月21日	IPAX Winter 2004出展（東京国際フォーラム）
	1月27日	新年賀詞交歓会（東京グランドホテル）
	1月29-30日	Developers Summit 2004後援
	1月29-30日	ジェトロ国際テクノビジネスフォーラム2004後援
2月	2月4-6日	NET&COM 2004　後援
	2月25-27日	活力自治体フェア04　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

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。

日本ネットワークセキュリティ協会、インプレス
個人情報保護法完全施行に向けた、企業対策ガイドラインを発行
～「個人情報保護法対策　セキュリティ実践マニュアル」発売～

JNSAでは、個人情報保護法に対応した企業対策ガイドライン「**個人情報保護法対策　セキュリティ実践マニュアル**」を書籍にまとめ、12月2日から、株式会社インプレス（本社：東京都千代田区、代表取締役社長：塚本慶一郎）より発売しました。

2003年5月に成立した「個人情報保護法」により、企業は、2005年4月の完全施行までに、個人情報保護法に対応した万全の社内体制作りが必須となっています。しかし、具体的にどのように対策を進めていいのか、プライバシーマーク制度など他の規範や制度との違いもわからず、どう行動すれば法に違反しないのか、企業にとってわかりやすい指針がないのが実情です。

こうした現状をふまえ、ネットワークセキュリティの専門企業178社が組織する日本ネットワークセキュリティ協会は、企業側がどのような対策をとるべきかをわかりやすく解説したガイドライン「個人情報保護法対策　セキュリティ実践マニュアル」をまとめました。
日本ネットワークセキュリティ協会では、2002年4月から、“個人情報保護ガイドライン作成ワーキンググループ”を設置して研究を開始してきました。本書はその成果をまとめたもので、個人情報保護法における企業対策を具体的にまとめたガイドラインの発行は初めてです。

企業における個人情報の扱い方と社内体制の構築方法、また対策が万全かどうかを調べるチェックシートや、契約書・誓約書の雛形など、企業の情報システム担当者から経営者まで、個人情報保護法に関わるすべての方を対象に具体的な対策を示します。

目　次

「個人情報保護法対策
セキュリティ実践マニュアル」
定価（本体3,500円＋税）

お買い求めは、最寄りの書店またはインプレスダイレクトでどうぞ。（http://direct.ips.co.jp/）

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