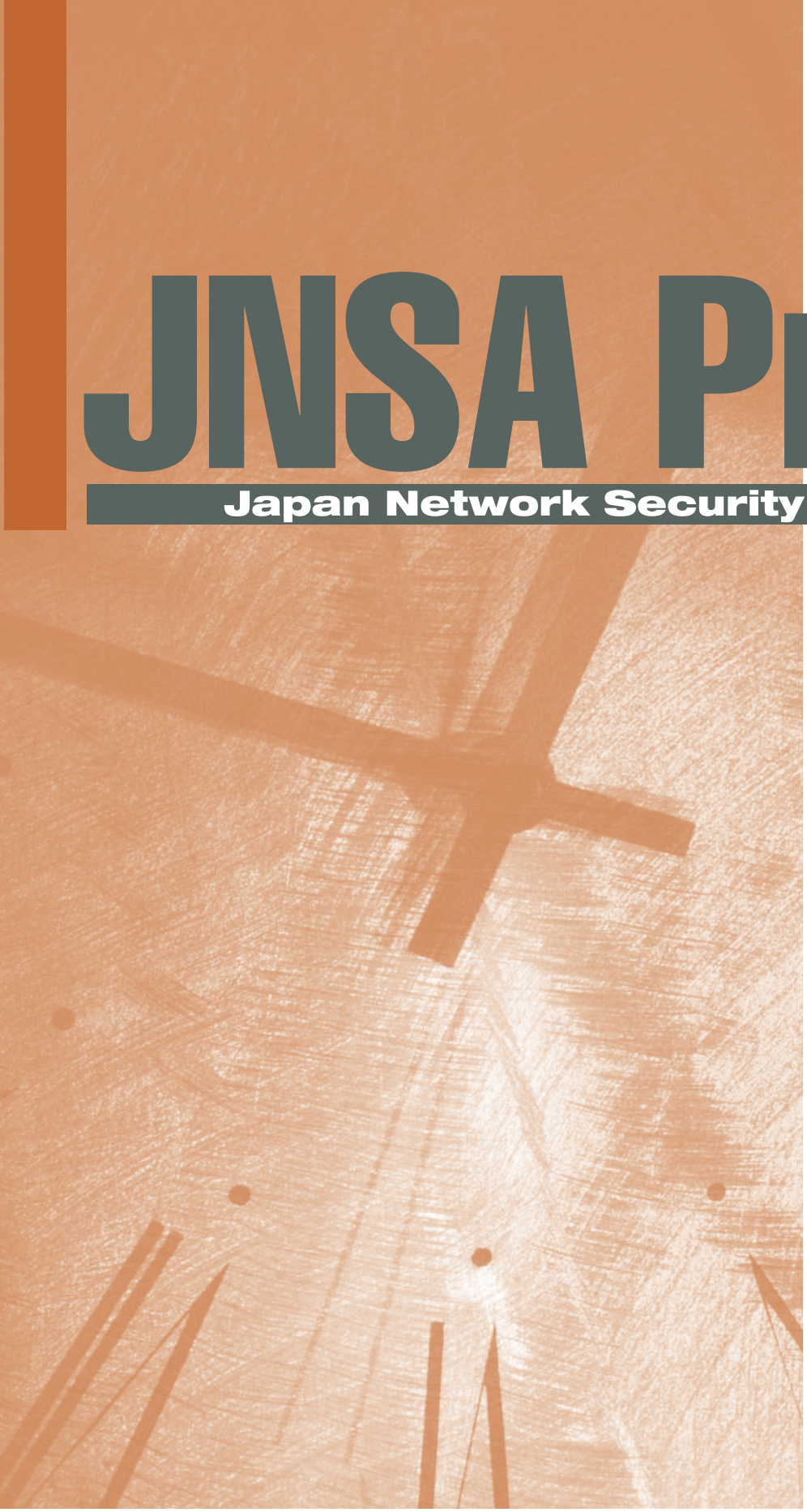
JNSA Press

Japan Network Security Association



Vol.18
December 2006

CONTENTS

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

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

JNSA「セキュリティ製品バイヤーズガイド」が誕生!

―セキュリティ製品・サービスの情報収集ならおまかせ―

http://**buyers.networkworld.jp**

>>http://buyers.networkworld.jp

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

情報セキュリティと適合性評価

独立行政法人 情報処理推進機構（IPA）セキュリティセンター
セキュリティセンター長 三角　育生

情報セキュリティの世界では、国際標準などに基づく認証制度が重要な役割を担っている。自分自身は、1999 年から 2001 年にかけて、通商産業省（当時）で国際標準や認証に関する政策に携わったが、そのときに、日本工業標準調査会（審議会のひとつ）で認定・認証などの適合性評価関連政策の整理をした報告書を事務局としてとりまとめた。ちょうどその頃、情報セキュリティマネジメントシステム（ISMS）適合性評価制度やコモンクライテリアに基づく IT セキュリティ評価・認証制度の立ち上げが議論・準備されていたと記憶する。現在、これらの制度はどうなったかというと、IT セキュリティ評価・認証制度は、国際的な相互承認の枠組みの下で、IPA が認証機関となり、我が国の基盤として機能するようになっており、また、ISMS 適合性評価制度も広く普及してきている。

さて、製品やサービスについて、なぜ、国際標準などがあるのか。消費者などにとっては、製品やサービスを購入しようとするときに、その製品などが、例えば乾電池のように互換性が確保されているかどうか、安全や健康の保持、環境保全などの観点から適当なものとなっているかどうかなどは、非常に気になる点であろう。そのときに、国際標準などがあると、その規格や基準に適合しているかどうかを確認することにより、こうした気になる問題を適切に解決できるわけである。

では、どうやって規格や基準を満たしているかどうかを確認するのかということになる。消費者などは、製造者やサービス提供者が規格や基準を満たしていると主張しているのを信じる、自ら試験などを実施して確認する、中立の第三者に依頼して規格や基準を満たしているかどうかを確認してもらうといういずれかの手段をとることになる。消費者などが、製造者やサービス提供者の主張を信じられると考えるときには、それでよいだろう。しかし、それでは不安があるときどうするか。まず、自らチェックして安心できればそれがよい。しかし、情報システムなどについては、複雑であるため、相当の専門的知識がなければ、自らチェックすることはできないし、不安は取り除けない。そのときに、中立の専門的能力のある第三者にチェックを依頼することの意味が出てくるわけである。情報セキュリティ分野における第三者による認証制度は、まさに、消費者などが情報システムなどを安心して利用していけるために整備されたものといえよう。

「Security」という単語の語源は、ラテン語の「se」（解放）と「curus」（不安）であるそうだ。情報システムの利用者が、不安から解放された状態でいられるように、情報セキュリティ分野の適合性評価制度が、今後とも、利用者（消費者など）のために役立つよう、運営していきたいと考えている。

現場まかせにしないセキュリティ設計、評価、実装のあり方について ーセキュリティは現場で起こっている

松下電工株式会社　福田　尚弘

複雑化、モジュール化したシステムからなるコンピュータ社会にあって、本来セキュリティ設計、評価、実装は重要な位置を占めている。システム開発、運用の分業化、モジュール化によってその傾向は強まっている。しかしながらISMSやISO15408、CMM、ISO12207などの仕組みや枠組みはドキュメントとして揃っているにもかかわらず、その手法に関してはいまだ職人芸に支えられているままである。仕組みや枠組みも重要であるが、本来、セキュリティの脆弱性はちょっとしたミスや理解不足から起こる。これは人間が行う以上どうしても発生する問題である。仕組みや枠組みは責任の所在を明らかにできるが、ミスや理解不足は現場で起こる問題であってゼロにすることは大変困難である。ここで問題なのが、最終的にセキュリティ設計、評価、実装の手法が依然として現場まかせとなっていることである。
ここでは、様々な業種におけるセキュリティ対策の実態を述べ、それを受けて現場まかせにしないためにはどのような工夫が考えられるかを述べ、最後に理想的なセキュリティ設計や実装方法のあり方を模索する。

1. セキュリティ対策の実体は現場のエンジニアに依存する

24（TWENTY FOUR）という米国で大ヒットしているテレビドラマをご存知だろうか？米国連邦機関の組織であるテロ対策ユニット（CTU）の捜査官ジャック・バウアーがテロリストと戦うサスペンス・アクションの内容である。ジャックはCTUから任務を受けてテロと戦うわけだが、神出鬼没で相手の裏をかくテロとの戦いでは往々にしてCTUのルール、CTUの指示を無視して行動することを余儀なくさせられるのである。また、CTUの指示を無視したり欺いたりと行動するため不遇であることが多い。

まさに情報セキュリティの分野とこの世界はオーバラップして見える。テロはセキュリティ上の脅威であり、セキュリティ対策を行う現場の担当者はジャックである。そしてこの戦いに終わりはない（人気シリーズなので次々と次回作がリリースされるのではあるが）。また、CTUは会社組織に見え、ISMSやISO15408、CMMなどのルールでジャックを縛っている構図が見て取れる。

何が言いたいかといえば、ここでの「主人公はジャック」であるということである。全てはジャック、つまり開発者の腕にかかっているのである。

2. 業種ごとに異なるセキュリティ意識

政府・自治体、教育などの機関、金融、エネルギー、情報通信、医療などのインフラ系、製造、運輸、サービス、不動産等の企業、または個人など、異なる業種または業態で異なるセキュリティが要求されると考える。つまり、業種毎にセキュリティ上で重要なポイントが異なる。たとえば、高レベルの顧客情報の保護（金融）、企業機密管理（エネルギー）、情報セキュリティ運用管理（金融）、外部との接続制限（エネルギー）、入退室管理（金融、エネルギー）、プライバシー（運輸）、システム運用管理（情報通信）、セキュリティ対応の手順化（金融）、セキュリティ教育（金融、運輸、情報通信）などである（警察庁：平成17年度「不正アクセス行為対策等の実態調査」からhttp://www.npa.go.jp/cyber/research/）。

それ以外にも、情報機器への信頼性やシステム管理における要求レベルも様々であり、それぞれが相互に接続される場合も考えられる。セキュリティ意識が異なれば、その対策も異なってくる。従って、業種ごとに異なるセキュリティ対応が要求されると考えられる。また、図1の警察庁の「不正アクセス行為

対策等の実態調査」にある「セキュリティポリシーの規定事項」(平成15年～17年までのデータ比較)を見ると、3年間の比較でも、基本方針、組織、運用管理においてはほぼ対応されているにもかかわらず、システム開発やメンテナンスの規定対応はほぼ低い数値のままである。つまり、セキュリティの方針、ルール、運用体制は確立したが、実質的なシステム開発やメンテナンスはまだ十分でないとも見て取れる。一方で、脆弱性調査は利用されてきている。脆弱性検査は全体で18.8%、意識の高い業種では約44%～28%行ったとされている(警察庁:平成17年度「不正アクセス行為対策等の実態調査」からhttp://www.npa.go.jp/cyber/research/)。

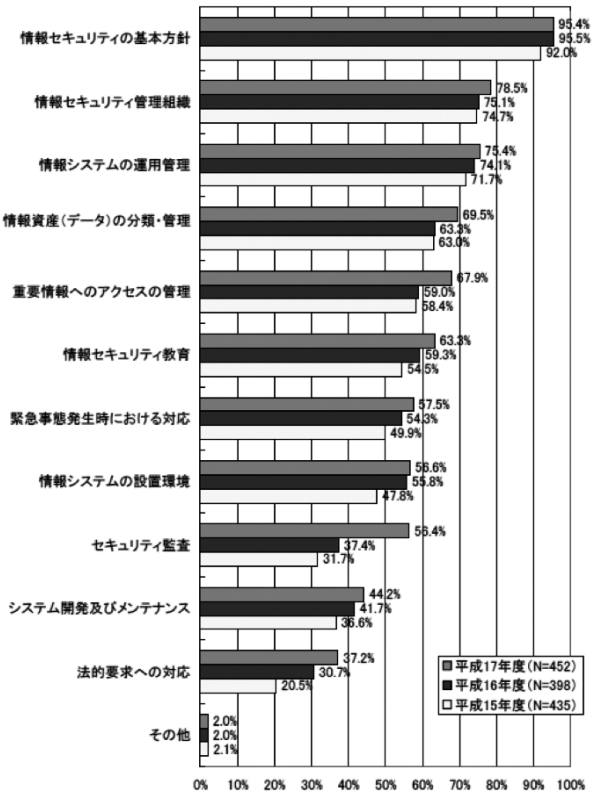
また、セキュリティ対策の効果については各業種から半数以上の回答で、「セキュリティの対投資効果」が見えない、「コストがかかりすぎる」という内容があった(警察庁:平成17年度「不正アクセス行為対策等の実態調査」からhttp://www.npa.go.jp/cyber/research/)。

3. システム開発者にとっての困りごと

ジャックのようにタフで優秀な捜査官であれば安心であるが、事はそうはいかないであろう。異なる業種に属する様々なレベルのエンジニアが様々な要求によって様々なセキュリティモジュールを組み合わせることでセキュリティ対策を行っているためだ。また、セキュリティの方針、ルール、運用体制が確立してきたことにより、どのように対応するかということが課題となってきている。さらに、「セキュリティ対策の効果が見えない」という問題がさらに事を難しくする。そこで、開発側にとっての課題をまとめると以下のようになると考える。

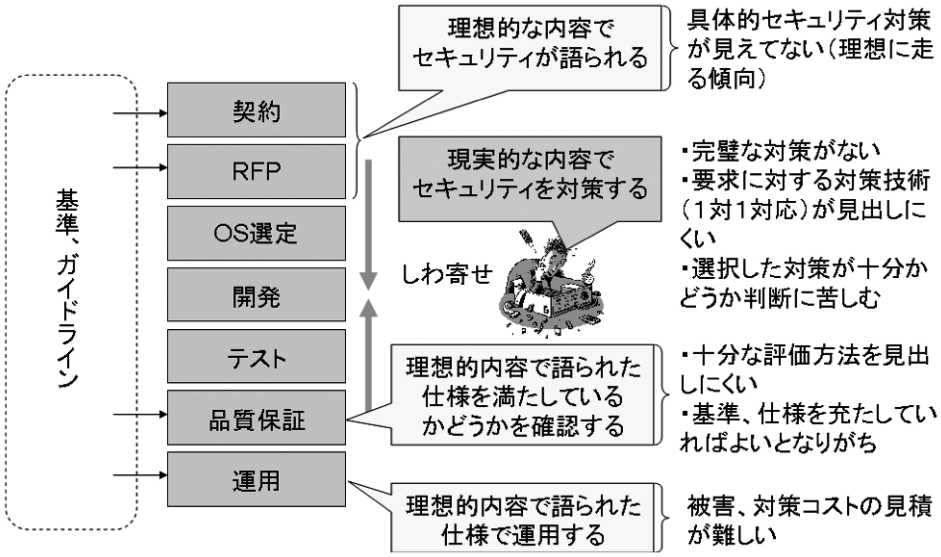
(1) セキュリティ対策をどのようにどこまでやったらよいか具体的にわからない。
(2) セキュリティの確保(担保)のためには様々な基準(ISMS、ISO15408等)はあるが、開発者にとっての具体的な手段を示していない
(3) 様々なセキュア化のための対策(脆弱性検査方法など)が存在するが、どれが何を担保してくれるのか明確ではない。
(4) システムの用途や条件によって(たとえば業種、業態によって)対策が異なる。

図1.「セキュリティポリシーの規定事項」
(平成15年～17年までのデータ比較)



出典:平成17年度「不正アクセス行為対策等の実態調査」のP.63、警察庁、HP:http://www.npa.go.jp/cyber/research/)

図2．セキュリティ対策のしわ寄せ構造



4

4. 開発プロセスの観点から見る

開発側にとっての課題を開発のプロセスから見ると、セキュリティ対策の実態は「しわ寄せ構造」として存在するとも言える。図2は、システムの開発プロセスをセキュリティ対策の観点から描いた図である（多少オーバーに書いた図なのでその点ご容赦願いたい。）

開発プロセスにおけるセキュリティ対策において、ISMSやISO15408、12207など基準やガイドラインは存在し、どのような項目を行えばよいかはある程度わかるが、具体的なセキュリティ対策は開発者に依存しているのが現状である。開発の契約またはRFPを作成する時点では、依頼者のセキュリティ要求が現実に可能な対策を超越する場合がある。特にセキュリティ技術は脅威に対する対策ということで成立している。従って、その時点で対策が成立したとしても、つまり品質側の立場からは、たとえその時点で脆弱性調査がパスされても保証はまったくないのである。完璧な対策は一切ないのである。また、運用側に至っては、被害と対策コストの見積もりが難しい点もある。本来、セキュリティの要求に対し対策技術が1対1に対応するのが理想であるが、実際の実装との整合を考えると必ずしもそのようにはならない。つまり、対策が十分かという問いに対しはっきりYESといえるレベルにないということになる。ここがセキュリティ対策の悩ましいところではないだろうか。

5. セキュリティ対策技術と実装の難しさについて

セキュリティの対策技術の例としてSSL/TLSを考える。ほとんどの人はSSL/TLSが安全かどうかを考えることはないであろう。個人情報の安全な通信にSSL/TLSはほとんど用いられている。IPsecについても同様であるが、ある種の「SSLまたはIPsec＝安全」という刷り込みがあるように思える。セキュリティプロトコルの専門化であれば、全てのバージョン、モード、パッチがあたっていないSSLやIPsecが安全であるということは言わないであろう。ここで問題となるのは、そのような刷り込みがセキュリティ対策で問題となる場合もある。また、SSLといっても正確にはHTTP、電子メール、VPNのSSLなどアプリケーションが異なれば若干異なるプロトコルになっ

ている。また、SSLを実装する場合での注意もある。HTTPはWebページへのアクセスを終了するとコネクションを切断する。一方、SSLは一度接続した相手のセッション鍵をしばらく保持する仕組みである。この問題はHTTPがKeep－Aliveすることで解決するが、システム設計者からするとサーバホストの構成によっては特性を理解して設計しないといけない。最近の開発スタイルで一からコードを書くものはないであろう。従って、深くは理解し得ないモジュール、OS、ライブラリおよびハードウェアを組み合わせ開発しているためどこかに落とし穴が存在する可能性が潜んでいると言えよう。業種によってセキュリティ要求やシステムが異なることを述べたが、標準技術で固めたシステムを開発する以上、適材適所というわけにいかず、どこかに歪が発生する。

6. OSIの階層別の観点から見る

単体のセキュリティ対策製品を考えるときOSIによるモデルで全てのレイアーで安全であることがその製品が安全であると言えよう。まずプラットフォームのOSが安全か、ミドルウェア、アプリケーション、ドライバに至るまでセキュリティ対策は必要であろう。その上でシステムとして構築した場合に全体で安全でなくてはならない。

7. 現場まかせにしない工夫

セキュリティ設計を行うには、シンプルかつモジュール化されていること、設計に透明性があること、最小限の情報を保持し最小権限で動作すること、エラー処理、ログ処理、性能低下を防ぐこと、フェールセーフ、耐障害など様々なことを検討しなければならない。それを業種別、業態別、実装形態別など様々なシステムの用途や条件に合わせて設計しなければならない。図2の「セキュリティ対策のしわ寄せ構造」で描いたが、開発プロセスの中で幾つかのプロセスはほぼ十分か、内容が充実しつつある。上流のセキュリティポリシーの方針、下流の脆弱性調査手法、監査方法などである。これら固まりつつある項目と、設計段階で必要となる対策技術とを結びつける対応マップが存在すると開発者には有用ではないかと考える。エンジニアは常に同じシステムを作っているわけではない。従って、違うセキュリティ要求に対し対応マップを参照することで容易に対策を導き出せるとありがたい。

8. まとめ

冒頭から多少偏った視点での寄稿であった点をご容赦いただきたい。「開発者の裁量/スキルによる対策にはしたくない」、「最終的に問題が起こったときその対策を選択した根拠を示したい」という思いがあってのことである。現状のセキュリティ対策状況を見ると、セキュリティ指針や仕組み、監査などが先行し、開発者がそれに難儀するまたは自分の裁量で対応するという状況ではないだろうか。真の意味でセキュアなシステムを作ることは難しい。このことを理解し、開発プロセスの上流から下流までにしわ寄せが発生しない開発体制の構築が望まれる。尚、本件は、セキュアプログラミングWGで検討中である。

参　考:

平成17年度「不正アクセス行為対策等の実態調査」、警察庁、HP:http://www.npa.go.jp/cyber/research/

デジタル・フォレンジックによる情報漏えい調査

NPO デジタル・フォレンジック研究会　理事
株式会社 UBIC　代表取締役社長
守本　正宏

1. デジタル・フォレンジックの必要性

現代ではIT技術の発達によって情報がより高速に大量にかつ容易に保管･移送･書き換え･消去が可能になった。これに伴い、企業の業務形態も大きく変化している。設計・会計・各種管理簿から、プレゼン資料作成・業務連絡に至るまで、コンピュータを使用しないオフィス業務は考えられないと思えるほどに広くコンピュータが普及し、紙媒体で管理・運営してきた膨大な情報は、デジタルデータに変わり保管・管理しやすくなったほか、今まで郵送していた社内・社外への重要情報はインターネット環境を利用することにより、一瞬にして相手に送付できるようになり、効率良く且つスピーディーに業務ができるようになった。まさにIT社会の到来といえる。

一方、上記のような特徴に加えデジタルデータは目に見えない形で存在するため、そのリスク管理は容易ではなくなった。デジタルデータをどれほど正確にかつ安全に管理できるかが、その情報を持つ団体や個人にとっての重要課題になっている。そのため、デジタルデータを守るさまざまな情報セキュリティ技術が発達してきた。しかし、現実的にはデジタルデータを守ることは非常に困難であり、完全に情報を守ることは不可能であるといわざるを得ない。

その結果、情報の不正使用などは必ず発生するものであるという観点にたった対策が必要になってきた。これまで主流であった防御的なセキュリティ対策に加えて、情報漏えいなどのセキュリティインシデント発生後の対応策が必要になった。

また、IT社会においては発生する全ての犯罪は何らかの形でデジタル機器が関与しているといっても過言ではない。誹謗中傷や、不正会計、横領といったローテクな犯罪であっても、その証拠が何らかの形でコンピュータに残っている可能性が高くなっている。そのため、捜査機関ではコンピュータなどのデジタル機器は指紋と同様に優先的に取得すべき重要な証拠として位置づけされている。すなわち、デジタル機器が関与している犯罪はハッカーによるものだけでなく、さほどITの知識を有しない人々にまで広がっていった。

そのような中、ハイテク機器のデータを高度な技術を用いて証拠性を維持しつつ取得・解析を行い、法的問題を解決する手段であるデジタル･フォレンジックは危機管理という観点からにわかに脚光を浴びてきた。

また、同時に、サーベンスオクスリー法や新会社法など、企業コンプライアンスのための内部統制を義務づけた法律が出され、その具体的な手法としてのデジタル･フォレンジックの役割は重要である。

今回は、フィクションの情報漏えいの事件を例に取り、デジタル･フォレンジックの技術と運用方法を紹介する。

2. 今回の事例の背景（機密情報の漏えい）

対象者(鈴木一郎氏：仮名)はあるサービス業の大手企業Ａ社で､営業職に就いていた｡鈴木氏が退職して、同業他社Ｂ社に移った後に、Ａ社が所有する、ある地域の顧客情報がＢ社に漏れているらしいとのうわさが立った。不審に思ったＡ社は鈴木氏が使用していたコンピュータをデジタル・フォレンジック専門企業に依頼して調査することにした。Ａ社では退職者のうち、重要人物、および要注意人物のコンピュータデータを適時保全し、1年間保管することを規定していたので、迅速に調査を開始することが出来た。コンピュータのデータは使用時間とともに、記録が書き換わる可能性が高いので、対象者が使用していたという証明が困難になってしまう。そのため、事件が起きた場合、安易にコンピュータを操作したりせず、コンピュータ内のデータが書き換わらないように保つことが非常に重要である。

3. 証拠保全の重要性

法的証拠能力を持たせたまま、証拠データを確保

する作業を証拠保全という。具体的には対象者のコンピュータのHDD：ハードディスクドライブ(保全元)に保存されているデータを別に用意した保全用HDD(保全先)に複製(物理コピー)を行なう。そこで重要になるポイントは主に保全元のデータと保全先のデータが書き換えないように複製すること及びその同一性を証明することの2つに絞られる。

証拠保全時における複製は必ず物理的複製が必要となる。物理的複製とはデータが格納されている部分だけの複製ではなく、セクター毎にHDDの全領域に対して複製を実施する。表面的にはデータが格納されていない箇所に、故意に容疑者がデータを隠蔽している可能性や、消去されたデータ等が存在している可能性があり、証拠となる重要データがその部分に隠されている可能性が高いからである。(図1)

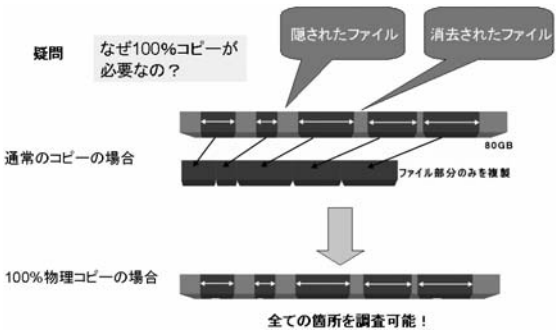


図1　物理的複製(コピー)の重要性

今回の作業では、A社では平時よりデジタル・フォレンジックの専門化により、物理コピーが実施されていたので、HDDの全ての領域に対して、退職時の状況が保存されたまま、調査を実施することが出来た。

4. 解析(コンピュータ端末調査作業)の実施

解析を実施する場合には、証拠保全して得た証拠データを直接解析することは禁じられている。それは直接解析することによって誤ってデータを破壊することを防ぐためである。

解析実施時はまず、証拠保全したデータを解析専用データ形式に変換する。変換後に専用ソフトウェアにてデータの解析を行なう。専用ソフトを使用することによってデータ領域を分けている部分へのアクセスや、消去されたデータあるいは、レジストリ保護領域へのアクセス等、通常Windows上で制限がかかっている領域での作業が可能となる。また、コンピュータ内の全ファイルを形式ごとに分類し、調査を容易に出来るようにしている。(図2参照)

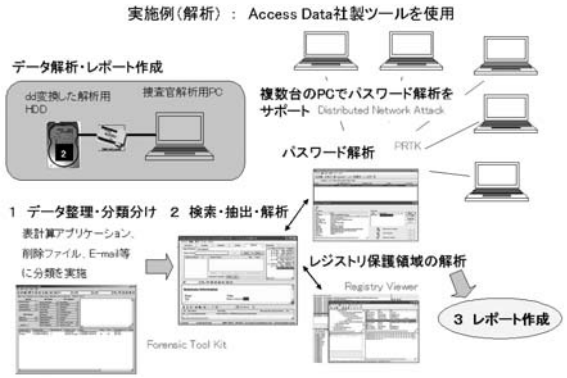


図2　解析工程

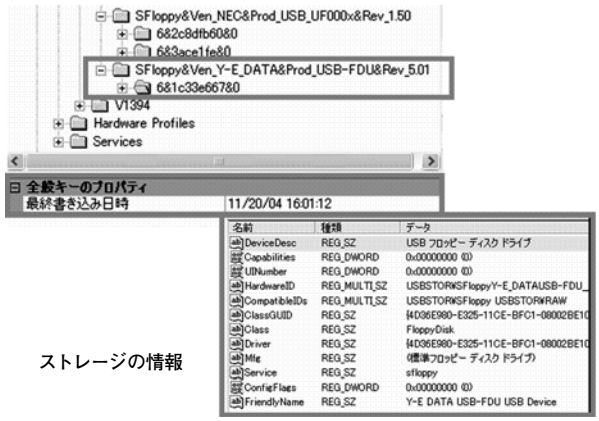
今回、機密情報の漏えいが考えられたので、ファイルのダウンロードが行われたかをレジストリ領域を調査したところ、実際の業務には必要のない地域の顧客情報ファイルを退職直前にダウンロードしていることを突き止めた。

最終書き込み日時	11/29/04 10:48:18
クラス名	Shell

名前	種類	データ
MRUList	REG_SZ	dcbajihgfe
d	REG_SZ	\\File-server\SEER\玉川店顧客情報\顧客名簿世田谷区.xls
c	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\inous_waka_05.jpg
b	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\images.jpg
a	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\00040170.jpg
j	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\480_663.jpg
i	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\kasuma_530_02.jpg
h	REG_SZ	C:\download\総務資料\顧客名簿世田谷区.xls
g	REG_SZ	C:\download\総務資料\わか\.jpg
f	REG_SZ	C:\download\総務資料\item_4.jpg
e	REG_SZ	C:\CCIS\db\create.sql

図3　NTUSER.DAT ／ OpenSaveMRU レジストリ

次に情報が漏えいした経路の調査を行った。まず、USBメモリ等の外部接続機器の履歴を確認した。(図4)　比較的多い情報の持ち出し手法はこういった外部メディアを使用したものである。しかし、今回は外部メディアへデータをコピーした形跡は発見できなかった。



ストレージの情報

図4　外部メディア接続情報の表示

次に、HDDに残るEメールデータの調査を行った結果、WEBメール(Yahooメール)にて社内の機密情報を売買する内容のやりとりを行っている事が判明した。送信相手は　“佐藤二郎＜sato_jiro@yahoo.co.jp>（仮名）で、11月20日から26日の間にかけて複数回データの売買に関する連絡をとっていた。社内サーバーからダウンロードした「顧客情報世田谷区.xls」ファイルをメールに添付し、11月22日の10:08に佐藤二郎宛てに送信していたことが判明した。このように、デジタル・フォレンジック解析ソフトウェアにより、Internetの閲覧画面の再構成や復元が容易に可能になる。

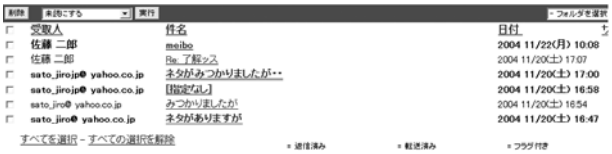


図5　Webメール:送信済みフォルダ(再構成)

図6　Webメール:メールの画面(再構成)

図7　Webメール:名簿の送信画面(再構成)

次に、鈴木氏の就業中の態度を調査する為に、Internetの閲覧履歴を確認したところ、オンライントレードサイトにアクセスしており、業務とは関係ないホームページを閲覧していたことが判明した。
◆11月25日にアクセスした履歴があった。

File Name	Full Path	Acc Date
ad[1].htm	M:¥NONAME-NTFS¥Documents and Settings¥Administrator¥Local Settings¥Temporary Internet Files¥Content.IE5¥QLMN61KL¥ad[1].htm	2004/11/25 15:05

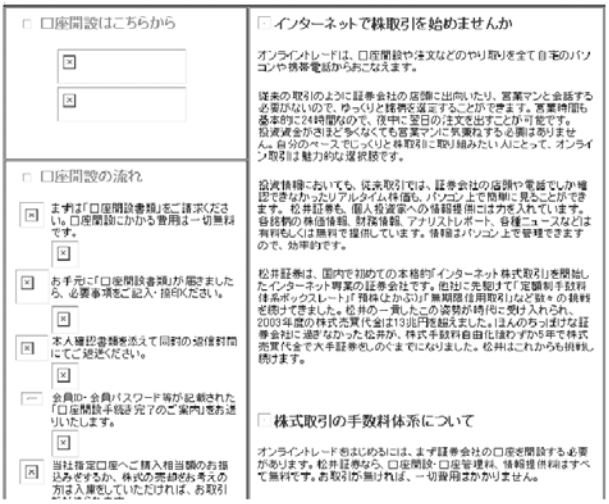


図8　オンライントレードサイト

5. 結論

対象者(鈴木一郎氏)は、退職前に社内の機密情報をダウンロードし、不正に外部へ持ち出しており、更には、就業時間中に業務とは関係ないホームページにアクセスしていたことも判明した。

ここでは、データを不正に流出させた証拠だけでなく、就業時間中に業務外のホームページの閲覧記録なども証拠としてあげている。これらの記録は、あまり問題にはならないように思えるが、実は訴訟になった場合は、裁判官の心証に与える影響は大きく、実際の事件においては貴重な証拠として採用されることがあるので軽視できない。

このように今まで困難であったコンピュータを利用した不正の証明を法廷でも利用できるような技術的手法(デジタル・フォレンジック)を用いて行うことが可能になった。

この事件ではInternetの閲覧履歴の調査を中心に記述したが、その他にも数多くのデジタル・フォレンジック調査技術・手法があり、さまざまなケースの調査を可能にしている。

現在、企業においてはその書類の90%以上がデジタル化されていると言われている。デジタル・フォレンジック調査体制の整備が、企業の危機管理体制における重要な鍵となることは疑い得ない。

6. おわりに

今回はデジタル・フォレンジックを不正調査で利用した例を紹介したが、デジタル・フォレンジックの最も記すべき特色は、開示する情報に関して訴訟にまで耐えうるほどのIntegrity（正当性)を維持していることである。ここ数年、わが国において企業コンプライアンスの重要性が叫ばれ、内部統制がキーワードになってきている。金融商品取引法(日本版SOX法)や会社法などの法整備も進んできている。時代はまさに企業や組織の信頼性を求めている。信頼性は正しい情報開示から生まれるといっても過言ではないだろう。そのためにデジタル・フォレンジックの重要性はますます高まっており、いまや普及・啓蒙からすでに実用化のフェーズに移行しているといえる。NPOデジタル・フォレンジック研究会では、そのような時代の要請に応え、“J-SOX時代のデジタル・フォレンジック”と題して第3回デジタル・フォレンジックコミュニティ 2006を12月18日、19日の2日間にわたり、グランドヒル市ヶ谷で開催した。そこでは各方面の専門家を招き、技術、法律、経営・監査の各分野から企業・組織における信頼性確保のためのデジタル・フォレンジックの実用化に関して提言している。J-SOX法対応に関して、企業・組織に具体的な指針を示す貴重な機会になったのではないかと考える。この場をお借りして紹介させていただきたい。もしご興味があり、レジュメ集(有料)をご希望される方は、NPOデジタルフォレンジック研究会事務局(ウェブサイト www.digitalforensic.jp)にお問い合わせ願いたい。

JNSA ワーキンググループ紹介

Webアプリケーションセキュリティ調査・検証 WG

WGリーダー
株式会社アイアイジェイテクノロジー　加藤　雅彦

本WGは今年で発足から3年目となり、Webアプリケーションのセキュリティに関わる問題について、分科会形式で様々な角度から評価、検討等を続けてまいりました。

WG発足当初は、Webアプリケーションセキュリティについての認知度もそれほど高くなかったのですが、様々な方々が認知に関して努力されてきたこと、また大規模なインシデントの発生によってマスコミにとりあげられることが増えた、といった要因もあり、3年前と比較すればWebアプリケーションセキュリティは一般によく知られるようになりました。その発生メカニズムや対策方法も3年前とは比較にならないほど情報が整理され、充実してきています。

しかし、認知度が上がってきたとは言うものの、Webアプリケーションの脆弱性やシステムプラットフォームそのものの脆弱性が残っているサイトも相変わらず多数存在しており、悪意ある攻撃を受け、被害にあうということが以前と変わらず見受けられるのもまた事実です。

そこで、今年度の活動としては、より広くユーザの皆様に向けてWebシステムの安全性を啓発することをWGの活動目標としました。具体的なプランとしては、わかりやすさ、伝わりやすさを考え、ケーススタディを通じて「よりよいWebセキュリティ」をユーザの皆様に伝えていきたいと考えております。よって、検討内容はWebアプリケーションに限定せず、システムプラットフォームや運用といった、Webサイトのライフサイクル全般とさせていただきました。

本WGの活動が Webサイトの安全性向上に少しでもつながっていけば幸いです。

皆様にも御協力の程、宜しくお願い申し上げます。

1. WG の活動目的

上記のとおり、今年度はWebシステムの安全性に関しての啓発を活動の中心とします。Webサイトのライフサイクルに着目し、それぞれのフェーズ(企画、設計、構築、テスト、運用)で検討、実施すべきセキュリティ要素を明らかにし、よりよいサイトにするにはどうすればよいかをフェーズ毎のケーススタディの形で提示していきます。

2. WG の年間活動予定

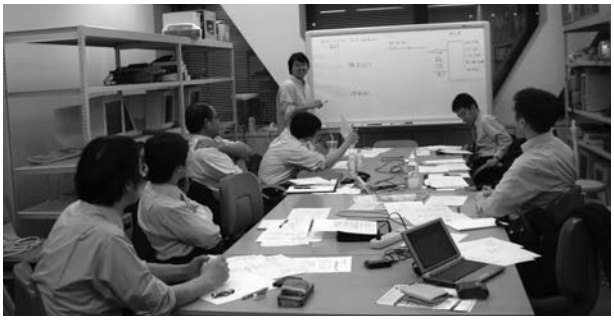
7月からWG活動を開始し、テーマ決定のためのブレーンストーミングを数回行った後、月次でミーティングを開催しています。今後は12月中にコンテンツ構成をfixし、以降は個々のメンバーでコンテンツ作成を行う予定です。進捗次第では集中的にミーティングを行うことも考えています。

3. 予定成果物

活動目的にも述べましたが、Webセキュリティに関する啓発コンテンツの作成を予定しています。コンテンツはJNSA成果報告会以外にも、可能であれば何らかのメディアを通して外部に公開したいと考えています。

4. メンバー募集の条件

条件は特にありません。昨年度活動いただいた方でも新たに活動いただける方でも、特に問いません。ただし、コンテンツのアウトプットを目的とするため、Webセキュリティに関してコンテンツが書ける方は積極的にご参加いただきたいと思います。



◆ 参加メンバー（2006年12月現在、順不同、敬称略）

NRIセキュアテクノロジーズ株式会社	観堂 剛太郎
NECネクサソリューションズ株式会社	中西 克彦
NTTコムウェア株式会社	丸尾 浩隆
クオリティ株式会社	山田 勝志
住商情報システム株式会社	二木 真明
住商情報システム株式会社	手塚 信之
株式会社ディアイティ	坂本 慶
テクマトリックス株式会社	澤崎 裕喜
テクマトリックス株式会社	酒井 喜彦
東京エレクトロン株式会社	水本 真樹
凸版印刷株式会社	辰己 元昭
日商エレクトロニクス株式会社	松尾 竹純
日本コモド株式会社	岩撫 義之
日本ヒューレット･パッカード株式会社	奥脇 佳
野村総合研究所	高橋 淳
株式会社日立製作所	井上 正規
富士通株式会社	加藤 智之
富士電機アドバンストテクノロジー株式会社	宗像 昌朗
株式会社 ブロードバンドセキュリティ	佐藤 友治
松下電工株式会社	横山 樹一郎
三菱電機株式会社 情報技術総合研究所	河内 清人
三菱電機情報ネットワーク株式会社	山村 竜也
富士通株式会社	奥原 雅之
ドコモ･システムズ株式会社	黒川 彰久
株式会社アイアイジェイテクノロジー	加藤 雅彦

内部統制におけるアイデンティティ管理WG

WGリーダー
グローバルセキュリティエキスパート株式会社　宮川　晃一

1. WGの活動目的

J-SOX法における「内部統制」の必要性が叫ばれている中で、ＩＴの全般統制として、ITセキュリティに関する対応の必要性が求められています。

その中でも、ＩＤ管理(アイデンティティマネージメント)分野については、セキュリティポリシーを実装する上での共通基盤として注目されている分野です。内部統制とアイデンティティ・マネジメントの関連をＷＧ討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を狙って行きたいと考えています。

重点整理テーマとしては、以下の3つを掲げました。

1. アイデンティティ･マネジメントの意義
2. 内部統制におけるアイデンティティ・マネジメントの位置づけ
3. アイデンティティ・マネジメント導入にかかる導入方針

2. 年間活動計画

6/22 に第１回のワークショップを開催し、本ＷＧでの討議内容について議論しました。

その後のワークショップでは、トーマツ監査法人の丸山さんを招待し監査側の立場からのご意見を伺いました。

8/25には正式に第１回のＷＧを発足し活動を開始いたしました。

現在まで、アイデンティティ・マネジメントとＩＴ内部統制を構築するためのフレームワークであるCOBIT との関連の議論や、そもそもアイデンティティ・マネジメントはなぜ必要なのかなど、各社から活発なご意見をいただきました。

11月、12月については、テーマ毎に分科会を設置し討議を進めます。

1月以降は成果物の取りまとめ作業を行ない3月末に完成予定です。

3. 予定成果物

序章．本書の目的
１章．ID管理とは
２章．ID管理の意義
３章．内部統制におけるID管理の位置づけ
４章．導入指針
５章．まとめ
付録．用語解説、関連資料、市場動向など

◆ WGメンバー（１１月現在）（社名昇順）

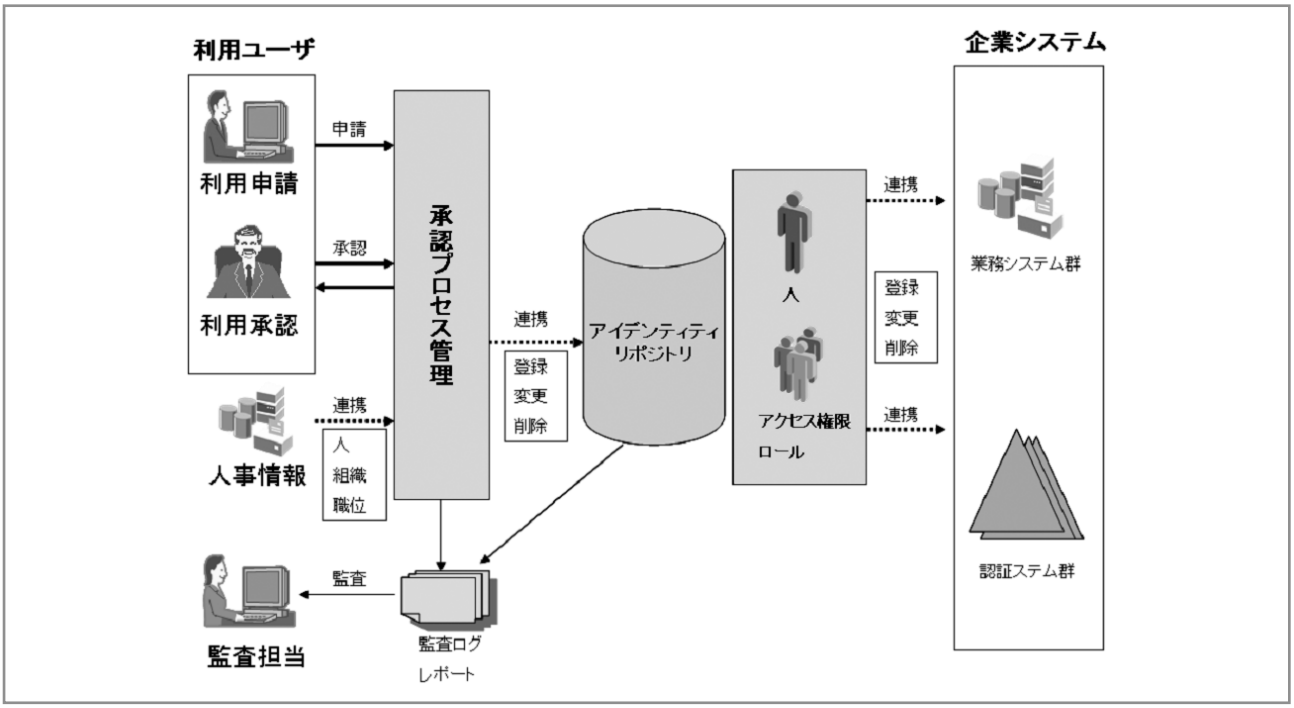
幹事会社

グローバルセキュリティエキスパート株式会社
日本オラクル株式会社
日本ＣＡ株式会社
日本ヒューレット･パッカード株式会社

メンバー会社

株式会社アクシオ
伊藤忠テクノソリューションズ株式会社
ＮＥＣネクサソリューションズ株式会社
ＮＴＴコミュニケーションズ株式会社
キャノンシステムソリューションズ株式会社
京セラコミュニケーションシステムズ株式会社
東芝ソリューション株式会社
日商エレクトロニクス株式会社
日本アイ･ビー･エム株式会社
日本アイ･ビー･エム　システムズ･エンジニアリング株式会社
日本電気株式会社
日本ユニシス株式会社
株式会社ネットマークス
株式会社日立製作所
富士通株式会社
株式会社富士通ソーシャルサイエンスラボラトリ
三菱電機情報ネットワーク株式会社
リコー･ヒューマンクリエイツ株式会社

合計:22社　41名



会員企業ご紹介⑱

LANDesk Software 株式会社

http://www.landesk.co.jp/

LANDesk® An Avocent® Company

Avocentのグループ会社であるLANDeskは、システム、セキュリティとITサービスの効率的な管理を実現する、費用対効果の高いソリューションを提供しています。LANDesk®ソリューションは、デスクトップ、サーバとモバイルデバイスなどのIT管理を簡単にし、リアルタイムの変更管理機能により、ITサービスの提供効率を飛躍的に向上させます。

- **10年以上にわたり、システム管理市場でトップベンダとして認知される**
- **全世界で何十億ノードがインストール済み**
- **TCOが低く、サーバインフラや帯域幅への負荷が少ない**
- **LANDesk® Management Suite 8の平均収率は、わずか90.5日で846%（2004年 IDC調べ）**

歴　史

LANDesk は 1985 年に LANSystem として設立。1991 年に Intel に買収されて同社の LANDesk 事業部となるが、2002 年にソフトウェアベンダとして独立。2006 年には Avocent に買収され、Avocent グループ内の独立事業部門として今日に至る。

世界展開

全世界 290 社以上の代表的なシステムインテグレーターを販売代理店としています。本社は米国ユタ州ソルトレーク市ですが、ブラジル、中国、フランス、ドイツ、アイルランド、イタリア、日本、メキシコ、イギリスに支社があり、全世界 18 カ国に 525 名の従業員がいます。

財　務

- 毎年 30%増収を継続
- 売上げの半数以上は北米外から
- 12 四半期連続で増収・増益

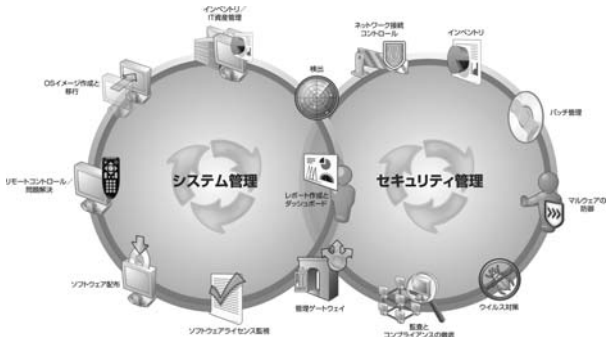
代表的なソリューション

- LANDesk® Management Suite
  異種混在環境にある全てのクライアントシステムを同一のコンソールから集中管理できるシステム管理ソリューション。IT システム統制に必要な管理を自動化し、コンプライアンス実現のための運用負荷を軽減します。

- LANDesk® Security Suite
  企業が所有する全てのデバイスのセキュリティ管理を包括的に実行し、ネットワークのエンドポイントセキュリティの確保をより確実にするセキュリティソリューション。ハードウェアに依存せず、インフラへの追加投資なく、セキュリティポリシーの徹底を実現します。

- LANDesk® Antivirus
  LANDesk Management Suite または Security Suite のアドオンとして使用するウイルス対策ソリューション。企業ユーザに特化し、システムとセキュリティの運用管理の一部として、共通の管理コンソールからウイルス対策も実行できます。

- LANDesk® Server Manager
  サーバの構成管理とセキュリティ保全をクライアントシステムと同一の管理コンソールから実施できるサーバ管理ソリューション。LANDesk Management Suite との併用により、デスクトップからサーバまで全てのシステムを共通コンソール、共通データベースで統合管理できます。



お問い合わせ先
LANDesk Software 株式会社
〒 105-0013 東京都港区浜松 1-27-16 浜松町 DS ビル 5F
TEL: 03-3435-8261　Email: Sales.Japan@landesk.com

株式会社ディアイティ

http://www.dit.co.jp/

安全、安心なネットワーク社会の実現にむけて

ディアイティが目指すのは、「安全・安心な高度情報通信ネットワーク社会」です。ディアイティは、その実現のために、技術・製品・サービスを提供するばかりでなく、情報セキュリティと安定した情報ネットワークを、社会インフラとして確立するためのあらゆる活動を行っています。

■ 企業戦略

ディアイティは、「安全・安心な高度情報通信ネットワーク社会」は以下7つの要素から構成され、これらが調和を取りながら発展することが、「安全・安心な高度情報通信ネットワーク社会」の実現につながると考えます。「技術」「製品」「サービス」の要素をディアイティの企業活動のテーマとしてとらえ、「モラル」「コンセンサス」「制度」の要素を業界活動への積極的参加により実現します。

○**知識と知恵**／　技術、製品、サービス、モラル、コンセンサス、制度を生み出す源であり、人類が過去から現在までに入手してきた知識と、その過程で習得した叡知

○**技　術**／　製品やサービスを創造するための基盤

○**製　品**／　コンピュータ、ルータ、ファイアウォールなど情報化社会の部品

○**サービス**／　ITシステムの構築、運用支援、障害対応などシステムの構築から運用までのすべてと、セキュリティコンサルティング、セキュリティ監査、教育など

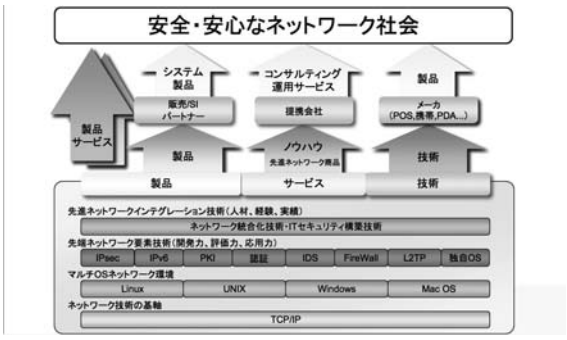
○**モラル(リテラシー)**／　利用者の知識や倫理観などの行動様式

○**コンセンサス**／　リスクとコスト、安全性と利便性など拮抗する要素の社会的合意

○**制　度**／　情報セキュリティ監査制度、ISO27000、ISO15408、個人情報保護法など

■ディアイティの技術基盤とサービス

長年の経験に基づいた技術・ノウハウを基に、さまざまなサービスを提供しています。



■ディアイティの事業内容

▼ネットワークプロダクト

ネットワーク社会の基本となるのがネットワーク製品です。20余年に及ぶコンピュータネットワーク事業の経験と知識を基に、市場のニーズに合ったハードウェア、ソフトウェアを国内外より取り揃え、コストパフォーマンスのよいネットワーク製品をご提供しています。

▼セキュリティプロダクト

高度に発達、進化し続ける情報通信社会において、企業内外からのセキュリティの脅威をいかに防ぐかは、企業にとっての重要課題であり使命です。PCまわりからゲートウェイまわり、さらに安全な通信を確保する為の暗号化通信にいたるまでの、セキュリティ製品をご提供しています。

▼インテグレーション

単なる製品の販売ではなく、UNIX、Linux、Mac、Windowsの豊富な知識と経験を基に、お客様のさまざまなニーズに合った安全・安心なネットワーク構築をするための、設計・インテグレーションを行っています。お客様のネットワークの障害にいち早く対応できるよう保守サービスや管理ツールの提供も行っています。

▼情報セキュリティコンサルティング

情報セキュリティポリシーの作成から、脆弱性検査、種々の認定取得、監査にいたるまでの情報セキュリティに関するコンサルティング／サービスを通じて、お客様の事業継続、企業価値を高めることに貢献できるよう、経験豊富なスタッフがお手伝いいたします。

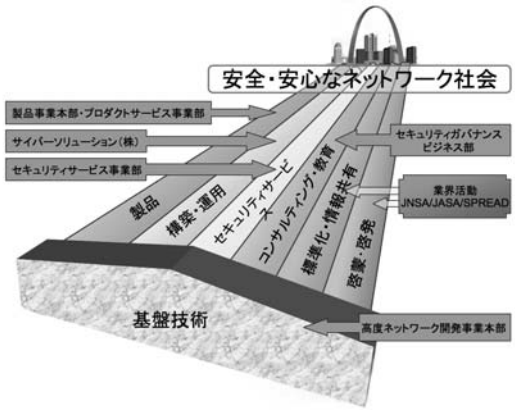
▼資格／教育

企業にとって重要な資産は人材です。人材を育成することが、安心・安全なネットワーク社会の実現にとって欠くことのできない要素です。セキュリティの基本からCISSPなどの資格取得までの教育プログラムをご用意しております。

▼研究／開発

明日の情報セキュリティの基盤となる技術を研究開発するとともに、独自の技術を開発し、明日のネットワーク社会に貢献します。

各事業部門が必要な要素をそれぞれ担い、事業活動を実施しています。



● 本社移転のご案内 ●

旧東陽町オフィスと新高円寺オフィスを統合し、新本社オフィスに11月6日移転しました。

〒135-0016 東京都江東区東陽三丁目23-21
プレミア東陽町ビル

Tel：03-5634-7651（大代表）

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■

○SafeProtector ～クライアント型セキュアOS ～

SafeProtectorは、アプリケーションの実行を、組織（企業・団体）のセキュリティポリシーに従い、システム管理者により集中管理することが可能です。また、アプリケーションからデータファイルへのアクセス制御も可能です。

SafeProtectorは、未許可アプリケーションのインストールをブロックし、マルウェア対策、不正アクセス防御、ファイル交換ソフトによる情報漏洩対策を実現します。

【製品情報詳細】
http://www.jtsl.co.jp/product/safeprotector/index.html

◆お問い合わせ先◆
日本高信頼システム株式会社
E-mail: sales_jts@jtsl.co.jp

○『Pointsec for PC』(ポイントセックフォー PC)

Pointsec for PC は、PCのハードディスク全体の暗号化によるアクセスコントロールを実現し情報漏えいを防ぎます。管理者がセキュリティ ポリシーを設定し、エンド ユーザーはポリシーを変更できません。さらに Smart CardやeTokenなどと連携したプリブート認証でも使用できます。世界で500万、国内でも50万ライセンスの出荷実績があり、世界で最も広く展開されているHDD暗号化ソリューションです。

【製品情報詳細】
www.pointsec.co.jp

◆お問い合わせ先◆
ポイントセック株式会社
TEL: 03-3560-3177
E-mail: hajime.ishii@pointsec.com

○「CompuSec」

PCの起動前認証、ハードディスク丸ごと暗号化ソフトです。PCの盗難・置き忘れ、PCの廃棄時、リースPCの返却時の際、第三者による不正利用から大切なデータを守ります。従来のファイルやフォルダ単位の暗号化とは違い、ハードディスク内全てを暗号化しているため、暗号化を意識して作業する必要はありません。またリムーバブルメディアの暗号化にも対応しており、クライアントPCの情報漏えい対策に最適です。

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

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

JNSA 西日本支部主催セキュリティセミナー

ＪＮＳＡ西日本支部　中小企業向け個人情報保護対策ＷＧメンバー
富士通関西中部ネットテック株式会社　嶋倉　文裕

個人情報保護法施行１年を経過！
迫りくる「中堅・中小企業に求められる内部統制への対応」

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９回セキュリティセミナー　個人情報保護法施行1年を経過！　迫りくる「中堅・中小企業に求められる内部統制への対応」が、近畿経済産業局、大阪商工会議所、財団法人関西消費者協会、社団法人関西経済連合会、財団法人ひょうご情報教育機構、NPO滋賀県情報基盤協会、NPOなら情報セキュリティ総合研究所、NPO情報セキュリティ研究所、NPO GIS総合研究所の後援のもと､7月21日（金）に大阪市にある大阪国際会議場において開催されました。当日は、あいにくの雨模様でしたが108名の方にご来場頂きました。
今回は「内部統制」をテーマとし、監査法人の立場から、また法曹界の立場から、およびJNSA研究員の立場からそれぞれご講演頂いたほか、フォレンジック調査を通じ、組織内部の情報セキュリティ事故発生時における現状と将来についてのご講演、および中小企業における個人情報保護対策WGから成果の報告がありました。本セミナーは、関西圏に多い中堅・中小企業にとって､「企業の内部統制強化」がどのように影響を及ぼすのか、また、その結果として、どのようなセキュリティ対策が、新たにクローズアップされていくのかを明らかにすることとなりました。簡単に内容をご紹介します。

まずプログラムの最初に井上JNSA西日本支部長から､「関西圏に多い中堅・中小企業にとって､「企業の内部統制強化」がどのように影響を及ぼすのか、また、その結果として、どのようなセキュリティ対策が、新たにクローズアップされていくのか、を明らかにすること」と本セミナーへの期待の挨拶があり、あわせてJNSA、各部会・WGの調査活動状況、および西日本支部の取り組みについても紹介がされました。

続いて最初の講演として、監査法人の立場から「財務報告に係る内部統制の評価と監査制度　IT部門におけるポイント」と題し、監査法人トーマツ パートナー 公認会計士 丸山満彦様からご講演を頂きました。丸山様からはまず、内部統制が注目されている背景と、いわゆるJ-SOXとはなにを指しているか、についてご説明を頂きました。さらに制度概要、内部統制の定義、重要なポイント、範囲、評価について説明を頂き、さらにIT統制の位置づけ、その概要についてご紹介して頂きました。その中で重要なポイントとして、自ら評価し管理体制に問題がないことを報告書にすること、また外部監査人はその報告書を監査し、結果の正しさのみならずプロセスも含めてその適正を保証することであり、結果適正ではないとの指摘がありました。これは今までの会社が経験したことがないことだという、説明がありました。さらに評価の対象は連結対象のみならず委託先にも及ぶことも指摘されています。これは、非上場の中小企業にとってもJ-SOXが他人事ではない、ということを指します。また最後にＩＴ部門への期待として、IT全般統制が信頼できると、IT業務処理統計のサンプル数が減少でき、評価コストも減少できる、との紹介がされました。本法律は平成20年4月1日以降に開始する事業年度から適用されることとなりますが、２年弱の間でやるべきことが本講演でいろいろ明確になり、中小企業にとってもこの期間に準備すべき方向が見えてきた、と期待されます。

イベント開催の報告

「監査法人トーマツ」丸山氏のご講演

2番目の講演は、「組織内部のフォレンジック調査における現状と将来」と題し、ネットエージェント株式会社 取締役の伊原秀明様からご講演を頂きました。フォレンジックは、まだ馴染みの薄い分野ではありますが、不正アクセスなどのハイテク犯罪に遭遇したときに必要な行動について、貴重な指摘、紹介を頂きました。その中で、情報システム部門の担当者がどこを調べれば良いかが判らないにも拘らず、いろいろ手探りで調査を行ってしまい、かえって証拠が残らなくなってしまうことがあるということの指摘がありました。必要な行動としては、まず現状保全する、ということでした。また、被害が発生しているにも拘らず業務に重要なサーバのため停止できない、という理由により稼動し続けるサーバが多い、との指摘がありました。これは、被害にあっているにも関わらずサーバを稼動し続け、より被害を拡大する、例えば個人情報などの重要情報の漏洩が拡大する危険性よりも、目の前の自分たちの業務を優先している、ということの指摘でした。伊原様からは、事故の発生を前提とし、発生時における体制の構築、および被害にあっているにも拘らずサーバを稼動し続け被害を拡大するような誤った判断を防ぐ体制や教育が必要、との貴重な提言を頂きました。また、常日頃から事故発生直後から調査に着手可能な体制、連絡先の確保も重要、との指摘も頂きました。内部統制の運用、事業継続という観点からもフォレンジックを通して見えてきたこれらの課題への対応の重要性を強く感じることができた内容でした。

3番目の講演は昼休み後の最初の講演で、法曹界の立場から「中堅・中小企業の個人情報保護・情報セキュリティと内部統制」と題し、稲垣隆一法律事務所 弁護士　稲垣隆一 様からご講演を頂きました。

講演の冒頭から稲垣先生の「真剣に考えていますか？」、「今日、何人の経営者のかたがこのセミナーに参加されていますか？」という厳しく、また非常に印象的なご発言がありました。本講演では、過去の情報漏洩事件を例にそれぞれの本質的な問題について掘り下げてご説明を頂きました。そのなかで稲垣先生が一番言いたかったものとして感じられたのが、冒頭にもあった「真剣に考えているのか」ということでした。例えば、宇治市の個人情報漏洩事件における委託先から個人情報が漏洩した原因のひとつに、再委託・再々委託における誤った判断を指摘されています。情報漏洩が発生する過程における誤った判断をした人の存在、その人はなぜそのような判断をくだしたのか、それ以前に判断を任せるに足る人材だったのか、セキュリティ教育を十分にうけ理解をしている人であったのか、ヒューマンエラーの要因を為す人間の不安定行動にまで言及されました。情報セキュリティ対策を考えるうえで、どこまで「真剣に考えているのか」という問題の貴重な事例でした。さらに、中小企業が抱える現在の情報セキュリティ対策の課題についても触れて戴きました。中小企業の情報セキュリティ対策は、まだまだ脆弱であり、経営者にとって情報セキュリティや個人情報保護が経営課題になっていません。そのような中小企業はまず、自らの力で対策を構築する組織体制、実現可能なスケジュールをたて、そのための体制、業務の振り分けを行うこと、経営課題とするために基本方針の確認、リスクの把握の必要性、などを明確化する必要がある、との提案を戴きました。

「稲垣隆一法律事務所」弁護士 稲垣先生のご講演

続いて､「内部統制とセキュリティのルール」と題し、日本ネットワークセキュリティ協会 研究員・独立行政法人情報処理推進機構 研究員の園田道夫様からご講演を頂きました。情報セキュリティは、ISMS、15408、個人情報保護、Ｐマークといろいろ対応してきたなかで、今度は内部統制が法制化されるということになったが、いったい何をどうして、どう棲み分け使い分けたらいいのか、そもそも棲み分けなければならないのか、などについて説明を頂きました。J-SOXの目的は会計上の不正行為の防止、翻れば正しいことの証明であり、不正行為を防ぐには単独処理をなくす、相互チェックの仕組みが大前提になる､という解説がありました。不正行為の検出には、ISMSやＰマークの管理項目としての従来から実施している対策のアクセスコントロールやログの取得を行うことであり、大きく変わることではない、ということの説明がありました。そして、会計における不正行為は、一従業員の行為よりむしろ経営層の行為であることから、これまでの情報セキュリティ対策として行われきた従業員の行動の監視、監査ではなく経営者の行動の監視、監査が必要、という指摘がありました。

最後に、中小企業向け個人情報保護対策WGから「個人情報保護法から1年、中小企業の対策と実情」と題し、ＷＧリーダー・伊藤忠テクノサイエンス株式会社　市川 順之様から講演を戴きました。個人情報保護法が施行されてから、この一年の状況についての説明と、昨年10月のJNSA西日本支部主催セミナーNSF in Osakaで来場者の皆さんに回答して頂いた個人情報保護に関するアンケート結果の報告、WGの活動を通してみえてきた中小企業の問題についての説明がありました。さらに、成果物としてのヒアリングシートの紹介が行われるとともに、本講演では来場者の方とのディスカッションの時間を設けました。大きな会場で、公の場での発言される来場者のかたは少なかったのですが、その中で「経営者の理解の乏しさ」という訴えがありました。稲垣先生のご講演にもありましたが、経営者にとって情報セキュリティが経営課題になっていない現実を垣間見ました。最後に井上ＪＮＳＡ西日本支部長からは、今回のようなセミナーに加えて、来場者を経営者に絞ってのインターアクティブな小セミナーも開催して見たいとの提案もさせて戴きました。

おわりに

非上場の中小企業にとってもJ-SOXは無関係ではなく取引企業の上場企業から同等なことは求められるという現実を認識したセミナーだったのではないか、と思います。J-SOXが適用される平成20年４月１日以降に開始する事業年度までには、まだ一年半ほどの時間がありますが、中小企業にとってこの期間はJ-SOXへの対応を検討、実施する貴重な時間であり、けっして余裕のある時間ではない、と感じました。また、これまでは情報セキュリティが経営課題として取り上げ難い現状にありましたが、今後は中小企業においてもJ-SOX対応に取り組む上で健全な情報セキュリティ対策こそが必須不可欠なものとして認識されるのでは、という期待を抱くことのできたセミナーになった、と感じました。

イベント開催の報告

インターネット安全教室まつり

『インターネット安全教室まつり』は好評のうち終了いたしました。
ご来場有り難うございました。

経済産業省とJNSA（NPO日本ネットワークセキュリティ協会）では、10月15日（日）にお台場アクアシティにて、「インターネット安全教室まつり」を開催しました。このイベントは、一般の方々がインターネットを安全に使うにはどうすればよいかを楽しく学べるイベントとして企画し、家族連れの方々など1000名を超える方が当日参加されました。

さわやかな秋らしい1日で、大勢のお子さんたちやカップルなども足を止め、はなわさんのエネルギッシュなベースギターとお話や、ヨーヨー釣り、射的、輪投げなどを楽しみながら、インターネットを安全に使うためのちょっとしたヒントを皆さんに考えていただきました。

◆名　称：「インターネット安全教室まつり」
http://www.jnsa.org/caravan/
◆日　時： 2006年10月15日（日）　11:00 ～ 17:00
◆場　所： アクアシティお台場3Ｆ アクアアリーナ
◆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

ステージでは、お笑いタレントのはなわさんをお招きして「はなわと遊ぼう！クイズ大会＆ライブ」と称して、全国各地の「インターネット安全教室」とライブトークを行ったり、安全教室生徒代表のはなわさんと一緒にセキュリティクイズを楽しんだりしました。

はなわさんのステージは、さすがに迫力満点で、ちょっとしたウイルスや詐欺師なんかは退散してしまいそうなパワーに溢れていました。そのパワーに吸い寄せられるように、実に多くの方々にお集まりいただき、通路いっぱいに広がったお客様で通り抜けるのもままならない状態でした。

午前11時のアクアアリーナ開場と同時に、多くの方々が立ち寄られ、はなわさんのステージが始まるまでの間、パネルをご覧になったり、体験コーナーでPCを操作されたりしていました。さすがにはなわさんのステージは満員で、ステージの周りは、手に手に色とりどりの風船を持ったお子さんやお父さん、お母さん、カップルなどで埋め尽くされました。

インターネットのお祭りらしく、今まで経済産業省とJNSAが主催してきた全国の「インターネット安全教室」の開催地のみなさまも、Webカメラで参加くださり、一緒になって「おまつり」を楽しんでいただけました。放送局のような業務用の機材ではなく、手軽に使える家庭用の機材でも、楽しいコミュニケーションが実現できることを、改めて体験できたのではないかと思います。パソコンの便利さを活かした、しかも安全な使い方を、もっともっと大勢の方に知って

もらいたいと思います。

また、午後2回目のステージとして「インターネットを楽しもうスペシャルステージ」が開催されました。全国で開催されている「インターネット安全教室」で講師をされている先生方による、インターネットの便利な使い方、活用の仕方、ブログの作り方などを教えてもらいました。ステージ上でお料理を作ってみたり、スタッフが試食をしたり、また、参加者に差し上げた「CD-ROM」の映像に出てくる悪役の黒子君も登場し、会場を沸かせていました。

ステージの周りでは、ヨーヨー釣り、射的、輪投げなどをやりながらセキュリティを楽しく学べる「セキュリティ村」や、全国の「インターネット安全教室」共催団体や情報セキュリティに関するパンフレットやパネル展示、実際にPCをさわりながらいろいろと体験したり学べるセキュリティ体験コーナーなどを設置し、親子や家族連れで楽しく遊べるイベントとして開催しました。

セキュリティ村のお祭りの出し物の周りには、子供さんたちが大勢集まり、とってもにぎやかでした。自動車事故にあわないようにするために、どうしたら良いのかご家族で話されることがあると思いますが、同じように、インターネットを安心して利用するための注意点を、ご家庭でも気軽にお話しされるようになっていただきたいな、と感じました。そのためにも、配布されたCD-ROMなどをご家族でご覧になり、一緒に考えていただければと思います。

「セキュリティ体験コーナー」のブース展示にも、大勢の方々が足を停められていました。「ドラえもん のび太のインターネット大冒険(小学館提供)」「ウイルス資料館」「警察庁キッズパトロール」「キーロガーによる盗聴デモ」「迷惑メール疑似体験」など、年齢に関係なく多くの方々が、用意されているパソコンを触っていました。

パネル展示には、2003年から現在までの「インターネット安全教室開催地一覧」の大きなパネルが掲示されました。これを見ると、北海道から沖縄、石垣島まで、全国各地で開催されていることが一目瞭然です。インターネットが社会基盤として一般社会へ普及してきた今、市民としてインターネットという道具をどのようにしたら安全・安心・快適に使えるかを身に付けることは大切なことになってきています。便利な道具を上手に使いこなすための、ちょっとしたコツを知ってゆくことで、もっと心豊かな生活が送れるのだと思います。これからもみなさまと一緒に、インターネットを上手に使う方法を考えてゆきましょう。

尚、ご意見や気が付かれたことなどがあれば、ぜひ運営事務局までご連絡くださるようお願いいたします。

2006 年度
「インターネット安全教室」

～パソコンや携帯電話で思わぬトラブルや犯罪にまきこまれないために～

誰でも手軽にインターネットに接続できるようになった今日、ウイルス感染、詐欺行為、プライバシー侵害など情報犯罪の被害にあう危険性がますます高くなってきています。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、これらの被害を防ぐことはできません。
こうした状況をふまえ、経済産業省と NPO 日本ネットワークセキュリティ協会（JNSA）では、家庭や学校からインターネットにアクセスする人々を対象に、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を 2003 年度より開催してまいりました。2006 年度の開催状況は以下のとおりです。

【開催概要】

［主　　催］経済産業省、NPO 日本ネットワークセキュリティ協会（JNSA）

［後　　援］警察庁、その他

［開催一覧］次の一覧をご覧下さい。（2006 年 12 月 8 日現在）

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

2006 年度「インターネット安全教室」開催一覧

日　程	開催地	共催団体	会　場
5月21日(日)	長野県	上田市マルチメディア情報センター	神科新屋生活改善センター
5月21日(日)	長野県	上田市マルチメディア情報センター	神科新屋生活改善センター
4月12日(水)	福井県	(特)ナレッジふくい	福井県生活学習館　ユー・アイふくい
5月12日(金)	福井県	(特)ナレッジふくい	福井市フェニックスプラザ
5月21日(日)	長野県	上野が丘公民館　青少年育成懇談会	上田市神科新屋生活改善センター
5月27日(土)	石川県	石川県健康福祉部子ども政策課　児童育成グループ (特)ナレッジふくい	石川県青少年総合研修センター (ユースパルいしかわ)
6月25日(日)	福井県	福井県生涯学習館(ユー・アイふくい) (特)ナレッジふくい	福井県生活学習館　ユー・アイふくい
6月29日(木)	千葉(新規)	NPO法人 松戸ITVネットワーク	松戸市民会館3F 301号室
7月6日(木)	長野県	上田市マルチメディア情報センター	市民プラザゆう
7月10日(月)	長野県	ひかり自治会、上田市マルチメディア情報センター	ひかり自治会館
7月15日(土)	愛媛県	愛媛県IT推進協会	アイテムえひめ(愛媛県国際貿易センター) 4F会議室
7月27日(木)	奈良県	NPOなら情報セキュリティ総合研究所 奈良県社会教育センター	奈良県社会教育センター
7月30日(日)	神奈川県	NPO情報セキュリティフォーラム	横浜市美しが丘西地区センター
8月3日(木)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
8月4日(金)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
8月4日(金)	鹿児島県	鹿児島大学学術情報基盤センター	鹿児島大学学術情報基盤センター 第1端末室・第2端末室
8月8日(火)	長野県	上田市マルチメディア情報センター、上田市教育委員会	上田市マルチメディア情報センター
8月12日(土)	福岡県	北九州市、財団法人ハイパーネットワーク社会研究所	ウエルとばた2階多目的ホール
8月22日(火)	埼玉県	NPO情報セキュリティフォーラム	埼玉県生活科学センター 総合棟7階　研修室
8月22日(火)	愛媛県	愛媛県IT推進協会	伊方町立瀬戸中学校　3Fコンピュータ教室
8月23日(水)	神奈川県	NPO情報セキュリティフォーラム	足柄上合同庁舎　2階大会議室
8月25日(金)	神奈川県	NPO情報セキュリティフォーラム	川東タウンセンターマロニエ　集会室202
8月27日(日)	島根県	NPO法人プロジェクトゆうあい	松江市市民活動センター　201,202研修室

9月9日(土)	神奈川県	NPO情報セキュリティフォーラム	平塚合同庁舎　別館1階　大会議室
9月13日(水)	神奈川県	NPO情報セキュリティフォーラム	厚木合同庁舎　新館4階　大会議室
9月20日(水)	福井県	(特)ナレッジふくい	福井市映像文化センター　メディア実習室
9月21日(木)	神奈川県	NPO情報セキュリティフォーラム	横須賀合同庁舎　5階　大会議室
9月25日(月)	神奈川県	NPO情報セキュリティフォーラム	相模原合同庁舎　3階　第一会議室
9月27日(水)	神奈川県	NPO情報セキュリティフォーラム	フォーラム南太田　3階　大研修室
9月29日(金)	兵庫県	財団法人ひょうご情報教育機構	三宮研修センター
9月30日(土)	奈良県	NPOなら情報セキュリティ総合研究所	帝塚山大学学園前キャンパス 16号館6F・564教室
9月30日(土)	神奈川県	NPO情報セキュリティフォーラム	小田原合同庁舎　3階　E・F会議室
10月7日(土)	岡山県	岡山県インターネットセキュリティ対策連絡協議会	くらしき健康福祉プラザ(倉敷市笹沖)
10月14日(土)	大阪府	大阪工業大学、NPO GIS総合研究所	大阪工業大学　枚方キャンパス　情報科学部
10月14日(土)	大分県	財団法人ハイパーネットワーク社会研究所	大分県立芸術文化短期大学　人文棟 大講義室
10月15日(日)	富山県	富山県総合情報センター	富山県ITセンター　情報工房施設
10月22日(日)	宮崎県	福祉情報ボランティア宮崎、宮崎公立大学	宮崎公立大学
10月25日(水)	兵庫県	財団法人ひょうご情報教育機構	四季の森生涯学習センター
10月28日(土)	広島県(新規)	広島市情報政策課	広島市まちづくり市民交流プラザ マルチメディアスタジオ
10月28日(土)	静岡県	しずおかITフェア実行委員会 (静岡県、静岡情報産業協会、(社)静岡県情報化推進協会)	「B-nest」静岡市産学交流センター
10月28日(土)	滋賀県	NPO滋賀県情報基盤協議会、滋賀県立彦根工業高等学校	滋賀県立彦根工業高等学校
10月28日(土)	新潟県	NPO新潟情報セキュリティ協会	朱鷺メッセ　新潟コンベンションセンター 2階　中会議室　201
10月29日(日)	神奈川県	NPO情報セキュリティフォーラム	秦野市立本町公民館　2階　大会議室
10月31日(火)	京都府	ITコンソーシアム京都	京都府消費生活科学センター
11月7日(火)	茨城県	茨城県消費生活センター、龍ヶ崎市	龍ヶ崎市役所
11月8日(水)	兵庫県	財団法人ひょうご情報教育機構	淡路夢舞台国際会議場
11月10日(金)	秋田県(新規)	NPO白神ねっと	能代キャッスルホテル平安閣
11月11日(土)	北海道	NPOくるくるネット	室蘭市中小企業センター
11月14日(火)	神奈川県	NPO情報セキュリティフォーラム	藤沢市役所　防災センター　6階　会議室
11月15日(水)	神奈川県	川崎市、NPO情報セキュリティフォーラム	ラゾーナ川崎プラザソル5階ホール
11月17日(金)	神奈川県	NPO情報セキュリティフォーラム	鎌倉生涯学習センター　4　第6集会室
11月17日(金)	福井県	(特)ナレッジふくい	福井県敦賀市西公民館
11月19日(日)	沖縄県(新規)	石垣市、八重山支庁、竹富町、石垣市商工会	石垣市民会館中ホール
11月23日(木)	三重県	NPO東海インターネット協議会、 財団法人 人工知能研究振興財団	四日市市総合会館　7F　第1研修室
11月25日(土)	千葉県	NPO法人松戸ITVネットワーク	松戸市民劇場　第3会議室
11月26日(日)	鳥取県(新規)	NPO法人はっぴぃりんく、 鳥取県ジゲおこしインターネット協議会	保健福祉センターなわ
12月2日(土)	北海道(新規)	旭川情報産業事業協同組合	旭川市科学館
12月3日(日)	愛知県	NPO東海インターネット協議会、 財団法人 人工知能研究振興財団	今池ガスビル7階　B会議室
12月6日(水)	山形県(新規)	山形大学　学術情報基盤センター	山形大学　小白川キャンパス　127教室
12月8日(金)	青森県	財団法人八戸地域高度技術振興センター	八戸インテリジェントプラザ　アイピーホール
12月23日(土)	石川県	NPO法人STAND	石川ハイテク交流センター
1月20日(土)	神奈川県	NPO情報セキュリティフォーラム	浦舟複合施設10階 みなみ市民活動センター研修室1・2
1月21日(日)	神奈川県	NPO情報セキュリティフォーラム	秦野市立南が丘公民館　2階　大会議室
1月26日(金)	和歌山県	NPO情報セキュリティ研究所	新宮市人権教育センター
1月27日(土)	福島県	NPO法人日本コンピュータ振興協会	福島県文化センター視聴覚室
1月28日(日)	熊本県	NPO熊本県次世代情報通信推進機構	パレアホール(くまもと県民交流館パレア)
2月5日(月)	神奈川県	NPO情報セキュリティフォーラム	横浜市鶴見区役所　大会議室
2月9日(金)	神奈川県	NPO情報セキュリティフォーラム	葉山町立保育園・教育総合センター会議室
2月17日(土)	長崎県	長崎県立大学、県立長崎シーボルト大学	長崎県立大学、県立長崎シーボルト大学 ※テレビ会議システムによる同時開催
2月22日(木)	香川県	香川県情報サービス産業協議会 香川県プロバイダ等防犯連絡協議会	e-とぴあ・かがわ「BBスクエア」
2月(予定)	滋賀県	NPO滋賀県情報基盤協議会、滋賀県立八幡工業高等学校	滋賀県立八幡工業高等学校
2月(予定)	滋賀県	NPO滋賀県情報基盤協議会、滋賀県立瀬田工業高等学校	滋賀県立瀬田工業高等学校
3月2日(金)	神奈川県	NPO情報セキュリティフォーラム	厚木シティプラザ5階 厚木市ヤングコミュニティセンター
3月10日(土)	北海道(新規)	公立はこだて未来大学	公立はこだて未来大学
3月10日(土)	神奈川県	NPO情報セキュリティフォーラム	平塚合同庁舎　別館1階　大会議室
3月(予定)	千葉県	NPO法人幕張メディアアソシエイツ	ベイタウン・コミュニティコア(打瀬公民館)
※以下開催検討中			
	徳島県		

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

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
参加費： 無料

経済産業省とNPO日本ネットワークセキュリティ協会では2003年度より開催している一般の方向けの情報セキュリティ啓発セミナー、「インターネット安全教室」を今年度も全国各地で開催中です。

今年度の開催地は22～23ページの一覧表を、各地の開催要項につきましてはホームページをご覧ください。
http://www.jnsa.org/caravan/

2. 後援イベントのお知らせ

1．NET&COM 2007

会期： 2007年2月7日(水) ～ 9日(金) 10:00 ～ 17:00
主催： 日経BP社
会場： 東京ビッグサイト
http://expo.nikkeibp.co.jp/netcom/

2．PAGE2007

会期： 2007年2月7日(水) ～ 9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/

3．HOSTING-PRO 2007 Spring

会期： 2007年2月20日(火)
主催： HOSTING-PRO実行委員会
会場： 青山TEPIA
http://hosting-pro.jp/

3. JNSA 部会・WG 2006 年度活動

1．政策部会

(部会長:西本逸郎 氏/ラック)

調査事業や様々な基準･ガイドラインの策定、他団体との連携などを行う。

成果物目的のワーキンググループ

【セキュリティ被害調査WG】
(リーダー:山田英史 氏/ディアイティ)

例年通り、2006年1月～12月の1年間に発生する個人情報漏えい事件・事故を集計し分析する。本年度は、代表的な事例を掘り下げた分析にも取り組む予定。
予定成果物は、
1.「2006年 情報漏えい事件･事故集計速報」
2.「2006年 情報漏えいによる被害想定と考察」の予定。

【セキュリティ会計ガイドライン検討WG】
(リーダー:佐野智己 氏/凸版印刷)

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

予定成果物は、成果報告書、雑誌コラム等の対外発表など。

【セキュア･システム開発ガイドラインWG】
(リーダー:丸山司郎 氏/ラック)

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

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

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

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

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

【内部統制におけるアイデンティティ管理WG】
(リーダー:宮川晃一 氏/グローバルセキュリティエキスパート)

J-SOX法における「内部統制」の必要性が叫ばれている中で、ITの全般統制として、ITセキュリティに関する対応の必然性が求められている。

その中でも、アイデンティティ管理(アイデンティティ・マネージメント)分野については、 セキュリティポリシーを実装する上での共通基盤として注目されている分野である。

内部統制とアイデンティティ管理の関連をWG討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的とする。

予定成果物は、内部統制におけるアイデンティティ管理の定義とアイデンティティ管理システム設計ガイドライン

【情報セキュリティ力ランキングWG】
(リーダー:佐野智己 氏/凸版印刷)

企業における情報セキュリティ確保に向けた取り組みを情報セキュリティガバナンスの構築状況やステークホルダとのコミュニケーション、情報開示の充実度、社会貢献活動などの観点からランキングを算定し、定期的に公表する。

このランキングにより、上位に位置づけられた企業の取り組みを模範事例として公開し、どこまでやればいいのか分からないと言われる情報セキュリティに1つの方向性/トレンドを示したい。

勉強会目的のワーキンググループ

【スパイウェア対策啓発WG】
(リーダー:野々下幸治 氏/ウェブルート・ソフトウェア)

現在の対策啓発Webの更新作業と関係省庁や他団体との勉強会及び啓発を行う。

プロジェクト

【セキュリティ市場調査WG】
(リーダー:勝見勉 氏/リコー・ヒューマン・クリエイツ)

活動テーマとして、次のものを候補として掲げ、現在WGで討議中

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

予定成果物は、市場調査報告書など。

2. 技術部会

(部会長:二木真明氏/住商情報システム)

ネットワークセキュリティに関する調査・研究や、実証実験などを行なう。その他、予算を得た活動は、プロジェクトとして活動を進める。

成果物目的のワーキンググループ

【不正プログラム調査WG】
(リーダー:渡部章 氏/アークン)

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

予定成果物は、マルウェアの実証実験。

【ハニーポットWG】
(リーダー:園田道夫 氏/JNSA研究員)

2006年度は大規模ネットワークなどの情報解析技術の追求を行う予定。

予定成果物は、大規模ネットワークなどの情報解析技術の検討報告書など予定。

【WEBアプリケーションセキュリティ調査・検証WG】
(リーダー:加藤雅彦 氏/アイアイジェイテクノロジー)

昨年度、完成できていない成果物についての継続作業と、タイムリーな技術トピックなどについての検証イベントや勉強会などを行う予定。会合中心の作業から、オンラインの掲示板やメールを活用した活動へ移行していく形で検討したい。

予定成果物は、セミナー用コンテンツ一式・Webアプリケーションセキュリティ要件ガイドライン・攻撃手法研究レポート など。

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

【セキュアプログラミングWG】
（リーダー:伏見論 氏/情報数理研究所）
セキュアプログラミングに関する話題と問題点の調査・討議・課題の整理、その他JNSAの活動として有益と思われる成果を出せるような活動を行う。
成果物は検討中。

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

勉強会目的のワーキンググループ

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

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

プロジェクト

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

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

【セキュリティ啓発WG】
（リーダー:古川勝也 氏/マイクロソフト）
経済産業省の委託事業である「インターネット安全教室」の企画・運営を通してセキュリティ啓発活動を行う。今年度は独自開催の浸透に重点を置き、10月15日に普及啓発イベント「インターネット安全教室まつり」を実施した。

【セキュリティスタジアム企画・運営WG】
（リーダー:園田道夫 氏/JNSA研究員）
セキュリティスタジアムや技術セミナーを開催し、広くセキュリティ技術の啓発を行う。

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

4. 教育部会

（部会長：佐々木良一 氏／東京電機大学教授）

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

【CISSP行政情報セキュリティ CBK－WG】
（旧ISSJP-WG）

（リーダー：大河内智秀 氏/NTTコミュニケーションズ）

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

プロジェクト

【情報セキュリティ教育実証実験プロジェクト】

（リーダー：松田剛 氏/JNSA研究員）

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

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

【セキュリティリテラシーベンチマーク作成WG】

（リーダー：大溝 裕則氏/JMCリスクマネジメント）

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

成果物は、Web上で公開する「セキュリティリテラシーベンチマーク」。

5. ユーザー部会（新設）

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

6. 西日本支部

（支部長：井上陽一 氏/JNSA顧問）

JNSA西日本支部は関西に拠点を置くメンバー企業の協賛の下、西日本におけるネットワーク社会のセキュリティレベルの維持･向上並びに、日々高まる情報セキュリティへのニーズに応えるべく、先進性を追及すると共に、質の高いサービスを提供する事を目的として活動する。今年度も引き続き関西方面でのセキュリティ啓発セミナーを中心に活動を行う。

【セミナー運営WG】

（リーダー：井上陽一 氏/JNSA顧問）

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

【情報セキュリティチェックシートWG】

（リーダー：嶋倉文裕 氏/富士通関西中部ネットテック）

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

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

4. JNSA 役員一覧

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

理　事（50 音順）

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

監　事

土井　充	（公認会計士　土井充事務所）

顧　問

井上　陽一	
今井　秀樹	中央大学　教授
北沢　義博	霞が関法律会計事務所　弁護士
佐々木良一	東京電機大学　教授
武藤　佳恭	慶応義塾大学　教授
前川　徹	早稲田大学　客員教授
村岡　洋一	早稲田大学　教授
安田　浩	東京大学　教授
山口　英	奈良先端科学技術大学院大学　教授
吉田　眞	東京大学　教授

事務局長

下村　正洋	株式会社ディアイティ

5. 会員企業一覧（2006年12月1日現在　207社　50音順）

【あ】

(株)アークン
RSAセキュリティ(株)
(株)アイアイジェイ テクノロジー
(株)アイ･ソリューションズ
(株) ITサービス
(株) ITプロフェッショナル･グループ
(株)アイ･ティ･フロンティア
(株) IDGジャパン
アイネット･システムズ(株)
(株) IPイノベーションズ
アイマトリックス(株)
(株)アクシオ
(株)アクセンス･テクノロジー
(株)網屋(株)
アライドテレシス
アラクサラネットワークス(株)
(株)アルゴ21
(株)アルテミス
(株) ISAO New
(株)イージーネット New
伊藤忠テクノサイエンス(株)
学校法人 岩崎学園
(株)インストラクション
インターネット セキュリティ システムズ(株)
インテック･ウェブ･アンド･ゲノム･インフォマティクス(株)
(株)インテリジェントウェイブ
インテリジェントディスク(株)
インフォコム(株)
(株)インフォセック
(株)インプレスR＆D
ヴァイタル･インフォメーション(株)
ウインモバイル(株)
ウェブルート･ソフトウェア(株)
ウチダインフォメーションテクノロジー（株）
ウッドランド(株)
AT＆Tグローバル･サービス(株)
(株)エス･アイ･ディ･シー
エス･アンド･アイ(株)
(株)エス･エス･アイ･ジェイ
SSHコミュニケーションズ･セキュリティ(株)
(株)エス･シー･ラボ
NRIセキュアテクノロジーズ(株)
NECエンジニアリング(株)
NECソフト(株)
NECネクサソリューションズ(株)
NTTアドバンステクノロジ(株)
NTTコミュニケーションズ(株)
エヌ･ティ･ティ･コムウェア(株)
エヌ･ティ･ティ･コムチェオ(株)
(株) NTTデータ
(株)エネルギア･コミュニケーションズ
F5ネットワークスジャパン(株)
エムオーテックス(株)
エリアビイジャパン(株)
(株)大塚商会
オムロンフィールドエンジニアリング(株)
(株)オレンジソフト

【か】

(株)ガルフネット
兼松エレクトロニクス(株) New
(株)ギガプライズ
キヤノンシステムソリューションズ(株)
キヤノンマーケティングジャパン(株)
九電ビジネスソリューションズ(株)
京セラコミュニケーションシステム(株)
(株)クインランド
クオリティ（株）
KLabセキュリティ（株）
(株)クルウィット
(株)グローバルエース
グローバルセキュリティエキスパート(株)
(株)コネクタス

【さ】

サードネットワークス(株)
サーフコントロール ジャパン

サイバーソリューション(株)
サイボウズ(株)
(株)サイロック
サン電子(株)
サン・マイクロシステムズ(株)
(株)シーエーシー
(株)シー・エス・イー
(株)シーフォーテクノロジー
(株)ＪＭＣリスクマネジメント
ジェイズ・コミュニケーション(株)
シスコシステムズ(株)
(株)シマンテック
(株)ジャパンネット銀行 New
寿限無(株)
(株)翔泳社
(株)ジュリアーニ・セキュリティ＆セーフティ・アジア
(株)情報数理研究所
新日鉄ソリューションズ(株)
Sky（株） New
(株)ステラクラフト
住商情報システム(株)
住生コンピューターサービス(株)
セキュアコンピューティングジャパン(株)
(株)セキュアスカイ・テクノロジー
(株)セキュアブレイン
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム(株)
セコムトラストシステムズ(株)
セントラル・コンピュータ・サービス(株)
ソニー（株）
ソフトバンクBB（株）
ソラン(株)
ソラン・コムセック コンサルティング(株)
(株)ソリトンシステムズ
ソレキア(株)
(株)損保ジャパン・リスクマネジメント

【た】

大興電子通信(株)
大日本印刷(株)
(株)タクマ
TIS（株）
(株)ディアイティ
テクマトリックス(株)
デジタルアーツ(株)
(株)電通国際情報サービス
監査法人トーマツ
東京エレクトロン(株)
東京海上日動火災保険(株)
東京日産コンピュータシステム(株)
東芝ソリューション(株)
東洋ネットワークシステムズ(株)
ドコモ・システムズ(株) New
凸版印刷(株)
トップレイヤーネットワークスジャパン(株)
トリップワイヤ・ジャパン(株)
トレンドマイクロ(株)

【な】

(株)ニコンシステム
西日本電信電話(株)
日商エレクトロニクス(株)
日信電子サービス(株)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム　システムズエンジニアリング(株)
日本SGI（株）
日本オラクル(株)
日本高信頼システム(株)
日本コモド(株)
日本CA（株）
日本ジオトラスト(株)
(株)日本システムディベロップメント
日本セーフネット(株)
日本電気(株)
日本電信電話(株) 情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
日本ヒューレット・パッカード(株)
日本ユニシス(株)

ネクストコム(株)
(株)ネット･タイム
(株)ネットマークス
ネットワンシステムズ(株)
(株)野村総合研究所

【は】

(株)ハイエレコン
バリオセキュア･ネットワークス(株)
(株)ハンモック
東日本電信電話(株)
(株)日立システムアンドサービス
(株)日立製作所
日立ソフトウェアエンジニアリング(株)
(株) PFU
(株)フォーバル　クリエーティブ
富士ゼロックス(株)
富士ゼロックス情報システム(株)
富士通(株)
富士通エフ･アイ･ピー（株）
富士通関西中部ネットテック(株)
富士通サポートアンドサービス(株)
(株)富士通ソーシアルサイエンスラボラトリ
(株)富士通ビジネスシステム
富士電機アドバンストテクノロジー（株）
扶桑電通(株)
(株)フューチャーイン
(株)ぷららネットワークス
(株)ブリッジ･メタウェア
(株)ブロードバンドセキュリティ
(株)プロティビティジャパン
ポイントセック(株)

【ま】

(株)マイクロ総合研究所
マイクロソフト(株)
マカフィー（株）
松下電工(株)
みすず監査法人
みずほ情報総研(株)
三井物産セキュアディレクション(株)
(株)三菱総合研究所
三菱電機(株)情報技術総合研究所
三菱電機情報ネットワーク(株)
(株)メトロ

【や】

ユーテン･ネットワークス(株)
横河電機(株)

【ら】

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

【わ】

(株)ワイ･イー･シー
ワンビ(株) New

【特別会員】

特定非営利法人 アイタック
韓国電子通信研究院
ジャパン データ ストレージ フォーラム
特定非営利活動法人デジタル･フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院　工学系研究科
社団法人 日本インターネットプロバイダー協会
社団法人 コンピュータソフトウェア協会

6. JNSA 年間活動（2006 年度）

4月	4月11～12日	Lim Tec 2006後援	
	4月12日	JSOX法勉強会（主婦会館プラザエフ）	
	4月14～15日	拡大幹事会（熱海大観荘）	
	4月19日	第1回幹事会	
	4月20日	第1回西日本支部会合	
	4月24日	2006年度理事会（八重洲富士屋ホテル）	
	4月28日	第1回教育部会	
5月	5月11日	セキュアプログラミングワークショップ	
	5月11～12日	ソフトウェアテストシンポジウム2006大阪協賛	
	5月15日	第1回政策部会	
	5月16日	第3回迷惑メール対策カンファレンス後援	
	5月18日	第1回技術部会リーダー会	
	5月25～27日	第10回コンピュータ犯罪に関する白浜シンポジウム後援	
	5月30日	2005年度WG成果報告会（大手町サンケイプラザ）	
	5月30日	2006年度総会（大手町サンケイプラザ）	
6月	6月5～9日	Interop Tokyo 2006 後援	
	6月15日	第4回セキュアOSカンファレンス後援	
	6月17日	ISACA大阪支部設立20周年記念講演会後援	
	6月19日	第2回幹事会	
	6月21日	第1回技術部会	
	6月22日	第2回西日本支部会	
	6月26日	内部統制におけるアイデンティティ・マネジメント研究にむけてのワークショップ	
7月	7月6日	HOSTING-PRO 2006協賛	
	7月6日	2006年度情報セキュリティ監査シンポジウム in 東京後援	
	7月7日	セキュリティ対策についてのワークショップ	
	7月12～14日	自治体総合フェア2006協賛	
	7月19日	S/MIMEワークショップ	
	7月19日	無線LANワークショップ	
	7月19～21日	ワイヤレスジャパン2006/EXPO COMM WIRELESS JAPAN 2006後援	
	7月21日	第9回西日本支部主催セキュリティセミナー（大阪国際会議場）	
	7月26日	第3回幹事会	
	7月28日	内部統制を見据えた、組織における情報セキュリティ人材育成セミナー後援	
8月	8月2日	第2回政策部会	
	8月8～12日	セキュリティキャンプ2006後援	
	8月25日	第3回西日本支部会	
9月	9月13日	「SCMフォーラム2006」協賛	2006年6月～2007年3月「インターネット安全教室」開催
	9月15日	平成18年度 情報モラル啓発セミナー福島 後援	
	9月19日	第4回西日本支部会	
	9月20日	第4回幹事会	
	9月25日	「CPO (Chief Privacy Officer) Japan Summit 2006」協力	
10月	10月5～7日	ネットワーク・セキュリティワークショップin越後湯沢2006協力	
	10月15日	インターネット安全教室まつり（お台場アクアシティ）	
	10月23日	平成18年度　情報モラル啓発セミナー松山　後援	
	10月26日	NSF2006 in Osaka（大阪国際会議場）	
11月	11月13～14日	「Network Security Forum2006」主催	
	11月15日	「第2回プライバシーコンサルタントサミット2006」協力	
	11月18日	「日本ITガバナンス協会設立記念カンファレンス」後援	
	11月21日	第5回幹事会	
	11月21～22日	「BUSINESS CONTINUITY MANAGEMENT 2006」「Compliance & IT 2006」「Storage Management World 2006」後援	
	11月29～30日	「Tokyo International Security Conference 2006」後援	
12月	12月7日	Security Day 2006開催（Internet Week 2006 内）	
	12月14日	第5回西日本支部会	
	12月15日	平成18年度 情報モラル啓発セミナー 後援	
	12月18～19日	「デジタル・フォレンジックコミュニティ 2006 in Tokyo」後援	
1月	1月23日	2007年 JNSA新年賀詞交歓会	
2月	2月7～9日	「NET&COM2007」後援	
	2月7～9日	「PAGE2007」後援	
	2月16～17日	拡大幹事会（予定）	
	2月23日	「インターネット安全教室」全国連絡会議	

★ JNSA 活動スケジュールは、http://www.jnsa.org/active/schedule.html に掲載しています。

★ JNSA 部会、WG の会合議事録は会員情報のページ http://www.jnsa.org/member/giji_2006/index.html に掲載しています。（JNSA 会員限定です）

7. JNSA について

■会員の特典

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

8. お問い合せ

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

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

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

JNSA Press vol.18

2006 年 12 月 20 日発行

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

印　刷
プリンテックス株式会社

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

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

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