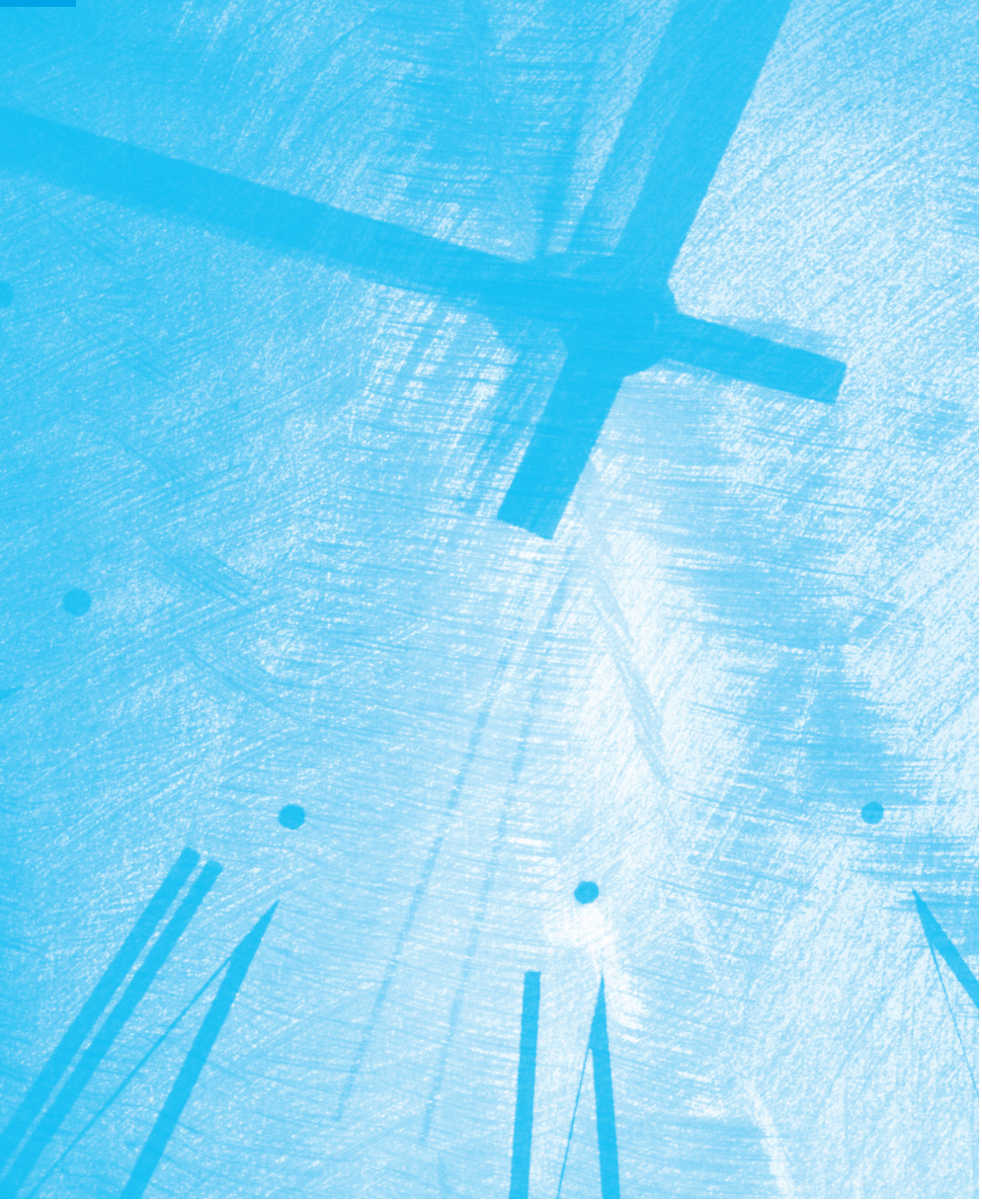
JNSA Press

Japan Network Security Association



Vol.16
March 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

インターネットの萌芽から飛躍をみつめて

NPO 日本ネットワークセキュリティ協会 主席研究員
株式会社ディアイティ 安田　直義

インターネットは、当初の大方の予想や希望を遥かに超え、既に研究者の手を離れ自立発展的な展開を行うまでになってきています。社会基盤として認知され、市民生活の中に浸透してきたということでしょう。

日本で最初の商用プロバイダが設立された13年前頃(1992年末)は、今日の隆盛は半分以上冗談として語られていた記憶があります。10数年ほどの間にこれほど普及し社会への影響力を強めたのは、携帯電話と双璧を成すと言っても良いでしょう。今後も通信と放送の融合など、必然の流れに沿った大きなうねりに呑み込まれ統合化と分化が進むのだろうと思います。これをユビキタスと呼ぶのかもしれません。

インターネットの利用者は、7000万人を越えた[1]そうです。日本の人口は約1億2776万人[2]だそうですから、老人から赤ちゃんまで含めて約55%の国民が何らかの形でインターネットを使っていることになります。

インターネットが犯罪などに使われたり、転落への道筋となっているのではないかという指摘がありますが、これは物事の一面でしかないと思います。確かにそのような事例も多いかもしれませんが、インターネットは今までできなかった個人と組織の圧倒的な格差を圧縮し、国境や地理的な格差もなくしてしまいました。少数派や日の目を見られなかった人たちもコミュニティを持てるようになったのです。この大衆が平等に議論に参加できるようになったことが、良くも悪くもインターネットがもたらした最大の成果ではないでしょうか。

輝く光が強ければ強いほど、遮るものの影の闇は深く濃くなります。この当然の原理がインターネットでも働いているのです。光だけを見てバラ色の世界を思い描くのも片手落ちですし、闇だけを見て恐れおののくのも芸がありません。全体を見て感じて自分の立ち位置を決めなければならないのだと思います。

ネットワークセキュリティは、多くのIT技術の中に要素として含まれ、それらが全体として機能して初めて効果が出るものです。また、技術の問題だけではなく、リテラシーや交通安全のように自分の身を守る基本的な約束事や知識でもあります。今までの経験や知見を生かすことができるのですが、法律などの抜け道があるのも事実です。技術面と運用管理面の双方から問題点を考えていくことが大切でしょう。JNSAのような中立的な団体の役割もこの辺りにあると考えています。

インターネットの萌芽に出会い、若葉の頃からの成長を見届け、立派な大樹に育った今、これからどのような森を築いて行くのか大変に楽しみです。ひとり立ちした子供を見るような感じかもしれません。これからは、『自分の人生を自分で決めて歩んでいくのだよ』と。

[1] 財団法人インターネット協会監修.「インターネット白書2005」2005年6月21日発行. インプレス発行. 6,800円+税.

[2] 総務省統計局.「平成17年国勢調査 全国・都道府県・市区町村別人口(要計表による人口)」全国の人口. http://www.stat.go.jp/data/kokusei/2005/youkei/01.htm

検疫システムの現状と標準とのギャップ
～悪意なき情報流失への対策～

東京エレクトロン株式会社
水本　真樹

組織のクライアントセキュリティ管理を取り巻く環境・制度が変わりつつある。ISMS、個人情報保護法によるクライアントPCの漏えい保護対策に対するニーズの高まり、日本版SOX法のITシステムへの影響など、今後も検討すべき点はある。
情報漏えい対策や企業のPCコンプライアンスを実現するために検疫ネットワークが注目されている。
実は検疫システムには標準が確立していない。各団体やベンダーから企業を中心とする組織に合うよう検疫ネットワーク標準が策定されつつあるというのが現状だ。
検疫ネットワークは、エンドユーザーの良識に任されがちなクライアントPCのセキュリティ対策をシステム側で管理するシステムだ。企業内ネットワークに接続しようとするクライアントPCに対して、ウイルス対策ソフトの起動の有無や定義ファイルのバージョン、パッチ適用の有無などのポリシーをチェックし、ここで「陽性」と判定されると接続を拒否。最新の定義ファイルをインストールするなどの「治療」を施してから、社内ネットワークへの接続を許す。
しかし実状は現段階の標準をベースとしたシステムでは要求にマッチしない場合が多い。どのような仕組みが必要とされるのか―検疫システムの構築経験を踏まえ考察する。

RSA Conference 2006

2006年2月、「RSA Conference 2006」がアメリカ サンノゼ カンファレンスセンターにて開催された。今回で記念すべき15周年を迎えるこのイベントは、情報セキュリティのプロフェッショナルをターゲットとしているセキュリティ技術をテーマとした世界最大のイベントだといえる。筆者が初めて参加したのは2001年の回だった。今回の寄稿にあたり当時の出張報告を読み直してみた。メインテーマはPKIで、当時のセキュリティ技術の中心。2001年はPKI元年と位置付けられてPKI関連のアプリケーションベンダーが数多く展示会に出展していた。

サンノゼ カンファレンスセンター（US）

ここ3年前から基調講演にマイクロソフト社のビル・ゲイツ氏が参加し始めたことが象徴的であるように、業界の動向が変わってきている。徐々にセキュリティ技術の中心がネットワーク・セキュリティ、エンドポイント、さらには企業のコンプライアンスを対象としてきている。

なお今回はシスコシステムズのジョン・チェンバース氏やサン・マイクロシステムのスコット・マクリーニー氏の皮肉たっぷりの講演、RSA暗号、Diffie-Hellman暗号など今日の暗号技術の考案者達によるパネルディスカッションなどあり非常に貴重だった。

この模様はWebキャストで閲覧可能なため、興味のある方は下記のURLにアクセスいただければと思う。
※ https://2006.rsaconference.com/us/conference/webcasts.aspx

さて、このConferenceでは17カテゴリの総計200クラスに及ぶEducational Trackが提供されている。4日間に及ぶこのセッションの中でも非常に多くテーマとして取り上げられていたのが企業のセキュリティ・ポリシーの遵守、とりわけ端末のセキュリティ管理とネットワーク接続制御だったと感じている。これらの核となるのが検疫ネットワークである。「Network Quarantine」や、「Endpoint Security」、単に「Network Access Control（NAC）」と分類されるものも同義と捉えて差し支えないと考えている。

後を絶たないウイルス感染による個人情報流出

さて、日本国内の情報漏えい事件に話を移す。つい先日も国家の機密情報を扱う組織から、私物パソコンに保存された秘密情報がウィルス感染によりネットワークに流出する、という事態が発生した。それ以外にも様々な組織で同様の事象が発生している。（次頁表参照）

各報道でさんざん取り上げられているはずのこういった事件。多くがファイル共有ソフト「Winny」のウイルス感染だと何かとニュースでも取り上げられるため、知っている方も多いだろう。特に本特集をご覧の方はセキュリティの知識としてもご存知だろう。ただ一般的な、ごく普通のパソコンユーザの場合はどうか。ピンとこない、というのが大半か、知人から「ゲームやソフト、音楽ファイルがダウンロードできるツールだ」として紹介されて軽い気持ちでインストールした結果、重大な事態を引き起こす可能性がある。「Antinny」やその亜種に感染した不運なユーザはマイドキュメント以下の重要な情報をWinnyネットワークに大放出して食い止められることのない個人情報流出被害が発生してしまうのだ。どこの組織でもセキュリティ規定策定や通達は行っているはずだ。つまりコンプライアンスのためのルールは存在しているのだが、往々にして遵守がなされない。すると事故も招きうるのだ。

別の側面だが国会では個人情報保護法改正案が提出されているようだ。個人情報を不正に漏らした企業の社員に対し「個人情報漏えい罪」を罰則規定として新設するというものである。成立かどうかは慎重に検討がなされるであろうが情勢は変化しつつある。

エンドポイントに必要とされる検査内容

組織には事故などの考えうるリスクに対し社会的責任を果たすための取り組みをどう行っているかを示すことが期待されている。情報漏えいが従業員への貸与端末や、ましてや個人の私用PCから発生しうるような取り組みでは、管理責任を問われても仕方がないであろう。検疫システムによる取り組みとしてWinnyをはじめとする不正なアプリケーションやプロセスの存在、固有のハードウェア情報による不正な端末の排除、ファイルの暗号化などの推奨設定を適切にチェックし未然にリスクを低減できることが必要とされる。

検疫と治療 ― 既存環境への適合

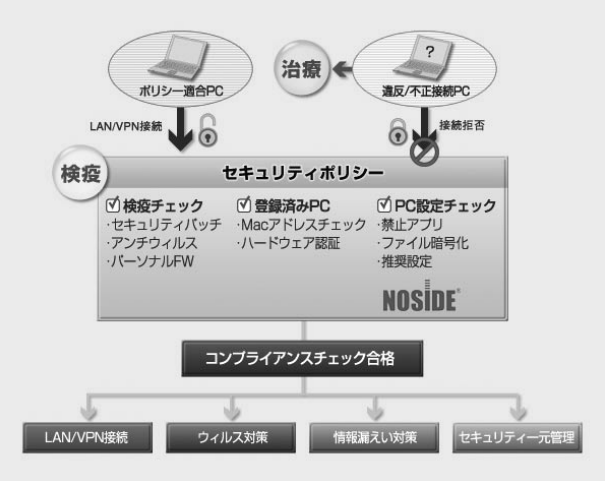
もちろんウイルス対策ソフトやOSパッチの適用状況のチェックも必須である。さらに不適合時の自動治療機能を提供すること、またシステムとして容易に日々更新されるパターンファイル番号やマイクロソフト社の月例パッチや累積パッチの変更・追加に追従できることが求められる。

この際、既存のウイルス対策ソフトの環境やパッ

最近の主なウイルス感染被害（報道発表記事より）

年月日	概要	詳細
2006/1	顧客情報が Winny に流出、私用 PC のウイルス感染が原因	コールセンタースタッフの私用 PC が Antinny に感染し、顧客情報を含む一部の業務ファイルが Winny 上に流出したことが明らかになった。
2005/12	再び Winny で情報流出、情報管理の徹底を指導	社員の個人所有 PC がウイルスに感染し、業務情報が Winny 上に流出したことを明らかにした。
2005/12	顧客情報、Winny で流出	同社社員が自宅で利用している PC が Winny に感染し、法人顧客の情報 82 件が流出したと発表した。
2005/12	取引先 104 件にウイルスメールを送信	一部顧客に対して、ウイルス「Netsky.P」を添付したメール 104 件を送信する事故が発生したと発表した。
2005/12	顧客リストが Winny に流出、私用 PC のウイルス感染で	同社が主催したイベントの案内送付先、286 社 528 名分の名刺情報が Winny ネットワークに流出したことを明らかにした。
2005/12	法人顧客情報などが Winny で流出、元社員の PC から	元社員の個人用 PC がウイルスに感染し、法人顧客と同社社員の情報、計 190 件が Winny ネットワークに流出した。
2005/12	顧客 7000 人にウイルス・メールを配信	同社のメール配信サービスに登録している顧客約 7000 人に対し、Worm_Netsky.P と呼ぶウイルスを添付したメールを配信した。
2005/12	PC のウイルス感染により生徒の個人情報を流出	生徒の個人情報が流出していることが判明したと発表した。原因は、パソコンのウイルス感染によるという。
2005/12	PC にウイルス感染、機密情報などが流出	自宅で使用している個人所有のパソコンへウイルスが感染し、業務上利用する暗証番号といった機密情報がインターネット上に流出したと発表した。
2005/12	私用 PC のウイルス感染で顧客情報が流出	職員の私用パソコンがウイルスに感染した事を原因とし、同社顧客情報 53 件がインターネット上に流出したと発表した。
2005/12	ウイルス感染で資料が流出	社員の私用パソコンがウイルスに感染し、技術資料などがインターネット上に流出したと発表した。
2005/11	ウイルス感染で Winny 上に個人情報を流出	社員が自宅で使用する私用パソコンにウイルスが感染し、顧客 2 名および社員 285 名の個人情報が Winny ネットワーク上へ流出したと発表した。
2005/11	設定ミスでユーザー 1518 人がワームに感染	会員向けに提供しているサービスのユーザーのうち、少なくとも 1518 名のパソコンが、同社のミスによってワーム型ウイルス「Sasser(サッサー)」に感染したことを明らかにした。さらに 2717 人のユーザーのパソコンに、ウイルスが感染を試みた形跡があったという。
2005/11	ショップが Winny で情報流出	ショップでユーザーの個人情報が流出したと発表した。スタッフが自宅で使用する個人所有の PC が Winny のウイルスに感染し、内部に保存していた情報が流出した。
2005/10	ウイルスで Winny 上に顧客情報が流出	県内の代理店において、Winny の感染により 4/4 ～ 9/29 の間、同店管理の 564 名分の顧客情報が Winny ネットワーク上に流出する事故が発生していたと発表した。
2005/9	ウイルス感染で Winny 上に顧客情報を流出	社員の個人パソコンがウイルスに感染し、137 件の顧客情報が記載されたリストが Winny ネットワーク上に流出したと発表した。
2005/9	また情報流出	個人パソコンが Winny に感染し、技術資料や出張手続きに関する書類が流出していたと発表した。
2005/9	ウイルス感染で Winny 上へ原発情報が流出	協力会社に所属する技術者のパソコンがウイルスに感染し、検査関連情報が Winny ネットワーク上に流出したと発表した。
2005/6	ウイルス感染により機密情報を流出	子会社の技術者が所有するパソコンがウイルスに感染し、同パソコンに保存されていた点検報告書などの機密情報が、Winny ネットワーク上に流出していた事実が、6 月 22 日に判明したと発表した。
2005/6	基地局情報が Winny で流出	管理する基地局情報が、Winny 経由で流出した。会社員が、情報を PC に入れて自宅に持ち帰り、Winny に感染したことが原因。
2005/5	メルマガ購読者にウイルスメールを大量転送	同社メールマガジン登録者 1 万 6233 人に対してウイルスメールを転送してしまったという事故が発生したことを発表した。今回転送されたウイルスは「NETSKY」の亜種などで、その対処法をサイトに掲載している。"
2005/5	PC のウイルス感染により一部の顧客にウイルスメールを送信	インターネット接続サービスにおいて、顧客対応用パソコンのウイルス「WORM_MYTOB.ED」への感染により、一部ユーザーへウイルスメールを配信したと発表した。
2005/4	ウイルス感染 PC から患者の個人情報が流出	かつて同院に在籍していた医師のパソコンから、2003 年 10 月 1 日から 2004 年 3 月 31 日の間に小児科に入院していた患者 63 名の個人情報が流出したと発表した。

チ管理システムとそのまま連携が取れることが好まれる。



検疫ネットワークの検査内容と機能概略図

検疫ネットワークの仕組みと必要性

ここで少し検疫ネットワークの話に戻す。「セキュリティの要件を満たしている端末だけネットワークに接続させる」―たったそれだけのことのようにも思えるが、インターネットを含むオープンなネットワークでは、この条件を満たすためのさまざまな仕組みが必要となる。

個人認証を例に取ると、LAN 接続認証、リモート VPN 接続やファイアウォール認証ログインなどの仕組みは、ユーザー名とパスワードなどを組み合わせ「本人しか知りえない情報を知っている」ことを「本人である」ということと関連付け、個人認証が得られたとして接続性を提供するという仕組みである。パスワードや個人を識別するための手法に十分な強度が確保できた場合には「本人である」ことは保証される。

このことと認証された本人が使用している「端末がセキュリティの要件を満たしているか」―特にウイルス対策ソフトや最新の OS アップデート、禁止アプリケーションの不使用や様々な推奨設定などの社内セキュリティ規定を怠りなく実施しているかというコンプライアンスの観点とは必ずしも一致しない。

こうした問題を解決するために検疫ネットワークソリューションの仕組みが今注目されている。これはネットワーク接続前に端末のセキュリティ要件をチェックし（検疫）、場合によっては接続制限を行い（隔離）、強制的にチェック項目を適用させて（治療）、さらに、認証が得られた場合に接続を許可する仕組みである。

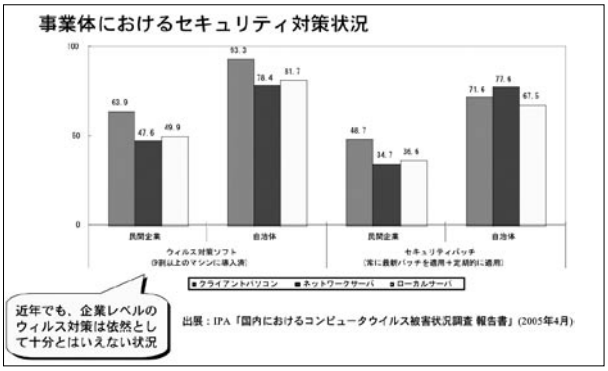
では企業のセキュリティ対策の実状は？

検疫システムの導入を検討している企業の一例を挙げる。提案や構築の経験から、ほぼ 3 パターンに分類される：

[大企業型]
大規模企業で、既に端末の標準化や体系的なパッチ管理、ウイルス対策や情報漏えい対策を行っている

[中企業型]
大～中規模な企業、もしくは教育機関などの組織で、システム管理部門の権限が弱くセキュリティ一元管理は行われていない

[管理外型]
管理外の端末、個人または各企業の端末が乗り入れるシステム



出展：IPA「国内におけるコンピュータウイルス被害状況調査 報告書」（2005 年 4 月）

細かく分析する。[大企業型] の場合は既に一元的に行われているセキュリティ対策の一環として導入を検討されるケースが多い。特長としては :

・Windows のパッチ適用・管理はコスト面から Windows 標準の Software Update Service（SUS）か Windows Server Update Service（WSUS） を採用
・標準端末化されていればパッチ管理とソフトウェア配布を兼ねるため専用のソリューションを採用
・大規模なほどエージェントの事前インストールは嫌われる
・同様に 802.1x は敷居が高い
・段階的に導入が可能な仕組みが好まれる
・ネットワーク機器の更改を要するスイッチベースの検疫は難しい
・シスコかマイクロソフトを待ちたいとは思う
・開発用など例外扱いの端末がある
・旧 OS の資産が結構存在している（Windows NT や 98 など）

[中企業型] の場合、管理者の方が苦慮しているケースが窺える :

・ウイルス対策ソフトはコーポレート版を導入済みだが、パッチ管理は個々のユーザの Windows Update 任せ
・資産管理やライセンス管理もシステム化されていない（管理者の調査による台帳管理）
・Active Directory 環境は存在していない、もしくは一部
・どうにかセキュリティ一元管理を行いたいと考えている

このように我々の知るセキュリティパッチ管理の実態と IPA での調査結果とほぼ一致していると考えられる。つまりまだ多くの組織ではルールを徹底する、というところまでたどり着いていないのだ。今後 PC コンプライアンスシステムとして検疫ネットワークが有効になるだろう。

検疫ネットワークの標準化動向

ここで、標準化動向にも触れておきたい。現在広く知られているものとして 3 つの標準化方式、およびその他の独自の実装が存在している。

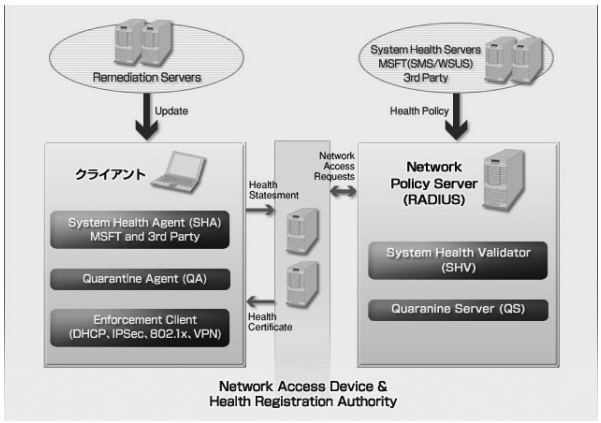
NAC（Network Admission Control）
シスコが提唱する、シスコのネットワーク製品をベースとしたエンドポイントセキュリティ管理のための標準規格。トレンドマイクロ、シマンテック、マカフィーをはじめとするベンダーが NAC パートナーとして参加。NAC Phase II で、スイッチベースの検疫システムに対応。

NAP（Network Access Protection）
マイクロソフトが提供予定のネットワーク検疫ソリューション。25 ベンダーの協業の元に、Longhorn Server で検疫ネットワーク対応機能を提供予定。2004/10/18 に NAC - NAP の互換性提供を発表。
Longhorn サーバと Vista クライアント間（ともにベータ中）で実現予定。

TNC（Trusted Network Connect）
米 Trusted Computing Group が 2005/5/3 に発表した、検疫ネットワークシステムに関するオープンな標準規格。HP、IBM、Sun、Symantec、Funk Software（現 Juniper Networks）等がメンバーとして参加

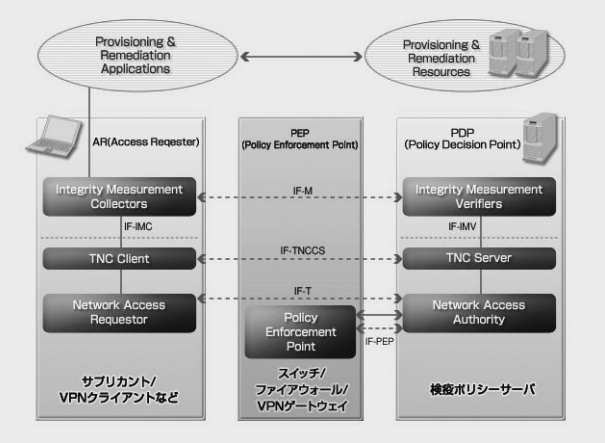
NAP に関して興味のある方は、今年リリース予定の Windows Vista バージョンと Longhorn サーバ（2007 年リリース予定）とを連携させた仕組みのベータ版テストが可能なはずである。様々な配置オプションやコンセプトなどを示したホワイトペーパーが公開されているので参考にしていただきたい。クライアントとネットワーク間の接続の制御方法として、802.1x

方式、DHCP 方式、VPN 方式、IPSec 方式などが存在する。この場合 Vista 標準のサプリカント機能、DHCP の場合は NAP に準拠した Longhorn などの DHCP サーバおよび DHCP クライアント機能と Network Policy Server（RADIUS）により、検疫時、ポリシー不適合時の制御を行う。この接続を治療に関しては Windows Server Update Services（WSUS）の機能を用いるか、サードパーティ性の検疫ポリシーサーバを連携させることになるだろう。



マイクロソフト Network Access Protection（NAP）概要

TNC は数十社からなるオープンな仕様であり、互換性や他の機能面で優れた設計思想を持っている。現在も TNC に準拠するいくつかの製品が実現されてきている。接続の制御を行うネットワーク機器やプロトコルを境界として、クライアント側の検査、接続制御層とサーバ側のポリシー検査、接続認証層を階層化しオープンなフレームワークを提供しているのが現段階のアーキテクチャだ。



Trusted Network Connect（TNC）概要

現段階で悪意あるユーザの悪意ある行動を防ぐ、というのは現実的に難しい。だが悪意なきユーザによる情報流出を水際で防ぐ可能性は検疫システムにより非常に高まる。現段階で導入が進んでいるもの、および既に稼働している検疫システムの多くは、下記のいずれかであろう。

1）パーソナルファイアウォールを中心としたシステム
2）認証 VLAN やゲートウェイを中心としたシステム
3）上記に DNS や DHCP、ホストスキャン、ARP や TCP リセットなどを組み合わせた方式

これらは前述の将来的な 3 つの標準と比較して、現時点の事実上の標準方式だといえる。ただこれらはユーザの操作に影響が及ぶことがあまり考慮されていない。例えば動作が重い、つながらない、余分な操作などがある。またこういった事実上の標準などによる分類だけでは図れない面がある。統一的な展開が図れない中規模な組織や、個人 PC や組織からみて管理外の機器が接続するシステムでは、導入時点でのハードルが多い。

悪意なき情報流出への対策として今後導入がより進むのは、導入や幅広い展開が容易なシステムになるだろう。

2005年および2005年第4四半期におけるスパイウェアの現状

ウェブルートソフトウェア株式会社
野々下　幸治

1. 概要

ここ近年日本でも、オンラインのビジネスの伸びと同時にオンラインでの詐欺がその数とともに内容も進化を遂げている。2004年は日本語のフィッシングメールが出現し、実際に被害者が発生する事件が発生し、フィッシングがオンライン詐欺の新たな手口として話題になった。2005年はオンライン銀行をターゲットとしてスパイウェアの事件がついに日本でも発生し、被害者が出ると共に、今年に入ってその犯人が捕まり、スパイウェアへの関心が高まった。

スパイウェアについては、ウイルス対策ベンダーとスパイウェア対策ベンダーとで定義が異なり、銀行の事件に利用されたキーロガーもウイルスベンダーは広義のウイルスに分類し、スパイウェアベンダーはスパイウェアと呼んでいる。

そもそも、コンピュータウイルスとスパイウェアは分類を行う観点が異なっている。

広い意味でのコンピュータウイルスはいわゆるマリシャスウェアとよばれ、ユーザーにとって悪意および害のあるソフトウェアをいい、その分類は感染方法によってウイルス、トロイの木馬、ワームに分類されている。

一方広い意味でのスパイウェアはユーザーの適切な同意なしにインストールされ、コンピュータの設定を変更したり、情報を勝手に送信したりするものをいい、その分類はウイルスと異なり、その目的によって基本的に分類されている。たとえば、広告を表示する目的のアドウェア、システムの状態を監視するシステムモニターなど。

したがって、そもそもキーロガーの機能を有するトロイの木馬は両方に分類されることになる。

ただし、ウイルス対策ベンダーは先にマリシャスウェアとしての分類分けを行った上で、スパイウェアの分類を行うので、トロイの木馬として届けられるキーロガーはスパイウェアの分類には入らず、商用のキーロガーなどがスパイウェアに分類される。

一方、スパイウェア対策ベンダーはそのような縛りがないので、たとえば、キーロガーは商用またはマリシャスの区別なくスパイウェアとして扱っている。

よって、ウイルス対策ベンダーはスパイウェアをマリシャスウェアに入れないが、スパイウェア対策ベンダーのスパイウェアにはマリシャスウェアも含まれている。この分類の違いがスパイウェアの定義において混乱をきたしていると思われる。

なお、よく、スパイウェアが金銭目的で、ウイルスは愉快犯との分類もするが、上記のようにウイルスの分類に愉快目的か、金銭目的かの分類はない。これまでの歴史を見れば、金銭目的は少なかったというだけで、現実にウイルスに分類されるトロイの木馬は、金銭目的の物が増えている。よって、これも当てはまらないと思われる。また、同様にウイルスは捕まえやすく、スパイウェアは捕まえにくいというのも同様に誤解である。

一口にスパイウェアとよんでいるが、人によってはキーロガーの問題であったり、アドウェアの問題であったり、その対象が異なっていることがある。今日、ブロードバンドの広がりと共にアドウェアのビジネスによる被害が増加し、キーロガーによるオンライン詐欺の被害もほぼ同時に増えたため、両方ともに代表されるスパイウェアが、コンピューティングの安全性にとって最重要な脅威になった。

ウェブルートはこのようなスパイウェアの問題の拡大に対して、その実際の状況を知り、適切な対策がおこなえるように、2004年より“State of Spyware”という報告書を出している。

この“State of Spyware”はPhileasと呼ばれる、インターネットを巡回し、スパイウェアの発見するシステムとSpy Auditと呼ばれるオンラインのスパイウェアの検査システムからのデータを元に分析されている。

今回、その“State of Spyware”の2005年の年間と第4四半期に関する最新の報告書が公開されたので、それを元にスパイウェアの現状を報告したい。

多くの企業や消費者はセキュリティの脅威に対処するために、すでにさまざまなセキュリティ対策製品を導入している。しかし、セキュリティ対策の導入の利用率が進んでいるにもかかわらず、新たな感染、新種のマルウェア、大規模なセキュリティインシデントが年間を通して業界ニュースを賑わした。

2. ニュースとインシデント

セキュリティアナリストから見れば、2005 年はデータセキュリティにとって最悪の年といえるかもしれない。米国ではさまざまなセキュリティ侵害が合計 130 件以上発生し、個人情報の盗難の可能性など、広範な不正行為の危険にさらされた被害者は 5,500 万人以上にのぼった。

大きく報じられたこれらの侵害事件は、引き続き消費者の財布に影響を及ぼしている。信用調査会社 ChoicePoint は、2005 年初めに個人情報の流出の事件を起こしたが、セキュリティ侵害に伴う費用をまかなうために、第 2 四半期の利益を調整しなければならなかった。さらに同社は、FTC との和解のために罰金 1,500 万ドルを支払うことに同意した。

そのようなセキュリティ侵害に伴う、ビジネス上の損失を被ったのは米国では ChoicePoint 1 社だけではない。そのほか、以下の組織や企業が被害を受けた。・H&R Block ・ BJ's Wholesale Club ・ DSW Shoe Warehouse・University of California・MasterCard ・Ford Motor Company・Sam's Club

上記の企業名は、顧客や消費者の個人情報が流出したため、年間を通してマスコミで大きく取り上げられた。しかし、これは全体の中の一握りのセキュリティ侵害に過ぎない。

日本においても、個人情報保護法の施行を受け、オンラインショッピングサイト等でのクレジットカードの情報流出等の事件が数多く報道された。

Sony BMG は猛反発と集団訴訟を受けて、不正コピー防止のためにルートキット技術を組み込んだ CD 数百万枚を回収した。問題のソフトウェアは、顧客のコンピュータをハッカーやウイルスに対して無防備にすると報じられている。訴訟では、Sony BMG は内密にスパイウェアを CD に組み込んだと申し立てられている。

このスキャンダルに続いて、マイクロソフトは、ハッカーに悪用されるとコンピュータに対するアクセスや乗っ取りが可能になる重大な脆弱性、WMF 欠陥を公表した。この独特の脆弱性は、Web ページの閲覧のような単純な行為でさえ安全でなくなるため、特に危険性が高かった。多くの技術系 Web サイトでは、セキュリティ脅威の進化を解説するために、この欠陥と関連するハッカーの行動を引き合いに出した。

3. インターネットの上のスパイウェアの配布状況

ウェブルートは Phileas という自動巡回ロボットによって、インターネット上のスパイウェアの配布状況や新しいスパイウェアを常に調査・研究している。その Phileas のデータによれば 2005 年にウェブルートはスパイウェアの配布サイトを 40 万以上検出した。

また、スパイウェア配布元として第 4 四半期は US が 30.54% と相変わらずトップであるが、第 2 位の中国が 30.31% とほぼ US の数に近づいてきている。

スパイウェア業者やスパイウェア作者にとっては 1 年を通して、検出と除去の回避が中心的な関心事になった。

そのためスパイウェア作者は、セキュリティ脆弱性を攻撃し、ポリモーフィックコードのような高度な技法を採用して、感染ユーザー層を拡大し続けている。

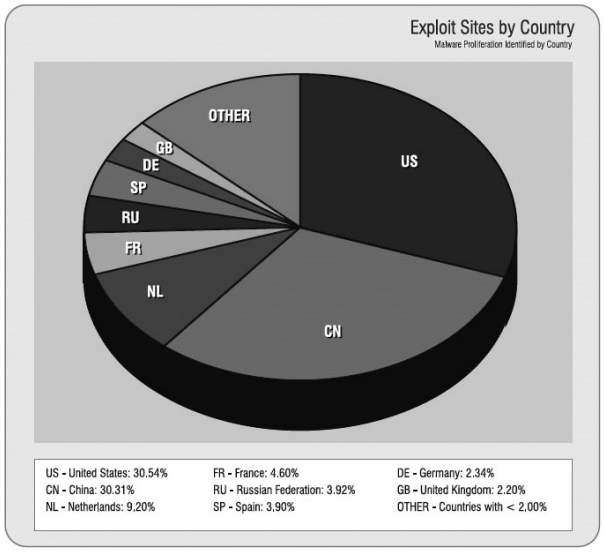
スパイウェア業者はより強力で除去しにくいプログラムの作成に努めており、ドライバベースの技術を使用したスパイウェアが増加した。

このようなプログラムは OS の最下位に入り込み、初期のスパイウェアよりもコンピュータの奥深くに自らを埋め込むもので、ユーザーの OS に広範なダメー

ジを与えることができる。

現在のスパイウェアの開発では、検出を回避するためにスパイウェアをユーザーから隠すだけでなく、自動更新技術を実装することにも力を注いでいる。

脅威は絶え間なく進化しており、スパイウェア対策業界は片時も目を離さないことが求められる。



今回、上位にランクインした脅威の以下のリストから、圧縮アルゴリズムと暗号化アルゴリズムが依然として使用されていることがわかる。トロイの木馬コード、ウイルスのインストール、ポリモーフィックエンジンをベースにしたスパイウェアでは、脅威の先手を打つために、新たな検出･除去手法が必要になる。

以下のトップ 10 のプログラムのうち、Spyware-Strike と PSGuard の 2 種類はスパイウェア対策ソフトを装ったスパイウェアであることに注意していただきたい。

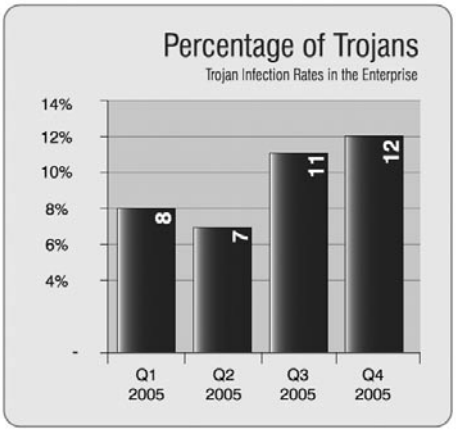
2005 年第 4 四半期のトップ 10

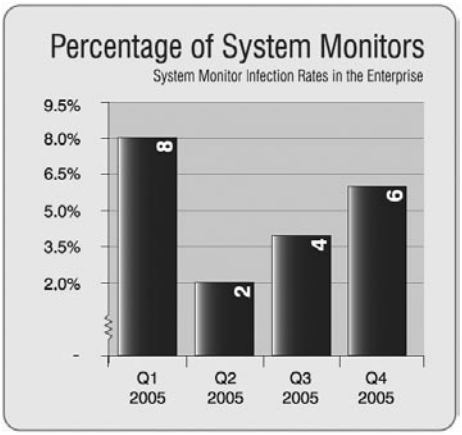
- 180 Search Assistant
- EliteBar
- PSGuard
- Apropos
- ISTbar
- SurfSideKick
- Virtumonde
- CoolWebSearch（CWS）
- DirectRevenue-ABetterInternet
- SpywareStrike

4. 企業についての調査結果

システムモニターやトロイの木馬などの悪意あるスパイウェアは、企業内の感染を広げている。

下図に示すように、2005 年第 3 四半期から第 4 四半期に、トロイの木馬は 9%増加した。第 2 四半期から第 4 四半期にかけては、システムモニターは四半期ごとに 50%ずつ増加した。





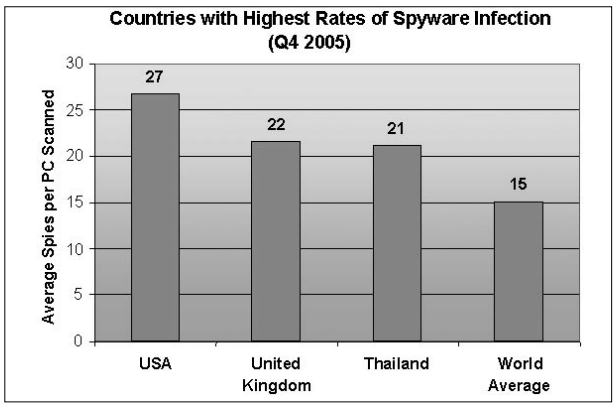
悪意あるスパイウェアはどんどん複雑化しており、旧来のウイルス検出および除去の手法では問題が生じる。

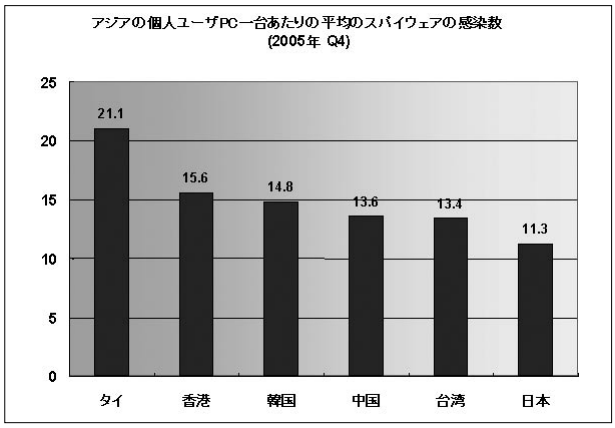
スパイウェアの場合、大半が旧来のウイルスよりも動作の変化が激しい。

ウイルス対策ソフトや無償のデスクトップ用ソリューションは、複雑で高度なスパイウェアに対しては効果的な保護と駆除が難しいことを認識することが重要だ。これらのプログラムで使われる検出・除去エンジンでは、ポリモーフィックコードやルートキット技術を使って検出を回避しようとする、悪質なスパイウェアを完全に除去することは難しい。

5. コンシューマーについての調査結果

スパイウェアに対する意識の高さにもかかわらず、望ましくないプログラム、特にトロイの木馬やシステムモニターのような悪意あるプログラムに感染される消費者は増加している。米国、タイ、英国の家庭用コンピュータのユーザーは依然として感染率がトップクラスだった。日本は平均 11.3 と世界の平均 15 よりも低い。これは多くのスパイウェアが英語圏をターゲットとしており、日本語のスパイウェアが少ないためだと思われる。しかし、最近は日本語のインストール用の Web ページを用意するなど、日本人をターゲットにしてきているので、今後は日本の感染が増える可能性も考えられる。





スパイウェア感染率が上昇する原因を 1 つに特定するのは難しいが、セキュリティアナリストは、パソコンの低価格化と、低料金化やアクセス増加によるブロードバンドの普及率の高まりを指摘する。コンピュータの価格が手頃になるにつれて、1 世帯で複数台のコンピュータを所有する傾向が強まる。

さらに、検出を回避するために、スパイウェア作者はプログラムを頻繁に変更する。家庭ユーザーが新種のスパイウェアから身を守るには、定義が頻繁に更新されるスパイウェア対策ソフトを使うことが必要だ。残念ながら、スパイウェア対策ソフトをインストールしても定義やバージョンを更新しないでいると、頻繁に更新を行う場合のような保護は得られない。

6. 米国における法規制

US においては、特にアドウェアのアフェリエイトのビジネスモデルが消費者の PC にいろいろな問題を起こしているために、SPAM と同様、法による規制が進んできている。2004 年 10 月にスパイウェア業者を相手に初のスパイウェア訴訟を起こした FTC は、2005 年には取締活動を強化し、スパイウェアや偽のスパイウェア対策ソフトの配布元とみられる業者に対して数件の訴訟を起こすとともに、FTC によれば顧客データを適切に保護できなかった企業に対して

も提訴に踏み切った。

その中でスパイウェアの配布元は、2005 年に議会を通過した新たなスパイウェア規制法案の重圧を感じ始めている。米国の多くの州がこのような業者の提訴に踏み切った。米国政府レベルでも米連邦取引委員会（FTC）が、自作のスパイウェアをスパイウェア対策ソリューションと偽って配布しようとした複数のスパイウェア作者を提訴した。

2005 年に、コンピュータユーザー数名が自分たちの手で問題を処理すべく、スパイウェアを欺瞞的に広めたとして複数の企業に対する集団訴訟を起こした。このアプローチは比較的目新しいため、これをきっかけに訴訟が急増するかどうか、業界では訴訟の成り行きを注意深く見守っている。

2005 年末までに、米国の 12 州でスパイウェア法案が可決された。そのうち 11 法案はすでに施行されており、ネバダ州については 2007 年 1 月 1 日から施行される。これらの新法はアラスカ州、アリゾナ州、アーカンソー州、カリフォルニア州、ジョージア州、アイオワ州、ニューハンプシャー州、テキサス州、ユタ州、バージニア州、ワシントン州で施行されているが、今後その効力が明らかになるだろう。2006 年会期のために州議会が招集されるため、米国では今後さらに多くの州でスパイウェア法案が検討される可能性は高い。

スパイウェアの脅威が加速する中、この災いの種からシステムを守ろうとする人々にとって 2006 年はどう展開するだろうか。

スパイウェア作者は審議中の米国政府法案に注意を払っており、悪意あるプログラムを配布する場合は、起訴の困難な中国やルーマニアなどの外国を経由するのを常套手段にしている。高度な暗号化技法をルートキット技術と合わせて使用することで、さらに悪質なタイプの望ましくないソフトウェアが引き続き蔓延するだろう。

2005 年に消費者と企業は、スパイウェアとその増大する影響についての認識を深めた。ユーザーはオンライン対策ツールの 1 つとして、スパイウェア対策ソフトを導入し始めている。ただし次のステップとして、導入した対策で問題を確実に解決し、対策ソフトを常時最新に保ち続けることを徹底しなければならない。

2005 年版「State of Spyware」に記されているように、スパイウェアの標的になるユーザーは増え続けており、オンラインセキュリティに対する脅威全体は飛躍的に増大している。

セキュリティ市場調査 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　勝見　勉

セキュリティ市場調査 WG は、国内の情報セキュリティの市場規模とその実態を調査する目的で活動しています。市場規模を捉える作業は、その基礎となるデータの収集段階で、様々な困難を伴います。アプローチとしては、供給サイドの数字をできるだけ個別に拾うか、需要サイドの数字を、サンプリング調査と統計手法を使って推測するか、が、主な方法論となります。

当 WG の沿革は、2004 年度にマーケットリサーチ WG としてスタートを切ったところに遡ります。まず取り組んだのは、ユーザサイドの実態把握で、ユーザ企業において何がどこまでできているか、どんな対策が実施済みで、どんなサービスが利用されているか、を探る事にしました。その際、ベンダの集りである JNSA としては、ユーザがセキュリティのツールやサービスにどの程度満足し、どんな不満を持っているかを知ることに意義がある、という視点から、満足度に焦点を当てた調査を行うことにしました。この調査は、WG に 13 社 17 名の参加を得て、2004 年夏～秋に実施し、「情報セキュリティ対策施策の実施状況とその満足度調査」という報告書をまとめ、NSF2004 で発表しました。

この成果を踏まえ、次はいよいよ、ベンダ側の実態にせまる調査に取り組みました。供給サイドから見た時の、その産業としての規模感や、技術面または産業としての課題、ひいては諸外国との比較における日本の市場の特徴、などが調査テーマとして浮上しました。これらはまた、経済産業省の関心事でもあることから、同省の委託と支援を受け、2004 年度後半のテーマとして取り組みました。

調査では、別表のようにセキュリティツールとサービスの両面を対象とし、それぞれを、機能区分に基づいて大分類、中分類にセグメント分けして、それぞれに該当する製品やサービスを回答してもらう形でアンケート調査を実施しました。その結果に基づき、また専門調査業者の分析・予測ノウハウも活用して、実態に迫るアプローチを試みました。その結果、2004 年度見込みでセキュリティツールが約 1500 億円、同サービスが 3000 億円程度、という数字が得られています。

2005 年度は、前半は 2004 年度の結果に関する補完的分析と今後の調査活動の方向付けの議論に時間を費やしました。そして、今年度もベンダサイドに対して継続調査を行うことに決定しました。新しい調査活動のスタートに際して、WG の名称も「セキュリティ市場調査 WG」と変更し、メンバーの新規参加も募りました。その結果、新しい陣容として以下のメンバーの参加を得て活発な調査活動を展開しています。現状は、前年度の反省を踏まえて改良した市場分類表を基に、JNSA 会員と SIer、サービス業者等約 700 社を対象にアンケート調査中で、集計終了次第分析を行って、報告書をまとめる予定です。

◆メンバーリスト（社名昇順）

村上　博	特定非営利法人アイタック
加藤 純	NTT コミュニケーションズ株式会社
佐藤 由佳子	NTT コミュニケーションズ株式会社
山田 実	NTT コミュニケーションズ株式会社
郷間 佳市郎	京セラコミュニケーションシステム株式会社
山田 勝志	クオリティ株式会社
勝見 勉	グローバルセキュリティエキスパート株式会社
鈎　俊行	グローバルセキュリティエキスパート株式会社
金子 以澄	コンピュータ・アソシエイツ株式会社
藤井 雅展	株式会社ディアイティ
中原 康	東芝ソリューション株式会社
大島 美香	日本ユニシス株式会社
長谷川長一	日本ユニシス株式会社
大槻　兼也	株式会社ヒューコム
大桃 浩輝	株式会社マイクロ総合研究所
江連 三香	株式会社三菱総合研究所
鶴野 アンドレイ	リコー・ヒューマン・クリエイツ株式会社
田中 秀幸	東京大学大学院（オブザーバー）

「2005 年度国内情報セキュリティ市場調査」分類表

■ セキュリティ製品販売額

大分類	中分類
統合型アプライアンス	統合型アプライアンス
	その他統合型アプライアンス
統合型アプライアンス 合計	
アクセス制御製品	ファイアウォール・アプライアンス
	ファイアウォール・ソフトウェア（企業向けライセンスタイプ）
	ファイアウォール・ソフトウェア（デスクトップ FW）
	VPN ソフトウェア
	VPN アプライアンス
	IDS/IPS アプライアンス
	IDS/IPS ソフトウェア
	その他のアクセス制御製品
アクセス制御製品 合計	
セキュアコンテンツ管理製品	アンチウィルス・アンチワーム・ソフトウェア（企業向けライセンス契約）/ アプライアンス
	アンチウィルス・アンチワーム・ソフトウェア（個人ユーザ向けパッケージタイプ）
	アンチスパム・ソフトウェア / アプライアンス
	URL フィルタリング・ソフトウェア / アプライアンス
	メールフィルタリング・ソフトウェア / アプライアンス
	アンチフィッシング・ソフトウェア / システム
	その他のセキュアコンテンツ管理製品
セキュアコンテンツ管理製品 合計	
アクセス管理製品	個人認証用デバイス及びその認証システム
	個人認証用生体認証デバイス及びその認証システム
	ログオン管理 / アクセス許可製品
	PKI システムおよびそのコンポーネント
	その他のアクセス管理製品
アクセス管理製品 合計	
システムセキュリティ管理製品	セキュリティ情報管理システム / 製品
	脆弱性検査製品
	ポリシー管理・設定管理・動作監視制御製品
	その他のシステムセキュリティ管理製品
システムセキュリティ管理製品 合計	
暗号製品	データ暗号化製品
	暗号化ミドルウェア
	その他の暗号製品
暗号製品 合計	
セキュリティ製品 総合計	

■ セキュリティサービス販売額

大分類	中分類
セキュリティ・コンサルテーション	セキュリティポリシー構築支援
	セキュリティ管理全般のコンサルテーション
	セキュリティ診断・監査サービス
	セキュリティ認証取得支援サービス
	セキュリティ認証・審査機関（サービス）
	その他のセキュリティコンサルテーション
セキュリティ・コンサルテーション 合計	
セキュアシステム構築サービス	IT セキュリティシステムの設計・仕様策定
	IT セキュリティシステムの導入・導入支援
	セキュリティ製品の選定・選定支援
	その他のセキュアシステム構築サービス
セキュアシステム構築サービス 合計	
セキュリティ運用・管理サービス	セキュリティ総合監視・運用支援サービス
	ウイルス監視・フィルタリング・運用支援サービス
	IDS/IPS 監視・運用支援サービス
	ファイアウォール監視・運用支援サービス
	脆弱性検査サービス
	セキュリティ情報提供サービス
	電子認証サービス
	VPN 通信サービス
	インシデント対応関連サービス
	その他の運用・管理サービス
セキュリティ運用・管理サービス 合計	
セキュリティ教育	セキュリティ教育コンテンツの提供
	セキュリティ教育実施
	セキュリティ教育の e- ラーニングサービス
	セキュリティ資格認定及び教育サービス
	その他のセキュリティ教育サービス
セキュリティ教育 合計	
セキュリティ保険	情報セキュリティ保険合計
セキュリティサービス売上高 総合計	

不正プログラム調査 WG

WG リーダー
株式会社アークン　渡部　章

■ 活動目的

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ます。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ありません。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ます。

■ 活動内容

様々な不正プログラムを分類化し、その利用目的を明らかにし、各分類における代表的な不正プログラムと、昨今話題となっている不正プログラムのメカニズムを説明できるような資料を作成公開します。合わせて具体的な対策方法も示して、この種の技術に関する正しい知識を広めていきます。また、既存のセキュリティ技術のこれら不正プログラムによる侵入、攻撃に対する有効性を検証します。

■ 年間活動予定

- 月1回程度の会合
- 年1回の合宿
- 成果物の取りまとめ

2006 年 3 月　合宿風景

■ 過去の成果物

「メモリ感染型ネットワーク・ワームの脅威とその対策」（2002年度）

当WGが発足した2002年度は、今後の方向性を見極めるために将来的成果物のインデックスを作成しました。その中から、年度中にまとめられる内容として、一連のワーム事件を特に取り上げ､「メモリ感染型ネットワーク･ワームの脅威とその対策」について報告書を作成しました。他の組織からの報告書と差別化するために、既存対策で検出できなかった理由、事件後の対応状況や、今後の対策への考察を中心にまとめました。

「不正プログラム対策ガイドライン」（2003年度）

不正プログラムの定義、分類、構造、対策についてまとめました。対策としては、セキュリティルールの策定方法について、また、対策ツールの導入については、スタンドアロン、LAN、インターネット接続、グループウェアなど環境別に取りまとめました。

「絵で見るネットワークのぜい弱性と脅威」（2004年度）

近年、不正プログラムがセキュリティ問題の中核を成していることを鑑み、特に注意を要するネットワーク上の脆弱性と脅威について、わかりやすく取りまとめました。その骨組みとして攻撃頻度の高い脆弱性を技術的に取りまとめた「SANSインターネットセキュリティ脆弱性トップ20」を利用し、特筆すべき近年の脅威について追加しました。

■ 本年度の活動

本年度は、不正プログラムを分類化し、タイプ別、レイア別に、その対策ソリューションを調査、整理し、マッピング化することにしました。予定している成果物としては、「不正プログラム対策ガイドライン ver.2」です。本ガイドラインは、「ユーザ企業の視点でセキュリティソリューション購入のガイドとなる」および「セキュリティソリューションの販売者がユーザ企業への説明用に使用できる」ことを目的としています。

■ 今後の展開について

ウイルスによる被害は、他のセキュリティ被害に比べて圧倒的なもので、これは今後も継続するに間違いないと思われます。ただし、ウイルス対策ソフトウェアなどの既存セキュリティ技術では対策が十分ではないワームや、キーロガーなどのトロイの木馬、そしてスパイウェアなどによる情報漏えいは、新しい脅威として既に多大な被害が出てきています。これらの背景から当WGは、不正プログラムをウイルスだけに留めず、広範囲にその現況と対策について調査研究を実施していきます。

会員企業ご紹介⑯

株式会社アルゴ 21

http://www.argo21.co.jp/

今日、情報システムと企業経営は切っても切れない関係にあり、かつ、お客様のニーズはますます多様化・高度化の一途をたどっています。こうしたニーズにお応えするために、アルゴ21は企画･提案からシステム構築、保守･運用までの情報システムに関するサービスを情報システム主幹事会社としてワンストップでご提供してまいります。

インフラ構築サービス

基幹インフラやネットワークの企画・コンサルティングから、ハードウェア/ソフトウェアの選定･調達、ネットワーク構築に至るまでトータルコーディネート。情報システムに関する様々な問題やご要望に対し、最適なソリューションをご提供いたします。

コンサルティングサービス

企業にとって大切な情報資産を守る仕組みであるISMS構築コンサルティングをご提供。ISO27001やプライバシーマーク取得対策、セキュリティポリシーの策定などのご支援をいたします。通常のコンサルタントによるヒアリングや改善対策案の提案等に加え、コンサルティング支援ツールSecure-Method Suiteシリーズを採用し、効率的なコンサルティングを実現。

セキュリティソリューションサービス

独立系IT企業の性質を生かした、メーカーにとらわれない幅広いご提案を特徴としております。金融系企業様・ホテル業様セキュリティシステム構築ノウハウを生かし、企業様の考えるポリシーに沿った対策に世の中の動向を踏まえながら、段階的かつ継続的に講じて行くお手伝いを行っております。

災害対策(ディザスタリカバリー)サービス

相次ぐ自然災害や企業を対象としたテロ事件の発生を背景に、「ビジネスの継続性(Business Continuity)」というキーワードが盛んに聞かれるようになりました。ビジネス継続性プラン(BCP)の一つとして企業のシステムデータをガードするディザスタリカバリーサービスを安価で手軽に対策できるものから広範囲にわたるまで3つのクラスに分けてサービスいたします。

システム運用サービス

情報システムの運用管理･保守を一括サポート!専門のサポートエンジニアによるサービスで、情報システムという資産の有効活用を可能にします。

★システム運用サービスメニュー★

① ヘルプデスクサービス
② 常駐サポートサービス
③ オンサイトサービス

リモート監視サービス

弊社MSPセンターにてご用意した監視･管理ツールを使用し、システムの監視・管理、障害の自動復旧などの運用管理を提供いたします。MSP方式により、24時間365日システムの監視･管理、及び障害復旧といった究極のアウトソーシングサービスをご提供いたします。 ※MSP･･･ManagementServiceProvider

お問い合わせ先

株式会社アルゴ 21 プロフェッショナルサービス事業部 営業部
〒 104-8580 東京都中央区勝どき 6-1-15 勝どき YS ビル
TEL:03-5548-4833　FAX:03-5548-6364　e-mail:ps-sr@argo21.co.jp

F5 ネットワークスジャパン株式会社

http://www.f5networks.co.jp

アプリケーションの「安全性・高速化・安定感」を求めるすべての企業とお話ししたい。私たちは、F5ネットワークスジャパンです。

インターネットを使った情報伝達のために、アプリケーションはどうあるべきか？

インターネットを利用したビジネスにおいて、すべての情報伝達はアプリケーションに依存しています。しかし、ネットワークの構成上、すべてのネットワークでアプリケーションがうまく動作するとは限りません。さらに、使用されるロケーションはオフィス・外出先・自宅などさまざまで、接続環境もモバイルやADSL、VPNを用いたWAN接続など多岐にわたっています。

最適なアプリケーション配信のために、F5ネットワークスができるコト

こうした環境のもと、ネットワーク上で動くすべてのアプリケーションを、いかに「安全に、速く、そして安定させて」配信できるかが重要なことは言うまでもありません。F5ネットワークスでは、この3つのキーポイントを「アプリケーション・デリバリ・ネットワーキング」と称し、ソリューションをお届けしています。

【Secure】
確かなセキュリティにより、配信の「安全性」を保証。
【Fast】
ネットワークの最適化により、配信の「高速化」を実現。
【Available】
ビジネスを決して止めない、絶対的な「安定感」を提供。

・・・その結果、以下のような劇的な効果が期待できます。

- ネットワークにインテリジェンスを付加することで、管理の効率性を高めながら、競争上の優位性をも手に入れることができます。
- アプリケーションをネットワークからオフロードすることにより、アプリケーションのパフォーマンスを最大限引き出します。
- アプリケーションとユーザの間を戦略的に構築することで、ネットワークとアプリケーションが十分に対応していない隙間を埋めます。
- 安全性と信頼性を高めるための開発リソースの無駄が解消されることにより、多大な時間とコストを費やす必要がなりなります。
- 共通のプラットフォームからなる統合型アーキテクチャを使用することで、単一用途製品の増加を防ぎ、ネットワークとアプリケーションの一元的なコントロールを可能にします。
- 拡張性の高いアプリケーション・デリバリ・ネットワーキングを構築することで、お客様にとって安全、高速かつ安定したネットワーク環境をご提供いたします。

《F5ネットワークスが提供するセキュリティ製品》

- 企業データへのセキュアなアクセスを実現するSSL VPNアプライアンス製品　→ FirePass®
- クロスサイド・スクリプティングやSQLインジェクションなどのアプリケーション層の攻撃に対して、高いレベルのセキュリティを備えたWebアプリケーション専用のファイアウォール　→ TrafficShield®
- アプリケーションをプロアクティブに保護しながら、優れたアプリケーション・パフォーマンスを確保。運用の煩雑さを軽減し、保守管理コストを低減
  → BIG-IP® Application Security Module

アプリケーションの「安全性・高速化・安定感」なら、F5ネットワークスとご一緒に。

お問い合わせ先
F5 ネットワークスジャパン株式会社
〒 107-0052 東京都港区赤坂 4-15-1
赤坂ガーデンシティ 19 階
Tel: 03-5114-3200　Fax: 03-5114-3201
e-mail:info@f5networks.co.jp

株式会社ガルフネット

Gulf Net Group

顧客に一番近い視点からITで経営を支援するソリューションサービスプロバイダー

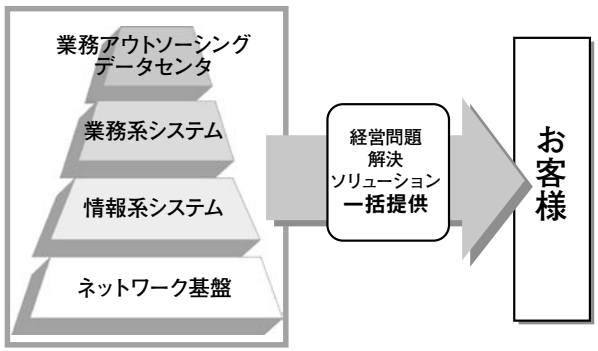
ガルフネットは、チェーンストアを全国に大規模に展開する企業を主に顧客として、ITを核としたソリューションを提供してきました。創業から10年経った現在まで、「顧客企業の視点に立ってITを提供し、顧客企業の経営を支援してゆくこと」という経営理念は変わっていません。
一般に顧客の企業にとって、ITとは、自社の利益を増大させる、あるいは、費用を低減させるための、幾つかある内のひとつの道具でしかありません。エンジニアならいくらでも薀蓄を傾けて語れるような技術も、顧客にとっては、それで自社の収益を向上させられるかどうかこそが最重要の関心事です。ガルフネットでは、このような認識に立って常に発想の原点を、システム的には最上位にあたる顧客の経営的な観点に置いています。

最速で提供される顧客毎に最適化されたITプラットフォーム

様々な顧客の要望を最速かつ低リスクで提供するのが、ガルフネットのソリューション提供のスタイルです。千を超えるノードをもつ全国ネットワークを構築し、その上で業務システムを稼動させるまでをガルフネットでは通常3か月で実現します。それを実現するために、ガルフネットでは自社開発製品を含め100を超えるソリューションを予めプールし、個々の顧客の必要に応じた形にそれらを組み合わせて提供します。また、ガルフネットでは低コストで導入できるASPサービスを用意しています。最初はそれを試して効果を確認した上で、顧客は本格導入に踏み切るかを判断できます。

必要かつ十分なトータルITプラットフォーム

ガルフネットは、ITを「ネットワーク基盤」「情報系システム」「業務系システム」「業務アウトソーシング・データセンタ」という4つの分野に分類し、それらを一括して提供します。顧客はITに関しては全てをガルフネットに任せることにより、IT基盤の開発やその維持といった派生的な事柄に煩わされることなく、本来の自社の本業のビジネス課題に集中できるようになります。



ガルフネットが提供する各種セキュリティソリューション

ガルフネットは、セキュリティ関連では次のようなソリューションを提供しています。

● **高セキュリティネットワーク基盤**

Gulf-BB-WIDEという全国規模のネットワークサービスは、顧客毎に設けられた3DESによる高強度のIPSecネットワークを提供するサービスであり、全国規模の安全なネットワーク基盤を顧客企業に提供します。このネットワーク基盤を実現するにあたり、独自の仕様による専用ルータを開発し、これにより安全性をさらに向上させています。このネットワーク基盤に、ウィルスチェック、メール監査・フィルタリング、データ暗号化、データ漏洩防止不正操作自動検知、といった様々なセキュリティオプションを、顧客の必要に応じて組み合わせて、最適なソリューションを提供しています。

● **フィジカルセキュリティオプション**

ガルフネットでは、指紋パターンによる認証技術を実用化したソリューションを他社に先駆けて既に5年前から提供し、数千店・数万人が利用する規模のチェーンストアの勤怠管理システムで、それを運用している実績をもちます。ある顧客ではそれにより人件費を4%削減(対売上)した事例をもちます。現在は声紋認証に取り組んでいます。この指紋パターンによる認証技術は入退室管理ソリューションにも使われています。

お問い合わせ先
株式会社ガルフネット
〒136-0071 東京都江東区亀戸 1-4-2
ダヴィンチ錦糸町ビル 3F
企画営業部 Tel:03-5858-1143 Fax:03-5858-1149
e-mail:Sales@gulfnet.co.jp

株式会社シマンテック

シマンテックは、世界40カ国以上にわたり1万4,000人以上の従業員を擁し、革新的なテクノロジ、ソリューションおよびサービスの提供を通じて、個人ならびに企業のお客様が保有する情報資産の管理と保護を実現します。
特に企業のお客様に関してあらゆるレイヤにおけるセキュリティソリューションの他、データ管理、アプリケーション/インフラストラクチャ管理、セキュリティ監査、ストレージ/サービス管理、マネージド･セキュリティサービスなど、多岐に渡るソリューションを提供しています。
ここでは数あるシマンテックのソリューションの中でも優れたテクノロジを持つアンチスパムソリューションについてご紹介します。

2つのテクノロジでスパムメールを削減

シマンテックではネットワークバウンダリにおけるスパムメール対策テクノロジである「Traffic Shaping テクノロジ」とゲートウェイ、グループウェアにおけるスパムメール対策テクノロジである「Brightmail テクノロジ」によってお客様の環境におけるスパムメールを削減します。

◆ Traffic Shaping テクノロジ

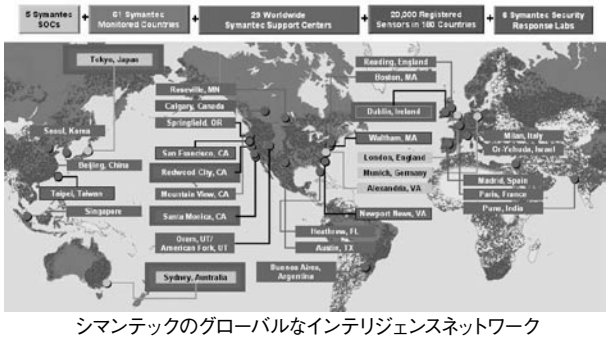
シマンテック独自のスパムメールへのアプローチ「Traffic Shaping テクノロジ」はメールトラフィックの帯域幅を調整します。これによりインターネットとメールゲートウェイ間のネットワークバウンダリで、企業ネットワークに送り込まれるスパムメールの流入を制限することが可能となります。

◆ Brightmail テクノロジ

アンチスパムの業界をリードする「Brightmail テクノロジ」は様々な検出機能を駆使してスパムか否かを判定し、優れたスパムメール検出を実現します。また、Brightmail テクノロジは誤判定率(必要なメールがブロックされる確率)も低く、100万通に1通以下とされています。

シマンテックのグローバルなインテリジェンスネットワーク

スパムメールの技法は巧妙化し、次々と新しい手口のスパムメールが生まれては消滅しています。ユーザが学習させることによりスパムメール判定を行う型のスパムフィルタでは進化するスパムメールの手口に対応するために多くの学習をさせなければならず、これに非常に多くの時間が必要となります。また、新たに開発されたスパムメールの技法には学習させない限り対応することができません。
この進化するスパムメールに対し、シマンテックはインテリジェントな「Traffic Shaping テクノロジ」と「Brightmail テクノロジ」にてお客様がスパムメール対策に多くの時間を必要としない環境を提供します。このテクノロジを支えるシマンテックのグローバルなインテリジェンスネットワークがシマンテックの最大の強みでもあります。
シマンテックでは3億以上のメールボックスからのスパムメール報告および、日本を含め世界中に展開される200万以上のおとりメールアドレスとドメインで構成されたハニーポットネットワークを活用した世界最大級のスパムメール情報収集機関にて、365日24時間体制でスパムメール情報を収集/解析し、この結果に基づきスパムフィルタを約10分間隔で継続的にアップデートします。一日に約1万5,000のスパムメールに対するシグニチャが作成され、短いサイクルで発生/消滅するスパムメールに対し高精度な検出を実現するとともに、自動化されたスパムフィルタのアップデートにより管理を省力化し、お客様のメール環境をスパムメールの脅威から守ります。



シマンテックのグローバルなインテリジェンスネットワーク

お問い合わせ先
株式会社シマンテック
〒107-0052 東京都港区赤坂1-11-44
赤坂インターシティ9階
コーポレートカスタマーサービスセンター
TEL: 03-3476-1426

株式会社ラック

http://www.lac.co.jp/

Little eArth Corporation

●会社概要

本社所在地	東京都港区東新橋1-5-2汐留シティセンター 11F
設立	1986年(昭和61年) 9月
資本金	11億5,482万円
売上高	5,841百万円(20期:2005年12月期)
従業員数	421名(2005年12月31日現在)
事業内容	総合セキュリティサービス事業(SNS:セキュアネットサービス) システムインテグレーション事業(SI) IT総合セキュリティサービス(セキュアネットサービス)事業ならびにSI事業を主な業務としています。常に半歩先のビジネスを考え、1995年に時代に先駆けてネットワークセキュリティ事業を立ち上げたリーディングカンパニーです。コンピュータセキュリティ研究所では、セキュリティ技術の調査・分析を行い、JSOCでは顧客システムのセキュリティ監視を24時間365日提供。その他、検査・コンサルティング、DBセキュリティなどのサービスを官公庁・企業等の顧客に提供しています。

● SNS（セキュアネットサービス）内容

JSOC

セキュリティ監視サービス

●Firewallセキュリティ監視サービス
●IDSセキュリティ監視サービス
●IPSセキュリティ監視サービス

JSOCは、ラックが運営するセキュリティ監視・運用を行うオペレーションセンター。
高度な分析システムや業界屈指の堅牢な設備を誇り、24時間365日、高度な技術者を配置し、顧客のネットワークやシステムを守っています。ラックのセキュリティサービスの実績は、2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業などを中心に、最高レベルのセキュリティが要求される顧客にその最高品質のサービスを提供しています。

SNS SecureNet Service

総合セキュリティサービス

●セキュリティ診断メニュー
・ホームページ情報漏えい診断サービス
・サーバセキュリティ診断サービス
・データベースセキュリティ診断サービス
・製品セキュリティ診断サービス
・無線LANセキュリティ調査サービス
●セキュリティコンサルティングメニュー
・総合セキュリティ評価・監査サービス
・ISMS・プライバシーマーク策定/導入支援
・情報セキュリティ策定・導入・運用支援
・テクニカルガイドライン策定・導入支援
・システム設計監査サービス
●セキュリティ教育・認証メニュー
・CISSP取得支援・企業向け教育
●個人情報119（不正アクセス緊急対応支援）

導入実績

●セキュリティコンサルティング:100社以上
●セキュリティ監視サービス:530センサー以上
●セキュリティ検査サービス:2300社以上
その他セキュリティ関連導入実績多数

お問い合わせ先
株式会社ラック
〒105-7111 東京都港区東新橋1-5-2 汐留シティセンター 11F
TEL: 3-5537-2610　FAX: 03-5537-2619　E-mail: sales@lac.co.jp

JNSA 会員企業情報

JNSA 会員企業のサービス・製品・イベント情報です。

■製品情報■

○Web/DBへの未知・既知の攻撃、不正侵入をブロックし企業資産を守る世界で認められたハイエンドなトータルセキュリティアプライアンス『SecureSphere v4.2』

～完全自動学習、高精度な攻撃検知によりTCOを劇的に削減 ～

《★評価機無料貸出キャンペーン実施中−テクニカルサポート付!★》
＝好評につき、申込期間 ～2006/4/30まで延長!=

『SecureSphere』の開発元Imperva社は、2006年2月13～17日、米国 San Joseで開催されたRSA Conferenceにおいて、"2006年の最も革新的なセキュリティベンチャー企業"に選定されました。

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

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

○業界最高水準のアンチスパイウェア技術を誇るウェブルート・ソフトウェア(株)のSpy SweeperをJNSA会員企業の社員の方へ特別価格でご提供。

購入はVectorのオンラインサイトからご購入ください。
Spy Sweeper 4.5はスマートシールド機能、スパイウェア除去技術とルートキットの無効化機能などがPC Magazine誌に認められ、「Editors' Choice Award」を五回受賞。

【製品情報詳細】
Spy Sweeper 1ユーザ特別価格
http://sw.vector.co.jp/swreg/detail.info?srno=SR076314
Spy Sweeper 2ユーザ特別価格
http://sw.vector.co.jp/swreg/detail.info?srno=SR076315

◆お問い合わせ先◆
ウェブルート･ソフトウェア株式会社
E-mail: jsales@webroot.com

○PCGUARDIAN WINCS

「PCGUARDIAN WINCS」は、クライアントPCからの情報漏えい防止を目的としたクライアントPCのアクセス制御ソフトウェアです。
重要な社内データの安全な運用管理は、企業にとって大きな課題です。CDやDVD、USBメモリなどの記録メディアの利用、ネットワークサーバーへのアクセス、プリンターの印刷を制御することで、クライアントPCからの情報漏えいを防ぎます。

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

◆お問い合わせ先◆
キヤノンシステムソリューションズ(株)
E-mail: pcgw-info@canon-sol.co.jp

○「追跡! ネットワークセキュリティー 24時」
著者:山羽 六 発売元:(株) IDGジャパン

セキュリティ事件・事故の背後には「ドロドロの人間関係」「権力争い」「システムのずさんな運用状況」といった問題が潜んでいるケースが多いものです。しかし、「一人の救世主」「経営者の決断」「人情」などによって救われることがあります。
そんな現場で赤裸々にされた真実に辟易(へきえき)としたり、感動して涙したりするのだということを本書は明らかにします。

【製品情報詳細】
http://direct.idg.co.jp/

◆お問い合わせ先◆
(株) IDGジャパン マーケティング部
TEL: 03-5800-3839

○ユーザ認証サーバ/EXERS AS for SMB

今、使っているネットワークは安全ですか?
誰でも簡単にネットワークにアクセスできるようになった昨今、その便利さの一方で無線LANへの不正アクセスなどの様々な問題の解決が急務です。これらの問題を1台で解決するのがユーザ認証サーバ“EXERS AS for SMB”です。Radiusサーバ機能に加え、デジタル証明書を発行できるCA機能やユーザ認証に基づくDHCPサーバ機能を装備しておりコスト面でも優れております。

【製品情報詳細】
http://www.dit.co.jp/product/security/exers_as_forsmb/index.html

◆お問い合わせ先◆
(株)ディアイティ
TEL: 03-5634-7653
E-mail: info@dit.co.jp

○セキュアOSで実現する信頼性の高いクライアンセキュリティ新登場
クライアント型セキュアOS「SafeProtector」のご紹介

「SafeProtector」はOSやプラットフォームの変更なしで容易に導入可能です。
未知ウイルス・スパイウェアなどのマルウェア対策、セキュリティポリシーで許可されていないアプリケーションの利用制御、持ち出し制御、自動暗号化など包括的なクライアントセキュリティを提供します。

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

◆お問い合わせ先◆
日本高信頼システム(株) システム営業本部
TEL: 03-3868-8921
E-mail: sales_jts@jtsl.co.jp

■ サービス情報 ■

○≪セキュリティ技術者の人材不足にお困りでしたら【SMS】≫
専門知識とノウハウの豊富な人材を貴社の即戦力に!

セキュリティマネジメントサービス【SMS】は、セキュリティに特化した教育と実務を積んだラックのエンジニアをお客様環境に常駐し、セキュリティ対策に従事致します。専門知識の豊富な人材をすぐに導入、教育・ノウハウ構築の手間を省き、効率的なセキュリティ対策が実現できます。

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

◆お問い合わせ先◆
株式会社ラック SNS営業本部
Tel: 03-5537-2610
E-mail: sales@lac.co.jp

○今すぐ実施!どのようなスパイウェアがどれだけ存在するの?
『スパイウェア診断サービス開始』のご案内(有料)

お客様の環境にどのようなスパイウェアがどれだけ存在するのかをお調べし、危険度の高いスパイウェアごとの対策、スパイウェアが多く発見されたマシンのランキングなどをまとめたレポートをご提供いたします。

【サービス情報詳細】
今すぐこちらのサイトまで:→http://www.caj.co.jp/eim/epp_ce.htm

コンピュータ・アソシエイツ株式会社は最新のスパイウェア及びウイルス対策専用製品 CA Integrated Threat Managementを発表いたしました

◆お問い合わせ先◆
コンピュータ・アソシエイツ株式会社
http://www.caj.co.jp/

■ イベント情報 ■

○「NETWORKWORLD Conference 2006/Spring」

早急に取り組むべき電子メール保護対策
「日本版SOX法」への備えはできているか!

「電子メール保護対策」に焦点を絞り、最新技術や法制度について解説するとともに、企業のソリューション事例を紹介し、「日本版SOX法」への対策のポイントを交えながら、どうすれば効率よく電子メールを保護・管理できるのかを明らかにします。

【イベント情報詳細】
http://www.networkworld.jp/conference/

◆お問い合わせ先◆
NETWORKWORLD Conference事務局
〒113-0033 東京都文京区本郷3-4-5
Tel: 03-5800-3534　Fax: 03-5800-3979
E-mail: nwc@idg.co.jp

○第4回「セキュアOSカンファレンス」

【日　時】2006年6月15日(木) 10:00～17:00 (予定)
【会　場】虎ノ門パストラル
【内　容】
「セキュリティ機能強化OSを利用した内部統制整備と運用」をテーマに、行政機関ならびに関係機関、監査法人をはじめとする民間企業の専門家により、様々な視点での内部統制確立への最新情報と、セキュリティ機能強化OSによって得られるメリット等をご紹介いたします。

【イベント情報詳細】
http://www.jtsl.co.jp/

◆お問い合わせ先◆
セキュアOSカンファレンス事務局(日本高信頼システム内)
Tel: 03-3868-8921
E-mail: sec4conf@jtsl.co.jp

NSF2005 概要報告

JNSA 主席研究員　安田　直義

2005年12月1日(木)～2日(金)に大手町サンケイホールでNetwork Security Forum 2005(NSF2005)が開催されました。今年は、コンファレンスに重点を置く形で実施され、事前申し込みが軒並み満席となる大盛況となりました。

<来場者数>

12月1日(木) 天候/晴れ 730名

12月2日(金) 天候/晴れ 337名

合計来場者数 1,067名

コンファレンスの構成

コンファレンスは、p28、p29のプログラムのように2日間に渡って開催され、両日とも午前中の基調講演、特別講演と、午後のJNSAセッションとソリューションセッションで構成されています。

基調講演は政府系の施策等の話、特別講演は学術系の技術や動向解説という、どちらかというと俯瞰的な立場からの話題が取り上げられています。一方午後のJNSAセッションは、技術系と管理系の2セッションがパラレルに走り、さらにJNSA会員企業の製品サービスを中心とした紹介セミナーが2セッション用意され、4セッションが同時進行する形で進められました。沢山のセッションが用意され、あるいは聞きたいセッションが重なってしまった方もいらっしゃるかもしれませんが、それだけネットワークセキュリティの内容の裾野が広がり、専門性も高くなってきたのだと思います。

1日目の概要

1日目の基調講演として、内閣官房情報セキュリティセンター（NISC)参事官補佐 山崎琢矢氏による「我が国の戦略はいかにあるべきか－内閣官房を中心とした情報セキュリティ政策の取り組み－」が話されました。

1日目の基調講演：山崎琢也氏

2日目の特別講演：安田浩教授

日本にとっての情報セキュリティの重要性を広く知ってもらうことが山崎氏の役割である、ということで、政府サイドの取組が紹介されました。情報セキュリティは決まった方法がある訳ではないので、色々な観点からの情報を示して考えてゆきたいということです。

技術と人間系が両輪にならなくてはいけないといわれていましたが、5年前は身にしみていなかったそうです。現在では、外からの攻撃の代表例であるサイバー攻撃や、非意図的要因、災害時の被害拡大、思わぬ連鎖反応等を視野に入れて対策を考えているとのことです。また、最近は、事業継続性の確保に関心が移ってきているので、この一環として情報セキュリティを位置づける方向にあることが指摘されました。

情報セキュリティは、法律で義務付けるべきであるという議論がありますが、法律で規制をすれば対策の推進になるのではなく、各推進主体・組織が自主的に対策を取る方が望ましいと考えているとのことです。政府が決めることではなく、国民の合意が重要であるので、今後ともご意見を是非いただきたいと締めくくられました。

続いて特別講演は、横浜国立大学大学院環境情報研究院の松本勉教授による「個人認証におけるバイオメトリクス技術の活用と課題」という話題です。

生体認証に係わる技術的な動向や問題提起をデモを交えて判りやすく説明されました。生体認証技術は、生体検知情報からテンプレート情報を作成し、データベース登録を行うのが基本となりますが、生体情報は本来アナログデータなので、デジタル化するデータ変換方法によっては登録できなかったり照合に失敗することがあるという本質論を踏まえた解説がされました。

生体情報は永久不変であることは確かですが、メリットばかりではなくデメリットもあります。正しい生体を「違う」と間違えたり、違う生体を「正しい」と受け入れてしまう誤認識は、パターン認識を利用している以上、避けて通れない根本的な問題であり、登録時の本人確認をどのように併用するかが重要であると指摘されました。これは、暗号システムが方式を明示しても鍵を安全に保持すれば安全を保てるのに対して、生体認証は方式とパターンデータが密接な関連を持つので、方式を公開できないのが現実だそうです。

デモ事例として、指紋認識でシリコンゴム製の擬似指を受け入れてしまったり、虹彩認識もお面ですり抜けられる例が示され、会場からため息が漏れていました。考えなければならない対策の概要が示されましたが、妄信せずうまく使いこなすことが重要であるということで締めくくられました。

午後のJNSAセッションは、前述したように技術系と管理系が平行して開催されましたが、技術系セッションから高木浩光氏のお話を紹介しましょう。

イベント開催の報告

独立行政法人産業技術総合研究所情報セキュリティ研究センター主任研究員の高木 浩光氏による「安全なWeb利用の鉄則～消費者に今伝えるべき本当のこと～」が話されました。高木氏は技術の裏付けの基に、歯に衣を着せない問題提起をされることで各方面で知られており、JNSAのNSF2004でもご講演いただいています。

まず、最近の脆弱性や不正アクセス関係は、多数のターゲットを対象にするのではなく、少数の特定ターゲットを狙ってくるので、メールを疑ってかかるというような対策では既に時代遅れになっているという指摘がありました。ウイルス対策ソフトは、無差別に攻撃してくるタイプには有効だが、個別攻撃をするスパイウエアなどには無力であるということです。

本当に大切なのは、どのようなファイルを開いたり操作をしてはいけないか、ということであり、例えば、DNSを騙すファーミング対策にしても、個人情報はSSLページにしか載せないようにすれば、認証で警告が出たときに「No」を押せばすむことであり、証明書の中身を確認するまでもない、との説明がありました。

HTMLメールを使ったメールマガジンは、もう役目を終わったということなど、さまざまな対応策や考え方の解説があり、いつもながら考えさせられる講演でした。

2日目の概要

2日目の基調講演は、経済産業省商務情報政策局情報セキュリティ政策室課長補佐 田辺雄史氏による「情報セキュリティエコシステムの構築に向けて～情報セキュリティガバナンスによる「系」の確立～」が話されました。

情報セキュリティは継続して達成し続けることが必要であることを踏まえ、これまでの経済産業省の情報セキュリティに対する取り組みのご紹介と情報セキュリティガバナンス確立の必要性について説明がありました。

これまで進められてきた技術的対策、情報共有、普及啓発・人材育成に加えて、これからは情報セキュリティを守るための組織体制の確立が重要であることが示されました。この問題は情報システムに限らず、企業全体の活動を適正なものとするための内部統制(コーポレートガバナンス)として考えられます。

米国のSOX法に基づいた内部統制の項目のうち、情報セキュリティ部分がIT統制と呼ばれます。IT統制のフレームワークとしてCOBITやISO/IEC17799があげられました。

情報セキュリティガバナンスを推進するために3つのツールが用意されるそうです。(1)現状を理解するための「情報セキュリティベンチマーク」、(2)法遵守や社会的責任を説明する「情報セキュリティ報告書モデル」、(3)IT事故に備えるための基準である事業継続計画を策定するための「事業継続計画策定ガイドライン」が該当します。最後に情報セキュリティガバナンスの確立に、これらツールを活用してほしいと締めくくられました。

特別講演は、東京大学 安田浩教授による「ユビキタス時代の個人情報保護と著作権管理」が話されました。

ユビキタスと情報セキュリティについて幅広い話題を解説されました。

インターネットや無線通信など、安心安全に使う

ためには多くの問題について考えていかなければならないことが、わかりやすく説明されました。

まず、個人認証について、認証そのものの仕掛けや考え方について分析がされました。一般的な個人認証の評価基準である「破られにくさ」以外に、盗まれる危険性や盗まれた後の対処についても説明され、関心を誘っていました。

情報の利用者としてはITセキュリティガバナンスの確立が必要であり、システムの提供者としてはより深い考察に基づいた開発が必要なのだ、ということが納得されていました。

最後に「最近のネットワークの脅威は何か、そして、我々は何をすべきか～脆弱性関連情報流通体制の現状と今後～」というテーマで、セキュリティ関係の官・民のコアメンバー7名を一堂に会したパネルセッションが行われました。詳しいメンバーはプログラム一覧をご覧ください。

最初に各メンバーからのショートプレゼンが行われ、モデレータの下村氏から、安全安心を実現するには、広い分野の関係者の協力が必要であり、経済産業省を中心とした情報セキュリティ早期警戒パートナーシップなどの広いスキームが作られ、そのスキームに添った形での活動が少し見えてきたので、今回関連するメンバーに出席してもらい、現状と今後についてディスカッションしていきたい、というパネルの趣旨について説明されました。

各パネラーからのさまざまな角度からの問題提起と会場からの質疑やコメントを含め、活発な議論が展開されました。まとめとしては、脅威そのものが変化しているので、新たな脅威への対応を行うために、対象の拡大や、共同戦線が必要であり、コスト負担についても考えなければならないだろう、ということで、時間切れぎりぎりまで熱い討論が続きました。このテーマは引き続き機会のあるごとに継続して考えてゆくことを参加者全員が確認をしてひとまず終了しました。

さいごに

2005年のNSFは、ネットワークセキュリティが新たな局面に到達したことを実感させられるものでした。確かに技術面は基礎的な部分は概ね見通しがつき、更に深い部分はより専門的になってきています。それに対応して、施策や運用管理面での基本的な問題がクローズアップされてきているようです。

来年はまた新たな試みや状況が出てくるかもしれません。会員の皆様からのいろいろなご意見やアイディアを頂戴できれば幸いです。

イベント開催の報告

プログラム一覧

■ 2005 年 12 月 1 日（木）

	A 会場	B 会場	C 会場	D 会場
10:30 ～ 11:30	【A-11】基調講演 1 我が国の戦略はいかにあるべきか ー内閣官房を中心とした情報セキュリティ政策の取り組みー 内閣官房情報セキュリティセンター（NISC）参事官補佐　山崎 琢矢			
11:35 ～ 12:35	【A-12】特別講演 1 個人認証におけるバイオメトリクス技術の活用と課題 横浜国立大学大学院環境情報研究院 教授　松本 勉			
12:35 ～ 13:20	休　憩			
	JNSA セッション		ソリューションセッション	
	技術系	管理系		
13:20 ～ 14:15	【A-13】 技術セッション 1 「安全な Web 利用の鉄則」～消費者に今伝えるべき本当のこと～ 独立行政法人産業技術総合研究所 情報セキュリティ研究センター主任研究員 高木 浩光	【B-13】 マネジメントセッション 1 デジタル・フォレンジックスの効用 弁護士 / 宇都宮大学工学部講師 高橋 郁夫	【C-13】 Web アプリケーション防御の切り札、Web アプリケーションファイアウォール機能のご紹介 F5 ネットワークスジャパン株式会社 プロダクトマーケティングマネージャ 福田 健男	【D-13】 消費者が求めるセキュリティ対策：次の一手 NRI セキュアテクノロジーズ株式会社 情報セキュリティ調査室 室長 工学博士　菅谷 光啓
14:25 ～ 15:20	【A-14】 技術セッション 2 インターネットハッキング最前線 株式会社セキュアブレイン チーフテクノロジーオフィサー　山村 元昭	【B-14】 マネジメントセッション 2 海外における内部統制と情報セキュリティに関する動向と我国への影響 KPMG ビジネスアシュアランス株式会社 常勤顧問　喜入 博	【C-14】 事故から学ぶスパイウェア対策 株式会社ラック 取締役執行役員 SNS 事業本部長 西本 逸郎	【D-14】 企業内業務システムにおけるセキュリティの課題と TCO に優れた効果的な対策 株式会社ディアイティ 製品事業本部エンタープライズセキュリティビジネスユニット マネージャ　今泉 拓
15:30 ～ 16:25	【A-15】 技術セッション 3 セキュア OS の特徴的機能とシステム適用 日本高信頼システム株式会社 代表取締役社長　澤田 栄浩	【B-15】 マネジメントセッション 3 医療現場でのセキュリティとリスク管理 NTT 東日本関東病院 運営企画部 医療情報 e-M 部門 宇羅 勇治	【C-15】 セキュリティ情報マネジメント（SIM）システムを使いこなすには 住商情報システム株式会社 情報システムグループ グループ長補佐兼セキュリティソリューション事業部 事業部長補佐　二木 真明	【D-15】 CA が提唱するアイデンティティ / アクセスマネジメントについて コンピュータ・アソシエイツ株式会社 プロダクト・マーケティング部エンタープライズ・プロダクト・プランニンググループ　プロダクトマーケティングマネージャー　金子 以澄
16:35 ～ 17:30	【A-16】 技術セッション 4 BOT を中心とした脅威とアジアでの動き マカフィー株式会社 AVERT（緊急ウィルス対策チーム）研究員 本城 信輔	【B-16】 マネジメントセッション 4 2004 年度個人情報漏えい事件の分析と想定賠償額の算定による評価 JNSA セキュリティ被害調査ワーキンググループリーダー 株式会社ディアイティ 山田 英史、CISSP	【C-16】 企業価値を高める最新セキュリティリスクマネジメント トランスデジタル株式会社 セキュリティ事業部 セキュリティコンサルタント　西野 光、GSEC	【D-16】 セキュリティ監査結果がもたらす、システム運用シナリオの変化 NEC ネクサソリューションズ株式会社 第三システム事業部マネージャ 小峰 光

■ 2005 年 12 月 2 日（金）

	A 会場	B 会場	C 会場	D 会場
10:30 ～ 11:30	【A-21】基調講演 2 情報セキュリティエコシステムの構築に向けて 経済産業省商務情報政策局情報セキュリティ政策室 課長補佐　田辺 雄史			
11:35 ～ 12:35	【A-22】特別講演 2 ユビキタス時代の個人情報保護と著作権管理 東京大学 教授　安田 浩			
12:35 ～ 13:20	休　憩			

	JNSA セッション		ソリューションセッション	
	技術系	管理系		
13:20 ～ 14:15	【A-23】 技術セッション 5	【B-23】 マネジメントセッション 5	【C-23】	【D-23】
	ネットワークセキュリティの知識体系化と浸透にむけて 奈良先端科学技術大学院大学 情報科学研究科 助教授　門林 雄基	情報セキュリティマネジメントに関わる ISO 規格化動向 ― ISO27000 シリーズのご紹介 日本電気株式会社 政策調査部 技術標準エキスパート　平野 芳行	1. 求められる情報セキュリティ専門家 2.BCM について～何があっても大丈夫？～ NTT コミュニケーションズ株式会社 プラットフォームサービス部 セキュリティコンサルタント　CISSP、副島 聡	トレンドの先端を行く米国 IT セキュリティの最新動向 株式会社フォーバル グループ最高技術責任者（CTO）兼 フォーバル クリエーティブ取締役 ウィリアム 齋藤
14:25 ～ 15:20	【A-24】 技術セッション 7	【B-25】 マネジメントセッション 7	【C-25】	【D-25】
	「セキュリティ対策としての暗号の実装と課題」 JNSA 技術部会 S/MIME ワーキンググループリーダー 磐城 洋介	戦略的に取り組む情報セキュリティ・ガバナンス アイ・ビー・エム ビジネスコンサルティングサービス株式会社 チーフ・セキュリティ・オフィサー、パートナー、IBM Distinguished Engineer、IBM アカデミー会員　大木 栄二郎	e- 文書法におけるタイムスタンプの必要性 日本セーフネット株式会社 エンタープライズセキュリティ事業部 事業部長　小池 康幸	ID 管理基盤システムの実現～現実と理想～ 東芝ソリューション株式会社
15:30 ～ 16:25	【A-25】 技術セッション 8	【B-25】 マネジメントセッション 8	【C-25】	【D-25】
	多様化するマルウェアの実態と対策～既存のウイルス管理ではなぜ駄目なのか？スパイウェアのポリシー管理～ 株式会社アークン 代表取締役　渡部 章	“(ECOM) セキュリティ対策評価モデル”の紹介 元電子商取引推進協議会（ECOM） 重松 孝明	マイクロソフトのセキュリティ関連技術解説 マイクロソフト株式会社 セキュリティ戦略グループ シニアプロダクトマネージャ　古川 勝也	導入時期迫る日本版 SOX 法に備えた IT ソリューションの紹介 菱洋エレクトロ株式会社 システム情報機器 営業第 2 本部 営業第 3 部 営業第 3 グループ グループリーダー 平野 元洋
16:35 ～ 17:30	【A-26】 パネルセッション ＜16：35 ～ 17：50＞	【B-26】	【C-26】	【D-26】
	最近のネットワークの脅威は何か、そして、我々は何をすべきか～脆弱性関連情報流通体制の現状と今後～ 日本ネットワークセキュリティ協会理事・事務局長　株式会社ディアイティ代表取締役社長　下村 正洋 内閣官房情報セキュリティセンター(NISC) 参事官補佐　岡谷 貢 独立行政法人 情報処理推進機構(IPA) セキュリティセンター 情報セキュリティ技術ラボラトリー長　福澤 淳二 有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）情報流通対策グループマネージャ 椎木 孝斉 株式会社 NTT データ セキュリティサービスユニット 部長 西尾 秀一 KDDI 株式会社 情報セキュリティ推進部 部長（兼務） NICT セキュリティ高度化グループリーダ 中尾 康二 日本電気株式会社 IT 戦略部 セキュリティ技術センター シニアマネージャー　宮地 利雄	不正アクセスによるサイト閉鎖・個人情報漏洩を防げ！Web セキュリティ実践セミナー 京セラコミュニケーションシステム株式会社 IT プラットフォーム事業本部 インターネットビジネス事業部 事業部長　徳丸 浩	マカフィーが考えるセキュリティ・ライフサイクル マカフィー株式会社 マーケティング本部 本部長 久保田 直己	導入・運用を容易にする PKI ソリューション（S/MIME、アクセスコントロール） サン電子株式会社 e ソリューション事業部 取締役 事業部長 小嶋 修

2005 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、情報犯罪を防ぐことはできません。
こうした状況をふまえ、経済産業省とNPO日本ネットワークセキュリティ協会(JNSA)では、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。2005年度の開催状況は以下のとおりです。

会場では、映像付きのCD-ROMの冊子とノベルティを参加者全員にお配りしています。2006年度も引き続き開催してまいりますので、ぜひ、お近くで開催の折はご参加下さい。

【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3月1日現在)

2005年度「インターネット安全教室」開催一覧

■ 新規開催 ■

	日　程	開催地	共催団体	会　場
1	6月17日(金)	岩手県	岩手県インターネットプロバイダー防犯連絡協議会、 財団法人いわて産業振興センター	マリオスビル
2	7月6日(水)	山形県	山形県高畠町	高畠町中央公民館
3	8月5日(金)	鹿児島県	鹿児島大学学術情報基盤センター (協力:財団法人ハイパーネットワーク社会研究所)	鹿児島大学
4	8月27日(土)	長野県	上田市、上田市教育委員会、丸子町、丸子町教育委員会、 真田町、真田町教育委員会、武石村、武石村教育委員会	上田市マルチメディア情報センター
5	9月8日(木)	静岡県	静岡情報産業協会、静岡市	B-nest静岡市産学交流センター
6	10月20日(木)	福島県	会津若松市、喜多方市	会津若松市文化センター
7	10月23日(日)	宮崎県	株式会社宮崎県ソフトウェアセンター、宮崎公立大学	宮崎公立大学
8	10月30日(日)	富山県	株式会社富山県総合情報センター	富山県総合情報センター
9	11月15日(火)	山梨県	玉穂町、NPO法人ITコーディネータ山梨(ITC山梨)	玉穂町「生涯学習館」
10	11月19日(土)	山口県	山口県セキュリティーマネジメントフォーラム	徳山大学
11	11月20日(日)	福岡県	北九州市 (協力:財団法人ハイパーネットワーク社会研究所)	西日本総合展示場
12	11月22日(火)	茨城県	茨城県消費生活センター	取手市福祉交流センター
13	11月26日(土)	石川県	NPO STAND	ITビジネスプラザ武蔵
14	12月22日(木)	埼玉県	秩父市	秩父市歴史文化伝承館ホール
15	1月17日(火)	京都府	京都高度情報化推進協議会、京都府	舞鶴市西駅交流センター
16	2月5日(日)	山口県	宇部市、宇部市教育委員会	宇部市ときわ湖水ホール
17	2月11日(土)	滋賀県	滋賀県立瀬田工業高等学校、滋賀県立瀬田高等学校、 NPO滋賀県情報基盤協議会(IT-shiga)	滋賀県立瀬田工業高等学校
18	2月24日(金)	香川県	香川県情報サービス産業協議会、 香川県プロバイダー等防犯連絡協議会	サンポート高松 e一とぴあ・かがわ 「BBスクエア」
19	2月26日(日)	群馬県	群馬県	ビジターセンター
20	3月4日(土)	長崎県	県立長崎シーボルト大学 (協力:財団法人ハイパーネットワーク社会研究所)	県立長崎シーボルト大学
21	3月8日(水)	三重県	鈴鹿工業高等専門学校、NPO東海インターネット協議会	鈴鹿工業高等専門学校
22	3月24日(金)	宮城県	NPO仙台インターネット推進研究会	せんだいメディアテーク

■ 独自開催 ■　※共催団体が中心となって運営・開催していただく会場です

日　程	開催地	共催団体	会　場
2005年5月～ 2006年3月	佐賀県	佐賀県ネットワーク・セキュリティ対策協議会、 NetComさが推進協議会、佐賀県	全県下8地域での分散開催 (1)武雄/杵島地区 (2)佐賀地区 (3)唐津地区 (4)伊万里/有田地区 (5)多久/小城地区 (6)鹿島/藤津地区 (7)鳥栖/三養基地区 (8)神埼地区"
2005年6月～ 2006年3月	神奈川県	NPO情報セキュリティフォーラム 他	県下19会場で順次開催 (1)横浜市　(2)秦野市 (3)相模原市　(4)茅ヶ崎市 (5)川崎市　(6)横浜市 (7)大和市　(8)小田原市 (9)厚木市　(10)横浜市 (11)横須賀市　(12)平塚市 (13)藤沢市　(14)横浜市 (15)松田町　(16)清川村 (17)秦野市　(18)葉山町 (19)鎌倉市
6月23日(木)	福井県	ナレッジふくい	福井県生涯学習館(ユー・アイふくい)
2005年10月～11月	奈良県	なら情報セキュリティ研究会	(1)奈良産業大学 (2)帝塚山大学学園前キャンパス
2006年11月～12月	兵庫県	兵庫県、財団法人ひょうご情報教育機構、 ひょうご情報セキュリティ推進会議	(1)神戸市産業振興センター (2)姫路商工会議所会館 (3)豊岡市民会館"
11月5日(土)	愛知県	NPO東海インターネット協議会	マナハウス
11月19日(土)	大分県	大分県立芸術文化短期大学 (協力: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
2006年11月	島根県	NPOプロジェクトゆうあい	(1)隠岐島文化会館 (2)テクノアークしまね"
11月26日(土)	新潟県	NPO新潟情報セキュリティ協会	NICOプラザ会議室
2005年11月～ 2006年1月	長野県	上田市マルチメディア情報センター	上田市マルチメディア情報センター（2回）
11月27日(日)	岡山県	おかやま情報ボランティアフォーラム、 株式会社エス・シー・ラボ	灘崎町総合福祉センター
12月3日(土)	和歌山県	NPO情報セキュリティ研究所	和歌山県情報交流センター Big・U
12月10日(土)	山口県	山口大学、 山口県セキュリティーマネジメントフォーラム	山口大学
12月22日(木)	栃木県	NPO栃木県シニアセンター、栃木県	栃木市市民会館
1月18日(水)	京都府	京都高度情報化推進協議会、京都府	キャンパスプラザ京都
1月27日(金)	岐阜県	かにぱそこんくらぶ	可児市文化創造センター
2月17日(金)	熊本県	NPO熊本県次世代情報通信推進機構	くまもと県民交流館パレア
2月25日(土)	滋賀県	NPO滋賀県情報基盤協議会(IT-shiga)	滋賀県立八幡工業高校
3月25日(土)	栃木県	おおひらパソコンクラブ、NPO栃木県シニアセンター	ゆうゆうプラザ
3月26日(日)	千葉県	NPO幕張メディアアソシエイツ	ベイタウン・コミュニティコア

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

事務局お知らせ

JNSA ANNOUNCE

1. 主催セミナーのお知らせ

●「2005年度JNSAワーキンググループ成果報告会」

日　時： 2006年5月30日(火)
会　場： 大手町サンケイプラザ
入場料： 無料

JNSAでは、ワーキンググループの成果報告会を開催します。
どなたでもご参加いただけますので、是非ご参加下さい。
詳細は近日中にJNSAのホームページに掲載いたします。
http://www.jnsa.org/

2. 後援イベントのお知らせ

1．LiM Tec 2006

会期： 2006年4月11日(火)～12日(水)
主催： オブジェクトテクノロジー研究所
会場： 秋葉原コンベンションホール
http://www.otij.org/event/limtec/2006/

2．RSA Conference Japan 2006

会期： 2006年4月26日(水)～27日(木)
主催： RSA Conference Japan 2006 実行委員会
会場： 東京プリンスホテル パークタワー
http://www.medialive.jp/rsaconference/

3．ソフトウェアテストシンポジウム2006大阪

会期： 2006年5月11日(木)～12日(金)
主催： ソフトウェアテストシンポジウム実行委員会
会場： 大阪商工会議所
http://www.jasst.jp/index.html

4．第10回コンピュータ犯罪に関する白浜シンポジウム

会期： 2006年5月25日(木)～27日(土)
主催： コンピュータ犯罪に関する白浜シンポジウム実行委員会(情報システムコントロール協会大阪支部、和歌山大学システム工学部、近畿大学生物理工学部、白浜町、和歌山県、和歌山県警察本部、特定非営利活動法人情報セキュリティ研究所)
会場:和歌山県立情報交流センター BigU
http://www.sccs-jp.org/SCSS2006/

5．ISACA大阪支部設立20周年記念講演会

会期： 2006年6月17日(土)
主催： ISACA（情報システムコントロール協会)大阪支部
会場： マイドーム大阪
http://www.isaca-osaka.org/

3. JNSA 部会・WG 2005 年度活動

1．政策部会

(部会長:下村正洋 氏/ディアイティ)

調査事業や様々な基準･ガイドラインの策定、他団体との連携を行う。

【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)

一年間に発生した情報セキュリティ被害の実態を調査することにより、情報セキュリティインシデントが組織に与えるインパクトを定量的に分析する。

主な活動内容としては、下記の通り。

･アンケートおよびヒアリングによる、年間の情報セキュリティ被害の実態調査

･年間の個人情報漏洩事故･事件の分析による、想定損害賠償額の算定と株価への影響の検証。

予定成果物は、情報セキュリティインシデントに関する調査報告書。

【セキュリティ市場調査WG】

(リーダー:勝見勉 氏/グローバルセキュリティエキスパート)

日本における情報セキュリティの実態を調べ、2005年度以降は実態調査数から今後の方向性を予測する。

2004年度に行った調査を基に今後の方向性を予測、更なる製品別の動向にも調査を継続する。

予定成果物は、調査レポート。

【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、JNSA活動報告書，論文など。

【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。

【スパイウェア対策啓発WG】

(リーダー:蛭間久季 氏/アークン)

ここ数年スパイウェア(不正プログラム)を利用したIT犯罪が大きく世間を賑わしている。本WGでは様々な団体、官公省庁との連携により、インターネット利用者へのスパイウェア(不正プログラム)対策の知識向上を目的として、幅広く啓発活動を実施することを主たる目的とし、JNSA版スパイウェア対策ポータルサイトを公開。

主な活動内容は以下を予定している。

- JNSA版スパイウェア(不正プログラム)の定義の作成
- 既存の他WGとの意見交換勉強会
- 各官公省庁等や産業界(団体)への啓発協力呼びかけ及び勉強会
- インターネット利用者へのスパイウェア対策の知識向上の普及活動
- 海外におけるスパイウェア対策啓発の調査･研究など

2．技術部会

(部会長:佐藤友治 氏/IRIコミュニケーションズ)

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

【セキュリティポリシーWG】

(リーダー:小杉聖一 氏/NECソフト)

2004年の活動を継続実施する。

ISMS認証基準にマッチしたサンプルポリシーを公開し、実際の策定方法を討議していく。また管理策に対応する適用すべきセキュリティ技術との対応についても調査し報告する。

予定成果物は、公開サンプルの改版とISMS（X5080）との対応表。

【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。当WGでは、不正プログラムを分類化し、タイプ別、レイア別に、その対策ソリューションを調査、整理し、マッピング化する。
予定成果物は、不正プログラム対策ガイドラインの策定。

【ハニーポットWG】
（リーダー:園田道夫 氏/JNSA研究員）
ハニーポット関連技術の研究と、実際の運用を通して得られるデータの解析とフィードバックを行う予定。
予定成果物は、ハニーポットから得られたデータの解析報告書。

【S／MIME検討WG】
（リーダー:磐城洋介 氏/NTTコムウェア）
2004年度より引き続き、メールクライアントのS/MIME機能の評価を行う。脆弱性を発見しIPA等に報告する。メール利用者向けのS/MIME機能ガイドライン（仮称）をWebコンテンツとして作成し公開する。S/MIMEメールの普及やベンダに対するメールクライアントの機能向上を促すことを目指す。
予定成果物は、S/MIMEメーラ検証レポート。

【WebアプリケーションセキュリティWG】
（リーダー:二木真明 氏/住商情報システム）
ここ1、2年でクローズアップされながら、ユーザーのみならず、ベンダにおいても、まだまだ認識が充分とはいえないWebアプリケーションのセキュリティについて考える。いくつかのテーマについて分科会的に検討を進めながら、月1回の全体会で、各分科会の進捗や成果についてレビューし、深めていく。当面のテーマとしては以下のようなものを考えている。
- Webアプリケーションセキュリティについての啓発コンテンツの作成
- Webアプリケーションセキュリティ受発注用ガイドラインの検討
- 攻撃手法などの技術的テーマを掘り下げる

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）
脆弱性の定量化アプローチについて、国外の情報を含め検討を行い、WGとしての検討結果を出す。
成果物として報告書を作成する予定。

【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）
以下の動向把握及び、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

予定成果物は、必要に応じて行う提言と研究報告の作成。

勉強会目的のワーキンググループ

【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。

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）
「インターネット安全教室」の企画·運営を通しセキュリティ啓発活動を行う。
2005年4月～8月にCD-ROM映像及び冊子のリニューアル製作を行なうと共に、2005年6月～2006年3月にかけて全国20ヵ所以上で「インターネット安全教室」を実施予定。

【セキュリティスタジアムWG】
（リーダー:園田道夫 氏/JNSA研究員）
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。

4. 教育部会

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

【CISSP-WG】
（リーダー:大河内智秀 氏/NTTコミュニケーションズ）
CISSP資格認定者が更に日本国のセキュリティ保全の価値を高めるための上級資格を日本向けに作成する際に新規追加すべきドメインについて検討し、策定を行う。

【情報セキュリティ推奨教育検討WG】
（リーダー:持田啓司 氏/SEA/J）
情報セキュリティ教育WGとして活動を始めていたが、内容を見直し再出発した。
既存の良く知られている教育コース等の調査と整理を行い、キャリアパスや研修ロードマップ等の関係を必要スキル項目などの観点で整理する。これを基にして、情報セキュリティ対策のための組織デザイン論に関する議論を行い、報告書としてまとめることを目標としている。

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/ヒューコム）
情報セキュリティ教育の実践を全国レベルで展開するために、教育に必要な実施環境や、サンプルとなる教育カリキュラムについての実証実験と評価検討を行う。経済産業省の委託プロジェクトとして、昨年度の東京電機大学での環境構築や実証教育の成果を生かし、更に複数の教育機関での実証実験を行い、情報セキュリティ教育を広く実施できる要件などを整理し報告書を作成する。

5. 西日本支部

（支部長:井上陽一 氏/ヒューコム）
JNSA西日本支部は関西に拠点を置くメンバー企業の協賛の下、西日本におけるネットワーク社会のセキュリティレベルの維持·向上並びに、日々高まる情報セキュリティへのニーズに応えるべく、先進性を追及すると共に、質の高いサービスを提供する事を目的として活動する。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:中台芳夫 氏/西日本電信電話）
西日本に拠点を持つ一般企業やユーザを対象に、ネットワークセキュリティに関する普及·啓発活動を行う。また西日本支部会員企業間の知識共有、西日本にてインターネット普及活動を行うNPOとのネットワークセキュリティ啓発に向けた連携を行う。その他、勉強会·セミナーの開催を予定している。

【中小企業向け個人情報保護対策WG】
（リーダー:市川順之 氏/伊藤忠テクノサイエンス）
2005年4月の個人情報保護法完全施行に対して中小企業がどのような状況に陥るのか、 また、できる対策は何があるのか、等について調査し、運用編としてまとめることを目的とする。

4. JNSA 役員一覧

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

理　事（50 音順）

井上　陽一	株式会社ヒューコム
後沢　忍	三菱電機株式会社　情報技術総合研究所
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	セコムトラストネット株式会社
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
鷲見　晴美	株式会社ネットマークス
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
松尾　直樹	ＮＴＴコミュニケーションズ株式会社
山野　修	ＲＳＡセキュリティ株式会社
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

今井　秀樹	東京大学　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2月6日現在 211社 50音順）

【あ】

(株)アークン
RSAセキュリティ（株）
(株) IRIコミュニケーションズ
(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)アイティインテグレーションズ
(株) IDGジャパン
(株) ITサービス
(株)アイ・ティ・フロンティア
(株) ITプロフェッショナル・グループ New
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)アクセンス・テクノロジー
(株)網屋
アライドテレシス(株)
アラクサラネットワークス(株)
(株)アルゴ21
(株)アルテミス
(株)イオノス
伊藤忠テクノサイエンス(株)
学校法人 岩崎学園
インターネット セキュリティ システムズ(株)
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
ウインモバイル(株) New
ウェブルート・ソフトウェア(株) New
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)
エー・アンド・アイ システム(株)
AT&Tグローバル・サービス(株)
(株)エクスフロント
(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)
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)
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)
(株)エム・ファクトリー
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)

【か】

(株)ガルフネット New
韓国電子通信研究院
(株)ギガプライズ
キヤノンシステムソリューションズ(株)
キヤノン・スーパーコンピューティング・エスアイ(株)
九電ビジネスソリューションズ(株)
京セラコミュニケーションシステム(株)
(株)クインランド
クオリティ（株）
KLabセキュリティ（株）
(株)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)クロスワープ
(株)コシダテック
(株)コネクタス
コンピュータ・アソシエイツ(株)
コンピューターサイエンス(株)

【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 New
サン電子(株)
サン・マイクロシステムズ(株)
(株) CRCソリューションズ
(株)シーエーシー
(株)シー・エス・イー
ジーエフケー マーケティングサービス ジャパン(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)
シスコシステムズ(株)
(株)シマンテック
シムデスク・テクノロジーズ
寿限無(株)
(株)翔泳社
(株)情報数理研究所
新星商事(株) New
新日鉄ソリューションズ(株)
新日本監査法人
図研ネットウエイブ(株)
(株)ステラクラフト
住商情報システム(株)
住生コンピューターサービス(株)
セ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
(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)
セコムトラストネット(株)
(株)セゾン情報システムズ
セントラル・コンピュータ・サービス(株)
ソニー (株)
ソニー・エリクソン・モバイルコミュニケーションズ(株)
ソフトバンクBB (株)
ソラン(株)
ソラン・コムセック・ コンサルティング(株)
(株)ソリトンシステムズ
ソレキア(株)
(株)損保ジャパン・リスクマネジメント

【た】

大興電子通信(株)
大日本印刷(株)
(株)タクマ
中央青山監査法人
TIS (株)
(株)ディアイティ
テクマトリックス(株)
デジタルアーツ(株)
デジボックス(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) New
東京海上日動火災保険(株)
東京情報コンサルティング(株)
東京日産コンピュータシステム(株)
東芝ソリューション(株)
東洋ネットワークシステムズ(株)
凸版印刷(株)
トップレイヤーネットワークスジャパン(株)
トランスデジタル(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)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム システムズエンジニアリング(株)
日本オラクル(株)
日本高信頼システム(株)
日本コムシス(株)
日本ジオトラスト(株)
(株)日本システムディベロップメント
日本セーフネット(株)
日本電気(株)
日本電気エンジニアリング(株)
日本電信電話(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
(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)

【は】

(株)ハイエレコン
(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)ヒューコム
(株)ビー･エス･ピー
(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
富士通電機アドバンステクノロジー（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)プロティビティジャパン

【ま】

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

【や】

ユーテン･ネットワークス(株)
横河電機(株)

【ら】

(株)ラック
リコーテクノシステムズ(株)
リコー･ヒューマン･クリエイツ(株)
菱洋エレクトロ(株)
(有)ロボック

【わ】

(株)ワイ･イー･シー

【特別会員】

特定非営利法人 アイタック
ジャパン データ ストレージ フォーラム
電子商取引安全技術研究組合
東京大学大学院 工学系研究科
社団法人 日本インターネットプロバイダー協会
社団法人 日本パーソナルコンピュータソフトウェア協会
ブエノスアイレス州情報セキュリティ協会

6. JNSA 年間活動（2005 年度）

4月	4月13日	第1回技術部会リーダー会
	4月13日	第1回幹事会
	4月19日	第1回教育部会
	4月26～27日	UML Forum/Tokyo2005 後援
	4月28日	第1回西日本支部会合
5月	5月10日	2005年度理事会
	5月10日	迷惑メール対策カンファレンス 後援
	5月11日	2005年度技術部会
	5月12～13日	RSAカンファレンス2005Japan 後援
	5月13日	第1回政策部会
	5月13日	第3回セキュアOSカンファレンス後援
	5月19～21日	第9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31日	第2回幹事会
6月	6月6～10日	NetWorld+Interop2005 Tokyo 後援
	6月13日	WG成果報告会開催（大手町サンケイプラザ）
	6月13日	2005年度総会（大手町サンケイプラザ）
	6月16日	HOSTING-PRO2005 後援
	6月21日	2005年度JASA情報セキュリティ監査フォーラム東京 後援
	6月28日	インターネット安全運動シンポジウム
7月	7月1日	第2回西日本支部会合・勉強会
	7月7日	第3回幹事会
	7月13～15日	自治体総合フェア2005 協賛
	7月13～15日	ワイヤレスジャパン2005 後援
	7月15日	JaSST in OSAKA 2005 後援
	7月25日	第1回 データベース・セキュリティ・コンソーシアム セミナー後援
8月	8月2～7日	セキュリティキャンプ2005後援
	8月29日	第3回西日本支部会合
	8月31日	第4回幹事会
	8月31～9月1日	2005年JESAP電子署名.認証フォーラム後援
9月	9月6～7日	SCMフォーラム 2005後援
	9月7～9日	モノづくり総合展九州2005後援
	9月16日	平成17年度 情報モラル啓発セミナー島根後援
	9月28～29日	第6回 ICCC（International Common Criteria Conference）2005後援
10月	10月6～8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2005協力
	10月11日	情報セキュリティ特別講演会後援
	10月25日	第5回幹事会
	10月25日	平成17年度 情報モラル啓発セミナー岩手後援
	10月27日	セミナー開催「NSF2005 in Osaka」
	10月28日	セミナー開催「PKI Day - PKI 技術最新事情」
11月	11月10～11日	ハイパーネットワーク2005別府湾会議後援
	11月15日	第5回enNetforumセミナー後援
	11月15～16日	HOSTING-PRO 2005 Fall協賛
	11月17～18日	Tokyo Intenational Security Conference 2005後援
12月	12月1～2日	「Network Security Forum2005」開催
	12月5～10日	KOREA ITビジネス商談会2005後援
	12月6～9日	Security Day開催（Internet Week 2005内）
	12月9日	第4回西日本支部会合
	12月14日	第6回幹事会
	12月16日	セミナー開催「情報セキュリティ人材育成シンポジウム in 岡山」
	12月19～20日	第2回デジタル・フォレンジック・コミュニティ 2005inTOKYO 後援
	12月20日	平成17年度 情報モラル啓発セミナー大阪 後援
1月	1月23日	2006年度JNSA新年賀詞交換会
	1月24～25日	STORAGE NETWORKING WORLD2006 後援
	1月25日	JASA情報セキュリティフォーラムIn Winter名古屋後援
	1月30～31日	ソフトウェアテストシンポジウム2006東京 後援
2月	2月1	JASA情報セキュリティフォーラムIn Winter大阪後援
	2月1日	LSForumSeminar 2006 Winter後援
	2月1～2日	情報セキュリティ総合的普及啓発シンポジウム後援
	2月1～3日	PAGE2006 後援
	2月1～3日	NET&COM2006 後援
	2月6日	第7回幹事会
	2月8日	日本PKIフォーラム協賛
3月	3月2日	セミナー開催「情報セキュリティ人材育成シンポジウム in 東京」
	3月16日	セミナー開催「第8回西日本支部主催セキュリティセミナー」
	3月17日	第3回政策部会
	3月22日	インターネット安全教室全国連絡会議

「2005年6月～2006年3月「インターネット安全教室」開催

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

★ JNSA 部会、WG の会合議事録は会員情報のページ http://www.jnsa.org/member/giji_2005/index.html に掲載しています。（JNSA 会員限定です）

7. JNSA について

■会員の特典

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

8. お問い合せ

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

西日本支部
〒 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

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.16

2006 年 3 月 31 日発行

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

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

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

西日本支部
〒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