

JNSA Press

Japan Network Security Association

Vol.24
December 2008

CONTENTS

ご挨拶

米国セキュリティベンチャー事情と 1
日本のセキュリティビジネス

特 集

- 「EV SSLと暗号の2010年問題」 3
- 「2008年上半期の個人情報漏えい」 7

JNSAワーキンググループ紹介

- 勉強会企画検討WG 12
- ISEPAスキルWG 14

会員企業ご紹介 16

JNSA会員企業情報 19

イベント開催の報告 20

「インターネット安全教室」 25

事務局お知らせ 28

JNSA年間活動 36

米国セキュリティベンチャー事情 と日本のセキュリティビジネス

住商情報システム株式会社
JNSA 幹事・技術部会長 二木 真明



この数年、米国のベンチャー企業を訪問し、日本で売れそうな製品を探してローカライズするなど、日本での販売まで持ち込む仕事を中心にしてきました。しかし、最近、そうした仕事に困難を感じるようになってきました。それは、かつて、夢と希望にあふれてIPO（株式上場）を夢見たベンチャー企業が、ITバブルの崩壊なども経験し、短期間でリターンを求める投資家の志向もあって、特定の狭い範囲の技術に特化してしまうようになってきたからです。これは、自ら新しい市場を切り開き、そのリーダーとなることを目標とするのではなく、既存の市場で優位性を確保する道具となりそうな要素技術に特化し、その技術をメジャープレイヤーに買ってもらうという方向にほかなりません。IPOを目指すには長い期間を要し、IPO後にはさらに大きな社会的責任が待ち受けています。より安易な道を目指す方向は、経営的な視点からは正しいのかもしれませんが。我々もかつては特徴ある製品を開拓し、日本で市場を開拓し、時間をかけて育て上げる余裕がありましたが、今はもうそんな余裕はありません。実際、こうした形で製品開拓をしてきた企業の多くが、同じ困難を感じているはずで、つまり、競争力のある製品をいち早くみつけ、先行利益を確保するようなビジネスモデルは難しくなりつつあり、大手のベンダが提供する製品やサービスを同業他社と競争して売りながら、自分たちの付加価値をつけ、それをいかにお金にしているのか、ということ、いままで以上に真剣に考えなければいけなくなっているわけです。

一方、セキュリティという世界も様変わりしつつあります。かつては、セキュリティといえば、専門性の高いビジネスであり、それ単独で成り立つと考えられてきました。しかし、実際は、ITのいたるところにセキュリティは必要で、それらのセキュリティはITの各分野と密接に関連しています。たとえばアプリケーションシステムの開発に業務知識が不可欠なように、セキュリティにおいても、その分野ごとに必要な知識が異なりますし、こうした知識がまったくない状態では、セキュリティを語るものが難しくなっています。たとえば、ネットワークを知らないファイアウォール技術者はもはや通用しませんし、Webセキュリティを語るには、データベースやプログラミングの知識や経験、開発プロセスの知識が不可欠です。そういう意味では、セキュリティというかつて独立していた世界の多くの部分が、ITというより大きな領域と融合しつつあると言えるでしょう。ITメジャー企業がセキュリティ企業を買収するという動きが激しくなっているのも、こうしたことを裏付ける現象では

ないかと思えます。こうした中で、ITの総合力をつけていくのか、もしくは、より専門特化した方向を目指すのか、米国のベンチャー企業と同じ選択を我々は迫られているのかもしれません。

ユーザとの関係も変化しつつあります。米国では、ユーザ企業の多くに、ベンダのカウンターパートとなりうる専門家がいます。これによって、おのずとユーザ、ベンダの責任範囲が決まり互いの仕事のバランスがうまくとれているように見えます。日本ではまだまだ、ユーザ側にそうした人材が少ないこともあり、ベンダが多く仕事をユーザにかわってしなければいけないケースも多くあります。しかし、セキュリティの要求が多様化する中で、ベンダ側にはセキュリティのみならずITの総合力も求められるようになる上、ユーザ側の担当者と共通する土俵がないために、意識や認識の違いが浮き彫りになってしまうことも少なくありません。こうした問題の解決には、ユーザ側にも我々のカウンターパートとなる専門家が重要なのではないかと思えます。これは、私自身がこの2年ほどのあいだで、自社のセキュリティに主体的にかかわるようになって特に感じ始めたことです。

現在、教育サービスで提供されているトレーニングは、どちらかといえば業界側の技術者を育成するものが中心です。(本来はそうでなくても、現実にはそうなってしまっているのではないかと思えます。)しかし、これからは、ユーザ側でプロジェクト全体を統括できる、ジェネラルなセキュリティ知識をもった専門家の育成も重要なのではないかと思えます。こうした方向での教育サービスを提供できないだろうか、提供できたとして、ユーザにうまく受け入れてもらえるのだろうか、など、なかなか悩みは尽きません。業界のこれからの方向を見極めていく上でも、大いに議論してみてもうかがうかと考えているこのごろです。

EV SSLと暗号の2010年問題

— 新たな国際標準化の流れと日本市場への影響 —

日本クロストラスト株式会社
代表取締役 秋山 卓司

1. EV SSL 登場の背景

インターネット上で最も広く使われている暗号プロトコルの一つにSSLがあります。SSLは米Netscape Communication社によって、インターネットというお互いの顔の見えない、オープンなネットワーク上で重要な情報をやり取りするために提案されたもので、通信経路の暗号化とWebサイト運営者の実在確認という2つの機能があります。インターネット上でのBtoC取引の拡大とともにSSLの需要も伸び、広く普及することとなりましたが、近年ではさらにその利用範囲も拡大し、メールの送受信(SMTP/POP over SSL)や、SSL-VPNなど、同一組織、あるいはグループ内で利用されるケースも増えてきました。

このような用途では、不特定多数を対象とするWebの場合と異なり、サーバ運営者の身元確認は特に必要ないため、通信経路の暗号化のみを目的とした低コストのSSLサーバ証明書が市場に提供されるようになったのです。またこれらの証明書はサーバ運営者の身元は確認せず、ドメインの所有者か否かを審査の対象としているため、匿名での取得も可能です。

これらの実在証明の審査を省いた証明書は、同一企業内、もしくはサーバ運営者とそれを利用するユーザーの間にあらかじめ信頼関係があること(例えば自社で管理しているメールサーバへのアクセスに利用するなど)を前提にしていたのですが、不特定多数からのアクセスを前提とした通常のWebサーバに導入された場合であっても、実在証明のあるSSL証明書と同様にユーザーのブラウザには南京錠マークが表示されるため、一般のユーザーが実在証明の有無を見分けることは事実上困難であるという問題を抱えていました。

各種調査等によるとユーザー側の南京錠マークに対する信頼度は非常に高く、例えばネットショッピングの際「南京錠マークがあれば安心」という認識が広がっている一方で、このユーザーの南京錠マー

クへの信頼感を逆手にとって、実在証明の無いSSLサーバ証明書を使ったフィッシングサイトが多数報告されるに至ったのです。

この事態を受け、主要なブラウザベンダーと世界各国の認証局が中心となり、証明書発行に際するサーバ運営者の審査基準を標準化することと、またその標準化された証明書を、一般のユーザーが容易に確認できる手段を提供することを目的として米国で設立されたのがCAブラウザフォーラム(CABF)です。
(<http://www.cabforum.org/>)

CABFでは、これまで各認証局が個別に定めていた審査プロセスについて、全世界で統一された非常に厳格なガイドライン(EVガイドラインと呼ばれる)を定め、さらに、第三者である監査法人が、認証局がEVガイドラインを厳守していることを確認することを義務付けました。このEVガイドラインに沿って発行された証明書がEV SSLサーバ証明書と呼ばれるもので、IE7やFirefox3、Opera9.5、あるいはGoogle Chrome等の最新ブラウザでこの証明書を取得したWebサイトにアクセスすると、アドレスバーが緑に変色するため、一般のユーザーにも一目で見分けることが可能になっています。

また、日本でも国内の認証ベンダー及びブラウザベンダーが発起人となって2006年1月に日本電子認証協議会(JCAF)が設立され、日本におけるEV SSLの標準化と普及促進を目的とした活動が開始されています。
(<http://www.jcaf.or.jp/>)

2. 暗号の2010年問題とは

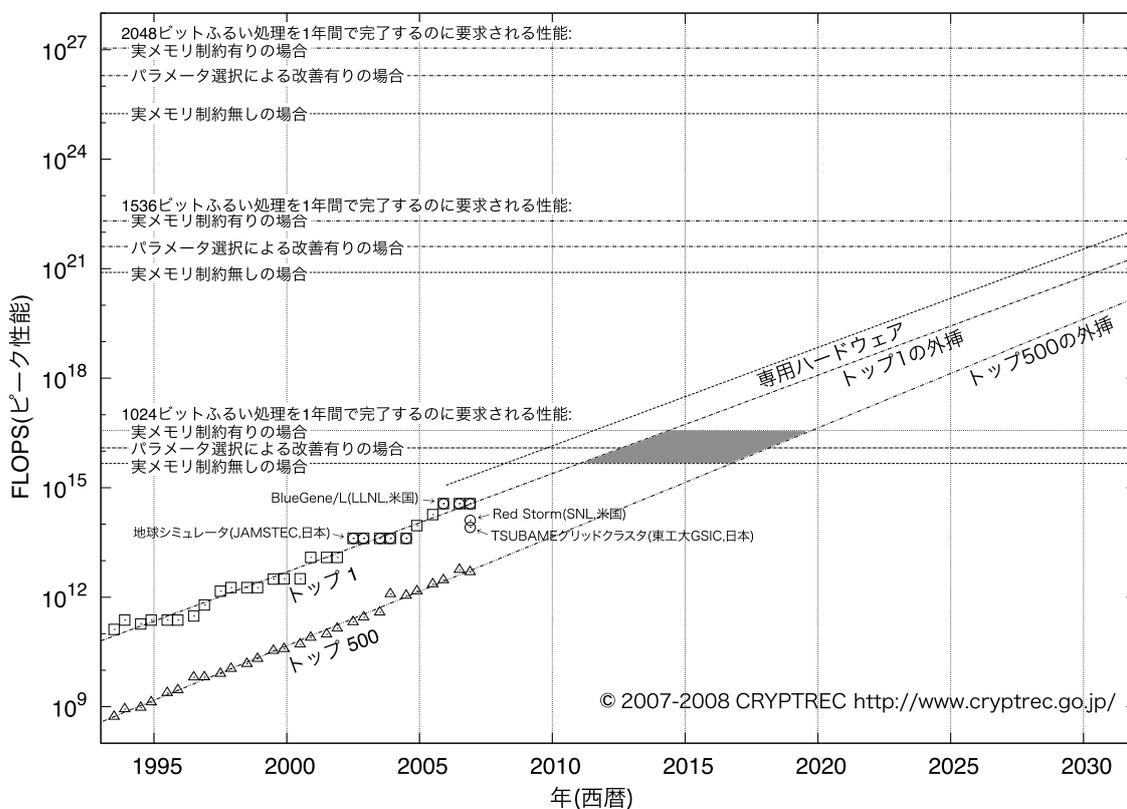
前述の通り、一般のユーザーにとってより安心、安全なインターネット環境を実現するために、世界各国30社以上の認証局と、主要なブラウザベンダーが参加して策定されたEV SSLですが、そのガイドラインには発行時の審査プロセスと合わせて、証明書の技術的仕様についても言及されており、特にSSLに使われている公開鍵暗号の鍵長については、

2010 年末を期限として、従来広く使われていた 1024 ビット RSA 鍵から 2048 ビット RSA 鍵へと移行することが義務づけられています。

暗号は解読に使われる計算機の性能向上や、特定のアルゴリズムについての研究が進むに従い、徐々にその相対的な強度は弱まっていくことになります。従って、長期間の利用が想定される場合には、将来

的な強度低下をあらかじめ想定した上で暗号の仕様が選定され、また定期的にその強度が検証されなければなりません。

では、暗号はどれくらいの強度を持つべきなのでしょう？それに答えるのは簡単なことではありませんが、政府の暗号技術検討会 2006 年度報告書に掲載された次のグラフが参考になるかと思います。



グラフの縦軸には解読の対象となる暗号の強度が示されており、斜めの線は各年代における計算機の処理能力向上を表しています。そして、2015年を中心とした赤い平行四辺形として示された部分が、従来広く使われてきた 1024 ビット RSA が計算機の処理能力向上とともに、解読の危険性が高まるであろう時期を示していることが、このグラフから読み取って頂けるかと思います。

つまり 2010 年は何十年に一度の暗号アルゴリズムの世代交代という大きな節目にあたり、その移行についてはコストや相互運用性の確保など、さまざま

な困難が予想されています。これがいわゆる「暗号の 2010 年問題」です。そしてこの「暗号の 2010 年問題」は、日本において、より深刻な問題となる可能性があります。

3. 日本特有の問題

EV SSL の場合には、日本市場において一部の携帯端末が 2048 ビット RSA 鍵に対応していないことが、移行における大きなハードルの一つとして指摘

されていました。現在、EV SSLのガイドラインでは、互換性確保のために1024ビットRSA鍵の利用が許されていますが、前述の通り、このまま行けば2011年以降は2048ビットRSA非対応の携帯端末からは、EV SSLサーバ証明書を採用したサイトとのSSL接続ができなくなってしまう。また、2048ビットRSAに対応した携帯であっても、現時点ではEV SSL対応のブラウザが搭載された機種はありません。

ご存じの通り、日本では多くのユーザーが携帯端末経由で日常的にインターネットにアクセスしており、携帯コンテンツについては、その絶対的規模と成長率において、世界でも類を見ない最先端の市場です。また、総務省の調査によると、Eコマースの実に20%が携帯を使用しているとのこと。

その一方で、世界的に最先端であることは、「特殊」であり、海外ではなかなか理解されにくいということでもあります。事実、当初のEVガイドライン策定段階においては、日本のベンダーが議論に参加していなかったこともあり、携帯端末をはじめとする組み込み系の機器でのSSL利用については元々想定されていませんでした。つまり、あくまでPCでの利用が前提ですから、暗号アルゴリズムの移行等に関してもオンラインアップデートで対応可能だろうと考えられていたのです。ところが、携帯端末にオンラインアップデートの仕組みはありません。新しい暗号アルゴリズムに対応するには、基本的にはユーザーに端末を買い替えてもらう必要があるのです。

JCAFでは、このように携帯がPCと比較して移行に長い期間が必要なことと、日本市場における携帯の重要性、また後述の通り日本政府が2048ビットRSAへの移行を2013年度までに完了させるという指針を出したことなどから、1024ビットRSAにしか対応していない携帯にも対応するEV SSL証明書の利用可能期間延長をCABFに対して提案しましたが、結果的に受け入れてはもらえませんでした。

4. 政府と民間の取り組み

2010年末に暗号アルゴリズムを移行させるよう

にとの勧告を出しているのは、アメリカ国立標準技術研究所(National Institute of Standards and Technology、以下NIST)という組織です。NISTは本来、米国政府の調達基準を定める機関ですが、民間にも極めて大きな影響力があり、暗号等についても事実上の標準となっています。CABFが定めたEV SSLのガイドラインも暗号の技術的仕様については、NISTの勧告に準拠しています。

一方日本では、本年4月に内閣官房情報セキュリティセンター(NISC)が、政府の情報システムで使用する暗号アルゴリズムを2013年度を目途に移行する方針を発表しました。しかし残念ながら、日本の場合は民間の規範となるべく発表されたものではなく、あくまで「政府の政府による政府のための」基準にすぎません。

つまり民間は、それぞれ独自に暗号に関する基準や移行のスケジュールを決定する必要に迫られるわけですが、個々の事業者が最新の学術的研究結果と実際に採用した場合の費用対効果、さらには相互運用性等のバランスを取って暗号アルゴリズムを適切に選定することはかなり困難な作業となることが予想されます。

前述の通り、日本市場においては、携帯をはじめとする組み込み系機器における暗号の利用も多く、移行には諸外国に比べてより長い期間が必要であると考えられます。従って本来は、より早い時期から準備を進めるべきなのですが、このまま民間における標準化やスケジュールのコンセンサスをとる動きが出ないまま進んだ場合、諸外国に比較して移行が著しく遅れることも危惧されます。そして、その結果としてもたらされるものは、単なる暗号の安全性の低下だけではありません。

相互運用性を考えなくて良い、閉じたシステムはともかく、そうでないシステムで移行が長期間にわたるということは、必然的に両方の標準を運用し続けるということになります。しかも、下位にあたる基準は日本国内でしか使えないとすれば、このダブルスタンダードを維持するコストは、国内の事業者およびユーザーが負担することになってしまいます。社会全体のコストを最小化するためにも、民間にお

けるプレーヤーの整理と情報共有、そしてアクションプランの策定が必要なのではないでしょうか。

5. 最後に： 「公開と標準化」によるセキュリティ

今回はEV SSLを例にして、運用基準と技術仕様の両方が世界的に標準化されることによって、SSLが新たなセキュリティの枠組みとして次の段階に進もうとしていることをお伝えしました。海外では、公開された標準ができることを新たなビジネス参入の機会として捉え、標準策定に積極的に関与しようとする動きが見受けられます。「公開と標準化」これはSSLに限らずセキュリティの様々な分野においても大きな流れであるかと思えます。

しかし残念ながら日本においては、標準が決まっ

た後でそれを「ローカライズ」することで手一杯で、一番重要な標準化の際の議論に直接参加していなかったり、あるいは、日本国内だけのための仕様策定に終始し、そこで標準化された成果を海外に送り出そうという動きが少ないように感じられます。また特にセキュリティの分野で「公開と標準化」の重要性があまり認識されていないと感じるのは筆者だけでしょうか。

2006年2月、政府は情報セキュリティ政策会議において「情報セキュリティ立国」の理念を掲げ、世界一安全な国として「ジャパンモデル」の確立を目指すとしました。暗号の研究において日本は世界有数の実力を持っているはずですが、その成果を社会が享受できるまでには、まだまだ道半ばと言わざるを得ません。今後の日本の取り組みが、将来他の国からお手本とされるような「ジャパンモデル」として実現されることをぜひ期待したいと思います。

参考

「CRYPTREC Report 2006 暗号技術監視委員会報告書」

<http://www.cryptrec.go.jp/report.html>

「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」

http://nisc.go.jp/active/general/pdf/crypto_pl.pdf

「次期情報セキュリティ基本計画に向けた第1次提言」説明資料

http://www.nisc.go.jp/conference/seisaku/strategy/dai10/pdf/10siryou_ref01.pdf

2008年上半期の個人情報漏えい 止まらない情報漏えいとやめられない Winny

株式会社ディアイティ
セキュリティ被害調査WGメンバー 山田 英史

本誌の読者をご存知と思われるが、JNSA セキュリティ被害調査WGでは年間の個人情報漏えいを集計分析した結果を報告書として毎年公開している。2002年度に個人情報漏えいの集計を開始してから、インシデント件数は個人情報保護法が完全施行された2005年をピークに2006年と2007年と若干の減少傾向にある。当WGの集計は、報道機関などにより公表された情報に基づくため、世の中の関心が薄れることで集計件数が減少するであろうことは予想していた。しかし、現実には思っていたほど大幅な減少は無く、2006年以降も一定の報道件数が保たれていることは想定外であった。個人情報漏えいも、他の不祥事と同じく組織にとって一般的なリスクとして認識されたのであろうということを、2007年度の報告書では述べている。

2007年のインシデント件数を超えるのは確実だろう。現時点で数字だけが一人歩きすると困るため具体的な数字は出せないが、2008年は漏えい人数(被害者)1名~数名の小規模なインシデントが占める割合が高いようだ。漏えい元の業種を見ると「公務(他に分類されないもの)」の比率が最も高く、この業種では漏えい人数が少数の場合でも公表する傾向が強いため、それが全体のインシデント件数を引き上げる要因になっていると思われる。

次に漏えい原因はどうだろうか。2007年は上位5位までの合計が全体の80%を占めていたが、2008年上半期は上位4位が全体の80%以上を占めている。また、2008年上半期は「誤操作」が大きな割合を占めているのだが、これはある特定の機関が大量に誤配送を発生させたことに影響された結果である。「管理ミス」は相変わらず上位に位置するが、これは例年通り金融機関が年度末の情報資産棚卸しの際に、保管しているはずの伝票等がなくなっていることに気がつくというケースだ。

2008年はインシデント件数が増加？

さて、2008年も残りわずかになった。年が明けると、当WGでは恒例となった前年の個人情報漏えいの集計と分析を始めるのだが、対象の件数が多いことから昨年からは半年毎に集計するようにしている。したがって、実はすでに2008年の1月から6月の上半期の集計結果が手元にある。

まだインシデントを時系列に並べただけで内容を精査していないため、個人情報以外の情報漏えいが含まれていたり、同じ事案をダブルカウントしているなどの誤差があることを前置きした上で、2008年上半期の集計結果を触りだけ紹介したい。

まずインシデント件数だが、2007年が通期で864件だったのに対し、おどろくべきことに2008年は上半期だけで700件を超えている。前述したように精査していないので最終的には件数が減ることになると思われるが、このままのペースで行くと通期では

表1:2007年と2008年の漏えい原因上位5位の比較(件数割合)

順位	2007年(通期)	2008年(上半期)
1位	紛失・置忘れ	誤操作
2位	管理ミス	管理ミス
3位	誤操作	盗難
4位	盗難	紛失・置忘れ
5位	ワーム・ウイルス	不正な情報持ち出し

繰り返しになるが現時点での集計は上半期までのものであり精査もしていないため、通期で集計・分析した結果は上記の結果と大きく離れている可能性もあるので、当WGの2008年度の報告書が公開されたら是非ともご確認いただきたい。

Winny は相変わらず

ところで、2008年上半期の集計で気になる点がひとつある。それは、Winny等ファイル交換ソフトでの漏えいが40件強と、全体の6%ほどを占めることだ。なお、その内Shareによるものが4件とLimeWireによるものが1件ある。

どうも数字だけ見ると少ないように感じるが、これだけ新聞沙汰になっているにもかかわらずまだ利用している人がいるということは理解に苦しむ。これらのソフトを使ったことがない人にとっては不思議でならないだろう。

では、なぜ利用がやめられないのか、簡単にいうとそれは趣味の世界だからだ。体に悪いことは分かっているけどタバコや深酒がやめられないのと同じで、頭で分かっているけど好きだからどうしようもないのだ。会社が社員に対し自宅でのWinnyの使用を禁止しても、実際どれだけの効果があるか疑問である。

やはり、大半の利用者は「自分は大丈夫」と思って(信じて)使い続けているはずだ。社員に対してWinny等による情報漏えいの危険性を説くときは、組織の問題として捉えるのではなく、漏えいさせた本人の個人の問題として認識させないと危機感を生

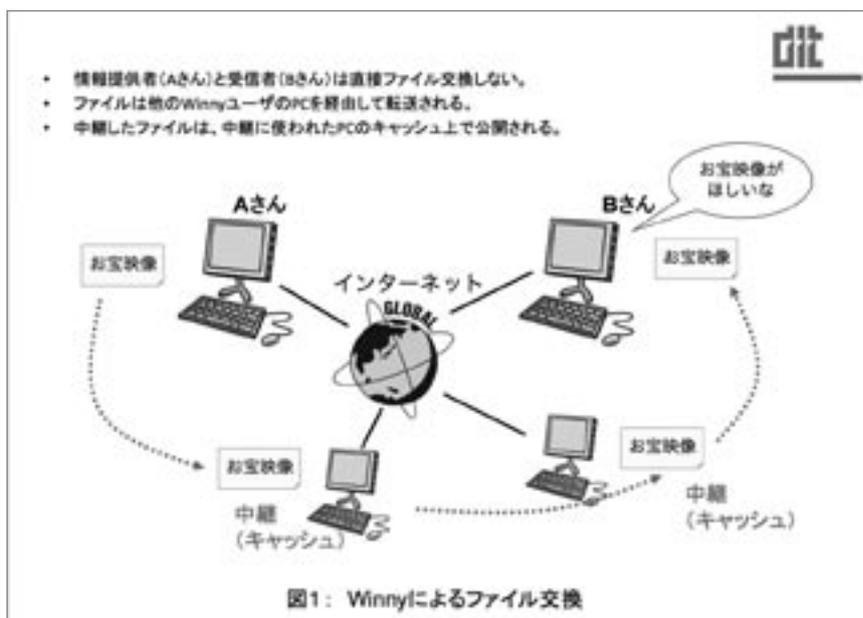
まれないのではないだろうか。

というわけで、ファイル交換ソフトの危険性について個人の問題として感じてもらうための助けになることを期待して、漏えい元の当事者がどのような顛末をむかえるのか、実際の現場の例を紹介してみたいと思う。

Winny が危険と言われる訳

いろいろな媒体でWinnyの仕組みは紹介されているので、ここではポイントだけ整理してみたい。Winnyはサーバを介さずPC間でファイル交換する機能を提供するソフトである。Winnyでは送信元PCと受信元PCは直接データを転送するのではなく、他のWinnyユーザのPCを幾つか経由してファイル交換する(図1)。その時、ファイル交換を希望したPCだけでなく中継したPCにも当該ファイルがキャッシュされ、以降公開される。複数のPCを中継することで、ファイルの提供者の匿名性を確保すると共に、キャッシュにより情報を広く拡散させることで検索・ダウンロードの効率を上げる効果がある。

ここで問題になるのは、中継したPC上において、持ち主の意思に関係なく様々なファイルを公開して



しまうことだ。キャッシュで公開しているファイルには違法に収集した著作物も含まれる。したがって、Winnyを使うということは、暴露ウイルス感染による情報漏えいと、著作権侵害という2つのリスクを負うこと意味する。ただし、WinnyやShareユーザの大半は違法なファイルを自覚的に交換しているはずなので、ここでは情報漏えいの危険性にフォーカスする。

Winny が危険と言われる訳

WinnyとShareで情報漏えいが多いのは、これらソフトの脆弱性を悪用する暴露ウイルスが数多く出回っているからだ。ではなぜその2つのソフトにウイルスが多いのか。両ソフトの技術的特性に理由がある。WinnyとShareは共に、どのファイルを公開するか等の設定情報をテキストファイルで保持している。設定をテキストで持っているがためにウイルスが利用し易く、そのために両ソフトを狙った暴露ウイルスが多く作られているのだ。特にWinnyは脆弱性が改善されることが期待できないため、より危険だといえるだろう。

さて、暴露ウイルスに感染したら、どのような情

報が漏れるのだろうか。図2は暴露ウイルス体験ツールで擬似的に漏えいさせた情報の例(一部)である。文書ファイルだけでなく画像・映像・メール・IEお気に入り等あらゆるものが漏えいする。それらは、ZIP圧縮ファイルとして一括して漏えいするため(ウイルスの種類によってZIP以外もある)、ほとんどの場合、ファイル名やそこに含まれる住所録やメールや写真画像などから漏えい元の個人が特定できる。

情報漏えいする人のプロフィール

Winny等で被害の大きな情報漏えいを起こすのはどのような人物なのだろう。幾つかの事例から以下のような人物像が浮かび上がる。

- ・男性
- ・30代半ば～50代
- ・既婚者
- ・几帳面でまじめ
- ・コンピュータにいくらか精通している

意外に30代半ば～50代の中堅社員や課長クラスの人が多い。その年代の人たちは、4～5年前まで会社の資料を持ち帰って家で仕事をするのが普通



だった。そのため、今でも家に会社の資料が保管されている可能性が高い。当時から使っている自宅のPCにWinnyをインストールしたところ、暴露ウイルスに感染し、消し忘れたあるいは存在を忘れていた会社の資料が流出するというパターンが多いようだ。現実最近流出したファイルでも作成は4～5年前という情報が良く見つかる。

また、ある程度コンピュータに詳しく、自分は危険性を認識した上で上手く使っているという自信もっている人も多い。実際に、ある会社の情報システム管理責任者が漏えいを起こしたケースもあった。

多くのWinnyの利用者は、好きな分野のファイルは徹底的にコレクションし、収集したファイルを分類整理するような几帳面さが見られる。仕事にも普段まじめに取り組んでいる人が多い。

ほとんどの人は、故意ではなく意図せず漏えいしてしまっているの、ある意味被害者でもある。

情報漏えいの顛末

一度漏えいした情報は形を変えながらコピーされ続ける。Winnyで流出した情報は、すぐさまShareにコピーされShare経由で拡散し、2ちゃんねる等の掲示板でも公表される。多くの場合、漏えい元組織(実際にはその組織に所属する個人が漏えい元だが)が自ら検知することは無く、匿名の警告FAXが送られてきたり、掲示板等を見て発見した親会社や取引先から通知されて初めて漏えいに気付くことになる。

この時点で、漏えい情報が保全されていれば、漏えい元組織は自らの分析で漏えい元となった人物を特定できていることが多い。漏えい情報の中身が自己の組織に関わるものだけであれば、内々に対処して終わるのだが、漏えい情報に親会社や取引先の内部情報が含まれている場合は、それら関係者から正式な報告を求められることになる。報告は客観的な内容を求められるので、インシデントレスポンスやフォレンジックを行なうベンダーに調査を依頼することが多い。調査依頼を受けたベンダーは、WinnyやShareのネットワークを監視し、本当に漏えいし

ているのかを確認し、漏えいしている場合はファイルを保全し、何人くらいがダウンロードして、何人くらいがキャッシュで公開しているのかといった漏えい規模を分析する。

さらに、実際に漏えいしている場合は、流出者を特定する証拠を用意した上で、次のような手続きで流出元のPCを差し押さえる。(あくまでも一例)

- (1) 就業時間中に直属の上司含め、多数の関係者で流出者を取り囲む。
- (2) 流出者には、自宅で使用しているPCの提出をお願いする。この時、自宅に電話はさせず会社のPCも使わせないようにする。
- (3) 車を使い、流出者の自宅へ移動してPCの回収に向かう。
- (4) できれば上司だけでも一緒に部屋まで入れてもらい、PCや外付けディスクを確認しながら回収する。部屋に入れてもらえない場合は、3分以内というように時間を制限する。
猶予を与えるとディスクを壊したり、別のPCやディスクを代わりに提出する可能性が高くなる。
- (5) 流出者本人もいっしょに、回収したPCや外付けディスクとともに引き揚げる。
- (6) Explorer等を操作しただけでも証拠(記録)が変化するため、引き揚げたPCは立ち上げず、専用の装置で内蔵ディスクの複製を取り、解析は複製に対して行なう。複製をとった後にPCは所有者へ返す。

残念ながら、この時、ほとんどの情報流出者は全てを話さず幾つかの事実を隠す。全てが露呈すると仕事も家庭も失うことが想像できるからだ。別のPCやディスクを提出して時間を稼ぎ、その間に本当のディスクをフォーマットしたり物理的な破壊を試みたりする。しかし、引き揚げたPCを解析すると隠している物が分かるので、いずれ本物を提出することになる。初期の調査や保全で、会社は相当な出費をしているのだが、破壊されたディスクの復旧などを行なうとさらに数百万円の出費になる。

情報漏えいにより関係者が大きな経済的損失や精神的苦痛を被り係争まで発展する場合を除き、会社

は流出者を必要以上に罰することは無い。しかし、証拠隠滅を図り余計な出費を会社にさせた場合はいくらか厳しい処分が下されることになるだろう。

また、Winny等ファイル交換ソフトを使っている人は、ほとんどの場合アダルト情報を収集しており、解析の過程でその人の趣味嗜好だけではなく性癖まで知ってしまうことになる。知られた方も知ってしまった方も、相手に対する接し方はそれまでの通りとはいなくなる。ほとんどの場合、故意ではない情報漏えいでクビにするほどの厳罰を会社が下すことはないが、流出者本人が会社にいづらくなることが多いようだ。

さらに、家庭でも「お父さんがWinnyを使っていた」という事実により家族の接し方が変わってしまい、発覚以後互いに気まずくなることもあると聞く。

状況によりインパクトは異なると思うが、情報を流出させた時点で会社での地位も家庭での立場も失い未来はなくなるということをWinnyユーザは覚悟しておくべきだろう。

今一度チェックを

ファイル交換ソフトによる情報漏えいの対策はいくつも考えられるが、まずは自宅のPCに会社の情報を保管しないことだろう。先にも述べたが、故意にデータを保管していることは少なく、保管したこと自体忘れていたり、削除したつもりが予想しなかったフォルダに残っていたりすることで被害に結びつく。

以前削除したという方も、今一度自宅のPCの中をチェックしていただきたい。

情報漏えいに責任を感じて自殺した人もいる。自分だけは大丈夫という根拠の無い自信は持たず、すべてを失い未来がなくなる前に、Winnyを使うという問題の考えをまじめに考えていただきたい。

チェックリスト(データだけでなく文書も含む)

<input type="checkbox"/>	自宅のPCのあらゆるフォルダをチェックして会社の業務情報が無いことを確認した
<input type="checkbox"/>	メール(添付ファイルを含む)にも業務情報はなかった
<input type="checkbox"/>	外付けディスクやUSBメモリにも業務情報はなかった
<input type="checkbox"/>	業務情報が家の中で放置されていなかった
<input type="checkbox"/>	引出や本棚に昔の紙資料がなかった
<input type="checkbox"/>	上記は記憶ではなく、実際に確認した
<input type="checkbox"/>	インターネットの脅威と被害について家族とも話し合った
<input type="checkbox"/>	情報の取り扱いについて、家族にも注意するように伝えた

勉強会企画検討 WG

WG リーダー

株式会社シマンテック 嘉津 義明

■ U40 部会とは？

若年層の積極的な運営参加による団体の若返り、会員間の交流の強化、若年層の活動活性化のための情報流通強化、セキュリティ業界・社会への貢献・関与などを目的として2007年に設立されました。

■ WG の目的・概要

U40 勉強会検討 WG は、U40 部会の下部組織で、セキュリティや IT 業界に関するテーマを中心に若手に有意義だと思われる幅広いテーマで、業界の最新知識取得や講師の方との交流・人脈作りなどを目的として、1～2ヶ月に1度 U40 向けの勉強会を開催しています。本 WG では、勉強会のアイデア出し・募集、講師の方への依頼・交渉・日程調整、会場の手配、議事録の作成及び勉強会後の懇親会企画・会場手配などを行っています。

■ 勉強会の様子

勉強会は随時ディスカッションを交え、原則2時間で行われます。毎回ざっくりばらんな質問が投げられ、和やかな雰囲気が進められています。



7/4 勉強会風景



11/19 勉強会風景

過去に行われた勉強会からいくつかをピックアップしますと、

- 2007/10/19「第一回著作権講座」
社団法人コンピュータソフトウェア著作権協会
中川文憲氏、太田輝仁氏
著作権とは何か？著作物とは？など著作権の基礎を学ぶ。会社で作ったプログラムの著作権についてなど、様々な質問が出され、あまりに盛り上がったために当初1回で終了する予定が、計3回行われることに。また、この勉強会は好評だったため JNSA 全体向けとしても別途行われました。
- 2008/7/4「インド IT 企業と日本」
イノソフトジャパン 社長
Andrew Larson 氏
R システムズ 日本支社長
Belinraj Matthias 氏
何故日本はインド IT 企業を使いたがらないのか、そこにある誤解と真実。
- 2008/8/29
「Web2.0 セキュリティの傾向と対策 2008」
セキュアスカイテクノロジー 執行役員
福森大喜氏
技術的に高度な内容で、Web2.0 のセキュリティの脆弱さを具体的な例を交えてご説明いただきました。

● 2008/10/17

「セキュリティ業界の若手におくるエール」

植松電機 専務取締役

植松努氏

セキュリティ・ITとはあまり関わりのない、ロケットや人工衛星の開発も行っている植松氏の熱いお話を聴講し、参加者一同、心が熱くさせられました。「思うは招く 夢があればなんでもできる」をテーマに、実際に不可能を可能にしてきた方ならではの説得力のあるお話でした。

■ 今後の予定

今後も1、2ヶ月に一度勉強会を開催して参ります。U40メンバーを優先に参加者を募集しますが、席に余裕がある場合は部会メンバー以外にも聴講枠を設けご案内して参りたいと考えております。

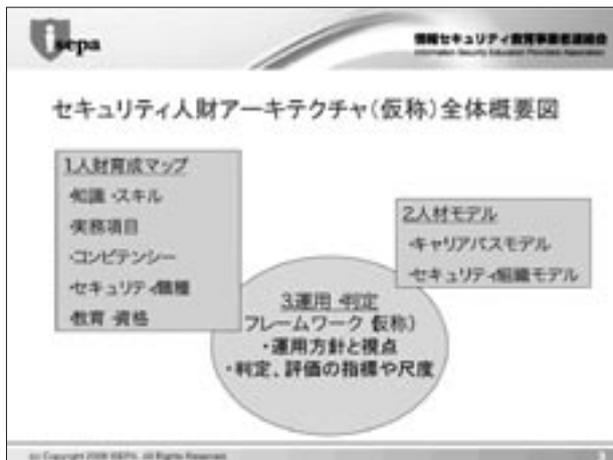
U40 部会勉強会 開催一覧

1	2007.7.12	VMWare 勉強会
2	2007.9.28	セカンドライフ勉強会
3	2007.10.19	第1回著作権講座
4	2007.11.30	カスペルスキーラボスジャパン勉強会
5	2007.12.14	第2回著作権講座
6	2008.2.20	DBSC 勉強会
7	2008.3.10	第3回著作権講座
8	2008.4.25	役に立たないHTML/JavaScript Hacks 4 連発
9	2008.5.21	IT 保険その1 Information Technology Business Guard
10	2008.6.25	IT 保険その2
11	2008.7.4	インドIT企業と日本
12	2008.8.29	Web2.0 セキュリティの傾向と対策 2008
13	2008.10.17	セキュリティ業界の若手におくるエール
14	2008.10.30	GPCode.ak ~ランサムウェアの脅威~
15	2008.11.19	暗号（特にMD5やSHA 1などのハッシュ関数）の危殆化について

情報セキュリティ教育事業者連絡会 (ISEPA) スキル WG

WG リーダー
(ISC)2 衣川 俊章

昨年11月に発足しましたISEPAですが、数回にわたるカンファレンスや、3つのワーキンググループ(WG)での活動を中心に行ってきました。今回は、3つあるWGの中の1つであるスキルWGのここまでの活動、及び12月18日のNSFで発表しました「情報セキュリティ人財アーキテクチャ(仮称)」についてご紹介したいと思います。



■ 目指す成果物

ISEPA 発足時に、情報セキュリティ人材育成の現状と問題点を指摘してきました。

これらの解決への指針としての「情報セキュリティ人財アーキテクチャ(仮称)」を作成する事を当WGの目標としています。「人財」の「財」には、人を「ひと、物、金」という有形資産としてだけではなく、無形資産としての財であるという認識をしてもらいたいという思い、「アーキテクチャ」には、育成という視点だけではなく、知識やスキルの活用・評価という観点まで含めた人財ライフサイクルを包含しているという意味が込められています。

この中では、現存する教育・資格と情報セキュリティ業務、職種、スキルといった物とを紐付けしていくだけではなく、実際の組織における組織モデルや個人のキャリアマップモデルを作成し、またこれらの使用手法や評価のフレームワークまでを提示する事で、人材育成・活用する側、される側の双方にとって使い勝手の良い ToBe モデルと成りえる物を提供する事を目指しました。

特に使用・運用方法や評価についてのフレームワークについては、今までの様々なスキルマップ的な物の問題点として、それらをどう使ったら良いか分からない、自分のスキルや知識レベルをどう評価すればいいのか分からないという問題点に対する解として初の試みとなっています。

■ 作成過程

作成に当たっては、「現存する教育・資格と情報セキュリティ業務、職種、スキルといった物とを紐付けしていく」を「人財育成マップ」、「実際の組織における組織モデルや個人のキャリアマップモデル」を「人材モデル」、「これらの使用手法や評価のフレームワークまでを提示」を「運用・評価フレームワーク」と名づけ、それぞれ作成する事にしました。

「人財育成マップ」の各項目については、WGメン

バーの思いだけで判断するのではなく、既に存在している信頼でき得る、指標となりえる資料からのリストアップを試みました。例えば、実務項目については、政府から種々の情報セキュリティに関する報告書6種類から実務・業務として当てはまるであろう文言をピックアップしました。スキル・知識についてはJNSAで作成されたSecBokをベースに項目選定をしています。こうする事によって、成果物が中立性、信頼性を保ち、また日本国として向うべき方向性と一致した物を作成する事が出来ると考えたからです。

「人材モデル」については、現存するであろう情報セキュリティにおけるキャリアパスを上の人財育成マップで取り上げた職種をベースに、具体的に事例を示すことにしました。組織モデルについても、実在する組織体において、情報セキュリティ業務遂行に必要な人員を「職種」「業務項目」で特定し、事例として示そうとしました。これによって、「人財育成マップ」では2次元レベルであったマップが、現状に即した次元にまで広げて理解をしてもらえるようになるのではと考えました。

そして最後に「運用・評価フレームワーク」ですが、人材モデルで示したキャリアパスや組織モデルを目指して人材育成、開発をしていく中で、これらをどう活用し、また実際のスキル・知識レベルの評価に使用していけば良いのかの指標を示す事を考えました。

■ 第1版の内容

こうして作成した「情報セキュリティ人財アーキテクチャ」ですが、今回発表の物は第1版という位置づけになっております。その内容ですが、

1. 「人財育成マップ」－職種は現存する職種名から研究、教育に関わる職種を除き、34職種に絞り込みました。業務項目は、総務省、経産省、NISCが出した各種報告書から抽出した業務項目を130項目ほどリストアップしました。知識・スキルについては、JNSAのSecBokの中項目を

ベースにしています。コンピテンシーは、「国家公務員採用1種試験 着眼点別評価段階と行動例」からピックアップしました。教育・資格は市場に現存する物は全て網羅しております。

2. 「人材モデル」－組織モデルについては、「企業内CSIRT」、「情報セキュリティシステム開発プロジェクト」、「組織内情報セキュリティ機能」という3モデルについて策定してみました。キャリアパスについては、職種としてあげました全職種を関連付けてパスを策定してみました。
3. 「運用・評価フレームワーク」－人材モデルを活用してもらう為の手法、指標について提示しております。これについては、更に今後の実証実験を経て、より具体的、実態に沿った内容に改定していく予定です。

■ 今後について

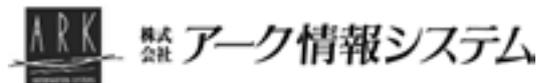
上でも申し上げましたように、今回発表させていただいたのは、あくまでも第1版となっております。今後、個人に当てはめたキャリアパス、組織に当てはめた組織モデルの事例をベースに、実証実験を行っていきます。個人に当てはめたキャリアパスについては、実は既に教育部会と共同で「スター育成プロジェクト」が始動しておりますが、これらの実証実験と通して、第1版の中身の検証を行っていきたくております。同時に、WGでは継続的に、モデル事例の追加作成を行っていき、より多くの方々、組織に方々にお使いいただける形物にしていく予定です。

いずれにしても、今回の発表で終わりではなく、ここから更に進化を続けていき、情報セキュリティの人材不足に少しでも貢献できればと思っております。皆さんからの様々なご意見、ご要望なども聞き入れていながら、活動を進めて行きたいと考えておりますので、今後ともよろしく願いいたします。

会員企業ご紹介 24

株式会社アーク情報システム

<http://www.ark-info-sys.co.jp>



アーク情報システムは、エンジニアリング系のソフト開発を得意としております。同時に、自社技術をベースにした自社パッケージの企画・開発・販売に力を入れております。仮想化ユーティリティ「CD革命シリーズ」、OS全体をバックアップする「HD革命シリーズ」等、三次元動解析ソフト「TDAP・FDAPシリーズ」等が良く知られています。その他、海外製品で優秀なパッケージがあれば、輸入・販売・サポートを行っております。現在、セキュリティ製品に注力し、自社製品の開発を含め特徴ある品揃えに力を入れてまいります。

日本の企業のためのスパム対策

増え続けるスパムメール。ネットワークインフラのリソースを浪費し、そのリスクは図りしれません。数ある対策製品の中でも、日本のスパム事情、企業のメールセキュリティポリシーにベストマッチする製品が、インターネット先進国韓国でシェアトップを誇るSpamSniper(スパムスナイパー)です。

2バイト圏から生まれたフィルタリング技術は、日本語環境において他社をリードする高い遮断性能をもち、多段階のフィルタ設定により、企業のメールポリシーにも柔軟に対応します。

- ネットワーク環境を変更しないBridge方式の設置
 - 送信メールにもフィルタリング可能
 - アンチウイルスも標準装備
 - ASPサービスをサポートする多彩な設定
- など、SpamSniperは豊富な機能を提供します。

使いやすさとパフォーマンス

最大の特徴は、管理者を含めた全てのユーザに、これらの豊富な機能を使いやすく提供します。複雑・難解な設定や、高度な技術も必要なく、安心かつ安全なメール環境を実現します。

アプライアンス製品のラインアップは4モデル。ユーザ数に依存しない価格体系は、中小規模の企業からASPサービスなどの大規模運用まで、高いコストパフォーマンスを発揮します。

高性能と豊富な機能を、コンパクトにまとめたエコなスパム対策。SpamSniperの実力を、実際の評価にてお試しください。



ファイル転送に大革命

大容量ファイルの受け渡し。

メール添付、第三者管理のASPサービス、FTPサーバ、メディアの送付などいずれの方法も、情報漏洩やコスト面での不安、不便が付きまといまいます。

GIGAPOD OFFICEHARDは、大容量データを気軽に送信でき、多くの需要に応えるファイル転送サーバーです。

添付ファイルからの情報漏洩をブロック

メール誤送信における情報漏洩防止にもつながります。パスワードや期間の設定など、マニュアル要らずのブラウザ操作で可能です。

SpamSniperで添付ファイルを禁止、全ての添付ファイルをGIGAPODでやり取りするポリシーを導入すれば、内部からのメールによる情報漏洩対策も完璧と言えるでしょう。



総合メールセキュリティソリューション

企業のメール環境に対する、不正攻撃やウイルス、スパムといった外部からの脅威に対する防御。

メールによる内部からの情報漏洩対策。

アーク情報システムは、メール環境の効果的なセキュリティソリューション、エコロジー対策を提案します。

お問い合わせ先

株式会社アーク情報システム

〒102-0076 東京都千代田区五番町 4-2 東プレビル

TEL: 03-3234-9232 FAX: 03-3234-9403

E-Mail: SpamSniper@ark-info-sys.co.jp

officehard@ark-info-sys.co.jp

社名に込める思いについて

「情報経済」とは：

- ・情報は、経営の中に真に生かされているか？
- ・情報は経営に対して、経済プロセスに対して、付加価値をもたらしているか？
- ・検証されないこの問いに向けて、跡付け、定量化し、言語化する試み、アンカリングへの取り組みを模索する。

「情報セキュリティ」の真の実現を目指して：

- ・情報の経済価値が同定されないところから、情報セキュリティの価値定義が進まない。
- ・情報セキュリティの経営価値が示されないために、情報セキュリティ対策が必要十分なレベルまで講じられない。
- ・情報のリスクを管理しきれないままの経営が、企業の存続を危うくすることはないか？
- ・情報セキュリティを、情報の経済的価値を明らかにするところからアプローチして実現し、定着させることを試みる。

情報経済研究所がご提供できるお役立ちについて

情報セキュリティ対策を
診断します
一緒に考えます
実装を手伝います
監査します

組織の対策を考えます
基準規律の整備実態はどうか
基準規律の遵守風土はあるか
経営層の理解は確立しているか
→経営課題整理、組織機能点検

情報セキュリティ市場の
調査分析をします
構造解析をします
動向を読みます
変化を見極めます

人の対策を考えます
業務実態に含まれるリスク
組織風土に含まれるリスク
士気・モラルに潜むリスク
→教育、業務改善、モラルアップ

技術実装をサポートします
ツールのご紹介・選定
実装事業者のご紹介
アーキテクチャ診断

代表取締役 **勝見 勉**

公認情報システム監査人(CISA)
ISMS審査員補
情報セキュリティ監査アソシエイト
情報セキュリティアドミニストレータ

〒227-0043
横浜市青葉区藤が丘2-1-3-826
Tel/Fax: 045-972-6548 携帯: 090-8753-4306
e-mail: info-economy@xvg.biglobe.ne.jp

株式会社ブロードバンドタワー

<http://www.bbttower.co.jp>



ブロードバンドタワーは、高度な運用技術と信頼性の高いハウジングサービス、インターネット接続サービス、およびホスティングサービスなどのiDCサービスを提供しています。アクセスの良い都心にインターネットデータセンターをはじめとしたネットワークインフラストラクチャー資産を有し、複数のインターネット関連企業から高い信頼を得ています。また企業向けストレージを展開するアイシロン・システムズの1次販売代理店として幅広くストレージソリューションを提供しております。

コロケーションサービス

ブロードバンドタワーのデータセンターでは、回線供給業者に制約を設けておりません。独立系運用会社としてのメリットを活かし、様々な回線事業者が提供する多種多様なサービスからお客様に最適なサービスを選択、引き込みが可能となります。ファシリティは大規模地震に備えた耐震構造・冗長構成による安定した電源供給、床吹き上げ方式空調管理による一定した温度・湿度調整管理が網羅されている施設で、高品質なファシリティを提供しています。また、非常用自家発電装置、不活性ガス消火システムによる防火設備を設置し、不測の事態への対策も備えております。



24時間365日の運用監視体制、ITVカメラによるモニタリングなど情報セキュリティの基本方針のもと、徹底したセキュリティ体制で信頼性の高いサービスを提供します。

ホスティングサービス

- Collective Hosting (コレクティブホスティング) サービスは、IBM社メインフレーム System z上のz/VM(仮想マシン)の仮想化技術にて仮想Linuxサーバを提供し、複数のお客様(システム)でご利用いただくホスティングサービスです。System z は金融系等のミッションクリティカルなシステムでも多く採用されている堅牢性の高いハードウェアであるため、高信頼、高可用なサービスを提供します。
- FlexHosting (フレックスホスティング) は新規ビジネスの立ち上げ、製品のキャンペーン時など、ビジネスの状況に応じて柔軟にシステムをご利用いただけるユーティリティ型サービスです。FlexHostingでは、お客様のシステムのご利用状況を調査し、ベストなソリューションをご提案いたします。システムの設計から運用監視までITシステムのライフサイクルをトータルにサポートいたします。

プロダクトサービス

ブロードバンドタワーはアイシロンVADパートナー(一次販売代理店)として、Isilon IQ クラスタストレージの各製品をご案内しております。Isilon IQクラスタストレージは、大容量のストレージ構成に最適で、従来のRAID構成によるNAS/SANシステムが有していた拡張性、管理の複雑さ、可用性などの問題を一挙に解決しており、画期的なパフォーマンスとともに高い信頼性を得ています。



お問い合わせ先

株式会社ブロードバンドタワー

〒107-0052 東京都港区赤坂4-2-6 住友不動産新赤坂ビル7階

TEL: 03-5573-8172 FAX: 03-5573-8180 Mail: pr-ir@bbttower.co.jp

JNSA 会員企業のサービス・製品・イベント情報

■製品情報■

○スパム対策のパイオニア『IronPort Cシリーズ』

ジェイズ・コミュニケーションが取り扱っているスパム対策アプライアンス『IronPort Cシリーズ』は IPレピュテーション、Domain Key、VOF (Virus Outbreak Filters: ウィルス拡散防止フィルター)、コンテンツフィルターなど、最新のテクノロジーを駆使し、企業の電子メールシステムを保護。不要なメールは事前にブロックします！

【製品情報詳細】

<http://jscom.jp/products/ironport>

◆お問い合わせ先◆

ジェイズ・コミュニケーション株式会社
担当：東日本営業部 吉岡
TEL: 03-6222-5858 FAX: 03-6222-5855
E-mail: yoshioka@jscom.co.jp

○統合ID管理システム『PMaid IDMaster』

統合ID管理システム『PMaid IDMaster』は、日本の組織風土に徹底的にこだわった新しいシステムです。ゴーストIDや過剰な権限の付与防止などの内部統制対策は勿論のこと、セキュリティ強化や社内に乱立する各種システムのID管理運用の効率向上に絶大な効果を発揮します。また、システム連携カスタマイズ機能を内蔵し、人事システムや業務システムとの連携を強力にサポートします。

【製品情報詳細】

<http://jp.fujitsu.com/group/kcn/services/products/software/product-pmaid-idm.html>

◆お問い合わせ先◆

富士通関西中部ネットテック株式会社
着信課金サービス 0120-008870 (平日 9:00~17:00)
web: <http://jp.fujitsu.com/kcn/>
e-mail: kcn-product@cs.jp.fujitsu.com
TEL: 06-6949-3702 FAX: 06-6949-3530

○リアルタイム・ネットワーク監視システム

リアルタイム・ネットワーク監視システムは、複数の1Gbpsで流れる高速ネットワークの packets を100%取り込み、リアルタイム解析/表示できるシステムです。Non-samplingフロー情報から網全体のトラフィック情報を秒単位でグラフ表示します。また蓄積データからあらゆるパケット情報を高速検索できます。これにより障害対応時間を大幅短縮、サービス運用効率上がりビジネスのROIを向上させることができます。

【製品情報詳細】

<http://www.u10networks.com/solution/realtime-system>

◆お問い合わせ先◆

ユーテン・ネットワークス株式会社
e-mail: sales@u10networks.com
TEL: 03-3723-5506

■サービス情報■

○Webアクセス『地域”見える化”サービス』

オンラインのビジネス展開では安全性確保が最重要課題。匿名性が高いインターネットでは、ユーザーの位置情報把握が不正防止に役立つ事例が多々あります。IPアドレスから位置や接続環境を判別するIP Geolocationデータは、オンライン取引の安全性向上に効果的。『地域”見える化”サービス』は、IP GeolocationによってWebサイトの傾向や地域性を分析するサービス。不正の徴候検出や現状把握に。

【サービス情報詳細】

<http://www.arearesearch.co.jp/>

◆お問い合わせ先◆

サイバーエリアリサーチ株式会社
e-mail: info@arearesearch.co.jp
TEL: 03-3243-1070(東京支社) 055-991-5544(本社)

PKI Day 2008 レポート

富士ゼロックス株式会社 横田 智文

JNSA PKI相互運用技術WG主催セミナー
【PKI-Day 2008-

<PKIの標準から実装まで最新動向>】

■日時：2008年7月3日(木)10時~18時半

■場所：東京ウィメンズプラザホール

■主催：JNSA PKI相互運用技術WG

PKI Day 2008は、京都大学の岡部氏の基調講演「全国大学電子認証基盤 (UPKI) とその先にあるもの」から始まりました。氏の講演では、国立7大学と国立情報学研究所等が共同で構築しているUPKIの現状として、UPKIが用途に応じた3つのPKI (PKI オープンドメインPKI、キャンパスPKI、グリッドPKI) から構成されていることやそれぞれのPKIの役割、UPKIを使ったシングルサインオン等の実証実験、キャンパスPKI間の相互運用性確保、CP/CPSのテンプレート化などを含むキャンパスPKI導入促進のためのUPKI共通仕様などが紹介されました。また講演の最後では、UPKIの先にあるものとして、もっと誰でも簡単にPKIを利用できるようにしていきたいという方向性が示されました。

続いての講演は、富士ゼロックスの稲田氏の「標準化の一側面 - IETFにおけるPKIの状況」でした。講演では、IETFのPKIX-WGで議論されている主要な話題と現状が紹介され、PKIX-WGの活動報告として、RFC 3280の後継であるRFC 5280が公開されたことや暗号アルゴリズムの移行 (世代交代) について議論がされていることが紹介される一方、暗号アルゴリズムの移行に考慮されていないプロトコルも存在し、これらのプロトコルに関してはさらに多くの議論が必要になると説明されていました。

午前最後の講演は、セコム株式会社IS研究所の島岡氏の「日本発のPKI国際標準を目指して」でした。講演では、氏が標準化を目指すきっかけとなったJNSAのChallenge PKIという活動や標準化活動から学んだ標準化活動の難しさといったことが紹介さ

れました。標準化文章というものは、バックグラウンドが違う人にも正確にその内容を理解してもらう必要があるため、非常に緻密な論理構造、内容が求められるということが、英語以上に苦勞したと説明されていました。また氏のRFCである「マルチドメインPKIの相互運用性に関するメモ」は、RFC 5217として近日中に公開されることが紹介されました (2008/07/04公開)。

午後最初の講演は、JPNICの木村氏の「電子認証プラクティスフォーラム」でした。講演では、電子認証技術を使うためには、技術だけではなく運用やノウハウも重要であるが、今のPKIはこの部分が足りていないため、適切な普及が図りにくい状況であると説明されていました。このノウハウを電子認証技術に携わる人々で共有できるように、電子認証プラクティスフォーラムでは、電子認証に関わるノウハウをBCPとして文書化する活動を行っていると紹介されました。また本活動においてBCP化を目指しているいくつかのドキュメントも紹介されていました。

続いての講演は、日本電気株式会社の木村氏の「電子署名JIS制定の背景と今後の展望」でした。講演では、2008年3月20日に制定された電子署名に関する初のJIS規格である「JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル」および「JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル」を制定するまでの経緯と電子署名文書の安全性を長期間保証するための長期署名技術



について紹介されました。またこの長期署名技術を使ったソフトウェアは、相互に長期署名を検証できなければならないため、ETSI(欧州電気通信標準化機構)と共同でソフトウェアの相互接続テストを行っている」と説明されていました。

続いての講演は、セコム株式会社IS研究所の松本氏の「PKI対応IDカードの相互運用とHPKI対応ICカードガイドライン」でした。講演では、PKI対応IDカードの相互運用の難しさと相互運用を行うために策定したICカードガイドラインが紹介されました。ICカードは安全性の確保のため多くの仕様が非公開となっているが、ICカードを広く利用(相互運用)していくためには仕様を公開する必要があり、この非公開部分と公開部分のバランスが相互運用を行っていく上で難しいところであると説明されました。そして相互運用を行うためには「特定のベンダー等に依存しないデータモデル」、「特定のベンダー等に依存しないカードエッジI/F」が必要であり、JAHIS(保健医療福祉情報システム工業会)が策定した「HPKI対応ICカードガイドライン」では、こうした仕様をカバーしていることが説明されました。

続いての講演は、有限会社ロボックの伊藤氏の「オープンなPKI対応ICカードを扱うオープンソースソフトウェアの紹介」でした。講演では、公開されている標準仕様に準拠しているICカードを使い、ICカードを利用するために使用するソフトウェアとそのICカードをPKIアプリケーションから利用できるようにするための手順が紹介されました。講演タイトルにもある通り紹介されたソフトウェアはオープンソース、つまり無料で利用できるものであり、標準仕様に準拠しているICカードを購入するだけで、ICカードを利用することができる」と説明されました。

続いての講演は、マイクロソフト株式会社の渡辺氏の「Windows Server 2008のPKI機能」でした。講演では、マイクロソフトのPKIに対する考え方と

Windows Server 2008のPKI機能について紹介されました。マイクロソフトのPKIに対する考え方は、ただ動くことだけを狙っており、囲い込み等は考えていない。そしてよく誤解されているが、マイクロソフトのPKIはマイクロソフト専用ではなく標準と同じものなので、安心して使って欲しいと説明されていました。またWindows Server 2008のPKIの機能については、Windows Vistaと同様にNSAのSuite-Bのアルゴリズムが実装済みであり、それらの暗号を使った証明書を発行することができること、証明書検証機能としてOCSPに対応したことが紹介されました。

最後はセコムIS研究所の松本氏をモデレーターとし、IPAセキュリティセンターの山岸氏、松下電工株式会社の福田氏、日本クロストラスト株式会社の秋山氏、富士ゼロックスの稲田氏により「暗号アルゴリズム移行問題」についてのパネルディスカッションがありました。パネラーは暗号研究者、製品を作る人、証明書を発行する人、標準化に携わる人とそれぞれ全く立場が違うため非常に興味深いパネルディスカッションでした。パネラーの共通認識として、近年騒がれているRSA1024bitやSHA-1はアルゴリズムの脆弱化ではなく、世代交代の時期に来たということである。しかし世代交代と言うと強制力が弱く、脆弱と言うと過敏に反応されてしまうため、暗号アルゴリズムの移行に関してその進め方が難しいということが説明されていました。

今年のPKI Dayは、PKIが広く使われて来ているという印象を強く感じることでできたセミナーでした。JPNICの木村氏の電子認証プラクティスフォーラム、セコムIS研究所の松本氏のICカードの相互運用、そして最後のパネルディスカッションなどは、PKIが使われているからこそ問題になる話題であり、このPKI Dayのような有益なセミナーによって、PKIに携わる多くの人たちの共通認識となり、これらの問題が解決に向かうことを期待するばかりです。

中小企業情報セキュリティ対策支援セミナー開催結果

西日本支部長 井上 陽一

日 時	2008年11月26日(水) 13時～17時50分(開場12時30分)
場 所	大阪国際会議場 10階 1008号室 (大阪市北区中之島5-3-51)
主 催	NPO 日本ネットワークセキュリティ協会 西日本支部
共 催	NPO 日本システムインテグレーションパートナーズアソシエーション (JASIPA) 関西支部
後 援 (申請中)	近畿経済産業局、大阪商工会議所、社団法人 関西経済連合会、財団法人 関西情報・産業活性化センター、社団法人 組込みシステム技術協会近畿支部

年の瀬も近づき慌ただしさが漂う多忙な時期のため、セミナーへの参加人数が気になりましたが、申込者の留保率が高かった事とJASIPAメンバーの参加で会場はほぼ満杯の状況であり、13時から18時までの時間を熱心に静聴いただいたと思います。今回はJNSA西日本支部としては第11回目のセミナーでした。これまでの単独開催から、JASIPAとの共催という、ある意味で節目に当たる意義あるセミナーであったと思います。

システムインテグレータ等に大きく依存している中小企業には、情報セキュリティチェックシートの開発はJNSAが行い、JASIPAがチェックシートを顧客に適合する形にアレンジを行う(特に、技術的対策部分について、サポートする企業の特性を捉え、チェックシートで求める対策の具体的な実施策を提案・紹介願ひ、チェックシートと具体的実施策を紐付けていただく)事が望ましいとの確信が得られたことで、今後も、関西でがんばる同種の団体とのジョイントセミナーをやらねばと感じさせてくれた今回のセミナー開催でした。

以下に、各テーマの講演者が主張された記憶にとどめたい内容を簡記します。

1. 【基調講演】

中小企業の情報セキュリティ対策に活用するツール類

IPAセキュリティセンター普及グループ・グループリーダの石井氏よりご講演いただきました。

説明資料は70ページに及ぶものであり、1時間ではとても説明しきれないボリュームを判り易く説明いただくと共に、語りきれない部分については、提供いただいたツール類で補足をされました。提供されたツール類は次の通りです。

- ・CD-ROM:情報セキュリティ対策の基礎知識
- ・小冊子(6種)
- ・パンフレット:中小企業経営者の皆様へ

昨年から中小企業における情報セキュリティ対策に関する研究会を立ち上げ、対策主体を4つに分類して研究を進めていますが、現在、検討結果の取りまとめの段階にあり、その成果を紹介出来ないため、



本日は「ここにこういった役立つ情報、ツールがあります」とご紹介いただきました。

2. 【JNSA セッション】

中小企業の情報セキュリティ対策について

JNSA 西日本支部情報セキュリティチェックシートWGリーダー(富士通関西中部ネットテック)の嶋倉氏より、前身の個人情報保護対策チェックシートWGから進化させた同WGの活動成果についてご紹介いただきました。IPAの講演資料と同様に50ページを超えるボリュームを45分間で説明されました。

3. 【JASIPA セッション】

(テーマ1)

JNSA チェックシートの利活用報告

JNSAのWGが作成した情報セキュリティ対策チェックシートを高く評価いただいております、実際にシステムインテグレータであるJASIPA関西のメンバー企業が体験した結果をご報告いただきましたが、システムインテグレータの20%強が情報セキュリティ対策に関心である事がアンケートから確認されました。この事から、中小企業をサポートするIT企業を対象とした啓発が必要との認識を強く持つと共に、IT事業者への警鐘としたいとのJASIPA関西副支部長のシステム・ファームズ代表取締役の上森 茂氏からの説明が補足されました。

(テーマ2-1)

製造業における情報セキュリティ対策の実情について

製造業向けITパートナーとして活躍をされている(株)フエムト代表取締役の梅谷氏より、製造業の現場における情報セキュリティ対策の実情をご紹介いただくと共に、「賢い管理」でも、「システム管理

責任者は絶対必要」とご講演いただきました。WGの金型、鞆の団体を訪問しヒアリングで得られたデータと相似した製造業における“特に重要な機密情報”が網羅されており、業界特有の表現、説明文等の必要を改めて感じさせられました。

(テーマ2-2)

製造・生産業務の標準化と過剰在庫の削減成功事例について

化粧品・医薬品製造業向けのITパートナーとして活躍されているシステム・ファームズ(株)部長の大上誠一氏から、IT活用事例をご紹介いただくと共に、システム面から見た情報セキュリティ対策についてご講演いただきました。情報セキュリティ対策を可用性の視点に立って、ビジネスと連動している活用事例をご紹介いただき、これまでのCI偏重のアプローチとは違ったアプローチとなる内容でした

4. 【BoF】

なぜ進まない中小企業における情報セキュリティ対策

(1)BoF開催の目的

中小企業の情報セキュリティ対策の実情を把握するために実施したアンケート・ヒアリングの結果を総括し、情報セキュリティ対策を必要としている企業にはJNSA西日本支部が作成した情報セキュリティチェックシートを活用し、自社の実施状況を診断、さらなる改善・PDCAに役立てていただき、一方、守るべき情報資産があり、守らねばならない必要意識があるが、費用対効果の面が見えず躊躇・逡巡し対策が伴わない企業には、対策することへの義務化・切迫感を感じていただくために引き続きワークを継続し、情報セキュリティ対策の入口と考えられる情報資産管理台帳ワークシートの活用を推奨する事とし、台帳への記載を支援するサンプルモデル等を用意して、アンケート調査を行いました。

イベント開催の報告

その結果は、従前同様に回答率は低かったものの、製造業の業種団体の協力を得てより現場に近づいたものと評価できる事から、再度総括し、情報セキュリティ対策のさらなる飛躍に向けての課題、対策へのステップとすべく開催したものです。

(2) B o F の実施

パネルディスカッション方式で、情報セキュリティ対策を啓発・支援する側、対策を実践する上でサポートする側・ユーザ側の代表者を配し、それぞれの立場からの知見による議論が期待できるものとなりました。

モデレータ:

元持 哲郎 氏(アイネット・システムズ株式会社)

パネラー:

石井 茂 氏(IPAセキュリティセンター)

嶋倉 文裕 氏(富士通関西中部ネットテック株式会社)

梅谷 康子 氏(株式会社フェムト)

林 道彦 氏(三星ダイヤモンド工業株式会社)

中小企業の情報セキュリティ対策につながる現実的な解とは何か、中小企業に共通的に感じられる費用対効果への不満、さらに、中小企業が実際に実践できるアプローチ手法をテーマに議論が進み、会場からは常識が守れない場合の内部・外部の反応がはっきりしました。セキュリティ対策を行ったことで儲かった事例、信頼が営業成約につながった等の事例集を作り、もっと啓蒙すべきでは、等の意見も出され、活発な討議が行われました。今後のセミナー活動継続に勇気を与えてくれたセミナーでした。



2008 年度 「インターネット安全教室」のお知らせ

～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。

2007年度は全国で130回のインターネット安全教室を開催、6835名の方々にご参加いただきました。家庭向けのリーフレット「親子で守って安全・安心10か条」を作成し、配布するなど、昨今の携帯電話などによるネット利用の低年齢化にも配慮しています。

2008年度も全国各地の共催団体の方々のご協力を得て、引き続き開催してまいります。なお、現時点での開催状況は次頁をご覧ください。



【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、その他各開催地大学・新聞社・県・県警等(以上予定)

【開催一覧】(次頁)一覧をご覧ください。(2008年12月1日現在)

開催状況については、随時更新しています。「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/>

◆「インターネット安全教室」共催団体募集について◆

以下の地域で活動している共催団体を募集しております。

岩手県・高知県・福岡県・茨城県

- ・一般市民向けの情報セキュリティセミナーを実施したいがコンテンツがない
- ・教材を製作するにもコストも手間もかかるのでなかなかできない
- ・セミナー運営のノウハウがない
- ・しかし、情報セキュリティは大切。普及活動を行わないといけないと思っている

とお考えの団体等におかれましては、是非とも「インターネット安全教室」の共同開催をご検討下さい。また、そのような団体をご存知の方は是非事務局までご紹介下さい。

詳しくは下記のお問い合わせ先までご連絡下さい。

【お問い合わせ先】

■NPO 日本ネットワークセキュリティ協会(JNSA)事務局(担当:林・平田)

E-Mail: caravan-sec@jnsa.org

2008年度「インターネット安全教室」開催一覧

(2008年12月1日現在)

日程	開催地	共催団体	会場
6月7日(土)	富山	株式会社富山県総合情報センター	富山市立鶴坂公民館 会議室
6月7日(土)	愛媛	愛媛県 IT 推進協会	アイテムえひめ 愛媛国際貿易センター
6月7日(土)	鹿児島	NPO 法人鹿児島インファーマーション	鹿児島市消費生活センター研修室
6月17日(火)	岐阜(新規)	高山市立国府中学校	国府中学校 体育館
6月21日(土)	北海道	国立大学法人北見工業大学	北見工業大学総合研究棟 2階 多目的講義室
6月24日(火)	鹿児島	NPO 法人鹿児島インファーマーション	鹿児島市消費生活センター研修室
6月30日(月)	富山	株式会社富山県総合情報センター	富山市総曲輪公民館
7月5日(土)	群馬	NPO おおた IT 市民ネットワーク	宝泉行政センター 多目的ホール
7月5日(土)	神奈川	NPO 情報セキュリティフォーラム(NPO-ISEF)	綾瀬市立中央公民館 3階 講堂
7月7日(月)	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山南警察署
7月8日(火)	群馬	NPO 法人おおた IT 市民ネットワーク	錦打中学校 体育館
7月11日(金)	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山市立福南中学校
7月12日(土)	沖縄(新規)	NPO 法人フロム沖縄推進機構	沖縄コンベンションセンター 会議場 A1
7月12日(土)	神奈川	NPO 情報セキュリティフォーラム(NPO-ISEF)	アートフォーラムあさみ野 セミナールーム
7月17日(木)	大阪	NPO 法人きんぎうえぶ	河内長野市立小山田小学校
7月29日(火)	神奈川	NPO 情報セキュリティフォーラム(NPO-ISEF)	伊勢原市商工会館 4階 中会議室
7月30日(水)	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山市立光南台中学校図書館
8月6日(水)	山形	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 学術基盤センター
8月20日(水)	大阪	GIS 総合研究所	堺市立女性センター 3階 大ホール
8月22日(金)	長野	上田市マルチメディア情報センター	上田市・東築地公民館
8月22日(金)	神奈川	NPO 情報セキュリティフォーラム	逗子市役所 5階 第7・8会議室
8月24日(日)	岐阜	NPO 法人生涯の地域活動支援の会 アツマルぎふ	岐阜県民ふれあい会館第2棟4F
8月25日(月)	鹿児島	NPO 法人鹿児島インファーマーション	奄美情報処理専門学校
8月27日(水)	東京	NPO 情報セキュリティフォーラム	中野区立武蔵台小学校 視聴覚教室
9月4日(木)	大阪	NPO 法人きんぎうえぶ	河内長野市南花台西小学校
9月12日(金)	宮城	仙台インターネット推進研究会	仙台市市民活動サポートセンター 4F 研修室 5
9月16日(火)	神奈川	藤沢市	藤沢市辻堂公民館1階 第1談話室
9月16日(火)	神奈川	NPO 情報セキュリティフォーラム	綾瀬市役所 3階 315 会議室
9月18日(木)	神奈川	NPO 情報セキュリティフォーラム	鎌倉商工会議所 3F 会議室
9月25日(木)	大阪	NPO 法人きんぎうえぶ	河内長野市三日市公民館
9月25日(木)	三重	くわな PC ネット	桑名市総合福祉会館(桑名市社会福祉協議会内) 第2会議室
9月29日(月)	東京	NPO 法人イーパーツ	世田谷文化生活情報センター
10月1日(水)	東京	NPO 法人 CANVAS、 (財) 日本情報処理開発協会「情報化月間」事務局	ANA インターコンチネンタルホテル東京 地下 1F「プリズム」
10月3日(金)	東京	NPO 情報セキュリティフォーラム(NPO-ISEF)	中野区立新山小学校 図書室
10月7日(火)	奈良	奈良県社会教育センター	斑鳩町中央公民館
10月8日(水)	福井	NPO ナレッジふくい	敦賀中郷公民館
10月10日(金)	大阪	NPO 法人きんぎうえぶ	河内長野市立楠小学校
10月12日(日)	福島	NPO 法人日本コンピュータ振興協会	公立大学法人 会津大学
10月17日(金)	神奈川	NPO 情報セキュリティフォーラム	ウエルネスさがみはら A館 7階 視聴覚室
10月18日(土)	福島	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
10月21日(火)	福井	NPO 法人ナレッジふくい	越前市ワークメイト
10月23日(木)	栃木	NPO 栃木シニアセンター	小山市中央公民館
10月24日(金)	神奈川	NPO 情報セキュリティフォーラム	秦野市立西公民館 2階 大会議室
10月25日(土)	北海道	旭川情報産業事業協同組合	旭川市科学館
10月25日(土)	和歌山	情報セキュリティ研究所	海南市立第3中学校
10月26日(日)	新潟	NPO 新潟情報セキュリティ協会	ほんぼーと(新潟市立中央図書館) 3階 研修室2
10月27日(月)	大阪	GIS 総合研究所	追手門学院大学
10月28日(火)	奈良	奈良県社会教育センター	かしはら万葉ホール
11月7日(金)	神奈川	藤沢市	藤沢市長後公民館 第2談話室

11月8日(土)	大阪	NPO 法人きんきうえぶ	河内長野市立長野小学校
11月8日(土)	徳島(新規)	財団法人 e- とくしま推進財団	アスティとくしま
11月8日(土)	滋賀	NPO 滋賀県情報基盤協議会	滋賀県立彦根工業高等学校
11月8日(土)	福井	NPO 法人ナレッジふくい	福井市春山公民館
11月8日(土)	神奈川	NPO 情報セキュリティフォーラム	南足柄市立向田小学校 図書室
11月12日(水)	青森	財団法人八戸地域高度技術振興センター	八戸市総合福祉会館 2階多目的ホール
11月12日(水)	大阪	NPO 法人きんきうえぶ	河内長野市立加賀田小学校体育館
11月15日(土)	群馬	NPO 法人おおた IT 市民ネットワーク	九合行政センター
11月15日(土)	神奈川	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 2階 集会室 202
11月16日(日)	宮崎	宮崎公立大学	宮崎公立大学 交流センター 多目的ホール
11月18日(火)	神奈川	NPO 情報セキュリティフォーラム	横須賀市役所 3号館 5階 正庁
11月18日(火)	神奈川	藤沢市	藤沢市明治公民館 第2 談話室
11月18日(火)	大阪	NPO 法人きんきうえぶ	河内長野市立高向小学校
11月18日(火)	東京	NPO 法人イーパーツ	世田谷ボランティアセンター
11月21日(金)	大阪	NPO 法人きんきうえぶ	河内長野市立加賀田小学校体育館
11月21日(金)	神奈川	藤沢市	藤沢市片瀬公民館 第2 談話室
11月22日(土)	福井	NPO 法人ナレッジふくい	福井市日新公民館
11月27日(木)	神奈川	NPO 情報セキュリティフォーラム	フォーラム南太田 3階 大会議室
11月27日(木)	和歌山	NPO 情報セキュリティ研究所	海南市立内海小学校
11月29日(土)	神奈川	NPO 情報セキュリティフォーラム	川崎市多摩市民館 3階 大会議室
11月29日(土)	岐阜	NPO 法人泉京・垂井(セント・タルイ)	垂井町文化会館 小ホール
11月29日(土)	奈良	奈良県社会教育センター	王寺町やわらぎ会館
11月29日(土)	福井	NPO 法人ナレッジふくい	福井厚生年金会館
11月30日(日)	愛知	東海インターネット協議会	愛知工業大学 本山キャンパス講義室1
12月2日(火)	神奈川	NPO 情報セキュリティフォーラム	相鉄岩崎学園ビル 8階 809号室
12月5日(金)	大分	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 102 講義室
12月8日(月)	神奈川	藤沢市	藤沢市湘南台公民館 第1 談話室
12月14日(日)	鹿児島	NPO 鹿児島インファーマーシオン	鹿児島アリーナ 1階 会議室 B
12月16日(火)	神奈川	藤沢市	藤沢市御所見台公民館 第2 談話室
12月19日(金)	神奈川	藤沢市	藤沢市村岡公民館 学習室
12月23日(火)	神奈川	NPO 情報セキュリティフォーラム	横浜リハビリテーション専門学校
1月16日(金)	神奈川	藤沢市	藤沢市湘南大庭公民館 第1 談話室
1月16日(金)	滋賀	NPO 滋賀県情報基盤協議会	龍谷大学 瀬田学舎 6号館 B108 教室
1月22日(木)	神奈川	NPO 情報セキュリティフォーラム	神奈川県平塚合同庁舎
1月23日(金)	神奈川	藤沢市	藤沢市鶴沼公民館 第3 談話室
1月27日(火)	神奈川	NPO 情報セキュリティフォーラム	厚木市ヤングコミュニティセンター
1月28日(水)	神奈川	NPO 情報セキュリティフォーラム	藤沢市役所
1月28日(水)	神奈川	藤沢市	藤沢市総合防災センター 6階 第1、第2 会議室
1月29日(木)	神奈川	NPO 情報セキュリティフォーラム	二宮町 IT ふれあい館
1月29日(木)	大阪	NPO 法人きんきうえぶ	河内長野市立南花台公民館
2月4日(水)	神奈川	NPO 情報セキュリティフォーラム	葉山町福祉文化会館
2月6日(金)	香川	e- とびあ・かがわ	e- とびあ・かがわ BB スクエア
2月13日(金)	熊本	NPO 法人 NEXT 熊本	くまもと県民交流館パレア パレアホール
2月13日(金)	神奈川	NPO 情報セキュリティフォーラム	神奈川県横須賀合同庁舎
2月13日(金)	神奈川	藤沢市	藤沢市六会公民館 第2 談話室
2月14日(土)	室蘭	NPO 法人くるくるネット	胆振地方男女平等参画センター(ミンクール) 2F大会議室 A
2月15日(日)	神奈川	NPO 情報セキュリティフォーラム	海老名市役所
3月2日(月)	神奈川	藤沢市	藤沢市遠藤公民館 第1 談話室
3月6日(金)	神奈川	NPO 情報セキュリティフォーラム	藤沢商工会議所
3月6日(金)	神奈川	藤沢市	藤沢市善行公民館
3月13日(金)	神奈川	藤沢市	藤沢市藤沢公民館 第2 談話室

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26～27ページの一覧表を、各地の開催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・協賛イベントのお知らせ

1. 2009年1月23日(金)ほか 後援イベント

「2008年度 全国縦断 情報セキュリティ監査セミナー」

会場：

【広島】2009年1月23日(金) 13:30-17:00 RCC文化センター

【富山】2009年2月13日(金) 13:30-17:00 タワー111スカイホール

主催：経済産業省、

特定非営利活動法人 日本セキュリティ監査協会(JASA)

<http://www.jasa.jp/seminar/secf2008lh.html>

2. 2009年1月28日(水)～29日(木) 協賛イベント

「ソフトウェアテストシンポジウム 2009 東京」

会場：目黒雅叙園

主催：特定非営利活動法人 ソフトウェアテスト

技術振興協会(ASTER)

<http://jasst.jp/archives/jasst09e.html>

3. 2009年2月4日(水)-6日(金) 協賛イベント

「PAGE2009」

会場：サンシャインシティコンベンションセンターTOKYO

主催：社団法人日本印刷技術協会

<http://www.jagat.or.jp/page/>

4. 2009年02月19日(木) 後援イベント

「HOSTING-PRO 2009」

会場：秋葉原コンベンションホール

主催：HOSTING-PRO 2009実行委員会

<http://hosting-pro.jp/>

5. 2008年2月開催予定 後援イベント

中小企業庁委託事業

「平成20年度 情報モラル啓発セミナー」

会場：【宮崎】2009年2月予定(会場・日時未定)

主催：中小企業庁、各経済産業局、

(財)ハイパーネットワーク社会研究所

<http://www.hyper.or.jp/moral2008/>

3. JNSA 部会・WG 2008 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：大谷尚通 氏/NTTデータ)

2008年1年間に発生した情報漏えいによる情報セキュリティ被害の実態を調査し、情報漏えいインシデントの傾向、対策状況、組織に与えるインパクト等を定量的に分析し、報告書として公開する。また、情報漏えい以外の情報セキュリティインシデントについて、算定モデルを検討し、同じく組織に与えるインパクト等の定量化を目指す。

過去の成果物は、年度毎の「情報セキュリティインシデントに関する調査報告書」(本編、英語版、データ集CD-ROM)

今年度の予定成果物は「2008年度情報セキュリティインシデントに関する調査速報」

【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)

2008年度は、企業におけるアクセス権付与に関する考え方と、アイデンティティの企業間連携を成果物テーマとして、第2版の発行を目的とする。また、インターネットにおけるアイデンティティ(OpenID, Liberty, SAMLなど)を勉強テーマとして活動する。

予定成果物は、内部統制におけるアイデンティティマネジメント解説書とセミナーの実施。

【情報セキュリティランキングWG】

(リーダー：佐野智己 氏/凸版印刷)

情報開示の充実度や取り組み姿勢、社会貢献活動などにも着目した、JNSA版情報セキュリティランキングを定期的に公表する。上位ランキング企業がどのような取り組

みをしているかを把握するとともに、真摯に取り組む企業を讃える仕組みとして定着を目指す。

予定成果物は、ランキング結果。

【情報セキュリティ関連パブコメ検討WG】

(リーダー：河野省二 氏/ディアイティ)

毎年、各省庁から情報セキュリティ関連の政策が数多く提出されており、これらの多くにパブリックコメントが求められている。

これらの政策についてよく理解するための勉強会を開催し専門家としての知識を得ること、そして専門家としての意見を政策に反映するためのパブリックコメントを提出することを目的として活動する。

【セキュリティ市場調査WG】

(リーダー：勝見勉 氏/情報経済研究所)

情報セキュリティに関する市場の状況ならびに規模等を調査・分析し、WG参加者、JNSA、業界、行政の参考として供する。併せて参加者の勉強・研鑽の場として活用してもらい、業界知識の拡大、人脈の展開、調査分析スキルの向上に資する。

2008年度も経済産業省委託事業の一環として実施。

予定成果物は、「2008年度版情報セキュリティ市場調査報告書」。

2. 技術部会

(部会長：二木真明 氏/住商情報システム)

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

成果物目的のワーキンググループ

【ハニーポットWG】

(リーダー：園田道夫 氏/JNSA研究員)

ネットを飛び交うマルウェアの実態を、ハニーポットやおとりサーバー、おとりのアカウントなどを用いて研究・解析する。

予定成果物は、マルウェア捕獲報告書。

【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の技術的課題の収集、および、アプリケーションセキュリティの国際規格の内容の検討とコメント作成を行う。

予定成果物は情報規格調査会に対するインプットコメント。

【セキュアOS普及促進WG】

(リーダー：澤田栄浩 氏/JTS)

セキュアOSの有効性をアピールするために活動内容をWebに公表し、公表している情報を見てもらえるように各種雑誌にアピールしていく。また、インシデントとセキュアOSの関係を紐解いていく。

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)

PKI相互運用技術の情報共有を行う。年間の活動としては、IETFの参加、PKI dayなどのセミナー開催など。予定成果物は、「暗号アルゴリズムの移行問題」について、何らかの報告書をまとめる可能性がある。

プロジェクト

【Challenge PKI】

(リーダー：松本泰 氏/セコム)

2008年度は、Multi-domain-PKIのRFC化の見通しが立っており、このRFC化を足掛かりとして、「暗号アルゴリズム移行問題」、「電子署名法に関連した相互運用技術の課題」など、幅広い問題の解決に取り組むことを検討している。

3. マーケティング部会

(部会長：高橋正和 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。

【会員製品 PR 企画検討WG】

(リーダー：小屋晋吾 氏/トレンドマイクロ)

IDGジャパン社に運営移管した「セキュリティ製品バイヤーズガイド」へのコンテンツ提供や製品登録への協力などについて検討を行う。

【セキュリティ啓発WG】

(リーダー：平田敬 氏/ブリッジ・メタウェア)

2007年度同様、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。

4. 教育部会

(部会長：安田直 氏/サイバー大学/JNSA主席研究員)

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】

(リーダー：大河内智秀 氏/NTTラーニングシステムズ)

2008年度は、CISSPに関する知名度向上に関する取り組みを行う。

【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リスクソリューションズ)

2008年2月に公開した組織管理者向け機能を追加した「情報セキュリティ理解度チェックサイト」のビジネスモデル案の検討を行うとともに、サイト全体の自主運営に向けた検討を行う。

【SecBok(セキュリティ知識分野作成) WG】

(リーダー：長谷川長一 氏/ラック)

引き続き、セキュリティ知識の策定と活用に関わる検討を行う。また、活動の目的や内容がほとんど重複する情報セキュリティ教育事業者連絡会(ISEPA)との棲み分けを検討し、今年度以降の役割分担と連携関係を明確にする。

予定成果物は、「セキュリティ知識分野2008年度版(仮)」、「セキュリティ知識分野活用ガイド(仮)」

【セキュリティ講師スキル研究WG】

(リーダー：長谷川長一 氏/ラック)

引き続き、セキュリティ講師に必要なスキルの調査研究および実証を行う。(情報セキュリティ教育事業者連絡会:ISEPAとの連携による活動も行う)

策定した「セキュリティ講師スキル(案)」をもとに更なる調査や実証実験を実施する。

予定成果物は、「セキュリティ講師スキル研究調査報告書」

【情報セキュリティ教科書執筆WG】

(リーダー：塩見友規 氏/オー・エイ・エス)

情報セキュリティのプロフェッショナルを目指そうというIT技術者向けの「教科書」を執筆することを目的とする。スキルマップなどの項目分類の更新情報等を参考にし、専門家としての初学者に知ってもらいたい内容をできるだけ網羅する。

予定成果物は、情報セキュリティのプロフェッショナル向け教科書(書名未定)の出版。

【教育アーカイブズ検討WG(仮称)】

(リーダー：河野省二 氏/ディアイティ)

JNSAメンバーを始め、非メンバーも、セミナーや研修用に色々なスライド等を持ち、大抵の場合再利用されずに埋もれている状態である。著作者本人が公開すれば権利関係の問題は無く、質の高い教育用資料を社会的に共有することができる。

教育用資料等の有効活用、歴史的なアーカイブを保管・検索できる「場」を作るということは意義があるだろうということから、具体的なアーカイブを作るための検討と試行をする予定である。

予定成果物は、試行用データの収集とデータベース化の試行報告書。

【情報セキュリティ基本教育実証WG

(旧:岡山理科大学遠隔授業実施WG)】

(リーダー：平山敏弘 氏/日本IBM)

今まで、情報セキュリティの教育者のスキルについて検討を行い、2006年度に「情報セキュリティ教育の指導者向け手引書」を公開した。これらの成果を実践に生かす形で、岡山理科大学で集中講義という形で遠隔授業を行ってみたい。

2009年度からは2単位(15駒)の正式単位認定講義となるのに伴い、カリキュラムやシラバス、講義内容、講義形式等々の検討を行うため、WGとして活動することにした。

講師候補の方々を始め、実際の大学での遠隔授業に一家言ある方の参加も可能である。

予定成果物は、講義のシラバス、講義資料、定期試験、等々のコンテンツ類と報告書。

5. U40部会

(部会長：加藤雅彦 氏/アイアイジェイテクノロジー)

若年層を対象メンバーとして、技術習得向上のための研鑽の場、人脈作りの場を提供する。また、JNSA運営への積極的な関与、会員間の交流の強化、活動活性化のための情報流通強化、セキュリティ業界や社会への貢献などを目的とする。

【JNSAラボネットWG】

(リーダー：坂本 慶 氏/ディアイティ)

ワーキンググループの活動における、実環境を使った技術検証などが円滑に行えるように、検証環境の設計と構築を議論し、実際の環境構築を行う。またU40部会のWGとして、本活動を通して若手メンバーのスキル向上を図る。

予定成果物は、検証環境の提供。

【勉強会企画検討WG】

(リーダー：嘉津義明 氏/シマンテック)

若年層の知識および技術向上のため、メンバー向けの勉強会を企画検討し、講師手配などを行なう。これにより外部との人脈作りおよび運営面についてのスキルアップも図る。また、良い企画があれば、JNSA会員向けのセミナーとして推薦する。

6. ユーザー部会 ※新設

(部会長：未定)

JNSA参加企業は、ISMSやPマークを取得し、かつ情報セキュリティベンダーとして、セキュリティビジネスを行っている。しかしながら、自社の企業内ユーザー(例えば、営業、エンジニア、管理系部署)の情報セキュリティモラルが上がっていないことも事実である。

このため、今年度は、成功失敗の事例紹介、テーマ毎の研究会を行い、効果的な企業内ユーザーのモラル醸成方法、効率的な情報セキュリティ運用方法を模索していくような活動を行う予定である。

7. 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。

【企画運営WG】

(リーダー：井上陽一 氏/JNSA顧問)

中小企業の情報セキュリティ水準の底上げ、中小企業の負担軽減に繋がる方策について、情報セキュリティチェックシートWGと共同して明示・PDCA定着化のための啓発を行うと共に、近畿経済産業局と協働して地域における産官共同の基盤づくりを行う。予定成果物として、情報セキュリティチェックシートWGと共同して、チェックシート作成・解析結果を報告書としてまとめる。

【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)

情報セキュリティチェックシートを使用することにより、中堅・中小企業の経営者(経営層)が気付きを超えた企業価値向上の視点で、自社のセキュリティ対策の現状を認識し、対応して頂く上でのガイダンスとなるような情報セ

キュリティチェックシートの作成を目標として活動する。

予定成果物は、チェックシートおよびアンケート解析結果報告。

情報セキュリティ教育事業者連絡会 (ISEPA)

(代表：与儀大輔 氏/ラック)

連絡会各会員団体の運営する資格の位置付け、キャリアパスに対する共通認識の提示、施策提案、さらには各種教育機関との連携によるコンテンツの共同利用など、情報セキュリティ人材育成に関する様々な情報を社会に広く提供し、人材育成の拡大に向けた様々な取り組みを推進する活動を行う。

【イベントWG】

(リーダー：杉本毅 氏/ITプロフェッショナル・グループ)

ホームページ、各種イベント、あるいは各種の広報活動により、ISEPA情報セキュリティ教育事業者連絡会の活動や取り組みを、社会に広く紹介していく。

【スキルWG】

(リーダー：衣川俊章 氏/ITプロフェッショナル・グループ)

各団体の資格試験の内容を体系的に整理し、各資格試験の相関図の作成やキャリアパスを提示し、情報セキュリティの分野で求められる人材像を具体的に示していく。

【相互認証WG】

(リーダー：関取嘉浩 氏/NRIセキュアテクノロジーズ)

各事業者間の相互認証の可能性の検討を行なう。また、必要に応じてWGを開催し、相互認証の可能性について検討していく。認定資格取得者数の調査も行う予定。

日本セキュリティオペレーション事業者協議会 (ISOG-J)

(代表：武智洋 氏/ラック)

セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進する事業を実施することにより、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に向けて寄与する目的として発足。JNSA下部組織として、ガイドラインの策定や技術向上に向けた検討、普及啓発活動を行う。

4. JNSA 役員一覧 2008年11月現在

会 長 佐々木 良一
東京電機大学 教授
副会長 高橋 正和
マイクロソフト株式会社
副会長 大和 敏彦
ブロードバンドタワー株式会社

理 事 (50音順)

足立 修 株式会社シマンテック
池田 修一 NTT コミュニケーションズ株式会社
後沢 忍 三菱電機株式会社 情報技術総合研究所
遠藤 直樹 東芝ソリューション株式会社
大坪 武憲 新日鉄ソリューションズ株式会社
勝見 勉 株式会社情報経済研究所
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
佐藤 邦光 大日本印刷株式会社
下村 正洋 株式会社ディアアイティ
立石 和義 NTT アドバンステクノロジー株式会社
橘 伸俊 株式会社ネットマークス
玉井 節朗 株式会社IDGジャパン
西尾 秀一 株式会社NTTデータ
西本 逸郎 株式会社ラック
野々下幸治 マカフィー株式会社
森田 次朗 インスパイアー株式会社
日暮 則武 東京海上日動火災保険株式会社
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

監 事

土井 充 公認会計士 土井充事務所

特別顧問

石田 晴久 サイバー大学 IT 総合学部 学部長

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
武藤 佳恭 慶応義塾大学 教授
前川 徹 サイバー大学 教授
村岡 洋一 早稲田大学 教授
安田 浩 東京電機大学 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 株式会社ディアアイティ

5. 会員企業一覧 (2008年12月5日現在 204社 50音順)

【あ】

株式会社アーク情報システム **New**
 (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
 アイエックス・ナレッジ(株)
 (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
 (株)アイティープレーン
 (株)アイテクノ
 アイネット・システムズ(株)
 (株)アイ・ビー・イー・ネット・タイム
 (株)IPイノベーションズ
 アイマトリックス(株)
 (株)アクシオ
 あずさ監査法人
 (株)網屋(株)
 (株)アルテミス
 (株)アルファシステムズ
 アルプスシステムインテグレーション(株)
 イー・ガーディアン(株) **New**
 (株)ISA O
 伊藤忠テクノソリューションズ(株)
 学校法人 岩崎学園
 (株)インストラクション
 インスパイアー(株)
 (株)インターネットイニシアティブ
 (株)インテックシステム研究所
 (株)インテリジェントウェイブ
 インフォコム(株)
 (株)インフォセック
 ヴァイタル・インフォメーション(株)
 ウェブセンス・ジャパン(株)
 ウェブルート・ソフトウエア(株)
 AT&Tジャパン(株)
 エクスジェン・ネットワークス(株) **New**
 (株)エス・エス・アイ・ジェイ
 (株)エス・シー・ラボ
 SBIネットシステムズ(株)
 NRIセキュアテクノロジーズ(株)

エヌアイシー・ネットシステム(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ー(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)
 NTTコムテクノロジー(株)
 (株)NTTデータ
 (株)NTTデータCCS
 NTTラーニングシステムズ(株) **New**
 (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)
 オー・エイ・エス(株)
 (株)オーク電子
 (株)大塚商会
 (株)オレンジソフト

【か】

(株)Kaspersky Labs Japan
 兼松エレクトロニクス(株)
 関電システムソリューションズ(株)
 キヤノンIT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)
 クオリティ(株)
 (株)グローバルエース
 グローバルサイン(株)
 グローバルセキュリティエキスパート(株)
 (株)ケーケーシー情報システム
 (株)コネクタス
 コンピュータエンジニアリングサービス(株)

【さ】

サードネットワークス(株)
 サイバーエアリサーチ(株)
 サイバーソリューション(株)
 (株)サイロック
 サン・マイクロシステムズ(株)
 (株)シー・エス・イー

(株)JMCリスクソリューションズ
 ジェイズ・コミュニケーション(株)
 (株)JTS
 JPCERTコーディネーションセンター
 シスコシステムズ合同会社
 システム・エンジニアリング・ハウス(株)
 (株)シマンテック
 (株)ジャパンネット銀行
 寿限無(株)
 (株)情報経済研究所 **New**
 (株)情報数理研究所
 新日鉄ソリューションズ(株)
 新日本有限責任監査法人
 (株)ステラクラフト
 住商情報システム(株)
 スミセイ情報システム(株)
 セキュアコンピューティングジャパン(株)
 (株)セキュアブレイン
 セキュリティ・エデュケーション・アライアンス・ジャパン
 セコム(株)
 セコムトラストシステムズ(株)
 (株)セラク
 セントラル短資オンライントレード(株)
 ソニー(株)
 ソフォス(株)
 ソフトバンク(株)
 ソフトバンク・テクノロジー(株) **New**
 ソフトバンクBB(株)
 ソラン(株)
 (株)ソリトンシステムズ
 (株)損保ジャパン・リスクマネジメント

【た】

大興電子通信(株)
 大日本印刷(株)
 (株)大和総研
 (株)タクマ
 チェックポイントソフトウェアテクノロジーズ(株)
 TIS(株)
 (株)ディアイティ
 デジタルアーツ(株)
 (株)電通国際情報サービス
 監査法人トーマツ
 東京エレクトロン デバイス(株)

東京海上日動火災保険(株)
 東京日産コンピュータシステム(株)
 東芝ITサービス(株)
 東芝ソリューション(株)
 ドコモ・システムズ(株)
 凸版印刷(株)
 トップレイヤーネットワークスジャパン(株)
 トリップワイヤ・ジャパン(株)
 トレンドマイクロ(株)

【な】

(株)ニコンシステム
 西日本電信電話(株)
 日信電子サービス(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)
 日本クロストラスト(株)
 日本CA(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)
 日本ビジネスコンピューター(株)
 日本ビューレット・パッカード(株)
 日本ベリサイン(株) **New**
 (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】

パスロジ(株)
 パナソニック電工(株)
 バリオセキュア・ネットワークス(株)
 (株)ハンモック
 (株)日立システムアンドサービス
 (株)日立情報システムズ
 (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
 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)
 (株)富士通エフサス
 富士通関西中部ネットテック(株)
 (株)富士通ソーシャルサイエンスラボラトリ(富士通SSL)
 (株)富士通ビジネスシステム
 富士電機アドバンステクノロジー(株)
 扶桑電通(株)
 フューチャーアーキテクト(株)
 (株)フューチャーイン
 (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)ブロードバンドタワー
 (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)
 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
 三菱総研DCS(株)
 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)
 (株)ユービーセキュア

【ら】

(株)楽堂 **New**
 (株)ラック
 LANDesk Software(株)
 リコー・ヒューマン・クリエイツ
 (有)ロボック

【わ】

(株)ワイ・イー・シー
 (株)ワイズ

【特別会員】

特定非営利活動法人 アイタック
 韓国電子通信研究院
 社団法人 コンピュータソフトウェア協会
 ジャパン データ ストレージ フォーラム
 財団法人 ソフトピアジャパン
 データベース・セキュリティ・コンソーシアム
 特定非営利活動法人デジタル・フォレンジック研究会
 電子商取引安全技術研究組合
 東京大学大学院 工学系研究科
 社団法人 日本インターネットプロバイダー協会
 社団法人 日本コンピュータシステム販売店協会
 特定非営利活動法人 日本セキュリティ監査協会
 有限責任中間法人 日本電子認証協議会

6. JNSA 年間活動 (2008 年度)

4月	4月23～24日	「RSA Conference Japan 2008」後援	
5月	5月1日	第1回幹事会	
	5月14日	2008年度理事会(虎ノ門パストラル)	
	5月26～27日	「CeCOS II Tokyo(Counter eCrime Operation Summit II in Tokyo)」後援	
6月	6月5～7日	「第12回サイバー犯罪に関する白浜シンポジウム」後援	
	6月9～13日	「Interop Tokyo 2008」後援	
	6月13日	2007年度WG活動報告会(ベルサール八重洲)	
	6月13日	2008年度総会(ベルサール神田)	
	6月18日	「平成20年度情報モラル啓発セミナー」(兵庫会場)後援	
	7月	7月1～2日	「SANS Future Visions 2008 Tokyo」後援
	7月3日	「PKI Day 2008」セミナー(東京ウィメンズプラザ)	
	7月4～5日	「WASForum Conference2008」後援	
	7月8日	第2回幹事会	
	7月9日	「2008年度 情報セキュリティ監査シンポジウム in Tokyo」後援	
	7月10～12日	「沖縄 ICT フォーラム 2008」後援	2008年6月～ 2009年3月 「インターネット 安全教室」開催
	7月16～18日	「自治体総合フェア 2008」協賛	
	7月17日	「平成20年度情報モラル啓発セミナー」(三重会場)後援	
	7月22～24日	「ワイヤレスジャパン 2008」後援	
	7月24日	リコー情報セキュリティ強化セミナー「今、再び考える『情報セキュリティ』」後援	
8月	8月13～17日	「セキュリティ&プログラミング・キャンプ 2008」後援	
	8月22日	「被害調査 WG・リテラシーベンチマーク作成WG合同セキュリティ対策セミナー」(メルパルク東京)	
	8月25日	「2008年度 全国縦断情報セキュリティ監査セミナー」(札幌会場)後援	
	8月26日	第3回幹事会	
	8月29日	「CompTIA Breakaway in Japan」後援	
9月	9月26日	「平成20年度情報モラル啓発セミナー」(北海道会場)後援	
	9月26日	「2008年度 全国縦断情報セキュリティ監査セミナー」(高松会場)後援	
	9月9～10日	「SCM フォーラム 2008」協賛	
10月	10月2日	「2008年度 全国縦断情報セキュリティ監査セミナー」(仙台会場)後援	
	10月21日	「2008年度 全国縦断情報セキュリティ監査セミナー」(福岡会場)後援	
	10月23～25日	「モノづくりフェア 2008」協賛	
	10月31日	「第1回全国情報セキュリティ啓発シンポジウム やろっさ『インターネット安全教室』 in ふくい」	
11月	11月11日	「2008年度 全国縦断情報セキュリティ監査セミナー」(大阪会場)後援	
	11月11日	「H@cker Halted Japan Visions 2008」後援	
	11月25～28日	「Internet Week 2008」後援	
	11月26日	「中小企業情報セキュリティ対策支援セミナー」(大阪国際会議場)	
	11月26日	「CMS Conference 2008」後援	
	11月29日	「第21回秋の学術講演会～インターネットの匿名性を考える～」後援	
12月	12月12～14日	「かごしま IT フェスタ 2008」後援	
	12月15～16日	「デジタル・フォレンジック・コミュニティ 2008 in TOKYO」後援	
	12月16日	「Security Day 2008」セミナー(ベルサール八重洲)	
	12月17～18日	「NSF 2008 (NetworkSecurityForum2008)」(ベルサール八重洲)	
	12月19日	「2008年度 全国縦断情報セキュリティ監査セミナー」(名古屋会場)後援	
1月	1月23日	「2008年度 全国縦断情報セキュリティ監査セミナー」(広島会場)後援	
	1月28～29日	「ソフトウェアテストシンポジウム 2009 東京」後援	
2月	2月4～6日	「PAGE2009」協賛	
	2月13日	「2008年度 全国縦断情報セキュリティ監査セミナー」(富山会場)後援	
	2月19日	「HOSTING-PRO 2009」後援	
	2月予定	中小企業庁委託事業 「平成20年度 情報モラル啓発セミナー」(宮崎会場)後援	
3月			

★ JNSA 活動スケジュールは、<http://www.jnsa.org/aboutus/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/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. お問い合わせ

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

〒105-0003 東京都港区西新橋 1-22-12 JC ビル 3F

TEL：03-3519-6440

TEL：03-3519-6441

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 事務局移転のお知らせ ■

JNSA 事務局は、2008 年 9 月に下記住所に移転致しました。

〒105-0003 東京都港区西新橋 1-22-12 JC ビル 3F

Tel: 03-3519-6440 Fax: 03-3519-6441

JNSA Press vol.24

2008 年 12 月 19 日発行

©2008 Japan Network Security Association

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)

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

〒105-0003 東京都港区西新橋1-22-12 JCビル 3F
TEL 03-3519-6440 FAX 03-3519-6441
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) デイアイティ内
TEL 06-6886-5540