JNSA Press

Japan Network Security Association

Vol.13
March 2005

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

JNSAのいままでとこれから

NPO日本ネットワークセキュリティ協会
事務局長 下村　正洋

JNSAは、任意団体として2000年4月に設立され、2001年5月に特定非営利活動法人（NPO）として認可され、同年7月からNPOとして活動してきました。2005年4月には、当初から数えると丸5年の活動の軌跡を残してきたことになります。その間にネットワークセキュリティをめぐる環境や社会意識は大きく変わってきました。まさに隔世の感があります。当初、JNSAはネットワークのセキュリティをテーマとして考えていたのですが、活動を開始して間もなくネットワークセキュリティではなく情報セキュリティ全般を対象とせざるを得なくなりました。これは振り返ってみれば当然のことでありました。たとえば、個人情報保護法に象徴されるように情報の所有権が明確になり、それに対処する必要があること、また、インターネット上のサービスの拡大と利用者の拡大により、情報の価値が増大し、その情報を悪用する行為が拡大していることなどが考えられます。これらに対処するためには、ネットワークシステムやITシステムを駆使しても完全に対処できるわけでもなく、社会として対処すべきことも必要です。まさに、情報セキュリティを文化として創造することが必要ではないでしょうか。

『技術だけでは問題は解決できない。しかし技術の裏付けがなければ施策もできない。』というのが現実だと思います。ほとんどの技術以外の問題は、すでに社会システムの中で似たような現象が発生していて対応策も考えられています。過去の英知を生かすことができるはずです。法律や制度の対応に抜け穴があるのであれば、塞げばいいことです。それが経験を生かすということです。イタチごっこは何も今に始まったことではありません。知恵比べは永遠でしょう。

さて、JNSAの「いままで」は、案外うまく行ってきました。かなり独創的な報告書や他ではあまりない活動の蓄積ができました。これらは原則としてJNSAなどのWebページで公開されています。今までの活動は、どちらかというと「問題意識共有型」といえるでしょう。同じ問題を抱えているメンバーが、いろいろな垣根を越えて共通する目的を目指して活動することにより、お金では換え難い成果が得られてきましたし、ビジネスマーケットを形成するために必須の情報を作り公開することができました。この意味で、JNSAは情報セキュリティ分野の成熟に微力ながら寄与できたのではないかと自負しています。

JNSAの「これから」ですが、「いままで」の活動を継続するとともに、新しい動きも出てきています。今までの活動を支えてきた参加者のモチベーションを更に高め、新しいメンバーに加わってもらうとともに、参加企業へのインセンティブも考える必要があります。またインターネット安全教室を通して家庭などITに縁遠かった方達への啓発活動のひとつの成果として、セキュリティ対策推進協議会（SPREAD）のアイディアが出てきたこと、ChallengePKIプロジェクトがインターネット標準を決めているIETF（The Internet Engineering Task Force）で行っている国際的な活動で貢献したり、インシデント被害調査WGが試案した個人情報漏洩の賠償額算定モデル式は、情報資産のリスク評価を行う際の指標となるでしょう。他にも、環境会計にアイディアを得たセキュリティ会計の検討は今後のITセキュリティの施策に重要な意味を持つでしょうし、ITセキュリティの専門家としての技術者の得意分野を分かり易く表現する目的で技術分野の分類整理を行ったスキルマップ、セキュリティポリシーを作るために考え方の叩き台となるポリシーサンプルの公開、等々に加え、これからの情報セキュリティを実現する上での政策を含めた公共的な活動も増えていきそうです。

情報セキュリティは深く考えれば考えるほど、色々なつながりが出てきて奥が深いものだと実感しています。色々な問題点を広く議論し考えられる場として、JNSAを利用していただければ幸いです。今後とも皆様のご協力・ご指導をどうぞよろしくお願いいたします。

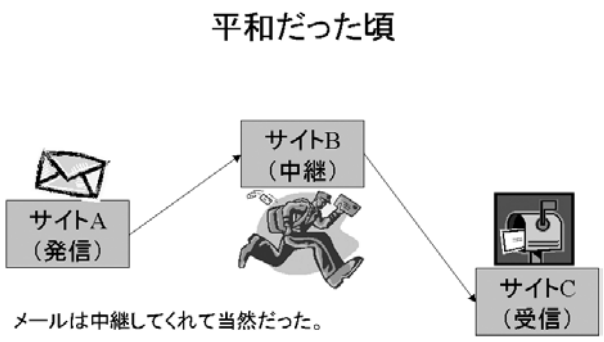
迷惑メール（スパム）対策技術の変遷

株式会社IRIコミュニケーションズ
安藤　一憲

メールボックスが頼んでもいないのに送られてくる広告メールで埋め尽くされている、という現象は昨今珍しくない。この招かざる客は一般に迷惑メールとかスパムと呼ばれる。いまやスパムの送信元は世界中に散らばっており、国内法だけで取締りが十分にできる保証はない。恐ろしいことに、たかがスパムに立ち向かうにも国を超えた対処が必要なのである。さらに言えば、スパムの受信量には著しい個人差がある。自分のメールボックスが無事でも会社の他の人間のメールボックスが無事だとは限らない。いまやスパム対策は新旧入り交じり、どの対策がどういう利点を持ち何に弱いのかを掴むのもひと苦労という状況になりつつある。本稿ではそれぞれのスパム対策技術がどのような経過で登場してきたかをひととおり振返ることで、最新の動きである送信ドメイン認証やレピュテーションといった技術がどういう意味を持っているのか改めて考えてみたい。

1. 平和だった頃

まだ世の中にWWWが存在せず、メール配送先の決定がDNSに依存していなかった時代、メール配送は中継によって成り立っていた。上流のサイトは善意でバケツリレーのようにメールを運んでくれたものである。よもやメールの中継そのものがスパム配送の温床になることを誰が想像しただろうか。しかし、善意に基づいて作られたシステムは悪用する者が現れると壊れる。スパム対策はメール配送設定の一部として不正中継防止策という形でスタートした。初期のスパム対策は、発信者のメールアドレスのドメイン部分によって中継の可否を判定するというものであった。考えるに自分のメールアドレスが流通しているからこそこれだけの数のスパムが届くのだが、いまどきワームまでもが検索エンジンを使ってメールアドレスを探す時代である。便利になる反面、悪用される度合いも増しているといえる。

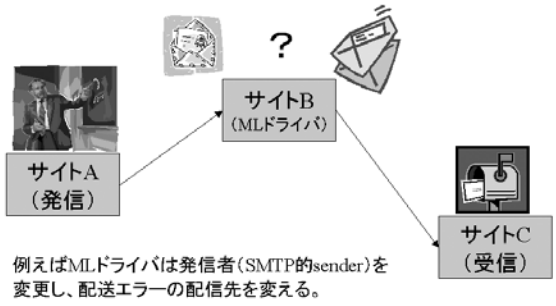


2. なりすまし

メール送受信の基本的な枠組は通信手順（RFC2821）と送信されるメッセージの形式（RFC2822）で規定されている。当初そこには発信者の認証という概念はなかった。極論すれば仕組みさえ知っていれば誰でも誰にでもなりすますことが可能であった。この便利ななりすましの枠組は現在においてもメーリングリストのアドレス展開や、メール転送（aliases）な

どでほぼ日常的に使われている。善意に基づいて作られたシステムゆえにこうなっているが、スパマー(SPAMer)は初期の不正中継対策をかいくぐるために、まずこのなりすましを利用し始めた。ISPではこれに対応して、認証方式としてはいささか邪道ではあるが、他のプロトコルであるPOPのユーザ認証を以てSMTPの認証のかわりをさせ、一定時間そのIPアドレスからのメール発信を許可する「POP before SMTP」という対策をとることになる。

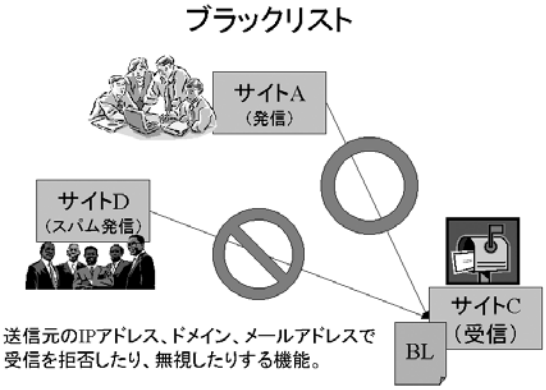
なりすまし



3. ブラックリスト

送信者のメールアドレスが詐称可能であるという事実は、送信者のメールアドレスだけに基づいた一切の不正中継対策が不完全であることを意味する。ここに至って不正中継の防止は発信サイトのIPアドレスに基づいてルールが書かれるようになった。同時に、確信犯でスパムを配信してくるサイトに対して発信サイトのIPアドレス、ドメイン、発信メールアドレスのいずれかを指定してピンポイントで配信を止める仕組みが登場する。これがブラックリストである。

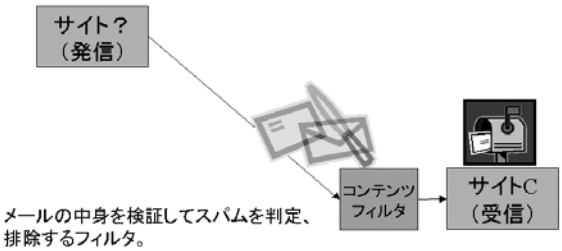
ブラックリスト



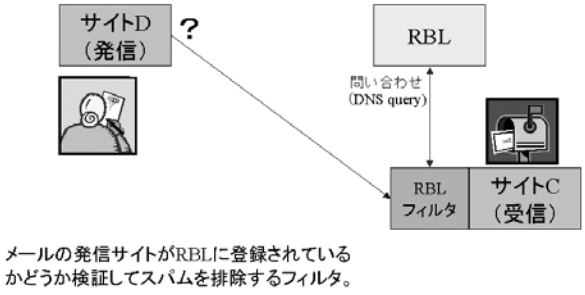
4. コンテンツフィルタとRBL (リアルタイムブラックホールリスト)

ブラックリストが普及すると、やがてスパムの発信サイトは次々に新しいアドレスを利用するようになる。その目的はブラックリストに載っていないアドレスからメールを送信することにある。その結果ブラックリストのメンテナンスコストが増大し、スパム対策は大きく2つの系統に分かれることになる。1つは送信サイトのIPアドレスには依存せず、メールの文面からスパムかどうかを判定するコンテンツフィルタのアプローチ、もうひとつは、ブラックリストを共有することでメンテナンスコストを下げるRBLのアプローチである。当初のコンテンツフィルタは単純なパターンマッチを基本としていたが、やがて正規表現が使えるようになった。しかし、スパマーはわざと単語のスペルミスをしたり、適当に「＊」をまぶしたり、HTMLのコメントを単語の途中に入れたり、ありとあらゆる手法で文面のバリエーションを増やしていくことになる。一方、RBLに待っていたのはブラックリスト情報の授受の通信そのものを妨害するサーバへのDoSであった。この頃からスパム送信へのすさまじい執念があちこちで感じられるようになる。

コンテンツフィルタ



RBLによるフィルタリング



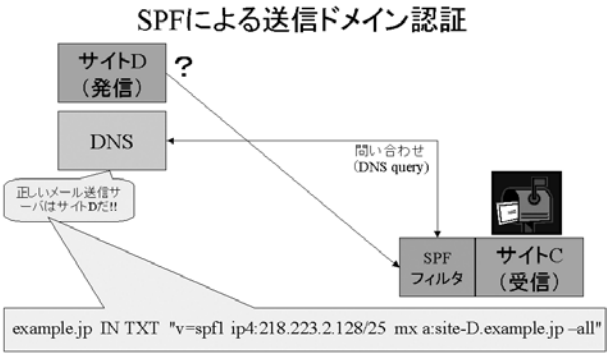
5. ベイジアンフィルタ

もともとは、文面に現れる単語の出現傾向から自然言語で書かれた文章を「区分け」する研究が行なわれていた学習型のフィルタ技術である。この技術が一斉にスパム対策に応用されたのは、Paul Grahamの「A Plan for Spam」という文章に触発されたからとされている。メールをスパムとハム（スパムでないメール）に区分けするため、単一のメールボックスしか持たないPOP（Post Office Protocol）との整合性が悪く、今まではMUA※やPOPサーバとMUAの間に入るPOP proxyの形で実装されてきた。各個人によって迷惑メールの定義が微妙に異なることもMUAへの実装が進んだ原因のひとつであろう。言うまでもなく学習型のベイジアンフィルタが登場した背景には、スパマーによる文面バリエーションの増大によりパターンマッチルールのメンテナンスコストが増大した事実がある。ベイジアンフィルタは辞書ベースであるため性能に言語依存性が存在する。不幸なことに最も知られた応用がスパム対策になってはいるが、メールを文面で仕分けする仕組みとして複数のメールフォルダを扱えるMUAかIMAPサーバで利用できるようになれば、それはそれで素晴らしい技術の応用になると言えるだろう。

6. 偽装単語列と人間の誤り訂正能力

ベイジアンフィルタは単語ベースのフィルタである。とすれば、当然スパマーは単語の出現傾向を変えてこのフィルタを突破しようとする。そこで登場してくるのが単語をランダムに並べたものや、全然関係のない文書をメールに混入するという手法である。その後の研究によりベイジアンフィルタで学習を続けると、辞書中にフィルタとして弱点となる単語が出てくることがわかっている。そのため、学習済の辞書を搭載して学習させない実装や、辞書に掲載される単語数を一定に限定する実装が出てきた。だが、困ったことに人間の誤り訂正能力はベイジアンフィルタをはるかに超越しており、例えば「V=i=a=g=r=a」のように「Viagra」と読める綴り方だけで60強通りもバリエーションがあるとする報告がある。これらをすべて辞書に持つのは現実的ではない。このバリエーションを吸収するため、辞書に正規表現のパターンを持たせたベイジアンフィルタを考えている向きもあるようだ。きっと今度は学習するうちに弱点となる正規表現のパターンが出てきて、そこを突く方策をスパマーが打ってくるという展開が待っているのだろう。コンテンツフィルタをめぐるスパマーと研究者の闘争は本当に果てしない...。だが、単に研究者とスパマーがベイジアンの木の下で鬼ごっこをやっているだけのようにも見える。

※MUA：Mail User Agent, いわゆるメーラー



7. 特徴抽出型(ヒューリスティック)フィルタ

簡単に言えば多数の判定アルゴリズムを用いて○×表を作り、○×の出現パターンによってスパムかどうかを判定するシステムである。コンテンツフィルタの一種と言って良いが、多くのシステムで判定項目の構成がブラックボックスになっており、どうやれば引っかからずに済むかを調べるのは非常に困難になっている。スパマーはこれをくぐり抜けるための努力も惜しんでいないので、固定的に判定アルゴリズムを集めただけでは、いつかはくぐり抜けられてしまうであろう。

前章でベイジアンフィルタのはまっている迷路についても書いたが、究極のフィルタは動的に判定項目が変えられるタイプのものになるであろうことが予測できる。アルゴリズムの構成が適度に変動することがスパマーによる解析を事実上不可能にする。実はコンテンツフィルタは本質的にオープンソースには向かず、少なくともプロプライエタリな部分を技術コアに持たないと成立しないのかも知れないと筆者は最近考えている。鬼がフィルタのソースを読んでしまうような鬼ごっこは、フィルタを書く側に圧倒的に不利に思えるがあなたの判断はいかがだろうか？

8. 送信者認証(SMTP AUTH)

一方、スパマーは「POP before SMTP」という陳腐化してしまった障壁をかいくぐる努力も忘れていないようだ。世の中には接続する毎にIPアドレスの変わるインターネット接続サービスがある。ということは、運が良ければ、直前にそのIPアドレスを利用していた人がPOPで認証していて、自分が認証せずともたまたまメールが送信できる状態のIPアドレスが当たるかも知れない。かくして、接続してはSMTPを叩き、接続してはSMTPを叩き、果てしなくIPアドレスを変えまくってスパム送信を試みる輩が出てくる。もはや執念と言って良いだろう。このアタックは送信者の認証がSMTPセッション自体に含まれていないことに根本的な原因がある。そこで、SMTPセッションの中でユーザ認証をする仕組みが考えられた。それがSMTP AUTHである。実は日本はISPレベルでのSMTP AUTHの普及が進んでいる国のひとつである。これはメール系の技術者の見識の高さを裏付ける事実のひとつであろう。次の段階では、認証されているという事実をいかにして送信先に伝えるかという課題が待っているわけだが、せっかく認証がSMTPセッションの中で閉じているのに、いくらでも詐称が可能なメールヘッダに認証結果を残すことが課題の解決にどれだけ貢献するかは不明である。

9. ゾンビPCとbotNET(ゾンビクラスタ)

スパマーは認証の壁をいかに破るか、RBLの壁をいかに破るかを追求してきた。その結果、ほぼ最終兵器ともいえる解答に到達する。現状で世界最大のクラスタリングマシンであろう「botNET」と呼ばれるメール送信用のPCクラスタである。インターネット上にランダムに分布する数十万とも数百万とも言われている数のPCがスパマーの出す指令の通りにスパムを送出するのである。PCはワームに感染することで、ゾンビクラスタの一部(ゾンビPC)となり、スパ

マーの指令を待つのである。ワームはOSやアプリケーションの脆弱性を利用して感染を試みるので、インターネットにマシンを繋ぐならくれぐれも発覚している脆弱性へのケアを忘れてはいけない。スパム受信側から見ると、数百万ものランダムなIPアドレスからスパムが届くという悪夢のような状態になる。結果、発信サイトのIPアドレスベースのスパム対策は実質的に無効化されてしまう。実際、これ以上発信者の隠蔽に適したシステムはない。これがフィッシングと呼ばれる詐欺メールが発生する温床のひとつとなった。

10. フィッシングメール

カード番号や暗証番号の詐取を試みるメール。差出人を詐称し、WWWブラウザの脆弱性を利用してURLをも偽装して偽のサイトへ被害者を誘導する。目的が目的だけに金融機関、カード会社、ショッピングサイト、ISPの名をかたるものが多い。実際に金銭被害が発生する犯罪であるため、各国の消費者保護を担当する役所が対策に乗り出してきており、日本の経済産業省、総務省、警察庁もその例外ではない。少なくとも初動では他の国に負けていないので、被害を最小限に押えることができたなら、彼らの対策は世界的に見て十分に賞賛に値すべきものになる。目下最も対策の緊急度が高いターゲットはこれである。メールサーバの話ではないが、フィッシングの誘導先に使われる偽のWWWサイトの7割以上がapacheだという数字がある。どうもWindowsに限った話ではないようなので、WWWサーバの管理者もサイト上にページをでっち上げられて悪用されないように注意しなければいけない。油断は禁物である。

11. 送信ドメイン認証（SPF,Sender-ID,DomainKeys）

「そのメールが送信者アドレスのドメインの正規のメール送信サーバから送出された」ことを確認するための認証技術。DNSのそのドメインに対応するエントリーにそのドメインの正規のメール送信サーバのIPアドレスを記述したり、正規のメール送信サーバに対応する公開鍵を記述することで、送信されたメールがそのドメインを持つ組織から正当に発信されていることを検証する。送信したユーザ個人を認証する技術はもともとあるが、この用途で個人を特定するのは明らかにオーバースペックなためか、普及してこなかったという背景がある。送信ドメイン認証は簡単に言えば、「この組織から発信されました」という事実を検証する枠組であり、ゾンビクラスタが存在する環境下でも発信者の詐称を著しく困難にする効果があるため、スパム及びフィッシング対策として導入が推奨されるべきものである。例えば、米国の組織が先にこの対策を導入した場合、DNSに対応するエントリーを書いておかないと日本からのメールが受けとってもらえなくなる可能性がある。その前に、最低でもどれか1種類、自社の正規のメール送出サーバの情報をDNSのエントリーとして設定しておきたい。

12. Port 25 blocking

送信ドメイン認証がメールを受信する際の対策とすれば、ポート25ブロッキングは自社のアドレスブロックにあるゾンビPCからのメール送信を遮断するための対策である。ISPの立場でいえば、コンテンツフィルタのようなサーバの高負荷を伴う対策よりはるかに小さな投資額で自分たちのアドレスブロックから発信されるスパムへの苦情に対応する労力を激減させることができるという意味で効果的な対策の1つである。仮にこの対策を怠った場合、後述するレピュテーション(ドメイン信用評価サービス)において、信用度が地に堕ちるリスクも考えられる。ポート25がブロックされた場合、ユーザは他のプロバイダからメールASPを使ってのメール送信ができなくなると考えるかも知れないが、他のプロバイダのメールサーバ

を使ったメール発信には、ポート25以外の通信を利用することで現状の使い勝手を維持することとなろう。例えば、メール発信はポート587(Message submission)を用いれば良いし、さらに、Message submissionをTLSで暗号化したり、SMTP/SSL(ポート465)を使用したりする手もある。心あるISPはこういった回避策をユーザに提供すべく必死に準備をしている。変化は発信と中継を完全に分離する方向に着実に進行している。

13. レピュテーション

あるドメインやIPアドレス、ドメイン保持者やIPアドレスブロックのオーナー情報とスパム発信履歴をもとにそのサイトの「信用度」を算出し提供するサービス。情報の取得手段はRBLに類似しているが、中身は単純なブラックリストではない。ISPが自社のアドレスブロックからのスパム発信を放置した場合、このサービスを利用しているサイトに受信を拒否される可能性が出てくる。モデルは実社会の信用調査と似ており、今後は信用度判定の情報源がどんどん高度化する方向へ進化することによりさらに似てくるものと思われる。

14. むすび

インターネット上に電子メールというメディアができて普及していく際にたどってきた過程は、使い方の自由度と対策の難しさの差こそあれ、他の社会インフラがたどってきた過程とそれほど違ったものではないように思う。この壮大なスケールでの実験はまだ続いており、メールサーバ管理者は否応なくその最前線に立たされていると思って間違いない。メールは依然としてインターネット上で最も利用されているサービスであり、ユーザの母数が多いだけに問題も最初に顕在化するからである。スパムの問題はNetnewsはもとより、今やブログのトラックバックにまで広がっており、あらゆるテキストを利用する通信サービスがその被害にあっている。問題はメールだけに留まらず、今後もユーザの多い順に次々と顕在化していくことが予想される。ユーザ側も、いつも使えているからといって、たかがメールとは思ってはいけないのだ。サーバ管理者の方は現状では高いスキルと低い労働単価を要求されているかも知れないが、気概を持って対策を検討されたい。メールサーバが機能を停止すると会社の機能がほぼまるごと停止するという事象はいまどき珍しいことではない。これは管理職もシステム管理者も必ず一度は考えておくべきリスクである。

送信者認証(SMTP AUTH)と送信ドメイン認証(SPF,DomainKeys等)は全く異なる技術であるが、あまり他の方の講演を聞く機会のない私でさえ、この2つを混同した講演に遭遇したことがある。300名近い参加者が間違った知識を持ったまま家路につくというのは痛恨の極みであり、本稿を書く動機としては十分なものであった。日本にインターネットが上陸して20年、私が初めてネットワークにIP接続されているマシンに触ってからもう17年ほどになる。ユーザの裾野は桁違いに広がり、メールなんざ誰でも使っているという時代になりつつあるが、昔も今も正しい知識の必要性は何ら変わっておらず、次の議論をするには以前の経緯を正確にふまえておくべきである。本稿がそのための何らかの助けになれば幸いである。

サーバハードニング（強化）の重要性

株式会社エス・アイ・ディ・シー
代表取締役　里吉　昌博

「情報セキュリティ」は、数年前はコンピュータおたくが、日の当たらない場所で取り交わす会話に出てくる程度でした。それが徐々に局面が広がり、今ではネットワーク世界でビジネスを行う上で必要不可欠なものと言われるまでになってきました。

企業は通常、ファイアウォールやウィルス対策ソフト、またセキュリティポリシーなどのソリューションを組み合わせて、自社のセキュリティ問題に対応しています。しかし、ポリシーや技術的に強固なファイアウォールを適切に実装することが、優れたセキュリティインフラ（基盤）を形成するベースとなるものですが、その一方で、BlasterやSoBigなどのワームによって引き起こされた最近のセキュリティインシデント（事故）により、ファイアウォールやポリシーだけでは、その手の攻撃から企業ネットワークを守れないことが浮き彫りになりました。

かつては、情報セキュリティを説明するのに「城」の例えが多く用いられておりました。中世の城のように外壁を強固にすれば、企業は安全だと教えられたものです。

しかし何度となく、それは間違いであることが明らかにされてきました。

本当に安全な環境にするためには、城内の各所にまた城を築き、それぞれが自分自身とお互いを攻撃から守るような仕組みになっていなければならないのです。

このように、セキュリティがいくつもの「層」のように配置され、その各層が中心部分を守る役目を担う構造を説明するために、最近では、「城」ではなく、「玉ねぎ」が最も適切な例えとして用いられるようになりました。まだ日本では馴染みが深くありませんが、セキュリティ先進国である北米においては、レイヤー化されたセキュリティアプローチを説明するのに、よく用いられております。

こうして、ホストベースのセキュリティとサーバ・ハードニングが脚光を浴びることになりました。サーバ・ハードニングとは、ビジネス要件を満たしながらも、サーバのセキュリティをより堅牢にする設定を行うことです。ほとんどのOSは、利用条件に対応した適切なアクセス制御などの設定が行われることが想定されており、デフォルト設定のままでは安全性に問題がある場合が多くあります。

本稿では初期設定のWindows 2000 Serverを例として、一般に広く見受けられる脆弱性と、サーバをハードニング（強化）してそれらの脆弱性に対処する方法について述べます。しかし本稿では、発生する可能性のある脆弱性のすべて網羅するわけではなく、代表的な例を取り上げて、それらを解消する方法を示すことに重点を置くことにします。

■ 攻撃のシナリオ

システム：Windows 2000 Server、Active Directory（AD）を使用
攻 撃 者：組織内のLAN上に存在する

これは最も一般的なシナリオで、悪意のある第三者が最も攻撃を行いやすいシナリオでもあります。攻撃者は、Windows 2000 ServerのCDに収められている一般的なリソースキットツールやサポートツールなどを悪用して、システムに関する非常に有用な情報を取得することが可能になります。

例えば、すべてのWindows 2000のCDに付属するサポートツールの「LDP」を使えば、ADオブジェクトを、LDAPを用いて一覧表示することができます。リソースキットに含まれている「Gettype」を使うと、攻撃者はリモートのWindows Serverのバージョンと種類を正確に特定できます。また同じく「ENUMPROP」を使うと、リモートのAD Serverをコマンドラインから一覧表示することが可能です。

攻撃の前にシステム情報を見ることができるという

のは、悪意のある第三者がターゲットを絞った攻撃を実行するための十分な情報を収集するのに最良の方法であり、そのおかげで攻撃が成功する確率も高くなり、不審なログファイルやアラートの発生を抑えることができます。

上に挙げた3つのツールを使用すれば、攻撃者は次のような情報を手にすることができます。

・ システム名
・ ドメイン名
・ ユーザリスト
・ 最終ログイン時間などのアカウント情報
・ オープン共有
・ 使用されている認証機能の種類　など。

さらに攻撃者は、単純なポートスキャンを行うことでも、貴重な情報を入手できます。この場合攻撃者は「Nmap」のようなツールを用いて、システム上で稼動しているサービスをすべて明らかにすることができます。

Windows 2000 Serverの初期設定では、次のようなサービスがデフォルトで提供されています。

```
# nmap 3.48 scan initiated Fri Jun 25 04:21:10 2004 as: nmap -sV 192.168.1.116
Interesting ports on 192.168.1.116:
(The 1633 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd 5.0
25/tcp   open  smtp         Microsoft ESMTP 5.0.2195.6713
53/tcp    open  domain     Microsoft DNS
80/tcp   open  http         Microsoft IIS webserver 5.0
88/tcp   open  kerberos-sec Microsoft Windows kerberos-sec
119/tcp  open  nntp?
135/tcp  open  msrpc        Microsoft Windows msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap         Microsoft LDAP server
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
464/tcp  open  kpasswd5?
1026/tcp open  msrpc        Microsoft Windows msrpc
1029/tcp open  ncacn_http   ncacn_http 1.0
1083/tcp open  mstask       Microsoft mstask (task server - c:winntsystem32Mstask.exe)
3372/tcp open  msdtc?
3389/tcp open  ms-term-serv?
```

■ 攻撃ベクトル

Windows 2000 Serverのようなシステムを首尾よく攻撃する方法は数多くありますが、ここではその一部を取り上げることにします。

• Kerberos攻撃 – システムでKerberos認証サービスが動作している場合、攻撃者はKerberos用ポート（TCP 88番）をトラフィックで溢れさせて、Kerberosサーバを使用不能にすることができます。これによりクライアントは、傍受やクラッキングが容易なSMB認証を使わざるを得なくなります。

• SMBによるパスワードの解読 – 初期設定のシステムでは、anonymous（匿名）ネットワーク接続が可

能で、これをブルートフォース（総当り）攻撃に使用することができるようになっています。システム情報列挙などによって集めた情報をもとに、攻撃者は特定のアカウントに照準を合わせることができ、さらにはパスワードポリシーを把握して、その要件を満たしていないアカウントに的を絞ることも可能です。

- RPC/DCOMの脆弱性－検索エンジンでインターネットを検索すると、リモートプロシージャコール（RPC）やDCOMの悪用に関するコンセプト証明用のツールが多数見つかります。RPCやDCOMは初期設定システム上で有効になっており、攻撃者はこれらを悪用して、管理者権利でコマンドを実行することが可能です。
- IIS－MicrosoftのIIS Web ServerとFTP Serverにはどちらも、RPC/DCOMの脆弱性によく似た、リモートからのシステムの不正使用につながる既知の脆弱性が存在します。これによって攻撃者は、リモートから管理者機能を使うことが可能になります。

上に挙げた攻撃に成功すると、悪意のある第三者はシステム上のあらゆるデータの閲覧、コピー、消去、改変が容易にできるようになり、場合によっては、そのシステムを踏み台にして他のシステムへの攻撃を実行することができます。このようなケースでは、攻撃者が追跡の手を逃れる可能性が通常より高くなります。

■ 防御のシナリオ

お気付きの通り、こうした攻撃のほとんどは、実質的な防御策としてファイアウォールだけしか設置していない企業が大半を占めている状況では、悪意のある第三者が企業LANの外部にいても有効に行うことが可能です。

またこれらのサービスがインターネット上で利用可能になっていれば、攻撃の対象とされる危険性があります。

事実、RPC/DCOMの脆弱性やIIS脆弱性は、Blaster、Code Red、Nimdaのような大量メール送信型ワームによる攻撃で悪用されてきました。

これらの攻撃に対処するポイントは、単にこれらのシステムを無効にしたり、ファイアウォールで阻止したりすることではありません。実際に、設計に工夫を凝らして安全性を高めたアーキテクチャすべてが、可用性が高く有効に業務が行えるものになっているわけではありません。

こうした攻撃のほとんどは、サーバ・ハードニングやホストベースのセキュリティ措置によって防ぐことができるのです。

最も単純なレベルのサーバ・ハードニングは、最低限のアクセスポリシーに従ったものです。サービス、機能、アクセスポイントなどで必要のないものは提供を停止するか、最低限、利用を制限する必要があります。

例えば、一覧表示のタスクの実行をほぼ不可能にするには、管理者はシステムへのanonymous接続ができないように設定するだけでいいのです。これにより、適正な信用証明を持たない者は、システム情報の一覧表示ができなくなります。

これを行うには、次のレジストリキーにレジストリ値（RestrictAnonymous）以下を追加することです：

システムキー：
　[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlLSA]
レジストリ値：
　RestrictAnonymous
データの種類：
　REG_DWORD (DWORD値)

値のデータ：
（0 = 許可, 1 = 許可しない, 2 = 匿名アクセス許可が必要）

使用しないサービスを無効にすることで、攻撃者がそれらのサービスの脆弱性を悪用するのを防ぐことができます。必要とされるサービスに関しては、攻撃に対するシステムの抵抗力を増すための詳細な設定が数多く用意されております。

また、ファイル、ディレクトリ、レジストリなどのパーミッションを変更するのも、自動化された攻撃を防ぐのに非常に有効な方法です。例えば、ワームやトロイの木馬の多くは、レジストリキーの「Run Once」（一度だけ実行）セクションに書き込みを行おうとします。これらのキーを書き込み不可にするだけで、この攻撃ベクトルを悪用する悪質コードが機能するのを阻止することが可能です。

パーミッションやコマンドプロンプト（cmd.exe）の位置を変更すれば、Code RedやCode Redに似た手動の（Unicode脆弱性の悪用）攻撃などを無効にできます。

また、組み込みTFTPクライアントを用いて、脆弱なシステムにファイルを転送したり、システムからファイルを転送する攻撃もよく行なわれます。この攻撃の発生を防止するには、「tftp.exe」のパーミッションを制限するか、場合によってはtftp.exeそのものを削除すれば解決します。

■サーバ・ハードニングに伴う問題点

サーバ・ハードニングに伴う実質的な問題点として、適用可能な設定が文字通り数百通りも存在することが挙げられます。これらの設定の中には、アプリケーションやその機能を実行できるかどうかに影響を及ぼすものもあれば、及ぼさないものもあります。

中には、ネットワーク全体に深刻な影響を及ぼす可能性があるものもあります。システムにいかなる変更を加える場合も、実装する前に、実際の本番システムではないシステムで、それぞれの設定を徹底的にテストしておくことをお勧めします。

OS内部の仕組みを完全に理解していない経験の浅いシステム管理者なら普通は、こうした問題の発生を危惧して、システムの強化には手を出さないことが多いのも事実です。

サーバ・ハードニングのリサーチ、テスト、実装には、熟練した外部の支援がなければコストがかさむ恐れもあります。しかし長い目で見て、システムのセキュリティ、信頼性、パフォーマンスの向上につながれば、実行する価値のある投資と言えるでしょう。

こうした問題に対応し、OSのセキュリティ設定を自動的にハードニング（強化）するツールを弊社でも開発しました。http://www.security-sensei.com/をご参照いただければ幸いです。

JNSA ワーキンググループ紹介

暗号モジュール評価基準 WG

暗号モジュール評価基準WGリーダー　　執筆者
株式会社シーフォーテクノロジー　小川　博久　　萩原 雄一

■ はじめに

ネットワークが身近になった現在では、安全な通信が必須となり、あらゆる場面で暗号が利用されています。しかしながら、暗号は実装を誤ると安全性を向上することになりません。

本WGでは、これらの暗号の実装に伴う評価や基準について議論、検討し、ベンダーが正しく理解することを目標とし発足しました。また、セキュアなネットワークの実現には、暗号の正しい評価や、実装が必要であり、利用者や、設計開発者など、暗号製品に関わる現場の担当者の知識を深めることも目的としています。

■ 活動目的

本WGでは「正しく」暗号を使用することに注目し、現存する規格・制度の他に今まさに日本で制定されようとしている規格・制度について議論し、提言を行うことを目的の一つとしています。

- 現存する規格・制度とは現在米国およびカナダで採用されている暗号モジュールのセキュリティ要件であるFIPS 140-2およびその評価制度CMVPを指します。本WGでは、この規格や制度について議論し、理解を深めることを目的にしています。必要があれば、積極的に提言などを行うことも視野に入れ活動します。
- 国際的な動向としてはFIPS 140-2ベースのISO 19790が2005年中に制定されることが予想されています。本WGでは、これらの国際的な動向を把握し、利用者や設計開発者が知識を深めることを目的としています。
- 日本でもCRYPTRECにて電子政府での使用が推奨される暗号が制定され、現在どの様にそれらの暗号を実装すればよいかが議論されています。最近では、独立行政法人 情報処理推進機構から、暗号モジュール評価制度に対する移行措置の提案も行われました。本WGでは、これらの日本の検討についても動向を把握し、ベンダーとしての取組み方を議論することを目的としています。

■ 今後の予定

昨年の11月に発足し、暗号実装と正しさと、評価や基準の重要性の理解を促す活動として、アットマーク・アイティ社に『暗号モジュール評価の基礎知識』を執筆しました。

また、昨年12月14日に、『暗号モジュール評価基準カンファレンス』を行い、国内外の暗号モジュールを取巻く動向について議論し、公開WGを開催しました。

今後、本WGでは、さらにCC（ISO / IEC 15408）とFIPS 140-2の関連性についても議論します。メンバー加入は随時受付けていますので、ご興味ある方は、是非、ご連絡ください。

■ WGメンバー

リーダー：小川　博久　（シーフォーテクノロジー）
オブザーバー：Travis Spann（InfoGard Laboratories）
メンバー：佐藤　能行　（みずほ情報総研）
　　杉本　浩一　（セコムトラストネット）
　　武部　達明　（横河電機）
　　中川路　哲男（三菱電機）
　　萩原　雄一　（シーフォーテクノロジー）

2004年12月14日『暗号モジュール評価基準カンファレンス』風景

脆弱性定量化に向けての検討WG

脆弱性定量化に向けての検討WGリーダー
京セラコミュニケーションシステム株式会社　郷間　佳市郎

■ はじめに

最近では「脆弱性」という言葉が、ずいぶんと一般的に通用するようになってきていますが、一昔前は「きじゃくせい」などと読まれたりと、あまりあちこちで通用する言葉ではなかったと記憶しています。今でも、読み間違えないようにと「ぜい弱性」と記述したり、あえて「欠陥」や「弱点」といった他の言葉に置き換えてしまう場合もあるようですが、さすがに「きじゃくせい」と読む方も減り、一般的な用語として浸透してきているように感じます。しかし、言葉は浸透してきたものの、では、個々の脆弱性がどれだけ危険なのかといった本質的な意味については、これを説明しようとすると、かなりの困難が伴います。立場や環境によって捉え方や理解度がまちまちであり、説明に苦労したり、場合によっては相手に誤解を与えてしまう場合も少なくありません。自分ではわかったつもりでも、いざ、自分の上司や他の部署の人に伝えようとしたら一苦労したという経験のある方も多いと思います。個々の脆弱性の説明でさえ難しいわけですから、では、あるサーバに複数の脆弱性が存在する場合に全体としても危険度はどうでしょうといった判断や、異なる脆弱性を複数持ったサーバ同士を比べて、どのサーバから最初に対処をはじめるべきかといった優先順位を判断をしようとした場合には、さらに困ってしまうわけです。

■ 活動目的と内容

どのようにしたら、脆弱性についてわかりやすくなるか。それに対する答えのひとつが定量化（数値化）です。定量化によって、個々の比較はもちろん、定量化によって求められた数値を統計計算することによって、その性質や相関関係も明らかにできる可能性があります。もしかしたら、その結果をトリガーにしてセキュリティ対処を自動化するといったことも、あながち夢物語とは言えないのではないかと思っています。

このように、脆弱性の複雑さに関する問題を解決できないかという意識から、本ＷＧがスタートしました。定量化できないのか、できるのか、もし定量化できるとしたら、それは脆弱性の何なのかといったことから議論がはじまったわけです。また、ベンダーとしては、とにかくパッチを提供したら、関係するすべてのサーバに適用してもらいたいと思っていますが、実はシステムの現場では、できればパッチはあてたくないのだという実情も、参加者の議論の中からあらためて明らかになってきました。実際にシステムの現場に携わっている参加者も多いことから、セキュリティ製品のベンダーとしての立場の方だけでなく、システムの運用を維持するという立場からの発言が多いことも特徴です。

異なる立場から脆弱性とその脅威、そしてその運

用についてと、議論が幅広く広がり、収拾できなくなる場面もありますが、これまで、脆弱性というキーワードで、このように多様な立場の人が定期的に会合を開くということは、あまり行われてこなかったのではないかと思っており、WGとしての存在意義を強く感じています。

■ 今後の予定

最終的には、自分たちで納得のいく定量化のアプローチを見つけたいということが目標です。

米国では、ネットワーク製品ベンダーやアンチウイルスベンダーの一部が中心になって、脆弱性の定量化の取組みが行われています。先日、米国において開催されたRSAカンファレンスでも発表があり、日本でも報じられたことから、すでにご存知の方も多いかもしれません。もちろん本WGの中でも、米国での取組みに対する勉強を行いました。自分たちの目指しているものと比べてどうなのか、実際それが利用できるのか、できないのかといったことにも踏み込んで、WGの場で意見交換を行っています。

■ WGメンバー

リーダー：郷間　佳市郎
（京セラコミュニケーションシステム）

メンバー：鹿児島　健　（インフォセック）
小野　泰司　（インフォセック）
北島　健治　（エス·アンド·アイ）
中嶋　一樹　（住商エレクトロニクス）
金岡　晃　（セコム）
坂本　慶　（ディアイティ）
松井　康宏　（日本アイ·ビー·エム）
宮永　直樹　（日本電気）
世良田　照治（日本電気）
奥原　雅之　（富士通）
長谷川　喜也（富士通）
伊藤　良孝
（三井物産セキュアディレクション）
横山　哲也　（横河電機）
岩井　博樹　（ラック）

CISSP-WG

CISSP WGリーダー
NTTコミュニケーションズ株式会社　大河内　智秀

■ はじめに

(ISC)^2(※1)が提供しているITセキュリティプロフェッショナル認定資格『CISSP』(※2)は、幅広いドメインに渡った試験内容で既にグローバルで実績があり、試験問題の日本語化に伴い、日本特有のドメインの新規策定などが望まれていました。このような要望に対し、検討母体となるべく2004年8月26日に(ISC)^{2}とJNSAがMOUを締結しました。その内容は次のようなものです。

(1) 世界中のCISSPによって更新されている試験問題を、日本在住のCISSPも作成し、(ISC)^{2}に提案すること。
(2) グローバル共通知識であるCISSPに加え、日本特有のドメインを追加した資格試験ISSJPN(仮称)を作成すること。

以上の2点についてJNSAが中心になって検討してゆくことになりました。

今後は、(1)は(2)の作業を優先させるため一時保留とし、(2)についての中間報告書を2005年3月末に(ISC)^{2}に対して提出するよう作業を行う予定です。また、9月末までに検討結果及びそれ以降の方向性を提出することにしています。

■ JNSAでのCISSP-WGの活動について

前記の動きを受け、CISSP-WG発足に向けて、教育部会として2004年9月27日に第1回CISSP-WG発足準備会を開催しました。これまでに18名が集まり、2005年3月までに計5回の会合を実施しました。また、2月24日の教育部会、3月2日の幹事会において、4月からCISSP-WGとして正式に活動することが承認されました。

ISSJPN策定にあたり、現メンバーに加えて総務省などからも数名のオブザーバーに参加頂き、9月末を目処に受験対象者の検討及び対象者に必要と思われる知識ドメインの検討を行う予定です。検討内容としては、例えば、自治体職員、ベンダー側の各案件責任者向けに日本の法律、倫理、通信、BCP、等々が考えられます。

■ GISSP-WGメンバー募集

ISSJPNを策定するにあたり、CISSP-WGのメンバーを募集していますが、このWGは参加条件を設定しています。ISSJPNは、グローバル共通知識を持つCISSP「＋α」の資格として位置づける為、CISSP取得者もしくは、既にCISSP/CBK10ドメインの内容を十分理解されている方の参加を希望しています。「＋α」は、日本特有の知識部分をイメージしています。

尚、このWGは、CISSP合格を目指す為の勉強会ではないことをご理解の上ご参加を頂けるようお願いいたします。また、このWGに参加頂くことにより、CISSP継続維持教育であるCPEクレジットが自動申請にて蓄積できます。

尚、WG活動に関する説明会を5月19日(木)、17時30分から開催予定です。説明会詳細およびWGに参加ご希望の方は、JNSA事務局までご連絡ください。


「CISSP-WG準備会活動」

(※1)(※2)の詳細については、https://www.isc2.org/japanを参照してください。

セミナーレポート

第61回IETFミーティング報告

富士ゼロックス株式会社　稲田　龍
セコム株式会社 IS研究所　島岡　政基
NPO 日本ネットワークセキュリティ協会　安田　直義

11月7日より12日まで米国ワシントンD.C. Hilton Washingtonにて開催された第61回IETF（http://www.ietf.org/）ミーティングに参加したので報告をする。

IETFは、インターネット上のプロトコルの標準化を行っている団体であり、8つのエリアで活動を行っている。通常は、8つのエリア上のWGで電子メールでの議論を行い、標準化を行っているが、年に3回（通常は米国内2回＋米国外1回）のペースでいわゆる「オフライン」の会合を行っている。

今回のミーティングは、26カ国、1314人の参加者があった。米国内でのミーティングであり、必要な人間が必要なタイミングで参加することが定着したためか、全体に出席者は減少している。

今回のミーティングの参加目的は

1. セコムトラストネット島岡氏のMulti-Domain PKI I-Dの共著者であるNIST Nelson E. Hasting氏（nelson.hasting@ nist.gov 以下Hasting氏と表記する）との打ち合わせ
2. IPA/JNSAで行う証明書のUTF8化に関してVPN Consortium Paul Hoffman氏（paul.hoffman@vpnc.org 以下Hoffman氏と表記する）/ PKIX Co-chairであるNIST Tim Polk氏（wpolk@nist.gov）と意見調整および協力の要請
3. PKI関係のWGの状況把握（LTANS/PKI4IPSEC/OPSEC/EASYCERT等）

の3点である。

写真1　会場となったHilton Washington

報告内容要約

1. Multi Domain PKIに関して
   セコム株式会社 島岡 政基氏によるI-D “Memorandum for multi-domain Public Key Infrastructure（PKI）Interoperability”に関して、NIST Hasting氏と意識あわせと、この後の方向性に関して合意を得た。
2. 「UTF8String問題」に関して
   証明書の国際化を行うためのI-DとしてUTF8Stringを扱うI-Dの共同著者であるVPN Consortium Hoffman氏（もう一人の著者であるOASIS PKI TC Chair Steve Hanna氏はIETFに参加していない）に対して、JNSAがIPAより請け負った調査業務の概要と今後のスケジュールおよび現時点での方向性を説明し、合意に至った。
3. セキュリティエリアの各WG（主にPKI関連）の動向を把握することができた。

概　要

Multi-Domain PKI I-D

Hasting氏との打ち合わせは、11/9の11:30より13:30に昼食をとりつつ行った。

Hasting氏は、NISTのInformation Technology LaboratoryのComputer Security Divisionに属するエンジニアであり、PKIX-WGのCo-ChairであるTim Polk氏の同僚にあたる。

島岡氏は、今年の10月にIPAセキュリティセンター宮川氏とNISTに出張し、Hasting氏に島岡氏が作成しているMulti-Domain PKIのI-Dの共著者になることを要請し、快諾されている。今回のIETFの前に島岡氏はHasting氏にI-Dを送付しており、70近くのコメントをもらい、そのコメントを元に新たなI-Dの方針、意識あわせおよび改版したI-Dのスケジュールの調整を行った。

写真２　Nelson E. Hasting氏との打ち合わせの風景
(左より富士ゼロックス 稲田、セコムIS研究所 島岡氏、
IPAセキュリティセンター 宮川氏、NIST Hasting氏)

Nelson氏は、Multi-Domain PKI/Single Domain PKIの用語の定義の明確化とTrust Anchorについての扱いを気にしており島岡氏との間で意見の調整を行った。

証明書のUTF8化

証明書のUTF8化に関しての打ち合わせは、VPN Consortium Paul Hoffman氏と11/10の17:00–18:00に行った。

IPA/JNSAのUTF8に関する今後の活動に関して事前にHoffman氏にはメールを送ってあり、そのメールの内容と今後の展開に関して情報の交換を行った。

Hoffman氏は、証明書におけるString Matchingに関してのI-DをOASIS PKI TC Steve　Hanna氏と記述しており、第60回のときにもこちらの現状を伝えてある。

今回は、IPAの公募に採択されたことにより具体的な活動計画とスケジュールの提示が出来た。JNSAが行う調査案件において2月にIPAに対しての報告書の提出と、それをベースにしたI-Dを書くという話をしたところ、Hoffman氏が記述しているI-Dとの併合を提案された。JNSA側で作成予定のI-Dは、UTF8による証明書発行によりおきうる問題点の提示と認証局に対してUTF8による証明書を発行する際のガイドラインとなる予定であるが、Hoffman氏の意見によると、JNSAが作るI-Dはサンプルを提供する側面が強く、Hoffman氏のI-Dはプロトコルを提示するI-Dになるはずであるとのことである。Hoffman氏は、JNSAのI-DとHoffman氏のI-Dを併合することにより、よりわかりやすく説得力のあるI-Dとなるはずであると主張している。Hoffman氏のI-Dは、12月に第2版(01)が発行される予定であるとのことである。
Hoffman氏の提案に関して即答は避けたが、最低でも互いに参照しあうこと、状況を交換し続けることは意見の一致を見た。

また、SAAG後にHoffman氏より、String Match I-DがSon of RFC 3280(後述)の一部として併合されたことが知らされ、急遽、Son of RFC 3280に対してIPA/JNSAとして活動を起こすことが必要となり、Issueリストとして認識されるように調整を行った(PKIXのセクションを参照のこと)。

写真３　Paul Hoffman氏との打ち合わせ風景


写真４　Paul Hoffman氏との打ち合わせの後
(左より富士ゼロックス 稲田、Paul Hoffman氏、
IPAセキュリティセンター 宮川氏、セコムIS研究所 島岡氏)

PKI関係のWG

LTANS

11/9 9:00–11:30に開催された。出席者は20人程度で低調。裏にBetter-Than-Nothing Security BoFが開催されたためそちらに人気が集中したためと考えられる。
Document Statusの確認を行われた。各ドキュメントのステータスは以下のとおり。

1. Long-term archive service requirementsはまだまだかかりそう
2. Notary requirements Data certificationにフォーカスをあてて作成中
3. ERS（Evidence Record Syntax）
   I-Dとしてほぼ完成しているが、Long-term archiveからのコメントにより調整が必要

Long-termのI-Dは10月に発行された。今後の予定として次回のMinneapolisミーティングまでに1つ以上のバージョンを発行する予定。

現行のLong-termのI-Dにおける問題点として以下のものがあがっている。

1. メカニズムをより中立化する
   暗号・PKI機能をどうするべきか
2. ERSで行うべきことをLong-termでしていないか?
3. ワークフローの定義
   マルチステージでの承認行為は必要なのか?
   →必要である
   ERSでこの要件をサポートする機能を入れるべきである→ERSのI-Dへコメント
4. ポリシー要件の確立と強化が必要
5. その他もろもろ

以上の問題点を議論し、以下のことが決定された。

1. Minneapolis（次回IETF）前にLast Callしたい
2. ERSとの連携
3. WebDAVとの連携の準備
4. DVCSのようなプロトコルの開発が必要

Better than Nothing BoF

11/9 09:00–11:30に開催された。盛況で200名ほどの出席者があった。

IETFにおいて、新規の標準化を行う際は、まず、BoF（Bird of a Feather）を行い、Charterを作り賛同者を集める。BoFを3回行い賛同者が集まらない場合には、その標準化はIETFでは行わない仕組みになっており、今回のBetter than Nothingは、初めてのBoFである。

Chairは Joe Touch <touch@isi.edu>である。

現行のIPsecプロトコルでは、セキュリティに関する設定はall or nothingという選択となっており、IPsecプロトコルは可能性のある脅威に対して広範な防護を行う仕組みを提供しているが使われていない場合がままある。

理由として以下にあげるものがある。

1. 鍵管理基盤が必要
2. 設定の煩雑さ
3. 性能への悪影響等

今回のBoFでは既存のIPsecプロトコルに対して、事前の鍵共有(pre-shared secret)や鍵管理基盤の必要性を減らし性能面で悪影響の少ない、セキュリティ要件を緩和した仕様の策定を行うことを提案した。

この仕様では、既存のIPsecプロトコルと比較してセキュリティ粒度は低くなるが限定した環境内での利用に関しては十分であるとしている(例：Man in the Middle Attack以外の経路外からの攻撃に対する防護は提供可能。通信相手の身元について、裏書きする仕掛けは無いがコネクションそのものは防護可能)。

BCPもしくは、標準化プロトコル仕様として、標準化活動をしたいとのこと。BGPやDNSと併せて利用したいという。

写真5　超満員のBTN-BoF会場

SecSH

11/9の1415–1515に開催された。出席者は150名ほど。SecSH WGは、幾つかのI-Dを提出しているがここ1年、1回もミーティングを行っておらずI-Dも手を入れられない状況になっている。すでにOpenSSHはシステム管理者が利用するリモートアクセスソフトウェアとしてはデファクトスタンダードであり、標準化を推進することが必要である。今回、新たに新著者としてBill Sommerfeld <sommerfeld@sun.com>氏が名乗りを上げ、チェア代理として「標準化を進めるにどうするべきか」に関して議論を行った。

核となるCore I-Dに関してはIESGからのコメントもあり、それらの各コメントに関して議論および今後の方向性を定めた。他にも複数の関連I-Dがあるがこれらの改定は行わないこととなった。

OpSec

11/9 15:45–16 45に開催された。150人ほどが参加し盛況であった。

Operational Security Capabilities for IP Network Infrastructure（opsec）はSan Diegoで開催された第60回IETFで行われたBoFであったが、今回は正規のWGとして活動が開始された。

前回よりCharterが制定され主にISP/Enterpriseレベルのネットワークに対してのBest Current Practiceを提供するようこととなった。

今後、全体のフレームワークに関する文書、BCP、個々のデバイスに関する文書をISP向け/エンタープライズ向けに作成することとなった。

pki4ipsec

11/10 09:00–11:30に開催された。150人ほどの参加者がおり盛況であった。

Chair Paul Knight <paul.knight@nortelnetworks.com>, Gregory Lebovitz <gregory-ietf@earthlink.net>

写真 6　pki4ipsec-WGの会場風景

IPsecにおいてPKIの利用を行うためのプロファイルを策定するためのWG。IPsecは、5年以上前に標準化されたものであり、X.509電子証明書の利用も仕様に含まれている。しかし、現時点では大半のIPsecを使える機器類は証明書を使っていない。これらの原因として、「X509電子証明書の利用に関しての規定がIPsecでは明確になっていない」もあげられている。また、証明書の取得方式およびその他の証明書の操作（更新、削除など）も具体的な記述がなされていないなどもあげられている。

今回のWGでは、IPsecにおける証明書検証要件に関する議論の中で、証明書の失効検証や中間証明書の（取得および）検証についての是非が議論された。これらの処理には、時間がかかりIPsecのような下位層で通信を維持しつつ行うことは困難が伴うという理由で、多くの実装はこれらの処理に関して手抜きを行っている。

この議論については微妙な表現があり、当初は“allow to verify”とすべきかどうかを議論していたが、途中から“deny to verify”とすべきかどうかの議論へとかわっていった。

1. “allow to verify”
   賛成：verifyをoptionalな実装として認める。
   反対：verifyを明確な要件とはしない。
2. “deny to verify”
   賛成：verifyを実装すると仕様から逸脱することになる。
   反対：verifyを明確な要件とはしない。

今回は“deny to verify”がagreeされたのだが、これは“allow to verify”に対するdisagreeを意味するわけではないので、今後の実装を左右する大きな判断となったと思われる。

また、peer同士が互いの自己署名証明書を用いることの是非についても議論が交わされた。

今回のWGでは、標準化の方向性に関して以下の合意を得た。

1. CRLの取得はネットワークを用いた取得は仕様としない。
2. 複数階層に渡るPKIにおいて、中間認証局の証明書はネットワークを用いて取得する仕様とする。

pkix

11/10 13:00–15:00に開催された。150名ほどの出席者があり盛況。

通常のPKIXのミーティングと異なり、今回は事前にMLに対してCRLの扱いに関して大量のメールがやりとりされており、CRLの扱いに関しては白熱した議論がなされた。

また、すでにアナウンスされているがPKIX WGは、現在扱っている事案の処理が終わり次第、WGがクローズすることが決まっている。なかなか、クローズできる状況

写真 7　pkix-WGのチェアのTim Palk氏（左）とStephen kent氏

ではなかったが、おそらく次回、遅くても次々回のミーティングではPKIX WGのクローズがほぼ確実であると見られる。

今後、PKIに関する話題はSAAG（Security Area Advisory Group）にて議論されることになる。

インターネットにおけるPKIの利用のプロファイルとなっているRFC 3280の改訂作業が行われており（Son of RFC 3280と呼ばれている）、著者としてNISTのDavid Cooper氏が選出されたことがアナウンスされた。また、Son of RFC 3280に盛り込むべき事柄を11/19に迄にDavid Cooper氏にインプットすることが要請された。JNSAとして証明書のUTF8関連の問題をインプットした。

Son of RFC 3280は、今年中にI-Dとして発行される予定である。

SCVP（Simple Certificate Verification Protocol）の状況が説明された。SCVPのI-Dは16版となっており、15版より大幅な変更が行われており注意の喚起がなされた。SCVPのI-Dは、17版で終わりとすることになり今後は編集上の修正のみとし、機能の拡張は行わないこととなった。

新たにCRLの扱いに関して、AIA（Authority Information Access）を用いてCRLの署名者の証明書を得る仕様が提案された。これはIn-direct CRLなどを用いた場合、CRL単体ではCRLの署名者が正当な署名者であることを確定できないという問題点を解決するために、証明書の拡張領域であるAIAに正当なCRLの署名者の証明書を得るための情報を入れることを提案している。この提案は受け入れられた模様。

inch

11/11 09:00–11:30に行われた。30名ほどの参加者であった。

インシデント（セキュリティ事故）情報の交換フォーマットとしてIODEFというものがあり、これの標準化を行うWGである。昨今は、RIDという追跡情報のフォーマットも標準化している。

日本からはIPAの非常勤研究員のGlenn Mansfield博士と松下電工の福田氏がそれえぞれRIDの関しての利用のアーキテクチャとRIDの実装に関する経験に関して発表を行った。

写真 8　inch-WGで発表するJNSAの福田氏（松下電工）

easycert

11/11 13:00–15:00に開催された。約200名が参加。盛況であった。

Easy-to-Use Certificate BoFは、前回の60th IETFのSAAGにて開催が決まったBoFである。

BoFのチェアは、セキュリティエリアのADであるRussell Housley氏<housley@vigilsec.com>およびSteven Bellovin氏<smb@research.att.com>が務めた。

今回のBoFでは、すでにPKIを広く利用している3者の経験を話してもらい、その内容に関しての議論を行った。プレゼンテーションを行ったのは、MIT（マサチューセッツ工科大学）、Johnson & Johnson社およびDoD（国防総省）である。

プレゼンテーションおよびその後の議論の結果、PKIを

写真 9　easycert-WGチェアのSteven Bellovin氏（左）と Russell Housley氏

適切に使うためにはPKIに参加するメンバーの情報のデータベースがあり、認証の基盤を事前に構築しておくことが重要であると認識された。

PKIを使うためのプロトコルに関しては、すでに十分なものになっているとも認識された。その一方で、各プロトコルはそれぞれが証明書を要求することが一般的になっており、利用者が複数の証明書を持つ可能性があり、利用者が適切な方法で証明書を選択できる仕組みが欠けていることも認識された。

議論と議論の結論は、Steven Bellovin氏によりInformational RFCとしてまとめられることとなった。

Open Security Area Directorate (saag)

11/11 15:30–17:00に開催された。200名ほどの出席者がおり、盛況であった。

Open Security Area Directorateは、Security Areaの各WGの進捗状況と方向性を確認する場となっている。また、適宜に招待講演を行い、その後にSecurity Area全般の話題が議論される（ここしばらくはPKIに関しての議論が行われている）。

写真 10　SAAG-WGのミーティングの様子

今回の招待講演は、VPN Consortium のHoffman氏のIPsecにおける鍵交換プロトコルであるIKE（Internet Key Exchange）v1の暗号アルゴリズムの選択に関してと、NSAの新しい暗号ライセンスの担当者であるジュン・スタサク氏が楕円暗号に関してのライセンスに関してのプレゼンテーションを行った。

Security Area全般の話題としては、他のエリアで策定されているセキュアでないプロトコルをどうセキュアにしていくのかに関しての話題があった。

またSecurity AreaのArea Directoryとして長く務めたSteven Bellovin氏が引退し、新たにSam Hartman氏<hartmans-ietf@mit.edu>が就任した。Sam Hartman氏はSASL-WGのチェアを長く務めSASLの標準化に貢献している。

IETF Plenary

11/10 19:30–22:00に開催された。

IETFでは通常、水曜日と木曜日の夜のセッションにPlenaryが当てられているが、今回は水曜日のみとなった。

今回のIETFの参加者は1314名であり、26カ国より参加しているとのことであった。参加者の国籍の内訳は、米国が53%、日本が10%、韓国が5%、以下ドイツ、フランスと続き全体としてアジア勢が多く参加している状況である。特に今回のIETFでは、日本人が目に付いた。多くの日本人は、IPv6関連の活動を行っている。

今後はセキュリティ関連にも日本人が増えることを期待している。

写真 11　IETF Plenaryの会場風景

Plenaryとしての話題は、IETFのリストラクチャリングが大きな話題となっており、今回、従来は独自の財源で運営されていたIETFがISOCの下部組織として性格が変わったというアナウンスがあった(従来もISOCより運営資金の寄付が行われていたが、今回の改革ではIETFはISOCの一部門として性格づけられるように思える)。また、RFC Editorの改革が行われ多くのドキュメント類を迅速に処理できるようになったことが報告された。今回のIETFでは、RFC EditorのHelp Deskが用意されていた。RFC/I-Dなどの作成に関しての全般的なサポートを行っており、これが好評であったとの報告もなされた。

端末ルーム

今回のターミナルルールは、今までのIETFとは異なり、PCの設置は行われず電源、ネットワークコネクションおよびプリンタ(HP)の提供のみとなった。また、Hilton Hotelの提供するHi-Speed network ConnectionもIETFのスタッフにより運営された。

ミーティングルーム、ロビーおよびバーでは802.11a/b/gの各規格の無線ネットワークが用意され随所に電源も用意されていた。

無線に関しては、WEPなし、WEPあり、802.11x認証つきの3種類の無線ネットワークが用意され必要に応じて使い分けることが行われていた。これらのネットワークを使う際に、「ネットワークは守られていない。パスワードなどの情報を流す場合は、別の手段で守ること」との注意が換起されていた。

Hilton HotelのHi-Speed network Connectionに関しても同様の注意が求められていた。

写真 12　ターミナルルームの風景

会員企業ご紹介⑬

エヌ・ティ・ティ・コム チェオ株式会社
(http://www.nttcheo.com/)

NTT Com チェオ株式会社は、ITスキルを有する人材を育て、その人材を有効に活用していくことで、IT社会におけるビジネスをサポートしていく「ヒューマンリソースソリューションカンパニー」です。

インターネット活用に関する総合的な知識やスキルを認定する資格、NTTコミュニケーションズ インターネット検定「.com Master」「.com Mate」の運営および教材の提供をしてきたノウハウを活かし、新たに、情報セキュリティ分野における教育サービスを開始いたしました。

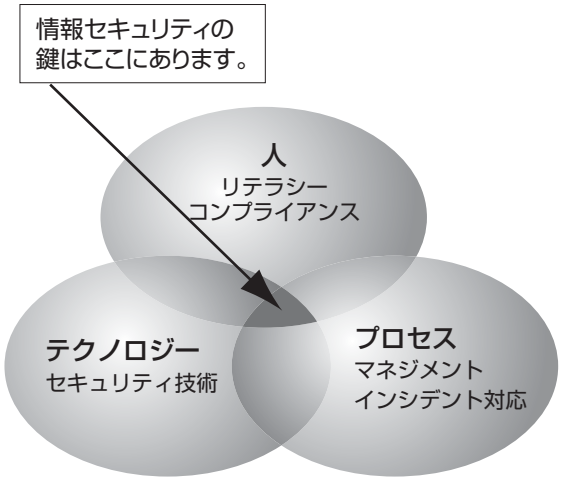
NTT Com チェオは、NTTコミュニケーションズ株式会社の100％出資子会社です。

NTT Com チェオでは、「新・情報セキュリティ対策ガイドブック .com Security Master」(NTTコミュニケーションズ発行)に準拠したセキュリティ研修コースをご提供しています。

◆NTT Com チェオの情報セキュリティ研修は・・・

これまでの情報セキュリティ研修は、
資格、認定取得や、システム技術者向けの技術研修に偏っていました。

NTT Com チェオの情報セキュリティ研修は、
**テクノロジーだけでなく、人やプロセスを含む幅広い知識の習得を目的とし、
システム技術者だけでなくセキュリティに携わる全ての方を対象として研修を行います。**



情報セキュリティの実現には、「人」
「プロセス」「テクノロジー」が欠かせません

◆研修コース

・個人情報保護対策コース（半日）

4月から施行される「個人情報保護法」の要件について、漏洩事例等を交えながら解説を行います。

お客様情報の管理に携わる方々を対象に、組織の一員として必要な知識や考え方を学び、情報セキュリティへの取り組みの重要性の理解を目標とします。

・1日コース

情報セキュリティ管理に携わる方を対象に、情報セキュリティの基本知識を習得・確認して頂く研修です。

業種に応じた実例等も交えて、情報セキュリティへの取り組みの重要性の理解を目標とします。

・3日コース

情報セキュリティ管理者の方を対象に、情報セキュリティ全般を網羅的に理解できる研修です。

演習を多く取り入れた実践な研修が特長です。

情報セキュリティ全般の考え方を、マネジメント～技術まで、幅広く関連付けて理解することを目標とします。

※上記コースの他にお客様のご要望に応じたカスタマイズ研修も行います。お気軽にお問い合せ下さい。

お問い合わせ先
エヌ・ティ・ティ・コム チェオ株式会社
教育事業部
〒105-0004　東京都港区新橋1-18-16
日本生命新橋ビル7F
TEL: 03-3539-5728　FAX: 03-3539-5714
E-mail: edu-sec@nttcheo.com
URL: http://www.nttcheo.com/

グローバルセキュリティエキスパート株式会社
(http://www.glbex.com)

GSX
GLOBAL
SECURITY
EXPERTS

グローバルセキュリティエキスパート株式会社は、セキュリティポリシーの導入、コンサルテーション、システム実装、アウトソーシングに至る広範なセキュリティサービスを提供する情報セキュリティ専門のコンサルティング会社です。情報セキュリティポリシーの国際標準となった英国規格協会(BSI)のBS7799を日本に初めて紹介し、同協会より高品質な情報セキュリティポリシーコンサルティングを行う専門会社としてのアソシエイツコンサルタント会社として認定されています。また、システム監査の一環としてハッカー(クラッカー)と同様の手法を用いてセキュリティ・ホールのチェックを行う“Tiger Team Service”(侵入検査サービス/模擬攻撃検査)を提供し、侵入検査サービスの分野では、検査手法、報告方法、メニューなどが国内のスタンダードとなり、大きな影響を与えています。GSXは最先端技術により、お客様の高い情報セキュリティ構築のためのご支援を行っております。

IJ00169/ISMS Certification Criteria(Ver.2.0)

IS71006/BS7799-2:2002

An ISO 17799 Associate Consultant of BSI Management Systems

■信頼性の高い情報セキュリティに関する調査分析及びコンサルティング事業

グローバルセキュリティエキスパートはセキュリティポリシーの導入、コンサルテーションからシステム実装、アウトソーシングに至る広範な情報セキュリティサービスを提供しています。

■セキュリティマネジメントコンサルティング

情報セキュリティを考えた場合、システムやアプリケーションに対しては、セキュリティソフト等の対処によりある程度のセキュリティレベルを保つことができます。しかしそれだけでは不充分であり、同時に大切なのは、企業(組織)が常日頃から情報セキュリティに関する意識を高く持つことが重要となります。GSXのSMC(Security Management Consulting)では、経験豊富なコンサルタントが確立された手法を通して、お客様のセキュリティ マネジメント システムの構築を支援します

■セキュリティインテグレーションサービス

ネットワークシステムの運用には、様々なセキュリティ上の問題がともないます。不正アクセス、情報漏洩、私的利用、障害発生／復旧、セキュリティ教育、等々。GSXのセキュリティ インテグレーション サービスは、これらの問題にトータルにお応えします。特に不正侵入の問題については、ホームページの改ざんや機密情報の流出／消失、システム破壊等、被害は甚大です。さらに、他サイトへの踏み台にされることにより加害者となり、管理責任を追及されかねません。GSXは不正侵入対策として、様々な要望に応えます。

■タイガーチーム™サービス

お客様のネットワークシステムのオープン化にともない、GSXは1977年にシステムの脆弱性を監査する手法として、タイガーチーム サービスの提供を始めました。タイガーチーム サービスは、監査法人系コンサルティング会社として培ってきたシステム監査手法と高度なネットワーク技術にもとづき、セキュリティ上の問題点の指摘や改善案の提示、Webシステムの構築支援および不正アクセスの被害にあわれた場合のための保険など、総合的なコンサルティング サービスを提供しています。

※“タイガーチーム”はGSXの登録商標です。

NETWORK SECURITY
TIGER TEAM SERVICE

FS66176 / ISO 9001:2000

セキュリティに限らず監査は、常にその質が一定でなくては意味がありません。GSXは監査レベルの一貫性を保つため品質保証の国際標準規格であるISO9000を取得しています。
当社は黎明期から情報セキュリティ業務に携わり、トップレベルのサービスクオリティをご提供できる信頼と実績の会社です。

お問い合わせ先

東京本社:
〒102-0083 東京都千代田区麹町5－3
第七秋山ビルディング6階
TEL: 03-5211-7731 FAX: 03-5211-7732

大阪支社：
〒530-0003 大阪市北区堂島1丁目2－5
堂北ダイビル1階
TEL:06-6347-5251 FAX:06-6347-5252
E-mail: tiger@glbex.com

セキュリティ・エデュケーション・アライアンス・ジャパン
(http://www.sea-j.net/)

セキュリティ・エデュケーション・アライアンス・ジャパン（通称：SEA/J シージェイ）は、経験年数が2～3年のIT技術者に対する情報セキュリティ技術の基礎教育を柱として、経験と専門性を兼ね備えた情報セキュリティプロフェッショナル育成のために、正会員9社※により教育プログラムを開発・提供している団体です。
昨年は発足から2年が過ぎ、認定取得者も1000名を超えるなど、市場から求められる声も大きくなってきていることから、よりいっそうの教育内容の充実を図っています。

SEA/J（シージェイ）の事業概要

SEA/Jでは、IPA情報セキュリティスキルマップを参考に、広範なセキュリティ技術項目を網羅的・体系的に学べるテキストを開発しています。情報セキュリティ技術の習得を目指す方々は、SEA/J認定校制度により全国の「認定校」を通じて教育を受けられるとともに、スキル習得の度合いを「認定試験」により確認することが出来ます。

教育プログラムの特徴

多くの仕事をこなしながら知識習得をしなければならない技術者の方々の現状を考え、受講しやすく身につきやすい教育コンテンツを目指して開発しており、次のようないくつかの特徴があります。

① **ITスキル標準への対応**
ITSS実証実験のノウハウを反映し、基礎は2～3、応用は2～4のレベルを想定した内容として、人材育成レベルを明確化しています。

② **IPAスキルマップに基づき、スキル項目全般を網羅**
広範な情報セキュリティスキル項目を網羅的に学習できるよう、整合性を図りながら開発しています。

③ **製品に依存しない、ニュートラルな教育**
ベンダー各社が専門知識を持ち寄り、対策を行うための基礎スキルを身につけることを目的にしています。

④ **日本国内での共同開発**
他国語の翻訳による誤解釈や一部掲載などの問題はなく、国内法適用などに早急に対応することが出来ます。

⑤ **受講しやすい時間数に必要要素を集約**
すでに習得しているはずのネットワーク知識や、逆に研究開発者のみが必要とする専門的な内容を省き、情報セキュリティの基礎を確実に習得するための最低限必要なスキル項目にまとめています。

認定試験の実施

試験は、試験配信専門会社の公開試験会場でのコンピュータベースによる試験です。
それぞれ60分間で、必要スキルを問い、選択肢から選択する形式となっています。
なお、合格者にはそれぞれ、基礎コースはCSBM（Certified Security Basic Master）、応用コースはCSPM（Certified Security Professional Master）として認定し、認定証を贈るとともに、名刺などに認定取得者のロゴ表示などができます。

認定教育及び試験の種類

提供しているコース体系は、基礎コースと応用コース(テクニカル編・マネジメント編)の全3コースです。
基礎コースでは情報セキュリティのスキル項目を網羅的に学習。応用コースは専門分野に絞り、考え方や対処法、手順を学ぶことに主眼を置くコースとしています。
また、それぞれに対応する試験があります。

認定教育コース及び試験の価格は次のとおりです。

- 受講料（テキスト・試験含む）
  - ○ 基礎コース　99,750円
  - ○ 応用コース テクニカル編　204,750円
  - ○ 応用コース マネジメント編　141,750円
- 試験料金：各試験とも15,750円

※ 正会員9社(50音順):
RSAセキュリティ、大塚商会、ソフトバンクBB、ディアイティ、トレンドマイクロ、日本ベリサイン、ヒューコム、マイクロソフト、マカフィー

お問い合わせ先

セキュリティ・エデュケーション・アライアンス・ジャパン
SEA/J（シージェイ）事務局
〒166-0011 東京都杉並区梅里1-7-7
新高円寺ツインビル2F
TEL：03-5306-7507　FAX：03-3313-5205
E-mail：seajinfo@sea-j.net
URL：http://www.sea-j.net/

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アプリケーション ファイアウォール、
『SecureSphere ver3』アプライアンス
～「Oracle」「MS-SQL」「DB2」「Sybase」の監視、
防御も可能。～】

Webアプリケーションの脆弱性を狙った攻撃がネット社会の深刻な問題となっています。『SecureSphere』はこのようなWebサイトへの攻撃、改ざん、内部データベース侵害、ワーム感染など、ゼロデイアタックを含む悪意のある攻撃からWebアプリケーション領域（Webサーバ＋Webアプリケーションサーバ＋データベースサーバ）を包括的に防御します。
http://www.ahkun.jp/company/news_press/download/p_ss_nr_30_sale.txt

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

○CompuSec シリーズ

モバイルPCやデスクトップPCを対象にしたPKI(公開鍵基盤)ベースの個人認証・暗号化セキュリティツールです。OS起動前に行うプリブート認証とハードディスクの丸ごと暗号化（OS含む）だけでなく、USBメモリや外部接続ディスク装置や電子メールの暗号化といったPKIベースの様々なセキュリティ機能を標準搭載しています。PCの盗難・紛失などの不測の事態においても情報漏えいを防止し、個人情報など重要なデータが不正利用されるのを防ぎます。
http://canon-sol.jp/product/cs/

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

○個人情報保護対策（フォレンジックサーバ）！
抑止力効果抜群！

情報漏洩を防止する100％の事前対策はありません。
最悪の事態に備えること、信用を失わないことが大切です。
もし、情報漏洩事故が起きてしまったら、迅速な謝罪と解明が必要です。
誰が・いつ・何を・どこで・どのように・何の為に、を解明する為の証拠保全を行うことが必要となってきます。
そこで、通信パケットレベルの正確なデータを記録・解析することにより、内部・外部の不正利用者を追跡・発見して解明する方法を「MSIESER」が提供いたします。

◆お問い合わせ先◆
菱洋エレクトロ株式会社　営業3部3G
URL http://www.ryoyo.co.jp
TEL：03-3546-5040
e-mail：motohiro_hirano@ryoyo.co.jp　平野

■サービス情報■

○「図解　個人情報保護法リファレンスガイド」と
「個人情報保護法スターターキット」の販売を開始

「図解　個人情報保護法リファレンスガイド」は、個人情報保護法対策で特に重要な従業員への周知徹底を目的に、事業者に課せられた義務をわかりやすく解説し、日常業務の中で浮かぶ疑問に答えられる参照型のハンドブックです。
「個人情報保護法スターターキット」は、個人情報保護法に未対応の事業者を対象に、「図解　個人情報保護法リファレンスガイド」、管理者向け実地教育、窓口対応に必要な様式・マニュアル、全社教育用教材などを加えたセット商品です。
サービス概要
http://www.hucom.co.jp/service/service.html
プレスリリース
http://www.hucom.co.jp/news/hmnr-0502.html

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

■イベント情報■

○【(株)アークン　製品紹介セミナー
４月19日(火)開催　　参加費無料】
世界の最新技術をデモや導入事例を盛り込みながら
ご紹介させていただきます。

●Imperva社『SecureSphere（セキュアスフィア）』
10:00-12:00
IPSでは護れない未知の攻撃も防御するWebアプリケーション ファイアウォール。
新登場のアプライアンスでは、防御データベースにDB2、Sybaseを拡張。
●Finjan社『Vital Security（バイタル セキュリティ）』
13:00-15:00
アンチウイルスソフトでは間に合わない新種/未知ウイルスの攻撃や不正コードの侵入を防御。
http://www.ahkun.jp/resource/event.html

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

事務局お知らせ

JNSA ANNOUNCE

1. 主催セミナーのお知らせ

●「2004年度JNSAワーキンググループ成果報告会」

日　時：2005年6月9日（木）
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、ぜひご参加下さい。
詳細はJNSAのホームページでご確認下さい。
http://www.jnsa.org/

2. 後援イベントのお知らせ

1．「UML Forum/Tokyo 2005」

会　期：2005年4月26日（火）～27日（水）
主　催：オブジェクトテクノロジー研究所
会　場：青山TEPIA
http://www.otij.org/event/umlforum/2005/

2．「RSA Conference 2005 Japan」

会　期：2005年5月12日（木）～13日（金）
主　催：RSA Conference 2005 Japan実行委員会
会　場：東京プリンスホテル
http://www.medialive.jp/events/rsa2005/

3．「第9回コンピュータ犯罪に関する白浜シンポジウム」

会　期：2005年5月19日（木）～21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
http://www.sccs-jp.org

4．「HOSTING-PRO 2005」

会　期：2005年6月16日（木）
主　催：HOSTING-PRO 2005実行委員会
会　場：TIME24
http://hosting-pro.jp/

5．「自治体総合フェア2005」

会　期：2005年7月13日（水）～15日（金）
主　催：社団法人日本経営協会
会　場：東京ビッグサイト
http://nomabs.noma.or.jp/lgf/

3. JNSA部会・WG 2004年度活動

1. 政策部会

（部会長：下村正洋/ディアイティ）

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

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

（リーダー：山田英史氏/ディアイティ）

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

【セキュリティベンダーとしての管理基準策定WG】

（リーダー：丸山司郎氏/ラック）

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

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

【セキュリティ監査WG】

（リーダー：大溝裕則氏/ジェイエムシー）

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

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

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

【マーケットリサーチWG】

（リーダー：玉井節朗氏/IDGジャパン）

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

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

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

【プライバシー保護実装研究WG】

（リーダー：久波健二氏/日本IBMシステムズ･エンジニアリング）

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

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

【セキュリティ会計ガイドライン検討WG】

（リーダー：佐野智己氏/凸版印刷）

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

予定成果物は『ガイドライン』の上程。

【個人情報保護法ガイドラインWG】

（リーダー：佐藤憲一氏/大塚商会）

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

2005年3月にガイドライン書籍を発行した。

2. 技術部会

（部会長：佐藤友治氏/IRIコミュニケーションズ）

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

【セキュリティポリシーWG】

（リーダー：小杉聖一氏/NECソフト）

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

【コンテントセキュリティWG】

（リーダー：松本直人氏/ネットアーク）

コンテントセキュリティに関するガイドラインドキュメントを作成。広く一般的に定義が無いコンテントセキュリティの定義と具体的なカテゴリー分けと手法を分類整理する。

【不正プログラム調査WG】

（リーダー：渡部章氏/アークン）

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

【ハニーポットWG】

（リーダー：園田道夫氏/JNSA研究員）

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

【データストレージ＆セキュリティWG】

（リーダー：立身俊雄氏/ディアイティ）

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

【暗号使用ポリシーテンプレート作成WG】

（リーダー：板倉行男氏/アークン）

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

【S/MIME検討WG】

（リーダー：磐城洋介氏/NTTコムウェア）

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

【Webセキュリティ調査･検証WG】

（リーダー：斉藤純平氏/アークン）

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

【脆弱性定量化に向けての検討WG】

（リーダー：郷間佳市郎氏/京セラコミュニケーションシステム）

脆弱性について、その危険度を定量化（数値化）する手法を検討する。

脆弱性の定量化については、すでにいくつかの方式がある。これらを検討した上で、実情に照らし合わせ、指標となりうる方式の検討を行っていく。

【暗号モジュール評価基準WG】

（リーダー：小川博久氏/シーフォーテクノロジー）

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

本WGはFIPS 140-2に対する疑問を解消し、啓発することを目的とする。

【PKI相互運用技術WG】

（リーダー：松本泰氏/セコム）

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

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

【ChallengePKIプロジェクト】

（リーダー：松本泰氏/セコム）

IPAの2004年度 情報セキュリティ関連の調査の「PKIにおけるUTF8String問題に関する調査」に応募し採択された。現在、報告書は、作成中であるが、この報告書に付随する成果は、IETFのPKIX WGにフィードバックすることも検討している。

3. マーケティング部会

（部会長：古川勝也氏/マイクロソフト）

JNSA自身の認知度向上と、ネットワークセキュリティに関する普及・啓発活動を行う。

【セキュリティ啓発WG】

（リーダー：古川勝也氏/マイクロソフト）

昨年度経済産業省の委託事業として行なった「インターネット安全教室」を拡張して今年度は全国25ヶ所以上で行っている。その企画・運営協力を行なう。

【セキュリティスタジアム企画運営WG】

（リーダー：園田道夫氏/JNSA研究員）

不正アクセス手法の攻防の一大実験場「セキュリティスタジアム」の企画と運営を行なう。

2004年度はセミナーとスタジアム本大会をさらにシステマチックに開催できる仕組みを整えていく予定。セキュリティトピックのセミナーの企画や本大会企画準備、技術教育講座の企画なども検討していく。

2004年11月2日～4日に、「セキュリティ・スタジアム2004」を開催した。

4. 教育部会

（部会長：佐々木良一氏/東京電機大学教授）

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

【スキルマップ作成WG】

（リーダー：佐久間敦氏/みずほ情報総研）

ネットワークセキュリティ技術者に求められる知識やスキルを整理、体系化した「スキルマップ」を整備し、ネットワークセキュリティ技術者の育成に向けた各種施策の検討を行うことを目的とする。

【JNSA推奨教育コース作業WG】

（リーダー：松田剛氏/ヒューコム）

情報セキュリティに関するビジネスが社会に浸透するに伴い、セキュリティ教育・トレーニングの市場が拡大基調にある。

市場の活性化は歓迎すべき傾向である反面、受講者の立場からはどのサービスが最も自分に適しているのか、その選択が極めて難しく、ミスマッチが多発することも否定できない。こうした事態を防止すべく、情報セキュリティ教育のあるべき姿について、カリキュラムに対する評価・認定（教育スタンダード）ガイドライン策定を通じ、教育市場のバランスの取れた発展に寄与することを目的とする。

【CISSP-WG】

（リーダー：大河内智秀氏/NTTコミュニケーションズ）

（ISC）^{2}が米国政府と提携し開発した「ISSEP」のように、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（仮にISSJPNとする）際に新規追加すべきドメインについて検討し策定する。

5. 西日本支部

（支部長：井上陽一氏/ヒューコム）

JNSA西日本支部は関西に拠点を置くメンバー企業の協賛の下、西日本におけるネットワーク社会のセキュリティレベルの維持·向上並びに、日々高まる情報セキュリティへのニーズに応えるべく、先進性を追及すると共に、質の高いサービスを提供する事を目的として活動致している。

今年度は、関西方面でのセキュリティ啓発セミナーを中心として活動を行なっていく。

【セミナー運営WG】

（リーダー：中台芳夫氏/西日本電信電話）

西日本支部主催セキュリティセミナーのコンテンツの企画検討と運営を行なう。

2004年11月11日には、NSF2004 in OSAKAと題して、大阪市新梅田研修センターにてセミナーを開催した。

また、2005年3月22日には、大阪商工会議所にて「個人情報保護法完全施行直前対策セミナー」を開催した。

【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、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？

たとえ自社で5000件以上の個人情報を保持しなくても委託元である企業からは様々な要求が出てくることは容易に想像がつく。これらに対してもどう対処したらいいのかについて調査し、運用編としてをまとめることを目的とする。

また、主務官庁分野別での事例も収集していくことで、対応企業の幅を広げる。

4. JNSA役員一覧（2005年3月31日現在）

会　長　石田　晴久
多摩美術大学教授・東京大学名誉教授

副会長　長尾　多一郎
株式会社ネットマークス 代表取締役社長

副会長　東　貴彦
マイクロソフト株式会社 業務執行役員

副会長　大和　敏彦
シスコシステムズ株式会社 執行役員CTO

理　事（50音順）

在賀　良助	株式会社アイアイジェイテクノロジー
井上　陽一	株式会社ヒューコム
宇佐美　慎治	株式会社大塚商会
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
浦山　清治	
岡村　靖	シムデスク･テクノロジーズ
甲斐　龍一郎	新日鉄ソリューションズ株式会社
勝見　勉	グローバルセキュリティエキスパート株式会社
川上　博康	セコムトラストネット株式会社
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
鈴木　優一	セコム株式会社
武智　洋	横河電機株式会社
田中　辰夫	マカフィー株式会社
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
中山　恵介	システムニーズ株式会社
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
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
吉澤　昭男	古河電気工業株式会社
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
綿引　宏行	東京海上日動火災保険株式会社

監　事

土井　充	清友監査法人　公認会計士

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
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（2005年3月2日現在　199社　50音順）

【あ】

（株）アークン
RSA セキュリティ（株）
（株）アイアイジェイ テクノロジー
（株）アイ・ソリューションズ
（株）IRI コミュニケーションズ
（株）IT サービス
（株）アイ・ティ・フロンティア
（株）IDG ジャパン
（株）アイネス
アイネット・システムズ（株）
（株）IP イノベーションズ
アイマトリックス（株）
（株）アクセンス・テクノロジー
あずさ監査法人
（株）網屋
アライドテレシス（株）
アラクサラネットワークス（株） New
（株）アルゴ21
（株）アルテミス
（株）アンラボ
イーディーコントライブ（株）
（株）イオノス
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
ウッドランド（株）
AT＆T グローバル・サービス（株）
（株）エクスフロント New
（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） New
（株）NTT データ
（株）エネルギア・コミュニケーションズ
エムオーテックス（株）
（株）エム・ファクトリー
エリアビイジャパン（株）
ELNIS テクノロジーズ（株）
（株）大塚商会
オムロンフィールドエンジニアリング（株）

【か】

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

【さ】

サーフコントロール　ジャパン New
サイバーソリューション（株）
サン・マイクロシステムズ（株）
（株）シー・エス・イー
ジーエフケー　マーケティングサービス　ジャパン（株） New
（株）シーフォーテクノロジー
（株）ジェイエムシー
ジェイズ・コミュニケーション（株）
（株）CRC ソリューションズ
シスコシステムズ（株）
システムニーズ（株）
（株）シマンテック
シムデスク・テクノロジーズ
寿限無（株）
（株）翔泳社
（株）情報数理研究所
新日鉄ソリューションズ(株)
図研ネットウエイブ（株）
（株）ステラクラフト

ストーンソフト・ジャパン（株）
住商エレクトロニクス（株）
住生コンピューターサービス（株）
セイコープレシジョン（株）
セキュアコンピューティングジャパン（株）
（株）セキュアソフト
（株）セキュアブレイン New
セキュリティ・エデュケーション・アライアンス・ジャパン（株） New
セコム（株）
セコムトラストネット（株）
（株）セゾン情報システムズ
（株）セタ
セントラル・コンピュータ・サービス（株）
ソニー（株）
ソニー・エリクソン・モバイルコミュニケーションズ（株）
ソフトバンクBB（株）
ソラン（株）
（株）ソリトンシステムズ
ソレキア（株）
（株）損保ジャパン・リスクマネジメント

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

【な】
（株）ニコンシステム
西日本電信電話（株）
日商エレクトロニクス（株）
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）
日本電気システム建設（株）
日本電信電話（株）　情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
ネクストコム（株）
（株）ネットアーク
（株）ネット・タイム
（株）ネットマークス
（株）ネットワークセキュリティテクノロジージャパン
ネットワンシステムズ（株）
ノベル（株）

【は】
（株）ハイエレコン
東日本電信電話（株）
（株）日立システムアンドサービス
（株）日立製作所
日立ソフトウェアエンジニアリング（株）
（株）ヒューコム
（株）ビー・エス・ピー
（株）PFU
ファルコンシステムコンサルティング（株）
（株）フォーバル クリエーティブ
富士ゼロックス（株）
富士ゼロックス情報システム（株）
富士通（株）
富士通エフ・アイ・ピー（株）
富士通関西中部ネットテック（株）
富士通サポートアンドサービス（株）
（株）富士通ソーシアルサイエンスラボラトリ
（株）富士通ビジネスシステム
扶桑電通（株）
（株）フューチャーイン

（株）ぷららネットワークス
（株）ブリッジ・メタウェア
古河電気工業（株）
（株）プロティビティ

【ま】

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

【や】

横河電機（株）

【ら】

（株）ラック
リコーテクノシステムズ（株） New
菱洋エレクトロ（株）
（有）ロボック

【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
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 New

6. JNSA年間活動（2004年度）

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

2004年10月～2005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/active6.htmlに掲載しています。

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

7. JNSAについて

■会員の特典

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

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

8. お問い合せ

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

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

JNSA Press vol.13

2005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会員 行動指針

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

そのため、以下の通り会員の行動指針を定め、規範とするよう努めます。

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

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

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

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

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