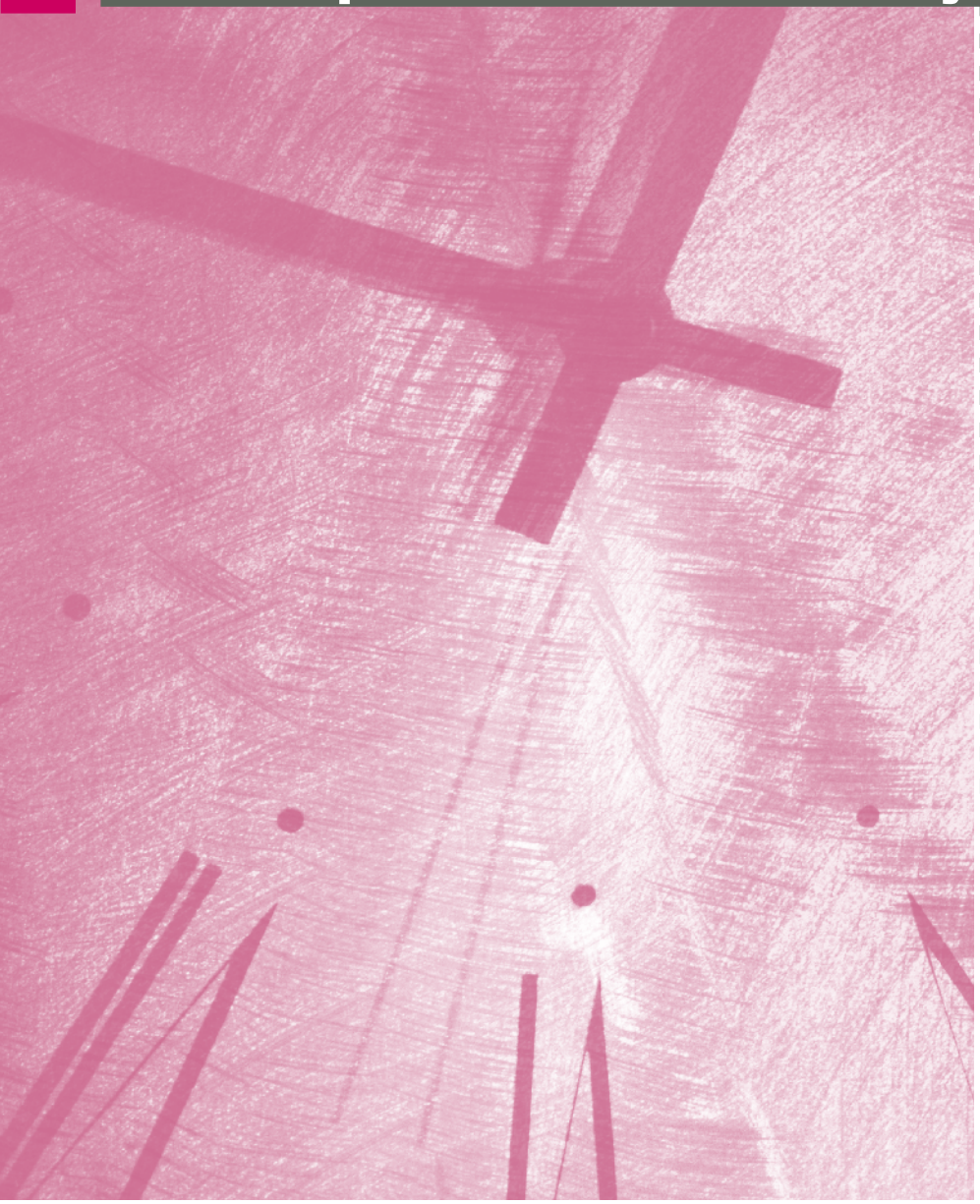
JNSA Press

Japan Network Security Association

Vol.15
December 2005



CONTENTS

ご挨拶
情報セキュリティと倫理 …… 1

特　集
- 社会システムとしての電子認証と電子署名 3
- 第63回IETF参加報告 …… 12

JNSAワーキンググループ紹介
- 情報セキュリティ推奨教育検討WG …… 17
- スパイウェア対策啓発WG …… 19
- 中小企業向け個人情報保護対策WG …… 20

会員企業ご紹介 …… 21

JNSA会員企業情報 …… 25

イベント開催の報告 …… 28

「インターネット安全教室」のお知らせ …… 35

事務局お知らせ …… 37

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

情報セキュリティと倫理

工学院大学大学院情報学専攻教授
淀川　英司

2001年1月に施行された高度情報通信ネットワーク社会形成基本法(通称:IT基本法)では、「高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない」と記述されている。また、教育においても、「すべての国民が情報通信技術を活用することができるようにするための教育および学習を振興するとともに、情報化社会の発展を担う専門的な知識又は技術を有する創造的な人材を育成する」ということが決められている。そして、当時の政府のIT戦略会議は、「2005年までに世界最先端のIT国家を目指す」という基本方針を打ち出している。

さて、2005年も過ぎようとしている今、わが国のIT社会の発展状況はどうであろうか?残念ながら、国民が安心して情報通信ネットワークを利用できる環境とはなっていないといわざるをえない。確かに、技術の進歩とサービスの低価格化により、インターネットは目覚しい発展・普及を見せ、今や職場や家庭になくてはならない存在になりつつある。しかし、コンピュータ・ウィルスの侵入、情報の改ざん、盗聴、フィッシング、スパイウェア、迷惑メール等々、情報セキュリティの問題が大きくクローズアップされている。この問題は当初より予想されていたことではあるが、安心・安全な高度IT社会の形成には、絶対に避けて通れない重要課題である。では、この情報セキュリティの問題にどう対処したらよいであろうか?以下、その対応策について、いくつか考えてみたい。まず、第一は「技術による対処」である。現在、暗号化技術・認証技術やウィルス対策ソフトウェア等の開発が進められ、実用化されているが、ハッカーやクラッカーの他、悪意ある人達の攻撃手法もより巧妙になり、イタチごっこが続いている状況である。このような状況は今後も変わらないと思われるが、より信頼性の高いデペンダブルなセキュリティ技術の開発が望まれる。

第二は、「情報セキュリティ分野の専門家の育成」である。わが国では現在、情報セキュリティ技術者が大幅に不足しており、その育成が急務となっている。大学や大学院における情報セキュリティ教育もようやく始まったところである。文部科学省も新興分野人材養成の一つとして、情報セキュリティの専門技術者の養成に力を入れている。

工学院大学では、平成15年度科学技術振興調整費のプログラムとして、「セキュアシステム設計技術者の育成」が採択され、平成16年度より社会人と大学院生を対象に約40名／年の人材育成を行っている。このプログラムは、産学連携を大きな特徴としており、JNSAに大変協力をいただいている。

第三は、「倫理教育の徹底」である。これからの高度IT社会においては、この「倫理教育」こそ、国をあげて取り組むべき最重要課題と思う。時間がかかっても幼児期から倫理・道徳教育をしっかり行うべきである。わが国は経済大国となり、物質的にはそれなりに豊かになった。しかし、最近の世相を見ると政治、経済、教育等あらゆる分野において倫理・道徳の喪失が目立つ。これは由々しいことである。例えば、携帯電話は大きな利便性をもたらした。しかし、その使用のマナーの悪さは嫌悪感を覚えるほどである。「衣食足りて礼節を知る」という諺は現在の日本社会には当てはまらない。倫理を喪失した組織は崩壊する。真に心の豊かな幸福な社会の形成には、国民の高い倫理観が基本になければならない。

第四は、「法律の整備」である。残念ながら、人間の心理的基本特性の中には、「善」だけではなく、「悪」と「非倫理性」が含まれている。したがって、いくら倫理教育を行っても悪いことを考え、実行する人がいなくなることはないであろう。したがって、適度な罰則をもつ法整備は必須である。しかし、法律で厳しく規制すればよいということではなく、自由とのよりよいバランスが肝要である。

高度IT社会の形成は、生活の利便性を高め、仕事の効率を上げるといったプラス面だけをもつものではない。大きなマイナス面もある。情報セキュリティが十分確保できなければ安全なIT社会は成立しない。悪意をもっている人にとって、IT社会のサイバースペースは、実世界に比べてはるかに犯罪を実行しやすい環境になっている。少しの知識さえあれば、中高生レベルでもほとんど罪意識なくゲーム感覚で、世界規模の影響を及ぼす罪を犯してしまう危険性がある。JNSAが、より健全なIT社会の形成に大きく貢献することを期待する。

社会システムとしての電子認証と電子署名

PKI 相互運用技術 WG リーダー
セコム株式会社 IS 研究所　松本　泰

インターネットバンキング等のサービスにおいてフィッシングサイト、スパイウェア等を利用した金銭目的の犯罪が増加しています。今後、インターネットの利活用が進むほどにこうした金銭目的の犯罪は増加する可能性があります。こうした中、インターネットバンキングに限らずネットワーク基盤の利活用が求められています。e-Japan戦略の成果としてインターネット等におけるブロードバンドの普及などが挙げられており、そして、これらのIT基盤の利活用が次の課題とされています。しかし、これまでのIT基盤は、利活用を進めるにふさわしい十分なユーザ認証(電子認証)、セキュリティを提供しているとはいえず、結果としてインターネットの利活用を阻むことになるのではないでしょうか。一方、ネットワーク社会の安全、安心を推進する法制度として2001年に施行された電子署名法がありますが、電子署名法に基づく電子署名はとても普及しているとは言いがたい状況にあります。電子署名法は来年で施行5年を向かえ、その改正も検討されています。社会がIT技術やネットワークへの依存度を深めていくとするならば、ネットワーク社会の安全、安心を推進するための技術や法制度のあり方を考え直す必要があるのではないでしょうか。本稿では、こうした問題を考察します。

1. ネットワーク社会における電子認証の重要性

人、サービス、デバイスがシームレスに接続されていくネットワーク社会における電子認証(Authentication)の重要性は、技術者ならば誰もが感じていることではないでしょうか。政府が進める「e-Japan戦略」は、「元気、安心、感動、便利」な社会を目指すとされています。これは、いつでも、どこでも、誰にでも(人)、何にでも(デバイス、サービス)ネットワークを介して接続され、その中で様々なサービスを享受できるであろうことを前提に考えられています。しかし、多くの感動、便利を提供するサービスでは、単にネットワーク上で接続されるだけではなく、信頼関係を確立するための認証(Authentication)が重要になります。

安全、安心なネットワーク社会を実現するための重要な要素のひとつだと考えられる認証に対しては、これまでにない多様な要求が浮上しています。人の認証ということだけをとっても、プライバシー保護のための仮名による認証、人の色々な属性に関する認証、これらの認証がシームレスに接続されたネットワークにおいて、より大規模に、更に色々な組織を超えて行われること等が要求されています。さらに、何にでも接続される今後のネットワーク社会においては、人の認証だけでなく、デバイスやサービス等の認証も重要な役割を果たします。

こうした中、様々な認証技術が登場しているものの、今後のネットワーク社会で安心して使え、個々のネットワークや組織を超えた広範囲な認証を実現するには、まだ大きな壁があります。壁のひとつは相互運用性の問題です。これまでの多くの認証技術は、限られた環境で動作すればよく、相互運用性の問題が大きくクローズアップされることはありませんでした。

認証のセキュリティレベルの向上も重要な課題です。e-Japan戦略の成果としてインターネットにおけ

るブロードバンドなどの普及が挙げられていますが、これらのIT基盤の利活用が次の課題とされています。しかし、これまでのIT基盤は、利活用を進めるにふさわしい十分なユーザ認証(電子認証)とセキュリティを提供しているとは言えません。インターネットにおける認証はごく当たり前に利用されているにも限らず、そのセキュリティ等に対して何の評価基準もなく、また、実際に利用されている電子認証も低いセキュリティレベルのものが主流だと考えて間違いありません。低レベルの認証だけが様々なサービスに広範に利用されていることは、ネットワークの実質的な価値を下げているとも言えます。

それでは、これまでこうした問題を解決する努力がなされてこなかったのでしょうか。一般には法制度における政府の取り組みとして2001年に施行された電子署名法があると考えられています。しかし、現時点において電子署名は普及しているとは言えず、また、電子署名に対する様々な誤解もあるように思われます。まずは、この電子署名法から考察します。

2. 電子署名法

IT社会、電子社会に対応する法律として電子署名法があります。電子認証(Authentication)の基盤に関して、電子署名法が重要な役割を果たしていると思われている節がありますが、これは必ずしも正しくありません。このあたりから説明していきます。

1990年代の後半に世界各国で電子署名法が成立した流れを受け、日本においても電子署名法が検討され2001年4月に電子署名法が施行されました。この電子署名法によって適正に行われた電子署名は、手書き署名や押印がなされた文書と同様に文書が真正に成立したとの推定効が与えられることとなりました。電子署名法は、旧来の紙文書における押印を、電子文書に対する電子署名により置き換えることを可能にすることで、紙を前提とした多くの法律を改正せずに、紙文書から電子文書への移行を可能にしています。

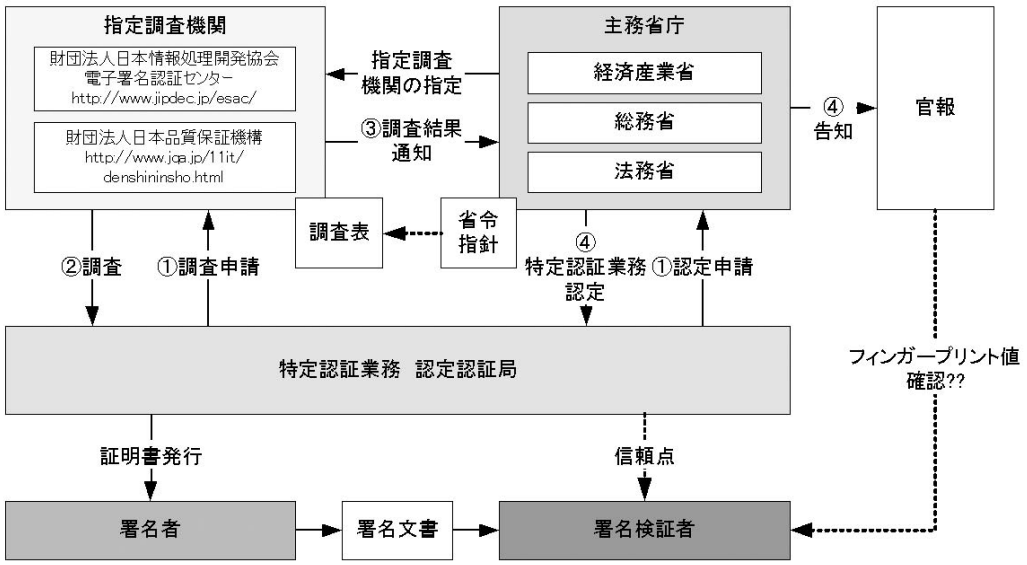
電子署名法は、これまで紙と押印を中心とした社会から、電子文書と電子署名を中心とした社会への足がかりとなり、今後の電子社会の中で大きな役割を担っていることは間違いありません。電子署名に利用されるPKI技術は、電子署名、電子認証、暗号などの機能を提供しますが、電子署名法自体の目的は、文書の署名に対するものです。従来の手書き署名や押印に代わる電子署名の役割は、現在の法制度の延長上にあり、法制度の上からは分り易いものがあります。しかしネットワークにおけるリモートの電子認証に対応する概念は、従来の法制度にはありません。そのため電子署名法は、ネットワーク環境における電子認証(Authentication)とは直接関係ないことに注意する必要があります。

電子署名法は民間に対する法律ですが、電子政府の認証基盤とされる政府認証基盤(GPKI: Government Public Key Infrastructure)も電子署名に対応した(Authenticationの基盤ではない) 基盤と言えます。実際GPKIが発行する証明書は、基本的に否認防止の署名を目的とした官職証明書(Certificate)です。政府認証基盤(GPKI)は、1999年末のミレニアムプロジェクトのアクションプランにおいて、電子申請、通知／交付のセキュリティを確保するための基盤の整備として始まっています。電子申請には民間からの申請書に申請者の電子署名を付すこと、政府からの通知／交付には政府官職の電子署名を付けることとされ、そのため電子署名は電子申請者や政府官職の本人性と申請文書や通知／交付文書の真正性を担保するために必須のものとされました。官職による署名は、多くの場合「人」の意思による署名ではありません。例えば電子申請の場合、何らかの府省内の一連の手続きや審査を経た後、申請に対して許可するといった文書に対して「官印」に代わる官職による署名がなされます。こうした官職の役割としても、一般的に電子認証(Authentication)は不要だったわけです。

電子署名と電子認証を理解する上で、認証(Authentication)と認証(Certification)、2つの「認証」という用語は、多くの混乱の元になっています。多くの法律用語において「認証」は、英語のCertificationを意味します。それに対して、サーバ等によるユーザの真正性の確認を意味することも認証(Authentication)と呼ばれます。Certificationは、何らかの権威者が発行する証明書により、何らかのことを証明することです。公としての行政機関は、従来からこのCertificationを数多く行っており、その証としての証明書の発行を行なってきました。そのため法制度等において「認証」は、Certificationを意味することが多い訳です。そのためCertificationの電子化自体も多くの場合、電子署名の技術を用いて実現されています。

電子署名法の施行により、民間に証明書を発行する認証業務のうち一定の基準を満たすものは総務大臣、経済産業大臣及び法務大臣の認定を受けることができる制度が導入されました。この特定認証業務認定では、認証局に対する認定の基準を定めていますが、内容としては認証局の設備や運用に関するものであり、特に、証明書を発行する本人身元確認と、証明書と鍵を本人に結びつける作業に関して非常に高いハードルを課しています。特定認証業務認定の基準は、現在のところ、電子署名、電子認証に関連した日本国内の唯一の基準と言えます。図1に特定認証業務認定の関連を示します。

図1

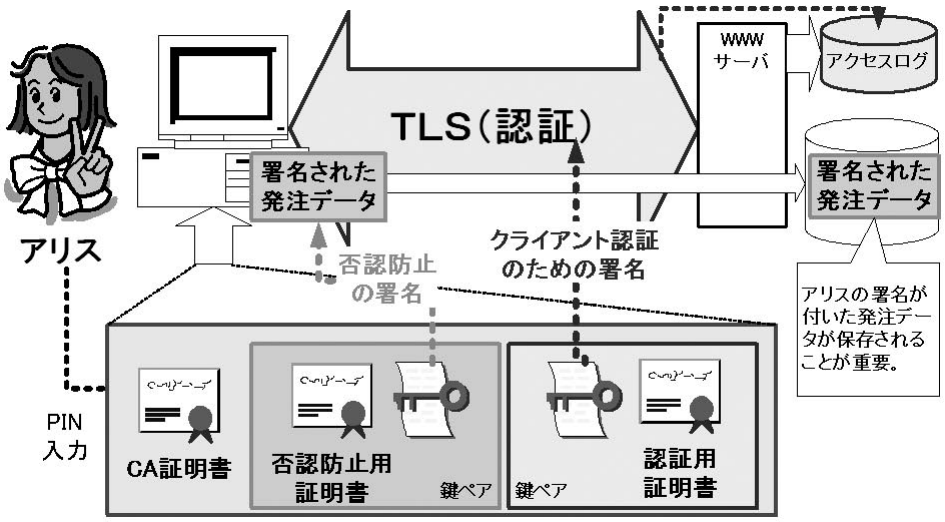


次に電子署名と電子認証を技術とビジネスの面から説明します。

3. 電子署名と電子認証の技術の違い

PKIを利用した否認防止のための署名(ここでは自署名と表現します)と認証(Authentication)は、共にプライベート鍵による署名(プリミティブな操作としての署名を単に「署名」と表現します)を利用して実現されています。しかし、自署名と認証では、そのプライベート鍵による署名の意味が大きく異なります。証明書の発行自体も、自署名と認証で使い分けている例もあります。図2に署名と認証を使い分けている例を示します。

図2



ここでアリスは、2つの証明書に対応した2つのプライベート鍵による署名を使いクライアント認証と文書への電子署名を行っています。PKIは、強い認証(Strong Authentication)を提供しますが、この強い認証を利用することによりセキュアにサーバに電子文書を渡すといったことができ、サーバ側ではそのアクセスログを残すことができます。しかし、それだけでは、電子契約などで要求される「実印での捺印」の代わりにはなりません。契約文書などに自署名を施す場合、アリスは、この文章の内容を熟読した上で自分の意志を持って自署名を行います。利害関係者間の文書のやり取り等では、アリスの自署名が施された電子文書自身が相手に送付され、その署名された電子文書が保存されることが重要になります。このような自署名は、否認防止の署名と呼ばれます。こうした否認防止目的で使用される証明書には、証明書に含まれる証明書拡張フィールドの鍵使用目的(Key Usage)に non-repudiation（否認防止）bit が設定されます。non-repudiation bit が設定された証明書に対応するプライベート鍵で(否認防止のための)署名を行う場合、そのアプリケーションは必ず署名者に自署名する文書を提示する必要があります。

自署名と認証では、その脅威も異なります。ネットワーク社会において、なりすましや盗聴といった脅威が語られていますが、自署名に対する脅威にもうひとつ、「内容を理解せず(させずに)自署名を行う(行わせる)」という脅威があります。例えば、「手形の裏書の意味を知らずにいわゆる自署名をさせられた」といったことが起きえます。PKIを利用した認証においては、その認証プロセスの中で乱数などに署名させて、その署名結果を検証することで認証を行います。認証のための署名においては、利用者は署名内容(認証プロトコル中の乱数など)を確認することはなく、また、認証のプログラムも利用者に意識をさせずに署名操作を行うことが多い訳です。それに対して自署名では、署名者が必ず自署名の対象となる文書を確認する必要があります。

以上のようなことからIDカードには、複数の証明書とプライベート鍵を格納して自署名や認証などの用途に応じて使い分ける例が多く見受けられます。欧州の市民カードや、米国の政府職員向けに発行されるPersonal Identity Verification（個人ID認証：PIV)等では、複数の証明書とプライベート鍵がIDカードに格納され、そのプライベート鍵を保護するためのメカニズムも異なります。欧州の市民カードの場合、認証用のプライベート鍵による署名では、

カード保有者がカードのPINを入力し保有者認証を行なった以降は、カードに記録された認証用のプライベート鍵が認証の都度自動的に署名します。これに対して自署名のプライベート鍵では、一回の自署名操作、つまりひとつの文書の自署名毎にPINの入力が必要な仕様になっています。これはカード自体が､「内容を理解せずに自署名してしまうこと」を防ぐ仕組みを有していると言えます。日本の公的個人認証サービスでは、証明書の non-repudiation（否認防止）bit が設定された否認防止目的の証明書のみが発行されています。従って、公的個人認証サービスの発行する証明書を電子認証(Authentication)に利用するのは避けるべきです。

次にビジネスの面から「電子署名」と「電子認証」の違いを考察します。

4. 電子署名と電子認証の用途の違い

電子署名は、契約文書などの経済活動等において必要不可欠な重要書類を紙文書から電子文書への移行を促すためには必須の技術です。電子署名法自体は、紙と押印を電子文書と電子署名に置き換える法律であり、主に既存の法制度に依存します。そのため既存の紙文書を中心とした業務が多い業界に対しての影響が大きいと言えます。

一方、ネットワークの安全、安心を提供するということ、特にネットワークを介した情報共有、機密情報保護等においては、電子署名ではなく電子認証が重要な役割を果します。また、現状の電子署名法に対応した電子署名は、非常に重要ではありますが、現時点において一般市民にとっては必要不可欠なものとは言いがたい面があります。一般市民にとっては電子署名以前に、実印を使用することもそれほど多くはありません。これに対してネットワークにおける電子認証は、インターネットが普及した現在では一般市民にとってもごく当たり前に利用されています。デジタルデバイドなどの問題はあるにしても、インターネットや社内イントラの利用者などは、ほとんどの場合、何らかのネットワークを介したリモート電子認証を利用しています。

このように当たり前に利用されているにも限らず、インターネット上で広く利用されている電子認証に対しては何の評価基準もなく、実際、低いセキュリティレベルの電子認証の利用に留まっていると考えて間違いありません。そして、低レベルの認証だけが様々なサービスに広範に利用されている事実は、結果としてインターネット上のサービスに対して不安を植えつけることとなり、そうしたことが、より高度なネットワークの利活用を阻むことになっている面があります。

前述したように旧来からの法制度には、ネットワークを介したリモート認証に対応するものがないこともあり、ネットワーク社会の安全、安心を提供する認証に対して、現状においては法制度、政策的な対応は何もない状況にあると言えます。インターネットビジネスは、法制度などからの規制に縛られず発展してきた経緯があり、結果として電子署名の要求は少ないというのが現状です。こうした業界でも高い付加価値のサービスを行うためには、一定の保証レベルを持った電子認証が必要とされているはずですが、認証の技術や運用の標準化、そのセキュリティ基準等は未整備であり、電子認証の利用者にとってもサービスを提供する側にとっても、その利便性とリスクを測りかねている状況にあると言えます。表1に電子認証(Authentication)と電子署名の比較を示します。

表１　電子認証と電子署名の比較

	電子認証（Authentication）	電子署名（Signature）
手段	現状は色々な認証のメカニズムが乱立しているが、広範に利用されているのは低レベルのものが多い	電子署名はPKI以外の現実的な手段はない
法制度	現状、法制度との結び付きはなく、認証のレベルもバラバラでユーザからは差がわからない（クライテリアが未整備）	電子署名法、e−文書法など法制度との結び付きが深い
マーケット＆利用	比較的新しい業界に需要がある。今後のユビキタスネットワーク時代のユーザ認証、機器認証の需要は測り知れない	紙に依存した比較的レガシーな業界に需要が多い。効率化するために電子化、IT化を推進したいが電子署名などの敷居の高さが壁になっている。
普及の鍵	普及には新しいビジネススキームの創造が重要（安全安心のための法整備が検討されるべき）	普及には業務知識、そして効率化のためのBPR（Business Process Reengineering）が伴うことを理解する必要がある
キーワード	ネットワーク上の安全、安心。ID管理、ID連携（Identity Federation）	e−文書法対応、電子文書保存、電子契約

それでは、色々な認証のメカニズムが乱立しておりユーザ(サービス利用者、サービス提供者)にとって差が分らない電子認証において、それらをわかりやすく利用するためのガイドライン作成などの動きはないのでしょうか。海外では、特に電子政府に関連した電子認証に関するガイドライン作りが積極的に行なわれており、次にその例を説明します。

5. 電子認証のガイドライン作り

認証に関連した技術は非常に幅広いものがあります。様々な電子認証技術はボトムアップに独自に発展してきた経緯があるため、それぞれの認証技術に依存した用語等も多く、これが混乱を招いている面もあります。認証技術の多様性は、その重要性とは裏腹に電子認証技術の全体像を非常に分かり難くしています。様々な認証技術が出現しており、そうした技術を利用した製品開発ベンダー等が、その技術の優位性をアピールしています。しかし、こうした技術が客観的に、まして経済性も含めて評価されることは、さほど多くありません。こうしたことからも経済性とセキュリティを考慮した認証のベストプラクティスを示すことは容易ではありません。

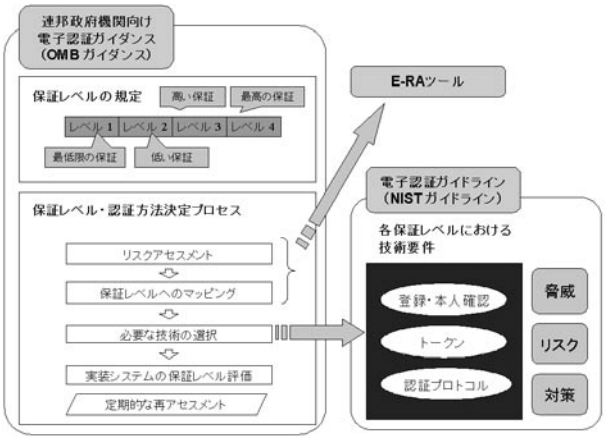
一般に電子認証を考えるには、認証対象のエンティティ（人、サーバ、デバイス等)、認証のメカニズム(認証方式、プロトコル等)、認証される範囲(認証ドメイン)などの明確化が必要になりますが、これからのネットワーク社会においては、より広い認証ドメインが求められ、この広い認証ドメインにおいて、広いが故に複数の認証対象のエンティティと、複数の認証メカニズムが混在していくことになると考えられます。

セキュリティへの要件が高まり個々の認証技術も複雑になる中で、用途に応じた認証のベストプラクティスを示すことが非常に重要になりつつあります。こうした動きが海外の電子政府における電子認証の取り組みとして見られるようになってきました。米国、英国、オーストラリア、ニュージーランドといった国々の電子政府では、複数の保証レベルを持った、また必ずしも特定の技術に依存しない電子認証のガイドラインを発行しています。その上で電子政府において利用する認証(Authentication)プラットフォームの

構築、または、検討を行なっています。これらの国々では、認証プラットフォームを使って電子政府のセキュリティレベルの向上を目指している訳ですが、それだけではなくコストの削減も目標にしています。

これらの中で実際に一番進展しているのは、米国電子政府における電子認証フレームワークを推進する米国e-Authenticationイニシアチブです。e-Authenticationイニシアチブでは、最上位のポリシを行政管理予算局(Office of Management and Budget：OMB)が電子認証ガイダンスとして提供しており、その中で4つの保証レベルを示しています。そして、この４つの保証レベルを前提に適応アプリケーションのリスク評価を行い、必要な保証レベルのマッピングを行なうなどの保証レベルと認証方法の決定プロセスを示しています。４つの保証レベルに対応した技術要件は、米国の標準技術局(NIST：National Institute of Standards and Technology)が「電子認証ガイドライン」として提供しています。この「電子認証ガイドライン」は、NISTの文書として「NIST Special Publication 800-63」として識別され、米国電子政府の情報セキュリティのための一連の文書のひとつという位置づけにもなっており、米国政府の調達などに要求される電子認証技術のガイドラインを実質的にも提供しています。図3に、これらの文書の関連を示します。

図３



このように電子認証は各国がガイドライン等の整備に乗り出した状況です。では日本においても既に整備が進んでいるはずの電子署名についてはどうなのでしょうか。

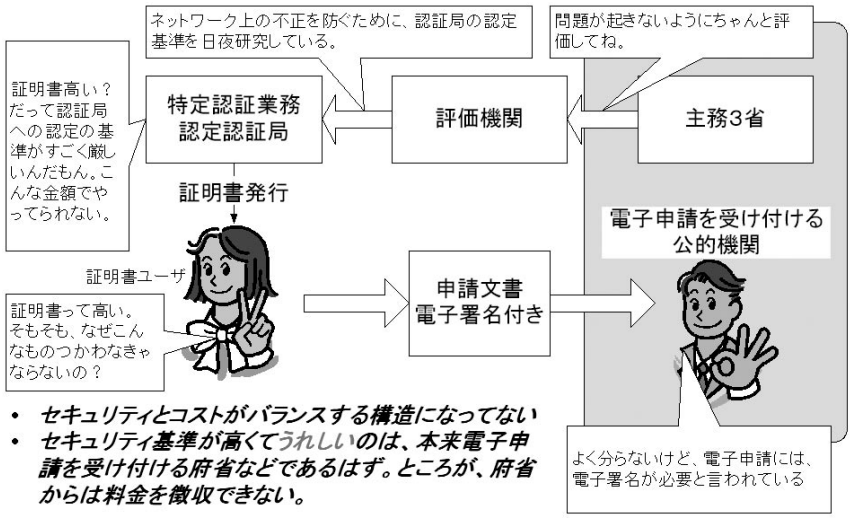
6. 電子署名の普及

ブロードバンド等のネットワークの普及や技術の発展に対して、電子署名の普及が進んでいないという声が強いのが現状です。電子署名の普及の課題は、技術的な問題以外の部分にあります。「紙と印鑑」の文化から「電子文書と電子署名」の文化へ移行するために、まずはこれまでの慣習の壁を越える必要があります。また、企業内だけであっても「紙と印鑑」から「電子文書と電子署名」への移行は、業務の本質的な変革が要求されます。電子署名がなされた電子文書は、これまでITの普及が困難だった業務を劇的に改善する可能性も秘めています。電子署名を利用した、更に効率的な電子社会へと移行させるために、これまでの人々が「最適」と思ってきた実務の意識を変える必要もあるかもしれません。

法制度との関係も深い電子署名は、法制度的な課題も多々あるという指摘もあります。電子署名法、IT書面一括法、e-文書法などIT関連の法制度の整備は進んでいますが、民事法領域のIT化対応には課題が多く、例えばこれまで商取引を支えてきた手形法は、紙の手形を前提としています。結局のところ、現在の社会は「紙と押印」を前提にした社会であり、様々な法制度も紙文書を前提に最適化されており、電子文書を前提にした社会への移行には大きな変革を伴うことになります。またIT技術による効率化も重要ですが、法制度の観点からは、同時に不正に強く、透明性の高い社会を目指すべきです。そのためには電子署名の普及は重要な意味を持つはずです。

電子署名の普及は、電子署名法自体がネックとなっている面もあります。電子署名法に付随して電子署名法特定認証業務認定制度がありますが、この認

図4



定制度は、良くも悪くも高い保証レベルの証明書を自然人に発行する認証局の認定制度だと言えます。この高い保証レベルは、結果として高いセキュリティ要件の電子署名に利用できることになりますが、その反面高いコストもかかります。電子署名法は、ネットワーク社会の基盤となる法律であり、そのため、この電子署名法の不備による不正などを防がなくてはならないという強い意向が働き、認定基準も非常に厳しいものになっています。これは、不正等が起きにくい一方、使われにくい状況も生み出し、結果としてネットワーク社会の安全、安心を提供するはずの電子署名の普及を阻害している可能性があることに注意すべきです。図4に電子政府における電子署名法特定認証業務認定制度の課題を示します。

2005年に施行された通称e-文書法に関連した動向としてタイムスタンプサービスの普及があります。タイムスタンプサービスの主な方式のうちのひとつは、時刻が何らかの形で保証されたサーバが行なう電子署名によって実現されます。ところが電子署名法は、自然人によるいわゆる自署名がその範疇であり、こうしたサーバによる署名は、電子署名法の対象外となっています。ユビキタスネットワーク社会においては、認証を要するデバイスが人口よりもはるかに多く、またサーバによる署名が、人間が行うよりもはるかに多く想定されます。このような将来社会に対する法制度は、これまでの法制度の延長上にある「電子署名法」などの枠組みだけではカバーできず、新たな枠組みも検討される必要があると考えられます。

■ まとめ

ネットワーク社会への移行という環境変化により、今では顔を突き合せなくてもリアルタイムの取引ができるような状況になりつつあります。これまで契約者同士の取引の時間的地理的な距離のために紙ベースの処理(署名)が必要だった業務であっても、オンラインの電子認証によりその大部分を解決できるように、ビジネススキームからして抜本的に変わってしまえば署名でなく電子認証で済みます。このようなネットワーク社会では、サービス自体が信頼のおけるものであれば、認証及びその後の手続きのログなどを証跡とするといったことが一般的だと考えられます。2001年施行の電子署名法をはじめとする現行のIT技術の関連した法制度は、こうした環境の変化に追随できていない側面があります。こうした中、認証にお

ける基準等は未整備であり、これらにも起因するインターネットバンキング等における犯罪は、「サービス自体が信頼のおけるもの」といったことに疑問を抱かせ、インターネット上のサービスの信頼を揺るがしています。このような状況ではe-Japan戦略の次の目標とされるＩＴ基盤の利活用は進まないでしょう。

一方、電子署名が役に立たないかというと、全くそういったことはありません。「認証とログ」は特定のシステムに依存するため、長期間のセキュリティ（たとえば重要文書の長期保存など）や、組織を超えた広域のセキュリティといったことに対応できないという問題があります。標準化されたデータフォーマットを使い電子署名が施されたデータは、特定のシステムに依存しない独立したデータとしての普遍性を持ちます。これは、正にネットワーク社会に求められていることであるはずです。そして、IT化、ネットワーク化は、利便性のみならず、新たな不正行為をも招いていますが、電子署名は、こうしたことに対抗する技術であるはずです。

電子署名と認証の違いを中心に説明してきましたが、安心・安全なネットワーク社会を構築するためには、これらの技術を適切に使い分けるための技術、法制度、ビジネスモデルの三位一体となった検討がなされるべきでしょう。電子署名の普及が思うように進まないのは、技術、法制度、ビジネスモデルのバランスの悪さに起因しているように思われます。今後、安心・安全なネットワーク社会を目指していく上では、電子署名・認証の更なる技術開発、法制度の整備、新たなビジネスモデル創造などの更なる努力が求められます。

6. 参考

米国のE-Authentication
http://www.cio.gov/eauthentication/
電子認証技術ガイドライン（SP800-63）
http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
偽造キャッシュカード問題と認証システムの考察
http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf
電子署名・認証利用パートナーシップ 2004 年度報告書
http://www.japanpkiforum.jp/shiryou/FY2004/fy2004_jesap_report.pdf
電子署名法の在り方と電子文書長期保管に関する現状調査報告書　平成17年3月（財）日本情報処理開発協会

第 63 回 IETF 参加報告

NPO 日本ネットワークセキュリティ協会
安田　直義

第 63 回 IETF 参加メンバー

セコム株式会社 IS研究所
島岡 政基
富士ゼロックス株式会社
稲田 龍
富士ゼロックス株式会社
黒崎 雅人
(社)日本ネットワークインフォメーションセンター
木村 泰司
NPO 日本ネットワークセキュリティ協会
安田 直義

2005年7月31日から8月5日までパリ凱旋門近くのLe Palais des Congress de Parisにて開催された第63回IETF（http://www.ietf.org/）ミーティングに、JNSA ChallengePKIプロジェクトとして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で電子メール上での議論を行い、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「オフライン」での会合を行っている。

今回のミーティングは、36カ国(前回比＋8ヶ国)、1,454人(前回比＋287人)の参加で行われた。ヨーロッパでのミーティングであり、バカンスをかねて家族づれで参加している人も多く、前回の米国開催より参加者は増えている。

今回のミーティングの参加目的と概要は、次のような3点にある。

1. PKI相互運用に関するMulti-Domain PKIの問題について、セコムトラストネット島岡氏のMulti-Domain PKI I-D を中心とした内容に関して、ETSIのPatrick Guillemin氏(以下Patrick氏と表記する)と広く意見交換を行った。Patrick氏は、ETSI（European Telecommunications Standards Institute）のPlugtests Technical Managerをしており、ヨーロッパの相互運用性に関するキーマンである。Patrick氏からETSIを始めとするヨーロッパや世界的な認証に関する動向に関して話が進み、主にUTF8String問題に関して、2006年1月16～17日にSophia AntipolisのETSIで開催されるETSI Security Workshopで講演するために島岡氏等Challenge PKIのメンバーを招待したい、という要請があった。
2. Hash BOFを始めとするハッシュ関数の脆弱性問題に対する最新動向を議論しているWGに参加した。SHA-1の対衝突性を向上するために下記のような提案が行われ議論された。
   - Truncate SHA-256
   - Random Hash
   - Preprocessこれらに関して、NIST Cryptographic Hash Workshopでの継続議論の告知が行われていた。
3. PKI関係だけではなく、情報セキュリティ全般の最新動向を知るため、Security Areaの主要WGに参加する。

SHA-1問題は、新しいアルゴリズムへの移行がポイントになりそうである。また、PKIマルチドメイン問題に限らず、UTF8コードの問題はしばらくはトレンドになる感じがする。匿名認証の関心も高まっており、認証自体の考え方が整理されようとしている。

PKI 相互運用に関する ETSI との意見交換

Patrick Guillemin氏と、Multi-Domain PKIを中心としたPKI相互運用に関連する問題について、広く意見交換を行った。

Challenge PKIの近況説明

島岡氏から、ChallengePKIに関する近況を説明した。

- マルチドメインPKI関連の話題
- 相互運用テストスィートの更新状況

マルチドメインPKI関連として、Multi-Domain-

PKI-I-D（mPKI I-D）の更新状況について説明し、mPKIに関する情報交換などを行った。

また、UTF8String問題に関しても情報交換を行い、ヨーロッパでのUTF8String問題への関心度が高いことを聞いた。

昨年のIETFでPKIX-WGに発表した相互運用テストスィートのその後の改良などについて情報提供と情報交換を行った。タイムスタンプやS/MIMEについてのテストケースを扱えるように拡張されていることについて、特に興味を示された。

Patrick Guillemin 氏との打ち合わせの風景
(左から：黒崎氏、Patrick 氏、稲田氏、木村氏、島岡氏)

JPNICのIPアドレス認証局の説明

木村氏から、JPNICで実現しようとしているIPアドレス認証局について説明がなされ、その後ディスカッションが行われた。IPアドレス管理者とJPNICとの間で双方向認証を行うというメカニズムだが、実用的に運用する際の問題点などについて、忌憚の無い議論が行われた。

ETSI Security Workshopへの招待打診

このようなディスカッションを行った後、Patrick氏からETSIを始めとするヨーロッパや世界的な認証に関する動向に関して話が進み、Patrick氏から、主にUTF8String問題に関して、2006年1月16～17日にSophia AntipolisのETSIで開催されるETSI Security Workshopで講演するために招待したい、という要請があった。

招待講演のお誘いが9月12日に届いており、島岡氏、稲田氏を中心に参加する方向で調整している。

参考：

http://portal.etsi.org/securityworkshop/Home.asp

> Date: Mon, 12 Sep 2005 15:49:01 +0200
> From: "Dionisio Zumerle"
>
> （中略）
>
> I have been discussing with Patrick on JNSA and UTF8 in Certificate/PKI.
>
> I think the occasion is ideal to invite you to the ETSI Future Security Workshop (see http://portal.etsi.org/securityworkshop/Home.asp) to be held in ETSI's Headquarters in Sophia-Antipolis, France on 16-17 January 2006.
> The workshop is about revising what has been done in the security areas (so PKI and Signatures is a significant part of it), and deciding on what has to be done from now on.
> I think it would be a good occasion to present your views and ideas. If of your interest you could propose a presentation.
>
> In parallel, I would like to have your view on a JNSA possible participation in ETSI's work on electronic signatures (TC ESI).
>
> Kindest Regards,
> Dionisio Zumerle
> ETSI Technical Officer

Hash BOF

8月1日 18:15～19:45に開催された。出席者は100人程度以上で満杯状態だった。HASHは直前にSHA-1の脆弱性が発表されるなど、高い関心を集めており、熱気にあふれていた。IETFでHashに関するBOFが開催された背景と論点、結論をまとめると下記のようになる。

- **背景：**
  - SHA-1に対する衝突攻撃の成立に対する検討が必要

- ハッシュ関数の衝突攻撃(Collision Attack)にフォーカスして議論
  ☆原像攻撃(Pre-image Attack)についてはOut of Scopeである

● **論点:**
- IETFの中で議論できるWGを立ち上げるべきか?
- ハッシュ関数の見直しを図り標準化すべきか?

● **結論:**
- IETFはハッシュ関数の設計には取り組まず、あくまでハッシュ関数を使ったプロトコルの設計をする
- NIST Workshopで、より詳細な情報が集まるはずなので、次回IETFで再度検討すべきだろう

次に、Hash BOFでの特徴的なプレゼンテーションを紹介しておく。

NIST Cryptographic Hash Workshop

NISTのCryptographic Hash Workshop開催の告知が行われ、議論の継続とIETFで対応できない課題についての議論を行いたいとの紹介があった。

● **発表者**
- NIST/CSDのWilliam Burr氏
- 口頭でのアナウンスのみ

● **開催要領**
- 期間: 2005年10月31日～11月1日
- 場所: Maryland州 NIST

● **詳細**
- http://www.csrc.nist.gov/pki/HashWorkshop/index.html
- SHA-256へ移行するにあたっての課題(移行、対症療法)
- 後述の一部のSHA-1対症療法の紹介

新しいハッシュ関数の展開

SHA-1に変わるハッシュ関数の実装とそれまでの対策についての検討を示した。

● **発表者**
- Steve Bellovin氏(元Security AD, コロンビア大)
- Eric Rescorla氏(TLS WG Chair, IESG)

● **課題**
- 次の新しい実装が入手できるまでの対策を考える
- S/MIME, TLS, IPsec/IKEについてハッシュ関数の影響を分析する
- ほとんどのプロトコルにおいて、移行のためのBCPが必要だろう

メッセージ前処理によるSHA-1の対衝突性向上

SHA-1を若干モディファイし、問題となった対衝突性を向上させるアイディアが説明された。

● **発表者**
- Russ Housley氏(元RSA社, Security AD)
- 現状の問題点の指摘
- SHA-1の耐衝突性低下のメカニズム等

● **提案内容**
- メッセージ前処理(SHA1pp)による耐衝突性向上を提案
- 前処理方法にはいくつかのバリエーションがある
  ☆2つの変換方式:
  Message WhiteningとMessage Interleaving
  ☆2つの実装方式:
  within SHA-1とoutside SHA-1
- 既存のSHA-1と互換性が高い

● **結論**
- 最小の影響でSHA-1を一時的に延命させる技術
- 最終的には新しいハッシュ関数が求められる

乱数をハッシュの一部に含める

ハッシュの一部に乱数を含めることにより、対衝突性を向上させようという提案で、以下にランダムなSaltを生成するかを熱心に説明していたが、かなり数学的な内容を含んでいたので、難解だった。

● **発表者**
- Ran Canetti氏(IRTF CFRG Chair, IBM)

● **提案内容:**
- Use Hr（x）instead of H（x）
  r is a random "salt value"
- To sign a message x:
  With new random salt r, set h = Hr（x）
  s = RSA-1（encode（h,r））
  The signature is the pair（r,s）

次世代ハッシュ関数の提案

NISTのTim Palkから、ハッシュ値長を固定と次世代ハッシュ関数の提案があった

● **発表者**
- Tim Polk（PKIX WG Chair, NIST）

● **次世代ハッシュの課題**
- ハッシュ値の長さを仮定しているアプリが多い

● **提案**
- ハッシュ値を160bitに切り捨て、互換性を保つ
- 耐衝突性を低下しないためにメッセージにIVを付与してからハッシュを取る

● **懸案**
- IVの計算方法、安全性証明などが課題

3つのアプローチの比較

以上の提案の新しいアプローチを比較してみた。それぞれ特徴があり、今後の議論が待たれる。

	Truncate SHA-256	Random Hash	Preprocess
Hash Output Truncation	√		
Change Signature Size		√	
Randomness Required		√	
Replace SHA1 Code	√		
Change Message before Hashing		√	√
Execution Cost (time increase)	50-200% Depends on SHA-256 slowdown on platform	(not %) Depends on random generation	33-100% Depends whitening parameter

セキュリティエリアの動向

今回のIETFでのセキュリティエリアでの動向は下記のような感じであった。

● **PKIX WG**
- SCVP, 3280bis, CAdESなどの議論が進んでいる

● **LTANS WG**
- "Notary"から"Data Validation and Certification"へ用語変更した

● **MASS（Message Auth Signature Service）BOF**
- DKIM（Domain Keys Identified Mail)にフォーカスしている
- まずは "threat analysis" から始めようという方向でで進んでいる

● **SAAG**
- ITU-T X.805の紹介
  ☆Security Architecture for System providing End-to-end Communications
- Unicode Security Considerations（TR#36)の解説がされていた

● **Alien BOF, BTNS WG, PKI4IPsec WG, etc.**
- 上記のWGでも活発な議論があったようである

セキュリティエリアのまとめ

セキュリティエリアの全体的な流れとして、SHA-1ハッシュ関数問題、マルチドメインでの相互運用性、UTF8コード問題、匿名認証等々の話題がホットであった。

● **SHA-1問題**
- 新しいハッシュ関数への移行方法が鍵である
- NISTのHash WorkshopはWatchしておく必要があるだろう
- SHA-1互換で安全なハッシュの検討が必要
- SHA-256への移行は本当に可能だろうか？

- 2回の移行プロセスを踏むインパクトやコストを議論しなければならない

● **マルチドメイン問題**
- PKIに限らずマルチドメインでの相互運用の課題は大きい
- Unicode問題はしばらくトレンドになるかもしれない

● **その他**
- 認証における仮名、匿名などの使い分けはIETFでも関心が高まってきている
- もしかするとSecurity AreaよりもApplication Area, Internet Areaの方で議論は進んでいるかも知れないのでもう少し調査が必要だろう

村井先生が Postel 賞を受賞

IETF Plenaryで慶應義塾常任理事、WIDEプロジェクト代表の村井純教授がPostel賞を受賞した。

Postel賞は、故Jonathan Postel氏にちなんで1999年ISOCが設置したもので、インターネットに多大な貢献をした人に贈られている。村井氏は、歴代7人目の受賞でアジア初となる。アジア太平洋地域でのInternet普及への貢献と、IPv6の技術開発と普及への努力が受賞理由である。

For his vision and pioneering work that helped countless others to spread the Internet across the Asian Pacific region.
アジア太平洋地域のインターネットの展開に注がれた、彼の広い視野と開拓精神に基づく計り知れない貢献に対して。

端末ルーム

今回のIETFのターミナルルームは、場所の制約のせいと思われるが、24時間営業をしていなかった。会場と隣接しているConcorde La Fayetteホテルのロビーと、会場向かいのLe Meridien Etoileホテルのロビーでは24時間の接続サービスが行われていた。今回は無線LANの802.1XとWPAが使えるようになっていた。インターネット接続の概要を下記にまとめておく。

● 有線LAN（1ヶ所）
- ターミナルルームのみ

● 無線LAN（3ヶ所）
- 会場全体（夜10時まで）
- Concorde La Fayette（ホテル, 24時間接続）
  ☆会場に隣接
- Le Meridien Etoile（ホテル, 24時間接続）
  ☆会場の向かい
- 今回初めて802.1X認証が提供された。（無線LANのみ）
  ☆WPA _ PEAP/MSCHAPv2
  ☆France Telecomから発行されたサーバ証明書

情報セキュリティ推奨教育検討 WG

WG リーダー
セキュリティ・エデュケーション・アライアンス・ジャパン　持田　啓司

■ 設立趣旨

情報セキュリティ対策における人材育成の必要性は叫ばれているものの、現状の人材育成においては、製品販売の必要性のみの教育や、短期的・場当たり的なものとなっているものが目に付きます。このため、本来必要な、組織全体を総括して各種対策を行うための人材配置を前提とした教育プログラムが提案できているとはいえない現状です。

本ワーキンググループでは、組織の底辺からそれぞれの情報セキュリティ専門職種への育成プロセスを示すことのできる教育の在り方を検討し、組織として隙の無い人材育成構築のための教育プログラムを検討することを目的としています。

この中では、現状ある教育コースを用いて、現在必要とされている職種別人材育成フローの提案を行うとともに、組織体制についても、情報セキュリティ専門職種の検討により、日本に合った新たな組織デザインを試みることとしています。

■ 検討フェーズごとの想定成果物

1. 情報セキュリティスキル項目の検討

(ア) 作業内容：

情報セキュリティ対策を行う上において必要となるすべてのスキル項目の検討を行います。

スキル項目については、大項目・中項目・小項目 (キーワード) でリスト化します。

(イ) 参考資料：

① 経済産業省教育研究会報告書
　カリキュラム
② 情報セキュアド試験スキル標準
③ 情報セキュリティスキルマップ
④ CISSP cbk

(ウ) 作業詳細：

参考資料を基に、最新技術項目の検討も加えながら、詳細スキル項目まで作成します。

2. 対象教育コース (資格) の調査・検討

(ア) 作業内容：

市場にある情報セキュリティ教育 (資格) を抽出し、そのカリキュラムを調査して、前フェーズでまとめたスキル項目と比較しながら教育内容の検討を行います。

(イ) 参考資料：

① 経済産業省教育研究会報告書
　教育制度および資格認定制度の現状
② ITSS ユーザー協会 資料 (ITSS とベンダー試験の関係)

(ウ) 作業詳細：

教育コースアウトラインとスキル項目とを比較し、知識のみか実技演習があるかも含めながら確認し、教育実施範囲を明確にします。

3. キャリアパスの作成

(ア) 作業内容：

情報セキュリティ専門職種ごとの研修ロードマップを検討し、チャートで表現します。

(イ) 作業詳細：

量・質ともに不足が叫ばれている数職種をピックアップし、必要スキルをスキル項目の知識のみで良いのか、実技演習も必要かなどを検討し、職種ごとの必要スキルを明確にします。

4. 組織デザインの検討

(ア) 作業内容：

あるべき姿の組織内での情報セキュリティ専門職種を検討し、組織デザインの検討を行うことにより、最適解としての組織デザインをチャートで表現します。

(イ) 参考資料：

PeopleCMM　etc

(ウ) 作業詳細：

情報セキュリティ対策のための組織デザインと、その構成要因としての職種を明示し、それぞれに必要な教育及び、それぞれのキャリアパスを提案します。

■ WG の運営方針

- 月 2 回程度の会合を工学院で行い、全体の意見調整を行います。
- 成果物は、分担しながら持ち帰って作成し、会合の場で調整します。
- 成果物については完成形ではなく、2005 年版として発表し、追加要望があるものは次年度検討します。
- メンバー加入は随時受け付けています。ご興味のある方は、JNSA 事務局までお問い合わせください。

■ スケジュール

作業項目＼作業月	05/7	05/8	05/9	05/10	05/11	05/12	06/1	06/2	06-3
キックオフ・方針決定	△								
必要スキル項目検討	△→	→→→							
教育コース (資格) 調査	△→	→→→→→→→→→							
キャリアパス作成	△→	→→→→→→→→→→→							
Web 公開（第 1 回目）						△			
組織デザイン検討					△→	→→→→→→→→→→→→→			
Web 公開（第 2 回目）									△

スパイウェア対策啓発 WG

WG リーダー
株式会社アークン　蛭間　久季

■ 設立趣旨

近年スパイウェア（不正プログラム）を利用し他人から ID・パスワードなどを不正に入手し、本人になりすましネットバンキングから不正に預金を引き出すなど、様々な犯罪が大きく世間を賑わすようになりました。ウィルスは自己増殖し、ファイルを破壊したり他人に感染させたりすること自体が被害となります。故に利用者から見て被害が簡単に見極められるケースがほとんどです。

しかしながら、スパイウェア（不正プログラム）は利用者が意図しないところで密かにインストールされ犯罪に利用される事が多く、利用者本人が気づかないケースが往々としてあります。またスパイウェア自体の定義が日本国及び海外諸国において、具体的に確立していないのが実態です。

当 WG ではスパイウェアの日本版定義の策定も含め様々な団体、官公省庁との連携によりインターネット利用者へのスパイウェア（不正プログラム）対策の知識向上を目的として安全な情報通信社会の一助となるように啓発活動を幅広く実施する事を主たる目的として設立致しました。

■ 活動内容

当 WG では具体的に下記活動を予定しています。

1) スパイウェアの定義策定（現在 IPA 様と連携して日本版スパイウェアの定義を策定しています）
2) 他の WG との意見交換や勉強会の実施
3) 官公省庁や産業界（団体）などへのスパイウェア対策の啓発協力の呼びかけとスパイウェア関連に関する勉強会の実施
4) 海外におけるスパイウェア対策啓発の調査研究など

■ 具体的な活動例

当 WG では啓発の内容などにより都度サブ WG を設立し活動を行っています。

最近の例をあげると下記のように分類されます。

1) メディアを通じてスパイウェア対策啓発の記事執筆と寄稿
2) 他団体と共同してのスパイウェア対策に関する講演
3) 他団体と共同してのスパイウェア対策の啓発活動
4) IPA 様と連携してスパイウェア定義の策定と Web サイトの構築

■ 今後の具体的な活動指針

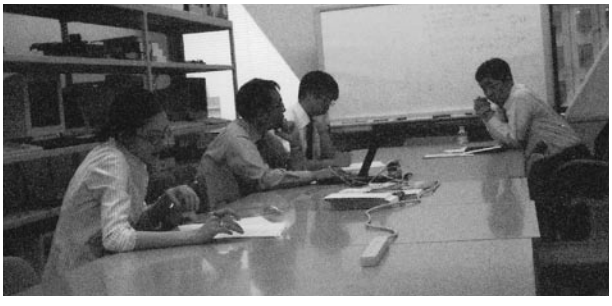
今後は技術革新によりウィルスとスパイウェアの垣根も段々と無くなっていく事が想定されます。欧米では「悪意のある」といった意味でウィルスもスパイウェアなども総称して「マルウェア」などと言われています。

これからは個人や企業を問わず、私達の生活自体にインターネットがより身近にかかわり、より便利な生活になる事でしょう。所謂本格的なユビキタス社会の到来です。

当 WG では対策啓発を教育現場・民間・行政を問わず幅広く「草の根運動」のごとく実施していきたいと思っています。

■ WG の運営

1. 月に 1 ～ 2 回程度の会合を工学院にて開催
2. 成果物のひとつであるスパイウェア対策ポータルサイトを 2006 年度内に完成し、幅広く産業界に告知しリンクしてもらう
3. WG 全体ではリーダーを蛭間が務めるが、啓発内容によってサブ WG を設立、サブリーダーを選任し活動する
4. メンバー加入は随時受け付けています
   御興味のある方は気軽に会合に御参加頂くか、事務局まで御問合せ下さい



中小企業向け個人情報保護対策 WG

WG リーダー
伊藤忠テクノサイエンス株式会社　市川　順之

■ 設立趣旨

2005年4月以降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きます。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、運用編としてまとめることを目的としています。

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(業種)の幅を広げたいと考えています。

中小企業は部門が分かれていない場合も多く、その場合のセキュリティ体制、対策についても研究します。

■ 想定成果物

中小企業向け個人情報保護対策マニュアル、というのを作成したいと考えております。

■ 目標レベル

事例やテンプレート等も充実させ、中小企業のオーナーが成果物を読んで「自社でも出来る、よしやろう!」と思える内容を目標としています。

■ 活動内容

月に一度の定例ミーティングを実施して各WGメンバーの活動報告や作成物の内容確認等を行っています。またアンケートについては西日本支部の「セミナー運営WG」と連携し集計させていただいています。
WG内は「コンサルティングチーム」「研究チーム」に分かれており、コンサルティングチームがモニタ企業へのコンサルティングを実施してその結果を成果物にまとめ,「研究チーム」がテンプレート作成等を実施していますが、現状明確に作業を分けているわけではありません(負荷に応じてどちらもやってもらっています)。

■ 最後に

メンバーがアクティブに参加してくれているので大変ありがたいです。モニター企業の方々も積極的で常に新鮮な感覚を持ってミーティングが出来ているので良いのですが、我々としてはWGメンバー、モニター企業をもっと増やす必要があると考えていますので興味があれば是非ともご参加お願い致します。

会員企業ご紹介⑮

株式会社エス・アイ・ディ・シー

http://www.sidc.net

COREsecureの概要

COREsecure開発背景

今日、利用可能なセキュリティ製品で、セキュリティの「最弱な要素」の一つとされているオペレーティング システム(OS)に焦点を当てている製品は非常に限られています。株式会社エス・アイ・ディ・シー（以下SIDCという)は、この事実をいち早く認識し、COREsecure の開発を開始しました。ファイアウォールや侵入検知システム(IDS)は、境界でのセキュリティ保護において非常に有効な手段です。しかし、これらの手段では、システムの「核」であるOSを攻撃者のアクセスから守ることはできません。

ウイルス対策ソフトウェアに関しても同様のことが言えます。ウイルス対策ソフトウェアは、既知のウイルスやワームによる感染からシステムを保護するために開発されたものです。よって、攻撃者によるOSへのアクセスを防止することはできません。マイクロソフト社は、互換性のないソフトウェアや基本的なセキュリティ問題に対して、定期的にセキュリティ修正プログラムや更新をリリースしています。しかし、同社の提供するこのようなソリューションは、単に一時しのぎの対策でしかなく、いずれ攻撃者にOSの「核」へのアクセスを許可してしまいます。攻撃者の狙いまたは目標は、OS上で「Admin」権限を取得することです。攻撃者に「Admin」権限を取得された場合、メールプログラム、機密データ、企業情報、顧客リスト、クレジットカード番号、価格リスト、企業文書、計画書など、コンピュータ上にあるほとんどすべての情報を支配される恐れがあります。

SIDCは、セキュリティを専門に取り扱う企業であるため、ユニークで効果的、かつ知的に設計されたセキュリティ製品を開発することができます。

これまでIT専門家は、INFファイルの作成など、様々なテクニックや技術を駆使して手動でOSの設定を調整する方法を考案せざるを得ませんでした。そして、これらのファイルを、OSの設定にインポートし、数多くのデフォルト設定からカスタマイズ化を実行しました。そうすることで、OSを攻撃に対してより堅牢にすることに成功したのです。

残念なことに、OSの大部分は、購入後、メーカが設定したデフォルト設定のままインストールされます。これらデフォルト設定は、幾度となく脆弱であることが立証されています。また、これら設定を変更せずにおくと、OSを脆弱なまま稼動させることになり、サーバが直ちにハッカーや不正ユーザーの攻撃の的になってしまいます。さらに、ほとんどのサーバは、インターネットに接続後20分以内に、第三者によってスキャンされることが明らかになっています。スキャンされたサーバが脆弱なデフォルト設定のまま稼動している場合、ほぼ間違いなく攻撃の対象となるでしょう。

COREsecureの特徴

● かつてない新しいセキュリティ製品

弊社の知る限り、COREseucreのような機能性およびデザインを提供するセキュリティ製品は他にありません。中でも、「ロールバック機能」は業界初の画期的な機能です。また、COREmonitorと併用することで、他の製品とは比較にならないほど、システムのセキュリティを強化することができます。

● OS のセキュリティ保護

COREsecureは、コンピュータの「核」であるOSを保護します。OSを攻撃から守るための、最後のセキュリティ層を提供します。

● 使用は簡単

COREsecureは、ユーザフレンドリーに設計されており、使用が簡単です。手動では面倒、または時間のかかるプロセスをツールによって自動的に行うことで、セキュリティ知識のレベルに関係なく、誰でも簡単にセキュリティを強化することを可能にしました。

● システムの「核」を保護

セキュリティ製品メーカの大部分は、境界セキュリティを中心とした製品を開発しています。COREsecureは、システムの「中枢神経」ともいわれるOSのセキュリティを強化します。

● 高い費用対効果

COREsecureは、他の製品と比べ、非常に手ごろな価格で入手することができます。COREsecureが自動で行うところの操作を、適度なセキュリティ知識を備えたIT 技術者が手動で実行しようとした場合、サーバ1台につき、推定で約2日間の時間を要します。このプロセスは、まず英語で提供されている情報を収集することから始まり、セキュリティパネルの各設定を手動で変更し、さらには設定の変更後、すべて正常に動作するかどうかの確認を行わなければなりません。それに対して、COREsecureのインストールは、10分ほどで完了します。

● 気分はセキュリティ専門家

企業のサーバシステムのセキュリティを強化し、安全を保証することは、その責任を担うIT担当者にとって決して簡単なことではありません。しかし、COREsecureを使用すると、IT担当者は、まるでセキュリティ専門家であるかのように業務を遂行することができます。COREsecureは、セキュリティ専門家によって設計、開発されたツールです。このツールの開発に要した知識や経験は、軽視できる、または簡単に真似できるものではありません。

今回SIDCからCOREsuiteシリーズとしてCOREsecureを販売することになりました。ご興味などありましたらぜひご連絡を頂ければ幸いです。

お問い合わせ先

株式会社エス・アイ・ディ・シー（SIDC）

〒158-0097 東京都世田谷区用賀 4-10-1

世田谷ビジネススクエアタワー 3F

Tel：03-5717-6540 ／ Fax：03-5717-6541

HP:http://www.sidc.net

株式会社コネクタス

http://www.connectous.co.jp/

CONNECTOUS

高まる電子メール保存のニーズに応えるメールタンクシリーズ

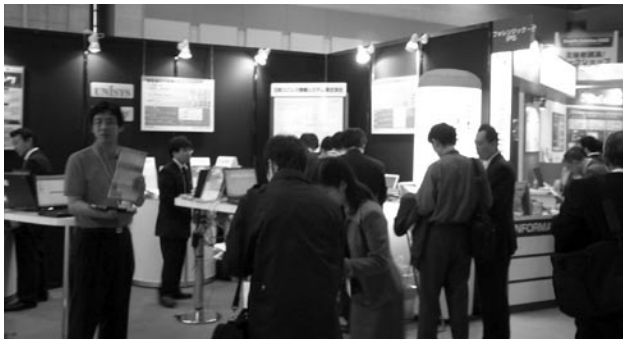
まだまだ電子メールを社員個人に管理させている企業は多いというのが実情ですが、しかし、それで大丈夫なのでしょうか？e-文書法が施行され、重要な取引や交渉の証拠として、電子メールの重要性はますます高まっています。既に米国の金融機関や上場企業に対しては、企業改革法(SOX法)によって、メール保存は義務づけられており、日本でも近い将来法令化されることは確実視されています。個人情報保護対策や内部監査の証拠集めとして、ネットワークフォレンジックが注目されています。その一環として、メール保存のニーズも当然日に日に高まって来ています。
私たちコネクタスは、このような「メール保存時代」の到来を早くから予測し、安い・簡単をコンセプトに手軽なメールアーカイブ機器としてメールタンクシリーズの開発･販売を行っております。

コネクタスの技術が 日本ユニシス情報システム様の 「メール監査/保存サービス」に採用

このような社会的背景の中、日本ユニシス情報システム株式会社様(以下､日本ユニシス情報システム様)もASPサービス「メール監査/保存サービス」を開始し、このコア技術には、弊社のメールアーカイビング技術が採用されています。採用されたメールアーカイビング技術は、メールタンク開発で培ってきたメール保存技術を発展させた、弊社独自の技術です。既にメールアーカイブ機器として一定の評価を得た「メールタンクシリーズ」の開発実績と、多くの大手優良企業への販売実績が高く評価され、弊社の技術が同サービスへ採用されたものです。

Security Solution 2005出展のご報告 大規模ネットワークに対応した「フォレンジアム」を参考出展

また､弊社コネクタスは､2005/10/26(水)～28(金) の期間、東京ビッグサイトで開催された「Security Solution 2005」(日経ＢＰ社主催)にも出展いたしました。その際弊社は、日本ユニシス情報システム様と共同でブースを運営し、弊社のメールタンクシリーズと、日本ユニシス情報システム様のASPサービス「メール監査/保存サービス」のご紹介を大々的にご紹介させていただき、大盛況に終わらせていただきました。会期中、参考出展として、大規模ネットワークに対応したメールタンクシリーズの新製品「メールタンク・フォレンジアム」の出展もさせて頂き、こちらにも多くの方から反響をいただくことができました。メールタンク「フォレンジアム」は、従来のメールタンクシリーズではカバーできなかった大規模なネットワークに対応したメールアーカイブソリューションです。この製品は、日本ユニシス情報システム様のASPサービス「メール監査/保存サービス」のために開発したメール保存･監査技術をフィードバックしたものです。
柔軟なマルチアドミン機能や、添付ファイルの中身までも精査できるコンテンツフィルタリング機能。拡張子やMIMEタイプではなく、添付ファイルの「中身」でファイルタイプを判断する添付ファイルポリシー設定機能など、膨大な数のエンドユーザからのヒアリングを元に実運用の際に必要となる様々な機能を多数備えています。数千名クラスの大規模ネットワークや、顧客への「メール保存サービス」の提供を考えておられているISP事業者様を対象として､来年初頭の発売を予定しております。ご期待ください。



お問い合わせ先
株式会社コネクタス
〒108-0023 東京都港区芝浦4丁目16番25号
第3安全ビル
Tel: 03-5730-4851　Fax: 03-5730-4853
e-mail:info-jnsa@connectous.co.jp

新日本監査法人
http://www.siai.co.jp

新日本監査法人 ERNST & YOUNG

新日本インテグリティアシュアランス

新日本監査法人は、世界140カ国で100,000名以上のスタッフを擁し、質の高い専門的サービスを提供する総収入145億ドルの世界最大級の会計事務所であるアーンスト･アンド･ヤングのメンバーファームとして、日本においても会計監査を始め高品質で専門性の高いアシュアランスサービスを提供しています。
新日本監査法人の100%子会社である新日本インテグリティアシュアランス株式会社(SIAI)は、グループ全体のCSR活動の推進を図るとともに､民間･公的機関などのあらゆる組織に対するCSRマネジメント並びに非財務分野における内部統制態勢のアドバイザリー業務を通じて、CSRの社会普及に尽力しています｡(下記サービスメニューをご参照ください｡)
SIAIでは、企業が持続的に成長するためには、事業上の資産価値をもつ情報資産である情報(文書、データ、会話など)と情報システムを保護することが必要不可欠と考え､｢情報管理コンプライアンス｣サービスをご提供しています。情報管理コンプライアンスとは、特定の法令等への準拠やBS7799やISMSといった第三者認証の取得だけを最終目的とはせず、各組織が表明する方針に基づく情報管理のルールを誠実に守り、顧客や株主といったステークホルダーへの説明責任を実質的に果たすための取組みを指します。我々、SIAIは、CSRマネジメント並びに内部統制態勢構築の一環として、情報管理コンプライアンス関連サービスを位置づけ、企業の持続的な成長をご支援したいと考えています。

SIAI サービスメニュー
(http://www.siai.co.jp/service/index.html)

CSR/USR/GSR 関連サービス
- 現状評価、ステークホルダー分析サービス
- CSR/USR/GSR 報告書、サステナビリティ報告書作成支援サービス
- AA1000 保証、GRI ガイドライン準拠性保証サービス

内部統制関連サービス
- 現状評価、リスクの棚卸しサービス
- 内部監査、グループ企業監査サービス

コンプライアンス関連サービス
- 現状評価、浸透度調査サービス
- 行動規範、コンプライアンス規程作成支援サービス
- 内部監査、ECS2000 保証サービス

情報管理コンプライアンス関連サービス
- 現状評価、リスク分析サービス
- 情報セキュリティポリシー等規程作成支援サービス
- 情報セキュリティ監査、個人情報保護監査サービス

事業継続管理（BCM/BCP）関連サービス
- 業務影響度分析（BIA）サービス
- 事業継続計画（BCP）作成支援サービス
- BCP 監査・レビューサービス

環境関連サービス
- 環境報告書作成支援サービス
- 環境報告書ガイドライン準拠性保証サービス
  （新日本監査法人グループにてご提供いたします。）

お問い合わせ先　新日本インテグリティアシュアランス株式会社
〒100-0011 東京都千代田区内幸町 2-2-3　日比谷国際ビル
Tel.03-3503-1116　Fax.03-3503-1151　http://www.siai.co.jp
担当：宮原　潤（miyahara-jn@shinnihon.or.jp）

マカフィー株式会社

http://www.mcafee.com/jp/

マカフィーは、不正侵入防止とリスクマネジメントのリーディングカンパニーです。マカフィーは、世界中で使用されているシステムとネットワークを、既知、未知の脅威からプロアクティブに防御しています。マカフィーの包括的なソリューションは絶え間ない技術研究に支えられており、個人ユーザをはじめ、中小企業、大企業、官公庁・自治体、ISPなど様々なユーザそしてパートナーから、高い信頼を獲得しています。マカフィーの実践的なアプローチは、効率的なセキュリティ投資に向けて、PDCAサイクルを通じたセキュリティの継続的なレベルアップを支援します。
代表的なソリューションは以下の通りです。

McAfee Secure Content Management Appliance

スパイウェア、スパム、フィッシング、ウイルス、トロイの木馬、メール/Webを介した情報漏洩等の脅威をゲートウェイで高速にかつ包括的にブロックするアプライアンス製品。従来のWebShield Applianceの機能とパフォーマンスを大幅に改善するとともに、名称変更いたしました。中小企業から大企業まで、幅広くサポートするラインナップで提供しています。

McAfee IntruShield

世界のIPS（不正侵入防止システム）市場におけるトップブランド。既知の脅威に対するシグネチャ解析、未知の脅威にも対応するアノマリ検知やDoS攻撃解析を統合し、暗号化攻撃への対応も含め、ゼロデイ攻撃にも対応するプロアクティブな不正侵入防止ソリューションです。また、1台のセンサーで多様なセグメントの監視が可能となり、他社製品より少ないセンサーで大規模ネットワークを防御できるため、企業ユーザのセキュリティ投資におけるROI向上に貢献します。

McAfee Managed VirusScan

運用管理に対するコストと負荷を劇的に低減する、管理サーバ不要のASP型全自動セキュリティ対策サービス。簡単なインストール、全自動の定義ファイル更新で、専任管理者のいない中小企業でも、この製品一つで、ウイルス、スパイウェア、バッファオーバーフローといった多種多様な攻撃から、ネットワークを防御できます。

詳しくは、
http://www.mcafee.com/jp/をご覧ください。

お問い合わせ先
マカフィー株式会社　営業統括本部
McAfee IntruShield: 03-5428-1104
McAfee IntruShield 以外の製品：03-5428-1228

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■

○フォレンジックサーバ「MSIESER」(エムシーサー)の紹介

「エムシーサー」はネットワークの状況を常時監視し、万一に備えてフォレンジックデータを蓄える製品です。
誰が・いつ・何を・どこで・どのように・何の為に・・・を解明し、内／外部の不正利用者／痕跡を追跡・発見して解明する手段を提供します。

【製品情報詳細】
http://www.ryoyo.co.jp/product/solution/it/security.html

◆お問い合わせ先◆
菱洋エレクトロ株式会社
システム情報機器営業第 2 本部 営業第 3 部
担当：平野
Tel：03-3546-5040
E-mail: msieser@ryoyo.co.jp

○BIG-IPアプリケーションセキュリティモジュール(ASM)

BIG-IPにWebアプリケーションセキュリティの機能が追加され、「プラグアンドプロテクト(導入後、即防御)」が可能になりました。
BIG-IPアプリケーションセキュリティモジュール(ASM)は、BIG-IPアプリケーショントラフィック管理プラットフォーム上で動作し、堅牢なアプリケーションセキュリティとトラフィック管理機能を1つのシステムで提供します。

【製品情報詳細】
http://www.f5networks.co.jp/ja/products/asm_index.html

◆お問い合わせ先◆
F5 ネットワークスジャパン株式会社 マーケティング
東京都渋谷区恵比寿 4-20-3
恵比寿ガーデンプレイスタワー 18F
Tel：03-5447-3370
E-mail: pr@f5networks.co.jp

○ SonicWALL Advanced Pack PLUS

「SonicWALL Advanced Pack PLUS」は、SonicWALL PROシリーズ(FireWall/VPN機能標準搭載)をベースに、有償のオプション製品(Gateway Anti-Virus/Anti-Spyware/IPS、Content Filtering Service)のライセンスを標準で付加した、キヤノンシステムソリューションズのオリジナルUTMアプライアンスです。現在「SonicWALL Advanced Pack PLUS」を特別価格にて提供しております。

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

◆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: snc-info@canon-sol.co.jp

○個人情報探索・監査 (棚卸し) ツール　P-Pointer

「Pポインター」は、ハードディスク内をスキャンし、個人情報と疑わしき情報を持つファイルを、独自アルゴリズムにてピックアップし、社内の誰のパソコンにどの位の個人情報があるかを、フォルダ、ファイル名、件数の一覧でレポートします。プライバシーマーク、ISMS取得活動における現状把握、個人情報対策の定期監査など、個人情報管理担当者や社員の労力を大幅に削減し、本来の業務に時間を充当することに貢献します。

【製品情報詳細】
http://www.klabsecurity.com/product/p-pointer/index.html

◆お問い合わせ先◆
KLab セキュリティ株式会社
Tel：03-5771-1107
E-mail: p-pointer@klabsecurity.com

○会員登録すると話題の雑誌・書籍の特別価格が見えるようになる！

IT業界で非常に高い信頼を獲得し、ゆるぎない実績を持つIDGジャパンでは現在、経営戦略を支援する新IT総合誌「CIO Magazine」、話題のIT情報の真実を語る「Computerworld」、電子自治体情報誌「e・Gov」、ネットワーク情報を網羅する「NETWORKWORLD」、Javaテクノロジー情報満載の「JavaWorld」、サーバ管理力強化マガジン「LinuxWorld」、Windowsを活用するための情報マガジン「Windows Server World」の7誌を発行。ぜひURLより直接ご購入ください。

【製品情報詳細】
http://direct.idg.co.jp

◆お問い合わせ先◆
株式会社 IDG ジャパン　出版販売部
Tel：03-5800-3661

JNSA 会員企業情報

○eTrust® PestPatrol Anti-Spyware Corporate Edition

従来のアンチウィルスソフトウェアでは防ぐことのできないスパイウェア、アドウェア、キーロガー、DoS攻撃、その他の悪意あるソフトウェアを検出し、完全に隔離または削除する総合スパイウェア対策ソリューションであり、あらゆる企業規模でご利用いただくことが可能です。
では、スパイウェアとは何でしょうか。その疑問にお答えします。ぜひこちらのページから、スパイウェアの定義と脅威の分類をチェックしてみてください。

【製品情報詳細】
http://www.caj.co.jp/focus/

◆お問い合わせ先◆
CA ジャパン・ダイレクト
Tel：0120-702-600

■ サービス情報 ■

○携帯電話による本人認証サービス「Secure Call」

サードネットワークスでは、携帯電話を本人認証の鍵として利用する新しいタイプの認証ASPサービス「Secure Call」を提供しています。
コールバック認証と発番号認証の2通りの認証方法を提供、なりすましアクセスを防止し、企業のリモートアクセスセキュリティを容易に実現します。
IPsecルーター、SSL-VPN装置との接続以外に、WEBサーバーとの連携によるEコマース向けソリューションも提供しています。

【サービス情報詳細】
http://www.thirdnetworks.co.jp

◆お問い合わせ先◆
サードネットワークス株式会社
Tel：03-3500-3030
E-mail: info@thirdnetworks.co.jp

○SSIJが国際規格ISO/IEC 27001:2005認証取得支援を開始しました

ISMS認証基準が国際規格化(ISO/IEC 27001)され、今後、情報セキュリティ対策への需要はますます高まることが必須であり、SSIJとしても、2005年10月よりISO/IEC27001:2005の認証取得支援コンサルティングを開始しました。
SSIJでは、情報セキュリティに関わるコンサルティング事業を行うとともに今後新たに生まれる規格･要求仕様(ＩＳＭＳのＩＳＯ化、ＣＳＲ等)に迅速に対応し、お客様にタイムリーなコンサルティングサービスを提供致します。

【サービス情報詳細】
http://www.ssij.co.jp/

◆お問い合わせ先◆
株式会社エス・エス・アイ・ジェイ
Tel：03-3432-1885
E-mail: info@ssij.co.jp

■ イベント情報 ■

○デジタル・フォレンジック・コミュニティ 2005MSIESER 展示

【日　時】12月19日(月)～20日(火)
【場　所】ホテルグランドヒル市ケ谷
【イベント情報詳細】
http://www.digitalforensic.jp/2005Work.html

◆お問い合わせ先◆
菱洋エレクトロ株式会社
システム情報機器営業第2本部　営業第3部　平野
Tel：03-3546-5040
E-mail：msieser@ryoyo.co.jp

○情報セキュリティ大学院大学シンポジウム「通信IP化と情報セキュリティ」

【日　　時】2005年12月23日(金) 9:45～17:10
【会　　場】岩崎学園横浜西口1号館
【参加費用】無料
【内容(講演)】
- 通信IP化の現状　寺崎明 氏
- 国際水準から見た日本の危機管理　小川和久 氏
- モバイル社会とセキュリティ　辻村清行 氏
- IPv6と情報セキュリティ　江崎浩 氏
- 高速URLフィルタリング技術とその応用　名古屋貢 氏
- 企業における実践的セキュリティ対策　牧野二郎 氏
- 信頼性とセキュリティを考える　林紘一郎
- 情報セキュリティ大学院大学における検討事例報告

【申込み】
電子メール(所属，氏名を明記)をevent@iisec.ac.jpへ
【イベント情報詳細】
http://www.iisec.ac.jp/

◆お問い合わせ先◆
Tel：045-410-0233
E-mail：event@iisec.ac.jp

○ SANS Tokyo 2006 Spring Conference 開催のお知らせ

2006年春のSANSトレーニング東京開催が決定しました。今回は以下の2コースを開催します。トレーニングの基本コンセプトは、「セキュリティ対策をどのように実施するのか」。豊富な演習によってベストプラクティスを習得することができます。
■SEC401：SANS Security Essentials Bootcamp Style
■AUD507：Auditing Networks, Perimeters & Systems
【日　程】2006年2月13日(月)～18日(土)
【会　場】新宿野村ビル44階
【イベント情報詳細】
http://sans-japan.jp/

◆お問い合わせ先◆
SANS JAPAN プロジェクト事務局（NRI セキュアテクノロジーズ内）
Tel: 03-5220-2298
E-mail：E-mail: info@sans-japan.jp

PKI Day － PKI技術最新事情

セコム株式会社　金岡　晃

日本ネットワークセキュリティ協会PKI相互運用技術WGが主催する「PKI Day－PKI技術最新事情」が10月28日(金)にセコムホールにおいて開催されました。会場は満員の盛況で、100名以上の方がセミナに参加されました。今回はPKIにおける「技術最新事情」をテーマとして、標準化の動向やPKIの利用法、運用における検討点などの広範にわたる講演があり、多数の参加者がPKIの理解を深めることができたセミナとなりました。

基調講演ではIPAセキュリティセンターの宮川氏が「経営幹部にPKIを理解してもらうためには…」と題して、技術者が非技術者、とりわけ経営幹部にPKIを理解してもらうことの困難さと、その解決法を示しました。最初に「PKIは正直難しい」としながらも、実は技術が難しいのではなく、利用技術が複合的であり、さらに利用目的も複数であることが難しさとなっていると指摘。そもそも複数の目的も許容する社会基盤であるPKIを単一の目的に絞って話そうとすると理解を妨げさせる原因になることから「まず『複雑』で『複合的』であることから話すべき」と示されました。PKIを説明する場合、公開鍵暗号技術の説明から始めることが多く見られますが、それではPKIの全体像までたどりつかなくなってしまいます。公開鍵暗号技術はPKIの要素技術でしかないことを考慮すべきで、その上でお勧めする説明方法として『信頼関係(trust)モデル』から説明し、デジタル証明書に関しても技術仕様の用語よりも、関係者が何をしなければならないかを示す証明書ポリシ(CP)を説明するという方法を示されました。信頼関係モデルの説明は、いわばPKIをトップダウンで説明するものであり、それは社会的なモデルを説明することでもあるから、公開鍵暗号技術の説明から始めるボトムアップの説明よりも、こちらの方が経営幹部に説明するには望ましいと述べられ、また専門用語を正しく使うことや無理のある比喩表現を避けることも重要であることを強調されました。

続いてのセッションでは、富士ゼロックスの稲田氏が「PKI標準化最新動向」と題してPKI関連標準の最新動向を紹介されました。まず稲田氏はSSL/TLSに焦点を当て「Amazon、楽天などのサービスを使ったことがある人」とセミナ参加者に投げかけました。ほぼ全員の人が挙手した結果を見て、稲田氏は「PKIはもはやすぐ隣に存在する技術」とした上で、インターネットは車や火と同じく利用法によっては非常に危険なものであり、その中でPKIが提供する機能が注目されている、と述

べられました。PKIの標準化について証明書自身のプロファイルはほぼ完成しているということを紹介されるとともに、証明書の検証やその応用系については標準化が現在も進んでいるという現状を紹介されました。また、証明書の検証については検証をクライアント側でやるのには相当な労力が必要であると指摘し、その回避策としてサーバサイドで検証プロセスを代行するためのプロトコル、SCVPやOCSPについて図解されました。最後に証明書の応用系の標準化として長期署名とタイムスタンプについて触れ、その最新動向を解説していただきました。

午後に入り、実際にPKIが利用されていくなかで現れてきた問題点や、運用上での注意点などに関して、PKIがどう使われているか、どう使われていこうとしているか、というセッションが続きました。

まず、「マルチドメインPKIと相互運用性のBCP(Best Current Practice)」がセコムの島岡氏より発表されました。あるポリシ下で運用されているPKIの単位「PKIドメイン」に対し、複数のPKIドメインをまたぎ、信頼関係を築く「マルチドメインPKI」がこれからのPKIが進んでいく方向であろうとした上で、自身がPKIの相互運用で苦慮された経験を、同じく米国で政府系のマルチドメインPKIのノウハウを持つNISTの方との共著で文書化しIETFへと標準化を提案していることを紹介されました。またこういった相互運用性のBCP策定にあたってのコンセンサス作りとして、海外での活動なども紹介されました。

続いてのセッションではNECの奥野氏による「グリッドコンピュータとPKI」の発表が行なわれました。グリッドコンピューティングで多く利用されているGlobus Tool Kit（GTK）や、グリッドコンピューティングの全機能をWebサービス技術によりサービス化するOGSA（Open Grid Services Architecture）を中心に解説を行い、その中でPKIが利用されている場面を説明されました。OGSAのセキュリティアーキテクチャの中では、複数の組織が資源を共有するために構築するVO（Virtual Organization）を紹介、ここでも組織間のポリシなどの相互運用性がポイントになっていることが伺えました。最後に、奥野氏が認証局ソフトの開発などで参加しているNAREGI（超高速コンピュータ網形成プロジェクト）の説明があり、認証局ソフトNAREGI-CAの構成図や運用概要が紹介されました。

日本ネットワークインフォメーションセンター(JPNIC)の木村氏からは「JPNIC認証局～IPアドレス認証局(認証)～」と題して、JPNIC CAの紹介、またご自身の経験などから得られたいくつかのポイントについて講演がありました。電子証明書を簡単に利用してもらう点として「本人性確認」と「手続きの複雑さ」を挙げ、それらの解決手段の1つとして商用サービスなどで多く適用されているRA（登録機関）を外部に持つモデルを示し、同モデルを提供しているJPNICの認証局が紹介されました。また、ご自身の経験からのCA構築時の検討ポイントや、整備されていると便利である事項などを示し、「こういったBCPを皆で持ち寄ることが大事」とセッションを締められました。

休憩を挟んだ午後の後半では2つのセッションがありました。1つ目はマイクロソフトの渡辺・鈴木両氏による「WS-FederationとPKI」。Federation（連携）は、PKIなどの認証基盤が整備されたあとに出てくる注目度の高い話であり、司会をされたJNSA安田氏や2つ目のセッションで講演されたセコム松本氏は「次回はFederationをキーワードにしてセミナを開催したい」という意向を持っており、今回の渡辺・鈴木両氏の発表は

イベント開催の報告

それに先駆けてのものとなりました。

発表ではまず渡辺氏が、現状持っている認証の基盤を利用して他の組織との柔軟なシステム間接続を可能にするFederationが今後重要になってくると強調。PKIとWS-Federationの連携方法の違いの解説などがされました。続いて鈴木氏が、マイクロソフトの取り組み詳細を紹介。WS-FederationやADFS（Active Directory Federation Service）の説明を頂きました。利用シナリオをいくつか紹介後、事例として、イラク戦争などにおける同盟国間のインターオペラビリティ実証実験「CWID2005」の紹介もあわせて行なわれました。

最後のセッションは本セミナを主催したPKI相互運用技術WGリーダであるセコムIS研究所の松本氏より「Challenge PKIプロジェクトとPKI技術最新事情」と題して、JNSAのChallengePKIプロジェクトの紹介と、最近のPKI関連トピックや今後の課題についての解説がありました。PKIの業界において、アイディアから仕様、仕様から標準、実装から標準という一連の標準化の流れにそれぞれプレーヤーがいる一方で、実際に標準・実装から展開し相互運用を行なう部分を担うプレーヤーがいないことを指摘しました。さらに、標準と呼ばれる文書は山のようにあるが、相互運用が可能なものはわずかであることも問題とし、解決していくにはベストプラクティスが重要である、と述べられました。これらを目標とし2001年よりスタートしたChallenge PKIプロジェクトの活動報告をされ、現在までの活動内容を振り返られました。成果はIPAの報告書や、Web上でのテストケースの公開、得られた知見のIETFへのフィードバックなどが挙げられます。PKIの最新事情としては、危殆化が指摘されたSHA-1からいかにしてSHA2ファミリーに移行していくかというSHA-1問題について、また近年IT化の動きが活発になってきた医療福祉分野へのPKI整備の動向という内容で医療PKIについて、さらに来年度に現状の問題点から改正がさけばれる電子署名法の改正についても解説されました。そして最後のまとめとして「PKIの本質的な問題とは相互運用性に集約されるが、同時に、ますます社会基盤として重要性も深まっていくだろう」と述べられて講演を終えられました。

PKIは情報社会における「信頼の拠りどころ」を提供するものであり、それ自身が社会基盤にもなれば、別の基盤における信頼性を保つ機構として利用される非常に重要な技術でもあります。PKIはすでにさまざまな分野で利用されており、今後の社会で浸透していくほどにその相互運用性の重要性が高まると言えます。またPKIはその複雑さや困難さが指摘される場面が多くありますが、本セミナの発表者はPKIの導入・利用においてさまざまな困難を経験されてきた方々であり、それらの方々からの発表による有用な事例や導入・利用における指針などが広く示された今回のセミナとなりました。

※当日のプレゼンテーション資料はJNSAのホームページより参照可能です。
http://www.jnsa.org/seminar/2005/seminar_20051028.html

IPA 宮川寧夫氏

JNSA 西日本支部主催セキュリティセミナー
NSF2005 in OSAKA

JNSA 西日本支部 セミナー運営 WG リーダー
西日本電信電話株式会社　中台　芳夫

日本ネットワークセキュリティ協会西日本支部主催の第 6 回セキュリティセミナー「NSF2005 in OSAKA」が、経済産業省、近畿経済産業局、大阪商工会議所、財団法人関西消費者協会、社団法人関西経済連合会の後援のもと、10月27日(木)に大阪市にある天満研修センターにおいて開催されました。当日は好天にも恵まれ、約90名の方にご来場頂きました。

今回は企業における「情報セキュリティガバナンス」をテーマとし、経済産業省からの基調講演、法曹界からの個人情報保護対策のあり方をそれぞれご講演頂いたほか、JNSA の各部会の WG から、最新の研究成果について報告し、本格的な情報セキュリティ対策を目指している企業等のお客様に対し、今すぐ着手すべき情報セキュリティ対策のポイントを明らかにするセミナーとなりました。

プログラムは最初に井上支部長から、「４月に個人情報保護法がスタートし、『日本版SOX（Sarbanes-Oxley）法』の導入の動きも見られる中、適切な情報セキュリティ対策を打つことが企業の価値に結びつく、と注目を浴びています。今回のセミナーを機に『情報セキュリティ・ガバナンス』に対する知識・研鑽を深めて頂きたいと思います」とご挨拶を頂き、あわせてJNSA、各部会・WGの調査研究活動状況、および西日本支部の取り組みについてもご紹介を頂きました。

続いて基調講演として、「企業における情報セキュリティガバナンスのあり方」と題し、経済産業省・商務情報政策局・情報セキュリティ政策室課長補佐の村野正泰様からご講演を頂きました。村野様からはまず、「政府では、世界最高水準の高信頼性社会の実現のため、しなやかな事故前提社会システムの構築、高信頼性を強みとするための公的対応の強化、内閣機能強化による統一的推進、の３つの戦略からなる情報セキュリティ総合戦略を掲げ、これに基づいて内閣官房の機能強化を図り、政府機関の総合対策促進として『情報セキュリティ基準』をまもなく策定予定です」と、政府全体的な動きについてご紹介頂き、関連して、企業等の情報セキュリティにおける組織的対策の推進、早期警戒体制の整備など、経済産業省として推し進めている各種事業についてご紹介頂きました。続いて今回のセミナーのメインテーマである「情報セキュリティ・ガバナンス」への取り組みについてご紹介頂きました。企業等における近年のIT事故は経営を左右し、社会的にも大きな影響が出ることになります。このため企業自身が情報セキュリティを自律的・継続的に改善するための組織的かつ包括的アプローチが求められます。また米国のSOX法の成立過程にも見るように、事業継続計画(BCP)を策定しておくことも、大規模な事件に遭遇した場合でも企業経営を健全に維持するための必須条件として求められつつあります。村野様はこれらの状況に端的に触れ、「情報セキュリティ・ガバナンス」の必要性を訴求されました。一方で、適正なセキュリティ投資の判断の難しさ、セキュリティ対策の企業価値への評価の反映等が、日本では適切に判断されていない問題点として存在しています。経済産業省では、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインの３つを、

西日本支部長 井上陽一氏

イベント開催の報告

情報セキュリティ・ガバナンスの確立を促進するツールとして策定し展開を行っています。村野様からはツールを利用した取り組みについて詳しくご紹介を頂きました。講演後の質問では「今回のツールが今後の日本版SOX法における企業の取り組みの指標として継続的に利用可能なのか」などの質問があり、企業でも日本版SOX法を意識した取り組みが少しずつ始まっていることがうかがわれました。

午後からは、JNSAの代表的なワーキンググループの調査活動報告を行いました。報告内容の選定にあたっては、セキュリティ対策の不備によって生じるインシデントによる被害額の算定、その対策の代表例としての個人情報保護対策、そして今年度上期に著しく話題を集めたマルウェアの動向と対策と言う形で、リスク分析と対策の双方の重要性を受講者に認識して頂く形式を取りました。

最初の報告は「2004年度個人情報漏えい事件の分析と想定被害額の算出による評価」と題し、JNSA政策部会・セキュリティ被害調査WGメンバーの山本匡様(株式会社損保ジャパン・リスクマネジメント)から発表頂きました。山本様からは「日本でセキュリティインシデントに対する被害額が端的に判るものがないか、とJNSA事務局で議論されたのがWG発足の契機であり、インシデント被害調査を2001年度から着手しました。2004年度は警察庁からの委託事業としてのインシデント被害調査(『不正アクセス行為対策等の実態調査』)と、JNSAの活動として個人情報漏えいにおける被害考察と分析を実施しました。前者のインシデント被害調査では、632の回答の中からインシデント被害に遭ったと言う回答が230事業体あり、被害後は技術的対策をとる例が多数見られました。また従業員1人あたりの被害額と対策費用との相関関係は明確ではないものの、2～3万円の対策費用で被害はある程度抑えられていると想定されます。後者の個人情報漏えいによる被害想定の調査においては、2004年度になって小さな『漏えい等事故』も報告されるようになって、調査対象件数も大きく増加しています。想定損害賠償額算定式のモデル化から、2004年度の想定損害賠償額総額は4,666億円以上に達すると想定されています。個人情報漏えいの被害が株価へ影響する点も分析を続けています」と、2004年度の調査報告の要点を講演して頂きました。講演後には、個人情報保護の賠償請求額の具体的な算出式についての質問などが寄せられていました。

経済産業省 林野正泰氏

続いて「中小企業に必要な個人情報保護対策の策定に向けて」と題し、JNSA西日本支部・中小企業向け個人情報保護対策WGメンバーの西村祥様(伊藤忠テクノサイエンス株式会社)から発表頂きました。西村様からは「当WGは、大企業とは異なった位置づけで個人情報保護が求められる中小企業の現状の取り組みについて調査し、具体的な対策･対応方法を運用マニュアルとして取りまとめ、各種中小企業での利用に役立てて頂けるものを策定したいと考えています。WGはコンサルティングチームと研究チームに分かれ、月1回のミーティングを基本として活動しています。モニタ企業様をチェックした現状報告としては、セキュリティに対する文書化の不徹底や、システム対策と運用とのバランス不足がみられています。またモニタ企業様の生の声として、保護法対策している企業としてのアピールの展開方法や、企業規模に応じたセキュリティ対策の指標化を模索している

点が課題として挙がっています」と報告が寄せられました。本WGの課題として、モニタ企業が1社に限定されている点、WGメンバが不足している点にあり、早急な対応が必要となっています。講演後はWG参画に興味を持った受講者からの問い合わせがあるなど、WG活動の活性化に向けて受講者からの反応を頂いた点が印象的でした。

三番目には「多様化するマルウェアの実態と対策」と題し、JNSA技術部会の渡辺章様(株式会社アークン)から発表頂きました。不正プログラム調査WGのリーダでもいらっしゃる渡辺様からは、最近著しく話題を呼んでいるスパイウェア、不正プログラム、ウェブアプリケーションへの攻撃等について詳しい解説を頂きました。渡辺様は「スパイウェアの定義はまだ曖昧であって、多種多様なものが分類されています。米国ではアドウェア等のスパイウェアモジュールを作成・配布しているソフトウェア会社もいて、ユーザはフリーウェア等のインストール時に、これらのモジュールを知らずに取り込んでしまっているケースもあります。国内でもネット銀行のユーザ等を標的としたスパイウェアの活動も報道されるようになりました。米国では、広告表示のプログラムがスパイウェア対策ソフトによる駆除対象と扱われて訴訟になったことをきっかけに、業界を主体に2つのスパイウェア規制法案が検討され、採決待ちになっています。国内でも問題が大きくなれば同様の動きになると想定されるでしょう」と語られ、パソコン上で自己修復機能・ステルス機能を仕掛けるマルウェアの実演も交え、マルウェアの現状について報告されました。またウェブアプリケーションへの攻撃についても、「2004年からSQLインジェクション攻撃が急激に増加していますが、悪用の危険性は旧来から言われていたもので、未だに事件が生じています」と、ウェブアプリケーションプログラム作成の陥穽について指摘され、網羅的な対策の必要性についても詳しくコメントを頂きました。

そして最後に「情報セキュリティ対策における実務上の法的課題について」と題し、きたおか法律事務所の北岡弘章弁護士にご講演頂きました。北岡様は、「企業において漏えいリスクの高い情報は多種ありますが、多数の相談を受けていることを背景に、個人情報保護関連で一般企業の懸念事項となっている点について解説します。個人情報の漏えいリスクを考えた場合、クレームや訴訟による金銭的な損害賠償を生じる例は少なく、むしろ信用喪失のリスクが大きく存在します。小額のお見舞い金を配布するかどうかは企業の姿勢であって必ず生じるリスクとは言えません。その他にもサービスの停止・解約やサイトの閉鎖による損害、株価への影響、行政処分等のリスクが存在します。その対策としての安全管理措置の中で、ここでは従業者の監督について詳説します。情報漏えいは内部からの犯行が多いものですが、従業者の管理を厳しくし過ぎた場合には人権侵害の問題になりえるため、法的には悩ましい部分です。『モニタリング』は従業者の個人情報を収集し、プライバシー侵害の問題にも関わってくるため、省庁の個人情報保護ガイドライン等に沿った形で実施する必要があります。また誓約書の提出は範囲の明確化と自覚を促す意味としての存在に留まると考えられるため、従業者の秘密保持義務については就業規則で明確化しておく必要があります。競業避止義務については職業選択の自由との関係で有効性が問題と思われます。情報を守るための社内規則等について、守れないルールは止めて合理的なルールを策定すべきであり、実行不可能と判明したルールはどんどん改訂していくことが大事です。内部犯行の特定のためにはアクセスログを記録することが重要ですが、今後は日本版SOX法の出現により、内部統制を行う上でのモニタリング、アクセスログ記録が不可欠になってきます。また財務情報の正確性の確保も求められるため、情報セキュリティの三要素のバランスを取ることが法的にも要求される傾向が想定されます」と講演され、従業者の立場も配慮した人的安全管理措置のあ

り方と、今後のセキュリティ対策の方向性について明確化して頂きました。

情報セキュリティ対策は、個人情報保護法が本格的な定着期に入ろうとする中で、3つの観点からの変容の時期を迎えようとしています。一つ目は「情報セキュリティ・ガバナンス」の観点からの組織的対策のシフト、二つ目は「システム防衛型」から「情報漏えい対策型」への技術的対策のシフト、三つ目は「予防偏重型」から「事故前提型」へのリスク管理のシフトです。すなわち、企業の発展に帰する「あるべき姿」を意識し、来たる「日本版SOX法」の到来も視野に入れ、情報セキュリティ対策機能をコーポレート・ガバナンス(企業統治)における内部統制機構に如何に取り込んで、どう運用していくかが、今後の情報セキュリティ対策のキーポイントになると言えるでしょう。今回のセミナーはその変革の前段階の時期にあって、今後の取り組みのありかたに対して一石を投じるものになりました。

2005 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、情報犯罪を防ぐことはできません。こうした状況をふまえ、経済産業省とNPO 日本ネットワークセキュリティ協会(JNSA)では、家庭や学校からインターネットにアクセスする人々を対象に、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を2003年度より開催しており、2005年度も継続して開催しています。

【開催概要】

[**主　　催**] 経済産業省、NPO 日本ネットワークセキュリティ協会 (JNSA)
[**後　　援**] 警察庁、その他
[**開催一覧**] 以下一覧をご覧下さい。(2005 年 12 月 1 日現在)

■ 新規開催 ■

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

■ **独自開催** ■　※共催団体が中心となって運営・開催していただく会場です

日　程	県　名	共催者	開催場所
2005 年 5 月～ 2006 年 3 月	佐賀県	佐賀県ネットワーク・セキュリティ対策協議会、 NetCom さが推進協議会、佐賀県	全県下 8 地域での分散開催
2005 年 6 月～ 2006 年 3 月	神奈川県	NPO 情報セキュリティフォーラム　他	全県下 16 会場で順次開催
6 月 23 日（木）	福井県	ナレッジふくい	福井県生涯学習館 （ユー・アイふくい）
10 月 15 日（土）	奈良県	なら情報セキュリティ研究会	奈良産業大学
11 月 2 日（水）	兵庫県	兵庫県、財団法人ひょうご情報教育機構、 ひょうご情報セキュリティ推進会議	神戸市産業振興センター
11 月 5 日（土）	愛知県	NPO 東海インターネット協議会	マナハウス
11 月 12 日（土）	奈良県	なら情報セキュリティ研究会	帝塚山大学学園前キャンパス
11 月 19 日（土）	大分県	大分県立芸術文化短期大学 （協力：財団法人ハイパーネットワーク社会研究所）	大分県立芸術文化短期大学
	島根県	NPO プロジェクトゆうあい	隠岐島文化会館
11 月 26 日（土）	新潟県	NPO 新潟情報セキュリティ協会	NICO プラザ会議室
	北海道	NPO くるくるネット	室蘭工業大学
	長野県	上田市マルチメディア情報センター	上田市マルチメディア情報センター
	島根県	NPO プロジェクトゆうあい	テクノアークしまね
11 月 27 日（日）	岡山県	おかやま情報ボランティアフォーラム、 株式会社エス・シー・ラボ	灘崎町総合福祉センター
11 月 30 日（水）	兵庫県	兵庫県、財団法人ひょうご情報教育機構、 ひょうご情報セキュリティ推進会議	姫路商工会議所会館
12 月 3 日（土）	和歌山県	NPO 情報セキュリティ研究所	和歌山県情報交流センター Big･U
12 月 8 日（木）	兵庫県	兵庫県、財団法人ひょうご情報教育機構、 ひょうご情報セキュリティ推進会議	豊岡市民会館
12 月 10 日（土）	山口県	山口大学、山口県セキュリティマネジメントフォーラム	山口大学
	高知県	高知県、社団法人高知県情報産業協会	高知市文化プラザ
12 月 22 日（木）	栃木県	NPO 栃木県シニアセンター、栃木県	栃木市市民会館
1 月 18 日（水）	京都府	京都高度情報化推進協議会、京都府	キャンパスプラザ京都
1 月 27 日（金）	岐阜県	かにぱそこんくらぶ	可児市文化創造センター
2 月 17 日（金）	熊本県	NPO 熊本県次世代情報通信推進機構	くまもと県民交流館パレア
その他、滋賀県でも開催予定			

「インターネット安全教室」は、参加費用は無料で、どなたでもご参加いただけます。
お近くで開催の際には、ぜひご参加ください。
開催状況については、随時「インターネット安全教室」ホームページをご確認ください。
http://www.jnsa.org/caravan/

事務局お知らせ

JNSA ANNOUNCE

1. 主催セミナーのお知らせ

● 情報セキュリティ人材育成シンポジウム in 岡山

日時：2005 年 12 月 16 日（金）
主催：経済産業省
共催：岡山理科大学・
NPO 日本ネットワークセキュリティ協会
※事前登録制／聴講無料

その他、2 月に教育セミナーを予定しております。
(開催場所：工学院大学)
詳細については決定次第、ＪＮＳＡホームページ上で皆様へお知らせいたします。

2. 協力イベントのお知らせ

1．JASA 情報セキュリティ監査フォーラム In Winter

会期：2005 年 12 月 6 日（火）　仙台
2006 年 1 月 25 日（水）　名古屋
2006 年 2 月 1 日（月）　大阪
主催：経済産業省
NPO 日本セキュリティ監査協会
会場：仙　台　仙台商工会議所
名古屋　メルパルク NAGOYA
大　阪　エル・大阪
http://www.jasa.jp/seminar/secf2005lh.html

2．第 2 回 デジタル・フォレンジック・コミュニティ 2005 in Tokyo

会期：2005 年 12 月 19 日（月）～ 20 日（火）
主催:特定非営利活動法人デジタル･フォレンジック研究会、
デジタル・フォレンジック・コミュニティ 2005 実行委員会
会場：グランドヒル市ヶ谷
http://digitalforensic.jp/2005Work.html

3．平成 17 年度 情報モラル啓発セミナー大阪

会期：2005 年 12 月 20 日（火）
主催：中小企業庁、近畿経済産業局、
財団法人ハイパーネットワーク社会研究所
会場：大阪国際交流センター（大会議室さくら）
http://www.hyper.or.jp/moral2005/osaka/

4．STORAGE NETWORKING WORLD Tokyo 2006

会期：2006 年 1 月 24 日（火）～ 25 日（水）
主催：IDG ジャパン、
SNIA（Storage Networking Industry Association）
会場：新宿 NS ビル
http://www.idg.co.jp/expo/snw/index.html

5．ソフトウェアテストシンポジウム 2006 東京

会期：2006 年 1 月 30 日（月）～ 31 日（火）
主催：ソフトウェアテスト技術者交流会（TEF）
会場：都市センターホテル
http://www.swtest.jp/symposium.html

6．PAGE 2006

会期：2006 年 2 月 1 日（水）～ 2 月 3 日（金）
主催：社団法人日本印刷技術協会
会場：サンシャインシティコンベンセンター TOKYO
http://www.jagat.or.jp/PAGE/index.html

7．NET & COM 2006

会期：2006 年 2 月 1 日（水）～ 2 月 3 日（金）
主催：日経ＢＰ社
会場：東京ビッグサイト
http://expo.nikkeibp.co.jp/netcom/

3. JNSA 部会・WG 2005 年度活動

1．政策部会

（部会長：下村正洋 氏 / ディアイティ）

調査事業や様々な基準・ガイドラインの策定、他団体との連携を行う。

【セキュリティ被害調査WG】

（リーダー：山田英史 氏 / ディアイティ）

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

主な活動内容としては、下記の通り。

・アンケートおよびヒアリングによる、年間の情報セキュリティ被害の実態調査

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

予定成果物は、情報セキュリティインシデントに関する調査報告書。

【マーケットリサーチWG】

（リーダー:勝見勉 氏 / グローバルセキュリティエキスパート）

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

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

予定成果物は、調査レポート。

【セキュリティ会計ガイドライン検討WG】

（リーダー：佐野智己 氏 / 凸版印刷）

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

予定成果物は、JNSA 活動報告書，論文など。

【セキュア・システム開発ガイドラインWG】

（リーダー：丸山司郎 氏 / ラック）

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

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

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

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

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

【スパイウェア対策啓発WG】

（リーダー：蛭間久季 氏 / アークン）

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

主な活動内容は以下を予定している。

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

2．技術部会

（部会長：佐藤友治 氏 /IRI コミュニケーションズ）

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

成果物目的のワーキンググループ

【セキュリティポリシーWG】

（リーダー：小杉聖一 氏 /NEC ソフト）

2004 年の活動を継続実施する。

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

査し報告する。
　予定成果物は、公開サンプルの改版とISMS（X5080）との対応表。

【不正プログラム調査WG】
（リーダー：渡部章 氏 / アークン）
　トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加している。また、ウイルス、ワームも同様に 近年では不正アクセスを目的としたものも少なくない。当WGでは、不正プログラムを分類化し、タイプ別、レイア別に、その対策ソリューションを調査、整理し、マッピング化する。
　予定成果物は、不正プログラム対策ガイドラインの策定。

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

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

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

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

【脆弱性定量化に向けての検討WG】
（リーダー：郷間佳市郎 氏 / 京セラコミュニケーションシステム）
　脆弱性の定量化アプローチについて、国外の情報を含め検討を行い、WGとしての検討結果を出す。
　成果物として報告書を作成する予定。

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

　予定成果物は、必要に応じて行う提言と研究報告の作成。

勉強会目的のワーキンググループ

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

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

【セキュリティ啓発WG】
（リーダー：古川勝也 氏 / マイクロソフト）
　「インターネット安全教室」の企画・運営を通しセキュリティ啓発活動を行う。
　2005年4月～8月にCD-ROM映像及び冊子のリニューアル製作を行なうと共に、2005年6月～2006年3月にかけて全国20ヵ所以上で「インターネット安全教室」を実施予定。

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

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

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

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

プロジェクト

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

5. 西日本支部
（支部長：井上陽一 氏 / ヒューコム）
JNSA 西日本支部は関西に拠点を置くメンバー企業の協賛の下、西日本におけるネットワーク社会のセキュリティレベルの維持･向上並びに、日々高まる情報セキュリティへのニーズに応えるべく、先進性を追及すると共に、質の高いサービスを提供する事を目的として活動する。今年度も引き続き関西方面でのセキュリティ啓発セミナーを中心に活動を行う。

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

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

4. JNSA 役員一覧

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

理　事（50 音順）

井上　陽一	株式会社ヒューコム
後沢　忍	三菱電機株式会社　情報技術総合研究所
浦野　義朗	株式会社フォーバルクリエーティブ
甲斐　龍一郎	新日鉄ソリューションズ株式会社
川上　博康	セコムトラストネット株式会社
後藤　和彦	株式会社大塚商会
小屋　晋吾	トレンドマイクロ株式会社
下村　正洋	株式会社ディアイティ
鷲見　晴美	株式会社ネットマークス
武智　洋	横河電機株式会社
玉井　節朗	株式会社ＩＤＧジャパン
辻　久雄	ＮＴＴアドバンステクノロジ株式会社
西尾　秀一	株式会社ＮＴＴデータ
西本　逸郎	株式会社ラック
野久保　秀紀	大日本印刷株式会社
野々下　幸治	株式会社シマンテック
坂内　明	東芝ソリューション株式会社
日暮　則武	東京海上日動火災保険株式会社
古川　勝也	マイクロソフト株式会社
松尾　直樹	ＮＴＴコミュニケーションズ株式会社
山野　修	ＲＳＡセキュリティ株式会社
若井　順一	グローバルセキュリティエキスパート株式会社

監　事

土井　充	（公認会計士　土井充事務所）

顧　問

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

事務局長

下村　正洋	株式会社ディアイティ

5. 会員企業一覧（2005 年 12 月 1 日現在　204 社　50 音順）

【あ】

（株）アークン
ＲＳＡセキュリティ（株）
（株）ＩＲＩコミュニケーションズ
（株）アイアイジェイ テクノロジー
（株）アイ･ソリューションズ
株式会社アイティインテグレーションズ New
（株）ＩＤＧジャパン
（株）ＩＴサービス
（株）アイ・ティ・フロンティア
アイネット･システムズ（株）
（株）ＩＰイノベーションズ
アイマトリックス（株）
（株）アクセンス・テクノロジー
（株）網屋
アライドテレシス（株）
アラクサラネットワークス（株）
（株）アルゴ 21
（株）アルテミス
（株）イオノス
伊藤忠テクノサイエンス（株）
学校法人 岩崎学園
インターネット セキュリティ システムズ（株）
インテック･ウェブ･アンド･ゲノム･インフォマテックス（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
ウチダインフォメーションテクノロジー（株）
ウッドランド（株）
エー･アンド･アイ　システム（株）
ＡＴ＆Ｔグローバル・サービス（株）
（株）エクスフロント
（株）エス･アイ･ディ･シー
エス・アンド・アイ（株）
（株）エス・エス・アイ・ジェイ
ＳＳＨコミュニケーションズ・セキュリティ（株）
（株）エス・シー・ラボ
ＮＲＩセキュアテクノロジーズ（株）
ＮＲＩデータサービス（株）
ＮＥＣソフト（株）
ＮＥＣネクサソリューションズ（株）
ＮＴＴアドバンステクノロジ（株）
ＮＴＴコミュニケーションズ（株）
エヌ･ティ･ティ・コムウェア（株）
エヌ･ティ･ティ・コムチェオ（株）
（株）ＮＴＴデータ
（株）エネルギア・コミュニケーションズ
Ｆ５ネットワークスジャパン（株）
エムオーテックス（株）
（株）エム・ファクトリー
エリアビイジャパン（株）
（株）大塚商会
オムロンフィールドエンジニアリング（株）

【か】

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

【さ】

サイバーソリューション（株）
サイボウズ（株）New
サードネットワークス（株）New
サーフコントロール ジャパン
サン電子（株）
サン・マイクロシステムズ（株）

（株）ＣＲＣソリューションズ
（株）シーエーシー
（株）シー・エス・イー
ジーエフケー　マーケティングサービス　ジャパン（株）
（株）シーフォーテクノロジー
（株）ジェイエムシー
ジェイズ・コミュニケーション（株）
シスコシステムズ（株）
（株）シマンテック
シムデスク･テクノロジーズ
寿限無（株）
（株）翔泳社
（株）情報数理研究所
新日鉄ソリューションズ（株）
新日本監査法人
図研ネットウエイブ（株）
（株）ステラクラフト
住商情報システム（株）
住生コンピューターサービス（株）
セイコープレシジョン (株)
セキュアコンピューティングジャパン（株）
（株）セキュアソフト
（株）セキュアブレイン
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム (株)
セコムトラストネット（株）
（株）セゾン情報システムズ
セントラル・コンピュータ・サービス（株）
ソニー（株）
ソニー･エリクソン･モバイルコミュニケーションズ（株）
ソフトバンクＢＢ（株）
ソラン（株）
ソラン・コムセック　コンサルティング株式会社 New
（株）ソリトンシステムズ
ソレキア（株）
（株）損保ジャパン・リスクマネジメント

【た】

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

【な】

（株）ニコンシステム
西日本電信電話（株）
日商エレクトロニクス（株）
日本アイ･ビー･エム（株）
日本アイ・ビー・エム　システムズエンジニアリング（株）
日本オラクル（株）
日本高信頼システム（株）
日本コムシス (株)
日本ジオトラスト (株)
（株）日本システムディベロップメント
日本セーフネット (株)
日本電気（株）
日本電気エンジニアリング（株）
日本電信電話（株）　情報流通プラットフォーム研究所
日本ビジネスコンピューター（株）
日本ユニシス（株）
ネクストコム（株）
（株）ネット・タイム
（株）ネットマークス
（株）ネットワークセキュリティテクノロジージャパン
ネットワンシステムズ（株）

【は】

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

【ま】

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

【や】

ユーテン･ネットワークス（株）
横河電機（株）

【ら】

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

【わ】

（株）ワイ・イー・シー New

【特別会員】

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

6. JNSA 年間活動（2005 年度）

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

2005年6月～2006年3月「インターネット安全教室」開催

★ JNSA 活動スケジュールは、http://www.jnsa.org/active/suchedule.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

8. お問い合せ

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

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

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

9. 編集後記

11 月初旬に山中湖周辺まで出かけてまいりました。紅葉を見るにはまだ早かったこともあり、のんびり景色を楽しむことができました。携帯電話の電波も PC のキーボードも無いところに行くと新鮮な気分を味わえます。

最近、電車でノート PC を開く姿をまったくといっていいほど見かけなくなりました。その反面、重要書類と思わしきプリントに熱心に目を通される方を見かけます。紛失したときの影響範囲は小さくなるかもしれませんが、情報セキュリティを推進する側の身としては少々奇異に感じました。

さて、もうすぐ年末さらには年度末と、家庭に仕事にと忙しい季節を迎えます。こんな時期は疲労のせいか暖かさのせいか電車の中で転寝をしてしまいますね。電車の中で眠ってしまう姿もみっともないものですが、熟睡してトラブルを引き寄せてしまうのではと不安になります。

巷では毒性の強いインフルエンザの流行が心配されているようです。会員の皆さまも健康に十分な気をつけてくださいませ。

JNSA Press vol.15

2005 年 12 月 25 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