JNSA Press

Japan Network Security Association

Vol.10
April 2004

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

セキュリティ技術の向上のために本当に必要なのは

早稲田大学理工学部情報学科教授 / JNSA顧問
村岡　洋一

住基システムが稼動を始めて、久しい時間が経ちました。この間、セキュリティ技術上の問題が皆無だったとはいえないのは、残念な事実ではあります。しかし、最近発覚した問題に、他人になりすましてIDカードを受け取るという事件がありました。凝りに凝った認証メカニズムも、この前には全く無力です。

パスポートでも、他人になりすましてパスポートの発給を受けるという確信犯であれば、これを単なる住基システムなどの導入だけでは、防ぐことは出来ません。
システム（特にこれが電子政府であれば、なおさらのこと）というのは、単に計算機システムだけに閉じません。いやしくも社会システムであれば、人と人の窓口での対応から、最終的に必要な書類の手交に至るまでの、人から始まって人に終わるend-to-endの全ての鎖がきちんと設計されてこそ、完璧な「システム」と言えるのではないでしょうか。そして、そのような「システム」が設計できてこそ、真のセキュリティ技術者です。

最近の事情は知りませんが、一頃のアメリカの優秀なシステム設計者（すなわち、SE）の多くはいわゆるITを専門としてきた人ではなく、むしろ社会学などの専門家でした。時にして、狭い範囲でしかものを見ないIT技術者よりも、そういった他分野の専門家のほうが、「システム」の設計に適しており、才能を発揮したのです。

最近は、幸か不幸かIT技術もより複雑になってきたために、計算機システムの設計も専門のIT技術者の能力が要求されています。

しかし、その反面、トータル「システム」の設計への気配りが疎かになっていないでしょうか。

昔は、いわゆる「使いやすさ」とか、「Man Machine Interface」という言葉で、この気配りの欠如を戒めてきました。これに対して、私達は「セキュリティ」という新しいキーワードで、この「システム」設計への気配りを進めなければなりません。

認証技術を知っている、セキュリティ・ホールへの対策を熟知している。こういった技術者を越えた、新しい「セキュリティ技術者」の育成のために、ぜひJNSAの活躍を期待しています。

公的個人認証サービスの技術

PKI相互運用技術 WGリーダ
セコム株式会社 IS研究所
松本　泰

2004年1月29日、地方公共団体が市民に電子証明書を配布する公的個人認証サービスが開始されました。公的個人認証サービスは、いくらか物議をかもしている住民基本台帳ネットワークの情報を元にしていることに対する不安の声や、民業を圧迫する官製認証サービスという批判の声もあるようです。しかし、現状では、公的個人認証サービスに関する技術情報は少なくその技術や背景を的確に理解している人も少ないと思われます。こうした事が、よく知られていない、そして分からないものに対する不安を掻き立てている面も否めないのではないでしょうか。私自身は、公的個人認証サービスの課題は多々あると感じていますが、まずは、多くの人々が、その背景などを正確に把握することが重要だと考えています。

本稿では、現在、公表されている資料や実際の証明書などの情報から、公的個人認証サービスの技術面の説明を行いますが、紙面の都合から信頼モデルを中心について説明するとともに今後の課題について考察します。

1.「公的個人認証サービス」の開始

これまで、中央政府の官職に証明書を発行する政府認証基盤GPKI、地方公共団体の職員に証明書を発行する地方公共団体組織認証基盤LGPKI、そして、民間の認証局が整備されてきました。そして、これらの認証局の証明書ユーザ間で、B2G（民間と政府間）、B2LG（民間と地方公共団体間）における電子申請、電子入札などで利用が始まっています。しかし、こうした認証基盤は業務上必要な人々が利用するだけで一般の市民には無縁な存在でした。公的個人認証サービスの開始で、C2G（市民と政府間）、C2LG（市民と地方自治体間）で認証基盤が利用可能な状況になりつつあります。公的個人認証サービスと、既に運用を開始しているGPKI、LGPKI、そして民間認証局などが揃い、これによってようやく日本の行政系の認証基盤の基本的な整備が出来たことになるかと思います。特に公的個人認証サービスは、広く市民が利用できるということから、これからのIT社会、電子社会への移行において、重要な役割を果たすと考えられます。

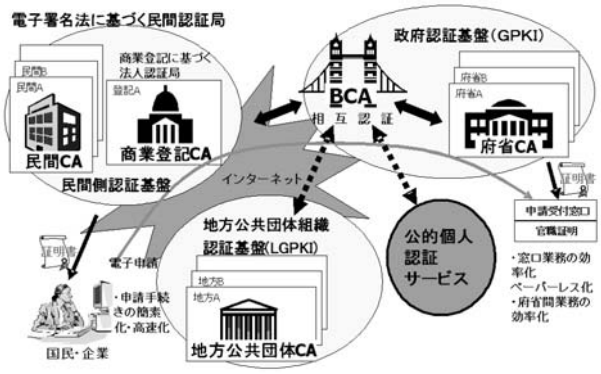


図1

2. 公的個人認証サービスの認証局

公的個人認証サービス（JPKI）の認証局（CA）は、市民に証明書を配布する都道府県CAと、各都道府県CAにCA証明書を発行するJPKIブリッジCAから構成されます。

都道府県CAは、市民に向けて公的個人認証サービスの証明書を発行します。都道府県CAは、各都道府県毎にひとつずつCAが存在します。例えば、三鷹市民であれば、東京都CAが証明書を発行します。この都道府県CAは、自己署名証明書を持った単独で運営が可能な独立したCAとなっています。また、都道府県CAは、JPKIブリッジCAへCA証明書を発行しています。この意味は後で説明します。

次にJPKIのブリッジCAがあります。JPKIのブリッジCAは、各都道府県CAにCA証明書を発行して

いる他、他のドメイン、すなわち、GPKIのブリッジCAへCA証明書（相互認証証明書）を発行しています。この相互認証証明書も後で説明します。通常ブリッジCAは、ユーザの信頼点にはならない、すなわちいわゆるroot CAにはなりません。それに対して、JPKIのブリッジCA はJPKIのWebアプリケーションの信頼点となっているようでありJPKIのWebサーバへSSL証明書を発行しています。

以下に認証局（CA）と証明書の関係を示します。

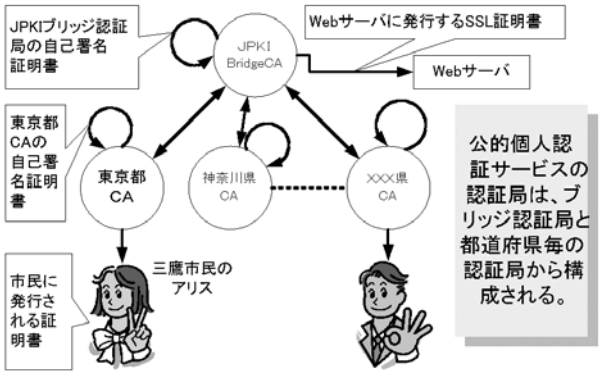


図2

3. 公的個人認証サービスと住基カード

公的個人認証サービス（JPKI）の「証明書と鍵」は、住基カードのJPKI領域に格納されます。JPKIの「証明書と鍵」の格納先は、住基カード以外でもかまわないとされていますが、現時点では、住基カード以外の選択肢はまだないようです。

住基カードのJPKI領域は、住基カード上のひとつのアプリケーションとして領域が確保され、その領域のためのパスワードで保護されます。ちなみに、住基カードを最初に取得した時にもパスワードを設定しますが、これは、住民基本台帳コード（住基コード）を住基カードに格納するためのアプリケーションのパスワードということになります。

住基カードのJPKI領域には、この住基カードホルダーの証明書（公開鍵証明書）とこの証明書に対応した秘密鍵（Private key）が格納される他、この証明書を発行した都道府県CAの自己署名証明書が格納されます。この領域には住基コード自体は格納されませんが、格納されている証明書には、基本4情報と呼ばれる、氏名、生年月日、性別、住所が含まれています。

住基カードのJPKI領域に格納される秘密鍵は、カード保有者の電子署名に使われる非常に重要な鍵です。この秘密鍵は、市町村のJPKIの発行窓口にある鍵ペア生成装置からローディングされます。そして、一旦ローディンされると、この秘密鍵は一生カード外には決して出ない仕組みとなっています。そのため、電子署名は必ずカード上で行われます。

都道府県CAの自己署名証明書も非常に重要な役割を果たします。この証明書の公開鍵は、住基カードホルダーの信頼点となります。市町村のJPKIの発行窓口が、住基カードホルダの信頼点をセキュアに渡し、住基カード上にセキュアに格納そして保護されるということが重要なポイントになります。

4. 公的個人認証サービスの証明書

JPKIは、市民に証明書を発行するのがその役目となります。しかし、JPKIではその他の色々な証明書を発行しています。以下にJPKIで発行される証明書の種類を示します。紙面の関係上個々の証明書については説明できませんが、ここでは、色々な証明書が発行されていることを覚えておいて下さい。

証明書の種類	発行認証局	内　容
BCA自己署名証明書	JPKI BCA	Webサーバなどの信頼点
相互認証証明書	JPKI BCA	都道府県CAへ発行。JPKIリポジトリに公開される。
相互認証証明書（GPKI）	JPKI BCA	GPKIのBCAへ発行
Webサーバ証明書	JPKI BCA	JPKIドメイン内のWebサーバ
コードサイニング証明書	JPKI BCA	アプレットなどへの証明書
都道府県自己署名証明書	都道府県CA	市民の信頼点。JPKIのICカードに格納される。
相互認証証明書	都道府県CA	JPKI BCAへ発行。JPKIリポジトリに公開される。
OCSPサーバ証明書	都道府県CA	JPKI外から証明書の失効を検証
証明書検証サーバ証明書	都道府県CA	市民が官職の証明書を検証
市民向け証明書	都道府県CA	個人の証明書。JPKIのカードに格納される。

5. 公的個人認証サービスの信頼点と証明書パス

ここで三鷹市民のアリスが登場します。アリスがJPKIの証明書発行を受けると、アリスの住基カードのJPKI領域に証明書と秘密鍵が格納されます。秘密鍵がセキュアに格納されることは、非常に重要なことですが、それとともに、アリスの信頼点がセキュアに渡されることも重要なポイントです。住基カードのJPKI領域に、アリスの信頼点である東京都CAの自己署名証明書が格納されますが、アリスはこの信頼点を手がかりに、JPKIに関連した信頼関係を検証することになります。

アリスが電子申請を行なったとします。アリスとA省大臣は、異なった認証主体、すなわち、別の認証ドメイン（別のポリシのドメイン）に所属しています。このような場合、JPKIとGPKIブリッジ認証CAが相互認証することにより、異なるドメインでの検証が可能になります。PKIにおいて相互認証とは、異なるドメインへCA証明書を発行することを意味します。異なるドメインへ発行するCA証明書の意味は後で説明します。

ここでは、アリスがA省大臣の署名を検証する場面を説明します。図3は、アリスの信頼点からA省大臣までの証明書パスなるものを示しています。アリスの信頼点は住基カードにセキュアに保管されています。アリスの信頼点である東京都CAの公開鍵は、アリスに発行された公開鍵証明書や秘密鍵と共に住基カードのJPKI領域に格納されています。アリスは、最初にこの信頼点の公開鍵のみを信頼します。この公開鍵を使って、東京都CAからJPKIブリッジCAへ発行している証明書の検証を行います。この検証が成功するとJPKIブリッジCAの公開鍵を信頼することができます。このJPKIブリッジCAの公開鍵を信頼することができると、JPKIブリッジCAからGPKIブリッジCAへ発行したCA証明書（相互認証証明書）の検証ができます。このようなことを続けていくとA省大臣に発行された証明書の検証ができます。この一連の作業は、証明書パス検証と呼ばれています。証明書パス検証が成功しA省大臣の公開鍵証明書が信頼できるとなると、その証明書に格納された公開鍵からA省大臣の署名文書の検証が可能になります。こうした検証は、アリスの住基カードのJPKI領域にセキュアに保護された公開鍵（東京都CAの自己署名証明書）が起点になっていることが重要なポイントです。

JPKIの場合、（官職）証明書検証サーバなるものが用意されています。実際の証明書検証はこのサーバに依頼して行うことができます。しかしこのサーバの応答の署名の検証は、やはり、アリスの信頼点である東京都CAの公開鍵を使って行われることが重要なポイントです。

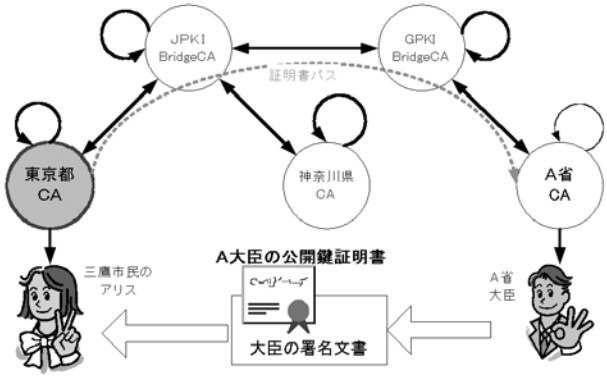


図4

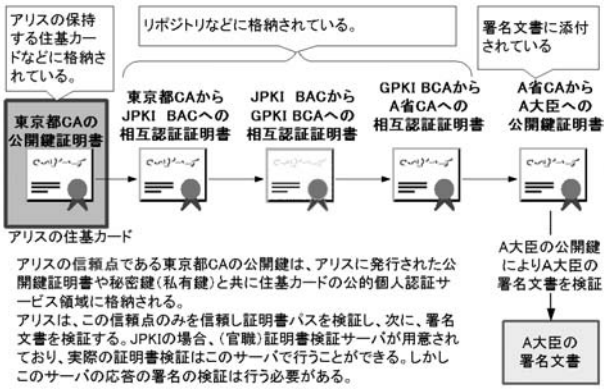


図5

6. 公的個人認証サービスのリポジトリとアプリケーションの構成

PKIではよくリポジトリなるものが出てきます。リポジトリには、一般に証明書ユーザ間で共有される色々な情報が置かれますが、これらの情報は、CAの署名が付与されてリポジトリに置かれます。このリポジトリは、JPKIの場合バックエンドに隠れているとも言えます。しかし、リポジトリ自体は存在し重要な役割を果たしています。JPKIでは、リポジトリにLDAPサーバが使用されており、証明書失効リスト(CRL)や自己署名証明書、相互認証証明書ペアなどが置かれます。これらは、証明書パスの構築や各証明書の失効検証のために利用されます。

署名検証者のアリスは、証明書パス検証のためにリポジトリ(LDAPサーバ)をアクセスしますが、アリスは、リポジトリに格納されたデータの内容を無条件に信頼するわけではありません。アリスの信頼点を元に証明書パス検証を行うことが重要です。

図6は、JPKIのクライアントのJPKIアプリケーション環境を示しています。アリス固有の情報でアリスのみがアクセスする情報である証明書や鍵をクレデンシャルと呼ぶことがあります。このクレデンシャルはアリスが保持する住基カードに格納され、そのクレデンシャルをアクセスするAPIが存在します。JPKIの証明書の取得時に配布されるCD-ROMには、この住基カードの公的個人認証サービスのクレデンシャルをアクセスするためのAPIであるPKCS#11モジュールやMicrosoftのCryptoAPIのためのCSP(Cryptographic Service Provider)といったものが含まれています。

証明書ユーザ間で共有する情報はリポジトリから取得します。これらの情報の多くは、証明書の検証を行なうために存在します。JPKIでは、官職証明書検証サーバが用意されているため、証明書ホルダーが、直接リポジトリにアクセスする必要はありません。しかし、官職証明書検証サーバのメッセージ自体は、やはり、住基カードのJPKI領域に格納されたアリスの信頼点を利用して検証を行います。また、この官職証明書検証サーバにアクセスするためのライブラリもCD-ROMからインストールできるようです。

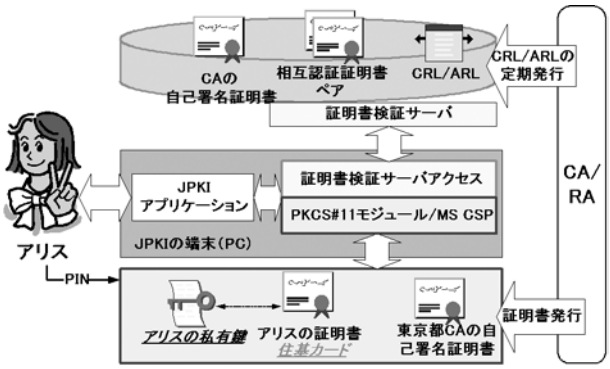


図6

7. 公的個人認証サービスの証明書ポリシーとポリシマッピング

証明書ホルダーの証明書には、証明書ポリシー拡張なるものが含まれています。この証明書ポリシー拡張には、この証明書のポリシーを現すOID(Object Identifiers)が記述されていますが、この証明書ポリシーOIDに対応するポリシーの文書は、東京都認証局運用規程などに記述されています。JPKIの場合、東京都CAに限らず、全都道府県CAで同じOID(1.2.392.200149.8.5.1.1.10)を使用しています。つまり証明書ポリシーを共有しています。例えば東京都CAは、将来東京都民だけのために独自のポリシーを持った証明書を発行することが可能だと考えられます。しかし、現時点では各都道府県CAは同一のポリシーの証明書のみを発行しており、JPKI全体でひとつのドメインを形成していると言えます。

これに対して、GPKIのブリッジCA、各府省CA、各民間CAは、独自の証明書ポリシーを持っています。こうした場合、異なったドメインを乗り越えるためのCA証明書を発行します。JPKIブリッジCAからGPKIブリッジCAへ発行しているCA証明書は、

JPKIの証明書ホルダーの証明書ポリシーと同等のポリシーで検証を行うために、ポリシマッピング拡張なるものが含まれています。このポリシマッピング拡張を含んだ証明書では、証明書発行ドメインのポリシーと、相手のドメインのポリシーが等価であることを宣言することができます。こうした証明書は、相互認証証明書（Cross Certificate）と呼ばれますが、これは、認証ドメインを横断するための証明書ということになります。

JPKIドメイン内では、証明書ホルダーに発行されている証明書以外にも、色々なポリシーの証明書が発行されています。しかし、他のドメインに渡って証明書のパスが検証できる、すなわち、ポリシマッピングが行なわれるものは、証明書ポリシーのOIDの末尾が10のものに限られます。これらの証明書の証明書ポリシー拡張は、クリチカルというフラグが設定されており、処理を必須としています。このように、ドメインを横断するために相互認証証明書が発行されますが、色々なポリシーの証明書が全て他のPKIドメインで有効になるわけではありません。これは、逆に言えば、JPKIドメインでは、自ドメインのユーザの利便性のために、自ドメインにおいてのみ有効な色々な証明書を発行できるということです。

この証明書のポリシーなどにより信頼を制御することをポリシー制御と呼んでいます。ポリシー制御を前提とした場合、証明書には各種の制約拡張なるものが含まれるのが普通です。この制約拡張は、証明書パスの検証を制約する方向に機能します。例えば、アプリケーションの要求により自ドメインのみを信頼するとか、自分の信頼点から遠く離れたCAは信頼したくないといったことが制約にあたります。これは、色々なドメインのPKIを相互認証する場合、特に重要な機能と言えます。ポリシー制御は、小規模なPKIやクローズドなPKIなどにおいては必要のない機能だったため、あまり知られていない面があります。しかし、オープンで広い認証ドメインにおいて、色々なポリシーの証明書が発行される中、自分の要求するポリシーの証明書を受け入れるための重要なメカニズムだと考えられます。

図7に、JPKI、GPKIにおけるポリシマッピングの様子を示します。“CP=J.10”は、JPKIの市民向けの証明書ポリシがOID（1.2.392.200149.8.5.1.1.10）であることを意味します。“PM J.10=X.10）は、JPKIのドメインのJ.10という証明書ポリシーが、GPKIブリッジCAドメインのX.10という証明書ポリシーと等価であるというポリシマッピングを行なっています。

JPKIの署名の検証における証明書パス検証は、ポリシー制御を行なうことを想定され、証明書には各種の制約拡張が含まれます。それに対して、WebサーバのSSL認証では、ブリッジCAから発行される自己書名証明書を信頼点とすることにより、単純な証明書パス検証のメカニズムのみを利用しています。こうすることにより、多くのブラウザ環境において動作させることを可能にしています。ブリッジCAから発行される自己署名証明書は、JPKIの証明書の取得時に配付されるCD-ROMからPCにインストールされます。逆に官職の証明書の検証には、ポリシマッピング拡張や、他の複雑な制約拡張の解釈を含んだ証明書のパス検証が要求されます。JPKIでは、官職証明書検証サーバを利用することにより、クライアントのソフトウェアの負担を減らしています。

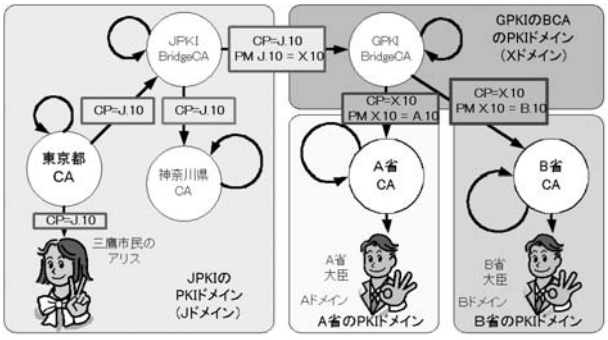


図7

8. 公的個人認証サービスの課題

公的個人認証サービスと似たようなサービスは、世界中で実施、または計画されています。実社会に

おける身分証明書が電子化したものは、よりバーチャルなこれからの情報化社会、ネットワーク社会、そして電子社会においてより重要なものになると考えている地域や国は多いのでしょう。しかし現在まで、こうした電子身分証なるものが成功した事例はまだ少ないようです。これから電子社会には必要になると考えられるが現在のところあまり使い道がないというのが一般的な状況のように見えます。日本の公的個人認証サービスも、現在の延長線上だけでは広く使われるとは考えにくい面があります。しかし、多くの地域や国で検討されているように、公的個人認証サービス、ないし似たようなサービスが来るべき電子社会において必要になると考えている方はやはり多いのではないかと思います。それは、本格化するネットワーク社会を成熟したものにするためには信頼の拠りどころが重要だと考えられているからです。そうした中、このようなサービスが、日本においてどのように計画されているのか、また、どのような技術で実現しようとしているのかといったことは非常に分かり難いものがあります。やはり広く技術情報が公開され多くの人にその内容が理解されることが望まれます。

公的個人認証サービスの普及の鍵のひとつは、セキュアで、かつ、使いやすいアプリケーションが数多く開発されることだと考えられます。しかし現実には、使いやすいアプリケーションを開発しようにも、あまりにも正確な情報が少ないのが現状ではないでしょうか。公的個人認証サービスに限らず、行政に関連したITに関する技術情報は、多くの場合、個々の政府機関や、業界団体などが情報を抱き込んでしまっており、そのため正確な情報が流通していないのが現状に見えます。これは、IT施策に関係している行政関係の方や、ITに関する行政関係の仕事に携われている多くの方にとっても全体像を的確に把握することを非常に困難なものにしています。公的個人認証サービスに関しても、使いやすくセキュアなアプリケーションの開発を促進することを阻害しているように見えます。

以上のようなことも踏まえ、JNSAのチャレンジPKIプロジェクトでは、技術的な観点からオープンで比較的大規模なPKIの相互運用技術の問題点を解決することを目標として活動を行っています。活動のひとつに、政府認証基盤（GPKI）の仕様に基づく相互運用テストフレームワークなどの開発があり、これはGPKIなどのアプリケーションの開発を促進することを目標としています。また、幅広い認証ドメインにおけるPKIのベストカレントプラクティスを示す「マルチドメインPKIの相互運用性に関するメモ」をIETF（Intenet Engineering Task Force）のRFCとして提案するなどの活動も行っています。IETFでの提案は、広く世界に受け入れられる必要があり、そのため、欧米の動向を調査するだけでなく海外とのPKIイニシアチブと連携していくことを検討しています。そして、こうした活動の成果をフィードバックすることにより、現在の技術の状況や、今後の電子署名・認証フレームワークの方向性を多少なりとも示すことができないかと考えています。本稿は、そのほんの一部分ですが、多少なりとも参考になれば幸いです。

参考文献

「公的個人認証サービス」は必要なのか
http://www.rieti.go.jp/it/column/column040210.html
公的個人認証サービスポータルサイト
http://www.jpki.go.jp/
Challenge PKI ホームページ
http://www.jnsa.org/mpki/index_j.html

セキュリティAPIに関する技術調査

富士ゼロックス株式会社
稲田　龍

JNSAでは、独立行政法人情報処理推進機構（略称: IPA Information Technology Promotion Agency）の「2003年度 情報セキュリティ関連の調査に関する公募」のテーマ4の「セキュリティAPIに関する技術調査」に応募し、採択された。
「セキュリティAPIに関する技術調査」の目的は、IPAのホームページにある公募要領に述べられている（http://www.ipa.go.jp/security/kobo/15fy/isec2/index.html）。

> セキュリティ機能の実装に関しては、開発者によるプログラムの作成負担を軽減し、入出力や設定等を統一するための汎用APIが整備されている。ソフトウェアベンダーにおけるセキュリティ機能の実装を促進するにあたっては、セキュリティAPIを用いた設計・実装のための最新の技術情報を提供する必要がある。（公募要領P.5より抜粋）

この公募要領を受け、JNSAでは、セコム株式会社IS研究所、大日本印刷株式会社、オレンジソフト株式会社および富士ゼロックス株式会社と共同で調査を行い、2003年11月末に報告書の納品をした。
納品物はすでにhttp://www.ipa.go.jp/security/fy15/reports/sec_api/index.htmlで公開されている（サンプルプログラムは現時点2004/3/4では未公開であるが、追って公開が予定されている）。
また、同時にIPA公募のテーマ3「タイムスタンプ・プロトコルに関する技術調査」の採択も受けた。「タイムスタンプ・プロトコルに関する技術調査」に関しては、次回に報告する。
「タイムスタンプ・プロトコルに関する技術調査」の納品物もhttp://www.ipa.go.jp/security/fy15/reports/tsp/index.htmlにて公開済みである。

「セキュリティAPIに関する技術調査」を行うにあたり、開発者が実際にAPIを利用する局面において具体的に有用となる情報の提供を目的とし、個別のAPIという観点ではなく、API群を横断する技術や機能という観点からAPI関数の利用に役立つ情報に焦点を絞って報告を行うことを目標とした。
具体的には、以下の四点に重点を当て、調査を行った。

1. セキュリティAPIのアーキテクチャ
2. セキュリティAPIが共通に提供する重要な機能
3. 普及しているプラットフォーム上で提供されているセキュリティAPIの利用法
4. 近年の技術動向の中で重要性が増している新しいセキュリティAPI

報告書は全部の6つのパートよりなる。各々のパートの表題は以下のとおりである。

Part 0. 報告書の構成、セキュリティAPIの利用に関する提言
Part 1. セキュリティ API の概要、アーキテクチャ、機能、暗号技術とアルゴリズム
Part 2. Java JCE（Java Cryptographic Extensions）：機能と利用法
Part 3. .NET Crypto API：機能と利用法
Part 4. ICカードなどのハードウェアトークンAPI
Part 5. バイオメトリック認証のAPI

Part 0では、報告書のサマリと電子政府に対しての提言を行っている。

Part 1では、セキュリティAPIが共通に前提とする階層アーキテクチャについて報告し、次いで、セキュリティAPIが提供する主要な機能について概説している。また、暗号技術とアルゴリズムに関して、セキュリティAPIの機能を理解する上で最低限必要となる知識の整理が行われている。

Part 2およびPart 3では、主要なプラットフォームであるJavaとWindowsの上で提供されるセキュリティAPIである、Java Cryptography Extension（JCE）とMicrosoft Windows .NET CryptoAPIにつ

いて報告した。それぞれのAPIについて、APIの基本的な構造を述べた後、API上を利用した上位のアプリケーションの開発方法およびプリミティブの暗号機能を提供する下位のプロバイダモジュールの開発方法に関して、サンプルプログラムを例示しながら解説を行った。特に、サンプルプログラムは、JCEとCryptoAPIとで同じ機能を実装しており、比較することでより具体的な理解が得られる様に考慮して作成した。

Part 4では、クレジットカード、交通機関、住民基本台帳などの利用で注目を集めているICカードなどのハードウェアトークン上でのセキュリティAPIを報告した。まず、ICカードなどのハードウェアトークンを利用するアプリケーション開発のための主要なセキュリティAPIとして、PKCS #11とCSP(CryptoAPI)を取り上げ、基本的な構造やサポートされている関数を整理し、開発上の留意するべき点を述べた。PKCS #11とCSPを相互に運用する場合の留意点についても述べた。また、ICカード内のファイル構造の標準としてPKCS #15を、ICカードのハードウェアの差違を隠蔽し共通の開発環境を提供するための標準化動向としてGSC-ISを報告した。

Part 5では、人間の生態的な特徴・特性に基づく本人認証(バイオメトリクス認証)のためのセキュリティAPIとして策定中のBioAPIを取り上げ、基本的な構造やサポートされている関数を整理し、開発上の留意するべき点を述べた。また、近年その重要性の認識が進みつつある、バイオメトリクス認証とスマートカード・PKIとの連携について述べるとともに、GSC-ISのバイオメトリクス認証への対応状況を解説を行った。

これらの調査の元に、以下にあげる電子政府に対してセキュリティAPIの利用に関する提言を行っている。

1. アプリケーション実装者が、どのセキュリティAPIを使うべきなのか、どのようにセキュリティAPIを利用するべきなのかを明確にした資料の作成とその更新、教育が必要である。
2. セキュリティ業界に対して、必要とされるセキュリティAPIの作成支援をすべきである。そのために必要となる、技術の供与、人材の育成を行なうべきである。
3. また、3に述べるように標準化に対して積極的に関与し、独自のものとしないようにしなければならない。
4. セキュリティ関連技術は、多くの標準が定められており、それらをベースに複数のセキュリティAPIが定義されつつある。
5. セキュリティに関する標準／セキュリティAPIは、複数の学会、業界団体、標準化団体において議論され策定されている。今後、アプリケーションが必要とするセキュリティプロトコル、セキュリティ技術に関して米国政府がICカードに対してGSC-ISを定義したように、わが国においてもこれらの学会、業界団体、標準化団体に対して標準化の状況の情報入手、標準化への関与を行なうべきである。
6. セキュリティAPIが正しく実装されている事、相互運用性に問題がない事を確認するための手法、手続きの策定とこれらの確認を行なうための仕組み、運用を考えるべきである。

以上、今後PKIを利用したアプリケーションを開発する際に一番大きな問題となるセキュリティAPIの標準化を見据え、関係者が共有してほしい情報を整理してまとめてある。ぜひ本文をご参照していただけると幸いである。

JNSA ワーキンググループ紹介

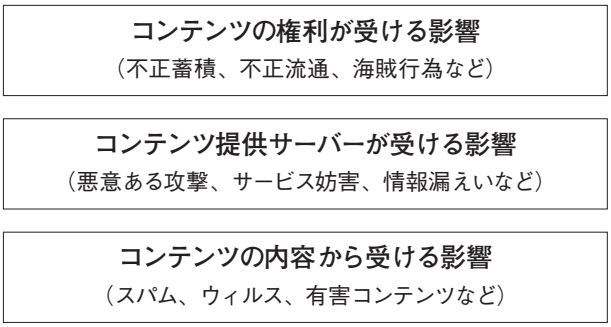
コンテントセキュリティ WG

コンセントセキュリティWGリーダー
株式会社ネットアーク
松本　直人

2004年2月に日本ネットワークセキュリティ協会コンテントセキュリティワーキンググループの第二回会議が行われた。セキュリティ技術の進展に伴い、新たに「コンテンツセキュリティ」技術の適応範囲が広がり、定義整理と実態把握が必要とされてきていたためコンテントセキュリティワーキンググループでは整理にあたることにした。

2002年度にまとめた「コンテンツセキュリティ・ガイド」では、コンテンツの不正蓄積、不正流通、海賊行為など「コンテンツの権利が受ける影響」をメインとして掘り下げた資料である。当時ストリーミングデータの不正蓄積、P2Pファイル交換による不正流通などのコンテンツの権利と保護技術を取り巻く環境が大きく変化した年でもあった。コンテンツ保護技術と実態を正確に把握し多くの技術者に伝えるため「コンテントセキュリティ・ガイド」が作られたのである。コンテンツ権利保護技術であるデジタル著作権管理（Digital Rights Management: DRM）システムの普及も多くはなく、著作権管理自体にも標準的に普及している状況では当時はなかった。現在は多くのサイトでDRM 技術を用いたコンテンツ権利保護と著作権管理が行われるようになり、技術的にも成熟してきていると言えるだろう。そこからさらに数年が経過した現在、コンテンツにまつわる様々な影響を現象としたセキュリティ上の問題点とその対策技術が開発されてきた。

コンテンツセキュリティの定義整理



ワーキンググループでは議論を経て、コンテンツセキュリティの定義を3つの分類として整理を行った。整理の基本スタンスはコンテントにまつわる影響を尺度とし、分類を行った。今後はこれら整理に則って技術詳細などを分類していきたいと思う。

コンテントセキュリティワーキンググループ議事録メモより抜粋

● コンテンツの権利が受ける影響（作品を主体とした考え方）
　・コンテンツ（作品）自体の保護
　・作品改ざんに対する保護・著作権保護など
　　→対策：電子透かしによる作品管理・DRMによる著作権保護、
　　→セキュリティが破られたときには作品の流出や改ざんなどの損害。

● コンテンツの内容から受ける影響（人を主体とした考え方）
　・人為的・故意的な不正アクセス保護
　・spam mail ,Virus, Worm などによる被害からの保護
　　→対策：Anti Virus, Anti spam製品による保護
　　URL filerなどによる保護
　　→セキュリティが破られたときにはVirusなどの被害等の損害
● （システムを主体とした考え方）
　・コンテンツを管理しているserver、ネットワークなどシステム機器に対する保護、将来的にはネット家電も?
　　→対策：IDS,アプリケーションファイアーウォール, IDP
　　Reverse Proxyなどによる保護
　　→セキュリティが破られた際には企業の信用などに損害

そして上記3点に共通して、運用管理および監視が必要。


コンテントセキュリティWGでのひとコマ

JNSA ワーキンググループ紹介

不正プログラム調査WG

不正プログラム調査WGリーダー
株式会社アークン
渡部　章

■ はじめに

近年、トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加しています。また、ウイルス、ワームも同様に近年では不正アクセスを目的としたものも少なくありません。実際の不正アクセス技術ではこれらのツールを組み合わせて利用するケースが多くなっています。これらの現状を踏まえ、本ＷＧは、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ために発足しました。

■ 活動の目的

本ＷＧでは、様々な不正プログラムを分類化し、その利用目的を明らかにし、各分類における代表的な不正プログラムと、昨今話題となっている不正プログラムのメカニズムを説明できるような資料を作成公開します。これらのプログラムの中には、ネットワーク管理ツールとして正規に使用しているものも多く、使用目的や使用者によっては、不正プログラムになってしまうグレーなプログラムも多くあるため、両刃の剣といえます。そのために既存のセキュリティ技術では対象とされていなかったり、脅威として意識していないユーザも多いようです。そこで、本ＷＧでは具体的な対策方法も示して、この種の技術に関する正しい知識を広めていきます。また、既存のセキュリティ技術のこれら不正プログラムによる侵入、攻撃に対する有効性を検証します。

■ 現在までの進捗

本ＷＧが発足した平成14年度は、SQL Slammerワームが大量発生し、インターネットのインフラに多大な被害を出しました。その時、本ＷＧのメンバー達は平成13年に猛威を振るったCordRedの被害からの教訓を何故生かせなかったのかについて、大きな疑問を抱きました。そこで、初年度の調査・研究として「メモリ感染型のワーム」について、構造、被害状況、対策について「メモリ感染型ネットワーク・ワームの脅威とその対策」というタイトルで取りまとめました。その成果として、2003年6月2-3日に東京国際フォーラムにて実施されたNSF2003 springにてＷＧ活動発表を実施しました。
http://www.jnsa.org/result.html

また、平成15年度は、不正プログラムの定義、分類、構造、対策について、「不正プログラム対策ガイドライン」というタイトルで取りまとめました。

■ 今後の予定

今後本ＷＧは、基本的に隔月の会合を実施し、年一回の合宿にて成果物を取りまとめていきます。

平成16年度は、近年話題になっている、不正なアクティブ・コンテンツについて調査していきたいと考えています。これらの不正なプログラム・コードは、Javaアプレット、ActivXコントロール、Javaスクリプト、Visual Basicスクリプトなどで作成されており、

不正プログラム	好意的な使用	悪意ある使用
スパイウェア	システムの稼動監視、ユーザサポート支援	重要情報の不正取得
キーロガー	ユーザの動向監視	パスワードの不正取得
パケットアナライザ	ネットワーク管理支援、トラブル対応	パスワードや重要なデータの不正取得
脆弱性検知ツール	セキュリティレベルの管理	攻撃対象の選定

Web閲覧時やHTML形式のメールによって、ユーザの意図しない危害を与える可能性があります。不正なアクティブ・コンテンツのことを各対策ベンダーでは、Malicial Mobile Cord、もしくは、Vandal Cordと呼んでいます。

また、将来は、ユーザが不正プログラムの脅威について、わかりやすく理解できるように、ウイルスやトロイの木馬、また不正なアクティブ・コンテンツを擬似体験できるWebサイトの構築も検討しています。

■ おわりに

ウイルスによる被害は、他のセキュリティ被害に比べて圧倒的なもので、これは今後も継続するに間違いないでしょう。ただし、ウイルス対策ソフトウェアなどの既存セキュリティ技術では対策が十分ではない「メモリ感染型のワーム」による感染や、キーロガーなどのトロイの木馬や、スパイウェアなどによる情報漏えいの被害は、新しい脅威として、間違い無く多大な被害をユーザや社会に与えるでしょう。これらの背景から本ＷＧは、不正プログラムをウイルスだけに留めず、広範囲にその現況と対策について調査研究を実施していきます。

会員企業ご紹介⑩

株式会社エス・アイ・ディ・シー
(http://www.sidc.net/)

株式会社エス･アイ･ディ･シーは「誰もが安心してネットワークを利用できる環境を整備することにより、ITを利用したビジネスのさらなる発展と社会に貢献できる企業となる」ことを目的として2001年8月に設立された情報セキュリティ総合コンサルティング会社です。
SIDCのコアバリューである「人材」「プロセス」「技術力」を活かし、主事業として、セキュリティコンサルティング事業とセキュリティ専門ポータル事業を展開しております。
特に2004年4月から本格始動するセキュリティ専門ポータル事業は、新たな手法でセキュリティ情報、ツール、サービス、教育をご提供するASPサービスで、既に様々な方面の方々に評価を頂いております。

◆SIDCコンサルティングおよび技術チーム

弊社コンサルティングチームは、北米のセキュリティ業界において実績のある世界トップレベルのセキュリティ技術者を組織化したプロフェッショナルの集団です。
メンバーは、政府系機関/軍事/金融/医療/航空/通信・メディア/公共サービス/IT/コンサルティング会社などあらゆる業界で、セキュリティ担当責任者や技術責任者を歴任し、脆弱性研究や、セキュリティコンサルティング、またセキュリティ教育や情報提供を行ってきました。
また、セキュリティ教本や関連書籍、セキュリティ雑誌への執筆、セキュリティに関するコラム・インタビューなどのアドバイス、セキュリティ関連Webサイトの運営および情報提供など、世界のセキュリティ発展の為の活動にも参画しております。
メンバーのうち6名が、世界のセキュリティ技術資格の中でも非常に信頼度の高い公認情報システムセキュリティプロフェッショナル(CISSP)の取得者です。また、CISSP以外にも公認情報システム監査人(CISA)、公認情報セキュリティマネージャー(CISM)、米国認定資格、ベンダー認定の上級資格など幅広い資格を保持しています。
これら、北米での長年にわたる実務経験と、有資格者により、あらゆる分野で網羅された専門知識から、洗練された方法論を導き、顧客ニーズに合わせたサービスをご提供してきました。

◆SIDCの世界的ネットワーク

コンサルティングチームの強みである「最先端のセキュリティ情報取得のためのヒューマン・ネットワーク」は、世界各所に配置されたセキュリティアナリストによって成り立っております。
セキュリティといっても非常に幅が広いのですが、情報セキュリティ、IDS、OSセキュリティ、ファイアウォール、ハニーポット、ウィルス・ワーム、ネットワークデバイスなど、あらゆる分野で活躍している著名なセキュリティアナリスト、権威者、研究者がSIDCをサポートしています。(※)
コンサルティング業務としての技術上の協力要請はもちろんのこと、セキュリティや脆弱性に関する最新情報などをいち早く入手することができます。

より強固なセキュリティを実現するためには、「あらゆる局面をカバーすること」「豊富な実務経験＋知識(情報)」、「実現のための高度な技術力」が必要条件であると弊社は考えております。これらの経験(実務)に基づいたコンサルタントと、リサーチチームからの最新セキュリティ情報により、クオリティの高いセキュリティサービスをご提供していきます。
(※セキュリティカンファレンスPacsec開催)

2003年11月6日7日の2日間において、SIDCの技術者およびセキュリティ専門家のネットワークを活用し、日本初のホワイトハットセキュリティカンファレンスを実施しました。
2004年秋第二回開催予定。(www.pacsec.jp)

お問い合わせ先
株式会社エス・アイ・ディ・シー　営業統括本部
〒101-0021
東京都千代田区外神田5-5-15　K'Sビル
Tel:　03-5807-6636
Fax:　03-5807-6637
e-メール：info@sidc.net

京セラコミュニケーションシステム株式会社
(http://www.kccs.co.jp/)

THE NEW VALUE FRONTIER
KYOCERA

京セラコミュニケーションシステム株式会社（KCCS）のトータルセキュリティーソリューション

ネットワークやシステムにおけるセキュリティ対策は、企業にとって最重要課題の一つとなっています。まず、侵入されない、対処よりも予防に重きをおいたセキュリティ対策を行うこと。そして、トラブルが発生した場合にもシステムのダウンタイムを最小に抑え、ビジネスチャンスの損失を防ぐために、脆弱性検査から不正侵入/改ざん検知、データ復旧までのトータルな対策が必要です。また外出先からノートPC、PDAなどのモバイルツールで社内システムに接続することが当然になり、モバイルを前提とした業務をビジネスに取り込む企業も増加してきました。万一被害を受けた場合、ビジネス停止やパートナー企業、取引先からの信用失墜の影響等も含めると、そのコストは巨額です。セキュリティに携わる技術担当者、マネジメント層だけでなく、経営者も含めてセキュリティに対する全社的な共通理解が不可欠なのです。KCCSでは、これらの課題を解決する多彩なセキュリティソリューションを提供しています。

【セキュリティリスク管理システム nCircle IP360】

当社では、セキュリティの判断基準をわかりやすく数値化できるセキュリティツール「nCircle IP360」を提供しています。ほぼリアルタイムで脆弱性を検出し、検査結果に基づいた効率的な侵入検知を実施。必要な対処方法も指定することで、ネットワーク管理者の作業負荷を大幅に軽減します。

nCircle IP360は、nCircle社独自の脆弱性検査方式"Reflex Testing"を用いてネットワークの脆弱性検査を行います。検査対象に疑似アタックを行う従来型の脆弱性検査ツールと異なり、検査対象機器に負荷を与えないため、ネットワークへの常時検査を可能にしています。セキュリティの現状を技術担当者、マネジメント層だけの閉じた専門家の範囲に止まらず、経営者に対しても「見せる」「わかる」「共有する」ことのできる次世代型セキュリティリスク管理システムです。

- 常時自動検査による運用負荷を大幅に軽減
- 従来不可能だった常時脆弱性検査と、誤検知を大幅に削減した侵入検知を実現
- システム内の危険度を数値化して表示
- 不正アクセス/セキュリティホールの対策方法を表示
- 広範囲な脆弱性検査による、企業内のセキュリティポリシーの監視も可能

【不正改ざん検知システム Tripwire】

企業システムのデータとネットワークの完全性を常に監視し、外部のみならず、内部からの不正な操作やオペレーションミスによる変更を検知し早期復旧をサポートする、情報資産保護ソリューションです。

- 比較対象となるベースラインデータの保持
- わずかな変更を見逃さない強力な検出機能
- システム構成に合わせたポリシー設定
- 卓越した復旧サポート機能
- 復旧コストの大幅削減

【統合認証ソリューション NET BUREAU（ネットビューロ）】

社内ネットワークへの接続場所、回線を問わず、セキュアなアクセス環境を短期間に構築するソリューションです。D@TA Centerで統合認証を行うことで、一つのID、パスワードで社内ネットワークへアクセスできるシングルサインオンを実現するサービスであり、アクセス回線の自動選択など複雑かつ高度なネットワークマネジメントをKCCS側ですべて引き受けることができます。

ITに求められているユビキタス社会を実践する統合認証ソリューションです。

- 専用のソフトが場所に応じて最適なアクセス回線を自動で選択するネットワークへのマルチアクセスを実現
- 認証は、KCCSのインターネットデータセンター「D@TA Center」の統合認証システムを活用
  一つのID・パスワードで複数のアクセス回線を利用可能
- 仮想的にLANを区切り、部門ごとに閉じたネットワークを構成する認証VLANに対応
- 無線LANの接続認証（IEEE802.1x対応）サービスを利用可能
- 独自開発のVPNインストーラにより、ワンクリックでクライアントPC側のVPN接続を設定することが可能

お問い合わせ先
京セラコミュニケーションシステム株式会社
〒108-8605 東京都港区高輪2-18-10
（日石高輪ビル）
広報宣伝部 児玉彩子・宮澤さおり
TEL（03）5792-0235
e-mail webmaster@kccs.co.jp

株式会社メトロ
(http://www.metro.co.jp)

株式会社メトロは、メーカーにとらわれず、マルチベンダとして、「ソフトウェア開発」「ネットワークセキュリティ」「マーケティングデータベース」をトータルソリューションとして、1971年に設立いたしました。
メトロは、社会に求められ、企業のニーズに沿った最適なソリューションを迅速かつ誠実に提案することを目指しております。

1991年からはネットワークセキュリティビジネスを新たに注力し、コンサルティング，セキュリティポリシー構築から運用支援まで、総合セキュリティサービスをご提供しております。セキュリティ事業に際しては、日本最初のワンタイムパスワード認証製品を展開し、Webシステムにおける認証セキュリティの先駆者として、多くの企業に導入していただきました。また、最近の個人情報保護や情報漏洩などについても、クライアントセキュリティの観点から、今までにない利便性と高いセキュリティ強度を兼ね備えた製品やハッキング対策に有効な次世代セキュリティＡＳＰサービスなど、常にセキュリティベンダーとして、様々な製品＆サービスをご提供しております。

＜代表的なセキュリティソリューション＞

◇クライアントセキュリティ

pointsec
ハードディスク丸ごと暗号化と強力な本人認証機能で、パソコン盗難／紛失によるデータ流出を防御します。会社・組織が決めたセキュリティポリシーを強制的に執行できる管理機能も特徴で、多くの政府機関や金融機関、大手企業に採用されています。

nProtect
クライアントパソコンに仕掛けられたハッキングツールやワームを検知して駆除する、新しい発想の「ハッキングツール防御」セキュリティサービス。検知／駆除は、センターと連携したWebサイトにアクセスするだけで実行されます。クライアントパソコンへのソフトウェアのインストールは一切不要。企業ポータルを利用したリモートアクセスやWebを利用したお客様サービス、住民サービスのセキュリティに最適です。

◇ネットワークセキュリティ

RSA SecurID®
ワンタイムパスワードの代表的な製品。毎回変化する使い捨てパスワードで、第三者の「なりすまし」不正アクセスを防御します。パスワードを用いるあらゆるネットワークと連携して、本人認証機能を実現します。

RSA ClearTrust®
Webアクセス管理／シングルサインオン製品。Webへアクセスする外部の人間や社員の資格や権限に応じて、閲覧できるサイトやページを制限できます。既存DBとの連携で、組織変更や人事異動、お客様のステータスの変化をアクセス権限に即反映させることも可能です。

secure soft
Firewall＋IDS＋VPN／IDPSアプライアンス製品。4種類のセキュリティシステムの組み合わせで、効率がいい管理と最適な運用管理を実現します。ハードウェアも一体化されているため、保守も一元的に行なえます。ネットワークへの不正侵入を検知して駆除するIDS／IDPS機能が特に評価されています。

お問い合わせ先
株式会社メトロ　情報通信営業部
〒141-0001 東京都品川区北品川5-9-15
TEL:03-5789-1022　FAX:03-5789-1014
E-Mail sales@tokyo.metro.co.jp

JNSA会員企業情報

JNSA会員企業の製品・サービス・イベント情報です。

■製品情報■

○SSL-VPNアプライアンス・サーバ「FirePass」とマトリクス認証ツール「SECUREMATRIX（セキュアマトリクス）」

モバイル端末から社内・社外を問わずどこからでも、セキュアに社内リソースへアクセスするニーズが増えています。
SSL-VPNである「FirePass」と、ハードやソフトを使わずに高セキュアなワンタイムパスワード認証を実現する「SECUREMATRIX」を組み合わせることで、このニーズに最適なソリューションを提供します。TCOの削減、IT部門の運用負荷軽減に加え、強固なユーザ認証ときめ細かいアクセスコントロールの集中管理が実現できます。
http://www.hucom.co.jp/

◆お問い合わせ先◆
株式会社ヒューコム　ITソリューション本部
〒166-8521 東京都杉並区梅里1-7-7 新高円寺ツインビル
Tel　：03-5306-7362
E-mail　：product@hucom.co.jp

○LivingPolicy：情報セキュリティポリシー運用管理ツール

ISMS適合評価制度の認証取得には情報セキュリティポリシーの「適切な」運用が不可欠です。
また、情報セキュリティポリシーを充分に機能させるためにも、適切なポリシー運用を行なうことは、企業にとっての重要な課題です。
LivingPolicyを利用して効率よくポリシーを運用することにより、効果的なセキュリティマネジメントを行なっていくことができます。
http://www.lac.co.jp/security/software/livingpolicy/lp.html

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

○GUARDIAN WALL

組織として取り組むべき機密情報・個人情報の漏えい対策は昨今、不可欠です。「GUARDIAN WALL」は、組織内のメール中継サーバに導入して、本文・添付ファイルを含めた電子メールの送受信記録の保存と、内容のフィルタリングを行う管理者向けのソフトウェアです。管理者はWEBブラウザからサーバにアクセスし、保存メールの検索・閲覧、各種フィルタリング条件の設定、統計情報の確認、システム管理等を行うことができます。
http://www.canon-sol.co.jp/guardian/product/gw/

◆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　：info-guardian@canon-sol.co.jp

○セキュリティ統合マネジメントシステム ArcSight

ArcSightはネットワークに存在する多くのセキュリティ製品から発生する膨大なログの中から、必要なセキュリティ対策を導き出す統合マネジメントシステムです。あらゆるデバイスのログを正規化して収集、データベース化し、膨大なログ、アラートをリアルタイムに相関分析。対策が必要な事象のみが抽出され、迅速かつ効率的なリアルタイム監視を可能にします。また、全てのログは保存され、事後調査、レポーティングが可能です。
http://sc-comtex.sse.co.jp/products/arcsight/

◆お問い合わせ先◆
住商エレクトロニクス株式会社
E-mail　：arcsight-info@scc.sse.co.jp
TEL　：03-5217-5851

■サービス情報■

○情報セキュリティ技術認定　応用コース開催

セキュリティ関連ベンダ8社による情報セキュリティ教育のアライランス、SEA/Jが提供する認定コースを開催します。
■応用コースマネジメント編
■日　時　3/31（水）、4/1（木）、5/13（木）、5/14（金）
■対象者　情報セキュリティ管理者、情報セキュリティ関連の内部監査担当者、システムエンジニア、セールスエンジニア、コンサルタント、情報セキュリティマネジメントに興味がある方
http://www.dit.co.jp/seminar/20040414.html

◆お問い合わせ先◆
株式会社ディアイティ　セキュリティビジネス推進室
Tel　：03-5634-7651

IW2003　JNSA+JPCERT/CC共催セミナー
『Security Day～技術だけでは守れない～』

「Internet Week 2003」が2003年12月2日(火)～5日(金)に社団法人日本ネットワークインフォメーションセンター(JPNIC)主催でパシフィコ横浜会議センターにおいて開催されました。ここで参加団体のイベントの1つとして、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)と有限責任中間法人JPCERTコーディネーションセンター(JPCERT/CC)が共催で、「Security Day～技術だけでは守れない～」を開催しました。JNSAとJPCERT/CCはこれまで、独立したプログラムでイベントを開催していましたが、Internet Weekで初めて共催しました。両団体にとっても今後更に協力関係を結ぶ上でのエポックメーキングとなる催しとなりました。

今回のプログラムは、2つの基調講演を柱に、JNSAとJPCERT/CCの活動紹介を絡め、最後にBoFで締め括るという構成でした。ここで主なプログラムについてご紹介します。

1. ふたつの基調講演

今回は基調講演として、奈良先端科学技術大学院大学教授・山口英先生とIT関係に詳しい牧野二郎弁護士からお話を頂きました。

まず山口英先生が「セキュリティ管理と高信頼性組織の構築」というテーマで大きな問題提起と考え方が提示されました。この基調講演では、組織のセキュリティ管理担当者が直面している典型的な悩みを考えてみようという切り口で、

1．セキュリティ管理強化の努力を継続的に行っているのに、なぜセキュリティトラブルは減らないのか
2．発生するトラブルはいつも思いもよらなかったことで発生し、その対応に右往左往してしまうのはなぜか

といった「悩み」や「疑問」に対する考え方を提示するとともに、その中に含まれる課題についての指摘がされました。特に2. に対する対策として「レスポンス力を高めるモデル」を分析してみると、それがかつての日本オリジナルの方法である「力ある技術者から生み出される知見」「経験則」「現場主義」などが重要であり、過去の知恵を現代に生かすことが重要であると言う提言がされました。

午後は、牧野二郎弁護士による基調講演「法的立場から見たITセキュリティ」というテーマで、法律の専門家からみたITセキュリティの問題について解説されました。「セキュリティ」の考え方や解釈について、ネットワーク管理者向けのポイントが整理して提示され、専門外だが重要な点について具体的な事例を交えてわかり易く説明されました。また、今ネットワーク管理者に求められているのは、技術的セキュリティ対策だけではなく、情報セキュリティ全般へ拡大しているという現状を把握できる有用なポイントを掴むことができました。まさに「技術だけでは守れない」ネットワークセキュリティを具体的にわかり易く解き明かしてくれましたが、今後ともこのようなお互いの専門性をクロスオーバーさせる場が必要であることも痛感したひと時でした。

各々の基調講演に続いて、JNSAのWGと、JPCERT/CCの活動報告が行われました。JPCERT/CCが11月から運用を開始した定点観測システムの紹介、JNSAのWGの中から、ハニーポットWGとセキュリティ被害調査WGなどが紹介され、正規のプログラムは終了しましたが、このあとBoFが開催されました。

2. BoF「眠れない夏、オペレータの戦い」

夜の部は誰でも参加できるBoFとして「眠れない夏、オペレータの戦い」が開催されました。昨夏のCisco IOSの脆弱性やBlaster/Nachiワームの蔓延などを踏まえ、「オペレータにとっての脆弱性情報の流通」をテーマにパネルディスカッション形式で会場の参加者も交えて活発な議論が行なわれました。

モデレータ　水越一郎氏（JPCERT/CC）
パネラー　（発表順）
寺田真敏氏（日立/慶應）
三ツ木絹子氏（MEX）
白橋明弘氏（ネットワンシステムズ）
佐藤慶浩氏（日本HP）

モデレータとして水越氏が口火を切り、まずパネラーから問題提起と現状が説明されました。最初は寺田氏が、セキュリティ関連の公開情報を時系列にまとめてWebで公開されている中から、Cisco IOSの脆弱性情報、Blaster/Nachiワームについてまとめた情報を紹介されました。2番目に、三ツ木氏がISPを取り巻く状況の変化と悩みについて率直に語られ、3番目に白橋氏がSIベンダの立場からの思いと現状を話された。脆弱性情報をCERT/CCからのアドバイザリで初めて知るのは不安があるので、あらかじめ人員などの体制を準備しておくことができように公開時期だけでもあらかじめわかっていると対応がしやすい、という提案がされました。最後に、佐藤氏が、脆弱性情報の流通に関して、国際標準などの策定に関わった立場から、公的な届出機関やISPやSIベンダといった特定の相手に、情報開示を事前にすることが難しい理由について説明がありました。

会場からは、「事前の情報開示は難しいということだが、実現できる可能性はないのか？」といった質問がでました。これに対し、万が一情報が漏れたためにインシデントが発生した場合、「一般ユーザ」の被害に対して損害賠償が請求されると、事前に情報を得て漏らしてしまった「特定ユーザ」が「被害に見合った莫大な金額」を支払わなければならない可能性があること、また情報を出す側も、いわば顧客でもある「特定ユーザ」に対して莫大な損害賠償を請求することは難しいということ、などが障害になっているとの説明がありました。この点については、他の場で行政府も含めて、JNSA、JPCERT/CCなどでの議論が行われており、更に意見交換をし議論を深める必要があると思われます。

朝10時から夜8時までという大変長い「セキュリティ・デイ」でしたが、ほとんどの参加者が最初から最後のBoFまで参加してくださいました。また、会場からの質問も積極的であり、大変有意義な一日であったと思います。参加者からいただいたアンケートの集計結果を見ても大変好評であり、次回Internet Week 2004では、より内容の充実したプログラムを用意したいと考えております。

事務局お知らせ
JNSA ANNOUNCE

1. 主催セミナーのお知らせ

●「JNSAワーキンググループ成果報告会」

■日　　時：2004年5月18日（火）

■会　　場：大手町サンケイプラザ

■入場料：無料

JNSAでは、ワーキンググループの成果発表会を開催します。
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ください。
http://www.jnsa.org/

2. 後援イベントの知らせ

1.「コンピュータ犯罪に関する白浜シンポジウム」

会　期：2004年5月20日（木）～22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
会　場：コガノイベイホテル（和歌山県）
http://www.sccs-jp.org

2.「第3回eビジネス2004」

会　期：2004年6月22日（火）～24日（木）
主　催：日刊工業新聞社
会　場：マリンメッセ福岡（福岡県）
http://www.nikkanseibu-eve.com/e-biz/

3.「AVAR2004 in Tokyo」

会　期：2004年11月4日（木）～5日（金）
主　催：AVAR
（Association of anti Virus Asia Researchers）
会　場：シェラトングランデ東京ベイ（千葉県）
http://www.aavar.org

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。

継続WG

【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：山本匡氏/損保ジャパン・リスクマネジメント）

2001年、2002年と継続して、被害調査を行い、被害額算定モデルを提案してきた。

今年の活動においても、前年同様なアンケートやヒヤリングによる被害調査を行い、算出モデルの精緻化を行うと共に、これらの被害の定量化について手がかりを掴みたい。

主な活動内容としては、下記の通り。

- 2002年度調査の課題への対応と再調査実施。
- 簡易算出方法、各種指標のさらなる拡大および整理・精緻化
- 被害発生時の緊急ヒヤリング体制整備、事故情報の収集

【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でメンバーによるコラムを執筆中である。
http://premium.nikkeibp.co.jp/e-gov/column/2003/column9_3a.shtml

新規WG

【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同行を把握し、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。

【プライバシー保護実装研究WG（仮称）】

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、Windows RMS等、各社製品技術でどこまで対応可能かの調査、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予定。

成果物としては、プライバシー保護IT要件の定義サンプル、定義に対する技術マッピング表サンプル、個人情報保護法の条文に対する技術マッピング表サンプルなどを予定。

---

2. 技術部会

（部会長：佐藤友治氏/インターネット総合研究所）

技術部会では、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：未定）

セキュリティポリシーの必要性は徐々に浸透しつつあるが、具体的に策定する場合、何を決めればよいのか、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議論しながら成果を公開していきたい。

【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。主な活動予定は、上記をふまえた勉強会およびドキュメント作成など。

【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。

【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。

【ハニーポットWG】

（リーダー：園田道夫氏）

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：内田昌宏氏/ネットマークス）

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。

【電子署名検討WG】
（リーダー：磐城洋介氏/NTTコムウェア）
電子署名法の施行以来、様々な電子署名システムが検討／構築されているが、現状では様々な問題／課題に直面しており方式やビジネスモデルの見直しなど利便性やコスト面におけるマイナスイメージが指摘される。これらの問題をもたらした原因を洗いだし、電子署名に関する世間の認知や正しい理解を促すと共に、社会的に必要とされている情報をレポート・ガイドラインとして公開することで、健全な電子社会の発展に貢献することを目的とする。予定成果物は、「公的個人認証基盤」の活用ガイドライン。

---

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」を拡張して今年度も行なう予定である。その企画・運営協力を行なう。

【セキュリティスタジアムWG】
（リーダー：園田道夫氏）
2003年度はセミナー1回とスタジアム本大会の開催準備で終わってしまったが、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。

---

4. 教育部会
（部会長：佐々木良一氏）
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/富士総合研究所）
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を育成に向けた各種施策の検討を行うことを目的とする。

---

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、日々高まる情報情報セキュリティへのニーズに応えるべく、先進性を追求すると共に、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。

【セミナー運営委員会】
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。

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　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 取締役
経営戦略担当

副会長　大和　敏彦
シスコシステムズ株式会社
CTOアライアンス＆テクノロジー本部長

理　事(50音順)

TIS株式会社
在賀　良助

株式会社ヒューコム
井上　陽一

株式会社大塚商会
宇佐美　慎治

三菱電機株式会社　情報技術総合研究所
後沢　忍

テクマトリックス株式会社
浦山　清治

岡村　靖

株式会社シマンテック
勝見　勉

セコムトラストネット株式会社
川上　博康

株式会社ネットマークス
亀井　陽一

トレンドマイクロ株式会社
小屋　晋吾

日本ヒューレット･パッカード株式会社
佐藤　慶浩

株式会社ディアイティ
下村　正洋

新日鉄ソリューションズ株式会社
杉田　寛治

ELNISテクノロジーズ株式会社
鈴木　伸秀

エントラストジャパン株式会社
鈴木　優一

横河電機株式会社
武智　洋

日本ネットワークアソシエイツ株式会社
田中　辰夫

株式会社IDGジャパン
玉井　節朗

NTTアドバンステクノロジ株式会社
辻　久雄

株式会社NTTデータ
中村　逸一

システムニーズ株式会社
中山　恵介

株式会社ラック
西本　逸郎

大日本印刷株式会社
野久保　秀紀

東芝ソリューション株式会社
坂内　明

株式会社フォーバル クリエーティブ
早水　潔

マイクロソフト株式会社
古川　勝也

ＮＴＴコミュニケーションズ株式会社
松尾　直樹

RSAセキュリティ株式会社
山野　修

古河電気工業株式会社
吉澤　昭男

グローバルセキュリティエキスパート株式会社
若井　順一

東京海上火災保険株式会社
綿引　宏行

監　事

清友監査法人　公認会計士
土井　充

顧　問

東京大学　教授
今井　秀樹

新東京法律事務所　弁護士
北沢　義博

東京電機大学　教授
佐々木　良一

慶応義塾大学　教授
武藤　佳恭

早稲田大学　客員教授
前川　徹

早稲田大学　教授
村岡　洋一

奈良先端科学技術大学院大学　教授
山口　英

東京大学　教授
吉田　眞

事務局長

株式会社ディアイティ
下村　正洋

5. 会員企業一覧

2004年2月25日現在　181社　50音順

【あ】
（株）アークン
RSAセキュリティ（株）
（株）アイセス
（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）アクセンス・テクノロジー
朝日監査法人
アマノ（株）
（株）網屋
アライドテレシス（株）
（株）アルゴ21
（株）アルテミス
（株）アンラボ
（株）イーツ
イーディーコントライブ（株）
伊藤忠テクノサイエンス（株）
学校法人 岩崎学園
（有）インターネット応用技術研究所
インターネット セキュリティ システムズ（株）
（株）インターネット総合研究所
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）栄光
（株）エス・アイ・ディ・シー
（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） *New*
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）
（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）
エリアビイジャパン（株）
ELNISテクノロジーズ（株）
エントラストジャパン（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】
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）
（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
コベルコシステム（株）
コンピュータ・アソシエイツ（株）

【さ】
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
シーティーシーエスピー（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）
（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
シャープシステムプロダクト（株）
Japan Cyber Security Institute
（株）翔泳社
（株）情報数理研究所
寿限無（株） *New*
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
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）セラク
セントラル・コンピュータ・サービス（株）
ソニー（株）
ソフトバンクBB（株）

ソラン（株）
（株）ソリトンシステムズ
（株）損保ジャパン・リスクマネジメント

【た】
大興電子通信（株）
大日本印刷（株）
ダイヤモンドコンピューターサービス（株）
中央青山監査法人
（株）ディアイティ
TIS（株）
（株）TBCソリューションズ
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
東京海上火災保険（株）
東芝ソリューション（株）
東芝情報システム（株）
東洋通信機（株）　トヨコムネットワークシステムズ New
（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）
日本エフ・セキュア（株）
日本オラクル（株）
（株）日本高信頼システム研究所
日本コムシス（株）
（株）日本システムディベロップメント
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
日本ネットワークアソシエイツ（株）
日本ビジネスコンピューター（株）
日本ヒューレット・パッカード（株）
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
（株）日立システムアンドサービス
（株）日立製作所
（株）ヒューコム
（株）ビー・エス・ピー
（株）PFU
日立ソフトウェアエンジニアリング（株）
東日本電信電話（株）
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）
（株）富士総合研究所
富士通（株）
（株）富士通ソーシアルサイエンスラボラトリ
富士通エフ・アイ・ピー（株）
（株）富士通ビジネスシステム
（株）フューチャーイン
（株）プラーナ
（株）ブライセン
古河電気工業（株）
（株）プロティビティ
ボーダフォン（株）

【ま】
マイクロソフト（株）
松下電工（株）
丸文（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）
三菱電線工業（株）
（株）メトロ

【や】
ユーディテック・ジャパン（株）
横河電機（株）

【ら】
（株）ラック
レインボー・テクノロジーズ（株）

【わ】
ワイ・エー・ピー・ホールディングス（株）

【特別会員】
社団法人日本インターネットプロバイダー協会
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

6. JNSA年間活動（2003年度）

4月	4月3日	第1回政策部会
	4月18日	第1回幹事会
	4月23日	理事会（九段会館）
	4月24日	第1回西日本支部主催セキュリティセミナー
5月	5月8日	技術部会
	5月21日	定期総会（スクワール麹町）
	5月21日	臨時理事会（スクワール麹町）
	5月22-24日	白浜シンポジウム後援
	5月17日	第2回政策部会
	5月28日	第2回幹事会
6月	6月2-3日	RSA Conference 2003後援
	6月2-3日	NSF2003 spring開催(東京国際フォーラム)
	6月9日	第1回西日本支部会合
	6月13日	セキュリティ監査サブ合宿（晴海グランドホテル）
	6月25日	第1回教育部会
7月	7月2-4日	NetWorld+Interop 2003 Tokyo後援
	7月9日	第3回幹事会
	7月16日	3回政策部会
	7月16-18日	Wireless Japan 2003 後援
8月	8月20日	第2回西日本支部主催セキュリティセミナー
	8月26-27日	情報セキュリティシンポジュウム
	8月28日	技術部会リーダー会
	8月28日	第4回政策部会
	8月28日	第4回幹事会
9月	9月4日	第2回西日本支部会合
	9月17-20日	WPC EXPO 2003　主催者企画「何でも相談コーナー」後援
	9月10日	セキュリティスタジアムセミナー（工学院）
	9月24-25日	電子署名・認証フォーラム後援
10月	10月2-4日	ネットワーク・セキュリティワークショップ ｉｎ越後湯沢協力
	10月8日	第3回西日本支部会合
	10月9日	第5回幹事会
	10月16日	技術部会リーダー会
	10月17-18日	スキルマップ作成WG合宿（マホロバマインズ三浦）
	10月22-24日	NSF2003開催（東京ビッグサイト）
	10月29日	第5回政策部会／全国情報セキュリティキャラバン実施
11月	11月6-7日	Pacsec.jp後援
	11月12-14日	まちと人のセキュリティシンポジウム協賛
	11月19日	技術部会リーダー会
	11月26日	第6回幹事会
	11月26日	日・韓セキュリティForum、商談会／全国情報セキュリティキャラバン実施
12月	12月3日	Internet Week 2003参加
	12月5日	第3回西日本支部主催セキュリティセミナー
	12月9日	第6回政策部会
	12月12-13日	セキュリティ標準調査WG合宿（初島）
1月	1月15日	第7回幹事会
	1月16-17日	不正プログラム調査WG合宿（マホロバマインズ三浦）
	1月21日	IPAX Winter 2004出展（東京国際フォーラム）
	1月27日	新年賀詞交歓会（東京グランドホテル）
	1月29-30日	Developers Summit 2004後援
	1月29-30日	ジェトロ国際テクノビジネスフォーラム2004後援
2月	2月4-6日	NET&COM 2004　後援
	2月10日	第4回西日本支部会
	2月13-14日	セキュリティポリシーWG合宿（箱根）
	2月17日	第7回政策部会
	2月25日	第8回幹事会
	2月25-27日	活力自治体フェア04　後援
3月	3月12日	第4回西日本支部主催セキュリティセミナー
	3月24日	教育部会勉強会

★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.10

2004年4月1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。

THE NEW VALUE FRONTIER

KYOCERA

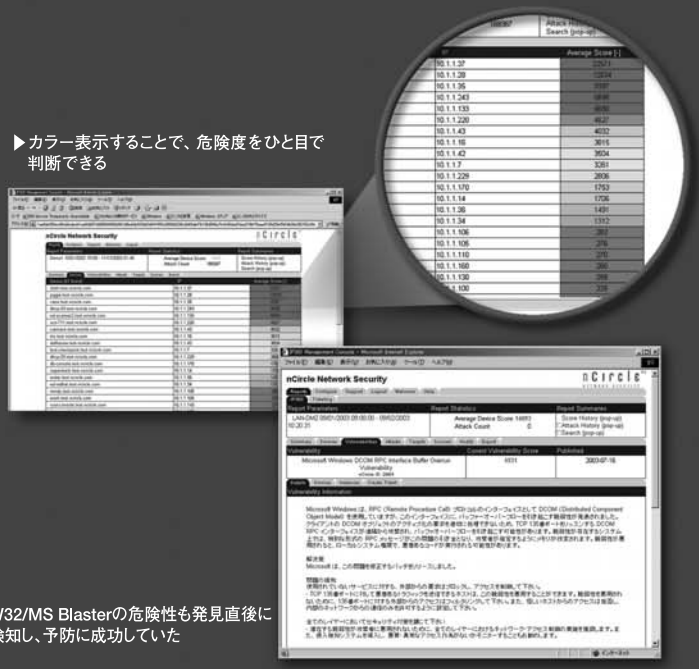
対処よりも予防。

nCircle
NETWORK SECURITY

セキュリティリスク管理支援システム

リアルタイムVA機能がネットワークの脆弱性を検知

企業セキュリティレベルを格付けしようという動きが出ています。ネットワーク社会では一度でも被害を受け、風評が広がると、企業活動そのものに影響が生じかねません。侵入検知で事後に対処するよりも、侵入を許さぬ事前対策を講じる。VA+IDS機能搭載の「nCircle IP360」が、一歩先行くプロアクティブなセキュリティソリューションを提供します。



▶カラー表示することで、危険度をひと目で判断できる

▶W32/MS Blasterの危険性も発見直後に検知し、予防に成功していた

京セラコミュニケーションシステム株式会社
専務取締役
北村 寛

▶電子行政に不可欠のセキュリティ対策

e-Japan戦略を背景に今、電子政府や電子自治体への取り組みが盛んです。ここで不可欠なのがセキュリティ対策。何故ならサイバーアタック（*1）が急増しているからです。例えば2003年8月12日に発見されたW32/MS Blasterというワームは、その後の10日間に情報処理振興事業協会セキュリティセンターに寄せられた感染被害等の届出だけでも2,400件以上に達しています。

これは氷山の一角で、水面下ではその10倍以上の被害があると見られます。事実、官公庁や自治体でも驚くべき台数の被害が出ており、VoIPの停止やオンライン業務の停止を余儀なくされたといった被害が頻発しています。こうしたサイバーアタックは、処置を怠ると被害者自らが加害者になる危険性もまた大きいのです。

セキュリティ対策はこれまで、IDS（侵入検知システム）が採用されてきました。しかしIDSは導入や運用に高い負荷とスキルを要求されます。また、大量のセキュリティホール情報や危険因子情報を提供しますが、ユーザにとって早急に必要な情報が得られてないのが実態です。そこで米国では、IDSからVA（脆弱性診断）への強化が始まっています。とくに政府や軍関係などでは先行しており、セキュリティレベルの統一、管理レベルの底上げ、そのための評価基準の策定に取り組んでいます。翻って日本ではどうかというと、大きく後れているのが実状です。

▶不正侵入を許さない「nCircle IP360」

サイバーアタックは、より強くより短期間になっています。例えば2003年1月に発生したSQL Slammerは、セキュリティホールの発表から発生までに5ヵ月を要していますが、W32/MS Blasterの場合は7月16日の警告発表から8月12日の最初の発生まで1ヵ月と経っていない。従来のIDSを使った手作業による監査や対応ではとても間に合わないのが現実なのです。

そこでIDS機能に新たにVA機能を連携させた強固なセキュリティリスク管理支援システムが「nCircle IP360」。アタックを検知してから対処する事後対策型のセキュリティツールが多いなかで、「nCircle IP360」は事前予防を可能にします。「nCircle IP360」が米国政府や金融機関をはじめ大手企業で導入が進んでいるのも、こうした事前対策が可能で、運用負荷も軽いからです。

「nCircle IP360」は24時間365日、セキュリティホールを常に自動的に監査して危険度を点数とカラー表示で一目瞭然にし、大事なサーバから順に手当が可能です。また自治体のようにさまざまなシステム運用形態を持つ場合でも柔軟に適用でき、組織内部での発生が多いと言われるセキュリティ被害にも有効な内部管理を可能にします。

こうした「nCircle IP360」の有効性を高く評価し、日本でも先進的な自治体では導入が始まりました。より安全性の高い電子行政システムのために、「nCircle IP360」をご活用戴きたいと思います。

*1：ネットワーク上のウイルス感染や不正侵入、データ改ざんや盗聴などの不正行為

京セラ コミュニケーションシステム株式会社
セキュリティシステム営業部 〒108-8605東京都港区高輪2-18-10（日石高輪ビル）
TEL: 03-5792-0270　FAX: 03-5792-0271
E-mail: webmaster@kccs.co.jp
http://www.kccs.co.jp/security/ncircle/

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