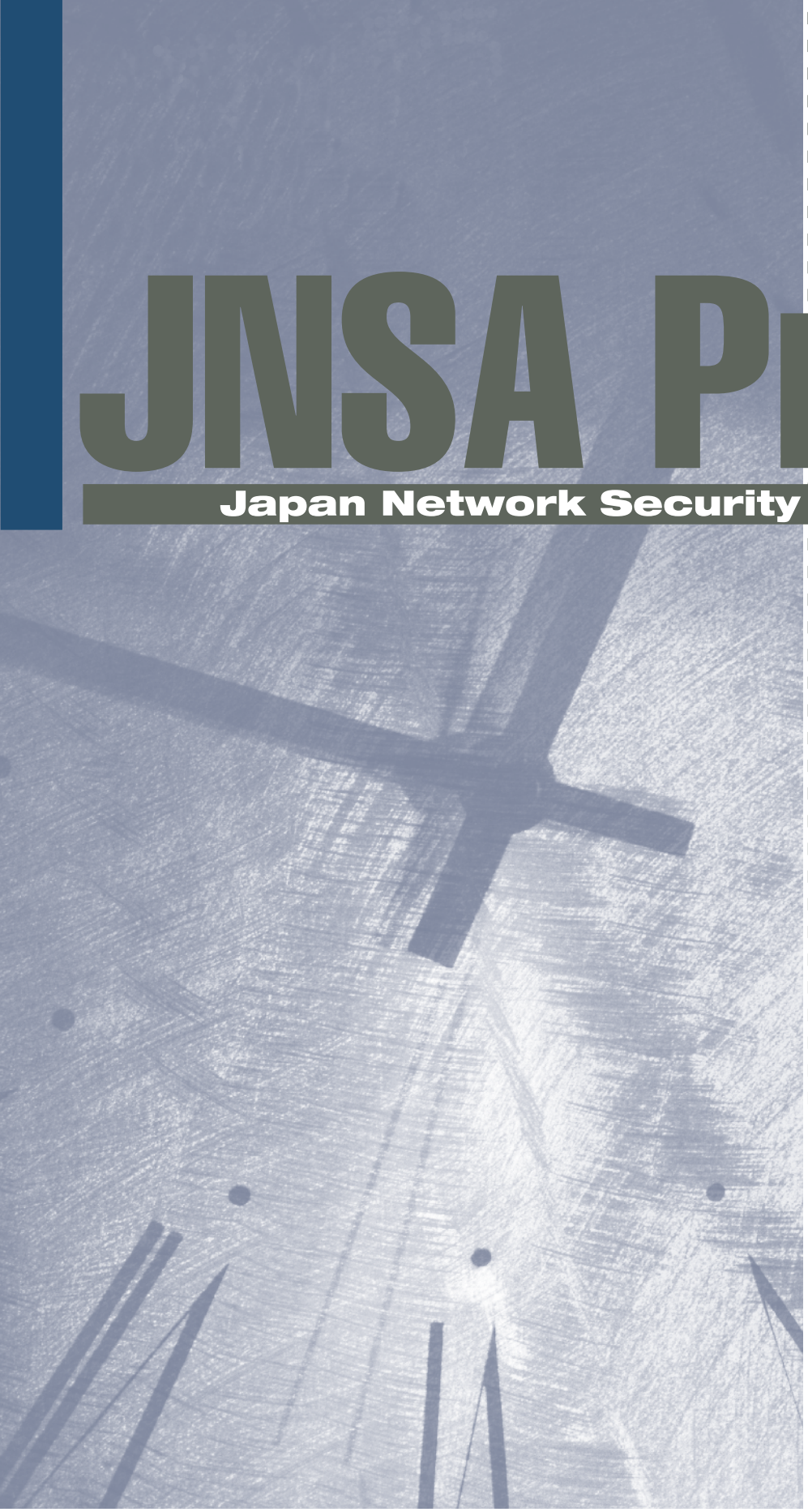


JNSA Press

Japan Network Security Association

Vol.14
August 2005

CONTENTS

特定非営利活動法人 日本ネットワークセキュリティ協会
NPO Japan Network Security Association

セキュリティの原点：日本の心

JNSA 顧問 東京大学教授 CISSP
安田　浩

個人情報保護法が 2005 年 4 月より完全施行され、個人情報保護に関する関心が日本社会でも急速に高まっています。水と空気と安全は「ただ：無料」と考えていた日本でも、安心・安全にはかなりコストがかかることを自覚するようになる、良い機会と思います。しかしながら、いたずらに危機感を煽るばかりで、情報の守秘感度に関する考察がおざなりにされているのではないかと心配です。

個人情報には 2 種類有り、変更が可能なので守秘感度が低い個人情報と、変更が不可能なため守秘感度が高い個人情報とがあります。前者の代表はクレジットカード番号などで、後者の代表は DNA 情報などです。前者は盗まれたことに気が付いたときに解約･変更すれば良く､盗まれてから解約･変更するまでの期間にしか被害は発生しません。したがって盗まれたかどうかをいかに迅速に知り、解約・変更手続きに入れるかがセキュリティの基本になります。

一方 DNA 情報などは、悪人に盗まれると変更がきかないために、一生苦しむことになります。たとえうっかりミスでも外に漏れては困る訳です。絶対に盗まれてはならない、これが後者の個人情報に関するセキュリティの基本方針です。盗まれたことを迅速に発見する技術は色々考案されていますので、この面のセキュリティはかなり高いレベルになってきたと思っています。しかしながら、ミスも許さない絶対に盗まれてはならない方策など存在するのでしょうか。

日本人は安全を｢ただ｣と思ってきました。その前提は､すべての人が｢一見さんお断り｣と「見ざる聴かざる言わざる」を理解し、実行しているということにあるのだと思っています。個人認証と漏洩後対策の原点をここに見ることができると思います。

この前提は、ネットワークで国外とつながれることによって崩れつつあります。契約万能の米国社会では､「一見さんお断り」と「見ざる聴かざる言わざる」とは全く理解出来ない世界だからです。一人でもこれらの原則を理解せずその逆手をとる人が出てくれば安全は脅かされ､次々に逆手を取る人が増える負の連鎖が始まります。そうなれば､ネットワークを切り離すか、新しいセキュリティ技術を導入するかの選択を迫られることになります。日本社会は今、後者の選択を否応なく迫られている事態といえましょう。

ポイントは、セキュリティ技術設計の基本方針にあります。米国流の基本精神では守ることと破ることがいたちごっこで、どこまでいっても安心・安全にはなれないようです。日本古来の「一見さんお断り」と「見ざる聴かざる言わざる」という基本精神を具現化するセキュリティ技術を地球上すべてに植え付けることができれば、安全は皆のものになると信じています。地球が宇宙に広がっても基本は同じです。

この日本的精神を具現化するセキュリティ技術を研究開発し、世界に普及することが日本セキュリティ技術陣に課せられた第一の使命と思います。JNSA が研究開発の先頭にたつことを心から祈念いたします。

セキュアOSを導入せよ～セキュリティ対策の限界を越える

日本高信頼システム研究所
主任研究員　田口　裕也

『セキュアOSの必要性』

「セキュアOSの導入を。」このような言葉が内閣官房情報セキュリティセンターの報告書「電子政府におけるセキュリティに配慮したOSを活用した情報システム等に関する調査研究」に提示され、「セキュアOS」を使用するべきと明示されました。この発表の背景には、数々の著名な企業のWebサイトが不正アクセス、不正侵入を受け、多くの情報が漏洩したり改ざんされる被害報告を多く聞く深刻な事態があったからです。これらの被害を受けたシステムの状況を調べてみると、必ずしもセキュリティ対策を怠っていたというわけではありません。通常は、構築するシステムにセキュリティ対策を施すことは「当然のこと」として認識されています。アンチウィルスやファイヤーウォール、IDSなど、いろいろな製品を組み合わせて、考えられる脅威からシステムを保護することはあたりまえの時代です。しかし、攻撃を受けてしまうといとも簡単にシステムが侵略され、企業にとってとても大切なお客様の個人情報や、経営にかかわる機密情報などがあっさりと外部に漏れてしまうのが現状です。このように、最近の著しいインターネットの普及に伴い、多くの事故やさまざまな脅威からシステムを保護するためのセキュリティ対策に注目が集まっています。その中でも、OSのセキュリティについては、より信頼性のあるシステムを構築するために特に注力しなければならない項目として政府から取り上げられているのです。今回は現在のセキュリティ対策になぜOSセキュリティが追加で必要なのか、また、政府が導入を促進しているセキュアOSとはどのようなものなのかを開発された歴史をたどり、OSそのものを強靭にする必要性を解説します。

1. 現在のセキュリティ対策の抜け道

近年のセキュリティ対策では、たくさんの導入費用と時間を使い、アンチウィルスやファイヤーウォール、IDSなどで、何重ものセキュリティ対策をすることは当然であると思います。これらの対策方法で大切な情報を格納しているシステムを間接的に守ろうとしていました。ネットワーク周辺からシステムを保護することによって、不正なアクセスを防止するアプローチです。しかし、これらのセキュリティ製品のほとんどが一般に公開されていない未発見のウィルスや、脆弱性への攻撃、また、脆弱性を直すパッチがリリースされるまでの対策ができない期間に対しては無意味に近いのではないかと言われています。なぜなら、ウィルスや不正な攻撃を事前に防ぐためには、世界中で発見されたたくさんの攻撃手法をパターンとして登録しているパターンマッチングという方式で動作している製品がほとんどだからです。もし、あらかじめ定義された攻撃手法のパターンと同じ攻撃が発生すれば、もちろんシステムを守ってくれますが、これらの防御機能を常に維持するためには、パターンを登録しているパターンファイルを最新の状態に更新しつづけなければならないのです。つまり、使用しているパターンファイルに定義されていない攻撃をシステムが受けた場合、当然ながら防ぐことができません。パターンに登録されていないので認識することができないため、問題なく通過してしまうのです。

そのため、現在のセキュリティ対策では抜け道が存在し、せっかく導入したセキュリティ対策も一瞬のうちにして無意味になってしまう可能性があるのです。多額の費用と時間をかけても思うように効果が現れないのはこの仕組みのためです。

また、実装しているたいていのアプリケーションには脆弱性（バグ）が発見され、修正パッチが多く提供されています。パッチを適用すれば不具合が修正されるのですが、そのためには稼働マシンへ適用す

る前にテスト機でパッチを適用し、システムに問題がないかを検証する段階を経ます。では、脆弱性が発見されてからパッチが提供されるまでの期間はどのようにしてシステムを保護すれば良いのでしょうか。現状ではパッチが提供されていない期間はシステムを保護する手立てはほぼ皆無に近いのです。つまり、パッチの提供を待っている間は不正なアクセスや攻撃を受ける危険性が高まり、とても不安定な状態で運用しなければなりません。さらに、世間一般には公開されていない脆弱性を発見されて、攻撃を受けたとします。これは、パッチそのものが最初から存在しないため防ぎようがありません。パッチマネージメントにおける未提供期間の問題は、現状の方式では対策が不可能であるため攻撃からシステムを守ることはできないのです。

2. OS の構造上の抜け道

現状の対策では、システムの内部に不正なアクセスを許してしまうと、保存されている大切な情報は全て漏洩する可能性がとても高いことがあります。これは OS の仕組みが根本的に全ての情報へアクセスできてしまう構造で作られている現実があるためで、機密度がとても高い情報を守るためには適切なアクセス制御の設定ができません。つまり、システム全体へのアクセス権を許可されている root ユーザや Administrator（システム管理者）の存在があるからです。もし攻撃を受けた場合、必ず犯人はシステムの管理者権限を奪取しようと試みます。奪取されてしまうと、保存している全ての情報にアクセスされてしまうため、システム全体に被害が発生します。つまり、これまでの OS を使用していたのでは、まったく無防備な状態で情報は保存されている状態に近いのです。この仕組みは全ての OS にあてはまります。OS そのものが貧弱すぎると、いくらネットワーク周りでセキュリティ対策をしても無意味なのです。例えば、家を建築するときにはコンクリートで基礎をしっかり作ります。基礎を作らず砂漠の砂の上にいくら立派な家を建ててもすぐに傾いて倒壊してしまいます。同じようにシステムを構築するためにも OS（システムの土台）が頑丈でなければ信頼性の高いシステムは構築できません。OS の問題を解決するためには、普通の OS を使用していたのでは構造上の問題からすでに限界であり、解決することができません。そのため、これまでにはまったくない概念を取り入れて対策をする必要があります。

3. 注目されるセキュア OS

民間企業にも情報保護のためにいままで以上に高度なセキュリティ対策が求められています。お客様の情報を漏洩した場合の社会に与える影響や、悪用され被害が発生した場合の賠償など、「システムを守る」ことは、企業経営に関わる影響がとても大きいのです。このことから「システムを守れない」ことは一定期間の業務停止など、経営の危機に発展することもありえるのです。

そこで、現状の対策ではすでにいくつもの限界が見えてきたことから、OS そのものを強靭にして、システムを保護する「セキュア OS」が話題になり始めています。

4. セキュア OS とトラステッド OS

日本では最近セキュア OS が注目を集めるようになりましたが、実は米国では 20 年以上前からすでに製品化され、政府機関や民間企業に提供されていました。1985 年に米国防総省指令として発令された TCSEC（Trusted Computer System Evaluation Criteria：セキュリティ機能評価基準書）というセキュリティ製品の機能を評価する規格が策定されているのです。

これは、米国の国防に関わる機関へシステムを導入するためには、TCSEC に規格されているセキュリ

ティ強度を満たしていなければならないという機能を評価する規格です。

この規格は A を最上位とした Division と呼ばれる４つの階層（A、B、C、D）に分かれており、さらに各 Division ごとに class と呼ばれる７つの階層（B1、B2、B3 数値が高いほうが上位）で分類されています。（図１）

Division	Class	代表的な評価基準
D	なし	TCSEC の評価に値しない製品
C	C1	任意アクセス制御を実装
	C2	C1 に監査機能等の実装を追加
B	B1	C2 に強制アクセス制御の実装
	B2	B1 に構成管理機能の実装を追加
	B3	B2 にリカバリー機能の実装を追加
A	A1	B3 に配布時の保証機能の実装を追加

図1 TCSEC におけるセキュリティ機能の評価分類

この TCSEC で B Division で定義されている規格をクリアした OS のことをトラステッド OS（Trusted OS）と呼んでいます。

今日のセキュリティ評価基準は「ISO/IEC15408」が国際的な規格の基準となっていますが、TCSEC で定義されている多くの規格をベースとし、プロテクションプロファイルとして継承されてます。日本でもトラステッド OS を入手することはもちろん可能でした。しかし、もともと国防 (軍用システム) 向けに開発された経緯もあって、あまりにも高すぎるセキュリティ機能は、当時の民間企業へはあまり普及しなかった現実もあります。しかし、最近の情報保護を民間企業に求める動きから高度なセキュリティ対策が必須となってきました。そのため、トラステッド OS は再び注目を集めています。さらに時代の流れに合わせて登場したのがセキュア OS です。セキュア OS はトラステッド OS の高いセキュリティ機能を保ちつつ、民間企業が要求する便利な機能を次々と実装し、導入、運用しやすいようにたくさんアレンジされています。そのため、セキュア OS は厳密に TCSEC の規格を満たしているとはいえませんが、普通の OS では解決できなかったセキュリティの問題点を解決する手段として、その必要性が認知されてきています。

5. 強制アクセス制御と任意アクセス制御

実際にセキュア OS やトラステッド OS を、普通の OS と比較したとき、どの機能が大きく異なるのかと言うと、システム管理者であっても回避することのできないアクセス制御機能を実装している点です。これを、強制アクセス制御（MAC : Mandatory Access Control）と呼びます。B Division では、強制アクセス制御機能を実装することを必要な条件として定義していますが、どのような機能なのでしょうか。

これには、現在の OS が実装しているアクセス制御の仕組みを理解するととても分かりやすくなります。普通の OS ではファイルの所有者がどのユーザクラスに対して必要なアクセス権を許可するのかという設定をしてアクセス制御を行います。これを任意アクセス制御（DAC : Discretionary Access Control）と呼びます。

しかし、任意アクセス制御の大きな欠点は、一般ユーザにのみ有効なアクセス制御機能であり、システム管理者にはまったく無効であることです。つまり、設定されているアクセス権を無条件に回避することができます。これは、システム全体へのアクセス権をシステム管理者は保持している意味を表します。例を上げると、もしファイルの所有者が読み取り専用のファイルと設定しても、システム管理者はファイルの所有者の許可なく無断で書き込むことができてしまうのです（図 2)。

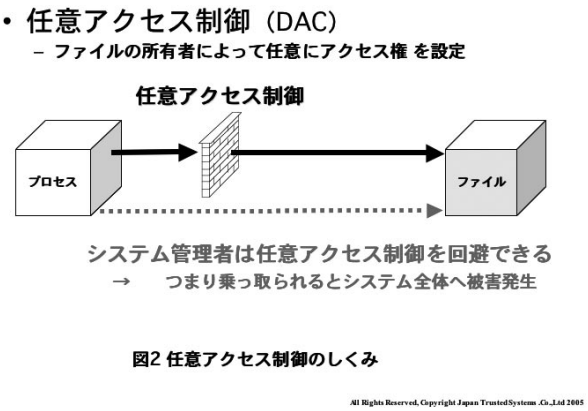


図2 任意アクセス制御のしくみ

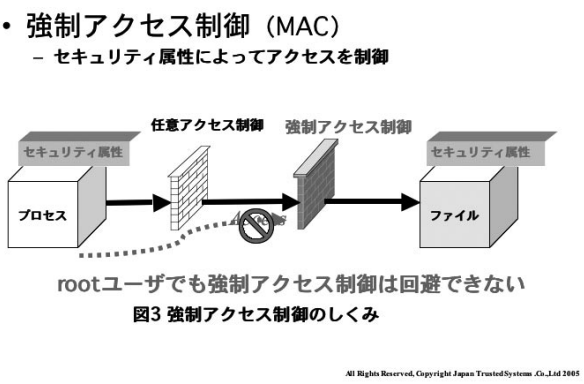


図3 強制アクセス制御のしくみ

この構造の仕組みでは、もしシステム管理者権限を保持したプロセスが悪意を持ったユーザに奪取されたり、システム管理者のパスワードが漏れてなりすまされてログインされたり、あるいはシステム管理者自身が情報を盗み見るために悪意を持ってアクセスした場合など、システムに存在する全ての情報へのアクセス許可を悪意あるユーザに与えたことと同じ状態になります。これではたくさんの時間をかけてセキュリティ設定を正しく行っていたとしても、セキュリティ機能を無効にされたり、ログを削除されるなどして痕跡を消すことができるため、いくら適切にアクセス権を設定してもまったく意味がないのです。一方、TCSEC で定義されている強制アクセス制御は、システム管理者であってもあらかじめ決められた動作以外は行えないようにする機能です。これは、システムに存在するすべてのプロセスやファイルにセキュリティ属性を付与します。この属性はセキュア OS や、トラステッド OS で追加された、これまでの OS にはない属性です。この属性をプロセスがファイルにアクセスするときは必ずセキュリティ属性のチェック機構（リファレンスモニタと呼ぶ）を通過しなければなりません。付与されたセキュリティ属性を識別して、プロセスからファイルへのアクセス可否を判断しています。つまり、強制アクセス制御はシステム管理者であっても決して回避することはできないのです。（図 3）

この仕組みを導入することによって OS そのものがとても強靭になるため、あらゆる攻撃からの耐性を OS 自身に持たせることができます。つまり、現状の OS の問題点であるアクセス制御の弱点や、現在のセキュリティ対策の問題点、パッチマネージメントの問題点をすべて解決することができるのです。

6. セキュア OS は標準の機能へ

セキュア OS やトラステッド OS に実装されている機能は、今後のセキュリティ対策に必要とされ、あたりまえの機能になっていくでしょう。そのため、最近では OS に標準の機能としてセキュア OS を取り組む動きが活発になってきています。セキュア OS をこれまでのセキュリティ対策と組み合わせて使用すれば、ほとんどの問題点を解決し、いままでとは比較にならないセキュリティ強度の高いシステムを構築することができるでしょう。

高まるITセキュリティプロフェッショナル認証の必要性

NTTコミュニケーションズ株式会社
滑川　愛恵

CISSP試験問題が日本語化され、2004年7月に東京で第一回試験が開催されてから、早いものでもう一年が経つ。日本語化される前は日本にたった40名ほど（うち日本国籍者は15名のみ）しかいなかったCISSP認定者も、2005年6月には300人以上にまで増加した。この驚異的な増加率は、情報セキュリティのプロフェッショナルとしての能力を証明（しかも国際的に）できるCISSPが、企業にとっても個人にとっても、まさに渇望された資格であったことを物語っている。

CISSP認定者の増加に伴い、CISSP認定者を中心としたセキュリティプロフェッショナルのコミュニティを作る動きも出てきた。例えば本年5月に(ISC)²日本支部により開催された「CISSP Forum 2005」には多くのCISSP認定者が集結し、最新情報プレゼンテーションやプロフェッショナル同士の交流を楽しんだ。こうした場で育まれる繋がりもまた、情報セキュリティのプロフェッショナル達にとって大変刺激的なものである。

また、小職が参加しているJNSA教育部会下のCISSPワーキンググループでは、(ISC)²とJNSAの提携により、日本に特化した分野や特有の問題等について検討し、調査を進めているところである。本調査は日本独自分野の策定、ひいては日本版・CISSP上位資格作成を目標としている。

このように日本における動きが盛り上がってきている今、他国での(ISC)²及びCISSPの動向について、いくつかニュースをご紹介したいと思う。

1. (ISC)²®とは

まず、そもそも(ISC)²とは何かを簡単にご説明したい。International Information Systems Security Certification Consortium、略して(ISC)²（アイエスシー・スクエア）は、全世界の情報セキュリティプロフェッショナルに対し認証資格を開発・提供しているNPO（非営利法人）である。1989年の創立以来、既に100カ国以上で34,000人以上のプロフェッショナルを認定しており、米国のフロリダに本拠地を置く他、ロンドン、香港、そして東京にオフィスを持つ。

(ISC)²は、「Certified Information Systems Security Professional（CISSP）」と「Systems Security Certified Practitioner（SSCP）、またそれぞれ特定の分野に特化したCISSPの上位資格（ISSEP、ISSAP、ISSMP）を提供している。なかでも情報セキュリティ資格のゴールドスタンダードであるCISSPは、資格試験システムの認証を実施するための国際的ベンチマークである「ISO/IEC 17024」に基づくANSI（American National Standards Institute: 米国規格協会）の厳格な基準を満たした、最初のIT資格である。認証を受けるには、まず4年間以上（大卒は3年間以上）の実務経験を有することが条件とされ、その上で6時間・250問の筆記試験に合格し、その後推薦状と職務経歴書を提出し審査を受けなければならない。

(ISC)²はまた、CBK（Common Body of Knowledgeの略。プロフェッショナルに必要とされる共通知識をまとめたもの）に基づく教育プロダクトやトレーニングサービスも提供している。さらにCBKの維持・更新についても責任を持ち実施している。

昨年12月、(ISC)²は世界各国の主要企業や政府などの後援のもとに、2005年を「The Year of the Information Security Professional（情報セキュリティプロフェッショナルの年」とする宣言を発表した。

この宣言の目的は、グローバル情報社会の中で、

情報セキュリティプロフェッショナルが果たす重要な役割に対しての理解を深め、また意識を向上させることにある。

宣言に基づき、情報セキュリティプロフェッショナルを支援する他の団体などと協同し、声明書や公共の場でのパネルディスカッション、スピーチ、記事執筆やその他の方法により、2005 年、さらにそれ以降もこの活動を実施していくこととしており、現在までに世界各国の 50 以上の企業や団体が、この宣言に賛同の意を表している。

2. 米国では

(ISC)^2 本部のある米国においては、政府機関を中心に様々な企業や団体において(ISC)^2 の資格(CISSP など）やトレーニングが奨励されている。

最近では 2005 年 6 月に米国従軍軍人省（U.S. Veterans Affairs Department :VA）において、100 人目の CISSP 認定者が誕生したことが話題にあがっていた。

(ISC)^2 によると、同省は近年プロフェッショナル認証資格の必要性を強調することで、サイバーセキュリティスタッフの強化に積極的に参加してきた。その目標の一つとして「CISSP 認定者の従業員を 100 名確保する」と掲げ、結果として CISSP 資格を持つ情報セキュリティスタッフの数は 2001 年時の 4 人からたった 4 年間で 100 人へ、驚異的な伸びを記録した。

VA の Office of Cyber and Information Security のトレーニングリーダーは、「VA は省内の情報セキュリティ能力の向上に大きな関心を寄せている」「CISSP 認定者を獲得することが、従業員の能力向上施策の一つとして、大いに奨励されている」と語っている。

ちなみに、2005 年 5 月 9 日から 13 日まで米国ダラスで開催された「The Veterans Affairs InfoSec 2005 Conference」は、今年で年次開催 9 年目を迎え、連邦政府の中では最大の非国防総省主催イベントとなった。

3. アジアでは

一方アジアにおいて最近の動向といえば、今年 4 月にタイの ACIS Professional Center Co. Ltd.（ACIS）との協定を発表したことが挙げられる。この協定では、タイにおける候補者に対し ISO/IEC17024 規格に適合した情報システムセキュリティの試験及び教育を提供することとしている。

（注：ACIS とは、タイにおいて最重視されている情報セキュリティトレーニング、監査及びコンサルティング会社であり、また、マネージドセキュリティソリューションプロバイダーでもある。）

バンコクで催された調印式には、タイ政府高官や IT プロフェッショナル、ジャーナリスト等が出席し、共同記者会見を行った。

その場で、ACIS の代表取締役及び CEO であり CISSP 認定者でもある Prinya Ho-anek 氏はこう語っている。

「昨今の情報セキュリティを取り囲む状況は、潜水艦を中心とした闘争のようである。その脅威はあらゆる方位から、あらゆる時にやってくる。そのため、CISSP のような情報セキュリティプロフェッショナルは、情報コミュニケーション技術の主要インフラの維持において必須と言える。

『人』は、情報コミュニケーション技術が依存する PPT 要素の三つ（People、Process、Technology）の中でも特に重要だ。情報セキュリティプロフェッショナルには深い知識と経験が求められる。彼らなしでは、技術は役に立たない。

情報セキュリティに従事するプロフェッショナルへの認証は、多くの場所で既にスタンダードになりつ

つある。タイは他のアジア諸国に比べ、十分な数の情報セキュリティプロフェッショナルが存在していないが、(ISC)^{2}との関係を軸にタイの情報セキュリティプロフェッショナルのスタンダードを高めるため、ACISも積極的に活動していくつもりだ。」

尚、タイにおける第一回CBK Review Seminarが2005年5月に開催された模様。

4. 終わりに

これまで見てきたように、情報セキュリティプロフェッショナル認証の必要性に対する認識はあらゆる所で年々高まってきている。ACISのHo-anek氏の言葉にもあるように、セキュリティの要は「人」だ。プロフェッショナルを育て、増やしていくことが今後より一層求められていくはずである。

最後に、(ISC)^{2}のウェブサイト上には、他にも多数の情報セキュリティに関連する最新ニュースが掲載されている。ぜひそちらもお時間のある時に一度アクセスされることをお薦めしたい。

セキュリティ対策情報流通の必要性

JNSA 研究員 兼 セキュリティ対策推進協議会 事務局
関　義和

■ 徹底されないセキュリティ対策

現在、多くの企業や団体では事業を支えるデータを蓄積・処理するコンピューターシステムを守るため多くの費用と労働力を割き、セキュリティ対策に努めています。その甲斐あってシステム管理者が管理するコンピューターがダウン、情報が漏洩するなどの危険性は確実に減っているようです。

しかし、一部のシステムでは対応が不十分なままとなっているようです。ファイアウォールや IDS のログを読む限り、国内の IP アドレスからも相当数のウイルスやワーム感染がうかがえます。

また、ユーザー個人の端末として使われる PC についてもセキュリティ対策は難しいのが実際です。集中管理によるセキュリティ対策が行える組織はまだ限られており、個人の資質に影響されるところが大きいままです。最近の個人情報漏洩事件の多くはユーザーの端末を原因としていることから、今後も対策が必要な部分です。

さらに、家庭を中心とした個人ユーザーにいたってはさらに深刻な状態でしょう。エンジニアに限らず、知人友人に頼まれて PC の操作を教える際に、ウイルス対策ソフトウエアの更新期限が切れたままであったり、パスワードが設定されていないなどの問題を目の当たりにし、頭を抱えるような体験も少なくないのではないでしょうか。

企業のシステムも個人の PC もインターネットを構成するメンバーです。企業は事業を続け、個人情報を守る努力をしていますが、その対となる個人の PC にセキュリティが配慮されていない現状でインターネット社会は安全で安心できる社会基盤になりません。

■ SPREAD の設立

セキュリティ対策の重要なポイントは最新の情報を元に対策を考え実行することです。ネットワーク OS や各種ソフト／ハードウエア製品についての脆弱性対策情報については経済産業省の主導による「情報セキュリティ早期警戒パートナーシップ」が重要な役割を果たすべく今年 7 月より運用開始されました。独立行政法人情報処理推進機構（IPA）と JPCERT コーディネーションセンター（JPCERT/CC）を中心に運用されています。このパートナーシップが目指すのは、脆弱性の発見を起点として、速やかな修正プログラムのリリースなど対策の確立と、確立した対策の実施です。

IPA と JPCERT/CC では脆弱性の情報を管理し、対策手段が整った段階で、脆弱性の情報とセキュリティ対策を対にして Web などを通して配信しています。

セキュリティ対策推進協議会（SPREAD）は情報セキュリティ早期警戒パートナーシップのメンバーとして、セキュリティ対策を実行しなければならないエンドユーザー、システム管理者、SI 事業者などに情報の配信を確実に行うことを目的として JNSA と Telecom-ISAC Japan が中心となって設立いたしました。

■ セキュリティ対策情報の流通という方法

脆弱性についての記述やその対策方法の多くは専門的な視点から記述されているため一般の PC ユーザーには理解が難しいままとなっています。PC や OS のメーカーは脆弱性情報と修正プログラムの提供を個人ユーザーにも理解してもらえるための努力を払っていますが、十分な効果が出てはいるとは言い難い面があります。個人ユーザーはシステム管理者に比べると最新のセキュリティ事情に触れる機会が少なく、日ごろからセキュリティについて考えさせられる機会が少ないことが原因とも考えられます。従来からセキュリティ対策が重ねられてきたサーバに対して攻撃を仕掛けるよりも、フィッシングやウィルス・ワームといったクライアント PC を標的にした被

害が広がりつつあるのが現実です。

こうした個人を中心とした一般のユーザーを対象にセキュリティ情報の浸透を図るために、SPREADではサポーター制度の実現を図っています。サポーターには一般ユーザーに近い方になっていただき、一般のユーザーを支援していただく制度です。従来のようにメールやWebからの情報配信を用意するだけでは一般ユーザーに情報を届けることは困難です。そこでサポーターというユーザー支援を行う人々を組織化してご協力いただき、エンドユーザーに対して直接、以下のような、情報をより確実に伝えることができるようにしたいと考えています。

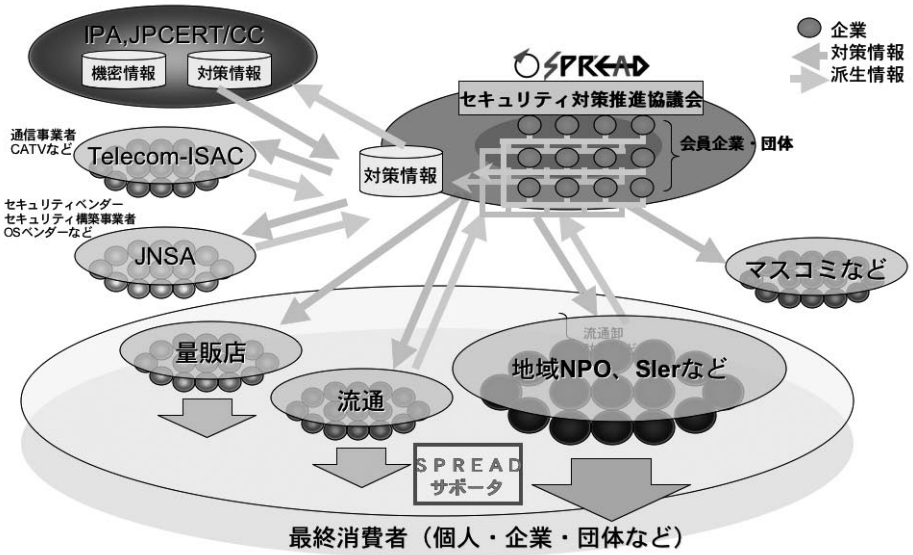
- 脆弱性の情報
- パッチなどの対策情報
- パッチプログラムの適用方法
- フィッシングなどの「騙し」の流行事情

これらの情報を身近に感じていただくことでセキュリティ対策の実効性を浸透させることができると考えています。サポーターにはIT普及を目的としたボランティア、PCを販売サポートする窓口など、PCの操作に詳しい方や、よく相談を受けるような方を一般ユーザーのサポーターになっていただくことを想定しています。

■ まとめ

情報配信は受け取り手に高い興味があれば効果的に活用されますが、関心が薄ければ情報が活用されることはありません。セキュリティの向上には情報の配信に加えて、注意点や身近な事例などの情報を流通し、興味をひきつける方策が必要でしょう。SPREADはPCやネットワークを使うすべての人が互いの安全・安心のために、新しい社会の動きを作る挑戦を行っていきます。

SPREADの位置づけ



JNSA ワーキンググループ紹介

セキュア・システム開発 ガイドライン作成 WG

WG リーダー
株式会社ラック　丸山　司郎

■ 設立趣旨

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ておりますが、具体的な項目やレベルなどの明確な基準は存在しておりません。

一方、開発システムのセキュリティ評価基準としてISO15408が存在しますが、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、なかなか実装は難しいものがあります。

そのような中、現実にサイバー攻撃にあい、事業継続に影響のでる企業も発生していることから、システム開発におけるセキュリティ要件の定義は喫緊の課題であります。

そこで、JNSAに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提示し、広く公開することで、システムオーナがその妥当性（システムの社会的責任とマイナスリスクの除去）を合理的に判断できる評価項目を提示するとともに、システム開発者や、運用者（SI/SO)が適切な競争を行うことで、IT社会の健全な発展の一助となることを目的として当WGを設立いたしました。

よって、当ガイドラインに期待する要件としては以下があります。

- 将来ISO15408等の国際標準への橋渡しとなる指標
- 段階的に分かりやすく実施できるガイドライン
- 利用者の財産などの保護対策内容を明示できる指標
- システムオーナがその妥当性を合理的に判断できる評価項目
- システム開発者や、運用者（SI/SO)が適切な競争を行えるセキュリティ基準

■ 想定成果物

システムオーナが、SI/SOを委託する際の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」作成を目指します。

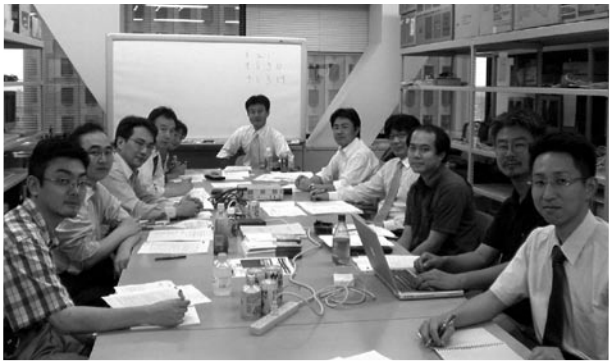
WGの中で成果物の形態について検討した結果、調達側・提供側の双方で使えるガイドラインとなるのが理想ではあるが、時間と体力の観点から、まずは調達側を意識した成果物を目指すべきだろう、という結論となりました。

つまり、『受注時の残留リスクに対する評価を、受注者側と発注者側が共通の基準で話せるもの』を目指して、発注者側のRFPという形で表現できればよいのではないかと考えております。

■ 目標レベル

「まずはJNSAとしての意思表示を」という観点から、当面は以下のようなレベルを想定し、濃度よりも速度を優先していきます。

ー 無いよりまし！（Better Than Nothing）
ー ボトムライン（最低限、実施すべきライン）の提示
ー 簡単・お手軽に使えるレベルの提示



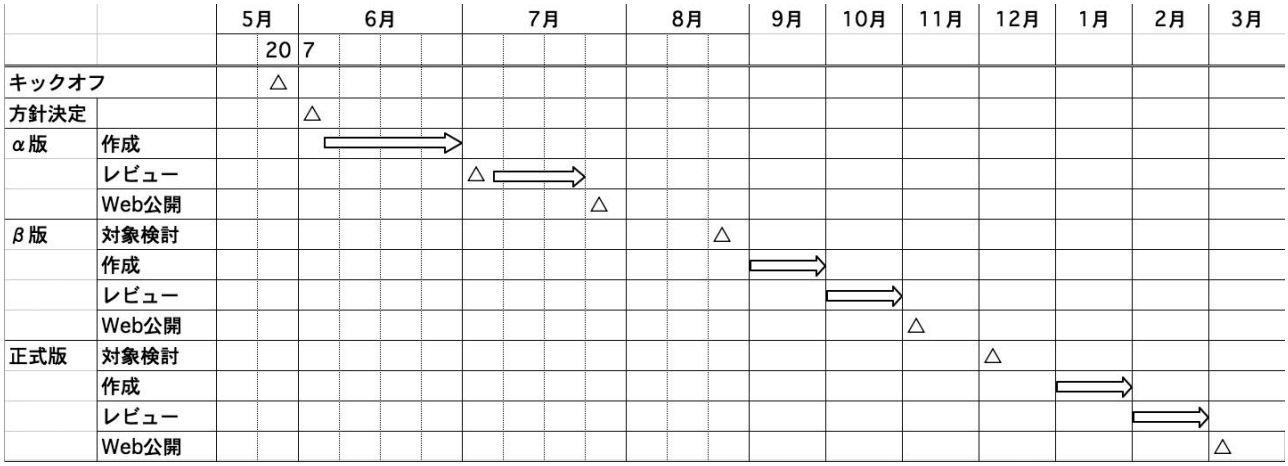
■ セキュア・システム開発ガイドラインの全体像（イメージ）

ガイドライン		検討期間
システム開発		2005 年度のスコープ
インフラ構築		2006 年以降の検討課題
アウトソース		
	IDC	
	運用	
製品導入		
家電組み込み		

■ WGの運営方針

・1 ～ 2 回 / 月の会合を工学院にて行い、全体の意見調整を行う。
・成果物については、メーリングリスト上で検討して、今年度中の公開を目指す。
・当面は、発起人である丸山がリーダを務めるが、内容展開によってはＷＧの細分化やリーダの交代を検討していく。
・メンバー加入は随時受け付けておりますので、ご興味がある方はお気軽に会合にご参加いただくか、JNSA 事務局までお問い合わせください。

年間スケジュール



Webアプリケーションセキュリティ WG

WGリーダー
住商情報システム株式会社　二木　真明

■ はじめに

昨今、またWebサイトが攻撃を受け、改ざんや情報漏洩が発生するという事件が頻発しています。セキュリティ対策はすでに万全と思われていたサイトがなぜ、このような事態に陥ったのでしょう。原因は、Webサーバやそのオペレーティングシステムの脆弱性ではなく、ユーザ自身が開発し、運用していたWebアプリケーションにありました。不正な入力を与えることで、アプリケーションが誤動作し、開発者が意図しない動作をしてしまったのです。大規模な顧客、会員データベースなどと直結して動作することも多いこれらのアプリケーションが誤動作することによる影響は、インフラの脆弱性以上に危険なものです。この点が、これまでのセキュリティ対策の盲点でした。

WebアプリケーションセキュリティWGでは、こうしたアプリケーションの脆弱性対策に焦点をあて、様々な研究活動、啓発活動を展開していきます。

■ 主な活動内容

Webアプリケーションセキュリティを考える場合、ソフトウエア開発、脆弱性検査、監査、侵入検知と防御など、様々な切り口があります。また、こうした切り口からのアプローチには、それぞれの分野での、知識や経験が必要です。今年度のWGでは、こうしたいくつかのアプローチについて分科会形式で検討し、それを全体会でレビューする、という形をとります。現在、作業が進んでいる分科会としては、以下のものがあります。

■ 啓発コンテンツ分科会

Webアプリケーションのセキュリティについての一般の認識はまだまだ浅い、と考えられます。これらを少しでも解消するための啓発活動に利用可能なコンテンツ（セミナー用プレゼンテーション）を作ろうというのが、この分科会の目的です。どちらかといえば、マネジメント層向けの「総合」コンテンツ、開発者向けの解説、運用現場向けの解説など、いくつかの切り口からコンテンツを作っていく予定です。また、出来たコンテンツは公開すると同時に、JNSAが企画、参加するイベントなどでのセミナー等にも活用していく予定です。

■ 受発注ガイドライン分科会

Webアプリケーションの問題を解消するには、まず開発の際にきちんとセキュリティを考慮することが必要です。しかし、このための公的なガイドラインは少なく、ともすれば、開発の際に発注側と受注側の認識のずれが生じることになり、後々、責任の所在

などを含めて混乱することも多いようです。この分科会では、ソフトウエアの受発注における、セキュリティの定義方法について検討し、その問題点や解決策などを議論します。可能であれば、発注側、受注側双方がコンセンサスを取りやすい方法をいくつか提示できればと考えています。

■ 技術研究分科会

Webアプリケーションの攻撃手法や脆弱性の検査、防御手法、ツールなどに関する技術的な研究を目的とした分科会です。日頃、こうした業務に携わる技術者が情報や意見を交換しながら、タイムリーなテーマについて研究を行います。また、この分科会は、各分科会からの要請に応じて、技術的な情報や意見を提供する役割も担います。

■ 最後に

Webアプリケーションセキュリティは、様々な側面からの検討が必要です。そういう意味では、もっと多くの分科会があってもいいかもしれません。実際に、こうした業務に携わっている方々、興味を持たれている方々の参加をお待ちしています。

会員企業ご紹介⑭

株式会社エクスフロント
(http://www.exfront.jp)

私ども株式会社エクスフロントは、今年1月に設立されたばかりの会社です。
私どもが JNSA に加入させていただいたのは、情報セキュリティ SDK「CRYPTER（クリプター)」という製品の販売を手掛けているからです。

このCRYPTERというSDK（ソフトウェア開発キット）は、Crypto++という暗号要素技術のOSSを利用して弊社の関連会社が独自開発した暗号応用ライブラリ集で、「暗号に詳しい技術者でなくても使いやすいAPI」というコンセプトで開発を進めてきたものです。このSDKを基礎として文書保護に特化した文書セキュリティキット（DRM機能、エンタープライズPKI機能、タイムスタンプ機能をオプション提供）も用意されています。

CRYPTERの暗号通信部分は（株）クセロ様のxeloDocumentMobilerに採用されましたが、それ以外にもいろいろなご相談を承っています。当然ながら、SDKをそのまま利用してご自分でシステムやパッケージにセキュリティ機能を組み込む場合のご相談もありますし、課題解決に関するコンサルテーションのご相談や弊社のknow-howを活かした新たなライブラリ開発や関連ソフトウェアの受託開発についてのご相談もあります。
上述した暗号応用技術だけでなく、弊社は自然言語処理技術も得意分野です。

この分野で一般的に良く知られているものとしては機械翻訳システムとか検索エンジンとかがあります。自然な形での言語を解析して英語から日本語に翻訳してくれたり、大量のデータの中からあるキーワードが使われている文書を探し出したりしてくれる技術ですが、この分野に関するコンサルテーションや受託開発も承っております。

弊社は会社立ち上げに当り、以下の経営理念を策定しました。

（1）ミッション
- 暗号技術の応用によって個人・企業にとって安心・安全な社会構築のインフラを提供する。
- 自然言語処理技術の応用によって異文化間コミュニケーションを促進させる。

（2）ビジョン
- 職人気質的アプローチによる製品開発及びソリューション提供を通じて、先端的な技術者集団としての確固たる地位をしめる。
- 情報セキュリティや自然言語処理といった分野において、ニッチでもNo.1になれる領域を開拓する。

（3）価値観
- 顧客ニーズからの発想を常に行う。
- 品質面での妥協をしない。
- 自分の開発した製品（作品）に誇りを持つ。

「職人気質的アプローチ」というのが弊社の大きな特長です。社員誰もが自分の会社に誇りを持ち、「人が人を呼ぶ会社」を目指して邁進する所存ですので、JNSA会員各位のご指導・ご鞭撻を宜しくお願い申し上げます。

お問い合わせ先
株式会社エクスフロント
（URL www.exfront.jp）
E-mail sales@exfront.jp
TEL 03-3596-7640

株式会社エス･エス･アイ･ジェイ

(http://www.ssij.co.jp/)

Security Systems Integration Japan

株式会社エス･エス･アイ･ジェイは、ISMS・P マーク等の情報セキュリティに関わるコンサルティング及び監査をビジネスの機軸として事業展開しています。

私たち株式会社エス･エス･アイ･ジェイのコンサルティングサービスは、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。

また、情報セキュリティの企業としての重要性がますます問われる中、需要の裾野はさらに広がっています。

弊社は今後、より効率的･効果的パフォーマンスに優れたコンサルティングサービスをご提供する為、従来より蓄積されたノウハウ、コンサルティング手法と IT 技術（Web 技術）を融合した新たなサービス（e コンサル、e ラーニング）を提供していきます。

弊社は、情報セキュリティに関わるコンサルティングを行うことで「認証取得」だけでなく、企業の継続と成長を支援しています。

また､私たちは CSR 活動の一環として､国連アナン事務総長が提唱する｢人権･労働･環境･腐敗防止｣の 4 分野と 10 原則からなる｢グローバル・コンパクト｣に、2005 年 1 月より国内 27 番目の加盟企業として参加しています。(http://www.unic.or.jp/globalcomp/) その活動のひとつとして、先日、愛知万博・国連館特別企画“In Larger Freedom”に賛同させていただきました。今後とも社会貢献意識の高い企業として情報セキュリティの普及活動とともに、｢グローバル・コンパクト｣への積極的な活動も展開して参ります。

◇ SSIJ の情報セキュリティコンサルティングとは・・・◇

現在の情報セキュリティ状態を診断したうえで、貴社に足りない部分を補いつつ、貴社にあわせたオリジナルのコンサルティングをご提案いたします。

情報セキュリティマネジメントの構築を通じて、認証取得に限らず、組織や業務を見直すことで生まれる、業務効率の改善、社員のモチベーションアップ、組織の活性化等企業価値の向上等にもお役立ていただきます。

認証取得後の各種運用支援サービスなど、万全のサポートをお約束します。

◇ SSIJ 新サービスメニュー◇

2005 年 10 月初旬 プライバシーマーク取得集中講座 いよいよ開講します！

認証取得に向けて、解決・実現していかなければならない事項を効率的な内容で集中的に修得できるサービスです。近日中に当社ウエブ等で詳細を発表いたします。ぜひご覧下さい。

◇その他 SSIJ のサービスメニュー◇

■情報セキュリティに関する認証取得支援
（ISMS 適合性評価制度、プライバシーマーク制度）

■情報セキュリティに関するサービス
（セキュリティポリシー策定支援、リスクアセスメント講座、情報セキュリティに関する規格の動向解説、等）

■e ラーニング「ネット de 納得！個人情報保護法！！」
（全従業員の個人情報保護やセキュリティに関する意識の啓発、教育）

■各種運用支援サービス

■情報セキュリティ監査

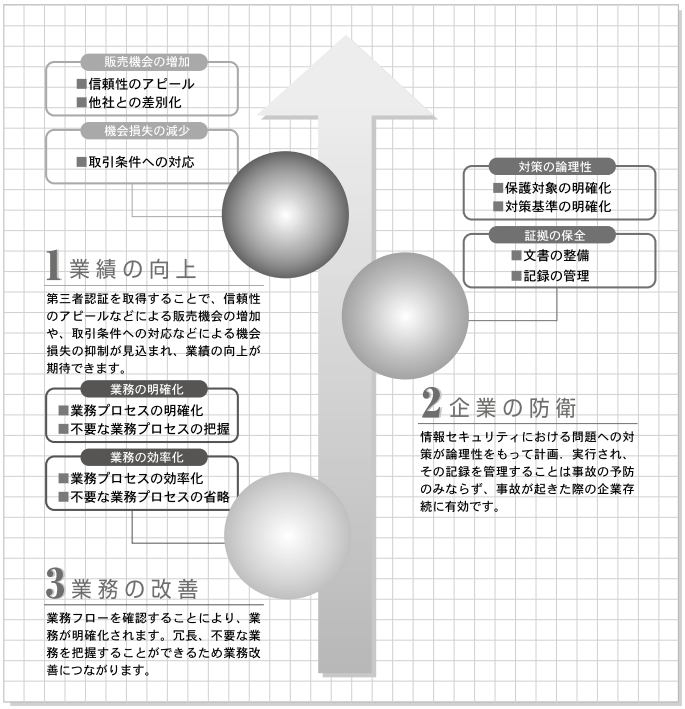
など、お気軽にご相談下さい。

お問い合わせ先
株式会社エス･エス･アイ･ジェイ
〒 105-0021 東京都港区東新橋二丁目 2 番 8 号
TEL : 03-3432-1885 ／ FAX:　03-3432-1760
E-mail : info@ssij.co.jp

◇マネジメントシステム構築のメリット◇

■メリット

情報セキュリティマネジメントシステムの構築によって得ることができる代表的なメリットをご紹介します。



エリアビイジャパン株式会社
(http://www.areabe.com)

個人情報の保護が叫ばれる今日、情報資産を安全に保護することが叫ばれています。しかし本来、情報資産は共有されて初めて真価を発揮するものですから、企業は「情報を“保護”しながら“安全に公開する”」という矛盾するテーマを今まで以上に高い次元で実現することを求められています。

エリアビイ社の SWANStor（スワンストア）は、企業ファイアーウォールの設定を一切変更することなく安全に情報を社内に格納しながら導入することができ、同時にアクセスデバイスを選ばないフットワークに優れたアクセシビリティを提供する、強力な SSL-VPN ソフトウェア製品です。

スワンストアの特徴

■ファイアーウォールの設定変更が不要

企業が情報を公開する際の一番の関心事は安全性です。スワンストアは企業のファイアウォールの設定を一切変更することなく導入できる唯一の SSL-VPN 製品です。セキュリティポリシはそのままに、企業情報を安全に社内に格納したまま導入することができます。

■デバイスを選ばない優れたアクセシビリティ

アクセスクライアントにソフトウェア導入の必要がなく、ブラウザさえあれば利用することができます。特に、携帯電話端末の対応機種は多岐に渡ります。ビジネスにはスピードが大切。優れたアクセシビリティで業務の効率化を図れます。同時に管理者の負荷を減らすという意味でもスワンストアは非常に優れたソリューションを提供します。

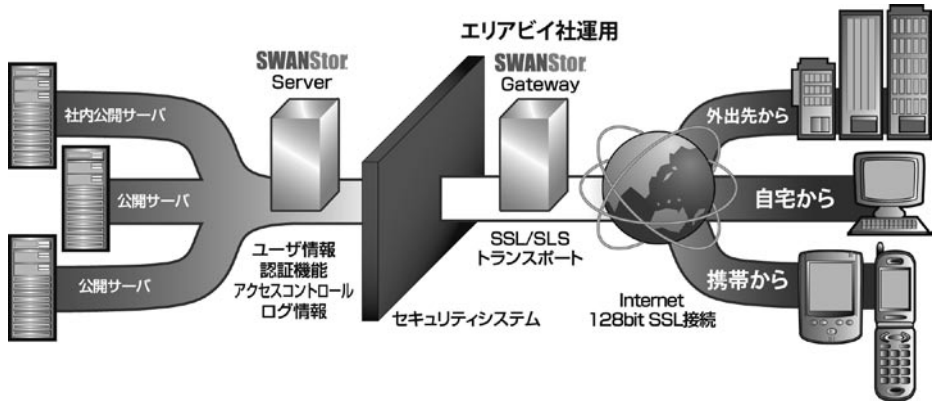
■強力で柔軟なアクセスコントロール

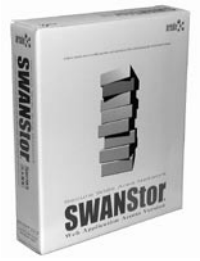
スワンストアのアクセスコントロールを利用すれば、グループ毎、個人毎に情報資産へのアクセス権限の設定を簡単に行うことができます。例えば、部署毎にアクセスする資源を設定したり、プロジェクト毎に委託会社に情報を公開する時など、利用シーンによって強力かつ柔軟に設定することができます。

■規模や予算に合わせた多彩なオプション

システム導入にあたっては、「企業の一部で利用を開始し、その後会社での導入を考えたい。」、「利用するのは一部門だけであって、全社的な導入は今のところ考えてない。」というニーズにもスワンストアは柔軟に応えることができます。低価格の小規模向けシステムから、個人証明書等の他の認証サーバーとの連携による認証強化、大規模企業向けにはクラスタオプションによる冗長構成の提供など、スワンストアなら規模やニーズに合わせてシステムを柔軟に導入、移行することができます。

スワンストアのシステムイメージ





エリアビイジャパン株式会社について

エリアビイは2000年12月に米シリコンバレーで創業、2001年11月にエリアビイジャパン株式会社を設立しました。物理的なネットワーク接続が生み出す様々な束縛から開放し、受け取りたい情報を自由に安全にアクセスしたいという「アクティブ・インフォメーション・ルーティング・テクノロジー (AIR)」をベースに製品開発を行なっています。エリアビイは、SSL-VPN を利用したリモート・アクセス・ソリューション分野において、国内における導入実績では No.1 のリーディングカンパニーです。

お問い合わせ先
株式会社エリアビィジャパン
〒 105-0013 渋谷区恵比寿 1-19-19
恵比寿ビジネスタワー 13F
TEL : 03-4360-3961
E-mail : sales@areabe.com

株式会社ソリトンシステムズ
(http://www.soliton.co.jp/)

ソリトンは日本で最初にLAN、ネットワークＯＳに取り組んだ会社で、数多くの大規模ネットワークを構築し、業界のパイオニアとしての役割を果たしてきました。最近は、「ブロードバンド」と「セキュリティ」をテーマとしてビジネスを展開しています。
ブロードバンドの分野では、映像配信プロジェクトに参画し、日本で初めての商用ビデオ･オン･デマンド（VOD）サービスを実現しました。
また、長年培ったネットワーク管理の技術とセキュリティを統合化したセキュリティ製品を開発。Soliton SmartSecurity として、物理的な入退室管理、コピー機を含むデバイスへのアクセス制御、ファイル暗号化、ログ収集などの情報漏洩対策、さらに無線アクセス対策や検疫ネットワークに至るまで、トータルなセキュリティソリューションを提供しています。

特に注目される２商品

デスクトップセキュリティ

SmartOn

SmartOnは､ICカードやUSBキーなどの認証デバイスを使って、ユーザ認証を強化します。PCを利用する際､ICカードやUSBキーなどの「電子の鍵」とパスワードを要求、それらが合致しないと利用できません。
ユーザーごとのアクセス制御、外部記憶媒体等の利用禁止、操作状況のログ収集などを行い、情報への不正なアクセスや情報漏洩を防止します。一括登録機能や、継続的に利用するための運用管理機能を豊富に搭載し、低コストで短期導入が可能です。
運用管理に優れた大規模向けSmartOn NEOと、ICカードのほかに携帯電話でも使えるパーソナル版のSmartOn Soloもあります。

■ログオン認証の強化
PC利用時のユーザー認証を強化します。ICカードなどがなければ単にID/Passwordの入力だけでは、Windowsへのログオンはできません。

■デスクトップ環境の固定化
共有PCで､ユーザー毎に（認証デバイス毎）にPCリソース各種にアクセス制限をかけられます。

■　ファイルの暗号化
グループ内で重要なファイルを暗号化し、その暗号鍵を共有する者同士で安全にファイル共有ができます。ユーザーの操作ミスによる情報漏洩も防止します。

■パスワード自動入力
PCログオン後に起動させる各種アプリケーションの認証用パスワードもICチップに記憶させ、自動送出します。

内部情報漏洩対策のためのPC用ログ収集・解析ソフトウェア

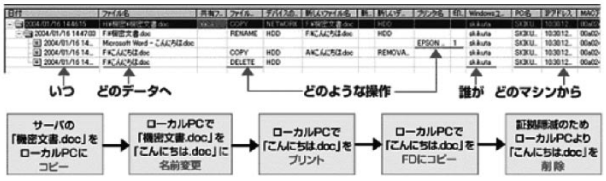
InfoTrace

InfoTraceは、各社員のPC操作をフライトレコーダ式にロギングし、電子データを中心とした情報流出過程の追跡を支援するソフトウェアです。特別なDBは不要でLogServerのインストールは約3分で完了します。Agentインストールも極めて簡単です。

■集　計
PCのログイン、ログオフ操作からネットワーク及びローカルファイル参照、削除、名前変更、コピーなどのファイルアクセス情報を全て収集します。アプリケーション操作やプリント出力も記録します。

■検　索
「このファイルをアクセスした履歴」､「このユーザーが行った操作」などのさまざまな条件で検索可能。結果はCSV形式で出力できます。

■追　跡（拡散トレースとバックトレース）
もとファイルからアクセス、操作、持ち出しまでのログを追跡。持ち出しデバイスなどのファイル名から親ファイルを見つけ出し、経路をツリー型で表示します。



■集　計
ユーザー別、プリンタ別で指定した期間や条件における印刷集計を行います。

お問い合わせ先
株式会社ソリトンシステムズ
ネットワーク事業部
TEL : 03-5360-3811
http://www.soliton.co.jp/

ユーテン・ネットワークス株式会社
(http://www.u10networks.com)

u10 Networks

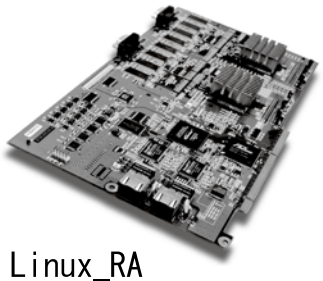
ユーテン・ネットワークス株式会社は、 アプリケーション・アクセラレーションをソリューション提供するソフトウェアベンチャー企業です。 最先端の並列プロセッシング技術、 リコンフィギュラブル技術を駆使し、 ネットワークアプリケーションをギガビットの速度に高速化致します。 製品として、 アクセラレーション・ボード製品、 アプライアンス・システム製品、 高速 IP コアを提供して参ります。

リコンフィギュラブルアクセラレータ製品「Linux_RA」、ギガビット VPN アプライアンスサーバ「SGV1000」をご紹介致します。

Linux_RA （Reconfigurable Accelerator）

今日までは、 エンタープライズレベルのネットワーク・アプリケーションの構築を行うにあたり、 高速処理が必要なものをハードウェアにて、 また複雑な処理や変化の激しいものはソフトウェアにて構築することが多く、“高速かつ柔軟性のあるシステム”の構築は困難でした。 しかし、 Linux_RA を導入することにより、 お客様の既存のソフトウェアアプリケーションを短期間で 10 倍以上高速化し、 ソフトウェアの柔軟性を併せ持つことが可能になります。

処理時間が掛かる部分は Linux_RA ボードのファームウェアとして実装し、 API でソフトウェアとの接続をすることで高速化が図れます。 短期間でファームウェアの開発ができ、 さらにめまぐるしく変化する仕様に対しては柔軟かつ敏速にファームウェアの機能をアップグレードすることが可能です。 システム管理制御は、 あらかじめ容易された汎用 CLI （ Command Line Interface） または Web GUI から運用することができます。 また、 制御ミドルウェアやドライバも付属していますので、 お客様はアプリケーションの開発に注力できます。 これにより、 高速 VPN （仮想接続網） / ネットワーク監視装置 / メールフィルタリング / データ暗号化 / 画像フォーマット変換など、 幅広いアプリケーションに対応することができます。 こうしたお客様のニーズや環境に合わせたシステムの構築が、 少ない投資で可能であり運用開始にも時間が掛かりません。 また、 別売の3DES、 Blow fish などの高速 IP コアと組み合わせることで、 高速な暗号処理が実現可能となり充実した開発環境をご提供することができます。



Linux_RA
Reconfigurable Accelerator

Linux_RA は、 これらの特長を生かすことにより、 既存のアプリケーションから新しいアプリケーションまで対応することができ、 基幹系から端末系への適用も可能です。 有線／無線を問わず、 通信業者向けシステムからコンシューマ製品まで、 各種各様のシーンで高速かつ柔軟な仕組みをご利用頂くことができます。

SGV1000 (u10 Scalable Gigabit VPN Solution)

SGV1000 – u10Scalable Gigabit VPN Solution は、 ギガビット転送性能を持つ VPN アプライアンスサーバです。 最先端並列コンピューティング技術を駆使し、 パケットストリームのパイプライン処理と、 バーチャルリソーススケジューリングアルゴリズムにより1Gbps Full duplex の高速な VPN 転送性能を達成しております。 また、 リソース・スケーラブル・アーキテクチャという独自のアーキテクチャを採用、 SGV1000 をカスケード接続することで、 ギガビット転送性能を維持したまま機能を追加することが可能です。 ニーズに応じて帯域制御機能、 フィルタリング機能、 セキュリティ機能などを追加することができます。

SGV1000
「今秋販売開始予定」

セキュリティ状況に代表されるように、 インターネットの環境もめまぐるしく変化します。 IT インフラが本質的に持つ将来の不確定性に対して、 その変化に適応し吸収できる機構がネットワーク機器には必須です。 SGV1000 の持つ、 リソース・スケーラブル・アーキテクチャは、 あたかもハードウェアを自由に再構築できる柔軟性を実現し、 将来の変化に適応できる斬新な仕組みを提供致します。

お問い合わせ先

ユーテン・ネットワークス株式会社
〒152-0031 東京都目黒区中根 2-20-8 Tel 03-3723-5506
e-mail sales@u10networks.com http://www.u10networks.com

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■

○専用管理ツール付き法人向けマルウェア対策製品「AntiMalware」販売開始

国産のスパイウェアやハイジャッカーなどに対する PC 防御を強化し、18 万種以上（2005 年 7 月現在）のマルウェア（不正プログラム）を検出します。また、自社に開設した「スパイウェア リサーチセンター」での研究・分析、その成果を「AntiMalware」へリアルタイムに反映することで、国内インターネット事情に最適なソリューションを提供します。

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

【スパイウェア リサーチセンター】
http://www.ahkun.jp/researchcenter/SpywareResearchCenter.html

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

○ SSH Tectia ソリューション

SSH Tectia は、政府関係機関、金融機関、大企業向けのエンドツーエンドのコミュニケーション セキュリティ ソリューションです。次のような 3 つのデータ通信セキュリティのニーズに対応できます。

①「セキュアなアプリケーション接続」：アプリケーションや IT インフラを変更することなく、イントラネットやＥＲＰ、ＣＲＭなどの自社開発および商用アプリケーションの両方を透過的に保護します。
②「セキュアなファイル転送」：内部と外部両方のファイル共有に対して、ネットワーク全体で自動や対話型の形式のセキュアなファイル転送を可能にします。
③「セキュアなシステム管理」：システム管理者に、異機種混在のＯＳ環境でリモートからサーバーを管理する機能を提供します。

【製品情報詳細】
http://www.jp.ssh.com/products/

◆お問い合わせ先◆
SSH コミュニケーションズ・セキュリティ株式会社　営業部
Tel: 03-3459-6830
E-mail: sales.jp@ssh.com

○ SecureCube シリーズ（PC Check、Site Security Check、Access Check、Mail Check）

NRI セキュアの「セキュアキューブ」では、社内で管理しているクライアント PC やサーバのセキュリティ状況を一元管理することができ、また、本番環境へのアクセスや電子メールの監査、外部メディアの接続のチェックなど、内部からの情報漏洩事故を防ぐことも可能です。
セキュリティ管理者の手を煩わせていた一連の業務を、一挙に省力化・効率化します。

【製品情報詳細】
http://www.nri-secure.co.jp/service/cube/

◆お問い合わせ先◆
NRI セキュアテクノロジーズ株式会社
E-mail: info@nri-secure.co.jp

○「Web アプリケーションファイアウォール」TrafficShield のご紹介

TrafficShield はクラッカーや悪意ある攻撃からアプリケーションを保護する「Web アプリケーションファイアウォール」と呼ばれる新しいタイプのセキュリティ製品です。TrafficShield では、あらゆる Web アプリケーションの脆弱性をターゲットにした攻撃から機密情報を保護するだけでなく、きめ細かいセキュリティポリシーを実行することで Web アプリケーションそのものを保護します。

【製品情報詳細】
http://www.f5networks.co.jp/ja/products/t-shield_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
http://www.f5networks.co.jp/

○電子メールフォレンジック機器「メールタンク」

従来のフォレンジック・メールアーカイブ製品は、コストの面で中小事業者の方には導入しづらいものでした。
しかし、メールタンクは設置・管理・監査と、導入から運用にかかわるすべての面での低コスト化を実現。専門の管理スタッフ（知識）も不要です。
さらに上位機種のメールタンク -R では、危険なメールを検知し警告を発するリアルタイム警告機能も備え、情報漏洩はもちろん、電子メールの不正利用をも見逃しません。

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

◆お問い合わせ先◆
株式会社コネクタス
Tel: 03-5711-3323
E-mail: mailtank@connectous.co.jp

JNSA 会員企業情報

○ eTrust PestPatrol Anti-Spyware Corporate Edition

本製品は、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す。
このソリューションの導入によって、不正なアクセス、情報漏えい、システムパフォーマンスの低下といったセキュリティ・リスクを低減することが可能です。
また、導入から運用、管理に至るまで、一元化された管理コンソールから操作することができ、大規模運用が可能です。

【製品情報詳細】
http://www.caj.co.jp/etrust/epp/

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

○認証最適化ソリューション（Secure Trust Link）

近年、認証の対象となるシステムが増加し管理が複雑になってきています。
ユーザ管理情報と人事情報を連動させ、統合管理された認証システムを独自に構築し運用していた実績とノウハウをご提供いたします。
本ソリューションの提供機能例

1．アカウント情報の一括管理と一括更新
2．パスワードのユーザー変更作業の軽減
3．人事異動時の管理作業の大幅削減
4．不要アカウント・不要権限の陳腐化防止
5．運用コストの大幅削減

【製品情報詳細】
http://www.comsys.co.jp/info/2005/pdf/ninsho_seculity.pdf

◆お問い合わせ先◆
日本コムシス株式会社
IT ビジネス事業本部　ソリューション部
ネットワークソリューション部門 セキュリティグループ
〒 141-8647　東京都品川区東五反田 2-17-1
Tel: 03-3448-7082
Fax: 03-3448-7177
E-mail: security.tokyo@comsys.co.jp
http://www.comsys.co.jp/

○リアルタイムデータベースセキュリティ Chakra

データベースセキュリティを向上させたいとお考え中の皆様を、Chakra はお助けします。
Chakra は、ネットワーク上を流れている SQL*NET のパケットをキャプチャし、プロトコルを解析することで、データベースへの処理要求とその結果を取得する構造になっているため、稼動しているデータベースに一切影響を与えずにデータベースアクセスを監視、ロギング、アラートを発生させ、不正アクセスからデータを防御します。

【製品情報詳細】
http://www.nst-japan.com/t_product/chakra/chakra.html

◆お問い合わせ先◆
株式会社ネットワークセキュリティテクノロジージャパン
Tel:03-5545-1801
E-mail: info@nst-japan.com
http://www.nst-japan.com

○迷惑メールをシャットアウトする、メール・フィルタリング装置「SurfControl RiskFilter E-mail」

日本語に完全対応した、導入が容易なアプライアンス型メール・フィルタリング製品で、優れた操作性によりすべての機能をすぐに稼動させることができます。
HTML やテキストベースの迷惑メールだけでなく、画像や動画などのあらゆるファイルをフィルタリングでき、社内のネットワークトラフィックを軽減できます。
また、各種の E-mail フィルタリングによる DoS 攻撃や DHA への対応など、E メールの脅威や脆弱性に対する確かなセキュリティを実現します。

【製品情報詳細】
http://www.hucom.co.jp/product/riskfilter/index.html

◆お問い合わせ先◆
株式会社ヒューコム
ITS 事業本部　営業推進グループ
Tel：03-5306-7362（直通）
E-mail: ml-product@hucom.co.jp

○情報リスクに対する企業防衛システム「MSIESER」（エムシーサー）の紹介

たった一度の事故で企業の信頼が失墜することがあります。
「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。
一刻も早い対策は、更なる企業の信頼向上に貢献します。
★誰が・いつ・何を・どこで・どのように・何の為に・・・を素早く解明できます。
★内／外部の不正利用者／痕跡を追跡・発見して簡単に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
営業第 3 部 3G
担当 : 平野
Tel:03-3546-5040
E-mail : msieser@ryoyo.co.jp

■ サービス情報 ■

○「メール ASP サービス、AAMS」

AAMS は、ISP 向けのメール ASP サービスです。アンチウィルス / アンチスパムフィルタを標準装備、ISP 毎に異なるセキュリティ設定のニーズに柔軟に対応することが可能です。
さらに SMTP Auth や Message submission、TLS/SSL による経路暗号化など、セキュアなメールサービス提供に必要な機能を完備しており、サーバやストレージの冗長化により、システムの信頼性と可用性を確保します。

【サービス情報詳細】
http://www.iri-com.co.jp/

◆お問い合わせ先◆
株式会社 IRI コミュニケーションズ　営業部
Tel: 03-5908-0715
E-mail: sales@iri-com.co.jp

○セキュリティ情報提供サービス DeepSight

JNSA 会員企業様向けに期間限定（9 月末）の特別割引販売を開始します。
世界 180 ヶ国以上 20,000 社超のパートナー企業、大学をはじめ研究機関のセキュリティシステムのほか、公開、非公開のさまざまな情報源から攻撃データを収集し、相関分析を行っています。
分析結果をもとにお客様のネットワーク環境に合わせた早期警告情報と、攻撃への対処方法を年間を通じ逐一お届けします。
※期間限定販売の詳細は担当までお問い合わせ下さい。

【サービス情報詳細】
http://www.symantec.com/region/jp/deepsight/index.html

◆お問い合わせ先◆
株式会社 シマンテック
担当 : 劔物（けんもつ）
E-mail:shuichiro_kenmotsu@symantec.com

○「IT セキュリティ評価・認証制度（CC 認証）における評価業務」および「関連するコンサルティング・サービス」を行います

「IT セキュリティ評価・認証制度」では、国際セキュリティ標準 ISO/IEC 15408 に基づき、認定された評価機関（弊社）がセキュリティ製品・システムの評価を行い、認証機関（IPA）より申請者に対して認証書が交付されます。
日本で取得した認証は、国内だけでなく諸外国政府等の調達にも有効となります。
弊社では、評価業務および認証取得のための各種コンサルティング・サービスを行っております。

【サービス情報詳細】
http://www.ecsec.jp/service/index.html

◆お問い合わせ先◆
株式会社電子商取引安全技術研究所
担当 : 長濱・針間
Tel: 03-5259-8061
E-mail: info@ecsec.jp

○プライバシーマーク取得のための「ラピッド・コンサルティング講座」

「プライバシーマーク認定取得」における取得申請までの各ステップ実務の、コンサルティングを含めながら約 4 ヶ月間（全 8 回）の研修を行う複数社参加での講座です。
【対象】 P マーク認定取得を目指す法人
【費用】 609,000 円（全 8 回分）

【サービス情報詳細】
http://www.rhc.co.jp/r-isap/

◆お問い合わせ先◆
リコー・ヒューマン・クリエイツ株式会社
Tel: 03-5148-5817
E-mail: tsuneo.nakamoto @ nts.rhc.co.jp

■ イベント情報 ■

○ CA ジャパンのイベントとセミナーのお知らせ

【イベント情報詳細】
http://www.caj.co.jp/events/

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

JNSA2004 年度ワーキンググループ成果報告会

JNSA 研究員　安田　直義

2005 年 6 月 13 日､大手町サンケイプラザに於いて、JNSA2004 年度ワーキンググループ成果報告会と定時総会が開催されました。ここでは、成果報告会の内容についてご紹介します。尚、当日のプレゼン資料などは下記の URL で公開されていますので、合わせてご覧ください。

http://www.jnsa.org/seminar/2005/seminar_20050613.html

成果発表会はプログラムのように、2 部屋に分かれて並行して報告されました。両方聞きたかった、というご意見は昨年もあったのですが、限られた時間と場所で JNSA の多くの活動報告を行いたいということで、趣旨をご理解いただけるようお願いいたします。また、トラック間の休憩時間も微妙にずれていることもご指摘を頂きましたが、これも画一的に時間を割り振るのではなく、成果発表会で各 WG から報告する内容によって調整した結果であることをご理解頂ければ幸いです。

さて、報告内容についてご紹介して行きましょう。2 トラックの 1 トラック目は、教育部会と政策部会、2 トラック目は技術部会が担当しました。順を追って報告内容を簡単にご紹介します。

311 号室
教育部会　10：00 ～ 10：50
10：00 ～ 10：30 スキルマップ作成 WG みずほ情報総研　佐久間敦氏 10：30 ～ 10：40 CISSP-WG NTT コミュニケーションズ 大河内智秀氏 10：40 ～ 10：50 情報セキュリティ教育 WG ヒューコム　松田剛氏
10：50 ～ 11：00　休憩
11：00 ～ 11：30 教育部会特別講演 東京大学大学院　工学系研究科 工学教育推進機構　教授 吉田眞氏
11：30 ～ 12：30 **昼休み**
政策部会　12：30 ～ 15：30
12：30 ～ 13：00 セキュリティ被害調査 WG ディアイティ　山田英史氏 13：00 ～ 13：30 個人情報保護法ガイドライン WG 大塚商会　佐藤憲一氏
13：30 ～ 13：40　休憩
13：40 ～ 14：10 マーケットリサーチ WG グローバルセキュリティ エキスパートジャパン 勝見勉氏 14：10 ～ 14：30 セキュリティ会計ガイドライン 検討 WG 凸版印刷　佐野智巳氏 14：30 ～ 14：50 セキュア・システム開発 ガイドライン WG ラック　丸山司郎氏

312 号室
技術部会　10：00 ～ 15：30
ごあいさつ 技術部会長　佐藤友治氏 10：20 ～ 10：40 セキュリティポリシー WG NEC ソフト　小杉聖一氏 10：40 ～ 11：10 脆弱性定量化に向けての検討 WG 京セラコミュニケーションシステム 郷間佳市郎氏
11：10 ～ 11：20　休憩
11：20 ～ 11：40 ハニーポット WG JNSA 研究員　園田道夫氏 11：40 ～ 11：50 不正プログラム WG アークン　渡部章氏
11：50 ～ 12：50 **昼休み**
12：50 ～ 13：20 PKI 相互運用技術 WG セコム IS 研究所　松本泰氏 13：20 ～ 13：40 S/MIME 検討 WG NTT コムウェア　磐城洋介氏
13：40 ～ 13：50　休憩
13：50 ～ 14：20 暗号モジュール評価基準 WG シーフォーテクノロジー 小川博久氏 14：20 ～ 14：40 Web セキュリティ調査・検証 WG 住商エレクトニクス　二木真明氏
西日本支部　14：40 ～ 15：00
14：40 ～ 15：00 中小企業向け個人情報保護対策 WG 伊藤忠テクノサイエンス 市川順之氏

トラック 1

教育部会

スキルマップ作成 WG

みずほ情報総研の佐久間敦氏から、スキルマップについて報告されました。スキルマップは、2002 年から IPA の課題として取り組んできたテーマで、現場で即戦力となる技術者を採用したり、人材流動の際に技術スキルを的確に把握して、需要と供給のミスマッチをなくすための評価方法について検討してきました。今回の報告はその集大成として行われました。

CISSP-WG

NTT コミュニケーションズの大河内智秀氏から、CISSP-WG について紹介がありました。この WG は、2004 年度の途中から準備会が設けられ、2005 年度に新設された WG で、CISSP の日本語化と日本の事情を反映した ISSJP の作成を目指しています。この WG には、東大の安田浩教授や総務省のご参加も頂いています。

情報セキュリティ教育 WG

ヒューコムの松田剛氏から、情報セキュリティ教育に関するカリキュラムの実証評価と、いろいろな教育カリキュラム等の整理を行い、JNSA としての推奨教育リストを作成する活動について説明がありました。この活動は、経済産業省からの課題として活動する実証評価プロジェクトと、JNSA としての推奨教育を提案する WG とに分かれて活動を行うことになりました。

教育部会特別講演

東京大学大学院・工学系研究科・工学教育推進機構 教授の吉田眞氏から、「これからの工学・技術者教育」について講演して頂きました。国際性、リーダーシップ、幅広い視点、等々を身につけられる教育について、環境や主義の対立、問題意識の指摘、工学・技術者教育を取り巻く問題等について考察が行われました。工学系修士課程のアンケート調査でも、基礎力不足と視野拡大の基盤不足が現れていましたが、底上げをしてもあまり効果はなく、トップを引き上げることにより全体がレベルアップするそうです。高い平均点ではなく、ここぞの 100 点を評価するような仕組みに変える必要があるとの方向性が示されました。最後に Alan Kay の『人間に知識を与える唯一の方法は、学びたくなるようなきっかけを与えることだ』という言葉を引き合いに出し特別講演を締めくくられました。

吉田先生には教育部会で更にディスカッションをしていただくことを企画しています。JNSA の Web ページを注意してみていてください。

政策部会

セキュリティ被害調査 WG

ディアイティの山田英史氏から、2004 年度・情報セキュリティインシデントに関する調査報告について説明されました。この調査報告は、アンケートとヒアリングによって 2001 年度から実施されています。当初からの情報セキュリティ事件・事故の実態調査および被害額算定式の提案と、2002 年度から考察している個人情報漏洩における被害想定と考察からなっています。公開されている個人情報漏洩に関する事例の情報資産価値（想定損害賠償額）は、2004 年度で 4,666 億 9,250 万円に上ると試算されていました。

個人情報保護法ガイドライン WG

大塚商会の佐藤憲一氏から、3 月に出版された「個人情報保護法対策セキュリティ実践マニュアル 2005 年度版」を中心に解説されました。この本は、企業の視点で実務に則した対策を行えることを目指して、5W1H による解決を考えられるように構成されてい

ます。対症療法的な具体例が盛り込まれ、すぐ役に立つ対応を用意できます。

マーケットリサーチ WG

グローバルセキュリティエキスパートジャパンの勝見勉氏から、IT セキュリティ対策施策の導入・実施状況とその満足度調査に関する報告が行われました。いろいろな観点から考察を加えていますが、技術的に難しいシステムや機材を採用したにも拘らず、外部サービスを利用せず、結果として問題を起こしている可能性があることが浮かび上がってきているとの指摘がありました。

セキュリティ会計ガイドライン検討 WG

凸版印刷の佐野智己氏から、企業における情報セキュリティ確保への取り組みを適切に評価し、把握し、そして伝達する仕組みとして、「環境会計」に倣って、「セキュリティ会計」の考え方の提唱がありました。本 WG では、目的×対策×対象による三次元モデル『情報セキュリティ会計キューブ』を提案し、コストと効果を定量化することを目指しています。まだ新しい分野なので、広く意見を聞きたいとのことでした。

セキュア・システム開発ガイドライン WG

ラックの丸山司郎氏から、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り、開発システムのセキュリティ評価基準として ISO15408 が存在するが、どのレベルを選択すべきかの判断基準がほとんどない、との問題提起がされました。この状態を改善するために、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したいという WG の趣旨と活動の方向性について説明がされました。

トラック２

技術部会

セキュリティポリシー WG

NEC ソフトの小杉聖一氏から、セキュリティポリシー策定を ISMS 認証基準などを参考にし、リスク分析や規程書（ドキュメント）作成のポイントや実際の実装方法について情報公開をしたいという WG の活動について説明がされました。ポリシー WG は 2000 年から活動していますが、2004 年度からは、(1) サンプルポリシーとＩＳＭＳ認証基準の対応確認、(2) ポリシー（管理策）に対応した技術対策の調査の両面から検討しています。

脆弱性定量化に向けての検討 WG

京セラコミュニケーションシステムの郷間佳市郎氏から、脆弱性の定量化アプローチについて説明がされました。意思決定者が脆弱性対策情報に対応する／しないの決定、あるいは、対応の緊急性を判断するための指標となる数値を算定するモデル式を作ろうという試みです。R ＝ T × A × V（R: リスク T: 脅威 A: 資産 V: 脆弱性）という式が有名ですが、定量化が難しいので、理論的には正しいけれど、現場で使うことが困難という認識が背景にあります。

ハニーポット WG

JNSA 研究員の園田道夫氏から、ハニーポットの実証実験について活動報告がありました。ハニーポットも最近は第 3 世代のシステムが出てきているので、2005 年度の活動の前半として第 3 世代のシステムの稼動実験を行いたいという企画が説明されました。また、ログの解析手法の研究も引き続き行い、ハニーポットの利用対象や効果について実証していくとの予定が示されました。

不正プログラム調査 WG

アークンの渡部章氏から、2004 年度の成果として、「絵で見るネットワークの脆弱性と脅威」についての説明がありました。SANS が公開している“The Twenty Most Critical Internet Security Vulnerabilities The Experts Consensus”をベースにして、最も危険なセキュリティの脅威 Top 20 を判り易く説明した結果について解説されました。

PKI 相互運用技術 WG

セコム IS 研究所の松本泰氏から、ChallengePKI プロジェクトと並行して情報発信している本 WG の活動が説明されました。年 3 回参加している IETF でのマルチドメイン PKI を始めとする今までの活動についての概要と、2004 年度に取り上げた PKI における UTF8String 問題（RFC 3280 の標準の問題）についての詳細が解説されました。現時点でも、アプリケーションの実行環境によって、証明書が等しく扱われていないことが報告され、RFC 標準に追加すべき提案について説明がされました。これは 2004 年 11 月に引き続き、2005 年 8 月の IETF でも議論されました。

S/MIME 検討 WG

NTT コムウェアの磐城洋介氏から、2004 年度の成果として「S/MIME メールクライアントの機能検証結果報告」が説明されました。メールソフトに PKI に基づいた S/MIME 機能がどれだけ正確に実装されているかについて、12 種のメーラでの検証を行った結果が紹介されました。メールヘッダの扱いに関する技術的な問題点、証明書の失効検証をしていないものが多かった現実、認証局に対する課題などが提起されました。

暗号モジュール評価基準 WG

シーフォーテクノロジーの小川博久氏から、暗号モジュールを評価するための要件である FIPS140-2 と、そのスキームとしての CMVP に関する解説がされました。2004 年 12 月 14 日(火)に情報セキュリティ大学院大学で開催された「暗号モジュール評価基準カンファレンス」の成果を中心に暗号モジュールの実装に関する問題点の指摘が行われました。

Web セキュリティ調査・検証 WG

住商エレクトロニクス（現 住商情報システム）の二木真明氏が急用の為、メンバーと一緒に活動している JNSA 研究員の安田から報告されました。Web アプリケーションが包含する脆弱性についての対策や回避策の検討を行うことを WG の目標としていることが紹介されました。現在 3 グループに分かれて活動しています。(1) Web アプリケーションセキュリティに関する啓発コンテンツの作成　(2) Web アプリケーション開発の受発注におけるセキュリティガイドラインの検討　(3) 攻撃手法の技術的研究

西日本支部

中小企業向け個人情報保護対策 WG

伊藤忠テクノサイエンスの市川順之氏から、西日本支部としての活動が報告されました。2005 年 4 月、個人情報保護法完全施行に対して中小企業がどのような状況に陥るのか？、できる対策は何があるのか？、といった観点から、モニタ企業を募って JNSA としてコンサルティングを実施し、進捗・結果を研究チームへフィードバックして、必要な対策を共有することを目指しています。

以上、2004 年度の JNSA 部会の成果報告会の内容を簡単にご紹介しました。2005 年度の活動は若干変更がある部分もありますので、ご質問、参加希望、新規 WG の立上げ等のご相談等があれば、遠慮なく JNSA 事務局までご連絡ください。

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～

【背景と目的】

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いたします。

【特　　色】

- ウイルス感染、詐欺行為、プライバシー侵害などの情報犯罪に対する正しい理解を広め、初心者でも安全快適にインターネットを楽しめるようにします。
- 各地でネットワークセキュリティの啓発に関わる人々に「インターネット安全教室」セミナーのノウハウやツールを提供し、「インターネット安全教室」の活動を全国に広めます。
- セミナーコンテンツとして、冊子付きのセキュリティ啓発 CD-ROM を作製し、セミナーで使用します。
- CD-ROM は開催地で配布するだけでなく、セミナー終了後は希望者へ広く配布し、セキュリティ啓発活動のツールとして役立てます。
- 2003 年度・2004 年度に開催した地域については、各地の共催団体が引き続き「インターネット安全教室」を独自に開催することにより本活動を全国的かつ継続的に展開します。

【内容（約 120 分）】

CD-ROM（ビデオ）の上映	20 分
講師による解説	30 分
警察による講話	20 分
クイズ学習	20 分
質疑応答	10 分

インターネット安全教室・鹿児島
主催者挨拶：経済産業省　成田氏

【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


インターネット安全教室・山形　会場風景

■ 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	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	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 12 日（土） ※予定	山口県	山口県セキュリティマネジメントフォーラム（Y-sec）	未定
その他、広島県・京都府・三重県・山口県（宇部市）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	開催地区の市町村施設 (1) 武雄／杵島地区 (2) 佐賀地区 (3) 唐津地区 (4) 伊万里／有田地区 (5) 多久／小城地区 (6) 鹿島／藤津地区地区 (7) 鳥栖／三養基地区 (8) 神崎地区
6 月 11 日（土）	神奈川県	学校法人岩崎学園	学校法人岩崎学園
6 月 23 日（木）	福井県	ナレッジふくい	福井県生涯学習館
10 月 1 日（土）	神奈川県	秦野市、NPO 情報セキュリティフォーラム	秦野市本町公民館
10 月 7 日（金）	神奈川県	相模原市、NPO 情報セキュリティフォーラム	ウェルネスさがみはら
10 月 15 日（土）	神奈川県	茅ヶ崎市、NPO 情報セキュリティフォーラム	茅ヶ崎市役所分庁舎
	奈良県	なら情報セキュリティ研究会	奈良産業大学
10 月 18 日（火）	神奈川県	川崎市、NPO 情報セキュリティフォーラム	川崎市産業振興会館
10 月 22 日（土）	神奈川県	NPO 情報セキュリティフォーラム	学校法人岩崎学園
10 月 24 日（月）	神奈川県	大和市教育委員会、NPO 情報セキュリティフォーラム	大和市役所会議棟
10 月 31 日（月）	神奈川県	小田原市、NPO 情報セキュリティフォーラム	小田原市中央公民館
11 月 4 日（金）	神奈川県	男女共同参画センター横浜南	フォーラム南太田 ※女性限定参加になります
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）	山口県	山口県セキュリティマネジメントフォーラ（Y-sec）	徳山大学
11 月 24 日（木）	神奈川県	横須賀市、 横須賀市 IT 戦略会議 NPO 情報セキュリティフォーラム	横須賀市役所
11 月 26 日（土）	新潟県	NPO 新潟情報セキュリティ協会	新潟県生涯学習推進センター
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	
12 月 2 日（金）	神奈川県	藤沢市、NPO 情報セキュリティフォーラム	藤沢市役所新館
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 10 日（土）	神奈川県	松田町、NPO 情報セキュリティフォーラム	松田町町民文化センター
2 月 7 日（火）	神奈川県	秦野市、NPO 情報セキュリティフォーラム	秦野市役所
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、島根県・愛知県・北海道でも開催予定			

（2005 年 8 月 18 日現在）

「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

● Network Security Forum 2005

日時：2005 年 12 月 1 日（木）～ 2 日（金）
会場：大手町サンケイプラザ 3F
※事前登録制／聴講無料

～個人情報保護法と情報セキュリティ対策にフォーカスしたコンファレンス～

2005 年 4 月、個人情報保護法が施行されました。
企業は、個人情報の利用目的の特定や利用制限、情報漏洩防止など、安全管理のための必要な対策を義務づけられ、さらには違反者への罰則規定も盛り込まれました。
一方、コンピュータウイルスや不正アクセスの被害は日々増加し、企業全体のネットワークセキュリティ対策は、経営者のみならず私たちユーザーにとっても重要な課題と位置づけられています。

そうした情報資産に関する意識が益々高まる中、NSF2005 では、経営戦略面と技術管理面の双方に注力したコンファレンスプログラムと JNSA 会員企業による“IT 資産をいかにして守るか”という知識向上に主眼を置いたセッションを展開していきます。

詳細は JNSA ホームページでご確認下さい。
（http://www.jnsa.org/）

2. 協力イベントのお知らせ

1．2005 年 JESAP 電子署名認証フォーラム

会期：2005 年 8 月 31 日（水）～ 9 月 1 日（木）
主催：（財）日本情報処理開発協会電子商取引推進センター（JIPDEC/ECPC）
電子署名・認証利用パートナーシップ（JESAP）
日本 PKI フォーラム（PKI-J）
会場：東京ウィメンズプラザ
http://www.japanpkiforum.jp/jesap/

2．SCM フォーラム 2005

会期：2005 年 9 月 6 日（火）～ 7 日（水）
主催：社団法人日本ロジスティックスシステム協会
会場：シェーンバッハサボー
http://www.logistics.or.jp/

3．モノづくり総合展九州 2005 エネルギー・環境ビジネス総合展 2005 eビジネス 2005

会期：2005 年 9 月 7 日（水）～ 9 日（金）
主催：日刊工業新聞社
会場：福岡国際センター
http://www.nikkanseibu-eve.com

4．平成 17 年度 情報モラル啓発セミナー（島根）

会期：2005 年 9 月 16 日（金）
主催：中小企業庁
財団法人ハイパーネットワーク社会研究所
会場：くにびきメッセ
http://www.hyper.or.jp/moral2005/shimane/

5．第 6 回 ICCC (International Common Criteria Conference) 2005

会期：2005 年 9 月 28 日（水）～ 29 日（木）
主催：独立行政法人 情報処理推進機構（IPA）
会場：東京全日空ホテル
http://www.ipa.go.jp/event/iccc2005/index.html

6．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

会期：2005 年 10 月 6 日（木）～ 8 日（土）
主催：NPO 新潟情報セキュリティ協会（ANISec）
会場：湯沢町公民館　イナモト旅館
http://www.yuzawaonsen.gr.jp/conf/

7. 平成 17 年度 情報モラル啓発セミナー（岩手）
会期：2005 年 10 月 25 日（火）
主催：中小企業庁
　　財団法人ハイパーネットワーク社会研究所
会場：ホテルメトロポリタン盛岡
http://www.hyper.or.jp/moral2005/iwate/index.html

8. SCMソリューションフェア 2005
会期：2005 年 11 月 29 日（火）～ 30 日（水）
主催：社団法人日本ロジスティクスシステム協会
会場：東京ビッグサイト
http://www.logistics.or.jp/scm.html

9. Internet Week 2005
会期：2005 年 12 月 6 日（火）～ 9 日（金）
主催：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）
会場：パシフィコ横浜 会議センター
http://internetweek.jp/index.html

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：玉井節朗 氏 /IDG ジャパン）
　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 グループでは様々な団体、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、ゆくゆくは JNSA 版スパイウェア対策ポータルサイトの公開を予定。
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

【データストレージ&セキュリティWG】
(リーダー：立身俊雄 氏 / ディアイティ)

ストレージ導入時にセキュリティ対策を求められているケースが増加。技術的、運用を含めた事例を基にセキュリティ対策の勉強会を開催の予定。

【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 月にかけて全国約 20 ヵ所で「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する。

4. JNSA 役員一覧（2005 年 7 月 31 日現在）

会　長　石田　晴久
多摩美術大学教授・東京大学名誉教授
副会長　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）

在賀　良助	株式会社アイアイジェイテクノロジー
井上　陽一	株式会社ヒューコム
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
田中　辰夫	マカフィー株式会社
玉井　節朗	株式会社ＩＤＧジャパン
辻　久雄	ＮＴＴアドバンステクノロジ株式会社
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8月2日現在　197社　50音順）

【あ】

（株）アークン
ＲＳＡセキュリティ（株）
（株）アイアイジェイ テクノロジー
（株）アイ･ソリューションズ
（株）ＩＲＩコミュニケーションズ
（株）ＩＤＧジャパン
（株）ＩＴサービス
（株）アイ・ティ・フロンティア
（株）アイネス
アイネット･システムズ（株）
（株）ＩＰイノベーションズ
アイマトリックス（株）
（株）アクセンス・テクノロジー
（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）New
ウッドランド（株）
エー･アンド･アイ　システム（株）New
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）New
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）
京セラコミュニケーションシステム（株）
（株）ギガプライズ
（株）クインランド
クオリティ（株）
ＫＬａｂ（株）
（株）グローバルエース
グローバルセキュリティエキスパート（株）
クロス・ヘッド（株）
（株）クロスワープ
（株）コシダテック
（株）コネクタス
コンピュータ・アソシエイツ（株）
コンピューターサイエンス（株）

【さ】

サーフコントロール　ジャパン
サイバーソリューション（株）
サン電子（株）New
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 New

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

【た】

大興電子通信（株）
大日本印刷（株）
ダイヤモンドコンピューターサービス（株）
（株）タクマ
中央青山監査法人
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） New
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

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）New
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）New
（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）New
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）New
菱洋エレクトロ（株）
（株）ロボック

【特別会員】

特定非営利法人　アイタック
ジャパン　データ　ストレージ　フォーラム
電子商取引安全技術研究組合 New
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

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/Tokyo 2005 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 2005 Japan 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+Interop 2005 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-PRO 2005 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
9 月	9 月 7 ～ 9 日	モノづくり総合展九州 2005 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
12 月	12 月 1 ～ 2 日	Network Security Forum 2005 主催
	12 月 6 ～ 9 日	Internet Week 2005 共催

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

今年の夏は記録的猛暑だと言われ、連日連夜、熱帯夜が続きました。
暦の上でもすでに秋､みなさまいかがお過ごしでしょうか。
現在事務局ではすでに、2005 年度を締めくくる " 年末の 2 大イベント " へ向けて大奮闘中です。

12 月 1 日（木）～ 2 日（金）は JNSA 主催のネットワークセキュリティに特化したイベント、『Network Security Forum（NSF)』が、翌週 12/6 日（火）から 4 日間、連日開催される "Internet week2005" では、JPCERT/CC、Telecom-ISac Japan と一緒に、8 日（木）の 1 日に限り、『Security Day』と称する情報セキュリティに注力したセッションの開催が予定されています。

気になるセッション内容の方は、2005 年度を語るにふさわしいトピックスが揃い、" これを聞かずして 2005 年のネットワークセキュリティは語れない !"･･･というと少々オーバーなようですが、会員企業の皆様に楽しんでいただけるラインナップではないかと思います。

イベントに関する詳細とお申し込みについては会員企業の皆様へメールで配信予定のお知らせか、JNSA のホームページをご確認下さい。

会員企業の皆様からの、多数のご参加、心よりお待ち申し上げます。

（事務局）

JNSA Press vol.14

2005 年 8 月 31 日発行

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

NPO 日本ネットワークセキュリティ協会会員 行動指針

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

そのため、以下の通り会員の行動指針を定め、規範とするよう努めます。

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

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

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

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

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