JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
SPRING 2013 VOL. 35

寄稿

セキュリティを「面」で考えてみよう

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

「産学連携による情報セキュリティ人材育成」にむけて

東京大学 大学院 情報理工学系研究科 教授
産学情報セキュリティ人材育成検討会 座長
江崎　浩

情報通信技術は、グローバルスケールにかつユビキタスに普及し、すべての社会・産業活動を支えるミッションクリティカルな基盤技術としての役割を果たさなければならなくなりました。 その一方で、情報通信システムがすべての人に容易に、かつストレスなく簡単に利用できるようになったため、セキュリティを意識することなく、また、安全性への思慮が不足したままで、情報通信システムの研究開発や利用が増加し続けています。我々は、安全性を持った社会・産業基盤の提供を可能とするための研究開発やシステムの運用を実現するに資する人材の育成と確保を行うことが、次世代の社会への責任と認識しなければなりません。残念ながら、我が国の情報通信基盤の整備と発展を支えるべき人材の供給は、その質と量の両面において需要を大きく下回っている状況であると言わざるを得ない状況にあります。

この、我が国の社会・産業活動の継続と発展・成長に必須となる、セキュリティ人材の育成に、JNSAが貢献できることを検討し、実現することを目指して、平成２４年2月に、産業界および教育機関の有識者から構成される「産学情報セキュリティ人材育成検討会」を発足し、情報セキュリティ人材育成のための産学協同スキームを検討してきました。基本的には、官に頼らず、産学の連携・共同による継続性を持った活動です。さまざまの問題・課題を議論・整理し、JNSAが自身の力で実現・推進可能なこととして、まず、「JNSAインターンシップ」を起動することにしました。

JNSA産学情報セキュリティ人材育成検討会（以下、「検討会」という）が支援するインターンシップ（以下、「JNSAインターンシップ」という。）は、将来情報セキュリティ技術を活かして活躍したいと考えている学生に対して、情報セキュリティ業界の魅力を感じてもらえるような就労機会の提供を目的としています。JNSAは、本インターンシップを通じて業界の知名度を向上させ、セキュリティ業界を活性化させることを目指しています。情報セキュリティ業界の魅力を感じてもらえるような就労機会を提供するとともに、インターンシップを通じて業界の知名度を向上させ、セキュリティ業界を目指す学生を増やし、セキュリティ業界を活性化させ、ひいては、我が国の社会・産業へ貢献することを目指します。

JNSA会員各位のご理解とご高配、さらにご参画とご貢献をお願い申し上げます。

セキュリティを「面」で考えてみよう

アルテア・セキュリティ・コンサルティング代表
二木　真明

変化の見え方は視点によって変わる

昨今、サイバー攻撃の中身が変化してきていると言われています。以前は、興味本位とか自己顕示的な「実験」であったサイバー攻撃が「営利」など明白な目的を持った実用的なものに変化しているという意味で、ここ数年のトレンドとして語られることが多い話です。たしかに、IT という視点から見れば、その傾向は間違いがないように思います。でも、それは正しい表現なのでしょうか。

また、攻撃が、いわゆる IT 技術だけではなく、ソーシャルエンジニアリングなど、人間系を標的にしたものと組み合わされ、「ハイブリッド化」しているとも言われています。これも、実際に起きている事件を見れば明らかです。こうした傾向は、最近のこととして話題に上りがちですが、はたして本当に新しいものなのでしょうか。

ちょっと視点を変えてみましょう。まだ IT がそれほどクローズアップされる以前、インターネットもなかった時代に、たとえば企業から情報を盗んでいた産業スパイの手口を考えて見てください。同じように、パソコンもネットも使わないお年寄りからお金をだまし取る「振り込め詐欺」の手口を考えてみてください。こうしたスパイや詐欺の手口も、昔々から大きく変わっていません。昨今「ソーシャルエンジニアリング」と言われているものの多くが、こうした手口と同じものです。つまり、これらは IT 以前に「犯罪」の手口として、ずっと存在していたものなのです。こうした「犯罪」の歴史という視点から見ると、「変化」は違った形で見えます。つまり、古くからあった犯罪、つまり、ある動機があって、目的があり、それを達成する手段があるという流れの中の「手段」にあたる部分に IT が使われ出したという見方になります。

つまり、我々の視点ではサイバー攻撃の「動機」、「目的」の大きな変化に見えたものが、実は犯罪という視点から見れば、単に手段の変化に過ぎなかったということになります。どちらが、より広い見方であるかは自明でしょう。犯罪の手段には様々あり、その一つの要素である IT が最近では大きな比重を占めるようになってきた、ということなのです。

単純に、犯罪のレベルとそれに使われる IT のレベルを軸とした面を考えてみれば、図1のようになります。

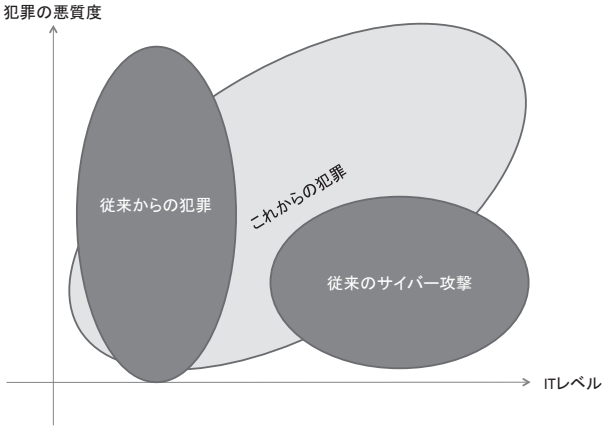


図 1

もちろん、これは犯罪だけではありません。戦争、テロ、過激な主張・抗議のための活動、いわゆるアクティビスムなどすべてにおいて同じことが言えるでしょう。最も身近な例は日常生活やビジネスなどです。これらも、IT を手段のひとつとして、どんどん変化しています。我々はついついセキュリティを中心に物事を見ようとしてしまいます。しかし、それが自分たちの視野をかなり狭めてしまっていることに気づいていなかったのかもしれません。IT ＋セキュリティとそれが手段になっている何かという、ふたつの軸を持つ面として全体をとらえてみると、これまで見えていなかった本質が見えてくることも少なくないのです。

ビジネス V.S IT V.S セキュリティ

ビジネスと IT、ビジネスとセキュリティ、IT とセキュリティの相関関係を同じように書いてみると面白い傾向が見えます。たとえば、IT 化はビジネスの効率を向上させますが、ビジネス効率に寄与する度合いの高い新技術ほど、安定性や安全性に問題がある傾向があります。これを図にしてみると図2のような形になるでしょう。

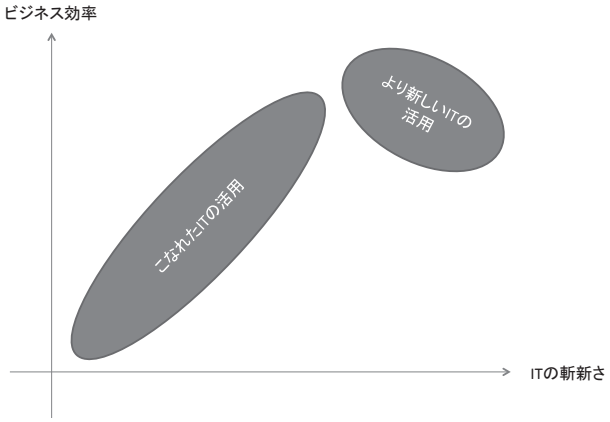


図 2

こうなる理由は、IT の斬新さとその安全性（安定性も含む）が、図3のような分布になってしまうからです。

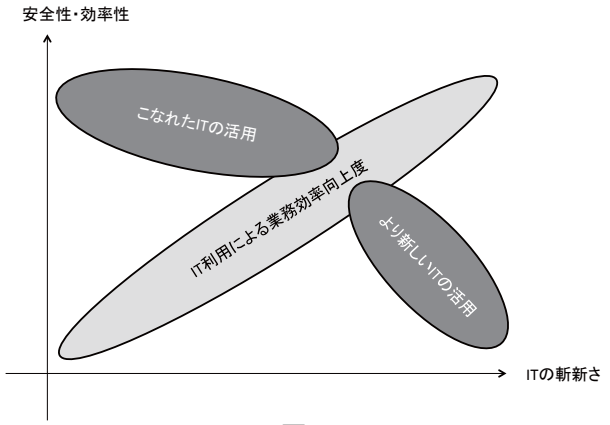


図 3

ビジネスの目的からすれば、可能な限り効率を上げるために IT を活用していきたいのですが、新しい技術にはリスクが伴います。つまり、図2のできるだけ右上に位置をとりたいのですが、図 3 の傾向があるため、より上に行こうとすると、逆にトラブルによって効率が下がってしまうリスクが大きくなってしまうわけです。

ここまで書けばもうおわかりでしょう。我々セキュリティに携わる関係者が何をすべきか、それは、図3の右下がりの傾きをできる限り小さくすることなのです。しかし、ともすれば我々は図3の右側のリスクの高い部分を使わないようにしようと考えてしまいがちです。極端な例を述べればノート PC の持ち出し禁止などがこれにあたります。これは、セキュリティからの偏った視点にほかなりません。ビジネスがセキュリティに求めていることとは本質的に違うのです。少なくともセキュリティのマネジメントに携わる人たちは、このことを決して忘れてはいけません。単に使うなと言うだけならば、こんな簡単なことはありません。いかに安全に使ってもらうか、そのために何をすべきかを一生懸命考えて実行するために給料をもらっている、セキュリティ部門のマネージャーはそう考えるべきなのです。また経営者はそれにみあった人材を正しい待遇をもって、そうした仕事に配置すべきなのです。決して、企業内のセキュリティ管理やリスク管理は「閑職」ではありません。もしそう考えている経営者がいるとしたら、会社の先行きは危ういと思うべきです。

情報技術（IT）V.S セキュリティ技術／IT 人材 V.S セキュリティ人材

昨今、情報セキュリティ人材の不足が叫ばれ、育成推進のかけ声高く、全国で CTF などが開催されています。では、「セキュリティ人材」とは、いったいどのような人材なのでしょうか。IT 人材全体のマッピングは ITSS などで細かく行われていますが、おおざっぱ

に見るならば、以下のようなものが上げられるでしょう。

・IT 企画やマネジメントにたずさわる人材
・IT 基盤技術者（ネットワーク）（設計、構築、運用・保守）
・IT 基盤技術者（サーバ・アプリ基盤）（設計、構築、運用・保守）
・アプリケーション技術者（設計、開発、構築、運用・保守）
・セキュリティ技術者（？？？？）

どうしてセキュリティ技術者の部分に？を入れたかというと、セキュリティのどの部分の仕事をするにしても、先に挙げたいずれかの知識や経験が必要になるからです。しかも、技術的に見れば、かなり高度な部類の知識や経験が必要になります。なぜなら、最先端のサイバー攻撃を考え出す連中は、こうした分野のトップクラスの技術者だと考えられるからです。必然的に、セキュリティ技術者も、レベルが上がるほど、それぞれの分野に分化していかざるを得ません。一方で、攻撃はあらゆる切り口から飛んできます。従って、どこから攻撃が行われているかを素早く判断して、適切な人材をディスパッチする役割も必要になるでしょう。こうした役割をになう人材は、幅広い技術全般にわたる一定レベルの知識とマネジメントスキルが必要になります。つまり、どれをとっても、「セキュリティ」という単独科目はないのです。むしろ、基本的なセキュリティの多くの部分は、IT の各分野に組み込まれています。つまり、本来ならば、その部分は「セキュリティ技術者」ではなく、その分野の「IT 技術者」がカバーすべき部分だと言えるのです。ここでも、セキュリティという単独の軸ではなく、IT という「面」でセキュリティをとらえると、問題の本質が見えてくるでしょう。強いて、セキュリティ技術者という名前をつけるならば、それは、IT 全般についてセキュリティがどうあるべきかを押さえられるジェネラリストか、もしくは特定の分野の技術の上に、そのセキュリティを極めたトップエンジニアに与えられる称号であるのかもしれません。これは極論かもしれませんが、それほどはずれた話ではないだろうと私は思っています。ゆえに、基本的なセキュリティ技術は、各分野の IT 技術に含まれる基礎科目として教えられていくべきものであって、それらと切り離されるべきものではないと考えます。

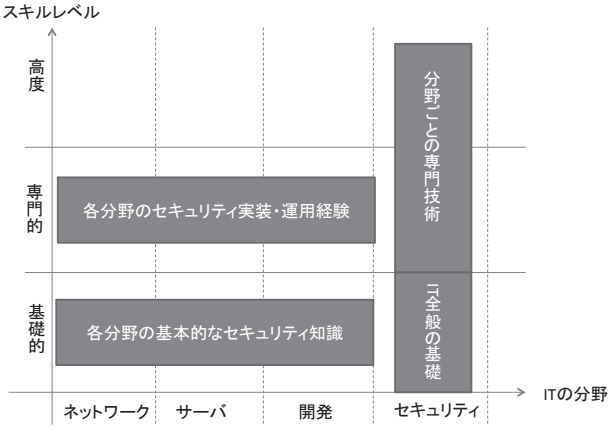


図 4

図 4 にそのイメージを示してみました。各分野の技術者には、基礎知識としての必要なセキュリティ技術と、その実装、運用の経験が求められます。たとえばネットワーク技術者ならば、ファイアウォールのポリシー実装や運用程度はできなくてはいけません。一方、セキュリティ技術者は、最低限、IT の全般的な基礎知識が求められます。その上に、セキュリティだけではなく、専門分野の知識が不可欠です。少なくとも、ネットワークセキュリティ技術者はネットワーク専門技術者と技術的な会話が出来る程度の知識がないと仕事になりません。こうした形でかみ合ってこそ、IT 分野にセキュリティが根付き、また、高度な相手に対して対抗できるセキュリティ専門家が活躍できる土俵ができるのです。

経験上申し上げれば、独学のみで育った中途半端なセキュリティ技術者ほど危ういものはないのです。きちんとした動機付けや倫理観の醸成が、セキュリティに携わるものにとってはきわめて重要です。CISSP のような国際的な資格取得時には、必ず職業倫理に関する宣誓書の提出が求められますし、ハッキ

ング技術などのセミナーを海外で受ける際にも同様の書面にサインを求められることが多々あります。そういう意味で、「とにかくCTF」というような昨今の風潮には大きな危惧を抱いています。

全国津々浦々から参加者を募って競技会を行い、トップレベルのチームを表彰することで、若者たちに与えられるモティベーションは、セキュリティを守ることではなく、単に勝って有名になることなのかもしれません。それでは、昨年、フィッシングサイトを作って補導された中学生の「目立ちたかった」という動機となにも変わらないのです。CTFの主催者は、こうした状況に陥らないように配慮する責任を負うのだということを忘れないでください。また、大量に技術者を育てたあげく、働く場所がないというような事態が生じれば、職にあぶれた技術者がダークサイドから誘惑を受ける可能性もあります。本当に今、それだけの技術者を育成して、働く場を提供できるのかどうかも、もう一度考える必要があります。

長年、JNSAも関わってきた育成イベントに「セキュリティキャンプ」があります。全国から応募してきた若者を書類で選考し、一堂に集めて集中的に高度なセキュリティ教育を行うのですが、そこでは技術のみならず、倫理観についての教育も必ず行われます。グループ活動を通じた一体感の醸成や、その中でセキュリティに関する正しい方向付けを行ってきました。また、キャンプ卒業生のコミュニティ育成にも力を入れ、彼らが孤立することがないように配慮し、さらに地方キャラバンなどを通じて、キャンプに直接参加できなかった若者たちへのフォローも行っています。残念ながら、予算、講師のキャパシティーなどの問題から限られた活動にとどまっていますが、卒業生にはセキュリティ分野で活躍している人も多く、着実に成果を上げてきたイベントと言えるでしょう。今回、このセキュリティキャンプの講師陣を中心に、新たなCTFイベント（SECCON）が進められています。JNSAでこのイベントを運営する意義は、単に優秀な若者を発掘するということではなく、地方大会に参加して敗れたチームをも含めて、その地域、地域にコミュニティ作りを進め、こうしたセキュリティに興味を持つ若者たちをダークサイドの誘惑から守っていくことにあるのだという点を強調しておきたいと思います。これも、CTFの優勝という「頂点」ではなく、裾野も含めて面として見ていくという考え方だろうと思います。

我々は、とかく物事をセキュリティ側から見ようとします。それを全否定するつもりはありませんが、時々は、セキュリティとそれが向かい合う別の何かをあわせて面で考えてみてください。きっと、新しいものが見えてくるだろうと思います。

JNSA ワーキンググループ紹介

組織で働く人間が引き起こす不正・事故対応 WG

WG リーダー　セコム株式会社　甘利　康文

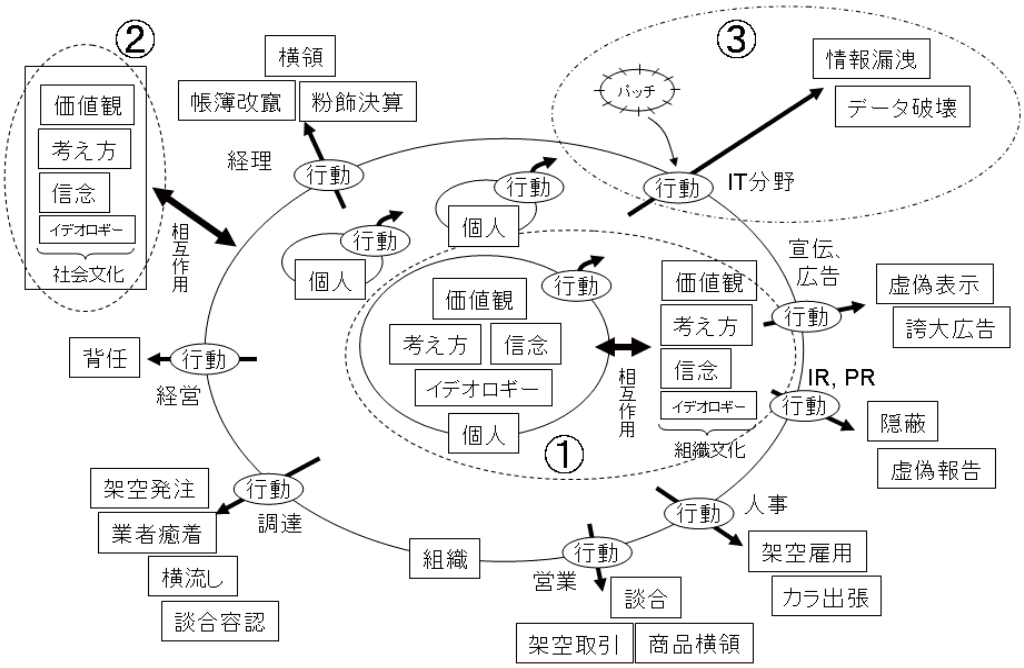
「組織で働く人間が引き起こす不正・事故対応 WG」は、JNSA の WG の中でも新しい（昨年 7 月発足）、そして少し変わった WG です。現在は、月に1回くらいのペースで集まり、勉強や、知見の共有を行っている段階です。今回はこの WG についての紹介をさせて頂きます。

これまで、多くの組織が、そこで働く人間のルール違反（不正）によって姿を消しています。エンロン、ワールドコム、アーサーアンダーセンなど、枚挙にいとまがありません。日本においても、組織で働く人間が引き起こす不正や事故がなんらかの原因となって、多くの組織が社会からの退場を余儀なくされています。このような背景もあり、「組織の内部統制」強化の必要性が指摘され、そのための法規やルールが作られてきています。

情報セキュリティ分野では、人による情報漏洩が話題になり、多くのベンダーから、技術的にその対策を行うソリューションが提供されています。この大きなトレンドも、もとをたどれば、組織の内部統制の強化が、社会的に求められ始めたことに、その源流の一つがあるのではないかと思います。

人による情報漏洩は重要な事故ですが、組織の内部に要因がある事故はそれだけとは言えません。その他にも、違法（脱法）行為、ルール違反に関係する事故としては、使い込み、内部窃盗、不正経理、取引先等との癒着、意図的不作為･隠蔽、組織の私物化（公私混同）などがあげられます。これらの事故は組織内部の問題として水面下で処理されることも少なくなく、社会的に顕在化することは多くありません。しかしながら、これらの事故が、組織や社会に及ぼす影響は決して無視できるものではありません。米国では、全

図 1「組織で働く人間が引き起こす不正」発生モデル



てのビジネスの約3割が、そこで働く人間のルール違反（不正）で立ち行かなくなるという調査もあります。組織で働く人間が引き起こす違法（脱法）行為、ルール違反への対応は、顕在化はしていないものの、社会的に具体的なソリューションが渇望されている分野ということです。

図1に本 WG の議論のために作成した「組織で働く人間が引き起こす不正」のモデルを示します。組織で働く人間の行動は、その人間の価値観や考え方が表出したものです。この個人の行動が、組織や社会にとって好ましくない形で顕在化したものが内部不正・事故になります。この行動が IT 分野において顕在化したものが、情報漏洩やデータ破壊などの情報セキュリティ関連の事故になります。一方、個人の行動が、組織や社会にとって好ましくない形で顕在化するのは IT 分野に限りません。情報漏洩やデータ破壊に対する対症療法（パッチ）的ソリューションは世にありますが、それだけでは内部不正・事故の根本対策にはなっていないのではという問題意識を表したものがこの図です。

一般に、組織が何らかの活動をすると様々な課題に直面します。これらの課題を解決する方法として「制度（組織、社会、ルール）」、「教育（人の啓発）」、「技術（システム）」の3つの方向性があるものと思います。「制度を作り、教育によって人を変え、技術で駄目押し」という形です。本 WG では、

① 人の意識や組織文化、
② 組織の行動が影響を受ける社会文化や規範、
③ 不正を防ぐシステム、

の3方向から「組織で働く人間が引き起こす不正･事故」に対する考察を深め、ソリューションの提言、提案を行うことをゴールとして見据えています。

そもそもの「セキュリティ」という言葉には、いわゆる「情報セキュリティ」をこえる幅広い概念が包含されています。本 WG では、セキュリティを「組織のオペレーションが、きちんと回っている状態」を指すものと広く捉え、組織で働く人間の、これに悪影響を及ぼす行為について考えて、その根本要因に働きかけることを考えています。いわゆる「情報セキュリティ」をスコープとする JNSA においては、異色の WG なのではないかと思います。

組織で働く人間が引き起こす不正・事故対応 WG メンバーリスト

氏　名	社　名
リーダー 甘利　康文	セコム株式会社 IS 研究所
田中　洋	株式会社インフォセック
野崎　真樹	株式会社インフォセック
佐佐木　賢二	グローバルセキュリティエキスパート株式会社
芳賀　政伸	グローバルセキュリティエキスパート株式会社
宮崎　亮	株式会社 JMC
新井　真司	セコム株式会社 IS 研究所
内田　順一	セコム株式会社 IS 研究所
松本　泰	セコム株式会社 IS 研究所
山田　英史	株式会社ディアイティ
遠藤　美貴恵	ドコモ・システムズ株式会社
藤原　隆徳	ドコモ・システムズ株式会社
粟津　朱実	トレンドマイクロ株式会社
岡本　勝之	トレンドマイクロ株式会社
小原　哲也	トレンドマイクロ株式会社
小屋　晋吾	トレンドマイクロ株式会社
林　憲明	トレンドマイクロ株式会社
北野　晴人	日本オラクル株式会社
塚田　孝則	株式会社日立ソリューションズ
小川　博久	みずほ情報総研株式会社
村上　晃	株式会社ラック

オブザーバー

島　成佳	独立行政法人情報処理推進機構 技術本部セキュリティセンター
高橋　潤	(株)リンク アンド モチベーション モチベーションマネジメントカンパニー

会員企業ご紹介35

セコムトラストシステムズ株式会社

http://www.secom-sts.co.jp/

セコムグループの情報・ネットワークシステムの構築・運用を担うと共に、そこで培った技術力と運用力、ノウハウを生かして、先進的なサービスの創造に取り組んでいます。

セコムのセキュリティ事業のノウハウを生かした「事業継続支援業務」をベースに、情報セキュリティ事業と大規模災害対策事業を主力に展開しています。セコムが誇るセキュリティと最新技術の粋を結集した"セキュアデータセンター"を基盤に、"高い技術力"と"24時間365日の有人対応"を融合した、独自の『機能レンタルサービス（セコムクラウド）』によって、様々なニーズにきめ細やかに対応することによりお客様のビジネス価値創出に貢献しています。

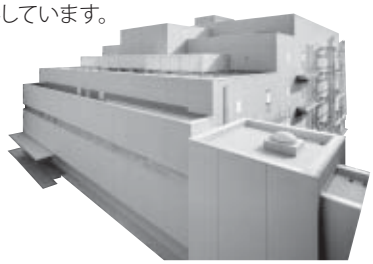
事業継続支援をベースに緊密に連携した高品質なサービス

セコムトラストシステムズの主力の情報セキュリティ事業と大規模災害対策事業は、セコムのセキュリティ事業のノウハウを生かした「事業継続支援業務」をベースに展開しており、それぞれが緊密に連携し高品質なサービスを提供しています。

その中で、情報セキュリティ事業では、

- ●システムの脆弱性を洗い出すセキュリティ診断サービス
- ●不正アクセスやウイルス感染がないか24時間365日有人によるシステム監視サービス
- ●ホームページの実在証明と暗号化通信（SSL）機能と端末や本人確認する電子認証サービス
- ●パソコンやサーバからの情報流失を防ぐ各種の情報漏洩対策サービス

などの提供により、お客様の重要な情報資産のセキュリティ対策をトータルにサポートします。



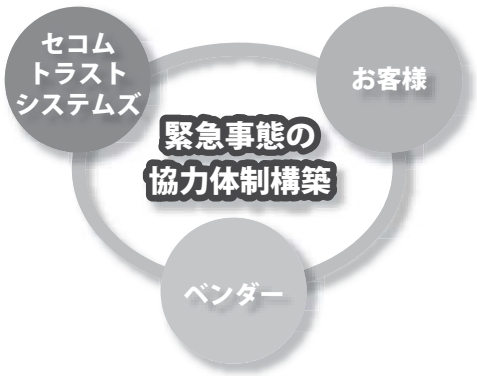
困った時の「セコムプロフェッショナルサポート」

セコムトラストシステムズでは、従来のインターネットの入り口対策だけでは防げない未知のウイルスを使った新しいタイプの標的型攻撃に対し、情報の「出口」対策を徹底することで、【機密情報】などの外部漏洩を防止する「セコム・サイバー攻撃対策サービス」の提供を開始し、お客様から有効な対策として高い評価をいただいております。しかし、これらの攻撃に対して100%の防御は難しいのが現状です。

万一ウイルスや不正アクセスの被害を受けた場合、豊富な経験を持つ「ITのプロ」「セキュリティのプロ」が現地に駆けつける「セコムプロフェッショナルサポート」は、初動対応から復旧までを支援することにより、被害を最小限に抑え早期の業務再開をサポートします。

「インターネットにつながり難い」「妙なアイコンや不可解なメッセージが出る」「各種データが参照不可」などの現象が出たら、セコムトラストシステムズにご一報をください。専門スタッフが現地に駆け付け対応いたします。

このように、セコムトラストシステムズは、先進的なサービスの創造に挑戦し続けることにより、安全・安心・便利・快適な社会を実現し、「困った時はセコム!」と頼りにされる存在になることを目指しています。



セキュリティのプロにお任せください
～「セコムプロフェッショナルサポート」提供内容～

現状把握	安全対策
●被害拡大防止の初期対策 ●影響範囲の確認 ●感染状況の把握 ●各種ログの調査	●ネットワーク上の通信データの確認 ●サーバ稼動状況の確認 ●再開のための残存リスクの確認
対策の立案	**業務再開と再発防止策**
●対策本部の設置 ●再開に向けての対策方針の立案 ●関係ベンダーへの協力要請	●業務再開テストの立ち会い ●残存リスクの再確認 ●再発防止策の立案

JNSA 会員企業のサービス・製品・イベント情報です。

■製品情報■

○鍵管理ソリューション
「Universal SSH Key Manager」

ITシステムで使用するSSHの鍵が可視化されていない企業・組織ではサイバーアタックに対して大きなITリスクをかかえることとなります。但し可視化に当たっては大きな管理コストが必要となります。本製品はOPEN SSH 及び商用SSHの公開鍵、秘密鍵を自動的に管理、制御することで、管理コストとITエンジニアの負荷を大幅に軽減します。不正アクセスリスクの排除と確実なコンプライアンスの遵守を実現します。

【製品情報詳細】
http://www.dit.co.jp/products/ssh_tectia_series/uskm.html

◆お問い合わせ先◆
株式会社ディアイティ
ネットワークセキュリティー事業部
セキュリティソリューション部
TEL：03-5634-7652
E-Mail：info@dit.co.jp

■サービス情報■

○CSIRT構築支援サービス

コンピュータセキュリティにかかるインシデント対応や関連情報、脆弱性情報、攻撃予兆情報などの収集や分析、対応方針や手順の策定などの活動を行うCSIRT(Computer Security Incident Response Team)に関して、企画、構築、運用までの一連のプロセス、外部CSIRTとの連携までを総合的に支援いたします。

【サービス情報詳細】
http://www.mbsd.jp/services/consulting/security_consulting_csirt.html

◆お問い合わせ先◆
三井物産セキュアディレクション株式会社
エンタープライズ営業部
TEL：03-5649-1981
E-Mail：Sales-info@mbsd.jp

○ボットネットチェックサービス

ボットネットチェックサービスは、リアルタイムスキャンによってWebを経由するあらゆる種類のマルウェアやそれにより感染したボットネットを検知する機能を備えた「Symantec Web Gateway」を活用し、感染有無を可視化する低コストなクラウドサービスです。本サービスは製品の設置、正常稼働監視、ログ収集と保管・解析、レポート作成まで一括して当社MBSDが運用いたします。

【サービス情報詳細】
http://www.mbsd.jp/

◆お問い合わせ先◆
三井物産セキュアディレクション株式会社
エンタープライズ営業部
TEL：03-5649-1981
E-Mail：Sales-info@mbsd.jp

NSF 2012 in Kansai

JNSA 西日本支部 企画運営 WG
齋藤　聖悟

JNSA 西日本支部では西日本地域のセキュリティレベルの向上を目的として NSF 2012 in Kansai を下記の要領で開催しました。

日　時 : 2012 年 10 月 24 日（水）13 時 00 分～ 17 時 45 分
会　場 : 新梅田研修センター
主　催 : NPO 日本ネットワークセキュリティ協会 西日本支部
定　員 : 200 名
概　要 : BYOD で持ち込まれた機器をどうすれば安全に利活用できるかについて考える
料　金 : 無料

スマートフォンの普及が進む環境においてクローズアップされてきたBYOD（Bring Your Own Device、個人所有デバイスの会社への持ち込み）ですが、どの様な情報セキュリティ対策を講じるかについてはまだまだ手探りな状態であり、どの企業でも試行錯誤しているかと思いわれます。そこで2012年度のNSF 2012 in Kansaiではテーマを「中小企業だからこそBYODを考えてみる」と題し、持込を単純に禁止するのではなくどうやって有効活用すべきかを考えることを目的として開催しました。

■ 開会挨拶

近畿経済産業局地域経済部 情報政策課 山口洋課長が、ITは非常に有用なツールだが重要情報を不正に取得する標的型攻撃なども起きており、それら負の側面を回避しつつITの利点を有効活用することが重要であるとお話され、そのために近畿経済産業局としてはJNSAと協力し合って情報交換を行い、啓発活動を行っていきたいとのお話を頂きました。

続いて西日本支部の井上支部長より本セミナーの位置づけとJNSAおよび西日本支部の活動状況の紹介がありました。

開会挨拶　山口洋氏

■ 基調講演

国立大学法人名古屋大学情報基盤センター 高倉弘喜教授より「凶悪化するサーバ攻撃の実態とその被害緩和手法」と題して、公開事例が少ない標的型攻撃の概要や被害を緩和するための対策設計について解説を頂きました。

冒頭では、マルウェアが2.5秒ごとに生成されるため、検体収集が追いつかず、解析も間に合わなくなっていることから、アンチウィルスの検知パターンが限界に来ていること、APT対策を謳っているものの多くは境界制御の延長線上やコンプライアンス系であり、APT対策とマルウェア対策はまた違うものとの解説に加えて、それら現状の整理をされた後に実際の事例を踏まえた標的型攻撃の説明を頂きました。侵入された後の組織内部での活動状況や、そこから情報をどうやって送信するか、証拠の隠滅方法までと詳細な内容であり、IPv6やスマートフォンを悪用した事例や組み込み機器の脆弱性の解説から、攻撃手法も日々進化しているとの印象を強く受けました。

後半ではそれらの事例を踏まえて、新たなセキュリティ対策について触れ、これまでのような怪しいファイルを開かないなどの対策は現実的には難しく、侵入されても情報を持ち出されないようにするなど守り方を変える必要があるとご指摘を頂き、対策の見直しとしてログの取得方法についても言及がありました。ログは日々増え続けかつ改ざんされる可能性があるため、VLANやSSIDの設定を適切に行い調査すべきログを減らし、早期発見に努める必要があるため、ログの定期検査を実施していくべきと提言していただきました。

最後にBYOD賛成だが製品のライフサイクルが短く、OSのサポートが追いつかないため、何処まで古い機器の利用を認めるかについて言及がありました。セキュリティを考慮しシステム購入時にライフサイクルをあらかじめ組み込んでおく必要性に触れられました。中小企業でも使用期限や保守を考えてシステムを導入していく必要があるとまとめて頂きました。

■ パネルディスカッション

「ちゃんと」、BYODを考えてみるというテーマで、株式会社KDDI研究所 竹森敬祐氏、日本マイクロソフト株式会社 香山哲司氏、株式会社神戸デジタル・ラボ 近藤伸明氏をパネリストとして迎え、富士通関西中部ネットテック株式会社 嶋倉文裕氏にモデレータを務めて頂きました。

冒頭では神戸デジタル・ラボと日本マイクロソフトそれぞれの社内環境、業務環境での業務の進め方や持ち込み端末の使い方などについて事例を交え、解説頂きました。その中でも印象深かったのは、「ブラックリスト（使用させない機能）だとどうしても抜け道を考えてしまうためホワイトリスト（許可する機能）によって管理している」という香山氏のお話でした。

続いて竹森氏からは、BYOD端末としてスマートフォンを前提とした安全性に関する技術解説を頂きました。個人が所有する端末のOSや機種は多種多様であるため技術的対策は非常に難しく、初期状態で安全なOSに制限する視点はOKだが個人所有デバイスへのインストール制限はやりすぎであるとのお話がありました。そして、社内規程で個人端末でも実施可能な対策、例えばルート化の禁止、ジェイルブレイクの禁止、リモートロックの実施程度なら可能であり、その上で企業所有デバイスだけMDMで管理する、などの提言を頂きました。また実際にBYODを運用するうえでUSB

バックアップ機能は使用しない、企業ネットワークではテザリングを使用させないなど具体的な部分にも触れて頂きました。

最後に具体的な対策に向けて「リスクと向き合いバランスの取れた対策のポイントは?」というテーマでは、竹森氏からは勝手に設置されているAPを探し出して停止させることや、法人契約のMDMなど運用の話や社員へお願いするべきことなどの対策が紹介され、近藤氏と香山氏からはスマートフォンで使用できる社内システムはWebのみに制限している運用状況から、Webで使用できるシステムかどうかで線引きするのも有効との提言を頂きました。

■ JNSA 拡大勉強会

JNSA西日本支部では定期的に情報セキュリティ勉強会を開催しており、本セミナーではその拡大版となる新たな試みとしてスマートフォンの「セキュリティ」ではなくスマートフォンの「新しい使い方」を知ることを目的として企画しました。

これまで開催してきた勉強会ではある程度対策が成熟した情報セキュリティを取り上げてきましたが、スマートフォンは、使用方法が多種多様で技術進歩が早く、対策が追いつかなくなる現状にあります。そこで、「対策」部分の勉強会ではなく技術や使い方そのものを勉強して対策のきっかけを作ることを目的としました。

前半はNHN Japan株式会社 増村洋二氏に「スマートフォンアプリ提供事業者におけるBYOD制度」と題して講演頂きました。LINEに代表されるスマートフォンアプリを作成する企業として、社内にはスマートフォンの購入には補助があり、積極的に使用させている一方で社内規程ではセグメント別ポリシーを整備し、ビジネスの成長を止めないセキュリティ対策を実施しているとの紹介を頂きました。

後半はPayPal Pte. Ltd. 井尾慎之介氏より「PayPal Here (tm)、スマートフォンの新たな可能性」と題して講演頂きました。PayPalでは誰でも使用できる決済システムとしてiPhone向けにPayPal Hereをリリースしており、その解説とデモを実施して頂き、私物のスマートフォンでも決済データが残らず、安全に使えるとのことでした。また、デバイスやアプリケーションのセキュリティ面でポイントとなるのはアカウントの管理であると補足頂きました。

■ NSF 2012 in Kansai のまとめ

本セミナーの締めくくりとして、高倉氏と嶋倉氏と筆者にて振り返りを行いました。

■ NSF2012in Kansai を終えて

当日は昨年とほぼ同じ130人の方にご参加頂きました。

アンケートではセミナーに参加した感想として回答者の99%が「大変有益だった・有益だった」と回答しており、情報セキュリティセミナーとしては成功したと思います。各セッションでは基調講演とパネルディスカッションについては「大変有益だった・有益だった」が98%でした。拡大勉強会では「大変有益だった・有益だった」が約6割となっています。これはある程度予想していた結果ではありますが、セッションの位置づけをしっかりと解説するなど次年度以降改善の余地がある部分です。

今年度も昨年同様に企業ブースを併設し、相談コーナーも設けると共に、西日本支部メンバーによる「出社してから退社するまで」ソリューションマップを配布しました。

これからも多くの方に参加いただける機会を作りまた関西圏のセキュリティレベル向上のためJNSA西日本支部としてセミナー・勉強会を継続していきますのでご期待ください。

PKI day 2012
「我が国における信頼基盤の連携に向けて」
「PKIへの攻撃とその対応」

セコム株式会社　IS 研究所
松本　泰・島岡　政基

今年度のJNSA PKI相互運用技術WGが主催するPKI day 2012は、2012年12月13日に100名弱の参加者のもと開催されました。会場の参加者のほか、PKI dayでは、昨年同様、Ustreamによるライブ中継を行い、会場外から参加する方もいらっしゃいました。

毎年、恒例となっているPKI dayですが、ここ数年は、PKIの社会基盤的な側面から、その役割と課題をテーマとして取り上げてきました。PKI day 2012でも、こうした社会基盤としてのTRUSTのあるべき姿をイメージし、午前と午後でふたつのテーマ（午前の部「我が国における信頼基盤の連携に向けて」、午後の部　「PKIへの攻撃とその対応」）で講演とパネルディスカッションを行い、それぞれ密度の濃い議論が展開されました。

午前の部

我が国における信頼基盤の連携に向けて

午前の部の「我が国における信頼基盤の連携に向けて」は、以下のようなテーマ設定を行いました。

> PKIは現在、様々な情報通信基盤の信頼の要として利用されています。例えば、インターネット上の通信におけるTLS/SSLや、電子政府の電子申請等で利用される電子署名法に準拠した証明書による電子署名、e文書法等で要求される時刻証明のためのタイムスタンプ等があります。我が国において、これらのPKIは、それぞれ別々の目的や成り立ちがあり、現在は、似て非なるフレームワークで、構築、運用されています。しかし、今後は様々な分野において情報連携が求められており、この情報連携を実現するうえで整合性の取れた信頼基盤構築のフレームワークが重要になると考え、そのため、これらのPKIにおいても制度的に整合性をもったフレームワーク作りが望まれます。
>
> 本セッションでは、PKIに関連した団体の活動を紹介すると共に、パネルディスカションでは日本社会における信頼基盤の連携を確立するため、各団体でどのような連携を図っていくか議論します。

講演者と講演、およびパネルディスカッションの登壇者は、以下のとおりです。

【講演】「我が国における信頼基盤の連携に向けて」
講師：セコム株式会社 IS研究所　松本　泰 氏

【講演】「電子認証局会議の活動」
講師：日本電子認証株式会社　高橋　章 氏

【講演】「タイムビジネス協議会の活動」
講師：アマノビジネスソリューションズ株式会社　市川 桂介 氏

【講演】「電子記録応用基盤フォーラム（eRAP）の活動」
講師：三菱電機株式会社　宮崎 一哉 氏

【パネルディスカッション】
＜モデレータ＞
セコム株式会社 IS研究所／
PKI相互運用技術WGリーダー　松本　泰 氏
＜パネリスト＞
高橋　章 氏　日本電子認証株式会社
市川 桂介 氏　アマノビジネスソリューションズ株式会社
宮崎 一哉 氏　三菱電機株式会社
秋山 卓司 氏　クロストラスト株式会社
宮内　宏 氏　宮内宏法律事務所

講演、およびパネルディスカッションの講演資料と動画のアーカイブが公開されていることもありますので、ここでは、パネルディスカッションでの議論の背景をもう少し補足して説明します。

PKI相互運用技術WGは、元々、WGの名前のとおりPKIの相互運用技術に注目した活動でした。繋がる事だけを目的とした「相互運用技術」とは違い、セキュリティ技術、暗号技術、更には信頼（TRUST）の形成まで目的とした「相互運用技術」は、別次元の難しさがあります。しかし、TRUSTに係わる「相互運用技術」に取り組む程に、「相互運用技術」では解決できないポリシーの不整合等の問題に突き当たるということが

ありました。これは、簡単に表現することが難しいのですが、IT社会における信頼（TRUST）であっても、社会基盤に組み込まれるほどに、既存の制度、慣習との整合が求められます。しかし、元々「紙文書」を前提に構築されてきた既存の社会の仕組み（TRUSTの仕組み）は、「デジタル」な技術を前提としたIT社会の信頼（TRUST）には適合しにくい面があります。そこで、従来の制度の延長線上だけではない新たな枠組みが必要になります。これらの課題をうまく表現した「絵」が三菱電機の宮崎氏の発表資料（図1）にあります。

このパネルディスカッションでの「密度の濃い議論」は、短い紙面では書ききれません。「密度の濃い議論」に関しては、公開されている講演資料及び動画のアーカイブを参照して頂ければ幸いです。

午後の部

PKI への攻撃とその対応

午後の部の「PKIへの攻撃とその対応」は、以下のようなテーマ設定を行いました。

近年、PKIへの攻撃が顕著になっています。例えば、以下の事例があります。

- 2011年3月Comodo事件：9件の証明書が不正発行
- 2011年8月DigiNotar事件：500以上の証明書が不正発行
- 2012年5月に発覚したFlame Malware

これらの事例では、不正な証明書発行やX.509証明書の偽造等、PKIへの攻撃が行われています。こうして

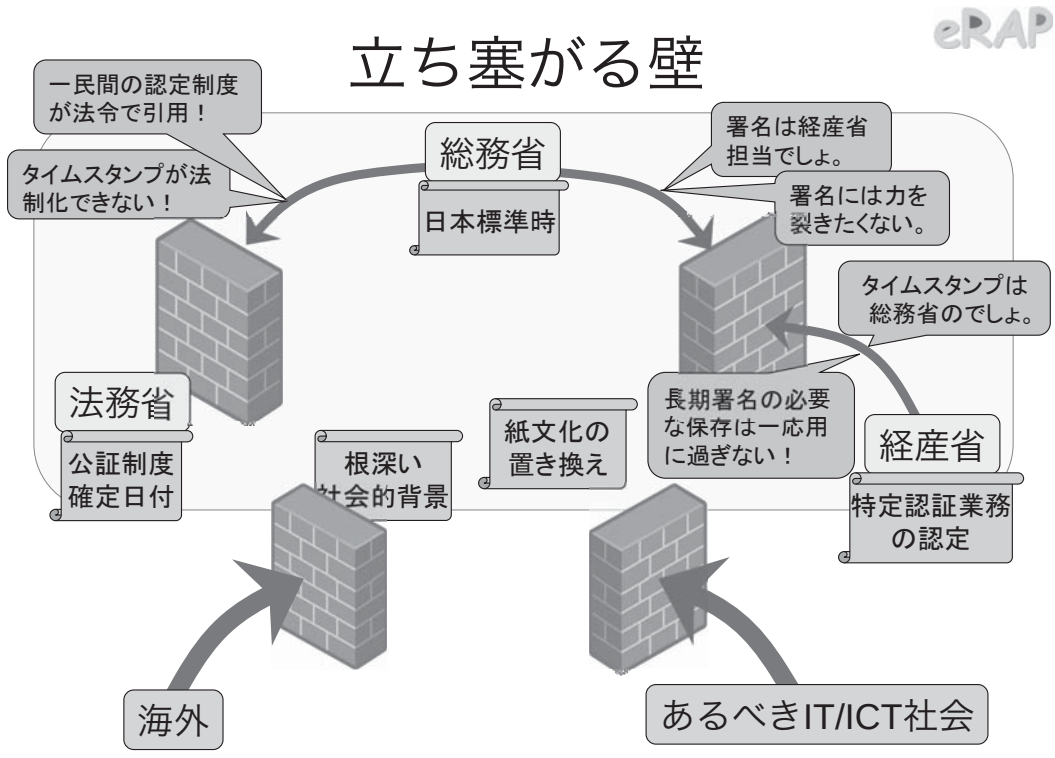


図 1 「立ち塞がる壁」
三菱電機 宮崎氏　講演資料より抜粋

不正に取得された証明書は、Flameで見られるように複雑で高度な攻撃を行うために使われています。これらの事例はたまたま発覚されたに過ぎず、水面下ではもっと多くの攻撃が準備されている可能性もあります。

また、SSL/TLS、SSHなどのセキュリティプロトコルで利用されている証明書を広く収集して様々な分析が行われています。2012年8月にはUSENIX Security SymposiumおよびCRYPTOにて収集された公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題が指摘されました。この問題は正しく鍵生成を行っていないことに起因し、もちろん攻撃の糸口に利用される可能性があります。

PKIが攻撃されるのは、現在の世の中において、PKIの仕組みが、世の中の信頼の起点として組み込まれていることに他なりません。PKIは、情報化社会の基盤技術ですが、このPKIを代替する技術は考えられず、今後の社会においても信頼の起点であり続ける必要があります。そのためには今後の攻撃に耐えうる技術・運用方法を確立する必要があります。

本セッションでは、

- これらの事件の内容を、その背景も含め正確に理解し
- 今後の考えられる攻撃を考察し
- 今後の中長期的な対策

について議論します。

講演者と講演、およびパネルディスカッションの登壇者は、以下のとおりです。

【講演】「サイバー攻撃ツールとしての公開鍵証明書の役割～信頼の起点にカモフラージュされた攻撃の起点～」

講師：(独) 情報処理推進機構 セキュリティセンター 暗号グループ 研究員　神田 雅透 氏

【講演】「公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題～いつのまにか他人と秘密鍵を共有してませんか？～」

講師：株式会社インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア 須賀 祐治 氏

【パネルディスカッション】

＜モデレータ＞

株式会社インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア 須賀 祐治 氏

＜パネリスト＞

神田 雅透 氏　(独) 情報処理推進機構 セキュリティセンター 暗号グループ　研究員

島岡 政基 氏 セコム株式会社　IS研究所

高橋 正和 氏 日本マイクロソフト株式会社 チーフセキュリティアドバイザー

佐藤 直之 氏 日本ベリサイン株式会社　主席研究員

■ 講演の概要

午後のセッションは、はじめにIPA神田氏から概略として最近の認証局に対する一連の攻撃について解説が行われました。

攻撃の対象となっているのはもっぱらトラストアンカとなるルート認証局であり、これらトラストアンカは様々なアプリケーションに予め組み込まれるものであるために、これを攻撃されるとユーザは何ら気づくことなく騙され続けてしまいます。

現在、PKIが攻撃されるケースは、大きく3つの要因に分類されます。一点目は認証局へのハッキング、二点目は暗号技術に対する攻撃、三点目は運用の問題です。三点目については次のセッションでIIJ須賀氏が解説されるため、神田氏からは前者二点について説明されました。

認証局へのハッキングは、ComodoおよびDigiNotar事件が知られています。特に後者のDigiNotar事件は、少なくとも531枚以上という大量の不正な証明書発行が行われ、実際にイランで不正な証明書を悪用した盗聴行為が行われた可能性が高く、最終的にこの

事件の影響によりDigiNotar社が1998年からの歴史に幕を閉じることになった（つまり倒産した）、という点で認証局業界にとってインパクトの高い事件でした。

これまでは、不正発行された証明書を悪用するためには、DNSサーバを改ざんするか、いわゆる中間者攻撃（Man-in-the-middle）を行う必要があり、不正発行だけで実害を発生させることは難しいとされてきたわけですが、DigiNotar事件では、これがいとも簡単に覆されてしまいました。このように証明書の不正発行とDNSサーバの改ざんといった複数の攻撃が同時に成立した背景には、大規模な組織的支援つまり政府機関の関与があったのではないかと推測されています。続いて暗号技術に対する攻撃事例としてFlame事件の解説が行われました。これもやはり政府機関の関与が指摘されていますが、特徴的なのはやはり暗号アルゴリズムに対する攻撃を成功させた点であり、従来の想定を覆す計算能力と解読技術を有する攻撃者の存在を知らしめたことでしょう。このように、認証局に対する攻撃は年々本格化しており、政府レベルの関与や世界トップレベルの暗号解読能力にもとづく攻撃が行われる可能性を無視できなくなりつつあることが再認識されました。

午後二本目のセッションは、IIJ須賀氏から公開鍵使いまわし問題について解説が行われました。本問題は、2012年8月に複数の暗号研究者からほぼ同時期に発表されたもので、インターネット上に存在するSSL/TLSやSSHなどの公開鍵（それぞれ約1,000万件以上）を収集・分析した結果、いずれも6割以上という多くのノードで私有鍵（又は秘密情報の一部）が重複していることを指摘したものです。こうした私有鍵の重複は一概に危険であるとは言えず、例えば負荷分散のための冗長構成で同じ鍵を利用しているケースなどもあると推測されます。しかしながら、機器出荷時の初期鍵をそのまま利用しているケースが5%以上(67万件以上)のホストで確認されており、これらについては盗聴やなりすましの危険性が懸念されています。

典型的な公開鍵暗号であるRSAは、二つの巨大な素数p, qを用いて構成されますが、この二つの素数のうちいずれかを他のユーザが用いていれば、公開鍵から私有鍵を解読するのは容易になります。これらの素数は、擬似乱数生成(PRNG)モジュールによって鍵ペア生成時にランダムに選択されますが、ここで十分な乱雑性が確保されなければ、pまたはqの重複や最悪の場合は鍵ペアそのものの重複が生じます。

この乱雑性は暗号アルゴリズムと無関係に実装に大きく依存しており、例えば某社の実装ではわずか9個の乱数即ち36通り(9C2)の公開鍵しか生成することができなかったことが明らかになっています。これは極端な例ですが、いずれにしてもこうした実装が増えることで「重複しやすい素数」が増えることになり、その素数を用いた「解読しやすい公開鍵」も増えることになります。つまり、RSA暗号の安全性は2つの巨大な素数を衝突することなく選択することに依存していたわけですが、その前提が機能しない場面が見受けられるようになりました。この安全性低下はRSA暗号だけの問題ではなく、例えばDSAも署名時にPRNGを用いて乱数を生成しますが、その乱数が重複していれば私有鍵を容易に解読できてしまうため、やはりRSAと同様に安全性が低下しつつあることが指摘されています。

こうした問題が生じる背景には、多くの暗号アルゴリズムが乱数生成において十分な乱雑性を期待しているのに対して、実装側がその重要性を理解できないままPRNGを実装・使用してしまっていること、また近年増加が著しいアプライアンスも含めた組込み機器にお

いては十分な乱雑性の確保と性能の両立が難しい上に、パッチなどの適用が難しいという問題があるのではないでしょうか。

■ パネルディスカッションの概要

最後に、こうした公開鍵暗号にまつわる様々な攻撃方法が顕在化していく状況を踏まえて、これらの事件・事故の全体像を正しく理解し、今後の対策や提案・提言を検討していくためにはどうしたらよいかというパネルディスカッションが行われました。このパネルに限っては、リアルタイムに可能な限り自由な意見交換を妨げないようにするため、Ustream中継およびTwitterによるtsudaりも禁止という条件で行われました。

パネルでは、最初にマイクロソフトの高橋氏から、昨年10月のWindows UpdateによってRSA1024bit未満の証明書は自動的に使えなくしたこと、これによるお客様対応の事例などについて説明が行われました。次に日本ベリサインの佐藤氏から、DigiNotar認証局事件について昨年末に公開された報告書をもとに解説が行われました。その後セコムIS研究所の島岡氏から、こうしたPKIへの攻撃に対する中長期的な対応の提言とともに、信頼の基盤としてPKIを維持していくことの重要性について説明が行われました。

こうした説明を受けた後のディスカッションでは、PKI業界はこれまであまり攻撃対象として注目されていなかったために対策も甘かったが、今後本格的な攻撃対象となってくるのは明らかなのでより厳格な対策が求められる、特に証明書はコスト構造が利用者から見えにくい面もあるので、コストの割に脆弱と指摘されかねない、など厳しい意見が相次ぎました。

こうした指摘に応えるために、例えばCAブラウザフォーラムでは脆弱性対策に対する要件を明確化してWebTrust for CAの認定要件に追加する動きがあることが報告されるとともに、一方で現状の認証局監査は認定の有無しかわからず、例えば鍵管理や脆弱性対策などの評価項目に対して各認証局がどの程度の水準にあるのかわかるようにしてはどうか、といった監査の透明性を求める意見も出ました。

PKI限界説や、PKIに代わる新しい信頼の基盤が成功する可能性はあるか、といった議論もされましたが、既存の様々な仕組みがサーバ認証やコード署名というPKI特有の技術に依存している現状を考えると切り替えは容易ではないこと、さらに信頼の基盤となるには信頼の起点となるトラストアンカを配布・普及させる必要があり、これは昔よりも組込み機器が多く普及した現在の方が遥かに難しく時間のかかる問題であり、これからも社会はPKIに依存せざるを得ない。つまりPKIの信頼を確保し続けるためにとにかく努力し続ける必要があるという話まで進んだところで残念ながら時間切れとなってしまいました。

■ おわりに

今回のPKI dayは、ここ数年のPKI day と同じくPKIの社会基盤的な側面をテーマとしました。今回は、PKIの既存の制度との不整合の問題、既存の社会基盤化したPKIの課題等、全体として既存のPKIの課題を取り上げたため、PKIの新たな技術の取り組みという点が、不足していたかもしれません。

次の社会基盤と言う観点からは、スマートグリッド、M2M等に組み込まれるPKIの技術研究が欧米では盛んに行われているようであり、今後は、こうした取り組みも取り上げていきたいと考えています。いずれにせよ、今後のIT社会における社会基盤には、デジタル化したTRUSTの構築が不可欠でありPKIの重要性は変わることはないでしょう。それが故に、今回の午後のようなテーマも真剣に議論する必要があると考えています。

◆参考

PKI Day 2012
http://www.jnsa.org/seminar/pki-day/2012/

JNSA/PKI相互運用技術ワーキンググループ
http://www.jnsa.org/result/pki/

Network Security Forum 2013

JNSA 幹事 / 株式会社 情報経済研究所
勝見　勉

JNSA 主催「Network Security Forum 2013」が、2013 年 1 月 25 日（金）、東京・ベルサール神保町で開催されました。情報セキュリティ政策会議、総務省、経済産業省、独立行政法人情報処理推進機構からの後援をいただき、情報セキュリティ月間の協賛・登録イベントでもある当シンポジウムは、209 名の参加を得て盛況のうちに終了しました。

プログラムは、名古屋大学・高倉弘喜教授の基調講演に始まり、JNSA のワーキンググループの成果発表など 3 講演、SNS とサイバー攻撃を各々テーマにしたパネルディスカッションという構成で、10 時 30 分から午後 6 時までという長い 1 日にも拘らず、多くの参加者に熱心に聴講、討議をしていただきました。

各プログラムの講演・ディスカッションの概要をご紹介します。

なお、各講演の資料（一部を除く）は JNSA の Web サイトで公開していますのでご参照下さい。

http://www.jnsa.org/seminar/nsf/2013/pro.html

【基調講演】

巧妙化するサーバ攻撃に備えたネットワーク運用

高倉　弘喜氏
名古屋大学情報基盤センター
情報基盤ネットワーク研究部門　教授

ますます巧妙化し、深刻化する標的型攻撃の実態と、サーバをいかに守るか、について実践を踏まえた具体的な指摘と提案を頂きました。

深刻化する脅威のポイントとしては、攻撃者は数ヶ月から数年かけて偵察と攻撃を繰り返して目的を遂げ、後は前線基地化して利用する、侵入を果たすとそのネットワークのセキュリティ対策を洗い出して迂回するので、発見は不可能に近い、と指摘。これに対処するのに、「侵入を 100% 阻止することは不可能で、侵入されていることを前提とした対策を考えるべき。狙われやすい場所・情報を重点的に守る考え方をしないと対策コストも追いつかないし効果も上げられない。情報セキュリティ対策も ROI で考えるべき時代だ。」との視点が示されました。

具体的な脅威や弱点の例として「特に狙われやすいのが認証系システムで、ここにネットワーク管理のすべての情報が集中しているので、ここを落とせば後の行動は自由になる。常時稼動が期待されるシステムでは、OS のアップデートも現実問題として不可能に近い状況がある。IPv6 は落とし穴になりやすい。最近の OS では自動化されたトンネリングサービスがあり、

IPv4 ネットワークに繋がっていれば OS が勝手に v6 をしゃべる状況なので、管理者の関知しない v6 ルーティングがいつの間にかできていた、ということが起こり、それが侵入ルートになるリスクが顕在化している。さらに、CPU を内蔵し無線 LAN を装備した SD メモリのようにシステムが小型化し、IPv6 レディな OA 機器、家電、センサーなどが出回っていて、ネットワークはいまや勝手に増殖すると想定しておかなければならない。Wi-Fi、テザリングなどの機能を持つスマートデバイスの普及も、同様のリスクをさらに大きくする。」と指摘され、高度化・複雑化するシステムや進化するデバイスが防御をいっそう困難にしている実態が語られました。

対策としては、「重要になるのは、ログの管理である。何のログをとるか、どこに保管するか、どのように監視・解析するかを正しく組み合わせなければ効果はない。取ればいいものではない。解析が追いつかない。ログサーバに全てを集約し、別セグメントで管理すべきである。監視対象を絞りログの量を圧縮するためにも、ネットワークのセグメンテーションは大事で、それとアクセスコントロールを適切に行うことで、セキュリティ対策も充実するし、ログ管理も容易になる。ただし、大規模システムではこの両立は至難の業で、ポリシーベースをしっかり構築し、ルールをモジュール化し、設定変更をある程度自動化できる仕組みを作らなくては、運用は不可能に近い。」と、重要ポイントを指摘されました。

このような具体的な説明と指摘を踏まえて「攻撃者は侵入するもの、ユーザは勝手にネットワークを持ち込むもの、を前提に、どの段階で発見するか、どのレベルで情報を取られることを押さえ込むか、を考えておかなければならない。」とまとめられました。

高倉　弘喜氏

【講演】

個人特性とインシデント発生確率の関係 ～個人のセキュリティ事故のデータを分析して～

大谷　尚通氏
株式会社エヌ・ティ・ティ・データ／
JNSA セキュリティ被害調査 WG リーダ

8 年以上継続して調査を行い、毎年その結果が注目を集めている個人情報漏洩インシデント調査の、2012 年上半期に関する分析結果の速報が報告・説明されました。

まず、「個人情報漏洩の 2012 年上半期集計の速報としては、漏えい件数 952 件（前年同期比+ 145 件）、漏えい人数約 151 万人（同－ 58 万人）、想定損害賠償総額 250 億円（同－ 323 億円）で、１人当り想定損害賠償額は約 6 万円（同＋約 2 万円）です。ここ数年は 1 件当りの漏えい人数が 100 万人を超えるインシデントが見られなくなっています。内訳として業種別（公務、金融業・保険業、教育・学習支援業、医療・福祉）、原因別（管理ミス、誤操作、紛失・置忘れ、盗難）媒体別(紙媒体、USB 等可搬記録媒体、電子メール、インターネット）の分析結果の各上位 4 項目は前

大谷　尚通氏

年と同じでした。

全体として、個人情報漏洩のインシデント件数は増加傾向にあるものの総漏えい人数は減少傾向にあり、原因としてはケアレスミスなどヒューマンエラーが大半を占めています。新しい傾向として、企業・組織の管理する情報に比べ、個人持ちのスマートデバイスから個人情報が漏えいするリスクが高まっています。」と調査結果の概要が紹介されました。

Webアンケートに基づき、インシデントの発生確率を調査した結果についても披露されました。紛失・盗難や誤送信などのインシデントを経験した人の割合は、携帯電話2.6%、パソコン1.5%、USBメモリ2.4%、電子メール11.8%となったこと、またサラリーマンとそれ以外の就業者の間の発生確率に顕著な差はなかったことが説明されました。

同調査の中で行った、個人の行動とインシデントの発生確率の相関性の分析結果は、「よく遅刻する」「約束を勘違いする」「仕事中にSNSなどの書き込みをする」「仕事中によく雑談・チャット等する」傾向の人はインシデントを起こす確率が高い傾向がある一方、「整理整頓が苦手」「忘れ物が多い」「仕事中に居眠りする」「仕事中にWebサーフィンする」傾向の人との相関は見られないとのことです。さらに、情報セキュリティやITの知識が多いこととインシデントの発生確率の関係では、知識を持っている人はパソコンやUSBメモリの紛失・盗難経験が高いという意外な関係性が見えたということに加え、知識とメール誤送信やSNS等への秘密情報の書き込みとの相関性は見られなかった、という興味深い分析が示されました。

このような分析結果を踏まえ、結論としては「個人の性格とインシデント発生確率との相関性は低い」が「行動パターンとインシデント発生確率との相関性はある」、知識に関しては、あるだけでは意味がなく実務に即して生かせるかが決め手になる、とまとめられました。

【講演】

情報セキュリティの国際標準の動向～ISO/IEC27002と外部委託関連の標準を中心に～

山下　真氏
富士通株式会社／
ISO/IEC JTC1/SC27 WG1国内幹事、WG4国内委員

情報セキュリティマネジメントシステムの国際標準であるISO/IEC27002を中心に、国際的標準化活動の概要や、現在進んでいる改訂の取り組み状況等について説明していただきました。

「国際的標準開発組織であるISO(国際標準化機構)とIEC（国際電気標準会議）の合同技術委員会・JTC1の下に小委員会（SC）が複数あり、セキュリティ関係はSC27で、その下にWG1（情報セキュリティマネジメントシステム）、WG4（セキュリティコントロールとサービス）など複数のワーキンググループがある。これらが27000シリーズの標準を開発･管理している。27000ファミリーには40ほどの標準が体系だって定義されている。」と全体構造の説明があり、「ISO/IEC27002は情報セキュリティの管理策集で、前回2012年10月のローマ会合で標準としての改訂を行う見通しがついた。改訂のポイントとしては技術的指針は他の標準に譲り、よりマネジメント寄りになった、陳腐化した内容の刷新や削除を行った。箇条の構成としては、Cryptographyの独立、Operations SecurityとCommunications Securityの分離、Supplier Relationshipの新設を行った。」等、構成の変更や、各箇条の変更内容のポイントの説明がされました。

次にクラウドコンピューティング関連の標準として27017の説明がありました。経済産業省からの提案を元に開発が進められていること、クラウドは第三者委託になることからリスクを特定できないことがリスクになるという課題があること、27017は27002の管理策に対してクラウドに固有の事項を追加する形で記述されていることを説明し、内容の例が紹介されました。

関連して27036「供給者関係」についても紹介され

ました。これは 27002 の Supplier relationship の新設を受けてその詳細を規定するもので、調達に伴うセキュリティリスクの管理と、委託先（供給者）管理について指針を提供するものです。このうち Part4 はクラウドサービスにおける情報セキュリティのガイドラインになっており、27017 がマネジメントベースであるのに対し、27036 では技術的内容を盛り込むことになる、とのことでした。

以上のように、情報セキュリティマネジメントシステムの中心となる 27002 と、クラウドコンピューティング関係の 27017、27036 の開発状況について、最新の状況の要点を教えていただきました。

【講演】

2012年度　セキュリティ市場調査結果の速報

勝見　勉
株式会社情報経済研究所／
JNSA セキュリティ市場調査 WG メンバー

2004 年度以来継続して実施しているセキュリティ市場調査の 2012 年度調査結果について、速報段階のデータとその説明を筆者から行いました。

まず、「2011 年度の市場規模の推定値は、ツール 3,551.5 億円、サービス 3,036.8 億円、合計約 6,588 億円になった。2012 年度は微増だが、2013 年度にはやや大きく成長して、2008 年度以来の 7000 億円台乗せが見込める。2008 年まで右肩上がりで伸びてきた市場はリーマンショックとそれに続く世界的不況で低迷していたが、2013 年度にはやや回復しそうだ。」との調査結果の概要の説明を行いました。

次いで、「情報セキュリティのツールやサービスを提供する主体としては、大手システムインテグレータや、SI・NI を提供する二次・三次の販売代理店と海外・国内のセキュリティベンダが中心である」との分析結果も説明しました。その他、ツール市場、サービス市場を構成する各個別市場の状況について市場規模の推計結果と、市場の動向について説明し、報告書に盛る新しい動向のトピックとして Security as a Service などを予定していることを紹介して、講演を終えました。

【パネルディスカッション】

SNSの安全な歩き方
～セキュリティとプライバシーの課題と対策～

＜モデレータ＞
高橋　正和氏　日本マイクロソフト株式会社／
JNSA SNS セキュリティ WG リーダ
＜パネリスト＞
守屋　英一氏　日本アイ・ビー・エム株式会社
岡庭　素之氏　キヤノン IT ソリューションズ株式会社
柳澤　智　氏　富士通株式会社

まず、モデレータであり JNSA の SNS セキュリティ WG リーダである高橋氏から同 WG が 2012 年 11 月に出した報告書「SNS の安全な歩き方」の紹介を兼ねたイントロがあり、SNS の問題とサイバー犯罪と実社会の問題との関連の絵解きや、プライバシーに忍び寄る SNS の危険、「SNS を安全に歩くための 10 項目」が紹介されました。

次にパネリスト 3 氏からポジショントークがあり、日本 IBM・守屋氏からは個人に浸透している SNS の実

態についてデータやトピックを説明いただき、キヤノンIT ソリューションズ・岡庭氏からは企業による SNS の活用（自治体や政府の利用も）の実態や課題についての紹介、富士通・柳澤氏からは SNS の今後の展開と題して SNS を活用した広告の実態やその裏にある SNS 上の個人に関するデータの利用のされ方とセキュリティ課題に関する提起がされ、その後ディスカッションに入りました。

ディスカッションでは、SNS で起きているセキュリティやプライバシーを脅かす事件や現象についてひとしきり紹介がありました。例えば、開示範囲をお友達にしていても、架空アカウントによるスパム的友達申請もあり、迂闊に友達申請に OK を出していると思わぬところまで広がっていく、ましてや友達の友達まで許容すれば実質野放しに近いとか、成りすまし被害、ストーカー被害など、知らないでいると危険な事例が多く紹介されました。

会場からの質問によるトークでは、mixi に足跡機能がなくなったことの是非など脱線気味の話もありましたが、SNS の危険性として捉えられているのが SNS に固有の問題なのか、とか、SNS のようなコミュニケーションの場はその構造や機能そのものはよいのではないか、問題はそのリスクをどう認識して自分の関心に合った使い方ができるのか、といったディスカッションが展開されました。

最後のテーマとして、SNS の将来については、企業による活用は今後も増える中、個人識別情報は持って行かれることを前提に、どこまで何の情報を出すかのコントロールが大事だが難しい問題だ、使い方のマナーは必要で特に若者に対する教育が必要だという意見、利用者像は今後もどんどん変わるだろう、その中でサービスも専門化や細分化が進み、リスクも多様化する、セキュリティ業界としては引き続き啓発警告を続けるべきだ、といった討論をしつつお開きとなりました。

【パネルディスカッション】

最近のサイバー攻撃に対する企業の自己防衛策

＜モデレータ＞
名和　利男氏　株式会社サイバーディフェンス研究所
＜パネリスト＞
小林　偉昭氏　独立行政法人情報処理推進機構
仁佐瀬剛美氏　NTT セキュアプラットフォーム研究所
山崎　英人氏　一般社団法人日本情報システムユーザ協会
岩井　博樹氏　株式会社ラック

まず、モデレータのサイバーディフェンス研究所・名和氏から「最近のサイバー攻撃に対する企業の自己防衛策」と題して、最近のサイバー攻撃のプロセス（いくつかのパターンがあり、多段的に仕掛けをし

て漸進的に情報を盗み、目的に迫る周到な手口)、注目すべき事例(米国でPOS端末から情報窃取、Anonymousによるイスラエルへのサイバー攻撃)、求められる防衛策のポイント(脅威を適切に把握、動向情報を積極的に収集、攻撃経路に対応した適切な対策、メリハリの利いた対策)についてプレゼンがありました。

次にパネリスト各位からのポジションプレゼンテーションが行われました。IPAの小林氏からは、最近の脅威の実態と対策の考え方、官民連携による情報共有や研究会の枠組み、IPAの取り組みとその活用勧奨について説明がありました。NTTの仁佐瀬氏からは、NTTグループのCSIRTであるNTT-CERTの組織、機能、活動について紹介があり、インシデント対応ライフサイクルに基づく対応や対策に近道はなく基本に忠実に、という視点、信頼できる情報共有の重要性等について指摘されました。続いてJUASのセキュリティ部会長の山崎氏からは、ユーザの立場からの問題提起ということで、ユーザ企業の悩み(トップの理解や予算の制約等)、ユーザ企業におけるセキュリティ人材の課題(教育、情報、処遇、モチベーション等)、経営者向け啓発への期待等が語られました。最後にラックの岩井氏からは、セキュリティオペレーション事業者の立場で、効果的対策とは何か、という観点から、MPS(Malware Protection System = Sandbox)やNGF(New Generation Firewall = UTM+AFW)の効果に関する考察や、深刻な新たな脅威の事例等の紹介があり、特性に応じたツールの使い分け、入口・出口・内部各々における対策、事故の定義を明確にして適切に対応する、という「心得」の指摘がされました。

続いてディスカッションに移り、「対策の限界」については、特にサプライチェーンの裾野には公的支援が必要ではないかという点や、被害発生時の情報の保全の重要性が指摘されました。「共有」というキーワードに対しては、相談相手がいないこと、特に地方は商業ベースでの対応が厳しいので公的支援が必要なこと、開示が難しい中でも情報共有が極めて大事なことや、今日のサイバー脅威に対しては、国家安全保障や諜報のセンスがなくては戦えないことなどの提起がされました。そして「ガイドライン」については、公的支援の必要性と、民間のサービスとの競合・棲み分け・連携に関する議論、学術的で高度すぎるものより具体的実践的なものの必要、事故・失敗事例だけでなく成功事例の共有が大事である点など、多彩な議論となりました。

締めくくりとしては、残念ながら攻撃側に構造的優位性がある中で、情報連携、官民連携、ベンダーユーザ連携の必要性などを確認して終了となりました。

以上をもって全プログラムを終了し、最後まで熱心に参加していただいた多くの聴衆の方の拍手の中、NSF2013は閉幕となりました。

JNSA 賀詞交歓会・JNSA 賞表彰式のご報告

賀詞交歓会

恒例のJNSA賀詞交歓会は、2013年1月25日（金）、東京のベルサール神保町にて開催されました。今回は、約100名の方にご参加いただき、盛況な会となりました。

冒頭、JNSA会長　田中英彦氏より挨拶を申し上げ、来賓としてお招きした、内閣官房情報セキュリティセンター 内閣審議官 占部浩一郎氏、総務省情報流通局行政局 大臣官房審議官 谷脇康彦氏、経済産業省商務情報政策局 大臣官房審議官　中山亨氏の各氏よりご挨拶を頂いた後、独立行政法人情報処理推進機構 理事長 藤江一正氏のご発声で乾杯を行い、引き続き和やかな懇談の場へと移りました。


占部　浩一郎氏


谷脇　康彦氏


中山　亨氏


藤江　一正氏

JNSA 賞 表彰式

しばらく歓談が続いた後、今回で7回目を迎えた恒例のJNSA賞の表彰式を行いました。各賞の受賞者が壇上に上がり、田中会長から表彰状と記念の盾、副賞が授与されました。各賞の受賞者と受賞理由は以下の通りです。受賞者の皆様、おめでとうございました。

個人の部（1件）

◇ 情報セキュリティ向上のための活動を積極的に行いJNSAの活動の活性化等に寄与
守屋 英一 氏（日本アイ・ビー・エム株式会社）

JNSAのSNSセキュリティWGを通し、対外的に広くSNSセキュリティ対策の啓発活動に従事している。
その活動の一端として、「フェイスブックが危ない」（2012年6月22日文芸春秋刊）を出版。
情報セキュリティ専門家としての知見とともに、豊富な調査データや事例、自身の実体験をもとに実名登録が原則であるフェイスブックに潜むリスクと安全に使う方法をITを得意としないユーザーにも広く伝えた。

ワーキンググループ（WG）の部（1件）

◇ WG の活動が協会の活性化ならびに情報セキュリティの向上に大きく貢献
在宅勤務における情報セキュリティ対策検討 WG（WG リーダ：みずほ情報総研株式会社　冨田 高樹 氏）

2011 年度に夏期の節電に向けて在宅勤務が増加することを想定し、その対策としてオフィスの節電対策のための「在宅勤務における情報セキュリティ対策ガイドブック」を公開。
2012 年度は改訂版として「オフィスの節電と在宅勤務における事業継続・情報セキュリティ対策ガイドブック」を公開した。両ガイドブックともに 1 カ月程度の短期間で執筆・とりまとめ・公開を行ない、即時性の高い情報提供に努めた。

特別賞（3件）

◇ インターネット安全教室を中心とする情報セキュリティ普及啓発活動を活発に実施することにより、広く一般社会のセキュリティ知識の向上に貢献
特定非営利活動法人なら情報セキュリティ総合研究所
特定非営利活動法人プロジェクトゆうあい

◇ 活動が情報セキュリティの向上に寄与
セキュリティ・キャンプ講師陣

IT に対する意識の高い若者に対し、情報セキュリティおよびプログラミングに関する高度な教育を実施し、将来の IT 産業の担い手となり得る優れた人材の発掘と育成を目的とした「セキュリティ・キャンプ」において、長年にわたり講師としてボランティア精神にあふれた活動を行い、わが国の情報セ キュリティの向上に貢献した。

「せきゅり亭」大賞・特別賞発表

引き続きしばらく歓談の後、今回から登場した新たなイベント、「せきゅり亭」の優秀作品の選出発表が行われました。「せきゅり亭」は、毎月お題を定めてセキュリティ川柳や狂歌などを募集し、JNSA のホームページに応募作品を掲載しているものです。この中からあらかじめ絞り込んだ 20 作品に対して、当日の日中に開催された JNSA 主催セミナー「Nework Security Forum 2013」の来場者から投票をいただき、受賞作品を選出しました。JNSA 大賞のほか、JNSA 会員企業がスポンサーとなった特別賞も選出・発表されました。各賞の受賞作品は次の通りです。

大　賞

なりすまし　怪しくないのが　なりすまし　（@M_Kazamidori_JP）

特別賞（以下、スポンサー社名あいうえお順）

カスペルスキー賞
つぶやいた 位置からバレる 浮気かな　（@sorcier_jp）

キヤノン IT ソリューション賞
嫁さんに　遠隔操作　されるオレ　帰りにたまご　買って来いって　(@masasama0616)

シマンテック賞
フォローした　女子高生は　家の妻　（@kannjyukukinoko）

ディアイティ賞
暗号化（餡豪華）美味い菓子かと おやじ問い　（いけねっと）

トレンドマイクロ賞　怪メール
「本物ですか」と返したら 返事が来たよ「あなたの方こそ」（おっちー）

JNSA 賞や「せきゅり亭」の各賞受賞作発表などで盛り上がる中、予定時刻が迫ってきたところで、JNSA 事務局長 下村正洋氏の発声で中締めとなりました。下村氏は、JNSA が発足 12 年干支一回りを迎える年になったことなど、感慨を述べた後、にぎやかに 3 本締めで参加者に和していただき、めでたく中締めとなりました。

ご参加いただいた方々、ご来賓の皆様、ありがとうございました。

2012年度
「インターネット安全教室」のお知らせ

～パソコンや携帯電話で思わぬトラブルや犯罪にまきこまれないために～

誰でも手軽にインターネットに接続できるようになった今日、ウイルス感染、詐欺行為、プライバシー侵害など情報犯罪の被害にあう危険性がますます高くなってきています。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、これらの被害を防ぐことはできません。

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

会場では参加者全員に、情報セキュリティ対策のポイントをわかりやすく解説する教材「インターネット安全教室」、子ども向けの「小中学生のためのインターネット安全教室」「まんがインターネット安全教室」、家庭向けリーフレット「親子で守って安全・安心10か条」を配布し、情報セキュリティの向上にお役立ていただいております。

今年度はインターネット安全教室のホームページをリニューアルし、新たに「Web版・インターネット安全教室」を公開いたしました。従来のビデオ教材に加え、講師による解説動画や、パソコン・ソフトウェアのセキュリティ設定の方法、実際の安全教室会場でよくある質問とその回答集なども紹介し、家庭や学校にいながらインターネットの安全な使い方をウェブサイト上で学習できます。

また、３月２日には「インターネット安全教室 in ソラマチ」と題し、第５回全国情報セキュリティ啓発シンポジウムを東京ソラマチにて開催いたしました。

経済産業省、NPO日本ネットワークセキュリティ協会（JNSA）は、引き続き全国各地の共催団体の方々のご協力を得て「インターネット安全教室」を開催し、さらなる情報セキュリティ普及啓発活動を展開してまいります。

【開催概要】

［主　　催］ 経済産業省、NPO日本ネットワークセキュリティ協会（JNSA）

［共　　催］ 全国各地のNPO・団体・自治体・学校など

［後　　援］ 情報セキュリティ政策会議、警察庁、その他各開催地新聞社・県・県警等（以上予定）

［開催一覧］（次頁）一覧をご覧下さい。（2013年2月現在）

最新の開催状況については、「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.net-anzen.go.jp/

◆「インターネット安全教室」共催団体募集◆

以下の地域での開催にご協力いただける団体を募集しております。
山形県、宮城県、茨城県、鳥取県、高知県、長崎県、その他離島など

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

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

詳しくは下記のお問い合わせ先までご連絡下さい。
【お問い合わせ先】 NPO日本ネットワークセキュリティ協会（JNSA）事務局（担当：林・坂内）
E-Mail:caravan-sec@jnsa.org

2012年度「インターネット安全教室」開催一覧

（2013年2月現在）

No.	日程	開催地	共催団体	会場
1	4月20日（金）	群馬	NPO法人おおたIT市民ネットワーク	ぐんま国際アカデミー
2	4月27日（金）	長野	NPO法人グループHIYOKO	安曇野市市民活動センター「くるりん広場」
3	5月16日（水）	岐阜	NPO法人泉京・垂井	垂井町立府中小学校
4	5月23日（水）	東京	NPO情報セキュリティフォーラム	板橋区消費者センター
5	5月26日（土）	岐阜	岐阜市消費生活センター	岐阜市消費生活センター ハートフルスクエアーG 2階 大研修室
6	5月29日（火）	長野	上田市マルチメディア情報センター	上田染谷丘高校 そめやホール
7	5月31日（木）	京都・京田辺市（新規）	京田辺市産業振興課	京田辺市社会福祉センター 第1研修室
8	6月12日（火）	北海道	旭川情報産業事業協同組合	末広公民館百寿大学
9	6月14日（木）	大阪	NPO法人きんきうぇぶ	河内長野市立千代田小学校
10	6月21日（木）	東京	三鷹市立井口小学校	三鷹市立井口小学校
11	6月22日（金）	群馬	NPO法人おおたIT市民ネットワーク	太田市立中央小学校
12	6月28日（木）	佐賀	NPO法人シニアネット佐賀	佐賀市高木瀬公民館
13	6月30日（土）	愛媛	NPO法人愛媛県IT推進協会	アイテムえひめ 第一会議室
14	6月21日（木）	岐阜	NPO法人泉京・垂井	郡上市総合センター
15	7月4日（水）	広島	福山市情報政策課	福山市竹尋公民館
16	7月10日（火）	東京	大正大学	大正大学
17	7月11日（水）	岐阜	NPO法人かにぱそこんくらぶ	みのかも文化の森 美濃加茂市民ミュージアム
18	7月13日（金）	佐賀	NPO法人シニアネット佐賀	大町町立大町中学校
19	7月15日（日）	北海道	北海道情報セキュリティ勉強会（せきゅぽろ）	北見市芸術文化ホール 5階 多目的室
20	7月18日（水）	東京	大正大学	大正大学
21	7月20日（金）	群馬	NPO法人おおたIT市民ネットワーク	太田市立城東中学校
22	7月20日（金）	佐賀	NPO法人シニアネット佐賀	佐賀市西与賀公民館
23	7月22日（日）	秋田	NPO法人ノースウインド	ITチャオ！
24	7月24日（火）	長野	NPO法人グループHIYOKO	松本市安原地区公民館
25	7月26日（木）	秋田	NPO法人ノースウインド	ITチャオ！
26	7月28日（土）	滋賀	NPO滋賀県情報基盤協議会	滋賀県立八幡工業高等学校
27	7月30日（月）	神奈川	NPO情報セキュリティフォーラム	相鉄岩崎学園ビル 6階604室
28	8月6日（月）	三重	PCシエル	四日市市　桜地区市民センター
29	8月7日（火）	福島	特定非営利活動法人日本コンピュータ振興協会	白河市役所
30	8月7日（火）	長野	NPO法人グループHIYOKO	たつのパークセンターふれあい
31	8月8日（水）	北海道	旭川情報産業事業協同組合	江丹別公民館百寿大学
32	8月16日（木）（午前）	沖縄	NPO法人フロム沖縄推進機構	宮古島市 マリンターミナルビル 2F 研修室
33	8月16日（木）（午後）	沖縄	NPO法人フロム沖縄推進機構	宮古島市 マリンターミナルビル 2F 研修室

No.	日程	開催地	共催団体	会場
34	8月22日（水）	広島	福山市情報政策課	福山市坪生公民館
35	8月23日（木）	佐賀	NPO法人シニアネット佐賀	アバンセ
36	9月4日（火）	大阪	NPO法人きんきうぇぶ	河内長野市立南花台西小学校
37	9月6日（木）	大阪	NPO法人きんきうぇぶ	河内長野市立南花台東小学校
38	9月6日（木）	大阪	NPO法人きんきうぇぶ	河内長野市立楠小学校
39	9月8日（土）	東京	中野区立新山小学校	中野区立新山小学校
40	9月14日（金）	北海道	旭川情報産業事業協同組合	旭川市シニア大学
41	9月14日（金）	神奈川	NPO情報セキュリティフォーラム	横浜市上白根コミュニティハウス
42	9月19日（水）	広島	福山市情報政策課	福山市津之郷公民館
43	9月20日（木）	佐賀	NPO法人シニアネット佐賀	アバンセ
44	9月28日（金）	佐賀	NPO法人シニアネット佐賀	佐賀市高木瀬公民館
45	10月4日（木）	山口・岩国市（新規）	NPO法人岩国パソコンの会	岩国市中央図書館 視聴覚室
46	10月13日（土）	神奈川	NPO情報セキュリティフォーラム	小田原市生涯学習センター けやき
47	10月13日（土）	宮崎	宮崎公立大学	宮崎公立大学 交流センター 多目的ホール
48	10月18日（木）	北海道	旭川情報産業事業協同組合	深川市立音江中学校
49	10月19日（金）	佐賀	NPO法人シニアネット佐賀	武雄市文化会館
50	10月20日（土）（午前）	兵庫	兵庫県立大学大学院応用情報科学研究科	兵庫県立大学神戸ポートアイランドキャンパス 大学院応用情報科学研究科情報処理室
51	10月20日（土）（午後）	兵庫	兵庫県立大学大学院応用情報科学研究科	兵庫県立大学神戸ポートアイランドキャンパス 大学院応用情報科学研究科情報処理室
52	10月28日（日）	神奈川	NPO情報セキュリティフォーラム	磯子区役所 いそご区民活動支援センター
53	11月6日（火）	福島	特定非営利活動法人日本コンピュータ振興協会	白河市立白河中央中学校
54	11月10日（土）	愛知	NPO東海インターネット協議会	ミッドランドホール A会議室
55	11月10日（土）	岐阜	NPO法人泉京・垂井	羽島市立小熊小学校
56	11月11日（日）	島根	NPO法人プロジェクトゆうあい	いきいきプラザ島根 3階 301・302研修室
57	11月13日（火）	福島	特定非営利活動法人日本コンピュータ振興協会	白河市立白河中央中学校
58	11月14日（水）	千葉	NPO浦安防犯ネット	浦安市立見明川中学校
59	11月15日（木）	沖縄	NPO法人フロム沖縄推進機構	浦添市立当山小学校 体育館
60	11月16日（金）	佐賀	NPO法人シニアネット佐賀	佐賀市西与賀公民館
61	11月17日（土）	神奈川	NPO情報セキュリティフォーラム	川崎市中原区民館 視聴覚室
62	11月19日（月）	神奈川	NPO情報セキュリティフォーラム	ヴェルク横須賀 6階 ホール
63	11月22日（木）	大阪	NPO法人きんきうぇぶ	大阪市立鯰江小学校
64	11月24日（土）	北海道・小樽市（新規）	NPO小樽ソーシャルネットワーク	小樽市生涯学習プラザ レピオ
65	11月26日（月）	神奈川	NPO情報セキュリティフォーラム	磯子区根岸地区センター
66	11月26日（月）	和歌山	NPO情報セキュリティ研究所	近畿大学附属和歌山高等学校
67	11月26日（月）	和歌山	NPO情報セキュリティ研究所	近畿大学附属和歌山高等学校
68	11月26日（月）	和歌山	NPO情報セキュリティ研究所	近畿大学附属和歌山中学校
69	11月26日（月）	佐賀	NPO法人シニアネット佐賀	佐賀市高木瀬公民館
70	11月30日（金）	三重	PCシエル	尾鷲市立尾鷲中学校 体育館
71	11月30日（金）	佐賀	NPO法人シニアネット佐賀	大町町立大町中学校
72	12月1日（土）	鹿児島	NPO法人鹿児島インファーメーション	鹿児島アリーナ 1階 会議室
73	12月3日（月）	大阪	NPO法人きんきうぇぶ	河内長野市立川上小学校
74	12月4日（火）	神奈川	NPO情報セキュリティフォーラム	磯子区屏風ヶ浦地域ケアプラザ
75	12月4日（火）	岐阜	NPO法人かにぱそこんくらぶ	可児市桜ヶ丘公民館
76	12月7日（金）	佐賀	NPO法人シニアネット佐賀	アバンセ
77	12月12日（水）	長野	NPO法人グループHIYOKO	山形村農業者トレーニングセンター
78	12月18日（火）	神奈川	NPO情報セキュリティフォーラム	ウェルネスさがみはら 7階 視聴覚室
79	1月10日（木）	三重	くわなPCネット	桑名市総合福祉会館
80	1月10日（木）	北海道	旭川情報産業事業協同組合	旭川市中央公民館
81	1月16日（水）	東京	八王子市立宮上小学校	八王子市立宮上小学校
82	1月18日（金）	島根	NPO法人プロジェクトゆうあい	出雲市立中部小学校
83	1月19日（土）	大阪	NPOなら情報セキュリティ総合研究所	大阪市立小松小学校
84	1月19日（土）	大阪	NPOなら情報セキュリティ総合研究所	大阪市立小松小学校
85	1月22日（火）	大阪	NPO法人きんきうぇぶ	河内長野市立石仏小学校
86	1月24日（木）	佐賀	NPO法人シニアネット佐賀	嬉野市中央公民館
87	1月25日（金）	群馬	NPO法人おおたIT市民ネットワーク	太田市立沢野小学校

No.	日程	開催地	共催団体	会場
88	1月26日（土）	栃木	NPO栃木県シニアセンター	栃木市栃木公民館 講堂
89	1月29日（火）	北海道	旭川情報産業事業協同組合	中富良野町公民館
90	1月30日（水）	佐賀	NPO法人シニアネット佐賀	佐賀市高木瀬公民館
91	1月31日（木）	大阪	NPO法人きんきうぇぶ	東大阪市立森河内小学校
92	1月31日（木）	大阪	NPO法人きんきうぇぶ	東大阪市立森河内小学校
93	1月31日（木）	大阪	NPO法人きんきうぇぶ	河内長野市立小山田小学校
94	2月4日（月）（午後）	大阪	NPO法人きんきうぇぶ	富田林市立人権文化センター
95	2月4日（月）（夜間）	大阪	NPO法人きんきうぇぶ	富田林市立人権文化センター
96	2月5日（火）	島根	NPO法人プロジェクトゆうあい	松江総合運動公園 会議室
97	2月7日（木）	群馬	NPO法人おおたIT市民ネットワーク	太田市立宝泉南小学校
98	2月6日（水）	秋田	NPO法人ノースウインド	ITチャオ！
99	2月7日（木）	沖縄	NPO法人フロム沖縄推進機構	久米島町立久米島小学校
100	2月7日（木）	沖縄	NPO法人フロム沖縄推進機構	久米島町立大岳小学校
101	2月7日（木）	沖縄	NPO法人フロム沖縄推進機構	久米島町立久米島西中学校
102	2月8日（金）	沖縄	NPO法人フロム沖縄推進機構	久米島町立美崎小学校
103	2月8日（金）	沖縄	NPO法人フロム沖縄推進機構	久米島町立仲里小学校
104	2月8日（金）	沖縄	NPO法人フロム沖縄推進機構	久米島町立比屋定小学校
105	2月12日（火）	秋田	秋田大学	秋田大学 5号館 101教室
106	2月13日（水）	神奈川	NPO情報セキュリティフォーラム	葉山町福祉文化会館 大会議室
107	2月16日（土）	三重	PCシエル	四日市市 塩浜地区市民センター　2階 大ホール
108	2月16日（土）	福井	NPO法人ナレッジふくい	永平寺町立志比南小学校 ランチルーム
109	2月16日（土）	香川	e-とぴあ・かがわ	情報通信交流館 e-とぴあ・かがわ BBスクエア
110	2月17日（日）	宮崎	宮崎公立大学	宮崎市佐土原総合文化センター 研修室
111	2月19日（火）	岡山	岡山県インターネットセキュリティ対策連絡協議会	岡山学芸館高校
112	2月20日（水）	大阪	NPO法人きんきうぇぶ	河内長野市立美加の台小学校 多目的室
113	2月21日（木）	東京	小金井市立小金井第一小学校	小金井市立小金井第一小学校
114	2月21日（木）	佐賀	NPO法人シニアネット佐賀	アバンセ
115	2月22日（金）	秋田	NPO法人ノースウインド	ITチャオ！
116	2月22日（金）	神奈川	NPO情報セキュリティフォーラム	海老名市役所 4階 401会議室
117	2月23日（土）	北海道	旭川情報産業事業協同組合	旭川市科学館　1階 研修室
118	2月27日（水）	福岡	NPO法人スキルアップサービス	曽根東市民センター 多目的ホール
119	3月2日（土）	神奈川	川崎市立下小田中小学校・ 土曜施設開放ボランティア	川崎市立下小田中小学校
120	3月6日（水）	長野	NPO法人グループHIYOKO	豊科交流学習センター「きぼう」 学習室1
121	3月6日（水）	鹿児島	財団法人ハイパーネットワーク社会研究所	鹿児島県肝属郡肝付町文化センター
122	3月7日（木）	大阪	NPO法人きんきうぇぶ	河内長野市立小山田小学校
123	3月7日（木）	鹿児島	財団法人ハイパーネットワーク社会研究所	鹿児島県肝属郡肝付町文化センター
124	3月8日（金）	富山	（株）富山県総合情報センター	大門企業団地協同組合 組合会館
125	3月9日（土）	北海道	NPO法人くるくるネット	室蘭市中小企業センター 中会議室
126	3月9日（土）	福岡	NPO法人スキルアップサービス	大里柳市民センター 会議室1、2
127	3月9日（土）	鹿児島	NPO法人鹿児島インファーメーション	かごしま県民交流センター 3階 研修室
128	3月10日（日）	宮崎	宮崎公立大学	放送大学宮崎学習センター 第1講義室
129	3月16日（土）	北海道	北海道情報セキュリティ勉強会（せきゅぽろ）	札幌市民ホール 第3会議室
130	3月16日（土）	熊本	NPO法人NEXT熊本	くまもと県民交流館パレア パレアホール
131	3月18日（月）	佐賀	NPO法人シニアネット佐賀	唐津情報ステーション
132	3月21日（木）	石川・金沢市（新規）	石川県消費者団体連合会 NPO法人石川県情報化支援協会	石川県地場産業振興センター 新館5階 第12研修室
133	3月21日（木）	福岡	NPO法人スキルアップサービス	葛原市民センター 大会議室
134	3月24日（日）	栃木	NPO栃木県シニアセンター	鹿沼市民情報センター 5階 マルチメディアホール
135	3月24日（日）	東京	NPO法人PEOPLE VINES	国分寺Lホール
136	3月29日（金）	三重	PCシエル	三重県総合文化センター内 三重県生涯学習センター 3階 ミーティングルーム

経済産業省 中小企業情報セキュリティ対策促進事業

情報セキュリティ対策

平成24年度

中小企業向け指導者育成セミナー

～グループ討議を中心とした実践型研修！～

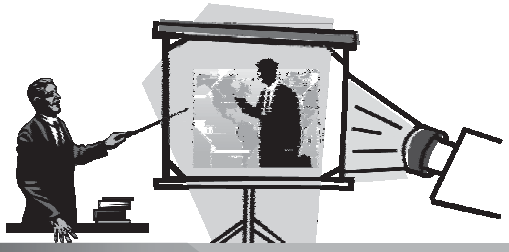
主催：経済産業省
特定非営利活動法人 日本ネットワークセキュリティ協会

ポイント その1
企業が知っておくべき最新の情報を解説

ポイント その2
PDCA を意識した実効性のある対策を演習で体感

ポイント その3
指導に役立つ資料やツールを無償提供

中小企業の経営者等に対して、情報セキュリティのアドバイスが適切に行える指導者を育成するため、全国で指導者育成セミナーを開催しました。



セミナー開催概要

http://www.jnsa.org/ikusei/seminar/

スケジュール	午前（9：30 ～ 12：15）			～昼食（12:15 ～ 13:15）～	午後（13：15 ～ 17：00）	
項目	情報セキュリティ重要ポイント解説（60 分）	日常業務上の運用チェック基本解説（20 分）	情報セキュリティ対策の課題洗い出し（85 分）		課題の実施状況チェックと見直しの討議（90 分）	企業ごとのルール見直し演習（60 分）
内容	テキストにより、最新情報や最近の注意点など、時流に沿ったポイント解説を行う。	日常業務の中で事故発生の危険性チェックや、計画や対策の段階にさかのぼって見直しをするための PDCA を解説する。	いくつかの企業の業務風景のビデオを視聴し、PDCA を意識したリスク発見演習を行う。		ビデオに出てくる課題の原因について、チェックや見直しの観点で討議する。	企業ごとのルールを、グループ討議により見直しを行う。
備考	講義	講義	グループワーク		グループワーク	グループワーク

※進行状況により途中の時間帯は変動することがあります。また、途中に事務局からの説明や休憩をはさみます。

主催	経済産業省、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）
後援	独立行政法人情報処理推進機構、日本商工会議所、全国商工会連合会、NPO法人ITコーディネータ協会、全国中小企業団体中央会、社団法人中小企業診断協会、株式会社商工組合中央金庫、開催地の商工会議所・商工会連合会・中小企業団体中央会・その他団体等
参加対象者	中小企業の経営者等に対して情報セキュリティを指導する立場にある次のような方々。 ITコーディネータ、中小企業診断士、日商マスター、EC実践講師、その他中小企業に対して指導的立場にある方々（各団体指導員、IT関連企業の方等）、団体職員（商工会議所関係者及び商工会関係者、中小企業団体中央会関係者）等 ※・前年度・前々年度のセミナー参加者の方にも受講をお勧めします。 ・ITコーディネータの方は本セミナーを受講されると知識ポイント（6.5 時間分）が付与されます。
参加者の特典	•指導用ツール（講習用テキスト、指導者用マニュアル、指導用ビデオ教材、IPA 資料）を無償でお渡しします。 •配布する指導用ツールで講習会を開催される場合、実施報告をいただくことで謝金をお支払します（2013年2月末開催分まで）。 •セミナー参加者専用サイトにより、その他指導用の補足資料等を随時提供します。
参加費	無料（事前登録制）
その他	•開催地域ごとの開催予定日、会場などは、裏面の会場別日程をご覧ください。 •本事業のホームページでは、情報セキュリティの基礎知識やビデオ解説入りeラーニング、確認テストなどを掲載しています。 •情報セキュリティの基礎知識の習得や再確認にお使い下さい。（http://www.jnsa.org/ikusei/）

本事業のホームページでは、情報セキュリティの基礎知識やビデオ解説入りeラーニング、確認テストなどを掲載しています。
情報セキュリティの基礎知識の再確認にお使いください。
中小企業情報セキュリティ対策促進事業ホームページ http://www.jnsa.org/ikusei/

セミナー実施会場別日程

全 23 回（今年度のセミナーは全て終了しました。）

ブロック	都道府県	地域後援団体	開催日	実施会場
北海道	北海道①（札幌）	札幌商工会議所	2012年10月12日(金)	北海道経済センター
	北海道②（函館）	北海道中小企業団体中央会道南支部/函館商工会議所/北海道渡島管内商工会連合会/北海道檜山管内商工会連合会/ITCはこだて/はこだてIKA	2012年10月30日(火)	函館商工会議所
東　北	宮城	仙台商工会議所	2012年9月18日(火)	仙台商工会議所
	岩手	岩手県商工会連合会	2012年12月6日(木)	岩手県商工会連合会
関　東	茨城	水戸商工会議所/茨城県商工会連合会/茨城県商工会議所連合会/NPO法人ITコーディネータ茨城/茨城県中小企業団体中央会/公益財団法人茨城県中小企業振興公社	2012年9月26日(水)	水戸プリンスホテル
	埼玉	NPO法人埼玉ITコーディネータ/さいたま商工会議所/埼玉県商工会連合会/埼玉県中小企業団体中央会/社団法人埼玉県商工会議所連合会/財団法人埼玉県産業振興公社	2012年10月18日(木)	大宮ソニックシティ
	千葉	柏商工会議所/NPO法人ちば経営応援隊	2012年8月28日(火)	柏商工会議所
	東京①	東京商工会議所	2012年10月29日(月)	ベルサール八重洲
	東京②	東京商工会議所	2013年1月22日(火)	東京商工会議所
	長野	一般財団法人塩尻市振興公社/塩尻商工会議所	2012年11月22日(木)	塩尻インキュベーションプラザ
中　部	愛知	名古屋商工会議所/一般社団法人中部産業連盟	2012年10月16日(火)	中産連ビル
	岐阜	大垣商工会議所/財団法人ソフトピアジャパン	2012年11月20日(火)	ソフトピアジャパンセンタービル
	三重	三重県商工会連合会/三重県中小企業団体中央会/NPO法人ITコーディネータ三重	2013年1月16日(水)	三重県総合文化センター
	富山	富山商工会議所/富山県中小企業団体中央会/社団法人富山県情報産業協会/NPO法人ITコーディネータ富山/株式会社富山県総合情報センター	2012年10月25日(木)	富山県総合情報センター
	石川	金沢商工会議所/石川県商工会連合会/NPO法人石川県情報化支援協会	2012年11月9日(金)	金沢商工会議所
近　畿	京都	京都商工会議所	2012年12月13日(木)	京都商工会議所
	大阪	大阪商工会議所	2012年9月11日(火)	大阪商工会議所
	奈良	奈良商工会議所/奈良県中小企業診断士会/奈良県商工会連合会	2012年11月6日(火)	奈良商工会議所
中　国	広島	広島商工会議所/NPO法人ITコーディネータ広島	2012年9月7日(金)	広島国際会議場
四　国	愛媛	松山商工会議所	2012年11月2日(金)	松山市男女共同参画推進センター
九　州	福岡	福岡商工会議所	2012年9月4日(火)	福岡商工会議所
	宮崎	宮崎商工会議所/宮崎県ソフトウェアセンター	2012年11月28日(水)	宮崎商工会議所
沖　縄	沖縄	沖縄県商工会連合会/沖縄県商工会議所連合会/那覇商工会議所/財団法人沖縄県産業振興公社	2012年10月2日(火)	沖縄産業支援センター

事務局お知らせ
JNSA ANNOUNCE

主催セミナーのお知らせ

● 第５回全国情報セキュリティ啓発シンポジウム インターネット安全教室 in ソラマチ

主　催：経済産業省
　　NPO日本ネットワークセキュリティ協会
日　時：2013年3月2日(土)
会　場: 東京ソラマチ　スペース６３４

後援・協賛イベントのお知らせ

1. 情報セキュリティシンポジウム道後2013

主　催：情報セキュリティシンポジウム
　　道後2013実行委員会
日　時：2013年2月28日(木)～3月2日(土)
会　場：【講演・パネルディスカッション】
　　松山市子規記念博物館 4階講堂
　　【ナイトセッション】
　　2013年2月28日(木)19：00－21：00
　　道後　茶玻瑠3階「太陽の間」
　　【意見交換会】
　　2013年3月1日(金)18：00－19：30
　　道後　茶玻瑠2階「花小路」
ＵＲＬ：http://ehime-it.org/ssd/

2. 情報セキュリティエコノミクスシンポジウム2013

主　催：独立行政法人情報処理推進機構
日　時：2013年3月5日(日)
会　場: コクヨホール
ＵＲＬ：http://www.ipa.go.jp/security/event/2013/eco_sympo/index.html

3. 第９回IPA情報セキュリティ標語ポスター ４コマ漫画コンクール2013

主　催：独立行政法人情報処理推進機構
会　期：2013年4月1日(月)～11月30日(土)
募集期間: 2013年4月1日(月)～9月9日(月)
　　11月下旬～12月中旬に授賞式開催予定
ＵＲＬ：http://www.ipa.go.jp/security/event/hyogo/2013/

4. 自治体総合フェア2013

主　催：日本経営協会
　　自治体総合フェア事務局
日　時：2013年5月15日(水)～5月17日(金)
会　場: 東京ビッグサイト(東京国際展示場)
　　西展示棟・西3ホール
ＵＲＬ：http://www.noma.or.jp/lgf/2013/

5. ワイヤレスジャパン2013

主　催：株式会社リックテレコム
　　日本イージェイケイ株式会社
日　時：2013年5月29日(水)～5月31日(金)
会　場: 東京ビッグサイト西3、4ホール、会議棟
ＵＲＬ：http://www.wjexpo.com

JNSA 部会・WG2012 年度活動

1.社会活動部会

（部会長：西本逸郎 氏／株式会社ラック
副部会長：丸山司郎 氏／株式会社ラック）

外部に向けた情報発信や対外的な社会貢献活動、国際連携や他組織との連携などを推進する。

具体的には、政府関連のパブコメ対応や勉強会などの対外活動、委託事業や外部への普及啓発などの社会貢献活動、指導者育成や講師派遣などの対外的支援活動、国際・他団体連携などを進める。

【セキュリティ啓発WG】

（リーダー：平田敬 氏／株式会社ブリッジ・メタウェア）

経済産業省委託事業「インターネット安全教室」の内容検討、シンポジウムの企画開催、共催団体へのサポートを行う。

【指導者育成セミナー講師WG】

（リーダー：持田啓司 氏／株式会社大塚商会）

経済産業省委託事業「中小企業情報セキュリティ対策促進事業」の枠組みの中、「中小企業向け指導者育成セミナー」の内容検討及びセミナー講師を行う。

【在宅勤務における情報セキュリティ対策検討WG】

（リーダー：冨田高樹 氏／みずほ情報総研株式会社）

昨年度に作成した「在宅勤務における情報セキュリティ対策ガイドブック」を改訂し、「オフィスの節電と在宅勤務における事業継続・情報セキュリティ対策ガイドブック」を公開した。

【日本の政党政策評価WG】

（リーダー：米澤一樹 氏／株式会社シマンテック）

日本の各党の情報セキュリティに対する政策を、民間という立場から評価し公表することで、我が国政府に対する、JNSAの存在価値を高める。

2．調査研究部会

（部会長：加藤雅彦 氏／株式会社インターネットイニシアティブ）

主に調査活動と技術的研究や勉強会などを行っていく。調査事業としては被害調査および市場調査を2大事業として推進し、技術的研究としてIPv6などの新コンピューティング技術の調査研究、およびスマートフォン、SNSの安全な利用に関する調査研究を行う。

また、新たな技術の調査研究に必要な勉強会、BoFなどは随時行う。

【セキュリティ被害調査WG】

（リーダー：大谷尚通 氏／株式会社NTTデータ）

発生確率調査（本調査）を実施し、報告書を作成し公開した。2011年発生確率調査の結果から本調査のテーマを選択・深堀り、および 2011年調査以外の他エリアの発生確率調査を実施。2011年個人情報漏えい調査報告書を作成し公開した。2012年の調査に向けて、調査項目の検討、準備および調査を実施。

＜予定成果物＞

「2011年情報セキュリティインシデントに関する調査報告書（発生確率編 サマリ版 英訳）」

【セキュリティ市場調査WG】

（リーダー：加藤雅彦 氏／株式会社インターネットイニシアティブ）

昨年度に引き続き、従来と同様の枠組みで市場調査を行い、結果を公表する。

＜予定成果物＞

2012年度市場調査報告書

【ＩＰｖ６セキュリティ検証WG】

（リーダー：許先明 氏／株式会社ラック）

IPv6対応時のセキュリティ確保のため、現状のIPv6環境に対する攻撃等を分析できる環境を構築し、基礎データを収集する。

【スマートフォン活用セキュリティポリシーガイドライン策定WG】

（リーダー：加藤智巳 氏／株式会社ラック）

スマートフォン活用セキュリティポリシーガイドライン正式版のリリースを予定。WGの開催と正式版リリース後に情報交換会の開催を行う。

＜予定成果物＞

スマートフォン活用セキュリティポリシーガイドライン（正式版）

【SNSセキュリティWG】

（リーダー：高橋正和 氏／日本マイクロソフト株式会社）

SNSのセキュリティ、プライバシーの扱い方を、報告書としてまとめる。

「SNSの安全な歩き方～セキュリティとプライバシーの課題と対策」を11月に公開した。

【組織で働く人間が引き起こす不正・事故対応WG】
（リーダー：甘利康文 氏／セコム株式会社）

組織で働く人間が引き起こす事故、すなわち意図を持った「内部不正」と、意図のない「ヒューマンエラー」を対象として、これらの「内部不正・事故」の防止／抑止方法論を具体的にまとめることを目的とする。
「内部不正・事故」の対象想定：
使い込み、内部窃盗、不正経理、取引先等との癒着、意図的不作為・隠蔽、カルテル、組織の私物化（公私混同）、ハラスメント、ヒューマンエラーなど、組織で働く人間が引き起こす違法（脱法）行為、ルール違反全般（システムからの情報漏洩などのIT分野に限りません）

＜予定成果物＞

・内部不正・事故抑制に関する具体的ソリューションの提案書（ソリューションガイド）
・内部不正・事故対応の具体事例（ベストプラクティス）集

3．標準化部会

（部会長：中尾康二 氏／KDDI株式会社）

昨年度に引き続き、業種・業界・分野等の標準化・ガイドライン化などを推進する。具体的には、JNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準との親和性の高い案件については、国際標準への提案も視野に入れて、議論を進めることとしたい。

【アイデンティティ管理WG】
（リーダー：宮川晃一 氏／日本ビジネスシステムズ株式会社）

アイデンティティ管理の必要性の啓発および導入指針の提示などによる普及促進、市場活性化を目的とする。

＜予定成果物＞

1．ロール管理ガイドライン
2．クラウド環境におけるアイデンティティ管理書籍改訂版

【セキュアプログラミングWG】
（リーダー：塩田英二 氏／TIS株式会社）

セキュアシステム構築技術の普及・啓蒙と関連する標準化活動への関与を通しての貢献を行う。
セキュアプログラミングの原則に関するSC27WG4ほか国際標準関連活動へのコメント、OWASP等他団体との連携等。

【情報セキュリティ対策マップ検討WG】
（リーダー：奥原雅之 氏／富士通株式会社）

「情報セキュリティ対策マップ」の作成に関する以下のアウトプットを作成する。
・組織全体の情報セキュリティ対策の状況を確認することができる「情報セキュリティ対策マップ」のコンセプト
・これを作成するための手法や記述モデル
・実例としての汎用的な標準情報セキュリティ対策マップ案

【国際化活動バックアップWG】
（リーダー：中尾康二 氏／KDDI株式会社）

JNSAとISFとの連携、およびKISIAとの連携など、JNSAと国際連携にかかわる検討を行い、必要な共同成果物の策定に努め、JNSAの他WG活動の活性化につなげる。
2度のISO/SC27会合（5月、10月）、ISF総会などへの参加を通じて、ISFとの国際連携につき、一定の方向性を出す。連携の方向性が見出せない場合は、ISFとの関係の見直しを考える。（年度末を目処）
また、韓国KISIAとの連携についても、具体的な活動に向けた整理を実施し、連携活動を軌道に乗せる。

＜予定成果物＞

「クラウドセキュリティにかかわる技術ガイドライン」のドラフト

【ＰＫＩ相互運用技術WG】
（リーダー：松本泰 氏／セコム株式会社）

PKIに関する課題をWGなどで議論し、活動の成果を12月13日開催の「PKI day 2012」で発表した。

4．教育部会

（部会長：安田直 氏／株式会社ディアイティ）

良質かつ社会のニーズに適合したセキュリティ人材の育成のため、必要とされる知識・技能等の検討を行い、実際の大学や専門学校等で評価実験を行うと共に、部会メンバーが実際に教育を行う機会を持ち、その成果を会員共同プロジェクトや産学協同プロジェクトとして実施することにより会員ならび社会に還元する。

【情報セキュリティ教育研究WG】
（リーダー：長谷川長一 氏／株式会社ラック）

今年度よりWG名を「セキュリティ講師スキル研究WG」から変更。情報セキュリティ教育に必要なインストラクションスキルの他、必要なスキル、教育の様々

な方式(座学、演習、ワークショップ、ケーススタディ、PBL、競技等)、手法や技術(クラウド、ソーシャルメディア、ストリーミング等)の研究を行う。

【情報セキュリティ教育実証WG】
(リーダー:平山敏弘 氏/日本アイ・ビー・エム株式会社)

平成24年度も、岡山理科大学において、履修2単位対象となる半期(6ヶ月)で計15回の講義を継続実施中。また東京デザインテクノロジー専門学校においては、昨年の情報セキュリティ講義の受講対象者を広げ通期(12ヶ月)で計30回の講義を実施中。講義内容は座学講義に加えて実機利用やケーススタディなどの実践力強化講義となっている。後期は、教育部会として人材育成に関わる新たな試みとして、「情報セキュリティ教育研究WG」で研究した成果を協力してくれる学校での実証を特別講義や公開講座として実施予定。

また、産学情報セキュリティ人材育成検討会メンバーとしても活動を実施中。

【IT・セキュリティキャリア女性活躍推進WG】
(リーダー:北澤麻理子 氏/ドコモ・システムズ株式会社)

IT業界で働く女性たちの環境やキャリアプラン等の実態および意識を調査し、課題を抽出して改善方策を考察する。

同時に、Face to Faceにこだわらない参加形態を模索。働き方の多様性を提言するための検証の場とする。働く女性の立場、女性の働きやすさについてアンケートを実施し、10月にその結果を公開した。

5. 会員交流部会

(部会長:小屋晋吾 氏/トレンドマイクロ株式会社)

情情報セキュリティ業界の健全な発展のために会員向けサービスを充実させ、業界の発展に貢献する。

具体的には、勉強会や製品紹介サイトの運営、情報交換・情報発信などを行う。

【セキュリティ理解度チェックWG】
(リーダー:大溝裕則 氏/株式会社JMC)

日本の情報セキュリティのリテラシー向上を目指し、「理解度セルフチェックサイト」、「情報セキュリティ理解度チェック」、「情報セキュリティ理解度チェック・プレミアム」の利用者増加のための活動を行う。

【JNSAソリューションガイド検討WG】
(リーダー:村上智 氏/株式会社シマンテック)

2011年度内のソリューションカイドのリリースを受け、2012年度は「JNSAソリューションカイド検討WG」から名称を変更。ソリューションカイドの更なる活用を踏まえ、年間の活動を通じて会員企業及び会員企業が有しているソリューションのPRを図る。

6. 西日本支部

(支部長:井上陽一 氏/JNSA顧問)

関西に拠点を置くメンバー企業が中心となり、提携団体との協働の下、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・向上に資すると共に、リスクの変化に応じた機動的な対応の実践を支援するため、先進性を追及、質の高いサービスを提供する事を目的として、中小企業に軸足を置いた活動を行う。

また新企画として、近畿経済産業局と情報セキュリティの現在について定例会議を開催する。

【情報セキュリティチェックシートWG】
(リーダー:嶋倉文裕 氏/富士通関西中部ネットテック株式会社)

リスクを洗い出し、評価、対策することを支援する「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」と情報セキュリティチェックシートとの対応付けを行い、現状の情報セキュリティチェックシートの不足内容や構成、整理の仕方を検討し、中小企業が実際にチェック・アクションに活用出来る情報セキュリティシートチェックシートへと改訂を行う。

また、クラウド、スマートフォンと言った新しいサービスやデバイスのセキュリティについても、情報セキュリティチェックシートへの取り込み方を検討する。

【出社してから退社するまでのリスク対策WG】
(リーダー:元持哲郎 氏/アイネット・システムズ株式会社)

2011年度版「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」で対応しなかったスマートデバイス、クラウド向けに、中小企業におけるセキュリティ対策を検討する

【企画・運営WG】
(リーダー:齋藤聖悟 氏/株式会社インターネットイニシアティブ)

西日本企業のセキュリティ啓発を目的として、セミナーおよび勉強会を実施していく。

7．U40部会

（部会長:前田典彦 氏／株式会社Kaspersky Labs Japan）

若年層を対象メンバーとして、JNSAの若返り、若年層の活動活発化、幅広い人脈形成を目的として活動を行う。

【JNSAラボネットWG】

（リーダー：一宮隆祐 氏／日本電気株式会社）

・JNSA内、ラボネットを利用した検証での環境の提供
・ラボネットを利用した技術検証の実施

【勉強会企画検討WG】

（リーダー:前田典彦 氏／株式会社Kaspersky Labs Japan）

U40部会員の知識・スキル向上を目指し、勉強会を企画・開催する。勉強会は講師からの講義だけにとどまらず、グループディスカッションやハンズオンも取り入れ活発な意見交換を行う。部会員以外のJNSA会員からも勉強会参加者を募り、部会員同士・JNSA会員・講師との人脈形成を行う。

8．情報セキュリティ教育事業者連絡会（ISEPA）

（代表:与儀大輔 氏/NRIセキュアテクノロジーズ株式会社）

今年度は、四半期ごとのセキュリティ人材数のWeb公開の継続及び事業者の連携事例の発表の継続を予定している。また、ISEPAイベント開催の検討も行う。

9．日本セキュリティオペレーション事業者協議会（ISOG-J）

（代表：武智洋 氏／株式会社ラック）

セキュリティオペレーションの普及・啓発及び事業者間の技術レベル及びサービスレベル向上にむけた各種活動を行う。

＜予定成果物＞

「セキュリティ診断・検査のためのガイドライン」（検討中）及び「情報セキュリティ小六法」改訂版

【セキュリティオペレーションガイドラインWG】

（リーダー：武智洋 氏／株式会社ラック）

新たにサービス利用者向けのガイドラインを作成に向けて、フィージビリティスタディを行うことで活動を進める。

【セキュリティオペレーション技術WG】

（リーダー：川口洋 氏／株式会社ラック）

セキュリティ技術の情報交換及びセミナー実施。また、事業者間の情報連携の実践を検討予定。

【セキュリティオペレーション関連法調査WG】

（リーダー：出口幹雄 氏／富士通株式会社）

法改正、警察庁からの情報提供、官民情報共有などのSOC事業者の契約に関する意見交換を予定。

【セキュリティオペレーション認知向上・普及啓発WG】

（リーダー：武智洋 氏／株式会社ラック）

内部及び外部セミナーの企画、その他イベント運営、ISOG-J全般運営を実施予定。

【標的型攻撃対策検討WG】

（リーダー:齋藤衛 氏／株式会社インターネットイニシアティブ）

標的型サイバー攻撃に関する情報共有と官公庁との情報連携を予定。

10．産学情報セキュリティ人材育成検討会

大学関係有識者やJNSA会員でインターンシップ受け入れ可能な企業が集まり2012年2月に発足。メンバーアンケートやヒアリング等を実施し、インターンシップのあり方に関する報告書を11月に公開。

その後、実用的なインターンシップ制度の実施の実現に向けた検討を行っていく予定。2013年4月にJNSAインターンシップの始動に向けて準備中。

11．セキュリティコンテスト実行委員会

JNSAで2003年～2004年度にかけてセキュリティ・スタジアムに協力してきたが、その流れをくむセキュリティコンテストの企画運営を行った。

2012年度は関東・地方を含めて4回程度、セキュリティコンテスト（SECCON）ならびにプログラミングコンテスト「ハッカソン」を行い、2013年2月に東京電機大学にて全国大会を実施した。

JNSA 役員一覧　2013 年 2 月現在

会　長	田中　英彦	情報セキュリティ大学院大学 学長
副会長	髙橋　正和	日本マイクロソフト株式会社
副会長	中尾　康二	ＫＤＤＩ株式会社
副会長	大和　敏彦	ＺＴＥジャパン株式会社

理　事（50音順）

遠藤　直樹	東芝ソリューション株式会社
大城　卓	新日鉄ソリューションズ株式会社
小橋　喜嗣	エヌ・ティ・ティ・アドバンステクノロジ株式会社
桑田　潤	大日本印刷株式会社
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
桜井　鐘治	三菱電機株式会社 情報技術総合研究所
下村　正洋	株式会社ディアイティ
橘　伸俊	株式会社ネットマークス
西尾　秀一	株式会社ＮＴＴデータ
西本　逸郎	株式会社ラック
藤川　春久	セコムトラストシステムズ株式会社
村上　智	株式会社シマンテック
吉原　勉	株式会社インターネットイニシアティブ

幹　事（50音順）

安達　智雄	日本電気株式会社
大島　耕二	株式会社ネットマークス
大溝　裕則	株式会社ＪＭＣ
岡庭　素之	キヤノンITソリューションズ株式会社
勝見　勉	株式会社 情報経済研究所
加藤　雅彦	株式会社インターネットイニシアティブ
北折　昌司	東芝ソリューション株式会社
北澤　麻理子	ドコモ・システムズ株式会社
郷間　佳市郎	株式会社日立システムズ
後藤　忍	セコムトラストシステムズ株式会社
小屋　晋吾	トレンドマイクロ株式会社
佐藤　憲一	株式会社OSK
嶋倉　文裕	富士通関西中部ネットテック株式会社
下村　正洋	株式会社ディアイティ
髙橋　正和	日本マイクロソフト株式会社
田中　年男	ネットワンシステムズ株式会社
中尾　康二	ＫＤＤＩ株式会社
西本　逸郎	株式会社ラック
森　直彦	エヌ・ティ・ティ・アドバンステクノロジ株式会社
半田　富己男	大日本印刷株式会社
樋口　健	株式会社インフォセック
平田　敬	株式会社ブリッジ・メタウェア
蛭間　久季	株式会社アークン
二木　真明	アルテア・セキュリティ・コンサルティング
安田　直	株式会社ディアイティ
油井　秀人	富士通エフ・アイ・ピー株式会社
与儀　大輔	NRIセキュアテクノロジーズ株式会社
米澤　一樹	株式会社シマンテック
渡辺　仙吉	日本アイ・ビー・エム株式会社

監　事

土井　充	公認会計士土井充事務所

顧　問

井上　陽一	
今井　秀樹	中央大学 教授
北沢　義博	法律事務所フロンティア・ロー 弁護士
武藤　佳恭	慶應義塾大学 教授
前川　徹	サイバー大学 教授
村岡　洋一	早稲田大学 教授
安田　浩	東京電機大学 教授
山口　英	奈良先端科学技術大学院大学 教授
吉田　眞	東京大学 名誉教授

事務局長

下村　正洋	株式会社ディアイティ

会員企業一覧　2013年2月現在　147社　50音順

【あ】

(株)アーク情報システム
(株)アークン
(株)アイ・ティ・フロンティア
(株)アイテクノ
アイネット・システムズ(株)
アイマトリックス(株)
アルテア・セキュリティ・コンサルティング
(株)アルテミス
アルプスシステムインテグレーション(株)
イーデザイン損害保険(株)
EMCジャパン(株)
株式会社イーセクター
伊藤忠テクノソリューションズ(株)
イルボンテ(株)
学校法人 岩崎学園
(株)インターネットイニシアティブ
(株)インテック
(株)インテリジェントウェイブ
インフォサイエンス株式会社
(株)インフォセック
ウェブルート株式会社
(株)AIR
エクスジェン・ネットワークス株式会社
SCSK(株)
SGシステム(株)　New
(株)エス・シー・ラボ
NRIセキュアテクノロジーズ(株)
NECネクサソリューションズ(株)
NHN　Japan(株)
NKSJリスクマネジメント(株)
エヌ・ティ・ティ・アドバンステクノロジ(株)
エヌ・ティ・ティ・コミュニケーションズ(株)
エヌ・ティ・ティ・コムウェア(株)
NTTコムテクノロジー(株)
(株)NTTデータ
(株)NTTデータCCS
NTTデータ先端技術(株)
F5ネットワークスジャパン(株)
オー・エイ・エス(株)
(株)OSK
(株)大塚商会

【か】

(株)Kaspersky Labs Japan
キヤノンITソリューションズ(株)
九電ビジネスソリューションズ(株)
京セラコミュニケーションシステム(株)
クオリティソフト(株)
グローバルセキュリティエキスパート(株)
クロストラスト(株)
(株)ケーケーシー情報システム
KDDI(株)
(株)コンシスト
CompTIA　日本支局

【さ】

(株)サイバーエージェント
サイバーソリューション(株)
(株)シー・エス・イー
CA Technologies
(株)JMC
ジェイズ・コミュニケーション(株)
JPCERTコーディネーションセンター
(株)シグマクシス
シスコシステムズ合同会社
システム・エンジニアリング・ハウス(株)
(株)シマンテック
(株)情報経済研究所
新日鉄住金ソリューションズ(株)
新日本有限責任監査法人
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム(株)
セコムトラストシステムズ(株)
ZTEジャパン(株)
ソニー(株)
ソフォス(株)
ソフトバンク・テクノロジー(株)
(株)ソリトンシステムズ

【た】

大興電子通信(株)
大日本印刷(株)
(株)大和総研ビジネス・イノベーション
タレスジャパン(株)

TIS(株)
(株)ディアイティ
デジタルアーツ(株)
(株)電通国際情報サービス
東京エレクトロン デバイス(株)
東芝ソリューション(株)
ドコモ・システムズ(株)
株式会社豊通エレクトロニクス
トレンドマイクロ(株)

【な】

西日本電信電話(株)
日信電子サービス(株)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム　システムエンジニアリング(株)
日本オラクル(株)
日本サード・パーティ(株)
日本セーフネット(株)
日本電気(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本ベリサイン(株)
日本マイクロソフト(株)
(株)ネクストジェン
(株)ネットマークス
ネットワンシステムズ(株)

【は】

パスロジ(株)
パナソニック(株)
(株)日立システムズ
(株)日立ソリューションズ
飛天ジャパン(株) New
(株)PFU
富士ゼロックス(株)
富士ゼロックス情報システム(株)
富士通(株)
富士通エフ・アイ・ピー(株)
富士通関西中部ネットテック(株)
(株)富士通ソーシアルサイエンスラボラトリ
(株)富士通マーケティング
フューチャーアーキテクト(株)
(株)ブリッジ・メタウェア
(株)ブロードバンドタワー

【ま】

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

【や】

(株)ユービーセキュア

【ら】

(株)楽堂
(株)ラック
リコージャパン(株)
(有)ロボック

【わ】

(株)ワイ・イー・シー
(株)ワイズ

【特別会員】

$(ISC)^2$　Japan
社団法人　コンピュータソフトウェア協会
ジャパン　データ　ストレージ　フォーラム
財団法人　ソフトピアジャパン
データベース・セキュリティ・コンソーシアム
特定非営利活動法人　デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院　工学系研究科
社団法人　日本インターネットプロバイダー協会
社団法人　日本コンピュータシステム販売店協会
特定非営利活動法人　日本システム監査人協会
特定非営利活動法人　日本セキュリティ監査協会
一般社団法人　日本電子認証協議会

JNSA 年間活動（2012 年度）

4 月	4 月 21 日、26 日	「Hardening Zero・Softening Zero」後援
	4 月 27 日	第 1 回幹事会
5 月	5 月 11 日	2012 年度理事会
	5 月 19 日～ 20 日	SECCON つくば大会（関東地区）
	5 月 23 日～ 25 日	「自治体総合フェア 2012」協賛
	5 月 24 日～ 26 日	「第 16 回サイバー犯罪に関する白浜シンポジウム」後援
	5 月 25 日～ 26 日	「学びのイノベーション&セキュリティフェア 2012」
	5 月 30 日～ 6 月 1 日	「ワイヤレスジャパン 2012」「スマートフォン / ケータイショップ EXPO」 「M2M クラウド EXPO」後援
	5 月 31 日	ISOG-J 主催セミナー「セキュリティ関連法律を学ぼう！！～ 改正不正アクセス禁止法と改正刑法（通称：ウイルス作成罪）について ～」
6 月	6 月 8 日	2011 年度 WG 活動報告会（ベルサール神田）
	6 月 8 日	2012 年度総会（ベルサール神田）
	6 月 12 日～ 15 日	「Interop Tokyo 2012」後援
	6 月 27 日	第 2 回幹事会
	6 月 29 日	第 10 回 関西情報セキュリティ団体合同セミナー
7 月	7 月 2 日～ 3 日	「ガートナー セキュリティ & リスク・マネジメント サミット 2012」後援
	7 月 3 日	第 2 回 鍵管理勉強会
	7 月 17 日～ 18 日	「SecureAsia@Tokyo2012 カンファレンス」後援
	7 月 25 日	節電環境における情報セキュリティ対策セミナー（大阪）
	7 月 27 日	JNSA WG 合同セミナー「セキュリティ事故の傾向とソーシャルメディアの 安全な使い方～最新の情報セキュリティ事情～」
8 月	8 月 8 日 他	「平成 24 年度情報モラル啓発セミナー」後援
		8/8 熊本、8/30 広島　他
	8 月 24 日	第 3 回幹事会
9 月	9 月 12 日	「平成 24 年度情報モラル啓発セミナー（香川）」後援
	9 月 19 日、21 日	「ID & IT Management Conference 2012」協賛
		9/19 大阪、9/21 東京　他
10 月	10 月 3 日～ 5 日	「Gartner Symposium/ITxpo 2012」後援
	10 月 5 日　他	「電子署名・認証業務普及セミナー」後援
		10/5 東京、10/26 名古屋　他
	10 月 12 日～ 13 日	「情報セキュリティワークショップ in 越後湯沢 2012」協力
	10 月 17 日	第 4 回幹事会
	10 月 24 日	NSF2012 in Kansai ～中小企業だからこそ BYOD を考えてみる～」
11 月	11 月 8 日	「ITGI Japan カンファレンス 2012」後援
	11 月 9 日　他	「電子署名・認証業務普及セミナー」後援
		10/9 横浜、11/22 大阪　他
	11 月 14 日～ 15 日	「PacSec 2012 セキュリティ カンファレンス」後援
	11 月 15 日	「2012 日韓情報セキュリティシンポジウム」（韓国ソウル）
	11 月 19 日～ 22 日	「Internet Week 2012」後援
	11 月 29 日	「OGC シンポジウム 2012」後援
	11 月 30 日～ 12 月 2 日	「かごしま IT フェスタ 2012」後援
12 月	12 月 1 日	産学情報セキュリティ人材育成交流会～インターンシップを考える～」
	12 月 4 日	第 5 回幹事会
	12 月 7 日	「電子署名・認証業務普及セミナー（東京）」後援
	12 月 10 日～ 11 日	「デジタル・フォレンジック・コミュニティ 2012inTOKYO」後援
	12 月 13 日	PKI day 2012
	12 月 14 日	「フィッシング対策セミナー 2012」後援
	12 月 22 日	SECCON 横浜大会
1 月	1 月 25 日	Network Security Forum 2013、JNSA 賀詞交換会・表彰式
2 月	2 月 5 日	第 6 回幹事会
	2 月 6 日～ 8 日	「page2013」協賛
	2 月 28 日～ 3 月 1 日	「Security Days」後援
	2 月 28 日～ 3 月 2 日	「情報セキュリティシンポジウム道後 2013」後援
3 月	3 月 2 日	第 5 回全国情報セキュリティ啓発シンポジウム 「インターネット安全教室 in ソラマチ」

2012 年 4 月～
2013 年 3 月
「インターネット安全教室」
開催

2012 年 8 月～
2013 年 2 月
「平成 24 年度中小企業向け
指導者育成セミナー」
開催

会員紹介（当コーナーでは、JNSA で活躍されている会員の方に、リレー方式で自己紹介をしていただきます。）

株式会社ディアイティ　青嶋　信仁

JNSA 会員の皆様、はじめまして。株式会社ディアイティの青嶋と申します。

この度、三井物産セキュアディレクション株式会社（MBSD）さんから紹介を受け、本コーナーの執筆を担当することとなりました。

私は、現在、情報漏えい対応およびサイバー攻撃対応を中心に活動をしています。ネット掲示板やP2Pの監視サービス、コンピュータやネットワークの解析サービスや解析の教育の提供を行っております。実際に顧客で発生する事件は、想像できないこともよく起こるため、現場で正しい判断や行動が短時間でできるように、広く経験や考えを身に着けることに努力をしています。また、新しい脅威が次々と生まれるなか、脅威の中にわざと飛び込んだり、経験したりして、それをもとに、より実践的な対応ができるようなことも行っています。

JNSAにおいては、過去、いくつかのイベントにスポット的に参加してきましたが、昨年の秋からISOG-Jに継続的に参加しております。まだ、情報を受ける中心ですが、今後、お役にたてるように活動に協力をしていきたいと思います。

私事で恐縮ですが、私にとっての最大のセキュリティ事件は、2013年1月、過去隠し通してきた、へそくり用の通帳を家のものに見つけられ、中身を見られてしまったことです。今後、このような悲惨な事件がおきないように、偽装の通帳の準備の検討やどのように隠せるかの工夫や相手の考え方の弱点についての発見と、仕事と同様に頭を悩ましています。

趣味は、ネット遊びと街歩きと飲食店の開拓ですが、最近は、腰を痛めたり、へそくりが使いにくくなったためと老後を考えて、趣味の変更を検討中です。参考にあるようなことがあれば、教えてもらえればと思います。

会員紹介

株式会社イーセクター　清水　聡史

JNSA会員の皆様、はじめまして。

今回本コーナーの執筆を担当することになりました株式会社イーセクターの清水と申します。

弊社は、株式会社シーイーシーのグループ会社として、「情報セキュリティを通じて人々に安心を提供する」という理念のもと、セキュリティソフトウェアの販売を業務としている会社です。

JNSAには昨年より参加しているのですが、この度個人として初めてWGに参加することになり、JNSAとの関わりを深めたいということで自己紹介の機会を頂きました。拙い文章ではございますが、ご一読頂けますと幸いです。

私は、パートナー企業やエンドユーザ企業の御客様に対して、様々なセキュリティの問題に対応できる「パッケージソフトを活用したソリューション」を企画提案する仕事をしております。

御客様のご要件は、ネットワークからWebサーバーへの攻撃対策、そして最近話題になっているスマートフォンのセキュリティ対策など多岐に渡りますので、日々勉強しながら業務に取り組んでいる毎日です。

今回JNSAの中ではセキュリティ市場調査WGに参加いたします。セキュリティの市場がどのように動いているのか、を調査し把握することは業務に活用ができる情報にもなりますので、参加がとても楽しみでもあり、一方で非常に緊張もしております。積極的にWGに参加し、少しでもJNSAの活動に貢献できればと考えております。

最後に趣味について少しお話させて頂きます。

私の趣味はマラソンです。昨年太ってしまったためとりあえずで始めたのですが、ハーフマラソンの大会に出るまで成長し、先日も西東京の横田基地の中を走る「横田フロストバイトロードレース」に参加し、無事完走してまいりました。ゴール直前は本当に苦しく、「なんでこんな事をお金を払ってやっているのか。」と毎回思うのですが、ゴール後の充実感とその後のお酒の美味しさは他では得難いものがあり、何とか継続しております。

このマラソンというスポーツですが、本当に自分との闘いで、自分さえ許してしまえばいくらでも手が抜けてしまいます。その中で自分の目標とするタイムを目指し、苦しくも手を抜かず頑張る、ということは仕事にも通じる部分がある、と感じております。

JNSAの活動でも高き目標を持って望みたいと考えておりますので、会員の皆様、どうぞよろしくお願いいたします。

JNSA について

■会員の特典

1. 各種部会、ワーキンググループへの参加
2. 会員勉強会への参加
3.「JNSA ソリューションガイド」
（製品・サービス紹介サイト）への情報登録
4. JNSA 会報の配布（年 2 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・報告書元データの提供（会員限定）
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

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
〒 105-0003 東京都港区西新橋 1-22-12 JC ビル 3F
TEL：03-3519-6440
TEL：03-3519-6441
E-Mail：sec@jnsa.org
URL：http://www.jnsa.org/

西日本支部
〒 532-0011 大阪府大阪市淀川区西中島 5-14-10
サムティ新大阪フロントビル（株）ディアイティ内
TEL：　06-6886-5540

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

JNSA Press vol.35

2013 年 3 月発行

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）
E-Mail: sec@jnsa.org　　URL: http://www.jnsa.org/

印　刷
プリンテックス株式会社

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

〒105-0003 東京都港区西新橋1-22-12 JCビル 3F
TEL 03-3519-6440　FAX 03-3519-6441
E-mail: sec@jnsa.org　URL: http://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島5-14-10 サムティ新大阪フロントビル（株）ディアイティ内
TEL 06-6886-5540