JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

AUTUMN 2011 VOL. 32

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

今後の情報社会とJNSA

情報セキュリティ大学院大学 研究科長 教授
会長　田中英彦

情報セキュリティは、従来、その重要性が様々なところで語られて参りました。また、各社では様々な施策が講じられ、様々なセキュリティ製品も開発されて参りました。それに伴って、一見、対策は十分なされてきたようにみえます。

しかしながら、情報セキュリティ対策と脅威は追っかけっこの様相を呈しておりますし、人間のやることですので、浜の真砂と同様、情報セキュリティに完成は無いようにも思います。

昨今、公的機関からの情報漏洩、グローバル企業からの大規模漏洩などもマスコミの話題になりましたが、それらをみると情報セキュリティを護る基本がまだまだ常識にはなっていないように思います。殆どのシステムは安全であると言っても、一か所でも不十分であればそこが弱点になりますし、グローバル企業は各国での文化や遣り方に応じた対策も必要です。

また、最近、情報セキュリティはグローバル問題であるとともに、社会問題であるという側面が強く出て参りました。セキュリティへの攻撃をかける目的も、以前は興味本位から、その後、お金を取る専門家として攻撃をかける職業へと変遷し、最近は、企業のやり方が気に入らないという理由からとか、公的情報 のあり方に関する信念からとか、更には国がその攻撃に関与している可能性すら出て来ています。

一方、ITが発達しFacebook等のSNSが普及するに連れ、個人に関わる情報が容易に取得できる状況になった結果、それら膨大な情報を集めて分析に使い、例えば生命保険や銀行で、その人の知らない所で個人の評価に利用することが始まっております。

これは単なるプライバシの問題ではなく、もっと根本的な問題を内包しており、ITは便利である反面､大きな社会問題を孕んでいると考えられます｡このような状況にあって、情報セキュリティを担保し情報 社会を健全に発展させることは大変重要な課題で、私たちのビジネス・生活の依って立つベースであります。

JNSAは､我が国の情報セキュリティを護る企業の先駆的な集まりとして､これまで様々な活動を通じて我が国の情報セキュリティに貢献して来ました。

特に、実務的で社会に根差した活動には素晴らしいものがあり、広く使われている統計情報を提供したり、また様々なノウハウ集、対処手法などを関係者が知恵を寄せあって作る、最近課題のワークショップや勉強会、更には情報セキュリティの啓発セミナを開催するなど、広範で活発な活動があり、今後とも社会のJNSAに対する期待は大変大きなものがあります。

私も、JNSA並びにセキュリティ業界の発展に努力致す所存ですので、是非、皆様、今後ともそれぞれの力を持ち寄り、共によりよい情報環境を作りあげようではありませんか。

リスクの可視化から見直す情報漏えい対策

セコムトラストシステムズ株式会社
後藤　忍

はじめに

本年4月に同一企業グループで発生した情報漏えい事案は大きな話題になりました。３月に発生した大震災による原発の放射能漏れに続いての事であり、上半期を一文字で表すと「漏」であると言う人もいます。情報漏えい事案発生以降、多くの企業が、類似事案防止の観点からインターネット網と社内ネットワークの接点に生じる脅威への緊急対策を実施し、外部公開サーバのセキュリティ診断の需要が高まっています。しかし、今回の事案に対して、インターネット経由での攻撃を防げばよいといった一面的な捉え方をするのではなく、水が高い所から低きに流れるがごとく最も弱いポイントが破綻したと捉えるべきです。そして誰しもが「わが社は本当に大丈夫か？」と懸念を抱いた今こそ、インターネット経由の脅威に加え、情報漏えいが発生する可能性をすべて洗い出し、自社にとって最も弱いポイントを見極めた上で次の一手を打つべきであると考えます。その為には、リスクの所在について網羅性をもって明らかにする所からはじめる必要があり、リスクを判りやすく可視化する手法についてご紹介します。

１．企業の情報漏えい対策

企業の重要情報（顧客データ等）が格納されているデータベースはよく金庫に例えられます。
サーバは金庫室であり、サーバにアクセスできる端末環境は金庫が設置されているビルの入り口といった具合です。リアルの世界ではオフィスビルの一階にゲートが設けられているのをよく見かけるようになりました。又、顧客情報、重要システム、バイタルレコード等の保管室等はセンサーで監視し、異常を検知すると直ちに警備員がかけつけます。さらに権限のない者が仮に侵入したとしても、外に出ることができないアンチパスバックというシステムもあります。

サイバーの世界で同じ仕組みがあったとすると、データベースへのアクセスは何重ものセキュリティシステムで守られており、データベースのどのデータに誰がいつアクセスしたかはすべてリアルタイムに監視され、異常があればセッションを切った上にネットワーク経由で犯人を追跡するといった具合になります。

しかし、このようなシステムを実現している企業は現実的には皆無でしょうし、現在の企業のセキュリティ対策は江戸時代の関所に似ていると感じます。関所は江戸時代に「入り鉄砲に出女」というポリシーで、国内治安維持を目的として運営されていました。江戸から出る婦女は関所を通過する際、乗物の戸を開き、笠頭巾を取り、手形を提示し、改女に入念に調べられました。また、江戸に入る鉄砲は火薬や弾丸含めて厳重な取り締まりを受け、長持なども中に武器がないか調べられました。逆に江戸から出る武器についてはまったく取り調べがなかったといいます。

関所と改女はサイバーの世界のFirewallとWAF（Web Application Firewall）を連想させるのですが、このように単層のラインを設け、そこで出入りを監視しコントロールをするという方式が企業の情報漏えい対策の主流であったように思います。そして昨今は単層の関所方式の限界が指摘され、例え侵入されたとしても重要情報が外に漏れないよう多段防御によるインターネットの出口対策についてさまざまなアイデアが出てきています。

その一方で、外部の委託先や取引先との接点及び社員や社内常駐している派遣社員からの漏えいなどインターネット経由を除いた脅威についての対策は、企業の現場に赴くとまだまだ取組みが不十分であるという印象を否めません。対策を実施しているとか、していないではなく、課題としてすら挙げられていないというケースがよく見られます。

たまたまガンブラーなどの流行で外部委託先からのアクセスが課題になったり、USB利用禁止などの部分的な対策を行っている事でよしとしているとい

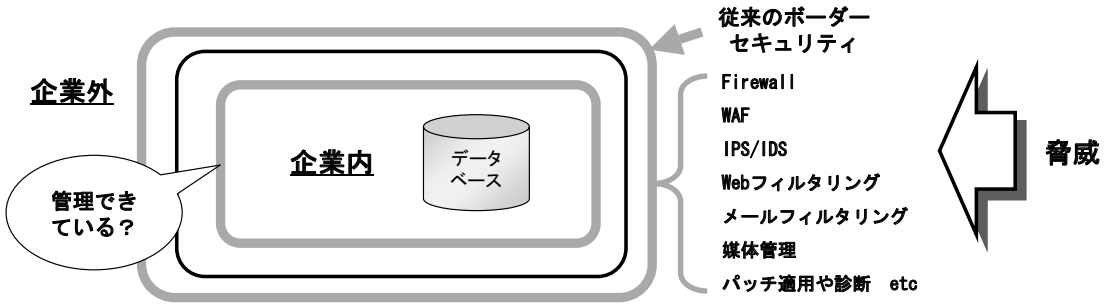


図1　脅威への対策の概念図

うのが実状であり、企業のセキュリティにおいて内部ネットワークやインターネット以外のポイントは「社員だから大丈夫」とか「長年、お付き合いのある委託先だから」「インターネットの口さえ守れば大丈夫」などの思い込みにより、対策がおろそかになっているのではないでしょうか。この部分に光を当て、内外すべての脅威を明らかにしないと本当の意味で情報は守れません。次項からはこのようなリスクをいかに洗い出すかという点について述べます。

2．リスク洗い出しの方法論

前項で情報漏えいの可能性を網羅的に把握すると述べましたが、リスクの把握に参考となる手法として幾つかのモデルがあります。NIST Risk Management Guide for Information Technology Systems（SP 800-30）、ISO/IEC 21827（ISSEAが開発したセキュリティエンジニアリングプロセス評価モデル）、ISO/IEC TR 13335（GMITS）などがそうです。SP 800-30は情報のオーナーやITシステムオペレーションの運用に関する最終決定者（Designated Approving Authority）、情報システムのセキュリティ責任者や経営者など幅広い層をターゲットにしたガイドラインです。リスクアセスメントのステップは次のようになっています。

- **Step 1**　System Characterization（システムの特徴の把握）
- **Step 2**　Threat Identification（脅威の特定）
- **Step 3**　Vulnerability Identification（脆弱性の特定）
- **Step 4**　Control Analysis（管理策の分析）
- **Step 5**　Likelihood Determination（発生可能性の決定）
- **Step 6**　Impact Analysis（インパクト分析）
- **Step 7**　Risk Determination（リスクの決定）
- **Step 8**　Control Recommendations（管理策の決定）
- **Step 9**　Results Documentation（文書化）

Step 1 System Characterization（システムの特徴の把握）では、システムの機能、システム及びデータの重要性や機密性を定義します。リスクアセスメントをはじめるにあたっての基礎データの収集です。次に**Step 2** Threat Identification（脅威の特定）でさまざまな脅威を洗い出します。例えば人的な脅威については、ハッカーやクラッカー、金銭取得等を目的とする犯罪者、テロリスト、産業スパイ、従業員（退職者を含む）に分け、それぞれにThreat Action（脅威の行動）を定義していきます。この際、挑戦や脅迫などといったMotivation（動機）にも着目せよとありますが、あまり詳細なステップは記載されていません。

Step 3 Vulnerability Identification（脆弱性の特定）は、NISTが公開している脆弱性データベース

（http://nvd.nist.gov/home.cfm）やベンダーが公開している脆弱性、脆弱性スキャンツールからの情報、ドキュメントレビューやオンサイトでのヒアリングを用いて、Threat-Source（何が？）とVulnerability（どのような脆弱性をついて）とThreat Action（どのような攻撃をする）の組み合わせ表（表1）を作成します。この組み合わせ表を用いてのリスク分析は通常よく行われていると思います。

Vulnerability	退職した従業員のIDがシステムから削除されていない。
Threat-Source	退職した従業員
Threat Action	企業のネットワークにダイアルし、機密データにアクセスする。

表1　脆弱性と脅威の組み合わせ

Step 4 Control Analysis（管理策の分析）で対策の検討を行います。その後、Step 5 Likelihood Determination（発生可能性の決定）でThreat-Sourceに強い動機があるか？及びStep 6 Impact Analysis（インパクト分析）で脅威が顕在化した場合の影響の大きさは？といった対策の優先順位付けの為の評価を行い、Step 7 Risk Determination（リスクの決定）以降でリスクの定量化→コントロールと代替コントロールの検討→リスクアセスメント報告書の作成をもってリスクアセスメント*が完了します。

これらの一連の手順での分析は有効であり、実際に利用されている組織もあると思います。しかし、Step 2 Threat Identification（脅威の特定）とStep 3 Vulnerability Identification（脆弱性の特定）についてもう少し詳細な手順を付け加えると、よりリスク洗い出しの網羅性を担保できるのではと考え、次項にそのステップについて記載します。

3.アクセス経路別のリスクの洗い出し

前述のように情報漏えい対策の網羅性を高める為には、脅威と脆弱性の洗い出しフェーズの精度に拠ります。よってもう少し詳細なステップを当該フェーズに付け加えることにします。

例えば物理的なセキュリティリスクの洗い出しの場合は人が動く導線を想定し、ゾーニングと併せてチェックを行いますが、それと同様にデータベースへの社内外からのアクセス経路、いわば情報の導線を特定し、経路別に脆弱点がないかをチェックするのです。

あるECサイトのデータベース内の情報を例に、アクセス経路別に分析を行なうステップについてご紹介します。

ステップ1
リスク洗い出しのスコープの決定

リスク分析を行なう範囲を決定します。（※ここではECサイトのシステムの内部セグメントにあるデータベースとします。）

ステップ2
データベースにアクセスする業務の洗い出し

まず、関係する業務をすべて洗い出します。業務から洗い出す事により、確実に簡単にデータベースのアクセス経路等の情報収集ができます。
例）コンテンツメンテナンス業務、コールセンター業務、システムメンテナンス業務等

ステップ3
データベースにアクセスする業務詳細の確認

ステップ2で業務を洗い出した後、業務を行なう拠点、業務を行なう社員や派遣社員の特定（Threat Sourceに相当）を行ないます。

ステップ4
データベースへアクセスするすべての経路及びその他のデータ伝送経路の特定

業務単位で、遠隔地の拠点からのアクセス経路、遠隔地の外部委託先からのアクセス経路、緊急メンテナンスの為の自宅からのアクセス経路、データセンターのメンテナンスルームからのアクセス経路、インターネット経由（会員のPC）というようにすべての経路を図2のように洗い出していきます。

＊リスクアセスメント：リスク分析からリスク評価までのすべてのプロセス(JIS TR Q 0008:2003)」

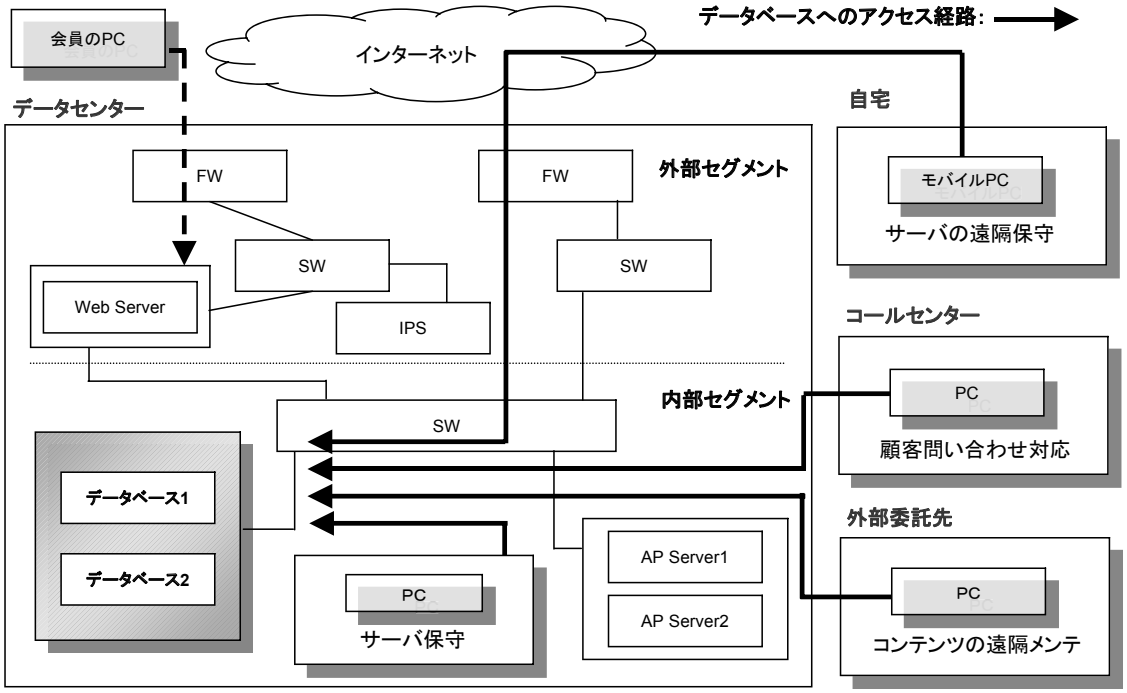


図2　データベースへのアクセス経路図の例

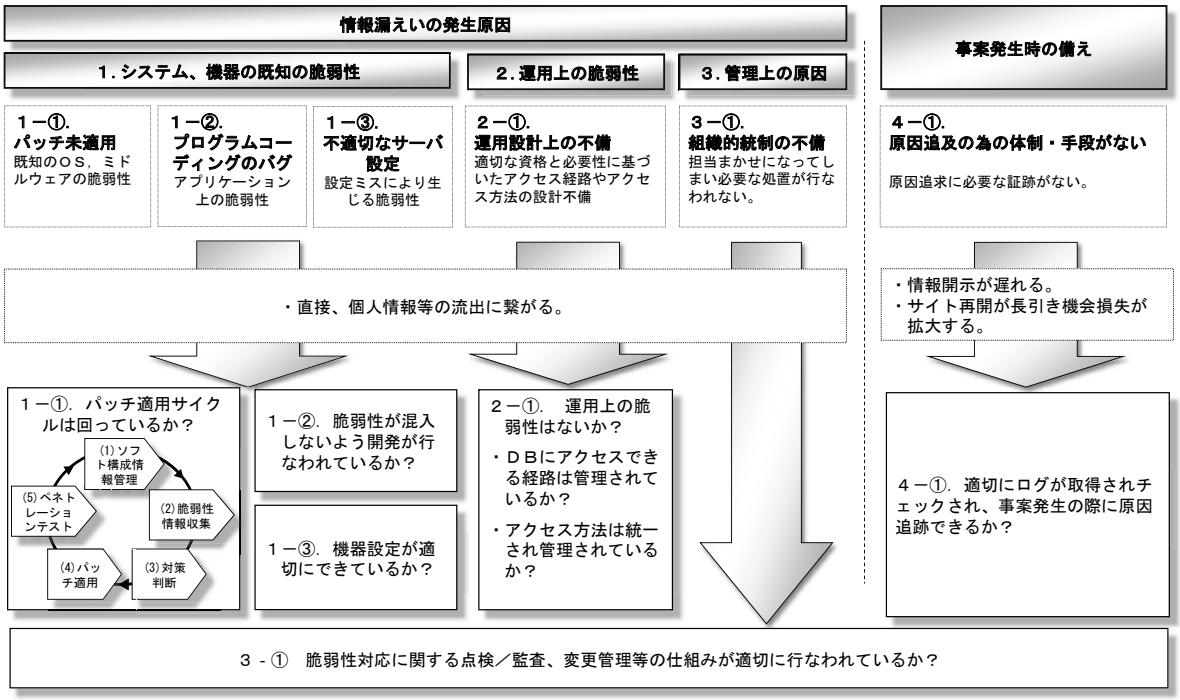


図3　情報漏えいの発生原因分類と分析のポイント

ステップ5
データベースへのアクセスの詳細確認

ステップ4とほぼ並行してアクセス経路別に誰が、いつ、どのような方法(ツール等)を用いて、どのようなデータにアクセスするかの組み合わせを特定します。データベースにアクセスする端末が設置されている部屋の入退室管理の内容や監視カメラのログの取得期間などのチェックも必要です。

ステップ6
アクセス経路別に脅威と脆弱性の洗い出し

脅威と脆弱性の洗い出しは、図3に示す情報漏えいの発生原因を念頭に置いて行ないます。図3の上段の1－①～3－①までが、直接個人情報等の重要情報の漏えいに繋がる原因です。これらに起因したどのような事案が自社に発生するかを洗い出します。

4－①は事案発生時、被害拡大に繋がる原因です。例え事案が発生しても早期に原因究明でき、情報開示およびシステム再開ができる備えが必要です。サイバーの世界ではリアルな世界と違って現行犯逮捕はできません。ログの取得を前提として、ログの解析等の対応については予め手順化されている必要があります。いざとなって慌てるようでは遅きに失するので、見落としてはいけないポイントです。

指摘しておきたい点として、脆弱性洗い出しの粒度があります。図3 1－①パッチ未適用を例にとると、図4のような脆弱性解消の為のパッチ適用のステップ(あるべき姿)に着目します。それぞれのステップが確実に実施されているか？実施されていないとしたら何が問題なのか？というような粒度で分析を行っていきます。パッチを適用しているか否かといった単純なベースラインによるチェックでは本質的な問題にたどり着かないからです。経験上、パッチ未適用の多くは技術的な問題の前に人的運用の問題が存在することが多いと考えられます。

このようにアクセス経路別に詳しく分析していくとよく見つかる脆弱性についてご紹介します。

(1) データベースのデータ参照制限を設けておらず、業務担当者がSELECT ALLで業務に必要のないすべての顧客情報(ID、パスワード、カード情報)を参照できてしまう。

(2) INSERT,UPDATE,DELETEに限定したデータベースログしか取得していない為、誰がいつどのようなデータを参照したか証跡がなく、事案発生時の原因追求が難しい。

(3) データベースにアクセスする端末で利用している独自ツールのログに、参照データ(個人情報など)が平文で保管されている。このように管理者が認識していない場所に重要データが保管されているケースがある。これでは、データベースだけを守っても意味がない。

これらの脆弱性はアクセス経路別に逐一精査し

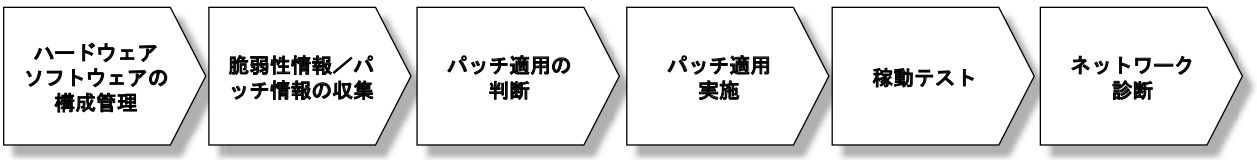


図4　パッチ適用のステップ

No.	アクセス					リスク	リスク詳細	改善策	区分
	拠点	部署	端末	手段	人				
1	本社オフィス	システム部	業務用PC	SQL-plus	パートナー30名	不正持出し	クレジットカード番号関連情報をデータベースから抽出し、業務用PCから印刷することによって不正に外部へ持出せてしまう。	クレジットカード番号情報のデータテーブルを暗号化する。	漏えい防止
2					社員5名	同上	社員はSQL-plusで抽出した情報をメールに添付して外部に送ることができる。	・メール監視システムを導入する。 ・データテーブルを暗号化する。	漏えい防止
3				FTP	社員5名	不要なサービスが有効	DBログにカード情報が平文で格納されており、FTPによりログファイルを取得する事ができる。	・DBログは直ちに他の要塞化したログ収集サーバに退避する。	漏えい防止
4				-	社員5名 パートナー2名	情報漏えい原因の特定が行えない	SELECT操作ログまでは取得されていないため、情報漏えい時に原因の特定が行えない可能性がある。	特定の行や列に対する SELECT を監査出来るファイングレイン(FGA)監査ログを取得する。	事後対策

表2　本社オフィスからデータベースにアクセスする経路のリスク分析の例

ないとなかなか気付かないポイントです。上記の表2のようにまとめ、データベースへのアクセス経路図(図2)と紐づければ、誰が担当している業務のどこにどのような脆弱性があるかを判りやすく可視化できます。

これでStep 2　Threat Identification(脅威の特定)とStep 3 Vulnerability Identification(脆弱性の特定)の部分をより効果的に実施していく事ができ、漏れなく改善すべきポイントを拾い上げることができます。このような作業を基点として、SP800-30のStep 4 Control Analysis(管理策の分析)以降の対策の決定および対策の優先順位付けへと繋げていきます。

アクセス経路別のリスク洗い出しの利点について、可視化と網羅性の確保以外にもう一つ付け加えておきます。例えばチェックリストを用いて監査を実施する場合、チェック項目毎に○：実施、△：一部実施、×実施していないなどのように合否チェックを行いますが、対象は漠然とサーバ全体、ネットワーク全体、端末全体とグループ化してチェックしているのが一般的です。

目的によりこのような粗い粒度のチェックも有効ではありますが、誰が何を改善すればいいのか判りやすく可視化するという点においては、拠点別、部門別にやるべき事を明確に整理できるアクセス経路別の分析は都合が良いと考えます。

アクセス経路別のリスク洗い出しを実際にやってみて判ることは、往々にして情報漏えい対策の対応がもぐら叩きになってしまっているという事です。当初システムを開発した担当者がいなくなり、アクセス経路やアクセスできる権限などの設計の考え方も明文化されておらず、そのシステムのセキュリティには疑問を抱かず日々運用がなされています。
改めてセキュリティ品質をシステム及びシステム運用のライフサイクルに練りこむような品質保証体制が必要と感じます。

4．最後に

過去の経験を振り返りますと企業のシステム及

び運用は、十分にセキュリティを考慮して設計されてはおらず、可用性偏重になっているものが多く見受けられました。パフォーマンスが気になるからとデータベースのログは取らず、運用に便利だからと過剰な権限を社員や委託先に付与しがちです。

「去るものは日々に疎まれ生ける者は日々に親しむ」という中国の詩があります。人は目の前からいなくなると忘れ去られてしまうという意味であり、人は見えないものには注意を払いません。システムや運用上のセキュリティ品質はシステム停止に繋がる品質と違って通常目に見えることはありません。日々に疎まれ、システム責任者や経営層は知る由もないのが実状ではないでしょうか。

しかし、それらはやがて情報漏えい事案という大きなインパクトをもって顕在化する可能性をはらんでおり、今が過日発生した大きな情報漏えい事案を他山の石とし、セキュリティリスクの総点検を行なう良い機会であると思います。是非、情報漏えいへの取組みを日々に親しむものにしていただきたいし、我々もそうなるように益々励んでまいります。

（参考文献）

「セキュリティはなぜやぶられたのか」ブルース・シュナイアー著、井口耕二翻訳　日経ＢＰ社

「関所　その歴史と実態」大島延次郎著　新人物往来社

「ネットワークセキュリティHACKS　プロが使うテクニック＆ツール　100+」Andrew Lockhart著、渡辺勝弘、鶴岡信彦、黒川原佳訳　オライリー・ジャパン

「今、必要な情報セキュリティマネジメント」村田一彦著　ジャストシステム

「ＩＴリスクの考え方」佐々木良一著　岩波新書

National Institute of Standards and Technology「Risk Management Guide for Information Technology Systems」（Special Publication 800-30）Gary Stonebumer,Alice Goguen,and Alexis Feringa
http://csrc.nist.gov/

迫りくるネットワークセキュリティのパラダイムシフト 注目を集めるネットワーク仮想化技術と OpenFlow/SDN

東京エレクトロン デバイス株式会社　ビジネス・デベロップメント部
水本　真樹

はじめに

先の東日本大震災を契機として、いま企業ではクラウド環境にITインフラを移行しようという流れが加速している。災害に備えたBCP（事業継続計画）の観点から、ビジネスの価値の源泉であるシステムを自社内のオンプレミスな環境で稼働させるのではなく、堅牢なデータセンターに移すことで、その安全性の確保を図ろうというのがそのねらいだ。

その一方で、こうしたクラウド環境へのニーズの高まりは、かねてより指摘されてきたセキュリティに関する懸念を改めて顕在化させている。具体的には、企業がこれまで自社内のオンプレミスの物理的な環境で確保していたのと同等のセキュリティを、仮想化技術を基盤とするクラウド環境においていかに確保するかが重要な課題として指摘されている。

そうした課題を解消するためには、特にネットワークにおいて、パラダイムシフトともいうべき技術革新が不可欠だといえる。ここでは、今後、企業の主要なITの利用形態になると目されるハイブリッドなクラウド環境において、セキュリティの担保に貢献するものとして注目されるネットワーク仮想化技術を取り上げ、その最新の技術動向と関連する業界の動きにもスポットを当てたい。

クラウド環境における ネットワーク仮想化の必然性

周知の通り、クラウド環境においては、サーバやストレージなどの物理リソースを隠蔽して分割利用する仮想化技術を基盤に様々なサービスが展開されている。近年、そうしたサーバやストレージに関する仮想化技術が急速に進化を遂げ、例えば物理的には1台のサーバを複数台のように扱ったり、複数のストレージを1つにまとめてその領域を分割するといったことが可能となっている。

これに対しネットワークの仮想化はというと、20年以上も前から利用されているVPNやVLANがいまだ現役であり、サーバやストレージの仮想化が提供する柔軟性や拡張性と比較し、それは極めて限られたものでしかないというのが実情だ。

今後、企業システムは、単一のクラウドからプライベート／パブリック間の相互連携、あるいはプライベートネットワークとクラウドの相互接続へと進化していくことが想定される。そうした環境にあって、ネットワークセキュリティを担保しながら、仮想化やアプリケーション分散化といったクラウドの提供する付加価値を享受するためには、サーバリソースやストレージリソースを含むインフラをトータルに仮想化するネットワーク仮想化技術が不可欠だといえる。

ネットワーク仮想化技術とは、端的に言うなら、スイッチやルータといった物理ネットワーク機器のリソースをアプリケーションなど上位プロトコルに対して隠蔽する技術だ。その利用により、クラウドネットワークの上に仮想化のレイヤを設けることで、ユーザーの要求に応じて、ネットワークやサーバ、ストレージなどのリソースを仮想的なスライスとして提供するということが可能となる。

現在のところ、大規模なネットワークを物理的に共有しながら、トラフィックについての分離を行って論理的なセキュリティを担保するための仕組みとしては、クラウド基盤環境においてもVLANが広く利用されている。複数のVLANを通過させるためにトランクポートを設定し、ユーザーごとに論理的に分割するための識別情報としてタグIDを付加して動作させるという形である。

しかし、こうした方法では、クラウド環境で提供されるプロビジョニングのメリットが十分に活かし切れないという問題がある。具体的には、プロビジョニングによって動的に追加されたサーバをいざネットワークに接続するとなると、ネットワーク管理者が各種設定や物理接続などを手作業

で変更する必要があり、相応の手間と時間を要するわけだ。このように仮想化によってモビリティを増したサーバ環境に対し、ネットワーク側がいかに追随していくかが重要な課題として浮上してきており、そうした課題を解消するものとして期待が寄せられているのがネットワーク仮想化技術だというわけである。

新たな設計思想に基づく ネットワーク技術の登場

そうしたネットワーク仮想化を支える技術として、最近、とりわけ注目を集めているのが「OpenFlow」だ。これは「ソフトウェア定義ネットワーク（Software Defined Network : SDN）」に基づくもので、SDNでは一元的に管理を行うコントローラがスイッチやルータなどの機器に対してソフトウェア的に指示を出すことで、フロー制御等の設定が可能になる。OpenFlowでも、フローテーブルを機器側に保持し、リモートでその内容をコントロールできるようになっている。

OpenFlow登場の背景には、既存技術に捉われない新たな設計思想・技術に基づいてインターネットのアーキテクチャを根底から考え直そうとする動きがある。例えば、現在、規格策定が進められている、「NWGN（NeW Generation Network）」や「FI（Future Internet）といった次世代ネットワークへの取り組みもこれにあたり、これらは現在のIPとは異なる技術に基づいて設計されるクリーン・スレート・アーキテクチャである。これらの技術の研究開発は、すでに実証フェーズを迎えている段階で、2020年頃には標準化が見込まれている。

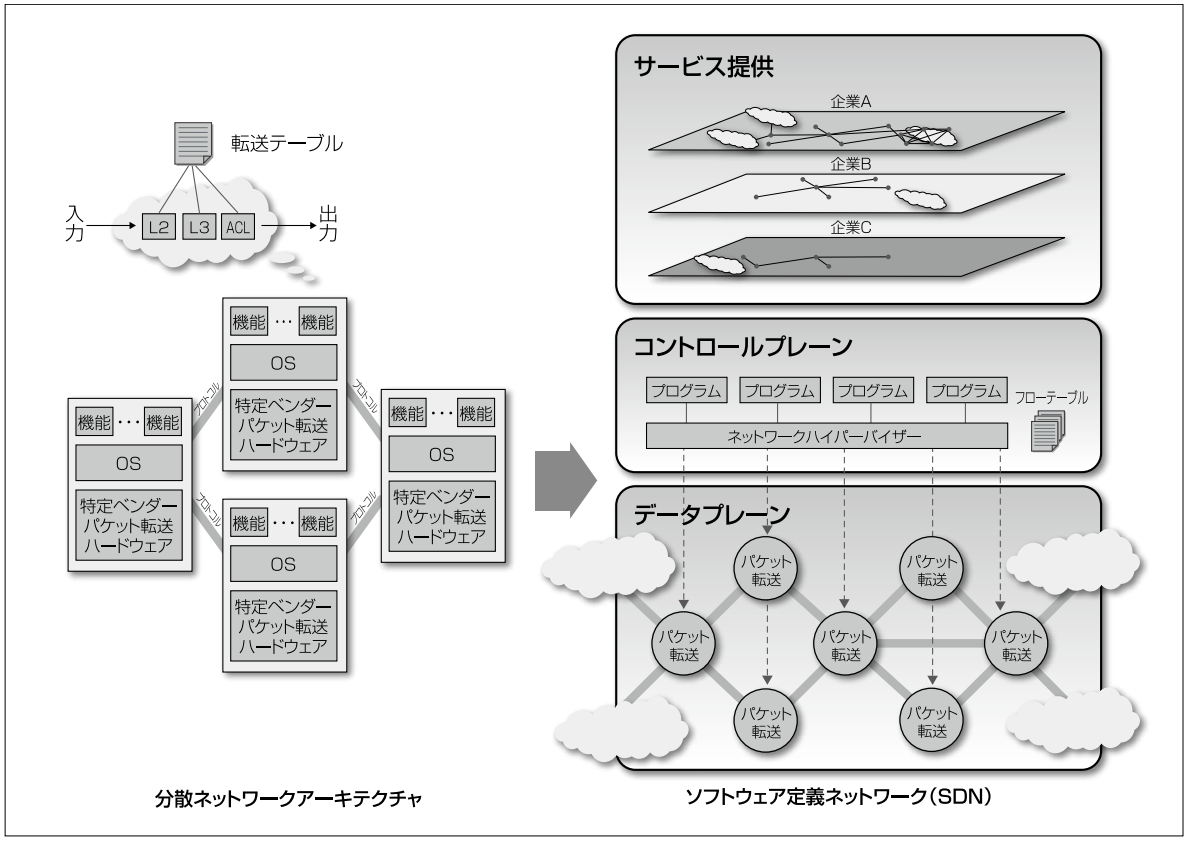


図1　ネットワーク仮想化で具現化する次世代インフラストラクチャ

日本においても様々な実証が進められている。

OpenFlowは、まさにそうした次世代ネットワークに向けた取り組みの中から生み出されたものである。その特徴は、入力ポートとMACアドレスやIPアドレス、ポート番号などの組み合わせによるフローエントリベースでネットワーク制御を行うことができる点と、セキュアチャンネル経由でコントローラからリモート制御ができる点で、通信品質の確保やネットワークの利用効率の向上などが期待されている。

OpenFlow仕様の最初のドラフトを作成したMartin Casadoによると、開発のきっかけはこれまでのネットワークは設計者が直面する様々な問題に対し対応できないことは明確だったためだということだ。コンピュータと異なり、ネットワークは強固なセキュリティを確保するためにプログラム化をすることができなかった。そのため運用者がセキュリティポリシーを適用しなければならなかったが、これは対応の遅れや事故やエラーの原因となる。彼がきっかけとなり、Stanford大学を始めとした同じ思いを持つコミュニティの力によってネットワークセキュリティに大きな転機が訪れようとしている。OpenFlowはWANや巨大なデータセンター、ネットワーク仮想化、モビリティ、non-IPネットワークなどに有効な解決策を提供していくだろう。

現在OpenFlowの推進には、ユーザー主導による新たなネットワーク技術の策定を目指すONF（Open Networking Foundation）が当たっており、この団体にはGoogleやYahoo、Facebookといった米国の主要なユーザー企業のほか、ネットワーク機器を提供する主要ベンダーなど44社も参加している。余談ではあるが、こうした構造からは、ONFがインターネットに関する標準化を行うIETF（Internet Engineering Task Force）と同様の役割を、NWGNやFIといった次世代ネットワークの分野で担おうと画策しているものとも考えられる。

OpenFlowをめぐっては、現状ではまずIP上に適用するという取り組みが進められており、データセンター内のサーバ間接続の用途に向けた製品などがすでに市場投入されている。SDNアーキテクチャに基づく製品自体は、かねてより各ネットワーク機器ベンダーから提供されてきてはいるが、その利用にはすべてそのベンダーの製品で統一しなければならないといった問題がある。これに対しOpenFlowは、その設計技術がオープンになっており、OpenFlowの仕様をサポートする複数のメーカーのコントローラやスイッチなどを自在に組み合わせて利用することが可能である。例えば、OpenFlowコントローラを開発している米国Nicira Networksなどは、オープンソースでOpenFlowに対応している分散仮想スイッチ「Open vSwitch」や、スイッチ提供メーカーとの提携を模索しているようである。

こうしたOpenFlowコントローラで制御できるフローを利用すれば、複数の物理スイッチや仮想スイッチで構成される仮想化環境において論理ポートや論理スイッチを構成することができる。これにより、例えば、プライベートネットワークにおいてアプリケーションの要求に応じる形で、ネットワークを仮想的に分割してシステム利用者に提供するといったことも可能になる。様々なセキュリティサービスを統合化したり、セキュリティポリシーをプログラマブルに適用する分散ファイアウォールや統合セキュリティシステムを開発できる可能性も広がる。注目されつつあるCloudStack、OpenStackなどのクラウド管理システムを起点に、ハイブリッドクラウドやクラウド間ネットワークを統合する動きも出てきている。

ライブマイグレーション実行時のネットワーク側の課題を解消

一方、冒頭でも触れた、震災を契機に加速している企業におけるBCPの取り組みにおいても、ネットワーク仮想化が持つ意義は大きい。一般にBCP

対応では、システムを広域分散させて冗長化することで、有事に際して速やかなサービスの回復を図ることになるが、そうした対策を効果的に支援する技術にライブマイグレーションがある。これは、仮想マシン上のサーバOSやアプリケーションを、稼働させたまま別の物理サーバ上に移動するというものだ。

ただし、ここで問題となるのが、地理的に異なるネットワークに配置された物理サーバ間を仮想サーバが移動することにネットワーク側が追従できないということだ。というのも、仮想マシンのIPアドレスといったレイヤ3の情報が移動先でも引き継がれるため、移動先で同一のネットワーク接続を持つことが求められるのである。このため、遠隔でライブマイグレーションを行うには、専用回線や機器を敷設する、あるいはリカバリ対象を一部のサービスに制限するという対応が必要となる。

これに対し、回線等の敷設を行うことなく、より柔軟なライブマイグレーションを実施するには、大規模でフラットなレイヤ2網を構成し、ネットワーク機器において物理的な接続や設定変更なしに対応できるようにしておくという方法がある。これに関しては、先頃、日本電信電話株式会社（以下NTT）が実施した遠隔ライブマイグレーションの実証実験が大いに参考になろう。NTTでは、米国Nicira社の仮想ネットワーク制御技術とOpenvSwitch、KVMというオープンな技術を用いて、専用のハードウェア機器を用いることなく、ソフトウェアによってトンネリング手法の一種であるL2 over L3による論理ネットワークを構築。遠隔地にある武蔵野と厚木の両センター間での遠隔ライブマイグレーションを実現している。

※NTTがNicira社と共同で遠隔ライブマイグレーションに成功
http://www.ntt.co.jp/news2011/1108/110802a.html

現実的なアプローチとなるオーバーレイネットワーク

最後に、企業におけるオンプレミスとクラウド、クラウド間のネットワーク接続におけるネットワーク仮想化のメリットをまとめておきたい。現在では、これらの接続を実現するために、データセンター内に他のユーザーからネットワーク的に隔離されたユーザー企業の専用領域を作り、その専用領域とユーザーのデータセンターとを、VPN回線やタグVLANを利用して、LANのセグメントを論理的に分割してつなぐという方法がとられている。ネットワーク仮想化では、こうした作業に伴う煩雑さをトータルに解消する。

ネットワーク仮想化には、大きく分けて2つのアプローチがある。1つは、ネットワークのエッジ側に存在する仮想マシンや物理サーバの接続を仮想化して、論理的にネットワークで接続するというオーバーレイネットワーク方式。そしてもう1つが、ネットワークのコア側をスライスする方式である。

このうち、現在のシステム環境に適用し易いのは、やはり前者のオーバーレイネットワーク方式である。何よりも、既設ネットワーク資源を活かすことができることに加え、物理的な回線の抜き差しやスイッチの設定変更などの手間も不要なので、機器のコストや運用コストの削減を実現できる。さらに、VLAN数の制限に縛られないプライベートネットワークを実現し、マルチテナントのクラウドの構築や課金処理など付加価値サービスの提供なども容易となる。

レイヤ2のクラウドや仮想化のインフラでは冗長構成なども考慮し、トラブルを回避する対策が必要でリング構成やマルチパス技術をベースにした大規模なイーサネット・ファブリックが用いられていくだろう。こうした冗長化は物理的な制約や相対的なコストがかかるため、OpenFlow技術とレイヤ3のマルチパス、ソフトウェア、仮想マシンを

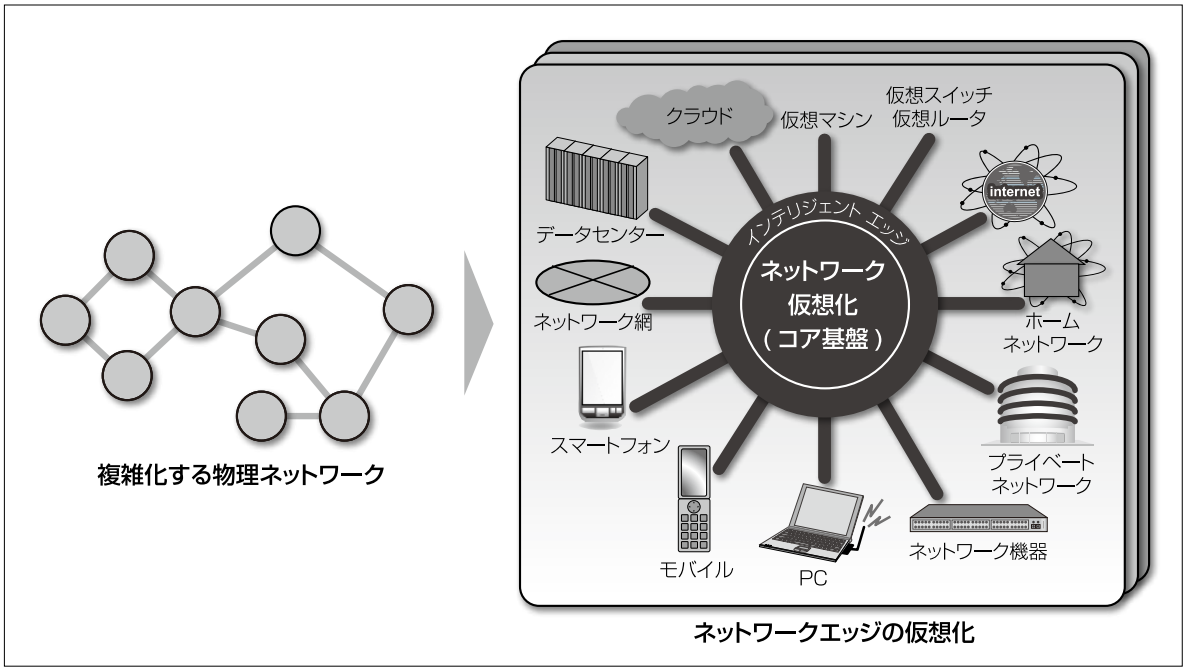


図2　インテリジェントエッジのオーバーレイネットワーク方式は、ネットワーク仮想化の現実解

利用したスイッチ技術とを組み合わせるオーバーレイネットワーク技術も出てきている。

さらに、本記事執筆中にも新たなVXLAN（Virtual eXtensible Local Area Network）仕様がIETFにドラフトが提出されている。これはレイヤ2オーバーレイヤ3（L2 over L3）のオーバーレイネットワーク技術であり、今後も目が離せない。またライブマイグレーションによる仮想マシンのインスタンス化や、インフラ内での仮想マシンの移行に対して自動的に追従するための仮想スイッチ処理や、プロファイル適用を外部スイッチにオフロードするエッジ仮想スイッチなどに関する標準として、IEEE802.1Qbgなどがいま審議されつつある状況だ。

今日では、例えば、電力は利用するものから保有するものへ、ICTについては所有するものから利用するものへといった社会インフラの大きな変化が起きており、こうした流れは今後一層加速していくことになる。ここで紹介したネットワーク仮想化や次世代ネットワークの世界でもパラダイムシフトと呼べる転換がいままさに眼前において展開されている。日本の競争力強化のためにも、そうした動向をしっかりと見据え、その動きに決して乗り遅れないことが何よりも肝要だ。

JNSA ワーキンググループ紹介

在宅勤務における情報セキュリティ対策検討 WG

みずほ情報総研株式会社
WGリーダー　冨田　高樹

■WG発足の経緯

東日本大震災をきっかけに、従業員の在宅勤務に関する新しい動きが出てきました。これまでも、育児や介護など自宅での対応が必要な従業員を支援する目的で、在宅勤務制度を整備する企業はありました。今回の動きはこうしたこれまでの取り組みとは異なり、交通機関の運休で出社できなかったり、職場の節電を実施する必要がある中で、事業継続を実現していこうという目的のもとで行われていることが特徴的です。一方で、急遽実施が決まったことで、十分な準備を行わずに見切り発車的に在宅勤務を開始した企業も多いと予想されます。海外には在宅勤務を積極的に推奨している企業も多数存在し、そうした環境における情報セキュリティを確保するための対策や製品等もさまざまに提供されていますが、そうした対策が存在することをよく知らずに在宅勤務が開始されてしまうことで、情報漏えい等の事故が増大することが懸念されました。そこで、JNSAとしてできる社会貢献活動のひとつとして、在宅勤務における情報セキュリティ対策に関する情報をまとめて公開することを事務局に提案し、6月上旬のWG発足に至りました。急な呼びかけにも関わらず、後述するように多くの方のご参加をいただくことができ、大変感謝しています。

■ガイドブックの公開までの取り組み

7月1日以降、東京電力と東北電力の事業区域においては、大企業から家庭まで一律15%の電力使用量の削減が求められることとなりました。したがって、夏期の間に在宅勤務を実施する企業が増えることが予想されましたので、この時期までに情報提供をしないと意味がありません。そこで、WGの活動も在宅勤務の情報セキュリティ対策に関する情報を6月末に公開することを目標として、それに合わせたスケジュールを組みました。会合は1回開催したのみで、それ以外はJNSAで運用しているWikiを使った共同作業の形で進めました。在宅勤務における情報セキュリティ上のリスクとしては、やはり情報漏えいの問題が大きいことから、「情報を持ち出して仕事する場合」と「情報を持ち出さずに仕事する場合」の2つに分けて内容を構成することとし、それぞれに応じた対策について、日頃そうした製品の販売やコンサルティングに従事している会員企業のみなさんに執筆していただいています。さらに、会員企業において在宅勤務を導入済みの2社に、具体的にどのような対策を講じたり、運用を行っているかについての紹介もしていただきました。

こうして、在宅勤務を行うにあたっての情報セキュリティ対策に関する基本的な考え方や対策方法についてのノウハウをまとめた、「オフィスの節電対策

8月3日開催「在宅勤務のセキュリティを考える! ～JNSAガイドブックの解説と事例セミナー～」

JNSA ワーキンググループ紹介

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」は無事完成し、7月1日に公開されました。さらに、この内容をもとにしつつ実際の会員企業における導入事例の詳細を紹介するJNSA主催のセミナーを8月3日に開催し、こちらも参加者のご好評をいただくことができました。

■今後の活動予定

上で述べたように、今回公開したガイドブックには、一日も早く実際に活用していただくことを優先して作成したため、項目ごとの内容の詳細度がまちまちであったり、必要とされる情報が十分に記載されていない箇所があります。電力不足については当分の間解消されない見込みであるとともに、セミナーにおいても在宅勤務への関心が高いことが示されており、こうしたニーズに応えていくために、第2版を近日中に作成・公開したいと考えています。会員企業かどうかに関わりなく、ガイドブックへのご意見、ご要望がございましたら、ぜひJNSA事務局までお知らせいただけると幸いです。

※「在宅勤務における情報セキュリティ対策ガイドブック」は、下記URLからダウンロードしていただけます。
http://www.jnsa.org/result/2011/zaitaku_guide.html

■メンバー紹介

WGリーダー	
冨田　高樹	みずほ情報総研株式会社
WGメンバー（氏名昇順）	
赤間　健一	トレンドマイクロ株式社
池永　章	株式会社シマンテック
市川　順之	伊藤忠テクノソリューションズ株式会社
稲場　未南	みずほ情報総研株式会社
小川　博久	みずほ情報総研株式会社
奥原　雅之	富士通株式会社
柊　　崇	日本アイ・ビー・エム システムズ・エンジニアリング株式会社
金子　以澄	日本CA株式会社
川辺　康史	株式会社メトロ
桐山　太一	株式会社アーク情報システム
小林　青己	ソフトバンク・テクノロジー株式会社
坂本　慶	サイバーソリューション株式会社
鈴木　英樹	株式会社 OSK
須永　知之	株式会社富士通ソーシアルサイエンスラボラトリ
仙田　健	株式会社富士通ソーシアルサイエンスラボラトリ
高橋　崇	株式会社インフォセック
田中　洋	株式会社インフォセック
手塚　信之	SCSK株式会社
徳田　敏文	日本アイ・ビー・エム株式会社
友國　直樹	トレンドマイクロ株式会社
永田　牧子	株式会社富士通ソーシアルサイエンスラボラトリ
西尾　秀一	株式会社エヌ・ティ・ティ・データ
肥田　雄一	クオリティ株式会社
藤田　延也	F5 ネットワークスジャパン株式会社
別府　卓也	株式会社 OSK
本多　規克	アルプスシステムインテグレーション株式会社
松木　豪	株式会社アーク情報システム
松田　康宏	株式会社メトロ
宮崎　亮	株式会社 JMC
森　真梨子	伊藤忠テクノソリューションズ株式会社
山本　総夫	ソフトバンク・テクノロジー株式会社
油井　秀人	富士通エフ・アイ・ピー株式会社
横川　典子	トレンドマイクロ株式会社
吉野　賢剛	F5 ネットワークスジャパン株式会社
渡辺　仙吉	日本アイ・ビー・エム株式会社

会員企業ご紹介32

CompTIA 日本支局

http://www.comptia.jp

CompTIA

CompTIAは、1982年、IT業界の要請から発足した非営利の業界団体です。ITに携わる企業や個人の利益を高めるための「文教活動」、CompTIA認定資格での「認定」、IT業界の声を反映しIT政策に反映するための「政策支援活動」、IT業界への「社会貢献」の4つを柱として活動を続けています。 米国シカゴ本部を中心に世界に10の拠点を持ち、2001年に日本支局が設立されています。

CompTIA認定資格

1993年より提供を開始してCompTIA A+をはじめとするCompTIA認定資格は、業界のエキスパートにより開発され、実践力、応用力を評価する認定資格として、法人を中心にワールドワイドで150万人以上に取得されています。現在、日本国内では、10の業務分野におよぶ認定プログラムとコミュニケーションに関連したスキル診断を提供しています。

特に、CompTIA A+、CompTIA Network+、CompTIA Security+の3つの認定資格は、ISO 17011/17024の認定を受け、国際的に認知された品質基準に準拠した信頼性の高い認定資格として評価されています。

CompTIA認定資格の特徴は、特定のベンダーや製品に依存しない「ベンダーニュートラル」、特定のテクノロジーに特化しない「テクノロジーニュートラル」であることがあげられます。現在のIT人材として求められている、IT環境を網羅的・横断的に理解しシステムのライフサイクル全般を理解している「マルチスキルな人材」を育成することが可能な認定資格です。

CompTIA認定資格（日本語試験配信済/2011年7月現在）

A+ Certification Program	PC環境の設計・構築、運用・管理を実施する上で必要とされる知識やスキル、現場能力・業務遂行のための考え方を問います。ソフトとハードの両面のITスキルに加え、セキュリティやコミュニケーション等の業務能力を証明します。
Network+ Certification Program	「ネットワーク技術」に携わる職種において、実務上共通して必須な"実務能力"とされる技術知識・スキル・問題解決能力・技術遂行能力の考え方を問います。
Security+ Certification Program	セキュリティの一般概念、インフラストラクチャセキュリティ、暗号技術や業務・組織面でのセキュリティポリシー等幅広くセキュリティの"実務能力"を評価します。
Server+ Certification Program	サーバーのハードウェアやソフトウェアの構築、メンテナンス、仮想化、災害復旧やトラブルシューティング等サーバー運営上で必要とされる知識やスキルを証明する業界初の認定資格です。
CDIA+ Certification Program	文書画像管理ソリューションのコンサルティング能力を評価する認定資格です。要求定義から導入まで一連の流れで起こりうる様々な局面での対応を問います。
CTT+ Certification Program	インストラクターをはじめ、人事/教育部門、管理職ならびに高等教育機関に従事する人のプレゼンスキル、コミュニケーションスキルを問う「人と向き合う業務」に必要な"実能力"を評価します。
Project+ Certification Program	小規模から中規模プロジェクトを遂行する際に必要とされる知識を体系的に学習することができ、業界を問わず、プロジェクトマネジメントに必要な標準知識とベストプラクティスに基づく"実務能力"を評価する認定資格です。
PDI+ Certification Program	プリンティング&ドキュメントイメージングのサービスおよびサポート業務に携わるプロフェッショナルに必要な知識と行動を評価する認定資格です。
Strata IT Fundamentals	PCコンポーネントの識別や利用用途の理解、各種設定、ソフトウェアインストールの実行、互換性により発生する障害の特定、セキュリティリスクの認識および予防等が出題。
Strata IT for Sales	有効なコミュニケーションスキルを使用しプロ意識を持った顧客とのコミュニケーション、ユーザーのIT環境の特定、顧客からの要求に適したソリューションの提供、セールス過程における技術スタッフとの調整などに関する知識が出題。
ビジネス・コミュニケーションスキル診断	ビジネスの集団の一員として、仕事の成果をあげる、事業目的の達成に貢献するといった目的を持った個人が主体となりコミュニケーションを行う目的やビジネスのゴールに近づくために必要なスキルを分析。

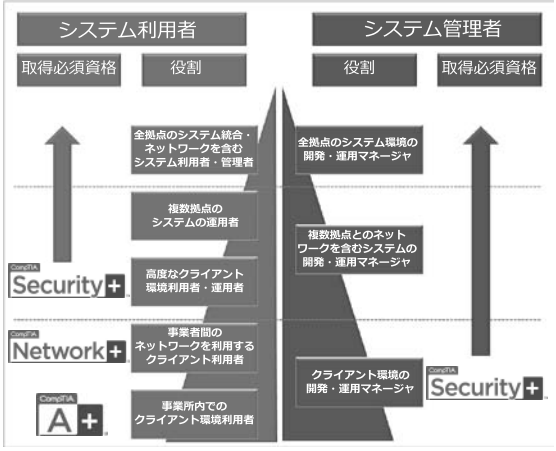
世界中で信頼を支える人材の証

CompTIA米国本部が実施したセキュリティ調査では、「セキュリティインシデントの原因」として約60%が「人為的エラー」と回答しています。そのため企業における「情報」という資産を守るため、認定資格によりスキルの可視化をする企業や機関が増えてきています。

一例として、米国国防総省では、PC利用者から管理者まで情報保証に携わる人材に対し、業務に就く際に、業務内容や役割に応じCompTIA A+、CompTIA Network+、CompTIA Security+の3つの認定資格を取得することを必須としています。

また、日本国内では、スマートフォン等の普及により様々なITデバイスが活用される中、企業のセキュリティを確保するために全社員に対しCompTIA Strata IT Fundamentalsを活用いただき「IT力」の向上を検討する企業が増えてきています。

CompTIAでは、これらのモデルをベースに様々なパートナーを通じて、企業でのネットワーク、セキュリティ人材育成のご提案・ご支援をさせていただきます。



お問い合わせ先

CompTIA 日本支局 http://www.comptia.jp/

〒101-0061　東京都千代田区三崎町3-4-9

水道橋MSビル7F

TEL 03-5226-5345　FAX 03-5226-0970

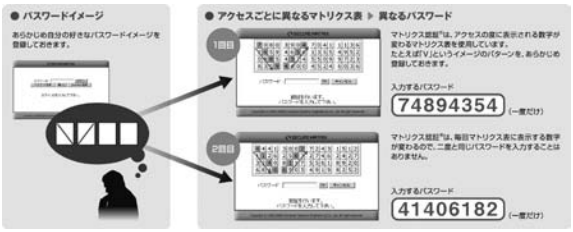
e-mail info_jp@comptia.org

株式会社シー・エス・イー
http://www.cseltd.co.jp/

株式会社シー・エス・イー（本社：東京都渋谷区、代表取締役社長：関 好行、以下CSE）は、創業以来約40年間に渡り独立系のソフトハウスとして、金融ならびにメーカー、官公庁、自治体などあらゆる分野におけるソフトウェアの開発実績を重ねてまいりました。「お客様と共に成長するサービスを提供する」をミッションとして、お客様の事業活動における業務効率化、顧客創造、リスクマネジメント等に貢献するサービスを提供します。セキュリティ分野においては、自社開発の本人認証システム「SECUREMATRIX®」（セキュアマトリクス）を始めとする豊富な取扱商品と長年に渡る開発やサポートの実績を活用し、日々変化する新しい脅威からお客様を守るべく提案から導入・運用サポートまで一貫したサービスを提供し、安全で便利な高度情報通信社会の構築へ向けた取り組みを行っております。

SECUREMATRIX® のご紹介

SECUREMATRIX® は、CSE が開発した、認証デバイスを一切使わない本人認証システムです。人が頭の中に想い描くイメージからワンタイムパスワードを生成する「マトリクス認証 ®」方式を採用し、セキュリティおよび利便性の向上、コスト削減のすべてを同時に実現します。複雑なパスワードをもう覚える必要はありません。また高価な認証デバイスを利用する必要はありません。コストを削減したい「企業」や、セキュリティを高めたい「IT 管理者」、また面倒なことはしたくない「社員」など、様々な立場の方が抱えるパスワードに関する悩みを一気に解決するのが「SECUREMATRIX」です。



SECUREMATRIX for CLOUD LOGON

「使いやすい認証で、もっと安全にクラウド環境を利用したい。」

クラウド環境のセキュリティは「マトリクス認証」

- 使い捨てのワンタイムパスワードで認証を強化
- IPアドレス制限やトークン型ワンタイムパスワードより利便性の高い認証を実現
- デバイス不要だから、管理工数やデバイス購入コストを一気に削減
- ブラウザだけで強固な認証を提供する「マトリクス認証」はクラウド環境と好相性

<Salesforce CRM 連携リーフレット>
http://cseltd.co.jp/smx/docs/case_SMX%20for%20SalesforceCRM.pdf

SECUREMATRIX for RADIUS LOGON

「通信経路が安全でも、「認証」が脆ければ意味がない。」

RADIUS対応機器の認証は「マトリクス認証」

- さまざまなVPNやファイアウォールと連携し、認証を強化
- SSL-VPNは、ブラウザだけでダイレクトログオン
- 独自のRADIUSサーバを実装。複数のRADIUSクライアントをサポート
- RADIUSアトリビュートに対応
- 認証VLAN等のRADIUS対応機器とも連携可能
- スマートフォンにも対応

SECUREMATRIX for DESKTOP LOGON

「社内も「マトリクス認証」に統一すれば、使い勝手はさらに高まる。」

「社内」でもデスクトップへのログオンは「マトリクス認証」

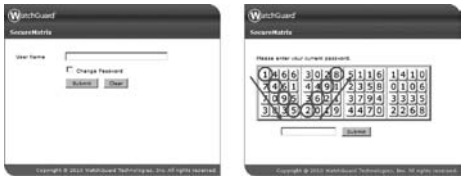
- 「Ctrl」+「Alt」+「Del」を押したら、「マトリクス認証」が可能
- 意識することなくActive Directoryと連携が可能
- ネットワークに接続されていなくても、利用可能（オフライン認証）
- スクリーンセーバーのパスワードロック時にも利用可能

SECUREMATRIX for APPLICATION INTERFACE

「マトリクス認証の可能性を思いのままに。」

既存システムやアプリケーションに「マトリクス認証」

- CまたはJAVAに対応した「マトリクス認証」用API
- 会員向けWEBサイトの認証や、既存システムの認証を強化
- API開発キットを提供
- セキュリティを考慮したシンプルなAPI



※画面は、WatchGuard SSL100/560 と API で連携した例

＊「SECUREMATRIX」、「マトリクス認証」は株式会社シー・エス・イーの登録商標です。
＊ 文中記載の社名、商品名は各社の商標または登録商標です。

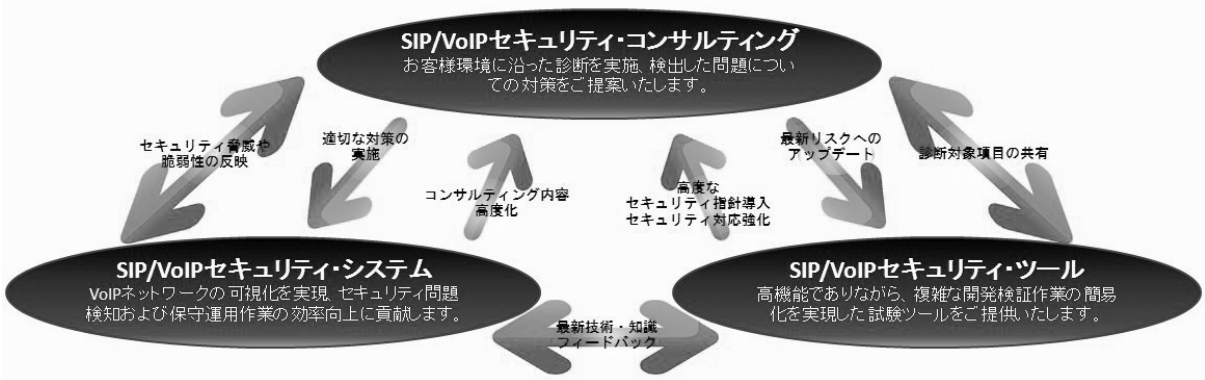
お問い合わせはこちらまで

株式会社シー・エス・イー　ICT営業部

TEL:　03-3463-5633　MAIL:　sales@cseltd.co.jp
WEB:　http://www.cseltd.co.jp/smx/ask.htm

株式会社ネクストジェン
http://www.nextgen.co.jp

株式会社ネクストジェンは設立以来、大規模IPセントレックスやIM/Presenceシステムといった専門的技術を必要とするソフトウェア製品を、多くの通信事業者や企業に提供してまいりました。また、製品の設計・開発だけでなく、検証や保守サポートまで、ワンストップで提供する体制を有しております。この中で蓄積した豊富な技術ノウハウを活かし、SIP/VoIPサービスを提供する通信事業者や企業向けに、ネットワークセキュリティの確保をサポートするのがSIP/VoIPネットワーク・セキュリティソリューションです。



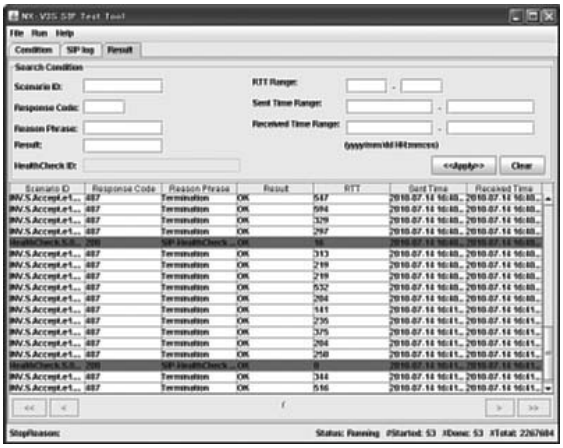
SIP/VoIPセキュリティ・コンサルティング

国内では唯一のSIP/VoIPシステムを対象としたセキュリティ診断サービスです。これまでにIP-PBXや端末、通信キャリアの網などを対象に100以上のシステム診断実績を持ち、盗聴、発着番号詐称やDoSアタック等によるサービス停止といった脅威を検出、お客様環境に即したリスク分析をいたします。また、既存のセキュリティ上の脅威だけでなく、対象システムの持つ脆弱性をも検出し、効率的なリスク対策・管理やシステムの品質向上に貢献いたします。

SIP/VoIPセキュリティ・システム NX-C6000

NX-C6000 は、VoIP やIMシステムなどの保守運用に不可欠な、ネットワークフォレンジック＆IDS製品です。SIPやH.323でのメッセージ詳細から流量マクロレベルまで、ネットワークの状態を可視化します。問題解析作業の効率向上、及びサイレント故障やセキュリティ脅威の検出といった保守上の課題を解決するために必要な機能を集約したシステムです。

SIP/VoIPセキュリティ・ツール NX-V3S



NX-V3SはSIPプロトコルの脆弱性テスターです。死活監視を行いながら250万以上の問題が発生しやすいメッセージを送信、試験対象とするSIPエンティティの脆弱性を特定します。製品出荷前の最終確認に使用することで、製品の品質向上にお役立ていただけます。

お問い合わせ先
株式会社ネクストジェン ネットワークセキュリティ事業本部
〒102-0083 東京都千代田区麹町3-3-4　Tel:03-3234-6855
URL:http://www.nextgen.co.jp　E-mail: sales@nextgen.co.jp

JNSA 会員企業のサービス・製品・イベント情報

■製品情報■

○ 特権ID管理、監査対策ソリューション 『Cyber-Ark PIM Enterprise Suite』

特権IDは権限が強力なため、不正な利用は情報システムに大きな脅威を与えます。会計監査や内部統制対策の重要項目であり、最近監査指摘が増えている分野でもあります。600社以上の導入実績を持つ『Cyber-Ark PIM』は、パスワードの自動変更、特権IDの利用申請・承認ワークフロー、操作履歴の記録などを実現するソフトウェアで、対象サーバやネットワーク機器にエージェントを必要としないソリューションです。

【製品情報詳細】
http://www.dit.co.jp/products/cyber-ark/

◆お問い合わせ先◆
株式会社ディアイティ
E-mail : info@dit.co.jp
TEL : 03-5634-7651

○ 暗号鍵管理のベストプラクティス 『タレス nShield HSM』

タレス nShieldは、暗号鍵を保護するHSM(ハードウェアセキュリティモジュール)です。
高速な暗号処理、強力なアクセス制御、物理的アクセスからの保護(耐タンパ性)といった機能を備え、FIPS140-2 Level3およびCommon Criteria EAL4+認定を受けた、クラス最高のセキュリティを実現します。
各種標準APIをサポートし、WebサーバのSSL暗号化や、データベース暗号化などの各種暗号アプリケーションとのシームレスな連携が可能です。

【製品情報詳細】
http://www.thales-esecurity.com/japan/Products/Hardware%20Security%20Modules.aspx

◆お問い合わせ先◆
タレスジャパン株式会社　e-セキュリティ事業部
TEL : 03-6234-8180
E-mail : jpnsales@thales-esecurity.com

○ 拡散してはもう遅い！”次世代”L2スイッチ 『SGシリーズ』でウイルスの蔓延を防ぐ！

『SG』シリーズL2スイッチはウイルスが拡散する際の調査行為を検知・遮断します。
クライアントPCに近い所に導入することで、万が一脆弱性を利用されウイルス感染してしまった場合でも拡散範囲を最小限に留めます。
また、ログの確認やレポートの自動生成機能、機器の状態監視等ができる無償のツールも付属しており、簡単に管理できます。

【製品情報詳細】
http://www.nttct.co.jp/products/products11.html

◆お問い合わせ先◆
NTTコムテクノロジー株式会社　SOC推進部
TEL：03-6218-0288
E-mail：info-security@nttct.co.jp

○ 最新のWebアクセスリスクに対応！ 「InterSafe WebFilter / CATS /LogDirector」

業界初のIPv6対応や、ソーシャルメディア・Webメールの普及で拡大が懸念されるHTTPS経由の情報漏洩・私的利用防止を実現した最新のWebフィルタリングソリューションをラインナップ。情報流出問題の表面化で重要性が増す組織のログ管理には、クリック操作だけで自在な分析が可能なログ分析ソフトを用意。多様化するWebアクセスリスクをALSIのアクセスマネージメントシリーズ製品が解決します。

【製品情報詳細】
http://www.alsi.co.jp/security/is/index.html

◆お問い合わせ先◆
アルプス システム インテグレーション株式会社
TEL : 03-5499-1331

■サービス情報■

○業界初！IPv4/IPv6トランスレータを独自開発。IPv6環境の検査に完全対応した『IPv6検査』が登場！

IPv4枯渇により、従来の検査ツールでは、IPv4だけの時に比べ、IPv6への対応が不完全となっているのが現状です。GSXの『IPv6検査』では、この問題を解決するために、業界初の「IPv4/IPv6」トランスレータを独自開発しました。
これにより、IPv4に対する検査と同等レベルの網羅性高い検査項目をIPv6で実現しました。混在環境でもシームレスな検査サービスを提供します。

【サービス情報詳細】
http://www.gsx.co.jp/service/J1_14.html

◆お問い合わせ先◆
グローバルセキュリティエキスパート株式会社
事業開発部　マーケティング担当　菅田
TEL：03-3457-1900
E-mail：mktg@glbex.com

■イベント情報■

○特権ID管理ソリューション セミナー 多くの企業での採用実績を有するCyber-Ark社の特権ID管理「PIMソリューション」の優位性と国内導入事例をご紹介

●監査の視点からみた特権管理の必要性と課題
情報セキュリティ大学院大学　原田 要之助 教授

●Cyber-Ark PIM Enterprise Suiteの優位性について
Cyber-Ark社
APACセールス バイスプレジデント　Dan Dinnar 氏

●PIMソリューションの導入事例
株式会社ディアイティ
ネットワークセキュリティ事業部　中林 聖裕

日　時：2011年 10月 5日(水)
会　場：ザ・キャピトルホテル東急
主　催：株式会社ディアイティ

【イベント情報詳細】
http://www.dit.co.jp/seminar/111005/index.html

JNSA 2010年度活動報告会

JNSA 主席研究員
やすだ　なお

JNSAのWG活動内容を報告する2010年度の活動報告会が下記の要領で開催されました。また、東日本震災後IT分野での支援を行っているHack for Japanの活動についての講演も行われました。当日は、160名以上の方に参加いただき、盛況な報告会となりました。

【日　時】2011年6月8日(水)10：30～15：30

【会　場】アルカディア市ヶ谷 6F　(千代田区九段北4-2-25)

【主　催】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)

【定　員】トラック１(阿蘇(東)／定員：80名)　　トラック２(阿蘇(西)／定員：80名)

【概　要】2010年度に活動したワーキンググループ(WG)の活動報告と今後の活動計画などの発表

【料　金】参加費無料

午前中は2トラック並行で実施され、午後は1部屋に統合して開催されました。ここでは発表された部会ごとに概要をご紹介します。なお、プログラム詳細と発表資料は次のURLからダウンロードできますので、ぜひご覧ください。

http://www.jnsa.org/seminar/2011/0608/

U40部会

ラボネットWGリーダーの一宮隆祐氏(日本電気株式会社)から発表されました。

U40部会は、若手技術者の参加する部会です。40歳で卒業することになっていますが、今までの活動では各方面の専門家を呼んでディスカッションを行う勉強会や、各種家電製品やIPv6の対応を実証実験する取り組みなどを行っています。また、ラボネットのシステム構成や評価テーマについて説明されました。

教育部会

コーディネーターは、やすだ なお教育部会長、パネラーにWGリーダーの長谷川長一氏(株式会社ラック)と平山敏弘氏(日本アイ・ビー・エム株式会社)を迎え、「社会基盤としてのセキュリティ教育」というテーマで、パネルセッションが行われました。

セキュリティ講師スキル研究WGでは、「セキュリティ講師スキルガイド2011年度版(仮)」を執筆中だそうです。これと関連して情報セキュリティ基本教育実証WGでは、遠隔地からの大学講義の実証実験を行い、成果を論文にまとめて日本教育情報学会誌に投稿したところ、査読論文として「教育情報研究」第27巻第1号に掲載される予定になりました。今後も、まだ定説になっていない教育方法や、方法論の実証実験を行っていくそうです。

標準化部会

標準化部会からは、２つのWGから報告が行われました。

(1) 情報セキュリティ対策マップ検討WG

「セキュリティ対策のモデル化と可視化(マップ化)への取り組み」というテーマで、リーダーの奥原雅之氏(富士通株式会社)から今までの検討内容や報告書内容のイメージなどが説明されました。今年度を最終年度として成果をまとめるそうで、「夢のあるマップ」を目指したいとのことでした。

(2) セキュリティにおけるアイデンティティ管理WG

「2010年度セキュリティにおけるアイデンティティ管理WG成果報告」というテーマで、リーダーの宮川晃一氏（日本ビジネスシステムズ株式会社）から発表されました。WGでは成果物として『クラウド環境におけるアイデンティティ管理ガイドライン』を出版しています。（http://www.jnsa.org/result/2010/idm_guideline.html）この内容について説明されました。また、もうひとつのテーマとしてまとめている、ID管理におけるロールマネージメントについての検討概要についても紹介されました。

日本セキュリティオペレーション事業者協議会（ISOG-J）

ISOG-Jは、JNSAの傘下にあり、4つのWGで活動しています。今回は出口幹雄氏（富士通株式会社）がリーダを勤めるWG3のセキュリティオペレーション関連法調査の成果報告として、関連法規を集約した「情報セキュリティ小六法」が紹介されました。（http://www.jnsa.org/isog-j/activities/result.html）また、WG2のセキュリティオペレーション技術WGが検討しているIPv6検証報告書についても紹介されました。（http://www.jnsa.org/isog-j/output/2011/ISOG-J_IPv6_Verification_Report.pdf）

調査研究部会

午後からは、調査研究部会の3つのWGのセッションがありました。

(1) スマートフォン活用セキュリティガイドライン策定WG

「ガイドラインβ版リリースまでの活動内容と今後」として、リーダーの加藤智巳氏（株式会社ラック）から概要や課題について発表がありました。スマートフォンの利便性を損なわないようなガイドラインを作りたいとのことです。新聞、雑誌やWebメディアなどにも紹介され、公開情報として効果を挙げているようです。

(2) セキュリティ市場調査WG

「2010年度セキュリティ市場調査結果について」としてリーダーの勝見勉氏（株式会社情報経済研究所）から国内の情報セキュリティ市場調査の概要報告が説明されました。2010年度調査結果の速報版をベースに独自に分類した区分による市場規模変遷の調査結果の概要が紹介されました。

ラック加藤氏による調査研究部会WG活動報告

(3) セキュリティ被害調査WG 活動報告

「発生確率調査と2010年個人情報漏えい調査の報告」として、リーダーの大谷尚通氏（株式会社ＮＴＴデータ）から活動内容と報告書について説明がありました。今までの個人情報漏えいについての調査は、マスコミ等に公開されている事例を対象としているため、マスコミの価値判断が入りやすいという問題点がありました。このため、インシデントの発生確率を調査することができないか、という新たな課題について試行を始めているそうです。

【講演】東日本大震災を IT で支援する Hack for Japan ほかのご報告

最後に、Hack for Japan スタッフでもある日本マイクロソフト エバンジェリストの西脇資哲氏の講演がありました。東日本大震災の後、実際に現地入りして、IT 技術者の目で見た災害の状況が紹介されました。百聞は一見に如かずの通り、現地を経験した迫力のあるお話に圧倒されました。大震災はIT 的にも単なるBCP やDR では解決しきれない問題を突きつけました。IT に関わる者として、どのように復興に関われるのか、という重い命題に頭がフル回転する思いでした。

マイクロソフト西脇氏による講演

JNSA では、今後もワーキンググループの活動を中心に様々な情報を発信して参りますのでご期待下さい。

2011 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年度より開催してまいりました。

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。

今年度は一般向けビデオ・冊子教材を新たに作成し、よりリアリティのある映像と初心者にもわかりやすい解説冊子が完成いたしました。新規教材の完成に伴い従来のプログラムも刷新し、来場者参加型でさらに楽しく学べるインターネット安全教室を開催いたします。

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、学校等
［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。（2011年9月22日現在）

◆「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、茨城県、高知県、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

2011年度「インターネット安全教室」開催一覧

（2011.9.22現在）

	日　程	開催地	共催団体	会　場
1	4月20日（水）	秋田	NPO 法人ノースウインド	IT チャオ！
2	4月22日（金）	福井	福井県立足羽高等学校	福井県立足羽高等学校　第1体育館
3	4月23日（土）	神奈川	NPO 情報セキュリティフォーラム	ゆめおおおかオフィスタワー
4	4月29日（金）	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 体育館
5	5月16日（月）	秋田	秋田大学	秋田大学　工学資源学部5号館　101 講義室
6	5月21日（土）	長野	NPO 法人グループ HIYOKO	塩尻市市民交流センター“えんぱーく” 2階　ICT ルーム
7	5月24日（火）	秋田	NPO 法人ノースウインド	IT チャオ！
8	5月26日（木）	富山	（株）富山県総合情報センター	富山県総合情報センター　セミナールーム
9	5月31日（火）	群馬	NPO 法人おおた IT 市民ネットワーク	太田市立南中学校　体育館
10	6月3日（金）	群馬	NPO 法人おおた IT 市民ネットワーク	太田市立毛里田小学校
11	6月6日（月）	大阪	NPO 法人きんきうぇぶ	河内長野市立南花台東小学校
12	6月7日（火）	群馬	NPO 法人おおた IT 市民ネットワーク	太田市立薮塚本町小学校　体育館
13	6月9日（木）	大阪	NPO 法人きんきうぇぶ	河内長野市立美加の台小学校
14	6月10日（金）	群馬	NPO 法人おおた IT 市民ネットワーク	太田市立強戸小学校　多目的ホール
15	6月10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　イングリッシュルーム
16	6月19日（日）	徳島	財団法人 e- とくしま推進財団	美馬市立江原中学校　体育館
17	6月20日（月）	秋田	NPO 法人ノースウインド	IT チャオ！
18	6月22日（水）	大阪	NPO 法人きんきうぇぶ	河内長野市立天野小学校
19	6月25日（土）	東京	三鷹市立井口小学校	三鷹市立井口小学校
20	6月25日（土）	愛知	NPO 東海インターネット協議会	東海高校・東海中学校 「サタデープログラム」会場内
21	7月1日（金）	大阪	NPO 法人きんきうぇぶ	河内長野市立三日市小学校
22	7月2日（土）	北海道	北海道情報セキュリティ勉強会（せきゅぽろ）	道民の森
23	7月9日（土）	東京	中野区立新山小学校	中野区立新山小学校
24	7月14日（木）	千葉	NPO 浦安防犯ネット	浦安市立入船中学校
25	7月26日（火）	神奈川	NPO 情報セキュリティフォーラム	相鉄岩崎学園　8階809室
26	7月27日（水）	福岡	西日本短期大学	西日本短期大学　パソコン教室
27	8月3日（水）	沖縄	NPO 法人フロム沖縄推進機構	沖縄産業支援センター　303 会議室
28	8月11日（木）	福井	NPO 法人ナレッジふくい	福井市消費者生活センター
29	8月21日（日）	神奈川	NPO 情報セキュリティフォーラム	横浜市立場地区センター
30	8月31日（水）	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」
31	9月2日（金）	大阪	NPO 法人きんきうぇぶ	河内長野市立南花台西小学校
32	9月5日（月）	大阪	NPO 法人きんきうぇぶ	河内長野市立南花台東小学校
33	9月9日（金）	沖縄	NPO 法人フロム沖縄推進機構	コリンザ 2 階 研修室
34	9月17日（土）	北海道	北海道情報セキュリティ勉強会（せきゅぽろ）	釧路市生涯学習センター
35	9月19日（月） 1回目	島根	NPO 法人プロジェクトゆうあい	松江市市民活動センター 503 会議室
36	9月19日（月） 2回目	島根	NPO 法人プロジェクトゆうあい	松江市市民活動センター 503 会議室

	日　程	開催地	共催団体	会　場
37	10月1日（土）	岐阜	NPO 法人泉京・垂井	郡上市立大和中学校
38	10月7日（金）	神奈川	NPO 情報セキュリティフォーラム	川東タウンセンター マロニエ
39	10月14日（金）	神奈川	NPO 情報セキュリティフォーラム	浦舟コミュニティハウス
40	10月16日（日）	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
41	10月21日（金）	岐阜	NPO 法人泉京・垂井	関市立洞戸中学校
42	10月27日（木）	神奈川	NPO 情報セキュリティフォーラム	綾瀬市民文化センター 3 階 視聴覚室
43	11月12日（土）	神奈川	NPO 情報セキュリティフォーラム	川崎市幸市民館
44	11月14日（月）	神奈川	NPO 情報セキュリティフォーラム	ヴェルクよこすか（横須賀市勤労会館）
45	11月18日（金）	神奈川	NPO 情報セキュリティフォーラム	浦舟コミュニティハウス
46	11月18日（金）	富山	（株）富山県総合情報センター	富山県ＩＴセンター マルチメディアシアター
47	11月19日（土）	富山	（株）富山県総合情報センター	富山県ＩＴセンター マルチメディアシアター
48	11月25日（金）	栃木	NPO 栃木県シニアセンター	下野市生涯学習情報センター
49	11月25日（金）	山梨・甲府市（新規）	山梨大学	山梨大学　甲府東キャンパス A2-21 教室
50	12月10日（土）	広島	近畿大学工学部	近畿大学工学部 マルチメディア講義室
51	12月20日（火）	大阪	NPO 法人きんきうぇぶ	河内長野市立千代田小学校
52	1月26日（木）	長野	NPO 法人グループ HIYOKO	塩尻市市民交流センター“えんぱーく” 2 階　ICT ルーム
53	1月27日（金）	大阪	NPO 法人きんきうぇぶ	河内長野市立川上小学校
54	2月2日（木）	大阪	NPO 法人きんきうぇぶ	河内長野市立楠小学校
55	2月3日（金）	大阪	NPO 法人きんきうぇぶ	河内長野市立天見小学校
56	2月5日（日）	神奈川	NPO 情報セキュリティフォーラム	小机スポーツ会館
57	2月19日（日）	神奈川	NPO 情報セキュリティフォーラム	十日市場スポーツ会館

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/

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

中小企業向け指導者育成セミナー

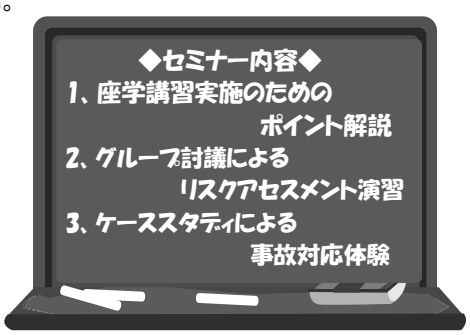
～ケーススタディによる実践型研修！～

平成23年度

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

中小企業の経営者等に対して、情報セキュリティに対する適切なアドバイスを行なう地域の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いたします。事業開始４年目となる今年度は、過去のセミナーの集大成として、「中小企業にこそ求められる情報セキュリティ対策」など指導者の実践に役立つ内容で展開します。

情報セキュリティ対策の指導力向上と、中小企業の情報セキュリティレベルの強化にお役立ていただくために、ぜひご参加ください。



セミナー開催概要

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

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	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、開催地の商工会議所・商工会連合会・中小企業団体中央会
開催地・日程	全国 25 箇所で 2011 年 8 月～2012 年 2 月に開催 （開催地別日程は別表のとおり）
開催時間	9:30～17:00 （9:00 受付開始）
参加人数	各会場 50～100 名
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、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。
セミナー内容	参加者の方々が、地域で講習会を実施したり、指導の実践に役立てるための内容で行います。 ① 座学講習実施のためのポイント解説 座学講習を行うための講習会スケジュール（2時間程度数種類）と説明ポイントの解説を行います。また、講習の中で、タイムリーで話題性のある情報を提供できるように、最新の情報セキュリティ動向をお伝えします。 例：スマートフォン、ソーシャルメディア、クラウドサービス、BCP 等 ② リスクアセスメント演習 ある企業の業務風景を映像化したビデオを見て、グループ討議でリスクアセスメントの演習を行います。直接的なリスクだけでなく関連して発生しうるものなど、そこに潜むリスクを探し出すことで、気づきを養うとともに中小企業に対して適切に対策提案を行うためのスキルを養います。 ③ ケーススタディによる事故対応体験 情報セキュリティ事故（インシデント）の事例を基にして、対応方法をグループ討議しながらロールプレイ形式で演習を行い、事故対応の疑似体験をします。セミナーにより体験したことを中小企業指導に役立ててもらうとともに、地域の講習会で事故対応時の注意点などとして伝えられるようにしていただきます。
参加者に期待すること	本セミナーに参加された方々へは指導用ツールの提供や中小企業向け講習会の開催を支援しますので、ぜひ情報セキュリティ普及啓発活動に本セミナーを役立てていただければ幸いです。 • 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）をお渡しします • 配布する指導用ツールを用いて中小企業の情報セキュリティ講習会を開催された場合、実施報告レポートを提出いただくことで謝金をお支払します（2012 年 2 月末開催分まで）。 • セミナー参加者専用サイトにより、その他の指導用の補足資料等を随時提供していきます。
参加費	無料（事前登録制）

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

※最新の情報は本事業のホームページをご覧ください。　9 月 28 日現在

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	札幌商工会議所　（終了）	2011 年 8 月 30 日（火）	北海道経済センター
	北海道②	帯広商工会議所 / 北海道中小企業団体中央会 十勝支部事務所 / 北海道十勝管内商工会連合会　※ 予定	2011 年 12 月 15 日（木）	帯広商工会議所
東　北	宮　城	仙台商工会議所　（終了）	2011 年 9 月 22 日（木）	仙台商工会議所
関　東	栃　木	宇都宮商工会議所	2011 年 10 月 26 日（水）	宇都宮商工会議所
	東京①	東京商工会議所　（受付終了）	2011 年 11 月 1 日（火）	東京商工会議所ビル
	東京②	東京商工会議所	2012 年 1 月 30 日（月）	東京商工会議所ビル
	神奈川	神奈川県商工会連合会 / 神奈川県商工会議所連合会　（終了）	2011 年 9 月 6 日（火）	相鉄岩崎学園ビル
	千　葉	柏商工会議所 /NPO 法人ちば経営応援隊　（受付終了）	2011 年 10 月 12 日（水）	柏商工会議所
	新　潟	新潟商工会議所 / 財団法人にいがた産業創造機構 / 特定非営利活動法人新潟情報セキュリティ協会※ 予定	2011 年 11 月 25 日（金）	NICO プラザ
中　部	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　※ 申請中	2011 年 12 月 13 日（火）	富山県総合情報センター
	愛　知	名古屋商工会議所 / 社団法人中部産業連盟　（終了）	2011 年 9 月 9 日（金）	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※ 予定	2012 年 1 月 18 日（水）	ソフトピアジャパンセンタービル
近　畿	京　都	京都商工会議所 ※京都会場は 10：00 ～ 17：00 の開催となります。	2011 年 12 月 9 日（金）	京都商工会議所
	大　阪	大阪商工会議所	2011 年 11 月 15 日（火）	大阪商工会議所
	兵　庫	神戸商工会議所 /NPO 法人 ITC 近畿会　（終了）	2011 年 9 月 15 日（木）	神戸市産業振興センター
	和歌山	田辺商工会議所 /NPO 情報セキュリティ研究所※ 予定	2011 年 12 月 1 日（木）	情報交流センター ビッグ・ユー
中　国	広　島	広島商工会議所 /NPO 法人 ITC 広島	2011 年 10 月 20 日（木）	広島商工会議所
	岡　山	岡山商工会議所	2011 年 11 月 22 日（火）	岡山商工会議所
	鳥　取	米子商工会議所	2011 年 11 月 8 日（火）	米子商工会議所
四　国	徳　島	徳島県商工会連合会	2012 年 1 月 13 日（金）	あわぎんホール
九　州	福　岡	福岡商工会議所　（終了）	2011 年 9 月 27 日（火）	福岡商工会議所
	大　分	大分商工会議所 /NPO 法人大分 IT 経営推進センター 財団法人ハイパーネットワーク社会研究所	2011 年 11 月 29 日（火）	大分商工会議所
	鹿児島	鹿児島商工会議所	2011 年 10 月 14 日（金）	鹿児島商工会議所
	宮　崎	宮崎商工会議所 / 宮崎県ソフトウェアセンター※ 予定	2012 年 1 月 20 日（金）	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	2011 年 10 月 7 日（金）	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

● JNSA西日本支部主催セキュリティセミナー NSF2011 in Kansai

主　催：JNSA西日本支部
日　時：2011年10月5日(水)
会　場：グランキューブ大阪
ＵＲＬ：http://www.jnsa.org/seminar/nsf/2011kansai/

● 2011日韓情報セキュリティシンポジウム

主　催：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)
特定非営利活動法人
日本セキュリティ監査協会(JASA)
韓国情報セキュリティ産業協会(KISIA)
日　時：2011年11月10日(木)
会　場：ゆうぽうと会議室

後援・協賛イベントのお知らせ

1. Gartner Symposium & ITxpo 2011

主　催：ガートナージャパン株式会社
日　時：2011年10月3日(月) ～ 5日(水)
会　場：Le DAIBAホテルグランドパシフィック
ＵＲＬ：http://www.gartner.co.jp/event/index.html

2. 情報セキュリティワークショップ in 越後湯沢 2011

主　催：特定非営利活動法人新潟情報セキュリティ協会
情報セキュリティワークショップin越後湯沢
実行委員会
日　時：2011年10月7日(金) ～ 8日(土)
会　場：新潟県南魚沼郡湯沢町(湯沢町公民館等)
ＵＲＬ：http://www.anisec.jp/yuzawa

3. 学びのイノベーション＆セキュリティフェア

主　催：ISEN（教育ネットワーク情報セキュリティ
推進委員会）
日　時：2011年10月7日(金) ～ 8日(土)
会　場：秋葉原UDX

4. ロジスティクスソリューションフェア2011

主　催：公益社団法人日本ロジスティクスシステム協会
日　時：2011年10月31日(月) ～ 11月1日(火)
会　場：東京ビッグサイト「西3ホール」
ＵＲＬ：http://logistics.or.jp/lsf/index.html

5. 中小企業庁委託事業 「平成23年度情報モラル啓発セミナー」

主　催：中小企業庁、各経済産業局
(財)ハイパーネットワーク社会研究所
日時／会場：
2011年11月1日(火)ホテル青森
2011年11月17日(木)岐阜グランドホテル
(今年度は全7会場で開催)
ＵＲＬ：http://www.hyper.or.jp/moral/

6. ハイパーネットワーク2011 別府湾会議

主　催：ハイパーネットワーク別府湾会議実行委員会
日　時：2011年11月4日(金)～5日(土)
会　場：杉乃井ホテル
ＵＲＬ：http://www.hyper.or.jp/staticpages/index.php/bbc2011/

7. ITGI Japan カンファレンス2011

主　催：日本ITガバナンス協会
共　催：ISACA東京支部、ISACA大阪支部
ISACA名古屋支部
日　時：2011年11月9日(水)
会　場：(社)全国社会福祉協議会　灘尾ホール
ＵＲＬ：http://itgi.jp/conf201111/index.html

8. PacSec2011

主　催：Dragostech.com inc
日　時：2011年11月9日(水) ～ 11月10日(木)
会　場：青山ダイアモンドホール
ＵＲＬ：http://pacsec.jp/index.html?language=ja

9. 子どもワークショップたじみ

主　催：多治見市情報センター
多治見市産業文化センター、多治見商工会議所
日　時：2011年11月12日(土)
会　場：多治見市産業文化センター5F大ホール
ＵＲＬ：http://www.city.tajimi.gifu.jp/jouhou/

10. Internet Week 2011 ～とびらの向こうに～

主　催：多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）
日　時：2011年11月30日(水) ～ 12月2日(金)
会　場：富士ソフト　アキバプラザ
ＵＲＬ：http://internetweek.jp/

11. かごしまITフェスタ

主　催：かごしまITフェスタ実行委員会
日　時：2011年12月2日(金) ～ 12月4日(日)
会　場：鹿児島アリーナ
ＵＲＬ：http://www.it-festa.jp/

12. デジタル・フォレンジック・コミュニティ 2011 in TOKYO

主　催: 特定非営利活動法人デジタル・フォレンジック研究会
デジタル・フォレンジック・コミュニティ2011実行委員会
日　時: 2011年12月12日(月)～13日(火)
会　場: ホテルグランドヒル市ヶ谷
ＵＲＬ: http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=329&continue=on

JNSA 部会・WG2011 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)

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)

2010年度に引き続き、経済産業省委託事業「平成23年度コンピュータセキュリティ早期警戒体制の整備事業『インターネット安全教室』」の企画・運営、共催団体へのサポート等を行っていく。

【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)

2010年度に引き続き、経済産業省委託事業「平成23年度コンピュータセキュリティ早期警戒態勢の整備事業『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」の内容検討を行っていく。

【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)

今夏は、節電に向けて在宅勤務が増加することが見込まれているが、十分な対策なしに在宅勤務等が実施されることで、情報漏洩のリスクが高まる恐れがあることから、限られた時間の中でどのような点に留意し、どのような対策を講じればよいかについて、会員の持つノウハウをオンラインで集成して文書としてとりまとめ、JNSAのWebサイトで無償公開し、一般企業等での対策の参考にしていただく。

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7月に公開した。

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)

2010年の発生確率調査(トライアル)の結果からテーマを選択・深堀りし、また2010年の調査項目以外の他エリアも追加検討し、2011年 発生確率調査(本調査)を実施する。リスク評価検討WGと連携し、発生確率調査の必要条件の決定や、統計的検証を行う。2010年個人情報漏えい調査の報告書の公開、および2011年の同調査も継続して実施する。

予定成果物は、

- 「2010年 情報セキュリティインシデントに関する調査報告書 個人情報漏えい編」(7月公開)
- 「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」
- 「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 個人情報漏えい編」

【セキュリティ市場調査WG】

(リーダー：勝見勉 氏／株式会社情報経済研究所)

国内の情報セキュリティ市場の現況を調査・分析し、報告書を作成する。今年度は、2010年度版完成予定。また、2011年度版の調査を行い、年内に報告書をまとめることを目指す。

予定成果物は、

- 「2010年度版国内情報セキュリティ市場調査報告書」
- 「2011年度版国内情報セキュリティ市場調査報告書」

【IPv6セキュリティ検証WG】

(リーダー：林憲明 氏／トレンドマイクロ株式会社)

組織内ネットワークに対し、意図せずにIPv6接続した利用者が及ぼしうる被害とその対策について検討を行う。
共同検証実施後、3回程度のミーティング開催により報告書を仕上げる。管理者の知らぬ間に一部IPv6化された場合にどのような管理手法が考えられるのか、制限していた項目が制限されなくなることはあるのか、IPv4環境下において、安全対策上実施していた項目が使えなくなることはあるのか等の項目について報告を行う計画。

予定成果物は、「2011年 IPv6セキュリティ検証報告書」

【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）

企業においてスマートフォンの利便性を損なわず安全に業務利用するためのガイドラインの策定と関連の研究、勉強会、情報交換の実施。「スマートフォン活用セキュリティガイドラインβ版」の続編となる完全版と、関連する情報資料の策定とリリース予定。

予定成果物は、「スマートフォン活用セキュリティガイドライン2011年度版」

3.標準化部会

（部会長：中尾康二 氏／KDDI株式会社）

【セキュリティにおける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。

今年度は、ロールマネジメントについての議論と成果物の作成、番号制度やプライバシについての勉強会と議論、ID管理のあるべき論の議論（グローバル環境、ハイブリット環境など）等を実施する予定。

予定成果物は、「アイデンティティ管理におけるロールマネジメント（仮）」

【セキュアプログラミングWG】

（リーダー：伏見論 氏／株式会社情報数理研究所）

セキュアなシステム開発を開発現場寄りの立場から考え、課題を討議する。なお、この2、3年は、国際規格を討議テーマとして地道な検討・評価を行う方針としている。
ISO/IEC 27034は、その第一部がISO/IEC JTC1/SC27で最終委員会ドラフトとなったが、依然として内容が抽象的であるため有効と思えず、日本として別の切り口からの貢献ができないかSC27/WG日本委員会とともに探っている。今後は、特に分散システムやプロダクトラインでのセキュリティ保証に役立つ規格内容への誘導といったアプローチに焦点をあてたい。

予定成果物は、討議成果の国際規格への反映、解説的文書の作成等。

【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」の作成に関し、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等のアウトプットを作成する。

WGでは、対策マップ記述モデル、作成手法、標準対策マップ案の作成等を検討する予定。

また、8月にキーマンズネットにてWG活動の内容を記事として公開した。（4回連載）

【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。

ISFとのワークショップ（2011年6月）の開催、ISF総会（2011年10月）への参加、KISIAとの連携支援、およびISFとの共同成果物の作成を進める。なお、ISO/SC27への成果物については、2011年10月会合への入力を目指す。

予定成果物は、「クラウドセキュリティにかかわる技術ガイドライン」ドラフト

なお、作成したドラフトは、2011年10月開催のISO/SC27会合で提案する予定。

【PKI相互運用技術WG】

（リーダー：松本泰 氏／セコム株式会社）

WG活動での情報共有、PKI day 2011などのイベントでの提案、提言を行う。また、ネット社会における信頼（TRUST）の仕組みを提案、提言していく。

予定成果物は、「番号制度とPKIの関係等」等のペーパを出すことを検討。

【リスク評価検討WG】

（リーダー：二木真明 氏／SCSK株式会社）

過去のインシデント事例や社会的な傾向などをもとに、ある組織のリスク量を実際に推定するための基本的なモデルを考える。当面、モデルの複雑化はなるべく おさえ、リスクの概観を定量化できるような「どんぶり」モデルを目標とする。
（その後の検証を経てモデルをより精緻なものにしていく）

予定成果物は、「情報セキュリティリスクの統計的推定手法に関する検討報告書（仮称）」

4.教育部会

（部会長：安田直 氏／株式会社ディアイティ）

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、教育に関する実証実験を行うことで、その成果を会員で共有し、更に論文発表や成果物を一般公開することにより会員のみならず社会に対しても還元することでJNSAの存在意義を高めていく。

【セキュリティ講師スキル研究WG】
（リーダー：長谷川長一 氏／株式会社ラック）

「セキュリティ講師スキル研究調査報告書（仮）」を作成し、その実証実験を行う。これにあたっては、基本教育実証WGやU40部会、女子BoFなどとも連携し、相互の活動を活性化し、成果を充実させたものとしたい。また、これらの結果は「セキュリティ講師スキル基準2011年度版（仮）」として、JNSA 会員や外部へ広く公開することを予定している。

予定成果物は、

- 「セキュリティ講師スキル研究調査報告書 2010年度版(仮)」
- 「セキュリティ講師スキルガイド 2011年度版（仮）」

【情報セキュリティ教科書執筆者WG】
（リーダー：塩見友規 氏／
三井物産セキュアディレクション株式会社）

作成した「情報セキュリティプロフェッショナル教科書」の普及、活用方法の検討、改版に向けての検討を行う。

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

平成23年度は、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回の講義を実施予定。その他、教育部会として人材育成イベントの実施を計画中。

合計15回分の講義資料の作成、およびWG活動成果の論文採録を予定。

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、勉強会や会員交流会の企画、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。

具体的には、新しい問題（目標40問）を作成し、プレミアム版のユーザ事例を収集して、サイト、セミナーなどで公開する予定。

予定成果物は、新しい問題の作成・公開、ユーザ事例の公開

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

JNSA会員企業のPRの場として、会員企業が有している各種ソリューションを紹介するWebサイト（JNSAソリューションガイド：仮称）の構築を目的に活動を継続する。

予定成果物は、
「JNSAソリューションガイド（仮称）」WEBサイト
- Webサイト
- 運用手順書他、関連ドキュメント一式

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。

【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）

「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」との紐付けによる情報セキュリティチェックシートの見直しや、新しいデバイスの出現に伴うリスクに対応する情報セキュリティ対策について整理を行う。

【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年度公表「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」の対象読者からのフィードバックを行う。

具体的には、対象読者からのフィードバック及び「情報セキュリティチェックシート」見直しに伴う手引きを修正する。また、新しいデバイス出現に伴うリスクに対応するための「追補版」作成を検討する。

予定成果物は、必要であれば以下2点の成果物を作成

- 「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修正版」
- 「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追補版」

【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た、セミナーおよびメンバー企業・連携他団体との交流による勉強会を実施

していく。

2−3ヶ月に一度の勉強会を企画。また秋に西日本支部としてのセミナー、他団体との合同セミナー開催を予定している。

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内にて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を実施する。具体的には、IPv6環境におけるセキュリティ検証、家電機器DLNA実地検証を行う予定。

予定成果物は、

- IPv6検証報告
- DLNA検証報告

【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。部会にて勉強会で取り上げたいテーマを持ち寄り、その中からテーマを絞って講師打診、会場や日程の調整を行う。1〜1.5ヶ月に一回のペースで開催する。U40メンバー優先にはなるが、継続してJNSA会員への聴講枠開放も行う予定。

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／株式会社ラック）

ISEPA情報セキュリティ資格マップをサイトにて公開。8月に情報セキュリティ大学院大学とセミナーを開催。

【広報WG】

（リーダー：勝見勉 氏/NPO日本セキュリティ監査協会）

イベントの企画・開催のみならず、ホームページなど、様々な媒体を通して、ISEPAの活動成果等のお知らせを発信する。

【スキルWG】

（リーダー：衣川俊章 氏／（ISC）2 Japan）

情報セキュリティ人財の育成を行うにあたって利用・参照できる指標を「人財アーキテクチャ」として策定し、その利活用についても「使える」情報を継続的に提供する。

【相互認証WG】

（リーダー：小林佑光 氏／SEA/J）

数多くある情報セキュリティ資格がそれぞれ発信している情報をまとめたり、資格や教育プログラム間で相互の認証が行われるような働きかけを行っていく。

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。

【セキュリティオペレーションガイドラインWG】

（リーダー：許先明 氏／株式会社ラック）

セキュリティ診断・検査のためのガイドラインを検討する予定。

予定成果物は、「セキュリティ診断・検査のためのガイドライン」

【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（IPv6、スマートフォン等）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）

「MSS事業者のための情報セキュリティ小六法」外部公開予定。また、これに関連するガイドラインを検討予定。

予定成果物は、「MSS事業者のための情報セキュリティ小六法」

【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:多田昭仁 氏／株式会社日立システムズ）

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。

JNSA 役員一覧　2011 年 10 月現在

会　長	田中　英彦	情報セキュリティ大学院大学 研究科長 教授
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	

理　事（50音順）

後沢　忍	三菱電機株式会社　情報技術総合研究所
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
勝見　勉	株式会社情報経済研究所
兜森　清忠	マカフィー株式会社
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
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
山田　秀樹	ＥＭＣジャパン株式会社
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
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
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
近藤　伸也	キヤノンＩＴソリューションズ株式会社
佐藤　憲一	株式会社ＯＳＫ
佐藤　徹次	ネットワンシステムズ株式会社
佐藤　友治	株式会社ブロードバンドセキュリティ
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
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
藤田　平	株式会社シマンテック
二木　真明	SCSK株式会社
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	株式会社ラック
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	慶応義塾大学　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　(2011年10月1日現在　146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)
(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)ISAO
伊藤忠テクノソリューションズ(株)
イルポンテ(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
(株)インフォセック
(株)ウィテック
(株)AIR
(株)エス・シー・ラボ
SCSK株式会社
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
関電システムソリューションズ(株)
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(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 New

【さ】

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
(株)情報数理研究所
新日鉄ソリューションズ(株)
新日本有限責任監査法人
(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)
セコムトラストシステムズ(株)
ソニー(株)
ソフォス(株)
ソフトバンク・テクノロジー(株)
ソフトバンクBB(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
有限責任監査法人トーマツ
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)
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　システムズエンジニアリング(株)
日本オラクル(株)
日本サード・パーティ(株)
日本サムスン(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)
パナソニック電工(株)
(株)日立システムズ
(株)日立ソリューションズ
(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(富士通SSL)
(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)ブロードバンドセキュリティ
(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
(株)MONET

【や】

(株)ユービーセキュア

【ら】

(株)楽堂
(株)ラック
リコー・ヒューマン・クリエイツ(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（2011 年度）

4 月	4 月 19 日	「セキュリティ & リスクマネジンメントサミット 2011」後援
	4 月 25 日	第 1 回幹事会
	4/27 ～ 28 日	「IT インフラストラクチャ&データセンターサミット 2011」後援
5 月	5 月 10 日	2011 年度理事会
	5 月 25 ～ 27 日	「ワイヤレスジャパン 2011/ モバイルパワー 2011」後援
	5 月 27 日	「第 9 回迷惑メール対策カンファレンス」後援
	5 月 26 ～ 28 日	「第 15 回サイバー犯罪に関する白浜シンポジウム」後援
6 月	6 月 1 日	第 2 回幹事会
	6 月 7 ～ 10 日	「Interop Tokyo 2011」後援
	6 月 8 日	2010 年度 WG 活動報告会（アルカディア市ヶ谷）
	6 月 8 日	2011 年度総会（アルカディア市ヶ谷）
	6 月 18 日	「ISACA 大阪支部設立 25 周年記念講演会」後援
7 月	7 月 7 日	「MCPC　スマートフォンセキュリティセミナー」後援
	7 月 13 ～ 15 日	「自治体総合フェア 2011」協賛
	7 月 22 日	「仮想化インフラ・ワークショップ 06」協賛
	7 月 26 日　他	「平成 23 年度情報モラル啓発セミナー」後援
		7/26 鹿児島、7/29 鳥取　他
8 月	8 月 4 日	「組織力向上を目指したキャリアパスとスキルの可視化セミナー」　後援
	8 月 17 日	第 3 回幹事会
	8 月 31 日～ 9 月 1 日	「Cloud Computing World 2011」「Next Generation Data Center 2011」後援
9 月	9 月 13 日	「平成 23 年度情報モラル啓発セミナー」後援　福井
	9 月 14 日、16 日	「ID & IT　Management Conference 2011」後援
	9 月 26 日	「PKI Day 2011」（山王健保会館）
10 月	10 月 3 ～ 5 日	「Gartner Symposium & Itxpo 2011」後援
	10 月 5 日	JNSA 西日本支部主催セキュリティセミナー「NSF 2011 in Kansai」（グランキューブ大阪）
	10 月 6 日	第 4 回幹事会
	10 月 7 ～ 8 日	「学びのイノベーション & セキュリティフェア」後援
	10 月 7 ～ 8 日	「情報セキュリティワークショップ in 越後湯沢 2011」協力
	10 月 31 日～ 11 月 1 日	「ロジスティクスソリューションフェア 2011」協賛
11 月	11 月 1 日　他	「平成 23 年度情報モラル啓発セミナー」後援　11/1 青森　11/17 岐阜
	11 月 4 ～ 5 日	「ハイパーネットワーク別府湾会議」後援
	11 月 9 日	「ITGI Japan カンファレンス 2011」後援
	11 月 9 ～ 10 日	「PacSec 2011」後援
	11 月 10 日	「2011 日韓情報セキュリティシンポジウム」
	11 月 12 日	「子どもワークショップたじみ」後援
	11 月 30 日～ 12 月 2 日	「Internet Week 2011」後援
12 月	12 月 2 ～ 4 日	「かごしま IT フェスタ」後援
	12 月 12 ～ 13 日	「デジタル・フォレンジック・コミュニティ 2011 in Tokyo」後援
1 月		
2 月		
3 月		

2011 年 4 月～
2012 年 3 月
「インターネット
安全教室」開催

2011 年 8 月～
2012 年 2 月
「平成 23 年度
中小企業向け
指導者育成
セミナー」開催

★ JNSA 活動スケジュールは、http://www.jnsa.org/aboutus/schedule.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　http://www.jnsa.org/member/index.html に掲載しています。（JNSA 会員限定です）

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。）

NTTコムテクノロジー株式会社　門田　剛

JNSA会員の皆様、はじめましてNTTコムテクノロジー株式会社の門田剛と申します。今回、株式会社インターネットイニシアティブの鈴木さんよりご紹介いただきましたので、僭越ながら自己紹介させていただきます。

弊社NTTコムテクノロジーは、NTTコミュニケーションズグループの一員として、お客様企業の情報システムネットワークの成長を支えるための一連の業務を提供する総合エンジニアリング会社ですが、そんななか現在私はセキュリティオペレーション業務に従事しており、お客様システム環境に対するセキュリティ監視・運用のために日々格闘しております。

その私も学生時代に話が遡ると、ITとはほど遠い金属材料学を専攻しており、超伝導環境で利用される超合金を極低温（マイナス269℃！）で引っ張って破断させる実験をしていました。空気が冷えて液体化する現象を目の前で頻繁に見ていたのを、今となっては貴重な体験をしていたものだと感じています。そしてその研究そっちのけ(？)で学生時代にはまっていたのが、SunワークステーションのX Windowシステムが配備された"計算機室"（呼び方が古い…）で、それ以降こちらのIT魔空空間に取り込まれたままとなっています。当時は性善説にもとづいた自由なインターネットの世界に入り浸っていましたが、現在のどこ見ても脅威が…という世知辛い状況を見ると隔世の感があります。

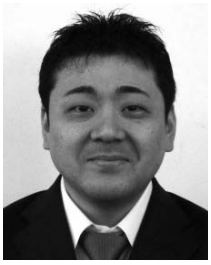
さて、前職ではインターネット技術全般を活用したSI業務に従事していましたが、実はそのときに一度JNSAの活動に関わったことがあります。2002年度の相互接続WGにおいて、無線LAN相互接続実験に参加していました。その時は先輩の後ろについていくのが精一杯の状態でしたが、それから時を経て、2008年から再び現職にてJNSAの活動に参加することになって意識していることは、以前よりも主体性を持って関わることです。

現在JNSAでは主にISOG-JのWG2、WG4、WG5でお世話になっていますが、さまざまな年代やバックグラウンドを持っておられる方々と身近に接することができ、非常に刺激を受けています。業界全体のため、ひいては日本のためにとこだわりを持って活動されてる方々のそばで、微力ながらも貢献できることがあればと思っています。

最後に。スキーと風景写真撮影、旨い酒と肴をこよなく愛でていますが、今年子供が生まれたこともあって全て活動が停止気味になっています。将来、子供と海外スキーにでも行って、一緒に写真を撮ったり酒を飲むのを夢見ながら我慢しているところですので、最近つれないなと思ってる方々も、見捨てないで今後ともよろしくお願いします。

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。）

NTT データ先端技術株式会社　小林　稔



皆様、はじめまして。NTT データ先端技術株式会社の小林と申します。

前号の日本アイ・ビー・エム株式会社の梨和さんから、会員紹介のバトンタッチをされ、今回担当させていただくことになりました。

まず､簡単に私の経歴と業務の説明をさせていただきます｡そもそも情報セキュリティに関心を持ったのは 2000 年に頻発した官公庁の Web サイト改ざんがきっかけでした。大学卒業を控え、ネットワークエンジニアを目指そうかと思っていた時期でしたが、このような業界もあるのかと大変興味を引かれました。

2001 年に某ベンチャー系セキュリティ企業に入社し、主に IDS の検証や導入を行う部署に配属されました。その他にもセキュリティ診断や雑誌記事の執筆などを行っていました。

その後、2003 年に NTT データ・セキュリティ株式会社に転職し、IDS/IPS の監視サービスを提供する部署に配属され、それ以来、同じ部署に所属しています。

現在の主な業務としては、監視サービスの運用を始め、導入提案、機器の検証、社内システム運用、顧客のトラブル対応、チームのとりまとめなどを行っています。ただ、年々、マネジメント的な業務が増えているのが悩ましいところです…。

会社は 2011 年 7 月 1 日に統合され、NTT データ先端技術株式会社となりましたが、業務内容やポジションは変わっていません。

JNSA には 2010 年 4 月より参加しており、主な活動としては、ISOG-J の WG2 にて技術情報の交換に参加させていただいています。また、ISOG-J では、標的型攻撃の情報共有を目的とした WG5 が最近立ち上がり、この WG にも参加させていただいています。

JNSA のような業界団体への参加は初めてなのですが、同じ業界で活躍されている他社のエンジニアの方々と意見交換ができたり、時にはハンズオン作業が行えるなど、非常に刺激的で貴重な場だと思っています。

今後も積極的に参加していきたいと考えていますので、よろしくお願いいたします。

事務局お知らせ
JNSA ANNOUNCE

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 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
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.32

2011 年 10 月 1 日発行

発行所
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
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