

# ISF とのコラボレーションと NSF2009 開催報告

JNSA 安田 直

2010年1月27日、1年ぶりにNSF2009（ネットワークセキュリティフォーラム2009）が、東京のベルサール神田で開催されました。「情報セキュリティ新時代」〈転換期を迎える情報セキュリティのこれからを考える〉と題し、12ページのプログラムのとおり、2トラック並列のセッションで開催されました。今年度の大きなトピックは、イギリスのISFとのコラボレーションを行うことが正式にアナウンスされたことです。JNSAも国際化が進められてきています。日本と諸外国での問題を共に考えていく試みが現実のものとなってきており、JNSAにとっては新しいチャレンジになりますが、この機会を活かすことが求められています。このような動向を含め、NSF2009の各セッションでの議論について、簡単にご紹介しましょう。

## 1. ISF とのコラボレーション

2009年度の大きな特徴は、基調講演でISFとのコラボレーションについて正式発表されたことにあります。ISFは、The Information Security Forumの略称で、イギリスのロンドンに本拠があります。ISFは1989年に設立され、300以上のグローバル企業や団体を会員に持つ非営利団体として活動しています（<https://www.securityforum.org/>）。標準の開発、脅威の予測、リスク分析ツールなどの開発を行っており、世界の情報セキュリティ分野で大きな影響力を持っています。

ISFの会員は、ITを利用する大きなユーザ企業がほとんどです。この意味ではJNSAの会員構成とは違った側面を持っていると言えます。ISFはこのようなメンバーに対して、専門知識や総合的な知識・経験を生かし、広範なセキュリティ戦略に対する実地的な解決方法を提供することを目指しています。JNSAとISFでは、情報セキュリティに対する世界標準を作っていく活動を実現するために、双方が蓄積している専門知識や実践的経験を活用していくことで合意しました。具体的にはIT統制や世界標準のベストプラクティス、ガイドライン等を開発することを目的に、共同プロジェクトや研究、ツールの開発などを進めることを考えています。

このため、JNSAとISFは2009年11月にバンクーバーでITガバナンスと情報セキュリティ分野にお

ける世界標準やベストプラクティスの開発について協業することに合意し、業務提携契約を締結しました。実際の活動内容についてはこれから調整することになりますが、手始めとして、クラウドコンピューティングをテーマにして議論を行い、双方の意識の違いの確認や、国際的な動きとして何をしていくかなどを検討して行くことを始めています。NSF2009翌日の28日に幹事会のメンバーや関係者を中心にしたメンバーでワークショップを行いました。図1にその時の様子を示しましたが、クラウドコンピューティングに関するアウトラインの共有を行い、さらに日本における言葉の意味や、課題などについてグループに分かれて討議し、発表するというを行いました。これらの結果のメモをまとめ、次の機会に更に問題点や解決案などを整理することから始めてみようとしています。まだJNSAとしては、途に就いたばかりで手探り状態ではありますが、今後の国際的な議論を盛り上げていくきっかけにしたいと考えています。



図1：JNSAとISFで試行したクラウドコンピューティングに関するワークショップ



図2：ハワード・シュミット氏のビデオメッセージ

さて、NSF2009 当日に戻って、改めて各セッションで議論されていた内容について簡単にご報告します。

## 2. 基調講演

今年度は JNSA と ISF (the Information Security Forum) のパートナーシップ提携契約が行われたこともあり、ISF 会長のハワード・シュミット氏の基調講演が予定されていましたが、昨年 (2009 年) 12 月 22 日に米国政府機関のサイバーセキュリティ調整官に任命されたのに伴い、代理で ISF COO のビル・コーシー氏が基調講演を行いました。ハワード・シュミット氏からは、ビデオメッセージが届けられ、会場で冒頭に放映されました。

ビル・コーシー氏からは、「情報セキュリティ・ベストプラクティスにおける将来の方向性」と題して ISF の活動や成果、今後の方向性について紹介があり、ISF の情報セキュリティに対する考え方や観点について説明されました。情報セキュリティのベストプラクティスは、恒常的に変化・進化する脅威よりも、常に一歩先を行っている必要があります。情報セキュリティの未来を考えるに当たり、近い将来に発生する可能性のある脅威についての考察を行い、その脅威の発生を見越した上で組織・企業を守るために、ベストプラクティスがどのように進

化していかなければいけないかについても説明されました。また、現在の経済状況の中、組織のリスクへの認識や考え方が変化してきていることに対して、具体的な対応策についての考え方が紹介されました。最後に、情報セキュリティの標準化やベストプラクティスに影響を及ぼすであろう情報セキュリティの世界で起こっている最新の事例やトピックについても言及されました。

ビル・コーシー氏の基調講演に続いて、JNSA の下村事務局長が加わり、「世界とのコラボレーションを目指して」と題して、下村氏から JNSA と ISF の提携の経緯や背景について説明がありました。この後、ビル・コーシー氏から、ISF としての立場での JNSA とのコラボレーションの目標や効果などについて、全体的な視点からのお話がありました。



図3：ISF のビル・コーシー氏と JNSA の下村正弘事務局長



図4：トラックAの会場

JNSA と ISF の連携は、主にベンダーとしての立場からユーザとの関わりを探ってきた JNSA と、ユーザ企業への情報提供を主に実現してきている ISF との、双方とも新たなチャレンジになると思われませんが、言語や文化の壁を越えて実りあるものにしていきたいと思えます。

基調講演のあと、昼休みをはさんで、2トラックに分かれて JNSA の活動を中心とした発表が行われました。トラック A は、パネルディスカッションを中心とし、トラック B は講演中心で構成されています。(A1 と B5 が都合で入れ替わっています) 各トラックは、どちらも満員御礼の状態でした(図4、図5)。多彩な内容が議論されましたが、各々のセッションについて、簡単に内容をご紹介します。

#### 【A1】講演「情報漏えい対策の次の一手に向けて」

セキュリティ被害調査 WG リーダー (株) NTT データ大谷尚通氏から、「情報漏えい対策の次の一手に向けて」というテーマで、今までの経緯と今後の調査内容について検討している案について解説がありました。

個人情報保護法が施行されて6年が経過しましたが、対策を行ってもインシデントは減らず、再発するといった現実が分かってきました。どこかに問題があるはずですが。これまでセキュリティ対策は、持ち出し禁止等のルールの策定、暗号化や書き出し禁止等の対策システムの導入、セキュリティ教育等が行われてきました。これらはトップダウンでもたら



図5：トラックBの会場

された対策ばかりということに気が付きます。次のステップの対策には、守るべき情報を扱う現場の人々が積極的に関わるボトムアップ的な対策が必要だと思われま。WGでは、現場主体の改善活動に基づく対策方法について考えようとしているそうです。また、2009年上半期の個人情報漏えいインシデント調査結果（速報）についても紹介されました。新しい評価方法についてのWG活動に参加されたい等のご希望があれば、事務局までご連絡ください。

## 【A2】パネル「リスクアセスメントの課題」

パネルディスカッションで「リスクアセスメントの課題」というテーマで議論がされました。モデレーターとしてJNSA会長でもある東京電機大学教授の佐々木良一氏に、パネラーにはJNSAのWGのメンバーから、二木真明氏、奥原雅之氏、大谷尚通氏、郷間佳市郎氏の各氏にご出席いただきました。

これまで、JNSAでは脅威や脆弱性、リスクの評価にまつわるさまざまなWG活動を行っています。2000年度からセキュリティポリシーWGがサンプルポリシーを作成・公開していますし、最近では、情報セキュリティ対策マップ検討WGが、対策効果の評価のベースとなりうる脅威と対策のマッピングを行うことを試みています。さらに、来年度に向けて、リスク定量化の方法論の検討WGを立ち上げる準備も行っています。これらを踏まえ、リスク評価のための大きな枠組み全体から見た位置づけで考えてみようというテーマでディスカッションが行われました。難しいテーマではありましたが、パネラーから活発な意見が出され、今後のJNSAのWG活動内容についてのヒントが出ていたと思われま。

## 【A3】パネル「クラウド（を使うための）セキュリティを考える」

パネルディスカッションで「クラウド（を使うための）セキュリティを考える」というテーマで議論がされました。クラウドコンピューティングというテーマは、トレンドになっているためか、多数の申

し込みがあり、満員御礼の状態でした。

モデレーターとして、A2でパネラーだった住商情報システム（株）の二木真明氏、パネラーには、調査研究部会長の加藤雅彦氏、（株）ラックの加藤智巳氏、Google（株）の山本真人氏にご出席いただきました。主なテーマとなったのは、下記のような項目でした。

- ユーザ目線からのクラウド
- クラウド要素技術 / ベンダー目線からのクラウド
- クラウドに関するセキュリティ問題と解決策
- 法制度、契約面から見たクラウド

クラウドコンピューティングについては、色々な期待や思惑、懸念が言われていますが、クラウドを効果的に活用するために考えるべきこと、実行した方が良いことなどについて、色々な観点から議論がされました。

## 【A4】パネル「IPv6導入でセキュリティはどう変わるか」

パネルディスカッションで「IPv6導入でセキュリティはどう変わるか」というテーマで議論がされました。モデレーターに（株）ブロードバンドセキュリティの佐藤友治氏、パネラーはマカフィー（株）の野々下幸治氏、金沢大学の北口善明氏、日本セキュリティオペレーション事業者協議会（ISOG-J）の許先明氏、それに（社）テレコムサービス協会の今井恵一氏にお願いしました。かなり白熱した議論が行われ、課題が見えてきたかもしれません。

IPv6は、IPv4枯渇問題と絡めて話されることが多いのですが、IPv6になった時のセキュリティ機能の実装については良く言われる割に、今までIPv4で対策していた多くの組織のF/WやNATなどを始めとする、アドレス等の扱いに関する対応策をどのように引き継げば良いのかについて、具体的な事例や情報が少ないようです。このようなこともあり、IPv6は10年前に登場したものの、これまで普及はなかなか進んでこなかったといえます。

一方、IPv4 の未使用アドレスは、2011 年までに使い切られる見通しですが、通信事業者が使っている通信機器は既に IPv6 対応が進んでいます。新しい OS では最初から IPv6 が使えるようになっているので、IPv4 アドレスを持たない IPv6-only な利用者が近々出てくることも予想されます。

今の課題は、サービス（アプリケーション）の IPv6 対応の確認、セキュリティ管理を含む運用体制、顧客サポート体制の IPv6 対応を、2011 年までの短い期間に準備する必要があるということにあります。実際には、色々な面での未確認、未対応な技術的な問題が課題として残っているので、まずはこれらの問題点を共有し、安心して V6 に移行できるような情報を関係者が共有できるようにすることが大切だということでもまとめられていました。

#### **【B1】 講演「ISO/IEC 27000 関連規格の最新動向」**

KDDI（株）の中尾康二氏は JNSA の副会長でもあります。ISO や ITU/T など活躍されていることでもよく知られています。このセッションでは、2009 年 11 月に米国のレッドモンドで開催された ISO/IEC JTC1/SC27 における WG1 及び WG4 において、ISO/IEC 27000 関連規格に関する審議を中心に話されました。

情報セキュリティマネジメント（ISMS）におけるコア規格となっている ISO/IEC 27001/27002 の見直し状況、セキュリティ監査ガイドライン、セキュリティガバナンスなどの規格審議の状況、ISMS を支える具体的な技術として、例えば、ネットワークセキュリティ、アプリケーションセキュリティ、インシデントマネジメント、アウトソーシングセキュリティ、及びデジタルエビデンス（フォレンジック関連）などに関する最新審議動向について解説されました。

#### **【B2】 講演「人財アーキテクチャーの活用・実証方法及び方向性について」**

教育事業者連絡会（ISEPA）の衣川俊章氏から「人財アーキテクチャーの活用・実証方法及び方向性について」というテーマで解説されました。ISEPA は JNSA の下部組織として位置付けられています。お話は、ISEPA で作成した人財アーキテクチャーの「人材モデルの活用」と「必要なスキル習得の事例」に基づいて、スキル習得についての教育、ISEPA の各参加団体の資格制度や CISSP コミュニティなどの活動、勉強会などでの情報共有の例などが紹介されました。必要とされる人材像のイメージや、必要なスキルの紐付けとそのスキル習得についての要点が説明されました。

#### **【B3】 講演「人材育成における産官学連携の重要性について」**

情報セキュリティ基本教育実証 WG リーダーである、日本アイ・ビー・エム（株）の平山敏弘氏から、「情報セキュリティ基本教育実証」結果に学ぶ人材育成における産官学連携の重要性について、というテーマで WG の活動成果について説明されました。

情報セキュリティ基本教育実証 WG は、情報セキュリティ基本教育の普及と社会貢献への意識向上、また、教育を受ける権利や機会の地域格差是正への取り組みを目指して、産学協力の具体的な実証を行うために 2007 年度に設立されています。活動としては、情報セキュリティ基本教育を実証するモデルケースとして、まず、岡山理科大学との提携を行っています。東京からのリモート授業を実施し、2009 年度は大学 3 年生を対象に、2 単位履修となる半期（6 ヶ月）で 15 回の正規講義を実施しました。

講演では、実証実験を通じて得た経験や受講生からのアンケートの分析と、情報セキュリティ教育カリキュラムに対する問題、Web 環境における遠隔講義の効果と課題等について、報告説明が行われました。

**【B4】講演「出社してから退社するまでのリスク対策」**

西日本支部の、出社してから退社するまでのリスク対策 WG リーダーのアイネット・システムズ (株) の元持哲郎氏から、「出社してから退社するまでのリスク対策」という WG の活動を通じた知見が解説されました。

中小企業への情報セキュリティ対策を実現するための方法論が各方面で求められています。中小企業が負担に感じる事無く実践できるアプローチとして、中小企業で想定される出社してから退社するまでの行動や業務作業に着目し、それぞれの業務に潜む情報セキュリティ上のリスクを洗い出し、分析・評価して、リスク毎にどのような取り組みを行うのか、許容範囲はどの程度なのか、といったリスク対応・対策のベストプラクティスを作成しています。このような WG の活動成果から、作業の進捗状況、作業の過程で判明した問題点、中小企業版 DSS 化の検討等について報告されました。

**【B5】パネル「個人情報保護法は、どこへ行く」**

JNSA の幹事でもある佐藤憲一氏のモデレータで、「個人情報保護法は、どこへ行く～事業者の誤解と、適正な個人情報保護のあり方～」と題してパネルディスカッションが行われました。パネラーは、経済産業省の西田淳二氏、(株) OSK の小林健氏、(株) NTT データの西尾秀一氏、ネットワンシステムズ (株) の山崎文明氏にご出席いただきました。

個人情報保護法の全面施行から 5 年を経過していますが、事業者の行うことや、保護の対象、内容はまだ明確でない部分があります。事業者と消費者、委託元と委託先、管理者と担当者、事業・業務内容、業種特性など、組織・立場等によって同法の解釈や運用が異なっている状態です。そればかりか、重大な問題が認識・報道されずに放置されて、問題点が潜在化してきています。パネルでは、これらの課題を踏まえ、個人情報を適正に取り扱う上で、事業者が実務的および技術的な面から行うべきことや、適正な対処や措置のあり方について説明されました。また、事業者が罰則を適用されたり、訴訟等を受けないようにするための注意点などが紹介されました。

## NSF2009 のプログラム

【S1】基調講演 10:30-12:30 (120分)	
<p>「The Future direction of Information Security Best Practices (情報セキュリティ・ベストプラクティスにおける将来の方向性)」                      情報セキュリティフォーラム (ISF) チーフ・オペレーティング・オフィサー Bill Caughie (ビル・コーシー) 氏</p> <p>「世界とのコラボレーションを目指して～ JNSA と ISF (Information Security Forum) の提携について～」                      JNSA 事務局長 下村正洋</p>	
トラックA	トラックB
【A1】講演 13:30-14:00 (30分)	【B1】講演 13:30-14:30 (60分)
<p>「情報漏えい対策の次の一手に向けて」                      セキュリティ被害調査 WG リーダー (株) NTT データ 大谷尚通氏</p>	<p>「ISO/IEC 27000 関連規格の最新動向」                      KDDI (株) 中尾康二氏</p>
【A2】パネルディスカッション 14:00-15:00 (60分) ～ JNSA WG 合同特別セッション～	14:30-14:40 休憩
<p>「リスクアセスメントの課題」                      モデレーター：                      東京電機大学教授 / JNSA 会長 佐々木良一氏                      パネラー：                      住商情報システム (株) 二木真明氏                      富士通 (株) 奥原雅之氏                      (株) NTT データ 大谷尚通氏                      (株) 日立情報システムズ 郷間佳市郎氏</p>	【B2】講演 14:40-15:10 (30分)
15:00-15:10 休憩	<p>「人財アーキテクチャーの活用・実証方法及び方向性について」                      教育事業者連絡会 (ISEPA) スキル WG リーダー                      (ISC) 2 ジャパン 衣川俊章氏</p>
【A3】パネルディスカッション 15:10-16:30 (80分)	【B3】講演 15:10-15:40 (30分)
<p>「クラウド (をを使うための) セキュリティを考える」                      モデレーター：                      住商情報システム (株) 二木真明氏                      パネラー：                      (株) アイアイジェイテクノロジー 加藤雅彦氏                      (株) ラック 加藤智巳氏                      Google (株) 山本真人氏</p>	<p>「情報セキュリティ基本教育実証」結果に学ぶ                      人材育成における産官学連携の重要性について                      情報セキュリティ基本教育実証 WG リーダー                      日本アイ・ビー・エム (株) 平山敏弘氏</p>
16:30-16:40 休憩	【B4】講演 15:40-16:10 (30分)
【A4】パネルディスカッション 16:40-18:00 (80分)	<p>「出社してから退社するまでのリスク対策」                      出社してから退社するまでのリスク対策 WG リーダー                      アイネット・システムズ (株) 元持哲郎氏</p>
<p>「IPv6 導入でセキュリティはどう変わるか」                      モデレーター：                      (株) ブロードバンドセキュリティ 佐藤友治氏                      パネラー：                      マカフィー (株) 野々下幸治氏                      金沢大学 北口善明氏                      日本セキュリティオペレーション事業者協議会 (ISOG-J)                      許 先明氏                      (社) テレコムサービス協会 今井恵一氏</p>	16:10-16:30 休憩
	【B5】パネルディスカッション 16:30-18:00 (90分)
	<p>「個人情報保護法は、どこへ行く                      ～事業者の誤解と、適正な個人情報保護のあり方～」                      モデレーター：                      (株) 大塚商会 佐藤憲一氏                      パネラー：                      経済産業省 情報経済課 西田淳二氏                      (株) OSK 小林健氏                      (株) NTT データ 西尾秀一氏                      ネットワンシステムズ (株) 山崎文明氏</p>