

## 「日経デジタルコア集中勉強会・セキュリティシリーズ第2回」

会期：2002年7月31日（水）

会場：日本経済新聞社本社11階A会議室



セキュリティシリーズ  
第2回

7月31日、日本経済新聞社本社11階A会議室にて、「日経デジタルコア集中勉強会・セキュリティシリーズ」の第2回を開催した。

この集中勉強会を通じて、デジタルコアからの提言をまとめる予定。今回は、中央大学研究開発機構 情報セキュリティ研究ユニット専任研究員 内田勝也氏よりセキュリティ全般についての解説に続き、重要なポイントを指摘いただいた。

エルティ総合法律事務所 所長弁護士の藤谷護人氏より、セキュリティについて法的な面から解説いただいた後、全体で討論を行なった。

### 情報セキュリティシリーズ 第2回 「管理・運用面から見たセキュリティ」

#### 【スピーチ1】情報セキュリティを考える

内田 勝也氏（中央大学研究開発機構 情報セキュリティ研究ユニット 専任研究員）

#### 【スピーチ2】ネットワーク時代の e R i s k

藤谷 護人氏（エルティ総合法律事務所 所長弁護士）

#### 【討論】

- 高木 寛氏（j TRUSTc, inc 代表取締役）
- 高木 浩光氏（産業技術総合研究所グリッド研究センター セキュアプログラミング長）
- 古川 泰弘氏（情報セキュリティアナリスト）
- 藤原 宏高氏（ひかり総合法律事務所 弁護士）
- 前川 徹氏（早稲田大学 国際情報通信研究センター 客員教授）

#### 【司会】

坪田 知己（日本経済新聞社 日経デジタルコア事務局代表幹事）

このページのレポートは、会議での発言を元にデジタルコア事務局で編集しました。

## スピーチ1 「情報セキュリティを考える」

---

内田 勝也氏（中央大学研究開発機構 情報セキュリティ研究ユニット 専任研究員）



内田 勝也氏

司会（坪田）

今回はセキュリティ勉強会の第2回目。前はホームページのセキュリティの甘さについて赤裸々に話していただき、議論した。

その中で、セキュリティの範囲が広いことが、改めてわかってきたと思う。今回は、セキュリティの専門家である内田氏からセキュリティ全体についてレクチャーしていただき、藤谷氏には法的面からセキュリティについての問題を解説していただく。

数回にわたる勉強会の成果として、デジタルコアから提言としてまとめる予定だ。そのために建設的な議論をしていきたい。

内田氏

セキュリティについて問題提起するために、前提となる知識について話をしていく。時間の制約もあるので、触れられない部分は資料を参考にさせていただきたい。

### 情報セキュリティの考え方

日本の国内で起こった情報セキュリティの事件を5つ、挙げた。参加している方は、どのくらい知っているだろうか。（会場では、半分は知っている人が約4割）過去に起こった事件をあまりに知らなすぎる。また、事件について日本で語られていることには、間違いも多い。

もうひとつ訊ねるが、見知らぬところで、誰も近くにいない場所にお金落ちていた。そのときどうするか考えてみて欲しい。落ちている金額によって、とる手段が変化するのではないか。このような気持ちの変化も、実は情報セキュリティの考え方につながっている。

また、コンピュータ犯罪者と聞くと、どのような人物をイメージとしてとらえるだろうか。1970年から80年代はじめに米国で起こったコンピュータ犯罪者を数百人プロフィールした結果、次のような人物像となった。

15～45歳の男性。コンピュータの専門知識はさまざまで、過去の犯罪歴はほとんどない。個人的な資質としては頭脳明晰、やる気があって企業にとって望ましい人間のように思われてきた。犯罪者のほとんどは、企業や政府機関内部で信頼される地位にあり、コンピュータシステムに簡単に接近できる。朝早くから夜遅くまで仕事をし、休暇をとることもない。

「犯罪者」と聞いて描くイメージと、異なっているのではないだろうか。このように情報セキュリティに関して、事件そのものも、どのような人間が、どのように起しているのかも、一般的に知識がないのが現状である。

### 論より実践。パスワードについて考える

情報セキュリティを守る第一歩は、パスワードにあると言われている。実際にパスワードを変えているだろうか。また、生年月日、電話番号等を使わない、定期的に変更する、6文字以上で英数記号を使う、定期的に変更するといったことが言われているが、これだけで良いパスワードを作れるのだろうか。一般ユーザーは、良いパスワードを作れと言われてもわからない。良いパスワードについて、具体論で答えてくれる人はあまりいない。これはセキュリティ関係者の怠慢だ。

効果的なパスワードを作る方法には、フレーズ・アクロニム（Phrase acronym = 何か文章を考えて、その語句の先頭の文字をパスワードに利用するもの）や、数字を英数記号に変換するテーブル（表）を利用する方法などもある。

また、パスワードの管理については可能なのだろうか。企業では、外出が多い人のユーザーIDで緊急にログインしたい時もあるという。そのためにパスワードを、部内でオー

ブンにして、他の人も使えるようにしている例もある。これではパスワード管理にならない。

私は、ユーザーIDとパスワードは封に入れてしまっておき、必要があれば取り出して使い、ログ（記録）を取っておくようにと指示している。こうしたルールを決め、実践することで、パスワードは個人個人に与え、かつ組織で管理することがわかるはずだ。

良いパスワードを設定できない人が多い現状で、ユーザーID、パスワードを個人に選択させるのは危険である。たとえば、国内企業の運営サイトで、会員登録画面から重複ID検索を行なうと、パスワードが類推できる場合がある。パスワードが分かれば、個人情報がかんにはいる。こうした危険性があるのだ。

パスワード設定に関する事件としては、ネットバンキングを使って顧客口座から詐取した事件や動的パスワード（暗証番号を毎回変える仕組み）設定を利用していた東海銀行のファームバンキング用パソコン端末から不正送金された事件もある。

動的なパスワード、暗号等が循環するシステムでは、その仕組みを知っている人間がパスワードの推測をしたり、暗号を解読する可能性が高くなる。二者が結託しても、セキュリティが破られない仕組みを考えることも、重要なシステムでは大切である。

### 「他山の石」にしないために

「ソーシャルエンジニアリング」の考え方も知っておくべきだ。言葉巧みに騙す相手に対して、正しく対応できずに事件が起きる。平和相互銀行で不正にお金を引き出させた例や、郵便局の窓口でも同様に事件が起きている。どんなに切迫した状況でも、どこまでに対応してよいかを判断できる教育・訓練が必要。多くの企業は、無防備であり、防御は非常に困難である。

電子ファイルの安全性についても、100%安全ではない。最近では、PDFやOffice製品ファイルなど、書き込み、印刷、コピー等を禁止したものが出てきているが、完全な安全を確保できるものではない。

### ハッキング行為の理由とネットワークシステムの脆弱性

ハッキング行為には、以下のような理由があると考えられる。

1. 知的好奇心を満たすため
2. 金銭の不正取得を目的としたもの
3. 個人的な恨みによるもの
4. 無意識（興味本位）に行なうもの
5. 自分の主義・主張を表明するもの
6. テロ行為を目的とするもの
7. 企業・国家スパイ行為

ハッキングを許してしまう、ネットワークセキュリティの脆弱性は、さまざまな点があげられる。加えてシステムの問題、Windowsシステムの脆弱性、UNIXシステムの脆弱性などもある。

米国ではセキュリティ調査として、CSI / FBIが企業を対象に調査を行なっている。攻撃経路、誰が攻撃者か、損害額、法執行機関に報告しない理由などを調査し、公開している。これによると、ハッキング行為の加害者は、ハッカーと不満をもった従業員である場合が多い。日本ではこのような調査が行なわれていない。

### 情報セキュリティで守るべきもの

情報セキュリティでは、以下の「CIA」を高めることが重要。

- 機密性 (Confidentiality)
- 完全性 (Integrity)
- 可用性 (Availability)

情報セキュリティで守らなければならないのは、以下もの。

- |           |                    |
|-----------|--------------------|
| 1. 関連設備   | 建物、電源、空調設備、監視設備等   |
| 2. ハードウェア | コンピュータ機器、ネットワーク機器等 |
| 3. ソフトウェア | 基本ソフト、アプリケーションソフト等 |
| 4. 情報     | IT情報、印刷物等          |

これらについて、不正行為として、機能破壊、機能障害、情報盗取、情報改ざん、情報破壊、情報利用、利用行為などに分けることができる。

自然災害への対策も必要な観点だ。地球温暖化が原因と考えられる局地的な集中豪雨が以前より多くなっており、河川氾濫の危険性が以前より増大している。2000年7月の集中豪雨で東京の地下鉄丸の内線の一部区間が浸水。他の路線でも運転中断などが出た。2000年9月の東海豪雨では、川が氾濫し、床上・床下浸水の被害が発生した。

東京の洪水氾濫危険区域図を見ると、オフィス地域も含まれる。氾濫した場合、オフィスビルは水没する。大抵、地下に電源設備があり、場合によってはバックアップ電源も地下の場合もある。停電したらどうなるのか。ネットワークセキュリティでは、このような災害まで含めて十分考えておいていただきたい。

### 歴史から学ぶ

セキュリティについては、過去から学ぶことが既にたくさんある。たとえば1988年のインターネットワームの発生。UNIXやインターネットに関するセキュリティに大きな影響を与えた。UNIXパスワードは、この事件以降、シャドウパスワードが使われるようになった。

この事件を教訓に、米国国防総省高等研究計画局（DARPA：Defense Advanced Research Projects Agency）は、コンピュータ緊急対応センター（CERT：Computer Emergency Response Team/Coordination Center）を作った。万一、コンピュータネットワークが破壊された場合のために、電子メールアドレスだけでなく、電話番号やFAX番号も公開している。

他にも1987年にメールアドレスを利用して感染した最初のワームが広がった。1999年2月には、アドレス帳を利用したコンピュータウイルス「メリッサ」が登場。2001年9月に被害をもたらしたNimdaワームは、複数の感染経路をもつ。

最近のCode Redのように攻撃すべきIPアドレスを取得し、DDoS攻撃の自動化が可能になっている。

データ漏洩についても、データが入ったパソコンが盗まれる例が多い。生きたデータであるほど怖い。米国の調査会社の調べでは、ノートパソコンに関する損失の26%は盗難によるものとなっている。

緊急時対応計画についても、検討しておくべきだ。2001年9月の同時多発テロの後に、PTSDが発生し、それによって企業の対策が進まなかった例もある。人間の心理面も考慮に入れ、対策を立てる必要があるだろう。

### アウトソーシングの危うさ、個人情報の問題

オウム真理教の関連ソフト事業会社や信者が190以上の官公庁、民間企業のコンピュータソフト開発に携わっていた。

宇治市の住民基本台帳データ漏洩事件では、宇治市とシステム開発会社に損害賠償責任を求めた。アルバイト男性が、MO（光磁気ディスク）にデータをコピーして持ち帰り、個人情報売り出したもの。

個人識別の3要素は、以下のとおり。

- 1．身体的な特徴
- 2．知っていること
- 3．持っているもの

個人識別のものなどを偽造し、戸籍を改ざんし、携帯電話を不正取得、窃盗団に売る事件も起きている。個人では対処しようもない、悪質なケースも出てきている。

### セキュリティ全体像を考える

情報セキュリティを考える場合、包括的な考え方で対応することが重要。情報セキュリティ管理マネジメントシステム（ISMS：Information Security Management System）とは、情報を資産としてとらえ、その情報資産を守るための経営管理上のガイドラインであり、必要な基準を満たした情報セキュリティ管理体制を整えているかどうかを第三者によ

る審査を行い、登録するもの。

ISMS構築のステップとして、セキュリティポリシーを定めて、教育・訓練の徹底をすること。

日本に足りない部分は、「リスク分析・リスク管理」の考え方。たとえば、リスク分析では、概要のみで詳細なリスク分析はしていないことが多い。損失金額について、算出しておくべきだ。

また、官公庁や企業もトラブルレポートを公開することで、リスク分析、リスク管理が行なえるようになる。少なくとも、省内で行なったトラブルは公開すべきではないか。トラブルレポートによって、修復するために必要な損失金額、必要な人や時間を計算することで、リスク分析を行なうためのデータベースの作成が可能になる。

また、リスク管理に関連することでは、リスク転化するための情報セキュリティ保険への関心も高まっている。

情報セキュリティ教育についても、日本は遅れている。情報システムの利用者、管理者、技術者それぞれに必要な。

内部監査も重要である。内部統制体制を確立し、検査と監査を行なっていく。日本的な検査では、1人の者が権限を行使できてしまうが、監査であれば2人が必要。重要なものについては、2人の鍵がないと開かないなどの仕組みにすべきだ。

e-Japan戦略を策定している、IT戦略会議のメンバーには、情報セキュリティの専門家は1人も入っていない。こうしたことも大きな問題だ。

#### 司会

これまでネットワークなど狭義のセキュリティについて議論してきたが、今のレクチャーを聞き、自然災害などを含め、セキュリティの範囲が広いことがわかった。

世界中のインターネットユーザーは、被害者にもなり、加害者にもなる。その中で、セキュリティについて正確なことが語られていない。われわれでしっかり議論をしていく必要がある。



藤谷 護人氏（エルティ総合法律事務所 所長弁護士）



藤谷 護人氏

司会（坪田）

続いて、法律面から情報セキュリティについて、藤谷氏からレクチャーしていただく。

藤谷氏

今回私のレクチャーは、以下のことを目標として進めていきたい。

1. セキュリティは組織の存亡に関わる重要な問題であることを理解する
2. 3つの脆弱性を理解する
  - コンピュータ技術のメリット、デメリット（光と影）を考えないと使えない
  - ネットワーク技術の根源的不完全性
  - 不可視性（デジタル情報は目に見えない）
3. 統制原理（天秤理論）を理解する
  - 内部統制原理
  - ネットワーク的統制原理
  - 系列統制原理
4. 行政権力におけるセキュリティの特別性を理解する
5. 住基ネットの構造的脆弱性を理解する

### コンピュータ・セキュリティに関わる事件

具体的な例を挙げて解説する。

平成10年 テンプスタッフの登録9万人の個人データ（美人度ランキング含む）が流出

テンプスタッフが、登録している派遣スタッフの個人情報が流出したもの。美人度のランクなども記載されており、被害者にとっては問題は大きい。

このように個人情報が流出した場合の、被害者への慰謝料はどのくらいになるだろう。この件は実際は和解したが、弁護士団が結成されて法廷で争ったら、1人10万円ずつとして慰謝料の総額は90億円になる。このようにデータベースのデータが盗まれたり、流出すると、1件1件の被害金額は少なくとも、データ件数が多ければ大きな経営上のリスクとなる。企業の存亡に関する問題だ。

平成6年 江戸川区で住民健康診断データ（病歴含む）で9万人分が流出

江戸川区が保管していた住民健康診断データ、9万人分が流出した事件。この場合、被害の中身が均質ではない。深刻な病歴がある人にとっては、データは非常に重要で慰謝料の請求額は100万円くらいになる可能性もある。そうすると賠償責任は総額で900億円。江戸川区の1年の総予算は1500億円。財政が破綻する。実際は、1件も訴訟は起こらなかったが。

平成11年 宇治市全住民のデータが流出。ネットで販売

宇治市でも全住民のデータが流出し、インターネットで取り引きされたことが発覚した。この事件も、1人のデータを1万5000円で計算すると、22万人分で賠償責任は33億円と計算できる。

自治体も国も、企業もリスクは同じ。情報セキュリティが、組織の存亡に関わってくるのだ。

### コンピュータ技術の脆弱性を理解する

コンピュータ技術のメリットの高速処理性は、裏を返すと、短時間に盗取改ざんが可能

ということでもある。コンピュータ技術の光（メリット）と影（デメリット）は、コインの表と裏のように切り離して使うことはできない。デメリットへの対策なくしては、メリットも享受できない。

ネットワーク技術の根源的不完全性が、脆弱性の原因になっている。UNIXやWindowsでは、セキュリティホールを完全になくすことはできない。永遠の後追いである。

コンピュータ・ネットワークの不可視性も原因のひとつ。通常、人間は情報の7～8割を「視覚」に依存して認識している。しかしデジタル情報で起こっていることは、イメージができず、本来的に弱い。そこで問題が起こる。たとえば、電源を落としたパソコンと、台帳を棚にしまった状態を、同じように考える人もいる。電源を入れれば、パスワードがかかっていない状態でも危険と思わない。

最近では、ノートパソコンの窃盗も多い。ハードディスクの容量が大きくなり、データを入れて盗まれた場合に、経済的損失は非常に大きい。

### 法律による抑止力の「穴」

昭和62年に改正された刑法で、電磁的記録不正作出罪、電子計算機損壊等業務妨害罪などはあるが、「電磁的記録窃盗罪」については、現在は結論が出ていない。

平成12年に施行された不正アクセス禁止法では、なりすまみや、セキュリティホールを攻撃する行為、他人のID、パスワードを第三者へ提供する行為などを定めているが、電子的記録の窃盗については、バリエーションが多すぎるので、法で抑止することができない。

### コンピュータ・セキュリティ確保の方策

組織統制の原理を考える。権限委譲が行なわれると、濫用・逸脱のリスクが起こってくる。企業は、リスクと同じ金額を用意しておく必要がある。

従来のタイプの企業では、発注したら元請との契約はしているが、その下の下請、孫請、フリーターには、直接統制できない。契約には守秘条項があるだけだ。

### コーポレートガバナンス、行政の優越性について

ネットワーク的統制が必要。コーポレートガバナンス（遵法経営）が求められている。自治体など、行政にとっても、コーポレートガバナンスが求められる。ただし、以下のような行政権力の特色を理解しておくこと。

- 1) 優越性
- 2) 一方性
- 3) 権力性
- 4) 公定力
- 5) 自力執行力
- 6) 不可争力

情報を集める場面でも、行政の優越性は変わらない。住民には選択肢はない。このような行政には、上記のような特色があるので、情報を正しく扱わなければならないのである。

### 住基ネットワークにおける個人情報の保護・セキュリティの構造的問題と対策

改正前の個人情報保護・セキュリティの統制は、当該地方公共団体の内部統制の問題だった。内部統制がされていれば、大きな問題は起こりにくい。

改正後は、3287団体と7省庁がネットワークされる。内部統制の問題を逸脱し、ネットワークされた分のリスクがおこる。たとえば、千代田区なら、これまで住民4万人の情報を内部統制で管理していたものが、1億2692万5843人のデータが見られるようになる。しかも、他の自治体の職員がデータを盗取するなどの行為について、当該の長の管理はおよばない。

ネットワーク運用管理組織の構造的脆弱性がある。住基ネットの行政事務の責任は、都道府県の長にあるが、その意識はない。市町村の長にあるように思われている。

また、通常は電子データは、サーバを管理する組織にあるが、住基ネットでは指定情報処理機関であるRASTEC（地方自治情報センター）には権限はない。

セキュリティ確保の根幹である内部統制原理を適用する基盤が欠如している。未知の巨大システム・リスクに対処するには、未曾有のリスクマネジメントが必須である。何らか

の手を打たないと、脆弱過ぎるのだ。

**司会**

情報セキュリティについて法的な解釈と、問題提起をしていただいた。ここからは、会場の参加者の方々も一緒に議論に入っていきたい。





会場風景

司会（坪田）

内田氏、藤谷氏に、情報セキュリティについての考え方や課題を解説していただいた。これからはみなさんとディスカッションしていきたい。

### セキュリティの実態と調査方法

前川 徹氏（早稲田大学 国際情報通信研究センター 客員教授）

内田氏のレクチャーの中で、ハッカーは内部犯罪が多いとのことだったが、どのように調査しているのか。産業スパイを目的としたハッキングは、痕跡を残さないこともあると思うが。

内田氏

内部犯行が7割と言われているが、実は米国のSCIの調査レポートには、内部犯行が7割とは記述していない。今から10年くらいまでに、PC WORLDなどのメディアに掲載されたコンサルタント会社が調べた資料で80%と書かれていたことが流用されているようだ。

SCI/FBIの報告書では、割合については述べていない。

質問のように内部犯行については、見つからないケースもあるだろう。届けなければ、犯罪統計などにも出てこないからだ。

古川 泰弘氏（情報セキュリティ アナリスト）

韓国のCERTでは、不正アクセス検知のソフトを配布している。そうしたソフトを使えば、情報が取れるのではないか。

オーストリアもCSI/FBIと同じ手法で調査しているが、日本は別の手法で調査しているので実態が分かりにくい。

内田氏

韓国は、不正検知するための情報を集めている。日本にはそのような仕組みがないが、日本でも行ないたい。

### 世界から孤立する、日本のネットワーク

藤原 宏高氏（ひかり総合法律事務所 弁護士）

情報セキュリティをひとつの学問対象にしたいと考えている。どうだろうか。

内田氏

確かにそう思う。日本のセキュリティ教育は、米国などに比べ、15年遅れている。文部科学省で認定する重点校、30校に入れて欲しい。それでも予算は、1年間に1億円。1桁、2桁違っているのではないか。

藤原氏

納めたソフトに一定のセキュリティ品質がないと、損害賠償を負うことにすると良いと考える。そのためにもセキュリティ教育が必要だ。

住基ネットは、明らかにセキュリティ意識がない人が設計したとしか思えない。日本の技術者がセキュリティ教育を受けていない例だと思う。

安田 浩氏（東京大学 国際・産学共同研究センター 教授）

まさにネットワークの利便性とセキュリティは、コインの裏と表。技術の後追いと言われたが、技術屋としては先取りが必要だ。誰が責任者なのかを明確にし、是正する。その上で取り組み、証拠を出すことだろう。

セキュリティを学問対象にすることについては、言い続けているが、基準がないことなどから確立していない。

重要なのは、日本のネットワークが外から見て安全かどうかを問うことだ。そうでないと、世界全体のネットワークから切り離されてしまうだろう。するとどうなるか。海外に行きたくても行けない。そうした時代になってくる。いかに早く意識を高め、進めるかが重要なのだ。

住基ネットは、それを問われているいい例だ。ここでセキュリティのレベルを上げるための最大の努力をする意識が必要。このままでは、3年後には、日本のネットワークは見向きもされなくなり、ビジネスもできなくなる。具体的に何ができるかを、みなさんと知恵を出していきたい。

**内田氏**

住基ネットについては、あまりに情報が少ないので、議論ができない。オープンにして欲しい。クローズになっていると、議論もできず、狂信的に反対する状態になっている。

リスクをどう考えるのか、どうするのかを考えずに、必要か必要でないかの議論が先走っている。

**藤谷氏**

システムというのは、組織を根本的に変えるパワーがある。たとえば、徴兵制をとるためには、これまで3280の地区町村に住民情報を出さなければできなかったが、今回、名簿を作るためのデータができる。また、関係者からは「徴税名簿ができる。国のためにいいのだ」という発言も聞かれるが、そのための議論はしたのかと問いたい。

### **見えない住基ネットのセキュリティ。情報をオープンに**

**司会**

ネットワークのセキュリティについてはどうなのか。

**高木 浩光氏（産業技術総合研究所グリッド研究センター セキュアプログラミング長）**

あやしいサイトにアクセスすると、モバイル攻撃といってクライアントが攻撃する、受動的攻撃が現われている。これはファイアウォールでも無効。

予防するひとつの方法は、同じ端末で住基ネットとインターネット接続を行わないことだが、住基ネットのソフトのカタログには同じ画面に両方のソフトの画面が出ているものもある。そのソフトを採用しているかどうか、自治体は情報を出してくれない。

認証方法についても問題がある。民間の認証局のものを利用してはどうかと提言したが、全部国で行なわなければならないという。信頼できない方法で統一すると、問題が起これるのではないか。

新しい開発手法を知っている人がいても、現場の人しか知らない状態だ。そうした技術情報をウォッチしている研究者の声を聞いてくれる場がない。なんとかして欲しい。

**内田氏**

現時点では、セキュリティ関係の学会3つで連携していく必要があると思っている。もっと提言をしていかななくてはならない。日本はセキュリティを専門にしている人は少ない。何かしないと、世界にどんどん置いていかれる。

**古川氏**

住基ネットは、動き出してしまうとその後は知ることができない。不正アクセスの数やウイルスによる攻撃があったことなど、情報を公開するといいいのではないか。

**藤原氏**

住基ネットについては、藤谷氏がマニュアルを配れと提言されたが、市町村は読む義務はない。また、読んでもわからないという。この仕組みがいかに間違っているかを表わす例だ。

1つのネットワークを、3つの法律でコントロールする。分断された何の脈絡もない法律になっている。

**前川氏**

いずれにしても情報を公開してもらいたい。便利な点もあるわけだから、情報を公開し、専門家が集まって、危険性をゼロに近づけるために正しく議論することが必要だ。

**川島 昭彦氏（日本ペリサイン 代表取締役社長兼CEO）**

個人認証についてもいろいろな動きがあるようだが、住基ネットに関しては現状が分からず、オープンにされていない。各家庭から接続できることがメリットだと言われているが、より危険でもある。将来に向けて明らかにし、問い詰めていく必要がある。

### **セキュリティ技術者の専門家教育が必要**

## 司会

会場からの質問やコメントはあるだろうか

## 意見 1

セキュリティ教育について、文部科学省では大学に任せるという姿勢だ。専門教育を受けた学生を企業が受け入れるかどうかが問題だ。現状では、企業の中でセキュリティ技術者が評価されにくい。資格制度もない。社会的なコンセンサス、資格制度も必要ではないか。

## 前川氏

確かに、情報処理試験にもセキュリティに関する問題は出ているし、情報セキュリティアドミニストレーターの資格もあるが、いずれも一般的な内容にとどまっている。

## 内田氏

現在の情報処理試験に懐疑的にならざるを得ないのは、継続的な教育がないことだ。

## 藤原氏

政府が、電子政府の構想の中で、セキュリティ技術者をおくことを義務づければ、1万人は雇用できる。行政が進めれば、民間も追随するはず。セキュリティ法制定にご協力いただきたい。

## 安田氏

藤原氏の意見を、大いに応援したい。私はセキュリティ技術者の認定機関をつくり、優遇しようと、ずっと言ってきた。これは一省庁ではできない。縦割り行政ではできない話。内閣府でないとだめだ。そうした努力をみなさんでしていきましょう、言いたい。

## 意見 2

セキュリティに関する問題などの情報をどう流すかも問題だ。米国ではCERTが協力している企業と情報チャンネルを持っているが、日本ではオープンか、秘密かのどちらかしかない。適切な情報交換チャンネルが必要。

## 高木 寛氏 ( j TRUSTc, inc 代表取締役 )

JP CERTには、その機能がない。何故か。日本ではベンダーとJP CERT間で信頼関係ができていない。しかし、CERTがそうした機能を持っているかということ、そうでもない。基本的には、ベンダーと直接交渉しろという姿勢。

前回の議論でも、セキュリティ技術者が何をしているのかわからないという意見があった。今は、システム管理が主なので、見えてこないのだろう。ソフトウェア開発をしている会社の中で、セキュリティ部門があれば、問題はわかってくるはずだ。しっかりとやって欲しい。

## 司会

今回もさまざまな意見が出た。今回、セキュリティの全体像を示していただいたが、非常に広い範囲であることがわかってきた。トータルに、どのように社会的に取り組んでいったらいいのか。われわれで、できるだけのことをしたい。

