

## 第4回高度情報セキュリティ実践講座の報告

2006年12月6日

NPO法人電子自治体アドバイザークラブ

### 第4回 高度情報セキュリティ実践講座の概要

日時: 平成18年12月6日(水) 受付: 13:00 ~ 13:30 講座: 13:30 ~ 16:50

会場: 奈良市北部会館 多目的会議室1 (近鉄高の原駅より、徒歩5分)

参加者: 28名 内訳: 自治体関係者 10名 企業関係者 10名 一般 8名

### 講演 - 1: 企業における情報セキュリティ確保に向けた政府の取組

13:30 ~ 15:00

経済産業省商務情報政策局 情報セキュリティ政策室 課長補佐 村野正泰氏

代理 同室担当係長 成田裕幸氏

#### 【概要】

近年、企業は自身の被害の局限化や法令遵守の観点に加え、社会的責任の観点も踏まえた形で情報セキュリティ対策に取り組むことが要請されている。このため、コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること、すなわち「情報セキュリティガバナンス」の確立が求められている。ここでは、情報セキュリティガバナンスの確立に向けた政府等の取組みについて紹介する。



【成田 裕幸氏のプロフィール】

経済産業省 商務情報政策局 情報セキュリティ政策室 企画係長  
平成 13 年経済産業省に入省。貿易経済協力局通商金融・経済協力課に配属。その後資源エネルギー庁資源・燃料部 石油・天然ガス課勤務を経て、平成 17 年 6 月より現職。商務情報政策局情報セキュリティ政策室では、主に情報セキュリティガバナンスの普及などを担当。

**休憩 10 分**

## 講演 - 2: 情報セキュリティ監査について

15:10 ~ 16:40

NTT 西日本(株)ソリューション営業本部担当部長 公認情報セキュリティ監査人 柚木勝博氏  
代理 ソリューションビジネス部 公認情報セキュリティ主任監査人 上山 太郎氏

【概要】

組織のセキュリティ対策が適切に実施されているかを、独立かつ専門的知識を有する専門家が客観的に評価する「情報セキュリティ監査」に対するニーズが高まっています。この講座では、情報セキュリティ監査基準や管理基準の概要、監査方法、監査の市場動向などについて解説します。また、監査の現場において実際にどのようなことが実施されているかを豊富な実績を持つ情報セキュリティ監査人が、経験を基に説明します。



【上山 太郎氏のプロフィール】

西日本電信電話株式会社 ソリューション営業本部 ソリューションビジネス部  
公認情報セキュリティ主任監査人 上山 太郎

## 所感

1. 講演 - 1: 企業における情報セキュリティ確保に向けた政府の取組(経済産業省成田裕幸氏)  
インターネットの爆発的普及により、IT は家庭での電子メール活用、職場での PC など、身近な生活の出来事になってきた情報セキュリティに関する現状を分析し、政府における統一的・横断的な政府全体の取組体制について説明があった。内閣官房情報セキュリティセンター(NISC)及び情報セキュリティ政策会議を設置し、「第 1 次情報セキュリティ基本計画」を作成した。政府機関統一基準の運用の下で、経済産業省施策の概要の説明があった。新たな脅威への対応のため、当省の施策も新たな対応策が必要になり、最近では早期警戒体制の強化・拡充(ポット対策事業)に取り組んでいる。当省が実施する主な普及広報活動として、企業向け普及広報、個人向け普及広報、人材育成(国家試験の実施)について詳しく紹介があった。組織的対策の推進として、ISMS 適合性評価制度の概要、情報セキュリティ監査制度、対策ベンチマークや報告書内容、その他、事業継続計画(BCP)、策定ガイドラインについて解説された。技術的対策の推進として、国際基準など、国際的な取り組みの説明があった。もりたくさんの内容であり、時間不足の状況であった。これらの国の施策が進められているが、特に地方の中小の自治体や企業にとって、なかなか進んでいないのが現実であり、強制力を持った施策やその現実的な支援策が必要ではないかとの質問があった。

2. 情報セキュリティ監査について(NTT 西日本公認情報セキュリティ主任監査人 上山太郎氏)  
本日の講演の内容は、情報セキュリティ監査の概要、他の制度と情報セキュリティ監査の関係、監査の実施フロー、情報セキュリティ監査の動向、監査における指摘事項の対策例、についての説明であった。情報セキュリティマネジメントと情報セキュリティ監査、及び監査のメリット、対象について説明があった。「情報セキュリティ制度」に関わる基準について、管理基準と監査基準があり、管理基準の構成として、10領域、36項目があり、監査基準の構成として、基準(一般基準、実施基準、報告基準)、ガイドライン(実施基準ガイドライン、報告基準ガイドライン)、モデル、また、助言型監査と保証型監査の違い、ISMS 認証と情報セキュリティ監査の関係、について詳細な説明があった。監査の実施フローについては、実施基準ガイドライン、準拠規範、個別管理基準、などに沿って行い、実施フレームワークとして、監査計画の立案、監査手続の実施、監査調書の作成と保存、監査報告書の作成、監査結果のフォローアップについての詳細な解説があった。監査のPDCA サイクル、監査の種類、外部監査と内部監査及び自己点検など、対象毎に使い分けが可能である。監査の動向として、都道府県では、大半の自治体で監査を実施しており、市町村ではこれから実施が進んでいく。NTT 西日本(株)の取り組み実績や、共同監査のメリットについて説明があった。

本日は、経産省の成田氏より、国の取り組み内容について詳しく説明があり、それを受けて、NTT 西日本(株)の上山氏より、監査人の立場で、監査主体、被監査主体の対応のあり方について詳しく解説され、監査の全体像が理解できた。時間が不足気味であった。成田氏より、パブリックコメントへの参加の要請があった。

## 講演会風景



次は最終回です。

第5回高度情報セキュリティ実践講座に、ぜひ、ご参加ください。

**予定日、会場の変更**

予定日: 1月10日(水)、 受付: 13:00~13:30 講座: 13:30~16:50

会場: 奈良市北部会館 3階 多目的会議室1 (近鉄高の原駅から徒歩5分)

講演 - 1: インターネット時代のネットワーク-クリテシ- (帝塚山大学経営情報学部教授 日置慎治氏)

講演 - 2: コンピューターウイルスの脅威と対策 (帝塚山大学経営情報学部教授 高瀬宜士氏)

懇親会

**【共催】:** 帝塚山大学 経営情報学部 高瀬研究室  
NPO 法人電子自治体アドバイザークラブ(e-AAC)  
( <http://e-aac.naist.jp/e-AAC/> )

**【後援】:** 近畿経済産業局、奈良県、奈良県市長会、奈良県町村会、  
奈良県中小企業支援センター

**【協力団体】:** 奈良県警、帝塚山大学、奈良先端技術大学院大学、富士通(株)  
NTT 西日本(株)、日本電気(株)、近鉄ケーブルネットワーク(株)