

# 会計システム専門監査人部会 活動報告

公認会計士事務所でのITセキュリティを考える - セミナー実施報告  
Thinking about IT security in CPA office

システム監査学会  
会計システム専門監査人部会

発表者: 平塚康哲

2013年 6月 7日

**JSSA**

# 会計システム専門監査人部会の活動

会計システム専門監査人とは、平成20年度から施行された改正金融商品取引法(J-SOX法)において、公認会計士による会計監査の中で、主にIT統制に対する監査を行う専門監査人。

ITのシステム監査知識と会計監査に対する理解が要求される。

これまでに、会計システム専門監査人が使用する目的で「会計システム監査実施ガイド」の作成、実践的な会計システムのシステム監査を行う事を目指し「SAP ERPの業務処理統制の実際的例の研究」における成果物の作成を行って来た。

昨年度は、新たな研究テーマの策定を進める一方で、日本公認会計士協会東京会と、「事業所運営におけるITセキュリティ」をテーマに共同で研究を行い、その結果としてセミナーの開催を実施した。

## テーマ概要

- ◆ 公認会計士協会では、世の中の情報セキュリティへの関心の増加に伴い、公認会計士の業務における情報セキュリティ向上を目指している。
- ◆ 基本的に各監査法人の責任で行われる為、社内に専門家を保持していない中小監査法人における情報セキュリティへの対応について、課題となる点が多い。
- ◆ セキュリティという専門的な分野を理解し、対応を実施する事は、一朝一夕にはできない面もあり、地道な理解と実施・点検の繰り返しになる事は理解されている。
- ◆ まずは、情報セキュリティ上のリスクを理解し、その対応を考えられる様になる事を目的とした。
- ◆ 情報セキュリティは、一般的には広い範囲にわたるが、今回は、特に、ITを利用する際に考慮すべきリスク、即ち、ITセキュリティを中心に、公認会計士の業務に即してリスクを検討する事になった。

## セミナーの実際

**実施日：2013年2月15日 金曜日**

**実施時間：合計2時間30分**

**実施場所：日本公認会計士協会 会議室ホール**

**対象者：公認会計士協会東京会所属会員**

**セミナー題目：**

**ITセキュリティ研修**

～実務に即した理解を目指して～  
公認会計士事務所におけるITセキュリティ

**当日参加者数：約500名**

# セミナーアジェンダ

**Session 1: 事務所運営におけるITリスクの実際**  
ある公認会計士事務所に潜むITセキュリティのリスク

☆シナリオに即して、ITセキュリティのリスクを指摘、解説

**Session 2: ITリスクの意味と対策**

ITリスクを回避する対策とは？  
世の中で発生している事例紹介

☆ITセキュリティのリスクに対する対策の解説

# セミナー内容(1)

## 典型的な公認会計士事務所の状況に即して

ITは今や私たちの日常に深く係っています。ITなくしては私たちの日々の業務は進めようもありません。しかし、そこには様々なリスクがありそうです

このコースでは、私たち公認会計士の業務に潜んでいる、ITに関係したリスクにはなにがあるのか、それはどういう意味を持っているのか、それを防ぐにはどうしたらよいか・・・を考えます。

一般の解説書では専門的な言葉が使われていて馴染みがなく、私たちの業務のどこに関係しているか即座には理解できないことがあります。

このコースでは、現実感をもってITリスクと対策が理解できるように、事例をもとにして進めます。

この事例を通じて、私たちの業務におけるITセキュリティについて、検討してみましょう。

2013/2/15

©2013 K.Kamachi/Right Way SAC株式会社&Partners

6

## セミナー内容(2)

### 1. Aさんの悩み

Aさんは、小規模な監査法人の代表社員であり、かつ税理士登録をして税理士事務所を開業しています。

また、新興市場上場会社Z社の社外監査役、他の会社の取締役、科学研究所の設立を支援した関係でその理事職に就いています。

Aさんは、最近、ITセキュリティに関する様々な報道や、協会での話題から、ITセキュリティにはとても関心を抱いています。パソコンのクラッシュにも再三遭遇し、いつからこんなにITに依存するようになってしまったのかと嘆きながらも、それなくしては、今のように効率的な業務ができないことも感じており、心は複雑です。

2013/2/15

©2013 K.Kamachi/Right Way SAC株式会社&Partners

7

# セミナー内容(3)

## 監査法人-2

### (2) IT環境

事務所は、所員全員の机のある大居室の他、応接室2つ、会議室1つがあり、  
#1 を繋げば、インターネットにアクセスし、インターネット通信会社のサービスを利用  
ドキュメントサーバーにアクセスは遮断できるようなセキュリティ対策を明を受けています。また、アン

#1

ドキュメントサーバーに  
保管中の資料の第三者  
による盗み見・書き換え

調査が電子化されているが、調査報告書の様式以外は紙(11.12)で作成し  
綴じていますが、最近は徐々に電子化が進んでいます。

事務所内にドキュメントサーバー(1.13,14,15)において、各人が作成した電子資料  
は基本的にこのサーバに収納し、各人のパソコンには置かないようにしています。  
このサーバは、値段は高いものですが、すでに、3年ほど前から、使用しています。  
クライアントのデータは、往査時にUSBメモリ(2.16,17)で入手することもあります、  
それを各人のパソコンに移してから作業をし、調書化した後は事務所のサーバ  
に格納します。

2013/2/15

©2013 K.Kamachi/Right Way SAC株式会社&Partners

14

## セミナー内容(4) [リスクの分類]

### 潜在リスクの分類(セッション指摘以外)

・潜在リスクについて、指摘セッション中に指摘しなかった事項を、ITセキュリティの観点から情報漏洩分類毎に特徴を挙げると以下ようになります。

- ①管理ミス(誤廃棄など)  
ウイルス感染が、サーバーやインターネットを通してPCに感染する潜在リスクが最も高いです。次にメールアドレス流用による業務上の信用に係る弊害が生じる可能性があります。
- ②誤操作(誤送付、誤送信など)  
圧倒的にメールアドレスの誤りや、関係者以外に誤送信する潜在リスクが高いです。また、添付ファイルを保護(暗号化、パスワード設定)漏れで送ることによる潜在リスクが高いです。
- ③不正な情報持出し  
サーバへの不正アクセスやウイルス感染による不正な情報持出しの潜在リスクがあります。また、ITセキュリティ以外のソーシャルエンジニアリングに分類されるなりすましやスキャベンジングによる不正な情報持出しの潜在リスクがあります。
- ④盗難、紛失・置忘れ  
PCの盗難・紛失や記録媒体の盗難・紛失による情報漏えいが多く潜在リスクが高くなっています。

2013/2/15

©2013 Right Way SAC株式会社&Partners

15

# セミナー内容(5) [指摘一覧]

## 潜在リスクの分類(セッション指摘)

セッション中に指摘した事項			
項番	潜在するリスク	情報漏洩分類	情報漏洩分類
1	ドキュメントサーバーに保管中の資料の第三者による盗み見・書き換え	不正な情報持出し	盗み見
2	事務所へ持ち帰る途中でのUSBメモリの盗難・紛失	紛失・置忘れ	記録媒体の盗難・紛失
3	誤った送信先にメールを送信	誤操作(誤送付、誤送信など)	メール誤送信
4	Winny等の無許可インストール	管理ミス(誤廃棄など)	その他
5	パスワードの設定漏れ、パスワードの漏えいによる不正アクセス	不正な情報持出し	不正アクセス
6	クラウド系サービスに存在するリスク	不正な情報持出し	マネジメントシステム不徹底
7	誤った上書きによる保存すべきバックアップデータの消失	誤操作(誤送付、誤送信など)	バックアップ誤操作
8	個人所有パソコンの業務使用	管理ミス(誤廃棄など)	マネジメントシステム不徹底
9	スマホからの情報流出	不正な情報持出し	その他(スマホ、フェイスブック、PGP)
10	パターンファイルの更新漏れ、ソフトのサポート契約切れ	管理ミス(誤廃棄など)	マネジメントシステム不徹底

2013/2/15

©2013 Right Way SAC株式会社&Partners

16

合計61個のリスクを指摘



# セミナー内容(6)

## 想定されるリスクと対策

### —ドキュメントサーバーの資料の盗聴・書き換え

<b>リスク</b>	<p>1 ドキュメントサーバーに保管中の資料の第三者による盗聴・書き換え</p> <p>【説明】 権限のない第三者によるアクセス</p> <p>【説明】 攻撃者は、サーバーのソフトに潜在している安全上の欠陥を発見し、攻撃し、侵入し、重要情報を搾取</p>
<b>対策1</b>	<p>【優先対策】</p> <ul style="list-style-type: none"> <li>・サーバーのアクセス権限の設定</li> </ul>
<b>対策2</b>	<p>【優先対策】</p> <ul style="list-style-type: none"> <li>・サーバーOSやWordなどのソフトの欠陥の修復</li> </ul>
<b>対策3</b>	<ul style="list-style-type: none"> <li>・専門家によるサーバーの安全性のチェック</li> </ul>

2013/2/15

©2013 Right Way・SAC株式会社&Partners

64

# セミナー内容(7)

## 補足説明

### リスクとなる理由

- 権限のない第三者によるアクセスが発生する。
- サーバーやパソコンのOSや、Wordなどの主要ソフトは、世界中の「攻撃者」の標的となりやすい。
- 攻撃者は、ソフトに潜在しているセキュリティホールと呼ばれる安全上の欠陥を発見し、攻撃し、侵入し、重要情報を搾取する。

### 具体的な対策例

- 資料毎にアクセス権を設定し、権限のない第三者によるアクセスを防止する。
- マイクロソフト社などのソフト会社は、安全上の欠陥を修正するためのプログラムを定期的に無償で発行している。

Windows Updateを「自動更新」に設定しておくことで、最新の修正プログラムをサーバーやパソコンに適用して欠陥を修復する。

2013/2/15

©2013 Right Way・SAC株式会社&Partners

201/5 65

## 実施後の考察

- 公認会計士業務及びその付随業務に関して、情報収集、意見交換が出来た。
- 会計システム専門監査人としての観点で、システム監査・セキュリティ監査視点でのITセキュリティのリスクの指摘が出来た。
- 実施アンケート結果からは、非常に良いという評価を受ける事が出来た。
- 業務に即した解説の方法が、高評価につながったと考えられる。
- 今後、次のステップについて検討を考えたい。
- 公認会計士協会東京会に対しては、このような機会を与えて頂いた事に大変感謝を感じている。

御清聴ありがとうございました

システム監査学会  
会計システム専門監査人部会