

～官民情報セキュリティ担当者連携！プラクティス交流セミナー～

「安心安全ネットワークによる情報セキュリティ対策底上げを考える」

## 開催結果報告書

日時: 2007年7月26日(木) 13:15 ~ 17:30

場所: 株式会社リコー 本社「i-salon」

主催: 電子申請推進コンソーシアム

後援: 財団法人 地方自治情報センター

日本行政書士会連合会 / MPUF

協賛: 株式会社 リコー 協力: MPUF ISMS研究会

## 開催風景

---



i-salon のシンボルモニュメント「RING of TRUST」で電子申請推進コンソーシアム セキュリティセミナーを投影案内。産公学民の皆さんにご参加いただき盛況な会となりました。



基調講演  
中田光一 氏  
内閣官房情報セキュリティセンター  
参事官補



主催者挨拶  
榎場博文 氏  
電子申請推進コンソーシアム 事務局長



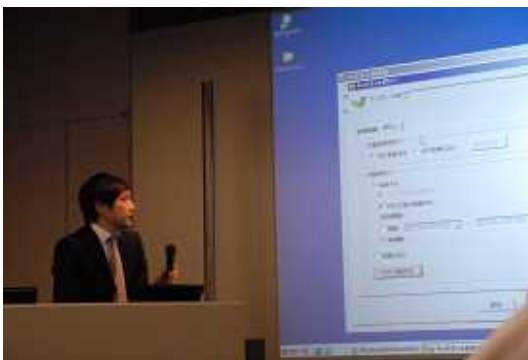
特別講演  
石川家継 氏  
財団法人地方自治情報センター  
セキュリティ支援室長



セミナー1  
栗原正美 氏  
電子申請推進コンソーシアム 委員



セミナー2  
小島英揮 氏  
電子申請推進コンソーシアム 会長代行



水野嘉仁 氏 電子申請推進コンソーシアム 委員



スマートチャットで自治体職員の疑問に答える中田氏



スマートチャット、グループディスカッションの様子



全体の意見交流の様子

## 開催概要

---

1. 名称とテーマ ~ 官民情報セキュリティ担当者連携！プラクティス交流セミナー ~  
安心安全ネットワークによる情報セキュリティ対策底上げを考える
2. 開催日 2007年7月26日(木) 13:15~17:30
3. 会場 株式会社リコー 本社「i-salon」  
東京都中央区銀座8-13-1 リコービル2F
4. 主催 電子申請推進コンソーシアム
5. 後援 財団法人 地方自治情報センター  
日本行政書士会連合会 / MPUF
6. 協賛 株式会社 リコー
7. 協力 MPUF ISMS研究会

## 8. プログラム

主催者挨拶 榎場博文氏 電子申請推進コンソーシアム 事務局長  
基調講演「我が国における情報セキュリティ政策の基本戦略について」  
中田光一氏 内閣官房情報セキュリティセンター 参事官補  
Q & A・意見交流

特別講演「地方公共団体の情報セキュリティ  
~ 自治体 ISAC から自治体 CEPTOAR へ ~」  
石川家継氏 財団法人地方自治情報センター セキュリティ支援室長  
Q & A・意見交流

セミナー1「情報のライフサイクルを意識したセキュリティ  
~ 電子情報と紙情報の2相において ~」  
栗原正美氏 電子申請推進コンソーシアム セキュリティ委員会委員  
(株式会社リコー MA事業部 公共ソリューション企画グループ)

セミナー2「経済産業省の事例に学ぶ！  
電子文書のライフサイクルポリシーに準じたセキュリティ統制のあり方」  
小島英揮氏 電子申請推進コンソーシアム 会長代行  
(アドビ システムズ 株式会社 マーケティング本部 部長)  
水野嘉仁氏 電子申請推進コンソーシアム セキュリティ委員会委員  
(日立ソフトウェアエンジニアリング株式会社 公共社会システム事業部)  
講師、情報セキュリティ担当者を中心とした交流  
(Q&A・問題、プラクティス共有)

## スマートチャット&ディスカッション

---



現在、様々な分野や立場の組織や人がチームを組んで、業界の問題、地域の問題に取り組む必要が増してきています。今後の電子地域に関する問題解決は、様々な業界、組織、職種の方が、問題を抱える当事者を中心に、対等な立場で自身のプラクティスや知恵を出し合いながら行っていくことが重要になります。シリコンバレーでは、この方式をジョイントベンチャーウェイと名づけ、経済、環境問題から、宇宙開発や地域イノベーションなどの、様々な分野の問題解決、価値創造に適用しています。

この交流セミナーには、様々な分野の方が参加されています。そこで、この交流セミナーを通して、参加者が業界、組織、立場の壁を越えて、自由に議論し、ネットワークを広げ、ジョイントベンチャーウェイを実践されることを目的に、各講演後にスマートチャット（15分の意見交流）を行いました。

今回、スマートチャットは6グループで行われ、講演内容について各グループで15分の意見交流後、講師を交えて全体でディスカッションを行いました。意見交流の内容、ワークシートの回答内容については次頁のとおりです。

## スマートチャット分析

### 『わが国における情報セキュリティ政策の基本戦略』

地震や台風などの自然災害が続いたことが影響しているのか、国家・自治体の緊急時の事業継続性の確保に関する問題意識の高さが目立った。また、欧米と比較して遅れている行政部門の情報開示やその根拠となるモニタリング方法や計測値については、全てのグループが課題として上げている。

この2点について、政府の政策担当者へのヒアリングや部会等で意見・提言の取りまとめを行いフォローアップしたいと考えている。

### 『地方公共団体の情報セキュリティ』

自治体の情報セキュリティに関する懲戒規定、情報公開、学校における情報セキュリティ、CEPTOARの脆弱性調査サービス等が、全てのグループに共通の話題となっていたようである。特に、CEPTOARのセキュリティ診断サービスについては、多くの賞賛の声が上がっており、同様のサービスの質、量、範囲の拡大を産官学民の連携により実現できれば、日本独自の情報セキュリティ体制の構築につながるのではないかと感じた。今後、LASDECと共催している電子地域連携部会の中で、WG化を検討したい。

## スマートチャット

この交流セミナーは、産公学民の様々な分野の方に参加いただき、問題点について語り、これを整理し、解決策を見つける場となることを目指しています。今後もコンソーシアムの重要な役割の1つとして、このような話し合いの場を設けていきたいと思えます。

以下に、講師の中田光一氏（内閣官房情報セキュリティセンター）、石川家継氏（地方自治情報センター）を交えたスマートチャットと、全体でのディスカッションの中から、主な要望、課題を紹介します。今回は、ランダムに要望、意見を出し合いましたが、今後のセミナーではテーマを絞って討論を行っ

ていく予定です。

### 統一基準、実務に応じた見直しを

今年6月の改訂版（『政府機関の情報セキュリティ対策のための統一基準（第2版）』）については、参加者から実務に応じた見直しが求められた。「全部をやると思うといつまでも出来ない。政府基準は、まさに、内閣官房情報セキュリティ政策会議の決定を各省庁に示したところ。各省庁自身、どうやって反映させていくか日々、一生懸命悩みながら取り組んでいるところです。よくない所については一つずつ直していかなければいけないでしょうし、見直しの機会をきちんと作って、次の改善につなげていく事が一番必要だ

と思います」(中田氏)と各省庁の取り組みについて報告された。

調達では外部委託の留意点も統一基準で明記

調達に絡んで民間への指導はどのように考えているかとの質問には、「当然、外部の委託先との関係について、どういう事に留意しなければいけないか統一基準の中に明記されている」こと、「政府間の合意基準は、あくまで最低限の基準です。基本重視事項については全て実施していただく。オプション条項については、それぞれの省庁の実状をみながら、きちんと各省庁の基準におとしていく作業を行う。その基準に基づいて委託先との関係について吟味が必要になると思う」(中田氏)と回答。

IPv6 導入に伴う必要な措置について

情報システムへの IPv6 導入に伴う脆弱性対策について、具体例をあげて説明いただきたいとの質問には、例えば、IPv6 over IPv4 トンネル方式の場合、攻撃の対象になるケースについて中田氏から説明があり、IPv6 の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずることが求められた。

職員のキャリアパスで情報セキュリティ担当者のノウハウを蓄積

人材育成については活発な意見交換が行われた。自治体職員の方からは、「情報セキ

ュリティ担当者が退職、人事異動した場合、その穴を埋める手だてがない状況です。他の自治体も同様の悩みを抱えていると思います」との実状が報告され、「人件費抑制のため職員定数削減を行っている自治体もある。情報システム要員の外部調達という話もありますが」との発言もあった。

中田氏からは、「成果を発揮していただくという時に、人事異動、退職となると育てた側もショックをうけるでしょう。そのような事にならない様に、それぞれの組織が人事政策にしっかり組み込んでいく必要があると考えます」と、情報セキュリティセンターの職員の交代についても同様のことが言えるとし、「人事異動で、いままで積み上げてきたことが引き継がれずに埋もれてしまう、そういう事はどの組織もあることです。そういう事が起きないように、常日頃から計画的に継続性という事を考えていかなければならない」と強調。



電子申請普及の阻害要因について総務省も検討

スマートチャットで、あるグループでは、韓国電子政府の取り組みや、国内でも岡山市

等でスタートした電子申請の取り組みについて意見交換がなされ、石川氏に対して全国に普及しないのは何故か、何がじゃまをしているのか、との率直な意見が出された。電子申請普及にむけては、行政の電子化に伴う法整備、セキュリティの仕組み作りが必要とし、総務省も阻害要因の検討を始めているとの報告があった。

現場では手順書を望む

オンラインポリシーはあるが手順やひな形が整備されていない点も指摘され、実際の現場ではどうすれば良いのか分からないといった現状や手順書が望まれているとの発言もあった。

## ディスカッション

人材不足と組織内の理解不足について

セミナー参加者の事前アンケートでは、「人材不足と組織内の理解不足」がネックになって情報セキュリティ対策がすすんでいないとの回答が多数寄せられた。

全体のディスカッションの冒頭は、中田氏とのスマートチャットでの議論を引き継ぐ形で、自治体職員の方から、セキュリティ担当者の異動の実態について報告があった。「セキュリティ担当のスキルを向上させていかなければいけないが、あるレベルまでいったところで穴があいてしまう。人材を外部に求めることもわかるが、内部でも深めていかなければいけない」との危機意識が強い。

自治体はセキュリティポリシーについて

意識が希薄ではないか、との問題提起には、民間企業からは以下のような様々な対応策が紹介された。

- ・ 誓約書の提出
- ・ 毎朝、PCの電源を入れて仕事をする前に、スクリーンセ이버でセキュリティ度のレベルチェックの質問に答えなければ、仕事ができない。
- ・ 懲戒規定（懲戒免職）一番効く。自治体のセキュリティレベルが上がらない理由はそこにあるのではないか。

民間企業でも情報セキュリティ人材の確保・育成では同様の問題を抱えているが、セキュリティポリシーを守るうえで、抑止効果を高めるために、上記のような様々な取り組みが行われている。誓約書は非常に抑止効果があり、1日1問のセキュリティ度チェックの質問も、社員の認識が変わったとの報告があった。



セキュリティオフィサーの役割はコーディネート

外資系企業のセキュリティオフィサーを経験された方のセキュリティのレベルを上

げるための取り組み、また、解決のアイデア、取り組み事例については、特に参加者の関心が集まった。

誓約書についても、「入社時に分厚い冊子になったセキュリティポリシーが渡され、読んで理解するために3日間の猶予期間が与えられ、誓約書の提出はその後である」ことや、「コーディネーションが一番必要である。内部のトレードオフ、説得をいろいろな場面でいながら、ユーザーがセキュリティポリシーを守れるような環境づくりに尽力した」といった、草の根で説得する活動を行っていたとの報告があった。

#### 日本では運用が課題

日本では、自動オートロックのマシンルーム、監査部門などのドアにもスリッパをはさんでおいて閉まらないようにしていたという80年代後半の実態や、現在でも運用ができていないと、日本のセキュリティオフィサーは可哀そうだ、との発言もあった。

#### 経営トップに情報セキュリティへの理解を

民間企業のケースとして、社長自らが最高情報セキュリティ責任者として全てを統括し、組織上、非常に情報セキュリティへの意識が高まったとの報告や、セキュリティの問題が発生すると、社長が現場にとんできて関係者を集めて緊急会議（別名、車座会議、膝詰め会議）を行う外資企業の事例も紹介された。この企業は、膝詰め談義をするというようにトップの意識も非常に高く、また、情報漏えい事故を未然に防ぐために500社ほどあったシステム開発の外部委託先を20

0社ほどに絞りこんだ。

#### 精神論は無理、適切なツール・ルールを取り入れる

セキュリティマネジメント関連のコンサルタントの方からは、米国の金融機関では、既に80年代から、アクセスコントローラ一つとってもディスクリーショナルな領域、マンドトリーな領域、そして、危険度の高いOSのユーティリティをセンシティブプログラムとしてリネーム、削除するといったルールが存在した。現在の日本ではそのレベルにも達していない組織が数多くあり、間違いを誘発するような要因が山のようにある環境にいるわけですから、精神論のみでやっても無理な面がある。適切なツールと適切なルールを取り入れていかなければいけない、との指摘もあった。

#### その他

その他、民間企業の情報システム部門の担当者からは、金融商品取引法、一般企業の財務情勢がかなり厳しくなってきたとの実態が報告され、情報セキュリティ対策のガイドライン等が出ているが、セキュリティの強度について具体的にどの程度まで対策が求められているか、官民を含めて実態をしりたくて参加したとのコメントや、省庁の情報セキュリティ監査のシュミレーション教材の開発を行っているソフトハウスの担当者は、自治体職員の情報セキュリティ教育にも、シチュエーションの中で自分が体験して判断を下していくタイプの教材を活用していったらどうかとの意見もあった。

## スマートチャット 回答

### 『わが国における情報セキュリティ政策の基本戦略』

統一基準について	政府機関統一基準。各府省庁で統一基準をモディファイしているの、実施レベルも満足している？	1
	政府機関統一基準（H18.6）	2
	各省庁の運用面 統一基準では見えていない。各省庁による。	3
	IT調達要求仕様に対する考え方が統一基準を満たすのか？その審査プロセスは？	4
	政府機関統一基準を適用する政府等が民間に要求すること。調達・予算から	5
	大学院のゼミで政府機関統一基準が使われていること	6
	文書管理規定の関係	7
情報漏洩	ファイル交換ソフト	8
	政府も会社も同じ悩み（自宅作業での情報漏洩）。	9
	ウィニーの一人歩き	10
	情報セキュリティ対策が情報漏えい対策（ファイル交換ソフト対策）に偏ってしまった。セキュリティ対策の重要性が広く意識されるようになったが・・・	11
	Windy：モラル。	12
組織体制	統一基準はシステム寄り。組織面は？ない。	13
	情報漏洩に対する懲戒規程はどうなっているか？	14
	NISC 8名（スタート時） 51名	15
	P D C Aサイクルがまわらない状態が多いことを改めて認識した。	16
改善案	自宅で私物PCでの仕事	17
	政府機関で私物パソコンの利用がまだ許されていること。	18
	セキュリティガバナンスはガイドラインでは実現出来ない。	19
	より、実用的なBCP&DRPの構築。企業、部門間の連携。	20
	セキュリティ対策のトランスファー方法は？人的な話が重要。	21
	NISCが評価した結果を公開する。順位が下がらないように努力。	22
	NISCは強制力がないと統一基準導入が足並みそろわないのでは？	23
	BCP計画は作られているのか？	24
	重要インフラの情報セキュリティ対策に関わる行動計画	25
	相変わらず、こうなればいいなあ（WishList）。政策と言うより自己満足。フィジビリティに欠けるのでは？	26
	ハードより人の教育が重要か。	27
	単年度毎にして、セキュリティジャパン施策が変更すると長期の戦略的対応は難しいのでは。	28
	情報セキュリティ技術を高度化しても、仕事のやり方に問題。	29
	重要インフラの対策について	30
	事故、災害時の重要インフラの情報共有を我々一般企業はどのように行い、得ていくようにしたら良いか。	31
	人材育成、流出の悩みはどこでも同じ	32
	人材育成 防衛省では？	33
	人的要素について	34
	I P V 6 対応。I P V 6 を使っていないのなら、使えない設定にすること。	35
	サイバー攻撃による脅威。非意識的要因による脅威。災害による脅威。	36
脅威（サイバー攻撃による脅威、非意識的要因による脅威、災害による脅威）	37	
国際的にみて誇れるようなことをなさっていると云えますか？	38	
評価モニタリング	評価の仕方 モニタリング	39
	セキュリティ対策評価をどのように実施していくか？	40
	実施のモニタリングとその評価は？	41
	評価。レベルの公表。人材の育成。	42
	N I S C のミッションが達成したとは、どういう現実ですか？何かメトリクスがあるのですか？	43
官民連携	官民連携。	44
	日本では民間主導のコンソーシアムが伸びないのはなぜ？	45
	新しい官民連携モデル	46
	企業への応用は実際には、どの位？	47
民間に対し、これはお勧め、とはどれですか？	48	
政府施策	H17.12.13 情報セキュリティ政策会議	49
	159 施策 P D C A	50
	政府のやっていること	51
	2006年 情報セキュリティ戦略元年	52
	新しい安全保障 スパイ対策、エシロン、日米貿易摩擦、NSA、犯罪レベルを越えたのか 具体的対策は？	53
	3カ年計画の中で2年目に入ったとのこと。我々も腰をすえて長い目で仕組み作りに取り組んでいこうと思いました。	54
	企業・個人についても各省庁の施策で逃げていないか？	55
その他	情報セキュリティにおける脅威。	56
	個別対策の限界	57
	インターネット経由でのサイバーテロは困難か。	58
	プロファイルを元にアプリが閲覧されている。	59
	機密性、安全性、可用性。	60
	ハッカーの脅威。	61
	具体的な問題点が見えなかった	62
	機能が網羅的で何が主眼なのかボケている。	63
	traffic lisht protocol	64

## スマートチャット 回答

### 『地方公共団体の情報セキュリティ』

改善点・疑問	公務員法との関係で懲戒規程とリンクしてないのでは？	1
	何故、日本では電子政府が調査段階なのか？	2
	住基情報は厳しくて、他の情報は甘いのは、懲戒規程との関係では、	3
	内部監査、人的要因が高い。代替案が必要。社員全員に浸透させる教育方法。インセンティブ、志を高く持つか？契約書。互いに監視。	4
	情報資産の調査～改訂がなされない。リスク分析～未着手。	5
	ミッションを達成したとは、どんな状態ですか。	6
	ポリシーはあるが手順書がない。	7
	現在の自治体の事務所等には、情報セキュリティに関するものがない。これではセキュリティは守れない。	8
	セキュリティ・アドバイザー派遣の要員は充分ですか？	9
	問題はわかっているが予算がない。	10
	公的個人認証は、税負担、国民の義務の見返りとして無料とすれば利用が広がる。	11
	ポータルサイトは民間でも見れるサイトかどうか？	12
	地方での業者のSMS、Pマークを取得しているところが少ない。	13
	BCP(事業継続対応)、証明書の電子交付。公的個人認証サービスの民間分野における利活用。金融分野へ。	14
	電子申請50%よりも、総務省では交付物のないもの対象に50%といっているが、住民の望む自動交付機など、住民生活に根ざしたものを目指すべきではないか。	15
	他の自治体との情報共有の場が少ない。	16
	電算処理の委託に関する検討(総務省)。罰則を設ける。委託先、評価。	17
	自治体の窓口では、セキュリティに甘い気がする。	18
	住基ネットのセルフチェック。	19
	格付け、HR機能、加句型。	20
	目的補助金の仕組み。	21
情報公開	情報管理セキュリティの格付け(企業体)。自治体は今のところ公表無し。公表していけば改善されレベルも上がるはず。	22
	達成を測定するメトリクスはどのようなものですか？	23
	CEPTOARの計画、目標がプレゼンでは理解できなかった。なぜ、自治体の情報対策を公表しないのか？	24
	事故後、どのような対策をとったかも事例で紹介。	25
	自治体間、第三者監査実施事例は？	26
	漏れた住基情報はどうしたのか。	27
CEPTOAR	CEPTOAR。住基法の見直し。情報の見直し。	28
	IDSによる庁内～インターネット監視	29
	センターの活動(存在)を知らなかったが興味深い。	30
	結局のところ自治体CEPTOARを目指しているのが分からなかった。LASDECの問題ではなく、自治体の本質的なHRMの問題かな。	31
	情報セキュリティ遠隔診断をやっていること、2割がOK。	32
	ISAC、CEPTOAR。	33
	IDSによる庁内インターネットの監視。	34
	IDS、80団体、公的個人認証サービス、Sec診断700団体 2割OK。リスク分析、BCP策定。証明書の交付。	35
	いわき市のセキュリティレポート。IDSを設置。監視していること。	36
学校	学校が一番遅れていること	37
	7/4官庁速報。学校現場。	38
	学校現場においては、IT自体の取り組みが遅れている。	39
	教育委員会からe-Learningの申込があること。学校が危ない。	40
感想	Winny。	41
	南郷市の電子申請事例	42
	啓蒙活動。	43
	実状と課題の多さは、一般企業と変わらない、もしくは、厳しい状況と感じました。	44
	カードによる自動交付は便利だが心配でもある。	45
	過剰反応(個人情報保護法)	46
	岡山市・・・証明書印刷。	47
	セキュリティ監査。PDCA。	48
	地方自治情報センター殿の様々な取り組みについて聞く事ができ、自治体団体の課題を改めて認識した。	49
	国の施策よりも具体的でわかりやすかった。	50

## スマートチャット 回答 『フリーディスカッション』

感想	様々なお立場の意見やお話が聞けて楽しめました。	1
	規則と利便性の排反性。	2
	I Tのイメージが困難なものについて、マネジメントが難しい。	3
個別技術	透かしを通用された文書をスキャンして、さらに透かした場合でも、漏洩日時や漏洩者を特定できるのですか？	4
	アドビ8より前では開かない(アクロバットも同じ)。	5
	旧バージョンのA Rでは開かない(対応できない)	6
セキュリティポリシー遵守	セキュリティポリシーを守る事の困難さ。	7
	柴崎氏の処ではログイン時にセキュリティの問題を出して、回答しないとログイン出来ないという話があった。	8
	組織連携。	9
	セキュリティオフィサー	10
	情報セキュリティは草の根活動が重要。	11
	P C立ち上げ時に質問が出る。	12
	F R B	13
	P Cの立ち上げ時に1日1問の質問をしている。これは面白い。	14

## 参加者分析

---

下記は事前アンケートの集計結果です。

### 1. 情報セキュリティ対策へのかかわりについて(該当しないものを削除)

組織における責任者・担当者(経営者・統括責任者含む)	27%
関連部署	20%
プロフェッショナル	6%
個人・ユーザー	47%

### 2. 情報セキュリティ体制について(該当しないものを削除)

専任体制	33%
兼任者( )名	33%
外部の委託	6%
特になし・個人	28%

3. 情報セキュリティ体制を構築するにあたって問題となっていることがあればご記入下さい。

- ・人材不足と上層部の認識不足
- ・リスクアセスメントの改善
- ・情報セキュリティの必要であるという総論は理解するが、具体的に展開するためには、時間を取られる、金がかかるという面で積極的な参画を得られないことが多い
- ・可用性と機密性のせめぎあい
- ・各種セキュリティ対策に費用がかかりすぎる。

4. 現状、情報セキュリティ対策で抱えている課題があればご記入下さい。

- ・セキュリティへの危機感(対策の必要性)を組織全体で共有するにはどうしたらよいか?(セキュリティ対策への予算を優先してもらうためにはどうしたら良いか?)
- ・予算・時間がない
- ・個人PCでのファイル共有ソフトの禁止をどこまで強制できるか
- ・各種対策に費用がかかりすぎる。

#### 4.1 運用面の課題について

- ・管理する対象（社内PC，持ち出し用PC，ファイルサーバ、外部メモリ、など）が多く存在し、セキュリティ管理コストがかかる（自治体等の場合は、外部接続PCと業務PCを分けていたり、複数職員で共用している場合があり、さらに管理が大変なのでは！？）
- ・セキュリティ監査を実施したいが、上記理由から手が付けられない状況にある。
- ・エビデンスの取得（有効性測定指標）
- ・中小企業のビジネスに適した情報セキュリティマネジメントシステムのデザイン

#### 4.2 マネジメント面の課題について

- ・セキュリティ教育の徹底（未教育者のフォロー）
- ・セキュリティ関連予算と投資対効果

#### 4.3 技術的な課題について

- ・アクセスログの取得方法
- ・メールのアーカイブ
- ・グループウェア（サイボアズ）の脆弱性
- ・Web2.0系サービス利用と情報セキュリティ対策のさじ加減

#### 4.4 ユーザーとしての課題・問題

- ・セキュリティパッチなど個人対応になっているので不安を感じる
- ・個人情報保護法との整合性
- ・テレワーキングの実施に際しての情報セキュリティマネジメント
- ・セキュリティ対策が現実的に業務上不可能なことが多すぎる
- ・機密情報と個人情報の取り扱いの関係について明確でなく、現場での混乱がみられる。

#### 5 . セキュリティポリシーはどの程度、遵守されていますか

- ・当社では誓約書に全社員がサインしている。
- ・職員のほとんどが認識していると思われる。
- ・サーバーでのセキュリティポリシーの管理を実施
- ・ポリシーレベルにとどまる
- ・ISMSの実施計画規程の通り

#### 6 . その他、家庭、職場での情報セキュリティ対策で困っていることがあればご記入下さい。

- ・大手ベンダーのセキュリティが厳しくなっており、ベンダー先にいる社員への情報伝達手段が制限されている（会社ノートPCの貸与、data card の貸与、携帯電話の貸与で対応）。
- ・電子申請の利用と生活の質の向上、そして行政書士として電子代理申請について興味が有り参加希望いたしました。よろしくお願いたします。

記入回答（一部抜粋）

ユーザーとして

1. 電子政府・電子自治体の情報セキュリティについて

経験（利用して感じたメリット）

- ・使用を始めるまでの手続きや手間、時間がかかる。
- ・e-tax等は、一度使い始めてみると、それなりに便利。

問題（利用して感じた問題点、それ以前のあり方に関する問題）

- ・使用を始めるまでの手続きや手間、時間がかかる。
- ・情報漏洩事故が続くと問題がある。
- ・省庁間の基準の不統一。

期待・提案（ユーザーとしての要望・期待、提案）

- ・自治体ごとの水準比較をすべきでは？

2. 民間のオンラインサービスの情報セキュリティについて

経験（利用して感じたメリット）

- ・納税の時、手書きの書類が減り、便利だと感じました。
- ・各種ASPサービスがあるが、一体どこが監査しているのか？
- ・サービスのレベルのバラツキ。
- ・インターネットバンキング等は、ワンタイムパスワードに移行して、セキュリティは高くなっているが、使いにくくなっている。

問題（利用して感じた問題点、それ以前のあり方に関する問題）

- ・PCを使い慣れていない人には未だ敷居が高いと感じました。
- ・セキュリティの強度が疑問。
- ・銀行カード、4桁の暗証番号が十分なのかどうか。

期待・提案（ユーザーとしての要望・期待、提案）

- ・ウィザード形式をさらに便利にしながら用語を調べやすくするなど。

3. 政府・自治体・NPOの政策形成や政府・自治体・NPOが運営するイベントについて

パブリックコメント、タウンミーティング、自治体SNS、政策提言等

経験（参加して感じたこと、メリット）

問題（参加しないのは何故か、参加して感じた問題点、それ以前のあり方に関する問題）

- ・時間がない。

期待・提案（ユーザーとしての要望・期待、提案）・反省

プロフェッショナルとして（専門家としての立場からご意見ください）

1. 電子政府・電子自治体の情報セキュリティについて

経験（セキュリティ対策に関わって感じたこと）

- ・調達側のノウハウに疑問。
- ・情報セキュリティ監査が品質監査部門の中にあり、監査手法の違いが問題となっている。
- ・自治体の予備監査に参加して、民間に比べて大変遅れている。
- ・自分達の都合のよい事しかしない。

問題（実行されないのは何故か、セキュリティ対策に関わって感じた問題点、それ以前のあり方に関する問題。）

- ・体制の不備。
- ・情報漏洩事故が続くと問題である。
- ・予算が単年度のため、セキュリティ教育用教材が更新できない（ISMS2.0 ISO/JIS など）、事故が起きないと予算がつかない。
- ・人の問題（セキュリティ意識が低い）。
- ・財政当局はその必要性、緊急性を強く感じない。

期待・提案（専門家としてのアドバイス・要望・期待）・反省点

- ・情報セキュリティに関する IT アーキテクトの部分は、非常に専門性を要求されるため、何らかの組織が全体を する必要がある。
- ・セキュリティコンサルタントを雇う予算をとるべし。
- ・政府は、NISC を先鋭として実施されるのかもしれませんが、地方自治体はそのような（早い）ペースでは実施できません！

2. 民間のオンラインサービスの情報セキュリティについて

経験（セキュリティ対策に関わって感じたこと）

- ・SPAM の混在など、まことしやかあ n 噂が出回っている。
- ・利便性の向上がなおざり。
- ・一般的なセキュリティ対策（ポリシー、認証と承認権限の設定・・・）24H365 日のシステム企画、設計、実装。

問題（実行されないのは何故か、セキュリティ対策に関わって感じた問題点、それ以前のあり方に関する問題。）

- ・サーバを立ち上げ、サービスを提供する場合、責任が明確ではない。
- ・知識不足な面も多いのでは？
- ・一般的なレベルでは、実施されている。

期待・提案（要望・期待、提案）

- ・何らかの規制が必要。

3. 政府・自治体・NPO の政策形成や政府・自治体・NPO が運営するイベントについて

パブリックコメント、タウンミーティング、自治体 SNS、政策提言等

経験（参加して感じたこと、メリット）

- ・パブリックコメントを総務省、経済産業省に対してしているが、結果公表が遅い、又は、されない。

問題（参加しないのは何故か、参加して感じた問題点、それ以前のあり方に関する問題）

- ・パブコメに対する検討が経過でなく、結果のみが発表。誤解されたことが修正不可。
- ・パブコメをしても反映されない（自分達もさほど聴く訳でもありませんが）。

期待・提案（専門家としての要望・期待、提案）・反省

- ・双方向性を確保したパブコメを試行する。