SAAJ 日本システム監査人協会報

＜特集：50号と2000年問題＞

コンピュータ2000年危機を乗り越えよう！

会長　橘和　尚道

「会員の所属・関係する企業や団体からは、西暦2000年問題のトラブルを、絶対に起こさないという覚悟で、この問題に対処して頂きたい。」
（通商産業省・情報処理振興課長　原山 保人 氏より）

折しも2000年問題に関する政府の「行動計画」を正式に決定し、実施に移すという高度情報通信社会推進本部（本部長 小渕首相）が開催される日の前夜、９月10日午後７時のことです。

毎月行われている当協会の定例理事会（第２木曜）に、翌日の準備でお忙しいところを同課安全指導係長の 澤野 弘氏とともに出席された原山課長のこのお言葉に、一同その責任の重大さに身が引き締まる思いでいっぱいでしたが、同時にご期待に沿うべく努力する旨お答えした次第でした。

会員の皆様には、システム監査人や情報システム部門の方々以外の他の部門にご勤務で直接この問題に無関係の方もおられるかと存じますが、それでもなんらかの形で社内で声を挙げて頂き、少なくとも「当社発のトラブル」は絶対に起こさないという努力を是非ともお願い申し上げます。

協会としても、この問題について、システム監査の視点から別掲のように積極的に取り組み中ですので、会員の皆様からのご意見、ご提言をお待ちしております。

会報第50号の発行を記念して ―当面の協会活動の現況と課題

No. 461　橘和　尚道

１．はじめに

No.1.FEB.1988と右肩に記した会報の創刊号が手元にある。1987.12.12に開催された設立総会の模様、そして設立時の苦労と発展への希望に燃えた初代川野会長の挨拶、活動方針、そして初年度合格者を中心とした120名の会員名簿が輝いている。８頁と薄いが中身も濃く、行間に滲み出るものがある。

その後の会報の充実には目ざましいものがあるのは、ご存じのとおりで、いよいよ本会報が50号である。協会と会員間のコミュニケーションの柱として、ますます付加価値の高い紙面となっており、ご同慶の至りである。この場をお借りして会報担当理事各位と投稿者の方々に深く感謝を申し上げたい。

ここで当面の協会の大きなプロジェクトについて、その現況と課題について報告する。

２．コンピュータ2000年問題

この2000年問題（以下Ｙ２Ｋと略称）は、もともと８月の下旬に情報処理振興課の原山課長からＹ２Ｋについてシステム監査人の立場からの意見を求められて発足したプロジェクトチームの迅速な活動（荒川レポートの提出）が先ず最初にある。

９月上旬には原山課長出席の「通産新報」の座談会に協会代表として、荒川副会長の参加、そして、本会報の冒頭にあるように理事会での要請に接したわけである。

この時のお話の要点は、三つある。一つは情報化人材対策に関連して、企業の情報化リーダー・CIOとシステム監査人の関係を考えよ。二つはＹ２Ｋについての冒頭の要請、三つは自社・関連企業に対するＹ２Ｋの適切な手段。特に中小企業対策の提言である。

その後、数度のＹ２Ｋプロジェクトチームの論議をまとめた三谷理事の原案をチェックし９月30日に「経営者の皆様へ　西暦2000年問題をご存じですか」(協会ホームページ参照)のリーフレットを提出し、２箇所の修正で通商産業省と当協会の連名としていただいた。しかも翌日の情報処理月間の開始式行事に早速ご利用いただけたのである。

現在、チームの作業は第二段階に入り続行中で、更に各企業で実際に使用できるチェックリスト、ワークシートや危機管理計画などの検討・作成を行っていて今月中に完了予定である。

次の第三段階は、会員の方々と共にＹ２Ｋのシステム監査を実践することである。

３．「情報システム実践マニュアル」の出版

新システム監査基準研究プロジェクトとして「新システム監査基準・実務手順書」(97.2)が10周年事業の成果となった。さらにその改訂版の「同・実務手順書98」(98.4)もFD手順書として無料配付されている。

今般、それを土台にした「情報システム実践マニュアル」が、別掲のように出版されることになり、97・98のプロジェクトリーダー小野・松枝理事を中心に多数のメンバーの方々の２年半にわたる労苦が結実した。

これには、通産省の澤野係長の序文もいただいており、それこそこのマニュアルを活用したシステム監査の実践が、我々にとって今後の重要な課題となっている。

４．地方自治体のシステム監査シンポジウム

昨年来地方自治体のシステム監査等実施状況を法人部会(一村・小野理事)でアンケート調査を行い、その結果は前号の会報(No.49)で報告した。これをうけて「地方自治体の情報システムの課題とシステム監査」をテーマとして、シンポジウムを行うこととし、別掲のように、11月18日午後の実施が決定した。

講師やパネリストにはこの問題で最高の方々に参画いただけることになったので、会員の皆様も是非パネル討議に参加していただきたい。

５．組織対策について

Last but not Least! 最後に最大の課題であるが、以上の諸活動とは無縁ではない。この問題は、かねてより組織委員会(荒川委員長)の論議が続いているが、Ｙ２Ｋプロジェクトで一時中断の形となっている。その論議を一部先取りし、私見を交えて以下述べさせていただく。

(1)会員の拡大策

システム監査技術者試験の合格者3,772名のうち600余名の個人会員である。合格者の住所が不明のため、入会の案内が出来ない。しかしいずれ、当協会の活動を知り、存在を知って加入を希望される人が増えることを信じて頑張っているのが現状である。しかしそれでは会員の拡大は不可能である。

〔試験制度〕平成６年度の合格者から激減し始め昨年度の合格者は146名である。平成５年度まで毎年6000人前後の受験者がいたが、今や2000人に減っているのである。合格者の一割にアプローチ出来ても、15名の規模である。先ず受験者の増加を図らねばならない。

平成５年の産構審の最終報告で情報化人材の類型を11に細分化され、それに基づいたカリキュラムによって、技術者試験も多様化していった。受験者が激減したのはこの時期からである。

その際の情報化人材の類型では、それまで「特種」の上で情報処理技術者の最高位に位置づけられていたシステム監査技術者が、新しいシステムアナリストの次であるような類型での位置づけになったからでもある。

理事会で、原山課長が言われたCIOとシステム監査人の関係とは、この点にあるのではないかと思慮されるのである。つまり、情報システムについてCIOにものが言えるという関係である。この点、情報システムの有効性の監査が大きく注目されるところである。

情報化人材の類型で考えると、システム監査人はシステムアナリテトの上に位置するか、別枠の位置づけとするかの検討が必要となる。

試験制度に関連して、当協会が主催する受験対策講座の設置も、会員拡大策の一環として考えることが組織委員会で議論されている。

〔台帳登録企業〕平成10年度登録企業59社中10社が法人会員である。法人部会では近日中に、当協会の活動状況と加入案内を送り、システム監査の普及・啓蒙活動に参加を呼びかける。

(2)システム監査能力の維持・向上

会員のシステム監査能力の維持・向上に効果を挙げているものに、月例研究会(勝田理事)と監査事例研究会(鈴木理事)がある。この他にもセキュリティ(金子理事)、技法(木村理事)、PC通信(蓮見理事)の研究会・部会があるが、ここでは上の二つに絞る。

〔月例研究会〕これは会員だけでなく、今後試

験合格者のフォローアップにすぐ活用できる内容と自負している。もしこの制度化が必要であれば、そのためのカリキュラムの作成も今後検討できる。現在はビデオ化され、地方支部にも配付、貸出制度も出来ている。

〔監査事例研究会〕 これも会員の監査技能向上のため、実費でシステム監査を受託し、実際に体験できる研究会である。また今年で3回目になるが、監査未経験の会員のために、監査実践体験セミナーも実施している。このセミナーについては、合格者のフォローアップにも効果的と考えられる。

6．おわりに

紙数の関係で言葉足らずの報告となったし、各支部の活動状況を省略せざるをえなかった。以上の諸点について、会員の皆様のご意見を是非いただきたい。(担当の理事各位宛でも可)

「ある私企業の2000年問題」対応状況について

No. 679　吉田　裕孝

当社は Global に Business を展開していることもあり、昨年から本年にかけて、欧米の取引先や外国系金融機関から当社の「2000年問題」の対策状況について頻繁に照会が来るようになった。一方 IR の観点から、Annual Report に対策状況及び対策費用の記述が必要になってきている。

当社では、「2000年問題」の範囲とリスクを以下のように定義している。

(1) 社内基幹コンピュータシステムの対応
(2) 商品部門、海外現地法人、関係会社の各個別コンピュータシステムの対応
(3) 取扱製品に関わる2000年問題の影響
(4) 取引先システムと製品の2000年問題の対応
(5) コンピュータを利用した施設インフラ関連の対応

上記定義の内、本報告では、(1)及び(2)を「狭義の2000年問題」として、主として社内情報システム部門からみた2000年問題の対応策やその課題について以下簡潔に報告したい。

当社の情報システムの現状

当社の基幹情報システムは、1994年から1996年にかけて、従来の大型汎用機ベースの集中処理による基幹システム(COBOLベース約3000万steps)から、オープンなクライアント・サーバ型の分散処理システムに切換えをおこなった。その結果殆どの業務システムについて、年号を4桁の数字で対応することについては、対策が完了している。

一方当社システム環境独自の対策が必要な課題としては、以下の事項があげられる。

(1) オープンなシステム環境となっているため、代表的なハードベンダーのパソコン、UNIX機を使用しており、その種類が多い。
(2) 基本ソフトについても、OS、DBMS、言語、各種utilityソフト等使用している。ソフトの種類が多様。
(3) 取引先の数が多く、多様な形態のEDIを運用している。

オープンシステム環境下での留意事項

(1) 使用している各ハード及びソフトについてベンダーへの対応の要否の確認

米国系ベンダーの提供基本ソフトについては、「2000年問題対応する基本ソフトのversion」と「対応しない基本ソフトのversion」が明確になっている。当社では、94−96年当時の最新version基本ソフトを導入設置しているにもかかわらず当該基本ソフトが2000年問題に対応しないとのベンダーからの回答により、version upを強要されるケースが散見されている。日本的感覚とすれば理不尽と思えるが、現状ではお金と時間をかけてversion upを実施せざるをえない。

(2) 組み合わせたハード／ソフト環境での実際のテストの実施

オープン環境下のシステムでは、複数のベンダーのハード及びソフトを使用していることが一般的になっている。この為、「2000年問題」をクリアーしているか否かの最終確認は、自社内に本番環境に準じたテスト環境を構築し、実際に稼働テストを実施することが必要で、それ以外方策がない。

EDIを実施している場合の留意事項

(1) EDI実施企業と伝送フォーマットの変更有無確認

相手先企業とフォーマット変更について事前確認が必要。私が知る範囲では、2000年問題を契機にから伝送フォーマットを変更するケースは、皆無に近い。

(2) 模擬テストの実施

理想を言えば相手先企業との連動テストが実施できればよいのであるが、現実的には相手先企業を巻き込んだテストの実施は無理がある。従い当社では、自社内にテスト環境を作成し、相手先企業に送信するデータが正しくセットされているか否かを検証している。

以上多少でも参考になると思われる事項を記述したが、会社経営者に「2000年問題」を社内の重要経営課題として認識させ、会社が持っている、人、物、金の経営資源を適切に配分し、必要な対策を地道に実施していくことが肝要であろう。

「2000年問題をコンサルタントの立場から考える」

No.6008 梅津 尚夫

1. 経営者の認識を高めることがコンサルタントの役割である。

2000年問題は技術の問題ではなく、経営の問題である。技術的には解決策も明確であり容易であるが、その量が膨大であるため費用と時間がかかり、そして、結果として発生する事態は経営の根幹に関わることになるからである。

しかし、このような認識がまだ経営者において、特に中小企業経営者において不足している傾向が顕著である。私は中小企業事業団の情報化推進アドバイザとして全国を回って啓蒙普及を行っているが、経営者の反応はいまだに次のようなものである。

「うちは関係ない」「うまく行けば、問題は回避できるだろう」「コンピュータの問題は社内の専門家に任せているから大丈夫」「いざとなれば誰かが助けてくれるだろう」「コピュータメーカーに駆け込めば、何とかしてくれるだろう」このように無理解、楽観論がはびこっている。なぜ、経営者は重要性を認めないのか。一つの原因は説明する側の問題がある。

まず、現実にどんな事態が起きるのかについ

訃 報

10月14日夜、当協会監事をお願いしていました藤森健次様が59歳の若さで他界されました。
協会として生前の会へのご貢献を感謝するとともに、慎んでご冥福をお祈りいたします。

「藤森健次監事を偲んで」

No. 008 鈴木 信夫

祭壇の写真の服装がくつろいだ感じのもので、それと斎場全体の沈んだ雰囲気との落差が突然の出来事の痛みを刻み込むかのようでした。ご本人、家族はもちろん、会社関係やわれわれを含む、すべての者の無念さが残ります。

藤森さんは事例研立ち上げの中心でした。初めに、事例研の構想を聞いた時には正直いってやれるかどうか心配でした(当時、私は事務局長でした)。

分科会のみんなの熱意はいいとして、最初の難問が監査対象企業の選定です。監査チームの方は模擬でも、対象は実際に稼働しているシステムというのがポイントです。監査に理解があり、先方にかかるいろいろ負荷を承諾してくれる所となります。この時、藤森さんが事もなげに「うちの会社でやりましょう」といわれました。当時は専門商社の情報システム部長でした。大変なことでも気負わず淡々といわれるのが藤森さんの持ち味でした。

まず、業界の状況のレクチュアから始めてもらいました。銀行勤務の会員は「これだけでも勉強になりました」といっていたくらいです。監査の現場では、やはり担当者レベルで抵抗もあったようですが、「何かあったら私にいってください。すべて出させますから」という対応でした。

この模擬監査で、事例研のメンバーは活動存続の確信を得ました。われわれもいけると思いました。今、事例研の活動は、その後の関係者のご努力もあり、本協会の最大の柱です。

藤森さんには、どうも業務がお忙しそうで協会としては理事にとはお願いできず、監事として指導いただきましたが、今回の訃報は何とも辛く、残念です。お別れに際し、多くの感謝を申し上げ、ご冥福をお祈りいたします。

ての情報を得ていない。説明を聞いても「データ入力の拒否、データ年限の判定ミス」などではピンとこない。ここは、自社の業務に即して実例を持って説明をする必要がある。

いわく「すべての注文がストップしてしまいますよ」「倉庫業務がストップしてしまい、出荷ができません」「あるはずの在庫が消えてしまい、せっかくの受注が品切れになります」「入金したはずが、残高不足で手形が不渡りになります」などなど、相手の業種に合わせた実際に発生する可能性ある問題を挙げて説明することが必要である。

これは、社内の専門家に任せられない。多額の予算を組まなければならないが、プラスの成果が期待できない提案では、予算取りもできない。下手をすれば「なぜ今まで放っておいたのか」と責任をとらされる。ここに外部から問題の重要性を認識させる必要がある。これがコンサルタントの役割である。

2. 危機管理体制を作る

コンサルタントの役割は、認識を持ってもらうだけではない。その先を考える必要がある。それは、経営組織の改善に取り組むことである。

2000年問題の修正をしたから大丈夫ということはない。どんなプログラム修正をしても必ず見落としはある。必ず、問題は発生するものと覚悟しなければならない。むしろ問題が発生したときにどう対応するか、危機管理体制を作る必要がある。

つまり、発生する可能性のある問題を列挙し、その対策を一つ一つ決めていく。対策の内容は、どんなクレームが来たら、誰がどのように対応するか、5W1Hを決めることである。応急対策だけでなく恒久対策も盛り込まれなければならない。このことは、その企業の組織体制を作ることであり、管理制度を明確にすることに他ならない。

いわば、災い転じて福となすという精神で、社内の体制固めに利用することが大切である。これこそまさにコンサルタントの役割である。このような行動リストを含めた計画が緊急時対応計画コンテンジェンシープランである。

システム監査講演会報告

主　催：EDPユーザー団体連合会
日　時：平成10年10月7日
場　所：東京有楽町よみうりホール

No.526　富山　伸夫

はじめに

EDPユーザー団体連合会主催のシステム監査講演会が、情報化月間恒例行事として行われ、よみうりホールに約600人が出席しました。正面垂れ幕に後援団体として日本システム監査人協会とセキュリティマネジメント学会の名が出ており、配布資料の中には、通産省と当協会連名の2000年問題文書があり、通産原山課長の言及もあって、協会のプレゼンスを特に感じさせられました。

1．通産省情報処理振興課 原山課長の挨拶

景気対策及び情報化対策の現状から、今後の情報化施策としてインフラ整備と人材育成をあげ、人材の中心として企業のCIOと彼らを補佐するシステム監査人の重要性を強調された。2000年問題について、国レベル特に中小企業において対策が進んでいない(状況が全く見えない)ことが緊急・重大な問題であると強調された。

政府のアクションプランや実施計画を策定公表するに当たって、システム監査人協会の助けを受けたことについて謝辞を述べられた。また、システム監査人がいる企業では、2000年問題で事故障害を起こさないことがシステム監査人の役割であることも述べていた。

2．講演内容

(1)サイバーテロリズムを許すな
ーその動向と対策ー
講演者：福井工業大学　細貝康夫氏

サイバーテロリズムとは、ネットワークを通じて政府や産業に対して行われる敵対的な行動であり、大規模で組織的な不正アクセスを試みることである。「グローバルな情報戦争」ともいわれ、これの動向と対策、法整備の動向等が述べられ、我が国でも避けてとおれない問題となってきている。

(2)D社におけるシステム監査導入・実施事例
講演者：日本ユニシス(株)
小野修一氏(当協会理事)

ある情報処理サービス会社が、講演者の指導のもとに、システム監査を導入した経緯と実施経過について、事例紹介がなされた。内部監査人主導で進めるシステム監査が、外部の監査人が入ることによってスムーズな監査体制を立ち上げることができた。

(3)ソフトウエア違法コピーと法的リスク管理
講演者：社団法人日本パーソナルコンピュータソフトウエア協会　西郷純夫氏

ソフトウエア違法コピーの問題が取り上げられて以来このことの認知度は上がっているが、実態として違法コピーはなくならない。これらの実態及び法的背景について説明された。違法コピーは放置すると法的リスクの問題となり、そのための管理の一貫として、ユーザー教育と監査がある。

ソフトウエア著作権保護に係わる団体としてJPSA((社)日本パーソナルコンピュータソフトウエア協会)、ACCS((社)コンピュータソフトウエア著作権協会)、SPA(ソフトウエアパブリッシャーズアソシエーション)、BSA(ビジネスソフトウエアアライアンス)等があり、なかでもACCSやSPAは先鋭的な活動をしており、法的処置まで及ぶ場合がある。

(4) 日本航空におけるシステム監査事例
講演者：JALインフォテック(株)
松原栄一氏

日本航空において、会計監査の一貫として、1983年から毎年計画的にシステム監査が行われた事例の紹介がなされた。

第59回研究会報告

開　催：平成10年７月10日
場　所：労働スクエア東京
テーマ：帳簿書類の電子データ等による保存
講　師：監査法人トーマツパートナー・
公認会計士　和貝亨介氏

No.750　畠中　道雄

１．電子帳簿保存法制定の背景

1.1 帳簿書類の電子データによる保存検討の背景

昭和40年代のコンピュータ導入以来、熱心な担当官はいたものの、また、利用者側から電子化できないかという要求はあったものの、一部、マイクロフィルムで認められただけであった。ペーパーレスの動きもあったが、法の枠内でペーパーレスを考えるにとどまった。おおもとになったのは1.1.1の規制緩和。

1.1.1 規制緩和推進：平成７年３月閣議決定、トリガーとして一番大きい。

1.1.2 企業取引の情報化：テクノロジーの発達

1.1.3 コスト削減、省資源：紙のコストを何億円もセーブできる。

1.1.4　諸省庁の対応：閣議決定に基づき各省庁が対応した。

1.2 国税庁の基本スタンスー国税庁の法制化のポリシーー

重要な部分は３つ

1.2.1 真実性の確保(経済取引のオリジナルな情報が偽造・変造ができないこと、消滅しないこと)
- 訂正・加除の履歴の確保
- 帳簿間記録の相互追跡の確保
- 処理過程の文書保存

1.2.2 可視性の確保(必要な情報が速やかに出力できること)
- 即時見読可能性の確保
- 検索可能性の確保

1.2.3 証拠能力・証明力(十分な証拠力が認められること)

1.3 帳簿書類の保存等の在り方に関する研究会

1.3.1 性格：国税審議官の私的研究会

1.3.2 検討期間：平成８年７月～平成９年３月

1.3.3 構成員：学界、経済団体、実務家、法務局、工業技術院(JIS)、国税OB

1.3.4 検討内容

1.3.4.1 実務界の現状
- 企業動向：ペーパーレス化が進んだ業界
- パッケージソフト
- 公認会計士協会：監査証跡の確保、納税者の負担の軽減、裁量の余地がない(調査官と揉めることがない)、などの意見・要望
- 税理士会

1.3.4.2 各省庁の現状
- 法務省：商法では商業帳簿が書面によらなければならないという規程はない、すなわち媒体は問わない。従って、商法ではOK、残るは国税だけ。
- 通産省、厚生省、労働省、警察庁、大蔵省(証券取引法)

1.3.4.3 海外の動向
- アメリカ、イギリス、ドイツ、各国とも認めている。イギリス・ドイツは対象者を問わないが、アメリカの場合は１千万

ドル以上の場合、強制的に電子データでの保存を義務づけている。

2．電子帳簿保存法

2.1 関連法規

・電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律
(平成10年３月31日)
・電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則
(平成10年３月31日)大蔵省令
・電子帳簿保存法取扱通達
(平成10年５月28日)法律、規則の解釈について
・その他
電子帳簿保存法関係申請書等の様式の制定について
撮影型マイクロフイルムについても制度改定
地方税についても同様の改定が３月末で行われている。

2.2 施行

平成10年７月１日
経過措置の最初
・12月決算法人は、平成11年１月１日開始事業年度から備え付け保存する場合、申請期限は平成10年７月31日(５か月前)
・３月決算法人は、平成11年４月１日開始事業年度から備え付け保存する場合、申請期限は平成11年11月２日(５か月前)
本則の最初
・10月決算法人は、平成11年11月１日開始事業年度から備え付け保存する場合、申請期限は平成11年８月２日(３か月前)

3．電子データ等による保存等

3.1 対象帳簿書類

以下の帳簿書類の全部または一部(これまで紙で出力していたものと変わらない。)
・仕訳帳、総勘定元帳
・補助簿：現金出納帳、売上帳、仕入帳、売掛金元帳、買掛金元帳、など
・決算書類：Ｂ／Ｓ、Ｐ／Ｌ、など
・証票書類：請求書控え、領収書控え、など

紙で受け取った領収書、請求書は電子データとしては認めない。当初から紙で受け取った書類は紙で保存しなければならない。これらの内容を電子データとしてやり取りしていれば認められる。紙になっていなければ印紙税は取られない。

国税関係の帳簿が出力できれば、常駐ファイルであれ、中間ファイルであれ、構わない。コピーしたものでもよく、原本性は問わない、媒体も問わない。

3.2 電子帳簿書類の要件

3.2.1 機能要件：システム変更により維持困難になった場合は、一定の届け出によりいつでも紙に切り替えられる。７年間保存しなければならないため、その間、システム変更が考えられる。

3.2.1.1 自己(保存義務者)が作成(通達４－10)

保存義務者が主体となって、その責任において開発したプログラムであること。システム開発業者に委託して開発したものも含まれる。

3.2.1.2 最初の記録段階から一貫して電子計算機を使用して作成：入力から最後までコンピュータを使う。

3.2.1.3 訂正削除の履歴確保(通達４－５～７)

方法としては
①反対仕訳を発生させる＝訂正前と訂正後を残す＝新たな取引として発生させるシステム。
②直接訂正＝履歴を残す＝何らかの訂正・削除の記録が自動的に残る。入力から１週間以内なら訂正・削除を認める(履歴を残さなくてよい)特例がある。但し、１週間過ぎたら認めない。

3.2.1.4 追加入力の履歴確保(通達４－８)

入力時に、個々のデータに入力日がシステムで自動的に付加されるとか、伝票番号としてシステムで自動的に一連番号が付番され、それらを訂正または削除できないようなシステムであること。

3.2.1.5 帳簿間の関連性の確保(通達４－９)

監査証跡が保証されないケース
①検索キーの不備：転記元・転記先の番号がないと、どういう経路で書き込まれたかがわからない。
②レコードの集約：明細データとの関係がないと、どのデータを集約して得られたデータがわからない。

従って、２つのファイル間で同一の取引にかかわるデータであることを明確にするための一連番号等の情報、どのデータを集計したかを明確にする情報を確保する。

＊3.2.1.3～3.2.1.5が真実性確保にかかわる。

3.2.1.6 検索機能の確保

・条件検索

①主要記録項目(一連番号、取引年月日、勘定科目(貸方・借方)、相手勘定科目(貸方・借方)、取引金額、その他(固定資産の資産名、人事の社員名など))による検索ができる。
②日付または金額による範囲指定ができる。
③主要記録項目のいずれか2つ以上のキーによる組み合わせ検索ができる。

3.2.1.7 画面および書面出力
3.2.1.8 出力の整然性、明瞭性、迅速性
＊3.2.1.6～3.2.1.8が可視性にかかわる。
＊機能要件として1～8すべて満足していること。

3.2.2 ドキュメント要件(通達4－10～11)
3.2.2.1 システム概要ドキュメント
システム全体構成および各システム間のデータの流れなど、国税関係帳簿書類の作成にかかわる処理過程を総括的に記載したドキュメント。
・システム基本設計書
・システム概要書
・フロー図

3.2.2.2 システム開発ドキュメント
システム開発に際して作成した、システムおよびプログラムごとの目的および処理内容などを記載したドキュメント。
・システム仕様書
・システム設計書
・ファイル定義書
・プログラム仕様書
・運用マニュアル

3.2.2.3 システム操作説明書
入出力要領などの具体的な操作方法を記載したドキュメント。
・操作マニュアル
・運用マニュアル

3.2.2.4 保存等に関する事務手続書
・入出力処理の手順・日程及び担当部署、ならびに保存等の手順および担当部署

3.2.3 運用要件
電子計算機、プログラム、プリンタ、ディスプレイ、操作説明書、など設備環境を示す。
出力用の設備であり、作成にかかわる電子計算機、プログラム、等でなくてよい。

3.2.4 要件の特例
・パッケージ等購入ソフト等の場合：パッケージ作成会社が公開していないため、ドキュメントの一部が備え付け不要。
・運用センター：通信回線を利用して納税地から見られればよいので、データ等が納税地に保存されている必要はない。
・外部委託：この場合は運用委託の契約書も備え付けること。
・COMによる保存代替：電子データによる保存をしていてもCOMに変えられる。ただし、3年間は併存する必要がある。

4．COMによる保存等

4.1 COMによる保存等の要件(COMはいわゆるマイクロフイルム)
4.1.1 電子データ備え付け(電子帳簿書類の要件)
4.1.2 機能要件
4.1.2.1 検索簿(インデックス)の備え付け
帳簿種類、取引年月日その他の日付、勘定科目
4.1.2.2 COM上のインデックス出力
4.1.2.3 画面および書面出力
4.1.2.4 出力の整然性、明瞭性、迅速性
4.1.3 ドキュメント要件
4.1.3.1 COM作成・保存事務手続書
4.1.3.2 真正COM出力証明書
・COM作成年月日
・COM作成責任者の記名押印
・保存事務責任者の記名押印
4.1.4 運用要件
4.1.4.1 マイクロフイルムリーダ、プリンタ
4.1.4.2 操作説明書

4.2 電子データの並行保存等
3年間の保存期間は以下のいずれかの確保を要する。設備とデータを併存させる。紙を撮影してマイクロフイルムとする場合、従来6年目以降であったものが、大量に発生する注文書等の書類については4年目、5年目の保存をOKにした。
・検索環境および検索機能を確保した電子データ保存
・インデックスデータ・システム

5．申請等の手続き

5.1 承認申請
5.1.1 申請先：所轄(納税地)の税務署長
5.1.2 申請日：備え付けを開始する日(課税期間の初日)の3か月前まで(施行後1年間は5か月前まで)
5.1.3 申請書類：申請書(申請書の名称・本店等の所在地、帳簿書類の保存場所・納税地、備え付け開始日など)、および添付書類(システム概要書、事務手続概要書、その

他参考資料)

5.2 変更(申請者側から)

5.2.1 取り止めの届出書：届出書提出日より承認は失効、止めた日から紙による保存を始める必要がある。

5.2.2 変更の届出書：システムが変わった場合は届け出る。添付書類の内容に変更があった場合も届け出る。どれくらいの変更が届出の対象となるかは議論のあるところだが、税務調書で判明するようなところは必須。

5.3 取り消し(当局の強制的な取り消し)

以下のいずれかの事実による承認の取り消し。罰則規定がないが、取り消しで対応。

・電子データの備え付けまたは保存が行われていない。

・電子データの備え付けまたは保存が施行規則によっていない。

6．電子取引情報の保存

帳簿保存とは直接関係ないが。

6.1 適用範囲

6.1.1 対象取引：EDI取引、インターネット取引など、取引情報の授受を電子データで行う取引。これらの取引を行った人は電子データの情報を保存しなければならない。

6.1.2 適用時期: 平成10年7月1日以降の取引

6.2 保存義務(強制)

所得税および法人税の保存義務者が電子取引を行った場合、電子取引情報保存を要する。但し、書面(紙に出力してあれば)またはCOMを保存すれば、電子取引情報保存を要しない。

6.3 保存要件

6.3.1 暗号化情報は認めない。復号化して保存する。

6.3.2 確定情報のみの保存を認める。仮情報ではない。

6.3.3 見積から決済までの取引情報を編集したものの保存を認める。

・EDI取引におけるメッセージ(見積書、注文書、納品書、支払通知書)、データ項目(注文番号、注文年月日、注文総額、品名、数量、単価、金額)

6.3.4 帳簿書類の電子データ、COMによる保存規定の準用

7．電子帳簿保存と情報システムの運営

7.1 情報システム体系と対象帳簿書類の選定

ドキュメント要件を満足して申請することはかなりの負担になる。従来のシステムについて、これからドキュメントを準備することは効率的ではない。例えば開発・更新に合わせて少しずつ整備・拡大していく方法が妥当か。どのシステムを対象とするか検討が必要である。

どのような媒体を使うか(CDR、MO、COM)、効率性、検索容易性、セキュリティなどの面から検討する。

帳簿作成システムをずっと維持していくのは大変なこと、保存については作成システムとは分けて、検索システムを別にすることも考えられる。

7.2 情報システム運営体制

7.2.1 組織体制の整備：法律に対応するため、方針を最初に固める必要がある。

7.2.2 ドキュメントの整備：システムの変更の時、特に注意が必要。

7.2.3 パッケージの評価：国税庁では○適マークは出さないので、個々に判断しなければならない。

機能要件を満足していないと認められない。利用者の立場からすると、今使っているパッケージがOKか確認が必要になる。新たに採用しようとする場合は要件をチェックしなければならない。バージョンアップの時には要チェック、しかも7年間保存する必要のあることも踏まえる。

7.3 会計監査等への対応

承認：紙のシステムの時にはあって、電子化したためになくなってしまうのはまずい。

セキュリティ：法律ではほとんど触れられていない。

インテグリティ(整合性)：

バックアップ：7年間保存するために重要紙よりも証拠力が弱くなり、企業にとって資産保護などの面で心配な面がある。

モニタリング：誰かが個々の取引や残高を管理していることでセキュリティやインテグリティを保証する。

確認・現物照合：現金、棚卸資産などを使って確認する手段はある。

7.4 システム監査

システム監査の立場で電子化に焦点をあてて監査してみるのもよい。

第60回研究会報告

日　時：平成10年９月18日
場　所：労働スクエア東京
講　師：(株)CRC総合研究所　芳仲　宏氏
演　題：「プライバシーマーク認定に向けて
　　ー認定のための体制整備と
　　システム監査ー」

No. 526　富山　伸夫

はじめに

第48号の会報で、プライバシーマーク制度について、講師により詳しく記載していただいたが、さらにこのマーク取得のための体制整備とシステム監査に関して、実際の経験に基づいて、解説がなされた。

講演要旨

プライバシー、OECDガイドライン、EU指令、通産省ガイドライン、プライバシーマーク制度概要等について説明があったが、会報48号の記事と重複するので省略する。

マーク付与の条件として、コンプライアンス・プログラム(C/P、実践順守計画)があるが、このプログラムの実効性の担保として監査が求められている。個人情報の収集・利用・提供に係わる業務を実施する部門とは独立した部門が監査(＝システム監査)を実施することになっている。

マーク取得の申請は、書類審査だけなので、適切に実施されているかどうかは、システム監査人に委ねている形になる。プライバシーマーク制度が要求している事項に対する監査項目、セキュリティ対策に関する監査、個人情報保護と各種基準(コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準、ソフトウエア管理ガイドライン等)の関連、監査体制と実施回数、監査報告のあり方等につき資料配付と説明があった。

尚、活発な質疑応答が交わされたが、紙面の関係もあり、当日配付された資料から、「システム監査の実施にあたって」の部分から一部を抜粋する。

「システム監査の実施にあたって」

年１回以上、事業者内部の個人情報の保護の状況を監査すること。

コンプライアンス・プログラムの実効性の担保としての監査が求められており、個人情報の収集・利用・提供に係わる業務を実施する部門とは独立した部門が監査を実施することになっている。従って、内部監査であれ、外部監査であれプライバシーマーク制度の趣旨に沿って、実効性の担保として実施するシステム監査の項目について記述する。

1.コンプライアンス・プログラムや社内規程類の整備状況

基本的には、プライバシーマーク付与認定基準とされている次の事項への対応が含まれていることを確認する。以下の事項は、プライバシーマーク取得への準備として、有効かもしれない。

(1) 通産省の個人情報保護ガイドライン又は業界ガイドラインに準じたC/P
(コンプライアンス・プログラム：実践順守計画)が作成されているか。
C/Pの内容について言い出せば、数多くの項目がある。
業界毎にこれから種々のモデル(サンプル)が出てくると思われる。
特に注意すべき点として、業界ガイドラインに準じたC/Pの作成では自社の特性に応じた部分の作成が重要である。
極端な丸写しでは、制度の趣旨に反するし、実効が伴わない。

(2) 次の事項が、規程類に判りやすく明文化されているか。

① 個人情報保護の管理者、社内の組織体制、責任、役割分担等
② 社員との間の個人情報保護に関する機密保持に関する条項。
(通常は、自社の機密や業務上知りえた顧客の秘密を守る条項が多い。)
③ 外部への個人情報の提供、取扱いの委託や受託を行う際の、責任分担や守秘に係る契約を締結する等の手続き。
④ 個人情報ドキュメントや電子化された記録(記憶)媒体の保管方法、廃棄方法等に関する手続き。
⑤ 個人情報保護に関する常設の相談窓口。
⑥ 年１回以上、個人情報の収集、利用及び提供に従事する者に対して個人情報の機密保持に係わる周知徹底の措置(教育・研修)。
⑦ 年１回以上、事業者内部の個人情報の保護の状況の監査等。
⑧ その他：関連規程の位置づけと相関関係を表す一覧表。

(3) 個人情報の直接収集に係わる業務について

は、運用業務の入力管理、データ管理、出力管理のルールに沿って集約した特定業務個別管理マニュアルとして、まとめられているか。センターのコンピュータを利用しない受託業務も同様。
(情報サービス業の場合、デジタル化された個人情報の受託処理業務を対象とし、それは運用業務の入力管理、データ管理、出力管理の範疇で一括管理される。
しかし、個人情報を直接収集する業務においては、個別業務として完結した管理マニュアルを作成することにより、プライバシーマーク制度の趣旨に沿ったセキュリティ対応や消費者対応がしやすいであろう。)

2.C/Pや社内規程類に準じた組織・体制等の整備状況

(1) 通産省の個人情報保護ガイドライン又は業界ガイドラインに準じたC/P
(コンプライアンス・プログラム:実践順守計画)の作成や見直しの担当者を指名し、活動しているか。
(2) 個人情報の直接収集に係わる業務に関する特定業務個別管理マニュアルの作成や見直しの担当者を指名し、活動しているか。
(3) 個人情報保護の管理者が指名され、社内の組織体制、責任、役割分担等に従った通達が、正式に社内アナウンスされているか。
(4) 個人情報の記録ドキュメント、記憶媒体の保管方法、廃棄方法等に関する手順・体制が整備されているか。(保管や廃棄の記録、保管場所、廃棄場所他)
(5) 個人情報保護に関する常設の相談窓口が設置され、外部に対して明示されているか。
(6) 年1回以上、個人情報の収集、利用及び提供に従事する者に対して、個人情報の機密保持に係る教育・研修を実施する計画を立案しているか。
(7) 年1回以上、個人情報の保護に関する監査を実施する計画を有しているか。

3. C/Pや社内規程類に則った運用状況

(1) C/Pや社内規程類は、定期的に見直しされ、自社の特性に応じた改廃が実行されているか。(改廃記録の確認他)
(2) 個人情報の直接収集に係わる業務に関する特定業務個別管理マニュアルは、定期的に見直しされ、自社の特性に応じた改廃が実行されているか。(改廃記録の確認他)
(3) 個人情報保護の管理者、社内の組織体制、責任、役割分担等が、実態に即して機能しているか。(実在確認と分担業務のヒアリング)
(4) 個人情報保護に関する常設の相談窓口が設置され、担当者は外部からの問い合わせ等に対して機能しているか。(実在確認と分担業務のヒアリング)
(5) 個人情報の記録ドキュメント、記憶媒体の保管方法、廃棄方法等は定められた手順に沿って実行されているか。(現場確認、記録確認)
(6) 年1回以上、個人情報の収集、利用及び提供に従事する者に対して、個人情報の機密保持に係る教育・研修を実施しているか。
(実施記録、テキストの確認、受講者へのヒアリング、教育・研修への参加)
(7) プライバシーマーク付与を受けた後、マークの使用に際しては、「プライバシーマーク使用規程」、「プライバシーマーク使用の手引き」を遵守しているか。

感 想

プライバシーマーク制度も国際的な協調を意図して、急いで対応した形式になっているが、これで個人情報保護の意識が高まれば、これに越したことはない。

個人情報保護の浸透策として、プライバシー侵害の法的罰則強化や裁判による社会的強制が始まる前に、プライバシーマーク制度によるインセンティブに訴える方法は、案外正解かもしれない。

実際には、システム監査人に下駄を預けたような形を作って、あとは現場でうまくやれということのようだが、これを機会に、プライバシーマーク制度の実効性の担保としての、システム監査が広まれば幸いである。

「情報セキュリティポリシーの必要性と策定方法」

～企業は従業員(人)による情報セキュリティの維持に、どう対処すべきか～
第3回(全3回)

日本ヒューレット・パッカード株式会社
マネージング・コンサルタント
佐藤 慶浩

具体例(序説)

内容を見てあまりに当たり前な文章でがっかりするかもしれないが、セキュリティ方針がどんなものかの具体例として紹介する。ただし、ここで紹介する例は、これからセキュリティ方針を策定しようとする方々にとってのたたき台にはならないし、推奨例にもならないことに注意していただきたい。その理由については、後程説明する。

1．序説 (参考例)

情報セキュリティの管理を実質的なものにするには、運用と権限と義務を定めたセキュリティについての方針が必要であり、方針は現場が受諾できるようなものであって、その方針を企業内全体で通用する包括的なものとなるように系統だてた構造とすることが必要です。

そのような構造を作成することで、方針についての包括的なフレームワークが構築されることになります。

このフレームワークは、セキュリティ維持に必要な指示を設定し、広範に用いる手引きを提供し、社内でのセキュリティ関連の施行への参画を上級管理職が支持していることを明らかにするものです。

▲ ▲ ▲

方針を徹底することによって、企業の情報資産が適切に確実に保護されるようにするために、セキュリティ・フレームワークは、分散コンピューティング環境において欠くことのできないものなのです。

▲ ▲ ▲

セキュリティ方針では、情報の機密性を保つだけでなく、情報の可用性や情報の有用性を確かにし、さらに、情報にアクセスできた際に、その情報の作成元および内容の正当性を保証することにも言及します。

▲ ▲ ▲

セキュリティ・フレームワークを作成することは、セキュリティ維持に必要な指示を設定し、広範に用いる手引きを提供し、管理職がセキュリティ戦略の実装を支援していることを認識してもらうことの手助けにもなります。

このフレームワークが存在しており、従業員に対して継続的な教育をすることは、情報が不正に扱われた際に、企業自身を法的に保護する上でも必要です。

序説には「このフレームワークはセキュリティ維持に必要な指示を設定し、広範に用いる手引きを提供し、社内でのセキュリティ関連の施行への参画を上級管理職が支持していることを明らかにする」とある。この文章では、セキュリティに関して自分の業務として参画するということについて会社が経営会議でそれを支持している、セキュリティ維持に時間を使うことは業務だ、ということを会社が認めていると宣言する。

次に「このセキュリティ方針のフレームワークが存在しており、従業員に対して継続的に教育をすることは、情報が不正に扱われた際に、企業自身を法的に保護する上でも必要です」という文章がある。これは、何か事が起こった時にそれが再発防止できるということを論理的に言えるように、それがこの「法的に」という言葉に表れている。これは必ずしも従業員の責任を明確にして、問題を起こした従業員を首にするぞという意味ではない。従業員に悪意があれば懲罰の対象かもしれないが、そうでないならば、どうすれば改善できるのかということを明瞭に、対外的にメッセージとして出せなければいけない。たとえば、セキュリティを一生懸命やっても間違って機密情報が外に出てしまうということがあるかもしれない。方針の目標と現実とは違うので現実には出てしまうことがあるかもしれないが、それが従業員の手落ちだったのか企業としての手落ちだったのかということが分からないと大変なことになる。従業員が手順書を守らなかったということであれば対外的な申し開きとして「手順書はきちんとできていました。ただ従業員が守りませんでした。恐らくこれは会社として従業員の教育が徹底してなかったからです。教育を再度徹底させていただきます。これによって今後はしかるべき事は起こらないということにしたいと思います」と表明できる。

顧客から預かった機密情報が間違って社外に出てしまったといったことになると、これは企業の信用問題に関わってくる。再発防止策を明確に説得できないと、もしかすると企業全体のビジネスが失墜する可能性がある。重要なことは、経営層にもこの認識を持っていただくことである。何故うちの会社はセキュリティ方針を立ててしっかりやっていこうと考えているのかを認識しなければいけない。

法律的には機密として扱われたものが機密情報だと定義されており、機密維持の努力を説得できないと、情報が不法に利用されたのではなく、必要な業務を怠ったのだとして、一方的に責められてしまうことになる。これは誰も運用していないセキュリティ方針があるだけでは不十分であることを意味する。また、従業員に対して継続的な教育をするということは、たとえば毎年1回説明すると中途で入ってきても必ず1年以内には方針を知るチャンスがある、ということで重要なのである。

具体例(パスワード方針)

5.15 パスワード方針 (参考例)

会社では、ユーザの識別にパスワードを用います。パスワードは秘密にしておかなければなりません。

目 的

会社はユーザそれぞれを唯一無二に識別できなければな

らず、その識別を認証できなければなりません。ユーザーのユニーク識別名とパスワード認証がシステム資源を保護するためのセキュリティの基本部分として使われます。
対象となるデータの機密種別によって、さらに追加の認証方式を採用することもできます。

パスワード
ユニークなユーザ識別を認証するのに使います。秘密にしておかなければなりません。
辞書にのっている単語であってはなりません。
ユーザの名前やユーザに関連する情報から簡単に派生させたものではなりません。
ユーザ本人が書き留めないと記憶できないようなものであってはなりません。
ユーザ本人が変更できなければなりません。

範　囲
唯一無二となるシステムのユーザとして識別されるすべての個人は識別認証のためにパスワードを利用しなければなりません。
ユニークなユーザー識別名はセキュリティのアクセス制御に用いられ、監査用の記録に記録される情報の基本となります。

方針への遵守
ユーザの識別と認証の基本を守るため、以下の基準が遵守されます。

ユーザ識別とパスワードが、すべての自動システムとデータアクセスの基本となります。
すべてのユーザは、識別名とパスワードの必要性を理解しなければなりません。
ユーザは、自分に与えられたものではない識別名を使用してはなりません。
自動化された処理では、ユーザの識別とパスワードによる認証を行わなければなりません。
パスワードの管理手順と処理が定められていなければなりません。
パスワード方針に対する違反は認められません。

「会社ではユーザの識別にパスワードを用います。パスワードは秘密にしておかなければなりません」と言うのが方針である。これに関して、それをなぜやるのかという目的、パスワードと言っている言葉の定義、それからこの方針に関する範囲、方針を守るということの具体的な例、それから違反ということを方針の補足的な説明文章として用意しておく形になる。議論に議論を重ねて最後の文章はこのように簡単な文章にしていかなければならない。

5.15　パスワード方針　(参考例)

違反
ユーザには自分のパスワードの機密を保つ義務があります。
パスワードの機密を保つことを怠った場合には、その結果として発生した問題についてユーザが責任を負う場合があります。
セキュリティ違反は会社からの信頼を裏切る深刻な問題とみなされます。
そのときの事情によっては、処罰などの対象となることがあります。

パスワード方針の違反の条項には「セキュリティ違反は会社からの信頼を裏切る深刻な問題と見なされます」と記述されている。パスワードをもらって機密情報にアクセスできるということは、その人に対して会社は信頼を与えており、このセキュリティ違反の本質的な問題は、機密情報をもらしたり、人のコンピュータを勝手に使うことではなく、会社からの信頼を裏切ったということにある。何故会社はセキュリティを守って欲しいかと考えているのかを認識させる必要があるのである。

「そのときの事情によっては、処罰などの対象となることがあります」の記述は、言葉の裏を返すと、事情によっては処罰などの対象とならないこともあることを意味する。どんな条件かはセキュリティ方針の次のステップであるガイドラインで決めていけばよく、ここまでのことでならば経営会議での承認は得られる。

費用対効果

セキュリティについての費用対効果を考える場合があるが、それよりはむしろ、怠った場合の対被害度合いを論じる方が現実的だ。しかし、それはセキュリティ技術へのことであり、セキュリティ方針の策定は必要最低限の必須事項と考えるべきである。先にセキュリティ方針なくして問題が起きたときに、企業としての社会的な信頼に重大な影響が考えられると言った。「セキュリティ方針がない場合の副作用に対処するよりも、セキュリティ方針があったほうがずっと楽だ」という言葉に尽きる。

セキュリティポリシーとは？
（一般の書籍における概念）

- **米IT＆T社**　株主への年次報告書
  セキュリティポリシーを導入した年、年次報告書でIT＆T社会長が「セキュリティはIT＆T社の重要な武器となる」と述べている。
- **ファイアウォール** 著 William Cheswick Steven Bellovin
  セキュリティに対する組織の姿勢を反映した取り決め事項である。どこまでを許容行為とし、それ以外の侵害行為に対してどのように対処するかをあきらかにしたものである。
- **FIREWALLS** 著 Brent Chapman, Elizabeth Zwicky
  セキュリティ方針をまとめるのは、長期にわたるプロセスであり、ほとんどの技術者が望むような作業とは正反対である。しかしセキュリティ方針がない場合の副作用に対処するよりもずっと楽である。

まとめ

完成したセキュリティ方針の文章は当たり前の内容であり、がっかりさせるものかもしれないと具体例のところで述べた。しかし、セキュリティ方針はそれを策定するために企業内で部門を超えて議論し共通の価値観を見出

すという過程に、むしろ重要な意味がある。よその会社の経営方針を文章としてだけまねる者はいない。セキュリティ方針もまた同じで、他から文書を借りてくるだけでは意味がない。自分の企業で議論して作成してはじめて意味のあるものになる。

情報システムの目的は、ビジネスでの積極的な情報利用である。

セキュリティ方針を考えるとき、情報システムの目的は情報の共有であることを忘れてはならない。その手段のひとつである情報セキュリティの議論に偏重してはならない。

セキュリティ方針は経営会議で承認する。

直接部門の生産性に影響を与えるものであることを認識し、セキュリティ方針は最終的に経営会議での承認を得たものとして発布する必要がある。

セキュリティ方針策定の起案を経営会議に付議することで、策定作業中には社内の広範な部門からの協力を得ることができる。

策定するセキュリティ方針を経営会議で扱えるものにするために、記述内容を「何」と「なぜ」の階層で限定する。

セキュリティ方針は目標を定める場である。

企業としてセキュリティはどうあるべきかを活発に議論して策定することが大切である。システムの現状や既存の技術などにとらわれて、最初から目標を限定してはならない。

「何」をすべきかに加えて、「なぜ」なのかを方針として明確にすることが重要である。逆に、「いつ」までに「どの部署」で「誰」がするのかは方針承認後に、経営会議の外の後工程で決定すればよい。どんな製品を使うのかは、更に後工程の「どうやって」で決める。

セキュリティ方針は継続的に維持しなければならない。

セキュリティ方針は一過性の文書ではない。系統立てたセキュリティ方針フレームワークを策定することで、運用の対象として継続的にその維持に努めなければならない。

セキュリティ方針をもとに、リスクを評価し対策を計画・実施して、その結果を監査するという一連の運用により、セキュリティ方針は企業の情報セキュリティの取り組みへの経営陣による意志表明となる。このことは品質に対する企業努力と同じように、今後の電子社会における企業の差別化点のひとつになると考えられる。

以上のようなことを議論する策定作業の運営にあたっては、最新の技術知識や、技術的なことに加えてディスカッションにまつわるスキルを必要とする場合があるが、そのような部分は社外から協力を得ることも検討できるであろう。日本ヒューレット・パッカードのセキュリティ方針策定支援コンサルティングは、そのようなお手伝いをするサービスである。

コンサルティングとしては、セキュリティ方針のたたき台を示して提供するのは比較的やさしい。しかし、それでは、その企業にとって実際に運用されるようなセキュリティ方針にはならない。当たり前と思っていることが、なぜ当たり前なのかをディスカッションするその過程によって、その言葉や言い回しは企業ごとの文化を反映し、全従業員が「セキュリティを守るのは当たり前」だと思える文章に仕上がるのである。

ここでの説明がセキュリティ方針の策定のきっかけや参考になれば幸いである。

「情報システム部長日誌」第3回

No. 999 新城 道彦

過日の常務会に「イントラネットの構築計画の全体構想及び第1期の実施計画」を提案した。

常務会は常務以上会長まで8名で構成し、取締役会以前の、いわゆる実質的経営意志決定機関であるが、実質決定はワンマン会長が仕切っているのだから、これも形骸化している。とはいえ、ここを通過しなければ、経費の執行は出来ないから、現場としては大きな関門である。

肝心の会長が新しい技術に懐疑的で、情報システムは子どもが新しいおもちゃを欲しがるように、いろいろやりたがっているのではないかという疑いを持っており、やりにくいのだが、やはり「こんなことに金をかけないでも、気の効いた人間は情報収集もし、ちゃんと業務を成り立たせているのではないか」といい出した。暗に、自分はそういうふうにやって来たぞいうわけである。

役員の方はまた会長の持論が始まったという顔付だが、衆人環視の中で単純に同調も出来ず、情報システム担当を含め反対もしない。海外事業担当の副社長などは早くからメールを使い、その効用をわかっているのに知らんぷりである。常務会に提案しながら結論が出ず、保留、再検討となれ

ば、次に前回案をそのまま再提案といかず、練り直しなど余計な手間がかかる。それより何より現場から、部長何やっているんですかといわれるのは必定で、会長に少し逆らうリスクと現場に戻ってからの突き上げのきつさ考えれば、やはり一言いわざるを得ない。

「基本的にはおっしゃる通りです。会社を実質的に回しているのは3割、あとの4割は可もなく不可もなく、あとの3割はぶら下がっているとすれば、初めの3割は何がなくてもどうにでも対応してくれる部分です。ですが、逆に、この部分はいい武器があれば、さらに力が出せるわけです。今度の計画は、その3割の生産性をさらに上げることになります。あとの7割との差はますます開きますが、これはまた別途縮める方策を考えます」──今会社を動かしているのは会長より若い層で、そちらを支援するのだ、彼らからの要請もあるのだといっているわけである。

雑誌や新聞などに出ているような、これで全社のコンピュータ・リテラシが向上して云々などといえば、海千山千里千がすかさず反論してくるのだが、やや虚をついたのか、一瞬静寂が流れる。ここはもう一押しである。

「社外との電子取引はますます拡大するわけで、社内に一定のインフラを備えていないと、取引の機会がなくなる可能性もあります。お宅ははずすなどといわれてから、やれといわれても間にあいません。全体的に見ても、今この段階というのは先進的ではなく、ほぼ平均で、これ以上は遅れたくありません」

会長が、しょうがないかという表情になった所で、司会の経営管理室長が「当面の投資は第1期分だけで、あとはまた個別計画がまとまった時点でそれぞれ審議するということですね」と確認してくる。第1期分なら数千万、全体では数億であるから、保留または却下にしなければならない額ではないといってくれている。「もちろん、第2期以降分は改めて審議いただきます」。結局、承認となり、情シス部長の威信は保たれた。

このあと、ある役員が「私はパソコン操作できないけど、3：4：3でいくと、どうなりますかね」といってきた。

なるほど難しい。会社全体を分母にすれば役員は自動的に上の3割かも知れないが、階層別に分ければ、役員の中で3：4：3論が出てくる恐れもある。そんな差し障りのある線引きは情シス部長の職責外であり、会長、社長と役員各自でやっていただくより他はないのである。

公開鍵方式暗号化ソフト（ＰＧＰ）の使い方の紹介　その2 Fingeprintとは？

セキュリティ・技法合同研究会

この小渕さんはあの小渕さんか？

前回は、メイルのやりとりをやる際に互いのプライバシーをのぞかれないように、メイルを公開鍵方式で暗号化してやりとりする方法を記載した。でもある日、突然、「私は、小渕といい、日本の総理大臣をしております。いろんな悩みや問題点をメイルにて送ってください。公開鍵は以下の通りです。」というメイルが届いた場合、この本人が本当の総理大臣であることをすぐに信じることができるであろうか。素直な方は、直ぐに自分が抱える問題点を書いて、添付してある公開鍵で暗号化して自分の悩みをメイルするだろう、そして、それが自称小渕さんに届くわけである。途中の人には見られることはないが、自称小渕君は、総理大臣として見てくれるのか、それとも、人の悩みを見てひっそりと笑うのだろうか。

今回は、この様な、本人確認の問題をどのようにして解決するためにどのようにしたらいいかについて記載する。まず、公開鍵の持ち主が本当に小渕さんであることを確認する方法について考えてみたい。

メッセージダイジェスト関数

その前に、ＭＤ４，ＭＤ５、SH関数などのメッセージダイジェスト関数というちょっとしたからくりについて勉強してみたい。まずこれらの関数は、不特定の長さの文章をある長さの文字にマッピングする関数である。すなわち夏目漱石の小説が電子化されてあるとすると、それをMD5などの関数を通すと、６４ビットの文字に変換してくれるものである。この変換されたビット列からは元の文章を復元することは非常に難しい。（または、人間の感覚でいうところの無限の時間がかかる。）それと、元の文章に対して一意にそのビット列はきまり、同じものが現れることがない。この様な関数をメッセージダイジェスト関数という。すなわち、元の文章を見せることなく、その文章によって一意に決まるビット列を対応させるのである。それも一方向関数なので、逆に解くことが不可能に近い。

（この応用事例は、ワンタイムパスワード、電子

署名などに応用されている。)

Finger Printとは？

この関数を使って、PGPでは公開鍵の指紋(Finger Print)を作成する。実際に、PGPを使ってFinger Printを作ってみよう。前回紹介した、PGPツールのPGPツール(図1)の一番左にあるPGPkeyをクリックすると登録されているkeyの一覧が表示される。自分の鍵を選んで、右クリックするとポップアップメニューが現れる。(図2)その一番下のkey propertiesを選んでクリックする。すると、図3のようなウィンドウが開く。この一番下にFingerprintとある。これが、選んだ鍵をメッセージダィジェスト関数を通して得られた結果である。これを選んで右クリックするとコピーのメニューが現れてクリップボードにコピーする事ができる。これを張り付けると下記のようなものが現れる。

AEAB 98AD 6487 2A53 4919 88B8 61C3 5A97 936B FDD9

これが筆者の公開鍵のFingeprintである。公開鍵に比べると短く、人に伝えやすい。
これを別の手段、たとえば、名刺に印刷するとか、電話で伝えるとか、多くの場合は、メイルと頻繁に交換する際にサインの部分にそれを記すことで相手に伝える。その上で、相手に自分の公開鍵を送る。すると、送られた相手は、同じ方法で、送られてきた公開鍵のFingerprintを作り、以前に知らされていたものと比較する。これが同じであれば、送られてきた公開鍵は確かに、その本人のものであることが照明されたことになる。
先ほどの、小渕さんの例でいえば、NHKなどのテレビなどで小渕総理の公開鍵のFingerprintは、××××ですよ、と公開すれば、小渕さんから公開鍵が送られてきたとき、そのFingerprintを計算して、テレビで見たものと同じであれば、確かに、小渕総理大臣だなと確信できるわけである。

小渕さんからメイルが、本当か？

これで、確かに本人の公開鍵を信頼する方法は確立できた。これで安心して、この公開鍵を使って本当の小渕さんに景気回復の秘策を教えられる。(すなわち、小渕さんになりすますことを不可能としたのである。)
次の課題は、小渕さんからその秘策についての質問と実際の不良債権の額が暗号化されて送られてきた。果たして、このメイルが小渕さん自身からのメイルであるか、また、この中に記載されている不良債権額が改竄されていないということをどのようにして保証することができるだろうか。
これが次の課題である。送ってきたメイルが本当に本人のものか、また内容が改竄されていないかどうか。これが電子署名という方式で解決される。次回にはこのメカニズムを解説したい。

図1 PGPtool

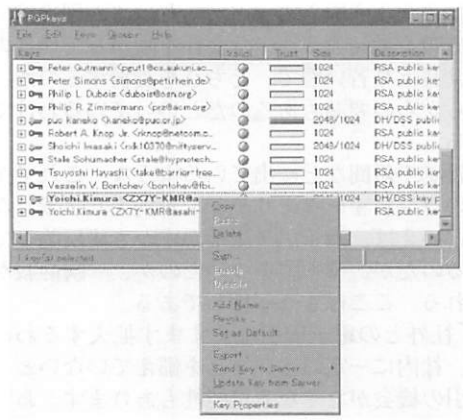

図2 PGPkey

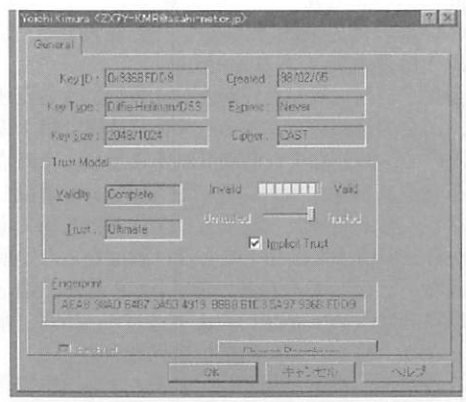

図3 Key Properties

中部支部だより

No. 124 原 善一郎

秋口になりまして、中部支部では多彩なイベントを行っております。

1.中部支部主催セミナ

岐阜市で行われました、「マルチメディア&VRメッセ岐阜'98」に協賛しまして、岐阜市にある未来会館でセミナを実施しました。

座長は、澤SAAJ中部顧問でした。

テーマ：「インターネットを300%仕事に生かす」

10月16日(金)

11:00～12:00 澤 貞夫
「良いソフトハウスを考える」

13:00～14:00 大野 淳一
「いろんな使い方でインターネット」

14:30～15:30 河内 隆
「インターネットで楽々情報検索(入門編)」

10月17日(土)

11:00～12:00 渡辺 利夫
「インターネット通販業 成功のカギ」

13:00～14:00 中西 昌武
「インターネットで情報の質があがるか？」

14:30～15:30 萬代 みどり
「川柳に見るEメールの使い方」

いずれのセミナも、10名前後の受講生がありました。

(財)ソフトピアジャパンは、「とても有意義なセミナでした。この件は、岐阜県知事にもぜひ報告をし、来年度以降はもっと、積極的に日本システム監査人協会に協力を依頼したい」と感想を漏らしていらっしゃいました。

2.中部支部主催 長野合宿

恒例となりました、中部支部主催の合宿です。

今年も、「よく遊びよく学べ」合宿となっております。

1. 日　　時　平成10年11月15日(土)14時
　　～16日(日)13時
　(但し、昼食が取れない場合は11時まで)
2. 場　　所　長野県塩尻近辺
　(東京から参加の方もあり、両方面から便利な場所)
3. 参加人数(見込)　20人前後
4. 参 加 費　未定
5. 合宿内容(案)
　昨年と同様に講演と分科会討論・発表とします。
　・講演　失敗要因が異なる3パターンの事例講演
　・討論・発表　分科会で討論し、分析結果(ノウハウ、監査ポイント)人材育成計画のまとめと発表
6. そ の 他
　会員の紹介があれば、会員以外の方も参加頂けます。

参加費が10月中旬時点では未定になっています。合宿のときの「討論会の時間があやしい」ということで確定しないのです。打ち合わせのメールでは、

＞・20人の会議室もOKです。
＞＊午後半日の料金で夜は9時まで使用できます。
＞＊夜の9時以降は＋3000円です。
＞(まさかとは思いますが、原支部長のことですから？)

読まれております。毎回、「みなさん、早く課題をこなして、早く遊びましょう。」と言いながら深夜まで課題をやるために会議室を開けておりました。女性会員の皆様からは「ゆっくりとお風呂に入る時間が無かった」との苦情を沢山頂いております。

等といいながら、ことしもにぎやかな合宿になりそうです。

3.「世界ソフトウエアテクノロジー会議準備会」参加

世界各国のソフトウエア技術に関係する地域の連携と連係を取ろうという試みを(財)ソフトピアジャパンが行っています。その会議のメンバーとして、日本システム監査人協会へもご招待がきました。地元の理事として、参加をしてきました。本会議は2000年の予定です。協会への期待も高まるでしょう。

九州支部だより

行武 郁博

「個人信用情報保護・利用の在り方に関する懇談会報告書」について

6月6日の日経新聞に「大蔵・通産両省は消費者信用情報保護・利用法(仮称)を制定する方針を固めた。これより多重債務者の増加を防止し同時にプライバシー保護のため悪質な情報漏洩には罰金や業務停止命令などの罰則を設けることにした。情報保護・利用の在り方に関する懇談会(両省共催の私的勉強会)が月内に「情報漏洩には法的措置を講ずるべきだ」との意見を纏める予定。大蔵・通産両省はこれを受けて法案を次期通常国会に提出する」という主旨の記事が掲載された。その後、大蔵省ホームページに

「個人信用情報保護・利用の在り方に関する懇談会報告書」が掲載された。以下、その所感を述べる。

まず第一に報告書は個人信用情報保護・利用の重要性、緊急性に鑑み、一般法での立法の立場は採らないといっている。「情報化白書1998」の「各国におけるプライバシー関連法の制定状況(P281)をみると法律の名称からの類推であるが、保護対象を特定の個人データに限定したものは殆ど見受けられない。わずかに韓国の「信用情報の利用および保護に関する法律」(1995)がある。国際的な対応からみても早晩一般法での対応が求められるのではないかと思われる。

第二に報告書は個人情報保護といういわば受け身だけでなく個人情報の利用促進という積極性を強調している。しかしながらそのために解決しなければならない多くの問題点の存在をも指摘している。

信用情報機関が業態別縦割であること、与信業者のすべてが信用情報機関に加入していないこと、またすべての信用情報が登録されてはいないこと、情報の質のばらつき等々である。これらの問題点の立法的検討のためには多くの時間を必要とするであろう。個人情報の利用促進の法制化検討のために立法化が遅れることになるおそれはないだろうか。すでに韓国での立法化の例があるので杞憂かも知れないが。

第三はシステム監査に関連する点である。情報の適正管理のため予信業者や信用情報機関自体による内部監査は必須であると述べている。この内部監査にはシステム監査が含まれていると理解される。信用情報機関を通じた情報の共有システムは適正与信のための社会的インフラであり、地方公共団体等による監督の強化も述べられている。そうであれば、システム監査においても一定の有資格者による監査や外部監査の実施をも検討すべきではないかと思われる。

前述の「各国におけるプライバシー関連法の制定状況」をみると多くの西欧諸国で立法化が行われ、またアジア地域においても韓国(1994－5)、香港(1995)、台湾(1995)と立法化が進んでいる。先進国である我が国は個人情報保護の立法化では完全に遅れをとっている。報告書が今後、「法的措置のタイミングなどにかかわらず……検討してゆくことが必要」といっているのは一寸気になるところである。

ことの重要性、緊急性に鑑みて、一日も早い立法化を望むものである

中国支部だより

No. 387 安原 節男

最初にお詫びと訂正です。前回の会報で、中国支部のメーリングリストのアドレスを、私個人のアドレスを書いてしまいました。"saajc@hiroken.ne.jp" が正当です。

10月は「情報化月間」とか、広島でも「情報化シンポジウム」などが盛んで、システム屋には忙しい月です。こうした背景もあって、中国支部のブロック研修会も11月中旬に計画しました。

広島・松江・岡山・高松と会員分布の広いなかで、年に一度はお顔を拝見できる機会をつくりたいと考えていますので、何とか都合をつけてご参加いただきたいと思います。会員の皆様には、メーリングリスト・FAXなどでご連絡を

「地方自治体のシステム監査を考えるシンポジウム」のご案内

当協会主催の掲題シンポジウムのご案内です。自治体関係者以外でも大いに参考になる内容ですので、会員の皆様の多数の参加をお願いいたします。

1．日　時：11月18日(水) 13:00～17:30
2．場　所：機械振興会館地下3階研究室2
3．参加費：3千円
4．プログラム：
　講演1：システム監査の役割
　　(通産省　澤野氏)
　講演2：アンケート結果報告
　　(協会理事　小野氏)
　講演3：藤沢市におけるシステム監査の事例(藤沢市　徳江氏)
　パネルディスカッション：地方自治体における情報システムの課題とシステム監査
　パネラー：徳江氏、深田氏(船橋市)、藤谷氏(協会顧問)、梅津氏(協会顧問)
　コーディネータ：橘和氏(協会会長)
5．お問合せ、申込みは協会事務局へ

さしあげます。

私事で恐縮ですが、今年3月ころからやっておりました、X運送(株)の「給与計算」のシステム監査が、10月中には一応終われそうです。

「情報システム監査実践マニュアル」発刊されました！

実践マニュアル分科会　松枝　憲司

10/15に(株)工業調査会から、日本システム監査人協会編「情報システム監査実践マニュアル」(定価4,200円)が発刊されました。本書は96、97年度と継続してきた「新システム監査基準実務手順書」をベースに、新たに「システム監査が必要とされている現在の社会状況」「本書の活用事例」などを書き加えました。また実務手順書で作成した「システム監査基準活用のポイント」や各書式類については、本書に一部掲載するとともに、実際に活用してもらえるようFDに収録し添付しています。

想定読者は、「システム開発管理者」「システム運用管理者」「システム監査人」「システムコンサルタント」「システム監査技術者試験受験生」などです。

96年4月から2年半かけて、完成したプロジェクトの成果物です。是非とも皆さんに手にしていただきたいと思い、本書のチラシを会報に同封しています。

このチラシで直接出版社に申し込めば、著者割引が適用され、2割引で購入できます。1冊からでも申し込めますが、本の送料及び振込手数料は自己負担なので1冊ではメリットがないかもしれません。

初版3000部です。「情報システムに関わる者必携の書」ですので、会員の方はもちろん、友人、会社などに積極的に販促をお願いします。また最寄りの図書館に対して、購入希望を提出してください。

今回の会報のメイン記事である「2000年問題」について、通産省と協会の連名で作成した「経営者の皆様へ 西暦2000年問題をご存じですか」の小冊子を、急遽本書に差込むことが出来ました。合わせてご覧ください。

本書刊行にあたりまして、過去2年半で延べ16名のプロジェクトメンバーの方及び理事各位の御努力と御協力に感謝いたします。

資格の値打ち

No. 76　中尾　宏

「取れないと気になるが、取っても食えない物なあに」答えは足の裏についた御飯粒、ほんとの答えは「○○資格」とか。ニフテイのフォーラムを覗いていると、資格にまつわる喧々諤々・悲喜こもごもの声が面白い。ところで最近、協会会員になじみ深い資格をもろに採用条件として公募している市役所がある。

その市役所とは、ベイスターズ歓喜にわいた横浜市で、公募要領をみると次のとおり。

1．受験資格　年齢　34歳から45歳
　　資格　システム監査技術者、システムアナリスト、プロジェクトマネージャ各試験いずれかの合格者
2．業務内容　課長補佐又は係長として、1乃至2人採用予定
　　①市のシステムを信頼性・安全性・効率性等の観点から評価・改善指導
　　②システム開発等に、企画立案・実施・評価までのプロジェクト統括
3．給与待遇　年収約700万から900万
4．試 験 日　平成10年12月13日(日)
5．申込受付　平成10年11月18日から27日まで
　　案内書・申込書は市の案内所、区広報相談係で貰える
　　ホームページ　http://www.city.yokohama.jp/

当協会では、地方公共団体へのシステム監査推進のPRを行ってきたが、そこへ行けばしかるべき有資格者へのコネがつけられそうだと、広告ならぬコラムで公募の片棒を担ぐ羽目となった。われと思わん方は、自薦他薦で挑戦してみられたら如何。

新規入会個人会員

番号	氏　名	勤務先・所属	
837	斧　政男	(株)日立ビジネス機器	第一システム部
838	谷本　佳己	日本電信電話(株)	第一法人営業本部第二営業部
839	寺下　厚二	(株)宮崎情報処理センター	大阪支社
840	奥野　公彦	住友金属システム開発株式会社	西日本サービス部
841	沼野　伸生	(株)富士総合研究所	システム業務部品質管理室
842	杉野　吉伸	横河ディジタルコンピュータ(株)	中部支社営業部
843	松本　竜	(株)アイ・シー・エス	システム部
844	吉田　進	(株)日立製作所	情報通信事業部

事務局よりのお願い

1．会員の宛先の郵便番号を７桁に変更しました。

パッケージソフトの機能を使って変更しましたので、完全に対応がとれてないところがあります。封書宛先の郵便番号をチェックして下さい。違っていましたら、住所・氏名・会員番号と正しい郵便番号を書いて、FAXで事務局に送付して下さい。

2．会費未納者へのお願い

10月20日現在の会費未納者に会費納入のお願いの手紙を差し上げております。
協会活動は会費によって成り立っています。また、会費が納入されることを想定して予算を組んであります。予定通り会費が納入されなかったり、納入時期が遅れると、支払いに支障が発生します。支払いができないと協会活動に大きな支障が発生します。
是非、未納分の納入を早急にお願いします。
また、会員の勤務先や住所が変わった場合、速やかに協会事務局にご連絡下さい。
以上、よろしくお願いします。　（会計担当理事）

発行所　日本システム監査人協会
発行人　橘和　尚道
事務局　〒151-0073
東京都渋谷区笹塚２－１－６
笹塚センタービル５Ｆ
(株)産能コンサルティング内
TEL. 03(5350)9268 FAX. 03(5350)9269
ﾎｰﾑﾍﾟｰｼﾞ　http://www.saaj.or.jp/
※ご連絡はなるべく郵便または、FAXでお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)
三谷慶一郎　(株)NTTデータ経営研究所
TEL. 03(5467)6321 FAX. 03(5467)6322
QZG07732@niftyserve.or.jp
金子　長男　(財)公営事業電子計算センター
TEL. 03(3343)4560 FAX. 03(3343)6758
kaneko@puc.or.jp
富山　伸夫　(株)データ総研
TEL. 03(5695)1651 FAX. 03(5695)1656
GFF00037@niftyserve.or.jp
片寄早百合　日本NCR(株)
TEL. 03(5456)6156 FAX. 03(5456)6436
Sayuri.katayose@Japan.NCR.COM
吉田　裕孝　三井物産(株)
TEL. 03(3285)2058 FAX. 03(3285)9939
Hi.Yoshida@xm.mitsui.co.jp