SAAJ 日本システム監査人協会報

クリフォード　ストール氏講演会に協賛

－　カッコウはコンピュータに卵を生む　－

去る10月7日、東京新宿センチュリー・ハイアットホテルに於てNHK放送研修センター主催のコンピュータ・セキュリティー・セミナー『国際スパイサッカーを摘発して』が開催された。このセミナーにはセコム㈱、㈱草思社とともに当協会も協賛した。

数年前、当時の西ドイツのハッカーがアメリカの軍事機密を東側の情報機関に流していた罪で逮捕された事件をご記憶の方も多いだろう。最初にハッカーの存在に気がつき1年にわたる追跡の末追いつめたのがクリフォード・ストール氏である。同氏は当時カリフォルニアのローレンス・バークレー研究所勤務の天文学者であったが、望遠鏡のレンズの設計担当からコンピュータ・センターのシステム監理者に異動した途端、同僚の発見した課金システムの75セントの齟齬の原因究明にあたることになった。課金システム自体には問題がないのに誰かが研究所のコンピュータを勝手に使っている。ストール氏は、ハッカーの動きをモニターするために、研究所のモデムをコンピュータの間にゲイトウェイを設けてハッカーの行動を逐一記録した。研究所のコンピュータは様々なネットワークにつながっている。ハッカーはTYMETから研究所のシステムに入り込み、ここを介して軍事ネットMILNETに入り、アメリカの軍事機密情報を得ていたのである。衛星回線や海底ケーブルを

Clifford Stoll
クリフォード・ストール

通じたはるかヨーロッパ大陸からのハッカーの侵入経路を逆探知するために、囮情報まで仕掛けて時間稼ぎをしたアイデアと努力には頭が下がる。我々は往々にして、近視眼的な対症両方に終始しがちだが、真理追求への科学者のあくなき探究心と執念が、長い追跡の末ドイツ・ハノーバー在住のハッカー逮捕となって実を結んだ。

ハッカーは何故ここまで跳梁できたのか。UNIXの暗号システムはパスワードから暗号を作ることはできるが、その暗号を元に戻すことはできない。ハッカーがユーザーファイルを手に入れてもパスワードを使うことはできない筈にもかかわらず実在のパスワードが次々に使われていた。ハッカーは実にUNIXの暗号システムで暗号辞書を作り、マッチングさせることによりパスワードを導出していた。また我々がセ

キュリティは万全と思っている軍事施設、軍事産業のシステムが天才ハッカーに簡単に門を開いてしまったことは多くの示唆を含んでいる。

ストール氏は演壇を右に左に忙しく走りまわり、見事なパフォーマンスであっという間の3時間であった。アメリカで150万部のベストセラーとなった同氏の著書『カッコウはコンピュータに卵を産む』(原題『The cucoo's Egg』草思社刊) を是非一読されたい。ニューヨーク・タイムズ・ブックレビューはこの著書を「コンピュータ・ネットワーク社会への興味深い入門書」と評している。

分科会報告

【セキュリティ分科会報告 (1)】

日時： 平成3年8月5日 (月)
18：30～20：40

場所： (監) トーマツ 2階会議室

出席： 梅津、荒川、木村、川辺、金子 (記録)

研究／検討事項

1. 安全対策実施事業所 (PUC) 運用規程事例の研究／検討

規程名称： 『安全対策に関する規程』

討議内容

(1) 規程の位置づけ (第1条～第4条)

(2) 組織について (第5条)

企業組織と安全対策組織とは別、安全対策組織はゾーン (物理的区画) または部屋に分けられ、企業組織上そこに配置された管理職が安全対策の管理者としての任を担う。

(3) 安全対策管理者の種類

入退管理、巡回監視、外注管理、教育・訓練、電算機管理等

(4) 事業所の入退管理 (第6条～第8条)

(5) 電算機室の管理 (第9条～第12条)

2. 他社の事例

安全衛生巡視の規則 (高齢者のオペレータや成果品処理作業者の安全衛生を考慮し、用紙の床への直置禁止などの規則がある)

3. 感想

○ 労働衛生面も重要な取組課題であることを出席者全員が認識した。

【セキュリティ分科会報告 (2)】

日時： 平成3年9月5日 (火)
18：30～20：30

場所： (監) トーマツ 2階会議室

出席： 金子、川辺、荒川、木村、梅津 (記録)

審議検討事項

1. 木村氏から日系新聞の連載講座「電算機の安全対策」全17項のコピーが配られ、内容についての検討会が行われた。

・ 安全対策として4つ言われているが、普通は抑制策、防止策を一緒にして3つである。他の2つは検知策、回復策。

・ 安全対策費用は半分以上の企業がコンピュータ投資額の1％以下である。

・ リスク管理の場合の損失費用の算定方法について、発生確率と損失額の予測がある程度の妥当な数字に落ち着かせる方法をとるのが良い。

・ アメリカのADPガイドライン、オレンジブックについてその概要の説明があった。

・ パスワードを忘れる人が多い。生年月日、電話番号でも暗号化ルールを決めておけば良い (例えば、平方根)。

・ パスワードに関連して、最近多くなった管理者の承認印鑑をコンピュータで行う場合の留意点がいくつか議論された。毎回管理者が自分で立ち上げをすること、5分くらい短時間でもノンアクセスの場合

は自動的に回線オフにすること。

・各省庁の安全対策基準ができている。通産省、郵政省、自治省以外にも、運輸省は情報関係の倉庫業についての基準を作っている（ドキュメントビラ）。

・バックアップセンターは、建物のみのコールサイト、コンピュータが入ったホットサイト以外に、最近はソフト（パッケージソフト）まで対応するところができている。

以上の総評として、ユーザーの安全対策への認識はいまだに低い。低くても今ではそれほど問題ではなかったが、これだけコンピューターが普及してきて大丈夫ではなくなっている。企業経営者は横並びであればそれほど気にはしていないが、災害は周期的にやってくる。FISCも、通産も今年は安全基準の見直しをした。

1. 記録の一部は会報に記事として載せるため、会報担当へも今後は毎回送る。
1. 分科会の発表会に合わせ、年度活動報告をキチンとまとめておこうということで、今から、一応の準備をする事とし、具体策は次回にでも検討予定。

【事例研究会】

日　時：平成3年8月6日（火）
18：30～22：00

場　所：虎ノ門琴平会館2F
監査法人トーマツ会議室

出席者：横田・村上・小坂・大島・蓮見・藤森・会田・吉川・木村・渡辺・鈴木（実）・打矢・梅津・黒熊・荒川（記録）（順不同・敬称略）

議事内容

1. U社監査

①7月22日に実施した現地調査報告

・野村・梅津・渡辺・大島の各氏の調書（監査意見付き）が披露され、意見交換を行った。

監査項目と担当

・売掛金の入金照合と消し込み（担当野村）
・入力業務の効率性（担当大島）
・入金時の売り掛け残との照合（担当打矢）
・請求と入金処理（担当梅津）
・出力の活用・チェックの合理化（担当渡辺）

②U社に対する主な質問事項の取りまとめ

・出荷と売上計上のタイミング（電機・自動車）
・出荷と検収が合わないときはどうしているか
・債権の回収と売掛金との突き合わせが合わないときはどうしているか
・株式公開の予定はあるか
・製造原価はどのように算出しているか
・製造原価と販売単価との対応はどうか
・検収後の値引き・単価変更要求への対応はどのようにしているか
・パッケージソフトウェアの使用範囲はどこまでか。

③今後の予定

次回9月10日にU社より再度来ていただく。

2. 他の模擬監査について

①トモノ農薬

・8月31日（土）に訪問する。参加予定者は小坂・矢田・打矢の各氏。参加希望者は、打矢氏まで至急ご連絡下さい。
0473－55－2735

・事前に詳細な質問書の作成が必要→参

加者で詰める。

・依頼内容からみて経営者にインタビューする必要がある。
・依頼内容を絞りたい（打矢氏意見）

②その他依頼元についての意見

・テーマは絞るべきである。
・メンバーをABチームに分けてこなすようにしてはどうか。
・依頼元より来ていただくようにして原則として現地調査はしない。
・各依頼元とも一度は訪問の必要がある。

第14回　研究会開催さる

第14回研究会「SIS成功の急所」（第1回目）
－5月24日 18時30分～
於：日本ユニシス飯田橋東海ビル－

（講師）アーサーアンダーセン会計事務所
ビジネスシステムコンサルティンググループ責任者　勝本宗男氏

講師の勝本氏は「SISプロジェクト・リーダーを命ず」（日本経済新聞社発行）の著者でもある。私も一読していたためか、駆け足ぎみになった後半部分もついていけたようだ。

「SIS構築の鍵」として、信長の侵略と対比させて5つのキーワードを挙げ、非常にわかりやすく説明された。その中で、明確な経営戦略を示し具体的な実現方法を考えるのは経営トップの責任で行わなければならないという部分が印象に残った。SISの基本は、情報技術をいかに戦略的に活用するかということであり、システムを作ることが最終目的ではないことを再認識した。また、システムを開発する立場から見れば、開発段階のリスクを最小にする意味でも、試行的あるいは段階的アプローチが、今後ますます重要になると感じた。

「SISの開発方法」としては、孫子の五事七計を例にとり、これまた明快に説明された。孫子の五事とは道（理屈）、天（タイミング）、地（地のり）、将（指揮官）、法（軍律）のことであり、SIS開発の五事とは企業風土、日程、基盤システム、プロジェクトリーダー、開発方法論の5つを指す。経営トップがなるほどという場面が目に浮かびそうである。

「SISとシステム監査」では、PLAN－DO－SEEの各サイクルでシステム監査を実施する場合のチェックポイントとして、計画段階は結果よりもプロセスの監査が重要であり、開発・導入段階ではリスク最小かつ無駄のないことを監査する必要があることを指摘された。氏のようなシステムコンサルタントと外部監査は両立するのか、コンサルタントと外部監査人の顧客に対する基本的な立場の違いは何か、また、顧客はそれぞれに何を期待するのか、話を聞きながらそんなことを考えた。外部監査人には問題の指摘と改善提案を、システムインテグレータには問題の解決そのものを、コンサルタントには問題を指摘し解決するまでのコントロールを顧客は求めている、そんなふうに割り切って考えることはできないだろうか。

カラーイラスト付きOHP資料による雑談を交えながらの講演は、システムに詳しいとは限らない聞き手を話に引き込み、なるほどと思わせる。プレゼンテーション技法の勉強としてもためになる2時間であった。（No.158 会田三雄）

第14回研究会（再）開催さる

第14回研究会「SIS成功の急所」（第2回目）
－8月23日18時30分～
於：日本ユニシス　飯田橋東海ビル－
（講師）　前　出

SISの構築、SIの運営という事業会社のシステム担当者、ソフトウェアメーカー、ハードウェアベンダーが共通に抱えている（であろう）難問に対する、解決のヒントを与えてくれる講演だった。

講師は「SISのシス（死す？）」と言いつつも差別的優位性を実現するSISの構築は可能であるとし、その基本は心の意味でのSI（システムズ・インテグレーション）であるとする。つぎに、そのSIの実施・運営に当たっての重要事項、必要な能力、基本計画策定のプロセス等について明快で、説得力のある説明があった。

SISの構築に当たっては経営トップから現場の担当者までの理解と期待が必要で、現行の業務・システムの分析・評価を十分に行う必要がある。あまりに大きな業務・組織の改革を伴うようなシステム開発は、プロトタイプでの試行、サブシステムごとの段階的移行でリスクを軽減すべきである。等々のお話しは開発担当者として印象に残るものである。

SIについて筆者は「SI業者に丸投げすればユーザーのシステム部門はほとんど手がかからない」のが理想的ではないかと考えていたが、講師はこの考えかたは幻想であると否定し、ユーザー会社のシステム部門もかなりの役割分担を覚悟するべきであるとする。しかし今後講師の言うところのSOS（システム・アウト・ソーシング）が進めば、ますますSI業者への期待は膨らむことになるので、企画力、技術力、業務知識、コンサルティング能力等を備えるSEの養成・確保がSI業者にとって今以上に重要になるのではなかろうか。

「遅れているプロジェクトに人を投入するともっと遅れる」という話もあったがそうはいっても現実に遅れているプロジェクトへの対応といえばSEの追加投入が唯一の対応策というのが実情であり、それ以外にどのような処方せんがあるのか、講師の過去の経験等からの具体的なお話しが聞けなかったのが残念である。

戦略性の高いシステムを構築する際に企画段階で明確にしなければならないこと、やっておくべきこととして、システムズ・インテグレーターの5つの必須能力を合わせて具体的に明示された15の項目は、今後のシステムの企画開発に直ぐにも役に立つものであり、筆者をふくめてシステム開発の現場で働く者にとっては大変有益な講演であったと思う。

最後に、システム監査についてはアウトプットの監査ではなく、システムの処理プロセスをよく見ないといけないのではないか、とのご意見であり、その観点からは、システム監査、システム・コンサルティング、システムズ・インテグレーションを一貫性のあるひとつの流れのなかで考えることができるのではないかという印象を受けた。　（No.233 小坂　志郎）

第15回　研究会開催さる

第15回研究会「SISの考え方と実例」
－ 9月27日 18時30分～
於：虎ノ門第17森ビル
NTTデータ通信会議室　－
（講師）NTTデータ通信株式会社
SIS推進本部　副本部長　斉藤正弘氏

SIS（戦略情報システム）に対する関心は依然と高い。しかし、その内容は、「SISとは何か」から「SISをどのように構築するか」に変わってきているようである。本研究会においてもSISをテーマにした講演が続いており、題記の第15回

研究会にも多くの出席者があった。

最初に、首都圏市場調査の結果を参考に、SISの生まれた背景と狙いについてのお話があった。調査結果によると、「顧客要求複雑化への対応」を図るため、事業戦略として「差別化商品の創造」と「顧客・取引先の囲い込み」が重視されているとのことである。そして、その事業戦略遂行上の手段として、情報統合の重要性を強調された。多様化・個性化する顧客要求に対し、変化追随ではなく、変化先取りの対応をするためには、情報を如何に駆使するかがポイントとなる。そこで、組織内の情報流通活性化を図るための情報システムの基盤整備が重要なことは間違いない。

次ぎに紹介があったのは、NTTデータ株式会社のSIS構築技法SEP（Strategic System Evaluation and Planning）である。これは、事業戦略策定コンサルテーションと、人材育成プログラム、情報システム構築支援からなる。SISを組織内に導入するには、単に情報システムを構築するだけでなく、業務改善とともに、それを実践する人の意識改革が必要であり、その意味で、人材育成プログラムが含まれていることは興味深い。

最後に、事例研究として、「姫路市医師会医療情報システム」の紹介があった。患者・介護者の方々へのサービス向上を目的に、医師会・保健所等の連携のスピードアップを実現したシステムである。本事例のポイントは、情報技術を活用して、在宅ケアをはじめ新しい業務の仕組みを構築したことと考える。その仕掛けは、「電子メール+データベース」が中心とのことであり、既存パッケージを活用することにより、短期間で高品質のシステムを比較的安価に構築できたのではないかと想像できる。この面からも興味深いシステムであった。

（No.373 水野　康彦）

90年度システム監査試験論文優秀答案

会報14号で90年度のシステム監査試験の論文問題に対する会員の解答を募集したところ力作が集まった、ここに優秀答案として行武郁博氏（No.307）の答案（一部）を掲載する。91年度についても次号において問題を掲載し会員諸氏の解答を募集する予定であるので奮って応募願いたい。行武氏には協会より薄謝を進呈する。

問2

情報処理システムの企画開発業務の監査について

設問ア. 省略

設問イ. ユーザーニーズ調査の留意点

1. ユーザーニーズは経営目標に合致していること。

今や情報システムは企業の日常の経営及び経営戦略にとって不可欠なものとなっている。それだけにユーザーニーズは量的にも質的にも複雑多岐にわたってきている。バッグログは数年分をかかえているといわれている。従ってどのユーザーニーズが経営目的に合致しているか否かによるニーズの篩い分けが必要となっている。そのためにはシステム部門自身が経営目標を十分に理解し、そのうえにたってユーザーニーズを反映したシステム、さらにはユーザーニーズを高めたシステムを構築することが必要である。

2. 要求部門以外の関連部門まで含めた調査を行なっているか。

ユーザーニーズが経営目標に合致しているならばそのニーズが要求部門だけのものなのか他部門にも同様のニーズがあるのではないか等について全社的な立場から検討をくわえ他部門にまたがるものについては全社的なシステムを構築していることが必要である。そうしないと後日、同様のニーズが他部門からでた場合、システムの二重開発となる。

3. 調査の方法は適切であるか。

要求部門へは面接調査、関連部門へはアンケート調査といった対象に応じた調査方法が必要なのはいうまでもないがこれはいわば受身の調査であって特に情報系システムの構築にあたってはシステム部門からの積極的な姿勢が必要である。つまりユーザー部門の業務やニーズの内容について詳細に理解、習得しユーザー部門のニーズを明確にするとともにより高度なものとしてシステム構築に反映することである。さらにシステム構築の各工程においてもユーザー部門と適時に打合せを行なって常にニーズを把握していなければならない。

4. 他行状況は調査されているか。

地方銀行としては他の地方銀行の実施状況や今後の動向は勿論であるが、都市銀行にも注意しておく必要がある。都市銀行の先行事例は地方銀行にとって参考になるケースがあると思われる。

設問ウ　監査の方法

1. 中期計画書、短期計画書により経営目標を確認し、ユーザーニーズが合致していることを確認する。

まず中期計画書が作成されそれをうけて年度ごとに短期計画書が設定される。これにより経営目標がどこにあるのかを確認することができる。

2. 稟議書により承認されていることを確認する。

中期計画書、短期計画書に記載されているものであっても個々のシステム導入に当たっては稟議による承認が必要である。従って稟議書により承認を受けているか確認する。

3. ユーザーニーズは一部門のみであるか他部門も関連しているかを調査しているか。

ユーザーニーズが他部門に亙る場合、通常は稟議書に承認印が押されているのでこれにより関連部門の承認は確認できるがその他の関連部門に亘る要求であるのかどうかは判らな。システムの内容や打合せ議事録等によってユーザーニーズの範囲が正確であるかを確認しなければならない。

4. 調査の方法は適切であったか。

打合せ議事録、アンケート、調査結果資料等により確認する。場合によっては担当者と面接して確認する。

5. ユーザーニーズは開発中においても適時に調査されているか。

特に情報系システムにおいてはユーザーニーズの把握がむづかしくかつ当初は明確でない場合が多い。システム部とユーザー部門の共通の認識がない場合がある。ユーザー部門からみればなんでもないことがシステム的には多大の労力を要することであったり又逆の場合もある。このような認識の差を排除するにはお互いに知識を習得すること。度重なる打合せを行なうことによってお互いを理解することでありこれによりニーズが明確化され実現の道が見えてく

ると思われる。従って開発の途中においても適時に打合せが行なわれていることが必要である。

6. 基本設計書により他行状況について十分調査が行なわれているか。

企画業務としての調査結果は最終的には基本設計書に纏められている。従って基本設計書の他行状況の記述をみればシステム部がどれだけの調査活動を行なったかが判る。他の地方銀行や都市銀行の実施状況や今後の動向について可能な限りの調査がおこなわれたかを確認し、それが当該システムの決定と矛盾のないことを確認する。

「システム監査企業台帳」閲覧開始さる

「システム監査企業台帳」が平成3年9月に通産省より発行された。

「システム監査企業台帳」はシステム監査企業(44社)から提出された申告書を本に綴じた物で、一般に公開されるが、当分の間は閲覧のみで販売や配布はされないとのこと。

事務局からのお知らせ

<会費振込みのお願い>

本年度(平成3年1月1日～平成3年12月31日)の会費(正会員10,000円準会員8,000円)を未納の方は、下記宛にお振込みください。

郵便振替口座　東京　1－352357
加入者名　日本システム監査人協会事務局
銀行振込口座　第一勧業銀行　北沢支店
普通　1053488
口座人名　日本システム監査人協会
事務局　鈴木　信夫

会費振込に際しては、必ず会員番号をご記入願います。

<住所変更について>

住所変更、所属変更等がございましたら、事務局へ書面でお知らせください。

<会員の声募集について>

会員相互のコミュニケーションを図るため、『会員の声』を募集します。また、会報についてのご意見、ご要望もお寄せください。

この件については、会報担当宛に郵便、またはFAXでお送り下さい。

<合格者の連絡先調査のお願い>

1月末日に昨年10月に実施された第5回システム監査技術者試験の合格者が発表になりました。ついては、会員の周辺で、合格者を発見(?)した時は、事務局まで至急FAX(03－3415－1388)でご連絡ください。事務局より折り返し、入会申込書を発送いたします。

発行所　日本システム監査人協会
発行人　川野　佳範
事務局
〒157 東京都世田谷区砧1－10－11
NHK放送研修センター内鈴木信夫
TEL. 03(3415)7111(内2631) FAX. 03(3415)1388
※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)
長野　正己　東京海上火災保険㈱財務企画部
TEL. 03(3212)6222 FAX. 03(3211)2430
小松原　拓　富士通㈱教育部
TEL. 03(3735)1111 FAX. 03(3730)1389
今井　純子　公認会計士今井純子事務所
TEL. 03(3992)9381 FAX. 03(3992)2450
波田　直登 NTTデータ通信㈱
TEL. 03(3847)8996 FAX. 03(3847)8999