特定非営利活動法人
日本システム監査人協会報

2014 年 10 月号
No 163

No. 163（2014 年 10 月号）＜9 月 25 日発行＞

今月号も投稿、報告記事
満載です。読書の秋に
会報で新たな発見を!!

紅葉　写真提供：中山孝明 副会長

巻頭言

テーマ：システム監査のいい話

会員番号 1143　中山 孝明（副会長）

システム監査に関することで良かったこと、嬉しかったなど、“いい話”は沢山あります。

現状や目標達成の課題が明確になった、システム監査人になって良かった、担当している仕事に役立ったなど。今回は、システム監査に関心や興味のある方や、情報システムを活用している方々のご参考に、“資格取得のいい話”を採りあげます。

「システム監査技術者試験」に合格すると、周りの人たちからちょっと違った目で見られたりします。“すごい”と。IT関係者はこの資格をよく知っていますし、難関資格などと言われたりもするので、大げさでなくリスペクトの視線を感じることも多いようです。

システム監査は自分には関係無いなどと、敬遠されたり聞き流されたりしますが、システム監査の知識や手法はIT担当だけでなく多方面の職種に生かせることが知られています。同試験には年間 4～5 千人が応募していますが、その勉強を通じて今すぐ自分の仕事に役立つことや、適用できる職種が多いことに気付いています。システム監査の視点を持って目から鱗が落ちたとか発言が注目されたとか、このような声を資格取得者から良く聞きます。繰り返しますが、情報システムの利用側の多くの方々にも当てはまります。今や、あらゆる仕事が情報システムによって成り立っていることからも当然のことでしょう。

このような観点や経緯から、システム監査に注目しその重要性認識を高めて、システム監査人を目指すキャリア形成も少なくありません。同試験は 1986 年の登場です。システム監査人は、既に欧米で見られるように我が国でも専門職として確立し、変貌激しい情報化社会のより健全な発展に、その役割・期待が益々高まっていくのではないでしょうか。“いい話”の続きは別の機会にまた触れたいと思います。

＜目次＞

2014.09

めだか　【　次世代のためのシステム監査　】

「だますやつが悪い。」のか、「だまされるほうが悪い。」のか。それはシステム監査人にとって頭の痛い問題である。フランシス・フクヤマは、著書「信なくば立たず」(Trust)で、歴史によって伝統的に信頼関係が形成されやすい地域とそうでない地域があるとしている。個人を取り巻く社会は、家族、中間組織(会社、宗教、地域コミュニティ、学校)、国の、3つの信頼の輪によって成り立っている。信頼関係の第一の輪は、家族である。信頼関係の輪が中間組織から国まで広がる信頼関係が形成されやすい地域では、ビジネスは円滑に行われる。例えば、納品請求書を送付すると相手は納品を確認し銀行振込で支払う商習慣があればビジネスは円滑に進む。しかし、信頼関係の低い地域では、いちいち集金に行くと支払う、また、銀行振込は入金を国が補足するため普及しないと聞いたことがある。

「中国の大問題」という本を読むと、チャイナ・リスクとして、“ビジネス習慣や文化の違いから、「中国でのビジネスは難しい」との嘆きをよく聞く。日本と中国で文化が違うのは確かである。”と書いている。また、“中国人は実利を優先することが多い。たとえば価格が100円の品物があるとする。日本人なら、せいぜい売値を150円ぐらいに設定するだろう。中国人なら10倍にふっかけて1000円という。・・・　日本人は元の価格がバレたら信用をなくすと考えるが、中国人は、利益は信用から得るものではないと考えている。だまされるほうが悪いという発想である。” という。以前に読んだ司馬遼太郎さんの本で、大阪では中国人との商取引の影響か、買い手は値札を見て、「台を下ろせ。= 一桁さげろ。」と言って値引きを始めると書いていた記憶がある。買い手は100円と1000円の中間の値段を探るわけである。もちろん、100円に近いほうから。ただし今は大阪でもそんなめんどうな売買は少ないと思う。

信頼関係が、家族、血族だけというのは、いかにも世間が狭くて生き難い。そこで、三国志で有名な、劉備、関羽、張飛の桃園の誓いにあるような義兄弟が朋友関係となる。再び「中国の大問題」という本を引用すると、“「自分で利益を独り占めするのではなく、中国人といっしょに仕事をすることだ。おいしいものを全部自分で食べようとするとお腹を壊す。中国人といっしょに事業を起こせば、彼らも自分の会社を攻撃することはないだろう。」” と論している。同じような考え方からと思うが私の台湾の先輩は、他人でも同じ姓の若い者へ奨学金を出し、また、LIONS CLUBの仲間と社会に貢献している。

「デフレの正体　ー経済は「人口の波」で動く 」という本では、これから、日本は、欧州の国々のようにブランド戦略をとり、高級なモノづくりやサービスを創出することが国の生残りに必要で、中国や韓国の人たちは得意先であるので大事にしないといけない旨、書いている。また、「中国の大問題」 でも、“相手とつきあうときに留意すべきは、まず相手をだまさないことである。対等につきあって信頼できる関係を築く。それは経済にかぎらず政治の世界も同様である。” と結んでいる。次世代のためのシステム監査を考えると、システム監査人はこのように「信頼」を大事にすることが大切であると思う。

(空心菜)

参考1:「中国の大問題」 丹羽宇一郎　PHP新書931

参考2:「デフレの正体　ー経済は「人口の波」で動く 」 藻谷浩介　角川oneテーマ21　C-188

(このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。)

＜目次＞

2014.09

めだか　【提案：次世代のため５%の時間を割こう！】

システム監査に限りませんが、研究会やセミナーに出ると、その主催団体の構成員像がなんとなく浮かび上がります。新技術に絡むフォーラムだと、会社から派遣されている参加者もいるせいか、若手の参加も多く、運営側もまだ熟達していない印象を抱きます。

これに対し、システム監査関連の会合だと、もちろん現役バリバリの参加者もいますが、多くの場合、セミリタイア世代、といったら失礼だと思いますが、中堅というよりシニアが多く、経験豊富で落ち着いた印象を与えます。自分は最初の会社で一通りのことは吸収してきた、これからはキャリアを活かして活躍したい、そういった方が多いのではないでしょうか。

このことは、シニア世代がシステム監査の担い手の中心になっていることを意味するかもしれません。発達理論からいえば、一般にシニア世代、準シニア世代は、経験知に優れているけれども、環境変化を先取りして、道を拓こう、という新種の気質には必ずしも恵まれていないように感じます。

しかし新たな担い手が増えていかなければ、システム監査の業務やビジネス基盤も次第に尻すぼみになりかねませんし、そのためには中核的な担い手として、常に新しい技術を吸収し、業務に適用するだけではなく、次世代の担い手たちの活躍の場を広げる努力をしなければなりません。

喩えて言えば、休日の公共施設が朝早くから、シニア世代の催し物で目一杯になり、若い世代が入る余地がない、そうした状況を招くことはぜひとも避けなくてはなりません。

システム監査もビジネスですから、商機があれば積極的に業務を受注し、顧客の期待に応えることは当然と言えます。しかし一方で、次世代の担い手に、自分のノウハウや経験をどう伝えるかにも、もっと腐心する必要があります。

当方は年来、本当のリタイア世代に向けて「時間長者」としての行動原理の確立を訴えています。これは、もちろん一定の生活水準が維持できる前提ではありますが、生活の質を形成するうえで「時間のゆとり」があることは本当の豊かさにつながるのではないか、という主張です。そのうえで、リタイア世代は金銭面での余裕度は様々であるにしても、時間長者である可能性は高いし、高齢化が進めば、一段と時間長者が増えていきます。

こうした時間長者が既得権を独り占めするのではなく、自分の時間（できれば金銭面も）の5%でよいから、次世代の支援に使ってはどうか、という提案です。

これを次世代のためのシステム監査、に当てはめれば、自分のビジネスや業務時間の5%は必ず次世代のために使う、そうした意識が必要ではないか、という主張になります。

ぜひ会員の皆様も、厳しい時間繰りの中から5%は次世代のために提供する、そんな取り組みを考えてみられてはいかがでしょうか。

（拡張子）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

＜目次＞

2014.09

投稿　【　次世代のためのシステム監査　】

会員番号　0557　仲　厚吉　（会長）

この世の中に「誤謬の無いもの」は無い。だから、情報システムには、ITガバナンスと、PDCAサイクルのCheck局面でシステム監査が必要になります。公共機関等の情報システムは、誤謬が発生した場合、多くの人に大きな悪影響を与えます。また、公共機関等の情報システムのうち個人情報を取り扱う情報システムは、個人情報の漏えい、滅失、き損が発生すると取り返しがつかなくなるおそれがあります。

私がシステム監査技術者になったころは、情報システムと言えばメインフレームによる情報処理の時代で、PCが普及しはじめエンドユーザ・コンピューティングが新しい課題でした。昨今、情報システムは、様々なシステムの中に組み込まれ生活の中で例えて言えば空気のような存在になっています。8月の月例研究会は、講師に一般財団法人日本情報経済社会推進協会（JIPDEC）電子情報利活用研究部部長　坂下哲也氏、テーマを「特定個人情報保護評価指針について　－　マイナンバーにおけるPIA実施の対策と課題等　－　」として講演頂きました。PIA（プライバシー影響評価）は、事務単位に実施されます。事務処理には情報システムが利用されるため、マイナンバーにかかわる事務システムにシステム監査が求められ、システム監査人の活躍が期待されています。

9月の月例研究会は、講師に東京海上日動リスクコンサルティング株式会社上席主席研究員　指田朝久氏、テーマを「首都直下地震の被害想定の警告　～　情報システムのバックアップは本当に機能するか～　」として講演頂きます。講演骨子は、“2013年末に公表された政府の首都直下地震の被害想定は、東日本大震災を踏まえて前回2005年に公表された想定を大きく変えている。しかしながらその被害想定の内容はあまり認識されていない。本セミナーでは今回公表された被害想定を解説し、企業はどのように対応すればよいかについて提言する。このように書くとありふれた内容に思われるかもしれないが、政府は首都直下地震につきかなり踏み込んだ被害想定を行ったことを理解していただきたい。政府は今回はじめて具体的なライフラインの途絶時間を公表した。その内容をみると情報システムの稼働に大きな影響を与える電力の被害想定が大幅に悪化したことがわかる。また通勤困難、飲食料入手困難さらに非常用発電機に不可欠な燃料の調達困難などがあり、これらを含め政府は過酷事象も想定外としないように求めている。それを踏まえると首都圏における経済活動が困難であり、企業はこれらを正しく踏まえたBCPを構築することが必要である。”　というものです。

2014年9月6日の朝日新聞「私の視点」に、元京都地検検事正・元内閣法制局参事官、古川元晴氏の「福島第一原発事故　国民が納得する再捜査を」　という記事があります。その中で、“過失を罪に問う場合、刑事法学には「具体的予見可能性説」と「危惧感説」という二つの考え方がある。前者は危険を具体的、確実に予測できることを必要とし、後者は高度の注意義務が課せられている事業者については、不確実であっても合理的・科学的に危険が危惧される程度で罪に問えるとする。”と書いています。公共機関等は、高度の注意義務が課せられている事業者です。それらの事業者は、情報システムにおいて、誤謬の発生をできるかぎり少なくするため、ITガバナンスと、PDCAサイクルのCheck局面でシステム監査が求められると認識する必要があります。当協会は、公共機関等の事業者へ、ITガバナンスと情報システムへのシステム監査の必要性を訴えていきます。

以上

＜目次＞

2014.09

第１９３回　月例研究会　（２０１４年７月開催）

会員番号 25069　野嶽俊一　（情報セキュリティ監査研究会）

【講演テーマ】「最近のサイバー攻撃と対策の解説」

【講師】独立行政法人 情報処理推進機構（IPA） 技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー
主任研究員 渡辺 貴仁 氏

【日時】2014 年 7 月 22 日（木曜日）18:30～20:30

【場所】機械振興会館 地下 2 階ホール

【講演骨子】:講演者より

オンラインバンキングにおける不正送金の被害が増加傾向にあり、警察庁によれば 2014 年の国内における被害額は、5 月 9 日の時点で 14 億円を超え、過去最大であった昨年の被害総額を既に超えたとあります。また多くのオンラインサービスサイトで第三者にログインされ、情報の不正取得やなりすましの被害が発生しています。

さらにホスティング事業者が攻撃を受け、そのサービスを利用しているウェブサイトが改ざんされ、エンドユーザにウイルスを感染させる事例が発生しております。

この様なサイバー攻撃を紹介するとともに、対策について解説をします。

【講演概要】

IPA が毎年発行している「10 大脅威」の 2014 年版を中心に、情報セキュリティに関する注目すべき脅威や懸念とその対策について紹介された(参考資料の URL は、文末にまとめて記載する)。

Ⅰ. 10 大脅威について

独立行政法人 情報処理推進機構（以下、IPA）では、2004 年から、毎年、「情報セキュリティ 10 大脅威」を発行している（資料1）。2014 年版は、「10 大脅威執筆者会」117 人のメンバーの投票により決定した。「情報セキュリティ 10 大脅威」の構成は、「1章：セキュリティ驚異の分類と傾向」、「2章：2014 年版 10 大脅威」、「3章：注目すべき脅威や懸念」となっている。

以下、この章建てにしたがって説明する。

1章　セキュリティ脅威の傾向と分析

近年、スマホやSNSといったIT機器やIT環境が年齢、社会階層を問わず急速に普及し、セキュリティ脅威が、あらゆる層に広がっている。また、ウイルス・ハッキングの国際問題化やIT 詐欺の横行といったように脅威の内容が変化し、より深刻化している。

国際政治・安全保障の分野が新たな問題として挙がってきた。「サイバー領域問題」と言われるもので、軍事的妨害活動、国家機密の窃取、社会インフラの破壊といったことが、現実化している。米国政府は、「第5の空間」として陸・海・空・宇宙の既存の4領域に加えてサイバー空間を新たな国防上の領域として捉えている。先の米中首脳会談においても本件がテーマとなったが、お互いのけん制で終わってしまった。これについては、国際的な共通のルール作りが求められている。

パソコンへのウイルス感染、サーバへの不正アクセスが広がり、ウイルス・ハッキングを用いたサイバー犯罪やインターネットを使った詐欺・犯罪行為が増加している。また、金銭を狙って攻撃者は組織化し、年々被害規模が拡大している。インターネット上でも、架空請求詐欺、偽者による成りすましや、偽物の販売行為等の詐欺行為が横行している。

一方、2000 年代前半から、日本国内でも内部統制やセキュリティマネジメントの体制の確立が浸透し、情報資産(データやシステム)の事故(漏えい、改ざん、消失、システム停止)の抑止に重要な役割を果たしている。

インターネット人口が増大するなか、インターネットを使う側のモラル(エチケットやリテラシー)、すなわち、インターネットモラルの問題が浮上してきた。誹謗中傷やいじめ、SNSによる本人の意図せぬ情報公開等が頻発している。現実社会と同様、法律遵守やモラルを意識した利用が必要である。

2章 2014 年版 10 大脅威

10大脅威について、順位にしたがって説明する。

《 1位 》 標的型メールを用いた組織へのスパイ・諜報活動

攻撃が見え難く容易に気づかない、メールやウェブを介して遠隔から侵入できるといった性質が悪用され攻撃に使われる。ターゲットは官公庁だけではなく、最近では民間企業も狙われている。手口としてはセキュリティの弱いところ(中小企業等)から狙われ、最終的に大企業等の機密情報が窃取される。外交問題に発展しており、2013 年7月に開催された「米中戦略経済対話」では、米国から中国に「サイバー攻撃による窃盗行為を止めるよう」強い要請が行われた(「Ⅱ」で詳述)。

《 2位 》 不正ログイン・不正利用

ウェブサービスへのハッキング、推測可能なパスワードの使用、利用者による ID/パスワードの使い回し等が原因で、ウェブサービスやシステムに不正にログインされる。とくに ID を「メールアドレス」として設定しているサイトは、そこが攻撃を受けたらパスワードリスト攻撃により他のサイトでも影響を受ける恐れがあり、要注意である。

クレジットカード会社やショッピングサイトなど幅広く狙われている。

2013 年の統計では、多くの不正ログイン成立率は0%台と低いものの、成功件数は相当数に上る。試行件数の0.15%にあたる 23,926 件が不正ログインに成功した事例がある。

不正ログイン、不正利用対策としては、長く複雑なパスワードの設定、パスワードの使いまわしの禁止、パスワード以外の認証方式、たとえば、ワンタイムパスワードや認証トークンの利用、2要素認証等を用いることが考えられる。

《 3位 》 ウェブサイトの改ざん

ウェブサイトの改ざんは、管理者端末が狙われる。FTPやSSH等、管理者用サービスから侵入し、管理者権限を奪い、コンテンツ管理システム(CMS)などの汎用的なソフトウェアを狙う。また、ウェブアプリケーションの脆弱性も狙われている。2013 年度のJPCERT/CC が 2013 年に受け付けた国内外で発生したウェブサイトの改ざん件数は、7,409 件、1 日平均 20 件にものぼる。SQLインジェクションの脆弱性を攻撃されウェブサイト改ざんとなった例もある。また、国内レンタルサーバ企業が管理する 8,438 サイト(そのレンタルサーバを使用する企業のサイト)が改ざんされる事件もあった。

《 4位 》 ウェブサービスからのユーザー情報の漏えい

インターネットは、生活に必要不可欠な存在になっている。とくにインターネットによる会員制サービスは、クレジットカード情報等の大量の個人情報を保持しており、格好のターゲットになっている。会員制サービスの眼鏡販売サイトのミドルウェア Apache Struts2 の脆弱性を悪用され、2059 件のクレジットカード情報が漏えいした事故がある。また、ネットスーパーのサイトで、最大 15 万 165 件のクレジットカード情報が不正に閲覧された可能性がある事件が発生した。さらに、ネット検索大手企業が、内部のパソコンが標的型攻撃を受け、最大 148.6 万件の情報漏えいの可能性が

あると発表した。

Apache Struts2、OpenSSL、Internet Explorer 等でウェブサービスを直撃する脆弱性が立て続けに露見した。また、2015 年 7 月に Windows Server 2003 のサポートが終了する。

ウェブサーバからのユーザー情報の漏えいを防ぐ対策は、ネットワークアクセス制御の強化、セキュアなサーバの設定、アカウント・パスワードの管理強化、OS・ソフトウェアの定期更新及びウェブアプリケーションの脆弱性の診断の実施等がある。また、外部からの侵入はもちろん、内部からも侵入されない対策を打つ必要がある。さらに、ネットワークやサーバを常時監視する必要がある。

《 5位 》 オンラインバンキングからの不正送金

2013 年、オンラインバンキングの不正送金の被害額が過去最大になった。これらは、フィッシング詐欺やウイルスにより窃取された認証情報を使って、本人に成りすまして不正送金を行うものである(「Ⅲ」で詳述)。

《 6位 》 悪意あるスマートフォンアプリ

スマートフォンをターゲットとしたマルウェアがこの1年で 614%も増加し、窃取された個人情報は、スパム送信や不正請求詐欺などに悪用されている。

このような状況に至った背景は、自由にアプリをインストールできるスマートフォンの急速な普及にある。これを利用してマルウェアが電話帳を盗み取るといった事件が頻発している。偽「ウイルス対策ソフト」を 81 万人がダウロードし、3,700 万人分の電話帳データが抜き取られる事件が起こった。この電話帳データをもとに、攻撃者が運営するサイトへメールで誘導し、攻撃者は約 3 億 8,900 万を売り上げた。

この被害を防ぐために、以下の対策をとる必要がある。

・スマートフォンのOSとアプリは常に最新の状態に
・アプリは信頼できる場所から、ユーザーレビュー/評価を確認してインストール
・Android 端末では、「提供元不明のアプリ」はインストールしない設定に
・Android 端末では、アプリをインストールする際にアクセス許可を確認
・セキュリティ対策ソフトを利用

《 7位 》 SNS への軽率な情報公開

自己表現やコミュニケーションのツールとして、ブログやSNS(ソーシャルネットワーキングサービス)の利用が増大している。一方で、従業員の投稿が原因で、企業・組織が損害を受ける事件、いわゆる「バカッター」が社会問題になっている。また、官僚が、Twitter やブログで不適切な発言をして停職処分を受ける事件も起こっている。

対策として、まずは、個人ユーザーのモラル向上、また、企業・組織では、不適切な投稿が損害を招く可能性を周知させる等の教育の実施、SNS利用ポリシーの規定等が必要である。

《 8位 》 紛失や設定不備による情報漏えい

ノートパソコンやUSBメモリなどの紛失による事故は後を絶たない。スマートフォンやクラウドサービスにより、情報漏えいを引き起こすリスクが拡大している。また、オフィス機器の設定不備が原因の情報漏えいも発生している。2013 年 7 月に、誤った設定によりクラウドサービス Google グループで情報公開をしていた情報が、誰でも閲覧できる状態になる事件が起こった。また、2013 年 11 月に、インターネットからアクセス可能になっている複合機の存在が明らかになった。

これらを防ぐために、以下の対策をとる必要がある。

・パソコンや電子媒体の外部への持ち出しをルール化し、さらに、ファイルを暗号化するなどのシステム的な対策をとる。

・個人が組織に持ち込む機器(BYOD)に対し、組織としてのポリシーを確立して徹底する。

・利用するサービスの仕様を理解し、適切な設定や運用を定める。

・アカウント及びアクセス権限を管理し、利用するユーザーを適切に制限する。

《 9位 》 ウイルスを使った詐欺・恐喝

パソコンをロックして身代金を要求するランサムウェアの被害が増加している。この被害に遭うとデータにアクセスできなくなり、業務や個人的趣味のデータが消失する。ファイルを暗号化するランサムウェア CryptoLocker の感染が拡大し、2013 年 10 月には前月比 3 倍を記録している。この攻撃では、ファイル復号鍵とツールを高額(日本円で約 300 万円)で売りつける。ウイルス対策ソフトの導入、Windows Update の実施等のOS・ソフトウェアの定常的な最新化、及び、データのバックアップを取得する等の対策が必要である。

《 10位 》 サービス妨害

サービス妨害とは、ウイルスによりシステムが破壊され、サービスや業務が停止状態になることをいう。パソコンやサーバが分散型サービス妨害(DDoS)攻撃の踏み台にされ、攻撃に加担してしまう事態も増加している。この問題が深刻化している背景には、ITの普及と依存度が日増しに拡大していることがある。

2013 年 3 月 20 日に、韓国の複数の企業の数万台のパソコンがマルウェアの攻撃により突如停止し、起動できない事態が発生し、業務に甚大な影響がでた。また、米国では、100Gbps のトラフィックが絶え間なく 9 時間継続するという史上最大の DDoS 攻撃があった。

セキュアなサーバの設定、DDoS 攻撃の特徴がある特定の通信をネットワーク機器などでブロックする等の通信制御、ウイルス対策ソフトの導入、OS・ソフトウェアの定常的な最新化等の対策をとる必要がある。

3章　注目すべき脅威や懸念

最近、新たに出てきた脅威や懸念を説明する。

(1)ネットワーク接続機器の増加

複合機、ウェブカメラ、ネットワーク対応ハードディスク、テレビなど、ウェブインターフェースにより設定・管理できるオフィス機器や家電機器が増加している。その一方で、機器の不適切な設定により、機器をインターネット接続することで世界中の誰でもアクセスできる状態になり、情報漏えいや機器の乗っ取りなどの被害が発生している。複合機がインターネットからアクセス可能な状態になった事件や、攻撃者が、インターネットから乳児見守り用機器を介して、赤ん坊に罵声を浴びせる事件などが発生している。

これらの事件は、ユーザー側が仕様を十分に理解していない、機器がインターネットに公開されることに気がついていない、オフィス機器についてはシステム管理部門ではなく総務系の部門が管理をしている等のユーザー側の認識不足が原因で発生している。機器の管理者は、機器に付属している説明書をよく読み、適切な設定を施す、必要がない限り機器をインターネットに接続しない、といった対策をとる必要がある。また、ネットワーク管理者は、ファイアウォールやブロードバンドルーターで、インターネットから機器への通信を制限するといった対策をとる必要がある。

(2)エンドポイントセキュリティの重要性

前述の１０大脅威は、パソコン等のエンドポイントへの攻撃が主流である。Oracle Java(JRE)、Adobe Acrobat/Adobe Reader、Adobe Flash Player、Microsoft Office など、パソコンを利用する上で欠かせない製品の脆弱性が悪用されている。新しいソフトウェアほどセキュリティ機能が強固である。たとえば、Windows XP は 11.3%のウイルス感染率であるが、Windows 7(32bit)は 4.8%に減少している。最新バージョンの使用がセキュリティ対策の近道である。

(3)インターネット利用者の低年齢化に伴う問題

未成年者がインターネットで犯罪に巻き込まれるケースが増えている。また、IT犯罪を起こした未成年者が逮捕・補導されるケースも増えている。携帯電話・スマートフォンを使用する小学生・中学生が増加し、オンラインゲームや学習教材、コミュニケーションツール等のコンテンツが充実し、年々利用開始年齢が低下していることが原因の一つである。

インターネットは利便性が高い反面、偽名でも利用可能であり、悪用や誹謗中傷に使われやすい。出会い系サイトでの被害者は、2013 年上半期だけで74名にも上る。子どもがゲームのアイテムを購入し、保護者が高額な請求をされる事件が増加している。国民生活センターへの相談件数が、2013 年は 3,000 件を超えた。一方で、同級生のID/パスワードを使って不正アクセスした 12 歳の児童が補導される事件も発生している。

幼少期や中高生にも教育や対策を行うことが必要である。

Ⅱ. 標的型サイバー攻撃の仕組みと対策

攻撃者は長い時間、場合によっては１年以上の時間をかけてターゲット攻撃に向けた事前調査を行う。標的のSNS等の活動の情報等により身辺を調査し、攻撃者を信じ込ませるメールを送信する。メールは、標的の興味を引かせる内容であり、標的に添付ファイルを開くことを促す。そしてそこには、Adobe Flash Player 等の脆弱性を突くマルウェアが仕込まれている。

このようなエンドポイントへの攻撃には、現在のネットワークセキュリティの仕組みでは対応が難しい。なぜなら、現在の仕組みは、外から内への侵入に備える境界防御の概念でできているからである。たとえば、FireWall は、許可された通信のみ通過させるが、通信の内容は関知しない。IDS(IPS)は、攻撃を行う通信を検知するが、未知の攻撃の阻止は難しい。Anti-Virus は、マルウェアの侵入を阻止するが、見逃す可能性がある。

一般的な対策としては、脆弱性対策としてのエンドポイントやサーバ機器等へのセキュリティパッチの適用、不審メールを開かない等の啓発活動やUSB媒体の持込み禁止等のルールによる制限がある。しかし、これらには、業務に支障をきたし、ルールの完全な遵守の困難性など、問題がある。

そこで、従来の入口対策に加え、出口対策を施し、入口と出口でセキュリティ対策を二重にする方式をご紹介する。

入口対策は従来の対策であり、前述の弱点があり、侵入を許してしまう可能性がある。出口対策は、たとえ侵入を許しても出口を押さえることにより、組織への影響を回避しようというものである。

一つは、バックドア通信の検知と抑止である。プロキシサーバと FireWall の設定により、出口側に正常な通信の流れを作り、ルール外の通信を試みるマルウェアの検知と遮断を行う。二つ目は、組織内への感染予防策としてVLANを構築し、VLAN 間の通信を制限し、マルウェアの偵察行為を阻止しようというものである。VLAN の通信を監視し、感染発覚時には VLAN を切り離す。三つ目は、早期発見のためのログの監視である。

詳しくは、IPAが発行した、「『標的型メール攻撃』対策に向けたシステム設計ガイド」(資料2)をご参照願いたい。

Ⅲ. ネットバンキングの不正送金

1. 被害状況

警察庁の発表によると、インターネットバンキングの不正送金は、国内で被害件数 873 件、被害額は 14 億 1700 万円を超え、過去最悪だった 2013 年の被害額を、2014 年 5 月時点で上回ってしまった。1 件当たりの平均被害額は、昨年が約 107 万円だったのに対して、今年は約 162 万円と 52%増になっている。また、被害にあった金融機関も拡大傾向にあり、昨年の32行から今年は 58 行に増えている。金融機関の規模も変化しており、都市銀行から地方銀行へ、地方銀行から信用金庫・信用組合に拡大している。また、法人口座の被害が目立っている。5 月 9 日現在、全体で 100 件、4 億 1500 万円の被害があったが、このうち法人口座は、69 件、3 億 7700 万円である。法人口座が狙われる理由は、取引額に上限額が無いことが多いためと考えられる。利用者の居住区も鳥取県を除いて、全国に拡大している。

フィッシング詐欺の基本的な手口は、攻撃者が偽メールをターゲットになる利用者に送り、利用者にメール本文中のフィッシングサイトのリンクをクリックさせ、ログインに必要なアカウント情報を入力させるものである。ウイルスによる情報窃取の手口もある。乱数表（第二暗証）を使った銀行の本人認証を悪用する事例もある。メールによって配信されるワンタイムパスワード情報を、ウイルスを使って盗む手口もある。後の二つはセキュリティ強化機能を悪用したものである。また、最近、ウイルスを使って自動送金する新手の手口が現れた。

ウイルスの感染経路は、標的型メールによるもの、ウェブページ経由、可搬型媒体(USBメモリ)経由、偽造プログラム(偽ウイルス対策ソフト)等、さまざまである。ウイルスを感染させる手口も大掛かりで巧妙なものになってきている。

ネットワークバンキングの不正送金対策は、以下のセキュリティ対策の基本を守ることである。まずは、ウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新に保つこと。有害サイトのブロック機能やパーソナルファイアウォール機能が使える統合型セキュリティソフトがお勧めである。また、OS(Windows など)、その他のソフト全てを最新にし、こまめにアップデートして、脆弱性を解消することである。

なお、IPA では、導入されているソフトが最新か否かをチェックする「MyJVN バージョンチェッカ」というサービスを用意しているので、ご利用されたい(資料3)。

企業においては、以下の不正送金対策をとることをお勧めする。

・インターネットバンキング取引専用のパソコンの導入

専用機を導入することにより、ウイルス感染のリスクを低減する。専用機では、ウイルスによる被害を防止するためにウェブの閲覧やメールの利用をせず、ウイルス対策ソフトを最新の状態にし、可能な限り脆弱性を解消しておく。専用機を設置するネットワークも専用のセグメントにすれば、他のパソコンからの感染のリスクを下げられる。

・電子証明書のエクスポート禁止

法人向けネットバンキングでは、標準的な認証としてパスワードと電子証明書による2要素認証を採用している。マルウェアは、電子証明書と秘密鍵をエクスポートし、攻撃者サーバへ送信するので、電子証明書は「エクスポート不可」と設定し、「秘密キーの保護」を「中または高」に設定する。なお、電子証明書は、あらかじめバックアップし、オフラインで保存しておく。

今後も攻撃者側と利用者側との攻防は続いていく。情報収集と積極的な対策が必要である。

【参考資料】

資料1：IPA、「2014 年版 情報セキュリティ 10 大脅威」、2014 年 3 月 31 日公表
https://www.ipa.go.jp/files/000037151.pdf

資料2：IPA、「『標的型メール攻撃』対策に向けたシステム設計ガイド」、2013 年 8 月 29 日公表
https://www.ipa.go.jp/files/000033897.pdf

資料3：IPA、「MyJVN バージョンチェッカ」
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

以上

＜目次＞

2014.09

【ＩＤ連携トラストフレームワークの実証事業ご紹介 ー 情報セキュリティ監査研究会だより No.18 ー】（連載）

会員番号 0056　藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会では、アン・カブキアン著、「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを、2013年8月から議論しております。

この情報セキュリティ監査研究会だよりでは、会報5月号から7月号まで、プライバシー・バイ・デザインの一実現形態であるID連携トラストフレームワークのご紹介をしてきました。8月号、9月号は、別のトピックスをご紹介いたしましたが、今回から元に戻って、ID連携トラストフレームの実証事業をご紹介したいと思います。

ご紹介するのは、経済産業省が平成25年度に実施した、「『ID連携トラストフレームワーク』の構築のための実証事業」(資料1)のなかのユースケース、「保証書管理サービス」です。今回は、ID連携トラストフレームワーク自体の解説は掲載いたしませんので、必要に応じて会報のバックナンバー5月号(158号)～7月号(160号)をご参照願います。なお、会報は、日本システム監査人協会のホームページからPDF形式でダウンロードできます(URL1)。

本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、我々の力不足のため、誤りも多々あるかと存じます。お気づきの点がございましたら適宜ご指摘いただきたいと存じます。ご興味のある方は、毎月20日前後に定例研究会を開催しておりますので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。

security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

【参考資料等】

＜テキスト＞

堀部政男／一般財団法人日本情報経済社会推進協会(JIPDEC、以下、同じ)編、アン・カブキアン著、JIPDEC 訳「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」、2012年10月、日経BP社

＜資料１＞平成25年度電子経済産業省構築事業、「ID連携トラストフレームワーク」の構築のための実証事業報告書、2014年3月、JIPDEC
http://www.meti.go.jp/policy/it_policy/id_renkei/houkokusyo.pdf

＜ＵＲＬ１＞日本システム監査人協会会報公開ウェブページ
http://www.saaj.or.jp/members/kaihou_dl.html

【報告】「平成 25 年度経済産業省『ＩＤ連携トラストフレームワーク』の構築のための実証事業におけるユースケース『保証書管理サービス』ご紹介」

経済産業省は、平成 25 年度電子経済産業省構築事業の一環として、「『ID連携トラストフレームワーク』の構築のための実証事業」を行い、2014 年 3 月に報告書を公開した(資料 1)。今回は、この報告書のなかの「第 5 章　ユースケースの具体化によるID連携トラストフレームワークの有効性、実用性の検証」(資料 1 pp108-152)をとりあげる。この章では、ID連携トラストフレームワークのユースケースを具体化し、実証実験を行い、ID 連携トラストフレームワークの有効性及び実用性を評価している。以下、ユースケースの概要、実証実験の実施形態及び評価(利用者の評価及び事業者にとってのインセンティブ評価)についてご紹介する。

１．実証実験の内容

本実証実験では、ユースケースとして、スマホを利用した「保証書管理サービス」をとりあげた。これを取り上げた理由は、家電製品等でリコールが発生すると企業は莫大な費用を投じて回収等を行わなければならないが、購買者を特定することが困難で、かつ、無理に対象者にアクセスしようとするとプライバシー侵害のリスクを負う可能性がある。そこで、この問題の解決に繋がる、「リコール発生時に、定期的に利用者の情報を確認している事業者（金融機関）から住所等の情報を取得し、確実に利用者へ連絡するユースケース」を実証実験の対象とし、このユースケース名を「保証書管理サービス」と名付けた(図1参照)。

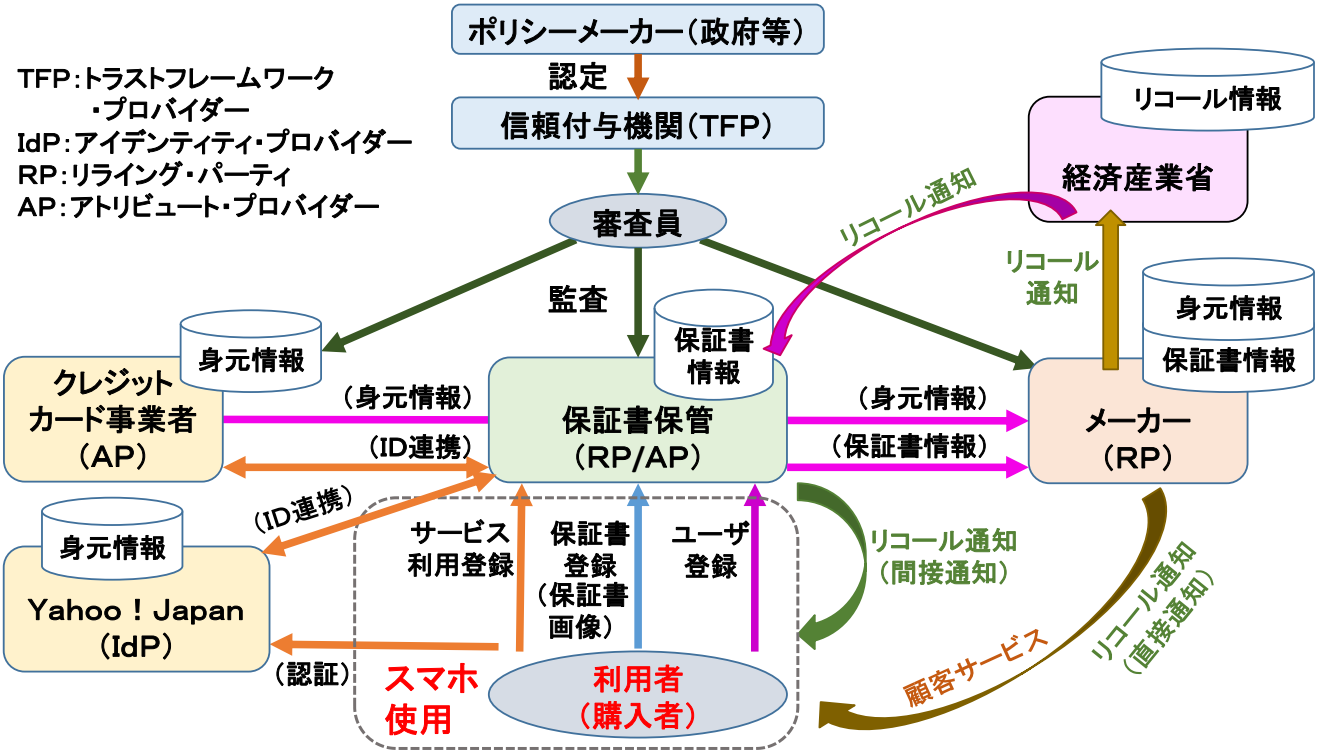


図１　トラストフレームワークを活用した「保証書管理サービス」のイメージ

保証書保管サービスとは、利用者が所有している製品の保証書をオンラインで管理することで、リコール発生時に迅速に対応するものである。その内容は、保証書保管サービスを運営する事業者（仮想の事業者）が、利用者にスマートフォン向けの保証書保管アプリを提供する。利用者は保証書保管アプリをスマートフォンにダウンロード・インストールし、金融機関に登録された身元情報と照会し、連携してサービス利用登録を行う。これにより、利用者は保証書をスマートフォンで撮影するだけで製品登録することが可能となる。なお、製品保証書の撮影データは自動的にテキストデータ化され、製品製造事業者（メーカー）に連携される。本実証実験では、モニター（利用者）を募集し、実証実験用の「保証書管理サービス」のスマートフォン向けアプリを配布した。

実証実験用の「保証書管理サービス」のシステムは、「実験用アイデンティティ・プロバイダ」と「実験用サービス・アプリ」で構成され、「実験用アイデンティティ・プロバイダ」にはアイデンティティ・プロバイダ及びアトリビュート・プロバイダとして「WEBアカウントサービス（Yahoo!Japanを利用）」、住所等の連絡先情報を提供するアトリビュート・プロバイダとして「金融機関（仮想クレジットカード会社）」を利用した。WEBアカウントサービスは、会員登録時に名前などの属性情報の取得元として、金融機関はリコール発生時の住所情報の取得元として想定した。

実験用サービス・アプリには、ID連携や保証登録の登録に関する機能の他に、利用者のプライバシーに関する志

向とサービス・アプリのコンテキストを考慮して、利用者が自分の情報の提供目的や提供先、提供確認の方法等の条件を選択して登録（同意）することがきる機能を設けた。表1に、実験用サービス・アプリの機能を示す。

表１　実験用サービス・アプリの機能

No.	機能	概要
1	ログイン	利用者が選択したWEBアカウントサービスのIDでログインするとともに、WEBアカウントサービスに登録されている利用者の氏名・性別・メールアドレスを利用者の同意を得た上で取得する機能。
2	情報提供範囲の登録	利用者が家電メーカー等に提供する情報に関して、サービスのコンテキストと利用者の志向の両方を尊重して、情報提供の目的や提供先、提供時の確認方法を選択して登録することができる機能。
3	デポジット支払い	アプリの利用開始時にクレジットでデポジットを支払う機能。リコール時に、クレジットカード会社に登録されている連絡先情報等との紐付けが行われる。
4	利用規約確認	情報提供範囲の登録で重要事項の同意を行うため、利用規約の確認は随時可能とする。
5	保証書撮影	保証書をスマートフォンのカメラで撮影しアプリに登録する機能。
6	保証書リスト	アプリに登録された保証書の一覧を表示する機能。
7	保証書内容	保証書リストで選択した保証書の内容を表示する機能。
8	通知リスト	家電メーカー等から受け取ったリコール通知や買い換えの推奨に関するメッセージの一覧を表示する機能。
9	通知内容	通知リストで選択したメッセージの内容を表示する機能。
10	ユーザ情報表示	利用者が登録した氏名・性別・メールアドレス・情報提供範囲等の情報を表示する機能。
11	ユーザ情報編集	利用者が上記の情報を変更する機能。

２．ユースケースの有効性・実用性の評価

２．１　利用者の利便性に関する評価

35名のモニターを募集しID連携トラストフレームワークやそれを活用したサービス・アプリ等の有効性及び実用性を評価するために、グループインタビューを実施した。その結果は以下のとおりである。

（１）ＩＤ連携トラストフレームワークを利用したサービス・アプリの有効性に関する評価

現在のWeb（PC）や紙（ハガキ）での方法と比較した結果、「保証書管理サービス・アプリ」を利用した、Yahoo!IDとのID連携による「利用者登録」の方法が、最も「利便性」が高いことが確認された。

リコール情報の伝わり易さも、7～8割程度のモニターから伝わり易いとの評価を得ることができたが、リコールの緊急性や重要度を考慮したメッセージの通知や表現方法については更に検討を要することが確認された。

「保証書管理」の方法としても、7割程度のモニターから、紙で管理するよりも、データの方が管理し易いとの評価を得た。しかし一部のモニターからは、利用者が死亡した場合に保証書の所在が分からなくなることの懸念が挙げられた。家族や組織での共用を想定したアプリの利用方法についても検討が必要であることが確認された。

また、複数のモニターから、保証書のQRコードの読み取りによる登録機能や、販売店等のレシートや保証書、延長保証書等の登録機能の必要性が指摘された。

このようなサービス・アプリが利用できることでのメーカーに対する顧客満足度の向上については、モニターの8割以上から「向上する」もしくは「やや向上」すると評価されたことから、メーカーに対する顧客満足度の向上に効果が

あることが確認できた。しかし一部のモニターからは、メーカーのアフターサポートは当然なのでアプリが利用できることで顧客満足度は上がらないとの意見もあった。

（２） ＩＤ連携トラストフレームワークの認定サービスの有効性に関する評価

「サービス・アプリ」の画面に表示される「WEBアカウントサービス（ここでは、Yahoo!Japanを利用）」と「金融機関（仮想クレジットカード会社）」の名称の横に、ID連携トラストフレームワークにより認定済みであることを示すマーク（「Tマーク」と仮称）を並べて表示した。

実証実験のモニターには、そのマークが、既に登録されている個人の情報を必要に応じて安全に連携するID連携サービスを提供する事業者であることを示すものであることを説明し、ID連携トラストフレームワークの「有効性」についてヒアリングをした。

その結果、「Tマーク等によって信頼度合いが上がる」、「信頼性のない企業に情報は預けたくない」という意見があった一方で、「外部機関による認定だけでは安心できない」、「自分があまり知らない企業に情報を預けるのは不安である」という意見もあり、より多くの利用者が、ID連携トラストフレームワークの認定サービスの「有効性」を理解するためには、認定サービスの内容や「有効性」に関する周知が重要であることが分かった。

（３） 自己情報の第三者への提供条件の選択性の確保に関する評価

「実験用サービス・アプリ」には、利用者の「プライバシーに関する志向」とサービス・アプリの「コンテキスト」を考慮して、利用者が自分の情報の第三者への「提供目的」や「提供先」、「提供確認の方法」等の条件を選択して登録（同意）することができる機能を設けた。モニターに対してこの機能の提供による事業者への安心感・信頼性向上についてヒアリングを行った。

モニターからは、「自分で情報を選択し、提供する企業や範囲を選択できるならば登録のハードルが下がる」、「情報の提供先についても利用者自身がコントロールできることによって安心感が増す」、「段階を追って承諾させるようにすれば信頼感は高まる（利用者側を考えてくれている）」との意見が多く出たことから、自己情報の第三者への提供条件の選択性を確保することで事業者への安心感・信頼性は向上するものと考えられる。ただし、一部のモニターからは、選択条件を理解することが難しかったという意見もあり、利用者にとって分かりやすい条件の表現方法の工夫が必要であることが分かった。

２．２　事業者のインセンティブ評価

グループインタビューの結果等を元に保証書管理サービスとの関連が考えられる事業者、家電メーカー2社、家電量販店1社、保証書管理サービス提供（予定）事業者1社に対して、事業者のインセンティブについてヒアリングを行った。家電メーカーからは、このサービスを利用することで、リコール発生時に製品購入者に対するハガキ発送の代行費用等として家電量販店等に支払っているコストの軽減が期待される一方で、自社の製品利用者向けサイトに登録されている製品利用者の属性やQ&A等の情報を活用して製品開発を行っているため、自社のサイトへの登録が減少するのではないかという懸念が指摘された。

家電量販店からは、自社のサイトが認定を受けることで利用者が安心してアイデンティティを預けられるようになる制度整備への期待が挙げられた。更に、保証書管理サービス提供（予定）事業者からは、ベンチャー企業として、トラストフレームワークで認定されることにより、消費者からの信頼が高まるようになることへの期待が挙げられた。

以上

＜目次＞

2014.09

～「経済産業省ガイドライン」の読みこなしポイント～
「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」その２
2-2. 個人情報取扱事業者の義務等
2-2-1. 個人情報の利用目的関係（法第 15 条～第 16 条関連）

会員番号 1760 斎藤由紀子 （個人情報保護監査研究会）

２．法令解釈指針・事例 の続きです。

2-2. 個人情報取扱事業者の義務等

2-2-1. 利用目的関係（法第15条～第16条関連）

（１）利用目的の特定（法第１５条第１項関連）

> **法第１５条第１項**
> **個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。**

事業者は、どのような目的で個人情報を利用するかを**できる限り具体的**に特定する必要があります。多くの場合、業種の明示だけでは利用目的をできる限り具体的に特定したことにはなりません。個人情報を第三者に提供することを想定している場合には、利用目的において、その旨特定する必要があり、従業者の雇用管理情報の利用目的の特定に当たっても、具体的、個別的に特定しなければなりません。

【具体的に利用目的を**特定している事例**】

事例1）○○事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします。

事例2）ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります。

事例3）給与計算処理サービス、あて名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。

【具体的に利用目的を**特定していない事例**】

事例1）事業活動に用いるため

事例2）提供するサービスの向上のため

事例3）マーケティング活動に用いるため

（２）利用目的の変更（法第１５条第２項、法第１８条第３項関連）

> **法第１５条第２項**
> **個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。**
>
> **法第１８条第３項**
> **個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。**

利用目的を変更した場合、変更前の利用目的と相当の関連性を有すると合理的に認められる場合は、本人に通知、又は公表します。 ホームページに公表することが一般的です。

【本人が想定することが困難でないと認められる範囲内に該当する事例】

事例　当社の行う○○事業における「新商品・サービスに関する情報のお知らせ」とした利用目的において「既存の商品・サービスに関する情報のお知らせ」を追加すること。

（３）利用目的による制限（法第１６条第１項）

法第１６条第１項
個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければなりません。

※個人情報保護監査研究会注：「あらかじめ」とは、「利用する前に」という意味です。本人に対し、変更後の利用目的を通知し、書面による同意を得てはじめて利用することができます。
16条に違反した場合は、法第34条（勧告及び命令）、第56条（罰則）の対象となる場合があります。

【同意が必要な事例】

事例　就職のための履歴書情報をもとに、自社の商品の販売促進のために自社取扱商品のカタログと商品購入申込書を送る場合

（４）事業の承継（法第１６条第２項関連）

法第１６条第２項
個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

個人情報取扱事業者が、合併、分社化、営業譲渡等により他の個人情報取扱事業者から事業の承継をすることに伴って個人情報を取得した場合であって、当該個人情報に係る承継前の利用目的の達成に必要な範囲内で取り扱う場合は目的外利用にはならず、本人の同意を得る必要はありません。

（５）適用除外（法第１６条第３項関連）

（ｉ）法令に基づく場合（法第１６条第３項第１号関連）

法第１６条第３項第１号
前２項の規定は、次に掲げる場合については、適用しない。
１．法令に基づく場合

法令に基づくとして通知・公表・同意を必要としない事例は、事業の内容に応じて多岐に渡ります。
例えば、以下の事例は、法令の規定により強制力を伴うものです。

事例　刑事訴訟法第218条（令状による捜査）

事例　少年法第6条の5（令状による触法少年の調査）

事例　地方税法第72条の7（事業税に係る徴税吏員の質問検査権、他各種税法に類似規定あり）

【その他法令に基づく強制力を伴う事例】

事例1）金融商品取引法第211条により裁判所許可状に基づいて証券取引等監視委員会の職員が行う犯則事件の調査への対応

事例2）犯罪による収益の移転防止に関する法律第9条第1項に基づく特定事業者による疑わしい取引の届出

事例3）児童虐待の防止等に関する法律第6条第1項に基づく児童虐待に係る通告

事例4）所得税法第225条第1項等による税務署長に対する支払調書等の提出

事例5）統計法第13条による国勢調査などの基幹統計調査に対する報告

【強制力を伴わないが法令に根拠がある事例】

事例1）刑事訴訟法第197条第2項（捜査に必要な取調べ）

事例2）少年法第6条の4（触法少年の調査に必要な質問や調査関係事項照会等）

※個人情報保護監査研究会注：法の定めにより提供する場合であっても、原則として、以下の手順を経て提供します。

1.提供を求めてきたものが正当な機関であることの確認。

2.提供する個人情報の内容、提供する目的等、依頼事項を書面で受理する。

3.代表者もしくは、個人情報保護管理者の承認。

4.上記の記録を規定に従い一定期間保管する。

【本人の同意を得ずに提供する場合、必要性と合理性が認められるか考慮が必要な事例】（抜粋）

事例1）金融商品取引法第210条により証券取引等監視委員会職員が行う犯則事件の調査への対応

事例2）刑事訴訟法第507条による裁判執行関係事項照会への対応

事例3）刑事訴訟法第279条、心神喪失等の状態で重大な他害行為を行った者の医療及び観察等に関する法律第24条第3項による裁判所からの照会への対応

（以後、事例10）まで省略）

※個人情報保護監査研究会注：「必要性と合理性が認められるか考慮が必要」とは、法の強制力は無いとしても、国民としてできる限り協力する姿勢が求められているものです。原則として、書面により要請を受け、責任あるものの承認を得て提供します。

（ⅱ）人の生命、身体又は財産の保護（法第１６条第３項第２号関連）

法第１６条第３項第２号

２．人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

人には（法人を含む。）とことわっており、具体的な権利利益が侵害されるおそれがある場合は、本人の同意を得ないで、個人情報を提供することができます。ただし、「本人の同意を得ることが困難であるとき。」という条件に注意が必要です。

【事例】

事例1）急病その他の事態時に、本人について、その血液型や家族の連絡先等を医師や看護師に提供する場合

事例2）私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合

事例3）製品事故が生じたため、又は、製品事故は生じていないが、人の生命若しくは身体に危害を及ぼす急迫した危険が存在するため、製造事業者等が消費生活用製品をリコールする場合で、販売事業者、修理事業者又は設置工事事業者等が当該製造事業者等に対して、当該製品の購入者等の情報を提供する場合

（iii）公衆衛生の向上等（法第１６条第３項第３号関連））

法第１６条第３項第３号

３．公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

この適用除外についても、「本人の同意を得ることが困難であるとき。」という条件に注意します。また、他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合は、本人の同意を不要とすることができません。

【事例】

事例1）健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合

事例2）不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

（iv）国の機関等への協力（法第１６条第３項第４号関連）

法第１６条第３項第４号

４．国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

【事例】

事例1）事業者等が、税務署の職員等の任意調査に対し、個人情報を提出する場合

事例2）事業者等が警察の任意の求めに応じて個人情報を提出する場合

事例3）一般統計調査や地方公共団体が行う統計調査に回答する場合

※個人情報保護監査研究会注：上記の事例も、任意の協力であり、必ずしも応じなくてもよいのですが、協力することが、市民の務めと考えるのが妥当でしょう。書面により要請を受け、責任あるものの承認を得て提供します。

次回は、「2-2-2. 個人情報の取得関係（法第17条～第18条関連」の読みこなしポイントを掲載します。

バックナンバー目次 http://www.saaj.jp/saajpmsMETIGL/000METIGL.html

個人情報保護監査研究会 http://www.saaj.or.jp/shibu/kojin.html

■

＜目次＞

2014.09

注目情報（2014.08～2014.09）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■IPA「企業の内部不正防止に関する緊急セミナー」開催資料、セミナー動画の公表（2014 年 9 月 1 日）

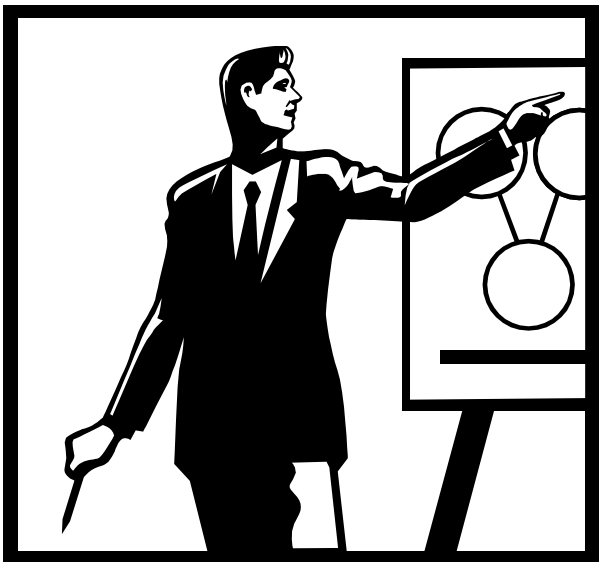
企業内部からの重要情報や個人情報の漏えいが大きなニュースとなり、システム監査やシステム運用に従事する関係者は再点検や改善活動を急遽実施されたのではないかと思われます。この状況を受けてIPAで「企業の内部不正防止に関する緊急セミナー」を 8 月 26 日に緊急開催されています。「内部不正の国内外の現状と事例の紹介」、「防止ソリューション選定のガイド」、「個人情報保護」について講演が実施されており、講演資料とセミナーの動画を下記サイトで公開されています。内部不正防止の点検、改善の際には参考としてご利用ください。

＜開催概要＞

IPA は、2013 年に策定した「組織における内部不正防止ガイドライン」を活用して内部不正対策の普及啓発を行ってきました。

これまで「組織における内部不正対策セミナー」を 3 回（6 月 26 日、7 月 24 日、7 月 30 日）開催してきましたが、教育関係の企業における個人情報漏えい事件の報道を受け、改めて同ガイドラインの周知徹底を図るとともに、多くの企業・組織の意識を高め対策を推進するため、「企業の内部不正防止に関する緊急セミナー」を経済産業省と共に開催します。

http://www.ipa.go.jp/security/event/2014/insider_semi_20140826.html



＜目次＞

2014.09

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第196回	日時：2014 年 10 月 30 日(木)　18:30～20:30　場所：機械振興会館　地下2階多目的ホール	
	テーマ	オープンデータを中心にIT政策の動向全般（仮題）
	講師	経済産業省 CIO補佐官　平本 健二 氏
	講演骨子 お申し込み	詳細確定次第、HPでご案内いたします。
第197回	日時：2014 年 11 月 19 日(水)　18:30～20:30　場所：機械振興会館　地下2階多目的ホール	
	テーマ	マイナンバーと民間サービスとの連携を目指して
	講師	経済産業省 CIO補佐官　満塩 尚史 氏
	講演骨子 お申し込み	詳細確定次第、HPでご案内いたします。

■中堅企業向け「6ヶ月で構築するPMS」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6 ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。（http://www.saaj.or.jp/shibu/kojin.html）
	基本コース	月 1 回（第 3 水曜日）14 時～17 時（3 時間）×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	料金	9 万円/1 名～（1 社 3 名以上割引あり）
	会場	日本システム監査人協会 本部会議室（茅場町）
	テキスト	SAAJ「個人情報保護マネジメントシステム実施ハンドブック」（非売品）

■システム監査普及サービス（全国）

申し込み常時受付中	情報システムの健康診断をお受けになりませんか。 実費のみのご負担でお手伝いいたします。	
	概要	・経験豊富な公認システム監査人が、皆様の情報システムの健康状態を診断・評価し、課題解決に向けてのアドバイスをいたします。これまでに多くの監査実績があり、システム監査普及サービスを受けられた会社等は、その監査結果を有効に活用されています。 ・システム監査の普及・啓発・促進を図る目的で実施しているものです。監査にかかる報酬は無償で、監査の実施に要した実費（通信交通費、調査費用、報告書作成費用等）のみお願いしております。 ・ご相談内容や監査でおうかがいした情報等は守秘します。 詳細はHPでご案内しています。（ http://www.saaj.or.jp/topics/hukyuservice.html ）
お問合わせ	システム監査事例研究会主査　大西（Email：　jireiken@saaj.jp　）	

【　外部のイベント・セミナーのご案内（会報担当収集分）】

■情報システム・ユーザー会連盟（FISA）

第 35 回監査講演会のご案内	
日時	2014 年 10 月 21 日（火）　10:20～17:00
場所	きゅりあん（品川区立総合区民会館／東京・大井町）
テーマ	『情報セキュリティとシステム監査』
概要	サイバーテロ対策や情報漏えいへの対応など各企業のセキュリティは一層重要となっており、システム監査の実施に際しても従来以上に厳格な対応が求められております。そこで本年度は「情報セキュリティとシステム監査」をテーマに、プログラムを企画いたしました。 現在検討されている情報セキュリティの国家資格を含むセキュリティ政策や、システム開発における情報セキュリティ関連の法的課題とシステム監査に関する講演、現場で実務に携わる方々をお招きしてのパネルディスカッションなど多岐にわたる内容となっております。 （詳細は下記 URL より案内状をご参照下さい。）
内容等	申込方法等の詳細はHPで紹介されています https://www.it-user.hitachi.co.jp/pdf/H26syskanannai.pdf

＜目次＞

2014.09

Welcome

新たに会員になられた方々へ

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/index.html
・会員規程にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・皆様の情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

特典

・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

ぜひ参加を

・各支部・各部会・各研究会等の活動です。 http://www.saaj.or.jp/shibu/index.html
　皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

ご意見募集中

・皆様からのご意見などの投稿を募集しております。
　ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

出版物

・協会出版物が会員割引価格で購入できます。 http://www.saaj.or.jp/shuppan/index.html
　システム監査の現場などで広く用いられています。

セミナー

・セミナー等のお知らせです。 http://www.saaj.or.jp/kenkyu/index.html
　例えば月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。

CSA・ASA

・公認システム監査人へのSTEP-UPを支援します。
　「公認システム監査人」と「システム監査人補」で構成されています。
　監査実務の習得支援や継続教育メニューも豊富です。
　CSAサイトで詳細確認ができます。 http://www.saaj.or.jp/csa/index.html

会報

・PDF会報と電子版会報があります。（http://www.saaj.or.jp/members/kaihou_dl.html）
　電子版では記事への意見、感想、コメントを投稿できます。
　会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

お問い合わせ

・右ページをご覧ください。 http://www.saaj.or.jp/toiawase/index.html
　各サイトに連絡先がある場合はそちらでも問い合わせができます。

＜目次＞

2014.09

【　ＳＡＡＪ協会行事一覧　】

2014 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
2 月	6 日 理事会:通常総会議案承認 21 日 通常総会・特別講演	CSA・ASA 春期募集(2/1～3/31) 1-2 日 事例研:第 23 回システム監査実務セミナー(前半)、22-23 日(後半) 5 日 CSA フォーラム 10 日 第 189 回月例研究会	
3 月	1 日 事務局:法務局登記、東京都への事業報告、変更届提出	1 日第 13 回課題解決セミナー 25 日 CSA フォーラム	
4 月	1 日 認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査 25 日 第 190 回月例研究会	20 日 2014 年春期情報技術者試験(9:30～16:30)
5 月	8 日 理事会 29 日 会費未納督促メール	認定委員会:新規 CSA/ASA 面接 15-16 日 事例研:第 26 回システム監査実践セミナー 22 日 第 191 回月例研究会	
6 月	12 日 理事会 末日 支部会計報告依頼(〆切 7/14) 末日 助成金配賦額決定(支部別会員数)	7 日事例研:第 14 回課題解決セミナー 10 日 新規 CSA/ASA 承認 10 日 CSA フォーラム	28 日 近畿支部:システム監査体験セミナー(入門編):
7 月	1 日 会費未納者督促状発送 8 日 支部助成金支給 10 日 理事会	1 日 秋期公認システム監査人募集案内〔申請期間 8/1～9/30〕 3 日 第 192 回月例研究会 22 日 第 193 回月例研究会	14 日 支部会計報告〆切
8 月	(理事会休会) 会費督促電話作業(役員) 23 日 中間期会計監査	秋期公認システム監査人募集開始～9/30 20 日第 194 回月例研究会 30-31 日 事例研:第 24 回システム監査実務セミナー(前半)	30～31 日東北支部:合宿研修会 30～31 日近畿支部:システム監査体験セミナー(実践編)
9 月	11 日 理事会	13-14 日 事例研:第 24 回システム監査実務セミナー(後半) 8 日 第 24 回CSAフォーラム 18 日 第 195 回月例研究会	6～7 日中部、北信越支部/JISTA 中部合同合宿
10 月	9 日 理事会	30 日 第 196 回月例研究会	25 日 近畿支部:IT-BCP 体験セミナー
11 月	13 日 理事会 13 日 予算申請提出依頼(11/30〆切) 20 日 会費未納者除名予告通知発送 30 日 予算申請提出期限 30 日 2015 年度年会費請求書発送準備	中旬 認定委員会:CSA 面接 19 日 第 197 回月例研究会 20 日 CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 28 日 認定委員会:CSA 面接結果通知	29 日 西日本支部合同研究会(開催場所:大阪市)
12 月	1日 2015 年度年会費請求書発送 2015 年度予算案策定 11 日 理事会:2015 年度予算案、会費未納者除名承認 12 日 支部会計報告依頼　(1/9〆切) 第 14 期総会資料提出依頼(1/9〆切) 19 日 会計:2014 年度経費提出期限	10 日 認定委員会:CSA/ASA 更新手続案内メール発信 16 日 第 198 回月例研究会 20 日 CSA 認定証発送	
2015 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	8 日 理事会:通常総会議案審議 9 日 総会開催案内掲示・メール配信 9 日 総会資料(〆) 19 日 会計:2013 年度決算案 24 日 会計:2013 年度会計監査 31 日 償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 20 日 第 199 回月例研究会 20 日 春期公認システム監査人募集案内〔申請期間 2/1～3/31〕	9 日 会計:支部会計報告期限 日付未定 近畿支部:支部総会

※注　定例行事予定の一部は省略。

＜目次＞

2014.09

会報編集部からのお知らせ

1. 会報テーマについて
2. 会報記事への直接投稿(コメント)の方法
3. 投稿記事募集

□■ 1. 会報テーマについて

2014 年度の年間テーマは、「○○○のためのシステム監査」とし、四半期ごとに「○○○のための」について具体的なテーマを設定して、システム監査に関する皆様からのご意見ご提案を募集しています。

これまで 2 月号から 4 月号までが「公(おおやけ)のためのシステム監査」、5 月号から 7 月号までが「情報化社会のためのシステム監査」、8 月号から 10 月号までが「次世代のためのシステム監査」をテーマとし、様々なご意見ご提案をいただきました。ありがとうございました。

11 月号から 1 月号までの3か月は、「情報システム部門のためのシステム監査」をテーマとすることとしました。情報システム部門を取り巻く方々に向けてのシステム監査について、皆様からの幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

1)PDF ファイルの全体を、URL(http://www.skansanin.com/saaj/)へアクセスして、画面で見る

2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る

3)会報 URL(http://www.skansanin.com/saaj/)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。動画でも紹介しますので、参考にしてください。

(http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」)

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

1. めだか (Word の投稿用テンプレート(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)

3. 会報投稿論文 （論文投稿規程があります）

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。 システム監査にとどまらず、情報社会の健全な発展を応援できるような内容であれば歓迎します。ただし、投稿された記事については、表現の訂正や削除を求め、又は採用しないことがあります。また、編集担当の判断で字体やレイアウトなどの変更をさせていただくことがあります。

次の投稿用アドレスに、次号会報募集案内メールに添付されるフォーマット(Word)を用いて、下記アドレスまで、メール添付でお送りください。

投稿用アドレス:saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）

バックナンバーは、会報サイトからダウンロードできます(電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります)。

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】(当協会ホームページ会員サイトから閲覧ください。パスワードが必要です)

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行： NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町2－8－8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】 http://www.saaj.or.jp/toiawase/

■会報は会員への連絡事項を含みますので、会員期間中の会員へ自動配布されます。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。

【送付停止】 http://www.skansanin.com/saaj/

■□■SAAJ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
編集委員： 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、中山孝明、藤野明夫
編集支援： 仲厚吉 （会長）
投稿用アドレス： saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

＜目次＞