特定非営利活動法人
日本システム監査人協会報

2015 年 3 月号
No 168

No. 168（2015 年 3 月号）＜2 月 25 日発行＞

今月号の注目記事は、インターネットバンキングに係る不正送金防止について掲載している

「月例研究会　2015 年 1 月報告」
「注目情報：警察庁発表」

の2本です。是非、ご一読を！

『上野公園ぼたん園』

写真提供
斎藤由紀子
副会長

巻頭言

『　初心にかえる　』

会員番号 1342 安部晃生　（副会長）

昨年、38 年間勤めた銀行を退職し、今年から或る会社のシステム監査態勢整備についてアドバイスする仕事をしている。システム監査態勢をどう整備していけばよいかを提案し、先方といっしょに今後の対応を考えていくわけだ。

そうした提案にあたっては、今までシステム監査においてそうするのが当たり前と考えていたことについても、そのような対応がなぜ必要なのかを説明しなければならない。こうした基本的なことを説明するために、初心にかえって「システム監査では何を検証しようとするのか？」「リスクベースアプローチはどのように進めていけばよいのか？」「オフサイトモニタリングはなぜ必要なのか？」等々、考えをめぐらしていくと、システム監査をどのように進めていくかについて、いろいろな気付きがあった。

システム監査も長くやっていると、自分なりの勘所もわかってきて、ついルーチンワーク化してしまっているといったことはないだろうか？

皆さんも、もう一度初心にかえって、現在やっている仕事を見直してみるのもよいのではないだろうか。

＜目次＞

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

2015.2

めだか 【 マネジメントシステム内部監査におけるシステム監査人の役割 】

マネジメントシステム(MS)は、一定の目標に向かってPDCA(Plan-Do-Check-Act)のマネジメントサイクルを回して継続的改善を図る体制である。品質向上、環境配慮、情報セキュリティ、食品安全、個人情報保護などに適用されている。マネジメントシステムの内部監査は、PDCA(Plan-Do-Check-Act)のマネジメントサイクルのC(Check)の機能を担っている。PD(Plan-Do)がしっかりと運用されていることを監査し、代表者に報告して代表者の見直し、すなわちA(Act)を導く役割である。システム監査人の役割は内部監査のうち情報システムへの監査をもとに情報システムにまつわるリスクに対するコントロールが適切に整備・運用されているかを点検することである。

企業などの組織体は、組織体の事業継続性のため、収入・支出のバランスをとり、かつ、品質向上、環境配慮、情報セキュリティ、食品安全、個人情報保護などの体制に瑕疵が無いよう継続的改善を図ることが求められる。また、入札や取引の条件でマネジメントシステム規格認証制度により認証を受けるよう求められることがある。無理な認証取得があったため、マネジメントシステム規格認証制度において、取得企業で認証に係る不祥事が頻発した時期があり、「マネジメントシステム規格認証制度の信頼性確保のためのガイドライン」が、2008年(平成20年)に、経済産業省より公表されている。抜粋してシステム監査人へ紹介したい。

〔認証機関に係るガイドライン〕

信頼性確保が認証機関の共通の課題であるとの認識の下、以下の点について取組みを進めること。

(1) 認証に係る規律の確保

(2) 審査員の質の向上と均質化のための取組の推進

(3) 認定機関への協力

注) 認証に係る規律の確保:認証を受けた組織において、審査の際に故意に虚偽の説明を行っていないこと、重大な法令違反が無いこと、組織の一部分を認証する場合にあっては重要な組織活動が認証範囲から欠落していないこと

〔認定機関に係るガイドライン〕

認定機関は、いわばMS認証制度の総括的管理者として、以下の点について取組を進めること。取組を進めるに当たって、認証機関が適切な対応をとるよう、認定行為において然るべき措置を講ずること。

(1) 認証を受けた組織の不祥事等への対応の適正化

(2) 認定行為の透明化

(3) 有効性審査の徹底

(4) MS認証制度の積極的広報

(5) MS認証に係る情報の積極的提供

(6) 国際整合性への配慮

注) 有効性審査:規格適合性だけでなく、規格がシステムとして有効に機能しているかどうか、パフォーマンスが向上しているかどうかで判断する審査のこと

(空心菜)

(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＞

2015.02

投稿【『時事論評』IoT/M2M 時代のシステム監査】

会員番号 0707 神尾博

1. IoT/M2Mとは？

コンピュータや通信機器以外の「モノ」が、インターネットに接続され、その情報を元に人々へサービスが提供される「IoT（Internet of Things）」。複数のマシンが、人間の介在無しで高度な情報のやり取りを行い、制御や計測といった機能を相互に連携する「M2M（Machine to Machine）」。当初はデジタル家電やFA（Factory Automation）等から歩み始めた「IoT/M2M」だが、もはやバズワードから離陸し徐々に社会に定着しつつある。そうした中、ここではIoT/M2Mにおけるシステム監査の着眼点等、他分野のシステム監査人であっても押えておきたい知識を、話題として提供したい。

さて、IoTとM2Mは比較的よく似た概念だが、最初にこれらの関係を整理しておきたい。まずは「①M2MはIoTの通信機能部分説」である。M2Mの一例として、セルラー通信モジュールが挙げられる。端的に言えば、携帯電話からHMI（マイク、PCMプロセッサ、液晶画面等）を除いたものだ。次に「②応用分野の違い説」がある。M2Mはビジネスやインダストリーで、IoTはソーシャルといった考え方だ。この分類では、複合機やエレベーターの遠隔保守はM2M。暮らしの中のウェアラブルやスマートテレビはIoTになる。そして最も有力なのは「③M2MはIoTのサブセット（部分集合）説」だ。たしかにRFID（無線タグ）はマシンとは言えないが、IoTには違いない。マシンは有体物だから、モノの一種であると言えるだろう。

ただし、これから述べるシステム監査というフレームワークでの考察の場合は、こうした分類自体にはあまり意味がなさそうだ。そこで、いっそのこと「IoT/M2M」と連記し、まとめて考察するというスタンスを選択した。

2. IoT/M2Mの構成要素は？

文献によって多少異なるが、IoT/M2Mは「デバイス/装置」「LAN」「WAN」「サーバ/端末」および「これらの統合サービス」で構成される。

最初の「デバイス」は、WSN（Wireless Sensor Network）ノード等であり、機能の大部分をエンベデッド（組込）システムが担う。たとえば、センサにより動きや温度等を検出・測定したりする。「装置」は、デバイスより複雑な機構を持ち、自動車やロボット等が該当する。

「LAN」は工業分野等でのフィールドネットワークを除き、無線が大勢を占めている。ただしおなじみのWiFiは少数派だ。デバイスや装置が多種多様のため、接続ノード数や帯域幅といった要求事項が異なり、1種のネットワークでの網羅は不可能である。たとえばセンサネットワークでも、BlueToothやZigbee等が使い分けられている。なお、IPプロトコルに対応していない通信方式を採用した場合は、中継ポジションにWSNエッジノードのような「IPゲートウェイ」に該当する機器が存在する場合もある。

「WAN」は通常のIPネットワーク網のインフラと考えてよい。無線での乗り入れはLTEや3G、WiMAX等でおこなわれる。

「サーバ/端末」には、当然アプリ等のソフトウェアも含まれる。ウェアラブル機器からのライフログのように、収集データの終着点がスマホやPCの場合もある。一方で巨大なビジネスチャンスを狙い、クラウド上のビッグデータとして蓄積・分析するといった動きもあり、IT業界のみならず利用価値のあるデータを保有する企業も虎視眈々だ。

これらの要素の「統合」、すなわち垂直型のソリューションでは、大手ITベンダーを中心に、各社が新規

市場開拓にしのぎを削っている。

3. IoT/M2Mの特質は？

「マシン」「センサ」といったキーワードから思い浮かぶのは「制御系」である。ここでは一般ビジネス系と対比した場合の制御系の3つの特質を基準に、IoT/M2Mのそれを抽出してみたい。

まずは「高信頼性」。制御系では、信号処理・演算処理・これらの連携が確実に実行されることが前提になるケースが数多い。「ミッションクリティカル」と呼ばれるものだ。たとえば、医療、交通、災害検知等の分野の場合は、デバイス/装置は極めて高レベルの信頼性が不可欠である。さらには熱、湿気、振動、ノイズ等への耐環境性も要求される。また次の第4節で述べるが、通信経路についても可用性確保が課題となってくる。

次に「タイムクリティカル性」。これも制御系の根幹の要素であり、一般に数msec～数十msecのオーダーでの時間内処理を指す。有線系のフィールドネットワークでは、この要求性能が保証されるプロトコルが用いられたりする。一方、無線ではパケット到達の遅れや欠落が想定されているため、高信頼性同様、この性能は系全体としてではなく、デバイス/装置の単体で担保することになる。むしろ電源の引き込みが困難な場合には、使用ビット数が少ないプロトコルの採用等、省エネ性能が優先される傾向にある。橋梁のひずみ等のインフラ監視のケースが当てはまる。メモリ節約のための短い変数名や、実行命令数を少なくすることで処理の高速化を図るといった、マイコン黎明期を彷彿させる。

最後に「多種多様性」。これは前の第3節の「デバイスや装置」「LAN」で述べた通りだ。後述するが、こうした特質により、システム監査実施の際の着眼点も大いに異なってくる。

4. 構成要素での注目は？

ズバリ、デバイスであるWSNノードと、統合における有益性の高いアプリケーションの発案力をあげておこう。WSNノードについては、小型大容量・高寿命電池の開発や回路の消費電力の削減等、まだまだ課題もある一方で無限ともいえる可能性を秘めている。

2014年12月の大雪の際に発生した、徳島県西部のIP電話網の不通は記憶に新しいはずだ。従来のアナログ回線に比べての、停電への無力さが招いた災難である。その際には「UPS（無停電電源装置）が有効」という上から目線のコメントも見かけたが、UPSは数年ごとに交換が必要であり、地方の高齢者には酷だろう。

WSNは、故障ノードを避けた経路選択をするメッシュ型ネットワーク、センサノードから中継ノードへの自動切替、百メートル近くまでの無線での到達距離、周囲の光や振動で必要な電力を発生させるエナジーハーベスティング（環境発電）といった優れた特徴を持つ。健康状態の赤/黄/緑の区分くらいの情報伝達なら、人家が極端に分散している地域以外では、災害時の非常通信網としての採用も検討に値するだろう。

5. システム監査での着眼点は？

最後に本稿の主題である、IoT/M2Mのシステム監査に際しての着眼点を、システム監査の主目的である「安全性」「信頼性」「効率性」の向上の観点から、いくつか並べあげてみたい。

安全性については、もはや「IoTは、Internet of Threat」と揶揄する声もあるくらいだ。たとえば、2013年にはアイロンの仕組まれたマルウェアによる、無線LANポートからのパソコン経由のSPAM攻撃が報告されている。また2014年には、ドローン（小型の無人操縦機）がハッキングされ、ゴール近くでトライアスロン選手の頭に衝突し、転倒させるという事件も起きている。さらにはIMD（Implanted Medical Devices）

への不正アクセスの懸念も指摘されており、テロリストによって、これを装着した政府要人への攻撃に利用される可能性もある。とうとう2015年1月には米連邦取引委員会（FTC）が、調査報告書でIoTのセキュリティリスク対応をデバイスメーカーに求めた。この分野のシステム監査に際しては、こうした脆弱性や関係機関の対応等の情報収集は不可欠である。

信頼性は、ほぼ第3節で解説した通りである。WSNではノード単体の電子回路の信頼性もさることながら、系全体の可用性の方が、エンドユーザ視点に近い指標となるだろう。ITIL（Information Technology Infrastructure Library）では、その対象とするデータセンター等のシステム運用を「システムではなくサービスとして捉える」としているが、IoT/M2Mにおいても同様の解釈が適用できる事が、このWSNの例を通じても改めて認識できる。

効率性に関しては、全世界の様々な意見に耳を傾けてみると「洗濯機とグリルの通信に、意味はあるのか」といった懐疑派や「つながりが生む新ビジネス」といった楽観論がある。こうして見ると文明論臭くなり、確固とした答えに定まらないような印象を受ける。しかし両面派の「様々な可能性の中から、真のニーズがどこにあるかは、いずれ市場が決める」といったあたりの見解が、システム監査でいう「有効性評価」と重なっているのではないか。少なくとも「システム監査的視点」での客観的判断を、社会が欲していないとは捉えがたい。

IoT/M2Mはメインフレームから分散系への移行に匹敵する、いやそれ以上のパラダイムシフトを引き起こす可能性がある。システム監査基準/管理基準の改訂まで、視野に入って来るのではないか。現代、そして未来を生きるシステム監査人なら、感度を高くして動向を見守るべきだろう。

最後に、本稿作成に際してご協力頂いた安本哲之助氏、田淵隆明氏に対し、この場を借りて御礼を申し上げる次第である。

（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。）

以上

＜目次＞

2015.2

投稿【　システム監査人の魅力　】

会員番号 0557 仲 厚吉 （会長）

会報 2015 年度テーマは、“システム監査人の魅力”です。当協会はシステム監査人の魅力を向上させるべく、協会運営の方向性として、システム監査の普及、促進活動の一層の推進に向け、協会の信頼性を高めるよう次の協会活動を行っていきます。

・会員各位から寄附を頂いた実績をもとに東京都へ申請した「認定 NPO 法人」の認定を目指します。認定によって協会の信頼性、システム監査人の社会的評価の向上を図ります。
・システム監査の活性化の一環として、IT-Audit 等の ISO 化、JIS 化、システム監査に関連する他団体との交流、会員とのコミュニケーション向上のためホームページの整備、会員ポータルサイトの導入を進めます。
・IT ガバナンス（Corporate governance of information technology）、IT 人材の育成をテーマにシステム監査の活性化、システム監査人の活用を図ります。

システム監査人の魅力を向上させるに当ってシステム監査人は幸福でなければならないと思います。ユングは、幸福の 5 条件（Carl Jung’s 5 Key Elements to Happiness）を挙げています。叶えたいものです。

1. 心身ともに健康であること（Good physical and mental health.）
2. 豊かで幅広い人間関係（Good personal and intimate relationships, such as those of marriage, the family, and friendships.）
3. 芸術や自然の美しいものに感動できること（The faculty for perceiving beauty in art and nature.）
4. 自分で程良いと思うお金や仕事があること（Reasonable standards of living and satisfactory work.）
5. 人生の変化に対処できる心構えを持つこと（A philosophic or religious point of view capable of coping successfully with the vicissitudes of life.）

さて、当協会では、公認システム監査人認定制度とシステム監査人推薦制度を設けています。公認システム監査人認定制度は、高度情報処理技術者試験合格者、公認会計士、ISMS、PMS 主任審査員などシステム監査レベル 4 の者に、システム監査の実務経験を審査し、レベル 5 の公認システム監査人（CSA：Certified Systems Auditor）資格を認定する制度で、2 年毎の資格更新審査があります。実務経験に不足がある場合、当協会の実務セミナーなどを受講し補うこともあります。

システム監査人推薦制度は、企業・団体がシステム監査を行うに当ってシステム監査人の推薦を当協会に求める際、予め登録してあるシステム監査人から最適の方を推薦する制度で、公認システム監査人を有する正会員団体もしくは公認システム監査人の正会員個人が推薦の対象者になります。昨年来、法令順守、情報セキュリティ対策、サイバー犯罪対策の時代を反映して、システム監査人の推薦を依頼する企業や団体が増えてきました。

会員の皆様には、公認システム監査人（CSA）になって、システム監査人の魅力を高めていただきたいと思います。先ずシステム監査人補（ASA: Associate Systems Auditor）になって公認システム監査人（CSA）を目指すこともできます。

以上

＜目次＞

2015.2

第１９９回　月例研究会　（２０１５年１月開催）

会員番号 0056　藤野明夫 （情報セキュリティ監査研究会）

【講演テーマ】 「インターネットバンキングに係る不正送金事犯被害の実態と防止策」

【講師】 警察庁 生活安全局 情報技術安全対策課 警察庁警視 小竹一則 氏

【日時】 2015 年 1 月 20 日（火曜日）18:30～20:30

【場所】 機械振興会館　地下 2 階ホール

【講演骨子】：講師より

社会問題化するインターネットバンキングに係る不正送金事犯。その被害額は昨年の5月の時点で過去最悪であった平成 25 年中の被害額約 14 億 600 万円を超え、その後も深刻なペースで被害が多発しました。

犯行の手口はフィッシングからウイルスによる ID・パスワードの不正取得へと、また、不正送金のターゲットは個人口座から法人口座へと変遷しています。

本講演では、インターネットを取り巻く犯罪情勢やこの種事犯の検挙事例等を織り交ぜながら、インターネットバンキングに係る不正送金事犯の発生状況及びその特徴、多発する要因、被害を未然に防止するための対策について説明します。

【講演内容】

はじめに

昨年の 3 月に 2 年契約で愛知県警察本部から警察庁に出向し、ウイルスに関する事件の指導を担当しているが、仕事の大半はインターネットバンキングにおける不正送金事犯への対応である。よって本日は、この不正送金事犯に係る、①インターネットを取り巻く現状、②インターネットバンキングに係る不正送金事犯の発生状況、③検挙状況、および、④防止対策についてお話する。なお、マルウェア（不正プログラム）についてはマスコミ各社にならい適宜「ウイルス」と表現する。また、本日の話には、講師の私見が多分に含まれていることをご承知おきいただきたい。

１．インターネットを取り巻く現状

スマホやタブレット端末の普及にともない、平成 25 年現在、国民の 82.8%がインターネットを利用している。13 歳～49 歳までの年齢層では、利用率が 9 割を超えており、60 歳以上も増加傾向にある。また、個人のインターネットの利用率は、大都市のある都府県を中心に高くなっている。

警察のサイバー空間の脅威への対応は大きく二つに分かれる。一つは、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、ネットワーク利用犯罪などの国民生活を脅かすサイバー犯罪への対応で、我々、サイバー課が担当する。もう一つは、サイバーテロやサイバーインテリジェンス等の国の重要な情報やシステムを標的としたサイバー攻撃への対応で、公安警察が担当する。本日は、国民生活を脅かすサイバー犯罪についてお話する。

近年、サイバー犯罪の質に変化がおきている。従来は、「・・・こんなことができる！」、「・・・凄いでしょう！？」といった自己顕示目的のものであった。しかし、現在は目的が金銭取得になり、個人による犯行から組織的犯行に変化している。また、サイバー攻撃の手口も巧妙化してきている。かつてはメールやウイルスを多数配布するばらまき型が主流であったが、現在は攻撃対象を絞り込み、深く調査してウイルスに感染させる方法が主流になっている。これには大きく二種の方法がある。一つは、やり取り型と呼ばれるもので、攻撃対象に対して偽りの立場でやり取りし、そのやりとりの過程で攻撃対象をウイルスに感染させるものである。たとえば、犯人が就職希望者を装い、対象企業の人事担当

者とやりとりしているなかでウイルスを忍びこませるものである。もう一つは、水飲み場攻撃と呼ばれるもので、攻撃対象が不安感を抱かずに思わずアクセスしたくなるようなサイトを作り、そこに呼び寄せてウイルスに感染させるやり方である。

平成 25 年中のサイバー犯罪の検挙件数は、8,113 件（前年比＋779 件、＋10.6%）に達し、過去最高を記録した。そのうち、ネットワーク利用犯罪（児童ポルノ、わいせつ画像の提供等）は、6,655 件で過去最高である。表1をご覧いただきたい。なお、この表の中には、インターネットに直接関係しないので、出し子（後述）や口座売買ブローカーの検挙数は含まれない。

表１　サイバー犯罪の検挙件数の推移

	H21	H22	H23	H24	H25	前年比増減	
不正アクセス防止法違反	2,534	1,601	248	543	980	＋ 437	＋ 80.5%
コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪	195	133	105	178	478	＋ 300	＋ 168.5%
ネットワーク利用犯罪	3,961	5,199	5,388	6,613	6,655	＋ 42	＋ 0.6%
合計	6,690	6,933	5,741	7,334	8,113	＋ 779	＋ 10.6%

「『平成 25 年中のサイバー犯罪の検挙状況等について』、警察庁広報資料、平成 26 年 3 月 27 日」により作成

ここで、平成 26 年中のサイバー犯罪の特徴について触れたい。一点目は、LINE の成りすまし詐欺である。流出した ID・パスワード情報が悪用されて仮想通貨が詐取される。二点目は、標的型攻撃の多発である。昨年上半期で 216 件に達しており、前年より 15 件増加している。三点目は、3D プリンターによる殺傷能力のあるプラスチック製拳銃の製造、ビットコイン不正アクセス、ソフトの脆弱性（Open SSL、IE6～11 等）を狙った攻撃等の新たなサイバー技術・サービスの犯罪への悪用である。とくにビットコイン等の仮想通貨は、闇取引の支払い手段に使われている点で大きな問題となっている。

米国、マカフィー社は 2014 年の十大セキュリティ事件を発表した。上位五つは、以下のとおりである。1位はＢ社顧客個人情報流出事件。2,900 万件の個人情報が流出し、損害額は 260 億円に上る。2 位は振り込め詐欺被害、これは、ネットバンキングの不正送金の被害額の 10 倍以上に上る。3 位は LINE 乗っ取り被害である。4 位はインターネットネットバンキングを狙う不正送金ウイルス、5 位は、金融機関を騙るフィッシングサイトである。4 位と 5 位に今日の話の中心となるインターネットバンキングに係る不正送金事犯が入っている。これが、インターネットバンキングの不正送金を本日の話の柱に据えた所以である。

２．インターネットバンキングに係る不正送金事犯の発生状況

（１）発生状況

インターネットバンキングには、すでに 6，850 万以上もの口座が存在する。かくも多くの口座が存在するのは、外出せずに残高照会、入出金明細照会、振り込み等ができる、窓口の行列に並ばなくてもよい、手数料が安いといったメリットがあるからである。しかし、同時に、ID・パスワードを忘れると利用できない、ID・パスワードを読み取られて不正に現金を引き出されるといったデメリットもある。

インターネットバンキングに係る不正送金とは、ウイルスやフィッシングサイトによって ID・パスワードを不正取得し、これによって他人の口座に不正アクセスをしたり不正送金指令をしたりして、予め用意した口座に送金し、これを引き出す、この一連の行為をいう。犯行にウイルスやフィッシングサイトが使われていることから、我々、サイバー課がその取り締まりに従事している。

インターネットバンキングに係る不正送金事犯の推移を図1に示す。平成23年の7月から9月ごろに第一のピークがある。金融機関と警察による対策以外の要因もあり、一旦は収まった。しかし、平成25年5月ごろに急増して平成25年の被害は、32金融機関、1,315件、約14億600万円に及んでいる。急増した原因はいくつかあるが、その一つには、被疑者がランゲージバリアを乗り越えたことが挙げられる。実は、サイバー犯罪には、ランゲージバリアが存在する。フィッシングサイトが不自然な日本語であれば、誰も騙されない。インターネットバンキングの不正送金事犯の被疑者は外国人が多数を占めるが、第一のピークでは、まだ、このランゲージバリアが越えられなかったのであろう。一昨年5月から急増したということは、犯人はこのランゲージバリアを越えた可能性がある。

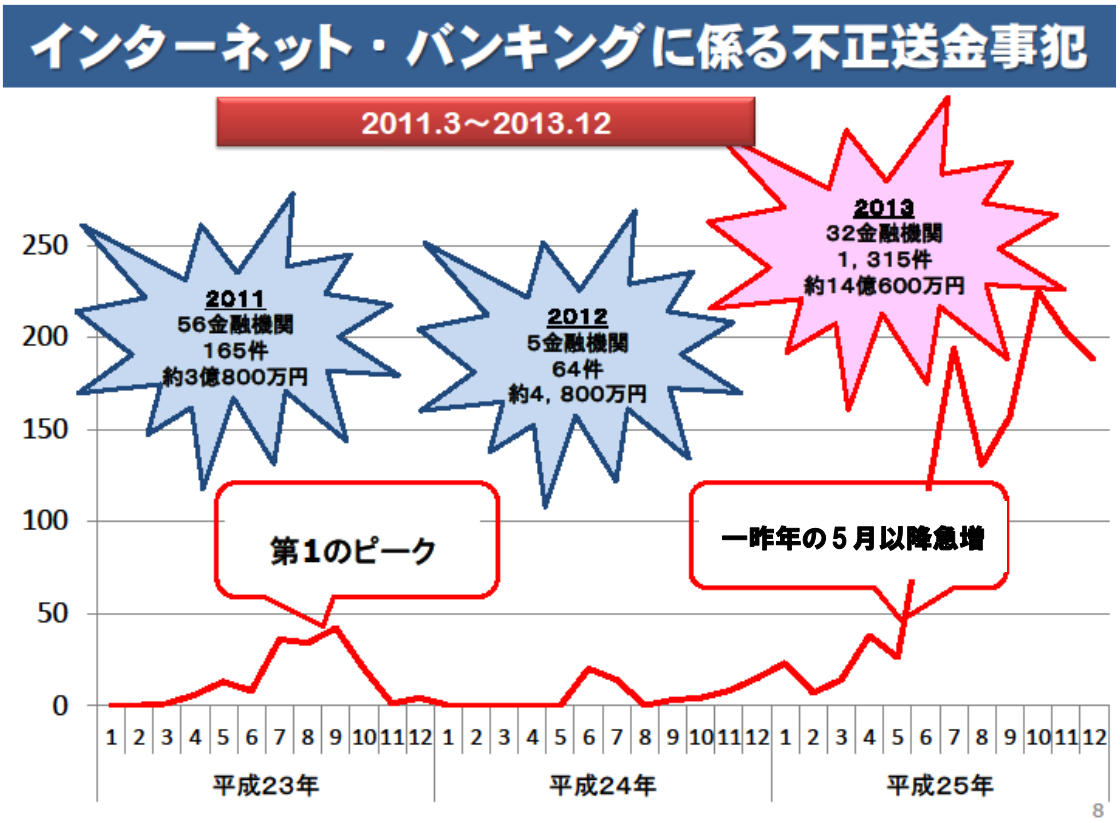


図1　インターネットバンキングに係る不正送金事犯の発生推移

なお、平成26年は上半期だけですでに被害は、73金融機関、1,254件、約18億5,200万円に達しており、被害金額は平成25年の一年分を超えている。ウイルスに亜種が発生し、それが阻止できなかったことと対策の遅れた地方金融機関の法人口座が狙われたことが主たる要因と推測される。なお、平成26年下半期は、まだ正式発表前で正確な数字は言えないが、金融機関等の対策が功を奏し、多少、落ち着いた感がある。

今、述べたように法人口座の被害が増加している。従来は個人口座が中心であったため、送金額の上限が低く、一件当たりの被害金額は少なかったが、法人の場合は、送金額の上限が高いか、または、制限がないため、一旦被害に遭うと高額が送金されてしまう。ちなみに、1件当たりの被害額は、平成25年一年間の平均で107万円であったのに対して、平成26年上半期は148万円に増加している。なお、法人のみで比較すると、一件当たりの被害額が、平成25年に181万円であったものが、平成26年上半期は、409万円と二倍以上になっている。また、被害を受けた金融機関の規模も、初期のころのメガバンク中心から、地方銀行、信用金庫、信用組合といった地方に被害が拡大している。メガバンクを中心に対策が強化されてきたため、対策が比較的手薄であった地方金融機関が狙われるようになったものと思われる。これも対策がとられつつあり、対策をとっている金融機関では被害は落ち着きつつあるが、未

だ、手を打っていない金融機関は、法人名義口座で被害が継続している。被害の特徴を一言でまとめると、対策が遅れた地方銀行、信用金庫、信用組合の法人名義口座から数千万円が不正に引き出されたということである。

（２）不正送金の態様

不正送金の手口の概要を説明する。

不正送金の 64.9%は、送金された口座から現金を引き出す役割を担う「出し子」による現金出金である。まず、口座ブローカー等が不正送金先口座（不正送金先口座の 69.5%は中国人名義）を準備する。次に指令役が被害名義人口座から、準備した不正送金先口座に不正送金をする。出し子リーダーが出し子に現金の引出場所等を指示する。なお、引出し場所のほとんどはコンビニ ATM であり、金融機関の ATM が利用されるケースは少ない。指示された出し子は、現金を引出し、指示に従い集金役に渡す、あるいは、駅のコインロッカー等に預ける。

次に多いのが、資金移動業者等による国外送金、すなわち、マネーミュールであり、不正送金の 7%を占める（図 2 参照）。国外にいる主犯格被疑者が、簡単な仕事で高収入が得られるという釣り文句で求人掲示板や求人メールを用いて口座の提供を求める。報酬は、送金額の 5%～10%である。国内の掲示板閲覧者・メール閲覧者がこれにより口座を提供すると、主犯格被疑者は不正送金処理をして提供された口座に送金する。これを口座提供者が現金化し、資金移動業者等を通じて国外の主犯格被疑者に送金する。この手口については、適用法令を検討して検挙を進め、平成 25 年はゼロだった検挙者が、平成 26 年上半期には 16 人に達した。また、警察庁からの申し入れに基づき、資金移動業者も身分、送金理由等の確認等の防止策を徹底し、平成 25 年には不正送金の約 20%を占めたこの手口が、平成 26 年上半期には 7%に減少した。

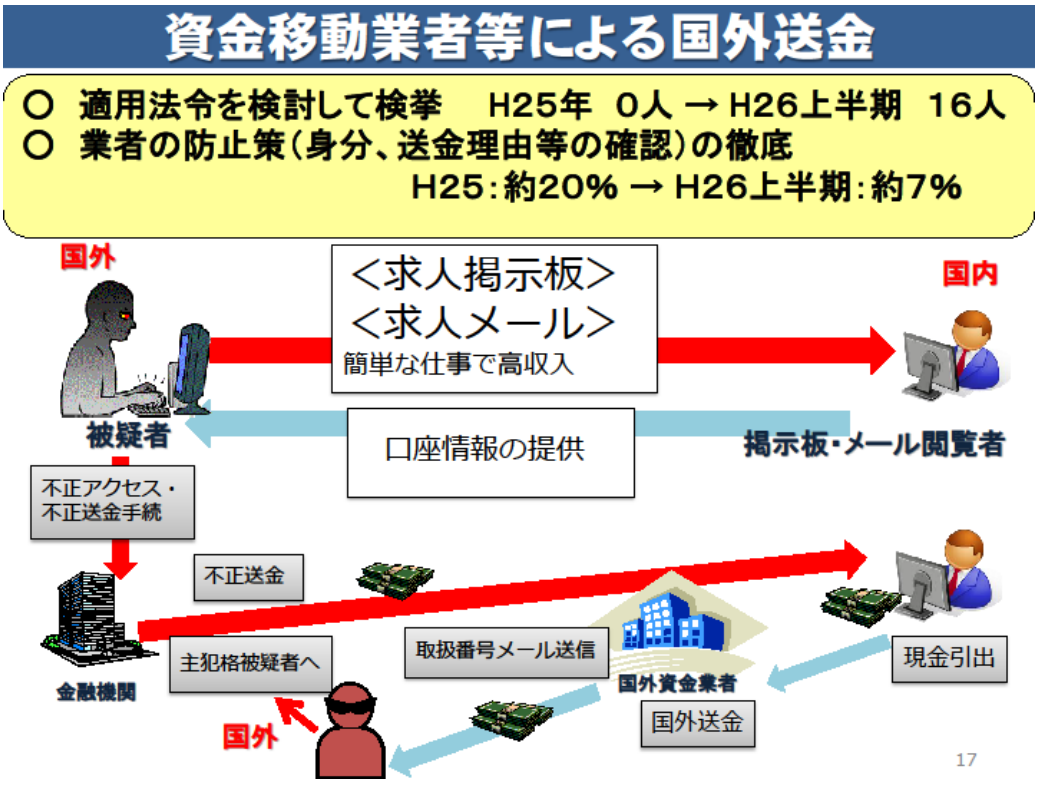


図 2　資金移動業者等による国外送金

三番目に多いのが、電子マネーを利用した不正送金であり、不正送金の 3.6%を占める。これは、不正送金先口座に異動した被害金をビットキャッシュ、Web マネー等の電子マネーに交換するものである。平成 25 年に不正送金が急増した当初、この手口が多発したので、メガバンクに対応策を取るよう要請したところ、ビットキャッシュや Web マ

ネー等の電子マネーの取扱いを停止した。この結果、この手口は一気に減少したのであるが、それに代わるように平成 26 年にはインターネット専用プリペイドカード、V プリカにチャージするという手口が現れるようになった。このインターネット専用プリペイドカードは、申込時本人確認なし、銀行口座登録不必要、購入後即時利用可、インターネットバンキング利用可といった、まさに犯罪者にもってこいのサービスである。現在、金融機関と対策を検討しているところである。

四番目に多い手口が商取引等へ充当するものであり、不正送金の 1.6%を占める。RMT(Real Money Trade:インターネット上のサイトでオンラインゲームに使用される仮想通貨等の現金交換所)を利用して不正送金被害金を仮想通貨に交換する、あるいはビットコイン交換所でビットコインを購入し不正送金被害金で支払うという方法でマネーロンダリングをするものである。

以上のようにいろいろな手口があるが、いずれも主犯格被疑者に捜査の手が伸びないように工夫されている。これらの現金化の手法が確立されているからこそ、不正送金事犯が成り立つのであり、警察としても金融機関等関係機関と協力して対策に努めている。

３．検挙状況

（１）検挙の罪名等

次に、検挙状況に触れる。サイバー課が担当しているので、サイバー捜査、すなわち、不正送金の送金元の IP アドレスに対する捜査やウイルスの解析による犯人特定による捜査といった捜査活動でどんどん犯人を逮捕しているということを想像されるかもしれないが、実はそのようなサイバー捜査で犯人を特定できたのは平成 26 年上半期で一名に留まっている。今日のサイバー犯罪者はそう簡単には捕まらない。IP アドレス等から送信元を追及していくと、ほとんどの場合、匿名プロキシサーバに辿りついてしまい、そこには接続記録が残されていないので犯人に行くつくことができない。そこで、昨年 11 月に全国の警察が連携して匿名プロキシサーバを運営する業者を一斉摘発した。この摘発により一時的に被害は減少した。今後も匿名プロキシサーバの立ち上げを把握して違法行為が認められれば摘発していく。

昨年上半期は、69 事件、133 人を検挙した(平成 25 年は、32 事件、68 人)。さきほど説明したとおり、出し子と国外送金事犯が大半を占めている。IP アドレスの追求等のサイバー捜査では犯人になかなか辿りつけないので、アナログ捜査により検挙している。検挙した犯人の 62%が中国人であるが、多くは出し子、口座売買である。日本人は 33%であるが、そのほとんどがマネーロンダリング行為である海外不正送金行為で検挙している。

罪名は、出し子については窃盗罪(払出盗)を、口座の売買については犯罪収益移転防止法を適用している。なかでも、始めから犯行グループに売り渡す目的で口座を開設した場合は、詐欺罪を適用している。集金役、すなわち、出し子から金を集める役割の者は、マネーロンダリング等を取り締まる組織犯罪処罰法を適用している。なお、この集金役が地下銀行役を兼ねている場合は、銀行法を適用している。マネーミュールについては、犯罪収益移転防止法を適用している。

すでに犯罪者による不正送金のインフラが確立されている。今後も上述したようなあらゆる法令を適用したアナログ的な取り締まりを、地道に粘り強く継続し、目の前の犯罪インフラをつぶしていくとともにサイバー的捜査も進めていかなければならないと考えている。

（２）不正な口座に送金する手口　-フィッシングと不正プログラム-

不正な口座に送金する手口について説明する。

まず、フィッシングであるが、これは、金融機関を装いメールを送りつけて偽サイト、すなわち、フィッシングサイトに誘導し、そこに ID・パスワードを入力させてこれを窃取し、この ID・パスワードを用いて不正送金をする手口である(図

3 参照)。不正送金以降の現金化の手口は前述のとおり。

平成23年の第一のピークは、ほとんどがフィッシングであると考えられるが、言葉の壁(ランゲージバリア・フィッシングサイトの日本語表現が不自然)と金融機関や警察による注意喚起等の諸対策が功を奏したと推測され、一旦は収まった。平成26年の年初にお客様のことを「貴様」と呼ぶサイトがあったがすぐに消えた。このように昨年の始めころまでは若干、日本語がおかしいサイトが残っていたが、現在はそのようなものはない。言葉の壁は完全に越えられている。今は、URL も本物そっくり、サイトのつくりも本物そっくりのものが出てきて、再び被害が増えてきた。なお、フィッシングサイトでは、ID・パスワードの他に乱数表の入力を求めるといった通常の画面ではない入力画面が現れるので、利用者がよく注意していれば、被害を防げるはずである。

フィッシングサイトの消長を理解していただくために、某メガバンクをターゲットとするフィッシングサイトの推移を示す。①平成 25 年夏ごろ、サイトが立ち始め、②同年 11 月、サイト数が増加、③平成 25 年 12 月から平成 26 年 2 月にかけて、サイト数が急増し猛威をふるう、④平成 26 年 3 月頃から減少傾向(金融機関の注意喚起のため)、⑤同年 4 月～5 月、発生せず、⑥同年 6 月にサイトが再確認され被害が発生している。

金融機関のホームページにおける注意喚起の徹底およびテレビ CM 等の効果により、フィッシングサイトによる被害はピークを越えたと見ている。しかしながら、未だフィッシングサイトは立っており、フィッシングサイトによる被害は減少したとはいえ、継続している。侮れない手口である。

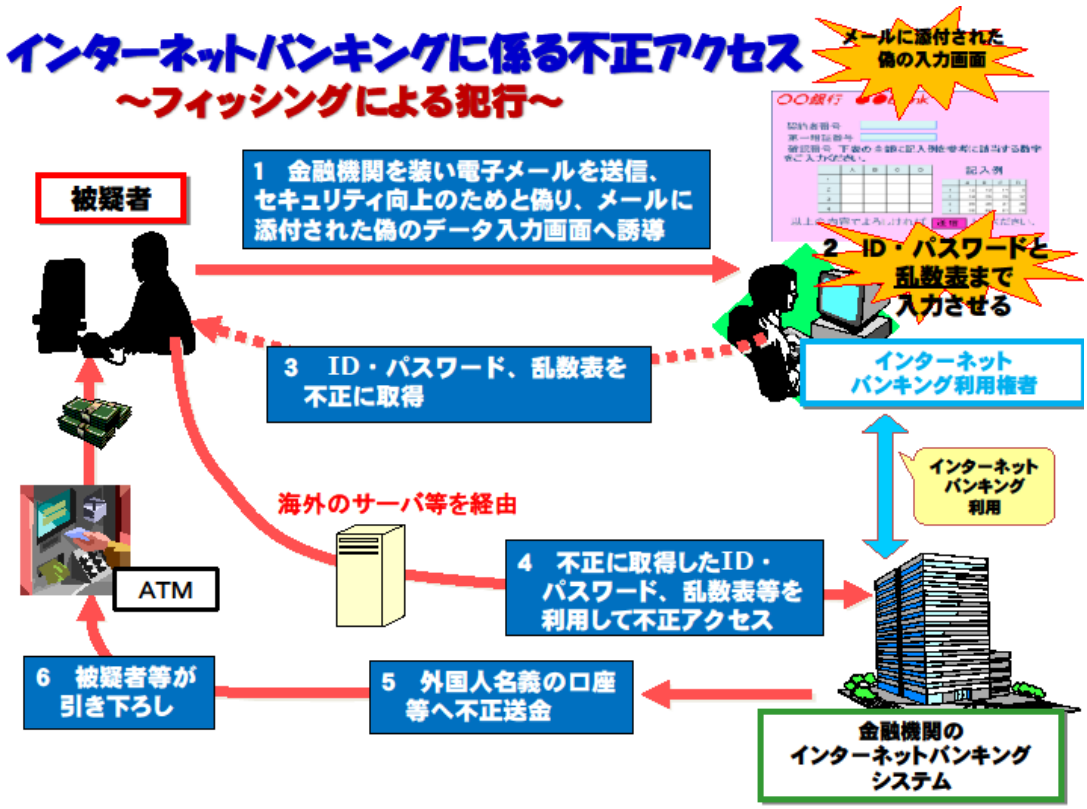


図３　フィッシングサイトによる不正送金の流れ

次に、ウイルスによる手口を説明する(図 4 参照)。何らかの手段でウイルスを感染させ、ID・パスワードを利用者が知らない間に取得し、これを用いて第三者のパソコン等を踏み台にする等して不正アクセスし、不正送金する手口である。不正送金以降の現金化の手口は前述のとおり。

ウイルスによって被害が多発したのは、ウイルスの高機能化が大きな要因となっている。インターネットバンキングへの不正アクセスに特化したトロイの木馬系の高機能不正プログラム(ウイルス)を総称して“Banking trojan”と呼ぶが、

その代表的なものに、“Citadel”と呼ばれるものがある。これは、正規の画面上に ID・パスワードを求めるポップ画面を表示させて、ID・パスワードを不正取得するものである。この亜種に電子証明書も窃取するものがある。また、“Game Over Zeus”と呼ばれる P2P 型のウイルスがある。通信先の特定など警察に捜査させないよう撹乱するために P2P 型をとったものと思われる。この他に高い機能をもつ新たなウイルスや、その亜種がどんどん出てきて対策が追い付かない。

このウイルスによる手口では、正規のサイトにアクセスしたにもかかわらず ID・パスワードを盗まれてしまうことが、被害を大きくする原因ではないかとみている。普通の人は正規のサイトにアクセスして ID・パスワードを盗まれるとは思わない。そのようなユーザの心理的な隙をついている。これらのウイルスに感染したときには、たとえば入力を求めるポップアップ画面の入力項目が増えるといった現象が現れるが、普通の人は気がつかない。

この高機能ウイルスでは電子証明書まで盗まれてしまうことがある。日本では電子証明書に対する安全神話があり、電子証明書は絶対的に安全だと思われているが、現実はそうではない。また、電子証明書と一緒に秘密鍵も盗まれている。法人口座は要注意である。電子証明書を盗む手口は以下のとおりである。犯人は、まず、電子証明書を盗もうとアタックする。ところがセキュリティが高くて盗めないと分かると、電子証明書を消してしまう。ユーザが再登録するときに、その再登録した電子証明書を盗んでしまう。この一連の処理をウイルスがやってのける。

この対策として、あるメガバンクでは電子証明書を IC カード化しようとしている。端末がウイルスに感染していても、証明書自体を外に出してしまえば安全だからである。また、あるメガバンクでは電子証明書を再発行する際に、窓口に連絡しなければいけないというルールを作って、この手口が使えないようにしている。

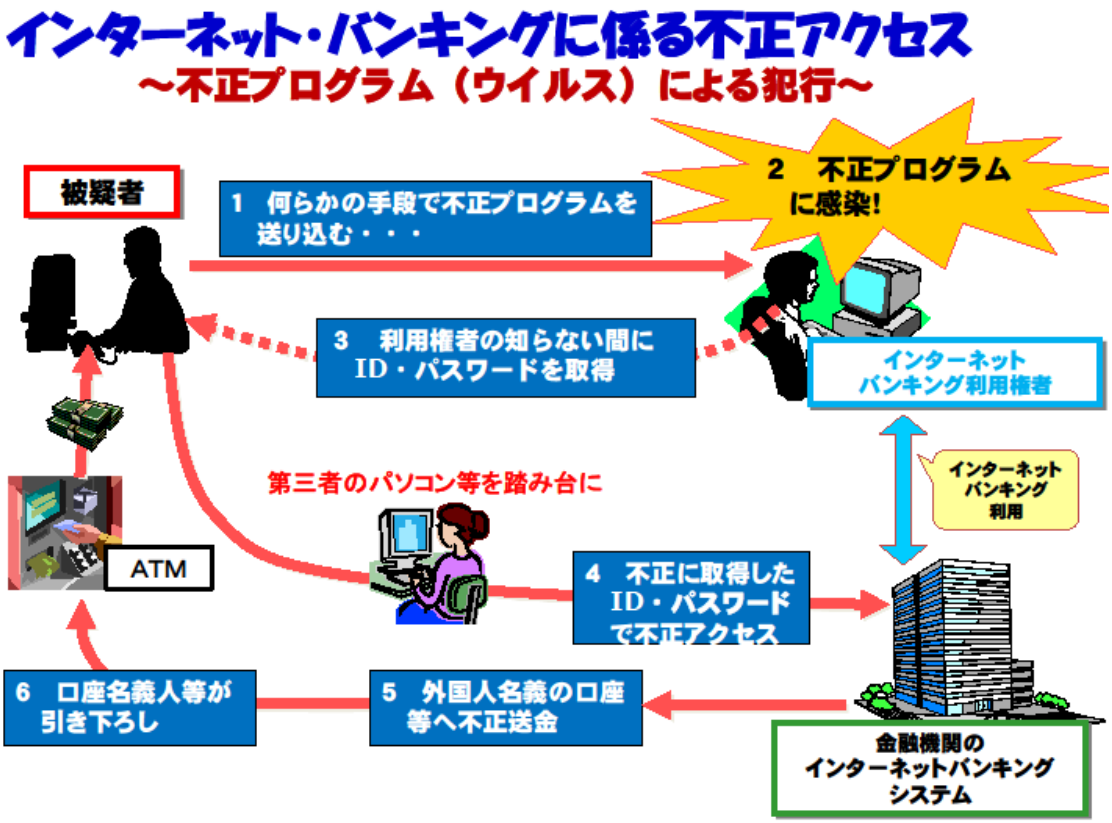


図 4　ウイルスによる不正送金の流れ

さらに、最近、ユーザの端末に感染したウイルスが、ウェブブラウザを乗っ取り、正しいセッションに便乗して不正操作を紛れ込ませる攻撃、“Man In The　Browser（MITB）”という自動送金型の手口も出てきた。ユーザが送金のため

に正規のサイトにアクセスしようとしてログインすると、いきなり「しばらくお待ちください」というプログレスバーが出てきて、しばらく待たされるが、その間にウイルスが裏で不正送金処理を進めている。最後に第二暗証番号を求める偽のポップアップ画面が出てくるが、この第二暗証番号を入れると万事休す、犯罪者の一時口座への不正送金が完了してしまう。

このウイルスに狙われると第二暗証番号が役立たない。あるメガバンクでは、振り込み先情報を入力させることで、新たな暗証番号を生成させるというハードウェアトークンを配っているが、まだそのシステムは稼働していない。そのようなカードを配っても顧客が面倒くさがってやってくれないというのが稼働しない理由の一つだそうである。

４．防止対策

（１）金融機関の不正送金未然防止対策に関する要請

インターネットバンキングにおける不正送金の未然防止対策について話を進める。これまでの話で、ウイルスが犯行に使用されていること、電子証明書ですら盗まれてしまうこと、また、MITB では通信が乗っ取られること等を話してきた。ただ単にパスワードの使いまわしは止めましょう、定期的に変更しましょうでは防げないことは分かっていただけたと思う。できることはすべてやるといった心構えで複合的な対策を取らなければならない。

一昨年、メガバンクに被害が集中したときは、メガバンクは、ウイルス対策や送金限度額の設定を下げる等の種々の対策を講じた。その結果、昨年は対策が遅れた地方銀行、信用金庫等の地域金融機関へと被害が移ってきた。まさにやりにくい対象から、やりやすい対象へと犯罪の対象が移った。実は、メガバンクも当初は腰が重かったと先任者に聴いている。なぜなら、サイバーセキュリティは、コストはかかるが利益を生み出せるものではないからである。企業にとって、なかなか投資しづらい。だが、時間はかかったが、利益か、信用かという狭間で揺れたメガバンクも英断をして各種対策をとっていただけるようになった。しかしながら、未だ対策がとられていない金融機関があり、そこが狙われているので、警察からも以下に述べる種々の対策をとるよう要請をしたところである。

金融機関がとるべき対策として、まず①ハードウェアトークンなどを配布することによるワンタイムパスワードの導入及び二経路認証システムの導入、②セキュリティ対策ソフトの無償配布、③送金限度額の引き下げを要請した。送金限度額に関しては、一昨年、ワーストワンになった某メガバンクは、汚名を返上したいということで数千万円から一気に 50 万円に引き下げた。この措置によって発生件数は増えても被害額はそれほど大きなものにならなくなった。

ここで問題になるのは、犯罪者がやりにくいと思う対策は、顧客にとっても面倒なものであるということである。セキュリティ対策ソフトを無償配布しても顧客側が面倒だから使わないと言ってくる。一手間かけることを仕方ないと思って実行するか否かが被害者になるか、ならないかの分かれ目になる。インターネットバンキングの不正送金対策は、顧客の面倒臭いという気持ちを如何に払拭させるかが鍵となる。

さらに、法人向け対策として金融機関に以下の要請をしている。①エクスポート機能の無効化や IC カード等への格納方式の採用といった電子証明書のセキュリティの強化、②事前登録先以外の振り込みの当日送金の制限、である。②の対策をとった某地方銀行では大きな効果を挙げている。

各金融機関はできるだけの対策をとっていただいている状況であるが、なかには、所詮インターネットバンキングは取引全体に占める割合が低く、手数料もわずかで、対策費用が高くつくということで全く対策をとらない金融機関もある。対策をとらずに放置している金融機関に対しては、不正送金問題が大きくなれば、監督官庁が出てくる可能性もあると考えている。

また、金融機関には、ユーザに対してインターネットバンキングに関し以下の注意喚起を行うこともお願いしている。

① インターネットバンキング利用端末へのセキュリティ対策ソフトの導入と、それを最新の状態に更新すること

② 基本ソフト(OS)、ウェブブラウザ等、インストールされているソフトウェアを常に最新の状態に更新すること

③ 不審な入力画面等が表示された場合は、ID・パスワードの入力はせず、金融機関等に通報すること

④ ワンタイムパスワードは、携帯電話のメールアドレスで受信すること

法人向けサービスの利用者に対しても、①送金限度額の引き下げ(高額な取引は年に数回だと思われるのでこれは可能であろう)、および、②不審なログイン履歴がないかをこまめにチェックすることの二つの呼びかけをしていただくよう金融機関に要請している。

町の小さな企業では、たとえば、決済端末は他の業務では使用しないというセキュリティ上の原則を適用しようにも、そもそも端末を複数所有し、目的別に分けて使うことが困難である。実は、そのような相手こそ注意が必要である。この小さな企業を相手にする信用金庫や信用組合は小回りが効くので、そのような企業には是非、直接、足を運んで指導していただきたいというお願いもしている。

なお、これからは顧客側も適切なセキュリティ対策をとっていないと補償の対象から外れるので注意が必要である。

(2) 警察の取組み

警察としては、最近のトレンドに則り、民間の知見を活用した捜査及び被害防止に取組んでいる。

先ごろ、産・官・学が協力してサイバー犯罪に立ち向かうための JC3(日本サイバー犯罪対策センター)という組織が立ち上がった。産官学が情報を持ち寄って、サイバー犯罪の捜査と被害の未然防止に活用することを目的としている。

また、従来からある金融機関の防犯対策基準に不正送金の防止対策を追加した。

さらに、アンチウイルスベンダー等と連携し、ウイルスに感染したサーバや端末に対してプロバイダー経由で注意喚起を行っており、8か月間のトータルで1万3千件の注意喚起をした。

昨年の目玉は、米国 FBI とユーロポール(欧州刑事警察機構)が中心となり、協力国の法執行機関が連携して、インターネットバンキングに係る不正送金事犯に使用される不正プログラム“Game Over Zeus”のネットワークを崩壊させる作戦、ボットネット(注)のテイクダウン作戦に参加したことである。このために用意された代替サーバに集められた情報を解析して参加国に提供した。日本においては、その情報をもとにプロバイダーに対して、契約者に注意喚起をするよう要請した。約15万もの端末がこの“Game Over Zeus”に感染していたということが確認された。未だに注意喚起は続いている。

(注)ボットネット:サイバー犯罪者がトロイの木馬等の不正プログラムを用いて乗っ取った多数のゾンビコンピュータにより構成されるネットワークのこと。

(3) 今後発生が予想されるサイバー犯罪

今後、発生が予想されるサイバー犯罪について触れておく。

まず、企業等に対する DDoS 攻撃である。欧米では10年以上前から発生している。この攻撃は、大量にデータを送りつけてサーバを止めてしまうもので、攻撃を止めてほしければお金を払えという恐喝の手段に使われている。サーバがダウンした際の顧客への補償や復旧の作業に必要な費用を考え、多くの企業がお金を払っているのではないかと考えられるが、報告は上がってこない。最近の DDoS 攻撃の主流は、かつてのようにボットネットを使って大量のメールを送りつけるのではなく、サーバがどれだけの負荷に耐えらるかを検証するサイトを使用している。比較的容易にこのサイトが使用できるので最近これを悪用する手口が増えている。今の時代、犯行ツールがネット上にごろごろ転がっており、容易にサイバー犯罪が実行できる。やっかいな時代になった。

何も知らない人が DDoS 攻撃に加担する可能性がある。ロジテックの一部のルータは初期設定では外部から認証用 ID・パスワードがまる見えで、パソコンが乗っ取られ、ボット化されて DDoS 攻撃に加担させられてしまう危険性がある。

次は、ランサムウェアである。このウイルスが添付されたスパムメールを受信し、添付ファイルを開くと、端末の中のデータが全て暗号化されて使用できなくなる。この時点で「暗号を解除してほしければ金を出せ」と言うメッセージが表示される。一種の身代金要求である。これらの動作を“CryptoLocker”というウイルスがやってしまう。最近、日本語バージョンが出てきた。今後、注意していかなければならない。

また、Pos 端末でクレジットカードを使うとクレジットカードの情報が盗まれてしまうという被害が米国で発生している。Pos 端末内で暗号化される前にクレジットカードの情報が抜かれてしまう。米国の大手スーパー「ターゲット社」では、これで1億1千万件のクレジットカード情報が流出した。この事例では、空調業者が持ち込んだ機器からウイルスが感染した。内部からの感染である。ウイルスは外部から侵入するだけではなく、内部からも感染することがあることに留意すべきである。日本でも Pos 端末でクレジットカードの情報を盗むウイルスが検知されているので注意が必要である。

さらに、スマホ内の情報を盗む偽アプリがすでに多数、発見されており、これからはスマホアプリを狙うウイルスに注意をする必要がある。

以上述べたように、常に新たな手口に目を光らせて対応できる準備をする必要がある。

おわりに

インターネットバンキングに限らずネット社会には危険が溢れている。日本のお金が犯罪組織に狙われているということが分かっていただければ、今日の話の目的は達せられる。5年後の東京オリンピック開催を視野に入れて、さらにサイバー空間の安全確保に努める所存であり、今後も皆様のご協力をいただけるよう、あらためてお願いする。

以上

[報告者注]当会報記事 注目情報：警察庁発表「平成 26 年インターネットバンキング不正送金事犯」参照

＜目次＞

2015.2

～「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６
2-2-4. 第三者への提供（法第２３条関連）

会員番号 6005 斉藤茂雄 （個人情報保護監査研究会）

※個人情報保護監査研究会注:「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」が、2014年（平成26年）12月12日付けで告示・施行されました。今回から本稿は改正版ガイドラインに沿って解説いたします。尚、改正部分は文中アンダーラインで表示しました。全てではありませんので、全文については、改正METIガイドライン本文を参照してください。

2-2-4. 第三者への提供（法第２３条関連）

（１）原則（法第２３条第１項関連）

法第２３条第１項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

１ 法令に基づく場合

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。

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。

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。

事業者は、原則として本人の同意を得ない限り、個人データを第三者に提供することはできません。

【第三者提供とされる事例】

事例1）親子兄弟会社、グループ会社の間で個人データを交換する場合

事例2）フランチャイズ組織の本部と加盟店の間で個人データを交換する場合

事例3）同業者間で、特定の個人データを交換する場合

事例4）外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】

事例）同一事業者内で他部門へ個人データを提供すること。

ただし、以下の場合は本人の同意なく第三者への提供を行うことができます。

（ｉ）法令に基づいて個人データを提供する場合

（ii）人の生命、身体又は財産を保護するために個人データの提供が必要であり、かつ、本人の同意を得ることが困難である場合

（iii）公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合

（iv）国の機関等への協力

（2）オプトアウト（法第２３条第２項関連）

> 法第２３条第２項
> 個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
> １　第三者への提供を利用目的とすること。
> ２　第三者に提供される個人データの項目
> ３　第三者への提供の手段又は方法
> ４　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

法律では、事業者は、オプトアウトを行っている場合には、本人の同意がなくても、個人データを第三者に提供することができます。ただし、公表している利用目的に、個人情報を第三者提供することが明記されていない場合は、第三者提供を行うことはできません。

【オプトアウトの事例】

事例1）住宅地図業者（表札や郵便受けを調べて住宅地図を作成し、販売（不特定多数への第三者提供））

事例2）データベース事業者（ダイレクトメール用の名簿等を作成し、販売）

※個人情報保護監査研究会注：「**オプトアウト**」とは、提供に当たりあらかじめ、上記の、法第23条第2項　1～4の事項を、本人に通知、または公表などをするとともに、本人の求めに応じて第三者への提供を停止する手順が明確になっている状態のことをいいます。

なお、JIS Q15001：2006規格（プライバシーマーク審査基準）では、通知し、又は公表するだけでなく、本人の明示的な同意がなければ第三者に提供することはできません。より厳しい要求事項となっています。

（3）第三者に該当しないもの（法第２３条第４項関連）

以下の（ⅰ）から（ⅲ）までの場合については、形式的には第三者に該当するものの、事業者と一体のものとして取り扱うことに合理性がある場合には、第三者に該当しないとしており、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができます。

※個人情報保護監査研究会注：今回のガイドライン改正では、「事業者と一体のものとして取り扱うことに合理性がある場合には、第三者に該当しないもの」とすべき、という考え方が補足されています。第三者に該当するかどうかの考え方の指針がより明確に示されたものといえます。

（ⅰ）委託（法第２３条第４項第１号関連）

> 法第２３条第４項第１号
> 次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。
> １　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合。

個人データの取扱いに関する業務の全部又は一部を委託する場合は、第三者に該当しません。

事業者には、委託先に対する監督責任が課されます。

事例１）データの打ち込み等、情報処理を委託するために個人データを渡す場合

事例2）百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

（ⅱ）事業の承継（法第２３条第４項第２号関連）

> **法第２３条第４項第２号**
>
> **次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。**
>
> **２ 合併その他の事由による事業の承継に伴って個人データが提供される場合**

合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合は、第三者に該当しません。

事例1）合併、分社化により、新会社に個人データを渡す場合

事例2）営業譲渡により、譲渡先企業に個人データを渡す場合

（ⅲ）共同利用（法第２３条第４項第３号関連）

> **法第２３条第４項第３号**
>
> **次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。**
>
> **３ 個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称につい て、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。**

個人データを特定の者との間で共同して利用する場合であって、以下の①から④までの情報をあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いておくとともに、共同して利用することを明らかにしているときには、当該個人データの提供を受ける事業者は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しません。

なお、共同利用か委託かは、個人データの取扱いの形態によって判断されます。例えば、グループ企業でイベントを開催する場合において、各子会社から親会社（幹事会社）に顧客情報を集めた上で展示会の案内を発送するときには共同利用となりますが、自社が保有するデータを利用して案内状を発送するために、グループ企業内の事業者に業務を依頼する場合は、委託であって、共同利用とはなりません。

【共同利用を行うことがある事例】

事例1）グループ企業で総合的なサービスを提供するために取得時の利用目的の範囲内で情報を共同利用する場合

事例2）親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合

事例3）外国の会社と取得時の利用目的の範囲内で個人データを共同利用する場合

事例4）企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合

※個人情報保護監査研究会注：共同利用は、第三者提供と異なり、本人の同意は必須ではありません。しかし、共同利用する企業名のリスト、代表して管理責任を持つ企業および責任者を明確にして、次に示す事項を、公表しなければなりません。

① 共同して利用される個人データの項目
本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。

② 共同して利用する者の範囲
「共同利用の趣旨」は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することである。したがって、共同利用者の範囲については、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。

事例）本人がどの事業者まで利用されるか判断できる程度に明確な形で示された「提携基準」及び「最新の共同利用者のリスト」等を、共同利用者の全員（全企業）が、本人が容易に知り得る状態に置いているとき

③ 利用する者の利用目的
共同して利用する個人データについて、その取得時の利用目的をすべて、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。

④ 当該個人データの管理について責任を有する者の氏名又は名称
開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称について、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。
ここでいう「責任を有する者」とは、共同して利用するすべての事業者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者をいい、共同利用者のうち一事業者の内部の担当責任者をいうものではない。

法第２３条第５項
個人情報取扱事業者は、前項第３号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

上記③利用する者の利用目的、及び④当該個人データの管理について責任を有する者の氏名又は名称、については、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することができます。
ただし、変更する前に、本人に通知又は本人が容易に知り得る状態に置かなければなりません。

また、上記①共同して利用される個人データの項目、及び②共同して利用する者の範囲、については原則として変更は認められません。ただし、次の場合は、引き続き共同利用を行うことができます。

【引き続き共同利用を行うことができる事例】

事例1）共同利用を行う事業者や個人データの項目の変更につき、あらかじめ本人の同意を得た場合

事例2）共同利用を行う事業者の名称に変更があるが、当該事業者の事業内容に変更がない場合

事例3）共同利用を行う事業者について事業の承継が行われた場合

※個人情報保護監査研究会注：今回のガイドライン改正のQ&A集に「共同利用開始後、途中から新たな事業者が共同利用に参入することはできますか。」という質問が追加されています。解説では「原則改めて共同利用手続をとる必要がありますが、本人がどの事業者まで利用されるか判断できる程度に共同利用者の範囲が明確にされている場合には、個別列挙が必要でない場合もあると考えられますので、その場合には、引き続き共同利用を行うことができるものと考えます。」 としています。

（4）雇用管理に関する個人データ関連

雇用管理に関する第三者提供としては、従業員が子会社等へ出向する際に、人事考課情報等に関する個人データを提供する場合や、労働者を派遣する際に、技術能力に関する情報等の個人データを第三者提供する場合があります。

- 提供先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。
- 当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。
- 提供先における保管期間等を明確化すること。
- 利用目的達成後の個人データを返却し、又は破棄し若しくは削除し、これと併せてその処理が適切かつ確実になされていることを事業者において確認すること。
- 提供先における個人データの複写及び複製（安全管理上必要なバックアップを目的とするものを除く。）を禁止すること。

※個人情報保護監査研究会注：出向や派遣などにおいては、通常企業間で労働者管理関係の契約を締結しますが、個人情報の取り扱いについても、上記に留意した取り決めを含めるよう留意する必要があります。

次回は、「2-2-5.保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止等（法第24条～第30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://1.33.170.249/saajpmsMETIGL/000METIGL.html

（↑バックナンバー目次のURLが変更となりました。）

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

■

＜目次＞

2015.2

支部報告【　近畿支部　第１５０回定例研究会　】

会員番号　1627　上村　智幸

１．テーマ　　ＩＴ－ＢＣＰの実効性を高める訓練・演習とその監査

２．講師　　日本システム監査人協会近畿支部会員　松井 秀雄 氏
（近畿支部　ＢＣＰ研究プロジェクトメンバー）

３．開催日時　　２０１５年１月１６日（金）　１９：００～２０：３０

４．開催場所　　大阪大学中之島センター　２階　講義室２０１

５．講演概要

当講演では、IT-BCPが有事の際に機能する「実効性」を高めるためにISO22301・ISO27031・IT-BCPガイドラインなどで求められている事項を紹介していただいた。訓練・演習に実機を使うタイプと机上で行うタイプの両方を紹介され、各々の長所・短所が明らかにされた。さらに、机上訓練の手法として一部の業界で採用されているDIG (Disaster Imagination Game)をIT-BCPへ応用した事例も紹介され、また、訓練・演習に取組んでいる組織に対する監査の要点について、システム管理基準を踏まえた説明がなされた。

（１）　ＩＴ－ＢＣＰの実効性を検証・向上するための推奨事項

・ISO での要求事項は、「事業継続マネジメント ISO22301」、「IT-BCM に関する ISO27031」などに訓練・演習・テストが記載されている。

・各種ガイドラインにおける推奨事項は、「IT サービス継続ガイドライン・改訂版」（経済産業省　平成 24 年）、「地方公共団体における ICT 部門の事業継続計画（BCP）策定に関するガイドライン」（総務省　平成 20 年）などにテスト・訓練が記載されている。

・「IT サービス継続ガイドライン・改訂版」では、テストの種類として、机上チェック、ウォークスルー、シミュレーション、ロールプレイング、実機訓練の5種類が挙げられている。

（２） ＩＴ－ＢＣＰ訓練・演習の実施状況

・民間企業における訓練・演習の実施状況は、

「本番機の停止を伴う訓練を実施しているか？」→「実施したことはない」が 83%

「ユーザ部門などを巻き込んで訓練を実施しているか？」→「実施したことはない」が 63%

を、それぞれ占めている（いずれも回答企業数 30 社）。

・自治体における訓練・演習の実施状況は、

「関係事業者を含めた大規模な実地演習実施」→都道府県（26 団体中）0%、市区町村（188 団体中）3.7%

「全庁で実地演習実施」→都道府県（26 団体中）0%、市区町村（188 団体中）4.8%

である。

・BCP 訓練・演習未実施の理由としては、「負担が多く実施できない」が 78%、「やり方がわからない」が 15%となっており、心配な状況であるが、「実施の必要性はない」が 0%であったことは一つの救いである。

（３） 実機テストで得られる気付きと改善

・実機テストにより発生した主な事象は、手順書の不具合（メーカー提出、自社作成の両方）、作業員の経験不足によるミス、システムの不具合であり、それぞれ、手順書の見直し、作業員の経験の蓄積、システムの不具合修正につなげている。

（４） 机上訓練で得られる気付きと改善

・有効な机上訓練実施方法として IT 版の DIG を考案した。DIG（Disaster（災害）Imagination（想像力）Game（ゲーム））とは、1997 年に開発された、一般市民が独力でも企画・運営できる簡易型の防災図上訓練ノウハウである。

・DIG の基本的な流れは、「①自然条件の確認→②都市構造の確認→③人的・物的防災資源の確認→④災害に対する強さ弱さの理解」であり、それを IT に応用した IT 版 DIG の流れは、「①外部インフラの確認→②内部インフラの確認→③適用業務単位に人的資源・バックアップ用 IT 資源の把握→④災害に対する備えがあるもの・ないものの理解」となる。

・IT 版 DIG の利点は、①外部インフラを含むシステム環境全体を可視化することで、詳しい知識がない人でも参加可能 ②手軽、簡単に実施できる ③「正解」がないため、色々な意見が出やすい などであり、注意点は、①確認できる内容に限界がある ②IT 版 DIG 不参加者への情報共有が難しい などである。

・「実機訓練」では、①本番機の稼働に悪影響を及ぼす危険性 ②テスト機での手順が本番機で使えるとは限らない ③訓練のためのシステム停止が難しい場合あり などのリスクを伴うが、「机上訓練」はそのリスクを低減できるため、先ずは机上訓練実施を推奨している。

・訓練・演習への取り組み方として、①先ずは IT 版 DIG ②次にテスト機、予備機を使った訓練 ③最終的に本番機を使った訓練を提案している。

（５） ＩＴ－ＢＣＰの実効性に関するシステム監査の視点

・IT-BCP の実効性に関してシステム監査の際に確認すべき事項としては、「組織体の長の承認」、「従業員の教育訓練」、「関係各部に周知徹底」、「見直しと更新」などが挙げられる。

（６） ＩＴ－ＢＣＰ「想定外」への備えは可能か？

・「想定」とは、物事を検討する範囲として仮に設けた制約事項である。

・「想定外」は起こり得ないのではなく、確率は低いながら起こる可能性がある。

・訓練の段階的高度化として、ステップ 1 では「手順書の内容に従って、作業が正しく完了できることを確認」し、ステップ 2 では「予め設定された手順の途中で条件が変更されても、正しく作業を完了できるかどうかを確認」する。これは、前記（1）テストの種類で述べた5種類のテストの4段階目「ロールプレイング」で訓練途中にテストシナリオに変更を加えて参加者に臨機応変の対応力を養う事が述べられているのに通じる話である。

６．所感

私はシステム監査業務に携わっており、コンティンジェンシープランについては、策定状況ならびに訓練実施状況を点検していますが、計画にはどこまで記載されていればよいのか、演習・訓練はどの程度やれば良しとするのか、大きな声では言えませんが、点検する側も懸念を抱きながら実施している部分がありました。また、訓練については実機を使用せず机上のみで済ませている企業もあり、その有効性には甚だ疑問を感じながら良しとしている部分もありました。しかし、本番環境の使用の難しさや机上訓練の利便性に改めて気付き、段階的に実施していくことの重要性を痛感しました。

講師とは、以前に仕事をご一緒させていただいたことがあって、その誠実さが非常に印象に残っていますが、今回の講演も興味深い話の進め方で、失敗談や時折ジョークを交えた本音トークなどもあって非常にわかり易く、参考となるものでした。

以上

＜目次＞

2015.2

注目情報（2015.1～2015.2）※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。

■ 警察庁「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況」を発表（2015/2/12）

警察庁は 2 月 12 日、「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を発表した。平成 26 年の発生状況は、1,876 件、被害額約 29 億 1000 万円（平成 25 年は 1,315 件、約 14 億 600 万円）で過去最高である。平成 26 年は、①被害が多くの地方銀行や信用金庫・信用組合に拡大し、かつ法人名義口座に係る被害が拡大、②不正送金処理を自動で行うウイルスの利用等手口の悪質・巧妙化、③資金移動業者を介して不法に国外送金する事犯が一昨年より減少、④不正送金先口座名義人の 64%が中国人といった特徴がある。

取締りの徹底により、115 事件、233 人（対平成 25 年比、+81 事件、+165人）を検挙している。また、金融関係団体との連携により多くの不正送金を阻止し、中国人留学生・技能実習生関係団体に対する指導・啓発の要請、ウイルス対策事業者等との連携による被害防止対策の推進を行っている。これらの措置により、平成 26 年下半期は、上半期に比し被害額が約 8 億円減少し、かつ、不正送金阻止率は、金額ベースで 31．4%（総被害額約 10 億 5800 万円に対して、実被害額約 7 億 2600 万円、阻止額約 3 億 3200 万円）に達している。なお、「不正送金阻止」とは、事前に凍結された口座への送金指示に対する送金処理の取り消し、法人サービスにおける当日送金の停止等により、金融機関が未然に阻止したものをいう。なお、平成 26年上半期の阻止率は、7.6%であった。

不正送金阻止状況

	被害額	実被害額	阻止額	阻止率
H25 上半期	約 2 億 1300 万円	約 2 億 300 万円	約 1000 万円	4.6%
H25 下半期	約 11 億 9300 万円	約 11 億 2700 万円	約 6600 万円	5.5%
H26 上半期	約 18 億 5100 万円	約 17 億 1000 万円	約 1 億 4100 万円	7.6%
H26 下半期	約 10 億 5800 万円	約 7 億 2600 万円	約 3 億 3200 万円	31.4%

当会報記事「第 199 回月例研究会報告『インターネットバンキングに係る不正送金事犯被害の実態と防止策』」を参照されたい。

警察庁発表資料の URL を右に示す。 http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

■ ＩＰＡ、「情報セキュリティ１０大脅威 ２０１５」を発表（2015/2/6）

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2014 年において社会的影響が大きかった情報セキュリティ上の脅威から「10 大脅威執筆者会」の投票によりトップ 10 を選出し、「情報セキュリティ10大脅威2015」として 2 月 6 日から IPA のウェブサイトで公開した。

URL：http://www.ipa.go.jp/security/vuln/10threats2015.html

「情報セキュリティ10大脅威 2015」は、2014 年に発生した情報セキュリティの事故・事件のうち、社会的に影響が大きかったと考えられる脅威から、情報セキュリティ分野の研究者、企業の実務担当者など 64 組織 96 名のメンバーからなる「10大脅威執筆者会」の審議・投票を経てトップ 10 を選出したものである。今年は近年の情報セキュ

リティの重要性や変化の速さを考慮し、順位を先行して公表した。また、例年通り 3 月にこの「情報セキュリティ10大脅威 2015」の詳しい解説資料を本ページで公開する予定としている。

＜今回選出された10大脅威＞
1 位「オンラインバンキングやクレジットカード情報の不正利用」
2 位「内部不正による情報漏えい」
3 位「標的型攻撃による諜報活動」
4 位「ウェブサービスへの不正ログイン」
5 位「ウェブサービスからの顧客情報の窃取」
6 位「ハッカー集団によるサイバーテロ」
7 位「ウェブサイトの改ざん」
8 位「インターネット基盤技術の悪用」
9 位「脆弱性公表に伴う攻撃の発生」
10位「悪意のあるスマートフォンアプリ」

■ ＩＰＡ、内閣サイバーセキュリティセンター（ＮＩＳＣ）と包括的な協力協定を締結（2015/2/10）

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、内閣官房内閣サイバーセキュリティセンター（NISC）との間で 2015 年 2 月 10 日、サイバーセキュリティ基本法等を踏まえた新たな包括的協力協定を締結した。今般、サイバーセキュリティ基本法（平成 26 年法律第 104 号）の施行により、「サイバーセキュリティ戦略本部」が設置され、また、NISC が改組され省庁横断の司令塔としての機能が強化されることとなった。これを受け、NISC と IPA の協力関係を見直し、IPA の実施する情報セキュリティ関連事業の成果はもとより、情報処理システムの信頼性向上及び IT 人材育成に関する事業成果についても包括的に対象に含めることとし、協力を実施していくものである。

本協定は、サイバーセキュリティ対策の推進に当たり NISC 及び IPA の間で包括的な協力関係を構築することにより、IPA に蓄積したサイバーセキュリティに関する広範な技術的専門的な知見の共有を図り、サイバーセキュリティに関する施策を総合的かつ効果的に推進することに寄与することを目的としており、脆弱性対応や暗号危殆化関連情報等に関する分野、標的型攻撃等に関する情報共有等に関する分野、政府機関等のシステム調達等に関するセキュリティ認証に関する分野、国民・企業等に対する普及啓発に関する分野等において協力を行うこととしている。

IPA 発表資料の URL を右に示す。http://www.ipa.go.jp/about/press/20150212.html

＜目次＞

2015.2

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第200回	日時:2015 年 3 月 4 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	「システム品質抜本改善、費用は40%減 ～日本空港ビルデング株式会社　販売流通系システム刷新の成果～」
	講師	日本空港ビルデング株式会社　管理本部 IT 推進室 主幹　堀 史晴 氏
	講演骨子	羽田空港国内線のターミナルビルを管理する日本空港ビルデングでは、店舗関連事業の売上高が全体の約 7 割を占めるなど、営業系（販売流通事業）の業務の 効率化や業績情報の可視化が重要課題となっていた。このため、2010 年の羽田空港再拡張を契機とし、営業系の基幹業務システム刷新に着手した。 これまでのシステム選定過程でも RFP を作成していたが、販売流通系システムの調達では、RFP の補足資料として新システム稼動後に用いる業務マニュアルを開示することで、業務の目的、あるべき手順等を明確にして取り進めた。 この結果、ＩＴコストは従来と比べ約 40%削減。経営・業務改革を後押しできる強力なシステム基盤が整備された。
	お申し込み	http://www.saaj.or.jp/kenkyu/kenkyukai200.html
第201回	日時:2015 年 4 月 28 日(火)　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	「企業 IT 動向調査2015（14年度調査） ～データで探るユーザー企業の IT 動向～」（仮題）
	講師	一般社団法人　日本情報システム･ユーザー協会 常務理事　浜田 達夫 氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申し込み	

■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 ）

＜目次＞

■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』

■公認システム監査人特別認定講習（東京・大阪）

開催中	公認システム監査人(CSA:Certified Systems Auditor)およびシステム監査人補(ASA:Associate Systems Auditor)の資格制度にもとづく、認定条件を得るための講習です。	
	概要	システム監査技術者試験と関連性のある各種資格の所有者については、特別認定制度に基づく本講習により、CSA・ASA 認定申請に必要な資格要件を満たすことができます。特別認定制度の詳細はHPで公開しています(http://www.saaj.or.jp/csa/shosai.pdf)。
お申し込み		講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saaj.or.jp/csa/tokubetsu_nintei.html)

【外部主催イベント・セミナーのご案内】

■ＩＳＡＣＡ東京支部 2015 年　月例会予定（東京）

日時: 2015 年 3 月例会　3/25(水)開催予定　18:30-20:10(受付開始:18:00) 2015 年 4 月例会　4/21(火)開催予定　19:00-20:40(受付開始:18:30) 2015 年 5 月例会　5/27(水)開催予定　18:30-20:10(受付開始:18:00)	
詳細	http://www.isaca.gr.jp/education/

＜目次＞

2015.2

協会からのお知らせ　【２０１５年度春期　公認システム監査人及びシステム監査人補の募集】

２０１５年度春期公認システム監査人及びシステム監査人補の募集の〔公告〕が協会のホームページに掲載されています。資格取得を企図されている各位はご参照願います。〔公告〕の概略は下記の通りですが、申請書等の資料のダウンロードなども、ホームページからお願い致します。(http://www.saaj.or.jp/csa/csaboshu.html)

---------- 記 ----------

2015年2月1日

特定非営利活動法人日本システム監査人協会

公認システム監査人認定委員会

2015年度春期　公認システム監査人及びシステム監査人補の募集について

〔公告〕

特定非営利活動法人日本システム監査人協会(以下、協会という)は、公認システム監査人認定制度(2002 年2月25日制定)(以下、制度という)に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」および「システム監査人補(Associate Systems Auditor：ASA)」を認定するため、2015年度春期公認システム監査人およびシステム監査人補の募集を行います。募集の概要と申請書等の資料の入手方法は、以下のとおりです。

1. 認定資格

公認システム監査人およびシステム監査人補とする。

2. 申請条件

(1)　認定申請者は、経済産業省が実施するシステム監査技術者(旧情報処理システム監査技術者)試験に合格していること。(制度2(5)特別認定制度に基づく特別認定講習の修了により、上記試験の合格者と同様に取り扱う者を含む)

(2)　公認システム監査人の申請者は、申請前直近6年間のシステム監査実務経験(実務経験みなし期間)が2年以上あること。

3. 認定申請

(1)　申請書類(記入方法は、募集要項参照)

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

申請書類	公認システム監査人	システム監査人補	記事
(1)認定申請書(様式1)	○	○	Word 形式
(2)監査実務経歴書(様式2)	○	－	Word 形式
(3)小論文 (様式3)	○	－	Word 形式
(4)宣誓書(様式4)	○	○	Word 形式
(5)資格証明(写)	○	○	
(6)申請手数料振込書(写)	○	○	
(7)面接試験	□	－	別途通知

（注1）〇印の資料一式を申請書類として提出する。

（注2）□印については、面接試験を実施する。

備考：公認システム監査人とシステム監査人補を同時申請する場合は公認システム監査人用の申請書類を提出する。

(2) 面接試験

申請書類審査後、認定委員会が別途指定・通知する日時場所において、面接試験を受ける。

4. 募集期間

2015年2月1日（日）～2015年3月31日（火）（同日消印まで有効）

5. 認定申請手数料（消費税８％を含む）

申請手数料	協会会員	非会員
(1) 公認システム監査人認定申請手数料（注1）システム監査人補と同時申請する場合も手数料は同じです。	21，000円	31，500円
(2) システム監査人補が申請する場合の公認システム監査人認定申請手数料	10，500円	15，750円
(3) システム監査人補認定申請手数料	10，500円	15，750円

6. 資料の入手方法

【個人情報の取り扱いについて】 を 【同意】して以下を表示

(1)「公認システム監査人、システム監査人補 募集要項」

ダウンロード（PDF 形式）

(2) 申請書等様式一式

・認定申請書（様式1）：Word 形式

・監査実務経歴書（様式2）：Word 形式

・小論文（様式3）：Word 形式

・宣誓書（様式4）：Word 形式

(3) 公認システム監査人認定制度のダウンロード

・PDF 形式

(4)「公認システム監査人制度」創設のお知らせ（2002 年7月1日）のダウンロード

・PDF 形式

(5) 特別認定講習に関する情報

（・特別認定講習機関認定については参照）

以上

＜目次＞

2015.2

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。

・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

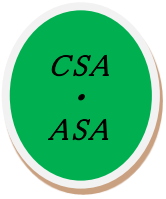
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・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。

・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。

・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。



・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

・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

・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＞

2015.2

【　ＳＡＡＪ協会行事一覧　】

赤字：前回から変更された予定

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
2 月	5 日 理事会:通常総会議案承認 **20 日 第 14 期通常総会・特別講演** 25 日 法務局:資産の変更登記、活動報告書提出 **28 日 年会費納入期限**	CSA・ASA 春期募集(2/1～3/31) 28 日-3 月 1 日 事例研:第 25 回システム監査実務セミナー(前半)	
3 月	2 日 東京都への事業報告書提出 2 日 年会費未納者宛督促メール発信 4 日 認定 NPO 法人東京都による調査 12 日 理事会	4 日 第 200 回月例研究会 14-15 日 事例研:第 25 回システム監査実務セミナー(後半)	
4 月	9 日 理事会 末日 法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査	19 日 2015 年春期情報技術者試験
5 月	14 日 理事会 29 日 会費未納者チェック	認定委員会:新規 CSA/ASA 面接	
6 月	1 日 会費未納者督促状発送 11 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)	10 日 新規 CSA/ASA 承認	
7 月	8 日 支部助成金支給 9 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〕	14 日 支部会計報告〆切
	以下は、2014 年に実施した行事一覧です。		
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 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 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 14 日 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/10〆切) 18 日 2015 年度年会費請求書発送準備 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	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	6 日 法制化検討 PT 事前打合せ 6 日 事例研:第 16 回課題解決セミナー 10 日 CSA/ASA 更新手続案内メール 16 日 第 198 回月例研究会 20 日 CSA 認定証発送 21 日 第 25 回 CSA フォーラム	13 日 東北支部:支部総会
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	7 日 16:00 総会資料(〆) 8 日 理事会:通常総会資料原案審議 9 日 総会開催案内掲示・メール配信 19 日 会計:2013 年度決算案 24 日 会計:2013 年度会計監査 26 日 総会申込受付開始(資料公表) 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〕	10 日 会計:支部会計報告期限 16 日 近畿支部:支部総会

※注　定例行事予定の一部は省略。

＜目次＞

2015.2

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

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。2 月号から 4 月号までは、「マネジメントシステム内部監査におけるシステム監査人の役割」をテーマといたします。皆様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 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」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、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＞