■第一回　有料の市販セキュリティソフトは必要ないかも
無料ソフトだけで「どこまでできるか」（2010 年 9 月）

何もかもが日進月歩である。今買ったモノが、すぐに後発製品に追い越されてしまう。こうなると買い控えをしていた方がいいのではないか、ついそう思えてしまう。セキュリティ対策製品についても例外ではない。聞くところによると、マイクロソフト社製の標準品 Security Essentials でかなりのところまで実現できると言うではないか。さっそく aism 談義が始まった。

■第二回 システムリソースの保守料金にまつわるセキュリティリスク（2010 年 11 月）

保守契約については、どの企業についても悩みが多いようだ。そこで aism ネットクラブでは、システムリソースに関する保守契約／保守料金について、現状の問題点を挙げて議論してみることとした。まずは会員相互の位相を合わせるために、aism 会員に向けたアンケート調査を実施してみた。結果、実に様々な保守問題が存在していることが、改めて確認された。一口に「システムリソース」と言っても、実に様々なリソースに関与していること、したがって、保守問題も、そのリソースの数だけ存在していることが確認できた。位相合わせが目的だったアンケートなのだが、実際の保守問題の具体論に入るや、以外や簡単には収束しそうにない。

■第三回　クラウドの仮想化サービスに潜む課金制度と保守料金問題（2010 月 12 月）

クラウドサービスが絶対的に安いということはない

保守契約および保守料金に関する議論は、クラウドサービス環境での課金問題へと発展してきた。仮想化、標準化、自動化とクラウドコンピューティング環境を実現する要素テクノロジーが力説されている程度で、統一されたサービスレベルの提案もできていない。官公庁などでは新興宗教的に「クラウドは安い」と信じ切っているようだが、まさに全体像を把握した上での結論ではない。aism ネットクラブで討議を始めたところで早くも「クラウドサービスが絶対的に安価というわけではない」の認識が出てきている。少なくとも、本格的な活用を始める前に、セキュリティ問題だけでなく、安いとされる料金課金制度の確認と確立をベンダー側に求めていく必要がありそうだ。

■第四回　「所有から活用の時代」はどこまで本当か
リスクがないなら万々歳（2011 年 1 月）

まだまだ、所有を止めるわけにはいきそうにない

クラウドサービスだけではなくアウトソーシングサービスの活用全般について言えることだが、どこまでを自前でやって、どこからを他人任せとするかは、今までもそして今後とも非常に大きな課題である。「所有の時代から活用の時代」などとクラウドサービスを売り込む側は、我が意を得たりと得意満面である。そこに何のリスクもなければ「御節御も

っとも」なのだが、そうは問屋が卸さない。システムリソースの保守課金問題を検討し、そこにリスクはないかと検証を始めた aism ネットクラブだが、出るは出るは、クラウドサービスに潜む問題点や課題が次々と出てくる。やはり、ビジネスコアの部分をはじめ、情報システム展開で全てのリソースの所有を停止するにはリスクが大きいようだ。合わせて、コストの殿堂と目されてきた情報システム部門／データセンターの存在が、実は大きなプロフィットセンターとして見直される可能性もあるという見解までも出てきた。

■第五回　本物のクラウドサービスの確認と課金設定の仕方／され方（2011 年 2 月）

何故クラウドサービスは従量課金が可能か

クラウドサービスが普及しているという喧伝から、実際のクラウドシステムの導入事例を見てみると、改めて「クラウドサービス／クラウドコンピューティングって何だ」という気がしてくる。酷いものになると、単なるアウトソーシングサービス、データセンターサービスをクラウドサービス／プライベートクラウドコンピューティングだといっているに過ぎないものもある。まあ、この業界の特有の「横並び戦術」はいつものことだが、将来的な成長性が認められるものから、期待感のなさそうなものまでいろいろあるようだ。改めて課金問題の本質を探るとともに、クラウドサービスの基本ポイントとは何かを検証してもらった。aism ネットクラブで討議は、アウトソーシングサービスの活用全般を今一度棚卸し直してみることも含めた議論に発展してきた。

■第六回　戸惑う日本ベンダーのクラウドビジネスと
クラウドサービスとしてのＢtoＣビジネス（2011 年 3 月）

クラウドの課金体系の話から、いろいろな話に展開してきているが、この辺で一回全体を整理して見たいと思う。2009 年 9 月号から始まり、５回にわたり、我々の議論の一部を紹介させていただいてきた。それぞれの回で述べさせていただいた要点をまとめてみた。

■第七回　一躍本命ＯＳに躍り出た Android と
これからの情報システムリスク（2011 年 4 月）

Win OS と同じ道を行くのか

圧倒的な市場占有率であった Windows OS を追い抜き、普及個数で一躍世界一となったフリーソフトウェア OS Android。その理由は、PC をはじめとして携帯電話を含めたあらゆるモバイル端末を普及範囲とするからだ。一方、従来の携帯端末は厳しいハードウェア性能の制約から、OS およびソフトウェアは非常にコンパクトに設計される必要があった。どうしても独自 OS／独自ソフトウェアにせざるを得ない理由だった。Android はこの常識を一変させようとしている。フリーかつオープンで、万人が共有できるソフトウェア開発環境を実現したからである。こうなると、フリーではなかったがデファクトスタンダードとして世界中に普及してきた Windows OS と同じ情報システムリスクが発生する可能性が出てくる。aism ネットクラブも傍観しているわけにはいかない。

■第八回　スマートフォンの普及と通信断絶

そして、我が国のビジネスコンテンジェンシープランの実力（2011 年 5 月）

3 月 11 日の東北関東大震災では、実に多くの犠牲者が出ている。行方不明者の数も確定していないほどだ。改めて犠牲者の皆様の冥福をお祈りするとともに、被災された方々に心よりお見舞い申し上げたい。直接的被災でないにしても、その影響を受けていない人はいないと言えるほど、今回の震災で日本人の受けた打撃は大きい。それは地震による家屋、施設、交通機関の倒壊だけでなく、巨大津波によって電力／ガス／水道のライフライン、オフィス／工場／農地／港など、あらゆる生産ラインが、根こそぎ倒壊したこと、そして追い打ちをかけた格好での福島第一原発事故。あらゆる面でセキュリティ対策とは何かという問題が大きくのしかかってきている。これまで多くの企業で取り組んできたビジネスコンテンジェンシープラン（BCP）をはじめとするセキュリティ対策を見直してみる必要があるだろう。aism としても、様々な角度から取り組んでいかなくてはいけないテーマ／課題だと認識している次第である。先月号で Android について、携帯各社の戦略に触れながら、その動向について紹介させていただいた。携帯電話における Android 自体が持つ課題、Android が搭載されることにより、我々利用者が享受できるサービスには、どのようなものあるだろうか。携帯電話の動向に詳しい aism 会員から報告があったので、今回はそれをベースに、今現在提供されているもの、将来的に期待されるものを含めて、報告させていただくこととする。aism 会員間の議論でも、携帯電話を電話機の延長で捉えることが多かった我々だったが、ネットワーク端末という形で位置づけから、発想の違いというか、当方の発想の乏しさを思い知らされる内容で、議論はなかなかに尽きそうにない。そして最後に、震災後初めて開催された aism オフ会での談義も報告させていただくことにした。能書きはこのくらいにして、まずは読み進んでいただきたいと思う。

■第九回　無尽蔵の巨大 CPU パワーによる

ハッキング時代の到来とリスクマネジメント（2011 年 6 月）

何故、ソニーの個人情報漏洩は防げなかったのか

これまで、aism ネットクラブでは、市販のウィルス対策ソフトウェアに対し、マイクロソフト社が無料提供している MS Essential の効用、クラウドコンピューティングサービス時代のソフトウェアライセンス管理、クラウドサービスの保守費用および課金問題等を論じてきたが、とりわけ、クラウドコンピューティングの根源的な絶対必要要素は、IT インフラ要素ではなく、アプリケーション機能要素であることの確認をしてきた。そうした様々な流動的な情報システムリソースの変遷、環境変化の中にあって必要とされるリスクマネジメントとは何かを追求してきている。クラウドが抱えるリスクや Android OS のセキュリティ上の脆弱性について、前回、前々回と、その周辺の技術動向等から、aism メンバーの切り口から洞察してきた。先般行われたコンピュータテクノロジーの関連ショウでも、Android OS をベースとしたスマートフォン関連商品のスペースが大きく割かれていた。さて、周知のことだろうが、ソニーが全世界規模でハッカー攻撃を受け、1 億人分を越える

個人情報が漏洩するという事件が起きた。これは漏洩というより、盗難といった方が正しいかもしれない。事件の概要を簡単にまとめてみると以下のような事件である。ソニーの子会社のオンライン･サービスが不正侵入を受けて､大量の個人情報が流出してしまった。また、ソネット・ポイントの不正利用等、ソニーおよび関連企業がサイバー攻撃の対象とされた事件である。犯人は、偽名でアマゾン EC2 のレンタルサーバーを契約し、このサーバーを用いてサイバー攻撃を仕掛けたと言われている。個人情報の流出件数については､1億件以上とも言われているが、正直、その全貌は判っていないのが実状のようだ。今回の事件は何故起こったのか、何が足りなかったのか、防御の方法はあったかを今一度考えてみたいと事務局としても考えていたところが、aism の例会でも、誰ともなく、その話題に議論は集中した。多くは、マスコミで報道されている内容を確認するような議論が多かったが、一般報道ではあまり触れられていないポイントと切り口での議論があったので、紹介させていただくこととする。

■第十回　多彩な部品パッケージ商品の台頭基本は

システム全体のセキュリティ対策（2011 年 7 月）

木を見て森を見ずとか、木を見て山を見ずとか、言われ方はいろいろとあるが、目先のことだけを見て、それを全てと判断してしまう無責任ぶりが目に付く一方、あるいは、見えているもの以外は知りませんと、端から全体に対する責任から逃避する態度、言動がある。いずれにしても、部分のことしか自らの範疇としない姿勢が横行している。セキュリティ対策についても同様である。当該範囲を限定してのセキュリティ対策でなく、システム全体のセキュリティ対策をどう追求していくか。この基本点を忘れてはならない。

■第十一回　Android 端末を検証せよ

ビジネス分野は時期尚早か、今すぐ使えるか（2011 年 8 月）

利便性に注目することは非常に大事なことであるが、合わせて、そこに潜む問題点を考慮しなくてはならないところが悩ましい。安価で便利な先端端末の導入は、システム関係者の永遠の課題である。iPad の活用、Android 端末への期待が高まっているのも、その例外ではない。いつものように利便性が先行／強調されている先端端末だが、さっそく検証してみることとした。どうしたらビジネスアプリケーションに使えるか、システム全体のセキュリティリスクを軽減できるかが最大のポイントである。

■第十二回　Android 端末を検証せよ　その２

ビジネス分野で今すぐ使うための考え方（2011 年 9 月）

どこにでも新しもの好きはいる。また､Android OS が注目されていることも確かである。かといって、藪から棒に採用し、既存システムに組み入れて良いというわけではない。それが、aism メンバーによる Android 検証の立ち位置である。しかしせっかちな上司の要求で、不安定な Android 環境で独自のアプリケーション開発を強烈に迫られているシステム

担当者が出てきている。改めて問題点を整理してみた。

■第十三回　Android 端末周辺を検証せよ　各種 OS の適材適所がポイント(2011 年 10 月)

相変わらずと言ってしまえばそれまでだが、携帯電話／タブレット端末の市場展開は早い。特に、Android OS 搭載のスマートフォン／タブレット端末の新製品ラッシュが続いている。次から次へと、出てきては消えていく。活用サイトも所有ベースも限りなく個人ユーザーではあるが、将来的な B to C 市場の展開を想定すると、企業情報システムサイトからも十分に視野に入れておく必要がある。それが悩ましい点である。特に注意すべきは Android OS 以外の OS 製品も数多く存在し、これからも新登場するであろうことである。「適材適所の OS 適用」、これが近未来の大きなポイントになりそうである。そして何と言っても注目するのは、これまで圧倒的な市場シェアを確保してきた WindowsOS 陣営の動向である。最新の Windows Phone7.5 の動向も報告しておきたい。

■第十四回　サイバー攻撃を検証せよ　データベース管理周辺まで視野に(2011 年 11 月)

利便性が高く、経済性もある。今、携帯電話／タブレット端末の市場が白熱している一番の理由である。いつでも、誰でも、どこからでも欲しい情報にアクセスすることの飽くなき要望があるからだ。しかしその利便性と隣り合わせのセキュリティ問題、特に Android という話題の OS 周辺に潜むハッキングなどの不正行為を忘れてはならない。本欄における検証／警鐘の背景である。政府も動き出したようだが、携帯／タブレット端末サイドの検証だけでは不十分である。ちなみに、我が国の防衛産業、重工業産業をターゲットにしたサイバー攻撃が多発しているが、その対応策は情報システム全体の中枢部分から見直すものでなくてはならない。中でも、重要情報の中核であるデータベース管理周辺のセキュリティ対策を含めて、今一度、根本的に検証してみる必要がある。

■第十五回　Android 端末周辺を検証せよ
データ管理はどこまでできているか（2011 年 12 月）

直接エンドユーザーが操作する端末マシンであるだけに Android OS フォンやタブレット PC が注目されているが、実際にはこれら端末マシンがアクセス可能なデータ管理がどこまでできているか、セキュリティ対策がどこまで行き届いているかが要の問題である。データベースの統合化を果たし、データの一元管理化を図ることで、セキュリティ対策はどれだけ推進できるか、業務監査の観点から今一度見直してみるべきだろう。

■第十六回　データベースの統合化は
セキュリティレベルの向上策でもある（2012 年 1 月）

オリンパス社の会計監査の虚偽報告は、日本中を驚愕させた。情報システム化がこれだけ進展した中で、これほど杜撰なシステム監査が存在していたのかという驚きである。と同時に、企業組織におけるセキュリティ対策とは、企業リスクを回避する手段であるとさ

れてきたが、その認識を覆す行為に経営トップが直接関与してきたという事実に驚いた。もちろんシステム監査が万能ではない。限界はある。今一度、原点に戻ってみたい。

■第十七回　東証、セキュリティ監査の根拠を否定

オリンパス事件で誤った判断（2012 年 2 月）

オリンパス社の会計監査結果の虚偽報告が日本中を驚愕させたと思いきや、今度は、こともあろうにこのオリンパスの上場継続を東証が認めてしまった。これほど公然とした法律違反はない。これでは、企業組織における会計情報システム上のセキュリティ対策を根底から否定することになる。何でもあり（許される）と宣言したようなものである。東証は、ただちに過ちを認め、本来の社会的責務を全うする道をとるべきである。一方、勢いが増しているのが Android 市場である。Android のアドバンテージは全てオープンであること。事業者はどんどん独自のカスタマイズができる。やりたい放題での市場開拓ができる。しかし、スマホ戦争は 3～5 年ぐらいで決着がつくだろうという分析もある。最初（今）の Android 関連商品は同じように見える（例えば、バラ色の花）が、間もなく種類の違う花がたくさん出来て、コストも横ばいになり、その時点で優劣が決まり決着がつくという。