NISC NEWS

第5号（２００６年9月４日発行）
内閣官房情報セキュリティセンター
National Information Security Center (NISC)

★目次

1. 情報セキュリティ施策紹介

【高セキュリティ機能を実現する次世代OS環境の開発について】

このほど、産学官の複数の研究機関による総合的な推進体制の下で**「高セキュリティ機能を実現する次世代OS環境の開発」**が進められています。

本開発は、ITの信頼性確保のための喫緊の取組みであり、**内閣官房情報セキュリティセンターとしても積極的に推進する施策**です。

本開発では、行政機関からの情報漏洩等、情報セキュリティを巡る問題が多発し、情報セキュリティ確保の取り組み強化が求められる中、

① Windows等の既存OS環境で提供されるセキュリティ機能に加え、**OSから独立した形でセキュリティ機能を実装**し、同時にOS及びアプリケーション等からなる**現在の利用者環境を活用可能**な、次世代のOS基盤環境の確立を目指します。
② **政府機関（内閣官房情報セキュリティセンター等）における実運用**を前提とします。
③ **優秀な若手研究者による集中的研究開発方式**を通し、**OS開発能力を有する人材を育成**することを目指します。

（参考１）開発内容のポイント

A) **Windows、Linux等の現在の利用者環境をゲストOSとして稼働可能**とし、同時に情報セキュリティ機能を利用者環境に依存しない形で集約的に提供する**仮想機械（VM：Virtual Machine）機能**と、これを稼働させるための**最小限のOS機能**（以下、併せてこれら機能を「セキュアVM」と呼ぶ）を開発します。

B) 利用者はゲストOSであるWindows等が提供する環境で業務を実施しますが、システム運用上の要となる**情報セキュリティ管理機能の基本的な部分は、セキュアVM側で多くを実現**し、ゲストOSに依存しない管理環境を構築します。

C) 統一のIDを利用してのPC起動管理、そのIDを利用してのハードディスクやUSBメモリ等の暗号化、さらにはVPNを利用した通信経路の暗号化などを、セキュアVMで実現し、**情報漏洩等のリスクを低減**します。将来は政府職員に平成18年度から導入が予定されている国家公務員ICカード等との連動も図ります。

D) **IPv6やそのほかの新しい技術を導入するための基盤環境**としても、このセキュアVMを活用します。

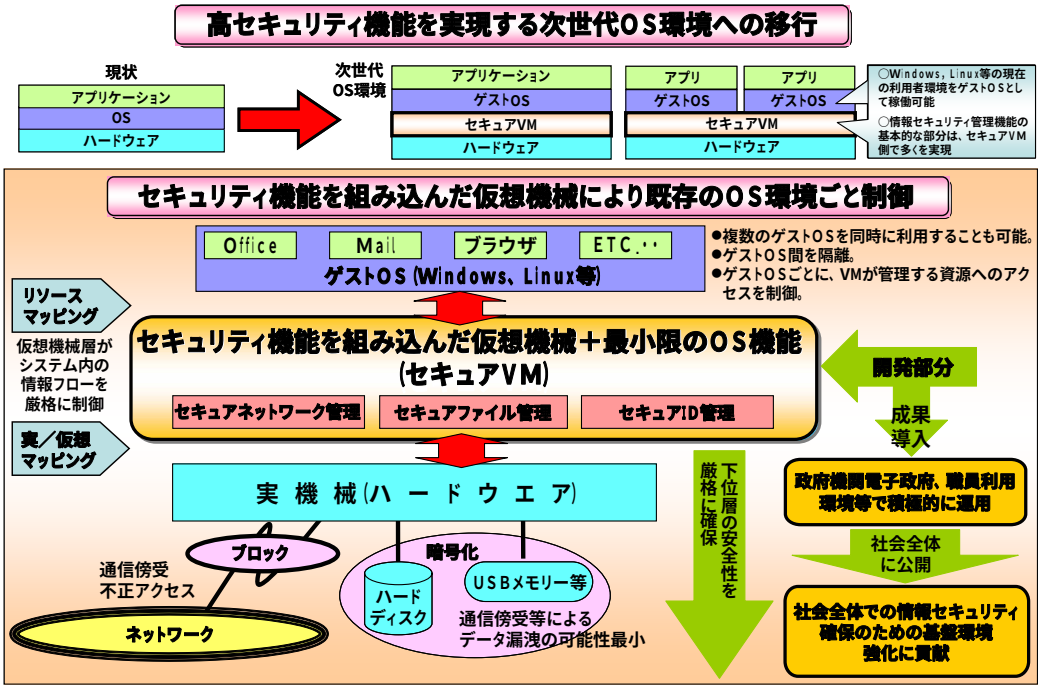

図１　セキュアVM及びその周辺に係る開発内容

（参考２）開発実施体制

全体の取りまとめを筑波大学が担当し、システム開発は**電気通信大学**、**東京工業大学**、**慶応義塾大学**、**奈良先端科学技術大学院大学**及び**豊田高専**による学術研究組織と民間企業（**富士通**、**NEC**、**日立製作所**、**NTT**、**NTTデータ**及び**ソフトイーサ株式会社**等）が担当します。同時に政府機関での利用を考えた場合の技術仕様、運用環境仕様について、内閣官房情報セキュリティセンターと協働して定めることで、実運用環境からの乖離が生じないように開発を行います。

また、研究開発の推進に当たっては、**独立行政法人情報通信研究機構（NICT）**、**独立行政法人情報処理推進機構（IPA）**ほか、産業界との連携を図ります。

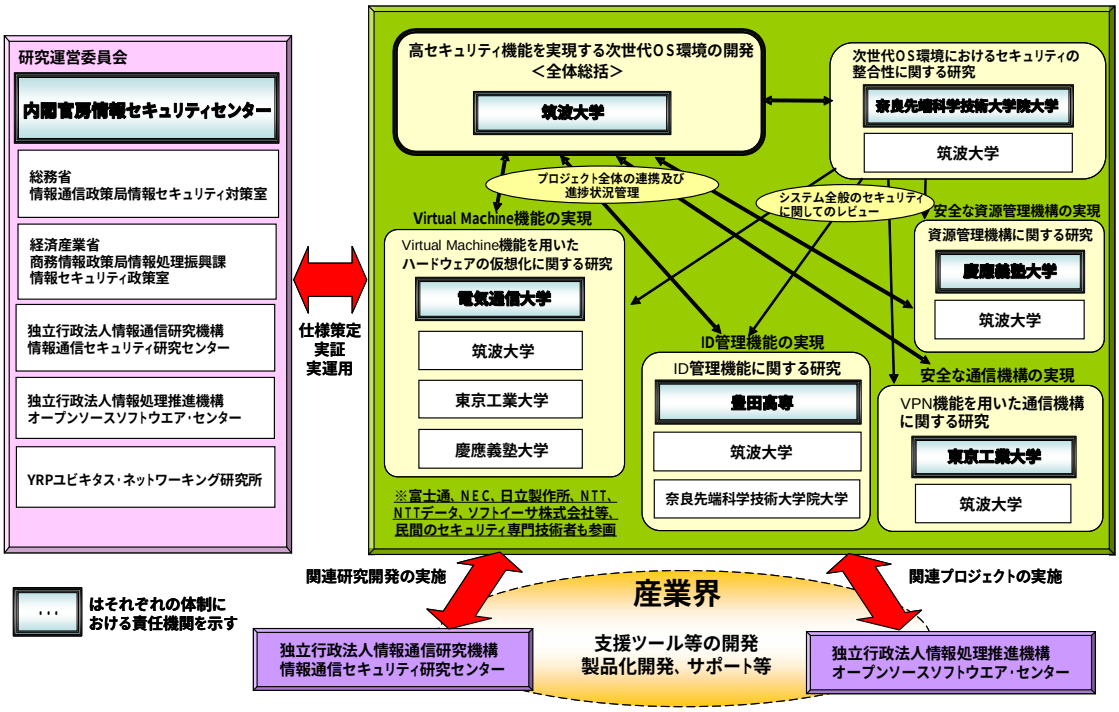

図２　セキュアVM及びその周辺に係る開発実施体制図

2．【補佐官ノート】「情報セキュリティにおける次の一手とは」

【あなたは何を持っているのか】

情報セキュリティ対策を設計する時に必ず行わなければならないのが、棚卸し作業である。一つは情報処理機器について、もう一つが情報資産のそのものについて、どのようなものがあり、その管理を誰が行っているのかに関する正確な情報を収集する作業だ。この棚卸し作業は、必ずしなければならないが、とてつもなく大きな面倒さがあるので、なかなか手を出したくない作業であるのも事実だ。ましてや定期的に棚卸し作業をしようとすると、現場の抵抗が余りにも大きくなってしまうことがある。しかし、これらの抵抗に挫けずに、管理作業の出発点として何としても行わなければならない。

この棚卸し作業で、更に問題を複雑にしているのが、情報資産の登録管理システムをどのように作るかという問題である。多くの組織では、情報資産として、最終成果物の登録システムは作ることが可能だろう。しかし、文書等の制作過程の文書の存在までも考えた場合の、バージョン制御までを含んだ管理システムを考えるのは相当難しい。さらに統一的な採番システムの構築と実施など、ディジタルでの情報資産生成に適合した管理システムをどのように構築するかを真剣に解決することが必要となる。

多くの組織では、この登録システムでの不備を理由に、情報資産の棚卸しをさぼってしまう傾向がある。棚卸しをしたとしても、特定の種類の資産（例えば個人情報）に限定して棚卸しを実施することが多い。まず、棚卸しを検討するところでは、順序だった検討が必要だ。棚卸し対象は限定するのか、しないのか。限定するとした場合の判断基準は何か。最終完成物のみを管理対象とするのか、作成途中の版も管理下にするのか。採番システムをどのように作るのか。データ登録は、発生源（すなわちユーザ）が行うのか、ライブラリアンが行うか。このような検討課題について深い検討を行うことによって、自ずと作るべきシステムが明確になる。

この明確化のプロセスを経ていないまま、情報資産登録管理システムを作るのは、多くのリスクを抱えることになり、また、この管理システムが稼働しないことには、情報資産の棚卸しも不可能だ。この意味で、情報資産管理を始めようと思っている組織では、まず情報資産登録管理システムを実装し、その上で棚卸し作業を行うのが定石といえる。

みなさん、情報資産の棚卸しに頑張ってください！

（山口　英　内閣官房情報セキュリティ補佐官）

3．誰でもわかる情報セキュリティ用語

【ＡＥＳ】

AESはAdvanced Encryption Standardの略で、アメリカ政府が2002年に政府内における標準として策定した暗号化規格を指します。

AESが策定される以前、同政府は同じ共通鍵暗号方式であるDES（Data Encryption Standard）を開発しました。DES自体は開発されてから20数年間、様々な分野において使用されてきましたが、コンピューターの処理能力が向上した結果、その56ビットの鍵長（これは、約7京通りの組み合わせに相当）全てを総当り探索しても、現実的な時間内で解けてしまうことが明らかになり、その後もDESを3重に組み合わせた「トリプルDES」等によって、耐久性を高めようとしたものの、相当十分な強度を得られないことに加え、処理速度の問題もネックになってきました。

そこで「DESに代わり、長期間の使用に耐え得る暗号化方式の開発」いう視点に立ち、アメリカ政府は世界中から様々な暗号技術を応募し、処理速度及び強度のバランスを考慮して、最終的にベルギーの暗号学者達が開発した「Rijndael（「ラインダール」等と発音される）」というアルゴリズムをAESとして採用しました。AESはDESとは異なり、128ビット、192ビット、256ビットの複数の長い鍵が選択可能なことや転置、換字、暗号鍵との排他的論理和の組み合わせ（この構成を「SPN構造」といいます）を用い、バイト単位で処理すること等を特徴としています。そしてこれらの性質により、高い強度を持ちつつ、高速な暗号化／復号処理を実現しています。

最近では、AESが利用できるセキュリティ関連のハードウエア／ソフトウエア製品も結構増えていますので、一度御自身で仕様等を確かめてみるのも良いかもしれません。

4. 情報セキュリティQ

コンピューターウィルスの名前は一般に、ウィルス対策ソフトベンダーの解析者がウィルス定義ファイルを作成する過程で命名する場合が多く、例えば、「Nimda（ニムダ）」は「Admin」（管理者）を逆手に取るという意味で名づけられたと云われています。それでは、HTTP サービスのポートに対し、ワームコードを含んだ HTTP コマンドを送り付け、バッファオーバーフロー攻撃をしかけることで悪名高い「Code Red」の語源は次のどれでしょうか？

① 解析者の住所（の一部）　② 解析者の好きな飲み物　③ 解析者のニックネーム　④ ①～③以外

（なお正解は次号にて掲載致します。）

【前号の答え】

正解は「② Netscape Navigator」です。

Cookie は Netscape Communications 社で開発され、同社の Web ブラウザである Netscape Navigator がはじめて対応しました、その後、他のブラウザにも次々と取り入れられ、今や Web ブラウザの標準技術と言っても良い技術となりました。

5. NISCOLUMN（ニスコラム）

【「かもしれない」インターネットを心がけて】

現在、インターネットを利用する人口は約 8000 万人とも言われています。実に国民の 3 人に 2 人がインターネットを利用している計算です。運転免許保有者数が約 7800 万人ですので、運転免許と同じくらい、社会に当たり前のように定着したといえます。

ところで、その運転免許ですが、更新の際、必ずと言ってよいほど「だろう」運転、「かもしれない」運転という話がされます。交差点の出会い頭の事故の原因は、「脇から車が出てこないだろう」と思って交差点を通過したからであり、「脇から車が出てくるかもしれない」と思って運転する必要がある、という話です。免許をお持ちの方ならば、誰でも聞いたことがあると思います（免許を持っていない方でも、自転車や歩行者として道を歩くときは心掛ける必要があります）。

話をインターネットに戻しますが、インターネットが普及するに従って、コンピューターウィルスによるデータの破壊、情報の流出といった「事故」も増加しています。こうした「事故」がおきる裏には、例えば「自分のアドレスは特定の人しか知らないから、送られてくるメールの添付ファイルは安全だろう。」「自分は普通の人よりインターネットに詳しいし、対策もきちんと取っているから、自分はウィルスから安全だろう。」といった、ある種「だろう」運転に近い感覚でインターネットを扱っているということがあります。警戒感の欠如です。特に、ある程度インターネットに馴れた人に多いのではないでしょうか。

インターネットを扱う際にも、「自分のところにも、ウィルス付きメールが送られてくるかもしれない。」といった、「かもしれない」運転に近い感覚で接する必要があるのではないでしょうか。先日、本年上半期に報道された情報セキュリティに関する事案を見返す機会がありましたが、その多くが、「だろう」運転ならぬ「だろう」インターネットの感覚でインターネットを扱っていた結果発生したように思えました。恐らく、インターネットが本来的に有する危険性に着目し、常に警戒を怠らない、「かもしれない」インターネットをしていれば、防げたものも多かったのではないでしょうか。

秋になり、まもなく行楽のシーズンを迎えます。インターネットのすばらしさは、知りたい情報をピンポイントで知ることができることです。今度の三連休、インターネットで情報を収集し、家族や仲間とドライブにでも出かけてみてはいかがでしょう？

もちろん、どちらも「かもしれない」の心を忘れずに…。

（井）

＜バックナンバー・配信先変更・配信中止＞

本メールマガジンにおけるバックナンバーの取得及び配信先の変更、配信の中止等は下記の URL から可能です。

http://www.nisc.go.jp/nisc-news/

＜御意見、御感想＞

http://www.nisc.go.jp/mail.html