

平成18年5月23日
内閣官房情報セキュリティセンター (NISC)

高セキュリティ機能を実現する次世代OS環境の開発実施について

本日、文部科学省より発表された平成18年度科学技術振興調整費^(※1)の重要課題解決型研究^(※2)で「高セキュリティ機能を実現する次世代OS環境の開発」(詳細は別紙参照)の採択が発表されました。

本件は情報セキュリティ政策会議(議長:内閣官房長官)にて策定中の「セキュア・ジャパン2006(案)」(5月26日までパブリックコメント実施中)の一項目^(※3)に該当する技術開発であり、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。

【本件に関する問い合わせ先】

内閣官房情報セキュリティセンター

山口補佐官、小林参事官、沓澤参事官補佐

電話 03-3581-3768(センター代表)

※1 **科学技術振興調整費**とは、総合科学技術会議(議長:内閣総理大臣)の方針に基づく科学技術の振興に必要な重要事項の総合推進調整のための経費として文部科学省の予算として計上された、政策誘導型の競争的資金です。

※2 **重要課題解決型研究**とは、国家的、社会的に重要な政策課題であって、単独の府省では対処が困難であり、政府として速やかに取り組むべき課題について、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具体的な達成目標を設定し研究開発を推進するものです。

※3 **セキュア・ジャパン 2006(案)における該当施策箇所**は以下の通りです。

第2章 対策実施4領域における情報セキュリティ対策の強化

第1節 政府機関・地方公共団体

第3章 横断的な情報セキュリティ基盤の形成

第1節 情報セキュリティ技術戦略の推進

イ) **高セキュリティ機能を実現する次世代OS環境の開発(内閣官房、内閣府、総務省及び経済産業省)**

2006年度において、ITの信頼性確保のための喫緊な取組みとして、OSにおいてアプリケーションに依存しない形でセキュリティを確保し、かつ、電子政府で直近に求められる基盤機能に絞り込んだ技術基盤の開発を推進する。

第5章 2007年度の重点施策の方向性

第3節 横断的な情報セキュリティ基盤の底上げ

ウ) **高セキュリティ機能を実現する次世代OS環境の実証利用・開発等(内閣官房、内閣府、総務省及び経済産業省)**

2006年度に実施する「高セキュリティ機能を実現する次世代OS環境の開発」における部分的成果の実証利用を2007年度から積極的に図るとともに、基盤機能拡大に向けた暗号化通信、ID管理及び資源管理等の開発を推進する。また、その実証結果を踏まえ、電子政府での利用を前提とした本格的な高セキュリティ機能を実現するOS環境の開発を射程に、OS等システム導入における政府調達仕様の策定も併せて推進する。

高セキュリティ機能を実現する次世代OS環境の開発概要

1. 開発内容のポイント

平成18年度科学技術振興調整費の重要課題解決型研究で採択された「高セキュリティ機能を実現する次世代OS環境の開発」のポイントは以下の通り。(参考1参照)

- (1) 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)を開発する。
- (2) 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するが、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する。
- (3) 統一のIDを利用したのPC起動管理、そのIDを利用した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する。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る。
- (4) 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を活用する。

2. 開発実施体制

本件の実施にあたり、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、独立行政法人情報処理推進機構ほか、産業界との連携を図ります。(参考2参照)

3. 開発成果がもたらす利点等

本開発の成果がもたらす利点及び波及効果として以下が考えられる。

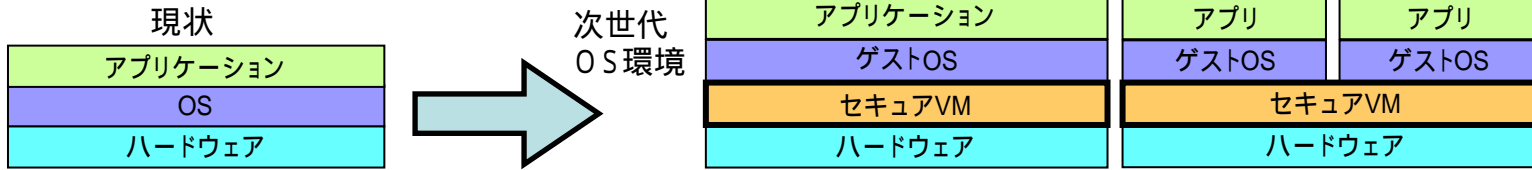
- (1) 既存の市販システムでは実現できない情報セキュリティ機能を政府システムに導入することが可能となる。
- (2) Windows や Linux 等の既存のユーザ環境を保持しつつ、信頼できない通信路での通信保護、内蔵ハードディスクの暗号化を行うことでシステム盗難等による情報漏洩対策などを実現する環境を提供する。
- (3) 実際に政府組織内で運用することを前提に開発することで、政府組織におけるセキュリティ対策の高度化に貢献することが可能となる。
- (4) 優秀な若手研究者による集中的研究開発方式で実施することにより、我が国における基盤ソフトウェア開発環境の向上及び優れたソフトウェア開発能力を有する人材の育成にも貢献する。
- (5) 開発したセキュアVMをオープンソースとして社会全体に公開し、開発成果を社会還元することにより、利用形態に適したOSを選択可能となるよう、社会全体での情報セキュリティ確保のための基盤環境強化に貢献する。

以上

開発内容

参考 1

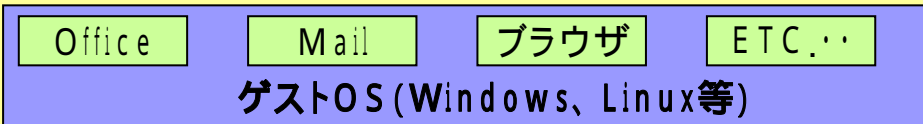
高セキュリティ機能を実現する次世代OS環境への移行



Windows, Linux等の現在の利用者環境をゲストOSとして稼働可能

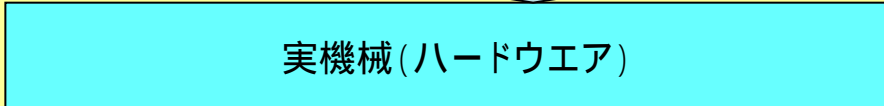
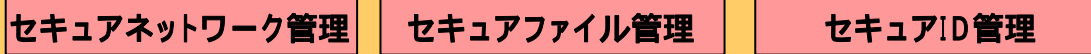
情報セキュリティ管理機能の基本的な部分は、セキュアVM側で多くを実現

セキュリティ機能を組み込んだ仮想機械により既存のOS環境ごと制御

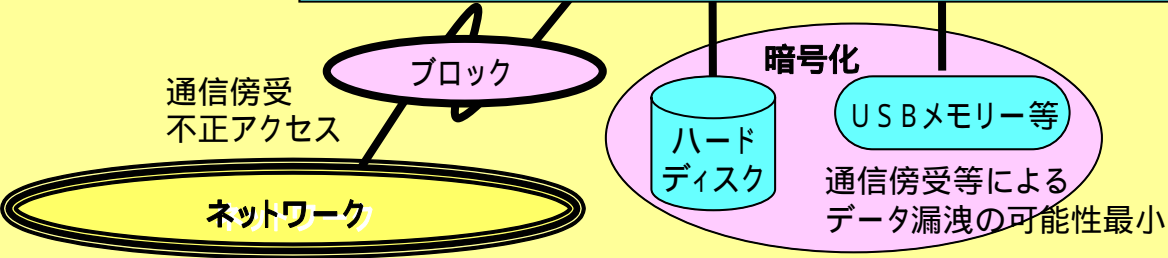


- 複数のゲストOSを同時に利用することも可能。
- ゲストOS間を隔離。
- ゲストOSごとに、VMが管理する資源へのアクセスを制御。

セキュリティ機能を組み込んだ仮想機械 + 最小限のOS機能 (セキュアVM)



リソースマッピング
仮想機械層がシステム内の情報フローを厳格に制御
実/仮想マッピング



開発部分
成果導入

政府機関電子政府、職員利用環境等で積極的に運用

社会全体に公開

社会全体での情報セキュリティ確保のための基盤環境強化に貢献

開発実施体制図

