

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PC起動管理、そのIDを利用したハードディスクや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。

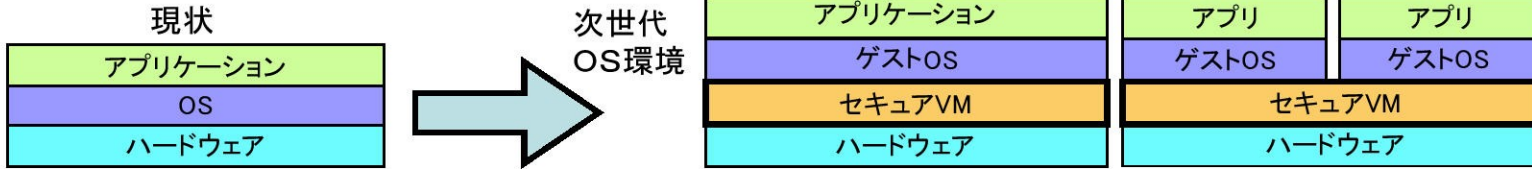
- (1) 既存の市販システムでは実現できない情報セキュリティ機能を政府システムに導入することが可能となる。
- (2) Windows や Linux 等の既存のユーザ環境を保持しつつ、信頼できない通信路での通信保護、内蔵ハードディスクの暗号化を行うことでシステム盗難等による情報漏洩対策などを実現する環境を提供する。
- (3) 実際に政府組織内で運用することを前提に開発することで、政府組織におけるセキュリティ対策の高度化に貢献することが可能となる。
- (4) 優秀な若手研究者による集中的研究開発方式で実施することにより、我が国における基盤ソフトウェア開発環境の向上及び優れたソフトウェア開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



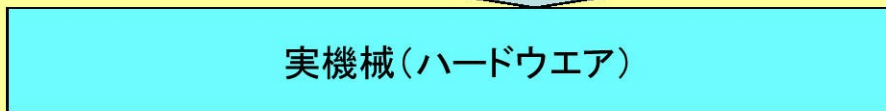
Windows, Linux等の現在の利用者環境をゲストOSとして稼働可能
情報セキュリティ管理機能の基本的な部分は、セキュアVM側で多くを実現

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

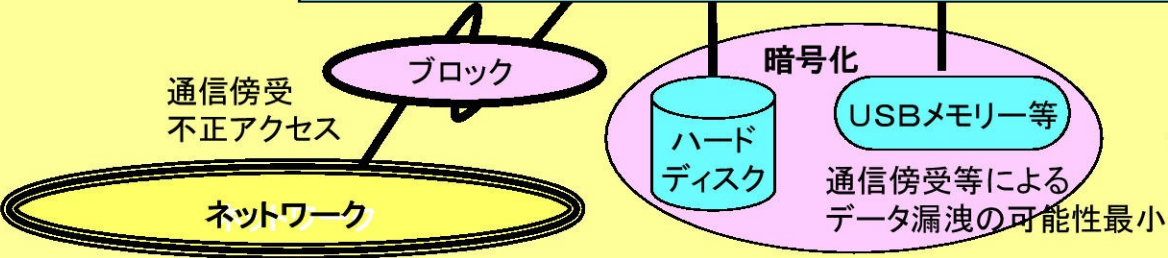


- 複数のゲストOSを同時に利用することも可能。
- ゲストOS間を隔離。
- ゲストOSごとに、VMが管理する資源へのアクセスを制御。

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



下位層の安全性を厳格に確保

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

