# 海外連携型調査研究

# プロポーザル

１．調査研究のテーマ

オペレーティングシステムのセキュリティ機能に関する調査研究

２．そのテーマの戦略的意義／位置付け

ネットワークを介した不正侵入や個人情報の漏洩が多発しており，計算機システムのセキュリティの向上が求められている．特に，計算機の基盤ソフトウェアであるオペレーティングシステム(OS)は，計算機のハードウェアとソフトウェアの両方を制御するため，そのセキュリティを強化することにより，システム全体のセキュリティを向上することが期待できる．また，電子政府などの構築も行われており，どのような OS を導入すべきかが大きな議論となっている．さらに，SELinux に代表されるセキュア OS が注目を集めており，OS のセキュリティ技術への関心が高まっている．
本研究調査では，現在の Linux などの OS，およびセキュア OS のセキュリティ機能の調査を行い，現在の OS のセキュリティ機能を強化する技術の現状を明らかにする．また，現在の OS のセキュリティ機能に関する研究動向を調査し，今後の OS に求められる機能や技術について検討する．

３．調査研究の概要

本調査は，OS をベースとしたセキュリティ機能に関して，以下の項目に関して調査研究を行う．
(1) アクセス制御機構
(2) カーネルベース侵入検知システム
(3) 情報フロー制御
(4) 認証機能
(5) バッファオーバフロー対策
(6) ログ監査機能

本調査におけるこれら６つの領域は，研究チームによって調査する予定であり，国内外の学会での発表や企業からの製品を調査分析する．また，韓国では，従来からセキュア OS に関する研究が行われてきており，韓国での過去の研究実績や動向などを Gwangju Institute of Science and Technology のメンバーとともに調査する．Gwangju Institute of Science and Technology のメンバーは，国際会議だけでなく，日本の国内会議でもその成果を積極的に発表しており，その研究能力は高い．また，調査結果を基に，今後の OS に求められるセキュリティ機能について検討し，その方向性を明らかにすることを目指す．SSR フォーラムの活動方針に従い，我々は，今年度末までにレポートを提供する．さらに，調査結果は全てウェブ上に保存する．

４．調査研究の進め方（共同研究者など）

調査グループ構成メンバーは以下のようである。

| | | |
|---|---|---|
| 主　査 | 櫻井　幸一 | 九州大学　大学院システム情報科学研究院 |
| メンバー | 田端　利宏 | 九州大学　大学院システム情報科学研究院 |
| | | (http://itslab.csce.kyushu-u.ac.jp/index-j.html) |
| | R. S. Ramakrishna | Department of Information and Communications, |
| | | Gwangju Institute of Science and Technology, Korea |
| | SHIN, Wook | Department of Information and Communications, |
| | | Gwangju Institute of Science and Technology, Korea |
| | KIM, Hyung Chan | Department of Information and Communications, |
| | | Gwangju Institute of Science and Technology, Korea |
| | Cho, Ji Ho | Department of Information and Communications, |
| | | Gwangju Institute of Science and Technology, Korea |
| | | (http://nwcl.gist.ac.kr/~seecure/index.html) |

５．関連発表論文


(1) Katsuya SUEYASU, Toshihiro TABATA, Kouichi SAKURAI: "On the Security of SELinux with a Simplified Policy," Proc. of IASTED International Conference on Communication, Network, and Information Security (CNIS 2003), pp.79-84 (12, 2003).

(2) 末安 克也, 田端 利宏, 櫻井 幸一: "SELinux アクセス制御設定項目の安全な統合方法に関する考察, " 2004年 暗号と情報セキュリティシンポジウム (SCIS2004), Vol.1, pp.287-292 (1, 2004).

(3) 鑪 講平, 田端 利宏, 櫻井 幸一: "プログラムの確率的挙動に基づく異常検知手法の実装, " 2004年 暗号と情報セキュリティシンポジウム (SCIS2004), Vol.2, pp.1047-1052 (1, 2004).

(4) Hyung Chan Kim (K-JIST), Wook Shin (K-JIST), R.S.Ramakrishna (K-JIST), Kouichi Sakurai (Kyushu University): “Conflicts of Role Based Access Control in Multi-domain Security,” 2004年 暗号と情報セキュリティシンポジウム (SCIS2004), Vol.1, pp.481-486 (1, 2004).

(5) 田端 利宏, 櫻井 幸一: "動的リンカを利用したユーザレベルアクセス制御機構の設計, " コンピュータセキュリティシンポジウム2003 (CSS2003) 論文集, Vol.2003, No.15, pp.457-463 (10, 2003).

(6) 末安 克也, 田端 利宏, 櫻井 幸一: "簡易化されたポリシに基づいたSELinux アクセス制御の安全性評価, " コンピュータセキュリティシンポジウム2003 (CSS2003) 論文集, Vol.2003, No.15, pp.253-258 (10, 2003).

(7) 鑪 講平, 田端 利宏, 櫻井 幸一: "確率ネットワークを用いたプログラムの異常動作を検知する手法, " コンピュータセキュリティシンポジウム2003 (CSS2003) 論文集, Vol.2003, No.15, pp.463-468 (10, 2003).

(8) 末安 克也, 田端 利宏, 櫻井 幸一, "UNIX/Linuxアクセス制御機構とSELinuxアクセス制御機構のセキュリティに関する比較", 電気関係学会九州支部連合大会(第56回連合大会), Sep. 2003.

６．Gwangju Institute of Science and Technology との過去の打ち合わせ内容

これまでの Gwangju Institute of Science and Technology との打ち合わせは以下の通りである．

■2003 年 12 月 22 日

場所：光州科学技術院

参加者：田端，許，鑪（九州大学から 3 名），光州科学技術院から 5 名，NSRI から 2 名

・光州科学技術院の発表は 2 件

(1) Introduction to Trusted Operating Systems (Hyung Chan KIM)

・SecureOS グループメンバーの紹介

・Trusted OS の必要性の説明

・Trusted OS の構成要素の説明(Reference Monitor, Access Control)

・提案したセキュリティモデルと実装例の説明(BLP Model)

[質疑]

Q1: No.16 の mode の意味は何か (田端)

A1: read-only, read-write などのモード

Q2: No.6 の Reference Monitor はどのように実装してあるのか (田端)

A2: Linux の LKM(loadable Kernel Module)の形で実装している．

詳しくは次の発表で Mr. Shin が述べる．

(2) CSRL: A Trusted Operating System (SHIN, Wook)

・CSRL Project の説明

大きく 6 つのテーマに分けられる. 現在その中心となる Themis(Reference Monitor)の研究を中心に行っている．

・Themis の説明

SELinux の機能を用いて実装している．Kernel Based IDS を実装している．参考にしている文献は鑪も参考としていて研究の関連性が高い．

・概要

1. Linux での実装は，LSM(Linux Security Module)を利用している．
   (実装を容易にするため．)
2. アクセス制御ポリシの研究も現在行っている．
3. 今後は Secure Smart-card / Embedded OS の研究を行う
   (ユビキタス環境を考慮)

[質疑]

Q1: Secure Embedded OS は，どの OS を利用して研究するのか(田端)

A1: Linux を利用する．新規に開発するよりも，既存 OS を利用する方がよい．

コメント: Linux は大きく組み込みに向かないが，組み込み製品の性能も向上するのでいい選択肢ではないか．

Q2: No.6 の Normal Behavior はどうやって生成しているのか(鑪)

A2: New Mexico の論文を参考にして実装をしている．

・ 九大側の発表は 3 件

(1) 櫻井研究室，システム LSI センターの説明(許)

(2) 櫻井研の OS 研究の説明(田端，鑪)

(a) User Level Access Control Mechanism Using Dynamic Linker(田端)

[質疑]

Q1: どういうアクセス制御モデルを使うのか
A1: 今回の研究は，プログラム実行時にユーザレベルでアクセス制御できる機構の提案であり，既存のモデルを利用することを考えている．

Q2: この方法だと動的リンカの仕組みを模倣したり，PLT や GOT の内容を書き換えたりした攻撃が可能ではないか．
A2: 指摘された問題は確かに重要だと思います．攻撃について検討します．(実際には PLT を書き換えられることはないので，攻撃の可能性は小さいと思います．GOT の整合性を確認することで対処可能です．)
Q3: どうしてオーバヘッドが減るのか?
A3: カーネルでライブラリ単位の呼び出し関係を把握するには, スタックを再帰的に解析する必要がある．提案方式は実行時に観測したいところの情報だけを取得でき，すべての情報を解析する既存手法よりもオーバヘッドは小さいと考えられる．

(b) On the Security of SELinux with a Simplified Policy(田端)
[質疑]
Q1: 話がよく分からなかったが，設定に欠陥があることが多いのか？
A1: SELinux は設定が複雑なので, 人為的ミスが発生しやすい．この問題を解決するには，設定項目を減らし，設定を簡単にすることがある．しかし，既存の簡易化手法ではセキュリティ上の問題が発生する．このため，安全な設定の簡易化手法を今後検討する．(CNIS に比べ発表内容を省略したため，発表だけでは理解されなかったようです)

(c) Secure OS Products(田端)
Secure OS の調査内容について説明した．

(d) Proposal of Probabilistic Method for Anomaly Program Detection　(鑪)
[質疑]
Q1: なぜベイジアンネットワークを使うのか
A1: ベイジアンネットワークだと確率が遷移するので利用した．

■ 2004 年 3 月 19，20 日

・セキュア OS セミナー
日時　：2004 年 3 月 19-20 日
場所　：韓国　光州　Kwang-Ju Institute of Science and Technology
参加者：光州科学技術院(7 人), NSRI (2 人), 九州大学(4 人)

・3 月 19 日
▼J.Y.Park
- "Data Protection in Mobile Agents; one-time key based approach"
ワンタイム対称鍵を利用することでエージェントの持つデータの完全性をフォワードセキュアに保つ方式。ワンタイム鍵はハッシュ関数によって生成される。データの暗号化には DES を利用。ワンタイム鍵はエージェントオーナの公開鍵で随時暗号化されてエージェントと共に移動する。エージェントオーナはワンタイム鍵列を秘密鍵で復号化し、そのワンタイム鍵を用いてエージェントのデータを復号化する。

▽質疑応答
Q.なぜ DES を利用したのか？
A.速度を重視した。他の対称暗号を利用することも可能。

Q.前のホストでの実行結果を再利用したい場合はどうするのか？
A.信頼できないホストがいることが前提で、他のホストとの連携は考えていない。今後の課題でもある。
Q.ベースとしているエージェントシステムはなにか？
A.オリジナルの X-math というエージェントシステムを使っている。

▼W.Shin
- "Procedural Constraints in the Extended RBAC and its Coloured Petri Net Modeling"
Procedural Restrictions を利用した The extended RBAC(RBBAC)についての発表および Coloured Petri Net(CPN)を用いた Procedural Constraints のモデリングに関する発表。CPN は IDS にも利用されていて、遷移した状態の危険度を評価できる。提案方式は危険度を基にアクセス制御を行うモデルである。

■3 月 20 日

▼Y.Kotegawa
- "Security and Applications of Mobile Agents"
MA の利点と応用可能分野について述べ、トレースを用いたエージェントのデータの検証メカニズムを述べた。最後に MA を利用した IDS の導入について述べた。

▽質疑応答
Q.トレースを用いたシミュレーションはどうやるのか？
A.エージェントへの入力をトレースとして保存する。そのトレースを用いて実際の実行と同様の処理を再び行う。
Q.トレースは信頼できるのか？
A.トレースはエージェントではなくサーバが送信する。サーバが送信したトレースには署名がついており、それによって確認される。
Q.マルチエージェントシステムとの比較調査はおこなったのか？
A.おこなっていない。マルチエージェントシステムではエージェントのホスト間移動は起こらないため、予めモバイルホストへ IDS エージェントを導入しておかなければならない。また、クライアントサーバ方式と変わらないため通信コストが高くなる。一方、提案方式ではゼロの状態から IDS エージェントを導入できるし、通信コストもホスト内通信になるため削減できる。

▼J.H.Cho
- "Security in Embedded Systems"
組み込みシステムにおけるセキュリティについての発表。セキュア組み込 OS に求められる機能として、プロセス制御、メモリ保護、セキュアファイルシステムをあげていた。その中でも特にプロセス制御あつかっており、あらたなプロセス特権分離機構を提案していた。提案方式ではプロセスの関数に着目しており、特権が必要でない関数は優先度が下げられた実行空間で実行されるように構成されていた。

▽質疑応答
Q.実際に携帯電話で i アプリなどのアプリケーションが携帯の OS のクリティカルなメモリ空間にアクセスすることができるのか？
A.できると考えている。
Q.特権分離機構はソフトで実現するのか？それともハードで実現？
A.ソフトで実現することを想定している。