2005 年度 SSR 海外連携型調査研究プロポーザル

１．調査研究のテーマ

計算機システムのセキュリティ機能に関する日中韓連携調査研究

--センサーネットワークとユビキタスシステムを含む分散環境下でのアクセス制御機能を中心とし--

-

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.

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，SELinux をはじめ、どのような OS を導入すべきか、国産独自セキュリティ OS を開発すべきか、が大きな議論となっている．われわれのグループでも、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と今後の OS に求められる機能について検討を行ってきた。

この５月価格比較サイト「価格.com」は、不正アクセスによる改ざんを受けたことで同サイトを閉鎖した。これは、サイトのデータベースの脆弱性をついた攻撃によるものであり、OS のセキュリティ機能強化だけでは万全ではないことを示唆している。
このような背景に対して、本研究では、OS だけではなく、データベースや web を含む計算機システムのセキュリティ機能をとりあげる。

特に、センサーネットワークやユビキタスシステムが普及する現状を踏まえ、分散環境下でのセキュリテイが要求されている。中でも、埋め込みＯＳとミドルウエアとは、今後重要な課題となると考えられ、この環境での、信頼できるシステム構造の研究が重要な課題となっている。
他方、技術開発だけではなく、アクセス制御技術おいては、ポリシーに関する国際標準化もＩＳＯで議論がはじまっている。

３．調査研究の概要

昨年度は OS を基盤としたセキュリティ機能、とくに、デスクトップ PC とサーバーを中心とした　Trusted OS に関する研究を調査した。

今年度は、昨年度の課題の一部を継続するとともに、ＯＳだけでなくデータベースを含む計算機システムのセキュリティ機能に関して，以下の項目に関する調査研究を予定している。

[GIST 側@韓国が提起している研究課題]

K1. センサーネットワークとユビキタスシステムをはじめとする分散環境化での TOS

分散センサーネットシステムに対するセキュリティをサポートする小型ミドルウエアＯＳ上で動作するセンサーネットワークプラットフォームの設計と開発。昨年度は、現実の不正侵入を拒否する、高度なアクセス制御の定式化を行った。今年は、これを、分散環境やミドルウエア環境化へ拡張する。また、センサーネットワークプロトコルの課題調査も行った。今年は、小型軽量のモバイル端末をはじめとする分散ネットワークに応用する。

具体的な課題候補のひとつとして 「位置情報に基づき、資源対象を制御する TOS の小型軽量化。これによる、分散環境への適用」 があげられる。

K2. Trusted OS に対するポリシー記述言語の開発

目的は、割り込みシステムコールをはじめとするプロセス処理の分離検証のためである。

[九大@日本側]

J1. セキュア OS のアクセスパーミッションの評価

申請者のグループは，これまでに指摘してきた SELinux の統合パーミッションによるセキュリティの問題点を整理し，情報処理学会論文誌の 2005 年 4 月号において発表した．セキュア OS の設定は複雑であり，設定をサポートする機構やツールが必要とされている．本プロジェクトでは引き続きアクセスパーミッションの安全性について調査研究を行う．

J2. RBAC を中心としたアクセス制御に関する ISO/IEC 標準化動向

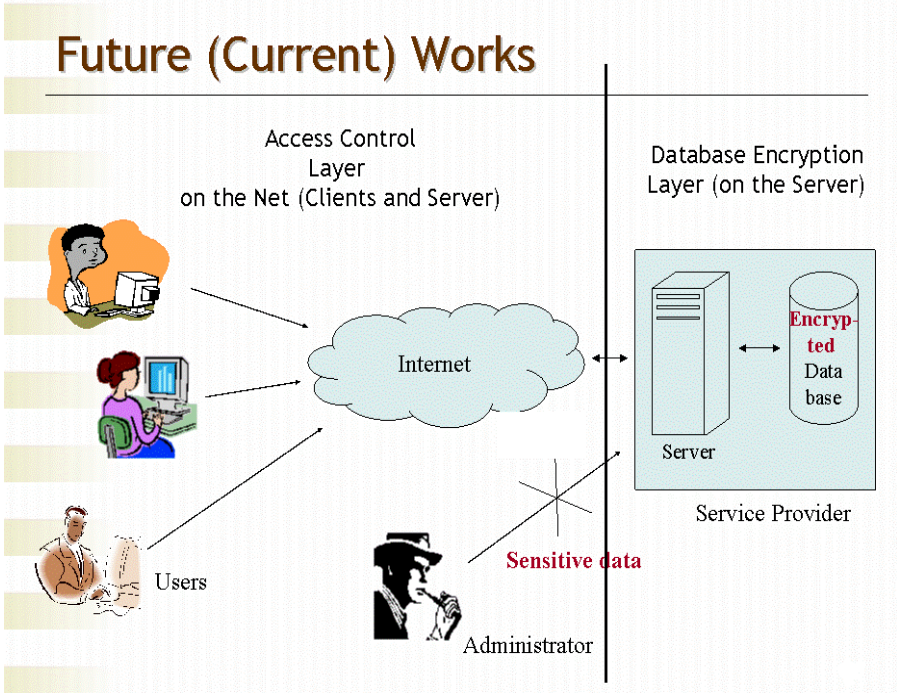
ロールに基づくアクセス制御(Role Based Access Control, RBAC)は、米国規格局（NIST は 2004 に国内規格とした。米国は、この RBAC をＩＳＯ国際規格に、提案してきた。NIST の米国規格は、国際の場で、各国の意見が盛り込まれ、修正される形となると予想される。本調査研究では、この動向も探る。

（本研究の主査である櫻井は、この RBAC が議論される ISO/SC27 国際会議へ日本代表として定期的に参加している。）

J3. データベースの暗号化とアクセス制御

特に、データベースサービスプロバイダーのセキュリテイ確保を中心に。RBAC などのアクセス制御モデルは、OS に限らず、データベースや web システムなどで実現可能であり、この理論的アプローチを、すでに昨年より、研究室ではじめている。（Amril Syalim, Toshihiro Tabata and Kouichi Sakurai. "Access Control Model for a Secure Enhanced Database Management System". コンピュータセキュリテイシンポジウム (CSS) 2004 年１０月） 今年は、さらにこの研究を発展させる。

また、データベースへの攻撃・アクセス制御技術を、OS のそれらと比較しつつ、調査検討することで、Trusted OS の限界と、計算機のシステムとしての脆弱性と防御機能を議論する。



J4. セキュアデータベースの製品動向

元データベース暗号化ソフトウェアの業界トップだった Protegrity 社（スウェーデン）からスピンアウトした InfiniSe 社（スウェーデン http://www.infinisec.se/）の InfiniSec DG/4 は、つぎのような特色をもつ:

(1)外からのアクセスを企業内ネットワークの入り口でとめるファイアウォール等で防ぎきれない不正アクセス（アウトソース先からの不正アクセス、内部犯罪等）からデータを守ることができる。

(2)データへのアクセス者の記録が残る（不正アクセスの追跡可能）。

(3)クライアントとデータベース間に入るミドルウェア的な製品。

(4) クライアントサイドではインストールなど不要、データベース管理者サイドで行う。

(5)あらゆるプラットフォーム（Oracle8i、９ｉ、10g、SQL200０、Window ｓ、Unix、Linux）に対応可。

国内では、

eCiphergate（ジャパン・インフォメーション・テクノロジー社@日本），

D’Amo （Penta Security Systems@韓国）

atbasH （イコン社@日本）

などの競合製品があるが、研究・開発は Secure OS ほど活発ではない。

本調査研究では、こうした製品の性能と限界を議論し、現在のデータベースのセキュリティ機能を強化する技術と今後のデータベースに求められる機能について検討を行う。

4. 研究体制と構成員

昨年度は、韓国での SecureOS に関する過去の研究実績や動向などを光州科学技術院(Gwangju Institute of Science and Technology, GIST)のメンバーとともに調査し，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，その方向性を与えた.
今年度も、韓国のパートナーとしては、同じく光州科学技術院 SeeCure 研究室と共同研究を行う。

さらに、今年は、中国での計算機セキュリティに関する研究の動向調査をはじめ、技術交流のパートナーとして、分散計算機システムのセキュリティ研究に関する権威である精華大学の林教授を構成員にむかえる。林教授は、シンガポールでは、PKI システムのベンチャー企業も経営しており、政府の顧問等の経験も豊富である。昨年は、アジア PKI 国際会議で、福岡に招聘して以来、主査の櫻井と交流がある。今回の主な研究テーマである Secure OS やデータベースセキュリティには、中国の立場としても、大変有意義と、積極的である。
また、この９月より、九州大学の支援により
University of California, Irvine(http://www.ics.uci.edu/)
へ、長期出張予定の九州大学堀助教授も構成員にいれて、海外、とくに米国の研究動向の調査を依頼する。 UC-Irvine 校では、本年３月に
Center for Cyber-Security and Privacy (http://www.ics.uci.edu/%7Eccsp/)
を立ち上げ、関連イベントとして、９月下旬に
First Southern California Security and Cryptography Workshop
September 24, 2005
を計画している。堀は、こうしたワークショップへ参加、本研究プロジェクトへ参加報告を行う。
さらに、昨年度まで、韓国側メンバーであった SHIN, Wook, PhD は、この 7 月より、University of Illinois at Urbana-Champaign Professor: Carl. A. Gunter (http://www-faculty.cs.uiuc.edu/~cgunter/) 研究室のポスドクとして移動予定であるが、今年度も本プロジェクトに参加し、米国での研究活動等も報告する。

<u>構成員</u>
調査グループ構成メンバーは以下のとおり。
〇主 査
(1)櫻井 幸一 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)

〇メンバー
[J]日本

(2)田端　利宏　　岡山大学　工学部　情報工学科
(http://www.swlab.it.okayama-u.ac.jp/~tabata/index-j.html)
(3)堀 良彰　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/%7Ehori/index-j.html)
9月より一年間　UC-Irvine校客員研究員。

[C]中国

(4) Kwok-Yan Lam　中国精華大学ソフトウエア学科 教授　兼　Privylink社 (www.privylink.com.sg) Founder and Executive Chairman

略歴：　1987年ロンドン大卒業（First Class Honours），1990年ケンブリッジ大で博士号取得（分散計算機セキュリティシステム）。1990年より、シンガポール国立大学およびロンドン大学faculty員。2002年より現職。研究分野は、システムセキュリティ、認証プロトコル、侵入検知、耐タンパーHW設計、セキュアアーキテクチャーなど。 ケンブリッジ大学アイザックニュートン研究所客員研究員、システムセキュリティヨーロッパ研究院客員教授経験。シンガポールと香港における電子銀行・電子政府など多数の電電子システムの主席セキュリティ設計者.1998年、シンガポールにおける彼の情報セキュリティにおける研究開発に貢献に対して、Singapore Foundation Awardを受賞。

研究論文：

http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/l/Lam:Kwok=Yan.html
http://www.scholar.google.com/scholar?hl=en&lr=&q=+Kwok-Yan+Lam+

[K]韓国側

Gwangju Institute of Science and Technology,
Department of Information and Communications,
SeeCureグループ(http://www.seecure.org/)
(5) R. S. Ramakrishna, Prof.
(6) KIM, Hyung Chan、PhD candidate,
(7) SHIN, Wook, PhD,　7月より、University of Illinois at Urbana-Champaign. Professor: Carl. A. Gunter (http://www-faculty.cs.uiuc.edu/~cgunter/)研究室のポスドク予定。

5. 研究会議形態

昨年度は、研究調査の方針決定や意見交換，成果報告を目的として4回打ち合わせを行った。キックオフ会議には、SSR事務局 佐藤さまに出席いただき、また、特別ゲストして、最後

の会議には、SecureOSに関する国家projectを指導されている内閣官房 青木さま, IPA宮川さまに参加いただき、意見交換を行った
また、国内シンポジウムにあわせて、韓国側研究者を招聘し、企業側参加と合同シンポジウムを開催した。調査結果は全てウェブ上に公開している。
　今回も同様の会議形態を考えている。 今年度も内閣官房、IPAとは非公式ながら連絡をとりあり、適宜、会議に出席いただき、産学官の情報交換を行う予定である。特に、中国の研究開発動向に関しては、日本政府側は重要視している。
企業側参加からは、反省事項の一つとして、全般にコミュニケーション不足だったというコメントをいただいた。今年は、海外研究者を含めたメイリングリストの活用やWikiやBlogで本プロジェクトサイトを構築するなどで、もっと活発に意見交換することを考えている。

6. 昨年度研究活動・発表論文

6.1 昨年度のSSR研究活動に関しては以下のwebより：

http://itslab.csce.kyushu-u.ac.jp/ssr/

ID: ssrgroup　PassWD: is0062

6.2 GIST@韓国との共著論文

1. Hyung-Chan Kim, R. S. Ramakrishna, Kouichi Sakurai: A Collaborative Role-Based Access Control for Trusted Operating Systems in Distributed Environment. IEICE Transactions
88-A(1): 270-279 (2005)
2. Wook Shin, Jeong-Gun Lee, Hong Kook Kim, Kouichi Sakurai: Procedural Constraints in the Extended RBAC and the Coloured Petri Net Modeling. IEICE Transactions 88-A(1):
327-330 (2005)
3. Hyung Chan Kim, R. S. Ramakrishna, Kouichi Sakurai, "On the Privilege Transitional Attack in Secure Operating Systems", Computer Security Symposium 2004(CSS2004), pp. 559-564, Oct. 2004.
4. Ji-Ho Cho, Dong-Hoon Yoo, Hyung-Chan Kim, R. S. Ramakrishna, Kouichi Sakurai,
"The Design of Convenient File Protection based on EXT3 File System",
Computer Security Symposium 2004(CSS2004), pp. 565-570, Oct. 2004.
5. Amril Syalim, Toshihiro Tabata, Kouichi Sakurai,
"Access Control Model for a Secure Enhanced Database Management System",
Computer Security Symposium 2004(CSS2004), pp. 589-593, Oct. 2004.

6. Wook Shin, Hong Kook Kim, Kouichi Sakurai,
"An Implementation of Extended-Role Based Access Control on an Embedded system",
Computer Security Symposium 2004(CSS2004), pp. 667-671, Oct. 2004.
7. Hyunjin Yoo, Minho Kim, R. S. Ramakrishna, Kouichi Sakurai
"Privacy Preserving Clustering using Joint Probability Density Functions",
Computer Security Symposium 2004(CSS2004), pp. 739-743, Oct. 2004.

6.3 関連の論文（九大側）

8. 田端 利宏, 末安 克也, 櫻井 幸一"設定ツールによるSELinuxアクセスパーミッション統合の安全性評価" 情報処理学会論文誌 テクニカルノート, Vol.46, No.4, (4, 2005).
9. Toshihiro TABATA, Kouichi SAKURAI, "Design of Intrusion Detection System at User Level with System-call Interposing," 1st International Conference on E-business and Telecommunication Networks (ICETE2004), (Aug, 2004).
10. 田端 利宏, 櫻井 幸一, "IEEE Symposium on Security and Privacyにおける研究動向調査", コンピュータセキュリティシンポジウム2004(CSS2004), pp. 55-60, Oct. 2004,

6.4 データベースSecurityに関する最近の研究（九州大学側）

11. Amril Syalim, Toshihiro Tabata and Kouchi Sakurai. "Usage Control Model and
Architecture for Data Confidentiality in Database Service Provider". Indonesia Cryptology and Information Security Conference (INA-CISC) 2005. March 2005. Jakarta.
12. Amril Syalim, Toshihiro Tabata and Kouchi Sakurai. "Usage Control Model for Data Confidentiality Problem in Database Service Provider". Symposium on Computer and Information Security (SCIS) 2005. Jan 2005. Kobe.
13. Amril Syalim, Toshihiro Tabata and Kouchi Sakurai. "Access Control Model for a Secure Enhanced Database Management System". Computer Security Symposium (CSS) 2004. Oct 2005. Hokkaido University. Hokkaido.

以上。