コンピュータセキュリティ　14－22
（2001．7．25）

マルチOS環境を利用したアクセス制御システムの実装と性能評価

佐々木 慎一† 荒井 正人† 永井 康彦† 梅都 利和‡

†(株) 日立製作所 システム開発研究所
‡(株) 日立製作所 情報機器事業部

神奈川県横浜市戸塚区吉田町292番
045-860-3075
sh-sasa@sdl.hitachi.co.jp

インターネットを利用したサービスが拡大する一方で，不正アクセスが深刻な問題となっている。報告者等は，インターネットにおける数多くのセキュリティ脅威の中でも，特にインターネットサーバへの侵入が引起す問題に着目し，たとえ侵入が発生した場合にも，情報資産の保護を可能とするアクセス制御システム(IRACS: Intrusion Resistant Access Control System)を考案した。本報告では，IRACS 自身の保護までも考慮した実装方式と，ファイルアクセスに関する性能テストの結果について示し，WWWをはじめとする各種インターネットサーバに適用可能であることを述べる。

マルチOS，不正アクセス，セキュリティ，アクセス制御，性能評価，WWW

Implementation and performance analysis of access control system using multi-OS

Shinichi SASAKI†, Masato ARAI†, Yasuhiko NAGAI†, Toshikazu UMEDU‡

†Systems Development Laboratory, Hitachi, Ltd.
‡Mechatronics Systems Division, Hitachi, Ltd.

292 Yoshida-cho, Totsuka-ku, Yokohama, 244-0817 Japan
+81-45-860-3075
sh-sasa@sdl.hitachi.co.jp

While services on the Internet increase, illegal accesses are serious issue. We focused on problems that are caused by intrusion into Internet Server , and proposed the access control system (IRACS: Intrusion Resistant Access Control System) that can protect informational assets even if intrusion occurred. In this paper, we describe the implementing means of IRACS with considering protecting itself. Moreover, we describe the performance analysis report, and state IRACS is applicable for the Internet Server such as WWW server.

Multi-OS, Illegal access, Security, Access control, Performance analysis, WWW

1. はじめに

インターネットを利用したサービスが拡大する一方で，不正アクセスが深刻な問題となっている。特にWWW サーバに対するページの改竄攻撃や，サーバを踏み台にした機密情報の盗聴攻撃が数多く発生している。報告者等は先に，一般的なセキュリティ対策では防ぎきれない不正アクセスから情報を保護するのに有効なアクセス制御システムを提案した[1]。本稿では，本システムを IRACS (Intrusion-Resistant Access Control System)と呼ぶ。

本報告では，IRACS 自身の保護も考慮したIRACSの実装方式について述べる。また，本システムのWWW サーバへの適用を想定し，WWW サーバの性能に与える影響を評価した結果と考察を述べる。

2. 一般的なセキュリティ対策

インターネットに公開するサーバは，セキュリティ攻撃に直接さらされる。そのため十分なセキュリティ対策を施す必要がある。

一般的なセキュリティ対策としては，下記のようなものがある。

(1) 暗号とディジタル署名

ネットワーク回線を流れるデータの機密性と完全性を保護する。

(2) サービス利用の制限

ファイアウォールによるサービスの利用とデータフローの制御と，サーバホストにおける不要なサービスや通信ポートの無効化を実施する。

(3) セキュリティ監査・監視

アクセスログを採取し，これらを収集・解析することで不正アクセスを追跡する。

(4) セキュリティ問題の修正

例えば，CERT/CC[2]等が発信している不正アクセス情報などを常にウォッチしながら，早期対策を実施する。

多くの場合，これらの対策が十分に施されていれば，不正アクセスを防止できる。しかし，実際には設定ミスや，セキュリティ問題を放置してしまう場合が多く，不正アクセスが発生しやすいのが現状である。特に，サーバプログラムのセキュリティホールを狙われた場合には，サーバホストに侵入されてしまうケースがある。そのため，サーバへの侵入を前提としたセキュリティ対策が求められる。

3. 不正アクセス対策方針

サーバへの侵入を前提とした場合に，最も大きな被害が起きるのは，管理者権限を悪用されたときである。通常のサーバプログラムは，アクセス制御機能を有するOS 上で動作しているが，それはアクセス主体が所有するユーザーアカウントによりアクセス権が決まるものである。つまり，アクセス権限を有するユーザーであれば，どのプログラムを用いてアクセスしても構わない。したがって，管理者権限等を乗っ取られた場合，サーバ内のファイルに対するアクセスには制限がなくなり，その完全性と機密性を著しく損なうことになる。

そこで，IRACS では，サーバ侵入時のファイルの完全性と機密性を確保するために，アクセス主体が所有するユーザーアカウントだけでなく，そのアクセス手段となるプログラムまで制限するといったアクセス制御ポリシーを採用した。さらに，アクセス制御ポリシー情報とアクセス制御機能自体を保護するためにアプリケーションレベルから容易に干渉及び回避できない領域にてアクセス制御機能を実装することを考えた。

4. IRACS の実装

4.1 IRACS の構成

IRACS の構成を図 1に示す。本システムは，ナノカーネル方式[3], [4]を利用して 1 台の PC 上にサービス用 OS とセキュリティ用 OS が共存可能な環境を築き，サービス用 OS 側で発生するファイルアクセスを，セキュリティ用 OS 側にて制御する。

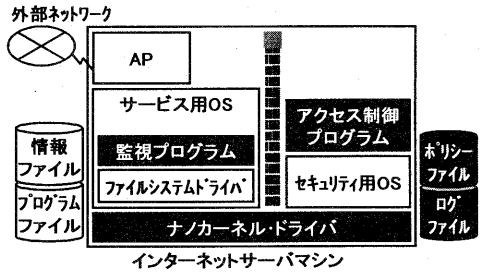

図 1 システム構成

・**ポリシーファイル**:ファイルのアクセス制御に関するポリシー情報を記述したものであり,セキュリティ側 OS にて管理する。

ファイル名	タイプ	プログラム名称	ユーザーID	特徴値	アクセス可能時間
C:¥HTTP-DOCS¥	read	C:¥Serv¥WWWServ.exe	SYSTEM	0x89E3	-
C:¥HTTP-DOCS¥	write	C:¥Prog¥WWWEdit.exe	WWW_Admin	0x3D20	08:00-17:30

図 2 ポリシーファイル

ポリシーファイルには,図 2のようにファイルまたはディレクトリに対してアクセス権限を有するアクセス主体を,プログラムの名称(実行ファイルのパス名)とユーザー ID,さらにプログラムファイルが有する特徴値(たとえば,ハッシュ値)の組み合わせで,アクセスタイプ毎に指定する。オプションとしてアクセス可能な時間帯を設定することもできる。

・**ログファイル**:不正ファイルアクセスに関するログ情報(アクセス発生日時,アクセス対象ファイル,ポリシー違反の理由等)を記述したものであり,セキュリティ用 OS 側にて管理する。ログファイルはその最大サイズおよび最長保存日数を設定できる。

・**ナノカーネルドライバ**:ナノカーネル方式を用いて 1 台のサーバ上にサービス用 OS とセキュリティ用 OS を共存させ,且つ OS 毎にデバイスとメモリ空間を分割・専有可能にする。

・**監視プログラム**:サービス用 OS 側の全てのファイルアクセスをインターセプトする。ファイルオープン要求時に,アクセス主体となるプログラムの情報(名称,特徴値,実行ユーザー ID)を取得する。取得したプログラム情報と,アクセス対象ファイルのファイル名をアクセス制御プログラムに通知し,ポリシーファイルにて認められたアクセスであるか否かの判断結果を受信する。判断結果に応じて,ポリシーで認められたアクセスであればファイルアクセスをフォワードさせ,ポリシー違反であればファイルアクセス要求元プロセスにエラーを返す。

・**アクセス制御プログラム**:監視プログラムからの通知内容を,ポリシーファイルに基づいてチェックし,その結果を返信する。ポリシー違反のアクセス要求については,結果の返信と共にログファイルへの登録も行う。

4.2 IRACS 自体の保護策

IRACS が確実に機能することを保証するために,不正にセキュリティ機能を無効化させない等,IRACS 自体のセキュリティを考慮する必要がある。

そこで報告者等は,下記 3 つの観点から脆弱性を排除することとした。

(1) 回避の防止

・**ファイルアクセスインターセプト機能の保護**:ファイルアクセスインターセプト機能を回避して,不正なファイルアクセスを行われない事が必要である。監視プログラムは,サービス用 OS における全てのファイルアクセス処理を司るファイルシステムドライバへの要求を全てインターセプトするように実装している。アプリケーションレベルからこのインターセプトを回避することは出来ない。

(2) 干渉の防止

・**ポリシーファイル・ログファイルの保護**:ポリシーファイルやログファイルは,その改竄や盗聴がされないようにセキュリティ OS が管理する記憶媒体に保管している。ナノカーネルドライバの機能により,ポリシーファイル・ログファイルをサービス OS から干渉できない。

・**プログラム間通信路の保護**:IRACS のプログラム間には,アクセス可否情報などセキュリティ上重要なデータが流れる。IRACS では,プログラム間を流れるデータを不正に盗聴・改竄されないように対策を行っている。また,プログラム間の通信路は必要最小限のものだけとすることで,IRACS への侵入を防止している。

・プログラムファイルの保護:IRACS のプログラムファイルはサービス OS の記憶媒体に保存されている。その改竄・消去を防止するために, IRACS では情報ファイルを保護する方法と同様に, ポリシーの設定によりプログラムファイルを保護している。

(3) 不活性化の防止

・プログラムの不停止:IRACS のアクセス制御機能を停止させ, 不正ファイルアクセスを行われないように, IRACS の各プログラムは, サービス用 OS 稼働中にユーザーの操作によって自由に停止出来ないように実装している。

5. WWW への適用例

IRACS の適用について, WWW サーバを利用した通信販売システムの要塞化を例にとって説明する。

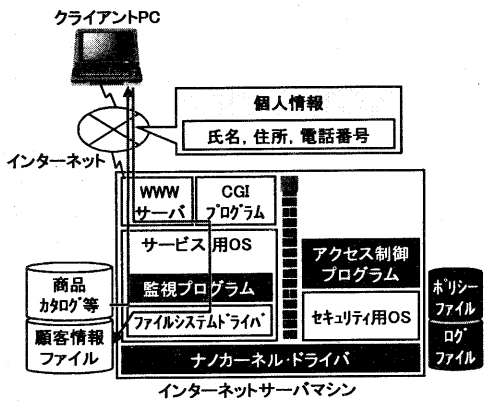

図 3 通信販売システムへの適用例

通信販売システムの概要を図 3に示す。通信販売システムの利用者は自宅等の PC を用いてインターネット経由で商品を購入することが出来る。通信販売システムを利用した商品購入の流れを図 4に簡単に説明する。

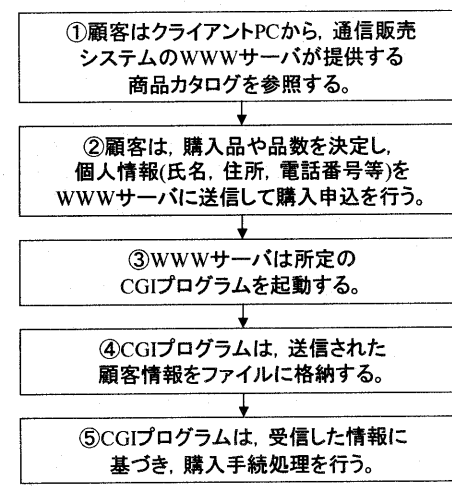

図 4 商品購入フロー

ここでは, WWW サーバが侵入されたことを前提とした場合の, IRACS によるファイルの完全性・機密性確保について述べる。商品カタログ等のファイルについては, その改竄をされないことが必要である。また, 顧客情報ファイルについては, 改竄防止だけでなく, 機密性の確保も必要である。IRACS に上記のファイルの保護を行うために, 通信販売システムを運用するために必要最小限のアクセスだけを許可するようにポリシーを設定する。

(1) 商品カタログ

・WWW サーバによる読み込み:商品カタログを公開するためには, WWW サーバプログラムが商品カタログを読み込む必要がある。

・商品カタログ編集用ツールを WWW ページ管理者が用いたときの読み込み・書き込み:商品カタログの更新を行うためには, その管理者が, 正規の編集用ツールを就業時間内に利用した場合に読み込み・書き込みが出来ればよい。

(2) 顧客情報ファイル

・CGI プログラムによる書き込み:通信販売システムを運用するためには, 所定の CGI プログラムのみが顧客情報ファイルに追記できれば良い。

上記に挙げたアクセスのみを許可するようにアクセス制御ポリシーを設定し，IRACS によるアクセス制御を行う。IRACS によるアクセス制御の流れを図 5に示す。

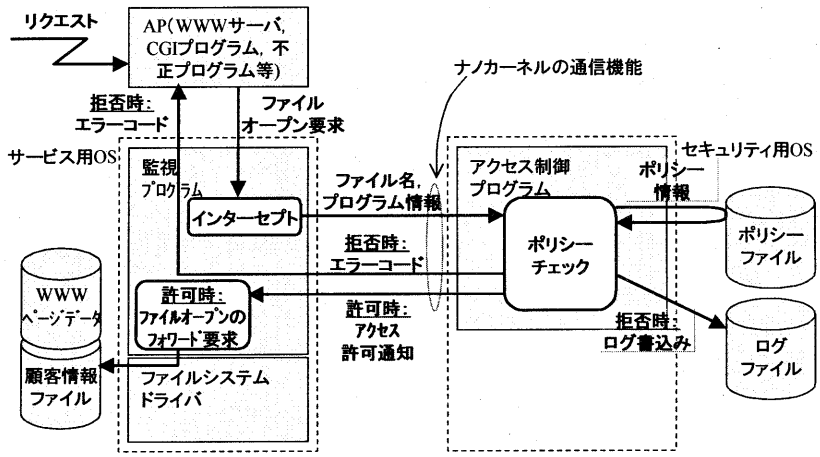

図 5 アクセス制御の流れ

IRACS によるアクセス制御を行うことで，攻撃者が WWW サーバに対し侵入などの攻撃を行った場合でも，商品カタログの改竄や，個人情報の盗聴・改竄の脅威の発生可能性を抑えることが出来る。さらに，ファイルへのアクセスが許可されたプログラムについては，例えば，商品カタログ編集用ツールを可搬記憶媒体に格納し，必要なときのみマウントして利用することで，より高いセキュリティを実現できる。

6. IRACS の性能評価

IRACS は，インターネットサーバにおける不正アクセス対策を目的として開発したものである。インターネットサーバは短時間に集中的なアクセスが行われることがあるため，その性能が重視される。IRACS のアクセス制御機能のオーバーヘッドがインターネットサービスの運用に大きな影響を与えないことが重要である。ここでは，WWW サーバへの適用を想定した性能評価結果を示す。

先ず，WWW サーバの一般的な性能を把握するため，米 Keynote 社による，著名な 40 サイトの WWW ページについての性能評価レポートの一部を表 1に示す[5]。

表 1 WWW サイト性能評価

(時間単位:ミリ秒)	40 サイト平均	高速 5 サイト平均	低速 5 サイト平均
コンテンツ数	20	13	39
WWW ページダウンロード時間	2640.0	1130.0	5790.0

表 1によると，WWW サイトの平均レスポンス時間は，約 2.6 秒である。一般に，オンラインマンマシンシステムの望ましいレスポンス時間は，3.0 秒以内であると言われている[6]。そこで，IRACS を搭載した WWW サーバの平均レスポンス時間が 3.0 秒以内であることを，IRACS の性能目標とする。

次に，IRACS の性能について検証する。IRACS の処理をポリシーチェック処理と，OS 間通信処理に大別し，それぞれの所要時間を計測するために3つのタイプのサーバを用意した。

(1) IRACS 無しサーバ

IRACS を搭載せずに，OS のファイルアクセスに掛

かる時間を計測する。

(2) マルチOS版IRAC搭載サーバ

本報告のIRACSをサーバに搭載し，IRACSによるオーバーヘッドを計測する。

(3) シングルOS版IRACS搭載サーバ

シングルOS版IRACSは，OS間通信処理を計測するために用意したものである。ナノカーネルドライバを使わずに，サービス用OS内に監視プログラムとアクセス制御プログラムを実装した。

上記(1)～(3)のそれぞれのタイプについてファイル読み込みに要する時間を実測した結果を表2に示す。本結果は，Pentium III 667MHz，128M RAM，HDD 12GBのマシンにWindows NT4 SP6をインストールして，1kバイトのファイルに対して1000回のファイル読み込みを行った場合に要した時間の平均をとったものである。また，表2には上記(1)～(3)をWWWサーバへ適用したことを想定して，WWWページダウンロード時間の予測値と，IRACS未使用時を100%としたときの低下率も示す。この予測値は，下式により算出している。

マルチOS版:(IRACS未使用時のWWWページダウンロード時間)＋((マルチOS版IRACS適用時のファイル読み込み時間)－(IRACS未使用時のファイル読み込み時間))×(コンテンツ数).

シングルOS版:(IRACS未使用時のWWWページダウンロード時間)＋((シングルOS版IRACS適用時のファイル読み込み時間)－(IRACS未使用時のファイル読み込み時間))×(コンテンツ数).

また，OS間通信処理の時間と，ファイルオープンインターセプト処理と，ポリシーチェック処理に要する時間は下式により求めることが出来る。

OS間通信処理時間:(マルチOS版IRACS適用時のファイル読み込み時間)－(IRACS未使用時のファイル読み込み時間).

ファイルオープンインターセプト処理時間＋ポリシーチェック処理時間:(シングルOS版IRACS適用時のファイル読み込み時間)－(IRACS未使用時のファイル読み込み時間).

表2 IRACSの性能評価結果

(時間単位:ミリ秒)	ファイル読み込み時間実測値	WWWページダウンロード時間予測値 (低下率:%)		
		40サイト平均	高速5サイト平均	低速5サイト平均
(1)IRACS未使用	0.114	2640.0 (100)	1130.0 (100)	5790.0 (100)
(2)マルチOS版IRACS	10.204	2841.8 (107.6)	1261.2 (111.6)	6183.5 (106.8)
(3)シングルOS版IRACS	0.250	2642.7 (100.1)	1131.8 (100.2)	5795.3 (100.1)

表2の予測値によると，マルチOS版IRACSをWWWサイトに適用したときのダウンロード時間は，平均で約2.8秒であることがわかった。これは，先に立てた目標レスポンス値の3.0秒を下回るものであるため，IRACSによる性能劣化は，WWWサイトの運用に影響を与えないと言える。また，IRACSのオーバーヘッドの原因は，マルチOS版IRACS適用時の性能低下率がシングルOS版IRACS適用時に比べて非常に大きいことから，インターセプト処理・ポリシーチェック処理よりも，OS間通信処理によるところが大きい。

7. まとめ

本報告では，IRACSの実装方式と性能評価結果について述べた。IRACSはその機能自体の保護を重視して実装し，回避・干渉・非活性化を防止し，より確実にアクセス制御機能を提供することが出来る。IRACSをインターネットサーバに適用することで，攻撃者がサーバへ侵入したときでも，ファイルの完全性と機密性を確保できる。また，IRACSのセキュリティ機能は，アプリケーションを一切書き換えることなく高いセキュリティを実現できる。

IRACSの性能評価結果によると，IRACS適用による性能の劣化はWWWサーバの性能にとって問題で

ないことがわかった。しかし，非常に高い性能を求められるWWWサイトへの適用を考えた場合は，OS間通信時間を重点に性能向上策を検討する必要がある。

[参考文献]

[1] 荒井他：マルチOS環境を利用したアクセス制御システム，情報処理学会，第61回全国大会 講演論文集(1), pp.45-46, 2000

[2] CERT®/CC, http://www.cert.org/

[3] 新井他：ナノカーネル方式による異種OS共存技術「DARMA」の提案，情報処理学会，第59回全国大会 講演論文集(1), pp.139-140, 1999

[4] 佐藤他：ナノカーネル方式による異種OS共存技術「DARMA」の実装，情報処理学会，第59回全国大会 講演論文集(1), pp.141-142, 1999

[5] Patrick Mills and Chris Loosley , Keynote Systems , A Performance Analysis of 40 e-Business Web site, http://www.keynote.com/services/assets/applets/Performance_Analysis_of_40_e-Business_Web_Sites.pdf , pp.3 , Copyright © 1996-2001 Keynote Systems, Inc.

[6] ヒューマンインターフェース調査研究会編："ヒューマンインターフェース", pp.48-49, 日本データ通信協会, 1990