社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (19)
2008－CSEC－ 40 (19)
2008／3／6

組込み機器におけるセキュアOSのポリシ追加機構

本田 篤史　朝倉 義晴　才田 好則　渡邊 光洋
NEC システムプラットフォーム研究所

概要

近年、組込み機器へソフトウェアを追加する機能が注目されている。これらソフトウェアにはバグやウィルスが存在する可能性があるため、セキュア OS を用いて安全性を確保する必要がある。セキュアOSがこれらのソフトウェアを適切に制御するために、セキュアOSのポリシを適切に設定する必要がある。そこで、組込み機器へのセキュア OS のポリシの追加を支援する機構を提案する。この機構は、各組込み機器のシステム構成に合わせて適切なポリシを設定する機能を持つ。さらに、ソフトウェアの動作をその信頼度に応じて限定させるために、設定可能なポリシを制限する機能を持つ。この機構を、SELinux を用いて実装し、その有効性を検証した。これにより、組込み機器でのセキュアOSのポリシの追加が容易になり、追加したソフトウェアを安全に動作させることが可能になった。

Policy addition mechanism of secure OS for embedded system

Atsushi Honda　Yoshiharu Asakura　Yoshinori Saida　Mitsuhiro Watanabe
NEC System Platforms Research Laboratories

Abstract

In recent years, a new function, which is to install software onto an embedded system, has been watched. However the installed software might include bugs or viruses. Then, it is necessary to protect the embedded system by secure OS. But the policy of the secure OS must set it strictly to control the installed software. Therefore, we propose the policy addition mechanism of secure OS for embedded system. The function of the proposed mechanism is an addition of the policy according to the system configuration. And it has the function to limit the policy that can be set to the software, because to limit the access of software according to the reliability of software. We implemented the proposed mechanism with SELinux, and verified the effectiveness. This mechanism achieves a secure software installation by adding the policy of secure OS.

1　はじめに

近年、携帯端末や情報家電といった組込み機器に対する要求が多様化している。これに伴い、製品出荷後の組込み機器に対してソフトウェアを追加する機能の実現が期待されている。この機能によりソフトウェアのバージョンアップや新規ソフトウェアの追加が容易になり、ユーザの要求に柔軟に対応できる。

製品出荷後の機器に対してソフトウェアを追加する機能を実現するためには、セキュリティの確保が重要な課題となる。組込み機器にはユーザの個人情報が記憶されているものが多い。また、電話機能のように常に稼動し続けなければならない機能が存在する。セキュリティを確保しなければ、追加したソフトウェアのバグや誤って追加されたウィルスによる、個人情報の外部への漏洩や、重要な機能の正常な実行の阻害といった事象が発生する可能性がある。

このような事象を防ぐ有効な手段としてアクセス制御がある。アクセス制御とは、あるサブジェクト（プロセス）による、あるオブジェクト（ファイル等）へのアクセスを制御することである。このアクセス制御を追加したソフトウェアに対して厳格に適用し、不必要な機能やファイルを操作させないことで、追加したソフトウェアのバグやウィルスから組込み機器を守ることができる。

このアクセス制御を実現するOSとして、セキュアOSがある。一般的にセキュアOSは、アクセス制御の規則が記述されたポリシ（セキュリティポリシ）を持ち、それに基づいて制御が行われる。このセキュア OS には、SELinux[1]やTOMOYO Linux[2]等がある。

セキュア OS が搭載された機器に新たなソフトウェアを追加する場合、セキュア OS によりその追加したソフトウェアを制御し、不正な処理や不正なアクセスを禁止する必要がある。しかし、セキュリティポリシにおいて想定していなかったソフトウェアが追加された場合、適切に制御することができない。そのため、追加したソフトウェアの実行が不可能になってしまう場合や、追加したソフトウェアによる不正な処理や不正なアクセスが可能になってしまう場合が考えられる。

追加したソフトウェアを適切に制御するためには、セキュリティポリシを設定する必要がある。そのため、追加するソフトウェアに応じて、そのソフトウェアに対するセキュリティポリシを同時に追加する機能が望まれる。

そこで我々は組込み機器に搭載されたセキュア OS におけるセキュリティポリシの追加を支援する機構を提案する。この機構によりソフトウェアに適用するセキュリティポリシの追加が容易になり、組込み機器において安全に新たなソフトウェアを追加・実行することができる。

2　組込み機器でのポリシ記述の課題

セキュリティポリシには、サブジェクトのオブジェクトに対するアクセス権限を記述する。そのため、各ソフトウェアがアクセスするファイルやディレクトリを把握していないとセキュリティポリシを記述する事ができない。つまり、セキュリティポリシの記述者はソフトウェアの詳細な動作とソフトウェアを実行するシステムのファイルやディレクトリの構成を熟知している必要がある。そのため、一般ユーザが使用する組込み機器において、ユーザ自身がセキュリティポリシの設定を行うことは困難である。また、セキュリティポリシをソフトウェア作成者が記述し、各組込み機器に配布し適用するという手法が考えられる。しかし、組込み機器は、メーカや機器によってファイルやディレクトリといったシステム構成が大きく異なり、必要なセキュリティポリシの設定も異なる。そのため、ソフトウェア作成者が、各組込み機器の構成を把握し、最適なセキュリティポリシをそれぞれ記述することは現実的でない。

このような理由から組込み機器では、追加されるソフトウェアに対するセキュリティポリシの適切な設定が困難である。追加されるソフトウェアに対して適切なセキュリティポリシが設定できなければ、十分なセキュリティを確保することができない。我々が提案するセキュリティポリシ追加機構は、追加するソフトウェアに対するセキュリティポリシを容易に設定可能にする。

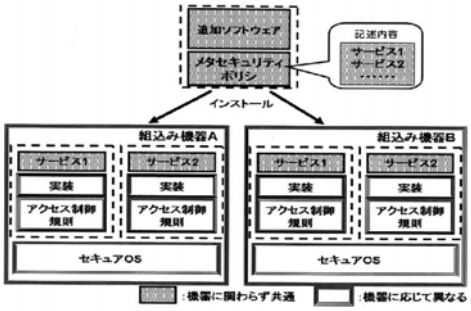

図 1　対象とする環境

3　セキュリティポリシ追加機構

提案するセキュリティポリシ追加機構では、組込み機器に搭載されたセキュア OS のセキュリティポリシの追加を支援する。

まず、対象としている環境について述べる。セキュリティポリシ追加機構は、次の 3 つの条件を満たしている環境を対象としている。1 つ目の条件は、各機器にはセキュア OS が搭載されていることである。ただし、各機器のファイルやディレクトリといったシステム構成と、搭載されているセキュア OS の種類は、それぞれ異なっていても良い。2 つ目の条件は、セキュリティポリシはソフトウェアと共に追加され、そのセキュリティポリシには同時に追加するソフトウェアに関する設定が記述されることである。3 つ目の条件は、各機器には追加されたセキュリティポリシをセキュア OS に適用する機能があることである。この対象とする環境を図 1 に示す。

次に、セキュリティポリシ追加機構の概要について述べる。セキュリティポリシ追加機構では、機器が追加するソフトウェアに対して提供しているネットワークの使用や画面への表示といった処理（サービス）を抽象化して定義する。この抽象化されたサービスとそのサービス名は、各機器の間で統一されている。そして、ソフトウェア実行時にこれらサービスを利用するためのアクセス権限を与える規則（アクセス制御規則）が各機器で定義されている。このアクセス制御規則は、各機器のファイルやディレクトリといったシステム構成に合わせてそれぞれ定義されている。このアクセス制御規則は、各機器のシステム構成を熟知している機器メーカ等が定義する。そして、ソフトウェア作成者は、作成したソフトウェアが使用するサービスをこの抽象化されたサービス

の中から選択し、そのサービス名をセキュリティポリシに記述する。このセキュリティポリシが追加されると、記述されたサービスを使用できるように、その機器のシステム構成に合わせたアクセス制御規則がセキュアOSに設定される。これにより、ソフトウェア作成者はそのソフトウェアが使用するサービスを指定するだけで、アクセス制御規則を考慮することなくセキュリティポリシを設定することができる。

セキュリティポリシ追加機構では、「メタセキュリティポリシ」、「アクセス制御マクロ」、「セキュリティポリシ設定モジュール」、「セキュリティポリシ制限モジュール」を要素として持つ。セキュリティポリシ設定モジュールで各機器のシステム構成に合わせたセキュリティポリシの適用を実現し、セキュリティポリシ制限モジュールで追加するソフトウェアの信頼度に応じたセキュリティポリシの設定の制限を実現する。構成を図2に示し、これら要素についてそれぞれ述べる。

3.1 メタセキュリティポリシ

メタセキュリティポリシは、ソフトウェアと同時に追加されるセキュリティポリシである。このメタセキュリティポリシには、同時に追加するソフトウェアが利用する機器内のサービスのサービス名を記述する。サービスとは、前述した抽象化したサービスであり、ネットワークの使用や画面への表示等の処理単位である。このサービスとそのサービス名は、各機器の間で統一されている。

3.2 アクセス制御マクロ

アクセス制御マクロは、前述した各機器で統一されているサービス毎にそれぞれ各機器で定義されている。1つのサービスに対して1つのアクセス制御マクロがそれぞれ定義され、ソフトウェアがそのサービスを利用するためのアクセス制御規則が記述されている。そして、その内容はシステム構成に基づいて機器毎に異なる。つまり、各機器でネットワークを使用するためのサービスが定義されている場合でも、アクセス制御マクロの内容は、そのシステムが搭載しているセキュアOSや、ポート毎にアクセス制御を実施しているか否かによって異なる。

3.3 セキュリティポリシ制限モジュール

セキュリティポリシ制限モジュールは、メタセキュリティポリシに記述可能なサービス名を制限する。まず、予めソフトウェア作成者の信頼度に応じて追加するソフトウェアに属性値を割り当てておく。そして、その属性値に応じてメタセキュリティポリシに記述可能なサービス名を制限する。これにより、追加するソフトウェア作成者の信頼度に応じたセキュリティポリシの適用の制限を実現する。

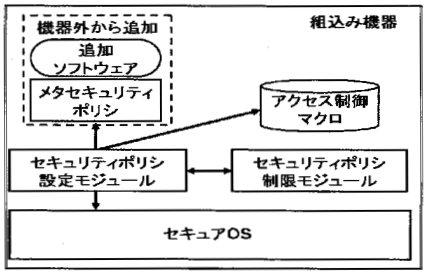

図2　システム構成

例えば、個人情報にアクセスするサービスを定義し、そのサービスの使用を機器メーカのソフトウェアだけに制限する。これにより、機器メーカ以外が作成したソフトウェアは、個人情報にアクセスを試みてもセキュリティポリシが設定されていないため、アクセスすることができない。つまり、個人情報へのアクセスを機器メーカだけに限定できる。

3.4 セキュリティポリシ設定モジュール

セキュリティポリシ設定モジュールは、メタセキュリティポリシからセキュリティポリシを作成する。前述したセキュリティポリシ制限モジュールによって記述内容が確認されたメタセキュリティポリシに記述されているサービスに対するアクセス制御マクロを展開し、追加するソフトウェアに対するセキュリティポリシを作成する。そして作成したセキュリティポリシをセキュアOSに適用する。

アクセス制御マクロは各機器のシステム構成に合わせてそれぞれ定義されているため、ソフトウェア作成者は、そのソフトウェアが利用する機器内のサービスさえ指定すれば、各機器に適したセキュリティポリシを適用することができる。これにより、各機器のシステム構成に合わせたセキュリティポリシの適用を実現する。

4 実装

我々は提案したセキュリティポリシ追加機構の実装を行った。その詳細と共にセキュリティポリシ追加機構の具体例として述べる。

今回の実装では、セキュアOSとしてSELinuxを使用した。SELinuxは、セキュリティポリシを部分適用する機能（Loadable Policy Modules[1]）を持つ。セキュリティポリシ追加機構を実現するためにメタセキュリティポリシ

とアクセス制御マクロを定義し、セキュリティポリシ制限モジュールとセキュリティポリシ設定モジュールを実装した。以降にその詳細を述べる。

4.1 メタセキュリティポリシの定義

メタセキュリティポリシは、サービス名のみが記述されている。1行に1つのサービス名が記述されており、これ以外が記述されていると記述規則違反となり、そのメタセキュリティポリシは追加されない。また、サービス名はアクセス制御マクロのファイル名同一であり、このメタセキュリティポリシに「service1」と記述してある場合は、アクセス制御マクロファイルの「service1」を展開することを意味する。メタセキュリティポリシの記述例を図3に示す。このメタセキュリティポリシはソフトウェアと一緒に機器に追加される。

4.2 アクセス制御マクロの定義

アクセス制御マクロは1つのファイルにつき、1つのサービスに対するアクセス制御規則が記述される。つまり、ネットワークを使用するためのアクセス制御規則が記述されたアクセス制御マクロや、X Window Systemを使用するためのアクセス制御規則が記述されたアクセス制御マクロをそれぞれ定義する。アクセス制御マクロを記述するファイル名は、そのファイルに記述されているサービスの名前と同一とした。アクセス制御マクロの記述例を図4に示す。allow文中の$1を除き、SELinuxのセキュリティポリシと同じ書式である。なお、allow文中の$1はアクセス制御マクロから実際のSELinuxのセキュリティポリシに変換される際に、追加したアプリケーションに割り当てられるSELinuxのドメインに置換される。ここで、ドメインとはアプリケーションに割り当てられるアクセス権限のことである。

4.3 セキュリティポリシ制限モジュール

セキュリティポリシ制限モジュールは、機器内にソフトウェアを追加するダウンローダからメタセキュリティポリシを受け取る。そして、受け取ったメタセキュリティポリシの内容を参照し、同時に追加されるソフトウェアの属性値に対して許可されていないサービスが指定されているかを検査する。

今回の実装では、追加されるソフトウェアは、その信頼度に応じて Operator/Manufacturer/Thirdparty/Untrusted の4種類の属性値に分類されるものとした。そこで、サービスもソフトウェアの属性値と同じく、Operator/Manufacturer/Thirdparty/Untrusted の4種類に分類した。属

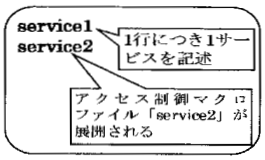

図3 メタセキュリティポリシ例

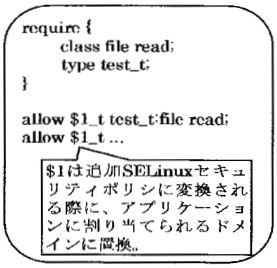

図4 アクセス制御マクロファイル例

表1 属性別アクセス制御マクロ記述可否

		アクセス制御マクロの属性			
		O	M	T	U
SWの属性	O	○	○	○	○
	M	×	○	○	○
	T	×	×	○	○
	U	×	×	×	○

O:Operator,M:Manufacturer,T:Thidparty,U:Untrusted
○：記述可、×：記述不可

性値がOperatorであるソフトウェアと一緒に追加されるセキュリティポリシには Operator/Manufacturer/Thirdparty/Untrusted の全てのサービスを指定でき、同様に Manufacturer には Manufacturer/Thirdparty/Untrusted 、 Thirdparty には Thirdparty/Untrusted、Untrusted は Untrusted のサービスをそれぞれ指定できる。これをまとめると表1のようになる。許可されていないサービスが指定されていた場合は、そのメタセキュリティポリシは追加されない。

4.4 セキュリティポリシ設定モジュール

メタセキュリティポリシに記述されているサービスとそれに対応するアクセス制御マクロを参照し、追加するソフトウェアに関するアクセス制御規則を記載した SELinux のセキュリティポリシを作成する。作成する SELinux のセキュリティポリシは Loadable Policy Modules に対応する形式である。

追加するソフトウェアに割り当てる SELinux のドメインは自動で決定する。そのドメイン名は「prefix_X_t」とし、"X"には0以上の整数が入る。この"X"に入る値は自動的に割り当てられる。

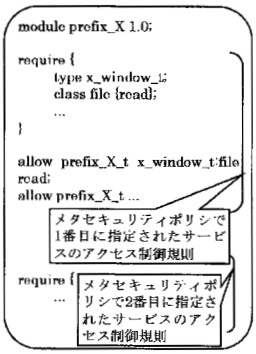

図 5　作成される te ファイル例

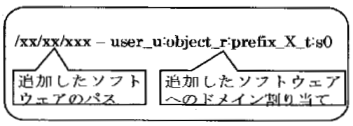

図 6　作成される fc ファイル例

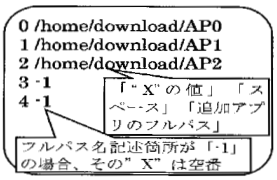

図 7　設定ファイル例

具体的に作成される SELinux のポリシファイルは te ファイルと fc ファイルの 2 つである。te ファイルは、メタセキュリティポリシに記述されているアクセス制御マクロを展開・マージして作成される。fc ファイルは、追加したソフトウェアのパスとそのソフトウェアに割り当てる SELinux のドメインが記述される。作成される te ファイルと fc ファイルの記述例を図 5 と図 6 に示す。そして、これら作成したセキュリティポリシを SELinux に適用する。

また、追加する SELinux セキュリティポリシの管理を行う。具体的には 4.4 節で述べた「prefix_X」の"X"に入る値を管理する。そのための、設定ファイルとして、追加したソフトウェアのパスと、そのソフトウェアのセキュリティドメインに割り当てた"X"の値を組みとして記述するファイルを保持する。この設定ファイルは、新たに追加したソフトウェアに割り当てる SELinux のドメイン名に含まれる"X"の値を決定するために参照される。"X"の値が決定されると、その値と追加したソフトウェアのパスを組みとして設定ファイルに記述する。この設定ファイルの記述例を図 7 に示す。

さらに、追加したソフトウェアを削除する際に、一緒に追加したセキュリティポリシも SELinux から削除する。そして、そのソフトウェアのパスを設定ファイルから削除し、設定ファイルを更新する。

表 2 類似技術との比較

	記述の容易性	異なるセキュア OS への適用	セキュリティ粒度
セキュリティポリシ追加機構	○	○	×
セキュリティポリシ編集エディタ	×	×	○

5　考察

提案したセキュリティポリシ追加機能について類似技術と比較し、4 章で述べた実装例に関する性能測定を行った。

5.1　類似技術との比較

提案したセキュリティポリシ追加機能との類似技術との比較を行った。対象とする類似技術は、セキュリティポリシの編集エディタである。セキュリティポリシ編集エディタには、SELinux のセキュリティポリシを設定する Tresys Brickwall[3]といった製品や、各セキュア OS の開発者が提供しているものがある。また、セキュリティポリシの設定を簡易化する研究[4]も行われている。これらセキュリティポリシ編集エディタは、複雑なセキュリティポリシの設定の支援を目的としている。そこで、提案したセキュリティポリシ追加機構とセキュリティポリシ編集エディタを比較し、システム構成に合わせたセキュリティポリシの作成の簡易さを比較する。ここでは、各機器に追加するソフトウェアに対するセキュリティポリシを対象とする。

比較する項目は、(1)記述の容易性、(2)構成が異なるシステムへの適用、(3)セキュリティ粒度の 3 点である。比較した結果を表 2 に示す。

(1)　記述の容易性

セキュリティポリシ追加機構はアクセス制御マクロ識別子をメタセキュリティポリシとして記述するのみなので、記述が容易である。セキュリティポリシ編集エディタでは、支援を行っているがセキュリティポリシの全てを記述する必要があり、セキュリティポリシ追加機構と比較し、記述が困難となる。

(2)　構成が異なるシステムへの適用

セキュリティポリシ追加機構は、メタセキュリティポリシに記述されているアクセス制御マクロを基に各機器のシステム構成に合わせてセキ

ュリティポリを作成する。そのため、構成が異なるシステムへも適用できる。セキュリティポリシ編集エディタでは、各セキュアOS専用のものを使用し、システム構成に合わせてそれぞれセキュリティポリシを作成する必要がある。そのため、構成が異なるシステムへの適用が困難である。

(3) セキュリティ粒度

セキュリティポリシ追加機構は、メタセキュリティポリシに記述されているサービスに対応するアクセス制御マクロを展開し、セキュリティポリを作成する。ソフトウェアの信頼度に応じてサービスの利用は制限されるが、アクセス制御マクロの内容は予め機器毎に静的に定義されているため、展開されるセキュリティポリシは機器毎に固定される。セキュリティポリシ編集エディタでは、セキュリティポリシをソフトウェアやシステム構成に応じて細かく記述できる。そのため、セキュリティポリシ追加機構と比較し、きめ細かなセキュリティポリシを設定することができ、よりセキュリティ粒度が小さくなる。

なお、これらセキュリティポリシ編集エディタは、セキュリティポリシ追加機構のアクセス制御マクロを作成する際や、各ソフトウェアの作成者がそれぞれの機器に合わせてセキュリティポリシを作成する際には非常に有効なツールとなる。ただし、2章で述べたように、セキュリティポリシをそれぞれの機器に合わせてソフトウェア作成者が作成するのは困難であり、本稿で提案したようにシステム構成を熟知している機器メーカがそれぞれセキュリティポリシを設定する方が現実的である。

5.2 性能測定

4章の実装例について性能を計測した。測定環境は以下の通りである。

- CPU：Pentium Ⅲ 1.0GHz
- メモリ：256M
- Linux：Fedora Core 5
- SELinux のベースポリシ：160KByte

上記測定環境においてメタセキュリティポリシから SELinux のセキュリティポリシを作成し、適用するのにかかるセキュリティポリシ追加機構の処理時間を計測した。この処理時間には、セキュリティポリシ追加機能によって作成された SELinux のセキュリティポリシをバイナリへコンパイルする時間およびインストールする時間は含まれていない。また、測定に使用した各ファイルは表3に示す3種類である。

表3 測定に使用したファイル

	メタセキュリティポリシ	アクセス制御マクロ	作成されるTEファイル
測定1	5個のサービス指定	「$1」が2箇所（「prefix_X」への置換2箇所）	全28行（300Byte）
測定2	9個のサービス指定	「$1」が2箇所（「prefix_X」への置換が2箇所）	全48行（500Byte）
測定3	13個のサービス指定	「$1」が2箇所（「prefix_X」への置換が2箇所）	全69行（700Byte）

表4 測定結果

	測定1	測定2	測定3
処理時間（秒）	0.013	0.032	0.050

測定はそれぞれ10回行い、その平均値を計算した。測定結果を表4に示す。処理時間は短く、組込み機器で十分利用できると考えられる。

6 おわりに

本稿では、組込み機器において安全に新たなソフトウェアを追加・実行するために、セキュアOSのポリシの追加を支援するセキュリティポリシ追加機構について述べた。提案した機構では、システム構成に合わせてセキュリティポリシを適用する機能と、ソフトウェアの信頼度によるセキュリティポリシの設定を制限する機能を持つ。そして、SELinux を利用したセキュリティポリシ追加機構の実装例を示した。さらに、評価を行い、その有効性を検証した。

今後の課題は、組込み機器に適したセキュリティポリシやアクセス制御マクロの考案、様々なセキュア OS への適用例を示すことである。また、追加するセキュリティポリシの正当性の保証と検証方法も検討すべき課題である。

参考文献

[1] NSA SELinux
http://www.nsa.gov/selinux/

[2] TOMOYO Linux
http://sourceforge.jp/projects/tomoyo/

[3] Tresys Technology Products
http://www.tresys.com/products.html

[4] 中村 雄一，鮫島 吉喜，“Security-Enhanced Linux のアクセス制御ポリシ設定の簡易化”，2003年暗号と情報セキュリティシンポジウム（SCIS2003）予稿集，vol.2，pp.831-836，2003