2ZA-8

ユーザモードプロセスからカーネルモードプロセスへ受け渡しするデータを外部秘匿するロード手法

義則隆之† 佐藤両† 福田洋治‡ 毛利公美†† 白石善明† 野口亮司‡‡

名古屋工業大学† 愛知教育大学‡ 岐阜大学†† （株）豊通シスコム‡‡

1. はじめに

クラウドコンピューティングの普及により，端末とインターネットに接続できる環境があれば，企業などの組織の情報システムを組織外から利用可能となった．組織のポリシーによっては，個人が所有する端末で情報システムにアクセス可能な場合もある．しかし，端末を個人の管理に任せると，セキュリティに不安のあるアプリケーションソフトウェアを導入した端末が情報システムにアクセスする可能性がある．このような端末から情報漏えいするかもしれないので，情報システムにアクセスする端末は組織が管理することが望ましい．

組織が端末を一元管理する方法に，端末にポリシーファイルを配付し，ポリシー強制ポイント（Policy Enforcement Point：PEP）がポリシーファイルをロードして，ポリシーに従って動作させることで，端末で利用者の操作に制限を加えるという方法がある．利用者は端末を組織が許可した範囲内でしか動作させることができず，組織の期待する端末のセキュリティレベルを確保することができる．

端末がポリシーで定められた範囲でしか動作しないときにその強制が強すぎる場合は，端末の利便性を損なうこともある．特に，私用端末では利便性が低くなった場合に利用者がポリシーをリロードしない，あるいは不正なポリシーをロードさせることによって PEP の正常な動作を妨げるといった懸念がある．PEP は，ポリシーを適切に読み込んだことを前提として動作しているため，更新されたポリシーを読み込まなかった PEP がアクセス制御を適切に行っている保証はない．

組織利用において，アクセス制御が正しく動作していることを第三者に証明できることは，デジタルフォレンジックの観点から望ましい．その動作保証のためには，PEP が不正なポリシーをロードしないことを保証する仕組みの確立が課題となる．

本稿では，カーネルモードの PEP がユーザモードプログラムからポリシーファイルを受け取って動作に反映する処理を安全に行う手法を提案する．提案手法はポリシーファイルを暗号化して利用者に見せないという特徴を持つ．なお，ポリシー配付が安全に行われていることを前提として以下では議論を進める．提案手法を端末に組み込んだ場合の CPU 使用率と使用メモリ量の増加量について評価を行う．

2. フィルタドライバを用いたアクセス制御

端末のアクセス制御をするソフトウェアには，パーソナルファイアウォール，アンチウイルスソフトなどがある[1]．ファイアウォールなどのルールの設定は，端末の管理者権限を持つ利用者によって変更可能であり，組織が端末を管理するためには，容易に PEP の動作を妨げられてはならない．

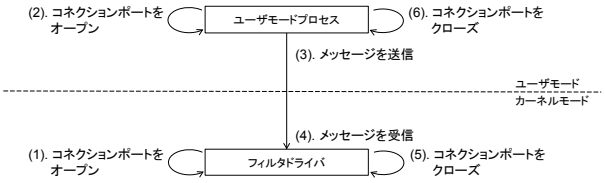

図 1 フィルタドライバによるメッセージ送受信方式

PEP は任意のアクセスを制御できなければならないので，一般にはカーネルモードで動作する．ここでは，カーネルモードのフィルタドライバを用いてアクセス制御することを考える．フィルタドライバとはシステム内の任意の入出力要求を捕捉，変更が可能なドライバであり，PEP の設定を変更されないようにするなどの強いレベルの制御が可能なものである．

ポリシーの更新があったときに，フィルタドライバが更新されたポリシーを受信してリロードするためには，組織のポリシー配付サーバと PEP 間でネットワーク通信を行う．しかし，カーネルモードプロセスにはネットワーク通信を行うライブラリが提供されていない．そこで，ユーザモードプロセスがネットワーク経由でポリシーをダウンロードし，フィルタドライバにポリシーデータを転送することで，フィルタドライバが更新されたポリシーをリロードする．

3. フィルタドライバのプロセス通信方法

プロセス間通信の方法は，メモリマップドファイル方式とメッセージ送受信方式の二つがある[2]．本稿では実装の容易さからメッセージ送受信方式を採用する．図 1 に示したメッセージ送受信方式の手順は以下のようになる．

(1) フィルタドライバがコネクションポートをオープン
(2) ユーザモードプロセスがコネクションポートをオープン
(3) ユーザモードプロセスがフィルタドライバにメッセージを送信
(4) フィルタドライバがメッセージを受信
(5) フィルタドライバがコネクションポートをクローズ
(6) ユーザモードプロセスがコネクションポートをクローズ

ポリシーデータをメッセージとして送受信することで，フィルタドライバにポリシーを渡せる．しかし，この方式では，(i)プロセス通信間（(3)~(4)の間）の通信パケットのキャプチャは容易であり，ポリシーデータの改ざんが行わ

A Method for Loading Data from User Mode Process to Kernel Mode Process with Confidentiality

† Takayuki Yoshinori, Ryo Sato and Yoshiaki Shiraishi・Nagoya Institute of Technology
‡ Youji Fukuta・Aichi University of Education
†† Masami Mohri・Gifu University
‡‡ Ryoji Noguchi・Toyotsu Syscom Corp.

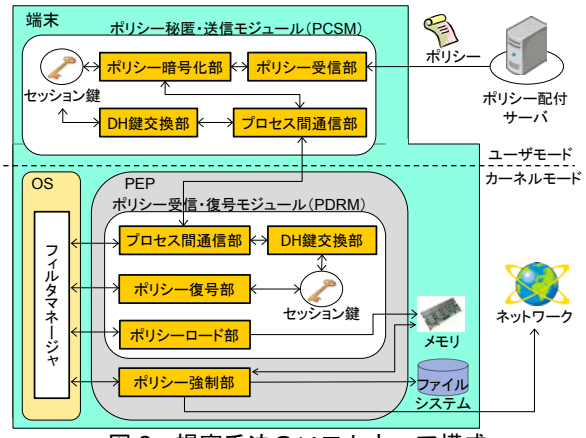

図２　提案手法のソフトウェア構成

れる恐れがある．また，(ii)フィルタドライバが受信したポリシーをファイルとして端末内に残してしまうと，ポリシーファイルに改ざんが加えられる恐れがある．

不正なポリシーが読み込まれることで，組織が意図するアクセス制御が適切に行われない可能性がある．そこで，ユーザモードプロセスとフィルタドライバ間のプロセス間通信を安全に行うために，ポリシーを利用者から外部秘匿する．

4.　提案手法の設計と実装

ポリシー配付サーバからのポリシーを受信するユーザモードで動作するポリシー受信プログラムに組み込まれる“ポリシー秘匿・送信モジュール”とカーネルモードで動作する PEP に組み込まれる“ポリシー受信・復号モジュール”を介した，プロセス間通信を用いた PEP へのデータロード手法を提案する．

提案手法は，ユーザモードアプリケーションからフィルタドライバに受け渡しされるポリシーを暗号化することで，ポリシーの改ざんがされないことを保証する．ポリシーの暗号化と復号には共通鍵暗号を用い，そのセッション鍵の共有は DH 鍵共有で行う[3].

ポリシー秘匿・送信モジュール(Policy Concealment / Sending Module：PCSM)：ポリシー配付サーバからポリシーを受信し，暗号化して PDRM に送信するモジュール．

ポリシー受信・復号モジュール(Policy Receiving / Decode Module：PDRM)：フィルタドライバで構成され，PCSM からポリシーを受信して復号し，メモリに格納するモジュール．

提案手法のシステムは図 2 のようになる．PCSM と PDRM を利用したプロセス間通信の流れを以下に示す．

(1) PCSM のポリシー受信部がポリシー配付サーバから更新されたポリシーをダウンロード
(2) PDRM のプロセス間通信部と PCSM のプロセス間通信部がコネクションポートをオープン
(3) PCSM のプロセス間通信部と PDRM のプロセス間通信部が互いの DH 鍵交換部により DH 鍵交換を行い，セッション鍵を共有
(4) ポリシー暗号化部がセッション鍵を用いてポリシーを暗号化し，PCSM のプロセス間通信部が PDRM のプロセス間通信部に暗号化されたポリシーを送信
(5) PDRM のプロセス間通信部はポリシーを受信し，フィルタマネージャはポリシー復号部に復号要求を渡し，ポリシー復号部はセッション鍵を用いてポリシーを復号
(6) フィルタマネージャはポリシーロード部に復号要求を渡し，ポリシーロード部はポリシーをロードし，メモリにポリシーを格納
(7) フィルタマネージャはポリシー強制部にロード要求を渡し，ポリシー強制部はメモリからポリシーをロードし，動作に反映

このようにプロセス間通信で送受信するポリシーデータを暗号化することで，(i)ポリシーデータの改ざんを防ぐことができる．また，ポリシーをメモリ内に格納し，ファイルとして端末内に残さないことで(ii)ポリシーファイルの改ざんを防ぐことができる．ポリシーが格納されているメモリの番地を取得し，指定のプロセス以外からはアクセスできないようにすれば，メモリ内のポリシーの改ざんを防ぐことができる．表 1 の開発環境で実装し，提案手法でポリシーファイルの受け渡しができることを確認した．

表１　開発環境と評価環境

CPU	Intel(R) Core™ i5-2504M CPU @2.60GHz
RAM	1GB
OS	Windows 7 Professional 32bit
Language	C
Development Tool	Microsoft Visual C++2010 Express

5.　評価

提案手法はプロセスが常駐してプロセス間通信を行うため，CPU やメモリへ負荷をかける．そこで，CPU 使用率と使用メモリ量の増加量を測定した．評価環境は表 1 と同一である．提案手法のプロセスが常駐するときは，常駐していないときに比べ，CPU 使用率は 0.1%，使用メモリ量は 1.02MB 増加した．また，容量 100KB のポリシーデータの受け渡しを 1 回の試行として，この試行を 10 回行い，平均を算出したところ，CPU 使用率は 15.8%，使用メモリ量は 13.20MB であった．このプロセス間通信に要した時間は約 0.01 秒であった．

6.　おわりに

組織の情報システムにアクセスする端末を管理するソフトウェアが，組織のシステム管理者によってインストールされるという状況の下でも，私用端末ではポリシーファイルの改ざんやリロードを妨害することで，アクセス制御を阻害することが可能となる．ポリシーファイルをポリシー強制の動作に反映させる処理を安全に行うために，ユーザモードプロセスからカーネルモードプロセスへ受け渡しするポリシーファイルを外部秘匿するロード手法を提案した．提案手法のフィルタドライバを組み込んだ場合で最も負荷がかかるプロセス間通信のとき，0.01 秒間だけ CPU 使用率は 15.8%，使用メモリ量は 1.02MB 増加すること，および，ポリシーファイルの受け渡しができることを確認した．

参考文献

[1] 東芝, “個人ユーザ向け常時接続端末におけるセキュリティ保護技術に関する研究開発” 研究開発成果報告書, http://itaku-kenkyu.nict.go.jp/seika/h14/seika/43/43toshiba.pdf, p.165, 2003 年 5 月(参照 2011-12-21)
[2] Microsoft Corporation, “User / Kernel Communication Model”, http://msdn.microsoft.com/ja-jp/windows/hardware/gg462968,pp.2-10, 2004 (参照 2012-1-10)
[3] W. Diffie and M. E. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, November, 1976.