ポリシー強制ポイントをエンドホストで実現するための通信制御機構の提案

大谷　佳輝† 毛利　公美† 白石　善明‡ 福田　洋治†† 野口　亮司†††
岐阜大学† 名古屋工業大学‡ 愛知教育大学†† 株式会社豊通シスコム†††

1. はじめに

近年，クラウドコンピューティングによるデータセンターサービスの需要が高まっている．このようなモデルでは，データセンター内のサーバはクラウド外の組織のホストから要求を受け付ける．しかし，セキュリティレベルの低いホストも存在し，データセンターを介してセキュリティ被害が拡大する恐れがある．

そこで本研究では，ポリシーアクセス制御を実施するために，ホスト側のフィルタドライバで信頼できる通信だけをセンター側に到達させる通信制御機構を提案する．

2. 想定しているモデル

我々の研究グループでは，エンドホストが端末検証局から端末の真正性を表す証明書を取得し，データセンターへの接続要求の際に証明書を提示することでホストの信頼性を保証するモデルを提案している[1][2]．従来のモデルでは，ポリシー強制ポイントがデータセンター側に存在していたため，データセンター以外へのきめ細かい通信制御サービスを提供することができなかった．これに対して，提案モデルではホスト側のフィルタドライバで宛先 IP アドレスや証明書の有無を判別し通信の制御を行う（ポリシー強制ポイントをエンドホストで実現）ことで，きめ細かい通信制御を実現できる．証明書はセキュリティレベルの高い信頼できるホストのみ発行されるため，データセンターの各サーバはセキュリティレベルの低いホストから接続要求を受けることはなく，信頼できるホストからの接続要求のみを受け付けることになる．

また，ホストはデータセンターの各サーバと通信する前に必ずデータセンター内のアクセス制御管理サーバと通信を行う．このとき，ホストはアクセス制御管理サーバからポリシーを元に作成された，通信を許可するサーバの宛先 IP アドレスやポート番号が記述されたリストを受け取る．これより，ホストはリストに記述されている宛先 IP アドレスやポート番号に通信データを送信することで目的のサーバと通信することができるようになる．

図1に想定しているモデルを示す．

3. 通信制御機構

3.1 モデルを実現するために必要なエンドホストの機能

図1に示した想定しているモデルにおいて，エンドホストで通信制御を行うためには，ホスト側に以下の機能が必要となる．

機能1　通信データの宛先判別
機能2　ホストの証明書の有無の判別
機能3　通信データのバッファリング
機能4　証明書の要求
機能5　証明書の取得確認

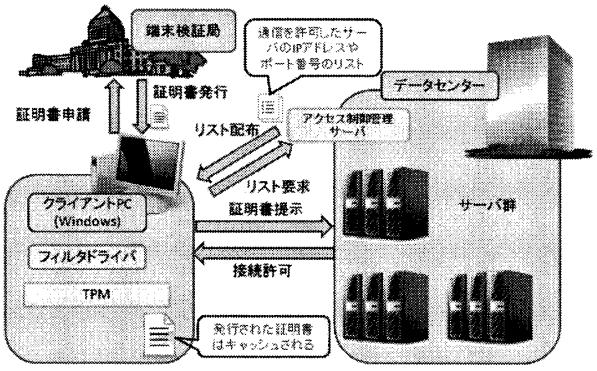

図1　ホストの信頼性を保証するクラウドコンピューティングによるデータセンターサービスのモデル

データセンターからサービスを受ける企業のネットワーク内の端末の多くは Windows 端末であるため，本研究のエンドホストは Windows 端末を対象とする．通信制御をアプリケーションで行うと，アプリケーションの停止やデータの改ざんなどの攻撃が容易に行われ信頼性が低下するため，フィルタドライバで通信制御を行う．フィルタドライバは NIC を制御するミニポートドライバに介入するデバイスドライバで，ローレベルで動作するため信頼性が高い．Windows では NIDS フィルタドライバ（以下，フィルタドライバ）が提供されているためフィルタドライバに各機能を実装し，通信制御を行う．これらの機能を用いたエンドホストで実現すべき通信制御機構の動作を図2に示す．

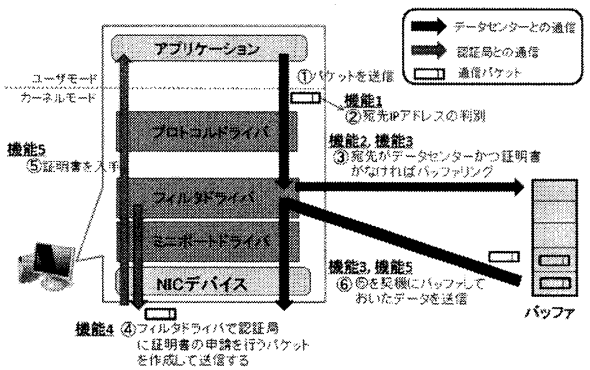

図2　エンドホストで実現すべき通信制御機構の動作

3.1.1 宛先判別部

ホストが通信を行うのはデータセンターだけではない．そのため，ホストが行う通信を制御するには通信データの宛先を判別する必要がある．

フィルタドライバの送信介入部の中にある宛先判別部では，送信するパケットの宛先 IP アドレスを読み取り，データセンター宛てのパケットであるかを判断する．データセンター宛てのパケットであれば証明書判別部にパケットを渡し，データセンター以外の宛先であればパケットを通過させるといった処理を行う．

これにより，通信データの宛先に応じた通信の制御を行うことができる．

Development of Communication Control Mechanism for Working as Policy Enforcement Point on End-Host
† Yoshiki Ohtani and Masami Mohri ・Gifu University
‡ Yoshiaki Shiraishi ・Nagoya Institute of Technology
†† Youji Fukuta ・Aichi University of Education
††† Ryoji Noguchi ・Toyotsu Syscom Corp.

3.1.2 証明書判別部

2 節で述べたように，ホストがデータセンターに接続要求を行うためには端末検証局から発行された証明書をホストが所持している必要がある．

フィルタドライバの送信介入部の中にある証明書判別部ではホストが証明書を所持しているかの判別を行う．証明書を所持していない場合は，データセンターに接続要求を行うことはできないため，バッファ部にパケットを渡す．証明書を所持している場合は，パケットを通過させデータセンターに送信する処理を行う．これにより，証明書を持たないホストとデータセンターの通信を制御することができる．

3.1.3 バッファ部

データセンター宛てかつ証明書を持たない通信データはバッファ部に渡される．

ホストがデータセンターに対して接続要求を行った時点で，ホストは証明書を確実に所持しているとは限らない．フィルタドライバの送信介入部の中にあるバッファ部では，証明書判別部から渡されたパケットをバッファリングする処理を行い，証明書要求部に証明書申請の要求を出す．バッファリングされたパケットは，バッファ部が証明書取得部から出された解放要求を受け入れた後に解放され，フィルタドライバを通過し，データセンターに接続要求が行われる．これにより，証明書を持たないホストがデータセンターに送信した通信データを破棄せずに通信を制御することができる．

3.1.4 証明書要求部

3.1.3 節で述べたように，ホストが証明書を所持していない場合は，通信データは送信されずにバッファリングされるため，データセンターに接続要求を行うためには端末検証局に対して証明書を要求し，発行してもらう必要がある．

フィルタドライバの送信介入部の中にある証明書要求部は，バッファ部でパケットがバッファリングされたことを契機に呼び出される．呼び出された証明書要求部は，端末検証局に対して証明書を申請するパケットを作成し，送信する必要がある．これにより，必要に応じて随時証明書の要求を行うことができる．

3.1.5 証明書取得部

証明書要求部が端末検証局に対して証明書を申請した場合，端末検証局により発行された証明書をホストが取得したことを確認する必要がある．

フィルタドライバの受信介入部の中に存在する証明書取得部では，証明書要求部が端末検証局に対して証明書の申請を行った後，端末検証局から証明書が発行されたことを判別する．証明書取得部で証明書の発行が確認されるとデータセンターとの通信が可能になる．また，バッファ部にバッファリングしたパケットが存在する場合はバッファ部に通信データの解放要求を出す．これにより，証明書を所持していない状態で接続要求を行い，バッファ部でバッファリングされたパケットは信頼できるホストからの接続要求ということが保証される．

3.2 フィルタドライバによる通信制御機構の実装

3.1 節で述べた機能をフィルタドライバに実装する．エンドホストでアクセス制御するための通信制御機構を図 3 に示す．ホスト側のフィルタドライバに図 3 のような通信制御機構を持たせることにより，エンドホストでアクセス制御を行うことが可能となり，2 節で示したモデルを実現することができる．

4. 実験

以下のようなデータセンターサービスを模倣した簡易な環境で，今回開発したフィルタドライバによる通信制御機構の動作確認を行った．

[動作環境]

・データセンターサービス
　データセンターで提供されるサービスを模倣するために FTP サーバと Web サーバを用意した．

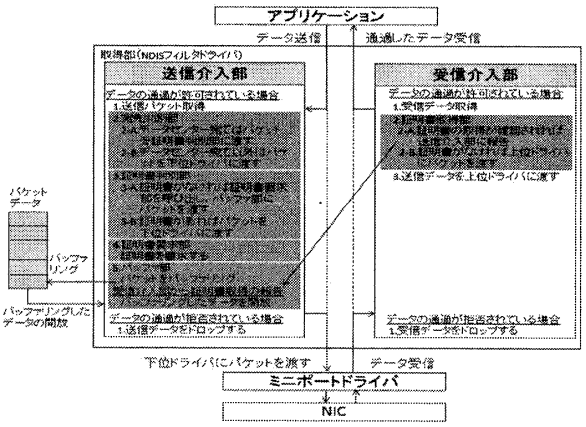

図 3　NDIS フィルタドライバによる通信制御機構

・端末検証局
　ホストから検証要求を受け取った際に，検証結果によって値（0：証明書なし or 1：証明書あり）を返す端末検証サーバを用意した．

・アクセスリスト
　今回の実験では，ホストがアクセス制御管理サーバから既にリストを入手している状態を仮定し，前述の Web サーバと FTP サーバの IP アドレスとポート番号の組をアクセスリストとしてホスト側に保持させて動作確認を行った．

[実験内容]

開発した通信制御機構を導入したホストでクライアントプログラムを利用し，アクセスリストに記載されている FTP サーバおよび Web サーバに接続を試み，以下の動作が正しく行われるか確認する．

ホストが端末検証サーバから 0 を受け取った場合，データセンター宛ての通信を遮断し，パケットのバッファリングを行う．1 を受け取った場合は，パケットを通過させ，バッファリングしているパケットを解放する．

また，ブラウザで Web ページを閲覧する場合のバッファリングされるデータ量についても測定する．

[実験結果]

・データセンターサービスを模倣した環境での動作検証
　ホストが 1 を受け取るまでは，コマンドライン上から FTP サーバに接続要求を出しても応答が返らず，1 を受け取った後に，先の要求に対する応答が返ってきた．これより，1 を受け取るまでは接続が遮断されており，ホストが 1 を受け取った後にバッファリングしたデータを解放していることが確認できた．

・バッファリングされるデータ量の測定
　ホストのブラウザを使って Web サーバにアクセスした場合，バッファリングされるデータ量は遮断時間に左右　されることなく，1 回のアクセス毎に 194Byte（SYN パケット 3 個分）ずつ増加することを確認した．

5. おわりに

ホスト側のフィルタドライバで通信制御を行うことにより，ポリシー強制ポイントをエンドホストで実現するための通信制御機構を提案・実装し，動作確認を行った．

参考文献

[1] 脇田知彦，白石善明，毛利公美，福田洋治，野口亮司，“サーバサイドのネットワークを保護するための TPM を用いた接続資格保障基盤”，情報処理学会第 72 回全国大会講演論文集，2010 年（掲載予定）．

[2] 佐々木啓，白石善明，毛利公美，福田洋治，野口亮司，“エンドポイントでポリシー強制を行うアクセス制御フレームワーク”，情報処理学会第 72 回全国大会講演論文集，2010 年（掲載予定）．

[3] 福田洋治，溝渕昭二，毛利公美，白石善明，野口亮司，“ネットワークフォレンジックのためのホスト型のロギングについて”，　電子情報通信学会総合大会基礎・境界講演論文集，AS-1-3，2009 年．