論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻

学生番号	12675013	氏　名	土田　賢太朗
論文題目	ファイルシステムキャッシュを考慮した仮想マシン監視機構		

1　はじめに

サーバへの攻撃を検知するために侵入検知システム（IDS）が用いられている．そのため，サーバホストに侵入した攻撃者は IDS を無力化してからサーバへの攻撃を行うようになってきた．このような攻撃に対して，仮想マシン（VM）を用いて IDS を別の VM にオフロードして監視を行う手法が提案されている．この手法では侵入困難な VM で IDS が動作するため，攻撃者は IDS を無効化することが難しくなる．しかし，オフロードした IDS は監視対象システムのディスクを直接監視することになり，監視対象 OS がメモリ上に保持しているファイルシステムのキャッシュを考慮できなくなる．その結果，ディスクに書き戻されていないデータは監視できなかった．

本研究では，監視対象 VM の仮想ディスクとファイルシステムキャッシュを統合する *CacheShadow* **ファイルシステム**を提案する．

2　CacheShadow ファイルシステム

CacheShadow ファイルシステムは図 1 のようにオフロード先の IDS VM 上で動作し，監視対象のサーバ VM のファイルシステムの情報を提供する．このファイルシステムはファイルシステムキャッシュをサーバ VM のメモリから取得し，ファイルシステムキャッシュ上に最新の情報があればその情報を返し，なければ仮想ディスク上の情報を返す．このようにして，IDS VM 上の IDS はサーバ VM のファイルシステムに関する最新の情報をより安全に得ることができる．

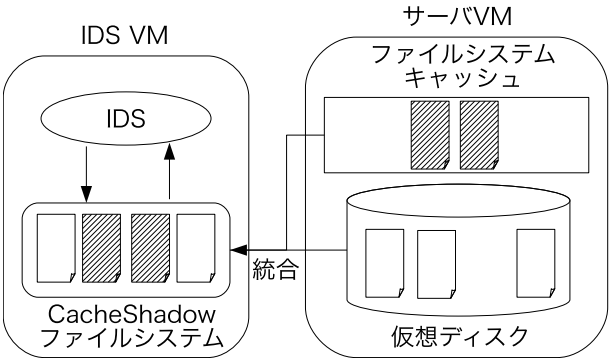

図 1: CacheShadow ファイルシステム

CacheShadow ファイルシステムは，ファイルシステムキャッシュとしてページキャシュ，ディレクトリキャッシュ，メタデータキャッシュを扱う．ページキャッシュはファイルのデータそのもののキャッシュである．CacheShadow ファイルシステムはサーバ VM 上のすべてのメモリページを調べ，ページキャッシュを見つけ出す．ファイルの読み込み要求の際に，ページキャッシュ上のデータを優先しながら仮想ディスク上のファイルのデータとマージする．

ディレクトリキャッシュは各ディレクトリに含まれるファイル情報やサブディレクトリ情報のキャッシュである．CacheShadow ファイルシステムはディレクトリをたどることでディレクトリキャッシュを取得する．ディレクトリの読み込み要求の際に，ディレクトリキャッシュを優先しながら仮想ディスク上のディレクトリ情報とマージする．

メタデータキャッシュはファイルの更新時刻やサイズの情報である．メタデータの読み込み要求の際に，CacheShadow ファイルシステムはメタデータキャッシュがあればそれを返す．

3　実験

Xen4.11 上に実装した CacheShadow ファイルシステムを用いて，サーバ VM 上で動作している Linux2.6.39 にキャッシュされたファイルを読み込む時間を測定した．本実験にはサーバ VM に 1GB のメモリを割り当てた．IDS VM からサーバ VM のメモリにアクセスするため，サーバ VM 上で直接ファイルを読み込む場合と比べて，約 7 倍の時間がかかることが分かった．

4　まとめ

本研究では，監視対象システムのファイルシステムキャッシュと仮想ディスクを統合する CacheShadow ファイルシステムを提案した．CacheShadow ファイルシステムを用いることで，オフロードされた IDS が常にファイルやディレクトリの最新情報を監視することができる．