M_024

シンクライアント環境におけるファイルシステムの完全性検証とその実装

Study and implementation of integrity verification for Thin Client

櫻井 恒男† 丹 英之† 阿部 大将† 北川 健司† 千葉 大作† 濱野 裕樹†
Tsuneo Sakurai Hideyuki Tan Daisuke Abe Kenji Kitagawa Daisaku Chiba Hiroki Hamano

1．はじめに

パスワード，バイオメトリックによるユーザ認証でサービスにアクセスするユーザを判別しても，そのユーザが扱う端末のファイルシステムに悪意あるソフトウェアがインストールされているかを判別することはできない．CD-ROMから起動し，起動するたびにクリーンなOSを使用することができるKNOPPIX[1]をシンクライント仕様にカスタマイズし，一般的な端末をシンクライアント端末として利用する．[2]

CD-ROM起動のOS，KNOPPIXを使用するにあたりそのファイルシステムの構成が管理者の意図した構成であるかを判別する必要がある．使用するKNOPPIXのファイルシステム完全性の検証方法とその実装についてまとめる．

2．シンクライアント

2005年から個人情報保護法執行や最近の内部情報の漏えい問題など企業におけるセキュリティ対策への意識は高まっている．[3]

セキュリティ対策として，ハードディスクの暗号化，アンチウィルスソフトウェア，バイオメトリックによるユーザ認証などがあげられるが，ハードディスクなどの記憶装置を持たず，必要最小限の機能だけを備える端末で，データやソフトウェアは全てサーバが保持し，サーバにアクセスしその資源を使用するシンクライントが注目されている．

以下にシンクライアントのメリットをまとめる．

- ハードディスクレスによるデータの持ち出し防止と維持管理費用削減
- クライアントが使用するソフトウェアの集中管理
- ファイルシステムやソフトウェアのアップデート作業の費用削減

しかし，シンクライアント専用端末を用意するにはコストがかかるため，一般的なPC端末をシンクライアント端末として使用する手法が注目されている．このような手法の中でも最も簡易なものが，CD-ROMなどのメディアにOSを格納し，格納されているOSイメージから毎回クリーンなOSを起動する方法である．このOSイメージにおいて，周辺デバイスへのアクセス，ネットワークアクセスの制限を加えることで情報漏えい経路を遮断したシンクライアント環境を一般的な端末を利用して構築することができる．ただし，確かに情報漏えい経路を遮断したシステムであることを確認する必要が残っている．

3．ファイルシステムの完全性検証

3．1先行研究

ファイルシステムの完全性検証に関する先行研究として，中村らによるTPM（Trusted Platform Module）にファイルシステム全体をブロック単位でハッシュ値（期待値）を計算し期待値リストとして保存し，アクセスのあった該当ブロックに対するハッシュ値が期待値リストに等しいかどうかを検証する手法が提案されている．[4]

本稿は読み込むファイルシステムをランダムに選択し、そのブロックからハッシュ値を算出し検証を行う点が特徴である．

3．2ファイルシステム完全性検証の手法

KNOPPIXのファイルシステムはcloop(Compress LOOPback device)ファイルと呼ばれる，ファイルをハードディスクドライブのように扱うことができる機能，ループバックデバイスに圧縮機能を備えたイメージファイルに保存されている．このイメージファイルは仮想的なブロックデバイスとして機能する．[5]

cloopファイルの完全性が検証されることは，そのブロックデバイス上にあるファイルシステムの完全性を検証されることに他ならない．

Linuxに用いられるExt2ファイルシステムは，起動するたびにスーパブロックの値が変更される．また，ファイルを作成・削除・変更を行った場合は，グループディスクリプタの値が変更される．

cloop上のファイルシステムも変更・削除を行った場合必ずスーパブロック，グループディスクリプタの値が変更される．その値を正規ファイルシステムと変更・削除されたファイルシステムとの比較値に利用することで，ファイルシステムの完全性を検証できる．

KNOPPIXのファイルシステム完全性を検証する際，ブロックグループ0にあたるデータブロックを検出する．検出したデータブロックからスーパブロック，グループディスクリプタ，データをそれぞれ含むように50ブロック，データブロックをランダムに選択する．選択したデータブロック値をシリアル結合しハッシュ値を算出する．算出した値とキーシードを乱数作成関数に代入し，作成された乱数を認証鍵とする

3．3ファイルシステム完全性検証の動作フロー

ファイルシステム完全性検証のクライアント，サーバ間の動作を以下にまとめる．

† （株）アルファシステムズ，AlphaSystems Inc.

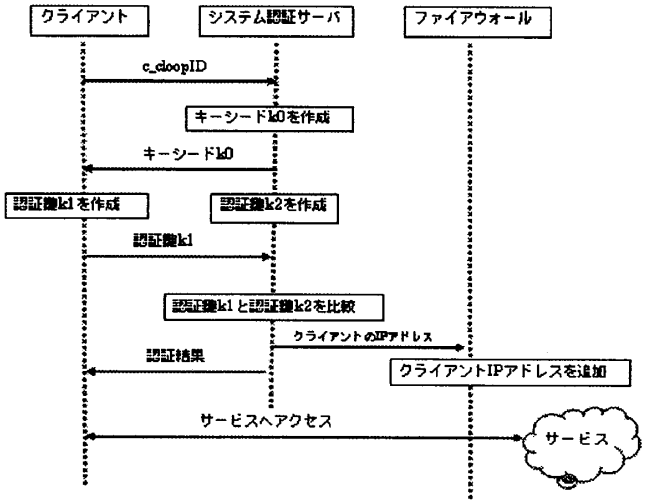

図１．ファイルシステム完全性検証のフロー

ファイルシステム完全性検証の動作フローを図１に示す．

1. クライアントは，システム認証サーバへサービスへのアクセス要求と cloopID（cloop ファイルを識別するための ID）を送信する．
2. システム認証サーバは，受信したシステムの cloopID と登録されたシステムの cloopID を比較する．一致したら，キーシード k0 を作成し，クライアントへキーシード k0 を送信する．次に一致したファイルシステムのデータブロックとキーシード k0 から認証鍵 k2 を作成する．
3. クライアントは受信したキーシード k0 とファイルシステムのデータブロックより認証鍵 k1 を作成し，システム認証サーバへ送信する．
4. システム認証サーバは認証鍵 k1 と認証鍵 k2 を比較し一致した場合，ファイアウォールにクライアントの IP アドレスを送信する．
5. ファイアウォールは受信した IP アドレスを登録し，クライアントからのアクセスを許可する．

3. 4 システムの構成

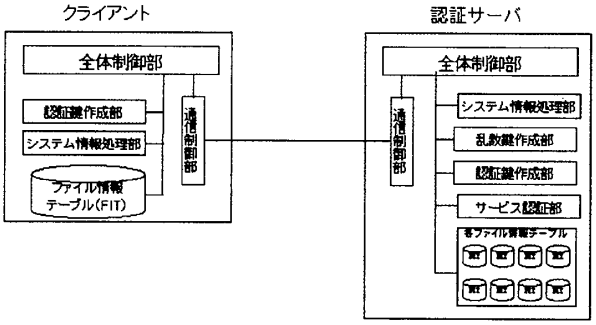

図２．システム構成図

ファイルシステム完全性検証の機能は以下のブロックに分かれる．システムの構成を図２に示す．

● クライアント

1. 全体制御部：各ブロックを管理し，各ブロックの起動，データの受け渡しを制御する．
2. 認証鍵作成部：ファイルシステムのデータブロック，キーシード **k0** と時刻を組合せて認証鍵を作成する．
3. システム情報処理部：ファイル情報テーブル(FIT)からファイル情報を取得し，cloopID を作成する．
4. 通信制御部：システム認証サーバへのデータ送受信を制御する．
5. ファイル情報テーブル(FIT：File Information Table) ファイルシステムの全情報を保存する．

● サーバ

1. 全体制御部：各ブロックを管理し，各ブロックの起動，データの受け渡しを制御する．
2. 認証鍵作成部：ファイルシステムのデータブロック，キーシード **k0** と時刻を組合せて認証鍵を作成する．
3. システム情報処理部：全体制御部から受信した cloopID を各ファイル情報テーブルに保存されている cloopID と一致するものを検索する．
4. 通信制御部：クライアントへのデータ送受信を制御する．
5. 乱数鍵作成部：クライアントへ送信するキーシード **k0** を作成する．
6. サービス認証部：クライアントが送信した認証鍵とシステム認証サーバが作成した認証鍵を比較する．一致した場合，クライアントのネットワーク識別子をゲートウェイに送信する．
7. 各ファイル情報テーブル(FIT：File Information Table)正規システムとして登録したファイルシステム，cloopID を保存する．

4. まとめ

CD-ROM から OS が起動する KNOPPIX を用いることで，一般的な端末をシンクライアントとして利用し，起動するシステムが正規なものであるかを判別する方法を示し実装した．ファイルシステムの特徴を利用することで信頼性の高いファイルシステムの完全性を検証することができた．

5. 今後の課題

miniroot とは linux カーネルが起動時に参照する暫定的なルートファイルシステムで本来のルートファイルシステムをマウントする．

ファイルシステムの検証を行うことはできたが，miniroot の検証ができていない．miniroot 内を変更しても，cloop ファイル外の内容なので変更を検出できないため miniroot 内でファイルシステムの完全性を偽るプログラムが実行された場合，対応できない．クライアントの完全性を高めるために，ミニルートに対しての検証も行えるよう開発を進めていきたい．

以上

参考文献

[1] KNOPPIX “http://www. knopper. net/knoppix/”
[2] 千葉 大作，大橋 拓朗，丹 英之，上原 光晶，松元 絹佳，須崎 有康，飯島 賢吾，八木 豊志樹，“KNOPPIX によるセキュアな Computer Based Testing の実践”，FIT2004 第３回情報科学技術フォーラム，Sep 2004
[3] 尾関隆章，蛭子隆彦”情報処理システムの潮流とシンクライアント”，No. 201 AP@PLAT(R)特集
[4] 中村めぐみ，宗藤誠治，吉濱佐知子，“シンクライアントにおける完全性検証とその効率化”，SCIS2006
[5] cloop “http://www. knoppix. net/wiki/Cloop”