ソフトウェア開発における作業履歴の非改ざん性保証と共有手法

池田祥平　上野秀剛
奈良工業高等専門学校情報工学科

1 背景と目的

ソフトウェア品質を確保するための取り組みの1つであるソフトウェアIV&V[1]では，開発組織から独立した第三者組織（以下，認証組織）が開発プロセスおよび開発製品の正当性を客観的に評価することで，ソフトウェアの信頼性を保証し，品質を確保する．しかし開発プロセスの品質評価は開発組織が組織内に独立した部門を設置することで行われており独立した第三者組織による客観的な評価が行えておらず，ソフトウェアの信頼性を保証するには弱い．本研究では開発組織が正しい開発プロセスで開発を行っていることを作業履歴の第三者評価から保証することを目的とし，独立した第三者組織が改ざんのない作業履歴を評価可能な手法を提案する．

2 提案手法

開発作業の計測記録である作業履歴は既存の作業計測システムにより記録可能であるが，作業計測システムには記録した作業履歴の変更を検出する機能がなく，開発組織が評価を高めるため作業履歴を改ざんし虚偽の作業履歴を報告しても，認証組織はそれを検出できず，誤った保証をしてしまう恐れがある．改ざんの対象としては作業履歴自体に加えて，作業計測システムが考えられる．システムを改ざんすることで誤った作業履歴を出力させることが可能になる．作業履歴と計測システムそれぞれに対する改ざんを検出するため，本研究ではハッシュ関数による検証を利用したサーバ・クライアントシステム（図1）を提案する．提案システムのクライアントは開発組織で利用され，開発者の作業履歴を計測する．サーバは認証組織で利用され，クライアントの認証と作業履歴が記録されるファイルの認証を行う．提案システムはハッシュ関数を用いてクライアントや履歴ファイルが変更されていないか検出する．

クライアント認証では認証組織は提供する前のクライアントの実行ファイルのハッシュ値H_{exe}を記録しておく．提供されたクライアントは作業計測を始める前にサーバと接続し，自身の実行ファイルのハッシュ値H'_{exe}を計算しサーバへ送信する．サーバはH_{exe}とH'_{exe}を比較して改ざんを検出する．改ざんが検出されれば接続を拒否して作業履歴を受け取らない．ログファイル認証ではクライアントは作業計測ごとに計測した作業履歴の作業履歴のハッシュ値Hlogを計算しサーバへ送信する．サーバはH_{log}を記録しておき，認証組織が評価時に作業履歴を開発組織から受け取ったときそのハッシュ値H'_{log}を計算し，記録しておいたH_{log}とH'_{log}を比較して改ざんを検出し，認証者に報告する．

3 実装と検証

クライアントを作業計測システム“TaskPit”を拡張して実装した．改ざん対象の作業計測システムと作業履歴ファイルの一部を改ざんして，サーバにより改ざん検出可能であることを確認した．検証ではあらゆる改ざんを検証したわけではないが，ハッシュ値は少しでも内容が異なれば値が変わるため，検証により改ざんした箇所以外を改ざんしても同様に検出可能であると考えられる．

4 今後の展望

本研究では認証組織が開発組織の改ざんされていない作業履歴を評価可能なシステムを提案した．今後の展望としては提案システムを実際の認証業務で運用し，問題がないかを検証する．

参考文献

[1] 宇宙航空研究開発機構：“IV&Vガイドブック”，(2013).

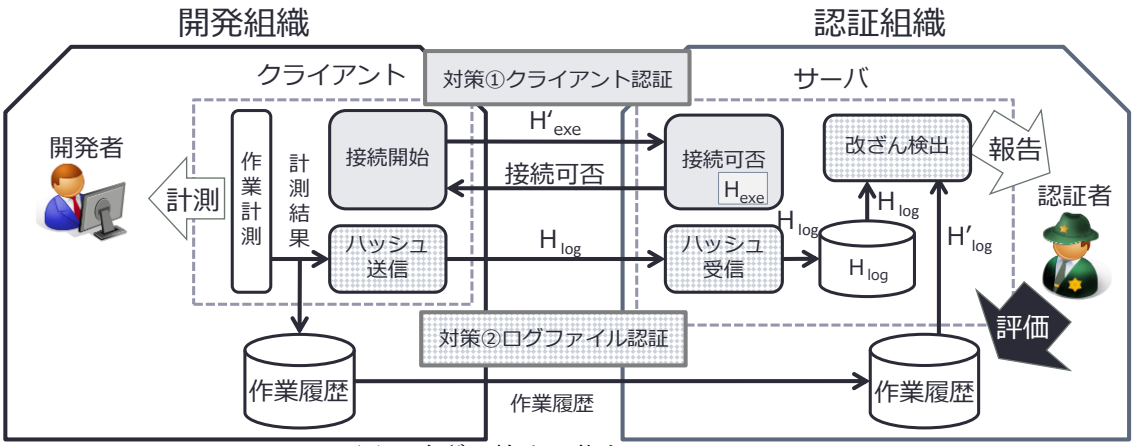

図1 改ざん検出可能なシステム