3Z-2

当事者のプライバシーを考慮したログの保管とその監査について

日比野　歩†　　福田　洋治†　　白石　善明‡　　毛利　公美††
愛知教育大学†　　神戸大学‡　　岐阜大学††

1　はじめに

PC や携帯端末の使用・操作や，ソフトウェア，ネットワークサービスの利用等で記録されるログは，利用者すなわち当事者のプライバシーを考慮する場合，当事者のみが閲覧可能なかたちで保管されることが望ましいと考えられる．この場合，当事者が制御できる PC や携帯端末でログを取得・保管する，あるいは PC や携帯端末でログを取得して当事者のみが知る鍵でログを暗号化してサーバに転送，保管する方法が挙げられる．

しかしながら，これらの方法では，ログの取得・保管が完全に当事者の制御下にあるので，デジタルフォレンジクスの観点でログの正確性や網羅性，継続性等[1]を客観的に示すには，ログの取得・保管についての監査が必要となる．このとき，監査人にログの一部を開示して，監査人が他の機器に保管されている当事者の行動やサービス利用のログと突き合わせを行うことになるので，当事者が望まない情報が監査人に閲覧されてしまうことが懸念される．

本研究では，当事者のみが閲覧可能なログの保管に関して，ログの内容を全て開示することなく，ログの存在，正確性，継続性等の確認が可能な監査を実現する，グラフ同型を証明するゼロ知識証明[2]を利用した手法を検討する．

2　当事者のプライバシーを考慮したログ保管とその監査の手法

PC や携帯端末で当事者が制御できるかたちでログを取得・保管する場合，当事者に都合のよいログの偽造，変更・削除を防ぎ，また継続して正確にログが取得・保管されていることを第三者が確認できることが重要である．

そこで，平時，当事者側で取得・保管されるログのダイジェストを定期的に監査者に提出させ，監査時，監査者がランダムに期間を指定して，当事者に該当する期間のログを提示させ，既に入手したログのダイジェストや他の手段で入手した関連ログとの突き合せを行う手法を提案する．

［平常時］

（a-1）当事者のデバイスで，対象の事象を観測して，ログレコードを作成，一定期間でまとめたもの L_l を用意する．

（a-2）ログレコードの集合 L_l からグラフ $G_{l,0}$ を作る（ログレコードの項目とノードの対応表 V_l とノードの接続関係の隣接行列 A_l を作る）．

（a-3）開示を望まないログレコードの項目について，対応表 V_l から該当する項目のノード番号を得て，未定義のノード番号と入れ替える置換 $S1_l$ から，グラフ $G_{l,1} = (V_l, S1_l(A_l))$ を作る．

（a-4）ランダムな置換 $S2_l$ を生成して，グラフ $G_{l,2} = (V_l, S2_l(S1_l(A_l)))$ を作り，グラフ $G_{l,2}$ を監査者に提出して，当事者のデバイスで L_l，$G_{l,1}$，$S2_l$ を保管する．

［監査時］

（b-1）監査者はランダムに期間 l を指定して，当事者に期間 l のログ $G_{l,1}$ を提出させる．

（b-2）監査者は $G_{l,1}$ と既に入手した $G_{l,2}$ が同型かどうかを，当事者とのゼロ知識対話証明により確認する．同型である場合，ログに偽造，変更・削除がないと判断する．

（b-3）監査者はV_lと$S1_l(A_l)$から得られるログレコードと，他の手段により入手した関連ログを突き合わせて，当事者側でのログ取得の継続性や正確性を確認する．関連ログとの整合がある場合，ログの継続性や正確性に問題がないと判断する．

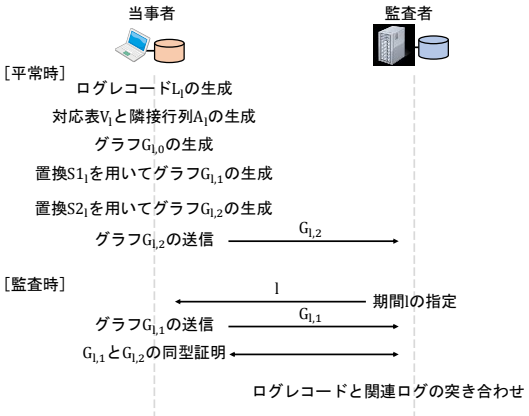

図 1　当事者のプライバシーを考慮したログの保管とその監査の手法

Fig.1　A method for log archiving and its auditing in considering privacy protection.

個人デバイスで取得されるログには，操作ログ，設定変更ログ，認証ログ，通話・通信ログ等の種類があり，これらには，種類により項目は異なるが，何時，何が，何を，何処で，どうやって，どうなった等の項目が含まれる．ログレコードに含まれるそれぞれの項目をノードと見なして，何時の項目のノードに対して，その他の項目のノードを無向エッジで繋ぐことにより 1 つのログレコードをグラフとして表現する．

Log Archiving and Its Auditing in Considering Privacy Protection
† Ayumi HIBINO and Youji FUKUTA・Aichi Univ. of Education
‡ Yoshiaki SHIRAISHI・Kobe University
†† Masami MOHRI・Gifu University

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

上の（a-2）では，ある期間に取得されたログレコード $R_i = \{I_{i,1}, I_{i,2}, \cdots, I_{i,m}\}$，$i = 1,2,\cdots,n$ （$I_{i,1}$ はログの取得日時の項目とする）がある場合，$i = 1,2,\cdots,n$ について，次の手続きを繰り返してグラフ化を行っている．

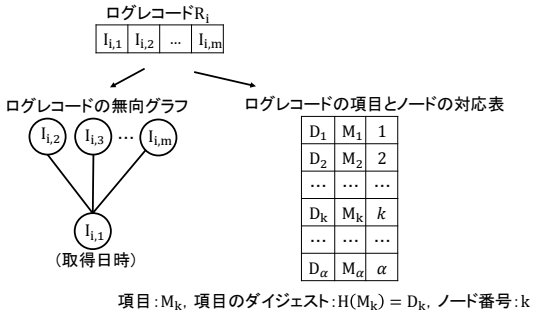

図 2 ログレコードを表現する無向グラフ
Fig.2 Non-directed graph expressing log records.

（a-2-1）$j = 1,2,\cdots,m$ について，ログレコード R_i の項目 $I_{i,j}$ がノードと項目の対応表 $V = \{(D_1, M_1, 1), (D_2, M_2, 2), \cdots, (D_k, M_k, k), \cdots (D_\alpha, M_\alpha, \alpha)\}$ に含まれるかどうか確認する．

（a-2-2）対応表Vに含まれている場合$H(I_{i,j}) = D_k$，$I_{i,j} = M_k$，該当のノード番号 $N_{i,j} = k$ を得る．$H(\,)$ はハッシュ関数である．Vに含まれていない場合またはダイジェストが衝突する場合 $H(I_{i,j}) = D_k$，$I_{i,j} \neq M_k$，対応表Vに項目（$H(I_{i,j})$，$I_{i,j}$，$\alpha + 1$）を追加して該当のノード番号 $N_{i,j} = \alpha + 1$ を得る．

（a-2-3）$j = 2,3,\cdots,m$ について，ノードの接続関係を表す隣行列Aに対して，$(N_{i,1}, N_{i,j})$ 成分，$(N_{i,j}, N_{i,1})$成分を 1 にする．さらに，ログレコードの取得日時の関係を表すために，隣接行列A に対して，$(N_{i-1,1}, N_{i,1})$成分，$(N_{i,1}, N_{i-1,1})$成分を 1 にする．

頂点数が同じである 2 つのグラフの間の同型判定は，n!通りの同型写像を調べる問題であるが，ノードの次数は変化しないので，2 つのグラフにおいて同じ次数のノードが対応することになり，実際にはノードの次数を降順に並べた次数列を調べることにより 2 つのグラフの各ノードの対応関係すなわち置換が簡単に分かってしまう可能性がある．

そこで，グラフ同型性判定を困難にするために，現在，効率的なアルゴリズムが見つかっていないとされている 2 部グラフ[3]を部分グラフとして含むかたちになるように，ログレコードの集合からグラフを作成するときに，上の（a-2-3）の後で，次のような変更を加えることにする．

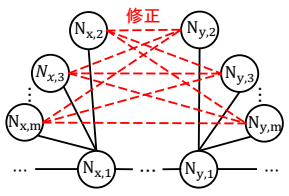

図 3 ログレコードの無向グラフの変更
Fig.3 Modif. of non-directed graph expressing log records.

（a-2-4）ログレコード R_x，R_y をランダムに選択して，$i = 2,3,\cdots,m$，$j = 2,3,\cdots,m$ について，ノードの接続関係を表す隣接行列A に対して，$(N_{x,i}, N_{y,j})$成分，$(N_{y,j}, N_{x,i})$成分を 1 にする．

3 考察

提案手法では，当事者側で取得・保管されたログのダイジェストとして，ログ（ログレコードの集合）から作成したグラフのノードをランダムに置換した，同型グラフを監査者に提出する．ここで，項目とノードの対応表を知っていても，ノードの接続関係が不明なので，個々のログレコードの内容を難読化したのと同様の効果が得られ，監査者がログレコードの内容を知ることは困難である．今回，ログから作成したグラフに 2 部グラフを含めることで，ノード数の等しい 2 つのグラフの同型判定を困難に（グラフの同型判定が，効率的なアルゴリズムが見つかっていないとされているグラフに対する難しさに近づくように）している．

提案手法では，監査時，監査者がランダムに期間を指定して，当事者に該当する期間のログ（ログレコードの集合）のグラフを提示させると，監査者は提示されたグラフから個々のログレコードの内容を確認する．当事者が開示を望まないログレコードの項目がある場合は，その項目に該当するノード番号を未定義のノード番号と入れ替えているので，監査者に対してログレコードの特定の項目を伏せたまま監査を受けることができる．ログレコードの項目の多くを監査者に伏せてしまうと，当事者のプライバシーは守られるが，監査において他の関連ログとの整合性チェックにおいて，ログの取得・保管の継続性や正確性の確認ができない可能性が高まると考えられるがこの対処の議論は今後の課題とする．

4 まとめ

当事者の制御下のデバイスで，事象を観測して，ログを取得・保管するような場面を想定して，当事者のプライバシーを考慮し，ログの内容を全て開示することなく，ログの存在，正確性，継続性等の確認が可能な監査を実現できる，グラフ同型を証明するゼロ知識証明を利用した手法を検討，提案した．

今後の課題として，当事者がログレコードの一部の項目を開示しないことで生じる監査時の問題への対処法や，提案手法と同等の問題を扱う他の手法と比較することで，提案手法の効果や利益が大きいこと等を定量的に示すことが挙げられる．

参考文献

[1] 間形文彦，高橋克巳，金井敦，”デジタル証拠の法的証明力を高めるための要件に関する一考察，” 信学会SCIS2008 予稿集，4E1-6，2008 年 1 月．
[2] 岡本龍明，太田和夫，暗号・ゼロ知識証明・数論，共立出版，1995 年．
[3] 戸田誠之助，”グラフ同型性判定問題の計算量,” 信学会論文誌 D-I, vol.J85-D-I，no.2，p.100-115，2002 年．

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.