訴訟対応のためのログの組合せと安定性対策の選定手法に関する検討

濱口 昌宏[†1]　加藤 弘一[†1]　間形 文彦[†2]　西垣 正勝[†3]　佐々木 良一[†4]　勅使河原 可海[†1]

[†1]創価大学大学院工学研究科　[†2]NTT 情報流通プラットフォーム研究所
[†3]静岡大学創造科学技術大学院　[†4]東京電機大学未来科学部

あらまし　情報システムに関する訴訟ではログが証拠となる場合があるため，事前にログを保管する必要がある．しかし，すべてのログの保管は運用負荷や費用を考えると現実的ではない．また，訴訟で問われるログの証明力について明確な規定はない．これに対し，先行研究によりデジタルデータの証明力を高めるための13要件が提示され，我々は13要件の根拠性と安定性を確保する方法をそれぞれ検討してきた．本稿では，これらを統合し，訴訟対応のための対策選定手法について述べる．まず，必要なログの組合せを決定して根拠性を確保する．そして，各ログの安定性に関する要件の達成度，敗訴確率や賠償額，対策費用等を考慮して，適切な対策を決定する．

A Study on a Selecting Method of Log Sets and their Stability Countermeasures to Deal with Lawsuits

Masahiro Hamaguchi [†1]　Koichi Kato [†1]　Fumihiko Magata [†2]
Masakatsu Nishigaki [†3]　Ryoichi Sasaki [†4]　Yoshimi Teshigawara [†1]

[†1]Graduate School of Engineering, Soka University
[†2]NTT Information Sharing Platform Laboratories
[†3]Graduate School of Science and Technology, Shizuoka University.
[†4]School of Science and Technology for Future Life, Tokyo Denki University.

Abstract To save logs is important for lawsuits relating to information systems because the logs can be used as evidence. However, storing all existing logs is not realistic due to operational loads and costs. In addition, there is no law and rule about probative value of logs. In contrast, 13 requirements to improve probative value of digital evidence were presented in a previous work, and then we have studied both methods to satisfy reasonability and stability of the 13 requirements. This paper shows a selecting method of log sets and stability countermeasures by integrating the above methods. First, our method fulfills reasonability by deciding necessary log sets. Next, the method selects appropriate countermeasures in consideration of degree of each log attainment of stability requirements, lost lawsuit probability, the amount of compensation and costs of countermeasures.

1. はじめに

近年，不正アクセス禁止法，個人情報保護法，金融商品取引法（通称，J-SOX 法）など，情報システムに関係する法整備が進んでいる．しかし，不正アクセス，不正会計などの違法行為は依然として絶えず，情報システムに関する刑事訴訟や民事訴訟が増加している．情報システムが関与する訴訟では，証拠として各機器やネットワークトラフィック等のログ

が利用されることがあり，証拠能力（刑事訴訟のみ）および証明力を具備するログを取得・保管することが重要である[1].

証拠能力とは，証拠として事実認定に利用できる適格をいい，刑事訴訟法で規定されている．一方，証明力とは，裁判官の心証を動かす力であり，証拠に信用性があり，その証拠が事実認定に役立つかどうかが焦点となる．しかし，証明力については，裁判官の自由な判断に委ねられており，法律等による明確な規定がない．

このような中で，ログの証明力について，先行研究によりデジタル証拠の法的証明力を高めるための 13 要件が提示された[2]．この 13 要件は根拠性と安定性の 2 つの観点で分類される．さらに我々は，根拠性，安定性のそれぞれについて，詳細な分析を行い，要件達成のための手法について検討してきた[3][4][5]．これらの検討を通して，訴訟対応のためのログを保管するためには，根拠性の要件を満たすような取得ログの組合せ，およびログの取得・保管に関して安定性の要件を満たすための対策（以下，安定性対策）を決定する必要があることが分かっている．

ところが，取得ログによって講じるべき対策が異なる可能性があり，適切な対策を決定するためには，根拠性と安定性を独立に扱わず，同時に考慮する必要がある．そこで本稿では，根拠性と安定性について独立に検討してきた手法を統合し，訴訟対応のためのログの組合せと安定性対策を選定する手法について述べる．

2. デジタル証拠の法的証明力を高めるための要件

間形らにより，デジタル証拠の法的証明力を高めるための要件が提示されている[2]．この文献では，証拠に関する規定の総称である証拠法の基礎概念と訴訟手続きから，「証拠能力」と「証明力」に分けて，訴訟においてデジタル証拠が追及される論点を明確にしている．そして，証明力について，「根拠性」と「安定性」の概念を導入している．根拠性とは，証拠により要証事実を導き出せることをいう．要証事実とは事案の判断に必要な事実のうち証明を必要とするものを指す．安定性とは，訴訟において反論を受けても再反論可能であり，裁判官の心証形成に動揺がないことをいう．

表 1 デジタル証拠の法的証明力を高めるための要件

根拠性	要件1	記録により必要な注意義務に従った運用実績を示すこと
	要件2	故意過失の記録が含まれていないこと
安定性	要件3	記録の実在を証明できること
	要件4	記録した主体が何かを証明できること
	要件5	記録した日時を証明できること
	要件6	記録の完全性を証明できること
	要件7	記録の発生契機を証明できること
	要件8	記録解釈の妥当性を証明できること
	要件9	記録の正確性を証明できること
	要件10	記録の網羅性を証明できること
	要件11	記録保管の継続性を証明できること
	要件12	記録の整合性があること
	要件13	異常時の検出と対処が記録されていること

さらに，実際の訴訟を想定した詳細な分析から表 1 のような 13 要件を導出している．これらの要件は，証拠法と訴訟手続き，仮想事例を基に検討されており，実際の訴訟に沿ったものである．したがって，13 要件を満たすことが，証拠としての有効性を評価する 1 つの基準となる．

3. 対策選定時に考慮すべき事項

3.1 事実の証明に必要な情報

訴訟において，起きた事実を証明するためには，いつ，何に対して，どのようなことが起きたのかを特定する必要がある．さらに，原因を追及するためには，誰が，どのような手順で行ったのか，なぜ起きてしまったかなども明らかにする必要がある．これは，根拠性の要件に相当する．

リスクは，複数の事象の発生を経て顕在化する．そのため，関連する事象の流れを考慮して，インシデントの有無とその原因を証明する必要がある．そして，事象を考慮したインシデントの証明のおいては，各事象に関連するログを用いることができる．つまり，5W1H 情報を満たすための単一または複数のログが必要となる．

3.2 ログの証明力の確保

ログの取得・保存の箇所や方法によっては，そのままでは信頼性の低いログもある．そのため，ログを証拠として利用するためには，ログの

改ざん防止対策などの安定性対策を実施し，安定性の要件を満たすことが重要である．

安定性の要件を満たすためには，証拠の収集・保全・提出の各フェーズにおいて，それぞれ演算処理を行う主体（以下，フェーズ主体）が満たすべき事項（機能要件）を達成する必要がある[3]．つまり，安定性対策は，各フェーズや演算機器に対して実施される．

3.3　訴訟に係わる費用

情報漏洩や不正会計など，組織に大きな損害をもたらすリスクに関する訴訟で敗訴してしまった場合，組織は賠償金の支払いを命じられる．また，社会的信頼を失墜させる場合もある．

一方で，ログの取得・保管，および安定性対策の導入・運用には，費用がかかる．例えば，ログの保管には膨大なストレージが必要であり，改ざん防止のための暗号化を行うためには機器やモジュールの導入が必要である．

そのため，訴訟により生じうる賠償額や対策費用を考慮して，組織にとって損失額が小さくなるような，適切な取得ログの組合せと安定性対策を決定する必要がある．

4. 提案手法

4.1　リスク，事象，ログの関係性分析

インシデントの有無を証明するために，関連事象において必要とする 5W1H 情報を記録するログを取得できなければならない．このとき，1 つのログで 5W1H 情報の特定が困難な場合には，複数のログを利用して情報を補完する．また，同様の情報を取得可能なログが複数ある場合には，代替も可能である．そこで，ログの補完関係を利用して事象の 5W1H 情報を得る[5]．

4.2　安定性の要件と対策の関係性分析

インシデントを抑制するためのセキュリティ対策と同様に，安定性対策は機器に実装する機能，運用手順など様々な手段が考えられる．そのため，対策が効果を発揮する対象も，特定のフェーズ全体や，特定のフェーズ主体，またはその主体における特定の処理などが考えられる．そこで，各対策について，対応する主体や，満たすことのできる要件を整理する．

4.3　対策効果・費用の定量化

それぞれの安定性対策は，4.2 節で分析された関係する要件に対して効果の程度が異なる．そこで，対策効果を対策選定時に考慮するために，各対策の効果の程度を割り当てる．

また，組織にとって，後述する賠償額を上回る費用を要する対策が必要かどうかを判断しなければならない．そこで，安定性対策の導入時にかかる初期費用や，運用費を割り当てる．

4.4　賠償額の期待値

本稿では，文献[6]に習い，訴訟による賠償額の期待値を次式で定義する．

$$\text{賠償期待値} = \text{敗訴 1 回あたりの賠償額} \times \text{敗訴確率}$$

敗訴確率とは，ログ以外に決め手となり得る証拠がないとき，ログを提出しても証明したい事実が認定されない確率と定義する．このとき，ログの組合せにより証明したい事実が認定されるために必要な条件は，5W1H 情報を網羅するログの組合せであること，および各ログについて安定性の要件を満たしていることである．

つまり，敗訴確率とは，証拠として提出するログの組合せが根拠性と安定性を満たせていない程度として表すことができる．具体的な算出方法については 4.5 節で述べる．

4.5　対策の決定手法

ログの組合せと安定性対策を決定する流れは，下記のようになる．

(1) 対象リスクを決定する．また，そのリスクに関する訴訟での敗訴時の賠償額を決定する．
(2) インシデントに至るまでの事象を分析する．
(3) 事象に関連するログを洗い出す．
(4) 各ログについて，保存に必要なストレージ量を割り当てる．
(5) 各ログについて，安定性対策をまったく実施していない状態における，安定性の要件の達成度と証拠率を評価する[4]．証拠率は，必要な物証・人証を残している程度を表す．
(6) (5) の結果から，ログの信頼度を算出する．ログ n の信頼度 R_n は，安定性に関する要件 i の達成度 L_i とその証拠率 E_i から，次式で求

める.

$$R_n = \min L_i \times \min E_i$$

(7) 安定性対策について，対策の対象となるフェーズ主体と機能要件，対策効果を明確にする．また，対策の導入・運用費を割り当てる．

(8) インシデントの有無の証明のために示すべき事項を，5W1H の観点で分析する．

(9) (8) で決定した5W1H情報に対し，各事象で示すべき 5W1H 情報を分析する．ただし，各事象で 5W1H の全要素をすべて示す必要があるとは限らない．

(10) 事象ごとに，(9) で決定した各要素に対し，(3) で洗い出したログのいずれで証明できるかを割り当てる．

(11) 事象ごとに，(9) で決定した要素すべてを示すことのできるログの組合せを列挙する．

(12) 事象ごとに，(11) で列挙した各組合せにおいて，“事象の証明度”を算出する．事象の証明度は，5W1H の要素ごとに，対応するログの信頼度の最大値（要素の証明度）を取り，(9) で決定した示すべき全要素の証明度の最小値を取ったものとして定義する．証明度とは，要証事実を証明できる確率である．

(13) (12) の結果をもとに，インシデントの証明度を算出する．インシデントの証明度は，インシデントを引き起こす一連の事象のうち，最小の証明度と定義する．

(14) 敗訴確率を，次式で算出する．

敗訴確率 ＝1－ インシデントの証明度

(15) 賠償額の期待値，ストレージや対策にかかる費用，要件の達成度を用いて目的関数や制約条件を設定する．そして，各ログの取得の有無および安定性対策の実施の有無を変数とする離散最適化問題を解くことにより，ログの組合せと安定性対策を決定する．

5. 本手法の利用例

5.1 想定環境

図 1 のような社内 LAN を想定する．データサーバには，財務諸表が格納されており，ファイルごとのアクセスコントロールが実施され，財務諸表に対しては経営者のみがアクセス可能とする．クライアント PC を管理する Active Directory（AD）サーバ，トラフィックを管理する IDS が設置されている．取得されたログはログ保管用のストレージで一括管理される．

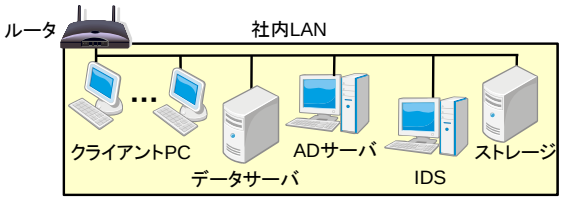

図 1 想定環境

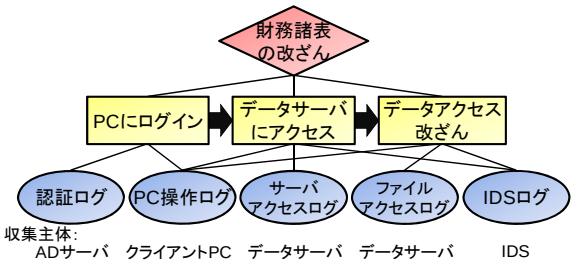

図 2 リスク・事象・ログの関係

5.2 想定事例

実際には不正をしていないにもかかわらず，内部統制の監査において，組織ぐるみの不正会計（財務諸表の改ざん）の疑いから訴訟を起こされる場合を想定する．この訴訟では，事実がなかったこと（誰も不正をしていないこと）を証明する必要がある（不存在の証明）．

5.3 ログの組合せと安定性対策の決定

4.5 節の手順に基づき，ログの組合せと安定性対策を決定する．

(1) 対象リスクは，財務諸表の改ざんである．敗訴した場合，社会的信頼の失墜がもたらす損失を考慮して，賠償額を 1 億円とする．

(2) リスク顕在化に至るまでの事象として，経営者によるデータ改ざんを想定し，PC にログイン，データサーバにアクセス，データサーバ内のデータ改ざんとする．なお，事象には流れが存在し，上記の順で事象が発生する．

(3) (2) の事象に関連するログを挙げた．リスク・事象・ログの関係と，各ログの収集主体を図 2 に示す．

(4) (3) の各ログについて，保存に必要なストレージ量を割り当てた．

表 2 ログのストレージ量と安定性の要件の評価

		認証ログ				PC操作ログ				・・・
ストレージ量		500Gバイト				2000Gバイト				・・・
		収集	保全	提出	合計	収集	保全	提出	合計	
達成度	要件3	0.5	0.5	1.0	0.25	0.1	0.5	1.0	0.05	
	要件4	0.5	0.5	1.0	0.25	0.2	0.5	1.0	0.10	
	要件5	0.5	0.5	1.0	0.25	0.4	0.5	1.0	0.20	
	要件6	1.0	0.5	1.0	0.50	1.0	0.5	1.0	0.50	
	要件7	1.0			1.00	1.0			1.00	・・・
	要件8	1.0	1.0	1.0	1.00	1.0	1.0	1.0	1.00	
	要件9	0.5	0.5	1.0	0.25	0.3	0.5	1.0	0.15	
	要件10	0.5	0.5	1.0	0.25	0.3	0.5	1.0	0.15	
	要件11		0.5		0.50		0.5		0.50	
	要件12	1.0	1.0	1.0	1.00	1.0	1.0	1.0	1.00	
	要件13	0.5	1.0	1.0	0.50	0.5	1.0	1.0	0.50	
証拠率	要件3	1.0	1.0	1.0	1.00	1.0	1.0	1.0	1.00	
	要件4	1.0	1.0	1.0	1.00	1.0	1.0	1.0	1.00	
	・	・	・	・	・	・	・	・	・	・・・
	・	・	・	・	・	・	・	・	・	
	・	・	・	・	・	・	・	・	・	
信頼度		0.25				0.05				・・・

表 3 各対策とその対策効果

	対策1			対策2			対策3			対策4		
フェーズ	収集	保全	提出	収集	保全	提出	収集	保全	提出	収集	保全	提出
要件3	×	×	×	◎	◎	×	×	×	×	×	×	×
要件4	○	○	×	×	×	×	×	×	×	○	○	×
要件5	×	×	×	△	○	×	×	×	×	△	○	×
要件6	×	○	×	×	○	×	○	○	×	×	○	×
要件7	×			×			×			×		
要件8	×	×	×	×	×	×	×	×	×	×	×	×
要件9	×	×	×	△	○	×	△	○	×	○	○	×
要件10	△	○	×	○	○	×	△	○	×	○	○	×
要件11		×			◎			×			×	
要件12	×	×	×	×	×	×	×	×	×	×	×	×
要件13	○	×	×	○	×	×	×	○	×	×	×	×
価格(万円)	150			120			160			100		

◎=1.0, ○=0.8, △=0.6, ×=0

(5) (3) の各ログについて, 安定性の要件の達成度と証拠率を評価する. ここでは, 達成度は仮の値を割り当てた. 証拠率は, 運用手順に則って操作記録等をすべて残しているものとして, すべて 1.0 とする.

(6) (5) の結果から, ログの信頼度を算出する. (4), (5), (6) の結果を表 2 に示す.

(7) 実在する製品等を参考に, 4 種類の安定性対策を挙げた. 対策 1～3 は, すべての収集主体に対して同時に対策効果を発揮する. 対策 4 は, 収集主体ごとに対策を実施する必要がある. 各対策とその対策効果を表 3 に示す.

(8) 財務諸表の不正操作がなかったことを証明するために, 表 4 の事項を示す必要がある.

(9) (8) で決定した 5W1H 情報に対し, 各事象で示すべき 5W1H 情報を分析した.

(10) (9) の結果に対し, 各要素を証明できるログを割り当てる. (9), (10) の結果を表 5 に示す. 運用記録はログとは異なるが, 業務の一環で作成されるため信頼度が高いものとする.

表 4 示すべき 5W1H 情報

When	データがアクセスされた時刻 (に不正がないという事実)
Where	データサーバ
What	財務諸表の不正な操作が 行われていないという事実
Who	経営者 (による操作がなかったという事実)
Why	アクセスコントロールなどが 適切に実施されていたという事実
How	運用規定に基づいた操作が されていたという事実

表 5 事象ごとに示すべき要素と対応するログ

	必要な要素	関連するログ
経営者権限でログイン	When	認証, PC
	How	認証, PC
	Who	認証, PC
データサーバにアクセス	When	PC, サーバ, IDS
	How	PC, サーバ, IDS
データにアクセス・改ざん	When	PC, サーバ, IDS
	How	PC, サーバ, IDS
	Why	運用記録など
	Where	PC, IDS, ファイル
	What	PC, IDS, ファイル

表 6 示すべき要素を見たすログの組合せ

	5W1Hを満たすログの組合せ
経営者権限でログイン	{認証}, {PC}, {認証, PC}
データサーバにアクセス	{PC}, {サーバ}, {IDS}, {PC, サーバ}, {PC, IDS}, {サーバ, IDS}, {PC, サーバ, IDS}
データにアクセス・改ざん	{PC}, {IDS}, {ファイル}, {PC, IDS}, {PC, ファイル}, {IDS, ファイル}, {PC, IDS, ファイル}

(11) 表 5 をもとに, 事象ごとのログの組合せを列挙する. この結果を表 6 に示す.

(12) (11) の組合せにおいて, 現状のログの信頼度における事象の証明度を算出する.

(13) (8) の結果をもとに, インシデントの証明度を算出する.

(14) (13) の結果から, 敗訴確率を算出する.

(15) 賠償額の期待値, ストレージや安定性対策にかかる費用から, 訴訟に関わる費用の期待値を算出する. ストレージにかかる費用は, 1000G バイトあたり 30 万円とした.

要件ごとの各フェーズの達成度は, 対策未実施の場合(表 2)と, 選択される対策の効果(表 3)の中で, 最大値を選択した.

そして, 目的関数を, 賠償期待値とストレージ・安定性対策にかかる費用の総和の最小化とし, ログの組合せと安定性対策を決定した.

表 7 ログの組合せと安定性対策による訴訟に関わる費用の期待値

ログの組合せ	実施する安定性対策	敗訴確率	賠償額の期待値（万円）	対策費用（万円）	訴訟の期待値（万円）
PC	対策2，対策4(PC)	0.52	5,200	280	5,480
認証，PC	対策2，対策4(PC)	0.52	5,200	290	5,495
PC，ファイル	対策2，対策4(PC)	0.52	5,200	310	5,510
認証，サーバ	対策2，対策4(PC)	0.52	5,200	310	5,510
認証，PC，ファイル	対策2，対策4(PC)	0.52	5,200	325	5,525
⋮	⋮	⋮	⋮	⋮	⋮

取得ログは PC 操作ログ，安定性対策は対策 2 と対策 4(クライアント PC)，訴訟に関わる費用の期待値は 5,480 万円となった．表 7 に，導出結果の一部を示す．

5.4 考察

ひとつのログについて，安定性の要件の達成度が 1 つでも極端に低いと，他の要件において安定性対策を実施したとしても，ログの信頼度が向上せず，敗訴確率も低くならないことがわかった．このことから，敗訴確率を低くするためには，達成度の低い要件に対して優先的に対策が必要である．

また，表 7 では PC 操作ログのみの場合と，他のログを併せた場合で，敗訴確率が同じである．これは，PC 操作ログが対策により信頼度が高くなり，信頼度の低い状態にある他のログを重ねても効果がなかったためである．

今回，不存在の証明に関する 1 つのリスクを対象として，賠償額の期待値とストレージや安定性対策にかかる費用を考慮して，ログの組合せと安定性対策が決定できた．このとき，安定性対策の効果を敗訴確率へ反映させることで，対策効果の違いが考慮されている．以上から，訴訟対応のために必要なログの組合せと安定性対策を決定できる見通しを得た．

6. まとめと今後の課題

本稿では，訴訟に対応可能なデジタル証拠を確保するために，根拠性と安定性の要件を満たすログの組合せと安定性対策を決定する手法を述べた．また，想定事例を通して，本手法が敗訴確率や賠償額，対策コストを考慮して取得ログと安定性対策を決定できることを示した．

今後の課題は以下の通りである．

(1) 敗訴確率などの数値の妥当性

ログが実際に訴訟に耐えうる証拠として利用できるのかなど，実際の訴訟での敗訴確率の数値の妥当性が不明確である．そのため，ログの信頼度や対策効果の数値の妥当性を評価する必要がある．

(2) 複数のリスクの考慮

組織が訴訟に備えるべきリスクは多く存在するため，複数のリスクに対応した場合，ログや安定性対策の組合せ数が膨大になる可能性がある．そのため，賠償額を考慮し，優先的に扱うリスクを決めるなどの対応を検討する必要がある．

(3) 相殺過失の定量化

訴訟時には，過失の大きさなどに対して善管注意義務に従った運用がなされていたかどうかも争点になりうる．そのため，ログ取得動作や各種対策が適切に管理されていたかどうかから判断される過失相殺を考慮する必要がある．

謝辞

本研究は，財団法人セコム科学技術振興財団研究助成金の一部を利用している．

参考文献

[1] 辻井重男監修:デジタル・フォレンジック事典，デジタル・フォレンジック研究会，2006.12

[2] 間形文彦 他: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，IEICE SCIS2008，2008.1

[3] 川西英明 他:デジタル・フォレンジック対策選定のための法的証明力を高める要件の関係性に関する検討，IPSJ DICOMO2008 シンポジウム，pp.580-586，2008.7

[4] 川西英明 他:デジタル証拠の法的証明力を高める要件の評価手法に関する検討，IEICE 2009 年総合大会，pp.S-23-24，2009.3

[5] 濱口昌宏 他:訴訟対応のためのログの組合せに関する検討，IPSJ DICOMO2009 シンポジウム，pp.991-999，2009.7

[6] 間形文彦，高橋克己:ログを証拠に事実を証明する機能に基づく敗訴リスクの定式化，IEICE 2009 年総合大会，pp.S-21-22，2009.3