情報セキュリティ事件の証拠となるログを収集する情報システムの要件に関する一考察

間形 文彦　　高橋 克巳

日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11

あらまし　ログ収集の目的が曖昧なままでは，不要なログが収集される一方で，逆に，必要なログが全く記録されないことがあり得る．本稿は，ログの目的を情報セキュリティ事件の証拠としたとき，情報システムにおける現象の何を観測し，ログに何を記録すべきかを考察した．事件の類型と当事者の立場により要証事実が異なり，ログの記述要素も異なることを示し，情報セキュリティの特性と情報処理プロセス，イベントログ，ステータスログの対応関係を明らかにして，証拠となるログを収集する情報システムの要件を定義した．

A study of requirements for the information system that collect logs as evidences of the information security incident

Fumihiko Magata　　Katsumi Takahashi

NTT Information Sharing Platform Laboratories, NTT Corporation
3-9-11 Midori-Cho Musashino-Shi Tokyo 180-8585 Japan

Abstract　Necessary logs cannot be collected when a purpose of the log collection is vague. If a purpose of the log is a evidence concerning the information security incident, the following matters are shown; the phenomenons and logs that should be observed and recorded; the proof necessary facts and the description elements of the log must be different according to the kind of incident and the standpoint of relevant party; relation between the characteristics of information security, information processing process, event logs, and status logs. And the requirements for the information system that collected logs are defined.

1　はじめに

情報システムにより生成される電磁的記録の一種であるログが訴訟における証拠となり得るか，そのための要件は何かについて，これまでに法学をはじめ，理工学の分野においても論じられてきた．

証拠とは，要証事実の存在または不存在について判断を下す根拠となる資料であり，命題「証拠があるならば事実がある（ない）」が成り立つ因果関係があるものをいう．訴訟においてこの因果関係は経験則に照らして判定され，「その判定は，通常人が疑を差し挟まない程度に真実性の確信を持ちうるものであることを必要とし，かつ，それで足りる」[1] とされている．

筆者らは，裁判官の心証は経験則に基づく因果関係の判断と当事者の攻撃防御の結果に基づいて形成されることに着目し，法的証明力について根拠性と安定性の 2 つの概念を提示した [2]．根拠性とは，証拠から経験則に従って当然に要証事実を導出できることであり，安定性とは，相手から証拠に対する反論を受けても再反論が可能で，裁判官の心証に動揺がないことであるとした．

観測された現象を，ある規則に従って，文字，記号，画像等により記述したものをログとするとき，ログが証拠となり得るためには，現象とログとの間の因果関係が説明でき，命題「ログがあるならば事実がある（ない）」が成り立たなければならない．しかし，情報システムにおいては，この因果関係の存在を通常人が確信できるための直接的な経験則は，存在しない．したがって，ログと要証事実の間にある因果関係は，そのログ自体とは別の証拠と経験則をもって証明されなければならない．筆者らは，この証明の働きを実現する機能として，証拠ログ機能を提案した [3]．

しかし，ログと事実との因果関係が問題となる以前に，そもそも証拠から導かれる事柄が要証事実を満たしているかが問題となることがある．例えば，次のような要証事実の主張とそれに対するログが提出される

とする．
要証事実：「x 月 x 日，使用禁止の USB メモリに，社員 M が，機密情報 S を，コピーした.」
ログ：「x 月 x 日，ユーザ M が，ファイル S に，アクセスした.」

このログでは，アクセスが，ディスプレイ表示か媒体への書込みか分からず，仮に書込みであるとしても書込み先が USB メモリかどうか不明である．したがって，このログは，要証事実を充足しない．

証拠から導かれる事柄が要証事実を示すことは，根拠性の要件の一つである．証拠となるログは，先ず要証事実として主張される事柄とログに記された事柄が比較され，次いでログと要証事実の因果関係が経験則によって判断されて，ログの根拠性が認められた後，安定性が問われる．

本稿では，証拠ログ機能が実装されることで法的証明力の根拠性と安定性が満足されることを前提に，情報セキュリティ事件への対応に目的を絞って，要証事実を特定するための構成要素とそれに対応する情報処理プロセスを明らかにし，記述されるべきログを過不足なく収集する情報システムの要件を示す．

2　情報セキュリティ事件の類型

情報システムの生成するログが，法的係争の争点となる要証事実に係る現象の何を観測し，何をログとして記録すれば証拠になるかについて検討するために，対象とする要証事実を定めなくてはならない．争われる事件によって要証事実は異なることから，本稿では，情報セキュリティ事件を扱うこととし，情報セキュリティ事件の判断に必要な事実のうち証明を必要とするものを検討対象の要証事実とする．次に，情報セキュリティ事件とは，情報資産の機密性，完全性または可用性が損なわれることにより，権利や利益が侵害され，損害が生じて問題となる出来事とする．本稿で扱う情報セキュリティ事件の類型は次のとおりである．

機密性に係る事件：情報の漏えい
完全性に係る事件：情報作成の否認／なりすまし，情報の改竄，情報処理の誤り，情報の偽造
可用性に係る事件：情報の消失，情報利用の停止

3　損害賠償請求とログ

情報セキュリティ事件のうち，生じた損害をめぐる当事者間の争いを裁判によって解決する手続を，本稿では，情報セキュリティ訴訟というものとする．情報セキュリティ訴訟は，情報セキュリティ事件によって生じた損害の賠償を請求するものが多い．このとき情報セキュリティ訴訟における要証事実は，損害賠償請求が認められるために証明を必要とする事実である．損害賠償請求には，(1) 違法行為，(2) 損害額，(3) 違法行為と損害との相当因果関係，(4) 行為者の故意・過失，が明らかでなければならない．これらの要件とログとの関係を以下に述べる．

(1) **違法行為**とは，権利または法律上保護される利益を侵害する行為のことであり，債務不履行（民法 415 条）と不法行為（民法 709 条）からなる．違法行為が情報システムと関連する場合，情報システムによって違法行為に係る現象を記述することができる．

(2) **損害額**とは，違法行為によって生じた損害の額であり，財産的な損害の他，精神的な損害も含まれる．一般に，情報システムの範囲外で生じた損害を検知して，情報システムのログに記述することは困難である．例外的に，勘定系システムの場合には，ログが現実の損害額を直接記録することがある．

(3) 違法行為と損害との**相当因果関係**とは，違法行為がなければ，損害も生じなかったであろうと考えられる関係のことである．一般に，情報システムの範囲外に及ぶ損害の因果関係をログに記述することは困難である．例外的に，勘定系システムの場合には，ログが情報システムの動作と損害額の因果関係を直接記録（送金，振込みなど）することがある．

(4) **故意**とは，罪を犯す意思（刑法 38 条）をいい，**過失**とは，自分の行為の結果が予見でき，結果を回避すべきなのにそれをしなかったことをいう．情報システムに保管されるコンテンツ（情報資産）を除けば，一般に，情報システムが生成するログに行為者の内心が直接記述されることは少ない．

以上より，損害賠償請求のために明らかにしなければならない事実のうち，ログによる証明が最も期待できるのは，(1) **違法行為**である．行為を表現するためにログに記述されるべき要素は，いつ，どこで，だれが，なにを，どうした，である．

4　情報セキュリティ訴訟の要証事実とログの記述要素

4.1　訴訟当事者と情報システム及びログ

情報セキュリティ訴訟の類型ごとに要証事実とログに記載されるべき要素を考察するにあたり，訴訟の当事者と情報システムとの関係を次のようにモデル化する．

情報セキュリティ訴訟の当事者には，責任を追求する側の原告（被害者）と責任を追及される側の被告（加害者）がある．原告は，被告の違法行為によって，情報資産の機密性，完全性または可用性が損なわれた結果生じた損害の賠償を被告に請求するものとする．このとき立証責任は原告にあるため，原告は証拠を提出し，被告の違法行為の存在の証明を試みるものとする．他方，被告には原則として立証責任はないが，被告は最大限の防御をするために，自らに有利な証拠を積極的に提出することによって，被告の違法行為がないことの証明を試みるものとする．

原告と被告は，それぞれが管理する情報システムのログを証拠として用いて，攻撃と防御を行う．

- 原告は原告が管理する情報システムのログを証拠として攻撃（図 1 参照）

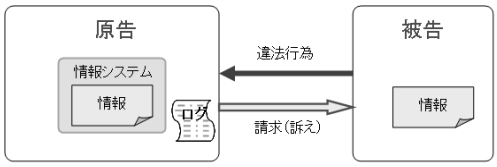

図 1: 原告の攻撃手段としてのログ

- 被告は被告が管理する情報システムのログを証拠として防御（図 2 参照）

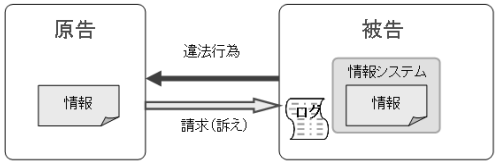

図 2: 被告の防御手段としてのログ

4.2 情報漏洩

情報漏洩に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，あってはならないところに，被告が，その情報を，漏洩した.」

被告側：「その時，あるべきところから，被告は，その情報を，漏洩しなかった.」

出来事がなかったことはイベントログには記述できないため，上記のログが存在しないことをもって，出来事がないことを証明しなければならない．不存在を証明するためには，出来事は漏れなく記録している，そこに出来事の記録がない，よって，出来事はない，という三段論法によるしかない．原告は事実の存在を示す 1 つのログを提出すれば十分であるのに対して，被告は全てのログを提出して，該当するログがないことを示さなくてはならない．したがって，不存在の証明には網羅性が要求されるため，被告は，原告の示すログをはるかに上回る膨大な量のログが必要になることがあり，被告の負担は大きい．

ログに記述されるべき要素は，いつ，どこで，だれが，なにを，どうした，であり，原告側と被告側の記述すべき要素量に違いはない．

4.3 情報作成の否認／なりすまし

情報作成の否認の例は，契約書に署名した者が契約書の作成を否認して契約を履行しない場合，なりすましの例は，他人の名において契約書に署名し，その他人に契約の履行を要求する場合などがある．一方の当事者にとって情報作成の否認事件は，身に覚えのない他方の当事者からみて，なりすまし事件と映ることがある．つまり，情報作成の否認となりすましは，加害者と被害者の立場を入替えたとき表裏の関係にあるので，以下，なりすましの説明は省き，情報作成の否認についてのみ述べる．

情報作成の否認に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，被告が，この情報を，作成した.」

被告側：(1)「その時，被告は，この情報を，作成しなかった.」(1) を証明することは，不存在の証明である．この証明の負担が大きいことは前述した．

しかし，情報にデジタル署名が付与されている場合には，被告は出来事の不存在の証明に依らず，デジタル署名の状態の証明で，原告の主張を退けることができる．

被告側：(2)「その時，被告以外の誰でも，デジタル署名を，作成できた.」なぜならば，(2) ’「その時，誰でも，知り得る，秘密鍵」だからである．

したがって，(2) ’は原告の主張のうちの「被告が」に対する反論となる．(2) ’を表すログはイベントログではなく，署名に関する状態を記述したステータスログである（例えば，単純すぎて誰でも分かる文字列の秘密鍵など）．

被告側：(3)「その時，被告は，デジタル署名を，作成できなかった.」なぜならば，(3) ’「その時，被告が，知り得ない，秘密鍵」だからである．

したがって，(3) ’は原告の主張のうちの「作成した」に対する反論となる．作成不可能な状態であったことを示すステータスログ（例えば，偽の電子証明書など）により原告の主張を否定できる．

不存在の証明をしようとすれば，網羅性を満たすために膨大なログの提出が必要になることがあるが，以上のように存在の証明に転換できれば被告の負担は大幅に低減する．(2) ’, (3) ’を表すログに記述されるべき要素は，いつの，どこの，どのような，なに，であり，原告側の記述要素よりも少ない．

4.4 情報の改竄

情報の改竄に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，その情報システムで，被告が，その情報を，改竄した.」

被告側：(1)「その時，その情報システムで，被告が，その情報を，改竄しなかった.」

(1) の証明は，不存在の証明である．この証明の負担が大きいことは前述した．しかし，出来事ではなく，情報の状態に着目するならば，被告は不存在の証明に依らずに，存在の証明によって原告の主張を退けることができる．

被告側：(2)「その時，その情報システムに，これと同じ情報があった.」換言すれば,「その時，その情報システムの中の，これと同じ，情報」を示せばよい．この要素は，いつの，どこの，どのような，なに，であり，原告側の記述要素よりも少なくなる．

過去と現在の情報の同一性を証明することで，原告の「改竄」の主張を否定できる．(2) を表すログはイベントログではなく，この情報と同じ情報が，争点となっている過去のある時点にも存在した状態を示すステータスログである．

4.5 情報処理の誤り

計算ミスなどの情報処理の誤りに係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，その情報システムで，被告は，その情報の，誤った処理をした.」

被告側：(1)「その時，その情報システムで，被告は，その情報の，誤った処理をしなかった.」(1) の証明は，不存在の証明である．この証明の負担が大きいことは前述した．

しかし，出来事ではなく，情報の状態に着目するならば，被告は不存在の証明に依らずに，存在の証明によって原告の主張を退けることができる．

被告側：(2)「その時，その情報システムでされた，その処理結果は，正しい処理結果に等しい.」換言すれば,「その時，その情報システムでされた，正しい，処理結果」を示せばよい．この要素は，いつの，どこの，どのような，なに，であり，原告側の記述要素よりも少なくなる．

あるべき処理がされた情報と，当該情報との同一性を証明することで，原告の「誤った処理」の主張を否定できる．(2) を表すログはイベントログではなく，この情報システムのあるべき処理を示した設計書，仕様書等どおりの処理結果が存在したことを示すステータスログである．

4.6 情報の偽造

架空の売上記録などの情報の偽造に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，その情報システムで，被告は，その情報を偽造した.」

被告側：(1)「その時，その情報システムで，被告は，その情報を，偽造しなかった.」

(1) の証明は，不存在の証明である．この証明の負担が大きいことは前述した．しかし，出来事ではなく，情報の状態に着目するならば，被告は不存在の証明に依らずに，存在の証明によって原告の主張を退けることができる．

被告側：(2)「その時，その情報システムで作られた，その情報は，事実に等しい.」換言すれば,「その時，その情報システムで作られた，事実と同じ，情報」を示せばよい．この要素は，いつの，どこの，どのような，なに，であり，原告側の記述要素よりも少なくなる．

取引の事実を表す伝票などと，当該情報との同一性を証明することで，原告の「偽造」の主張を否定できる．(2) を表すログはイベントログではなく，この情報システムに入力されるべき事実を表す伝票の記載と同じ値が入力されていることを示すステータスログである．

4.7 情報の消失

情報の消失に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：「その時，その情報システムで，被告が，その情報を，削除した.」

被告側：(1)「その時，その情報システムで，被告が，その情報を，削除しなかった.」

(1) の証明は，不存在の証明である．この証明の負担が大きいことは前述した．しかし，出来事ではなく，情報の存在自体に着目するならば，被告は不存在の証明に依らずに，存在の証明によって原告の主張を退けることができる．

被告側：(2)「その時以後，その情報システムに，その情報があった.」換言すれば,「その時以後，その情報システムに，保存されていた，情報」を示せばよい．この要素は，いつの，どこの，どのような，なに，であり，原告側の記述要素よりも少なくなる．

過去のある時点における情報の存在を証明することで，原告の「削除」の主張を否定できる．(2) を表すログはイベントログではなく，この情報が争点となっている過去のある時点に存在した状態を示すステータスログである．

4.8 情報利用の停止

システムダウンなどによる情報利用の停止に係る行為とその有無を示す要証事実の記述構成は次のとおりである．

原告側：(1)「その時，その情報システムで，被告は，その情報を，利用できないようにした.」

(1) は被告の作為が原因である場合である．

原告側：(2)「その時，その情報システムで，被告は，その情報を，利用できるようにしなかった.」

(2) は被告の不作為が原因である場合であり，この証明は，不存在の証明である．被告の作為・不作為を原告が証明できない場合でも，原告が情報を利用できなかった事実の証明に換えることができる場合がある．

原告側：(3)「その時，その情報システムで，原告は，その情報を，利用できなかった.」

(3) には，被告は原告に情報を利用させることを契約しているにもかかわらず，原告がそれを利用できなかったのは契約違反だ，という前提がある．

原告側：(4)「その時，その情報システムで，原告は，その情報の，利用に失敗した.」

(4) は，(3) の利用の不可能性という状態を,「利用の失敗」という出来事の証明に換えたものである．

一方，(1)〜(4) に対抗する被告の要証事実は，それぞれ以下の (1) ’〜(4) ’である．

被告側：(1) ’「その時，その情報システムで，被告は，その情報を，利用できないようにしなかった.」

被告側：(2) ’「その時，その情報システムで，被告は，その情報を，利用できるようにした.」

被告側：(3) ’「その時，その情報システムで，原告は，その情報を，利用できた.」

被告側：(4) ’「その時，その情報システムで，原告は，その情報の，利用に成功した.」

(4) は「利用の失敗」であるのに対して，(4) ’は「利用の成功」という出来事である．

(1)，(2) ’；(4)，(4) ’の証明は出来事の存在の証明，(1) ’；(2) の証明は出来事の不存在の証明である．不存在の証明よりも存在の証明の方が負担の少ないことは前述した．ログに記述されるべき要素は，いつ，どこで，だれが，なにを，どうした，であり，原告側と被告側が記述すべき要素量は変わらない．

他方，(3)，(3) ’は状態の証明である．前項までに述べてきた状態は，情報の性質・存在に係る状態であって，誰にとっても同じである．しかし，(3)，(3) ’の指す状態は，情報の利用可能性であって，全ての利用者が同様に利用可能であるとは限らない．よって，ログに記載すべき要素のうち，だれ，の要素を外すことはできない．したがって，ログに記述されるべき要素は，いつ，どこで，だれが，なにを，どうした，であり，原告側と被告側の記述要素量は同じである．

5 情報処理プロセスと機密性・完全性・可用性

観測されログに記述されるべき現象に係る情報処理プロセス（入力，処理，出力）について考察する．守るべき情報資産を保護する情報システムの範囲を考えるとき，この範囲の情報処理プロセスと機密性，完全性，可用性に係る要証事実のイベントとステータスの対応関係は次のとおりである（図 3 参照）．

機密性：保護範囲外への情報の出力のイベント（例 read, copy, move, print, etc.），イベントに換わるべきステータスはなし．

完全性：保護範囲内の情報への入力及び保護範囲内における情報の処理のイベント（例 write, edit, rename, insert, update, etc.），情報のステータス（例 identity, verify, correct, equal, etc.）

可用性：保護範囲外への情報の出力，保護範囲内の情報への入力，及び保護範囲内における情報の処理のイベント（例 success, failure, error, down, up, erase, delete, etc.），情報処理プロセスのステータス（例 fault, enable, disable, found, not found, etc.）

したがって，情報資産の保護範囲外のイベントログやステータスログ，保護範囲内であっても，情報資産とその利用に影響を与えないイベントログやステータスログは，情報セキュリティ事件の証拠にはなり得な

い．例えば，情報システムのパフォーマンスログの多くは，情報セキュリティ事件とは直接の関係がないログである．

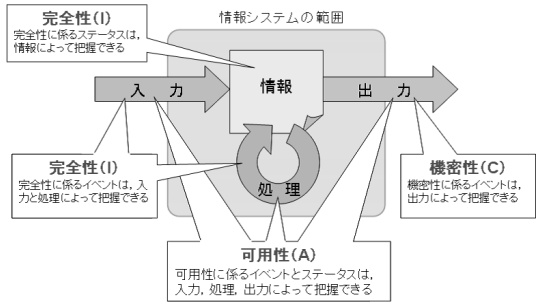

図 3: 情報処理プロセスと機密性・完全性・可用性

6　情報処理プロセスと責任追跡性

ログに記述されるべき要素と情報処理プロセスが特定できたとしても，それだけでは十分ではない．情報システムの操作の主体（だれ）と客体（なに）が記録されているにもかかわらず，それらが特定できないことがあるからである．

- 同一ユーザに異なるユーザ ID が割り当てられ，かつ，それら ID が一対一で対応しない，または対応関係が分からない．
- ファイル名を変更，別のファイル名で新規保存，ファイルの一部をコピーして別ファイルを新規作成など，ファイルが遷移するときの前後のつながりが記録されない．

上記はいずれも，その操作の記録から，操作の主体又は客体を一意に追跡することを不可能にする．したがって，ログは，情報処理プロセスに一連の操作の遷移があっても，主体及び客体が一意に追跡可能な特性を具備しなくてはならない．これを責任追跡性という．

ただし，４章で考察したとおり，原告は，操作主体である被告（だれ）の特定が必須であるが，被告は必ずしも操作主体を特定できなくとも良い場合がある．

7　証拠となり得るログを収集する情報システムの要件

以上より，情報セキュリティ事件の証拠となるログを収集する情報システムの要件を，以下のとおり定義する．

情報セキュリティ事件の証拠となるログを収集する情報システムは，

1. 目的とする情報セキュリティの特性（機密性，完全性，可用性），事件及び用途（原告：責任追及，被告：責任追及への反論）に応じて，
2. 必要な記述要素（いつ／いつの，どこで／どこの，だれが／だれの，なにを／なに，どうした／どのような）を含む，
3. 客体（情報）に係る情報処理プロセス（入力，処理，出力）のイベントログ，ステータスログ，または客体（情報）のステータスログを，
4. 情報システムの操作の主体（操作者：だれが）と客体（情報：なに）を一意に追跡できるように，

証拠能力と証明力とを具備しながら収集できること．

8　まとめ

ログの証明力の評価は次のプロセスを経る．先ずログに記された事柄に要証事実が含まれるかが確認され，ログと要証事実の因果関係が経験則により判断されることで根拠性が評価され，さらに対立当事者の反論を経て安定性が評価される．本稿は，1 章で証明力の評価の最初のステップである，ログに記すべき事項と要証事実の間に見られる課題を述べ，2 章で情報セキュリティに係る事件を類型化し，3 章で損害賠償請求におけるログの役割を見極め，4 章で事件の類型ごとに原告と被告に分けて要証事実とログの記述要素を整理し，5，6 章で情報処理プロセスと機密性，完全性，可用性，責任追跡性との関係を論じ，7 章で要件定義を行った．本考察は，より目的に合致したログを収集するシステムの仕様検討に向けた第一歩としたい．

参考文献

[1] 『最高裁判所民事判例集』, 29 巻 9 号, pp1417.

[2] 間形文彦, 高橋克巳他,“ 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 ”, 電子情報通信学会 SCIS2008 予稿集,4E1-6,2008 年 1 月.

[3] 間形文彦, 高橋克巳,“ 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 ”, 電子情報通信学会総合大会 予稿集, AS-1-1, 2009 年 3 月.