訴訟リスクを考慮した情報セキュリティ対策選定方式に関する検討

臼井　佑真*1　山本　匠*5　間形　文彦*2　勅使河原　可海*3　佐々木　良一*4　西垣 正勝*5,*6

*1 静岡大学大学院情報学研究科 〒432-8011 静岡県浜松市中区城北 3-5-1
*2 NTT 情報流通プラットホーム研究所〒180-8585　東京都武蔵野市緑町 3-9-11
*3 創価大学大学院工学研究科 〒192－8577 東京都八王子市丹木町 1－236
*4 東京電機大学未来科学部〒101-8457　東京都千代田区神田錦町 2-2
*5 静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市中区城北 3-5-1，*6 JST，CREST

あらまし　セキュリティインシデントが生じなければ訴訟も起きないため，企業や組織のセキュリティ対策としてはまず，ファイアウォールやデータの暗号化等の既存の ISMS 対策を適切に実施することが肝要である．しかし，現実には完全な対策は存在しない．このため，インシデントの発生，またそれに係る訴訟が発生した際に備えて，システム稼動ログやユーザの操作ログの保管といった DF(Digital Forensics)対策も併用する必要がある．本稿では，ISMS 対策と DF 対策の両者について，費用対効果を見込んだ上でセキュリティ対策の選定を最適化する方式を提案し，ケーススタディを用いてその有効性に関する検討を行う．

A case study of a security measure selection scheme with consideration of potential lawsuit

YUMA USUI*1 TAKUMI YAMAMOTO*5 FUMIHIKO MAGATA*2
YOSHIMI TESHIGAWARA*3 RYOICHI SASAKI*4 MASAKATSU NISHIGAKI*5,*6

*1 Graduate School of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011, JAPAN
*2 NTT Information Sharing Platform Laboratories, 3-9-11 Midori-Cho, Musashino, Tokyo, 180-8585, JAPAN
*3 Graduate School of Engineering, Soka University, Tangimachi, Hachioji, Tokyo, 192-8577, JAPAN
*4 School of Science and Technology for Future Life, Tokyo Denki University,
2-2 Kanda-Nishiki-Cho, Chiyoda-Ku, Tokyo, 101-8457, JAPAN
*5 Graduate School of Science and Technology, Shizuoka University, *6 JST, CREST

Abstract　Incidents on ITC systems will result in lawsuits. Needless to say, information security countermeasures (firewall, data encryption and so on) are essential; if we could protect our system against any security threats including viruses and hackers, incidents such as information leakage due to illegal accesses and/or service suspension due to denial-of-service attack will not occur. However, there could be no perfect countermeasures. Therefore, companies and organizations need to be prepared for litigation. That is, digital forensic countermeasures (management of a variety of system event logs) should be applied with information security countermeasures together. This paper proposes an approach to formulate an optimization problem to select both security and forensics countermeasures that maximizes cost-effectiveness.

1. はじめに

今日，ほとんどの業務基盤が ITC（Information Technology and Communication ）システムによって支えられている企業や組織において，システムのセキュリティを確保することは避けて通れない課題となった．特に，企業や組織は相次ぐ情報漏洩事件の発生により，機密情報や機微情報の保護の徹底が望まれている．そのため，多くの組織が ISMS（Information Security Management System）を構築するためのポリシーを策定しており，ISMS のためのツールや対策の研究開発が進められている[1][2].

しかし，依然として情報漏洩事件は後を絶たず，

JNSA の調査によると 2008 年の個人情報漏洩事件は過去最高の 1,373 件を記録している[3].

約 450 万人の情報が流出した Yahoo! BB の顧客情報漏洩事件では，集団訴訟にまで発展し，原告 5 人に対し一人5500円の賠償金を支払うよう命じられている[4]．また，TBC グループの漏洩事件では，原告 14 人による集団訴訟が発生し，13 人に対し過去最高の賠償額である 3 万 5000 円の支払いを命じる判決が下されている[5].

両者の事件から最悪のケースを想定すると，もし被害者全員による集団訴訟が起こった場合には，何百万人という被害者に数万円の賠償金を払わなければならなくなる．また，工業製品の設計データや製造ノウハウが漏洩した場合の損害賠償額などもとりわけ大きなものになり得るだろう．故に企業や組織は，セキュリティインシデントによる直接的な被害だけでなく，それに起因した訴訟についても検討し，対応しなければならないと考えられる.

これに対し，冒頭で記した ISMS 支援に関する既存方式や既存製品においては，インシデントの発生によって被る直接被害のみの最小化を目的としたものがほとんどである．そこで本研究では，インシデントが訴訟に発展した場合の損害賠償についても考慮に入れ，最適なセキュリティ対策を選定する方式を検討する.

セキュリティインシデントが生じなければ訴訟も起きないため，企業や組織のセキュリティ対策としてはまず，ファイアウォールやデータの暗号化等の既存の ISMS 対策を適切に実施することが肝要である．しかし，現実には完全な対策は存在しない．このため，インシデントの発生，またそれに係る訴訟が発生した際に備えて，システム稼動ログやユーザの操作ログの保管といった DF(Digital Forensics)対策も併用する必要がある．本稿では，ISMS 対策と DF 対策の両者について，費用対効果を見込んだ上でセキュリティ対策の選定を最適化する方式を提案する．また，ケーススタディにより提案方式の有用性を示す.

2. 提案方式

2.1. ISMS 対策

セキュリティインシデントの発生を抑える対策を ISMS 対策と定義する．基本的には，ファイアウォール，データの暗号化，アクセス制御など，ISMS 支援に関する既存方式[1] [2]等において検討されているセキュリティ対策を指す．適切な ISMS 対策を施すことにより，情報漏洩や不正アクセスなどのインシデントの発生を抑え，企業や組織の資産の直接的な損失を抑えることができる．また，インシデントの発生を防ぐことで訴訟も生じ得なくなるため，訴訟発生の確率も低減できる.

ISMS を構築するためにはリスク分析を行う必要がある．まず，情報資産を洗い出してその資産価値を算出した上で，資産へ影響を与える脅威を洗い出しその発生確率を見極める．洗い出した資産の資産価値，脅威の発生確率の積を計算することで，損失期待値（EVL）を算出することができる．よって，EVL は下記の式により定式化できる.

$$EVL = \sum_k VA_k PI_k \qquad (1)$$

ここで，VA_k は組織が持つ k 番目の情報資産の資産価値を表し，PI_k は k 番目の資産が失われる脅威の発生確率を表す.

リスク分析に続いて，採りうる対策の対策効果を分析する必要がある．リスク分析により定義された脅威に対する対策となりえる全てのセキュリティ対策を洗い出し，その対策により脅威が生じる確率をどれほど低減できるのか評価する.

対策の選定では，より少ない費用でより高い効果を得られる対策，つまり，費用対効果が最大になる対策が選ばれるべきである．そのため，ISMS 対策の選定は，式(2)を満たす ISMS 対策を選ぶ方式として定式化されることとなる.

$$Min(EVL \cdot E_{ISMS} + C_{ISMS}) \qquad (2)$$

ここで，EVL は損失期待値，E_{ISMS} は採択された対策の対策効果（脅威の発生をどれほど低減できるか），C_{ISMS} は採択された対策の導入にかかる費用を表す.

2.2. DF 対策

セキュリティインシデントが訴訟へと発展した際に，企業や組織が被る損害を軽減するための対策を DF 対策と定義する．文献[6]にて提案されているようなシステム稼動ログやユーザの操作ログを保管する技術などを指す.

組織が DF 対策を施しておくことには 2 つの利点が考えられる．まず 1 つは犯人（内部犯を含む）により被害を受けたとき，DF 対策によりその犯人を特定し犯人に賠償訴訟を起こす助けになる点である．2 つ目は，組織がセキュリティ事故を起こして起訴されたとき，DF 対策により組織の過失の範囲を法的な証拠により証明し，無過失の部分に対してまで賠償を命じられることを防止できる点である.

DF 対策を適切に選ぶためには訴訟リスクの分析を行う必要がある．まず，起こりうる訴訟を洗い出し

その賠償金を算出した上で，訴訟の起きる確率，その訴訟に負ける確率（敗訴確率）を見極める．洗い出した訴訟の賠償金や発生確率，敗訴確率の積を計算することで，賠償期待値（EVC）を算出することができる．

一般的に，被害を被った被害者は失った「資産」の賠償を求めて訴訟する．そのため，我々は EVC を計算するため，資産を基準とした賠償金を考えることとした．I_k を k 番目の資産が失われる脅威として定義し，L_k を I_k によって起こされる訴訟として定義する．このとき，EVC は下記の式により定式化できる．

$$EVC = \sum_k VC_k PO_k PL_k \quad (3)$$

ここで，VC_k は L_k によって起きる訴訟の賠償金を，PO_k は L_k の発生確率を，PL_k は L_k に敗訴する確率を表す．

式(3)の訴訟リスクの分析においては，まだ，DF 対策について考慮していないことに注意されたい．本稿では，組織が何の DF 対策も採用していない場合には常に敗訴するという仮定をおくこととする．つまり，式(3)での PL_k は 1.0 であり，式(3)は単純に式(4)となる．

$$EVC = \sum_k VC_k PO_k \quad (4)$$

リスク分析に続いて，DF 対策の対策効果を分析する必要がある．リスク分析により定義された訴訟に対する対策となりえる全ての DF 対策を洗い出し，その対策により敗訴確率をどれほど低減できるのか評価する．本稿では，DF 対策の敗訴確率に関しては文献[7]の評価式を利用することとする．

DF 対策も費用対効果が最大になるように選ばれる．よって，DF 対策の選定は，式(5)を満たす DF 対策を選ぶ方式として定式化されることとなる．

$$Min(EVC \cdot E_{DF} + C_{DF}) \quad (5)$$

ここで，EVC は賠償期待値，E_{DF} は DF 対策の対策効果（訴訟の敗訴確率をどれほど低減できるか），C_{DF} は採択された対策の導入にかかる費用を表す．

2.3. ISMS 対策と DF 対策の選び方

式(1)～(5)を用いて，ISMS 対策と DF 対策の選択は以下の式で定式化できる．

$$Min(Loss + Cost) \quad (6)$$

$$Loss = EVL \cdot E_{ISMS} + EVC \cdot E_{DF}$$

$$= (\sum_k VA_k PI_k) E_{ISMS} + (\sum_k VC_k PO_k) E_{DF} \quad (7)$$

$$Cost = C_{ISMS} + C_{DF} \quad (8)$$

ある ISMS 対策のセットが ITC システムに適用されると仮定する．脅威は資産ごとに異なり，対策は脅威ごとに異なるため，適用された ISMS 対策の効果は資産ごとに異なることになる．そのため，本稿では ISMS 対策の対策効果（E_{ISMS}）を資産ごとに算出することとする．EI_k を I_k ごとの ISMS 対策の効果として定義する（2.2 節で，I_k は k 番目の資産が失われる脅威として定義されている）ことによって，式(9)が得られる．

$$(\sum_k VA_k PI_k) E_{ISMS} = \sum_k VA_k PI_k EI_k \quad (9)$$

同様に，訴訟の内容も失われる資産ごとに異なり，対策も訴訟ごとに異なる．そのため，適用される DF 対策の対策効果（E_{DF}）も資産ごとに異なる．よって本稿では，E_{DF} についても資産ごとに算出することとする．EL_k を L_k ごとの DF 対策の効果として定義する（2.2 節で，L_k は I_k によって起こされる訴訟として定義されている．I_k は k 番目の資産が失われる脅威である）ことによって，式(10)が得られる．

$$(\sum_k VC_k PO_k) E_{DF} = \sum_k VC_k PO_k EL_k \quad (10)$$

基本的に，脅威が発生し，脅威が資産に影響を与えて初めて訴訟が発生する．つまり，脅威 I_k（資産 k が失われること）が訴訟 L_k を引き起こすと考えられる．よって，脅威の発生確率 PI_k と訴訟の発生確率 PO_k は従属関係にある．ISMS 対策によって脅威 I_k の発生確率は $PI_k EI_k$ となるため，式(11)が成立する．

$$PO_k = \alpha PI_k EI_k \quad (11)$$

ここで，α は資産が失われた結果，実際に訴訟に発展する確率（訴訟係数）を表す．

式(9)～式(11)を用いて，式(12)を得ることができる．

$$Loss = \sum_k PI_k EI_k (VA_k + \alpha VC_k EL_k) \quad (12)$$

以上より，式(6)，(8)，(12)を計算することで最も費用対効果の高い ISMS 対策と DF 対策の両者を選ぶことができる離散最適化問題に落とし込むことができる．

3. 提案方式の検討

本稿で定式化した ISMS・DF 対策選定法式の有用性を確かめるため，ケーススタディを用いて検討する．今回のケーススタディでは「情報漏洩事故」を対象とし，ある組織が情報漏洩事故を起こした際に被害者から無過失の部分の賠償まで訴えられるケースについて，提案方式を適用し有用性を検討する．

なお，提案方式による対策選定のためには離散最適化問題を解く必要があるが，本稿ではヒューリスティックな解法によって準最適解を求めることとする．

3.1. 想定対象

本ケースでは医療機関の資産として個人情報に着目した．緒元を表 1 に示す．スタディを簡素にするため，情報資産の数は1つである．

表 1：想定対象（医療機関）

資産番号（k）	1
資産の名称	個人情報（通院履歴，身体情報等を含む）
資産価値	3 万円/1 件×1 万件
資産に対する脅威（I_k）	情報漏洩
ISMS 無対策時の脅威の発生確率(PI_k)	0.57
脅威発生により引き起こされる訴訟（L_k）	プライバシ侵害に対する損害賠償
訴訟における損害賠償請求額（VC_k）	3 万円/1 件×漏洩データ件数
訴訟に発展する確率（訴訟係数α）	0.03
DF 無対策時の敗訴確率(PL_k)	1.0

医療機関の個人情報であるので，名前や住所だけでなく，通院履歴や身体情報などプライバシの高い情報も含む．このような情報は，情報漏洩の際に被害者が被る精神的苦痛が大きいため，損害賠償額も高額になると考えられる．事実，先述したように TBC（エステティックサロン）の個人情報漏洩事件訴訟では一人 3 万 5 千円の支払いが命じられている[5]．これを参考に，今回のケースでは 1 データ当たりの個人情報を 3 万円とした．また，この医療機関が保持する個人情報のデータ数は1万件と設定した．

個人情報という資産(k)に対する脅威（I_k）は，機密性の喪失（個人情報の漏洩）である．情報漏洩を発生させる原因としては，不正アクセスやマルウェアなどのシステムクラックから USB メモリの紛失などの運用ミスまで種々のものが考えられる．リスク分析によってそれらをすべて洗い出し，各々の発生確率を算定する．紙面の都合上，詳細は割愛するが，今回のケースでは，情報漏洩を発生させる原因として 10 個の原因が抽出されたとする．

これらの原因のうち，いずれかが一つでも発生することにより，情報漏洩が起こる．今，i番目の原因の発生確率をP_iとすると，i番目の原因が発生しない確率は $1-P_i$であり，すべての原因が発生しない確率は$\Pi(1-P_i)$となる．よって，いすれかの原因が発生する確率，すなわち，情報漏洩が発生する確率（PI_k）は$1-\Pi(1-P_i)$[☆]である．今回のケースでは，スタディの簡単化のために，10 個の原因の発生確率をすべて 0.08 とした．よって，PI_kは 0.57 である．なお，この時点でのPI_kは，ISMS無対策事の情報漏洩発生確率であることに留意されたい．

情報漏洩は情報の消失をともなわないので，情報漏洩発生後もこの医療機関の情報システムは健全に動作し続ける．よって，情報漏洩の発生による一次損失（VA_k）は 0 である．情報漏洩の発生によって医療機関が被る被害は，患者のプライバシ侵害に対する賠償請求や信用失墜に起因する風評被害などの二次損失が主なものとなる．本稿では，スタディの簡単化のため，脅威発生により引き起こされる訴訟(L_k)，すなわち，患者からの損害賠償請求訴訟のみを扱うこととする．訴訟（L_k）の発生確率（PO_k）は，情報漏洩の発生確率(PI_k)と訴訟係数(α)の積であるが，今回はαを，JNSA[3]で情報漏洩による賠償金を計算する際に用いられている値に合わせ，0.03 と置いた．また，DF 無対策時の敗訴確率（PL_k）は 1.0 である．

訴訟における損害賠償請求額は，1 データ当たりの資産価値（3 万円）と漏洩したデータ数の積によって算出する．例えば，1,000 件のデータが漏洩した場合であれば，損害賠償請求額（VC_k）は 3 千万円（3 万円/件×1,000 件）である．しかし，情報漏洩事故が発生した以上，被害者の心情としては「自分の情報も漏洩したのではないか」という疑心暗鬼に囚われることは必然であり，最悪，この医療機関に関係するすべての患者が集団訴訟を起こす可能性がある．その場合，医療機関が「漏洩したデータは本当に 1,000 件のみである」ということを立証することができない限り，すべての被害者に対して総額3億円（3 万円/件×1 万件）の損害賠償を支払わなければならなくなるという事態になり得る．

3.2. 対策効果

医療機関が採りうる対策とその対策効果について検討する．対策には，脅威（I_k）に備える ISMS 対策，訴訟（L_k）に備える DF 対策が存在する．ISMS 対策の対策効果の評価には既存方式[1]を，DF 対策の対策効果の評価には文献[7]の評価式を参考にした．

ISMS 対策においては，3.1 節のリスク分析によって洗い出した「脅威を引き起こす原因」のそれぞれ

☆ 文献[2]などのようにフォールトツリー解析によって情報漏洩（頂上事象）の発生確率を計算する方法もある．

に対して，その原因の発生確率を低減する対策（その原因がクラッキング等の攻撃である場合には，その攻撃の成功確率を低減する対策も含む）を列挙するとともに，その対策効果（原因の発生をどれほど低減できるか）と導入コストを評価する．ISMS 対策の例としては，ファイアウォール，アンチウィルスソフト，アクセス制御等が挙げられる．紙面の都合上，詳細は割愛するが，今回のケースでは，考えられる ISMS 対策として 10 個の対策が挙がったとする．

既存方式[1]では，「脅威を引き起こす原因」と「その対策」のマトリクスを用いて対策効果（E_{ISMS}）を表現する．今回用いたマトリクスの一部を表 2 に示す．今回のケースでは，3.1 節のリスク分析にて，10 個の情報漏洩の原因が抽出されており，それが縦軸に列挙されている．また，ISMS 対策として挙がった 10 個の対策が横軸に列挙されている．縦軸と横軸の交点に記されている値が，それぞれの「情報漏洩の原因」に対する各「ISMS 対策」の対策効果である．

表 2：情報漏洩の原因と ISMS 対策効果

	ISMS 対策 1	ISMS 対策 2	…	ISMS 対策 9	ISMS 対策 10
不正アクセス	0.5	0	…	0	0
マルウェア	0	0.7	…	0	0
:	:	:	…	:	:
紛失・置忘れ	0	0	…	0.8	0
盗難	0	0	…	0.6	0.7
対策コスト	500	300	…	500	450

（対策コストの単位：万円）

今回のケースでは，10 個の「情報漏洩の原因」のそれぞれの発生確率 P_i(i=1～10)はすべて 0.08 と置いた．よって，情報漏洩の原因が 1 つでも生じてしまう確率，つまり情報漏洩の発生確率 $1-\Pi(1-P_i)$は 0.57 である．表 2 より，例えば ISMS 対策 1 は，情報漏洩の原因のうちの「不正アクセス」の発生確率（または不正アクセスの成功確率）を 0.5 の割合だけ減少させることが読み取れる．よって，ISMS 対策 1 のみが採用された場合，不正アクセスの発生確率が 0.04 となり，情報漏洩の発生確率は PI_k=0.55 となる．同様に表 2 より，ISMS 対策 2 は，情報漏洩の原因のうちの「マルウェア（による不正操作）」の発生確率を 0.7 の割合だけ減少させることが読み取れる．よって，例えば ISMS 対策 1 と ISMS 対策 2 が併用された場合，ISMS 対策 1 によって不正アクセスの発生確率が 0.04 となり，かつ，ISMS 対策 2 によってマルウェアの発生確率が 0.024 となるため，情報漏洩の発生確率は PI_k=0.52 となる．しかし，対策コストとして，ISMS 対策 1 を導入した場合は 500 万円，ISMS 対策 1 と 2 を導入した場合は 800 万円が必要となる．

一方，DF 対策においては，基本的に訴訟の際の証跡を残すためのシステム稼動ログやユーザの操作ログを保管する技術を導入することになる．DF 対策の例としては，タイムスタンプやヒステリシス署名等が挙げられる．紙面の都合上，詳細は割愛するが，今回のケースでは，考えられる DF 対策として 13 個の対策が挙がったとする．

間形らは，文献[8]にて訴訟における証跡としてログが備えるべき 13 の要件を提示している．13 要件のうち，要件 1，2 が根拠性を，要件 3～13 が安定性を満たすための要件となっている．根拠性とは，そのログが裁判で証明したい事実，つまり，要証事実を立証ための証拠になり得るかの度合いを示す．今回のケースでは，「何件分のデータの漏洩があったのか」という内容が記載されているログであるか否かが根拠性の論点となる．また，例えログに要証事実に関する記載があったとしても，そのログが誰でも作成できるものであった場合，もしくは，ログが改竄可能な状況下におかれていた場合には，そのログは証拠として認められない．そのログがどれだけの証明力を有しているかの度合いが安定性である．

間形らは，また，上記の 13 要件と敗訴確率の関係を定式化している[7]．本稿では，文献[7]の定式化を参考に，各 DF 対策の対策効果（E_{DF}）を 13 要件のそれぞれの充足率という形で表現し，採用されている全対策を通じ一番充足率の低い要件を考慮することによって敗訴確率（PL_k）を計算するという方法を用いることとする．

表 3：DF 対策の要件と DF 対策効果

	DF} 対策 1	DF 対策 2	…	DF 対策 12	DF 対策 13
要件 1	1	0.8	…	0	0
要件 2	0.8	0.7	…	0	0
:	:	:	…	:	:
要件 12	0	0	…	0.8	1
要件 13	0	0.7	…	0	0
対策コスト	200	100	…	50	150

（対策コストの単位：万円）

「各 DF 対策の 13 要件ごとの充足率」と「敗訴確率」の評価については，ISMS 対策の場合にようにマトリクスによる表記を利用することとする．今回用いたマトリクスの一部を表 3 に示す．今回のケースでは，DF 対策として挙がった 13 個の対策が横軸に列挙されている．縦軸は証明力に関する 13 個の要件で

ある．縦軸と横軸の交点に記されている値が，それぞれの「要件」に対する各「DF 対策」の対策効果（充足率）である．

本稿では，DF 無対策時の敗訴確率を 1.0 としている．表 3 より，例えばDF 対策 1 は，要件 1 の充足率が 1.0 で，要件 2 の充足率が 0.8 であることがわかる．これは，DF 対策 1 を採用することによって，要件 1 の不備のために敗訴する確率は 0.0 となり，要件 2 の不備のために敗訴する確率は 0.2 となることを意味している．DF 対策 1 は要件 3～13 の充足率には寄与しないため，DF 対策 1 を採用しても，要件 3～13 の不備のために敗訴する確率は 1.0 のままである．同様に表 2 より，DF 対策 2 は，要件 1 の充足率が 0.8，要件 2 の充足率が 0.7，要件 13 の充足率が 0.7 であることがわかる．DF 対策 1 および 2 を併用した場合，要件 2 には両方の対策が寄与する（DF 対策 1 の充足率が 0.8，DF 対策 2 の充足率が 0.7）が，今回は対策併用時の充足率は両者の充足率の最大値であると考える．すなわち，DF 対策 1 と 2 を併用した場合の要件 2 の充足率は 0.8 である．

説明を簡単にするために，要件 1，2，12，13 に対する充足率が 0.0 であり，要件 3～11 のすべてに対する充足率が 1.0 であるDF 対策 X（導入コスト 80 万）が存在すると仮定しよう．その場合，例えば，DF 対策 X，1，2，12 を併用した場合の要件 1 の充足率が 1.0，要件 2 の充足率が 0.8，要件 3～11 の充足率が 1.0，要件 12 の充足率が 0.8，要件 13 の充足率が 0.7 となる．本稿では，採用されている全対策を通じ一番充足率の低い要件を考慮することによって敗訴確率（PL_k）を計算する．よって，DF 対策 X，1，2，12 を採用した場合の敗訴確率は，要件 13 の充足率 0.7 に支配される．すなわち，敗訴確率（PL_k）は 0.3 となる．このときの対策コストは，430 万円である．

3.3. 最適解の導出

今回のケースでは，医療機関が実際に何件分のデータを漏洩してしまったのかが問題となる．ここでは，情報漏洩の規模が ISMS 対策の強度に依存すると仮定し，ISMS 対策効果（E_{ISMS}）を用いて，$(1-E_{ISMS})\times$1 万件分のデータが漏洩したとする．

一方，3.1 節で述べたように，被害者全員から集団訴訟を受けた場合の損害賠償請求額（VC_k）は 3 億円である．何の DF 対策も採っていない場合は，最悪，3 億円の賠償が命じられる．これに対し，適切な DF 対策を実施しておくことによって，実際の漏洩データ数が（$1-E_{ISMS}$）×1 万件であることが立証できれば，損害賠償額は（$1-E_{ISMS}$）×3 億円にまで低減し得る．

今回のケーススタディでは，式(6)，(8)，(12)の離散対数問題に表 1～3 の緒元を代入し，（準）最適な ISMS 対策, DF 対策を計算したところ, 損失期待値, 賠償期待値，対策コストの和を 2 億 4000 万円（無対策時）から約 8000 万円まで下げることができた．

4. おわりに

本稿では，ISMS・DF 対策の両者を，費用対効果が最も高くなるように選ぶことのできる方式の定式化を行い，その有用性をケーススタディにより示した．今後は情報漏洩以外のセキュリティインシデントでのケーススタディを検討し，より広い意味での提案方式の有用性を確かめたい．

謝辞　本研究は一部，（財）セコム科学技術振興財団の研究助成を受けた．ここに謝意を表する．

参考文献

[1] 中村他：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45, No8，pp.2022-2033，2004.8

[2] 永井他：セキュリティ対策目標の最適決定技法の提案，情報処理学会論文誌，Vol.41，No8，pp.2264-2271，2000.8

[3] JNSA：2008 年度　情報セキュリティインシデントに関する調査報告書, http://www.jnsa.org/result/2008/surv/incident/index.html

[4] INTERNET Watch : Yahoo! BB顧客情報流出の損害賠償訴訟，1人5,500円の賠償が確定, http://internet.watch.impress.co.jp/cda/news/2007/12/17/17899.html

[5] Security Next : TBCの個人情報漏洩訴訟，損害賠償額は3万5000円, http://www.security-next.com/005434.html

[6] 芦野他佑樹, 藤田圭祐, 入澤麻里子, 佐々木良一：デジタルデータ証拠保全プラットフォーム『Dig-Forceシリーズ』の開発と評価，DICOMO2008 論文集，pp.1523-pp.1530，2008.7

[7] 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，2009年電子情報通信学会総合大会発表論文集，AS-1-1，2009.3

[8] 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，2008 年暗号と情報セキュリティシンポジウム予稿集, 2008.1