情報処理学会論文誌　Vol. 52　No. 3　1173–1184 (Mar. 2011)

賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価

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

情報漏洩などのインシデントが生じなければ損害賠償も発生しないため，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などの既存の情報セキュリティ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，またそれに係る損害賠償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デジタルフォレンジック対策も併用する必要がある．本論文では，情報セキュリティ対策とデジタルフォレンジック対策の両者について，費用対効果を見込んだうえ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

Masakatsu Nishigaki,[†1,†2] Yuma Usui,[†3]
Takumi Yamamoto,[†1] Fumihiko Magata,[†4]
Yoshimi Teshigawara[†5] and Ryoichi Sasaki[†6]

Incidents on ICT 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 crackers, 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ICT（Information and Communication Technology）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)–3)]．

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[4)]．その中で，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1人5,500円の賠償金を支払うよう命じられている[5)]．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3万5,000円の支払いを命じる判決が下されている[6)]．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．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や，企業が企業を訴える場合の訴訟額などもとりわけ大きなものになりうるだろう．ゆえに企業や組織は，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，それに起因した損害賠償についても検討し，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

†1 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†2 独立行政法人科学技術振興機構，CREST
Japan Science and Technology Agency, CREST
†3 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University
†4 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories
†5 創価大学大学院工学研究科
Graduate School of Engineering, Soka University
†6 東京電機大学未来科学部
School of Science and Technology for Future Life, Tokyo Denki University

で本論文では，インシデントにより損害賠償が発生した際の対策も考慮に入れ，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損害賠償が発生する事態も起きないため，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などの既存の情報セキュリティ対策（以下，Information Security 対策，略して IS 対策と呼ぶ）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，またそれに係る損害賠償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デジタルフォレンジック対策（以下，Digital Forensics 対策，略して DF 対策と呼ぶ）も併用する必要がある．なお，損害賠償の手段としては，当事者間による示談や和解，第三者を介した裁判による判決などが考えられる．いずれにしても，支払うべき賠償額の根拠や責任の所在を明らかにする必要があり，電子データを証拠として扱う以上は DF 対策を用いて証拠を収集・保管することが必須であるといえよう．

そこで本論文では，IS 対策と DF 対策を考慮したうえで，両者の対策を費用対効果をふまえて効率的に決定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．

本論文の以下の構成は次のようになっている．2 章では，IS 対策や DF 対策の選定法についての関連研究を述べる．3 章では，IS 対策と DF 対策の両者について，費用対効果を見込んだうえでセキュリティ対策の選定を最適化する方式の定式化を行う．4 章では，ケーススタディを用いて提案方式の有用性を検討する．5 章で本論文のまとめと今後の課題を述べる．

2. 関 連 研 究

2.1 IS 対策の選択について

情報漏洩や不正アクセスなどのセキュリティインシデントの発生を抑える対策を IS 対策と定義する．ファイアウォール，データの暗号化，アクセス制御などのセキュリティ対策を指す．

組織の ISMS 構築の第一歩はリスク分析である．情報資産は一般的に年間予想損失額 ALE（Annual Loss Expectancy）として定式化される[7]．すなわち，情報資産を洗い出してその資産価値（損失額）を算出したうえで，資産へ影響を与える脅威を洗い出し，その（年間）発生確率を見極める．洗い出した資産の資産価値と脅威の発生確率の積を計算することで，ALE が算出される．

IS 対策選択の最適化は，組織におけるセキュリティ投資の費用対効果を高めることにほかならない．このため，経済学的なアプローチによって，IS 対策にかかる最適なセキュリティ投資総額を求めるための様々な手法が提唱されている[8),9)]．文献 8) では，投資額を z，投資により得られる収益の期待値を $EBIS$ とし，投資による純利益の期待値 $ENBIS$（$= EBIS - z$）を最大にする z が最適投資額であるという定式化を示しており，文献 9) では保険による効果をさらに加味したモデルを提唱している．また，上記の手法に金融工学におけるリアルオプションの考えを適用し，セキュリティ投資のタイミングの最適化を行う手法[10)] や，セキュリティ投資が株式時価総額に影響することに着目し，株価の増減により費用対効果を判断する手法[11)] なども提案されている．

一方，数ある対策案の中から最適な対策を合理的に決定するための方法についても研究が進められている[1),2),12)]．文献 1) では，ある対策を採用した際の脅威の発生確率の低減をモデル化し，各対策案の効果を残存資産という指標で定式化する．これは，脅威，資産，対策の関係に着目して IS 対策の選定を離散最適化問題として定式化するものであり，残存資産が最大になる対策を選ぶ手法である．文献 2) は，各脅威の発生がインシデントに至る過程を Fault Tree によってモデル化し，ミニマルパス解析によって，脅威に対抗する必要かつ最低限の対策を導出する．これは，脆弱性と資産価値に着目して，リスクに対抗する「必要最低限の IS 対策」を選定する手法である．さらに文献 12) では，文献 2) の方法を不正コピー防止対策に適用することによって，「費用対効果が一番高い不正コピー対策」を選定する方法を示している．これらは，詳細なリスク分析を通じて脅威の発生確率，情報資産の資産価値，脅威に対する対策の効果，対策に要するコストの関係を細かく洗い出すことで IS 対策効果を数学的に導出し，規定された制約条件を満たす IS 対策案の中から目的関数（残存資産または対策効果）が最大になる対策を選ぶという最適化問題型のアプローチである．

さらに，この最適化問題に対する解をリスクコミュニケーションによる合意形成によって求める方法[13)] や，最適化問題の定式化にあたって対策による利便性の低下[14),15)] や脅威が発生するまでの状態遷移[16)] を考慮するアプローチなども提案されている．

2.2 DF 対策の選択について

セキュリティインシデントにより損害賠償が発生した際に，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 17)，18) で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[19)]．1 つは，組織がセキュリティ事故を起こして損害賠償が発生したとき，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被害者から賠償を請求されたとしてもこれ

表 1　デジタル証拠の法的証明力を高めるための要件[21)]
Table 1　Requirements for enhancing legal basis of log.

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	記録に故意・過失が含まれていないこと
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

を阻止できる点である．つまり，訴訟に備える側（損害賠償を請求される側）から見た DF 対策の効果である．2 つ目は，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請求を行う助けになる点である．つまり，訴訟する側（損害賠償を請求する側）から見た DF 対策の効果である．これら 2 つの DF 対策効果を考慮することで，組織が内包する賠償リスクに柔軟に対応できると考えられる．

組織が DF 対策を選ぶ際には，DF 対策に求められる要件を認識し，その要件を過不足なく満たす必要がある．たとえば，裁判においてあるログを証拠として提出したとしても，そのログがだれ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．DF 対策の選択に関してはその研究がまだ緒に就いた段階であるが，文献 20) では，DF の定義に着目し，複数の DF 用ガイドラインを分析し，デジタル証拠作成のために共通する 4 つの要件の抽出を行っている．

また，文献 21) では，デジタル証拠（ログ）の法的証明力を高めるための 13 個の要件（**表 1**）を洗い出しており，文献 22) ではその要件に則って DF 対策を選ぶ方式が提案されている．13 要件のうち，要件 1，2 がデジタル証拠の証拠としての根拠性を，要件 3〜13 が証拠としての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，要証事実を立証するための証拠になりうるかの度合いを示す．また，安定性とは，提出した証拠に対して証拠としての力がどれくらい強いか（たとえば，「捏造されたログではないのか」といった反論に対して再反論が可能であるか，など）の度合いを示す．

なお，一般に，違法な行為によって受けた不利益を「損害」，損害を補填することを「賠償」と呼び，合法な行為によって受けた不利益を「損失」，損失を補填することを「補償」と呼ぶが，本論文においては簡単のために特に賠償，補償の区別はせず，両者を賠償と呼ぶこととする．

3. IS 対策と DF 対策の両対策選定の定式化

組織としては IS 対策，DF 対策の両者を具備することが必要であると考えられるが，前章で述べたようにそれぞれの対策の役割は異なっている．ここで，セキュリティインシデントによる損害賠償に着目すると，IS 対策はインシデントの発生を防ぐことで損害賠償の発生を抑える対策であり，DF 対策は訴訟などの損害賠償が発生した際に，ログにより証明したい事実を納得させるための対策であるといえる．しかし，著者らの調査した限りでは，IS 対策支援に関する既存方式や既存製品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．よって，本論文では，両者の対策を組み合わせることで，損害賠償までを考慮に入れた形で組織を取り巻くリスクに対して費用対効果が最も高くなるような IS 対策と DF 対策の両者を選ぶための方式を検討する．

組織がサービスを展開するにあたり，顧客情報を自組織内に管理することになる．この場合，組織（個人情報取扱事業者）は通常，顧客との契約上，顧客から提供を受けた個人情報を善良なる管理者としての注意義務をもって取り扱う責務を負担し，組織がこの注意義務を怠ったことにより個人情報が漏洩した場合には「債務不履行による損害賠償」を負うことになる．また，組織が事業を展開するにあたっては，業務上の秘密情報（出願前の特許情報など）が自組織内で管理されており，事業遂行のために従業員に秘密情報を開示することになる．この場合，従業員は通常，組織（雇用者）との労働契約における信義則上または就業規則上の秘密保持義務を負担し，従業員が雇用関係中に知りえた業務上の秘密を不当に開示した場合には「秘密保持義務違反による損害賠償」を負うことになる．このため本論文では，組織の保持する資産ごとに損害賠償を考えることとする．たとえば，顧客の個人情報という資産が不正アクセスなどの脅威により漏洩したとすれば，個人情報が漏洩したことにより被った分の損失を取り戻すための賠償請求が顧客側から発生すると考えられる（4 章のケーススタディにおけるケース 1）．また，特許情報という資産が内部犯によって外部に漏洩した場合には，特許情報が漏洩したことにより被った分の損失を取り戻すための賠償請求が組織側から発生すると考えられる（4 章のケーススタディにおけるケース 2）．つまり，資

産が脅威に侵されることで，資産に固有の損害賠償が発生するといえる．このため今回は，組織が持つ資産を基準として賠償金を考えることとする．

3.1 IS 対策の選定

企業や組織は適切な IS 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，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損害賠償も生じえなくなるため，損害賠償が発生する確率も低減させることができる．

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うえで，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．なお，無形物である情報資産の価値の算出は実際には難しい問題を含むが，本論文ではセキュリティ対策選択問題に焦点を絞り，リスク分析については確実に行えるものとして扱う．洗い出した資産の資産価値と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．

$$EVL = \sum_k VA_k PI_k \tag{1}$$

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．一般的に，それぞれの資産に対する脅威は 1 つではなく複数存在する．I_k を k 番目の資産 VA_k の損失を引き起こす脅威の集合として定義すると，PI_k は I_k のいずれかの脅威が発生する確率である．

リスク分析に続いて，とりうる対策の対策効果を分析する必要がある．リスク分析により顕在化された脅威に対する対策となりうるすべてのセキュリティ対策を洗い出し，その対策により脅威の発生確率（脅威が外部からの攻撃である場合には，その攻撃の成功率）をどれほど低減させることが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，IS 対策の選定は，式 (2) を満たす IS 対策を選ぶ方式として定式化されることとなる．

$$\mathrm{Min}(EVL \cdot E_{IS} + C_{IS}) \tag{2}$$

ここで，EVL は式 (1) の損失期待値，E_{IS} は採択された対策の対策効果（脅威の発生確率，攻撃の成功率をどれほど低減させることができるか），C_{IS} は採択された対策の導入にかかる費用を表す．選択する IS 対策によって E_{IS} の値は $0 \leqq E_{IS} \leqq 1$ の範囲で変動する．同時に C_{IS} の値も変動する．EVL は固定値であり変動することはない．

3.2 DF 対策の選定

DF 対策を適切に選ぶためには賠償リスクの分析を行う必要がある．まず，起こりうる損害賠償係争を洗い出しその賠償金予想額を算出したうえで，損害賠償係争の起きる確率，係争に負ける確率（敗訴確率）を見極める．なお本論文では，式 (1) で資産損失を正の数値として計算しているため，組織が他者から損害賠償請求を受ける場合の賠償金額を正，組織が他者に損害賠償請求を求める場合の賠償金額を負の数値として算出する．洗い出した賠償金額や発生確率，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」の賠償を求めて損害賠償を請求する．そのため本論文では，EVC の計算に対しては資産を基準とした定式化を考えることとした．前節で記したように I_k を k 番目の資産 VA_k の損失を引き起こす脅威の集合として定義し，L_k を資産 VA_k の損失によって起こされる損害賠償係争とする．このとき，EVC は下記の式により定式化できる．

$$EVC = \sum_k VC_k PO_k PL_k \tag{3}$$

ここで，VC_k は損害賠償係争 L_k における賠償額を，PO_k は損害賠償係争 L_k の発生確率を，PL_k はその損害賠償係争 L_k に敗訴する確率を表す．

式 (3) の賠償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．本論文では，組織が何の DF 対策も採用していない場合には（自らの主張を正当化するに足る証拠を提出できないため）つねに敗訴するという仮定を置くこととする．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．

$$EVC = \sum_k VC_k PO_k \tag{4}$$

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．リスク分析により顕在化された損害賠償係争に対する対策となりうるすべての 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させることができるのか評価する．DF 対策の敗訴確率に関しては文献 22) の評価式などを利用することができる．

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．

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

ここで，EVC は式 (4) の賠償期待値，E_{DF} は DF 対策の対策効果（損害賠償係争の敗訴確率をどれほど低減させることができるか），C_{DF} は採択された対策の導入にかかる費用

を表す．選択する DF 対策によって E_{DF} の値は $0 \leqq E_{DF} \leqq 1$ の範囲で変動する．同時に C_{DF} の値も変動する．EVC は固定値であり変動することはない．

3.3 両対策の選定

式 (1)〜(5) を合算することにより，IS 対策と DF 対策の両対策を合わせた形での対策選定は以下の式で定式化できる．

$$\mathrm{Min}(Loss + Cost) \tag{6}$$

$$\begin{aligned} Loss &= EVL \cdot E_{IS} + EVC \cdot E_{DF} \\ &= \left(\sum_k VA_k PI_k\right) E_{IS} + \left(\sum_k VC_k PO_k\right) E_{DF} \end{aligned} \tag{7}$$

$$Cost = C_{IS} + C_{DF} \tag{8}$$

ある IS 対策のセットが ICT 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 IS 対策の効果は資産ごとに異なることになる．そのため，本論文では IS 対策の対策効果（E_{IS}）を資産ごとに算出することとする．採用する IS 対策の効果のうち，資産 k の損失を引き起こす脅威（脅威集合 I_k に含まれる脅威）に寄与する対策の効果を EI_k（$0 \leqq EI_k \leqq 1$）と定義することによって，式 (9) が得られる．

$$\left(\sum_k VA_k PI_k\right) E_{IS} = \sum_k VA_k PI_k EI_k \tag{9}$$

式 (9) における $PI_k EI_k$ の項は，無対策の場合は PI_k であった資産 k の損失確率が，IS 対策の実施によって $PI_k EI_k$ に減少するということを意味している．

同様に，損害賠償係争の内容も失われる資産ごとに異なり，対策も損害賠償係争ごとに異なる．このため，適用される DF 対策の対策効果（E_{DF}）も資産ごとに異なる．よって本論文では，E_{DF} についても資産ごとに算出することとする．採用する DF 対策の効果のうち，資産 k の損失により引き起こされる損害賠償係争 L_k に寄与する対策の効果を EL_k（$0 \leqq EL_k \leqq 1$）と定義することによって，式 (10) が得られる．

$$\left(\sum_k VC_k PO_k\right) E_{DF} = \sum_k VC_k PO_k EL_k \tag{10}$$

式 (10) における $PO_k EL_k$ の項は，資産 k の損失に起因する損害賠償係争 L_k が PO_k の確率で発生するにあたり，無対策の場合は 1.0 であった敗訴確率が，DF 対策の実施によって EL_k に減少するということを意味している．

資産 k の損失により損害賠償係争 L_k が発生する．つまり，資産 k の損失確率と損害賠償係争 L_k の発生確率 PO_k は従属関係にある．式 (9) より，IS 対策によって資産 k の損失確率（攻撃の成功確率）は $PI_k EI_k$ となるため，式 (11) が成立する．

$$PO_k = \alpha PI_k EI_k \tag{11}$$

ここで，α は資産の損失が実際に損害賠償係争に発展する割合（係争係数）を表す．「インシデントの発生がある集団に損失を与えた場合は，$PI_k EI_k$ の確率で資産 k の損失が発生した結果，全被害者 X 人のうちの αX 人が損害賠償係数 L_k を求める訴えを起こす」という意味で係争係数をとらえてもよい．式 (9)〜式 (11) を式 (7) に代入して，式 (12) を得ることができる．

$$Loss = \sum_k PI_k EI_k (VA_k + \alpha VC_k EL_k) \tag{12}$$

以上より，IS 対策と DF 対策の両者の最適な組合せを選択する問題が，式 (6)，(8)，(12) による離散最適化問題として定式化される．すなわち，候補となりうるすべての IS 対策と DF 対策の組合せに対して $Loss$（式 (12)）と $Cost$（式 (8)）を計算し，$Loss + Cost$ が最小（式 (6)）となる対策セットを採用することによって，最も費用対効果の高い IS 対策と DF 対策の組合せを選ぶことができる．

4. ケーススタディ

本論文で定式化した IS・DF 対策選定方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」を想定し，

- ケース 1：クラッキングによるサーバダウンの際に情報漏洩を疑われる．
- ケース 2：組織内の機密情報を盗んだ犯人に賠償請求する．

のそれぞれの場合において提案方式を適用する．なお，被害規模の違いが対策の選定に与える影響を検討するため，ケース 1 および 2 に対して規模の異なる 2 つの組織を想定し，計 4 つのケースで検討を行う．

4.1 ケース 1：クラッキングによるサーバダウンの際に情報漏洩を疑われる

4.1.1 想 定 対 象

本ケースでは，顧客の個人情報を保持するオンラインショップ販売業者（個人情報取扱事業者）のサーバが不正アクセスやマルウェア感染によってクラッキングされた際に，情報漏洩の疑いをかけられて顧客に賠償請求される場合を想定する．個人情報の保有件数により，ケース A）大手販売業者（個人情報保有件数 100 万件），ケース B）中小販売業者（個

表 2　想定対象（ケース 1）
Table 2　Case study 1.

ケース	ケース A		ケース B	
組織	大手ネットショップ販売業者		中小ネットショップ販売業者	
個人情報の保有件数	1,000,000 件		5,001 件	
資産番号（k）	1	2	1	2
資産の名称	顧客の個人情報	業務サーバ	顧客の個人情報	業務サーバ
資産に対する脅威（I_k）	情報漏洩	サーバダウン	情報漏洩	サーバダウン
IS 対策無しの時の脅威の発生確率(PI_k)	0.9706	0.9460	0.9706	0.9460
脅威発生時の直接損失額（資産価値 VA_k）	88,700 万円	7,253 万円	444 万円	1,546 万円
資産損失により発生する損害賠償係争（L_k）	プライバシ侵害に対する損害賠償	なし	プライバシ侵害に対する損害賠償	なし
損害賠償係争における賠償額（VC_k）	950,000 万円	0 円	4,751 万円	0 円
損害賠償係争に発展する確率（係争係数 α）	1.0			
DF 無対策時の敗訴確率(PL_k)	1.0			

人情報保有件数 5,001 件：個人情報取扱事業者としての最低保有件数）に分け，検討を行う．**表 2** に想定対象の概要を示す．

今回は，検討の簡単化のため，資産を「顧客の個人情報」と「業務サーバ」の 2 つに絞った．また，厳密には大手業者と中小業者とで脅威の発生確率，賠償係数などの諸元が異なりうると考えられるが，ここでは同じ値を用いている．これは，組織が所有する個人情報の規模（被害規模）による対策選定結果の違いを検討することが，本ケーススタディの主目的であるためである．

個人情報という資産（資産 1）に対する脅威は，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．いずれかの原因が 1 つでも発生することにより，情報漏洩が起こる．また，業務サーバという資産（資産 2）に対する脅威は，可用性の喪失（サーバダウン）である．サーバダウンを発生させる原因についてもリスク分析を行い，各々の発生確率を算定する．今回のケースでは，既存研究において過去に実施された実在する組織の ISMS リスク分析の結果[1] を基に，情報漏洩やシステムダウンを発生させる原因として**表 3** にあげた 10 個の脅威要因 i（$i = 1, 2, \cdots, 10$）を抽出した．このうち，表 3 の「情報漏洩の原因」の列に YES と記載されている脅威要因の集合が，個人情報（資産 1）に対する脅威である情報漏洩を引き起こす要因集合（I_1）である．同様に，表 3 の「サーバダウンの原因」の列に YES と記載されている脅威要因の集合が，業務サーバ（資産 2）に対する脅威であるサーバダウンを引き起こす要因集合（I_2）である．

表 3　情報漏洩/サーバダウンの原因
Table 3　Possible factors of information leakage or server down.

要因番号 i	脅威要因	発生確率	情報漏洩の原因	サーバダウンの原因
1	権限者による不正（漏洩・改竄・破壊・持ち出し）	0.5	YES	YES
2	ウイルス対策ソフトウェア及び管理策の不備	0.5	YES	YES
3	計算機の不正使用（直接操作）	0.3	YES	YES
4	計算機の不正使用（内部ネットワークからの侵入）	0.3	YES	YES
5	計算機の不正使用（外部ネットワークからの侵入）	0.3	YES	YES
6	運用時における記憶媒体の取得・盗難	0.3	YES	NO
7	廃棄時における記憶媒体の取得・盗難	0.3	YES	NO
8	通信の盗聴	0.3	YES	NO
9	メンテナンス不備による故障	0.3	NO	YES
10	バックアップ電源の不備	0.1	NO	YES

今，I_1 の要素となる脅威要因 $\{1, 2, 3, 4, 5, 6, 7, 8\}$，および，$I_2$ の要素となる脅威要因 $\{1, 2, 3, 4, 5, 9, 10\}$ を，それぞれ I_{ki}（$k = 1, 2$，$i = 1, 2, \cdots, 10$）と表すこととする．I_{ki} の発生確率を P_{ki} とすると，I_{ki} が発生しない確率は $1 - P_{ki}$ であり，各々の要因集合 I_k（$k = 1$，2）に含まれるすべての脅威要因が発生しない確率は $\Pi(1 - P_{ki})$ となる．よって，I_1 または I_2 に対して，要因集合に含まれるいずれかの脅威要因が発生する確率，すなわち，脅威（情報漏洩またはサーバダウン）が発生する確率（PI_k）は $1 - \Pi(1 - P_{ki})$ である[⋆1]．

⋆1 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．

以上から，情報漏洩の発生確率（PI_1）とサーバダウンの発生確率（PI_2）を求めると，それぞれ 0.9706，0.9460 となる．なお，この時点での発生確率（PI_k）は，IS 対策なしのときの発生確率であることに留意されたい．

脅威が発生した場合には，販売業者は直接損失を被ることになるが，今回はやはり簡単化のために，情報漏洩（I_1）による直接損失は，個人情報流出による被害者への見舞金対策費用[⋆1]のみを，サーバダウン（I_2）による直接損失は，ネットショップ操業停止による逸失利益のみを考えることとする．

Yahoo! BB やアリコジャパンの漏洩事件では，被害者への謝罪として金券配布が行われた[25),26)]．Yahoo! BB の事件では，451 万人の全顧客に対して 500 円相当の見舞金（金券）を送付しており，これにインシデントに関する調査費用，対策室人員の人件費や謝罪広告掲載費用などの事後対応費用[23),24)] なども加わることによって，対策費は 40 億円にのぼっている．今回のケースでは，上記の例をもとに 40 億円を 451 万人で割ることによって，顧客 1 人あたりの見舞金対策費用を算出することとする．よって，組織が保有する個人情報の件数 X とすると，情報漏洩（I_1）による直接損失額 VA_1 は式 (13) のように計算される．

$$VA_1 = 887X \tag{13}$$

式 (13) を今回のケースに適用すると，情報漏洩による直接損失額 VA_1 は，ケース A においては 88,700 万円，ケース B においては 444 万円となる．

ネットショップ事業を行う組織としては，サーバダウンが発生することで操業停止に陥り，多大な逸失利益が発生する．IPA の被害調査[27)] によると，大手・中堅企業（従業員 300 人以上）の操業停止による年間売上減分の平均は約 7,253 万円であり，中小企業（従業員 300 人未満）の操業停止による年間売上減分の平均は約 1,546 万円であると報告されている．今回はこの損害額を採用し，サーバダウン（I_2）による直接損失額 VA_2 は，ケース A においては 7,253 万円，ケース B においては 1,546 万円とする．

情報漏洩（I_1）が起こった場合には，損害賠償係争にまで発展すると考えられる．今回のケーススタディでは，賠償額 VC_1 は，損害賠償を求める被害者（原告）の数と原告 1 人あたりに支払う賠償金との積によって算出することとする．宇治市の情報漏洩事件[6)] では 1 件あたり 10,000 円の賠償金を命じられており，今回はそれに倣うものとする．ただし，式 (13) に示した顧客 1 人あたりの見舞金対策費用のうち，500 円の見舞金はその時点ですでに顧客に支払われるため，その分を減じる．これに原告数 X を乗ずることにより，VC_1 は式 (14) のように計算できる．

$$VC_1 = 9500X \tag{14}$$

式 (14) を今回のケースに適用すると，賠償額 VC_1 は，ケース A においては 950,000 万円，ケース B においては 4,751 万円となる．

個人情報の漏洩（I_1）により引き起こされる損害賠償係争（L_1）の発生確率（PO_1）は，式 (11) で示したように，情報漏洩の発生確率（IS 対策なしのときは PI_1，IS 対策導入時は PI_1EI_1）と損害賠償係争に発展する割合（係争係数 α）の積である．JNSA の算出では，TBC の漏洩事件における漏洩件数（被害者数）と原告数（被害者のうちで訴訟に参加した数）の比率より，α を 0.0002 と計算している[4)]．このように，係争を「訴訟」に限定した場合，係争係数はかなり小さな値となるだろう．しかし，日経 BP が個人情報流出について 4773 人に実施したアンケートを見てみると，500〜1000 円の金券配布に関して計 94.9%が不満を持っていることが分かる[28)]．また，係争の種類としては，訴訟だけでなく示談や和解も考えられ，訴訟に至るケースは非常に少ないことを考慮しなくてはならない．たとえば，交通事故における損害賠償はその 95%が示談により解決しており[29)]，また，日本 IBM が神奈川県立高校の生徒の個人情報を流出させた事件のように賠償金を支払っているが訴訟は行われていない[30)] ケースも存在する．以上より，損害の発生によって何らかの賠償が発生することはむしろ必至であると考えられる．よって今回は，係争係数 $\alpha = 1.0$ として計算するものとした．

今回のケーススタディでは，クラッキングを受けてネットショップサーバがダウンしてしまったが，幸い顧客の個人情報の漏洩は免れたという状況を想定する．しかし，顧客の心情としては，ネットショップのサーバがクラッキングされたということは当然ネットショップに預けてある個人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，すべての顧客が集団で賠償を求める可能性がある．これに対し，被告であるネットショップが原告である顧客の「サーバダウンによって情報が漏洩した」という主張に対して有効な抗弁をすることができない場合，原告の主張がそのまま事実認定され，損害賠償請求が容認されてしまうという事態にもなりうる[⋆2]．

⋆1 損害賠償とは，債務不履行をはじめとする不法行為など一定の事由に基づいて損害が生じた場合に，その損害を補填し，損害がなかったのと同じ状態にすることをいい，損害額は，債務不履行・不法行為と損害との相当因果関係の認められる範囲の損害を金銭で評価して算定されることになる．いわゆる見舞金は，こうした算定手続きを経ていないため，損害賠償とはなりえず，法的には贈与に該当するとされている[31)]．このため本論文では，見舞金を直接損失として扱う．

⋆2 わが国の裁判制度，とりわけ民事訴訟では弁論主義が徹底されている．その内容は，当事者が主張しない事実は裁判の基礎にしてはならない（第 1 原則），当事者間で争いのない事実はそのまま裁判の基礎にしなければならない（第 2 原則），当事者間で争いのある事実の認定は当事者が申し出た証拠によらなければならない（第 3 原則），の 3 原則である[32)]．この結果，裁判官の判断は当事者による主張立証の訴訟行為に拘束されるため，特に民事裁判においては，有効な抗弁がない場合は客観的な真実の究明とは独立に事実認定されて判決が下されることにつながりうる．

表 4　脅威要因と IS 対策効果の関係（抜粋）
Table 4　Relation between incident's factors and IS countermeasures.

	セキュリティポリシーの設置	監査組織の設置	…	検査ソフトによるサーバの定期診断	インシデントレスポンスチームの設置
権限者による不正（漏洩・改竄・破壊・持ち出し）	0.8	0.5	…	0.1	0
:	:	:	…	:	:
計算機の不正使用（外部ネットワークからの侵入）	0	0	…	0.3	0
:	:	:	…	:	:
バックアップ電源の不備	0	0	…	0	0
対策コスト	20 万円	500 万円	…	200 万円	2,000 万円

4.1.2　対 策 効 果

組織がと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_1，I_2）に備える IS 対策，損害賠償（L_1）に備える DF 対策が存在する．

IS 対策においては，表 3 の脅威要因のそれぞれに対して，その発生確率を低減させる対策（それが外部からの攻撃である場合には，その攻撃の成功確率を低減させる対策も含む）を列挙するとともに，その対策効果（発生確率または攻撃成功確率をどれほど低減させることができるか）と導入コストを評価する．IS 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，アクセス制御などがあげられる．今回は，既存研究[1)] で使用された 18 種の IS 対策を候補として用いるものとした．**表 4** に脅威要因に対する対策効果（E_{IS}）とコスト（C_{IS}）の関係（紙面の都合上，その抜粋）を示す．表 4 の縦軸が表 3 で列挙された各脅威要因，表 4 の横軸が 18 種の IS 対策である．縦軸と横軸の交点に記されている値が，それぞれの脅威要因に対する各 IS 対策の対策効果である．表 4 の最下行が各対策の導入コストである．

表 4 より，たとえば「セキュリティポリシの設置」という対策は，脅威要因のうちの「権限者による不正」の発生確率を 0.8 の割合だけ減少させることが読み取れる．表 3 より無対策時の「権限者による不正」の発生確率は 0.5 であるため，「セキュリティポリシの設置」の対策のみが採用された場合，権限者による不正の発生確率は 0.5 から 0.1 となる．この結果，たとえば情報漏洩（I_1）の発生確率（PI_1）は 0.9706 から 0.9471 となる．同様に，たとえば「セキュリティポリシの設置」と「検査ソフトによるサーバの定期診断」が併用された場合，「権限者による不正」の発生確率が 0.09 となり，「計算機の不正使用（外部ネットワークからの侵入）」の発生確率は 0.3 から 0.21 になるため，情報漏洩の発生確率は $PI_1 = 0.9395$ となる．しかし，それに応じた対策コストとして，「セキュリティポリシの設置」を導入した場合は 20 万円，これに加え「検査ソフトによるサーバの定期診断」を併用した場合は計 220 万円が必要となる．

一方，DF 対策においては，損害賠償係争に関する証拠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．また，たとえログに要証事実に関する記載があったとしても，そのログがだれ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．このため，そのログの証明力を保つためのタイムスタンプやヒステリシス署名なども DF 対策としてあげられる．今回の DF 対策は，複数の市販製品の機能と価格の調査を通じ，ログ収集・解析システムの利用，電子署名の採用，ヒステリシス署名の採用，ログの外部保管（第三者委託），ログデータの暗号化，ログへのタイムスタンプの付与，NTP（Network Time Protocol）の採用によるサーバにおける正確な時刻の把握，ログの WORM（write once read many）装置での保管，の 8 種の DF 対策を候補として用いることとした．

2.2 節で述べたように，文献 22) ではログを証拠として利用するにあたってログが具備すべき 13 の要件がまとめられており（表 1），文献 22) ではこれら 13 要件の充足率という形で DF 対策の対策効果（E_{DF}）が表現されている．今回のケースタディでもこれに倣い，候補となっている全 DF 対策の各々に対して，13 要件のそれぞれの観点からの充足率を算出し，そこから DF 対策の対策効果（E_{DF}）および DF 対策採用時の敗訴確率（PL_k）を計算する．

今回の 8 種の各 DF 対策に対して，13 要件のそれぞれの充足率とコスト（C_{DF}）をまとめたもの（紙面の都合上，その抜粋）を**表 5** に示す．表 5 の横軸が 8 種の DF 対策，縦軸が表 1 であげられている 13 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．

本論文では，DF 無対策時の敗訴確率を 1.0 としている．表 5 より，たとえば「ログ収集・解析システムの利用」における要件 1，要件 2，要件 11 の充足率はそれぞれ 1.0，0.8，0 であることが分かる．これは，この対策を採用することで，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．

表 5　DF 対策の要件と対策効果の関係（抜粋）
Table 5　Relation between requirements for log and DF countermeasures.

	ログ収集・解析	電子署名	…	NTP（Network Time Protocol）	WORM（Write Once Read Many）装置
要件 1	1	0	…	0	0
要件 2	0.8	0	…	0	0
:	:	:	…	:	:
要件 11	0	0	…	0.8	0.6
要件 12	1	1	…	1	1
要件 13	0.8	0	…	0	0
対策コスト	200 万円	75 万円	…	80 万円	500 万円

要件 11 の充足率には寄与しないため，要件 11 の不備のために敗訴する確率は 1.0 のままである．一方，表 5 より「ログの WORM 装置での保管」は要件 11 の充足率が 0.6，NTP は要件 11 の充足率が 0.8 であることが分かる．ここで，WORM および NTP を併用した場合，要件 11 には両方の対策が寄与するが，今回は対策併用時の充足率は各対策の充足率のうちの最大値であると考えるものとする．すなわち，WORM と NTP を併用した場合の要件 11 の充足率は 0.8 である．

説明を簡単にするため，要件 1，2，11，12，13 に対する充足率が 0.0 であり，要件 3〜10 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，たとえば，「対策 X」，「ログ収集・解析システムの利用」，「電子署名の採用」，「ログの WORM 装置での保管」の 4 つの対策を採用（併用）した場合の充足率は，要件 1 が 1.0，要件 2 が 0.8，要件 3〜10 が 1.0，要件 11 が 0.6，要件 12 が 1.0，要件 13 が 0.8 となる．セキュリティにおいては一番脆弱な点がウィークポイントとなるため，今回は，13 の要件に対するそれぞれ充足率の中で値が一番低い充足率を「採用されている DF 対策全体の対策効果（EDF）」と見なす．よって，上記の例における対策効果は，要件 11 の充足率 0.6 と計算される．すなわち，敗訴確率（PL_k）は 0.4 となる．このときの必要なコストは，採用された 4 つの対策の対策コストの和 430 万円である．

4.1.3　最適解の導出

ケース A，ケース B において，式 (6)，(8)，(12) の離散最適化問題に表 2〜5 の緒元を代入し，最適な IS 対策，DF 対策を計算した結果を**表 6** に示す．

ケース A においては，無対策時に約 102 億円と見積もられた正味損失期待値が，計 5,737 万円の IS 対策および DF 対策の導入により約 9 億円の損失にまで抑えられるという結果となった．比較のため，DF 対策を想定せず，IS 対策しか存在しないと仮定した状態で離散最適化問題を解いた場合は，6,237 万円の IS 対策によって約 30 億円の損失に減少するという結果であった．よって，IS 対策だけでなく，DF 対策を適切に併用することで効果的にリスクヘッジが可能であることが確かめられた．ケース B においても，同様の結果が得られている．

表 6　ケース 1 の対策選定結果（単位：万円）
Table 6　Countermeasure selection in case study 1.

		ケース A	ケース B
損失額（Loss）	無対策時	1,015,010	6,504
	IS 対策導入時	298,224	3,221
	IS・DF 対策導入時	81,987	2,004
対策コスト（Cost）	無対策時	0	0
	IS 対策導入時	6,237	1,342
	IS・DF 対策導入時	5,737	737
正味損失期待値（Loss＋Cost）	無対策時	1,015,010	6,504
	IS 対策導入時	304,461	4,563
	IS・DF 対策導入時	87,724	2,741

なお，今回はあくまでも，クラッキングによってサーバはダウンしたが顧客の個人情報の漏洩はなかったという事態に対するケーススタディであることに注意されたい．実際に個人情報も漏洩してしまった場合には，サーバダウンという組織側の過失によって情報を漏洩させてしまった以上，いかなる DF 対策を施していようとも，原告である顧客の主張がそのまま事実認定され，賠償に応じなければならなくなる可能性が大きい．

4.2　ケース 2：組織内の機密情報を盗んだ犯人に賠償請求する

4.2.1　想 定 対 象

本ケースでは，機密情報を保持する製造業者が不正者（たとえば内部犯）に情報を盗まれた際に，ログなどを手がかりに犯人を特定してその人物に損害賠償を請求する場合を想定する．機密情報の保有件数により組織を分類し，ケース C）多国籍企業などの大手製造業者，ケース D）町工場などの中小製造業者，として検討を行う．**表 7** にその緒元を示した．

簡単のため，本ケースにおける資産は機密情報のみを，脅威は情報漏洩（情報の盗難）のみを想定することとし，また，その脅威を引き起こす原因やそれに対抗するための IS 対策の候補についてはケース 1 と同じであるとした．今回の機密情報の価値は 1 件あたりの単

表 7　想定対象（ケース 2）
Table 7　Case study 2.

ケース	ケース C	ケース D
組織	大手製造業者 （多国籍企業など）	中小製造業者 （町工場など）
機密情報の保有件数	1,000 件	100 件
資産番号（k）	1	1
資産の名称	機密情報 （設計図面データ）	機密情報 （設計図面データ）
資産に対する脅威（I_k）	情報漏洩	情報漏洩
脅威発生時の 直接損失額（VA_k）	50,000 万円	5,000 万円
資産損失により発生する損害賠償係争（L_k）	知的財産侵害 に対する損害賠償	知的財産侵害 に対する損害賠償
損害賠償係争における 償請額（VC_k）	-50,000 万円	-5,000 万円
損害賠償係争に発展する確率（係争係数 α）	0.5	

価を一律 50 万円と仮定した．機密情報を保存しているストレージに不正アクセスされることによって，単価 × 保有件数に相当する直接損失（VA_k）が発生する．

本ケースにおける損害賠償係争は，組織の損失を補填するために犯人への損害賠償請求である．賠償請求の目的は，損失 VA_k を賠償金の取得により回復することであるため，賠償額 VC_k は直接損失額 VA_k と同値とした．ただし，3.2 節で述べたように，組織が他者に損害賠償請求を求める場合であるので賠償金額は負の数値として考える．係争係数 α は，犯人が特定できたとしても雲隠れしてしまっている場合には犯人に賠償請求ができないという点を考慮して，0.5 と想定した．また，不正アクセスのログが正しく取得・保管されていなければ，係争を起こしたとしても犯人にシラを切られる可能性がある．これに対抗するため対策が DF 対策となるが，その候補についてはケース 1 と同じであるとした．

4.2.2　最適解の導出

ケース C，ケース D において，式 (6)，(8)，(12) の離散最適化問題に表 7 および表 3〜5 の緒元を代入し，最適な IS 対策，DF 対策を計算した結果を**表 8** に示す．

ケース C においては，無対策時に約 4.9 億円と見積もられた正味損失期待値が，計 3,537 万円の IS 対策および DF 対策の導入により約 1.3 億円の損失にまで抑えられるという結果となった．比較のため，DF 対策を想定せず，IS 対策しか存在しないと仮定した状態で離散

表 8　ケース 2 の対策選定結果（単位：万円）
Table 8　Countermeasure selection in case study 2.

		ケース C	ケース D
損失額 （Loss）	無対策時	48,529	4,852
	IS 対策導入時	15,336	2,295
	IS・DF 対策導入時	9,201	2,242
対策コスト （Cost）	無対策時	0	0
	IS 対策導入時	3,142	1,342
	IS・DF 対策導入時	3,537	717
正味損失 期待値 （Loss＋Cost）	無対策時	48,529	4,852
	IS 対策導入時	18,478	3,637
	IS・DF 対策導入時	12,738	2,959

最適化問題を解いた場合は，3,142 万円の IS 対策によって約 1.8 億円の損失に減少するという結果であった．よって，IS 対策だけでなく，DF 対策を適切に併用することで効果的にリスクヘッジが可能であることが確かめられた．ケース D においても，同様の結果が得られている．

5. おわりに

本論文では，IS 対策および 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．

今回は情報漏洩による損害賠償に焦点をあて，組織が訴えられる場合と訴える場合のいずれの立場においても提案方式を用いることで費用対効果の高い対策を選ぶことができることを示した．しかし，係争係数 α の扱いについてはまだ課題が残る．本論文では α を 1.0 として用いているが，実際には適切な α の値はケースバイケースであると考えられるため，広く調査を行う必要があるだろう．また，示談における損失と訴訟に発展した際の損失の違いも考慮しなければならない．これは，訴訟に発展することで弁護士費用などの訴訟費用だけでなく，逸失利益や企業イメージの低下が発生し，示談による解決よりも多くの損失を被ると考えられるためである．そこで，係争係数 α を示談や訴訟になる確率に分けて考え，各ケースにおける損失額を導出することで，より現実に即した対策が選定できると考えられる．

また，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についても検討し，提案方式の適用可能範囲を確かめる必要がある．組織ごとに異なる固有の状況による対策選

定結果の違いを検討することが本研究のケーススタディの最終的な目的である．本論文では，組織が所有する個人情報の規模（被害規模）の違いに主眼をおいてケーススタディを実施したが，将来的には他の各種パラメータについても変化させて感度分析を行いたい．

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) 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝：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, No.8, pp.2022–2033 (2004).
2) 永井康彦，藤山達也，佐々木良一：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, No.8, pp.2264–2271 (2000).
3) 西　真弓，山田辰也，小田原育也：セキュア SI と流通ソリューションへの適用，東芝レビュー，Vol.62, No.7, pp.7–10 (2007).
4) 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
5) 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
6) 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
7) Bojanc, R. and Jerman-Blazic, B.: An economic modeling approach to information security risk management, *International Journal of Information Management*, Vol.28, Issue 5, pp.413–422 (2008).
8) Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. Information and System Security*, Vol.5, No.4, pp.438–457 (2002).
9) 松浦幹太：情報セキュリティと経済学，2003 年暗号と情報セキュリティシンポジウム（SCIS2003）予稿集，Vol.1, pp.475–480 (2003).
10) Tatsumi, K. and Goto, M.: Optimal timing of information security investment: A real options approach, *The 8th Workshop on the Economics of Information Security* (*WEIS 2009*). (see http://weis09.infosecon.net/programme.html)
11) 石黒正輝，村瀬一郎，松浦幹太，田中秀幸：情報セキュリティ対策による企業価値向上の影響分析，2009 年暗号と情報セキュリティシンポジウム予稿集，2D1-3 (2009.1).
12) 佐々木良一，吉浦　裕，伊藤信治：不正コピー対策の最適組合わせに関する考察，情報処理学会論文誌，Vol.43, No.8, pp.2435–2446 (2002).
13) 佐々木良一，石井真之，日高　悠，矢島敬士，吉浦　裕，村山優子：多重リスクコミュニケータの開発構想と試適用，情報処理学会論文誌，Vol.46, No.8, pp.2120–2180 (2005).
14) 榊　啓，矢野尾一男，小川隆一：多目的最適化によるセキュリティ対策立案方式の提案，2007 年コンピュータセキュリティシンポジウム（CSS2007）論文集，pp.193–198 (2007.10).
15) 加藤弘一，勅使河原可海：利便性とセキュリティを両立させるための最適対策組合せに関する検討，DICOMO2007 論文集，pp.1578–1585 (2007.7).
16) 大谷尚通：不正アクセス行為の状態遷移モデルに基づくセキュリティ脅威と対策作成方法，2007 年コンピュータセキュリティシンポジウム（CSS2007）論文集，pp.283–288 (2007.10).
17) 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.1523–1530 (2008.7).
18) 福田洋治，溝渕昭二，毛利公美，白石善明，野口亮司：ネットワークフォレンジックのためのホスト型のロギングについて，2009 年電子情報通信学会総合大会発表論文集，AS-1-3 (2009.3).
19) 辻井重男（監修），特定非営利活動法人デジタル・フォレンジック研究会：デジタル・フォレンジック事典，pp.2–18, 日科技連出版社 (2006).
20) McKemmish, R.: When is digital evidence forensically sound?, *Research advances in digital forensics IV*, pp.3–15, Springer (2008).
21) 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，4E1-6 (2008.1).
22) 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).
23) JNSA：2007 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/2007/pol/incident/index.html
24) 日本経済新聞：臨時もの料金表. http://www.nikkei-ad.com/paper/ad/ad_chart02_a.html
25) CNET JAPAN：ソフトバンク BB 孫社長が顧客情報流出で謝罪，データ流出は約 451 万人分．http://japan.cnet.com/news/media/story/0,2000056023,20064584,00.htm
26) MSN 産経ニュース：顧客情報流出でアリコジャパンが 1 人一万円の商品券. http://sankei.jp.msn.com/economy/finance/091006/fnc0910061657016-n1.htm
27) IPA：2005 年企業における情報セキュリティ事象被害額調査. http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html
28) Nikkei BP：個人情報流出時に望まれるのは「金券」より「情報開示」. http://www.nikkeibp.co.jp/archives/331/331093.html
29) 弁護士事務所ドットコム：交通事故解決までの流れ. http://www.bengoshijimusho.com/kotuflow/
30) 日本個人情報保護協会：神奈川県立高の情報流出，日本 IBM が賠償. http://jpdpa.jp/news/523
31) 松田政行，三好秀和（監修），IT 企業法務研究所，IT 知財と法務編集委員会（編著）：IT 知財と法務，p.516, 日刊工業新聞社 (2004).

32) 小林秀之：新証拠法第 2 版，p.14, p.48, p.220, 弘文堂 (2003).

(平成 22 年 5 月 21 日受付)
(平成 22 年 12 月 1 日採録)

西垣　正勝（正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授．2007 年同准教授，2010 年同教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．

臼井　佑真

2008 年静岡大学情報学部情報科学科卒業．2010 年同大学大学院修士課程修了．同年 NEC ソフト株式会社入社．在学中，情報セキュリティに関する研究に従事．

山本　　匠（正会員）

2006 年静岡大学情報学部情報科学科卒業．2007 年 9 月同大学大学院修士課程修了．2010 年 9 月同創造科学技術大学院博士課程修了．日本学術振興会特別研究員（DC1）を経て，現在，同研究員（PD）．博士（情報学）．情報セキュリティに関する研究に従事．

間形　文彦（正会員）

1992 年中央大学法学部法律学科卒業．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所に所属．社会科学と情報工学の境界領域から情報セキュリティの研究に従事．日本セキュリティ・マネジメント学会，情報ネットワーク法学会各会員．技術士（情報工学）．

勅使河原可海（フェロー）

1970 年東京工業大学大学院理工学研究科制御工学専攻修了．工学博士．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1994〜1996 年ハワイ大学アロハシステム客員研究員．1995 年創価大学工学部教授，工学部長，工学研究科長を歴任．ユビキタスコンピューティング，グループウェア，e-learning，ネットワークセキュリティ等の研究に従事，情報処理学会，オペレーションズリサーチ学会各フェロー，電子情報通信学会，経営情報学会，IEEE，ACM 各会員．

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所でシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2007 年総務大臣表彰（情報セキュリティ促進部門）．2007 年度「情報セキュリティの日」功労者表彰．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『IT リスクの考え方』（岩波新書，2008 年）等．日本セキュリティ・マネージメント学会会長，日本学術会議連携会員，内閣官房情報セキュリティ補佐官．