Vol.2009-GN-72 No.11
2009/5/21

情報処理学会研究報告
IPSJ SIG Technical Report

仕事量及び利便性低下度に着目したセキュリティ対策選定手法

芝口誠仁[†1] 稲場太郎[†1]
中山佑輝[†1] 岡田謙一[†2]

近年では企業は情報セキュリティ対策に力を入れるようになってきている．しかしセキュリティとコストの間にはトレードオフの問題があり，適切なセキュリティ対策選定手法が必要である．そこで本稿では仕事量を考慮したセキュリティ対策選定手法を提案する．本手法は，就業者に対する脅威，採用可能な対策を分析し，各対策に徹底度を付与する．そして一定期間ごとに就業者の仕事量を評価し，その仕事量と徹底度をもとにその期間に採るべき対策を決定する手法である．ケーススタディによる評価の結果，単位時間当たりの残業コストが比較的高く，仕事量が一定でないような企業の場合，対策固定のときと比較して 10% 以上も期待支出を削減できることが示された．

Security Countermeasure Optimization Considering Work Volume

Seiji Shibaguchi,[†1] Taro Inaba,[†1] Yuki Nakayama[†1]
and Kenichi Okada[†2]

In recent years, companies are strengthening information security. Since information security costs a lot, it isn't always good for companies to bolster security level. In this paper, I propose security countermeasure optimization considering work volume. This method gives each countermeasure priority, which indicates when the countermeasure is used. If a countermeasure has low priority, it is used only when the employee has little work while he always has to use countermeasures which have high priority. I conducted a case study to confirm the effectiveness of my method. As a result, my method contributes to reducing cost in the companies which don't have certain fixed work time or which have to pay a lot for overtime allowances. Such companies can reduce the expense for information security with my method.

1. はじめに

近年では情報漏洩が問題となってきており，企業は情報セキュリティ対策に力を入れるようになってきた．しかしながら，情報セキュリティ対策には常にコストが伴うものであり，強化すればするほどよいものではない．

そこで必要となってくるのが最適なセキュリティ対策の選定手法である．しかしながら従来研究では利便性の低下は往々にしてコストに含まれて計算されており，これにフォーカスを当てた研究は少ない．また，利便性の低下コストに注目した場合，そのコストは仕事が忙しい時期とそうでない時期で大きく値が異なるはずであるが，これまで研究されてきた手法は対策選定に「仕事量」を考慮しているものは存在していなかった．

そこで本研究では，特に利便性低下コストと仕事量に注目したセキュリティ対策選定手法を提案する．本手法は，数式モデルを用いてコストと効果のバランスを定量的にとりながら対策を決定する．これは忙しい時期は利益を上げるために多少セキュリティ強度を緩めてでも利便性を向上させて速く仕事を行えるようにし，逆に閑散期では仕事速度を犠牲にしてセキュリティを強化して損失の発生を防ぐ，という観点に立ったものである．以下の本稿の構成は次のようになっている．まず 2 章で関連研究について述べ，3 章で仕事量を考慮したセキュリティ対策選定手法を提案し，4 章でケーススタディによる評価について述べる．そして 5 章で結論を述べて本稿のまとめとする．

2. 関連研究

セキュリティ対策の最適組み合わせに関する研究としては，中村らが提案した，資産，脅威，対策の関係のモデル化から，最も効果的なセキュリティ対策を選択する手法がある[1)]．この手法では，数ある資産と脅威，脅威と対策の関係を総当り的に評価することで相

†1 慶應義塾大学理工学研究科
Graduate School of Science and Technology, Keio University
†2 慶應義塾大学理工学部, 独立行政法人科学技術振興機構
Faculty of Science and Technology, Keio University, JST

互の関係を定量化している．

続いてユーザの利便性を考慮した対策選定手法として，加藤らは，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のための交渉方式を提案している[2]．この方式は，ユーザが求める利便性と管理者が求めるセキュリティレベルの両立を図るための交渉方式である．この提案では利便性はユーザが求め，セキュリティレベルは管理者が求めるという立場をとっている．そのため，交渉結果は両者の主観が交わった最適組合せということになる．しかしながら，本来の最適組合せとは客観的な視点での最適解であるべきである．したがって，この提案は利便性を考慮した最適組合せ選定手法とはいえない．利便性を客観的に評価した対策選定モデルの研究は行われていないのが現状である．

3. 仕事量を考慮したセキュリティ対策選定手法

3.1 提 案 概 要

本提案手法は，企業を対象とし，数式モデルを用いてコストと効果のバランスを定量的にとりながら適切なその就業者がとるべき対策の選定，運用を行うことを目的としている．セキュリティ対策選定に際しては，効果，利便性低下コスト，その他コストから各対策候補に 5 段階の「徹底度」を付与する．運用の際は定期的に対象従業員の仕事量を評価し，その仕事量と対策徹底度に応じてその期間に採るべき対策を決定する．本提案手法の流れは以下のようになる．

(1) リスク分析の実施
(2) セキュリティ対策分析の実施
(3) セキュリティ対策徹底度の決定
(4) セキュリティ対策徹底度の運用

これらの各フェーズについて以下の節で詳述する．

3.2 リスク分析

本提案手法において実行されるリスク分析の対象は，企業における就業者とし，就業者 1 名単位でフォールトツリー法によるリスク分析を行う[3]．具体的な分析手順は以下の通りとなる．

(1) 発生しうる脅威の列挙と被害額の推定
(2) 各脅威を頂上事象とするフォールトツリーの作成
(3) 各基本事象に対する発生確率の設定

それぞれについて以下で詳説する．

3.2.1 脅威の列挙と被害額の推定

このフェーズでは，就業者に対して起こりうるセキュリティインシデント（脅威）を挙げ，それによる推定被害額を設定する．ここでは想定しうる脅威を漏れなく被りなく挙げなくてはならない．

3.2.2 フォールトツリーの作成

脅威を列挙したら，その各脅威を頂上事象とするフォールトツリーの作成を行う．フォールトツリーとは，頂上に好ましくない事象を配置し，その事象を AND/OR のゲートを用いて分解していく分析手法である．その結果，頂上事象の発生は全て基本事象の和と積で表すことができ，基本事象に発生確率を与えることで頂上事象の発生確率の計算ができるようになる．図 1 に「紛失による情報漏洩」を頂上事象とした場合のフォールトツリー分析の例を示す．またこのカットセットは，冗長なものが含まれている場合があり，それらを取り除く必要がある．冗長なものを抜いた必要最小限の事象の集合のことをミニマルカットセットという[3]．

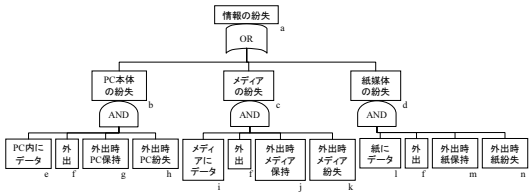

図 1 紛失による情報漏洩の分析例
Fig. 1 An example of analysis of information leakage

3.2.3 各基本事象発生確率の設定

図 1 のように脅威に対しフォールトツリー解析を行うと，脅威は全て基本事象で表すことが可能となる．脅威自体に発生確率を当てはめるのは困難であるが，基本事象ならば比較的容易に発生確率を推定することができる．

3.3 対 策 分 析

リスク分析が終了したら，それぞれの脅威の発生を抑えるための対策について考える必要がある．ここでは各対策候補のコストと効果を設定する．

3.3.1 コストの設定

本提案手法ではコストは利便性低下度と，その他コストの 2 種類に分類して考える．

利便性低下度とはその対策を採用することによって就業者の利便性がどれほど低下するかを表したもので，0 から 1 までの値で表される．ここで言う利便性の低下とは，同じ仕事を行う際の仕事速度がどれだけ低下するかを示すものであり，通常 T_{before} 時間で終わる仕事がある対策を実施した際に T_{after} 時間かかるとすると，その際の利便性低下度 DU は以下の通りとなる．

$$DU = 1 - \frac{T_{before}}{T_{after}} \quad (1)$$

その他コストは，利便性低下以外の全てのコストを表す．コストには大きく初期導入コストと維持コストが考えられるが，脅威の発生確率と同様，就業者 1 人，1 日当たりの値に換算して表すこととし，初期導入コストが C_{first} 円，継続期間が T 日，維持コストが C_{day} 円/日であった場合，1 日あたりコスト C は，以下の式で表わされる．

$$C = C_{first} \div T + C_{day} \quad (2)$$

3.3.2 効果の設定

各対策の効果は，リスク分析を行った際に分解された各基本事象の発生確率をどれだけ減じるかという値で表される．たとえば発生確率が P_{before} の基本事象が，ある対策を施すことによって P_{after} になったとする．するとこの対策のこの基本事象に対する効果 E は，

$$E = \frac{P_{before} - P_{after}}{P_{before}} \tag{3}$$

と算出される．逆に，ある対策を施すことによって基本事象の発生確率が増加する場合，この効果はマイナスの値で表す．

3.4 対策徹底度の決定と運用

リスク，対策の分析が行われたら，各対策に徹底度と呼ばれる値を割り当てる．徹底度とは，その対策がどの程度徹底的に実施されるべきかを表す値で，5 段階で設定される．この決定は，各仕事量における最適対策組合せの算出を行い，それを元に徹底度を割り当てる，という手順で行われる．

3.4.1 各仕事量における最適対策組合せの算出

このフェーズでは，各仕事量ごとに最適な対策の組合せを考える．仕事量とは，就業者が 1 日当たりにこなさなければならない仕事の量のことで，本研究においてはその仕事にかかる時間で量を評価する．

最適な対策の組合せは，企業の期待支出を最小化する対策の組合せとする．本研究では企業の期待支出を「脅威の発生による損害の期待値」「セキュリティ対策の利便性低下によるコスト」「セキュリティ対策にかかるコスト」の 3 つの値の合計とする．

3.4.2 最適組合せ算出式

最適な対策組合せは，期待支出を最小化する対策の組合せである．ここで T_k は脅威として ID を下付きの k で表すものとする．企業の期待支出 L は脅威の発生による損害の期待値 D とセキュリティ対策にかかるコスト TC とセキュリティ対策における利便性低下コスト OC の和で以下のように表せる．

$$L = D + TC + OC \tag{4}$$

ここで，損害期待値 D は脅威 T_k の発生確率 PT_k と 1 回当たりの被害額 DT_k の積の総和で表せる．

$$D = \sum_k PT_k \times DT_k \tag{5}$$

PT_k はリスク分析をした結果のミニマルカットセットを用いて算出される．リスク分析で用いた手法を一般式化すると次のようになる．ここで，PMC_{km} は脅威 T_k のミニマルカットセット m の発生確率である．

$$PT_k = 1 - \prod_m (1 - PMC_{km}) \tag{6}$$

また，基本事象 B_j の発生確率を PB_j とする．このとき各対策 M_i の B_j に対する効果 E_{ij} を考慮した基本事象の発生確率を PBA_j とすると以下のようになる．

$$PBA_j = PB_j \times \prod_i (1 - E_{ij} AF_i) \tag{7}$$

AF_i は，対策を採用するかのフラグであり，採用するならば値は 1，採用しないならば値は 0 となる．よって，PMC_{km} は，ミニマルカットに含まれる全ての事象を考慮するので，脅威 T_k のミニマルカットセット m に基本事象 B_j が含まれているかのフラグを F_{jkm}（含まれている：1，含まれていない：0）として，以下のように表わされる．

$$PMC_{km} = \prod_j (1 - PBA_j \times F_{jkm}) \tag{8}$$

1 日あたりコストは対策 M_i にかかるコスト C_i とその対策を採用するかのフラグの積の総和で決まるので次のように表せる．

$$TC = \sum_i (C_i \times AF_i) \tag{9}$$

利便性低下によるコスト，すなわち残業コスト OC は，定時の就業時間 NWT を超えた分にかかってくると考えられるので，以下のように算出される．

$$OC = (WT - NWT) \times OH \tag{10}$$

ここで，仕事時間 WT は，仕事量 WA と採用する対策の利便性以下度から以下のように表される．ここで，DU_i は対策 M_i を採用することによる利便性低下度である．

$$WT = WA \div \prod_i (1 - DU_i \times AF_i) \tag{11}$$

最適対策組合せを求めるには，(4) 式を最小化する対策の組合せを求めればよいこととなる．これは (4) 式を最小化する AF_i の組合せを求める離散最適化問題を解くことと等価である．

3.4.3 徹底度の割り当て

このフェーズではまず，仕事量が十分少ない場合から十分多い場合を想定し，それぞれの場合での最適な対策組合せを前述の方法で求める．すると，表 1 のような表が出来上がる．なお，表中の仕事量は 8 を標準仕事量とし，仕事量が 1 から 15 の場合について最適な対策組合せを求めたものである．また，各対策の○は最適組合せにおいて採用することを表し，×は採用しないことを表す．

本研究においては，仕事量が多くなればなるほどセキュリティ対策は最小限にとどめて利便性を重視するという考えなので，仕事量が少ない場合には採用したほうがよい対策の中には，仕事量が多くなることによって採用しなくなる場合がある．そこで，表 1 における各対策の採用から不採用となる閾値に注目し，その閾値によって徹底度を決定する．閾値 k は，値 k では採用するが，$k+1$ では採用しなくなる値とする．このように定義すると表 1 の対策 3 の閾値は 7 となり，対策 5 の閾値は 0 となる．このとき，例として閾値である仕事量が 3 以下の場合徹底度 1，4 以上かつ 7 以

表 1 各仕事量における最適対策組合せ例
Table 1 An example of the best combination in each work volume

仕事量	対策採用フラグ					
	対策 1	対策 2	対策 3	対策 4	対策 5	…
1	○	○	○	○	×	…
2	○	○	○	○	×	…
3	○	○	○	○	×	…
4	○	○	○	×	×	…
5	○	○	○	×	×	…
6	○	○	○	×	×	…
7	○	○	○	×	×	…
8	○	○	×	×	×	…
9	○	○	×	×	×	…
10	○	○	×	×	×	…
11	○	×	×	×	×	…
12	○	×	×	×	×	…
13	○	×	×	×	×	…
14	○	×	×	×	×	…
15	○	×	×	×	×	…

下の場合徹底度 2，8 以上かつ 10 以下の場合徹底度 3，11 以上かつ 13 以下の場合徹底度 4，それ以上の場合を徹底度 5 とする．すると，対策 1 は徹底度 5 であり，対策 2 は徹底度 3 と各対策に徹底度が割り当てられる．その結果，表 2 のような表が完成する．運用の際はこの表を用いて採用すべき対策の決定を行う．

表 2 対策候補例
Table 2 An example of security countermeasure

徹底度	採用仕事量	対策
1	常に不採用	NET 接続禁止
2	5 以下	シンクライアントの利用
3	8 以下	可搬メディア使用禁止
4	11 以下	情報の印刷禁止
5	常に採用	ウイルス対策ソフトの導入

3.4.4 対策の運用

対策徹底度の運用フェーズでは，就業者の一定期間の仕事量を評価し，その仕事量に応じた対策を採用する．先ほど述べた手法により，各徹底度に対策候補が割り当てられている表ができる．いま，表 2 のような割り当てがなされていると考える．

この割り当て表を用いて一定期間ごとに採用対策の決定を行う．たとえば，ある就業者が 10 日間で 120 時間分の仕事をこなさなければならないとする．すると 1 日当たりの仕事量は 12 であるから，この就業者は徹底度 5 の対策であるウイルスソフトの導入のみを行えばよいことになる．しかし，次の 20 日間での仕事量は 100 時間分であったとすると，1 日当たりの仕事量は 5 となり，徹底度 2 以上の対策は全て採用しなければならない．このように一定期間ごとの仕事量に応じて採用すべき対策を変更していくことで，企業の支出期待値を最小化することを図る．

4. ケーススタディによる評価

仕事量に応じて動的に対策を採用することによる効果を確かめるため，そして本提案手法がより効果を発揮する場合を確かめるためにケーススタディによる評価を行った．

4.1 評価方法

4.1.1 評価概要

想定したケースは，1 就業者の在宅勤務である．本評価では 500 日間の勤務を想定し，この間，徹底度と仕事量に応じて対策を変更していくことを考える．そして 500 日経過後の企業の期待支出を算出し，その大小によって評価を行う．

4.1.2 評価手順

以下の手順で評価を行った．

(1) 在宅勤務における脅威のリスク・対策分析
在宅勤務における脅威として 5 つを想定し，1 回当たりの被害額を設定した．表 3 にはミニマルカットセットを構成する基本事象を示し，表 4 には分析された脅威を示す．さらに各対策候補による利便性低下度，コスト，各基本事象への効果を与えた．その分析結果を表 5 に示す．

(2) 対策徹底度の設定
分析した脅威，対策をもとに，対策徹底度の決定を行った．定時就業時間 NWT は 8 時間，単位時間あたりの残業コスト OH は 5000 円として算出を行った．その結果，各徹底度に割り当てられた対策は表 6 のようになった．

(3) 各条件における期待支出額の算出
先述した徹底度と仕事量をもとに，対策を動的に変化させていき，500 日経過後の企業の期待支出を算出した．期待支出は (4) 式に示されるように，期待被害額とコストと残業コストの和で表されるものである．また，比較対象のために対策固定の場合（標準仕事量 8 における最適な対策組合せに準拠）についても 500 日間の期待支出額を算出した．

4.1.3 評価条件

以下に示す 2 通りの評価を行った．

(1) 仕事量の分布を変化させた場合
本評価で想定する 500 日間中の仕事量の分布の内訳はピーク値が 1 つと 2 つの場合で，ある平均値をもった正規分布として仕事量が分布している場合を想定した．本評価は，この 2 つの場合についてそれぞれピーク値を動かし，各条件における期待支出額の算出を行った．

(2) 単位時間当たり残業コストを変化させた場合
単位時間当たりの残業コストを変化させ，それぞれの条件で期待支出額の算出を行った．なお，仕事量のピークは 1 つ，平均仕事量 10 で評価を行った．また，単位時間当たり残業コストを変化させる度に，その都度最適な徹底度に変更して評価を行った．

表 3 脅威を構成する基本事象
Table 3 Basic events which construct threats

ID	基本事象	発生確率	ID	基本事象	発生確率
B_1	PC 内にデータ保存	0.9	B_{15}	外出時機密情報閲覧	0.5
B_2	外出	0.125	B_{16}	外部犯の盗み見企図	0.005
B_3	外出時 PC 保持	0.3	B_{17}	外出時に仕事の会話	0.4
B_4	外出時 PC 紛失	0.0001	B_{18}	外部犯の盗み聞き企図	0.005
B_5	メディア内にデータ保存	0.8	B_{19}	インターネットの使用	0.9
B_6	外出時メディア保持	0.5	B_{20}	ウイルスをダウンロードして実行	0.01
B_7	外出時メディア紛失	0.001	B_{21}	ウイルス対策ソフトが脆弱	0.5
B_8	紙媒体への印刷・筆記	0.8	B_{22}	外部からのワーム感染企図	0.01
B_9	外出時紙媒体保持	0.5	B_{23}	自宅で無線 LAN 使用	0.5
B_{10}	外出時紙媒体紛失	0.001	B_{24}	無線 LAN 暗号脆弱	0.5
B_{11}	自宅が脆弱	0.2	B_{25}	自宅への盗聴企図	0.001
B_{12}	外部犯の自宅盗難企図	0.001	B_{26}	経路上の暗号脆弱	0.5
B_{13}	外出時の盗難に対する脆弱	0.2	B_{27}	経路上盗聴企図	0.005
B_{14}	外部犯の外出時盗難企図	0.005			

表 4 分析した脅威
Table 4 Analyzed threats

脅威	被害額（円）	ミニマルカットセット
情報の紛失	10,000,000	$B_1B_2B_3B_4$，$B_2B_5B_6B_7$，$B_2B_8B_9B_{10}$
情報の盗難	15,000,000	$B_1B_{11}B_{12}$，$B_5B_{11}B_{12}$，$B_1B_2B_3B_{13}B_{14}$， $B_8B_{11}B_{12}$，$B_2B_5B_6B_{13}B_{14}$，$B_2B_8B_9B_{13}B_{14}$
盗み見・盗み聞き	5,000,000	$B_1B_2B_3B_{15}B_{16}$，$B_2B_3B_5B_6B_{15}B_{16}$， $B_2B_8B_9B_{15}B_{16}$，$B_2B_{17}B_{18}$
ウイルス・ワーム感染	10,000,000	$B_{19}B_{20}B_{21}$，$B_{19}B_{21}B_{22}$
ネットワーク上の盗聴	10,000,000	$B_{19}B_{23}B_{24}B_{25}$，$B_{19}B_{26}B_{27}$

表 5 分析した対策候補
Table 5 Analyzed countermeasures

ID	対策	利便性	コスト
M_1	シンクライアント	0.2	500
M_2	PC 保持制限	0.005	0
M_3	メディア使用制限	0.03	0
M_4	メディア保持制限	0.01	0
M_5	印刷・筆記制限	0.05	0
M_6	紙媒体保持制限	0.02	0
M_7	ホームセキュリティ	0	300
M_8	外出時情報閲覧制限	0.05	0
M_9	仕事会話制限	0.01	0
M_{10}	インターネット使用制限	0.8	0
M_{11}	ウイルスソフト強化	0.001	100
M_{12}	無線 LAN 使用制限	0.005	0
M_{13}	VPN 接続	0	0

表 6 各徹底度に割り当てられた対策
Table 6 Allocated countermeasures

徹底度	採用仕事量	対策
1	常に不採用	M_{10}
2	5 以下	M_3，M_5，M_8，M_{12}
3	8 以下	M_1
4	11 以下	M_6
5	常に採用	M_2，M_4，M_7，M_9，M_{11}，M_{13}

4.1.4 評価項目

評価項目としては以下の式で表される支出削減率（R）を使用した．

$$R = \frac{L_{fix} - L_{move}}{L_{fix}} \tag{12}$$

L_{fix}：対策固定の場合の期待支出額
L_{move}：動的対策の場合（本提案手法）の期待支出額

すなわち R は，対策固定の場合に対して動的に対策を採った場合にどれだけ支出が削減できたかを表す値である．この値を用いて本提案手法の有用性評価，また本提案手法が効果的な条件の評価を行った．

4.2 結果と考察

4.2.1 仕事量の分布を変化させた場合

仕事量のピークが 1 つのときの結果を図 2 に示す．図 2 において横軸はピークとなる仕事量を表し，縦軸は支出削減率 R を示す．この図から，平均仕事量が標準仕事量である 8 付近であるときは支出削減率が小さいのに対し，4 や 12 と離れるにつれて削減率が大きくなっていることがわかる．図 3 は仕事量のピークが 2 つの場合の結果である．この図の横軸は 2 つの仕事量ピークの位置を表しており，右に行くほどそのピークが標準仕事量である 8 からは遠ざかることになる．結果を見ると，右に行くにつれ，すなわち標準仕事量から遠ざかるにつれて支出削減率が大きくなっていることがわかる．

以上 2 つの結果より，本提案手法がより効果を発揮するのは仕事量が大きく変動する企業であるといえる．このような現状閑散期と繁忙期が大きく分かれるような企業であっても，その時期ごとに対策の変更を行っている企業はほとんど見受けられず，そういった企業でも平均の仕事量を考えて対策を決定するしかなかった．本提案手法で最大 10% 以上の期待支出削減が図れたことは，このような企業が対策を動的にすることで支出の削減ができると示せたこととなり，この点に

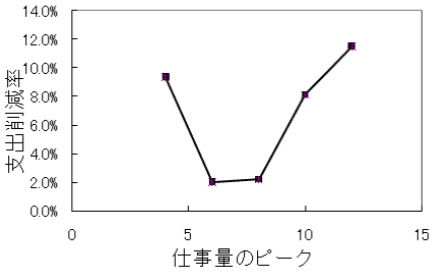

図 2 仕事量ピークが 1 つの場合の結果
Fig. 2 The result with one peak

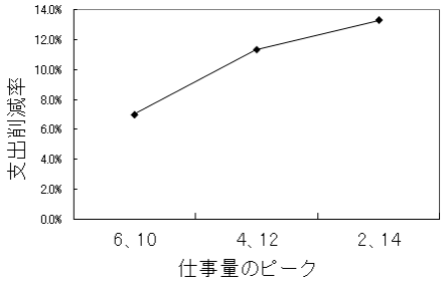

図 3 仕事量ピークが 2 つの場合の結果
Fig. 3 The result with two peak

大きな価値があると考える．

4.2.2 残業コストを変動させた場合

単位時間残業コストに対する結果を図 4 に示す．図 4 における横軸は単位時間当たり残業コストを表し，縦軸は支出削減率を示す．図を見ると，単位時間当たりの残業コストが 3000 円以下の場合は削減率は非常に小さいが，4000 円を超える場合は大きな値となっていることがわかる．本提案手法は，残業コストが小さい環境であれば仕事量の変化による残業代の増減が小さくなるため，対策固定の場合との変化が小さくなり，結果として支出削減率が低い値となる．

また，単位時間残業コストが大きい場合は削減率も大きくなっているのだが，6000 円を境に減少傾向があることも見て取れる．これは，あまりに単位時間当たり残業コストを大きくしすぎると，対策固定の場合と動的対策の場合での差が小さくなることに起因しているだろう．動的対策と対策固定の場合の差は当然，各対策の徹底度に依存する．本評価では徹底度が 5 のものは常に採用，1 のものは常に不採用としているため，徹底度が 2〜4 の対策が多ければ多いほど動的の場合と固定の場合との差が大きいことになる．しかしながら，単位時間当たりの残業コストが非常に大きくなった場合，対策固定の場合でも利便性が特に重視されることになり，対策を採用しない，すなわち徹底度 1 の対策が増えてくる．すると，動的の場合との差がなくなり，削減率が小さくなってくると考えられる．

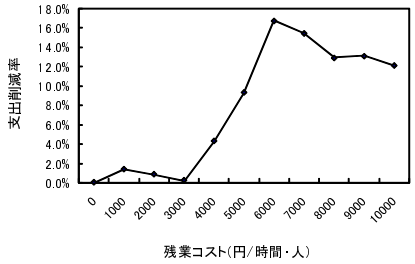

図 4 単位時間残業コストに対する結果
Fig. 4 The result of overtime working cost per time

5. おわりに

近年ではセキュリティインシデントが多く発生し，企業では情報セキュリティ対策に力を入れるようになってきた．しかしセキュリティとコストの間には常にトレードオフの問題があり，これらのバランスを考える研究として，セキュリティ対策選定手法が数多く行われてきたが，従来のセキュリティ対策選定手法は「利便性低下コスト」や「仕事量」に注目していなかった．

そこで本稿では仕事量を考慮したセキュリティ対策選定手法を提案した．この手法は就業者に対する脅威，採用可能な対策を分析し，各対策にどれだけ徹底して行うかを示す値である徹底度を付与する．そして一定期間ごとに就業者の仕事量を評価し，その仕事量と徹底度をもとにその期間に採るべき対策を決定する手法である．

本研究ではケーススタディによる評価を行った．その結果，本提案手法が向いている環境とそうでない環境があることがわかり，単位時間当たりの残業コストが比較的高く，仕事量が一定でないような企業の場合，対策固定のときと比較して 10% 以上も期待支出を削減できることが示され，本提案手法の有用性が示された．

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, No8，pp.2022-2033，2004.
2) 加藤弘一，勅使河原可海．ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案．情報処理学会論文誌，Vol.49, No.9，pp.3209- 3222，2008.
3) McCormic, N.J. Reliability and Risk Analysis. Academic Press Inc. 1981.