Vol.2017-CSEC-79 No.1
2017/12/4

経営陣を含めたサイバーセキュリティ対策案合意形成手法の改良と企業への試適用

福島章太[†1]　佐々木良一[†1]

概要：経営陣と管理者層のサイバーセキュリティに関わる共通認識が乏しく，経営陣主導によるセキュリティ対策が十分行えていないことが指摘されている．この課題に対する取り組みは数多く行われており，その中の一つに米国国立標準技術研究所 (NIST)が開発した Cybersecurity Framework というセキュリティマネジメントに関わる枠組みが存在する．Cybersecurity Framework は，現状と目標のギャップを比較検討することによって，経営陣と管理者層の間で共通認識を得ることが出来る枠組みである．しかし，Cybersecurity Framework は共通認識に基づき，現状と目標のギャップを埋めるための具体的な対策を列挙・選定する手法を示していない．この課題に対して筆者らは，Cybersecurity Framework と Intel 社の適用例を基に，経営陣と管理者層がサイバーセキュリティに対する共通認識を得た上で具体的な対策を列挙出来る手法およびプロセスを提案し，その手法を補助するシステム RC4T を実装した．また，許容可能な総コストという制約条件下で最も現状と目標のギャップを埋めることが出来る「対策案の組み合わせ最適化機能」を RC4T に実装した．しかし，現実の問題に適用しようとすると，提案手法に適合するための組織の要件整理が困難であることや，対策案の数が多いとその最適な組み合わせの求解が困難になるという問題があった。そのため本稿では，GSN (Goal Structuring Notation)という手法を用いてティアを定義する方法を提案するとともに，定式化結果の特徴に着目し最適化アルゴリズムを見直すことで高速近似解法を開発し，具体的企業への適用を試みた結果を報告する。

キーワード：Cybersecurity Framework，対策案合意形成，セキュリティマネジメント

Improvement of Method for Establishing Consensus with Executives on Cybersecurity Measures and Trial Application to Enterprise

SHOTA FUKUSHIMA[†1]　RYOICHI SASAKI[†1]

1. はじめに

近年，情報社会の進展に伴い，サイバーセキュリティに関わる事故が数多く発生している．一方で，企業のセキュリティ対策に対する認識が不十分であることが指摘されている[1]．その原因として，経営陣と管理者層の間でのセキュリティに関する共通認識が乏しいことが挙げられている[2]．共通認識が乏しい場合，組織のセキュリティのリスクを経営陣が適切に認識出来ず，セキュリティ対策に投資がされにくくなる．このため，経営陣主体の全社的なセキュリティ対策が行われなくなる等の弊害が起き，組織全体のセキュリティの水準が低下してしまう恐れがある．

その問題を解決するため，セキュリティの技術的な知識が乏しい経営陣に対してはセキュリティをリスクとして説明するという手法が提案されている[2]．この課題を補助可能な取り組みの一つに Cybersecurity　Framework[3]（以下，CSF）という枠組みがある．CSF はセキュリティ管理の現状と目標を比較検討することでセキュリティに関わるリスクを把握・管理し，それを表現することを補助する．一般に，現状との比較として説明を行うと，セキュリティの知識が乏しい経営陣においても組織のセキュリティの状況を把握することが容易になるため，CSF の利用により経営陣と管理者層の間で共通認識を得られることが期待される．また，米 Intel 社による CSF 利用例[4]が提示されており，CSF の実用性も期待できる．しかし，組織の要件を満たすためには，組織が定めた目標に至るための対策を列挙・選定する必要がある．また，CSF は現状と目標を比較検討することに留まっているため，目標に到達するための対策を列挙及び選定する段階には至っていない．この課題に対して，筆者らは Intel 社の CSF の利用例[4]を基に，共通認識を得ながら対策を列挙する手法を提案し，その手法を補助するシステム RC4T の開発を行った[5]．更に，RC4T に目標と現状のギャップを最も埋めることが出来る対策の組み合わせを導出する「対策案の組み合わせ最適化機能」を実装し，筆者らの所属研究室に試適用することで提案手法の検証を行った[6]．しかし試適用により，組織の要件を CSF に適応させることが困難であることが分かった．また，現実的な問題に合わせて対策数を多くすると，最適化に多大な時間がかかり，最適化が困難になることが分かった．

本稿では，GSN(Goal Structuring Notation)を用いた要件分析法により CSF への適応プロセスを明確にすると共に，最適化のための高速近似解法によって最適化の時間を短縮する改良を施し，企業へ試適用を行う．これにより，提案手法が実際の現場において有用であるかを検証すると共に，改良の効果を検証する．

†1 東京電機大学
Tokyo Denki University

2. CSF について

CSF[3]は，組織のサイバーセキュリティを向上することを目的に,リスク管理原則をまとめた枠組みである.また，リスクベース的なアプローチをとることで，共通認識を得ながら経営陣と管理者層における理解度のギャップ，及び現状と目標のギャップを埋める役割を果たしている． CSF は以下の 2.1～2.3 節の３つの要素で構成されている.

2.1 フレームワークコア

フレームワークコア (以下コア) は「機能」「カテゴリー」「サブカテゴリー」「参考情報」から構成される.「機能」はセキュリティ対策の最も基本的な内容を示す.「カテゴリー」は「機能」を細分化したものである（図 1)．コアの構成に関する詳細は参考文献[3]を参照されたい.

2.2 フレームワークインプレメンテーションティア

フレームワークインプレメンテーションティア（以下ティア）は，組織のリスク管理における認識やそのプロセスを４段階で示したものである．ティア 1 からティア 4 に上がるに連れてよりアダプティブな状態であることを示す.

2.3 フレームワークプロファイル

フレームワークプロファイル（以下プロファイル）は，組織毎の要件に基づいてコアから必要なカテゴリー及びサブカテゴリーを抜粋した上で独自に評価し，まとめたものである．各組織で，必要なセキュリティ管理体制に合わせた目標を設定し，その目標に対して現状の管理体制を確認することで，ギャップ（差異）が評価出来る.

3. Intel 社による CSF の適用例

Intel 社は CSF の試適用である Pilot Project を行った[4].

Pilot Project は「SMEs」「コアグループ」「意思決定者および利害関係者」の 3 グループに分かれて実行された．本稿ではこれらを順に管理者層，CISO，経営陣として扱う.

Pilot Project では，簡略化のためにコアのサブカテゴリーを全て除外し，カテゴリーを充実させたコアを使用することで，独自のカスタマイズを行っている．また，ティアの段階毎に，その段階の状態を表す定義「ティアの定義」を箇条書きで一覧表にし，ティアによる評価の指標とした.

更に，管理者層は，カテゴリー毎にティアの数値で現状の評価を取り，数値が低ければ赤くするなどのヒートマップを作成することで，比較検討を行った.

Pilot Project は CSF の要素に Intel 社独自の要素である「ティアの定義」「ヒートマップ」を加えて 7 ヶ月間行われた.

4. 関連研究

その他の CSF の適用例としては，シカゴ大学における適用例がある[7]．また，CSF を応用した例としては Cybersecurity Assessment Tool （CAT）がある[8]．CAT は主に金融機関が自組織のセキュリティ成熟度評価を行えるようにするためのツールであり，CSF の枠組みを金融業界の業務に整合させている.

対策案に関わる合意形成を得るための研究に関連する報告としては, Multiple Risk Communicator (MRC)がある[9]. MRC は目的関数，制約条件，対策の効果とコストを入力することで費用対効果が最適な対策案の組み合わせを出力するシステムである．すなわち，経営陣の要求に応じて制約条件を設定することで，経営陣の要求の下で最適な対策案の組み合わせを出力することが可能である．よって，MRC は対策案の選定に関わる合意形成に有効であると言える.

5. 提案手法

CSF は現状と目標を比較することに留まっており，現状を目標に近づけるための対策を選定する段階には至っていない．また，CAT も現状の成熟度と目標とする成熟度の評価に留まっており，CSF と同様に対策案の列挙選定までを考慮していないという課題が懸念されている[10].

MRC は, 経営陣と管理者層のセキュリティに関わる共通認識が乏しい場合，セキュリティ対策の合意形成が困難であることが分かった[11]. よって, 経営陣と管理者層の共通認識を得た上で対策案の合意形成を得る手法が求められる.

5.1 RC4T について

筆者らは Intel 社が行った適用を基に, 対策の列挙選定も考慮した CSF 適用プロセスを提案した．また，そのプロセスを補助する RC4T というシステムを開発した[5]．RC4T の開発言語は Java8, ステップ数は約 2800 ステップである. RC4T は「現状入力ツール」「現状把握ツール」を持つ.

「現状入力ツール」は管理者層が現状満たしているティアの定義をカテゴリー毎に入力することを補助する. また,「現状把握ツール」は経営陣と CISO が「現状入力ツール」で入力された現状と目標を比較することを補助するツールである．さらに，管理者層が決定した対策とその効果を閲覧する事もできる．これらのツールの詳細については参考文献[5]を参照されたい．また，RC4T は許容可能なコスト内で最も目標とのギャップを埋められる対策案の組み合わせを総当たりによって求める機能である「対策案の組み合わせ最適化機能」が「現状把握ツール」に実装されている[6]．最適化方式の詳細は，参考文献[6]を参照されたい.

5.2 CSF 利用プロセス

筆者らは，CSF の利用プロセスを提案した（図 1）[6]. このプロセスは，経営陣と管理者層が CISO を介して対策案に関わる合意形成を得るためのプロセスである．本プロセスでは Intel 社が行った適用の流れを汲み取りつつ, 対策案の列挙及び選定も行っている．図 1 に示すプロセスの各ステップの説明を以下に示す.

(1) CISO は経営陣と合意の上で，カテゴリー，ティアの定義を RC4T に入力する.

(2) 管理者層はカテゴリー毎の現状を RC4T に入力する.

(3) RC4T は現状を経営陣と CISO に表示する.

(4)　経営陣と CISO はプロファイルで現状を把握し，カテゴリーごとにティアの目標値を設定する．併せて，許容可能なコストを提示する．

(5)　CISO と管理者層は RC4T から対策が必要な範囲を把握する．

(6)　CISO と管理者層は対策について協議し，RC4T に対策名，対策のコスト，効果を 5.3 節に示す形で入力する．

(7)　RC4T は経営陣と CISO に許容可能なコスト内でティアの目標値と対策後のティアのギャップを最小にすることが出来る最適な対策案の組み合わせを求め，表示する．

(8)　経営陣と CISO は，対策コストの合計，対策後のティアの実態，対策案の組み合わせに満足なら対策を採用する．ティアの目標と対策後の予想実態の間に許容できないギャップがあるなら，新たな許容可能なコストやギャップを確実になくすべきカテゴリーを明確にした上で(6)に戻る．

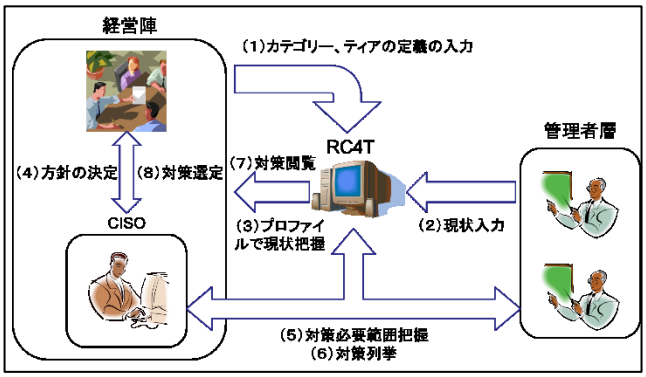

図 1　CSF 利用プロセス

Figure 1　Process of using CSF

5.3　対策列挙手法

筆者らはティア 1 をティア 2～4 のいずれのティアにも当てはまらない状態と定義した．また，特定のティア以下のティアの定義を全て満たした場合のみに特定のティアになると定義した．さらに，筆者らは各ティアの定義毎に ID を付与した．これらの定義を前提として，対策の効果を「対策の対象管理者」「対策の対象カテゴリー」「対策によって解決するティアの定義」とする手法を提案した[10].

以下の図 2 に示すティアの定義と対策の表では，「○」を現状満たしている部分，「△」を対策によって満たされる部分を示す．ここで，「対策 3」の効果を「管理者 1」の「カテゴリー 1」の「ティアの定義 3-1」，「対策 4」の効果を「管理者 1」の「カテゴリー 1」の「ティアの定義 3-2, 3-3」とすると，対策 3 と対策 4 を行う事でティア 3 の定義が満たされ，「管理者 1」の「カテゴリー 1」がティア 3 に上昇する．このような手法を取ることで，コスト制約下で，ティアに関する目標と現状の差を最小とする対策案の組み合わせを求める最適化が可能となる．

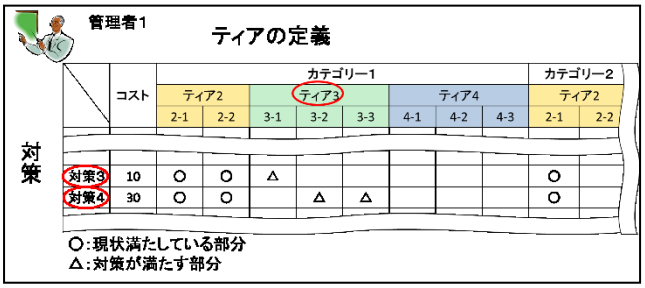

図 2　ティアの定義と対策のテーブル例

Figure 2　Table of Tier definitions and measures

6.　研究室に対する試適用と課題

筆者らは，筆者らが所属する研究室に対して図 1 のプロセスを踏むことで，経営陣と管理者層にとって望ましい対策案の組み合わせが得られるかどうかの検討を行った．その結果，提案したプロセス（図 1）と RC4T を利用することで，経営陣と管理者層は CISO を介して対策案の合意形成を行える見通しが得られることが分かった．

しかし，組織の要件をティアの定義にするプロセス（図 1 の(1)）が困難であることが分かった．よって，要件をティアの定義に落とし込む議論を円滑に進める手法が求められる．更に，対策案の組み合わせ最適化機能は総当たりによって最適解を導出するため，対策の数が増えるにつれて時間コストが指数関数的に増大してしまう．よって，総当たりによる最適化に代わる手法が求められる．

適用に関わる詳細は参考文献[6]を参照されたい．

7.　企業への試適用

筆者らは 6 章の課題を踏まえて提案手法の改良を行い，実際の企業への試適用を行った．

7.1　ティアの定義決定手法

筆者らはティアの定義決定に関わる議論を円滑に進めるため，GSN (Goal Structuring Notation)[12]という手法を用いることにした．GSN は議論をグラフィカルに記述する手法であり，要件分析や要件を満足する証跡の有無の確認などに利用される．GSN をサイバーセキュリティに利用した例としては金子の研究[13]が挙げられる．GSN の具体的な記述方法は参考文献[12]を参照されたい．

GSN によるティアの定義決定手法は下記の通りである．

1. 頂上のゴール「自身が管理している範囲においてこのカテゴリーは組織の要件に適応している」を設定する．
2. 頂上のゴールを解決する戦略「組織の要件に適応しているかを確認」を設定する．また，戦略に関わるコンテキストとして組織の要件を列挙する．更に，列挙した組織の要件毎に，戦略の下にサブゴール「【組織の要件】に適応している（【組織の要件】には列挙した組織の要件が入る）」を設定する．（組織の要件レイヤ）

3. サブゴールを解決する戦略「【組織の要件】への対応がティアに適応しているか確認」をサブゴール毎に設定する．また，戦略に関わるコンテキストとしてティア 2～4 を記述する．更に，ティア 2～4 に応じて戦略の下にサブゴールを設定する．（ティアレイヤ）
4. 末端のサブゴールを，CISO が満足するまで同様の手順で細分化し，最終的に末端となったサブゴールをティアの定義とする．

図 3 は組織の要件を「セキュリティ人材育成」「標的型攻撃への対応」にした場合の例である．前述の手順の通り，組織の要件レイヤでは組織の要件ごとに，ティアレイヤではティア 2～4 毎にゴールを細分化している．その後，任意に細分化を行い，末端をティアの定義としている．

また，GSN の定義として，末端のゴールに対しては，そのゴールを満たす証跡の有無を記述する必要がある．提案手法では，入力した現状と対策の効果が証跡に該当するため，GSN の定義を満たしていると言える．

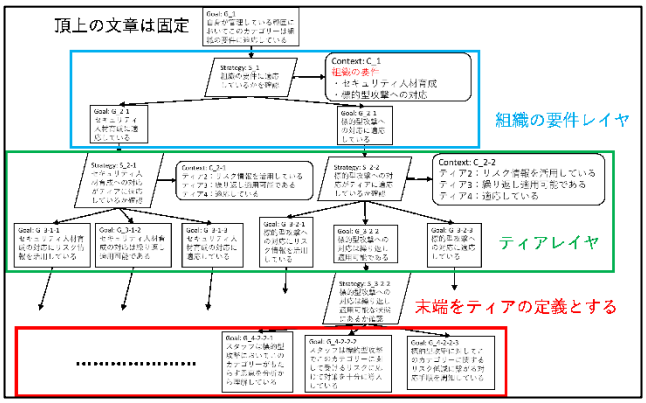

図 3　GSN によるティアの定義決定例
Figure 3　Example of deciding tier definition by GSN

7.2 対策案の組み合わせ最適化のための高速近似解法

筆者らは，特定のティア以下のティアの定義を全て満たした場合のみに特定のティアになるという特徴を踏まえ，欲張り法のアルゴリズムによって最適化のための高速近似解（以下，近似解）を求めることとした．提案するアルゴリズムは，各カテゴリー-管理者の組み合わせで最も目標値とのギャップが大きい部分に注目して局所最適な対策を施すことでティアを上昇させることを目的としている．下記にアルゴリズムの概要を示す．

1. 全てのカテゴリー-管理者の組み合わせで「目標値 – 現状値」を計算し，目標値とのギャップを調べる．故に，ギャップの最大値は 3 である．例えば下記の表 1 では，ギャップ 3 は「資産管理-管理者２」，ギャップ 2 は「資産管理-管理者１」「保守-管理者１」，ギャップ 1 が「保守-管理者２」となる．

表 1　カテゴリー-管理者の表例
Table 1　Example of Category-Administrator table

カテゴリー	管理者１	管理者２	目標値
資産管理	2	1	4
保守	1	2	3

2. 配列 Gap_1, Gap_2, Gap_3 を用意し，ギャップ 3 のカテゴリー-管理者の組み合わせを Gap_1～3 に，ギャップ 2 の組み合わせを Gap_1, 2 に，ギャップ 1 の組み合わせを Gap_1 に格納する．
3. 変数 I にギャップの最大値である 3 を格納する．
4. Gap_I に格納されたカテゴリー-管理者の組み合わせを一つ取り出す．
5. 取り出したカテゴリー-管理者の組み合わせの現状のティアの値を調べ，そのティアの値+1 において満たしていないティアの定義を調べる．
6. 満たしていないティアの定義を一つ選択し，そのティアの定義に対して有効な対策を全て調べ，現在残っている予算よりコストがかかる対策を取り除く．その結果として有効な対策が 1 つの場合はその対策を採用する．有効な対策が複数ある場合は「対策が埋めるティアの定義の数÷コスト」をそれぞれの対策で計算し，最も値が大きい対策を採用する．その後，採用した対策によって埋まるティアの定義を満たしている状態に変更し，予算を対策のコスト分減らす．この処理をティアの定義ごとに逐次的に行う．
7. Gap_I が空になるまでプロセス 4～6 を繰り返す．Gap_I が空になった場合，I - 1 を行う．
8. I > 0 ならばプロセス 4 に戻る．I = 0 ならば最終的に採用された全ての対策を近似解とする．

本アルゴリズムの計算時間は O(n^4)である．これは従来の総当たりによる最適化の計算時間 O(2^n)より高速であると言える．また，9 回の小規模なテストによる近似率の実験的評価を行った．近似率は「近似解のティアの上昇値 ÷ 最適解のティアの上昇値」で求める事とする．すなわち，近似解の上昇値が 2，最適解の上昇値が 3 ならば約 66.7%となる．結果，9 回中 7 回が 100%であり，平均近似率は約 90.7%であった．

7.3 試適用結果

提案手法がセキュリティの現場においても有効であるかを検証するために，実際の企業への試適用を行った．適用対象は主に保険業を営む企業 X 社である．X 社は数多くの事業会社である子会社を保有している．今回の適用ではその子会社の一部である A 社，B 社，C 社のセキュリティ評価を X 社の者が行い，各子会社のセキュリティの現状を管理者層の現状として評価することとした．すなわち，試適用に参加した管理者層は以下の表 2 の通りである．

表 2　試適用に参加した管理者

Table 2　Administrators who participated for trial application

管理者 ID	管理者名
A	事業会社 A
B	事業会社 B
C	事業会社 C

また，今回の適用では CISO と経営陣が参加できなかったため，第 1 著者が CISO 役としてロールプレイを行い，管理者における提案手法の使用感を評価することとした．

以下に，図 1 のプロセスに従った試適用の結果を示す．

(1) **カテゴリー，ティアの定義の入力**

経営陣が不参加のため，ここでは CISO と管理者層がカテゴリーとティアの定義を決定し，CISO が RC4T に入力した．ティアの定義決定手法は 7.1 節の GSN を利用した．表 3，4 に採用したカテゴリーとティアの定義を示す．

表 3　試適用で利用したカテゴリー

Table 3　Categories used for trial application

機能	カテゴリーID	カテゴリー名	目標値
防御	PR.PT	保護技術	4
防御	PR.AT	意識向上およびトレーニング	4

表 4　試適用で利用したティアの定義

Table 4　Tier definitions used for trial application

ティア	定義 ID	定義の説明
2	2-1	セキュリティ人材育成を実施している
	2-2	リスク管理プロセスがポリシーレベルで文書化されている
	2-3	リスク管理プロセスが手順書レベルまで文書化されている
	2-4	ミニマムマストのテクノロジーが採用されている
3	3-1	セキュリティ人材育成を繰り返し実施している
	3-2	リスク管理プロセスがポリシーレベルで文書化され定期的に見直しされている
	3-3	リスク管理プロセスが手順書レベルまで文書化され定期的に見直しされている
	3-4	標準的なテクノロジーが採用されている
4	4-1	セキュリティ人材育成が最適化されている
	4-2	リスク管理プロセスがポリシーレベルで文書化され定期的に見直しされ最適化されている
	4-3	リスク管理プロセスが手順書レベルまで文書化され定期的に見直しされ、最適化されている
	4-4	ベストプラクティスのテクノロジーが採用されている

(2) **現状入力**

(1)で入力したカテゴリーとティアの定義に従って各管理者はセキュリティの現状を入力した．入力した結果を表 5，6 に示す．なお，表中の「○」を現状満たしている部分，「×」を現状満たしていない部分（ティアを上昇させるために対策を必要とする部分），「—」を X 社の要件に基づいて評価対象外とした部分とする．

表 5　カテゴリー「保護技術」の現状

Table 5　Current state of　“Protective Technologies” category

定義 ID	事業会社 A	事業会社 B	事業会社 C
2-1	—	—	—
2-2	○	○	○
2-3	○	○	×
2-4	○	○	○
3-1	—	—	—
3-2	○	○	○
3-3	○	○	×
3-4	○	○	×
4-1	—	—	—
4-2	○	○	○
4-3	○	×	×
4-4	×	×	×

表 6　カテゴリー「意識向上およびトレーニング」の現状

Table 6　Current state of　“Awareness/Training” category

定義 ID	事業会社 A	事業会社 B	事業会社 C
2-1	○	○	○
2-2	○	○	○
2-3	—	—	—
2-4	—	—	—
3-1	○	○	×
3-2	○	○	○
3-3	—	—	—
3-4	—	—	—
4-1	×	×	×
4-2	○	○	○
4-3	—	—	—
4-4	—	—	—

更に，入力した現状の根拠を，各カテゴリーにおける各ティアの定義毎に記述し，現状入力の説得性を補強した．

(3) **現状把握**

(2)で入力した現状から RC4T は各カテゴリー-管理者の現状のティアを算出した．算出結果を以下の表 7 に示す．

表 7　各カテゴリー-管理者の現状

Table 7　Current state of each Category-Administrator

カテゴリーID	管理者 ID			管理者平均	目標値
	A	B	C		
PR.PT	3	3	1	2	4
PR.AT	3	3	2	2	4

(4) **方針の決定**

表 7 より，全てのカテゴリー-管理者が目標値に至っていないため，CISO は全体的に対策を列挙するよう管理者層に指示した．

(5) **対策必要範囲把握**

CISO と管理者層は表 5，6 を閲覧し，対策が必要な範囲を把握した．今回は全体的に対策を行うことを目的としたため，全ての「×」部分に対して対策を挙げることとなる．

(6) **対策列挙**

管理者層は全ての「×」部分に対して対策を列挙した．また，CISO は(2)で記述された現状の根拠を基に，列挙された対策によって「×」部分が解決するかを確認した．列挙された対策は以下の表 8 の通りである．

表 8　列挙された対策

Table 8　Enumerated measures

対策 ID	対策名	対策の効果			コスト（万円）
		管理者 ID	カテゴリーID	定義 ID	
1	リスク管理プロセス手順書作成	C	PR.PT	2-3	300
2	セキュリティ人財育成の繰り返し	C	PR.AT	3-1	150
3	リスク管理プロセス手順書の定期見直し	C	PR.PT	3-3	80
4	ふるまい検知導入	C	PR.PT	3-4	800
5	IDS/IPS 導入	C	PR.PT	3-4	350
6	WAF 導入	C	PR.PT	3-4	400
7	セキュリティ人財育成最適化に向けた外部ベンダーによる研修実施	A	PR.AT	4-1	500
8	セキュリティ人財育成最適化に向けた外部ベンダーによる研修実施	B	PR.AT	4-1	250
9	セキュリティ人財育成最適化に向けた外部ベンダーによる研修実施	C	PR.AT	4-1	200
10	リスク管理プロセス手順書の最適化に向けた見直し	B	PR.PT	4-3	120
11	リスク管理プロセス手順書の最適化に向けた見直し	C	PR.PT	4-3	90
12	インターネット接続環境分離	A	PR.PT	4-4	20000
13	端末操作ログ取得（EDR 導入）	A	PR.PT	4-4	6000
14	インターネット接続環境分離	B	PR.PT	4-4	8000
15	端末操作ログ取得（EDR 導入）	B	PR.PT	4-4	1200
16	インターネット接続環境分離	C	PR.PT	4-4	4000
17	端末操作ログ取得（EDR 導入）	C	PR.PT	4-4	1100

(7) **対策閲覧**

今回の適用では一定間隔の許容可能なコスト毎に上昇するティアを比較するグラフを作成することによって対策の効果を表示した．また，従来手法であった最適化厳密解では 1 回の解の出力に 1 時間以上かかってしまうため，7.2 節で述べた近似解によってグラフを作成した．近似解の導出は，いずれも 10 秒以内に終了した．以下の図 4 に近似解結果グラフを示す．なお，「費用対効果」は「ティアの上昇値÷対策の総コスト×1000」によって算出される。また，横軸が許容可能なコスト，左縦軸が「対策の総コスト」に掛かる目盛、右縦軸が「ティアの上昇値」「費用対効果」に掛かる目盛である．

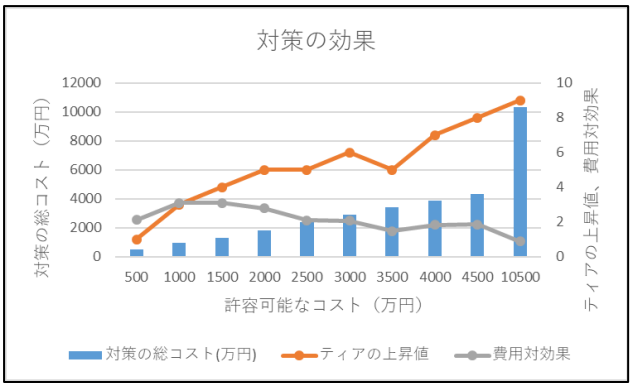

図 4　近似解結果グラフ

Figure 4　Graph of the optimized approximate solution

許容可能なコスト毎の対策の内訳は以下の表 9 の通りである．

表 9　近似解の対策

Table 9　Measures of the optimized approximate solution

許容可能なコスト（万円）	対策 ID	対策の総コスト(万円)
500	1, 3, 11	470
1000	1, 2, 3, 5, 11	970
1500	1, 2, 3, 5, 9, 10, 11	1290
2000	1, 2, 3, 5, 7, 9, 10, 11	1790
2500	1, 2, 3, 5, 9, 10, 11, 17	2390
3000	1, 2, 3, 5, 7, 9, 10, 11, 17	2890
3500	1, 2, 3, 5, 10, 11, 15, 17	3390
4000	1, 2, 3, 5, 8, 9, 10, 11, 15, 17	3840
4500	1, 2, 3, 5, 7, 8, 9, 10, 11, 15, 17	4340
10500	1, 2, 3, 5, 7, 8, 9, 10, 11, 13, 15, 17	10340

7.4 アンケート結果

今回の試適用終了後，管理者層に対してアンケートとヒアリングを行った．アンケートは参加した管理者 3 名が議論を行い，総意として 1 つのアンケートに記入した．アンケートの結果を以下の表 10 に示す．なお，表 10 中の数値は「1：思わない」「2：やや思わない」「3：どちらとも言えない」「4：やや思う」「5：思う」を意味する．

表 10　試適用に関わる質問

Table 10　Questions rerated to trial application

番号	質問内容	数値
1	GSN の表記方法は分かりやすいと思いましたか.	4
2	GSN を利用したティアの定義決定方法についての説明後, ティアの定義を決定するのは容易であると思いましたか.	4
3	あなたが経営陣として参加した場合, 目標値の設定は容易であると思いますか.	3
4	今回の適用において, 現状の入力は容易であると思いましたか.	3
5	今回の適用において, 現状入力の根拠の説明は容易であると思いましたか.	5
6	今回の適用において, 対策の列挙は容易であると思いましたか.	2
7	今回の適用において, 対策の効果を決定するのは容易であると思いましたか.	3
8	列挙された対策はセキュリティの向上としての効果が望めると思いますか.	4
9	現状入力の根拠などを提示することによって, 列挙された対策の効果を経営陣に説明しやすくなると思いますか.	4
10	現場の実際の状況とティアの定義から考えて現状ティアの数値は妥当だと思いましたか.	4
11	あなたが経営陣として参加した場合, 現状ティアを見て自社のセキュリティ状況を把握できると思いますか.	2
12	あなたが経営陣として参加した場合, 近似解の結果を見て納得すると思いますか.	4

また，ヒアリングにより下記のような意見を得られた．

1. 合意形成のための議論を行う上で, 列挙された対策案を最適化する処理に望ましい時間は 20 秒以下である．
2. サイバー対策のベストプラクティスを求めていくには相当のコストが必要となるという現状と「効果＝ティアの上昇」ととらえる今回のモデルにおいて，ティアを上げていくために費用対効果は下がっていくという今回の結果は実態と合っている．
3. サイバーセキュリティ対策の全てに対応するためには GSN 含め今回のモデルは複雑になりすぎて，難解となるかもしれない．
4. 経営目線として,「ティアの上昇＝効果」と捉えているが, 個々の対策毎にもそれぞれの個別の対策としての効果もあるので, 効果に対する考えをどう整理していくかは将来的な課題となると思われる．

7.5 考察

(1) 最適化のための高速近似解法について

図 4 とヒアリング 2，およびアンケートの質問 10 を見ると，グラフの結果とセキュリティの現場の実態が合致していると考えられる．また，近似解を導出する時間はいずれも 10 秒以下であったため，ヒアリング 1 の要件を満たしていると言える．しかし，許容可能なコスト 3500 の地点でティアの上昇値が減少していることが分かる．これは，対策をするにあたって費用対効果の高いカテゴリー-管理者よりも先に費用対効果の低いカテゴリー-管理者を走査してしまう時に発生する恐れがある誤差であることが分かった．すなわち，本試適用では事業会社 A と C の PR.AT のティア 4 の定義 4-1 を満たす対策 7, 9 を採用する方が効率的であるにも関わらず, 先に B の PR.PT のティア 4 を走査してしまい，費用対効果の悪い対策 15 を採用してしまった．これにより，効率の良い対策 7, 9 を採用する予算が無くなってしまったため生じる誤差であることが分かった．よって，このような誤差を減少させるためには最適化のための高速近似解法の再検討が必要であると考えられる．

(2) **提案手法について**

質問 1, 2 を見ると，前回の試適用で課題となったティアの定義を決定するプロセスの困難さが，GSN を利用することで改善されたことが分かる．また，質問 5, 9 を見ると本手法を利用することでセキュリティの現状と対策の効果を経営陣に説明することが容易になったことが分かる．更に，質問 8 を見ると，本手法で列挙された対策はセキュリティの現場においても有効であると考えられる．しかし，質問 6 を見ると，対策の列挙が困難であることが分かる．更に，質問 11 を見ると，提案手法では経営陣が現状を把握するのが困難である恐れがあることが分かる．これらは，ヒアリング 3 の結果から見て，提案手法のモデルが複雑であるが故に生じる困難であると考えられる．よって，これに対しては，適用を周回することによる慣れやモデルの簡略化が必要であると考えられる．

(3) **対策案合意形成について**

質問 12 を見ると経営陣との対策案合意形成を行える見通しは得られたと言える．しかし，ヒアリング 4 の結果を見ると，対策の効果を「満たすティアの定義」としている性質上，対策毎の特徴が削がれてしまう恐れがあることが分かった．これは，今回は比較的小規模に適用を行ったため，ティアの定義が不足しているためであると考えられる．よってこれに対しては，より大規模な適用を行った場合の結果と照らし合わせる必要があると考えらえる．

8. おわりに

本稿では，前回の試適用[6]で浮上した課題を改善する手法として「GSN によるティアの定義」「最適化のための高速近似解法」を提案し，実際の企業への試適用を行った．これにより，提案手法によって経営陣に対して現状と対策案の説明が容易になり，対策案に関わる合意形成を行える見通しが得られた．しかし，より実用的な手法とするには下記のような課題が判明した．

- 本稿で提案した最適化のための高速近似解法では従来手法と比較して大幅な高速化が行えたが，ティアの上昇値に関わる誤差を減らす工夫が必要である．
- 提案手法のモデルが複雑である．
- 対策毎の特徴が削がれてしまう恐れがある．

よって，下記の事項を今後の課題としたい．

- 最適化のための高速近似解法の再検討．
- 提案モデルの簡略化，適用の周回による変化の考察．
- より大規模な試適用．

謝辞 本稿の試適用に参加し研究の改良に尽力して頂いた企業の皆様，GSN によるティアの定義決定手法について様々なご指導，ご助言をして頂いた東京電機大学の勅使河原可海先生および(独)情報処理推進機構の金子朋子様，筆者らの所属する研究室での試適用に参加頂いた係長の皆様に謹んで感謝の意を表する．

参考文献

[1] “情報セキュリティガバナンス導入ガイダンス”. http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf, (参照 2017-10-30).
[2] 林紘一郎. 係長セキュリティから社長セキュリティへ:日本的経営と情報セキュリティ. 情報セキュリティ総合科学, 2010, vol. 2, p. 1-42.
[3] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity version 1.0. 情報処理推進機構（訳）. 重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版. https://www.ipa.go.jp/files/000038957.pdf, (参照 2017-10-30).
[4] T. Casey, K. Fiftal, K. Landfield, J. Miller, D. Morgan, and B. Willis. The Cybersecurity Framework in Action: An Intel Use Case. https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/cybersecurity-framework-in-action-use-case-brief.pdf, (参照 2017-10-30).
[5] 福島章太, 佐々木良一. Cybersecurity-Framework を用いた対策案合意形成手法の提案. マルチメディア，分散，協調とモバイルシンポジウム 2016 論文集, 2016, vol. 2016, p. 1699-1704.
[6] Shota Fukushima, Ryoichi Sasaki. Proposal and Evaluation of Method for Establishing Consensus on Combination of Measures Based on Cybersecurity Framework. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2016, vol. 5, no. 3, pp. 155-165. doi:10.17781/P002209.
[7] “Applying the Cybersecurity Framework at the University of Chicago–An Education Case Study”. http://security.bsd.uchicago.edu/wp-content/uploads/sites/2/2016/04/BSD-Framework-Implementation-Case-Study_final_edition.pdf, (cited 2017-10-30).
[8] “Cybersecurity Assessment Tool,”. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf, (cited 2017-10-30).
[9] 佐々木良一，日高悠，守谷隆史，谷山充洋，矢島敬士，八重樫清美，川島泰正，吉浦裕．多重リスクコミュニケータの開発と適用．情報処理学会論文誌, 2008, vol. 49, no. 9, p. 3180-3190.
[10] 『FFIEC Cybersecurity Assessment Tool に関する調査研究』調査報告書. http://www.fsa.go.jp/common/about/research/20160815-1/01.pdf, (参照 2017-10-30).
[11] 谷山充洋，日高悠，荒井正人，甲斐賢，伊川宏美，矢島敬士，佐々木良一．多重リスクコミュニケータの企業向け個人情報漏洩問題への適用．日本セキュリティマネジメント学会論文誌, 2009, vol. 23, no. 2, p. 34-51.
[12] “GSN COMMUNITY STANDARD VERSION 1”. http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf, (cited 2017-10-30).
[13] 金子朋子．より安全なシステム構築のために～CC-Case_i によるセキュリティ要件の見える化．日本セキュリティマネジメント学会論文誌, 2016, vol. 30, no. 1, p. 11-22.