Cybersecurity-Framework を用いた対策案合意形成手法の提案

福島章太[1]　　佐々木良一[2]

概要：近年，情報社会の進展に伴い，IT システムに依存する企業が増加した．一方，企業内において，経営陣と管理者層の情報セキュリティに関わる共通認識が乏しく，十分な情報セキュリティ対策が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の NIST が開発した「Cybersecurity-Framework」がある．しかし，「Cybersecurity-Framework」は経営陣と管理者層で共通認識を得ることに留まっており，共通認識に基づき具体的な対策を列挙・選定する手法を示していない．本稿では，「Cybersecurity-Framework」とその利用例を基に，経営陣と管理者層が情報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の提案と，その手法を実現可能にするシステムを実装する．

Proposal of the method for establishing the consensus on the measures based on Cybersecurity-Framework

SHOTA FUKUSHIMA[1]　　RYOICHI SASAKI[2]

1. はじめに

近年，情報社会の進展に伴い，情報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，企業の情報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情報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[1]．共通認識が乏しい場合，組織の情報セキュリティのリスクを経営陣が適切に認識出来ず，情報セキュリティ対策に投資がされにくくなる，経営陣主体の全社的な情報セキュリティ対策が行われなくなる等の弊害が起き，組織全体の情報セキュリティの水準が低下してしまう恐れがある．そのため，情報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情報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おり[2]，この手法は昨今の情報セキュリティにおいて重要視されている．この課題を補助可能な取り組みの一つに「Cybersecurity-Framework[3]（以下 CSF)」というフレームワークがある．CSF は情報セキュリティ管理のフレームワークであり，情報セキュリティ管理の現状と目標を比較検討することで情報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．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．米 Intel 社も実際には対策を行ったと考えられるが，対策を列挙及び選定する手法を提示した例はまだ見当たらない．本研究では，経営陣と管理者層の間で共通認識が乏しく，十分な情報セキュリティ対策が行えないという課題に対して，米 Intel 社の CSF の利用例[4]を基に，共通認識を得ながら情報セキュリティ管理に対する対策を列挙する手法を提案する．また，その手法を実現可能にするシステムの開発を行う．

2. CSF について

CSF は，重要インフラ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フレームワークである．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，各組織の必要に応じた独自のカスタマイズで適用を行うことが出来る．CSF は以下の３つの要素で構成されている．

（１）フレームワークコア
（２）フレームワークインプレメンテーションティア
（３）フレームワークプロファイル

1 東京電機大学
2 東京電機大学　教授

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（図１）.

「機能」は情報セキュリティ対策の最も基本的な内容を示し，「特定」「防御」「検知」「対応」「復旧」が含まれる.

「カテゴリー」は「機能」を細分化したものである（図２）.

「サブカテゴリー」は「カテゴリー」を細分化したものであり，所属している「カテゴリー」の達成に必要な情報をまとめたものである.

「参考情報」は「サブカテゴリー」毎に割り当てられており，「サブカテゴリー」を達成する際に参考となる各種規格などが記載されている.

機能	カテゴリー	サブカテゴリー	参考情報
特定			
防御			
検知			
対応			
復旧			

図１　コアの構造（[3]を参考に作成）

機能	カテゴリー
特定	資産管理
	ビジネス環境
	ガバナンス
	リスクアセスメント
	リスク管理戦略
防御	アクセス制御
	意識向上およびトレーニング
	データセキュリティ
	情報を保護するためのプロセスおよび手順
	保守
	保護技術
検知	異常とイベント
	セキュリティの継続的なモニタリング
	検知プロセス
対応	対応計画の作成
	伝達
	分析
	低減
	改善
復旧	復旧計画の作成
	改善
	伝達

図２　コアのカテゴリー（[3]を参考に作成）

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がどの段階であるかを４段階で評価したものである．ティア１からティア４に上がるにつれて，よりアダプティブな状態であることを示す（図３）.

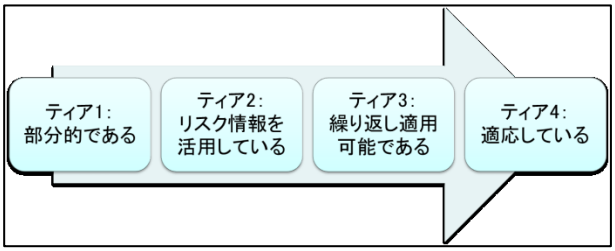

図３　ティアのイメージ

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，独自に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. 米 Intel 社による CSF の利用例

米 Intel 社は CSF の実用性を検証するプロジェクト「Pilot Project」を行った[4].

3.1 Pilot Project のグループについて

Pilot Project は以下の（１）～（３）の３つのグループで行った.

（１）コアグループ

コアグループは 8～10 人の高度な知識を持った情報セキュリティ技術者である．コアグループは，コアのカテゴリーを選択・編集，目標を設定する権限を持つ．本研究ではコアグループを，より一般的な概念である CISO として扱う.

（２）SMEs

SMEs は Subject Matter Experts の略であり，内容領域専門家らを意味する．SMEs は各専門分野のリスクを評価する権限を持つ．本研究では SMEs を，より一般的な概念である管理者層として扱う.

（３）意思決定者及び利害関係者

意思決定者及び利害関係者は，ティアの目標を認可，評価結果をレビュー，許容できるリスクを設定する権限を持つ．本研究では意思決定者及び利害関係者を，CISO 以外の経営陣として扱う.

3.2 Pilot Project の方針について

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，代わりに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を箇条書きで一覧表にし，これを満たしているかどうかをティアによる評価の指標とした（図４）．更に，リスク評価対象の管理者らは，カテゴリー毎にティアの数値で現状の評価を取り，ティアの数値が低ければ赤く強調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（図５）．ヒートマップは，Pilot Project におけるプロファイルであると言える．

ティア1	ティア2	ティア3	ティア4
【定義1-1】教育を実施していない	【定義2-1】教育を実施している	【定義3-1】試験による能力把握を行っている	【定義4-1】方針に応じて教育を改善している
【定義1-2】リスク情報を用いていない	【定義2-2】リスク情報を基に対策を決定している	【定義3-2】リスク情報を基に対策を改善している	【定義4-2】リスク情報から兆候を察知している

図４　ティアの定義例（[4]を参考に作成）

	管理者1	管理者2	管理者3	管理者4	目標値
カテゴリー1	1	2	2	2	2
カテゴリー2	2	3	1	2	3
カテゴリー3	1	2	1	3	3
カテゴリー4	4	3	3	4	4
カテゴリー5	3	4	3	4	4

図５　ヒートマップ例（[4]を参考に作成）

3.3 Pilot Project のプロセスと効果

CSF の要素に加えて，米 Intel 社が独自に導入した要素である「ティアの定義」および「ヒートマップ」を利用して，Pilot Project を以下の（１）～（４）の流れで７ヶ月間実行した．

（１）CISO がカテゴリー毎にティアの目標を設定
（２）管理者毎に現状を評価
（３）評価した結果を分析
（４）分析結果を基に経営陣と協議

米 Intel 社はこれらのアクションを行ったことで，社内における情報セキュリティの議論が補助された，利害関係者に現状を説明しやすくなった，等の効果を得られたという．

4. CSF の課題

4.1 「経営陣」「管理者層」の利用イメージ

Pilot Project における CSF 利用の流れから，図６の（１）～（３）の様な，CSF の利用イメージが考えられる．

始めに管理者層がカテゴリー毎の現状を入力する．また，入力した現状をプロファイルという形でまとめた．また，プロファイルを用いて経営陣が現状を把握し，今後の方針を決定するという流れである．

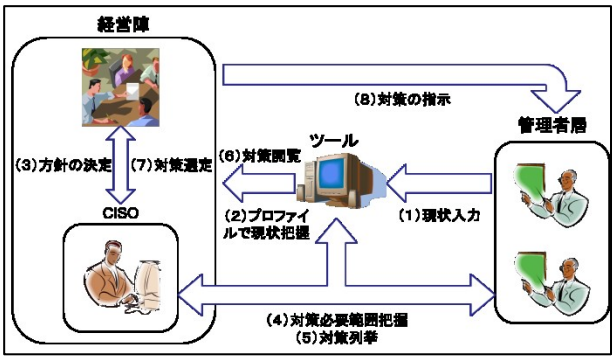

図６　経営陣，CISO，管理者層の CSF 利用イメージ図

4.2 CSF の利用における課題

組織が求めるセキュリティ管理の要件を満たすためには，組織が定めた目標に到達するために対策が必要な範囲を把握し，対策を列挙及び選定する手法が必要である（図６の（４）～（７））．しかし，２章の通り，CSF は組織全体の情報セキュリティに対する共通認識を得ながら現状と目標を比較し，対策が必要なギャップを把握する為のフレームワークである．すなわち，CSF は目標に到達する為に必要な対策を列挙及び選定するという段階には至っていない．Pilot Project においても実際には対策を行ったと考えられるが，どのようにして対策を決めたのか示されておらず，その他にも CSF を基とした対策を列挙及び選定する手法を示した例はまだ見当たらない．本研究は，この課題を踏まえて CSF を利用した対策列挙手法を提案する事が目的である．

5. 提案

４章の課題を踏まえて，著者らは米 Intel 社の CSF 利用例を基に対策列挙手法の提案を行う．これは，CSF で把握した現状と目標のギャップを埋めるために必要なセキュリティ管理対策を，効果を明らかにしつつ列挙するためのものである．これにより，経営陣と管理者層の共通認識を得た上で対策及び効果を示すことが出来るため，セキュリティ管理対策を目標とするティアの数値に向かう形で列挙出来るようになる．

5.1 対策を列挙する上での課題

一般的に，対策の効果は定量的・定性的に示される．しかし，対策の効果をティアの上昇値とすると，ティアの定義と矛盾する恐れがある．例として以下の表１のような対策の一覧表を考える．

表１　対策一覧表例

対策名	対象管理者	対象カテゴリー	上昇値
対策１	管理者１	カテゴリー１	0.5
対策２	管理者１	カテゴリー１	0.7

表１の通りに対策が列挙されている場合，「対策１」と「対策２」を行うことで，「管理者１」における「カテゴリー１」のティアが１以上上昇する．しかし，この２つの対策を行うだけで１つ上のティアの定義を全て満たすとは限らず，計算結果と対策後の状況に矛盾が生じてしまう．そのため，現状より上のティアの定義を満たした上で，ティアを上昇させるための工夫が必要である．

5.2 対策列挙手法

５．１節の通り，対策の効果をティアの上昇値とすると，対策による効果と対策後の状況に矛盾が発生するという問題が発生する．そこで，対策の効果を，目標と比較して不足しているティアの定義を補う形とすることで，ティアの定義と矛盾せずに対策を評価出来る．例として以下の表２のような対策一覧表を考える．

表２　提案手法を用いた対策一覧表例

対策名	対象管理者	対象カテゴリー	解決する定義
対策１	管理者１	カテゴリー１	ティア２の定義１
対策２	管理者１	カテゴリー１	ティア２の定義２

表２の通りに対策が列挙されている場合，「対策１」「対策２」を行うことで，「管理者１」における「カテゴリー１」のティア２における定義１及び２を満たすことが出来る．これらの対策によってティア２の定義を全て満たした場合，「管理者１」における「カテゴリー１」のティアが１から２に上昇する．このように，対策の効果を，目標のティアと比較して不足しているティアの定義を補う形とすることで，ティアの定義と矛盾せずに対策を評価出来る．

6. RC4T(Risk Communicator for Tier)の実装

５．２節で提案する手法は，目標とするティアに至るための必要条件となるティアの定義に対して、そのティアの定義を満たす対策を列挙するという手法である．故に，この提案を実現するには，図６の（１）（２）（４）（５）（６）において，以下のような操作を行う必要がある．

（１）ティアの定義に厳密な現状入力．

（２）管理者が入力した現状満たしているティアの定義から，各管理者がどのティアまで至っているかを算出し，プロファイルとして提示．

（４）管理者が入力した現状満たしているティアの定義から，各管理者が満たすべきティアの定義を表示．

（５）５．２節の手法のように，満たすティアの定義を効果とした対策の列挙．

（６）列挙した対策の表示．

以上の事から，図６に示す（１），（２），（４），（５），（６）のプロセスを行うには，データ入力の簡略化やデータの可視化等の支援が無ければ困難だと分かった．そこで，５．２節の手法を満たし，これらのプロセスを支援するシステム RC4T(Risk Communicator for Tier)を実装した．RC4T は，「現状入力ツール」「現状把握ツール」を備えている．

以下の表３，４に実装環境，実装ステップ数及び動作環境を示す．

表３　実装環境と実装ステップ数

開発OS	Windows7 Professional
開発環境	Eclipse4.4
開発言語	Java8
使用データベース	PostgreSQL4.3
ステップ数	約2400ステップ

表４　動作環境

CPU	Intel Core i5 vPro
メモリ	8GB
OS	Windows7 Professional

また，RC4T に備わる各ツール・機能を動作させる際に用いた模擬データは以下の表５～８の通りである．

表５　動作に利用した管理者一覧

管理者ID	管理者名
NET	ネットワーク
PRO	データプロテクション

表６　動作に利用したティアの定義一覧

ティア	定義ID	定義名
2	2-1	従業員はトレーニングを受けている
3	3-1	従業員は責任と役割を理解している
	3-2	従業員は責任と役割を実行できるスキルを持っている
4	4-1	従業員は企業のニーズに合わせて自ら知識を拡充している
	4-2	従業員は定期的に講演を受けている

表 7　動作に利用した機能一覧

機能ID	機能名
ID	特定
PR	防御

表 8　動作に利用したカテゴリー一覧

カテゴリーID	カテゴリー名	目標ティア
ID.AM	資産管理	3
ID.GV	ガバナンス	4
ID.RA	リスクアセスメント	4
ID.RM	リスク管理戦略	3
PR.AC	アクセス制御	2
PR.DS	データセキュリティ	3
PR.IP	情報を保護する為のプロセス	2
PR.MA	保守	2

6.1　現状入力ツール

本ツールは，管理者層が各カテゴリーに対して，現状におけるティアの定義の達成度を入力する為のツールである．本ツールは，図６の「（１）現状入力」に対応する．ティアの定義一覧から，満たしているティアの定義を全て選択することで，そのカテゴリーにおいて現状充足しているティアの定義を入力出来る（図７）．本ツールは，カテゴリーが無数に存在するときに画面が煩雑とすることを防ぐために，カテゴリー毎に逐次的に現状を入力する形とした．
本来は管理者が現状を把握し，評価を入力するためのツールだが，６．２節及び６．３節で現状を表示する動作を検証するために，著者らの任意で本ツールに現状を入力した．

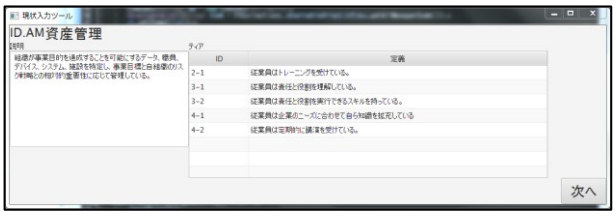

図 7　現状入力ツール

6.2　現状把握ツール

本ツールは，経営陣及び CISO が，各管理者の現状と目標を比較する為のツールである．本ツールは，図６の「（２）プロファイルで現状把握」に対応する．各管理者が現状入力ツールで入力したティアの定義に応じて，ティアの数値を一覧で表示する．合わせて，各カテゴリーの目標値も表示され，現状と目標を比較検討出来る．その他，管理者の平均値や，経営陣の主観的な評価，目標値と全体の平均値を比較したギャップが表示される（図８）．これにより，経営陣と管理者層の理解のギャップや，目標値と現状のギャップを把握することが出来る．

また，本ツールは「対策必要範囲把握機能」と「対策列挙機能」という２つの機能を有する．

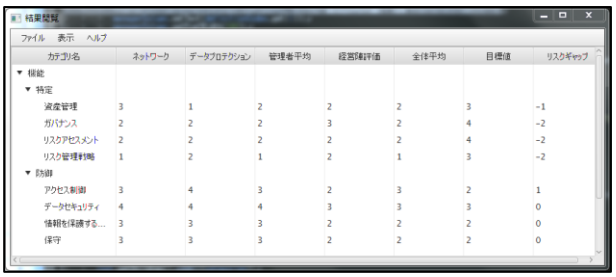

図 8　現状把握ツール

6.3　対策必要範囲把握機能

本機能は，具体的にどのティアの定義が目標に届いていないかを把握する機能である．本機能は，図６の「（４）対策必要範囲把握」に対応する．本機能は６．２節の「現状把握ツール」に付随する．本機能は対策の必要な範囲を記号で示し，経営陣や管理者層等の利用者が範囲を把握することを補助する（図９）．下記に本機能で表示される記号の意味を示す．

○：入力した現状がティア定義を満たしており，且つ目標に至るために必要な部分

●：入力した現状がティア定義を満たしているが，目標に至るために不必要な（過剰な）部分

×：目標に至るために必要だが現状満たしていない部分（対策必要範囲）

―：目標に至るために不必要な部分

△：目標に必要かつ列挙した対策で解決する部分

▲：目標に不必要かつ列挙した対策で解決する部分

「△」「▲」の仕様については６．５節で動作検証する．

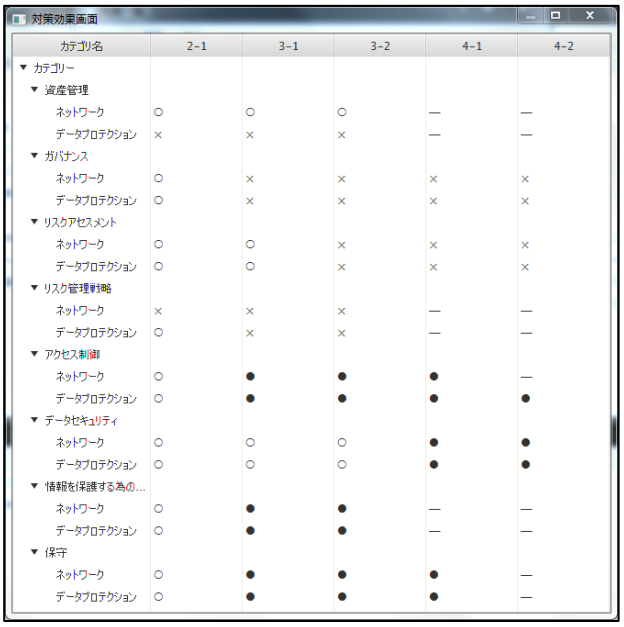

図 9　対策必要範囲把握機能

6.4 対策列挙機能

本機能は，CISO および管理者層が，５．２節の提案手法に基づき，対策によって充足するティアの定義を対策の効果として対策を列挙する機能である．本機能は，図６の「（５）対策列挙」及び「（６）対策閲覧」に対応する．本機能は６．２節の「現状把握ツール」に付随する．本機能に「対策コード」「対策名」「対策の影響を受ける管理者・カテゴリー・ティアの定義」「対策コスト」を入力することで，対策を列挙することが出来る（図１０）．なお，「対策を受ける管理者・カテゴリー・ティアの定義」は，１つの対策で複数のティアの定義を満たす場合を考慮したため，複数選択することが可能となっている．

また，列挙した対策は対策一覧画面から閲覧および削除を行うことができる（図１１）．

ここでは，６．５節で説明する対策列挙後における対策必要範囲把握機能の動作検証の為に，管理者「データプロテクション」におけるカテゴリー「資産管理」のティアの定義２－１および定義４－１を満たす対策「資産管理の教育と啓発」を列挙した．なお，対策コードは「M001」，コストは 500 とした．

図 10　対策列挙機能

図 11　対策列挙後の対策一覧画面

6.5 対策列挙後の対策必要範囲把握機能

以下の図１２は対策列挙後の対策必要範囲把握機能を示したものである．図９と図１２を比較すると，５．４節で列挙した対策の影響範囲，管理者「データプロテクション」におけるカテゴリー「資産管理」のティアの定義２－１，４－１に変化があることが分かる．則ち，定義２－１は「×」から「△」に，定義４－１は「―」から「▲」に変化している．よって，６．３節の通り，対策必要範囲把握機能から対策がどのティアの定義に対して効果を及ぼすのかを「△」及び「▲」で閲覧することが出来ることが分かる．

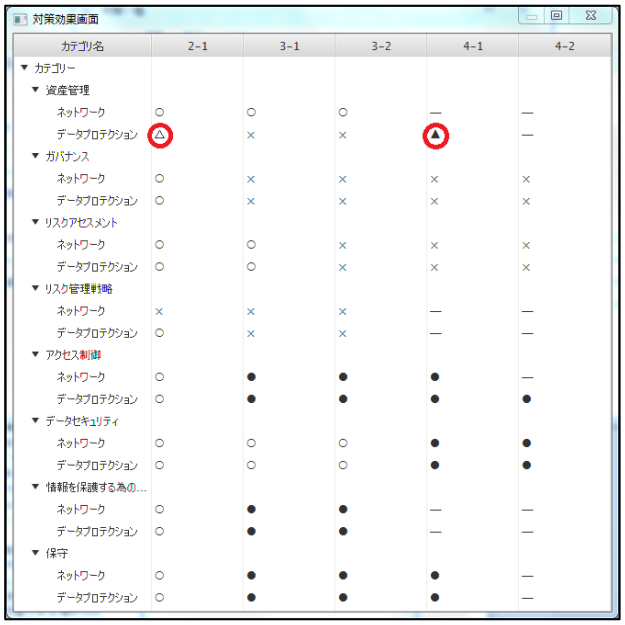

図 12　対策列挙後の対策必要範囲把握機能

7. おわりに

本研究では，米 Intel 社の CSF 利用例を基に，ティアを目標に到達させるための対策列挙手法を提案した．また，その手法に基づいた対策列挙機能及び手法の実現に必要なシステム RC4T を開発した．これにより，経営陣が現状と目標のギャップを把握した上で，ギャップを埋めるための対策及び効果を示すことが出来るため，経営陣と管理者層の共通認識を促進しつつ対策案の合意形成を補助出来る見通しが得られた．今後は，提案手法によって実際にティアが目標値に近づくかを，試適用によって検証したい．

参考文献

[1]　経済産業省：情報セキュリティガバナンス導入ガイダンス，pp.2-3　（オンライン），入手先 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf>，(2009).

[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，情報セキュリティ大学院大学，情報セキュリティ総合科学，No.2，pp.39-40　（オンライン），　入手先 <http://www.iisec.ac.jp/proc/vol0002/iisec_proc_002_p001.pdf>，(2010).

[3]　National Institute of Standards and Technology: 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，　pp.5-15（オンライン），入手先 <http://www.ipa.go.jp/files/000038957.pdf>，(2014).

[4]　Casey, T., Fiftal, K., Landfield, K., et al.: The Cybersecurity Framework in Action: An Intel Use Case, Intel Corporation, pp.1-10 (online), available from <http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/cybersecurity-framework-in-action-use-case-brief.pdf>, (2015).