データマイニング技術を活用した社会インフラシステムにおける セキュリティ対策方針立案支援手法の提案

太田原　千秋†　　井口　慎也†　　熊谷　洋子†　　萱島　信†

†日立製作所　横浜研究所
224-0817　神奈川県戸塚区吉田町２９２番地

{chiaki.otahara.qv，shinya.iguchi.uj，yoko.kumagai.su，
makoto.kayashima.hh}@hitachi.com

あらまし　社会インフラシステムのオープン化に伴い，サイバー攻撃数は増加傾向にある．これを受け，セキュリティ設計の実施が要求されている．セキュリティ設計の課題として，膨大な工期を要すること，作業者のスキルに依存した分析精度のばらつきが発生することが挙げられる．情報システム分野ではこれらの課題を解決する手法がいくつか存在する．しかし，これら従来技術は社会インフラシステムへ適用することは困難である．本稿では，社会インフラシステムを対象としたデータマイニング技術を活用したセキュリティ対策方針立案支援手法を提案する．

A Proposal of the Security Design in Social Infrastructure Systems by Means Data Mining Technology

Chiaki Otahara†　　Shinya Iguchi†　　Yoko Kumagai†　　Makoto Kayashima†

†Hitachi，Ltd.，Yokohama Research Laboratory
292，Yoshida-cho，Totsuka-ku，Yokohama-shi，Kanagawa-ken，244-0817 Japan

{chiaki.otahara.qv，shinya.iguchi.uj，yoko.kumagai.su，
makoto.kayashima.hh}@hitachi.com

Abstract As Social infrastructure systems have introduced general OS and protocol, cyber attacks tend to increase. In response, the security design process is required to be performed. The first problem is how precisely the security design process is perfumed depend on the performers skill. Hence the analysis result is not always precise. The second problem is the security design work takes too much time. Some technique to solve these problems exists in the information system. However, it is difficult to these conventional techniques apply to the security design process regarding the social infrastructure system. In this paper, we propose a security policy planning support method by means of data mining technology that target social infrastructure system.

1　はじめに

近年，社会インフラシステムの IT 化・オープン化による汎用技術の採用に伴い，社会インフラシステムに対するサイバー攻撃報告数も増加傾向にある[1][2]．この状況を受け，IEC62443[3]等，制御システム向けセキュリティ標準規格・ガイドラインが策定されている．セキュリティ設計とは，セキュアなシステムを構築するため，分析対象システムにおいて価値があるもの（以降，資産とする）に対して，発生しうる脅威の抽出を行い，抽出した脅威に対して適切なセキュリティ対策を講じるためのセキュリティ対策方針の立案を実施する一連のプロセスである．

情報システムでは，90 年代後半よりインターネットの発展に伴い，情報系システムの脆弱性を狙った攻撃が年々増加したことから，効果的かつ効率的に攻撃を防ぐためのセキュリティ設計手法が検討されてきた.そのため，情報システム分野では FT 分析を活用した対策方針立案手法[4]をはじめとするセキュリティ設計を効率的に実施するための様々な技術や支援方式が確立されている．このセキュリティ設計の特徴として，分析対象システムにおける資産の数に応じてセキュリティ設計の工期が増加することが挙げられる．社会インフラシステムは大規模システムであるがゆえ，保護すべき資産とシステム構成が膨大となるため，情報システム分野で確立された従来技術の適用が困難である．さらに，セキュリティ設計の精度は設計者の経験と知識に依存するため，複数人で作業を分担した場合に分析精度がばらつく課題がある．そこで本稿では，社会インフラシステムを対象として，既存セキュリティ分析結果の利活用を実現する対策方針立案支援手法を提案する．提案手法では、既存セキュリティ分析結果をデータマイニングの技術で機械処理可能な形式に変換し類似システム情報と比較可能な形式に変換する手順と変換方法を述べる．

第 2 章では，社会インフラシステムの特徴を，第 3 章では，セキュリティ設計の概要と手順を，第 4 章では従来の対策方針立案手法とその課題を説明する．第 5 章では，本提案手法の実現方法を説明する．最後に，第 6 章で，まとめと今後の方向性を示す.

2　社会インフラシステムの特徴

社会インフラシステムとは，社会や生活を支える公共的な基盤や仕組みのことを指す．具体的には，電力，ガス，水道をはじめ，交通など，生活に欠かせない基盤となるシステムのことを指す．近年，社会インフラシステムでは業務効率の向上のため，汎用 OS・通信プロトコルの導入が進んでいる．社会インフラシステムの特徴として，特徴の異なる情報システムと制御システムを組み合わせて構成される点が挙げられる．表 1 に情報システムと制御システムの特徴を示す.

表 1 ：情報・制御ステムの特徴

項目		情報システム	制御システム
保護対象資産		情報	機器
リスク顕在化の影響		情報漏えい 金銭的被害	人命損失
ライフサイクル		3～5 年	10～20 年
セキュリティ 三大特性の 優先度	高	機密性	可用性
	中	完全性	完全性
	低	可用性	機密性

以上より，社会インフラシステムにおけるセキュリティ設計では，制御システムと情報システムが混在する点を考慮する必要がある.

3　セキュリティ設計

3.1　セキュリティ設計の概要

セキュリティ設計では，十分でバランスのとれた適切な対策方針を確保するため，組織に内在する様々な脅威を洗い出すとともに，その影響度を分析・評価し，有効な対策を導

き出すための一連のプロセスを許容可能な工数で完了する必要がある．このため、保護すべき資産の網羅，それに対する効果的かつ合理的な対策を講じることが求められる．

一般的なセキュリティ設計手順は，以下の通りである[4].

（1） 評価対象の定義

分析対象となるシステムの範囲や前提条件，保護すべき資産などを定義する．

（2） 脅威分析・リスク評価

分析対象システムにおける資産に対して，発生しうる脅威を分析する．洗い出した各脅威に対してリスク評価をする．

（3） 対策方針立案

脅威分析とリスク評価の結果に基づき，セキュリティ対策の実施範囲を明確にし，対策方針を立案する．

（4） 要件定義

立案した対策方針を具体化した要件を定義する．

3.2 制御システムにおけるセキュリティ規格･ガイドライン

今後幅広く参照される可能性がある汎用制御システム向けのセキュリティ規格 IEC62553 では，簡易的な脅威分析を行い，分析対象のセキュリティポリシーから，システムをゾーンとコンジットに分割し，その結果からさらに詳細な脅威分析を行う．ゾーンとは，同一のセキュリティポリシーで分割しは範囲を指し，コンジットとはゾーンとゾーンの接続部分(ネットワーク)を指す．

他にもスマートグリッドシステムに関するセキュリティガイドライン NIST IR 7628[6] では，機器の特徴から実施すべきセキュリティ対策を決定する方法が行われている．以上より，社会インフラシステムにおけるセキュリティ設計に関する規格･ガイドラインでは，セキュリティ設計の簡略化が図られている．しかし, IEC62443 におけるゾーン分割でも，リスクレベルが高い箇所に関しては，ゾーンをさらに細分化して脅威分析を実施する．また，NIST IR 7628 でも同様に，具体的な要件の決定を行う際, 脅威分析を要求している．

本稿では，詳細セキュリティ設計における「対策方針立案」を対象とする．

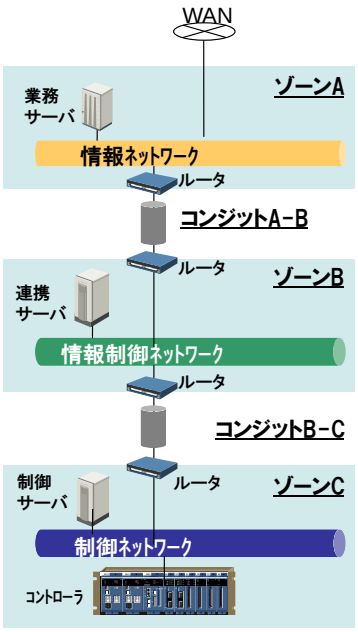

図 1 システムの分割

3.3 従来の対策方針立案手法

セキュリティ設計では，膨大な工期を要すること，分析精度のばらつきが課題として存在する．対策方針立案では，特にセキュリティ知識・セキュリティ設計経験を要する作業であるため，作業者によって分析精度が依存する傾向が高い．そのため，多くの時間と労力を要する. そこで, 情報システム分野では，これらの課題を解決するため，いくつかの対策方針立案の支援手法が存在する．情報システム分野を対象とする対策方針立案支援手法の 1 つに，資産・脅威・対策方針の組み合わせをモデル化することで対策方針立案支援を実現する手法[7] (以下，資産・脅威・対策方針モデル化手法) が挙げられる．資産・脅威・対策方針モデル化手法では，セキュリティ専門家がセキュリティ対策を決定する際の手順を模範にし，「資産と脅威の関係」と「脅威と対策の関係」に分け，資産・脅威・対策方針モデル化を行うことで，セキュリティ知識

がなくとも，対策方針を立案することが可能となる．さらに，選択した対策の組み合わせ毎に対策コストと平均残存資産を算出し,「残存リスクー対策コスト」の期待値を最大にするというアプローチにより，対策方針の導出を行う．

3.4　従来技術の課題

資産・脅威・対策方針モデル化手法を社会インフラシステムに適用した場合,「残存リスクー対策コスト」の期待値算出に要するコストに関連するパラメータを設定しており，可用性が重視される機器では運用やシステム構成面での対策が導入される場合が多いことから ，資産・脅威・対策方針モデル化手法による対策方針の選定方法では，適用が困難であるといえる．

情報システム分野で確立された従来技術を社会インフラシステム分野に適用すると、システムが大規模であるがゆえ，脅威が数千～数万個抽出されることもあり，セキュリティ設計に膨大な工期を要するという課題が残る．また，情報システムと異なり，社会インフラシステムでは，可用性を重視する必要があるなど(2 章参照)，対策実施箇所のシステム特性を考慮する必要がある．さらに脅威数が膨大なため、作業を複数人で行うこととなる．そのため，セキュリティ設計の精度は設計者の経験とセキュリティ知識に依存するという特徴から，分析精度がばらつく課題がある．

4　既存セキュリティ設計結果利活用を実現する対策方針立案手法

本稿では，社会インフラシステムを対象として，対策方針立案の工期削減を実現するため，データマイニング技術を活用した対策方針立案支援手法を提案する．

4.1　本提案手法の概要

本提案手法では，既存セキュリティ分析結果に対してデータマイニングを行い，有用な情報を抽出し，活用することを目的とする。

データマイニングは，大量のデータから有用な知識を取り出すための一連のプロセスである[7]．データマイニングは通常，大きく 4 つのステップで構成される．

- 第 1 ステップ：関連するデータを獲得・選択するプロセス
- 第 2 ステップ：関連するデータに前処理と変換を施すプロセス
- 第 3 ステップ：データからパターンを発見するプロセス
- 第 4 ステップ：パターンを解釈・評価し，知識として活用するプロセス

本稿では，有用なパターンを発見することを目的として，セキュリティ分析結果の情報変換方法について述べる．

本提案手法の処理概要は，以下の通りである(**図 2** 参照)．ちなみに，**図 2** における「脅威特徴ー対策方針パターン」は既存セキュリティ分析結果から，テンプレート化により脅威特徴を作成し，紐づく対策方針の情報を格納したものである．

- 処理 1：入力となる，脅威分析結果一覧とリスク評価一覧をテンプレート化する
- 処理 2:処理 1 で作成した脅威特徴を「脅威特徴ー対策方針パターン」の情報とマッチングする

処理 1 の詳細は 4.2 節で，処理 2 の詳細は 4.3 節で説明する。

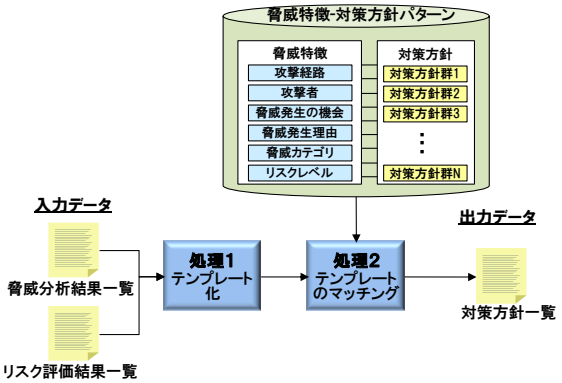

図 2 既存セキュリティ設計結果利活用を実現する対策方針立案支援手法の処理概要

4.2 テンプレート化

対策方針立案では，脅威分析とリスク評価の結果を踏まえて行う．脅威分析では，「資産」「攻撃経路」「攻撃者」「脅威事象」を明確にする必要がある.またリスク評価では，脅威分析で洗い出した脅威に対して「資産」「脅威」「脆弱性」の観点からリスク評価を行う[9]．この対策方針立案の工程で，既存セキュリティ設計を利活用するためには，対策方針立案時に用いる脅威分析とリスク評価の情報(以下，脅威特徴とする)を，比較可能な形式の情報にする必要がある(以下,テンプレート化)．

既存セキュリティ設計結果における脅威特徴の比較を可能とするため，以下の通り指標を定義した．

（1）脅威発生箇所

保護すべき資産を保有する脅威発生箇所の種別と重視するセキュリティ特性によって，対策方針は異なることから，脅威発生箇所の指標を**表 1**，**表 2** の通り定義する．

表 1 脅威発生箇所の種別指標

機器	可搬型媒体
	非可搬型媒体
NW	広域ネットワーク
	狭域ネットワーク

表 2 脅威発生箇所の重視するセキュリティ特性指標

機密性	資産における機密性を重視する
完全性	資産における完全性を重視する
可用性	資産における可用性を重視する

（2）攻撃者

対策を導入する際，攻撃者が内部者か外部者か，また攻撃者のスキルが高いか低いかによって，実施すべき対策が異なることから，攻撃者に関する指標を**表 3**，**表 4**，**表 5** の通り定義する．攻撃者のポジション指標の作成に当たり，共通脆弱性評価システム(CVSS)[10]における攻撃前の認証要否を適用した．また，攻撃者のスキル指標の作成に当たり，CVSS の攻撃条件の複雑さを社会インフラシステムに合わせて定義を行った．攻撃者のスキル指標におけるゾーンは，IEC62443 におけるゾーンと同義であり，ネットワーク構成とセキュリティポリシーからゾーン分割したものとする．さらに，攻撃者の存在箇所指標の作成に当たり，CVSS における攻撃元区分を適用した．

表 3 攻撃者のポジション指標

複数	攻撃する場合，2 つ以上の物理認証が必要である ＝外部者
単一	攻撃前に物理認証が必要である ＝権限ない内部者
不要	攻撃前に物理認証が不要である ＝権限ある内部者

表 4 攻撃者のスキル指標

高	資産までのゾーンが 2 つ以上
中	資産までのゾーンが隣接したゾーン
低	資産が同一ゾーン内

表 5 攻撃者の存在箇所指標

ローカル	資産への物理アクセスが可能
隣接	資産があるゾーン/コンジットへの接近が必要
ネットワーク	資産があるゾーン/コンジットへの接近が不要

（3）脅威発生の機会

システムのライフサイクルにおけるどのタイミングで脅威が発生するかにより，対策方針が異なることから，脅威発生の機会を一般的なシステムのライフサイクルから，**表 6** の通り定義する．

表 6 脅威発生の機会指標

開発	システムの開発時に発生しうる脅威
運用	システムの運用時に発生しうる脅威
保守	システムの保守時に発生しうる脅威

（4）脅威発生理由

関係者の過失による脅威の発生では，運用面での対策方針が実施されることが多い．そのため，脅威が発生する際，攻撃者が故意

か過失かによって対策方針が異なる.そこで,脅威発生理由の指標を**表 7** の通り定義する.

表 7 脅威発生理由指標

故意	悪意を持つ目的・意図のある攻撃
過失	悪意を持たない過失による攻撃

(5)脅威カテゴリ

資産に対して，どのように脅威を引き起こすかによって，対策方針が異なる．例えば，資産が漏えいすることにより脅威が発生する場合，対策として「暗号化」を講じることとなる．資産になりすまされることにより脅威が発生する場合，対策として「認証」講じることとなる.そこで,脅威カテゴリの指標を,Microsoft 社が提唱する脅威モデル[11]より,**表 8** の通り定義する.

表 8 脅威カテゴリ指標

なりすまし
改ざん
否認
情報漏えい
サービス拒否
特権昇格

(6)リスクレベル

リスクレベルは，「資産」「脅威」「脆弱性」から評価される．これらの指標からリスク値を算出し，対策を実施する脅威を選定する．脅威が発生した場合どれほどインパクトがあるかを考慮して対策を立案するため，リスクレベルのうち,資産価値を考慮するため,FIPS199[12]より，リスクレベル指標を**表 9** の通り定義した.

テンプレート化の例として，**表 10**脅威分析と**表 11**リスク評価があったとする．ここで,表10～12で登場する,サーバAは図 1におけるゾーンAに，サーバBとセンサーAは図 1におけるゾーンCに存在するものとする.

表 9 リスクレベル(資産価値)指標

	低	中	高
機密性	資産の不正開示により，業務や資産，または個人に限定的な悪影響を及ぼす	資産の不正開示により，業務や資産，または個人に重大な悪影響を及ぼす	資産の不正開示により，業務や資産，または個人に致命的または壊滅的な悪影響を及ぼす
完全性	不正な資産の改変･破壊により，業務や資産，または個人に限定的な悪影響を及ぼす	不正な資産の改変･破壊により，業務や資産，または個人に重大な悪影響を及ぼす	不正な資産の改変･破壊により，業務や資産，または個人に致命的または壊滅的な悪影響を及ぼす
可用性	業務の実行ができないことにより，業務や資産または個人に限定的な悪影響を及ぼす	業務の実行ができないことにより，業務や資産または個人に重大な悪影響を及ぼす	業務の実行ができないことにより，業務や資産または個人に壊滅的な影響を及ぼす

表 10の脅威分析結果の「脅威発生箇所」「攻撃者」「攻撃タイミング」「動機」「脅威カテゴリ」と**表 11**リスク評価の「資産」からテンプレート化した例が，**表 12**である．**表 12** に記載の(1)～(6)は，5.2節に対応している.

表 10 脅威分析の例

脅威ID	資産	攻撃経路		攻撃者	攻撃タイミング	動機	脅威事象	
		脅威発生箇所	攻撃者の存在箇所				脅威カテゴリ	脅威詳細
T1	制御命令A	サーバA	サーバB	内部者	運用	故意	改ざん	内部者が，サーバBからサーバAへ改ざんした不正な制御命令を送信する
T2	測定値A	センサーA	サーバA	第三者	運用	故意	サービス拒否	第三者がサーバAからセンサーAにDoS攻撃を行う
…	…	…	…	…	…	…	…	…

表 11 リスク評価の例

脅威ID	資産			攻撃可能性	リスク値
	機密性	可用性	完全性	脅威×脆弱性	
T1	高	高	高	低	中
T2	中	低	中	中	中
…	…	…	…	…	…

表 12 脅威特徴のテンプレート例

脅威ID	(1) 脅威発生箇所		(2) 攻撃者			(3) 脅威発生の機会	(4) 脅威発生理由	(5) 脅威カテゴリ	(6) リスクレベル(資産価値)		
	種別	特性	ポジション	スキル	存在箇所				機密性	可用性	完全性
T1	非可搬型機器	可用性重視	不要	高	ネットワーク	運用	故意	改ざん	高	高	高
T2	可搬型機器	機密性重視	複数	中	ネットワーク	運用	故意	サービス拒否	中	低	中
…	…	…	…	…	…	…	…	…	…	…	…

4.3 テンプレートのマッチングと検証結果

本提案では，データマッチング技術を用いることでテンプレートのマッチングを行う．マッチングにはコサイン類似度以外の手法も適用可能だが，本稿における検証では，代表的な検索モデルの 1 つである，ベクトル空間モデルに基づくコサイン類似度を適用する[13]．今回コサイン類似度により類似度を算出するため，各脅威特徴をベクトルで表す．脅威特徴の各項目のテンプレートにおいて，該当するパラメータを「1」，該当しないパラメータを「0」とすることで各脅威特徴をベクトル表現する(図 3 参照)．例えば，**表 12** における脅威 ID：T1 の「脅威発生箇所」は非可搬型媒体かつ可用性重視であるため，ベクトル表現すると，(0,1,0,0,0,0,1)となる．脅威 ID:T01 の脅威特徴をベクトル表現すると以下の通りになる．

$$T_1^T = (0,1,0,0,0,0,1,0,0,1,1,0,0,0,0,1,$$
$$0,1,0,0,1,0,1,0,0,0,0,1,0,0,1,0,0,1,0,0)$$

このように脅威特徴をベクトル表現することで，各脅威の類似度が判定可能となる．本稿での検証では，完全マッチングによる判定を行った．実際に，既存セキュリティ設計結果を用いて，有効性を確認する．検証に当たり，セキュリティ設計結果の公開は出来ないため，マッチングの結果を記す．

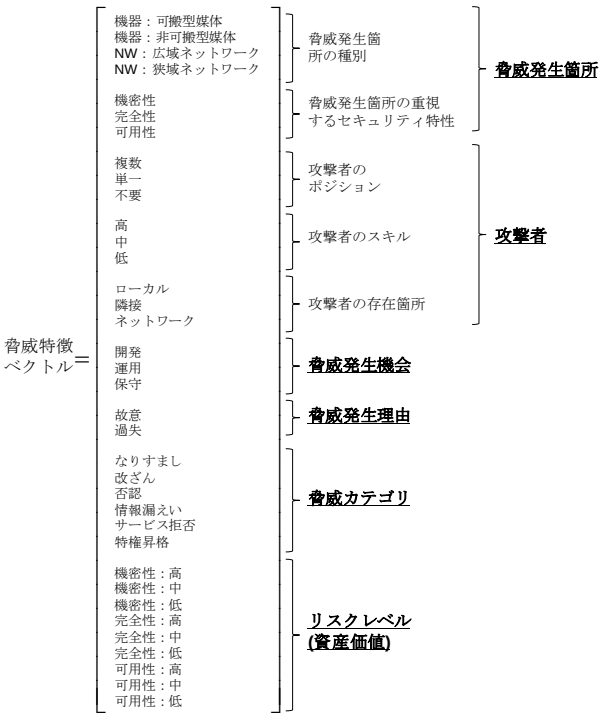

図 3 脅威特徴ベクトル

検証では，図 4 で示す通り，分析対象システム A のセキュリティ設計結果から，予め脅威特徴のテンプレート化を行い，「脅威特徴–対策方針パターン」を作成した．次に入力データとして，分析対象システム A における業務フローA に関する脅威分析結果とリスク評価結果をテンプレート化し，「脅威特徴–対策方針パターン」との完全マッチングを行った．結果，実際に立案した対策方針と完全に合致する結果を抽出できることを確認した．今後，入力データと脅威特徴パターンが部分的にマッチする場合においても妥当な対策を抽出できる手法を検討する．

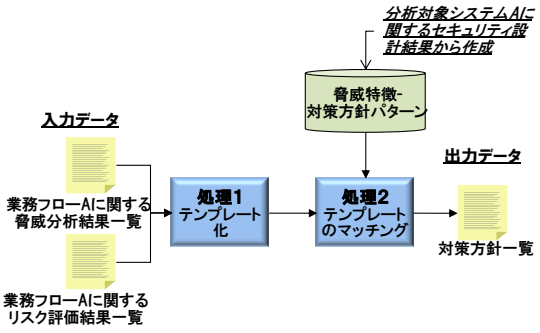

図 4 テンプレート検証の概要

5　まとめと今後の課題

本稿では，社会インフラシステムにおけるセキュリティ設計の対策立案における工期削減と分析精度のばらつき改善を目的として，データマイニングの考えを導入し，推奨される対策方針を導出する手法を検討した．社会インフラシステムにおける対策方針立案の工期削減を実現するため，既存セキュリティ分析結果を活用して新たな分析対象に対して推奨対策方針を出力する手法を提案した．本手法では，データマイニングの技術を活用し，既存セキュリティ分析結果を機械処理可能なベクトル表現に変換することで比較を可能とした．また，コサイン類似度を用いることで，類似脅威の抽出を可能とした．本手法を実案件で適用した結果，完全マッチングにより，実際に立案された対策方針を導出することを確認した．

今後は本手法の精度を向上するため，以下の検討が必要と考える．

（1）パラメータの妥当性の検証
（2）テンプレートのパターンマッチングに最適な手法の検討
（3）脅威特徴の各項目と対策方針の依存度を考慮した部分マッチングによる対策方針立案手法の考案

参考文献

[1] ICS-CERT,　ICS-CERT Incident Response Summary (2009-2011),　2011

[2] ICS-CERT,　ICS-CERT Year in Review 2012,　2012

[3] 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

[4]IEC,　Industrial communication networks – Network and system security – Part2-1:Establishing an industrial automation and control system security program,　2013

[5]ISO/IEC,　Information technology – security techniques－ evaluation criteria for it security – Part1: Introduction and general model,　2005.

[6]NIST,　NIST IR 7628 -Guidelines for Smart Grid Cyber Security- ,　2010

[7]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，pp2022-2033，2004

[8] 元田浩，津本周作，山口高平，沼尾正行，データマイニングの基礎，オーム社，2006

[9]ISO/IEC,　Information technology –Security techniques- Code of practice for information security controls，2013

[10]ITU-T,　SERIES X: DATA NETWORKS,　OPEN SYSTEM COMMUNICATIONS AND SECURITY Cybersecurity information exchange – Vulnerability/state exchange，2011

[11] Frank Swidersk,　Window Snyder,　脅威モデルーセキュアなアプリケーション構築ー，日経BPソフトプレス，2005

[12]NIST,　FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION,　Standards for Security Categorization of Federal Information and Information Systems,　2004

[13] 北研二，津田和彦，獅子堀正幹，情報検索アルゴリズム，共立出版，2002