情報処理学会論文誌　Vol. 52　No. 9　2575–2585 (Sep. 2011)

情報セキュリティ対策間の相互依存関係を用いた内部犯行防止対策のための有効性評価手法

鈴木智也[†1]　田沼均[†2]　今井秀樹[†1,†2]

情報化が進んだ今日，情報セキュリティに関わる内部犯行も重要な問題である．これに対応するためには内部犯行防止に必要な情報セキュリティ対策を実施し，適切な防御体制を敷く必要がある．本稿ではフォールトツリー分析手法を応用し，内部犯行防止に不足する情報セキュリティ対策を適切に指摘する手法を提案する．本手法では情報セキュリティ対策間の相互依存関係に注目し，内部犯行に対する情報セキュリティ体制（実施している情報セキュリティ対策の集合）の有効性を評価し，不足する情報セキュリティ対策を指摘する．対策指摘の手順は，(1) 関連する情報セキュリティ対策の抽出，(2) 情報セキュリティ体制の有効性評価，(3) 不足する情報セキュリティ対策の指摘，の 3 つのプロセスからなる．対策間の相互依存関係の分析にあたっては，情報セキュリティ対策集として充実している ISO/IEC 27002 を用いる．さらに本手法検証のために，実際の事故事例に対し 5 つのケーススタディを行い，うち 1 つを詳細分析した結果，他の情報セキュリティ対策では代替できない 1 つの不足する情報セキュリティ対策を指摘できた．

An Evaluation Method against Insider Threat Based on Interdependent Relationship for Information Security

Tomoya Suzuki,[†1] Hitoshi Tanuma[†2] and Hideki Imai[†1,†2]

Information security against insider threat is indispensable in our information society. It has been seriously required to institute sufficient information-security measures against insider threats. In this paper, we propose a method which indicates the missing information-security measures against insider threats. In particular, we focus on the interdependent relationship of information-security measures based on ISO/IEC 27002 to get the effectiveness evaluation of currently used measures for information security. The method uses a fault tree analysis technique and consists of three processes: (1) an extraction of the related information-security measures, (2) an effectiveness evaluation of currently used measures for information security and (3) an indication of the missing information-security measures. The validity of the proposed method is verified by applying it to the actual information-security accidents.

1. はじめに

近年，情報漏洩をはじめとする情報セキュリティに関わる内部犯行が問題となっている．内部の者による攻撃や外部の攻撃者と内部の協力者が連携する攻撃に対しては，外部からの攻撃のみを想定した防御体制では不十分であり，情報セキュリティ上の脅威が残る．そのため，内部犯行防止のための情報セキュリティ対策（以下，管理策）の実施は必須である．しかし，多くの内部犯行防止に関連する管理策の効果は不明確であるため，内部犯行防止対策が進んでいない組織も多い．

これまで内部犯行者の動機や内部犯行の防止に関して多くの研究がなされてきた．これにより内部犯行を行う動機の抑制，内部犯行の検知が可能となった．しかし，内部犯行防止に対する管理策や情報セキュリティ体制（以下，管理体制）の評価に関しては，明確な基準は存在しない．内部犯行を防止するには内部犯行におけるリスクを評価し，そのリスクに有効な管理体制を敷く必要がある．つまり，内部犯行に対する管理体制の有効性を評価することができれば，内部犯行を防止・検知できる．

組織は内部犯行防止のために有効と考える様々な管理策を実施する．内部犯行防止の効果は実施した管理策の総体，すなわち実施した管理策集合により決まる．そこで管理体制とは実施している管理策の集合と考えることができる．さらに管理策間には，ある管理策を有効とするために前提となる管理策，ある管理策を補間する管理策，といった相互依存関係を持つものがある．つまり組織の内部犯行防止の有効性を評価するには，その組織の管理策の集合である管理体制に対し，管理策間の相互依存関係を考慮した評価を行う必要がある．

本稿では管理策間の相互依存関係に着目して，内部犯行防止に不足する管理策を適切に指摘する手法を提案する．管理策は単独で機能せず，1 つの管理策を満足するには複数の管理策を必要とするため，管理策間には相互依存関係が存在する．その相互依存関係に基づい

†1 中央大学理工学研究科
Graduate School of Science and Engineering, Chuo University
†2 産業技術総合研究所情報セキュリティ研究センター
Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST)

て，内部犯行防止に対する管理策の効果および管理体制の有効性を評価する．本手法では，内部犯行防止に直接的に有効である管理策を抽出し（3.2.1 項参照），ここで抽出した管理策を内部犯行防止に有効な要件と考える．この要件を管理策間の相互依存関係に基づいて展開し，内部犯行防止に効果がある管理策のすべてを抽出する．個々の管理策の効果は，内部犯行防止に対するその管理策の影響である．この影響を「内部犯行防止に有効な要件に対し，その管理策の寄与する要件の割合」とし，影響程度と呼ぶ．また，管理体制とは実施した管理策の集合であるので，管理体制の有効性を「管理体制に属する管理策の影響程度の総和」とし，機能程度と呼ぶ．つまり，効果の高い管理策は内部犯行防止に重要であり，有効性の高い管理体制は内部犯行に対して十分な防御体制である．また，管理策間の相互依存関係を分析するにあたって，分析手法としてフォールトツリー分析手法（Fault Tree Analysis，以下，FTA）[1]，管理策集として ISO/IEC 27002 [2] を用いた．

以下，2 章では内部犯行と先行研究の調査に基づき，解決したい課題について述べる．3 章では提案手法の詳細を説明し，4 章では実際に事例を用いて提案手法の検証を行う．最後に 5 章で今後の課題とともに本研究についてまとめる．

2. 内部犯行と解決したい課題

2.1 内 部 犯 行

内部犯行について様々な研究が行われている．特に犯行者の動機[3)–6)] や犯行を行う機会[7] などの犯罪学の立場からの研究[8)–10)] が数多く存在する．また，Theoharidou ら[11] は ISO/IEC 17799 [12] を分析し，ISO/IEC 17799 が犯罪学上も有効であることを示している．さらに最近では犯罪学の理論にとらわれず，内部犯行の分析が行われている．たとえば Schultz [13] は環境や言葉の振舞いから内部犯行発生の予測を行っている．Hui ら[14] は内部犯行保護のためのフレームワークを提案し，Pfleeger ら[15] は内部犯行の分類法を提案している．また，Hunker ら[16] は経済学の観点から内部犯行を分析している．しかし，内部犯行に対する管理体制の有効性評価について，明確な基準を与えた研究は存在しない．

一方，カーネギーメロン大学に設置されているコンピュータ緊急対応センター（Conpyuter Emergency Respones Team．以下，CERT）でも内部犯行に対する様々な調査が行われている．内部犯行の防止・探知のための共通ガイドライン[17] では事例分析を行い，内部犯行を防止・探知するために有効な管理策を解説している．他にも金融[18] や知的財産[19]，コンピュータ破壊[20] を対象としたものなど活発に調査が行われている．しかし，これらは内部犯行の実情を調査したものであり，体系的に管理体制の有効性を評価していない．

> 現，若しくは元従業員，契約者，又はビジネス・パートナーで次に該当する者をいう．
> - 組織のネットワーク，システム，又はデータへのアクセスが与えられている者，又は与えられていた者で，
> - 組織の情報若しくは情報システムの機密性，完全性，又は有用性に悪影響を与えるような方法で，このアクセスレベルを故意に越えて使用する者又はこのアクセスを悪用する者

図 1　CERT の悪意ある内部犯の定義[17]
Fig. 1　Definition of insider threat in CERT [17].

2.2 先行研究と解決したい課題

本稿では対象とする内部犯行として CERT の定義を用いる[17]．CERT の調査は詳細で内部犯行に明確な定義を与えている．CERT の内部犯の定義を**図 1**，具体的な犯行の種類を**図 2** に示す．

情報セキュリティにおいて管理策を実施するためには想定されるリスクを抽出し，そのリスク防止に必要な管理策を実施する必要がある．本稿では情報セキュリティ全般に対する管理策集として情報セキュリティマネジメントシステムの国際規格である ISO/IEC 27002 [2] を用いた．ISO/IEC 27002 中の管理策の「参照」という記述に着目して管理体制の有効性を評価し，不足する管理策を指摘する．同様の試みとして，高橋ら[21),22)] が行った ISO/IEC 17799 管理策の新しい分類基準の検討がある．

一方，システムの評価に関して対象システムに想定されるリスクを抽出し，その発生頻度，損失額から影響の度合いを評価するリスク分析手法が提案されている．宝木ら[23)] は故障分析に用いられていた FTA を用いて，不正行為に起因するセキュリティ事象のリスク分析を行う手法を提案した．さらに織茂ら[24)] は宝木らの手法の考え方を発展させ，ターゲットになるシステムに対応したセキュリティ対策を体系的に実施するためのセキュリティ計画手法を提案した．しかし，この手法は情報システムのセキュリティ機能とその保証という機器認証（ISO/IEC 15408 [25)]）に主眼を置いたものであり，情報セキュリティ管理が主眼ではない．また佐々木ら[26)–28)] はリスクに直接，間接に関係する人々の合意を形成するために多重リスクコミュニケータを提案した．しかし，これらの研究では管理策の効果および管理策に要するコストについては専門家が決定するとし，具体的な指定はない．

本稿では管理策間の相互依存関係を明らかにし，内部犯行防止に不足する管理策を適切に指摘する手法を提案する．現状では内部犯行防止に対する管理策の効果および，管理策間

IT サボタージュ：現，もしくは元従業員，契約者，又はビジネス・パートナーが，特定の個人，組織，又は組織のデータ，システム及び日常の業務遂行を害するために，ネットワーク，システム，又はデータへの許可されたアクセスレベルを意図的に超えた又は悪用した事例.

金銭的利益のための窃盗又は改ざん：現，もしくは元従業員，契約者，又はビジネス・パートナーが，経済的利益のために，組織の機密又は専有情報（企業が知的所有権を有する情報）を窃取，又は改ざんする意図をもって，ネットワーク，システム，又はデータへの許可されたアクセスレベルを故意に超えた，又は悪用した事例.

ビジネス上の利益のための窃盗又は改ざん：現，もしくは元従業員，契約社員，又はビジネス・パートナーが，ビジネス上の利益を目的のために，組織の機密又は専有情報を窃取，又は改ざんする意図をもって，ネットワーク，システム，又はデータへの許可されたアクセスレベルを故意に超えた，又は悪用した事例.

その他：現，もしくは元従業員，契約社員，又はビジネス・パートナーが，経済的利益以外，又はビジネス上の利益以外の動機により，組織の機密又は専有情報を窃取する意図をもって，ネットワーク，システム，又はデータへの許可されたアクセスレベルを故意に超えた，又は悪用した事例.

図 2　内部犯行の種類[17)]
Fig. 2　Types of insider threats [17)].

の相互依存関係は明確化されていない．また，1 つの管理策を満足するには複数の管理策を必要とするため，管理策間には相互依存関係が存在する．そこで管理策間の相互依存関係を把握し，管理策群を構造化することができれば管理策の効果を明らかにできる．さらに，管理策の効果を明らかにすれば管理体制の有効性を評価でき，内部犯行を防止・検知する管理策を適切に指摘できる．

3. 内部犯行に対する管理体制の有効性評価手法

3.1 提案手法の概要

本稿では内部犯行防止に不足する管理策を適切に指摘する手法を提案する．本手法は管理策間の相互依存関係に基づいて，管理策の効果および管理体制の有効性を評価することで，管理体制にとって必要な管理策を過不足なく適切に指摘するものである．本手法では，内部犯行防止に直接的に有効である管理策を抽出し（3.2.1 項参照），ここで抽出した管理策を内部犯行防止に有効な要件と考える．この要件を管理策間の相互依存関係に基づいて展開し，内部犯行防止に効果がある管理策のすべてを抽出する．個々の管理策の効果は，内部犯行防止に対するその管理策の影響である．この影響を「内部犯行防止に有効な要件に対し，その管理策が寄与する要件の割合」とし，影響程度と呼ぶ．また，管理体制とは実施した管理策の集合であるので，管理体制の有効性を「管理体制に属する管理策の影響程度の総和」とし，機能程度と呼ぶ．つまり，内部犯行防止に重要な管理策は有効性に寄与する影響程度が高く，内部犯行防止に有効な多くの管理策を実施している管理体制は有効性が高い．提案手法では管理策間の相互依存関係を明らかにするために，内部犯行防止に関連する管理策を FTA により木構造で表現する．手法の手順として，(1) 関連する管理策の抽出，(2) 管理体制の有効性評価，(3) 不足する管理策の指摘，の 3 つのプロセスが存在する．以下，手順に沿って提案手法を説明する．

3.2 関連する管理策の抽出

3.2.1 有効な管理策の抽出

内部犯行に対する管理体制の有効性を評価するためには，まず内部犯行防止に関連する管理策をすべて抽出する必要がある．そのために内部犯行防止に有効であると示された管理策に対し，その管理策と相互依存関係がある管理策をすべて抽出する．内部犯行防止に有効な管理策は，CERT の調査[17)] に基づいて抽出した．この調査をもとに，本手法の中心となる管理策として内部犯行防止に有効な 16 項目の管理策（以下，有効管理策）を抽出した．ここで抽出した管理策を中心に内部犯行防止に関連する管理策を抽出し，管理策間の相互依存関係を構造化する．CERT の調査では内部犯行防止に直接効果のある管理策しか示されていないため，関連する管理策の抽出には情報セキュリティ全体を対象とした管理策集を利用する．

3.2.2 有効な管理策を満足するための管理策の抽出

内部犯行防止に関連する管理策間の相互依存関係を構造化するために，内部犯行防止に関連する管理策をすべて抽出する．内部犯行防止に直接効果のある管理策だけでなく，関連する管理策をすべて抽出するために管理策集として充実している ISO/IEC 27002[2)] を用いた．

まず，有効管理策と同様の効果を期待できる管理策として，ISO/IEC 27002 に掲載されている 58 項目の管理策（以下，当該管理策）を選び出した．CERT では，管理策ごとに内部犯行防止のための要件を示しているため，その要件を満たすように当該管理策を選び出した．

次に，当該管理策を中心に内部犯行防止に関連する管理策をすべて抽出する．そのため

6.2.3　第三者との契約におけるセキュリティ

管理策

組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい．

実施の手引き

契約は，組織と第三者との間に誤解がないことを確実にすることが望ましい．組織は，第三者の補償について納得していることが望ましい．

明確になったセキュリティ要求事項（6.2.1 参照）を満たすために，契約には，次の事項を含めることを考慮することが望ましい．

図 3　「参照」の例[2)]
Fig. 3　An example of "see" description [2)].

に，ISO/IEC 27002 の「参照」という記述を利用し，当該管理策を満足するために必要な管理策をすべて抽出した．当該管理策およびそれを満足するための管理策が内部犯行防止に関連する管理策となる．

本稿では「参照」を次のように定義する．1 つの管理策を満足するために，いくつかの要件が存在する．ISO/IEC 27002 ではその要件の記述中に**図 3** のような「参照」という記述がある．参照先の管理策は参照が記述されている管理策を満足するために必要な管理策とする．この関係性を「直接参照」とする．直接参照を用いることで，管理策の要件を自身のみで満たせる要件と参照を必要とする要件とに展開できる．そのため，直接参照には参照先の管理策に展開元の管理策の一部を含める．展開元の要件を「管理策（要件）」，展開先の一部を「管理策（実施策）」と表記する．また，直接参照した管理策がさらに直接参照する管理策も元の管理策にとって必要な管理策となる．このような関係性を「間接参照」とする．そして，直接参照と間接参照を合わせたものを「参照」とする．

本稿では，管理策中の「管理策」という項目に記述されている「参照」についてのみを用いて管理策を抽出した．58 項目の当該管理策それぞれに対して「参照」を用いることで，当該管理策を満足する管理策として延べ 3,324 項目の管理策（以下，参照管理策）を抽出した．これが内部犯行防止に関連する管理策となる．

3.3　管理体制の有効性評価

3.3.1　有効性評価の方針

管理体制の有効性を評価するためには，管理策が内部犯行防止に寄与する影響程度を把握する必要がある．そのため，FTA を用いて抽出した内部犯行防止に関連する管理策の相互依存関係を構造化する．FTA は故障の発生原因をトップダウンに分析し，その結果を用いて信頼性解析を行うための手法であり，長年の実績から確立された手法である．FTA は以下の 2 つのフェーズからなる．

(1)　故障原因の分析，Fault Tree の作成（本手法では管理策間の相互依存関係の構造化に相当する）

(2)　Fault Tree に数値を付与することによる信頼性解析（本手法では内部犯行防止に寄与する影響程度を付与することによる有効性解析に相当する）

FTA はリスク管理においても脅威の発生要因の分析[24)] などに利用されている．提案手法では FTA を用いて (1) を実施することにより，内部犯行防止に関連する管理策の抽出・構造化を行い，(2) を実施することにより，内部犯行に対する管理体制の有効性を評価する．

通常 FTA では望ましくない事象を頂上に置きその事象が発生する条件を展開する．しかし，提案手法では頂上事象に「内部犯行に対する管理体制」という望ましい事象を置きその事象が要件を達成する条件を展開する．この違いは，通常の FTA が故障原因の解析を主な目的にするのに対し，提案手法では実施している管理策により内部犯行がどの程度防止できるか評価することを目的としているためである．つまり，提案手法は FTA の構造を利用して管理策の実施による内部犯行防止への影響を求め，その影響の大小により内部犯行防止の効果を評価しており，内部犯行の発生確率を求めているわけではない．このため頂上に望ましい事象である「内部犯行に対する管理体制」を置き，管理体制が完全に実施された場合の要件を展開して，評価の基盤となる木構造を構成する．この木構造は厳密には FTA で使われる Fault Tree とは異なるが，非常に Fault Tree と類似した構造となるため本稿ではこの木構造も Fault Tree と呼ぶこととする．

3.3.2　管理策間の相互依存関係の構造化

Fault Tree ではルートである頂上事象から始め，それぞれの事象を詳細化することにより構造化を実現する．提案手法では頂上事象に「内部犯行に対する管理体制」，1 次事象に「有効管理策」，2 次事象に「当該管理策」を配置し，当該管理策を「参照」に基づいて展開する．これにより頂上事象を内部犯行に対する管理体制として，内部犯行防止に関連する管理策をすべて構造化できる．

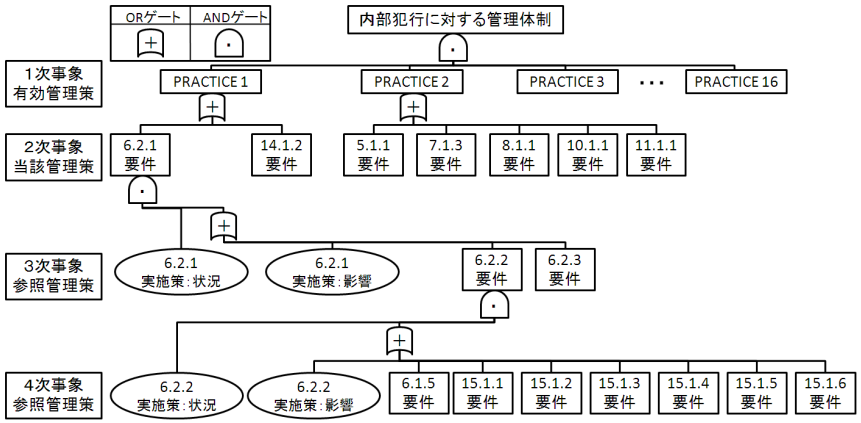

図 4　内部犯行防止に関連する管理策の構造の一部
Fig. 4　A part of structure of measures against insider threats.

「参照」という関係性は階層関係にあるため，この関係性を分岐数に制約のない木構造で表現できる．各管理策を「節点」とし，「親」である管理策に参照先として記述されている管理策を「子」とする．「子」とされた管理策に対しても「参照」が存在するかをたどり，木を作成する．なお「子」となる管理策が生成している木内にすでに存在する場合は省く．このようにして内部犯行防止に関連する管理策を論理的に展開し，それ以上展開できない事象（以下，基本事象）に至るまで続け，関連する管理策をすべて構造化する．**図 4** は内部犯行防止に関連する管理策の構造の一部であり，図 4 中の円形で囲まれた事象が基本事象である．

管理策の展開には，OR ゲートや AND ゲートなどの論理ゲートを使用する．OR ゲートは下位事象のどれかが生起したときに上位事象が発生する場合に用いられ，下位事象の数値の加算値を上位事象の数値とする．提案手法では評価値として確率ではなく上位事象の達成に有効な要件に対し，下位事象が寄与する要件の割合を算出し，必要とする管理策の満足の度合いにより評価する．たとえば上位事象の要件を満たすために 2 つの管理策が必要な場合は 2 つの管理策をともに実施すれば上位事象の要件が満たされたとし，片方のみ実施した場合は半分の実施，すなわち満足の割合が 50%と評価する．また，AND ゲートは下位事象のうちのすべてが生起したときに上位事象が発生する場合に用いられ，下位事象の数値の積算値を上位事象の数値とする．

このような展開を実施することにより，基本事象から中間の事象を経て頂上事象に至るまでの事象間の因果関係を論理的に明らかにできる．そのため，頂上事象である内部犯行に対する管理体制を適切に機能させるにはどの基本事象が重要なのか検討できる．通常の FTA では障害発生の確率を計算するが，提案手法では内部犯行防止の要件の満足割合をもって評価する．これは評価を簡潔で明確に行うためである．実際の管理策の実施には様々な自由度が存在し，確率を決定するのは非常に困難である．さらに複数の管理策を同時に実行した場合の効果の評価は様々な条件が絡み合い，確率として評価することは不可能に近い．そこで提案手法では確率に代えて要件の満足割合を採用した．ISO/IEC 27002 における管理策間の考慮すべき影響はすべて「参照」により記述されていると仮定し，参照の関係がない管理策間の影響は無視した．OR ゲートに並ぶ管理策間にも参照の関係が存在する場合があるが，展開に際しサブツリー上で二重に出現する管理策は除き，重複して評価することを防いでいるので，管理策間に参照の関係があったとしても OR ゲートに並ぶ管理策はそれぞれ独立した影響程度と評価できる．また，本手法では当該管理策ごとに参照に基づいた展開を行っているので，異なるサブツリー上で同一の管理策が出現することはありうる．しかし，提案手法では上位の管理策が機能するために必要となる管理策を下位に展開しているため，下位の管理策は上位の管理策を機能させる範囲での有効性を評価している．このため異なるサブツリー上に出現する場合，同一の管理策であっても評価している効果が異なるため，効果を二重に積算することはない．ただし，Fault Tree を構成する際に当該管理策をルートとするサブツリー上では同一の管理策の出現は 1 度だけとした．なお厳密には管理策により上位事象の要件への効果の違いが考えられるが，すべて同一と見なした．これにより OR ゲートを構成する管理策に対する評価は，接続している管理策中で実施されている管理策の割合とした．以下，内部犯行に対する管理体制の具体的な FTA の構成について述べる．

- 「頂上事象」—「1 次事象」
  内部犯行に対する管理体制は抽出したすべての有効管理策で構成する．1 つの有効管理策でも未実施ならば内部犯行を防止できないため，内部犯行を防止するにはすべての有効管理策が必要となる．そのため，「頂上事象」—「1 次事象」については図 4 のように AND ゲートで構成する．また図 4 中の有効管理策および当該管理策の番号は，CERT の調査[17] および ISO/IEC 27002[2] の表記に従った．
- 「1 次事象」—「2 次事象」
  有効管理策はそれぞれいくつかの当該管理策で構成する．1 次事象から 2 次事象への展開は，1 次事象の要件達成に直接的に資する管理策を ISO/IEC 27002 から抽出し，2

次事象として展開する．抽出に際し，それぞれ単独で要件達成に効果がある管理策を抽出している．2 次事象の要件をすべて満足すると 1 次事象の要件を完全に達成するが，すべて満足しなくても 2 次事象の 1 つの管理策は単独で 1 次事象の要件達成にある程度の効果を持つ．そのため「1 次事象」—「2 次事象」については図 4 のように，1 つの当該管理策でも実施していれば生起する OR ゲートで構成する．ただし危機管理的観点に立ち，考えうるすべての管理策を実施した場合にのみ要件達成と見なし，OR ゲートにおいて不足する管理策があった場合にはその影響程度に合わせて減点する．

- 「2 次事象」—「それ以降」
  当該管理策はそれぞれいくつかの参照管理策で構成する．参照に従っての展開は 2 種類存在する．1 つは参照管理策への展開である．ISO/IEC 27002 においては参照管理策は参照元の管理策を補強する関係にあるため，参照管理策は元の要件に対し独立して補強する効果を持つ．このため 1 つの参照管理策でも実施していれば生起する OR ゲートで構成する．もう 1 つの種類の展開として，管理策が機能するために必要となる管理策への展開がある．参照管理策が機能するには上位事象である被参照管理策を実施する必要がある．しかし，参照管理策を展開した際に構成している Fault Tree の上位事象に被参照管理策がすべて含まれているわけではない．そこで参照管理策への展開に際し，漏れた被参照管理策を抽出し，必要条件として AND ゲートで接続し展開する．また，実施状況を入力するための基本事象を「管理策（実施策：状況）」，影響程度を付与するための基本事象を「管理策（実施策：影響）」と表記する．

3.3.3　内部犯行防止に寄与する影響程度を付与することによる有効性解析

内部犯行に対する管理体制の有効性を評価するために，それぞれの管理策に内部犯行防止に寄与する影響程度を付与する．Fault Tree によって図 4 のように，内部犯行防止に関連する管理策が機能する条件が示されている．そこで管理体制の構造を考慮して，各管理策に内部犯行防止に寄与する影響程度を付与する．影響程度とは「内部犯行防止に有効な要件に対し，各管理策が寄与する要件の割合」である．図 4 より，「頂上事象」—「1 次事象」は有効管理策がすべて必要であることを示すだけなので，影響程度の付与には関係しない．そのため，それ以下の事象に対して管理体制に寄与する影響程度を付与する．内部犯行防止に寄与する各管理策の影響程度は (1) 有効管理策に寄与する当該管理策の影響程度，(2) 当該管理策に寄与する参照管理策の影響程度，のように付与する．

(1)　有効管理策に寄与する当該管理策の影響程度（「1 次事象」—「2 次事象」）
内部犯行に対する管理体制の有効性を評価するには，有効管理策に寄与する当該管理策の影響を求める必要がある．ここでは「有効管理策の要件に対し，当該管理策が寄与する要件の割合」を有効管理策に寄与する当該管理策の影響程度とする．厳密な影響評価は困難であるため，簡略化して有効管理策に寄与する当該管理策の影響程度を有効管理策の有効性（有効管理策がどの程度機能しているのか）とする．有効管理策に寄与する当該管理策の影響程度は，その有効管理策が包含する当該管理策に寄与する参照管理策の影響程度の総和とその有効管理策が包含する当該管理策数で割った値との積になる．つまり，有効管理策の要件を当該管理策ごとに等分した値が各当該管理策の寄与する要件の割合となり，各当該管理策が達成した要件の総和が有効管理策の有効性となる．こうすることで「有効管理策」の有効性を 0.00〜1.00 で表すことができる．

(2)　当該管理策に寄与する参照管理策の影響程度（「2 次事象」—「それ以降」）
有効管理策に寄与する当該管理策の影響程度を求めるには，当該管理策に寄与する参照管理策の影響程度を求める必要がある．ここでは「当該管理策の要件に対し，参照管理策が寄与する要件の割合」を当該管理策に寄与する参照管理策の影響程度とする．厳密な有効性の評価は困難であるため簡略化し，当該管理策に寄与する参照管理策の影響程度を求めることで当該管理策の有効性（当該管理策がどの程度機能しているのか）として代用する．当該管理策に寄与する参照管理策の影響程度は，当該管理策が完全に機能していることを示す「1.00」を各当該管理策が包含する管理策数で割った値となる．つまり，当該管理策の要件を参照管理策ごとに等分した値が各参照管理策の寄与する要件の割合となり，各参照管理策が達成した要件の総和が当該管理策の有効性となる．こうすることで「当該管理策」の有効性を 0.00〜1.00 で表すことができる．

上記のように数値を付与し，FTA で分析することで内部犯行に対する管理体制の有効性を評価できる．しかし，FTA は基本事象にのみ数値を付与するため，「1 次事象」—「2 次事象」で数値を付与できない．そのため，FTA を構成する際には基本事象に対して，有効管理策に寄与する参照管理策の影響程度を付与し，有効管理策の有効性（有効管理策がどの程度機能しているのか）を求める．ここでは「有効管理策の要件に対し，参照管理策が寄与する要件の割合」を当該管理策に寄与する参照管理策の影響程度とする．したがって参照管理策に付与する値は，有効管理策が完全に機能していることを示す「1.00」を各有効管理策が包含する参照管理策数で割った値となる．つまり，有効管理策の要件を参照管理策ごとに等分した値が各参照管理策の寄与する要件の割合となり，各参照管理策が達成した要件の総

和が有効管理策の有効性となる．こうすることで，「有効管理策」の有効性を 0.00〜1.00 で表すことができる．

内部犯行を防止するにはすべての有効管理策が必要なので，すべての有効管理策の有効性の積算値が「内部犯行に対する管理体制」の有効性となる．また，有効管理策は「内部犯行に対する管理体制」に対してすべて AND ゲートで接続しているため，「内部犯行に対する管理体制」の有効性を 0.00〜1.00 で表すことができる．ただし，管理策の実施を判定するための基本事象（図 4 中の AND で直接つながれた基本事象）には影響程度を付与せず，実施状況を入力する．入力値は実施なら「1」，未実施なら「0」とする．管理策を実施と入力することでその管理策が機能し，内部犯行防止に寄与する影響程度が加算される．その結果，内部犯行に対する管理体制がどの程度機能しているのかが分かり，これが管理体制の有効性となる．

3.4　不足する管理策の指摘

内部犯行に対する管理体制の有効性を用いて，内部犯行防止に不足する管理策を指摘する．提案手法に管理策の実施状況を入力することで，管理体制の有効性を評価できる．そこで，実施する管理策の変更による有効性の変化を評価することで，不足する管理策の指摘を行う．つまり，現状の管理体制に対して実験的に管理策を実施した際，有効性が増加すればその管理策は評価した管理体制に有用な管理策となる．逆に有効性の変化がなければ，その管理策は評価した管理体制に不要な管理策となる．

4. 検　　証

4.1　検証の方針

提案手法の有用性を検証するために，情報セキュリティ事故の事例を用いて管理体制の有効性の評価実験を行った．まず提案手法に基づいて，内部犯行に対する管理体制の有効性評価システムを作成した．作成したシステムは，3 章で構成法を示した FTA を「表計算システム（MS-Excel）」上でプログラムを書き実装し，ISO/IEC 27002 に基づいた内部犯行防止に関連する管理策実施の有無を入力することにより，自動的に管理体制の有効性を計算する．提案手法は FTA を応用することで，内部犯行に対する管理体制を分析し，その有効性を評価できる．管理体制の有効性とは「管理体制に属する管理策の影響程度の総和」である．つまり提案手法は，実施している管理策が内部犯行防止に有効な要件をどの程度満たしているかを評価している．したがって，作成したシステム用いることで内部犯行に対する管理体制の有効性を評価でき，かつ不足する管理策を指摘できる．

入力：ISO/IEC 27002 中の管理策の実施状況「実施：1，未実施：0」

処理：内部犯行に対する管理体制が完全に機能している状態を「1.00」とし，そこからどの程度の機能が欠けているかを評価する．

出力：管理体制の有効性（管理体制がどの程度機能しているのか）「0.00〜1.00」

次に作成したシステムに対し，実際に発生した情報セキュリティ事故の事例から読み取り可能な管理策の実施状況を入力することで，管理体制の有効性評価を行った．内部犯行防止に有効なすべての管理策を実施している場合に評価値は「1.00」となり，未実施が確認される管理策はその影響程度に合わせ減点してゆき，有効な管理策をまったく実施していない場合に評価値は「0.00」となる．使用したデータは情報セキュリティ事故に対する一般向けの記事であるため，実施せずに事故に重大な影響を及ぼしたとされる管理策の記述が中心であり，実施しているすべての管理策が記述されているわけではない．そこで実施状況が不明な管理策は，データ作成者としては実施することが当然であり，あえて記する必要がないために実施状況の記述がないものと考え，「実施」しているものと仮定した．また，入力した事故事例は雑誌，新聞，Web サイトなどで公開されている事例から選択した．評価実験は以下の手順で行う．

(1)　管理体制の有効性評価の検証

(a)　内部犯行が発生した管理体制を用いた検証

ここでは内部犯行に対する管理体制の有効性が評価可能であることを検証する．そのため，内部犯行が発生した組織の管理策の実施状況をシステムに入力する．評価実験の結果，管理体制の有効性が低ければ内部犯行発生の可能性を指摘できており，本手法の有用性を検証できる．また，データのばらつきを抑えるために内部犯行の種類を分類し，それぞれの集合から事例を摘出して検証を行う．内部犯行の分類は CERT の定義（図 2）を用いた．ただし，その他については発生件数が少なく特徴も一定でないため，検証には用いない．

(b)　内部犯行以外の情報セキュリティ事故が発生した管理体制を用いた検証

ここでは内部犯行防止に関連する要素にのみ反応して評価していることを検証する．そのため，内部犯行以外の情報セキュリティ事故が発生した管理体制をシステムに入力する．評価実験の結果，管理体制の有効性が高ければ内部犯行防止に関連する要素にのみ反応して評価しており，本手法の有用性を検証できる．

(2)　不足する管理策の指摘が可能であることの検証

ここでは内部犯行防止に不足する管理策の指摘が可能であることを検証する．そのため，内部犯行が発生した管理体制に対してシステム上で実験的に管理策を実施し，管理体制の有効性の変化を評価する．評価実験の結果，管理策ごとに有効性が変化し，不足する管理策を指摘できれば本手法の有用性を検証できる．

4.2　内部犯行が発生した管理体制を用いた検証

提案手法の有用性を検証するために，情報セキュリティ事故の事例を用いて管理体制の有効性の評価実験を行った．ケース A についてのみ詳細を説明し，以降のケースについては同様の手順で行ったため結果のみを示す．

ケース A [29]**：**IT サボタージュ

1. 事故の記事から管理策の実施状況を推測する

記事の内容から管理策の実施状況を推測し，該当する ISO/IEC 27002 中の管理策を抽出する．

概要　元派遣社員が元の勤務場所である銀行のネットワークへの不正アクセスを行った．元派遣社員は，自宅のパソコンから，銀行の内部ネットワークのサーバに 67 回侵入し，約 2,600 個のファイルを削除してシステムの破壊を行った．

2. 管理策の実施状況をシステムに入力する

ケース A は元従業員によるシステム破壊である．記事から以下の 2 つの管理策が未実施であると考えられる．未実施と考えられる管理策には「0」，それ以外の管理策は実施しているものと仮定し，「1」をシステムに入力する．

未実施と考えられる管理策

- 8.3.3 アクセス権の削除
- 11.7.2 テレワーキング

3. 管理体制の有効性の評価値を算出する

手法に基づいて，未実施の管理策が内部犯行防止に寄与する影響程度を減算し，有効性の評価値を算出する．

システムでの評価による管理体制の有効性：0.32

ケース B [30]**：**金銭的利益のための窃盗または改ざん

概要　システム部の部長代理が権限を悪用し，148 万 6,651 人の顧客情報を流出させ，4 万 9,159 人分が 80 社以上にわたった．

未実施と考えられる管理策

- 10.1.3 職務の分割
- 10.2.1 第三者が提供するサービス
- 11.2.2 特権管理
- 15.1.5 情報処理施設の不正使用防止
- 15.2.1 セキュリティ方針および標準の順守

システムでの評価による管理体制の有効性：0.00

ケース C [31]**：**ビジネス上の利益のための窃盗または改ざん

概要　従業員が退職する前に営業秘密をコピーして保有しており，退職後に外国のライバル会社に当該営業秘密を漏示していた．従業員は，就業中に当該営業秘密にアクセスする権限を与えられており，コピーすることも十分にありうる状況だった．

未実施と考えられる管理策

- 8.3.2 資産の返却

システムでの評価による管理体制の有効性：0.42

4.3　内部犯行以外の情報セキュリティ事故が発生した管理体制を用いた検証

ケース D [32]**：**内部犯行以外の情報セキュリティ事故で高い有効性を示したケース

概要　携帯電話のサービスにおいてユーザ本人宛ではないメールが送られてきたり，メール送信者アドレスが異なる第三者のものに変わったりするという不具合を起こした．

未実施と考えられる管理策

- 10.3.1 容量・能力の管理
- 10.3.2 システムの受け入れ
- 12.1.1 セキュリティ要求事項の分析および仕様化
- 12.2.2 内部処理の管理
- 12.2.4 出力データの妥当性確認

システムでの評価による管理体制の有効性：0.86

ケース E [33]**：**内部犯行以外の情報セキュリティ事故で低い有効性を示したケース

概要　データセンタサービスにおいて 1 つのサーバが乗っ取られ，その LAN 上のサーバも将棋倒しのように乗っ取られた．

未実施と考えられる管理策

- 11.2.3 利用者パスワードの管理
- 11.3.1 パスワードの利用

表 1　ケース B における未実施管理策の効果
Table 1　Effectiveness of unimplemented measures in case B.

	実施する管理策	管理策実施後の管理体制の有効性
1回目	職務の分割	0.26
	第三者が提供するサービス	0.00
	特権管理	0.00
	情報処理施設の不正使用防止	0.00
	セキュリティ方針及び標準の順守	0.00
2回目	特権管理	0.56
	セキュリティ方針及び標準の順守	0.38
	情報処理施設の不正使用防止	0.33
	第三者が提供するサービス	0.26

- 11.4.5 ネットワークの領域分割

システムでの評価による管理体制の有効性：0.02

4.4　不足する管理策の指摘が可能であることの検証

管理体制の有効性が低く，未実施と考えられる管理策が多かったケース B を用いて検証を行う．システム上で実験的に管理策を実施し，それによる管理体制の有効性の変化を**表 1** に示す．表 1 より，職務の分割以外の管理策を実施しても有効性が増加しないことが分かる．そのため，職務の分割を実施したと仮定して，他の管理策の実施による管理体制の有効性を評価した．その結果，有効性の増加が大きかった以下の順番で内部犯行防止に効果的であることが示せた．

(1)　10.1.3 職務の分割
(2)　11.2.2 特権管理
(3)　15.2.1 セキュリティ方針および標準の順守
(4)　15.1.5 情報処理施設の不正利用防止
(5)　10.2.1 第三者が提供するサービス

また，表 1 に示した管理策をすべて実施すると有効性は 1.00 になるが，これはほかの管理策をすべて実施していると仮定しているためである．実際には事例から読み取れる以外にも実施していない管理策があると考えられるため，当該組織に対し，詳細な監査を実施したうえでの有効性評価は 1.00 とはならないものと考えられる．

4.5　検 証 結 果

内部犯行に対する管理体制の有効性が評価可能であることをケース A〜C により検証した．3 ケースの内部犯行が発生した管理体制をシステムに入力した結果，それぞれが低い有効性を示した．有効性の低さは内部犯行に対する脆弱部分の多さを表しているため，内部犯行発生の可能性が高いことを示している．これにより提案手法を用いることで，内部犯行に対する管理体制の有効性評価が可能であることを検証した．

内部犯行防止に関連する要素にのみ反応して評価していることをケース D・E により検証した．内部犯行以外の情報セキュリティ事故が発生した管理体制をシステムに入力した結果，ケース D は高い有効性，ケース E は低い有効性を示した．ケース D より，複数の管理策が未実施でも内部犯行防止に有効な管理策を実施していれば，高い有効性を示すことを検証した．これにより本手法が内部犯行防止に関連する要素にのみ反応して評価していることを検証した．またケース E より，内部犯行が発生していない場合でも低い有効性を示す可能性があることを示した．これはパスワードの漏洩やネットワーク領域の不適切な設定など，内部犯行が発生する可能性があるためである．また，アカウントの管理などは情報セキュリティ全体の問題であり，内部犯行と共通しているためケース D は低い有効性を示したと考えられる．この結果より，内部犯行が未発生でも内部犯行に対する管理体制の有効性の評価が可能であることを検証した．また，情報セキュリティ共通の問題に対して，管理体制の有効性の評価が可能であることを示した．

不足する管理策の指摘が可能であることを 4.4 節により検証した．ケースの中で最も有効性の低かったケース B に対して，システム上で実験的に管理策を実施することで，管理体制の有効性が変化することを示した．また表 1 より，職務の分割以外の管理策を実施しても有効性が増加しないことが分かる．このことから「10.1.3 職務の分割」は他の管理策で代替できず，実施しなければ内部犯行の発生を防ぐことが困難であることが分かる．さらに，職務の分割を実施したと仮定して評価実験を続けた結果，他の管理策の実施についても管理体制の有効性の変化を評価できた．表 1 のように管理体制の有効性が変化したことから，不足する管理策の指摘が可能なことを検証した．

以上のことから，本手法が内部犯行に対する管理策の効果および管理体制の有効性が評価可能であることを検証した．ゆえに，提案手法は内部犯行防止に対する管理策の実施に際して，きわめて有効に働くといえる．

5. おわりに

本稿では情報セキュリティ対策間の相互依存関係を用いて，内部犯行防止に不足する情報セキュリティ対策を指摘する手法を提案した．本手法は，(1) 関連する情報セキュリティ対策の抽出，(2) 情報セキュリティ体制の有効性評価，(3) 不足する情報セキュリティ対策の

指摘，の 3 つのプロセスを実施するものである．それにより情報セキュリティ対策の実施状況を確認することで，内部犯行に対する情報セキュリティ体制の有効性を評価でき，かつ不足する情報セキュリティ対策を指摘できる．また，実際に情報セキュリティ事故が発生した情報セキュリティ体制を提案手法に入力することで，内部犯行に対する情報セキュリティ体制の有効性の評価が可能であることを検証した．さらに，内部犯行が発生したケースの情報セキュリティ体制に対して，実験的に情報セキュリティ体制を変更することで，内部犯行防止に不足する情報セキュリティ対策を指摘できた．ゆえに本手法は，内部犯行防止に対する情報セキュリティ対策の実施に際して，きわめて有効に働くといえる．

今後の課題として提案手法の一般化，コスト評価の導入が考えられる．存在する様々なリスクに対して情報セキュリティ体制の有効性を評価できれば，内部犯行だけでなく情報セキュリティ全体に対して不足する情報セキュリティ対策を指摘できる．また，情報セキュリティ対策を実施するためには軽減すべきリスクに対する情報セキュリティ対策の効果とともに，実施に要するコストの評価も重要である．本手法を用いることで内部犯行防止に対する情報セキュリティ対策の効果を評価できるため，実施に要するコストを評価することで必要な情報セキュリティ対策をさらに効果的に指摘できる．

参 考 文 献

1) Ericson, C.: Fault Tree Analysis – A History, *Proc. International Conferences on International System Safety*, pp.87–96 (1999).
2) ISO/IEC 27002:2005: Information technology – Security techniques – Code of practice for information security management (2005).
3) Beccaria, C., Newman, G. and Marongiu, P.: *On crimes and punishments*, Transaction Pub. (2009).
4) Hirschi, T.: *Causes of delinquency*, Berkeley: University of California Press (1969).
5) Sutherland, E.: *Criminology*, Philadelphia, J.B. Lippincott (1924).
6) Ajzen, I. and Fishbein, M.: *Understanding attitudes and predicting social behavior*, Prentice Hall (1980).
7) Clarke, R.: Situational crime prevention: theory and practice, *British Journal of Criminology*, Vol.20, No.2, pp.136–137 (1980).
8) Straub, D. and Welke, R.: Coping with systems risk: security planning models for management decision making, *Mis Quarterly*, Vol.22, No.4, pp.441–465 (1998).
9) Lee, S.M., Lee, S. and Sangjin, Y.: An integrative model of computer abuse based on social control and general deterrence theories, *Information and Management*, Vol.41, No.6, pp.707–718 (2003).
10) Lee, J. and Lee, Y.: A holistic model of computer abuse within organizations, *Information Management and Computer Security*, Vol.10, No.2, pp.57–63 (2002).
11) Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E.: The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, Vol.24, No.6, pp.472–484 (2005).
12) ISO/IEC 17799:2005: Information technology – Security techniques – Code of preactice for information security management (2005).
13) Schultz, E.: A framework for understanding and predicting insider attacks, *Computers & Security*, Vol.21, No.6, pp.526–531 (2002).
14) Hui, W., Heli, X., Bibo, L. and Zihao, S.: Research on Security Architecture for Defending Insider Threat, *Proc. IEEE International Conferences on Symposium on Information Assurance and Security* (*IAS2009*), pp.30–33 (2009).
15) Pfleeger, S., Predd, J., Hunker, J. and Bulford, C.: Insiders Behaving Badly: Addressing Bad Actors and Their Actions, *Information Forensics and Security*, Vol.5, No.1, pp.169–179 (2010).
16) Hunker, J. and Probst, C.: The Risk of Risk Analysis And its Relation to the Economics of Insider Threats, *The 9th Workshop on the Economics of Information Security* (*WEIS 2010*) (2010).
17) Cappelli, D., Moore, A., Trzeciak, R. and Shimeall, T.: *Common Sense Guide to Prevention and Detection of Insider Threats*, *3rd Edition Version 3.1*, Carnegie Mellon University, Software Engineering Institute, CERT Program (2009).
18) Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D. and Moore, A.: Insider threat study: Illicit cyber activity in the banking and finance sector, *Joint SEI and U.S. Secret Service Report* (2005).
19) Moore, A., Cappelli, D., Caron, T., Shaw, E. and Trzeciak, R.: Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model, *Proc. International Workshop on Managing Insider Security Threats* (*MIST 2009*) (2009).
20) Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. and Rogers, S.: Insider threat study: Computer system sabotage in critical infrastructure sectors, *Joint SEI and US Secret Service Report* (2005).
21) 高橋達明，ギジェルモ・オラシオラミレス・カセレス，勅使河原可海：XML を用いた ISO/IEC 17799 の構造化に関する検討，情報処理学会研究報告（CSEC），Vol.2005, No.122, pp.43–48 (2005).
22) 高橋達明，ギジェルモ・オラシオラミレス・カセレス，勅使河原可海：ISO/IEC 17799 の管理項目の関連性を考慮したセキュリティ対策の選択基準の検討，情報処理学会研究報告（CSEC），Vol.2007, No.16, pp.447–452 (2007).
23) 宝木和夫，佐々木良一，永井康彦：情報システムにおけるリスク分析の一方法，電気学会論文誌 C，Vol.108, No.4, pp.260–267 (1988).

24) 織茂昌之，津原　進，山本倫子，佐々木良一：情報システムにおけるセキュリティ対策立案のための計画手法，情報処理学会論文誌，Vol.41, No.1, pp.177–187 (2000).
25) ISO/IEC 15408: 1999: Information technology – Security techniques – Evaluation criteria for IT security (1998).
26) 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.2120–2128 (2005).
27) 渡部知浩，山本裕志，矢島敬士，佐々木良一：多重リスクコミュニケータにおける関与者情報獲得支援方式の評価，電気学会論文誌 C（電子・情報・システム部門誌），Vol.128, No.2, pp.310–317 (2008).
28) 谷山充洋，佐々木良一：多重リスクコミュニケータの教育方法の提案と分析，日本セキュリティ・マネジメント学会誌，Vol.23, No.2, pp.52–64 (2009).
29) インド人元 SE を逮捕，読売新聞 2008 年 7 月 19 日，p.32 (2008).
30) 中井　奨：「権限者の不正」で 148 万人分流出，日経コンピュータ，No.729, p.19 (2009).
31) 財団法人比較法研究センター：意匠登録出願における「特徴記載書」に関する調査研究，技術報告，特許庁企画調査課 (2007).
32) 白井　良：他人のメールボックスが見えてしまう通信の根幹にかかわる重大事故に，日経コンピュータ，No.743, pp.88–90 (2009).
33) 安東一真：新手の Web 改ざんが日本上陸，日経コンピュータ，No.706, p.19 (2008).

(平成 22 年 11 月 30 日受付)
(平成 23 年 6 月 3 日採録)

鈴木　智也（正会員）

2011 年中央大学大学院理工学研究科電気電子情報通信工学専攻修士課程修了．同年（株）NTT データ入社．2011 年辻井重男セキュリティマネジメント学生賞受賞．

田沼　　均（正会員）

1986 年東北大学大学院工学研究科電気および通信工学専攻博士前期課程修了．同年通産省工業技術院電子技術総合研究所，組織変更により 2001 年より（独）産業技術総合研究所．2002〜2008 年内閣官房情報セキュリティ対策推進室（現，情報セキュリティセンター）兼務．2010 年中央大学大学院理工学研究科情報セキュリティ科学専攻博士後期課程修了．博士（工学）．電子情報通信学会，日本セキュリティ・マネジメント学会各会員．

今井　秀樹（正会員）

1966 年東京大学工学部電子工学科卒業．1971 年同大学院博士課程修了．工学博士．現在，中央大学理工学部教授，理工学研究所所長，東京大学名誉教授．産業技術総合研究所情報セキュリティ研究センター長兼務，日本学術会議会員．情報理論，情報セキュリティ等の研究に従事．1975 年，1990 年本会著述賞，2001，2002，2003，2007 年同論文賞，2001 年同米澤ファウンダーズ・メダル，1992 年 IEEE Fellow，1994 年本会業績賞，2002 年同猪瀬賞，2003 年同功績賞，1998 年 IEEE シャノン 50 周年記念論文賞，2002 年総務大臣表彰，経済産業大臣表彰，2005 年エリクソン・テレコミュニケーション賞，2007 年 IACR Fellow，2008 年大川賞，IEEE Life Fellow, 2009 年内閣官房長官表彰，NHK 放送文化賞，電子情報通信学会名誉員，1999，2002 年名誉博士等．