セキュアトロポス（Secure Tropos）概論

Haralambos Mouratidis[*1]　田口 研治[*2]

[*1] University of East London　[*2] 国立情報学研究所

現在，多くの情報システムにおいてセキュリティ面での脆弱性が発見されている．その対処方法として，要求獲得・分析フェーズにおいて，網羅的にセキュリティ要件を獲得・分析することで，システムのセキュリティ面を強化するさまざまな方法論が提案されている．本稿においては，そのような方法論の１つである，セキュアトロポスについて，事例を基に紹介をする．

セキュリティへの要求工学からのアプローチ

本稿は，セキュリティ要件の獲得・分析方法論の１つであるセキュアトロポスについて，その方法論としての特徴を，簡単な事例を通して紹介する．

今現在においても，多くの情報システムがセキュリティ機能を実装して稼働している．多くのシステムにおいて，その脆弱性が発見されているが，原因としては人間による誤操作や装置の故障など以外に，ソフトウェアシステムにおけるディフェクトが主要因として挙げられる．ソフトウェアのディフェクトをいかになくすかは，ソフトウェア工学における大きな課題の１つであるが，その解決策として認知されているのが，*要求と設計の段階においてディフェクトを発見，修理する*というものである．セキュリティに関してもこの原理は成り立ち，いかに要求獲得・分析フェーズにおいてシステムに関するセキュリティ要件をもれなく分析するかは非常に重要な技術課題である．

残念ながら，情報システムの開発においては，要求獲得・分析プロセスにおいて，本特集が紹介するような方法論はほとんど利用されていないのが現状である．利用されていないのは，そもそもセキュリティを考慮する場合の開発コストの点で，セキュリティ要件の獲得・分析にコストが掛けられないといった点や，従来の開発方法論がセキュリティに対する対策が考慮されていない点など，さまざまな理由がある．さらに，実はこのような方法論が，現場の開発者にまだ広く知られていない，という大きな理由がある．筆者は，セキュリティ要件の獲得・分析について，特にCC（Common Criteria）を題材にして講義を行っている[5]．その題材を元に，CCに関連するさまざまな企業に話を伺う機会があったが，本特集で取り上げるような方法論を知っているか利用しているという企業はほとんどなかった．本特集が契機となり，これらの方法論を現場で試行・実践する組織が増え，よりセキュアなシステムの開発が行われることを望む．

セキュアトロポス

セキュアトロポス（Secure Tropos）は，本稿の第一著者ら[2]により提唱されたセキュリティ要求の獲得・分析を主目的とするセキュリティ要求分析方法論であり，新たにセキュリティに特化した要求工学の方法論を生み出すのではなく，すでによく研究されている方法論をセキュリティに拡張・適用する，というアイディアのもとに生まれた．要求工学の分野においては，本特集で紹介するようなゴール指向，エージェント指向といった方法論が多くの研究者により研究，開発されてきた．エージェント指向の代表的な方法論としてはトロポス（Tropos）[1]がある．トロポスはYuのi*によるモデリング方法論を採用しており，アクター，ゴール，アクター間の依存関係の記述が基本となる．本方法論は，現在においてもさまざまな拡張とそれに基づいたツール開発が行われている．

トロポスにはセキュリティを含む非機能要件を記述するためのソフトゴールという概念がある．ソフトゴールは元々NFR[6]において提唱されたものであり，明確に定義できない，非機能要求を記述するために用いられる．しかし，セキュリティ要件の分析の重要性が認識されたとき，ソフトゴールだけではセキュリティに関する制約を明確に定義することが難しいことから，さまざまな拡張が試行された．拡張には，セキュリティ制約，セキュアな依存関係，さまざまなセキュアなモデル要素（ゴール，タスク，リソース）などがある．これらの新しいモデル要素を用いることで，セキュリティに関する要素間の関係や，制約をより明

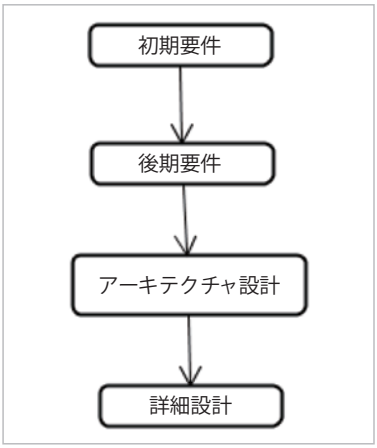

図 -1　セキュアトロポスにおける開発プロセス

確に分析，獲得することが可能になった．

トロポスにおいては，本来，開発プロセス全体（要求分析，設計，実装）を支援するという考え方や，段階的に要求を詳細化するという考え方が支援されている．トロポスでは，初期要件（Early Requirements），後期要件（Late Requirements），アーキテクチャ設計（Architecture Design），詳細設計（Detailed Design），実装といった開発プロセスが支援されている（**図 -1**）．それに対して，セキュアトロポスにおいては，実装を除いた同様なプロセスが定義されている．

セキュアトロポスの特徴を挙げると以下のようになる．

- セキュリティに特化した方法論を提供することで，システム開発者がセキュリティに関する問題の解決に集中することができる
- システムの分析だけではなく，システムを取り巻くシステム環境の分析を行える
- セキュリティと機能要件の両方の分析が同時に行える
- 開発プロセス全体を通して支援が行われる

セキュアトロポスでは，セキュリティの要求分析において重要な，セキュリティに関するさまざまな制約をアクターにおけるセキュリティに関するポリシー，資源，ゴール等を用いて定義するモデル記述方法を提供することで，上記の特徴を実現している．

セキュリティモデリング

セキュリティのモデリングのためには，以下のようなプロセスを経る．初期要件プロセスにおいては，アクターの依存関係の分析から始まり，依存関係間におけるセキュリティ制約の定義がアクター図として作成される．さらに，各アクターにおける詳細なゴールの分析が行われる．次に後期要件においては，設計対象となるシステムが導入され，その動作環境などとともに分析が行われる（**図 -2**）．

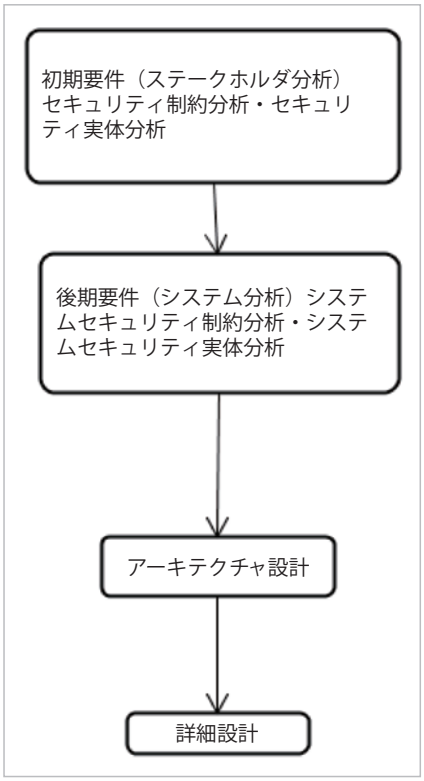

図 -2　セキュリティモデリングのプロセス

本稿においては，ページ数の都合上，初期要件に的を絞って説明を行う．

初期要件

セキュリティに関する要件を記述する方法はさまざまあるが，本方法論においては，アクター間の依存関係において，システムに関するセキュリティに大きな影響を及ぼす要因である，プライバシー，完全性，可用性などに関する制約を記述することが，大きな特徴になっている．セキュリティ依存関係は，依存者（Depender）と被依存者（Dependee）が依存物（Dependum）を介して定義され，依存関係上に定義された制約が満たされることにより，その依存関係自身が満足されると考える．依存関係は向きを持っており，それは依存関係を表す実線上の大文字 D で表されている．

利用される基本的な 4 つのモデル要素について示す．正八角形はセキュリティ制約を表し，円はアクターを，そして角が丸い四角はハードゴールを表し，雲形はソフトゴールを表す．ハードゴールは，非機能的な要件に関するソフトゴールと対比されるものであり，明確に定義できるゴールを表す．これらの表記法は本稿の第一著者が開発したセキュアトロポスのモデリングツール SecTro に基づいている（**図 -3**）．

依存物としては，ハードゴール，ソフトゴールのほかにも，計画や資源があるが，本稿ではハードゴールとソ

フトゴールだけを用いる．

セキュリティ実体としては，セキュアハードゴール，セキュアアクションなどがある．セキュアハードゴールはアクターのセキュリティに関する戦略的興味を表す．セキュリティのゴールはアクターに規定されたセキュリティ制約を遂行するために導入されている．セキュリティゴールがどのように遂行されるかは，セキュアアクションにおいて記述される（**図-4**）．

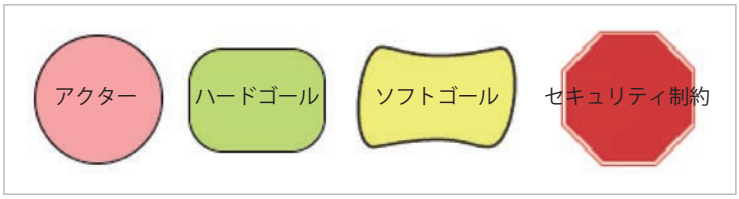

図-3　基本的なモデル要素

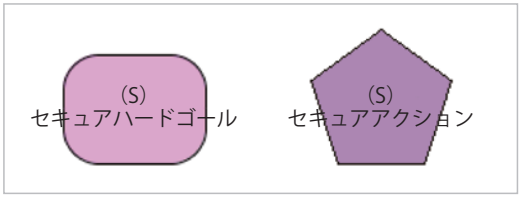

図-4　セキュアな実体

次にセキュアな依存関係について説明をする．**図-5** は，ハードゴールを依存物とした場合の，セキュリティ制約が定義されない場合と，定義される3つの場合について示してある．(1) は，セキュリティ制約が定義されていない場合であり，依存者と被依存者の間には依存物（ハードゴール）が定義されているだけである．それに対して，(2) は依存者がセキュリティ制約を導入した場合，(3) は依存者がセキュリティ制約を導入した場合，(4) は両者が導入した場合を示している．(2) を例にとると，依存者は被依存者にハードゴールにおいて記述される関係において依存し，それはセキュリティの制約が満たされて初めて，そのセキュアな依存関係が成立する，と定義される．

初期要件フェーズにおけるアクター図は，アクターの同定と，アクター間の（セキュアな）依存関係の定義を行うことで記述される．

簡単な例を用いて，どのように依存関係が記述されるかを見てみよう（**図-6**）．ここでは，英国における医療システムのモデル化を用いる[3]．アクターとしては，「高齢者」，「福祉事務所」，「医療関係者」が同定されたとする．次にアクター間の依存関係を分析・定義する．「高齢者」は「福祉事務所」に対して，「経済的支援を受ける」が，個人情報（財務関連）の情報を漏らしてもらっては困るので，「福祉事務所」に対して，「個人情報の漏洩をしない」というセキュリティの制約を導入している．次に，「高齢者」と「医療関係者」に関しては，「健康を維持する」というソフトゴールにより「高齢者」は「医療関係者」に依存しているが，「医療関係者」は「高齢者」に対して，さまざまな「医療情報を得る」ことに関して依存している．その際，「高齢者」は「医療関係者」に対して，

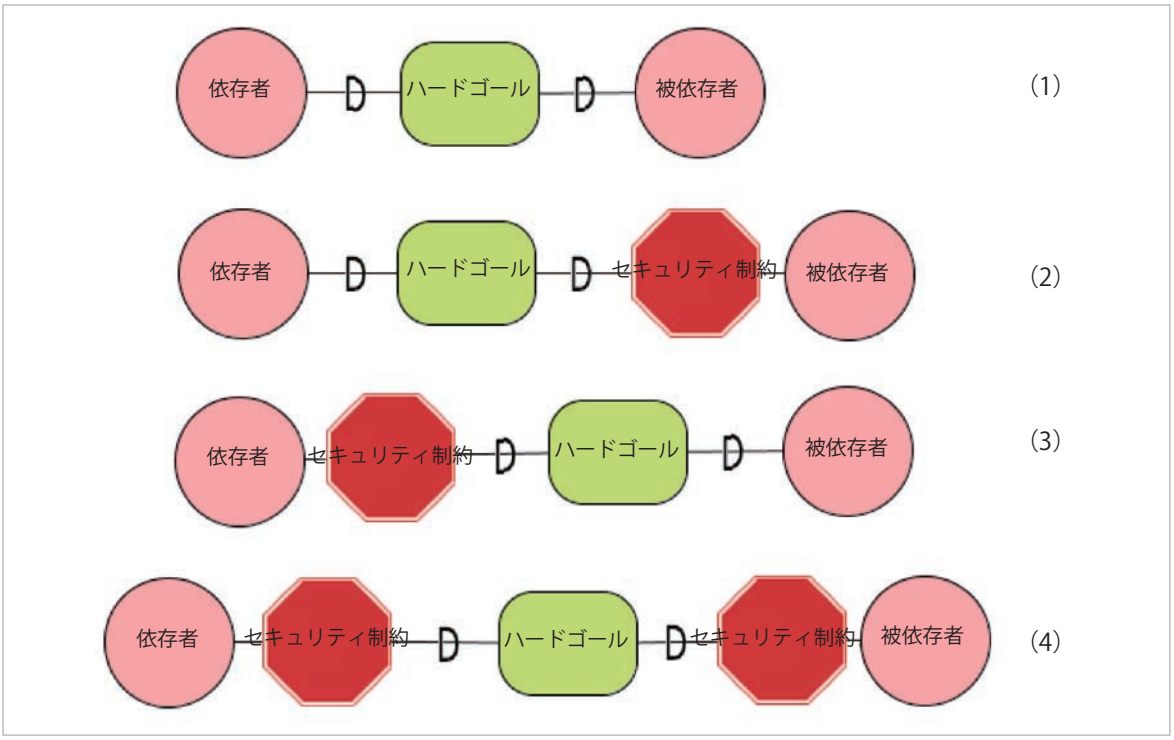

図-5　依存関係

「同意が得られた場合のみに，情報が提供される」，という制約を課している．セキュリティ制約は必ずしも定義する必要はなく,「高齢者」の「医療関係者」に対する「健康を維持する」という依存関係がその例になる．

ここで，依存物としては，ソフトゴールとハードゴールが現れるが，「経済的支援を受ける」や「健康を維持する」といった，定義が明確でない場合にはソフトゴールが用いられ，「医療情報を得る」といった明確に定義が可能なゴールに対してはハードゴールが用いられている．

次に，各アクターにおけるゴールの分析を行う．ゴールの分析とは，各アクターの行動のポリシーなどを，すでに定義された依存関係を元に，より高い抽象度をもったゴールから，より具体的なゴールへとどのように詳細化されるかを記述するものである．ゴール間の定義としては，ハードゴールの場合には，より具体的なゴールへと分解する Means-End 分解（**図 -7** における（1））があり，ソフトゴールの場合はゴールを満たすために，否定的（– で表される）か肯定的（+ で表される）に貢献（contribution）するサブ（ソフト・ハード）ゴールを同定する（図 -7 における（2））ことができる．肯定的に貢献するとは，他のゴールの達成に貢献する，ということであり，否定的に貢献するとは，他のゴールに対して否定的である場合である．計画に関する分解にはここでは触れないことにする．

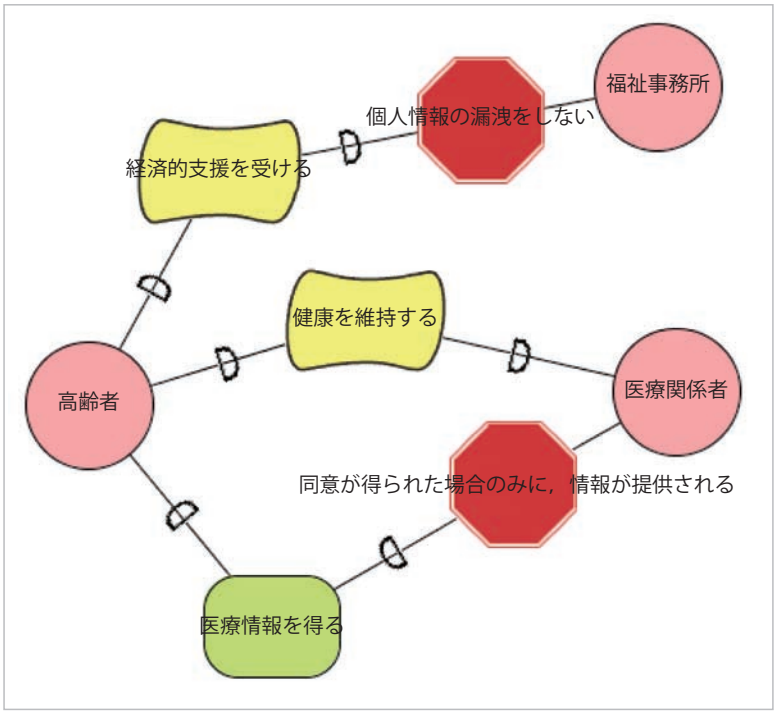

図 -6　eSAP 事例

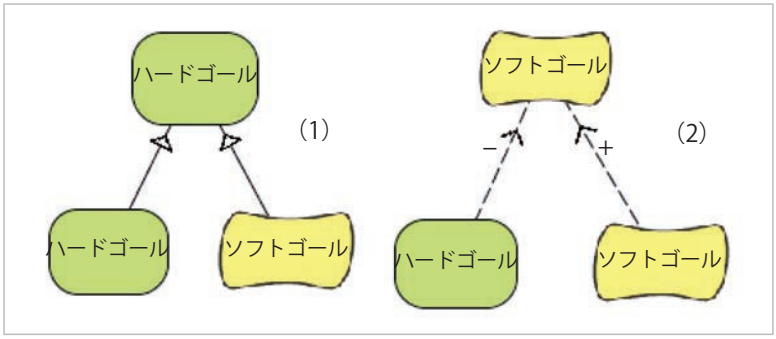

図 -7　ゴールの分解方法

次に図 -6 で示された eSAP システムの中で，アクター「医療関係者」を選び，そのゴールモデルを説明する（**図 -8**）．「医療関係者」に関連したゴールとしては，すでに，「健康を維持する」，「医療情報を得る」があったので，それらは「医療関係者」のゴール図においても現れる．「医療関係者」のセキュリティ制約である，「同意が得られた場合のみに，情報が提供される」を満足させるために，セキュアゴール「高齢者の同意を得る」が導入される．「健康を維持する」ソフトゴールを分析すると，「医療を提供する」というゴールがあり，両者の間には肯定的な貢献のリンクが張られる．「医療を提供する」というゴールは，さらに「医療計画を立案する」に分解され，それは「必要な医療内容を診断する」と「医療情報を得る」に分解される．

以上で駆け足だったが，セキュアトロポスにおけるアクター図とゴール図におけるモデル化の基本について述べるのを終わる．

事例と関連研究

セキュアトロポスを用いた事例としては，本稿で取り上げた英国における医療システムのモデル化が挙げられる．本モデル化においては，医療関係者，高齢者，福祉事務所，などのアクター間における，プライバシー情報などの守秘義務などについて分析を行ったものである．事例研究はまだ進んでいない状況であるが，これからさらにさまざまなシステムに対して適用例が出てくることが期待される．

セキュアトロポスと呼ばれるものには，本稿で紹介するものと，イタリアのトレント大学で開発したものがある．また，トレント大学の方で開発された方法論については Si*-Tool と呼ばれるツールが開発されており，Tropos のページからダウンロードができる [4]．本稿における事例はすべて，第一著者により開発された SecTro ツールを用いて記述されており，利用に興味が

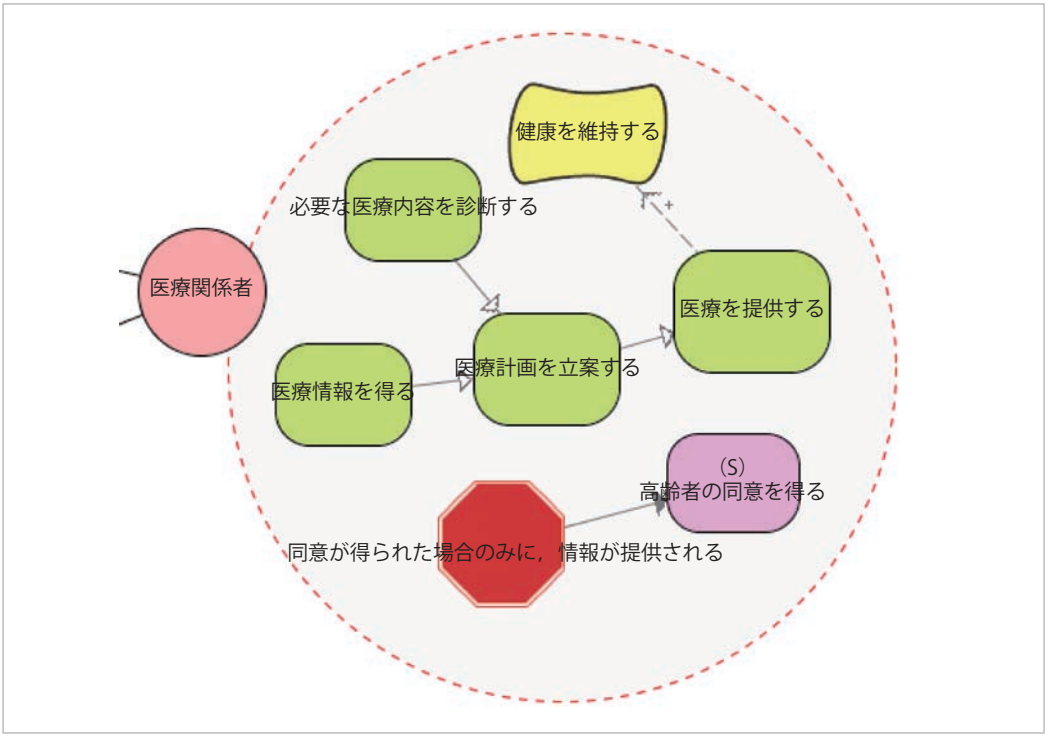

図 -8　医療関係者のゴール図

ある場合には第一著者にコンタクトされたい．

今後の展望

今後，本特集で紹介した多くのセキュリティ要件の分析・獲得方法論の利用は，セキュリティが重要な情報システムの開発において，非常に重要な地位を占めることが予想される．セキュアトロポスは完成された方法論ではなく，いまだに進化している方法論である．たとえば，筆者は現在，セキュアトロポスを用いて内部統制・IT 統制に関するモデリングを行っている．そこで得られた知見としては，「妥当性」や「信頼性」といった非機能要件と，コンプライアンスといった，法規制による制約という概念をモデル化するのに，セキュアトロポスが非常に適しているという点である．また，信頼（Trust）に関するモデリングの重要性が注目されているが，それらに対する研究においても用いられつつある．筆者は，さらに，セキュアトロポスによるモデルをより形式的に検証するための，フォーマルセキュアトロポスについての研究も今後行うことを予定している．

参考文献

1）Bresciani, P., Giorgini, P., Giunchiglia, F., Mylopoulos, J. and Perini, A. : TROPOS : An Agent Oriented Software Development Methodology, Journal of Autonomous Agents and Multi-Agent Systems, Kluwer Academic Publishers Vol.8, Issue 3, pp.203-236 (May 2004).
2）Mouratidis, H. and Giorgini, P. : Secure Tropos : Dealing Effectively with Security Requirements in the Development of Multiagent Systems, in Safety and Security in Multiagent Systems - Selected Papers, Barley, M., Masacci, F., Mouratidis, H. and Unruh, A, (eds), LNCS, Springer-Verlag (2006).
3）Mouratidis, H. : A Security Oriented Approach in the Development of Multiagent Systems : Applied to the Management of the Health and Social Care Needs of Older People in England, Ph.D. thesis, University of Sheffield, U.K., (2004)
4）Tropos web page, http://www.troposproject.org/
5）Taguchi, K. and Tahara, Y. : Curriculum Design and Methodologies for Security Requirements Analysis, Progress in Informatics, No.5, pp.19-34 (2008).
6）Chung, L., Nixon, B. A., Yu, E. and Mylopoulos, J. : Non-Functional Requirements in Software Engineering, Kluwer Academic (2000).

（平成 21 年 2 月 2 日受付）

Haralambos Mouratidis　▶H.Mouratidis@uel.ac.uk
2004 年英国シェフィールド大学 Ph.D. in Computer Science 取得．現在は，イーストロンドン大学 Principal Lecturer in Secure Systems and Software Development．これまでに，セキュアソフトウェア工学，要求工学，知的システム開発，マルチエージェントシステムなどについて 60 以上の論文を発表．Safety and Security in Multi-agent systems 国際ワークショップ，Global e-Security 国際会議などを創立．多くの国際会議において，委員長などを歴任．英国におけるサイバーセキュリティ知識移転ネットワークのメンバ．

田口 研治（正会員）　▶ktaguchi@nii.ac.jp
2001 年スウェーデン王国ウプサラ大学 Ph.D. in Computer Science 取得．九州大学助手，ウプサラ大学講師，ブラッドフォード大学講師を経て，2005 年 4 月より国立情報学研究所特任教授．主に，セキュリティ要求工学，形式手法などの研究・教育に従事．Integrated Formal Methods 国際会議シリーズを 1999 年に共同で創立，多くの形式手法，ソフトウェア工学の国際会議でプログラムコミッティを務める．