セキュリティ要求工学の概要と展望

吉岡 信和[*1]　Bashar Nuseibeh[*2]

[*1] 国立情報学研究所　[*2] The Open University

さまざまなインフラがIT化され，便利になるに従い，セキュリティの問題は社会の根幹にかかわる重大な問題になってきている．本稿では，まず，安全なシステムを構築するために必要なセキュリティソフトウェア工学の1つであるセキュリティ要求工学に焦点を絞って，現状と展望を解説する．セキュリティソフトウェア工学とは，セキュリティの関心事を，セキュリティとソフトウェア工学の専門家の双方により，要求工学，モデリング，アーキテクチャ，デザインやソフトウェア工学の実践に統合しようとする研究の1つであり，セキュリティ要求工学はその最も上流工程に位置する．本稿では，まずその必要性を説明した後，定義および，その難しさを整理する．そして，それに対して何をすべきかを概論する．

なぜ，今，セキュリティ要求工学が重要なのか？

近年，ネットバンキングや携帯を用いた株取引など，個人や経済の根幹部分にまで情報サービスが普及し，暮らしが便利になっている反面，安全上の問題も指摘されている．実際に，公式サイトを装ってクレジットカード番号やパスワードを盗むフィッシング（Phishing）の被害は社会問題にまで発展している．そのため，安全にそして安心して情報サービスが利用できるようにすることは，社会的にも急務の課題である．

セキュリティに関する脆弱性は，あらかじめすべてを把握することは難しい．そのため，インシデント（事件，事故）が起きてから，それに対応するためのソフトウェアパッチが作られたり，システムの運用ルールを厳重にするなどで対応することが多かった．たとえば，Windowsアップデートや，ノートPCを社外に持ち出さないようにするなどである．

これまではOSやライブラリ，SSH，Webサーバなどの広く一般に用いられているソフトウェア・言語の脆弱性を狙った攻撃が多かったため，システム管理者が注意深くそれらのアップデートをすることでセキュリティの対応をしていた．たとえば，バッファオーバフローを利用した攻撃がその代表である．しかしながら，この数年で，被害の形態が徐々にホスト，ネットワーク自身の脆弱性を狙ったものから，アプリケーション自身の脆弱性を狙ったものに変化してきている．たとえば，Webアプリケーションの場合，HTML中のスクリプトやブラウザのCookie情報を利用して，パスワードをアタッカに送信するような攻撃や，銀行口座の振込み処理のセッションを奪ってしまう攻撃が多くなってきている．これらの攻撃は，OSやブラウザのセキュリティアップデートだけで防ぐことは難しく，アプリケーションを構築する際に，このようなことを想定してHTML中のフォームにスクリプトが入力されていないか，Cookie情報が書き換えられていないかなどの対策が必要となる．

現状の情報システムの多くは，必要なセキュリティを考慮せずに，十分な理解なしで構築されている．そして，インシデントが起こってからその回避策のパッチを当てているのが実情である．しかしながら，多様な攻撃が次々に発見される現状では，パッチワークを繰り返していては，本質的な解決はできないばかりか，新しいパッチが新たな脆弱性を増やすことにもなりかねない．そして，場合によってはシステムの作り直しという膨大なコストをかけてしまうことになる．そのため，アプリケーションを開発する際に，セキュリティに関してそもそもどのような要求があり，どこまで対応すべきかを整理してから，その要求を満たすシステムを開発することが重要である．このようなセキュリティ要求が整理されていないシステム開発では，必要な要求が漏れ，抜けている可能性があるばかりか，（パッチを当てる作業も含めて）セキュリティに無駄なコストをかけている可能性がある．要求漏れは，ビジネスに多大な被害を及ぼす可能性があり，セキュリティにはコストがかかるため無駄も省く必要がある．

セキュリティ要求工学とは？

セキュリティ要求工学は，セキュリティに関する工学的アプローチ[1)]の1つである要求工学であり，要求工

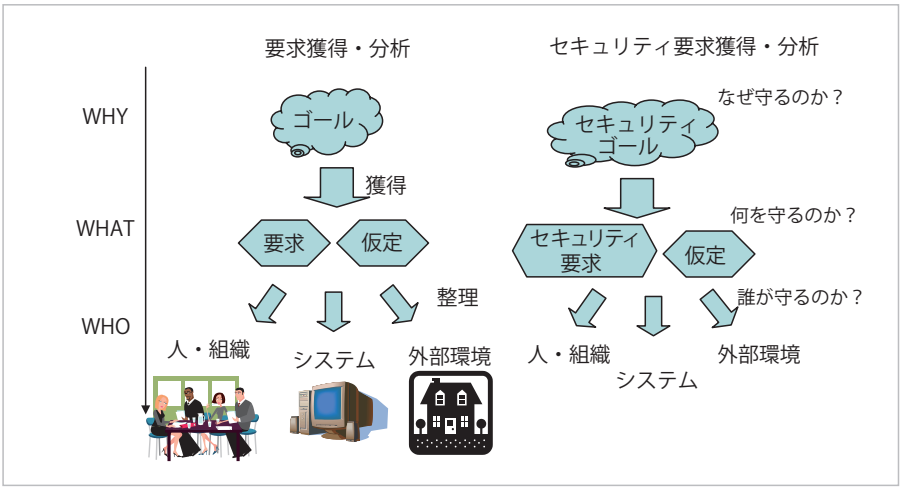

図 -1　セキュリティの要求の獲得と整理

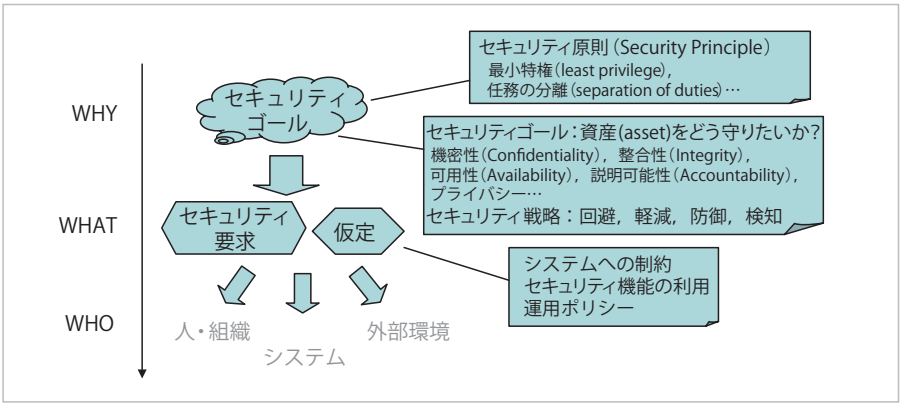

図 -2　セキュリティ要求工学に関する関心事

学の言葉[☆1]を借りれば，「セキュリティに関する要求をいかにしてまとめるかといった技術や技法の集大成」ということになる．

セキュリティに関する要求工学という意味で，要求工学と同様に獲得・整理できる部分もある．具体的には，**図 -1** の左に示すとおり，要求工学では，妥当な要求を獲得するために，要求そのもの（WHAT）とともに，その要求が必要な理由（WHY）となるゴールも分析する．そして，要求（WHAT）を整理した結果，その要求を満たす対象（WHO）を明らかにし，システムの要求部分を切り出し，最終的なシステムの要求仕様とする．WHAT には，システム運用環境など，要求が生じる仮定や前提条件なども整理する必要がある．要求のすべてがシステムにより満たされるわけではない．そのため，運用ルールなどの人や組織でカバーする範囲や，外部のシステムの利用など対象となっているシステムの外部環境で要求のどこまでをカバーするかを整理する必要がある．

セキュリティの場合も同様である．**図 -2** の右に示すように，セキュリティそのものの要求とともに，その理由をセキュリティゴールとして分析し，妥当な要求を獲得する．セキュリティゴールとは，顧客情報，決済情報など組織にとって重要な資産（asset）に対する組織の方針であり，セキュリティ原則（Security Principle）や機密性（Confidentiality），整合性（Integrity），可用性（Availability）などが含まれる．セキュリティ原則とは，資産をどのように扱いたいかという原理原則で，最低限の人にしか扱わせないという最小特権（least privilege）や予算執行者と監査人は同一人物では行わないといった任務の分離（separation of duties）がある．さらに，資産が攻撃されたときにどのように対処するかの戦略を定めたセキュリティ戦略もゴールとして定める必要がある．その戦略には，そもそも攻撃できないようにする回避（avoid），攻撃されても被害を最小限に抑える軽減（mitigate），被害が出ないようにする防御（prevent），または，攻撃されたことを記録だけ行う検知などがある．

セキュリティの要求と通常のシステムの機能に対する要求との違いは，セキュリティの場合，性能，ユーザビリティなどの非機能要求（機能以外の要求）という点である．つまり，セキュリティの要求は，それ自身システムが外部に提供する主機能に直結するわけではなく，機

☆1 要求工学についての詳細は，“情報処理，Vol.49, No.4, 2008”の特集「要求工学」を参照してほしい．

能への制約や付随的に提供すべきセキュリティ機能に関連する．たとえば，セキュリティライブラリパッケージでない限りは，通常，認証や暗号化などのセキュリティの機能は，システムの主目的に必要なわけではなく，主になる機能に安全という性質を持たせる際に必要な従属的な機能である．これは，主になる機能に対して性能や使いやすさの性質を求めること（非機能要求）と同様である．そのため，セキュリティの要求には，システムの使い方や振舞いに関する制約やセキュリティ機能を使ってどのように機能を実現したか，システムをどう運用したいか（機能をどう扱いたいか）などの運用ポリシーが含まれる．

セキュリティゴールやセキュリティ戦略を定めるためには，システムに対してどのような脅威やそれに対する被害がどれくらいありそうかというリスク分析が重要になる．セキュリティに関する脅威は，攻撃者によるシステムへの攻撃☆2による機密性などのセキュリティゴールの破壊である．たとえば，スパイウェアによる顧客情報（資産）の漏洩（機密性の破壊）などである．

リスク分析では，それらの攻撃がどの程度（確率，および頻度）で発生するかを予測した後，それによってどれくらい組織に被害が及ぼされるかを分析する．たとえば，顧客情報に被害が発生した場合，顧客情報に対する詫び状やクーポン券などの慰謝料☆3にかかる費用や，それによる製品の売れ行きの低下を予測する．

以上のように，セキュリティ要求工学では何を守るか（資産）を考え，それをどのような原則・方針で守るか（セキュリティゴール）を脅威などを考慮しながら定め，最終的には，システムの主機能に対する取り扱い・影響をセキュリティ要求として規定することがポイントとなる．以下では，そのようなセキュリティ要求を適切に獲得することに対する難しさを整理する．

セキュリティ要求の獲得・整理の難しさ

セキュリティ要求を獲得する方法は，通常の要求を獲得することと同様に，その理由（WHY）をあらわすゴールから分析できる．しかし，一方で，通常の要求とは異なる難しさが存在する．次では，技術的な観点と人・組織に依存した観点の両方から，その難しさを整理する．

☆2 セキュリティの定義に対してはコラムのセキュリティゴールの定義を参照のこと．

☆3 実際に 2004 年には，某大手企業の顧客情報が漏洩した際，450 万人の顧客に対して 500 円相当の金券を配布して詫び状を送った事件が発生している．そして，その後の民事裁判により，慰謝料として一人 5,000 円が妥当という判決が下りている．つまり，この場合の被害額は 225 億円にも上る！

セキュリティ要求を獲得する際の技術的な難しさには，(1) 扱う情報に対する複雑性，(2) 状況の変化，(3) トレードオフの 3 点がある．扱う情報に対する複雑性とは，セキュリティに関する関心事がさまざまな領域にまたがっていて，かつ，それらの情報が複雑に絡み合っているという状態を指す．たとえば，攻撃者の攻撃を分析するためには，IT に対する深い知識が必要になるが，その被害を予測するためには経済や法律に関する知識が必要となる．

さらに，資産やセキュリティ原則を決定するためには経営にかかわらなければならない．

その上に，攻撃が実際に起こり得るかどうかの発生確率の精度を上げるためには設計や実装の情報が必要になるが，その被害の予測などのリスク分析は，要求の重要度・優先度を決めるために要求を定める段階で行う必要がある．すなわち，さまざまな情報に依存関係があり，一筋縄ではすべての情報を決定することができないのである．

さらに，セキュリティの複雑性には，考慮できる可能性が膨大になるという点も挙げられる．たとえば，攻撃を列挙するだけでも，システムに対する攻撃のほかにも，クレジットカードを盗むことや建物に火をつけるなどの物理的な攻撃，人に対する脅しやだましなどの攻撃などあまりにも多くの可能性が存在する．さらに，これらに対する対策も，法律で罰を与えるなど，多種・多様になる．これらの攻撃は，建物に進入しやすい，教育が行き届いていないなど，特定の条件のときにしか発生しないものが多いが，要求を獲得する段階では曖昧なことも多い．これらは，要求として獲得すべき範囲が曖昧であることが問題の要因である．

Windows の頻繁なセキュリティアップデートに見られるように，日々新たな攻撃の可能性が見つかるのが現状である．セキュリティの要求を適切に獲得することにより，攻撃の可能性を減らすことはできるが，上記のように考慮すべき可能性が多いためすべてを網羅して対応するのはバグ発生率を 0%にするのと同様不可能である．そこで，安全なシステムとは，新しい攻撃が発見され，状況が変化してもそれに対応できるシステムであるといえる．

セキュリティは，考慮すべきことが多いことに加え，セキュリティの要求はそれぞれ優先度もあり，かつ，通常の要求とは矛盾する可能性すらある．たとえば，ネットバンクで機密性を保って振込みをしたいというセキュリティゴールに対して，機密性を完全に保つために攻撃者が口座にアクセスできないようにするという要求は，誰でもネットワーク経由でバンキングできるようにするという要求とは一見矛盾する．そのため，攻撃者が口座

にたとえアクセスしようとしてもアクセスできないようにするという要求の妥協が必要になる．また，この要求は，なるべく操作を簡略化しユーザに使いやすい機能を提供するという要求とも競合する．

これに加え，セキュリティの強度は，システムに対するリスクに依存する．たとえば，ネットバンクでは，口座残高が攻撃者によって操作されたときのリスクが非常に高いため，認証カードというハードウェアや複数の認証パスワード，強度の高い公開鍵暗号など，高いセキュリティが必要となる．それに対して，Blog の管理システムは，簡単なパスワード認証など低いセキュリティでも十分なことが多い．このように，セキュリティ要求を考えるときには，他の要素や優先度などを考慮したトレードオフがどうしても必要になる．

上記のように，セキュリティ要求の獲得は，技術的な難しさがあり，セキュリティに特化した新しい要求工学技術が求められている．本特集では，ゴール指向に基づく獲得手法と新しいセキュリティ要求獲得プロセスを紹介している．

セキュリティ要求を獲得するときの難しさは，純粋な技術的な難しさ以外にも組織や人がそれを獲得する意欲が非常に低く十分な予算・リソースが確保できない，責任の所在が明確にならないという非技術的な難しさも存在する．一般にセキュリティはなくてもシステムは機能するため，残念ながら，必要に迫られないと対応しない人や組織が多く存在する．理想的には，リスク分析を行った結果，どこまでセキュリティを考慮すべきか決定するのが望ましいが，そもそもシステムの要求獲得の既存プロセスにリスク分析が含まれていないため，その判断が存在しない組織が多いのが現状である．

その結果，分析のための十分な予算・リソースが確保できずに，結局，セキュリティに対する正しい理解がシステムの要求側と提供側の双方に得られないという悪循環になってしまう．しかしながら，金融基盤に IT を活用するようになった現在，セキュリティのリスクが増大しているのは明らかであり，それを無視し続けるのはリスクの拡大を助長することになりかねない．加えて，現在，政府機関のシステムをはじめとして，ソフトウェアの安全性を保証[☆4]する動きが広がってきている．

セキュリティに関する関心事は，さまざまな領域にまたがることを説明した．攻撃に対する対応は，頑丈な錠前やセキュリティカードなどのハードウェアを用いるものから，法律，教育，ネットワークの暗号化などさまざまな方法が考えられる．そのため，その対応を行う主体（組織・人）の種類が非常に多く，誰が何をすべきか，また，どのような方針で行うべきかが組織的に曖昧になってしまうという問題がある．誰に対して行うべきかを明確にし，情報を共有するために，技術ができることは多いが，それをうまく運用する体制作り[☆5]も重要である．

セキュリティのために何をしなければならないのか？

これまでに説明したとおり，セキュリティの要求を獲得するためには，資産の決定，リスク分析，セキュリティゴールの決定などさまざまなことを行う必要がある．その具体的な方法については，本特集では，続く「SQUARE ではじめるセキュリティ要求工学」で，セキュリティを考慮した要求獲得プロセスを紹介し，その次の 2 つの記事で，KAOS と Secure Tropos というゴール指向モデリングに基づく方法を紹介している．ここでは，一般にどのようなことをすべきかを紹介する．

図 -3 は，Haley[2] らが提案するセキュリティ要求工学のフレームワークにおけるセキュリティゴール・要求とシステムアーキテクチャの関係の抜粋である．この図は，セキュリティのみならず，一般的なゴール・要求とセキュリティに関する関心事の依存関係を示している．図の中の四角は，考慮すべき事柄を示し，破線矢印でその間の依存関係，実線で継承関係を示している．たとえば，資産は，ビジネスゴールから導出され，それからセキュリティゴールが導出される．そのセキュリティゴールは，セキュリティ要求を運用したり，セキュリティ機能要求の操作により満たされる．

この破線を逆にたどりおのおのの情報を中間生成物として作成するのがセキュリティ要求のための活動となる．しかしながら，図 -3 は，すべての情報，および，依存関係が表現されているわけではない．攻撃・脆弱性の情報などリスク分析に必要な情報は明記されていない．また，この図をみると，ゴールから要求の手順で情報を整理すればよいように見えるが，実際には，資産を守るために必要なセキュリティ要求は，パスワードやクレジットカードなど二次資産とよばれる新たな資産を仮定する必要があったり，制約を明らかにするために，セキュリティゴールを再考したり，さまざまな要求を一度に満たすような優先度付けが不可能になりビジネスゴールまで立ち戻って再考することが起こり得る．

図 -4 は，Lin Liu らが提案しているセキュリティ要求

☆4 安全性の保証に関する具体的な内容に関しては本特集の「コモンクライテリアにおけるセキュリティ要求の規定の現状と課題」を参照のこと．
☆5 組織体制に対する事例は，本特集の「日本ユニシスにおけるエンタープライズ・セキュリティ・アーキテクチャ（ESA）」で紹介している．

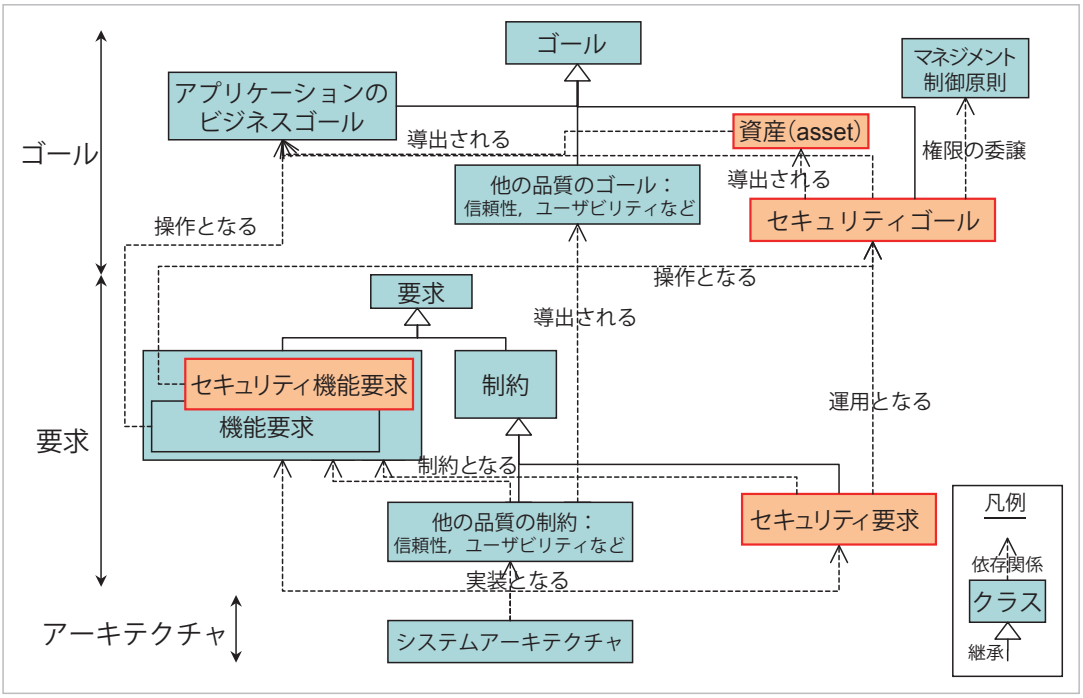

図 -3　セキュリティゴール，要求，アーキテクチャ間の依存関係

の獲得手順[☆6]である．この図の中の，赤色の箱が攻撃に対する分析であり，最終的には，対抗策であるセキュリティ要求を獲得する．この図を見ても分かるとおり，セキュリティ要求は，一度に獲得することは難しく，適宜再考しながら，内容を洗練する必要があり，洗練をサポートする技術的な仕組み[☆7]が求められる．

現状と今後の展望

本特集では，セキュリティ要求を獲得するための課題を解決するためのさまざまな技術，取り組みを紹介[☆8]している．それでは，それらの技術や取り組みを実践すれば誰でもセキュリティ要求を獲得できるのであろうか？　残念ながら現時点ではノーである．現状，さまざまな技術的，組織的課題が残っている．本特集で紹介しているプロセスやモデル，手法を使えば，さまざまな情報を獲得・整理する手助けになるであろう[☆9]．

しかしながら，どこまでの範囲を分析すればよいのかという明確な基準はなく，適切なコストで必要な要求を獲得するには，まだセキュリティ専門家のカンや経験に

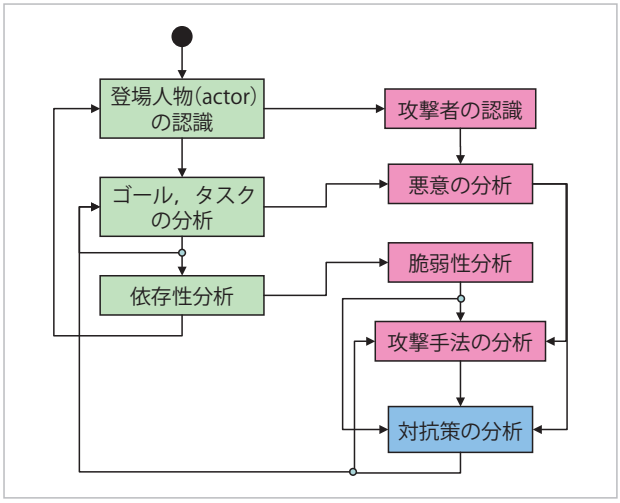

図 -4　セキュリティ要求の獲得手順例

依存する部分も多い．また，セキュリティに関係する利害関係者（ステークホルダ）に，どのように参加してもらうかに関しては，システムがおかれた組織的状況やその性質に依存する部分が多く，最適なプロセス（手順）を定める指針は明らかにされていない．適切なセキュリティレベルを設定し，保証する仕組みに関しては，まだまだ研究が始まったばかり[☆10]である．

今後，これらを解決するための，ビジネス分析などを含むより広い範囲の業務プロセスへのセキュリティの統合が必要になるであろう．そのプロセスでは，経営に携わるものはもちろん，法律家なども適切なタイミングで参加できる必要がある．これらのステークホルダは，ソフトウェア工学，システム工学の領域とはあまりにも違

☆6 文献 3）の図では，すべてのアクティビティは，Identification となっているが，図 -4 では，文脈に合わせて認識と分析に分けた．
☆7 セキュリティ要求を整理・獲得するさまざまな取り組みは，本特集の「実践的セキュリティ要求工学に向けて」で紹介している．
☆8 他の技術や取り組みなどは，文献 4）が参考になる．
☆9 そういう意味で本特集が読者の手助けになれば幸いである．
☆10 セキュリティに関する将来的な課題に関しては，文献 5）や 6）にも解説がある．

うため，コミュニケーションをどのようにうまくとるかがポイントとなる．

現在，ソーシャルエンジニアリングといわれる分野があり，人間・組織活動をいかにモデル化するかが議論されている．セキュリティでは，人間・組織活動をモデル化するとともに，異分野間の活動をサポートする技術が重要となる．危機管理などセキュリティはITシステムだけでなく，いろいろな分野で別々に発展をしている．これらの異分野の技術をうまく統合することも必要であろう．さらに，安全を保証するための数学的な基盤と，それをプロセスに取り込むことが将来にわたった課題といえる．

参考文献
1) Anderson, R. J. : Security Engineering : A Guide to Building Dependable Distributed Systems, John Wiley & Sons Inc. (2008).
2) Haley, C. B., Laney, R., Moffett, J. D. and Nuseibeh, B. : Security Requirements Engineering : A Framework for Representation and Analysis, IEEE Transactions on Software Engineering, IEEE, Vol.34, Issue 1, pp.133-153 (2008).
3) Liu, L., Yu, E. S. K. and Mylopoulos, J. : Security and Privacy Requirements Analysis within a Social Setting, In Proceedings of RE'03, IEEE Computer Society, pp.151-161 (2003).
4) Allen, J. H., Barnum, S., Ellison, R. J., McGraw, G. and Mead, N. R. : Software Security Engineering, Addison-Wesley (2008).
5) Beznosov, K. and Chess, B. : Software Security for the Rest of Us : An Industry Perspective on the Secure-Software Challenge, IEEE Software Vol.25, No.1, pp.10-12 (2008).
6) Devanbu, P. T. and Stubblebine, S. : Software Engineering for Security : a Roadmap, The Future of Software Engineering, ACM Press, pp.227-239 (2000).

（平成21年2月6日受付）

コラム◆セキュリティ用語

◆セキュリティゴール：
資産を被害（harm）から守ることに関するゴール．セキュリティにおいては，被害を悪意のある攻撃者によるものと限定する場合が多い．その場合，悪意のない事故は，セーフティとして扱い，本特集でもそのように定義する．悪意があるかどうかという意味で，セキュリティはセーフティの一部の領域を扱っているともいえる．しかしながら，攻撃者の能力が高い場合，ミスでは通常起こり得ない（無視できるほどの確率の）複雑なステップを経た攻撃があり得るため，考慮すべき点はセーフティに比べ少なくなるわけではなく，むしろ多くなる．ちなみに，日本語ではセキュリティとセーフティの間には用語の区別はなく両者とも安全性と訳す．

◆資産（asset）：
あるステークホルダにとって価値（value）のある有形・無形の資産．たとえば，お金，リソース・情報・ハードウェアなど．

◆リスク（risk）：
資産に対して，その被害が起こる確率，および，被害の大きさの双方を表す．被害が起こる確率を考慮するために脆弱性（vulnerability）や脅威（threat）を分析したり，被害の大きさを測るために資産価値を分析したりする必要がある．

◆攻撃者（attacker）と攻撃（attack）：
意図的にシステムに悪影響を及ぼす操作（attack）を行う利用者や他のシステムインシデント（incident）：想定外のイベント，特にシステムや資産に被害を及ぼす，もしくは，可能性がある事象を指す．

◆機密性（Confidentiality）：
限られた人・組織のみが閲覧，書き換えなどができること．そのルールはアクセス制御ポリシーとして規定され，セキュリティ要求の代表例である．

◆整合性（Integrity）：
完全性とも言われ，情報が変化せずに完全に保たれている状態で，その情報をだれがいつ作成，変更したかを同時に証明できるようにすることが多い．

◆可用性（Availability）：
必要なときに必要な情報・サービスが利用可能になっていること．

◆セキュリティ戦略：
攻撃を受けたときの対応方針のことで，一般に，そもそも攻撃を受けないようにする回避，攻撃の被害が広がらないようにする軽減（mitigate），被害を出さなくする防御（prevent），および，攻撃を受けたことを検知（detection）するなどがある．この戦略は，攻撃に対する被害の度合いや対応策（counter-measure, objective）にかかるコストにより決定し，被害が少ない場合，検知だけして，後から対策を検討する場合もある．

吉岡 信和（正会員）　▶nobukazu@nii.ac.jp
1998年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了．博士（情報科学）．同年（株）東芝入社．2002年より国立情報学研究所に勤務，2004年より同研究所 特任助教授，現在准教授．エージェント技術の研究，ソフトウェア工学の研究に従事．日本ソフトウェア科学会，電子情報通信学会各会員．

Bashar Nuseibeh　▶B.A.Nuseibeh@open.ac.uk
Imperial CollegeのSoftware enineeringでPh.D.を取得．Imperial Collegeを経て，現在，the Open University教授．Imperial College，および，国立情報学研究所 客員教授．ソフトウェア工学，デザイン，ソフトウェアモデリング技術等に興味を持つ．the British computer Society，the Institution of Engineering and Technology，および，Chartered Engineer フェロー．IEEE Computer Society 会員．