プライバシとセキュリティの要求工学の統合化するフレームワーク

吉　岡　信　和[†1,†2]

本稿では，プライバシを配慮したシステムを構築する際の要求に関する課題を整理し，その課題を解決するフレームワークを提案する．

Research Challenges on Integration of Privacy into Security Requirements Engineering

Nobukazu Yoshioka[†1,†2]

We illustrate research questions on privacy requirements which we need to consider during development of a system. We, then, propose a framework to answer the questions.

1. はじめに

近年，クラウド上のサービスやモバイルサービスを提供する際に，プライバシが問題となることが多くなってきている．ウェアラブル機器など個人が身につける電子機器から得られるセンサー情報を使った便利なサービスが増え，利用者は個人に関する情報をサービスに提供する機会が多くなってきている．これらの情報と，決済や認証のために必要な個人を特定する情報（個人情報）を組み合わせると簡単にプライベートな情報[⋆1]を知ることができるようになる．

ここでプライバシの配慮は，サービス利用者の権利を守るために必要である．そして近年プライバシ関連の法案が整備されるなど，プライバシは社会としても重要な関心事である．このプライバシの考慮は，サービスの提供方法や内容に影響を及ぼすため，要求仕様の策定段階から考えておく必要がある．しかしながら，プライバシをどこまで考慮すべきかは，個々の利用者の主観や社会性に依存し，時間や状況によっても変化するため，容易に明確にできない．また，プライバシの保護は，一般にサービスの利便性やセキュリティ，機能性等と相反することがあり，適切にその要求を決定することが難しい．

加えて，プライバシ要求の考慮は，セキュリティを切り離して考えることはできない．なぜならば，プライバシ要求はセキュリティ要求と相互に依存しているからである．OECD が 1980 年に採択したプライバシ・ガイドラインには，安全保護の原則として個人データの合理的安全保護措置が含まれている．つまり，個人に関するデータのセキュリティの担保がプライバシの担保の必要条件となっている．また，セキュリティ要求を考慮する際には，個人の確認を前提とする事が多く，これがプライバシ要求と対立する可能性がある．そのため，プライバシ要求とセキュリティ要求は同時に考慮し，適切な要求を決定する必要がある．そのため，プライバシ要求とセキュリティ要求の抽出・分析・規定といった双方の要求工学を統合化したフレームワークが必要である．

本稿では，プライバシとセキュリティの関心事に関する要求工学を統合化する際の技術的課題を整理し，その課題を解決する統合フレームワークを提案する．

2. プライバシをセキュリティ要求工学に統合する際の研究課題

プライバシ要求の抽出・分析・規定をセキュリティ要求工学に統合する場合，大きく分けてプライバシ固有の課題と，両者の要求を統合する時の課題の 2 種類の研究課題がある．以下で，それぞれの課題に関連したリサーチ・クエスチョンを整理する．

2.1 プライバシ固有のリサーチ・クエンチョン

プライバシは，個人の主観や個人が置かれる状況に左右され，個々人や状況によりその要求は異なってくる．また，個人が考えている都合と，開発したいシステムとの関係は必ずしも明確ではない．そのため，個

†1 国立情報学研究所 GRACE センター
GRACE Center, National Institute of Informatics
†2 総合研究大学院大学 複合科学研究科 情報学専攻
The Graduate University for Advanced Studies (SOKENDAI)

⋆1 本稿では利用者がプライベート（他者に秘密にしたい）と思う情報をプライバシ情報と呼ぶ．

人が求めるプライバシ要求（もしくはプライバシポリシー）を抽出し，その要求を満たすサービスの仕様に関連づけるためには，以下のリサーチ・クエンチョンに答える必要がある．

(RQ1:抽出方法) 曖昧で一貫性がなく，暗黙的である個々のプラバシポリシーをどう明確化するか？

(RQ2:関連付け) システムに関連するプライバシポリシーをどう選択し，関連付けるか？

(RQ3:範囲の規定) システムでは，どこまでの範囲のプライバシポリシーを受け入れ，それ以外のポリシを持つ顧客[⋆1]を取り扱かわないか？

ここで，(RQ3) で規定した範囲外のポリシを持つ顧客に対しては，システム利用に関する留意事項に利用に関するプライバシポリシーを明記し，これに合意できない顧客は利用しないよう呼びかけるなどの運用が必要となる．

2.2 統合化に関するリサーチ・クエンチョン

1 章で述べたようにプライバシ要求とセキュリティ要求はお互い密接な関係がある．そこで，プライバシ要求の抽出・分析・規定を従来のセキュリティ要求工学に統合する場合，以下のリサーチ・クエンチョンに答える必要がある．

(RQ4:帰着) どこまでのプラバシ要求をセキュリティ要求工学の問題に帰着させられるか？既存の手法で代用できる部分はどこか？

(RQ5:拡張) 既存の手法で不足している部分はどこか？既存の手法をどう拡張すればよいか？

(RQ5:競合発見と解決) プライバシとセキュリティの要求の競合をどのように発見し，それを解決するか？

3. プライバシとセキュリティ要求を統合化した要求分析フレームワーク

2 章で述べたリサーチ・クエスチョンに答えるために，プライバシとセキュリティ要求を統合化した要求分析フレームワークの概念図を図 1 に示す．

本フレームワークでは，まず，(RQ1) に答えるため，顧客のプライバシに関する考え方（プライバシニーズ）をマーケティングの技術を活用して整理し，典型的なターゲット顧客が考えるプライベートな事象を規定する．マーケティングの技術を使って，ターゲット顧客を規定することで，(RQ3) の扱う範囲が明確になる．

また，上記とは並行してシステムの機能要件を規定しておく．次に，(RQ2) に答えるため，プライベートな事象と，システムが利用可能な情報や振る舞いとの関連を整理する．具体的にはプライベートな事象が知られたくない人に知られてしまう可能性があるシステム上の情報やイベントを関連付け，それらの情報をプライバシ資産として規定する．この段階でプライバシ資産として規定できれば，セキュリティ資産と同様，その保護はセキュリティの従来手法が適用可能である．これは，(RQ4) の解答につながる．

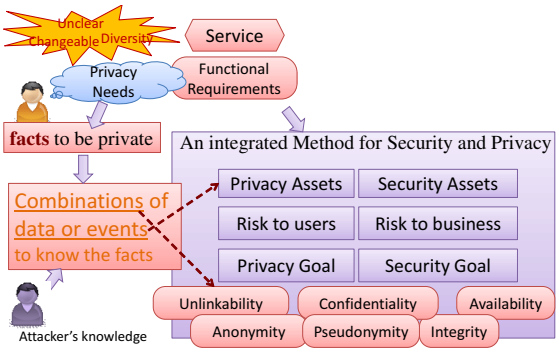

図 1 プライバシとセキュリティ要求の統合フレームワーク

さらに，知られたくない人に対する知られたくない事象は，従来のセキュリティ要求の機密性 (Confidentiality) の概念を拡張して扱うことができる．セキュリティ要求では，機密性の定義を公開相手と内容といった単純な形式で規定することが多い．しかしながら，プライバシ要求では公開相手や内容の抽象度（匿名の度合い）が状況によって変化するため，それらに対応するための拡張が必要である．秘匿性に加えてリンク可能性など，セキュリティ要求にない概念も取り扱う必要がある．

(RQ5) に対しては，セキュリティとプライバシ要求が競合するパターン，およびその解決のパターンを提示する．競合の解決には，どちらかの要求を優先させるなどの緩和パターンやどちらの要求も同時に満たす Win-Win パターンを開発者に提示する．そして，これらのパターン間の関係を整理したセキュリティとプライバシに関するパターン言語を開発者に提供する．

4. おわりに

本稿では，プライバシ要求に関する課題と，それをセキュリティ要求工学に統合する際のリサーチ・クエスチョンを整理した．そして，リサーチ・クエスチョンに解答するための統合フレームワークを提案した．今後，このフレームワークを詳細化し，具体的な提案につなげていく予定である．

⋆1 本稿では，システムを利用する可能性のある人を“顧客”と呼び，システムを実際に利用する“ユーザ”と区別する．