平成 25 年度
ＳＳＲ産学戦略的研究フォーラム応募書類
(研究計画書)

情報セキュリティ大学院大学 情報セキュリティ研究科
准教授 大久保隆夫

2013 年 5 月 15 日

1　調査研究テーマ名

セキュリティとプライバシーを考慮したソフトウェア開発における共通問題の調査研究

2　そのテーマの戦略的意義／位置付け

本研究の戦略的意義は，産学が共同で用いることのできる，セキュアなソフトウェア開発手法の実験，評価用の標準的なデータ（共通問題）を作成することにある．

昨今の遠隔操作事件など，ソフトウェアの脆弱性をついた攻撃は後を断たない．また，ビッグデータ利用の推進にともない，個人のプライバシー情報の漏洩事故も問題になっている．脆弱性を持たず，プライバシーにも配慮したセキュアなソフトウェア開発が社会にとって必須である．しかし，従来のソフトウェア開発手法のみでは解決は困難であり，開発の最上流工程からセキュリティを意識した開発方法が現場に望まれる．これらの開発方法は主に大学などの学術系研究期間で研究が行なわれており，海外では SQUARE[3]，SDL[1]，ミスユースケース [6]，UMLsec[2] など，国内においても MASG[5]，Twin peaks のセキュリティ応用 [4]，セキュリティパターンを用いた手法 [7] などが提案されている．しかし，特に日本において開発現場への適用が進んでいるとは言いがたい．その主な原因は，プラクティカルなデータを用いて手法の実験，評価を行なうことが困難になっているためと考えられる．

産業側の開発に関わるデータを直接学術側に提供することには，データが企業機密や顧客情報，また成果物がノウハウや知財情報などを含むため，産業側からの抵抗が強い．また，逆に研究開発した手法を開発現場に導入，試行することについても，手法が十分な評価を得ていないことに対する品質面の不安や，納期などの問題により産業側としては導入しにくくなっている．このように，データと手法が産学間で相互提供，評価されないことにより，ソフトウェア開発におけるセキュリティの問題はなかなか改善しない負のスパイラルを生んでいる．

学術側がセキュアな開発手法の評価に用いることのできるデータは，大学側で独自に作成したものか，オープンに提供されているデータが中心になるが，これらは評価そのものを主眼としているものが多く，産業界における現状に即したものという保証はない．

後者については，ソフトウェア開発全般を対象として，国内外でいくつか事例が存在する．TEFSE Workshop[*1]では，トレーサビリティを検証するベンチマークを提供している．また，コードメトリクス，開発履歴から欠陥などを予測するデータセットを開発する PROMISE SOFTWARE ENGINEERING PROJECT[*2]や，国内では大阪大，和歌山大等複数大学が共同で教材向けベンチマークを開発する IT Spiral プロジェクト[*3]などが存在する．PROlMISE プロジェクトは，開発の断片的な側面を示すデータを提供するのみで，欠陥予測や見積手法の検討には使えても，開発手法検討のベンチマークにはならない．またこれらはいずれもセキュリティに重点を置いたものではないため，セキュリティの評価のためのデータセットとしては十分とは言えない．

セキュリティに特化して評価可能なものは，iTrust[*4]など，数少ない．iTrust においても，特にセキュリティが必要な状況を想定していない，要求のみで設計情報がないためトレーサビリティの評価として不十分である，など評価として十分なものとは言えない．

上記のソフトウェア評価事例の問題は，ソフトウェア工学では「ソフトウェア工学の共通問題[*5]」の問題として知られているが，セキュリティに限定すると，共通問題の例は更に少なく，より深刻な問題となっている．

3 調査研究の概要

本研究では，上記の負のスパイラルを断つために，開発の最上流工程からセキュリティを意識した開発方法の確立を目標とし，産学の参加者が共同で，開発手法の実験評価のためのソフトウェア（共通問題）事例を策定する．産業側の関係者が参加することで，開発現場から乖離した事例作成を防止し，かつ独自に作成することで機密情報や知財情報の漏洩に関係ないデータを作成できる．作成した事例が世界的に標準事例として用いられるようになれば，様々な手法を同一のデータで比較評価することができるようになり，手法の進化の促進が期待できる．また，現場の実例に近い事例の評価結果が得られることで，産業側としても手法の導入への抵抗が少なくなる．産業界への手法の導入が進めば，その適用の評価のフィードバックを学術側が受けることができるようになる．

本研究におけるセキュアな開発手法は，下記要件要件の一部，もしくは全てを満たすことを目標としている．

- 開発のあらゆる段階・工程でセキュリティを明示的に扱う
- 開発のあらゆる段階・工程でセキュリティ以外の品質特性への影響を明示的に扱える
- セキュリティの分析や対策の結果（例えばセキュリティ要求分析，セキュリティ設計，セキュアコーディング，セキュリティテスティング）が段階・工程をまたいで接続され，追跡できる，
- セキュリティ上の新たな脅威や対策の発見に応じて絶えず更新，保守できること

具体的には下記の作業を計画している．

1. 既存のセキュリティ向け共通問題例，および適用開発手法の調査
   国内外を問わず，公開されているソフトウェアの事例，および，適用対象となるセキュアなソフトウェア開発手法（要求分析，設計，開発，テスト手法）の候補について調査を行なう．

[*1] http://www.coest.org/index.php/resources/tefse
[*2] http://promise.site.uottawa.ca/SERepository/datasets-page.html
[*3] http://www.kantei.go.jp/jp/singi/it2/ithyouka/hearing/kyouiku/dai3/siryou1.pdf
[*4] http://agile.csc.ncsu.edu/iTrust/wiki/doku.php?id=start
[*5] ウィンターワークショップ２０１３・イン・那須 http://www.kishi.mgmt.waseda.ac.jp/wws2013/

2. 共通問題例の作成
   共通問題として必要な要件を整理した上で，事例の作成を行なう．事例は（要求仕様，設計仕様，プログラム成果物（予定），テスト仕様で構成される．
3. 適用開発手法候補の選定
   ソフトウェア開発に適用する手法の候補を選定する．
4. 開発手法に基づくソフトウェア開発（一部）
   作成した共通問題例に基づき，手法の適用を行なう．ただし今年度は完全適用ではなく，一部の工程および手法について試験的に行なう．

なお，本研究の成果物であるプログラムについては，OSS に準ずる形で公開し，誰もが利用可能な標準的データセットとして提供する予定である．

4　調査研究の進め方（共同研究者など）

本研究は．大学側共同研究者，企業研究者に SSR 賛助会員のメンバーを加えた構成で遂行する．大学側のメンバーは，ソフトウェア工学（要求および開発手法）の研究者およびセキュリティの研究者で構成される．企業側および SSR 賛助会員のメンバーは，開発現場でソフトウェア開発に携わる部署，ないしその関連部署を想定している．

本年度は，セキュリティを考慮した開発を行なう上で，適用する開発手法の評価に適したソフトウェア仕様（要求仕様，設計仕様，プログラム）を産学共同で作成する．ソフトウェアは以下の要件を満たす必要がある．

1. ソフトウェア事例は，実際に現場で運用できる機能を有する実用的なものか，あるいは現実のソフトウェアに置換えて手法評価を行えるもの．
2. 特定のドメイン（複数）に属するものであるが，他のドメインにも転用可能と考えられるもの
3. スケーラビイティ評価に十分であるが，一方，限られた時間で評価が可能である適切な規模のもの
4. 一般化可能なセキュリティ脅威，脆弱性を包含する可能性のあるものであり，かつ現実的に解決可能な対策が存在するもの

上記要件 1 については，企業メンバーおよに賛助会員，2，3 についてはソフトウェア工学の研究者，4 についてはセキュリティ研究者の意見を汲みつつ，共同で作業を進める．対象とするソフトウェアは，現在開発中の情報セキュリティ大学院大学教務システムをベースに検討を予定している．ソフトウェアの策定までに，概ね月 1 回程度のミーティングによる作業を予定している．また，調査および手法評価，ソフトウェア開発については各担当者により作業を進める．開発にあたっては，主査の豊富な開発・コンサル経験を活かして開発を進める．

本研究の調査研究メンバーの所属，および専門領域は，下記の通りである．

- 主査
  - 大久保 隆夫：情報セキュリティ大学院大学 情報セキュリティ研究科 准教授
    アプリケーションセキュリティ，Web セキュリティ，ソフトウェア工学
- 大学側共同研究者
  - 吉岡 信和：国立情報学研究所 准教授
    ソフトウェア工学，特に要求工学，セキュリティ，プライバシー保護

- 海谷 治彦：信州大学工学部 准教授
  ソフトウェア工学，特にトレーサビリティ，インパクト分析
- 鷲崎 弘宜：早稲田大学基幹理工学部情報理工学科 准教授
  ソフトウェア工学，特にソフトウェア設計，ソフトウェア品質保証，ソフトウェア再利用，ソフトウェアセキュリティ
- 柿崎淑郎：東京電機大学 未来科学部情報メディア学科 助教
  情報システム，情報セキュリティ，電子認証，アイデンティティ管理

- 産業界（共同研究者）
  - 現在打診中

参考文献

[1] Howard, M. and Lipner, S.: *The Security Development Lifecycle*, Microsoft (2006).

[2] Jürjens, J.: UMLsec: Extending UML for secure systems development, *Fifth International Conference on The Unified Modeling Language (UML 2002)*, LNCS, Vol. 2460, Springer, pp. 412–425 (2002).

[3] Mead, N. R. and Stehney, T.: Security quality requirements engineering (SQUARE) methodology, *ACM SIGSOFT Software Engineering Notes*, Vol. 30, No. 4, pp. 1–7 (2005).

[4] Okubo, T., Kaiya, H. and Yoshioka, N.: Mutual Refinement of Security Requirements and Architecture Using Twin Peaks Model, *Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual*, pp. 367–372 (2012).

[5] Okubo, T., Taguchi, K. and Yoshioka, N.: Misuse Cases + Assets + Security Goals, *CSE (3)*, pp. 424–429 (2009).

[6] Sindre, G. and Opdahl, A. L.: Eliciting security requirements with misuse cases, *Requir. Eng.*, Vol. 10, No. 1, pp. 34–44 (2005).

[7] 小橋孝紀，大久保隆夫，海谷治彦，吉岡信和，伊永祥太，鷲崎弘宜，深澤良彰モデルテストによるセキュリティ分析・設計パターンの適用支援，コンピュータセキュリティシンポジウム 2012 論文集，Vol. 2012, No. 3, pp. 655–662 (2012).

付録 A　申請者

- 氏名：大久保 隆夫
- 学歴：
  1989 年 3 月 東京工業大学工学部情報工学科卒業
  1989 年 4 月 東京工業大学大学院総合理工学研究科物理情報工学専攻入学
  1991 年 3 月 東京工業大学大学院総合理工学研究科物理情報工学専攻修了 (工学修士)
  2006 年 4 月 情報セキュリティ大学院大学情報セキュリティ研究科博士後期課程入学
  2009 年 3 月 情報セキュリティ大学院大学情報セキュリティ研究科博士後期課程修了 (博士 (情報学))
- 職歴：
  1991 年 4 月 ～ 2004 年 12 月 株式会社富士通研究所 ソフトウェア研究部

2004 年 12 月 ～ 2013 年 3 月 同研究所セキュアコンピューティング研究部
2013 年 4 月 ～ 現在 情報セキュリティ大学院大学 情報セキュリティ研究科 准教授

- 連絡先：
  情報セキュリティ大学院大学 情報セキュリティ研究科
  〒221-0835 横浜市神奈川区鶴屋町 2-14-1
  Tel，FAX:045-310-0232
  E-Mail: okubo@iisec.ac.jp

以上