Vol.2014-CSEC-65 No.4
Vol.2014-IOT-25 No.4
2014/5/22

Web アプリケーション更改時の セキュリティ要求/要件獲得手法の検討

野口睦夫[†,a)]　大久保隆夫[†,b)]　田中英彦[†,c)]

あらまし　近年，インターネットに公開されている Web サイトに対して，日常的に不正アクセスが行われている．それにともない，情報セキュリティ対策の重要性が認識されてきた．しかし，発注者がセキュリティ対策を受注者に任せっきりの状況があり，開発の最上流からセキュリティを考慮した対策が行われないことが，脆弱性を生む一因となっている．受入試験での確認を前提に，筆者らは，必要とされるセキュリティ知識を極力減らすために，システム機能ベースセキュリティパターンを拡張した手法を検討している．それにより，発注者でもセキュリティ要件を導き出すことが可能になることが期待できる．本稿では，検討中の手法を紹介するとともに，Web アプリケーション更改時のセキュリティ要求/要件を獲得するためのアプローチに関する検討状況を示す．

Study of security request / requirement acquisition technique of Web application renewal time

MUTSUO NOGUCHI[†1,a)]　TAKAO OKUBO[†1,b)]
HIDEHIKO TANAKA[†1,c)]

Abstract Recently, the Web site that is exposed to the Internet, unauthorized access is routinely performed. Along with it, the importance of information security measures has increased. However, that there are situations in which the purchaser is left to the discretion of the contractor security measures, measures that takes into account the security from the most upstream of the development process is not performed, have contributed to produce a vulnerability. Assuming confirmation of acceptance test, in order to reduce as much as possible the security knowledge that is required, we have considered an approach that extends the feature-based system security pattern. Thus, it is expected that it is possible to derive the security requirements in the ordering party. In this paper, we introduce the technique under consideration, shows the situation on the study approach for obtaining a security request / requirements for the Web application renewal time.

1. はじめに

インターネット上では不正アクセスが日常的に行われており，Web サイトの改ざんなどのインシデントも多く報告されている．[1] それにともない，Web サイトを構成する OS やネットワーク機器，セキュリティ機器などのプラットフォームだけではなく，Web サイト上のサービスを実現するソフトウェア，すなわち Web アプリケーションに対する情報セキュリティ技術の重要性が認識されてきた．[2]

また，一度 Web サイト上で公開されたサービスは，幾度もの更改を繰り返して，継続的にサービスが提供されている．そのサイクルのなかで，特に独自に作り込まれた機能が修正される際に，セキュリティ対策が漏れ，脆弱性が埋め込まれることも多い．筆者の脆弱性診断を実施してきた経験でも，新規に開発された Web アプリケーションでは存在しなかった脆弱性が，更改時にセキュリティ対策の漏れにより，脆弱性が埋め込まれてしまう事例を体験している．その際に要件定義書や設計書を確認する機会もあるが，明確なセキュリティ要件が定義されていることは，ほとんど存在しない．

そこで，本稿では，Web アプリケーション更改時に実施すべきセキュリティ要求/要件の獲得手法についての検討を行う．

2. 背景と関連研究

筆者の経験上，Web アプリケーションの開発プロジェクトにおける各開発プロセスにおける発注者と受注者の責任範囲の関係は Figure 1 のようになっている．

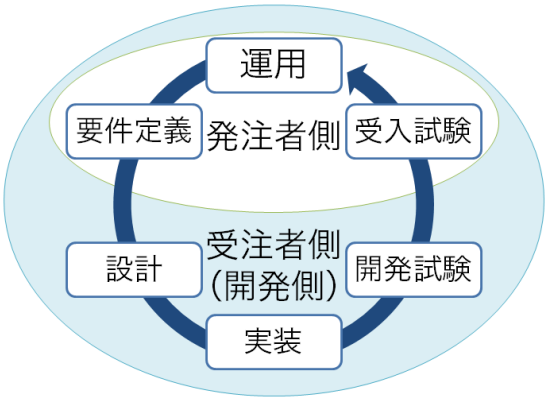


Figure 1　各開発プロセスにおける
発注者と受注者の責任範囲

† 情報セキュリティ大学院大学
Institute of Information Security
a) mgs115502@iisec.ac.jp
b) okubo@iisec.ac.jp
c) tanaka@iisec.ac.jp

発注者側は『実現したい機能を決める要件定義』『受注者側によって実装された Web アプリケーションに対して要件の充足度を確認する受入試験』『実際に利用する運用』の各プロセスに責任を持つ．そして，受注者側は開発のプロフェッショナルとして，発注者が責任を持つ各プロセスに対しても，支援という形で関わることになる．しかし，開発現場の実態として，発注者は実現したい要求を受注者側に伝えるだけで，要件定義は支援の枠を越えて受注者側任せになっていることも少なくない．

インターネット上に公開された Web サイトであれば，Web アプリケーションに脆弱性が存在すると，Web サイトの提供元である発注側の責任が問われる．そして，不正アクセスによる Web サイトの改ざんなどのインシデントが身近な存在になっている現在，発注者側が Web サイトに対してセキュリティ面での安全性が確保されていることを確認する責任の重要性が増している．そこで重要になるのがセキュリティ対応の要件を決める『要件定義』と要件に従って実装されたかを発注者側が最終確認する『受入試験』の各開発プロセスである．これは[3]でも紹介されているようにシステム全体のコストに大きく影響することからも，発注者側が開発プロセスに関わることの重要性がわかる．

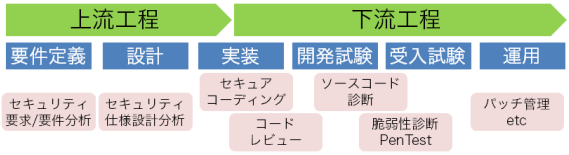


Figure 2　各開発プロセスにおけるセキュリティ対策

Figure 2 は筆者の経験上，Web アプリケーションの開発プロセス内に組み込まれることがあるセキュリティ対策である．これらセキュリティ対策の内，実際に現場レベルで浸透しているものは，パッチ管理とセキュアコーディング，コードレビューくらいである．次いで脆弱性診断やソースコード診断が行われており，すべて受注者側が主に責任を持つ下流工程の開発プロセスにおけるセキュリティ対策となっている．

上流工程に位置する要件定義で実施するセキュリティ対策として，セキュリティ要求/要件分析があるが，実際に行われているプロジェクトを筆者の経験ではほとんど見たことがない．実際に行われない主な理由として，大久保らは以下を挙げている．[4]

1) 要求分析においてセキュリティが重要視されていない
2) セキュリティ要求分析のためのノウハウを持つ開発者がいない
3) 要求分析のために用意された時間が短く，セキュリティ要求分析を行う時間が確保出来ない

1)は，‘‘開発に関係するステークホルダ（利害関係者）のセキュリティに対する意識や知識不足’’に起因するとしているが，不正アクセスが常態化している近年の状況では少数派になって来ていると想定される．2)3)は，‘‘開発体制の中でセキュリティの開発に必要な知識を持つ人材が不足していることが原因’’としているが，セキュリティ対策技術が通常の開発作業とは別の特別な技術として受け取られていることも，知識が浸透していかない原因だと考えられる．

要件定義プロセスを対象としたセキュリティ対策に関連する研究を調査した結果[5][6]を見ても，セキュリティ対策のために共通化されていない特別なアプローチの提案ばかりとなっており，実際の開発現場で利用可能な内容となっていないのが現状である．

大久保らによる研究では，セキュリティパターンを用いることで要求されるセキュリティ知識を最小化する手法が提案されているが，システム機能要件を定義する期間とは独立して非機能要件であるセキュリティ要件を導き出す期間が必要になり，最小化したとしてもセキュリティ知識を持つ人材不足への解とはなっていないと想定される．

また，セキュリティパターンを利用する手法については，吉岡らによって示されている研究動向[7]の中で以下の傾向が読み取れると述べている．

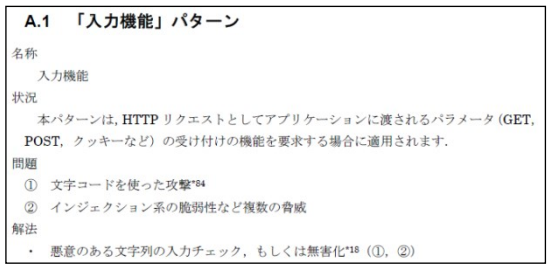
- 要求・分析工程では，攻撃に関するパターンが多く，対策に関するパターンが少ない
- アーキテクチャ設計や詳細設計工程では，攻撃に関するパターンと次にセキュリティ仕様に関するパターンが少ない
- 実装工程では，攻撃や対策に関するパターンが多いが，セキュリティ仕様に関するパターンが少ない

不足しているパターンを開発プロセスの繋ぎ部分に注目して，今後充実すべきとしており，発注者側よりも受注者側である下流工程の開発者のために，設計工程の攻撃に関するパターンが必要であるとしている．しかし，発注者側が責任を持つ要件定義プロセスにおいては，言及されていない．他にもセキュリティパターンに関する提案はあるが，設計プロセスに着目したものが[8]をはじめとして，多く見られた．

吉岡らのセキュリティパターンを取り巻く研究状況や大久保らのセキュリティパターンを利用することで，必要となるセキュリティ知識を省力化できることに着目し，発注者側や受注者側に共通した知識であるシステム機能をベースにしたセキュリティパターンを宇野が提案している．[9]

提案された手法では，Figure 3 に示すように，Web アプリケーションに求められる機能（例示では，「入力機能」）に着目し，その機能を利用する上で，どのようなセキュリティ上の問題が存在するか，その問題を解決するためにどのような解法が存在するかを事前にパターンとして準備して示すことで，セキュリティ知識が乏しい技術者であって

も，セキュリティ要件を導き出すことが可能になることを目的としている．


A.1 「入力機能」パターン

名称
入力機能
状況
本パターンは，HTTP リクエストとしてアプリケーションに渡されるパラメータ（GET，POST，クッキーなど）の受け付けの機能を要求する場合に適用されます．
問題
① 文字コードを使った攻撃*84
② インジェクション系の脆弱性など複数の脅威
解法
・ 悪意のある文字列の入力チェック，もしくは無害化*18（①，②）

Figure 3 「入力機能」パターン

3. 検討手法について

既存研究では，新規にシステムを開発することを想定しており，ソーシャルメディアサービスをはじめとしたサービスを提供しながら，新たな要件を獲得し，Web アプリケーションの更改を繰り返すことが想定された研究はあまりない．

そのため，短期にサービスを開始し，更改を繰り返す開発スタイルを意識したセキュリティ対策が漏れにくい手法が必要である．

また，公開後に脆弱性が見つかり，炎上による風評被害など組織運営にまで影響を及ぼさないためにも，設計前に定義したセキュリティ対策が確実に実施されていることを確認するための手法も必要であると考える．

本研究では，宇野が提案しているシステム機能ベースセキュリティ要求分析を拡張することで，要件定義プロセスにおいて，受入試験プロセスで必要となるセキュリティ対策が実施されていることを確認する方法を導き出すと同時に，Web アプリケーション更改時のセキュリティ要求/要件を導き出せる手法の検討を行う．

3.1 システム機能ベースセキュリティパターンの拡張

宇野の提案するセキュリティパターンの内，A.22「動的な表示機能」パターンを例に現在検討中の拡張方法について示す．

下記が宇野の提案するセキュリティパターンである．

‘‘A.22「動的な表示機能」パターン

■名称

動的な表示機能

■状況

本パターンは，外部からの入力に応じて，Web アプリケーション上で HTML や JavaScript を動的に生成する機能が要求され場合に適用される．

■問題

① クロスサイト・リプティング（XSS）

② エラーメッセージからの情報漏えい

■解法

・ XSS 対策（①）

・ 詳細なエラーメッセージの抑止（②）’’

このセキュリティパターンは「名称」「状況」「問題」「解法」の 4 つの部品から構成されており，ここに「試験方針」を追加した場合，下記のように拡張可能である．

■試験方針

・ XSS 文字列に対する無害化処理の確認（①）

・ エラーが発生する文字列を入力した際に，エラーメッセージが出力されないことの確認（②）

なお，この「試験方針」に出てくる『XSS 文字列』や『エラーが発生する文字列』が実際に受入試験を実施する際に必要となってくるが，発注者側としては結果が確認出来れば良いことや，Web アプリケーションの環境に依存するためにパターン化が困難なため，本研究の対象として扱わない．

システム機能ベースセキュリティパターンは，例示したように「問題」あるいは「解法」に対応する形で定義することで拡張が可能であり，個別の Web アプリケーションに特化しないように汎化することでパターンとして示すことが可能であると考える．

しかし，既存のセキュリティパターンに「試験方針」を拡張するだけでは，更改にともなう機能差分の影響範囲を把握することが出来ない．そのため，「問題」に対して重要度の設定を行うことで，既存のシステム機能に対するセキュリティ要件を導き出した場合と更改後のシステム機能に対するセキュリティ要件を導き出した場合とで，重要度による試験方針の見直しが可能になり，更改にともなう影響度や影響範囲の把握が可能にならないか検討を進めている．

現在検討中の「問題」に適用する重要度は大中小で表現し，以下の内容で影響度や影響範囲の把握が可能か確認中である．

・ 大：試験方針の見直しが必要

・ 中：既存試験方針を踏襲可能

・ 小：更改による影響なし

3.2 ケーススタディの検討

本研究手法の検証を行うために現在ケーススタディを作成中である．

ケーススタディで用いるシステムについては，システム機能要件が公開されている事例の多い図書館システムを考えている．図書館システムは，図書館内に閉じたシステムではなく，インターネット上に公開された Web アプリケーションである事例が増えており，他の図書館と連携することで，予約システムの更改や検索可能な図書館数の拡大に伴う更改など，Web アプリケーション更改時を想定する上で公開情報をもとに設計出来るため，ケーススタディで用いるには最適だと考える．

現在，具体的かつ現実的なシステム構成と更改システム機能要件の検討を進めている段階であるため，詳細については記載出来ないが，現段階でケーススタディを行う上で確認すべき課題として，インターネットバンキングやショッピングサイト，ソーシャルメディアサービスなどの図書館以外のシステムにおいてもセキュリティパターンとして有効であるか検証が必要であると考える．

また，新規に Web アプリケーションを開発するよりも，要件獲得までのアプローチが複雑になることが想定されるため，パターン化に適さない事例が出てくる可能性があるため，その場合にどのようにパターンを活用可能かも検討が必要になるのではないかと考える．

4. おわりに

本稿では，Web アプリケーションの開発プロセスにおける発注者と受注者の責任分担や関係を示した上で，発注者側が開発プロセスにおいてセキュリティ対策に関わる重要性を説明し，セキュリティ知識に乏しい発注者側の技術者でも利用可能なシステム機能ベースのセキュリティパターン拡張の提案を行った．

その上で，近年のインターネットへ公開後にシステムの更改を繰り返す Web アプリケーションを対象としたアプローチについて検討状況を示した．

今後は，セキュリティパターンの拡張を行いながら，ケーススタディで用いるシステム構成を完成させ，更改システム要件のさらなる検討・精査を行う．また，ケーススタディを行い，既存研究との有効性について検証を行う．

参考文献

1) JPCERT/CC インシデント報告対応レポート [2013 年 10 月 1 日～2013 年 12 月 31 日]
https://www.jpcert.or.jp/pr/2014/IR_Report20140116.pdf
2) McGraw, Gary. "Software security." Security & Privacy, IEEE 2.2 (2004): 80-83.
3) J.Stecklein, Error cost escalation through the project life cycle, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100036670_2010039922.pdf, NASA, Tech. Rep., 2004.
4) 大久保隆夫，田中英彦：セキュアなアプリケーション開発のための要求・デザインパターンの提案，情報処理学会研究報告. CSEC, [コンピュータセキュリティ] 2009(20), 241-246, 2009-02-26
5) Tondel, Inger Anne, Martin Gilje Jaatun, and Per Håkon Meland. "Security requirements for the rest of us: A survey." Software, IEEE 25.1 (2008): 20-27.
6) Elahi, Golnaz, et al. "Security requirements engineering in the wild: A survey of common practices." Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual. IEEE, 2011.
7) 吉岡信和, 鷲崎弘宜, and 丸山勝久. "セキュリティパターン技術に関する研究動向 (検証/セキュリティ)." 情報処理学会研究報告. ソフトウェア工学研究会報告 2007.107 (2007): 39-46.
8) Ferraz, Felipe Silva, Rodrigo Elia Assad, and S. R. Lemos Meira. "Relating security requirements and design patterns: Reducing security requirements implementation impacts with design patterns." Software Engineering Advances, 2009. ICSEA'09. Fourth International Conference on. IEEE, 2009.
9) 宇野健二 : Web アプリケーション開発におけるシステム機能ベースセキュリティ要求分析，情報セキュリティ大学院大学 2011 年度修士論文