2015 年度 SSR フォーラム

クラウドサービスの開発運用におけるセキュリティとプライバシの確保のためのメタモデルに基づく知識ベースと参照アーキテクチャの調査研究

―知識ベース 初期モデル―

2016 年 2 月　1 日

早稲田大学 基幹理工学部 情報理工学科

福本創太

鷲崎弘宜

知識ベース（メタモデルの活用方法）

ここでは前節で示したメタモデルの実際の活用方法について述べる。
本メタモデルの活用方法の一つとしてメタモデルをもとにパターンやプラクティスなどの知識群を適切な関係や軸を設定し体系化することにより知識ベースを作成するといったことが挙げられる。現在のクラウドサービスはセキュリティやプライバシーの対策が不十分なことが多くその理由は解決策となるパターンやプラクティスといった知識群自身の理解不足、あるいはパターン間同士の関係性への認識が足りないといったことが挙げられる。有用な解決策は個々に提唱され、独立しあっているため、検索するときにも手間がかかり、また個別に定義されたパターン同士の関連性はどこにも提唱されていないためパターンを組み合わせるといったことへの敷居は高い。そこで本メタモデルを用いた知識ベースを作成することでパターンやプラクティス等の個別に提唱された知識群をメタモデルに基づいたクラウドシステムの開発・運用においてのセキュリティとプライバシーを確保した軸を選定し、適切な分類を行うことができる。そうすることで従来別々に定義されていたパターンやプラクティス等の知識群を一括にまとめることができ、なおかつそれらパターン同士の関係性等を定義することができる。本知識ベースはメタモデルを基に Wiki をつかって作成し、一つのパターン毎に一つのページを割り振り、そのページにカテゴリーとしてメタモデルを用いた軸で分類を行った。これらの軸はすべて本メタモデルに記載されている要素を用いたもので、クラウドサービスの開発・運用におけるセキュリティとプライバシーにおいて適切なものになっていると考えられる。図 1 に知識ベースの例として SQL Injection パターンのページを示す。

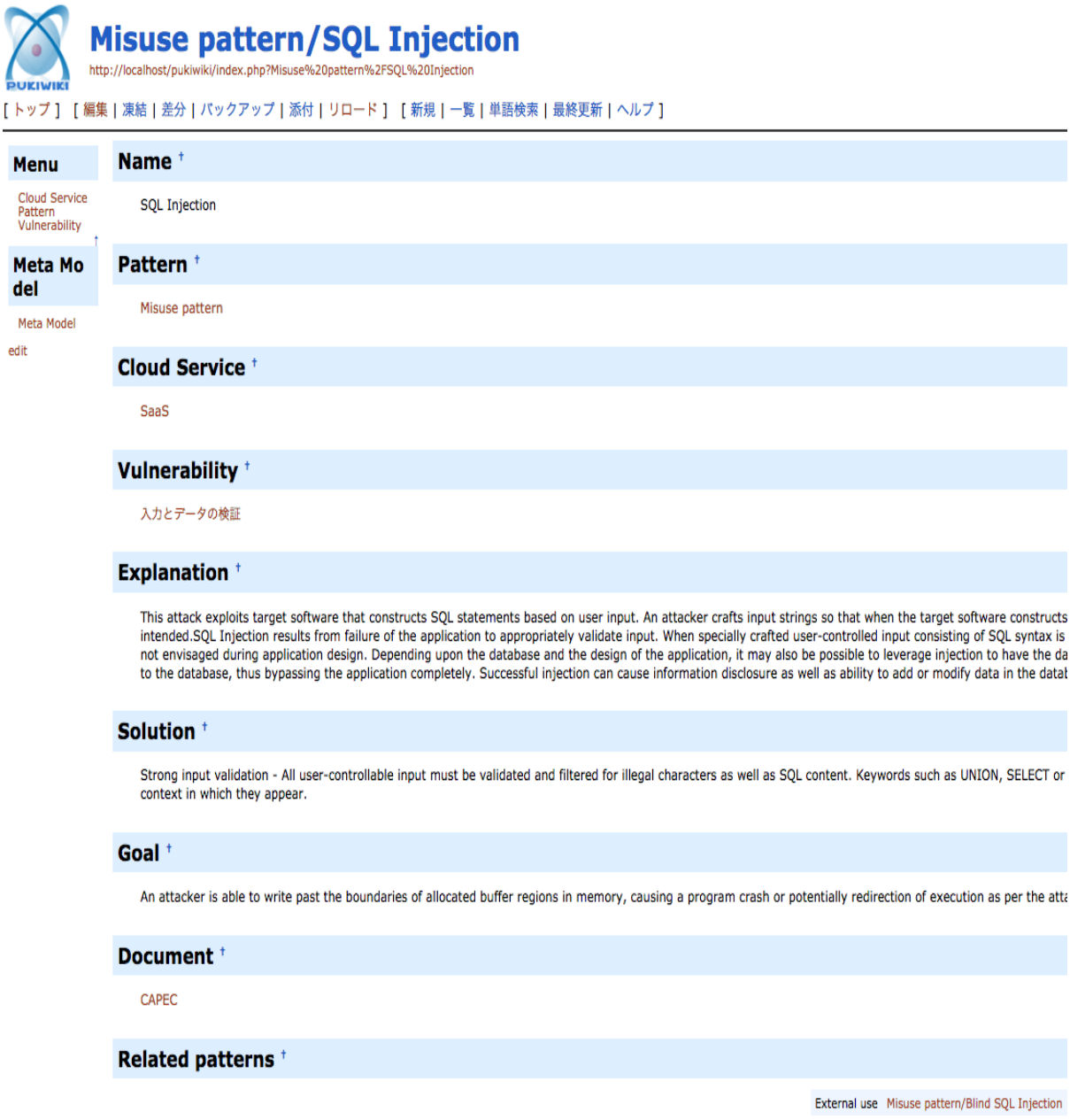

図 1：SQL Injection パターンのページ

図 1 のように、パターンやプラクティスなどの知識群を一ページに記載し、メタモデルに基づいて以下の 9 つの軸により属性をつけ分類している。

・ Name

パターンやプラクティス等の知識の名称を記載する。

・ Pattern

このパターンが Security、Privacy、Misuse のどのパターンに分類されるかを示す。まだパターン化される前のプラクティス等の知識はその旨を記載する。

・ Cloud Service

このパターンが Cloud Service の SaaS、PaaS、IaaS のどのレイヤーに主に関係するのかを記載する。これにより階層別に対策を行いたいときに簡単に検索することができ、適切な対策が行えるようになる。

・ Vulnerability

ここでの脆弱性(Vulnerability)とはパターンを脆弱性によって分類する目的で利用するため Microsoft のセキュリティフレームカテゴリによるどの脆弱性に分類するかを示している。Microsoft のフレームカテゴリとは入力とデータの検証、認証、認定、構成管理、機密データ、セッション管理、暗号化、例外管理、監査とログ記録の 9 つで既存の脆弱性はすべてこの 9 つに分類することができると考えられている。この分類により自身のシステムがもつ脆弱性等対応するべき脆弱性がはじめから分かっている開発・運用者はそのカテゴリーを見ればよいため効率がよく、自身のシステムの脆弱性を知らない開発・運用者でも別のルートからそのパターンにたどり着いたときに自分が対応する脆弱性がどの分類なのかが分かり、また自身のシステムにはまだその脆弱性についての対応が必要なのではないかとセキュリティ対策をより深く進めることができる。

・ Explanation

このパターンの概略を示す場所であり、これによりこのパターンがなんなのか、自分の探しているパターンと一致しているのか等を確認することができる。

・ Solution

そのパターンで問題にしている解決策を示す。Security パターンや Privacy パターンの場合具体的なパターンの適用方法やこのパターンを適応することにより、どのような問題を解決できるのかを示し、Misuse パターンでは Explanation で説明している攻撃手法に対するセキュリティを守る側の視点での具体的な対処方法を記入している。

・ Goal

そのパターンで達成するべき目的を示す。Security パターンや Privacy パターンの場合はそのパターンを適用してなにが守られたのか、あるいはどのような脅威を防ぐことができたのかを記述する。Misuse パターンの場合にはそのパターンを用いてシステム攻撃者目線でどのような成果が得られるのか、どこまでシステムに影響を及ぼすのか等を記述する。

・ Document

そのパターンの引用先を示す。このパターンの Explanation や Solution、Document はどこから引用したものなのか論文名や Web サイトのリンクを貼り、すぐに引用先にアクセスすることができるようにする。そうすることでパターンのさらなる詳細が知りたいときにすぐに確認することができるとともに、そのパターンの信憑性を示す基準ともなる。

・ Related Pattern

そのパターンが関連するパターンやプラクティスを示す。パターンの関連付けの方法として、同じパターンの種類同士の関係性を External use、Internal use、Similarity の 3 つで分類し、そのパターンが外部で使われているのか、内部で使われているのかそれとも類似しているのかを表し、関連づけている。異なるパターン同士つまり Security パターンと Privacy パターンに対しての Misuse パターンの関係は解決策と課題という構成になっているため、それぞれ Problem of と Solution of といった関連付けを行い異なるパターン同士を結んでいる。この Related Pattern を用いることで例えば自分がいまある Security パターンを参照しているとしてそのパターンと似ているもの、そのパターンを利用している他のパターン、そしてそのパターンによって解決できる Misuse パターンをすぐに参照することができるようになり、いままで散在していた個々のパターン同士を体系的に結びつけることができるようになるのである。このようにメタモデルにはクラウドシステムのセキュリティやプライバシーに関するパターンやプラクティスを適切に分類した知識ベースを作成することができるといった活用方法がある。ほかにもクラウドサービスの開発・運用におけるセキュリティやプライバシーに関することならばこのメタモデルを参照して作成することで効率を上げることが可能となる。

知識ベースの評価

ここでは前節で紹介した知識ベースについての評価・考察を行う。知識ベースの評価として、知識ベースの解決策を発見する効率と、その解決策への理解度の向上を測るために事前知識(セキュリティ関連の解決策の知識)がある人とない人それぞれ 2 名、計 4 名に次のテストを行った。テスト内容はクラウドサービスの開発・運用者がセキュリティとプライバシーの対策をたてるといった立場のもとから機密情報への適切なアクセス権限の管理ができておらず、外部からの機密情報へのアクセスといった脅威を対策するといったもので、課題を知識ベース未使用と知識ベースを使用した場合の 2 パターンでそれぞれ発見時間、理解度、達成度等を調査した。以下の表 1、2 にその結果を示す。

事前知識	発見時間	理解度	達成度
あり	0:03:25	3	5
あり	0:02:07	3	4
なし	0:04:40	2	4
なし	0:04:11	2	5

表 1：知識ベース未使用時の理解度と達成度

事前知識	発見時間	理解度	達成度
あり	0:00:55	4	5
あり	0:01:45	4	4
なし	0:00:52	5	5
なし	0:00:38	5	5

表 2：知識ベース使用時の理解度と達成度

このテストにより、知識ベースを利用することで解決策の発見時間の短縮と理解度、達成度の向上を確認することができた。なお理解度、達成度はともに 5 段階評価を用いていて理解度については被験者の自己判断、達成度は課題に対しての成績を示している。この結果によりメタモデルの三つ目の要求であったパターン・プラクティスへの容易なアクセスを行えることというのは満たされていると考えることができる。また以上の結果をふまえ、この知識ベースを作成するメリットとして 3 つ挙げることができる。一つは多くの文献を参照することなく適切な解決策としてのパターンを見つけることが容易となることであ

る。従来パターンとは様々な論文やWebサイトで公開されてきたが、これでは、論文の執筆者やそのWebサイト運営者の知識の範囲のものでしかパターンとして公開されないため他の論文やWebサイトで公開されたパターンとの関連性は示されておらず、存在するすべてのパターンから最適な解決策を選ぼうとすると様々な論文やWebサイトを確認していかなければならなかった。しかしこの知識ベースでは様々な論文やWebサイトから引用してきたパターンを一カ所にまとめているため、個々の知識の範囲に縛られず、絶えず存在するパターンを集めることができる。したがってこの知識ベースにアクセスし検索するだけで適切なパターンを見つけるための様々な論文やWebサイトを見て探し回るといった無駄を省くことができるのである。二つ目はパターン同士の関連性を明らかにし、より適切な対応ができるようになるということである。前述の通りパターンは個別に定義、提唱されているため、パターン同士の個々の関連性というものは存在しなかった。しかしこの知識ベースを使えばパターン毎にメタモデルに基づいた軸によりパターンを体系化することができ、様々な要求から適切なパターンを導きだすことができるのはもちろん、見つけたパターンの関連パターンを参照することでより深くそのパターンを理解できることにもつながり、さらには自分が気づいていなかった潜在的な問題も発見できる可能性が広がる。したがってより緻密にクラウドシステムのセキュリティ、プライバシー対策を行うことができるのである。最後の三つ目はクラウドサービスのセキュリティ、プライバシー対策を管理することが容易になることである。従来ではクラウドシステムに問題が生じたときいくつかの文献を参考にその中で一番有用性のあるパターンを適用して対応していたが、それでは適応してから数年が経った後にそのパターンに問題が見つかった場合などはどこの文献を参考にしたのか等が不鮮明となることがあり適応パターンを見直すといったことが難しい。しかしこの知識ベースにはログが残っており、自分の参照したパターンが分かるだけでなく、このパターンの概要、目的、解決策等がどのパターンも同じ形式でまとめられているため、数年経った後でも利用したパターンの内容を参照、理解しやすく、使用したパターンに問題が生じたのであれば関連パターンに表示される類似パターンなどを試してみるといった対応策がスムーズに適用できる。したがってクラウドサービスの管理や保守の面でもこの知識ベースは有用であるといえる。以上の三点からこのクラウドサービスの開発・運用者のセキュリティやプライバシーを守るためのメタモデルを用いた知識ベースは、

クラウドサービスのセキュリティやプライバシーの問題を解決する際、最適解のパターンを見つける手助けをし、また関連パターンから潜在的な問題も発見することもでき、管理や保守にも役に立つものとなっている。また知識ベース本来のメリットではないが、この知識ベースは Wiki をベースにシステムを構築しているため、第三者がパターンの拡充、または更新ができるので鮮度の高い知識を扱うことができる。例えばあまり使われていないパターンは一度掲載されたきりだが、流行のパターンなどについては何度も更新され洗練されていくのでよりクラウドサービス開発者のニーズにあった知識ベースとなり得る。さらに問題が発生したパターン等も対策が組まれれば早急にパターンが更新されるのでクラウドサービス開発・運用者もいち早く問題の検知と対応が行える。そしてもちろん知識ベースに表示されたパターンの詳細を知りたいときは Document から引用元にアクセスできるため信憑性も保証されている。