Vol.2018-SE-198 No.25
2018/3/10

セキュリティパターン研究の分類体系と文献調査

鷲崎弘宜 夏天 鎌田夏実[†1] 大久保隆夫[†2] 小形真平[†3] 海谷治彦[†4] 加藤岳久[†5]
鹿糠秀行[†6] 田中昂文[†7] 櫨山淳雄[†8] 山本暖[†6] 吉岡信和[†9] 吉野雅之[†6]

概要：セキュリティパターンとは、セキュアなソフトウェアシステムの開発運用における特定の文脈上で繰り返されるセキュリティに関する問題と解決を一定の抽象度でまとめたものである。1990 年代後半からこれまでに 500 近くのセキュリティパターンの特定と蓄積、共有がなされている。それに伴い、それらの適用や抽出といった技術研究も進められているが、その傾向や全体像、技術的課題および展望は明らかではない。そこで我々は最初に、セキュリティパターン研究を分類整理する際の基本的な用語間の関係を整理した概念モデルを提案する。さらに我々は同モデルに基づいた研究の分類体系（タクソノミ）を提案し、同分類体系に基づき 200 を超える文献の内容を分類した結果を報告する。

キーワード：セキュリティパターン、ソフトウェアパターン、タクソノミ、体系的文献調査

Taxonomy and Literature Survey for Security Pattern Researches

Hironori Washizaki, Tian Xia, Natsumi Kamata[†1] Takao Okubo[†2] Shinpei Ogata[†3]
Haruhiko Kaiya[†4] Takehisa Kato[†5] Hideyuki Kanuka[†6] Takafumi Tanaka[†7]
Atsuo Hazeyama[†8] Dan Yamaoto[†6] Nobukazu Yoshioka[†9] Masayuki Yoshino[†6]

1. はじめに

セキュリティパターンとは、セキュアなソフトウェアシステムの開発運用における特定の文脈上で繰り返されるセキュリティに関する問題と解決を一定の抽象度でまとめたものである [1][2][3]。1990 年代後半からこれまでに 500 近くのセキュリティパターンの特定と蓄積、共有がなされている。

ソフトウェア開発におけるセキュリティパターンの適切な利用は容易なことではない [2]。それらの適用や抽出といった技術研究も進められているが、その傾向や全体像、技術的課題および展望は明らかではない。そこで本稿では最初に、セキュリティパターン研究を分類整理する際の基本的な用語間の関係を整理した概念モデルを提案する。さらに我々は同モデルに基づいた研究の分類体系（タクソノミ）を提案し、同分類体系に基づき、Systematic Literature Review (SLR) [4]を用いて 200 を超える文献の内容を分類した結果を報告する。

2. 分類のための概念モデルと体系

2.1 概念モデル

セキュリティパターン研究の分類の基盤として、セキュリティやセキュリティパターンおよびその活用に特有の概念を整理する必要がある。そこで我々は、クラウドサービス開発運用におけるセキュリティおよびプライバシ知識を整理した Cloud Security and Privacy Metamodel (CSPM) [5]においてクラウドに依存せず、セキュリティパターン研究に関連する概念を図 1 に整理した。

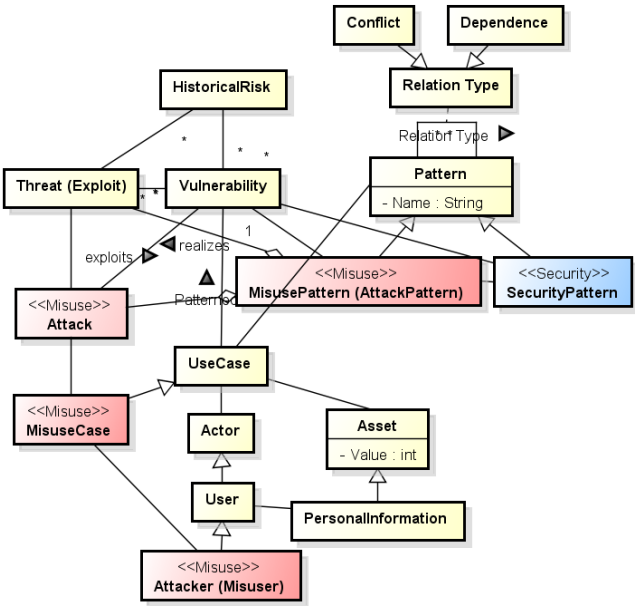

図 1: 概念モデル（CSPM [5]からの抜粋）

2.2 分類体系

前述の概念モデル中の主要な概念に基づき、セキュリティパターン研究の分類上のファセットとして以下を識別した。

†1 早稲田大学
†2 情報セキュリティ大学院大学
†3 信州大学
†4 神奈川大学
†5 東芝インダストリアル ICT ソリューション社
†6 日立製作所
†7 東京農工大学
†8 東京学芸大学
†9 国立情報学研究所

(1)研究の目的: 当該セキュリティパターン研究が扱う話題（トピック）、対象とするシステム・ソフトウェアライフサイクル上の段階（フェーズ）、および、研究成果の利用者（ユーザ）が挙げられる。
(2)研究成果の実現方法: セキュリティパターン研究成果を実現する形についてプラットフォーム、ツール・自動化、セキュリティ測定、研究評価が挙げられる。
(3)セキュリティ特性: セキュリティパターン研究が扱う品質特性として情報の機密性、完全性、可用性に代表されるセキュリティ特性が挙げられる。
(4)セキュリティ関連パターン: セキュリティパターン研究が扱うセキュリティパターン、アタックパターン、ミスユースパターンの種別が挙げられる。
(5)セキュリティ手法: セキュリティパターン研究の手法上の特徴として、方法論やモデリング手法、さらにはパターン間関連の扱いの有無が挙げられる。

3. 体系的文献調査プロセス

大規模な文献データベース Scopus 上で、"Security Pattern" を検索キーワードとして 2014 年に文献を検索し、500 以上の初期候補を得た。それらに対して著者複数名が各文献をチェックし、パターンそのものを提案している文献や、セキュリティパターン研究と無関係のものを除外し、最終的に 212 件の文献を得た。

4. ファセット単独の調査結果

4.1 研究の目的

(1) 話題（トピック）
結果: 話題の内訳を図 2 に示す。開発上のセキュリティパターン適用、および、より抽象的な開発の方法論やプロセスの提案が大多数である。一方、ケーススタディや実証系の研究は限られている。
考察: 適用・方法論系の研究成果に基づいた事例および実証の拡充が望まれる。セキュリティパターンそのものの新たな提案は PLoP を中心に 90 年代後半より活発になされているが、その抽出は人手によるものであり、我々の調査対象となりうるシステマチックな手法としては確立されていないことが見て取れる。また、セキュリティや脆弱性の評価の観点からは、アタックパターンやセキュリティパターンの存在を要求や設計、コード上で自動的に検出できることが望ましい。特に、セキュリティパターンの検出や抽出の取組みは期待にされているにもかかわらず、ほとんどなされていないことは問題である。

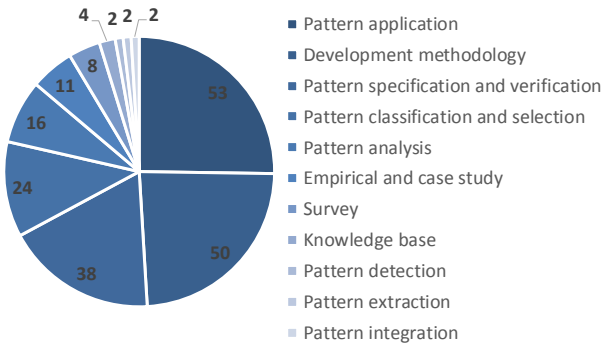

図 2: 話題の内訳

(2)ライフサイクル段階
・段階の明示
結果: 各種論文が扱うパターンを 16 段階に分類した結果、図 3 となった。本分析では、論文 1 本に対して 0 以上の段階を分類した。また、分類には階層性があり、たとえば Any は Design などのより低粒度な段階を含みうる。その結果、分析結果には曖昧さが生じている。
考察: Any であっても Evolution を含むかどうかは個別に異なる。分析から進化まで多様な段階が対象となりうる以上、各論文では可能な限り低粒度で対象段階を明確にすべきであろう。
・段階から見た研究の潮流
結果: また、分類したパターンの対象段階は Design が最も多く、次いで Analysis、Implementation となり、上流工程に寄っていた。一方では、下流、運用保守、進化などの実装後の工程も僅かながら対象となっており、フロンティア分野となっている可能性が窺える。具体的なトピックに関しては、実装後が段階に含まれている論文ではたとえば次のトピックを扱う：パターン分類、ソースコードからのパターン検出、セキュリティパターンによるレガシーシステムの改善、運用時のダイナミクスを扱うセキュリティパターンがある。
考察: システムのライフサイクルにおけるパターン分類、動的振舞いに対応するパターン定義、または定義済みパターンを既存システムへ利活用法などをトピックとする必要があろう。

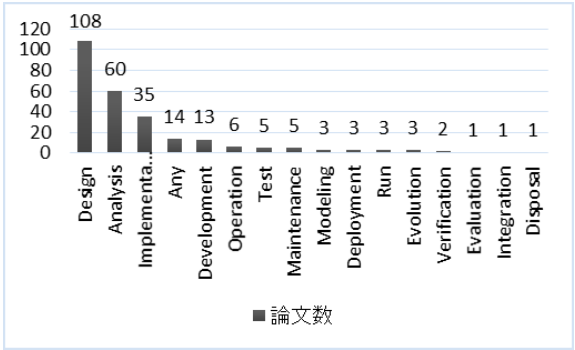

図 3: セキュリティパターンが対象とする段階.

4.2 研究成果の実現方法

(1)プラットフォーム

結果: 211 件中、何らかのプラットフォームを前提とするものは 49 件（約 1/4, 23%）。Web, Cloud, 分散システムが多数。そのほかに BPM や MAS など。そもそも約 3/4 はプラットフォームに言及していない。

考察: IoT システムの進展を鑑みると、クラウドやアプリケーション周辺のみならず、IoT や組込み・制御系のプラットフォーム上の実現の研究成果も求められる。

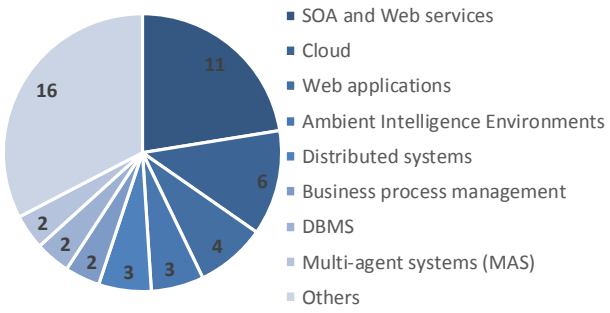

図 4: プラットフォームの内訳

(2)ツール・自動化:

結果: 何らかのツール・自動化への言及は 68 件（約 1/3、32%）。モデリングを伴うツールや取組みが多数。他には形式手法・検証、アスペクト指向、コード生成など。大多数はその他のそれぞれの手法のツール化。モデリング、分析・設計におけるツール化が多い。

考察:セキュリティは本来あらゆる段階で扱われるべきであり、実装やテスト、そして運用段階におけるセキュリティパターンのツール化を通じた直接的な扱いが求まれる。セキュリティライフサイクル全体をカバーすべきである。

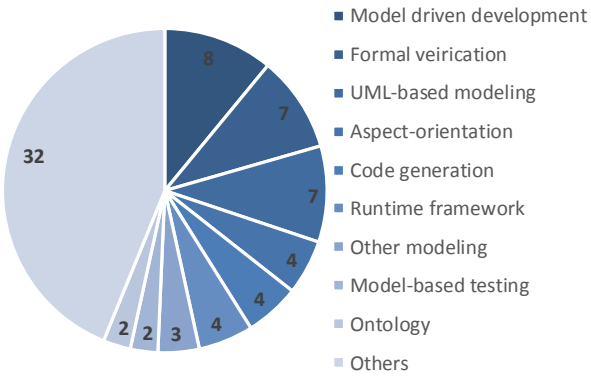

図 5: ツール・自動化の内訳

(3)セキュリティ測定

結果: 17 件の論文が，パターンの評価を行っていた．詳細は表 1 に示す．17 件のうち 2 件が STRIDE[6]を使った評価を行っていた．[FWYV2011]は，グラフを用いて想定される脅威について対策されているかを評価し，Nonsecure system および Secure System に対する Primary attack について，STRIDE における Categories of attacks を示している．[HCS2006]は攻撃に対するシステム評価について，STRIDE を用いて評価している．さらに Fuzzy 理論を使った評価では，主な 5 つのイベントに対し 5 段階，および STRIDE のどれに対応しているかを評価している.段階数や観点の若干の違いはあるが、パターンが扱う脆弱性の発生確率や影響の大きさをセキュリティレベルとして 3〜5 段階程度で離散的に評価するアプローチが多く見られた。

考察: 独自の評価だけでは，その評価が妥当であるのかわかりにくい．品質の評価には，STRIDE の様な統一的な指標があると良い．

表 1. 調査文献におけるセキュリティ測定の概要

文献	セキュリティ測定の概要
13	文献では, 23 文献のセキュリティパターンについて 14 の分類に分け，それらについて 9 つの品質基準分類を用いて評価している．
47	文献では，Attributes，Risk Reduction Frequency, Risk Reduction Consequence, Annual Number Attacks, Cost per Attack, Cost Solution に対し，Forces，Solution で評価を行った．さらに，XSS をケーススタディとして評価した．
52	文献では，9 つの security pattern に対し，security criteria について 7 つのレベルで比較評価を行った．また，Performance の増減の比較評価，および criteria について Implementation Cost と Security degree を 3 段階で評価を行った．

65	220 パターンについて，Publication year (年毎のパターン数)で core pattern と all とを比較している． ・the discription elements (記述要素) として，{problem and forces/structure description/structure image/behavior description/behavior image/consequences/example} について，not provided, minimal, satisfactory のスコアで評価している． ・年毎に function of the quality (品質機能) について，発表されたパターン数のスコアで評価している． ・記述要素として problem={problem description}, Solution={structure description, behavior description, structure image, behavior image}, others={example, consequences} 別の重み (weights assigned to the various elements of description)で評価している． ・quality lebel (品質レベル) として low/midium/high の 3 段階で評価し，そのパターンの割合を core/others に分けて評価している． ・access control や privacy など 15 の security objective (セキュリティ対策/対象？) について，パターン数を core/others に分けて評価している．
67	文献では，グラフを用いて想定される脅威について対策されているかを評価した．
96	9 つの Case について，Resitance of the Security Patterns，Likelihood of an attack など 4 つの項目を STRIDE を用い 4 段階で評価している．また Nonsecure system および Secure System に対する Primary attack について，STRIDE における Categories of attacks を示している．
99	roll に対する resource への権限 C (create)，R (retrieving)，U (updating)，D (deleting) の 4 つのオペレーションについて評価している．
129	アスペクト指向で，Account Lockout with Selective Event Looging (ALSEL) と IMAP システムについて, Object Constraint Language (OCL) を用いた評価を提案している．
213	threats and attacks to be avoided misuse pattens to be applied, threats to be passed, security requirements など 9 つの concern について, quality を 9 つのレベルで評価している．
231	Accountability, Confidetiality, Integrity など 8 項目を Security Pattern について評価している．
270	攻撃に対するシステム評価を, STRIDE を用いて評価している．また Fuzzy 理論を使った評価は, 主な 5 つのイベントに対し 5 段階, および STRIDE のどれに対応しているかを評価している．またシステムに Security pattern が無い場合とある場合について, 5 段階評価を行っている．
290	分散システムの security pattern を分類し, 5 つの Quality Indicator について程度の大小を評価している．
295	6 σ のアプローチを利用し Undesireble Properties を 6 つの項目について, 12 のセキュリティパターンの評価をしている．
375	Patterns に対する Aplicability を独自の評価式を用いて割合で評価している．
378	Security kernel について 3 つの completeness, isolation, verifiability を engineering principle を評価指標として示している．
379	Grid System の security pattern に関するもので, authentication pattern について password と digital signature を Graphic Extension of Backus Normal Form / Buckus-Naur Form で表記している．
380	ATM terminal を例に，セキュリティ目標 (security object) とパターンを 8 つのメトリクスで評価している．
381	pattern を 3 つのレイヤで分類し評価している．

4.3 品質特性

各論文が扱うセキュリティパターン研究の傾向を調べるために、論文で言及されるセキュリティの特性に着目し調査を行った。その結果、何らかのセキュリティ特性について明記している論文が調査対象の 211 件中 121 件あった。

121 件の内 CIA 特性について明記している論文が 112 件あった。CIA 特性とは情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)の頭文字から取った特性であり、ISO/IEC 27002 の中では「情報セキュリティとはそれら CIA を維持すること」であるとして定義されている。CIA 特性を明記した 112 件の内、機密性が 94 件、完全性が 72 件、可用性が 63 件、それぞれ明記されていた。各 CIA 特性の重なりも含めた内訳を図 6 に示す。

また CIA 特性だけではなく、それ以外のセキュリティ特性について明記した論文が 31 件あった。具体的には、アクセス制御(Access Control)、責任追跡性(Accountability)、真正性(Authenticity)、認証(Authentication)、認可(Authorization)、否認防止(Non-repudation)などが特性として明記されていた。31 件の内、それらの特性のみを明記している論文は 9 件、CIA 特性に加えて明記している論文が 22 件あった。

以上のことから特性を明記している多くの論文が CIA 特

性に関わるセキュリティパターンの研究であることがわかった。特に、認められた者だけが情報にアクセスできる状態を確保するという機密性は、多くの論文で RBAC に代表される機密性に関わるパターンについて触れられていることからも重要視されていることが伺える。

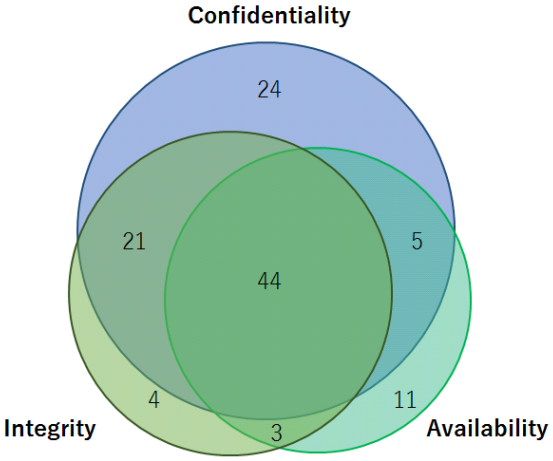

図 6: セキュリティ特性別の内訳

4.4 セキュリティ関連パターン

(1)パターンの種別

結果: 論文中で扱われるパターンは大別して、security pattern と、misuse pattern または attack pattern の 2 種類ある。単に’security pattern’を扱っている論文が 179 に対し、misuse, attack pattern を扱うものは 11 と相対的に少ない。Attack pattern を扱うものには、具体的問題の解決にフォーカスしたものが多い。今回、security pattern を対象に論文を集めたが、dependability や usability など、他の非機能要件に関するパターンもいくつかみられた。開発フェースを明記したパターンは、requirement が 3 に対し、design が 13 と多い。

考察: security pattern に対し，attack 系のパターンが多い理由は，本サーベイの検索方法に起因する可能性もあるが，相対的に attack や misuse 系の研究は少なく，より活発な研究が望まれる分野と推察される．同様に，開発フェーズの中で，design 以外のフェーズに対応した研究は少なく，要求分析やテストに関するパターンの研究の活発化が望まれる．

表 2: セキュリティパターン種別の内訳

セキュリティパターン種別	論文数
security pattern	179
misuse pattern	6
attack pattern	6
privacy	1
dependability	9
usability	1
requirement	3
design	13
architecture	6

(2)アタックパターン

何らかのアタックが記述されていた論文は 33 編であった。重複を排除して以下のパターンを抽出した。misuse patten, threat pattern, attack pattern (STRIDE), problem pattern, abuse, leaks, Identity spoofing, Session state poisoning, Message secrecy violation, phishing, Resource Usage Monitoring Inference, Malicious Virtual Machine Creation, Malicious Virtual Machine Migration, Message secrecy violation, Data inference, Unauthorized access, Message integrity violation, Session hijacking, Route poisoning, Scanning, Injection, Message authenticity violation, Invoking unauthorized operations, Output information disclosure, Message flooding, Resource exhaustion, Targeted process crashing, Guess ID and Password, Dictionary Attack, Brute Force Attack, Social Engineering, Eavesdropping, parameter modification, bulletin modification, illegal execution, inconsistency, physical, wrong command, malicious alteration of runtime parameters, malicious alarm, sniffing, tampering with log files, access to sensitive data by unauthorized parties, malicious data input, improperly configured redirector, illegal money transferring, test footprinting, application integrity, data confidentiality, Theft of Service, four attacks (detect, stop or mitigate, react, recover), input validation-related attacks (ex. SQL injection and cross-site scripting (XSS) attacks), Deals with hostility of the environment, Threat Assessment, Vulnerability Assessment

複数の文献で出現したパターンとその出現回数を以下に示す。

表 3: 複数の論文で出現したアタックパターンとその出現回数

パターン名	出現回数
spoofing	6
DoS	5
information disclosure	4
tampering	4
misuse	3
injection	3
attack	2
session state poisoning	2
message secrecy violation	2
malicious Virtual Machine Migration	2
threat	2
repudiation	2
integrity	2
elevation of privilege	2

アタックパターンが記述されていたのは 33 編の論文で記述されていた割合は 15.6%であった。これは後述のセキュリティパターンの言及の割合に比べて極めて低い。また、記述されていたパターンの抽象度は異なっていた。アタックパターンの分類である STRIDE やセキュリティ特性である CIA などの抽象的なものから、“illegal money transferring”のような特定のアプリケーションにおけるアタックパターンまで多岐にわたっている。ただし、特定の

アプリケーションにおけるパターンはこの 1 事例であった。また出現頻度としては、多くのアタックの出現頻度は 1 度であった。複数の論文で出現しているアタックとしては Spoofing が最多の 6 回、次いで DoS が 5 回、tampering と information disclosure が 4 回、injection と misuse が 3 回、repudiation、integrity, message secrecy violation, Session state poisoning, attack, Malicious Virtual Machine Migration, threat が 2 回であった。アタックパターンやセキュリティ特性の分類を示すものが多く出現していることが明らかになった。具体的な事例に関する報告は少ないのが現状である。

(3)セキュリティパターン
結果: 全 211 対象論文中, 78.6%にあたる 166 篇の論文において，具体的なセキュリティパターン名の言及があった．パターン名の言及の累積数は，1063 回であるため，言及があった 166 論文において，1 篇あたり，6.4 個のパターンが言及されていることになる．論文中に言及があったパターンの種類数は 466 である．このうち，36%にあたる 172 個のパターンは 2 篇以上の論文で言及されていた. 表 X に 10 編以上の論文で言及された 14 個の具体的なパターン名を列挙する．図に示すようにアクセスコントロール，認証，認可に関係するパターンが多い．
考察: 具体的なパターン名の言及が無い論文が 20%を超えることは驚くべきことである．なぜならば，具体的なパターン無しでは，提案するアイディアや手法の説明が難しいからである．ただし，命名が無いのみで，具体的なパターンの記述がある可能性も否定できない．結果から，およそ 1/3 のパターンは，単一著者や研究グループ内での方言的なパターンではなく，広く認知されたパターンであるものと思われる．これらのパターンはクラス図等に代表される有向グラフ構造的な表記で記述しやすい．そのため多くの論文において利用されているものと思われる．一方，可用性等の構造的な記述で表現しにくいパターンについても，今後扱われることを期待したい．

表 5: 10 編以上の論文で言及された具体的なパターン名

参照している論文数	パターン名
45	rbac
31	authorization
23	access control
20	authentication
18	authenticator
18	check point
16	reference monitor
14	secure logger
13	secure pipe
13	single access point
11	authentication enforcer
10	replicated system
10	abac
10	xacml

4.5 セキュリティ手法

(1)パターン間関連
結果：セキュリティのパターンには、セキュリティリスクの軽減方法を記述したセキュリティパターンと、攻撃者の観点でセキュリティリスクを説明した misuse pattern または attack pattern の 2 種類ある。そのため、セキュリティ特有のパターン間の関連としては、セキュリティパターン同士の関連（以下、関連 A）と misuse pattern または attack pattern と、そのリスクを軽減するためのセキュリティパターンの関連（以下、関連 B）２種類考えられる。 セキュリティのパターン間の関連を扱った論文は全体の 40%にあたる 85 件あり、その中で関連 B に言及した論文はそのうちの 14%にあたる 12 件あった。
考察：多くのセキュリティパターンは、組み合わせて適用されるため、パターン間の関連を明記し、それに従わせる方法を考慮することは重要である。論文中では、40%が何らかの関連を考慮しているのはそのためであろう。しかしながら、セキュリティのリスク分析に必要となる misuse pattern または attack pattern とセキュリティ対策のパターンとの関連について言及している論文は、その中の 14%と少なく研究全体から見ると 5.6%にすぎない。今後セキュリティ特有のセキュリティリスクとその軽減といった分析・開発プロセスとセキュリティのパターンとの関係を含め、関連 B を考慮したパターン研究を行うべきであろう。

5. ファセット間の分析

論文内で同時に出現しやすいファセットの特徴を調査するため、相関ルール分析を実施した。ファセットの特徴については、各ファセットの分析結果から、「目的に開発手法の提案が含まれる」、「設計工程を対象としている」、「セキュリティパターン（以降、SP）の表記に UML を用いている」といった項目を抽出し、各論文で各項目が成立するか否かを特徴とした。なお、ひとつのトピッ

ク中の複数の特徴を同時にもつ論文も存在する。

分析にあたっては、R[]の Apriori アルゴリズム[]を用いた。相関ルールの抽出条件は、支持度 0.05 以上、信頼度 0.40 以上、リフト値 1.00 以上と設定した。

分析結果の一部を表 6 に示す。

表 6: 相関ルール分析の結果

			1	2	3	5	7	8	9	10	12
トピック	1	Development methodology		N	N	0.60	0.58	0.40	N	N	0.40
	2	Pattern application	N		0.49	0.53	0.53	N	N	N	0.49
ユーザ	3	Developer	N	N		0.44	0.66	N	N	N	0.45
	4	Designer	N	N	N	0.54	0.74	N	N	N	0.40
パターン表記	5	UML	N	N	0.41		0.66	N	N	0.44	0.57
対象工程	6	Analysis and requirement	N	N	0.44	0.48	0.66	N	N	0.45	0.47
	7	Design	N	N	0.50	0.53		N	N	0.41	0.42
	8	Implementation	0.43	N	0.61	0.50	0.65		N	N	0.50
ツール化	9	Tooling	N	N	0.43	0.46	0.59	N		N	N
パターン間の関連の言及	10	Relationships among patterns	N	N	N	0.47	0.53	N	N		N
開発手法	11	Model Driven	0.41	0.41	0.53	0.59	N	0.44	0.41	N	0.47
参照パターンの被参照数	12	20以上	N	N	0.48	0.65	0.59	N	N	N	

表 6 中の#1 から#12 は、それぞれ次の特徴を表す。

特徴1. 開発方法論の提案を目的とする

特徴2. パターンの適用を目的とする

特徴3. 研究成果のユーザが開発者である

特徴4. 研究成果のユーザが設計者である

特徴5. パターンの表記に UML を用いている

特徴6. 対象工程が分析・要求工程である

特徴7. 対象工程が設計である

特徴8. 対象工程が実装である

特徴9. ツール化に関する言及がある

特徴10. パターン間の関連について言及がある

特徴11. モデル駆動開発を対象とする

特徴12. 論文で参照しているパターンに、他の調査対象論文 20 件以上が参照しているパターンが含まれる

表 6 中の数値は、各行の特徴を条件部、他の特徴を結論部としたときの信頼度を表す（N は、相関ルールなし）。また、条件部が特徴 1 から特徴 12 で、結論部が特徴 4, 6, 11 となるルールは抽出されなかった。

開発方法論を提案した論文では、設計および実装について言及する傾向がある。また、パターンの適用に関する論文は、設計段階を対象とする傾向がある。しかしながら、分析・要求工程など他工程に言及した論文が少ないことが課題であると言える。

分析・要求工程または設計工程を対象とする論文では、パターン間の関連について言及する傾向がある。一方で、実装工程を対象とし、かつパターン間の関連に言及する例は少ない傾向がある。

実装工程について言及した論文は、開発方法論の提案を目的としている傾向がある。また、上述のように、開発方法論の提案を条件部とした場合にも、実装工程との相関ルールが抽出されている。このことから、開発方法論の提案は実装工程を含めて行われ、実装工程に関する言及は開発方法論の提案を背景に行われる傾向があると言える。

ツール化に関する言及がある論文は設計工程を対象としている傾向があり、分析・要求工程や実装工程については、相関ルールが抽出されなかった。今後は、これらの工程を含むライフサイクル全体におけるパターンの適用等を支援するツールの整備が望まれる。また、ツール化に関する言及がある論文では、被参照 20 件以上のパターンの参照との間に相関ルールが抽出されなかった。今後は、広く認知されたパターンに言及したツールの評価や実践等が活発に行われることが期待される。

開発手法については、モデル駆動開発のみ相関ルールが抽出された。モデル駆動開発を対象にしている論文のおよそ 4 割でツール化に関する言及があることは注目すべき点である。また、モデル駆動開発を対象とした論文では、パターンの表記に UML がよく用いられる。モデル駆動開発ではパターンを適用しやすく、モデル駆動支援のツールが充実していることから、このような傾向が生まれていると考えられる。

6. おわりに

我々はに、セキュリティパターン研究を分類整理する際の基本的な用語間の関係を整理した概念モデルを提案した。さらに我々は同モデルに基づいた研究の分類体系（タクソノミ）を提案したうえで、同分類体系に基づき 200 を超える文献の内容を分類した結果を報告した。

今後は、各ファセットの詳細およびファセット間の関係を精査し、今後のセキュリティパターン研究の展望を明らかとする予定である。

参考文献

[1] Nobukazu Yoshioka, Hironori Washizaki, Katsuhisa Maruyama, “A survey on security patterns,” Progress in Informatics, 5, 2008.

[2] 吉岡信和, 鷲崎弘宜, 丸山勝久, “セキュリティパターン技術に関する研究動向”, 情報処理学会, SE158, 2007.

[3] 吉岡信和, “セキュリティの知識を共有するセキュリティパターン”, 情報処理, 52(9), 2011.

[4] Muhammad Ali Babar and He Zhang, “Systematic literature reviews in software engineering: Preliminary results from interviews with researchers,” ESEM, 2009.

[5] Tian Xia, Hironori Washizaki, Takehisa Kato, Haruhiko Kaiya, Shinpei Ogata, Eduardo B. Fernandez, Hideyuki Kanuka, Masayuki Yoshino, Dan Yamamoto, Takao Okubo, Nobukazu Yoshioka and Atsuo Hazeyama, “Cloud Security and Privacy Metamodel: Metamodel for Security and Privacy Knowledge in Cloud Services,” MODELSWARD, 2018.

[6] Adam Shostack, Threat Modeling: Designing for Security, WIELY, pp.61-86, 2014-2