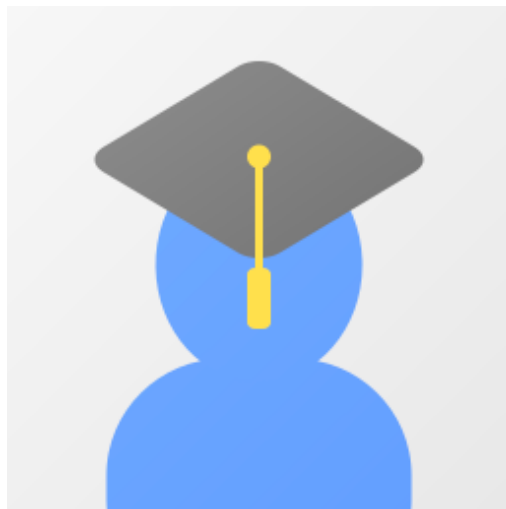
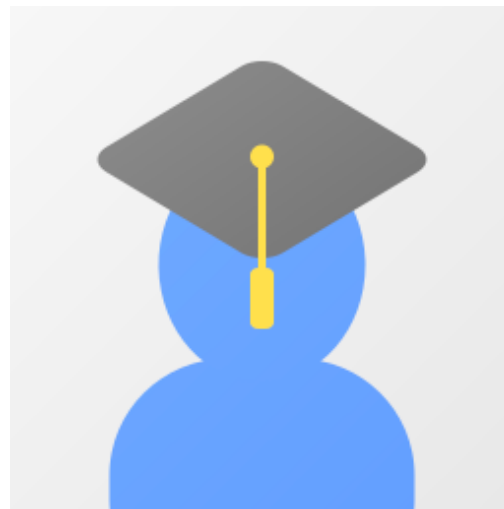


A Legal Cross-References Taxonomy for Identifying Conflicting Software Requirements



Jeremy C. Maxwell



Peter Swire



Annie I. Antón

The 19th International Requirements Engineering Conference
(RE '11), pp.197-206.

背景

- 開発者はソフトウェアが関連法・規則に準拠していることを確証する必要がある
 - セキュリティ侵害によるブランドの損害は裁判の原因になる
- にもかかわらず、法合法的なソフトウェアを開発するのは困難
 - 法律文書は曖昧[1]で、開発者は要件抽出する前に、ドメイン知識を理解しておく必要がある
 - 法律文書をクロスリファレンスしている場合、分析しないとならない法律文書が多くなる

詳しくは[1]を参照すること



これがクロスリファレンス

関連研究

- 法律文書のクロスリファレンスに関する研究が行われている
 - クロスリファレンスを分類する研究[2]
 - 判例法に基づいてクロスリファレンスのネットワークを作成する研究[3]
- 他の法律文書のクロスリファレンスを対象にした研究はされていない
 - すでに定義した要件とコンフリクトする場合があるので、他の法律文書のクロスリファレンスを分析することは重要

[2]M. Hamdaqa, A. Hamou-Lhadj, “Citation Analysis: An Approach for Facilitating the Understanding and the Analysis of Regulatory Compliance Documents,” 6th Intl. Conf. on Information Technology: New Generations, 2009, pp. 278-283.

[3]P. Zhang, L. Koppaka, “Semantics-Based Legal Citation Network”, 11th Intl. Conf. on AI and Law, 2007, pp.123-130.

研究の目的・アプローチ

- 目的

- コンフリクトを起こしている遵守要件の特定を支援し，コンフリクトを解消すること

- アプローチ

- 法律文書进行分析しクロスリファレンスの分類を定義する
 - ▶ Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule（医療保険に関する法律）を対象に分析を実施

相互参照のパターン

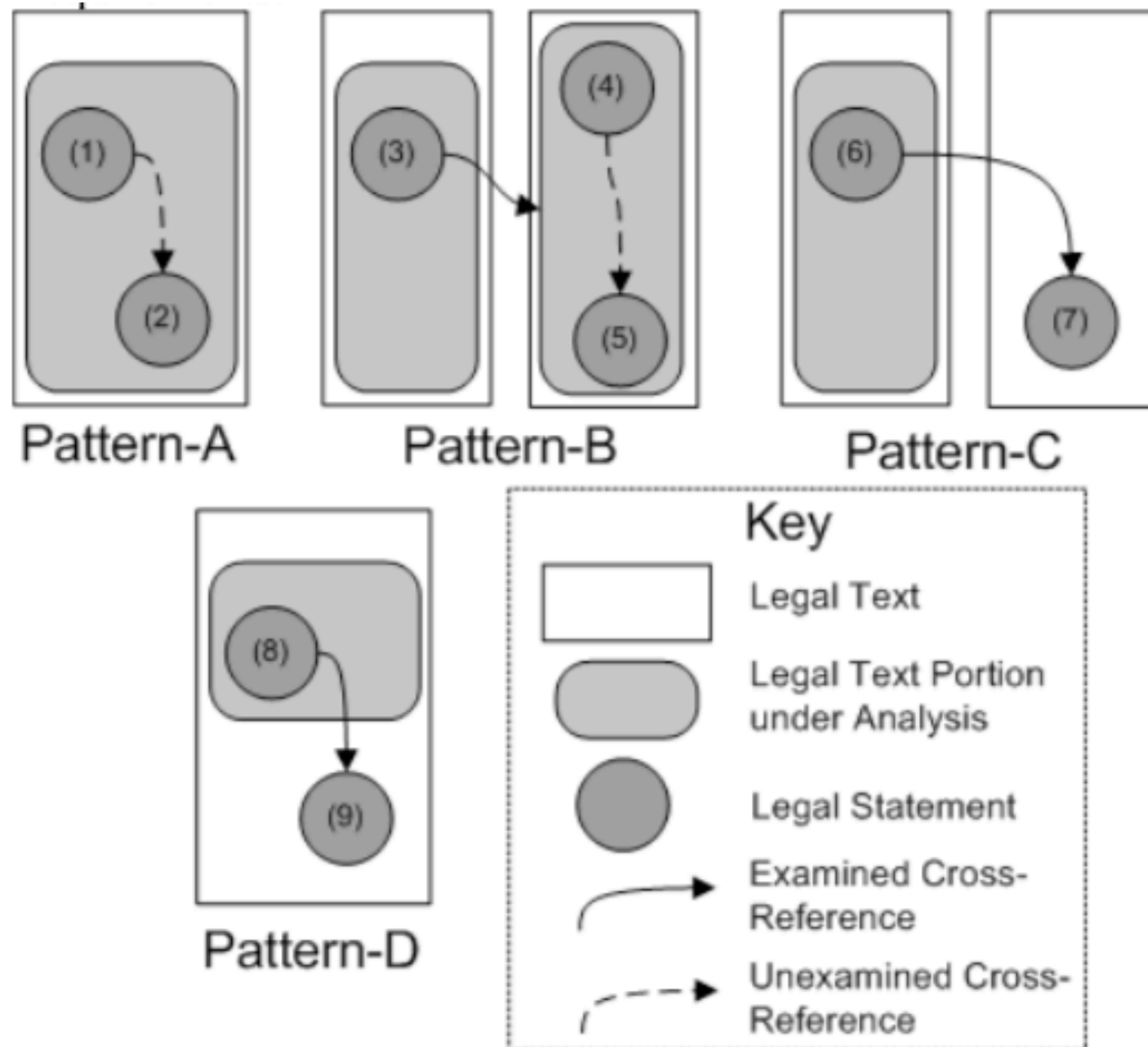


Figure 1. Possible Cross-References

- 内部参照 (A, Bの (4) → (5))
→ 参照元と参照先の法律文書が同じ
- 外部参照 (C, D)
→ 参照元と参照先の法律文書が異なる

内部参照は既存研究の対象のため除外, 外部参照のみを分析対象とする

分析対象

- 分析対象
 - Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule：医療保険に関する法律文
 - 177件の参照パターンC・D
- 分析方法
 - グランデットセオリーを実施し，クロスリファレンスを与える遵守要件への影響を分類する
 - それぞれのクロスリファレンスについて分類を実施



Figure 2. Unique Pattern-C and Pattern-D Cross-References in the HIPAA Privacy Rule

分析結果

- 以下の6つにクロスリファレンスは分類できた

分類	概要	件数
Constraint	既にある遵守要件に制約を追加する場合	51
Exception	既にある遵守要件に例外を追加する場合	18
Definition	他の法律文書の定義や用語を引用する場合	30
Unrelated	ソフトウェアに関係のない法律文を参照している場合	58
Incorrect	クロスリファレンスした先に誤りがある	2
General	具体的な法律文書の名を記さずに参照している場合 “other law”, “state law”, “applicable law”などの表現	18

Constraint

.....

- 曖昧さをなくすように使われるクロスリファレンスのこと

A covered entity may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056.

- 18 U.S.C. 3056はアメリカのシークレットサービスの権限・義務に関する法律
 - ▶ 対象を「シークレットサービスの法律によって許可された人」と具体的にしている

18 U.S.C. 3056の内容を反映すると,
...provision of protective services to the President, the Vice-President, their immediate families, former Presidents and their families, visiting heads of state, and Presidential candidates

Exception

- 例外を追加することで対象を明確にするためのクロスリファレンスのこと

individuals are given the right to inspect and obtain a copy of their PHI, except for health information that is covered by the Clinical Laboratory Improvement Amendments (CLIA) of 1988 8.

- 開発者がExceptionを見つけた際には、例外のケースを表現した要件を作成するようになる

Definition

- 他の法律文書の定義や用語を引用する際のクロスリファレンスのこと
- 複数の法律文書に用いられていると、それぞれが矛盾した定義になってしまう場合がある
 - HIPAAの"individual"
 - “person who is the subject of PHI”
 - Privacy Act of 1974の"individual"
 - “citizen of the United States or an alien lawfully admitted for permanent residence”
 - 異なる定義をしなければ法律違反の原因となる可能性がある

コンフリクトを起こしている要件

- 5つのコンフリクトを起こしていた

TABLE III. CONFLICTING REQUIREMENTS

Index	Conflicting Legal Texts	Summary of Conflict	Applicable Resolution Strategies
1	• HIPAA §164.530(j)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of data retention: • HIPAA: at least 5 years • Privacy Act: at least 6 years or the life of the record, whichever is longer • 29 CFR 1910.1020: at least 30 years if the employee worked for longer than a year	• Comply with most restrictive law • Keep data separate
2	• HIPAA §164.524(b)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of time an organization has to respond to a request for access to data: • HIPAA: in fewer than 30 days • Privacy Act: in fewer than 10 days • 29 CFR 1910.1020: in fewer than 15 working days	• Comply with most restrictive law • Keep data separate
3	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Under HIPAA, a covered entity may charge a reasonable, cost-based fee when providing copies of PHI to an individual, whereas in 29 CFR 1910.1020, employers must provide the first copy of an employees medical record free of charge	• Obligations supersede legal privileges • Keep data separate
4	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	HIPAA and 29 CFR 1910.1020 contain different conditions that prevent the release of protected information to individuals. Even if an organization can withhold information under one law, they must release it under the other law.	Consult legal domain expert
5	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Under HIPAA, covered entities must de-identify health information before they release it, but under 29 CFR 1910.1020, they may release data to employees if personal identifiers cannot be removed.	• Do not exercise legal privileges • Keep data separate

コンフリクトの解消方法

1	• HIPAA §164.530(j)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of data retention: • HIPAA: at least 5 years • Privacy Act: at least 6 years or the life of the record, whichever is longer • 29 CFR 1910.1020: at least 30 years if the employee worked for longer than a year	• Comply with most restrictive law • Keep data separate
2	• HIPAA §164.524(b)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of time an organization has to respond to a request for access to data: • HIPAA: in fewer than 30 days • Privacy Act: in fewer than 10 days • 29 CFR 1910.1020: in fewer than 15 working days	• Comply with most restrictive law • Keep data separate
		Under HIPAA, a covered entity may charge a	• Obligations supersede

- 最も制限の強い法律を適用する
 - 1の場合は30年間保存, 2の場合は1日未満でレスポンスする
- データを種類によって保存先を分割する

コンフリクトの解消方法

.....

3	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Under HIPAA, a covered entity may charge a reasonable, cost-based fee when providing copies of PHI to an individual , whereas in 29 CFR 1910.1020, employers must provide the first copy of an employees medical record free of charge	• Obligations supersede legal privileges • Keep data separate
---	---	--	---

- “must”や”cannot”と”may”でコンフリクトを起こしている場合はmustの方を適用する
- これまで述べた3つの解決策で解決できない場合は， 専門家に
お願いする

まとめ・所感

- まとめ

- 開発者のコンプライアンスに関する要件の特定を支援するために、法律文書のクロスリファレンス进行分析し分類法を提案した
- クロスリファレンスが起こすコンフリクトの解決策を提示した

- 所感

- 結果はまあそうだろうなあという感じ
- 背景の部分や引いている論文は参考にできそう