ユースケースを用いた
安全要求分析

2010年6月30日

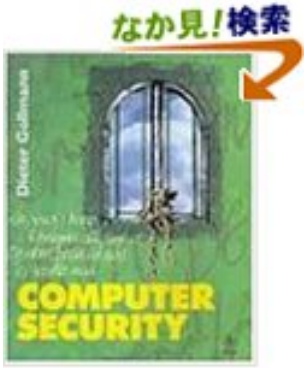
海谷 治彦

目次

- セキュリティ関係の一般的教科書紹介
- 3つの代表的なユースケース拡張
  - Misuse Cases
  - Abuse Cases
  - Security Use Cases

教科書 その一

- Dieter Gollmann. **Computer Security**. John Wiley & Sons, Feb. 1999. ISBN 0471978442, 336 pages.
- なかなか簡単でわかりやすく，広く浅く扱っているので，全体像を把握しやすい.
- 一応，RBACにも触れている.

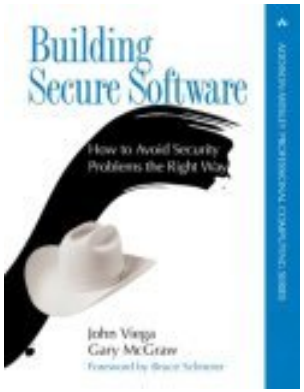


教科書その二

- Cyrus Peikari, Anton Chuvakin　著西原 啓輔　監訳伊藤 真浩, 岸 信之, 進藤 成純　訳 **セキュリティウォリア ― 敵を知り己を知れば百戦危うからず**. 2004年10月 発行 564ページ定価5,040円 ISBN4-87311-198-6.
- 教科書というより実学的？な本.

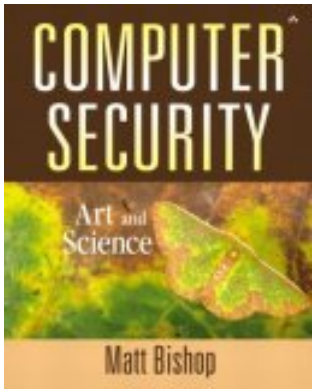
教科書 その三

- John Viega and Gray McGraw. **Building Secure Software: How to Avoid Security Problems the Right Way**. Addison-Wesley Pub, 2001. ISBN 020172152X, 493 pages.
- これも割りと実用的，というかコード寄りっぽい内容.



教科書その四

- Matt Bishop. **Computer security: art and science**. Addison-Wesley, Pearson Education, Inc, Mar. 2003. ISBN 0-201-44099-7, 1084 pages.
- NIIの中島先生に紹介してもらいました.
- 分厚くちょっと難しい・・・



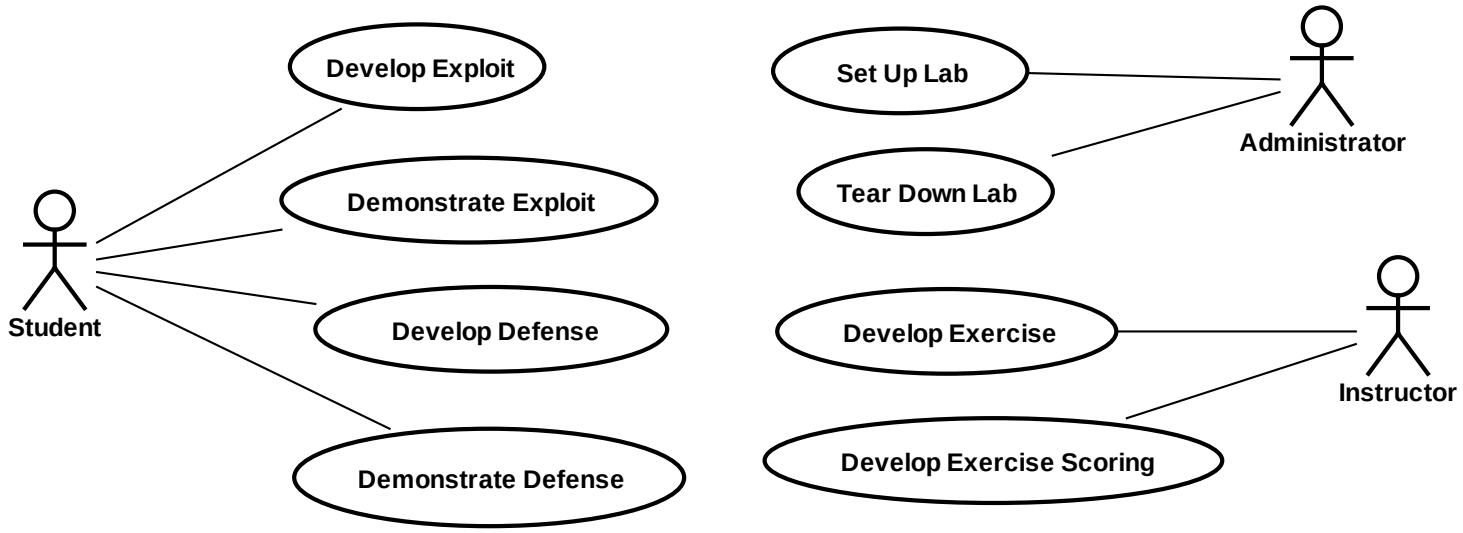
代表的なユースケースの拡張法

- Abuse Cases
  - by J. McDermott 他 (1999～)
  - 単に悪意あるアクター，処理を別途書く.
- Misuse Cases
  - by G. Sindre 他 (2000～)
  - 悪い処理と良い処理の関係．脅威と軽減
- Security Cases
  - by D. Firesmith (2003～)
  - Security use case を明示化.
  - 再利用に着目.

Abuse Casesの特徴

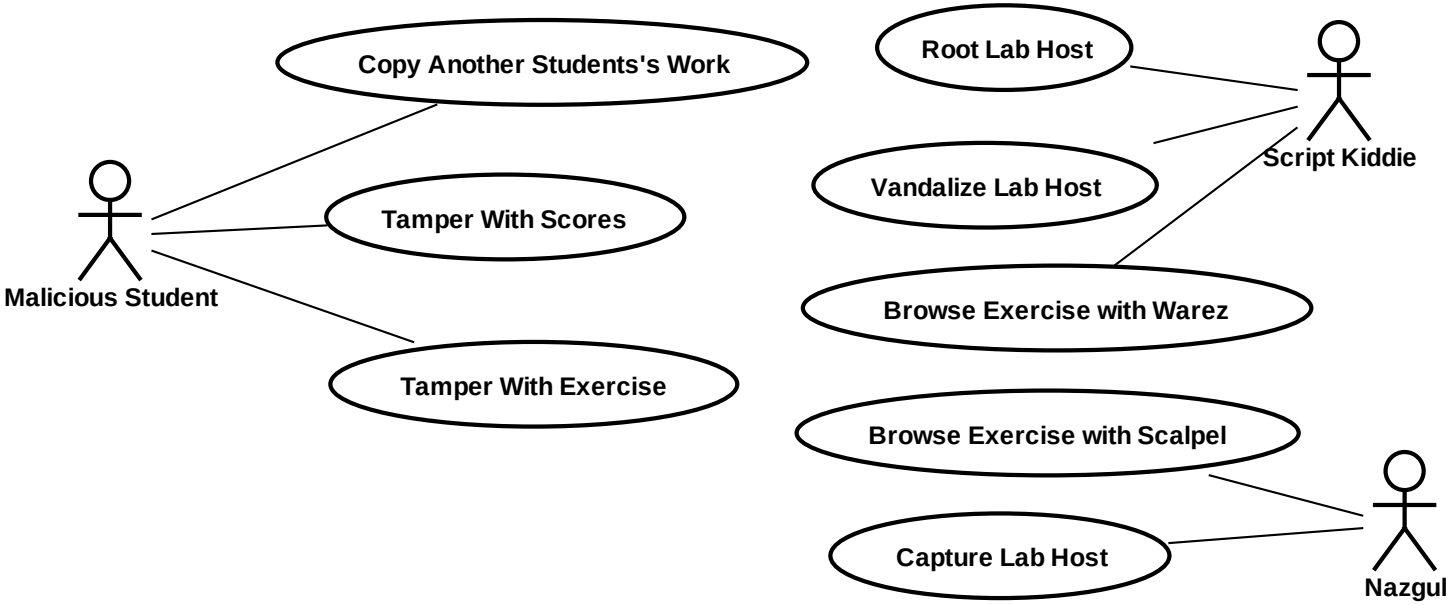
- ステレオタイプを含め文法的な拡張は行わない.
- 通常ユースケース図とアブ・ユースケース図は完全に分けて書く.
- アブ・ユースケース図のアクターに関しては，資源，技能レベル，目的を詳細に書いてもよい.

通常のユースケース



セキュリティ教育のWBTらしい.

アブユースケース


Copy Another Students's Work
Tamper With Scores
Tamper With Exercise
Malicious Student
Root Lab Host
Vandalize Lab Host
Browse Exercise with Warez
Script Kiddie
Browse Exercise with Scalpel
Capture Lab Host
Nazgul

Script Kiddieの仕様

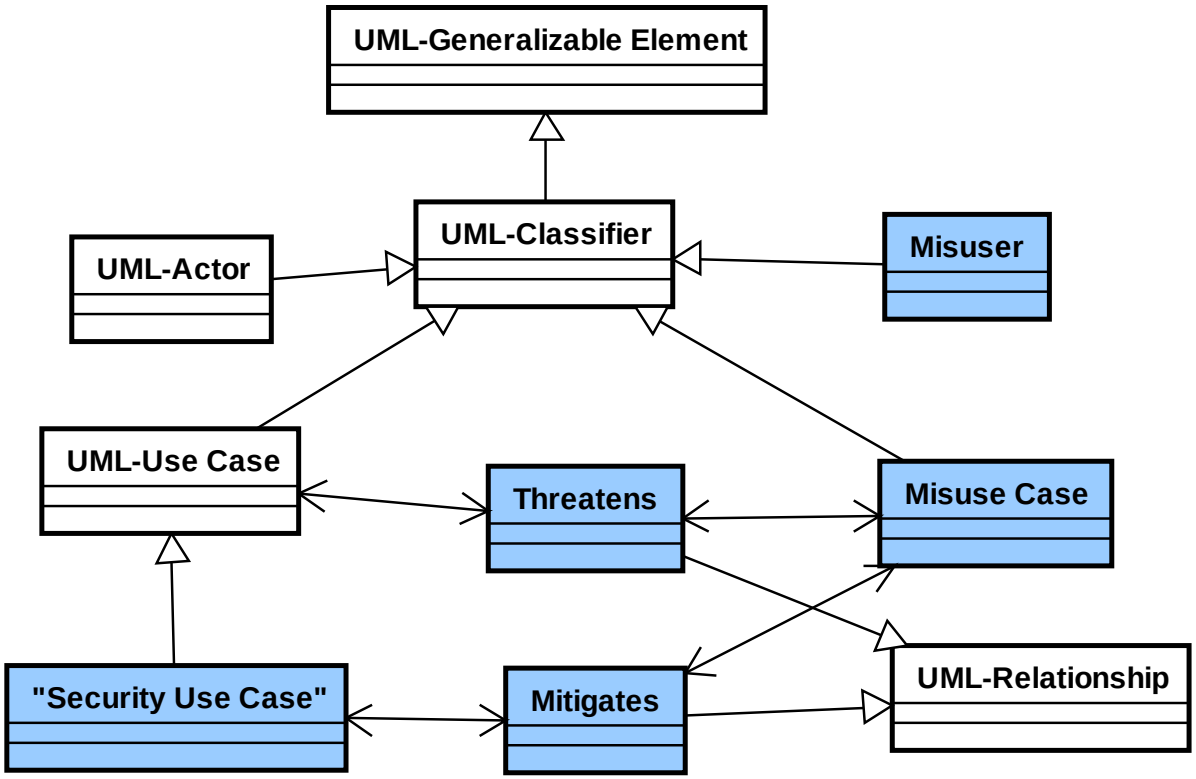
Script Kiddie

[資源] 通常一人で作業を行うが，他のScript Kiddieと情報交換をする場合もある.
必要なハードウェア，ソフトウェア，インターネット接続を有している.
これらは個人で購入したものか，もしくは職場等の資源を悪用する場合もある.
本分析でのScript Kiddieは常時攻撃を行っているものと想定する.
[技能レベル]
高くない．他者が提供するツールや技術の利用法を知っているだけである.
[目的]
暴力行為や窃盗そのものを目的としており，中には自分の腕前を自慢する目的の者もいる.

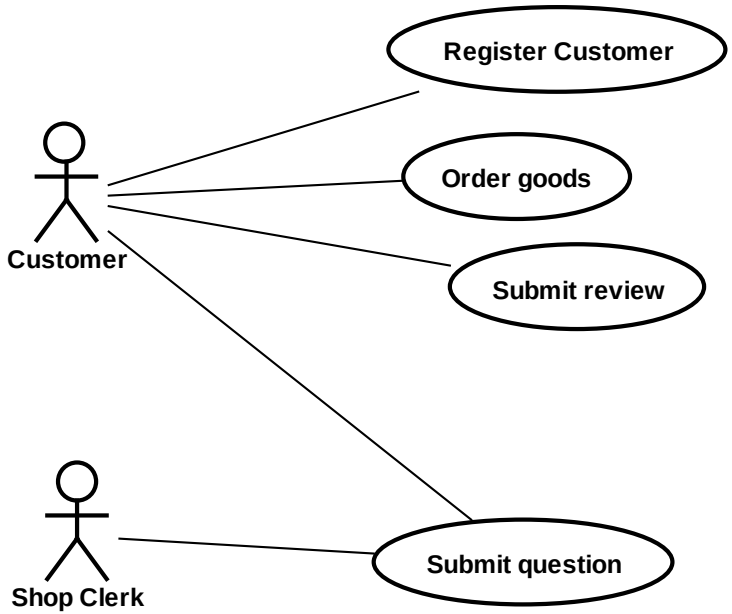
Misuse Casesの特徴

- 害となるユースケース，害をなすアクターを構文的に分けて書く.
- 通常なものと害なものを1つの図に書く.
- あるMisuse Caseがユースケースに脅威を与えることを threaten という関連で仕様化.
- あるユースケースがMisuse Caseの脅威軽減となることをmitigateという関連で仕様化.
  - コレはセキュリティケース(後述)に相当する.

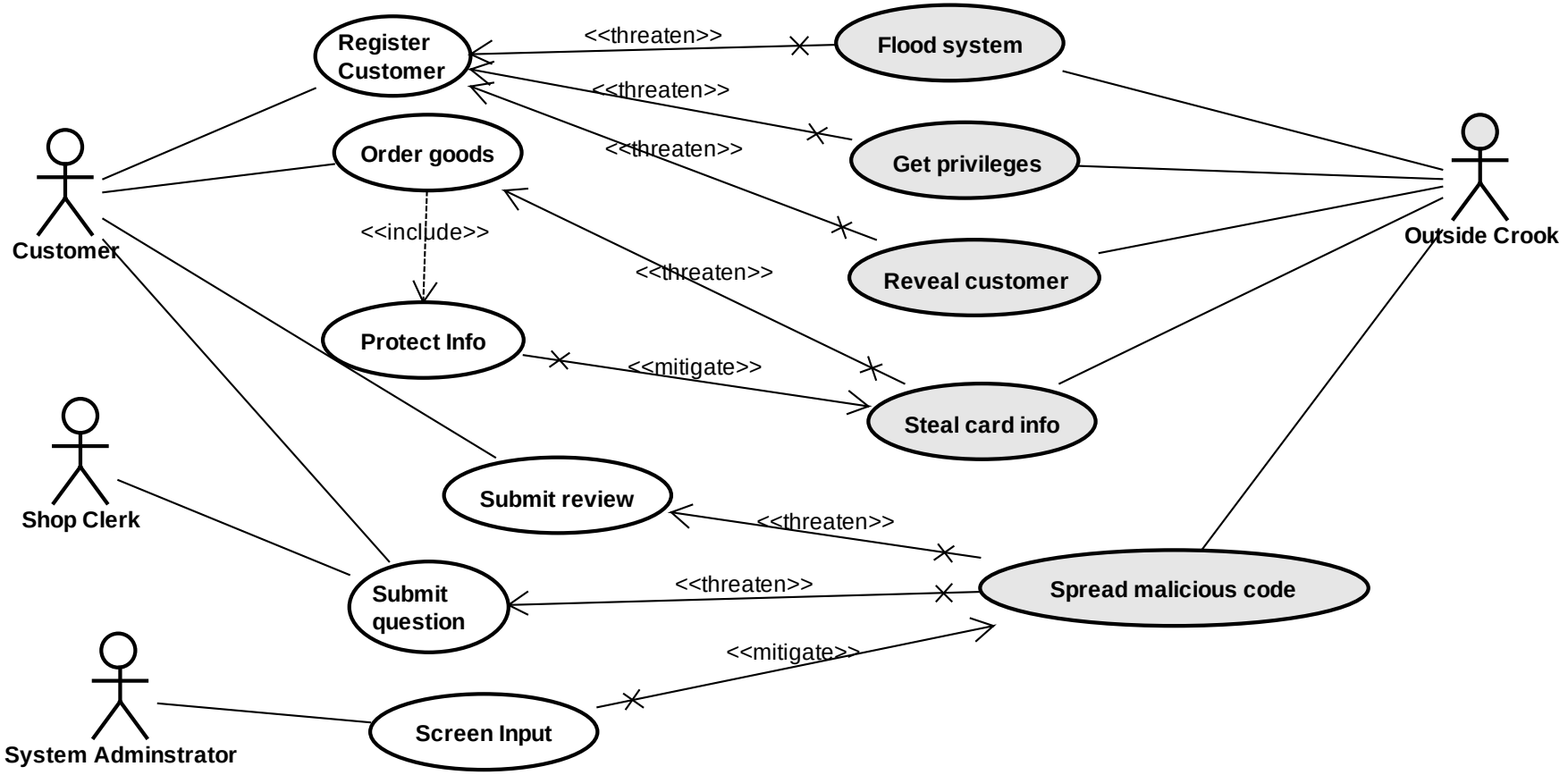
メタモデル (データ構造)


UML-Generalizable Element
UML-Classifier
UML-Actor
Misuser
UML-Use Case
Threatens
Misuse Case
"Security Use Case"
Mitigates
UML-Relationship

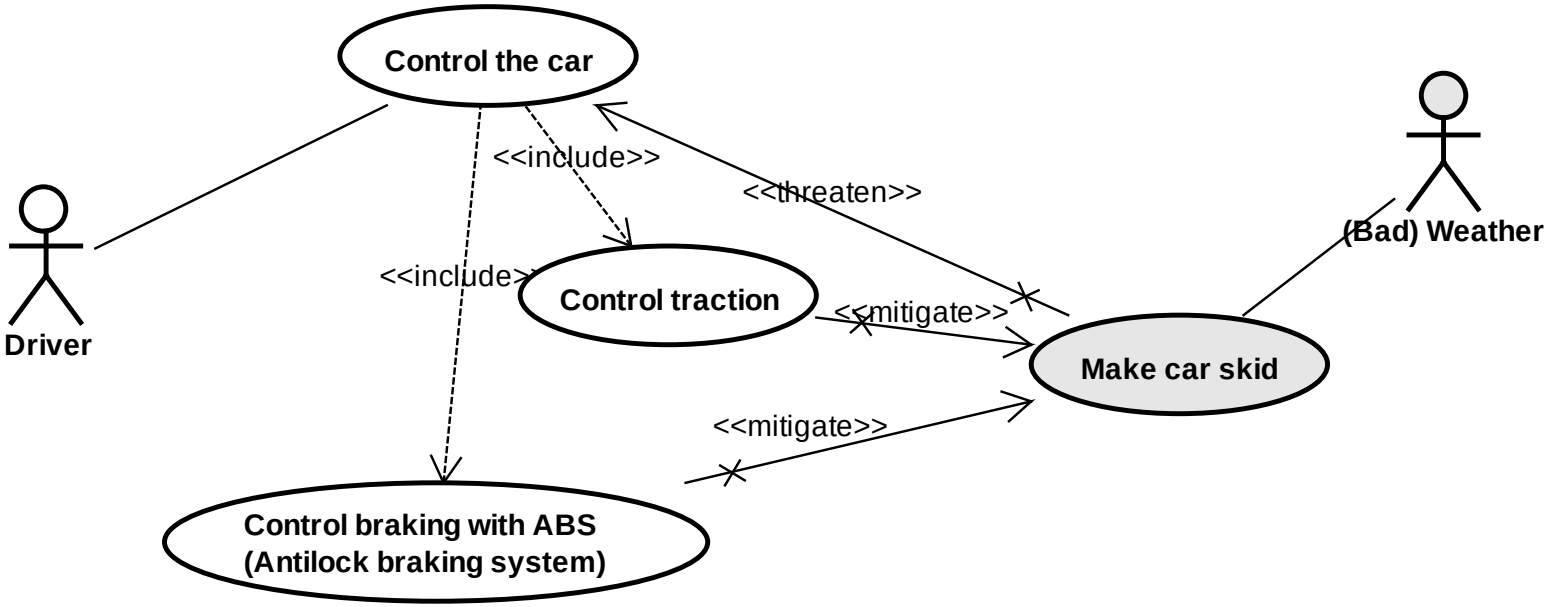
電子ショップ (普通のUCD)



Misuse Casesを含めたUCD



安全要求についても対応可能



ユースケース記述について

- 軽量化記法と，広範囲記法がある.
- 軽量化記法: 通常ユースケース記述に「脅威」項目を付加したもの.
- 広範囲機能: ミスユースケース主体で書く.

軽量化記法の例 1/2

名前: 顧客登録
概要: 顧客は氏名，住所，メールアドレス，電話番号を与え，eショップに顧客登録する.
正常パス: bp-1. 顧客は「登録」を選択する.
bp-2. システムはフォームを提示する.
bp-3. 顧客はフォームを埋めて，送信する.
bp-4. システムは登録完了を知らせ，顧客の参照番号を返す.
代替パス: (略)
例外パス: E1. bp-3において顧客が必須情報を埋め忘れた場合，
より詳細な情報を示しbp-3に戻る.
E2. bp-3において既登録ユーザーの情報と一致した場合，
システムはユーザーに対して既に登録されているので，
現登録作業は破棄される旨と提示する.
そして，本ユースケースを終了する.

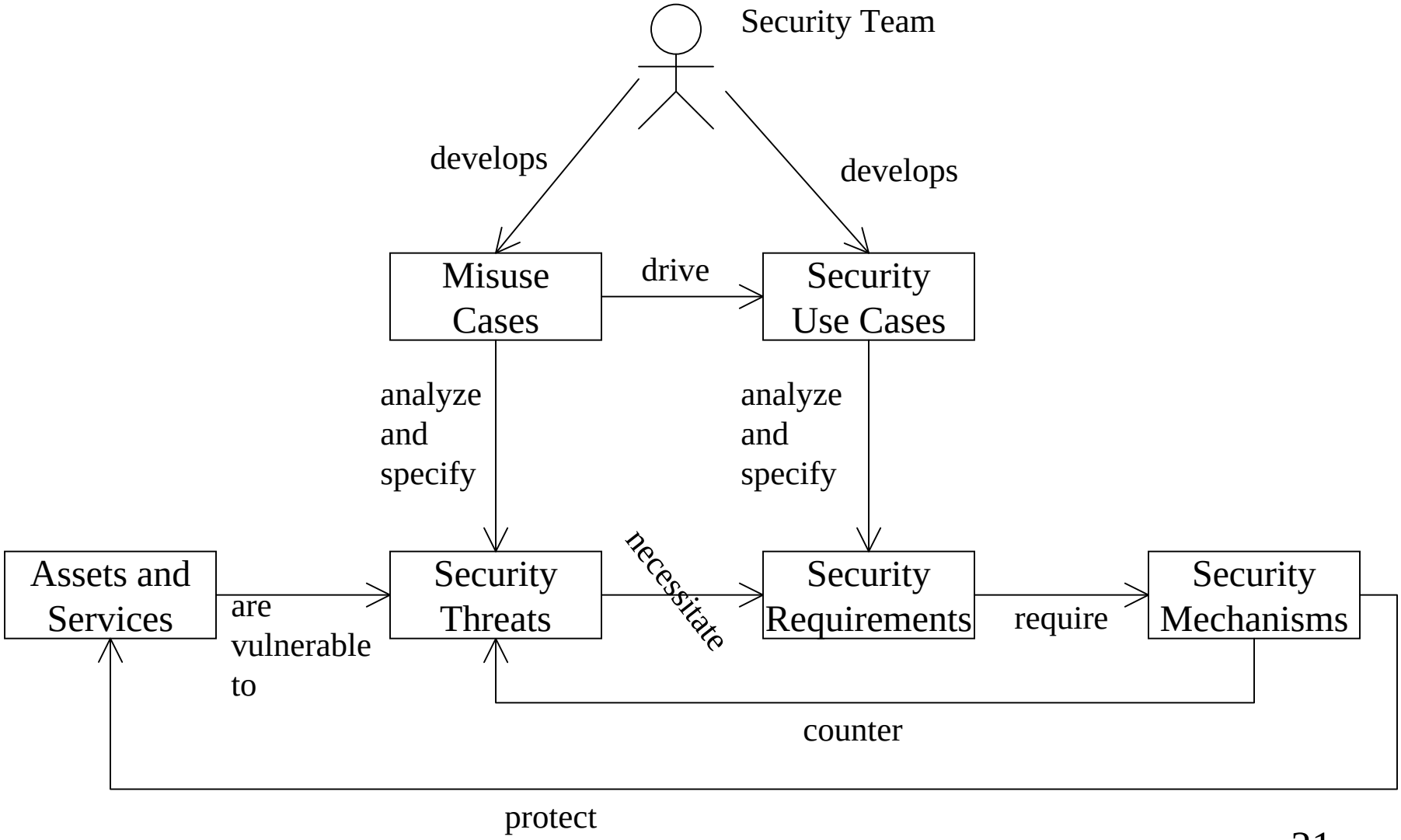
軽量化記法の例 2/2

仮定: (略)
事前条件: (略)
事後条件: 顧客は登録され，新規に連絡情報等を与えなくてもeショップで
　　商品を注文することができるようになる.
脅威: T1: 顧客が自身の本名，本住所でなく，仮(偽り)のもので登録しようとする.
　起こりうる事態は以下の通り.
　T1-1. 実在しない人物が登録されてしまう.
　T1-2. 実在人物が本人の意に反して登録されてしまう.
　T1-3. 既に登録されている人物が誰かを第三者がチェックできてしまう(E2を用いて).

Security Casesの特徴

- 基本的なアイディアはMisuse Casesと同じ.
- しかし，セキュリティ面の概念と要求との関係をよく整理している(後述).
- 特に以下の二点が特徴.
  - 実現機構(パスワード認証等)と要求(識別，認証，認定を必要とする等)の区別を明確化.
  - セキュリティ要求は比較的アプリによらず再利用しやすいことを主張.

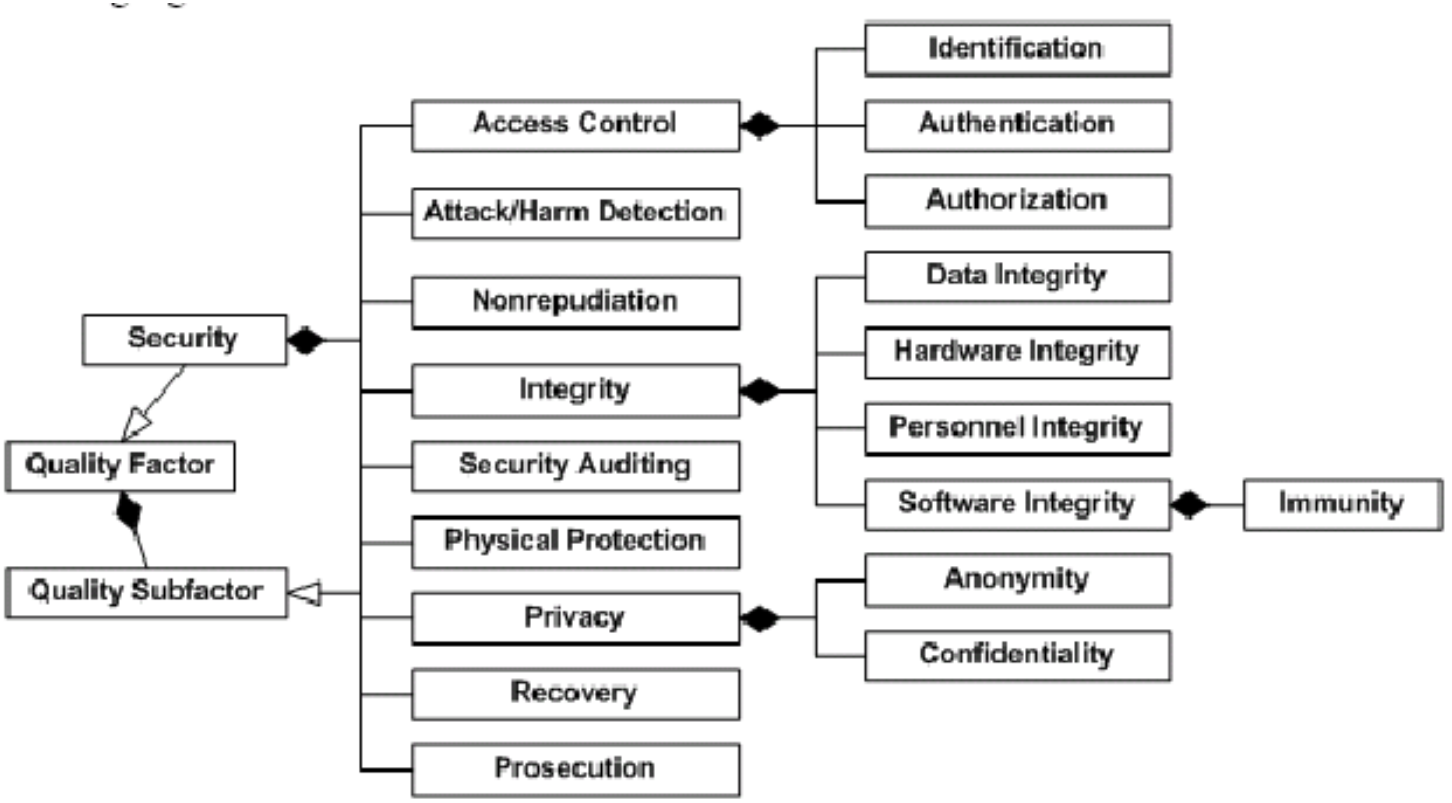
Security Cases関係の概念と関係



Security Casesの再利用

- セキュリティに関わる品質要因を階層的に分類する.
- それぞれの分類に対して一般的なユースケース記述を事前に与える.
- これら一般的なユースケースを個々の事例に適用することで，再利用の促進を図る.

分類


Identification
Access Control
Authentication
Authorization
Attack/Harm Detection
Data Integrity
Nonrepudiation
Hardware Integrity
Security
Integrity
Personnel Integrity
Quality Factor
Security Auditing
Software Integrity
Immunity
Physical Protection
Anonymity
Quality Subfactor
Privacy
Confidentiality
Recovery
Prosecution

Integrity その一

Use case: Integrity		
Use Case Path: システムのデータ保護		
脅威: ミスユーザーがシステムの重要なデータを改悪する.		
事前条件: 改悪されうるデータをシステムに保存する.		
事後条件: 重要なデータが改悪されていないことが確認されていること.		
ミスユーザーの相互作用	システム要求	
	相互作用	アクション
ミスユーザーは重要なデータを改悪しようとする.		
		改悪を阻止するようなアクションをとる.
	管理者に改悪の試行があったことを報告する.	

Integrity その二

Use case: Integrity			
Use Case Path: システムのメッセージ保護			
脅威: ミスユーザーがシステムからユーザーへのメッセージを改悪する.			
事前条件: (1) ミスユーザーはメッセージを横取りする手段を持つ. (2) 横取りしたメッセージを改変する手段を持つ. (3) 改変したメッセージをユーザーへ再送信する手段を持つ.			
事後条件: システムはメッセージが改変された旨をユーザーに通知する.			
ユーザーの相互作用	ミスユーザーの相互作用	システム要求	
		相互作用	アクション
		システムがユーザーにメッセージを送る	メッセージの改変があった場合, その旨がユーザーにわかるようにする.
	メッセージを横取り, 改変し, 改変したものをユーザーに転送する.		
改変されたメッセージを受信する.			システムはメッセージ改変を認識しておく.
		システムはメッセージ改変が起こった旨をユーザーに通知する.	

Integrity その三

Use case: Integrity			
Use Case Path: ユーザーメッセージ保護			
脅威: ミスユーザーがユーザーからシステムへのメッセージを改悪する.			
事前条件: ミスユーザーはユーザーとシステムの間の割り込む手段を持つ.			
事後条件: システムはユーザーにユーザーの入れたメッセージが改変された旨を通知する.			
ユーザーの相互作用	ミスユーザーの相互作用	システム要求	
		相互作用	アクション
ユーザーはシステムにメッセージを送る.			
	ミスユーザーはユーザーメッセージを横取り改変しシステムに転送する.		
			システムはユーザーメッセージが改変されたことを識別する.
		システムは改変された旨をユーザーに通知する.	

参考文献

1. John McDermott and Chris Fox. **Using Abuse Case Models for Security Requirements Analysis**. In 15th Annual Computer Security Applications Conference (ACSAC'99), pp. 55-64, Phoenix, Arizona, Dec. 1999.
2. J. McDermott. **Abuse-Case-Based Assurance Arguments.** In 17th Annual Computer Security Applications Conference (ACSAC'01), pp. 366-374, New Orleans, Lousiana, Dec. 2001.
3. G. Sindre and A. L. Opdahl. **Eliciting Security Requirements by Misuse Cases.** In 37th International Conference on Technology of Object-Oriented Languages and Systems (TOOLS-37'00), pp. 120-131, Nov. 2000.
4. Guttorm Sindre and Andreas L. Opdahl. **Eliciting security requirements with misuse cases.** Requirements Engineering, Vol. 10, No. 1, pp. 34 - 44, Jan. 2005.
5. Ian Alexander. Misuse Cases: **Use Cases with Hostile Intent**. IEEE Software, Vol. 20, No. 1, pp. 58-66, Jan./Feb. 2003.
6. Donald Firesmith. **Security Use Cases**. Journal of Object Technology, Vol. 2, No. 3, pp. 53-64, May-Jun. 2003.
7. Donald Firesmith. **Specifying Reusable Security Requirements**. Journal of Object Technology, Vol. 3, No. 1, pp. 61-75, Jan.-Feb. 2004.