クラウドサービス選択支援のためのセキュリティ評価について

2011SE116　片岡　優貴　　2011SE145　楠　実悠

指導教員　青山　幹雄

1. 研究背景

近年，クラウドサービスを利用する企業が増えている．しかし，セキュリティの懸念が増大している[3]．また，提供されるサービスが抽象化されるため，サービスの詳細が隠ぺいされ，最適なサービスの選択が困難である．

2. 研究課題

本研究では前述を踏まえ，クラウドの特性から，ニーズにあったクラウドサービスの選択が困難であるという課題を解決するため，新たな要求工学アプローチを提案する．

企業がクラウドを選定する際に，自社のニーズにマッチしたサービスを選択するため，ミスユースケースによってステークホルダの関係を明示し，ETA による情報漏洩発生確率の解析を行うことによって，クラウドサービスの選択を支援する，セキュリティ評価手法を提案する．

3. 関連研究

3.1. ミスユースケース分析

ミスユースケース分析[5]とは，機能要求を把握する手法であるユースケースに，攻撃者や脅威，それに対する対応策を明示し，モデル化を可能にする拡張を加えたものである．以下の表 1 にミスユースケース図の構成要素を示す(表 1).

表 1 ミスユースケースの構成要素

構成要素	詳細
アクタ	システムを利用するユーザ
ユースケース	アクタのシステムに関する振舞い
ミスアクタ	攻撃を与えるアクタ
ミスユースケース	システムに関する攻撃の振舞い
theraten	脅威
mitigate	緩和

3.2. ETA(Event Tree Analysis)

ETA[2]では，ミスユースケース分析で明らかになった攻撃に関して全ての対応策が機能しないことを前提にし，解析を行う．また各分岐点の対策失敗確立を求めることにより，初期事象の攻撃成功確率を解析することができる．

4. アプローチ

本稿では，クラウドサービス比較要素の1つであるセキュリティに着目する．セキュリティ要求満足度の評価のため，ミスユースケース分析と ETA を用いる．ミスユースケース分析によって，クラウドサービスを利用するコンシューマにどのようなリスクがあるのかを明確にできる．また，ETA により，主観や分析者の経験によらないサービスの選択が可能になる．よって，コンシューマのニーズにマッチしたクラウドサービスの選択が可能になると期待できる．

5. 提案方法

5.1. 提案プロセス

REBOK[4]の要求工学プロセスを参考とし，クラウドサービス選択におけるセキュリティ評価に特化した新たな要求プロセスを定義する(図 1).

新たに定義するプロセスは，ミスユースケースと ETA を組み合わせ，情報漏洩確率を求めることによってセキュリティを評価するものである．そして，各クラウドサービスの評価を行い，比較する．

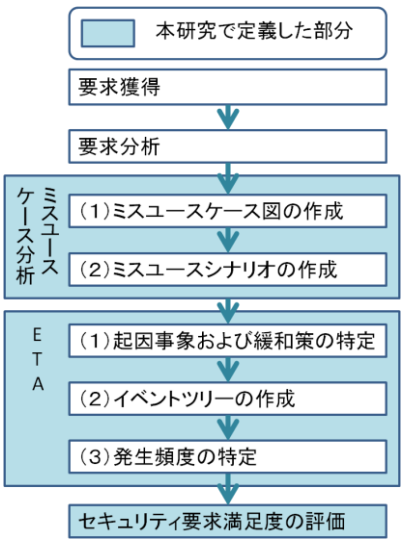

図 1　提案するセキュリティ評価プロセス

5.2. ミスユースケース分析

(1)ミスユースケース図を作成

上記の 5.2.1 を用いてミスユースケース図を作成する．

1.ユースケースを記述する

2.システムに関する資産(データ)を抽出し記述する

3.各資産についてセキュリティのゴールを設定する

4.ゴールを侵害する可能性のある脅威をミスユースケースとして，その当事者をミスユーザとして記述する

5.ミスユースケースを緩和する対策を記述
(3)ミスユースシナリオを作成
上記5.2.1を用いて，表2ミスユースケースシナリオの項目を記述する.

5.3. ETA

5.3.1. 定義

本稿では，初期事象である攻撃をα0，対応策の各分岐点の失敗確率をα1，α2 などの変数で表す．それぞれの失敗確率を掛け合わせていくことで最終的に攻撃の成功確率を表す．ここでは攻撃成功確率の低い順番に1，2，3と割り当てる.

5.3.2. 手順

(1)初期事象および緩和ポイントの特定
初期事象は，上記 5.2.2 で示した攻撃のことであり，緩和策とは，上記 5.2.2 に示した通りである.
(2)イベントツリーの作成
ページの上方に初期事象と，関連する緩和策の応答を時系列に配列する．次に成功と失敗のパスに分岐する(成功パスを上に，失敗パスは下に)．すべての緩和ポイントについて同様の分岐を続け，最終的な結果事象を記述する.
(4)発生頻度の推定
初期事象の発生頻度と，緩和策の成功/失敗の分岐確率を設定すれば，各事故シーケンスの発生頻度を計算することが出来る.

5.3.3. パターン

本稿では攻撃成功確率を変数で表すので，サービス比較を行うことができないという問題が発生する．そのため，以下の方法で攻撃成功確率の比較を行う．2つのクラウドサービス，クラウド A とクラウド B に関して，同じ攻撃に対する緩和策がα0×α1×α2とβ0×β1×β2の場合，3つのパターンに分けて比較し,評価値を割り当てる.
(1)α0×α1×α2＞β0×β1×β2の場合
クラウド A 評価値:2　　クラウド B 評価値:1
(2)α0×α1×α2＝β0×β1×β2の場合
クラウド A 評価値:1　　クラウド B 評価値:1
(3)α0×α1×α2＜β0×β1×β2の場合
クラウド A 評価値:1　　クラウド B 評価値:2
本稿では，クラウドサービスのセキュリティ分析方法におけるプロセスを提案しているため，上記の 3 パターンの内，どのパターンを用いるかについては任意で決定する.
また，実際には対応策は実数値で表せられるため，上記のような方法を用いる必要はない.

5.4. セキュリティ要求満足度の評価

5.2.2「要求分析」で定義されたセキュリティの項目を照らし合わせ，サービスを評価する.「サービスを評価する」とは，コンシューマの要求を，クラウドサービスがどの程度満たしているかを見極めるために，値を算出することである．サービスを評価した値を，評価値とする．サービスを評価するために，セキュリティ要求に対応するセキュリティ項目の状態を評価し，要求の優先順位によって重み付けを行う.
セキュリティ項目の状態評価を以下のように定義する.
(1)記載なし
あるセキュリティ要求の項目に対し，対応するセキュリティ項目が記載されていない状態.
(2)記載あり
各選択肢を比べ，発生確率の低い方が優れたクラウドサービスであるとし，優れたものから順番に順位付けする.
サービスの評価に反映させる重みは，セキュリティの優先順位の逆数を用いる．これにより，優先順位が高いものを含むサービスほどセキュリティ評価値が高くなる.
セキュリティ評価値の算定式を以下のように定義する(式1).

(式 1)セキュリティ評価値の算定式

$$\sum_{k=1}^{n}(\text{優先順位k の発生確率順位の逆数}) \times (\text{優先順位k の逆数})$$

n:最下位の優先順位の値

6. 要求分析方法の評価

6.1. 評価の目的

例題を用いて提案プロセスを行うことで，サービス比較の考察と評価を行う.

6.2. 評価範囲

提案する要求工学プロセスの妥当性を確認するために，適当なセキュリティ要求の例を用いて検証と評価を行う．また，要求獲得，要求分析は REBOK の要求工学プロセスに沿って行う．そのため，評価の範囲をミスユースケース分析，ETA，セキュリティ要求満足度の評価の 3 つのプロセスとする.

6.3. 評価の前提条件

評価の前提条件として，以下の 4 つを挙げる.
(1) SaaS，PaaS，IaaS を対象とし，独立事象として考える.
(2) 要求獲得，要求分析はすでに終わっている.
(3) ETA は緩和策の具体的な数字が確立されていないため，変数を用いて行う.
(4) セキュリティ評価における攻撃発生確率の変数の比較を 5.3.3 のように 3 つのパターンに分け行う.
このように各選択肢を比べ，発生確率の低い方がより優れたクラウドサービスであるとして評価を行う.

6.3.1. セキュリティ要求の優先順位付け

クラウドサービス形態毎のセキュリティ要件の優先順位を以下の表 2 に示した.
ここでは SLA のクラウドリスクコントロールのセキュリティ項目を参照し，優先順位付けを行った[1].

表 2　PaaS に対するセキュリティ要求の優先順位

優先順位	リスク要求
1	特権IDの悪用
2	解約時の利用者データが消去されない
3	二次記憶媒体からのデータ漏洩
4	分散された転送データの盗聴
5	他の利用者による不正行為
6	利用者間のデータ漏洩
7	不正アクセスによる情報漏洩
8	リソース分離不備による情報漏洩
9	安全性・信頼性の高いデータセンタを利用しない
10	他の利用者の被害が自社に及ぶ
11	IDの管理不備によるインシデント発生時のトレース不可能
12	利用者の想定外のデータ入力
13	パブリックネットワーク利用による脅威

6.4. 検証評価

SLA のクラウドリスクコントロールのセキュリティ項目とサービス選択の検証評価について説明する

6.4.1. PaaS の検証評価

(1)ミスユースケース分析

緩和策を攻撃の分類に最も有効であるものと結びつけ，なおかつ攻撃はリスク要求に最も意味の近いものに結びつけた．また，パスワード設定などの設定強化をユーザが，ユーザのアクセス管理などをユーザ管理者が行うこととする．そして，サービスの監視や管理を運用担当者が，攻撃を受けた際に拡張機能や新サービスの提供を開発担当者が行うこととする．

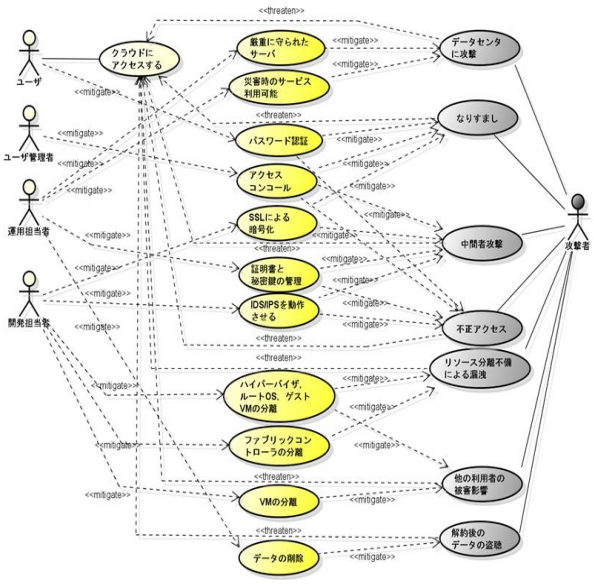

図 2　WindowsAzure のミスユースケース

(2) ETA

優先順位 7 の「不正アクセス」の緩和策の ETA について説明する．また，WindowsAzure の緩和策の変数を α，α'などで表した．

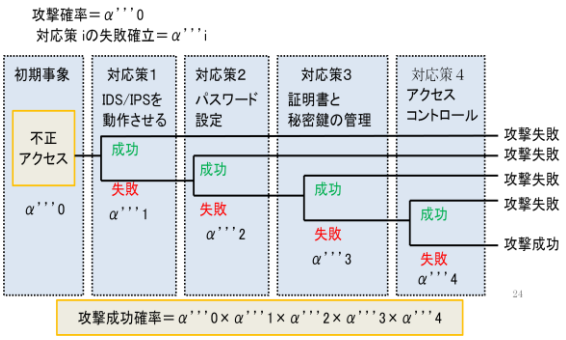

図 3　WindowsAzure の ETA

(3)セキュリティ評価値の算出

全ての攻撃に対する緩和策の ETA を行い，攻撃発生確率のパターン分けから評価値を求め，求めた値を基にセキュリティの評価値の算出を行った．

(4)セキュリティ評価値算出によるサービスの評価

ETA の評価値とセキュリティ評価値を基に，クラウドサービスのセキュリティについて以下の表●にまとめた．

表 3　WindowsAzure のセキュリティ評価値

優先順位	リスク要求	リスク	確率	評価値
1	特権IDの悪用	なりすまし	α'0×α'1×α'2×α'3	2
2	解約時の利用者データが消去されない	解約後のデータ盗聴	α''''0×α''''1	1
3	二次記憶媒体からのデータ漏洩			0
4	分散された転送データの盗聴	中間者攻撃	α''0×α''1×α''2×α''3×α''4	1
5	他の利用者による不正行為			0
6	利用者間のデータ漏洩			0
7	不正アクセスによる情報漏洩	不正アクセス	α'''0×α'''1×α'''2×α'''3×α'''4	2
8	リソース分離不備による情報漏洩	リソース分離不備による情報漏洩	α''''0×α''''1×α''''2	1
9	安全性・信頼性の高いデータセンタを利用しない	データセンタに攻撃	α0×α1×α2	1
10	他の利用者の被害が自社に及ぶ	他の利用者の被害影響	α''''0×α''''1×α''''2	1
11	IDの管理不備によるインシデント発生時のトレース不可能			0
12	利用者の想定外のデータ入力			0
13	パブリックネットワーク利用による脅威			0
WindowsAzure セキュリティ評価値				
1.66				

6.5. クラウド連携による検証評価

PaaS と同様に，SaaS と IaaS についてもセキュリティ評価を行い，この検証評価を基にクラウド連携によるサービス評価を行った．

クラウドサービスは SaaS，PaaS，IaaS のそれぞれが関連し合い，サプライチェーンを形成し，サービス全体を提供することがある．よって，評価を行った 6 つのクラウドサービスを組み合わせた際に，最もセキュリティ要求満足度が高い

クラウドサービスについて説明する．また，セキュリティ評価値が高いクラウドサービスであっても，いくつかのクラウドサービスには連携が不可能であるサービスもあるため，連携可能であることが明らかとなっているサービスの組み合わせについて紹介する．

表 4　クラウドサービス評価値一覧

リスク要求	要求分析によるリスク優先順位					
	SaaS		PaaS		IaaS	
セキュリティ評価値	Desknet's	Google Apps	Windows Azure	Force.com	NIFTY Cloud	Amazon EC2
	1.35	1.72	1.66	1.46	0.94	1.20

クラウド連携が可能であることが明らかである組み合わせから，連携評価値を求めた．

表 4 を基にこれらのクラウドが連携した際のセキュリティ評価値を以下の表 5 に示す．

表 5　クラウド連携によるセキュリティ評価値

	1	2	3	4
SaaS	Desknet's	GoogleApps	GoogleApps	GoogleApps
	1.35	1.72	1.72	1.72
PaaS	Windowsazure	Windowsazure	Force.com	Force.com
	1.66	1.66	1.46	1.46
IaaS	NiftyCloud	NiftyCloud	NiftyCloud	AmazonEC2
	0.94	0.94	0.94	1.20
評価値	2.10	2.68	2.36	3.01

表 5 より SaaS，PaaS，IaaS のクラウドサービス連携の内，最もセキュリティ要求満足度の高い組み合わせは，Google Apps，Force.com，Amazon EC2 であった．

7. 評価プロセスの評価

7.1. ミスユースケース分析

このプロセスで，セキュリティのモデル化を行うことにより，リスクを洗い出し，様々なステークホルダの振舞いと結びつけ，次に行う ETA に繋げることができた．また，ETA の欠点である「適切な起因事象を識別できない点」や，「寄与する対応策の全てを識別できない点」などを防ぐことができた．

7.2. ETA

ETA により，多重の緩和策をもつ複雑なサービスにおいて，ひとつの起因事象に対する攻撃成功確率を特定することが出来た．しかし，本稿で示したサービスの緩和策についての情報は，一部公開していないプロバイダが多い．

7.3. セキュリティ要求満足度の評価

要求の優先順位とセキュリティ評価値を照らし合わせることで，コンシューマに最適であると考えられるサービスのセキュリティ要求満足度の評価が可能となった．しかし，リスクを要求の分類に振り分けなければならないため，リスクに対する前提知識が必要であるといえる．

7.4. 要求分析方法の評価

実際にクラウドサービスの評価を行い，定量的にセキュリティ要求満足度を評価することが出来たので，コンシューマのニーズにマッチしたサービスを選択するための支援ができた．

8. 今後の課題

今後の課題として，以下のものが挙げられる．

(1)クラウドサービスの攻撃緩和策の明確化

本稿では，クラウドサービスの緩和策を調査し，セキュリティリスクを結びつけた．しかし，実際には緩和策の一部の情報しか公開していないプロバイダも多い．よって，影響度や発生頻度の高いセキュリティリスクの緩和策を絞り込み，分析を行う必要がある．

(2)評価値の妥当性の検証

今回，記載なしのものは評価値を0とした．しかし，記載のあるものの方が優れているとし評価値を 1，記載がないものを 2 とする評価方法も考えられる．

よりサービス評価に適している方を採用するため，どちらの評価方法が妥当であるか検証する必要がある．

(3) 評価システム構築の作成支援

提案した分析方法を適用すると，ミスユースケースや ETA の作成に工数を要す．工数削減を行うためには，ミスユースケースとETAを自動作成し，セキュリティ要求満足度を自動評価できるシステムの構築が必要である．

9. まとめ

本研究では，近年利用が増加しているクラウドサービスにおいて，セキュリティに関する課題と,サービスの不透明性に着目し，コンシューマが最適なクラウドサービスを選択するための支援となるセキュリティ評価手法を提案した．ミスユースケースと，ETA を用いることによって，セキュリティの評価を可能にする．

10. 参考文献

[1] 一般社団法人電子情報技術産業協会ソリューションサービス事業委員会，民間向け IT システムの SLA ガイドライン，第 4 版，日経 BP 社，2012.

[2]松岡 俊介，プラントの安全性評価，2008.
http://hazop.jp/pdf/guide4.pdf

[3]NRI セキュアテクノロジーズ,企業における情報セキュリティ実態調査，2009.

[4]REBOK 企画 WG，要求工学知識体系 第1版，近代科学社，2011.

[5] Guttorm Sindre，Andreas L. Opdahl，Requirements Engineering，2005.