3V-7

脅威の変化に対応した動的なリスク分析手法の検討

川西　英明[†]　　ラミレス・カセレス・ギジェルモ・オラシオ[‡]　　勅使河原　可海[‡]

創価大学工学部[†]　　創価大学大学院工学研究科[‡]

1.　はじめに

現在，数多くのリスク分析の手法が存在する．それらの多くは，企業のある時点におけるリスクを分析するものである．しかし，企業をとりまく環境は常に変化するものであり，それに伴いリスクの大きさも変化する．既存のリスク分析では，分析に数週間から数ヶ月かかり，費用も多額になるため，日々の組織の環境の変化に対応した分析を行うことが困難である．また，日々の環境の変化に対応するものとして，デバイスの脆弱性を常時把握し，統合的に管理する脆弱性診断ツールも存在する．しかし，脆弱性だけではなく，脅威や資産も変化するものである．そこで，本研究では環境の変化による，資産・脅威・脆弱性の変化を考慮に入れた動的なリスク分析手法の検討を行なっている．本稿では，特に脅威に着目し，脅威が資産に及ぼす影響の変化を考慮に入れた，動的なリスク分析手法の検討を行なう．

2.　ISO/IEC TR 13335

ITセキュリティマネジメントのためのガイドラインであり，GMITSと呼ばれる．GMITSは，情報技術のセキュリティに関連した運用管理，計画を対象とした標準を設定することを目的としている．本稿では，GMITSを基に用語の定義を行なっているため，以下にGMITSにおける用語の定義を示す[1].

2.1 責任追跡性

あるエンティティの動作が，そのエンティティに対して一意に追跡できることを保証する特性.

2.2 真正性

対象またはリソースが要求されているものと同一であることを主張する特性．ユーザ，プロセス，システム，情報などに対して適用する.

2.3 信頼性

矛盾のない計画どおりの動作および結果を確保する特性.

3.　提案手法

3.1 提案手法におけるリスク分析手順

本提案手法におけるリスク分析の手順の詳細について説明する.

3.1.1　資産の識別・評価

資産の業務における重要度により価値を５段階に分類する．さらに，資産にとって重要なセキュリティの項目を機密性，完全性，可用性，責任追跡性，真正性，信頼性の６項目から選択する.

3.1.2　脆弱性の識別・評価

資産に対応する脆弱性を選択し，悪用の頻度，脆弱性が悪用された際に発生する被害により識別する．悪用の頻度は，４段階に分類する．また，脆弱性の識別の際は，JP Vendor Status Notes[2]などの公開されている脆弱性情報を利用する.

3.1.3　脅威の識別・評価

本稿では，本研究室のラミレスが提案する脅威モデルを基に，以下の５項目を用いて脅威を識別・評価する[3].

1）Who

脅威となる人物が誰であるかを，2 つのパラメータから識別する．一つ目には，脅威エージェントが人間か非人間かのどちらかであるか識別する．2 つ目には，認証されているか，されていないかによって識別する.

2）Why

攻撃者の目的を 2 つのパラメータから識別する．1 つ目は，脅威が発生した原因である．本稿では，偶発的，故意，敵意を持った故意の 3 つに分類する．２つ目には，攻撃者の目的である．本稿では，盗難，破壊，侵入，成りすましの 4 つに分類する.

3）Where

攻撃者がどこから攻撃を行なうかを識別する．攻撃はリモートもしくはローカルから行なわれるものとする.

4）When

脅威の発生する時間を識別する．本稿では，組織の業務時間内，業務時間外の 2 つに分類するものとする.

この「Who」，「Why」，「Where」，「When」の各項目から，脅威の特徴を選択することで，脅威の識別をする．図 1 のように 6 個のパラメータを組み合わせることで脅威を識別する.

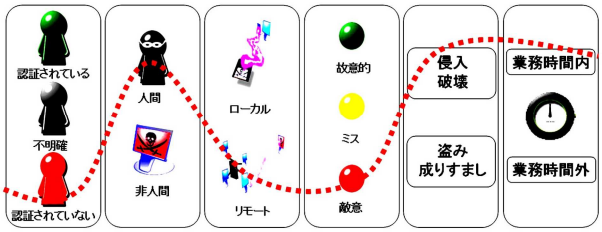

図 1　脅威の分類のイメージ

English Title. Study on Dynamic Risk Analysis corresponding to Threat Variation

Hideaki Kawanishi[†], Ramirez Caceres Guillermo Horacio[‡],Yoshimi Teshigawara[‡]

[†]Faculty of Engineering,Soka University

[‡]Graduate School of Engineering, Soka University

5） What

脅威が資産の何に影響を及ぼすかの評価をする．資産の機密性，完全性，可用性，責任追跡性，真正性，信頼性に対する影響度から脅威の大きさの評価を行う．分類された脅威を，大きさと発生確率から 5 段階で評価する．情報セキュリティポリシーに関するガイドライン[4]を基に，セキュリティ 6 項目は 5 段階，脅威の発生確率は 5 段階に分けるものとする．

3.1.4 リスク評価

リスク評価では，資産価値・脆弱性・脅威の評価の値を基に，マトリクスによりリスクの値を算出する． 表 1にマトリクスの例を示す．本稿では，リスク値は 14 段階となる．また，各評価の度合いを追加することで，列及び行を追加することが出来る．そのため，マトリクスのサイズは組織の必要性に応じて調整することが出来る．

表 1 リスク評価マトリクスの例[1]

脅威レベル		低			中			高		
脆弱性レベル		低	中	高	低	中	高	低	中	高
資産価値	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

3.2 脅威分析

組織の環境は，時間の変化とともに常に変化するものである．それに伴い，脅威が資産に与える影響も変化する．例えば，システム管理者の帰宅による被害の発見・回復の遅れである．表 2に環境の変化に伴う脅威の変化の例を示す．

表 2 環境の変化に伴う脅威の変化

環境の変化	脅威の変化
管理者の在･不在	被害の発見･修復までの期間
使用者の健康状態	ミスの発生確率
起動デバイス数	被害の発生確率
業務人数の変化	ローカルからの攻撃の発生確率

そこで，本提案手法では，脅威の分類項目である「When」の変化とともに脅威の大きさを変化させることで，動的なリスク分析を行なう．

3.3 提案手法の具体例

3.3.1 提案手法を用いた分析

提案手法を用いて，資産として「顧客情報」，脆弱性として「パスワードの強度が弱い」，脅威として「業務時間内のローカルからの第三者によるシステムへの不正アクセス」が存在する場合の分析の手順を示す．

1） 「顧客情報」の保護は，企業にとり重要であるため，資産価値は「5」となる．

2） 「パスワードの強度が弱い」は，攻撃の手法や手順が明らかになっているため，悪用される可能性が高い．悪用の頻度は，「4」となる．

3） 「業務時間内のローカルからの第三者によるシステムへの不正アクセス」を本手法で利用する脅威モデルにより分類すると，「非認証」，「人間」，「ローカル」，「敵意を持った」，「侵入」，「業務時間内」となる．この場合の発生確率は「3」，セキュリティ項目への影響の大きさは表 3のようになる．

表 3 セキュリティ項目への影響

	機密性	完全性	可用性	責任追跡性	真正性	信頼性
影響度	5	3	1	5	2	4

この値を基に，脅威の評価をする．この場合は，「2」となる．

4） 資産・脆弱性・脅威の値からマトリクスを用いてリスク値を算出する．この場合のリスク値は「9」になる．

3.3.2 時間を変化させた場合

次に，3.3.1と同じ条件で「when」のみを「業務時間外」に変更した場合を考える．この場合は，環境の変化として，「管理者の不在」，「業務中の人数の減少」がある．それにより，脅威の変化が起こり，「可用性」への影響度が「3」に，発生確率が「4」に変化する．それに伴い，脅威の評価が「3」となる．

変化した脅威の評価値を利用して，リスク値をマトリクスにより算出すると「10」となる．

4. 提案手法の利点

提案手法の利点として，環境の変化に対応した分析を行なうことが出来る．それにより，システムを運用していく上でのリスクの変化を把握でき，組織の環境の変化に即したセキュリティ対策の導入・改善を行なうことができる．

5. まとめと今後の課題

本稿では，組織の環境の変化による，脅威が資産に及ぼす影響の変化を考慮に入れた，動的なリスク分析の手法を提案した．今後は，資産・脆弱性の変化についても検討を行ない，本提案手法の実現方式の検討を行なう．

参考文献

[1] ISO/IEC TR 13335-1~5, Information technology - Guidelines for the management of IT Security

[2] JP Vendor Status Notes ：http://jvn.jp/

[3] ラミレス・カセレス・ギジェルモ・オラシオ，勅使河原可海：”セキュリティターゲットを作成するための国際標準に基づいた脅威モデルの検討”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）シンポジウム論文集，pp.189-192，2005.10

[4] 情報セキュリティポリシーに関するガイドライン：情報セキュリティ対策推進会議 2000.7