Vol.2021-CSEC-94 No.18
Vol.2021-SPT-43 No.18
2021/7/19

セキュリティインシデント対応の組織およびプロセスのシミュレーションによる検討手法の提案と評価

粕淵卓[1,2]　稗方和夫[2]

概要：サイバー攻撃が高度化・複雑化する中で，的確なセキュリティインシデント対応が求められている．本研究は，インシデント対応の所要時間を短縮できるプロセスや対応体制をシミュレーションにより検討し，その結果で得られた有効なインシデント対応プロセスを提案，評価することを目的とする．
シミュレーションでは，インシデント対応のタスクおよびその依存関係・要員を離散イベントとしてモデル化し，不確実性をタスクの所要時間の変動と仮定した．開発したシミュレータは，インシデントの検知から対応までのプロセスおよび所要時間を出力する．ケーススタディとして一般的なインシデント対応プロセスを対象に評価を行い，リソースやプロセス改善によりインシデント対応に要する時間を削減できることが得られた.また，シミュレータによるプロセスや対応体制の検討の有効性およびシミュレーションモデルの有効性が確認できた．今後実務への適用を検討する．

キーワード：情報セキュリティ，インシデント対応，意思決定

Propose and evaluate the methods for considering how organizations and processes should be in the case of security incidents by using simulation

TAKASHI KASUBUCHI[1,2]　KAZUO HIEKATA[2]

1. 緒言

1.1 背景と目的

サイバー攻撃は年々増加し，最近では AI を使ったもの，クラウドやテレワークを狙ったものなど，攻撃が複雑化，多様化している[1][2]．セキュリティ対策における重要な課題の一つが，インシデント対応である．過去には，不正な通信の検知をしたにもかかわらず，対策までに数日から数週間の時間がかかったことから，大規模な情報漏洩につながったケースが存在した．

多くの企業で，CSIRT(Computer Security Incident Response Team）と呼ばれるセキュリティインシデント対応の専門チームが準備されるようになった．しかし，専門チームを組んだとしても，インシデント発生時の意思決定は非常に難しい[3]．確認すべきログは大量であり，なおかつ攻撃者が巧みであるため，明確な痕跡が残さない場合もある．また，フォレンジックなどの本格的な解析をするには専門的な能力が求められる．なおかつ，多くの企業では，他の業務も実施しながらインシデント対応をしなければいけない．

本論文は，インシデントの検知から対応までのプロセスの所要時間を見積もるシミュレーションモデルを開発し，その結果で得られた有効なインシデント対応プロセスを提案，評価することを目的とする．

1.2 関連研究

インシデント発生時の対応手順に関しては，NIST の論文[3][4]に整理されている．また，セキュリティインシデントレスポンスチームの有効性として，「組織」や「個人」などに求められることを明らかにした研究[5]もある．Theodore Reed ら[6]は，セキュリティインシデント対応チームのワークフローと脅威特性のシミュレーションを行った．これらの研究から人材の重要性と，専門知識の習得や解析のためのソフトウェアツールの習熟の必要性が指摘されている．

1 西日本電信電話株式会社
NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION, Osaka 530-0011, Japan
2 東京大学大学院 新領域創成科学研究科
Graduate School of Frontier Sciences, The University of Tokyo, Chiba 277-8563, Japan

一方で，日本の多くの企業では専門的な人材を確保できないという現実があり，予算や人員の制約がある中でのシミュレーションによる研究は進んでいない．また、整理されているタスクは、連絡先の電話番号を調べたり、報告書を書くなどの実作業レベルまでは踏み込まれていない．

参考ではあるが，セキュリティインシデント対応の難しさは，救急医療の現場にも似ている．事前予測不可能なタイミングで急患が訪れ，短時間で対応する必要がある．Parameshwara らは救急外来における臨床プロセスのモデルやシミュレーションモデルを開発した[7]．一連のモデリングテンプレート（目標･演算子･メソッド･選択ルール）を使用することで、救急現場のタスク処理をシミュレーションした．

2. セキュリティインシデント対応プロセスの分析

2.1 インシデント対応プロセス分析の概要

インシデントが発生した際に，即座に対応できた企業もあれば，対応の遅れにより，情報漏洩が発生してしまった企業もある．対応の遅れによる事故が発生しないようにするために，まずはインシデント対応プロセスを分析する．

具体的には，インシデントの定義やインシデントにかかわる利害関係者の整理から始め，利害関係者がインシデント対応に何を望んでいるのかまで整理する．

次節以降で分析する内容を整理したものが表 1 である．

表 1　インシデント対応プロセスの分析内容

節	内容
2.2	セキュリティインシデントの定義
2.3	インシデント対応にかかわるステークホルダーの整理
2.4	インシデント対応プロセスの整理
2.5	インシデント発生時のシーケンス図
2.6	インシデント対応プロセスの困難性
2.7	ステークホルダーの要求分析

2.2 セキュリティインシデントとは

セキュリティインシデントとは，情報漏洩などのセキュリティに関する事件のことである．また，実際に情報漏洩が起きたかどうかにかかわらず，「疑わしい」段階もセキュリティインシデントに含まれる．

インシデントには，外部の攻撃者によるものもあれば，内部の犯罪者によるものもある．また，紛失や設定ミスなどのヒューマンエラーに起因するもある．

2.3 インシデント対応にかかわるステークホルダーの整理

ステークホルダーとは，利害関係者のことである．今回はインシデント発生時の対応および意思決定に関して，直接または間接的に利害のある人または組織を明らかにする．

表 2 に，インシデント対応プロセスにおける主なステークホルダーを整理する．

表 2　主なステークホルダーの一覧

id	ステークホルダー	説明
1	経営層	コストおよびリスク管理を経営の視点で考える．さらに，経営の観点から収益確保も重要である．
2	営業部門	サービスを顧客に販売する部門．顧客を獲得すること，サービスを提供してすることがミッションである．顧客からの問い合わせやクレームなども直接受ける．
3	CSIRT	セキュリティインシデントが発生したときに対応する専門チーム
4	システム主管	企業にはいくつものシステムが存在し，そのシステムを設計，維持，運用している組織．本論文では CSIRT と統一組織として進める．
5	広報部門	各種状況について社外に広く発信する．この発信方法の良し悪しで，企業イメージおよび経営に大きなインパクトを与える可能性がある．
6	SOC(Security Operation Center)	システムの監視部門．CSIRT と同一組織の場合もあれば，外部にアウトソーシングする場合もある．
7	外部ベンダ	システム主管からの要求に基づき，システムを設計（セキュリティ対策も含む）し，構築する．実際の攻撃が起こった場合に，解析も行う．また，解析を専門に行う会社もある．
8	顧客	サービスを受けている顧客
9	政府などの公的機関	NISC，JP/CERT や企業の監督省庁，IPA など．日本のセキュリティ対策を推進するだけでなく，企業に対して業務改善命令を出すこともある．
10	一般の人，マスコミ	顧客に限らず，一般の人．彼らの評判，口コミが企業のイメージを著しく変化させる場合がある．

セキュリティインシデントが発生すると，この中の，1～7 が連携してインシデント対応を行う．特に，CSIRT が対応の中心となり，最終意思決定は経営層が行うことが多い．

2.4 インシデント対応プロセスの概要

NIST の資料[3]では，インシデント対応プロセスの主なフェーズには，1)準備，2)検知と分析，3)封じ込め/根絶/復旧，4)事件後の対応があると記載されている（図 1）．

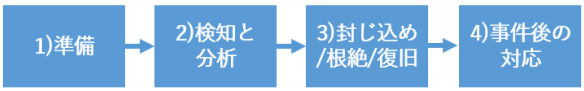

図 1　インシデント対応プロセス([3]を参考に作成)

この中で 2)と 3)は早急な対応が求められ，この対応が遅れると，情報漏洩事故につながる可能性がある．特に 2)の「分析」では、攻撃の状況および，システムの状況（防御ができているのか，情報漏洩は発生していないかなど）を正確に分析する必要があり，専門知識も求められる難しい工程である．

2.5 インシデント対応発生時のシーケンス図

先のインシデント対応プロセスにおいて，特に緊急な対応が求められる 2)と 3)に関して，インシデント発生時のシーケンス図を図 2 に示す．

この図にあるように，コンピュータセキュリティの事故対応チームである CSIRT は，同時に複数のことを複数の部署と連携して実施する作業がある．さらに，それらをほぼ

同時に．かつ短時間で実施することが求められる．

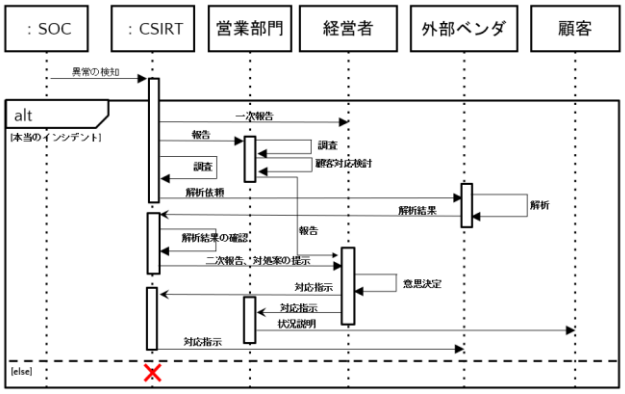

図 2　インシデント対応時のシーケンス図

2.6 インシデント対応プロセスの困難性

セキュリティインシデント対応の意思決定が簡単ではない理由を，以下に整理する．

(1)一刻を争う緊急性（短時間での対処が必要）

救急医療の現場の状況と同じで，事前に予測不可能な攻撃,インシデントが突然やってくる．もちろん，至急かつ短時間での対応が求められる．また，通常のオペレーションのために準備されたコミュニケーション方法などは，十分ではない場合が多い．

(2)調査の困難性

「故障」は，故障したことが明確な場合があることが多い．一方，「インシデント」は，本当に攻撃されたかどうかが判断できない，という場合がある．

また，事実確認のためにログを調査するが，ログは大量に存在する．さらに，攻撃者は巧妙で，攻撃の痕跡を残さないように攻撃する（または，自らログを消去する）こともある．

(3)体制の不十分さ（専門員が不在）

攻撃されたかやどれだけの影響範囲なのかなどについては，専門家による分析が必要である．O’Hagan は，不確実性の下での意思決定に関する 3 つの方法を述べているが，すべての方法において，多くの特に専門家の時間を投入する必要があるとしている[8]．しかし，多くの企業では，高度なスキルを持った人材が不足している[9]．

さらに，Frey S.Rashid らの研究[10]では，セキュリティの専門家が対応した方が必ずしも最善とは限らないとある．俯瞰的に見るなどのバランスも必要であり，インシデント対応に十分に対応できる組織を作る難しさがある．

本論文では，これら 3 つの困難性がある中で，短時間かつ的確なインシデント対応ができるためのプロセスや体制を検討する．

2.7 要求分析

最後に，ステークホルダーの要求を分析する．その理由は，ステークホルダーごとに望む要求事項が異なるからである．要求事項が異なれば，対応の内容も変わる．

今回は，インシデント対応の最終意思決定をする経営層と，組織内で経営層による統制が可能な組織である CSIRT と営業部門に着目する．

以下が要求分析の結果である．要求は,「機能要求」と「非機能要求」に区分した．機能要求は，無くてはならない要件である．非機能要求は，より望ましい状態にするための要求であり，可用性，性能要件，保守性などが該当する．

表 3　重要ステークホルダーの要求分析

対象	機能要件			非機能要件（例）
	対象	属性	望ましい変更	
経営層	機密情報，顧客情報	経営に影響するセキュリティ事故発生率	下げる	網羅性と効率性（軽微な攻撃も含める、コストに対して大きな効果を得る）
	提供サービス	サービスの継続性	高める	セキュリティ事故による影響度を小さく
CSIRT	システムや機密情報，顧客情報	攻撃に対する状態	攻撃の範囲と影響度を計測・推定可能にする	正確性（状況を完璧に理解する）
	セキュリティ対策の機器や設定	セキュリティ対策の状態	向上させる	網羅性（小さな攻撃も完全に封じ込める）
営業部門	提供サービス	サービスの継続性	（代替え手段も含め）高める	効果性（最良の状態でサービス提供）
	インシデントやサービス状況	状況の説明性	（状況が説明できるように）高める	応答性、正確性、詳細度（素早く，詳細な説明ができる）
	インシデント対応プロセス	機動性・柔軟性	高める	コスト効率

2.8 まとめ

要求分析結果から，CSIRT と営業部門では，要求が異なることがわかる．たとえば， CSIRT は「セキュリティ対策の状態を高める」という要求を持ち，営業部門では「サービスの継続性を高める」という要求を持つ．攻撃を防ぐには，調査や対策のためにシステムを止めたりすることも求められる．両者はトレードオフの関係にあり，インシデント対応の意思決定に遅れが出る場合がある．

すると，意思決定までの時間をかければかけるほどリスクは高まる．そのイメージを図 3 に示す．意思決定までの時間が t2，t3 と遅れるほどに情報漏洩リスクは飛躍的に上がる．しかし，誤検知の可能性もあり，その場合はリスクではない．逆に，早期の意思決定の判断を下す場合は，過剰にシステム停止などをする可能性もあり，サービス提供へのインパクトも大きくなる．攻撃であるかを的確に見極め，なおかつ早期の意思決定が必要である．

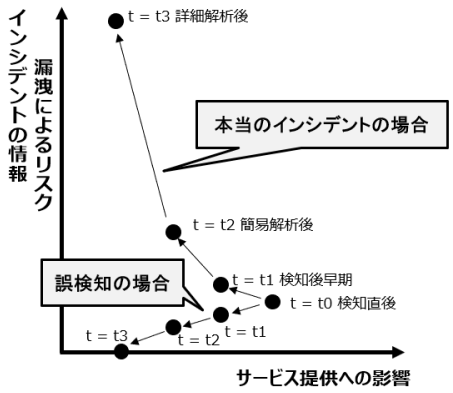

図 3　インシデント疑い検知時点から対応までの経過時間と情報漏洩リスクの変化

次から述べるシミュレーションでは，人数や作業工程を変化させることで，インシデント対応までの時間短縮について検討する．

3. シミュレーションモデル

3.1 シミュレーションモデル

シミュレーションとは，あるプロセスにおける時間経過を伴う操作を，実物を用いずに模擬することである[11].

シミュレーションには，大きく，離散型シミュレーション，連続型シミュレーション，統計的シミュレーション（モンテカルロ）の 3 つがある．

表 4　シミュレーションの種類

	離散型シミュレーション（離散事象型）	連続型シミュレーション（System Dynamics 含む）	統計的シミュレーション（モンテカルロ）
状態変化	動的	動的	静的
モデル	待ち行列型	微分方程式 差分方程式	統計モデル
目的	待ちや混雑が発生する現象を模擬する	微分方程式の数値解を得る	確率的なメカニズムをもつシステムの性質を乱数を用いて調べる

3.2 離散イベントシミュレーション

本論文では，離散イベントシミュレーションを利用して，人数や作業工程を変更によるインシデント対応までの時間短縮を検討する．

インシデント対応においては，複数の検討項目を考慮する必要があり，工程が変化することでクリティカルパスが動的に変化する．今回は，離散イベントシミュレーションを活用して論理的に適切と思われるインシデント対応のプロセスを評価する．本論文で提案するシミュレーションモデルの主な特徴を表 5 に示す．

表 5　利用する離散イベントシミュレーションの主な特徴

項目	内容
利用目的	インシデント対応における複数の検討項目をモデル化し，検討項目の変更に対する総時間などのパフォーマンス指標への影響を推定し，意思決定を支援する
状態変化	イベントの発生により，インシデント対応プロセスの各タスクの状態が動的に変化する

今回は，[12]で開発したソフトウエア開発プロジェクトのプロセスシミュレーションを活用し，改善した．具体的には，インシデント対応のタスクおよびその依存関係・要員，タスクの所要時間を離散イベントとしてモデル化した．このシミュレータは，インシデントの検知から対応までのプロセスおよび所要時間を出力する．シミュレータの概要を図 4 に示す．

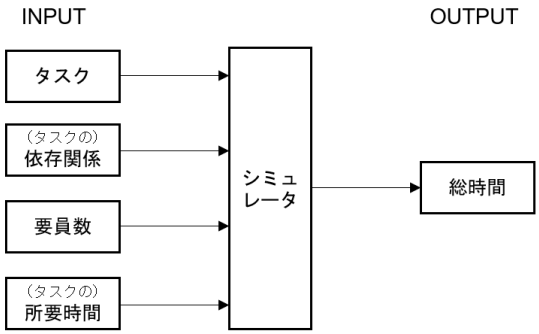

図 4　シミュレータ概要

3.3 プロセスのモデル化

(1)タスクリスト

シーケンス図を元に，インシデント発生時のタスクリストを表 6 に示す [13][14]. インシデントは重要な被疑があると判断され，解析が必要となり，対応策の実施するようになった場合を想定している．各タスクの所要時間は、連絡先を調べたり，連絡がつくまでの時間なども含め，実業務に即した工程で想定した．

表 6　タスクリスト

id	タスク	担当	所要時間	先行タスク	備考
A	異常の検知	SOC	0	-	監視機器からのアラート，社内外からの通報など
B	CSIRT での状況確認	CSIRT	1	A	内容確認
C	エスカレーション（準備含む）	CSIRT	1	B	誰に連絡するかを調べる時間，実際に連絡がつくまでの時間，報告文書の作成時間も含む
D	外部の構築ベンダへの解析依頼	CSIRT	2	B	依頼先を確認する時間，依頼文を作成する時間，依頼先と連絡がつくまでの時間なども含む
E	（自社で）解析	CSIRT	5	B	CSIRT のメンバーが自ら解析し，状況を確認する

F	営業部門での状況確認	営業部門	1	C	顧客への影響範囲などを正確に確認する
G	対外対応検討	営業部門	1	F	顧客向けの対応の検討（または検討準備）
H	詳細解析	外部ベンダ	6	D	専門員が解析をする．精度はかなり高い．
I	エスカレーション，指示受領	CSIRT	1	E	経営層へのエスカレーション，指示受領
J	解析結果の確認	CSIRT	2	D,H	外部ベンダの解析結果を確認．報告が送信されてから受領するまでの時間等を含む
K	報告，指示受領	営業部門	1	G	経営層への報告（エスカレーション），指示受領
L	対応策の協議	営業部門,CSIRT	2	E,I,J,K,G	対応策を協議する時間．受け取った内容を確認する時間なども含む
M	報告まとめ，報告準備，報告	CSIRT	2	L	経営層が意思決定できるための資料を作成する．経営層とのスケジューリング，報告などの時間を含む
N	経営層による意思決定	経営層	1	M,I	各種の情報をもとに，対処方法を決定
O	対応策実施の準備	CSIRT	4	E,J,N	対応策の検討，手順の確認，スケジューリング，実施日までの待ち時間も存在する
P	対応策の実施	CSIRT，営業部門，外部ベンダ	-	O	夜間や週末などに実施し，確認作業，報告までを行う．確認の後，問題がなければクローズ．（作業時間にバラツキが大きすぎるので，今回の検討外）
	Total		37		

(2)PERT

上記のタスクリストを PERT で表したものが図 5 であり，赤字が Critical Path である．

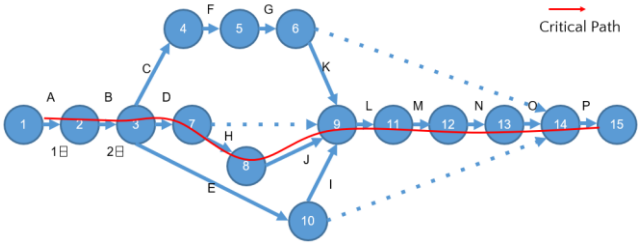

図 5　PERT

4. ケーススタディ

4.1 ケーススタディの目的と概要

(1)ケーススタディの目的

ここでは，要員数やプロセスを変えながら，開発したシミュレータを用いて，インシデント対応の所要時間を計測する．

セキュリティインシデント対応は 2.6 で述べた困難性があり，対応に時間がかかる．しかし，早期の発見が求められるため，このケーススタディごとのシミュレーション結果を，最適なインシデント対応プロセスの解明に役立てる．

(2)検証するケース

シミュレーションで検証したのは，大きく 3 つのケースである．1 つ目が基準となるケース，2 つ目と 3 つ目は改善したケースで、リソースマネジメントによる改善，プロセスマネジメントによる改善，である．

❶基準となるケース

多くの企業でありがちな，営業部門の「サービスの継続性」の要求が強く反映された条件とする．具体的には，インシデントの状況が詳細に明らかになるまでは、システムを可能な限り停止しない（または影響を与えない）という条件である．

❷ リソースマネジメントによる改善

短期にインシデント対応をするために，人員を増加する．

❸プロセスマネジメントによる改善

インシデント対応のプロセスを抜本的に変える．具体的には、営業部門が「効果性（最良の状態でサービス提供）」という非機能要件を追求しすぎないことである．本当のインシデントか否かの調査が十分ではない段階であっても，サービス停止などの影響がでる対策を取ることを許容する．それ以外には、事前に準備できることを済ませておくことや、防御策を単純化すること、訓練の実施などである．

以下の表 7 は，上記 3 つのケースを整理したものである．表の右側には 2.6 で述べた困難性への対処方法をまとめた．

表 7　シミュレーションのケーススタディ

Case	概要	内容	困難性への対応		
			緊急	調査	体制
❶	基準	作業員 1 名で実施	未対応	外部ベンダに依存	
❷	リソースマネジメント	作業員の増員	増員		
❸	プロセスマネジメント	プロセスの改革	（・増員） ・事前準備 ・防御策の単純化，訓練	工程改革	

(3)シミュレーション条件

インシデント対応のプロセスや対応時間は，事故の規模やシステムおよび組織によって大きく異なる．そこで，今回のシミュレーションに際しては，以下のモデル環境として想定した．

表 8　インシデント対応のモデル環境

項目	条件
対象となるシステムの状況（端末，サーバの数，複雑さ）	システムは Web サーバとアプリケーションサーバ，社内にある顧客データベースを含む DB サーバが主なサーバとし，外部からの攻撃が発生したことを想定．

調査するログの内容	アラート情報をもとに，それぞれのサーバのログを調査する．攻撃がされたかがわからない場合や，危険度が高い場合は，高度な技術が求められるフォレンジック解析が求められる．また，ログは複数サーバに散在し，10 ファイル，10 万件以上があると想定．
組織の大きさ	エスカレーション（または情報共有）すべき組織は，主に情報システム部内と，3 営業部門と経営層，広報室，拠点は国内のみ．

4.2 シミュレーション結果

(1)Case❶：基準となるケース

基準となるシミュレーションとして，通常のスキルを持つ作業員が 1 名かつ，先に示した標準的なタスクストで実施する．1 名で実施するというのは，CSIRT の体制としては不十分である．しかし現実的には，多くの企業では本来業務が多忙であり，よくある事例と言える．

攻撃の状況を完璧に理解するには詳細な解析が必要であり，解析作業を外部ベンダに委託する．同時に，外部に委託することで，2.6 で述べた「調査の困難性」や「体制の不十分さ」を補う．

表 9　シミュレーションの基本情報

項目	条件
作業員	1 名
プロセス	表 5 のタスクリストに従う

図 6 がシミュレーション結果である．インシデント対応にかかる総時間は，19 時間である．

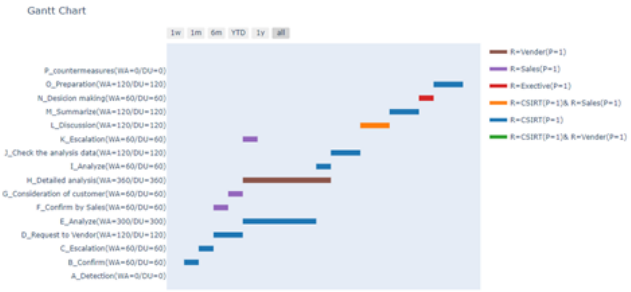

図 6　シミュレーション結果 Case❶

(2)Case❷：リソースマネジメント

2.6 で述べた短時間での対処を達成するために，作業員を 2 名に増員する．条件は表 10 のとおりである．

表 10　シミュレーションの条件

項目	条件
作業員	2 名
プロセス	表 5 のタスクリストに従う

図 7 がシミュレーション結果である．青色の CSIRT で実施するタスクの時間が短縮されることで，インシデント対応にかかる総時間は 13.5 時間である．5.5 時間の大幅な短縮が図れた．

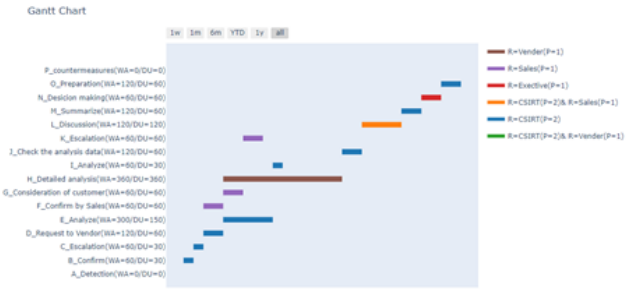

図 7　シミュレーション結果 Case❷

表 11 は，作業員をさらに増やしてシミュレーションを実施した結果である．作業員を 3 人にするとさらに 1.5 時間の短縮，4 人だとさらに 0.7 時間の短縮が図れた．

表 11　人数を変化した場合の総時間の変化

作業員の数	総時間	削減時間
1 名	19	-
2 名	13.5	5.5
3 名	12	1.5
4 名	11.3	0.7

(3)Case❸-1：プロセスマネジメント

ここからは，プロセスの改善による時間短縮を図る．4.1(2)❸で述べたように，「状況を完璧に理解する」ことを目指さないのであれば，「外部」のベンダによる詳細な解析は必須ではない．加えて，2.6 で述べた困難性への負荷も減る．そうすれば，インシデント対応において，攻撃の封じ込め（通信の遮断，システム停止などの応急処置）までを「社内」で完結することができ，作業時間短縮が図れる．求められる詳細な解析に関しては，暫定対処をした後に，外部ベンダに時間をかけて依頼すればよい．また、外部ベンダによる解析作業は、場合によっては長時間に及ぶ可能性がある．作業時間のバラツキを減らす効果も期待できる．

この場合における，インシデント対応の主な変更点を表 12 に整理する．

表 12　インシデント対応の主な変更

項目	変更前	変更後
外部ベンダへの依頼	必要	不要
インシデント対応の判断基準	詳細な分析結果を経て判断	判断しやすい基準に変更．たとえば，個人情報があるか，重要なサーバへのアクセスか，管理者権限での操作がされているか，など
求められる対応	完全な復旧	封じ込めまで
サービス提供	本来のシステムで提供	代替えサービスも選択肢

この変更をもとに，タスクリストおよび所要時間を見直して，表 13 の条件でシミュレーションを実施する．

表 13　シミュレーションの条件

項目	条件
作業員	2 名
プロセス	外部ベンダを活用せず，社内で完結．それに伴い，表 5 のタスクリストを変更

図 8 がシミュレーション結果である．インシデント対応

にかかる総時間は 9.3 時間で，4.2 時間の短縮が図れた．

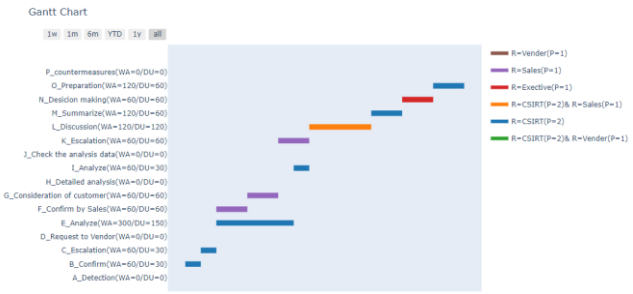

図 8　シミュレーション結果 Case❸-1

(4)Case❸-2：事前準備の実施

次のプロセス改善は，事前にできることを準備し，作業工程そのものを短縮する方法である．インシデント対応は一刻を争う事態である．にもかかわらず，現実的には，単純作業に無駄に時間を費やすことが多い．たとえば，幹部の携帯番号がわからずに誰かに確認したり，エスカレーションをするメールをゼロから書いたり，やるべき作業その場で考えたり，などである．

ここでは，表 5 のタスクリストにおいて，単純作業が中心の 6 つのタスクを抽出した．さらに事前準備によって以下の時間削減ができると想定し，表 14 の変更に基づいてシミュレーションを行った．

表 14　事前準備による所要時間の変更

id	タスク	担当	変更前	変更後
B	CSIRT での状況確認	CSIRT	1	2/3
C	エスカレーション（準備含む）	CSIRT	1	0.5
G	対外対応検討	営業部門	1	0.5
K	報告，指示受領	営業部門	1	0.5
L	対応策の協議	営業部門,CSIRT	2	1
M	報告まとめ，報告準備，報告	CSIRT	2	1

図 9 がシミュレーション結果である．インシデント対応にかかる総時間は 7.6 時間で，1.4 時間の短縮が図れた．

図 9　シミュレーション結果 Case❸-2

(5)Case❸-3：防御策の単純化，訓練の実施

次はタスクリストの中で，主に 2 時間以上の工程を改革すべく，防御策を単純化することを検討した．

防御策の検討や準備に時間がかかる理由は，攻撃は複雑であり，その攻撃に対処した方法を検討して対策をしようとするからである．しかし，単に攻撃の封じ込めという機能要件を目指すのであれば，IPS(Intrusion Prevention System)で該当通信を防御することや，システムを停止するなどの単純な対応策を取ることもできる．また，その対策を事前に手順化し，訓練まで実施しておけば，攻撃によって防御策をするに比べて格段に速く対応できる．また，意思決定の判断も速くなる．

ここで，表 5 のタスクリストにおいて，防御策を単純化し，訓練までも実施した場合で短縮できる 6 つのタスクを抽出した．さらに表 15 の時間削減ができると想定し，シミュレーションを行った．

表 15　事前準備による所要時間の変更

id	タスク	担当	変更前	変更後
E	（自社で）解析	CSIRT	5	2
L	対応策の協議	営業部門,CSIRT	2	0.5
M	報告まとめ，報告準備，報告	CSIRT	1	0.5
N	経営層による意思決定	経営層	1	0.5
O	対応策実施の準備	CSIRT	4→2	0.5

図 10 がシミュレーション結果である．インシデント対応にかかる総時間は 4.1 時間で，3.5 時間の大幅な時間短縮が図れた．

図 10　シミュレーション結果 Case❸-3

4.3　まとめ

シミュレーション結果を表 16 にまとめる．

表 16　シミュレーションのケーススタディ

Case	概要		総時間
❶	基準	作業員 1 名で実施	19
❷	リソースマネジメント	作業員 2 名で実施	13.5
		作業員 3 名で実施	12
		作業員 4 名で実施	11.3
❸	プロセスマネジメント	工程の抜本改革	9.3
		事前準備の実施	7.6
		防御策の単純化，訓練	4.1

シミュレーションの結果からは，インシデント対応の要件として，作業員の増員によるリソースマネジメントや、工程の改革によるプロセスマネジメントによって、インシデント対応の時間を削減することができた．特に、外部ベンダの利用を見送るという工程の抜本改革は、4.2 時間の大幅な短縮効果があった（作業員 2 名の条件で 13.5 時間⇒9.3 時間）．さらに、作業時間のバラツキ低減にも寄与できることが想定される．

5. 考察

(1) リソースマネジメント

人員を 1 名から 2 名に増員することで，インシデント対応の時間の短縮が図れた．しかし，仮に 3 人や 4 人とさらに増員しても，改善効果は少ないという結果がでた．また，人数が増えれば，メンバー間でコミュニケーション時間，作業調整時間なども必要である．実際のインシデント現場では，インシデント発生などの有事においては，闇雲に頭数だけをそろえようとする場合もある．しかし，このシミュレーション結果から，頭数だけ増やす対応というのは，改善効果がほとんど期待できない．

(2) プロセスマネジメント

インシデント対応は事前準備が非常に大事であり[3]，プロセス改善によって，大幅な時間の短縮が図れることを具体的な数字で算出できた．

(1)と(2)の結果から，インシデント対応の迅速化のために必要なリソースおよびプロセスの改善は以下である．

・2 名以上の体制でインシデント対応を実施する
・インシデント対応を外部ベンダに依存しない
・非機能要件を求めすぎない
・事前準備と社内体制およびルールの整備
・防御策の単純化，訓練の実施

(3) シミュレーションモデルの評価

インシデント対応時の対応プロセスに関して，プロセス改善によりどれくらいの時間が削減できるか，具体的な数字を算出することができた．また，先行論文では検討されていない，連絡先を探したり，報告文書を書いたりなどを含めた詳細な作業レベルの時間まで考慮することができた．

さらに，この結果を数社の CSIRT にインタビューをしたところ，内容の妥当性の裏付けが取れた.開発したシミュレータおよびそのモデル、およびその結果の精度が高いことが確認できた．

6. 結論

本研究では，インシデント対応のタスクおよびその依存関係・要員を離散イベントとしてモデル化し，インシデントの検知から対応までのプロセスおよび所要時間を出力するシミュレータを開発した．開発したシミュレータを活用し，最適なインシデント対応プロセスの解明に役立てるために，ケーススタディごとのシミュレーション結果を出力した．

その結果，機能要件に着目することや，外部ベンダに依存せず，事前準備などによってインシデント対応に要する時間を削減できることが得られた．また，本シミュレータおよび作成したモデルが有効であることから，実務への適用を検討する．

謝辞

本研究のシミュレーションモデル作成にあたり，東京大学工学部非常勤講師の笈田佳彰先生には多くの有益な助言をいただきました．ここに記して感謝の意を表します．

参考文献

[1] Mcafee 脅威レポート.(2021). https://www.mcafee.com/enterprise/ja-jp/lp/threats-reports/apr-2021.html
[2]FireEye,セキュリティ動向予測レポート.(2021). https://www.fireeye.jp/current-threats/annual-threat-report/cyber-security-predictions.html
[3]Computer Security Incident Handling Guide, Special Publication (NIST SP) - 800-61 Rev 2 (2012)
[4]NIST, Framework for Cyber-Physical Systems (2017)
[5]Van der Kleij R.Kleinhuis G.Young H. Frontiers in Psychology (2017) ,Computer security incident response team effectiveness
[6] Reed T.Abbott R. G.[...]Forsythe C (2014) Simulation of workflow and threat characteristics for cyber security incident response teams
[7]Parameshwara, N., Kim, J. H., Guo, W., & Pasupathy, K. S. (2016). Ngomsl simulation model in an emergency department. Proceedings - Winter Simulation Conference, 0, 1938–1949.
[8]O'Hagan, A. (2019). Expert Knowledge Elicitation: Subjective but Scientific. The American Statistician, 73(sup1), 69–81.
[9]総務省「我が国のサイバーセキュリティ人材の現状について」(2018), https://www.soumu.go.jp/main_content/000591470.pdf
[10]He, M., Devine, L., & Zhuang, J. (2018). Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. Risk Analysis, 38(2).
[11] J. Banks; J. Carson; B. Nelson; D. Nicol (2001). Discrete-Event System Simulation. Prentice Hall.
[12]Taiga Mitsuyuki, Kazuo Hiekata, Takuya Goto, Bryan Moser. Evaluation of Project Architecture in Software Development Mixing Waterfall and Agile by Using Process Simulation, Journal of Industrial Integration and Management: Innovation and Entrepreneurship, Vol.2, No.2, 1750007, 2017.
[13]Andrade R. O.Yoo S. G. (2019),Cognitive security: A comprehensive study of cognitive science in cybersecurity
[14]Van der Kleij R.Kleinhuis G.Young H.Frontiers in Psychology (2017).Computer security incident response team effectiveness: A needs assessment