Vol.2018-CSEC-83 No.3
2018/12/13

サイバーインシデントの損害発生モデルシミュレータによるサイバーリスク評価手法の提案

磯部義明[†1]　藤田淳也[†1]　上脇正[†1]　中畑昌也[†1]
末岡正嗣[†2]　藤井裕之[†2]　落合正人[†2]

概要：近年，サイバー攻撃の脅威は深刻化しており，その対象は工場・プラントなどの産業設備だけでなく，エネルギー，交通，金融といった社会を支える重要インフラにも拡がるなど，さまざまな分野でサイバーセキュリティ対応の重要性が増しています．一方，セキュリティインシデントの発生リスクや対策の投資対効果（ROSI）が不明瞭なため，事業責任者において，どこまでコストをかけて対策をとるべきかの判断が困難となっている．本報告では，これらの判断を支援するため，産業・重要インフラ分野において適切なセキュリティ投資判断を支援するため，セキュリティインシデントによる年間損害額とその発生確率（超過損害確率カーブ）にて定量化する方法を検討し，損害発生モデルシミュレータの開発および技術検証を行った結果について報告する．

キーワード：サイバーセキュリティ，セキュリティリスク分析，セキュリティ投資効果，サイバー保険

Proposal of Cyber Risk Assessment Method based on Loss Occurrence Simulator for Cyber Incident

YOSHIAKI ISOBE[†1]　JUNYA FUJITA[†1]　TADASHI KAMIWAKI[†1]
MASAYA NAKAHATA[†1]　MASATSUGU SUEOKA[†2]　HIROYUKI FUJII[†2]
MASATO OCHIAI[†2]

Abstract: In late years the menace of the cyber-attack worsens. The target spreads to not only the industrial facilities such as the factory, the plant but also critical infrastructure supporting energy, traffic, society such as the finance. Importance for cyber security response increases in various fields. On the other hand, the business decision is difficult such as “How much cost and should I take countermeasures?”, because the occurrence rate of security incident and the return of security (ROSI) are indistinct. In this report, we studied a method to quantify at the annual loss by the security incident and the probability of occurrence (Exceedance Probability Curve). and we developed the damage outbreak model simulator to support an appropriate security investment decision in the field of industrial critical infrastructure.

Keywords: Cyber Security, Security Risk Analysis, Business Risk Assessment, Return of Security Investment

1. はじめに

高い関心を集めた「Heartbleed」や「Shellshock」と呼ばれる脆弱性は，脆弱性情報を公開した直後から，同脆弱性を狙った攻撃が急増したため，迅速な対処が求められた[1-2]. 一方で，2015 年 6 月に発覚した年金事務所に対するサイバー攻撃による個人情報漏えい事件など，対処判断に時間が掛かり，適切な対処・対策が遅れ，その結果，被害拡大を招いた．こうした対処判断の遅れの原因の一つに，セキュリティ対策に対して経営者のリーダーシップが十分発揮されていないことが経産省が公開したガイドラインにおいて指摘されている[3]．本ガイドラインでは，企業の競争力に不可欠な IT 活用を進めていくうえで，システムの可用性や機密情報の事業戦略上の価値・役割を十分認識し，加えてサイバー攻撃によるビジネスリスクへの対処判断することは，経営者の役割であると指摘されている．

一方で，これら脆弱性情報などのセキュリティ情報は，専門家による技術文書であり，経営者が判断するための経営情報としては，ギャップがある．

そこで，本報告では，既報告の攻撃経路を考慮して各機器のリスクを攻撃到達性で評価する技術[4]によるビジネスリスク評価システム[5]を拡張し，経営層の判断を促すことを目的として，想定される年間被害額を超過する確率を示す超過確率曲線（EP カーブ）を算出することにより，セキュリティ投資効果を提示する，サイバーリスク評価手法を提案する．

2. 関連研究

2.1 ビジネス影響評価

1)　事業継続マネジメントシステム

†1 (株)日立製作所
Hitachi Ltd.
†2 SOMPO リスクマネジメント(株)
Sompo Risk Management Inc.

IT システムの障害等によるビジネス影響を評価する検討は，災害発生に対する事業継続マネジメントシステム（BCMS : Business Continuity Management System）において，進んでいる[6]．BCMS は 2012 年に ISO 22301 として要求条件が明確化されている．この条件に基づいた各社の事業継続に対する PDCA（Plan，Do，Check，Act）の取り組みが，第三者認証される．この中で，BIA（Business Impact Analysis）と RA（Risk Assessment）が計画（Plan）と管理（Check）のフェーズにて求められる．これら 2 つの分析により，以下の３つが明確とされる．

- ビジネスプロセスとその脆弱性
- ビジネスプロセスを支える経営資源とその脆弱性
- ビジネスプロセスを阻害・中断のリスク

しかし，これらの分析は，定期的に行われる PDCA の担当者や専門家に委ねられており，本報告で課題とした突発的な脆弱性公開によるサイバー脅威の増大に対して迅速に対応するには，適切に分析結果を更新する必要があり，課題があった．

2) 年間損害推定額：ALE（Annualized Loss Expectancy）

セキュリティ被害額算定指標として，1979 年に米国規格基準局から発行された FIPS PUB 65：リスク分析ガイドラインにおける ALE が有名である[7]．ALE はインシデント当たりの損害額（SLE : Single Loss Expectancy）と予測される年間発生回数（ARO : Annualized Rate of Occurrence）により，年間損害額を推定した指標である．この指標はセキュリティのみならず，災害や故障，ヒューマンエラーなどによるビジネスリスク指標として広く利用されている．

この ALE を利用した費用対効果を導出するアプローチが報告されている．中村らは，対策採用による脅威発生確率の低減をモデル化し，各対策案の効果を残存資産として定式化し残存資産を最大となる対策選択方法を提案している[8]．さらに，インシデント発生を抑制する事前対策とインシデント発生後に行うデジタルフォレンジック対策（事後対策）を分けてそれぞれの費用対効果を最適化する方式を提案している[9]．

3) Gordon & Loeb 経済モデル[10]

Gordon らはセキュリティ投資回収（ROSI : Return Of Security Investment）に関する理論的な枠組みを提案し，所与の潜在的な損失の下では，企業は必ずしも最も脆弱性の高い情報資産を保護する必要がないことを示した．本モデルは，松浦らにより，市町村の情報セキュリティ投資に関する統計データを利用して実証的に確認された[11]．さらに，モデルの拡張が提案され，被害額の 37%以上のセキュリティ投資は過剰であること示している[12]．これらは各企業のマクロなセキュリティ投資方針に大きな示唆を与えるものの，日々のサイバー脅威に対するセキュリティ対策に関する判断に利用することは困難である．

4) 攻撃経路を考慮したリスク評価に基づくビジネスリスク評価[4][5]

脆弱性のリスクを評価する標準として，CVSS（Common Vulnerability Scoring System）がある[13]．CVSS では，以下の三つの観点毎にいくつの評価指標で定められた評価値を統合し，セキュリティリスクを評価する．

- 基本評価基準（Base metrics）：脆弱性そのものの特性を評価する基準．ネットワークからの攻撃可能性などを評価
- 現状評価基準（Temporal metrics）：脆弱性の現在の深刻度を評価する基準．対策の有無や攻撃状況などを評価
- 環境評価基準（Environmental metrics）：該当製品の利用環境などを評価する基準．

環境評価において，システムの構成による到達可能性や影響範囲，システムへの秘匿性・完全性・可用性への要求度を明確化して，最終的なリスク値を明確にする．しかし，この標準化したリスク値を求めるためには，システム環境を適切に理解した上で，専門家と連携して評価する必要があった．また，この標準化した値は，本報告で提案する想定被害額などを算出するものではなく，経営者の判断を下すには十分ではない．

そこで，CVSS の環境評価に関し，自動収集したシステム構成情報からベイジアンネットワークによるリスク評価モデルを自動生成し，攻撃経路を考慮したセキュリティリスク評価システムを提案した[4]．本システムの概要を図に示す．

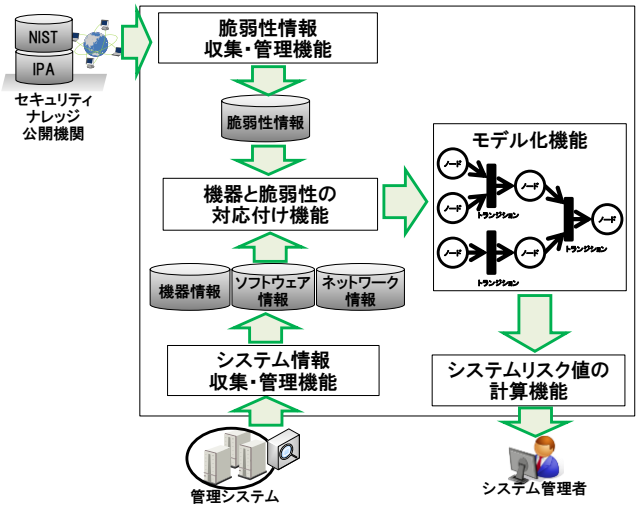

図 1 セキュリティリスク評価システムの全体構成[4]

この評価システムにより，脅威発生源から各機器への攻撃到達可能性をベイジアンネットワークにより算出することで，CVSS の環境評価の一部を自動化することができ，システム管理者による対処判断を支援することができる．

さらに，この評価システムと連携し，攻撃到達可能性に応じてビジネスリスクを評価・算出し，経営者のセキュリ

ティ対処の判断を支援するビジネスリスク評価システム（BRASS：Business Risk Analysis System on Cyber Security）を提案した．概要を図に示す．

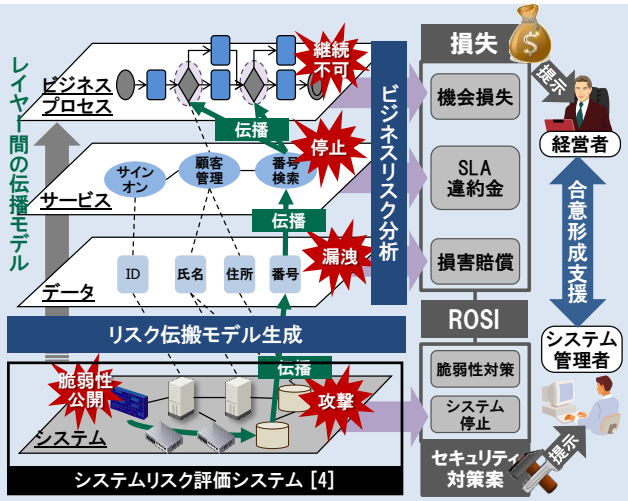

図 2 BRASS（Business Risk Analysis System on Cyber Security）の概要[5]

ビジネスプロセスを支えるシステムリソースのサイバーセキュリテイリスクを明確にした上で，ビジネスプロセス上のリスクをサイバー攻撃によるシステム停止等の損失額の期待値として算出する．この想定損失額に基づき，セキュリティ対策の効果（ROSI）を算出して経営者等に提示し，システム管理者他のステークホルダとの合意形成や対処判断を支援する．

2.2 損害保険のリスク査定

1) 統計による損害保険のリスク査定[14]

損害保険を適切に設計するためには，保険引き受け期間（1 年）の間に，どのくらいの大きさの損失がどのくらいの確率で起こるかを定量的に求める必要がある．火災や自動車事故を対象とした損害保険では，家屋種別や車種別の統計情報に基づいた分析により，保険対象となる財産の属性に応じて将来の災害や事故の発生確率を予測し，保険引き受けによる損害を予測してリスクを査定する．

2) 自然災害脅威（CAT）モデルによるリスク査定[15]

自然災害のリスクは，あまり頻繁には起こらないため，十分な統計量が得られない．このため，理論的な方法（リスク分析・評価）を組み込んだ自然災害による損害発生モデル（CAT ：CATastrophe モデル）を作成してリスク評価を行う．

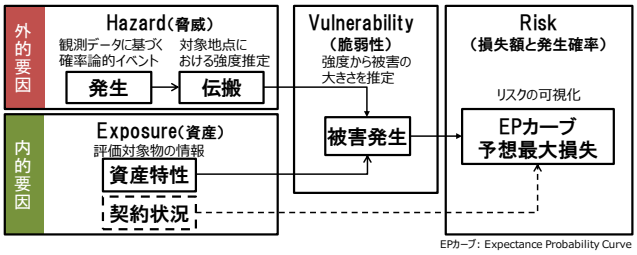

図 3 CAT モデルの構成モジュール

（1）Exposure のモデル化

Exposure では，資産を定義する．これらが入力データとなる．資産の属性情報なども明確にする．地震や台風などでは，建物の構造や建築方法などが相当する．

（2）Hazard のモデル化

Hazard では脅威発生をモデル化する．これらをモデル化したモジュールをハザードモジュールと呼ぶ場合もある．

まず，一般的には観測データに基づいて確率論的にイベントカタログを生成する．例えば，過去の地震の発生や台風の発生に関するデータに基づき，発生頻度やその属性（マグネチュード，発生地点など）の生成をモデル化する．

続いて，評価対象の地点におけるハザード強度を算定する．例えば，地震の場合は，発生地点と評価対象地点との間の地盤データによる地震の伝わり方などをモデル化し，評価対象地点の震度を算定する．台風の場合は，発生地点から台風のコースを季節ごとにモデル化し，評価対象地点での最大風速などを算定する．

（3）Vulnerability のモデル化

Vulnerability では，被害関数等を用いて被害を算定する．これらをモデル化したモジュールを脆弱性モジュールと呼ぶ場合もある．

具体的には，モデルの対象となる災害において，（1）と（2）の情報における被害発生関数を明確にし，被害額を算定する．例えば，地震の場合は，建物の構造（RC や木造など）と震度による被害額発生を統計情報に基づき，関数でフィッティングし，確率的な関数としてモデル化し，被害額を算定する．

（4）Risk のモデル化

Risk では，ハザードモジュールと脆弱性モジュールの計算結果を掛け合わせて各ハザードイベントの物理的な損害を計算し，保険契約条件などを考慮した保険金支払い額の総和を損失額として計算する．これらのモデルをファイナンシャルモジュールと呼ぶこともある．これらの分析モデルの結果，超過確率曲線（Exceedance Probability Curve: EP カーブ）と年平均損失（Annual Average Loss）を得る．これは，一年間の損失額とその一年でそれ以上の損失額が発生する確率（年超過確率）との関係で表現される．

サイバーにおけるリスク査定においても，システムの特性や属性に応じた統計情報が十分に揃っていないため，個

表 1 地震災害の CAT モデルとサイバーインシデントのアナロジー分析

モデル		アナロジー分析	
		地震災害	サイバーインシデント
Exposure モジュール	資産特性モデル	構造種別 用途種別 建築年数 階数，地域性	業種 用途 システム構成 セキュリティ対策状況
Hazard モジュール	発生モデル (イベントカタログ)	気象庁地震データに基づき震源タイプ等の発生モデルを構築	各ソフトウェアの脆弱性情報の発行頻度にて，攻撃発生をモデル化
	影響伝搬モデル	表層地盤マップ等による各地点の震度（加速度）予測モデルを構築	攻撃発生源からの各機器への侵入されやすさを日立侵入経路シミュレーション[4]によりモデル化
Vulnerability モジュール	被害発生モデル	資産の各種別と震度（加速度）による被害発生モデルを構築	各脆弱性情報の CVSS により侵入しやすさをモデル化．脆弱性公開からの経過日数により被害発生をモデル化
Risk モジュール	超過確率曲線 (EP カーブ)	イベントを確率論的に発生させた結果を統計的な確率曲線で算出	各機器の価値と上記の到達確率により乱数で攻撃成功を決定(被害確定)．繰り返して統計的な確率曲線を得る
	予想最大損失	同上の最大損失	同上の最大損失

別システムの発生確率を予測することが困難な状況である．このため，本報告では，CAT モデルに基づいて，Exposure，Hazard，Vulnerability，Risk の各モジュールのモデルを構築し被害発生を予測する方法を検討することとした．

3. 損害発生モデルシミュレータによるサイバーリスク評価手法の提案

3.1 アナロジー分析

地震災害の CAT モデルの各モジュールに基づき，サイバーインシデントの損害発生について，アナロジー分析をおこなった結果を表 1 に示す．

本分析を参考にサイバーインシデントの損害発生をモデル化し，超過確率曲線を算出するシミュレータによるリスク査定方法を提案する．

3.2 損害発生モデルシミュレータの概要

既報告[4]の侵入経路シミュレーションを行うシステムリスク評価システムのプログラムを活用した，損害発生シミュレータを次図に示す．

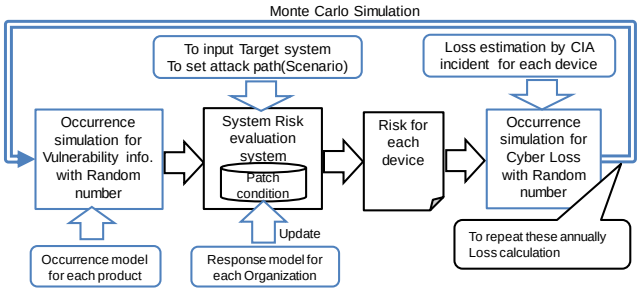

図 4 損害発生モデルシミュレータの概要

システムの脆弱性が発見される確率を NIST などの脆弱性情報[16]に基づいて，統計的な確率モデルで定義し，確率モデルに従って脆弱性情報を発生させるシミュレータと，システムの脆弱性状況に従って，損害発生をシミュレーションする損害発生シミュレータを開発した．

さらに，このシミュレーションをモンテカルロ・シミュレーションのように，繰り返し実行し，損害発生の結果を統計的にまとめ，損害の超過確率曲線を算出するスクリプトを開発した．

1) 脆弱性情報発生シミュレーション機能

プロダクト毎に脆弱性情報の発生頻度は年毎に次図のように異なる．これらの相違を確率分布でモデル化する．

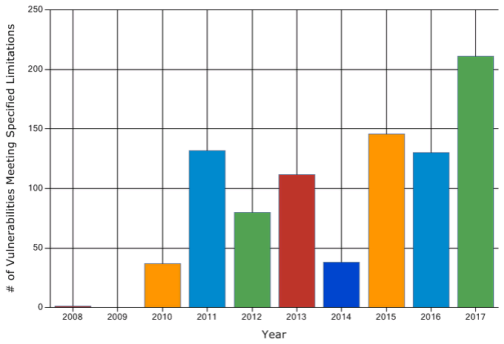

図 5 Microsoft Windows Server 2008 の脆弱性発生[16]

これらの発生の確率分布を製品ごとにモデル化するため，(a)ポアソン分布，(b)負の２項分布の２つの分布モデルでモデル化可能とした．統計的な分析により，年毎で分散が広く出る場合は，負の２項分布を採用し，製品ごとの脆弱性発生を確率分布モデルでモデル化した．

また，発生した脆弱性の特性である CVSS ベクトル値および CWE，Exploit コードの出現可能性についても，各製品や製品属性ごとに NVD の統計情報に基づいた確率分布により，特性を定義することとした．

これらの定義に基づいて，脆弱性情報発生シミュレーション機能を次図のように実装した．

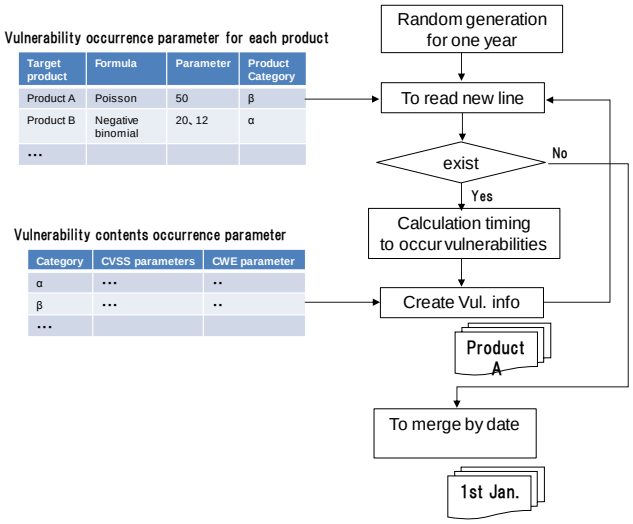

図 6　脆弱性情報の発生シミュレーションの処理フロー

2)　パッチ状況反映シミュレーション機能

既報告[4]の侵入経路シミュレーションによるリスク評価システムを活用し，評価対象システムの脆弱性リスクを評価するとともに，定期的なパッチ対策や，被害発生時の緊急対策をシミュレーションする機能を開発した．

3)　被害発生シミュレーション機能

脆弱性があっても被害が発生するわけでは無いので，脆弱性を利用した攻撃による被害発生についてもモデル化を行った．

ベライゾン[17]より，1 年間に攻撃された全脆弱性情報について，脆弱性が公開されてから攻撃が発生するまでの期間について，正規化された累積頻度分布が公開されている．本情報によると，約 50%の脆弱性情報が最初の 1 か月の間に攻撃されおり，以降，11 か月かけて徐々に 100%に漸近していく．

4)　超過確率曲線算出機能

被害発生シミュレーションを 1 年間実施し，年間累積被害額を算出し，この 1 年分のシミュレーションを繰り返し，年間累積被害額のバラツキの統計を取り，超過損害額の確率曲線を得ることで算出する．

4.　評価実験

1)　実験シナリオ

対象システムの概要を図 7 に示す．対象システムは仮想的に自動車生産工場を想定しており，また，攻撃シナリオとして，インターネット経由した攻撃と USB からマルウェア感染した場合の被害波及をシミュレーションした．

表 2 に想定システムの各機器にインストールされている想定ソフトウェアを示す．

2)　実験パラメータ

本実験シナリオを構成するソフトウェアの脆弱性発生のタイミングパラメータを表 3 に示す．

また，損害発生パラメータは以下とした．

- Exploitable な脆弱性情報の出現確率：20%
- パッチ対策反映間隔：60 日，および，30 日
- 各機器の CIA 別損害金額：一律 1,000 円
- シミュレーション繰り返し回数：100 回

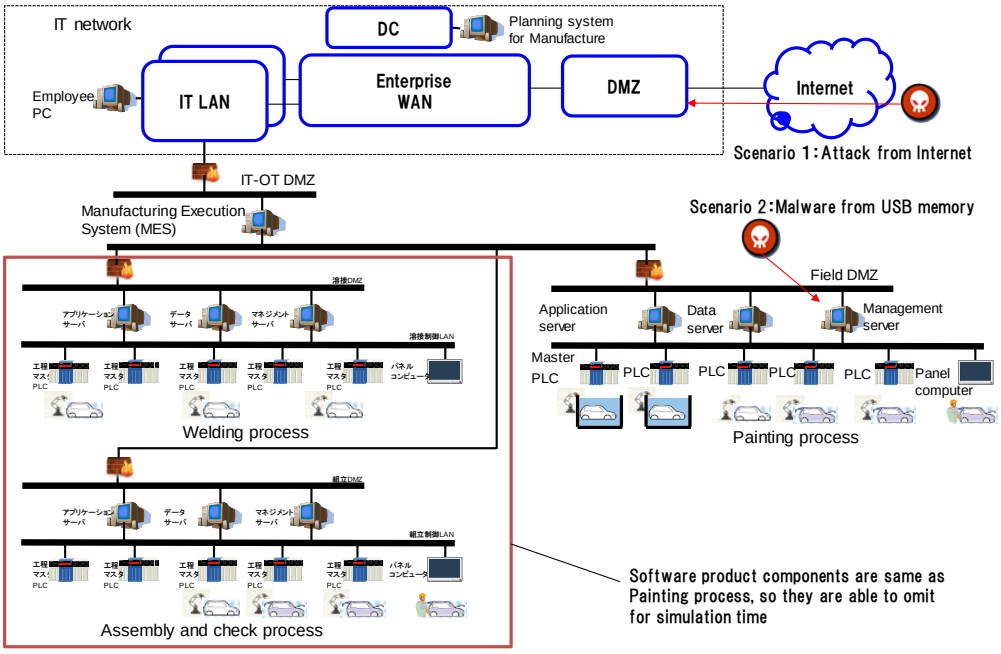

図 7　実験シナリオの概要図

表 2　想定システムのソフトウェア構成

#	Device	Software components (CPE)
1	マスタ PLC	cpe:/o:linux:linux_kernel:4.10 cpe:/a:3s-software:codesys_runtime_system
2	パネルコンピュータ(Field HMI)	cpe:/o:microsoft:windows_7 cpe:/a:3s-software:codesys_runtime_system cpe:/a:microsoft:.net_framework
3	アプリケーションサーバ	cpe:/o:microsoft:windows_server_2008:r2 cpe:/a:3s-software:codesys_gateway-server
4	データサーバ	cpe:/o:microsoft:windows_server_2008:r2 cpe:/a:osisoft:pi_server cpe:/a:microsoft:.net_framework
5	マネージメントサーバ	cpe:/o:microsoft:windows_server_2008:r2 cpe:/a:3s-software:codesys_runtime_system cpe:/a:microsoft:.net_framework
6	生産実行システム(MES)	cpe:/o:microsoft:windows_server_2008:r2 cpe:/a:microsoft:.net_framework
7	生産計画システム	cpe:/o:microsoft:windows_server_2008:r2 cpe:/a:microsoft:.net_framework
8	従業員 PC	cpe:/o:microsoft:windows_7

表 3　脆弱性情報の発生パラメータ

製品名	数式	期待値	分散
cpe:/o:linux:linux_kernel:4.10	2	132	17
cpe:/o:microsoft:windows_7	2	164	45
cpe:/o:microsoft:windows_server_2008	2	187	37
cpe:/a:3s-software:codesys_runtime_system	1	1.0	-
cpe:/a:3s-software:codesys_gateway-server	2	1.2	6.0
cpe:/a:microsoft:.net_framework	2	12.4	2.6
cpe:/a:microsoft:sql_server	2	3.8	5.2
cpe:/a:osisoft:piserver	1	0.2	-

*：数式 1:ポアソン分布，2:負の 2 項分布

3)　実験結果

以上のパラメータにより，実験を行った．結果を表 4 におよび，図 8 に損害額に対する再現期間のグラフを示す．

表 4　実験結果

Attack scenario	Expected Average annually Loss（Yen）		Reduced Loss（Yen）	Reduced percentage
	Response Interval ： 60 days	Response Interval : 30 days		
1:インターネット経由	144,630	123,515	21,115	14.6%
2：USB からのマルウェア感染	172,400	142,605	29,795	17.3%

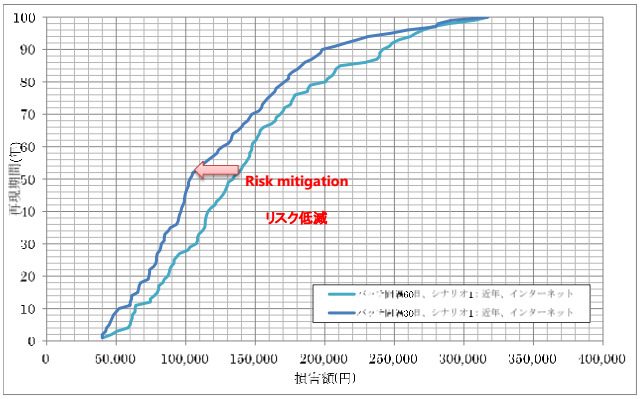

図 8　パッチ対応期間による推定損害確率の算出結果

ここで，超過確率は再現期間の逆数となる．

インターネットからの侵入シナリオで，パッチ間隔 60 日に対して，パッチ間隔 30 日は損害額が約 15%低減し，USB からの感染シナリオで，約 17%低減する結果が得られた．

5.　考察

（1）　構築モデルについての妥当性の考察

構築したモデルに従い，セキュリティインシデントによる損害額の算出を行っており，また，対策頻度（セキュリティパッチの適用する間隔）により，インシデント発生回数の相違が損害額の相違に適切に反映されており，モデルとして相対的な妥当性はあるものと考えられる．

さらに，各リソースのビジネスインパクトを明確化しパラメータとしてモデルに代入したシミュレーション結果と，実際の損害額（あるいは損害見積額）とで妥当性を検証していくことが必要と考える．この過程でモデルの調整などを行う必要がある．

（2）　グラフのがたつきの考察

モンテカルロ法では確率分布で定義される要素の振る舞いを乱数でバラツキをモデル化し，多数回シミュレーションすることで，全体のモデルの結果の確率事象をグラフ化するものであるが，今回のシミュレーションで 1 回（1 年分）のシミュレーションに 20 分弱の計算時間を要しており，100 回分計算するのに 30 時間程度要した．このため，回数を稼げず，グラフにおけるがたつきの原因となっている．今回は，既存の処理プログラムを可能な限り流用する方針で実装したため，効率的な実装とはなっていない．今後，高速化を進めていく．

6.　結言

自然災害の CAT モデルを参考に以下のサイバー攻撃における損害発生シミュレータを開発した

- Exposure, Hazard, Vulnerability, Risk の各モジュールを，サイバーインシデントによる損害発生を論理的にモデル化して構築
- 各論理的モデルにおいて，統計的な確率分布モデルを適用し，モンテカルロ法による損害発生のばらつきもモデル化

セキュリティ対策頻度の異なる自動車工場を想定したシナリオで損害発生をシミュレーションし，それぞれの超過確率曲線を算出し，頻度に応じてリスク軽減する効果を示すことを確認した．

本成果により，サイバーインシデントの損害発生を超過確率曲線で算出し，損害発生インパクトとその発生頻度を示すことが可能となることを示した．

今後は，セキュリティ対策モデルの組み込みやインシデント発生についての統計情報を用いた確率密度関数の調整などにより，リスク評価の精度向上を目指していく．

商標および登録商標　本論文で使われているシステム・製品名は，各社の商標または登録商標です．

謝辞　本報告は，2017 年度に行った損保ジャパン日本興亜，SOMPO リスクマネジメント，日立製作所 3 社の共同研究成果を纏めたものである．本研究にご協力頂いた関係各社の皆様に，謹んで感謝の意を表します．

参考文献

[1] JP CERT/CC．OpenSSL の脆弱性に関する注意喚起．JPCERT-AT-2014-0013 (2014-04-11 更新), https://www.jpcert.or.jp/at/2014/at140013.html (参照 2016-04-11)
[2] IPA．” 更新：bash の脆弱性対策について(CVE-2014-6271 等)”，https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html.
[3] 経済産業省，IPA(Information-technology Promotion Agency). サイバーセキュリティ経営ガイドライン V1.0. http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf.
[4] 杉本，磯部，仲小路，サイバー攻撃の侵入経路を考慮したセキュリティリスク評価技術，情処論文，Vol.57 No.9 pp.2077-2087(2016)
[5] 杉本，磯部，中小路，セキュリティ運用のための経営層向けビジネスリスク評価技術の開発，情処論文，Vol.58 No.12 pp1926-1934(Dec.2017)
[6] 渡辺他編著. BCMS 強靭でしなやかな組織をつくる．日刊工業新聞社 (2013/3/25)
[7] National Bureau of Standards：FIPS PUB 65 ”Guidelines for automatic data processing risk management(1975-8)
[8] 中村，兵頭，曽我，水野，西垣．セキュリティ対策選定の実用的な一手法の提案とその評価．情処論文，Vol.45, No.8, pp2022-2033(2004).
[9] 西垣，臼井，山本，間形，勅使河原，佐々木．賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価．情処論文，Vol.52，No.3, pp1173-1184(2011).
[10] L. A. Gordon, M. P. Loeb．The Economics of information Security． ACM Transactions on Information and System Security, 5 (4), pp.438-456.
[11] H. Tanaka, K. Matsuura and O. Sudo．Vulnerability and information security investment: An empirical analysis of e-local government in Japan．Journal of Accounting and Public Policy, 2005, 24(1), pp.37-59.
[12] K. Matsuura．Productivity Space of Information Security in an Extension of the Gordon-Loeb’s Investment Model．in Johnson, M.E. (ed.), Managing Information Risk and the Economics of Security, pp.99-119, Springer(2009).
[13] Peter Mell, et al. A Complete Guide to the Common Vulnerability Scoring System Version 2.0．http://www.first.org/cvss/cvss-guide.pdf
[14] 下和田功編：”はじめて学ぶリスクと保険（改訂版）“，有斐閣ブックス，2007 年 4 月 15 日
[15] エーオン ベンフィールド ジャパン(株)：”自然災害リスクに係る外部調達モデルの構造等に関する調査報告書”，金融庁委託調査,平成 24 年 3 月，https://www.fsa.go.jp/common/about/research/20120706/01.pdf
[16] NIST Information Technology Laboratory:”Search Vulnerability Database”, https://nvd.nist.gov/vuln/search
[17] Verizon Enterprise．2015 Data Breach Investigations Report(DBIR)．Verizon Enterprise (2015). http://www.verizonenterprise.com/DBIR/2015/