Vol.2016-CSEC-74 No.16
Vol.2016-SPT-19 No.16
2016/7/14

サイバーセキュリティ脅威対策のための ビジネスリスク評価システムの提案

磯部義明[†1]　杉本暁彦[†1]　仲小路博史[†1]

概要：2015 年 6 月に発覚した日本年金機構の個人情報漏洩事件より，組織内のリスク共有体制の不備や対処判断の遅れが一つの要因となり，被害拡大を招いたと分析されている．また，日本ではサイバーインシデントにあたって，経営者のリーダーシップが十分に発揮されていない組織が多いことも課題となっている．経営者のセキュリティに関するリスク管理が十分でない原因として，ビジネス上のリスクとして判断に資する情報を経営者に提供できていないことが挙げられる．本報告では，既報のセキュリティリスク評価技術の結果を活用し，ビジネス上のリスクを経営者に提供するため，(1)その脅威によるインシデント発生可能性と影響業務，(2)インシデント発生時の想定損失額，(3)事前対策した場合の投資効果の３つの指標を提示するシステムを提案する．これらの指標により，サイバーセキュリティ脅威におけるビジネス上のリスクを把握しやすくし，組織内のリスクコミュニケーションと組織のリスク経営を支援し，適切なセキュリティ対策を促進することができると考える．

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，ビジネスリスク分析，セキュリティ投資効果

Proposal of Business Risk Assessment System for Cyber Security Threats

YOSHIAKI ISOBE[†1]　AKIHIRO SUGIMOTO[†1]　HIROFUMI NAKAKOUJI[†1]

Abstract: It is analyzed that lack of risk sharing structure and delay of response decision are the significant causes for the incident of personal data breach found at Japan Pension Service in June, 2016. In addition, it is the problem that many business managers don't show leadership on cyber incidents because of lack of information for evaluating business risks needed for making decision. This paper proposes a system showing three indexes to take risk in the business to the business manager, (1) an incident occurrence probability and suspended business activity by the threat, (2) an amount of assumption loss when occurs the incident, and (3) a return investment for a countermeasures of the threat in advance to utilize the result of the security risk evaluation technology of the previous report. Our proposal make it easy to understand risk in the business in the cyber security threat by these indexes and support the risk communication between stakeholders and the risk management of the business system and it can promote an appropriate security countermeasure.

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，我々で開発した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]を拡張し，事業への影響を想定被害額に換算して提示することで経営層の判断を促すことを目的に，ビジネスリスク評価システムを提案する．

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

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[5]．BCMS は 2012 年に ISO 22301 として

†1 (株)日立製作所
Hitachi Ltd.

ⓒ2016 Information Processing Society of Japan

Vol.2016-CSEC-74 No.16
Vol.2016-SPT-19 No.16
2016/7/14

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，適切に分析結果を活用する必要があり，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[6]．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[7]．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[8]．

また，永井らは脅威発生がインシデントに至る Fault Tree をモデル化しミニマルパス解析により，必要最低限のセキュリティ対策選定方法を提案している[9]．また，佐々木らは，この Fault Tree 分析を不正コピー防止対策に適用し，費用対効果の高い不正コピー防止対策の選定方法を提案している[10]．

3)　Gordon & Loeb 経済モデル[11]

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[12]．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[13]．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，個別脅威の対策に関する判断に利用することは困難である．

2.2 セキュリティリスク評価

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[14]．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．

2.3 攻撃経路を考慮したリスク評価

筆者らは，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．

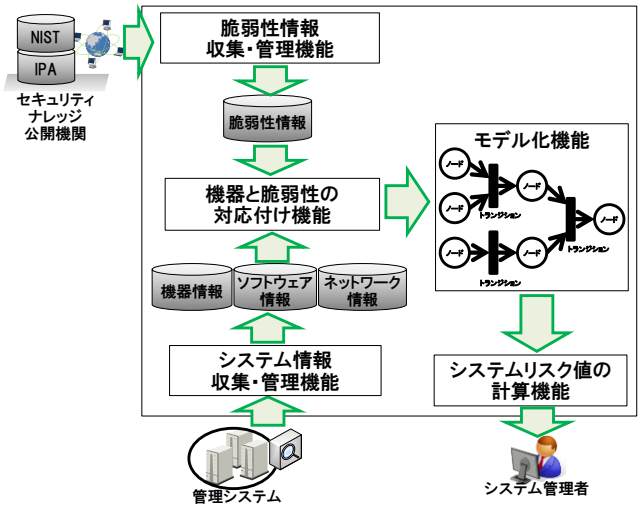


図 1 セキュリティリスク評価システムの全体構成[4]

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，

ⓒ2016 Information Processing Society of Japan

Vol.2016-CSEC-74 No.16
Vol.2016-SPT-19 No.16
2016/7/14

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．しかし，この評価システムでも攻撃到達可能性を示すに留まっており，経営者の判断に資する情報提示には十分では無い．そこで，本報告では，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システムを提案する．

3. ビジネスリスク評価システム（BRASS）の提案

3.1 全体像

本報告で提案するビジネスリスク評価システム（BRASS：Business Risk Analysis System on Cyber Security）の概要を図に示す．

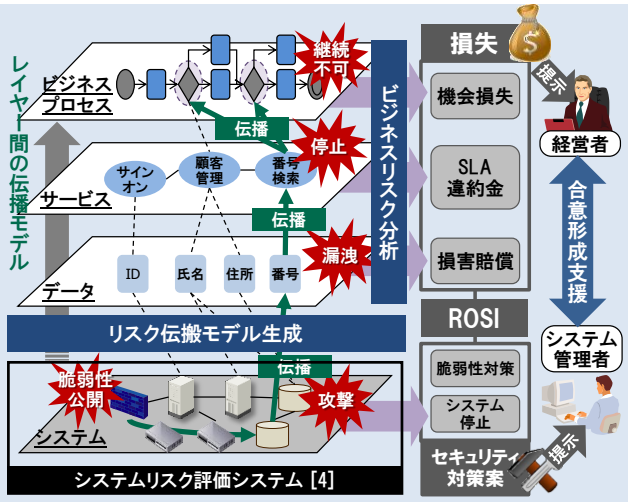


図 2 BRASS（Business Risk Analysis System on Cyber Security）の概要

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．本システムのビジネスリスク算出モデルを次節以降で説明する．

3.2 ビジネス影響伝搬モデル

ビジネス影響評価については，NIST SP800-34 Rev.1[15]に準じて予め実施する．本ガイドラインでは以下の 3 つのステップで，ビジネス影響評価を行う．

1. ミッションあるいはビジネスプロセスを特定し，業務阻害時の復旧の必要性とその許容停止時間を明確にする．
2. システムとビジネスプロセスの依存関係を特定し，システムリソースの復旧要件（目標復旧時間）を明確にする．
3. システムリソースの復旧優先度を明確にする．

上記の結果得られる，項番 2 のシステムとビジネスプロセスの依存関係を図 3 に示す．この関係が明確であれば，サイバー攻撃の対象となるシステムリソースの影響を逆に伝搬することができ，ビジネスプロセス上の影響を明確にすることができる．

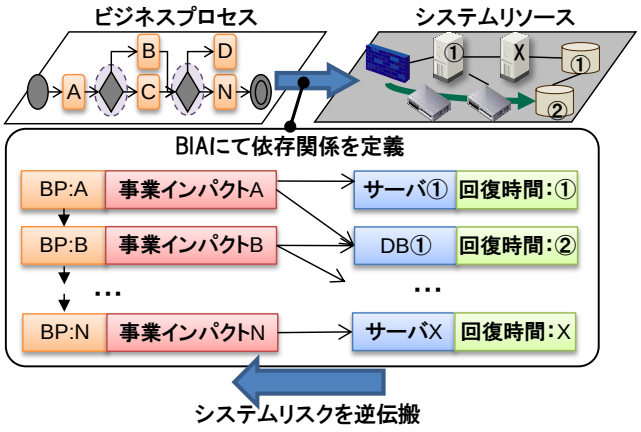


図 3　Business Impact Analysis[15]と伝搬モデル

さらに，これらの評価結果と，このビジネスプロセスやビジネスフローにより得られる利益や便益が明らかにされれば，経営上のインパクトが明確にできる．

3.3 想定損失額算出モデル

サイバー攻撃が管理対象のシステムリソースに到達されたことにより，システムのセキュリティの三要件が阻害され，損失が発生する．

1. 可用性阻害（Availability）：業務停止（業務継続性）されることによるビジネスリスク
2. 秘匿性阻害（Confidentiality）：情報漏洩されることによるビジネスリスク
3. 完全性阻害（Integrity）：情報改ざんされることによるビジネスリスク

これらの損失に加えて，セキュリティ対策に費用を要す．それぞれについて，想定損失額算出モデルを説明する．

3.3.1 可用性阻害に関する想定損失算出モデル

3.2 章で対象としたビジネスプロセスが構成されるビジネスフローに対する利益（事業上の便益を含む）を特定し，そのビジネスプロセスを支えるシステムリソースの依存関係を用いて，サイバー攻撃到達時のビジネス影響を評価できる．事業継続（可用性）に関するビジネスリスクBR_aは，次式により表現できる．

$$BR_a = Pr \times RT \quad \cdots（1）$$

ここで，

ⓒ2016 Information Processing Society of Japan

Pr：その業務の単位時間の利益（便益）（￥/Time）
RT：阻害原因となるリソースの回復時間(Time)

サイバーセキュリティ被害に対するシステム回復までのステップを以下に示す.

(1)インシデント発生認知しシステム停止
(2)インシデント要因の特定
(3)対処/対策の方法検討
(4)対処/対策による可用性阻害テスト
(5)対処/対策の方法決定
(6)対処/対策の実施し，システム再起動

以上は，既設のセキュリティアプライアンス等の設定や情報更新により，対処/対策を行う場合であり，新規にセキュリティアプライアンスを導入する場合は，発注～納品のステップが必要となる．これらのステップに要する時間により失われる利益などで損害算出が可能となる．

3.3.2 秘匿性阻害に関する想定損失算出モデル

情報漏洩に関するビジネスリスクはサイバーセキュリティ脅威により漏えいした情報の価値や秘匿義務違反による保証により定義することができる．情報の価値の考え方は，情報種別により異なる．例えば，音楽や映像等のコンテンツ配信サービスであれば，各コンテンツ受信の対価が情報の価値として考えられる．この場合の情報漏洩のビジネスリスクBR_cは次式により表現できる．

$$BR_c = C_V \times Qc \quad \cdots (2)$$

ここで，
C_V：各コンテンツの平均価格（¥）
Qc：漏洩元となるリソースで保持するコンテンツ数

外注された設計情報などで秘匿義務違反のペナルティが契約で明確な場合は，図面数などで同様のリスク査定が可能である．

一方で，自社で秘匿管理している知財情報や機密情報などのコンテンツやデータは，個別に秘匿することで得られる価値や漏洩時の損害を事前に査定しておく必要がある．

秘匿義務違反の一つである個人情報の漏えいに関しては，漏洩レコードあたりの賠償額について，いくつかの事例から，推定する方法が提案されている[16-19].

米国ベライゾン社は NetDiligence 社と協力し，サイバー保険会社への損害賠償保険金請求に関するデータから，漏洩元のレコード数に対し両対数回帰モデルで近似した賠償額見積もりモデルを提案している[19].

本研究では，これらのモデルのうち，各ビジネスフローに適した推定モデルを選択し，個人情報漏洩に対する損害額推定を行うこととした.

また，これらの情報漏洩に関する損失に加え，漏洩したシステムを停止し必要なセキュリティを復旧するまでの事業継続阻害に関する損失を加えて負うこととなる.

3.3.3 完全性阻害に関する想定損失算出モデル

情報改ざんに関するビジネスリスクは，情報改ざんにより発生する損害として，定義する．このような損害につながる情報を扱うシステムでは，異常値をはじくための上限値や下限値をプログラムに組み込む必要がある．これらのデータ改ざんは，このアプリケーションプログラムの異常値検知により，損害を上記機能の上限値の範囲に留めることができる.

この場合の情報改ざんに関するビジネスリスクBR_iは次式で定義できる.

$$BR_i = L \times I_T \quad \cdots (4)$$

ここで，
L：改ざんされるシステムリソースの（取引等の）各セッションの上限値（あるいは下限値．最悪値となる値を選択）による被害想定額（¥）
I_T：改ざんされるシステムリソースが可能な違法取引数（異常な繰り返しセッションの上限回数値）

これらに関するリスクがクリティカルなアプリケーションには，デジタル署名技術により完全性要件の対策される場合が多い．一方で，2014 年 4 月に公開された脆弱性「Heartbleed 」により，OpenSSL で実装された多くの Linux ベースで構築されたサーバやアプライアンスにおいて，完全性担保の前提となる秘密鍵が漏えいし，データの完全性が侵される脅威が現実化し，多くのシステムで，システム停止の伴う緊急対処に迫られた[1]．このような場合，これらの情報改ざんに関する損失に加え，必要なセキュリティを復旧するまでの事業継続阻害に関する損失を加えて負うこととなる.

また，データの改ざんに留まらず，アプリケーションプログラムのチェック機構の回避するようにプログラムを改ざんするなどで，サービスシステムの完全性が脅かされる脆弱性が公開される場合もある．この場合，正しいサービス提供が損なわれており，サービス提供を即座に停止する必要がある．このため，サービス再開までの期間に得られるはずの利益や便益がビジネスリスクとなり、数式 (1) で示したリスクも合わせて負うこととなる.

3.3.4 セキュリティ対策費用の見積もり

セキュリティ対策費用の見積もりを表 1 に示す. ここで，脆弱性公開に関するリスクについては，サイバー攻撃（の検知）に先立って事前対処/対策することで，脅威予防に効果的である．この場合，表 1（6）の対策実施/対処期間以外をシステム停止することなく並行して実施することが可能であり，これにより事業停止によるビジネスリスクを軽減することも可能である．また，事前対策では要因特定に時間を要す必要もないため, この分の人件費も削減できる.

これらの工数や損失をインシデント後の対処と比較することで事前対処の経済性（*ROSI*）を算出する．

表 1 対策時間と停止時間の例

#	対策ステップ	対策時間と停止時間	
		事後対処	事前対処
(1)	インシデント発生検知し，システム停止	30 分	N/A
(2)	インシデント要因の特定	半日	N/A
(3)	対処/対策の方法検討	半日	半日(無停止可)
(4)	対処/対策の可用性阻害テスト	1~3 日	1~3 日(無停止可)
(5)	対処/対策の決定	30 分	30 分(無停止可)
(6)	対処/対策を実施し，システム再起動	~1 日	~1 日

本報告では，セキュリティリスク評価結果に基づき，対応/対策すべき攻撃到達可能性に対し，しきい値T_{ar}を設定し，このしきい値T_{ar}を上回る機器の対策・対応人件費：EC_{wl}を各機器の対策対応人件費の積算で定義した．

$$EC_{wl} = \sum_{T_{ar}<D_{ar}} D_{wl} \cdots （5）$$

ここで，

D_{ar}：各機器への攻撃到達確率

D_{wl}：各機器に対する対応/対策人件費

各機器に対する対応/対策人件費は，機器の種別によって平均値や最悪値も異なることも考えられる．機器種別によって，この人件費のパラメータを調整することで，より精度の高いビジネスリスクを推定することも可能である．

3.4 脆弱性対処の ROSI 算出モデル

ROSI（Return Of Security Investment）の算出は，インシデント発生時の想定被害額に対し，セキュリティ対策に費やすコストを算出し，差額を投資効果として算出する．

前節までで，対処/対策工数とインシデント発生時の想定被害額を算出しており，この算出結果を利用し，次式により算出する．

$$ROSI = \sum BR_x - (EC_{wl} + P_{cm}) \cdots （6）$$

ここで，

P_{cm}：新規セキュリティ対策（アプライアンス等）の導入費

また，インシデント発生前の対処/対策とインシデント発生後の対処対策及び被害額との差額をインシデント発生前での対処/対策の *ROSI* として算出することも考えられる．この場合の *ROSI* を *dROSI* とし，次式で定義する．

$$dROSI = (\sum BR_x + (EC_{Postwl} + P_{Postcm})) - (BR_a + EC_{prewl} + P_{precm}) \cdots （7）$$

ここで，

EC_{Postwl}：インシデント発生後の対処/対策に関わる人件費

P_{Postcm}：インシデント発生後の新規セキュリティ対策の導入費

EC_{prewl}：事前対処/対策に関わる人件費

P_{Precm}：事前対処に導入する新規セキュリティ対策の導入費

事前対処においてもシステム停止が必要となるため，このビジネス影響BR_aについても，評価に考慮することが必要である。しかし，表 1 に示した通り，事前対処であれば，対策の検討やテストを別途用意した環境で実施することができ，対策・適用する時間のみにシステム停止時間を留めることができる．このため，インシデント発生時と比較してビジネス継続性への影響も抑制できる．

本報告の前提技術である既存研究では，脆弱性公開の脅威が主なシステムリスクの評価ターゲットとしているため，脆弱性に対する事前対処を行うことによるセキュリティ投資効果 *dROSI* を本試作では算出することとした．

4. プロトタイプ開発

既存研究のシステムリスク評価システム[4]を拡張し，図 2 の機能ブロックで構成されるプロトタイプを開発した．

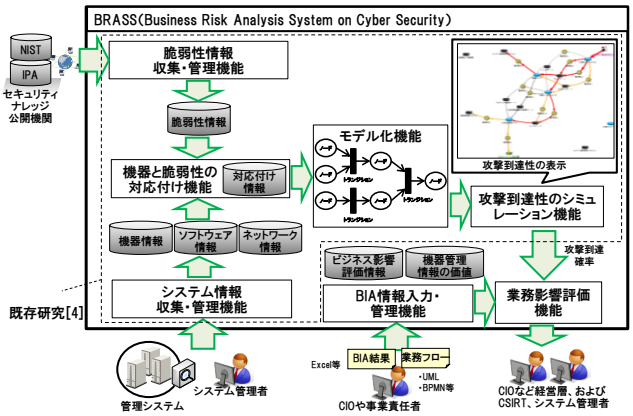


図 2 BRASS の機能ブロック図

ここで，以下の情報を事前にパラメータとして既報に追加して入力する GUI を用意した．

(1) 業務情報
  (ア) ビジネスプロセスフロー図（XML 形式）
  (イ) ビジネス情報（平均売上，平均利益・便益等）
(2) BIA 情報
  (ア) システムや機器との依存関係および依存度
  (イ) 機器ごとの対応時間および停止時間

ⓒ2016 Information Processing Society of Japan

(3) 対処検討しきい値

セキュリティリスクの評価結果を受けて，対処検討することを判断するためのしきい値．各機器への攻撃到達可能性（攻撃容易性）に対して組織の対処ポリシーとして事前設定する．

5. ユースケース評価

本報告では，評価サンプルとして架空の会社の「インターネットショッピング」をユースケースとし，サイバーセキュリティ上のビジネスリスクを評価した．表 2，3 に前提条件となるパラメータを，表 4 に BIA 評価の結果，ビジネスプロセスとシステムリソースの関連を示す．

表 2 評価サンプルのビジネス情報

#	項目	内容
(1)	ビジネスフロー名	オンラインショップ
(2)	平均売上	100 万円／日
(3)	平均利益（便益）	10 万円／日
(4)	システムエンジニア	3 人
(5)	対応人件費	2,000 円/時
(6)	ビジネスプロセス	①注文を受ける ②在庫を照会する ③クレジットカードを確認する ④注文を確定する ⑤一日の売上に計上する ⑥ピッキングする ⑦配達経過を記録する ⑧売掛金の入金を受ける

表 3 評価サンプルのシステム情報

#	機器	内容
(1)	ショッピング Web サーバ	Red Hat enterprise Linux 7 他
(2)	ショッピング AP サーバ	Red Hat enterprise Linux 7 他
(3)	ショッピング DB サーバ	Red Hat enterprise Linux 7 他
(4)	在庫・配送管理 Web サーバ	Red Hat enterprise Linux 6 他
(5)	在庫・配送管理 AP サーバ	Red Hat enterprise Linux 6 他
(6)	在庫・配送管理 DB サーバ	Red Hat enterprise Linux 6 他
(7)	顧客管理 Web サーバ	Red Hat enterprise Linux 7 他
(8)	顧客管理 DB サーバ	Red Hat enterprise Linux 7 他
(9)	売上管理サーバ	Windows Server 2012R2
(10)	業務用クライアント PC	Windows 10

表 4 評価サンプルの BIA 情報

#	業務活動	リソース
①	注文を受ける	表 3 項番(1)(2)(3) (10)
②	在庫を照会する	表 3 項番(4)(5)(6) (10)
③	クレジットカードを確認する	表 3 項番(7)(8) (10)
④	注文を確定する	表 3 項番(1)(2)(3) (10)
⑤	一日の売上に計上する	表 3 項番(9) (10)
⑥	ピッキングする	表 3 項番(4)(5)(6) (10)
⑦	配達経過を記録する	表 3 項番(4)(5)(6) (10)
⑧	売掛金の入金を受ける	表 3 項番(9) (10)

ここで，各システムリソースに合計 75 の脆弱性が存在する場合の攻撃経路シミュレーションを行った結果を図 3 に，各機器への攻撃容易性を表 5 に示す．

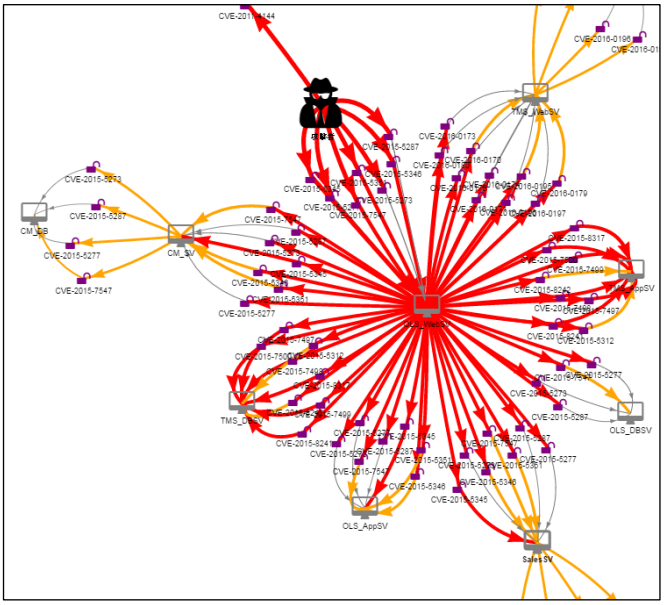


図 3 評価サンプルにおける攻撃シミュレーション結果

表 5 各機器の攻撃容易性（シミュレーション結果）

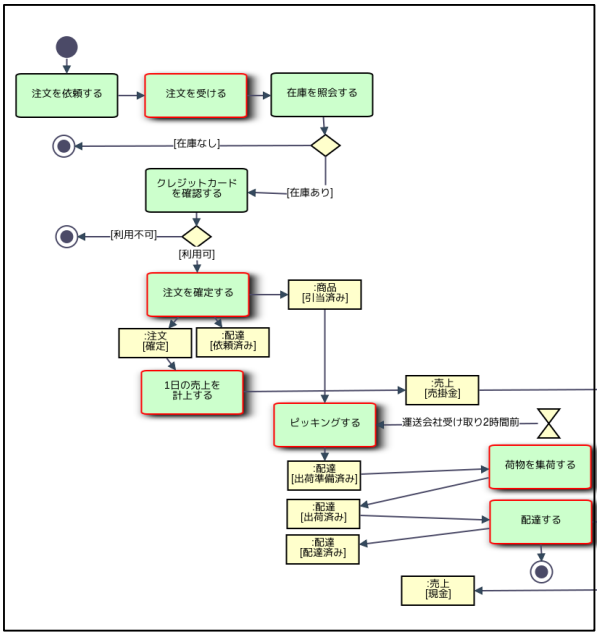
#	機器	攻撃容易性
(1)	ショッピング Web サーバ	8.0
(2)	ショッピング AP サーバ	6.4
(3)	ショッピング DB サーバ	6.2
(4)	在庫・配送管理 Web サーバ	6.4
(5)	在庫・配送管理 AP サーバ	6.4
(6)	在庫・配送管理 DB サーバ	6.4
(7)	顧客管理 Web サーバ	6.4
(8)	顧客管理 DB サーバ	4.9
(9)	売上管理サーバ	6.4
(10)	業務用クライアント PC（3 台）	4.9, 4.9, 1.9

この攻撃シミュレーションによる攻撃容易性に基づいて，想定される被害額，および，事前対策の *dROSI* を算出した結果を表 6 に示す．ここでは，被害発生の前提を攻撃容易性に対して 7.0 以上，5.0 以上とした場合を示す．

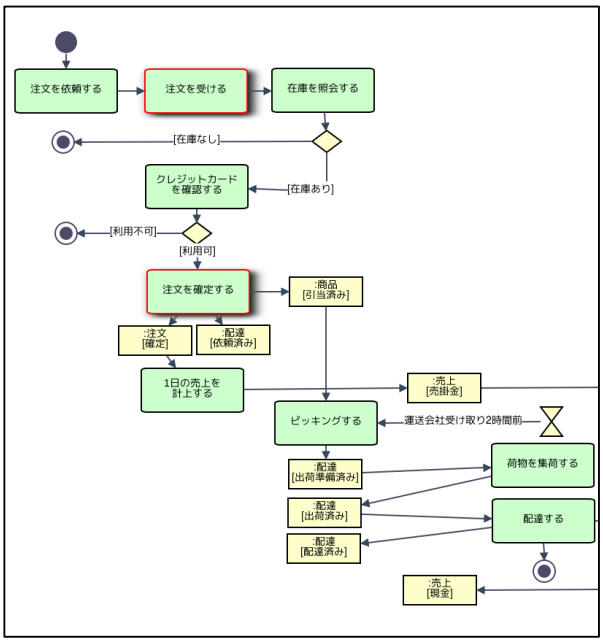
表 6 ビジネスリスク評価結果

#	項目	被害発生の前提基準	
		5.0	7.0
(1)	影響するビジネスプロセス数	7	2
(2)	被害発生時の推定損失	¥30,150,000	¥3,350,000
(3)	事前対策の ROSI	¥22,950,000	¥2,550,000

ⓒ2016 Information Processing Society of Japan



(a)前提基準：攻撃容易性>5.0 の場合



(b)前提基準：攻撃容易性>7.0 の場合

図 4　ビジネスプロセスへの影響評価結果
（赤枠が影響ある業務）

被害発生の基準を厳しく設定した場合、攻撃を受けるサーバ数が拡大し，それにより影響を受けるビジネスプロセスも増加する．このため，対策する機器が増加し，業務停止による想定損失も拡大するシミュレーション結果が確認できた．

今回の評価は，架空のサンプル業務を支える IT システムを設定し，原理試作したビジネスリスク評価プログラムが設計通り動作するか検証することに留まるが，以下の効果が期待できると考える．

- サイバーセキュリティ上のリスクをビジネスプロセスフロー上で業務停止可能性の高いビジネスプロセスにおけるリスクの高まりとして示すことで，業務への影響範囲が明確にできる
- ビジネスプロセスとシステムの依存関係により，システム停止時による業務阻害による想定被害額を算出することで，ビジネス上のリスクとして明確にできる
- 被害発生前のセキュリティ対策による想定被害の発生抑止額を *dROSI* として示すことで，迅速なセキュリティ対策の必要性・合理性を判断できる

これらの評価の妥当性や評価結果の提示内容の有効性について，関係者と議論するとともに，実際の業務へ適用した有効性や妥当性評価が必要である．

6. おわりに

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．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．そこで，本研究では，既報告で開発した攻撃経路を考慮して各機器のリスクを攻撃到達可能性(攻撃容易性)で評価する技術を拡張し，事業への影響を想定被害額に換算して提示することで経営層の判断を促すことを目的に，ビジネスリスク評価技術の研究・開発を開始した．

本報告では，以下の結果を得た．

(1) 既報[4]のシステムリスク評価結果に基づいて，サイバーセキュリティにおけるビジネスリスクを想定被害額として推定するアルゴリズム，および，*ROSI*（セキュリティ投資効果）を推定するアルゴリズムを明確化した．

(2) とくにビジネス継続性に関わる想定被害額を推定する方法として，災害脅威に対して制定された BCMS（ビジネス継続性管理システム）で利用されているビジネス影響評価方法に基づき，依存関係を明確化することで，システムリソース上のシステムリスクを伝搬させるアルゴリズムとして明確化した．

(3) これら明確化した方法に基づき，プロト開発を行い，以下を得た．

・ビジネス活動フロー図上にて，ビジネスリスク評価された結果，影響ある活動を図示する方式を明確化した．この機能により，サイバーセキュリティが実際のどの業務に影響あるか，経営層に提示することができる一方で，サイバーリスクの影響範囲を認知できるものと考える．

・想定被害額と *ROSI*（セキュリティ投資効果）を算

ⓒ2016 Information Processing Society of Japan

出・推定する方式を明確化した．この機能により，セキュリティ対策を放置するリスクを金額ベースで認識できる．さらに，事前に対処・対策することにより将来発生する損害の抑止効果（*dROSI*）を示すことができる．これらにより，セキュリティ対策の投資効果を認識でき，対策判断をサポートすることができるものと考える．

(4) 上記の原理試作プログラムに対し，インターネットショッピング業務をサンプルケースとして，動作検証・評価を行い，アルゴリズムに従った動作であることを確認した．

今後は，今回開発したプロトシステムに基づき，ビジネスリスク評価方法の妥当性や有用性などを関係するステークホルダにヒアリングし，プロトシステムをブラッシュアップしていく．さらに，有用性やパラメータの妥当性を検証していく．

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　本研究にご協力頂いた皆様に，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] 磯部，杉本．ベイジアンネットワークを利用した動的モデリングによるセキュリティリスク評価システムの開発．情処研究報告, Vol.2015-CSEC-68 No.6 (2015/3/5).
[5] 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)
[6] National Bureau of Standards：FIPS PUB 65 ”Guidelines for automatic data processing risk management(1975-8)
[7] 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).
[8] 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).
[9] 永井，藤山，佐々木．セキュリティ対策目標の最適決定技法の提案．情処論文 Vol.41, No.8, pp2264-2271(2000).
[10] 佐々木，吉浦，伊藤．不正コピー対策の最適組合せに関する考察．情処論文 Vol.43, No.8, pp2435-2446(2002).
[11] L. A. Gordon, M. P. Loeb．The Economics of information Security． ACM Transactions on Information and System Security, 5 (4), pp.438-456.
[12] 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.
[13] 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).
[14] Peter Mell, et al. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. http://www.first.org/cvss/cvss-guide.pdf
[15] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes．Contingency Planning Guide for Federal Information System．NIST Special Publication 800-34 Rev.1(2010-5)
[16] 日本ネットワークセキュリティ協会　セキュリティ被害調査 WG．2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～．第 1.2 版(2015/2/23), http://www.jnsa.org/result/incident/data/2013incident_survey_ver1.2.pdf.
[17] 石川，櫻井．個人情報漏洩補償に関する一検討．CSS2014, pp1185-91(2014/10)
[18] Ponemon Institute．2014 Cost of Data Breach Study: Global Analysis． Ponemon Institute Research Report, May 2015.
[19] Verizon Enterprise．2015 Data Breach Investigations Report(DBIR)．Verizon Enterprise (2015). http://www.verizonenterprise.com/DBIR/2015/

ⓒ2016 Information Processing Society of Japan