ITリスク学研究会発表資料

HITACHI
Inspire the Next

セキュリティリスクマネジメント態勢を支援するリスク評価・リスク可視化技術

2017年2月20日

(株)日立製作所　研究開発グループ
システムイノベーションセンタ・セキュリティ研究部
磯部義明(yoshiaki.isobe.en@hitachi.com)

© Hitachi, Ltd. 2017. All rights reserved.

HITACHI
Inspire the Next

セキュリティリスクマネジメント態勢を支援する リスク評価・リスク可視化技術

Contents

1. 研究の背景と目的
2. 脆弱性リスク評価技術
   - 標準方式(CVSS)とその課題
3. 提案するセキュリティリスク評価技術[CSEC68、IPSJ57]
4. ビジネスリスク評価システムのご紹介[CSEC74]
5. デモ
6. まとめ

[CSEC68] 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」
[CSEC74] 磯部、杉本、仲小路「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」
[IPSJ57] 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 No9(2016.9)

1. 研究の背景と目的

HITACHI
Inspire the Next

- サイバー空間において、ブラックマーケットが成熟。基盤ソフトの脆弱性を利用した攻撃ツールが迅速に開発・展開され、被害が激甚化。
  →85%の攻撃が良く知られた脆弱性を使った攻撃(ベライゾン調査)。
- 一方で、IoTの普及が本格化。社会インフラシステムもインターネットに接続されるようになり、サイバー攻撃の対象エリアが増大。
  →サイバーセキュリティ脅威のリスク管理ができていない

経営層を含めたセキュリティ態勢構築が必須。経営層がセキュリティに関与するには、ビジネス上のリスクおよびセキュリティ対策の効果の明確化が必要

本研究の目的

経営者が判断しやすい指標でセキュリティリスクを提示し、サイバーセキュリティ経営と脆弱性管理を支援

- インシデントの発生確率(発生しやすさ)
- インシデント発生時の想定損失額
- セキュリティ対策による効果(ROSI)

© Hitachi, Ltd. 2017. All rights reserved.

HITACHI
Inspire the Next

セキュリティリスクマネジメント態勢を支援する リスク評価・リスク可視化技術

Contents

1. 研究の背景と目的
2. 脆弱性リスク評価技術
   - 標準方式(CVSS)とその課題
3. 提案するセキュリティリスク評価技術[CSEC68]
4. ビジネスリスク評価システムのご紹介[CSEC74]
5. デモ
6. まとめ

[CSEC68] 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」
[CSEC74] 磯部、杉本、仲小路「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」
[IPSJ57] 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 No9(2016.9)

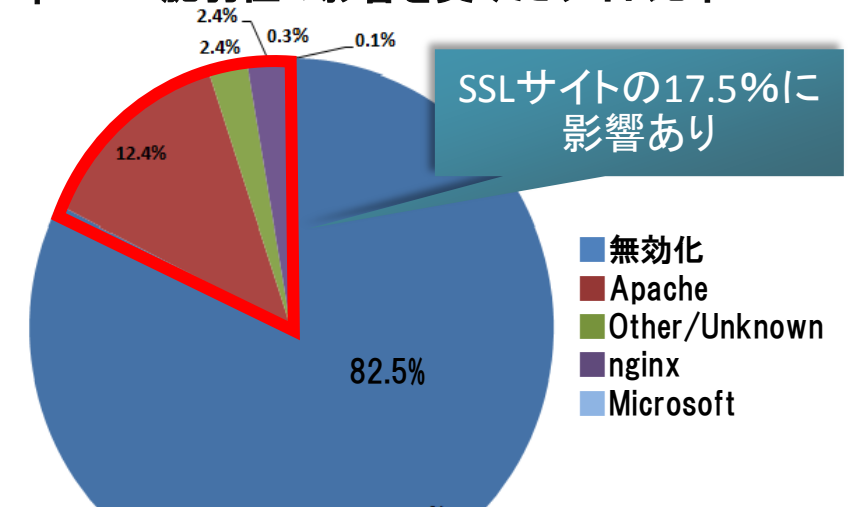
2.1 近年の傾向：深刻な脆弱性

HITACHI
Inspire the Next

2014年、広く利用されているライブラリに脆弱性が発見

① **OpenSSL（4/7）：** Heartbleedの脆弱性を利用し、リモートからメモリ情報を摂取される危険性
② **Apache struts（4/17、4/24）：** ClassLoaderの操作される脆弱性、バージョン1.Xも対象に
③ **Internet Explorer（4/28）：** 細工がされたコンテンツを開くことで任意のコードが実行される
④ **Bash（9/24）：** Shellshock　CGI、sshなどを介してリモートから任意のコマンドを実行される

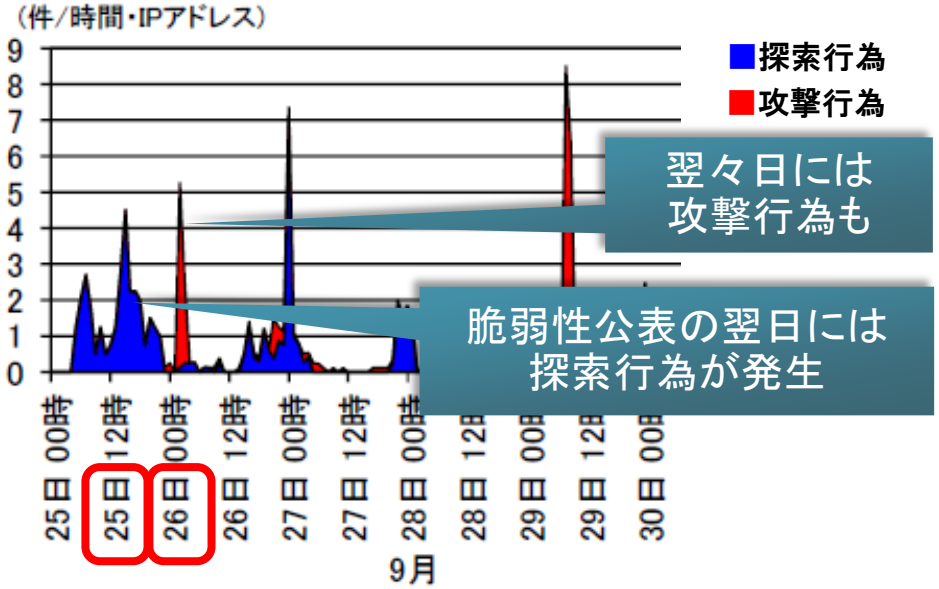
OpenSSL脆弱性の影響を受けたサイト比率



ログが残らないため、攻撃を受けたか分からず
SSLサーバ証明書3万件で失効手続きがされた

Netcraft「Half a million widely trusted websites vulnerable to Heartbleed bug」

Bash脆弱性を標的としたアクセス観測



@police「Bash の脆弱性を標的としたアクセスの観測について（第2報）」

社内システムの構成情報の把握、脆弱性に対する迅速な判断・対応が求められる

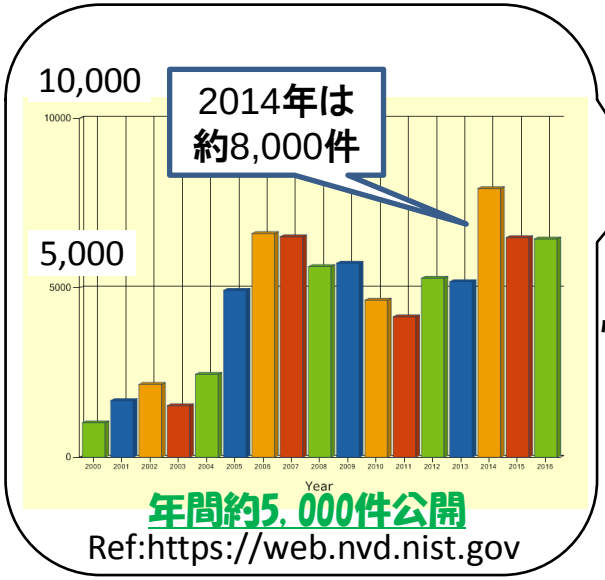
© Hitachi, Ltd. 2017. All rights reserved.

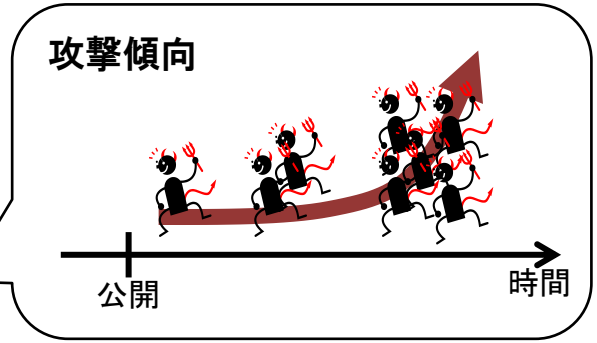
2.2 研究の背景

HITACHI
Inspire the Next

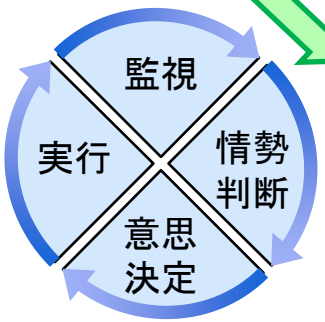
■IPAやNISTから年間約5,000件の脆弱性情報が公開。

–公開直後から同脆弱性を利用した攻撃が急増する傾向があるため，システム管理者は効率よく必要な脆弱性対策を行う必要がある。

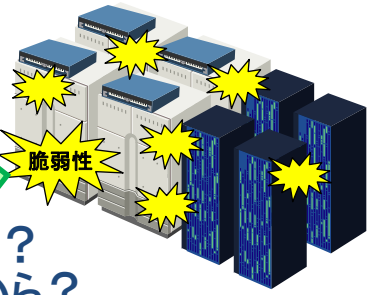




脆弱性情報



脆弱性対策



・どこに？
・どれから？
・いつ？

適切な脆弱性リスク管理に課題

© Hitachi, Ltd. 2017. All rights reserved.

2.3 CVSS(Common Vulnerability Scoring System)

HITACHI
Inspire the Next

- 情報システムの脆弱性の脅威を評価する汎用的な方法
- 脆弱性の深刻度を同一の基準で比較可能とする
- 以下の3つの基準で脆弱性を評価

  - 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。評価結果は利用環境や時間変化に依存しない。(→IPAやNISTなどの公開情報にも含まれる)
  - 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。攻撃ツールの有無や対策公開状況などで変動

  → 各組織のCSIRTはこれらを評価し、注意喚起/警告等を実施

  - 環境評価基準(Environmental Metrics)
    ユーザの利用環境を考慮して最終的な脆弱性深刻度を評価する基準。

  → 各システムの構成等を熟知したシステム管理者に評価は委ねられる

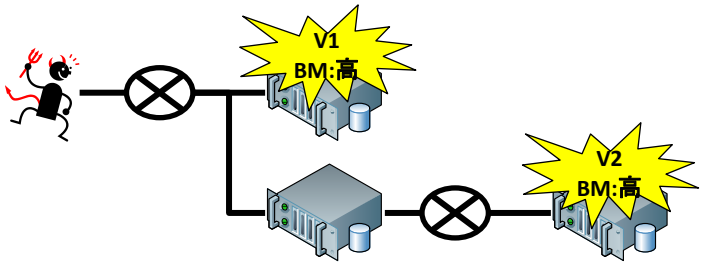
↓

それぞれのシステム管理者の取り組み内容に依存(例:基本評価のみで判断)

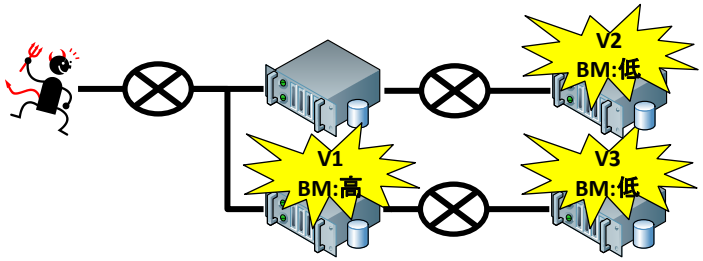
https://www.ipa.go.jp/security/vuln/CVSSv3.html

© Hitachi, Ltd. 2017. All rights reserved.

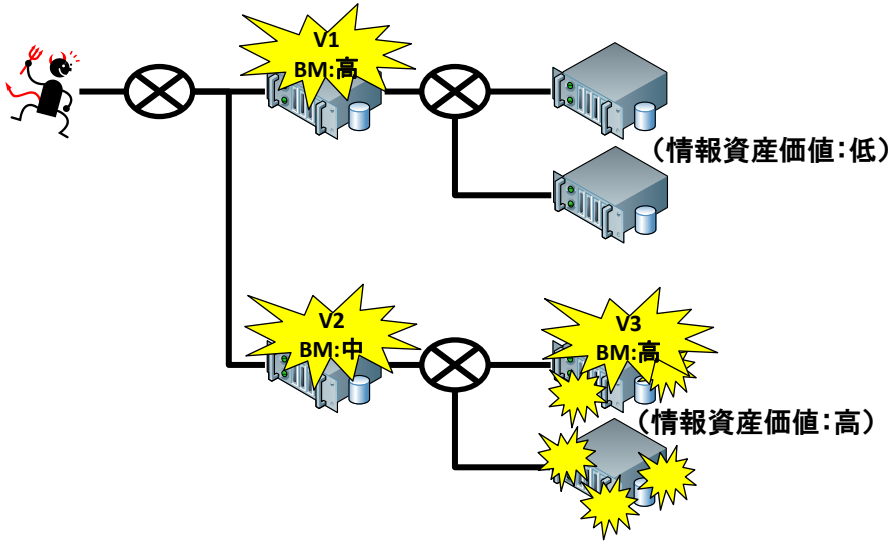
2.4 CVSS基本評価のみでのリスク評価の課題



(1)攻撃手数に関わらず評価



(2)攻撃容易性に関わらず評価



(3)資産価値の所在に依らずに評価

安全に倒すと、すべて同じように対応しなければならず、
一時的な工数の集中や工数爆発により、対応しきれない

対応漏れによるインシデント発生するリスクも

© Hitachi, Ltd. 2017. All rights reserved.

HITACHI
Inspire the Next

セキュリティリスクマネジメント態勢を支援する リスク評価・リスク可視化技術

Contents

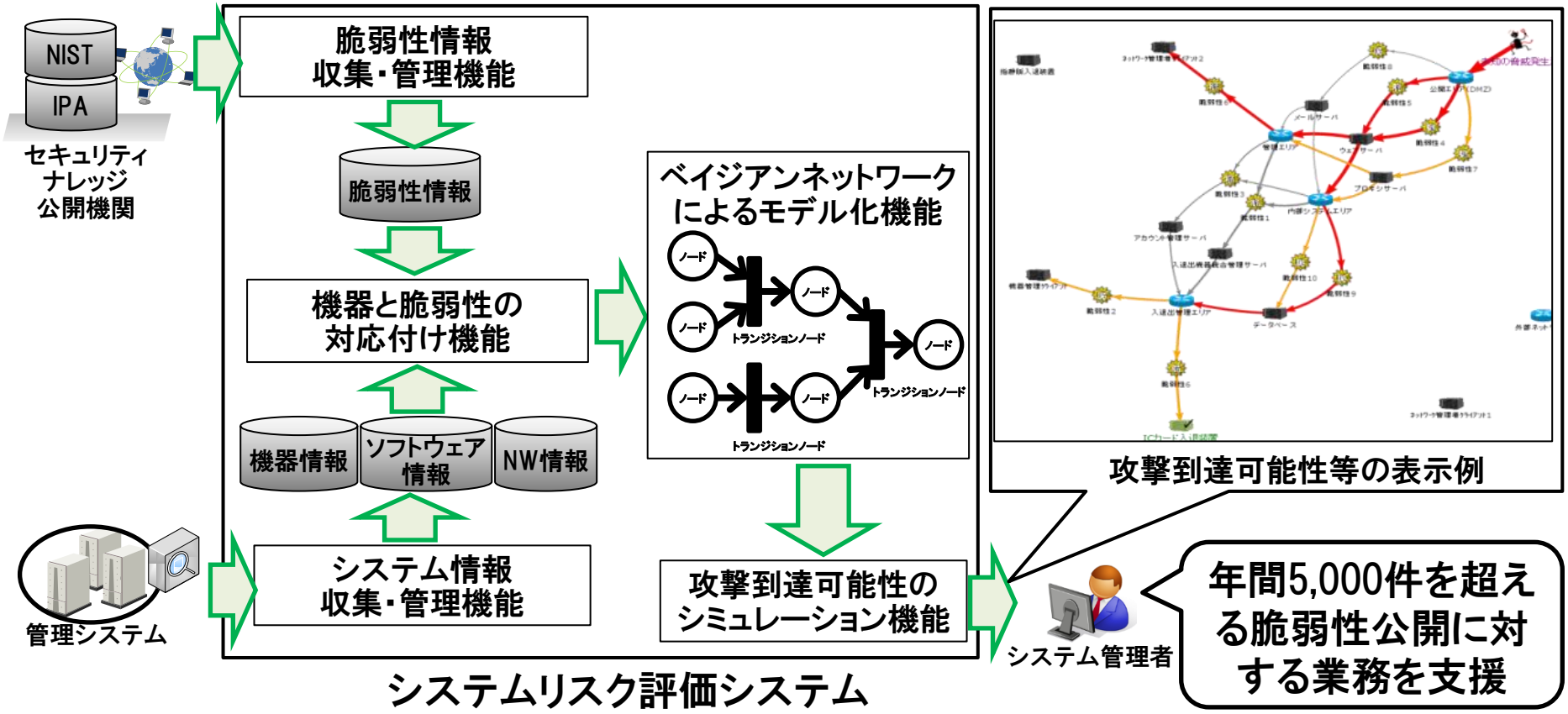
1. 研究の背景と目的
2. 脆弱性リスク評価技術
   - 標準方式(CVSS)とその課題
3. 提案するセキュリティリスク評価技術[CSEC68、IPSJ57]
4. ビジネスリスク評価システムのご紹介[CSEC74]
5. デモ
6. まとめ

[CSEC68] 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」
[CSEC74] 磯部、杉本、仲小路「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」
[IPSJ57] 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 No9(2016.9)

3.1 攻撃経路を考慮したリスク評価技術の概要

HITACHI
Inspire the Next

- 脆弱性の所在を特定し、システムトポロジに応じて自動でベイジアンネットワークモデル化。各機器への攻撃到達可能性をシミュレート。
- 各システム管理者に任されていたCVSSの環境評価の一部(TD:システムの影響範囲)や攻撃到達可能性評価を自動化し、緊急対処が必要な機器を特定。



© Hitachi, Ltd. 2017. All rights reserved.

3.2. ベイジアンネットワークによるリスク評価の実装

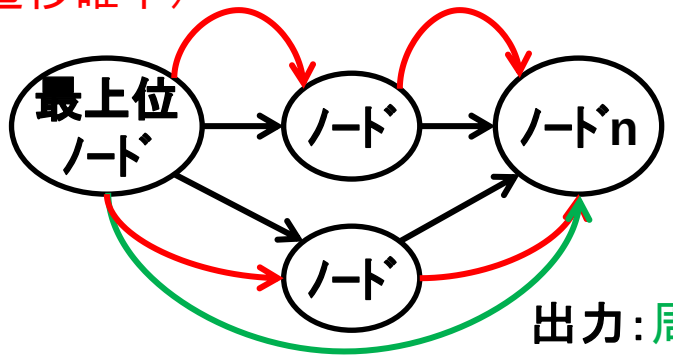
HITACHI
Inspire the Next

■ 各機器、各脆弱性のリスクを定量化する実装として、ベイジアンネットワークによるモデル化を利用

ベイジアンネットワークとは

隣接ノード間の遷移確率を入力することで，最上位ノードからの遷移確率を出力

入力：条件付き確率
（隣接ノードからの遷移確率）



出力：周辺確率
（最上位からノードnまでの遷移確率）

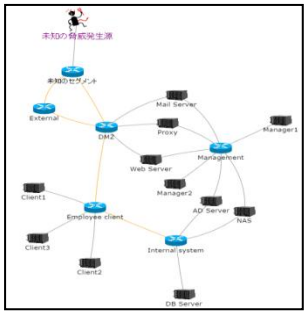
各ノードへの複数の攻撃経路を組合わせ，
正規化された攻撃可能性を算出可能

© Hitachi, Ltd. 2017. All rights reserved.

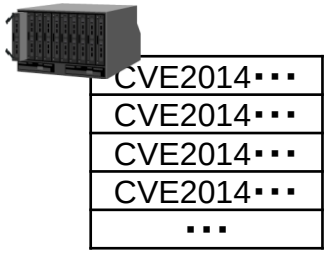
3.3. グラフモデルの構築 (1)

HITACHI
Inspire the Next

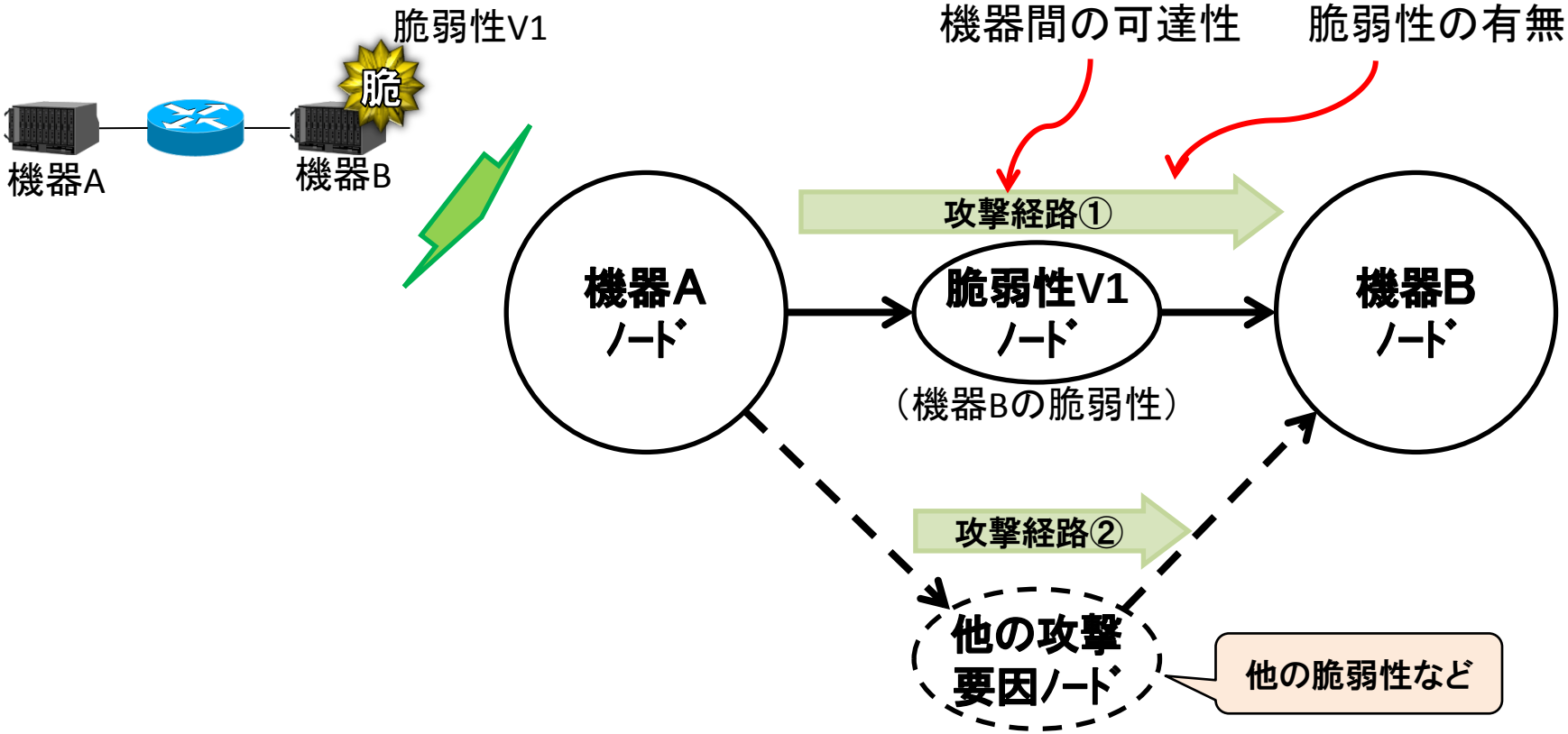
■ 有向非巡回グラフを構築
– 機器間の可達性，脆弱性（攻撃要因）の有無からアーク（矢印）を接続



（from トポロジ情報）
機器間の可達性



（from 脆弱性管理）
脆弱性の有無



© Hitachi, Ltd. 2017. All rights reserved.

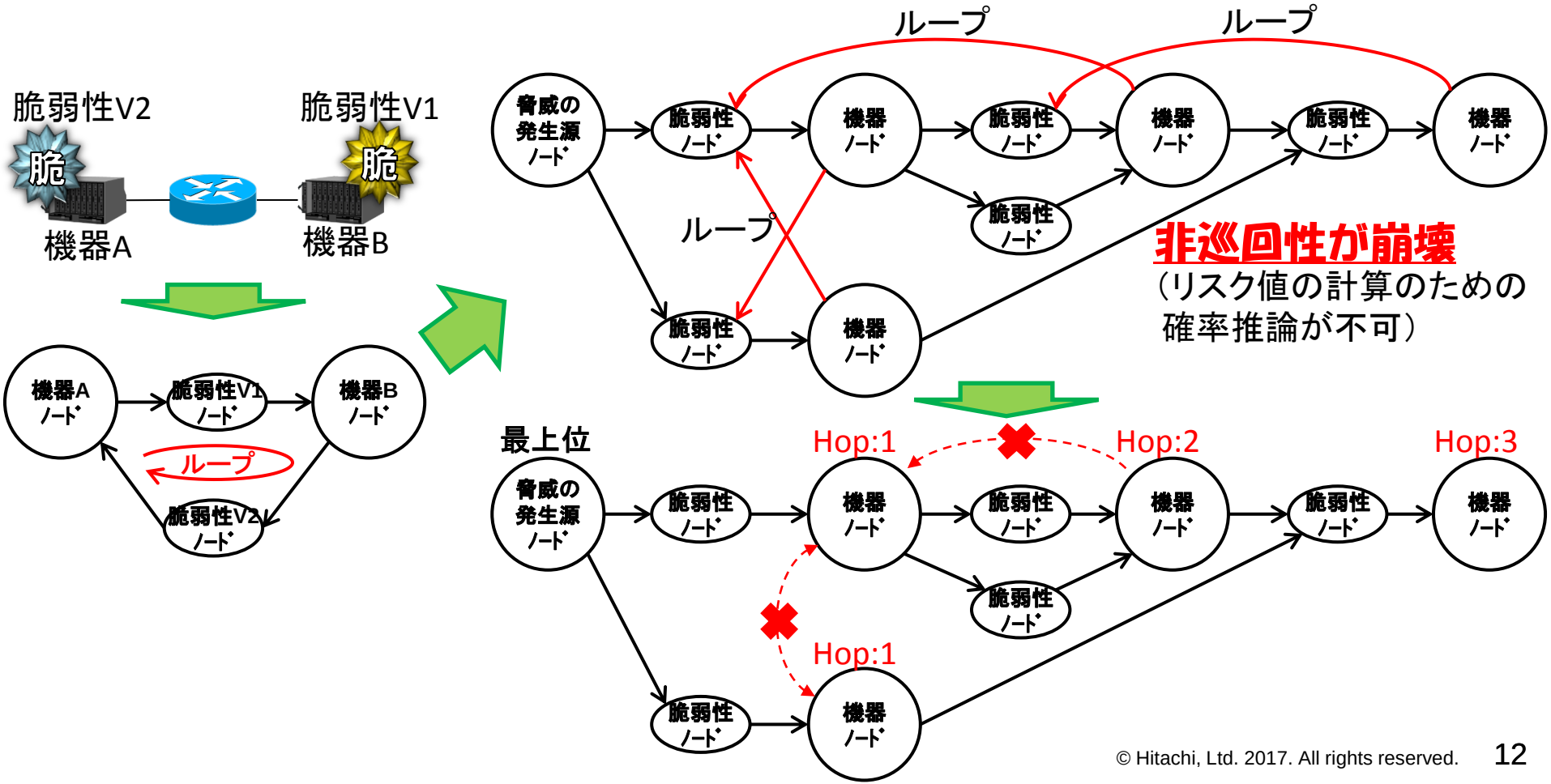
3.4. グラフモデルの構築 (2)

HITACHI
Inspire the Next

■ 有向非巡回グラフを構築

– ベイジアンネットワークでの計算上の制約条件を導入

「Hop数が少ない機器からHop数が多い機器へのみアークを接続する」



© Hitachi, Ltd. 2017. All rights reserved.

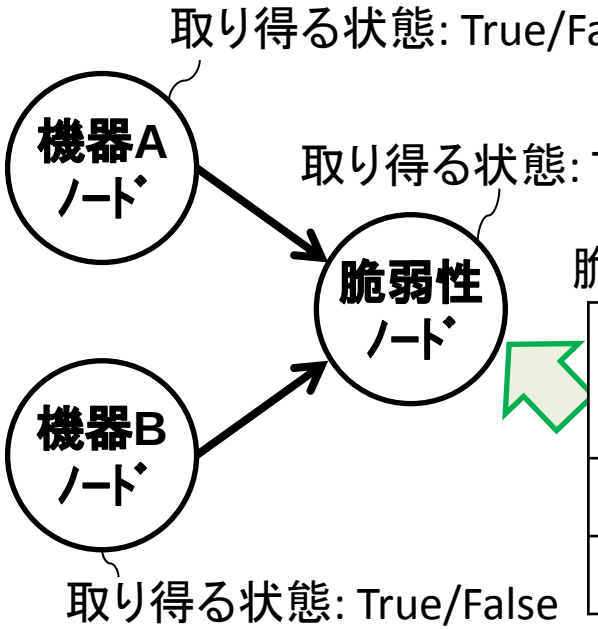
3.5. 条件付き確率表の設定（1）

HITACHI
Inspire the Next

■ ベイジアンネットワークで計算するため，条件付き確率表を設定

– 各ノードが取り得る状態を各機器，各脆弱性が侵害された状態，あるいは侵害されていない状態の2値（True/False）で定義

– 隣接する機器の脆弱性ノードの条件付き確率表については，CVSSの攻撃容易性（AV：攻撃元区分、AC：攻撃条件の複雑さ、Au：認証の要否）を利用



CVSSの攻撃容易性を利用

脆弱性ノードの条件付き確率表

	機器A	True		False	
	機器B	True	False	True	False
True		0.7	0.7	0.7	0
False		0.3	0.3	0.3	1

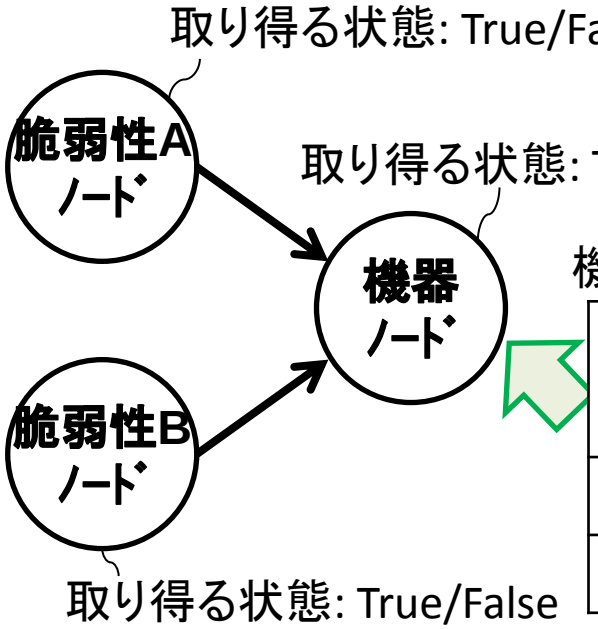
© Hitachi, Ltd. 2017. All rights reserved.

3.6. 条件付き確率表の設定 (2)

HITACHI
Inspire the Next

■ ベイジアンネットワークで計算するため，条件付き確率表を設定

– 各機器の各脆弱性ノードの攻撃が成功すれば，必ずその機器が侵害されると仮定し，脆弱性ノードには，必ず1を設定*



どちらかの脆弱性攻撃が成功すれば，
必ず機器が侵害されると仮定

機器ノードの条件付き確率表

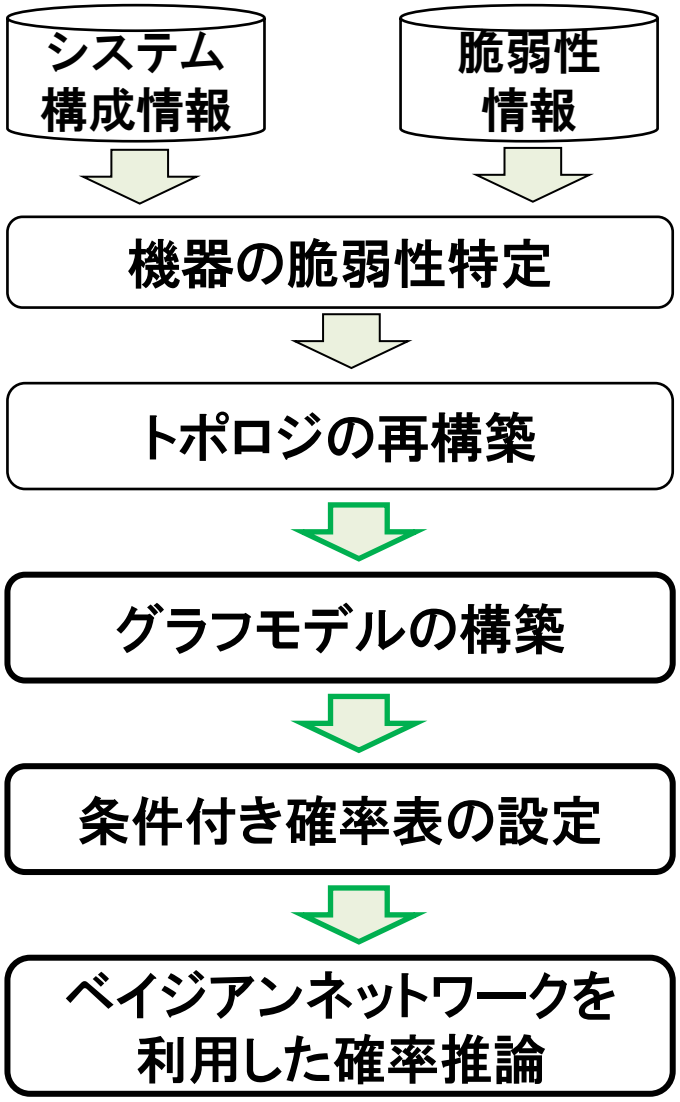
	脆弱性A	True		False	
	脆弱性B	True	False	True	False
True		1.0	1.0	1.0	0
False		0	0	0	1.0

© Hitachi, Ltd. 2017. All rights reserved.

3.7 セキュリティリスク評価処理フロー　まとめ

HITACHI
Inspire the Next

1. システム構成情報の各機器のソフトウェアに合致する脆弱性情報を特定
2. システム構成情報のネットワーク情報からトポロジの再構築
3. ネットワーク到達性と各機器の脆弱性からグラフモデルを構築
4. 各機器ノード、各脆弱性ノードに条件付き確率表を設定
5. ベイジアンネットワークを利用して確率推論により、各ノードへの周辺確率を攻撃到達可能性として算出



© Hitachi, Ltd. 2017. All rights reserved.

HITACHI
Inspire the Next

サイバーセキュリティ脅威対策のための セキュリティリスク評価システムのご紹介

Contents

1. 研究の背景と目的
2. 脆弱性リスク評価技術
   - 標準方式(CVSS)とその課題
3. 提案するセキュリティリスク評価技術[CSEC68、IPSJ57]
4. ビジネスリスク評価システムのご紹介[CSEC74]
5. デモ
6. まとめ

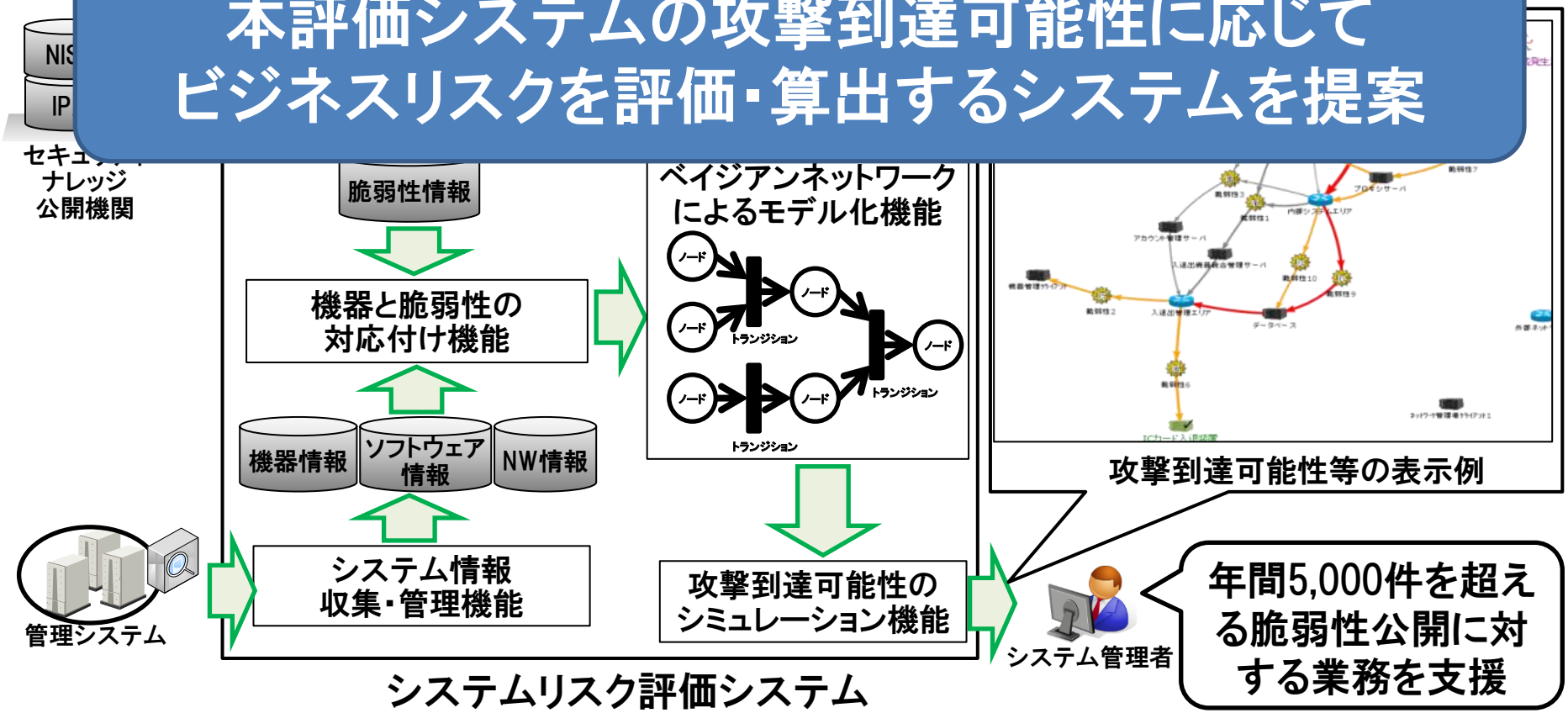
[CSEC68] 磯部、杉本「ベイジアンネットワークを利用した動的モデリングによるセキュリティリスク評価システムの開発」
[CSEC74] 磯部、杉本、仲小路「サイバーセキュリティ脅威対策のためのビジネスリスク評価システムの提案」
[IPSJ57] 杉本、磯部、仲小路「サイバー攻撃の侵入経路を考慮したセキュリティリスク評価技術」情処論文Vol.57 No9(2016.9)

3.1 攻撃経路を考慮したリスク評価

HITACHI
Inspire the Next

- 脆弱性の所在を特定し、システムトポロジに応じて自動でベイジアンネットワークモデル化。各機器への攻撃到達可能性をシミュレート。
- 各システム管理者に任されていたCVSSの環境評価の一部(TD:システムの影響範囲)や攻撃到達可能性評価を自動化し、緊急対処が必要な機器を特定

本評価システムの攻撃到達可能性に応じて
ビジネスリスクを評価・算出するシステムを提案

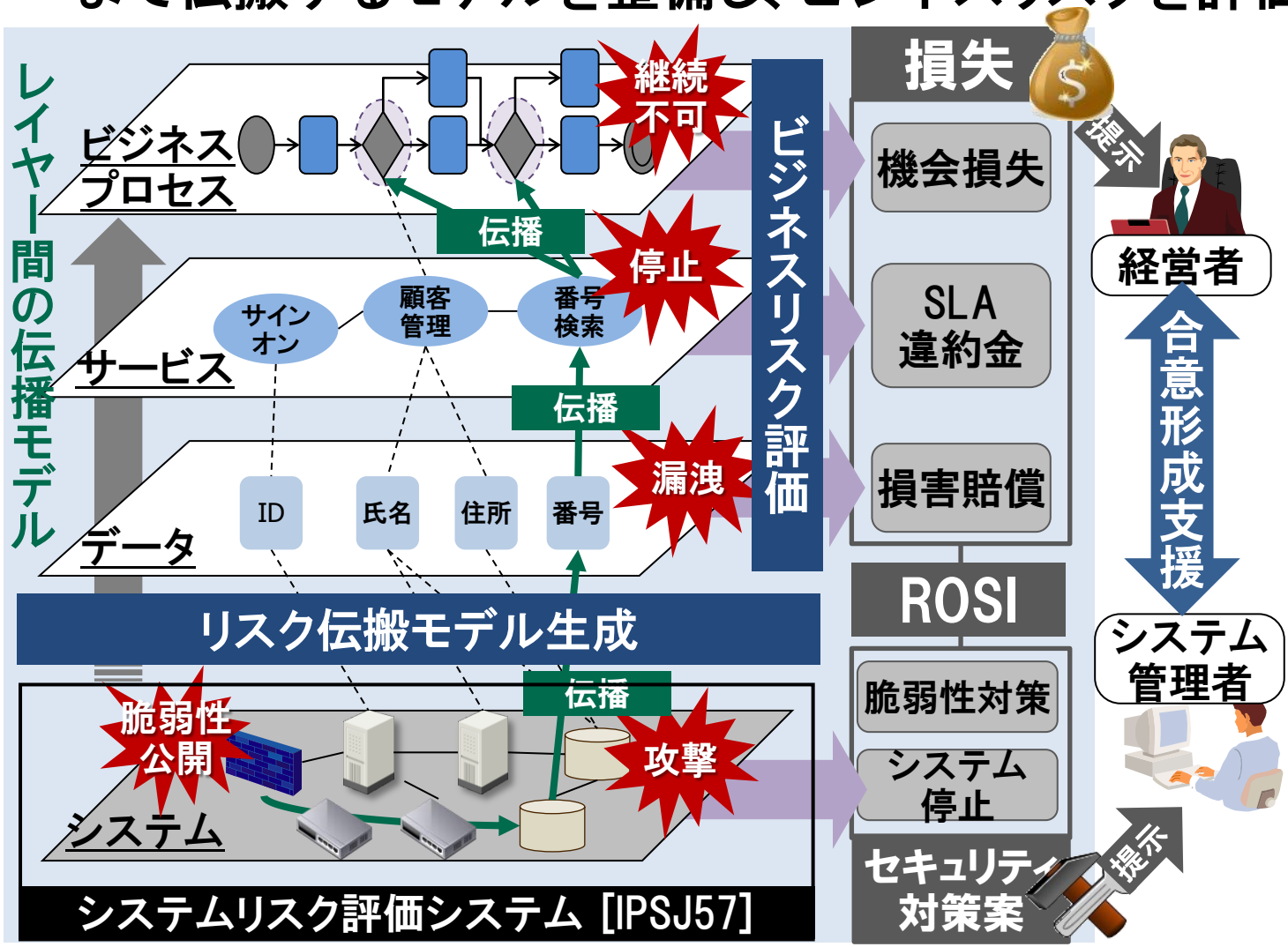


© Hitachi, Ltd. 2017. All rights reserved.

4.1 ビジネスリスク評価システムの概要

HITACHI
Inspire the Next

■システムリスク評価システムの攻撃到達可能性をビジネスプロセスレイヤーまで伝搬するモデルを整備し、ビジネスリスクを評価



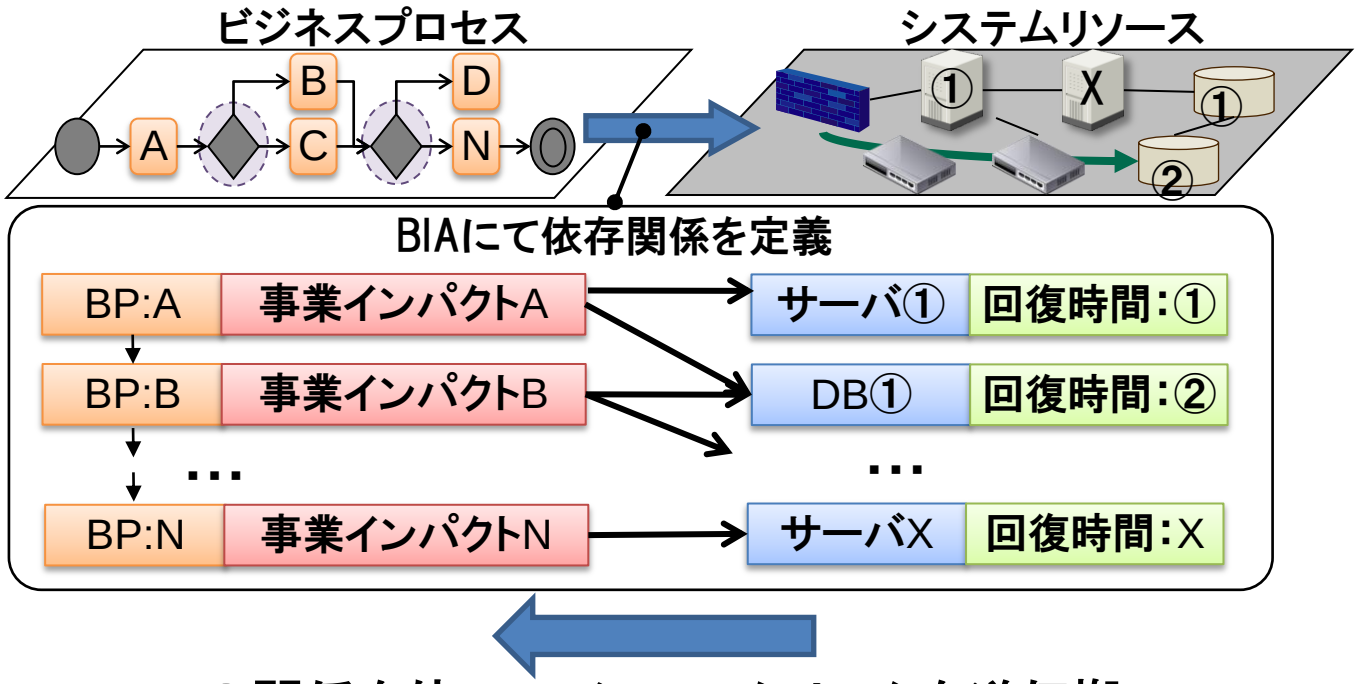
© Hitachi, Ltd. 2017. All rights reserved.

4.2 ビジネス影響伝搬モデル

HITACHI
Inspire the Next

■ 例えば、NIST SP800-34 Rev.1に基づきBIAを実施、結果を活用

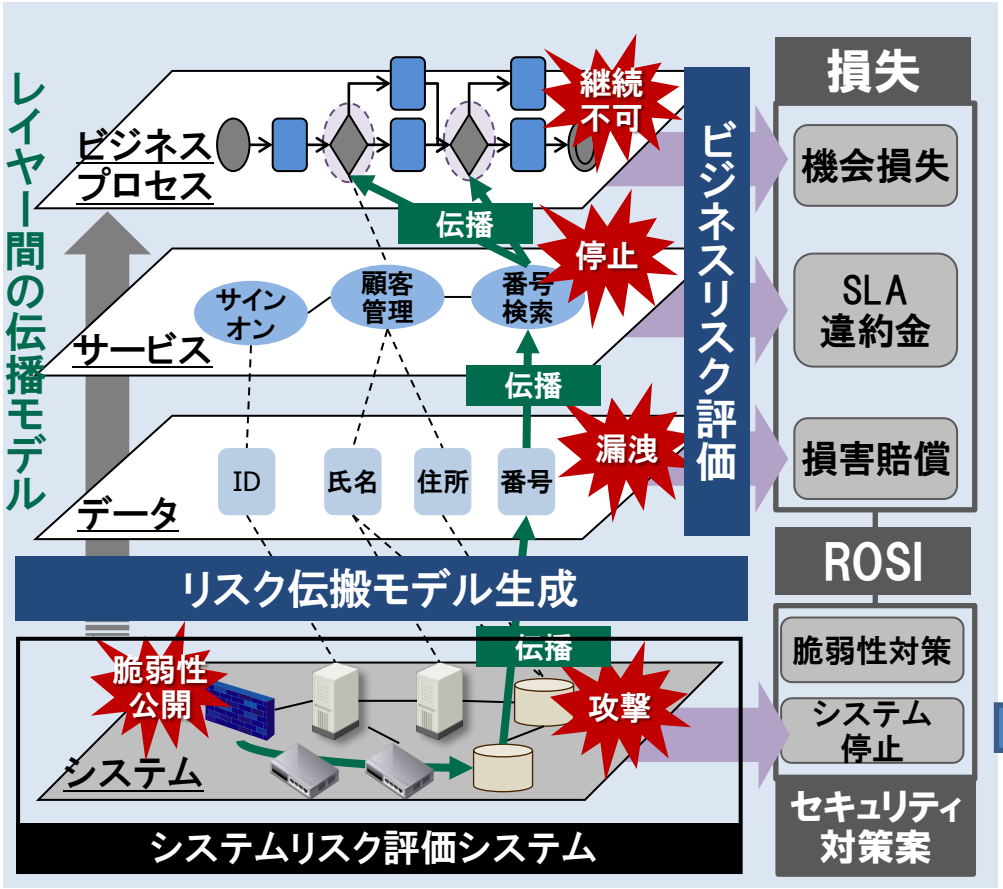
1. ミッションあるいはビジネスプロセスを特定し、業務阻害時の復旧必要性とその許容停止時間を明確化
2. システムリソースとビジネスプロセスの**依存関係を特定**してシステムリソースの復旧要件を明確化
3. システムリソースの復旧優先度を明確化



この関係を使って、システムリスクを逆伝搬

© Hitachi, Ltd. 2017. All rights reserved.

4.3 セキュリティ対策効果(ROSI)の算出モデル



想定損失算出モデル例

可用性

$$BR_a = \underline{Pr} \times \underline{RT} \quad 等$$

単位時間当たりの利益や便益　回復時間

秘匿性

$$BR_c = \underline{C_V} \times \underline{Qc} \quad 等$$

レコードあたりの価値　レコード数

…

人件費

$$EC_{wl} = \sum_{\underline{T_{ar}<D_{ar}}} \underline{D_{wl}}$$

各機器の対策人件費

攻撃到達可能性が高い機器

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

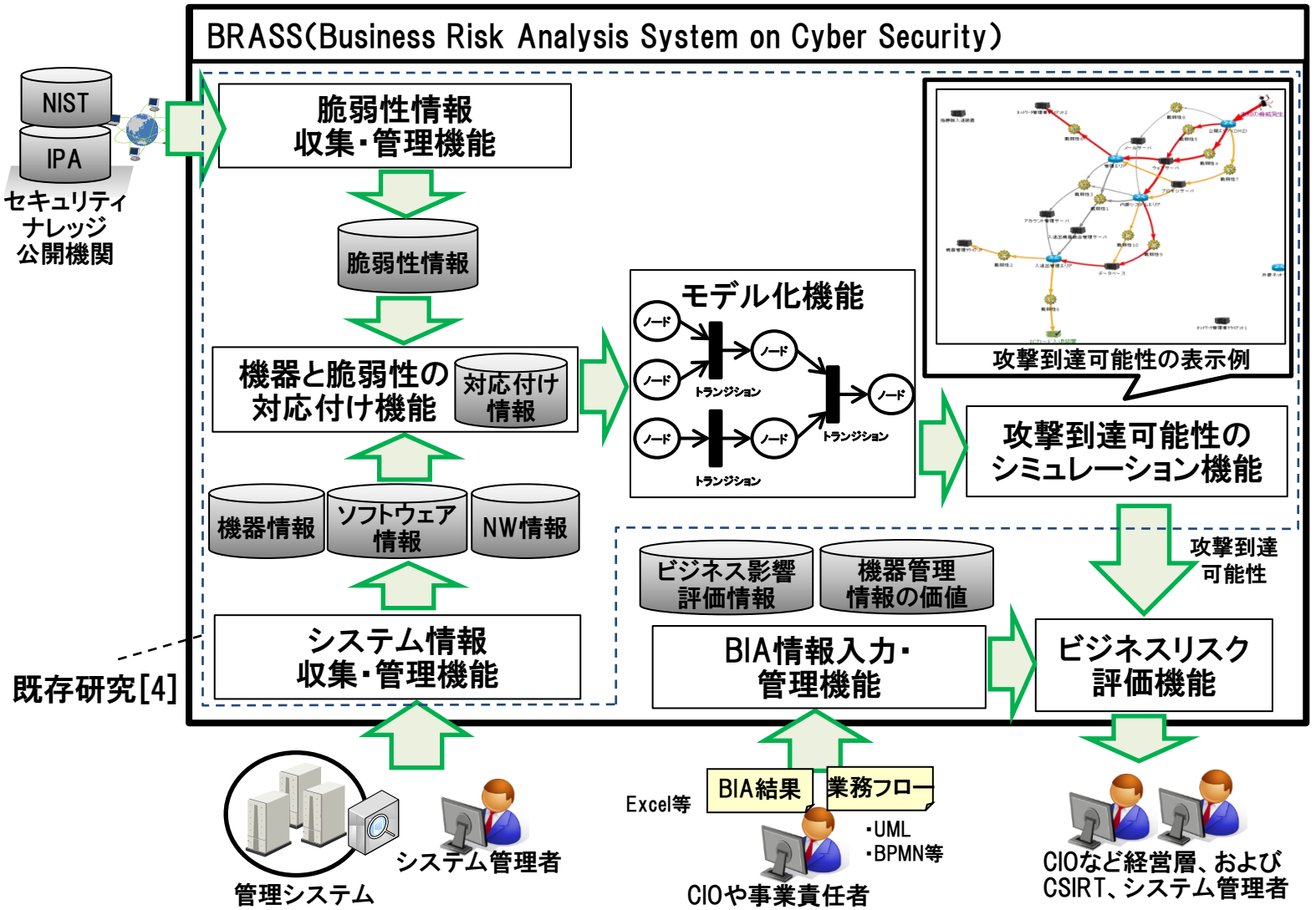
対策導入費

© Hitachi, Ltd. 2017. All rights reserved.

4.4 ビジネスリスク評価システムの機能構成

HITACHI
Inspire the Next

■BIA情報を入力・管理し、ビジネスリスク評価を行うプロトを開発



© Hitachi, Ltd. 2017. All rights reserved.

HITACHI
Inspire the Next

セキュリティリスクマネジメント態勢を支援する リスク評価・リスク可視化技術

Contents

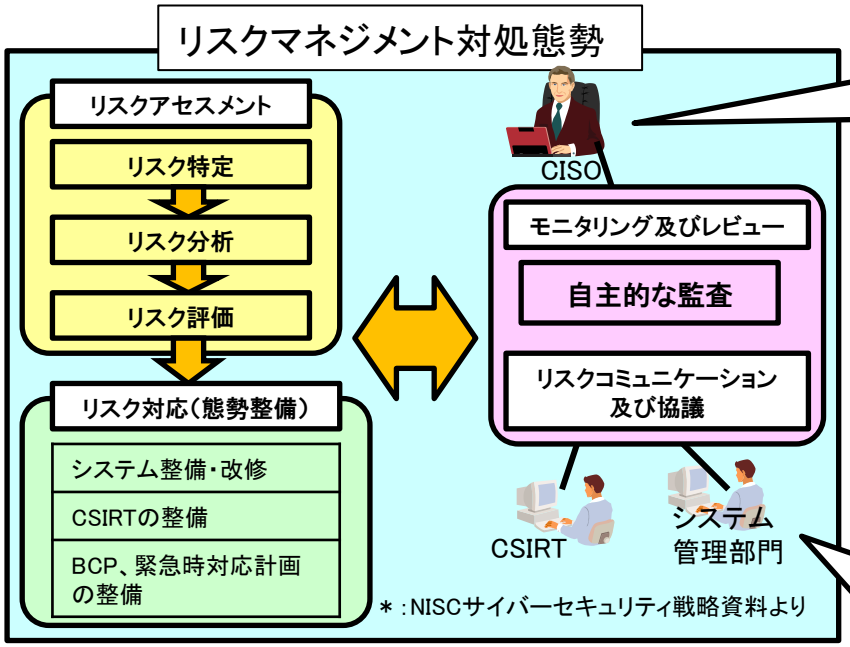
1. 研究の背景と目的
2. 脆弱性リスク評価技術
   - 標準方式(CVSS)とその課題
3. 提案するセキュリティリスク評価技術[CSEC68、IPSJ57]
4. ビジネスリスク評価システムのご紹介[CSEC74]
5. デモ
6. まとめ

[CSEC68] 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」
[CSEC74] 磯部、杉本、仲小路「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」
[IPSJ57] 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 No9(2016.9)

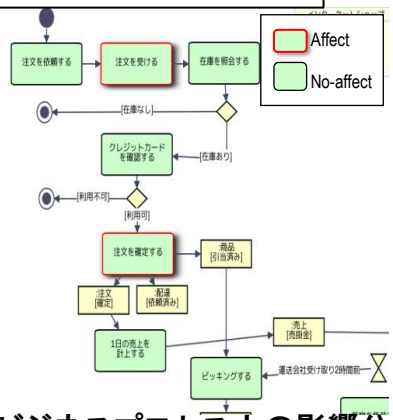
5 デモシナリオ

HITACHI
Inspire the Next

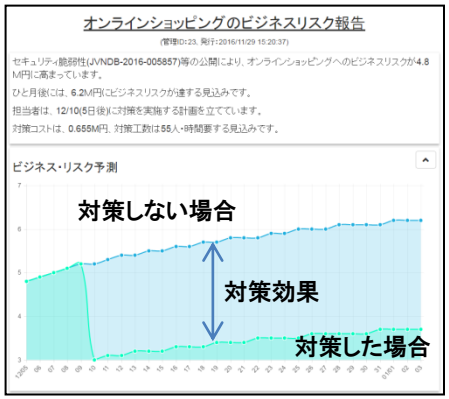
◆NISCサイバーセキュリティ戦略により、リスクマネジメント態勢として、セキュリティ監査・CISRT構築が進み、CISOを中心としたセキュリティリスク管理を行う重要インフラを想定
◆システム管理を行う現場とCISOとのリスクコミュニケーションを本技術で支援



CISO(経営層)向け

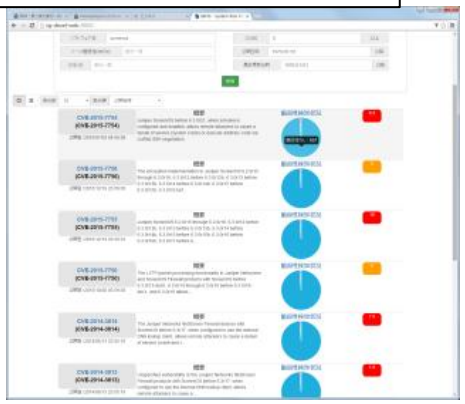


ビジネスプロセス上の影響分析

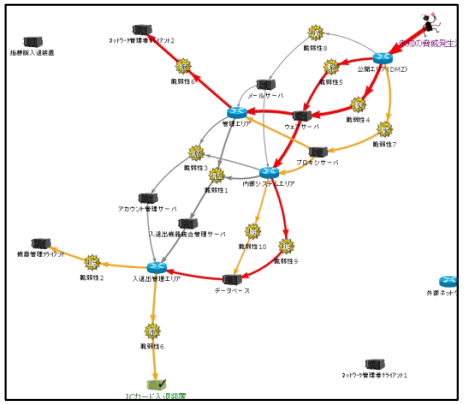


対策効果＆ビジネスリスク分析

システム管理部門向け



脆弱性リスク特定ダッシュボード



攻撃経路シミュレーション

デモ

© Hitachi, Ltd. 2017. All rights reserved.

6 まとめ

HITACHI
Inspire the Next

■「ベイジアンネットワークを用いた攻撃経路を考慮したシステムリスク評価技術」を開発
- 資産管理情報と脆弱性情報を照合し、脆弱性があるサーバ・デバイスを特定
- サーバ・デバイスのネットワークトポロジより攻撃経路を分析。攻撃到達可能性により、システム内のリスクを評価
- 脆弱性毎の対策効果を攻撃到達可能性の低減により可視化

→ 対策の効果を可視化することで、対策の優先度判断を支援

■ 上記と連携した「ビジネスリスク分析技術」を開発
- 攻撃到達可能性の高いシステムリソースを想定される攻撃範囲と仮定
- これら機器停止による想定損失を算出（デモでは可用性に関する阻害）
- これら機器からのデータ漏えいなどの情報セキュリティ上の損失のモデルも例示
- 対策を実施することによるビジネスリスク低減効果も可視化

→ 経営者判断に資する情報も提示、組織内のリスクコミュニケーションを支援

© Hitachi, Ltd. 2017. All rights reserved.

HITACHI

Inspire the Next