第四十五回ネットワーク仮想化（NV）研究会

脅威と対抗策による セキュリティモデル表現を用いた セキュアシステム自動設計技術

2023/11/21

NEC, セキュアシステムプラットフォーム研究所
堀地亮佑, 黒田貴之

© NEC Corporation 2022

サマリ

「対抗策」の概念を用いた
セキュアシステム自動設計技術について

◆ 背景

- ICTシステムの設計を自動化する技術として，セキュアシステム自動設計技術が知られている．

◆ 課題

- 従来の自動化技術では脅威の存在不存在によるセキュリティ評価のみを実施しており，「脅威に対して対策を講じたセキュアなシステム」を設計することが困難であった．

◆ 提案

- 新たに「**対抗策**」という概念を導入し，「脅威に対して対策を講じたセキュアなシステム」の表現方法を有する新規のセキュアシステム自動設計技術を提案する．

◆ 評価

- ある入力要件において従来手法と提案手法での自動設計結果を比較する．

© NEC Corporation 2022

目次

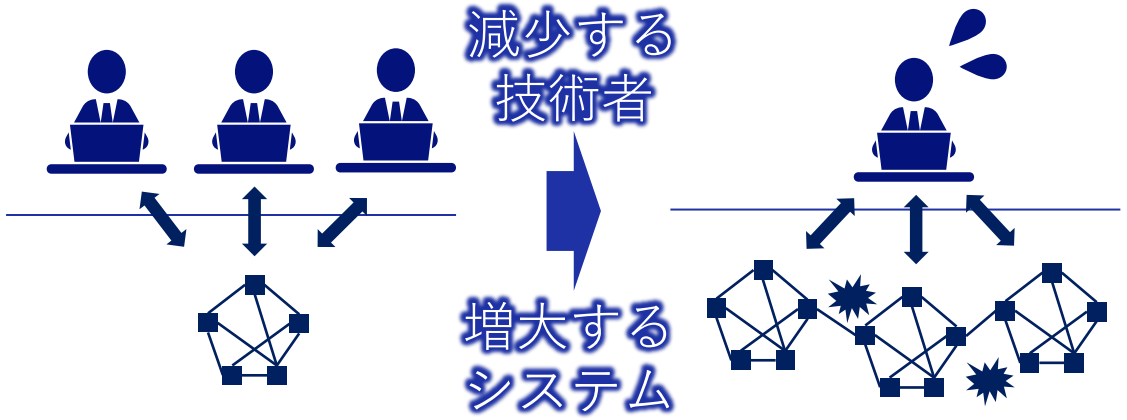
1. セキュアシステム自動設計の概要と課題
2. 脅威と対抗策によるセキュリティモデル
    1. 脅威モデル
    2. 対抗策モデル
    3. 攻撃パスとセキュリティ判定方法
3. 実験結果
4. まとめ

1. セキュアシステム自動設計の概要と課題

[1/5] 背景

ICTシステムの運用に掛かる負荷の増大 → 自律運用技術への期待

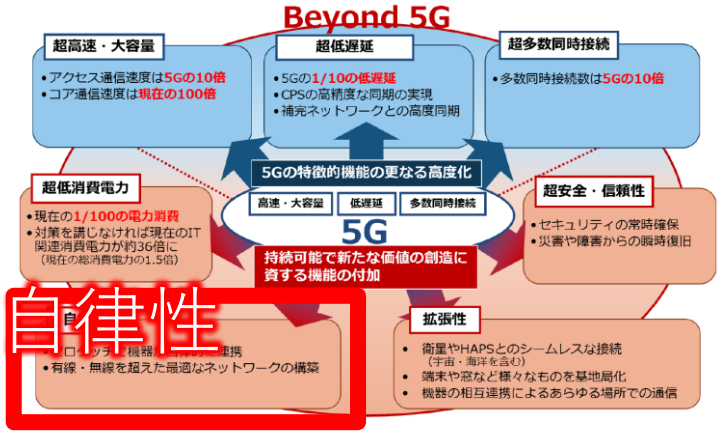
運用に掛かる負荷の増大



- **2030年に国内IT人材78万人不足**
  ※ 経産省, IT人材白書
- 国内IT市場規模: CAGR 2.6% (FY'20-25)
  法人向け5G関連: CAGR 198%(FY'20-26)
  ※ IDC Japan, 国内法人向け5G関連IT市場予測

技術動向: 自律運用の研究開発

総務省, Beyond 5G推進戦略



国際標準団体による提言事例

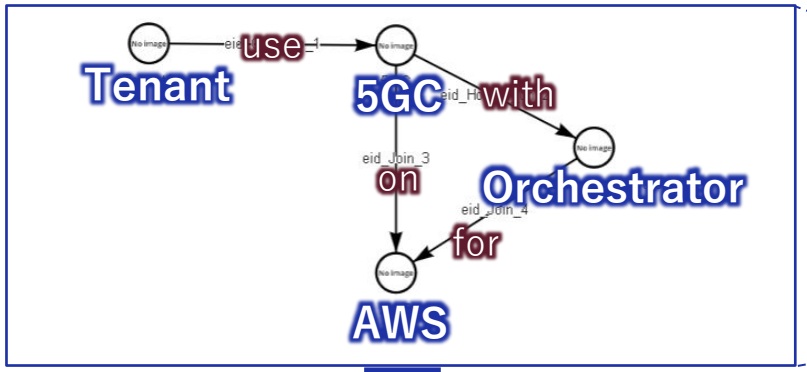
- TMForum: Autonomous Networks
- ETSI: Zero touch management(ZSM)
- ITU-T: Autonomous Networks
- O-RAN: RAN Intelligent Controller(RIC)

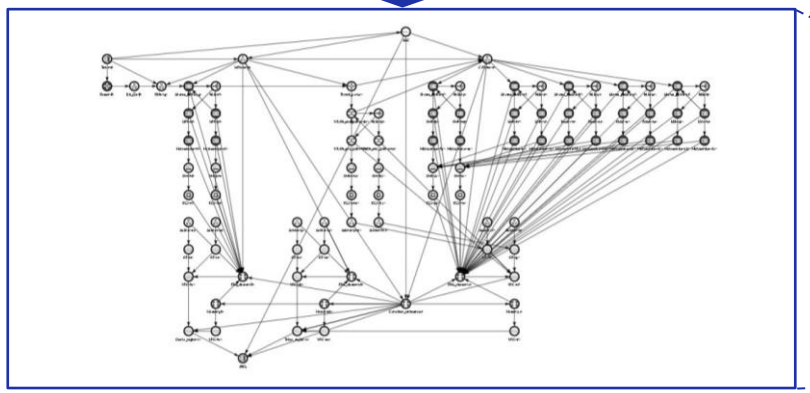
© NEC Corporation 2022

[2/5] NECで開発中のシステム自動設計の概要

「抽象的なシステム要件」から「具体的なシステム構成」を出力する技術

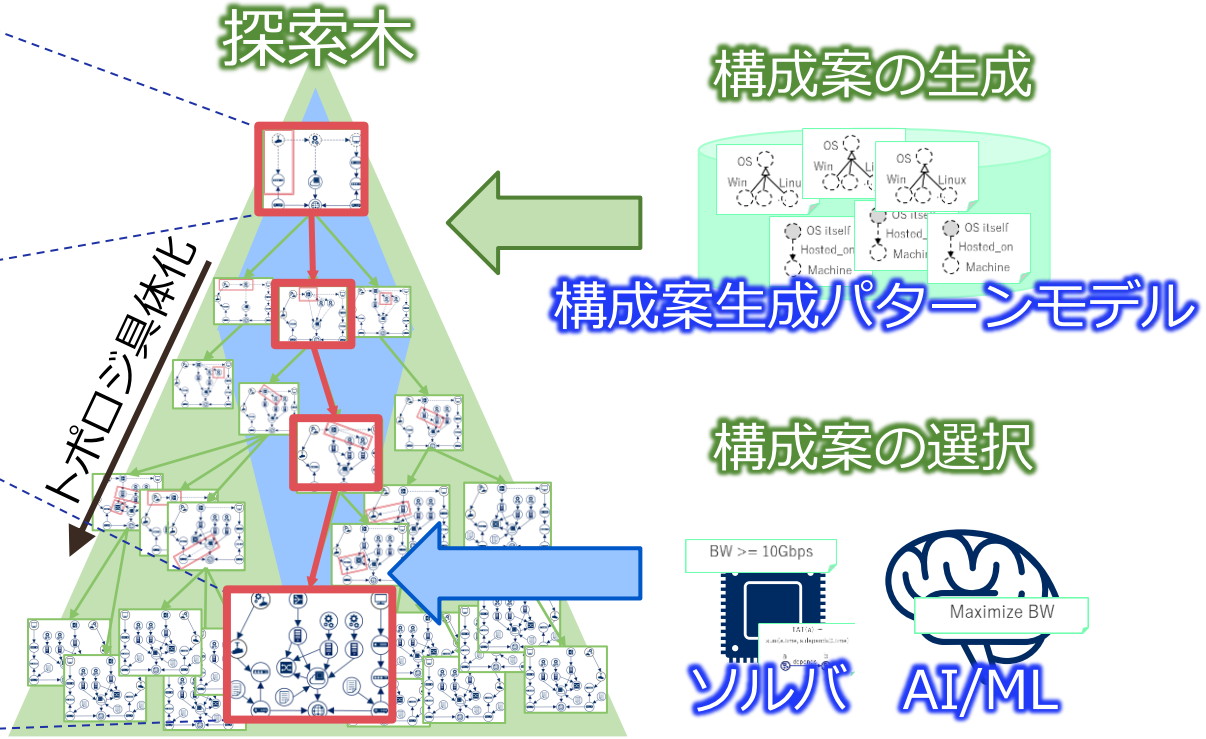
入力: 抽象的なシステム要件





出力: 具体的なシステム構成

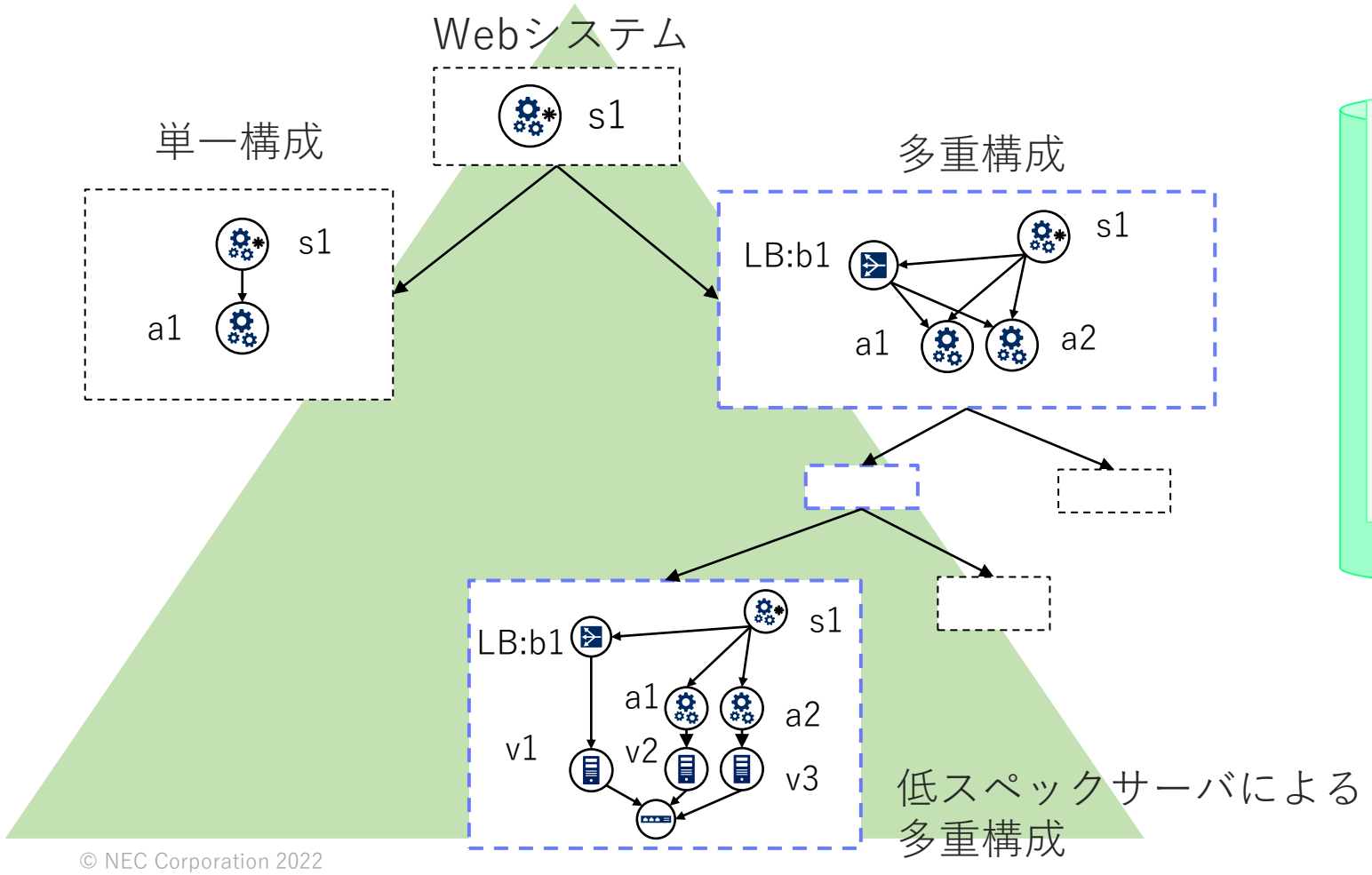
システム自動設計技術

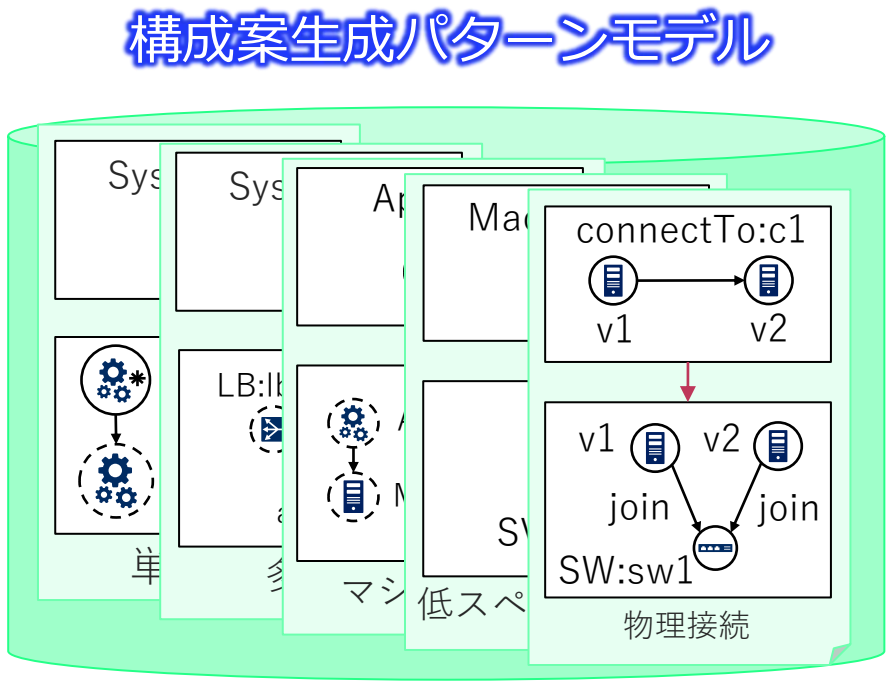


© NEC Corporation 2022

[3/5] システム自動設計の動作原理

構成案の生成と評価を繰り返し
完全に具体化された構成案を導出





設計AI

© NEC Corporation 2022
\Orchestrating a brighter world NEC

[4/5] 従来のセキュアシステム自動設計の概要

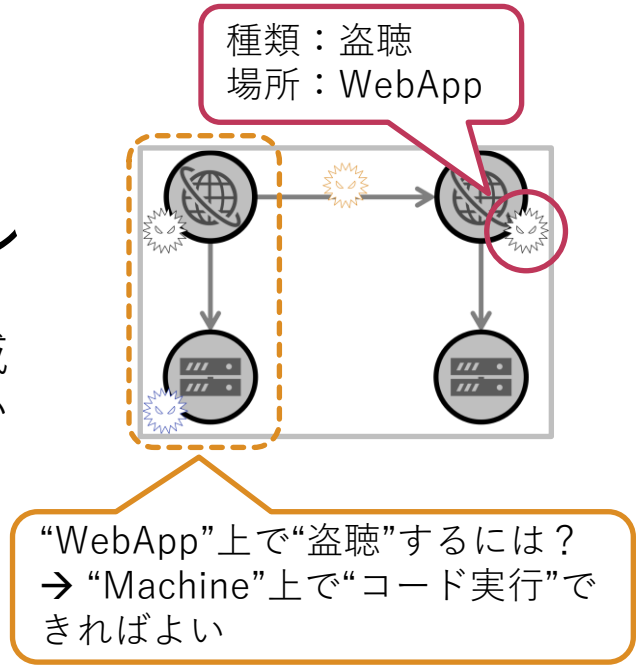
「脅威モデル」によるセキュリティ評価を組み込んだ自動設計技術

データ：脅威モデル

脅威型モデル
- 脅威の種類(型)
- 脅威の存在場所

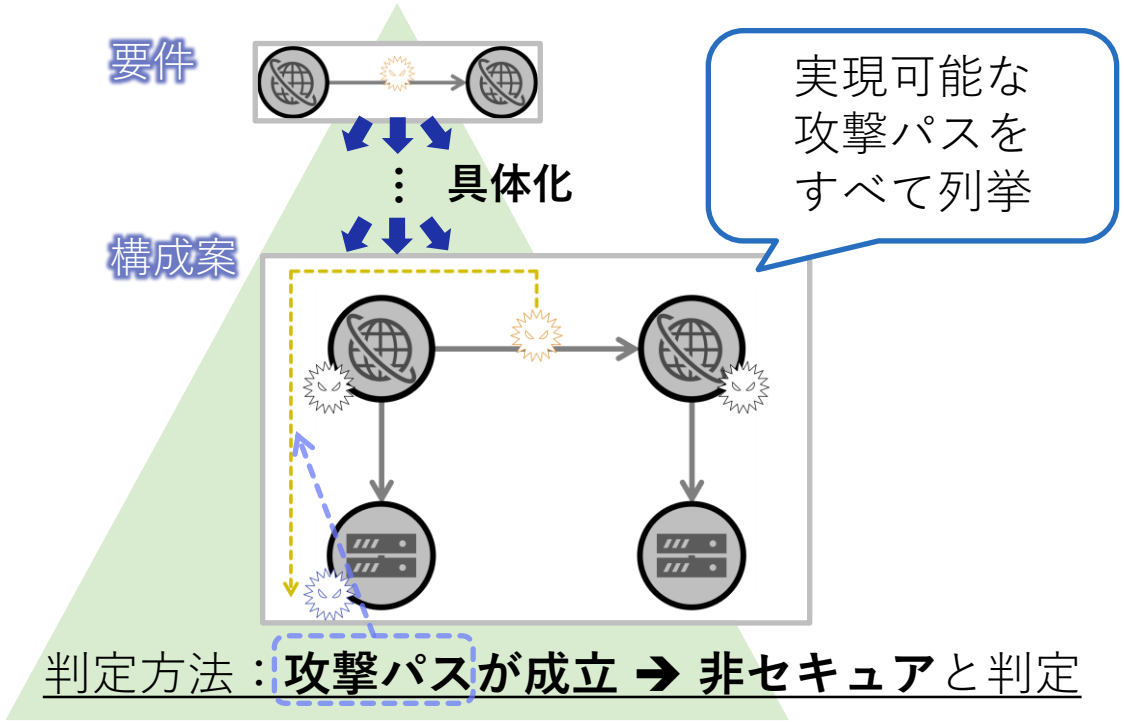
脅威実現方法モデル
ある脅威を実現するには、他のどの脅威を実現すればよいか

脅威型モデルの例



脅威実現方法モデルの例

動作：脅威の具体化と攻撃パスの生成



攻撃パス：サイバー攻撃実現方法を示す脅威の鎖状ルート

© NEC Corporation 2022
\Orchestrating a brighter world NEC

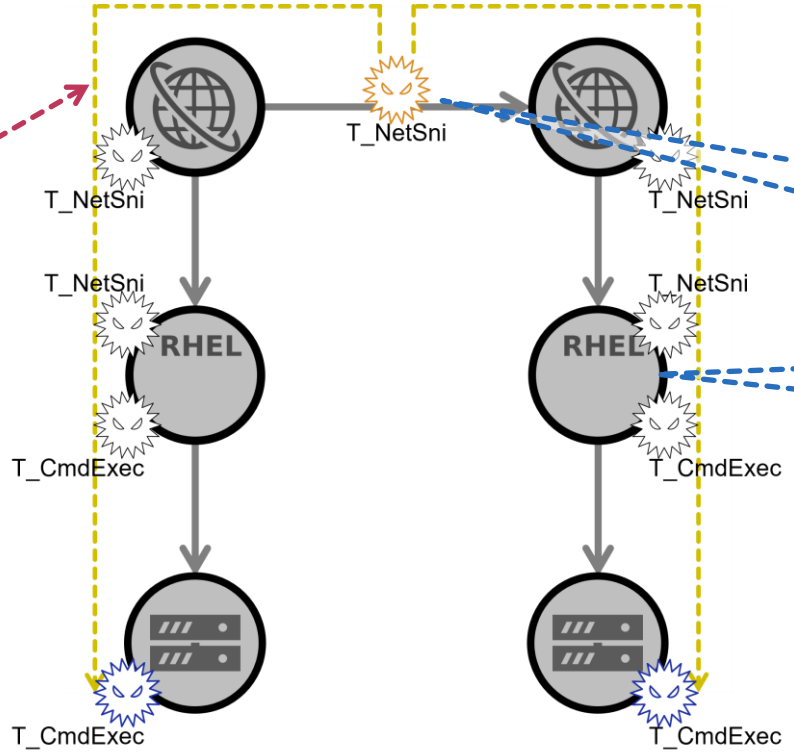
[5/5] 従来のセキュアシステム自動設計の課題

「脅威に対して対策を講じたシステム」の自動設計

従来のセキュア自動設計の場合

攻撃パスが成立

「セキュア」と判定されるのは
攻撃パスが存在しない構成のみ
↓
攻撃パスが存在⇒非セキュア



実世界における手動設計の場合

「通信内容を暗号化」することで
盗聴の脅威を対策

「最新OSバージョン」を利用して
攻撃コード実行の脅威を対策

攻撃パスは存在するが
適切にセキュリティ対策を
実施しているためセキュア

「脅威に対して対策を講じているためセキュアであるシステム」
を自動設計することができなかった。

© NEC Corporation 2022
\Orchestrating a brighter world NEC

2. 脅威と対抗策によるセキュリティモデル

1. 脅威モデル
2. 対抗策モデル
3. セキュリティ判定方法

2.1. 脅威モデル

脅威型モデル＋脅威実現方法モデル

[1/2] 脅威モデル

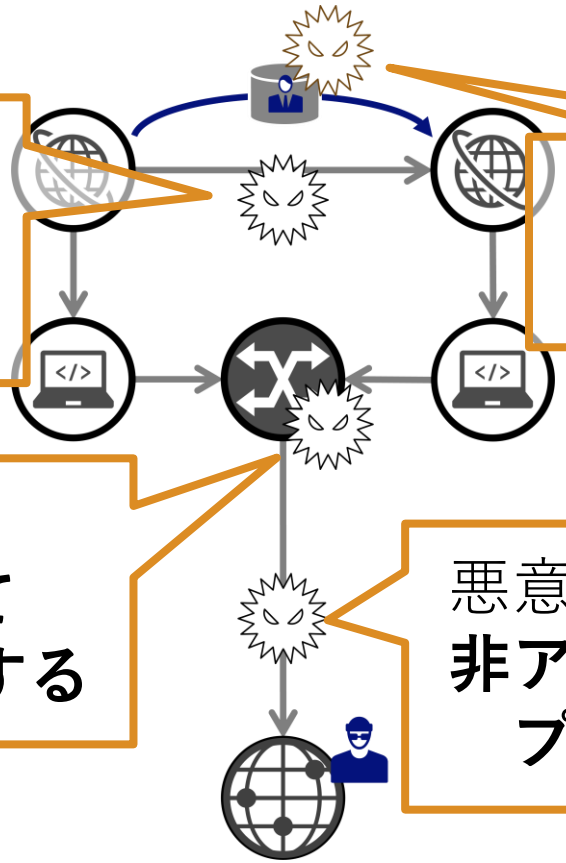
脅威(threat)：攻撃者が実行する特定の操作を表現するエンティティ

◆脅威モデル

攻撃者の実行する
操作を表現するモデル.
以下の2要素からなる.

- 脅威型モデル
  脅威の種類(型)と
  脅威の存在場所を
  定義したモデル
- 脅威実現方法モデル
  ある脅威を実現する
  ために必要となる
  別脅威の情報を
  定義したモデル

脅威型モデル例



アプリ同士の
通信内容を
盗聴する

通信でやり取りされる
個人情報を盗む

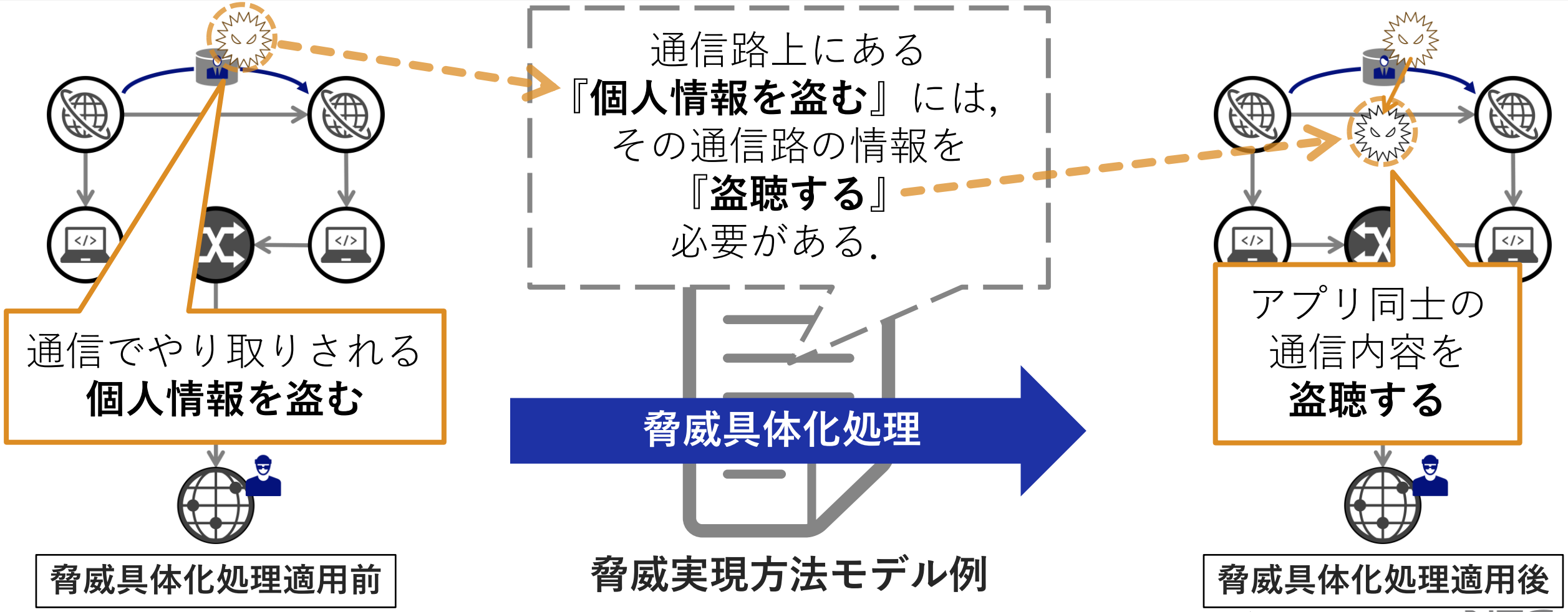
ルータにて
CLIを用いて
コードを実行する

悪意のあるデータの送信に
非アプリケーションレイヤ
プロトコルを使用する

© NEC Corporation 2022
\Orchestrating a brighter world NEC

[2/2] 脅威実現方法モデルと脅威具体化処理

脅威具体化処理：ある脅威の実行に必要となる別の脅威を生成する処理



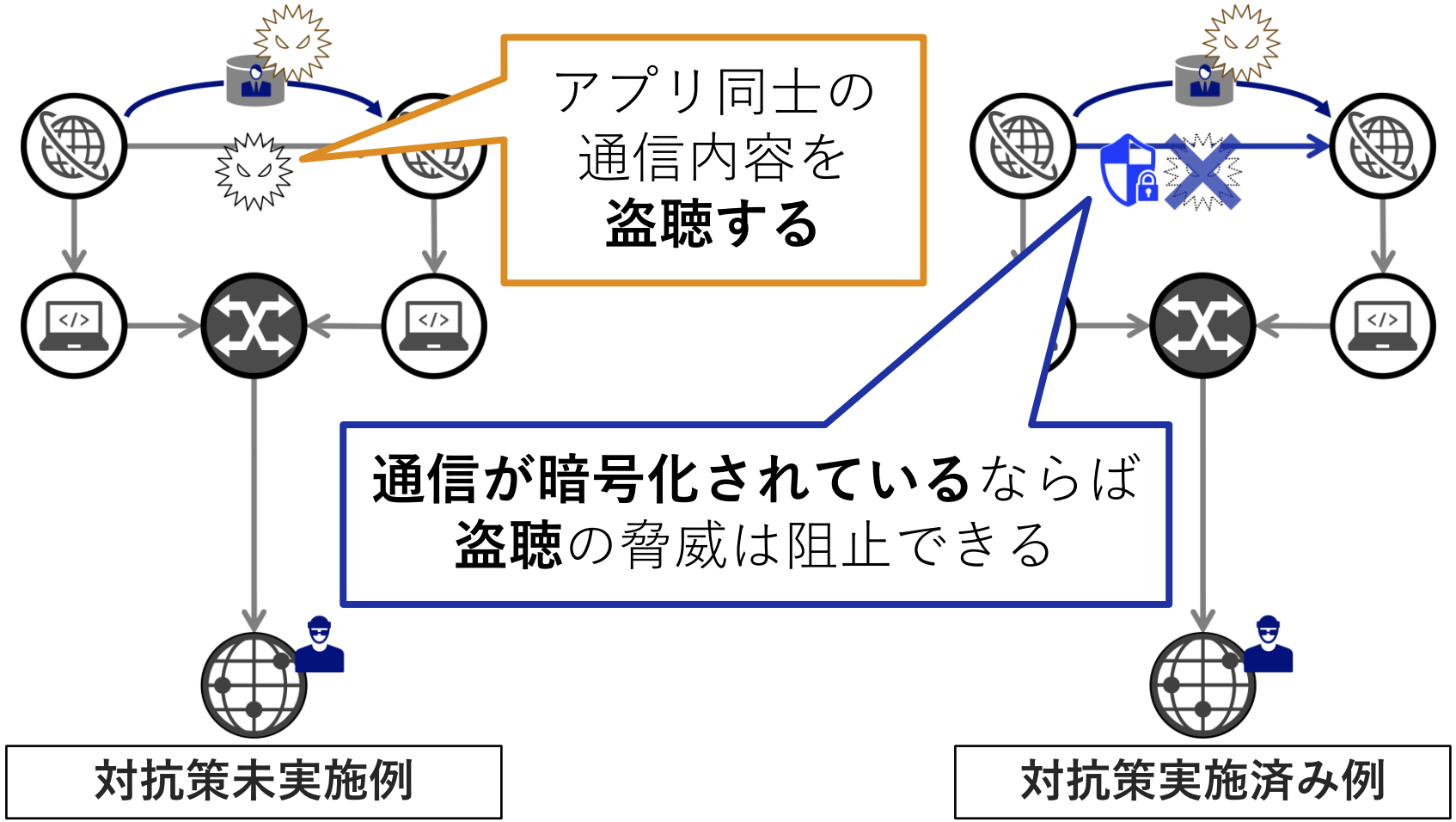
© NEC Corporation 2022
\Orchestrating a brighter world NEC

2.2. 対抗策モデル

[1/2] 対抗策モデル

対抗策(mitigation)：脅威を阻止・緩和する手法あるいは機能

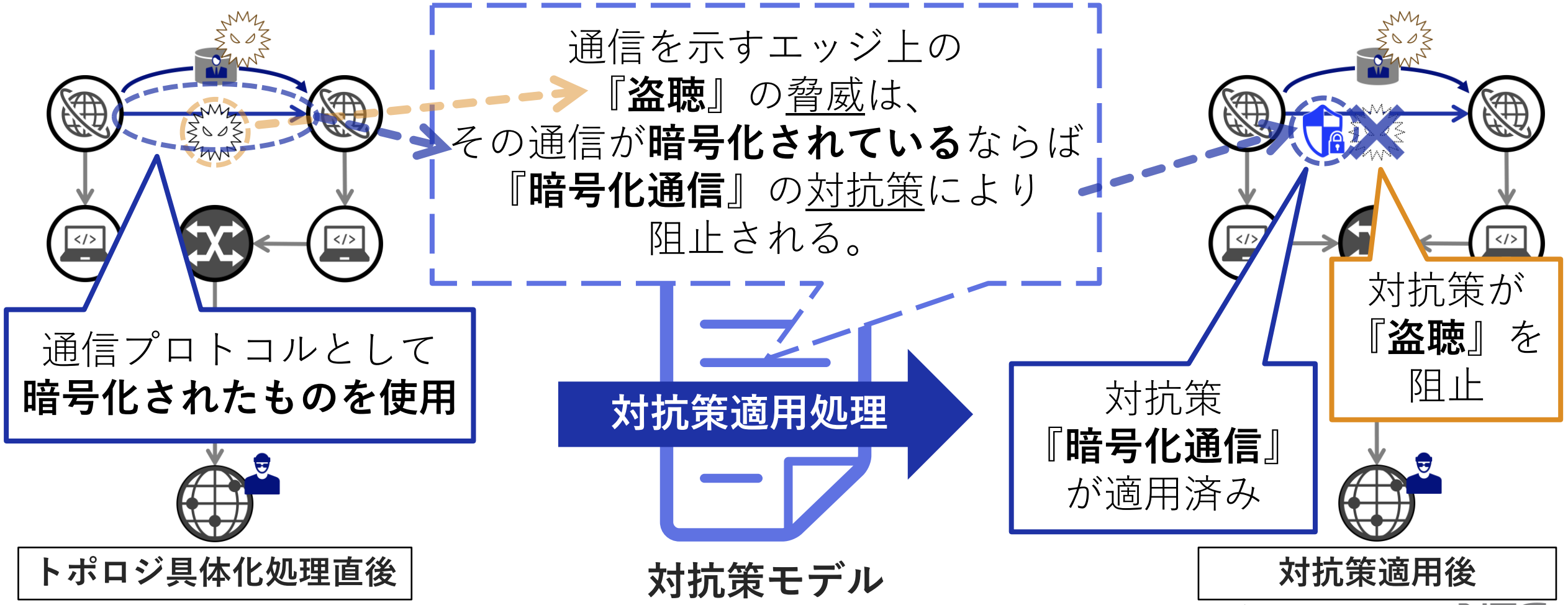
◆対抗策モデル
システム構成に存在する
セキュリティ機能を
表現するモデル.
対抗策を実施することで
対応脅威を阻止・緩和
することができる.



© NEC Corporation 2022

[2/2] 対抗策の運用仕様

対抗策適用処理：対抗策の情報をトポロジに適用する処理



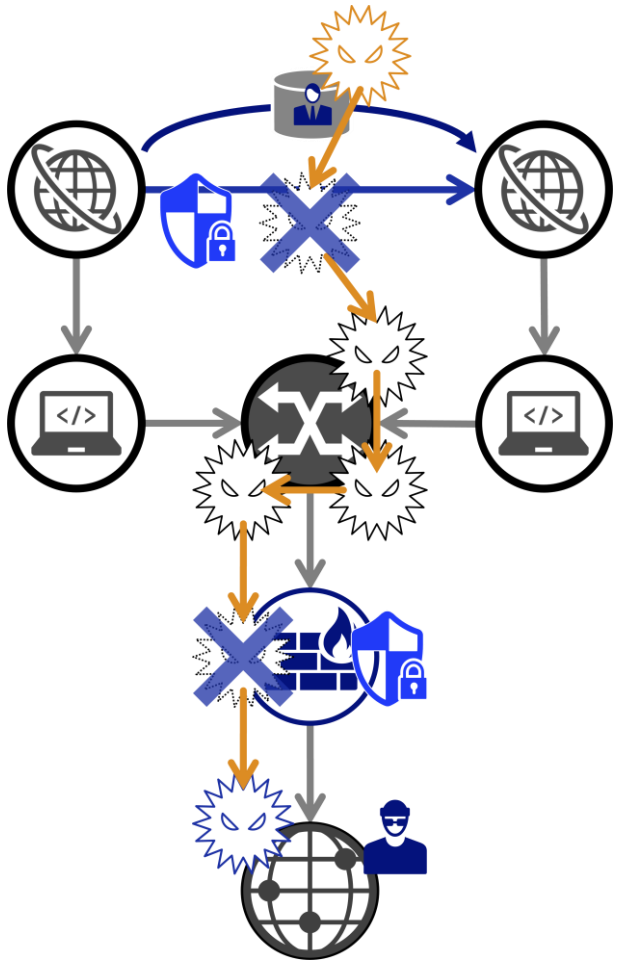
© NEC Corporation 2022
\Orchestrating a brighter world NEC

2.3. 攻撃パスとセキュリティ判定方法

[1/3] 攻撃パスとその有効性

攻撃パス：攻撃終点型脅威から攻撃起点型脅威への脅威の鎖状ルート

システム自動設計と並行して
脅威具体化処理と
対抗策適用処理を
繰り返していくと…



攻撃終点型脅威：
（最終的に達成されたら困る脅威）

攻撃起点型脅威：
（攻撃者が明確に実行可能な脅威）

上記以外の脅威：

攻撃パスの有効性：
当該攻撃パスを構成する脅威に紐づく対抗策の有無により決定

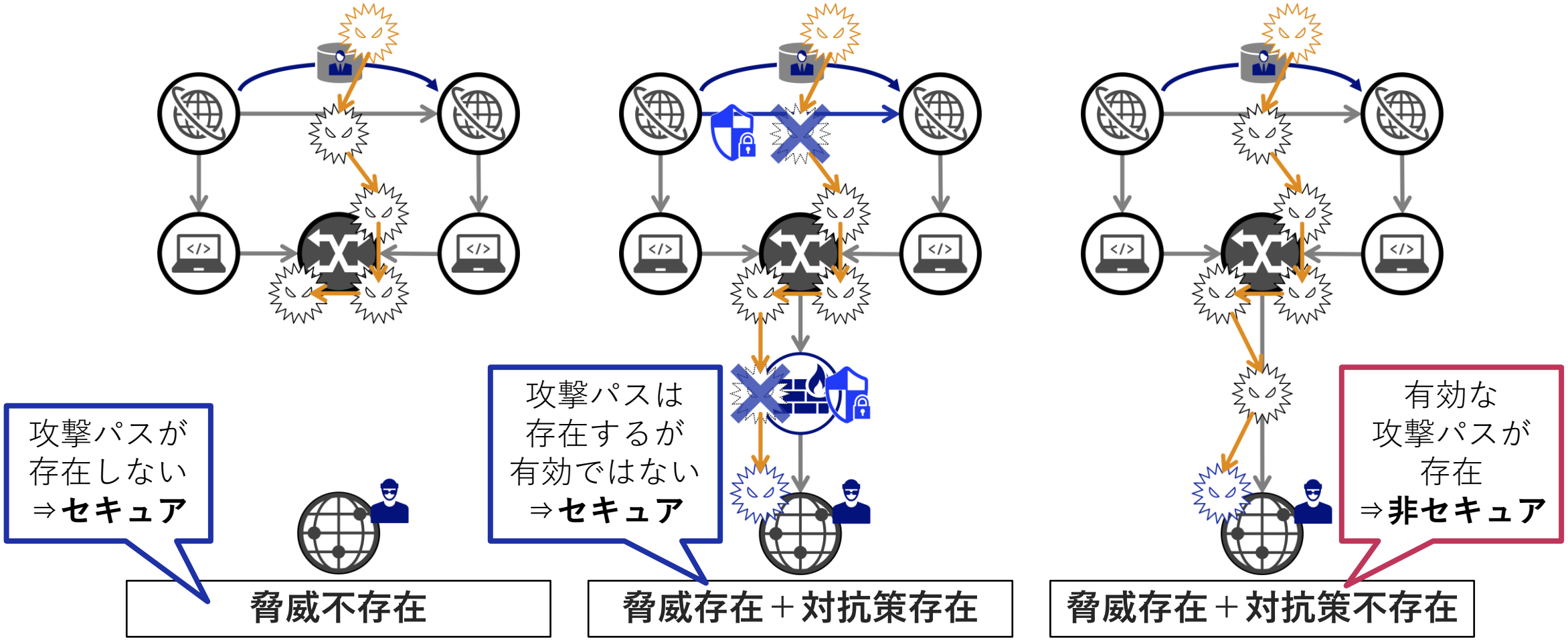
- 攻撃パスを構成する脅威全てに対抗策が紐づいていない
  →有効な攻撃パス

- 攻撃パスを構成する脅威のうち1つ以上の脅威が対抗策により対策済み
  →有効でない攻撃パス
  （＝無効な攻撃パス）

© NEC Corporation 2022
\Orchestrating a brighter world NEC

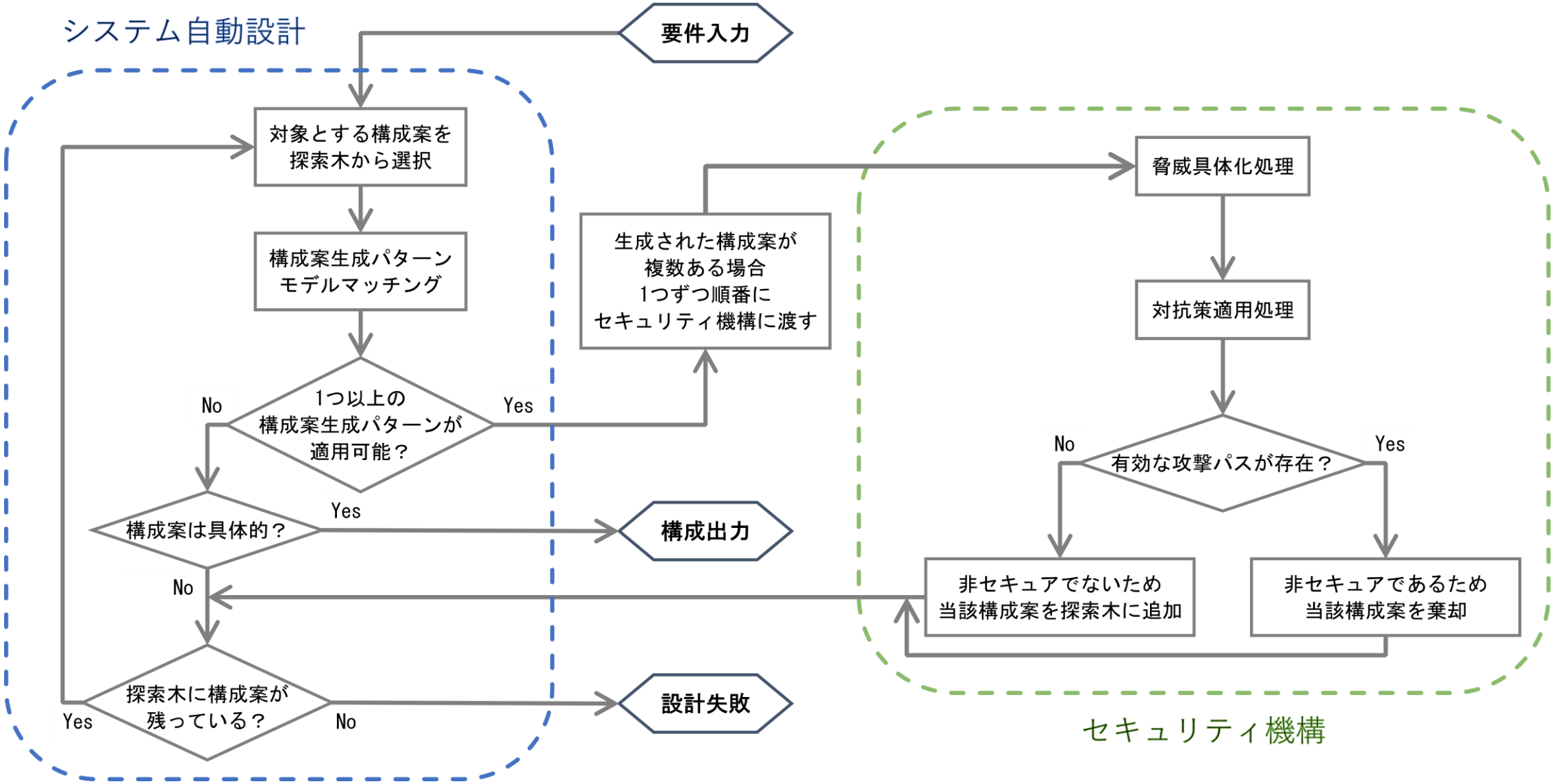
[2/3] 攻撃パスの有効性に基づくセキュリティ評価

「有効な攻撃パスが存在する」⇒構成は非セキュア



© NEC Corporation 2022
\Orchestrating a brighter world NEC

[3/3] システム全体のフローチャート

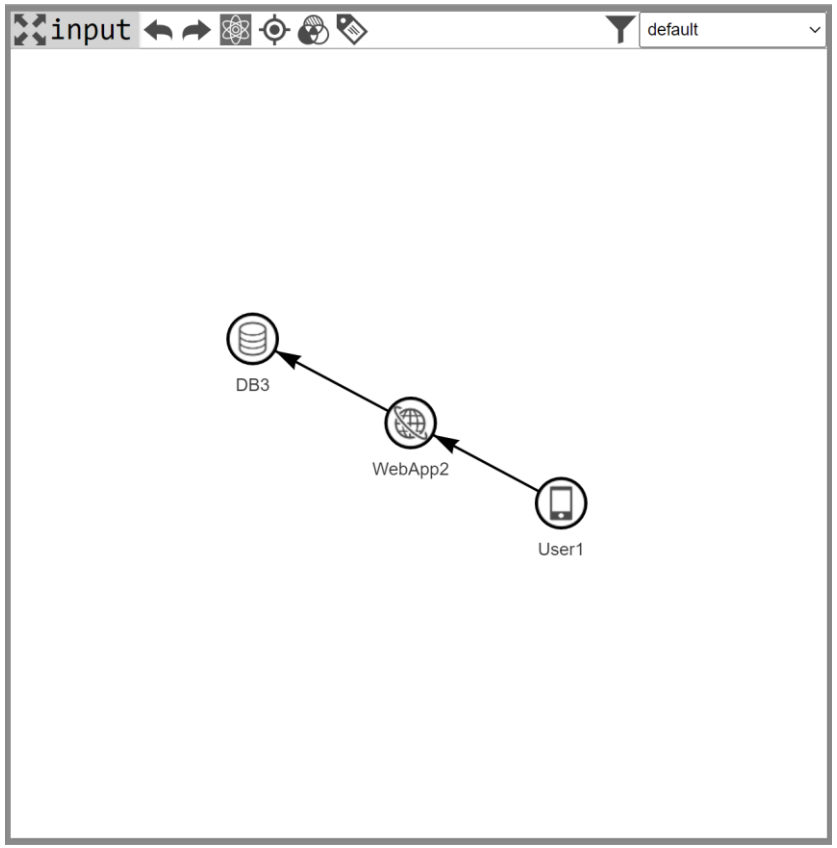


© NEC Corporation 2022
\Orchestrating a brighter world NEC

3. 実験結果

[1/4] 実験条件

入力要件



- DB上に「**データ破壊**」の脅威が存在
- DB上の「データ破壊」の脅威は、接続されたOS上の「**unix shellによるコード実行**」の脅威により実現可能
- 物理マシン上の「unix shellによるコード実行」の脅威は、接続されたSwitch上の「**非アプリケーションレイヤプロトコルによる通信**」により実現可能

⋮

脅威モデル

対抗策モデル

- 「非アプリケーションレイヤプロトコルによる通信」の脅威は、SwitchとRouter間の通信経路にFirewallとNIPS*を接続することで「**ネットワーク不正侵入防止**」の対抗策により阻止可能

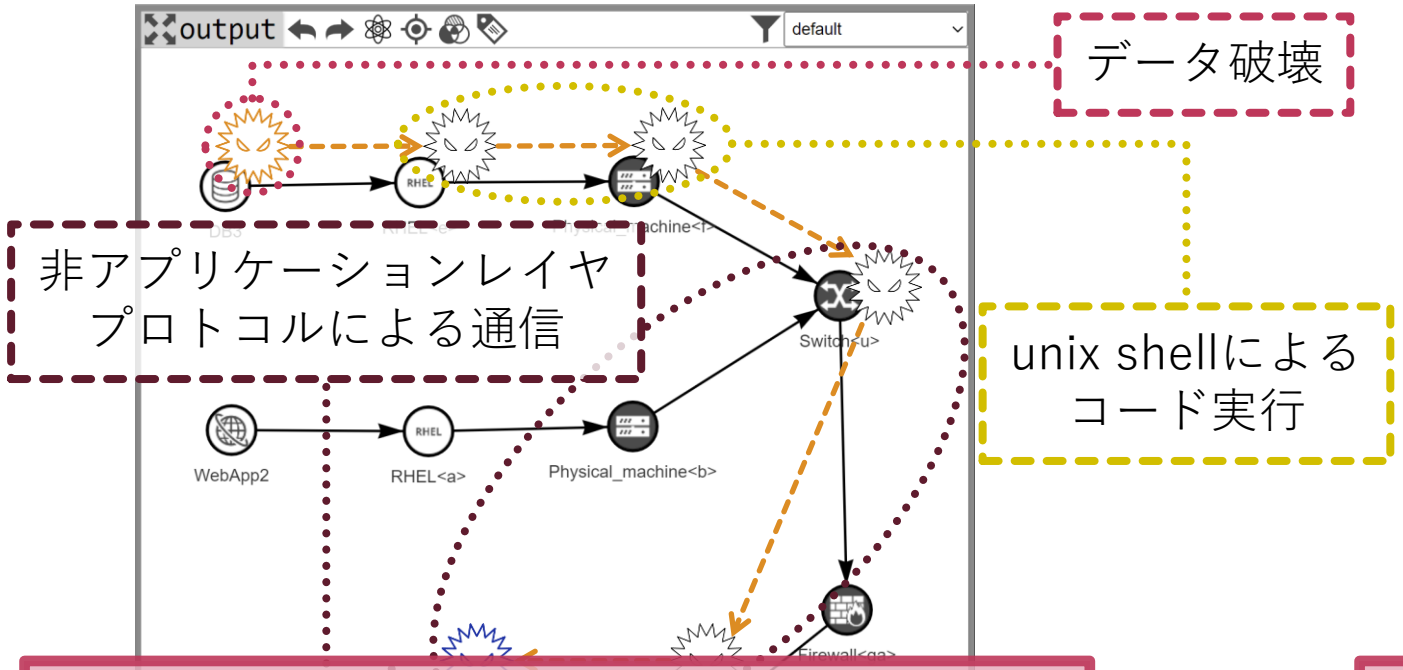
NIPS*: Network Intrusion Prevention System

© NEC Corporation 2022
\Orchestrating a brighter world NEC

[2/4] 従来手法での自動設計結果

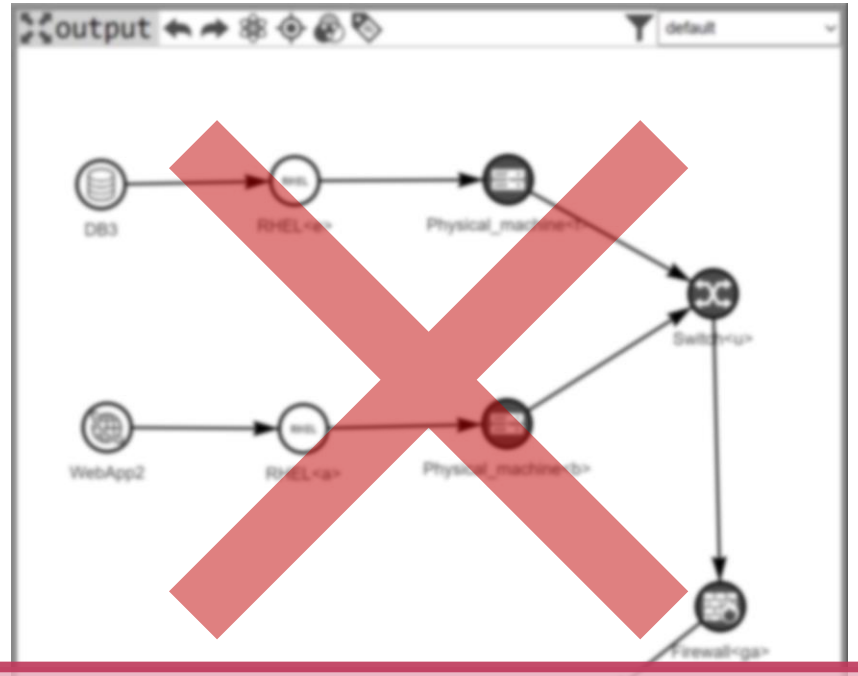
セキュリティ機能なし⇒**非セキュア**
脅威モデルのみ⇒**設計失敗**

セキュリティ機能なしの設計結果



対策の講じられていない攻撃パスが
成立した設計を出力⇒**非セキュア**

脅威モデルのみを用いた設計結果



攻撃パスの成立が回避できないため
設計結果出力不可⇒**設計失敗**

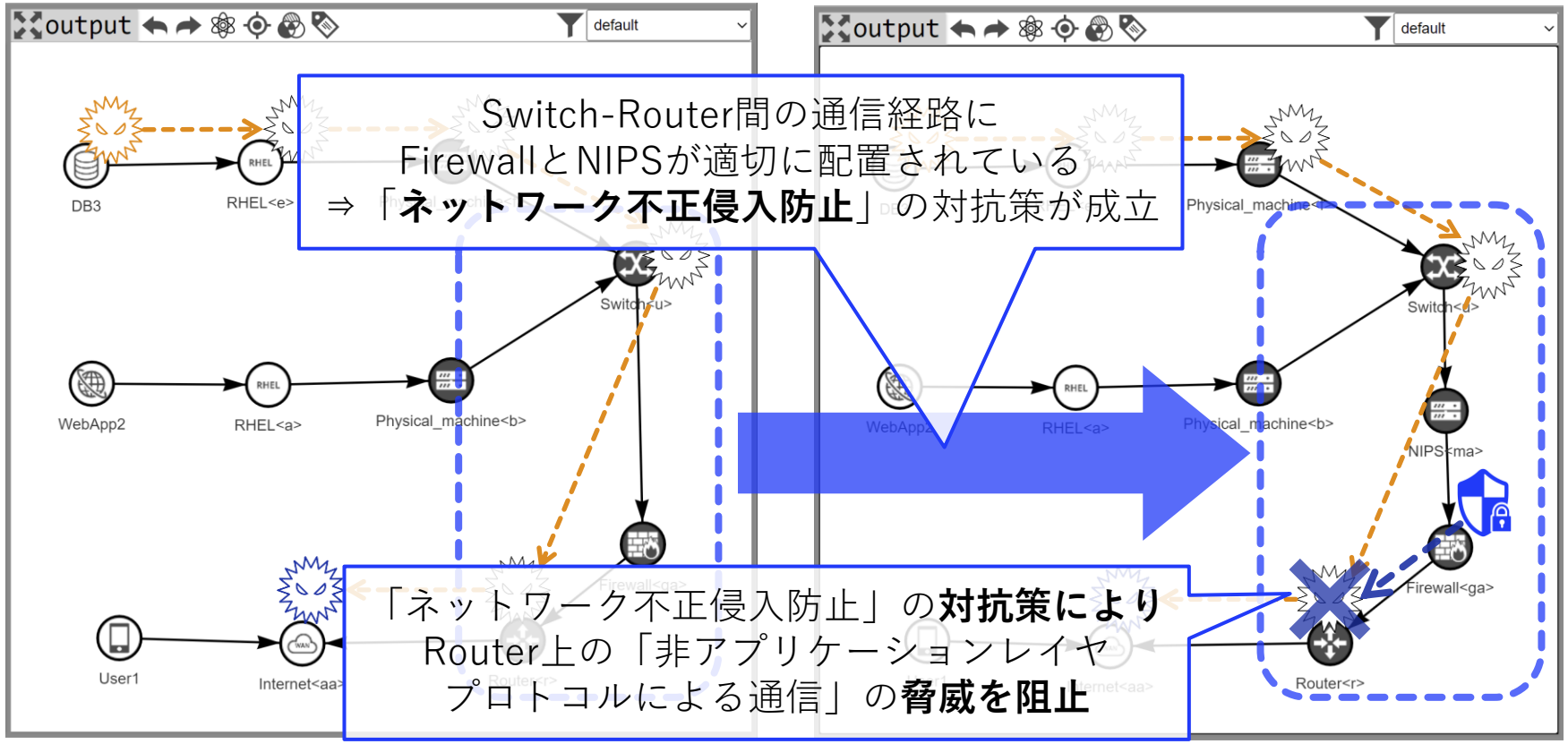
© NEC Corporation 2022
\Orchestrating a brighter world NEC

[3/4] 提案手法での自動設計結果

対抗策によりセキュアとなった設計を出力可能

セキュリティ機能なしの
設計結果

脅威モデルと対抗策モデルを
用いた設計結果



対抗策が脅威を阻止
↓
攻撃パスを無効化
↓
<u>攻撃パスが存在するが
セキュアな設計</u>となる

有効な攻撃パスが
存在しない
セキュアな
設計を出力可能

© NEC Corporation 2022
\Orchestrating a brighter world NEC

[4/4] 設計時間の評価

提案手法の設計時間は
セキュリティ機能なしの設計に比べて1割程度の増加に抑制

	1回目	2回目	3回目	4回目	5回目	平均
設計時間（セキュリティ機能なし）	9.38 s	11.05 s	9.27 s	8.91 s	9.11 s	9.54 s
設計時間（提案セキュア自動設計）	10.36 s	10.53 s	10.67 s	10.28 s	9.42 s	10.25 s
脅威具体化処理時間（提案セキュア自動設計）	0.01 s	0.08 s	0.03 s	0.05 s	0.02 s	0.04 s
対抗策適用処理時間（提案セキュア自動設計）	0.01 s	0.01 s	0.01 s	0.01 s	0.02 s	0.01 s
セキュリティ判定処理時間（提案セキュア自動設計）	1.51 s	1.37 s	1.41 s	1.41 s	1.06 s	1.35 s

7.4%程度の
設計時間増加

より複雑な要件やモデルにおける検証が今後の課題

© NEC Corporation 2022
\Orchestrating a brighter world NEC

4. まとめ

まとめ

「対抗策」の概念を用いた
セキュアシステム自動設計技術について

◆ 課題

- 従来の自動化技術では「脅威に対して対策を講じたセキュアなシステム」を設計できなかった.

◆ 提案

- セキュリティモデルとして「脅威」に加えて「**対抗策**」の概念を導入した.
- 対抗策を加味した「**有効な攻撃パスの有無**」を基準とするセキュリティ判定方法を提案した.

◆ 成果

- 実験にて対抗策を用いたセキュアシステム自動設計の動作とその有効性を確認した.

◆ 今後

- 対抗策により脅威が阻止ではなく緩和される場合のセキュリティ評価方法を検討する.
- より複雑な要件やモデルを用いた際の設計時間の評価や設計の高速化手法を検討する.

© NEC Corporation 2022

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

\Orchestrating a brighter world

NEC