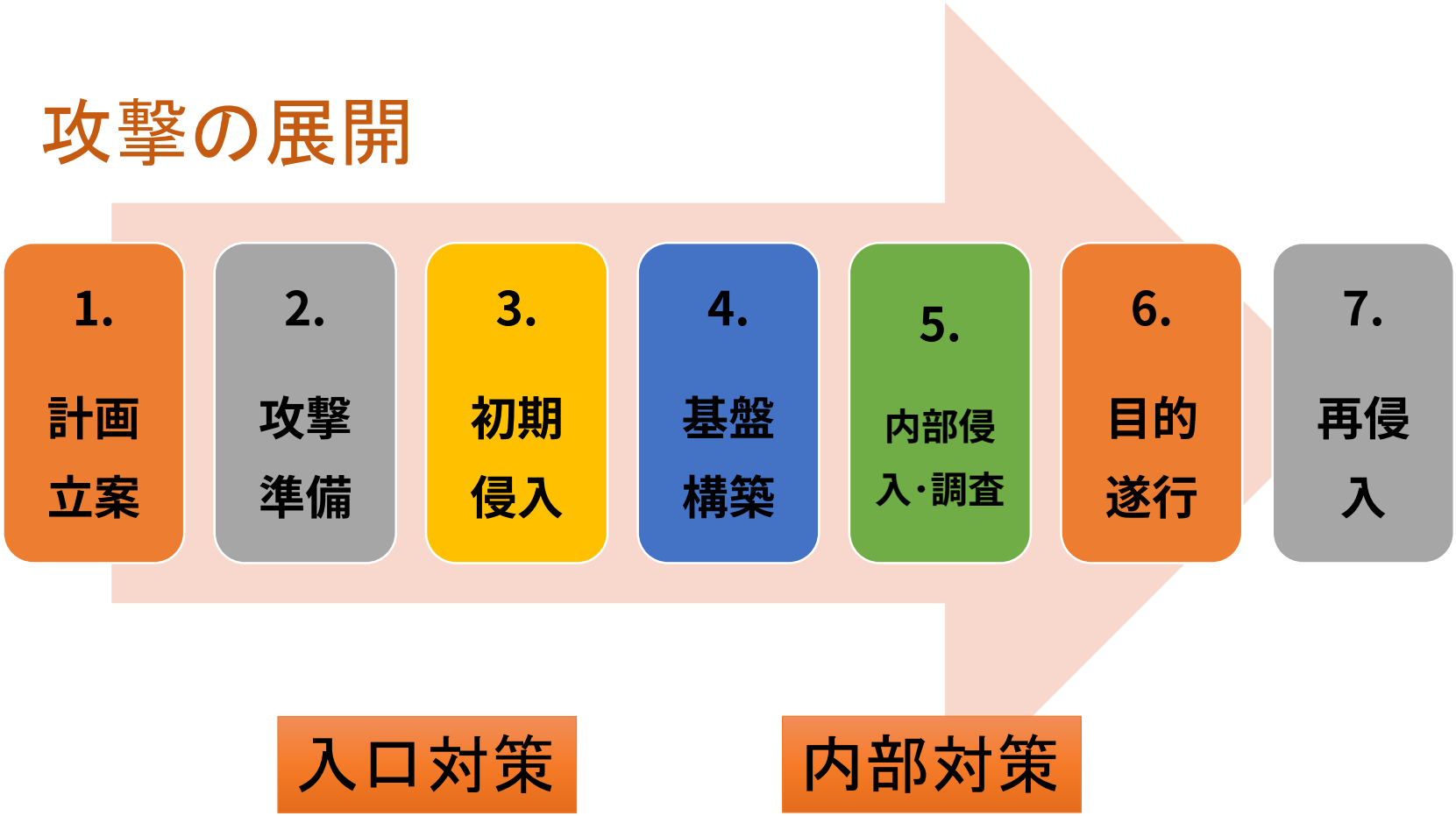
ネットワークフォレンジックにおけるAI応用技術の研究

東京電機大学　情報環境学部
八槇　博史

標的型サイバー攻撃



ネットワークフォレンジック

- ネットワーク内で「何が起きているか」を監視装置の警告（アラート）やサーバログなどから分析する.

- SIEM (Security Information and Event Management) 製品群
  - セキュリティポリシー監視
  - セキュリティ情報のリアルタイム監視

- AIの適用
  - この2，3年で急激に適用が進む
  - 多くは機械学習によるもの
    - セキュリティインシデントの事例からの学習
    - マルウェアのコード，挙動からの学習
  - すでに起きている事件からそれに類似した事象を発見するのが得意

標的型サイバー攻撃におけるマルウェア

- 特定組織を狙って特化した攻撃を継続的に行う
  - 「サイバー戦争」では主流
  - カスタムされたマルウェア
- RAT (Remote Access Tool)
  - 対象組織内に侵入する(「うちこまれる」)
  - 攻撃制御サーバ(C&Cサーバ)と通信する
    - 組織内の情報をアップロード
    - コマンドや攻撃用ソフトウェアをダウンロード
  - 攻撃を実施する

＝　攻撃者が用いるマニピュレータ

問題意識:
受動的なマニピュレータが能動的・知的ロボットに進化するのでは？

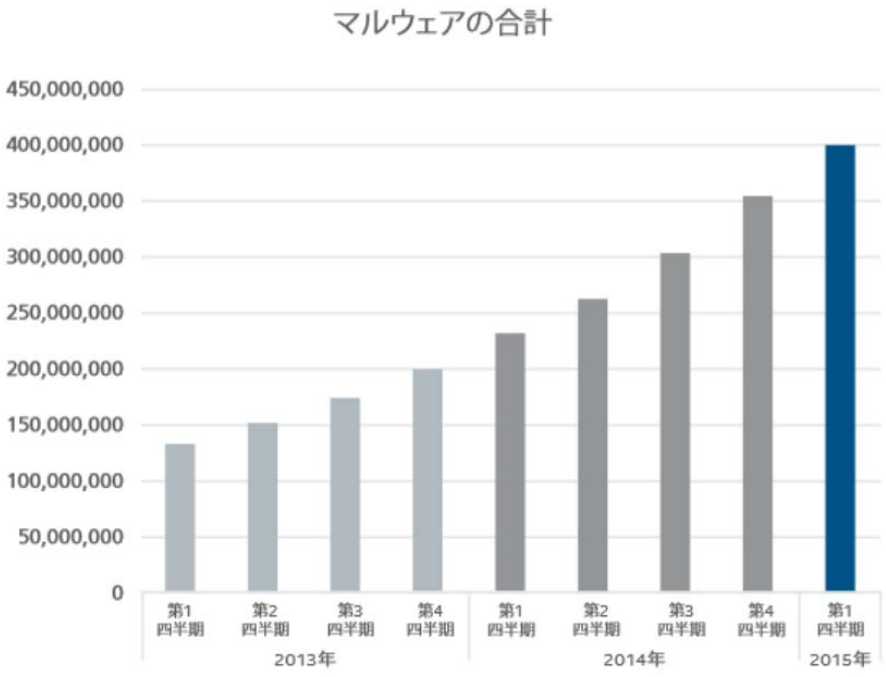
AIにより高度化するマルウェア

- 攻撃の自動生成
  - 攻撃者によるコーディングを要さない攻撃の登場
    （←機械学習，進化プログラミング）
- 高度な推論・プランニング能力
  - 外部との通信をせずに動けるマルウェア （←プランニング）
- 高度化する潜伏能力
  - 「正しい通信」を検出して模擬 （←ルール学習）
  - 「正しい通信」に基づく脆弱性発見 （←知識，推論）
  - 防御側の対策の先手を打つマルウェア
- 全体像を掴ませない攻撃
  - 複数のマルウェアによる協調攻撃 （←マルチエージェントシステム）
    - 複数が動くことにより，可能な状態数がかけ算で増える
- 自律的ソーシャルエンジニアリング
  - AIの対話能力の向上，センサの多様化，実世界との相互作用
    （←対話エージェント，「人狼知能」）

マルウェアの進化

- 合成されるマルウェア
  - スクラッチからマルウェアを作っていることは極めて稀
  - 大多数は既存のマルウェアの変形やエクスプロイトキットの組合わせによる

- 生物進化に類似
  - 設計の変異，組換えに基づく漸進的な変化
  - 大量の生成と実環境への投入による淘汰



出典: McAfee Labs, 2015

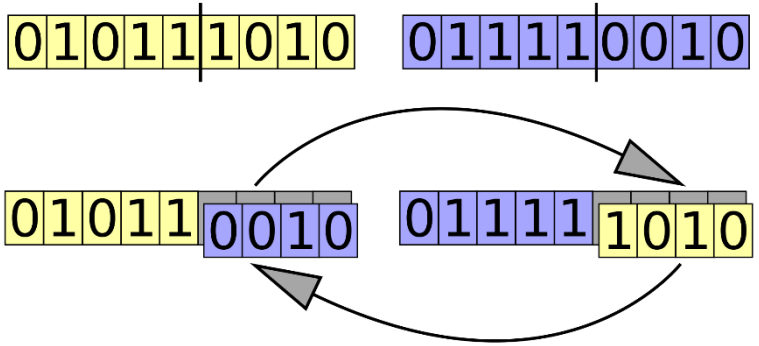
着目点：進化のイタチごっことしてのサイバー攻撃とその対策

- イタチごっこ
  - コンピュータウィルスの蔓延→アンチウィルスの普及→亜種の大量発生→マルウェア分類技術の発展→・・・
  - コンピュータウィルスの蔓延→アンチウィルスの普及→標的型攻撃の増加→防御技術の発達→・・・
  - 不正アクセスの増加→認証方式の高度化→DoS攻撃の脅威増大→・・・
  - 不正アクセスの増加→ファイアウォール、IDSの普及→内部侵入手法の高度化→SIEM等による検知、LIFT→・・・

- 共進化
  - どちらか一方が単独で進化するのではなく、互いへの対応の中で高度化していく

進化的計算 (evolutionary computation)

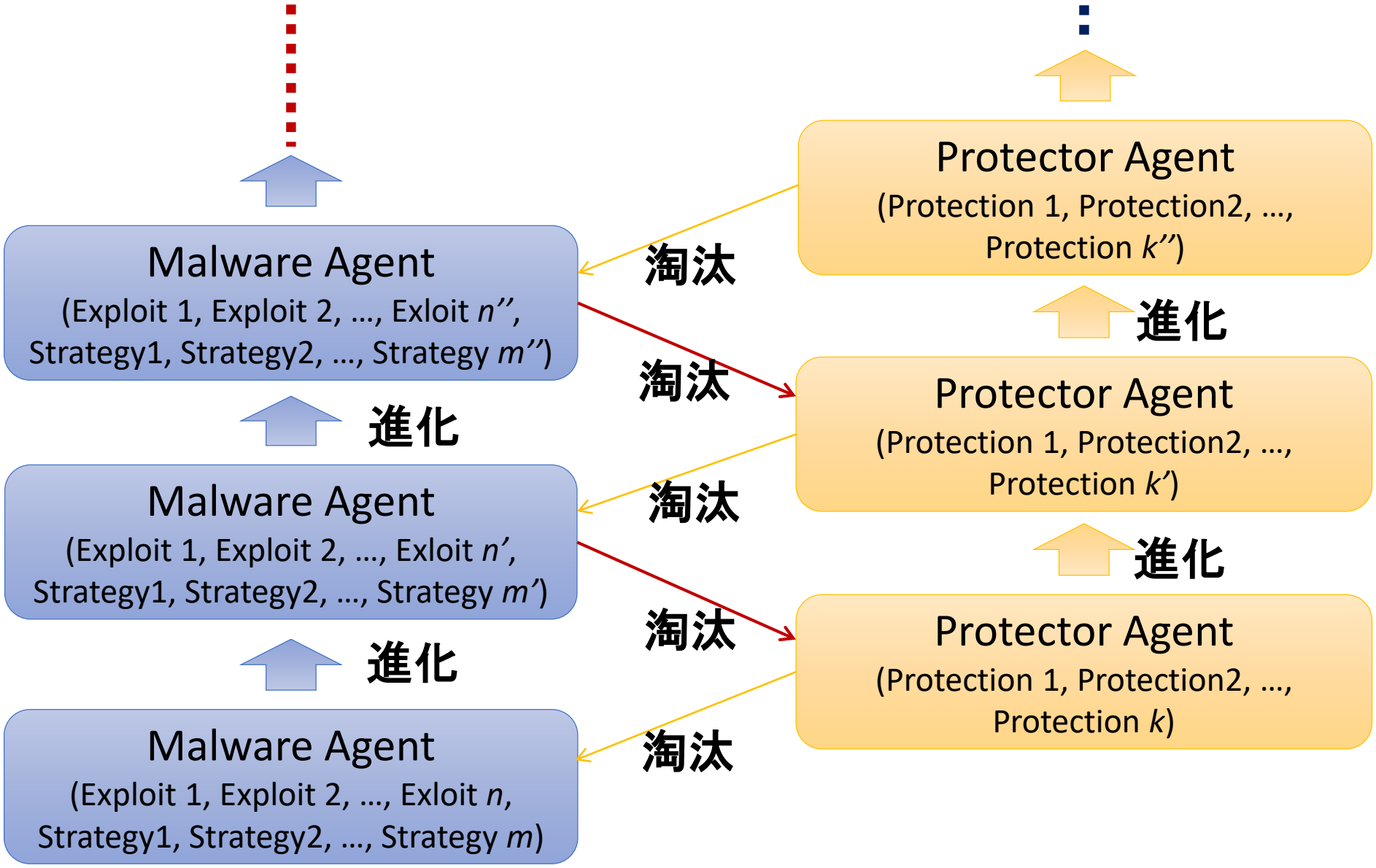
- 変異（mutation）・評価（evaluation）・選択（selection）を繰り返すことによって行う最適化・探索・学習などのための計算方式
- 代表例：Genetic Algorithm（GA）
  1. 最適化問題におけるパラメータセットをベクトルで表し、これを「遺伝子」と呼ぶ。初期値として複数の遺伝子を用意する。
  2. 遺伝子それぞれに対する評価関数の値を計算する（評価）。
  3. 評価関数値の上位の遺伝子を高確率、下位の遺伝子を低確率で残し、残りを捨てる（選択）
  4. 残った遺伝子をもとに一部のパラメータを変更（変異）したり、遺伝子同士の部分を交換（交叉）したりして、新しい世代の遺伝子群を生成する。
  5. 2～4を繰り返す。



共進化（Co-evolution）

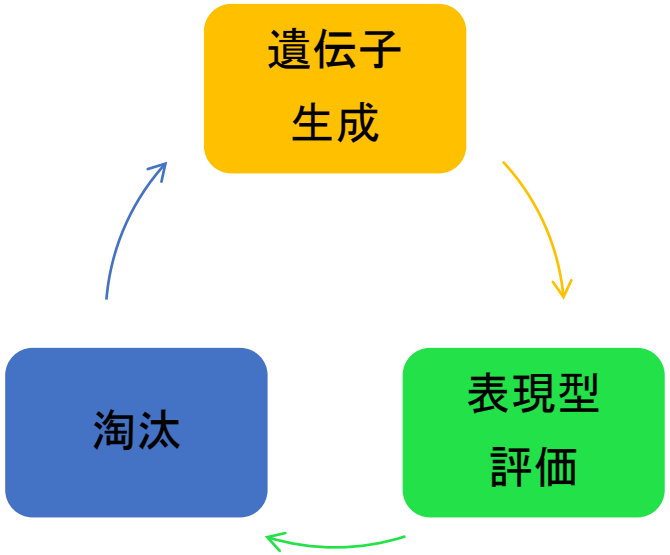
- 一つの生物学的要因の変化が引き金となって別のそれに関連する生物学的要因が変化すること（Wikipedia）
  - 事例：捕食者の登場と防御戦略の発達、共生、寄生、生態系の変遷

- 生物以外にもメタファが有効
  - 産業社会（技術と資本の相互作用）
  - 商品と消費者行動
  - 酒税とビールもどき　←イタチごっこ
  - 武器と戦術
  - サイバー攻撃とサイバー防御　←イタチごっこ


Malware Agent
(Exploit 1, Exploit 2, …, Exloit n'', Strategy1, Strategy2, …, Strategy m'')
進化
Malware Agent
(Exploit 1, Exploit 2, …, Exloit n', Strategy1, Strategy2, …, Strategy m')
進化
Malware Agent
(Exploit 1, Exploit 2, …, Exloit n, Strategy1, Strategy2, …, Strategy m)
淘汰
淘汰
淘汰
淘汰
Protector Agent
(Protection 1, Protection2, …, Protection k'')
進化
Protector Agent
(Protection 1, Protection2, …, Protection k')
進化
Protector Agent
(Protection 1, Protection2, …, Protection k)

研究手法：共進化計算

- 攻撃と防御の変遷を進化計算にマッピング
  - 遺伝子
    - 攻撃側： エクスプロイトの組合わせ
    - 防御側： サイバー攻撃対策技法の組合わせ
  - 表現型の評価
    - ネットワークシステムの上でのシミュレーション
  - 進化アルゴリズムの適用
    - 遺伝子生成と評価，淘汰を繰り返す



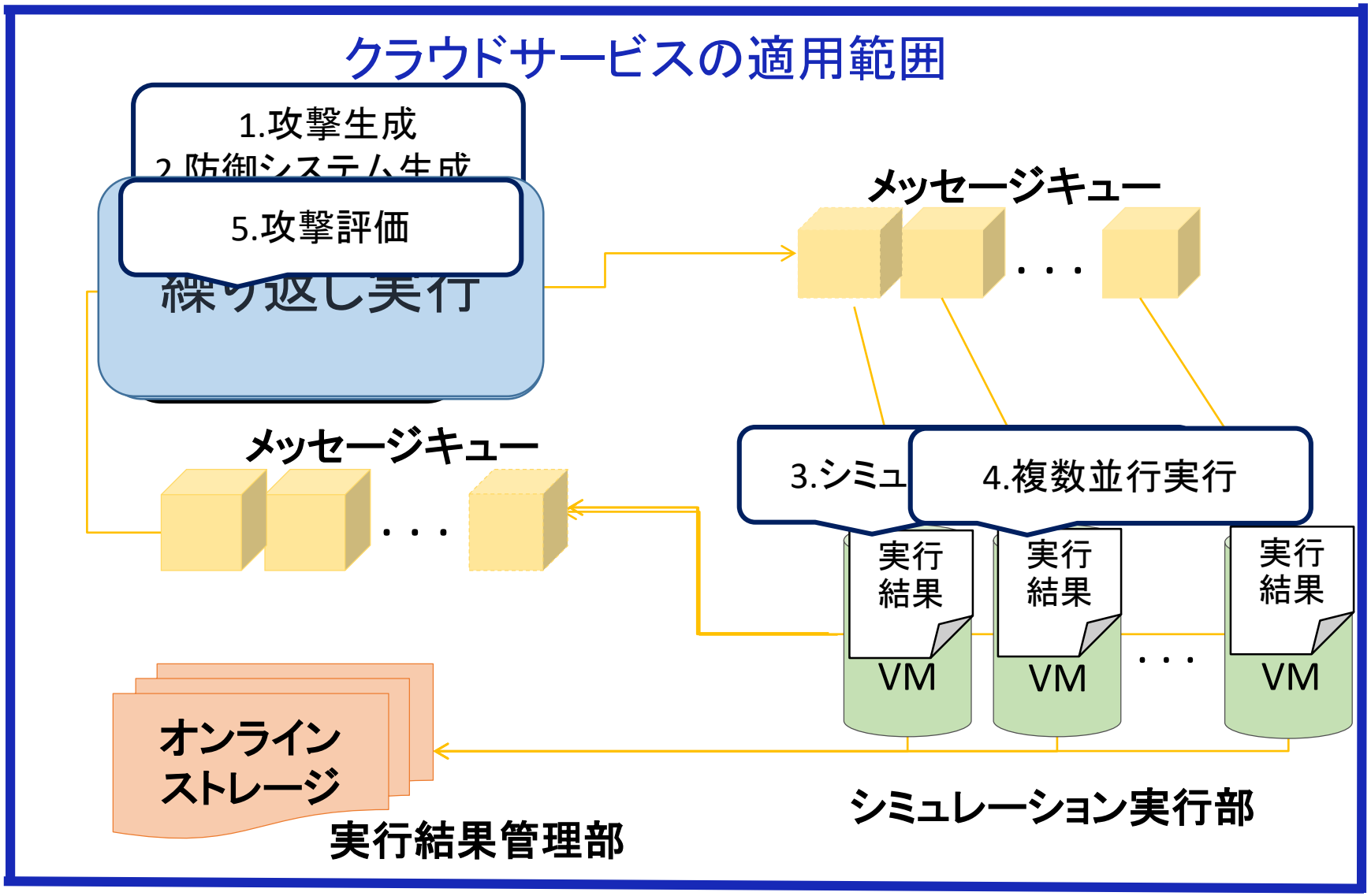
- クラウド環境の活用
  - 膨大な量の試行錯誤
    - 遺伝子生成と評価を並列実行
  - 様々なネットワーク環境への適用
    - 仮想化技術（VM, SDN等）によるソフトウェア化

amazon web services™

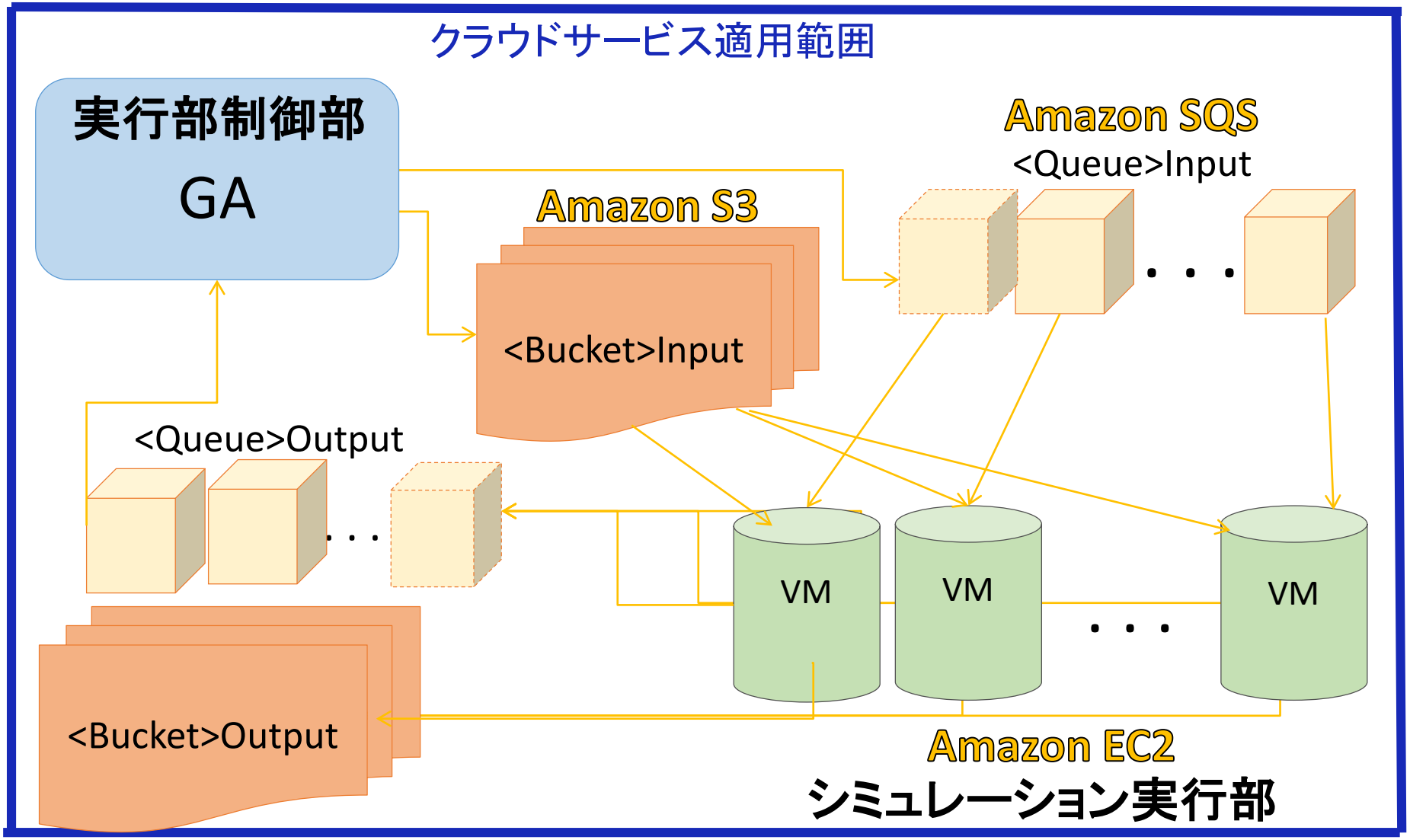
docker

OvS Open vSwitch

クラウドによる進化計算機構　概要図



進化計算機構　GPGCloud

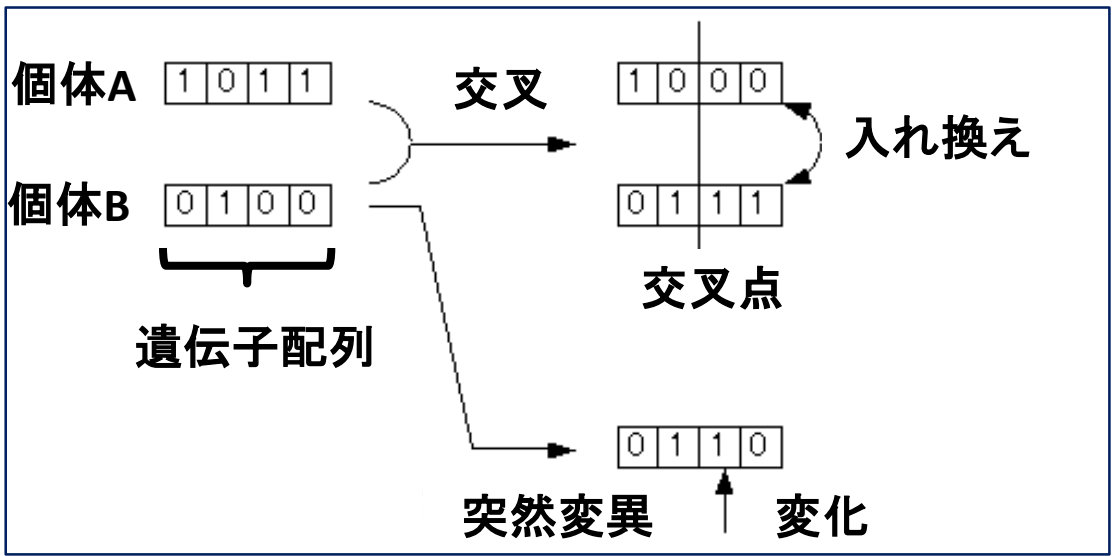


進化計算手法

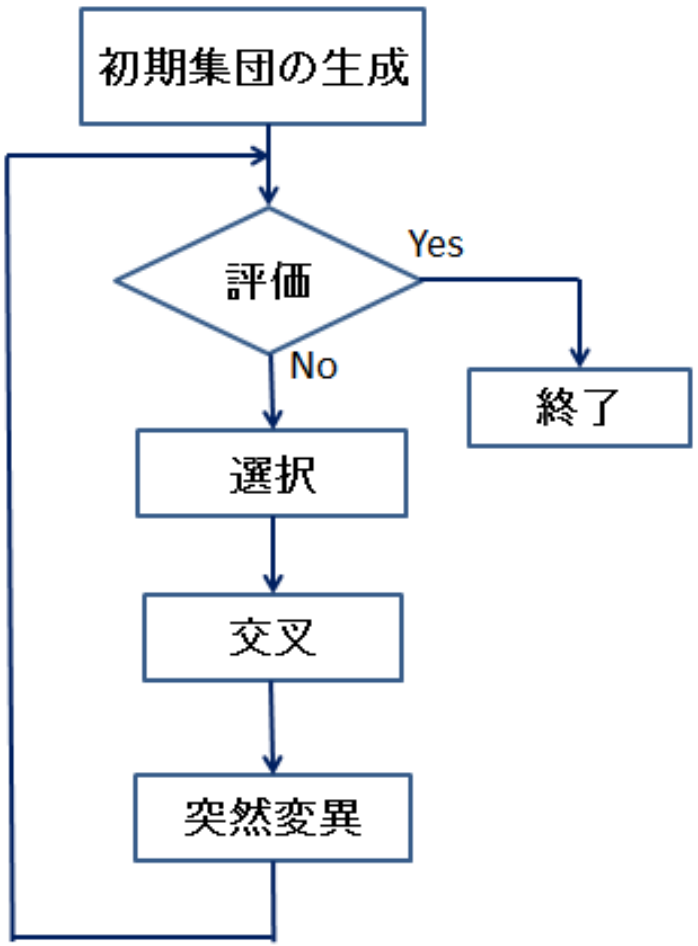
遺伝的アルゴリズム GA　[Holand 1975]

選択：遺伝子の適応度（問題に対する評価値）を
もとに選択淘汰
交叉：生物の交配をモデル化
突然変異：遺伝子の突然変異をモデル化
乱数やビット反転して表現

より良い評価値（適応度）を**繰り返し探索**する



フローチャート



攻撃 ・ 防御モデル定式化

・プレイヤー　　攻撃者と防御者

・戦略　　個々のプレイヤーがとることのできる行動
　攻撃側：　攻撃コードの選択
　防御側：　防御施策の選択

・利得　　起こりうる行動の組み合わせに応じた効用
　攻撃側：　成功報酬期待額　－　不法行為の期待損失
　防御側：　情報資産　－　防御施策コスト

取りうる戦略によって各々の組合せが決まる

シミュレーション検証システム

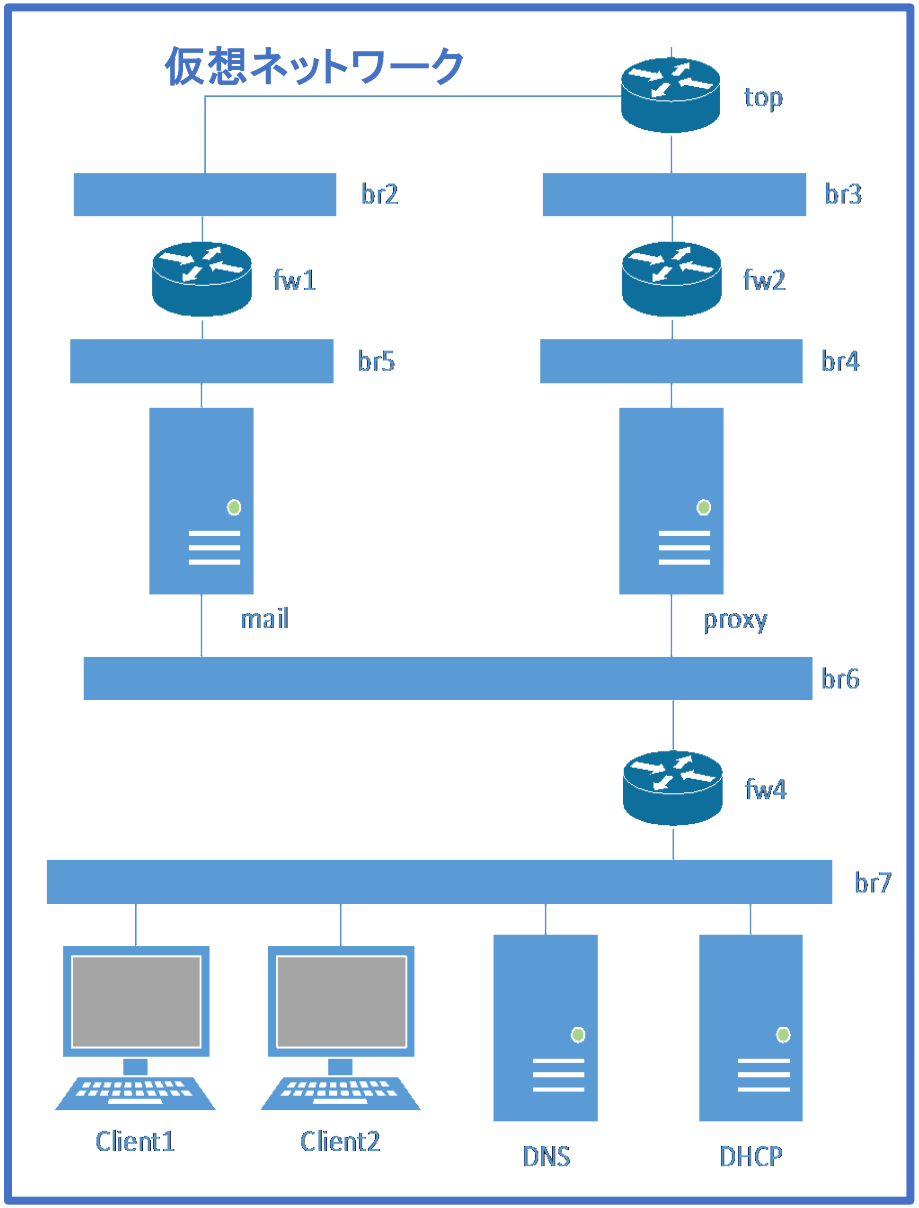
amazon web services EC2

シミュレーション
実施ツール

EXPLOIT DATABASE

metasploit®

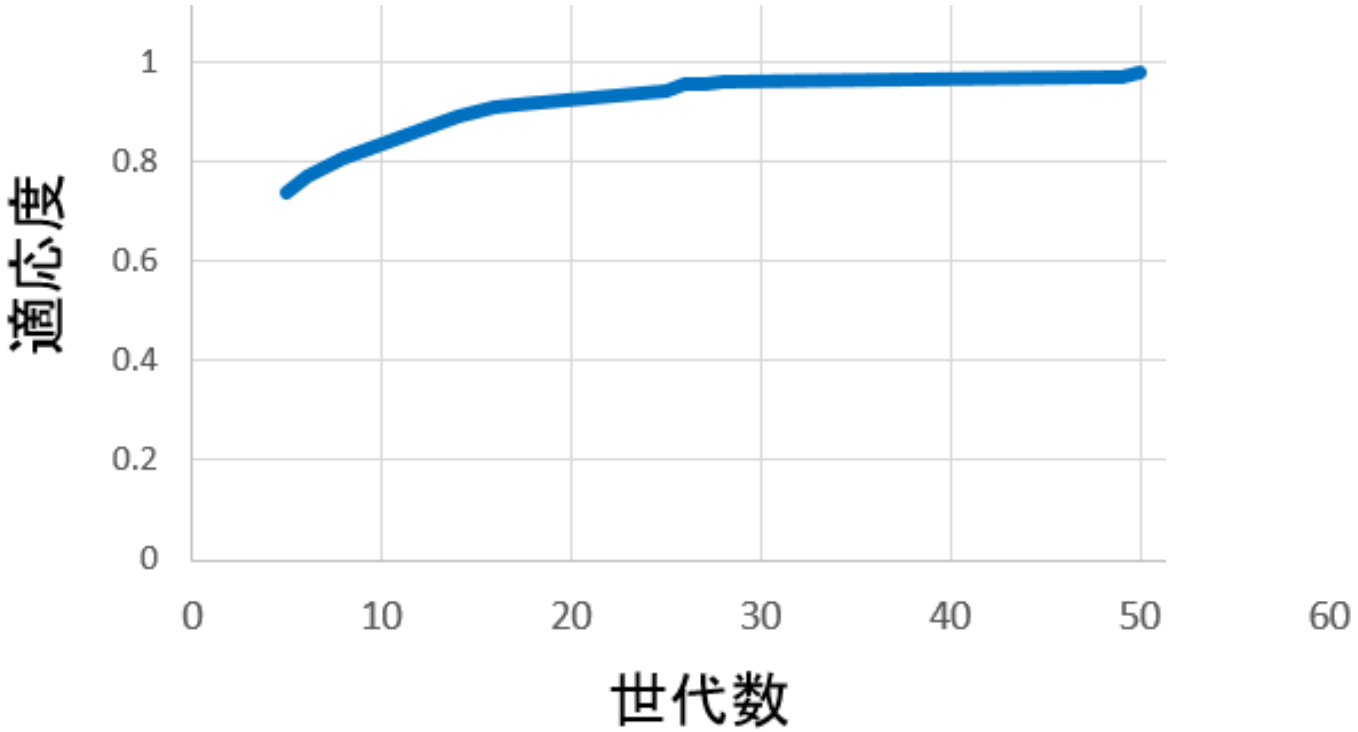
Nessus® vulnerability scanner



ログ収集

ZABBIX

攻撃のシミュレーション結果



50世代までシミュレーション
遺伝子配列は32ビット　　個体集団　1世代30個体
適応度 (攻撃手法の網羅度)　最適値　1.0

進化計算によって
評価値が上昇していることが確認された

まとめ

- ネットワークフォレンジック
  - ネットワーク中で何が起きているか／何が起きうるかをいち早く知って対策に繋げたい
- AIの活用
  - 現在の機械学習に基づく方式の多くは後追い
- 目標:「先回り」の実現
  - 防御，そして攻撃側もAIを搭載してくる中で，どのような事象・状況が発生しうるかを事前に検証
  - 共進化アプローチ