テストベッドを何に使うのか

- 情報セキュリティ技術開発の視点から考える -

山口 英
奈良先端科学技術大学院大学情報科学研究科

概要

- 近年の情報セキュリティ管理技術の研究開発には、様々な軸が存在するが、「良好な規模拡張性の確保」と「自動化の実装」が必須の達成目標となっている。開発した技術の検証のために、本当はテストベッドを活用したいと考えていることが多い。近年の情報セキュリティ管理技術のチャレンジと、テストベッド活用の可能性について述べる。

IMPROVEMENT ON “SCALABILITY”

リスクの多様化

（これでも全部じゃない!）

- 攻撃の個別化
  - 目標にチューニングされた手法による攻撃
  - No more “pandemic” by single malware.
  - 膨大な attack warning の中から、本当の攻撃を特定し、その状況を確認する必要がある
- 多種多様なデバイスによる情報の拡散
  - Mobile device & high-capacity mobile storage
  - もはや複製管理を徹底することは困難
  - 情報漏洩を発見し、その影響範囲を確定する必要がある
- 相互に接続される情報システム
  - 広義の Supply Chain System を形成
  - 業種や国境を越える情報システム
  - システム構成や規制は多種多様

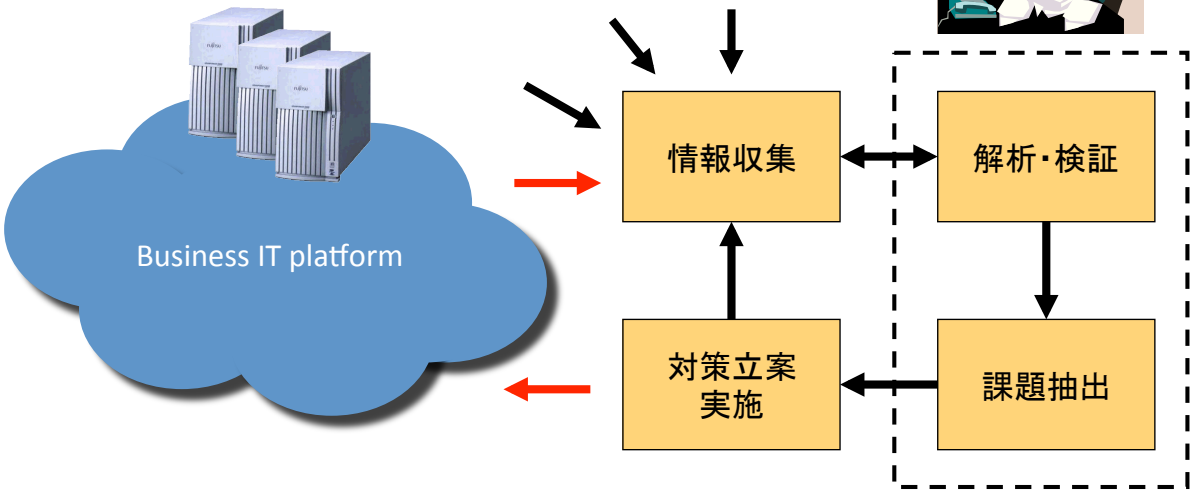
急激に変わる情報処理環境

- 管理対象の増加、多様化
  - (プライベート)クラウドの展開
  - モバイルデバイスの一般化
- リスクの多様化

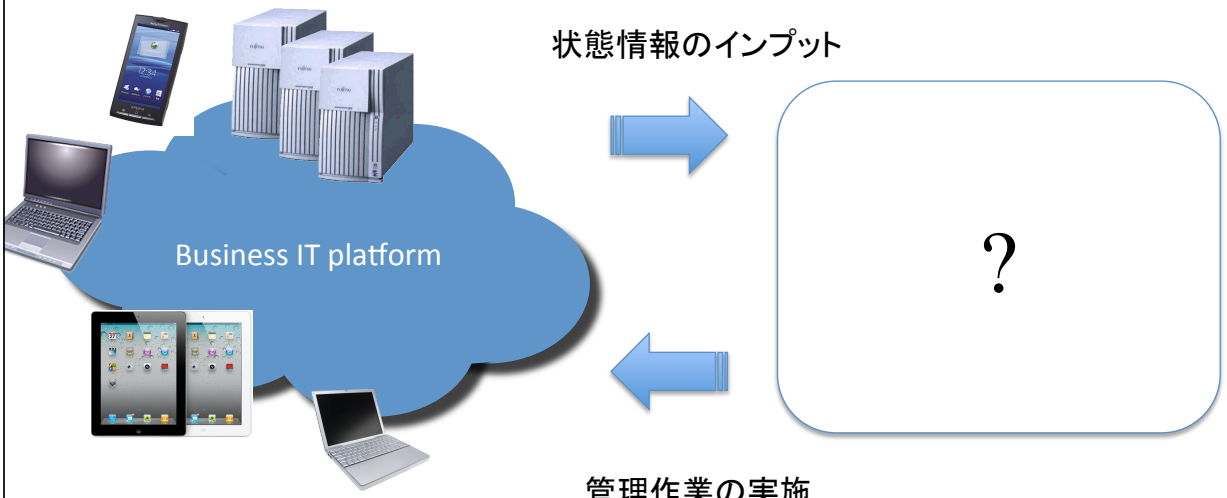
- 管理の規模拡張性 scalability は健全か?
  - クラウド
    - 管理対象の集約 / リスクの集中
  - モバイルデバイス
    - 管理対象の激増 / リスクの分散 / 管理密度の稀薄化

情報セキュリティ対策は科学である

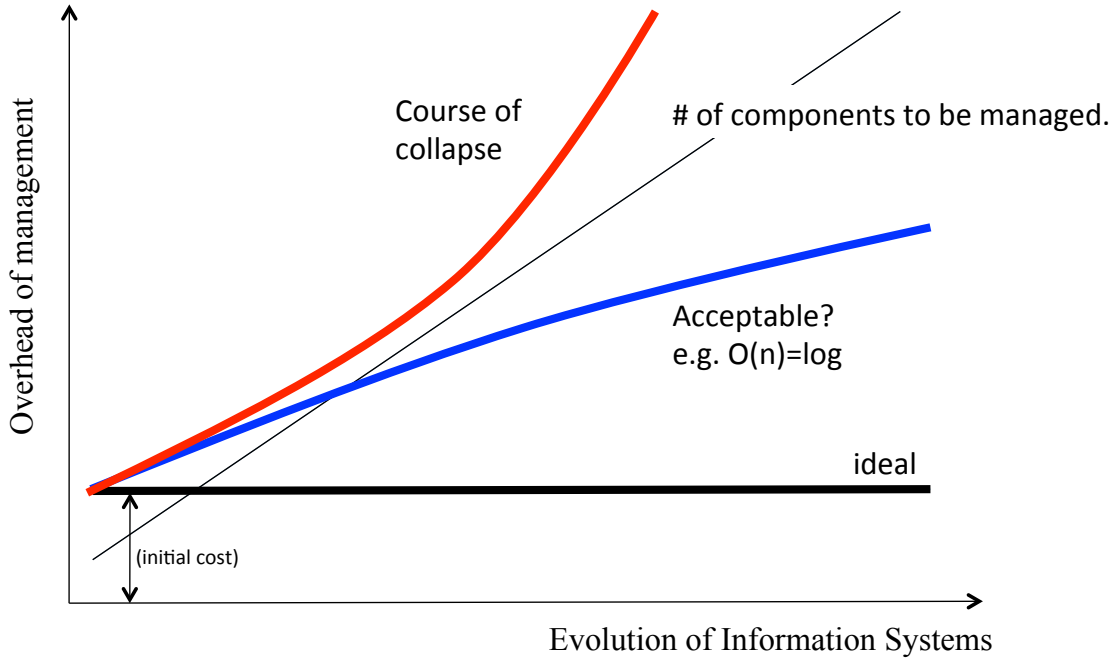
- システムの連続的かつ合理的な改善作業
- 認知、仮説設定、検証
- 対策による「系」の変化を理解する
- リスク顕在化による「系」の変化を設計する



良好なスケーラビリティ維持



Scalable, Sustainable and Resilient Management



管理情報収集の自動化

- 「管理者が登録する」は無理
  - 利用者が登録をする、自動的に登録する
  - IEEE802.1x, 検疫機能, Active Directory, Network Login, …
  - 利用に応じた登録とアクセス制御
- コンピュータはセンサー
  - 管理作業は、多数のセンサーからの信号をみながらシステム全体の安定性を制御するタスク
  - ビッグデータとして捉えるシステムが必要
  - データマイニングではなく、確実な捕捉が必要

全部やらない

- 観測に基づいた、優先順位設定
  - 許容リスク acceptable risk という考え方を取り入れる
  - 全部対応しない
    - ゼロリスクの強迫観念を克服する
    - 「自分はちゃんとやっている」という言い訳のために、経営資源を浪費するのは悪だ
- 必要なことを、適切に行う
  - 専門家、専門サービスを活用するチャンスはここにある
  - 分からないから全部やってしまう → 疲弊する

Security Management Automation

- セキュリティ管理作業の自動化
  - なんでも人手を掛けるのは効率が悪すぎる
  - 人間は、人間しかできないことをすべき
  - 管理作業の自動化
- やり過ぎも良くない
  - 判断するところは人間でないとできないものが多い
  - 過度の自動化は false positive を増やし使い物にならない
    - 常に警報が出ていると感度が悪くなる

これからの技術開発

- 情報セキュリティ管理作業の自動化
- どこまで効率化できるか
  - 人間は、人間しかできないことをやるべき
- どこまで情報共有をスマートにできるか
  - Spam detection, malware analysis, web contents inspection, IDS/IPS, ….
  - 色々なデータを上手く収集して、防御に使う
  - 攻撃の多様化にどのように対応するか
  - 一人で全部できるわけがない
- 実際に効果のある基盤技術を開発できるか
  - 効果がなければ意味がない

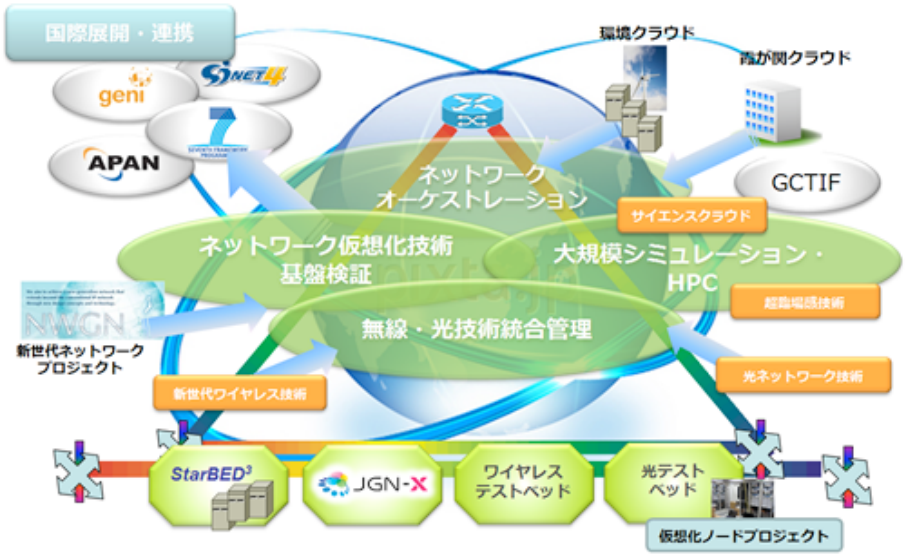
WISH JGN WORKING FOR OUR SOCIETY…

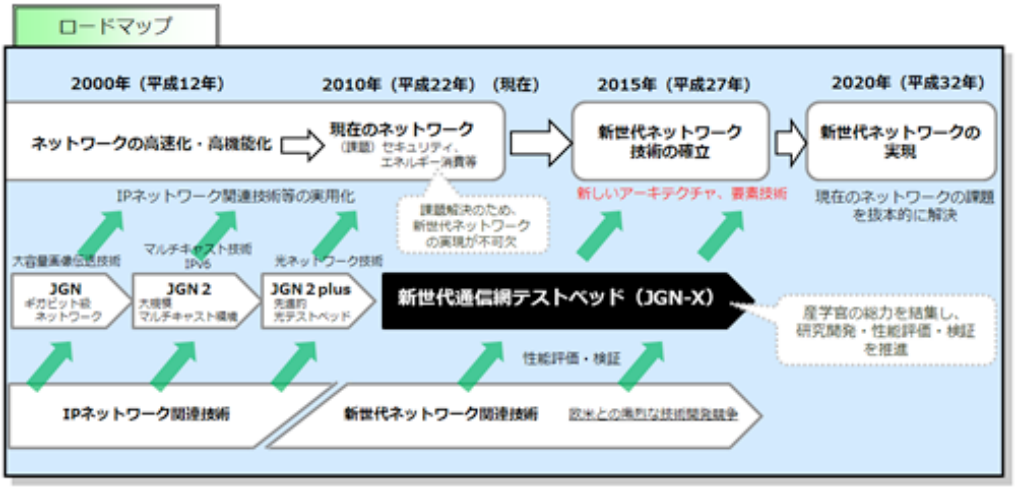
テストベッドの役割

- 外部環境に影響を与えず、様々な技術実証実験が可能な空間
  - 「箱庭」
  - 高い計測性を持つ基盤環境で、観測に伴うデータ収集が十分にできる
  - 再現可能な実験、対照実験を行うことができる
  - 実際の対象環境に匹敵する規模性を持つ
  - ….

JGN-Xでの役割定義

- テストベッドでの実験支援
- テストベッドによる技術試験と製品化促進
- テストベッドによる事前検証と人材育成
- テストベッドによる知の蓄積と共有


国際展開・連携
geni
APAN
環境クラウド
霞が関クラウド
GCTIF
ネットワーク
オーケストレーション
サイエンスクラウド
ネットワーク仮想化技術
基盤検証
大規模シミュレーション・
HPC
超臨場感技術
無線・光技術統合管理
新世代ネットワーク
プロジェクト
光ネットワーク技術
新世代ワイヤレス技術
StarBED³
JGN-X
ワイヤレス
テストベッド
光テスト
ベッド
仮想化ノードプロジェクト


ロードマップ
2000年（平成12年）
2010年（平成22年）（現在）
2015年（平成27年）
2020年（平成32年）
ネットワークの高速化・高機能化
現在のネットワーク
（課題）セキュリティ、
エネルギー消費等
新世代ネットワーク
技術の確立
新世代ネットワークの
実現
IPネットワーク関連技術等の実用化
課題解決のため、
新世代ネットワーク
の実現が不可欠
新しいアーキテクチャ、要素技術
現在のネットワークの課題
を抜本的に解決
大容量画像伝送技術
マルチキャスト技術
IPv6
光ネットワーク技術
JGN
ギガビット級
ネットワーク
JGN 2
大規模
マルチキャスト環境
JGN 2 plus
先進的
光テストベッド
新世代通信網テストベッド（JGN-X）
産学官の総力を結集し、
研究開発・性能評価・検証
を推進
性能評価・検証
IPネットワーク関連技術
新世代ネットワーク関連技術
欧米との熾烈な技術開発競争

National Cyber Range (US)

- DARPA project (2008 – present)
  - the architecture and software tools for a secure, self-contained testing capability to rapidly emulate large-scale complex networks that match the depth and diversity of real-world networks.
  - The capability will enable realistic testing and evaluation of new cyberspace concepts, policies and technologies by the Department of Defense (DoD) and other federal entities.
  - demonstrated at scale with an operational prototype,
  - "DoD's Strategy for operating cyber space" (July 2011)
- Participants
  - Johns Hopkins University, Lockheed Martin, …

NCR (US)

- テスト対象
  - host security systems
  - local and wide area network (LAN and WAN) security tools
  - New network protocol
  - Satellite and RF communications
  - Mobile communication systems
- テスト方法
  - 脆弱性評価
  - ネットワークとシステムの両方で試験
  - 攻撃再現実験
  - シミュレーション
  - システム解析 / a large-scale Global Information Grid (GIG)

NCR (US)

- 求められる最低限度の機能
  - 一対一の攻撃試験
  - 新しい攻撃試験の迅速な開発
  - 迅速なテストベッドの構成変更
  - テスト管理
  - 高精度の時刻管理
  - データ収集ツール（パケットキャプチャ、イベント収集、マルウェア事象データ収集、自動攻撃検知）
  - トラヒック生成システム（任意のリアリティあるトラヒック生成）
  - 疑似ユーザシステム (human replicant)
  - 実際の通信の模倣を行うシステム
  - 全設備を使った巨大試験機能
  - 動的な資源管理と、他のテストへの割当て
- 規模は1万テストノードが最低ライン

提案

- JGN-X では、主にネットワーク機能に注目してテストベッド構築をしてきたが、セキュリティの取組は非常に少ない
- 日本版の National Cyber Range を JGN-X 上でちゃんと作って、技術研究開発のために提供するのはどうだろう
  - セキュリティ技術開発に真剣にフォーカスを当てた環境構築を JGN-X で行う
    - 仮想化技術により他に影響を与えない環境構築は簡単にできるはずだ
  - JGN-X単独ではできないが、必要となる設備はNICTが全部持っている
    - StarBED, 光テストベッド、ワイヤレステストベッド, …
  - 技術の集積と流通を、JGNが主導的に行う
    - 情報セキュリティ技術開発を行う多くの人達を主導する
    - テスト技術を確立する→これぞNICTの役割

まとめ

- セキュリティ技術開発では、自動化をどのように実現するかが喫緊の課題
- JGN-X の規模と先進性を考慮し、大規模情報セキュリティ試験環境の構築をするのが良いのではないか
  - 日本版 National Cyber Range