TOHOKU BUNKA GAKUEN UNIVERSITY
東北文化学園大学

インターネット観測システムに対する攻撃とその防御手法に関する研究

平成27年度　石田實記念財団　研究発表会

東北文化学園大学　科学技術学部
知能情報システム学科
成田匡輝

研究背景

サイバー攻撃被害の増加

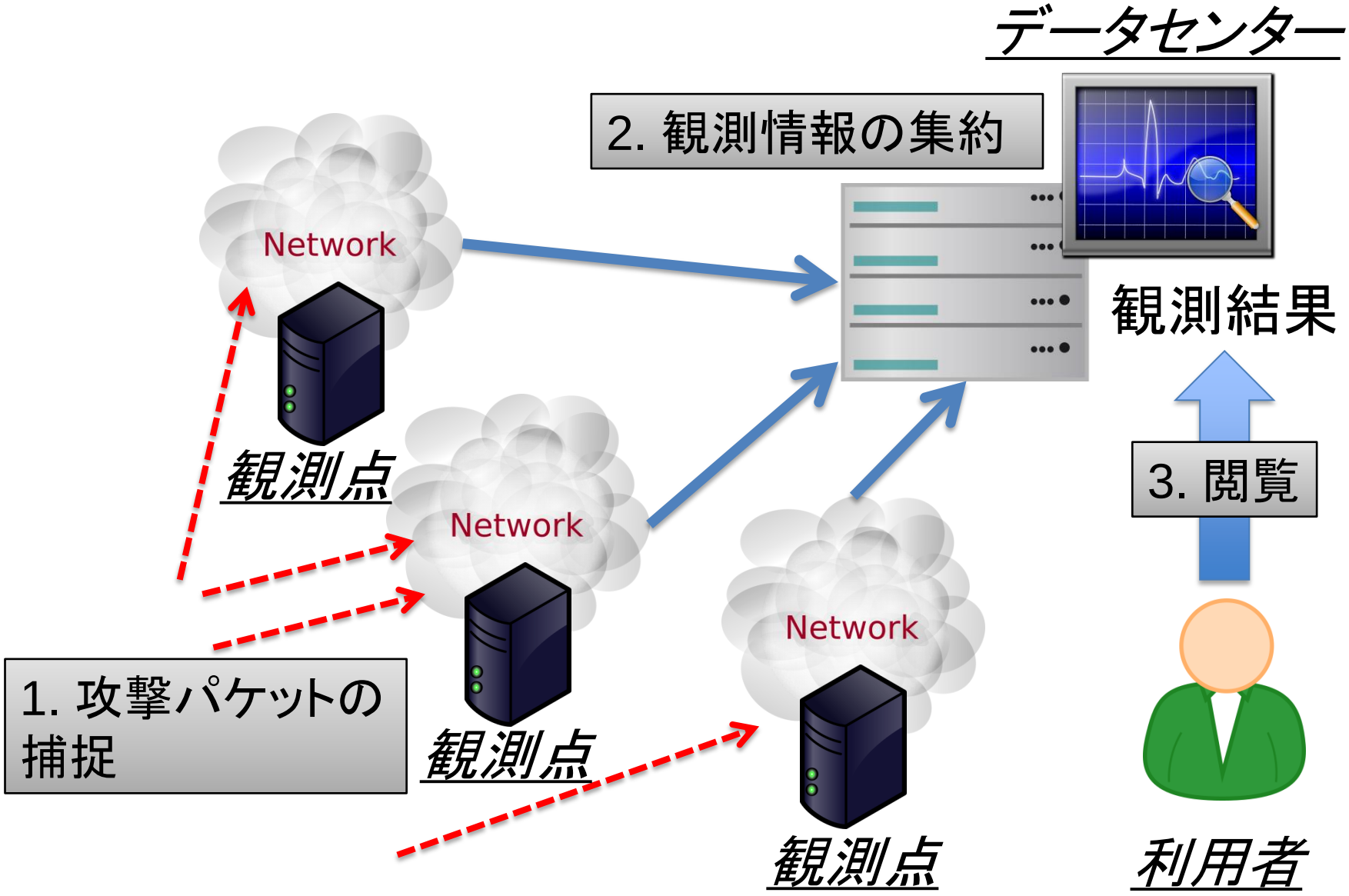
- 世界のサイバー攻撃による被害額は年間113億ドル
  - Hewlett-PackardやAppleの年間純利益に匹敵
- 2015年4月，仏TV局でサイバー攻撃の影響により数時間番組が放送できない事態に

サイバー攻撃の動向を早期に把握する必要性

インターネット観測システムの開発へ

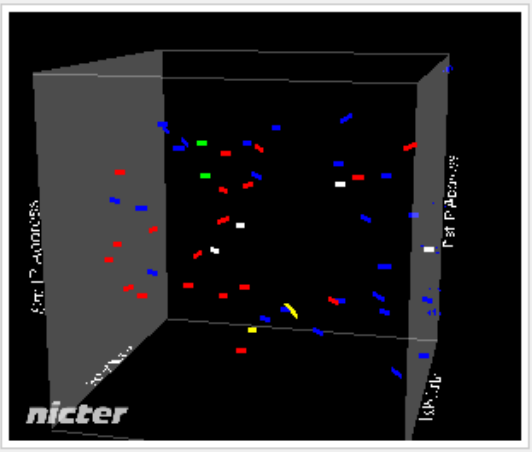
参考：AppSec APAC 2014 基調講演レポート, http://itpro.nikkeibp.co.jp/article/NEWS/20140320/545025/
IIJ, Internet Infrastructure Review, Vol.28, 2015.

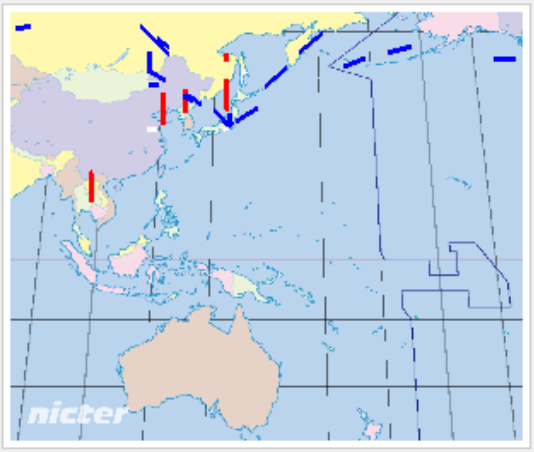
インターネット観測システムの概要



インターネット観測システム

nicter（情報通信研究機構の例）





TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
22	1,079,446	45%
80	225,402	9%
23	148,404	6%
1433	124,116	5%
3389	121,599	5%
443	66,467	3%
8080	42,953	2%
21320	28,687	1%
445	21,271	1%
0	18,512	1%

- 20万以上の観測点（IPアドレス）で観測を行う国内最大規模の観測網

しかし，近年．．．

観測システムを構成する観測点への攻撃が問題視

参考：nicter, http://www.nicter.jp/nw_public/scripts/index.php#nicter

研究の目的

- 観測点検出攻撃

インターネット上に配置した観測点を検出してしまう攻撃

観測点の存在が外部に露呈すれば

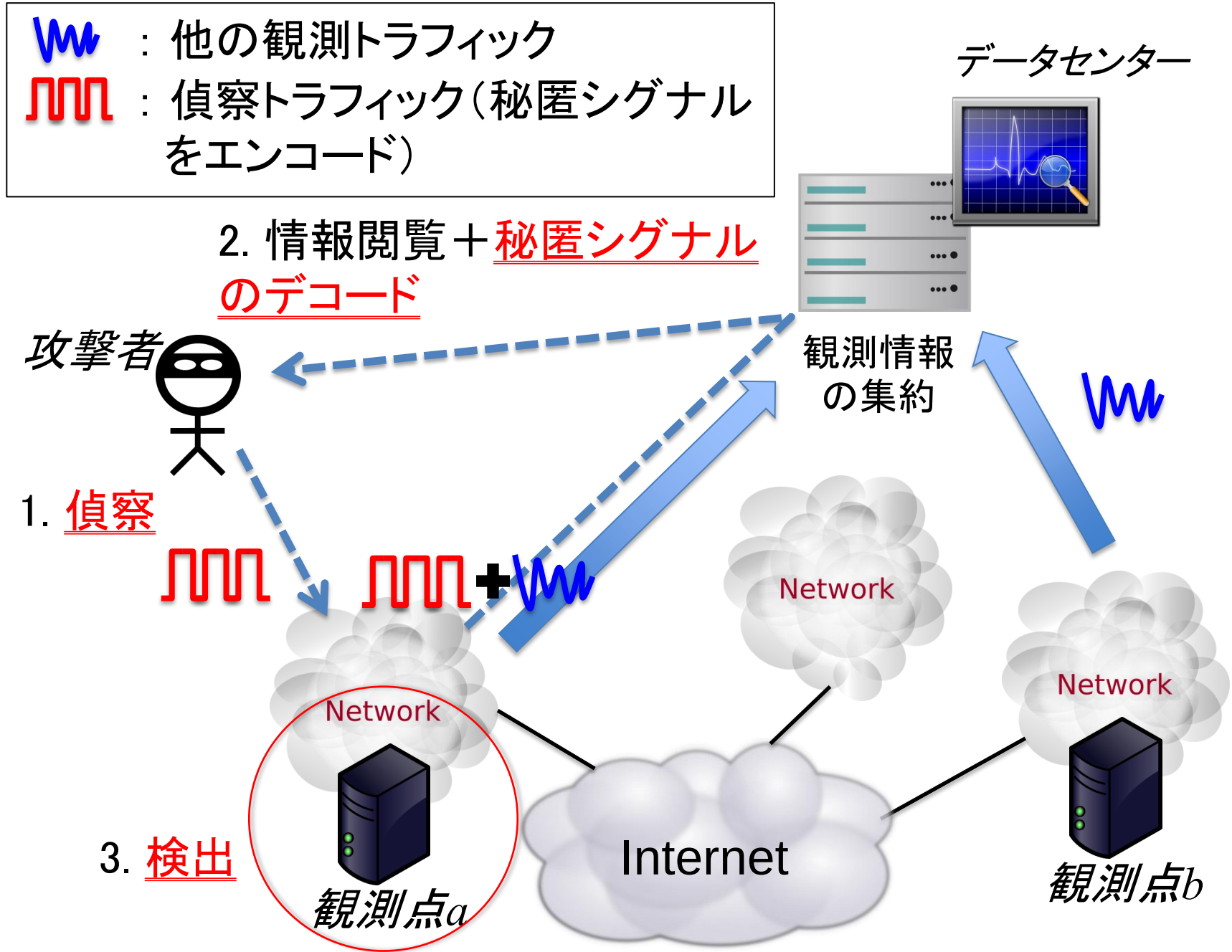
観測網が迂回されてしまう

観測点検出攻撃の検証と対策を行う

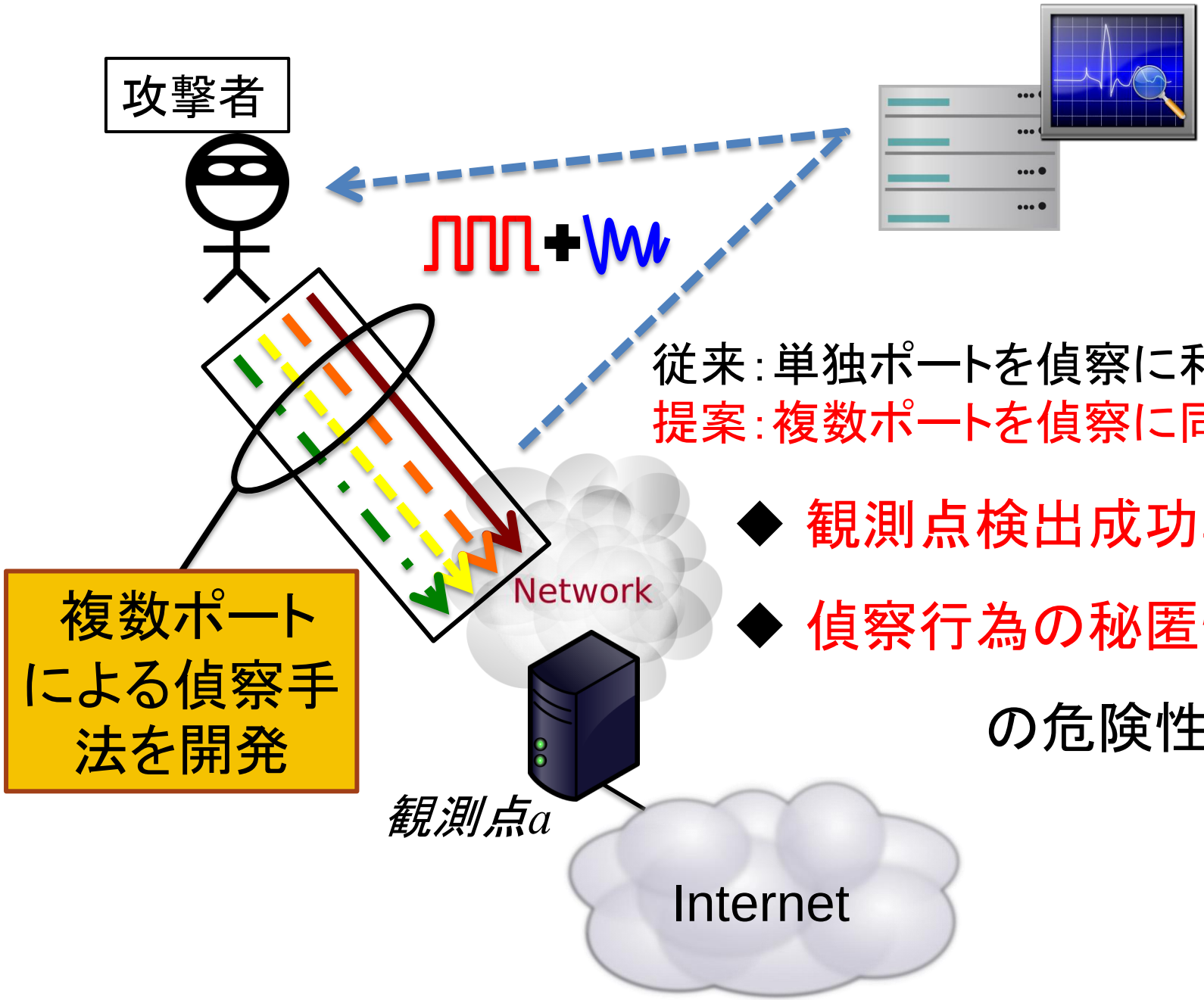
観測点検出攻撃

- W. Yu *et al.* 2010

：他の観測トラフィック
：偵察トラフィック（秘匿シグナルをエンコード）



研究成果① 新たな攻撃手法の検討



従来：単独ポートを偵察に利用

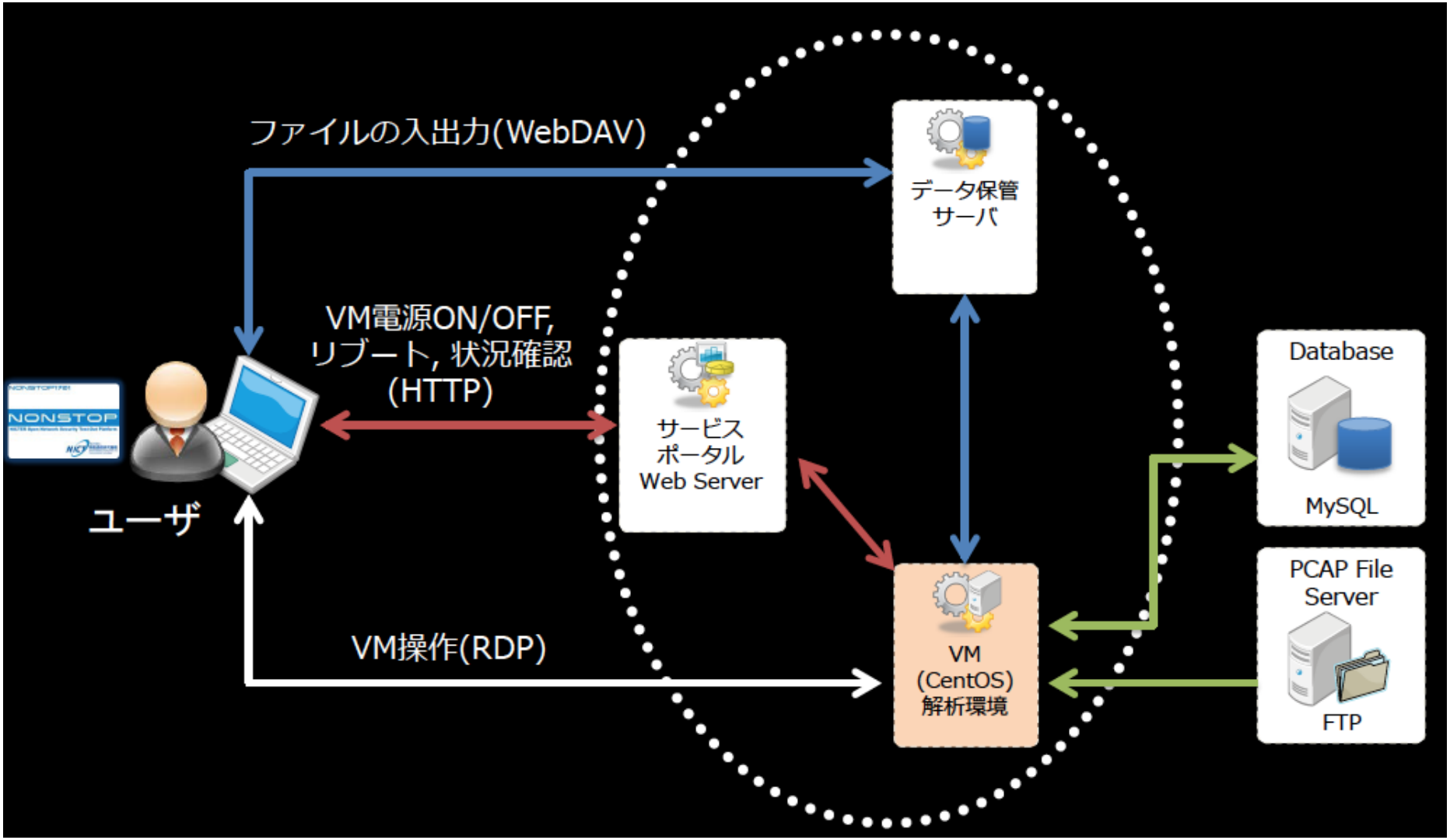
提案：複数ポートを偵察に同時利用

- 観測点検出成功率Up
- 偵察行為の秘匿性Up

の危険性を示した

複数ポートによる偵察手法を開発

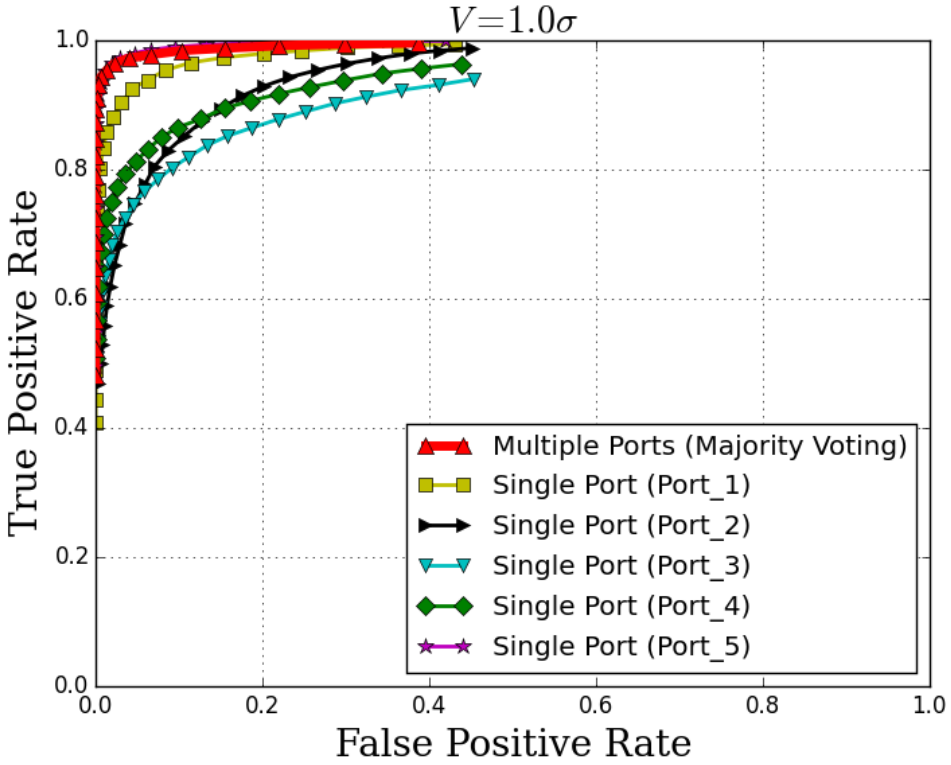
評価環境 (NONSTOP by nicter)



提供資料: 情報通信研究機構 サイバーセキュリティ研究室 笠間氏

攻撃性能の評価結果

ROC曲線：縦軸が観測点検出成功率，横軸が誤検出率
→ 曲線が左上に近づくほど正確な検出ができることを意味する



Parameters	Value
秘匿シグナルパターン	10,000
偵察利用ポート数	5
偵察パケット数 (V)	0.8σ ～ 1.0σ
符号語長	64
観測点判定の閾値	0.02 ～ 0.50

攻撃者が，より高い精度で観測点を検出できる可能性

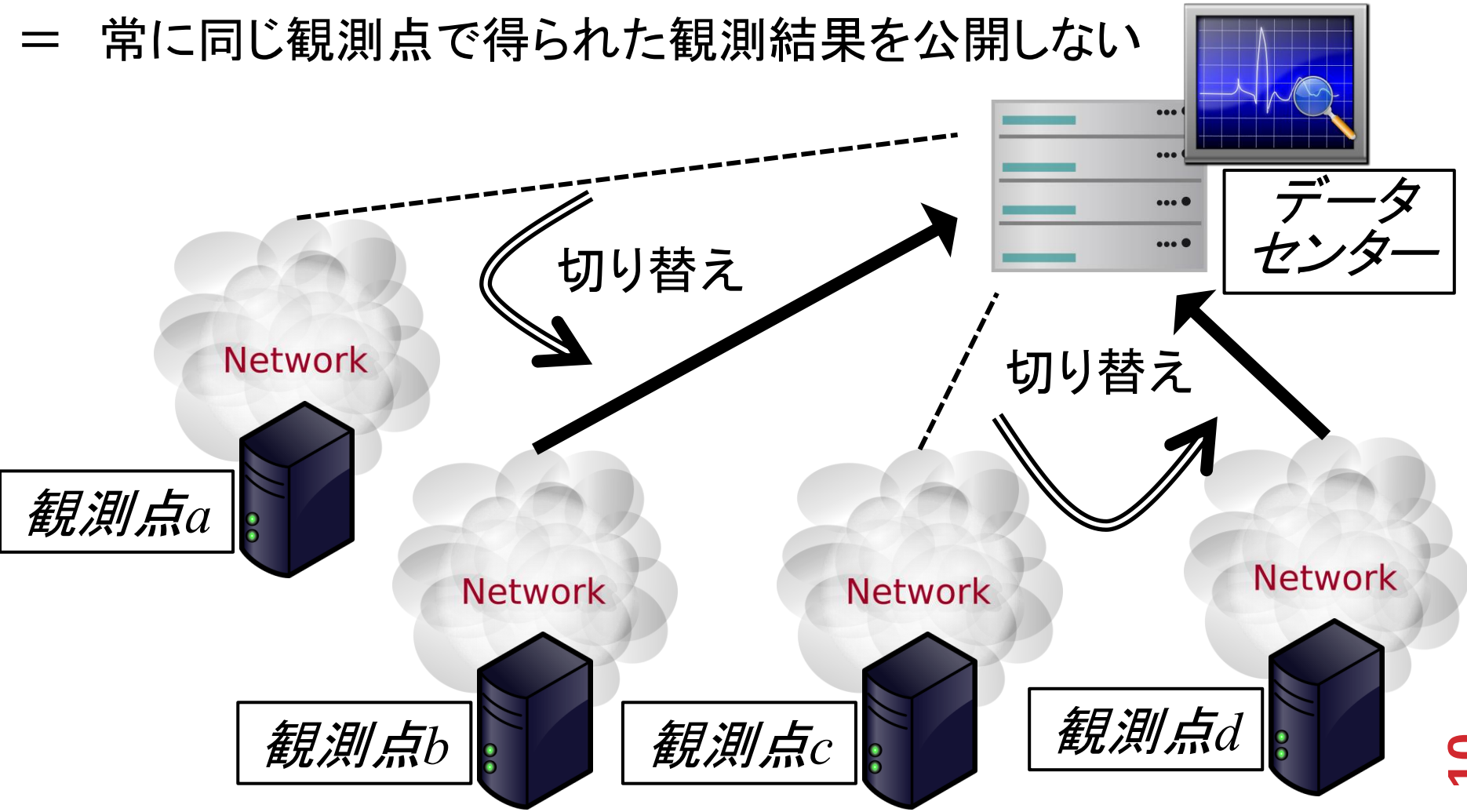
σ：各ポート平常時の到着パケット数の標準偏差（送出する偵察パケット数の基準となる）

研究成果② 防御手法の提案

動的観測手法という新たな観測手法を開発

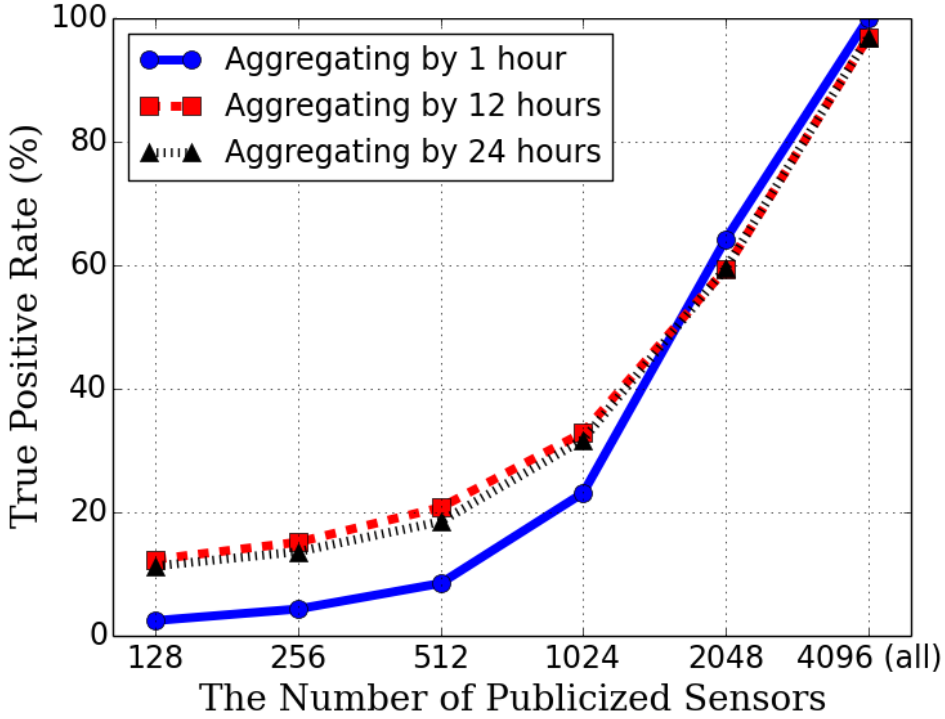
観測点を動的に切り替えながら到着パケットの捕捉を行う

＝　常に同じ観測点で得られた観測結果を公開しない

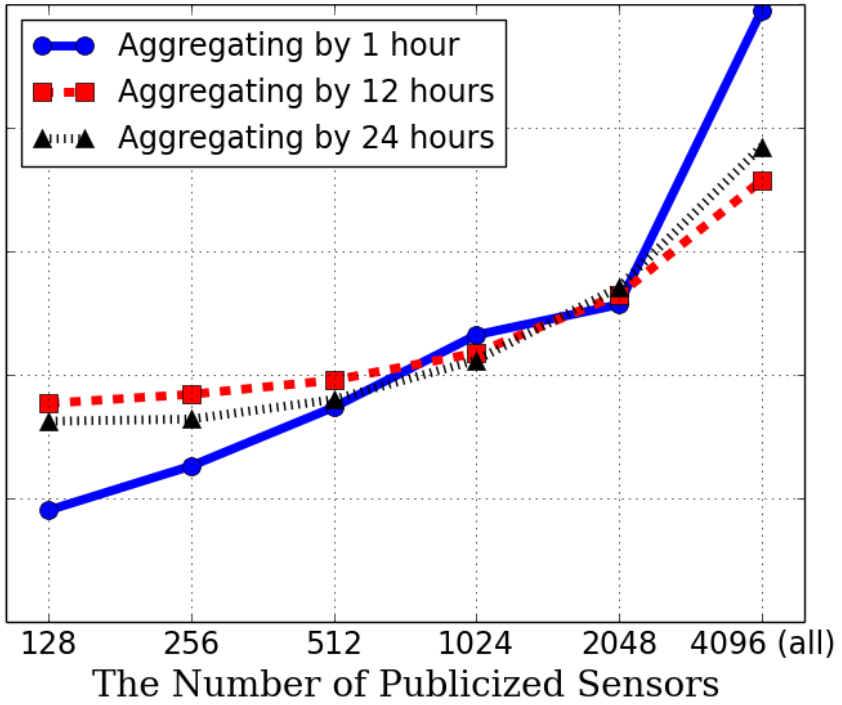


防御性能の評価結果

22/tcpポートへの偵察の防御結果



8080/tcpポートへの偵察の防御結果



各ポート平常時の到着パケット数の影響は受けるが
総じて攻撃者の攻撃成功率を低下させた

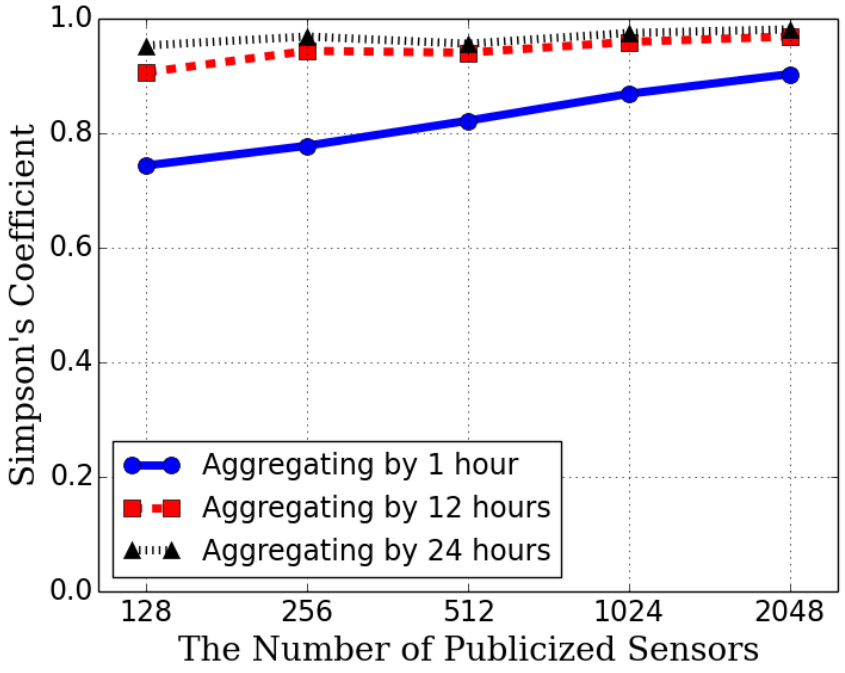
提供可能な観測情報の比較

既存手法

全観測点を集約して得られた観測パケット数の上位10件のポート番号の集合A

提案手法

動的観測手法で得られた観測パケット数の上位10件のポート番号の集合P



上記がどの程度一致するか
シンプソン係数で評価

$$sim = \frac{|A \cap P|}{min(|A|, |P|)}$$

従来システムに約80%～90%
近似した情報を提供可能

まとめ

- 攻撃者の視点から観測点検出攻撃の改良を検証
  - 実際の観測データを基にシミュレーションを行い，有効な防御手法の開発が必要であることを示した
- 観測点検出攻撃に対して動的観測手法による対策を提案
  - 攻撃者の観測点検出成功率を低下させることができた
  - 従来手法と比較しても遜色ない観測情報の提供が可能

本研究の貢献と応用例

本研究の貢献

インターネットの安全な利用を促進

→ 今後の情報通信技術の発展に不可欠

応用例

サイバー攻撃情報を迅速に提供する方法の研究

→ 災害情報と同様にサイバー攻撃情報も迅速に提供する

今後の展望

- モノのインターネット (Internet of Things, IoT) 時代のサイバーセキュリティ
  - パソコンやスマートフォン等のようなIT機器だけでなく，家電製品をはじめとしたあらゆるモノがインターネットに接続する時代が到来

➢ インターネットへの接続機能を持った組み込み機器への攻撃が今後増加すると考えられる

- 新たな攻撃監視対象の例
  - スマートホーム
  - ドローン
  - 自動運転車　など