TDU 東京電機大学 TOKYO DENKI UNIVERSITY

インターネットセキュリティのフルスペックを極める

自律分散型インターネットセキュリティ基盤
Autonomous and Distributed Internet Security Infrastructure
の概要と実現課題

AIS研究プロジェクト

2017年3月14日

東京電機大学

小林 浩†, 八槇 博史‡, 米﨑 直樹, 君山 博之

上野 洋一郎, 堤 智昭, 佐野 香, 佐々木 良一

†プロジェクト代表, ‡プロジェクト副代表

内　容

1. 研究の背景
2. サイバー脅威根絶に向けて
3. 自律分散型セキュリティ基盤の概要
4. サイバー攻撃遮断実験
5. 技術課題
6. まとめ

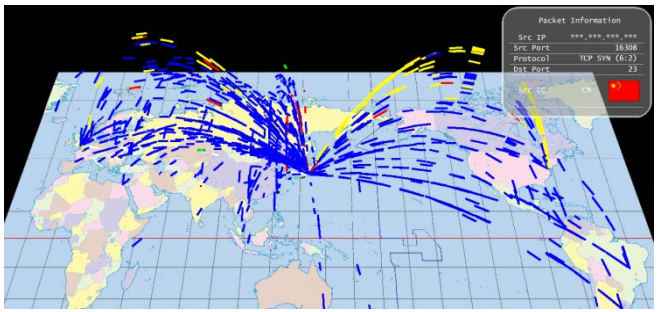
1. 研究の背景

- 過激化・組織化するサイバー攻撃が世界の大きな脅威
  - DDoS攻撃や標的型メール攻撃等々
    - 2011年のサイバー攻撃による全世界の損害額：0.3～1兆米ドル
  - IoTデバイスの急増は，さらなるサイバー脅威に
    - 探索パケットによるマルウェア感染，製造工程で埋め込まれることも
    - 数万台のIoTデバイスをハイジャックした600Gbps超のDDoS攻撃が2016年散発
    - 2020年には500億台のIoTデバイスがインターネットに接続
    - もし500億台の1%が悪用されれば，6Pbps超のDDoS攻撃も
      500億台×1%×（1500B×1kpps）/台 ⇒ 6Pbps
  - “自分を守るセキュリティ”から“グローバルセキュリティ”への転換が必要!
- インターネット全体の安全性を高める“自律分散型インターネットセキュリティ（AIS）基盤“を提案.

DDoS：Distributed Denial of Service, IoT：Internet of Things

2. サイバー脅威根絶に向けて

- 攻撃パケットをIPレイヤで分類
  1. **送信元詐称IPアドレス**
     - ランダムな送信元IPアドレス
       DDoS攻撃で多用
     - 特定送信元IPアドレス（標的ノードのIPアドレス）
       DNSリフレクション攻撃やNTPリフレクション攻撃など
  2. **送信元非詐称IPアドレス**
     - 不特定宛先IPアドレス（ダークネット*で観測）
       無防備なIoTデバイスを，総当たり攻撃でマルウェア感染させる**探索パケット**など
     - 特定宛先IPアドレス
       ハイジャックされたIoTデバイスからのDDoS攻撃など
  3. **匿名IPアドレス**（接続経路を隠ぺい e.g. **Tor**）
     サイバー犯罪やDDoS攻撃の首謀者らが多用



ダークネットを飛び交う探索パケット
出典：nicterweb http://www.nicter.jp/#

*未使用アドレス空間，Tor：The Onion Router

サイバー攻撃対策上の制約と課題

- 日本では「通信の秘密」法から，ISPは大規模なDDoS攻撃を察知しても，ユーザからの対処要請または自身のサービス継続が危うくならない限り対処できない．
- エッジルータのuRPF機能は，送信元アドレスがルーティングテーブルの経路情報に存在しないアドレス詐称パケットを遮断する．
  - ルータの過負荷回避などから，ISPの多くはuRPF機能を設定していない．
    - 攻撃側が圧倒的に有利な原因の一つ．
  - uRPF機能は，不正パケットの転送を逆行経路（送信元IPアドレスへ到達可能な経路）が存在するもののみに制限する重要な役割を担う．

uRPF：unicast Reverse Path Forwarding

既存技術 BGP Flowspecとその課題

- BGP flowspecとは
  - フロースペック・メッセージは，ISPのサービス継続が危うくなった事態やユーザからの対処要請を受けて発行される．
  - BGPルータは，フロースペック・メッセージを受信すると，L3/L4ヘッダ情報をもとに攻撃パケットを遮断または転送先を変える．
- 限界と課題
  - パケットの詳細な属性情報を指定できないため，C&Cサーバからの攻撃指令や探索パケットなどを遮断できない．
  - 偽装メッセージをチェックする手段を持たない．
  - TCPベースのプロトコルであるため，帯域圧迫攻撃を受けると機能しない可能性がある．

BGP:Border Gateway Protocol, C&C:Command and Control

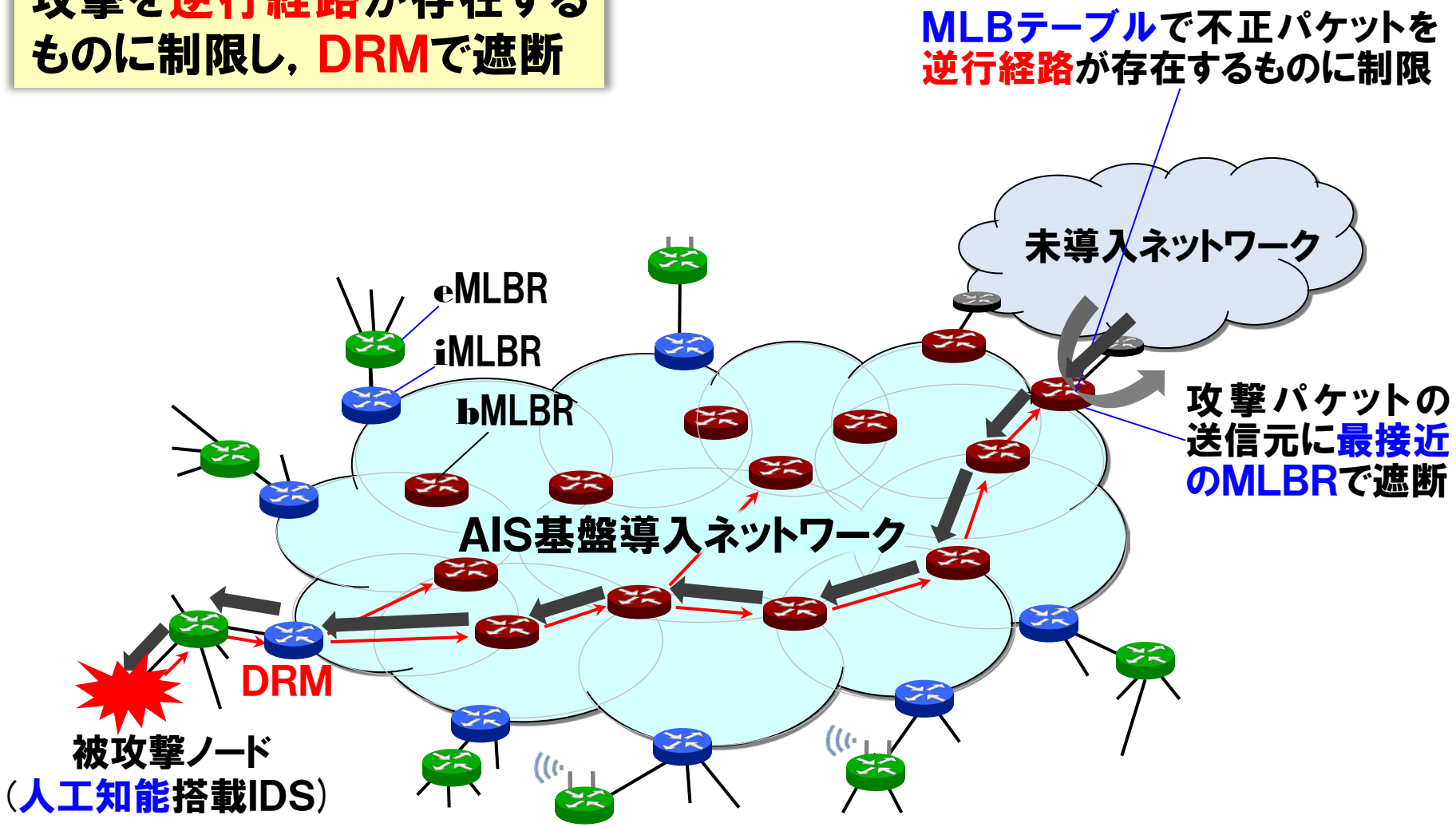
3. 自律分散型セキュリティ基盤の概要

1. ユーザネットワークの出口と，インターネットの入口，及びISP間の境界に，各々eMLBR, iMLBR, bMLBRを配備し，適応型ファイアウォールとして機能するAIS基盤を形成する.
2. MLBRは，MLBテーブルを用いて（uRPFのように）アドレス詐称パケットをフィルタリングし，不正パケットを逆行経路が存在するもののみに制限する.
3. 被害ノードからの逆行経路に向けた廃棄要請（DRM）により，攻撃パケットの送信元IPアドレスに最も接近したMLBRで遮断する.
4. ソフトステート型の認証・検疫などにより，すべてのパケットの送信元をセキュリティ評価し，結果をIPヘッダのTOSフィールドに附す．パケットを受信するか否かの判断は受信者に委ねる.
5. AIS基盤は，人の作為が入らないよう機械的運用を軸に，公平・中立・公正性をベストエフォートで実現する.
6. ISPやエンドユーザに自発的な導入を促すインセンティブ・メカニズムを導入する .

MLBR:Multi-Layer Binding Router, e:egress, i:ingress, b:border, DRM:Dropping Request Message, TOS:Type of Service

自律分散型セキュリティ基盤のキー機能（1）

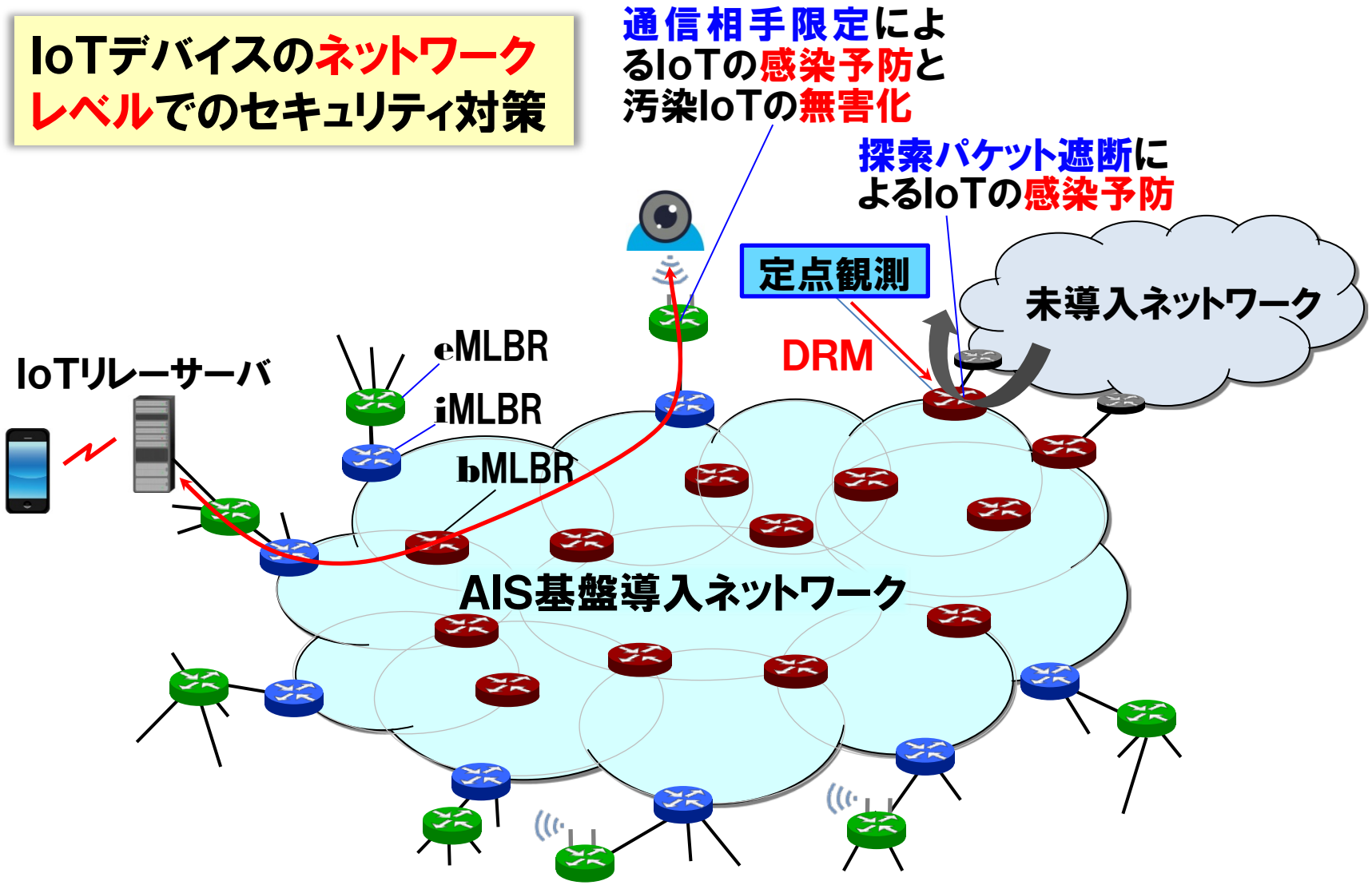
攻撃を逆行経路が存在するものに制限し，DRMで遮断



IDS：Intrusion Detection System

自律分散型セキュリティ基盤のキー機能（2）

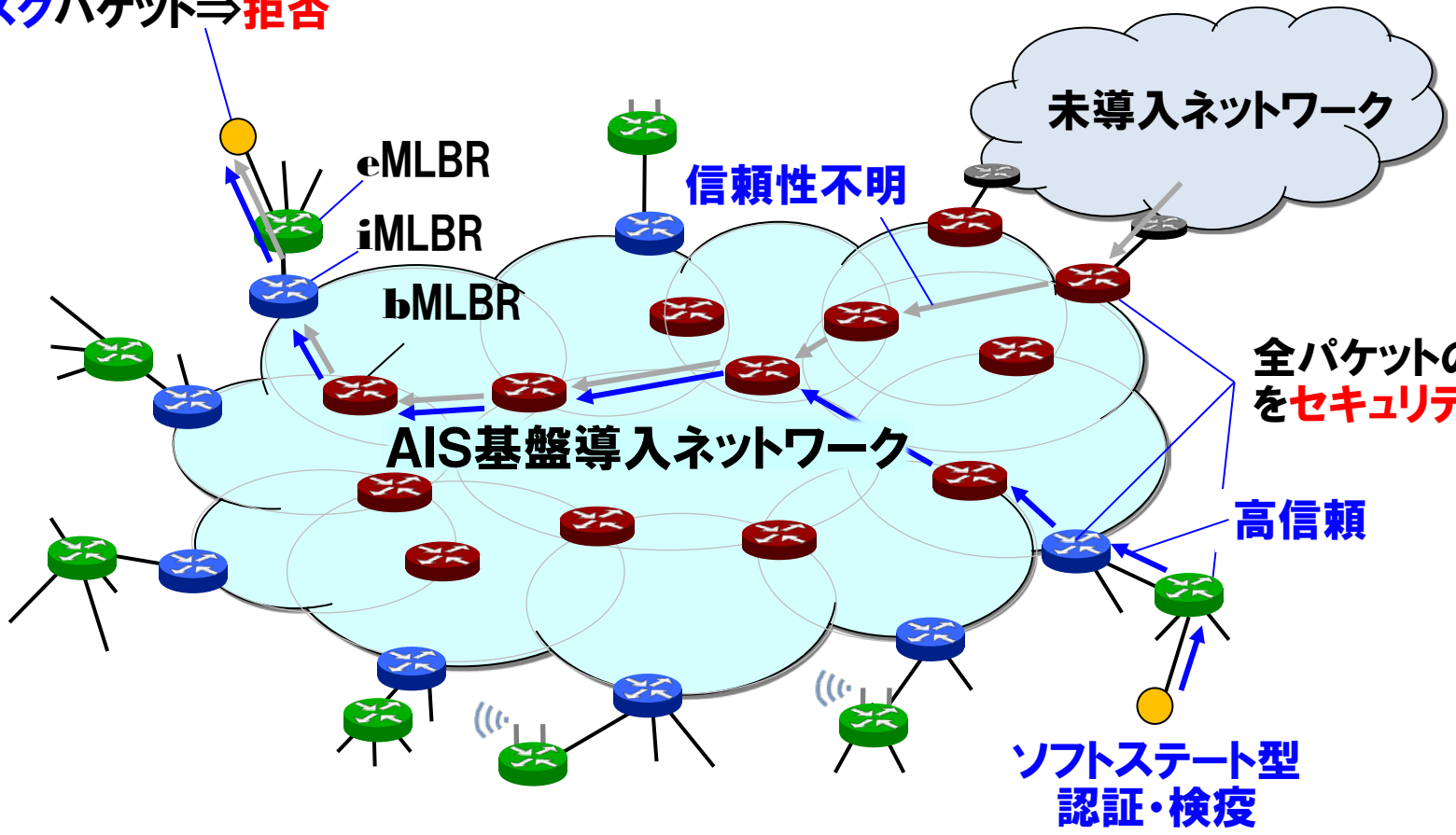
IoTデバイスのネットワークレベルでのセキュリティ対策



自律分散型セキュリティ基盤のキー機能（3）

【受信側での判断例】
高信頼パケット⇒受信
信頼性不明パケット⇒検査のうえ受信
匿名アドレスパケット⇒拒否
ハイリスクパケット⇒拒否

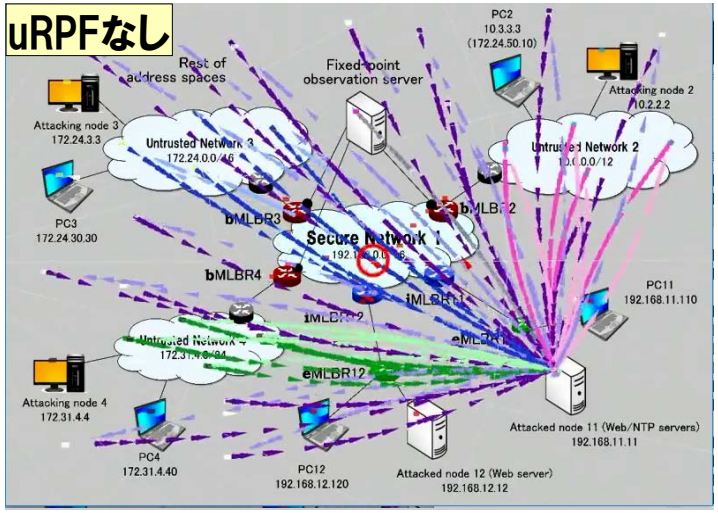
すべてのパケットに
セキュリティ評価を附す



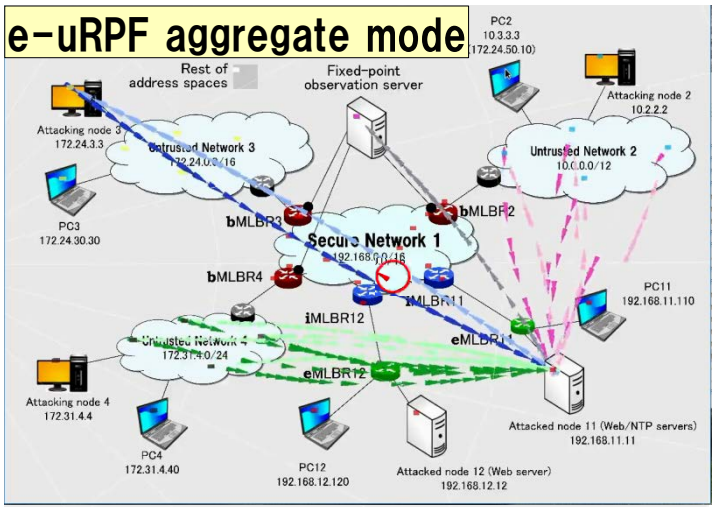
4. サイバー攻撃遮断実験

OpenFlowでMLBRを試作し，実験用テストベッドを構築
NIRVANA-Rでトラヒックを可視化（送信元と宛先IPアドレス2点間の軌跡として描画）

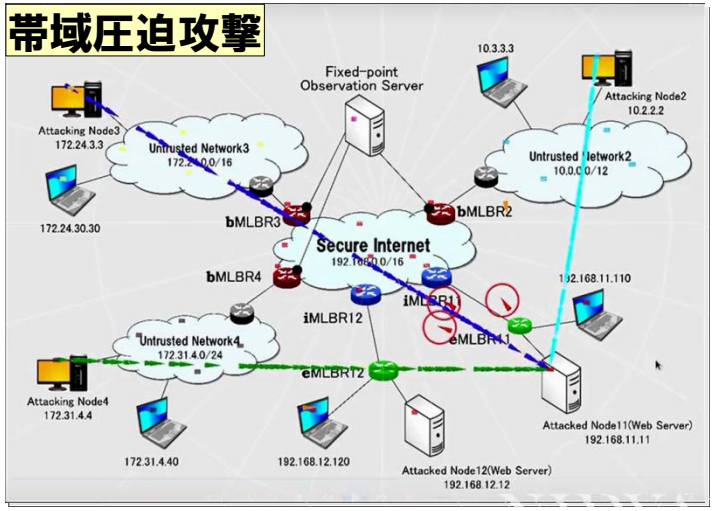
uRPFなし



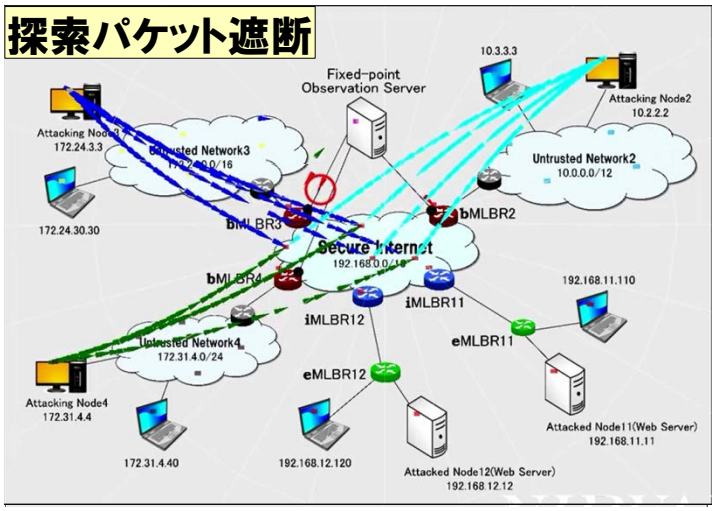
e-uRPF aggregate mode



帯域圧迫攻撃



探索パケット遮断



【他に行った遮断実験】

e-uRPF loose mode
パケットの誤廃棄抑制

NTPリフレクション攻撃
DRMリレーによる攻撃元最接近MLBRでの遮断
ほか

5. 実現課題 MLBテーブルとスケーラビリティ

- 不正パケットを**逆行経路**が存在するもののみに制限するよう，各ルータには次の**e-uRPF mode**を設定する．

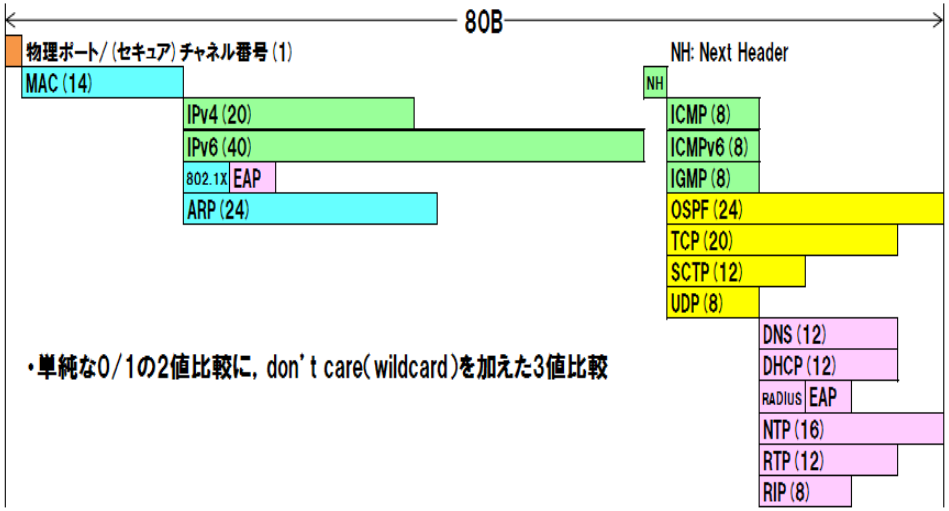
ルータ	e-uRPF mode	対象アドレス	サイズ	備　考
eMLBR	fully strict mode	L1, L2, L3+AH	10～1k	詐称パケットを完全排除
iMLBR	strict mode/ loose mode	L1, L3/L3+AH	2k～3k	エッジルータのuRPF相当
bMLBR	aggregate mode	他ISPから流入する全L3	0～**1M**	逆行経路上でuRPFが機能していれば**不要**

- 未導入ISPに隣接するbMLBRのサイズ肥大対策
  - uRPF設定状態**調査ロボット**の導入
  - uRPF未設定ISPへの**uRPF設定**要求，**ペナルティ課金**請求
  - **高性能ソフトルータ**（100Gbps）の出現により，コストは1/10以下に

e-uRPF:equivalent uRPF, AH:Authentication Header

廃棄要請プロトコル（DRP）と廃棄テーブルのスケーラビリティ

- DRPは，被害ノードから攻撃パケットの送信元に最接近のMLBRへDRMをUDPを用いてリレー転送するためのプロトコル．
  - DRMには，正常パケットの誤廃棄を防ぐため，L1～L7のヘッダ情報を記述でき，その真正性・統合性検証のための認証コードが付加される．
- 未導入ISP隣接bMLBRのサイズ肥大対策
  - TCAMは消費電力大（50W）かつ高価
    - ソフト処理による低コスト化
    - 廃棄テーブルのコンパクト化が必要
  - 1対多／多対多型断続的攻撃遮断用DRMの集約化
    - 標的型攻撃やゼロディ攻撃の抑制
  - 複数MLBRによる分散遮断

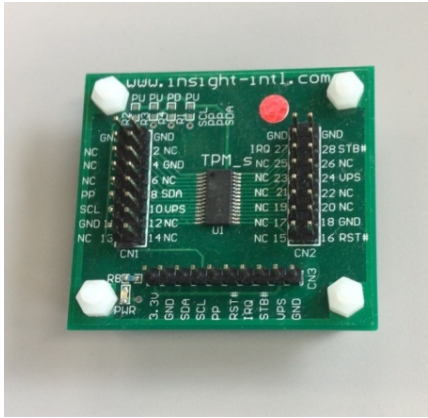


- AIS基盤内は，TCAMを用いてワイヤスピードで処理

DRP：Dropping Request Protocol, TCAM：Ternary Content Addressable Memory

TPMによる信頼基盤と，安全なプロトコルの実現

- MLBRやDRMを発信するIDSがマルウェアに感染すれば，AIS基盤の**安全**や**信頼**は成り立たなくなる．
- MLBRやIDS，DRMの**真正性・統合性**を検証できる仕組みが必要．
- **TPM**：耐タンパー性のあるセキュリティモジュール
  - EK鍵（TPM識別用），AIK鍵（署名用），STK鍵（暗号用）などを提供
  - **認定機関**は，各機器の**EK公開鍵**とMLBRのディスクイメージや検知エンジンの機械学習済みデータの**ハッシュ値**を管理し，各機器の真正性の保証やDRMの統合性検証，AH用共有鍵交換などのための**信頼基盤**を担う．
- 標準化への取り組み
  - AIS基盤実現に必要な**プロトコル**を形式的に厳密に定義し，**形式手法**を用いてプロトコルにセキュリティホールがないことを証明する．
  - プロトタイプ実装を行い，様々な検証実験を通して**機能上の完全性**を検証した上で，IETFなどで標準化していく．



TPM

TPM：Trusted Platform Module, EK：Endorsement Key, AIK：Attestation Identity Key, STK：Storage Key

機械学習を用いたサイバー攻撃検知/認証・検疫

- 過去の経験から未知の攻撃を検出する機械学習（AI）は，プログラムコードやパケットシーケンス，ログを入力すると，直ちに判定結果を出力する．
  - Cylance/日立：数100万の特徴コードを機械学習し，既知・亜種・未知のマルウェアを検出
  - Cybereason/ソフトバンク：プログラムの挙動を機械学習し，脅威を自動検出
  - NTT Com：過去の侵入手口を機械学習し，機密情報の漏洩前に自動遮断
  - MIT CSAIL：攻撃検知システムAI2…2000万ユーザ/36億ログを学習
- 機械学習には膨大かつ新鮮な学習用データと，GPUなどを用いたHPC環境が必要だが，学習済データを用いた判定は汎用PCで実行できる．
  - 研究用データセット：BOS, NICTER Darknetset, CCC DATAset, D3M他
- IDSは，検出漏れや誤検出を抑制するため，専門ベンターや手法が異なる複数の検出エンジンを組み合わせる必要がある．
- ソフトステート型認証・検疫によるパケットのセキュリティ評価
  - ログイン後の継続的本人確認
  - マルウェアからパケット送信していないか常時監視

HPC：High Performance Computing, GPU：Graphics Processing Unit

インセンティブ・メカニズム・デザイン

- ISPやエンドユーザにAIS基盤の自発的導入を促す仕組みが必要

【エンドユーザ】
- 企業ユーザ：現行の自分を守るセキュリティ対策コスト » 導入後コスト
  〃 〃 セキュリティ脅威リスク » 導入後リスク
- 一般ユーザ：プロバイダ接続料 « 移動体通信料金
  - 料金制度の見直しが必要

【AIS基盤導入ISP】
- 企業や一般ユーザとのセキュリティ脅威対処契約による収入増
- Tier-1：サービス品質の向上
- Tier-2：トランジット料金の削減

【AIS基盤未導入ISP】
- 未導入ISPからのパケットのセキュリティ評価は“信頼性不明”に設定される，
  - パケットごとに検査＋MLB/廃棄テーブルでのソフト処理⇒レスポンスの低下
  - 受信者によっては受信拒否⇒サービス性の低下
- bMLBRで詐称パケットを廃棄したISPは，uRPF未設定ISPからペナルティとして廃棄処理料金を徴収する．

6. まとめ

- 攻撃側が圧倒的に有利なゆえに，これまでの“自分を守るセキュリティ”から“グローバルセキュリティ”への転換が必要である．
- AIS基盤が，極めて有効なソリューションになる．
- 構成要素：MLBR，TPM，AI技術
- キー機能：(1) 攻撃を逆行経路が存在するものに制限し，DRMで遮断
  (2) IoTデバイスのネットワークレベルでのセキュリティ対策
  (3) すべてのパケットにセキュリティ評価を附す
- 上記機能のプロトタイプをOpenFlowで試作し，小規模なテストベッドで様々な検証実験を行ってきた．
- AIS基盤の自発的導入を促せれば，無防備なIoTが大量に存在しても，インターネット全体の安全性を高められる．
- 実現には，共同研究／研究支援／研究助成が必要．

“自分を守るセキュリティ”から“グローバルセキュリティ”へ

towards Global Security from Individual Security

ご清聴ありがとうございました.

AIS研究プロジェクトは，公益財団法人セコム科学技術振興財団
の研究助成を受けて進めています.