National Institute of Advanced Industrial Science and Technology
AIST

KDDI R&D LABS

超高速ネットワークに対応した悪意のある通信の遮断技術の研究開発（072003008）

数十ギガ～数テラbpsの超高速ネットワークに対応するセキュリティー装置

（独）産業技術総合研究所
戸田賢二

National Institute of Advanced Industrial Science and Technology
AIST

KDDI R&D LABS

概要

1. 悪意のある通信とネットワークの超高速化

2. テラbps対応ネットワークセキュリティー装置
   - ハードウエア：拡張可能60ギガbps光通信FPGAボード
   - 論理回路：有害サイト遮断、ネットワーク侵入遮断、
     コンピューターウイルス遮断、パケットキャプチャー
   - ソフトウエア：フィルタリングリストの自動生成
   - 性能と機能の強力な拡張性

3. 成果のまとめ

National Institute of Advanced Industrial Science and Technology
AIST

悪意のある通信とネットワークの超高速化(1)

KDDI R&D LABS

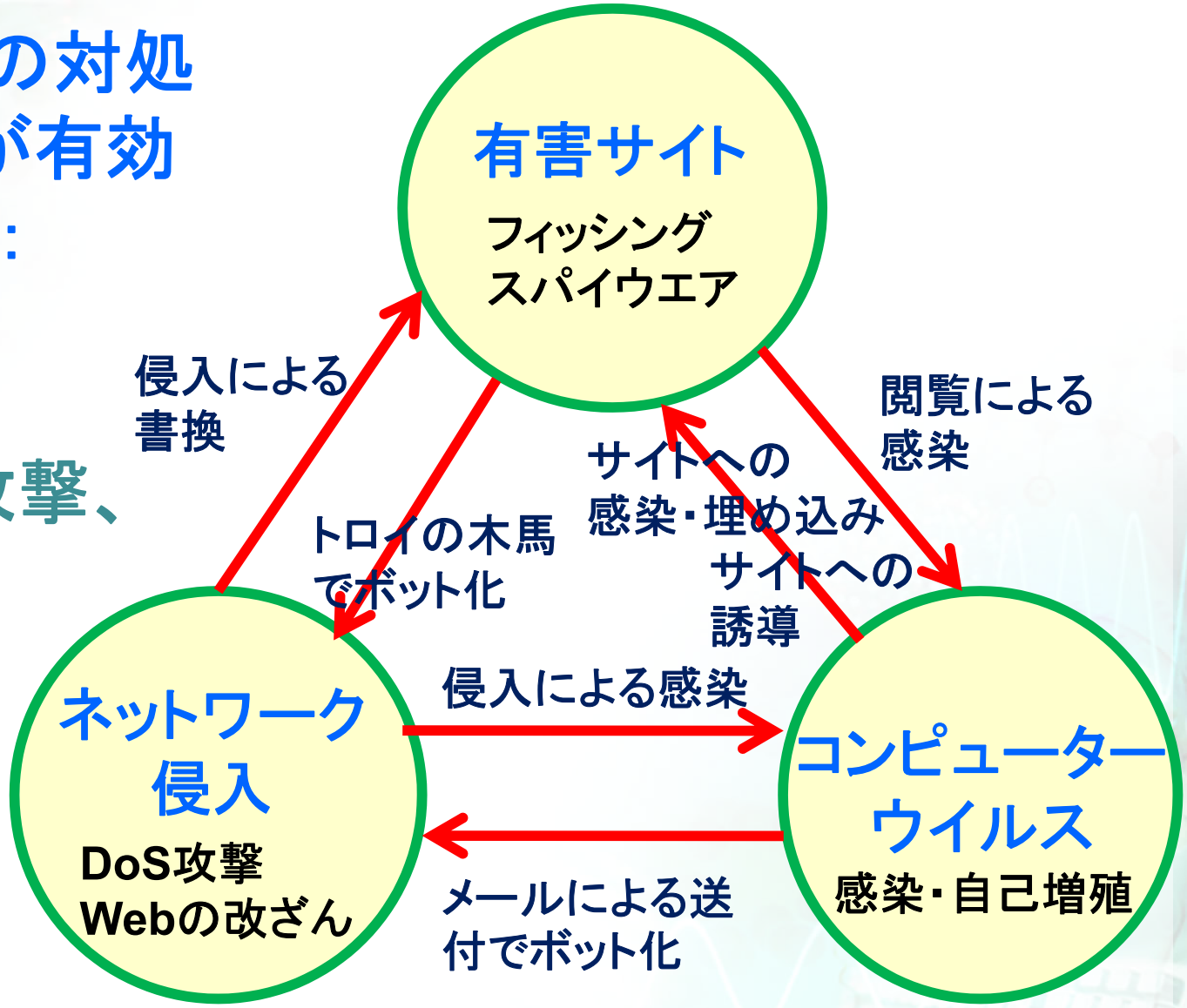
悪意のある通信への対処にはこれらの遮断が有効(ソフトウエアのみ):

重い ← CPU時間

遅い ← 検疫など

無理 ← サイバー攻撃、携帯など

プロバイダや企業では今後、数十ギガbpsを超える速度が必要!



National Institute of Advanced Industrial Science and Technology
AIST

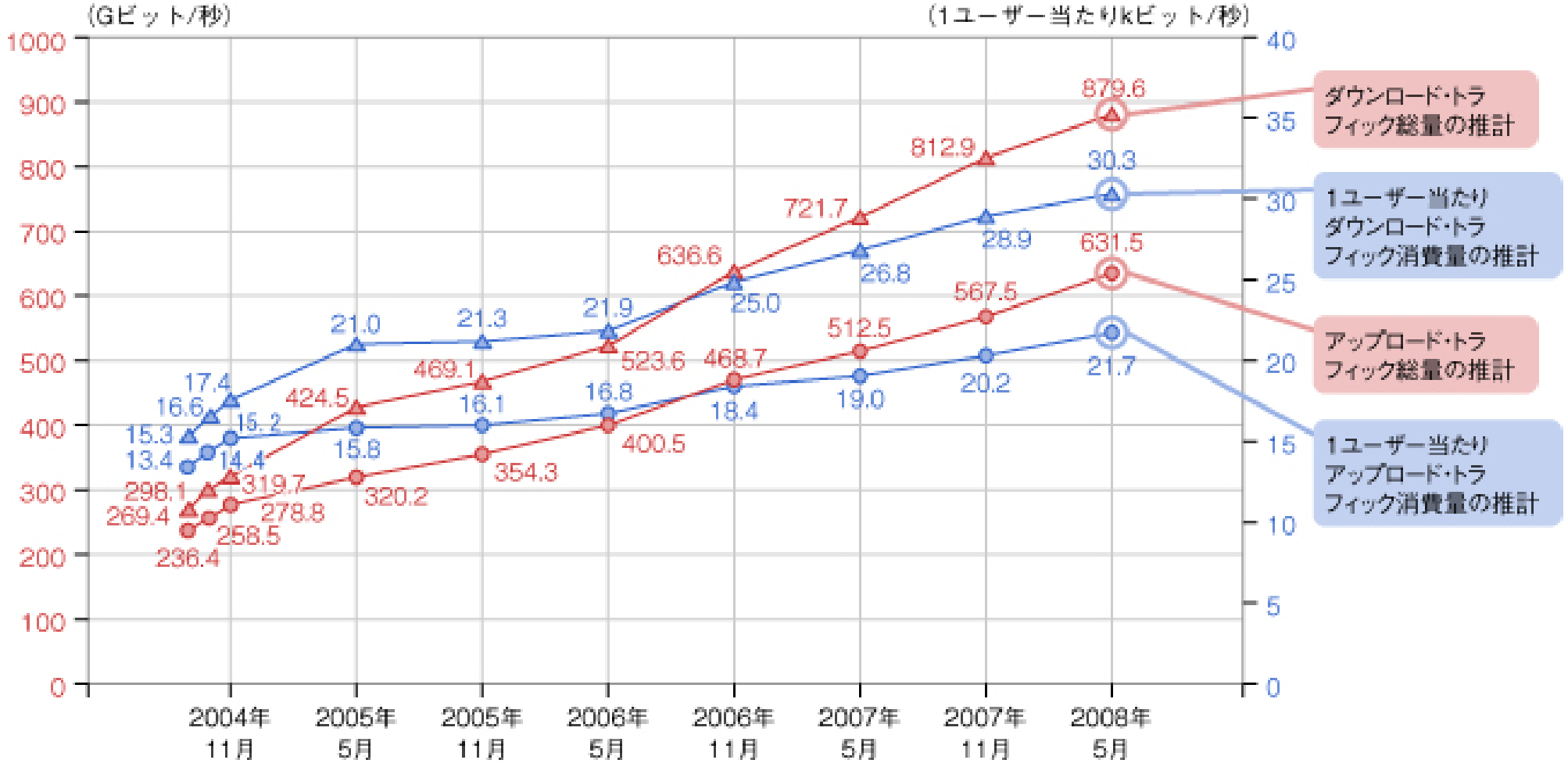
悪意のある通信とネットワークの超高速化(2)

KDDI R&D LABS

●日本のブロードバンド・トラフィック総量の推計

インターネットイニシアティブ(IIJ), NTTコミュニケーションズ, ケイ・オプティコム, KDDI, ソフトバンクBB, ソフトバンクテレコムの6社のデータを基に推計

(出典ITPro http://itpro.nikkeibp.co.jp/article/COLUMN/20081203/320647)



ネットワークセキュリティー装置（全体構成：達成状況）

National Institute of Advanced Industrial Science and Technology AIST

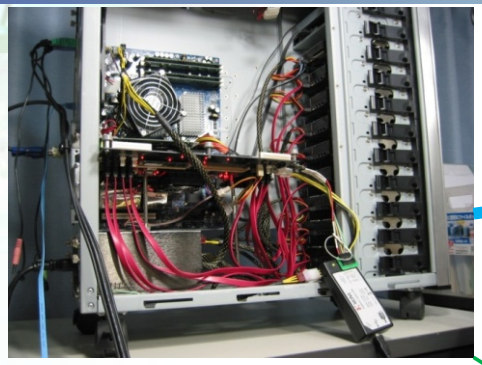
KDDI R&D LABS

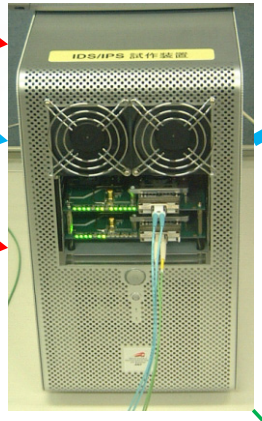
インターネット

有害サイト

ネットワーク侵入

コンピューターウイルス





ユーザー機器

ハードウエアによる高速セキュリティ装置の開発への取り組み

論理回路 on FPGA →

ハードウェア →

侵入遮断（回路）10 ギガbps実測（2007.2発表済）	ウイルス遮断（回路）6.4ギガbps実測（デモ中）	
旧型FPGAボード＋10ギガイーサインタフェースボード		

自動フィルタリングリスト生成（ソフトウェア）		
有害サイト遮断（回路）60 ギガbps実測（デモ中））	キャプチャ（回路）～10 ギガbps	
拡張可能60 ギガbps 光通信FPGAボード on PC		

National Institute of Advanced Industrial Science and Technology
AIST

ネットワークセキュリティー装置（全体構成：見通し）

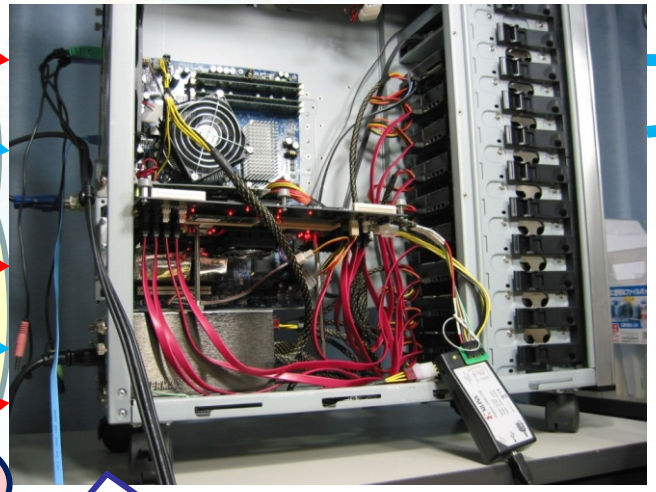
KDDI R&D LABS

インターネット

有害サイト

ネットワーク侵入

コンピューターウイルス



企業やネットワークプロバイダーなどで利用

ユーザー機器

ネットワーク透過型で悪意のある通信のみを超高速で即時に遮断！

論理回路 on FPGA →

ハードウェア →

自動フィルタリングリスト生成（ソフトウェア）

侵入遮断（回路）	ウイルス遮断（回路）	有害サイト遮断（回路）	キャプチャ（回路）
30 ギガbps見込	30 ギガbps見込	60 ギガbps実測	～10 ギガbps

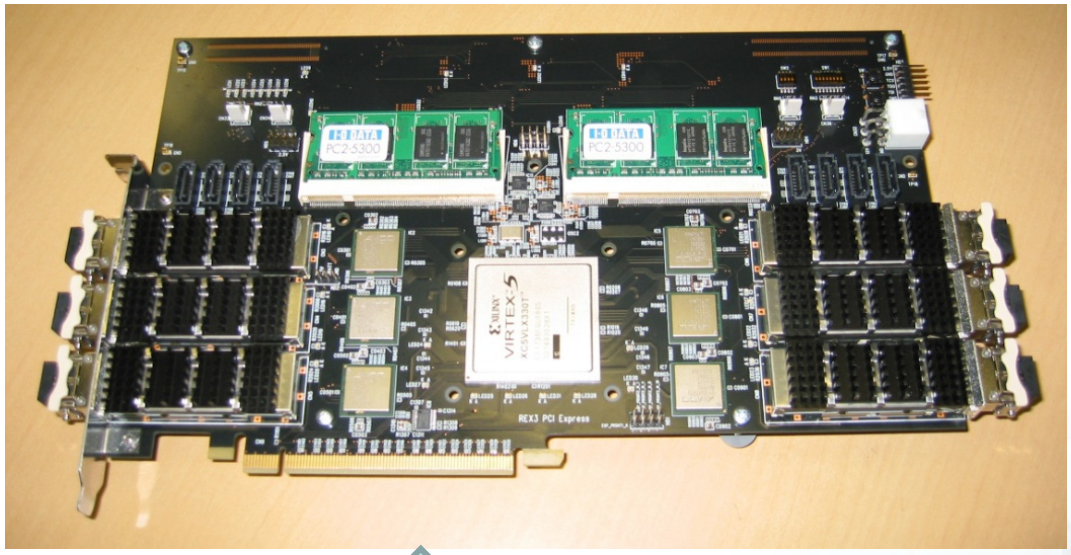
拡張可能60 ギガbps 光通信 FPGAボード on PC

National Institute of Advanced Industrial Science and Technology
AIST

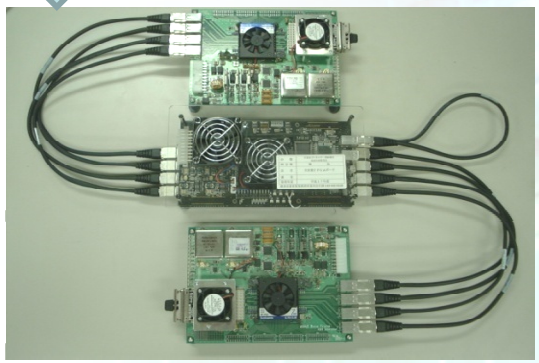
拡張可能60ギガbps光通信FPGAボード

KDDI R&D LABS

- 大容量FPGAデバイス
  （論理回路はネットワークから書換可能）
- 10ギガビットイーサ　6ポート
  (60ギガbps光通信機能)
- PCI-Express カードエッジ
  (16レーン)
- メモリー（DRAM）用ソケット 2個
- ハードディスク接続用（SATA）ポート 8個
- 拡張用ソケット
- サイズ　15cm × 27cm
  （デスクトップPCに1～6枚内蔵可能）



体積当たり
30倍の性能！



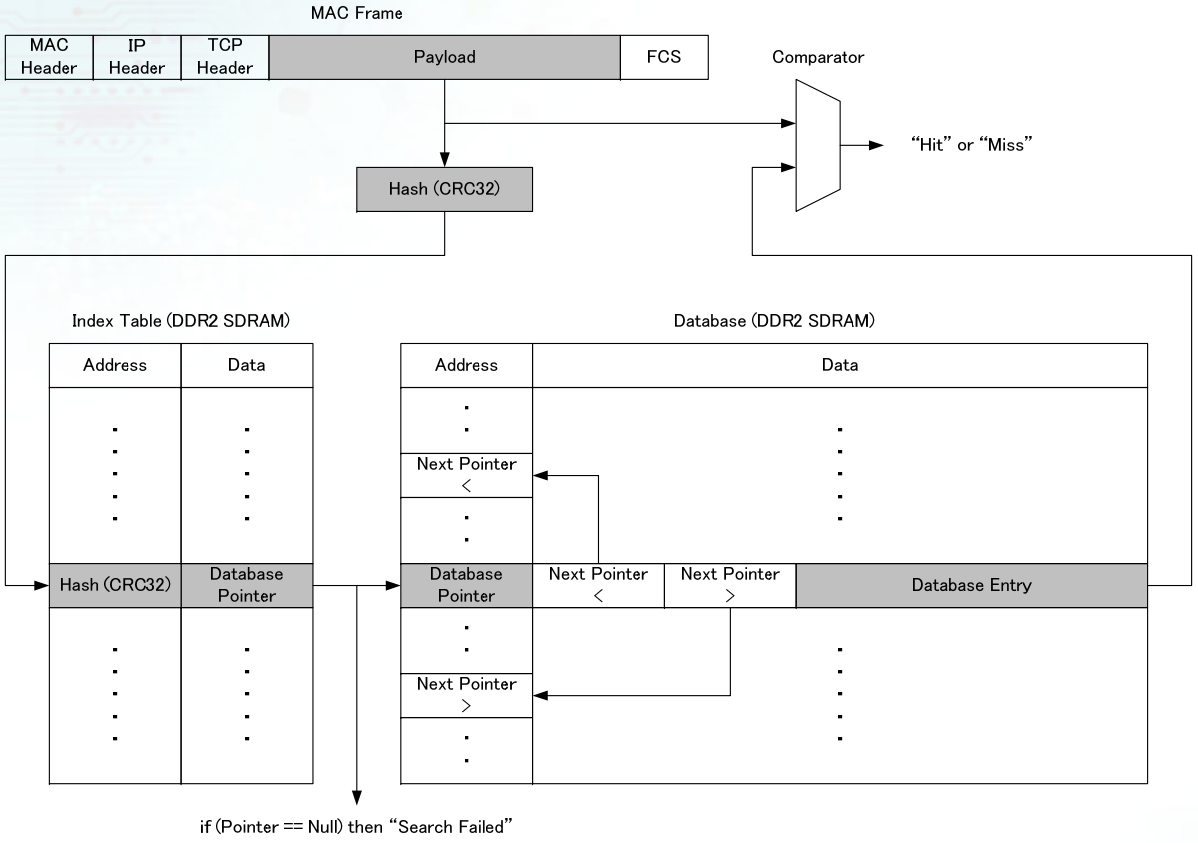
2007.2発表の10ギガbps
侵入防御装置（旧型ボード）

National Institute of Advanced Industrial Science and Technology
AIST

有害サイトの遮断（URLフィルタリング：方式）

KDDI R&D LABS

- ハッシュ＋バイナリサーチ方式をパイプライン回路化
  - 初回、ハッシュを用いることでメモリー参照回数を低減
  - ハッシュ値に複数候補がある場合、バイナリサーチを適用
  - パイプライン化によりメモリバンド幅を有効利用し高速化



自動収集した
34,000エントリー
のリストを使用
（大規模でも問題なし）

→ **256 Bパケットで**
40メガパケット/s
のエンジン性能

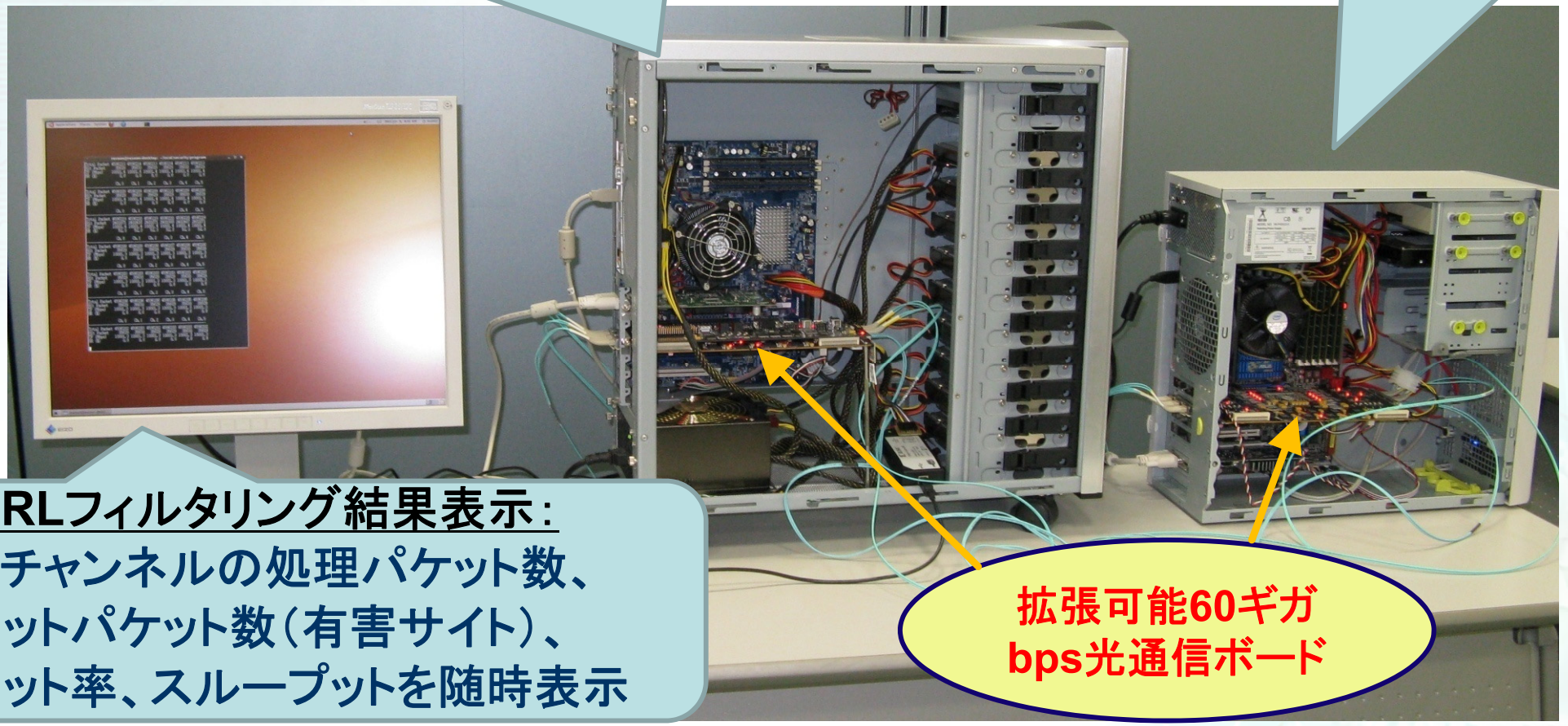
National Institute of Advanced Industrial Science and Technology
AIST

有害サイトの遮断（URLフィルタリング：デモ）

KDDI R&D LABS

URLフィルタリング試験装置：
60ギガbpsのフルレートで有害サイトを含んだデータを送信

URLフィルタリング装置：
有害サイトのみを漏れなく遮断



URLフィルタリング結果表示：
6チャンネルの処理パケット数、
ヒットパケット数（有害サイト）、
ヒット率、スループットを随時表示

→ **60ギガbps達成！**　**消費電力40W！（ボードのみ）**

National Institute of Advanced Industrial Science and Technology AIST

ネットワーク侵入遮断（サイバー攻撃などの遮断）

KDDI R&D LABS

- Snortの1200ルールを論理回路化

条件 & 条件 & … & 条件 → アクション

条件 & 条件 & … & 条件 → アクション

条件 & 条件 & … & 条件 → アクション

条件 & 条件 & … & 条件 → アクション

⋮

→ 複数ルールのパターンマッチング処理を
並列化及び冗長論理削減で高速化＆コンパクト化

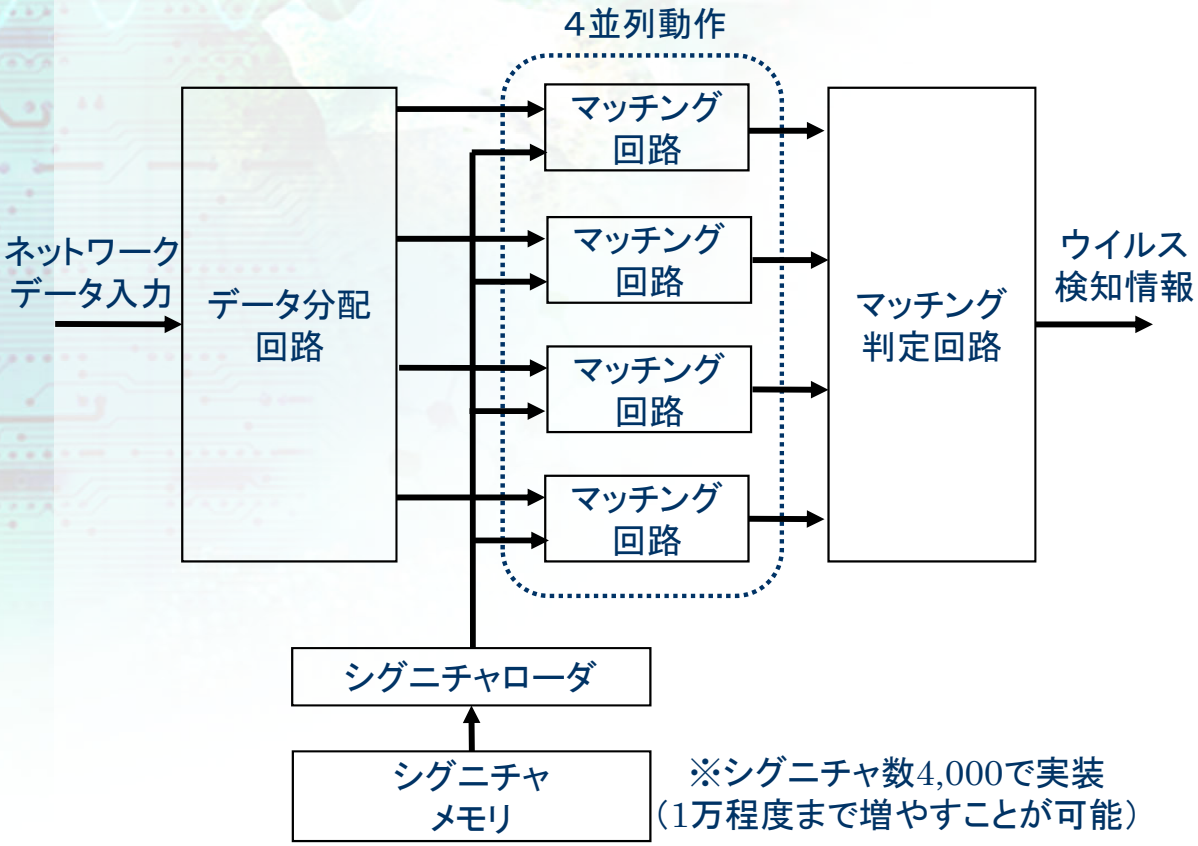
旧型ボードで10ギガbpsを達成済（2007.2発表）

今回開発のボードで 30ギガbpsの予測値

National Institute of Advanced Industrial Science and Technology
AIST

コンピューターウイルス遮断

KDDI R&D LABS



- 多くのウイルス対策ソフトと同じシグニチャ方式を採用
- オープンソースのウイルス対策ソフトClamAVのシグニチャデータベースを使用可能
- 旧型ボード（REX2）上の実装ながら、6.4Gbpsの処理性能を達成
- 高速化の鍵は、元々高速なハードウェアでの実装に加えて、マッチング回路の4並列化、シグニチャデータ配置方式の工夫など

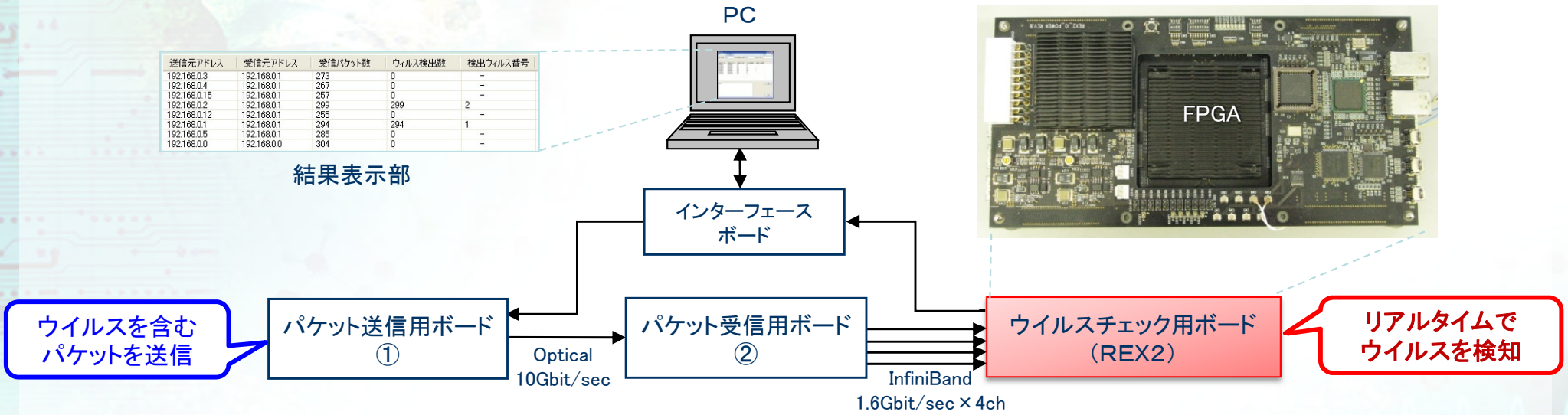
今回開発のボード（REX3）での予測性能は10.4Gbpsであり、3つのデータストリームを並列処理することで30Gbpsで処理できる見通し

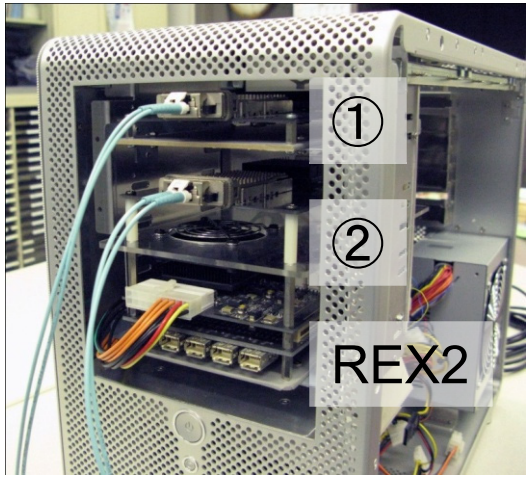
National Institute of Advanced Industrial Science and Technology
AIST

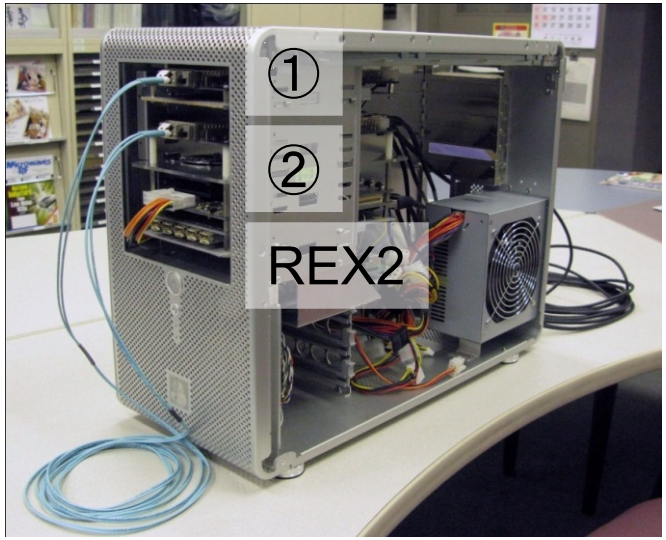
コンピューターウイルス遮断

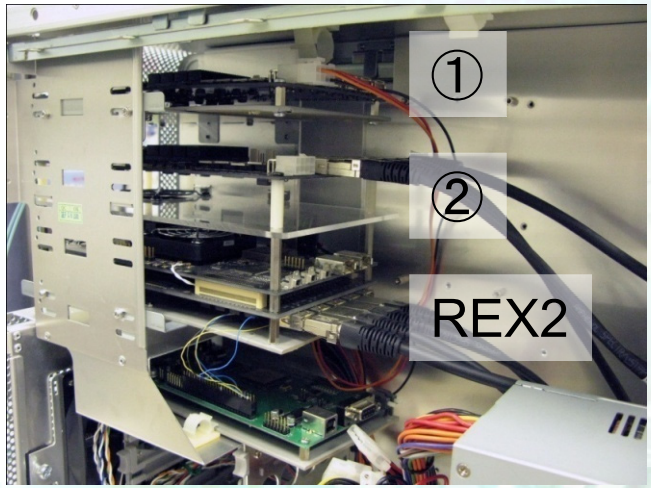
KDDI R&D LABS

展示中のデモシステムの概要





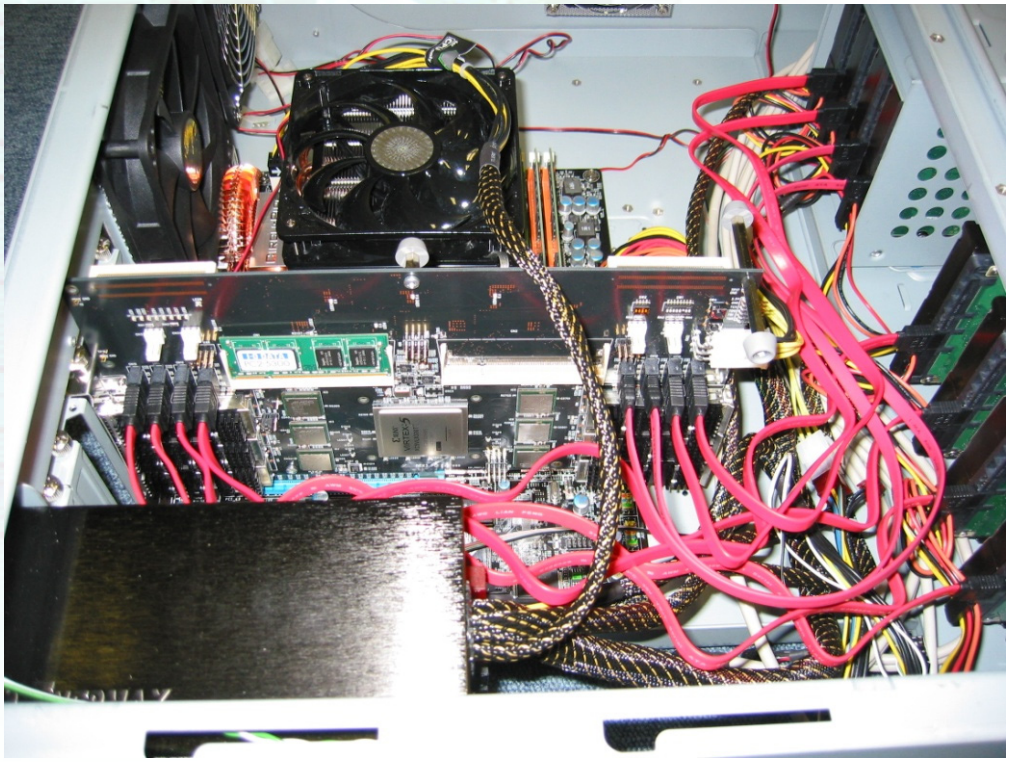




National Institute of Advanced Industrial Science and Technology
AIST

KDDI R&D LABS

パケットキャプチャー

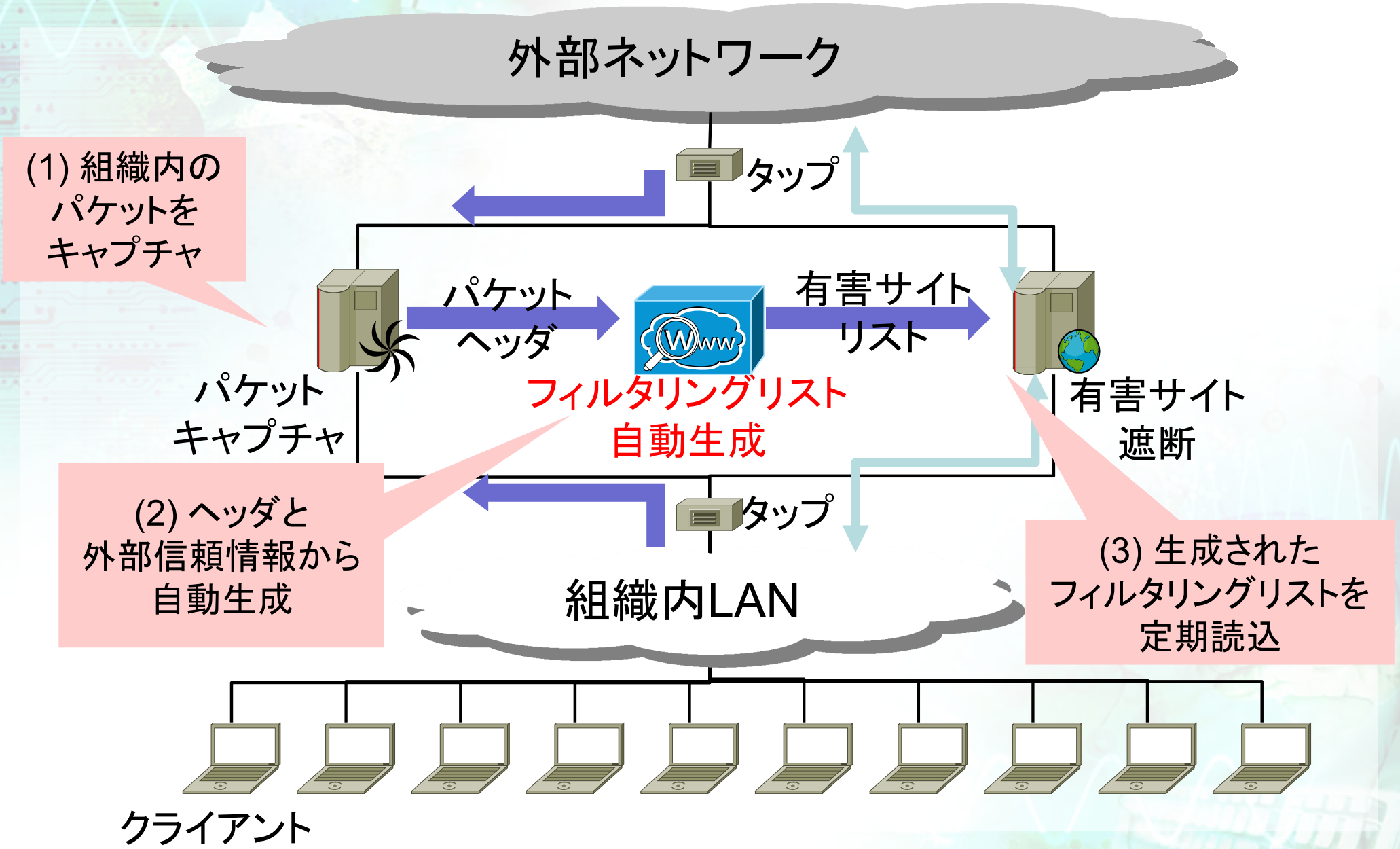


- SATA　8ポートを用いてパケットキャプチャーが可能
- 通信レコーダーやデータベースマシンとして活用可能
- SATAにはHDDの他、RAIDやシリコンディスクも接続可能

National Institute of Advanced Industrial Science and Technology AIST

フィルタリングリスト自動生成

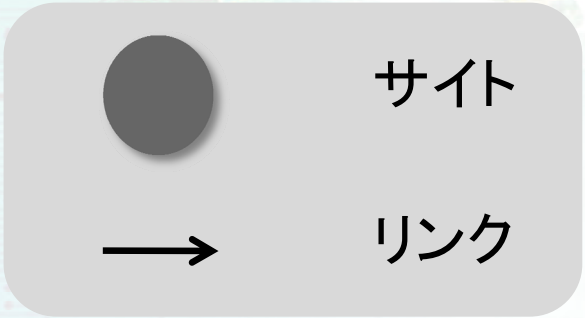
KDDI R&D LABS

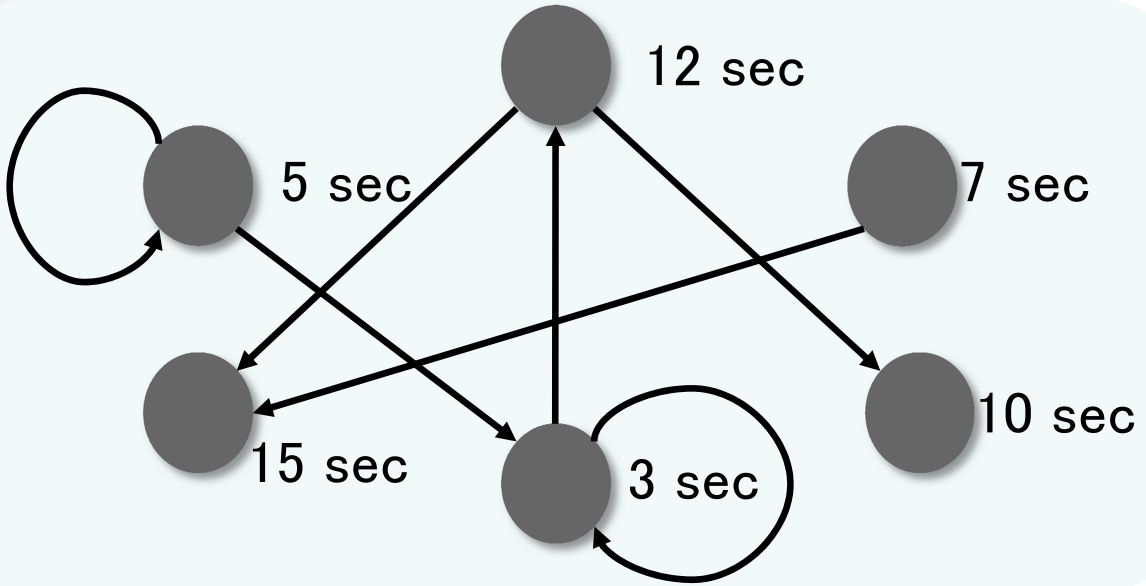


National Institute of Advanced Industrial Science and Technology AIST

フィルタリングリスト自動生成

KDDI R&D LABS





- 時間を考慮したリンク解析
  - HTTPヘッダからユーザのサイト滞在時間を推定
  - サイト間のリンク関係を表すグラフを構築
  - 滞在時間とリンク関係から有害サイトを判定する
  - ユーザ情報を収集するWebバグサイトに対して未知のサイトを含む73.0%以上の検知率を達成
  - 公開されているブラックリストの検知率は約15.5から70.5%程度

National Institute of Advanced Industrial Science and Technology AIST

フィルタリングリスト自動生成

KDDI R&D LABS

4文字	5文字	6文字	7文字	8文字
done	login	paypal	halifax	customer
ebay	index	online	account	security
info	logon	update	banking	includes
aspx	files	images	confirm	wachovia
data	lycos	access	updates	axisbank
hdfc	poste	aecure	catalog	dispatch
bofa	cache	signin	modules	citibank
free	media	lloyds	uploads	language
http	olobi	action	content	onlineid
vndv	abbey	webscr	natwest	register

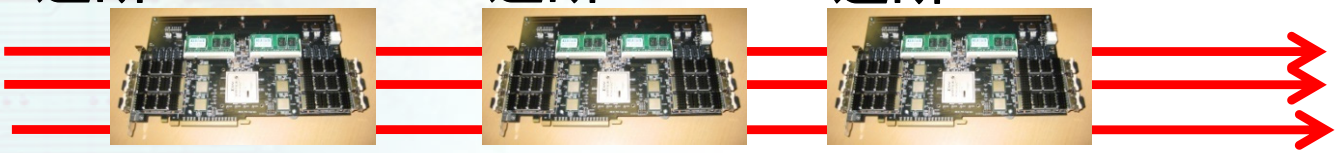
- 文字列の頻度解析
  - HTTPヘッダおよび外部信頼サイトURLを収集
  - URLに含まれる文字列をNグラムによる頻度解析する
  - ユーザのアカウント情報を詐取するフィッシングサイト検知のための文字列を抽出

National Institute of Advanced Industrial Science and Technology
AIST

性能と機能の強力な拡張性

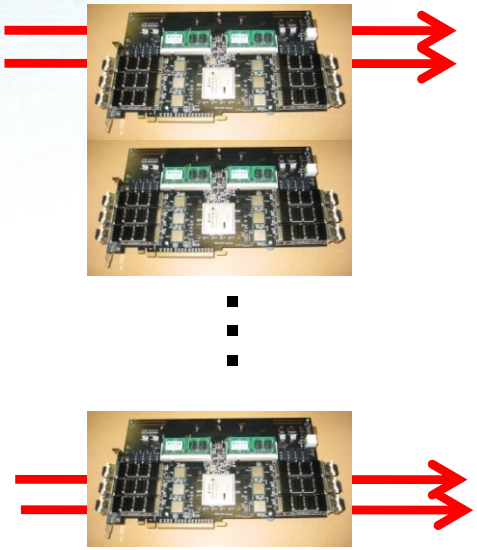
KDDI R&D LABS

ネットワーク侵入遮断　ウイスル遮断　有害サイト遮断



全ての機能を3枚で
30ギガbpsで処理可能！
（デスクトップPC 1台）

有害サイト遮断（60ギガbps/40W）



有害サイト遮断は
17枚で1テラbps！
（デスクトップPC　3台～）

従来の製品の性能を大幅に向上！

（Force10社のPシリーズは、
10ギガbpsでパケット監視を行う）

National Institute of Advanced Industrial Science and Technology
AIST

KDDI R&D LABS

成果のまとめ

- 拡張可能60ギガbps光通信ボードを開発し、セキュリティ装置として、コンパクトかつ省電力でありながら、テラbpsの超高速ネットワークにも対応させた
  - 有害サイト遮断60ギガbps（実測） 40W
  - 侵入遮断30ギガbps（見込）、
  - ウイルス遮断6.4ギガbps（実測）・30ギガbps（見込）

- 即時で高精度な有害サイトの自動収集方式を開発

- 今後、完成度を高め製品化を目指す

- FPGAの回路の書き換えにより、情報収集・データベース応用など用途が広く今後の活用が期待！

National Institute of Advanced Industrial Science and Technology
AIST

参考：6／9プレス発表

KDDI R&D LABS

「数十ギガ～数テラbpsの超高速ネットワークに対応するセキュリティー装置」

http://www.aist.go.jp/aist_j/press_release/pr2010/pr20100609/pr20100609.html

（6月10日新聞掲載）

○日刊工業新聞　朝刊　20面　「産総研とKDDI研、セキュリティー装置を開発、高速ネットワーク対応」

○日経産業新聞　朝刊　12面　「産総研など、テラ級ネット、セキュリティー装置開発、有害サイトを遮断」

（Web情報発信）

○日刊工業新聞 (2010.6.10)

産総研とKDDI研、高速ネットワーク対応のセキュリティー装置開発

http://www.nikkan.co.jp/news/nkx0220100610eaal.html

○朝日新聞 (2010.6.10)

産総研とKDDI研、高速ネットワーク対応のセキュリティー装置開発

http://www.asahi.com/digital/nikkanko/NKK201006100017.html

○RBB TODAY (2010.6.10)

KDDI研、数テラbpsの超高速ネットワークにも対応するセキュリティ装置を開発 ～ 侵入や脅威を即時遮断

http://www.rbbtoday.com/article/2010/06/09/68279.html

※YAHOO!ニュース：http://headlines.yahoo.co.jp/hl?a=20100609-00000026-rbb-sci

National Institute of
Advanced Industrial Science
and Technology
AIST

KDDI R&D LABS

ご清聴ありがとうございました