Android 端末をターゲットとしたボットによる被害防止策の提案

戸田　尚希[†]　鈴木　秀和[†]　渡邊　晃[†]

名城大学理工学部[†]

1　はじめに

近年のスマートフォンの普及に伴い，Android 端末をターゲットとしたボットが登場している．今後のさらなる普及を考えると，Android 端末をターゲットとしたボット対策は重要な課題であると考えられる．しかし，ボットの感染を完全に防ぐ事は難しい．そこでボットの感染は避けられない事を想定し，2 次被害を防止する方法について検討した．

本稿では，Android 端末でユーザが行う特徴的な操作に着目し，ユーザによる操作か，ボットによる操作かを判断して通信の遮断やユーザへの警告を行う事により，Android 端末におけるボットによる被害を防止する方法を提案する．

2　Android 端末で動作するボット

Android 端末で動作するボットは PC の場合と同様に，複数の感染した Android 端末同士でボットネットを構成し，攻撃者（Herder）の命令に従って様々な被害を引き起こす．

図 1 に Android 端末で動作するボットの概要を示す．Android 端末に感染したボットはバックグラウンドで動作し，Herder により指定されたサーバに定期的にアクセスして Herder からの命令を待ち受ける．サーバ経由で Herder からの命令を受けたボットは，その命令に従って Android 端末の位置情報や，保存されている個人情報を送信する．他にも，他端末へのスパムメールの送信や，特定の Web サーバに対して DDoS 攻撃を行う等，ユーザの知らない間に加害者にされてしまう可能性がある．また，ボットの活動によりバッテリの消耗が激しくなる等の被害を受ける可能性がある．

Herder は複数のサーバに接続しているため，仮に 1 つのサーバを停止出来たとしても他のサーバを介して命令を送り続ける事が出来る．このため，ボット対策をサーバに対して施す事は，難しいとされている．

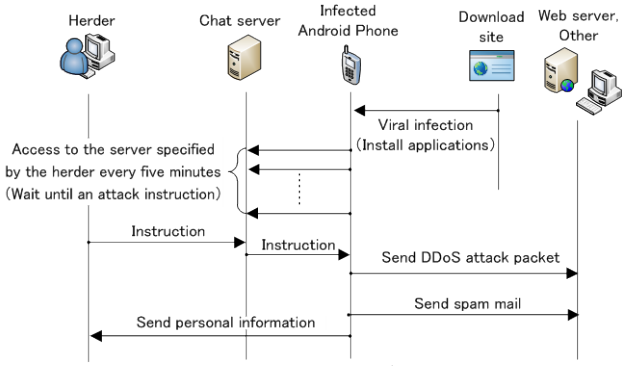


図 1　Android 端末で動作するボットの動作概要

3　既存のボット対策

既存のボット対策として，以下のような方法がある．

① セキュリティ対策ソフトを導入する．
② 信頼できないサイトからアプリケーションは取得しない．
③ Android 端末側で提供元不明のアプリケーションをインストールしない設定をする．
④ アプリケーションインストール時のアクセス許可から必要以上にアプリケーションにアクセス権限を与えていないか確認する．

①における対策は，ボットを含むウイルスの検知・駆除に有効である．対策ソフトとしてはノートン，マカフィー，ウイルスバスターをはじめとするアンチウイルスソフトがある．しかし，新種や亜種といったウイルスは，アンチウイルスソフトでは即座に検出する事が出来ないという問題点がある．

②，③における対策は，正規アプリケーションにボットが内包された海賊版アプリケーションのインストールを防ぐ事が出来る点で有効である．しかし，②，③における対策はユーザ自身が意識して行う対策であり，システムとしてボットの感染を完全に防ぐ訳ではない．

④における対策は，ボットによる必要以上のアクセス許可要求に気付く事が出来ればボットを感染の段階で防ぐ事が出来る点で有効である．

“Proposal of Measures to Prevent Damage from Bots on Android terminals”
†Naoki Toda, Hidekazu Suzuki, and Akira Watanabe
Graduate School of Science and Technology, Meijo University

しかし，一般のユーザが表示されるアクセス許可から不正なアプリケーションかどうかを判断する事は極めて困難である．

このように既存のボット対策は，ほとんどがボットの感染を防ぐための対策であるが，新種や亜種が容易に出回るボットに対応して感染を完全に防ぐ事は難しいのが実状である．

4　提案方式

4.1　ボットとユーザ操作の違い

ボットによる操作とユーザが行う操作には以下のような違いが存在する．メール送信時の送信ボタンを押す操作，Web 閲覧時のブラウザボタンを押す操作，検索時の入力操作がボットにはできないユーザ特有の操作である．従って，Android 端末がネットワークにアクセスする際，直前にこれらの操作があったか確認する事により，正常な送信とボットによる送信を区別できる．

4.2　動作概要

図 2 に提案方式の動作概要を示す．提案方式では，監視プログラムの操作監視モジュールによって常に指定したアプリケーションのキー／ボタン操作を監視して，時間情報と共にログとして残す．ファイアウォールは，通常時は通信を遮断しておく．監視プログラムのパケット監視モジュールは常に送信パケットを監視し，Android 端末からの送信パケットが発生した際に操作監視モジュールによって記録された上記ログをチェックし，正常な送信であるかどうかを確認する．

パケット送信の直前にキー／ボタン操作が行われていた場合，ユーザの意志で送信が行われたものと判断し，パケット監視モジュールによりファイアウォールに対してパケットの通過許可を行う．これにより，正規の動作としてネットワークにパケットが送信される．

パケット送信の直前にキー／ボタン操作が行われていない場合，ボットによる操作であると判断する．パケット監視モジュールは，ファイアウォールに対して通過許可を出さずに通信の遮断を継続する．また，ユーザが意図した通信なのかを確認するための警告や，不正な通信を行おうとしたアプリケーションのアンインストールを促す警告を出す．

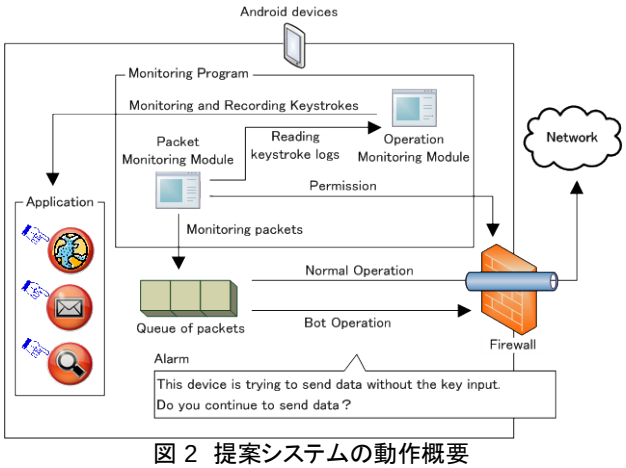


図 2　提案システムの動作概要

4.3　実装方法

監視プログラムの操作監視モジュールとパケット監視モジュールの 2 つをバックグラウンドで動作するように実装する．操作監視モジュールはキー／ボタン操作を時間情報と共にログファイルに出力する．パケット監視モジュールはパケットの送信を監視し，送信の際にはログファイルを確認し，ユーザの操作と判断した時に限り，ファイアウォールに対して通信の許可を出す．

5　むすび

Android 端末におけるボット対策として，Android 端末でユーザが行う特徴的な操作を考察した．メール送信やネットワークアクセス時の直前にボタン操作がない場合の通信の遮断により，ボットによる 2 次被害を防止する方法を提案した．今後は，ボタン操作の有無の検出方法を検討し，この方法の有効性を確認するための実装を行う．

参考文献

[1] 戸田，他，“Android 端末をターゲットとしたボットによる被害防止策の検討”，平成 23 年度電気関係学会東海支部連合大会論文集，F1-4，2011

[2] 平田，他，“ボットによる不正メールの送信を防止するための検討”，平成 20 年度電気関係学会東海支部連合大会論文集，講演番号 0-077，2008

[3] 間宮，他，“ボットネットによるスパムメール送信防止方法の検討”，平成 19 年度電気関係学会東海支部連合大会論文集，講演番号 0-373，2007

[4] 三根，他，“Windows API の監視による未知ウイルス検出手法の検討”，平成 19 年度電気関係学会東海支部連合大会論文集，講演番号 0-372，2007

Android端末をターゲットとした ボットによる被害防止策の提案

名城大学　理工学部　情報工学科
渡邊研究室
080425210　戸田　尚希

Watanabe Lab.

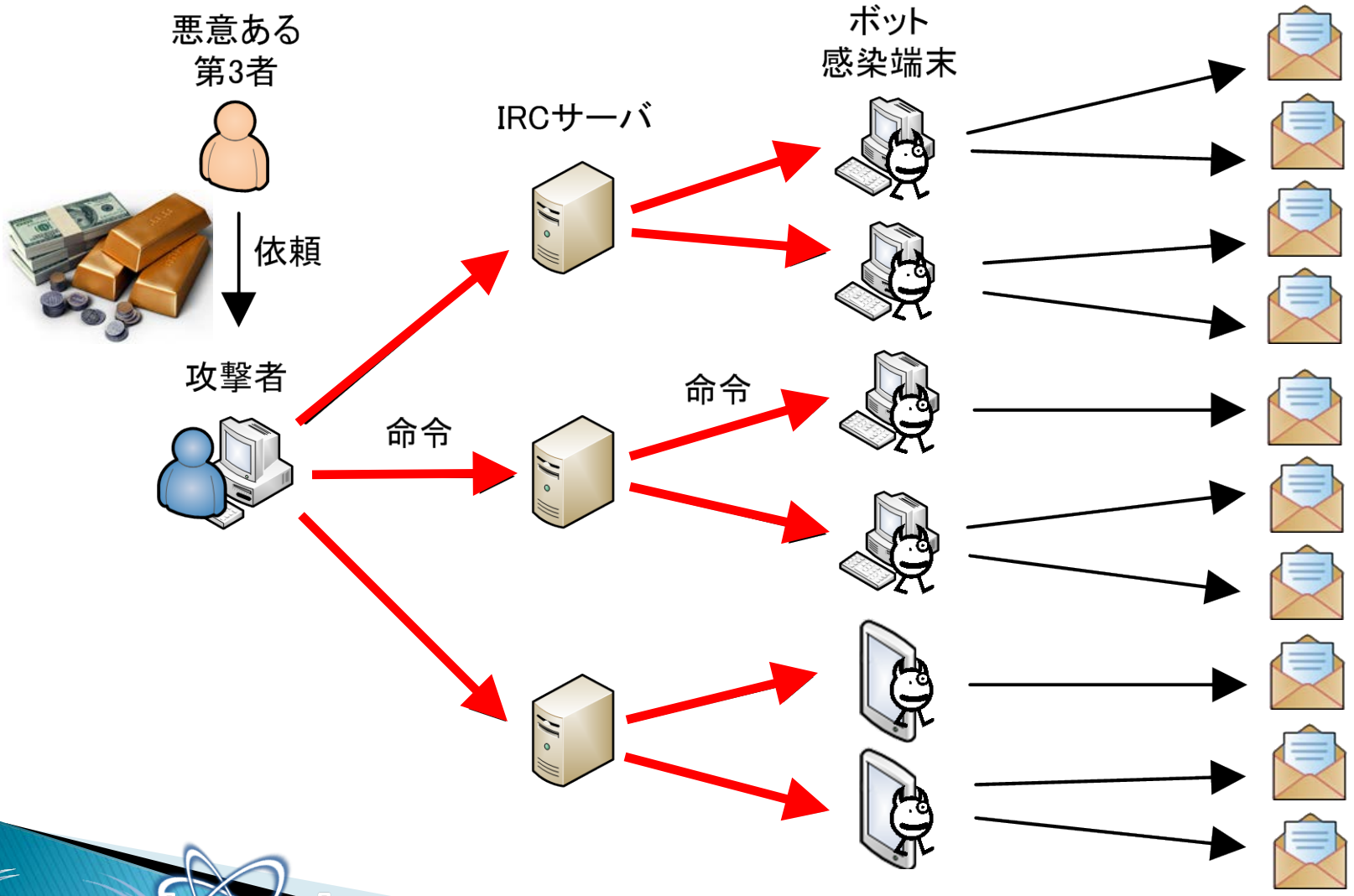
研究背景

- スマートフォンの普及
- Android OSの脆弱性をついたボットの出現
  - ボット・・・悪質化したウイルスの一種
- ユーザのセキュリティ対策不足

Android端末にボットが
急速に広まる恐れがある

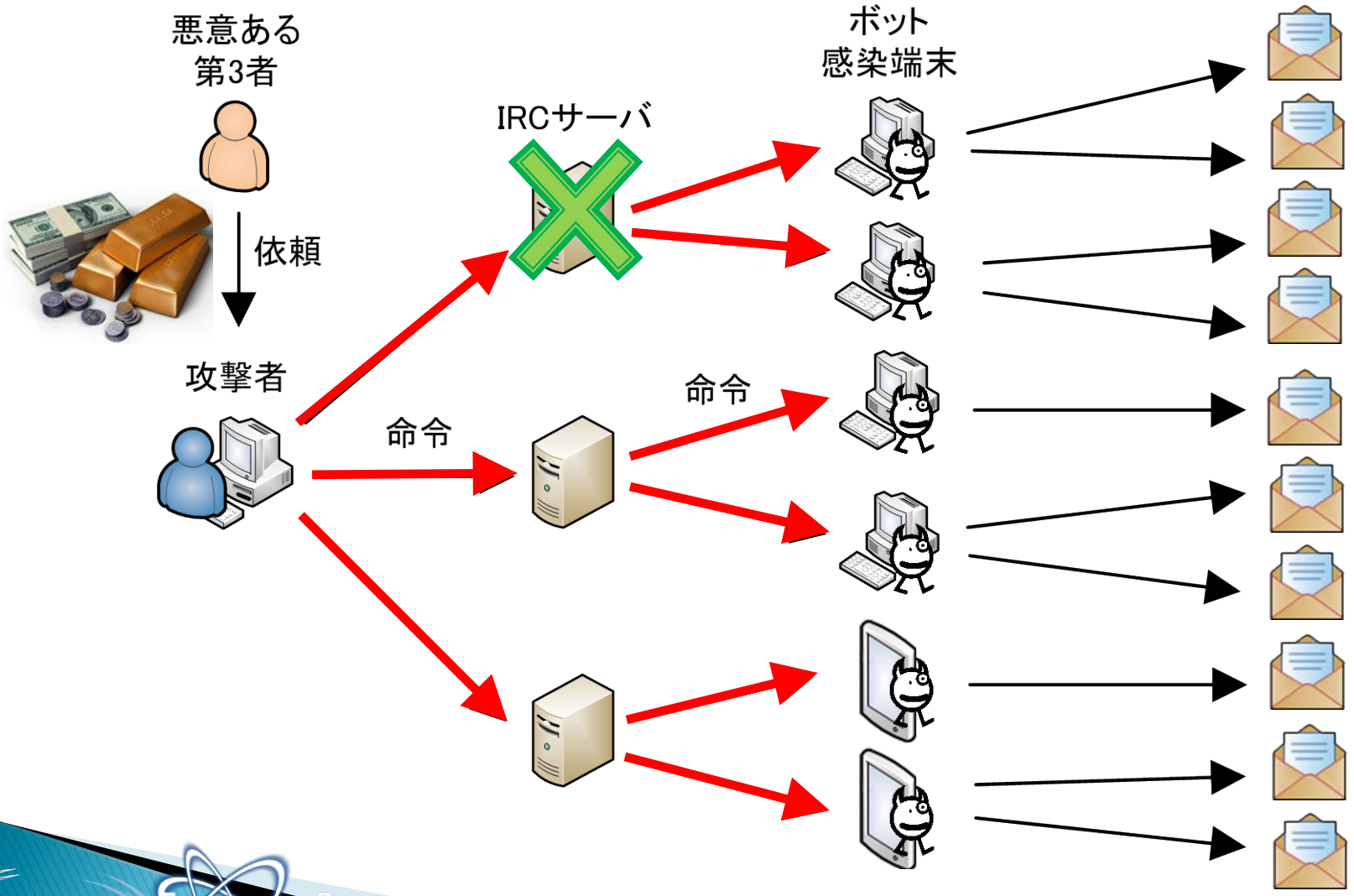
ボットとは

IRC：Internet Relay Chat



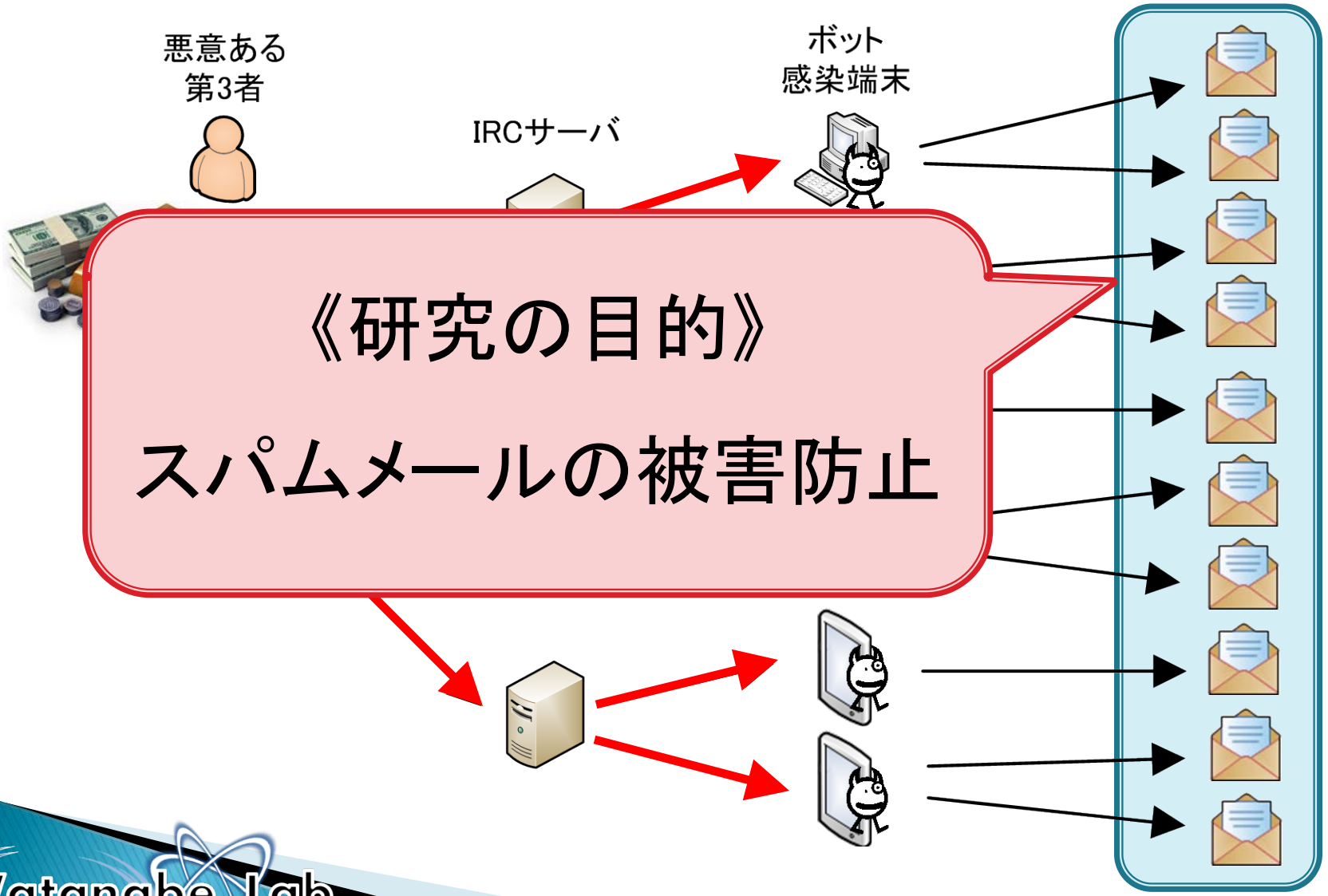
ボットとは

IRC：Internet Relay Chat



ボットとは

IRC：Internet Relay Chat



ボット対策の既存技術

- ウイルス対策アプリ
  - ウイルスバスター
  - ノートン
  - MacAfee

ウイルス定義ファイルを利用したパターン・マッチングが主流

新種や亜種のウイルスに対応出来ない

ユーザによる対策

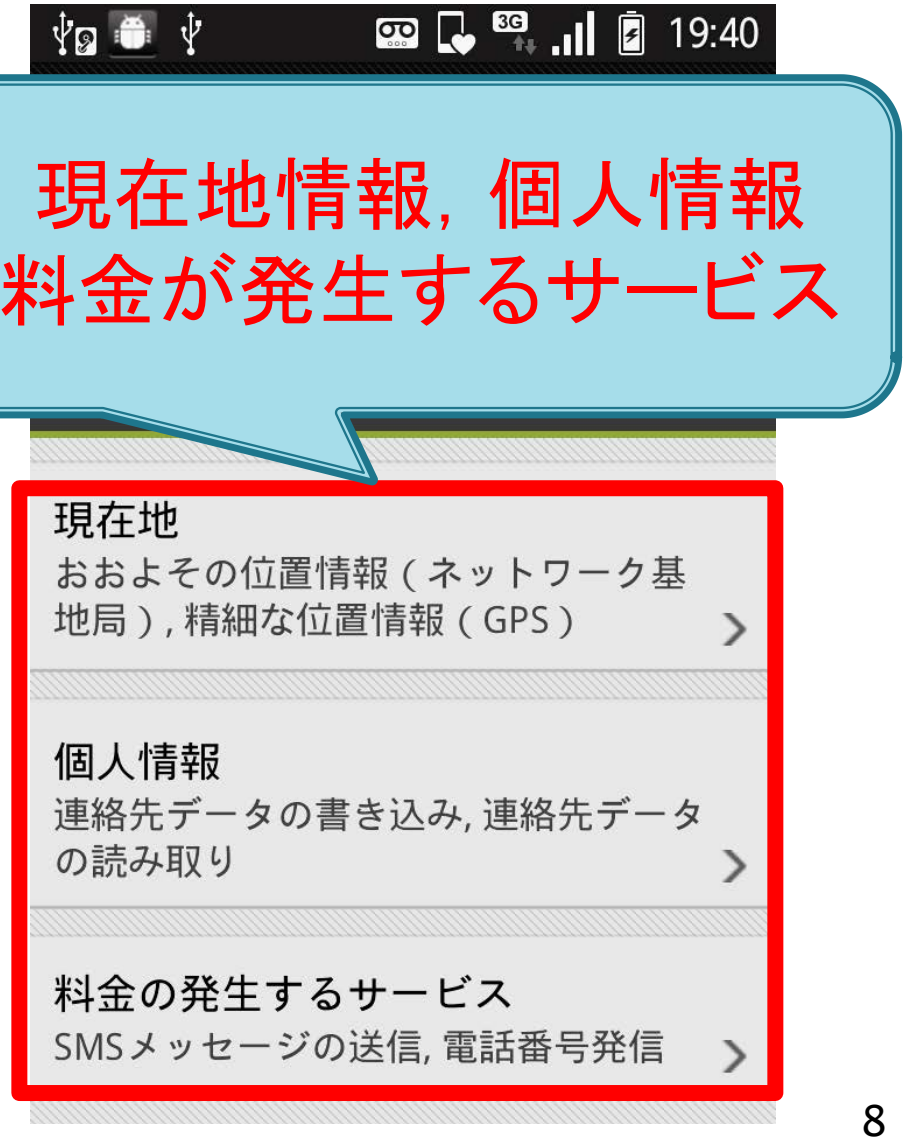
- アプリインストール時のアクセス許可を確認する
- 信頼できるダウンロードサイトからアプリケーションを入手する
  - （例）Android Market，au one Market
  - 公開アプリが海賊版である可能性が低い

システムとして被害を防ぐ訳ではない

アクセス許可の確認

- アプリのインストール時に表示される
- 表示されるアクセス許可により，不正アプリかどうかを判断する

非常に困難



提案方式

ボットの感染を防ぐのは難しい事を
前提とした**2次被害の防止策**を提案

- ユーザが行う特徴的な操作
  - ユーザによる操作かボットによる操作かを見分ける
- 監視プログラムによる通信制御
  - ボットによる操作と判断した場合のアラームの提示とパケットの破棄

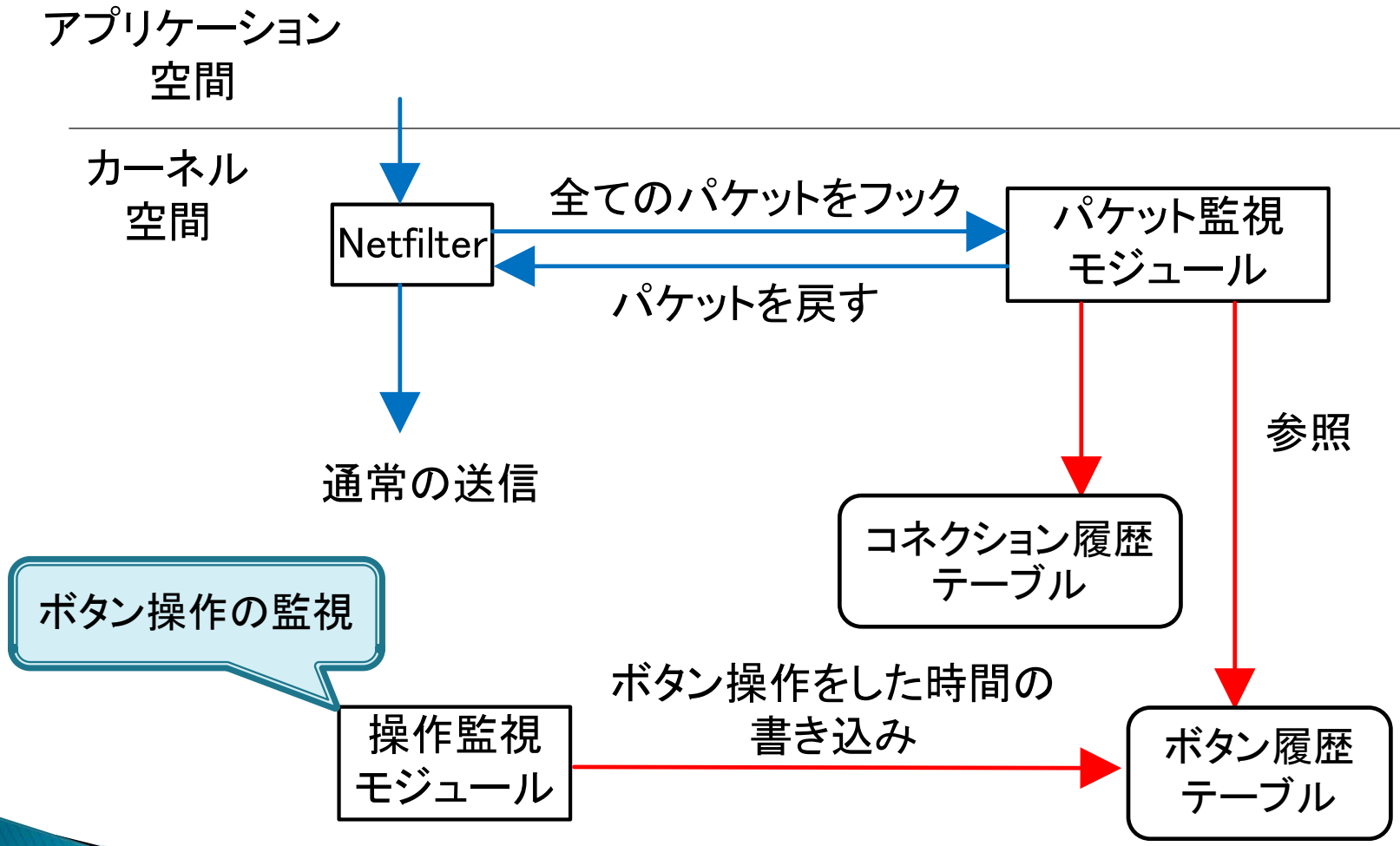
ユーザが行う特徴的な操作

- メール送信時の送信ボタンを押す操作

ボットには出来ない操作

- カーネルレベルでのボタン操作検出

提案方式の概要


アプリケーション
空間
カーネル
空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視
モジュール
通常の送信
参照
コネクション履歴
テーブル
ボタン操作の監視
操作監視
モジュール
ボタン操作をした時間の
書き込み
ボタン履歴
テーブル

ユーザ操作の場合

アプリケーション空間

カーネル空間

Netfilter

全てのパケットをフック

パケットを戻す

パケット監視モジュール

通常の送信

ボタン履歴テーブル

現在時刻の直前でない

コネクシ
テー

ボタン操作の監視

操作監視モジュール

ボタン操作をした時間の書き込み

ボタン履歴テーブル

ユーザ操作の場合

アプリケーション空間

カーネル空間

Netfilter

全てのパケットをフック

パケットを戻す

パケット監視モジュール

通常の送信

ボタン履歴テーブル

2012/03/08 12:09:16

コネクシ
テー

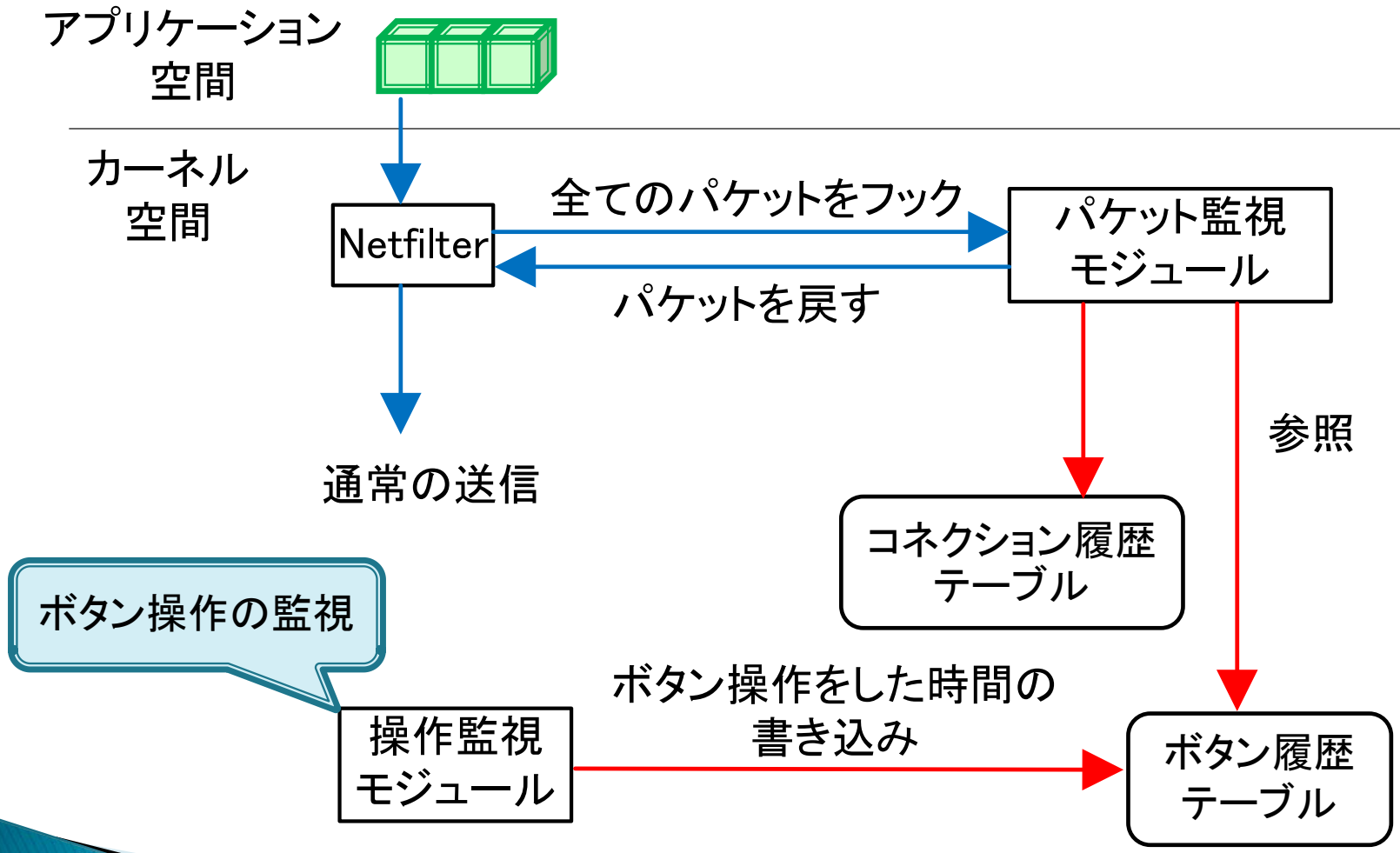
ボタン操作の監視

操作監視モジュール

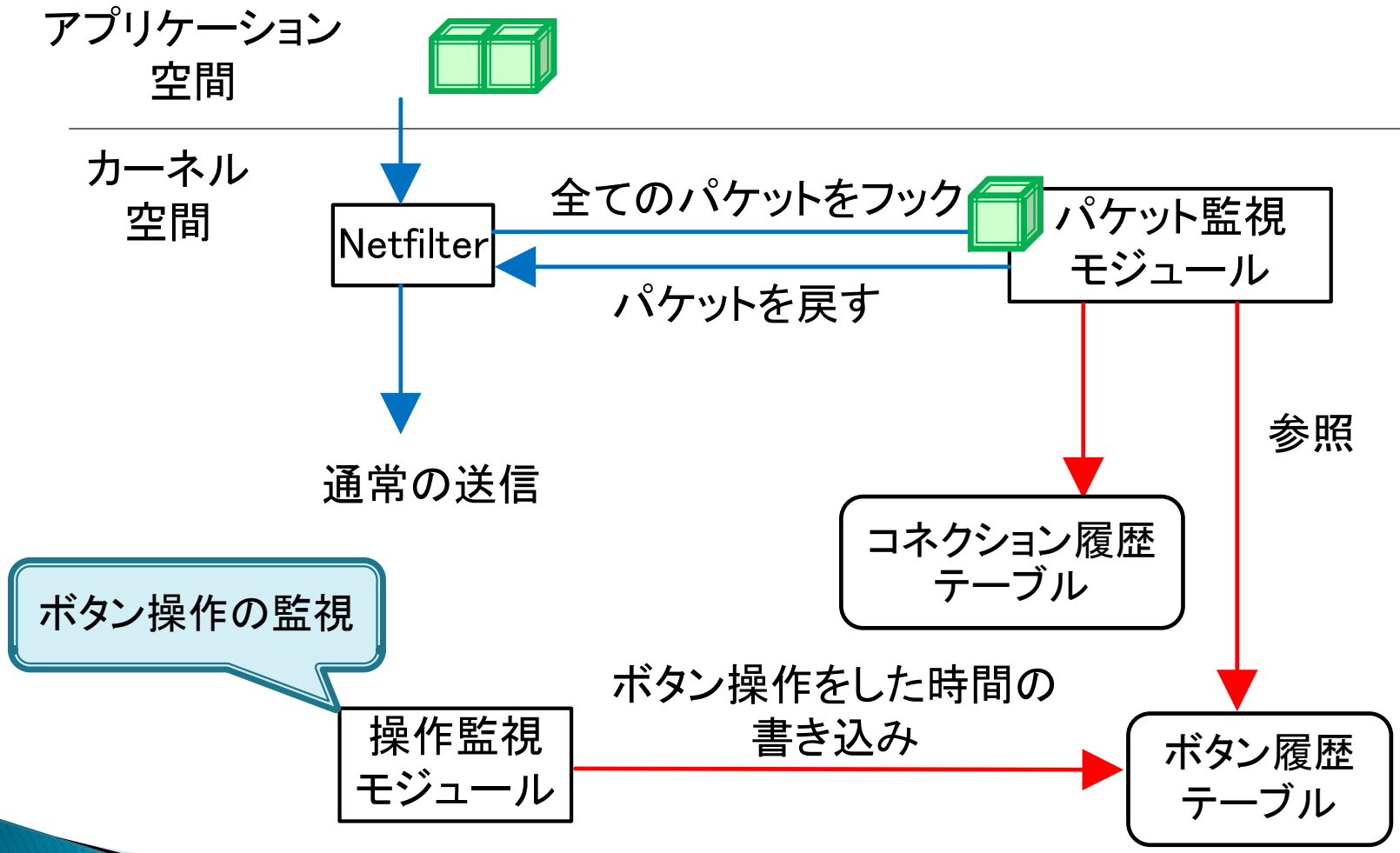
ボタン操作をした時間の書き込み

ボタン履歴テーブル

ユーザ操作の場合

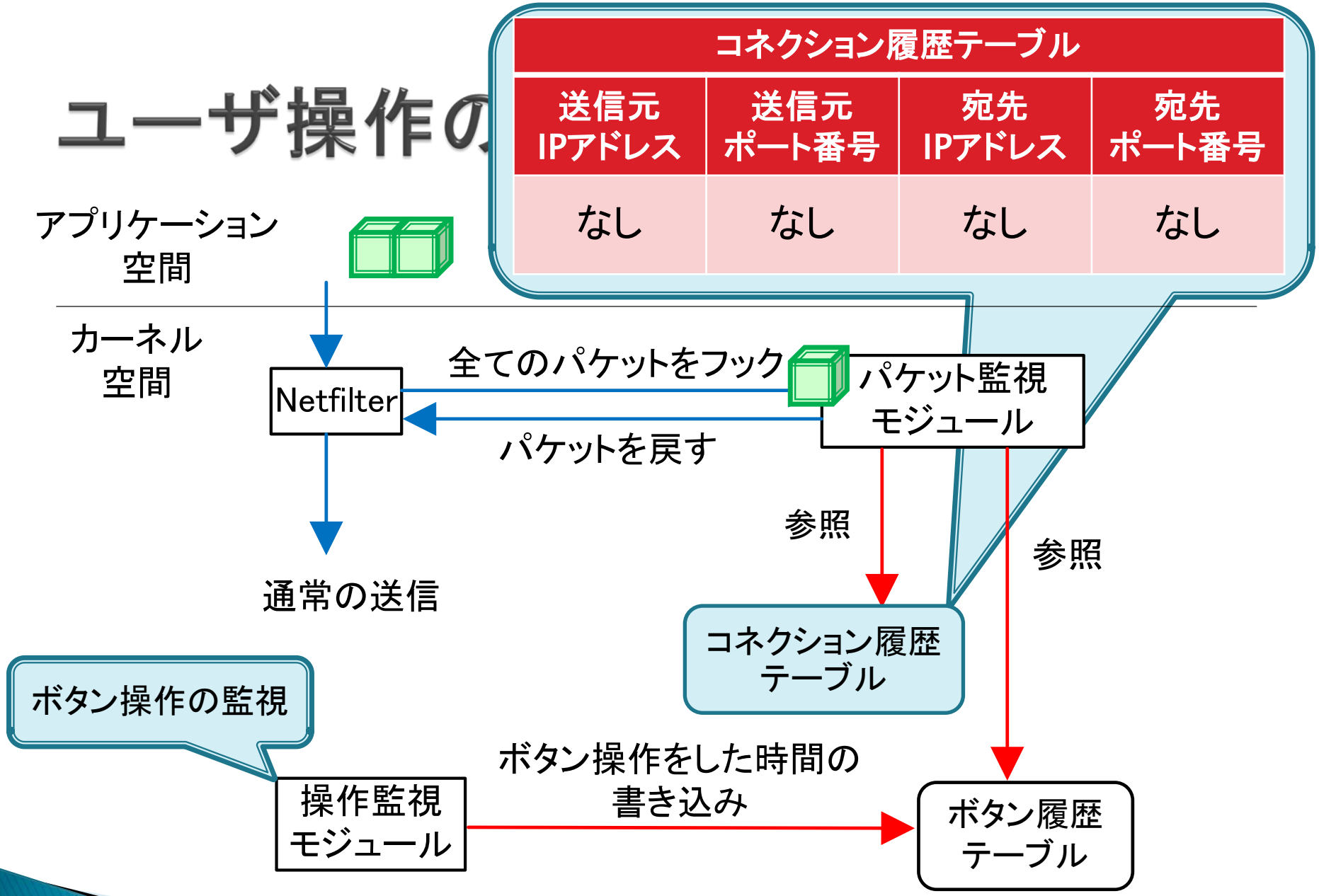

アプリケーション
空間
カーネル
空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視
モジュール
通常の送信
参照
コネクション履歴
テーブル
ボタン操作の監視
操作監視
モジュール
ボタン操作をした時間の
書き込み
ボタン履歴
テーブル

ユーザ操作の場合

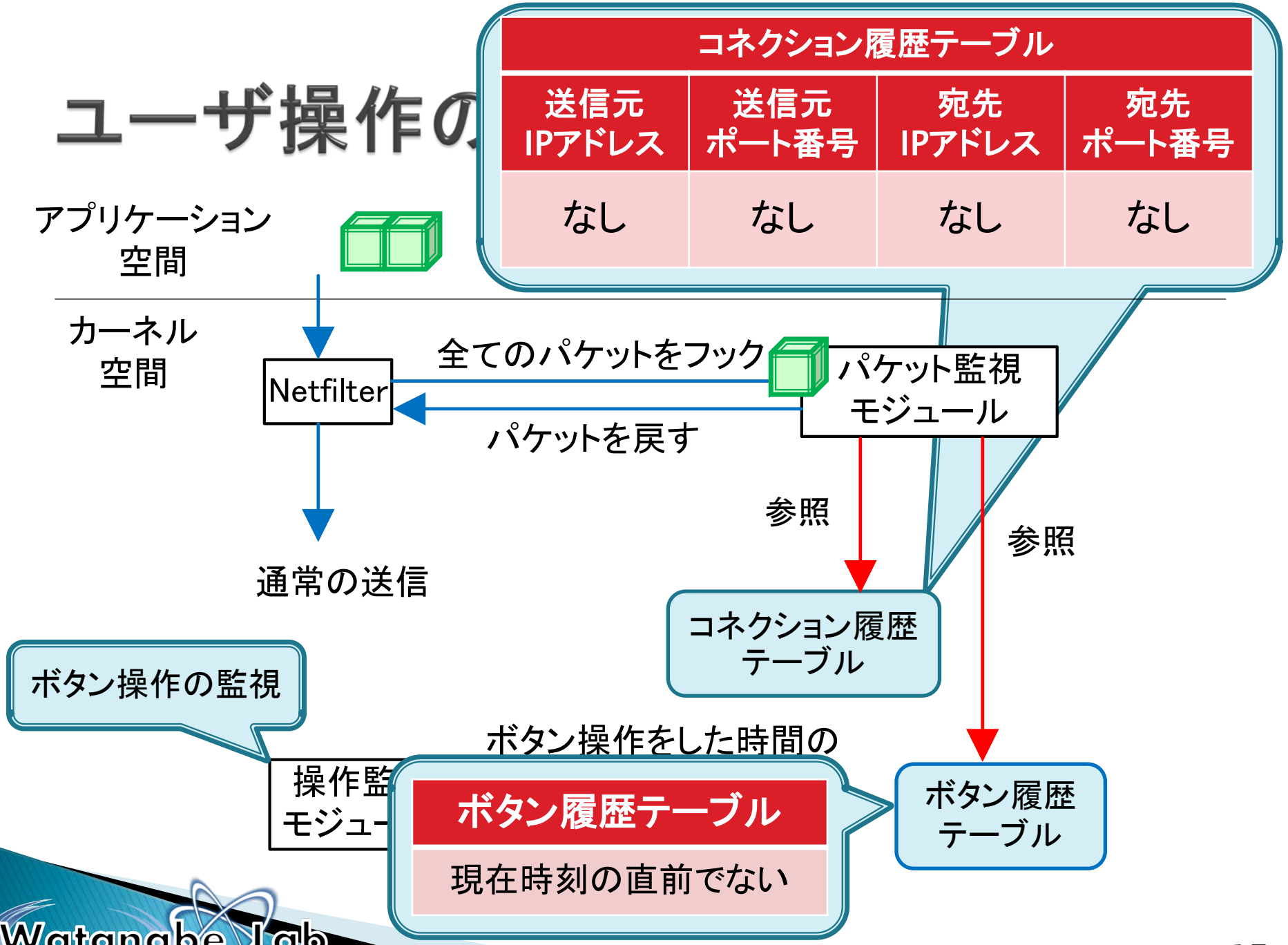

アプリケーション
空間
カーネル
空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視
モジュール
通常の送信
参照
コネクション履歴
テーブル
ボタン操作の監視
操作監視
モジュール
ボタン操作をした時間の
書き込み
ボタン履歴
テーブル

ユーザ操作の

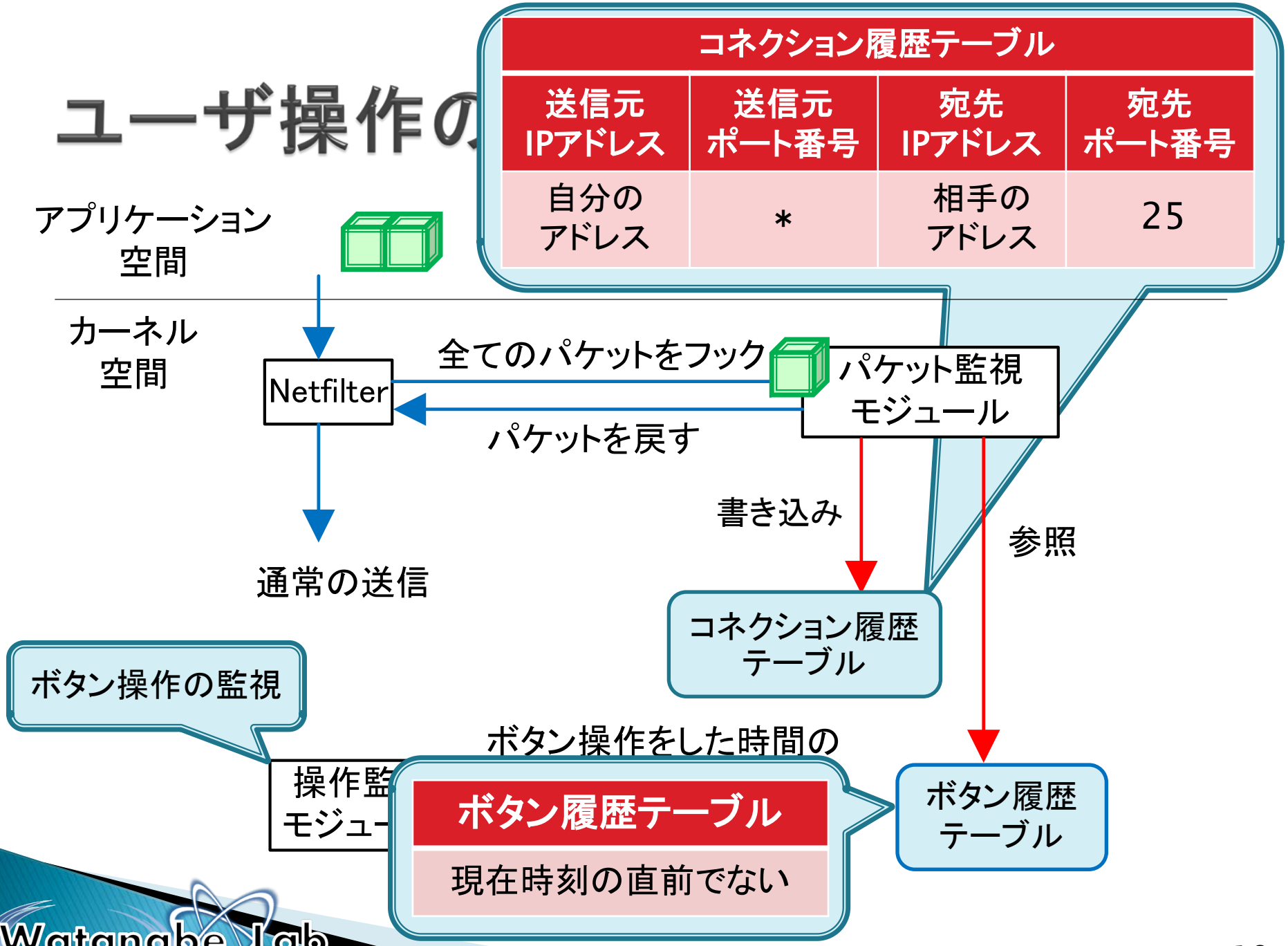
コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
なし	なし	なし	なし



ユーザ操作の

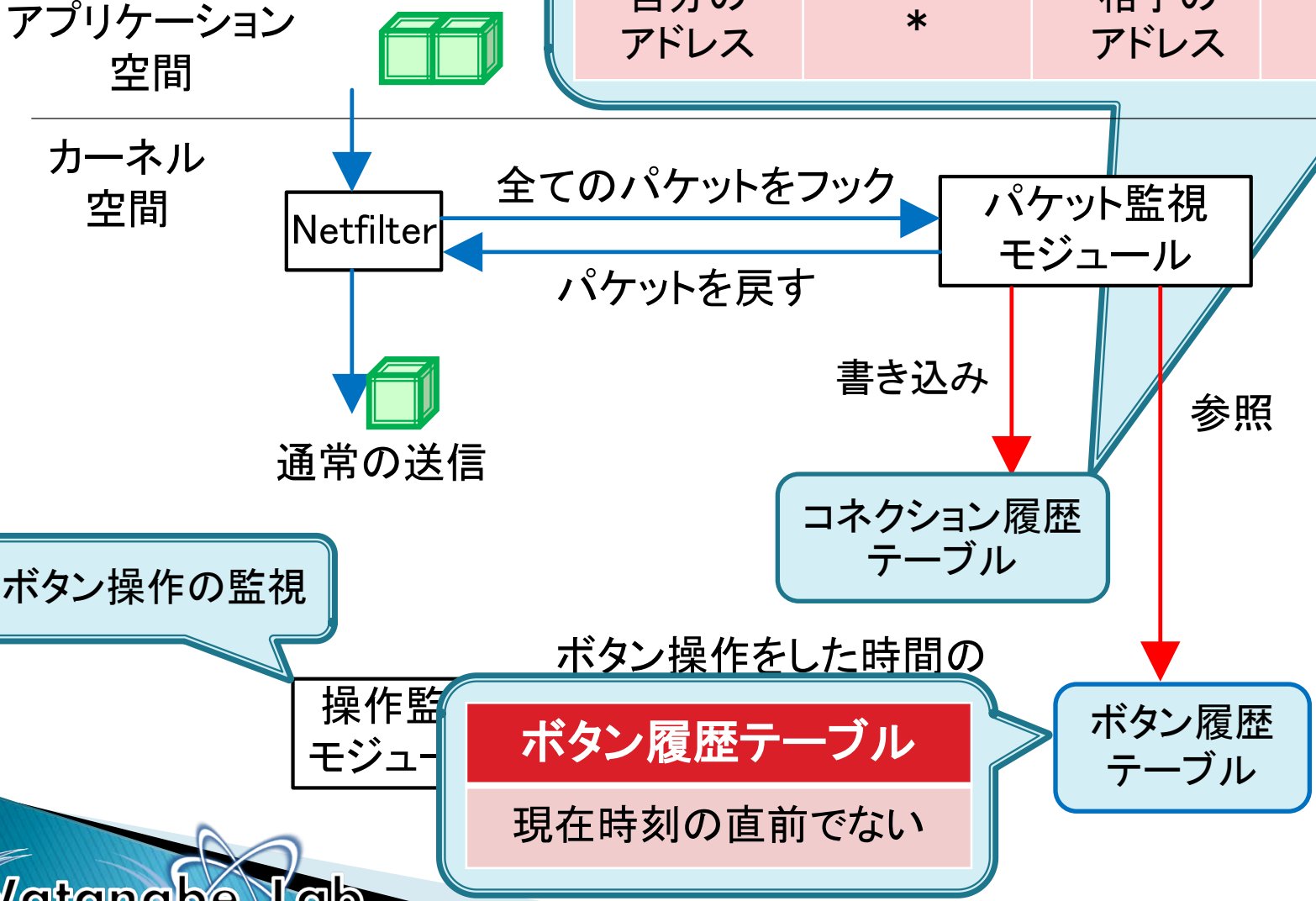

コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
参照
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル

ユーザ操作の


コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
自分の アドレス
*
相手の アドレス
25
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
書き込み
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル

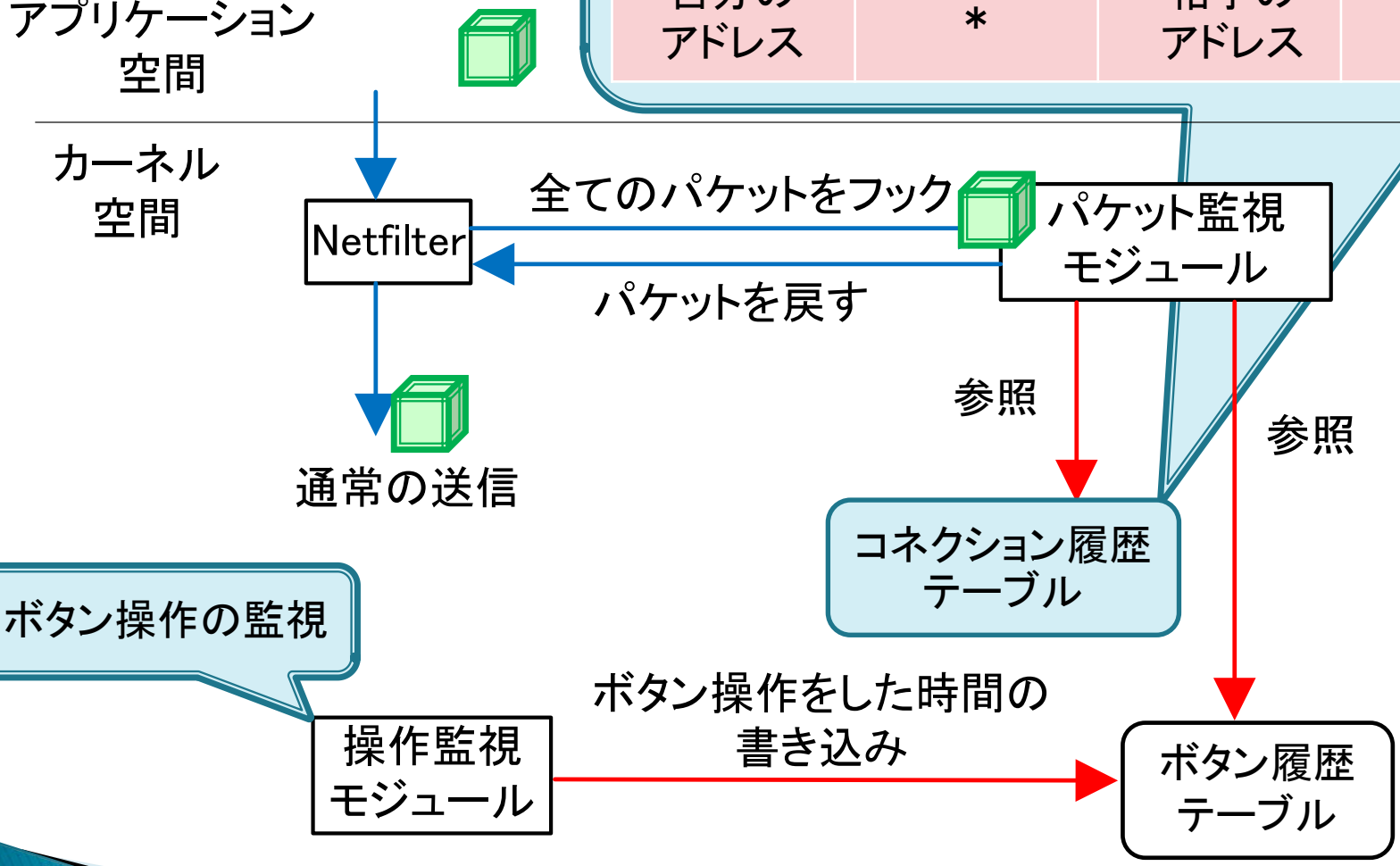
ユーザ操作の

コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
自分の アドレス	*	相手の アドレス	25



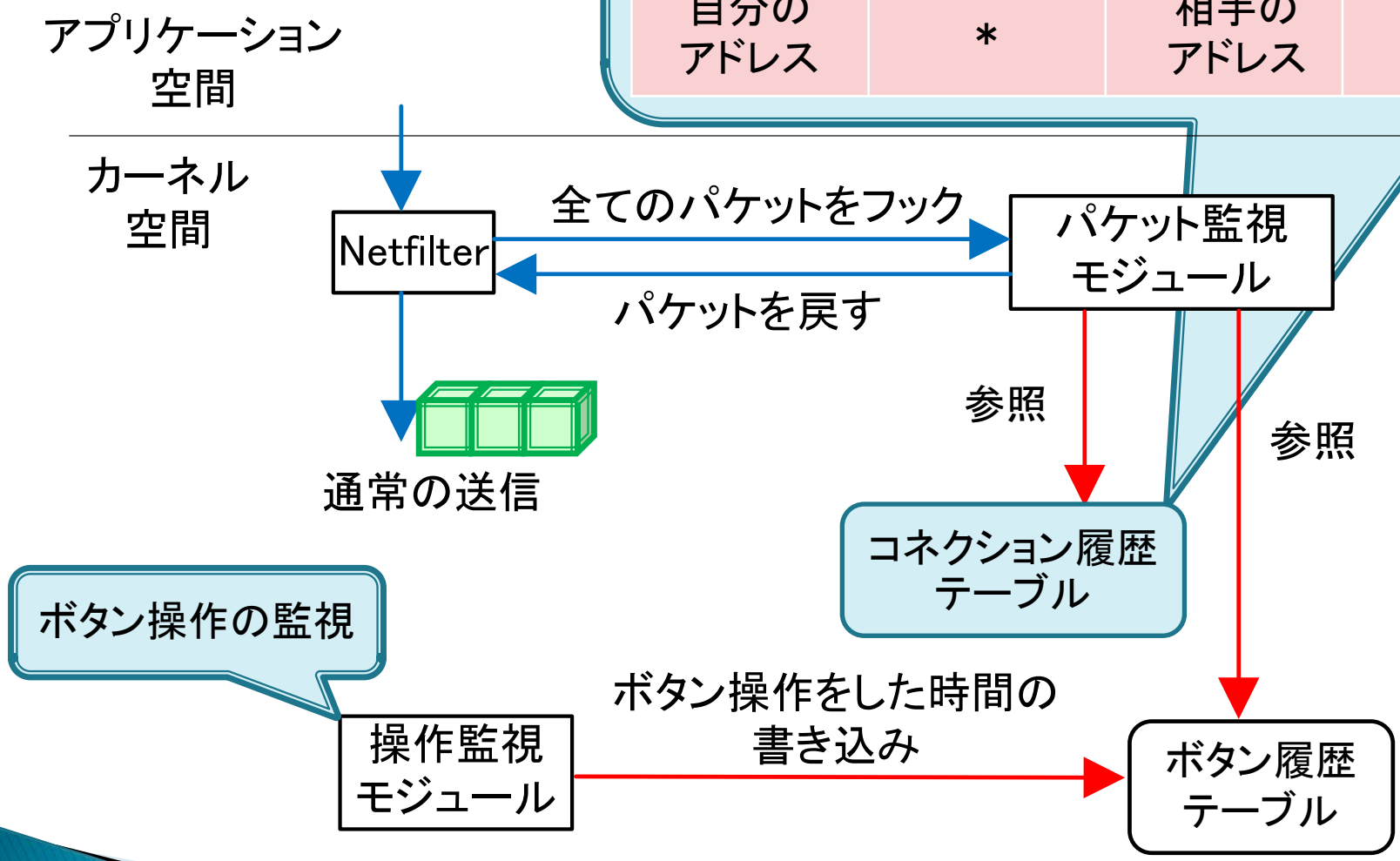
ユーザ操作の

コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
自分の アドレス	*	相手の アドレス	25



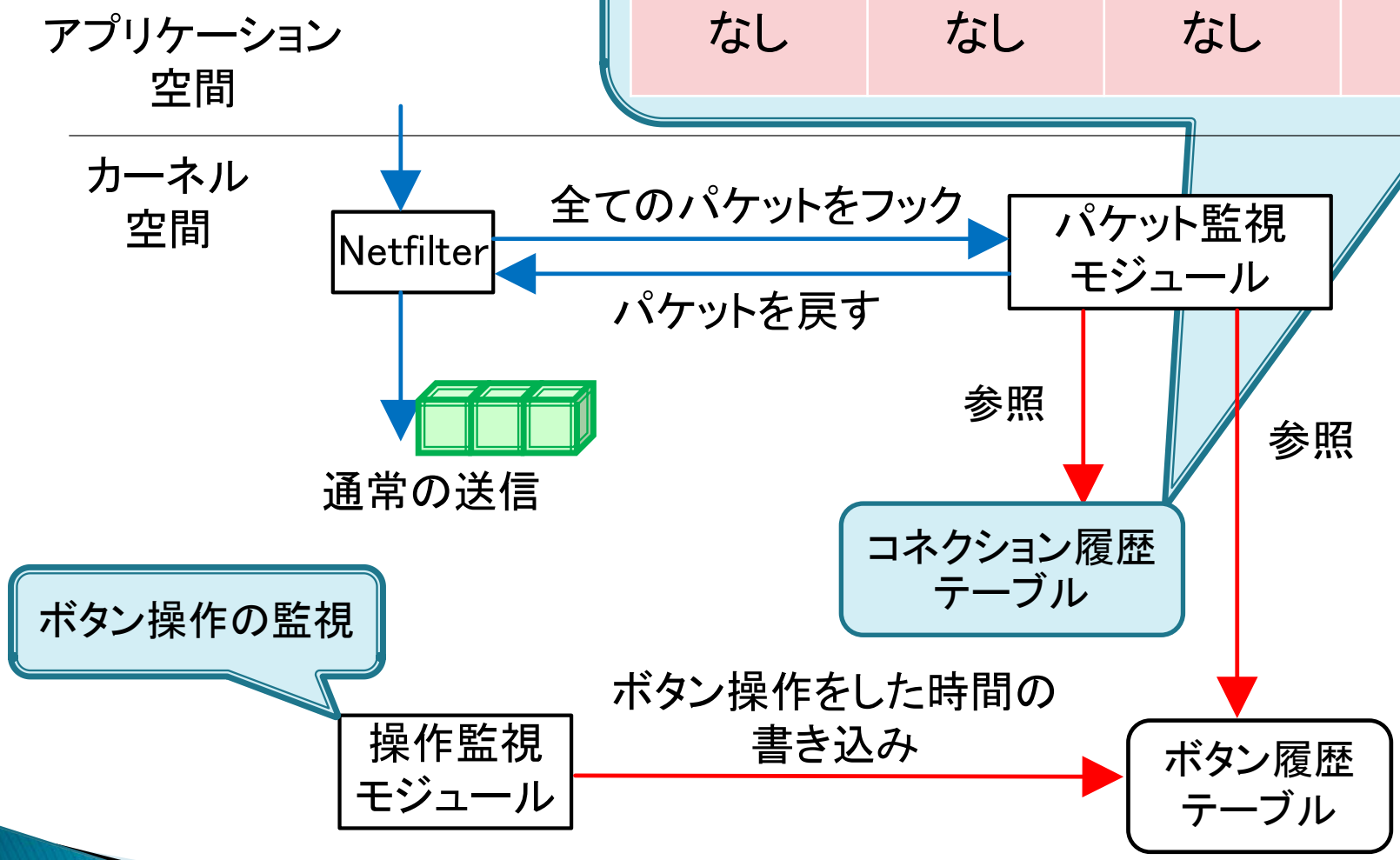
ユーザ操作の

コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
自分の アドレス	*	相手の アドレス	25

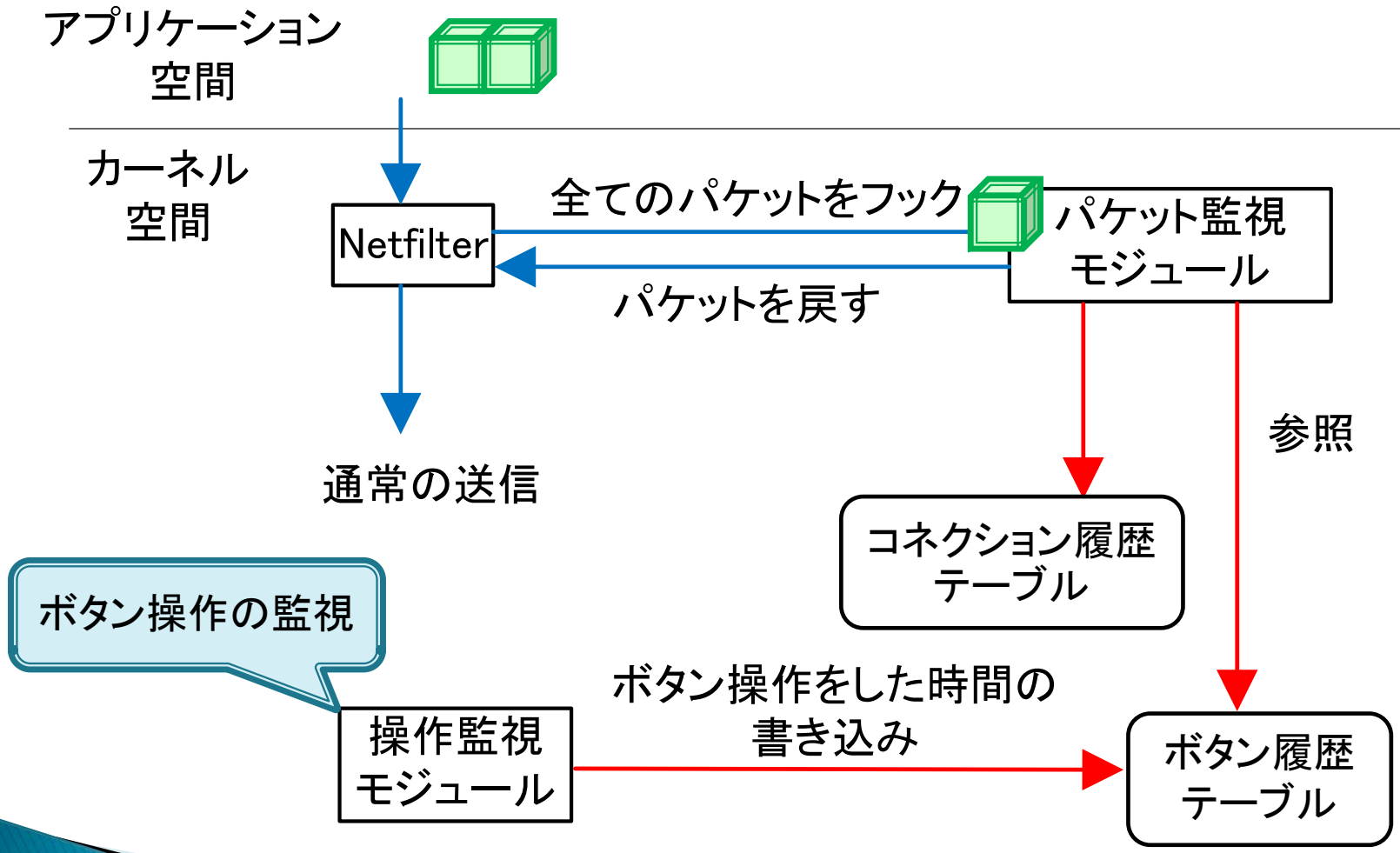


ユーザ操作の

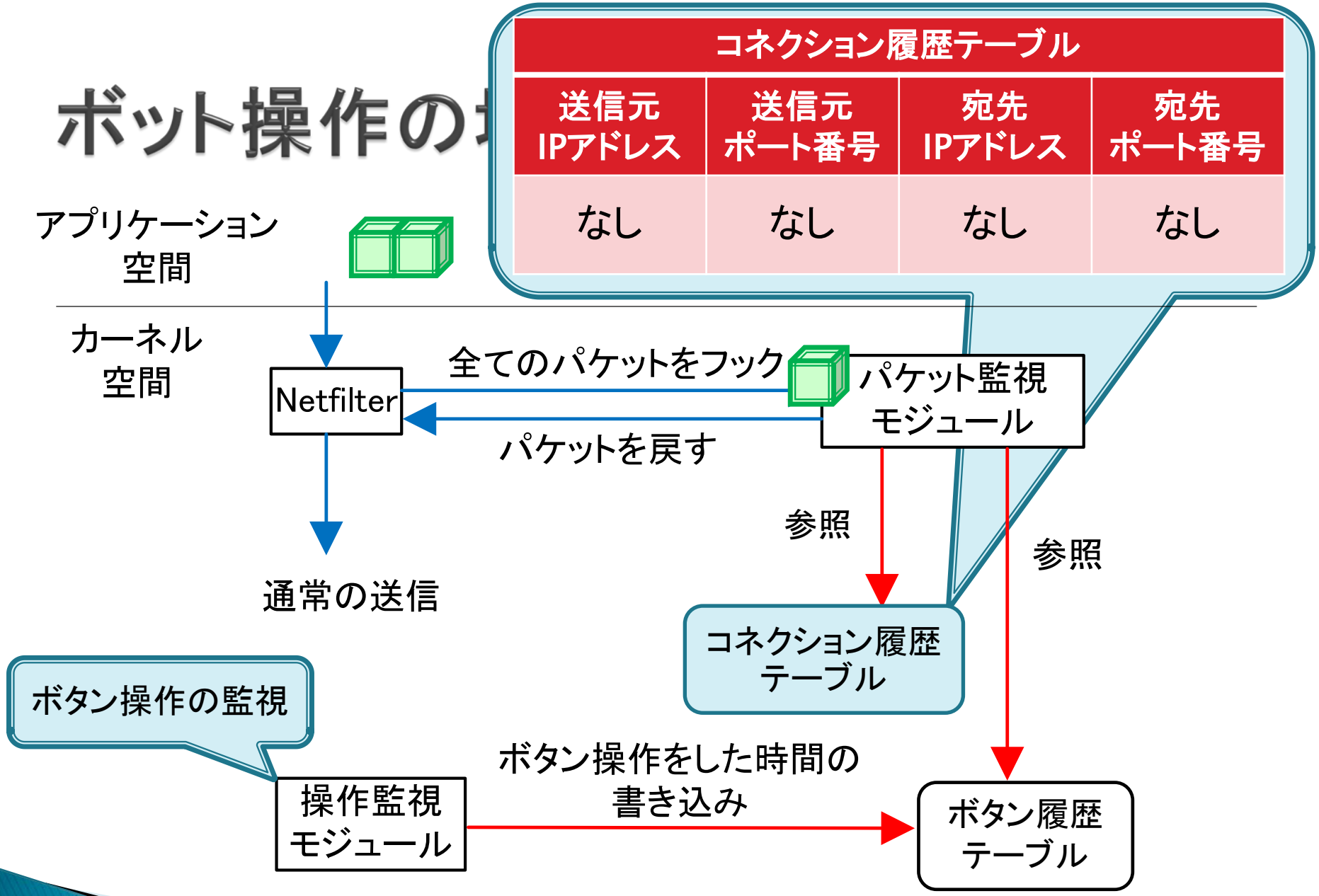
コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
なし	なし	なし	なし



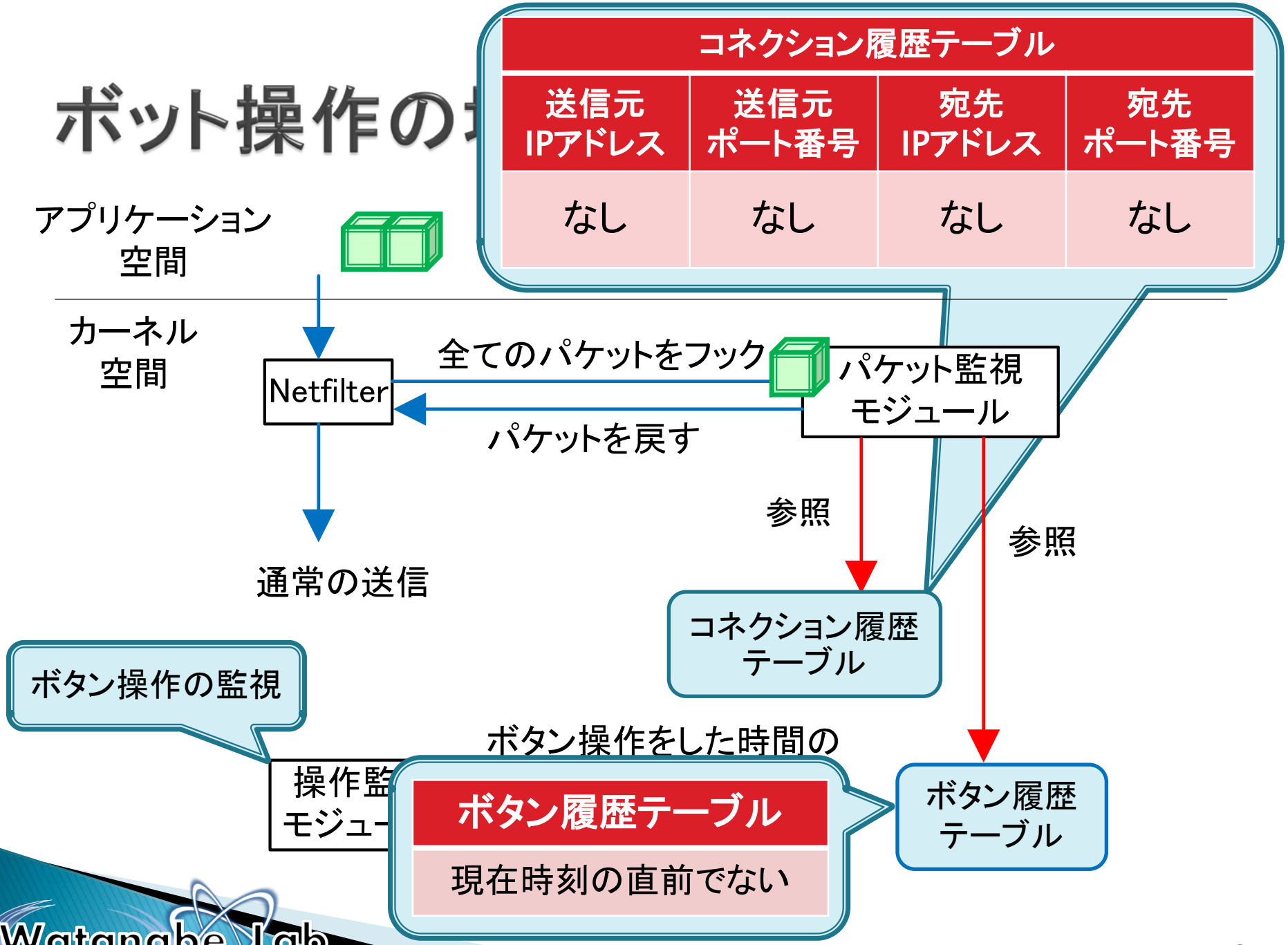
ボット操作の場合


アプリケーション
空間
カーネル
空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視
モジュール
通常の送信
参照
コネクション履歴
テーブル
ボタン操作の監視
操作監視
モジュール
ボタン操作をした時間の
書き込み
ボタン履歴
テーブル

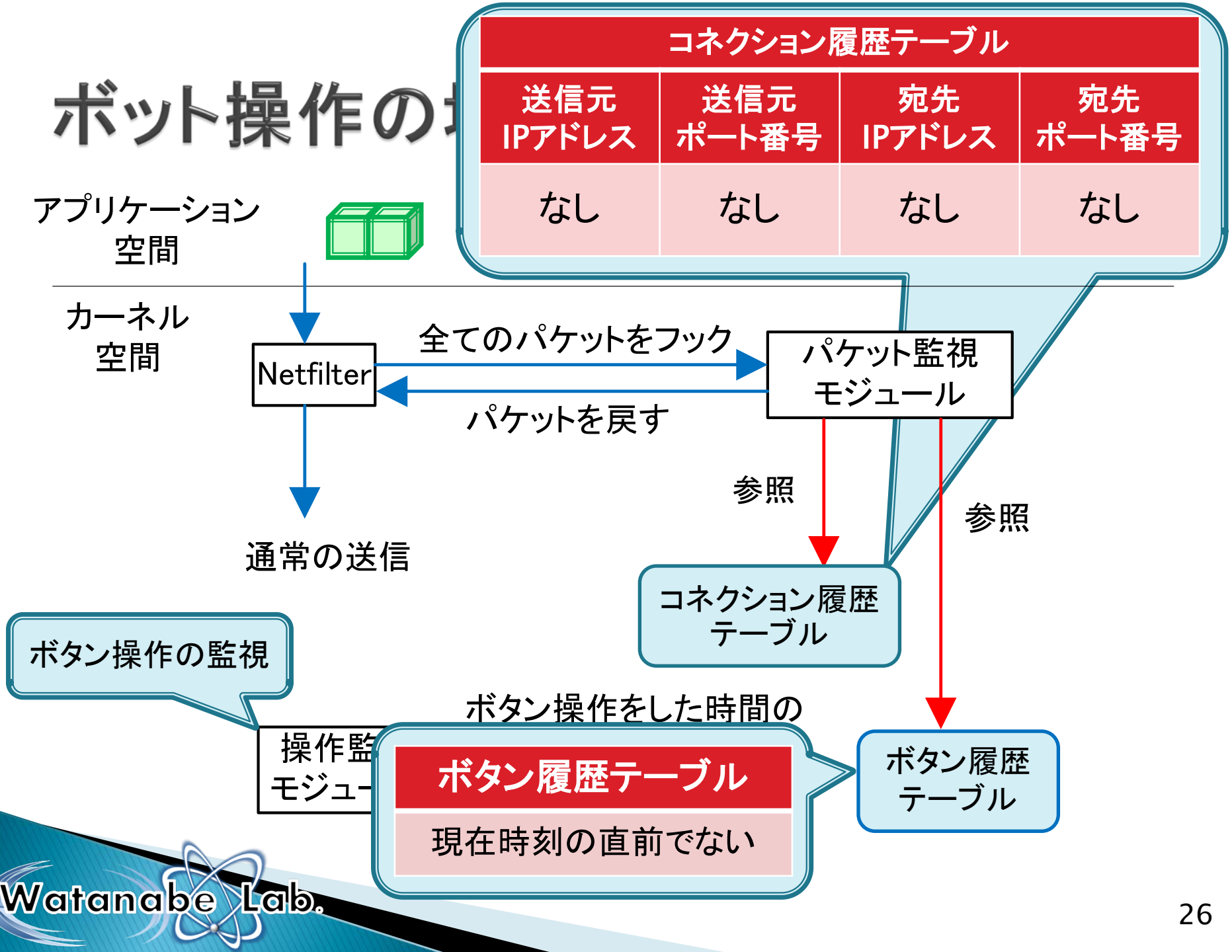
ボット操作の


コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
参照
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
操作監視 モジュール
ボタン操作をした時間の 書き込み
ボタン履歴 テーブル

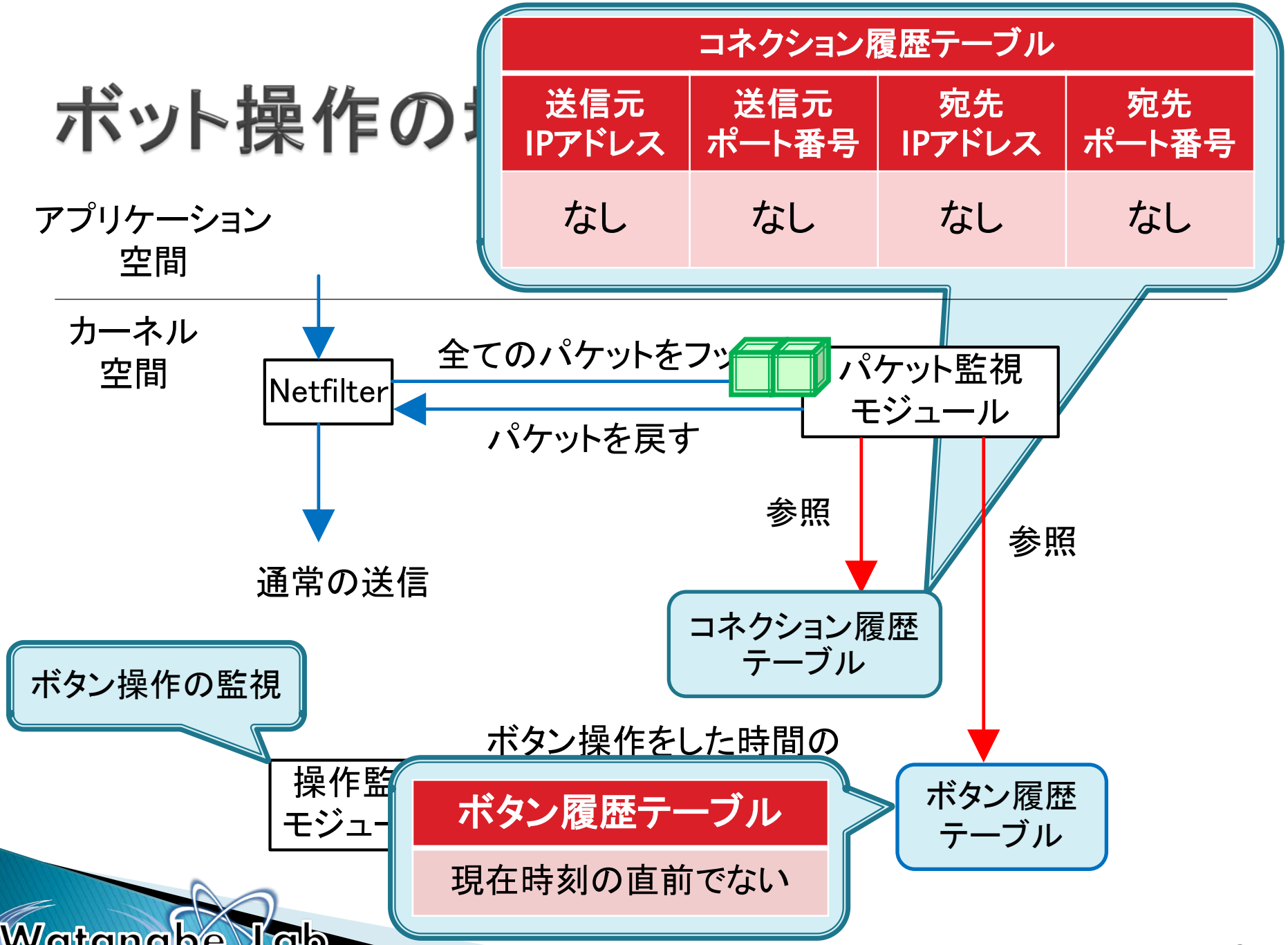
ボット操作の


コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
参照
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル

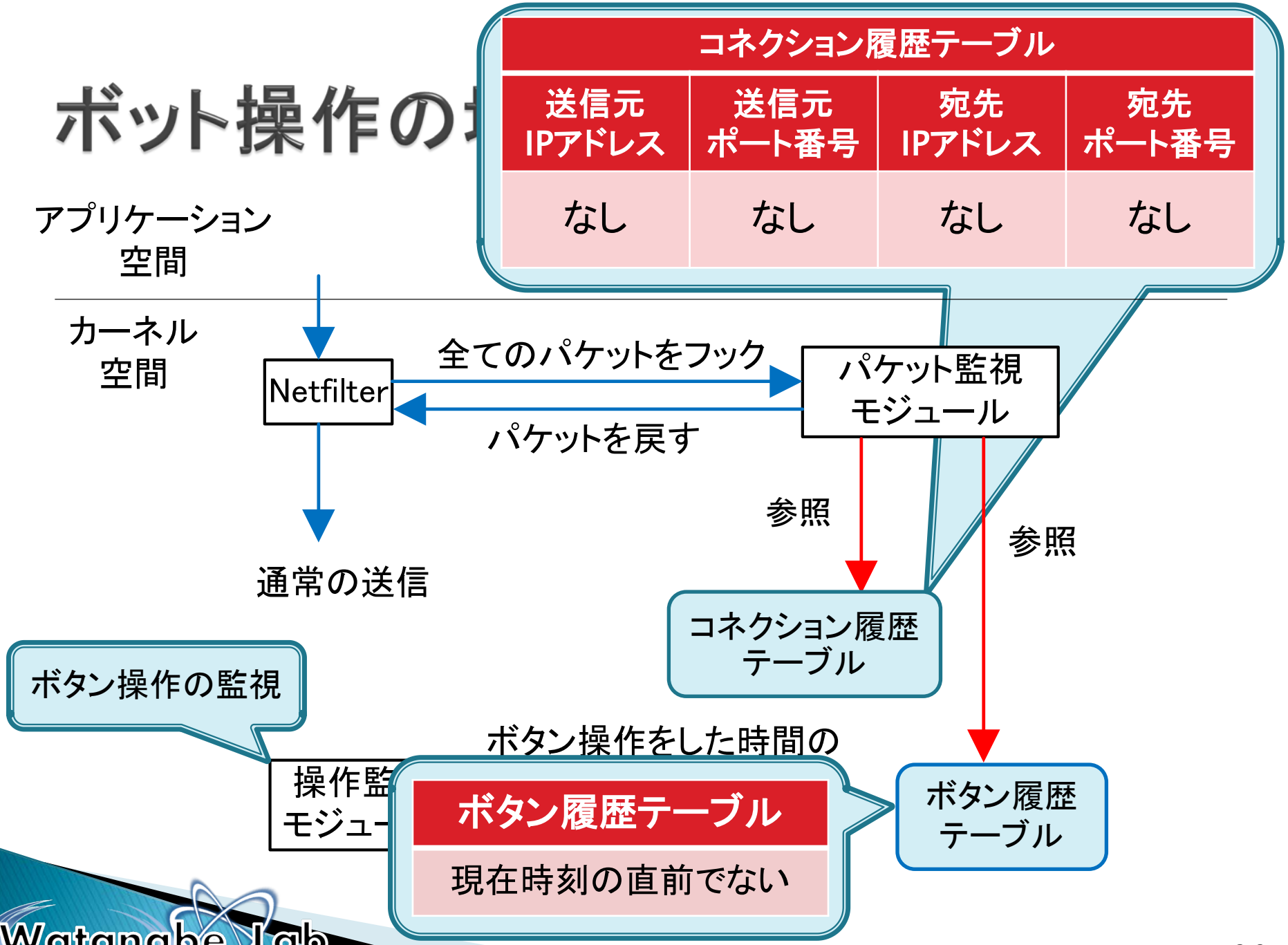
ボット操作の


コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
参照
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル

ボット操作の

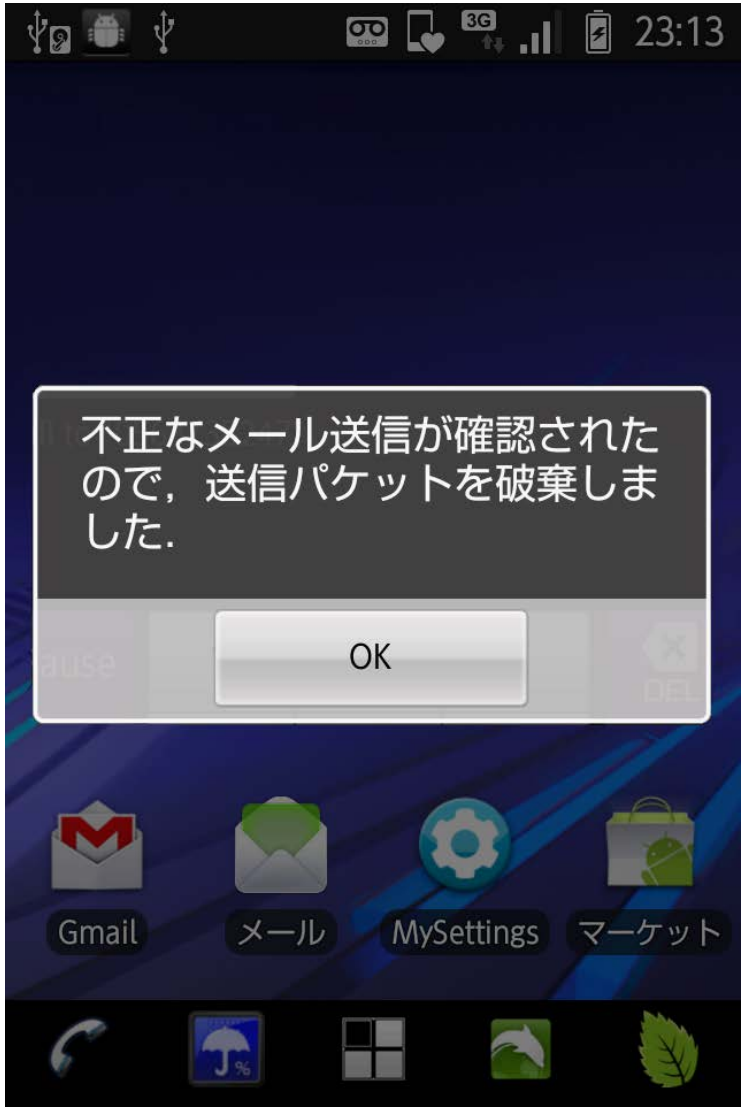

コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフッ
パケットを戻す
パケット監視 モジュール
参照
参照
通常の送信
コネクション履歴 テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル

ボット操作の


コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション空間
カーネル空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視モジュール
参照
参照
通常の送信
コネクション履歴テーブル
ボタン操作の監視
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴テーブル

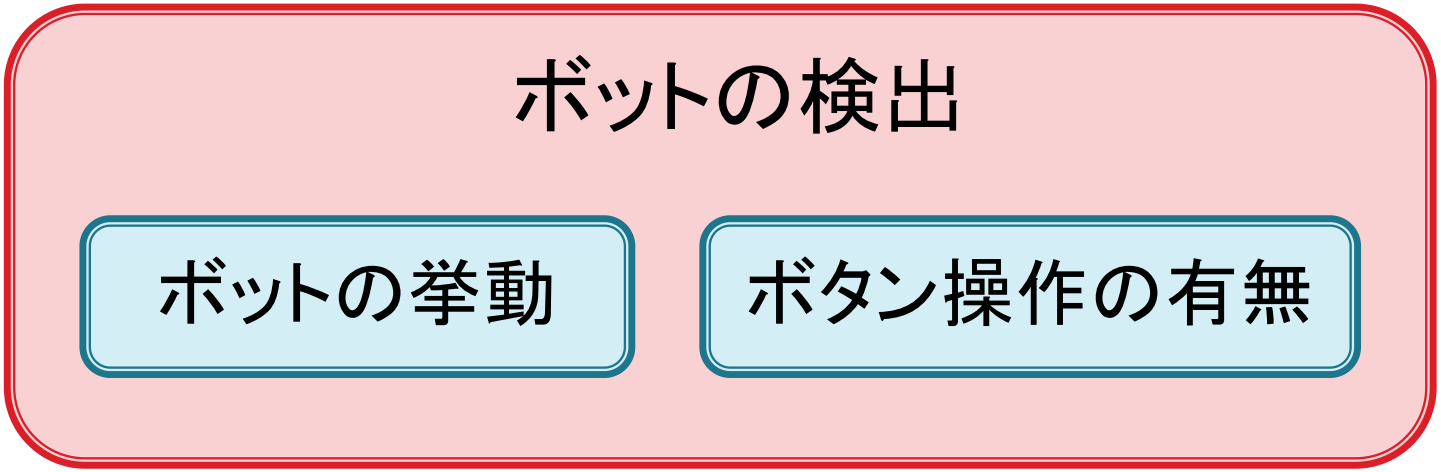
ボット操作の場合

- 右図のようなアラームをユーザに提示
- 内容
  - 意図しないメールが送信されたが，パケットを破棄したこと



提案方式の利点

- スパムメール送信の防止に有効
- 新種・亜種のボット対策に有効
  - ウイルス検出がパターン・マッチングと異なる



まとめ

- ボットによる2次被害の防止策の提案
  - Android端末でのボタン操作の有無により，ボットによる操作を検知し，パケットの破棄を行う
- 今後の課題
  - 提案方式の実装と評価
  - DDoS攻撃への加担防止法の検討

付　録

DDoS攻撃
(Distributed Denial of Service Attack)