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

080425210　戸田 尚希
渡邊研究室

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．スマートフォン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ことは難しい．そこでボットの感染は避けられないことを想定し，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ことにより，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，ボットの活動で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．

ボット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受け取ることが出来る．このため，ボット対策をサーバに対して施すことは，難しいとされている．

3. 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ことにより，正常な送信とボットによる送信を区別できる．

4. 提案方式

図 1 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．

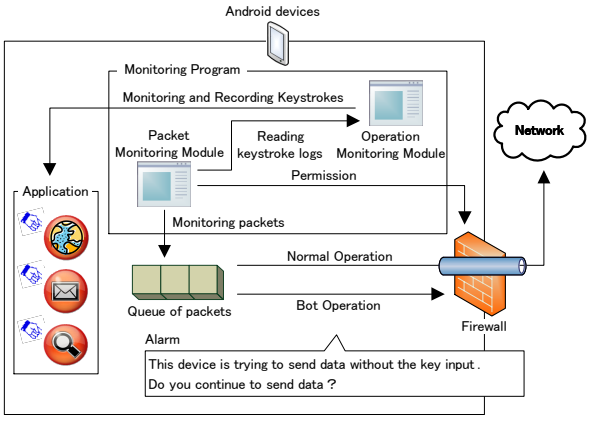


図 1: 提案方式の動作概要

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は通信の遮断を継続することにより，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 O-077，2008

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.

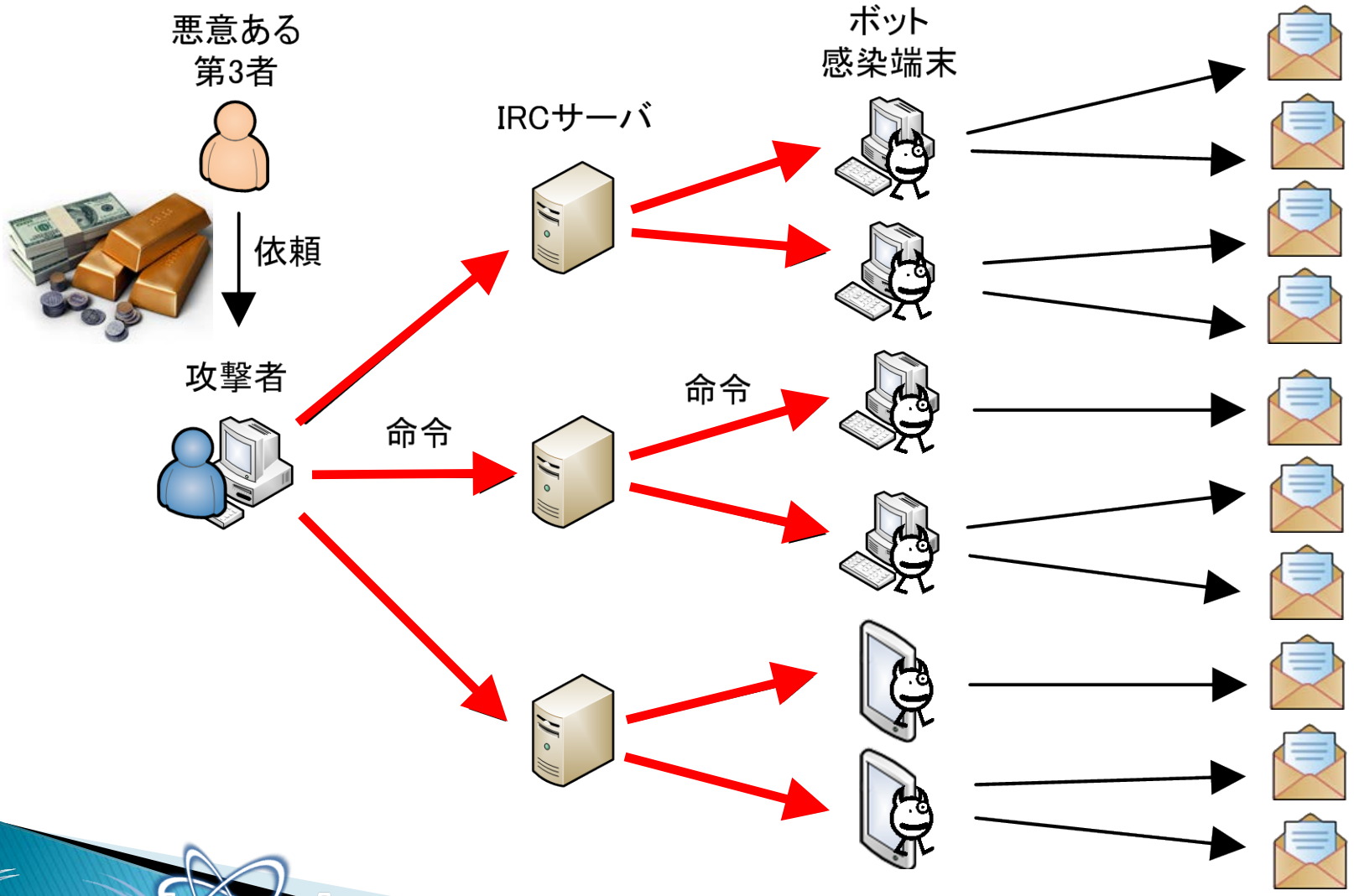
研究背景

- 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

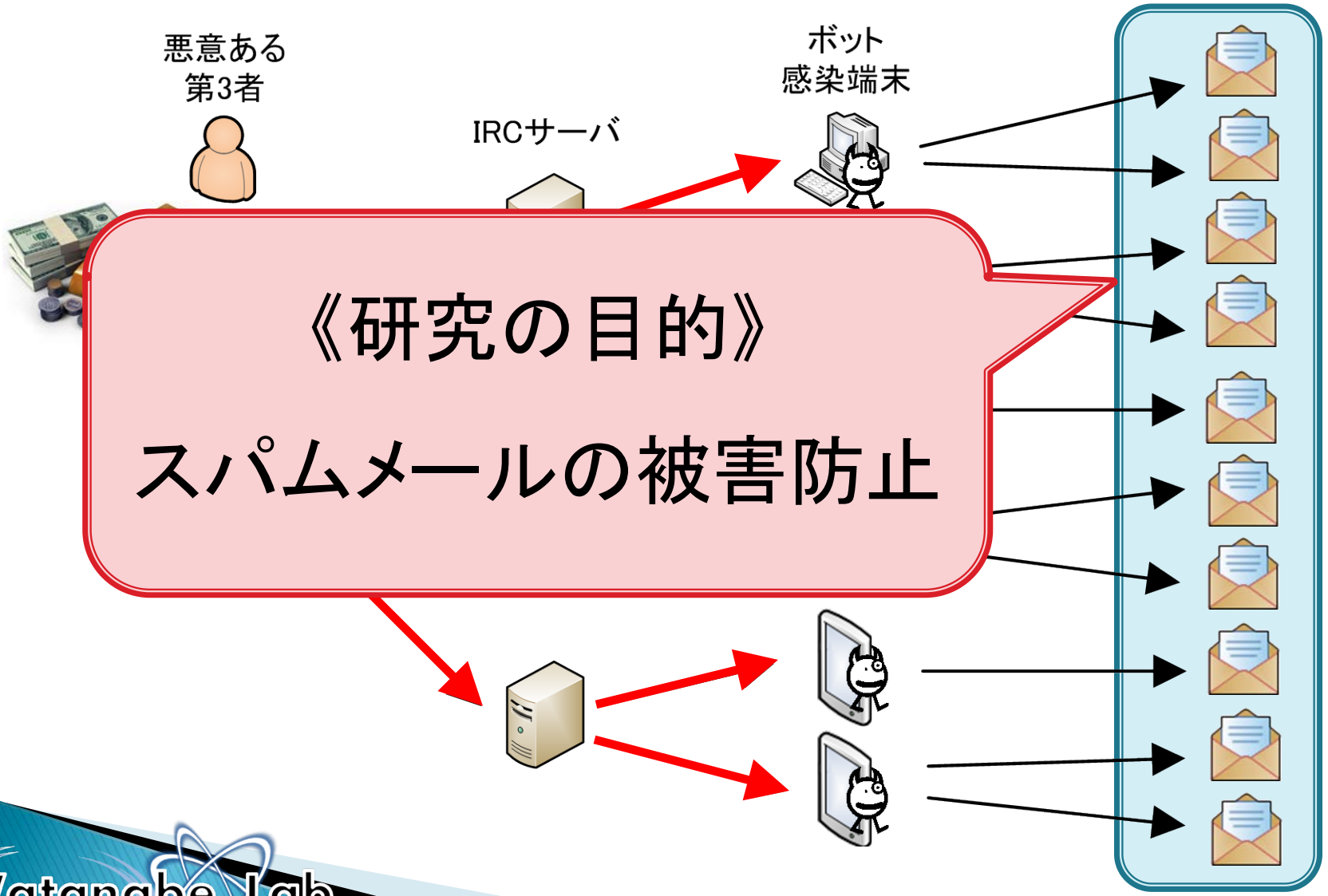
ボットとは

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

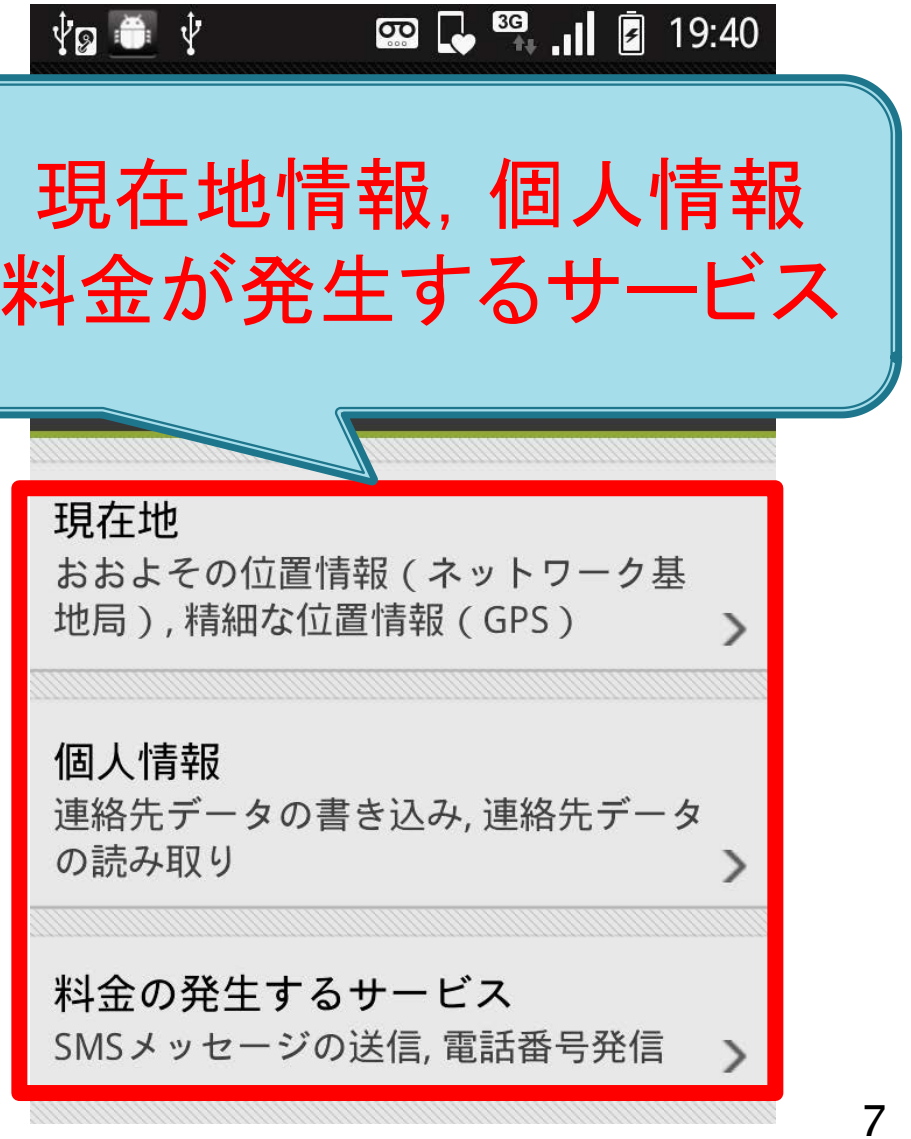
- アプリインストール時のアクセス許可を確認する
- 信頼できるダウンロードサイトからアプリケーションを入手する
  - （例）Android Market，au one Market
  - 公開アプリが海賊版である可能性が低い

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

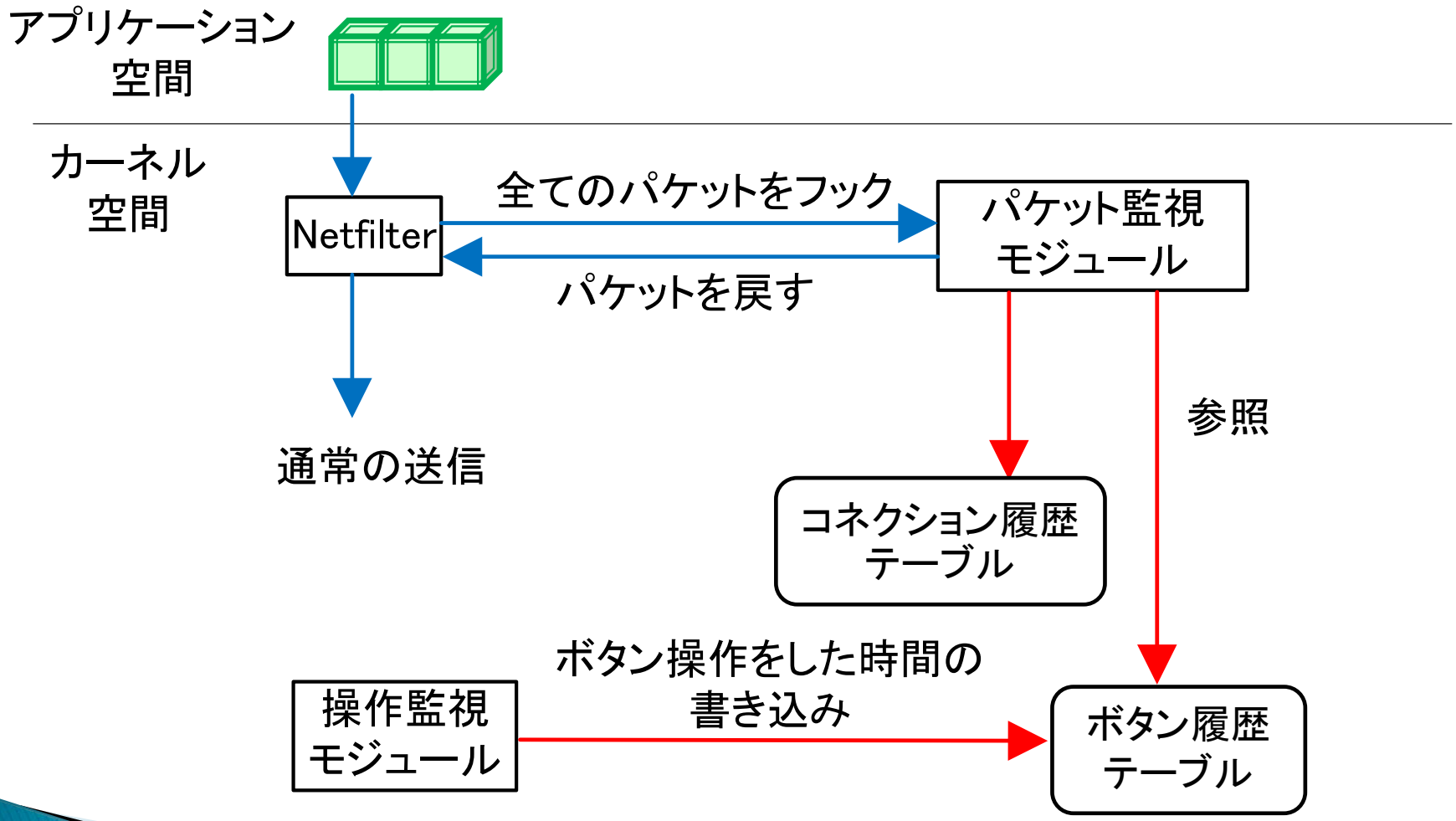
ユーザが行う特徴的な操作

- メール送信時の送信ボタンを押す操作

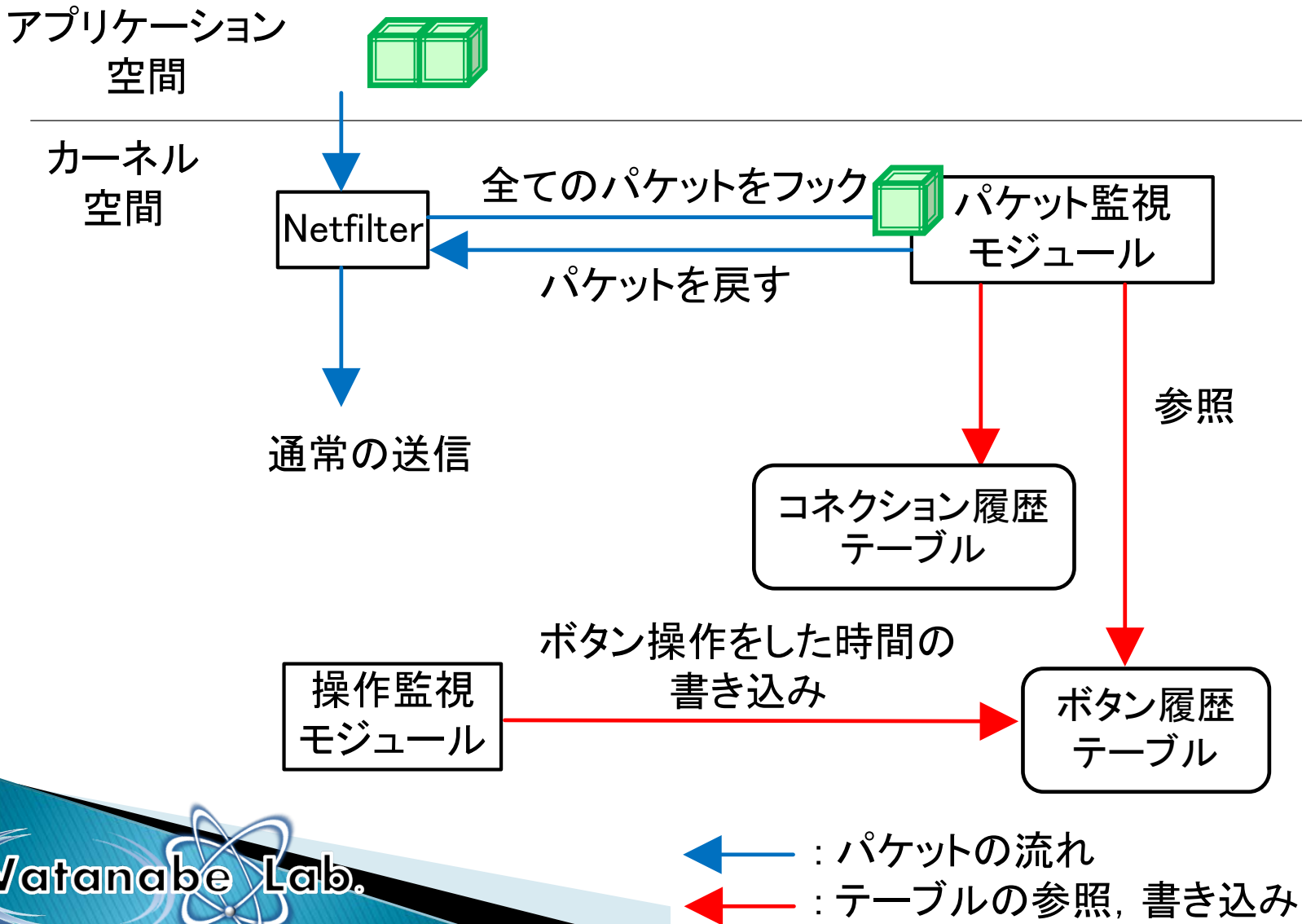
ボットには出来ない操作

- カーネルレベルでのボタン操作検出

提案方式の概要

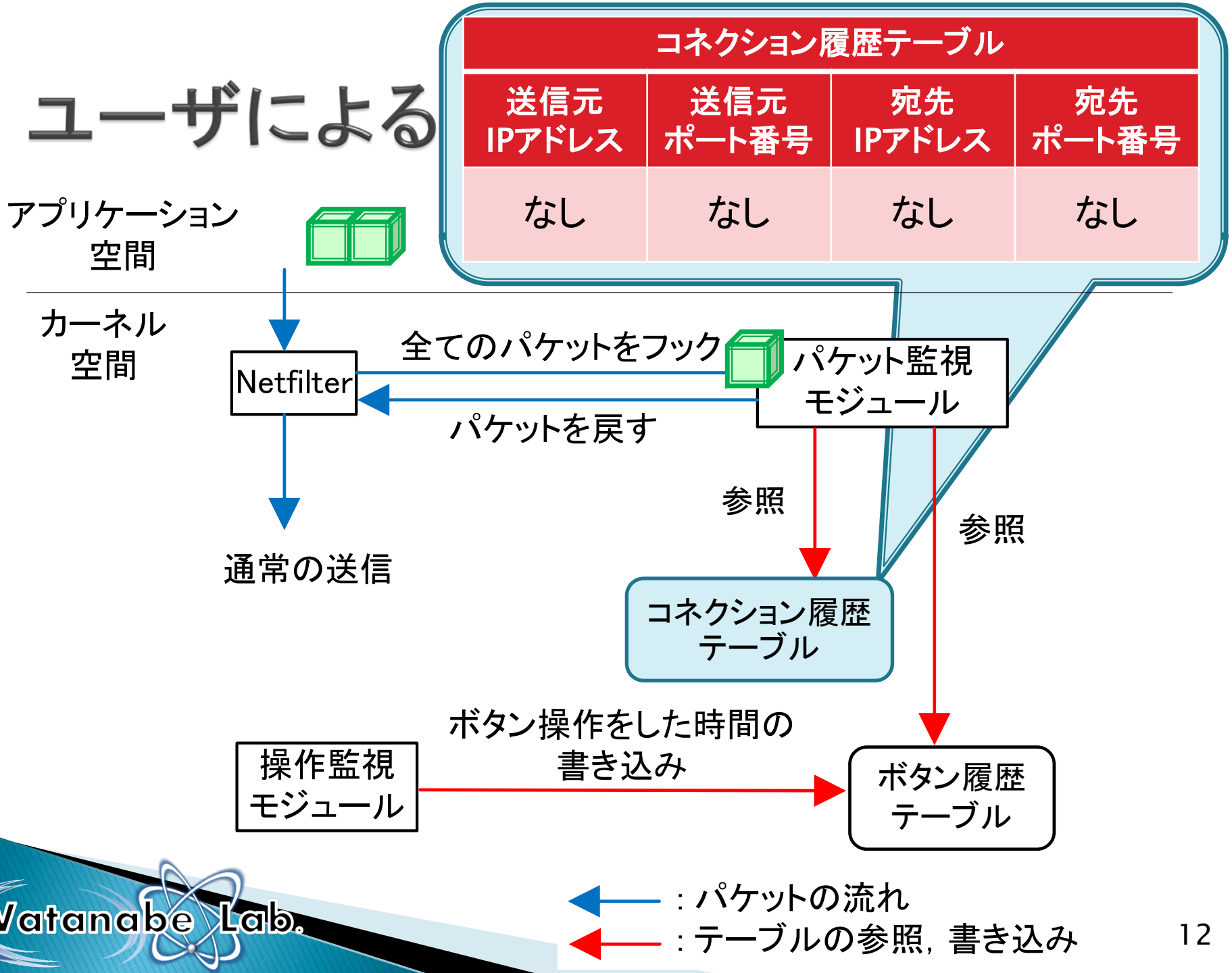

アプリケーション
空間
カーネル
空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視
モジュール
通常の送信
参照
コネクション履歴
テーブル
ボタン操作をした時間の
書き込み
操作監視
モジュール
ボタン履歴
テーブル
：パケットの流れ
：テーブルの参照，書き込み

ユーザによる操作の場合

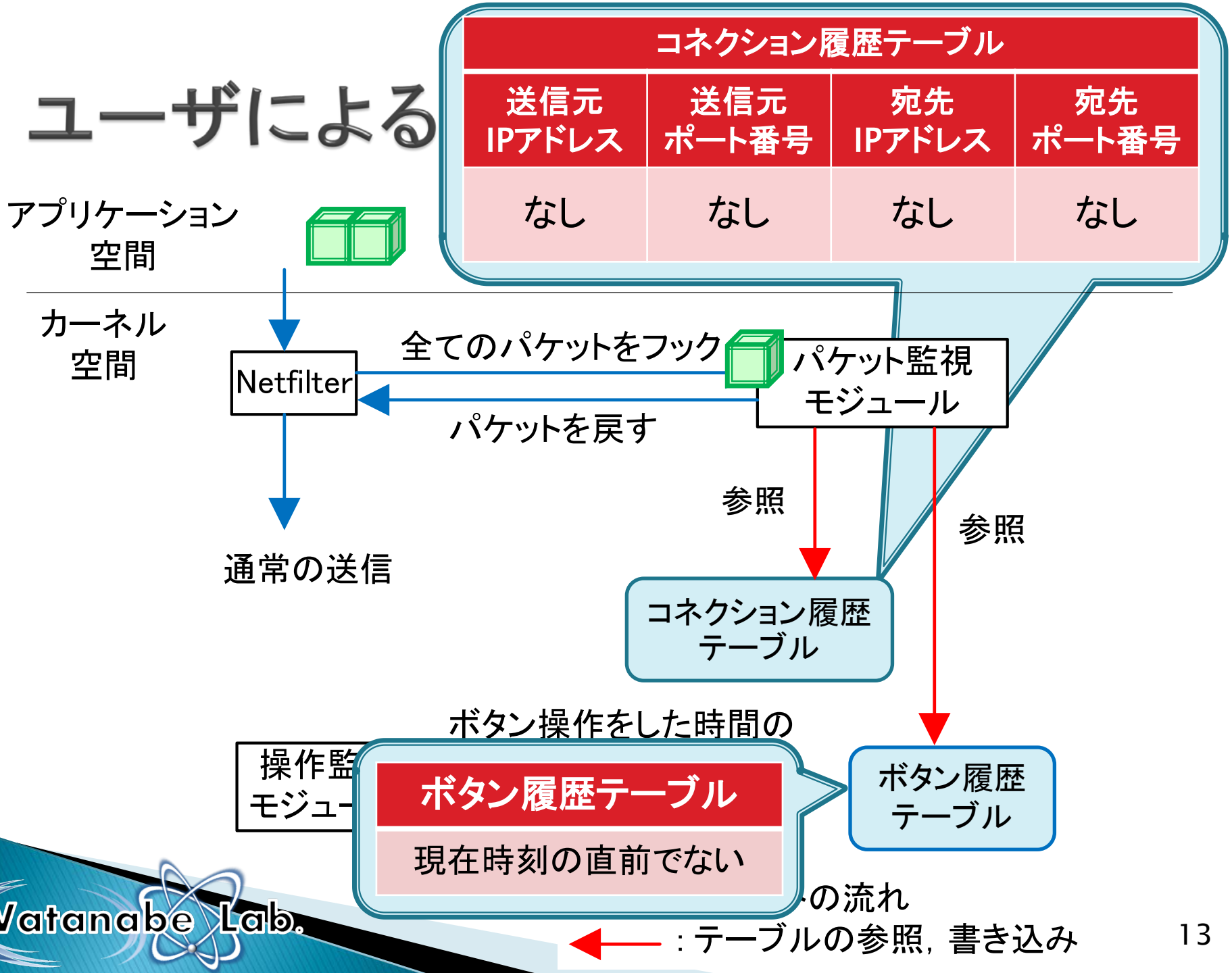


ユーザによる

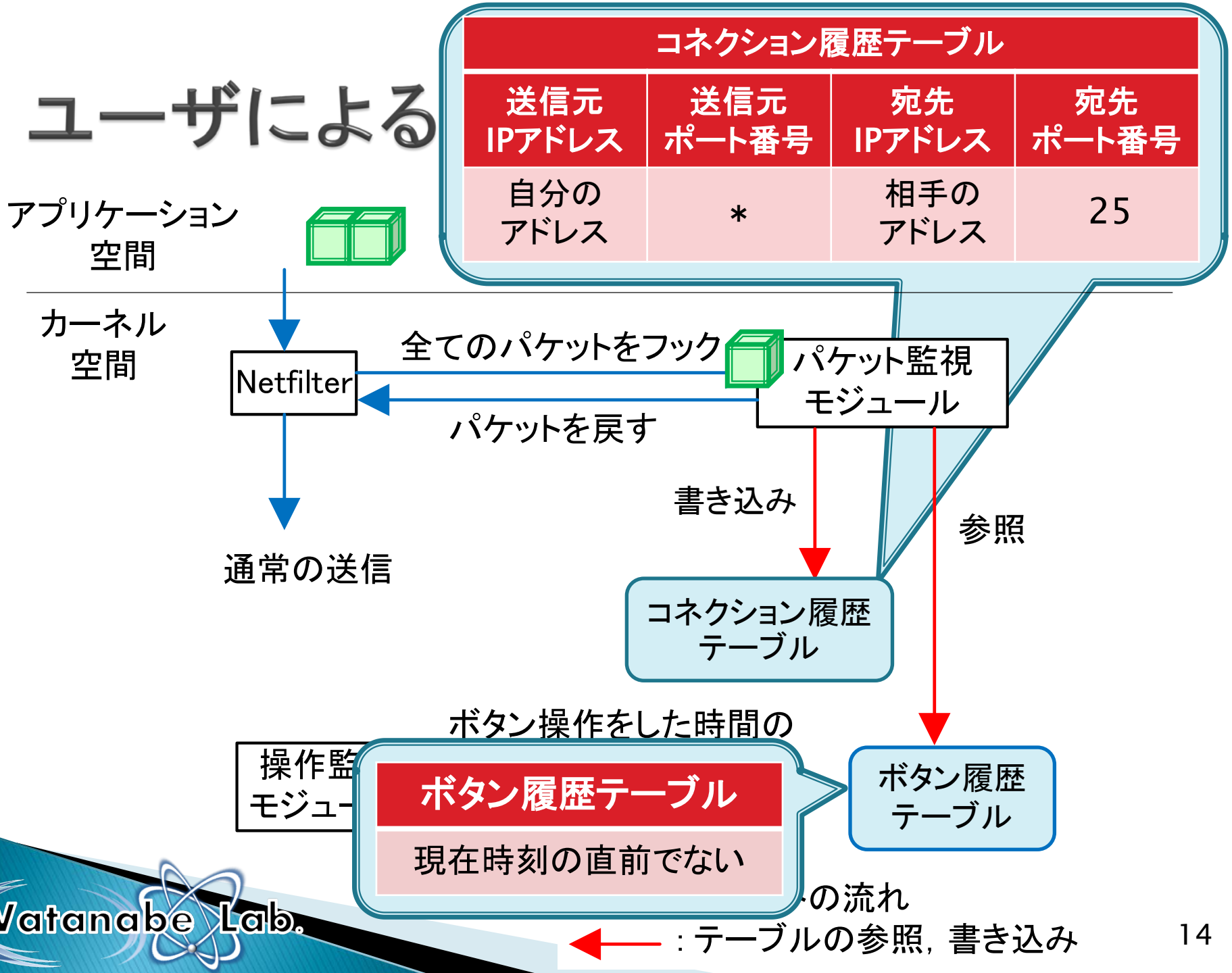
コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
なし	なし	なし	なし



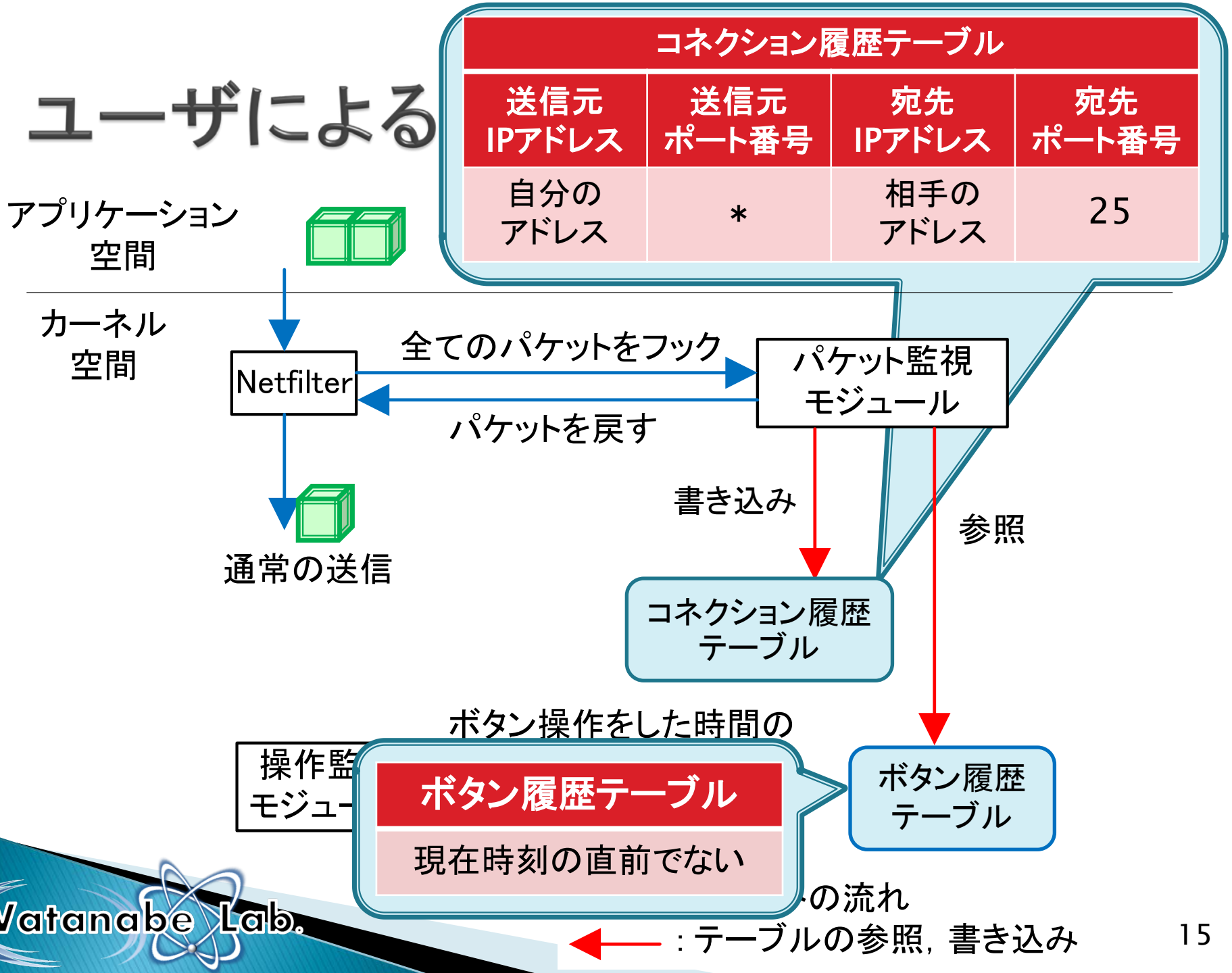
ユーザによる


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
の流れ
：テーブルの参照，書き込み

ユーザによる

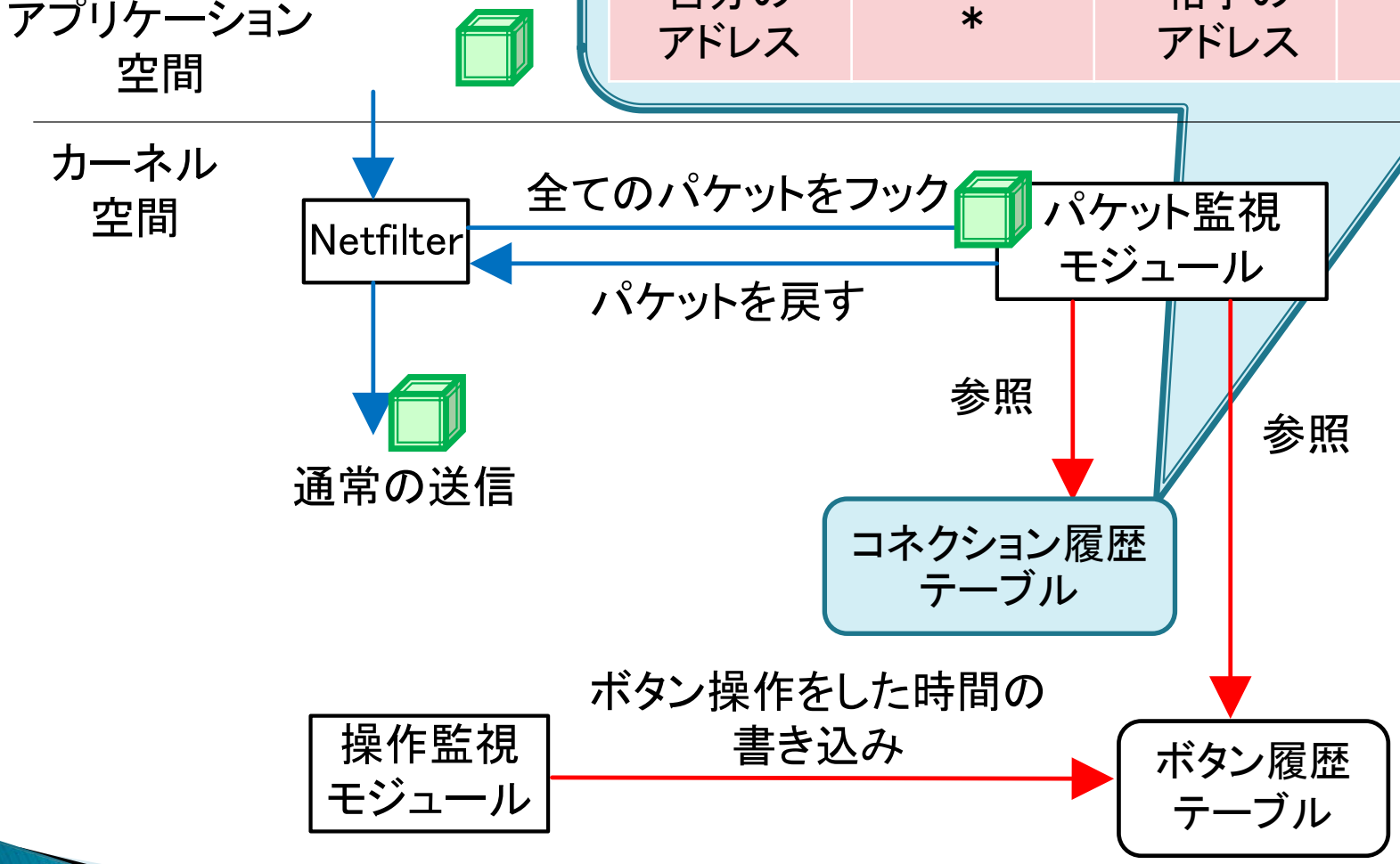

コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
自分の アドレス
*
相手の アドレス
25
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフック
パケットを戻す
パケット監視 モジュール
書き込み
参照
通常の送信
コネクション履歴 テーブル
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル
の流れ
：テーブルの参照，書き込み

ユーザによる


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
の流れ
：テーブルの参照，書き込み

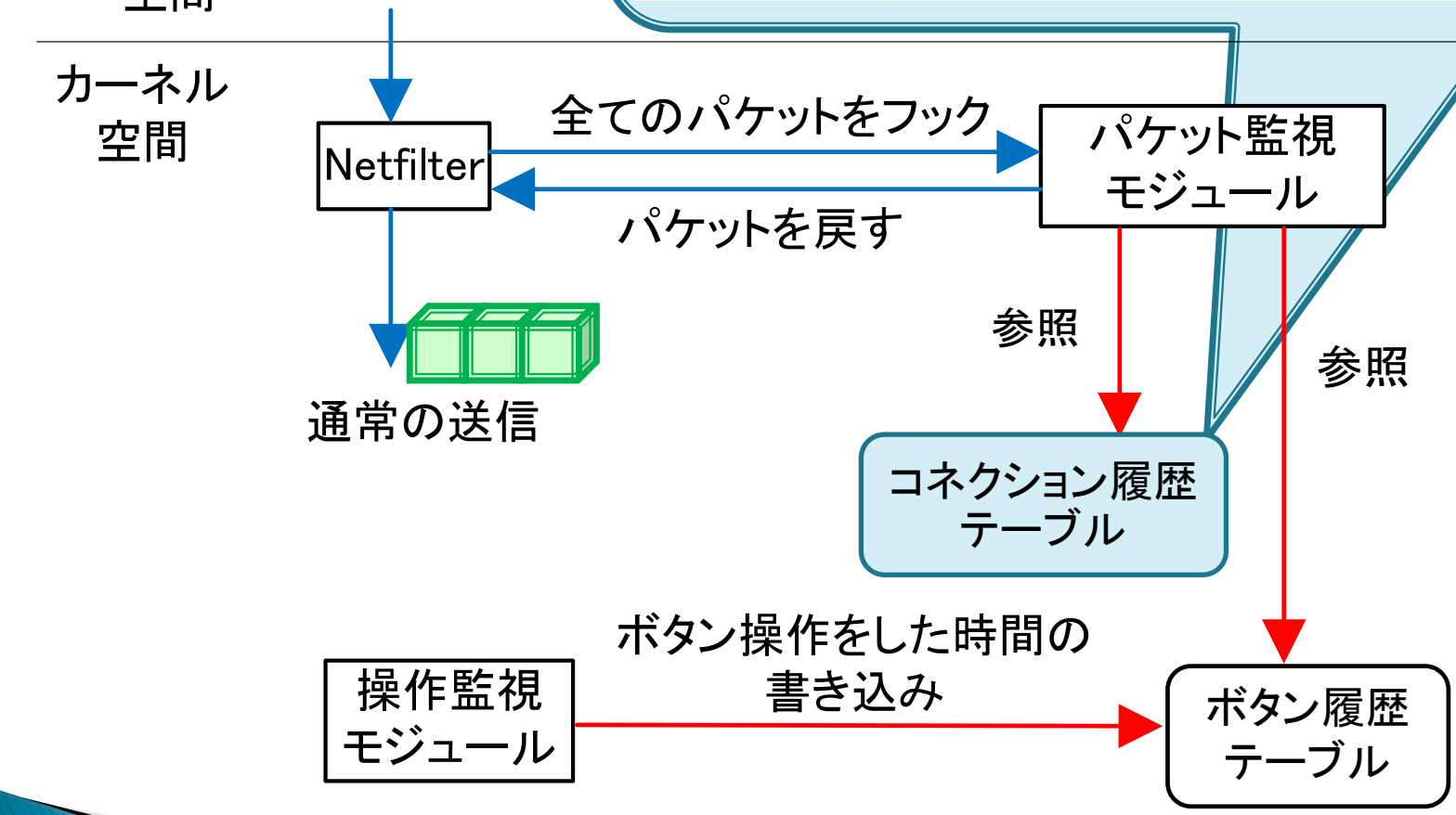
ユーザによる

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



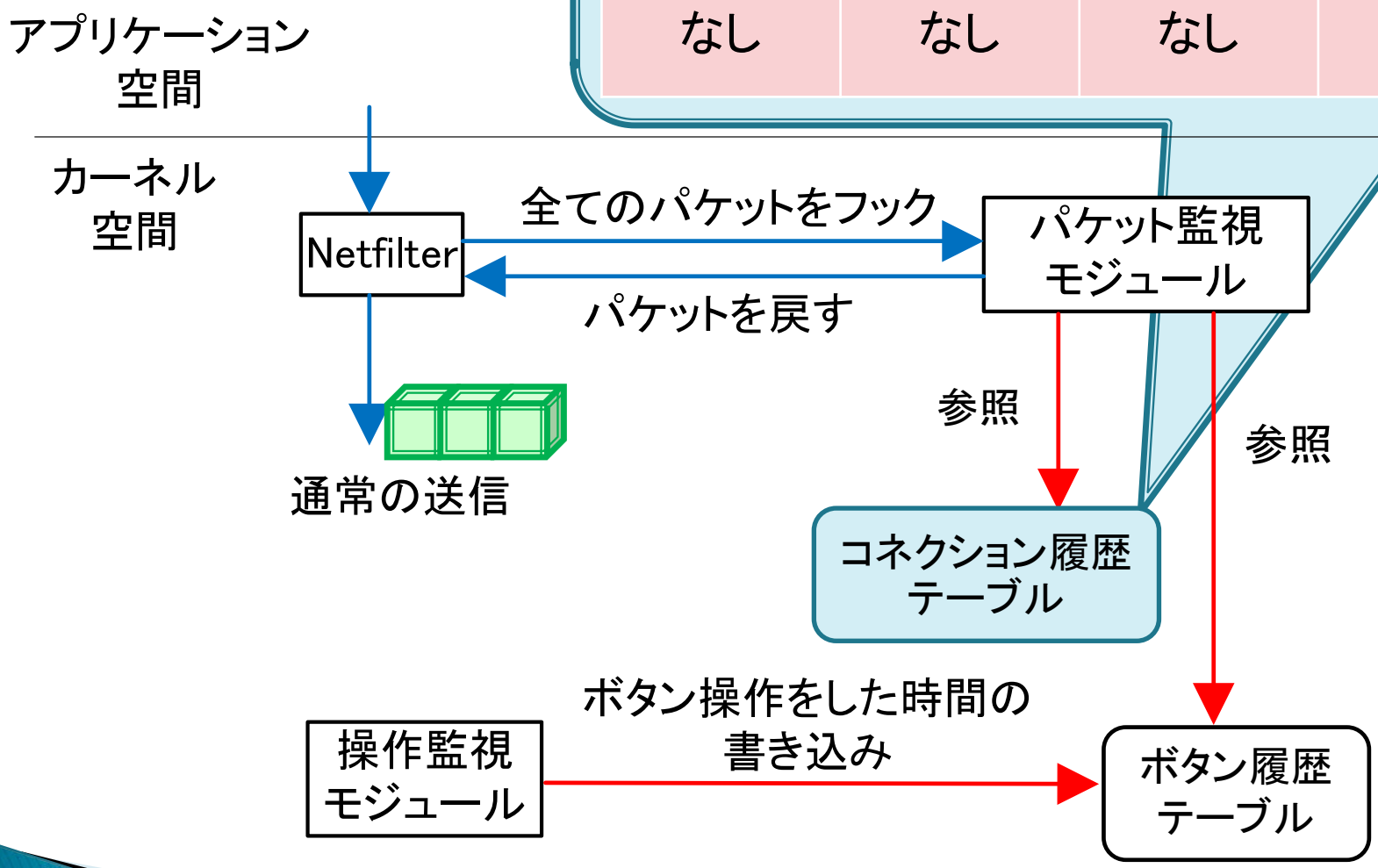
ユーザによる

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

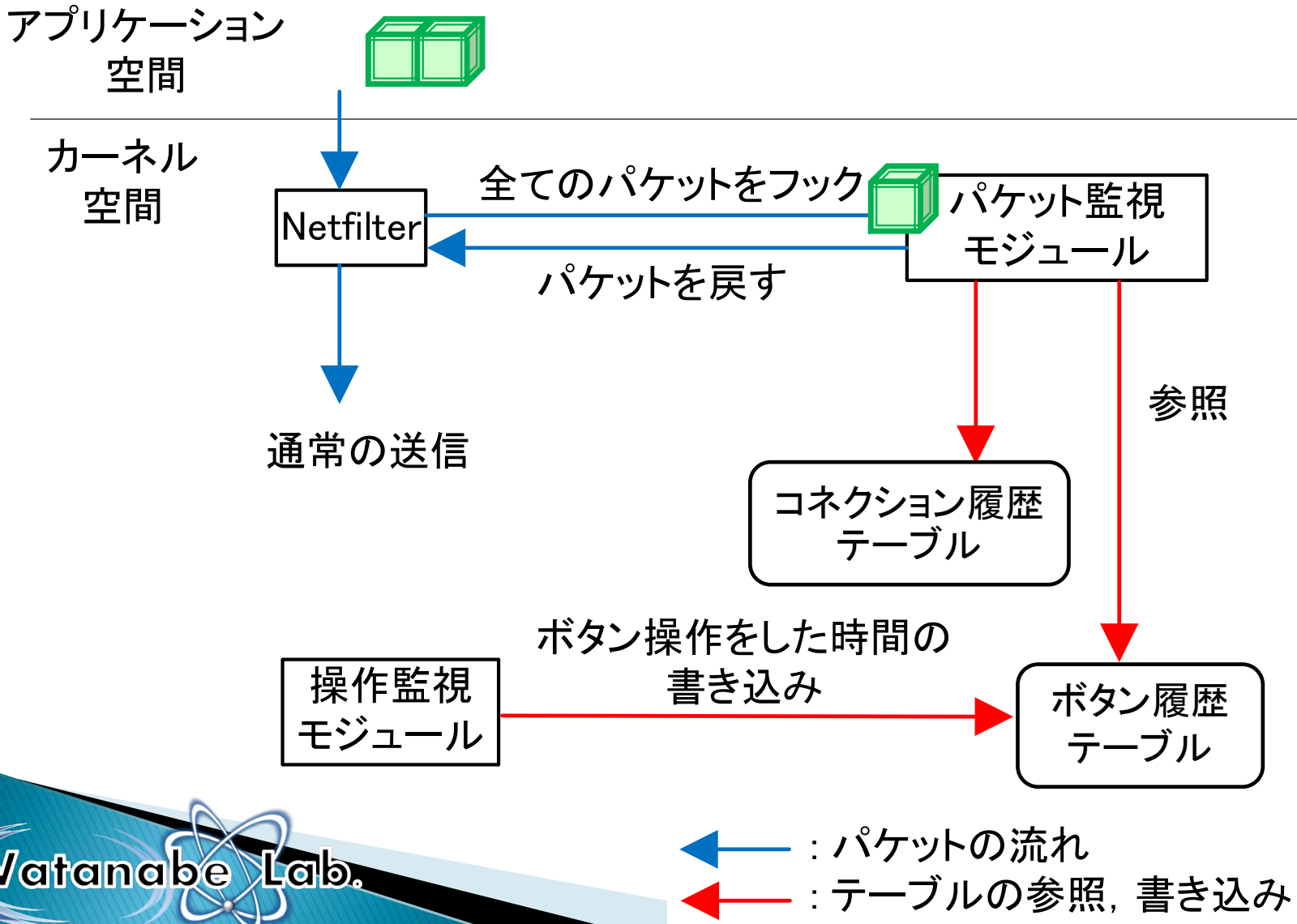


ユーザによる

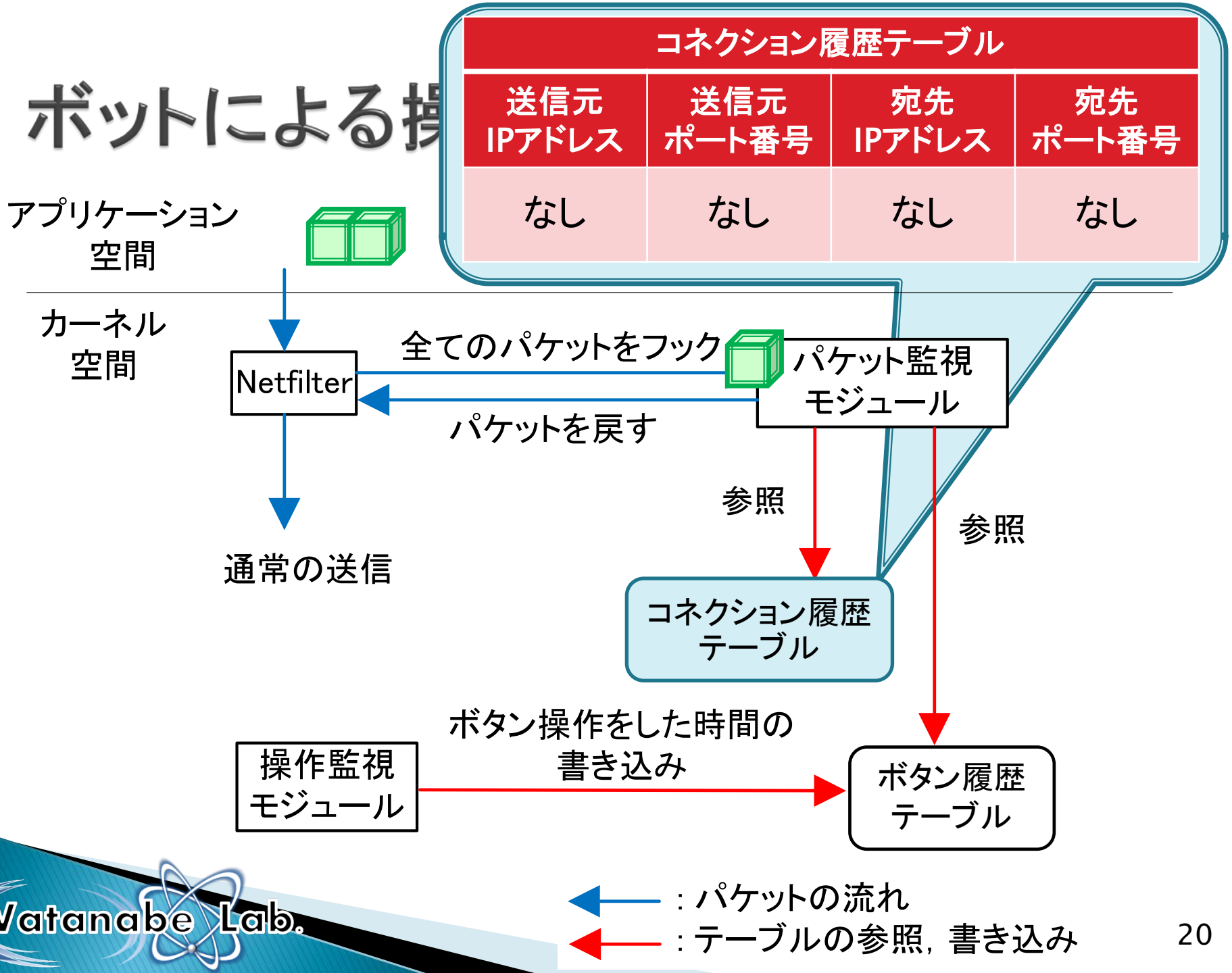
コネクション履歴テーブル			
送信元 IPアドレス	送信元 ポート番号	宛先 IPアドレス	宛先 ポート番号
なし	なし	なし	なし



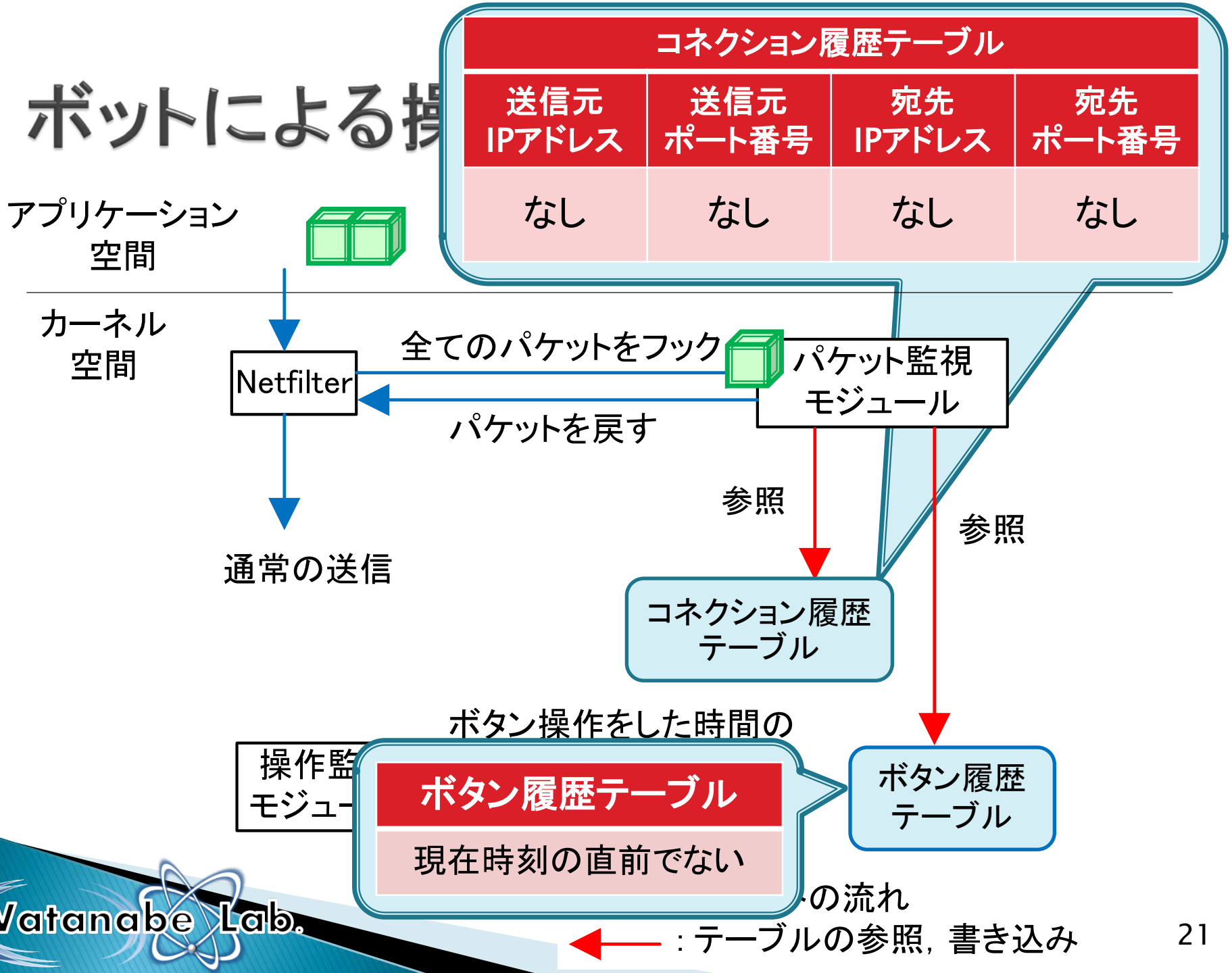
ボットによる操作の場合



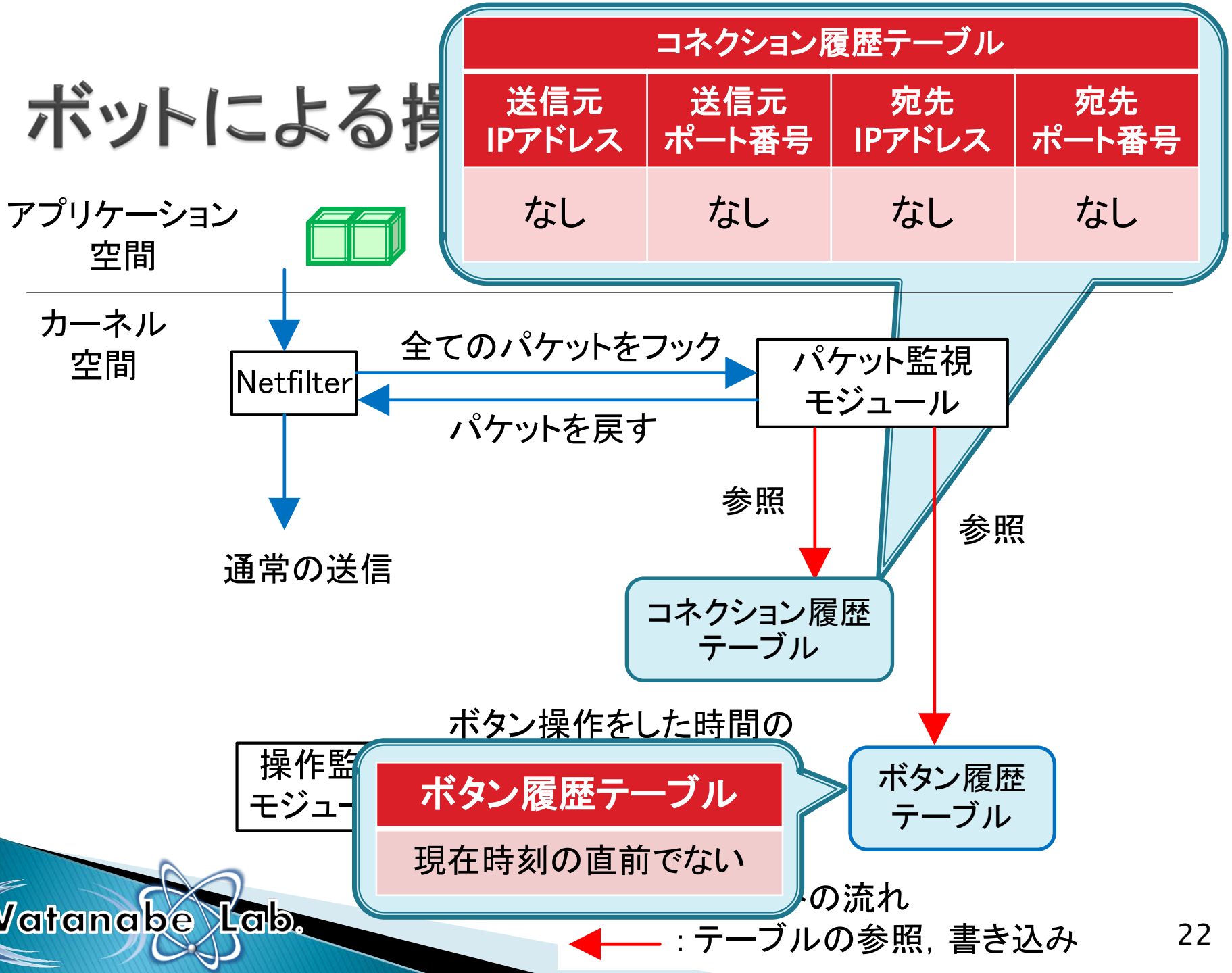
ボットによる操


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
ボタン操作をした時間の 書き込み
操作監視 モジュール
ボタン履歴 テーブル
：パケットの流れ
：テーブルの参照，書き込み

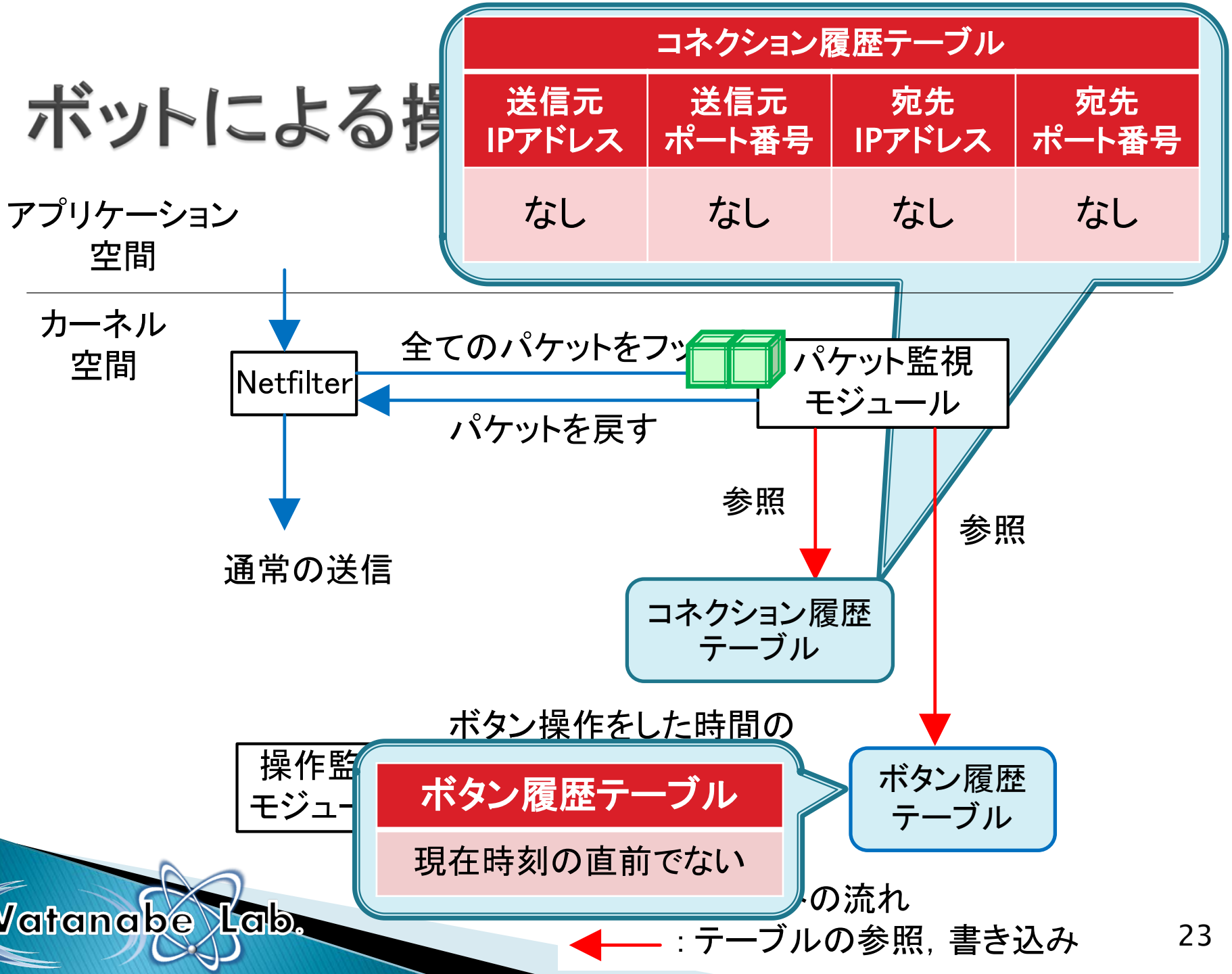
ボットによる操


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
の流れ
：テーブルの参照，書き込み

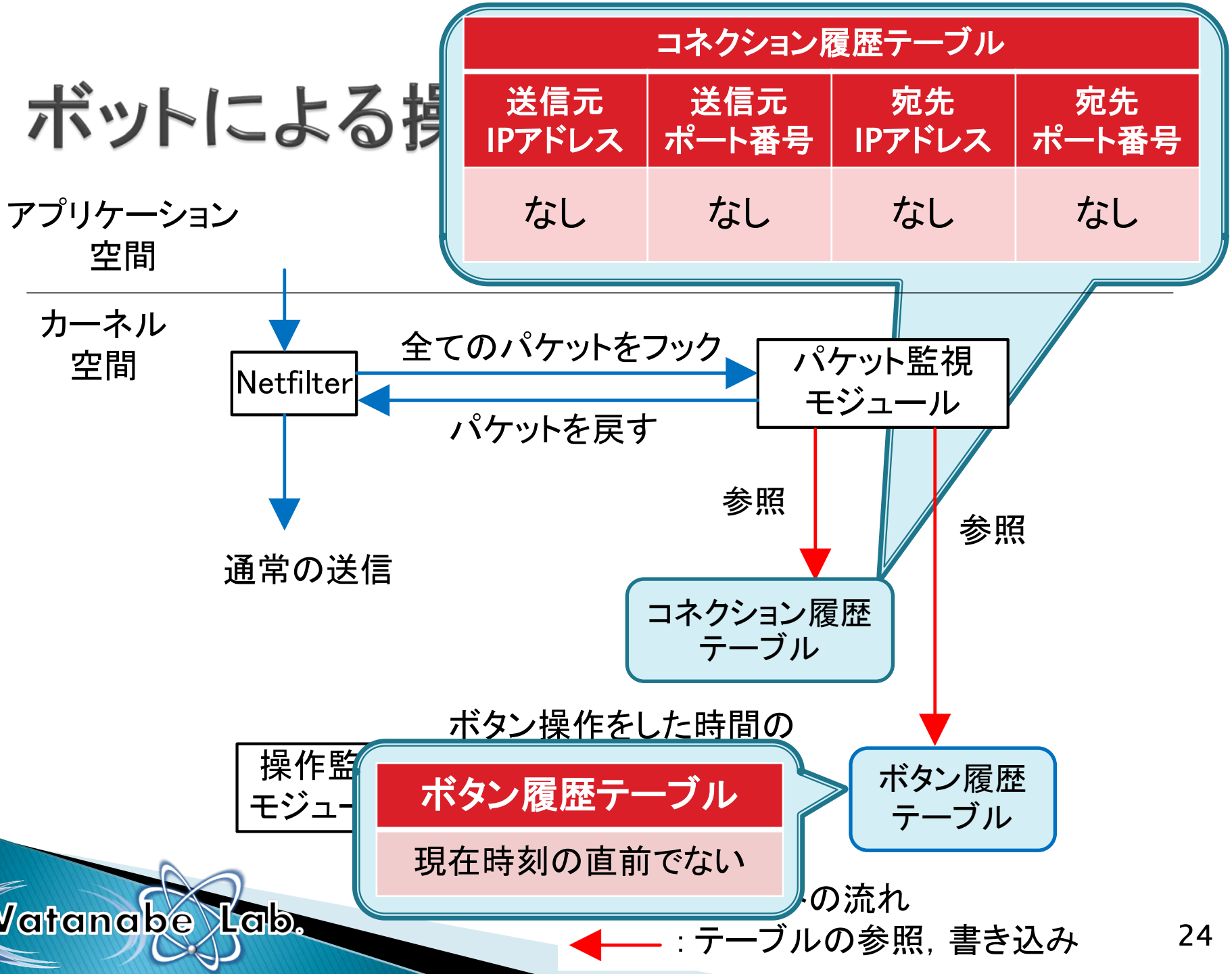
ボットによる操


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
の流れ
：テーブルの参照，書き込み

ボットによる操

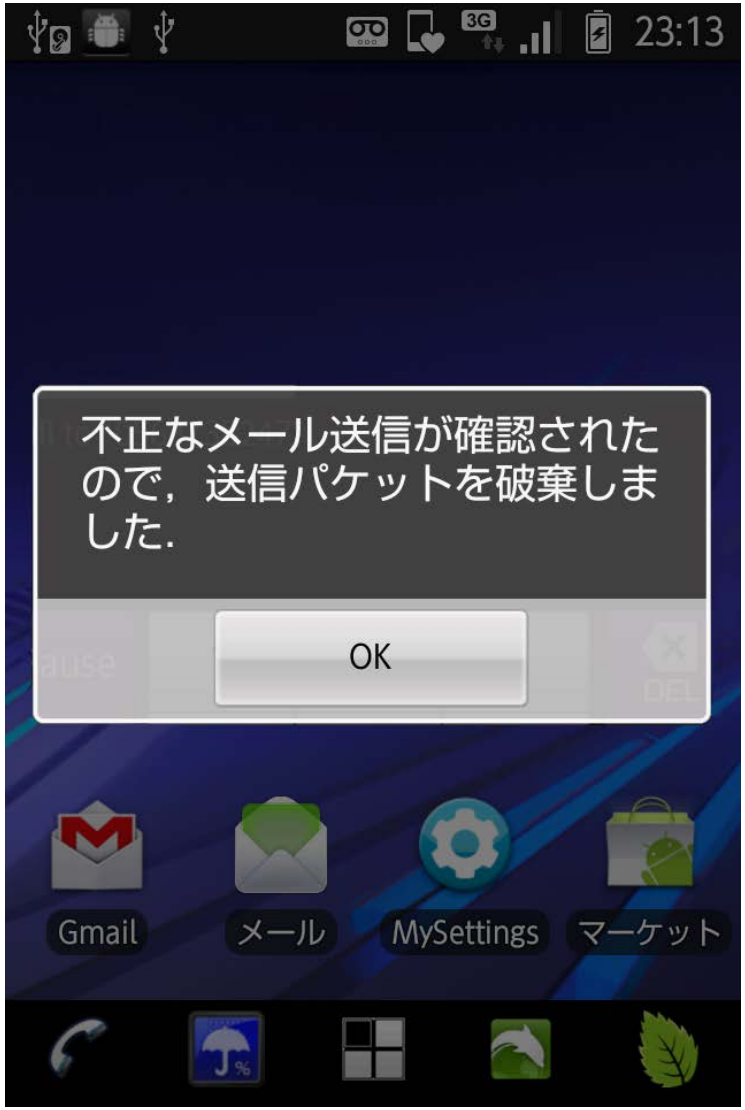

コネクション履歴テーブル
送信元 IPアドレス
送信元 ポート番号
宛先 IPアドレス
宛先 ポート番号
なし
なし
なし
なし
アプリケーション 空間
カーネル 空間
Netfilter
全てのパケットをフッ
パケットを戻す
パケット監視 モジュール
通常の送信
参照
参照
コネクション履歴 テーブル
ボタン操作をした時間の
操作監
モジュー
ボタン履歴テーブル
現在時刻の直前でない
ボタン履歴 テーブル
の流れ
：テーブルの参照，書き込み

ボットによる操


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
通常の送信
参照
参照
コネクション履歴 テーブル
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
の流れ
：テーブルの参照，書き込み

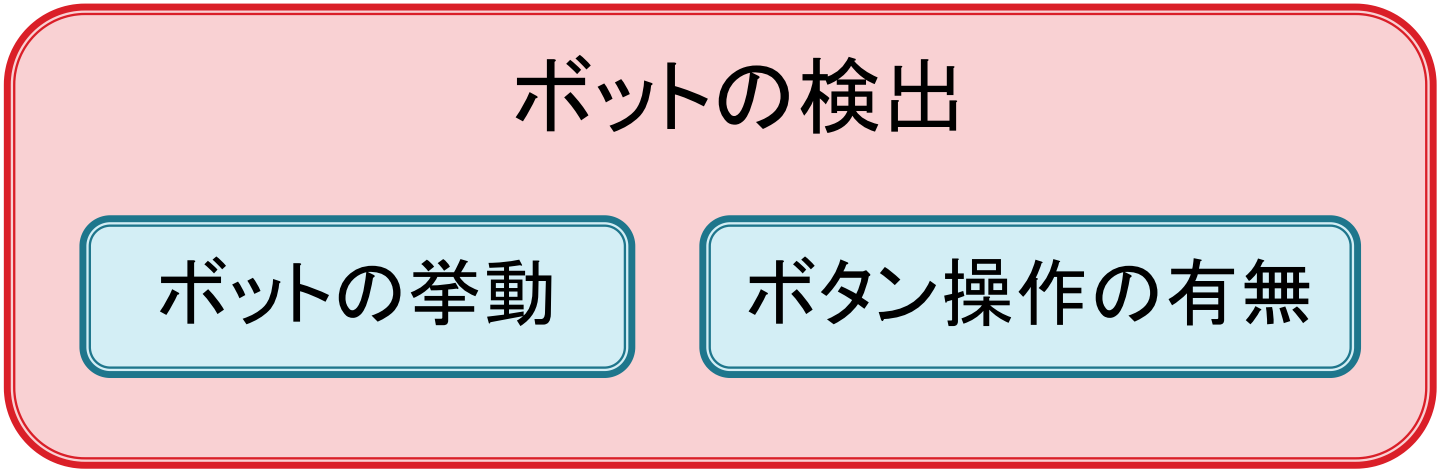
ボットによる操作の場合

- 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)