# 割り込みの禁止/許可の調査と実装

2015/11/11

藤田将輝

## 1 はじめに

本デバッグ支援環境を用いて短い間隔で連続で割り込みを発生させ，NIC ドライバにパケットを処理させた際，IPI の送信間隔が 3 μ s までの場合，一定して 256 個のパケットしか処理できない．この原因について調査したところ，本デバッグ支援環境では割り込みを禁止できていないことが原因であることを特定した．本資料では，この調査，割り込みの禁止/許可の実装，および再測定について記述した．

## 2 取得できるパケットの調査

現在のデバッグ支援環境では，256 回以上デバッグ支援機構を動作させた際，パケットのサイズによらず，IPI 送信間隔が 3 μ s 以下であれば，256 個しかパケットが取得できない．各パケットにシーケンス番号を付与し，どのパケットを取得できているかを調査した．具体的には，以下の処理流れで調査した．

(1) 1000 個のパケットを生成し，順に番号を付与する．
(2) デバッグ支援機構を 1000 回連続で動作させる．この際，(1) で生成したパケットを順に NIC ドライバに格納し，IPI を送信する．
(3) NIC ドライバでパケットを処理する際，処理するパケットを静的に確保した配列に格納する．
(4) デバッグ支援機構の動作が終了すると，配列からパケットを取り出し，シーケンス番号を確認する．

この結果，最後の 256 個のパケットを処理できていることが分かった．

## 3 取得したパケットが 256 個である原因

パケットの受信処理では，受信バッファにあるパケットを全て処理する．2 章の実験では最後の割り込みにのみ反応し，受信バッファに残っている 256 個のパケットを処理していると考えられる．受信バッファのエントリは 256 個であるため，残っているすべてのパケットを処理している．最後の 256 個のみを処理していることから，2 章の実験では割り込み処理中に新たな割り込みが入ることで，パケットの受信処理まで処理を進めていないと考えられる．パケットの受信処理は割り込みハンドラ内でパケットを処理するのではなく，割り込みハンドラで割り込みを禁止し，パケットの処理は他の関数でするように依頼する．この処理流れが守られているとすると，割り込み処理中に他の割り込みは禁止されるはずである．したがって，本デバッグ支援環境では適切に割り込みを禁止できていないことが考えら

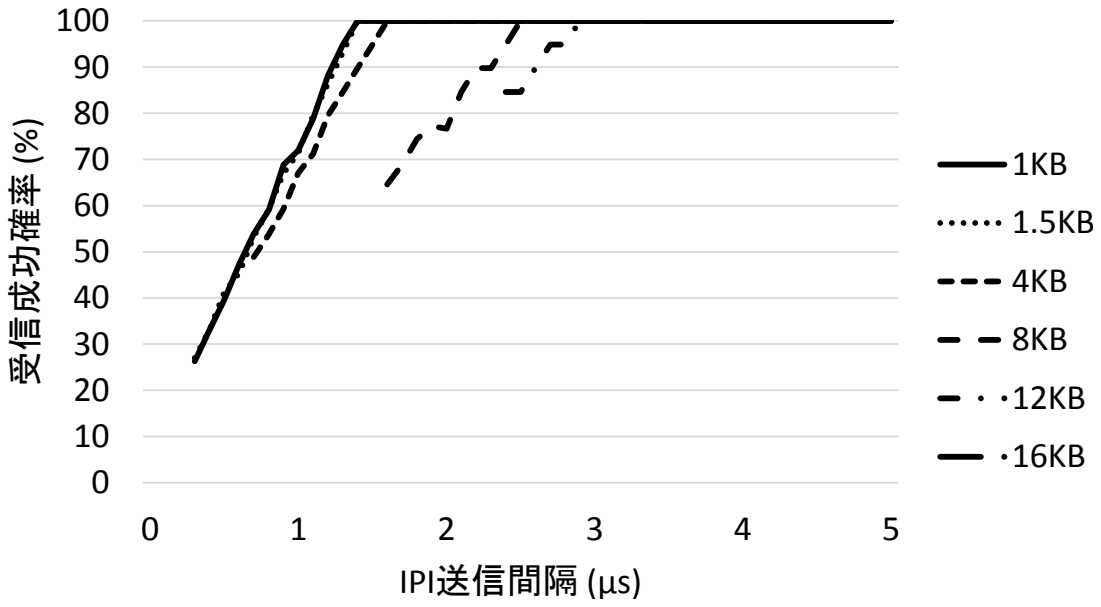


図 1　ドライバを対象とした測定

れる．このため，割り込みを禁止する処理について調査する必要がある．

# 4　割り込みの禁止/許可の処理流れ

NIC ドライバが割り込みハンドラ内で割り込みを禁止し，許可するまでの処理流れを以下に示す．

(1) 割り込みが発生すると，割り込みハンドラ (`rtl8169_interrupt()`) が動作する．
(2) 割り込みハンドラではパケットの受信処理を行わず，割り込みを禁止して受信処理用のポーリング関数をカーネルの管理する `poll_list` に格納し，ソフト割り込みを発生させる．割り込みの禁止には `IntrStatus` という割り込みの状態を表すレジスタを更新し，割り込みの禁止状態にすることで NIC からの割り込みを禁止する．
(3) ソフト割り込みを受け，ハンドラである `net_rx_action()` が動作する．
(4) `net_rx_action()` は `poll_list` からポーリング関数を取り出し，実行する．
(5) NIC のポーリング関数 (`rtl8169_poll()`) がパケットの受信処理関数である `rtl8169_rx_interrupt()` を実行する．
(6) `rtl8169_rx_interrupt()` でパケットを処理する．処理が終わると `rtl8169_poll()` に処理が戻る．
(7) 全てのパケットを処理すると割り込みを許可し，処理を終える．許可する際も，`IntrStatus` を更新することで割り込みを許可する．

`IntrStatus` を更新して禁止される割り込みは NIC からの割り込みである．本デバッグ支援環境は NIC を用いず，コア間の割り込み (IPI) を用いているため，割り込みを禁止できていない．このため，適切に割り込みを禁止する機能が必要である．

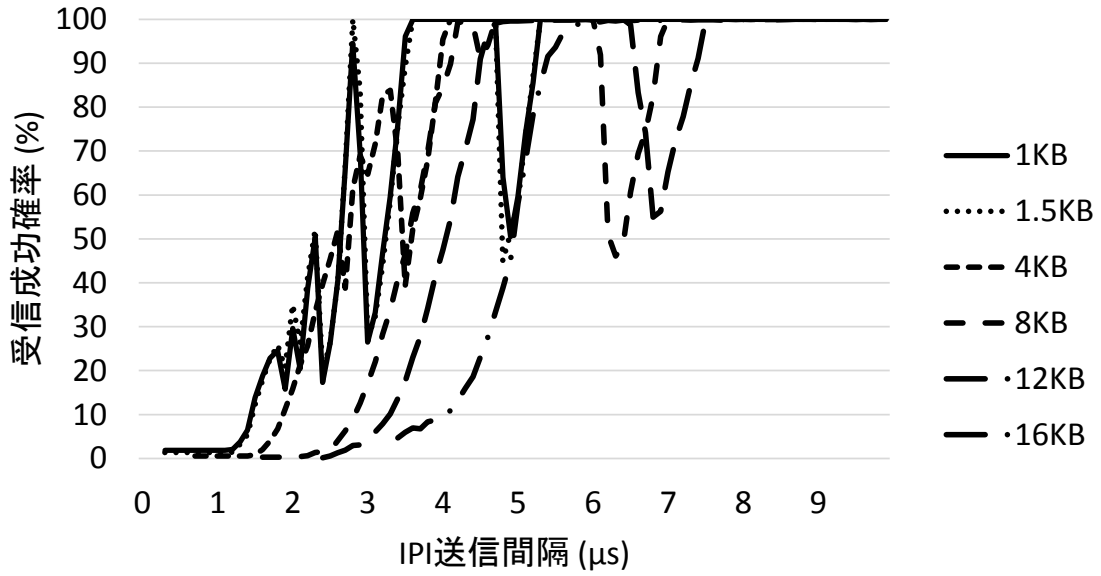


図 2　プログラムを対象とした測定

# 5　対処

割り込みの禁止/許可の実装のため，共有メモリに割り込みの禁止/許可を表すフラグを配置し，これが 1 であれば割り込みを禁止し，0 であれば割り込みを許可することとした．NIC ドライバの処理中で，割り込みを禁止するタイミングでこのフラグを 1 に更新し，許可するタイミングでこのフラグを 0 に更新することで，割り込みの禁止/許可を実現した．

# 6　再測定

## 6.1　ドライバを対象とした測定

割り込みの禁止/許可を実装したデバッグ支援環境で，どの程度のパケットのサイズと IPI の送信間隔ならば NIC ドライバでパケットを取得できるかについて再測定を行った．結果を図 1 に示す．結果から，IPI の送信間隔が 3 μ s 以下の場合でも，1 次関数的に受信成功率が上昇していることがわかる．このことから割り込みが適切に禁止/許可できていることが分かる．

## 6.2　プログラムを対象とした測定

6.1 節と同様に，デバッグ対象 OS 上で動作する UDP の受信用プログラムでどの程度のパケットを受信できるかを再測定した．結果を図 2 に示す．結果から，サイズが大きくなるほど全てのパケットを受信するのに時間がかかることが分かる．また，度々パケット受信成功率が大きく減少する．これはタイマ割り込み等が原因かと考えているが詳細は不明である．

# 7　おわりに

本資料では，割り込みの禁止/許可を本デバッグ支援環境に実装し，これを用いてどの程度パケットを取得できるかを再測定した.