

IronPort パケットキャプチャ手順書(Vesion : AsyncOS 7.x 以降)

・AsyncOS 7.x 以降は CLI からのパケットキャプチャ(TCPDUMP)に加え GUI での取得も可能です。

*CLI からの操作方法はこちらを参照してください：

http://gold.nvc.co.jp/supports/ironport/folder.2009-12-20.5000992028/folder.2009-12-20.9928859880/FAQ-sozai/copy_of_capture.pdf

1. パケットキャプチャを取得したい機器にログイン後、画面右上の「ヘルプとサポート」を選択します。



2. 次に取得条件の設定を行います。

2-1. 設定は「パケットキャプチャ設定」の「設定を編集」から行えます。

パケットキャプチャ

現在のパケットキャプチャ

パケットキャプチャは利用されていません。

[キャプチャを開始](#)

パケットキャプチャファイルの管理

C170-503DE59CBFAA-FGL15344060-20120524-100655.cap (132K)

C170-503DE59CBFAA-FGL15344060-20120309-160553.cap (222K)

C170-503DE59CBFAA-FGL15344060-20120309-160151.cap (2M)

[選択ファイルの削除](#) [ダウンロードファイル](#)

パケットキャプチャ設定

キャプチャファイルサイズ制限:	200 MB
キャプチャ期間:	制限無しでキャプチャを実行
選択したインターフェイス:	ALL
選択したフィルタ:	フィルタなし

[設定を編集...](#)

2-2. キャプチャファイルサイズ設定

取得するファイルのサイズを設定します。(デフォルトは最大値の 200MB となっています)

パケットキャプチャ設定の編集

パケットキャプチャ設定

キャプチャファイルサイズ制限: ① 200 MB 最大ファイルサイズ: 200MB

キャプチャ期間: ②

③

④

⑤

⑥

⑦

⑧

⑨

⑩

⑪

⑫

⑬

⑭

⑮

⑯

⑰

⑱

⑲

⑳

㉑

㉒

㉓

㉔

㉕

㉖

㉗

㉘

㉙

㉚

㉛

㉜

㉝

㉞

㉟

㊱

㊲

㊳

㊴

㊵

㊶

㊷

㊸

㊹

㊺

㊻

㊼

㊽

㊾

㊿

注: パケットキャプチャ設定は、実行するとその日に有効状態になります。

キャンセル 実行

2-3. キャプチャ期間

キャプチャを行う期間を設定します。下記の 3 つから選択してください。

- ファイルサイズ期限に達するまでキャプチャを実行
- 時間制限になりまでキャプチャを実行
- 制限なしでキャプチャを実行(デフォルト設定)

* 「ファイルサイズ制限に達するまで…」以外を選択した場合はサイズが「キャプチャファイルサイズ制限」に達し次第古いパケットから削除されていきます。

2-4. インターフェース

パケットキャプチャを取得するインターフェースを選択します。特に制限がない場合は「Use all interfaces」を選択します。

2-5. パケットキャプチャフィルタ

ここでは、特定のポートやクライアント IP、サーバ IP を指定できます。

- ① 特定のポートや IP を指定しない場合は「フィルタなし」
- ② 特定のポートや IP を指定する場合は「事前定義されたフィルタ」
*全ての条件を埋める必要はございません
- ③ パケットキャプチャの Syntax が分かっている場合はカスタムフィルタにその Syntax をいれることでフィルタリングを行うことができます。

2-6. 設定が完了したら右下にある「実行」ボタンをクリックしてください。

*「変更の確定」は必要なく、実行ボタンをクリックした段階で即時反映となります。

3. キャプチャの取得

3-1. 「現在のパケットキャプチャ」の右端にある「キャプチャを開始」をクリックするとパケットキャプチャを開始します。

3-2. 開始が成功すると下図のように「成功 — パケットキャプチャを開始しました。」と表示されます。また、「現在のパケットキャプチャ」にはステータスや設定が表示されます。

パケットキャプチャ

成功 — パケットキャプチャを開始しました。

現在のパケットキャプチャ

ステータス: キャプチャ実行中(経過: 16s)
ファイル名: C170-503DE59CBFAA-FGL15344060-20120524-130731.cap (サイズ: 136K)

現在の設定:
最大ファイルサイズ: 200MB
キャプチャ制限: 無制限
キャプチャインターフェイス: ALL
キャプチャフィルタ: フィルタなし

キャプチャ停止

パケットキャプチャファイルの管理

- C170-503DE59CBFAA-FGL15344060-20120524-100655.cap (132K)
- C170-503DE59CBFAA-FGL15344060-20120309-160553.cap (222K)
- C170-503DE59CBFAA-FGL15344060-20120309-160151.cap (2M)

選択ファイルの削除 ダウンロードファイル

パケットキャプチャ設定

3-3. 3-2 の図で「キャプチャ停止」をクリックするとキャプチャが停止され、下図のようにキャプチャしたファイルが作成されます。

パケットキャプチャ

成功 — パケットキャプチャは停止しています。
ファイル "C170-503DE59CBFAA-FGL15344060-20120524-130731.cap" は作成されました。

現在のパケットキャプチャ

パケットキャプチャは利用されていません。

キャプチャを開始

パケットキャプチャファイルの管理

- C170-503DE59CBFAA-FGL15344060-20120524-130731.cap (144K)
- C170-503DE59CBFAA-FGL15344060-20120524-100655.cap (132K)
- C170-503DE59CBFAA-FGL15344060-20120309-160553.cap (222K)
- C170-503DE59CBFAA-FGL15344060-20120309-160151.cap (2M)

選択ファイルの削除 ダウンロードファイル

パケットキャプチャ設定

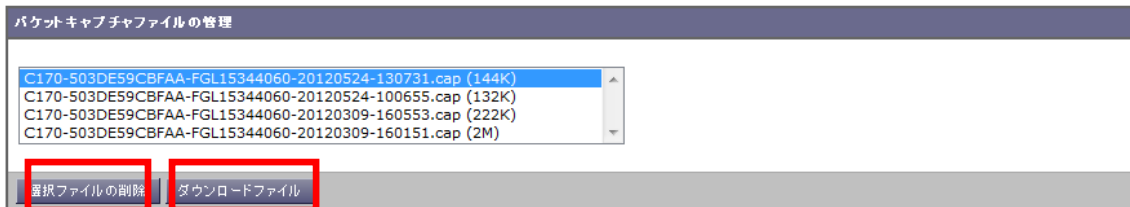
キャプチャファイルサイズ制限:	200 MB
キャプチャ期間:	制限無しでキャプチャを実行
選択したインターフェイス:	ALL
選択したフィルタ:	フィルタなし

設定を編集...

NVC

4. ファイルの管理

4-1. 中段の「パケットキャプチャファイルの管理」にて、「ダウンロードファイル」をクリックすることにより先ほど取得したファイルをダウンロードすることが可能です。



4-2. ファイルの削除

過去のファイルを削除したい場合は削除したいファイルを選択し、「選択ファイルの削除」から削除してください。