CHAPTER 3

# NetFlow レコード：フォーマットおよびフィールドの内容

この章では、NetFlow レコードに含まれるフィールドについて説明します。

NetFlow は、次の RDR に含まれるデータに対して生成することができます。

- Subscriber Usage RDR（SUR）
- Package Usage RDR（PUR）
- Link Usage RDR（LUR）
- Virtual Links Usage RDR（VUR）
- Malicious Usage RDR (MALUR)



## NetFlow

- Cisco Service Control Application for Broadband（SCA BB）は、NetFlow v5 および v9 をサポートしています。
- NetFlow の詳細については、次の資料を参照してください。
  - 『*Cisco IOS NetFlow Version 9 Flow-Record Format, EDCS-307741*』
  - RFC 3954

# NetFlow フィールド タイプ

**表 3-1　NetFlow フィールド**

| フィールド タイプ | 値 | 長さ（バイト数） | 説明 |
|---|---|---|---|
| sceSubscriberId | 300 | 64 | サブスクライバ管理インターフェイスを介して導入されたサブスクライバ ID ストリング。不明なサブスクライバの場合、このフィールドには空のストリングが格納されます。このストリングには、必要な桁数だけ 0 が入力されます。 |
| scePackageId | 301 | 2 | サブスクライバに割り当てられたサービス コンフィギュレーション パッケージ / プロファイルの ID |
| sceServiceId | 302 | 4 | レポートされたセッションのサービス分類 |
| sceProtocolId | 303 | 2 | レポートされたセッションに対応付けられたプロトコルを示す固有の ID。<br><br>PROTOCOL_ID は、トランザクションの特定のトランスポート プロトコルに応じ、汎用 IP/ 汎用 TCP/ 汎用 UDP プロトコル ID になります。ただし、レポートされたセッションと一致する、より具体的なプロトコル定義（シグネチャベース プロトコルまたはポートベース プロトコルなど）がサービスに割り当てられる場合を除きます。 |
| sceSkipppedSessions | 304 | 4 | 前回のこの種類のレポート レコード以降の、レポートされていないセッションの数 |
| sceInitiatingSide | 305 | 1 | トランザクションの開始側<br><br>• 0：サブスクライバ側<br>• 1：ネットワーク側 |
| sceReportTime | 306 | 4 | このレポート レコードの終了タイムスタンプ。このフィールドは、1970 年 1 月 1 日の夜 12 時以降の秒数を表す UNIX time_t フォーマットの値です。 |
| sceTransactionDuration Millisec | 307 | 4 | このレポート レコードでレポートされているトランザクションの有効期間（ミリ秒単位） |
| sceTimeFrame | 308 | 1 | 4 つの有効な時間枠のどれが、レポート レコードが生成された期間として使用されたか。<br><br>このフィールドの値は 0 ～ 3 の範囲のいずれかです。 |

表 3-1　NetFlow フィールド（続き）

| フィールド タイプ | 値 | 長さ（バイト数） | 説明 |
|---|---|---|---|
| sceSessionUpstreamVolume | 309 | 4 | トランザクションのアップストリーム ボリューム（バイト単位）。ボリュームは、トランザクションにバンドルされたすべてのフローの両方のリンクに関する集約アップストリーム ボリュームを表します。 |
| sceSessionDownstream Volume | 310 | 4 | トランザクションのダウンストリーム ボリューム（バイト単位）。ボリュームは、トランザクションにバンドルされたすべてのフローの両方のリンクに関する集約ダウンストリーム ボリュームを表します。 |
| sceIpProtocolType | 311 | 1 | IP プロトコル タイプ |
| sceProtocolSignature | 312 | 4 | このセッションに対応付けられたプロトコル シグニチャの ID |
| sceZoneId | 313 | 4 | このセッションに対応付けられたゾーンの ID |
| sceFlavorId | 314 | 4 | フレーバを持つプロトコル シグニチャの場合、このフィールドにはこのセッションに対応付けられたフレーバを示す ID が格納されています。 |
| sceFlowCloseMode | 315 | 1 | フローが終了する理由 |
| | 316-319 | | 予約されています。 |
| sceAccessString | 320 | 128, 256, 512, 1024 | トランザクションから抽出されたレイヤ 7 プロパティ |
| sceInfoString | 324 | 128, 256, 512, 1024 | トランザクションから抽出されたレイヤ 7 プロパティ |
| | 328-350 | | 予約されています。 |
| sceServiceUsageSubscriber CounterId | 351 | 2 | 各サービスは、カウンタにマッピングされます。サブスクライバの有効範囲内に 32 のカウンタがあります。 |
| sceBreachState | 352 | 1 | サブスクライバのクォータに違反があるかどうか<br>• 0：クォータの違反はない<br>• 1：クォータの違反がある |
| sceReason | 353 | 1 | レポート レコードが生成された理由<br>• 0：定期的なレコード<br>• 1：サブスクライバのログアウト<br>• 2：パッケージの切り替え<br>• 3：ラップアラウンド<br>• 4：集約期間の終了 |
| sceConfiguredDuration | 354 | 4 | 連続するレポート レコードの間の、設定された時間（秒単位） |

表 3-1　NetFlow フィールド（続き）

| フィールド タイプ | 値 | 長さ（バイト数） | 説明 |
|---|---|---|---|
| sceDuration | 355 | 4 | 前回のこの種類のレポート レコード以降、経過した秒数 |
| sceEndTime | 356 | 4 | このレポート レコードの終了タイムスタンプ。このフィールドは、1970 年 1 月 1 日の夜 12 時以降の秒数を表す UNIX time_t フォーマットの値です。 |
| sceUpstreamVolume | 357 | 4 | 現在のレポート期間の、すべてのセッションの両方のリンク上の集約アップストリーム ボリューム（キロバイト単位） |
| sceDownstreamVolume | 358 | 4 | 現在のレポート期間の、すべてのセッションの両方のリンク上の集約ダウンストリーム ボリューム（キロバイト単位） |
| sceSessions | 359 | 2 | 現在のレポート期間の、レポートされたサービスの集約セッション数 |
| sceSeconds | 360 | 2 | 現在のレポート期間の、レポートされたサービスの集約セッション秒数 |
| scePackageCounterId | 361 | 2 | 各パッケージは、カウンタにマッピングされます。64 のパッケージ使用カウンタがあります。 |
| sceGeneratorId | 362 | 1 | レポート レコードを生成するプロセッサを識別する数値 |
| sceServiceGlobalCounterId | 363 | 2 | 各サービスは、カウンタにマッピングされます。64 のグローバル使用カウンタがあります。 |
| sceConcurrentSessions | 364 | 4 | このレポート レコードの生成時にレポートされたサービスを使用する同時セッション数 |
| sceActiveSubscribers | 365 | 4 | このレポート レコードの生成時にレポートされたサービスを使用する同時サブスクライバ数 |
| sceTotalActiveSubscribers | 366 | 4 | このレポート レコードの生成時の、システム内の同時サブスクライバ数 |
| sceLinkId | 367 | 1 | レポートされたネットワーク リンクに対応付けられた数値<br>• 0：物理リンク 1<br>• 1：物理リンク 2 |
| sceVirtualLinkId | 368 | 1 | レポートされた仮想ネットワーク リンクに対応付けられた数値 |
| | 369-399 | | 予約されています。 |
| sceAttackId | 400 | 4 | 固有攻撃 ID |
| sceAttackIp | 401 | 4 | この攻撃に関連した IP アドレス |

表 3-1　NetFlow フィールド（続き）

| フィールド タイプ | 値 | 長さ（バイト数） | 説明 |
|---|---|---|---|
| sceAttackOtherIp | 402 | 4 | この攻撃に関連する他の IP アドレスが存在する場合は、そのアドレス。存在しない場合は –1。 |
| sceAttackPortNumber | 403 | 2 | この攻撃に関連するポート番号が存在する場合は、そのポート番号（たとえば IP スキャンの場合）。存在しない場合は –1。 |
| sceAttackType | 404 | 4 | sceAttackIp の所属<br>• 0：被攻撃側<br>• 1：攻撃側 |
| sceAttackSide | 405 | 1 | IP アドレス側<br>• 0：サブスクライバ<br>• 1：ネットワーク |
| sceAttackIpProtocol | 406 | 1 | IP プロトコル タイプ<br>• 0：他<br>• 1：ICMP<br>• 6：TCP<br>• 17：UDP |
| sceAttacks | 407 | 1 | 現在のレポート期間中の攻撃の数。攻撃レポートは攻撃ごとに生成されるため、0 または 1 の値を取ります。 |
| sceAttackMaliciousSessions | 408 | 4 | 現在のレポート期間の、レポートされた攻撃の集約セッション数。SCE プラットフォームが攻撃をブロックする場合は、このフィールドは –1 の値をとります。 |
| | 409-499 | | 予約されています。 |