



## データ構造の例

この付録には、一部の侵入、相関、ディスカバリの各イベントのデータ構造の例が記載されています。それぞれの例は、各ビットがどのように設定されているかを明確に示すため、2進数形式で表示されます。

詳細については、次の各項を参照してください。

- [侵入イベントのデータ構造の例](#)
- [ディスカバリ データ構造の例 \(A-31 ページ\)](#)

## 侵入イベントのデータ構造の例

このセクションには、侵入イベントについて eStreamer で送信される可能性があるデータ構造の例が記載されています。ここでは、次の例を示します。

- [Management Center 5.4+ の侵入イベントの例 \(A-1 ページ\)](#)
- [侵入影響アラートの例 \(A-7 ページ\)](#)
- [パケット レコードの例 \(A-9 ページ\)](#)
- [分類レコードの例 \(A-10 ページ\)](#)
- [優先度レコードの例 \(A-12 ページ\)](#)
- [ルール メッセージ レコードの例 \(A-12 ページ\)](#)
- [6.1.x の接続統計データ ブロックの例 \(A-15 ページ\)](#)
- [バージョン 5.1+ ユーザー イベントの例 \(A-28 ページ\)](#)

## Management Center 5.4+ の侵入イベントの例

次の図に、イベント レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    | 2  |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |    |    |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|
| ビット | 0 | 1 | 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 |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1 | 0 |

## ■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|
|     | 0 | 1 | 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 |   |   |   |
| 3   | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  |   |   |   |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 5   | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  |   |   |   |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 7   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 8   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 9   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 10  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 11  | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  |   |   |   |
| 12  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  |   |   |   |
| 13  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 14  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 15  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 16  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 17  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
| 18  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |   |   |   |
|     | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0 | 0 |   |
| 19  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1 | 1 |   |
|     | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
| 20  | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0 | 0 |   |
| 21  | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
| 22  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|
|     | 0 | 1 | 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 |   |   |   |   |   |   |   |   |   |
| 23  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |   |   |   |   |   |   |   |
| 24  | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 0  |   |   |   |   |   |   |   |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  |   |   |   |   |   |   |   |   |   |
|     | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1 |   |   |   |   |   |   |   |   |
|     | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0  |   |   |   |   |   |   |   |   |   |
| 25  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |   |   |   |   |   |   |
| 26  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1 | 1 | 1 | 1 |   |   |   |   |   |
| 27  | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 1 | 0 | 0 |   |   |   |   |   |   |
| 28  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0 | 0 | 1 | 0 | 0 |   |   |   |   |
| 29  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 1 |   |   |   |
| 30  | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 0 | 0 | 1 | 1 | 1 | 0 |   |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0 | 0 | 1 | 0 | 0 |   |   |   |   |
|     | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0 | 0 | 1 | 0 | 0 | 1 |   |   |   |
|     | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1 | 0 | 1 | 0 | 0 |   |   |   |   |
| 31  | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1 | 0 | 0 | 0 | 1 | 1 |   |   |   |
|     | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0 | 0 | 0 | 1 | 1 |   |   |   |   |
|     | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0 | 1 | 1 | 0 | 1 | 0 | 1 |   |   |
|     | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1 | 0 | 0 | 1 | 1 | 0 | 0 |   |   |
| 32  | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0 | 0 | 1 | 1 | 0 | 1 | 0 |   |   |
|     | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0 | 0 | 0 | 1 | 1 |   |   |   |   |
|     | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |   |
|     | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |   |
| 33  | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
|     | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0 | 0 | 0 | 1 | 1 |   |   |   |   |
|     | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |   |
|     | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |

■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
| 34  | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  |
|     | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  |
|     | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  |
|     | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  |
| 35  | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 1  |
| 36  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  |
| 37  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 38  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 39  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 40  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 41  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 54  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 43  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 44  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

上記の例では、次のイベント情報を確認できます。

| ケース | 説明   |
|-----|--|
| 1   | この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージタイプ 4)であることを示しています。   |
| 2   | この行は、後続のメッセージの長さが 294 バイトであることを示しています。   |
| 3   | この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 400 を示し、侵入イベント レコードを表しています。 |
| 4   | この行は、後続のイベント レコードの長さが 278 バイトであることを示しています。   |
| 5   | この行は、イベントの保存時のタイムスタンプです。この場合、2014 年 7 月 2 日(水)の 16 時 11 分 27 秒に保存されています。   |
| 6   | この行は、将来使用するために予約されており、ゼロが入っています。   |
| 7   | この行は、ブロック タイプが 45 であることを示しています。これは、バージョン 5.4+ の侵入イベント レコードのブロック タイプです。   |
| 8   | この行は、データ ブロックの長さが 278 バイトであることを示しています。   |
| 9   | この行は、イベントがセンサー番号 5 から収集されることを示しています。   |
| 10  | この行は、イベント ID 番号が 65580 であることを示しています。   |
| 11  | この行は、イベントが 1404317489 秒で発生したことを示しています。   |
| 12  | この行は、イベントが 46542 マイクロ秒で発生したことを示しています。  |
| 13  | この行は、ルール ID 番号が 4 であることを示しています。  |
| 14  | この行は、イベントがジェネレータ ID 番号 119(ルールエンジン)で検出されたことを示しています。  |
| 15  | この行は、ルールのリビジョン番号が 1 であることを示しています。  |
| 16  | この行は、分類 ID 番号が 1 であることを示しています。   |
| 17  | この行は、優先度 ID 番号が 3 であることを示しています。  |
| 18  | この行は、送信元 IP アドレスが 10.5.61.220 であることを示しています。このフィールドには IPv4 アドレスと IPv6 アドレスのいずれかが含まれる可能性があることに注意してください。  |
| 19  | この行は、宛先 IP アドレスが 10.5.56.133 であることを示しています。このフィールドには IPv4 アドレスと IPv6 アドレスのいずれかが含まれる可能性があることに注意してください。   |
| 20  | この行の最初の 2 バイトは送信元ポート番号が 33018 であることを示し、2 番目の 2 バイトは宛先ポート番号が 8080 であることを示しています。   |

| ケース | 説明  |
|-----|---|
| 21  | この行の最初のバイトは、TCP(6)がイベントで使用されているプロトコルであることを示しています。2番目のバイトは影響フラグであり、2番目のビットが1であるため、イベントがレッド(脆弱)であることを示します。また、送信元または宛先ホストはシステムによってモニターされているネットワーク内にあること、送信元または宛先ホストがネットワーク マップにあること、送信元または宛先ホストがイベント発生ポートでサーバーを実行していることを示します。さらに、2番目と3番目のフラグが1であるため、これがオレンジ(脆弱の可能性あり)のイベントであることを示しています。この行の3番目のバイトは影響フラグです。2であるため、イベントがオレンジ(脆弱の可能性あり)であることを示しています。最後のバイトはイベントがブロックされなかったことを示しています。 |
| 22  | この行には、MPLS ラベルが含まれます(存在する場合)。   |
| 23  | この行の最初の2バイトはVLAN IDが0であることを示しています。最後の2バイトは、予約されており、0に設定されています。  |
| 24  | この行には、侵入ポリシーの一意のID番号が含まれます。   |
| 25  | この行には、ユーザーの内部ID番号が含まれます。該当のユーザーが存在しないため、すべてゼロになっています。   |
| 26  | この行にはWebアプリケーションの内部ID番号が含まれ、この場合は847となっています。  |
| 27  | この行にはクライアントアプリケーションの内部ID番号が含まれ、この場合は2000000676となっています。  |
| 28  | この行にはアプリケーションプロトコルの内部ID番号が含まれ、この場合は676となっています。  |
| 29  | この行には、アクセス制御ルールの一意のIDが含まれ、この場合は1となっています。  |
| 30  | この行には、アクセス制御ポリシーの一意のIDが含まれます。   |
| 31  | この行には、入力インターフェイスの一意のIDが含まれます。   |
| 32  | この行には、出力インターフェイスの一意のIDが含まれます。このイベントはブロックされています。   |
| 33  | この行には、入力セキュリティゾーンの一意のIDが含まれます。  |
| 34  | この行には、出力セキュリティゾーンの一意のIDが含まれます。  |
| 35  | この行には、侵入イベントに関連付けられている接続イベントのUNIXタイムスタンプが含まれます。   |
| 36  | この行の最初の2バイトは、接続イベントが生成された管理対象デバイスのSnortインスタンスの数値IDを示します。残りの2バイトは、同じ秒の間に発生する接続イベントを区別するために使用される値を示します。   |
| 37  | この行の最初の2バイトは、送信元ホストの国のコードを示します。残りの2バイトは、宛先ホストの国のコードを示します。   |
| 38  | この行の最初の2バイトには、このイベントに関連付けられている侵害のID番号が含まれます。残りの2バイトには、トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)のID番号の最初の部分が含まれます。   |
| 39  | この行には、トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)のID番号の残りの部分が含まれます。   |

| ケース | 説明  |
|-----|---|
| 40  | この行の最初の 2 バイトには、トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の最後の 2 バイトが含まれます。SSL が使用された場合、2 番目の 2 バイトには、SSL サーバー証明書の SHA1 ハッシュの最初の部分が含まれます。   |
| 41  | SSL が使用された場合、この行には、SSL サーバー証明書の SHA1 ハッシュの残りの部分が含まれます。  |
| 54  | この行の最初の 2 バイトには、SSL サーバー証明書の SHA1 ハッシュの最後の 2 バイトが含まれます。2 番目の 2 バイトには、実際に実行された SSL アクションが含まれます。この接続では SSL が使用されなかったため、0 になっています。         |
| 43  | この行の最初の 2 バイトには、SSL フロー ステータスが含まれます。この接続では SSL が使用されなかったため、0 になっています。2 番目の 2 バイトには、このイベントに関連付けられているネットワーク分析ポリシーの UUID の最初の 2 バイトが含まれます。 |
| 44  | この行には、このイベントに関連付けられているネットワーク分析ポリシーの UUID の残りの部分が含まれます。  |

## 侵入影響アラートの例

次の図に、侵入影響アラート レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|
|     | 0 | 1 | 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 |   |   |   |   |   |   |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0 |   |   |   |   |   |   |   |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0 |   |   |   |   |   |   |   |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | 1 |   |   |   |   |   |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1 | 0 | 0 | 1 | 0 |   |   |   |
| 5   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 1 | 0 | 0 | 0 |   |   |   |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1 | 0 | 0 | 1 | 0 |   |   |   |
| 7   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1 | 0 | 0 | 0 | 0 |   |   |   |
| 8   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 1 | 0 |   |
| 9   | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1 | 0 | 0 | 0 |   |   |   |   |
| 10  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 11  | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 12  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## ■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|
| ビット | 0 | 1 | 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 |   |
| 14  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0 |
| 15  | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0 |
|     | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0 |
|     | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 1  | 0  | 1  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |

上記の例では、次の情報を確認できます。

| ケース | 説明  |
|-----|---|
| 1   | この行の最初の2バイトは、標準ヘッダー値 <sub>1</sub> を示しています。2番目の2バイトは、メッセージがデータメッセージ(メッセージタイプ4)であることを示しています。  |
| 2   | この行は、後続のメッセージの長さが58バイトであることを示しています。   |
| 3   | この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の15ビットは、イベントが検出されたドメインのNetmap IDを含むオプションフィールドです。行の残りの部分は、レコードタイプの値 <sub>9</sub> を示し、影響アラートレコードを表しています。 |
| 4   | この行は、後続のデータの長さが50バイトであることを示しています。   |
| 5   | この行には値 <sub>20</sub> が含まれており、侵入影響アラートデータブロックが後に続いていることを示しています。  |
| 6   | この行は、影響アラートブロックヘッダーを含む影響アラートブロックの長さを示し、この場合は50バイトです。  |
| 7   | この行は、イベントID番号が201256であることを示しています。   |
| 8   | この行は、イベントがデバイス番号2から収集されることを示しています。  |
| 9   | この行は、イベントが1087223700秒で発生したことを示しています。  |
| 10  | この行は、イベントに関連付けられている影響レベルが1(赤、脆弱)であることを示しています。   |
| 11  | この行は、違反イベントに関連付けられているIPアドレスが172.16.1.22であることを示しています。  |
| 12  | この行は、違反に関連付けられている宛先IPアドレスがないことを示しています(値は0に設定)。  |
| 13  | この行は、文字列ブロックの長さとテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は影響名です。文字列ブロックの詳細については、 <a href="#">文字列データブロック(3-64ページ)</a> を参照してください。                                |
| 14  | この行は、文字列ブロックインジケータを含めた文字列ブロックのトータル長が18バイトであることを示しています。これには、影響の説明の10バイトと文字列ヘッダーの8バイトが含まれています。  |
| 15  | この行は、影響の説明が「Vulnerable(脆弱)」であることを示しています。  |



## パケット レコードの例

次の図に、パケット レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    | 2  |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  |    |
| 5   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  |
| 7   | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  |    |
| 8   | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  |    |
| 9   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  |
| 10  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  |
| 11  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  |
| 12  | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  |

上記の例では、次のパケット情報を確認できます。

| ケース | 説明  |
|-----|---|
| 1   | この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(メッセージタイプ 4)であることを示しています。  |
| 2   | この行は、後続のメッセージの長さが 989 バイトであることを示しています。  |
| 3   | この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 2 を示し、パケット レコードを表します。 |
| 4   | この行は、後続のパケット レコードの長さが 981 バイトであることを示しています。  |
| 5   | この行は、イベントがデバイス番号 3 から収集されることを示しています。  |
| 6   | この行は、イベント ID 番号が 195430 であることを示しています。   |
| 7   | この行は、イベントが 10572378 秒で発生したことを示しています。  |

| ケース | 説明   |
|-----|--|
| 8   | この行は、パケットが 10572380 秒で収集されたことを示しています。                                    |
| 9   | この行は、パケットが 254365 マイクロ秒で収集されたことを示しています。                                  |
| 10  | この行は、リンク タイプが 1(イーサネット層)であることを示しています。                                    |
| 11  | この行は、後続のパケット データの長さが 953 バイトであることを示しています。                                |
| 12  | この行と次の行は、実際のペイロード データを示します。実際のデータは 953 バイトであり、この例では切り捨てられていることに注意してください。 |

## 分類レコードの例

次の図に、分類レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0  |
| 5   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  |
| 7   | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  |
|     | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  |
|     | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 1  |
|     | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  |
|     | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  |
|     | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  |
|     | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  |
|     | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  |

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|
| ビット | 0 | 1 | 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 |   |   |   |
| 8   | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0 | 0 | 0 |
|     | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0 | 1 | 0 |
|     | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1 | 0 | 0 |
|     | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
| 9   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |

上記の例では、次のイベント情報を確認できます。

| ケース | 説明   |
|-----|--|
| 1   | 行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(メッセージ タイプ 4)であることを示しています。  |
| 2   | この行は、後続のメッセージの長さが 92 バイトであることを示しています。  |
| 3   | この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 67 を示し、分類レコードを表します。              |
| 4   | この行は、後続の分類レコードの長さが 84 バイトであることを示しています。   |
| 5   | この行は、分類 ID が 35 であることを示しています。  |
| 6   | この行の最初の 2 バイトは、後続の分類名の長さが 15 バイトであることを示しています。2 番目の 2 バイトは、分類名自体で始まり、この場合は「trojan-activity (トロイの木馬アクティビティ)」です。  |
| 7   | この行の先頭バイトは、行 6 で説明している分類名の続きです。この行の最初の 2 バイトは、後続の説明の長さが 29 バイトであることを示しています。残りのバイトは、分類の説明で始まり、この場合は「A Network Trojan was Detected. (ネットワークでトロイの木馬が検出されました。)」です。 |
| 8   | この行は、分類の一意の ID としての役割を果たす分類 ID 番号を示します。  |
| 9   | この行は、分類のリビジョンの一意の ID としての役割を果たす分類リビジョン ID 番号を示し、この場合、分類のリビジョンがないため、Null です。  |

## 優先度レコードの例

次に、優先度レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|
| ビット | 0 | 1 | 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 |   |   |   |   |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1 | 0 | 0 |   |   |   |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | 0 | 0 |   |   |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1 | 0 | 0 |   |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1 | 0 | 0 | 0 |
| 5   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 1 |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1 |   |   |   |   |   |
|     | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1  | 0  | 1  | 0  | 0  | 0  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |   |   |   |   |   |

上記の例では、次のイベント情報を確認できます。

| ケース | 説明   |
|-----|--|
| 1   | この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(メッセージ タイプ 4)であることを示しています。      |
| 2   | この行は、後続のメッセージが 16 バイトであることを示しています。   |
| 3   | この行は、レコード タイプの値 4 を示し、優先度レコードを表します。  |
| 4   | この行は、後続の優先度レコードの長さが 8 バイトであることを示しています。   |
| 5   | この行は、優先度 ID が 1 であることを示しています。  |
| 6   | この行の最初の 2 バイトは、優先度名に 4 バイトが含まれていることを示しています。2 番目の 2 バイトと次の行の 2 バイトは、優先度名自体(「high(高)」)を示しています。 |

## ルール メッセージ レコードの例

次に、ルール メッセージ レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|
| ビット | 0 | 1 | 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 |   |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1 | 0 | 0 |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1 |

| バイト       | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |   |   |   |
|-----------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|
|           | 0 | 1 | 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 |   |   |   |   |   |   |   |   |   |
| <b>3</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0 |   |   |   |   |   |   |   |   |
| <b>4</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1 |   |   |   |   |   |   |   |   |
| <b>5</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1 |   |   |   |   |   |   |   |   |
| <b>6</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 0 | 1 |   |   |   |   |   |   |   |
| <b>7</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 1 |   |   |   |   |   |   |   |
| <b>8</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 0 | 1 |   |   |   |   |   |   |   |
| <b>9</b>  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1 |   |   |   |   |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1 |   |   |   |   |   |   |   |   |
|           | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0 | 1 |   |   |   |   |   |   |   |
|           | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1 | 1 |   |   |   |   |   |   |   |
| <b>10</b> | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1 |   |   |   |   |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1 |   |   |   |   |   |   |   |   |
|           | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0 | 1 |   |   |   |   |   |   |   |
|           | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1 | 1 |   |   |   |   |   |   |   |
| <b>11</b> | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0 |   |   |   |   |   |   |   |   |
|           | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 0 | 1 |   |   |   |   |   |   |   |
|           | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0 | 0 |   |   |   |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1 |   |   |   |   |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0 | 0 | 1 |   |   |   |   |   |   |
|           | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 0 | 1 | 0 | 0 |   |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0 | 0 | 1 | 0 | 0 |   |   |   |   |
|           | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0 | 1 | 0 | 0 | 1 |   |   |   |   |
|           | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 1 | 0 | 1 | 0 | 1 |   |   |   |   |
|           | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1 | 0 | 1 | 1 | 0 | 1 |   |   |   |
|           | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
|           | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |   |

## ■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |  |  |  |  |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|--|--|--|
| ビット | 0 | 1 | 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 |  |  |  |  |
|     | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  |  |  |  |  |
|     | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  |  |  |  |  |
|     | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  |    |  |  |  |  |
|     | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  |    |  |  |  |  |
|     | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  |    |  |  |  |  |
|     | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  |    |  |  |  |  |
|     | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |

上記の例では、次のイベント情報を確認できます。

| ケース | 説明  |
|-----|---|
| 1   | この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。   |
| 2   | この行は、後続のメッセージが 129 バイトであることを示しています。   |
| 3   | この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 66 を示し、ルール メッセージ レコードを表します。   |
| 4   | この行は、後続のルール メッセージ レコードの長さが 121 バイトであることを示しています。   |
| 5   | この行は、ジェネレータ ID 番号が 1(ルール エンジン)であることを示しています。   |
| 6   | この行は、ルール ID 番号が 28069 であることを示しています。   |
| 7   | この行は、ルールのリビジョン番号が 1 であることを示しています。   |
| 8   | この行は、Cisco Secure Firewall システム に渡されたルール ID 番号が 28069 であることを示しています。   |
| 9   | この行の最初の 2 バイトは、ルール テキスト名に 71 バイトが含まれていることを示しています。2 番目の 2 バイトは、ルールの一意の ID 番号で始まります。  |
| 10  | この行の最初の 2 バイトは、ルールの一意の ID 番号で終わります。次の 2 バイトは、ルールのリビジョンの一意の ID 番号で始まります。   |
| 11  | この行の最初の 2 バイトは、ルールのリビジョンの一意の ID 番号で終わります。2 番目の 2 バイトは、ルール メッセージ自体のテキストで始まります。送信されたルール メッセージのフルテキストは「APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn(domain 360.cn に対する潜在的なマルウェア SafeGuard に関する APP-DETECT DNS 要求)」です。 |

### 6.1.x の接続統計データ ブロックの例

次の図に、接続統計レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|
|     | 0 | 1 | 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 |   |   |   |   |   |   |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0 |   |   |   |   |   |   |   |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1 | 0 | 0 |   |   |   |   |   |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0 | 0 | 1 | 1 | 1 |   |   |   |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1 | 1 | 1 | 0 | 0 |   |   |   |
| 5   | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1 | 0 | 1 | 0 | 0 |   |   |   |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 |   |   |   |
| 7   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 1 |   |   |
| 8   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 9   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 10  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 11  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 12  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 13  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |   |   |
| 14  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 1 |   |
| 15  | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0 | 1 | 1 | 1 | 1 | 1 |   |   |
| 16  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |
| 17  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |
| 18  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |
| 19  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |
| 20  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|
| ビット | 0 | 1 | 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 |   |   |   |
| 21  | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0 |   |   |
|     | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0 |   |   |
|     | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1 |   |   |
|     | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  |   |   |   |
| 22  | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
|     | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0 |   |   |
|     | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0 | 0 |   |
|     | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | 0 |
| 23  | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  |   |   |   |
|     | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0 |   |   |
|     | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1 |   |   |
|     | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 0 |   |   |
| 24  | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0  |    |   |   |   |
|     | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0 |   |   |
|     | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0 | 0 |   |
|     | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | 0 |
| 25  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1 |   |   |
|     | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1 | 0 | 1 |
| 26  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |   |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1 | 1 |   |
|     | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0 |   |   |
| 27  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |   |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 |



| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 28  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 1  |    |
| 29  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 1  |    |
| 30  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 31  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 32  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  |    |    |
| 33  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 34  | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 35  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  |    |
| 36  | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  |    |
| 37  | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  |    |
| 38  | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 39  | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 40  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  |    |
| 41  | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |

■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|     | 0 | 1 | 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 |
| 54  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 43  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 44  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 45  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 46  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 47  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 48  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 49  | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 50  | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 51  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 52  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 53  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 54  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 55  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 72  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 57  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 58  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 59  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 60  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

| バイト | 0 |   |   |   |   |   |   | 1 |   |   |    |    |    |    | 2  |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|     | 0 | 1 | 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 |
| 61  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 62  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 63  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 64  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 65  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 66  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 67  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 68  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  |
| 69  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 70  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 71  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 72  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 73  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 74  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 75  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 76  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 77  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 78  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 79  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 80  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 81  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 82  | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

■ 侵入イベントのデータ構造の例

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 83  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 84  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 85  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 86  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 87  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 88  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 89  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 90  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 91  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 92  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 93  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
| 94  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |    |

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット | 0 | 1 | 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 |
| 95  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 96  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 0  |
|     | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  |
|     | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  |
| 97  | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 1  |
| 98  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 99  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 100 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 101 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 102 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 103 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  |
| 104 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 105 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 106 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

## ■ 侵入イベントのデータ構造の例

|     |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
| ビット | 0 | 1 | 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 |
| 107 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

上記の例では、次のイベント情報を確認できます。

| ケース | 説明   |
|-----|--|
| 1   | この行の最初の2バイトは、標準ヘッダー値1を示しています。2番目の2バイトは、メッセージがデータメッセージ(つまり、メッセージタイプ4)であることを示しています。  |
| 2   | この行は、後続のメッセージの長さが716バイトであることを示しています。   |
| 3   | この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の15ビットは、イベントが検出されたドメインのNetmap IDを含むオプションフィールドです。行の残りの部分は、レコードタイプの値71を示し、接続統計レコードを表します。 |
| 4   | この行は、後続のイベントレコードの長さが700バイトであることを示しています。  |
| 5   | この行は、イベントの保存時のタイムスタンプです。この場合、2016年10月10日(月)の午前8時48分52秒に保存されています。   |
| 6   | この行は、将来使用するために予約されており、ゼロが入っています。   |
| 7   | この行は、ディスカバリ イベントを生成したデバイスのID番号を指定しています。デバイスIDは1です。   |
| 8   | この行は、レガシーIP(IPv4)アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4アドレスはIPv6フィールドに保存されます。  |
| 9   | この行には、イベントに関連するホストのMACアドレスが含まれます。MACアドレスは00:00:00:00:00:00です。  |
| 10  | この行の最初の16ビットには、MACアドレスの残りの部分が含まれます。次の8ビットでは、ホストがIPv6アドレスであるかどうかを示すフラグです。最後の8ビットは空白です。これは将来の使用に備えて予約されています。                                 |
| 11  | この行には、イベントが発生した時刻のUNIXタイムスタンプが含まれます。   |
| 12  | この行には、イベントマイクロ秒が含まれます。この場合は、0です。   |
| 13  | この行には、イベントタイプが含まれます。この場合、タイプは1003です。   |
| 14  | この行には、イベントサブタイプが含まれます。この場合、イベントサブタイプは1です。これは、イベントタイプ1003とともに、これが接続統計イベントであることを意味します。   |
| 15  | この行はファイル番号に使用されます。これは内部専用です。   |
| 16  | この行はファイルの位置に使用されます。これは内部専用です。  |
| 17  | この行には、IPv6アドレスが含まれます。このフィールドは、IPv6フラグが設定されている場合に存在し、使用されます。この場合、IPv6アドレス0:3eb:0:1:d184:fb57:8ba:c00が含まれています。                               |
| 18  | この行には、ブロックタイプが含まれます。値は163です。これは、接続統計データブロックタイプを示しています。   |

| ケース | 説明   |
|-----|--|
| 19  | この行には、データ ブロックの長さが含まれ、644 バイトのデータが含まれていることを示しています。   |
| 20  | この行は、ディスクバリエーション イベントを生成したデバイスの ID 番号を指定しています。デバイス ID は 1 です。  |
| 21  | 入力セキュリティ ゾーンが含まれます。ゾーンは 59e4505c-4493-11e6-a62d-f1dff731a85 です。  |
| 22  | 出力セキュリティ ゾーンが含まれます。ゾーンは 60d50c80-4493-11e6-9843-84d8d6a3e008 です。   |
| 23  | 入力インターフェイスが含まれます。インターフェイスは 599126de-4493-11e6-a62d-f1dff731a85e です。  |
| 24  | 出力インターフェイスが含まれます。インターフェイスは 608d6cf4-4493-11e6-9843-84d8d6a3e008 です。  |
| 25  | この行には、接続イベントで示されているセッションを開始したホストの IP アドレスが含まれます。IP アドレスは 172.16.3.5 です。  |
| 26  | この行には、開始ホストに応答したホストの IP アドレスが含まれます。IP アドレスは 72.48.149.244 です。  |
| 27  | 要求の送信元であるプロキシの背後にあるホストの IP アドレス。この例では、これは空白です。   |
| 28  | この行には、トリガーされた関連イベントに関連付けられたルールのリビジョン番号が含まれます。リビジョン番号は 00000000-0000-0000-0000-000057e9c39d です。   |
| 29  | イベントをトリガーしたルールの内部識別子が含まれます。このルールは、268439603 です。  |
| 30  | この行には、イベントをトリガーしたトンネル ルールの内部識別子が含まれます。このイベントはトンネル ルールでトリガーされなかったため、値は 0 です。  |
| 31  | この行の最初の 2 バイトには、ルールで指定されたアクションが含まれます。この場合、値は 4 で、アクションがブロックであったことを示しています。最後の 2 バイトにはルールの理由が含まれます。この場合、64 で、侵入ブロックを意味します。   |
| 32  | 最初の 2 バイトには、ルールの理由の残りが含まれます。次の 2 バイトには、イニシエータ ホストで使用されたポートが含まれます(43786)。   |
| 33  | この行の最初の 2 バイトには、レスポンド ポートが含まれます(443)。残りの 2 バイトには、TCP フラグが含まれます。  |
| 34  | この行の最初のバイトには、プロトコルが含まれます(6)。これは、このイベントが TCP を介して発生したことを示します。残りの 24 バイトには、Netflow ソースの IP アドレスの最初の部分が含まれます(00000000-0000-0000-0000-000000000000)。                 |
| 35  | この行の最初のバイトには、Netflow ソースの最後の 8 ビットが含まれます。次の 2 バイトには、イベントを生成した Snort のインスタンスの識別子が含まれます(7)。残りのバイトには、接続数カウンタが含まれます。   |
| 36  | この行の最初のバイトには、接続数カウンタの残りの部分が含まれます。最後の 24 ビットには、セッションで交換された最初のパケットの UNIX タイムスタンプの先頭が含まれます。このタイムスタンプは 1476103731 です。これは、2016 年 10 月 10 日(月)午前 8 時 48 分 51 秒を示しています。 |

| ケース | 説明   |
|-----|--|
| 37  | 最初のバイトには、最初のパケットのタイムスタンプの残りの部分が含まれます。残りの 3 バイトは、セッションで交換される最後のパケットのタイムスタンプが含まれています。このタイムスタンプも 2016 年 10 月 10 日(月)午前 8 時 48 分 51 秒を示し、セッションが 1 秒未満で終了したことを示しています。 |
| 38  | この行の最初のバイトには、最終パケットタイムスタンプの最後の 8 ビットが含まれます。残りの 24 ビットには、開始ホストから送信されたパケット数が含まれます。この場合は 13 です。   |
| 39  | この行の最初のバイトは、イニシエータ送信パケット数の残りの部分です。次の 24 ビットには、レスポンドから送信されたパケット数が含まれます(o)。  |
| 40  | この行の最初のバイトは、レスポンド送信パケット数の残りの部分です。次の 24 ビットには、イニシエータから送信されたバイト数が含まれます(1743)。  |
| 41  | 最初のバイトはイニシエータ送信バイトの最終バイトで、残りの 24 ビットでレスポンド送信バイトが開始します(o)。  |
| 54  | 最初のバイトはレスポンド送信バイトの最終バイトで、残りの 24 ビットでイニシエータ パケット ドロップが開始します(o)。   |
| 43  | 最初のバイトはイニシエータ パケット ドロップの最後で、残りの 24 ビットでレスポンド パケット ドロップが開始します(o)。   |
| 44  | 最初のバイトはレスポンド パケット ドロップの最後で、残りの 24 ビットでイニシエータ バイト ドロップが開始します(o)。  |
| 45  | 最初のバイトはイニシエータ バイト ドロップの最後で、残りの 24 ビットでレスポンド バイト ドロップが開始します(o)。   |
| 46  | 最初のバイトはレスポンド バイト ドロップの最後で、残りの 24 ビットでレート制限が適用されたインターフェイスの名前が開始します(00000000-0000-0000-0000-000000000000)。   |
| 47  | この行の最初のバイトは、QOS 適用インターフェイスの残りの部分です。残りの部分は、接続に適用された QOS ルールです。このインターフェイスには QOS ルールが適用されていないため、ID は 0 です。  |
| 48  | この行の最初のバイトは、QOS ルール ID の残りの部分です。残りの部分は、トラフィックを生成したホストに最後にログインしたユーザーの ID 番号です(16466)。   |
| 49  | この行の最初のバイトは、ユーザー ID の残りの部分です。残りの部分は、接続で使用されたアプリケーション プロトコルです。1122 は HTTPS 接続であることを示しています。  |
| 50  | この行の最初のバイトは、アプリケーション プロトコル ID の残りの部分です。残りは、URL カテゴリです。   |
| 51  | この行の最初のバイトは、URL カテゴリの残りの部分です。残りは、URL レピュテーションです。0 は、「リスク不明」を意味します。   |
| 52  | この行の最初のバイトは、URL レピュテーションの残りの部分です。残りは、クライアント アプリケーション ID です。1296 は、「SSL クライアント」を意味します。  |
| 53  | この行の最初のバイトは、クライアント アプリケーション ID の残りの部分です。残りは、Web アプリケーション ID です。0 は、「不明」を意味します。   |
| 54  | この行の最初のバイトは、Web アプリケーション ID の残りの部分です。この行の残りの部分では、ブロック タイプが開始します。0 は、文字列ブロック タイプの先頭を示します。   |



| ケース | 説明  |
|-----|---|
| 55  | この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、クライアントアプリケーション URL に、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、クライアントアプリケーション URL にデータが存在しないことを意味します。                                  |
| 72  | この行の最初のバイトは、文字列ブロック長の残りの部分です。クライアントアプリケーション URL にはデータが存在しないため、この行の残りはブロックタイプ 0 で開始しています。これは、NetBIOS 名の文字列ブロック タイプの先頭を示しています。  |
| 57  | この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、NetBIOS 名に、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、NetBIOS 名にデータが存在しないことを意味します。  |
| 58  | この行の最初のバイトは、文字列ブロック長の残りの部分です。NetBIOS 名にはデータが存在しないため、この行の残りはブロックタイプ 0 で開始しています。これは、クライアントアプリケーションバージョンの文字列ブロック タイプの先頭を示しています。  |
| 59  | この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、クライアントアプリケーションバージョンに、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、クライアントアプリケーションバージョンにデータが存在しないことを意味します。                                  |
| 60  | この行には、クライアントアプリケーションバージョンブロック長の残りのバイトが含まれます。最後の 3 バイトは、接続イベントに関連付けられている 1 番目のモニター ルールの ID です(268439553)。  |
| 61  | この行には、1 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、2 番目のモニター ルールの ID です(o)。  |
| 62  | この行には、2 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、3 番目のモニター ルールの ID です(o)。  |
| 63  | この行には、3 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、4 番目のモニター ルールの ID です(o)。  |
| 64  | この行には、4 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、5 番目のモニター ルールの ID です(o)。  |
| 65  | この行には、6 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、7 番目のモニター ルールの ID です(o)。  |
| 66  | この行には、7 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、8 番目のモニター ルールの ID です(o)。  |
| 67  | この行には、8 番目のモニター ルールの ID の最終バイトが含まれています。この行の 2 番目のバイトは、送信元または宛先の IP アドレスが IP ブロックリストと一致しているかどうかを示しています。この行の 3 番目のバイトは、IP ブロックリストに一致した IP 層です。最後のバイトで、ファイル イベントカウントが開始します(o)。 |
| 68  | この行の最初のバイトは、ファイル イベントカウントの残りの部分です。次の 2 バイトには、侵入イベントカウントが含まれています。最後のバイトには、イニシエータの国が含まれます。この場合は 0 で、「不明」を意味します。   |
| 69  | この行の最初のバイトは、イニシエータの国の第 2 バイトです。次の 2 バイトは、レスポндаの国です(840)。最後のバイトで、クライアントのオリジナル国が開始します。この場合は 0 で、「不明」を意味します。  |

| ケース | 説明  |
|-----|---|
| 70  | この行の最初のバイトは、クライアントのオリジナル国の最後です。次の 2 バイトは、IOC 番号です (o)。最後のバイトは、送信元自律システムの先頭バイトです (o)。  |
| 71  | この行の最初の 3 バイトは、送信元自律システムです。最後のバイトは、宛先自律システムの先頭バイトです (o)。  |
| 72  | この行の最初の 3 バイトは、宛先自律システムです。最後のバイトは、入力インターフェイスの SNMP インデックスです (o)。  |
| 73  | この行の最初のバイトは、入力インターフェイスの SNMP インデックスです。次の 2 バイトは、出力インターフェイスの SNMP インデックスです (o)。この行の最後のバイトは、着信インターフェイス用のタイプ オブ サービス設定です (o)。  |
| 74  | この行の最初のバイトは、発信インターフェイス用のタイプ オブ サービス設定です (o)。2 番目のバイトは、送信元マスクです (o)。3 番目のバイトは、宛先マスクです (o)。最後のバイトは、トラフィックが通過したセキュリティ コンテキストの ID 番号の先頭です。この場合、セキュリティ コンテキストは 00000000: 0000: 0000: 0000-0000000000000000 です。 |
| 75  | この行の最初の 3 バイトは、セキュリティ コンテキストの残りの部分です。最後のバイトは VLAN ID です (o)。  |
| 76  | 最初のバイトは VLAN ID です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、参照ホストの名前が含まれています。   |
| 77  | 最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、参照ホストがないため文字列ブロックにはデータが存在しないことを意味します。  |
| 78  | 最初のバイトは、文字列ブロック長の残りの部分です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、ユーザー エージェントが含まれます。  |
| 79  | 最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、ユーザー エージェントがないため文字列ブロックにはデータが存在しないことを意味します。  |
| 80  | 最初のバイトは、文字列ブロック長の残りの部分です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、HTTP リファラが含まれます。  |
| 81  | 最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、HTTP リファラがないため文字列ブロックにはデータが存在しないことを意味します。  |
| 82  | この行の最初のバイトには、文字列ブロック長の最後が含まれます。最後の 3 バイトには、SSL 証明書のフィンガープリントが含まれます (000000000000000000000000)。  |
| 83  | この行の最初のバイトには、SSL 証明書のフィンガープリント ID の最後が含まれます。この行の残りの部分には、SSL ポリシー ID が含まれます (00000000-0000-0000-0000-000000000000)。  |
| 84  | この行の最初のバイトは、SSL ポリシー ID の最後です。最後の 3 バイトは、SSL ルール ID です (o)。   |

| ケース | 説明  |
|-----|---|
| 85  | この行の最初のバイトは、SSL ルール ID の残りの部分です。次の 2 バイトは、SSL 暗号スイートです。o は、TLS_NULL_WITH_NULL_NULL を意味します。最後のバイトは、SSL バージョンです(o)。                                 |
| 86  | この行には SSL サーバー証明書ステータスが含まれます。o は、未チェック を意味します。  |
| 87  | この行の最初の 2 バイトは、実際の SSL アクションです。o は、不明 を意味します。次の 2 バイトは、予想された SSL アクションです。o は、不明を意味します。  |
| 88  | この行の最初の 2 バイトは、SSL フロー ステータスです。o は、不明 を意味します。次の 2 バイトは、SSL フロー エラーです。o は、不明を意味します。  |
| 89  | この行の最初の 2 バイトは、SSL フロー エラーの残りの部分です。次の 2 バイトは、SSL フロー メッセージです(o)。  |
| 90  | この行の最初の 2 バイトは、SSL フロー メッセージです。次の 2 バイトは、SSL フロー フラグです(o)。  |
| 91  | この行の最初の 2 バイトは、SSL フロー フラグの残りの部分です。次の 2 バイトで、SSL サーバー名の文字列ブロックが開始します(タイプ o)。  |
| 92  | この行の最初の 2 バイトで、文字列ブロック タイプが終了します。次の 2 バイトには、文字列ブロック長が含まれます。ブロック長は 8 です。これには、ブロックのタイプと長さが含まれ、文字列ブロックにデータが含まれていないことを意味します。                          |
| 93  | 最初の 2 バイトには、文字列ブロック長の残りが含まれます。次の 2 バイトには、SSL URL カテゴリが含まれます。o は、不明を意味します。   |
| 94  | この行の最初の 2 バイトには、SSL URL カテゴリの残りの部分が含まれます。次の 2 バイトで、SSL セッション ID が開始します(00000000000000000000000000000000)。   |
| 95  | この行の最初のバイトには、SSL セッション ID の最後が含まれます。次のバイトには、SSL セッション ID の長さが含まれます(o)。次の 2 バイトで、SSL チケット ID が開始します(00000000000000000000)。                         |
| 96  | この行の最初の 2 バイトには、SSL チケット ID の最後が含まれます。3 番目のバイトには、SSL チケット ID の長さが含まれます(o)。最後のバイトで、ネットワーク分析ポリシー リビジョンが開始します(4e78cb70-7842-11e6-a99b-cdb19cb553fd)。 |
| 97  | この行の最初の 3 バイトには、ネットワーク分析ポリシー リビジョンの最後が含まれます。最後のバイトで、エンドポイント プロファイル ID が開始します(o)。  |
| 98  | この行の最初の 3 バイトは、エンドポイント プロファイル ID です。残りのバイトで、セキュリティ グループ ID が開始します(o)。   |
| 99  | この行の最初の 3 バイトは、セキュリティ グループ ID です。残りのバイトで、ロケーション IPv6 が開始します。これは、ISE と通信するインターフェイスの IP アドレスで、空白です。   |
| 100 | この回線の最初の 3 バイトは、ロケーション IPv6 の最後です。残りのバイトで、HTTP レスポンスが開始します。o は HTTP レスポンスがないことを意味します。   |
| 101 | この回線の最初の 3 バイトは、HTTP レスポンスの最後です。残りのバイトで、文字列ブロックが開始します。タイプ o は DNS クエリです。  |
| 102 | 最初の 3 バイトで、文字列ブロック タイプが完了します。残りのバイトには、ブロックのタイプと長さを含む文字列ブロック長が含まれます。8 バイトは、DNS クエリにデータが存在しないことを意味します。  |
| 103 | 最初の 3 バイトで、文字列ブロック長が終了します。この行の残りのバイトで、DNS レコード タイプが開始します(71)。   |

| ケース | 説明   |
|-----|--|
| 104 | この行の最初のバイトで、DNS レコードタイプが終了します。次の2バイトは、DNS レスポンス タイプです(o)。最後のバイトで、DNS TTL が開始します。           |
| 105 | この行の最初の3バイトは、DNS TTL です。最後のバイトで、シンクホール UUID が開始します( 00000000-0000-0000-0000-000000000000)。 |
| 106 | この行の最初の3バイトで、シンクホール UUID が終了します。最後のバイトで、最初のセキュリティ インテリジェンス リストが開始します(o)。                   |
| 107 | この行の最初の3バイトで、最初のセキュリティ インテリジェンス リストが終了します。最後のバイトで、2番目のセキュリティ インテリジェンス リストが開始します(o)。        |

## バージョン 5.1+ ユーザー イベントの例

次の図に、ユーザー イベント レコードの例を示します。

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|
|     | 0 | 1 | 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 |   |   |   |   |   |   |
| 1   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 |   |   |   |   |
| 2   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 1 | 1 | 0 | 0 | 1 |   |
| 3   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1 | 1 | 1 | 1 |   |   |
| 4   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0 | 1 | 0 | 0 | 1 |   |
| 5   | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 1  | 0  | 0 | 1 |   |   |   |   |
| 6   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 |   |   |
| 7   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 1 | 1 |   |
| 8   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 |   |
| 9   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 |   |
| 10  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 |   |   |
| 11  | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0 | 0 | 1 | 1 |   |   |
| 12  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1 | 1 | 1 | 1 |   |   |
| 13  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1 | 0 | 0 | 0 |   |   |
| 14  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 1 | 0 |
| 15  | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 1  | 0  | 0 | 1 | 0 | 0 |   |   |
| 16  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 |

| バイト | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|
| ビット | 0 | 1 | 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 |   |   |
| 17  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 18  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 19  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 20  | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  |    |   |   |
| 21  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 22  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 23  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |   |   |
| 24  | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0 | 1 |
| 25  | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0 |   |
| 26  | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0 | 1 |
| 27  | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0 | 1 |
| 28  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 29  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 30  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 31  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
|     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |   |

上記の例では、次の情報を確認できます。

| 番号 | 説明   |
|----|--|
| 1  | この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージタイプ 4)であることを示しています。   |
| 2  | この行は、後続のメッセージの長さが 153 バイトであることを示しています。   |
| 3  | この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 95 を示し、ユーザー情報更新メッセージを表します。                            |
| 4  | この行は、後続のデータの長さが 137 バイトであることを示しています。   |
| 5  | この行には、アーカイブのタイムスタンプが含まれます。23 ビットが設定されたため、含まれています。タイムスタンプが UNIX タイムスタンプである場合は、1970 年 1 月 1 日以降の秒数として保存されます。このタイムスタンプは 1,391,789,354 であり、2014 年 2 月 3 日(月)の 19 時 43 分 49 秒を表しています。 |
| 6  | この行にはゼロが含まれており、将来使用するために予約されています。  |
| 7  | この行は、検出エンジン ID 番号が 3 であることを示しています。   |
| 8  | この行は、レガシー IP(IPv4)アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4 アドレスは IPv6 フィールドに保存されます。  |
| 9  | この行には、イベントに関連付けられている MAC アドレスが含まれます。MAC アドレスがないため、ゼロが含まれています。  |
| 10 | この行の前半は、MAC アドレスの残りの部分であり、ゼロです。次のバイトは、IPv6 アドレスが存在することを示しています。この行の最後のバイトは将来使用するために予約されており、ゼロが含まれています。  |
| 11 | この行には、システムがイベントを生成した時刻の UNIX タイムスタンプ(1970 年 1 月 1 日以降の秒数)が含まれます。   |
| 12 | この行には、システムがイベントを生成した時刻をマイクロ秒(100 万分の 1 秒)単位で表した値が含まれます。  |
| 13 | この行には、イベントタイプが含まれます。ユーザー変更メッセージを示す値 1004 が含まれています。   |
| 14 | この行には、イベントサブタイプが含まれます。ユーザー ログイン イベントを示す値 2 が含まれています。   |
| 15 | この行には、シリアルファイル番号が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。  |
| 16 | この行には、シリアルファイル内のイベントの位置が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。   |
| 17 | この行には、IPv6 アドレスが含まれます。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。ただし、この場合は IPv4 アドレス 10.4.15.120 が含まれています。   |
| 18 | この行は、ブロックタイプ 127 で示されるユーザー ログイン情報データブロックで始まります。  |
| 19 | この行は、後続のブロックの長さが 81 バイトであることを示しています。   |

| 番号 | 説明   |
|----|--|
| 20 | この行は、ユーザー ログインのタイムスタンプが 1,391,456,7 であることを示しています。これは、2014 年 10 月 3 日(月)の 19 時 43 分 47 秒(GMT)に生成されたことを意味します。  |
| 21 | この行は、レガシー IP(IPv4)アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4 アドレスは IPv6 フィールドに保存されます。  |
| 22 | この行は、文字列ブロックの長さでテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列はユーザー名です。文字列ブロックの詳細については、 <a href="#">文字列データ ブロック (3-64 ページ)</a> を参照してください。  |
| 23 | この行は、文字列ブロック内のデータの長さが 16 バイトであることを示しています。  |
| 24 | この行は、ユーザー名が「301@10.4.11.175」であることを示しています。  |
| 25 | この行は、ユーザーの ID 番号を示します。   |
| 26 | この行は、ログイン情報の取得元の接続で使用されているアプリケーションプロトコルのアプリケーション ID を示します。   |
| 27 | この行は、文字列ブロックの長さでテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は電子メールアドレスです。文字列ブロックの詳細については、 <a href="#">文字列データ ブロック (3-64 ページ)</a> を参照してください。  |
| 28 | この行は、文字列ブロック内のデータの長さが 0 バイトであることを示しています。なぜならば、このユーザーに関連付けられている電子メールアドレスがないためです。  |
| 29 | この行には、ユーザーのログインが検出されたホストの IP アドレスが含まれます。   |
| 30 | 先頭バイトには、ログイン タイプが含まれます。この行の残りの部分は、文字列ブロックの長さでテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は、ログインを報告した Active Directory サーバーの名前です。文字列ブロックの詳細については、 <a href="#">文字列データ ブロック (3-64 ページ)</a> を参照してください。 |
| 31 | この行の先頭バイトで、文字列データ ブロックの開始が完了します。この行の残りの部分は、文字列ブロック内のデータの長さが 0 バイトであることを示しています。なぜならば、このログインに関連付けられている Active Directory サーバーがないためです。   |

## ディスカバリ データ構造の例

このセクションでは、ディスカバリ イベントに関して eStreamer で送信されることがあるデータ構造の例を紹介します。ここでは、次の例を示します。

- [新しいネットワークング プロトコル メッセージの例 \(A-32 ページ\)](#)
- [新しい TCP サーバー メッセージの例 \(A-33 ページ\)](#)

## 新しいネットワーク プロトコル メッセージの例

次の図に、3.0+ の新しいネットワーク プロトコル メッセージの例を示します。

| バイト                                 | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |   |   |   |              |                         |  |
|-------------------------------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|--------------|-------------------------|--|
| ビット                                 | 0 | 1 | 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 |   |   |   |   |              |                         |  |
| ヘッダーバージョン 1                         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0 | イベント<br>メッセージ<br>(4)を含む標<br>準メッセー<br>ジヘッダー<br>の開始 |   |              |                         |  |
| メッセージ長<br>(49 バイト)                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0 | 0 | 1   |   |              |                         |  |
| 新しいネット<br>ワークプロ<br>トコルメッ<br>セージ(13) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1 | 0 | 1   |   |              |                         |  |
| メッセージ長<br>(41 バイト)                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0 | 0 | 0   |   |              |                         |  |
| 検出エンジン<br>ID(2)                     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1   | 0 |              |                         |  |
| IP<br>(192.168.1.1<br>0)            | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1 | 0 | 1   | 0 |              |                         |  |
| MAC アドレ<br>ス(なし)                    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0   | 0 | 予約バイト<br>(0) |                         |  |
| UNIX 秒<br>(1047242787)              | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 0 | 0 | 0   | 1 | 1            |                         |  |
| UNIX ミリ秒<br>(973208)                | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1 | 1 | 0   | 0 | 0            |                         |  |
| 予約バイト<br>(0)                        | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0 | 0 | 0   | 0 | 0            | イベントタ<br>イプ 1000—<br>新規 |  |
| イベントサ<br>ブタイプ 4—<br>新しい転送プ<br>ロトコル  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1   | 0 | 0            |                         |  |
| ファイル番号                              | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0 | 1 | 0   | 0 | 0            | 1                       |  |



| バイト           | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |  |  |  |  |  |
|---------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|--|--|--|--|
| ビット           | 0 | 1 | 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 |  |  |  |  |  |
| ファイルの位置       | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  |  |  |  |  |  |
| プロトコル (6—TCP) | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |

標準メッセージヘッダーの終了

## 新しいTCP サーバー メッセージの例

次の図に、3.0+ の新しい TCP サーバー メッセージの例を示します。

| バイト                  | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |
|----------------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ビット                  | 0 | 1 | 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 |
| ヘッダーバージョン1           | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  |
| メッセージ長 (256 バイト)     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 新しいTCPサーバーメッセージ (11) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  |
| メッセージ長 (248 バイト)     | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  |
| 検出エンジン ID(2)         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  |
| IP (192.168.1.10)    | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  |
| MAC アドレス(なし)         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| UNIX 秒 (1047242787)  | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1  | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  |
| UNIX ミリ秒 (973208)    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 0  | 0  | 0  |

予約バイト(0)

## ■ ディスカバリ データ構造の例

| バイト                                    | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    |    | 2  |    |    |    |    |    |    |    | 3  |    |    |    |    |    |    |    |   |                        |                        |  |
|--|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|------------------------|------------------------|--|
|  | 0 | 1 | 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 |   |                        |                        |  |
| 予約バイト<br>(0)                           | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0 | 0                      | イベントタイプ<br>1000—新規     |  |
| イベントサブ<br>タイプ2-<br>新しいホスト              | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 1                      | 0                      |  |
| ファイル番号                                 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1 |                        |                        |  |
| ファイルの<br>位置                            | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 標準メッセー<br>ジヘッダーの<br>終了 |                        |  |
| サーバーブ<br>ロックヘッ<br>ダー(12)               | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0 | 0                      | サーバーデー<br>タブロックの<br>開始 |  |
| サーバー長<br>(208バイト)                      | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 0 |                        |                        |  |
| サーバー<br>ポート(80)                        | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | ヒット                    |                        |  |
| ヒット(1)                                 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 文字列ブロッ<br>クヘッダー        |                        |  |
| 文字列ブロッ<br>クヘッダー<br>(0)                 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 文字列ブロッ<br>ク長           |                        |  |
| 文字列ブ<br>ロック長<br>(13バイト)                | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 1  | 0  | 1  | 0 | 0                      |                        |  |
| サーバー名<br>(https)                       | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 文字列ブロッ<br>クヘッダー        |                        |  |
| 文字列ブロッ<br>クヘッダー<br>(0)                 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 文字列ブロッ<br>ク長           |                        |  |
| 文字列ブ<br>ロック長<br>(15バイト)                | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 0  | 0  | 0 | 0                      | 1                      |  |
| サーバーベ<br>ンダー<br>(Apache +<br>Null バイト) | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 1  | 0  | 1  | 0  | 0 | 0                      |                        |  |
|  | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0                      | 文字列ブロッ<br>クヘッダー        |  |

| バイト                   | 0 |   |   |   |   |   |   |   | 1 |   |    |    |    |    |    | 2  |    |    |    |    |    |    | 3  |    |    |    |    |    |    |  |    |               |
|-----------------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|----|---------------|
|                       | 0 | 1 | 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            |
| 文字列ブロックヘッダー (0)       | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | 文字列ブロック長      |
| 文字列長(8-製品なし)          | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | 文字列ブロックヘッダー   |
| 文字列ブロックヘッダー (0)       | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | 文字列ブロック長      |
| 文字列ブロック長 (22 バイト)     | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | 文字列ブロック長      |
| バージョン - 1.3.26 (UNIX) | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | 文字列ブロック長      |
| リストブロックヘッダー (11)      | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーリストの開始  |
| リストブロックサイズ (94 バイト)   | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーリストの開始  |
| サブサーバーヘッダー (1)        | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーブロックの開始 |
| サブサーバー長 (46 バイト)      | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーブロックの開始 |
| 文字列ブロックヘッダー (0)       | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーブロックの開始 |
| 文字列長 (16 バイト)         | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーブロックの開始 |
| サブサーバー名 - mod_ssl     | 0 |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |    | サブサーバーブロックの開始 |





■ ディスカバリ データ構造の例

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。