HazardFilter アクセスログ形式

株式会社 YE DIGITAL

【 質問 】

出力されるアクセスログ(Hazard_http.log)の項目について詳細を教えてください。

【 回答 】

以下項目順に出力されます。

項目	説明
1.日付	リクエストされた日付(YYYY/MM/DD 形式)
2.時刻	記録した時刻(HH:MM:SS 形式)
3.プロトコル	使用したプロトコル(HTTP、HTTPS、FTP)
4.クライアントアドレス	クライアントの IP アドレス **※1**
5.グループ名	リクエスト元クライアントのグループ名(認証時) サブグループの区切りは「¥」
6.アカウント名	リクエスト元クライアントのユーザ名(認証時)
7.ブラウザバージョン	リクエスト元クライアントのブラウザバージョン
8.転送状態	リクエストの転送状態 **※3**
9.WWW サーバ IP	リクエスト先ホストの IP アドレス(Ver8.5 SP2 以降の ICAP 版では出力不可)
10.応答コード	レスポンスのステータスコード **※2**
11.WWW サーバ名	リクエスト先 Web サーバのホスト(FQDN)名
12.転送時間	転送に要した時間（単位：ミリ秒） **※2** （転送時間は上位サーバへのリクエスト送信～クライアントへの レスポンス送信の時間）
13.送信データサイズ	リクエスト時にクライアントから転送されたデータサイズ(単位：Byte)。 プロトコル別に、HTTP は HTTP ボディのサイズ、 HTTPS は HTTPS ヘッダとボディの合計サイズ、 FTP は FTP ヘッダとボディの合計サイズ
14.受信データサイズ	レスポンス時にクライアントに転送したデータサイズ(単位：Byte)。 プロトコル別に、HTTP は HTTP ボディのサイズ、 HTTPS は HTTPS ヘッダとボディの合計サイズ、 FTP は FTP ヘッダとボディの合計サイズ **※2**
15.ファイルタイプ	設定ファイル（mime_type.lst）で設定された MIME タイプ
16.コンテンツタイプ	HTTP ヘッダの Content-Type から取得した MIME タイプ **※2**
17.判定理由	**※4** 参照
18.判定カテゴリ	判定理由が「セキュリティ」「データベースマッチ」「優先カテゴリ」の 場合に、判定理由となったカテゴリを「メイン¥サブ」形式で出力する。 判定理由が優先カテゴリの場合は「,」（カンマ）区切りで出力。

	（例）カテゴリ 1 が「自動車」、カテゴリ 2 が「ブログ」で登録された URL の場合 例 1：「自動車」が許可で「ブログ」が規制の場合 →「ブログ」が出力される 例 2：「自動車」が規制で「ブログ」も規制の場合 →「ブログ」が出力される 例 3：「自動車」が規制で「ブログ」も規制で「自動車＆ブログ」が 優先許可の場合 →「自動車,ブログ」が出力される
19.カテゴリ 1	登録されているカテゴリ名
20.カテゴリ 2	1 つの URL に対して複数のカテゴリが登録されている場合、2 つ目の カテゴリ名。2 つ目のカテゴリない場合は、-（ハイフン）が出力されます。 複数のカテゴリが登録されている URL は下記例のように出力されます。 （出力例） 判定カテゴリ コミュニケーション¥SNS・ミニブログ カテゴリ 1 IT サービス¥IT カテゴリ 2 コミュニケーション¥SNS・ミニブログ
21.セキュリティカテゴリ	URL がセキュリティカテゴリに登録されている場合下記のカテゴリ名が 出力されます。 セキュリティ¥マルウェア セキュリティ¥DBD 攻撃
22.リクエスト URL	リクエストされた URL
23.HTTP バージョン	リクエストの HTTP バージョン
24.リクエストメソッド	リクエストされた HTTP メソッド
25.リンク元サイト	取得可能なリファラ URL

※1 リクエスト元 IP：proxy.inf にて[LOG_CFG]LOG_HNCONV=TRUE と設定している場合は、PC ホスト名が出力されます。

※2 ICAP 版では取得されないため、応答コードとコンテンツタイプは「-」、転送時間と受信データサイズは「0」が出力されます。

※3 転送状態

出力内容	説明
Proxied	URL データベースに登録がない(未分類に該当する)許可されたリクエスト、または、例外 URL 設定[許可カテゴリ]の登録と一致したリクエスト
Confirm	グループの適用ルールで規制されたリクエスト（一時解除ボタンあり）
Blocked	グループの適用ルールで規制されたリクエスト（一時解除ボタンなし）
Allowed	URL データベースに登録があり、グループのカテゴリルールで許可されたリクエスト
Release	一時解除機能によって転送したリクエスト
CfmPost	書き込み規制によって規制されたリクエスト（一時解除ボタンあり）
BlkPost	書き込み規制によって規制されたリクエスト（一時解除ボタンなし）

※４　判定理由として出力する内容と判定カテゴリ、登録カテゴリ

出力内容

出力内容	説明
データベース更新中	データベース更新中のリクエスト
ブラウザ規制	ブラウザ規制対象のリクエスト
HTTPS 規制	HTTPS 規制対象のリクエスト
ポート番号規制	ポート番号規制対象のリクエスト
IP アドレス規制	IP アドレス規制対象のリクエスト
検索キーワード規制¥XXX	検索キーワード規制対象のリクエスト (XXX は規制したキーワード)
マルチパートリクエスト規制	マルチパートリクエスト規制対象のリクエスト
書き込みキーワード規制¥XXX	書き込みキーワード規制対象のリクエスト (XXX は規制したキーワード)
一括書き込み規制	一括書き込み規制対象のリクエスト
セキュリティ	セキュリティカテゴリにマッチ
データベースマッチ	URL データーベースにマッチしたリクエスト
許可カテゴリ¥許可カテゴリ	「許可カテゴリ¥許可カテゴリ」対象のリクエスト
許可カテゴリ¥閲覧のみ許可	「許可カテゴリ¥許可カテゴリ」対象のリクエスト
優先カテゴリ	「優先カテゴリ」に判定されたリクエスト
未分類 URL	未分類 URL に該当したリクエスト