

【公開日】

2018年3月28日 (Rev.1)

【テンプレート名】

Digital Arts i-FILTER

【テンプレート概要】

デジタルアーツ製 Web フィルタリング製品「i-FILTER」シリーズに対応したマッピング定義です。

【テンプレート作成環境(バージョン)】

i-FILTER Ver.9

ALog EVA v7.3.2

※ALog ConVerterは株式会社網屋の登録商標です。

※記載された会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

※記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。

サンプルログ

Mar 11 09:00:00 7968 940/01/ - 192.23.22.160 - 1234 [11/Mar/2018:09:00:00 +0900] 302 1886 1848 all
ow -1 -1 125 -1 -1 %E4%B8%80…(省略)… -1 - "GET https://www.google.com/" - Mozilla%2F5.0 text%2Fh
tml%3B+charset%3DUTF-8 241FF631

i-FILTER アクセスログ

列 No	列名	値
1-3	アクセスログ出力時刻	Mar 11 09:00:00 未使用
-	(省略)	
7	クライアント IP アドレス	192.23.22.160
8	コンピューター名	-
9	認証ユーザー名	1234
10-11	アクセス開始日時	[11/Mar/2018:09:00:00 +0900]
12	HTTP レスポンスコード	302
-	(省略)	
15	フィルターアクション	allow
-	(省略)	
18	URL カテゴリリスト	125
-	(省略)	
25	リクエスト情報 (HTTP メソッド)	"GET https://www.google.com/"
26	リクエスト情報 (URL)	
-	(省略)	
29	HTTP User-Agent	Mozilla%2F5.0
30	HTTP Content-Type	text%2Fhtml%3B+charset%3DUTF-8
-	(省略)	

ALog EVA

列名	値
① 時刻	2018/03/11 09:00:00
② ユーザー	1234
③ サーバ	i-FILTER 固定値
④ 対象	https://www.google.com/
⑤ 操作	IFILTER_GET_ALLOW
⑥	ClientIP
⑦	ClientName
⑧	CategoryIDs
⑨	ContentType
⑩	ResponseCode
⑪	UserAgent

"IFILTER_" + #25 列
+ #15 列 (*1)
*1 … 全て大文字化

"-" の時は、空白文字に置換

[#30] 列を URL デコード化、さら
に ";" 以降の文字コードを削除

[#29] 列を URL デコード化

ALog ConVerter v7

[ホーム](#)
[検索](#)
[集計](#)
[監視](#)
[管理](#)
[管理者](#)

198 件中 1 - 100 件

☒ 折り返して全体を表示する

[PDF出力](#)
[CSV出力](#)

		時刻	ユーザー	サーバ	対象	操作	詳細
1	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	CONNECT api.onedrive.com:443 HTTP/1.1	IFILTER_CONNECT_BLOCK	CategoryIDs:43, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:503, UserAgent:Mozilla/5.0 (Windows NT X.X; WOW64; Trident/X.X; rv:X.X)"
2	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	www.google.com:443	IFILTER_CONNECT_ALLOW	CategoryIDs:-125, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:200, UserAgent:Mozilla/5.0 (Windows NT X.X; WOW64; Trident/X.X; rv:X.X)
3	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
4	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
5	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
6	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
7	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
8	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
9	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
10	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
11	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
12	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
13	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	www.google.com:443	IFILTER_CONNECT_ALLOW	CategoryIDs:-125, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:200, UserAgent:Mozilla/5.0 (Windows NT X.X; WOW64; Trident/X.X; rv:X.X)
14	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	www.google.com:443	IFILTER_CONNECT_ALLOW	CategoryIDs:-125, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:200, UserAgent:Mozilla/5.0 (Windows NT X.X; WOW64; Trident/X.X; rv:X.X)
15	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
16	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1
17	+	2018/03/01 11:00:00	AMIYA#1234	i-FILTER	https://www.google.com/image/abc/images/test.jpg	IFILTER_GET_ALLOW	CategoryIDs:-1, ClientIP:172.20.1.201, ContentType:*/*, Count:1, ResponseCode:302, UserAgent:Microsoft-CryptoAPI/1.1