

RTmetricsのプライバシー保護対応

～GDPRに対応した運用を構築するために～

プライバシー保護の世界的な潮流と関連法規について

2022年4月から、日本において改正個人情報保護法が施行されます。世界では、EUのGDPR(一般データ保護規則)や米国カリフォルニア州のCCPA(カリフォルニア州 消費者プライバシー法)が相次いで施行され、中国においてもほぼGDPRとほぼ同等の個人情報保護法が可決、2021年11月1日から施行されます。

多くの国で個人情報の定義に新たにIPアドレスやCookieが含まれるようになり、より厳罰化された罰則規定が設けられ、GDPRが適用されている欧州では、裁判で高額な賠償金を求める判決が現実化する中、個人のプライバシー保護とデータセキュリティに対する注目が急速に高まっています。日本においても、改正個人情報保護法の施行に合わせて、どのような運用を行うべきか、本格的な検討に着手する企業が急増しています。

RTmetricsでは、プライバシー保護関連の対応が必須な企業様に向け、個人情報を含まない匿名情報としてデータを保存し、アクセス解析を行うオプション機能を最新バージョン (v9.3.0) で追加しました。また、より厳格な運用構築を必要とする企業様に向け、指定したCookieに紐づくWebサイト上のアクセス履歴データをDB上から過去に遡って消去する機能をリリースいたします。(2021年10月リリース予定)

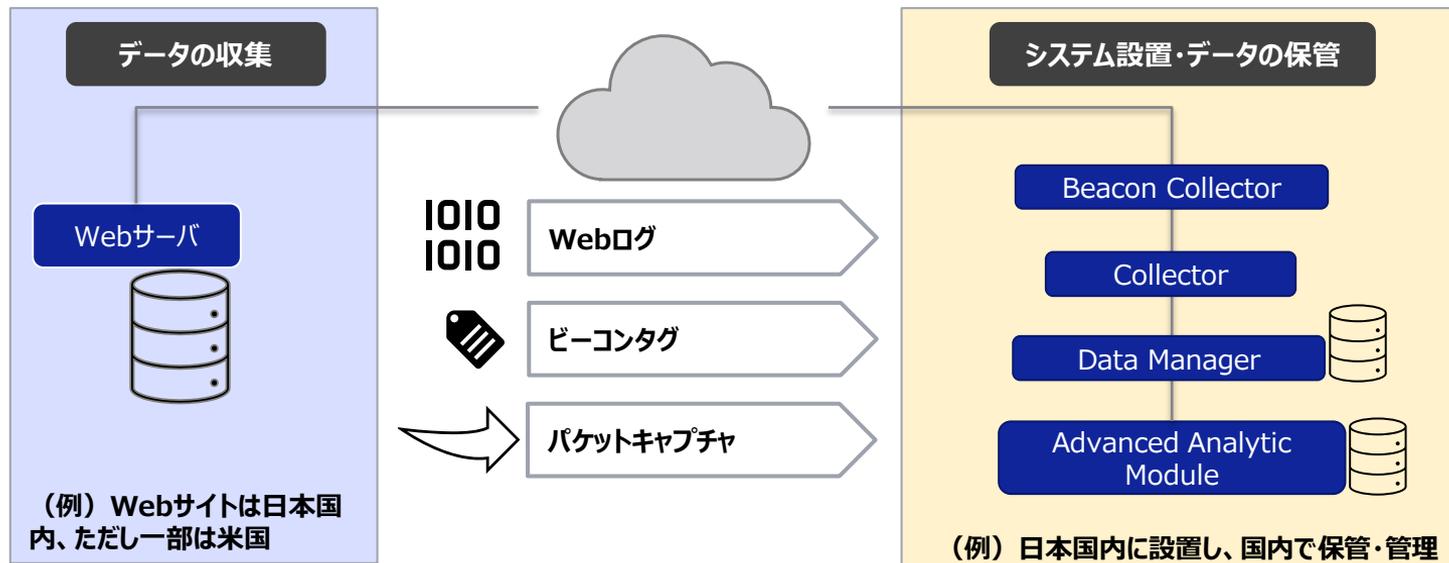
RTmetricsに従来から標準搭載されている機能と組み合わせてご利用頂くことで、ポリシーに沿ったデータを収集・管理し、法令を遵守しながら、企業の成長に不可欠なデータ活用に取り組んで頂けます。

はじめに：アクセス解析データの保管場所

現在、業務に広く浸透している無償・有償のSaaSの利用にあたり、見落されがちなのが、データの保管場所です。非公開なケースが多く、自社のデータが国内にあるのか、国外にあるのか、利用者側が把握されていないケースが数多く見受られます。

GDPR対応に際して、個人データ移転（EU圏内外、越境移転など）と合わせて論じられることが多いこの問題について、RTmetricsでは、ご利用際してまずシステムの設置場所、データの保管場所を自社で決めて頂くことを基本としています。

RTmetricsはソフトウェアとしてご提供しており、実機上でも、クラウド上でも問題なく動作し、ご利用頂くことができます。



対策レベルの検討①：CookieやIPアドレス

日本のユーザ向けにサービスを提供（日本の法令を遵守）、グローバルに事業を展開（関連各国の法令を遵守）など、自社が展開しているサービスや事業に合わせて、必要とされるプライバシー保護の対策レベルをご検討下さい。

RTmetricsでは、必要とされる対策レベルに対応した実装を標準機能でご提供できます。

※RTmetricsの機能を使った実装と取得したデータおよび運用について、法令遵守していることを保証するものではありません。法的な観点については、自社の法務部門や企業弁護士にご相談下さい。

1

Cookieレス

Cookieをデータベースに一切保存しない実装です。②の匿名化と併用することでIPアドレスもマスク化できます。アクセス解析の標準的な指標（PV、UU、SS等）は、通常どおりレポートします。

※UUをカウントしたい場合は、IP+UA等、Cookieではない値をカウントする設定を実装します。

利用機能
ビジタ、匿名化データとして取得

2

Cookie匿名化

CookieやIPアドレスを匿名化およびマスク化して保存する機能です。アクセス解析の標準的な指標（PV、UU、SS等）は、通常どおりレポートします。

利用機能
メンバー、匿名化データとして取得

3

オプトインされたCookieを保存

Webサイト側でCookieバナーツール等を用いて、Webサイトへの来訪者からCookie収集についてオプトインを明示的に取得し、匿名化せずにRTmetricsのデータベースに保存する実装です。後にデータ主体からデータ消去の依頼があった場合は、RTmetricsのデータ消去機能を利用し、履歴データから削除します。アクセス解析の標準的な指標（PV、UU、SS等）は、通常どおりレポートします。

※匿名化して保存した場合は、データ消去時のIDの指定を匿名化後の文字列で行います。（同一条件でハッシュ化）

利用機能
メンバー、指定したCookieデータの消去

対策レベルの検討②：URLやID等の文字列

Cookie以外にも個人情報に該当するデータを収集・記録していないか、確認を行います。ログインID、会員番号、サイトのURLの文字列やパラメータの一部、マイページ、購入完了時のトランザクションIDなどが、確認のポイントになります。

RTmetricsでは、データの対象を指定し、加工する機能（マッピング）が標準で搭載されています。例えば、個人情報に該当する文字列のみを切り出し、「記録しない」、「他の文字列に変換する」など、加工して保存する設定を行います。

※RTmetricsの機能を使った実装と取得したデータおよび運用について、法令遵守していることを保証するものではありません。法的な観点については、自社の法務部門や企業弁護士にご相談下さい。

1

ログインID・会員ID

ログインページで取得、Cookieの一部に文字列として含まれる、httpの拡張ヘッダに含まれる等、サイトの仕様により異なりますが、収集している場合は、個人情報に該当する可能性があります。

対策内容

マッピングによる削除、もしくは文字列の変換

2

サイトのURLの文字列・パラメータ

サイトのURLや動的に付与されるパラメータ内に個人情報に該当する文字列が含まれている場合があります。収集している場合は、個人情報に該当する可能性があります。

対策内容

マッピングによる削除、もしくは文字列の変換

3

マッピングを使用せずそのまま保存

RTmetricsのデータベース上に個人情報のまま保存する場合、後にデータ主体からデータ消去の依頼があった際は、データ消去機能を利用し、履歴データからの削除を実行します。Cookie値、URL内の文字列、ログインID等、いずれもRTmetricsの機能を用いて、文字列として記録していれば、後から指定し、削除することができます。

※一部2021年10月リリース予定の機能を含みます。

対策内容

マッピング、データの消去機能

RTmetricsでの具体的な実装

各種機能について

アクセス解析における個人情報について

アクセス解析の情報の中で、個人情報となりうるデータについて、ここで確認を行います。

IPアドレスは、RTmetricsでは設定に関わらずレポート対象の項目となっており、GDPRにおいては、IPアドレスやCookieなどのオンライン識別子は、「個人情報として識別されうるもの」として定義されています。RTmetricsの**初期状態では**、IPアドレスはそのままの値で保存されるため、GDPRの定義では、「個人情報として保存」されていることとなります。

下表のIPアドレス以外の項目は、RTmetricsでは明示的に設定で記録対象に指定する必要があります。アクセス解析を開始するにあたり、取得・レポート対象のデータに該当項目を含めたいか、含める場合はどのような形式で記録したいか（そのまま保存・匿名化して保存）など、自社のポリシーに合わせて、方針を策定して下さい。

個人情報の例	取得条件
IPアドレス	設定に関わらず取得
Cookie	マッピング設定次第で取得可能
ユーザーID（ログインID等）	マッピング設定次第で取得可能
位置情報	マッピング設定次第で取得可能

上表の情報以外にも、個人情報となりうる項目（氏名、会員番号、メールアドレス等）を記録対象として明示的に設定した場合、個人情報として保存することとなります。

データ取得要件の策定：個人情報として取得

アクセス解析においてデータを取得するにあたり、個人情報として取得し保存するか、匿名情報として取得し保存するか、方針を決めた上で、適切な対応を行います。

個人情報として取得し保存する場合

個人情報として取得し保存する場合、事前にユーザーへの意思確認を行った上で、取得に同意した場合のみデータを取得する、という流れが基本となります。

サイト側の対応	詳細	RTmetrics側の対応
訪問者に個人情報の取得に同意する・同意しないを意思確認する仕組みの導入	意思確認を行うポップアップやモーダルダイアログ等の仕組みを導入します。意思確認の結果は、Cookieにセットします。	Cookieにセットされた値から、個人情報の取得に同意したユーザーのアクセスのみを記録するマッピング設定を実装します。（標準機能）
ユーザがデータの削除要求を申請できる仕組みの導入	ユーザが個人情報取得に同意した後、その同意を撤回し、過去データの削除の申請が可能な仕組みを実装・構築します。削除要求を受けたIDは一時的に保存する場所を構築しておき、対象となるIDの情報をRTmetricsの履歴データから削除できるようにします。	データ削除の対象となるIDを定期的に一時保存場所から取得し、RTmetricsの機能を使って、対象となるIDの情報を履歴データから削除します。（標準機能）

データ取得要件の策定：匿名情報として取得

アクセス解析においてデータを取得するにあたり、個人情報として取得し保存するか、匿名情報として取得し保存するか、方針を決めた上で、適切な対応を行います。

匿名情報として取得し保存する場合

匿名情報として取得し保存する場合、以下の対応が基本になります。

サイト側の対応	詳細	RTmetrics側の対応
匿名加工情報を作成する場合の法令遵守対応（個人に関する情報の項目の公表）	個人情報保護方針への定義の追加等	とくになし
匿名加工情報の作成	とくになし	匿名化データとして取得する設定を有効にし、ユニークユーザーID（Cookie）のハッシュ化、およびIPアドレスのマスク化（0.0.0.0に変換）を行います。その他、個人情報または他のデータと組み合わせることで個人情報に該当する文字列が、URLやパラメータ等のアクセス解析データに含まれる可能性がある場合は、それらの文字列をカットするマッピング設定を行い、データとして保存されないよう、合わせて対策を実施します。

解析要件に応じた柔軟な解析グループ設計

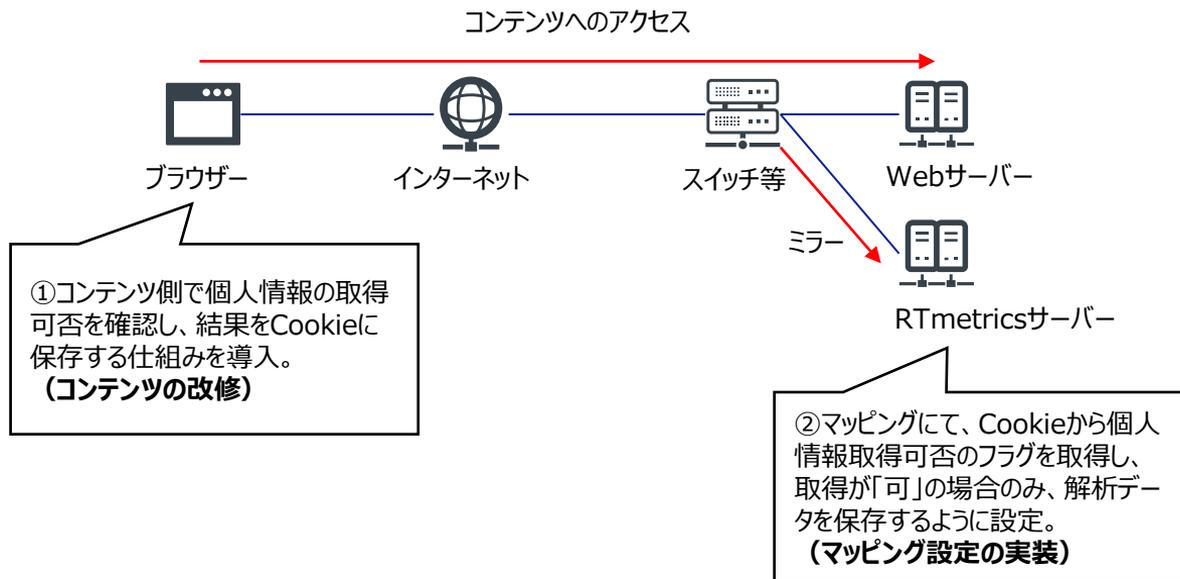
RTmetricsでは、グループ単位でデータを保管・管理しています。個人情報的一切保存しないグループでサイト全体のアクセス解析の基本指標を把握し、かつ、CRMやMA、BI等の外部システムと連携した高度なデータ活用に個人情報を保存したい要件が共存している場合、RTmetrics上でグループを分けて設定することでプライバシー保護と高度なデータ活用のニーズの両方の要件を満たす環境を構築することができます。

名称	管理ポリシー	RTmetricsの設定方針	使用目的
Cookieレスグループ	個人情報は一切保存しない	Cookieは保存しない IPアドレスはマスク化する	アクセス解析の基本指標の把握
匿名グループ	個人情報は匿名化し、保存する	Cookieは匿名化し保存 IPアドレスはマスク化する	UU数や再来訪など、匿名化されたCookie単位のWeb上の行動履歴の把握など高度なアクセス解析データの収集
個人情報保存グループ	個人情報はそのまま保存する	Cookieはそのまま保存 IPアドレスはそのまま保存 データ連携用のログインID等をマッピングで取得し保存する	ユーザからの申請があった場合にデータを消去することを前提とした、個人情報を活用した高度なデータ活用、分析利用

※ユーザからの申請があった場合、匿名グループのデータも消去対象とする場合、サイト側で意思確認をし、個人情報の取得に同意しなかったCookieの一時保存場所から、削除対象のIDをRTmetricsに転送し、RTmetrics上でデータ削除を実行する際、IDを同一のアルゴリズムでハッシュ化し、両者の値が同一になるようにします。

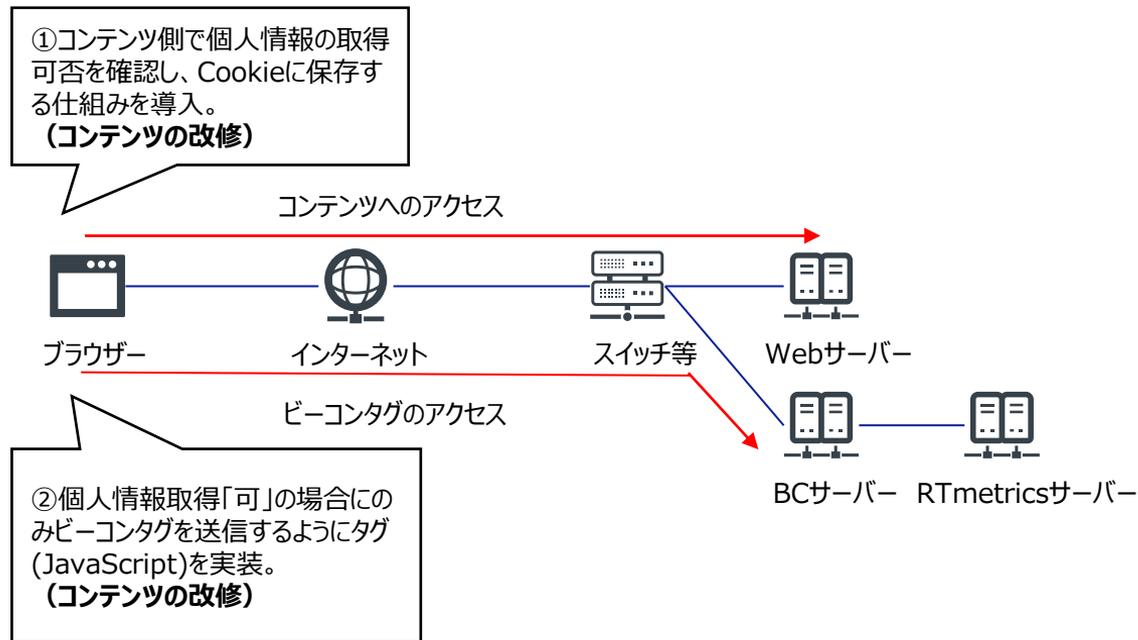
方式別の実装例：パケットキャプチャ

パケットキャプチャでの実装例になります。来訪時に確認した個人情報の取得可否の意思確認の結果は、Cookieにフラグとして保存しておくことで、次回、ユーザがサイトに来訪した際、クライアントが保持しているCookieから判定し、可の場合はデータ収集の対象に、否の場合はデータ収集の対象外にRTmetrics上で振り分けることができます。他にもURLのパラメータにフラグを入れ、同一セッション内で引き回す実装、などがありますが、Cookieが消去されていなければ、再来訪時にもフラグを再利用できるため、効率的に実装できる例となります。



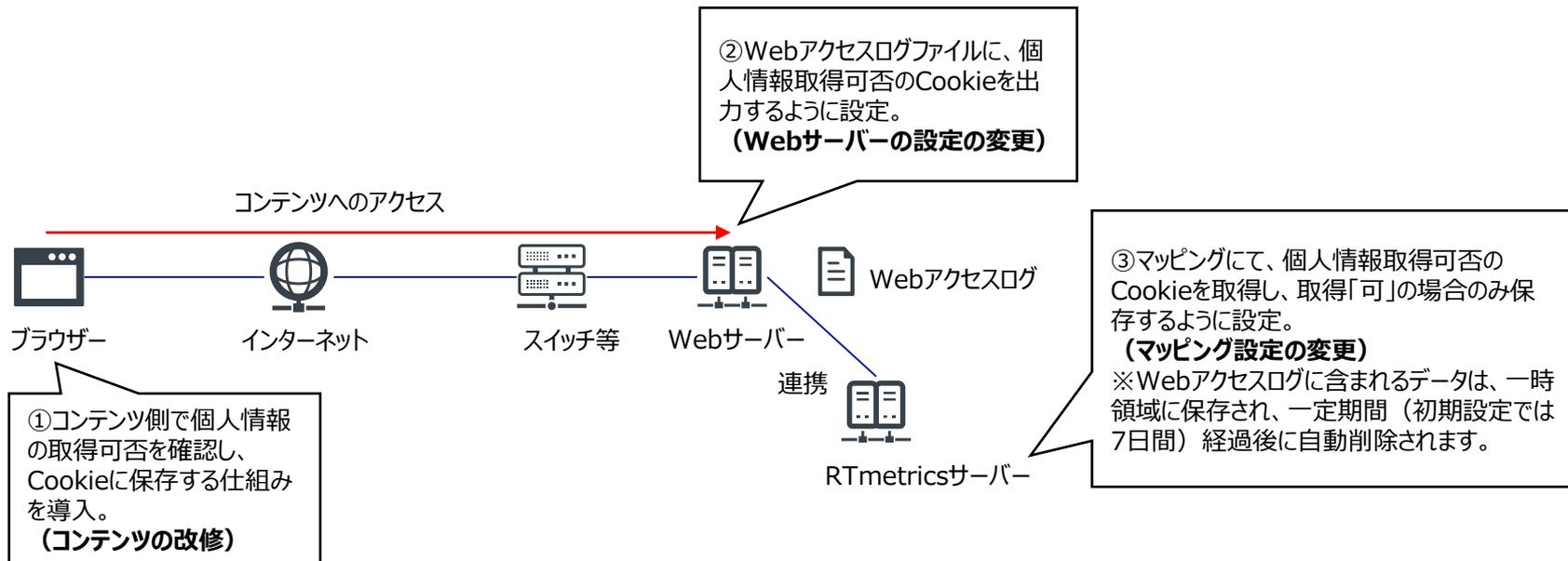
方式別の実装例：ビーコンタグ

ビーコンタグでの実装例になります。来訪時に確認した個人情報の取得可否の意思確認の結果は、Cookieにフラグとして保存しておくことで、次回、ユーザがサイトに来訪した際、クライアントが保持しているCookieから判定し、可の場合はデータ収集の対象に、否の場合はデータ収集の対象外にRTmetrics上で振り分けることができます。ビーコンタグでの実装の場合は、可の場合のみビーコンタグを送信するなど、タグの実装により、より厳密な制御が可能です。この実装の場合、RTmetricsのデータベースには、取得可のデータしか蓄積されません。マッピングによる可のデータのみ記録する（不可のデータは記録しない）設定の実装を不要にできます。



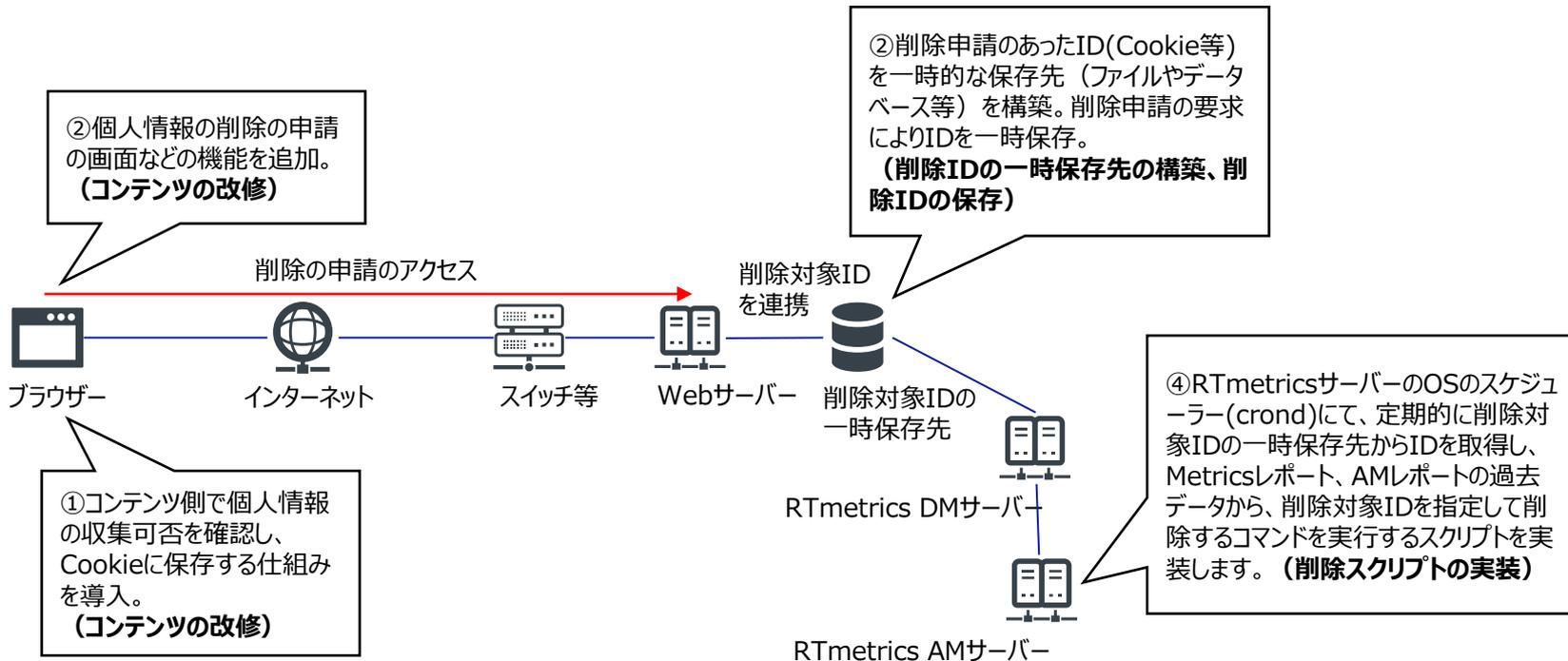
方式別の実装例：ログ

ログでの実装例になります。来訪時に確認した個人情報の取得可否の意思確認の結果は、Cookieにフラグとして保存しておくことで、次回、ユーザがサイトに来訪した際、クライアントが保持しているCookieから判定し、可の場合はデータ収集の対象に、否の場合はデータ収集の対象外にRTmetrics上で振り分けることができます。ログでの実装の場合、サイト側で実装したコンテンツの改修が、Webアクセスログにも吐き出されるよう、アクセスログ側の設定にも留意して下さい。



過去データの削除について

ユーザによる個人情報取得の同意の撤回があった場合、個人情報の収集確認を否とした以降については、アクセス解析データに記録されません。過去データについて、削除の申請があった場合は、RTmetricsのMetricsレポートおよびAMLレポートから、該当するユーザーIDに関するデータを削除する作業を行います。削除対象のIDを指定した上で、各レポートの削除用コマンドを実行する形式となっており、運用に合わせて、スケジュールによるバッチ処理によるデータ消去などを適宜実装します。



参考情報

匿名化データのRTmetricsでのレポート例

グループ管理の解析オプション「匿名化データとして取得する」について

RTmetrics-9.3.0にて新たに追加された機能(グループ管理の解析オプション「匿名化データとして取得する」)を有効にすることで、ユニークユーザーIDのハッシュ化、および、IPアドレスのマスキ化が行われ、RTmetricsのアクセス解析情報を匿名情報として保存することが可能です。

システム設定 - グループ管理

📄 エクスポート 🖨 印刷 🗉 ヘルプ

現在の設定 修正ログ 新規作成

Wed 06/09/2021 17:11:48 JST

現在の設定 > 1 ~ 2 (総数: 2) 表示件数 20 最初 最後

	グループID	タイムゾーン	データマネージャーIP	コレクターIP	HTTPステータスコードフィルター	アクセス元フィルター	解析対象サーバーフィルター	拡張子フィルター	検索エンジン定義	解析オプション
1.	test_01	Asia/Tokyo	192.168.1.147	192.168.1.147	[含む] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[デフォルト設定を追加]	[匿名化データとして取得する] [ユニークユーザーIDをハッシュ値に変換する]
2.	test_02	Asia/Tokyo	192.168.1.147	192.168.1.147	[含む] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[含まない] [デフォルト設定を追加]	[デフォルト設定を追加]	

匿名化されないデータの取得例

匿名化されないデータの場合、ユニークユーザーIDや接続元が画面上への表示はもちろんのこと、データとしても保存されます。

サイト - リアルタイム

設定

サイト 

[\[適用\]](#) [\[リセット\]](#)

開始時刻: Wed 06/09/2021 17:00:00 JST 期間: 35:01

全サイト  詳細  トップテン

サマリー	ページ	アプリキー	参照元	検索エンジン	クローラー	ユニークユーザー	未定義ユーザー	ドメイン	国	ブラウザ	OS	デバイスタイプ	
ユニークユーザー						> 1	~ 1	(総数: 1)	表示件数	20	 	最初	最後
ユニークユーザーID (*) @ 接続元 (*)						最終アクション	滞在時間	PV	参照元ドメイン (*)	検索ワード (*)	閲覧開始ペー:		
[全てのデータ(1)件の合計]						2:33	0:04	4	-	-	-		
1.		172.17.16.12.1623227258625439	@	192.168.1.147	2:33	0:04	4	www.auriq.co.jp		/training/			

匿名化データとしての取得例

匿名化データとして取得する場合、ユニークユーザーIDはハッシュ化され、接続元のIPアドレスは「0.0.0.0」と変換され、データとしても保存されます。

サイト - リアルタイム

設定

サイト auriq_01 

[適用] [リセット]

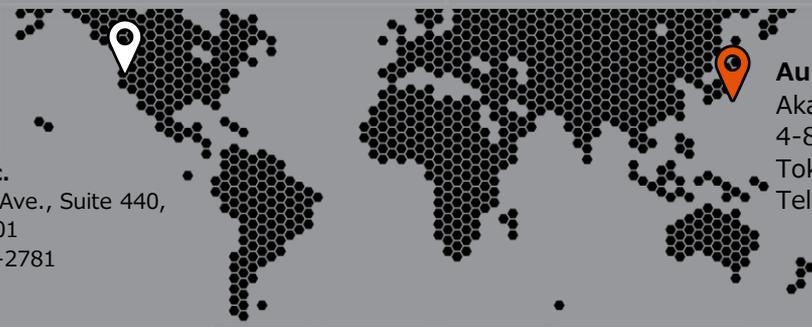
開始時刻: Wed 06/09/2021 17:00:00 JST 期間: 33:44

全サイト  詳細  トップテン

サマリー	ページ	アプリケー	参照元	検索エンジン	クローラー	ユニークユーザー	未定義ユーザー	ドメイン	国	ブラウザ	OS	デバイスタイプ		
ユニークユーザー						1	~ 1	(総数: 1)	表示件数	20		最初	最後	
ユニークユーザーID (*) @ 接続元 (*)	最終アクション (分:秒)	滞在時間 (分:秒)	PV	参照元ドメイン (*)	検索ワード (*)	閲覧開始ページ (*)								
[全てのデータ(1)件の合計]	1:16	0:04	4	-	-	-								
1.  XZbJ5@DB @ 0.0.0.0	1:16	0:04	4	www.auriq.co.jp		/training/								



AuriQ System Inc.
199 S. Los Robles Ave., Suite 440,
Pasadena, CA 91101
Tel: +1 (626) 564-2781



AuriQ Systems Japan Co.,Ltd.
Akasaka Yoko Building, 4th floor
4-8-6 Akasaka, Minato-ku
Tokyo 107-0052 Japan
Tel: +81-3-3560-8083

Thank you!