

注目されているセキュリティ事故・事件に関する情報 ＜2017年9月版（第22号）＞（選り抜き版）

2017年9月25日
NTTデータ先端技術株式会社
セキュリティ事業部

フリマアプリ「メルカリ」の個人情報流出とその後の対応

オンラインのフリーマーケットサービスを提供している「メルカリ」のウェブ版サービスにおいて、2017年6月22日に個人情報の流出が発生しました。情報流出が発生してしまった経緯と、メルカリがとったその後の対応について振り返ります。

フリマアプリ「メルカリ」の 個人情報流出とその後の対応

1. 事故の概要

2017年6月22日(木)、メルカリはウェブ版サービスのパフォーマンス改善のために、CDN上のキャッシュサーバの切り替えを行いました。

切り替え作業から5時間後、ユーザからの問い合わせにより、一部ユーザの個人情報が他者から閲覧可能となっていることが判明します。

メルカリはウェブ版サービスをメンテナンス状態にするとともに、事故の原因究明と対策を行いました。

事故発生日時	2017年6月22日(木) 9:41～15:05
対象サービス	メルカリ ウェブ版 ※iOS/Androidアプリ版のメルカリは対象外
個人情報を閲覧された可能性のあるユーザ数	最大54,180人 (このうち、個人を特定可能な情報が閲覧可能となっていたユーザ数 → 最大29,396名)
閲覧された可能性がある個人情報	・ 名前/住所/メールアドレス/電話番号 ・ 銀行口座/クレジットカード番号の下4桁と有効期限(※登録したユーザのみ) ・ 購入/出品履歴 ・ ポイント・売上金/お知らせ/やることリスト

2. タイムライン

2017年6月22日の問題発生から問題終結までのタイムラインを以下に示します。

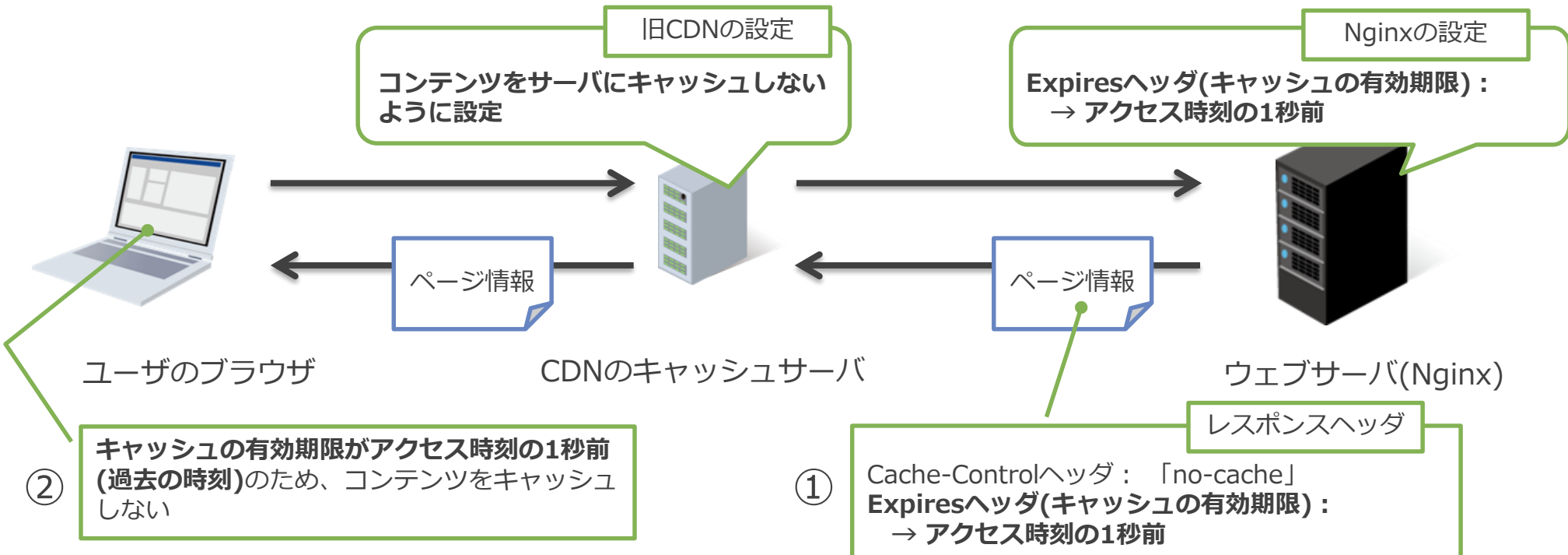
時間	内容
09:41	キャッシュサーバーの切り替えを実施
14:41	カスタマーサポートにてお客さまからの問い合わせ(「マイページをクリックしたら他人のアカウントのページが表示された」旨)を確認し、社内へ報告
15:05	キャッシュサーバーの切り替えを中止し、従来の設定へ戻す
15:16	ウェブ版のメルカリをメンテナンスモードへ切り替え
15:38	キャッシュサーバーへのアクセスを遮断し、問題を完全解消
15:47	ウェブ版のメルカリメンテナンスモードを終了

引用 : https://www.mercari.com/jp/info/20170622_incident_report/

3. CDN切り替え前の構成

メルカリではCDN※を利用し、ユーザからのリクエストはCDNを経由してメルカリが管理するウェブサーバ(Nginx)へ届きます。

事故発生前は、**CDN側とウェブサーバの設定**から、コンテンツをCDNとブラウザにキャッシュさせないようにしていました。

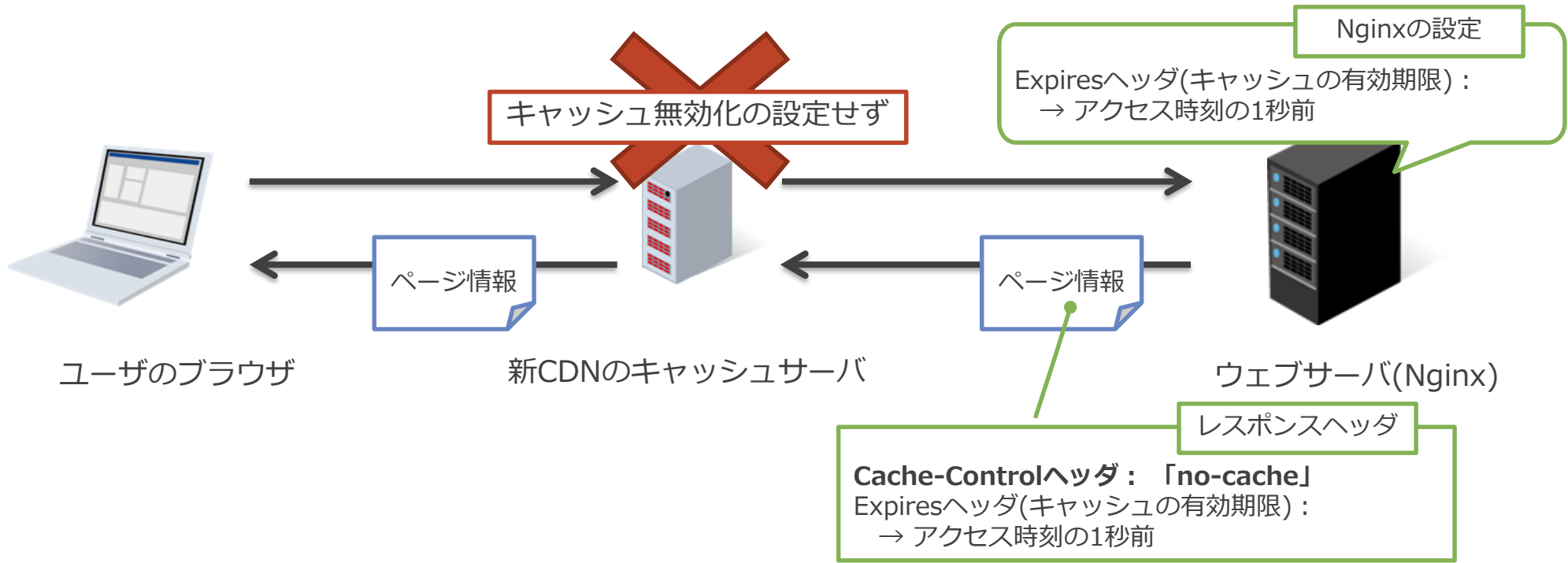


※ CDN(Contents Delivery Network)- ウェブコンテンツの配信を高速化するための仕組みのこと

世界各地に配置されたCDNのキャッシュサーバにコンテンツをキャッシュさせ、ユーザは最寄りのCDNのキャッシュサーバにアクセスすることで、コンテンツの高速な読み込みが可能となる。

4. CDN切り替え後の構成

切り替え後のCDNでは、ウェブサーバからのレスポンスヘッダに記載された「**Cache-Control**」ヘッダによりCDNのキャッシュ機能の制御が可能でした。そのため、メルカリでは**CDN側の設定によるキャッシュ無効化設定は行わず**、CDNのキャッシュ制御はすべてウェブサーバの設定から行うことになりました。

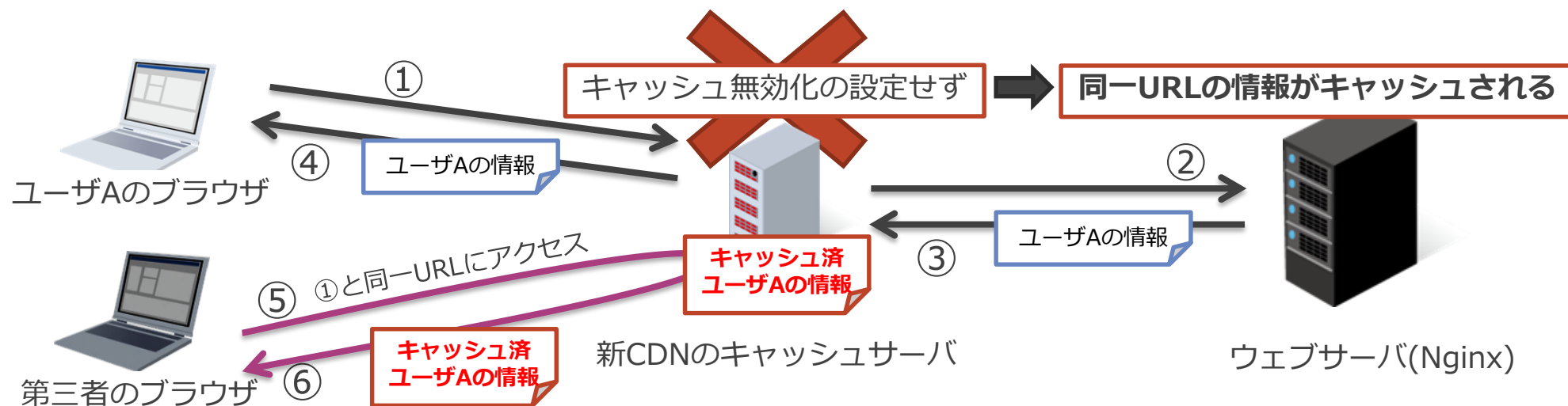


5. CDN切り替え後の問題

しかしながら、この構成では、**Cache-Controlヘッダの設定ミス**により、ウェブサーバからの情報がCDNでキャッシュされてしまうことが発覚します。これにより、以下の手順によってCDNにキャッシュされたユーザの情報を第三者が閲覧可能になってしまいました。

- ① ユーザAから新CDNへアクセス
- ② 新CDNからウェブサーバへアクセス
- ③ ウェブサーバから新CDNへユーザAの情報を送信、**ユーザAのデータをCDNがキャッシュ**
- ④ 新CDNからユーザAのブラウザへ、ユーザAの情報を送信
- ⑤ 第三者のブラウザから ①と同一URLにアクセス
- ⑥ 新CDNが**ユーザAのキャッシュされたデータを第三者のブラウザ宛に返送**

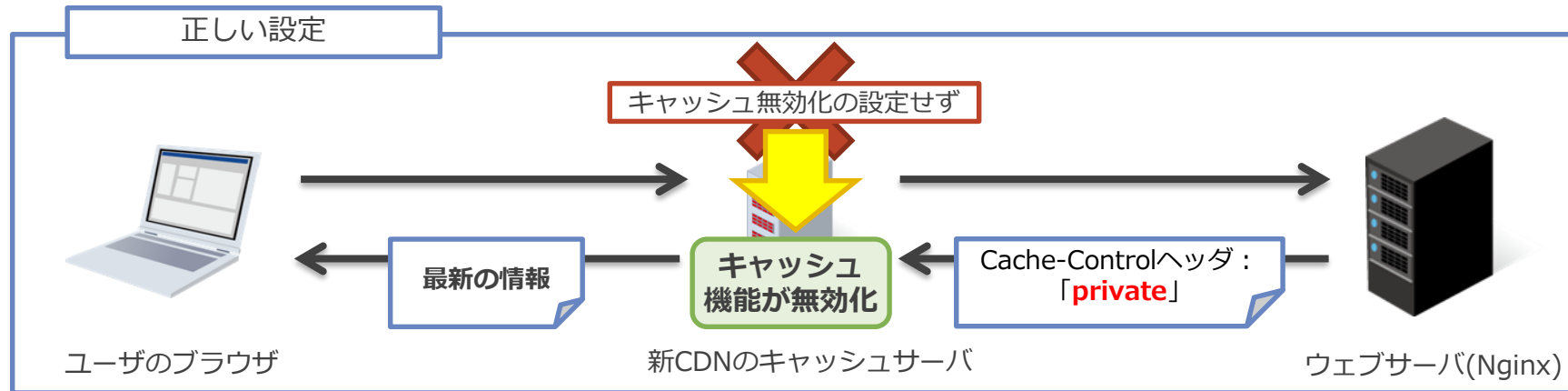
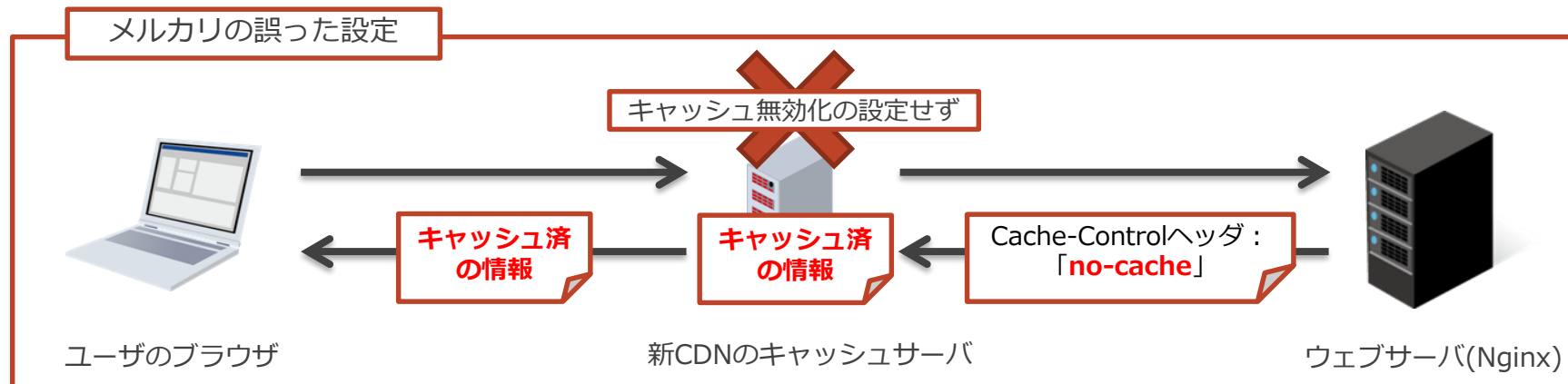
↓
第三者がユーザAの情報を閲覧可能



6. Cache-Controlヘッダの設定ミス

当初、メルカリはCache-Controlヘッダが「no-cache」であればCDNのキャッシュ機能が無効化できると認識していました。

しかしながら、実際に**CDNのキャッシュ機能が無効化できるのはCache-Controlヘッダが「private」の場合のみ**でした。



7. Cache-Controlヘッダの設定ミス(参考)

■ Cache-Controlヘッダの仕様

HTTP/1.1のキャッシュの仕様(RFC7234)によれば、Cache-Controlが「no-cache」の場合の動作は以下のように定義されています。

The “no-cache” response directive indicates that the response MUST NOT be used to satisfy a subsequent request without successful validation on the origin server. This allows an origin server to prevent a cache from using it to satisfy a request without contacting it, even by caches that have been configured to send stale responses.

引用 : <https://tools.ietf.org/html/rfc7234#section-5.2.2.2>

これは、同じURLに対する後続のリクエストへのレスポンスとして、以前返されたレスポンスを使用するには、まずサーバに問い合わせるレスポンスに変更があるかを確認する必要があることを示しています。

すなわち、レスポンスに変更がなければ、キャッシュの使用が許可されます。
「no-cache」 = 「キャッシュしない」という意味ではありません。

8. 対応と再発防止策

メルカリは、問題発覚後に以下の対応と再発防止策を行いました。

■ 対応

- ✓ DNS設定の切り戻しにより、切り替え前のCDNを利用する状態に戻す
- ✓ 切り替え後のCDNのコントロールパネルより、キャッシュされた情報を削除

■ 再発防止策

- ✓ 外部から定期的にウェブ版のメルカリにアクセスを行い、またCDNのアクセスログをリアルタイムに監視することで、意図しないキャッシュの早期発見と、関係するエンジニアへ通知を行うシステムの導入
- ✓ CDNサービスの配信設定を定期的にダウンロードし、キャッシュに関わる設定が正しく行われていることを自動で検証するプログラムの構築
- ✓ CDNサービス提供元の協力による、設定レビューの実施

9. まとめ

CDNの切り替えによって、個人情報の流出が発生してしまったメルカリですが、幸いにも、現時点では個人情報の悪用は確認されていません。

ユーザからの問い合わせによって発覚したこの問題は、その後速やかに社内に報告され、対応と再発防止策が講じられました。

個人情報の流出という重大な事故が発生してしまいましたが、その一方で、以下の教訓が得られたと考えられます。

- ✓ Cache-Controlヘッダの設定のように、「no-cache」＝「キャッシュしない」という英語の表面的な意味をとらえるのではなく、本来の仕様を確認して設定を行う
 - ✓ 有識者による設定レビュー等が効果的です
 - ✓ CDN業者へのサービス仕様の確認も必要です
- ✓ 万が一に備え、CDNとウェブサーバの両方からキャッシュの制御をする(多重のセキュリティ対策を施す)
- ✓ 事故の詳細を公表することによって、同様の設定をしている可能性のある他組織に対する啓発ができた

10. 参考URL

- Web版のメルカリにおける個人情報流出に関するお詫びとご報告 ※6/23追記あり
https://www.mercari.com/jp/info/20170622_incident_report/
- CDN切り替え作業における、Web版メルカリの個人情報流出の原因につきまして - Mercari Engineering Blog
<http://tech.mercari.com/entry/2017/06/22/204500>
- 「メルカリ」の個人情報漏えい、原因はCDNキャッシュの仕様、技術的な詳細情報を公表 - INTERNET Watch
<http://internet.watch.impress.co.jp/docs/news/1066949.html>
- ニュース解説 - メルカリの個人情報流出、陥った「no-cache」の罠 : ITpro
<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/062601030/>
- ニュース - 「続報」メルカリが個人情報流出で新情報、実際は「有効期限0秒のキャッシュ」 : ITpro
<http://itpro.nikkeibp.co.jp/atcl/news/17/062701776/>
- 「メルカリ」Web版で個人情報流出、閲覧された可能性のある2つのケース公開 | マイナビニュース
<http://news.mynavi.jp/news/2017/06/24/033/>
- 「メルカリ」で個人情報流出…問われる運営側の安全対策 : 科学 : 読売新聞(YOMIURI ONLINE)
<http://www.yomiuri.co.jp/science/goshinjyutsu/20170627-OYT8T50066.html>
- メルカリの個人情報流出 閲覧された可能性のあるケースは？ - ライブドアニュース
<http://news.livedoor.com/article/detail/13245878/>
- RFC 7234 - Hypertext Transfer Protocol (HTTP/1.1): Caching
<https://tools.ietf.org/html/rfc7234>
- Module ngx_http_headers_module
http://nginx.org/en/docs/http/ngx_http_headers_module.html#expires

