

# エグゼクティブサマリー： [インターネットの現状] / セキュリティ

第6巻、第3号

## リワーズポイント詐欺

## 小売・ホスピタリティ業界における 詐欺の実態



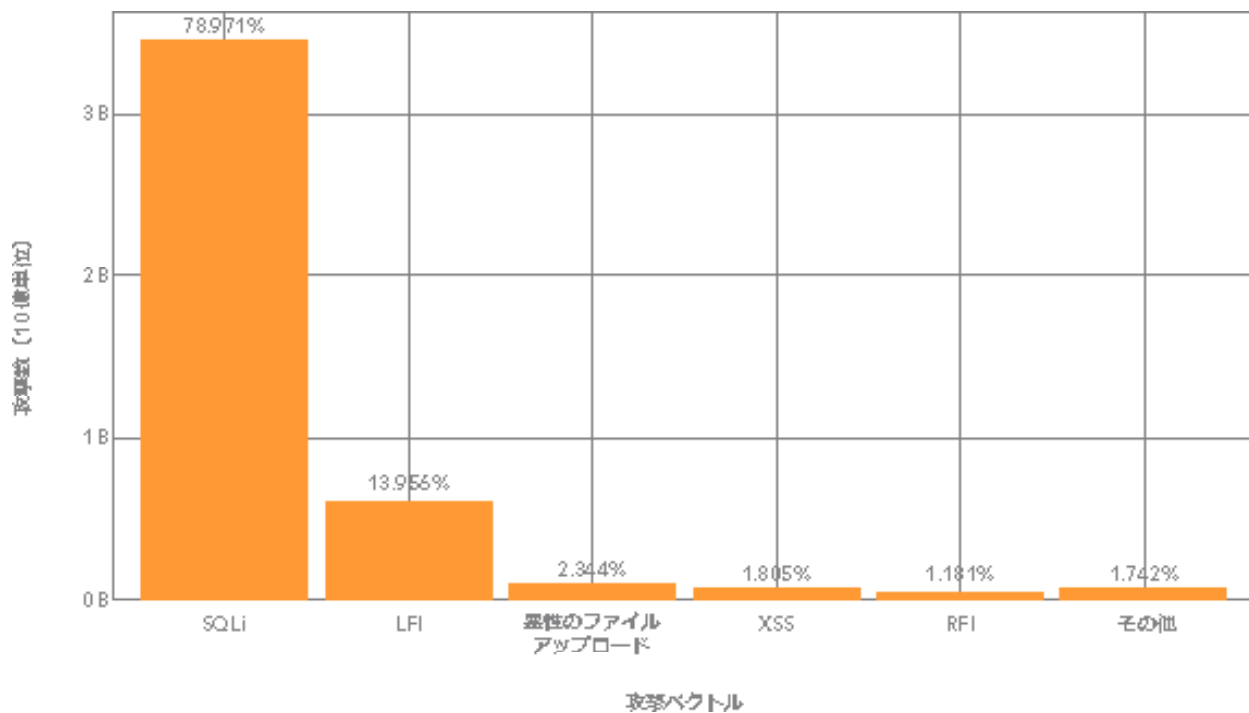




```
...    http.Redirect(http.RedirectRequest(r.Request, http.RedirectURL(r.FormValue("target")), count)); });
...    http.ListenAndServe(":1337", nil)); };package main;
...    statusPollChan := statusPollChannel); for { select { case respChan := <- statusPollChanne
...    r.ParseForm(); count, err :=
...    http.ResponseWriter, r *http.Request) { reqChan := make(chan
```

犯罪者が小売、旅行、ホスピタリティの各業界を攻撃する手段として利用するのは、Credential Stuffing だけではありません。発信元では SQL インジェクション (SQLi) やローカル・ファイル・インクルージョン (LFI) 攻撃も使用して、これらの業界の組織を攻撃します。2018 年 7 月から 2020 年 6 月までの期間では、43 億 7,571 万 1,860 件の小売、旅行、ホスピタリティの各業界に対する Web アプリケーション 攻撃が観測されました。これは全業種への攻撃数の 41% を占めています。このコマース業界を狙った Web アプリケーション攻撃のうち 83% が小売業界を標的とするものでした。

### コマース業界を標的とする主な Web 攻撃ベクトル 2018 年 7 月～ 2020 年 6 月

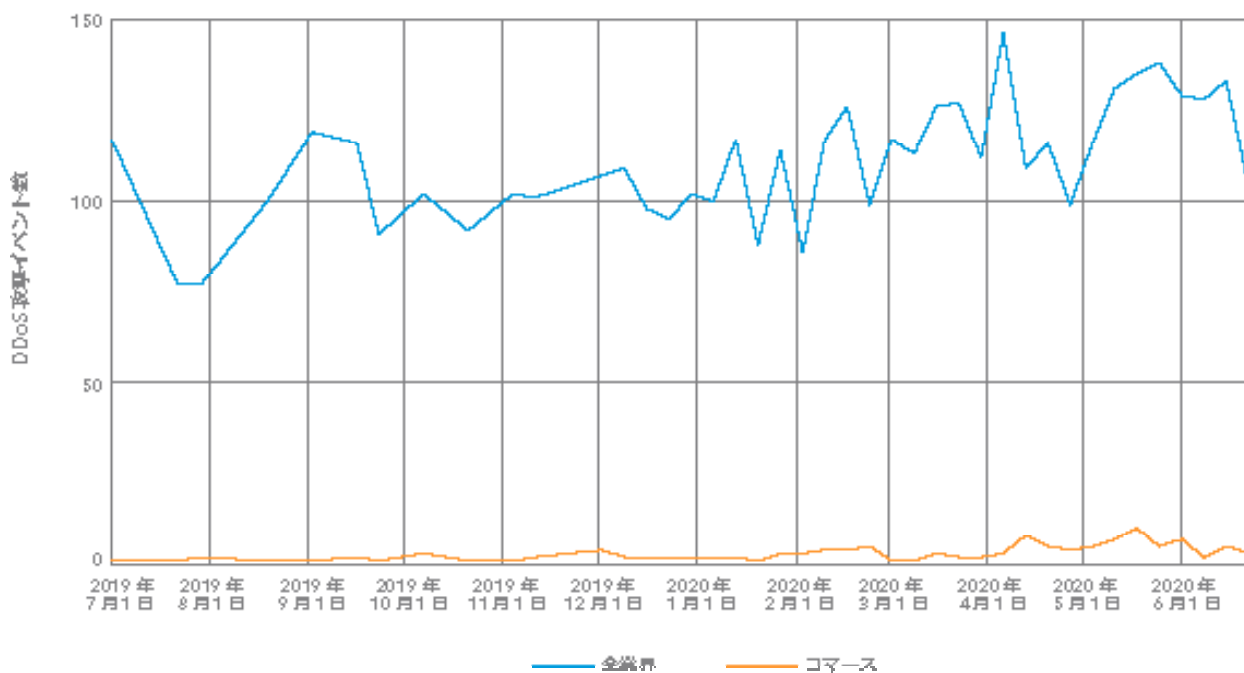


```
... final EscapeString(r.FormValue("target")), count); });
... http.ListenAndServe(":1337", nil)); };package main;
... statusPollChannel); for { select { case respChan := <- statusPollChanne
... r.Host, ":")); r.ParseForm(); count, err :=
... http.ResponseWriter, r *http.Request) { reqChan := make(chan
```

分散型サービス妨害（DDoS）攻撃についても忘れてはなりません。分散型サービス妨害（DDoS）攻撃は、どの小売企業も恐れている攻撃です。膨大な量のパケットや悪性トラフィックが流入してオンライン・コマース・ポータルが崩壊すれば、1秒あたり何千ドルもの損失となります。

以下のグラフが示す通り、2019年7月から2020年6月までに、コマースカテゴリでは125件のDDoS攻撃を観測しました。そのうち90%が小売業界で事業を展開する組織に対するもので、残りが旅行およびホスピタリティ業界に対するものでした。

週次 DDoS 攻撃イベント数  
2019年7月～2020年6月



```
...    fmt.Println("Final EscapeString(r.FormValue("target")), count); });
...    http.HandleFunc(func(w http.ResponseWriter, r *http.Request) { reqChan := make(chan
...    statusPollChannel := statusPollChannel); for { select { case respChan := <- statusPollChannel:
...    resp := http.Response{Status: http.StatusOK, Body: strings.NewReader("OK")}; count, err :=
...    http.ResponseWriter, r *http.Request) { reqChan := make(chan
```

小売、ホスピタリティ、旅行の各業界は、一貫して犯罪者の標的となっています。これらの業界は犯罪者が商品に置き換えやすい資産にアクセスできるためです。ここで言う資産とは、個人情報、金融情報、各ブランドのロイヤルティプログラム、またはこれらすべての組み合わせです。

標的の上位になっているロイヤルティプログラムには、携帯電話番号と数字のパスワード以外は不要なものもあれば、容易に手に入る情報を認証の手段に利用しているものもあります。アイデンティティの制御と対策を強化し、API とサーバーリソースへの攻撃を回避することは、今喫緊の課題となっています。

小売、旅行、ホスピタリティの各業界の防御担当者と犯罪者の攻防は、常に一進一退を繰り返しています。常に最先端の状態を維持できるかどうかは、組織自体、そして組織内のチームに掛かっています。

## レポートの全文を読む

[インターネットの現状] / セキュリティ 第6巻、第3号  
リワーズポイント詐欺—小売・ホスピタリティ業界  
における詐欺の実態

今すぐダウンロード



Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、Web / モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 / 24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、[www.akamai.com](http://www.akamai.com)、[blogs.akamai.com](http://blogs.akamai.com)、および Twitter の [@Akamai](https://twitter.com/Akamai) でご紹介しています。全事業所の連絡先情報は、[www.akamai.com/locations](http://www.akamai.com/locations) をご覧ください。公開日：2020 年 10 月。