ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●PayPay加盟店情報等約2,000万件流出か…サーバーへの不正アクセス発覚

https://www.itmedia.co.jp/news/articles/2012/07/news091.html
https://www.asahi.com/articles/ASND74R7ZND7ULFA01P.html
https://paypay.ne.jp/notice/20201207/02/

### このニュースをザックリ言うと･･･

- 12月7日(日本時間)、PayPay社より、同社運営の電子決済サービス「PayPay」の加盟店情報等が不正アクセスを受け流出した可能性があると発表されました。

- 被害を受けたとされるのは、同サイトの加盟店やその営業先の情報(店名・住所・代表者名等)の他、PayPay社従業員情報(氏名・所属・役職等)、同社パートナー・代理店情報(社名・連絡先・担当者名等)および加盟店向けアンケート回答者情報(氏名・電話番号・メールアドレス)の計20,076,016件に上り、約260万店とされる全加盟店に関連するものとされています(PayPay利用者側の情報は被害を受けていないとのことです)。

- 12月1日に外部からの連絡を受けて調査したところ、11月28日にブラジルからのアクセスが確認され、12月3日までに遮断を行ったとのことです。

### AUS便りからの所感等

- 2020年10月18日～12月3日にかけてデータベースへのアクセス権限設定に不備があり、本来同社内の店舗営業に関わる従業員のみがアクセス可能であったところ、外部からもアクセスが可能になっていたことが流出の原因とされています。

- 試験・診断等の目的でサーバー等に外部からのアクセスを許可する設定を行うことは多々あり、一部報道によればではこれもそのケースとみられ、10月に一時的な設定を行った後それを無効にし忘れていたものと推測されます。

- そのようなアクセス許可設定は、IPアドレス等のアクセス元およびサーバー上のアクセス可能な範囲を基本的に必要最小限とし、設定を実施したことおよび無効にしたことを確実に記録し、また無効にした後は外部からアクセスできない状態であることを必ず確認することが重要です。

- 発表時点での情報の悪用は確認されていないとのことですが、大手人気決済サービスで発生した事案であり、全加盟店に関わる大規模な情報が奪取された恐れも考えられ、より厳密な被害範囲等の続報が待たれるところであり、そのためにアクセス状況が把握できるような環境の構築もまた肝要です。

ITmedia NEWS

### PayPayのサーバに不正アクセス　加盟店情報など2000万件に流出の可能性

2020年12月07日 13時56分 公開　[ITmedia]

スマートフォン決済サービス「PayPay」を運営するPayPayは12月7日、同社が管理するサーバが不正アクセスの被害を受け、加盟店の名称、住所、代表者名など2007万6016件の情報が流出した恐れがあると発表した。現時点でこれらが悪用された形跡はなく、一般ユーザーの個人情報は流出していないという。

流出の恐れがある情報は上記の他、PayPayの営業先の名称と住所、PayPay従業員の氏名と連絡先、PayPayの代理店・パートナー企業の社名と担当者名など。11月28日にブラジルからの不審なアクセス履歴を発見し、12月1日から調査した結果、情報流出の可能性を確認したという。

朝日新聞 DIGITAL

### ペイペイ加盟全260万店情報流出か　第三者がアクセス


ソフトバンク系の スマートフォン 決済「PayPay（ペイペイ）」は7日、第三者からのアクセスで、ペイペイ で決済できる全加盟店約260万店の情報が流出した可能性があると発表した。ペイペイ を使って買い物をする利用者の情報は、店舗情報とは別に管理されていて被害はないという。

1日に同じソフトバンク系のヤフーから連絡を受け、社内でアクセス履歴を調査したところ、11月28日に ブラジル からデータベースにアクセスされていたことを確認した。アクセス権限は本来、社内で店舗営業に関わる従業員のみに設定していたが、10月にサーバーの更新をした際にアクセス権限の変更を行った後、設定を元に戻さず、外部からもアクセスできる状態になっていたという。(益田暢子)

## ● EXILE所属事務所ECサイト、クレジットカード情報44,000件以上流出か

https://www.itmedia.co.jp/news/articles/2012/08/news139.html
https://www.ldh.co.jp/info/notice/important-notice/

### このニュースをザックリ言うと・・・

- 12月8日(日本時間)、EXILE等が所属する芸能事務所LDH JAPANより、同社が運営するECサイト「EXILE TRIBE STATION ONLINE SHOP」が不正アクセスを受け、クレジットカード情報が流出した可能性があると発表されました。

- 被害を受けたとされるのは、同サイトで2020年8月18日～10月15日に登録または変更されたカード情報(名義人・番号・有効期限およびセキュリティコード(CVV))44,663名分とされています。

- 10月15日に提携するカード会社から情報流出の可能性の指摘を受けてサイトを停止、その後第三者機関への調査依頼により、11月17日に流出の可能性が確認されたとのことで、11月27日までの時点で209件のカード情報が不正利用された可能性があるとされています。

### AUS便りからの所感

- 流出の原因として、不正アクセスにより決済処理プログラムの改ざんが行われたことが発表されており、一方でカード情報以外の個人情報の流出は確認されていないとのことです。

- ECサイト上でカード情報を保持しない「非保持化」が求められるようになり、CVVを含むカード情報の入力時に外部サイトへ移動するケースが多くなったことで、フォームやプログラムの改ざんにより利用者を偽フォームに誘導する手口への移行が近年目立っており、今回の事例はその例の一つである可能性が高いです。

- このようなWebサイト等の改ざんは利用者側で確実に検知することは難しいとみられ、サービス提供者側においては、根本的な対策としてWebアプリケーションの脆弱性を突かれないようにすることが重要であり、加えてサーバー上に不正プログラムが設置された場合の外部通信遮断といった出口対策等を実施するよう推奨致します。

ITmedia NEWS

**EXILEの公式ECサイトに不正アクセス　カード情報4万4000件が流出か**

2020年12月08日 18時04分 公開　[吉川大貴，ITmedia]

音楽ユニット「EXILE」などが所属する芸能事務所LDH JAPANは12月8日、同社が運営するECサイト「EXILE TRIBE STATION ONLINE SHOP」が不正アクセスを受け、4万4663件のクレジットカード情報が流出した可能性があると発表した。このうち209件のカード情報については、11月27日時点で第三者に不正利用された可能性がある。

同サイトでは、LDH JAPANに所属するアーティストのグッズなどを販売している。流出の可能性があるのは、8月18日～10月15日に同サイトでカード情報を登録するか、登録済みの情報を変更した利用者のカード名義人、カード番号、有効期限、セキュリティコード。

## ●ホテル利用者の個人情報21万件、サーバーと共に紛失

https://www.itmedia.co.jp/news/articles/2012/07/news096.html
https://www.orix-realestate.co.jp/news/pdf/press_20201204_2.pdf

### このニュースをザックリ言うと・・・

- 12月4日(日本時間)、オリックスグループのホテル運営会社であるオリックス・ホテルマネジメント社より、同社運営ホテル「ハンドレッドステイ 東京新宿」の顧客情報を保存したサーバー機が紛失したと発表されました。

- 当該サーバーに保存されていたのは、同ホテルを2010年7月14日～2018年2月2日に利用・予約した顧客情報約209,000件で、うち氏名のみが約102,000件、住所・電話番号・メールアドレス・生年月日等含むものが約107,000件で、クレジットカード・パスポートの情報は対象外とされています。

- 10月の設備棚卸しの際に当該サーバー機が見つからず、調査の結果12月2日に紛失を確認したとのことです。

### AUS便りからの所感

- 個人情報の紛失事案としてはノートPCやUSBメモリー等の記録媒体のイメージが強い一方で、7月にはみずほ銀行・みずほ総研の顧客情報が入った磁気テープがサーバー機と共に破棄された可能性があるとする事案も発表されています(https://www.asahi.com/articles/ASN7P65XPN7PULFA023.html )。

- また今回のケースは盗難の可能性もありますが、2018年には他の社員の業務用PCを分解してHDDから内部情報データを抜き取るというケースが発覚しています(AUS便り 2018/7/9号参照)。

- 紛失・盗難に備えてのデータの暗号化は、ことノートPCや媒体上のデータについてはよく言われ、実施されるケースも多いですが、このような事案が以後も目立って発生するようになれば、通常は移動することのないサーバー機においても、実施を検討する流れになることが予想されるでしょう。

ITmedia NEWS

**オリックス孫会社、個人情報21万件入りサーバを紛失　外部に持ち出された可能性も**

2020年12月07日 14時47分 公開　[吉川大貴，ITmedia]

旅館やホテルを運営するオリックス・ホテルマネジメント（東京都港区）はこのほど、約20万9000件の個人情報を記録していたサーバを紛失したと発表した。何者かがサーバを外部に持ち出した可能性もあるとして、紛失に至るまでの経緯などを調査している。

サーバに記録していたのは、2010年7月14日～18年2月2日に同社が運営するホテル「ハンドレッドステイ 東京新宿」を利用・予約した顧客の氏名（約10万2000件）と住所、電話番号、メールアドレスなど（約10万7000件）。