

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。

●クロネコメンバーズで不正ログイン被害…リスト型攻撃で3,467件の個人情報流出か

<https://www.itmedia.co.jp/news/articles/1907/25/news095.html>
<https://internet.watch.impress.co.jp/docs/news/1198096.html>



このニュースをザックリ言うと…

- 7月24日（日本時間）、ヤマト運輸より、同社の会員制サービス「クロネコメンバーズ」が不正ログイン被害を受け、3,467件の個人情報が発見された可能性があると発表されました。
- 同23日にいわゆる「**リスト型攻撃**」とみられる約3万回のログイン試行が行われたことにより、ユーザのID・メールアドレス・氏名・電話番号・性別・住所・クレジットカードの一部情報（カード番号の下4桁・有効期限・氏名。セキュリティコードは対象外）およびアドレス帳情報等が第三者に閲覧された可能性があるとのことです。
- 同社では、**不正ログインが確認されたアカウントについてパスワードを変更しなければ使えないよう対策し**、今後も再発防止に向けてセキュリティの高度化を図るとする一方、ユーザに対してもパスワードの使い回しをしない等の注意を呼び掛けています。

AUS便りからの所感等

- クロネコメンバーズでは二段階認証が使用可能でしたが、PCサイト以外では二段階認証を要求しない仕様になっていたため（モバイルサイトにPCからアクセスした場合含む）、回避可能な状態にあったことが事件の発表後に指摘されています（<https://togetter.com/li/1381019>）。
- 「鎖の強度は最も弱い環で決まる」という原則はセキュリティ界隈においても良く取り上げられますが、今回のケースはこの原則に如実に当てはまったものと言え、当初8月5日に開始予定だったスマートフォン向けサービスが延期となったのも、指摘された問題点を改修する必要が生じたためと考えられます。
- 一方のユーザ側においても、「二段階認証があるから」と簡単なパスワードや他のサービスと同じパスワードを設定するのではなく、**普段から推測されにくく十分に長いパスワードを設定すること**を心がけるべきでしょう（ヤマト運輸では「定期的なパスワードの変更」も呼び掛けていますが、それ以上に重要なのは、強いパスワードを設定することです）。



クロネコメンバーズで不正ログイン被害 リスト型攻撃で3467件の個人情報流出か

2019年7月25日 14時02分 公開 [出典元: ITmedia]

ヤマト運輸は7月24日、同社の会員制サービス「クロネコメンバーズ」が不正ログイン被害を受け、3467件の個人情報が発見された可能性があると発表しました。

クロネコメンバーズにおける不正ログインに

その後の調査で、不正ログインで使われたIDとパスワードはクロネコメンバーズで使われていないものが多く含まれていることが分かり、他社サービスから流出した可能性のあるIDとパスワードで不正ログインを試す「リスト型攻撃」によるものとみられるという。第三者が不正ログインを試みた数は約3万件に上った。

不正ログインが確認されたクロネコメンバーズのアカウントはパスワードを変更しなければ使えないように対策し、対象ユーザには個別に対応するという。

同社は「今回の事態を機業に受け止め、再発防止に向けてセキュリティの高度化を図る」としつつ、定期的なパスワードの変更やパスワードの使い回しをしないなど、ユーザ対策を呼び掛けている。



「クロネコメンバーズ」で不正ログイン、3467件の個人情報が発見された可能性

「パスワードリスト攻撃」を確認、パスワードを使い回している場合は注意

報告 2019年7月25日 13:39

ヤマト運輸株式会社は24日、会員サービス「クロネコメンバーズ」が不正ログイン被害を受け、3467件の個人情報が発見された可能性があると発表しました。

その後の調査で、不正ログインで使われたIDとパスワードはクロネコメンバーズで使われていないものが多く含まれていることが分かり、他社サービスから流出した可能性のあるIDとパスワードで不正ログインを試す「リスト型攻撃」によるものとみられるという。第三者が不正ログインを試みた数は約3万件に上った。

不正ログインが確認されたクロネコメンバーズのアカウントはパスワードを変更しなければ使えないように対策し、対象ユーザには個別に対応するという。

不正ログインにより閲覧された可能性のある情報は、ID、利用の端末別（PCまたは携帯・スマートフォン）、電話番号、性別、郵便番号、住所、クレジットカード情報（有効期限・氏名）、アドレス帳情報（氏名・住所・電話番号）がメンバーズ会員のうち、メールアドレスを登録していないユーザの被害の可能性はない。

個人情報を不正に閲覧されたユーザについては、パスワードを変更しなくても同サービスを使用できないようにした。また、対象のユーザについては個別に案内している。

不正ログインを防止するために、パスワードを変更する際は、1) 他社サービスで利用しているパスワードの利用を控えること、2) 極力、過去に使ったことのないパスワードを使用すること、3) 第三者が容易に推測できるパスワードの使用を控えること—などをヤマト運輸では挙げている。

●本田技研の内部情報約1億3,400万件が外部からアクセス可能な状態に

<https://gigazine.net/news/20190802-honda-leaks-database-employee-data/>



このニュースをザックリ言うと…

- 7月31日（現地時間）、Cloudflare社でセキュリティ担当ディレクターを務める「Justin」氏より、**本田技研工業（以下、ホンダ）の内部情報を格納したデータベースが外部からアクセス可能な状態になっていた**と発表されました。
- 同氏はデータベースを7月4日に発見したとしており、格納されていた情報は、従業員の名前・メールアドレス・連絡先といった個人情報や、従業員が使用する端末情報を含めたホンダ社内ネットワーク情報等、**合計約1億3,400万件（約40GB）**に上るとされています。
- ホンダでは同7日に同氏からの連絡を受けて適切なアクセス設定を行っており、第三者への情報流出はアクセスログからは確認されなかったとしています。

AUS便りからの所感等

- データベースは分散処理型検索エンジン「Elasticsearch」のものですが、同様のケースとしては、例えば3月にデータベースサーバ「MongoDB」に格納された約20億7,000万件のデータにアクセス可能だったことが発覚した事例が挙げられます（AUS便り 2019/03/18号参照）。
- Webサーバと連携するデータベースソフトウェア等が同じホストで稼働している場合は、ホスト自身やルータ・UTMのファイアウォール機能で適切なアクセス制限を設定し、**データベースソフトウェア等に外部の不特定多数から直接アクセスされないようにすることが肝要**です。
- これに加え（別のホストと連携する必要がある場合には特に）、パスワード設定によるアクセス保護を行うことは不可欠ですし、不正アクセスの有無やアクセス元等の分析のため、アクセスログを確実に取得する設定を行うこともまた強く推奨致します。



ホンダ社員の個人情報を含む1億3400万件ものデータがクラウド上でダダ漏れ状態にあったことが発覚

本田技研工業（ホンダ）が社内で使用しているElasticsearchのデータベースが、特別な設定なしでアクセスできる状態にアクセスされていることをCloudflareで働くJustinさんが発見しました。

Honda leaks database with employee computer data
<https://infosec.siftlab.eu/2019/07/31/honda-motor-company-leak/>

Justinさんが発見したのは、ホンダ社内ネットワークで稼働するデータベース。データベース内に格納されているデータは、「ホンダの内部ネットワークのログのようなもの」です。Justinさんは述べています。データベースには多くの個人情報が含まれており、それは、個人情報、メールアドレス、連絡先情報、エンジンID、エンジンソフトウェア、ソフトウェアのバージョンなどの情報が含まれていたとのこと。なお、Justinさんは問題を発見したのと同様に連絡し、セキュリティチームが既に問題を解決済みであるため、記事作成時点ではデータベースへのアクセスは不可能になっています。

●夏季休暇における情報セキュリティに関する注意喚起、IPA呼びかけ

<https://www.ipa.go.jp/security/topics/alert20190801.html>



このニュースをザックリ言うと…

- 多くの企業が長期休暇となるお盆の時期を迎えるにあたり、8月1日（日本時間）にIPAより、情報セキュリティに関する注意喚起が出されています。
- システム管理者が長期間不在になることにより、ウイルス感染や不正アクセス等のインシデント発生に気がつくに遅く対処が遅れてしまう可能性、および**従業員等が友人や家族と旅行に出かけた際のSNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性**を指摘しています。
- 休暇前にシステムのセキュリティ対策が十分に確認すること、休暇期間中のインシデント対応体制や関係者への連絡方法を調整すること、および休暇明けには不正アクセス・侵入等の痕跡をサーバ等のログから確認することを呼びかけており、実施すべき項目をまとめています。

AUS便りからの所感等

- IPAおよびJPCERT/CCでは、毎回長期休暇の前に、組織内に常駐する人が少なくなる等**「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得る**ことを鑑み、そういった問題にも早く確実に対応することへの注意を促しています。
- 参考として挙げられている相談事例は「佐川急便や日本郵便をかたる不在通知のSMSが届きフィッシングサイトへ誘導された、あるいは不正なAndroidアプリをインストールするよう要求された」というケースですが、特に組織で配布されたモバイル機器が情報流出や踏み台の餌食となることはその組織に打撃となる可能性が高いため、改めて注意を払うようにしましょう。
- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言えます。



夏休みにおける情報セキュリティに関する注意喚起

情報処理推進機構（IPA）は、2019年8月1日、独立行政法人情報処理推進機構（IPA）から、

多くの人が夏休みや長期休暇となるお盆の時期を迎えるにあたり、IPAが呼びかけている長期休暇における注意喚起、セキュリティ対策に関する事項です。

組織内のセキュリティ対策が十分に確認されていない、関係者への連絡方法が不明である、夏休み期間中は関係者への連絡方法が不明である、ウイルス感染や不正アクセス等の被害が発生した場合の対応が不明である、SNSへの書き込みにより踏み台の餌食となるなど、関係者によっては関係者の個人情報や機密情報が流出する可能性があります。このような事態を防ぐため、（1）組織内のセキュリティ対策、（2）関係者への連絡方法、（3）関係者の個人情報や機密情報の保護について関係者へ注意喚起をお願いします。

- 関係者への連絡方法を事前に確認してください。
- また、長期休暇に際して、関係者への連絡方法やセキュリティ対策を確認をお願いします。
- 関係者への連絡方法を事前に確認してください。

関係者に連絡がとれない状況に陥らないよう、関係者への連絡方法を事前に確認をお願いします。