

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。

●愛知県、新型コロナウイルス感染者約500件の非公開情報を誤って公開

https://www.47news.jp/national/new_type_pneumonia/4784153.html
<https://www.pref.aichi.jp/site/covid19-aichi/pressrelease-ncov200505.html>



このニュースをザックリ言うと…

- 5月5日(日本時間)、愛知県庁より、**県内での新型コロナウイルス感染者の非公開情報を誤って県Webサイトに公開**していたと発表されました。
- 対象となるのは、**同4日までの感染症発生事例に関する患者のべ495人分全員**についてで、含まれていた情報は**入転院先医療機関・入退院日・発生届提出保健所・クラスターの分類**となっており、うち**396人分については氏名も**含まれていたとされています。
- 5日午前9:30~10:15の間、感染症に関するページに掲載される「**県内発生事例一覧表**」に、誤って非公開情報が含まれた状態で掲載されていたことが問合せで発覚したとのことです。

AUS便りからの所感等

- 県では「**県内発生事例一覧表**」をExcelファイルで作成・管理し、そこから非公開情報を削除した上でExcelおよびPDFに変換したものを掲載していたところ、5日に掲載するファイルについては**非公開情報を削除し忘れた上、別の職員によるペアチェックが連休中のために行われなかった**ことが原因としており、今後はペアチェックの徹底や、PDFのみの掲載に切り替える等の対策をとるとしています。
- 感染者に対する風評被害が特に地方において問題となっている中、**今回のようなセンシティブな情報の掲載は痛恨と言え、全国の自治体等において決して対岸の火事ではありません**。
- **非公開情報を含むデータから公開用のデータファイルが自動的に生成されるようなシステムや、Web上から適切な内容のみが表示されるか事前に確認**するための、実際のWebサイトと同様の内部環境等も、導入を検討すべきと思われます。



新型コロナウイルス感染症ページへの患者に関する非公開情報の掲載について

[通常ページに戻る](#) 掲載日:2020年5月5日更新

新型コロナウイルス感染症ページへの患者に関する非公開情報の掲載について

愛知県新型コロナウイルス感染症に関するWebページ上に、本日午前9時30分頃から午前10時15分まで、県内発生事例1例目から495例目までの患者に関する非公開情報を誤って掲載しました。
このような事態を招いたことを深くお詫びするとともに、今後、ダブルチェック等の対応を徹底し、再発防止に努めてまいります。

1 経緯

- 5月4日(月曜日)午後9時30分頃
愛知県新型コロナウイルス感染症に関するWebページに、「県内発生事例一覧表」を5月5日(火曜日)午前9時15分に掲載されるよう設定した。(患者個人情報も掲載されたファイルを誤って登録)
- 5月5日(火曜日)午前9時30分頃
愛知県新型コロナウイルス感染症に関するWebページに、上記「県内発生事例一覧表」が掲載された。
- 同日 午前10時5分頃
県民の方から、「県内発生事例一覧表」に個人情報掲載されている旨の問合せが電話であった。(同様の問合せが他に2件あり。)
- 同日 午前10時15分頃
当該Webページから誤って掲載された「県内発生事例一覧表」を削除し、閲覧できないようにした。

●4月のフィッシング報告件数、1万件を超える…対策協議会発表

<https://this.kijii.is/630919639692133473>
<https://www.antiphishing.jp/report/monthly/202004.html>

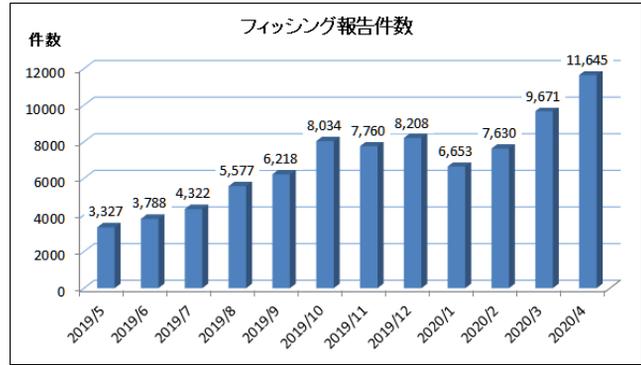


このニュースをザックリ言うと…

- 5月1日(日本時間)、フィッシング対策協議会より、4月に同協議会に寄せられたフィッシング報告状況が発表されました。
- **4月度の報告件数は11,645件**(3月度9,671件、2月度7,630件)で、2005年の協議会設立以来初めて**10,000件を超えている**他、フィッシングサイトのURL件数は4,283件(3月度4,136件)となっています。
- **Amazon・Apple・LINE・楽天を騙るフィッシング**が報告の多数を占める傾向が数ヶ月以上続いている模様で、特に**Amazonを騙るフィッシングは前月度の約1.4倍の報告**があったとのこと。

AUS便りからの所感

- 2月度から3月度で2,041件の増加、3月度から4月度で1,974件の増加と、**毎月度の報告件数が約2,000件ずつ増加**しており、新型コロナウイルス感染症の影響による**通信販売やマスク需要の増加を狙ったことによる激増**とみられます。
- 同対策協議会からは4月にも、住信SBIネット銀行・ヨドバシカメラ・au(AUS便り 2020/04/27号参照)あるいはNTTドコモのdアカウントに関する警告を騙るフィッシング(https://www.antiphishing.jp/news/alert/nttdocomo_20200430.html)が報告されています。
- **Webブラウザやメーラー、アンチウイルスおよびUTMによるアンチフィッシング機能を有効化**するとともに、当AUS便りや同協議会でもたびたび挙げている回避策として、利用しているサービスの正規のサイトへは、**不審なメール・SMS上のリンクからではなく、正規のアプリや事前に登録したブックマークからアクセス**するよう是非とも心がけてください。



●1つのパスワード、平均して2.7アカウントで使い回されている…1万人超調査

<https://news.mynavi.jp/article/20200509-1033329/>
<https://www.balbix.com/resources/state-of-password-use-report-2020/>



このニュースをザックリ言うと…

- 5月7日(現地時間)、セキュリティベンダーのBalbix社より、1万アカウントを対象としたパスワードの利用状況に関する調査結果が発表されました。
- 発表によれば、**99%以上のユーザーが、仕事用のアカウントで、あるいは仕事用アカウントとプライベートアカウントの間で、同じパスワードを使い回している**とのこと。
- また、**平均して、1つのパスワードが2.7アカウントで共有**されているとしています。

AUS便りからの所感

- 発表のあった5月の第1木曜日は2013年に大手セキュリティベンダーのMcAfee社(当時Intel Security)によって「World Password Day」に制定されており、海外において啓発活動が行われています。
- パスワードの使い回しを行っているサービスの**いずれかで攻撃が発生しパスワードが流出した場合、他のサービスもたちどころに不正ログインの影響を受ける可能性がある**ことはここ何年もの間注意喚起がされており、今後も折に触れて啓発は続くことでしょう。
- **全く同じパスワードを使用せず、推測されにくい強力なパスワードを利用**すること、場合によっては**パスワード管理ツールを用いての生成や管理**を行うこと、さらには**多要素認証の利用も視野**に入れたアカウントの保護を常に意識することが重要です。



1つのパスワード、平均して2.7アカウントで使い回されている - 1万人超調査

後藤大地 © 2020/05/09 18:32

Balbixはこのほど、「State of Password Use Report 2020 | Balbix」において、99%以上のユーザーが仕事用のアカウントでパスワードを使い回しているほか、仕事用アカウントとプライベートアカウントの両方でさらに同じパスワードを使い回していると伝えた。平均して、1パスワード当たり2.7アカウントで共有されているという。

