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。

## ● KDDIのISP向けメールシステムから最大1,422万件のアカウント情報流出…@nifty・BIGLOBE・J:COM等影響

https://pc.watch.impress.co.jp/docs/news/2119390.html
https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-71_4593/kddi_nr_s-71_4593_pdf_01.pdf
https://support.biglobe.ne.jp/news/news796.html
https://support.nifty.com/topics/2026/06232410
https://notices.jcom.co.jp/notice/95116.html

### このニュースをザックリ言うと･･･

- 6月23日(日本時間)、KDDI株式会社より、同社がISP事業者に提供しているメールサービスが不正アクセスを受け、メールアカウント情報が流出した可能性があると発表されました。

- 影響を受けたとされるのは、@nifty、BIGLOBE、「J:COM NET」およびJCOM系CATV、STNet社「ピカラ光サービス」他、ctc社「コミュファ光」他、KDDIウェブコミュニケーションズ社「CPI」の計6社が提供するメールサービスのアドレス・パスワード最大1,422万件とされています。

- 6月17日にKDDI社において不正アクセスを確認しており、各事業者からは該当するユーザーに対しパスワードの変更が呼び掛けられています。

### AUS便りからの所感等

- 特に@niftyからは、@niftyメールの対象ユーザーについて、指定の日時までに更新されなかった「メールパスワード」を無効化するとしており、対象のユーザーであるか確認して対応するとともに、デフォルトでは@niftyの回線サービスやWebサイトへのログインに用いられるパスワードがメールパスワードと同一であるため、こちらも更新することが推奨されています。

- パスワードの扱いについては既に「推測されにくいものを設定する」「複数のサービスで使い回さない」「定期的な変更は推奨しない」といったことが10年以上呼び掛けられていますが、今回のように流出が発覚したアカウントについては可及的速やかにパスワードを変更すること、またそこで設定されていたものと同じパスワードを他のサービスで使っていた場合、「リスト型攻撃」で芋づる式に不正ログイン攻撃を受ける恐れがあるため、そちらもまた別のパスワードに変更することが重要です。

- 事業者から各対象ユーザーに対しメールで連絡を行っている中、既に流出したメールアドレスを悪用してフィッシングを行っている事例も確認されており、このような通知メールが本物か、メーラー・アンチウイルスソフト・UTM等のアンチフィッシング機能で確認するとともに、本文にURLが記載されていたとしてもまずは利用しているサービスのトップページからアクセスする(フィッシング回避のため事前にブックマークしておく)等、普段から慎重な行動を心掛けることにより、今回のようなインシデントに便乗したフィッシングに対しても被害を最小限に留めることが期待できます。

Impress Watch

**KDDI、ISPメールシステムに不正アクセス、最大1,422万件漏洩か。BIGLOBE、niftyなど影響**

宇都宮 充　2026年6月23日 18:31

漏洩した可能性があるのは、本システムを利用した各ISP事業者のメールサービスにて作成されたメールボックスに紐づくメールアドレスとパスワード。解約したユーザーや、休眠アカウントのものも含まれ、件数は最大1,422万件にのぼるとしている。影響を受けるISP事業者およびメールサービスは以下の通り。

- STNet
  「ピカラ光サービス」、「ピカラモバイルサービス」、「お仕事ピカラサービス」に係るメールサービス
- KDDIウェブコミュニケーションズ
  レンタルサーバー「CPI」のメールサービス
- JCOM
  「J:COM NET」とケーブルテレビ事業者向けメールサービス
- 中部テレコミュニケーション
  コミュファ光・ビジネスコミュファのメールサービス
- ニフティ
  @nifty メール
- ビッグローブ
  BIGLOBEメール

## ●官庁・大学サイト改ざん相次ぐ…ワールドカップ便乗の詐欺行為への誘導

https://www.sankei.com/article/20260612-FMXGZPRVLZKV7AKLSALKQ3GXUU/
https://www.sankei.com/article/20260618-RXSFRK6ZFJCZJA27DHMMAMUQXY/
https://www.wakayama-u.ac.jp/news/2026061700015/
https://www.seijo.ac.jp/news/cvt4qu0000019vig.html
https://www.keio.ac.jp/ja/news/20260619-2/
https://rocket-boys.co.jp/security-measures-lab/fifa-world-cup-2026-phishing-campaign/

### このニュースをザックリ言うと･･･

- 6月12日および同18日(日本時間)、産経新聞より、海上保安庁および複数の大学のWebサイトが改ざんされ、「FIFAワールドカップ2026」の映像配信を騙るページが表示されていたと報じられています。

- 同紙が報じた範囲では、被害を受けたのは海上保安庁・和歌山大学・成城大学・慶應義塾大学のバーチャル見学ページ等とされ、また検索サイトで「ワールドカップ」等と検索した結果にこれらのページが表示されるようになっていたとしています。

### AUS便りからの所感

- ワールドカップやオリンピック等スポーツイベントから、地震・台風といった事故・災害に至るまで、世界が注目する大きな出来事には必ず便乗したサイバー犯罪が起こり得ます。

- 今回のワールドカップにおいても、この他、ホテル等の予約サイトの偽物や、FIFA公式サイトの複製サイト等が報告されています。

- 非公式で安価に何らかのサービスが受けられるようなものを安易に検索して素性の知れないサイトに軽率に個人情報・クレジットカード番号等を入力することは決して行わないようにし、また不審な宣伝や通知を騙ったSMSやメールを受け取った際にも、セキュリティ関連団体・組織からの注意喚起、本物の業者からのメールやSMSの運用に関するポリシーを確認し、無闇にリンクをクリックしない等に注意してください。

海上保安庁と和歌山大のサイトが乗っ取り被害　「W杯放送　無料生配信」サイトに書き換え

2026/6/12 20:08

西山 諒　事件・疑惑　サイバー攻撃




改竄された海上保安庁のサイトからリダイレクトされるページ。サッカーのワールドカップの無料視聴をうたっている

海上保安庁と和歌山大のホームページの一部が、サッカーのワールドカップ（W杯）の「映像配信」をうたうページに改竄されていたことが12日、分かった。ともに、ページの公開を停止し、内部情報の流出などの被害状況を調査している。

改竄されたのは、海保の「坪田港防波堤灯台」のバーチャル見学ページと和歌山大の「バーチャル ツアー」のページ。接続すると、「W杯放送　無料生配信」などと、無料視聴をうたうページに移動するよう設定が変更されていた。

## ● D-Link製ルーター等の古い機種に感染か、ボットネット構築するマルウェア「AryStinger」に注意喚起

https://news.mynavi.jp/techplus/article/20260625-4618569/
https://www.bleepingcomputer.com/news/security/arystinger-botnet-infected-thousands-of-d-link-routers-worldwide/

### このニュースをザックリ言うと･･･

- 6月17日(中国時間)、中国のセキュリティ企業・奇安信(Qianxin)より、D-Link社製のルーター等でボットネットを構築するマルウェア「AryStinger」の存在を確認したとして注意喚起が出されています。

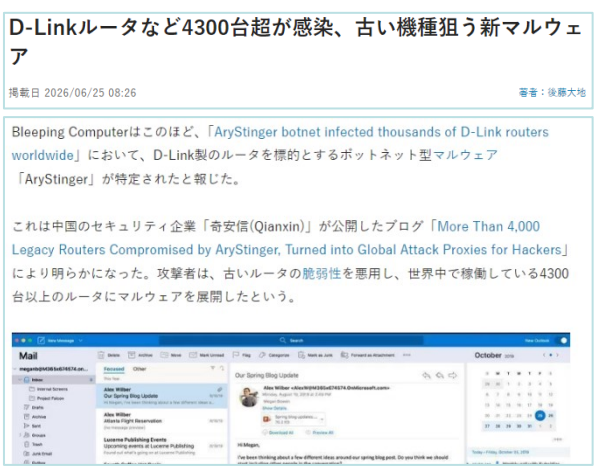
- AryStingerは古い機種のルーター4,300台以上の脆弱性を突いて拡散されており、他にもLinksys製機器やQNAP製NAS等がターゲットとなったとしています。

- 被害を受けた機器が設置されている主な地域・国は韓国(約48.45%)と中国(約31.82%)、次いでスウェーデン(約6.4%)、マレーシア(約3.5%)、シンガポール(約2.5%)となっています。

### AUS便りからの所感

- 今回取り上げられたのは日本国外での被害事例が多いものではありますが、例えば過去に猛威を振るった「Mirai」は、NICTERプロジェクトによる2025年10月～12月の調査(https://blog.nicter.jp/2026/03/nicter_statistics_2025_4q/ )によれば、現在も国内で日々約180～790台程度が活動していると推測されています。

- 組織内の機器を確実に管理下に置き、サポートが切れた古い機器は確実にリプレースし、サポート中の機器についてもファームウェア等を常時最新に更新できるようにする体制を整えることが肝要です。



D-Linkルータなど4300台超が感染、古い機種狙う新マルウェア

掲載日 2026/06/25 08:26　　著者：後藤大地

Bleeping Computerはこのほど、「AryStinger botnet infected thousands of D-Link routers worldwide」において、D-Link製のルータを標的とするボットネット型マルウェア「AryStinger」が特定されたと報じた。

これは中国のセキュリティ企業「奇安信(Qianxin)」が公開したブログ「More Than 4,000 Legacy Routers Compromised by AryStinger, Turned into Global Attack Proxies for Hackers」により明らかになった。攻撃者は、古いルータの脆弱性を悪用し、世界中で稼働している4300台以上のルータにマルウェアを展開したという。