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。

●快活CLUBから不正アクセスで個人情報約730万件流出か…昨年の流出トップ3合計に並ぶ規模

https://www.itmedia.co.jp/news/articles/2501/28/news121.html
https://ir.aoki-hd.co.jp/ja/news/news/auto_20250121553444/pdfFile.pdf
https://ir.aoki-hd.co.jp/ja/news/news/auto_20250127555905/pdfFile.pdf

このニュースをザックリ言うと･･･

- 1月21日(日本時間)、AOKIホールディングス社より、「快活CLUB」および「FiT24」を運営する子会社・快活フロンティア社のサーバーが不正アクセスを受け、両サービス利用者の個人情報が流出した可能性があると発表されました。

- 同28日に発表された詳報では、被害を受けたとみられるのは、2015年10月1日以降の快活CLUB会員、2019年3月25日以降の同仮会員(店舗で会員登録していない者)、および2018年10月30日以降のFiT24・FiT24インドアゴルフ会員の、合計7,290,087人分の氏名・性別・住所・電話番号・生年月日および会員番号等の会員情報とされています。

- 同18日にサーバーへの不正アクセスを検知、当該サーバーをネットワークから切り離す等の対策を行い、調査した結果、会員アカウントを管理するシステムにアクセスされた形跡があったとのことです。

AUS便りからの所感等

- 流出規模は2024年に発覚した上場企業からの個人情報流出事案(東京商工リサーチ発表、https://www.tsr-net.co.jp/data/detail/1200872_1527.html)で最も多かった東京ガス(4,163,090人、AUS便り2024/07/18号参照)、さらには続くトップ3(三菱電気ホーム機器の2,310,000人、SOMPOホールディングスの991,000人)の合計(7,464,090人)に並ぶものとされています。

- 身分証明書(運転免許証など)情報・クレジットカード情報・メールアドレスおよび会員アプリのパスワードは被害を受けたサーバーでの管理でないため被害対象に含まれておらず、また現時点で実際の流出～二次被害の事実は確認されてないとしています。

- 不正アクセスによる個人情報流出の事例における侵入経路は、VPN装置からの侵入(脆弱性の悪用、推測されやすいパスワードの突破等)、管理者に対するフィッシング攻撃等様々で、今回の事例についてどうだったかは今後発表があるとみられますが、ともあれ社内ネットワークないし個人情報等を保存するサーバーへの不正アクセスの可能性を抑止するため、PC・サーバー・ネットワーク機器等についてOS・ファームウェアおよび使用アプリケーションを最新のバージョンに保つ、VPN・サーバーのログインアカウントに推測されやすいパスワードが設定されている(＆その状態で使用されないまま残されている)ものは削除する、アンチウイルス・UTM等による防御を固める、等の様々な防衛策の実施が肝要です。

ITmedia NEWS

「快活CLUB」への不正アクセスで続報　会員の一部個人情報729万件漏えいか

2025年01月28日 11時36分 公開　[ITmedia]

漫画喫茶「快活CLUB」を運営する快活フロンティア（神奈川県横浜市）は1月28日、21日に公表した外部からの不正アクセス被害について、会員の一部個人情報729万87件が漏えいした可能性があると発表した。

「快活CLUB」への不正アクセスで続報　会員の一部個人情報729万件漏えいか

対象者は、快活CLUB会員（2015年10月1日～25年1月20日に登録した一部）と快活CLUB仮会員（19年3月25日～25年1月20日に登録した一部）、同社の運営するフィットネスジム「FiT24」会員および室内ゴルフ練習場「FiT24インドアゴルフ」会員（18年10月30日～23年4月1日に登録した一部）。

● IPA「情報セキュリティ10大脅威 2025」、組織側に「地政学的リスクに起因するサイバー攻撃」初登場

https://www.ipa.go.jp/security/10threats/10threats2025.html

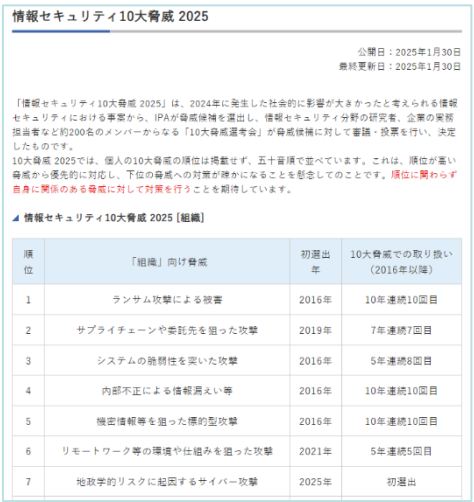
このニュースをザックリ言うと・・・

- 1月30日(日本時間)、IPAより「情報セキュリティ10大脅威 2025」の概要が発表されました。
- 2024年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約200名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。
- なお、昨年発表の「10大脅威 2024」以降、個人向け脅威については「順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念」して順位付けは行わず、「順位に関わらず自身に関係のある脅威に対して対策を行う」ことを期待するとしています。
- 今後、2月末に組織側の10大脅威に関する詳細の解説書が発表(個人側は5月末)される等、追加コンテンツが随時公開される予定となっています。

AUS便りからの所感

IPA 独立行政法人 情報処理推進機構

- 個人側の10大脅威は「インターネット上のサービスへの不正ログイン」「クレジットカード情報の不正利用」「ネット上の誹謗・中傷・デマ」「不正アプリによるスマートフォン利用者への被害」が10年連続、これら含め9つが6年以上連続で入るなど、顔触れは完全に固定されています。
- 組織側の10大脅威も8つが5年以上連続でランキング入り、うち「ランサムウェア攻撃」「サプライチェーンや委託先を狙った攻撃」が3年連続で1・2位となっている中、7位に「地政学的リスクに起因するサイバー攻撃(国家の関与が疑われる攻撃等)」が初登場、8位には5年ぶりに「DDoS攻撃」が入っています。
- 12月にJNSAから発表された「2024セキュリティ十大ニュース(https://www.jnsa.org/active/news10/)」では国内で話題になった個々のインシデントが多く取り上げられる等、特に年末年始あるいは半期・四半期においては、大手セキュリティベンダーや関連団体等より、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度等における業界の動向予測等がリリースされますので、自分自身や自組織に関連するもの以外も含め各種脅威について知識を得ること、過去に得た知見についても随時更新していくことを推奨致します。



情報セキュリティ10大脅威 2025

公開日：2025年1月30日
最終更新日：2025年1月30日

「情報セキュリティ10大脅威 2025」は、2024年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。
10大脅威 2025では、個人の10大脅威の順位は掲載せず、五十音順で並べています。これは、順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念してのことです。順位に関わらず自身に関係のある脅威に対して対策を行うことを期待しています。

情報セキュリティ10大脅威 2025【組織】

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い(2016年以降)
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出

● Google Chromeのセキュリティアップデートリリース、開発ツールに脆弱性

https://forest.watch.impress.co.jp/docs/news/1658496.html
https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_28.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-0762

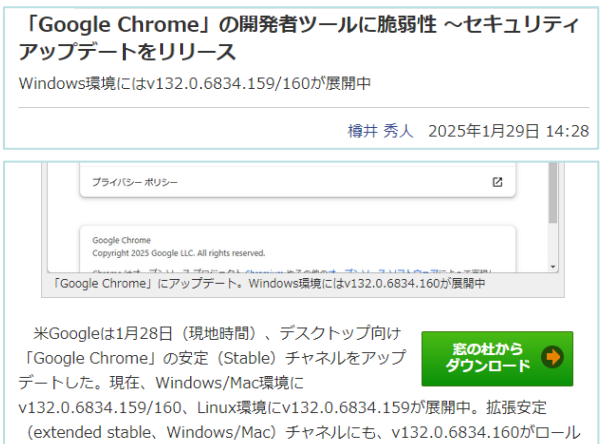
このニュースをザックリ言うと・・・

- 1月28日(現地時間)、GoogleよりChromeブラウザーの最新バージョン(v132.0.6834.159/.160)がリリースされました。
- 開発者ツール(DevTools)に存在する脆弱性「CVE-2025-0762」を含む2件の脆弱性を修正するセキュリティアップデートとなっています。
- CVE-2025-0762の危険度は中程度で、CVEに掲載された情報では、悪意のある拡張機能から攻撃される可能性があるとしています。

AUS便りからの所感

Impress Watch

- 最近も既存の拡張機能の更新版を騙った悪意のある拡張機能がGoogle公式の拡張ストアに公開される事案(AUS便り 2025/01/09号参照)等が発生しており、拡張機能のインストールにあたってはネット上のレビュー・報告に注意してください。
- 2週間前にメジャーバージョン132となりましたが、程なく133のリリースが見えてきており、そこでも多数の脆弱性の修正が予想されます。
- Chromeブラウザーは日本時間の毎週水曜日(あるいは木曜日)がセキュリティアップデートのリリースの目安となりますので、「ヘルプ」→「Google Chromeについて」(あるいは chrome://settings/help)でバージョン情報を確認し、手動でアップデートを行う習慣をつけるのが肝要です。



「Google Chrome」の開発者ツールに脆弱性 ～セキュリティアップデートをリリース

Windows環境にはv132.0.6834.159/160が展開中

樽井 秀人　2025年1月29日 14:28

プライバシー ポリシー

Google Chrome
Copyright 2025 Google LLC. All rights reserved.

「Google Chrome」にアップデート。Windows環境にはv132.0.6834.160が展開中

米Googleは1月28日（現地時間）、デスクトップ向け「Google Chrome」の安定（Stable）チャネルをアップデートした。現在、Windows/Mac環境にv132.0.6834.159/160、Linux環境にv132.0.6834.159が展開中。拡張安定（extended stable、Windows/Mac）チャネルにも、v132.0.6834.160がロールアウトされている。

窓の杜からダウンロード