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。

● 4桁のPINコード、最も頻繁に使われるのは「1234」「1111」「0000」等

https://www.phonearena.com/news/do-not-use-these-pin-numbers_id170732
https://www.abc.net.au/news/2025-01-28/almost-one-in-ten-people-use-the-same-four-digit-pin/103946842
https://internet.watch.impress.co.jp/docs/yajiuma/2017067.html

このニュースをザックリ言うと･･･

- 5月24日(現地時間)、スマートフォン等を取り上げるネットメディア「PhoneArena」において、スマホで頻繁に使用されているという4桁のPINコード上位50が取り上げられています。

- 流出したメールアドレス・パスワードのデータベース「Have I Been Pwned?(以下HIBP)」に保管されている2900万件のデータをAPIを用いて取得・分析したものとされています(なお、1月にオーストラリア放送協会(ABC)が取り上げた記事を元としており、そちらには頻度をビジュアル化した画像も掲載されています)。

- 最も頻繁に使われるのは「1234」で全体の9%、以下「1111(1.6%)」「0000(1.1%)」「1342(0.6%)」「1212(0.4%)」となっており、以下同じ数字の繰り返しや西暦(ユーザーの生まれた年とみられる)が多くを占めています。

AUS便りからの所感等

- HIBPから取得したとするデータは実際に設定されていたPINコードから取ったデータベースではなく、パスワードとして4桁のPINコード全てを試行した(即ち、流出したパスワードのうち4桁の数字のみからなるものに絞った)結果を当てはめたとみられます。

- 上位50で前述したパターンに当てはまらないとみられるもののうち、4位の「1342」は「1234」を組み替えただけのもの、28位の「2580」はテンキー上の並びで縦に順番に押したものとのことです。

- 50位以下も併せると、誕生日(「日・月」の順番も含む)を使用しているとみられる数字も頻出しており、キャッシュカード・クレジットカードの暗証番号と同様の傾向が見受けられます。

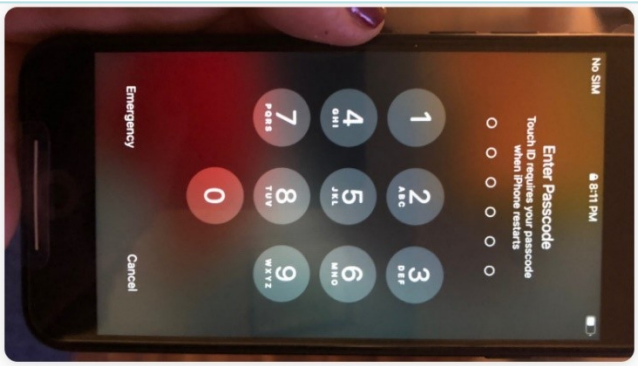
- PINコードに対する限られた試行回数で、攻撃者が真っ先に試す数字のパターンはある程度限定されるものと思われますので、そういった数字を避け、より長い桁数や指紋認証等が使えるならばそれを使うこと等を心掛けるべきです。

PHONE ARENA

If you are using these PIN numbers on your iOS or Android phone, change them immediately

These are the 50 PIN codes you need to avoid using on your iPhone.

By Alan Friedman PUBLISHED: MAY 24, 2025, 8:14 PM 5 COMMENTS



PINs are important. You probably have a four-digit PIN to guard access to your phone, your bank account, and other online portals that you want to keep others away from. The problem, according to a report from the Australian Broadcasting Corporation (ABC), is that the PINs most used are so popular that *someone might be able to break into a phone they found or stole*. ABC went to website "Have I Been Pwned" and analyzed 29 million PIN codes. What they found is pretty disturbing.

●イベント申し込みフォームのURL誤掲載…入力者30名分の個人情報、他者から閲覧可能状態に

https://cybersecurity-jp.com/news/109929
https://g-sleep.jp/archives/805

このニュースをザックリ言うと・・・

- 5月21日(日本時間)、ヘッドスパ店「睡眠専門ヘッドスパ Dr.ぐっすり～」(以下・同店)より、同店のイベント参加申し込みフォームの掲載ミスにより、参加者の個人情報が他者から閲覧可能な状態にあったと発表されました。

- 対象となるのは、新店舗オープン記念イベント申し込み用のGoogleフォームから申し込みを行った30人分の氏名・電話番号・メールアドレスおよび要望・質問内容となっています。

- 店舗Instagramへの投稿にフォームのURLを掲載した際、誤って編集用URLを掲載したとのことです。

AUS便りからの所感

- Googleフォームへの回答内容を閲覧・管理する「編集者ビュー」がデフォルトで特定のGoogleアカウントのみアクセス可能な「制限付き」の設定であるところ、アカウントを持たない管理者との共有のため「リンクを知っている全員」へ変更したこと、また公開ページへのリンク貼り付けの際に「回答者へのリンクをコピー」で表示されるURLではなく、アドレスバーに表示されている編集者ビューのURLを貼り付けたことが原因と推測されます。

- Googleフォームでは2024年12月に現行仕様への変更があり、その際にも巷では多少の混乱が生じていた様子が窺えます。

- このようなリンクの取り違えはGoogleドライブやその他オンラインストレージサービスでも往々にして起き得るものであり、「アカウントを持っていない一部の相手と情報を共有したい」という状況が発生した場合には外部への情報漏洩の恐れに特に注意を払い、リンク貼り付け後にはプライベートウィンドウ等非ログイン状態でのアクセスにより、適切なページ等が表示されているか確認することが肝要です。

Cyber Security.com

公開日：2025.05.29 | 最終更新日：2025.05.29

Googleフォーム設定ミスで利用者の情報が第三者閲覧可能に｜睡眠専門ヘッドスパ Dr.ぐっすり～

無料 メルマガ登録でプレゼント！書籍「セキュリティ対策の基礎知識」

画像：睡眠専門ヘッドスパ Dr.ぐっすり～より引用

睡眠専門ヘッドスパ Dr.ぐっすり～は2025年5月21日、同社が運営するインスタグラムのストーリーズにて公開したイベント用Googleフォームにて設定ミスがあり、利用者30名の個人情報を第三者が閲覧できる状態にした旨、発表しました。

●DNSサーバー「BIND」9.20・9.21系にDoS攻撃の脆弱性…影響有無の確認を

https://japan.zdnet.com/article/35233324/
https://jprs.jp/tech/security/2025-05-22-bind9-vuln-tsig.html
https://kb.isc.org/docs/cve-2025-40775

このニュースをザックリ言うと・・・

- 5月22日(日本時間)、DNSサーバー「BIND」に1件の脆弱性が発見されたとして、修正バージョン(9.20.9, 9.21.8)がリリースされました。

- 脆弱性は最新メジャーバージョン9.20系(9.20.0～9.20.8)および開発版の9.21系(9.21.0～9.21.7)にのみ存在し、9.18系には影響しないとのことです。

- 悪用により、BINDのサーバープロセスを不正にダウンさせられるという、外部からのDoS攻撃に繋がり得るものとなっており、同日にはJPRS等より、該当するバージョンを利用している場合は速やかにアップデートするよう注意喚起が出ています。

AUS便りからの所感

- BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあり、近年は殆どの脆弱性がサーバープロセスのダウンやパフォーマンス低下といったDoS攻撃に繋がるものとなっています。

- 主なLinuxディストリビューション(安定板)では、Ubuntu 24.10・25.04についてセキュリティアップデートがリリースされている一方、同24.04以前やDebian、およびRHELとその派生であるRocky Linux・Almalinux等については、BIND 9.18系以前を使用しているため影響は受けないとのことです。

- 代替として他のソフトウェアあるいはAWSのRoute53といったクラウドサービスを使用するケースも多くなっているものの、メーカー製ネットワーク機器においてBINDを組み込んでいるケース等にも影響し得ることを鑑み、使用しているソフトウェア・機器のファームウェアについて脆弱性の有無やアップデートのリリース状況を随時確認すること、リリースされ次第適用を行うことが肝要です。

ZDNET

DNSサーバーソフト「BIND 9」に新たな脆弱性情報、深刻度「高」の評価

ZDNET Japan Staff 2025-05-22 15:03

シェアする 2 | ポスト | B! 1 | noteで書く | Pocket 8

Internet Systems Consortium（ISC）は米国時間5月21日、DNSサーバーソフト「BIND 9」に関する脆弱（ぜいじゃく）性「CVE-2025-40775」の情報を公開した。脆弱性の悪用攻撃によってnamedが異常終了する恐れがあり、ISCは利用者に修正版の適用を呼び掛けている。

ISCによると、脆弱性が存在するのは、BIND 9.20.0～9.20.8および同9.21.0～9.21.7で、リゾルバーと権威サーバーの双方に影響がある。脆弱性はISC内部のテストで見つかり、情報公開時点で悪用は確認されていないという。深刻度で「高」、CVSS値（最大10.0）で「7.5」と評価している。なお、9.18.0より前の古いバージョンについては評価していない。