

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。

●電車内広告のQRコードから不審な文書へ…広告元の大学が注意喚起

<https://www.itmedia.co.jp/news/articles/2510/21/news093.html>
<https://x.com/uctokyo/status/1980433168881922461>
<https://togetter.com/li/2618526>



このニュースをザックリ言うと…

- 10月20日(日本時間)頃、X(旧Twitter)上において、京王線車内等に掲示された**広告のQRコード**から**不審なPDFの表示に誘導**されたとする報告がありました。
- QRコードのURLはGoogle Drive上のものとなっており、PDF文書は多数のYouTube動画やGoogle Drive上の別の文書にリンクされていた模様です。
- 同21日には**当該広告を掲出した電気通信大学**より、当該広告には**本来QRコードを記載しておらず**、悪意のあるページへの誘導の可能性があるため、**このようなコードを読み込まないよう注意喚起**が出されています。

AUS便りからの所感等

- 第三者が**広告に勝手にQRコードを貼り付けた**ものとみられ、またPDF文書の内容も、同大学と全く無関係の、第三者によるWebサイト・動画の宣伝目的とみられます。
- **QRコードをフィッシング詐欺に悪用するケース**は数多く、コード決済サービスを騙って**不審なサイトに誘導するコード**を送り、**偽のアプリをインストール**させる、**外部サービスに連携**させる、あるいは**個人情報を入力**させることで**不正な支払を行わせる**手口等が知られており、ユーザー側にはこういった**手口**の存在を熟知し、**本物の決済サービス側からの注意喚起を確認**すること、外部サイトにアクセスするような**不審なコードのスキャンを求められた場合はアクセス先URLが明らかに不審なものでないか確認**するよう心掛けましょう。
- 今回のケースに類似した例として「**実店舗で決済用に提示していたコードの上に偽のコードが貼りつけられ、支払代金を騙し取られた**」事例が報告されていますが、偽の店舗がサービスに登録しているような場合、前述した手口よりも**不審がられることなく詐欺行為が行われる恐れ**がある上、**返金等の補償を受けられないこともある**とされ、**店舗側**においても**本物のコードに細工されないよう対策**する必要があるでしょう。

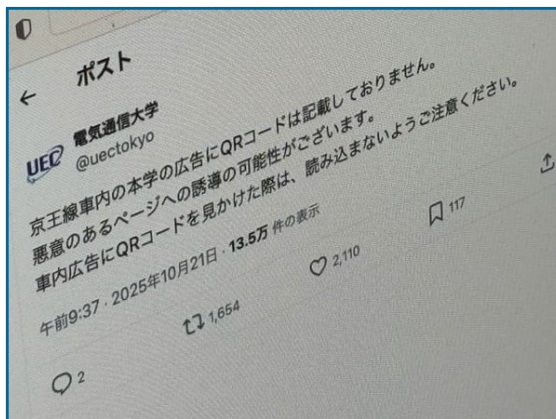


京王線の車内広告に“不審なQRコード” 電通大が注意喚起

© 2025年10月21日 13時23分 公開

[ITmedia]

電気通信大学は10月21日、京王線の車両内に掲出されている同大学の広告に「QRコードは記載していない」と公式Xアカウントで注意喚起した。X上では20日ごろから、車内広告にあったQRコードを読み込んだところ「よく分からんPDFに飛ばされた」という投稿が一部で注目を集めていた。



電気通信大学のポスト（出典：X）

乗客とみられるXユーザーが投稿した写真には、広告の「電気通信大学」という文字の下にQRコードが映っている。位置的に不自然さはなく、大学Webサイトへの誘導と受け取られそう。しかし実際に読み込んだ別のユーザーによるとGoogleドライブの共有ファイルのURLだったという。

●複雑さより長さ重視を…NISTパスワードルール改訂

<https://internet.watch.impress.co.jp/docs/yajiuma/2056544.html>

<https://www.malwarebytes.com/blog/news/2025/10/your-passwords-dont-need-so-many-fiddly-characters-nist-says>

<https://pages.nist.gov/800-63-4/sp800-63b.html>



このニュースをザックリ言うと…

10月10日(現地時間)、セキュリティベンダーのMalwarebytes社より、米国立標準技術研究所(NIST)が8月に更新した**デジタル認証に関するガイドライン「SP800-63B」**の、**パスワード設定に関する節**について言及されています。

本節では、**パスワードの内容**について「**印字可能なASCII文字とスペースを受け入れる必要**、さらにはUnicode文字を受け入れるべき」「**最低15文字以上**(多要素認証と組み合わせる場合は8文字以上)かつ**64文字まで受け入れるべき**」「**記号・数字・アルファベット大文字・小文字を含めるといった複雑性は要求しない**」とし、推測されやすい等脆弱なパスワードの「ブロックリスト」を使用することも推奨しています。

ユーザーにパスワードを**定期的に変更**することを「**要求してはならない**(ただしアカウント侵害の可能性がある場合は変更を要求する必要がある)」とし、またパスワードを忘れた際の**回復手段**として、出身地や母親の旧姓等いわゆる**秘密の質問**の登録を「**推奨しない**」とし、電子メール・SMS・音声もしくは郵便を用いることを推奨しています。

AUS便りからの所感



8文字程度で記号等を含めたパスワードよりも、**アルファベットだけでもより長いパスワードの方が**、推測されやすい単語でない限り**破られるのに時間がかかる**とされ、また複数の単語からなる(適宜スペース等で区切る)、いわゆる「**パスフレーズ**」も同様に強力でかつ**比較的記憶しやすい**とされており、**最大長を少なくとも64文字**としていることも、特にパスフレーズを利用する場合を考慮したものと考えられます。

ガイドラインではこの他にも**パスワード管理ツール**の使用、パスワード入力欄への**コピーアンドペースト**(Webサイトによっては禁止しているところも依然目立っています)を「**許可すべき**」等の記述がみられ、長年蓄積された「常識」を覆すためにまた長い年月がかかるとしても、**着実に適宜ルールを変えていくことを意識**すべきでしょう。

パスワードは、特殊文字などの「複雑さ」ではなく「長さ」を求めることを推奨 ~NISTがガイドライン更新

編集部 2025年10月21日 11:59

●特殊文字(&、%など)や数字、大文字の混在など「複雑さ」を求めない
複雑なパスワードを設定させようとしても、「password」が「Password1!」になるだけとしている。その代わり、次に挙げるように文字数を増やすことを推奨する意図がある。

●パスワードのみで認証する場合、長さを15文字以上に設定させる
多要素認証と併用する場合は8文字程度でもよいとしている。

●定期的なパスワード変更は求めない
漏えいなど、セキュリティ侵害が明らかになったタイミングでパスワードを変更するべきとしている。

●WSUSに脆弱性、Windows Serverに定例外パッチリリース

<https://forest.watch.impress.co.jp/docs/news/2057711.html>

<https://www.microsoft.com/en-us/msrc/blog/2025/10/202510-security-update/>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287>

<https://cybersecuritynews.com/hackers-exploiting-microsoft-wsus-vulnerability/>



このニュースをザックリ言うと…

10月25日(日本時間)、**マイクロソフト(以下・MS)より、Windows Server(2012・2012 R2・2016・2019・2022・23H2・2025)に対する定例外のセキュリティアップデート**がリリースされています。

Windows Server Update Services(WSUS)の脆弱性「CVE-2025-59287」を修正するもので、悪用により**サーバーを乗っ取られる可能性**があるとされています。

リリース時点で脆弱性を悪用するコードが出回っていたことから早急なアップデートの適用が求められています。

AUS便りからの所感



同15日の**月例アップデートで完全に対策されなかった脆弱性**とされており、今回のリリース後の同28日には**2800台のサーバーが未修正かつオンラインからアクセス可能な状態**にあるとするセキュリティ企業の報告もあります。

MSでは2024年にWSUSを非推奨としているものの、多くの企業で組織内へのWindows Update配信負荷対策のため依然利用されています。

特にWSUSを導入している場合は、月例アップデートと同様に**脆弱性の根本的対策のため必ず適用**すること、またWSUSが使用する**TCPポート8530・8531番についてくれぐれも不特定多数からアクセスされる状態でないか確認**することが肝要です。

Windows Serverのセキュリティパッチが緊急公開、「WSUS」にリモートコード実行の脆弱性

すでに概念実証(PoC)コードあり、できるだけ早い対応を

梅井 秀人 2025年10月24日 13:59

米Microsoftは10月23日(現地時間)、「Windows Server Update Services」(WSUS)のWSUS Reporting Web Serviceでリモートコード実行(RCE)の脆弱性(「CVE-2025-59287」)を確認したとして、更新プログラムを定例外(Out of Band: OOB)でリリースした。Windows Serverの各バージョンで、以下のパッチが提供中だ。

- Windows Server 2025 : KB5070881
- Windows Server バージョン 23H2 : KB5070879
- Windows Server 2022 : KB5070884
- Windows Server 2019 : KB5070883
- Windows Server 2016 : KB5070882
- Windows Server 2012 R2 : KB5070886
- Windows Server 2012 : KB5070887