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。

● Webサーバー証明書の最長日数、2026年3月から段階的に短縮へ …2029年3月からは47日に

https://news.mynavi.jp/techplus/article/20250417-3190551/
https://securityonline.info/ssl-certificate-validity-reduced-to-47-days-after-apple-proposal/

このニュースをザックリ言うと・・・

- 4月13日(現地時間)、Webサーバー証明書に関する認証局とブラウザーメーカーによる「CA/Browser Forum」において、サーバー証明書の最長有効期限を将来的に短縮させる決議が承認されました。

- Apple社からの提案によるもので、2026年3月14日までは現行の最長有効期限である398日(約1年1ヶ月)となりますが、以後同3月15日以降は200日、2027年3月15日以降は100日と段階的な変更を経て、2029年3月15日以降に発行される証明書については47日が最長となるとのことです。

AUS便りからの所感等

- サーバー証明書の最長有効期限は2010年代半ばから段階的な変更が進んでおり、現在の398日も今回同様Apple社の提案により2020年から実施されているものです。

- 証明書の更新・管理に関するコストの増加を懸念する声がある一方、特にLet's Encryptをはじめとした無料発行サービスを中心に、ツールによる自動的な発行・更新を前提とする管理が進んだことが最長有効期限の短縮を現実的としていった一面もあります。

- 最終的に最長47日での更新となった場合、特に組織の実在性の認証等が必要となるOV証明書ないしEV証明書においては、毎月の更新毎に書類の提出等が発生する運用となるのか、認証の簡略化がなされるのか、またそれによって逆に問題が発生するのかや、OV証明書の利用を断念するケースが出てくるのか等も注目されるところです。

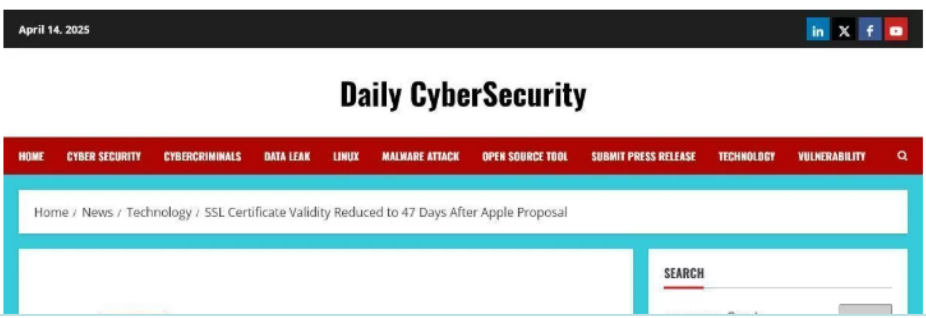
TECHF Powered by マイナビニュース

SSL/TLS証明書の有効期間が47日に短縮、2026年から段階的に実施

掲載日 2025/04/17 10:02　　著者：後藤大地

Cybersecurity Newsは4月14日(現地時間)、「SSL Certificate Validity Reduced to 47 Days After Apple Proposal」において、SSL/TLS証明書の最大有効期間が47日に短縮されると報じた。

SSL/TLS証明書の最大有効期間は改訂を繰り返し徐々に短くなっている。現在の最大有効期間は398日だが、Appleが漏洩した場合の影響を軽減するためとして47日への短縮を提案(SC-081v3)し、関係機関およびコンシューマーの賛成多数で承認されたことがわかった。



●3月フィッシング報告件数は249,936件、今後は20万件超が常態化か？

https://www.antiphishing.jp/report/monthly/202503.html

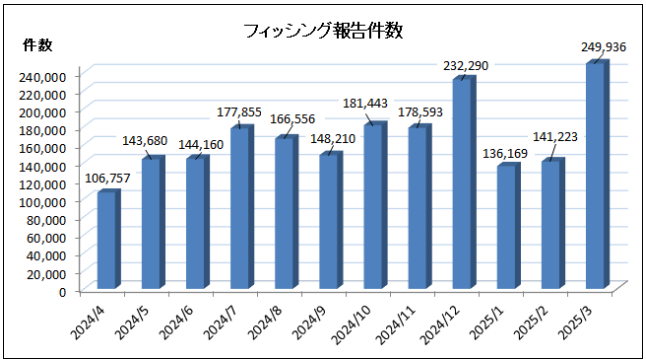
このニュースをザックリ言うと・・・

- 4月18日(日本時間)、フィッシング対策協議会より、3月に寄せられたフィッシング報告状況が発表されました。
- 3月度の報告件数は249,936件で、2月度(https://www.antiphishing.jp/report/monthly/202502.html)の141,223件から108,713件増加しています。
- フィッシングサイトのURL件数は51,735件で2月度(22,518件)から29,217件増加、使用されるTLD(トップレベルドメイン名)の割合は .com(約36.3%)、.cn(約27.5%)、 .net(約11.1%)、.goog(約6.7%) .xyz(約6.2%)でこの5つで約87.7%を占めています。
- 悪用されたブランド件数は84件で2月度(99件)から15件現象、最も割合が多かったブランドとしてはAmazonとAppleがそれぞれ全体の約22.5%と14.2%、次いで1万件以上報告されたANA、VISAと合わせて約58.2%、さらに1,000件以上報告された35ブランドまで含めると約97.2%を占めたとのことです。

AUS便りからの所感

- 報告件数は2024年12月度の232,290件を超えて過去最多を更新しており、今後も20万件超が常態化する可能性が考えられます。
- フィッシングサイトはURL件数が同じく2024年12月度の120,415件を最後にこの3ヶ月間は大きく減少状態となっており、一方TLDの割合ではトップ2以外で .netが久々に10%超えとなっています。
- 大手ネット証券各社への攻撃が相次ぐとともに各社を騙るフィッシングも多発し、同協議会からは3月31日から4月8日までに5社のフィッシングに関する注意喚起が出されており(https://www.antiphishing.jp/news/alert/)、利用しているサービスを発信元とするメールが届いた場合には日本データ通信協会の迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/news/alert.html)他ネット上でのフィッシング報告等と照らし合わせる、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする、また適宜追加認証を設定する等、慎重に行動することを日々心掛けましょう。

フィッシング対策協議会 Council of Anti-Phishing Japan



●不正なSMSを送信、携帯電話の「偽基地局」東京・大阪等で発生

https://www.itmedia.co.jp/news/articles/2504/15/news133.html
https://togetter.com/li/2537666

このニュースをザックリ言うと・・・

- 4月12日(日本時間)、日本国内で携帯電話の電波に干渉する偽の基地局を確認したとX(旧・Twitter)で報告されています。
- 報告によれば、NTTドコモ回線の電波状況が「圏外」になった後、GSM(2G)規格の回線と繋がり、中国語による不審なSMSが送信されてきたとのことです。
- これを受けて他のユーザーからも、東京や大阪等で回線が繋がりにくくなる等の事象が発生していたとの報告が相次ぎ、同15日には総務大臣が記者会見で言及する事態となっています。
- 不審なSMSについては中国からの旅行者を狙った可能性の指摘があり、これ以外にも偽のGSM回線と接続することによる通信傍受等の恐れもあるとされています。

AUS便りからの所感

- 今回のような偽の基地局による不正行為(ないしそのための装置)は「IMSIキャッチャー」と称され、海外では20年近く前から知られる手口とされています。
- 今日一般に用いられるより安全な通信ではなく、安全でない古い通信で接続させることにより、接続先を容易に騙ったりする攻撃手法はこの他にもインターネット上で多く存在します。
- GSMは日本で使われた実績はないものの、現在国内で出回っている機種でも対応しているものがあり、Androidでは「2Gを許可する」設定を無効にする、iPhoneでは「ロックダウンモード」を有効にすることが推奨されます。

ITmedia NEWS

スマホの回線を乗っ取る、“ニセ基地局”が国内で出現 詐欺SMSを強制送信　携帯各社も対策へ

2025年04月15日 14時29分 公開　[三好一葉，ITmedia]

携帯電話の基地局を装い、違法な電波を発射する「偽基地局」（IMSIキャッチャー）の存在が、東京都内や大阪市などで確認されている。X上では「不審なSMSを送り付けられた」という指摘が多く上がっており、キャリア各社も対応に乗り出す事態となっている。

どんな手口？

事態を指摘したのは、Xユーザーの電波やくざ（@denpa893）氏だ。同氏は4月12日、「docomoが圏外になった後、回線がGSMになり、突然不審なSMSが送られてきた」という趣旨のポストを投稿。妨害電波（ジャミング）によって「Band3（1.8GHz帯）」以外のdocomoの周波数帯が正常に通信できなくなっている状況を報告している。