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。

●スマートフォン等で大規模なネットワーク構築か、悪性プロキシー「IPIDEA」Googleが無力化

https://www.itmedia.co.jp/news/articles/2601/30/news070.html
https://cloud.google.com/blog/ja/topics/threat-intelligence/disrupting-largest-residential-proxy-network/

このニュースをザックリ言うと・・・

- 1月28日(現地時間)、米GoogleのThreat Intelligence Group(GTIG)より、「世界最大級の住宅用プロキシーネットワーク」とされる「IPIDEA」の停止措置を講じたと発表されました。

- GTIGが住宅用プロキシーネットワークの調査を行ったところ、IPIDEAにより、外部から踏み台として利用可能とされるプロキシーネットワークが、数百万台のスマートフォン等で動作していたとされ、中国・北朝鮮・イラン・ロシア等の攻撃者グループが悪用していたとされています。

- アプリにIPIDEAのプログラムを埋め込む開発キット(SDK)がAndroid・Windows・iOS・webOSに対応していたとされ、「空き帯域幅を収益化」を謳うアプリや、10以上のブランドによる無料VPNサービスのアプリにIPIDEAを動作させる不正プログラムが入っていたとされています。

AUS便りからの所感等

- このような不正なアプリをインストールし、攻撃者がユーザーのネットワークから外部へ不正活動を行うことにより、ISPによって不審なユーザーとして報告されたり、ブロックされたりする恐れもあるとしており、スマートフォン以外のIoT機器あるいはWindows PCにインストールされるプログラム、ブラウザーの拡張機能においても仕込まれている可能性も考えられます。

- 不審な通信を適切に検知ないし遮断できるよう、企業・組織においてはUTMや、管理する個々のスマートフォン・PC等へのEDRの導入が推奨されますが、家庭のネットワーク、個人のスマートフォン等を同レベルに保護するソリューションが現れるかは未知数であり、アプリの導入あるいはインストーラーの入手の段階において、ネット上のレビュー・注意喚起を基に慎重に吟味することが重要です。

- なお1月下旬(26日ごろ)以降、特に中国を中心に頻繁に送信されていた迷惑メールの流量が著しく減少しており、同時期のIPIDEAの停止による可能性も考えられますが、GTIG等からの発表等確固たる根拠はなく、春節(2/17~3/3・旧正月)の時期に関連したためも考えられ、こちらについては引き続き様子を見るべき段階と思われます。

ITmedia NEWS

Google、世界最大級の悪性プロキシ「IPIDEA」を無力化　数百万台のデバイスを解放

2026年01月30日 06時58分 公開　[ITmedia]

米Googleの脅威インテリジェンスチーム（GTI）は1月28日（現地時間）、中国を拠点とするグループが運営する世界最大級の住宅用プロキシネットワークである「IPIDEA」を無力化するための作戦を実行したと発表した。これにより、攻撃者が利用可能なプロキシデバイスを数百万台規模で削減し、ネットワークの機能を大幅に低下させる成果を上げたとしている。

Googleはパートナー企業や法執行機関と連携し、当該ネットワークを制御していたドメインの法的差し止めを行うとともに、Androidのセキュリティ機能「Google Play Protect」を通じて、関連する悪意あるアプリの削除やインストールブロックを実施した。

IPIDEAのような住宅用プロキシネットワークは、一般家庭のインターネット回線（IPアドレス）を経由して通信を行うことで、攻撃者が自身の活動を隠蔽するために悪用されている。Googleの調査によると、このネットワークは中国、北朝鮮、イラン、ロシアなどの脅威グループによるサイバー諜報活動やパスワードスプレー攻撃（よく使われるパスワードを大量のアカウントに対して試すサイバー攻撃）、ボットネットの運用基盤として利用されているという。また、ユーザーの端末が踏み台にされることで、ユーザー自身のホームネットワークが外部からの攻撃にさらされるセキュリティリスクも生じている。

Google Cloud　ブログ

ホーム ネットワークに潜む脅威: 世界最大級の住宅用プロキシ ネットワークの活動を阻止

2026年2月4日

Google Threat Intelligence Group

※この投稿は米国時間 2026 年 1 月 29 日に、Google Cloud blog に投稿されたものの抄訳です。

はじめに

今週、Google とパートナーは、世界最大級の住宅用プロキシ ネットワークの一つと考えられている IPIDEA プロキシ ネットワークを停止させる措置を講じました。IPIDEA のプロキシ インフラストラクチャは、さまざまな不正な行為者が利用するデジタル エコシステムのコンポーネントになっていますが、このことはほとんど知られていません。

Google Threat Intelligence Group（GTIG）が主導し、他のチームと連携して実施したこの不正ネットワーク阻止の活動では、主に以下の 3 つの活動が行われました。

●農水省職員・家族約4,600人分の個人情報流出、送信先の通知に誤り

https://www.nikkei.com/article/DGXZQOUA231NH0T20C26A1000000/
https://www.maff.go.jp/j/press/kanbo/keiri/260123.html

このニュースをザックリ言うと･･･

- 1月23日(日本時間)、農林水産省より、同省職員および家族計4,571人分の個人情報が外部に流出したと発表されました。
- 流出したのは源泉徴収票等に関する情報で、同省職員の氏名・生年月日・住所・マイナンバー・給与支給金額・源泉徴収税額・保険料等控除情報、および家族の氏名・マイナンバー等となっています。
- 当該情報を省内にて一元化する際、提出先として誤ったメールアドレスを通知し、情報が外部メールサーバーに送信されていたことが同19日に発覚したとしています。

AUS便りからの所感

- 同省では「同様の事態が生じないよう、個人情報の厳重かつ適正な管理を徹底する」としており、例えば日経新聞の報道では、機微情報の共有は専用サイトで管理する等の対策検討が報じられています。
- これまで多く発生している、メーラーにおけるメールアドレスの誤入力による流出(あるいはBcc: ではなくCc: に入力したケースも含む)とは異なり、多数の職員がそれぞれの環境からメールを送信してくる場面において、外部への誤送信をシステムで阻止するやり方はとりにくい場合があるとみられます。
- 一方で特に今回取り扱っていた情報の種類を鑑みれば、誤入力で第三者に情報が送信される恐れがあるメールの仕組みはやはり適切ではなく、例えば組織のグループウェア等でのアップロードを受け付ける方がまだ安全と言えるでしょう。

日本経済新聞

農水省が個人情報漏洩、職員と家族4571人分　書類提出先アドレス誤り

経済
2026年1月23日 12:24

農林水産省は23日、職員やその家族合計4571人分の個人情報が外部に漏洩したと発表した。省内で職員の源泉徴収票に関する情報を一元化する際に、提出先に誤ったメールアドレスを示した。現時点で不正利用などの二次被害は確認されていないという。

情報漏洩は本省に勤務する職員約5000人のうち2593人とその家族1978人で確認した。氏名、生年月日、住所、マイナンバー、給与などの情報を含む。2025年12月23日に省内で税務関係の事務作業を行うため、担当者が部局ごとにメールでの情報提出を求めた。一部のメールが担当者に届かず、1月19日に情報漏洩が発覚した。

● OpenSSLに計12件の脆弱点、アップデートの確認を

https://jvn.jp/vu/JVNVU91919266/
https://scan.netsecurity.ne.jp/article/2026/02/05/54558.html

このニュースをザックリ言うと･･･

- 1月28日(日本時間・以下同様)、暗号化通信ライブラリ「OpenSSL」に12件の脆弱点が存在するとして、修正バージョン(3.6.1, 3.5.5, 3.4.4, 3.3.6, 3.0.19他)がリリースされています。
- 脆弱点のうち危険度が高いとされる1件(CVE-2025-15467、バージョン3.0系以降に影響)、中程度1件(CVE-2025-11187、バージョン3.4系以降に影響)はいずれもDoS攻撃や任意のコード実行、その他危険度が低い10件もDoS攻撃等の可能性があるとされています。
- 2月3日にはIPA・JPCERT/CC運営の脆弱点情報サイト「JVN」でも注意喚起が出されています。

AUS便りからの所感

- OpenSSLはHTTPSのみならずメール送受信やVPNといった広範囲なSSL/TLS暗号化通信等で使用され、脆弱点の内容によってはOpenSSLを使用するサーバー側・クライアント側両方が攻撃を受ける恐れがあります。
- 主なLinuxディストリビューションにおいては、RedHat Enterprise Linux(RHEL)9・10(同ベースのAlmaLinux/Rocky Linux含む)やDebian 12・13、Ubuntu 25.10・24.04以前のLTS等で修正バージョンがリリースされています(なおRHEL8ではCVE-2025-15467の影響を受けず、影響を受ける他の脆弱点も多くは危険度が低いため、修正バージョンはまだリリースされていません)。
- この他、OpenSSLを独自に組み込んでいるソフトウェア・アプライアンス等においても脆弱点の影響を受ける可能性があり、ベンダーからアップデートがリリースされる場合がありますので、更新情報を随時確認し、必要なアップデートがあれば即時適用できるような体制を整えることが重要です。

公開日:2026/02/03　最終更新日:2026/02/03

JVNVU#91919266
OpenSSLにおける複数の脆弱性(OpenSSL Security Advisory [27th January 2026])

概要
OpenSSL Projectより、OpenSSL Security Advisory [27th January 2026]が公開されました。

影響を受けるシステム
CVE-2025-11187

- OpenSSL 3.6.1より前の3.6系バージョン
- OpenSSL 3.5.5より前の3.5系バージョン
- OpenSSL 3.4.4より前の3.4系バージョン

CVE-2025-15467

- OpenSSL 3.6.1より前の3.6系バージョン
- OpenSSL 3.5.5より前の3.5系バージョン
- OpenSSL 3.4.4より前の3.4系バージョン
- OpenSSL 3.3.6より前の3.3系バージョン
- OpenSSL 3.0.19より前の3.0系バージョン