— AUS（アルテミス・ユーザ・サポート）便り 2018/12/10号 —
https://www.artemis-jp.com

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。

●ソフトバンク通信障害、原因はエリクソン社交換機の不具合…海外でも同様の障害

https://japan.cnet.com/article/35129765/
https://japan.cnet.com/article/35129773/
https://www.softbank.jp/corp/group/sbm/news/press/2018/20181206_02/
https://www.ericsson.com/jp/ja/press-releases/2/2018/12/1

このニュースをザックリ言うと･･･

- 12月6日（日本時間）、ソフトバンク社の携帯電話等サービスで大規模な通信障害が発生し、同社より、原因はエリクソン社製の交換機のソフトウエアに異常が発生したためと発表されました。

- 同日には英国の携帯電話会社O2社等11ヶ国の通信業者においても障害が発生し、これらについてもエリクソン社製交換機が原因とされています。

- 問題となったソフトウェアは9ヶ月前から運用されており、旧バージョンに戻すことで復旧したとのことです。

AUS便りからの所感等

- 同7日にはエリクソン社より、問題となったバージョンに含まれていた電子証明書の期限切れが大元の原因であることが発表されていますが、9ヶ月前という比較的新しい時期から使われていたバージョンでこのような問題が発生した詳しい事情は不明です。

- この例よりも一般的に起こり得る問題としては、サポート期限が切れた機器を利用し続けたり、ファームウェアの更新を怠ったりしていることにより、証明書の期限が切れてしまい、アクセス時に警告が出るようになったり、最悪機器同士や外部との通信ができなくなるケースが考えられます。

- セキュリティホールが修正されずに攻撃を受ける可能性も考慮し、ハードウェア・ソフトウェアともに適切なアップデートを行うことが重要です。

cnet Japan

ソフトバンクの通信障害、エリクソン製交換機が原因と公表--海外11カ国でも同様の障害

山川晶之（編集部） 2018年12月07日 00時13分

ソフトバンクは12月6日、13時39分～18時4分の約4時間半にかけて発生した通信障害について、エリクソン製の交換機に問題があったと公表した。

このトラブルは、全国のソフトバンク、ワイモバイルの4Gネットワーク（各MVNOサービスを含む）、固定電話サービス「おうちのでんわ」にて、利用できない・利用しづらい状況が続いたというもの。ワイヤレスブロードバンドサービス 3G/4Gを行き来した

同社では、通信障 ソフトウェアを挙げて ソン製パケット交換機 で3Gネットワークに輻

ソフトバンクの通信障害、「原因はソフトウェア証明書の期限切れ」--エリクソンが認める

Corinne Reichert（ZDNet.com.au） 翻訳校正：編集部 2018年12月07日 10時11分

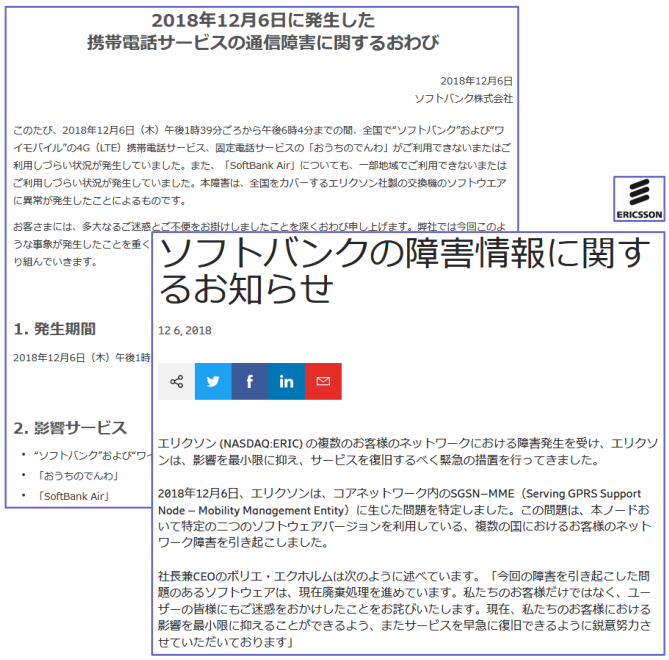
Ericssonは、英国のO2や日本のソフトバンクのモバイルサービスで発生した通信障害について、ソフトウェアの証明書の期限切れが原因だったことを明かした。

Ericssonは、「初期の根本原因分析では、これらの顧客がインストールしていたソフトウェアバージョンの証明書の期限切れが主な問題だったことが明らかになった」と述べた。

「完全かつ包括的な根本原因分析は現在も進行中だ。われわれは今、緊急の問題を解決することに全力を挙げている」

Ericssonによると、この問題は、「Serving GPRS Support Node - Mobility Management Entity」（SGSN-MME）の2つのバージョンのソフトウェアを使用する顧客のコアネットワークのノードに影響を及ぼしたという。また、同社はサービスを復旧するため、直ちに対策を講じたとしている。

SoftBank



2018年12月6日に発生した
携帯電話サービスの通信障害に関するおわび

2018年12月6日
ソフトバンク株式会社

このたび、2018年12月6日（木）午後1時39分ごろから午後6時4分までの間、全国で"ソフトバンク"および"ワイモバイル"の4G（LTE）携帯電話サービス、固定電話サービスの「おうちのでんわ」がご利用できないまたはご利用しづらい状況が発生していました。また、「SoftBank Air」についても、一部地域でご利用できないまたはご利用しづらい状況が発生していました。本障害は、全国をカバーするエリクソン社製の交換機のソフトウエアに異常が発生したことによるものです。

お客さまには、多大なるご迷惑とご不便をお掛けしましたことを深くおわび申し上げます。弊社では今回このような事象が発生したことを重く り組んでいきます。

1. 発生期間

2018年12月6日（木）午後1時

2. 影響サービス

- "ソフトバンク"および"ワ
- 「おうちのでんわ」
- 「SoftBank Air」

ERICSSON

ソフトバンクの障害情報に関するお知らせ

12 6, 2018

エリクソン (NASDAQ:ERIC) の複数のお客様のネットワークにおける障害発生を受け、エリクソンは、影響を最小限に抑え、サービスを復旧するべく緊急の措置を行ってきました。

2018年12月6日、エリクソンは、コアネットワーク内のSGSN−MME（Serving GPRS Support Node − Mobility Management Entity）に生じた問題を特定しました。この問題は、本ノードおいて特定の二つのソフトウェアバージョンを利用している、複数の国におけるお客様のネットワーク障害を引き起こしました。

社長兼CEOのボリエ・エクホルムは次のように述べています。「今回の障害を引き起こした問題のあるソフトウェアは、現在廃棄処理を進めています。私たちのお客様だけではなく、ユーザーの皆様にもご迷惑をおかけしたことをお詫びいたします。現在、私たちのお客様における影響を最小限に抑えることができるよう、またサービスを早急に復旧できるように鋭意努力させていただいております」

●サンドラッグからの不審な「仮登録の受付完了」メール出回る

https://news.biglobe.ne.jp/domestic/1130/blnews_181130_4204010139.html

このニュースをザックリ言うと・・・

- 11月30日（日本時間）、サンドラッグ社の通販サイト「サンドラッグe-shop本店」から身に覚えのない仮登録メールが送信されているとする報告がネット上等で相次ぎ、同社からも注意喚起が出されています。

- 第三者が外部で入手したメールアドレスを会員登録ページへ入力していたことが原因としており、攻撃者が会員登録ページにメールアドレスを入力することにより、そのアドレスが当該サイトで登録済みかを調査していた可能性がありますが、当該サイトにおける個人情報の漏洩やサーバの乗っ取りなどの事実はないとのことです。

- 同社では、仮登録メールに身に覚えがない場合はそこからの会員登録はしないよう求めています。

AUS便りからの所感等

- 仮登録メールは件名が「【サンドラッグお客様サイト/e-shop本店】仮登録の受付完了のご案内」のもので、実際に当該サイトから発信されている本物のメールです。

- 今回のようなシステムでは、メールが送信されたアドレス自体を乗っ取られる等して仮登録メールを攻撃者に見られない限り、通常は本登録に至ることはありません（本登録ページへのURLが推測されにくいものでないと意味はありません）。

- しかし、第三者のメールアドレスを悪用して本人の確認なしでアカウントが登録可能なサイトも未だ珍しくなく、自分の知らない間に何らかのサイトに登録されている可能性にも十分に注意が必要でしょう。


BIGLOBEニュース

サンドラッグからの不審な「仮登録の受付完了」メール出回る
個人情報漏洩やサーバ乗っ取りは確認できず、第三者がアドレス入力か

11月30日（金）12時40分　BIGLOBEニュース編集部

ドラッグストアのサンドラッグは30日、同社の通販サイト「サンドラッグe-shop本店」の仮登録案内メールが身に覚えのない人に配信されていると公表。第三者が、入手したメールアドレスを実際に「サンドラッグe-shop本店」で入力している可能性があるとして、注意を呼びかけている。

この仮登録案内メールは、「サンドラッグe-shop本店」で会員登録を行う際に入力したメールアドレス宛てに届くもの。「【サンドラッグお客様サイト/e-shop本店】仮登録の受付完了のご案内」という件名で、実際にサンドラッグから配信されている。30日朝からTwitterなどでは、登録した覚えがないのに届いたという投稿が相次いでいる。

- 同社では、機械的に大量の仮登録が行えないよう画像認証の追加等の対応をとったとしており、ECサイト運営者においては、登録の仕組みを悪用されて第三者に被害が及ぶ可能性を抑制するため、今回どういった対応がとられたかを参考にしたり、適宜セキュリティ診断を受けたりすることを推奨致します。

●HTTPポートへのSynFlood攻撃・SYN/ACKリフレクター攻撃の可能性

https://securityinsight.jp/news/13-inbrief/3522-181205-1

このニュースをザックリ言うと・・・

- 12月3日（日本時間）、警察庁より、同庁のインターネット定点観測システムにてTCPポート80番（HTTP）を利用したSYN/ACKリフレクター攻撃とみられるパケットが観測されたとするレポートが発表されています。

- 9月26日～10月上旬と11月5日に、短期間に大量のパケットが観測されており、例えば9月26日には約6時間の間、1IPアドレスに対し1分間に200～250件のSYN（接続要求）パケットが送信されていたとのことです。

- 発信元が特定の単一IPアドレスあるいは同一ネットワーク内とみられる複数のIPアドレスとなっていたことから、SYN Flood攻撃に関連した観測であると推測しています。

- レポートではWebサーバ等の管理者に対し「上位通信事業者やサービスプロバイダが提供するDDoS攻撃対策サービスの利用」「SynFlood攻撃に対応したOSやIDS製品の導入」等を行うよう推奨しています。

AUS便りからの所感等

- SYN/ACKリフレクター攻撃は、TCPプロトコルにおける「3ウェイ・ハンドシェイク」の仕組みを悪用し、発信元を偽装したSYNパケットを大量に送信し、それに対するSYN/ACK（応答）パケットをターゲットとなるホストに向けることにより、ターゲットホストの正常な動作を妨害することを目的としています。

- 今回観測されたパケットの発信元が同一のIPアドレス等になっていたのも、攻撃者がそこからパケットを送信したのではなく、逆にそこをリフレクター攻撃のターゲットとしていたということが考えられます。


Security Insight

警察庁@police、宛先ポート80/TCPを利用したSYN/ACKリフレクター攻撃とみられる観測等について発表

2018/12/05 10:00
SecurityInsight

警察庁@policeは12月3日、警察庁のインターネット定点観測システムにおいて、今年９月26日頃から、宛先ポート80/TCPに対するアクセスの増加を断続的に観測したと発表した。その概要は以下のとおり。

今回の観測はSYNパケットを短期間に多数検知したもので、それらSYNパケットの特徴は、ウェブサーバー等で使用される80/TCPを宛先ポートとし、発信元が特定の単一IPアドレスまたは同一ネットワーク内とみられる複数のIPアドレスとなっているものだった。これらはSYN Flood攻撃に関連した観測と考えられる。

- 不審な大量のSYNパケットへそのまま応答することは、受信したサーバ自身が正常な動作を行えなくなることにも、またリフレクター攻撃の踏み台になることにも繋がり得ますので、これを考慮するのであれば、警察庁が推奨している対策やUTMの導入等、各種防衛策を検討するのが良いでしょう。