— AUS（アルテミス・ユーザ・サポート）便り 2016/02/01号 —

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。

●厚生労働省サイトに2度の閲覧障害･･･DDoS攻撃か

http://www.sankei.com/affairs/news/160126/afr1601260031-n1.html
http://www.sankei.com/affairs/news/160126/afr1601260049-n1.html

このニュースをザックリ言うと･･･

- 1月25日（日本時間）午後9時頃から翌26日午後12時50分頃にかけて、厚生労働省のWebサイト（http://www.mhlw.go.jp/）において、DDoS攻撃(※)によるとみられる閲覧障害が発生していました。

- 25日午後10時20分頃には、国際的クラッカー集団「Anonymous(アノニマス)」(※)のものとみられるTwitterアカウントが「日本のイルカ漁への抗議」としてサイバー攻撃を示唆する投稿をしていたとされ、DDoS攻撃は彼らの指示で行われた可能性があります。

- 26日には再度同様のDDoS攻撃を受け、午後7時から翌午前0時15分頃まで再び閲覧障害が発生していました。（なお、厚労省サイトは昨年11月にもDDoS攻撃を受けていました。）

AUS便りからの所感等

- 官公庁WebサイトにおけるCDN(※)の導入は、いまのところまだ十分ではない模様です。（CDN業者は、最大手のAkamaiから個人サイトに人気のある業者まで様々であり、Webサイトの閲覧障害がビジネスに影響を及ぼす可能性を考慮し、導入を検討することが良いと思われます。）

- この他、サーバ自体が過負荷で落ちてしまうような事態を避けるよう、UTMの導入により、パケットの流入量を抑えるアプローチも一考に値するものと思われます。

産経ニュース

2016.1.26 13:56

文字の大きさ 小 中 大 印刷

厚労省HP15時間ぶり復旧　アノニマス関与か

ブログに書く 0　ツイート 反応　おすすめ 15　G+1 0

厚生労働省のホームページ（HP）が25日夜から閲覧できなくなっていた問題で、HPが26日午後0時50分ごろ、約15時間ぶりに復旧した。

厚労省によると、25日午後9時半過ぎから、大量のデータを送り付けてサービス不能にする「DDoS攻撃」を受けたとみられる。同日午後10時20分ごろ、国際的なハッカー集団アノニマスのものとみられるツイッターに、厚労省に対するサイバー攻撃を示唆する投稿があったという。厚労省は警視庁公安部に連絡するとともに、調査をしている。

厚労省のHPは昨年11月にも外部から大量のデータを送りつけられるサイバー攻撃を受け、閲覧できない状態になった。このときもアノニマスのものとみられるツイッターに攻撃を示唆する投稿があった。

2016.1.26 20:49

文字の大きさ 小 中 大 印刷

復旧したばかりの厚労省HPにまたサイバー攻撃　2日連続、3回目

ブログに書く 0　ツイート 反応　おすすめ 30　G+1 1

厚生労働省は26日、ホームページ（HP）がサイバー攻撃を受け、同日午後7時ごろから閲覧できない状態になったと発表した。

同省HPは25日午後9時半過ぎから約15時間にわたり大量のデータを送られる「DDoS攻撃」を受け、26日昼に復旧したばかり。国際的なハッカー集団アノニマスのものとみられるツイッターが25日、攻撃を示唆する投稿をしていた。

厚労省のHPは昨年11月にもサイバー攻撃を受けており、今回が3回目。厚労省の担当者は「国民に（HPによる）情報を提供できなくなり、申し訳ない。速やかに調査を進めるとともに、対策を考えたい」としている。

IT用語辞典 e-Words

（※）DDoS攻撃【 Distributed Denial of Service attack 】分散DoS攻撃

DDoS攻撃とは、複数のネットワークに分散する大量のコンピュータが一斉に特定のネットワークやコンピュータへ接続要求を送出し、通信容量をあふれさせて機能を停止させてしまう攻撃。

電子掲示板（BBS）などで参加者を募って大勢の攻撃者が意図的に一斉に攻撃を実行する場合と、コンピュータや通信機器が攻撃者に乗っ取られ、所有者の知らないうちに攻撃に参加させられてしまう場合がある。

後者の場合、攻撃者は攻撃対象とは無関係な多数のコンピュータに侵入し、その管理者や利用者に気づかれないように攻撃実行用のプログラム（トロイの木馬など）をこっそりしかける。攻撃を開始する時には、あらかじめ仕掛けたプログラムに対して、一斉に接続要求データの送出命令を発行する。標的となったコンピュータには、乗っ取られたコンピュータから要求が送られてくるため、真の攻撃元である「黒幕」のコンピュータを割り出すことは難しい。

（※）CDN【 Contents Delivery Network 】コンテンツデリバリネットワーク

CDNとは、ファイルサイズの大きいデジタルコンテンツをネットワーク経由で配信するために最適化されたネットワークのこと。CDNを構築・運用し、企業などに有料で利用させるサービスをコンテンツデリバリサービス（CDS）という。

狭義にはデジタルコンテンツの大量配信に対応したネットワークを指し、広義にはファイルの配布ポイント管理から課金・認証システムまで、デジタルコンテンツの配布や販売に必要な機能をひととおり揃えたシステムを指す。

音楽や動画といったデジタルコンテンツは、従来インターネット上で流通してきたHTMLファイルなどと比べてサイズが大きく、ネットワーク越しで配信を行うとネットワークに多大な負荷がかかってしまう。

このとき、ネットワーク上のさまざまな場所にデジタルコンテンツの配布ポイントを用意し、ユーザのネットワーク位置に応じた最適な配布ポイントを指示することで、大容量のコンテンツをスムーズにユーザに配信できるようになる。

コトバンク

（※）アノニマス　あのにます　Anonymous

匿名（Anonymous=アノニマス）で活動する国際的ハッカー集団。

政府や企業に対する抗議活動の手段として、DDoS攻撃（Distributed Denial of Service attack=分散型サービス拒否攻撃）によって、インターネット上の特定のサーバーをアクセス不能にしたり、サーバーに侵入し、データの改ざんや流出を行ったりする。

●「標的型メールで流出」想定、インフラ事業者と訓練･･･警視庁

http://www.jiji.com/jc/zc?k=201601/2016012600045&g=soc

このニュースをザックリ言うと･･･

- 1月26日から29日（日本時間）にかけ、警視庁が「標的型攻撃」メールにより重要インフラ事業者から情報が流出する事態に備えた訓練を行いました。

- 訓練は、本年5月の伊勢志摩サミットや2020年の東京オリンピック・パラリンピック等を控え、重要インフラ事業者が標的になる恐れは高いとし、連携強化や緊急時の対応能力向上を目指すもので、情報通信・金融・航空および水道等都内の59事業者から約210人が参加して行われました。

- 訓練では、事業者の職員が不正プログラムが添付された「標的型攻撃」メールを開封し、PCがウイルスに感染して情報を窃取される状況等の体験や、被害拡大の防止、原因調査、証拠保全などの手順が確認されたとのことです。

AUS便りからの所感等

- 昨年は特に下半期以降に被害が多く報じられる等
「標的型攻撃」が大きくクローズアップされ、
「感染しない」ためだけではなく
「感染した場合の被害を最小限に抑える」ための
対策が叫ばれた年でした。

時事ドットコム jijicom

「標的型メールで流出」想定＝インフラ事業者と訓練－警視庁

警視庁は26日、情報を盗み取るウイルスを仕込んだ標的型メールによって、重要インフラ事業者のパソコンから情報が流出する事態に備えた訓練を東京都内で行った。29日までの4日間に、情報通信や金融、航空、水道など都内の59事業者から約210人が参加する。重要インフラ事業者を集めたサイバー攻撃の対策訓練は5回目で、標的型メールの想定は初めて。

訓練で事業者は、メールに添付されたファイルを開封。「不審な通信がある」との指摘を受け、ウイルス感染を把握する。警視庁と連絡を取りながら、感染源と被害の広がりを確認したり、証拠保全や被害拡大防止の措置を取ったりする。(2016/01/26-10:10)

- この他にも、PCやネットワークでつながるNAS上のファイルを事実上破壊していく「ランサムウェア」等、これまでにない対策のセオリーが求められる攻撃が目立っています。

- 標的型攻撃等がどのようにして行われるかについて十分な情報収集と組織内への啓発を行い、一方でUTMの導入を含めた社内システム・ネットワーク構成の抜本的な見直しも重要となることでしょう。

●Windows XPがウイルスに感染して病院のネットワークが大混乱･･･オーストラリア

http://gigazine.net/news/20160125-hospital-attacked-by-damaging-computer-virus/

このニュースをザックリ言うと･･･

- 1月18日（現地時間）、オーストラリアの新聞The Age紙は、同国のロイヤル・メルボルン病院を運営する「メルボルン・ヘルス」社のネットワークで大規模なウイルス感染が発生したと報じました。

- 記事によれば、メルボルン・ヘルスの病理部で使われていたWindows XPがウイルスに感染したことにより、病院内のPCが使用できなくなり、一時は各種検査や記録などの作業を手動で行い、FAXや電話で結果をやりとりせざるを得ない状況になった模様です。

- 同社からは病院スタッフに対し「起動しているPCの電源を切らないこと、起動していないPCの電源を入れないこと」「Facebook・GMail・銀行などパスワードが必要なアカウントにログインしないこと」等の通達があったとのことで、19日までには大半のPCからウイルスの除去に成功したとされています。

- The Age紙では、システムのアップグレード予算が不足していたことが今回の原因としており、ビクトリア州の厚生大臣はアップグレード予算1000万豪ドル（約8億3000万円）を用意すると発表しています。

AUS便りからの所感等

- 大規模なウイルス感染までは至らなかったものの、
国内でも昨年、東京電力のような大企業や多くの
官公庁がWindows XPからのアップグレードが
できていなかったことについて、会計検査院が指摘するといったニュースもありました。

GIGAZINE

2016年01月25日 13時30分00秒

Windows XPがウイルスに感染して病院のネットワークが大混乱

オーストラリアの都市、メルボルンで最も大きな病院で使われているコンピューターネットワークがウイルスに感染し、病院内のコンピューターが全て使用不可になるという事態が発生しました。この影響で、病院では検査や記録など多くの作業が手動で行うなどの対応に追われることとなりました。

- ソフトウェアのアップデートは、公開サーバへの直接的な攻撃や、内部ネットワークにひとたび侵入したマルウェアの連鎖感染を防ぐ根本的な対策として欠かせませんが、予算等やむをえない事情によりアップデートができないコンピュータについては、せめて可能な限り隔離し、アンチウイルスやUTMによる防御を万全に行うことが求められます。