電気通信事故検証会議（第４回）　議事要旨

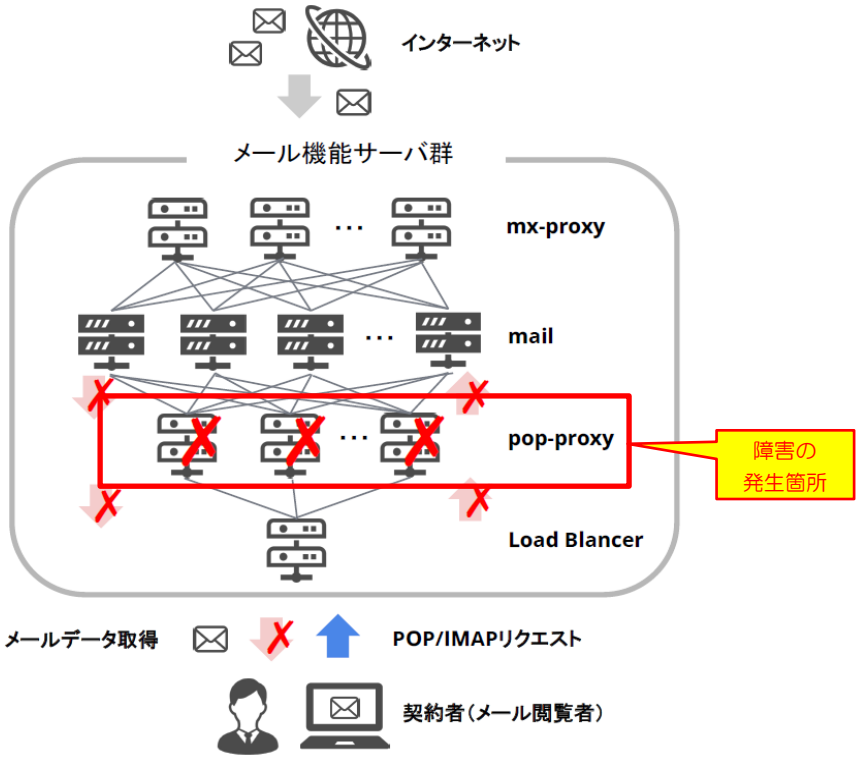
１　日　時：令和３年11月17日（水）10:00～

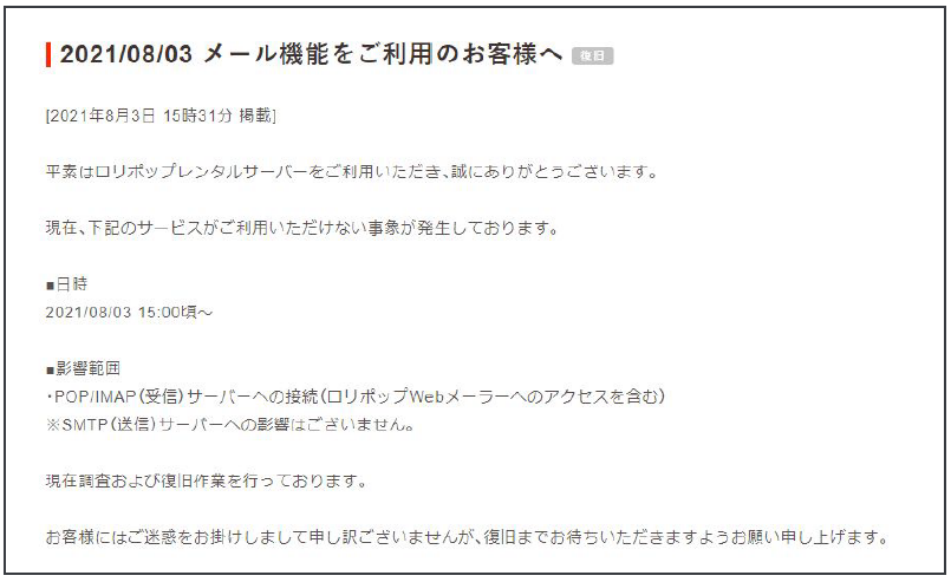
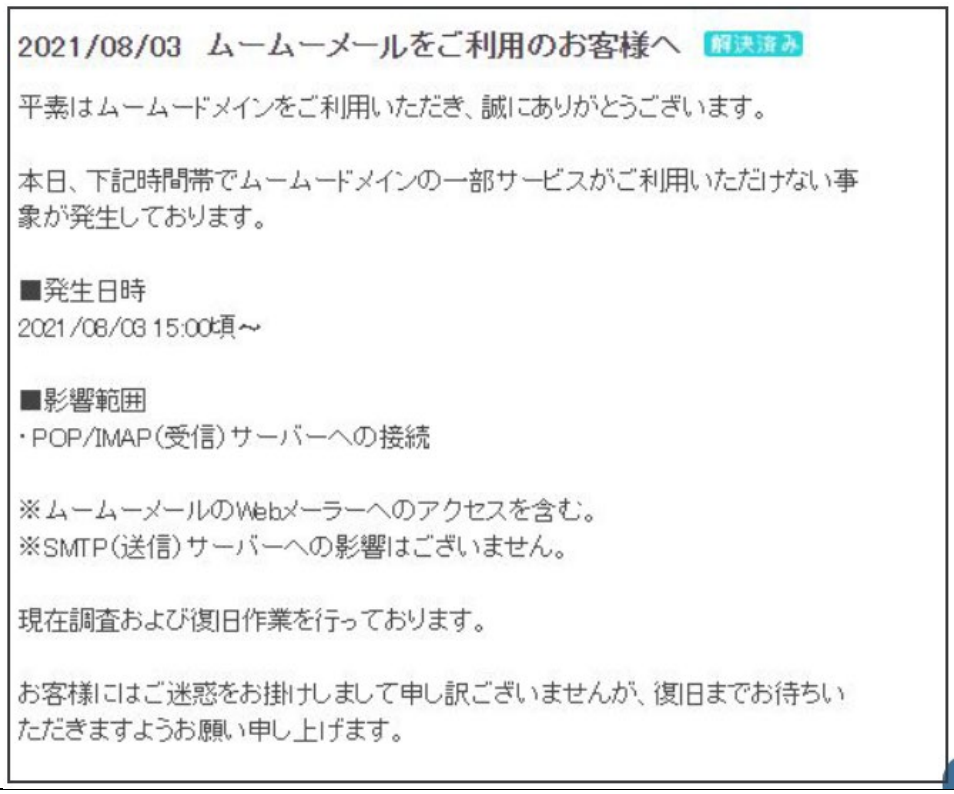
２　場　所：Web会議

３　議事

（１）GMO ペパボ株式会社から、令和３年８月に発生した重大な事故について説明が行われた。本事故の概要は以下のとおり。

事業者名	GMOペパボ株式会社	発生日時	令和３年８月３日 15時00分頃
継続時間	２時間25分	影響利用者数	最大456,516人
影響地域	全国	事業者への問合せ件数	1,767件
障害内容	事業者が運営するレンタルサーバーサービス「ロリポップ！」及びドメイン登録サービス「ムームードメイン」のオプションサービスである「ムームーメール」において、令和３年８月３日１５時００分から令和３年８月３日１７時２５分まで、メールサーバーで受信したメールを契約者が閲覧することができない事象が発生した。		
重大な事故に該当する電気通信役務の区分	五「一の項から四の項までに掲げる電気通信役務以外の電気通信役務」（インターネット関連サービス（有料）（電子メール））		
発生原因	＜発生原因の概要＞ メールサーバーに格納されたメールデータを契約者の代わりに代理で取得し、契約者にそのメールデータを提供する複数台のリバースプロキシサーバー（POPプロキシ）が、想定を超える多数の接続が集中したことより連鎖的にメモリ不足に陥り、全台が動作を停止した。 ＜長期化した原因＞ 復旧作業中に、リバースプロキシサーバーに再度障害が発生し、すべてのリバースプロキシサーバーの再起動及び再構築が必要となったため、復旧に時間を要した。		

機器構成図	
再発防止策	＜暫定対処＞ リバースプロキシサーバーの台数を増強する。 【令和３年８月３日実施完了】 ＜恒久対処＞ １．リバースプロキシサーバーのソフトウェアを、処理能力を高めるためのソフトウェアへ変更する。 【「ロリポップ！」：令和４年６月３０日実施完了予定】 【「ムームーメール」：令和３年１２月３１日実施完了予定】 ２．リバースプロキシサーバーの再構築の手順書を修正し、本件のような事象の発生時にも、より迅速にリバースプロキシサーバーの再構築を行えるようにする。 【令和３年９月３０日実施完了予定】

<table>
<tr><td rowspan="3">情報周知</td><td>自社サイト</td><td>令和3年8月3日15時31分
「ロリポップ！」のサービスサイトへ掲載
 
令和3年8月3日15時20分
「ムームードメイン」のサービスサイトへ掲載
  </td></tr>
<tr><td>その他</td><td>―</td></tr>
</table>

（２）議事（１）について、主に「アクセス数の原因及び兆候」、「運用・体制」、「再発防止策」及び「HP上での周知」についての観点について、GMOペパ

ボ株式会社及び構成員間で質疑応答が行われた。主な内容は、以下のとおり。

＜アクセス数の原因及び兆候＞

・アクセス数の増加の原因及び兆候についての質問があり、ログインを受け持つサーバーのログを確認する必要があるが、ログが残っていないため不明との回答があった。
・サイバー攻撃の可能性について質問があり、何らかの形でログインの試行が増えたということであり、攻撃の可能性はないと考えているとの回答があった。
・過去アクセス数が突発的に増大した事例について質問があり、今すぐの回答は困難との回答があった。

＜運用・体制＞

・監視項目についての質問があり、ロードアベレージ、トラヒック、コネクション数、あるいは、プロセス数、メモリ利用量などを、各サーバーに対してソフトウェアを入れて監視をしているとの回答があった。
・サーバーの状況なども把握して運用しているかといった質問があり、先ほど述べた項目でモニタリングをすると同時に、そこで問題があった場合、即座に通知を受けて、それに対して対応するというような体制を整えているといった回答があった。

＜再発防止策＞

・今後、サイバー攻撃等を受ける可能性を考えると、監視し迅速に対応する人的体制はできているということだが、制限をかけるようなメカニズムというようなことも考えたほうが良いという印象を受けたといったコメントがあった。

質疑応答を踏まえ、構成員より総括が行われた。主な発言内容は、以下

のとおり。

・同時アクセスユーザー数に関する負荷の見積りが甘かったのではないか。ロードバランサーを使っているがために各サーバーの負荷が均等に上がっていって、ほぼ一斉に総倒れになるという事象が起きてしまったので、メモリ使用量などを見て入り口で制限かけるようなメカニズムを本来作っておくべきだったのではないかという印象。

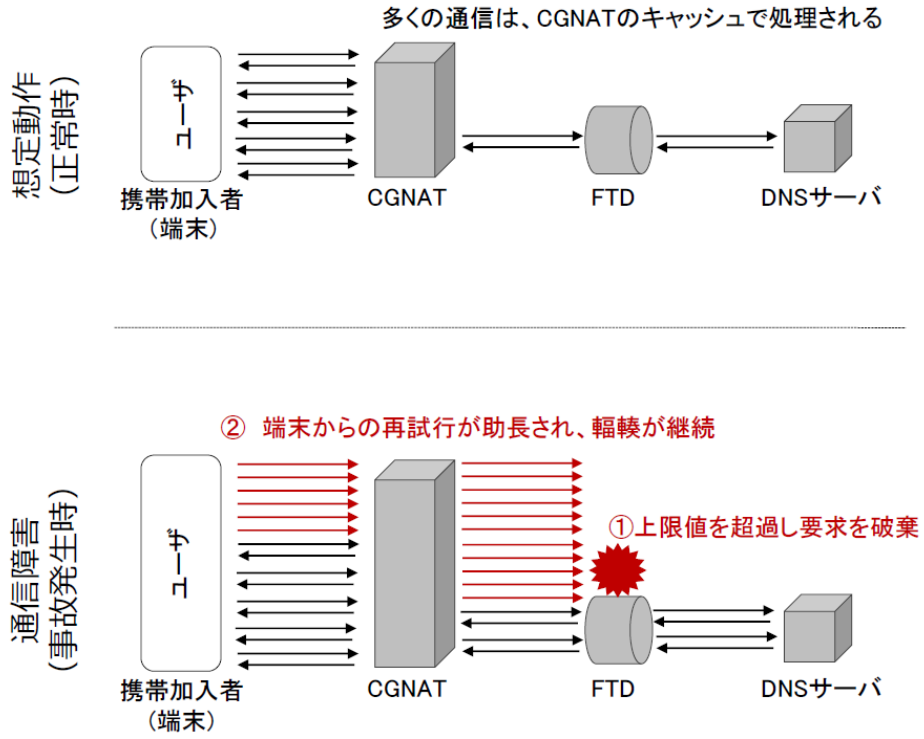
・今の対処の方法だと、基本的に負荷を全部受け止めてしまうやり方を検討しているようで懸念がある。

・この事業者は安価で、スモールビジネス、大学の研究室、個人の団体などに使われているサービスを提供している事業者。インターネットの黎明期から、ユーザーが増えたらシステムも増やすといった対処をしてきているという印象があった。しかし、そういう対処だと、攻撃された場合などに直ちに障害に繋がる懸念がある。また、カスタマーサービスに関しても割とローコストでやっている印象を受けている。ローコストというのも悪いことではないが、今回、ユーザーに向けてのアナウンスというのも、色々とウェブページを見ていたら、分かりにくい面があり、改善の余地があると思う。

（３）楽天モバイル株式会社から、令和３年９月に発生した重大な事故について説明が行われた。本事故の概要は以下のとおり。

事業者名	楽天モバイル株式会社	発生日時	令和３年９月11日 13時23分頃
継続時間	４時間３分	影響利用者数	100万人以上
影響地域	全国	事業者への問合せ件数	901件
障害内容	DNSを用いて攻撃されるセキュリティ脅威に備えてDNSサーバにアクセスする前段に設けられたファイアウォールにおいて、DNS解決要求が増加し、セキュリティ監査用のセッション保持数上限値に達したため、ファイアウォールが以降のDNS解決要求を破棄したことにより、端末より送信されるDNS解決要求の再試行と思われる事象が助長され、輻輳状態が４時間程度継続し、通常時よりデータ通信が利用しにくい状況となった。		
重大な事故に該当する電気通信役務の区分	五「一の項から四の項までに掲げる電気通信役務以外の電気通信役務」 携帯電話　三・九一四世代移動通信システムを使用するもの 第五世代移動通信システムを使用するもの		

発生原因	＜発生原因の概要＞ 　DNSサーバのUDP受信バッファの設計に問題があり、一部のDNS解決要求処理が破棄された。これにより、端末DNS解決要求の再試行が発生し、DNS攻撃防御装置（以下、ファイアウォール装置という）のセキュリティ監査用セッションの滞留が発生し上限に到達した。DNS解決要求はファイアウォール装置でも破棄されることになり、端末からのDNS解決要求の再試行をさらに助長し、問題が顕在化・長期化した。 ＜大規模化した原因＞ ① DNSサーバのUDP受信バッファサイズの考慮漏れ 　アプリケーション側のリソース設計に関しては実施していたが、プラットフォームレイヤーのパラメーターがデフォルト値のままであった。 ラボ検証においても負荷試験は行っていたが、データ通信におけるDNS解決要求処理について、バースト性の観点における負荷考慮が不足していた。 ② サービス影響の見積もり誤り 　ファイアウォール装置のセッション上限値に到達する可能性があることは以前より懸念していたが、過去の状況からその一部によるサービス影響が無いと言う前提で調査を実施していた。 ＜長期化した原因＞ ③ UDP受信バッファ溢れの監視漏れ 　DNSサーバにおける、プラットフォームレイヤーのKPIに関し、監視対象から漏れていた。 ④ DNS解決要求の成功率の検知遅延 　アプリケーションレイヤーのKPIの監視は行っていたが、監視周期が１時間毎のため、認識に至るまでにタイムラグがあった。 ⑤ DNS周辺の障害時の対処方法が未確立 　DNS周辺の障害を想定した社内マニュアル等が未整備であり、障害認知、およびサービス復旧に時間を要した。 ⑥ 社内における事故レベル判断の遅れ 　既存の事故レベル判断基準が不十分であり、社内エスカレーションに時間を要し、重大事故判定が遅れた。

機器構成図	
再発防止策	① 「DNSサーバのUDP受信バッファサイズの考慮漏れ」に対して 1) 他で利用されているDNS/DHCPサーバで現在UDP受信バッファ溢れがあるかを確認する。（暫定対処） 【令和3年9月17日完了】 2) 1)の結果、問題のあるサーバに対してバッファ溢れが発生しないように変更する。(恒久対処) 【令和3年10月1日完了】 3) DNS解決要求処理のバースト性の観点における負荷試験を追加する。（恒久対処） 【令和3年12月末 完了予定】 ② 「サービス影響の見積もり誤り」に対してサービス影響がなかったとして、繰り返し起きているものに関しては サービス影響があるものと同等のプライオリティで調査する。(恒久対処) 【令和3年9月11日完了】 ③ 「UDP受信バッファ溢れの監視漏れ」に対して該当項目を監視項目へ追加する。(恒久対処) 【令和3年9月13日完了】 ④ 「DNS解決要求の成功率の検知遅延」に対して アプリケーションレイヤーのKPIの監視を1時間毎→15分毎に短縮する。（恒久対処） 【令和3年9月12日完了】 ⑤ 「DNS周辺の障害時の対処方法が未確立」に対して手順の整備による復旧時間の短縮。(恒久対処) 【令和3年10月末 完了】 ⑥ 「社内における事故レベル判断の遅れ」に対して エンドユーザー体感に関係するKPI群を見直し、重要指標およびその閾値を再定義し、事故レベルの判定を速やかに実施。（恒久対処） 【令和3年10月末 完了】

情報周知	自社サイト	令和３年９月11日 15:25 初報掲載  令和３年９月11日 18:20 復旧報掲載 

	その他	ＳＮＳを用いた周知 

（４）議事（３）について、主に「パラメーターや監視項目の点検」及び「異常なデータに対する事前の原因分析」についての観点について、楽天モバイル株式会社及び構成員間で質疑応答が行われた。主な内容は、以下のとおり。

＜パラメーターや監視項目の点検＞

・どのように障害を検知したのかについての質問があり、ＫＰＩを１時間毎に監視しており、そこから検知したといった回答があった。
・監視が１時間毎ということは実際のユーザーへの影響は最大で検知の１時間前から発生していた可能性があるということかといった質問があり、指摘どおりその可能性があるといった回答があった。
・今回の対策として、監視の後にエスカレーションのルールや対処の方法についてもマニュアル化して進めるということかといった質問があり、そのとおりといった回答があった。

＜異常なデータに対する事前の原因分析＞

・セッション数に異常なスパイクが出ているのはいつ頃からかといった

質問があり、今回の事故の数週間前からスパイクが出ているのを認識しており、直接障害に繋がるとは思っていなかったものの、このようにスパイクが出るのはおかしいということで調査中だったといった回答があった。

・スパイクが出ている現象について、調査はしていたが、その原因は分からないまま障害が起こってしまったという理解なのか、それとも、障害にはつながらないと判断していたが実際は障害につながってしまったという認識なのかといった質問があり、トラヒックのスパイクは毎日発生しており、少しずつ量が増加している状況だったため、このままいくと容量オーバーとなり事故につながるということで調査を行っていた、ファイアウォール装置のセッション数をオーバーする可能性は認識していたものの、ここまでの事故になるというのは想定していなかったので、今回、利用者の再試行みたいな振る舞いがここまで大きくなるというところは想定外だったが、セッションが上限の５０万セッションに達する可能性があり、そうすると破棄が発生するので問題が顕在化するという意味においては、その認識でいたといった回答があった。

質疑応答を踏まえ、構成員より総括が行われた。主な発言内容は、以下のとおり。

・事故が起こってからは原因究明を適切にやっており、原因を突き止めたということは評価する。一方で、ファイアウォール装置セッションには目が行っていたが、ＤＮＳサーバーのバッファあふれというところに少なくとも当初は目が行ってなかったという辺りで、スパイクが毎日発生していることに気がついていながら、少なくとも事前に原因に行き着くことができなかったというのは残念だったという印象である。

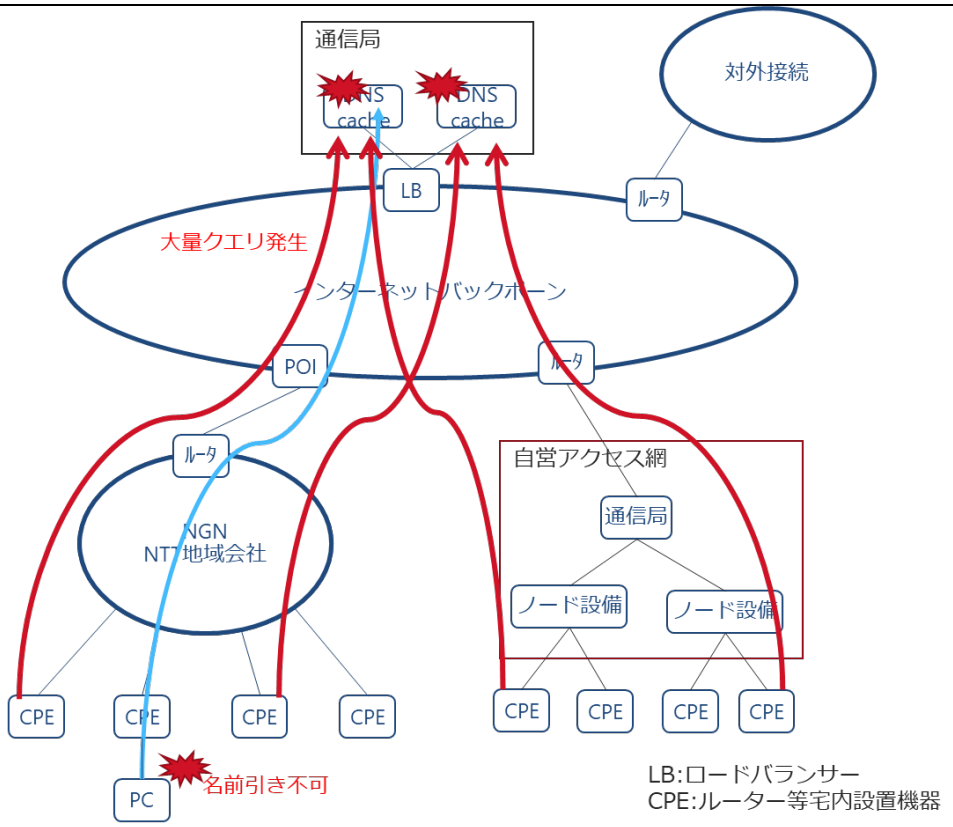
・こういうのは実際に運用してみないと分からない部分もあると思う。いろんな原因究明などをやられていることは良いが、全体的に、運用に対して、ドキュメント化やルールなどがまだ十分できていないので

はないかと感じた。なので、ある程度直感的に、問題の予兆などは進めていくと分かる部分も多いと思うので、そういう知識を今後早く蓄積して運用をしっかりやっていっていただくというのが必要だと感じた。

・ＫＰＩについてふだんのモニタリングでも可視化されているのであれば、異常検知とか故障検知の立場から見れば、この異常さに気がつくと思う。それを気がつかずに対処の優先順位も下げていたのだとしたら、可視化することや、異常さについてアドバイスするような賢い仕組みは必要だと強く感じた。数字として確認した時の認識とグラフとして描かれたときの認識は異なり、認知の限界があるのではないか。もし、スパイクがいつも１２時半に起きている場合、調べていける可能性があるため、可視化は重要と考える。しかし、サーバーの上でログを可視化すると、メモリなどの問題があるので、あまり導入されてないケースというのが多いかもしれない。これからのシステムで故障を検知する仕組みが入っていなかったとしたら、人が故障検知で認識しやすいようなビジュアライズの仕組みなどが大事になると強く感じたケースだった。

（５）アルテリア・ネットワークス株式会社から、令和３年９月に発生した重大な事故について説明が行われた。本事故の概要は以下のとおり。

事業者名	・アルテリア・ネットワークス株式会社 ・つなぐネットコミュニケーションズ株式会社※ ・株式会社ファミリーネット・ジャパン※ ・株式会社Ｕ－ＮＥＸＴ※ ・楽天モバイル株式会社※ ※アルテリア・ネットワークス株式会社からサービスの提供を受けて再販を行う電気通信事業者	発生日時	令和３年９月８日 20:48
継続時間	２時間59分	影響利用者数	最大約50万人
影響地域	全国	事業者への問合せ件数	・アルテリア・ネットワークス株式会社（37件） ・つなぐネットコミュニケーションズ株式会社（913件） ・株式会社ファミリーネット・ジャパン（25件） ・株式会社Ｕ－ＮＥＸＴ（3,935件） ・楽天モバイル株式会社（1,271件）
障害内容	事業者の払出しIPアドレスから大量の名前解決要求が発生し、DNS cacheサーバの負荷高騰により、名前解決応答不可の事象が発生。 名前解決ができないため、利用者がインターネット接続しづらい状態が発生。		
重大な事故に該当する電気通信役務の区分	一の項から四の項までに掲げる電気通信役務以外の電気通信役務（インターネット接続サービス）		
発生原因	1.ルーター等宅内設置機器が攻撃を受けDNSクエリの踏み台となったと想定。 2.想定外の名前解決要求の集中によりDNS cacheサーバが応答不可となった。		

機器構成図	
再発防止策	1. ルーター等宅内設置機器のセキュリティ上の注意点について、ユーザや卸先ISPに周知や注意喚起を実施。 【令和3年9月以降、継続して実施予定】 2. DNS cacheサーバに対して過大な名前解決要求に対して秒間クエリ数を制限する規制制御を行う運用とした。 【令和3年9月9日実施完了】

情報周知	自社サイト	＜ルテリア・ネットワークス株式会社＞ ・令和３年９月８日 23:25 初報掲載 ・令和３年９月９日　1:45 復旧報掲載  ・令和３年９月９日 10:18 続報（インターネットの接続ができない場合、再起動を促す内容を追記）掲載

ucom光 Close

UCOM光 障害情報

公開日 2021年09月09日
更新日時 2021年09月09日 02時56分

エリアコード G_AC0001
お客様各位

アルテリア・ネットワークス株式会社

【09月08日 サーバ・システム障害のご報告】

拝啓

時下、益々ご清祥の事とお慶びを申し上げます。

日頃は、弊社の『法人向け 光ファイバインターネット接続サービス UCOM光』 をご利用頂きまして、誠に有難うございます。

さて、掲題につきまして、下記サービスの障害が発生しておりましたが、 復旧作業を終え、現在は正常にご利用頂ける状態となっております。

ご利用のお客様には、 大変ご迷惑をおかけいたしましたことを深くお詫び申し上げます。

敬具

記

■対象サービス
DNS

■発生日時
09月08日(水) 20:48 ～ 09月08日(水) 23:47

■障害内容
DNSサーバー(61.122.127.154 61.122.127.74 61.122.112.1 61.122.112.97 61.122.127.90 61.122.127.106 61.122.127.122 61.122.127.138 61.122.116.174 61.122.116.147 61.122.116.179 163.139.8.202 163.139.9.202)にて障害が発生しました。

■障害原因
原因調査中

■詳細
上記DNSサーバーをプライマリ（優先）DNSサーバーに設定されている場合には、 名前解決に時間がかかった、または失敗した可能性がございます。

以上

文章番号 T0018907

ucom光 RESIDENCE

2021年9月17日

インターネット通信障害に関するお詫びと今後の対策について

2021年9月8日（水）に発生いたしました障害につきまして、弊社インターネットサービスをご利用のお客様に大変ご迷惑をお掛けいたしましたこと、深くお詫び申し上げます。
今回の障害の概要、再発防止策につきまして、以下の通りご報告申し上げます。

1．概要：
広域障害
障害内容： 外部攻撃を起因とした弊社 DNS サーバー不具合によるインターネット接続不可
発生日時： 2021年9月8日（水） 20時48分（24時間表記）
復旧日時： 2021年9月8日（水） 23時47分（24時間表記）

2．原因：
外部攻撃者が、サービスご利用中のお客様の宅内設置ルーターの脆弱性を悪用し、一時的に乗っ取り、弊社サーバーに対し大量の通信を発生させました。その結果、サーバーが高負荷となり、正常な処理を行うことができなくなったため、インターネット接続障害が発生したと判断いたしております。

3．再発防止策：
サーバーへの要求数に上限を設け、万一同様の大量リクエストが発生した場合も、高負荷状態が発生しないよう、体制を構築済です（9月9日完了）。

＜つなぐネットコミュニケーションズ株式会社＞
・令和３年９月９日 2:54 初報掲載

障害情報

お客様各位

2021年9月9日

9月8日 DNS 障害のお詫び

アルテリア・ネットワークス株式会社

拝啓　時下、益々ご清祥の事とお慶びを申し上げます。
日頃は弊社の「インターネット接続サービス」をご利用いただきまして誠に有難うございます。

さて、掲題につきまして、下記サービスの障害が発生しておりましたが、復旧作業を終え、現在は正常にサービスをご利用いただける状態となっております。
ご利用のお客様には、大変ご迷惑をおかけいたしましたことを深くお詫び申し上げます。

敬具

記

■対象ユーザー様 ： DNSをご利用のお客様

■発生日時 ： 2021年9月8日(水) 20:48頃 ～ 9月8日(水) 23:47頃

■障害内容 ： DNSサーバー(61.122.127.154 61.122.127.74 61.122.112.1 61.122.112.97 61.122.127.90 61.122.127.105 61.122.127.122 61.122.127.138 61.122.115.174 61.122.116.147 61.122.116.179 163.139.9.202 163.139.9.202)にて障害が発生しました。

■障害原因 ： 原因調査中

■詳細
上記DNSサーバーをプライマリ(優先)DNSサーバーに設定されている場合には、名前解決に時間がかかった、または失敗した可能性がございます。

以上

▲このページの先頭へ戻る

CLOSE

・令和３年９月17日 17:13 続報掲載（今後の対策について告知）

NEWS

2021年9月17日

インターネット通信障害に関するお詫びと今後の対策について

2021年9月8日（水）に発生いたしました障害につきまして、弊社インターネットサービスを ご利用のお客様に大変ご迷惑をお掛けいたしましたこと、深くお詫び申し上げます。
今回の障害の概要、再発防止策につきまして、以下の通りご報告申し上げます。

記

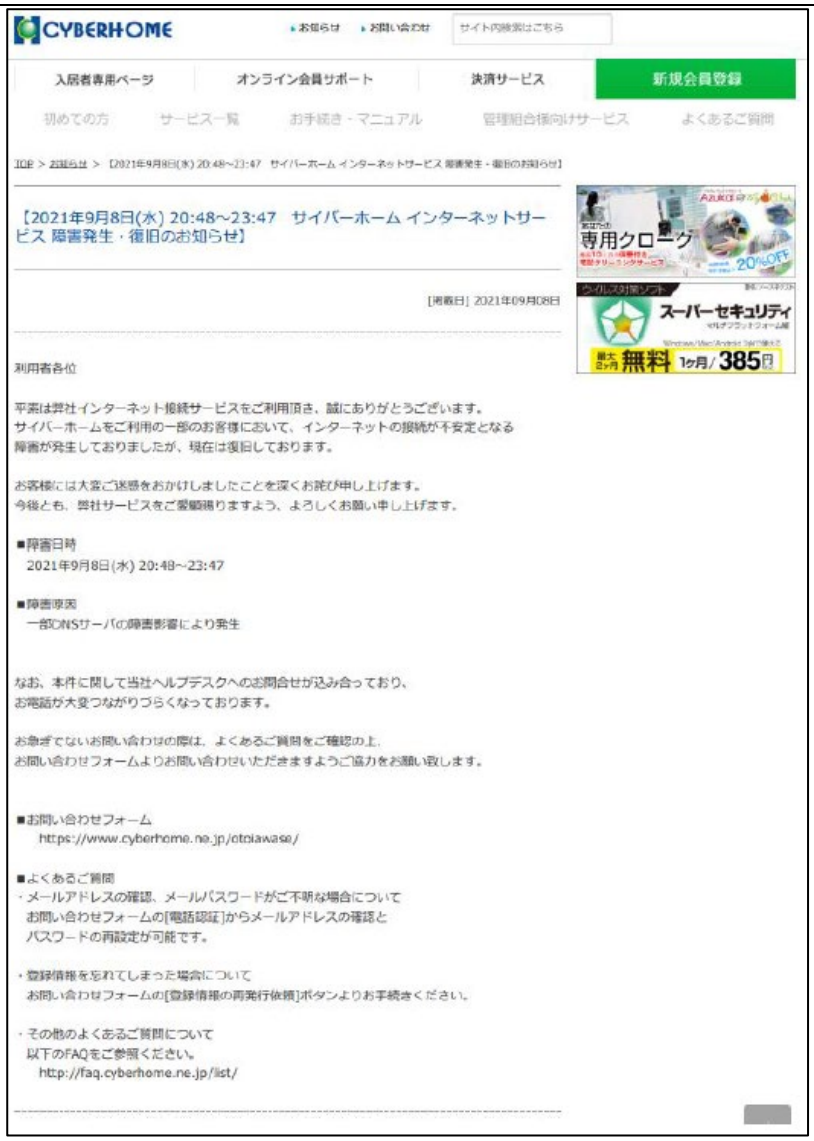
1．概要：
広域障害
障害内容： 外部攻撃を起因とした弊社DNSサーバー不具合によるインターネット接続不可
発生日時： 2021年9月8日（水） 20時48分（24時間表記）
復旧日時： 2021年9月8日（水） 23時47分（24時間表記）

2．原因：
外部攻撃者が、サービスご利用中のお客様の宅内設置ルーターの脆弱性を悪用し、一時的に乗っ取り、弊社サーバーに対し大量の通信を発生させました。その結果、サーバーが高負荷となり、正常な処理を行うことができなくなったため、インターネット接続障害が発生したと判断いたしております。

3．再発防止策：
サーバーへの要求数に上限を設け、万一同様の大量リクエストが発生した場合も、高負荷状態が発生しないよう、体制を構築済です（9月9日完了）。

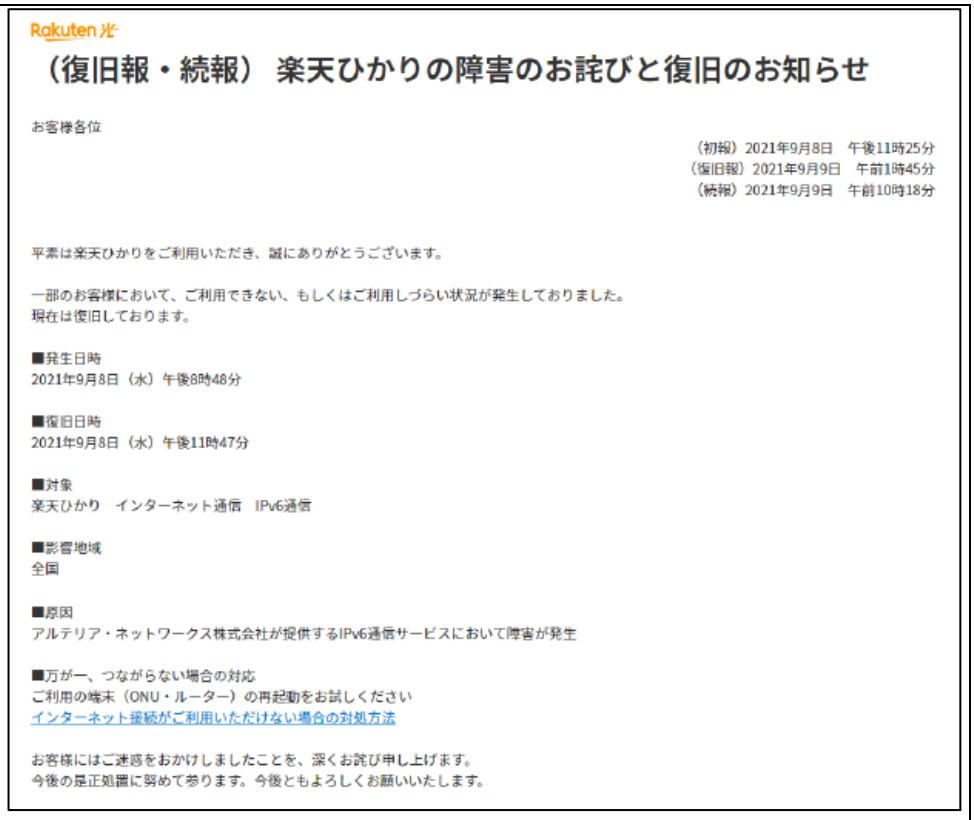
以上

＜株式会社ファミリーネット・ジャパン＞
・令和３年９月８日 21:30 初報掲載
・令和３年９月９日 6:54 復旧報掲載



＜株式会社Ｕ－ＮＥＸＴ＞
・令和３年９月９日 13:37 初報・復旧報掲載

＜楽天モバイル株式会社＞
・令和３年９月８日 23:25 初報掲載
・令和３年９月９日 1:45 復旧報掲載
・令和３年９月９日 10:18 続報（インターネットが接続できない場合、再起動を促す内容を追記）掲載

		 Rakuten 光 （復旧報・続報） 楽天ひかりの障害のお詫びと復旧のお知らせ お客様各位 （初報）2021年9月8日　午後11時25分 （復旧報）2021年9月9日　午前1時45分 （続報）2021年9月9日　午前10時18分 平素は楽天ひかりをご利用いただき、誠にありがとうございます。 一部のお客様において、ご利用できない、もしくはご利用しづらい状況が発生しておりました。 現在は復旧しております。 ■発生日時 2021年9月8日（水）午後8時48分 ■復旧日時 2021年9月8日（水）午後11時47分 ■対象 楽天ひかり　インターネット通信　IPv6通信 ■影響地域 全国 ■原因 アルテリア・ネットワークス株式会社が提供するIPv6通信サービスにおいて障害が発生 ■万が一、つながらない場合の対応 ご利用の端末（ONU・ルーター）の再起動をお試しください インターネット接続がご利用いただけない場合の対処方法 お客様にはご迷惑をおかけしましたことを、深くお詫び申し上げます。 今後の是正処置に努めて参ります。今後ともよろしくお願いいたします。
	その他	＜アルテリア・ネットワークス株式会社＞ ・令和３年９月８日 23:25 障害発生の旨 報道発表 ・令和３年９月９日　1:45 復旧の旨 報道発表

（６）議事（５）について、主に「障害の原因」及び「再発防止策」についての観点について、アルテリア・ネットワークス株式会社及び構成員間で質疑応答が行われた。主な内容は、以下のとおり。

＜責任分界点について＞

・今回の障害の原因というのが、ＣＰＥが乗っ取られてそれが原因でアタックを受けたというようなことが想定されるが、ＣＰＥルーターの管理は、ユーザー側の責任なのか、サービス提供業者の責任なのか教えて欲しいとほしいといった質問があり、ＣＰＥルーターはユーザーの設備であり、通信事業者のものではないため、責任分界点ということでは、ユーザー側のものになるといった回答があった。

＜障害の原因及び再発防止策について＞

・今回の障害の原因がＣＰＥルーターであること、サイバー攻撃であることの根拠について質問があり、各ＣＰＥルーターが持っているソースのＩＰアドレスまでは確認できており、ＣＰＥルーターからの通常のクエリと考えていること、そのクエリが複数のＣＰＥから同時並行的に来ているため、外部からの攻撃者によるものだと判断しているが、通信の復旧のためにＣＰＥの再起動や初期化をユーザーにお願いしたこともあり、ログ等の証拠が中々つかめない状況であるといった回答があった。また、ユーザーに注意喚起をしても、対策はそれだけで十分なのかどうかというのは難しいのではないかといった質問があり、ＣＰＥのセキュリティを高めるためにユーザーに対する啓蒙活動をやっていくのは通信事業者の責務だと考えているので、今後も続けていきたいといった回答があった。
・ＤＮＳキャッシュサーバーのリソース関して問題はなかったかといった質問があり、ピーク時においても５０%以下のロードになるようにキャパシティーの設計をしており、今回のような異常時には対応できなかったが、念のため、キャパシティーアップを図ることが必要ということで、現状は設備の増設を行った次第であるといった回答があった。
・ＤＤｏＳ等への対処について、サービス提供側でトラヒック等を見てブロックするなどの対処をする必要があるため、今後、ＤＤｏＳに対応した装置や対応方法などを検討して、システムとして投入することが望ましいといったコメントがあった。
・秒間クエリ数の制限について、どこで規制を行うのかといった説明があり、ＤＮＳキャッシュサーバーで規制を行うといった回答があった。
・ＩＰアドレスをブロックしたにもかかわらず、状況は改善しなかったことについて質問があり、当時、攻撃の内容が理解できていなかったので、恐らく集中的なクエリがあるのではないかということで、クエリを受けている上位のＩＰアドレスを制限したが、実態は広く多くの複数のＣＰＥからクエリが発出されていたため、１ＩＰごとのｑｐｓを制限するというような対策につながったといった回答があった。

・１ＩＰ毎のｑｐｓ制限を平時から行わないのかといった質問があり、通常時に行ってしまうと通常の通信にも影響が出てしまう。そのため、障害時のみ対策としているといった回答があった。

質疑応答を踏まえ、構成員より総括が行われた。主な発言内容は、以下のとおり。

・各所からのクエリ数はそれほど多くないということだと、これがＤＤｏＳ攻撃だったのかどうかというようなことを確認するのはなかなか難しいかと思う。今回の件も恐らくそうだったということで、今、こういうサイバー攻撃は増えつつある。少なくともこのような件があったということについては通信事業者の間でも共有していくことが必要かと思う。その一方で、構成員からも指摘があったように、狙われたのが責任分界点よりも内側にあるユーザーの装置だということになると、完璧な対策というのは難しいかと思う。
・そもそもアルテリアではレガシーなシステムで運用されているというのが、大変だろうと思った。もう一つ、対処方法としては、ユーザーに周知して対策を個別に取ってもらうしかないのかなというのが、とても難しい案件だと思った。　ユーザーへの周知となると、新しいルーターに替えようとか、パスワードは変えましたかとか、注意喚起をし過ぎてしまうと別の業者に変えてしまう可能性もある。逆に言えば、そういったユーザーというのは別の業者に行っても同じ危険性を持って渡り歩いていくのかなとか、懸念のある案件な気がしている。
・最低限、ルーターの初期パスワードを別のものに変えるといったセキュリティ対策というのはやる必要があり、それを義務化するのかについてはまだまだ今後も検討する必要があると思う。現状、サイバーセキュリティの案件が増えているということも踏まえて、ソフトウェア的な設定の必要性を今後どう徹底していくかという問題かと思う。
・対策が難しいという感想ではいるが、ＣＰＥだけの問題かというと、そこにつないでいるユーザーの端末も何がつながっているのか分からないし、ユーザーもよく分からないところがあるかと思う。だから、

対策はどうするかというのは本当に難しいとしか言いようがない。ただ、今後、こういうことを想定してサービス提供事業者がどういうふうに対応していくかって、ＤＤｏＳのアタックの検出とか、そういうのを積極的にやることが必要になってくるのかなという気はする。ただ、パケットの中身まで見てコントロールしようとするのはいろんな面で課題があり、通信の秘密といった、当然、法的な問題を言うユーザーも出てくるし、そこも全部含めてうまくできるような方法を模索していく必要がある。そういうことを考慮して、今後、議論をして進めていく必要があるというのを再認識した。

（７）総務省から、令和３年度第１四半期に発生した電気通信事故の集計結果について説明が行われた。

以上