

お客様各位

2010年2月1日

株式会社北都

DDoS 攻撃によるサーバ通信障害のご報告

謹啓 平素は格別のお引き立てを賜り、厚くお礼申し上げます。

このたび、弊社が OEM で提供するサーバホスティングサービス（OEM 元 GMO ホスティング&セキュリティ株式会社）におきまして、2010年1月27日12時55分頃より、全世界140万IPから1時間に4億3000万パケットを超える大規模かつ執拗なサービス妨害攻撃（DDoS 攻撃※）を受けました。その結果、長時間かつ複数回にわたりネットワーク（ファイアウォール）が通信障害に陥り、ご利用中の約40,000アカウント（弊社提供84アカウント）のお客さまに、ウェブサイトへのアクセス不可、メールの送受信不可といった多大なご迷惑をおかけいたしました。このような事態を招きましたことにつきまして、改めて衷心よりお詫び申し上げます。

※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サーバーへパケットを送出し、通信路をあふれさせて機能を停止させてしまう攻撃のこと

ただし、通信の障害中においてもサーバは稼動しており、クラック等の被害には遭っておりません。したがって、サーバに收容されているお客さま情報の漏洩や、データの破損はございませんのでご安心ください。

現時点でも、依然として大規模な DDoS 攻撃は続いておりますが、問題解決に向け、さまざまな手段での対策を講じた結果、現在、約99.6%のお客さまにおかれましては通信が完全に復旧しております。

弊社では、本件の問題解決に全力で取り組んでまいりましたが、結果としてお客さまに多大なご迷惑をおかけいたしました。これを真摯に受け止め、今回の経緯につきましてご報告申し上げるとともに、DDoS 攻撃に対し、サービス根幹部分で更なる増強対策を行うことをご報告申し上げます。

お客さま各位におかれまして何卒事情ご理解のうえ、格段のご配慮を賜りますとともに、サーバホスティングサービスを今後もお引き立ていただきますよう、謹んでお詫び方々お願い申し上げます。

謹白

記

■概要

2010年1月27日12時55分頃よりホスティングサービスにおきまして、DDoS攻撃が確認されました。この攻撃によるファイアウォールへの負荷により、全てのお客さまのウェブサイト閲覧とメールの送受信ができない状況が発生しました。

2010年1月29日9時00分現在、DDoS攻撃対応機器の増強などにより、約99.6%のお客さまの通信は完全に復旧しており、残りの約0.4%のお客さまに関しましてはウェブサイトのみ閲覧しづらい状況です。

○通信障害時間

1月27日 12時55分～19時30分 (395分)

1月27日 21時40分～26時17分 (277分)

1月28日 10時10分～16時25分 (375分)

1月28日 18時00分～23時18分 (318分)

■障害原因

ボットネット※を利用したと思われるDDoS攻撃(4億3000万パケット/時)により、ファイアウォールが高負荷となり、お客さまのデータが収容されているサーバへのアクセスが極端に行いづらいという障害が発生いたしました。

※ボットネットとは、マルウェアなどによって多くのパソコンやサーバーに遠隔操作できる攻撃用プログラム(ボット)を送り込み、外部からの指令で一斉に攻撃を行なわせるネットワークのこと

■対応内容

DDoS攻撃対応機器を増強することで、攻撃と思われる通信を遮断し、ファイアウォールの負荷軽減を行いました。

■今後の対応

(1) 被害届の提出

現在、OEM元であるGMOホスティング&セキュリティ株式会社が警察と相談を行っており、近日中に被害届を提出いたします。また、IPA(独立行政法人情報処理推進機構)へ状況を届け出ることによって、同種攻撃に対する被害防止策の啓蒙に役立ててまいります。

(2) システム構成の強化

今回受けた、DDoS 攻撃 (4 億 3000 万パケット/時) よりもさらに大規模な攻撃を受けた場合でも、お客さまへの被害を最小限に抑えるべく、より高性能な DDoS 攻撃対応機器を追加増強いたします。

■お客さま対応方針

お客さまより情報の開示 (ログ等) に関する要請があった場合には開示いたします。

■経緯報告

2010 年 1 月 27 日

12 時 55 分

DDoS 攻撃を受け、ファイアウォールが高負荷になる

16 時 55 分

攻撃対象の IP アドレスを特定し、同 IP アドレスへのアクセスを遮断、約半分のお客さまのウェブサービスが利用可能な状態になる

全てのお客さまのメールサービスが利用可能になる

19 時 00 分

攻撃対象のお客さまの IP アドレスを変更開始

IP アドレスが変更されたお客さまのウェブサービスも順次利用可能になる

19 時 30 分頃

攻撃が収束し、全てのお客さまにおいて全サービスが利用可能となる

21 時 40 分

攻撃が再開され、ファイアウォールの負荷増のため全サービスが不安定な状態になる

2010 年 1 月 28 日

02 時 17 分

弊社ファイアウォールの上位にて攻撃対象 IP アドレスへのアクセスを遮断することで、一部のお客さまを除いてはウェブ、メールサービスがともに利用可能となる

04 時 30 分

攻撃対象であったお客さまの IP アドレスをさらに複数に分散、変更する対応を開始

06 時 54 分

約 96%のお客さまにおいて、ウェブ、メールサービスが利用可能になる

10 時 10 分

新しい IP アドレスに対する攻撃が開始され、再びファイアウォールの負荷が増大し、全サービスが不安定な状態になる

13 時 00 分

攻撃元や攻撃対象を分析するため機器の増強

13 時 45 分	攻撃元と疑われる IP アドレスと攻撃対象 IP アドレスを特定、 攻撃元と特定した IP アドレスからのアクセスを遮断するも、フ ァイアウォールの負荷が下がらず状況好転せず
16 時 25 分	攻撃対象の IP アドレスへのアクセスを遮断し、一部のお客さま を除き、全サービスが利用可能な状態となる
23 時 18 分	DDoS 攻撃対応機器の増強が完了し、約 99.6%のお客さまにおい て全サービスが復旧

本件に関し、以上ご報告申し上げます。

長時間にわたりお客さまに多大なるご迷惑をおかけしましたこと、改めて深くお詫び申し
上げます。

以上

■本件に関するお問い合わせ先

株式会社北都 制作企画部 IT 事業課

電話：025-385-4225（直通）

025-385-4333（代表）

FAX：025-385-3974

フォーム：<http://www.hokuto-com.co.jp/web/>