

バラクーダネットワークスジャパン株式会社

バラクーダレピュテーション について

2014年12月
第1.3版

本文書の内容は予告なく変更される場合があります。

本文書の内容の無断転載はできません。

Copyright 2004-2014 Barracuda Networks, Inc.

改版履歴

日付	変更箇所
2010年9月15日	初版
2012年10月31日	オフィス住所を新住所に変更
2013年2月22日	IPレピュテーションへの登録の仕組みを追記
2014年12月9日	ロゴを新ロゴに変更

目次

1	本書の目的	4
2	バラクーダレピュテーション	5
2.1	バラクーダセントラルについて	5
2.2	バラクーダレピュテーションについて	5
2.2.1	バラクーダ IP レピュテーション	5
2.2.2	バラクーダ IP ホワイトリスト	5
3	バラクーダ IP レピュテーションに登録される主な理由	6
3.1	バラクーダ IP レピュテーションに IP アドレスが登録される主な原因	6
3.1.1	メールサーバのオープンリレーの許可	6
3.1.2	ボット感染による無差別大量メールの送信	6
3.1.3	大量の広告メールやメールマガジンを一気に送信してしまう	6
3.1.4	大量のメールを存在しない受信者宛てに送信する	7
3.1.5	NDR スпам (Backscatter) 対策を実施していない	7
3.2	DHA 攻撃について	7
3.3	NDR スпам について	8
4	バラクーダレピュテーションの登録解除方法	9
4.1	登録状況の確認	9
4.2	登録解除申請	10
4.3	解除申請のタイミング	12
4.3.1	バラクーダ製品をご利用されている場合	12
4.3.2	バラクーダ製品をご利用されていない場合	13
5	参考	14

1 本書の目的

バラクーダレピュテーションは、米国バラクーダネットワークスが運営しているバラクーダセントラルによって管理されております。バラクーダセントラルでは、世界中でご使用中のスパムメール対策製品である **Barracuda Spam Firewall** からのフィードバックやハニーポットに送信されたメールを解析して、バラクーダレピュテーションの IP リストを作成しております。

本文書は、バラクーダ IP レピュテーションに登録された場合の解除の申請方法、バラクーダ IP レピュテーションに登録される主な原因について説明致します。

尚、バラクーダネットワークスジャパンでは、バラクーダ IP レピュテーションに登録された理由についてお問い合わせいただいても、お答えすることはできませんので予めご了承願います。

2 バラクーダレピュテーション

2.1 バラクーダセントラルについて

米国バラクーダネットワークスが運営するオペレーションセンターであるバラクーダセントラルは、スパム、スパイウェア、ウィルス、その他のセキュリティ脅威に対する定義ファイル・データベースの開発・運営・提供を実施しております。バラクーダセントラルでは、常時インターネットを監視し、新たな脅威に備え、早期にこうした傾向を発見することで、新たなセキュリティ脅威を検出しそれを遮断する技術を迅速に対応しています。

2.2 バラクーダレピュテーションについて

バラクーダレピュテーションはバラクーダセントラルによって管理されており、正当な送信者の IP アドレスと、スパム送信者として知られる IP アドレスのリストを保持しています。バラクーダレピュテーションのデータベースの更新は、エネルギー充填サービスを利用して **Barracuda Spam & Virus Firewall** に配信されます。バラクーダレピュテーションサービスには以下の 2 種類が含まれます。

2.2.1 バラクーダ IP レピュテーション

スパムの送信元であると検証された IP アドレスのデータベースです。このリストにある IP アドレスからのメール送信は拒否されます。

2.2.2 バラクーダ IP ホワイトリスト

スパムを送信していないと分かっている IP アドレスのデータベースです。

3 バラクーダ IP レピュテーションに登録される主な理由

広告メールを一度に大量に送信していたり、そのようなことがなくとも知らぬ間に、スパムメールを送信またはリレーしてしまっているメールサーバは、バラクーダ IP レピュテーションにそのメールサーバの IP アドレスが登録される恐れがあります。

バラクーダ IP レピュテーションへの登録は弊社管理のハニーポットへのスパムメールの解析、及びお客様がご使用中の Barracuda Spam & Virus Firewall からのフィードバックにより自動的に行われますので予期せぬ IP アドレスが登録されてしまうこともございます。予めご了承ください。

3.1 バラクーダ IP レピュテーションに IP アドレスが登録される主な原因

バラクーダ IP レピュテーションにメールサーバの IP アドレスが登録される主な原因となる事例についてご説明致します。

3.1.1 メールサーバのオープンリレーの許可

オープンリレーとは、IP アドレスやドメイン、送信元、宛先などの制限無く、誰でも自由にメール送信を依頼することができるメールサーバを意味します。オープンリレーはスパムなどの迷惑メールの送信手段として利用されてしまうことが多いため、現在のメールサーバプログラムのほとんどはデフォルトでオープンリレーの設定は無効にされています。

3.1.2 ボット感染による無差別大量メールの送信

ウイルスやスパイウェアに感染してしまったパソコンで、無差別大量にスパムを送信するようなプログラムに感染してしまったために、無差別大量にスパムメールを送信するパソコンがお客様の環境内に存在する場合があります。このようなパソコンは別名ゾンビ PC とも呼ばれています。

通常、IRC と言われるプログラムを利用して、親プログラム（スパム送信業者）が感染したゾンビ PC を自由にあやつり、知らない間にある感染源のパソコンから大量スパムが送信されているケースが多いです。

3.1.3 大量の広告メールやメールマガジンを一気に送信してしまう

大量のメールマガジンやダイレクトメールを一度に大量に送信してしまうと、短時間に大量のスパムを送信する攻撃として認識され、バラクーダ IP レピュテーションに登録される可能性があります。

3.1.4 大量のメールを存在しない受信者宛てに送信する

DHA (Directory Harvest Attack) 攻撃と呼ばれ、あたかも存在しそうなメールアドレスに対して、大量にメールを送信することで、実際に有効なメールアドレスを探し出す攻撃手法として知られています。DHA 攻撃により、実際に存在するメールアドレスを収集した後、スパム送信用のメールアドレスリストとしてスパム業者間でリストの売買が行われ、悪用される可能性が高いことで知られています。

DHA 攻撃は、ボット感染したパソコンなどから送信されるものが一般的です。DHA 攻撃については、[DHA 攻撃について](#)を参照してください。

3.1.5 NDR スпам (Backscatter) 対策を実施していない

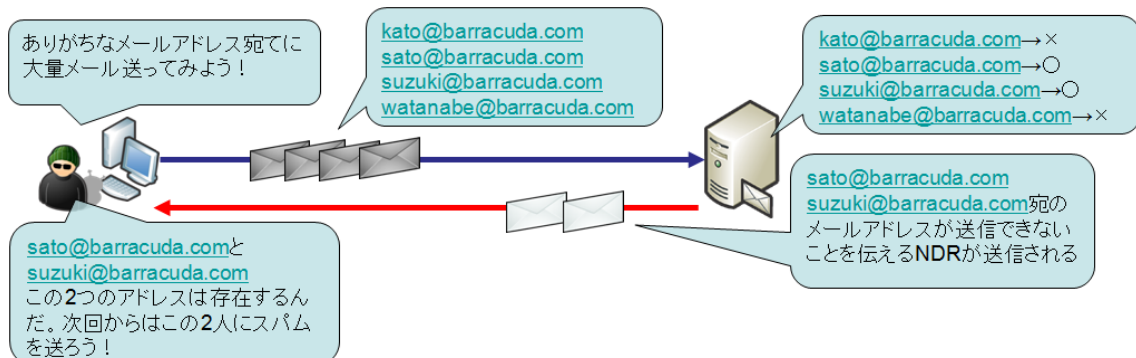
メールサーバの配達不能レポート (NDR) 機能を利用して、スパムを配信する新たなスパム送信手法で 2008 年ごろから日本国内でも被害例が報告されています。正常なメールサーバに関わらず、バラクーダ IP レピュテーションに登録される原因が一番高いスパム送信手法です。別名 Backscatter とも呼ばれています。

NDR スпамについては、[NDR スпам について](#)を参照してください。

3.2 DHA 攻撃について

DHA 攻撃例を図式にてご紹介します。

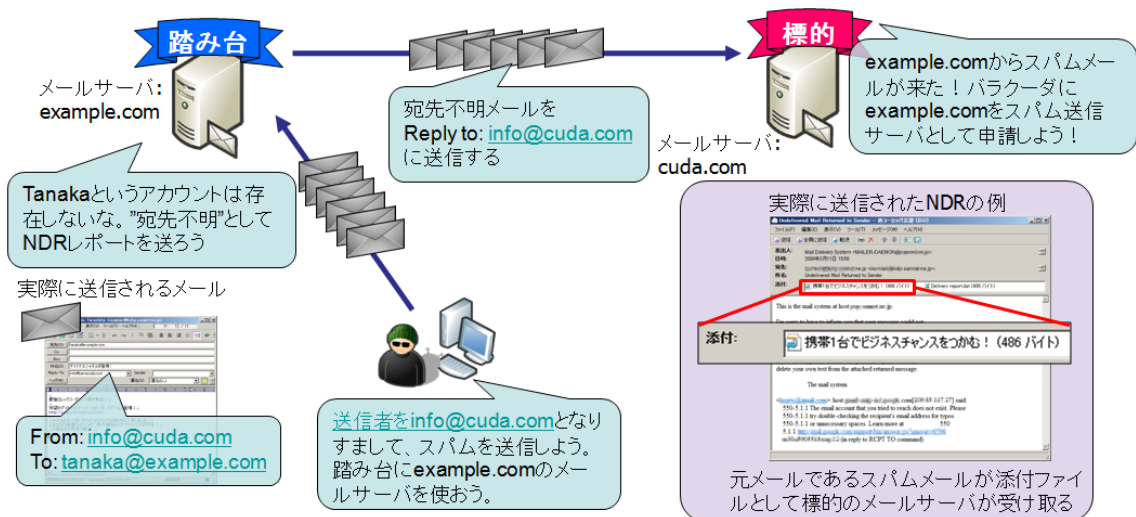
あたかも存在しそうなメールアドレスに対してメールを送信すると、正常な動作を行うメールサーバでは、存在しないメールアドレス宛てにメールが送信されると、それを配信不達レポート (NDR) として送信者に自動的にメールを送信します。送信者は配信不達レポートを受信することで、実際に有効なメールアドレスを割り出し、スパム送信用のメールアドレスリストとして悪用されることがあります。



3.3 NDR スпам について

スパム送信者は送信元メールアドレスを標的となるメールサーバが使用するメールアドレスになりまし、DHA 攻撃同様、存在しないメールアドレス宛てにメールが送信します。メールサーバは、配信不達レポート (NDR) を送信者元のメールサーバに送信しますが、実際には送信されたメールアドレスがなりすまされているため、実際の送信元とは別の、標的となるメールサーバに配信不達レポート (NDR) が送信されます。

踏み台となったメールサーバは、知らずうちに配信不達レポートを利用して、スパムメールを送信しており、その結果、スパムの送信者として認識される可能性があります。



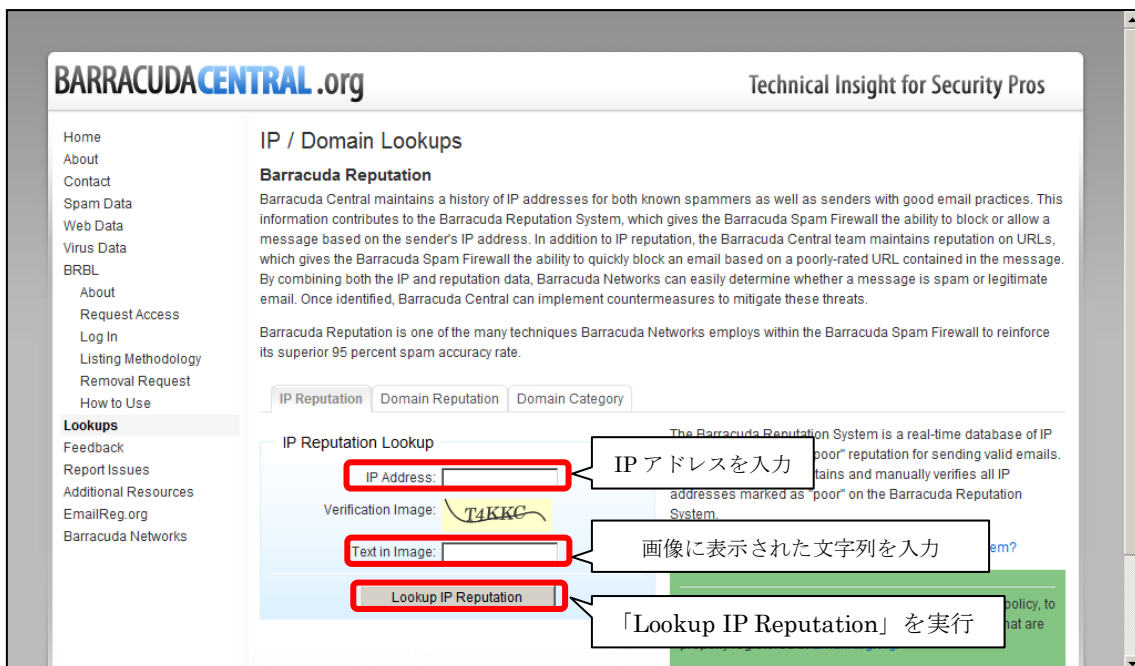
4 バラクーダレピュテーションの登録解除方法

バラクーダ IP レピュテーションにお客様がご使用になられている IP アドレスが登録されてしまった場合、お客様ご自身で米国バラクーダセントラルに登録解除依頼をする必要があります。バラクーダネットワークスジャパンでは、登録された IP アドレスの解除依頼を承ることができませんので、ご了承願います。

4.1 登録状況の確認

まずバラクーダセントラルにお客様の IP アドレスがバラクーダ IP レピュテーションとして登録されているかどうか、登録情報を調べます。

<http://www.barracudacentral.org/lookups> にアクセスします。「IP Address」欄にお客様がご使用の IP アドレス、「Verification Image」に画像で表示されている文字列を入力し、「Lookup IP Reputation」をクリックします。



「Lookup IP Reputation」を実行後、緑色で「**The ip address xxx.xxx.xxx.xxx is not currently listed as “poor” on the Barracuda Reputation System.**」と表示される場合、その IP アドレスはバラクーダ IP レピュテーションに登録されていないことを示します。



BARRACUDACENTRAL.org Technical Insight for Security Pros

Home
About
Contact
Spam Data
Web Data
Virus Data
BRBL
 About
 Request Access
 Log In
 Listing Methodology
 Removal Request
 How to Use

Lookups
Feedback
Report Issues
Additional Resources
EmailReg.org
Barracuda Networks

IP / Domain Lookups

Barracuda Reputation
Barracuda Central maintains a history of IP addresses for both known spammers as well as senders with good email practices. This information contributes to the Barracuda Reputation System, which gives the Barracuda Spam Firewall the ability to block or allow a message based on the sender's IP address. In addition to IP reputation, the Barracuda Central team maintains reputation on URLs, which gives the Barracuda Spam Firewall the ability to quickly block an email based on a poorly-rated URL contained in the message. By combining both the IP and reputation data, Barracuda Networks can easily determine whether a message is spam or legitimate email. Once identified, Barracuda Central can implement countermeasures to mitigate these threats.

Barracuda Reputation is one of the many techniques Barracuda Networks employs within the Barracuda Spam Firewall to reinforce its superior 95 percent spam accuracy rate.

IP Reputation Domain Reputation Domain Category

IP Reputation Lookup

The ip address **77.81.107.110** is not currently listed as "poor" on the Barracuda Reputation System.

IP Address:

Verification Image: 

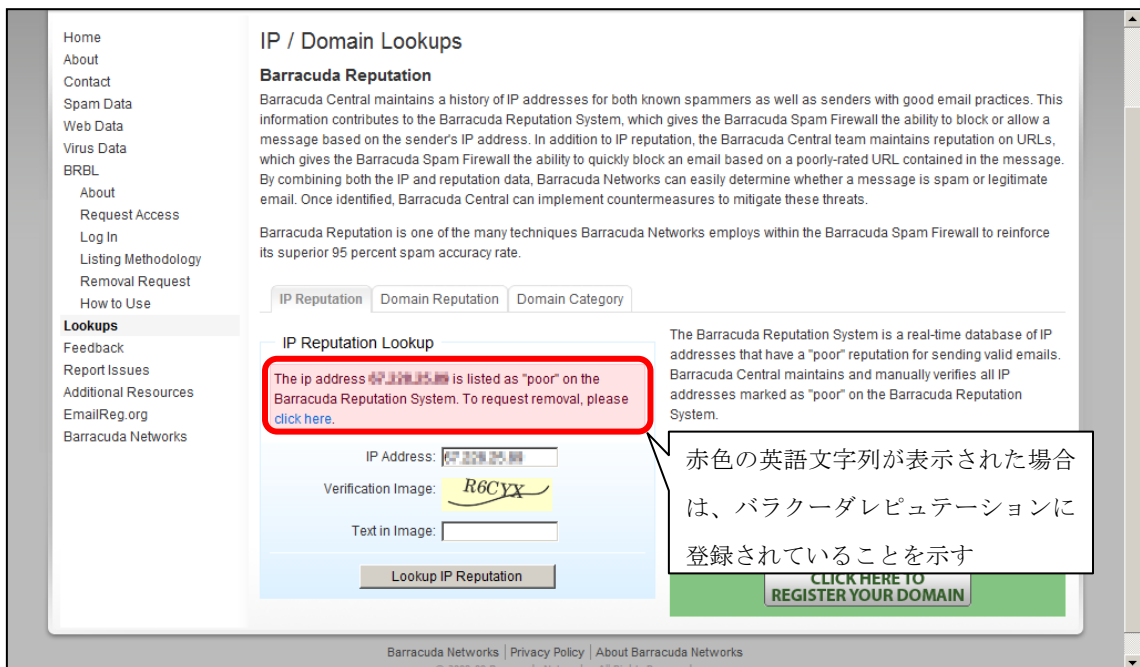
Text in Image:

Lookup IP Reputation

The Barracuda Reputation System is a real-time database of IP addresses that have a "poor" reputation for sending valid emails. Barracuda Central maintains and manually verifies all IP addresses marked as "poor" on the Barracuda Reputation System.

緑色の英語文字列が表示された場合は、バラクーダレピュテーションに登録がないことを示す

「Lookup IP Reputation」を実行後、赤色で「**The ip address xxx.xxx.xxx.xxx is listed as "poor" on the Barracuda Reputation System. To Request removal, please click here**」と表示される場合、その IP アドレスは現在、バラクーダ IP レピュテーションに登録されていることを示します。



Home
About
Contact
Spam Data
Web Data
Virus Data
BRBL
 About
 Request Access
 Log In
 Listing Methodology
 Removal Request
 How to Use

Lookups
Feedback
Report Issues
Additional Resources
EmailReg.org
Barracuda Networks

IP / Domain Lookups

Barracuda Reputation
Barracuda Central maintains a history of IP addresses for both known spammers as well as senders with good email practices. This information contributes to the Barracuda Reputation System, which gives the Barracuda Spam Firewall the ability to block or allow a message based on the sender's IP address. In addition to IP reputation, the Barracuda Central team maintains reputation on URLs, which gives the Barracuda Spam Firewall the ability to quickly block an email based on a poorly-rated URL contained in the message. By combining both the IP and reputation data, Barracuda Networks can easily determine whether a message is spam or legitimate email. Once identified, Barracuda Central can implement countermeasures to mitigate these threats.

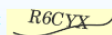
Barracuda Reputation is one of the many techniques Barracuda Networks employs within the Barracuda Spam Firewall to reinforce its superior 95 percent spam accuracy rate.

IP Reputation Domain Reputation Domain Category

IP Reputation Lookup

The ip address **87.238.89.81** is listed as "poor" on the Barracuda Reputation System. To request removal, please [click here](#).

IP Address:

Verification Image: 

Text in Image:

Lookup IP Reputation

The Barracuda Reputation System is a real-time database of IP addresses that have a "poor" reputation for sending valid emails. Barracuda Central maintains and manually verifies all IP addresses marked as "poor" on the Barracuda Reputation System.

赤色の英語文字列が表示された場合は、バラクーダレピュテーションに登録されていることを示す

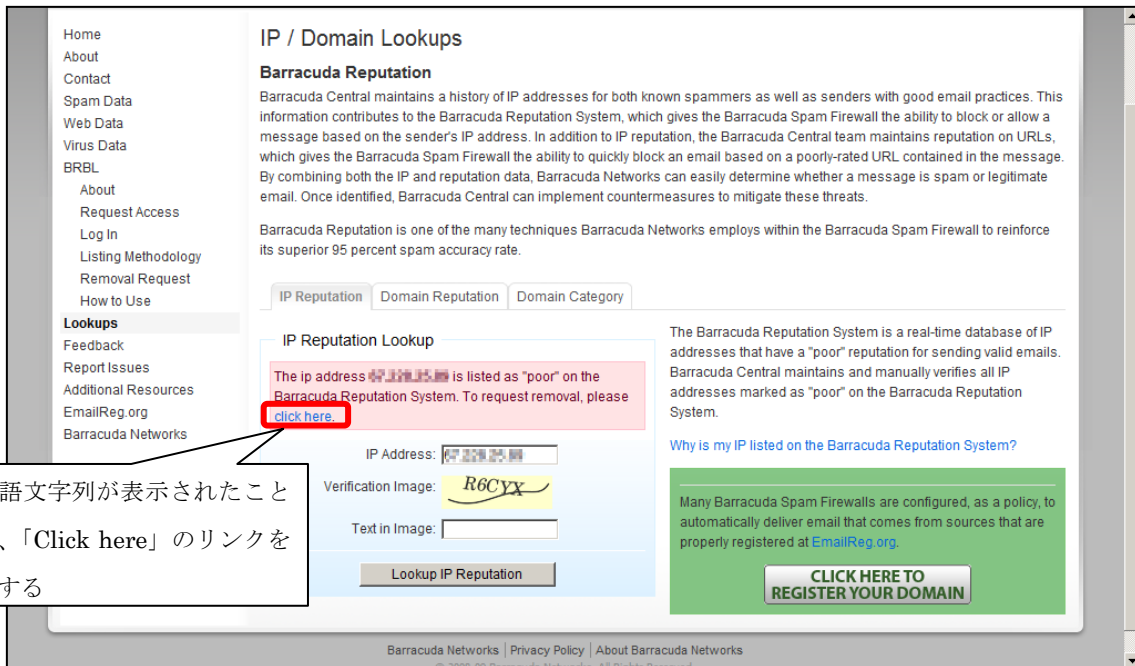
[CLICK HERE TO REGISTER YOUR DOMAIN](#)

Barracuda Networks | Privacy Policy | About Barracuda Networks
© 2008-09 Barracuda Networks. All Rights Reserved.

4.2 登録解除申請

IP アドレスの登録を確認した後、バラクーダ IP レピュテーションの登録解除申請を行う場合は、IP Reputation Lookup の実行結果の「Click here」リンクをク

リックします。



Home
About
Contact
Spam Data
Web Data
Virus Data
BRBL
 About
 Request Access
 Log In
 Listing Methodology
 Removal Request
 How to Use
Lookups
Feedback
Report Issues
Additional Resources
EmailReg.org
Barracuda Networks

IP / Domain Lookups

Barracuda Reputation

Barracuda Central maintains a history of IP addresses for both known spammers as well as senders with good email practices. This information contributes to the Barracuda Reputation System, which gives the Barracuda Spam Firewall the ability to block or allow a message based on the sender's IP address. In addition to IP reputation, the Barracuda Central team maintains reputation on URLs, which gives the Barracuda Spam Firewall the ability to quickly block an email based on a poorly-rated URL contained in the message. By combining both the IP and reputation data, Barracuda Networks can easily determine whether a message is spam or legitimate email. Once identified, Barracuda Central can implement countermeasures to mitigate these threats.

Barracuda Reputation is one of the many techniques Barracuda Networks employs within the Barracuda Spam Firewall to reinforce its superior 95 percent spam accuracy rate.

IP Reputation Domain Reputation Domain Category

IP Reputation Lookup

The ip address 172.16.17.17 is listed as "poor" on the Barracuda Reputation System. To request removal, please [click here](#)

IP Address: 172.16.17.17
Verification Image: R6Cyx
Text in Image:

The Barracuda Reputation System is a real-time database of IP addresses that have a "poor" reputation for sending valid emails. Barracuda Central maintains and manually verifies all IP addresses marked as "poor" on the Barracuda Reputation System.

Why is my IP listed on the Barracuda Reputation System?

Many Barracuda Spam Firewalls are configured, as a policy, to automatically deliver email that comes from sources that are properly registered at [EmailReg.org](#).

Barracuda Networks | Privacy Policy | About Barracuda Networks

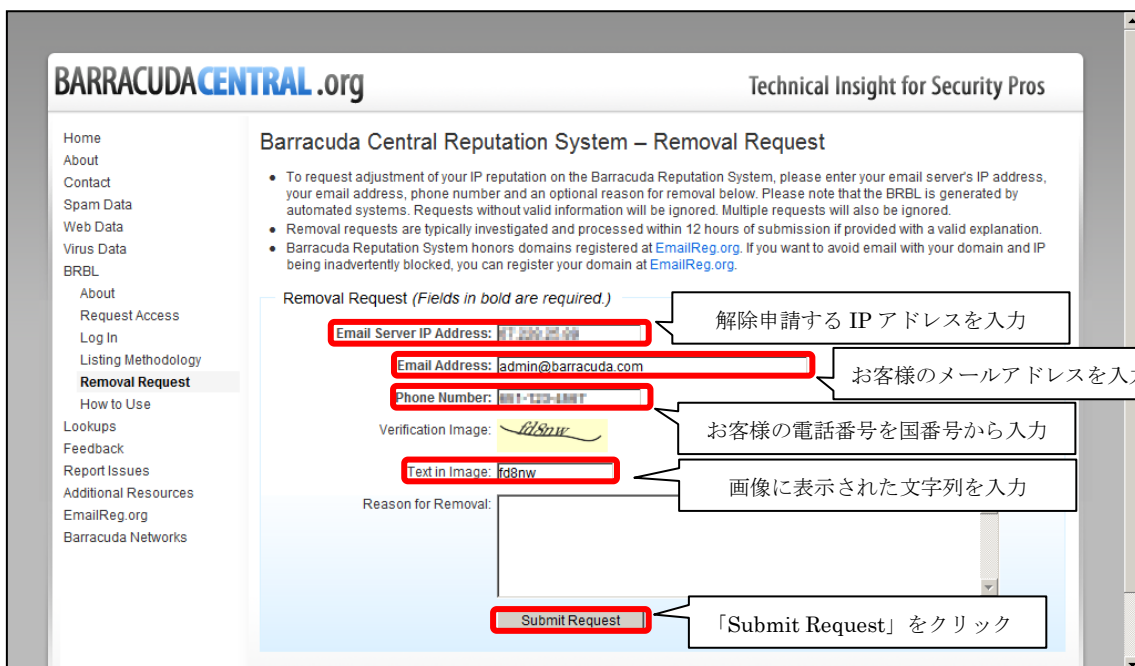
赤色の英語文字列が表示されたことを確認し、「Click here」のリンクをクリックする

登録解除申請ページに移動しますので、必要事項を記入し、「Submit Request」をクリックします。記入の必須項目は以下のとおりとなります。

- **Email Server IP Address:** 解除申請をする IP アドレスを入力
- **Email Address:** お客様のメールアドレス
- **Phone Number:** 電話番号を国番号から入力

(例) 03-1234-5678 の場合「81-3-1234-5678」と入力

「Reason for Removal」は未記入で構いません。



BARRACUDA CENTRAL.org Technical Insight for Security Pros

Barracuda Central Reputation System – Removal Request

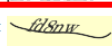
- To request adjustment of your IP reputation on the Barracuda Reputation System, please enter your email server's IP address, your email address, phone number and an optional reason for removal below. Please note that the BRBL is generated by automated systems. Requests without valid information will be ignored. Multiple requests will also be ignored.
- Removal requests are typically investigated and processed within 12 hours of submission if provided with a valid explanation.
- Barracuda Reputation System honors domains registered at [EmailReg.org](#). If you want to avoid email with your domain and IP being inadvertently blocked, you can register your domain at [EmailReg.org](#).

Removal Request (Fields in bold are required.)

Email Server IP Address: 172.16.17.17 解除申請する IP アドレスを入力

Email Address: admin@barracuda.com お客様のメールアドレスを入力

Phone Number: 81-3-1234-5678 お客様の電話番号を国番号から入力

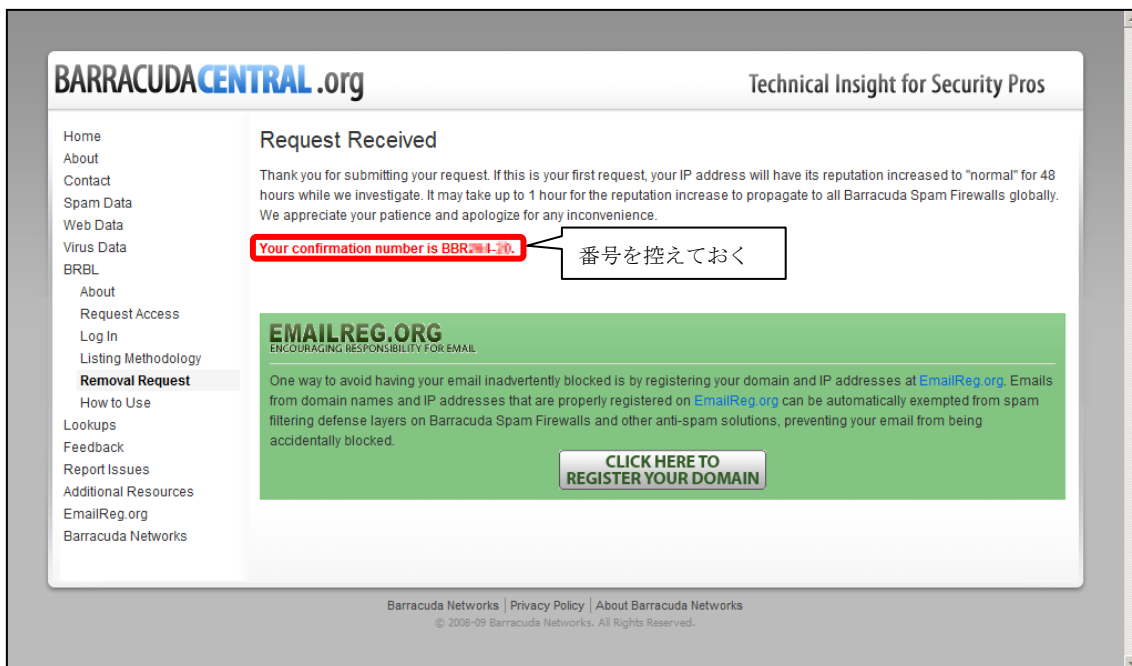
Verification Image:  お客様の電話番号を国番号から入力

Text in Image: fd8nw 画像に表示された文字列を入力

Reason for Removal:

 「Submit Request」をクリック

解除申請を受け付けると以下の画面が表示され、Confirmation Number が発行されますので、この番号を控えとして保存してください。



4.3 解除申請のタイミング

バラクーダ IP レピュテーションの登録解除申請を受け付けると、バラクーダセントラルではその IP アドレスの妥当性を調査・開始します。調査結果、その IP アドレスからスパムを大量送信していないことが確認できると、バラクーダ IP レピュテーションから登録解除されます。登録解除申請が受理されるまで、通常約 12 時間ほどお時間がかかります。

バラクーダ IP レピュテーションの登録解除申請を行っても、継続してスパムを送信している場合は、登録解除が行われない場合がございますので、ご了承をお願いします。また一時的に登録解除が行われても、再度スパムを送信するような事態が発生した場合は、再登録される可能性があります。何度もバラクーダ IP レピュテーションに登録されるような場合は、[バラクーダ IP レピュテーションに登録される主な理由](#)をご参考の上、セキュリティの高いメールサーバの運用をされることをお勧め致します。

4.3.1 バラクーダ製品をご利用されている場合

バラクーダ製品をご利用されているお客様から IP アドレスの登録解除申請があった場合、IP アドレスの妥当性が確認されると、登録解除申請から最大 24 時間以内にバラクーダ IP レピュテーションの配布リストに反映されます。



4.3.2 バラクーダ製品をご利用されていない場合

バラクーダ製品をご利用されているお客様から IP アドレスの登録解除申請があった場合、IP アドレスの妥当性が確認されると、登録解除申請から最大 48 時間以内にバラクーダ IP レピュテーションの配布リストに反映されます。



5 参考

以下のサイトでは、バラクーダ IP レピュテーション以外でも、お客様がご利用されている IP アドレスの一般的なリアルタイムブラックリスト (RBL) の IP アドレス登録状況を確認することができます。他のリアルタイムブラックリストに登録されていないかをご確認いただくことができます。

MXTOOLBOX

<http://www.mxtoolbox.com/blacklists.aspx>



バラクーダネットワークスジャパン株式会社

テクニカルサポート

<http://www.barracuda.co.jp>

お問い合わせ先：

〒141-0031

東京都品川区西五反田 8-3-16

西五反田 8 丁目ビル 5 階

E-mail: jpinfo@barracuda.com