石原 清輝
KDDI株式会社
向井 将
KDDI株式会社
馬渡 将隆
株式会社ドリーム・トレイン・インターネット

Date. 2006/04/18

xSP のルータにおいて設定を推奨するフィルタの項目について (IPv6版)

概要

本文書は、インターネットの安定性を保つ為に、xSP の内部および外部への接続部分において、xSP で運用をしている IPv6 ルータに設定をする事が推奨される IPv6 のパケットフィルタや経路フィルタについてまとめた文書です。

本文書で提示をしている "最低限、設定をする事が推奨されるフィルタ" については、xSP ネットワークの運用において基本的な部分となるので、文字通り、最低限設定をする必要があると考え、それに加えて併記してある "(運用者、ルータの) リソースにより設定を考慮するフィルタ" については、ネットワークの運用をしている NOC のメンバー、および、ネットワーク内で使用をしているルータのパフォーマンスにより設定の可否を検討する事が必要であると考えます。

本文書で提示している全てのフィルタの項目は、以下の項目を前提にして考えられてあり、全ての xSP のネットワークで適用される事を期待しています。

- o IPv6 ネットワークを対象とする
- o エンドユーザの正常な通信には影響を与えない
  (アドレス詐称やアタックなどへの対策方法の1つとしてフィルタを考える)
- o 不必要なパケットや経路は出さない/受け取らない
- o 下記に例としてあげてある特定アプリケーションの通信のパケットフィルタについては対象としない
  (例) Outbound Port25 Blocking (迷惑メール対策用途)、P2P トラフィックフィルタ など

目次

1. はじめに

IPv6 のネットワークが実運用サービスに入る状況になり、IPv6 のセキュリティに関しても、IPv4 と同様の配慮が必要です。

パケットフィルタ、経路フィルタでのセキュリティ対策については、基本的に、IPv4 と IPv6 とで考慮をすべき点に大きな差はそれほど無いと思いますが、IPv4 には無い特徴や機能が、IPv6 には新しく追加されている為、IPv4 ネットワークで設定を推奨されるフィルタと IPv6 ネットワークで設定を推奨されるフィルタの違いについては、きちんと把握をしておく必要があります。

現在のところ、IPv4 と比較をすると IPv6 の運用経験は歴史が浅い為、設定を推奨するフィルタの内容については、いくらかの修正を重ねていく必要があるのかもしれませんが、この文書は、現時点の状況で設定を推奨するフィルタの項目についてまとめたものとなっています。

2. 言葉の定義

この文書内で使用する言葉を、この文書内においては、以下のとおり定義します。

1. xSP とは、
   以下の条件を満たしているサービスプロバイダの総称
   - o インターネットへの接続性がある事
   - o グローバル AS 番号を所有している事
   - o 他 AS と BGP を利用した相互接続を行っている事

2. パケットフィルタ とは、
   IP パケットのヘッダの情報を元にしてフィルタリングを行う方法
   本文書内にあるパケットフィルタの項目では、特に Source アドレスと Destination アドレスの情報を元にしたフィルタを扱っています。

3. Prefix フィルタ とは、
   Prefix 長の情報を元にしてフィルタリングを行う方法
   別名 : Prefix Based フィルタ

4. AS-PATH フィルタ とは、
   AS-PATH 属性の情報を元にしてフィルタリングを行う方法

5. 経路フィルタ とは、
   "Prefix フィルタ" および "AS-PATH フィルタ" の双方を包括したフィルタの総称

6. トランジット とは、
   フルルートの広告を受ける接続の形態、および、フルルートの広告を受けている状態の事

7. ピア とは、
   xSP 同士において、お互いの内部および顧客の経路交換をする接続の形態、および、経路交換をしている状態の事

3. トランジット接続部分

3-1. 最低限、設定をする事が推奨されるフィルタ

3-1-1. パケットフィルタ

3-1-1-1. Ingress のパケットフィルタ

[1] Path MTU Discovery や Neighbor Discovery を機能させる為に、ICMPv6 の全パケットを accept する

[2] 以下の Special-Use Prefix が Source アドレスになっているパケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8
- サイトローカルアドレス : fec0::/10
- ユニークローカルアドレス : fec0::/7
- マルチキャストアドレス : ff00::/8
- ドキュメントアドレス : 2001:db8::/32

[3] 自 AS で持っている Prefix が Source アドレスになっているパケットを reject する

- 衛星インターネットサービスでの UDLR やその他の非対称ルーティングを利用しているネットワークへの影響が発生する場合があるので、注意が必要となる

3-1-1-2. Egress のパケットフィルタ

- 特に無し -

3-1-2. 経路フィルタ

3-1-2-1. Ingress の Prefix フィルタ

[1] 以下の Special-Use Prefix を reject する

- デフォルト : ::/0 exact
- ループバックアドレス (::1/128)、未指定アドレス (::/128)、

IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96)
を含んだ Prefix : ::/8 or longer
- リンクローカルアドレス : fe80::/10 or longer
- サイトローカルアドレス : fec0::/10 or longer
- ユニークローカルアドレス : fec0::/7 or longer
- マルチキャストアドレス : ff00::/8 or longer
- ドキュメントアドレス : 2001:db8::/32 or longer

[2] 自 AS で持っている Prefix を reject する

(例) 自 AS で持っている Prefix を 2001:db8::/32 と仮定した場合、2001:db8::/32 or longer を reject する

3-1-2-2. Egress の Prefix フィルタ

[1] 自 AS で持っている Prefix を aggregate して accept をする

- 自 AS 内部で使用している細かい Prefix をそのまま外部に広告をしないようにする

[2] 以下の Special-Use Prefix を reject する

- デフォルト : ::/0 exact
- ループバックアドレス (::1/128)、未指定アドレス (::/128)、
IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96)
を含んだ Prefix : ::/8 or longer
- リンクローカルアドレス : fe80::/10 or longer
- サイトローカルアドレス : fec0::/10 or longer
- ユニークローカルアドレス : fec0::/7 or longer
- マルチキャストアドレス : ff00::/8 or longer
- ドキュメントアドレス : 2001:db8::/32 or longer

3-1-2-3. Ingress の AS-PATH フィルタ

- 特に無し -

3-1-2-4. Egress の AS-PATH フィルタ

[1] プライベート AS 番号を外部に広告しないようにする

- 概要 : プライベート AS 番号を顧客に割り当てているなどの場合には、AS 外部にプライベート AS 番号が入った AS-PATH の経路を広告しないようにする必要がある為、AS-PATH からプライベート AS 番号を削除する
(例 : remove-private-as などを利用する)

- 効果 : プライベート AS 番号が入った AS-PATH の経路を広告する事によって発生するトラブルを事前に防ぐ

3-2. (運用者、ルータの) リソースにより設定を考慮するフィルタ

3-2-1. パケットフィルタ

3-2-1-1. Ingress のパケットフィルタ

[1] トランジット接続で使用をしているインターフェース宛となっている ICMPv6 パケットの制限をする

(例) ICMPv6 TYPE を制限して accept をする

- 前提条件 : Path MTU Discovery や Neighbor Discovery は機能が出来るようにしておく

- 長所 : ICMPv6 パケットを利用したアタックに関して、ある程度の防御をする事が可能となる

- 短所 : ICMPv6 パケットの制限をしたルータを経由する traceroute などをした場合、パケットの到達性が確認しにくくなる恐れがある

3-2-1-2. Egress のパケットフィルタ

[1] 以下の Special-Use Prefix が Source アドレスになっているパケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、
  IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96)
  を含んだ Prefix　　:　::/8
- サイトローカルアドレス　:　fec0::/10
- ユニークローカルアドレス　:　fec0::/7
- マルチキャストアドレス　:　ff00::/8
- ドキュメントアドレス　　:　2001:db8::/32

3-2-2. 経路フィルタ

3-2-2-1. Ingress の Prefix フィルタ

[1] 細かい Prefix (Long Prefix) を reject する

- 到達性がなくなってしまう xSP が出てこない範囲の中で細かい
  Prefix を reject する

(例) /33 or longer を reject する
     /49 or longer を reject する

[2] 未割り当ての Prefix を reject する

- Bogon List を参照して未割り当ての Prefix を reject する

3-2-2-2. Egress の Prefix フィルタ

- 特に無し -

3-2-2-3. Ingress の AS-PATH フィルタ

[1] 一定値以上の長い AS-PATH 長の経路を reject する

- AS-PATH 長が 50 Hop 以上になっている経路を reject する
  (接続性がなくなってしまう xSP が出てこない範囲内)

3-2-2-4. Egress の AS-PATH フィルタ

- 特に無し -

3-3. フィルタの運用を軽減する為に有効な技術

[1] Max-Prefix-Limits

- 概要 : 1つの BGP ピアから受信する Prefix 数の最大値を制限する
  設定で、この設定で定義した閾値以上の Prefix は受信をし
  ないようにする

- 効果 : BGP ピアの相手側のトラブルなどによって、相手側から大量
  の経路広告が発生した場合、その経路の受信によって生じる
  自 AS のルータの過負荷を防止する事が出来る

4. ピア(パブリック/プライベート)接続部分

4-1. 最低限、設定をする事が推奨されるフィルタ

4-1-1. パケットフィルタ

4-1-1-1. Ingress のパケットフィルタ

[1] Path MTU Discovery や Neighbor Discovery を機能させる為に、
    ICMPv6 の全パケットを accept する

[2] 以下の Special-Use Prefix が Source アドレスになっているパ
    ケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、
  IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96)
  を含んだ Prefix　　:　::/8
- サイトローカルアドレス　:　fec0::/10
- ユニークローカルアドレス　:　fec0::/7
- マルチキャストアドレス　:　ff00::/8
- ドキュメントアドレス　　:　2001:db8::/32

[3] 自 AS で持っている Prefix が Source アドレスになっているパケットを reject する

- 衛星インターネットサービスでの UDLR やその他の非対称ルーティングを利用しているネットワークへの影響が発生する場合があるので、注意が必要となる

4-1-1-2. Egress のパケットフィルタ

- 特に無し -

4-1-2. 経路フィルタ

4-1-2-1. Ingress の Prefix フィルタ

[1] 以下の Special-Use Prefix を reject する

- デフォルト : ::/0 exact
- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8 or longer
- リンクローカルアドレス : fe80::/10 or longer
- サイトローカルアドレス : fec0::/10 or longer
- ユニークローカルアドレス : fc00::/7 or longer
- マルチキャストアドレス : ff00::/8 or longer
- ドキュメントアドレス : 2001:db8::/32 or longer

[2] 自 AS で持っている Prefix を reject する

(例) 自 AS で持っている Prefix を 2001:db8::/32 と仮定した場合、2001:db8::/32 or longer を reject する

4-1-2-2. Egress の Prefix フィルタ

[1] 自 AS で持っている Prefix を aggregate して accept をする

- 自 AS 内部で使用している細かい Prefix をそのまま外部に広告をしないようにする

[2] 以下の Special-Use Prefix を reject する

- デフォルト : ::/0 exact
- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8 or longer
- リンクローカルアドレス : fe80::/10 or longer
- サイトローカルアドレス : fec0::/10 or longer
- ユニークローカルアドレス : fc00::/7 or longer
- マルチキャストアドレス : ff00::/8 or longer
- ドキュメントアドレス : 2001:db8::/32 or longer

4-1-2-3. Ingress の AS-PATH フィルタ

- 特に無し -

4-1-2-4. Egress の AS-PATH フィルタ

[1] プライベート AS 番号を外部に広告しないようにする

- 概要 : プライベート AS 番号を顧客に割り当てているなどの場合には、AS 外部にプライベート AS 番号が入った AS-PATH の経路を広告しないようにする必要がある為、AS-PATH からプライベート AS 番号を削除する (例 : remove-private-as などを利用する)

- 効果 : プライベート AS 番号が入った AS-PATH の経路を広告する事によって発生するトラブルを事前に防ぐ

4-2. (運用者、ルータの) リソースにより設定を考慮するフィルタ

4-2-1. パケットフィルタ

4-2-1-1. Ingress のパケットフィルタ

[1] IX 接続やプライベートピア接続で使用をしているインターフェース宛となっている ICMPv6 パケットの制限をする

(例) ICMPv6 TYPE を制限して accept をする

- 前提条件 : Path MTU Discovery や Neighbor Discovery は機能が出来るようにしておく

- 長所 : ICMPv6 パケットを利用したアタックに関して、ある程度の防御をする事が可能となる

- 短所 : ICMPv6 パケットの制限をしたルータを経由する traceroute などをした場合、パケットの到達性が確認しにくくなる恐れがある

4-2-1-2. Egress のパケットフィルタ

[1] 以下の Special-Use Prefix が Source アドレスになっているパケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8
- サイトローカルアドレス : fec0::/10
- ユニークローカルアドレス : fec0::/7
- マルチキャストアドレス : ff00::/8
- ドキュメントアドレス : 2001:db8::/32

4-2-2. 経路フィルタ

4-2-2-1. Ingress の Prefix フィルタ

[1] 細かい Prefix (Long Prefix) を reject する

- 到達性がなくなってしまう xSP が出てこない範囲の中で細かい Prefix を reject する

(例) /33 or longer を reject する
/49 or longer を reject する

[2] ピアの相手から広告をすると通知があった Prefix のみを accept する

- ピアの相手からの経路更新通知を元にしてフィルタを設定する

[3] 未割り当ての Prefix を reject する

- Bogon List を参照して未割り当ての Prefix を reject する

4-2-2-2. Egress の Prefix フィルタ

- 特に無し -

4-2-2-3. Ingress の AS-PATH フィルタ

[1] 一定値以上の長い AS-PATH 長の経路を reject する

- AS-PATH 長が 50 Hop 以上になっている経路を reject する (接続性がなくなってしまう xSP が出てこない範囲内)

[2] ピアの相手から広告をすると通知があった AS-PATH の経路のみを accept する

- ピアの相手からの経路更新通知を元にしてフィルタを設定する

4-2-2-4. Egress の AS-PATH フィルタ

- 特に無し -

4-3. フィルタの運用を軽減する為に有効な技術

[1] Max-Prefix-Limits

- 概要 : 1つの BGP ピアから受信する Prefix 数の最大値を制限する

設定で、この設定で定義した閾値以上の Prefix は受信をしないようにする

- 効果 : BGP ピアの相手側のトラブルなどによって、相手側から大量の経路広告が発生した場合、その経路の受信によって生じる自 AS のルータの過負荷を防止する事が出来る

5. 顧客接続部分

5-1. 最低限、設定をする事が推奨されるフィルタ

5-1-1. パケットフィルタ

5-1-1-1. Ingress のパケットフィルタ

[1] Path MTU Discovery や Neighbor Discovery を機能させる為に、ICMPv6 の全パケットを accept する

[2] 以下の Special-Use Prefix が Source アドレスになっているパケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8
- サイトローカルアドレス : fec0::/10
- ユニークローカルアドレス : fec0::/7
- マルチキャストアドレス : ff00::/8
- ドキュメントアドレス : 2001:db8::/32

[3] (トランジット顧客の場合) 自 AS で持っている Prefix が Source アドレスになっているパケットを reject する

5-1-1-2. Egress のパケットフィルタ

- 特に無し -

5-1-2. 経路フィルタ
(※ BGP 接続顧客を対象にした経路フィルタ)

5-1-2-1. Ingress の Prefix フィルタ

[1] (プライベート AS を利用した BGP 接続の場合) 顧客に割り当てている Prefix のみを accept する

(例) 顧客に割り当てている Prefix を 2001:db8::/32 と仮定した場合、2001:db8::/32 exact のみを accept する

[2] (トランジット顧客の場合) 顧客側 AS から広告をすると通知があった Prefix のみを accept する

(例) 顧客側 AS から 2001:db8::/32 の Prefix を広告すると言う通知があったと仮定した場合、2001:db8::/32 exact を accept する

5-1-2-2. Egress の Prefix フィルタ

[1] 自 AS で持っている Prefix を aggregate して accept をする

- 自 AS 内部で使用している細かい Prefix をそのまま外部に広告をしないようにする

[2] 以下の Special-Use Prefix を reject する

- デフォルト : ::/0 exact
- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8 or longer
- リンクローカルアドレス : fe80::/10 or longer
- サイトローカルアドレス : fec0::/10 or longer
- ユニークローカルアドレス : fec0::/7 or longer
- マルチキャストアドレス : ff00::/8 or longer
- ドキュメントアドレス : 2001:db8::/32 or longer

5-1-2-3. Ingress の AS-PATH フィルタ

- 特に無し -

5-1-2-4. Egress の AS-PATH フィルタ

[1] プライベート AS 番号を外部に広告しないようにする

- 概要 : プライベート AS 番号を顧客に割り当てているなどの場合には、AS 外部にプライベート AS 番号が入った AS-PATH の経路を広告しないようにする必要がある為、AS-PATH からプライベート AS 番号を削除する
(例 : remove-private-as などを利用する)

- 効果 : プライベート AS 番号が入った AS-PATH の経路を広告する事によって発生するトラブルを事前に防ぐ

5-2. (運用者、ルータの) リソースにより設定を考慮するフィルタ

5-2-1. パケットフィルタ

5-2-1-1. Ingress のパケットフィルタ

[1] IX 接続やプライベートピア接続で使用をしているインターフェース宛となっている ICMPv6 パケットの制限をする

(例) ICMPv6 TYPE を制限して accept をする

- 前提条件 : Path MTU Discovery や Neighbor Discovery は機能が出来るようにしておく

- 長所 : ICMPv6 パケットを利用したアタックに関して、ある程度の防御をする事が可能となる

- 短所 : ICMPv6 パケットの制限をしたルータを経由する traceroute などをした場合、パケットの到達性が確認しにくくなる恐れがある

[2] 顧客側で持っているアドレスブロックが Source アドレスとなっているパケットのみを accept する

- 顧客のネットワーク形態を考慮した上で、設定をする必要がある
(このフィルタを設定する事により、非対称ルーティングなどを利用している顧客の通信に影響が発生する場合があるので、注意が必要となる
例 : 衛星インターネットサービスを利用している顧客など)

[3] 自 AS と接続をしている IX セグメントのアドレスが Destination アドレスとなっている BGP (179/TCP) パケットを reject する
(もしくは、IX 接続ルータのコア側インターフェースにおける Ingress フィルタにて reject をすると言う方法もある)

- 効果 : BGP の脆弱性対策として有効となる

5-2-1-2. Egress のパケットフィルタ

[1] 以下の Special-Use Prefix が Source アドレスになっているパケットを reject する

- ループバックアドレス (::1/128)、未指定アドレス (::/128)、IPv4 互換アドレス (::ffff:/96)、IPv4 射影アドレス (::/96) を含んだ Prefix : ::/8
- サイトローカルアドレス : fec0::/10
- ユニークローカルアドレス : fec0::/7
- マルチキャストアドレス : ff00::/8
- ドキュメントアドレス : 2001:db8::/32

5-2-2. 経路フィルタ
(※ BGP 接続顧客を対象にした経路フィルタ)

5-2-2-1. Ingress の Prefix フィルタ

- 特に無し -

5-2-2-2. Egress の Prefix フィルタ

- 特に無し -

5-2-2-3. Ingress の AS-PATH フィルタ

[1] ピアの相手から広告をすると通知があった AS-PATH の経路のみを accept する

- ピアの相手からの経路更新通知を元にしてフィルタを設定する

5-2-2-4. Egress の AS-PATH フィルタ

- 特に無し -

5-3. フィルタの運用を軽減する為に有効な技術

[1] Max-Prefix-Limits

- 概要 : 1つの BGP ピアから受信する Prefix 数の最大値を制限する設定で、この設定で定義した閾値以上の Prefix は受信をしないようにする

- 効果 : BGP ピアの相手側のトラブルなどによって、相手側から大量の経路広告が発生した場合、その経路の受信によって生じる自 AS のルータの過負荷を防止する事が出来る

6. ルータ自身へのアクセス

6-1. 最低限、設定をする事が推奨されるフィルタ

6-1-1. パケットフィルタ

6-1-1-1. Ingress のパケットフィルタ

[1] ルータで動かしている以下のサービスについて、アクセスが可能な Source アドレスを限定して、限定した Source アドレスからのパケットのみを accept する

- telnet
- ssh
- snmp (ReadOnly / ReadWrite)
- ftp
- tftp
- ntp

※ 利用をしていない不必要なサービスについては、サービスの停止をすべきである

(例) NOC のネットワークからのみアクセスを可能にするか、もしくは、アクセスが可能なホストを最小限に限定する

[2] eBGP および iBGP の Neighbor アドレスが Source アドレスとなっている BGP (179/TCP) パケットのみを accept する

[3] 各リンクが接続されているインターフェースにおいて、Source アドレスが Neighbor のリンクローカルアドレスとなっているパケットを accept する

- Neighbor Discovery などを機能させる為に、accept をする必要がある

6-1-1-2. Egress のパケットフィルタ

- 特に無し -

6-2. (運用者、ルータの) リソースにより設定を考慮するフィルタ

6-2-1. パケットフィルタ

6-2-1-1. Ingress のパケットフィルタ

[1] ルータのインターフェース宛となっている ICMPv6 パケットの制

限をする

(例) ICMPv6 TYPE を制限して accept をする

- 前提条件 : Path MTU Discovery や Neighbor Discovery は機能が出来るようにしておく

- 長所 : ICMPv6 パケットを利用したアタックに関して、ある程度の防御をする事が可能となる

- 短所 : ICMPv6 パケットの制限をしたルータを経由する traceroute などをした場合、パケットの到達性が確認しにくくなる恐れがある

6-2-1-2. Egress のパケットフィルタ

- 特に無し -

6-3. フィルタの運用を軽減する為に有効な技術

[1] System Protection ACL (IP Receive ACL, Loopback0 ACL)

- 概要 : ルータのリソース (ルーティングプロセッサなど) を保護する為のフィルタ技術

- 効果 : ルータ自身に対する攻撃パケットの対策の為に有効となる

7. 謝辞

この文書の作成にあたっては、Interdomain Routing Security Workshop の参加者の皆様、および JANOG メーリングリストのメンバーの皆様からのご協力とサポートが不可欠なものでした。皆様に感謝を致します。

8. 参考文献

8-1. この文書の作成にあたり、参考にさせていただいた文献

8-1-1. IPv6 BGP filter recommendations
http://www.space.net/~gert/RIPE/ipv6-filters.html

8-2. その他に有益な文献

8-2-1. IPv6 Routing Policies Guidelines
http://www.ietf.org/internet-drafts/draft-blanchet-v6ops-routing-guidelines-01.txt

8-2-2. 各 RIR が公開している IP アドレス割り振りリスト

- APNIC
  http://ftp.apnic.net/stats/apnic/delegated-apnic-latest

- RIPE/NCC
  ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest

- ARIN
  ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest

- LACNIC
  ftp://lacnic.net/pub/stats/lacnic/delegated-lacnic-latest

- AfriNIC
  ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest

9. 著者

氏名 : 石原 清輝 [ISHIHARA Kiyoteru]
所属 : KDDI株式会社
EMail : ki-ishihara@kddi.com

氏名 : 向井 将 [MUKAI Masaru]

所属　: KDDI株式会社
EMail : ms-mukai@kddi.com

氏名　: 馬渡 将隆 [MAWATARI Masataka]
所属　: 株式会社ドリーム・トレイン・インターネット
EMail : mawatari@dti.ad.jp

10. 免責事項

本文書によって発生した損失や損害について、著者は一切責任を負いません。

11. この文書の配布に関して

以上