WG3-7

『インターネットにおける障害連鎖の防止方法について』

2004年3月10日

株式会社パワードコム

Agenda

1. 通信障害の定義
2. 連鎖する通信障害の種別と原因
3. 連鎖する通信障害の予防方法
4. 連鎖する可能性のある通信障害が発生した場合の対処方法
5. 事業者間での障害情報等の共有について
6. 課題
7. まとめ

1． 通信障害の定義

- 通信障害とは、通信事業者の通信装置の故障やネットワーク運用時のオペレーションミスなどにより通信に支障が生じることを指す。障害の種類としては、通信ができなくなるケースや回線容量に対して過度のトラヒックが集中することにより発生する輻輳等が考えられる。通信障害は、その種別により、連鎖するものとそうでないものに区別することができる。
  - 連鎖する障害
    - 複数の通信事業者に障害の影響が波及して被害が拡大するもの。これには、経路障害など事業者網に原因があるものと、DoS(Denial of Service)攻撃やウィルスなどエンド端末に原因があるものがある。
      - 例）不適切な経路情報の伝播 － 事業者網に原因
        DoS攻撃による回線輻輳 － エンド端末（他の事業者のお客様を含む）に原因
  - 連鎖しない障害
    - 障害の影響範囲が通信事業者に閉じており、他通信事業者に影響が波及しないもの
      - 例）事業者の内部ネットワークにおける機器故障

今回の検討では、連鎖する障害に対象を限定

2． 連鎖する通信障害の種別と原因

- 経路障害
  - 各事業者が取得しているIPアドレス空間以外の不適切な経路情報が伝播し、通信できなくなるケース
  - BGPピアがフラップして、経路交換が不安定になるケース
  - 主な原因
    - 通信装置の故障やバグ
    - オペレーションミス
    - 不正アクセス、不正制御
- パケット転送障害
  - 異常なトラヒックが発生することにより、回線が輻輳するケース
  - 主な原因
    - エンド端末がウィルス等に感染し、不正なトラヒックを送出
    - DoS攻撃等
- アプリケーション障害
  - DNS（上位レベル）の障害による、名前解決が不可になるケース（現実的には希少ケース）
  - 主な原因
    - オペレーションミスや不正アクセス、不正制御

3． 連鎖する通信障害の予防方法

- 連鎖する通信障害のうち、予防の対策が可能なものとしては、経路障害がある。各事業者により適用手法は異なるものの、概ね以下の手法を利用している。
  - 他事業者とのBGPピアにおける設定
    - AS-path filtering
      - AS-path情報を交換し、BGPピアにおいてこのAS-path情報にあった経路のみを受け取る
    - Prefix filtering
      - Prefix情報を交換し、BGPピアにおいてこのAS-path情報にあった経路のみを受け取る
    - Maximum prefix filtering
      - 受信するPrefix数の上限を設定し、それを超える経路を受け取った場合に、アラーム発出またはPeer downを行う。
    - インターネット上へ流すべきでない経路のフィルタアウト
      - デフォルトルート、プライベートアドレス、マルチキャストアドレス、ループバックアドレス等
- 上記の設定は、直接接続を持つ事業者間同士で行われ、主にお客様向けのBGPピア及びPeering接続へ適用される。また、上記設定にIRR（Internet Routing Registry）を利用する手法もある。IRRへの登録により、その経路の信頼性を明確化することができる。

4． 連鎖する可能性のある通信障害が発生した場合の対処方法

- 経路障害など事業者網にて対応が可能なもの
  - 不適切な経路情報が受信された場合
    - BGPピアの設定にて当該Prefixをフィルタアウト
  - BGPピアがフラップ等により不安定になった場合
    - 該当BGPピアを一時的にダウンさせる
- 上記対応を可能とするためには、他事業者への通信経路を複数確保しておくことが必要である。

- DoS攻撃
  - 攻撃先が事業者網の配下にある場合、一時的に攻撃先特定アドレス向けのパケットを廃棄する。
  - 攻撃元が特定でき、事業者網の配下にある場合には、該当する端末の管理者へ対応を依頼する。または、一時的に特定アドレスからのパケットを事業者網にて廃棄する。

- ウィルス等エンド端末が原因となるもの
  - ネットワーク側にて対応できない場合、該当する端末の管理者へ対応を依頼する。

5． 事業者間での障害情報等の共有について

- これまで見てきたように、連鎖する可能性のある障害に対する対応方法としては、各事業者が接続している他の事業者との2者間での対応が中心となっている。

- 事業者間にて障害等の情報を共有する（できる）主な手法としては、以下の手法が挙げられる。
  - 接続している通信事業者間（Transit接続、Peering接続等）
  - オペレータのコミュニティー
    - 任意団体　（例：NANOGやJANOG等のxNOG）
  - 各Internet Exchange（IX）で運用しているMailing List

- エンド端末や機器の脆弱性については、以下の団体等にて情報提供が行われている。
  - JPCERT/CC等のCERT（Computer Emergency Response Team）
  - 社団法人日本インターネットプロバイダ協会（JAIPA）
  - Telecom-ISAC Japan他

- 現状では上記手法や情報提供を組み合わせ、障害情報の共有が行われているのが実態となっている。これらの情報から、障害対応を機動的に行うことが可能となっている。

6． 課題

- 経路障害予防
  - オペレーションミス（設定ミス）による経路障害を防ぐ手法の確立
    - Prefix Filteringの導入が望ましいが運用面で負担がある。
    - IRRを利用する方法もあるが全事業者が登録していないため適用範囲が限定される。
      （参考） JPNICにてIRR企画策定専門家チームを設立し、この問題に対して取り組んでいる。

- DDoS攻撃への有効な対策の確立
  - DoS攻撃の検出方法の確立が必要
  - ソースアドレスを偽る攻撃に対する対処策がない。
    - RPF(Reverse Path Filtering)の導入が提唱されているが全事業者で導入していないと効果が薄いため、採用が進んでいない。また、非対称ルーティングを導入している場合には、RPFを適用できない等、課題もある。

7． まとめ

- 障害連鎖を防止する方策としては、各事業者で他社からの障害波及を自衛する方法が有効であり、これによりインターネットの安定した運用が可能となっている。

- また、インターネットは各事業者等のネットワークが相互接続されて成り立っているため、各事業者網を安定的に運用するよう努めることが重要である。

- 一方、DoS攻撃やウィルス感染などによる不正トラヒックに対しては、エンド端末のセキュリティを向上させていくことが重要となる。これと併せ、管理者や利用者のセキュリティ意識の向上促進や、事業者によるユーザセキュリティのサポートが必要となる。