キャンパスネットワークにおける上流ネットワークの冗長化

葭葉 純子 [1)], 中村 直毅 [1)], 長田 典久 [1)], 秋山 英明 [2)],
小松 雄一 [2)], 大泉 洋貴 [2)], 阿部 陽介 [2)], 中山 雅晴 [1)]

1) 東北大学医学系研究科 情報基盤室
2) 東日本電信電話株式会社

yoshiba@med.tohoku.ac.jp

Upstream Redundancy in Campus Networks Using Server Functions

Junko Yoshiba [1)], Naoki Nakamura [1)], Norihisa Osada [1)], Hideaki Akiyama [2)],
Yuichi Komatsu [2)], Hiroki Oizumi [2)], Yosuke Abe [2)], Masaharu Nakayama [1)]

1) Tohoku University Graduate School of Medicine Information Inf
2) NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION

概要

COVID-19 の蔓延に伴ってオンライン授業や Web 会議が頻繁に使われるようになり、教育・研究環境で安定したインターネット通信環境を提供することがますます重要なものとなっている。そこで、東北大学医学系研究科は、キャンパスネットワークの上位で障害が発生した際にも、オンライン授業や Web 会議に支障を与えないように、上位ネットワークの冗長化を行った。現状のキャンパスネットワークでは、上位の学内ネットワーク、SINET を経由してインターネットに接続しているが、上位の学内ネットワークや SINET で障害が発生した場合にはインターネット通信を継続できないため、バックアップ回線として学内ネットワークや SINET とは独立している商用プロバイダ回線を用意し、ネットワークを冗長化することにした。冗長化には一般的にルーティングプロトコル BGP[1] [2]などを用いた仕組みが必要であるが、技術的、運用的な敷居が非常に高い。そこで、ネットワーク機器やサーバを効果的に組み合わせて簡単な仕組みで実現することにした。この仕組みによって障害時には、バックアップ回線を利用してインターネット向けの通信を維持し、学外からキャンパスネットワークの DMZ で稼働しているメールやウェブサービスの通信も維持できるようになった。本稿ではネットワークの冗長化の概要および評価について報告する。

1 はじめに

昨年度以降、COVID-19 対応のためにオンライン授業や Web 会議が一斉に行われるようになり、安定したインターネット環境がますます重要なものとなっている。医学系研究科のキャンパスネットワークは、大学本部で管轄しているネットワーク機器を経由して、SINET に接続している。そのため、大学本部管轄のネットワーク機器、回線、SINET 等に障害が発生するとインターネット向けの通信が不通になってしまう懸念がある。実際、昨年度にはキャンパス間の通信で利用する光ファイバーケーブルが小動物に切断され長時間通信が停止したことで、授業や会議を突然中断せざる得ない状況が発生した。そこで、上位のネットワークで障害が発生した際にもインターネット通信が継続できるようにするため、SINET と独立している商用プロバイダ回線を用いてネットワークを冗長化することにした。障害時には、このバックアップ回線を利用してインターネット向けの通信を維持できるようにするとともに、キャンパスネットワークの DMZ で稼働しているメールやウェブサービスの通信も合わせて維持できるようにした。本稿では、これらのネットワークの冗長化の概要および評価について報告する。

2 上位ネットワークの障害を考慮したネットワークの冗長化

2.1 ネットワークの冗長化の概要

学内の端末は、平常時は帯域が広く高速な上位

の学内ネットワーク（以降、上位学内回線と記載する）をメイン回線として利用しインターネット向けの通信を行う。上位学内回線では、SINET が使われており、SINET に依存しない商用プロバイダをバックアップ回線として準備することで、学内ネットワークに障害が発生した際にもインターネット通信が維持できるようにする。以下にネットワークの冗長化の概要について説明する。

2.2 キャンパス内の端末からインターネット向け通信

通常、キャンパス内の端末は、Link0 を経由して上位学内回線から Web 会議やオンライン授業、ウェブ閲覧、GSuite 等のサービスを利用している（図 1）。上位学内回線で障害が発生した際には、Link1 を経由してバックアップ回線から通信するように制御する。内部からインターネット向けの通信は、NAPT（Network Address Port Translation）によって通信が維持される。

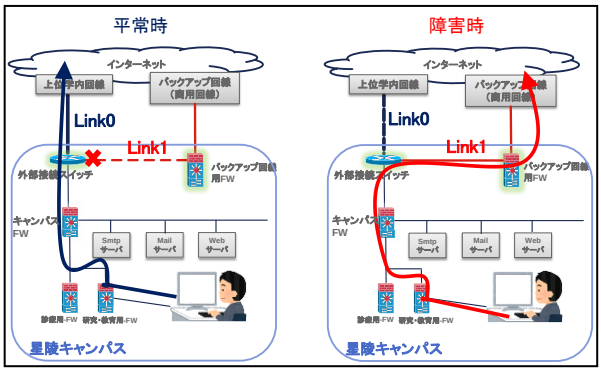

図 1. キャンパス内の端末から外部へのインターネットアクセス

上位学内回線とバックアップ回線を簡単に切り替えるため、外部接続スイッチで、上位学内回線およびバックアップ回線向けのデフォルトルートを 2 つ設定する。バックアップ回線向けのデフォルトルートの優先度を上位学内回線向けよりも高く設定し、平常時には、バックアップ回線向けの Link1 を無効化し、Link0 を経由して帯域の広い上位学内回線を経由して通信する。上位学内回線において障害が発生した際には、Link1 を手動で有効化し、Link1 を経由してバックアップ回線から通信が行われるように制御する（図 2）

なお、インターネット上の特定のサーバを ping 監視し、応答がない場合にデフォルトルートを自動切り替えることも技術的には可能であるが、意図しない回線切り替えが頻繁に発生することが懸念されるため、手動で切り替えることにした。

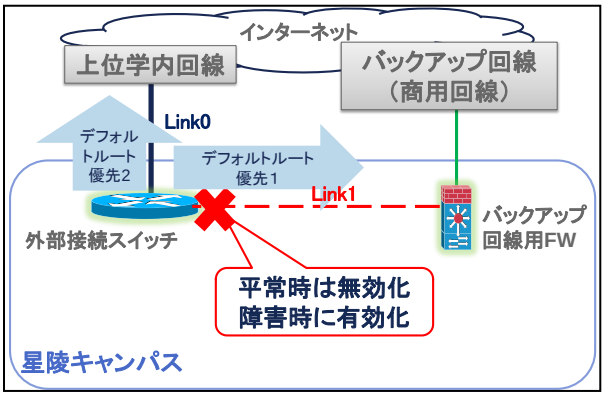

図 2. 障害発生時の回線切り替え

2.3 メール・ウェブメールサービス公開のための学外からキャンパス向けの通信

メール・ウェブサービスを提供するため、キャンパス内の DMZ にメールおよびウェブサーバを配置している。これらのサーバ宛の通信は、平常時には上位学内回線から Link0 を経由して通信し、障害時にはバックアップ回線から Link2 を経由して通信されるようにする（図 3）。ここで、Link1 ではなく、Link2 を用いるのは、メール・ウェブサービスを平常時もバックアップ回線を利用できるように設定しておくためである。バックアップ回線向けの Link1 は平常時には無効化され、この経路を使って通信できないため、外部接続スイッチとバックアップ回線用 Firewall（以降、バックアップ回線用 FW と記載する）間に Link2 を追加し、平常時においてバックアップ回線経由でのメール・ウェブサービスが通信できるようにする。

バックアップ回線では、固定のグローバル IP アドレスを 1 つ取得し、外部からこの IP アドレス宛に通信が届くと Port Forwarding により、DMZ に設置されている指定されたサーバに通信を転送し、メールやウェブサービスを提供する。

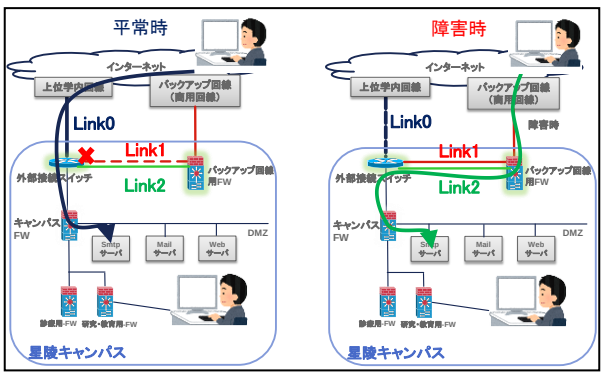

図 3. 学外からのメール・ウェブサービス利用

3 実装

2 章で述べた仕組みを実環境に適用した。なお、外部接続スイッチは、Cisco 社製 Catalyst 3850、バックアップ回線用 FW は、Fortinet 社製 FortiGate 200E、キャンパスネットワークの Firewall（以降、キャンパス FW と記載する）は、Cisco 社製 Firepower 4110 を利用しており、各サーバの OS は、CentOS 7 もしくは CentOS8 を利用している。

3.1 接続構成およびルーティング制御

既存の外部スイッチおよびバックアップ回線用 FW に対してそれぞれ、Link1 の障害時用インタフェースおよび Link2 の常時接続用インタフェースを新規作成し、図 4 に示すように接続し、外部接続スイッチ側の障害時用インタフェースを shutdown とした。

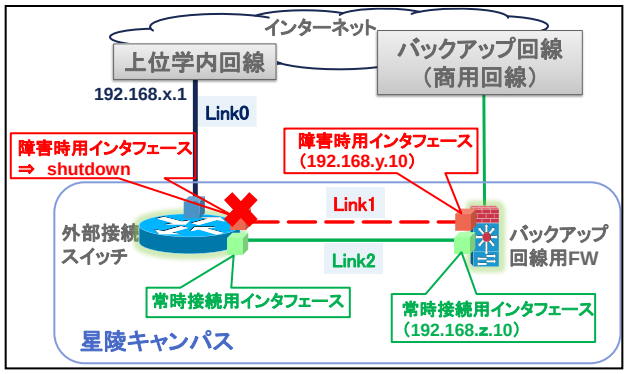

図 4. バックアップ回線用 FW への接続

外部接続スイッチでは、図 5 の赤枠内に示すように、バックアップ回線向けのデフォルトルートの優先順位が上位学内回線向けのデフォルトルートの優先順位よりも高くなるようにするため、上位学内回線向けは 40 を指定し、バックアップ回線向けを未指定(0)とした。

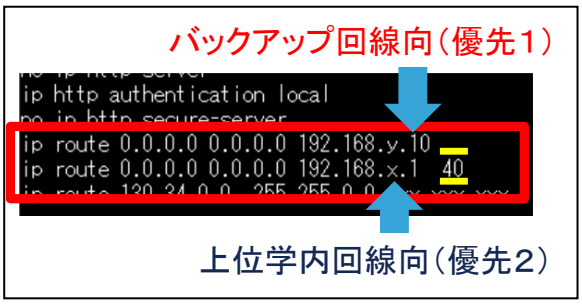

図 5. 外部接続スイッチのデフォルトルート設定

3.2 メール・ウェブサーバのマルチホーミング設定

インターネットからバックアップ回線を経由してメールおよびウェブサーバに接続できるようにするため、メール・ウェブサービスを提供するサーバに対して、既存の IP アドレスと同じネットワークアドレスの IP アドレスを新規で割り当てた（図 6 の①、②、③）。外部接続スイッチでは、新規で割り当てた IP アドレスから発信される通信がバックアップ回線用 FW の常時接続用インタフェース(192.168.z.10)宛にルーティングするようにソースルーティングの設定をした（図 7）。また、インターネットからバックアップ回線用 FW の WAN に設定されているグローバル IP アドレス（160.x.y.100）に着信する通信が、キャンパス FW の DMZ 上に配置されているサーバに転送されるようにするため、バックアップ回線用 FW において表 1 示す Port Forwarding の設定を行った。

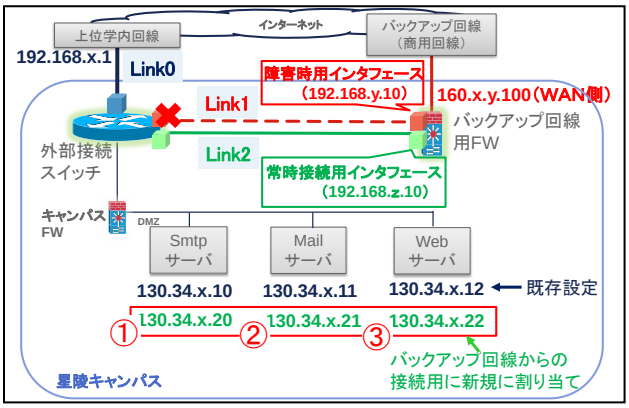

図 6. サーバの IP アドレス冗長化設定

```
ip access-list extended Backup-FW_inside2
 permit ip host 130.34.x.20 any
 permit ip host 130.34.x.21 any
 permit ip host 130.34.x.22 any
!
access-list aa permit 130.34.x.0 0.0.0.255
!
route-map Backup-FW_inside2 permit 10
 match ip address Backup-FW_inside2
 set ip next-hop 192.168.z.10
!
```

図 7. 外部接続スイッチにおけるソースルーティング設定

表 1. バックアップ回線用 FW の Port Forwarding 設定

Port Forwarding設定	
160.x.y.100(TCP/25) → 130.34.x.20(TCP/25)	①Smtpサーバ
160.x.y.100(TCP/587) → 130.34.x.20(TCP/587)	①Smtpサーバ
160.x.y.100(TCP/465) → 130.34.x.20(TCP/465)	①Smtpサーバ
160.x.y.100(TCP/110) → 130.34.x.21(TCP/110)	②Mailサーバ
160.x.y.100(TCP/143) → 130.34.x.21(TCP/143)	②Mailサーバ
160.x.y.100(TCP/993) → 130.34.x.21(TCP/993)	②Mailサーバ
160.x.y.100(TCP/995) → 130.34.x.21(TCP/995)	②Mailサーバ
160.x.y.100(TCP/80) → 130.34.x.22(TCP/80)	③Webサーバ
160.x.y.100(TCP/443) → 130.34.x.22(TCP/443)	③Webサーバ
160.x.y.100(TCP/53) → 130.34.x.2(TCP/53)	DNSサーバ
160.x.y.100(UDP/53) → 130.34.x.2(UDP/53)	DNSサーバ

以上によって、バックアップ回線側からのメール・ウェブサービスへの通信が、DMZ に設置されているメール・ウェブサーバへ転送され、サーバからの戻りの通信もバックアップ回線を経由して送信元のクライアントに応答する構成とした（図 8）。

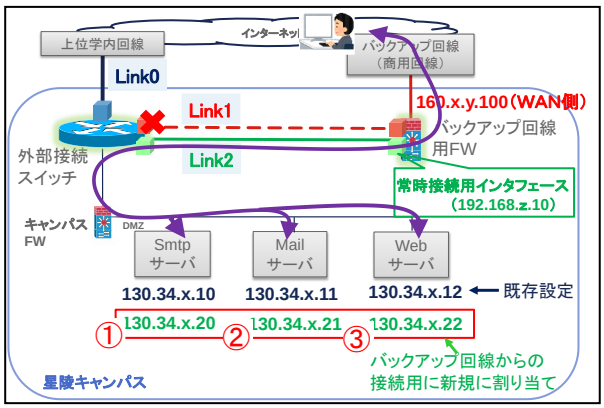

図 8. バックアップ回線経由のメール・ウェブの通信

なお、クライアントがアクセスするサーバの指定は、以降で記載する DNS を用いて制御する。

3.3 DNS 設定

利用者はメールやウェブサービスを利用するため、ホスト名を指定して接続する。ホスト名が上位学内回線用の IP アドレスで名前解決される場合は、上位学内回線経由の通信となり、バックアップ回線用 FW の WAN のグローバル IP アドレス（160.x.y.100）で名前解決される場合は、バックアップ回線経由の通信となる。平常時と障害時に DNS の登録情報を修正することなくサービスを継続するため、平常時用のゾーン情報を保持する DNS1 と障害時用のゾーン情報を保持する DNS2 の 2 つ用意し、平常時には DNS1 のゾーン情報のみ参照でき、障害時には DNS2 のゾーン情報のみ参照できるように設定した。

平常時と障害時の DNS 設定を図 9 に示す。障害時用 DNS（DNS2）設定では、メール・ウェブサーバのホスト名は、バックップ回線のグローバル IP アドレス（160.x.y.100）を設定する（図 9 赤枠）。平常時用（DNS1）と障害時用（DNS2）ともに、NS レコードは DNS1 および DNS2 の両方を指定する（図 9 黄枠）。また、平常時に DNS2 のゾーン情報を参照できなくするため、バックアップ回線側から DNS2 へは Link1 を経由して通信するようにバックアップ回線用 FW でポリシー（図 10）とルーティング設定を行う。これによって、平常時には、DNS2 は参照されず、メール、ウェブサービスへのアクセスは、DNS1 で設定した名前解決が行われ、上位学内回線経由で通信が行われる（図 11）。反対に障害時は、DNS2 のみが参照され、DNS2 で設定した名前解決が行われ、バックアップ回線経由でメール、ウェブサービスへアクセスする（図 12）。なお、MX レコードについては、学内回線およびバックアップ回線経由からメールを受信できるように設定した（図 9 緑枠）。

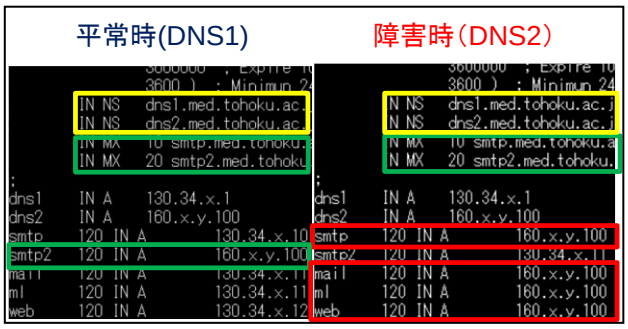

図 9. DNS 設定

名前	送信先	宛先	サービス	アクション
★outsideから障害時用インタフェース(Link1)へ				
dns	all	dns2-server	DNS	許可
外部からLink1への通信はDNSを許可				
★outsideから常時接続用インタフェース(Link2)へ				
mail	all	mail-server	IMAP IMAPS POP3 POP3S	許可
smtp	all	smtp-server	SMTPS SMTP Submission	許可
web	all	web-server	HTTP HTTPS	許可
all_deny	all	all	ALL	拒否
外部からLink2への通信はメールとウェブを許可、その他拒否				

図 10. バックアップ回線用 FW のポリシー設定

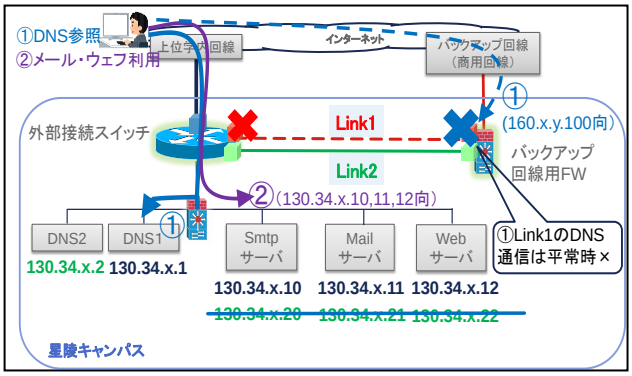

図 11. 平常時の DNS 参照とサーバへのアクセス

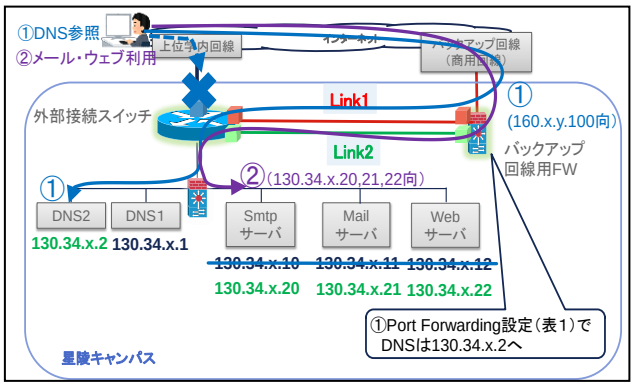

図 12. 障害時の DNS 参照とサーバへのアクセス

4 評価と考察

構築したバックアップ通信回線が正常に動作するか切り替え試験を休日の 9 月 11 日（土）に実施した。

・9/11 15:37　外部接続スイッチの link1 のインタフェースを有効化（no shutdown）
・9/11 15:52　外部接続スイッチの link1 のインタフェースを無効化（shutdown）

15:37 の切り替えでは、内部から外部向けの通信においては ping 落ちが生じることなく、バックアップ回線用 FW 側へ通信が切り替わり、ウェブサイトの閲覧を継続できることを確認した。外部向けに公開しているウェブサービスでは、20 秒程度で表示できるようになることが確認でき、メールサービスについても、バックアップ回線への切り替え後も学内・学外からともに送受信することが可能であった。

以上より、当初想定していた以下の 3 点が実現できていることが確認できた。

1. キャンパス内からインターネット上のサーバにアクセス可能
2. 学外からキャンパス内の DMZ で運用しているメール・ウェブサービスを利用可能
3. 障害発生時に簡単な操作で切り替え可能

バックアップ回線へ切り替えた際に、バックアップ回線用 FW のステータス画面で利用帯域などを確認した（図 13）。バックアップ回線は、最大速度 1Gbps の IPoE を用いたプロバイダ回線であるが、利用帯域は最大 400Mbps 程度、内向きの利用帯域は、100Mbps 程度を推移し、帯域的な問題は発生しなかった。平日に利用した場合の通信状況の確認については、今後の課題である。また、今回のバックアップ通信回線の整備では、基幹で運用しているウェブ、メールサービス以外の各研究室管理のサーバは、冗長化の対象外としていたが、ウェブサーバでリバースプロキシを使い、研究室管理のサーバも対象にすることを検討している。

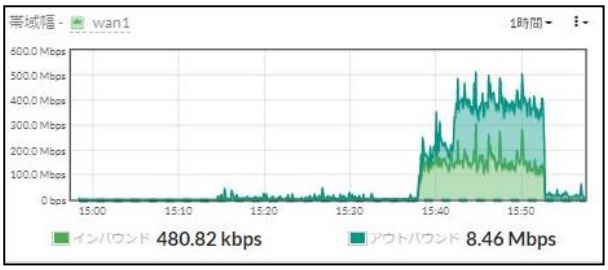

図 13. バックアップ回線切り替え時の利用帯域

東日本大震災（2011 年 3 月）の際には、上位学内回線が不通になり、メール・ウェブ通信が一切できない状況が長時間続いた。今回構築した仕組みにより、これらの課題が解決することが見込まれる。一方、バックアップ回線への切り替えは、手動で行う必要があるため、職員自身が切り替え作業を行えるようにするため、回線を切り替えるための訓練を定期的に行い、災害や障害に備えたい。

5 おわりに

オンライン授業や Web 会議が頻繁に使われるようになり、安定したインターネット通信環境を提供するため上位ネットワークの冗長化を検討した。一般に上位ネットワークを冗長化するには、ルーティングプロトコル BGP[1] [2]等を用いて実現することが一般的であるが、技術的、運用的な敷居が非常に高い。そこで、ネットワーク機器、サーバを効果的に組み合わせた簡単な仕組みによって、ネットワークを冗長化する仕組みを検討し、実際のネットワーク上で動作することを確認した。現時点では、提供できる帯域は限られているため、アナウンス方法やサービスの提供範囲などの運用について検討を進めていきたい。

参考文献

[1] 学術情報ネットワーク(SINET)BGP サービス: https://www.sinet.ad.jp/connect_service/service/bgp.
[2] 伊藤智博 他、災害時に備えた分散キャンパスによる情報基盤の整備、学術情報処理研究 15 巻、1 号、p.5-11、2011 年.