サイバーセキュリティレポート 1

学籍番号: 03-240712 氏名: 松本熙正

2026-06-02

課題１

まず、以下のコマンドでグーグル DNS サーバへの経路を調査した。

```
☒ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  ap68e1dc89c210 (192.168.11.1)  0.716 ms  0.537 ms  0.388 ms
 2  ne-ote301.kddnet.ad.jp (118.155.198.251)  4.620 ms  4.797 ms  4.656 ms
 3  * * *
 4  * * *
 5  dns.google (8.8.8.8)  7.990 ms  8.129 ms  7.531 ms
```

Google Public DNS(8.8.8.8) への経路は 5 ホップで到達した。途中の 2 箇所で応答が得られなかったが、これはルータが ICMP パケットへの応答を制限しているためと考えられる。最終的な RTT は約 8ms と非常に小さく、KDDI 網と Google ネットワークの接続が良好であることが分かる。

次に一般的なウェブサイトである Ubuntu 公式サイトのサーバへの経路を調査した。

```
☒ traceroute jp.ubuntu.com
traceroute: Warning: jp.ubuntu.com has multiple addresses; using 185.125.190.21
traceroute to jp.ubuntu.com (185.125.190.21), 64 hops max, 40 byte packets
 1  ap68e1dc89c210 (192.168.11.1)  0.946 ms  0.644 ms  0.448 ms
 2  ne-ote301.kddnet.ad.jp (118.155.198.251)  13.797 ms  4.939 ms  4.902 ms
 3  27.86.120.153 (27.86.120.153)  5.104 ms  6.666 ms  6.209 ms
 4  27.86.120.206 (27.86.120.206)  4.723 ms
    27.85.230.58 (27.85.230.58)  4.909 ms
    27.86.120.206 (27.86.120.206)  4.649 ms
 5  * * 27.85.134.14 (27.85.134.14)  5.366 ms
 6  103.22.201.25 (103.22.201.25)  12.610 ms
    103.22.201.87 (103.22.201.87)  10.235 ms
    103.22.201.95 (103.22.201.95)  6.081 ms
```

```
 7  162.158.117.248 (162.158.117.248)  6.219 ms
    172.64.214.89 (172.64.214.89)  5.406 ms
    172.68.41.45 (172.68.41.45)  5.601 ms
 8  172.68.117.79 (172.68.117.79)  5.955 ms
    172.71.4.17 (172.71.4.17)  4.492 ms
    162.159.109.55 (162.159.109.55)  5.497 ms
 9  172.68.117.221 (172.68.117.221)  5.744 ms
    172.64.214.57 (172.64.214.57)  4.916 ms
    162.158.117.247 (162.158.117.247)  5.574 ms
10  172.64.212.50 (172.64.212.50)  5.237 ms
    172.70.121.163 (172.70.121.163)  5.886 ms
    172.70.121.150 (172.70.121.150)  5.266 ms
11  * * *
12  lo.il3-gre1.canonical.com (185.125.191.2)  235.781 ms  237.269 ms
    lo.il3-gre2.canonical.com (185.125.191.4)  232.564 ms
13  website-content-cache-2.ps5.canonical.com (185.125.190.21)  232.089 ms  232.128 ms  232.650 ms
```

jp.ubuntu.com への traceroute では、13 ホップで宛先に到達した。宛先名には複数の IP アドレスが割り当てられており、今回は 185.125.190.21 が使用された。

経路の前半では、自宅ルータを通過した後、KDDI のネットワークを経由している。その後、6〜10 ホップ目では、同じホップ番号に対して複数の異なる IP アドレスが表示された。これは、経路上で負荷分散が行われているためと考えられる。

特に特徴的なのは、10 ホップ目までは応答時間が約 5〜6ms 程度であったのに対し、12 ホップ目以降で約 232ms まで大きく増加している点である。このことから、10 ホップ目付近までは国内または利用者に近いネットワークを経由し、その後、国際回線を通って Canonical 側の遠方のサーバへ到達したと考えられる。

```
☒ traceroute serika.work
traceroute: Warning: serika.work has multiple addresses; using 104.21.0.164
traceroute to serika.work (104.21.0.164), 64 hops max, 40 byte packets
 1  ap68e1dc89c210 (192.168.11.1)  0.891 ms  0.599 ms  0.441 ms
 2  ne-ote301.kddnet.ad.jp (118.155.198.251)  4.654 ms  4.628 ms  4.420 ms
 3  27.86.46.213 (27.86.46.213)  4.828 ms  6.214 ms  6.480 ms
 4  27.85.228.34 (27.85.228.34)  5.033 ms
    27.86.45.2 (27.86.45.2)  4.998 ms
    106.139.192.98 (106.139.192.98)  5.213 ms
 5  210.171.224.134 (210.171.224.134)  9.781 ms  5.787 ms *
 6  103.22.201.36 (103.22.201.36)  37.447 ms
    103.22.201.87 (103.22.201.87)  6.319 ms
    103.22.201.21 (103.22.201.21)  15.909 ms
```

```
 7  104.21.0.164 (104.21.0.164)  5.182 ms  5.406 ms  5.084 ms
 traceroute 100.111.***.***
traceroute to 100.111.***.*** (100.111.***.***), 64 hops max, 40 byte packets
 1  ***.***.ts.net (100.111.***.***)  5.633 ms  0.960 ms  0.505 ms
```

自身が Cloudflare でホストしている serika.work への traceroute では、7 ホップで宛先に到達した。宛先名には複数の IP アドレスが割り当てられており、今回は 104.21.0.164 が使用された。これは CDN を利用している Web サイトでよく見られる挙動である。

経路を見ると、最初に自宅ルータを通過し、その後 KDDI のネットワーク内を経由している。6 ホップ目では、3 回の測定で異なる IP アドレスが表示されており、経路上で負荷分散が行われている可能性がある。

最終的な応答時間は約 5ms であり、非常に短い。これは、serika.work が Cloudflare などの CDN を利用しており、利用者に近いエッジサーバから応答しているためと考えられる。したがって、物理的な Web サーバの所在地にかかわらず、CDN によって通信遅延が小さく抑えられていることが確認できた。

さらに、Tailscale VPN を使用してホストしている自分用のサーバへの経路も調査した。上記のコードでは IP アドレスを伏せているが、実際には Tailscale の割り当てたプライベート IP アドレスが表示される。

VPN を介しているため、通常のインターネット経路とは異なり、1 ステップで宛先に到達した。これは、Tailscale が直接的なピアツーピア接続を確立しているためである。応答時間は約 0.5ms と非常に短く、VPN 接続の効率性が示された。

課題２

インターネット黎明期には利用者数が少なく、主に大学や研究機関の研究者によって利用されていた。そのため、ネットワーク機器やプロトコルは利用者が悪意を持たないことを前提として設計されていたため、応答などの真正性確認がなかった。

ところが、インターネットの普及に伴い、悪意のある攻撃者が増加し、ネットワーク機器やプロトコルの脆弱性を突いて攻撃を行うようになった。IP プロトコルでは送信元アドレスの偽装、DNS では偽の応答によるキャッシュポイズニング、BGP では経路情報の偽装によるハイジャック、SMTP では送信者詐称によるフィッシングメールなどが問題となった。

これにより、ネットワーク機器やプロトコルの設計において、セキュリティを考慮する必要が生じた。いかにその例をあげる。

- IPsec: IP プロトコルにセキュリティ機能を追加するためのプロトコルスイートで、認証と暗号化を提供する。
- DNSSEC: DNS のセキュリティ拡張で、DNS 応答の真正性を検証するための署名機能を提供する。
- BGP セキュリティ拡張: BGP のセキュリティを強化するための拡張で、経路情報の認証や検証を行う。
- SMTP 認証: SMTP プロトコルに認証機能を追加するための拡張で、送信者の真正性を確認するための機能を提供する。