

## 1. デジタル署名と証明書に関する課題

<解答>

- ・ 1.1 Web page は amazon に所属している。

(ブラウザの補完機能で amahon.com から amazon.com に転送された。)

当該ページのデジタル証明書を確認すると、以下のような記載になっていることが確認できる。

証明書ビューア: www.amazon.com

全般(G)

詳細(D)

発行先

一般名 (CN)

組織 (O)

組織単位 (OU)

www.amazon.com

<証明書に含まれていません>

<証明書に含まれていません>

発行元

一般名 (CN)

組織 (O)

組織単位 (OU)

DigiCert Global CA G2

DigiCert Inc

<証明書に含まれていません>

有効期間

発行日

有効期限

2022年10月19日水曜日 9:00:00

2023年10月19日木曜日 8:59:59

指紋

SHA-256 指紋

SHA-1 指紋

C7 5C 68 98 4D CB 21 22 75 F9 F8 92 E8 D9 DC 93  
88 39 72 29 AA D5 38 EA B1 9F 79 61 DD 24 F8 0B

E4 13 1E 9E 4C 94 C7 7E DF 59 34 FA D8 82 F9 2E  
37 CE 69 D9

この証明書の、「発行先」欄にある「一般名」がこの Web page の所有者を示すのが本解答の根拠である。ただし、組織名には本来 Web page を所有、運営する企業名が入るはずだが amazon.com の証明書には含まれていないため非表示のようだ。

・ 1.2 amahon.com にクレジットカード情報は送信しない方が良い。

理由としては、amahon.com の CA 認証証明書（以下、証明書）を確認できないのが理由である。

証明書のない Web page では、HTTPS 通信を介して、ユーザーとサーバー間の安全な接続を確立することができない、その上、HTTPS を介さないという事は、ユーザーの情報はすべて暗号化されず平文で送信される。ゆえに、入力したクレジットカードなどの決済情報が、ユーザーとサーバー間の通信経路上で盗聴される可能性がある。

2.

<解答>

以下は Python 記法による解答。

```
def L(x: str) -> bool:
    if "ab" == x:
        return True
    else:
        return False
```

平文での解答。

$$L(x) = \begin{cases} True & \dots \text{入力 } x \text{ が } ab \text{ である時} \\ False & \dots \text{それ以外のすべての場合} \end{cases}$$