# 令和元年度 秋期 情報処理安全確保支援士

## ＜午後 I 解答・解説＞

### ＜問 1＞　電子メールのセキュリティ対策

●設問 1

**［試験センターによる解答例］**

a：MAIL FROM

SMTP で、エンベロープの送信者メールアドレスを指定するときに発行するコマンドは「MAIL FROM」である。

●設問 2

**［試験センターによる解答例］**

(1) b：×
　　c：×
　　d：×
　　e：×
　　f：×
　　g：○
　　h：×
　　i：×

(2) j：x1.y1.z1.1

(3) 送信側の DNS サーバに設定された IP アドレスと SMTP 接続元の IP アドレスが一致しないから（45 字）

(4) メール本文及びメールヘッダの改ざんの有無（20 字）


©2020 Takayuki Uehara

(1)b：取引先の DNS サーバに SPF の設定がないため、攻撃 1 が行われても、N 社では送信者メールアドレスが詐称されていることを判断できない。

c：取引先のメールサーバでメール受信時に SPF に必要な問合せが実施されないため、攻撃 2 が行われても、取引先では送信者メールアドレスが詐称されていることを判断できない。

d：N 社の外部メールサーバでメール受信時に SPF に必要な問合せが実施されないため、攻撃 1 が行われても、N 社では送信者メールアドレスが詐称されていることを判断できない。

e：取引先のメールサーバでメール受信時に SPF に必要な問合せが実施されないため、攻撃 2 が行われても、取引先では送信者メールアドレスが詐称されていることを判断できない。

f：N 社の外部メールサーバでメール受信時に SPF に必要な問合せが実施されないため、攻撃 1 が行われても、N 社では送信者メールアドレスが詐称されていることを判断できない。

g：取引先のメールサーバでメール受信時に SPF に必要な問合せが実施されるため、攻撃 2 が行われた場合、取引先では送信者メールアドレスが詐称されていることを判断できる。

h：N 社の外部メールサーバでメール受信時に SPF に必要な問合せが実施されないため、攻撃 1 が行われても、N 社では送信者メールアドレスが詐称されていることを判断できない。

i：N 社の外部 DNS サーバに SPF の設定がないため、攻撃 2 が行われても、取引先では送信者メールアドレスが詐称されていることを判断できない。

したがって g のみが“○”で、他は全て“×”となる。

(2) SPF では、［ j ］の部分にメールを送信するホストの IP アドレスを設定する。図 2 より、N 社のメールサーバの IP アドレスは“x1.y1.z1.1”であることがわかる。


©2020 Takayuki Uehara

(3) SPF では、メール受信者側のメールサーバが、Envelope-FROM をもとに、メール送信側の DNS サーバに問い合わせ、TXT レコードに設定された IP アドレスと SMTP 接続元の IP アドレスが一致することを確認する。下線①のケースでは、SMTP 接続元は最初にメールを送信したメールサーバではなく、最後にメールを転送したメールサーバとなるが、Envelope-FROM を変えずに転送しているため、メール受信側のメールサーバは、最初にメールを送信した側の DNS サーバに問合せを行うことになる。その結果、DNS サーバに設定された IP アドレスと SMTP 接続元の IP アドレスが一致せず、SPF 認証が失敗してしまうのである。

(4) 下線②にあるように、DKIM では、署名対象としたメール本文及びメールヘッダをもとに作成したハッシュ値を用いて検証を行っている。このことから、メールの送信元の正当性だけでなく、メール本文及びメールヘッダの改ざんの有無についても確認することができる。

●設問 3

**[試験センターによる解答例]**

k：mail.x-sha.co.jp.
l：x2.y2.z2.1
m：quarantine
n：r

k：図 7 で追加するべき MX レコードは、X 社のメールサーバのホスト名であるから、 k  には“mail.x-sha.co.jp.”が入る。ここで注意が必要なのは、ホスト名の末尾に“.”（ドット）を付けることである。図 2 にあるように、DNS のリソースレコードでドメイン名を設定する際には、ドメインの終端を明示するため、末尾に“.”を付ける。

l：追加するべき TXT レコードは X 社のメールサーバの IP アドレスであるから、 l  には“x2.y2.z2.1”が入る。

m：表 2 の p タグの説明にあるように、受信側で検証に失敗したメールを隔離するには、“quarantine”を設定する。

n：問題文にあるように、ニュースレターの配信時には、Header-FROM に N 社ドメイン名の


©2020 Takayuki Uehara

メールアドレス（例：letter@n-sha.co.jp）を設定し、Envelope-FROM に N 社のサブドメイン名 a-sub.n-sha.co.jp のメールアドレス（例：letter@a-sub.n-sha.co.jp）を設定する。表 2 の aspf タグの説明にあるように、このような場合、Header-FROM と Envelope-FROM に用いられているドメイン名の組織ドメインが一致していれば認証に成功とする必要があるため、設定するのは“r”である。

●設問 4

**［試験センターによる解答例］**

**N 社の取引先と似たメールアドレスから送信ドメイン認証技術を利用してメールを送信する。(42 字)**

N 社が SPF、DKIM、DMARC を導入していたとしても、攻撃者が送信ドメイン認証技術を利用し、N 社の取引先とよく似た紛らわしいメールアドレスを用いて N 社にメールを送信した場合には防ぐことはできない。その場合、メール受信者が攻撃者のなりすましであることに気付かなければ、フィッシング詐欺、標的型攻撃等の被害を受ける可能性がある。

## ＜問２＞　セキュリティインシデント対応におけるサイバーセキュリティ情報の活用

●設問 1

**［試験センターによる解答例］**

**(1) プロキシ認証に失敗したから（13 字）**

**(2) a：(b)**

**(3) ・グローバル IP アドレス M への HTTP 通信成功のログ（25 字）**
**・パブリック DNS サービス L への DNS 通信成功のログ（25 字）**

**(4) ・イ**
**・ウ**


©2020 Takayuki Uehara