メールアドレスです。”と表示するようになっている。そのため、攻撃者は任意のメールアドレスを入力して会員登録を試みれば、そのメールアドレスが N システムに会員登録されているものかどうかを判別することができ、自身のもつリストをスクリーニングできる。本設問で問われているのは、攻撃者がスクリーニングに利用した（する）と考えられる N システムの挙動であるから、「メールアドレスが会員登録されているかどうかで表示が異なるという挙動」が該当する。

(2) 上述のように、入力されたメールアドレスが会員登録されているかどうかで表示されるメッセージが異なっていることが問題であるため、これを修正し、入力されたメールアドレスの会員登録有無にかかわらず、同じメッセージを表示するようにする必要がある。したがって、表 3 で修正すべき処理は 2-b であり、修正後の処理は、「2-a と同じメッセージを表示する」である。

＜問 2＞　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]

(1) a：LDAP（4 字）
(2) b：OCSP（4 字）

＜解説＞

(1) ディレクトリサービスへのアクセスに用いるプロトコルであり、標準で TCP ポートの 389 番を使用するのは、LDAP（Lightweight Directory Access Protocol）である。

(2) Web サーバのサーバ証明書が失効していないことを確認するのに用いるプロトコルであり、RFC 6960 で規定されているのは、OCSP（Online Certificate Status Protocol）である。

●設問 2

[試験センターによる解答例]

(1) メールサーバ上では、メールが暗号化されていないから（25 字）
(2) c：メールサーバ（6 字）
(3) 復号に必要な秘密鍵を意図せず削除した場合（20 字）

＜解説＞

(1) 表 3 の項番 1 にあるように、「送信者から受信者まで暗号化された状態でメールを送受信する」ことが要件となっているが、SMTP over TLS、POP3 over TLS、STARTTLS 等でメールの通信を暗号化したとしても、メールサーバ上ではメールそのものは暗号化されていないため、この要件を満たすことはできない。

(2) 攻撃者が委託先になりすましたメールを送るために用意するものであり、その真正性を確認することでなりすましを検出できるものであるから、［ c ］に該当するのはメールサーバである。

(3) S/MIME（Secure Multipurpose Internet Mail Extensions）は画像、音声などのバイナリファイルを送信するための規格である MIME を拡張したものであり、添付ファイルも含めて暗号化することができる。S/MIME は、PKCS（Public Key Cryptography Standard）に従って暗号化、ディジタル署名などを行うことで、電子メールの機密性と完全性を高めることができる。S/MIME は不特定多数のユーザ間で安全性、信頼性の高い通信を行うことを想定しているため、利用にあたって各ユーザは公的な第三者機関が発行するディジタル証明書（S/MIME 証明書）を取得することが前提となる。S/MIME を利用する範囲が特定の組織内であれば、当該組織内にプライベート CA を設置・運営する方法もある。
S/MIME では、受信者がメールを参照する際に自身の秘密鍵を用いて復号する必要があるため、それができなくなるケースとしては、当該秘密鍵を意図せず削除してしまった場合が考えられる。

●設問 3

[試験センターによる解答例]

d：ディジタル署名（7 字）
e：検証（2 字）
f：ML の登録メンバ（8 字）
g：ML（2 字）

＜解説＞

d、e：S/MIME では、送信者によってメールに付されたディジタル署名を検証することで、受信したメールが確かに当該送信者によって送られたものであり、途中で改ざんされていないことを確認することができる。R 社の従業員が送信したメールのディジタル署名を検証するためには、当該従業員の S/MIME 証明書を発行した R 社 CA のルート証明書を受信者の PC に登録しておく必要がある。

f、g：ML 宛てのメールを暗号化できないという課題に対する解決案である。ML 宛てのメールは、送信者によって ML のアドレスに送信された後、G サービスによって ML の登録メンバ宛てに送信される。この仕組みにおいて S/MIME を用いた暗号化を行うには、次のような方法が考えられる。

・あらかじめ G サービスに ML の登録メンバ各々の S/MIME 証明書を登録しておく。
・あらかじめ ML のメールアドレスの S/MIME 証明書を G 社から発行してもらう。
・メール送信者は、上記 ML の S/MIME 証明書を使って暗号化したメールを ML 宛てに送る。
・G サービスは受信した ML 宛てのメールを復号した後、ML の登録メンバ各々の S/MIME 証明書を使って当該メールを暗号化し、各 ML の登録メンバ宛てに送信する。

したがって、[f] には“ML の登録メンバ”、[g] には“ML”が入る。