

問4 VPN（Virtual Private Network）に関する記述を読んで、設問1～3に答えよ。

A社は、関東のN事業所で利用している営業支援システムを、関西のM事業所でも利用することにした。営業支援システムのサーバはN事業所のコンピュータセンタに設置されている。M事業所でN事業所の営業支援システムを利用するために、システム部が中心となってIPsecを利用したVPNの導入を検討し、報告書を作成した。

〔報告書の内容（抜粋）〕

(1) ネットワーク構成

M事業所からN事業所の営業支援システムに接続するためのネットワーク構成を図1に示す。VPNの実現には、VPNルータを利用する。

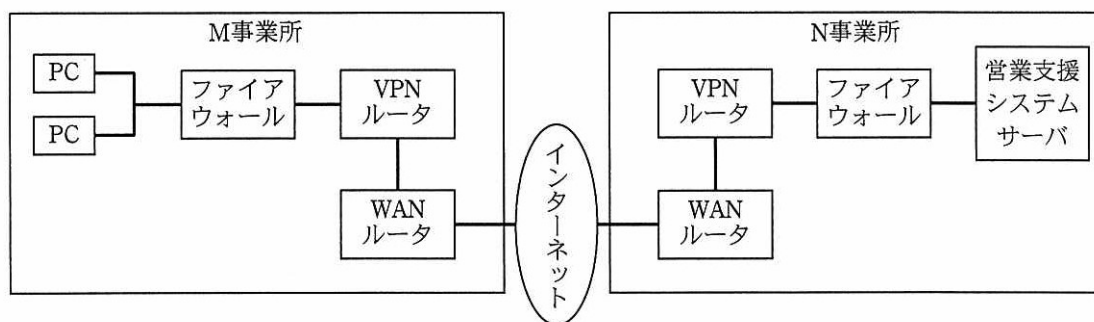


図1 ネットワーク構成

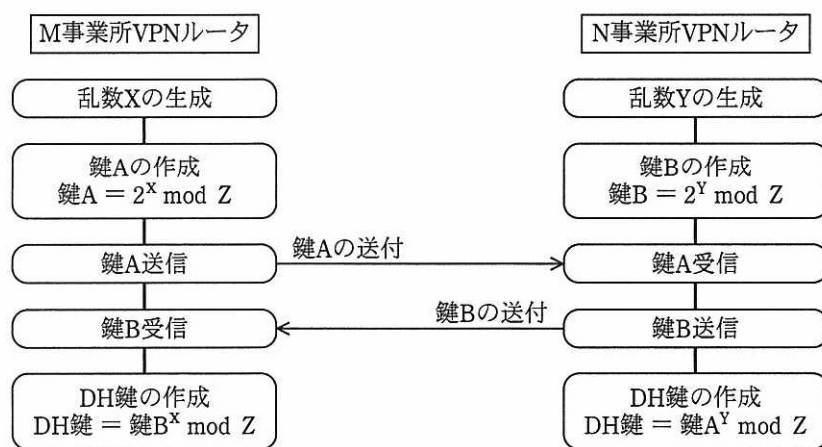
(2) IPsecの説明

IPsecは、暗号技術を用いてインターネットでデータを安全に送受信するための規格である。IPsecには、暗号化に利用する鍵を安全に交換する仕組みや、相手のVPNルータを認証する仕組みがある。

(3) IPsecの要素技術の説明

① 暗号化に利用する鍵を安全に交換する仕組み

IPsec では、VPN ルータ間で暗号化に利用する鍵を、安全に交換する仕組みの一つとして、Diffie-Hellman 鍵交換法（以下、DH 法という）を利用している。DH 法の例を図 2 に示す。DH 法で作成された鍵（以下、DH 鍵という）を暗号化に利用する。



注記1 X, Yは正の整数とする。

注記2 2^X は、2のX乗を示す。

注記3 $P \bmod Q$ は、PのQによる剰余を示す。

注記4 Zは、M事業所VPNルータ、N事業所VPNルータに事前に設定された素数である。

図2 DH法の例

② 相手の VPN ルータを認証する仕組み

IPsec では、データ受信側の VPN ルータがデータ送信側の VPN ルータを認証する仕組みの一つとして、RSA アルゴリズムを用いたデジタル署名を利用している。その仕組みを図 3 に示す。

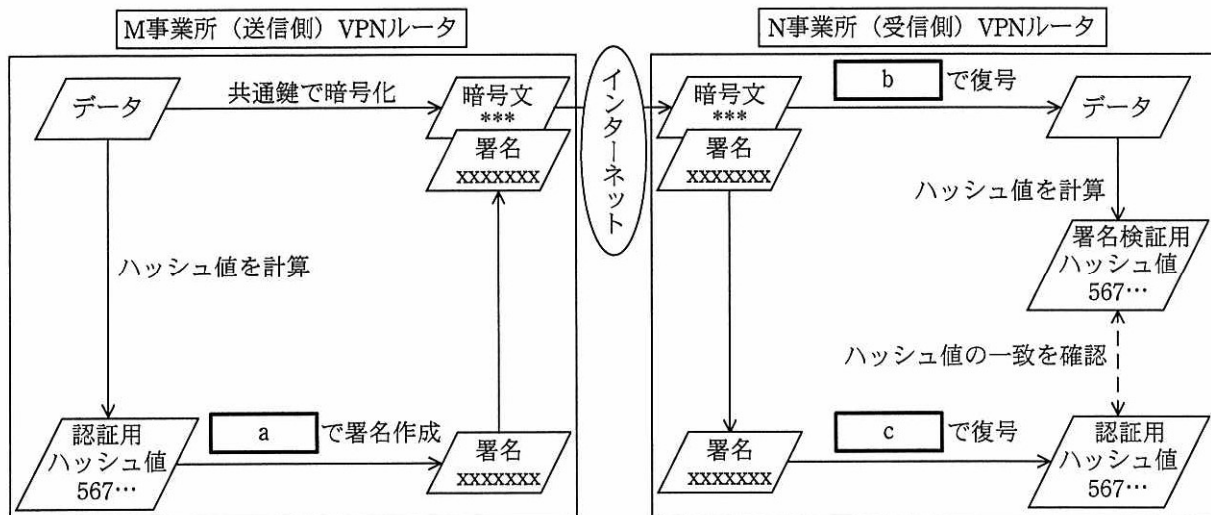


図 3 相手の VPN ルータを認証する仕組み

(4) IPsec を利用した VPN の導入効果

IPsec は、**d** 層でセキュリティを実現するプロトコルであるので、アプリケーションを変更せずに通信のセキュリティを担保できる。そして、パケットを暗号化することによって **e** を行い、RSA アルゴリズムを用いたデジタル署名を利用することによって **f** 及び改ざんの検知を行っている。

設問 1 図 2 で $Z=11$, $X=7$, $Y=5$ の場合, DH 鍵として正しい値を, 解答群の中から選べ。

解答群

ア 2 イ 5 ウ 7 エ 10 オ 13

設問 2 図 3 中の に入れる適切な答えを, 解答群の中から選べ。

a～c に関する解答群

ア 共通鍵 イ 受信側の公開鍵 ウ 受信側の秘密鍵
エ 送信側の公開鍵 オ 送信側の秘密鍵

設問 3 (4)の IPsec を利用した VPN の導入効果に関する記述中の に入れる正しい答えを, 解答群の中から選べ。

d に関する解答群

ア アプリケーション イ データリンク ウ トランスポート
エ ネットワーク

e, f に関する解答群

ア DoS 攻撃の対策 イ ウイルス感染の検知
ウ セキュリティホールの修正 エ 送受信するデータの圧縮
オ 盗聴の対策 カ なりすましの検知