問040012問題

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。

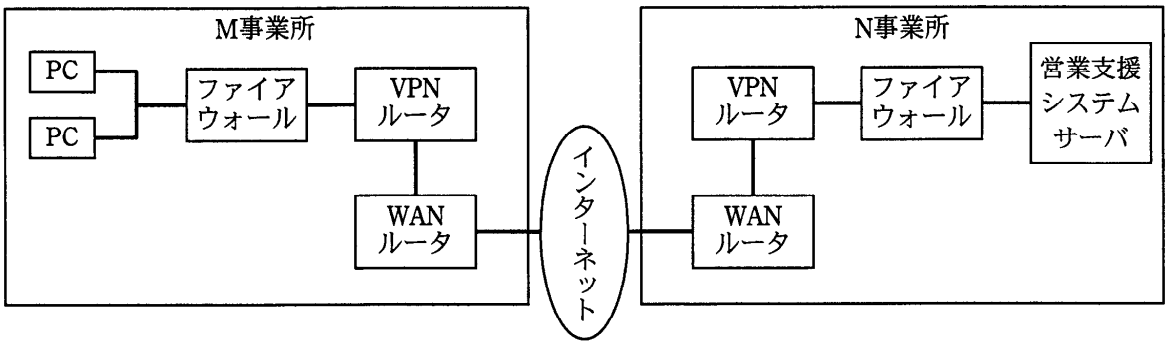


図１　ネットワーク構成

（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ｏ

（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

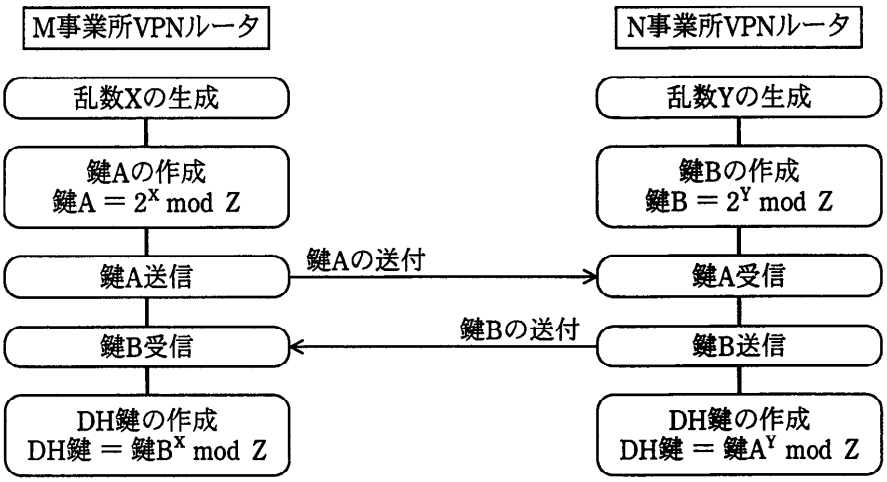
IPsecでは，ＶＰＮルータ間で暗号化に利用する鍵を,安全に交換する仕組みの一つとして,Diffie-Hellman鍵交換法（以下，ＤＨ法という）を利用している。ＤＨ法の例を図２に示す。ＤＨ法で作成された鍵（以下，ＤＨ鍵という）を暗号化に利用する。

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ィジタル署名を利用している。その仕組みを図３に示す。

（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ィ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。



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 mod 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

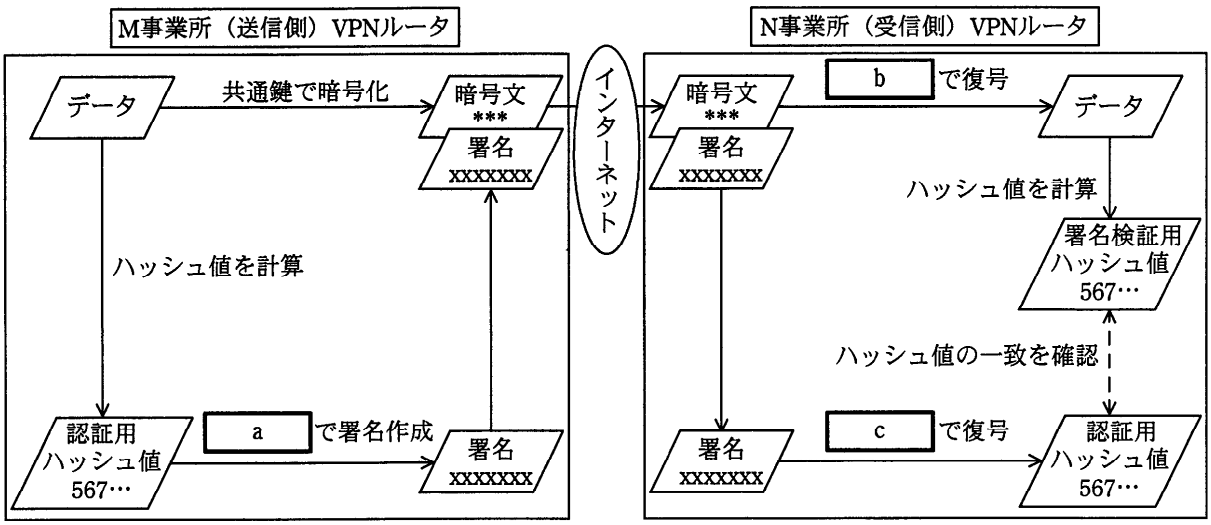


図３　相手の VPN ルータを認証する仕組み

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