問040012解説

◆解答

設問１　エ

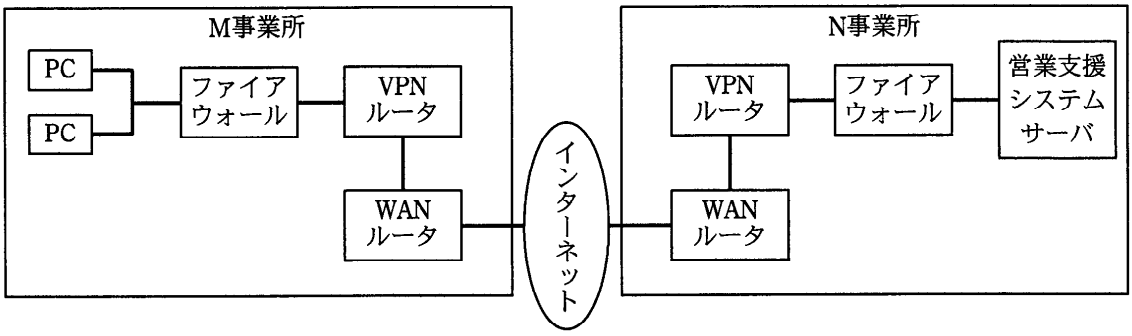
設問２　ａ　オ　　ｂ　ア　　ｃ　エ

設問３　ｄ　エ　　ｅ　オ　　ｆ　カ

◆解説

ＶＰＮに関する問題である。

ネットワークの構成図



ネットワーク構成

ＩＰsecとは

ＩＰsecは暗号技術を用いることで、ＩＰパケット単位で改竄検知や秘匿機能を提供するプロトコルである。ＩＰsecはネットワーク層でセキュリティを実現するプロトコルであり、暗号化をサポートしていないトランスポート層やアプリケーションを用いても、通信路の途中で、通信内容を覗き見られたり改竄されることを防止できる。

ＩＰsecの構成

ＩＰsecは、２つのピアの間にＳＡという単方向コネクションを確立ｄ、ピア間にセキュアな通信を確立する。ＳＡは単方向であるため、双方向通信を行う場合には、上りと下りの２つのＳＡが必要とある。

ピアは、ホストとセキュリティ・ゲートウェイの二種類に分類できる。前者は、個人端末やサーバのようなＩＰ通信の端点に相当する機器であり、後者は、ルータのようなＩＰ通信の中継を担う機器である。ホストからホストまでの通信全体を直接１つのＳＡで保護することもできるし、２つの中継地点間毎に別々のＳＡを確立して通信を保護するリレー形態の運用も可能である。

ＩＰsecの各ピアは、ＳＰＤ、ＳＡＤの２つのデータベースで管理する。ＳＰＤは、ＩＰアドレス、プロトコル、ＴＰＣポートといった情報に応じて、パケットを破棄、ＩＰsecを使わずに送信、ＩＰsecを使って送信のいずれかを決めるセキュリティポリシーのデータベースである。ＳＡＤは各ピアとＳＡを確立する際に用いるパラメータのデータベースである。

プロトコルの流れ

ピアＭがピアＮに向けてＩＰsecで通信するには、以下の３ステップで行う。

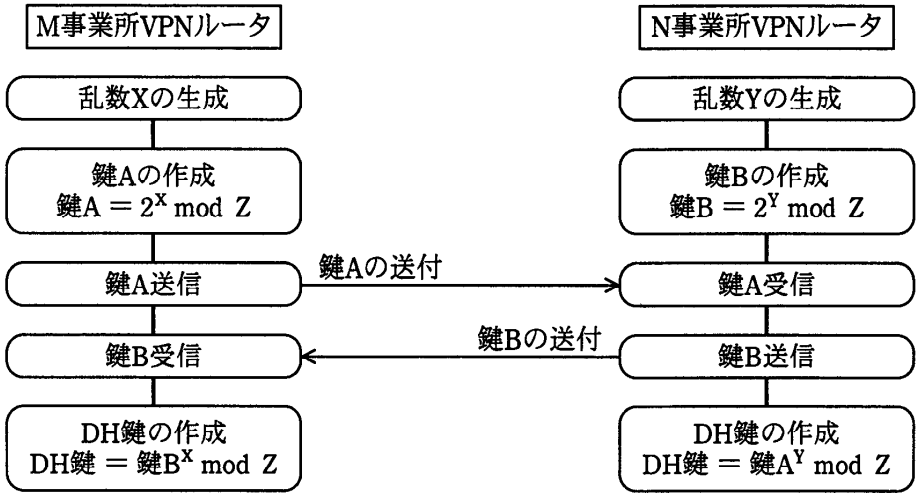
① ＭからＲへのＳＡを確立する。
　鍵共有プロトコルが実行される。

② ＳＡを使ってパケットをＭがＮに暗号通信する。
　共有された鍵を用いて、通信を暗号化する。

③ Ｎがデータを受信し、復号などの必要処理を行う。
　共有された鍵を用いて、通信を復号する。

暗号化鍵を交換する仕組みと手順

ルータ間での共通鍵の交換にＤＨ鍵交換法を使用する。



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 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。

DH 法の例

① ＭとＮが通信を行うとき、ＭとＮはそれぞれ正の整数Ｘ，Ｙを乱数で生成する。

② Ｍは次の値Ａを計算してこれをＮに送信する。

$$A = 2^X \bmod Z$$

③ Ｎも次の値Ｂを計算してこれをＭに送信する。

$$B = 2^Y \bmod Z$$

④ Ｍは受信したＢを使用してＫＡを計算する。

$$KA = B^X \bmod Z = (2^Y \bmod Z)^X \bmod Z = 2^{YX} \bmod Z$$

⑤ Ｎも受信したＡを使用してＫＢを計算する。

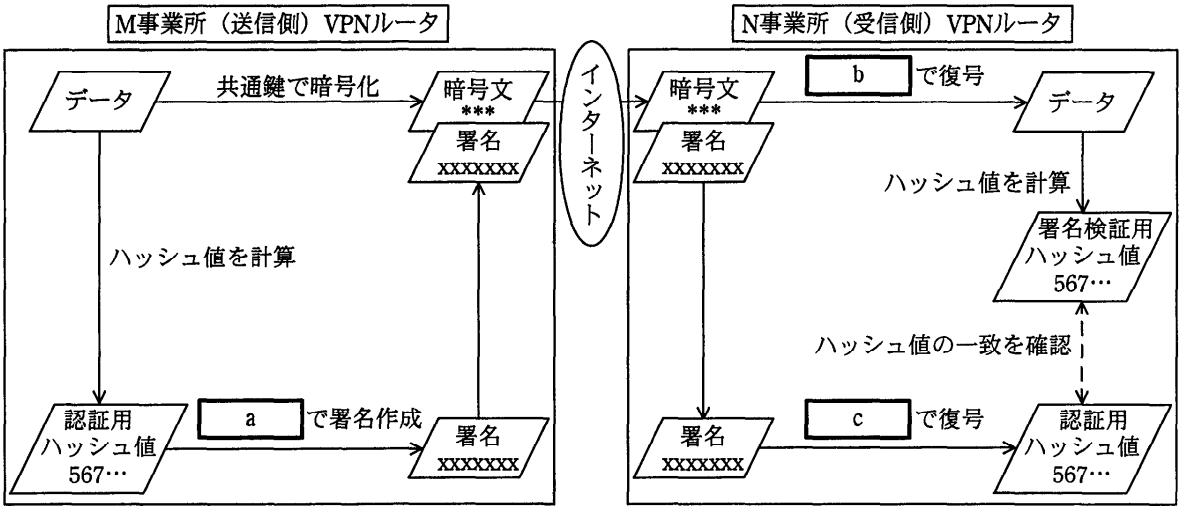
$$KB = A^Y \bmod Z = (2^X \bmod Z)^Y \bmod Z = 2^{XY} \bmod Z$$

⑥ ＭとＮが計算したＫＡ、ＫＢは

$$KA = KB = 2^{XY} \bmod Z$$

になっているため、以後この値を共通鍵暗号方式の鍵として使用する。

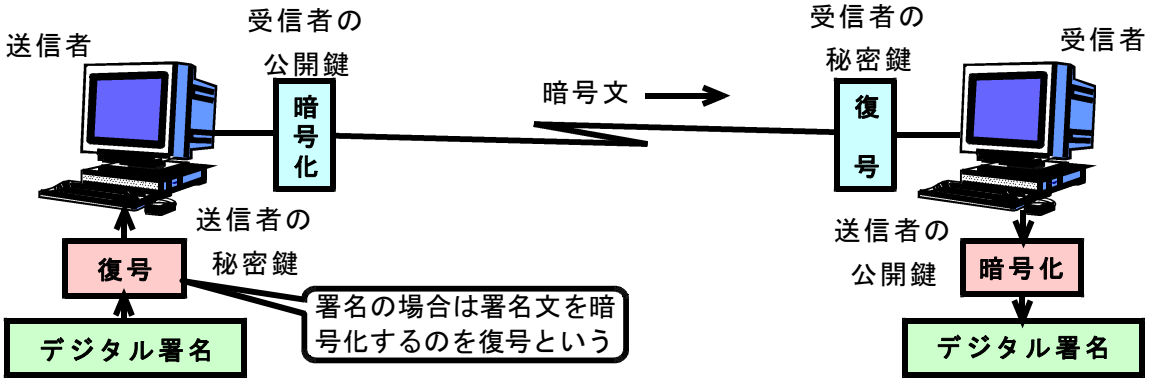
相手ルータ認証の仕組み



相手の VPN ルータを認証する仕組み

Ｎ事業所のルータがＭ事業所のルータを認証するのにＲＳＡアルゴリズムを用いたディジタル署名を利用する。

デジタル署名の仕組み



デジタル署名は個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。

デジタル署名システムは、メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッ

セージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

このシステムでは、署名の暗号化を「復号」といい、署名の復号を「暗号化」という。

デジタル署名実現の条件

① Ａを確認するには、署名者Ａだけが署名でき、Ａ以外は署名できない条件が必要である。

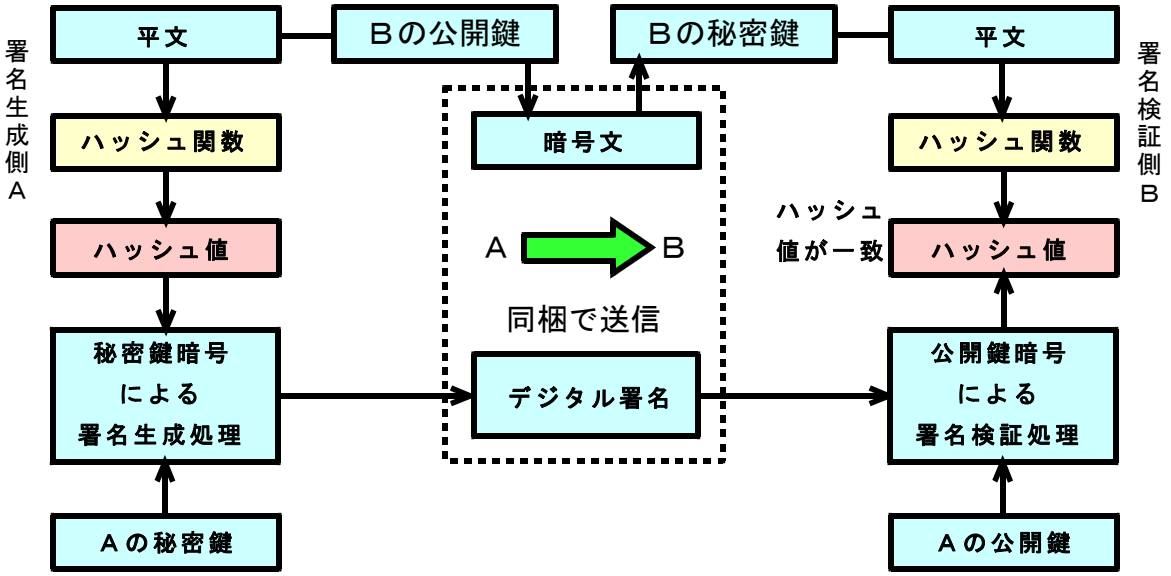
② Ａ以外のＡの関係者が、だれもがＡの署名であることを確認できる必要がある。

公開鍵暗号方式の基本原理

① 「Ａだけができる」に対して、Ａだけが持っているＡの秘密鍵による処理で可能である。

② 「誰でもできる」に対して、みんなが持っているＡの公開鍵による処理で可能である。

ハッシュ値とハッシュ関数



デジタル署名はメッセージに署名して初めて意味のあるものになる。しかし、長いメッセージにデジタル署名することは効率的でない。そこで、長いデータに署名する代わりに、そのデータのハッシュ値に署名することによって効率的になる。長いデータを攪乱し、一定の長さのハッシュ値に圧縮する操作に利用される数学的処理法がハッシュ関数である。

安全なハッシュ関数の条件は、ハッシュ値から入力を推定することが困難であり、異なるデータのハッシュ値が一致する確率が極めて小さいということである。標準的に用いられている関数としては、ＭＤ５、ＭＡＳＨ、ＳＨＡ−１、ＳＨＡ−２などがある。

ハッシュを活用したデジタル署名の手順

① 送信者は送信するデータを作成する。

② 作成したデータを基にハッシュ関数を使ってハッシュ値を算出する。

③ 公開鍵暗号方式を利用してハッシュ値を送信者の秘密鍵を使って暗号化する。

④　①で作成したデータと③で作成した「送信者の秘密鍵で暗号化したハッシュ値」を合わせて受信者に送付する。

⑤　受信者は，受信データを基に，送信者が使ったものと同じハッシュ関数を使ってハッシュ値を算出する。

⑥　送信者が送ってきた「送信者の秘密鍵で暗号化されたハッシュ値」を，あらかじめ入手していた送信者の公開鍵で復号する。

⑦　⑤で算出したハッシュ値と，⑥で復号したハッシュ値を比較する。両者が一致すれば，「伝送経路上でデータが改ざんされていない」，「送信者が正しい」という点を確認できる。

この仕組みを実現するために、受信者はあらかじめ送信者の公開鍵を入手している。

設問１

ＤＨ鍵の値を計算する問題である。

Ｘ＝７、Ｙ＝５、Ｚ＝１１の場合について計算する。

Ａ＝2^{7} mod １１＝（８×１６）mod １１＝１２８ mod １６＝７

ＤＨ＝7^{5} mod １１＝１０

Ｂ＝2^{5} mod １１＝３２ mod １１＝１０

ＤＨ＝10^{7} mod １１＝１０００００００ mod １１＝１０

ＤＨは１０となり、求める答えはエとなる。

設問２

ａは認証用ハッシュ値を署名を作成する問題であり、送信側の秘密鍵を使用する。求める答えはオとなる。

ｂはデータの暗号文を復号する問題であり、データの暗号化、復号は共通鍵で行う。求める答えはアとなる。

ｃは署名を復号する問題であり、送信者の公開鍵を使用する。求める答えはエとなる。

設問３

ｄはＩＰsecのセキュリティを実現するプロトコルの層を求める問題であり、ネットワーク層である。求める答えはエとなる。

ｅはバケットの暗号化で盗聴対策を実現する。求める答えはオとなる。

ｆは公開鍵を利用したディジタル署名を利用してなりすましの検知を行う。求める答えはカとなる。