1 暗号化技術

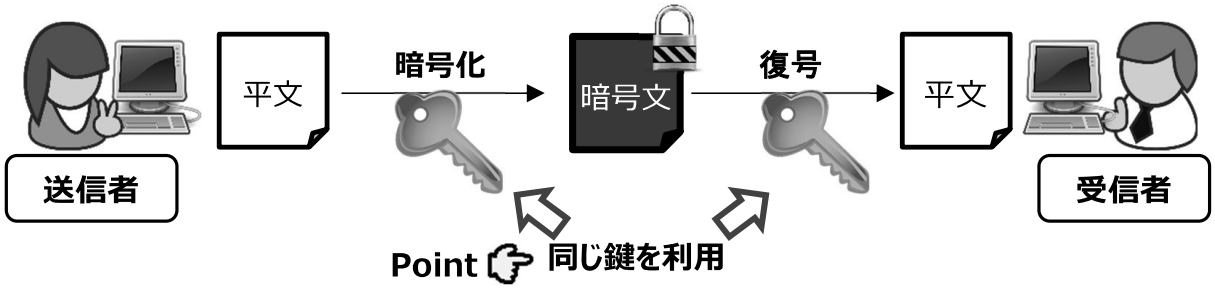
データを権限なしの照会や使用から保護する方法に、暗号化技術があります。通信データの漏えいや改ざんといった犯罪を防止するためには暗号化は欠かせません。

暗号化とは、データを第三者が解読できないように一定のルールで変換することで、暗号化する前のデータを**平文**、暗号化されたデータを**暗号文**と呼びます。また、暗号文を平文に戻すことを**復号**といいます。

暗号化の代表的な方法には、共通鍵暗号方式と公開鍵暗号方式があります。

１．共通鍵暗号方式

共通鍵暗号方式は、暗号化も復号も共通の鍵（共通鍵）を用いる方式です。そのため、鍵情報は公開せずに秘密にします。この方式では、仮にＮ人の相手とデータのやり取りをする場合にはＮ個の鍵を必要とするため、鍵の管理（鍵管理）が問題となります。また、鍵情報を安全に相手方に渡す方法を工夫する必要があります。



共通鍵暗号方式

例題 1-A1　平成25年度秋午前Ⅱ　問3　[出題頻度：★★★]

共通鍵暗号方式で，100 人の送受信者のそれぞれが，相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか。

ア 200　　イ 4,950　　ウ 9,900　　エ 10,000

各人がもっている鍵の総和は「（人数－１）×人数」となります。

ただし、鍵の種類で考えると、ＡのＢに対する鍵と、ＢのＡに対する鍵は同一のものになるため、共通鍵の総数は「（人数－１）×人数÷２」となります。

したがって、必要な鍵の個数は「(100－１)×100÷２＝4,950 個」となります。

解答－イ

１）ストリーム暗号とブロック暗号

共通鍵暗号方式には、ストリーム暗号とブロック暗号の２つの方法があります。

①ストリーム暗号

ストリーム暗号は、データをビット単位で暗号化する方法です。具体的には、**疑似乱数生成器**（PRNG：PseudoRandom Number Generator）よって生成された**疑似乱数**を暗号化鍵として、ビット単位にデータと暗号化鍵を XOR で重ね合わせて暗号化します。

ストリーム暗号は、無線 LAN の暗号化方式の一つである WEP（Wired Equivalent Privacy）で使われている RC4（Ronald's Code 4）で採用しています。

また、KDDI 研究所と九州大学がモバイル機器向けに共同で開発した **KCipher-2** は軽くて安全性も高い高速ストリーム暗号です。

②ブロック暗号

ブロック暗号は、データを一定の大きさ（ブロック）に分割してブロックごとに暗号化する方法です。

ブロック暗号には、１ブロックずつ単純に暗号化する **ECB**（Electronic CodeBook）、前のブロックを暗号化した結果を次のブロックに XOR で重ね合わせ、その結果に対して暗号化する **CBC**（Cipher Block Chaining）、前のブロックを暗号化した結果を暗号アルゴリズムで暗号化した値を XOR でブロックに重ね合わせて暗号化（暗号アルゴリズムの出力を暗号アルゴリズムの入力にフィードバック）する **CFB**（Cipher FeedBack）、外部からの初期値を暗号化し、それをまた暗号化することで乱数を生成し、生成した乱数列を XOR でブロックに重ね合わせ暗号化する **OFB**（Output FeedBack）、１ずつ増加していくカウンタを暗号化した値（鍵ストリーム）を XOR でブロックに重ね合わせて暗号化する **CTR**（CounTeR）などの暗号利用モードがあります。

また、暗号化・復号と同時に認証コードの生成・検証を行うことでデータの秘匿と認証の機能を併せ持つ**認証付き暗号**（**AEAD**：Authenticated Encryption with Associated Data）と呼ばれる暗号利用モードもあります。

例題 1-A2　令和５年度春午前Ⅱ　問７　[出題頻度：★☆☆]

ブロック暗号の暗号利用モードの一つである CTR(Counter)モードに関する記述のうち，適切なものはどれか。

ア　暗号化と復号の処理において，出力は，入力されたブロックと鍵ストリームとの排他的論理和である。

イ　暗号化の処理において，平文のデータ長がブロック長の倍数でないときにパディングが必要である。

ウ　ビット誤りがある暗号文を復号すると，ビット誤りのあるブロック全体と次のブロックの対応するビットが平文ではビット誤りになる。

エ　複数ブロックの暗号化の処理は並列に実行できないが，複数ブロックの復号の処理は並列に実行できる。

イ　ECB モードに関する記述です。

ウ　CBC モードや CFB モードに関する記述です。

エ　CBC モードに関する記述です。

解答－ア

２）暗号アルゴリズム

代表的な暗号アルゴリズムには、DES、Triple-DES、AES（Advanced Encryption Standard）があります。これらはいずれも、CBC モードのブロック暗号です。

①DES と Triple-DES

DES は、IBM が開発し 1977 年にアメリカ合衆国の標準となった暗号アルゴリズムですが、実質的な鍵の長さが 56 ビットと短く現在では安全性が低くほとんど使われていません。その後、DES の改良版として、暗号化、復号、暗号化の順に３回繰り返す **Triple-DES** が開発されました。鍵の長さは 168 ビットですが、処理速度が遅く、この暗号アルゴリズムも安全性には不安があります。

②AES

AES は、平文を 128 ビットの固定長のブロックに分け、暗号化の鍵として 128、192、256 ビットの３つの長さが選択できる暗号アルゴリズムです。処理速度が速く、安全性も高いため、2000 年に **NIST**（National Institute of Standards and Technology：国立標準技術研究所）によりアメリカ合衆国の標準的な暗号アルゴリズムとなりました。

なお、鍵の長さによって変換の回数（段数）が、128 ビットは 10 段、192 ビットは 12 段、256 ビットは 14 段と決まっています。暗号化の際には段数の分だけ暗号化処理を行います。

例題 1-A3　平成30年度秋午前Ⅱ　問1　[出題頻度：★★★]

AES の特徴はどれか。

ア　鍵長によって，段数が決まる。
イ　段数は，６段以内の範囲で選択できる。
ウ　データの暗号化，復号，暗号化の順に３回繰り返す。
エ　同一の公開鍵を用いて暗号化を３回繰り返す。

AES（Advanced Encryption Standard）は、平文を固定長のブロックに分け、ブロック長によって 128、192、256 ビットの３つの暗号化の鍵が選択でき、処理速度が速く、安全性も高いため、2000 年に NIST（National Institute of Standards and Technology：国立標準技術研究所）によってアメリカ合衆国の標準的な方法となりました。

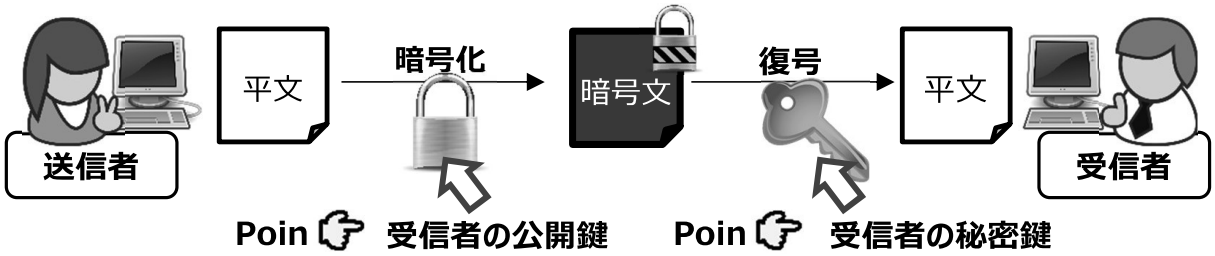
なお、鍵の長さによって変換の回数（段数）が、128 ビットは 10 段、192 ビットは 12 段、256 ビットは 14 段と決まっています。暗号化の際には段数の分だけ暗号化処理を行います。

解答－ア

別冊演習ドリル　1-A1

２．公開鍵暗号方式

公開鍵暗号方式は、データ受信者の公開鍵（暗号化のための鍵情報と暗号アルゴリズムを不特定多数の者に公開）を使ってデータを暗号化する方式です。暗号化と復号のための鍵情報は共通でなく、復号のための鍵情報は公開しません。暗号文の受信者は、公開鍵と対の秘密鍵で復号します。この方式は、暗号化の鍵を公開できるため、不特定多数との通信に向いています。ただし、共通鍵暗号方式に比べて、鍵情報を複雑にする必要があり、暗号化に多くの時間が必要となります。応用したものにデジタル署名（後述）があります。



公開鍵暗号方式

１）暗号アルゴリズム

代表的な暗号アルゴリズムに、1976 年に発表された世界初の公開鍵暗号アルゴリズムである **DH**（Diffie-Hellman）、現在最も広く使われており開発者の頭文字（Ronald Rivest、Adi Shamir、Leonard Adleman）を取って命名された RSA、楕円曲線暗号（ECC:Elliptic Curve Cryptography）があります。

①DH

DH は、離散対数問題を利用して、送信者と受信者が各々公開鍵と秘密鍵を用意し、公開鍵のみを相手に送信し、各自、自分の秘密鍵と受信した公開鍵から共通鍵を作成し共有する**鍵共有方式**です。**共有鍵**を共通鍵暗号方式に利用することができます。

②RSA

RSAは、桁数の多い数の素因数分解が極めて困難という原理を利用したもので、鍵長が1,024ビットや2,048ビットと極めて長く、暗号化や復号に時間がかかります。

③楕円曲線暗号

楕円曲線暗号は、楕円曲線と呼ばれる数式によって定義される特殊な加算法に基づいて暗号化や復号を行なう方式で、解読が非常に困難です。なお、楕円曲線暗号を用いてDSA（Digital Signature Algorithm）署名（デジタル署名専用の公開鍵暗号アルゴリズム）を実現する方式を**ECDSA**（Elliptic Curve Digital Signature Algorithm）といいます。

例題 1-A4　　平成25年度春午前Ⅰ　問13　[出題頻度：★★★]

公開鍵暗号を使ってｎ人が相互に通信する場合，全体で何個の異なる鍵が必要になるか。ここで，一組の公開鍵と秘密鍵は２個と数える。

ア　ｎ＋１　　イ　2n　　ウ　n(n－1)／2　　エ　$\log_2 n$

公開鍵暗号方式では、送信データは受信者の公開鍵で暗号化し、受信データは受信者の秘密鍵で復号します。すなわち、１人につき公開鍵と秘密鍵の２つがあれば、データの送受信が可能です。したがって、ｎ人が相互に暗号化通信を行うためには、全体で２ｎ個の鍵が必要になります。

解答－イ

別冊演習ドリル　1-A2～A4

２）前方秘匿性（PFS）

暗号化に使用する秘密鍵を公開鍵暗号方式で交換したときに、誤って秘密鍵が漏えいした場合、過去に暗号化した情報が解読される恐れがあります。

仮に、鍵交換に使用した秘密鍵が漏えいした場合でも、過去に暗号化した情報は解読されない性質を**前方秘匿性**（PFS： Perfect Forward Secrecy）と呼びます。PFS でない暗号アルゴリズムを用いて暗号化されたデータは、鍵情報が漏えいした場合には、過去に暗号化されたデータも含めてすべてのデータが復号される可能性があります。

なお、PFS である暗号アルゴリズムに、DH を発展させた、**DHE**（DH Ephemeral：DH 使い捨てアルゴリズム）と **ECDHE**（Elliptic Curve DHE：楕円曲線 DH 使い捨てアルゴリズム）があります。

例題 1-A5　　令和4年度秋午前Ⅱ　問8　[出題頻度：★☆☆]

前方秘匿性（Forward Secrecy）の説明として，適切なものはどれか。

ア　鍵交換に使った秘密鍵が漏えいしたとしても，それより前の暗号文は解読されない。
イ　時系列データをチェーンの形で結び，かつ，ネットワーク上の複数のノードで共有するので，データを改ざんできない。
ウ　対となる二つの鍵の片方の鍵で暗号化したデータは，もう片方の鍵でだけ復号できる。
エ　データに非可逆処理をして生成される固定長のハッシュ値からは，元のデータを推測できない。

イ　ブロックチェーンで使用される分散型台帳の性質の説明です。
ウ　公開鍵暗号方式の性質の説明です。
エ　ハッシュ関数の原像計算困難性の説明です。

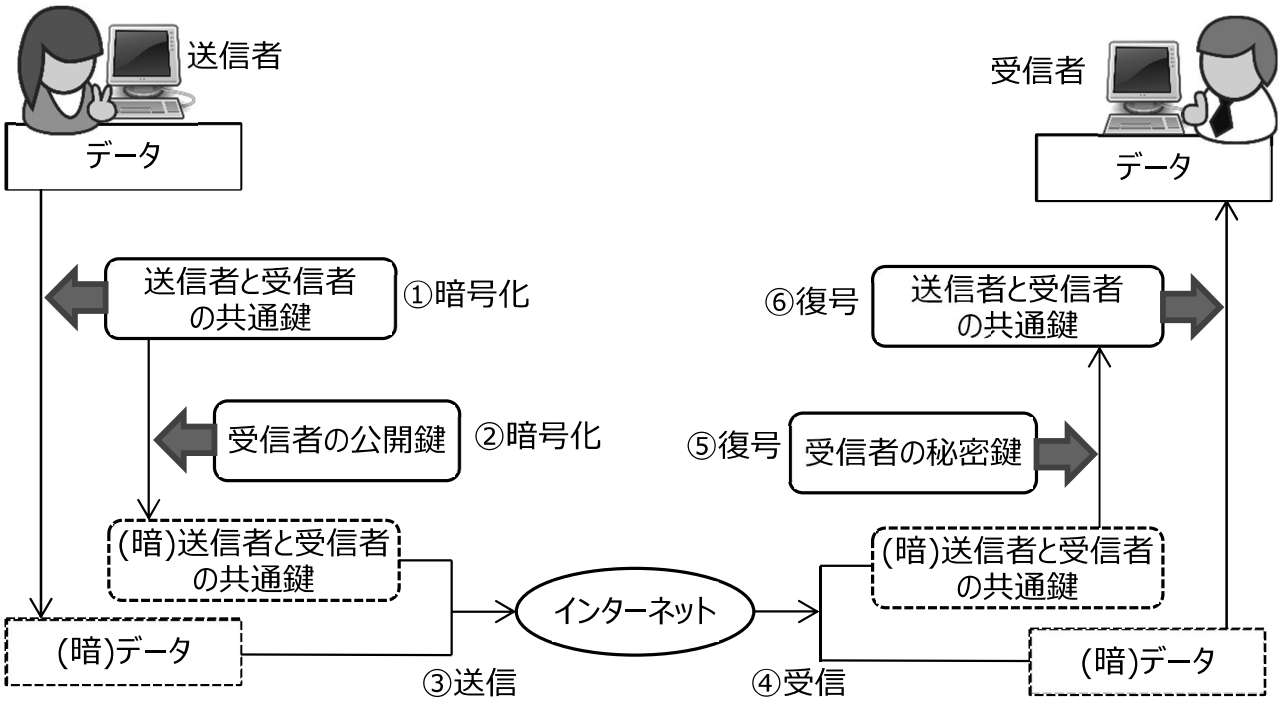
解答－ア

３．ハイブリッド暗号方式

共通鍵暗号方式は、公開鍵暗号方式に比べ処理は高速ですが、鍵情報を安全に配布することが難しいという問題があります。これに対して、公開鍵暗号方式は、鍵情報の管理は容易ですが、処理に時間がかかるという問題があります。この２つの相反する性質をもつ暗号方式を組み合わせることで互いの問題点を解決したのが、ハイブリッド暗号方式です。

ハイブリッド暗号方式では、まずデータを共通鍵で暗号化します。次に、受信者の公開鍵でデータを暗号化するために使った鍵情報（共通鍵）を暗号化し、暗号化したデータとともに受信者に送信します。受信者は、送信者から送られてきた鍵情報（共通鍵）を自分の秘密鍵を用いて復号し、復号された共通鍵を使って暗号化されたデータを復号します。

なお、暗号化の鍵情報（共通鍵）は通信（セション）のつど生成し、相手方の公開鍵を使って渡すので、セション鍵方式とも呼ばれます。



※ (暗)は暗号化されたデータを表す

ハイブリッド暗号方式

４．秘密分散

秘密分散は、RSA 暗号の開発者の一人である Adi Shamir が開発した、データを複数部分に分割し、それぞれの部分だけでは元のデータを復元できないようにすることで暗号化する方法です。分割されたデータを**電子割符**と呼びます。

５．秘密計算

秘密計算は、処理の過程での情報漏洩のリスクをなくすために、暗号化されたデータをそのまま処理する技術です。具体的には、秘密分散を施したデータを複数のサーバに送信して処理し結果を集約する**秘密分散方式**と、暗号化したデータをサーバに送り、その状態のままで処理し結果を復号する**準同型暗号方式**の２つがあります。

６．軽量暗号

軽量暗号は、リソースが限られたデバイスに実装するために開発された低コスト、低消費電力等の特徴を持つ暗号技術で、IoT におけるセキュリティ確保の手段となる技術です。

７．ストレージ暗号化とファイル暗号化

ストレージ暗号化は、ハードディスクや SSD などのストレージ上に専用の IC チップを搭載して、データ入力の際に暗号化して情報漏えいを防ぐ方法です。その結果、仮にストレージの盗難や紛失が発生しても、認証鍵がないとデータは解読できません。

また、**ファイル暗号化**は、アクセス権限を持たない利用者がファイルの閲覧や編集できないようにする方法です。

８．ハッシュ関数

データ（メッセージ）をそのサイズに関わらず 128 から 512 ビット程度の一定のサイズに変換する関数を**ハッシュ関数**と呼び、ハッシュ関数によって演算した結果を**ハッシュ値**（**メッセージダイジェスト**）と呼びます。

ハッシュ関数から得られたハッシュ値は、異なるデータが同じ値になることがほとんどありません。

したがって、ハッシュ値が一致するデータを発見することは困難です。これをハッシュ関数の**衝突発見困難性**と呼びます。また、あるデータのハッシュ値が与えられたとき、そのハッシュ値と一致する別のデータを発見することは困難です。これをハッシュ関数の**第二原像発見困難性**と呼びます。そのため、送信者はデータと共にハッシュ値を送信し、受信者は受け取ったデータからハッシュ値を生成し、これと送信者から受け取ったハッシュ値との一致を確認することで、データが改ざんされていないこと（**データの完全性**）を確認できます。これを**メッセージ認証**と呼びます。

また、ハッシュ値から元のデータを求めることは計算量的に困難です。これをハッシュ関数の**原像計算困難性**（**一方向性**）と呼びます。そのため、サーバにパスワードのハッシュ値を保存しておき、利用者がアクセスする際は入力されたパスワードをハッシュ関数で変換して保存されているハッシュ値と比較して一致すればアクセスを許可することで、仮にサーバに保存されているパスワードのハッシュ値が盗難にあっても、なりすましを防止できます。これを**送信者認証**と呼びます。

代表的なハッシュ関数には、MD5（Message Digest 5）、SHA-1（Secure Hash Algorithm-1）、SHA-2（SHA-224、**SHA-256**、HA-384、SHA-512 の総称）があります。

MD5 は、RSA 暗号の開発者の一人、Ronald Rivest らによって開発されたアルゴリズムで、元のデータから 128 ビットのハッシュ値を生成します。デジタル署名などさまざまな場面で用いられていますが、ある条件下ではハッシュ値の衝突を意図的に起こすことができるという脆弱性が見つかっています。

SHA-1 は、アメリカの国家安全保障局（NSA：National Security Agency）によって開発され、NIST によってアメリカ政府標準のハッシュ関数に採用されたアルゴリズムで、2^{64} 以下の長さの元のデータから 160 ビットのハッシュ値を生成します。デジタル署名などさまざまな場面で用いられていましたが、MD5 と同様の脆弱性が指摘されたため、2011 年以降、2^{64} 以下の長さの元のデータから 256 ビットのハッシュ値を生成する **SHA-2** に移行しました。

さらに NSA が SHA-2 の後継として公募し 2015 年に正式に公表されたアルゴリズムが SHA-3 です。なお、**SHA-3** はそれまでのアルゴリズムとは全く異なるもので、任意の長さのデータからハッシュ値を生成します。

例題 1-A6　令和5年度春午前Ⅱ　問4　[出題頻度：★★★]

ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256 の衝突発見困難性を示す，ハッシュ値が一致する二つの元のメッセージの発見に要する最大の計算量は，256 の 2 乗である。
イ　SHA-256 の衝突発見困難性を示す，ハッシュ値の元のメッセージの発見に要する最大の計算量は，2 の 256 乗である。
ウ　衝突発見困難性とは，ハッシュ値が与えられたときに，元のメッセージの発見に要する計算量が大きいことによる，発見の困難性のことである。
エ　衝突発見困難性とは，ハッシュ値が一致する二つのメッセージの発見に要する計算量が大きいことによる，発見の困難性のことである。

ハッシュ値が大きいほどが、衝突発見困難性は大きくなります。
ア　SHA-256 は 256 個のハッシュ値を出力するので、ハッシュ値が一致する 2 つのメッセージの発見に要する最大の計算量は、256÷2 ＝128 から、2 の 128 乗です。
イ　ハッシュ値の元のメッセージの発見に要する最大の計算量は 2 の 256 乗とは限らず、発見できないこともあります。
ウ　ハッシュ関数の性質の一つである原像計算困難性に関する記述です。

解答－エ

別冊演習ドリル　1-A5～A8

９．無線LANにおける暗号化方式

無線 LAN では、盗聴の危険に備えて、暗号化することは必須です。暗号化の方式には、暗号アルゴリズムに共通鍵暗号方式の RC４を用いた **WEP**、無線 LAN の認証規格である IEEE802.1X の規格に沿った利用者認証や暗号化プロトコルに TKIP（Temporal Key Integrity Protocol）を採用することで WEP の脆弱性を改善した **WPA**（Wi-Fi Protected Access）、暗号アルゴリズムに AES を用いた **WPA2**、WPA2 で見つかった脆弱性を排除した **WPA3** などがあります。

WPA2 には、WPA2-Enterprise（企業用）と WPA2-Personal（個人用）の２つの規格があります。**WPA2-Enterprise** は、RADIUS などの認証サーバを利用できる環境で、認証サーバから動的に配布される暗号化鍵を用いて認証を行います。これに対して、**WPA2-Personal** は、利用者が限定された無線 LAN での使用を前提に、アクセスポイントと端末間で事前に共通鍵（Pre-Shared Key)を共有し、その事前共有鍵と SSID によって認証を行います。WPA2-Personal は、**WPA2-PSK** とも呼ばれています。

また WPA3 にも、認証サーバから動的に配布される暗号化鍵を用いて認証を行う **WPA3-Enterprise**（企業用）と、端末に設定された事前共通鍵によって認証を行う **WPA3-Personal**（個人用）の２つの規格があります。

例題 1-A7　令和5年度春午前Ⅱ　問14　[出題頻度：★★★]

無線 LAN の暗号化通信を実装するための規格に関する記述のうち，適切なものはどれか。

ア　EAP は，クライアント PC とアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実装するための規格である。
イ　RADIUS は，クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実装するための規格である。
ウ　SSID は，クライアント PC で利用する秘密鍵であり，公開鍵暗号方式による暗号化通信を実装するための規格で規定されている。
エ　WPA3-Enterprise は，IEEE802.1X の規格に沿った利用者認証及び動的に配布される暗号化鍵を用いた暗号化通信を実装するための規格である。

ア　EAP（Extensible Authentication Protocol：拡張認証プロトコル）は、デジタル証明書を使用した認証方式です。
イ　RADIUS は、無線 LAN や VPN 接続などで利用され、利用者を認証するためのシステムです。
ウ　SSID は、無線 LAN において接続先のネットワークを識別するための ID です。

解答－エ

別冊演習ドリル　1-A9～A11

１０．暗号アルゴリズムの危殆化

暗号の安全性とは、暗号化されたデータが第三者によって解読されないことです。

一般に、暗号化鍵のビット数が大きいほど、解読のための処理時間も長くなり、安全性は高まります。これを**暗号強度**（ビットセキュリティ）と呼びます。

危殆化とは、「危険な状態になる」という意味で、コンピュータの処理能力の向上や暗号解読技術の進歩は、既存の**暗号アルゴリズムの危殆化**を招いています。これを防ぎ無条件安全性を確保する暗号技術に、量子力学の理論をもとにした**量子暗号**（Quantum Cryptography）があります。さらに、将来的に量子コンピュータを用いた攻撃に対しても、安全性を保つことができる暗号方式を**耐量子暗号**（**PQC**（Post-Quantum Cryptography：耐量子計算機暗号））と呼びます。

なお、無限の処理能力をもつコンピュータを用いても解読できないことを**情報量的安全性**と呼びます。１回ごとに暗号化鍵を使い捨てる**ワンタイムパッド**は情報量的安全性をもつ暗号方式です。

また、現有するコンピュータの処理能力をすべて費やしても解読までに十分な時間が必要であることを**計算量的安全性**と呼びます。多くの暗号方式は計算量的安全性に基づくものです。

例題 1-A8　令和4年度春午前Ⅱ　問6　[出題頻度：★☆☆]

量子暗号の特徴として，適切なものはどれか。

ア　暗号化と復号の処理を，量子コンピュータを用いて瞬時に行うことができるので，従来のコンピュータでの処理に比べて大量のデータの秘匿を短時間で実現できる。

イ　共通鍵暗号方式であり，従来の情報の取扱量の最小単位であるビットの代わりに量子ビットを用いることによって，瞬時のデータ送受信が実現できる。

ウ　量子雑音を用いて疑似乱数を発生させて共通鍵を生成し，公開鍵暗号方式で共有することによって，解読が困難な秘匿通信が実現できる。

エ　量子通信路を用いて安全に共有した乱数列を使い捨ての暗号鍵として用いることによって，原理的に第三者に解読されない秘匿通信が実現できる。

ア　量子暗号は、量子コンピュータを用いるのではなく量子力学的粒子を用いて暗号化と復号に用いる共通鍵を作成し、暗号通信を行います。

イ　データの送受信は従来通りビットで行い、共通鍵（量子鍵）の配送は微弱な粒子である光子を用います。

ウ　共通鍵は公開鍵暗号方式で共有されるのではなく光子で共有されます。

解答－エ

別冊演習ドリル　1-A12，A13

１１．ゼロ知識証明

ゼロ知識証明（ZKP：Zero-Knowledge Proof）は、自分が持つ情報を何も与えずに、真実であることを証明する方法です。

例えば、公開鍵暗号を利用したデジタル署名では、デジタル署名に利用した秘密鍵は明らかにせずに署名は真実であることを証明しています。また、ハッシュ関数を利用したパスワード認証では、パスワード自体は明らかにせずに使用したパスワードは真実であることを証明しています。

なお、取引履歴などのデータとハッシュ値の組みを順次つなげて記録した分散型台帳をネットワーク上の多数のコンピュータで同期して保有し、管理することによって、一部の台帳で取引データが改ざんされても、取引データの完全性と可用性が確保されることを特徴とする技術である**ブロックチェーン**は、暗号資産を支える技術として用いられていますが、ブロックチェーン上に登録されたデータは全て公開されているため透明性が非常に高いという性質があります。企業や金融機関は個人情報を守ることが法律上で規定されているため、ブロックチェーンに匿名性を与える方法としてゼロ知識証明が注目されています。

例題 1-A9　令和4年度秋午前Ⅱ　問12［出題頻度：★☆☆］

ブロックチェーンに関する記述のうち，適切なものはどれか。

ア　RADIUS を必須の技術として，参加者の利用者認証を一元管理するために利用する。
イ　SPF を必須の技術として，参加者間で電子メールを送受信するときに送信元の真正性を確認するために利用する。
ウ　楕円曲線暗号を必須の技術として，参加者間の P2P（Peer to Peer）通信を暗号化するために利用する。
エ　ハッシュ関数を必須の技術として，参加者がデータの改ざんを検出するために利用する。

ブロックチェーンは、取引履歴などのデータとハッシュ値の組みを順次つなげて記録した分散型台帳を、ネットワーク上の多数のコンピュータで同期して保有し、管理することによって、一部の台帳で取引データが改ざんされても、取引データの完全性と可用性が確保されることを特徴とする技術です。そのため、ハッシュ関数の強度が台帳の堅牢性に直結します。

解答－エ

１２．CRYPTREC 暗号リスト

CRYPTREC 暗号リストは、総務省と経済産業省が共同で運営する暗号技術検討会及び関連委員会（**CRYPTREC**）が、安全性と実装性能が確認された暗号技術のうち、電子政府の調達時に利用することを推奨する暗号技術のリストで、推奨候補暗号リスト、電子政府推奨暗号リスト及び運用監視暗号リストという区分から構成されています。

推奨候補暗号リストは、CRYPTREC によって安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性がある暗号技術のリストです。

電子政府推奨暗号リストは、推奨候補暗号リストのうち、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストです。

運用監視暗号リストは、実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリストです。

電子政府推奨暗号リストに掲載されているアルゴリズムには次のようなものがあります。

①共通鍵暗号方式	AES、3-key Triple DES、Camellia など
②公開鍵暗号方式	RSA-PSS、DSA、ECDSA（楕円 DSA）など
③ハッシュ関数	SHA-256、SHA-384、SHA-512
④暗号利用モード	CBC、OFB など

例題 1-A10　令和4年度春午前Ⅱ　問10　[出題頻度：★★★]

CRYPTREC の主な活動内容はどれか。

ア　暗号技術の技術的検討並びに国際競争力の向上及び運用面での安全性向上に関する検討を行う。
イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ政策の推進に係る企画などを行う。
ウ　組織の情報セキュリティマネジメントシステムを評価して認証する制度を運用する。
エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

イ　内閣官房情報セキュリティセンターの活動内容です。
ウ　情報マネジメントシステム推進センタの活動内容です。
エ　JCMVP（Japan Cryptographic Module Validation Program）の活動内容です。

解答－ア

別冊演習ドリル　1-A14, A15

１３．FISC 安全対策基準

FISC（The Center for Financial Industry Information Systems：公益財団法人金融情報システムセンタ）は、日本国内の金融システムの安全性向上を目的に、銀行、保険、証券、クレジット会社などの金融機関とコンピュータメーカや通信会社等の出資により大蔵省（当時）の外郭団体として 1984 年 11 月に設立された機関で、現在は金融庁の所管となっています。

FISC 安全対策基準は、金融機関がシステムを安全に運用するために従うべき指針やガイドラインがまとめられたもので、「設備基準」、「運用基準」、「技術基準」の３つから構成されています。

なお、CRYPTREC 暗号リストの要件を満たす暗号化技術の利用が、「技術基準」において求められています。

１４．FIPS PUB 140

FIPS PUB 140（Federal Information Processing Standardization 140：連邦情報処理標準 140）は、米国政府職員が使用するすべてのソフトウェアに必要とされる暗号モジュールのセキュリティ要件を定義したものです。最新版は **FIPS PUB 140-3** です。

FIPS PUB 140 の認定要件を満たしたアルゴリズムには次のようなものがあります。

①共通鍵暗号方式　　AES、DES、Triple-DES など
②公開鍵暗号方式　　RSA、DSA、ECDSA（楕円 DSA）など
③ハッシュ関数　　SHA-1、SHA-256、SHA-384、SHA-512、SHA-224 など

なお、コンピュータの処理能力の向上や暗号解読技術の進歩により既存の暗号アルゴリズムの危殆化が問題となっており、2011 年以降は RSA-2048 及び SHA-256 の使用を求めています。

例題 1-A11　令和3年度秋午前Ⅱ　問7　[出題頻度：★★★]

FIPS PUB 140-3 はどれか。

ア　暗号モジュールのセキュリティ要求事項
イ　情報セキュリティマネジメントシステムの要求事項
ウ　ディジタル証明書や証明書失効リストの技術仕様
エ　無線 LAN セキュリティの技術仕様

イ　JIS Q 27001 の記述内容です。
ウ　ITU-T X.509 の記述内容です。
エ　IEEE 802.11i の記述内容です。

解答－ア

例題 1-B1　　平成27年度秋午後Ⅱ　問2　[出題頻度：★☆☆]

データの取扱いに関する次の記述を読んで，設問１～６に答えよ。

Ｖ社は，CM，プロモーションビデオなどのコンテンツを受託制作する従業員数 500 名の会社である。従業員はコンテンツの素材撮影のために国内外に出張する機会が多い。Ｖ社は，コンテンツの制作の一部を他の事業者に委託している。委託先事業者（以下，委託先という）には個人で事業を行うデザイナやクリエイタも多い。

コンテンツの受託制作では，必要なデータを顧客から受け取り，その全部又は一部を委託先と共有して作業を進める場合がある。受け取ったデータだけでなく，当該データから派生した中間データ，及び，撮影又は作成された素材も含めて，適切な保護が必要である。

Ｖ社では，従業員には，業務に応じてデスクトップPC（以下，DPCという）又はノートPC（以下，NPC という）を貸与している。従業員の識別と認証に必要な利用者情報は，ディレクトリサーバ（以下，Ｄサーバという）で管理している。Ｄサーバは IT 部が運用している。

〔オンラインストレージサービスの導入決定〕

Ｖ社では，業務効率の向上のために，クラウドベースのオンラインストレージの導入を決定し，IT 部のＭ部長を導入責任者に任命した。オンラインストレージの用途は，次のとおりである。

- 出張者と内勤者の間で，サイズが大きいデータを共有する。
- 委託先とＶ社の間で，データを共有する。
- デモやその他の目的のためにデータを取引先に送信する。
- NPC などにプレゼンテーション資料を配布する。

Ｍ部長は，IT 部内のチームに複数のオンラインストレージサービスを比較検討させた結果，Ｘ社のＱサービスを採用することにした。

〔Ｑサービスの概要〕

Ｑサービスの利用者は，インターネット経由で，Ｑサービスに任意のファイルを保管できる。Ｑサービスの概要を表１に，Ｑサービスの利用者用の専用アプリケーションソフトウェア（以下，同期アプリという）の概要を表２に，Ｖ社におけるＱサービスの利用方法案を図１に，それぞれ示す。

表１　Ｑサービスの概要

項目	説明
アカウント管理	・ 利用者に，個別のアカウントを割り当てる。 ・ 利用企業は，利用者のアカウントを自社で登録して管理するための機能（以下，管理者機能という）を利用できる。アカウントをもたない者も，Ｑサービスの一部の機能は利用できる（項目“ファイル管理”参照）。
管理者機能	・ 管理者は，アカウントの作成・停止・再開・廃止，パスワードの初期発行・再発行，ファイル及びフォルダへのアクセス履歴の閲覧，その他の管理のための機能を利用できる。
利用者識別・認証	・ 利用者 ID とパスワードを用いて利用者を識別・認証する。 ・ 利用者は，インタフェースを利用して，パスワードを変更できる。
ファイル管理	・ 各アカウントには，それぞれ専用のフォルダ（以下，ルートフォルダという）が与えられる。利用者が登録したファイルやフォルダは，ルートフォルダの下に配置される。 ・ 利用者は，インタフェースを利用して，次の機能を実行できる。 - ファイルの登録・更新・削除・取得・プロパティの閲覧 - フォルダの作成・削除・閲覧・プロパティの閲覧 - バックアップからのファイルの復元・取得・削除（補足説明１参照） - 他の利用者へのファイル又はフォルダのアクセス権の付与・変更（補足説明２参照） - ファイルにアクセスするための共有リンクの作成・削除（補足説明３参照） 【補足説明】 １．ファイルが更新又は削除された場合，元のファイルはバックアップとして保管される。利用者は，バックアップとして保管されたファイルのうち，バックアップから削除が行われていないものを，復元・取得できる。 ２．他の利用者に付与できる権限には“読み”と“読み書き”の２種類がある。“読み”は，ファイルの取得機能などの，ファイルやフォルダの変更を伴わない機能を利用する権限である。“読み書き”は“読み”の権限に加え，ファイルの更新機能などの，変更を伴う機能を利用する権限である。 ３．アカウントをもたない者にファイルを配布するための URL を“共有リンク”という。Web ブラウザで当該 URL にアクセスすると利用者認証なしにファイルを取得できる。 ４．アカウントが廃止されると，そのアカウントで登録したファイルとフォルダが削除される。
インタフェース	・ 同期アプリ，Web インタフェース，API の三つのインタフェースがある。 - 同期アプリの機能については，表２に概要をまとめる。 - Web インタフェースを用いる利用者は，Web ブラウザでＱサービスの Web サーバ（w.example.com）にアクセスし，Ｑサービスの各機能を利用する。 - API を用いて，Ｑサービスと連携するアプリケーションソフトウェアを開発できる。
暗号化	・ 同期アプリとＱサービス間の通信，及び Web ブラウザとＱサービスの Web インタフェース間の通信は，TLS で暗号化される。 ・ Ｑサービスは複数のサーバで構成されており，ファイルは，他の利用企業又は個人利用者のファイルと同じサーバに保管される場合がある。登録されたファイルは，暗号化して保管される。暗号鍵は，サーバごとに生成し，Ｑサービス内で管理する。利用者がＱサービスのインタフェースを利用してファイルにアクセスすると，Ｑサービスは，ファイルを復号した後に引き渡す。

注記　Ｑサービスでは，“利用者”とは，アカウントをもつ者だけを指す。

表２　同期アプリの概要

項目	説明
ファイル管理	・ 表１の項目“ファイル管理”の機能を提供する。
同期機能	・ 同期アプリは，利用者の PC のローカルディスク上に特別なフォルダ（以下，同期用フォルダという）を作成する。 ・ 同期用フォルダには，利用者のアカウントのルートフォルダと，当該利用者がアクセス権をもつ他の利用者のファイル及びフォルダの複製が作成され，これらはＱサービス上のそれぞれのフォルダ又はファイルと自動的に同期される。例えば，利用者が同期用フォルダ配下に複製されたファイルを更新した場合，更新内容は，Ｑサービスの該当ファイルにも適用される。また，更新されたファイルについて，他の利用者にアクセス権が付与されていた場合，他の利用者の PC の同期アプリがＱサービスの該当ファイルを同期用フォルダにコピーする。
同期管理	・ 同期機能について設定を行う機能を提供する。自動的な同期を行わない場合は，その旨を設定できる。 ・ 同期の状況を表示する。
その他	・ 同期アプリは，ＱサービスのＡサーバ（a.example.com）と通信し，各処理を行う。プロキシサーバを経由した通信もサポートしている。 ・ 同期アプリは，Ｘ社がインターネットで配布しており，誰でもダウンロードできる。

・ Ｑサービスの利用に関する社内の管理は IT 部が主管する。
・ IT 部は，業務上Ｑサービスの利用が必要なＶ社の従業員及び委託先の作業者に対してアカウントを作成する。

図１　Ｑサービスの利用方法案（抜粋）

〔Ｑサービスの試験導入〕

Ｍ部長は，Ｑサービスの導入に先だって，３か月間の試験導入をすることにした。オンラインストレージの利用が想定される部門の中から，試験導入への参加者を偏りなく選ぶことにし，最終的に 30 名の参加者を決定した。この中には，委託先の５名のクリエリタが含まれていた。試験導入では，次の項目を確認することにした。

・　機能は，利用目的に照らし，必要十分で使いやすいか。
・　管理は，シンプルで，実用に耐えるか。
・　セキュリティ及びその他の問題点がないか。

以降，Ｑサービスについては，Ｖ社が利用する部分だけに限定して述べる。

〔Qサービスの試験導入において表出した問題〕

試験導入の結果，機能及び管理については大きな問題は発見されなかった。しかし，セキュリティについては，同期アプリが，マルウェア感染を拡散させるという問題が認識された。

実際に発生した事件は次のとおりである。委託先のクリエイタが PC で編集していたファイルがマルウェアに感染した。そのことに気付かずにクリエイタが Web インタフェースを使って当該ファイルをQサービスに登録した結果，同ファイルにアクセス権をもつ複数の利用者の PC の同期アプリが，感染ファイルをQサービスから同期用フォルダにコピーした。本件では，それぞれの PC にインストールされていたウイルス対策ソフトが感染ファイルを検知したので，大事には至らなかった。しかし，V社では，事態を重く受け止め，対応について検討することになった。

〔Qサービス利用方法の見直し〕

M部長は，PC のウイルス対策ソフトだけではなく，複数の対策が必要だと考え，IT 部のUさんに，情報セキュリティ室のR主任の支援を受けて，マルウェア感染ファイルの拡散について対応を検討するように指示した。

Uさんは，検討を進め，専用のサーバ（以下，同期用 FS という）及び専用のディスク（以下，同期ディスクという）を介して，社内ネットワークに接続された PC とQサービス間でのファイルの交換を行う仕組みを提案した。そのネットワーク構成を図２に，ファイル交換の仕組みの概要を図３に，同期用 FS の機能の説明を図４に示す。

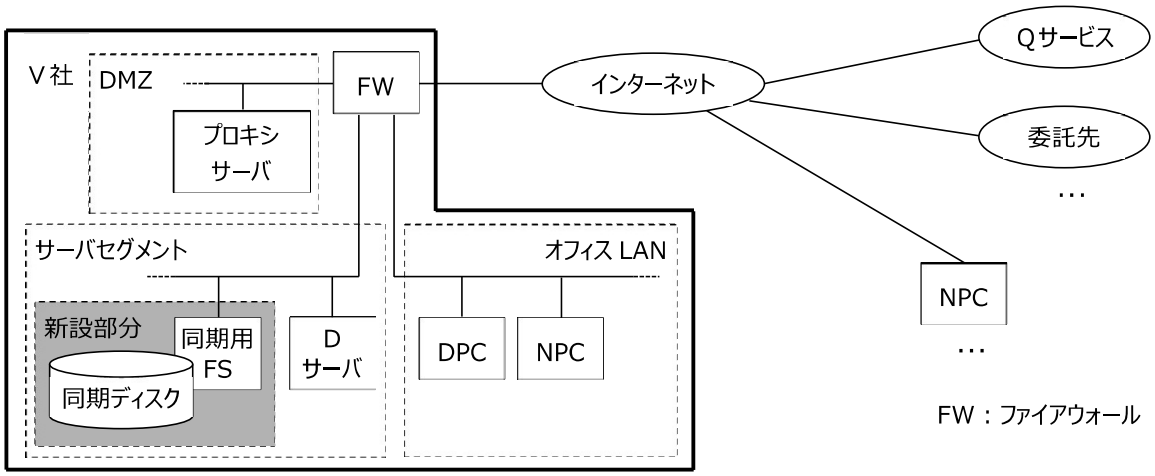


図２　ネットワーク構成

- 同期用 FS は，Qサービスに登録された利用者のアカウントのルートフォルダ及びその配下のフォルダ（以下，Qサービス利用者フォルダという）を監視し，新たに登録された又は更新されたファイルがある場合は，それを取得してマルウェアスキャンを行った後，同期ディスクに保管する。
- ①同期アプリの利用を禁止する。
- 同期用 FS へのアクセスは，FW によって，オフィス LAN からだけに限定する。

図３　ファイル交換の仕組みの概要

１．ファイルの同期

・ ルートフォルダの複製を同期用 FS 内の同期ディスクに保持し，ファイルを同期する。同期は次のように行う。

Ａ） Ｑサービス利用者フォルダにおいて，ファイルの登録又は更新があった場合は，当該ファイルを取得してマルウェアスキャンを行う。その結果，問題がなければ同期ディスクに反映する。マルウェアが検知されたら，Ｑサービス利用者フォルダにある当該ファイルを削除し，もし対応するファイルが同期ディスクに存在する場合はそれも削除する。登録・更新以外の変更があった場合は，同等の変更を同期ディスクに反映する。

Ｂ） 同期ディスクのファイルに変更があった場合は，Ｑサービス利用者フォルダにある対応するファイルに反映する。

２．フォルダの同期

・ Ｑサービス利用者フォルダに変更があった場合は，同期ディスクの対応するフォルダに反映する。

・ 同期ディスクのフォルダに変更があった場合は，対応するＱサービス利用者フォルダに反映する。

３．アカウントとアクセス制御

・ Ｄサーバに登録された従業員の利用者情報とＱサービスのアカウントの対応表をもつ。

・ 同期ディスクにアクセスがあった場合，Ｄサーバと連携して従業員を識別した後，前記の対応表を基に利用者のアカウントを判別する。この結果に基づいて，次の処理を許可する。

Ａ） 判別されたアカウントのＱサービス利用者フォルダ又はそこにあるファイルに対応する同期ディスクのフォルダ又はファイル：全ての処理

Ｂ） 他の利用者のファイル又はフォルダに対応する同期ディスクのファイル又はフォルダ：判別されたアカウントに付与された権限内の処理

４．補足事項

・ Ｑサービスに保管されたバックアップのファイルについて，同期用 FS は一切処理を行わない。

図４　同期用 FS の機能の説明（抜粋）

Ｕさんがこれらの検討結果をＭ部長に報告したところ，②試験導入において表出した問題を踏まえると，同期用 FS には，マルウェア対策に関して追加すべき機能があると指摘された。Ｕさんは追加機能を提案し，Ｍ部長は，Ｕさんの提案どおり対応を進めることを承認した。その後，Ｑサービスと同期用 FS の利用が，全社で開始された。

〔顧客からの要求〕

Ｖ社でＱサービスの利用を開始してから１年が経過した頃，重要な顧客であるＪ社から，情報セキュリティに関して新しい要求の通知があった。Ｊ社の別の委託先において，Ｊ社が開示した新製品に関する CAD データが漏えいするという事件が発生し，対策の一環として，Ｊ社が重要なデータを開示する全ての委託先に対して，新たな要求を課す方針になったとのことであった。Ｊ社からの要求を図５に示す。

Ｊ社が開示する全ての重要な情報（以下，Ｊ社重要データという）について，次の措置を行うこと
・業務上，必要最小限の者しかＪ社重要データにアクセスできないように管理する。
・Ｊ社重要データをインターネット上に送信する場合には，暗号化する。
・Ｊ社重要データを社外に保管する場合には，暗号化する。
・Ｊ社重要データを可搬型機器又は可搬型デバイスに保管する場合には，暗号化する。
・業務上不要となったＪ社重要データは，直ちに，Ｊ社に返却するか，削除する。
・何らかの事故が発生した場合に備え，非常時の連絡体制・手順を確立する。
・Ｊ社重要データについて，法令による保護が受けられるように，十分に配慮して管理する。
・Ｊ社から受託した業務の一部を再委託する場合は，当該委託先に対して本要求と同等の措置を求め，かつ，その実施について監督する。

図５　Ｊ社からの要求（概要）

次は，Ｊ社からの要求に関する，Ｍ部長とＵさんとの会話である。

Ｕさん：Ｊ社から受け取るデータの大半はＪ社重要データですが，当社は，Ｊ社の要求を満たしていないと思います。
Ｍ部長：お客様のデータの保護は最優先事項だ。最近，Ｊ社以外にも，複数のお客様から，データの取扱いについての問合せや要求が寄せられている。この機会に，当社の現状を調査し，必要なら見直すことにしよう。
Ｕさん：分かりました。ところで，法律の規定との関係はどうでしょう。お客様のデータは，［　a　］で規定されているの［　b　］に該当しますか。
Ｍ部長：［　a　］で規定されている［　b　］に該当するためには，当該データが，秘密として管理されていること，有用な情報であること，及び［　c　］こと，の三つの要件を満たす必要がある。秘密として管理されているというためには，その情報が，客観的に見て秘密として管理されている状態になっていなければならない。
Ｕさん：他の法令はどうでしょうか。
Ｍ部長：［　d　］の 235 条で規定されている窃盗罪は，他人の財物を窃取した場合に適用される。しかし，情報そのものは物ではなく，財物には当たらないので，適用は難しいという解釈があるようだ。思想又は感情を創作的に表現したと考えられるデータであれば，［　e　］の保護の対象となる。また，サーバなどの電子計算機に接続して行う不正行為に焦点を当てた［　f　］がある。ただし，［　f　］はネットワークを通じて行われる攻撃を対象としているので，攻撃対象の機器を直接操作するケースは対象外だ。
Ｕさん：ありがとうございます。教えていただいたことも参考に調査を進めます。

〔顧客データの取扱要件〕

Ｕさんは，受託業務で顧客から開示を受けた重要なデータ（以下，顧客データという）の取扱状況を調査し，Ｍ部長に報告した。Ｍ部長は，調査結果を見て，顧客データの取扱いについて改善が必要だと判断した。Ｍ部長は，Ｕさんに，Ｊ社の要求を満たすような顧客データの取扱要件及びその実装方法，並びにその他の必要な措置について検討して提案するように指示した。

Ｕさんは，業務上の必要性のある従業員だけがアクセスできる場所への顧客データの保管，及び顧客データを NPC 又はオンラインストレージに保管する場合の暗号化について検討した。

〔NPC のディスクの暗号化〕

Uさんは，顧客データの暗号化のため，NPC のディスクの暗号化，及びオンラインストレージに登録するデータの自動暗号化の導入を検討した。

Uさんが検討した，NPC のディスクの暗号化方式を表３に示す。

表３　NPC ディスクの暗号化方式

名称	説明
フルディスク暗号化方式	ディスク内の全ての領域を暗号化する方式。PC の全ディスクにこの方式を用いた場合，パスワードがないと，［　g　］を起動できない。起動後，データの保護は，PC の［　g　］が提供する機能に委ねられる。本方式に対応する製品の多くは，PC が休止モードになる際にメモリの内容を書き出すハイバネーション用ファイルの［　h　］に対応している。
仮想ディスク暗号化方式	コンテナと呼ぶ仮想的な入れ物を用いて暗号化する方式。コンテナは仮想ディスクとして機能する。コンテナ内にアクセスする場合，利用者の認証が行われる。認証に成功すると，一定の間，通常のディスクと同様に，コンテナにファイルやフォルダを保管したり取り出したりすることができる。データは暗号化された上でコンテナ内に保管される。コンテナは，PC のデータディスク，USB メモリなどに置かれる。スワップ領域やハイバネーション用ファイルには［　h　］されていない状態のデータが存在する可能性があるが，これらは保護されない。
ファイル・フォルダ暗号化方式	ファイル単位・フォルダ単位で暗号化する方式。暗号化されたデータは，一つのファイルになる。当該ファイルへのアクセス権があれば，鍵情報を知らなくても，格納されたファイルやフォルダの名称及び他の属性情報を取得できる場合がある。

Uさんは，検討した結果，フルディスク暗号化方式を採用することを提案した。

次は，暗号化製品に関する，UさんとR主任との会話である。

Uさん：幾つかの暗号化製品の説明書に“暗号の利用モード”や“CBC モード”という記述がありました。これは何でしょうか。

R主任：利用モードとは，ブロック暗号アルゴリズムを用いてブロック長よりも長いデータを暗号化する際に使われる技術のことだ。CBC モードは，よく使われる利用モードの一つだよ。

Uさん：利用モードは他にもあるのですか。

R主任：図６に代表的な暗号の利用モードがまとめられているので見てごらん。ブロック暗号アルゴリズムの利用時には，暗号化の目的や利用方法に合わせて，適切な利用モードを選ぶ必要がある。例えば，<u>③ディスクやファイルの暗号化に ECB モードをそのまま用いるのは，セキュリティ上の問題がある</u>。

利用モードによって，ランダムアクセス時の性能が大きく異なる場合もある。例えば，512 バイトの平文Ｐを，ブロック長が 128 ビットのブロック暗号アルゴリズムで暗号化した暗号文Ｃがあり，この暗号アルゴリズムでは平文と暗号文の長さは同じとする。平文Ｐにおいて 1,025 ビット目から始まる１ブロック分のデータを修正した場合，平文Ｐの修正に対応して暗号文Ｃを修正するためには，暗号化処理を，ＥＣＢ モードでは［　i　］回，ＣＢＣ モードでは［　j　］回実行しなければならない。

また，別の暗号文Ｃ’で，513 ビット目から始まる１ブロック分のデータを復号するためには，暗号化処理又はその逆処理を，ECB モードでは［　k　］回，CBC モードでは［　l　］回，OFB モードでは［　m　］回実行する必要がある。

複数ブロックの並列処理は，［　n　］の場合，暗号化時は不可能だが，復号時は可能だ。［　o　］の場合は，鍵ストリームに相当するデータを事前に計算することができる。

ただし，一部の利用モードは，特定の攻撃に弱いので注意が必要だ。

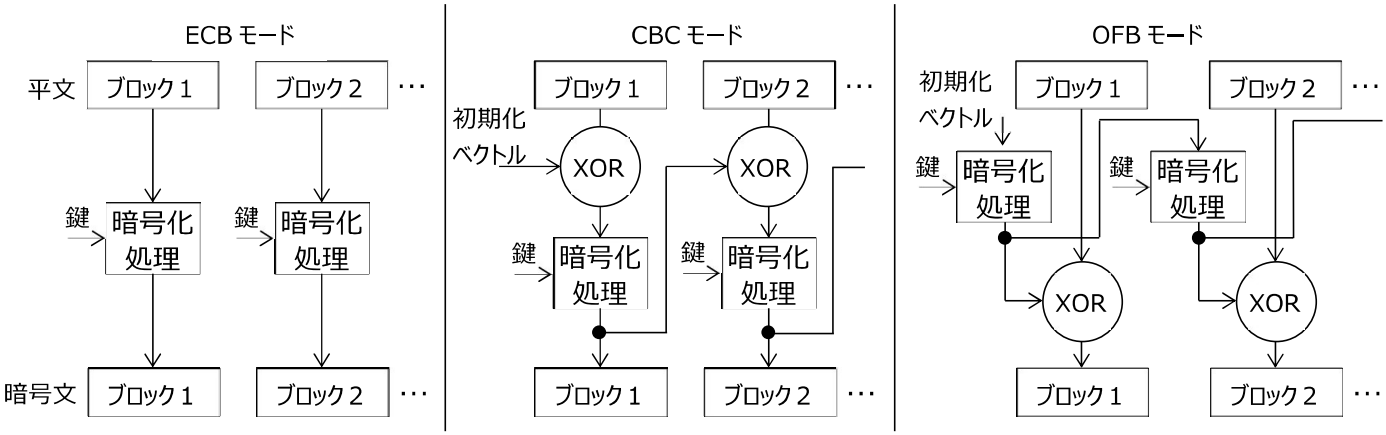


図６　代表的な暗号の利用モード

〔同期用 FS の機能拡張〕

表１に示したように，Ｑサービスは，元々，登録されたファイルを自動的に暗号化する機能をもつ。しかし，Ｑサービスの暗号化機能は，④Ｑサービスに対するクラッキングやＸ社自身のある種の行為に対して効果が期待できない場合があり，これを補完する措置が必要と考えられた。一方，Ｖ社内では，Ｑサービスの有益性が高く評価されており，継続利用したい。そこで，Ｕさんは，同期用 FS の機能を拡張し，Ｑサービスに登録する一部のファイルを自動的に暗号化する措置を提案した。同期用 FS の拡張機能を図７に，ファイルの暗号化と復号のフローを図８に，それぞれ示す。

１．機密フォルダと暗号化フォルダの定義・導入

・利用者が同期ディスク中のフォルダに“_[c1]”で始まる名称を付けると，そのフォルダは機密フォルダになる。機密フォルダの同期先となるＱサービス上のフォルダを暗号化フォルダという。

２．機密フォルダにアクセスしたときの処理

・利用者が機密フォルダにファイルを登録した場合又は機密フォルダ内のファイルを更新した場合，同期用 FS はファイルを暗号化した上で，Ｑサービス上の暗号化フォルダに登録するか，暗号化フォルダ内のファイルを更新する。

３．Web インタフェースを用いて暗号化フォルダにアクセスしたときの処理

・利用者は，暗号化フォルダにファイルを登録する場合又は暗号化フォルダ内のファイルを更新する場合，事前に，指定された鍵と暗号化ソフトを用いてファイルを暗号化する（“４．暗号化のアルゴリズムと鍵”参照）。同期用 FS は，暗号化されたファイルを取得してマルウェアスキャンを行い，マルウェアが検知されなければ，復号した上で，同期ディスク中の対応する機密フォルダに配置する。暗号化フォルダに平文のファイルが登録された場合又は平文のファイルで既存のファイルが更新された場合，同期用 FS は当該ファイルを暗号化して更新した後，利用者に警告メールを送信する。また，暗号化された当該ファイルは，初めから正しく暗号化されたファイルで更新された場合と同様の手続で，同期ディスクに同期される。

・利用者は，暗号化フォルダからファイルを取得した場合，指定された鍵と暗号化ソフトを用いて復号した上で利用する。

４．暗号化のアルゴリズムと鍵

・暗号化のアルゴリズムは鍵長 128 ビットの AES，暗号の利用モードは CBC モードとする。

・同期用 FS は，機密フォルダ又は暗号化フォルダが作成された際に，作成されたフォルダごとに数字 16 文字のパスワードをランダムに生成し，さらにそれを基に鍵を生成する。⑤生成された鍵は，当該フォルダ内に

登録されるファイルの暗号化と復号だけに利用される。ただし，名称が“_[c1]”で始まるサブフォルダがある場合は，そのフォルダを別の機密フォルダ又は暗号化フォルダとみなし，新しいパスワード及び鍵を割り当てる。
・ 同期用 FS は，生成したパスワードを，当該フォルダの利用者に電子メールで通知する。
・ 暗号化ソフトは，暗号化と復号の機能をもつ PC 用ソフトウェアであり，利用者に配布される。

図 7　同期用 FS の拡張機能（概要）

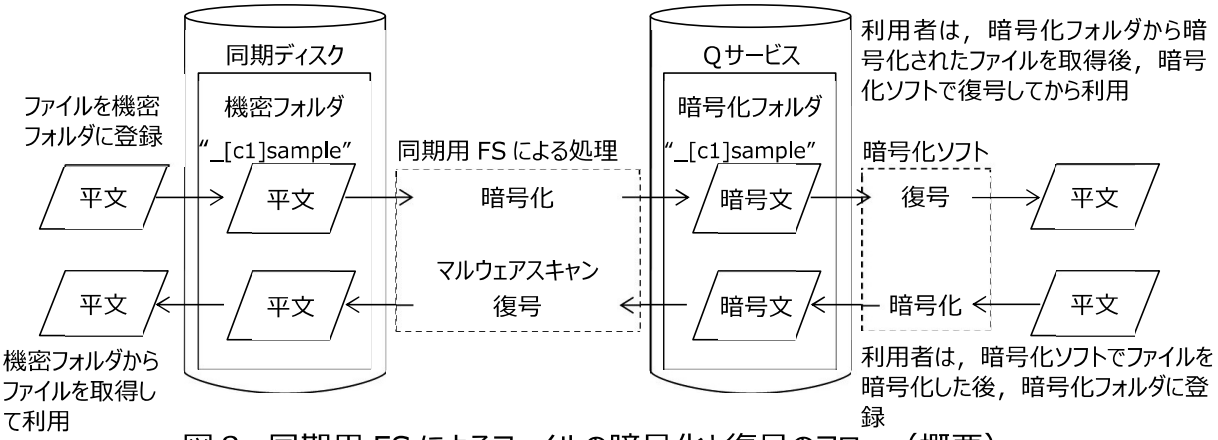


図 8　同期用 FS によるファイルの暗号化と復号のフロー（概要）

Uさんは，図 7 の方法では，⑥暗号化対象ファイルに関係する情報の一部は秘匿されないが，セキュリティ上容認できると考えた。

Uさんが図 7 のパスワードについて R 主任に相談したところ，R 主任は問題を指摘した。R 主任は，図 9 を示し，数字 16 文字のパスワードの場合の数は，英数字［　p　］文字のパスワードの場合の数より小さいことを説明した。また，この場合の数は，最近のコンピュータの能力向上を考慮すると，いつまでも安全とはいえないと指摘した。Uさんは，R 主任の指摘を受けて，パスワードの構成を見直した。

英数字 x 文字のパスワードについて，その場合の数が，数字 16 文字のパスワードの場合の数より大きくなる最小の x を考える。ただし，大文字と小文字は区別する。

次の式から，求めるパスワードの文字数 x は［　p　］となる。

［　q　］$^{x} > 10^{16}$

$$x > \frac{16\log_{10}10}{\log_{10}[\ \ r\ \ ] + \log_{10}[\ \ s\ \ ]} = [\ \ t\ \ ]$$

参考　$\log_{10}2 \fallingdotseq 0.301$，$\log_{10}3 \fallingdotseq 0.477$，$\log_{10}13 \fallingdotseq 1.114$，$\log_{10}31 \fallingdotseq 1.491$

図 9　パスワードの検討

〔レビューと修正〕

Uさんは，IT 部と情報セキュリティ室のメンバ（以下，WG という）に，顧客データの取扱要件とその実装方法の案についてのレビューを依頼した。レビューの結果，オンラインストレージについて，次の点が指摘された。

・ ⑦マルウェア感染ファイルの拡散防止対策が不十分である。
・ ⑧暗号化フォルダに登録された一部のファイルが，平文のままQサービスに保管され続ける場合がある。

Uさんは，これらの指摘について検討し，修正案を作成した。修正案について，再度 WG でレビューした結果，指摘は解決されていることが確認された。

〔M部長の最終確認〕

Uさんは，修正案及びその他の必要な措置について，M部長に報告した。

M部長：修正案は技術的に妥当であり，効果がある。当社は委託先との契約の中で，顧客データについて目的外利用の禁止と適切な管理を委託先に要求している。だが，事故の発生を防ぐ点で十分だろうか。

Uさん：当社の現状について調査した結果，委託先の管理が不十分だったので，IPA が公表している“組織における内部不正防止ガイドライン”を参考にして，技術的対策とは別に⑨対策をまとめました。

M部長はUさんの提案を承認し，提案どおり見直しが行われることになった。

設問１〔Ｑサービス利用方法の見直し〕について，(1)，(2)に答えよ。

(1) 図３中の下線①について，この措置は，マルウェア感染ファイルの拡散がどのように起こることを想定したものか。40 字以内で具体的に述べよ。

(2) 本文中の下線②について，同期用 FS にどのような機能を追加すればよいか。追加機能の内容を，30 字以内で具体的に述べよ。

設問２〔顧客からの要求〕について，(1)，(2)に答えよ。

(1) 本文中の［ a ］，［ d ］～［ f ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア 刑法	イ 個人情報保護法
ウ サイバーセキュリティ基本法	エ 情報公開法
オ 著作権法	カ 犯罪収益移転防止法
キ 不正アクセス禁止法	ク 不正競争防止法
ケ マイナンバー法	コ 民法

(2) 本文中の［ b ］，［ c ］に入れる適切な字句を，［ b ］は５字以内で，［ c ］は 15 字以内でそれぞれ答えよ。

設問３〔NPC のディスクの暗号化〕について，(1)～(4)に答えよ。

(1) 表３中の［ g ］，［ h ］に入れる適切な字句をそれぞれ５字以内で答えよ。

(2) 本文中の下線③について，セキュリティ上の問題を，45 字以内で具体的に述べよ。

(3) 本文中の［ i ］～［ m ］に入れる適切な数値を答えよ。

(4) 本文中の［ n ］，［ o ］に入れる適切な暗号の利用モードを，図６中の三つの利用モードの中から選んで答えよ。

設問４〔同期用 FS の機能拡張〕について，(1)～(4)に答えよ。

(1) 本文中の下線④について，Ｑサービスの暗号化機能の効果が期待できないのは，Ｑサービスのどのような仕様によるものか。30 字以内で述べよ。

(2) 図７中の下線⑤について，別の方法として，一つの鍵を全ての機密フォルダで共有して利用する方法がある。これらの二つの方法を比較した場合に，下線⑤の方法が優れている点は何か。35 字以内で具体的に述べよ。

(3) 本文中の下線⑥について，暗号化対象ファイルに関係するどのような情報が秘匿されないか。二つ挙げ，それぞれ 15 字以内で答えよ。

(4) 本文中又は図９中の［ p ］～［ t ］に入れる適切な数値を答えよ。［ p ］～［ s ］は整数で，［ t ］は小数第２位を四捨五入して，小数第１位まで求めよ。

設問５〔レビューと修正〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑦について，指摘に対応するには，図７の拡張機能をどのように修正すればよいか。修正内容を，50 字以内で具体的に述べよ。

(2) 本文中の下線⑧について，どのような場合にファイルが平文のままＱサービスに保管され続けるのか。35 字以内で具体的に述べよ。また，この状況を防ぐには，同期用 FS の拡張機能にどのような修正を行えばよいか。修正内容を 30 字以内で述べよ。

設問６　本文中の下線⑨について，Ｕさんがまとめた対策を，35 字以内で述べよ。

《解答》

設問１　(1) マルウェア感染ファイルが複数の利用者の同期用フォルダ間で自動同期される。
　　(2) マルウェア感染ファイルの発見時に利用者に警告を発する機能
設問２　(1) ａ：ク
　　ｂ：ア
　　ｅ：オ
　　ｆ：キ
　　(2) ｂ：営業秘密
　　ｃ：公然と知られていない
設問３　(1) ｇ：OS
　　ｈ：暗号化
　　(2) 平文が同じブロックは同じ暗号文になるので，暗号文から平文を推測されやすい。
　　(3) ｉ：１
　　ｊ：24
　　ｋ：１
　　ｌ：１
　　ｍ：５
　　(4) ｎ：CBCモード
　　ｏ：OFBモード
設問４　(1) 鍵は，サーバごとに生成し，Ｑサービス内で管理される。
　　(2) 鍵が危殆化しても，当該鍵が利用されるフォルダ以外には影響がない。
　　(3) ①・ファイルの名称
　　②・おおよそのファイルサイズ
　　(4) ｐ：９
　　ｑ：62
　　ｒ：２
　　ｓ：31　（ｒとｓは順不同）
　　ｔ：8.9
設問５　(1) 暗号化フォルダに登録されたファイルは，復号した後で，マルウェアスキャンを行うようにする。
　　(2) 場合：利用者が，暗号化していないファイルをWebブラウザで登録した場合
　　修正内容：暗号化されていないバックアップのファイルを自動で削除する。
設問６　委託先のデータ管理の実態を監査によって把握して監督する。

《解説》
設問１
(1) 表２の「同期機能」の説明に、「同期アプリは，利用者のPCのローカルディスク上に特別なフォルダ（以下，同期用フォルダという）を作成する。同期用フォルダには，利用者のアカウントのルートフォルダと，当該利用者がアクセス権をもつ他の利用者のファイル及びフォルダの複製が作成され，これらはＱサービス上のそれぞれのフォルダ又はファイルと自動的に同期される。」と記述されています。
〔Ｑサービスの試験導入において表出した問題〕に、「試験導入の結果～（省略）～同期アプリが，マルウェア感染を拡散させるという問題が認識された。実際に発生した事件は～（省略）～ファイルがマルウェアに感染した。～（省略）～複数の利用者のPCの同期アプリが，感染ファイルをＱサービスから同期用フォルダにコピーした。」と記述されています。
したがって、「マルウェア感染ファイルが複数の利用者の同期用フォルダ間で自動同期される。」のを防

ぐために、同期アプリの利用を禁止します。

(2)〔Qサービスの試験導入において表出した問題〕に、「実際に発生した事件は次のとおりである。委託先のクリエイタがPCで編集していたファイルがマルウェアに感染した。そのことに気付かずにクリエイタがWebインタフェースを使って当該ファイルをQサービスに登録した結果」と記述されており、マルウェアに感染したことに気付かなかったことが感染拡大につながったと考えられます。

したがって、図4には、「マルウェア感染ファイルの発見時に利用者に警告を発する機能」がないので追加します。

設問2

(1) 空欄a　「M部長：［　a　］で規定されている～（省略）～当該データが，秘密として管理されていること，有用な情報であること，及び～（省略）～の三つの要件を満たす必要がある。」という記述から、「ク　不正競争防止法」です。

空欄d　「M部長：［　d　］の235条で規定されている窃盗罪」という記述から、「ア　刑法」です。

空欄e　「思想又は感情を創作的に表現したと考えられるデータであれば，［　e　］の保護の対象」という記述から、「オ　著作権法」です。

空欄f　「また，サーバなどの電子計算機に接続して行う不正行為に焦点を当てた［　f　］がある。」という記述から、「キ　不正アクセス禁止法」です。

(2) 空欄b　不正競争防止法の保護の対象となるデータは「営業秘密」です。

空欄c　正競争防止法における営業秘密とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の秘密であって、「公然と知られていない」ものをいいます。

設問3

(1) 空欄g　「パスワードがないと［　g　］を起動できない。起動後，データの保護は，PC の［　g　］が提供する機能に委ねられる。」という記述から、「OS」です。

空欄h　「仮想ディスク暗号化方式」の説明の「［　h　］されていない状態のデータが存在する可能性があるが，これらは保護されない。」という記述から、「暗号化」です。

(2) 図6の記述から、ECB モードでは、平文ブロックごとに同じ暗号化処理を行っていると分かります。したがって、「平文が同じブロックは同じ暗号文になるので，暗号文から平文を推測されやすい」というセキュリティ上の問題があります。

(3) 空欄iと空欄jの前の「512 バイトの平文Pを，ブロック長が 128 ビットのブロック暗号アルゴリズムで暗号化した暗号文Cがあり」という記述から、ブロック数を計算すると次のようになります。

512 バイト÷128 ビット（＝16 バイト）＝32 ブロック

次に、「平文Pにおいて 1,025 ビット目から始まる1ブロック分のデータ」が先頭から何ブロック目になるか計算すると次のようになります。

1,025 ビット÷128 ビット≒9（切上げ）ブロック

空欄i　図6の記述では、ECB モードでは暗号化対象の平文Pのブロックごとに暗号化して暗号文Cのブロックを生成しています。したがって、平文Pの9ブロック目を修正した場合には対応する暗号文Cの9ブロック目を修正する必要があるので、暗号化処理を1回実行しなければなりません。

空欄j　図6の記述では、CBC モードでは暗号化対象の平文Pのブロックと一つ前の暗号文Cのブロックの XOR を暗号化して暗号文Cのブロックを生成しています。したがって、平文Pの9ブロック目を修正した場合には対応する暗号文Cの9ブロック目以降をすべて修正する必要があるので、暗号化処理を 32－9＋1＝24 回実行しなければなりません。

次に、「暗号文C'で，513 ビット目から始まる1ブロック分のデータ」が先頭から何ブロック目になるか計算すると次のようになります。

513 ビット÷128 ビット≒５（切上げ）ブロック

空欄ｋ　ECB モードでは、ブロックごとに暗号化処理の逆処理を行えば良いので、暗号文Ｃ′の５ブロック目を復号するには、暗号化処理の逆処理を１回実行します。

空欄ｌ　CBC モードでは、復号対象の暗号文Ｃ′に対して暗号化処理の逆処理を行った結果と一つ前の暗号文のブロックの XOR を取れば良いので、暗号文Ｃ′の５ブロック目を復号するには、暗号化処理の逆処理を１回実行します。

空欄m　図６の記述では、OFB モードではブロックの数だけ暗号化処理を繰り返した初期化ベクトルと平文Ｐのブロックの XOR を暗号文Ｐとしています。したがって、暗号文Ｃ′の５ブロック目を復号するには、ブロックの数である５回暗号化処理を繰り返した初期化ベクトルと暗号文Ｃ′の XOR を取れば良いので、暗号化処理を５回実行します。

(4) 空欄ｎ　(3)の解説の記述から分かるように、複数ブロックの並行処理が「暗号化時は不可能だが，復号時は可能」なモードは CBC モードです。なお、ECB モードでは暗号化時も復号時も複数ブロックの並行処理が可能です。

空欄ｏ　「鍵ストリームに相当するデータ」とは、CBC モードや OFB モードで平文ブロックと XOR を取るデータのことです。(3)の解説の記述から分かるようにそのデータの生成に CBC モードでは平文ブロックが使われていますが、OFB モードでは初期化ベクトルが使われています。したがって、OFB モードでは鍵ストリームに相当するデータを事前に計算することができます。

設問４

(1) 表１の「暗号化」の説明に、「Ｑサービスは～（省略）～暗号鍵は，サーバごとに生成し，Ｑサービス内で管理する。利用者がＱサービスのインタフェースを利用してファイルにアクセスすると，Ｑサービスは，ファイルを復号した後に引き渡す。」と記述されています。

したがって、Ｑサービスに対するクラッキングが行われて利用者のＩＤとパスワードが流出してしまうと、悪意のある第三者が、利用者に成りすましてＱサービスのインタフェースを利用してファイルにアクセスし、復号したファイルを入手できてしまいます。

また、Ｘ社自身の行為としてＱサービスの管理者が不正行為を行った場合も復号したファイルを入手できます。

いずれも、暗号鍵がサーバごとに生成されＱサービス内で管理されているからです。

(2) 「⑤生成された鍵は，当該フォルダ内に登録されるファイルの暗号化と復号だけに利用される。」場合には、一つの鍵が危殆化して無効となっても被害は当該鍵が使用されるフォルダだけに限定されますが、「一つの鍵を全ての機密フォルダで共有して利用する」と、一つの鍵が危殆化して無効となった場合には被害が全てのフォルダに及びます。

(3) 図７の「１．機密フォルダと暗号化フォルダの定義・導入」に、「利用者が同期ディスク中のフォルダに“_[c1]”で始まる名称を付けると」と記述されています。そして、図８に、「機密フォルダ“_[c1]sample”」、「暗号化フォルダ“_[c1]sample”」と記述されています。したがって、「ファイルの名称」は秘匿されません。

また、図７の「４．暗号化のアルゴリズムと鍵」に、「暗号化～（省略）～暗号の利用モードはCBC モードとする。」と記述されています。そして、CBC モードを利用した場合、平文と暗号文の長さは同じです。したがって、「おおよそのファイルサイズ」は秘匿されません。

(4) 数字は 0 ～ 9 の 10 種類なので、数字 16 文字のパスワードの数は 10^{16} です。英字は大文字と小文字を区別すると 52 種類なので、英数字では 62 種類で、p 文字のパスワードの数は 62^{p} です。数字 16 文字のパスワードの数が英数字 x 文字のパスワードの数より小さいので、x を求めると次のようになります。

$$62^{x} > 10^{16}$$

この式を図 9 の記述をもとに解くと次のようになります。

両辺について底を 10 の対数をとります。

$$\log_{10}62^{x} > \log_{10}10^{16}$$

$\log_{10}M^{N}$ は $N\log_{10}M$ と書き換えることができます。

$$x\log_{10}62 > 16\log_{10}10$$

$$x\log_{10}(2\times31) > 16\log_{10}10$$

$\log_{10}(M\times N)$ は $\log_{10}M+\log_{10}N$ と書き換えをことができます。

$$x(\log_{10}2+\log_{10}31) > 16\log_{10}10$$

$$x > \frac{16\log_{10}10}{\log_{10}2+\log_{10}31} \fallingdotseq \frac{16\times1}{0.301+1.491} \fallingdotseq 8.9$$

したがって、空欄 p は 9 、空欄 q は 62、空欄 r は 2 、空欄 s は 31、空欄 t は 8.9 です。

設問 5

(1) 図 7 の「３． Web インタフェースを用いて暗号化フォルダにアクセスしたときの処理」に、「利用者は，暗号化フォルダにファイルを登録する場合～（省略）～同期用 FS は，暗号化されたファイルを取得してマルウェアスキャンを行い，マルウェアが検知されなければ，復号した上で，同期ディスク中の対応する機密フォルダに配置する。」と記述されています。しかし、暗号化されたファイルは元のファイルとビット構造が異なるためマルウェアスキャンを行ってもマルウェアを検知できません。したがって、「暗号化フォルダに登録されたファイルは、復号した後で、マルウェアスキャンを行うようにする」ことにします。

(2) 図 7 の「３． Web インタフェースを用いて暗号化フォルダにアクセスしたときの処理」に、「利用者は，暗号化フォルダにファイルを登録する場合又は暗号化フォルダ内のファイルを更新する場合，事前に，指定された鍵と暗号化ソフトを用いてファイルを暗号化する～（省略）～暗号化フォルダに平文のファイルが登録された場合又は平文のファイルで既存のファイルが更新された場合，同期用 FS は当該ファイルを暗号化して更新した後，利用者に警告メールを送信する。」と記述されています。また、表 1 の「ファイル管理」に、「【補足事項】１． ファイルが更新又は削除された場合，元のファイルはバックアップとして保管される。」と記述されています。

したがって、「利用者が暗号化していないファイルを Web ブラウザで登録した場合」には、平文のままＱサービスに保管され続ける場合があります。この状況を防ぐには、「暗号化されていないバックアップのファイルを自動で削除する」機能を同期用 FS に追加します。

設問 6

〔Ｍ部長の最終確認〕のＭ部長の発言に、「当社は委託先との契約の中で，顧客データについて目的外利用の禁止と適切な管理を委託先に要求している。」と記述されています。しかし、IPA が公表している“組織における内部不正防止ガイドライン”には、「委託する業務内容と重要情報の重要度に応じて、セキュリティ対策を事前に確認・合意してから契約し、委託先が契約通りに情報セキュリティ対策を実施しているか定期的及び不定期に確認しなければならない。」と記述されています。また、具体策として、「業務を委託する場合、重要情報の取り扱いについて必要なセキュリティ対策が確実に実施されることを事前に確認するために、委託する業務内容に沿って、委託先の体制や規程等の点検、委託後の監査が可能かどうかの確認、必要に応じて実地調査等を実施し、その結果について、総括責任者または部門責任者等が適

切に評価することが望まれます。」と記述されています。
　したがって、技術的対策とは別に、「委託先のデータ管理の実態を監査によって把握して監督する」ようにします。