問2　データの暗号化とバックアップに関する次の記述を読んで，設問1～3に答えよ。

G社は，従業員数800名の医薬品販売会社であり，全国15か所に営業所をもっている。3か月前，ある営業所で火災が発生し，その営業所内のPCとサーバが被害を受けた。顧客データや注文データなどの電子データが消失してしまい，顧客データを再入力したり，顧客に注文データを確認したりするなどの復旧作業に1か月を要するなど，事業に大きな影響が出た。G社の経営陣は，今後同様のデータ消失が起きないように，営業所を対象としたデータバックアップを見直すよう，情報システム部に指示した。また，営業所ではPCに顧客データなどの機密データを保管している一方，従業員が社外にPCを持ち出して仕事をしているので，これらの機密データの社外への漏えいを防ぐ対策についても見直すよう，経営陣は指示した。

情報システム部のL課長は，これら二つの指示を受けて，部員のY君にバックアップ方式と機密保護方式を検討するように指示した。

Y君は，対象とするデータを整理するために，営業所に対して，保有しているデータの洗出しを依頼した。その結果，PCに保存されているデータのうち，バックアップ又は機密保護が必要なものは表のとおりであった。

表　PCに保存されていて，バックアップ又は機密保護が必要なデータ

データ	バックアップ	機密保護	データの取扱い	データの保存形式
顧客データ	必要	必要	表計算ソフトで顧客（医療機関の関係者）の連絡先などを管理している。パスワードなどによる保護はしていない。電子メール（以下，メールという）による表計算ファイルの送受信は行っていない。	(a) 表計算ファイル
注文データ	必要	必要	顧客から送付されてくるメールの本文中に医薬品の注文が記載されており，これで注文を受け付けている。	(b) メールボックスファイル内のメール（MIME形式）
仕入原価データ	不要	必要	本社からメールの添付ファイル（PDFファイル）として医薬品の仕入原価などが定期的に送付されてくる。添付されているPDFファイルはパスワードなどによる保護はされていない。	(b) メールボックスファイル内のメール（MIME形式）
			本社からメールの添付ファイルとして送付されてくるPDFファイルをメールから取り出してPCに保存し，参照している。	(c) PDFファイル

注　G社が使用しているメールソフトは，すべてのメールをPC上の一つのメールボックスファイルに格納する。

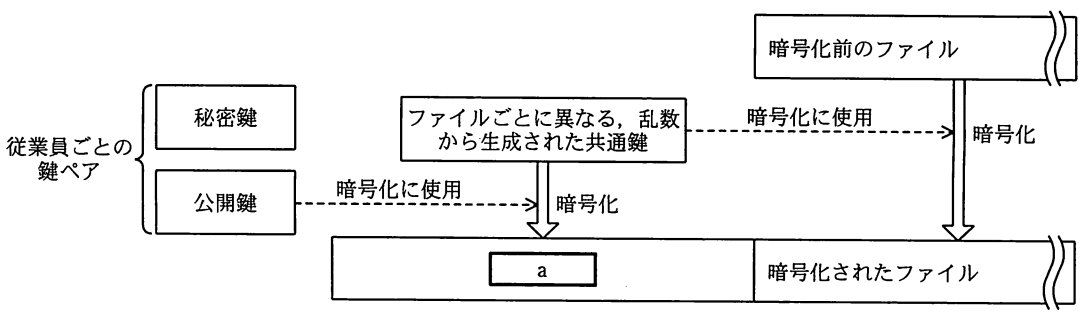
各営業所には，営業所内での情報共有のために医薬品のカタログデータなどを保管しているファイルサーバ（以下，営業所サーバという）が，サーバルーム内に設置されている。機密保護の観点から営業所サーバの管理状況を確認したところ，データの管理に問題はなかった。また，営業所サーバについては容量が比較的小さいので全データをバックアップの対象にすることにした。

〔暗号化方式の検討〕

まずY君は，表中の(a)と(c)の形式のデータについて暗号化を検討した。

Y君は，暗号化の方法として，PCのハードディスクをすべて暗号化するソフトウェアを利用する方式（以下，ハードディスク暗号化方式という）と，従業員ごとに公開鍵暗号方式の鍵ペアをもち，ファイル単位で暗号化を行うソフトウェアを利用する方式（以下，ファイル暗号化方式という）の比較を行った。その結果，ファイル暗号化方式に比べ，ハードディスク暗号化方式はG社で利用しているPCでは動作速度が著しく低下することが分かり，ファイル暗号化方式を採用することにした。

ファイル暗号化方式における暗号化は，図1のように行われる。従業員は，暗号化を開始するに当たって，まず秘密鍵と公開鍵の鍵ペアを生成する。ファイルの暗号化は，ファイルごとに異なる，乱数から生成された共通鍵を使用して行われる。暗号化に使われた共通鍵は従業員の公開鍵を使用して暗号化され，暗号化されたファイルとともにハードディスクに保存される。



注　ファイル暗号化方式によってファイルを暗号化すると，暗号化に関する情報がファイルに付加される。

図1　ファイル暗号化方式におけるファイルの暗号化

また，ファイル暗号化方式におけるファイルの復号は図2のように行われる。

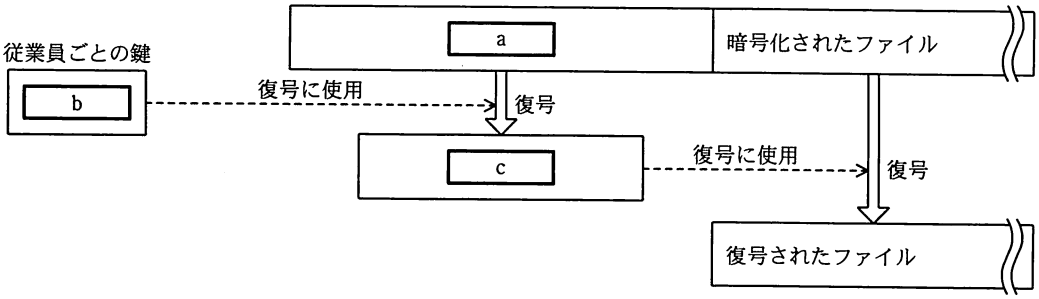


図２　ファイル暗号化方式におけるファイルの復号

従業員が OS にログインしている状態であれば，暗号化されたファイルは通常のファイルと同様に，暗号化・復号を意識することなく利用することができる。しかし，従業員が OS にログインしていない状態では，従業員の［　b　］にアクセスすることができないので，ファイルが暗号化されたままの状態となり，PC からハードディスクが外された場合でも，ハードディスクからのデータ漏えいを防止することができる。

次に Y 君は，表中の (b) の形式のデータについて，暗号化を検討した。調査の結果，G 社及び顧客のメールソフトはすべて S/MIME に対応しており，暗号メールの利用に問題がなかったので，注文データ又は仕入原価データを含むメールはすべて S/MIME で暗号化してやり取りすることにした。さらに，G 社のすべての PC には，［　d　］に基づいて評価及び認証された TPM（Trusted Platform Module）バージョン 1.2 対応製品が搭載されていることが分かった。そこで，この TPM を用いて，ファイル暗号化方式の鍵ペア及び S/MIME 用の鍵ペアを安全に保管することにした。

〔バックアップ方式の検討〕

続いて Y 君は，バックアップ方式の検討を行った。営業所から，PC だけが被害を受けてデータが消失した場合は前営業日のデータに回復し，営業所全体が被害を受けた場合は最悪でも 2 週間前のデータに回復したいとの要望が出たので，これらの要望に基づいて検討することにした。Y 君は，バックアップ方式として，図 3 のように，PC のデータを営業所サーバにバックアップし，次に営業所サーバのデータを磁気テープ（以下，テープという）にバックアップする方式を考えた。

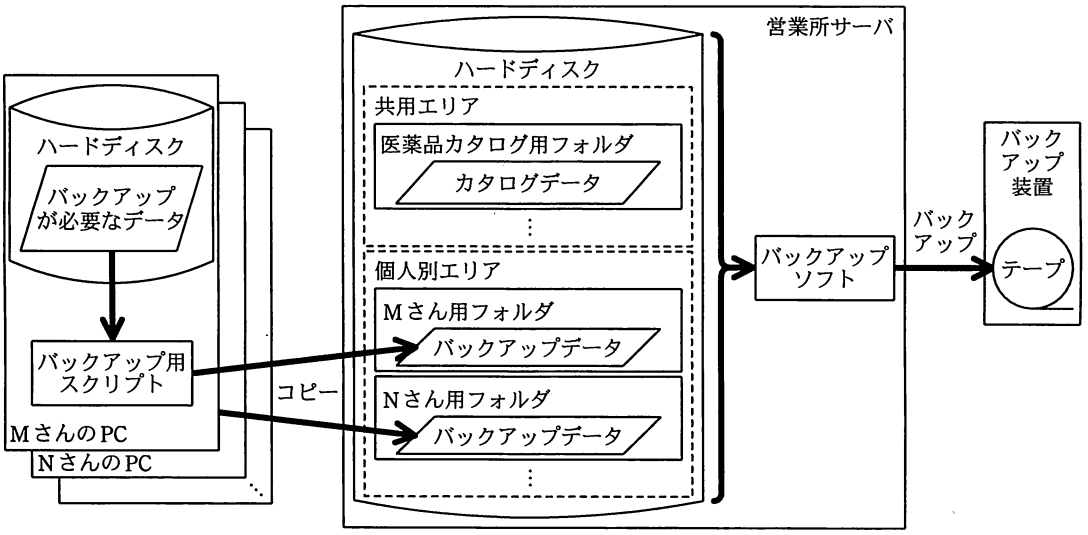


図3　バックアップ方式

PC のデータのバックアップを定期的に実行するため，ログアウト時に実行するバックアップ用スクリプトを設定する。そのスクリプトが，PC から営業所サーバへのバックアップ処理を実行する。退社時に従業員が OS からログアウトする際に，表中の (a) と (b) の形式のデータが，営業所サーバの個人別エリアに作成された各従業員のバックアップ用フォルダ内にコピーされる。営業所サーバにファイルがコピーされる際には，ファイル暗号化方式によって暗号化されているものは復号された上でコピーされる。

営業所サーバにバックアップソフトとバックアップ装置を導入する。毎週土曜日，バックアップソフトのスケジューラで，1 本のテープに全データのフルバックアップを行う。土曜日のバックアップが正常に完了していることを月曜日に確認した後，バックアップ装置のテープを未使用のものに交換し，取り出したテープを営業所のサーバルームに保管する。その週の金曜日に，保管しておいたテープを梱包し，商品配送などで利用している通常の宅配便サービスによって本社に送付する。本社では届いたテープを 1 年間安全に保管した後，古いものから順に安全に廃棄していく。

このバックアップ方式に対して L 課長は，①このバックアップ方式を導入することによって，社外への情報漏えいのリスクが高くなる可能性があると指摘した。

Y 君は，これを受けてバックアップ方式に新たな対策を加えた。

〔バックアップ方式の検証と改善〕

Y 君は，検討したバックアップ方式で運用できることを検証するために，まず，バックアップ用スクリプトで PC のデータを営業所サーバにコピーし，次に PC のデータ領域のファイルを消去した上で，営業所サーバからバックアップしたデータを PC に戻し，データを確認した。その結果，すべてのデータが問題なく使用できたので，一つの営業所でパイロット運用を開始した。

パイロット運用を開始して 2 週間後，ある従業員の PC が故障し，マザーボードの交換修理を行った。すると，暗号化されたデータが全く読めなくなってしまった。そこで，営業所サーバからバックアップしたデータを PC に戻したが，②それでもサーバから戻したデータの一部は PC で読めなかった。

Y 君は，この原因を調査したところ，TPM の利用方法を改善する必要があることが分かった。そこで，③ファイル暗号化方式の手順を一部修正した。修正された方式に基づいて実施したパイロット運用の結果は順調で，順次，すべての営業所で本格運用を開始していくこととなり，G 社営業所データの，暗号化とバックアップが実施されるようになった。

設問 1　〔暗号化方式の検討〕について，(1)～(3) に答えよ。

(1) 図 1，2 及び本文中の［ a ］～［ c ］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　暗号化された共通鍵　　イ　公開鍵　　ウ　電子署名

エ　ハッシュ値　　オ　秘密鍵　　カ　ファイルを復号する共通鍵

(2) ファイル暗号化方式において，G 社が利用している PC の TPM で必ず実行できる機能はどれか。解答群の中から二つ選び，記号で答えよ。

解答群

ア　暗号化された共通鍵を，ハードディスクに格納する機能

イ　共通鍵でファイルを暗号化する機能

ウ　従業員の鍵ペアを生成する機能

エ　乱数を生成する機能

(3) 本文中の［ d ］に入れる適切な情報セキュリティに関係した評価基準を解答群の中から選び，記号で答えよ。

解答群

ア　CC（ISO/IEC 15408）　　イ　JIS Q 15001

ウ　JIS Q 27001（ISO/IEC 27001）　　エ　PCI DSS

設問2　〔バックアップ方式の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線①において，どのような情報漏えいのリスクが高くなる可能性があるとL課長は指摘したか。40字以内で述べよ。

(2) 上記(1)で述べた情報漏えいのリスクが高くなる可能性について，それに対する対策を30字以内で述べよ。

設問3　〔バックアップ方式の検証と改善〕について，(1)～(3)に答えよ。

(1) 本文中の下線②において，読めなかったデータは表中のどれか。そのデータの保存形式を，表中の(a)～(c)からすべて選び，記号で答えよ。

(2) 本文中の下線②において，一部のデータが読めなかった理由を60字以内で述べよ。

(3) 本文中の下線③において，どのように暗号化方式の手順を修正したか。60字以内で述べよ。