## 問題５　次のアクセス制御に関する記述を読み各設問に答えよ。

Ｊ社には，全社員が遵守しなければならないセキュリティポリシがある。このたび，Ｊ社のセキュリティポリシに基づき，各部門に機密情報の漏えい防止対策の強化を通達した。図１に情報管理に関する箇所を示す。

| |
|---|
| 第３節　機密情報の管理<br>第 31 条　当社の機密情報は，三つの機密区分に分類する。機密度の高い順に，管理職以上に読取り権が与えられる“管理”，一般社員以上に読取り権が与えられる“一般”，協力社員以上に読取り権が与えられる“協力”とする。<br>第 32 条　当社の機密情報に対するアクセス権の付与は，業務上必要最小限とする。<br>第 33 条　機密情報が漏えいしないように，技術面，設備面及び運用管理面から十分なセキュリティ対策を実施しなければならない。 |

**図１　Ｊ社のセキュリティポリシ（抜粋）**

Ｊ社の開発本部は，開発第一課，開発第二課の二つの課から構成されている。開発本部では，これまで，機密情報の管理方法が課ごとに異なっていた。そこで，今回の機密情報の漏えい防止対策の強化をきっかけに，機密情報はすべてファイルサーバで一元管理することにし，新たに開発本部ファイルサーバ（以下，開発サーバという）を導入することにした。

［開発サーバのアクセス制御の仕様］

① 利用者 ID とログインパスワードによってユーザ認証を行う。

② 利用者 ID の属性として，必ず利用者グループを一つ設定する。

③ ファイルはすべてフォルダに格納され，フォルダ単位でアクセス権を設定する。

④ フォルダに設定するアクセス権は，表１のように３種類であり，利用者グループ単位で設定する。各フォルダには，複数の利用者グループのアクセス権を設定することができる。

**表１　フォルダに設定するアクセス権**

| アクセス権 | 動作 |
|---|---|
| 読取り権 | そのフォルダ内の参照が可能 |
| 作成権 | そのフォルダ内に新規作成が可能 |
| 更新権 | そのフォルダ内の削除および変更が可能 |

⑤ フォルダには，階層構造を構成できる。上位フォルダと下位フォルダに設定されたアクセス権が異なる場合には，下位フォルダのアクセス権が優先される。ただし，上位のフォルダには最低でも読取り権があるものとする。また，どのグループのアクセス権も下位フォルダに設定が無い場合には，上位フォルダのアクセス権が引き継がれる。

⑥ フォルダには,読み取り時と作成時に共通して用いるフォルダパスワードを設定することができる。ただし，フォルダパスワードは必要な場合のみ設定する。

＜設問１＞　次のアクセス権の設定方針に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

開発サーバの導入および運用管理の担当者が開発サーバの設定方針を次のようにまとめた。

開発サーバのフォルダ構成案を，図２に示す。


**図２　開発サーバのフォルダ構成案**

開発部利用者グループを，表２に示す。利用者 ID は，協力社員も含めて全員に発行する。利用者 ID には職位と合致する利用者グループを設定する。

**表２　アクセス権グループ**

| 利用者グループ名 | グループ構成員 |
|---|---|
| KANRI | 開発部管理職(課長以上) |
| IPPAN | 開発部一般社員 |
| KYORYOKU | 開発部協力社員 |

開発サーバのフォルダ構造とアクセス権の設定に関する要件を表３に示す。

**表３　開発サーバのフォルダ構造とアクセス権の設定に関する要件**

| フォルダ構造 | | アクセス権の設定に関する要件 |
|---|---|---|
| ルート | 階層１ | |
| 開発 | 管理 | KANRI には，読取り権，作成権，更新権を与える。 |
| | 一般 | IPPAN には，読取り権，作成権，更新権を与える。<br>KANRI には，読取り権を与える。 |
| | 協力 | KYORYOKU には，読取り権，作成権，更新権を与える。<br>KANRI，IPPAN には，読取り権を与える。 |

アクセス権の設定状況を示す表を，アクセス権テーブルという。表３の要件を適用すると，アクセス権テーブルは表４のようになる。アクセス権テーブルでは，読取り権を与える場合を“R”，作成権を与える場合を“C”，更新権を与える場合を“U”，読取り権と作成権を与える場合を“RC”，読取り権，作成権及び更新権のすべてを与

える場合を“RCU”，読取り権，作成権及び更新権のいずれも与えられていない場合を“-”で表す。

表４　アクセス権テーブル

| フォルダ / 利用者グループ | 管理 | 一般 | 協力 |
|---|---|---|---|
| KANRI | (1) | (2) | (2) |
| IPPAN | “-” | (1) | (2) |
| KYORYOKU | “-” | “-” | (1) |

(1)，(2) の解答群

ア．“R”　　イ．“C”　　ウ．“U”
エ．“RC”　　オ．“RCU”　　カ．“-”

＜設問２＞　次のフォルダ構成の変更に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

開発第一課，開発第二課より，課員だけがアクセスできるフォルダが必要であると要望があり，開発サーバのフォルダ構成を図３のように変更した。

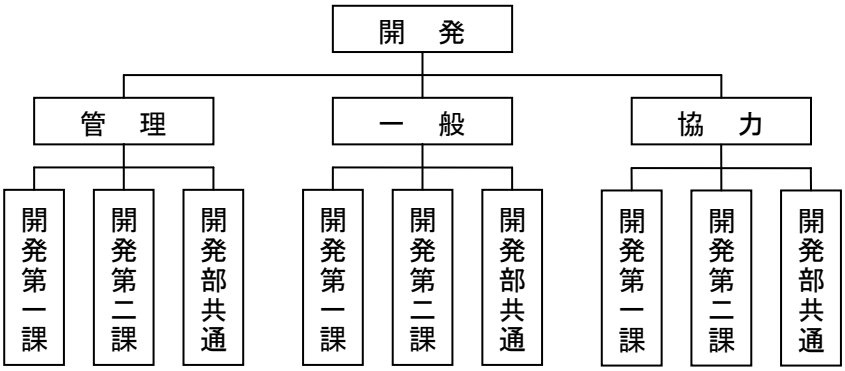


図３　開発サーバのフォルダ構成変更案

利用者 ID と利用者グループは，設問１と同じように設定し，フォルダのアクセス権とフォルダパスワードを利用してアクセス制御を行う。セキュリティポリシ第 32 条と，［開発サーバのアクセス制御の仕様］⑥ に従うと，図３最下層の三つの“開発第一課”フォルダには，同じフォルダパスワードを設定する。同様に“開発部共通”フォルダには，［　(3)　］。このことから，開発サーバ全体では，最低でも［　(4)　］種類のフォルダパスワードが使用される。

**(3) の解答群**

ア．同じフォルダパスワードを設定する
イ．開発第一課と同じフォルダパスワードを設定する
ウ．それぞれ異なるフォルダパスワードを設定する
エ．フォルダパスワードは設定しない

**(4) の解答群**

ア．1　　イ．2　　ウ．3　　エ．6　　オ．9

＜設問３＞　次のアクセス権の設定に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

表１の 3 種類のアクセス権（読取り権，作成権，更新権）は，それぞれに 1 ビットを使って許可，不許可を設定し，8 進数（0～7）で設定する。

［試行結果］
・0 を設定したら，一切のアクセスができなくなった。
・3 を設定したら，読取り権と作成権は与えられたが更新権は与えられなかった。
・5 を設定したら，読取り権と更新権は与えられたが作成権は与えられなかった。

この試行結果から，アクセス権の設定を次の 4 種類に限定し，それぞれのアクセス権を次のように設定した。

① すべて不可にするために 0 を設定する。
② 読取りのみを可能とするために［ (5) ］を設定する。
③ 読取りと作成を可能にするために［ (6) ］を設定する。
④ すべてを可能にするために［ (7) ］を設定する。

**(5) ～ (7) の解答群**

ア．1　　イ．2　　ウ．3　　エ．4
オ．5　　カ．6　　キ．7