次の問1は必須問題です。必ず解答してください。

問1　情報セキュリティ事故と対策に関する次の記述を読んで，設問1～3に答えよ。

自動車の販売代理店である A 社は，Web サイトで自動車のカタログ請求を受け付けている。Web サイトは，Web アプリケーションソフト（以下，Web アプリという）が稼働する Web サーバと，データベースが稼働するデータベースサーバ（以下，DB サーバという）で構成されている。Web サーバは A 社の DMZ に設置され，DB サーバは A 社の社内 LAN に接続されている。Web サイトの管理は B 氏が，A 社の社内 LAN に接続されている保守用 PC からアクセスして行っている。カタログ請求者は，Web ブラウザからインターネット経由で HTTP over TLS によって Web サイトにアクセスする。

〔カタログ請求者の情報の登録〕

A 社では，次の目的で，カタログ請求者の情報を保持し，利用することの同意を，カタログ請求者から得ている。

・情報提供や購入支援を行う。
・カタログ請求者が別のカタログを請求したいときなどに，登録した電子メールアドレスとパスワードを使用してログインできるようにする。

同意が得られたときは，氏名，住所，電話番号，電子メールアドレス，パスワード，購入予定時期，購入予算，希望車種などの情報を，Web アプリに入力してもらい，データベースに登録している。パスワードはハッシュ化して，それ以外の情報は平文で，データベースに格納している。A 社では，カタログ請求者から要求があったときにだけ，データベースからそのカタログ請求者の情報を消去する運用としている。

〔カタログ請求者への対応〕

A 社では，カタログ請求者へのカタログ送付後の購入支援を，データベースに登録されている情報を基に，電子メールと電話で行っている。

〔情報セキュリティ事故の発生〕

ある日，A 社の社員から，“A 社のカタログ請求者一覧と称する情報が，インターネットの掲示板に公開されている”と B 氏に連絡があった。公開されている情報を B 氏が確認したところ，データベースに登録されている情報の一部であったので，自社のデータベースから情報が流出したと判断して上司に報告した。B 氏は上司からの指示を受けて，Web サイトのサービスを停止し，情報が流出した原因と流出した情報の範囲を特定することにした。

〔情報セキュリティ事故の原因と流出した情報の範囲〕

B 氏の調査の結果，Web アプリに SQL インジェクションの脆弱性があることが分かった。そのことから B 氏は，攻撃者が①インターネット経由で SQL インジェクション攻撃を行い，データベースに登録されているカタログ請求者の情報を不正に取得したと推測した。Web サーバとデータベースではアクセスログを取得しない設定にしていたこともあり，流出した情報の範囲は特定できなかった。そこで，データベースに登録されている全ての情報が流出したことを前提に，A 社では，データベースに登録されている全てのカタログ請求者に情報の流出について連絡するとともに，対策を講じることにした。

〔情報セキュリティ事故を踏まえたシステム面での対策〕

B 氏は，今回の情報セキュリティ事故を踏まえたシステム面での対策案を，表 1 のようにまとめた。

表 1　情報セキュリティ事故を踏まえたシステム面での対策案

目的	対策
SQL インジェクション攻撃からの防御	・SQL 文の組立てはプレースホルダで実装する。 ・［　a　］
情報流出リスクの低減	・［　b　］
情報流出の原因と流出した情報の範囲の特定	・［　c　］

設問1　本文中の下線①について，この攻撃の説明として適切な答えを，解答群の中から選べ。

解答群

ア　攻撃者が，DNS に登録されているドメインの情報をインターネット経由で外部から改ざんすることによって，カタログ請求者を攻撃者の Web サイトに誘導し，カタログ請求者の Web ブラウザで不正スクリプトを実行させる。

イ　攻撃者が，インターネット経由で DB サーバに不正ログインする。

ウ　攻撃者が，インターネット経由で Web アプリに，データベース操作の命令文を入力することによって，データベースを不正に操作する。

エ　攻撃者が，インターネット経由で送信されている情報を盗聴する。

設問2　表 1 中の［　　］に入れる対策として最も適切な答えを，解答群の中から選べ。

a に関する解答群

ア　Web アプリへの入力パラメタには，Web サーバ内のファイル名を直接指定できないようにする。

イ　Web サーバのメモリを直接操作するような命令を記述できないプログラム言語を用いて，Web アプリを作り直す。

ウ　Web ページに出力する要素に対して，エスケープ処理を施す。

エ　データベース操作の命令文の組立てを文字列連結によって行う場合は，連結する文字列にエスケープ処理を施す。

b に関する解答群

ア　カタログ請求者の情報の適切な保管期間を定め，カタログ請求者の同意を得た上で，保管期間を過ぎた時点でデータベースから消去する。

イ　カタログ請求者の情報を，カタログ送付後に直ちに，データベースから消去する。

ウ　カタログ請求者へ送付する電子メールにディジタル署名を付ける。

エ　データベースに登録されている情報を定期的にバックアップする。

cに関する解答群

ア　Webサイトの管理に使用する保守用PCは，必要なときだけ起動する。

イ　WebサーバとDBサーバにインストールするミドルウェアは，必要最低限にする。

ウ　WebサーバとDBサーバのハードディスクのデフラグメンテーションを，定期的に行う。

エ　データベースへのアクセスログを取得する。

設問3　B氏は上司から，表1にまとめた対策案だけで十分なのか検討せよとの指示を受けた。そこで，社外のセキュリティコンサルタント会社に相談したところ，“Webアプリに脆弱性がないか調査をした方がよい”と助言され，Webアプリの一部について脆弱性の調査を依頼した。その結果，クロスサイトスクリプティングの脆弱性が存在することが判明した。また，“Webアプリの他の部分にも脆弱性があることが疑われるので，Webアプリ全体の調査を行うとともに，新たな対策を講じた方がよい”と助言された。新たな対策として適切な答えを，解答群の中から選べ。

解答群

ア　DBサーバを，Webサーバと同じく，DMZに設置する。

イ　不正な通信を遮断するために，WAF（Web Application Firewall）を導入する。

ウ　Webサーバを増設して冗長化した構成にする。

エ　保守用PCのログインパスワードには英数字及び記号を使用し，推測が難しい複雑なものを設定する。