## 問040009問題

セキュリティ事故の対応に関する次の記述を読んで，設問１～４に答えよ。

自転車用品の中堅通信販売会社のＤ社では，顧客からの注文を郵便及び電話で受け付けていた。顧客へのサービスの拡大を目的として，インターネットを利用した会員制のサービスを開始することとした。

会社の紹介だけを掲載していた従来のＷｅｂサイトを改修し，Ｗｅｂサイトでの会員情報の登録及び修正，会員に対するＷｅｂサイトでの商品の販売並びに会員向けのメールマガジン送付の登録を行う。

なお，Ｗｅｂサイトでの商品の販売における決済手段はクレジットカードだけとする。

改修後のＷｅｂサイトは，Ｄ社のＤＭＺ上に設置されたＷｅｂサーバと，社内ＬＡＮ内に設置されたデータベースサーバで構成される。データベースサーバのデータは平文で保存しており，会員情報の登録及び修正，商品の販売並びに会員向けのメールマガジン送付の登録を行う際には，ＳＳＬによってネットワーク経路の暗号化を行う。

〔会員情報の登録〕

Ｄ社では，Ｗｅｂサイトで取得する個人情報の利用目的を，注文の受付，決済，商品の配送，及びメールマガジンの送付に限定し，会員登録の希望者に対し，登録時に利用目的を通知して同意を得ることとした。同意を得た会員に対しては，会員情報として次の情報を登録してもらうこととした。

【全員に登録してもらう情報】

利用者ＩＤ，パスワード，メールアドレス，メールマガジン送付の有無

【任意に登録してもらう情報】

性別，生年月日

【商品を購入する会員に登録してもらう情報】

氏名，配送先住所，電話番号，クレジットカードの発行会社名，クレジットカード番号，クレジットカードの有効期限

〔セキュリティ事故の発生〕

複数の会員から，″Ｄ社のサービスに登録したメールアドレス宛てに迷惑メールが大量に送られてくるようになった″との連絡がお客様相談窓口に入った。さらに，連絡があった会員のうち数名については，迷惑メールの宛先メールアドレスはＤ社以外のサービスでは利用していないことが分かった。

この報告を受けてＤ社の情報システム部のＹ部長は，会員情報が漏えいしている可能性があると判断した。また，会員情報として登録されているクレジットカード情報が漏えいしていることも考えられると判断した。そこで，情報システム部のＷｅｂサイト担当者Ｚ氏に対し，Ｗｅｂサ

イトを停止して調査するよう指示した。

Ｚ氏の調査の結果，Ｄ社のＷｅｂサイトにおいて，会員が利用者ＩＤとパスワードの入力を行うログインの処理に不備があり，外部からＳＱＬインジェクション攻撃を受けていたことが判明した。

〔セキュリティ事故への対応〕

Ｚ氏は，一般的なＷｅｂサイトにおけるセキュリティ事故に関して考えられる対策と対応を調査し，今回のセキュリティ事故において会員とＷｅｂサイトに対して必要と思われる対策と対応を表１にまとめて，Ｙ部長に報告した。

**表１　セキュリティ事故の対策と対応の概要**

| 対象 | 対策と対応 |
|---|---|
| 会員 | ①　全ての会員に対する謝罪<br>②　事故の公表と被害状況の説明<br>③　会員への事故対応の依頼 |
| Webサイト | ④　被害状況の把握及び原因の特定<br>⑤　SQLインジェクション攻撃を防ぐためのWebサイトの改修<br>⑥　Webサイトへのアクセスの常時監視<br>⑦　ネットワークを介した攻撃によるネットワークアクセス負荷上昇に対応するためのネットワーク回線の二重化 |

Ｙ部長は，表１の⑦は実施を見合わせ，Ｚ氏に①～⑥の実施を急がせるとともに，更なる情報セキュリティ対策の実施を指示した。

***設問１***　今回受けたＳＱＬインジェクション攻撃に関する記述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に登録されたドメインの情報を改ざんすることによって，利用者をフィッシングサイトに誘導し，そこで入手した利用者ＩＤとパスワードを用いて，データベースを不正に操作した。

イ　攻撃者が，Ｄ社のＷｅｂサイトの入力項目に対し，命令文を送り込むことによって，データベースを不正に操作した。

ウ　攻撃者がＤ社のデータベースの管理ツールを入手し，管理ツール経由で直接Ｄ社のデータベースを不正に操作した。

エ　攻撃者がネットワーク上で情報の盗聴を行い，Ｄ社のデータベースの管理者のＩＤとパスワードを入手し，データベースを不正に操作した。

***設問２*** 表１中の③に関して，今回のセキュリティ事故の対応として適切な答えを，解答群の中から選べ。

解答群

ア　安易なパスワードの設定を防止するために，パスワードは英字，数字，記号が混在する８文字以上のものにするよう会員に依頼する。

イ　攻撃を受けた場合の被害を抑えるために，メールマガジン購読だけを利用する会員の会員情報を格納したデータベースと商品の購入を行う会員の会員情報を格納したデータベースとを分離し，商品の購入を行う会員だけには，利用者ＩＤ及びパスワードの変更を依頼する。

ウ　個人情報の目的外利用を避けるために，Ｄ社が取得する個人情報の利用目的に事故の対応を追加し，同意を会員に依頼する。

エ　クレジットカード情報が漏えいしている場合の不正利用を防止するために，登録されたクレジットカードの停止及び番号変更の手続を会員に依頼する。

***設問３*** 表１中の⑦に関して，Ｙ部長が実施を見合わせた理由として適切な答えを，解答群の中から選べ。

解答群

ア　Ｗｅｂサーバの増設が必要となる。

イ　稼働中のサービスの停止が必要であり，事業への影響が大きい。

ウ　今回のＳＱＬインジェクション攻撃を防ぐ対策にならない。

エ　セキュリティ事故発生時に攻撃者の侵入経路の特定に時間が掛かる。

***設問４*** Ｙ部長は，Ｚ氏に事故の再発防止のために更なる情報セキュリティ対策の実施を指示した。次の記述中の［　　］に入れる適切な答えを，解答群の中から選べ。

〔ＳＱＬインジェクション攻撃への追加対策〕

ＳＱＬインジェクション攻撃は，システム開発の際にセキュリティを考慮した設計及び実装を行うことで回避できる。例えば，［　a　］ことで，アプリケーション開発時に脆弱性が作り込まれる可能性を減らすこととする。

〔会員情報に対するその他のセキュリティ対策〕

会員情報を格納したデータベースサーバへの不正アクセス対策として，［　b　］こととする。また，情報漏えいが発生した場合の原因の分析や犯人の追跡を行うための証拠の確保には，［　c　］を行うこととする。

ａに関する解答群

ア　開発担当者と運用担当者の職務を分離する

イ　開発用の端末と通常利用の端末を分離する

ウ　瑕疵の発生に備えた保険に加入する

エ　機密保持に関する誓約書を作成する

オ　セキュアプログラミングのルールを作成する

カ　負荷分散装置を設置する

ｂに関する解答群

ア　Ｗｅｂサーバとデータベースサーバの時刻を同期させる

イ　会員情報を暗号化する

ウ　社内からのインターネット利用時にフィルタリングを実施する

エ　共有ＩＤを利用する

オ　データベースサーバを乱射Ｄ構成にする

ｃに関する解答群

ア　アクセスログやエラーログの保管

イ　外部記憶媒体の利用禁止を明文化

ウ　業界団体との連携によるセキュリティ事故情報の共有

エ　担当する業務に応じた情報セキュリティ教育の実施

オ　内部不正に対する罰則の強化