問2 Web アプリケーションのセキュリティ対策に関する次の記述を読んで，設問 1～3 に答えよ。

O 社は従業員数 20 名のインターネット通販会社であり，通販サイト（以下，X サイトという）で会員向けに化粧品を販売している。X サイトは O 社が開発し，運用している。

ある日，会員からの問合せがあり，X サイトで管理している会員の個人情報が流出していることが判明した。O 社は，被害拡大防止のために X サイトを一旦停止した上で，流出件数，原因などを明らかにするために，情報システム担当者である V さんから，セキュリティ専門会社 D 社の S 氏に調査を依頼した。

S 氏は，V さんから X サイトのシステム構成を聞いた後，関係するログを調査した。

X サイトでは，会員 ID 及びパスワードを，データベースの m_user テーブルの cust_id 及び pwd という列にそれぞれ格納しており，ログイン機能（login.cgi プログラム）では cid，pw という引数とデータベースに格納されている値を照合している。表 1 は，Web サーバの HTTP アクセスログのうち不正アクセスに関連する部分の抜粋であり，左から順に，便宜上付けた番号，クライアントの IP アドレス，HTTP のアクセスメソッド，cgi プログラム名，クエリ文字列である。

〔調査結果〕

S 氏が表 1 の HTTP アクセスログを調査した結果，次の攻撃が判明した。

- 攻撃 1：IP アドレスが［ a ］の攻撃者が，［ b ］.cgi に対し SQL インジェクションによって全会員分に当たる約 8,000 件の会員 ID 及びパスワードを窃取していた。
- 攻撃 2：SQL インジェクションによって X サイトのデータが改ざんされ，その後アクセスした会員の PC にマルウェアを強制的にダウンロードさせられていた。（表 1 中の 20 番）
- 攻撃 3：SQL インジェクションによってデータが改ざんされ，会員 ID 及びパスワードを詐取されていた。（表 1 中の 22 番）
- 攻撃 4：不正ログインを試行されていた。

S 氏は，調査結果を V さんに説明した。次は，そのときの会話の一部である。

Vさん：攻撃2ですが，IPアドレスがipJの攻撃者（以下，攻撃者ipJという）によって，画面の一部であるバナーとして表示されるデータ（ban_url）が改ざんされていたということですね。Xサイトにアクセスした一部の会員から“ウイルス対策ソフトが警告を表示する”という問合せがあったのは，それが原因ですね。

S氏　：はい。会員が，改ざんされたデータを含む画面に表示された“重要なお知らせ”をクリックすると，攻撃者ipJが用意した外部サイトに誘導されて，ブラウザが誘導先ページのコンテンツと一緒に，不正な動作を引き起こすファイルをダウンロードします。それから，そのファイルが，ブラウザの［　c　］で処理される過程で，ブラウザの［　c　］の脆弱(ぜい)性を突くコードを実行することで，PCが感染し，その後，別のファイルがダウンロードされます。もし途中でPCのウイルス対策ソフトが検知，駆除しなければ，最終的にはキーロガーとして存在していました。

表1　Webサーバの HTTP アクセスログ（不正アクセスに関連する部分の抜粋）

番号	IP	メソッド	cgi	クエリ文字列 1)
1	ipA	GET	login.cgi	cid=yamada&pw=fajsl334
2	ipB	GET	login.cgi	cid=cust51&pw=password
3	ipC	GET	login.cgi	cid=tanaka&pw=p7g3dfb0
4	ipB	GET	login.cgi	cid=cust51&pw=pass
5	ipB	GET	login.cgi	cid=cust51&pw=cust51
6	ipB	GET	login.cgi	cid=cust51&pw=
7	ipC	GET	search.cgi	item=gf34' and select cust_id, pwd, null, null from m_user where '1' = '1&kind=09
8	ipB	GET	login.cgi	cid=cust51&pw=15tsuc
9	ipB	GET	login.cgi	cid=cust51&pw=a
10	ipB	GET	login.cgi	cid=cust51&pw=b
11	ipB	GET	login.cgi	cid=cust51&pw=c
12	ipD	GET	search.cgi	item=gf44' union select pwd, null, null, null from m_user where '1' = '1&kind=09
13	ipB	GET	login.cgi	cid=cust51&pw=d
14	ipE	GET	login.cgi	cid=cust01&pw=password
15	ipG	GET	confirm.cgi	cat=0217&iname=../ls |
16	ipE	GET	login.cgi	cid=cust12&pw=password
17	ipF	GET	search.cgi	item=gf36' union select cust_id, null, null, null from m_user where '1' = '1&kind=9
18	ipC	GET	confirm.cgi	cat=1127&iname=tanaka><script>alert("test");</script>
19	ipE	GET	login.cgi	cid=cust33&pw=password
20	ipJ	GET	search.cgi	item=0b24';update m_contents set ban_url = ban_url || '">重要なお知らせ
21	ipH	GET	search.cgi	item=gf12' union select cust_id, pwd, null, null from m_user where '1' = '1&kind=09
22	ipI	GET	search.cgi	item=0b24';update m_contents set ban_url = ban_url || '"><script type="text/javascript" language="javascript">document.write("<html>（省略）</html>");</script>

注 1)　クエリ文字列は，URLデコード済である。

Vさん：なるほど。では，攻撃3についても説明をお願いします。

S氏　：攻撃3も同じくデータ改ざんによるものですが，攻撃2の後しばらくしてから攻撃を受けており，①攻撃1とは異なる手口で会員IDとパスワードの詐取が試みられていました。

続いてS氏はVさんに，攻撃3の具体的な手口や攻撃4のログの特徴についても説明した。

〔パスワード格納方法の検討〕

S氏はVさんに，HTTPアクセスログの調査結果から判明した不正アクセスについて説明した後，SQLインジェクションに関係していたm_userテーブルを調査して気付いたことを指摘した。次は，そのときの会話である。

S氏　：m_userテーブルを見ていて気付いたのですが，パスワードは暗号化されていますよね。どのような暗号アルゴリズムで暗号化しているのですか。

Vさん：暗号アルゴリズムは自作しました。例えば，元の文字列がpasswordの場合，まず，［　d　］式暗号でdrowssapに変換し，次に，［　e　］式暗号でespxttbqに変換します。

S氏　：そのアルゴリズムは変更すべきです。CRYPTREC（暗号技術評価プロジェクト）が電子政府推奨暗号リストに公開している暗号アルゴリズムと異なり，自作アルゴリズムは，［　f　］について公的な機関の評価を受けていないので推奨できません。

Vさん：なるほど。それでは，修正を検討します。

S氏　：それから，攻撃者が何度も会員登録した上で，攻撃者の指定したパスワードとそれに対する暗号文から解読する［　g　］攻撃によって会員のパスワードを解読された可能性が高いので，サイトの再開前に全会員のパスワードを初期化し，初期化する前のパスワードへの変更を禁止すべきです。

Vさん：承知しました。会員にはパスワードを初期化したことを通知します。

S氏　：それだけではなく，②初期化する前のパスワードが解読されている可能性が高いことも通知してください。

その他，S 氏は V さんに，改ざんされたデータの復旧方法や攻撃に対するプログラムの修正方法などを説明した。

O 社は，S 氏の指摘に従って，被害の状況や再発防止策などの情報を自社の Web サイトで公表した。その後，プログラム修正，パスワードの格納方法の改善などの対策を完了させ，全会員のパスワードを初期化して会員に連絡した上で，X サイトを再開させた。

設問 1　〔調査結果〕について，(1)～(3)に答えよ。

(1)　本文中の［ a ］に入れる IP アドレスを一つ答えよ。

(2)　本文中の［ b ］に入れる cgi プログラム名を 7 字以内で答えよ。

(3)　表 1 に示されている IP アドレス ipB による攻撃は，ログを調査した結果，ある特徴から不正ログインの試行と判明した。その特徴について 35 字以内で述べよ。また，その不正ログイン試行対策を 35 字以内で述べよ。

設問 2　〔パスワード格納方法の検討〕について，(1)，(2)に答えよ。

(1)　本文中の［ d ］～［ g ］に入れる字句をそれぞれ解答群の中から選び，記号で答えよ。

解答群

ア　DoS	イ　Exploit	ウ　安全性	エ　換字
オ　サイドチャネル	カ　辞書	キ　市場性	ク　選択平文
ケ　誕生日	コ　転置	サ　分散性	

(2)　本文中の下線②について，初期化する前のパスワードへの変更を禁止する以外に，会員に通知する理由は何か。その理由を 50 字以内で述べよ。

設問 3　SQL インジェクションによるデータ改ざんについて，(1)，(2)に答えよ。

(1)　本文中の［ c ］に入れる字句を 10 字以内で答えよ。

なお，会員の PC の OS 及びブラウザ本体への攻撃は実施されなかったものとする。

(2)　本文中の下線①について，会員 ID 及びパスワードを詐取する方法を 50 字以内で具体的に述べよ。