＜問3＞ プロキシサーバによるマルウェア対策

■設問１

〔試験センターによる解答例〕

a：エ

インターネットから Web サーバへの通信を中継する機能であるから，該当するのは「リバースプロキシ」である。

■設問２

〔試験センターによる解答例〕

(1) b：イ

c：オ

(2) プログラムの内容を変え，かつ，プログラム名を変える場合（27 字）

(1)

b : 問題文にあるように，マルウェア Z が社員 PC 上にダウンロードした攻撃用プログラムが OS の管理用コマンドを複数ダウンロードして起動させ，サーバ情報を窃取した。したがって，社員 PC で起動禁止設定すべきプログラムは攻撃用プログラムと OS の管理用コマンドであり，解答群の**イ**が該当する。なお，マルウェア Z は単体のプログラムではなく，文書ファイルのマクロとして実装されているため，起動禁止設定することはできない。

c : 管理 PC では，OS の管理用コマンドを起動禁止設定することはできないため，攻撃用プログラムのみ起動禁止設定を行う。したがって解答群の**エ**が該当する。

(2) プログラム名を指定して起動を禁止する方式では，プログラム名が変わると起動を防ぐ

ことができない。また，プログラムの実行ファイルのハッシュ値を指定して起動を禁止する方式では，プログラムの内容が変わるとハッシュ値も変わるため，起動を防ぐことができない。したがって，上記の二つの方式でプログラム起動禁止設定を行ったとしても，自身の名称と内容を変える攻撃プログラムについては起動を防ぐことができない。

■設問３

〔試験センターによる解答例〕

(1) 送信元 IP アドレスがプロキシ 1 の IP アドレスとなるので（27 字）

(2) d：オ

(1) フェーズ 1 では，社員 PC はインターネット接続時にはプロキシ 1 と通信しており，プロキシ 2 は，プロキシ 1 とインターネットへ間の通信を全て中継する構成となっている。そのため，プロキシ 2 が中継する通信の**送信元 IP アドレスは全てプロキシ 1 となり**，プロキシ 2 のログから送信元 PC を特定することはできない。

(2) フェーズ 1 のような構成において，送信元 PC の IP アドレスをプロキシ 2 で特定できるようにするために使用する HTTP ヘッダは“**X-Forwarded-For**”（XFF）ヘッダフィールドである。XFF は，プロキシサーバや負荷分散装置等を経由して通信するホストの送信元 IP アドレスを特定する用途で標準的に使用されるヘッダフィールドである。

■設問 4

〔試験センターによる解答例〕

(1) Web ブラウザからプロキシサーバへの通信を盗聴して認証情報を取得し，プロキシサーバに送信する。(47 字)

(2)

URL フィルタリング機能：ホワイトリストに業務に必要かつ安全であることを確認した URL を設定する。(36 字)

カテゴリ単位フィルタリング機能：業務に不要であるカテゴリを遮断する。(18 字)

(1) プロキシ認証に対応したマルウェアは，まず感染した PC とプロキシサーバとの通信を

盗聴し，そこに含まれる認証情報を取得する。続いて，取得した認証情報をそのまま**プロキ**

[旧 SC・H28 秋　午後 I 解答・解説]

シサーバに送信し，認証を成功させる。このような機能を持つマルウェアは数多く存在し，プロキシの認証機能を危殆化させている。

(2) 問題文にあるように，プロキシ 2 のフィルタリング機能では，URL フィルタリングとカテゴリ単位フィルタリングで同じ URL が設定された場合は URL フィルタリングが優先される。また，URL フィルタリングのホワイトリストとブラックリストで同じ URL が設定された場合はホワイトリストの設定が優先させる。

このように，ホワイトリストの設定が最優先されるため，**業務に不要であるカテゴリをカテゴリ単位フィルタリング機能で遮断する**ように設定し，**業務に必要かつ安全であることを確認した URL を URL フィルタリング機能のホワイトリストに設定**し，許可すればよい。