

対策とはならないため、③を候補として具体的なフィルタリング方法を考察する。マルウェア感染時の HTTP リクエストが図 11 に示されているので、そこから JRE の脆弱性を悪用した攻撃をフィルタリングする上で使えそうな文字列を探すと、リクエスト 2、リクエスト 3 の User-Agent ヘッダに“Java/1.6.0_21”が含まれていることがわかる。“/”以降はバージョン情報であるため対象外とし、③の機能を用いて **User-Agent ヘッダの内容に文字列“Java”が含まれるリクエストをフィルタリングすることが有効な対策となる。**

- (3) マルウェアから C&C サーバへの HTTP 通信をプロキシで止める上で有効と思われる対策を表 3 から探すと、該当するのはプロキシの利用者認証機能である。当該機能の詳細は示されていないが、図 2 より、マルウェア P は「プロキシ設定を参照する」以上のことは行わないため、**利用者の認証を有効にすることが対策となると推測される。**
- (4) N さんの PC が L さんの PC の通信を盗聴できたのは、L3SW になりすました N さんの PC に対し、L さんの PC からのパケットが送信されたことによる。したがって、N さん、L さんのいずれかの PC のパーソナルファイアウォールの設定によってこれを防ぐとすれば、N さんの PC で**インバウンド通信を禁止することである。**

<問2> スマートフォンを利用したリモートアクセス環境

■設問 1

〔試験センターによる解答例〕

(1)

アクセス：

- ・スマートフォンから社内 Web サーバへのアクセス (23 字)
- ・スマートフォンからメールサーバへのアクセス (21 字)

対策：

- ・スマートフォン用の DMZ2 を追加し、スマートフォンとモバイル PC の通信経路を分離する。(43 字)
- ・FW4 でスマートフォンから社内 Web サーバ及びメールサーバへの通信を禁止する。(39 字)

(2)

	送信元	宛先	プロトコル
FW3	Any	VPN サーバ 2	L2TP over IPsec
FW4	Web メールサーバ	メールサーバ	POP3
	Web メールサーバ	メールサーバ	SMTP

(3)

問題：VPN アカウントを停止すると、モバイル PC から社内ネットワークに接続できなくな

る。(41 字)

対策：スマートフォンで利用する VPN アカウントを、モバイル PC で利用するものと別に作成する。(43 字)

(4) C15

- (1) 「D 社が認めていないアクセス」に該当するものとして、[スマートフォンを利用したリモートアクセス環境の構築]に、「スマートフォンから社内 Web サーバへのアクセスは認めない」という記述がある。また、案 1 における実現方式の(2)に、「スマートフォンのメールクライアントからメールサーバにアクセスすることは禁止する」という記述がある。

一方、案 1 における実現方式の(1)に「スマートフォンもモバイル PC も VPN サーバ 1 に接続された状態では、(中略) DMZ1 に接続されているのと同じように通信できる」とあり、表 4 を見ると、DMZ1 から社内 Web サーバへの通信 (HTTP, HTTP over TLS) , DMZ1 からメールサーバへの通信 (POP3, SMTP) がともに許可されている。つまり、上記の「D 社が認めていないアクセス」が技術的に可能となっている状態である。

これに対し、案 2 では DMZ2 が新設されている。DMZ2 にはスマートフォンのブラウザから利用するために構築した Web メールサーバが接続されていることから、スマートフォン用のセグメントであることがわかる。一方、Web メールサーバが移設されたこと以外は FW1, FW2 の設定を含め、案 1 と同様の構成である DMZ1 はモバイル PC 用のセグメントであることがわかる。つまり、DMZ2 を新設することにより、アクセス権の異なるモバイル PC とスマートフォンの通信経路を分離したのである。

また、案 2 では DMZ2 とサーバ LAN との間には FW4 があることから、スマートフォンから社内 Web サーバ及びメールサーバへの通信を FW4 で禁止していると推測できる。

- (2) 案 1 における実現方式の(1)に「スマートフォンの VPN クライアント機能を用いて、L2TP over IPsec で既存の VPN サーバ 1 に接続する」とあるが、案 2 では、VPN サーバ 1 に代わって VPN サーバ 2 に同様に接続する必要がある。したがって、FW3 は、スマートフォンから VPN サーバ 2 への L2TP over IPsec を許可する必要がある。記述形式は表 3 の 1 行目を参考にするとよい。

続いて、FW4 で許可する通信について考察する。スマートフォンから社内 Web サーバへのアクセス及びメールサーバへのアクセスは禁止する必要がある。一方、案 1 における実現方式の(2)に「Web メールサーバは、メールサーバに対してはメールクライアントとして動作」とあることから、FW4 ではこれを許可する必要があることがわかる。Web メールサーバがメールクライアントとして動作するには、送信元が Web メールサーバで宛先がメールサーバの POP3 通信及び SMTP 通信を FW4 で許可する必要がある。記述形式は表 4 の 1 行目、2 行目を参考にするとよい。

- (3) スマートフォンの盗難及び紛失の届出があったときにとられる対策とは、図 2 の 6にある通

り、「VPN サーバ 1 の設定において当該利用者の VPN アカウントを停止する」ことであり、これによって引き起こされる問題が問われている。案 1 では、モバイル PC とスマートフォンがともに VPN サーバ 1 に接続する形態となっていることから推測されるように、スマートフォンの盗難及び紛失によって **VPN アカウントが停止されると、モバイル PC から社内ネットワークに接続することができなくなる**という問題が生じる。

これに対し、案 2 では、DMZ2 を追加することにより、スマートフォンとモバイル PC の通信経路を分離している。これにより、**スマートフォンで利用する VPN アカウントを、モバイル PC で利用するものとは別に作成することが可能となるため**、スマートフォンの盗難及び紛失によって当該 VPN アカウントが停止されたとしても、モバイル PC を利用する上で特に問題はない。

- (4) 表 5 において、R1～R3 のリスクに対する対策 C1～C8 については D 社のネットワークやサーバ側の設定によって対応するものであるため、確実に管理できる。残る C9～C17 についての対応を確認すると、C15 以外については次のように管理していることがわかる。

C9 : Web メールサーバのみを使用可能とすることにより管理

C10 : 図 4 の 7 によって管理

C11 : Web メールサーバによって管理

C12 : 図 4 の 6 によって管理

C13 : 図 4 の 6 によって管理

C14 : 図 4 の 4 によって管理

C16 : 図 4 の 5 によって管理

C17 : 図 3 の 2(1)によって管理

表 1 にあるように、スマートフォン B では、T 社ストアや携帯電話事業者の Web サイトで提供されているものであっても、アプリケーションの安全性審査及び導入時のデジタル署名の検証は行われず、導入するアプリケーションの選択は利用者に任されている。したがって、C16 を実施したとしても、**C15 については D 社の管理が及ばない。**

■設問 2

〔試験センターによる解答例〕

(1) 携帯電話網を介さずにインターネットに接続されている状態 (27 字)

(2)

仕様：一部の機種では、デフォルト設定の状態で自動同期機能が有効になっている。

内容：自動同期機能を無効にする。

(3) C5, C12, C13, C14, C16, C17

- (1) 図 5 にあるように、スマートフォンのインターネット接続形態には、携帯電話網を介する場

合と介さない場合とがあるが、〔リモートアクセス環境の改善〕の(2)にある通り、D 社ではスマートフォンの携帯電話網を介したデータ通信を無効化して、無線 LAN 経由でリモートアクセスを行っている従業員が多いのが実情である。下線③のサービスは、携帯電話網を介したデータ通信を用いて提供されるため、上記のように、スマートフォンが**携帯電話網を介さずにインターネットに接続されている状態**ではデータを消去することができない。一方、製品 E では、スマートフォンが携帯電話網を介さずにインターネットに接続されている状態であってもデータを消去することが可能である。

(2) Z 主任は案 3 のレビューにおいて「スマートフォンの仕様の一部が D 社の業務データ取扱事項違反の原因となる」と指摘した。図 6 で業務データの取扱いに関するものを確認すると、データの暗号化や盗難・紛失時の消去のほか、「バックアップデータの保管先として（中略）D 社の管理及び規程が及ばないサービス又はシステムを利用することを禁止する」とある。問題文の冒頭に例示されている通り、「D 社の管理及び規程が及ばないサービス又はシステム」とは、クラウドサービスによって提供されるサービス、オンラインストレージサービス、ファイル共有システムなどである。

続いて表 2 で「クラウドサービスの利用」に関する機能を確認すると、スマートフォン A、B ともに、一部の機種では、スマートフォンに保存されているデータをクラウドサービスのサーバに定期的にコピーする**自動同期機能がデフォルトの状態でも有効**になっており、これが D 社の業務データ取扱事項違反の原因となることがわかる。

自動同期機能を無効に設定すれば対策が可能であるため、この問題への対策としてスマートフォン利用手続に追加すべき内容は、「**自動同期機能を無効する**」である。

(3) 〔リモートアクセス環境の改善〕にある、製品 E の機能に関する記述部分を表 5 に照らしながら確認することで解答を導き出すことができる。

まず、本文中の「デバイス保護機能の設定及びスマートフォンの設定の監視と強制」が C5、「改造されたスマートフォンの検知」が C14、「OS 及びスマートフォンに導入されているアプリケーションの名称及びバージョンなどの取得」が C12、C13 が該当する。

続いて、図 6 の項番 1 にある「製品 F が導入・設定されていることを、製品 E によって監視する」が C17、項番 2 にある「安全性が疑わしいアプリケーションを導入しているスマートフォンを、製品 E によって検知する」が C16 に該当する。

■設問 3

【試験センターによる解答例】

スマートフォンの盗難又は紛失の届出があったときに、従業員個人のデータも消去されること（42 字）

〔リモートアクセス環境の改善〕にあるように、製品 E のデータ消去機能は、スマートフォン及び外部記憶媒体に保存された全てのデータを対象としている。したがって、スマートフォ

ンの盗難又は紛失の届出によって製品Eのデータ消去機能を実行すれば、業務データに限らず、スマートフォンや外部記憶媒体に保存された従業員個人のデータも全て消去されることになる。この点について事前に従業員に説明し、同意を得ておかないと、当該対策の実施において支障をきたすおそれがある。