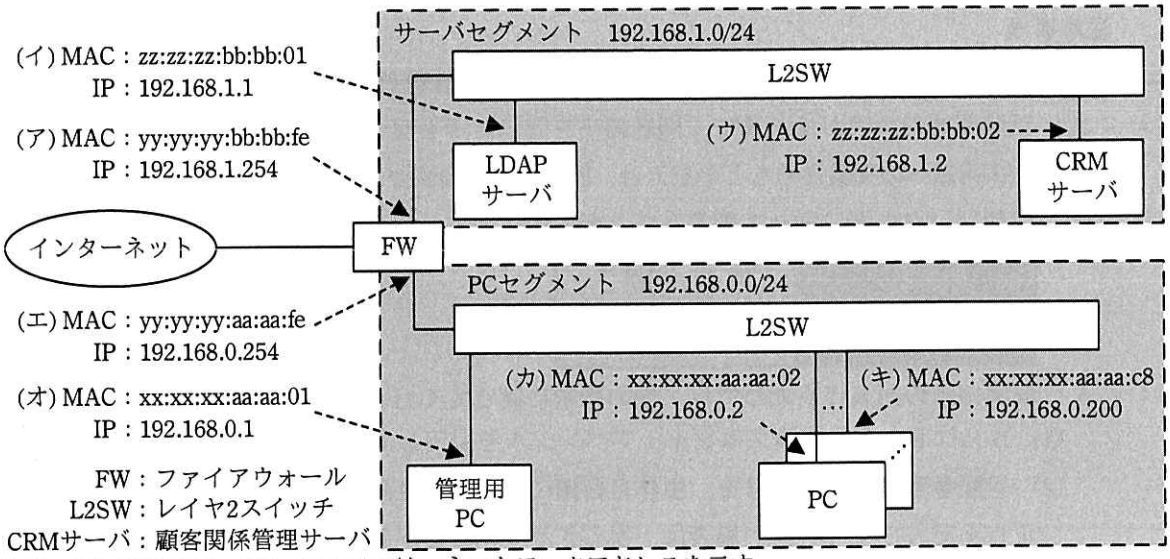
問1　社内で発生したセキュリティインシデントに関する次の記述を読んで，設問 1～3 に答えよ。

D 社は，従業員数 100 名のシステム開発会社である。D 社のネットワーク構成を図 1 に示す。



注記　192.168.0.0/24，192.168.1.0/24 は，ネットワークアドレスを示す。

図 1　D 社のネットワーク構成

D 社のネットワークでは静的に IP アドレスが付与され，各セグメント間の通信はステートフルパケットインスペクション型の FW で制限されている。FW のフィルタリングルールを表 1 に示す。

表 1　FW のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログの記録
1	PC セグメント	インターネット	HTTP, HTTP over TLS	許可	する
2	PC セグメント	LDAP サーバ	LDAP	許可	しない
3	PC セグメント	CRM サーバ	HTTP over TLS	許可	する
4	管理用 PC	サーバセグメント	SSH	許可	する
5	PC セグメント	サーバセグメント	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
20	全て	全て	全て	拒否	しない

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。

従業員には，個人ごとに PC と利用者 ID が割り当てられており，自身の PC 上では，自身の利用者 ID に対して管理者権限が付与されている。利用者 ID は，LDAP サーバで一元管理されており，PC にログインする際，LDAP サーバで利用者認証が行われる。D 社の顧客情報は全て CRM サーバに保管されており，営業業務に携わる従業員は，PC から Web ブラウザで CRM サーバにアクセスして，顧客情報の登録・参照を行っている。

サーバ及びFWは，入退室管理されたサーバルーム内に設置されている。利用者ID作成などのサーバの運用は，サーバ管理者が，事前申請をした上で，管理用 PC から SSH でサーバにログインして行っている。SSH でログインする際も PC にログインする際と同様に，LDAP サーバで利用者認証が行われる。

D 社では，事前申請なしで CRM サーバへの SSH によるログインがあった場合，そのことを日次のバッチ処理によって顧客情報管理責任者である N 部長に電子メールで通知する仕組みを導入している。通知にはログイン時刻，SSH の接続元 IP アドレス及び利用者 ID が記載される。

〔セキュリティインシデントの発生〕

ある日，サーバ管理者の Y 主任の利用者 ID で，管理用 PC から CRM サーバにログインしたことを示す通知が N 部長に届いた。N 部長が，Y 主任に確認したところ，その時間帯にはログインしていないとのことであった。

Y 主任が CRM サーバの SSH 認証ログを確認すると，身に覚えがない自分のログイン（以下，不審ログインという）の記録が残っていた。Y 主任の報告を受けて，N 部長は，不正侵入のセキュリティインシデント（以下，インシデントという）が発生したと判断し，インターネット接続を遮断した上で，セキュリティ専門業者 Z 社に調査を依頼した。

Z 社の W 氏が，サーバへの不正侵入の有無，侵入手口及び顧客情報窃取の有無に関する調査を進めることになった。

〔サーバへの侵入手口の調査〕

W 氏は，まずサーバへの不正侵入の有無及び侵入手口の調査を行った。その調査結果を図 2 に示す。調査結果から，W 氏は図 3 に示す手順でサーバへの不正侵入が行

われていたと推測した。

- 従業員 A さんの PC が遠隔操作型マルウェアに感染していたが，その他のサーバ及び PC のマルウェア感染は確認されなかった。
- A さんの PC に，ARP ポイズニングに使われるツールが削除された形跡があった。
- 不審ログインからログアウトまでの時間帯に，管理用 PC にログイン中の利用者はいなかった。
- 不審ログインがあった 5 分前に，LDAP サーバの SSH 認証ログに Y 主任の利用者 ID によるログインの記録があった。
- LDAP サーバ及び CRM サーバの SSH 認証ログに記録された接続元 IP アドレスは，全て管理用 PC の IP アドレスであった。

図 2　W 氏の調査結果

1. マルウェアに感染した A さんの PC を遠隔操作する。
2. A さんの PC 上で ARP ポイズニングを用いて，通信を盗聴する。
3. A さんの PC 上で通信を盗聴して，LDAP サーバ及び CRM サーバの IP アドレスを特定する。
4. A さんの PC 上で LDAP 通信を盗聴して，従業員の利用者 ID とパスワードを収集する。
5. A さんの PC から LDAP サーバ及び CRM サーバの SSH ポートへのアクセスを試みるが，アクセスに失敗する。
6. A さんの PC 上で通信を盗聴して，管理用 PC の IP アドレスを特定する。
7. A さんの PC 上で通信を盗聴して，サーバ管理者である Y 主任の利用者 ID とパスワードを入手する。
8. A さんの PC 上で管理用 PC の IP アドレスを詐称して，LDAP サーバ及び CRM サーバの SSH ポートにアクセスし，Y 主任の利用者 ID とパスワードでログインする。

図 3　W 氏が推測したサーバへの不正侵入手順（抜粋）

図 3 の 2 の通信が盗聴されている時点では，FW，管理用 PC 及び A さんの PC の ARP テーブルが，それぞれ表 2～4 に示すようになっていたと W 氏は推測した。

表 2　盗聴されている時点の FW の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.0.1	xx:xx:xx:aa:aa:02
192.168.0.200	xx:xx:xx:aa:aa:02

表 3　盗聴されている時点の管理用 PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.0.254	a

表4　盗聴されている時点のAさんのPCのARPテーブル（抜粋）

IPアドレス	MACアドレス
192.168.0.1	b
192.168.0.254	c

図3の6の特定方法としては，管理用PCのIPアドレスを総当たりで推測することも考えられるが，そのような方法が採られた場合にFWのフィルタリングルール d によって記録されるはずのログが残っていなかった。このことから，①通信の盗聴によって管理用PCのIPアドレスが特定されたとW氏は推測した。

〔顧客情報窃取の有無の調査〕

続いて，W氏は顧客情報窃取の有無を調査した。CRMサーバの顧客情報を窃取する手口として三つ考えられたので，それぞれ調査を行った。

一つ目は，不正侵入されたCRMサーバからの直接の情報窃取である。調査した結果，CRMサーバからの直接の情報窃取はなかったと判断した。

二つ目は，AさんのPCからAさんがCRMサーバにアクセスした際の，AさんのPC又は通信からの情報窃取である。調査した結果，AさんはCRMサーバにはアクセスしていないことがFWのログ及び聞き取りから確認できた。

三つ目は，その他のPCからCRMサーバにアクセスした際の通信からの情報窃取である。D社内のWebブラウザの設定は，②サーバ証明書の検証に失敗した場合は接続しない設定にしている。このことから，CRMサーバにアクセスした際の通信からの情報窃取はなかったと判断した。

W氏は更に調査した結果，顧客情報の窃取はなかったとN部長に報告した。

〔セキュリティ対策の実施〕

Y主任は今回のインシデントを受けて，まず，マルウェアの駆除，ARPテーブルの初期化，全利用者IDのパスワード変更などの暫定対応を行った。その後，W氏の助言を受けながら，今回のように社内ネットワークに侵入された場合の被害拡大を防ぐために，社内ネットワークにおいて，二つのセキュリティ対策を実施することにした。

第一に，図3の8を防ぐために，図4のようにネットワーク構成を変更し，表5のようにFWのフィルタリングルールを変更することにした。これらの変更によって，③図3の6が行われることも防ぐことができる。また，④仮に図3の6とは異なる方法で管理用PCのIPアドレスが特定され，図3の8が試みられた場合でも，TCPコネクションの確立を防ぐことができる。

第二に，図3の4を防ぐために，LDAPサーバへの通信ではLDAP over TLSを利用することにした。

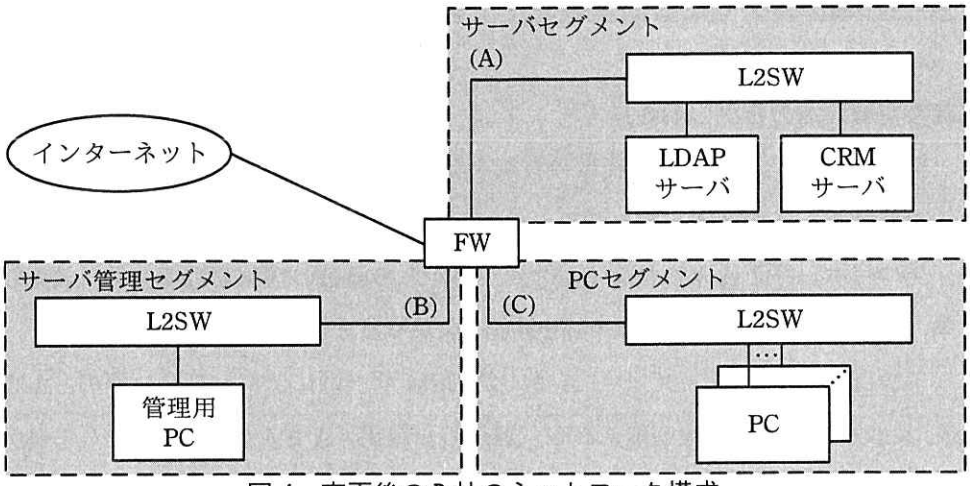


図4　変更後のD社のネットワーク構成

表5　変更後のFWのフィルタリングルール

項番	送信元	宛先	サービス	動作	ログの記録
1	PCセグメント	インターネット	HTTP, HTTP over TLS	許可	する
2	PCセグメント	LDAPサーバ	LDAP over TLS	許可	しない
3	PCセグメント	CRMサーバ	HTTP over TLS	許可	する
4	管理用PC	サーバセグメント	SSH	許可	する
5	PCセグメント	サーバセグメント	全て	拒否	する
6	PCセグメント	サーバ管理セグメント	全て	拒否	する
7	サーバ管理セグメント	脆弱性修正プログラム提供元, ウイルス定義ファイル提供元	HTTP over TLS	許可	する
8	サーバ管理セグメント	LDAPサーバ	LDAP over TLS	許可	する
9	サーバ管理セグメント	PCセグメント	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
24	全て	全て	全て	拒否	しない

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。

これらの対策は N 部長によって承認され，今回と同様のインシデントに対する社内ネットワークのセキュリティ耐性が高まることになった。

設問1　〔サーバへの侵入手口の調査〕について，(1)～(3)に答えよ。

(1)　表 3 中の [a] 及び表 4 中の [b]，[c] に入れる適切な字句を，図 1 中の機器の MAC アドレスから選び，(ア)～(キ)の記号で答えよ。

(2)　本文中の [d] に入れる適切なフィルタリングルールを，表 1 中の項番 1～5 から選び，数字で答えよ。

(3)　本文中の下線①について，攻撃者が管理用 PC の IP アドレスを特定するために盗聴したのはどのような通信か。送信元，宛先及びサービスを，それぞれ解答群の中から選び，記号で答えよ。

解答群

ア　ARP	イ　A さんの PC	ウ　FW
エ　HTTP over TLS	オ　LDAP	カ　LDAP サーバ
キ　SSH	ク　インターネット	ケ　管理用 PC

設問2　本文中の下線②について，このような設定にすることは，A さんの PC に侵入した攻撃者によって行われるどのような攻撃への対策になるか。攻撃名を 10 字以内で答えよ。また，攻撃に際して詐称される対象の機器名を図 1 中から選び，答えよ。

設問3　〔セキュリティ対策の実施〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，防ぐことができる理由を 35 字以内で具体的に述べよ。

(2)　本文中の下線④について，TCP コネクション確立開始時の SYN パケットと SYN-ACK パケットはそれぞれどのような経路をたどるか。図 4 中の経路を通過する順に選び，(A)～(C)の記号で答えよ。