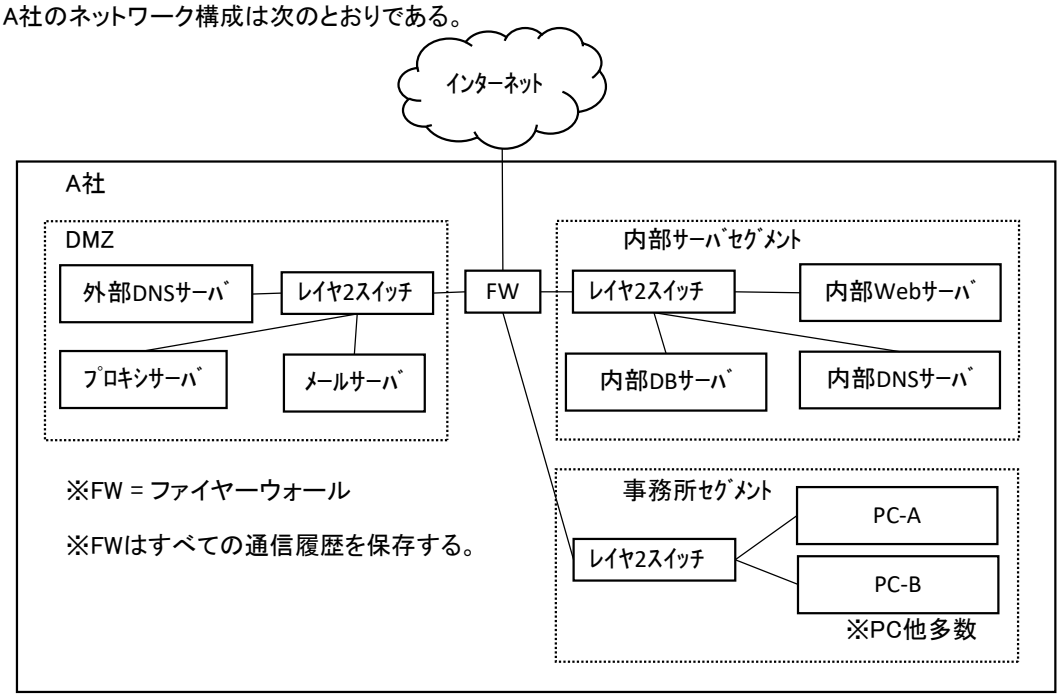
A社は従業員約200名の卸売業者である。多くの顧客情報を保有している。
A社のネットワーク構成は次のとおりである。



FWのフィルタリングルールは次のとおり。

No	送信元	宛先	プロトコル	動作
1	事務所ｾｸﾞﾒﾝﾄ	DMZ	HTTP , HTTPS , DNS , POP , SMTP	許可
2	事務所ｾｸﾞﾒﾝﾄ	内部ｻｰﾊﾞｾｸﾞﾒﾝﾄ	HTTP , HTTPS , DNS	許可
3	ｲﾝﾀｰﾈｯﾄ	DMZ	SMTP	許可
4	DMZ	ｲﾝﾀｰﾈｯﾄ	HTTP , HTTPS , SMTP	許可
5	全て	全て	全て	拒否

※Noの昇順にルールが摘要される。
※許可された通信に対するレスポンスは無条件に許可する。

機器の詳細は次のとおり。

機器	詳細
ﾌﾟﾛｷｼｻｰﾊﾞ	PCからｲﾝﾀｰﾈｯﾄへのHTTP , HTTPSを中継する。PCからｲﾝﾀｰﾈｯﾄにアクセスする際、利用者はIDとパスワードを入力し、ﾌﾟﾛｷｼｻｰﾊﾞによるBASIC認証を受ける必要がある。
PC	マルウェア対策ソフトが導入されている。同ソフトは、PC内のファイルのハッシュ値を同ソフトの開発元ベンダーに問い合わせる。ハッシュ値がマルウェアであるとして、ベンダーに登録されている場合は、警告を発する(以降、これをマルウェアチェックと呼ぶ)。

2021年7月、次の時系列順でPC-Aにインシデントが発生したことが認められた。

1: 7/11、PC-A上で、マルウェア対策ソフトによるマルウェアチェックが行われたが、警告は
発生しなかった。
2:7/15、PC-A上で、マルウェア対策ソフトによるマルウェアチェックが行ったところ警告が発生した。
同PC上にマルウェアの疑いがあるファイルが存在することが確認された。
3:7/15、PC-Aの利用者に聴取を行ったところ、7/8にメールに添付されたファイルを開いた事が確認できた。
同ファイルがマルウェアのインストーラーである可能性が濃厚となった。
4:7/16、7/15に検知したマルウェアは、ｲﾝﾀｰﾈｯﾄ上のC&Cｻｰﾊﾞから指令を受け、侵入先の重要情報を
盗み出す「マルウェアX」であることがわかった。

マルウェアXの挙動はつぎの通りであることが判明している。
・感染先のPCから、C&Cｻｰﾊﾞに向け指示を要求するHTTPリクエストを送信する。これを受けたC&Cｻｰﾊﾞは
　PCから接続可能なｾｸﾞﾒﾝﾄ上の情報を収集し、C&Cｻｰﾊﾞに送信する命令を出す。
C&Cｻｰﾊﾞ のIPｱﾄﾞﾚｽは判明している。

A社情報システム部は、顧客情報が流出した可能性を危惧し調査を実施した。その結果、顧客情報が
流出した可能性が高いことが判明した。ﾌﾟﾛｷｼｻｰﾊﾞのログから、流出した日は7/10であることが濃厚である。
ただ、7/8よりPC-AからC&Cｻｰﾊﾞに対し情報を送信しようとした痕跡が、多く確認できた。

問10
7/11時点にPC-Aの感染を検知できなかったか理由を、情報システム部は次のように判断した。
A、Bに当てはまる語句として適切な組み合わせはいずれか？

7/11時点ではウイルス対策ソフトの開発元ベンダーに「A」の「B」が登録されていなかった。

1. A：C&Cｻｰﾊﾞ　B：ハッシュ値
2. A：C&Cｻｰﾊﾞ　B：暗号化データ
3. A：マルウェアX　B：ハッシュ値
4. A：マルウェアX　B：暗号化データ

問11
7/8から情報をC&Cｻｰﾊﾞに送ろうとしていたに関わらず、7/10までそれができなかった理由を情報システム部は
次のように判断した。A、Bに当てはまる語句として適切な組み合わせはいずれか？

マルウェアXが7/10に至るまで、「A」による「B」に成功することができなかった。

1. A：外部DNSｻｰﾊﾞ　B：バックアップ
2. A：外部DNSｻｰﾊﾞ　B：認証
3. A：ﾌﾟﾛｷｼｻｰﾊﾞ　B：バックアップ
4. A：ﾌﾟﾛｷｼｻｰﾊﾞ　B：認証

問12
情報システム部は、次の理由により7/10からC&Cサーバへの情報流出が開始されたことに気づいた。
A、Bに当てはまる語句として適切な組み合わせはいずれか？

FWに「A」から「B」に対する通信記録が残されていた。

1. A：ﾌﾟﾛｷｼｻｰﾊﾞ　B：C&Cｻｰﾊﾞ
2. A：ﾌﾟﾛｷｼｻｰﾊﾞ　B：内部Webｻｰﾊﾞ
3. A：ﾒｰﾙｻｰﾊﾞ　B：C&Cｻｰﾊﾞ
4. A：ﾒｰﾙｻｰﾊﾞ　B：内部Webｻｰﾊﾞ

問13
なぜ7/10からC&Cｻｰﾊﾞに対する情報送信が可能となった理由として、マルウェアXは7/10に至るまで
次の動作を行っていたと結論づけられた。
A、Bに当てはまる語句として適切な組み合わせはいずれか？

「A」上の「B」を行っていた。

1. A：外部DNSｻｰﾊﾞ　B：ファイル探索
2. A：ネットワーク　B：盗聴
3. A：ﾌﾟﾛｷｼｻｰﾊﾞ　B：CPU負荷確認
4. A：内部DNSｻｰﾊﾞ　B：ファイル探索

問14
恒久的な対策が完了するまでの暫定策として、フィルタリングルールの一部を変更することにした。
変更の内容として適切なものはどれか？
なお、感染によって発生したインシデントのみに対応するものとし、予防的な措置はとらない。

1.DMZからインターネットへのHTTP通信を許可するルールを削除
2.事務所ｾｸﾞﾒﾝﾄからDMZへのHTTP通信を許可するルールを削除
3.DMZからインターネットへのHTTPS通信を許可するルールを削除
4.事務所ｾｸﾞﾒﾝﾄからDMZへのHTTPS通信を許可するルールを削除