再帰的クエリを送信し、C&C 通信が確立される。したがって、 b には「権威 DNS サーバ」、 d には「再帰的クエリ」が入る。

(5) DNS トンネリング攻撃の特徴として、攻撃者が用意した権威 DNS サーバのホスト名にはランダムな長い文字列が使われる。また、大量の情報を持ち出す場合には、攻撃者が用意した DNS サーバとの間で多数の DNS クエリが発生することになる。したがって、大量の情報を持ち出す場合の特徴として「長いホスト名を持つ DNS クエリの発生」と「特定のドメインに対する多数の DNS クエリの発生」が挙げられる。

＜問３＞　標的型攻撃への対応

●設問 1

［試験センターによる解答例］

(1) メモリ上の情報が失われないようにするため（20 字）

(2) ・J 社情報システムに感染を拡大する。(17 字)
・インターネットに情報を送信する。(16 字)

(1) マルウェアが活動状態にある PC では、不審なプロセス等がメモリ上に存在している可能性が高い。また、ファイルは一切残さず、メモリ上にのみ存在するタイプのマルウェアも多い。当該 PC の電源を切ってしまうと、メモリの情報が失われ、マルウェアの存在や痕跡、特徴等を調査することが困難になってしまう可能性がある。そうならないように、不審 PC の電源を入れたままにしておくことで、メモリ上の情報が失われないようにしているのである。

(2) 不審 PC を利用者 LAN から切り離さないと、マルウェアがネットワークを通じて被害を拡大させる可能性が高い。マルウェアの典型的な活動内容として、LAN に接続された他の PC、サーバ等、J 社情報システムに感染を拡大することが考えられる。また、インターネット上の C&C サーバ等に接続し、感染した PC 内の情報や、当該 PC からアクセス可能なサーバ等にある情報を送信することが考えられる。それ以外にも感染した PC からアクセス可能なサーバ等のファイルを暗号化する、LAN 内を流れるパケットを盗聴する等、様々な活動が考えられるが、J 社にとって望ましくないという点からすると、感染拡大とインターネットへの情報送信の二点が解答として適切だろう。

●設問２

［試験センターによる解答例］

a：ウ
b：イ
c：オ
d：ア

a：“ipconfig”は、ネットワークアダプタの設定情報を取得するコマンドである。“/all”オプションを付けることで、攻撃者は L-PC の IP アドレス、サブネットマスク、デフォルトゲートウェイ、MAC アドレスなど、詳細な情報を確認することができる。

b：“systeminfo”は、ホスト名、OS 名、OS バージョン、BIOS バージョン、脆弱性修正プログラムの適用状況など、システムに関する詳細な情報を取得するコマンドである。これにより、攻撃者は L-PC 内で悪用できる脆弱性の有無を確認することなどができる。

c：“tasklist”は、実行中のプロセス（タスク）の一覧を取得するコマンドである。攻撃者は、サンドボックスと関連するプロセスの有無により、マルウェアの解析環境でないかを確認する。

d：“net view”は、当該 PC と同じワークグループやドメインに所属するコンピュータを一覧表示するコマンドである。これにより、攻撃者は L-PC からその時点で接続可能なコンピュータを確認することができる。

●設問３

［試験センターによる解答例］

(1) e：IP アドレス w1.x1.y1.z1 との通信履歴（23 字）

(2) 感染したが、C&C サーバと通信する前にネットワークから切り離された状態（35 字）

(3) R ログをマルウェア M のハッシュ値で検索する。(22 字)

(1) G さんが調査したのは、P サービスから通知を受けた L-PC の範囲にとどまっているが、L さんと同様にマルウェア M に感染している PC やサーバ等がないかについて調査する必要がある。これを FW のログから調査するには、13:17:15 より以前のログに、P サービスから通知された C&C サーバの IP アドレスである“w1.x1.y1.z1”との通信履歴が含まれていないかを確認するのが有効である。

(2) FW のログを使った調査では、マルウェア M に感染した PC やサーバがインターネット上の C&C サーバと通信した場合のみ検知が可能である。マルウェア M に感染したとしても、当該機器が C&C サーバと通信する前にネットワークから切り離された状態であったり、電源が切られたりしている可能性がある。また、ネットワークに接続されていても、マルウェア M がまだ C&C サーバとは通信しておらず、初期調査や探索活動のために当該機器や周辺の PC から情報収集中であることも考えられる。

(3) 表 1 の R システムの概要にあるように、R システムは、PC やサーバの全てのプロセスの生成から終了までの動作や実行したプログラムのハッシュ値、通信履歴等をログとして取得するとともに、管理サーバに登録されたハッシュ値を持つマルウェアの実行を禁止することができる EDR (Endpoint Detection and Response) 製品である。R ログには上記のようなプロセスの活動履歴や通信履歴等が記録されており、マルウェアのハッシュ値で検索することによって、当該マルウェアが実行された痕跡があるかどうか調査することができる。したがって、マルウェア M に感染している PC やサーバを R ログを使って検知するには、マルウェア M のハッシュ値で検索すればよい。