問2　セキュリティインシデント対応に関する次の記述を読んで，設問1～4に答えよ。

Z社は，Network Attached Storage（NAS）製品，ルータ製品などのネットワーク機器を開発，保守している従業員200名の会社であり，国内の中小企業の顧客を中心に事業を展開している。NAS製品である製品Xは，ファイル共有の用途で利用され，ルータ製品である製品Yは，インターネット接続の用途で利用されている。製品X及び製品Yは，LinuxをベースとしたOSを搭載している。

Z社では，インターネットドメイン名z-sha.co.jpを取得している。製品Xの利用者は，インターネットからWebインタフェース経由で自身の製品Xにアクセスするに際して，Z社が提供しているダイナミックDNSサービス（以下，DDNS-Zという）を利用することができる。

〔障害の発生〕

ある日，製品Xと製品Yを利用しているA社から，Z社の保守サポート窓口に障害の報告が入った。製品X（以下，A社に設置された製品XをNAS-Aという）上のファイルにおいて，ファイル名は表示されるがファイルを開くことができないとのことであった。

障害報告によると，A社は，オフィス環境のデザイン及び施工を行う従業員30名の会社であり，デザインデータのファイルをNAS-Aに保存して社内で共有している。在宅勤務者の増加に伴い，7日前に，NAS-A及び製品Y（以下，A社に設置された製品Yをルータ-Aという）の設定を変更して，A社の従業員の自宅からNAS-A上のファイルにアクセスできるようにしていた。

〔NAS-A及びルータ-Aの調査〕

Z社の保守サポート課のK氏は，A社の障害調査を担当することになった。

NAS-Aは，DDNS-Zを使用して，https://nas-a.z-sha.co.jp/のURLでアクセスできるようになっていた。ルータ-Aのグローバル IPアドレスが変更された場合，Z社のDNSサーバの設定でホスト名nas-aに割り当てているIPアドレスを変更するために，［　a　］レコードを更新する。そのレコードの［　b　］は，300秒に設定されていた。

A 社のネットワーク構成を図 1 に，NAS-A の設定内容を表 1 に，ルータ-A の設定内容を表 2 に示す。

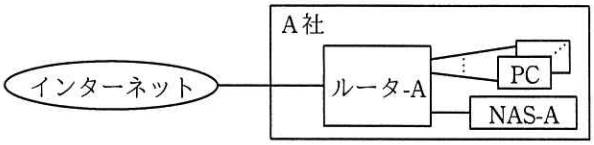

図 1　A 社のネットワーク構成（抜粋）

表 1　NAS-A の設定内容（抜粋）

設定項目	設定値	説明
ファイル共有機能	・SMB：有効 ・NFS：無効	有効に設定したプロトコルで，ファイルを共有する。
UPnP [1] 設定要求機能	・有効 ・製品 Y の WAN 側 TCP ポート：443 ・NAS-A の TCP ポート：443	左記の設定にすると，製品 Y の WAN 側ポート宛てのパケットを NAS-A のポートにフォワードする設定を製品 Y に要求する。
Web 操作機能	・有効	Web ブラウザから HTTPS で，一般利用者権限のアカウントで本機能にログイン後，ファイルの操作ができる。
Web 管理機能	・有効	Web ブラウザから HTTP で，管理者権限のアカウントで本機能にログイン後，NAS-A の設定変更などができる。

注 [1]　Universal Plug and Play の略称。認証なしでリクエストを受け付ける仕様のプロトコルである。

表 2　ルータ-A の設定内容（抜粋）

設定項目	設定値	説明
ファイアウォール機能	・インバウンド通信：全て拒否 [1] ・アウトバウンド通信：全て許可	ステートフルパケットインスペクション型である。
UPnP 機能	・LAN 側：有効	LAN 側の機器から受け付けたリクエストの内容で，ポートフォワーディングの設定とファイアウォール機能の設定を行う。① WAN 側は，本機能を有効にできない仕様になっている。

注記　ルータ-A がインターネットに接続するための ISP 回線では，グローバル IP アドレスが動的に割り当てられる。

注 [1]　UPnP 機能による設定が優先される。

K 氏が NAS-A を調査した結果，次のことが分かった。

・デザインデータのファイルが暗号化され，ファイル名の拡張子が変更されていた。

・A 社では身に覚えのない，英語で書かれた脅迫文のテキストファイルが，NAS-A に

保存されていた。

・ファイル共有機能でも Web 操作機能でもアクセスできない /root ディレクトリ配下のファイルも暗号化されていた。

K 氏は，今回の障害がランサムウェアに起因するものであり，さらに，②A 社の PC がランサムウェアに感染したのではなく，NAS-A 自体がランサムウェアに感染したことによって NAS-A のファイルが暗号化された可能性が高いと判断した。そこで，脆弱性，アクセスログ，DDNS-Z の三つの観点から更に調査を進めることにした。

〔脆弱性の調査〕

NAS-A における脆弱性修正プログラムの適用状況を確認したところ，数週間前にリリースされた製品 X の脆弱性修正プログラム（以下，パッチ M という）が未適用であった。パッチ M は，Web 管理機能に関する二つの脆弱性（以下，脆弱性 1 と脆弱性 2 という）について対策したものである。脆弱性 1 及び脆弱性 2 の概要を図 2 に示す。

脆弱性 1

製品 X では，除外リスト[1)]に次のディレクトリが指定されている。

```
/css
/images
/js
```

認証なしアクセスの処理に脆弱性があり，除外リストに指定されていないディレクトリ配下のファイルにも認証なしでアクセスできてしまう。例えば，http://192.168.0.1/images/..%2fstatus.cgi の URL にアクセスすると，http://192.168.0.1/status.cgi に認証なしでアクセスできてしまう。これは，URL に“..%2f”を使用した［ c ］と呼ばれる攻撃手法である。

脆弱性 2

製品 X には，Web 管理機能の一つとして，IP アドレスを指定して ping を実行する機能がある。この IP アドレスの処理に脆弱性があり，任意の OS コマンドを実行できてしまう。次は，その脆弱性を悪用した例であり，“ping 127.0.0.1;whoami”というコマンドが実行される。

```
POST /ping.cgi HTTP/1.0
Content-Length: 21

addr=127.0.0.1;whoami
```

図 2　脆弱性 1 及び脆弱性 2 の概要

これは，[d] と呼ばれる攻撃手法である。脆弱性 1 と脆弱性 2 を組み合わせると，認証なしで任意の OS コマンドの実行が可能になる。次は，その例である。

```
POST /images/..%2fping.cgi HTTP/1.0
Content-Length: 21

addr=127.0.0.1;whoami
```

注 [1] 除外リストに指定されたディレクトリ配下のファイルには，認証なしでアクセスできる。除外リストは，利用者が変更できない。

図 2　脆弱性 1 及び脆弱性 2 の概要（続き）

パッチ M では，脆弱性 1 の対策として，認証なしアクセスの処理の流れにパス名の正規化の処理を加え，さらに，図 3 に示す順序にした。パス名の正規化とは，相対パスで記述されたパス名を，相対パス記法を含まない形式に変換することである。

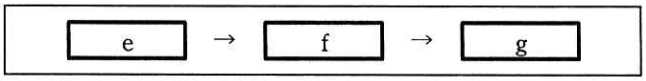

図 3　パッチ M 適用後の認証なしアクセスの処理の流れ

〔アクセスログの調査〕

NAS-A のアクセスログを調査したところ，外部から HTTPS リクエストを使用して OS コマンドを実行する攻撃ツール（以下，WebShell という）が NAS-A に配置されており，OS コマンドが実行されたことが分かった。NAS-A のアクセスログから WebShell に関連するものを抽出した結果を表 3 に示す。

表 3　WebShell に関連する NAS-A のアクセスログ

No.	時刻	リクエスト	ステータスコード	応答バイト数
1	13:01	GET /images/..%2fstatus.cgi HTTP/1.1	200	634
2	13:02	POST /images/..%2fping.cgi HTTP/1.1	200	418
⋮	⋮	⋮	⋮	⋮
18	13:05	GET /images/shell.cgi?cmd=whoami HTTP/1.1	200	1418
⋮	⋮	⋮	⋮	⋮
89	13:18	POST /images/shell.cgi HTTP/1.1	200	2490

注記　一部の項目は省略している。

表 3 からは，GET メソッドを使用して実行された OS コマンドの内容は分かったが，③POST メソッドを使用して実行された OS コマンドの内容は分からなかった。WebShell が配置されたディレクトリは，書込み不可であるが，root アカウントを用いれば書込み可能に変更できる。製品 X では，sudo コマンドの設定ファイルが図 4 のようになっている。

```
www ALL=NOPASSWD: /bin/tar
```

図 4　sudo コマンドの設定ファイル（抜粋）

tar コマンドは，標準の OS コマンドであり，複数のファイルを一つのアーカイブファイルにまとめたり，アーカイブファイルを展開したりできる。製品 X では，ファームウェアのアップデート時，www アカウントの権限で sudo コマンドを使用して tar コマンドを実行することで，root アカウントの権限でアーカイブファイルを展開している。この tar コマンドには，任意の OS コマンドを実行できるオプションがある。ただし，ファームウェアのアップデート時にこのオプションは使用していない。当該オプションを悪用する例を図 5 に示す。

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=whoami
```

図 5　tar コマンドのオプションを悪用する例

K 氏は，“攻撃者が，Web 管理機能の脆弱性と tar コマンドのオプションを悪用し，書込み不可のディレクトリを書込み可能に変更して WebShell を配置した後，WebShell を使用してランサムウェアを実行した”と推測した。そこで，④製品 X で tar コマンドのオプションが悪用されるのを防ぐ対策を検討することにした。

〔DDNS-Z の調査〕

DDNS-Z を使用して製品 X にアクセスするための URL は，インターネットの検索エンジンで特定のキーワードを検索すると容易に見つけることができてしまい，攻撃対象になりやすいことが分かった。インターネットの検索エンジンで検索されないようにするために，各 Web ページの<head>セクションに<meta name="robots" content="[h]">を記載することを検討した。

これまでの検討を踏まえ，A 社及び Z 社は必要な対策に着手した。

設問 1　〔NAS-A 及びルータ-A の調査〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　A　　イ　MX　　ウ　TLS

エ　TTL　　オ　TTY　　カ　TXT

(2) 表 2 中の下線①について，WAN 側で UPnP 機能を有効にできる仕様とした場合，ルータ-A が操作されることによって，どのようなセキュリティ上の問題が発生するか。発生する問題を，30 字以内で述べよ。

(3) 本文中の下線②のように判断した理由を，40 字以内で述べよ。

設問 2　〔脆弱性の調査〕について，(1)～(3)に答えよ。

(1) 図 2 中の［ c ］に入れる適切な字句を，15 字以内で答えよ。

(2) 図 2 中の［ d ］に入れる適切な字句を，15 字以内で答えよ。

(3) 図3中の［ e ］～［ g ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　URL デコード　　イ　除外リストとの比較

ウ　パス名の正規化

設問 3　〔アクセスログの調査〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，実行された OS コマンドの内容が分からなかった理由を，35 字以内で述べよ。

(2) 本文中の下線④について，対策を，50 字以内で具体的に述べよ。

設問 4　本文中の［ h ］に入れる適切な字句を，英字 10 字以内で答えよ。