問1　インシデント対応体制の整備に関する次の記述を読んで，設問1～5に答えよ。

N社は，従業員800名のドラッグストアチェーンである。グローバルに事業を展開する海外の企業B社のブランドライセンスを取得し，同ブランドの下，国内80店舗の展開，及びN社Webサイト（以下，通販サイトという）での通信販売を行っている。N社は，消費者向けの会員制度を設けており，会員は商品購入時に特典を受けられる。N社の組織図を図1に示す。

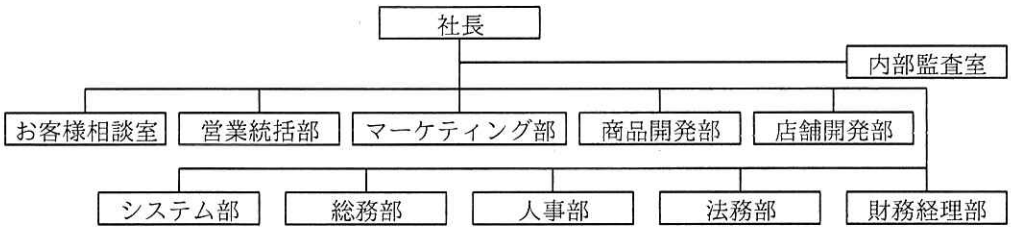


図1　N社の組織図

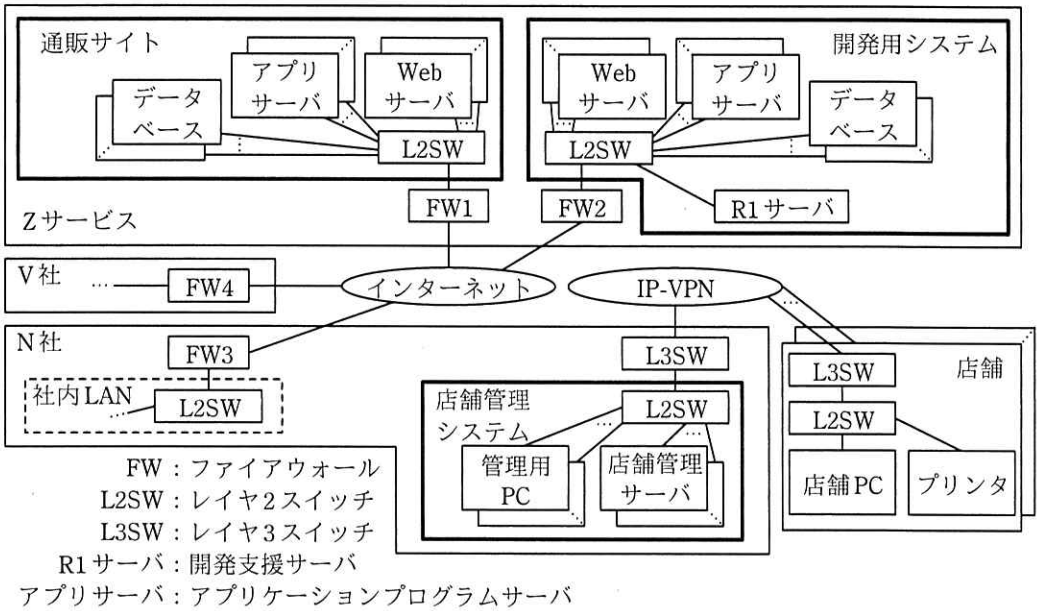
N社は，情報セキュリティ委員会を設置している。同委員会は，経営陣が委員となり，情報セキュリティについての基本方針（以下，基本方針という）及び重要な課題を取り扱う。セキュリティ対策は主にシステム部が担っており，セキュリティインシデント（以下，インシデントという）が発生した場合は，対応チームを立ち上げて対応する。基本方針では，消費者に影響を与えるインシデントの場合，社外に向けて速やかに情報開示することを挙げている。

B社は，同社がブランドライセンスを提供する店舗運営会社を対象にしたインシデント対応ポリシ（以下，B社インシデント対応ポリシという）を定めている。B社インシデント対応ポリシは，インシデントによるB社ブランドの毀損を最小限にすることを目的として策定された。

N社は，B社インシデント対応ポリシを順守する契約をB社と締結しており，N社でインシデントが発生した場合は，B社のセキュリティ担当部署（以下，B社セキュリティ部という）に報告し，指示に基づき対応する。分析対象となるログは，N社のシステム部が取得し，インシデント発生時にはB社セキュリティ部に送信する。

通販サイトは，Z社が提供するクラウドサービス（以下，Zサービスという）上に

構築し，設計，開発及び運用をV社に委託している。Zサービス上には開発用システムも構築している。また，各店舗の情報を一元管理し，運営を支援するためのシステム（以下，店舗管理システムという）をN社に設置しており，設計，開発及び運用の一部を外部に委託している。N社が利用するシステム及びネットワークの概要を図2に，開発用システムの概要を図3に，N社の脆弱性管理プロセスを図4に示す。



注記1　Zサービス上の機器及びネットワークは，仮想化技術で実現されるものを含む。

注記2　店舗管理システムと店舗との間は，IP-VPNで接続されている。一方，店舗管理システムと社内LANとは，ネットワークが分離されている。N社の関係部門は，管理用PCを操作して店舗管理サーバを利用する。また，店舗管理システムと社内LANとの間でデータの受渡しが必要な場合は，USBメモリを用いる。

注記3　店舗では，店舗PCからIP-VPN経由で店舗管理サーバを利用する。また，販売促進施策の検討などのため，店舗PCは，Wi-Fiルータなどでインターネットに接続する。

注記4　割り当てられたグローバルIPアドレスの範囲は，次のとおりである。

- N社　　：x1.y1.z1.0/28
- V社　　：x2.y2.z2.128/30
- 通販サイト　：x3.y3.z3.0/28
- 開発用システム：x4.y4.z4.0/28

図2　N社が利用するシステム及びネットワークの概要

(1) 開発用システムの接続制御
・N 社及び V 社はインターネットを介して，HTTP 及び HTTPS を用いた接続（以下，HTTP 接続という）を行い，システムのテストを行う。
・N 社及び V 社はインターネットを介して，R1 サーバに SSH 接続を行い，開発業務を行う。R1 サーバ以外の開発用システム内にあるサーバ（以下，他サーバ群という）を操作する場合は，R1 サーバから SSH 接続を行う。
・インターネットからのインバウンド通信は，FW2 において，各サーバへの SSH 接続及び HTTP 接続を許可し，その他の通信を遮断している。また，インターネットへのアウトバウンド通信は，R1 サーバからの通信だけを許可し，その他の通信を遮断している。
・開発用システムと通販サイトの間には，通信経路は存在しない。通販サイトにプログラムを配備する際は，開発用システムから該当するプログラムを取得し，V 社環境から配備を行う。
(2) R1 サーバの構成
・R1 サーバに導入されているソフトウェアは，OS，SSH サーバプログラム，及び Web インタフェースをもつ開発支援ツール J である。
・開発支援ツール J は，OS の一般利用者権限を割り当てた利用者アカウントで動作する。OS の一般利用者権限には，開発支援ツール J が動作するための，必要最小限の権限だけが与えられている。
・R1 サーバには，ソースコード，バイナリコード，テスト用データなどを保存しているが，会員情報，取引情報などの秘密情報は保持していない。
(3) R1 サーバへの接続制御
・R1 サーバの“/etc/hosts.allow”ファイルの設定において，SSH 接続の接続元を N 社と V 社に限定している。このファイルの変更には，管理者権限が必要である。
・SSH 接続で R1 サーバにログインするための認証情報は，“/etc/shadow”ファイルに格納されている。具体的には，利用者アカウント，利用者アカウントごとに異なるソルト値，及びソルト値と平文パスワードから計算したハッシュ値が含まれている。
・HTTP 接続で開発支援ツール J を操作できる。接続制限は行っていない。
(4) 他サーバ群の概要
・他サーバ群では，それぞれの目的に必要なソフトウェアに加え，SSH サーバプログラムが動作している。他サーバ群それぞれの“/etc/hosts.allow”ファイルでは，SSH 接続の接続元を R1 サーバに限定している。また，他サーバ群それぞれには，複数の利用者アカウントが登録されている。
(5) 開発用システムにおけるセキュリティ対策
・WAF や改ざん検知の仕組みは，各種テストに支障を来す可能性があり，導入していない。
・開発用システムで作成されたソフトウェアは通販サイトに配備する前に脆弱性診断を行う。

unixでは、一般権限でアクセスできる /etc/password と 管理権限が必要な /etc/shadowがあること知っていなければ、解答できません

図 3　開発用システムの概要（抜粋）

（ア） 4 日に 1 回以上の頻度で脆弱性情報を収集する。
（イ） （ア）で収集した脆弱性情報を基に，脆弱性が悪用される可能性を評価する。
（ウ） （イ）で，悪用される可能性が高いと判断した場合は，悪用されたときの N 社のシステムへの影響を評価する。
（エ） （ウ）の評価の結果，対応が必要であると判断した場合は，対応方法，対応の優先度，対応期限を決定する。

図 4　N 社の脆弱性管理プロセス

〔インシデントの発生と対応〕

ある日，複数の会員から N 社のお客様相談室に，身に覚えのない商品購入を知らせる電子メールが届いたという連絡があった。N 社は，対応チームを立ち上げて調査した結果，通販サイトが不正アクセスを受けたと判断した。N 社は，直ちにこのインシデント（以下，インシデント P という）を B 社セキュリティ部に報告した。N 社と B 社セキュリティ部が協力して対応したが，問題が幾つか発生し，対応を終えるまでに 1 か月掛かった。

インシデント P について，判明した被害状況及び対応の概要を図 5 に示す。

(1) 被害状況
- 16 名の利用者 ID が不正ログインされ，総額 130 万円の商品が不正に購入されたことが判明した。 外部から入手した利用者IDとパスワードの組みのリストを使ってログインを試行する攻撃
- ログの調査から，①パスワードリスト攻撃と推定された。
- 攻撃の接続元 IP アドレスは五つであった。

(2) 対応
- 不正に購入された商品の半数は，注文及び発送を取り消した。
- 不正ログインされた 16 名の利用者 ID について，パスワードを強制的にリセットした。
- ②パスワードリスト攻撃の被害を防ぐ上で必要な，パスワードの安全な設定方法を全会員に案内した。他のサービスで利用したパスワードとは別のものを設定すること
- 通販サイトに不正アクセスがあったことを情報開示した。
- 認証に対する攻撃を検知するため，次の二つの仕組みを通販サイトに導入した。
  - 同じ IP アドレスから行われる多数のログイン試行を攻撃と判断する。
  - 一定時間ごとの認証失敗数を記録し，特定のしきい値を超えた場合は，攻撃と判断する。
- ③ログインが普段と異なる環境から行われた場合，会員が事前に登録した電子メールアドレスにその旨を通知する仕組みを通販サイトに導入した。

(3) 対応を通じて顕在化した課題 ・IPアドレスからわかる地理的位置について、過去のログインのものとの違いを確認する ・WebブラウザのCookieを利用し、過去のログインした端末化を判定する
- B 社セキュリティ部がログを分析した際に誤解が生じた。N 社が提供したログの大半は，記録されていた時刻情報の［ a ］が日本標準時であり，協定世界時に対し時刻情報が［ b ］時間進んだ値で記録されていた。しかし，協定世界時で記録されていたログや，［ a ］を示す情報が記録されていなかったログも存在した。
- B 社インシデント対応ポリシでは，インシデントに関わる情報を不特定多数に情報開示するのは法令に規定されているなどの幾つかの場合だけであった。そのため，N 社は速やかな情報開示を要望したものの，当初，B 社から認められなかった。N 社社長から B 社の経営陣に特別な要請を行うことによって，ようやく情報開示が認められた。しかし，情報開示のタイミングが遅くなり，N 社の基本方針にはそぐわなかった。

図 5　判明した被害状況及び対応の概要

〔インシデント対応方法の変更〕

インシデントPの対応が一段落した後，N社の経営陣は，N社で今後インシデントが起きた場合には，N社の基本方針に従って対応する契約に変更したいとB社に申し入れた。B社は，この申入れに対し，次の条件を満たすことを前提として了承した。

条件1：N社は，ISO/IEC 27001を利用して，自社の情報セキュリティ対策を評価し，その結果と対策案についてB社の了承を得る。

条件2：N社は，B社の支援なしにインシデント対応を行う体制を整備し，その体制についてB社の了承を得る。

条件3：N社は，インシデント対応後，B社に事後報告を行う。ただし，両社で別途定める基準によって，B社ブランドを著しく毀損するインシデントと判断された場合は，直ちにB社に報告し，対応を協議する。

N社は，条件1～3を含め，包括的なインシデント対応体制を実現するプロジェクトを発足させた。システム部のG部長を責任者に，システム部のHさんを担当者にそれぞれ任命するとともに，情報セキュリティ分野でコンサルティングサービスを展開するE社に支援を依頼した。E社のコンサルタントである情報処理安全確保支援士（登録セキスペ）のT氏がN社を支援することになった。

〔条件1への対応〕

条件1に対応すべく，Hさんは，情報セキュリティ対策の評価をT氏に依頼した。T氏は，ISO/IEC 27001附属書Aを基に評価し，指摘事項と対策案を表1のとおりに整理した。

表1　T氏の指摘事項と対策案（抜粋）

番号	指摘事項	対策案
1	店舗PCがインターネット経由で侵入され，店舗管理サーバがマルウェアに感染するリスクがある。	（省略）
2	④店舗管理システムは社内LANと分離されているが，社内LANにマルウェアが侵入した場合，店舗管理サーバにもマルウェアが侵入するリスクがある。	（省略）

マルウェアに感染したUSBメモリを介して管理用PCに侵入し、さらに店舗管理サーバへ侵入する

N社は，T氏の対策案を参考に，N社としての対策をまとめ，B社の了承を得た。

〔条件2と条件3への対応〕

条件2と条件3に対応すべく，Hさんは，図6に示すN社インシデント対応ポリシ案を作成し，T氏のレビューを受けた。

(1) 取り扱うインシデントの範囲
サイバー攻撃，不正行為，及びその他の情報セキュリティに関する事件事故を対象とする。
(2) インシデント対応のための組織
インシデント対応を行うためにCSIRTを設置する（以下，N社に設置するCSIRTをN-CSIRTという）。システム部長をN-CSIRTの責任者（以下，N-CSIRT長という）とし，表2に示す部門で構成する。インシデントを発見した時点で初期調査を行い，重大なインシデントの可能性があるとN-CSIRT長が判断した時点で，その重大なインシデントに対応するチーム（以下，PTという）を発足させる。
(3) N-CSIRTの権限
N社の全てのシステムについて，停止又は変更を指示できる。その他の権限が必要な場合，N-CSIRT長は，情報セキュリティ委員会の承認を得る。
(4) インシデントの深刻度と対応方針の基準
（省略）
(5) 情報開示方針
N-CSIRT長は，別途定める基準に従い，対象となるインシデントについて，情報開示の内容を決定する。不特定多数への情報開示は，事前に情報セキュリティ委員会の承認を得る。

図6 N社インシデント対応ポリシ案（抜粋）

表2 N-CSIRTの構成部門

部門	役割
システム部	インシデント対応における技術面を担当する。
人事部	従業員による不正が発覚した場合，その対応を担当する。
c	基本方針の策定やN社インシデント対応ポリシの承認を担当する。
運用委託先	各委託先が担当するシステムについて，N-CSIRTと協力し，インシデントの調査，証跡の取得，システムの停止，復旧などを行う。

オ:情報セキュリティ委員会

次は，レビューの際のT氏とHさんの会話である。

T氏　：インシデント対応プロセスも整理すべきです。NISTの文書SP 800-61 Rev. 2に記載されているインシデント対応のライフサイクルを図7に示します。

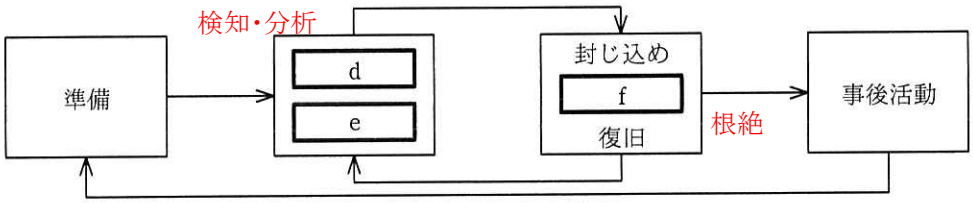


図7　インシデント対応のライフサイクル

H さん：分かりました。図6の一部として整理します。ところで，今後のインシデント対応における技術面について不安があります。

T 氏　：インシデント対応サービスを提供し，登録セキスペが多数在籍する専門事業者が幾つかあります。そのような事業者に支援を依頼するとよいと思います。

H さん：分かりました。表2に専門事業者とその役割を追加します。

N 社は，検討結果を取りまとめ，B 社の了承を得た。

〔新たなインシデントの発生と対応〕

N 社インシデント対応ポリシの運用を開始してから約1か月後の 11 月 22 日，V 社は，不審な利用者アカウント（以下，AC-X という）が R1 サーバに作成されていることを見付け，N-CSIRT に報告した。G 部長は，インシデントであると判断し，初期調査を H さんに指示した（以下，このインシデントをインシデント Q という）。H さんは，V 社と協力してインシデント Q について調査した。その結果を図8に示す。

・利用者アカウントの作成には管理者権限が必要である。AC-X は 11 月 19 日の深夜 1 時に作成された。V 社ではその時間帯に誰も作業していなかったことから，不正アクセスの可能性が高い。
・R1 サーバに一部残っていたアクセスログと FW2 のログから，AC-X が作成されてから発見されるまでの 4 日間，N 社でも V 社でもない複数の IP アドレスから SSH 接続があり，合計 10 回以上 AC-X を利用して不正ログインが行われていたことが判明した。
・N 社及び V 社からの通信は正規のものだけであった。

図8　インシデント Q の調査結果（抜粋）

図9は，FW2において，AC-Xが作成されてから発見されるまでの4日間，通信に成功した全てのパケットを対象とし，通信方向，接続元及び宛先のIPアドレス，サービスの組合せで通信量を集計し，降順に並べたものである。Hさんは，⑤図9を基に，不正ログインを行ったと推測される接続元IPアドレスを割り出した。5

インバウンド通信			
接続元IPアドレス	宛先IPアドレス	サービス	通信量（kバイト）
x2.y2.z2.130	R1サーバ	HTTPS	492
x2.y2.z2.129	R1サーバ	HTTP	382
x2.y2.z2.129	R1サーバ	HTTPS	379
x2.y2.z2.130	R1サーバ	SSH	320
x2.y2.z2.129	R1サーバ	SSH	232
x1.y1.z1.10	R1サーバ	HTTP	228
x1.y1.z1.200	R1サーバ	HTTPS	123
x1.y1.z1.100	R1サーバ	SSH	112
x1.y1.z1.240	R1サーバ	HTTPS	69
x2.y2.z2.60	R1サーバ	SSH	48
x1.y1.z1.240	R1サーバ	SSH	37
x1.y1.z1.10	R1サーバ	HTTPS	14
x2.y2.z2.58	R1サーバ	SSH	12
a2.b2.c2.d2	R1サーバ	SSH	6
アウトバウンド通信[1)]			
接続元IPアドレス	宛先IPアドレス	サービス	通信量（kバイト）
R1サーバ	a2.b2.c2.d2	HTTP	960
R1サーバ	a1.b1.c1.d1	HTTP	320

注[1)] アウトバウンド通信には，R1サーバ上のファイルの持出しに使われたと推測され，かつ，通信量が大きいものだけを示す。

図9　FW2での通信量の集計

Hさんから調査結果について報告を受けたG部長は，R1サーバの隔離を指示した上で，インシデントQは重大なインシデントの可能性があると判断し，PTを発足させた。PTは専門事業者の支援を受けて調査を行い，R1サーバには，脆弱性L及び脆弱性Mが残っていることが判明した。脆弱性Lと脆弱性Mの概要，及びそれぞれの対応を見送った経緯とその理由を表3に，PTによる調査結果を図10に示す。

表３　脆弱性Ｌと脆弱性Ｍの概要，及びそれぞれの対応を見送った経緯とその理由

脆弱性名称	脆弱性の概要	対応を見送った経緯とその理由
脆弱性Ｌ	OSコマンドAの脆弱性である。OS コマンド A は，指定したプログラムを起動する。脆弱性 L を悪用すると，一般利用者権限で OS コマンド A を実行した場合でも，指定したプログラムを管理者権限で起動できる。	脆弱性修正プログラムが 9 月末に公開されたが，R1 サーバでは適用が見送られた。 理由：脆弱性 L の悪用には，OS コマンド A を実行する必要がある。OS コマンド A を実行するには，R1 サーバに SSH 接続してログインする必要があり，脆弱性 L が悪用される可能性は低い。さらに，R1 サーバは会員情報及び秘密情報を保持しないので，影響は小さい。
脆弱性Ｍ	開発支援ツール J の脆弱性である。細工された HTTP リクエストを送信することによって，開発支援ツール J を実行している利用者アカウントの権限で任意のコマンドを実行できる。	脆弱性修正プログラムが 11 月 10 日に公開されたが，R1 サーバでは 11 月末に予定されている月例メンテナンスで適用することにした。 理由：開発支援ツール J は，OS の一般利用者権限で動作しており，変更可能なファイル及びディレクトリが限定されている。さらに，R1 サーバは会員情報及び秘密情報を保持しないので，影響は小さい。

次の(1)～(3)に示す順で R1 サーバに攻撃されたことを確認した。

(1)　“/etc/shadow” ファイルの参照

脆弱性Mを悪用しても一般利用者権限であるが、"/etc/shadow"ファイルの閲覧には管理者権限が必要であるから

・⑥脆弱性 L と脆弱性 M を悪用して，“/etc/shadow” ファイルを参照した。

(2)　利用者アカウントの作成と SSH 接続

・管理者権限で AC-X を作成した。

攻撃の接続元IPアドレスを"/etc/hosts.allow"ファイルに追加した

・⑦R1 サーバをインターネット経由で操作するために設定を変更した。

・AC-X を利用して SSH 接続で R1 サーバにログインした。

(3)　外部へのスキャン

・SSH 接続で R1 サーバにログインした後，脆弱性スキャンを行うツール X を使って多数の IP アドレスをスキャンし，スキャン結果を二つのファイル（以下，F1 ファイルと F2 ファイルという）に格納して，攻撃者のサーバにアップロードした。

・コマンド履歴とフォレンジック調査結果から次に示す内容が判明した。

- ツール X は R1 サーバにダウンロードされていた。
- F1 ファイルは，AC-X のホームディレクトリに配置された後，IP アドレス a1.b1.c1.d1 のサーバにアップロードされ，その後ホームディレクトリから削除されていた。F1 ファイルはフォレンジック調査によって復元でき，サイズは 320 k バイトであった。F1 ファイルには，ツール X が 8 個の IP アドレスをスキャンした結果が格納されており，IP アドレスごとの出力結果は固定長であった。
- ⑧F2 ファイルは一部しか復元できなかったが，F1 ファイルと同様の形式で，ツール X によるスキャン結果が格納されていると考えられた。

図 10　PT による調査結果

開発システム内部からの攻撃なので、FWのことを気にすることはない、
5WのWhereをちゃんと認識しないと、
大幅に違く答えになるので、注意

引き続いて，R1 サーバ以外への侵入拡大の有無を確認した。

(4) 他サーバ群への侵入拡大の有無

・他サーバ群には，開発支援ツール J がインストールされていない。したがって，脆弱性 M が悪用されることはなく，上記(1)～(3)の攻撃は発生しない。

・他サーバ群に登録されている利用者アカウントには，十分な複雑性をもち，異なるパスワードが設定されていた。また，SSH 接続による不審なログイン試行が行われていないことをログから確認した。

(5) 通販サイトへの侵入拡大の有無

・通販サイトには，脆弱性 L が残っているサーバも，開発支援ツール J がインストールされているサーバも存在しない。また，開発用システムの接続制御から，R1 サーバから通販サイトへの侵入拡大も困難である。したがって，通販サイト内への侵入はないと判断した。

図 10 PT による調査結果（続き）

この報告を受けた G 部長は，幸いにも被害が限定的であり，顧客への影響が全くないことから，インシデント Q について情報開示する必要はないと判断し，情報セキュリティ委員会に報告し承認を得た。

その後，G 部長は，利用者アカウントのパスワード変更，R1 サーバの復旧，脆弱性 L 及び脆弱性 M を解消する脆弱性修正プログラムの適用，⑨SSH 接続及び HTTP 接続を使った攻撃から開発用システムを保護するための措置などを指示した。

FW2において、インターネットからのインバウンド通信は、N社とV者からの通信だけを許可する

〔脆弱性管理プロセスの改善〕

インシデント P と比較してインシデント Q の対応は迅速に行われ，N-CSIRT のインシデント対応は有効であると，N 社の経営陣からも B 社からも一定の評価を得た。一方，インシデント Q で R1 サーバが不正にログインされたことを考えると，⑩図 4（イ）及び（ウ）において，悪用される可能性の評価についての観点の不足，又は影響の評価についての観点の不足があり，悪用される可能性又は影響を過小評価したのではないかという指摘があった。そのため，脆弱性管理プロセスを見直すことにした。

・複数の脆弱性が同時に悪用される可能性の視点
・対処を見送った脆弱性の影響への視点

インシデント P の終息から 1 年後，表 1 の指摘事項及びインシデント Q で明らかになった課題は全て解決できた。N-CSIRT は，関係者の訓練を進め，更に迅速かつ効果的なインシデント対応が可能になった。

設問1　〔インシデントの発生と対応〕について，(1)～(5)に答えよ。

(1) 図5中の下線①で示したパスワードリスト攻撃とは，一般にどのような攻撃か。45字以内で具体的に述べよ。

(2) 図5中の下線②について，パスワードの安全な設定方法とは何か。35字以内で具体的に述べよ。

(3) 図5中の下線③について，ログインが普段と異なる環境から行われたことを判定する技術的手法を，45字以内で具体的に述べよ。

(4) 図5中の［ a ］に入れる適切な字句を8字以内で答えよ。

(5) 図5中の［ b ］に入れる適切な数値を答えよ。

設問2　表1中の下線④について，社内LANから店舗PCを経由せずにどのようにマルウェアが侵入すると想定されるか。侵入方法を50字以内で具体的に述べよ。

設問3　〔条件2と条件3への対応〕について，(1)，(2)に答えよ。

(1) 表2中の［ c ］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　IPA　　イ　JIPDEC

ウ　JPCERT/CC　　エ　財務経理部

オ　情報セキュリティ委員会　　カ　総務部

キ　内部監査室

(2) 図7中の［ d ］～［ f ］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　開示　　イ　検知　　ウ　根絶　　エ　トレーニング

オ　復習　　カ　分析　　キ　レビュー

設問4　〔新たなインシデントの発生と対応〕について，(1)～(5)に答えよ。

(1) 本文中の下線⑤について，図9中の接続元IPアドレスのうち，不正ログインを行ったと推測される接続元IPアドレスは幾つか。個数を答えよ。

(2) 図10中の下線⑥について，脆弱性Mだけを悪用しても“/etc/shadow”ファイルを参照できない理由を，“/etc/shadow”ファイルの性質を含めて，70字以内で述べよ。

(3) 図 10 中の下線⑦について，攻撃者が行った設定変更の内容を，45 字以内で具体的に述べよ。

(4) 図 10 中の下線⑧について，F2 ファイルには，幾つの IP アドレスをスキャンした結果が格納されていると考えられるか。図 9 中の値及び図 10 中の値を用いて求めよ。

(5) 本文中の下線⑨について，措置を 75 字以内で具体的に述べよ。

設問 5 本文中の下線⑩について，悪用される可能性を評価する際に加えるべき観点，又は影響を評価する際に加えるべき観点を，今回の事例を踏まえて 30 字以内で述べよ。