**問2**　Webサイトのセキュリティに関する次の記述を読んで，設問1～3に答えよ。

A社グループは，サービス業，小売業，ネットビジネス業及び情報サービス業のA社～G社の7社から成る企業グループである。A社を含むグループ各社が運営しているWebサイトは，企業情報サイト，BtoCサービスサイト，BtoBサービスサイト，一時的なキャンペーンサイトなど，様々である。グループ各社及びその情報システム関連部門の概要を，表1に示す。

**表1　グループ各社及びその情報システム関連部門の概要**

| 社名 | 概要 | 情報システム関連部門の概要 |
|---|---|---|
| A社 | ・A社グループの持株会社<br>・従業員数は100名 | ・情報システム部は部員数が20名で，A社グループ共通の情報システムの企画とグループ各社情報システム部の統括を行う。<br>・サーバ構築，アプリケーションソフトウェア開発（以下，アプリ開発という）及び情報システムの運用はD社に委託する。 |
| B社 | ・ホテル，ゴルフ場などの施設を運営するサービス業<br>・A社グループの中核企業<br>・従業員数は5,000名 | ・情報システム部は部員数が20名で，B社の情報システムの企画を行う。<br>・サーバ構築，アプリ開発及び情報システムの運用はD社に委託する。 |
| C社 | ・水族館，遊園地，大型商業施設などの施設を運営するサービス業<br>・30年前に，A社グループ内に設立<br>・従業員数は3,000名 | ・情報システム部は部員数が10名で，C社の情報システムの企画を行う。<br>・サーバ構築，アプリ開発及び情報システムの運用は，D社及びA社グループ外の情報システム会社H社に委託する。 |
| D社 | ・情報サービス業<br>・30年前に，B社から独立<br>・従業員数は500名 | ・情報システム部は部員数が10名で，D社の情報システムの企画を行う。<br>・開発部は，主にA社，B社，C社及び自社の情報システムのサーバ構築，アプリ開発を行い，運用部はその運用を行う。 |
| E社 | ・スーパーマーケットなどの小売業<br>・10年前に，A社グループに参加<br>・従業員数は10,000名 | ・情報システム部は部員数が20名で，E社の情報システムの企画を行う。<br>・サーバ構築，アプリ開発及び情報システムの運用はG社に委託する。 |
| F社 | ・ネットビジネス業<br>・E社が5年前に設立<br>・従業員数は300名<br>・ショッピングサイトαなどを運営 | ・情報システム部は部員数が10名で，F社の情報システムの企画を行う。<br>・サーバ構築，アプリ開発及び情報システムの運用は，G社及びA社グループ外の情報システム会社J社に委託する。 |
| G社 | ・情報サービス業<br>・15年前に，E社から独立<br>・従業員数は100名 | ・情報システム部は部員数が10名で，G社の情報システムの企画を行う。<br>・開発部は，主にE社，F社及び自社の情報システムのサーバ構築，アプリ開発を行い，運用部はその運用を行う。 |

〔4年前までのグループ各社の状況〕

4年前まで，グループ各社は，Web サイトのセキュリティ対策に各社それぞれの考えで取り組んでいた。

A 社は，セキュリティ対策や個人情報の保護について，B 社～G 社に対して業界ガイドラインへの準拠をポリシとして求めていたが，具体的な指示も準拠状況の確認も行っていなかった。

〔セキュリティ対策プロジェクトの立上げ〕

その後，セキュリティに詳しい L 氏が A 社の経営陣に加わった。L 氏は，A 社グループ内でセキュリティ事故が発生すれば，A 社グループ全体の信頼を損なうおそれがあると取締役会で問題提起した。取締役会では，セキュリティ対策プロジェクト（以下，プロジェクトという）を立ち上げ，グループ全体のセキュリティ対策を推進することを決定した。

この決定を受けて，プロジェクトの責任者には A 社情報システム部長が，プロジェクトリーダには A 社情報システム部の U 課長がそれぞれ任命された。プロジェクトメンバはグループ各社から数名ずつ選出された。

U 課長は，公開しているグループ各社の Web サイトに脆弱(ぜい)性が潜在していたり，今後作り込まれたりするおそれがあり，次の二つが必要であると考えた。

・脆弱性を作り込まず，Web サイトを安全に構築するための対策を実施する。
・攻撃を受け，セキュリティ事故となった場合に，セキュリティ事故の情報は緊急にグループ各社に展開し，対策を実施する。

そこで，部下の P さんとともに，セキュリティ専門家の支援を受けて，次のセキュリティ対策を推進する計画を立案した。

(1) セキュアサイト構築ガイドラインの制定
(2) セキュアサイト構築ガイドラインを踏まえた，具体的な内容を記載した各社セキュアサイト構築基準の制定及び定期的な見直し
(3) セキュアサイト構築基準に従った，サーバ構築及びアプリ開発
(4) セキュリティ事故が発生した直後の A 社情報システム部への報告

(1)～(4)は，グループ各社の取締役会で承認され，3 か月後，(1) が完了し，(2)～(4)についてもグループ各社に指示が出された。

〔F 社ショッピングサイトαへの攻撃〕

F 社から G 社に運用を委託している，ショッピングサイトα（以下，サイトαという）には，PC サイト，携帯サイト及びスマートフォンサイト（以下，スマホサイトという）があり，それぞれ 30 画面で構成されている。今年になって，サイトαの携帯サイトに不審なアクセスがあった。G 社の運用担当者が週 1 回のメンテナンス中にログインのエラーログを確認したところ，利用者 ID に特殊記号を含んだものを多数発見した。通常の利用では考えられないエラーだったので，F 社のサイトα担当者に報告した。

F 社のサイトα担当者から連絡を受けた F 社情報システム部の N さんは，不正アクセスの可能性があると考え，セキュリティ専門業者の X 社に調査を依頼した。X 社の T 氏が調査した結果，携帯サイトの Web アプリケーションソフトウェア（以下，Web アプリケーションソフトウェアを Web アプリという）が，SQL インジェクション攻撃を受けていたことが分かった。そこで，N さんはサイトα担当者に対し，携帯サイトのサーバをネットワークから切り離すように指示した。

次は，そのときの N さんと T 氏の会話である。

N さん：サイト利用者の情報を読み出されたのでしょうか。

T 氏　：いいえ。携帯サイトのアクセスログと，携帯サイトの Web アプリが記録していた POST データのログを確認しましたが，サイト利用者の情報を読み出すリクエストは受信していませんでした。どうやら，脆弱性を探す目的で攻撃を仕掛けられたようです。

N さん：なるほど。それで，脆弱性はあったのでしょうか。

T 氏　：はい。表 2 に示す，携帯サイトのアクセスログを見てください。Web サーバのアクセスログのうち，前回メンテナンス以降の部分について確認したところ，特定の IP アドレスから 27 画面に対して，SQL インジェクションの代表的なパターンが試行されていました。このうち，ステータスコードが 200 であり，かつ，応答のサイズが通常のアクセス時と比較して [ a ] であ

るアクセスログの番号 [ b ] を見つけることができます。このログから，脆弱性があると考えられる URI のパス名は [ c ] であり，クエリ文字列中のパラメタ名は [ d ] であることが分かります。

Nさん：分かりました。攻撃が行われた27画面について，早急に対策を行います。

T氏　：念のために，①それらの画面だけでなく，携帯サイト全体に対して SQL インジェクション対策を行ってください。そのほか，PC サイトとスマホサイトの対策はどのようになっていますか。

Nさん：PC サイトは2年前にリニューアルし，スマホサイトも同時にリニューアルしました。いずれも公開前及びその後の改修時にセキュリティ診断（以下，診断という）をしたので大丈夫だと思います。一方，携帯サイトは 5 年前に公開してから，一度も診断をしていません。アクセスを携帯キャリアのゲートウェイからだけに制限していたので，大丈夫だと思っていました。

T氏　：そうですか。今後は，携帯サイトも診断してください。

Nさん：分かりました。

**表2　携帯サイトのアクセスログ（抜粋）**

| 番号 | IP アドレス | メソッド | URI のパス名 | クエリ文字列 1)2) | ステータスコード | 応答のサイズ（バイト） |
|---|---|---|---|---|---|---|
| 1 | ipA | GET | / | | 200 | 3,284 |
| 2 | ipA | POST | /Login | | 302 | 0 |
| 3 | ipA | GET | /top | | 200 | 3,165 |
| 4 | ipA | GET | /Catalog | category=shirt | 200 | 1,840 |
| 5 | ipA | GET | /Catalog | category=shirt' | 200 | 1,840 |
| 6 | ipA | GET | /Catalog | category=shirt" | 200 | 1,840 |
| 7 | ipA | GET | /Catalog | category=shirt' and '1'='1 | 200 | 1,840 |
| 8 | ipA | GET | /GoodsSearch | word=new | 200 | 3,877 |
| 9 | ipA | GET | /GoodsSearch | word=new' | 200 | 3,877 |
| 10 | ipA | GET | /GoodsSearch | word=new" | 200 | 3,877 |
| 11 | ipA | GET | /GoodsSearch | word=new' and '1'='1 | 200 | 3,877 |
| 12 | ipA | GET | /GoodsDetail | goodsNo=10001 | 200 | 1,798 |
| 13 | ipA | GET | /GoodsDetail | goodsNo=10001' | 500 | 527 |
| 14 | ipA | GET | /GoodsDetail | goodsNo=10001 and 1=1 | 200 | 1,806 |
| 15 | ipA | POST | /CartAdd | | 200 | 1,611 |
| 16 | ipA | POST | /Order | | 200 | 2,239 |
| 17 | ipA | POST | /OrderConfirm | | 200 | 1,818 |

注 1)　クエリ文字列は，URI デコード済みである。
　 2)　クエリ文字列中の"は，一重引用符（シングルクォーテーション）が二つ連続している。

数日後，N さんは G 社から携帯サイトの対策が完了したという報告を受けた。そこで，N さんは，X 社にソースコードを提示し，脆弱性が修正されていることを確認してもらった。その後，F 社では携帯サイトを再開し，N さんは A 社情報システム部に，F 社でセキュリティ事故が発生したことを報告した。

〔グループ各社の管理強化〕

F 社から報告を受けた U 課長は，F 社のセキュリティ事故を分析し，次のような施策案を考えた。

(1) 今回の携帯サイトの脆弱性を含め，脆弱性の多くは診断によって発見できるので，Web サイトの公開前の診断を義務付ける。また，稼働中の全 Web サイトに対しては，優先順位を決めて，順次診断をしていく。

(2) Web サイトによってリスクが異なるので，実施すべき対策を Web サイトごとに各社で決める。

(3) 対策の実施状況と併せて，グループ各社のセキュアサイト構築基準の制定状況と定期的な見直し状況を調査し，問題があれば改善を指示する。

次は，上記の施策案の具体的な進め方に関する，U 課長と部下の P さんの会話である。

U 課長：インターネットに公開している Web サイトでは診断を必須とするが，インターネットに公開していない社内用 Web サイトでは診断はどうしたらいいだろうか。

P さん：グループ各社に任せるにしても判断に困るでしょうね。

U 課長：それなら，基準を統一するために診断ガイドラインを作成しよう。また，グループ各社の Web サイトについて，診断履歴の調査はもちろん必要だが，サイトについてもっと詳しく情報を収集した上で，診断していない Web サイトについて，診断の優先順位を整理してほしい。

P さん：Web サイトの情報収集は調査票を用意して，グループ各社の情報システム部に回答してもらいます。

U 課長：しかし，情報システム部で Web サイトをよく把握していない場合もあるな。

P さん：そうですね。そのような場合の情報システム部への指示方法も検討します。

U課長：セキュアサイト構築基準についても，制定状況及び見直し状況について調査票に回答してもらえばよいだろう。

Pさん：分かりました。

〔診断ガイドラインの制定〕

U課長は，セキュリティ専門家の協力を得て診断ガイドラインを作成するようPさんに指示した。1か月後，図1に示す診断ガイドライン案が作成された。

1. 診断の種類
   - 診断には，プラットフォーム診断とWebアプリ診断の2種類がある。
   - プラットフォーム診断では，OS，ミドルウェア及びネットワーク機器の脆弱性を検出する。ただし，ネットワーク機器では，不要なサービスが稼働していないかを確認する。
   - Webアプリ診断では，Webアプリの脆弱性を検出する。
2. 診断の実施時期
   - 対象Webサイトの公開前に，プラットフォーム診断及びWebアプリ診断を行う。
   - 対象Webサイトの公開後，1年ごとに，プラットフォーム診断及びWebアプリ診断を行う。
3. 診断の実施方法
   - 社内ネットワークからの攻撃を想定する場合，ファイアウォールの内側から診断する。
   - インターネットからの攻撃を想定する場合，ファイアウォールの内側又は外側のいずれかから診断する。
   - IPS，WAFなどによって，[ e ]からの通信が遮断されると，対象Webサイトの脆弱性を検出できないので，[ e ]からの通信は遮断しないように設定した上で診断する。IPS，WAFなどの制約によって，これができない場合は，IPS，WAFなどの内側から診断する。
   - PCサイト，携帯サイト及びスマホサイトのそれぞれについて診断する。ただし，動的ページのプログラムが同じソースコードのプログラムであれば，いずれか一つのサイトについて診断すればよい。
   - ASPサービス及びパブリッククラウドサービスは，サービス提供事業者の許可を得た上で診断する。ただし，サービス提供事業者が診断を許可しない場合は，セキュリティ対策についてサービス提供事業者に説明を求め，確認する。（省略）
4. Webサイトの特徴に応じた診断項目
   - Webサイトが次のいずれかに該当する場合は，詳細な診断を行う。そうでない場合は簡易な診断を行う。
     - インターネットに公開しているWebサイト
     - 決済機能をもつWebサイト
     - 個人情報を扱うWebサイト
5. 診断項目

   （省略）
6. 診断実施後の対応
   - 検出された脆弱性については，リスクの大きさによって修正の要否を検討し，対策を行う。
   - ファイアウォールの内側から行った診断で検出された脆弱性のうち[ f ]については，深刻な脆弱性であっても，対策の優先順位を下げてよい。
   - ②脆弱性の修正完了後，公開前にプラットフォーム診断及びWebアプリ診断を再度行う。

（以下，省略）

**図1　診断ガイドライン案**

U 課長は，診断ガイドライン案を確認するとともに，それをグループ各社へ展開することについてA社取締役会で承認を得た。その後，グループ各社のWebサイトについて診断ガイドラインに沿って診断を進めるよう指示した。

〔新技術によって生じる脆弱性への対応〕

グループ各社のセキュアサイト構築基準について調査した結果，制定はしているが，見直しをしていないことが分かった。

U 課長は，最近の脆弱性への対応に加え，今後Webサイトに新技術を採用した場合の対応も必要になると考えた。そこで，グループ各社の情報システムで今後採用する可能性がある技術を調査した上で，その技術を使った場合に考えられる脆弱性について，セキュリティ専門家に調査を依頼した。

セキュリティ専門家の調査結果によると，セキュアサイト構築ガイドラインに追加が必要な項目は次の三つであった。

(Ⅰ) DOM（Document Object Model）ベースのXSS（クロスサイトスクリプティング）の対策

(Ⅱ) クリックジャッキングの対策

(Ⅲ) HSTS（HTTP Strict Transport Security）の使用

(Ⅰ) DOMベースのXSSの対策

JavaScriptによるWebページ操作に問題がある場合に起きるXSSは，DOMベースのXSSと呼ばれている。JavaScriptを利用する場合は，注意が必要である。

例えば，図2に示すHTML（http://www.example.jp/domxss.html）があった場合に，図3に示すURIにブラウザからアクセスすると，“1”という警告ダイアログが表示される。

```
<html>
<body>
<script>
 document.write(decodeURIComponent(location.hash));
</script>
</body>
</html>
```

図2　HTML（http://www.example.jp/domxss.html）

```
http://www.example.jp/domxss.html [ g ] <script>alert(1) [ h ]
```

図3　警告ダイアログが表示される URI

反射型（reflected 型，non-persistent 型）の XSS と違って，DOM ベースの XSS では攻撃者が注入するデータが Web サイトからの応答中に出力されない。ブラウザ上の HTML データに入力データを動的に挿入するような JavaScript が応答中に含まれていると，入力データにスクリプトが含まれていたときに，そのスクリプトがブラウザ上で実行されてしまう。そのため，DOM ベースの XSS は，③反射型の XSS とは診断方法が異なる。

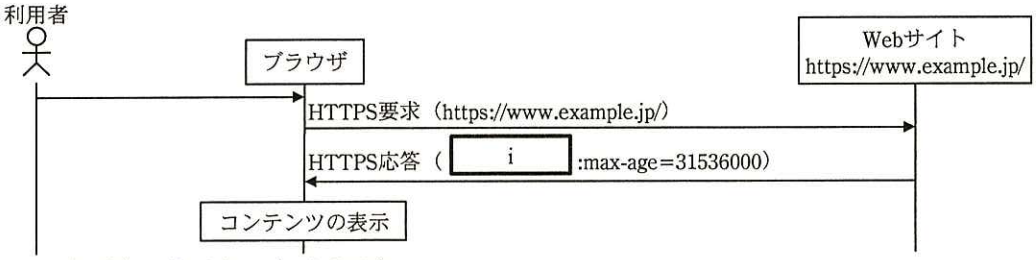
DOM ベースの XSS の対策のためには，“document.write”，“innerHTML” などの，動的にブラウザ上の HTML データを操作するメソッドやプロパティを使用するのではなく，“createElement” などの DOM 操作用のメソッドやプロパティを使用して，ブラウザ上の HTML データを構築することが必要である。

(Ⅱ)　クリックジャッキングの対策

クリックジャッキングの対策には，④HTTP 応答ヘッダで “X-FRAME-OPTIONS” に DENY を指定することによって，自サイトをフレーム内で表示させないようにする方法がある。近年，クリックジャッキングによると思われる事件が発生しており，この応答ヘッダに対応したブラウザが増えている。

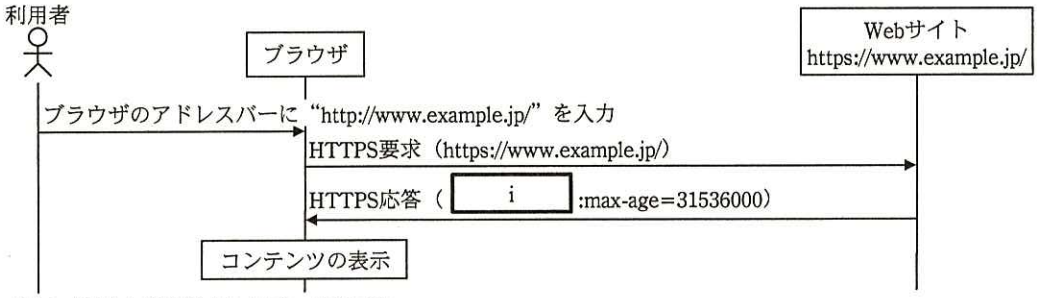
(Ⅲ)　HSTS の使用

HSTS とは，Web サイトが HTTPS の使用をブラウザに強制させる機能である。HSTS がブラウザで有効となるまでの通信の流れを，図 4 に示す。また，HSTS が有効になったブラウザのアドレスバーに “http://www.example.jp/” を入力した場合のブラウザの挙動を，図 5 に示す。HSTS は，HTTPS 応答のヘッダに [ i ] を指定することによって有効となる。




注記　括弧内は送信されるデータを示す。

**図4　HSTS がブラウザで有効となるまでの通信の流れ**




注記　括弧内は送信されるデータを示す。

**図5　HSTS が有効になったブラウザの挙動**

正規の Web サイトで HSTS が有効になるように設定していない場合，正規の Web サイトが HTTPS 通信だけを受け付けるように構成していても，中間者攻撃が行われると，⑤ブラウザが HTTP 通信で接続してしまい，中間者によって通信を盗聴されてしまう。

利用者は毎回 [ j ] ことでこの攻撃を受けても気付くことができる。しかし，[ j ] ことを利用者に徹底させるのは難しいので，HSTS のプロトコルが開発され，2012 年に RFC 6797 として公開された。その後，この機能に対応するブラウザが増えている。

P さんは，グループ各社の Web サイトにおける(Ⅰ)～(Ⅲ)の取組状況を Web サイトの概要と併せて調査した。調査結果を表 3 に示す。

なお，クリックジャッキングについては，フレーム内での表示有無だけでなく，クリックジャッキングによって被害を受けるおそれについても整理している。

表3　グループ各社のWebサイトの調査結果（抜粋）

| サイト名 / 調査項目 | サイト1 | サイト2 | サイト3 | サイト4 | サイト5 | サイト6 |
|---|---|---|---|---|---|---|
| 運営会社 | A社 | A社 | B社 | C社 | E社 | F社 |
| サイトの種別 | 企業紹介 | ポータル | ホテル予約 | レジャー施設<br>入場券販売 | ショッピング | ショッピング |
| 機能の概要 | 検索 | ログイン<br>予定表<br>資料集<br>掲示板 | 会員登録<br>ログイン<br>会員ページ<br>空室検索<br>宿泊予約<br>問合せ | 会員登録<br>ログイン<br>会員ページ<br>入場券購入<br>メールマガジン<br>問合せ | 会員登録<br>ログイン<br>会員ページ<br>商品検索<br>商品購入<br>問合せ | 会員登録<br>ログイン<br>会員ページ<br>商品検索<br>商品購入<br>問合せ |
| JavaScriptの利用 | なし | なし | あり | あり | あり | あり |
| DOMベースのXSS脆弱性 | なし | なし | なし | なし | あり | あり |
| フレーム内での表示の有無 | なし | なし | なし | なし | あり<br>（同じドメインページ内で表示） | あり<br>（同じドメインページ内で表示） |
| 対策なしの場合にクリックジャッキングによって被害を受けるおそれ | なし | あり | あり | あり | あり | あり |
| クリックジャッキング対策の有無 | 対象外 | なし | なし | あり | なし | なし |
| HTTPSの利用 | なし | なし | あり | あり | あり | あり |
| HSTS対応の有無 | 対象外 | 対象外 | なし | あり | なし | なし |

表3の調査結果から，対応の必要なWebサイトがあることが分かったので，U課長は，セキュアサイト構築ガイドラインに項目(Ⅰ)～(Ⅲ)を追加した上でグループ各社に伝え，さらに，各Webサイトでの対策を検討するよう指示した。

以上の対策によって，グループ各社のWebサイトのセキュリティが強化された。

**設問1**　〔F社ショッピングサイトαへの攻撃〕について，(1)～(4)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　6％未満　　イ　45～55％　　ウ　95～105％　　エ　200％以上

オ　2　　カ　7　　キ　11　　ク　14

(2) 本文中の［ c ］に入れる URI のパス名と，本文中の［ d ］に入れるパラメタ名を，それぞれ 15 字以内で答えよ。

(3) 本文中の下線①について，T 氏が携帯サイト全体に対して対策を行うべきであると考えた理由を，40 字以内で述べよ。

(4) 事故発生後の N さんの対応について，改善すべき点を 30 字以内で述べよ。

**設問 2** 〔診断ガイドラインの制定〕について，(1)～(3)に答えよ。

(1) 図 1 中の［ e ］に入れる適切な字句を 15 字以内で答えよ。

(2) 図 1 中の［ f ］に入れる適切な内容を，“ファイアウォール”と“ポート”の二つの用語を用いて 40 字以内で述べよ。

(3) 図 1 中の下線②の診断は，検出された脆弱性が適切に修正されたこと以外に何を確認することを目的としているか。30 字以内で述べよ。

**設問 3** 〔新技術によって生じる脆弱性への対応〕について，(1)～(6)に答えよ。

(1) 図 3 中の［ g ］，［ h ］に入れる適切な文字列を答えよ。

(2) 本文中の下線③について，反射型の XSS の診断方法を 65 字以内で述べよ。また，その診断方法では DOM ベースの XSS を発見できない理由を 35 字以内で述べよ。

(3) 本文中の下線④の対策を行うと，正規の利用において不具合が発生するサイトを，表 3 の中から選び，全て答えよ。また，不具合が起こらないようにするためには，下線④の対策をどのように変更すればよいか。45 字以内で述べよ。

(4) 本文中，図 4 中及び図 5 中の［ i ］に入れる適切な応答ヘッダフィールド名を解答群の中から選び，記号で答えよ。

解答群

ア Content-Disposition　　イ Content-Security-Policy

ウ Strict-Transport-Security　　エ X-Content-Type-Options

オ X-XSS-Protection

(5) 本文中の［ j ］に入れる，利用者のすべきことを，40 字以内で具体的に述べよ。

(6) Web サイトで HSTS が有効になるよう設定している場合でも，本文中の下線⑤の事象が起きる場合がある。HSTS の有効期限が切れた場合以外に，どのような場合に起きるのか。35 字以内で述べよ。