問2　インシデントレスポンスチームに関する次の記述を読んで，設問に答えよ。

K 社は，従業員 500 名の輸入卸売業者である。拠点は，本社，営業所 2 か所，倉庫 1 か所の計 4 か所である。K 社のネットワーク及び機器並びに関連する規程の整備は，情報システム課が担当している。K 社のネットワーク構成を図 1 に，各サーバで取得しているログの内容を表 1 に示す。

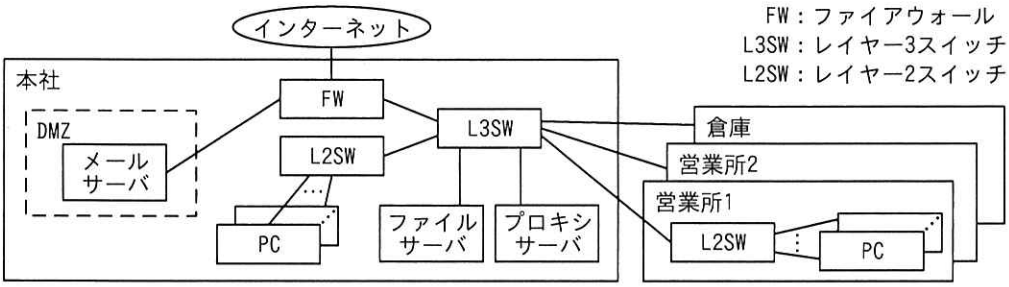


図 1　K 社のネットワーク構成（抜粋）

表 1　ログの内容（抜粋）

サーバ名	ログに記録される項目
メールサーバ	イベントの発生日時，送受信メールの送信元メールアドレス，送受信メールの宛先メールアドレス，メール全体のサイズ，添付ファイルの名称，添付ファイルのサイズ
ファイルサーバ	イベントの発生日時，アクセスされたファイルのパス名，アクセス元の IP アドレス，読込み書込みの種別
プロキシサーバ	イベントの発生日時，アクセス元の IP アドレス，アクセス先の URL，転送したデータのサイズ，アップロードされたファイルのサイズ

〔マルウェアαの検知と対応〕

K 社では，PC にマルウェア対策ソフトを導入しており，リアルタイムスキャンとスケジュールスキャンを実施している。マルウェア対策ソフトの管理サーバはクラウドサービス上にある。マルウェア定義ファイルは，PC を起動したときに更新される。スケジュールスキャンは，毎週月曜日の 10:00 に実施される。

ある月曜日，情報システム課の W 主任がスケジュールスキャンの結果を確認したところ，10 台の PC でマルウェア α が検出され，駆除されていた。W 主任が，マルウェア α についてインターネット上で公開されている情報を調べたところ，次のことが

分かった。

・マルウェアαは，8日前に発見された。

・K社で利用しているマルウェア対策ソフトの定義ファイルにマルウェアαが登録されたのは，昨日だった。

・細工されたマクロ（以下，マクロGという）が仕込まれている，表計算ソフト（以下，Vソフトという）のデータファイル（以下，ファイルGという）を開いて，マクロGを実行してしまうと，攻撃者のWebサーバからマルウェアαがダウンロードされ，起動される。

・マルウェアαは，起動すると，PC上のメールフォルダにある電子メール（以下，電子メールをメールという）を読み出して，攻撃者が用意したWebサーバにアップロードする。その後，OS設定を変更して，OSログイン時にマルウェアαが自動起動されるようにする。

なお，K社で利用しているメールソフトでは，メールは1通が1ファイルとしてPCのメールフォルダ内に保存されている。

マルウェアαが検出されたPCのログと，プロキシサーバのログを調べた結果，これらのPCの中には，先週の水曜日以降，攻撃者のWebサーバのものと思われるURLにファイルをアップロードしていたPCがあったことが分かった。W主任は，調査の結果を上司のM課長に報告した。

M課長から調査と対応の指示を受けたW主任は，K社に機器を納入しているP社に支援を依頼した。依頼に応じたP社の情報処理安全確保支援士（登録セキスペ）であるU氏の協力を得て，W主任は，アップロードされたファイルの特定並びにマルウェアα及びファイルGの削除を進め，調査と対応を完了した。

〔定義ファイルに登録されていないマルウェアの検知〕

マルウェアαへの調査と対応が完了した後，W主任は，マルウェア対策ソフトの定義ファイルに登録されていないマルウェアも検知したいと考え，どうすればよいかU氏に相談した。U氏は，その用途に使用可能な製品として，EDR（Endpoint Detection and Response）があることを説明し，製品Cを提案した。製品Cは，各PCに導入し，クラウドサービス上の管理サーバから操作する。製品Cの機能を表2に示す。

表 2　製品 C の機能（抜粋）

機能名称	機能詳細
イベントの記録機能	PC で起きたイベントを，表 3 に示すイベントの情報とともに記録する。
検知ルールの定義機能	特徴的なイベント又はその並びを，検知ルールとして登録する。複数の検知ルールを登録することができる。検知ルールの仕様を図 2 に，製品 C の製品出荷時に組み込まれている検知ルールを図 3 に示す。
検知機能	PC で起きたイベントが検知ルールに合致したときは，管理サーバから，事前に登録したメールアドレス宛てに警告をメールで送信する。
インシデントレスポンス機能	管理サーバを操作して，指定した PC を対象に，ネットワークからの切離し，OS 設定の変更又は OS コマンドの実行を行う。

表 3　イベントの情報

イベント種別	イベントの情報
ファイル操作	プロセス名，操作種別（読込み，書込み，上書き，削除など），操作されたファイルのパス名・ファイルサイズ・タイムスタンプ・種別（OS のシステムファイル，ログファイルなど）
ネットワーク動作	通信相手先の IP アドレス，サービス，通信の方向，通信データのサイズ，通信相手先の URL，動作種別（ファイルのアップロード，ファイルのダウンロードなど），アップロード又はダウンロードされたファイルのサイズ
プロセス状態の変化	変化種別（開始，終了），プロセス名
OS 設定の変更	変更された設定項目，変更前の値，変更後の値
USB メモリの操作	操作種別（装着，取外し），USB メモリの ID[1]（以下，USB-ID という）
OS 起動・終了	操作種別（起動，終了）
ログイン操作	操作種別（OS ログイン，OS ログアウト），操作結果

注記　全てのイベントにおいて，発生日時及びイベントを起こした利用者 ID も記録する。
注 [1]　USB メモリの識別番号

- 検知ルールには，単純ルールと複合ルールの 2 種類がある。
- 単純ルールには，一つのイベント内の各イベントの情報を条件として複数組み合わせて指定できる。条件として，値が一致する／しない，範囲内である／ない，列挙された値のいずれかに一致する／いずれにも一致しない，文字列として含まれる／含まれないが指定できる。
- 複合ルールは，単純ルール又は複合ルールを組み合わせたものであり，次のようなルールを指定できる。
  - 指定した複数の単純ルールに合致するイベント全てが，指定した時間内に発生した。
  - 指定した単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した回数以上発生した。
  - 指定した複数の単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した順に発生した。
- 複合ルール内で，複数のイベントの間でイベントの情報の値が一致することを条件として指定できる。

図 2　検知ルールの仕様

ルール1：OS設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール2：OS設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール3：OSのシステムファイルが上書きされた，又は削除された。
ルール4：ログファイルが削除された。
ルール5：次の複合ルールが1時間以内に10回以上発生した。
　－何らかのファイルが読み込まれた後，1分以内に，同一のサイズのファイルがHTTPでアップロードされた。

図3　製品Cの製品出荷時に組み込まれている検知ルール

例えば，マルウェアαは，PCで起きたイベントから製品Cを使って検知できる。マルウェアαの特徴的なイベントは，同じサイズのファイルに対する①ファイル操作のイベント及び②ネットワーク動作のイベント，並びにログイン時の自動起動に関するOS設定の変更のイベントである。これらのイベントが，短時間のうちにこの順序で発生したことを検知すればよい。

続けて，U氏は，P社が提供可能な，製品Cに関連するサービスを表4を示して説明した。

表4　製品Cに関連するサービス（抜粋）

サービス名称	主なサービス内容
解析サービス	・PCのイベントを解析し，解析結果を報告する。
運用サービス	・管理サーバを監視し，正常に稼働していることを確認する。 ・新たな攻撃手法に対応する検知ルールを登録する。
監視サービス	・警告を監視し，明らかな誤検知及び重複を除いて直ちに顧客に連絡する。

W主任は，次の三つを軸としたEDR導入案をまとめ，M課長の承認を得た。

・社内の全PCに製品Cを導入する。
・製品Cを使ったマルウェアの検知及び対応のための体制（以下，E体制という）を立ち上げる。
・表4の解析サービスは必要に応じて利用するが，その他のサービスは利用しない。

3か月後，製品Cを全PCに導入し，E体制を立ち上げた。E体制のチームリーダはM課長，メンバーはW主任を含む情報システム課の課員3名である。

まずは，図3の検知ルールだけを用いて試験運用を開始した。

〔マルウェアβの検知〕

製品C導入から6か月ほど経ったある日，マルウェア対策ソフトのスケジュールスキャンの結果を確認したところ，3台のPC（以下，PC1，PC2，PC3という）で同一のマルウェアが検知され，駆除に失敗していた。図4は，製品Cが記録したPC1～3のイベントのうち，PC1～3に共通しており，特徴的と思われたVソフト及びUSBメモリに関するイベントを，OSログインのイベントとともに抜粋したものである。

PC1	PC2	PC3
5月19日(木)	5月19日(木)	5月19日(木)
14:27 OSログイン	13:05 OSログイン	09:57 OSログイン
15:03 USBメモリ装着	13:15 USBメモリ装着	10:10 V-開始
15:15 ファイルコピー	13:16 ファイルコピー	10:13 V-読込 N:¥file2.v
E:¥file1.v→C:¥file1.v	E:¥file3.v→C:¥file3.v	10:25 V-書込 N:¥file2.v
15:16 USBメモリ取外し	13:17 USBメモリ取外し	10:35 V-読込 C:¥file4.v
15:18 V-開始	16:47 V-開始	10:40 V-終了
15:18 V-読込 C:¥file1.v	16:48 V-読込 C:¥file3.v	16:30 USBメモリ装着
15:18 V-読込 N:¥file2.v	16:49 V-終了	16:35 ファイルコピー
15:18 V-書込 N:¥file2.v	17:12 V-開始	C:¥file4.v→E:¥file4.v
15:25 V-書込 C:¥file1.v	17:25 V-読込 N:¥file2.v	16:39 USBメモリ取外し
15:26 V-終了	17:25 V-読込 C:¥file6.v	
	17:25 V-書込 C:¥file6.v	
	17:43 V-終了	
5月20日(金)	5月20日(金)	5月20日(金)
動作記録なし	11:14 OSログイン	13:32 OSログイン
	11:15 V-開始	14:36 V-開始
	11:15 V-読込 C:¥file6.v	14:39 V-読込 N:¥file2.v
	11:15 V-読込 C:¥file8.v	14:39 V-読込 C:¥file4.v
	11:15 V-書込 C:¥file8.v	14:39 V-書込 C:¥file4.v
	11:15 V-終了	15:03 V-終了
	11:22 V-開始	15:46 V-開始
	11:24 V-読込 C:¥file3.v	15:48 V-読込 C:¥file7.v
	11:43 V-終了	16:23 V-終了

V-開始：Vソフトのプロセス開始　V-終了：Vソフトのプロセス終了
V-読込 ○○：Vソフトでファイル○○を読込み
V-書込 △△：Vソフトでファイル△△を書込み又は上書き
注記1 C:は，内蔵SSDに割り当てられたドライブ名である。
注記2 E:は，USBメモリを装着した場合に割り当てられたドライブ名である。
注記3 N:は，ファイルサーバ上の同じ共有フォルダに割り当てられたドライブ名である。
注記4 ファイルの拡張子“v”は，Vソフトのデータファイルの拡張子である。
注記5 PC1～3に装着されたUSBメモリは，それぞれ異なるUSBメモリである。

図4　製品Cが記録したPC1～3のイベント（抜粋）

W主任は，調査のためP社に解析サービスを発注し，図4のイベントの解析を依頼した。

P社は，推測した状況を表5のとおり報告した。

表5　P社による推測

発生順序	日時	事象
1	5月19日(木) [a]	USB メモリが，[b] に装着された。その USB メモリには，[c] というファイルが存在していたが，そのファイルにはマルウェアβという新種のマルウェアが潜んでいた。
2	(省略)	[c] が [b] の C ドライブにコピーされた。
3	(省略)	C ドライブ上の [c] を開いて，マクロを実行したところ，マルウェア β が起動した。その直後に，ファイル利用履歴の中から選ばれたと思われる [d] というファイルが開かれ，マルウェア β がマクロとして埋め込まれた後，直ちに上書き保存された。
4	(省略)	[e] 上で，利用者が [d] を開いて，マクロを実行したので，[e] にも感染が広がった。
5	(省略)	さらに，3台目の PC にも感染が広がった。
6	5月23日(月) 10:00	5月22日に更新されたマルウェア定義ファイルにマルウェア β が登録されたので，スケジュールスキャンによって PC1～3 の C ドライブでマルウェア β が検知された。(駆除失敗の理由については省略)

P 社の報告を受けた W 主任は，③マルウェア β が埋め込まれたファイルの削除など必要な対応を完了した。P 社がマルウェア β の検体を静的解析したところ，表5の発生順序3～5の事象について裏付けが取れた。また，マルウェア β は，追加のマルウェアをダウンロードする機能をもっていたが，ダウンロードに失敗していたことも分かった。その後，U 氏は，“P 社の運用サービスでは，このような場合は，すぐに検知ルールを作成し，登録します”と W 主任に提案した。

〔運用サービスの利用〕

K 社は，マルウェアをより早期に検知するために有効かどうかを確認しようと考え，表4のサービスについての当初の方針を変えて，3か月ほど試験的に P 社の運用サービスと監視サービスを利用することにした。P 社は，まず，④マルウェア β と同じ手段による感染の拡大を検知するための検知ルールを作成して製品 C に登録した。その後2週間，V ソフトの正常なデータファイルを開くといった，PC の通常利用に起因する誤検知が起きないか確認を続けた。

サービス利用開始から1か月後，ある従業員がメールに添付されていた V ソフトのデータファイルを開いて，マクロを実行した直後にマルウェア β の亜種を検知する

ことができた。さらに，E 体制のメンバーが直ちに必要な対応を指示することによって被害の拡大も防ぐことができた。

〔運用体制の組替え〕

試験期間が終了し，K 社は，運用サービス及び監視サービスを正式に利用することにした。それらに加え，インシデント対応を円滑に行うために，被害状況の把握及び侵入経路の特定を行う P 社のインシデント対応支援サービスも利用することにした。

インシデント対応支援サービスの利用には，インシデントレスポンスチーム（以下，IRT という）の整備が前提となっている。M 課長は，IRT の体制案をまとめ，経営層の承認を得た。IRT では，通常時は，1 名が通報窓口の要員として対応する。招集時は，情報システム課，営業所 1，営業所 2 及び倉庫の従業員計 10 名が参加する。

M 課長は，W 主任にインシデント対応の流れを整理して，必要となる規程及び通報窓口の要員が社内から通報を受けるための通報専用メールアドレスを整備するように指示した。また，規程を整備する際は，インシデントの重大さ（以下，レベルという）を定義し，レベルに応じて対応に必要な体制が変わることに注意するように付け加えた。

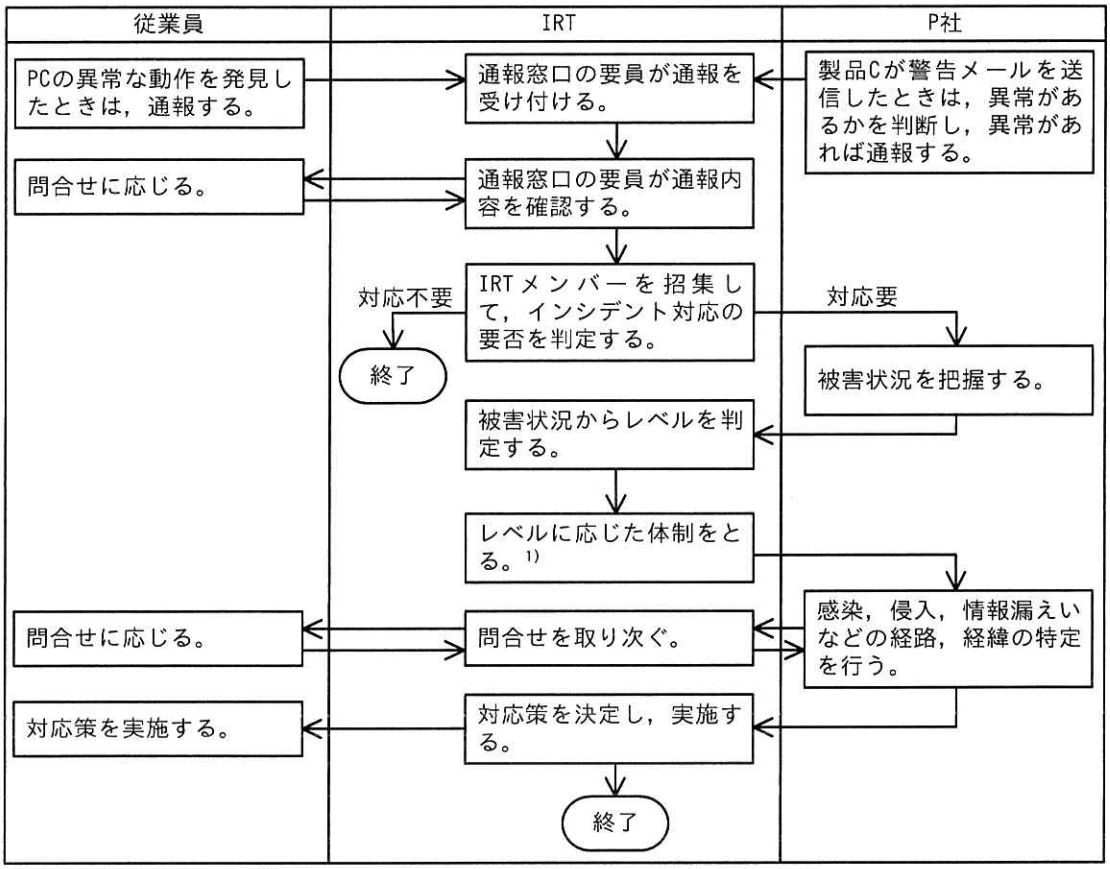
W 主任は，レベルの判定の際に使用する基準の案を図 5 に，マルウェアによる情報漏えいを想定したインシデント対応の流れの案を図 6 にまとめ，M 課長に提出した。M 課長は，図 5 と図 6 の案を承認して IRT の活動を開始した。

1. レベルは，緊急，重要，軽微の 3 段階とし，次の表によって判定する。

	影響の深刻さ：大	影響の深刻さ：中	影響の深刻さ：小
影響の広がり：大	緊急	緊急	重要
影響の広がり：中	緊急	重要	軽微
影響の広がり：小	重要	軽微	軽微

2. 影響の深刻さは，インシデントの事業への影響に基づいて判定する。
   大：一部の事業が継続できない可能性がある。
   中：一部の事業の継続に影響がある。
   小：事業活動でよく起きる程度の影響である。
3. 影響の広がりは，インシデントのシステムへの影響に基づいて判定する。
   大：サーバ複数台，又は PC 30 台以上が影響を受ける。
   中：サーバ 1 台，又は PC 10 台以上が影響を受ける。
   小：PC 1 台以上 10 台未満が影響を受ける。

図 5　レベル判定基準（案）



注 1) レベルが緊急の場合は，IRT 全員の体制とする。重要の場合は，IRT メンバー5 名の体制とする。軽微の場合は，IRT メンバー2 名の体制とする。レベルが緊急の場合は経営層に報告する。

図 6　インシデント対応の流れ（案）

〔秘密ファイルの流出〕

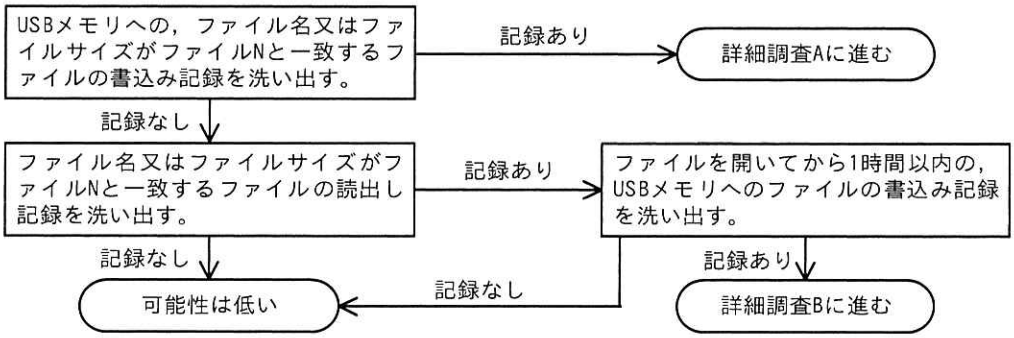
IRT の体制が整った 1 週間後の 9 月 29 日，社内からの通報専用メールアドレス宛てにある従業員からメールが届いた。そのメールの内容は，“S 社が提供するオンラインストレージサービスである S サービスにおいて，K 社の取扱商品の価格表（以下，ファイル N という）と思われるファイルが一般公開されていて，仕入原価も記載されていると 9 月 26 日に取引先から連絡があった”というものだった。メールを見た通報窓口の要員は IRT 全員を招集して会議を開催しようとしたが，日程調整が難航し，開催できたのは 10 月 4 日だった。10 月 3 日には，営業部門から，“顧客から，S サービスで公開されているファイルについて苦情が来ているので対応を急いでほしい”と，M 課長に抗議が来ていた。

会議の中で，S サービスで公開されているファイルが，秘密情報に該当するファイルNであることを確認した。ファイルNに含まれている商品の売上高は全社の売上高の 5%であった。IRT では，インシデント対応要と直ちに判断して，まず S 社にファイルの公開停止を依頼した。続いて，P 社に解析サービスを発注して PC のマルウェア感染の調査を依頼した。1 時間後，P 社から，“製品 C の記録を確認したが，マルウェアのものと思われるイベントは発見できない”との報告があった。これらの状況を基にレベルの判定を行おうとしたが，“影響の広がり”の区分のどれにも該当しないので，とりあえず“軽微”と判定した。その後，インシデント対応支援サービスを利用して，ファイルNの公開の経緯の特定を依頼した。

最初に P 社は，K 社のほかのファイルが S サービスで公開されていないかどうかを調査した。ファイルN以外に，価格表が幾つか公開されていたが，いずれも公開されても差し支えないものであった。これらは，アップロード日時からファイルNと同時にアップロードされたものだと推測できた。念のため，マルウェア α 及びマルウェア β の再感染も調査したが，その形跡はなかった。その後，ファイル N が公開された経緯として可能性の高いものを四つ，表 6 に示すとおりに想定して順に調査した。

表 6　ファイルNが公開された経緯の想定

項番	公開された経緯	調査方法
想定 1	従業員が，攻撃者にだまされた結果，又は意図的に，ファイル N を攻撃者のメールアドレスに送信し，攻撃者が S サービスにアップロードした。	メールサーバのログについて，[f] 又は [g] が，ファイル N と一致するものを洗い出す。
想定 2	従業員が，攻撃者にだまされた結果，又は意図的に，HTTP で攻撃者のサーバにファイル N をアップロードし，攻撃者が S サービスにアップロードした。	プロキシサーバのログについて，ファイル N の [h] と，[i] が一致するものを洗い出し，その [j] が信頼できるサイトのものかどうか確認する。
想定 3	ファイルサーバが不正アクセスを受けて，何らかの方法で攻撃者のサーバにファイル N が送信され，攻撃者が S サービスにアップロードした。	ファイルサーバのログについて，製品 C の記録と突き合わせて一致しないものを洗い出す。
想定 4	従業員が，USB メモリにファイル N を書き込み，社外に持ち出してから S サービスにアップロードした。	図 7 に示す調査計画に従って各 PC を調査する。



注記　詳細調査A及び詳細調査Bは，想定4が実際に起きたかどうかを確認するための調査であり，PC内のファイルの調査及びログの突合せを行うものである。

図7　想定4の調査計画

P社が調査を進めた結果，想定1～3の可能性は低いことが分かったので，想定4について調査を進めた。

調査の中間報告のために，U氏がK社を訪問した。W主任はU氏に，図7で“詳細調査Bに進む”と判定されるのは，従業員がどのような操作をして，どのようなファイルをUSBメモリに書き込んだ場合が考えられるか聞いた。U氏は，従業員がファイルを書き込む際に，［　k　］という操作をして，ファイルNと同じ内容が含まれるものの，［　l　］及び［　m　］が異なるファイルへと変換した場合が考えられると答えた。

〔原因の特定〕

図7に基づく調査では，従業員のJさんが使用しているPCだけが詳細調査Aに進み，そのほかのPCは全て可能性は低いとの結果になった。P社から報告を受けたIRTでは，Jさんに聞き取り調査を行った結果，公開可能な価格表ファイルを持ち出すために，個人所有のUSBメモリにファイルをコピーした時に，誤ってファイルNもコピーしてしまい，その後USBメモリを紛失していたことが分かった。

IRTでは，紛失したUSBメモリを手に入れた何者かが，ファイルNを含む幾つかの価格表をSサービスにアップロードしたと推測した。今回のインシデントはこれ以上被害が拡大することはないと考え，インシデント対応は完了とした。体制不足もあり，取引先からの連絡から，インシデント対応完了までに12日間掛かった。

〔再発防止〕

M 課長は，ファイル持出しに起因する同様のインシデントの再発を防止するためには，個人所有の外部記憶媒体の使用制限を含めた対策が必要であると考え，必要な規程を策定するように W 主任に指示した。W 主任は，規程案を図 8 のとおりにまとめ，M 課長に提出した。

［業務で使用する USB メモリの指定］
・業務で使用する外部記憶媒体は，情報システム課が調達する USB メモリに限定する。調達した USB メモリの USB-ID は情報システム課が管理する。
・USB メモリは，必要時に情報システム課から借用し，利用終了後速やかに返却する。

［秘密ファイルの指定］
・秘密情報に該当するファイルは，ファイル名の先頭に“【秘密】”又は“(CONFIDENTIAL)”の文字列を付加する。

［秘密ファイルの持出し］
・秘密ファイルを社外に持ち出す場合は，暗号化した上で，情報システム課から借用した USB メモリに保存し，各部門で用意した秘密ファイル持出台帳に記録する。
・暗号化には，表計算ソフトなどの暗号化機能，又は AES を使用したファイル暗号化ツールを利用する。パスワードは十分な長さの推測困難なものを設定する。
・秘密ファイル持出台帳は，電子ファイルとしてファイルサーバに保管する。

図 8　規程案（抜粋）

M 課長は，この規程案を承認するとともに，情報システム課が管理する USB-ID を P 社に伝え，この規程に違反する持出しを製品 C で検知するように P 社に依頼した。P 社は，違反する持出し操作のうち製品 C で検知可能な操作について⑤新たな検知ルールを作成して，製品 C に登録した。一方，製品 C で検知できない操作については，別の対策を提案した。

〔事後評価〕

インシデント対応について，P 社と K 社が合同で見直しを実施した。この見直しの結果を受けて，M 課長は幾つかの修正を W 主任に指示した。W 主任は修正案を表 7 のとおりまとめた。

表7　インシデント対応についての修正案（抜粋）

項番	方針	具体的内容
1	IRTでの通報受付を早めるために，通報窓口を見直す。	n
2	図5中の“影響の広がり”の判定基準を見直す。	（省略）
3	インシデント対応の開始を早めるために，図6を見直す。	通報の受付時には，IRTメンバー全員の集合を待たず，最低限のメンバーが集合した時点で対応を開始するかどうかを決定する。
4	体制のとり方を見直すために，レベルの判定のタイミングを見直す。	o

M課長は，これらの案を承認し，後日正式な規程とした。

設問1　本文中の下線①，②について，検知するための単純ルールを，それぞれ30字以内で具体的に答えよ。

設問2　〔マルウェアβの検知〕について答えよ。

(1)　表5中の［a］～［e］に入れる適切な時刻，ファイル名又はPC名を答えよ。

(2)　本文中の下線③について，PC1～3の内蔵SSD及びファイルサーバから削除すべきファイルは何か。解答群から全て選び，記号で答えよ。

解答群

ア　PC1のC:¥file1.v　　イ　PC2のC:¥file3.v　　ウ　PC2のC:¥file6.v

エ　PC2のC:¥file8.v　　オ　PC3のC:¥file4.v　　カ　PC3のC:¥file7.v

キ　共有フォルダ内のfile2.v

設問3　本文中の下線④について，作成した検知ルールを60字以内で答えよ。

設問4　〔秘密ファイルの流出〕について答えよ。

(1)　表6中の［f］，［g］に入れる適切なログの項目名を，表1から選び答えよ。

(2)　表6中の［h］に入れる適切な字句を答えよ。

(3)　表6中の［i］，［j］に入れる適切なログの項目名を，表1から選び答えよ。

(4)　本文中の［k］～［m］に入れる適切な字句を，それぞれ10

字以内で答えよ。

設問５　本文中の下線⑤について，新たに作成した検知ルールを 60 字以内で答えよ。

設問６　表 7 中の［　n　］，［　o　］に入れる適切な字句を，［　n　］は 30 字以内で，［　o　］は 50 字以内でそれぞれ答えよ。