明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ事故対応ガイドブック

情報セキュリティ大学院大学

本書について

情報化社会と言われて久しい現在、私たちの暮らしや経済活動は情報化の進展により便利かつ高度化した反面、個人情報漏えいをはじめとする情報セキュリティに関する事件・事故が後を絶ちません。情報セキュリティは事故を未然に防止することも必要ですが、万一、事故が起こった場合の被害を最小限に抑えるため、日ごろから情報セキュリティ事故発生時の対応技術を備えておくことが重要となります。

各企業・団体においては、情報セキュリティの重要性を認識し、事故発生時の対応についても様々な対策を講じているものと思われます。しかし、これまで情報セキュリティ事故の対応技術について体系的かつ実践的な内容の教材がなかったことから、特に、中・小規模の組織では技術を備えた人材を育成することが難しい状況となっています。

そこで、このたび、情報セキュリティ大学院大学と神奈川県との協働による「情報セキュリティ事故の対応技術に関する教材の作成事業」の一環として、中・小規模の組織の方が情報セキュリティ事故の対応技術について習得していただくことを目的として、想定される事故の内容に応じた対応手順を示し、事故の発生に備えるとともに、実際に事故が発生した際に活用できる教材を作成しました。

本書は、情報セキュリティ事故対応の準備をあまり実施していない中・小規模の組織を主な対象として作成したもので、情報セキュリティに関する知識をあまり持っていない人（組織）でも内容を理解し活用できるよう配慮しています。本書では、冒頭で情報セキュリティや情報セキュリティ事故対応に関する基本的な最低限の知識を示した上で、情報セキュリティ事故対応の大まかな流れがわかるフローや詳細な対応手順について汎用性を持った内容で示しています。汎用性を持たせることで、様々な企業規模や業種・業態のある組織がそれぞれの状況に合わせて修正、追加をして使用することができ、それにより実態に即したものとなりますが、場合によっては修正を加えずにそのまま使用し、必要に応じて修正を加えていくこともできます。

また、情報セキュリティ事故対応を実施するにあたって、事前に実施しておくべき対策（データのバックアップ等）を容易に確認できるよう事故対応チェックシートを作成しました。このチェックシートに記載されている準備が実施できていれば、実際に事故が発生した場合でも、問題なく対処が可能な環境が整えられているといえますが、逆に実施できていない場合は、事故の対応が取れない可能性が出てくるといえます。

したがって、本書の使い方として、冒頭から通読するという使い方もありますが、まずは事故対応チェックシートを実施して、自組織で不足している事故対応の準備を明確にした上で、実施していくという使い方もできます。また、本書では、企業規模（小規模または中規模）に応じた本書の適用例も示しているため、自組織の規模に合った適用例を参考にしながら事故対応の準備を実施していくという使い方もできます。このような教材の使い方の例についても、本書に掲載しておりますので、是非ご活用くださるようお願いします。

最後に、本書を作成するに当たって、アンケートやインタビューにご協力いただいた企業、自治体の皆様に感謝申し上げます。

目次

1　はじめに

1.1 頻発する情報セキュリティ事故

近年、個人情報の漏えい事故が後を絶ちません。公開されている情報漏えい事故だけでも連日のように報じられており、公開されていない事故を含めれば、膨大な件数になると思われます。

情報システムの故障やソフトウェアの不具合によるシステム停止などにより、社会の重要なインフラが使えなくなり、国民の生活に支障をきたすような事故も発生しています。組織においても情報システムは業務やサービスの中核に組み込まれ、情報システムが停止してしまうと組織の存続にもかかわるような状況になっています。

1.2 情報セキュリティ事故対応

情報セキュリティ事故を起こさないようにするためには、様々な予防対策を実施する必要があります。しかし、どんなに予防対策を施しても、100%事故を無くすことはできません。

したがって、情報セキュリティ事故が発生してしまった時を想定し、事故発生時にいかに被害を最小限に抑え、速やかに復旧させるかが重要になってきます。例えば、PC にウイルスが感染したときを考えてみると、その PC の復旧を図る前に、他の PC への感染を防ぐために、ネットワーク回線を外すことが優先されます。あるいは、不正アクセスが行われたときは、復旧作業の前に、PC の状況や操作の記録を不正アクセスの証拠として保持しておくことが必要になってきます。

1.3 情報セキュリティ事故対応の準備の必要性

このように、情報セキュリティ事故の内容によって、取るべき対応、順序が変わってくるために、事故の内容ごとにその対応手順をまとめ、準備しておく必要があります。準備をしておかないと、実際に事故が発生したとき、どう対処して良いか分からず、対応が遅れ、被害が拡大してしまう恐れがあります。また、事故の準備を行うことで、事前に用意しておくべきことが明確になり、情報セキュリティ対策の効率的な構築につなげることができます。

2　情報セキュリティ事故対応の概要

本章では、情報セキュリティについての基本的な事項について確認し、これを踏まえ、情報セキュリティ事故とその対応について考えていきます。

2.1 情報セキュリティとは

情報セキュリティとは、端的に言えば「重要な情報を守ること」です。この言葉をもう少し詳しく解説していきます。

ここで言う「情報」は、実際には紙媒体で保管されているケースや電子データとして情報システム内や USB メモリなどの電子媒体で保管されているケースがあり、ときにはネットワーク回線を通じてやり取りされています。したがって、紙媒体や電子媒体に保管されている情報だけではなく、情報を扱う情報システムも含めて守る必要があります。

次に「重要」という言葉ですが、何が重要かは組織の状況によって変わってきます。顧客情報や機密情報など組織にとって重要かどうかも当然一つの尺度になりますが、近年では特に顧客側から見てどのように見られるかも重大な問題となっています。例えば、その組織では機密事項でないような情報が漏えいした場合でも、顧客側からその組織の管理体制について不審に思われてしまうのであれば、その情報は漏えいしてはならない「重要な情報」と考える必要が出てきます。

そして「守る」という言葉は、具体的に言うと、情報セキュリティの３要素と呼ばれる下記の事項を、それぞれ確保し、維持することと言えます。

①機密性：決められた人以外には利用させない（情報漏えいすることがない）

②完全性：情報の完全さ正確さを保護する（改ざんされることがない）

③可用性：必要なとき確実に使えるようにする（利用できないことがない）

【参考】＜情報セキュリティの定義＞

情報セキュリティ管理に関する規格（JIS Q 27002:2006）の中で、情報セキュリティは下記のように定義されています。ここで、エンティティとは情報資産として管理すべき対象を指します。

情報セキュリティの定義：情報の機密性，完全性及び可用性を維持すること。さらに、真正性、責任追及性、否認防止及び信頼性のような特性を維持することを含めても良い。

- 機密性：許可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性
- 完全性：資産の正確さおよび完全さを保護する特性
- 可用性：許可されたエンティティが要求したときに、アクセスおよび使用が可能である特性
- 真正性：ある主体または資源が、主張通りであることを確実にする特性
  真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
- 責任追及性：あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡出来ることを確実にする特性
- 否認防止：ある活動または事象が起きたことを、後になって否認されないように証明する能力
- 信頼性：意図した動作および結果に一致する特性

【参考】＜リスク分析＞

重要な情報は組織により異なりますが、一人一人の考えによっても異なるため、組織としての共通認識の下でまとめる必要があります。

守るべき重要な情報は「情報資産」と表現され、まずは、組織内にどのような情報資産が存在するか洗い出す必要があります。このとき、上記情報セキュリティの３要素ごとに情報資産の重要性を組織内で検討し、共通認識とすることが必要です。

また、情報資産はウイルス感染や不正アクセス、紛失などの様々な「脅威」にさらされており、情報資産を守るために、様々な対策を施す必要があります。しかし、その対策に不備があったり、費用の面で限られた対策を取らざるを得ないときがあります。これらの不備を「脆弱性」と言います。

洗い出された情報資産にどのような脅威と脆弱性が存在するかを明らかにし、情報資産の価値、脅威、脆弱性の大きさを算定し、これらを比較することにより、守るべき情報資産が明確になります。そして、これら一連の作業をリスク分析と呼びます。

2.2 情報セキュリティ事故と実施すべき対応

情報セキュリティ事故とは、前述の表現を使うと「重要な情報を守ることができなかった結果の事象」と言え、下記のような事象が考えられます。

①重要な情報を決められた以外の人が利用した（重要な情報が漏えいした）

②重要な情報の完全さ正確さを保護できなかった（重要な情報が改ざんされた）

③重要な情報が必要な時使えなかった（重要な情報(システム)が利用できなくなった）

そして、これら事故内容によって、取るべき対応は当然異なってきます。

また、これらの事故の要因により、対応内容も変わってくる場合があります。例えば、上記①について、意図的な内部犯行であれば、これは犯罪行為であり証拠保全が必要になりますが、偶発的な過失によるものであれば、特に証拠保全は必要ありません。

【参考】＜情報セキュリティ事故：情報資産、脅威、脆弱性と事故の関係＞

情報資産に内在した弱い点（脆弱性）が、情報資産を取り巻く様々な脅威により突かれ、顕在化した（目に見える形になった）ものが情報セキュリティ事故となります。リスクとは、脅威が顕在化する可能性、ともいえます。

また、情報セキュリティ事故は情報セキュリティインシデントと呼ばれることもあり、事故対応は、インシデントレスポンスとも呼ばれます。

図 1　情報資産、脅威、脆弱性と事故の関係

2.3 情報セキュリティ事故対応の実施フェーズ

このように、事故の内容により対応は異なりますが、一般的な事故対応のフェーズは次のようになります。

① 検　　知：人や様々な仕組みにより、事故の発生を検知する。

② 初期対応：問題の切り分けや被害拡大の防止、犯罪行為時の証拠保全など、まず始めに実施すべき対応を行う。

③ 回　　復：事故を復旧し、元の状況に戻すための対応を行う。

④ 事後対応：事故の原因・経緯等から、今後同じようなことが起きないような対策について検討、実施する。

図 2　情報セキュリティ事故対応の実施フェーズ

2.4 情報セキュリティ事故対応のプレイヤー

情報セキュリティ事故への対応にあたっては、これを実務的に対応する人（または組織）や、これを組織として大局的に判断し、指揮する人（または組織）が必要になります。これらのプレイヤーは一般的には次のような構成になります。

① 管理者：事故に対する大局的な判断や指揮を行い、事故全体を統括する。通常、経営層が含まれる。

② 窓口、実務担当：事故の受け付け、事故の切り分けや、回復作業、事故対応実務を行う。

③ 従業員：業務に従事している組織員であり、事故の検知の役割を負う。

④ その他：顧客（事故の検知）、保守委託業者、システムベンダ、警察など状況によって異なる。

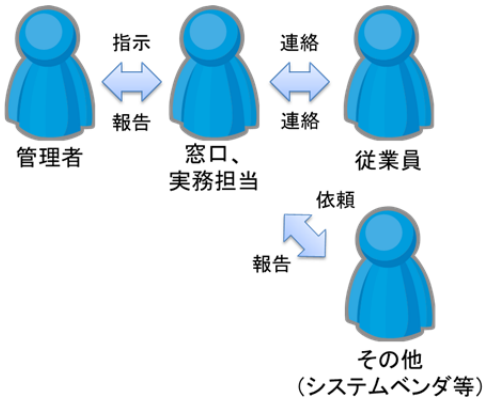


図 3　情報セキュリティ事故対応のプレイヤー

【参考】＜組織の規模と体制＞

組織の規模が大きくなると、守るべき情報資産も増え、窓口への連絡も増加してきます。そして、様々な技術等による対策も高度になり、事故対応もより重要性を増すことになります。そうなると窓口業務（検知した事故の報告を受け、軽微な問題の切り分け）と、システム担当（事故の原因究明や復旧作業）を分け、システム担当部署ではより高度な教育や情報収集を行い、事故対応に当たる方が効率的になってきます。

これら事故に対応する部署・チームを CSIRT（Computer Security Incident Response Team、シーサート）とよび、各組織の CSIRT が情報共有や連携することで、より高度な事故対応を目指す協議会も設立されています。（CSIRT は、必ずしも組織の 1 部署であるとは限らず、部署をまたがったチーム構成のこともある。）

また、組織の規模が大きくなると、管理者単独の判断ではなく経営層や各部署長などで構成される「情報セキュリティ委員会」が組織され、総合的に検討された後、判断が下されるようになります。

2.5 情報セキュリティ対策と事故対応

情報セキュリティ対策は、情報セキュリティを維持するための施策です。組織の脆弱な部分を把握し、これを補強するような対応策を事前に施し、情報セキュリティ事故が起きないようにするものです。

完璧なセキュリティ対策を目指しても、完璧になることはあり得ず、事故が発生する可能性は無くすことができません。また、事故が起こらない確率を上げようとすればするほど、セキュリティ対策にコストがかかってきます。最近では事故を前提とした対策を考えるべきとの考え方のもと、故障してもすぐに復旧できるような対策を検討することや、情報漏えいしても問題を最小限にするために、データの暗号化を行うことなどの重要度が上がってきています。いずれにせよ、事前の対策も事後の対策もバランスよく構築することが求められます。

情報セキュリティ対策には様々ありますが、組織に必要な対策とその管理について記述したJIS 規格（JIS Q 27001,27002）などもあり、これらを基に組織の要件に沿って適用すれば、最良と考えられる網羅的なセキュリティ対策を施すことができます。また、この規格に沿った対応が実現できている組織に認証を与える ISMS(Information Security Management System)認証制度もあり、この認証を得ると組織の情報セキュリティの信頼性を社外にアピールできます。そして、この JIS 規格の中で、必ず計画しておくべき情報セキュリティ対策の１つとして情報セキュリティ事故対応の準備が挙げられており、このことからもその重要性が伺えます。

また、これらの施策への取り組み方も組織の状況に応じて決定していく必要があります。情報セキュリティ対策とその管理システムは組織全体に渡るため、通常はトップダウンで組織全体に実施することが求められます。事故対応も様々な事故を想定し、これらすべての準備を一度にすることが理想ですが、組織に必須な事故対応ごとに優先順位を決めて順次構築することも出来るため、組織の状況に適した取り組みを行っていくことが大切です。

情報セキュリティ対策を実施する上で参考となる中小企業向けの資料としては、IPA（独立行政法人情報処理推進機構）の「中小企業の情報セキュリティ対策ガイドライン」があります。このガイドラインは、「投資対効果が見えづらい」、「どこまで対策すべきか不明である」、「対策を推進する人材が不足している」といった課題を抱える組織がセキュリティ対策を実施していくために役立つツールとなっており、コストをあまりかけずとも実施できる最低限の対策がチェックシートとしてまとめられています。情報セキュリティ対策があまり進んでいない組織にとっての入門書として使いやすい資料となっておりますので、ぜひご活用ください。

【参考】IPA「中小企業の情報セキュリティ対策ガイドライン」
URL: http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html

2.6 BCP (Business Continuity Plan：事業継続計画)

情報セキュリティ事故対応は、事故そのものを復旧することに主眼が置かれていますが、大きな事故では、事業そのものが止まってしまうことも想定されます。BCP (Business Continuity Plan：事業継続計画)は、情報セキュリティ事故だけではなく、地震や火災、深刻な基幹情報システムの故障などの原因によって､組織の事業が継続できなくなった時に最低限の事業継続や短時間での復旧をどの様にして図るかについて計画するものです。BCM (Business Continuity Management：事業継続管理)は計画だけでなく、継続的に改善していく管理システムまで構築することを言います。

近年では、組織はいろいろな外部組織の業務の流れにサプライチェーンとして組み込まれており、１つの組織の業務停止が、他の組織にも影響を及ぼす状況にあります。したがって、自組織が事業継続を行うためには､サプライチェーンとなる他組織の事業継続が必須事項になるために、他組織にも BCP、BCM の対策を求めることが必要になってきます。

BCP を策定する上で参考となる中小企業向けの資料としては、中小企業庁の「中小企業 BCP 策定運用指針」があります。この指針では、中小企業の特性や実状に基づいた BCP の策定及び継続的な運用の具体的方法がわかりやすく説明されており、指針に沿って作業すれば、BCP を完成することができます。

【参考】中小企業庁「中小企業 BCP 策定運用指針」
URL: http://www.chusho.meti.go.jp/bcp/

3　情報セキュリティ事故対応フローとチェックシート

本章では、想定される事故の内容に応じた対応フローと手順を、汎用性を持った内容で示しています。その上で、その手順に沿って事故対応を行うために必要となる事前対策をチェックシートの形式で掲載しています。

3.1 事故対応の汎用パターンと利用方法

２章で述べたように、事故の対応は事故内容に応じて取るべき対応は変わってきます。しかし、発生する可能性のある事故を全て洗い出し、その対応手順を１つ１つ検討してまとめることは現実的ではありません。そこで、ある程度事故の内容をグループ化し、その対応手順をまとめることが必要になります。ここではその事故のグループをなるべく単純化し、下記３つのパターンに分けて対応手順を考えています。

A. 情報システムの障害（利用不能、データ喪失 等）

情報システムの障害により、情報が利用できない、情報の一部を喪失したなどの事故に対する対応手順。主に誰が、どの様に復旧作業を行うかが焦点になります。

B. 情報システムへの攻撃（ウイルス感染、不正アクセス、改ざん 等）

情報システムがウイルス感染や不正アクセス、改ざんなどの攻撃を受けた事故に対する対応手順。意図的な犯行に対して法的措置を検討するかどうかやどの様に復旧するかが焦点になります。

C. 情報漏えい（可能性も含む）

紛失や盗難、または原因が不明な情報漏えい事故の対応手順。情報漏えいを起こした人物が分かっているかどうかにより対応が分かれ、意図的な犯行に対しては法的措置の検討や情報漏えいの被害者に対する対外対応などが焦点になります。

そして、ここでまとめた対応手順は、様々な組織規模や業種での利用を考慮し、汎用的な内容で作成されています。したがって、この汎用的な手順、フローを元に、自組織でそれぞれの事故が発生したときの対応を机上でシミュレーションし、自組織に合わせた修正、追加などを行うことが望まれます。参考として、４章には小規模企業の利用例、５章には中規模企業の利用例を掲載しています。

また、これら自組織の対応手順、フローを一度作成しても、それで終わりではありません。組織の情報システムの構成や外部からの攻撃の内容などの情報システムを取り巻く外部環境は時間の経過とともに変わってきます。このような変化に適応するために対応手順、フローを定期的に見直していく必要があります。

3.2 事故対応フローと対応手順

それでは、上記３つのパターンそれぞれについての事故対応フローと対応手順を見ていきます。まず、フローは、2.3 節で示した情報セキュリティ事故対応の実施フェーズ を縦軸とし、2.4 節で示した情報セキュリティ事故対応のプレイヤー を横軸として作成されています。フローの作成により文章を読むことなく、図で直感的に理解でき、全体の把握が容易になります。

次に対応手順では、事故対応の具体的な手順やポイントを解説しています。各ステップの項目番号は、フローに記入している番号と対応しているので、フローと結び付けて参照することができます。また、対応手順では、具体的な対応を実施するにあたって事前に準備しておくべき対策を、その必要性に応じて***＜事前準備が必須な項目＞***あるいは、***＜事前準備が望まれる項目＞***と記述しています。そして、これらの事前対策については、予め実施できているかを容易に確認できるようにするために、事故対応チェックシートとしてまとめました（※事故対応チェックシートの詳細は、次節（3.4 節）を参照）。

すなわち、本章では、図 4 に示すとおり 3 つの事故のパターンそれぞれについて、フロー、対応手順、チェックシートの 3 つを示しています。

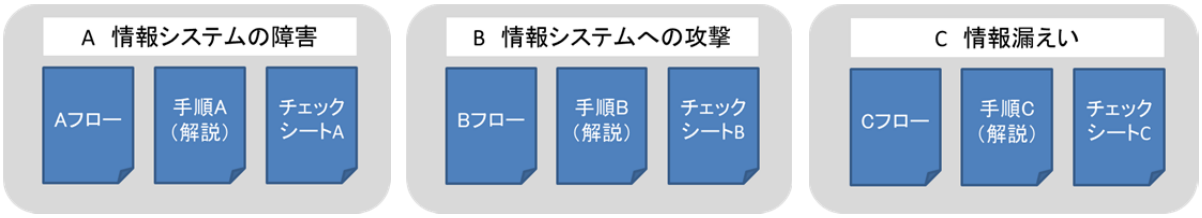


図 4　事故対応フロー・手順とチェックシート

（1）A フロー：情報システムの障害（利用不能、データ喪失 等）

「ファイルサーバが故障して利用できなくなった」あるいは、「ルータが故障してインターネットが利用できなくなった」といったような情報システムの障害の場合の対応フローは、図 5 のようになります。

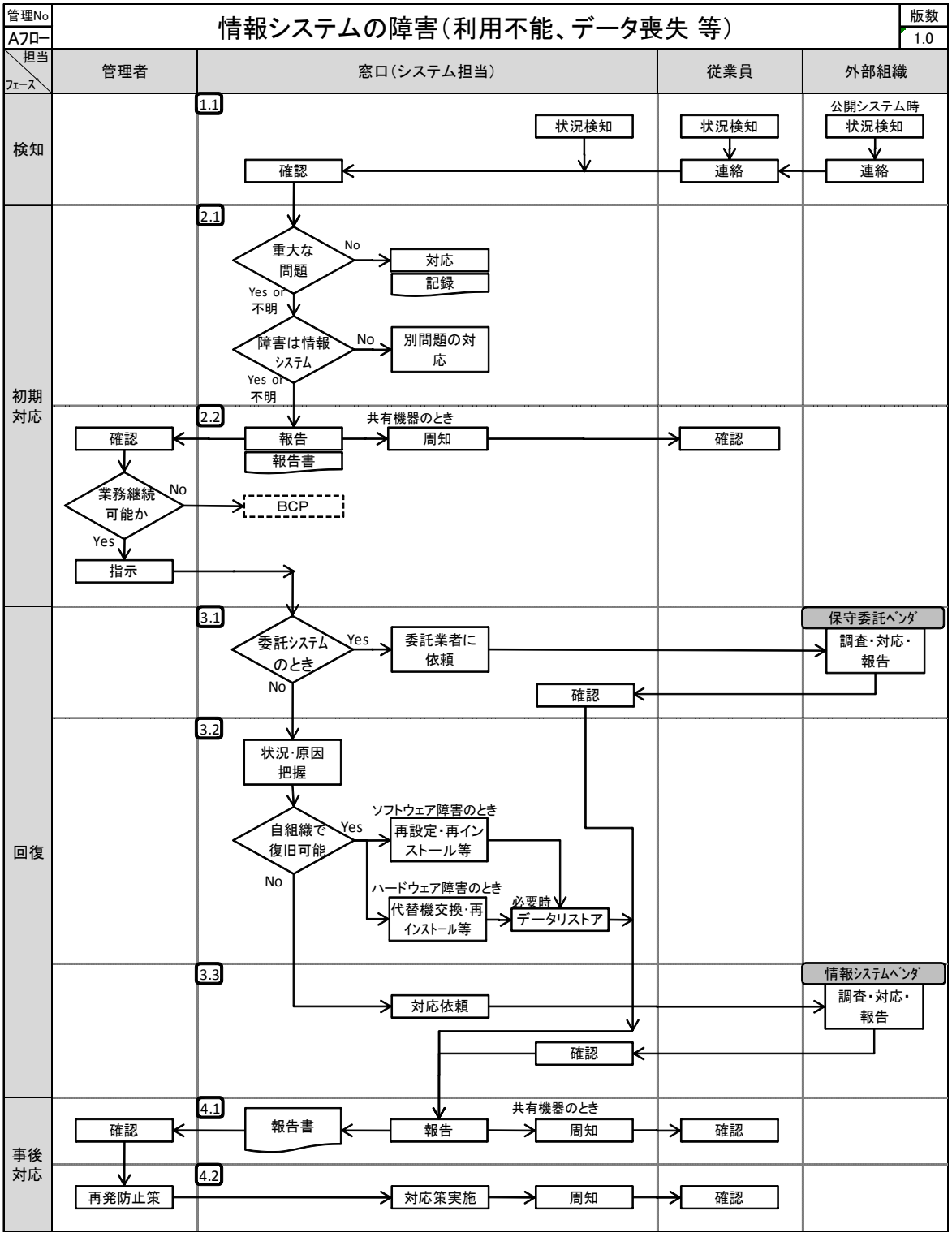


図 5　A フロー：情報システムの障害対応

そして、このフローに沿った具体的な対応手順は以下のようになります。

【フェーズ 1. 検知】

《ステップ 1.1》検知・連絡

① 従業員：情報システムに障害を感じたら、窓口に連絡する。

重要な情報システムにアクセス出来なかったり、アクセス出来ても動作が非常に遅かったなどの場合、事前に定められた窓口に状況を報告する。また、存在するはずのデータが無くなっていたり、あり得ない変更がされているときなども報告する。

＜事前準備が必須な項目＞体制（窓口）の構築、事故発生時の窓口への連絡とその教育

＜事前準備が望まれる項目＞（可用性の面で）重要な情報システムリストとその周知

② 窓口(システム担当)：情報システムの障害を監視し、検知を行う。

各情報システムやネットワークなどを定期的に監視する。正常な稼働状況や高負荷時などのシステムの特性を通常から把握・監視していれば、障害を迅速に検知し、その前兆を早期に把握できる。また、定期的に障害（あるいは障害の前兆）を検知できるような装置・体制を設置し、監視する。

＜事前準備が望まれる項目＞情報システムの定期的監視、障害検知装置の設置

③ 顧客：公開システムで異常を感じたら、組織に連絡がある（ことがある）。

その組織が一般に公開している情報システムで顧客が利用した時に異常（HP が開かない、メールが送れない等）を感じた場合、会社の代表窓口や付き合いのある従業員に連絡が入ることがある。この時も連絡を受けた従業員は、通報者の情報（連絡先、操作内容等）を控え、窓口に連絡を入れる。

④ 窓口(システム担当)：障害の連絡を確認する。

障害の連絡を受けた時、その状況を確認する。

【フェーズ 2. 初期対応】

《ステップ 2.1》問題の切り分け

① 窓口(システム担当)：重大な問題か調査する。

連絡してくる従業員は情報システムの仕組み等に精通していない人が多いため、勘違いや大した問題でない場合でも連絡してくることがある。これを質問や実際の操作等により状況を確認し、勘違いや軽微な問題であれば、その場で解決し、軽微な問題として取り扱う。軽微な問題のときでもこれらは記録し（【付録１】情報システム事故受付表を参照）、定期的にこの記録から情報システムの問題点を検知するのも予防的な情報セキュリティ対策として重要である。そして、その場で解決できず対応が必要な場合、次の手順へと進む。

＜事前準備が望まれる項目＞窓口要員の技術的教育、

情報システム事故受付表と定期的な解析による対策の検討

② 窓口(システム担当)：情報システムの問題か調査する。

実際に障害になっているのが、情報システム自体の問題かどうかを判断する。同一ネットワーク上の他のサーバにも接続が出来ないような問題であれば、LAN 機器やケーブルの問題も考えられる。このときは、対象となる機器やケーブルを絞り込む調査を行う。

情報システムが全く起動できないような問題であれば、設備側の電源系統の問題も考えられる。このときは、同系統の電源の状況、ブレーカーの状況などを確認する。

公開している情報システムの場合は、インターネット接続環境の障害や、サービス拒否攻撃（DoS 攻撃）※1などの可能性がある。これらの障害の切り分けにはインターネット接続環境の確認やログ解析等が必要になる。

また、その他の要因の可能性があるかについても調査・検討する。情報システムへの攻撃（ウイルス感染・DoS 攻撃等）による障害の可能性があれば、「B フロー：情報システムへの攻撃」を参照し、対処する。

＜事前準備が望まれる項目＞窓口要員の技術的教育

システム・ネットワーク構成図、電源系統図

【参考】警察庁「DoS/DDoS 対策について」
URL: http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf

《ステップ 2.2》報告

① 窓口(システム担当)：管理者へ報告する 。

現状および問題解決までの復旧時間や必要な人的、金銭的資源の概要を合わせて管理者に報告し、判断してもらう。このとき、事故の内容について報告するフォーマット（【付録２】情報セキュリティ事故発生報告書を参照）を用意し、記録する。また、事故対応に携わる人に情報が正確に伝わるよう指示・命令及び報告系統を一本化する。

＜事前準備が望まれる項目＞情報セキュリティ事故発生報告書

② 管理者：業務継続に関わる場合、BCP の実施を検討する。

情報システムの復旧に時間がかかりそうな場合、次に取るべき対応を検討する。事業継続に関わる重大な問題であれば、経営者を交え、別途 BCP で検討していた代替運転（オペレーション）を検討する必要がある。通常、BCP は情報システムが機能していない状態でも何とかして業務を継続させるための計画であり、一度その計画での運転が実施されれば元の運用に戻すのにも労力を要するため、BCP の実施には慎重な判断が必要になる。

また、公開している情報システムでは、発表する内容（障害内容等）の検討も行う。

＜事前準備が望まれる項目＞BCP の策定

※1 DoS は、Denial of Services の略。インターネット経由での攻撃の一つで、大量のデータや不正なデータを送りつけることにより相手のコンピュータやルータなどを使用不能に陥らせたり、ネットワークを流れるデータの量を増大させて相手のネットワーを麻痺させる攻撃。

③　窓口(システム担当)：(共有機器の場合）利用者に利用できないことを通知する。

重要な問題のとき、基幹システムやファイルサーバなど、複数の人が利用している情報システムの場合、当該情報システムが利用できない現状を利用者に通知する。その際に、できればある程度の復旧予定時間も通知する。

公開システムでは可能な限り、外部の利用者に正確な現状を公表するように努める。

【フェーズ 3. 回復】

《ステップ 3.1》状況・原因把握と復旧（保守委託品）

①　窓口(システム担当)：(保守委託品の場合）保守委託ベンダに状況を連絡する。

当該情報システムが保守委託品であり、保守契約内容に該当すると考えられる場合は、該当する保守委託ベンダに状況を連絡し、対応を依頼する。このとき、データ復旧（リストア）が必要な場合には、バックアップデータが必要になることがあるので注意する。

＜事前準備が望まれる項目＞保守委託業者の一覧（契約内容含む）

《ステップ 3.2》状況・原因把握と復旧（自社対応）

窓口(システム担当)は、当該情報システムが自社管理品である場合は、障害の原因がソフトウェアの問題か、ハードウェアの問題かを調査・検討し、下記の対応を行う。

①　窓口(システム担当)：(ソフトウェアの問題の場合）再インストール、再設定の実施。

ソフトウェアの問題の場合、障害発生する直前の作業(誤設定はないか)の確認や、ソフトウェアの再インストールが必要か、OS を含めたクリーンインストールが必要かを判断し、実施する。再インストール後、ソフトウェアのアップデート※2が必要な場合があるので、確認する。

＜事前準備が必須な項目＞各情報システムの設定内容リスト、インストール手順書

②　窓口(システム担当)：(ハードウェアの問題の場合）ハードウェア代替機の用意、再インストール。

ハードウェアの問題の場合、部品交換で済むのか、代替機に入れ替える必要があるのかを判断し、実施する。代替機に入れ替えた場合、ソフトウェアのインストールや再設定が必要であればこれも実施する。

＜事前準備が必須な項目＞各情報システムの設定内容リスト、インストール手順書

＜事前準備が望まれる項目＞各情報システムの代替機、予備部品の用意

※2　ソフトウェアを最新のものに更新すること。ソフトウェアには不具合などの脆弱な部分があり、これを放置しておくと、ウイルス感染や不正アクセス等により外部から攻撃ができる状態にしていることになる。ソフトウェアの開発元からはこれを修正するプログラムが提供されることがあるため、ユーザはインターネットなどを介して取り込み、脆弱な部分を解消していく必要がある。

③　窓口(システム担当)：(ソフト/ハードの問題の場合）データ復旧（リストア）の実施。
ソフトウェアの入替え後に、データのリストアが必要な場合は実施する。
＜事前準備が必須な項目＞各情報システムのバックアップ
＜事前準備が望まれる項目＞バックアップデータの定期的な復旧テスト

《ステップ 3.3》状況・原因把握と復旧（対応委託）

①　窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。
原因究明、再設定、再インストール、予備機交換などが（技術的、時間的に）自社で実施できない場合は、対応できる情報システムベンダに状況を説明し、対応を依頼する。データ復旧（リストア）が必要な場合にはバックアップデータが必要になるので注意する。
＜事前準備が望まれる項目＞情報システムサポートベンダ一覧

【フェーズ 4. 事後対応】

《ステップ 4.1》報告

①　窓口(システム担当)：管理者に報告する。
管理者に復旧したことを連絡し、その後、事故の内容等を管理者に報告する。このとき、事故の原因、経過や再発防止策等について記載できるフォーマット（【付録４】情報セキュリティ事故最終報告書を参照）を用意し、これにより報告する。（なお、【付録４】情報セキュリティ事故最終報告書には、再発防止策の記入欄があるが、この内容については管理者の判断が必要になる場合があるため、その場合は《ステップ 4.2》で記入する。）
＜事前準備が望まれる項目＞情報セキュリティ事故最終報告書

②　窓口(システム担当)：(共有機器の場合）利用者に回復したことを連絡する。
情報システムが復旧し、当該情報システムが共有機器のときは、利用者に回復したことを連絡する。代替運転等を実施していた場合は、管理者に連絡し、BCP の手順に従い復旧する。公開システムでは可能な限り、外部の利用者に現状を公表するように努める。

③　管理者：報告の確認。
窓口（システム担当）から受け取った報告書を確認する。

《ステップ 4.2》再発防止

①　管理者：報告書等を元に、再発防止策を検討する。
経営層を交えて、報告書より今後の再発防止策となる情報セキュリティ対策を検討する。
＜事前準備が望まれる項目＞定期的な事故事例の解析と今後の対策

②　窓口(システム担当)：再発防止策を実施し、周知する。
検討された再発防止策を実施し、従業員にその内容を周知、教育する。

上記で述べた事前対策以外にも、情報システムの障害を起こさないために必要な対策があり、以下のようなものが挙げられます。

＜事前準備が必須な項目＞（障害による停止が許されないような情報システムについて）

- 情報システム機器のハードディスクの二重化を実施する。
- 供給する電源異常から情報システムを守るために、無停電電源装置（UPS）等を導入する。
- 盗難や偶発的な破壊などから情報システムを守るために、専用の部屋などに隔離し、安全に管理する。

（2）B フロー：情報システムへの攻撃（ウイルス感染、不正アクセス、改ざん 等）

「ファイルサーバに不正アクセスされた形跡があった」あるいは、「公開しているホームページが改ざんされた」といったような情報システムへの攻撃の場合の対応フローは図 6 のようになります。

そして、このフローに沿った具体的な対応手順は以下のようになります。

【フェーズ 1. 検知】

《ステップ 1.1》検知・連絡

① 従業員：各自の PC でウイルス感染等の兆候を感じたら、LAN ケーブルを切り離し窓口に連絡する。

自分が利用している PC でウイルス感染の兆候、不正アクセスの形跡等を感じた場合、周りの PC への感染や情報漏えいの恐れがあるので、LAN ケーブルを切り離すようにする。そして、事前の操作内容を含め、現在の状況等を窓口に連絡する。また、利用しているサーバ等で同様の兆候を感じたときも同様に窓口に連絡する。

＜事前準備が必須な項目＞体制（窓口）の構築、事故発生時の窓口への連絡とその教育

② 窓口(システム担当)：情報システムへの攻撃を監視し、検知を行う 。

各情報システムやネットワークなどを定期的に監視する。正常な稼働状況や高負荷時などのシステムの特性を通常から把握・監視していれば、攻撃を迅速に検知し、その前兆を早期に把握できる。

例えば、ウイルス検知では、各クライアント PC のウイルス検知状況をサーバ側で一元管理できるウイルス対策ソフトを導入して監視することがあげられる。不正アクセス検知では、重要な情報システムのアクセスログを収集し、定期的に解析したり、IDS（不正侵入検知システム）※3、IPS（不正侵入防止システム）※4などの装置を導入し検知することがあげられる。

＜事前準備が望まれる項目＞情報システムのアクセスログ取得と定期的なログ解析、
サーバ側で一元管理可能なウイルス対策ソフトの導入、
ネットワークの定期的監視、不正侵入検知装置の設置

③ 顧客：公開システムで異常を感じたら、組織に連絡がある（ことがある）。

その組織の HP やメールなど、顧客が利用した時に異常（HP が改ざんされている等）を感じた場合、会社の代表窓口や付き合いのある従業員に連絡が入ることがある。この時は連絡を受けた従業員が、通報者の情報（連絡先、改ざん内容等）を控え、窓口に連絡を入れる。

※3 IDS は Intrusion Detection System の略。ネットワーク回線を監視し、侵入を検知して通知するシステム。不正アクセスでよく用いられる手段をパターン化して記録しておき、ネットワーク回線内を流れるパケット（データ）とパターンを比較することにより不正アクセスを検知する。

※4 IPS は Intrusion Prevention System の略。IDS の機能を拡張し、侵入を検知するだけではなく侵入を検知したら通信を遮断するなどの防止策を自動的に実施する機能を持っている。

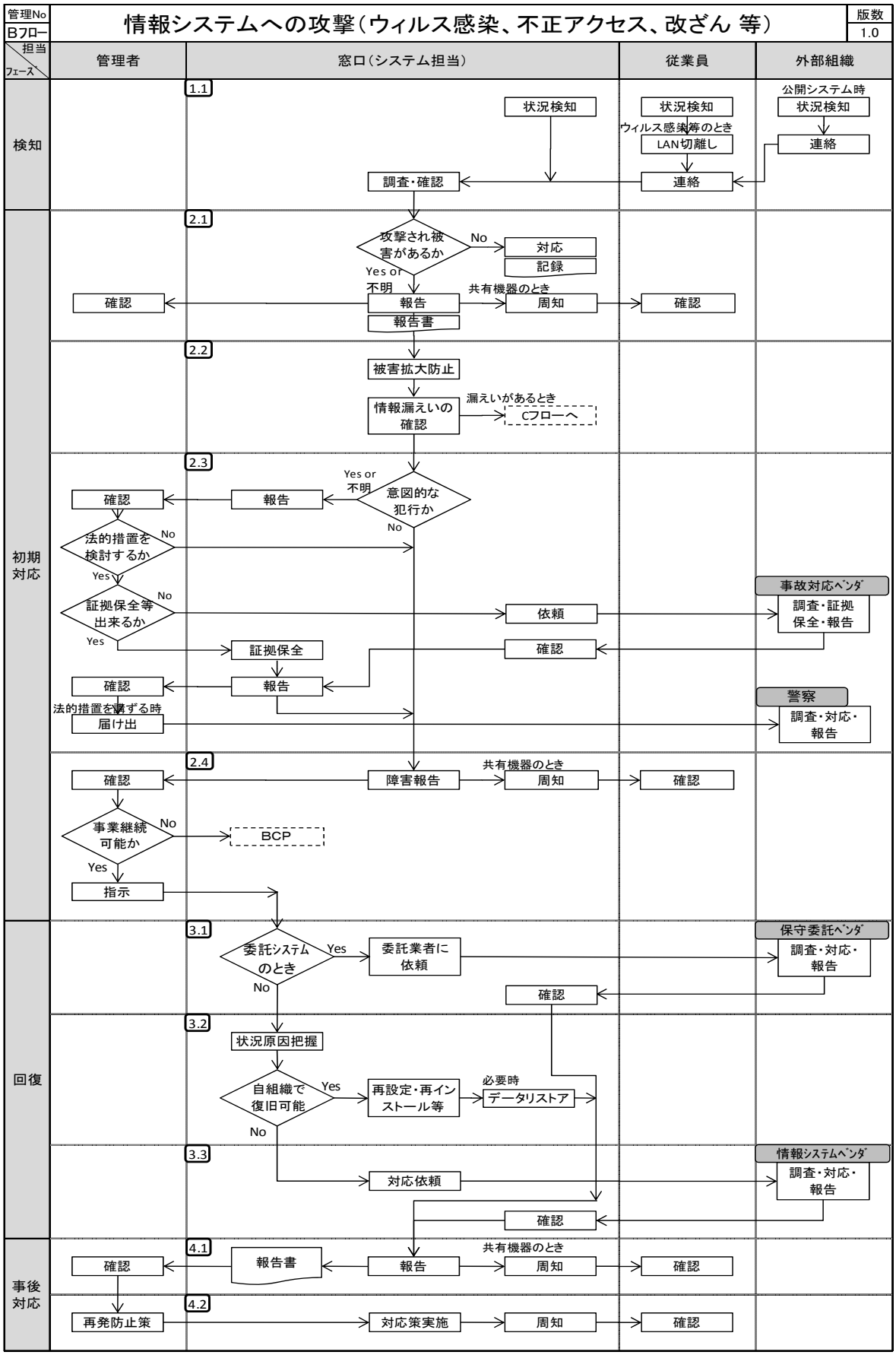


図 6　B フロー：情報システムへの攻撃対応

④　窓口(システム担当)：攻撃の連絡を確認する。

攻撃の連絡を受けた時、その状況を確認する。

【フェーズ 2. 初期対応】

《ステップ 2.1》問題の切り分けと報告

①　窓口(システム担当)：情報システムへの攻撃で、被害があるか確認する。

連絡を受けた内容を確認し、思い違いや別の問題でないかなどを調査する。また、ウイルス対策ソフトがウイルスを検知したときでも、ウイルスとして検知して即時に駆除した場合は、記録で留める（【付録 1】情報システム事故受付表を参照)。不正アクセスの兆候が確認された場合は、最終的に実際には不正アクセスされていないと判断できるまで、表面的に被害がないかどうかだけで判断せずに調査を続ける。

このとき、《ステップ 2.3》意図的犯行時の対応 を実施する可能性があるので、情報システムを停止したり、情報システムの設定やデータを不用意に操作することは控える必要がある。

思い違いやウイルス対策ソフトの誤検知などウイルス感染ではなかった場合や、ウイルス対策ソフトでの即時駆除などの場合でも、これらは記録する。そして、定期的にこの記録から情報セキュリティ対策の問題点を把握することも予防的な情報セキュリティ対策として重要である。また、情報システムの障害による問題であれば、「A フロー：情報システムの障害」を参照し対処する。

＜事前準備が望まれる項目＞窓口要員の技術的教育、

情報システム事故受付表と定期的な解析による対策の検討

【参考】IPA では、コンピュータウイルスや不正アクセスについての相談窓口を設けている。

「情報セキュリティ安心相談窓口」

URL:http://www.ipa.go.jp/security/anshin/

TEL:03-5978-7509

②　窓口(システム担当)：管理者へ報告する。（共有システムの場合）利用者に使用中止を呼びかける。

攻撃が考えられる場合、管理者に連絡し、複数の人が利用している情報システムの場合、利用者に使用の中止を呼びかける。

このとき、事故の内容について記録出来るフォーマット（【付録２】情報セキュリティ事故発生報告書を参照）を用意し、記録する。また、事故対応に携わる人に情報が正確に伝わるよう指示・命令及び報告系統を一本化する。

＜事前準備が望まれる項目＞情報セキュリティ事故発生報告書

《ステップ 2.2》被害拡大の防止

① 窓口(システム担当):攻撃を受けた状況により、被害拡大が防止できる対策があれば実施する。

サーバでのウイルス感染や不正アクセスが予想される時は、サーバを隔離（ネットワークケーブルを外す）し、感染拡大を抑える。

② 窓口(システム担当):（攻撃を受けた場合）情報漏えいの有無を確認する。

攻撃を受けた場合、情報漏えいの恐れがある。情報が漏えいしていないかログ等で確認し、重要な情報が漏えいしていた場合、これに対応する必要がある。このとき、「C フロー：情報漏えい」を参照し対処する。

＜事前準備が望まれる項目＞情報システムのアクセスログ取得とログ解析

《ステップ 2.3》意図的犯行時の対応

① 窓口(システム担当):意図的な犯行による攻撃が疑われるときは、管理者に報告をする。

ログの確認や情報システムの状況により、不正アクセスや改ざんなど、犯罪が疑われるときは、管理者に報告する。

＜事前準備が望まれる項目＞情報システムのアクセスログ取得とログ解析技術

② 管理者：意図的な犯行による攻撃が疑われるときは、法的措置を検討するか判断する。

意図的な犯罪による攻撃が疑われ、被害があるときは、経営層を交えて法的措置を検討する。このとき、証拠保全を行う必要がある。情報システムの証拠保全にはフォレンジック※5の高度な技術が必要となる。システム担当者と相談し、自社で対応できない場合は、情報セキュリティ事故対応ができるベンダに依頼することを検討する。

＜事前準備が望まれる項目＞情報セキュリティ事故対応ベンダ一覧

【参考】特定非営利活動法人デジタル・フォレンジック研究会
「証拠保全ガイドライン　第１版」
URL: http://www.digitalforensic.jp/eximgs/100405gijutsu.pdf

※5　デジタル・フォレンジックまたはコンピュー・フォレンジックと呼ばれる言葉を指し、不正アクセスや機密情報漏えいなどコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称を意味する。

③　窓口(システム担当)：意図的な犯行による攻撃が疑われるときは、証拠保全を行う。

管理者より証拠保全の指示があった場合、証拠保全を行い、管理者に報告する。

また、自社で証拠保全が対応できない場合は、情報セキュリティ事故対応ベンダに依頼し、ベンダからの調査結果を確認後、管理者に報告する。

＜事前準備が望まれる項目＞（自社で証拠保全を行う場合）

システム担当者のフォレンジック技術習得

④　管理者：調査報告を受け、法的措置を講ずるか判断する。

証拠保全等の調査結果がまとまった段階で報告を受け、その内容を精査し（本当に意図的な攻撃だったのか、証拠として出せるものがあるか、法的措置に意味があるか等)、場合により弁護士と相談する。法的措置を講ずると決定した場合、警察に証拠とともに届け出る。

《ステップ 2.4》（障害）報告

①　窓口(システム担当)：管理者に障害の状況を報告する。

管理者へ情報システムの障害状況を報告し、下記②の状況も踏まえつつ、次の対応を検討する。

②　管理者：（事業継続に関わる場合）BCP の実施を検討する。

情報システムの復旧に時間がかかりそうな場合、次に取るべき対応を検討する。事業継続に関わる重大な問題であれば、経営者を交え、別途 BCP で検討していた代替運転（オペレーション）を検討する必要がある。公開システムでは、発表する内容（障害内容等）の検討も行う。

＜事前準備が望まれる項目＞BCP の策定

③　窓口(システム担当)：（共有システムの場合）利用者に利用できないことを通知する。

重要な問題のとき、基幹システムやファイルサーバなど、複数の人が利用している情報システムの場合、当該情報システムが利用できない現状を利用者に通知する。その際に、できればある程度の復旧予定も通知する。 公開システムでは可能な限り､外部の利用者に現状を公表するように努める。

【フェーズ 3. 回復】

《ステップ 3.1》復旧（保守委託品）

①　窓口(システム担当)：（保守委託品の場合）保守委託ベンダに状況を連絡する。

当該情報システムが保守委託品であり、保守契約内容に該当すると考えられる場合は、該当する保守委託ベンダに状況を連絡し、対応を依頼する。データ復旧が必要な場合にはバックアップデータが必要になるので注意する。

＜事前準備が望まれる項目＞保守委託業者の一覧（契約内容含む）

《ステップ 3.2》復旧（自社対応）

① 窓口(システム担当)：再インストール、再設定の実施。

（ウイルス感染の場合）感染したウイルス名を特定し、ウイルス対策ベンダの Web サイト等で対処方法を確認し、実施する。可能であれば、クリーンインストールを実施する。

それ以外にソフトウェアに問題がある場合、設定変更で済むのか、ソフトウェアの再インストールが必要か、OS を含めたクリーンインストールが必要かを判断し、実施する。

再インストール後、ソフトウェアのアップデートが必要な場合があるので、確認する。

＜事前準備が必須な項目＞各情報システムの設定内容リスト、インストール手順書

② 窓口(システム担当)：データ復旧（リストア）の実施。

ソフトウェアの入替え後に、データのリストアが必要な場合は実施する。

＜事前準備が必須な項目＞各情報システムのバックアップ

＜事前準備が望まれる項目＞バックアップデータの定期的な復旧テスト

《ステップ 3.3》復旧（対応委託）

① 窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。

再設定、再インストールなどが（技術的、時間的に）自社で実施できない場合は、対応できる情報システムベンダに状況を説明し、対応を依頼する。データ復旧（リストア）が必要な場合にはバックアップデータが必要になるので注意する。

＜事前準備が望まれる項目＞情報システムサポートベンダ一覧

【フェーズ 4. 事後対応】

《ステップ 4.1》報告

① 窓口(システム担当)：管理者に報告する。

管理者に復旧したことを連絡し、その後、事故の内容等を管理者に報告する。このとき、事故の原因、経過や再発防止策等について記載できるフォーマット（【付録４】情報セキュリティ事故最終報告書を参照）を用意し、これにより報告する。（なお、【付録４】情報セキュリティ事故最終報告書には、再発防止策の記入欄があるが、この内容については管理者の判断が必要になる場合があるため、その場合は《ステップ 4.2》で記入する。）

＜事前準備が望まれる項目＞情報セキュリティ事故最終報告書

② 窓口(システム担当)：（共有機器の場合）利用者に回復したことを連絡する。

情報システムが復旧し、当該情報システムが共有機器のときは、利用者に回復したことを連絡する。代替運転等を実施していた場合は、管理者に連絡し、BCP の手順に従い復旧する。公開システムでは可能な限り、外部の利用者に現状を公表するように努める。

③　管理者：報告の確認。

窓口（システム担当）から受け取った報告書を確認する。

《ステップ 4.2》再発防止

①　管理者：報告書等を元に、再発防止策を検討する。

経営層を交えて、報告書より今後の再発防止策となる情報セキュリティ対策を検討する。

*＜事前準備が望まれる項目＞*定期的な事故事例の解析と今後の対策

②　窓口(システム担当)：再発防止策を実施し、周知する。

検討された再発防止策を実施し、従業員にその内容を周知、教育する。

上記で述べた事前対策以外にも、情報システムへの攻撃を受けないために必要な対策があり、以下のようなものが挙げられます。

＜事前準備が必須な項目＞

- 情報システム（OS、アプリケーション）は可能な限り最新の状態を保つように更新する。
- クライアント PC への不用意なソフトのインストールを制限し、私有 PC や USB メモリ等の業務使用の是非を明確にする。
- 情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにする。
- 情報システムへのアクセスのためのパスワードは他の人に分からないように管理する。

（3）C フロー：情報漏えい（可能性も含む）

重要な情報の紛失、置き忘れ、盗難、誤廃棄、誤送信等の情報漏えいの場合の対応フローは、図 7 のようになります。

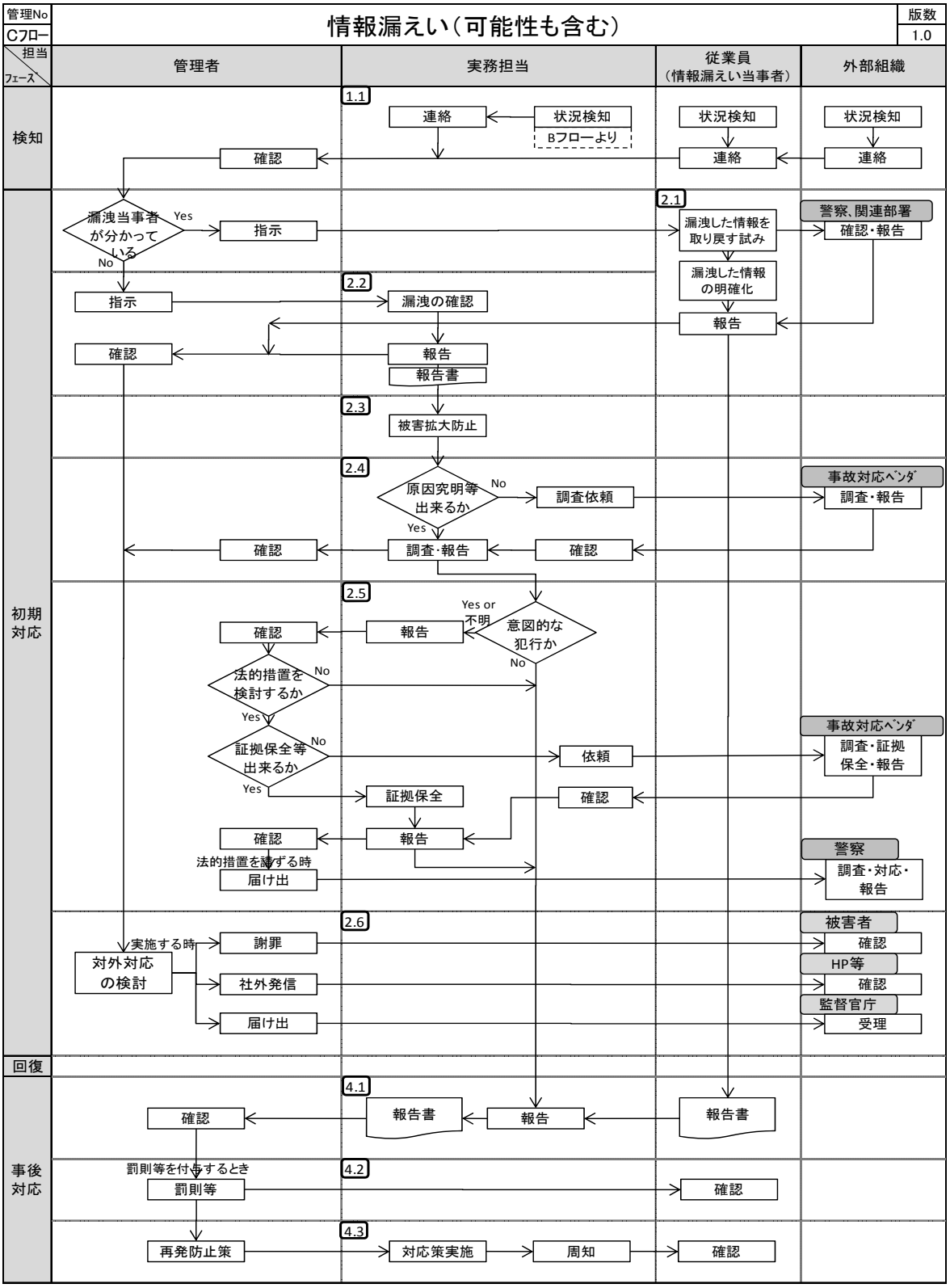


図 7　C フロー：情報漏えいの対応

そして、このフローに沿った具体的な対応手順は以下のようになります。

【フェーズ 1. 検知】

《ステップ 1.1》検知・連絡

① 漏えい当事者：管理者に連絡する。

重要な情報を漏えい（紛失、盗難、誤送信、誤公開、誤廃棄 等）してしまった場合、直ちに管理者に連絡する。

＜事前準備が必須な項目＞体制（連絡窓口）の構築、
事故発生時の管理者への連絡とその教育

＜事前準備が望まれる項目＞（機密性の面で）重要な情報(システム)リストとその周知

② 実務担当：情報システムからの情報漏えいを監視し、検知を行う。

各情報システムやネットワークなどを定期的に監視し、漏えいを検知した場合は、管理者に連絡する。なお、「B フロー：情報システムへの攻撃」の《ステップ 2.2》で情報漏えいが確認されたときも、ここで検知されたことに相当するため、以降の手順に沿って同様な対応を実施する。

情報漏えいを検知するには、重要な情報システムのアクセスログを収集し、定期的に解析することが有用である。情報漏えいを非常に問題視するようであれば、コンピュータの操作内容を記録したり、情報漏えいを検知するようなソフトウェアを導入することも検討する。

＜事前準備が望まれる項目＞情報システムの定期的監視、アクセスログ取得と定期的なログ解析

③ 顧客：情報が漏えいしているのに気付いた時、組織に連絡がある（ことがある）。

インターネット上の掲示板に情報が漏えいしていたり、情報が格納された情報システムやファイル等を入手した時、組織に連絡があることがある。この時は連絡を受けた従業員が、通報者の情報（連絡先等）を控え、詳細を聞きとり、管理者に連絡する。

④ 管理者：情報漏えいの連絡を確認する。

漏えいの連絡を受けた時、その内容を確認する。

【フェーズ 2. 初期対応】

《ステップ 2.1》当事者の初期対応

① 管理者：漏えい当事者が分かっている場合（紛失、盗難 等）、当事者に指示を出す。

紛失や盗難など、漏えいの当事者が明らかな場合は、その当事者に、下記②、③の対応を行うよう指示を出す。

② 漏えい当事者：(情報の紛失等の場合) 関係各所へ連絡し捜索の依頼、警察への届出等を行う。

紛失、盗難、誤廃棄等では、当事者が関連場所に連絡をし、発見に努め、警察への届け出も行う。誤公開では、公開してしまった情報を削除したり、公開設定を直す。誤送信では、送り先に送信してしまった情報の削除を依頼する。

③ 漏えい当事者:(情報の紛失等の場合)紛失した情報にどんなものがあったか明確にし、管理者に報告する。

紛失した情報（システム）にはどのような重要な情報があったか、アクセス制御、暗号化の有無なども明確にする必要がある。したがって、平常時からこれらを明確に把握するために持ち出す情報の内容を記録しておく必要があり、あわせて、情報を持ち出すときの許可手順など持ち出しに関する規定を事前に定めておく必要がある。上記②、③の結果はすぐに管理者に報告する。

＜事前準備が必須な項目＞（持ち出す情報の記録を含めた）重要な情報の持ち出しに関する規定の整備

《ステップ 2.2》問題の切り分け

① 管理者：漏えい当事者が不明な場合、実務担当に指示を出す。

漏えいの当事者が不明な場合（漏えいした事実のみ明らかな場合）は、実務担当に漏えいの確認の指示を出す。このとき、実務担当は事前に体制構築時に決定しておく事項であり、情報システムに関わる漏えい事故が考えられる場合は、システム担当等が確認作業を行う必要がある。

＜事前準備が望まれる項目＞体制（実務担当）の構築

② 実務担当：情報漏えいか確認し、管理者に報告する。

管理者からの指示により、本当に漏えい事故か確認し、漏えい事故と考えられる場合は、管理者に報告する。

このとき、事故の内容について記録出来るフォーマット（【付録２】情報セキュリティ事故発生報告書を参照）を用意し、事故対応に携わる人に情報が正確に伝わるようにする。

【参考】IPA「情報漏えい対策のしおり」
URL: http://www.ipa.go.jp/security/antivirus/documents/5_roei_v3_2.pdf

＜事前準備が望まれる項目＞実務担当の技術的教育、
情報セキュリティ事故発生報告書

③ 管理者：情報漏えいに関して、報告を受ける。

実務担当や、漏えい当事者から情報漏えいの状況について報告を受ける。そして、対外対応（被害者への謝罪、社外発信、監督官庁への届け出）について検討を始める。

《ステップ 2.3》被害拡大の防止

① 実務担当：情報漏えいした情報・状況により、被害拡大が防止できる対策があれば実施する。

情報システムにリモート接続可能な PC やアカウントの紛失時には、リモートアカウントの停止、パスワードの変更などを実施する。Web での誤公開時は、公開情報をすぐに修正するなど、被害が拡大しない対策があれば実施する。

このとき、下記《ステップ 2.4》意図的犯行時の対応 を実施する可能性があるので、システムを停止したり、システム内への不用意な操作は控える必要がある。

＜事前準備が望まれる項目＞実務担当の技術的教育

《ステップ 2.4》情報漏えい元、情報漏えい原因の調査

① 実務担当：情報漏えいした情報・状況により、情報漏えい元、情報漏えい原因を調査する。

実際に漏えいした情報や状況などから、情報漏えい元（誰が、何によって漏えいさせたか）や情報漏えいの原因（どんな理由、状況で漏えいさせたか）を調査する。

状況によっては、ログの解析や高度な技術が必要になることがある。自社で対応できない場合は、管理者と相談し、情報セキュリティ事故対応ができるベンダに依頼することも検討する。

＜事前準備が望まれる項目＞情報システムのアクセスログ取得とログ解析技術、
情報セキュリティ事故対応ベンダ一覧

② 実務担当：調査結果を管理者に報告する。

調査結果を管理者に報告する。また、自社で証拠保全が対応できない場合は、情報セキュリティ事故対応ベンダに依頼し、ベンダからの調査結果を確認後、管理者に報告する。

③ 管理者：調査報告を受ける。

調査報告を受ける。場合により、この結果を《ステップ 2.6》対外対応 における報告、発表内容に含めることを検討する。

《ステップ 2.5》意図的犯行時の対応

① 実務担当：意図的な犯行による情報漏えいが疑われるときは、管理者に報告をする。

ログの確認や情報システムの状況により、意図的な漏えいなどの犯罪が疑われるときは、管理者に報告する。

＜事前準備が望まれる項目＞情報システムのアクセスログ取得とログ解析技術

② 管理者：意図的な犯行による情報漏えいが疑われるときは、法的措置を検討するか判断する。

意図的な犯罪による漏えいが疑われ、被害があるときは、経営層を交えて法的措置を検討する。このとき、証拠保全を行う必要がある。情報システムの証拠保全にはフォレンジックの高度な技術が必要となる。システム担当者と相談し、自社で対応できない場合は、情報セキュリティ事故対応ができるベンダに依頼することを検討する。

＜事前準備が望まれる項目＞情報セキュリティ事故対応ベンダ一覧

③ 実務担当：意図的な犯行による情報漏えいが疑われるときは、証拠保全を行う。

管理者より、証拠保全の指示があった場合、証拠保全を行い、管理者に報告する。また、自社で証拠保全が対応できない場合は、情報セキュリティ事故対応ベンダに依頼し、ベンダからの調査結果を管理者に報告する。

＜事前準備が望まれる項目＞（自社で証拠保全を行う場合）
システム担当者のフォレンジック技術習得

④ 管理者：調査報告を受け、法的措置を講ずるか判断する。

証拠保全等の調査結果がまとまった段階で報告を受け、その内容を精査（本当に意図的な情報漏えいだったのか、証拠として出せるものがあるか、法的措置に意味があるか等）し、場合により弁護士と相談する。法的措置を講ずると決定した場合、警察に証拠とともに届け出る。

《ステップ 2.6》対外対応

① 管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP 等での社外発信を行うか検討する。

顧客への二次被害の防止等もあり、顧客への謝罪を行う。規模や影響が大きい場合、HP 等での社外発信やマスコミへの発表等を検討する。また、このときは相談窓口の設置も検討する。

② 管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。

個人情報保護法の観点から、監督官庁への届出を行う必要がある。各事業領域の「個人情報の保護に関するガイドライン」等参照のこと。

【参考】消費者庁「個人情報の保護」
URL: http://www.caa.go.jp/seikatsu/kojin/

【フェーズ 3. 回復】

※情報漏えいの場合、回復フェーズとして必ず実施すべき手順はない。

【フェーズ 4. 事後対応】

《ステップ 4.1》報告

① 漏えい当事者、実務担当：情報セキュリティ事故の内容を報告書にまとめ、管理者に提出する。

漏えい当事者や実務担当は、事故の内容等を管理者に報告する。このとき、事故の原因、経過や再発防止策等について記載できるフォーマット（【付録４】情報セキュリティ事故最終報告書を参照）を用意し、これにより報告する。（なお、【付録４】情報セキュリティ事故最終報告書には、再発防止策の記入欄があるが、この内容については管理者の判断が必要になる場合があるため、その場合は《ステップ 4.3》で記入する。）

＜事前準備が望まれる項目＞情報セキュリティ事故最終報告書

② 管理者：報告書の受理とその他の事後対応を行う。

漏えい当事者、実務担当から報告書を受け取り確認する。また、HP 等で情報漏えいの内容を発信した場合、最終的にどのようになったかをまとめ、再発信する。

《ステップ 4.2》処罰等

① 管理者：漏えい当事者に対し、処罰等を行うか検討する。

経営層を交え、社内規定、状況などを勘案し、情報漏えいを起こした当事者に対し、処罰を行うかどうか検討する。また、委託業者が漏えい事故を起こした時は、経営層を交え、秘密保持契約、状況などを勘案し、情報漏えいを起こした委託業者に対し、損害賠償請求を行うか検討する。

＜事前準備が必須な項目＞従業員に対する守秘義務規定および委託先との機密保持契約

＜事前準備が望まれる項目＞従業員への処罰基準、委託業者への損害賠償請求基準

《ステップ 4.3》再発防止

① 管理者：報告書等を元に、再発防止策を検討する。

経営層を交えて、報告書より今後の再発防止策となる情報セキュリティ対策を検討する。

＜事前準備が望まれる項目＞定期的な事故事例の見直しと今後の対策

② 実務担当：再発防止策を実施し、周知する。

検討された再発防止策を実施し、従業員にその内容を周知、教育する。

上記で述べた事前対策以外にも、情報漏えいを起こさないために必要な対策があり、以下のようなものが挙げられます。

＜事前準備が必須な項目＞

- 事務所における情報システムや重要な書類の盗難防止策を実施する。
- 情報破棄時の情報が読めなくなるような施策（紙・CD のシュレッダー、HDD の完全消去等）を実施する。

- メール利用時の誤送信（宛名間違え、BCC 未活用等）防止や添付ファイルの暗号化を実施する。
- 盗難や偶発的な破壊などから情報システムを守るために、専用の部屋などに隔離し、安全に管理する。
- ウイルス対策ソフトを導入し、常に最新の状態を維持する。
- 情報システム（OS、アプリケーション）は可能な限り最新の状態を保つように更新する。
- クライアント PC への不用意なソフトのインストールを制限し、私有 PC や USB メモリ等の業務使用の是非を明確にする。
- 情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにする。
- 情報システムへのアクセスのためのパスワードは他の人に分からないように管理する。

3.3 事故対応チェックシート

3.2 節の対応手順で示した*＜事前準備が必須な項目＞*と*＜事前準備が望まれる項目＞*を抽出し、事故対応を実施する際に必要となる事前対策を確認するために事故対応チェックシートを作成しました（図 8～図 10）。 このチェックシートでは、本書をチェックシートから利用し始めるケースを想定して、チェック項目に書かれた対策を実施することの必要性がわかるよう項目ごとに解説を「解説」欄に記載するとともに、3.2 節で示した対応手順の該当箇所を「ステップ」欄に示しています。また、項目ごとにその項目をチェックして対策を実施すべき人が異なるため、その項目の対象が管理者か窓口（または実務）か従業員かを「担当」欄に記載しています。今回、3 つの事故のパターンそれぞれについて、チェックシートを作成しているため、3 つの間で共通する項目が存在します。そのため、各パターン固有の項目か他のパターンとも共通している項目かが判別できるよう「共通」欄を設けてあります。

このチェックシートの項目について、事前に対応が出来ていれば、実際に事故が発生した場合でも、問題なく対処が可能な環境が整えられていることになります。逆にこれらの項目が事前に対応できていないときには、事故の対応が取れない可能性が出てきます。特にチェックシートの「レベル」欄に「必須」と記載された項目については注意する必要があります。なお、「レベル」欄に「必須」と記載された項目は、3.3 節の対応手順で示した*＜事前準備が必須な項目＞*に相当し、「検討」と記載された項目は、*＜事前準備が望まれる項目＞*に相当します。

情報システムの障害対策チェックシート							
No	共通	Check	レベル	チェック項目	解説	ステップ	担当
A01			必須	事故発生時の窓口組織等の体制を構築し、これを従業員に周知していますか？	事故が発生したときに連絡する窓口などの体制を事前に構築し、これを従業員が理解し実践することが必要になります。	1.1.①	従業員
A02			検討	可用性の面で重要な情報システムを把握し、これを従業員に周知していますか？	利用ができないことで業務に支障が出るような情報システムを重要な情報システムと定め、これを従業員全体で認識することで事故検知が確実に行えるようになります。	1.1.①	従業員
A03			検討	情報システムの定期的な監視や障害検知装置の設置を実施していますか？	情報システムを定期的に監視したり、障害検知装置を導入することで、障害の事前検知や障害の早期検知が可能になります。	1.1.②	窓口
A04			検討	事故対応の窓口要員に対して技術的な教育を受けさせていますか？	事故対応では、問題の切り分けや復旧など、技術的な知識が必要になるため、これらの知識を事前に身につけることが求められます。	2.1.① 2.1.②	窓口
A05			検討	情報システム事故を受け付けたときにこれを記録(情報システム事故受付表 等)し、定期的にこの記録を評価していますか？	事故の連絡を受けたが、実際には事故では無く軽微な問題だった時も、これを記録し評価することで、事故を未然に防ぐことや他の問題解決に繋がることがあります(ヒヤリ・ハットの考え方)。	2.1.①	窓口
A06			検討	システム・ネットワーク構成図や電源系統図を管理していますか？	システム・ネットワーク構成図や電源系統図は、ネットワーク障害や電源障害の問題解決に役立ちます。これらの文書の用意と更新管理を実施することが重要です。	2.1.②	窓口
A07			検討	事故内容とその対応について記録し事故対応者で記録・共有するもの(事故発生報告書 等)を用意し利用していますか？	事故の内容やその対応について逐次記録することで、対応内容を忘れず、事故対応する人の中で情報が共有できます。そのための様式を事前に作成し利用することで、記録漏れなどが防げ、管理も容易になります。	2.2.① 4.1.①	窓口
A08			検討	BCP(事業継続計画)を策定し、どの様な情報システムの事故のとき、これを実施するか定めていますか？	情報システムの中には、事故により事業の継続が出来なくなるようなものも考えられます。これらを事前に検討し、事故が起きた時の計画(BCP)を策定し、運用することが求められます。	2.2.②	管理者
A09			検討	情報システムの中で保守を委託しているシステムの保守委託業者を、その契約内容を含め、把握していますか？	情報システムは、その環境、ハードウェア、ソフトウェア、コンテンツなどから構成され、それぞれ管理を委託しているものがあると思われます。これらをその契約内容と共に事前にまとめておくことで迅速な対応が可能になります。	3.1.①	窓口
A10			必須	自社で管理している情報システムの各設定内容や、インストールの手順書などを事前にまとめ、管理していますか？	自社で管理を行っている情報システムでは障害復旧時には自社で対応する必要があります。そのためには各種の設定内容やシステム構築のための手順などを事前にまとめ管理しておくことが求められます。	3.2.① 3.2.②	窓口
A11			検討	各情報システムの代替機や予備部品などを事前に用意していますか？	情報システムの障害復旧のために、ハードウェアを修理したり、1からシステムを再構築し直していると時間がかかります。長時間の停止が許されない情報システムでは、代替機や代替部品を事前に用意することが求められます。	3.2.②	窓口
A12			必須	各情報システムで、データのバックアップのルールを決め、定期的に実施していますか？	情報システムの事故により、作成されたデータは利用できなくなることがあります。データを定期的にバックアップするルールを決め、実施することは必須事項です。	3.2.③	窓口
A13			検討	バックアップデータを定期的にリストアするようなテストや確認を定期的に実施していますか？	バックアップを定期的に実施しているつもりでも、実際にデータが正しく取れていないことがあります。定期的にバックアップデータを戻すことで、バックアップが正しく行われていることを確認することが望まれます。	3.2.③	窓口
A14			検討	自社で管理している情報システムで事故の復旧が出来ない場合など、事故復旧をサポートできるベンダを事前に把握していますか？	自社で管理している情報システムでは、自社で事故の復旧が必要とされます。迅速に復旧できない時など、これらの作業をサポートできる業者(ベンダ)を事前に把握しておくことが求められます。	3.3.①	窓口
A15			検討	定期的に発生した事故を組織的に評価・検証することで、今後のセキュリティ対策に役立てていますか？	情報システムの事故は定期的に要因の分析や対応内容などを分析し、事前対策に活かすことで、事故を未然に防げる可能性が高まります。	4.2.①	管理者
A16			必須	重要な情報システム機器ではハードディスクの二重化が行われていますか？	ハードディスクは情報システムの中で故障が起こりやすい部品です。障害による中断が許されないような情報システムでは、ハードディスクの二重化が求められます。	事前準備	管理者
A17			必須	重要な情報システムでは無停電電源装置が導入されていますか？	停電等により、情報システムの停止やこれによるハードディスクやデータの破壊などが発生する恐れがあります。重要な情報システムでは無停電電源装置の導入が必要となります。	事前準備	管理者
A18			必須	重要な情報システムは専用のエリアに入れ、安全に管理されていますか？	盗難や偶発的な破壊、温度上昇などから守るために、重要な情報システムは専用のエリア、部屋などに集約、隔離し、安全に管理することが必要となります。	事前準備	管理者

図 8　情報システムの障害対策チェックシート

情報システムへの攻撃対策チェックシート							
No	共通	Check	レベル	チェック項目	解説	ステップ	担当
B01	A01 共通		必須	事故発生時の窓口組織等の体制を構築し、これを従業員に周知していますか？	事故が発生したときに連絡する窓口などの体制を事前に構築し、これを従業員が理解し実践することが必要になります。	1.1.①	従業員
B02			必須	情報システムでアクセスログを取得し、定期的にログをチェックしていますか？	情報システムでは、ユーザの操作等のログを取り、このログを定期的にチェックすることで、不正なアクセスの検知や事故後の原因究明に活かしたり、証拠とすることができます。	1.1.② 2.2.② 2.3.①	窓口
B03			必須	各コンピュータでウイルス対策ソフトを導入し、常に最新の状態を維持し、動作の確認を行っていますか？	コンピュータにウイルス対策ソフトを導入し、常に最新の状態を維持することで、ウイルス検知・駆除が行えます。またこれらを管理できるソフトであれば検知・駆除の状況が一覧できます。	1.1.②	窓口
B04			検討	ネットワークの定期的な監視や不正侵入検知装置（IDS等）の設置を実施していますか？	ネットワークを定期的に監視したり、不正侵入検知装置（IDS）を導入することで、不正侵入の早期検知が可能になります。	1.1.②	窓口
B05	A04 共通		検討	事故対応の窓口要員に対して技術的な教育を受けさせていますか？	事故対応では、問題の切り分けや復旧など、技術的な知識が必要になるため、これらの知識を事前に身につけることが求められます。	2.1.①	窓口
B06	A05 共通		検討	情報システム事故を受け付けたときにこれを記録（情報システム事故受付表 等）し、定期的にこの記録を評価していますか？	事故の連絡受けたが、実際には事故では無く軽微な問題だった時も、これを記録し評価することで、事故を未然に防ぐことや他の問題解決に繋がることがあります（ヒヤリ・ハットの考え方）。	2.1.①	窓口
B07			検討	情報システムの故意による事件の原因究明や証拠保全を自社で対応できない場合、事故対応をサポートできるベンダを事前に把握していますか？	不正侵入や改ざんなどの故意による犯罪の場合、事件の原因究明や証拠保全が必要とされます。しかし自社で対応できない場合、これらの作業をサポートできる業者（ベンダ）に依頼する必要があり、事前に把握しておくことが求められます。	2.3.②	管理者
B08			検討	情報システムの故意による事件の原因究明や証拠保全を自社で実施する場合、システム担当者にこれらの対応技術を習得させていますか？	情報システムの故意による事件の原因究明や証拠保全には高度な技術が求められます。これを自社で行うには、対応するシステム担当者にこれらの対応技術を習得させることが求められます。	2.3.③	窓口
B09	A07 共通		検討	事故内容とその対応について記録し事故対応者で記録・共有するもの（事故発生報告書 等）を用意し利用していますか？	事故の内容やその対応について逐次記録することで、対応内容を忘れず、事故対応する人の中で情報が共有できます。そのための様式を事前に作成し利用することで、記録漏れなどが防げ、管理も容易になります。	2.1.② 4.1.①	窓口
B10	A08 共通		検討	BCP（事業継続計画）を策定し、どの様な情報システムの事故のとき、これを実施するか定めていますか？	情報システムの中には、事故により事業の継続が出来なくなるようなものも考えられます。これらを事前に検討し、事故が起きた時の計画（BCP）を策定し、運用することが求められます。	2.4.②	管理者
B11	A09 共通		検討	情報システムの中で保守を委託しているシステムの保守委託業者を、その契約内容を含め、把握していますか？	情報システムは、その環境、ハードウェア、ソフトウェア、コンテンツなどから構成され、それぞれ管理を委託しているものがあると思われます。これらをその契約内容と共に事前にまとめておくことで迅速な対応が可能になります。	3.1.①	窓口
B12	A10 共通		必須	自社で管理している情報システムの各設定内容や、インストールの手順書などを事前にまとめ、管理していますか？	自社で管理を行っている情報システムでは障害復旧時には自社で対応する必要があります。そのためには各種の設定内容やシステム構築のための手順などを事前にまとめ管理しておくことが求められます。	3.2.①	窓口
B13	A12 共通		必須	各情報システムで、データのバックアップのルールを決め、定期的に実施していますか？	情報システムの事故により、作成されたデータは利用できなくなることがあります。データを定期的にバックアップするルールを決め、実施することは必須事項です。	3.2.②	窓口
B14	A13 共通		検討	バックアップデータを定期的にリストアするようなテストや確認を定期的に実施していますか？	バックアップを定期的に実施しているつもりでも、実際にデータが正しく取れていないことがあります。定期的にバックアップデータを戻すことで、バックアップが正しく行われていることを確認することが望まれます。	3.2.②	窓口
B15	A14 共通		検討	自社で管理している情報システムで事故の復旧が出来ない場合など、事故復旧をサポートできるベンダを事前に把握していますか？	自社で管理している情報システムでは、自社で事故の復旧が必要とされます。迅速に復旧できない時など、これらの作業をサポートできる業者（ベンダ）を事前に把握しておくことが求められます。	3.3.①	窓口
B16	A15 共通		検討	定期的に発生した事故を組織的に評価・検証することで、今後のセキュリティ対策に役立てていますか？	情報システムの事故は定期的に要因の分析や対応内容などを分析し、事前対策に活かすことで、事故を未然に防げる可能性が高まります。	4.2.①	管理者
B17			必須	情報システム（OSやアプリケーション等）は可能な限り最新の状態を保つように更新していますか？	情報システム（OSやアプリケーション等）は内在する脆弱性を修正した最新版が随時公開されています。可能な限り最新の状態を保つように更新することは必須の対策です。	事前準備	管理者
B18			必須	クライアントPCへの不用意なソフトのインストールや私有PC,USBメモリ等の業務使用を制限する社内ルールを定め、周知していますか？	クライアントPCに業務に無関係なソフトを不用意にインストールしたり、個人所有のPCやUSBメモリ等を業務に使うことでウイルス感染の恐れが増大します。これらを軽減させるための社内ルールを定めることは必須の対策です。	事前準備	管理者
B19			必須	情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにしていますか？	情報システムや共有フォルダをアクセスさせたい人だけに許可を与えるアクセス制御は必須の対策です。	事前準備	管理者
B20			必須	情報システムへのアクセスのためのパスワードは他の人に分からないように管理されていますか？	情報システムにアクセスするためのパスワードを不適切に管理すると、アクセス制御が正常に機能しないことになります。パスワードの安全管理は必須の対策です。	事前準備	従業員

図 9　情報システムへの攻撃対策チェックシート

情報漏えい対策チェックシート							
No	共通	Check	ﾚﾍﾞﾙ	チェック項目	解説	ステップ	担当
C01	A01 共通		必須	事故発生時の窓口組織等の体制を構築し、これを従業員に周知していますか？	事故が発生したときに連絡する窓口などの体制を事前に構築し、これを従業員が理解し実践することが必要になります。	1.1.① 2.2.①	従業員
C02			検討	機密性の面で重要な情報（システム）を把握し、これを従業員に周知していますか？	情報が漏えいすることで業務に支障を及ぼすものを重要な情報（システム）と定め、これを従業員全体で認識することで事故検知が確実に行えるようになります。	1.1.①	従業員
C03	B02 共通		検討	情報システムでアクセスログを取得し、定期的にログをチェックしていますか？	情報システムでは、ユーザの操作等のログを取り、このログを定期的にチェックすることで、不正なアクセスの検知や事故後の原因究明、証拠とすることができます。	1.1.② 2.4.① 2.5.①	実務
C04			必須	重要な情報の持ち出しの制限や、持ち出し時の許可手順・記録・暗号化等を実施する社内ルールを定め、周知していますか？	情報を持ち出すことが漏えい事故の大きな要因に繋がっています。重要な情報の持ち出しの制限や、持ち出す場合の許可手順の策定、持ち出す情報の内容等を記録、必要に応じた暗号化等の実施が必須の対策です。	2.1.③	実務
C05	A04 共通		検討	事故対応の窓口要員に対して技術的な教育を受けさせていますか？	事故対応では、問題の切り分けや復旧など、技術的な知識が必要になるため、これらの知識を事前に身につけることが求められます。	2.2.② 2.3.①	実務
C06	A07 共通		検討	事故内容とその対応について記録し事故対応者で記録・共有するもの（事故発生報告書 等）を用意し利用していますか？	事故の内容やその対応について逐次記録することで、対応内容を忘れず、事故対応する人の中で情報が共有できます。そのための様式を事前に作成し利用することで、記録漏れなどが防げ、管理も容易になります。	2.2.② 4.1.①	実務
C07	B07 共通		検討	情報システムの故意による事件の原因究明や証拠保全を自社で対応できない場合、事故対応をサポートできるベンダを事前に把握していますか？	不正侵入や改ざんなどの故意による犯罪の場合、事件の原因究明や証拠保全が必要とされます。しかし自社で対応できない場合、これらの作業をサポートできる業者（ベンダ）に依頼する必要があり、事前に把握しておくことが求められます。	2.4.① 2.5.②	管理者
C08	B08 共通		検討	情報システムの故意による事件の原因究明や証拠保全を自社で実施する場合、システム担当者にこれらの対応技術を習得させていますか？	情報システムの故意による事件の原因究明や証拠保全には高度な技術が求められます。これを自社で行うには、対応するシステム担当者にこれらの対応技術を習得させることが求められます。	2.5.③	実務
C09			必須	従業員との守秘義務の取り決めや、委託先への機密保持契約の実施を行っていますか？	雇用や退職時の従業員との守秘義務の取り決めや、委託先との機密保持契約締結、安全管理対策の取り決め等の実施は必須の対策です。	4.2.①	管理者
C10			検討	従業員や委託業者が漏えい問題を起こした時の処罰基準や損害賠償請求基準などを事前に定めていますか？	従業員や委託業者が漏えい問題を起こした時、処罰や損害賠償請求を行うときがあります。これを想定し、処罰基準や損害賠償請求基準などを設け、事前に規定や契約を交わすことことが求められます。	4.2.①	管理者
C11	A15 共通		検討	定期的に発生した事故を組織的に評価・検証することで、今後のセキュリティ対策に役立てていますか？	情報システムの事故は定期的に要因の分析や対応内容などを分析し、事前対策に活かすことで、事故を未然に防げる可能性が高まります。	4.3.①	管理者
C12			必須	事務所における情報システムや重要な書類の盗難防止策を実施する社内ルールを定め、周知していますか？	事務所における情報の盗難が情報漏えいに繋がります。情報システムや重要な書類を施錠管理するなどの盗難防止策は必須の対策です。	事前準備	管理者
C13			必須	情報破棄時にこれを読めなくなるような施策（紙・CDのシュレッダー、HDDの完全消去等）を実施する社内ルールを定め、周知していますか？	情報を破棄する時にそのまま捨てると情報漏えいに繋がります。情報が読めなくなるような施策（紙・CDのシュレッダー、HDDの完全消去等）の実施が必須の対策です。	事前準備	従業員
C14			必須	メール利用時の誤送信（宛名間違え、BCC未活用等）防止や添付ファイルの暗号化を実施する社内ルールを定め、周知していますか？	メール利用時の誤送信（宛名間違え、BCCを使わないためのアドレス暴露等）防止や重要な添付ファイルの暗号化の施策は必須の対策です。	事前準備	従業員
C15	A18 共通		必須	重要な情報システムは専用のエリアに入れ、安全に管理されていますか？	盗難や偶発的な破壊、温度上昇などから守るために、重要な情報システムは専用のエリア、部屋などに集約、隔離し、安全に管理することが必要となります。	事前準備	管理者
C16	B03 共通		必須	各コンピュータでウイルス対策ソフトを導入し、常に最新の状態を維持し、動作の確認を行っていますか？	コンピュータにウイルス対策ソフトを導入し、常に最新の状態を維持することで、ウイルス検知・駆除が行えます。またこれらを管理できるソフトであれば検知・駆除の状況が一覧できます。	事前準備	管理者
C17	B17 共通		必須	情報システム（OSやアプリケーション等）は可能な限り最新の状態を保つように更新していますか？	情報システム（OSやアプリケーション等）は内在する脆弱性を修正した最新版が随時公開されています。可能な限り最新の状態を保つように更新することは必須の対策です。	事前準備	管理者
C18	B18 共通		必須	クライアントPCへの不用意なソフトのインストールや私有PC,USBメモリ等の業務使用を制限する社内ルールを定め、周知していますか？	クライアントPCに指定されていないソフトを不用意にインストールしたり、個人所有のPCやUSBメモリ等を業務に使うことでウイルス感染の恐れが増大します。。これらを禁止することは必須の対策です。	事前準備	管理者
C19	B19 共通		必須	情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにしていますか？	情報システムや共有フォルダをアクセスさせたい人だけに許可を与えるアクセス制御は必須の対策です。	事前準備	管理者
C20	B20 共通		必須	情報システムへのアクセスのためのパスワードは他の人に分からないように管理されていますか？	情報システムにアクセスするためのパスワードを不適切に管理すると、アクセス制御が正常に機能しないことになります。パスワードの安全管理は必須の対策です。	事前準備	従業員

図 10　情報漏えい対策チェックシート

4　実際の適用例１（小規模企業）

３章で紹介した事故対応フローや事故対応チェックシートを小規模な企業で利用した場合の一例を示します。手間やコストをあまりかけずに、差し当たり情報セキュリティ事故対応の準備を導入したい場合の利用例となります。

4.1 想定企業１の現状

（１）会社概要

- 会 社 名：横崎食品販売株式会社（仮名）
- 業務概要：食品加工品の卸売販売
  食品メーカーから小売店に商品の卸売。数年前からインターネット通販で個人客への販売を開始、拡張中。
- 資 本 金：１千万円
- 社 員 数：２５名（事務職員２０名）
- 売 上 高：１０億円
- 拠　　点：神奈川県横浜市

（人数には、パートアルバイト、派遣者等も含む。）

（２）各部課の業務概要

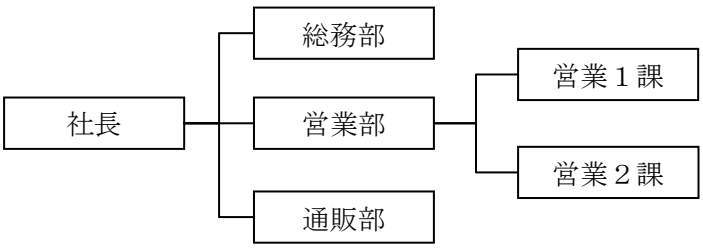


図 11　想定企業１の組織図

- 総務部：人事、経理、情報システム管理 など。
  情報システム管理は、兼任１人体制。セキュリティ管理も兼ねる。
- 営業部：小売店からの受注、食品メーカーへの発注、納期・在庫管理 など。
- 通販部：ネット通販（ネット上にショッピングサイト開設）の受付、発送、顧客対応 等。

（３）情報システムとセキュリティ対策

１）業務システム、サーバ関連

- 営業部、通販部の受発注、納期、在庫、顧客管理は MS-Access のシステムで管理（ファイルサーバに格納）。
- 社内にファイルサーバを置き、ファイル共有している（アクセス制御 一部実施）。
- ショッピングサイトをインターネット上に開設（構築、運用管理含め業者に委託）。

- インターネット上で ASP 形式のグループウェアを利用し、情報を共有している。
- その他、経理ソフトをパッケージで経理担当の PC に導入。
- 社外向け会社ホームページ、メールはレンタルサーバで稼働（ドメイン名の管理を含めて業者に任せている）。
- ホームページの構築は業者に委託して作成、一般的な更新は自社で実施。

2）クライアント PC（事務職員に一人一台：計 20 台）

- OS は WindowsXP、最近購入した数台は Windows 7 。
- 事務処理（ワード、エクセル、アクセス）、メール、WEB 閲覧に使用。
- グループウェアでスケジュール、共通文書などを共有。
- 各自の PC にはそれぞれウイルス対策ソフトが導入され、OS のアップデートも各自が実施している（はずである）。

3）ネットワーク

- 社内 LAN は 100BASE-T の Ethernet で、HUB（L2 スイッチ）で繋がれている。（無線 LAN 無し）
- WAN はルータから光変換機、光回線、ISP 経由でインターネットに接続。

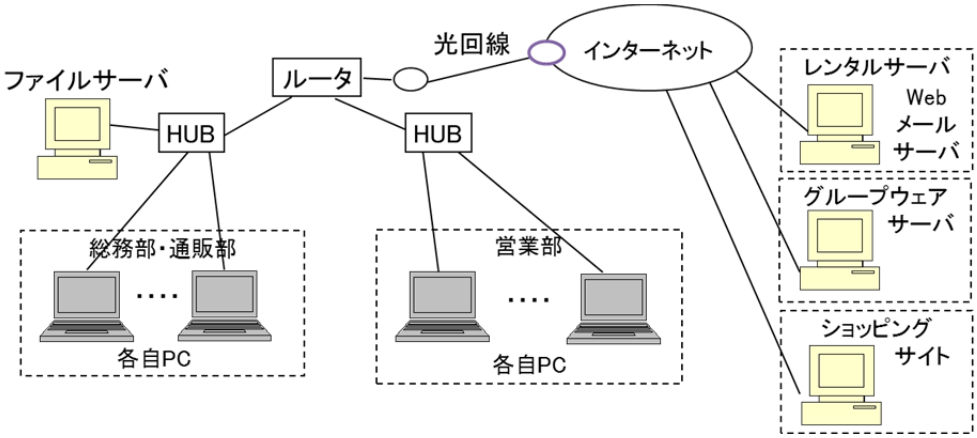


図 12　想定企業 1 のシステム構成図

（4）情報セキュリティ管理

1）情報セキュリティ規定・マニュアル等

特になし。

2）情報セキュリティ体制、教育

- 特に体制無し。総務部の Y 氏が比較的 IT に詳しいので、トラブル時は Y 氏に頼っている。
- 通販部では個人の顧客データを取り扱うため、情報漏えいに関する教育は一度実施した。

4.2 事故対応への取り組み（想定企業１）

（１）はじめに

横崎食品販売株式会社（仮名）は、食料品の卸売をしている会社で、最近ではインターネット通販に力を入れており、売上も伸びている。社内の情報化も進んできているが利便性優先で、情報セキュリティ対策については何から手を付けて良いか分からず、後回しにしている状況である。

先日、社長はインターネット通販を手掛ける同業者が顧客情報の情報漏えい事故を起こし、その事後対応に手間取り、撤退を余儀なくされたと聞いた。自社で同様のことが起こったとき、どんな対応を取れば良いのか、不安であった。

自社でも半年前、インターネット回線の障害が発生し、ネット通販の受付が滞る事故があった。受付対応が遅れて迷惑を掛けてしまい、何人かの顧客がこの事故をきっかけに離れて行ってしまった。故障を絶対に起こさないのは無理であろうが、迅速に対応しないとまた同じようなことが起こるという危機感があった。

（２）事故対応の検討開始

社長は上記２つの問題の対応を、自社の情報システムの対応を実施している総務課Ｙ氏に指示した。Ｙ氏は、「情報セキュリティ事故対応ガイドブック」の資料（本書）がネットに公開されているのを知り、これを元に、「インターネット事故対応」「情報漏えい事故対応」の検討を行なおうと考えた。

まずは、資料から以下のことを理解・検討することとした。

- 一般的な情報セキュリティ事故対応の全体像の理解（1 章、2 章より）
- 自社の実際の情報セキュリティ事故対応の検討（3 章より）

はじめは、上記２つの事故対応だけを考えようとしたが、資料を読み進めていく中で、ショッピングサイトやファイルサーバの障害も組織にとって大きな問題であることが認識された。また、ウイルス感染がシステムの障害、情報漏えいにも結びつくことから、資料に記載されている３つの事故のパターン（情報システムの障害、情報システムへの攻撃、情報漏えい）すべてについての対応を検討することにした。

（３）事故対応チェックシートの実施

まずＹ氏は、事故対応チェックシートを実施してみた。このチェックシートで実施する事故対応のための事前チェックとは、例えば情報システムの障害が発生したとき、いきなり対応フローA を見ても、データのバックアップが取られていないのでは、復旧させることができない。したがって、バックアップの取得が事前に実施されているかをチェックするものである。

チェックシートの「Check」欄に、チェック項目の内容が部分的に実施できている場合は「△」を、全く実施できていない場合は「×」を記載して一通りチェックをした結果、多くの部分で自社の事前準備が不足していることが分かった。これらを実施するには、仕組みや規則を

作り社員に教育したり、機器やソフトウェアを購入したりする必要があるものもあった。（※チェック結果については、図 13、図 14 を参照）

事故発生時に必要となる報告書のフォーマットについては、この資料に掲載されているもの（【付録１】～【付録４】）があったので、これを活用し、使いながら自社に合わせて修正していくことにした。

資金や全社的な取り組みが必要な部分は、社長にこれらの資料の概要を説明し、業務の継続上必須のものは実施する許可を得た。ただ、日常の監視やログの監査などについては今後順次整備していくこととなった。

No	共通	Check	ﾚﾍﾞﾙ	チェック項目	対応内容	ステップ	担当
A 情報システムの障害(利用不能、データ喪失 等)							
A01		×	必須	事故発生時の窓口組織等の体制を構築し、これを従業員に周知していますか？	下記のような体制をとり、朝の朝礼の時、全従業員に通達し、文書を回覧する。 管理者:社長、窓口(システム担当)、実務:総務課Y氏	1.1.①	従業員
A02		×	検討	可用性の面で重要な情報システムを把握し、これを従業員に周知していますか？	ショッピングサイト、Webサーバ、メールサーバ、グループウェア、ファイルサーバ、インターネット、クライアントPC は、いずれも重要な情報システムであり、これらの異常時に窓口に連絡するように通達。	1.1.①	従業員
A03		×	検討	情報システムの定期的な監視や障害検知装置の設置を実施していますか？	システム担当Y氏に一任(ただし、新規投資の資金は無いので、定期的な監視のみ)。	1.1.②	窓口
A04		×	検討	事故対応の窓口要員に対して技術的な教育を受けさせていますか？	どんな教育が必要か不明なため保留。ただし、必要な図書等はY氏に購入を許可。	2.1.① 2.1.②	窓口
A05		×	検討	情報システム事故を受け付けたときにこれを記録(情報システム事故受付表 等)し、定期的にこの記録を評価していますか？	【付録1】「情報システム事故受付表」を採用。	2.1.①	窓口
A06		△	検討	システム・ネットワーク構成図や電源系統図を管理していますか？	ネットワーク構成図:一度作ったままで更新していなかったので、Y氏が更新。 電源系統図:事務所の管理会社に入手依頼。	2.1.②	窓口
A07		×	検討	事故内容とその対応について記録し事故対応者で記録・共有するもの(事故発生報告書 等)を用意し利用していますか？	【付録2】「情報セキュリティ事故発生報告書」、【付録3】「情報セキュリティ事故経過報告書」、【付録4】「情報セキュリティ事故最終報告書」を採用。	2.2.① 4.1.①	窓口
A08		×	検討	BCP(事業継続計画)を策定し、どの様な情報システムの事故のとき、これを実施するか定めていますか？	ショッピングサイトのダウン時は代替運転を検討。 インターネット接続の不可時は代替運転を検討。 (BCPとしてまとめるのは全体的な話もあるため、保留)	2.2.②	管理者
A09		×	検討	情報システムの中で保守を委託しているシステムの保守委託業者を、その契約内容を含め、把握していますか？	それぞれ調査しまとめ、事故対応一覧表に付記。	3.1.①	窓口
A10		×	必須	自社で管理している情報システムの各設定内容や、インストールの手順書などを事前にまとめ、管理していますか？	ファイルサーバは設定リスト用意、他は代替機の用意を検討。	3.2.① 3.2.②	窓口
A11		×	検討	各情報システムの代替機や予備部品などを事前に用意していますか？	ファイルサーバ、クライアントPCは古いものがまだあるので、いつでも置き換えが出来るようにY氏が対応。	3.2.②	窓口
A12		×	必須	各情報システムで、データのバックアップのルールを決め、定期的に実施していますか？	ファイルサーバのデータを毎日2回、別のHDDにバックアップし、週に一回DVD－RAMにバックアップすることをY氏が対応。	3.2.③	窓口
A13		×	検討	バックアップデータを定期的にリストアするようなテストや確認を定期的に実施していますか？	週に1回、バックアップが実行されているかY氏が確認。	3.2.③	窓口
A14		×	検討	自社で管理している情報システムで事故の復旧が出来ない場合など、事故復旧をサポートできるベンダを事前に把握していますか？	それぞれ調査しまとめ、事故対応一覧表に付記。	3.3.①	窓口
A15		×	検討	定期的に発生した事故を組織的に評価・検証することで、今後のセキュリティ対策に役立てていますか？	半年に1回、セキュリティ会議を開き、「情報システム事故受付表」と「情報セキュリティ事故最終報告書」を見ながら、今後必要なセキュリティ対策を検討することにする。	4.2.①	管理者
A16		×	必須	重要な情報システム機器ではハードディスクの二重化が行われていますか？	ショッピングサイトでは必要であるが、次期サイトリプレース等の際に検討することにする。	事前準備	管理者
A17		×	必須	重要な情報システムでは無停電電源装置が導入されていますか？	次項目A18の対応で用意するボックス全体に供給できる無停電電源装置を設置する。	事前準備	管理者
A18		×	必須	重要な情報システムは専用のエリアに入れ、安全に管理されていますか？	サーバ類とルータを1か所に集め、かぎ付きのボックス(空調ファン付き)に格納する。	事前準備	管理者

図 13　事故対応チェックシート実施結果１（想定企業１）

No	共通	Check	レベル	チェック項目	対応内容	ステップ	担当
B 情報システムへの攻撃(ウイルス感染、不正アクセス、改ざん 等)							
B02		×	必須	情報システムでアクセスログを取得し、定期的にログをチェックしていますか？	現状のファイルサーバにはログを記録する機能なし。 次期リプレース時にはログが取得できるものを検討する。	1.1.② 2.2.② 2.3.①	窓口
B03		△	必須	各コンピュータでウイルス対策ソフトを導入し、常に最新の状態を維持し、動作の確認を行っていますか？	現在各PCにはウイルス対策ソフトが導入されているが、ばらばらに導入されているため、管理が出来ていない。各PC(クライアント)のウイルス対策ソフトの状況をサーバで管理ができるウイルス対策ソフトを全社的に導入する(更新時)。 また、ファイルサーバはウイルス対策ソフトが導入できない。	1.1.②	窓口
B04		×	検討	ネットワークの定期的な監視や不正侵入検知装置(IDS等)の設置を実施していますか？	システム担当Y氏に一任(ただし、新規投資の資金は無いので、定期的な監視のみ)。	1.1.②	窓口
B07		×	検討	情報システムの故意による事件の原因究明や証拠保全を自社で対応できない場合、事故対応をサポートできるベンダを事前に把握していますか？	外部からの攻撃などが起こったら、証拠保全などの自社対応はまず無理なので、IPAの相談窓口に連絡する。	2.3.②	管理者
B08		×	検討	情報システムの故意による事件の原因究明や証拠保全を自社で実施する場合、システム担当者にこれらの対応技術を習得させていますか？	上記B07に同じ。	2.3.③	窓口
B17		×	必須	情報システム(OSやアプリケーション等)は可能な限り最新の状態を保つように更新していますか？	現状、クライアントPCは個人管理になっており、これを管理するのは費用等が掛かりそうなので、当面はこのままとし、OSやアプリケーションの更新を教育し、Y氏が定期的に確認することにする。 サーバ類は、Y氏により定期的に更新してもらう。	事前準備	管理者
B18		×	必須	クライアントPCへの不用意なソフトのインストールや私有PC,USBメモリ等の業務使用を制限する社内ルールを定め、周知していますか？	現状、クライアントPCは個人管理になっており、これを制限するのは難しい面がある。危険なソフト(Winny、Share等)や、入手先が不明(あやしい)なソフトの導入の禁止のみ、教育により実施する。	事前準備	管理者
B19		×	必須	情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにしていますか？	現在もある程度は実施しているが、Y氏が再確認する。 また、クライアントPCのログインパスワードの設定は今まで実施していなかったので、実施することに決定。	事前準備	管理者
B20		×	必須	情報システムへのアクセスのためのパスワードは他の人に分からないように管理されていますか？	教育により実施。	事前準備	従業員
C 情報漏えい(可能性も含む)							
C02		×	検討	機密性の面で重要な情報(システム)を把握し、これを従業員に周知していますか？	とりあえず、顧客情報を重要な情報と定義し、教育を実施。	1.1.①	従業員
C04		×	必須	重要な情報の持ち出しの制限や、持ち出し時の許可手順・記録・暗号化等を実施する社内ルールを定め、周知していますか？	持ち出し原則禁止、どうしても必要な場合は管理者の許可を得るようにする。 持ち出し時は暗号化を実施(ノートPC)、携帯電話はパスワード設定実施。	2.1.③	実務
C09		×	必須	従業員との守秘義務の取り決めや、委託先への機密保持契約の実施を行っていますか？	守秘義務、処罰規定は社則に盛り込む。 委託作業時は、IPAの「委託関係における情報セキュリティ対策ガイドライン」を参照する(まだ顧客情報委託は未実施)。	4.2.①	管理者
C10		×	検討	従業員や委託業者が漏えい問題を起こした時の処罰基準や損害賠償請求基準などを事前に定めていますか？	処罰規定は社則に盛り込む。 基準については、個別の要因で変わってきそうなので、定められない。	4.2.①	管理者
C12		×	必須	事務所における情報システムや重要な書類の盗難防止策を実施する社内ルールを定め、周知していますか？	ノートPCはワイヤーロック設置、かぎ付きキャビネットを導入し、紙の顧客情報はここに格納する運用とする。	事前準備	管理者
C13		△	必須	情報破棄時にこれを読めなくなるような施策(紙・CDのシュレッダー、HDDの完全消去等)を実施する社内ルールを定め、周知していますか？	教育により廃棄時の処理を説明、中型のシュレッダー導入(今までもあったが、処理能力が低く不評だったため)。	事前準備	従業員
C14		×	必須	メール利用時の誤送信(宛名間違え、BCC未活用等)防止や添付ファイルの暗号化を実施する社内ルールを定め、周知していますか？	教育によりメールの誤送信、BCCの使い方などを説明。	事前準備	従業員

図 14　事故対応チェックシート実施結果２（想定企業１）

（４）事故対応一覧表の作成

次にＹ氏は、資料に掲載されている３つの汎用パターンについてのフローは自社のシステムを当てはめてもそのまま使えそうなので、そのまま利用しようと考えた。そして、情報システムや状況によってそれぞれ対応が違ってくる部分については、別に一覧表を作成することにした。その結果、下記フローとそれに対応する表が３つずつできあがった。（※図 15～図 20 を参照）

- Ａフロー：情報システムの障害対応
- Ｂフロー：情報システムへの攻撃対応
- Ｃフロー：情報漏えいの対応
- 情報システムの障害対応表
- 情報システムへの攻撃対応表
- 情報漏えいの対応表

障害、攻撃の対応表については、自社の情報システムを横軸にし、フローの各ステップを縦軸にし、フローと対応させる形で一覧表にした。そして、各情報システムの障害、攻撃の対応方法についてシミュレーションし、具体的な対応などを表に書き込んでいった。

情報漏えいの対応表については、縦軸は同じだが、横軸は典型的な漏えい事故の要因にし、これらの事故のシミュレーションを行い、具体的な対応などを表に書き込んでいった。

（５）見直し

事故対応フローが出来て、運用開始してから半年がたった。今のところは事故までには至っていないが、軽微な問題はいろいろ発生していた。これらを見直すことで、不足している事前対策が明らかになってきた。

また、ファイルサーバを高機能なものに変更した。これにより、ログが取れるようになり、バックアップ機能も改善されたので、今後もし事故が発生した時も、迅速な対応が可能になると思われる。

Ｙ氏は、これらの内容を対応表にも反映した。Ｙ氏は今後、これらの対応をＹ氏がいなくても出来るような体制にしていきたいと考えている。

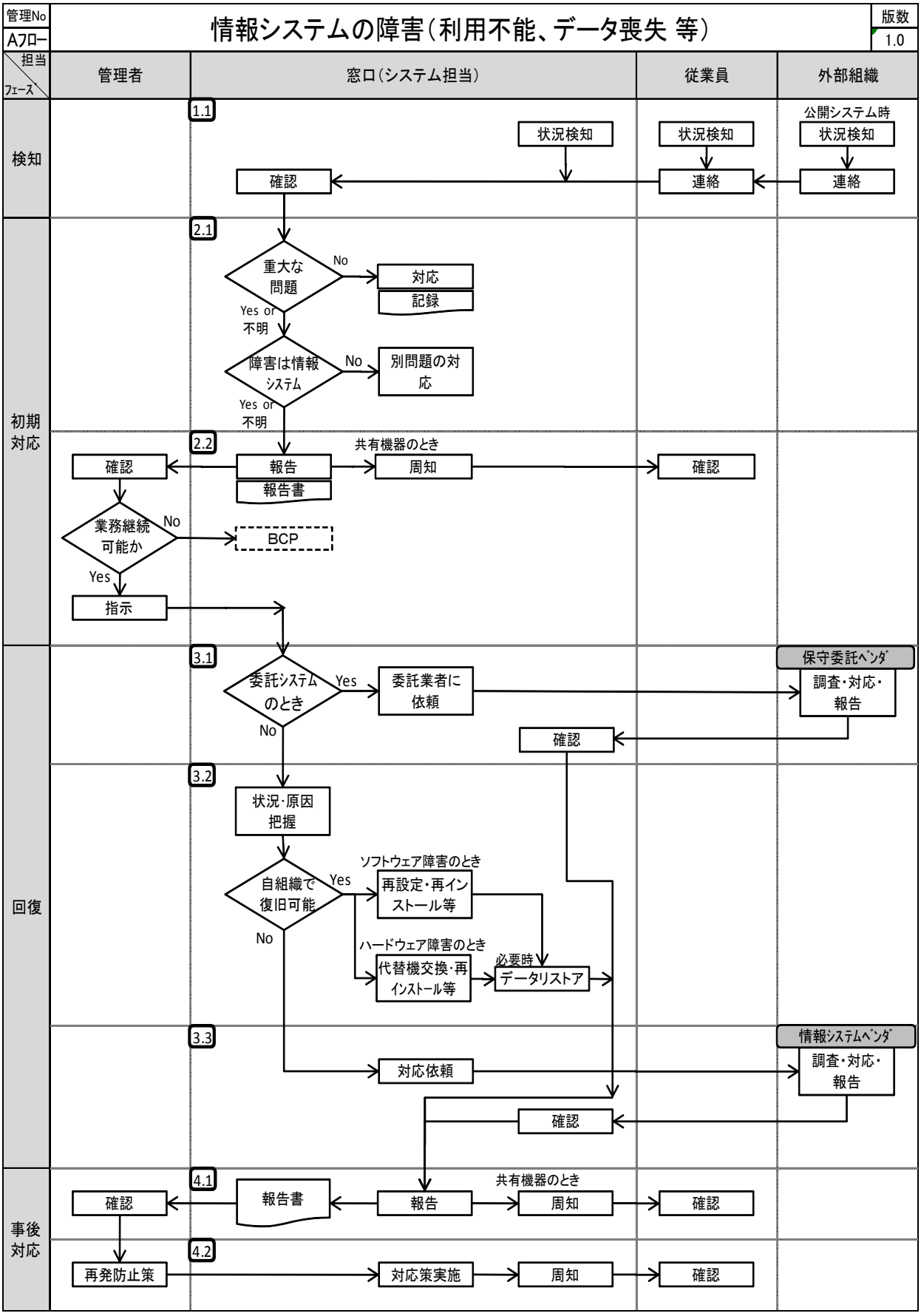


図 15　A フロー：情報システムの障害対応（想定企業 1）

情報システム別 障害対応一覧<想定企業1>　　主に、窓口（システム担当）利用用

ｼｽﾃﾑ	ショッピングサイト	Web,メールサーバ	グループウェア	ファイルサーバ	インターネット		クライアントPC
					ルータ	ISP	
区分	公開ｼｽﾃﾑ(管理委託)	公開ｼｽﾃﾑ(管理委託)	共有ｼｽﾃﾑ(管理委託)	共有ｼｽﾃﾑ(自社管理)	自社管理	管理委託	個人ｼｽﾃﾑ(自社管理)
1.1 検知	従業員はシステムの障害を検知した場合、窓口に連絡する。 公開システムでは顧客から従業員に連絡が入ることがあるので、従業員は窓口に連絡する。						
2.1 問題切り分け	①実際にアクセスして状況を確認する。（軽微な問題で解決できたときは、情報システム事故受付表に状況を記入する。） ②障害がその情報システム自体の問題かどうか切り分ける。（社内LANの問題、電源の問題などが考えられるので、調査、対応する。） 情報システムの障害と判断された場合は、情報セキュリティ事故発生報告書に記入する。（事故受付表にはその旨記入。） 公開システムではDoS攻撃の可能性もあるため、これも調査する。						
2.2 周知 報告 BCP 検討	障害を社長に報告し、従業員に利用できないことを周知する。 公開システムでは、（できるたけ）利用者に利用できないことを公知する。 停止時間に応じてBCP実行（代替運転）を社長と共に検討する。						
3.1 回復 （管理委託）	A社サイト構築ベンダ（XX-XXXX-XXXX） Webサイトに障害報告ページあり。 バックアップはA社実施。	B1社ホスティングサービス（XX-XXXX-XXXX） Webサイトに障害報告ページあり。 B2社Webサイトコンテンツ作成会社（XX-XXXX-XXXX）	C社ASPｻｰﾋﾞｽ（XX-XXXX-XXXX） Webサイトに障害報告ページあり。 バックアップはA社実施。			D社ISP（XX-XXXX-XXXX） Webサイトに障害報告ページあり。	
3.2 回復 （自社対応）				予備のファイルサーバに交換。（ファイルサーバ構築手順書、設定リストを参照） バックアップからデータリストア実施。	ルータ故障の場合、予備機のルータに交換する。（機器マニュアル、設定リストを参照） 障害が解消されない場合は、WiFiルータを仮設して対応。		予備機を貸与。 PCメーカーの対応窓口とやり取りし、ハードウエアの問題のときは修理依頼。 ソフトウェアの問題のときは、設定変更や再インストール。（機器取扱説明書を参照）
3.3 対応 委託				E社ITサポート（XX-XXXX-XXXX）	E社ITサポート（XX-XXXX-XXXX）		E社ITサポート（XX-XXXX-XXXX）
4.1 周知 報告	従業員に復旧したことを周知する。 社長に情報セキュリティ事故最終報告書を提出する。						復旧を本人に通知し、予備品と入れ替え。
4.2 再発 防止	定期的に再発防止を社長と検討し、対策を実施し、関係者に周知する。						

図 16　情報システムの障害対応表（想定企業１）

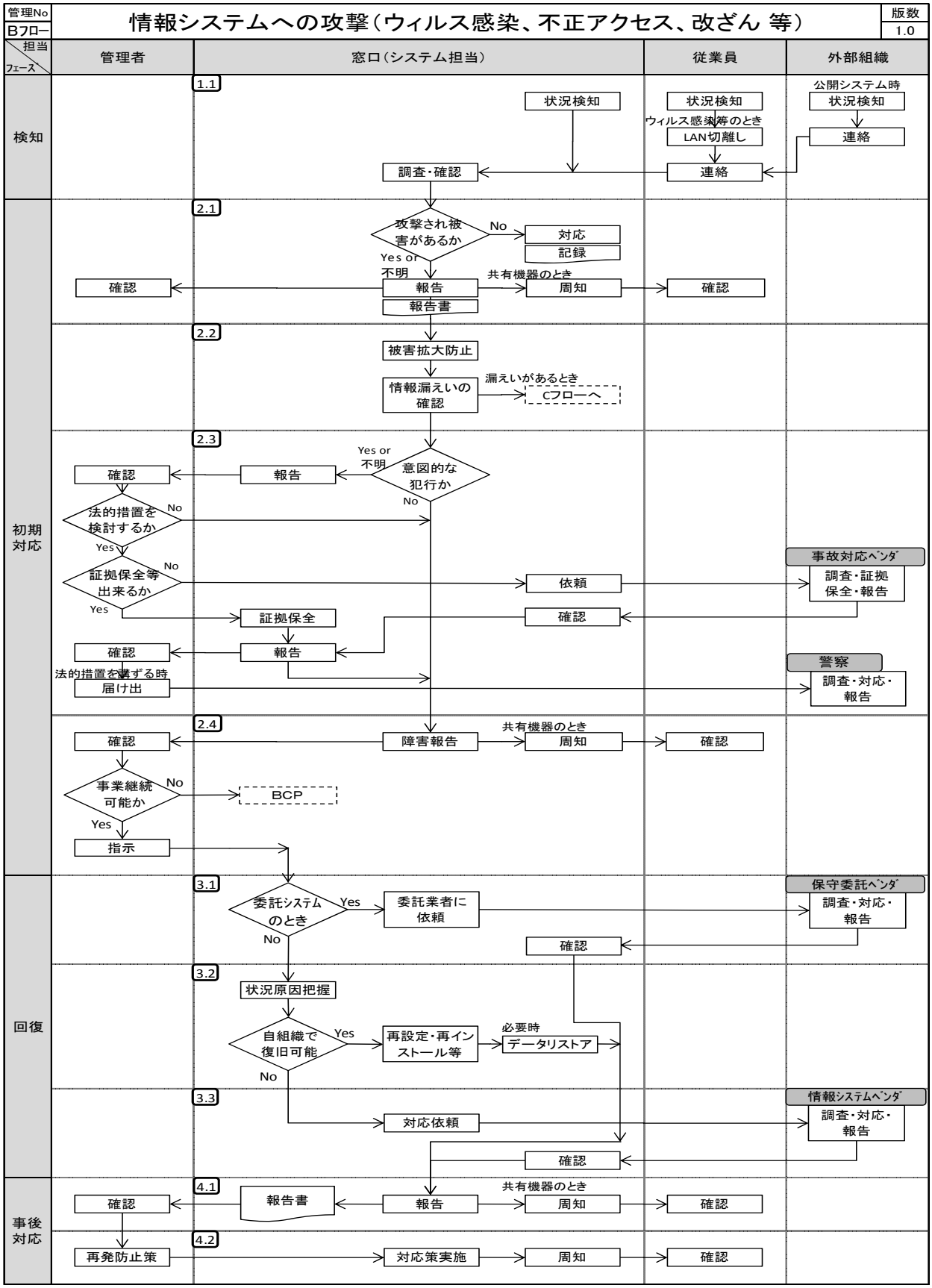


図 17　B フロー：情報システムへの攻撃対応（想定企業１）

攻撃（ウイルス感染、不正アクセス、改ざん）対応一覧<想定企業1>　　主に、窓口（システム担当）利用用

ｼｽﾃﾑ	ショッピングサイト	Web,メールサーバ	グループウェア	ファイルサーバ	クライアントPC
区分	公開ｼｽﾃﾑ(管理委託)	公開ｼｽﾃﾑ(管理委託)	共有ｼｽﾃﾑ(管理委託)	共有ｼｽﾃﾑ(自社管理)	個人ｼｽﾃﾑ(自社管理)
1.1 検知	従業員は攻撃を検知したら窓口に連絡する。				従業員は、ウイルス感染のときは、念のためにLANケーブルを外す。
2.1 問題切り分け報告	攻撃かどうか調査する。 攻撃でなかったときは情報システム事故受付表に状況を記録する。				
	攻撃の場合(または不明時)は、社長に報告し、システム利用者に利用の停止を呼びかける。 また、情報セキュリティ事故発生報告書に記入する。（事故受付表にはその旨記入。）				
2.2 被害拡大防止	(可能であれば)公開システムを利用できなくするような施策を実施する。			ウイルス感染の場合はLANケーブルを外す。	
	不正アクセス、改ざんのときは、ログインID、パスワードを変更する。 法的措置を検討する可能性があるときは証拠保全に努める。				
	情報が漏えいしていないか確認する。情報が漏えいしている場合は、Cフローの対処も合わせて実施する。				
2.3 法的措置	狙われてウイルスを送りつけられたような標的型攻撃の場合や不正アクセス、改ざんのときは、 意図的な犯行であり、被害が出る可能性がある場合、法的措置を検討する。 ※とりあえず、下記IPA窓口で相談。 （自社での証拠保全は現状無理。どうしても必要な場合は事故対応ベンダに対応依頼。） ■情報セキュリティ安心相談窓口：ウイルス対策、不正アクセス等 http://www.ipa.go.jp/security/anshin/ TEL：03-5978-7509				
2.4 周知報告	状況を社長に報告し、従業員に利用できないことを周知する。				
	公開システムでは、（できるだけ）利用者に利用できないことを公知する。				
	停止時間によりBCP実行（代替運転）を社長と共に検討する。				
3.1 回復（管理委託）	A社サイト構築ベンダ（XX-XXXX-XXXX）Webサイトに障害報告ページあり。	B1社ホスティングサービス（XX-XXXX-XXXX）Webサイトに障害報告ページあり。 B2社Webサイトコンテンツ作成会社（XX-XXXX-XXXX）	C社ASPｻｰﾋﾞｽ（XX-XXXX-XXXX）Webサイトに障害報告ページあり。		
3.2 回復（自社対応）				予備のファイルサーバに交換。（ファイルサーバ構築手順書、設定リストをト参照） データリストア。	予備機を貸与。 設定変更や再インストール。（機器取扱説明書を参照）
3.3 対応委託				E社ITサポート（XX-XXXX-XXXX）	
4.1 周知報告	従業員に復旧したことを周知する。 社長に情報セキュリティ事故最終報告書を提出する。				復旧を本人に通知し、予備品と入れ替え。
4.2 再発防止	定期的に再発防止を社長と検討し、対策を実施し、関係者に周知する。				

図 18　情報システムへの攻撃対応表（想定企業１）

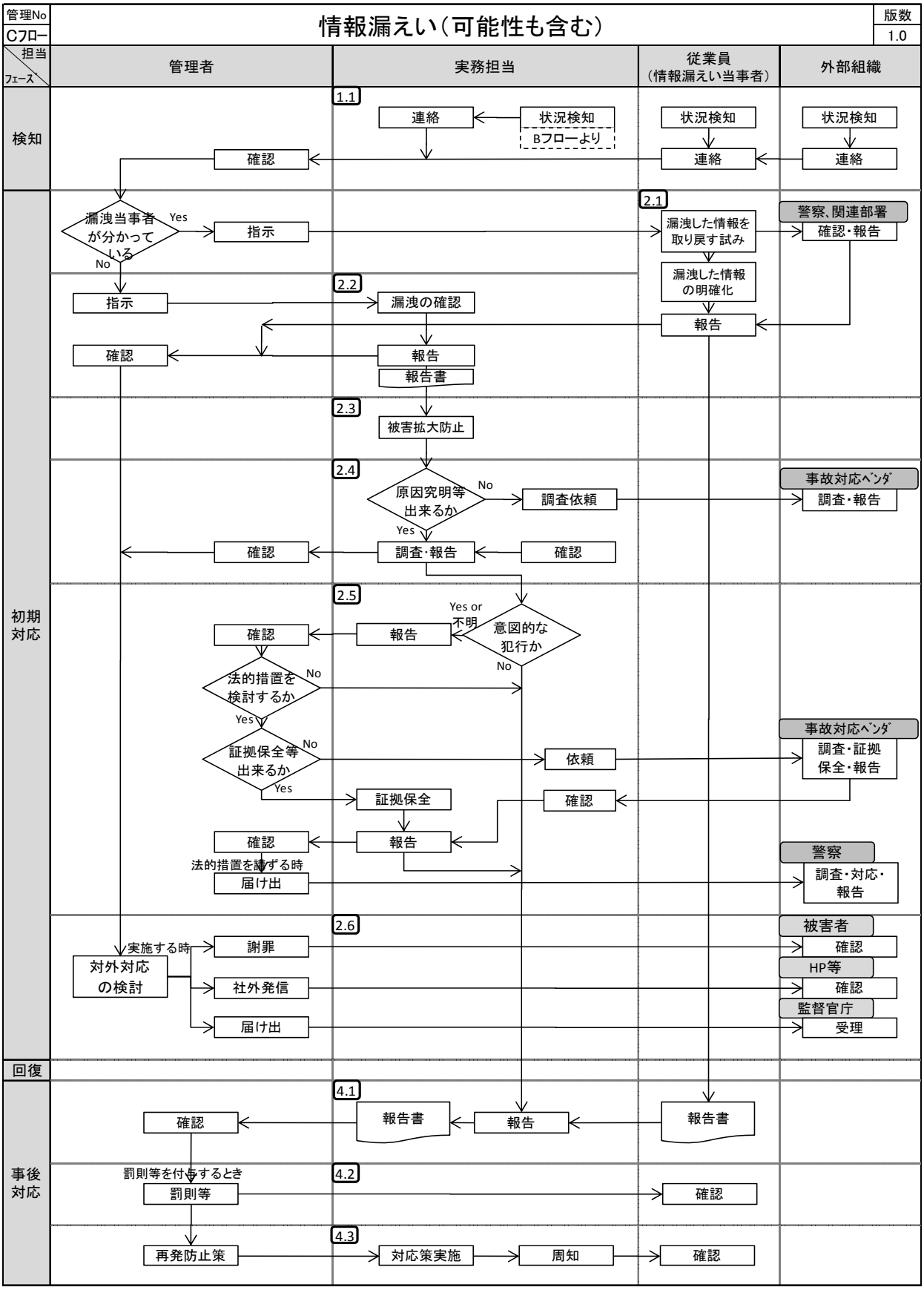


図 19　Ｃフロー：情報漏えいの対応（想定企業１）

情報漏えい状況別 対応リスト<想定企業1>			主に、窓口（システム担当）利用用	
状況	**置き忘れ（不明）、盗難、誤廃棄**	**誤送信、誤公開**	**漏えいの連絡を受けた**	
区分	当事者既知	当事者、漏えい場所既知	当事者、原因不明	
1.1 検知	漏えい当事者は、社長に状況を報告する。		情報漏えいしていることを検知または連絡を受けた従業員は社長に報告する。	
2.1 自己対応	警察等へ連絡する。 漏えいした情報が何か明確にしておく。	誤送信した相手に情報を削除してもらう。 誤公開の設定を修正する。		
2.2 漏えい確認			社長は漏えいの事実を確認する。（または実務担当に確認を指示する。）	
	情報セキュリティ事故発生報告書を記入し、社長に報告する。 IPA情報漏えい対策のしおり 参照			
2.3 被害拡大防止			漏えいの被害拡大を防止する取り組みを行う。	
2.4 原因究明			情報漏えい元、漏えい原因を究明する。状況などから原因を分かる範囲で推測する。（自社での原因究明は状況により難しい場合がある。どうしても必要な場合は事故対応ベンダに対応依頼。）	
2.4 法的措置			意図的な犯行であり、被害が出る可能性がある場合、法的措置を検討する。 （自社での証拠保全は現状無理。どうしても必要な場合は事故対応ベンダに対応依頼。）	
2.5 対外対応	状況により下記対外対応を実施する。 ①被害者への謝罪 ②HP等での社外発信 ③監督官庁（通産省）への届け出			
4.1 周知報告	①社長に情報セキュリティ事故最終報告書を提出する。 ②HP等での社外発信実施時には続報発信。			
4.2 処罰	社長は事象が社則に反するとき、漏えい実施者に罰則を付与する。			
4.3 再発防止	定期的に再発防止を社長と検討し、対策を実施し、周知する。			

図 20　情報漏えいの対応表（想定企業１）

5　実際の適用例２（中規模企業）

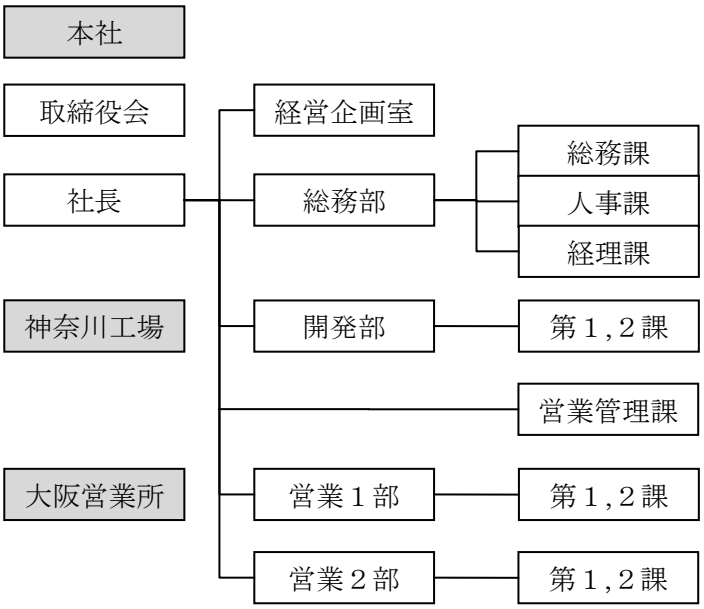
３章で紹介した事故対応フロー、事故対応チェックシートを中規模な企業で利用した場合の一例を示します。ある程度情報セキュリティ対策が実施されており、しっかりとした情報セキュリティ事故対応を検討したい場合の利用例となります。

5.1 想定企業２の現状

（１）会社概要

- 会 社 名：岩浜食品工業株式会社（仮名）
- 業務概要：加工食品の製造、販売。
  主に、大手食品メーカー数社から製造委託を受け、納入。自社企画製品の食品メーカーへの売上げが伸びてきている。自社ブランド品の一般消費者向け食品販売も開始、拡張中。
- 資 本 金：１億円
- 社 員 数：２００名（事務職：１００人、製造職：１００人）
- 売 上 高：５０億円
- 拠　　点：本社　神奈川県横浜市（事務職：７０人）
  神奈川工場(事務職：１０人、製造職：１００人）
  大阪営業所（事務職：２０人）
  （人数には、パートアルバイト、派遣者等も含む。）

（２）本社各部課の業務概要



（各課５人前後）

図 21　想定企業２の組織図

- 経営企画室：商品の総合的なマーケティングや企画、業績管理、業務計画などの立案など。
- 総務課：各種社員の届出や各種契約書、規定類の管理、施設、情報システム管理 など。
  情報システム管理は、専任１人、兼任２人体制。セキュリティ管理も兼ねる。
- 人事課：社内人事、人の採用、教育・研修の施策・管理 など。
- 経理課：売掛、買掛管理、入出金管理、小口現金管理、決算処理 など。
- 開発部：製品の開発、品質管理（自社内、顧客製品クレーム対応） など。
- 営業管理：営業の伝票類の管理、基幹システムへ登録 など。
- 営業部：既存、新規顧客からの受注、納期管理 など。

（神奈川工場：本社からの製造指示により原料購買・入庫・製造・出荷業務。 各営業所：営業部、営業管理課業務と同様。）

（３）情報システムとセキュリティ対策

１）業務システム、サーバ関連

- 基幹システム：販売の受発注、売掛け・買掛けを管理するクライアント・サーバシステムは、開発・導入ベンダと保守契約を結び、システムのアップデートやトラブル対応などを委託している。
- クライアント PC 管理：ActiveDirectory でドメイン管理、ファイルサーバも兼ね、アクセス制御、ログ取得実施。
- OS のアップデート管理サーバで、アップデートパターンの管理実施。
- ウイルス対策ソフト管理サーバでパターンファイルの管理実施。
- 上記サーバは情報システムベンダに導入を依頼し、自社で管理。（トラブル等必要時には対応を依頼することもある。）
- グループウェアサーバ（アクセス制御、ログ取得実施）を、パッケージソフトにより自社で導入。
- その他、経理システム、人事・給与システムの PC システム（スタンドアロン）をパッケージソフトにより自社で導入。
- 上記サーバは、LTO（磁気テープ装置）等で毎日バックアップ実施。
- 社外向け会社 Web、社外メールはレンタルサーバで稼働。（ドメイン名の管理も含めて業者に任せている。）

2）クライアント PC（事務職員に一人一台）

- OS は Windows2000 または XP。（Windows2000 は Windows 7 の PC に移行中）
- 事務処理（ワード、エクセル）、メール、HP 閲覧に使用。
- グループウェアでスケジュール、共通文書などを共有。
- ドメイン管理されており、PC は一般ユーザ権限で利用。
- 各自の PC にはウイルス対策ソフトが導入され、OS のアップデートも適宜実施されている。
- 社内 LAN は 100BASE-T の Ethernet で、HUB（L2 スイッチ）で繋がれている。（無線 LAN 無し）
- WAN はルータから光変換機、光回線、ISP 経由でインターネットに接続。
- 本社と各拠点とは、ルータの VPN で接続（ルータ、VPN はネットワークベンダに保守委託。）

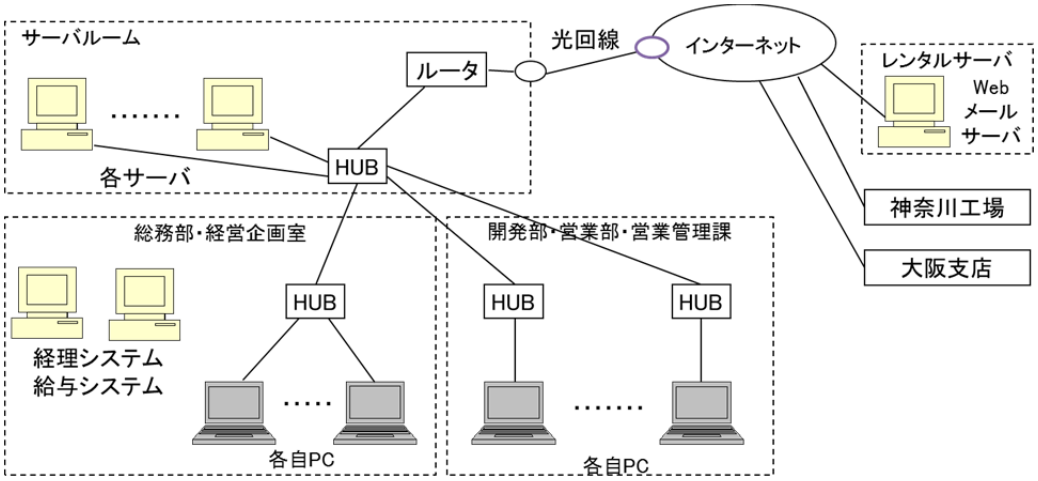


図 22　想定企業２のシステム構成図

（４）情報セキュリティ管理

1）情報セキュリティ規定・マニュアル等

- 基本方針、情報セキュリティ管理基準を定め、主要な情報システムに関する管理規定は定めている。
- 自社管理の情報システムについては、インストール手順、バックアップ・リストア手順をまとめている。別途、BCP 策定済み。

2）情報セキュリティ体制、教育

総務課システム担当 Z 氏がセキュリティ事故等トラブルの窓口。総務部長がセキュリティ管理者。ただし、重要な決定事項は経営陣を交えた「情報セキュリティ委員会」を開催し、検討される。管理職、一般職員向けに年１回（かつ必要時に）情報セキュリティ教育を実施。

5.2 事故対応への取り組み（想定企業２）

（１）はじめに

岩浜食品工業株式会社（仮名）は、加工食品を製造、販売している会社で、主として大手食品メーカーから製造委託を受け生産している。最近ではオリジナル食品の開発、製造、販売が軌道に乗り、一般顧客に直販も行っている。

情報セキュリティ対策は取引先からの意向もあり、一般的に実施すべき対策は既に実施している。しかし、情報セキュリティ事故の対応については、あまり考えられておらず、今後の課題になっていた。

先日、ファイルサーバの故障事故が発生し、たまたま情報システム全般を管理しているＺ氏が不在だったため、どうにもならず、１日業務が出来なかったということがあった。

この事故を教訓に、情報セキュリティ事故対応の検討が急務となった。

（２）事故対応の検討開始

社長はこのような問題の対応を、総務課Ｚ氏に「Ｚ氏がいなくても、事故の対応が総務課内で対応できるように」と指示した。

Ｚ氏は、「情報セキュリティ事故対応ガイドブック」の資料（本書）がネットに公開されているのを知り、これを元に、自社の事故対応の検討を行なおうと考えた。

（３）事故対応チェックシートの実施

Ｚ氏はまず、事故対応チェックシートを実施してみた。チェックシートの「Check」欄にチェック項目の内容が実施できている場合は「○」、部分的に実施できている場合は「△」、実施できていない場合は「×」を記入して一通りチェックをした結果、数か所、不足気味の点があることが分かったが、ほぼ事前の対応は取れていた。不足箇所は、総務部長に報告し、順次対応していくこととなった。（※チェックシートの実施結果は、図 23、図 24 を参照）

No	共通	Check	ﾚﾍﾞﾙ	チェック項目	対応内容	ステップ	担当
A 情報システムの障害(利用不能、データ喪失 等)							
A01		○	必須	事故発生時の窓口組織等の体制を構築し、これを従業員に周知していますか？	検討済み。(漏えい時の実務担当のみ今回決定。) 管理者:総務部長、情報セキュリティ委員会 窓口(システム担当):総務部システム担当、ただし漏えい時の実務担当は総務部システム担当と総務課長の双方が担当する。	1.1.①	従業員
A02		○	検討	可用性の面で重要な情報システムを把握し、これを従業員に周知していますか？	リスク分析実施済、周知済。	1.1.①	従業員
A03		○	検討	情報システムの定期的な監視や障害検知装置の設置を実施していますか？	定期的な監視をツールで実施。	1.1.②	窓口
A04		△	検討	事故対応の窓口要員に対して技術的な教育を受けさせていますか？	一部の要員には未実施。 OJTで今後実施予定。	2.1.① 2.1.②	窓口
A05		△	検討	情報システム事故を受け付けたときにこれを記録(情報システム事故受付表 等)し、定期的にこの記録を評価していますか？	実施中。 定期的な評価はあまりしていないので、今後検討する。	2.1.①	窓口
A06		○	検討	システム・ネットワーク構成図や電源系統図を管理していますか？	管理している。	2.1.②	窓口
A07		○	検討	事故内容とその対応について記録し事故対応者で記録・共有するもの(事故発生報告書 等)を用意し利用していますか？	事故発生報告書および事故最終報告書を用意している。	2.2.① 4.1.①	窓口
A08		×	検討	BCP(事業継続計画)を策定し、どの様な情報システムの事故のとき、これを実施するか定めていますか？	BCPはあるが、地震を想定したもので、セキュリティ事故は想定していない。今後、販売管理システムについて構築する。	2.2.②	管理者
A09		○	検討	情報システムの中で保守を委託しているシステムの保守委託業者を、その契約内容を含め、把握していますか？	把握している。(ただし、分散しているので、対応フローに記入する予定。)	3.1.①	窓口
A10		○	必須	自社で管理している情報システムの各設定内容や、インストールの手順書などを事前にまとめ、管理していますか？	自社で管理している情報システムの設定リスト、インストール手順書あり。	3.2.① 3.2.②	窓口
A11		○	検討	各情報システムの代替機や予備部品などを事前に用意していますか？	自社管理品は代替機用意。予備品は二重化しているHDD用意。インターネットの代替として、ルータ1台、ADSL回線を予備回線として用意。	3.2.②	窓口
A12		○	必須	各情報システムで、データのバックアップのルールを決め、定期的に実施していますか？	定期的に実施中。(頻度はシステムによって異なる。)	3.2.③	窓口
A13		×	検討	バックアップデータを定期的にリストアするようなテストや確認を定期的に実施していますか？	何度かリストアテストをしたのみ。 定期的に実施するように計画する。	3.2.③	窓口
A14		○	検討	自社で管理している情報システムで事故の復旧が出来ない場合など、事故復旧をサポートできるベンダを事前に把握していますか？	付き合いのある情報システムサポートベンダあり。 (費用はかかるが、適切な対応を期待できる。)	3.3.①	窓口
A15		○	検討	定期的に発生した事故を組織的に評価・検証することで、今後のセキュリティ対策に役立てていますか？	毎年の情報セキュリティ委員会の議題としてあげている。	4.2.①	管理者
A16		○	必須	重要な情報システム機器ではハードディスクの二重化が行われていますか？	実施済み。(基幹システム、ファイルサーバ) ディレクトリサーバはサーバ自体を二重化している。	事前準備	管理者
A17		○	必須	重要な情報システムでは無停電電源装置が導入されていますか？	専用ラックにUPS設置済。	事前準備	管理者
A18		○	必須	重要な情報システムは専用のエリアに入れ、安全に管理されていますか？	専用ラックを用意し、空調管理、施錠を実施。 専用ラックは執務室の奥の目立たないところに設置済。	事前準備	管理者

図 23　事故対応チェックシート実施結果１（想定企業２）

No	共通	Check	ﾚﾍﾞﾙ	チェック項目	対応内容	ステップ	担当
B 情報システムへの攻撃(ウィルス感染、不正アクセス、改ざん 等)							
B02		△	必須	情報システムでアクセスログを取得し、定期的にログをチェックしていますか？	基幹システム、ファイルサーバ、ディレクトリサーバでアクセスログ取得。ただし、現状チェックが手動のため、問題があったときのみ見ている。将来的にはログ解析の自動化を検討。	1.1.② 2.2.② 2.3.①	窓口
B03		○	必須	各コンピュータでウィルス対策ソフトを導入し、常に最新の状態を維持し、動作の確認を行っていますか？	すべてのクライアント、サーバにウィルス対策ソフトを導入し、ウィルス対策ソフトの管理サーバ稼働中。	1.1.②	窓口
B04		△	検討	ネットワークの定期的な監視や不正侵入検知装置(IDS等)の設置を実施していますか？	ネットワークの定期的監視をツールで実施中。 IDSは費用の関係から導入未定。	1.1.②	窓口
B07		×	検討	情報システムの故意による事件の原因究明や証拠保全が自社で対応できない場合、事故対応をサポートできるベンダを事前に把握していますか？	事前にベンダのリストアップまでは未実施。 今後、付き合いのあるベンダからも情報収集予定。	2.3.②	管理者
B08		×	検討	情報システムの故意による事件の原因究明や証拠保全を自社で実施する場合、システム担当者にこれらの対応技術を習得させていますか？	フォレンジック技術までは未習得。 ログの解析や状況の保全等基本的なところは習得予定。	2.3.③	窓口
B17		○	必須	情報システム(OSやアプリケーション等)は可能な限り最新の状態を保つように更新していますか？	Microsoft製品の自動アップデートはサーバで管理。 その他の基本アプリも自動アップデート処理実施中。	事前準備	管理者
B18		△	必須	クライアントPCへの不用意なソフトのインストールや私有PC,USBメモリ等の業務使用を制限する社内ルールを定め、周知していますか？	規定と教育で制限実施。 自動的に制限がかかるようなソフト等は導入していない。(運用面、金額面から)	事前準備	管理者
B19		○	必須	情報システム、共有フォルダにはアクセス制御を施し、必要な人以外は取り扱えないようにしていますか？	アクセス制御はサーバ、クライアント共に実施。	事前準備	管理者
B20		△	必須	情報システムへのアクセスのためのパスワードは他の人に分からないように管理されていますか？	サーバのパスワード管理はかなり厳密に実施中。 クライアントは今のところ管理は緩くしている。(運用面から)	事前準備	従業員
C 情報漏えい(可能性も含む)							
C02		○	検討	機密性の面で重要な情報(システム)を把握し、これを従業員に周知していますか？	リスク分析実施済、周知済。	1.1.①	従業員
C04		△	必須	重要な情報の持ち出しの制限や、持ち出し時の許可手順・記録・暗号化等を実施する社内ルールを定め、周知していますか？	持ち出しに関する一連の規定を策定済み。規定では持ち出すPCや媒体に保管されている情報をリストアップさせている。(ただし、正確に運用されているかは未確認。)	2.1.③	実務
C09		○	必須	従業員との守秘義務の取り決めや、委託先への機密保持契約の実施を行っていますか？	入社時、退職時の守秘義務契約実施。 委託先とは委託契約の中で秘密保持契約の取り決め実施。	4.2.①	管理者
C10		○	検討	従業員や委託業者が漏えい問題を起こした時の処罰基準や損害賠償請求基準などを事前に定めていますか？	罰則規定、委託契約時の損害賠償規約は入れている。 (ただし、これらを発動する基準は一概に決められないと考えているので、あまり明確にはしていない。)	4.2.①	管理者
C12		○	必須	事務所における情報システムや重要な書類の盗難防止策を実施する社内ルールを定め、周知していますか？	キャビネット施錠、ノートPCのワイヤ施錠、退社時のノートPCのキャビネットへの格納、施錠は実施済み。	事前準備	管理者
C13		○	必須	情報破棄時にこれを読めなくなるような施策(紙・CDのシュレッダー、HDDの完全消去等)を実施する社内ルールを定め、周知していますか？	各部署に中型シュレッダー設置。大量廃棄時は専門業者への引き渡しを実施。PC、サーバ廃棄時は、システム担当が完全消去を実施した後に廃棄処理を実施。	事前準備	従業員
C14		△	必須	メール利用時の誤送信(宛名間違え、BCC未活用等)防止や添付ファイルの暗号化を実施する社内ルールを定め、周知していますか？	教育で誤送信の注意は呼び掛けている。 添付ファイルの暗号化も規定として実施。(ただし、正確に運用されているかは未確認。)	事前準備	従業員

図 24　事故対応チェックシート実施結果２（想定企業２）

（４）事故対応フローの作成

Z 氏は、資料に掲載されている３つの汎用パターンについてのフローは自社においてもそのまま利用できると思ったが、自分以外のシステム担当者がこれらのフローのみで、事故対応をきちんと取れるか不安があったため、自社の情報システムや状況に合わせて詳細化を図ることにした。

情報システムの障害と情報システムへの攻撃の事故対応については、まず、自社の主だった情報システムで起こりうる事故をある程度列挙し、事故対応の内容について考えていったところ、事故対応の内容が同じになるものがあることがわかった。そのため、それらをグループ化し、このグループ毎に汎用パターンのフローを修正した。情報漏えいの事故対応については、考えられる漏えい事故の要因をグループ化し、このグループ毎に汎用パターンのフローを修正した。その結果、下記１５個のパターンのフローができあがった。

汎用パターンの修正方法であるが、まず、汎用パターンをもとに、下記１５個のパターンそれぞれについて事故をシミュレーションしてみた。これにより汎用パターンの不要な手順を削除し、必要な手順を加えた。同時にフローだけでは具体的な対応に不安があったので、フローの右に対応内容を文書で記述（主に汎用パターンの解説文からコピー）し、ポイントなどを付加していった。これにより、ページ見開きで左にフロー、右に対応内容（解説）となり、事故発生時の緊急時でも見やすくなった。（※作成したフローと対応手順は、図 25～図 54 を参照。ただし、汎用パターンとの差異を分かりやすくするために、汎用パターンでの付番（ステップの番号等）をそのままにしてあり、連番になっていない箇所がある。）

（情報システムの障害対応フロー）

- A1：管理委託している情報システムの障害
- A2：自社管理している情報システムの障害
- A3：社内 LAN の障害
- A4：WAN の障害
- A5：外部公開サーバの障害
- A6：設備の障害（災害時の設備崩壊等は除く）

（情報システムへの攻撃対応フロー）

- B1：ウイルス感染
- B2：不正アクセス、改ざん
- B3：情報システムの盗難、破壊

（情報漏えい対応フロー）

- C1：社外での置き忘れ、盗難、誤廃棄
- C2：メールや FAX の誤送信、Web での誤公開
- C3：業務委託先による情報漏えい
- C4：P2P ソフトのウイルスによる情報漏えい
- C5：掲示板等への書き込みによる情報漏えい
- C6：その他の情報漏えい（原因不明、C1-C5 以外の原因）

作成したフローを元に、総務課システム担当３名で事故のシミュレーションを行いながら、社員に対して事故対応について解説、教育を行った。その中で、不足している対策、手順書、説明不足な点などが明確になり、これらを補完し運用を始めた。

（５）見直し

事故対応フローの運用を開始してから半年がたった。今のところは事故までには至っていないが、軽微な問題はいろいろと発生していた。これらの問題点からフローや手順を見直したことで、事故の前兆と言うべき事象が明らかになり、事故が発生する前に対応することが出来たと思われる事例もあった。

また、人事異動で総務課システム担当が１人異動し、代わりの人間が来たが、この事故対応資料のおかげで、引き継ぎも容易にできた。いずれ Z 氏が異動しても、後任者が問題なく対処できるようになると思われる。

（６）発展

岩浜食品工業では、今回、事故対応のフロー、手順を順次検討することで、今まで抜けていた情報セキュリティ対策を補うことができた。今までの情報セキュリティ対策の網羅性をより向上させることができ、近い将来には ISMS 認証取得も可能な状況になってきた。

作成済みの BCP は、親会社から作成を指示されたもので、地震発生を想定し、製造部門を対象として考えられているものであった。今回、基幹システム障害時の BCP については検討してみたが、今後、対象を他の情報システムにも広げ、より詳細な検討をしていく予定である。

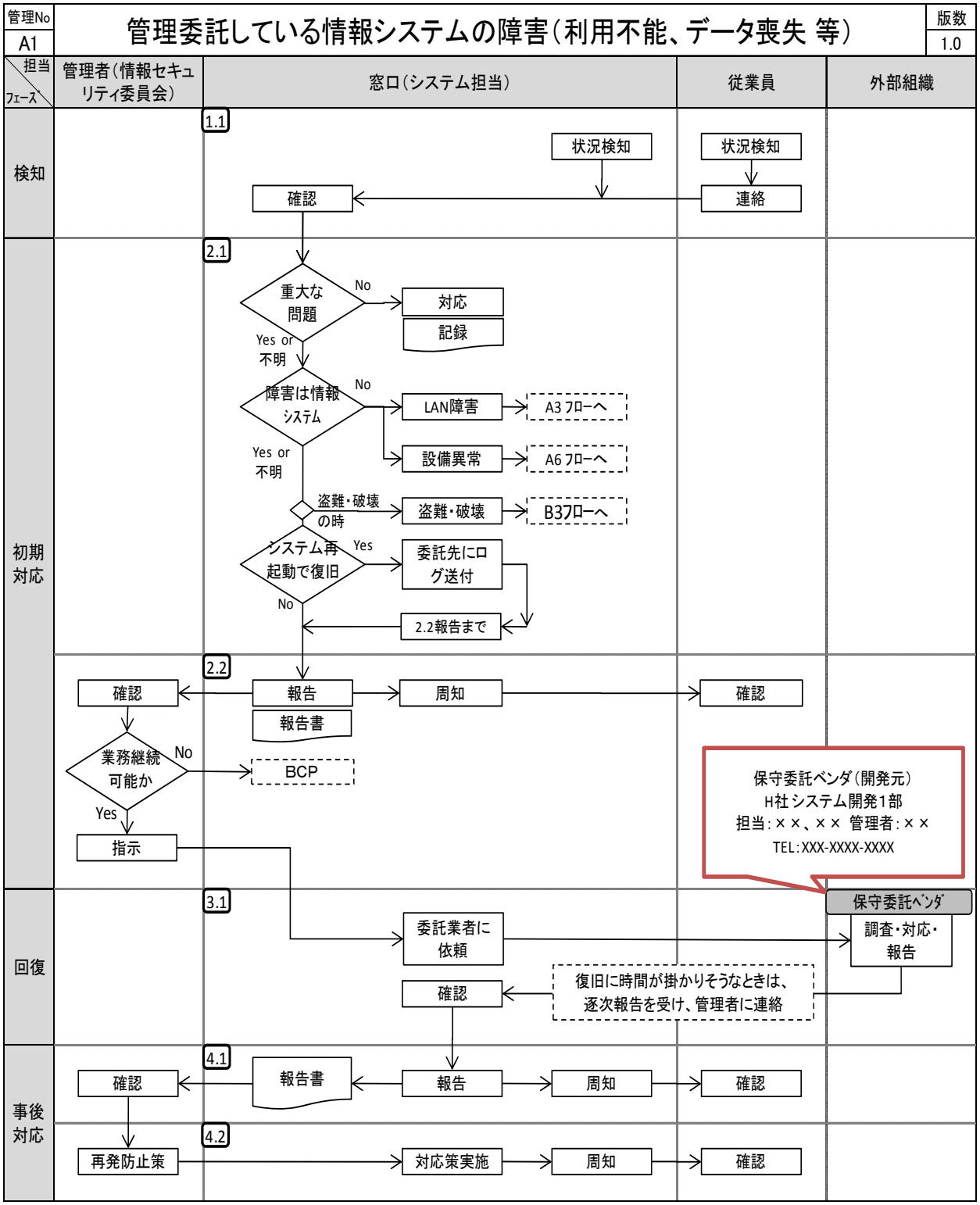


図 25　A1 フロー：管理委託している情報システムの障害対応

A1解説

【対象情報システム】　基幹システム（販売管理システム）

【概要】管理を委託している情報システムが利用できなくなったときは、その事象が情報システムの問題であるかどうかを切り分け、迅速に委託先への状況報告と対応の依頼を行う。

【事例】

1 販売管理システムが、サーバ機器故障のため利用できなくなった。
2 販売管理システムがアプリケーションソフトの不具合で利用できなくなった。
3 販売管理システムで昨日登録したデータを誤って削除してしまった。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：情報システムに障害を感じたら、窓口に連絡する。
②窓口(システム担当)：情報システムの障害を監視し、検知を行う。
障害の監視：開発ベンダから提供されている障害監視ツールを起動し、異常時にメールで通知させるように設定。
④窓口(システム担当)：障害の連絡を確認する。

2. 初期対応

2.1. 問題の切り分け

①窓口(システム担当)：重大な問題か調査する。
障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。
実際にアクセスして確認、問題があるときはサーバ本体のモニタでシステムの状態を確認し、軽微な問題かどうかを切り分ける。
注）昼休みのバッチ稼働時の障害連絡は、単に動作が遅くなったことが考えられる。

②窓口(システム担当)：情報システムの問題か調査する。
LAN障害調査：各エリアのクライアントからサーバにアクセスするなどを実施。（LAN障害時はA3フロー参照）
設備異常調査：サーバ本体の電源LED確認、UPSの状況確認、ブレーカー確認。（設備障害時はA6フロー参照）
盗難・破壊確認：サーバ本体の外観確認、サーバラックの施錠状態なども確認。（盗難・破壊時はB3フロー参照）

③窓口(システム担当)：情報システムの問題だと考えられるとき、システム再起動を実施。
システム再起動を実施。(販売管理システム 運用マニュアル1-10参照)
これで復旧した場合は、マニュアルにあるシステムログをコピーし、保守委託ベンダ担当者にメールで連絡、送付。
かつ、2.2報告のステップを実施。（再起動でシステムが復旧したことを連絡、報告書に記入・提出）

2.2. 報告

①窓口(システム担当)：管理者へ報告する。
「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。
②管理者：業務継続に関わる場合、BCPの実施を検討する。
情報システムの障害状況（深刻度）が定かでないときは、保守委託ベンダから状況、復旧の目処を確認する。
復旧に時間が掛かりそうな場合は、情報セキュリティ委員会を緊急招集し、BCP発動の検討を行う。
③窓口(システム担当)：利用者に利用できないことを通知する。

3. 回復

3.1. 状況・原因把握と復旧（保守委託品）

①窓口(システム担当)：保守委託ベンダに状況を連絡する。
保守委託ベンダに連絡し、対応の依頼を行う。
時間があれば今までの委託ベンダとのやり取りの記録を参照する。（システム連絡簿ファイル参照）
復旧に時間が掛かる場合は、BCP発動を実施するため、管理者に状況を逐次連絡する。

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口(システム担当)：利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口(システム担当)：再発防止策を実施し、周知する。

図 26　A1 手順：管理委託している情報システムの障害対応

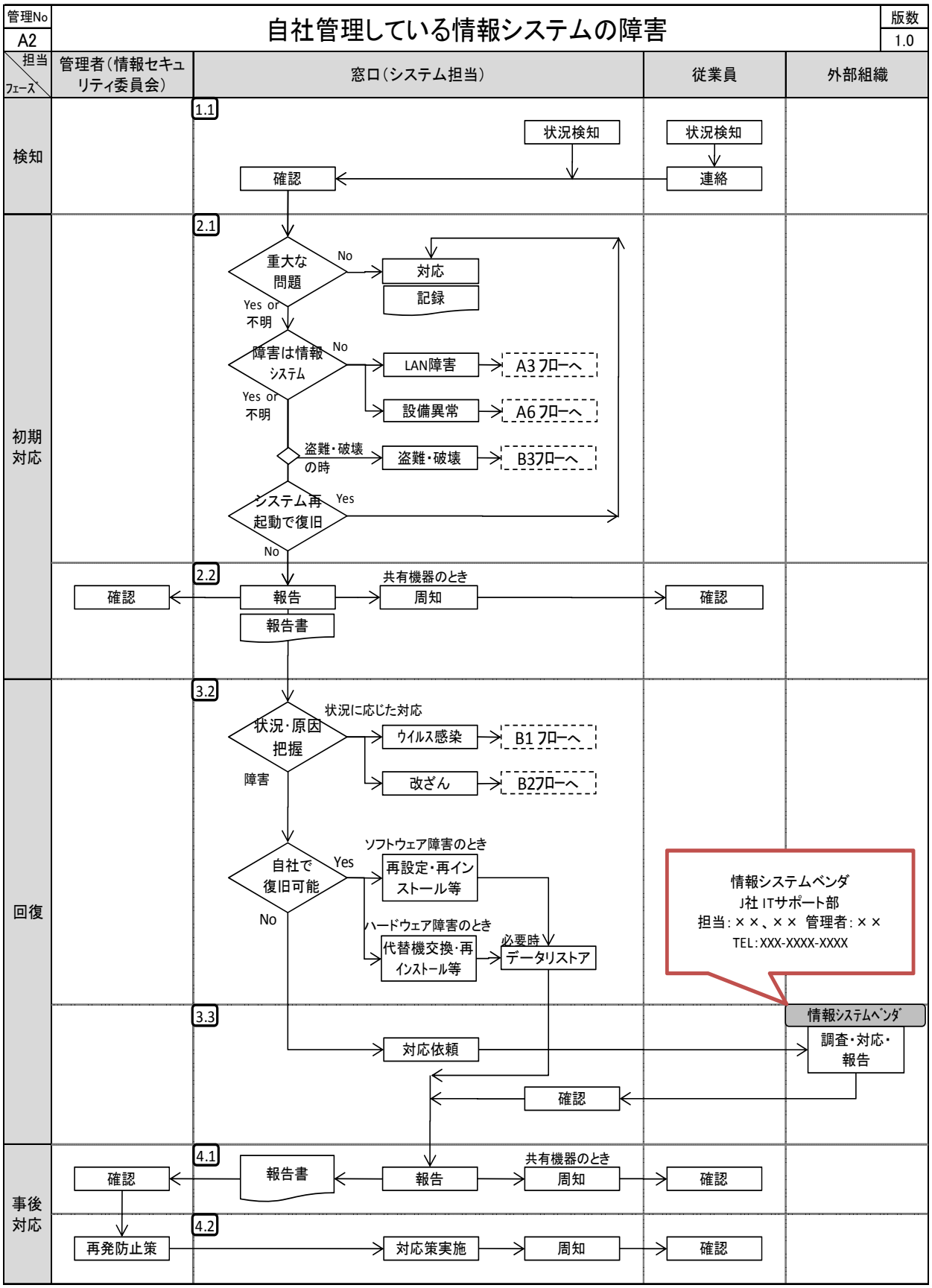


図 27　A2 フロー：自社管理している情報システムの障害対応

A2解説

【対象情報システム】　ファイルサーバ（兼 ドメイン管理サーバ）、OS管理サーバ（兼 ウイルス対策管理サーバ）、グループウェア

【概要】自社管理している情報システムが利用できなくなったときは、その事象が情報システムの問題であるかどうかを切り分け、さらに要因を分析し、これに合った迅速なシステムの復旧を実施する。

注）経理システム、人事・給与システム、各クライアントPCは重要情報システムとしては位置づけられていない。
これらのシステムでは、下記、2.2、4.1、4.2のステップを除いて対応する。

【事例】

1 ファイルサーバが、サーバ機器故障のため利用できなくなった。
2 ファイルサーバのアクセス制御を間違って設定したため、アクセスができなくなった。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：情報システムに障害を感じたら、窓口に連絡する。
②窓口(システム担当)：情報システムの障害を監視（始業時、終業時の状況監視）し、検知を行う。
④窓口(システム担当)：障害の連絡を確認する。

2. 初期対応

2.1. 問題の切り分け

①窓口(システム担当)：重大な問題か調査する。
障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。
実際に操作して確認。問題があるときは本体のモニタでシステムの状態を確認し、軽微な問題かどうかを切り分ける。

②窓口(システム担当)：情報システムの問題か調査する。
LAN障害調査：各エリアのクライアントからサーバにアクセスするなどを実施。（LAN障害時はA3フロー参照）
設備異常調査：サーバ本体の電源LED確認、UPSの状況確認、ブレーカー確認。（設備障害時はA6フロー参照）
盗難・破壊確認：サーバ本体の外観確認、サーバラックの施錠状態なども確認。（盗難・破壊時はC3フロー参照）

③窓口(システム担当)：情報システムの問題だと考えられるとき、システム再起動を実施。
システム再起動を実施。
これで復旧した場合は、軽微な問題として記録。（多発するようであれば、原因究明、システムの見直し等実施。）

2.2. 報告

①窓口(システム担当)：管理者へ報告する。
「情報セキュリティ事故発生報告書」を起票し、状況を記入し、これをもとに管理者に報告する。
③窓口(システム担当)：（共有機器の場合）利用者に利用できないことを通知する。

3. 回復

3.2. 状況・原因把握と復旧（自社対応）

※状況を確認し、ウイルス感染の可能性であれば、B1フローを参照し、改ざんの可能性があればB2フローを参照する。
①窓口(システム担当)：（ソフトウェアの問題の場合）再インストール、再設定の実施。
②窓口(システム担当)：（ハードウェアの問題の場合）ハードウェア代替機の用意、再インストール。
③窓口(システム担当)：（ソフト/ハードの問題）データリストアの実施。
※共通予備サーバ（倉庫棚Aにあり、サーバOSインストール済み）、インストールメディア、手順書キャビネット、設定リスト、バックアップデータは、キャビネットに保管
ファイルサーバ（兼 ドメイン管理サーバ）
予備機から、ファイルサーバ、ドメイン管理機能の設定、ドメインユーザリスト等のデータリストアを手順書により実施。
OS管理サーバ（兼 ウイルス対策管理サーバ）
予備機から、OS管理アプリケーション、ウイルス対策管理アプリケーションのインストール、再設定を手順書により実施。
グループウェア
予備機から、グループウェアアプリケーションのインストール、再設定、データリストアを手順書により実施。

3.3. 状況・原因把握と復旧（対応委託）

①窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。
（バックアップデータ、設定リストは提供する必要がある。）

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口(システム担当)：（共有機器の場合）利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口(システム担当)：再発防止策を実施し、周知する。

図 28　A2 手順：自社管理している情報システムの障害対応

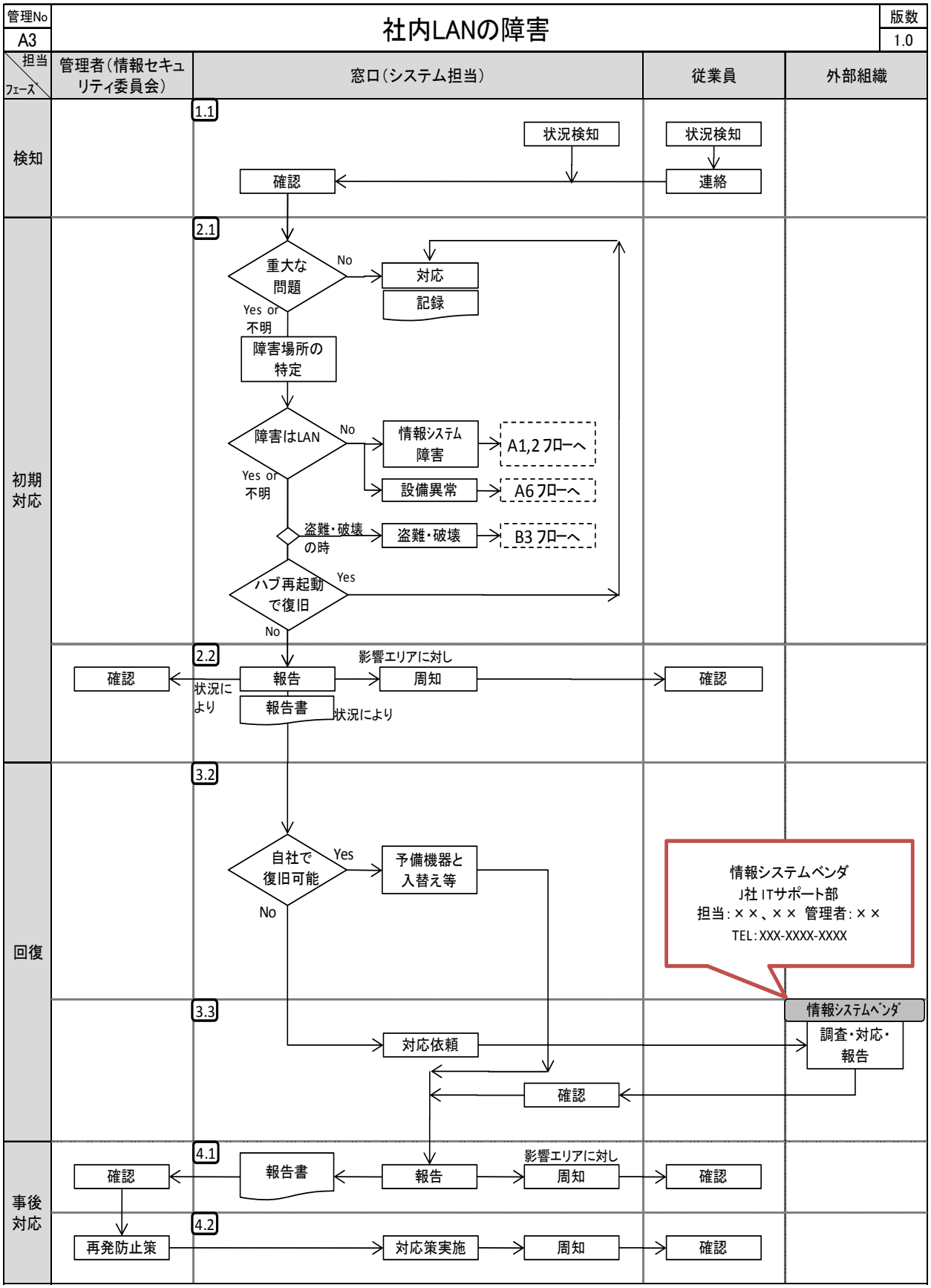


図 29　A3 フロー：社内 LAN の障害対応

A3解説

【対象情報システム】　LAN機器（ハブ、LANケーブル）

【概要】社内LANが利用できなくなったときは、その事象が社内LANの問題であるかどうかを切り分け、原因個所を特定し、迅速なLANの復旧を実施する。

【事例】

1 営業部に設置しているハブが故障し、営業部でLANが利用できなくなった。
2 サーバルームと総務部間のLANケーブルが断線し、総務部でLANが使えなくなった。
3 開発部の従業員が余っていたLANケーブルをハブに差し込んだところ、LANがループしてしまいLAN全体が使えなくなった。

【対応】

1. 検知
   1.1. 検知・連絡
      ①従業員：情報システムに障害を感じたら、窓口に連絡する。
      ②窓口(システム担当)：情報システムの障害を監視し、検知を行う。（特に具体的な監視作業は無し）
      ④窓口(システム担当)：障害の連絡を確認する。

2. 初期対応
   2.1. 問題の切り分け
      ①窓口(システム担当)：重大な問題か調査する。
         障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
            ※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。
         障害範囲（LANの一部か全部か、一部ならどのあたりか）を絞り込み、同時に軽微な問題かどうかを切り分ける。

      ②窓口(システム担当)：LANの問題か調査する。
         情報システムの障害：別のPCから各情報システムを確認。（情報システム障害時はA1、A2フロー参照）
         設備異常調査：ハブ本体の電源LED確認、場合によりブレーカー確認。（設備障害時はA6フロー参照）

      ③窓口(システム担当)：情報システムの問題だと考えられるとき、ハブ再起動を実施。
         ハブ再起動を実施。
         これで復旧した場合は、軽微な問題として記録。（多発するようであれば、原因究明、システムの見直し等実施。）

   2.2. 報告
      ①窓口(システム担当)：状況により、管理者へ報告する。（影響範囲がLAN全域に及ぶ場合等に限る。）
         管理者に報告時のみ「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。
      ③窓口(システム担当)：影響エリアに対し、利用者に利用できないことを通知する。

3. 回復
   3.2. 状況・原因把握と復旧（自社対応）
      ②窓口(システム担当)：（ハードウェアの問題の場合）ハードウェア代替機の用意。
         ※ハブ予備機、LANケーブル（倉庫棚Aにあり）
         状況により、ハブの予備機との交換、LANケーブル取り換えを実施し確認する。
         ハブのランプを確認。（場合により、LANがループ状に接続されている可能性もある。）

   3.3. 状況・原因把握と復旧（対応委託）
      ①窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。

4. 事後対応
   4.1. 報告
      ①窓口(システム担当)：（状況により）管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
      ②窓口(システム担当)：影響エリアに対し、利用者に回復したことを連絡する。
      ③管理者：報告の確認。

   4.2. 再発防止
      ①管理者：報告書等を元に、再発防止策を検討する。
      ②窓口(システム担当)：再発防止策を実施し、周知する。

図 30　A3 手順：社内 LAN の障害対応

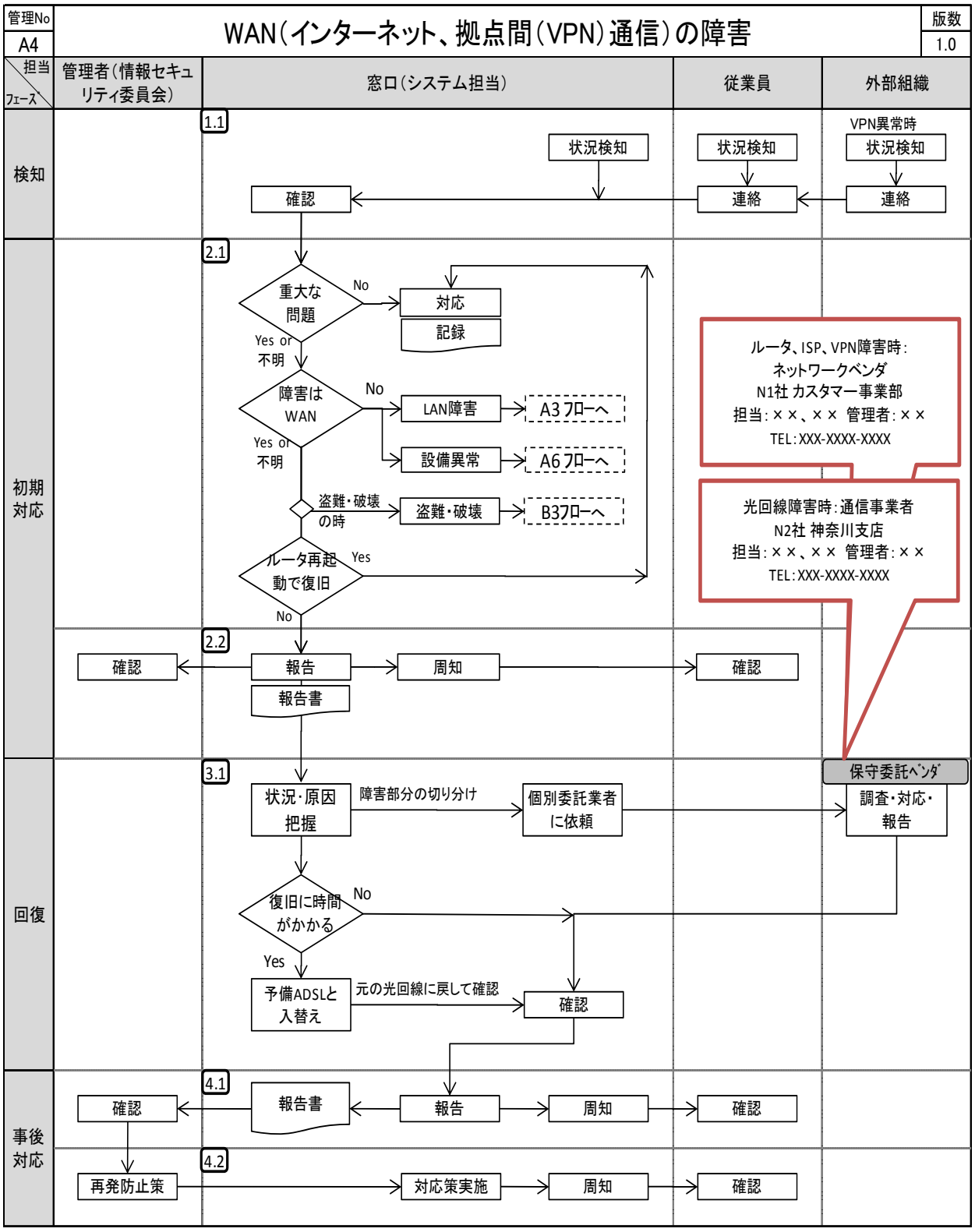


図 31　A4 フロー：WAN の障害対応

A4解説

【対象情報システム】　ルータ（ISP接続、VPN接続）、光終端装置、光ケーブル、ISP（インターネットサービスプロバイダ）

【概要】WANが利用できなくなったときは、その事象がWANの問題であるかどうかを切り分け、さらに要因を分析し、管理委託先に迅速なシステムの復旧を依頼する。

【事例】

1 ルータが故障し、インターネット通信、拠点間通信ができなくなった。
2 光ケーブルが断線し、インターネット通信、拠点間通信ができなくなった。
3 ISP側のトラブルで、インターネット通信ができなくなった。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：情報システムに障害を感じたら、窓口に連絡する。
②窓口（システム担当）：情報システムの障害を監視し、検知を行う。（特に具体的な監視作業は無し）
③VPNベンダ：VPNで異常を検知たら、システム担当にメール送信される（ことがある）。
④窓口（システム担当）：障害の連絡を確認する。

2. 初期対応

2.1. 問題の切り分け

①窓口（システム担当）：重大な問題か調査する。
障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。
実際に操作して状態を確認し、軽微な問題かどうかを切り分ける。

②窓口（システム担当）：情報システムの問題か調査する。
LAN障害調査：各エリアのクライアントからサーバにアクセスするなどを実施。（LAN障害時はA3フロー参照）
設備異常調査：ルータ、光終端装置の電源LED確認、UPSの状況確認、ブレーカー確認。（設備障害時はA6フロー参照）
盗難・破壊確認：ルータ本体、光終端装置、光ケーブルの外観確認。（盗難・破壊時はB3フロー参照）

③窓口（システム担当）：情報システムの問題と考えられるとき、システム再起動を実施。
ルータ再起動を実施。
これで復旧した場合は、軽微な問題として記録。（多発するようであれば、原因究明、システムの見直し等実施。）

2.2. 報告

①窓口（システム担当）：管理者へ報告する。
「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。
③窓口（システム担当）：利用者に利用できないことを通知する。

3. 回復

3.1. 状況・原因把握と復旧（保守委託品）

①窓口（システム担当）：保守委託ベンダに状況を連絡する。
障害箇所を切り分ける。
・ルータ、ISP、VPNが障害の場合：ネットワークベンダN1社に連絡し、対応を依頼する。
・光回線が障害の場合：通信事業者N2社に連絡し、対応を依頼する。
（上記どちらが障害か判断がつかない場合、ネットワークベンダN1社に連絡し、指示を仰ぐ。）
②窓口（システム担当）：復旧に時間がかかるとき、予備のWAN回線で仮復旧させる。
復旧に時間が掛かる場合は、予備のADSL回線（事務所入り口の電話回線）に予備のルータ（倉庫棚Aにあり）を取り付け、インターネット接続させる。
（ただし、現状、VPN機能が無いため、拠点間通信は利用不能。）
復旧が確認できたら、予備のADSL回線を撤去し、元に戻す。

4. 事後対応

4.1. 報告

①窓口（システム担当）：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口（システム担当）：利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口（システム担当）：再発防止策を実施し、周知する。

図 32　A4 手順：WAN の障害対応

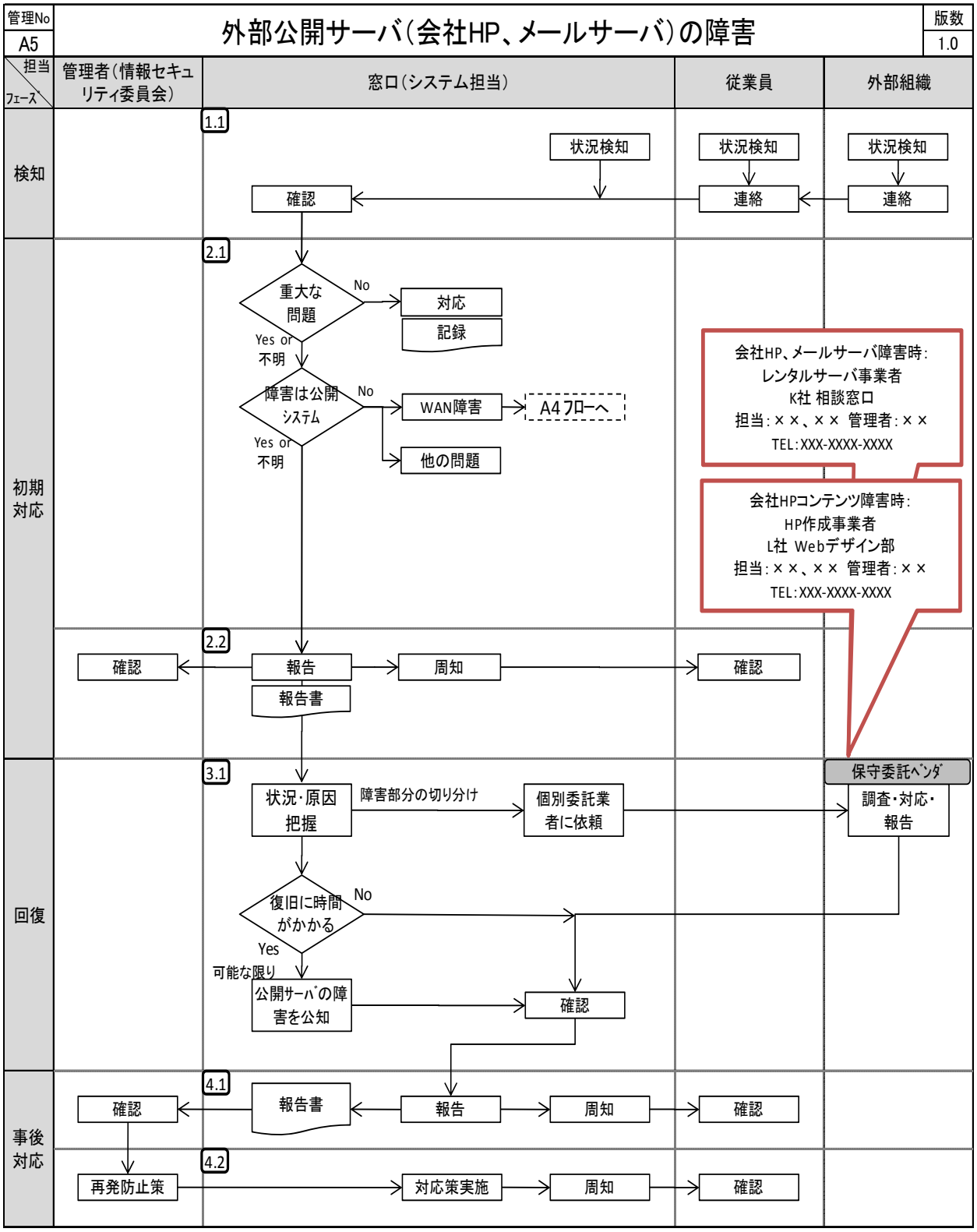


図 33　A5 フロー：外部公開サーバの障害対応

A5解説

【対象情報システム】　レンタルサーバ（会社HP、メールサーバ）

【概要】外部に公開している情報システムが利用できなくなったときは、問題の切り分け、要因を分析し、要因により各委託先に対応を依頼する。

【事例】

1 会社のHPを公開しているサーバが故障し、利用できなくなった。
2 会社のHPのアクセスが非常に遅くなったと顧客から連絡があった。
3 メールの送受信ができなくなった。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：情報システムに障害を感じたら、窓口に連絡する。
②窓口(システム担当)：情報システムの障害を監視し、検知を行う。（特に具体的な監視作業は無し）
③顧客：公開システムで異常を感じたら、組織に連絡がある（ことがある）。
④窓口(システム担当)：障害の連絡を確認する。

2. 初期対応

2.1. 問題の切り分け

①窓口(システム担当)：重大な問題か調査する。
障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。
自分で操作して状態を確認し、軽微な問題かどうかを切り分ける。

②窓口(システム担当)：公開システムの問題か調査する。
WAN障害：自社から自社HPにアクセスが出来ない、メールの送受信が出来ないとき、他のHP等を見てみる。
他の問題：顧客からの以上の連絡では、顧客側の問題の可能性あり。
メール：ISP側の制限（迷惑メール送信対策等）の可能性もあるため、ISPのHPで情報を収集する。

2.2. 報告

①窓口(システム担当)：管理者へ報告する。
「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。
③窓口(システム担当)：利用者に利用できないことを通知する。

3. 回復

3.1. 状況・原因把握と復旧（保守委託品）

①窓口(システム担当)：保守委託ベンダに状況を連絡する。
障害内容を切り分ける。
・会社HP（の環境）、メールの送受信が障害の場合：レンタルサーバ事業者K社に連絡し、対応を依頼する。
（障害ではなく、会社HP(あるいは同一サーバ内の他社HP)がDoS攻撃を受けている可能性もある。）
・会社HP（コンテンツ）の場合：通信事業者N2社に連絡し、対応を依頼する。
（コンテンツの作成、転送ミスで会社HPが見れない可能性もある。）
（コンテンツ転送アカウントを盗まれた、コンテンツの作成ミス等で会社HPにウイルスが埋め込まれた可能性もある。）
上記どちらの障害か判断がつかない場合、レンタルサーバ事業者K社に連絡し、指示を仰ぐ。

②窓口(システム担当)：復旧に時間がかかるとき、（可能な限り）利用者にこれを公知する。
会社HPのコンテンツ復旧に時間が掛かる場合などは、「コンテンツ修復中」の旨を表示させるようにする。

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口(システム担当)：利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口(システム担当)：再発防止策を実施し、周知する。

図 34　A5 手順：外部公開サーバの障害対応

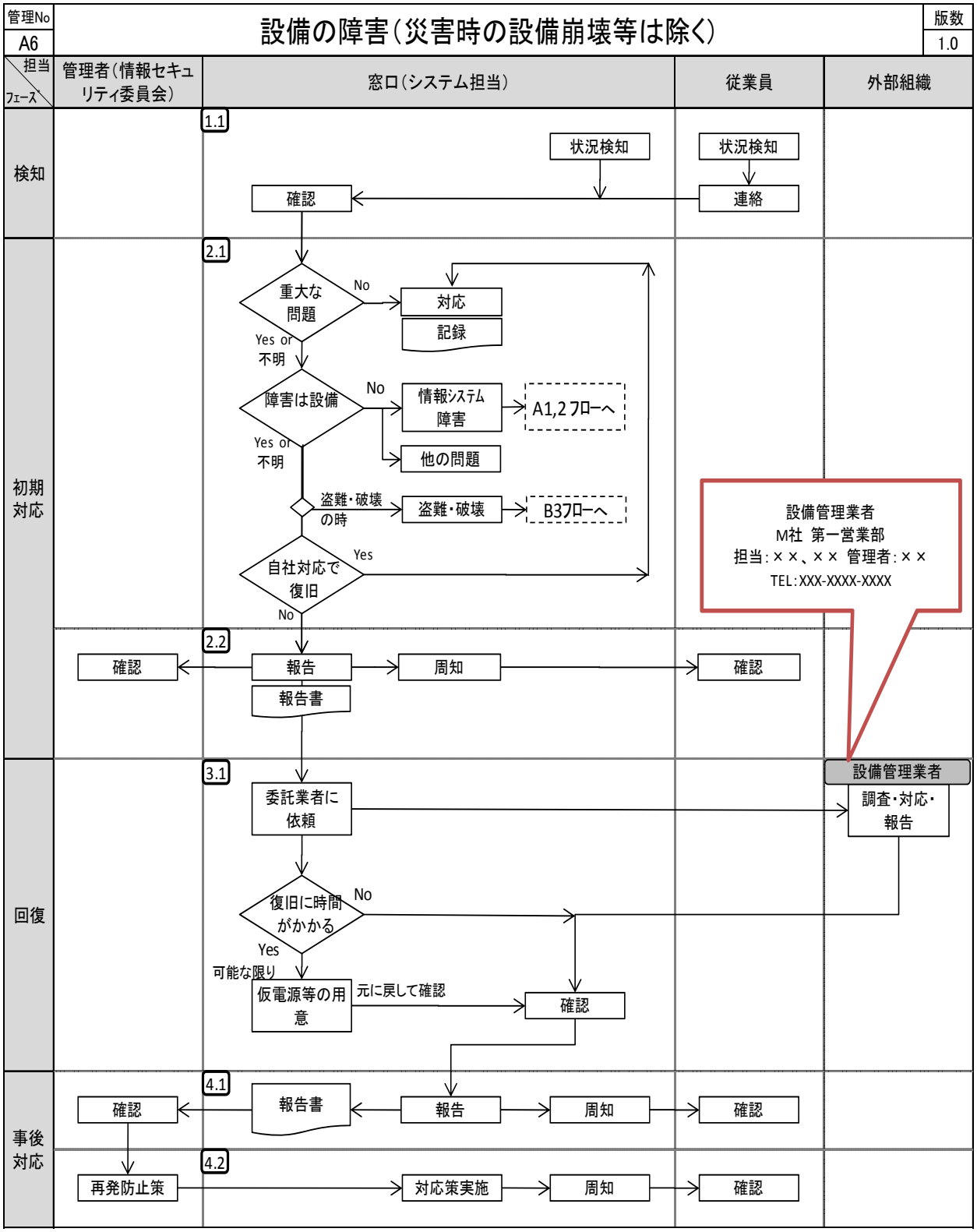


図 35　A6 フロー：設備の障害対応

A6解説

【対象情報システム】　電源、空調（情報システムに供給している部分に限る）

【概要】設備（電源、空調）が異常を起こし、情報システムが利用できなくなったとき、その要因が自社で対応可能であれば対応し、不可であれば設備管理事業者に対応を依頼する。（大きな災害等はBCPとして別途検討が必要）

【事例】

1 サーバラックに供給している電源のブレーカーが落ち、UPSで稼働し、その後、電源供給ができなくなった。

2 サーバラック内の温度が上昇し、サーバが異常を検知して停止した。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：情報システムに障害を感じたら、窓口に連絡する。

②窓口(システム担当)：情報システムの障害を監視し、検知を行う。（特に具体的な監視作業は無し）

④窓口(システム担当)：障害の連絡を確認する。

2. 初期対応

2.1. 問題の切り分け

①窓口(システム担当)：重大な問題か調査する。

障害の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）

※情報システム事故受付表は、内容を分析し、半年に1回報告書にまとめる。

自分でサーバラックや他の情報システムへの電源供給状態を確認し、軽微な問題かどうかを切り分ける。

②窓口(システム担当)：設備（電源、空調）の問題か調査する。

情報システム自体の障害：情報システムの電源が入っていない場合など、情報システム自体（ハードウェア）の問題か確認する。

他の問題：サーバラック電源障害のとき、UPSの問題の可能性を検討する。

③窓口(システム担当)：設備（電源、空調）の問題と考えられるときは下記を実施。

電源の問題：ブレーカーが落ちている場合は、これを上げてみる。

空調の問題：空調機器を確認し、自社で対応できれば実施する。

2.2. 報告

①窓口(システム担当)：管理者へ報告する。

「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。

③窓口(システム担当)：利用者に利用できないことを通知する。

3. 回復

3.1. 状況・原因把握と復旧（保守委託品）

①窓口(システム担当)：保守委託ベンダに状況を連絡する。

設備業者に状況を説明し、対応を依頼する。

②窓口(システム担当)：復旧に時間がかかるとき、（可能な限り）仮電源等で運転を再開する。

設備の復旧に時間が掛かる場合などは、他の電源系統から電源が取れる場合など、他の電源を仮配線し、運転する。

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）

②窓口(システム担当)：利用者に回復したことを連絡する。

③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。

②窓口(システム担当)：再発防止策を実施し、周知する。

図 36　A6 手順：設備の障害対応

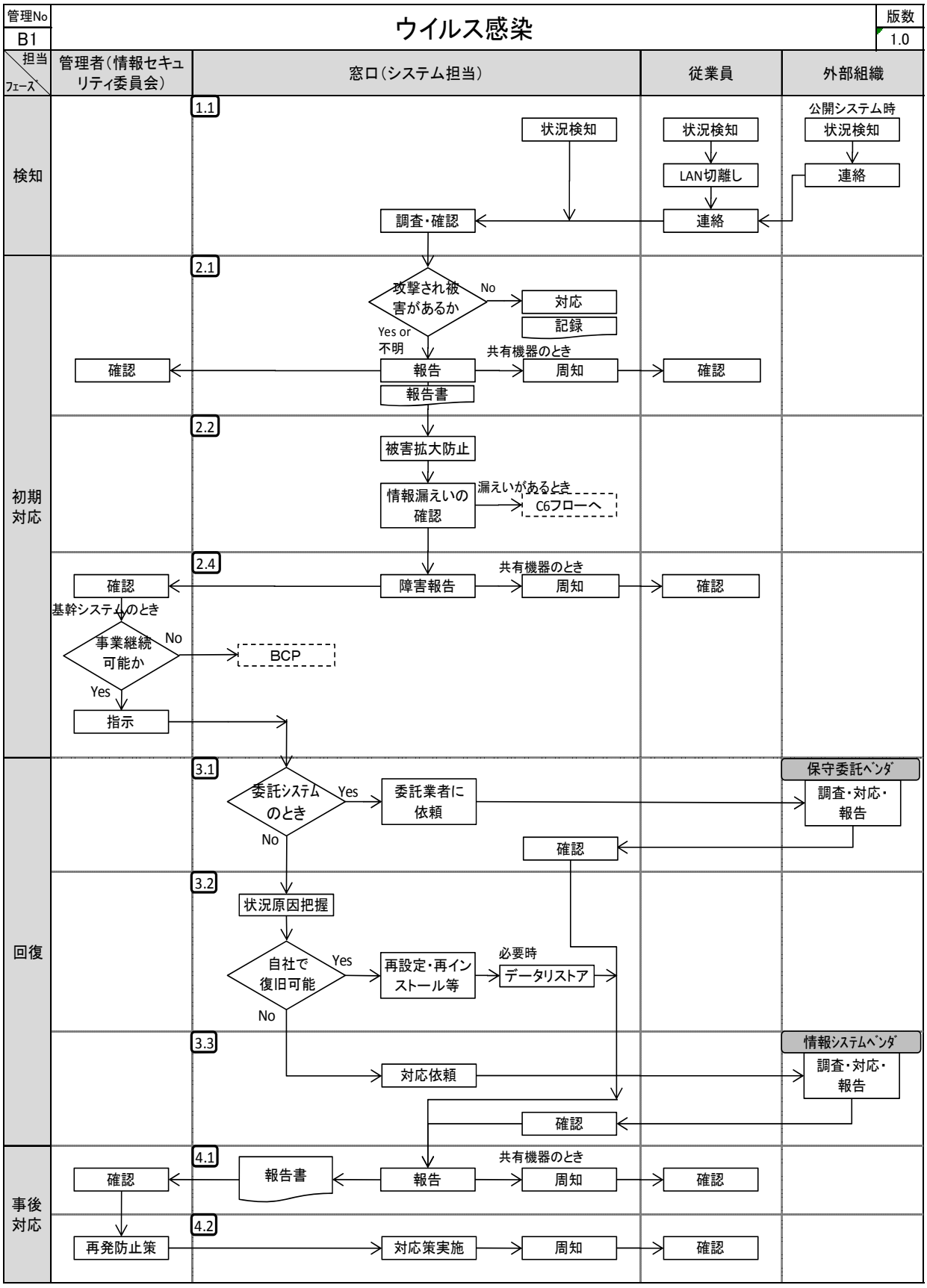


図 37　B1 フロー：ウイルス感染対応

B1解説

【対象情報システム】　基幹システム（販売管理システム）、各種サーバ、クライアントPC

【概要】情報システムがウイルスに感染したときはその事象を確認し、被害拡大防止、情報漏えいの確認を行い、ウイルスを駆除またはシステムの再インストールを実施し対応する。

【事例】

1 事務用PCの動作に異常があり、ウイルス感染したのかもしれない。（ウイルス対策ソフトは検知していない。）
2 ファイルサーバがウイルス感染し、感染したウイルスにより情報が漏えいしてしまったようだ。
3 顧客から「受け取ったメールの添付ファイルがウイルスに感染していた」と連絡があった。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：各自のPCでウイルス感染等の兆候を感じたら、PCに接続されているLANケーブルを切り離し窓口に連絡する。
②窓口(システム担当)：情報システムへのウイルス感染を監視し、検知を行う。
定期的にウイルス監視ソフト管理画面を閲覧し、ウイルスの検知・駆除状況を確認する。
③顧客：公開システムで異常を感じたら、組織に連絡がある（ことがある）。
④窓口(システム担当)：ウイルス感染の連絡を確認する。

2. 初期対応

2.1. 問題の切り分けと報告

①窓口(システム担当)：情報システムへのウイルス感染で、被害があるか確認する。
ウイルス感染の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
被害が無い場合（ウイルス対策ソフトが駆除済等）は記録で終了。被害を受けた可能性がある場合は以下のステップへ。
ウイルス感染か不明な場合は、ウイルスチェックを実施する。
ウイルスが検知できないときは、他社ウイルス対策ソフトベンダのソフトでのチェックも実施してみる。
（ウイルス対策ソフトベンダ各社で保持するウイルスパターンが違うため）
参考）情報セキュリティ安心相談窓口：ウィルス対策、不正アクセス等
http://www.ipa.go.jp/security/anshin/、TEL:03-5978-7509
②窓口(システム担当)：管理者へ報告する。（共有システムの場合）利用者に使用中止を呼びかける。
「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。

2.2. 被害拡大の防止

①窓口(システム担当)：ウイルス感染の状況により、被害拡大が防止できる対策があれば実施する。
共有システムが感染した場合など、感染が拡大しないように接続されているLANケーブルを外し、隔離する。
②窓口(システム担当)：情報漏えいの有無を確認する。
ウイルスが情報システム内の情報を漏えいした可能性があるので、調査を行う。
情報漏えいがあった場合は、C6フローを参照し対処する。（2.3以降のステップと同時に実施）

2.3. 意図的犯行時の対応

（基本的には、このステップなし。ただし、標的型攻撃など、意図的に自社のシステムにウイルス感染を狙ったような場合は、検討実施。この時は、B2フロー等を参照。）

2.4.（障害）報告

①窓口(システム担当)：管理者に障害の状況を報告する。
②管理者：事業継続に関わる場合、BCPの実施を検討する。（基幹システムの場合のみ：A1フロー参照）
③窓口(システム担当)：（共有システムの場合）利用者に利用できないことを通知する。

3. 回復

※ウイルス駆除：ウイルス対策ソフトが検知のみで駆除できなかった場合は、対策ソフトベンダのHP等で対応方法を確認し実施。
ウイルス感染かどうか不明だが動作がおかしい場合は、OSからクリーンインストール実施。
※回復フェーズの詳細はA1、A2フロー参照

3.1. 復旧（保守委託品）

①窓口(システム担当)：（保守委託品の場合）保守委託ベンダに状況を連絡する。

3.2. 復旧（自社対応）

①窓口(システム担当)：再インストール、再設定の実施。
②窓口(システム担当)：データリストアの実施。

3.3. 復旧（対応委託）

①窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口(システム担当)：（共有機器の場合）利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口(システム担当)：再発防止策を実施し、周知する。

図 38　B1 手順：ウイルス感染対応

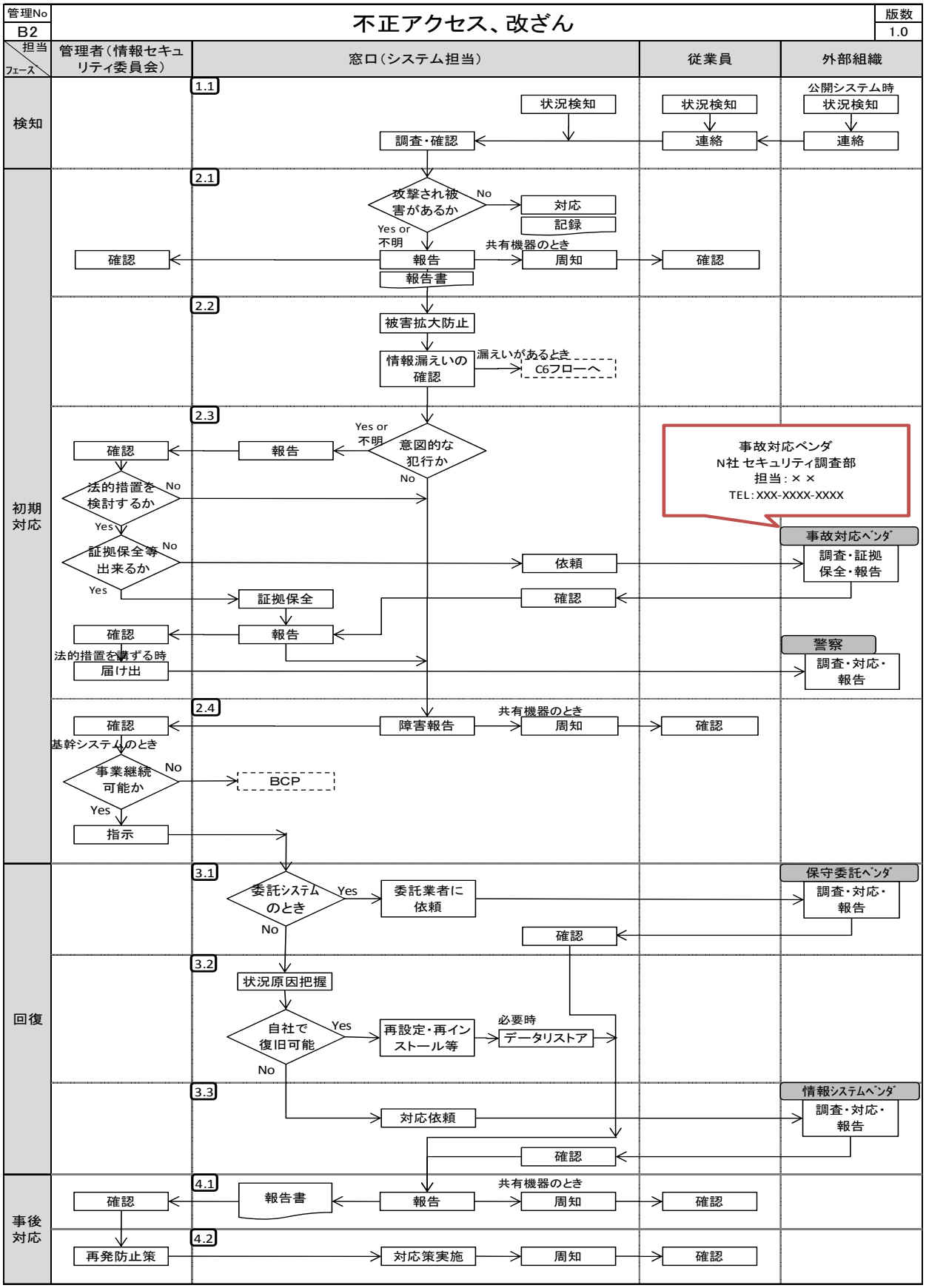


図 39　B2 フロー：不正アクセス、改ざん対応

B2解説

【対象情報システム】　基幹システム（販売管理システム）、各種サーバ、クライアントPC

【概要】情報システムが不正アクセス、改ざんにあったときはその事象を確認し、被害拡大防止、情報漏えいの確認を行い、犯罪行為への法的措置を講じるかを検討し、再設定またはシステムの再インストールを実施し対応する。

【事例】

1 ファイルサーバのログをチェックしていたら、不正にアクセスされた形跡があった。
2 基幹システムに不正アクセスされ、情報が漏えいした。
3 公開しているHPが改ざんされていると、外部の人から連絡があった。

【対応】

1. 検知
   1.1. 検知・連絡
   ①従業員：各自のPCで不正なアクセス、改ざんを感じたら、窓口に連絡する。
   ②窓口(システム担当)：情報システムへの不正アクセス、改ざんを監視し、検知を行う。
   現状は、不正アクセス、改ざんの監視は特になし。（将来的には不正アクセスの検知を検討。）
   ③顧客：公開システムで異常を感じたら、組織に連絡がある（ことがある）。
   ④窓口(システム担当)：不正アクセス、改ざんの連絡を確認する。

2. 初期対応
   2.1. 問題の切り分けと報告
   ①窓口(システム担当)：情報システムへの不正アクセス、改ざんで、被害があるか確認する。
   不正アクセス、改ざんの連絡を受けた時点で、「情報システム事故受付表」に状況を記録。
   被害が無い場合（不正アクセスの試みのみ、間違って書き換えてしまった等の改ざんとは言えないような場合）は記録で終了。
   被害を受けた可能性がある場合は以下のステップへ。
   参考）情報セキュリティ安心相談窓口：ウィルス対策、不正アクセス等
   http://www.ipa.go.jp/security/anshin/、TEL:03-5978-7509
   ②窓口(システム担当)：管理者へ報告する。（共有システムの場合、必要に応じて）利用者に使用中止を呼びかける。
   「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。

   2.2. 被害拡大の防止
   ①窓口(システム担当)：不正アクセス、改ざんを受けた状況により、被害拡大が防止できる対策があれば実施する。
   情報システムの（不正アクセスに利用されている）ログインIDの無効化、パスワードの変更を実施する。
   不正アクセス、改ざんが現在も行われている形跡があれば、LANケーブルを外し、ネットワークから隔離することを検討する。
   ②窓口(システム担当)：不正アクセスを受けた場合、情報漏えいの有無を確認する。
   情報漏えいがあった場合は、C6フローを参照し対処する。（2.3以降のステップと同時に実施）

   2.3. 意図的犯行時の対応
   ※現状の体制では、正式な証拠保全ができないと思われるので、事故対応ベンダへの依頼が必要と考えられる。
   ①窓口(システム担当)：意図的な犯行による不正アクセス、改ざんが疑われるときは、管理者に報告をする。
   ②管理者：意図的な犯行による不正アクセス、改ざんが疑われるときは、法的措置を検討するか判断する。
   ③窓口(システム担当)：意図的な犯行による不正アクセス、改ざんが疑われるときは、証拠保全を行う。
   ④管理者：調査報告を受け、法的措置を講ずるか判断する。

   2.4.（障害）報告
   ①窓口(システム担当)：管理者に障害の状況を報告する。
   ②管理者：事業継続に関わる場合、BCPの実施を検討する。（基幹システムの場合のみ：A1フロー参照）
   ③窓口(システム担当)：（共有システムの場合）利用者に利用できないことを通知する。

3. 回復
   ※不正アクセス、改ざんされた場合は、基本的にはOSからクリーンインストール実施
   明らかに被害個所が特定され、これが修復出来るときは修復のみとする
   ※回復フェーズの詳細はAフロー参照
   3.1. 復旧（保守委託品）
   ①窓口(システム担当)：（保守委託品の場合）保守委託ベンダに状況を連絡する
   3.2. 復旧（自社対応）
   ①窓口(システム担当)：再インストール、再設定の実施
   ②窓口(システム担当)：データリストアの実施
   3.3. 復旧（対応委託）
   ①窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する

4. 事後対応
   4.1. 報告
   ①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
   ②窓口(システム担当)：（共有機器の場合）利用者に回復したことを連絡する。
   ③管理者：報告の確認。

   4.2. 再発防止
   ①管理者：報告書等を元に、再発防止策を検討する。
   ②窓口(システム担当)：再発防止策を実施し、周知する。

図 40　B2 手順：不正アクセス、改ざん対応

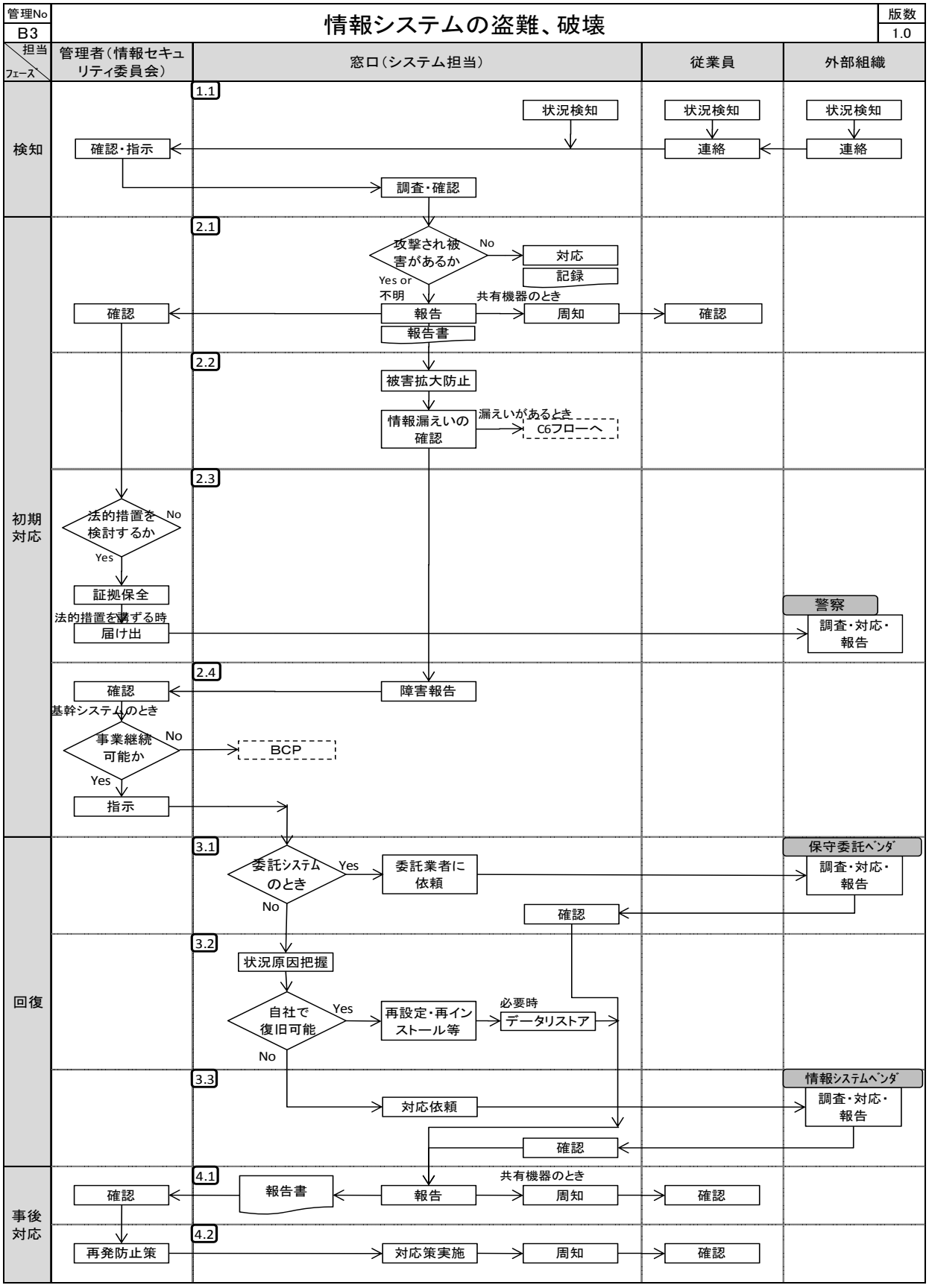


図 41　B3 フロー：情報システムの盗難、破壊対応

B3解説

【対象情報システム】　基幹システム（販売管理システム）、各種サーバ、クライアントPC

【概要】情報システムが盗難、破壊にあったときはその事象を確認し、被害拡大防止、情報漏えいの確認を行い、犯罪行為への法的措置を講じるかを検討し、再設定またはシステムの再インストールを実施し対応する。

【事例】

1 事務所に泥棒が入り、情報システムが盗まれた。
2 事務所に泥棒が入り、情報システムが壊された。
3 外部の人が、中古PCショップで会社のPCが売られているのを見て連絡をくれた。

【対応】

1. 検知

1.1. 検知・連絡

①従業員：各自のPCで盗難、破壊があったら、管理者に連絡する。
②窓口(システム担当)：情報システムへの盗難、破壊があったら、管理者に連絡する。
③管理者：盗難、破壊の連絡を確認する。
④窓口(システム担当)：盗難、破壊調査を開始する。

2. 初期対応

2.1. 問題の切り分けと報告

①窓口(システム担当)：情報システムの盗難、破壊で、被害があるか確認する。
盗難、破壊の連絡を受けた時点で、「情報システム事故受付表」に状況を記録。（勘違い等であれば記録しない。）
被害が無い場合は記録で終了。被害を受けた可能性がある場合は以下のステップへ。
②窓口(システム担当)：管理者へ報告する。（共有システムの場合）利用者に利用できないことを通知する。
「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。

2.2. 被害拡大の防止

①窓口(システム担当)：状況により、被害拡大が防止できる対策があれば実施する。
②窓口(システム担当)：盗難があった場合、情報漏えいの有無を確認する。
情報漏えいがあった場合は、C6フローを参照し対処する。(2.3以降のステップも実施)

2.3. 意図的犯行時の対応

②管理者：意図的な犯行による盗難、破壊が疑われるときは、法的措置を検討するか判断する。
③管理者：同時に、証拠保全を行う。
④管理者：法的措置を講ずるか判断する。

2.4. （障害）報告

①窓口(システム担当)：管理者に障害の状況を報告する。
②管理者：事業継続に関わる場合、BCPの実施を検討する。（基幹システムの場合のみ：A1フロー参照）

3. 回復

※回復フェーズの詳細はA1、A2フロー参照

3.1. 復旧（保守委託品）

①窓口(システム担当)：（保守委託品の場合）保守委託ベンダに状況を連絡する。

3.2. 復旧（自社対応）

①窓口(システム担当)：再インストール、再設定の実施。
②窓口(システム担当)：データリストアの実施。

3.3. 復旧（対応委託）

①窓口(システム担当)：復旧作業を自社で実施できない場合、情報システムベンダへ対処を依頼する。

4. 事後対応

4.1. 報告

①窓口(システム担当)：管理者に報告する。（後日、「情報セキュリティ事故最終報告書」をまとめ提出。）
②窓口(システム担当)：（共有機器の場合）利用者に回復したことを連絡する。
③管理者：報告の確認。

4.2. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②窓口(システム担当)：再発防止策を実施し、周知する。

図 42　B3 手順：情報システムの盗難、破壊対応

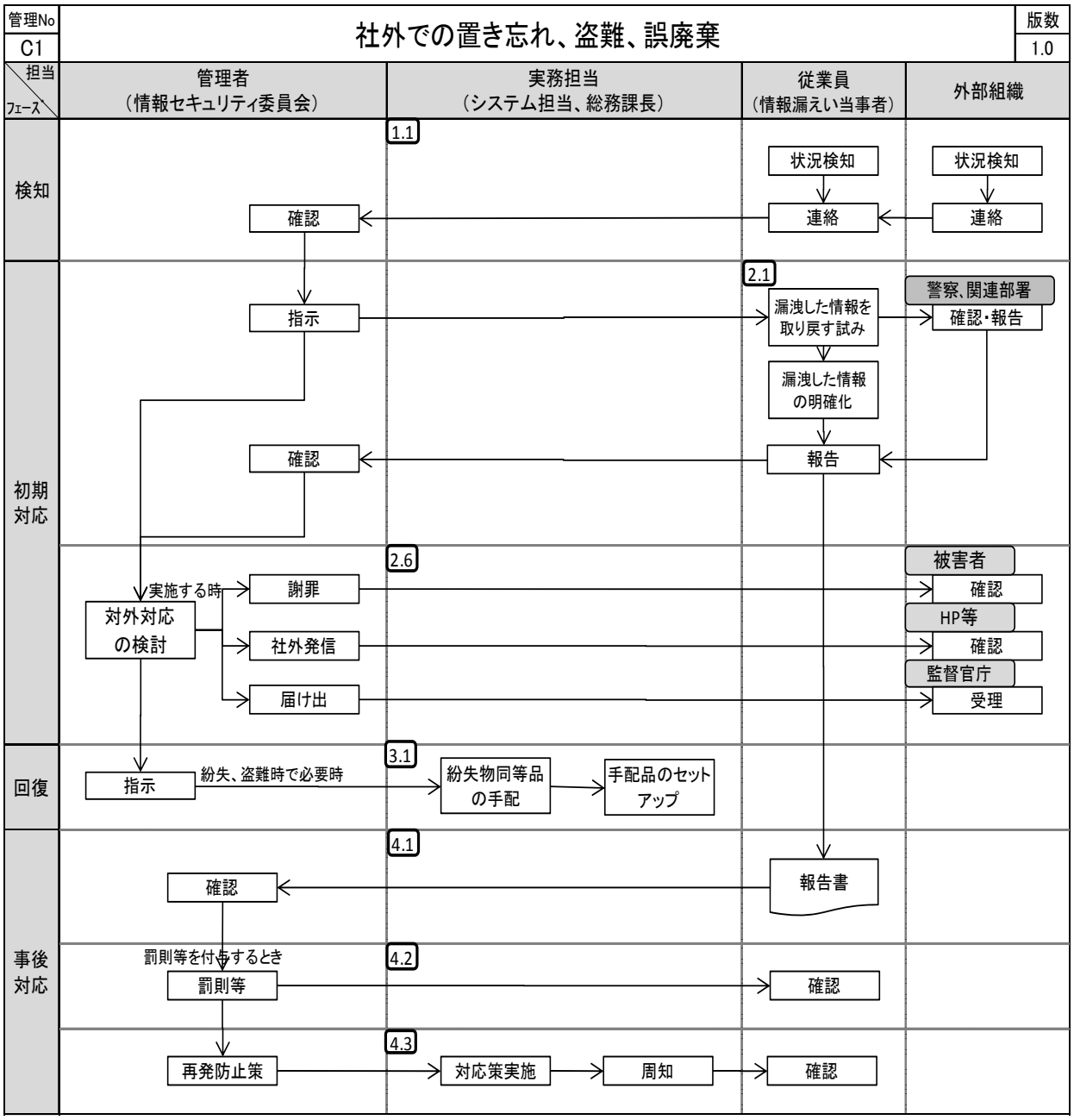


図 43　C1 フロー：社外での置き忘れ、盗難、誤廃棄対応

C1解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】重要な情報を格納した携帯機器や媒体を無くしたり、盗まれたりしたときや重要な情報が入ったままの情報システムをそのまま廃棄してしまったときは情報漏えいの可能性がでる。対外対応を行うか検討し対応する。

【事例】

1 顧客情報を入れたUSBメモリをカバンに入れておいたら、カバンを電車内に置き忘れた。
2 携帯電話を入れたカバンを盗まれた。
3 事務用PC内のデータを完全に消去しない状態で廃棄し、これを中古機器として購入した人から連絡を受けた。

【対応】

1. 検知

1.1. 検知・連絡

①情報漏えい当事者：（自分で情報漏えいに気がついたとき）管理者に連絡する。
③顧客：情報が漏えいしているのに気付いたとき（無くしたものを見つけたとき）、組織に連絡がある（ことがある）。
④管理者：情報漏えいの連絡を確認する。

2. 初期対応

2.1. 当事者の初期対応

①管理者：情報漏えい当事者が分かっている場合（紛失、盗難 等）、当事者に指示を出す。
②情報漏えい当事者：（情報の紛失等の場合）関係各所へ連絡し捜索の依頼、警察への届出等を行う。
紛失、盗難時：可能な限り、無くしたもの、盗難にあったものを探し、警察に紛失、盗難届を提出する。
誤廃棄：可能な限り、誤廃棄したものを探す。（また、廃棄されたものがどの様な経路でどうなったかを確認する。）
③情報漏えい当事者：（情報の紛失等の場合）紛失した情報にどんなものがあったか明確にする。
事前に記入した、「持ち出し情報一覧」を確認し、実際にこの情報に間違いが無いか再確認する。
④情報漏えい当事者：管理者に報告する。

2.6. 対外対応

①管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。
被害者（漏えいしてしまった顧客情報の顧客）に謝罪する。
社外発信（HP掲載）について検討し、必要に応じて実施する。
②管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。
届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復

3.1. 復旧

①実務担当：（必要に応じて）紛失、盗難にあった同等品を手配する。
②実務担当：（必要に応じて）手配したものが来たら、利用可能なようにセットアップする。

4. 事後対応

4.1. 報告

①漏えい当事者：情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。

4.2. 処罰等

①管理者：情報漏えいを起こした当事者に対し、処罰等を行うか検討する。
社則の処罰規定に基づき、処罰を行う。

4.3. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②実務担当：再発防止策を実施し、周知する。

図 44　C1 手順：社外での置き忘れ、盗難、誤廃棄対応

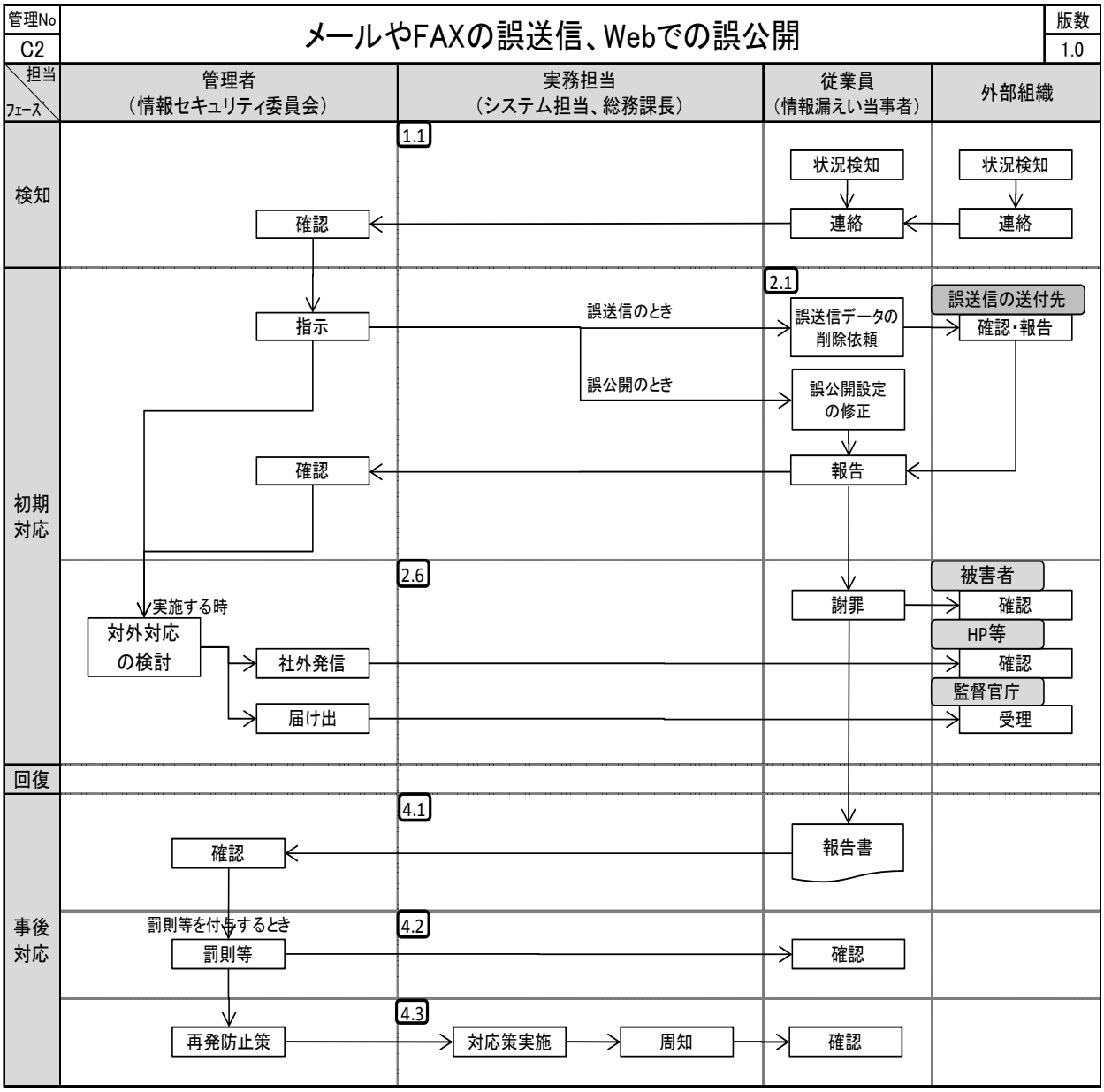


図 45　C2 フロー：メールや FAX の誤送信、Web での誤公開対応

C2解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】重要な情報を含むメールやFAXを誤送信したり、Web等で重要な情報を誤公開したときは情報漏えいとなる。誤送信先への破棄依頼などを行い、対外対応を行うか検討し対応する。

【事例】

1 メール（FAX）の宛先を間違えて重要な情報を送信した。

2 メールの同報送信で、宛先に様々な顧客のメールアドレスを入れて送信したため、顧客のメールアドレスが漏えいしてしまった。

3 会員制のWebサイトで、設定ミスから、非公開の顧客情報を公開してしまった。

【対応】

1. 検知

1.1. 検知・連絡

①情報漏えい当事者：（自分で情報漏えいに気がついたとき）管理者に連絡する。

③顧客：情報が漏えいしているのに気付いたとき（誤送信、誤公開に気付いたとき）、組織に連絡がある（ことがある）。

④管理者：情報漏えいの連絡を確認する。

2. 初期対応

2.1. 当事者の初期対応

①管理者：情報漏えい当事者に指示を出す。

②情報漏えい当事者：（誤送信の場合）誤送信先にデータの削除依頼を行う。

③情報漏えい当事者：（誤公開の場合）公開してしまった設定を修正する。

④情報漏えい当事者：管理者に報告する。

2.6. 対外対応

①情報漏えい当事者：（漏えいした情報が顧客情報のとき）顧客への謝罪を行う。

被害者（漏えいしてしまった顧客情報の顧客）に経緯を含め謝罪する。

②管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。

社外発信（HP掲載）について検討し、必要に応じて実施する。

③管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。

届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復（なし）

4. 事後対応

4.1. 報告

①漏えい当事者：情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。

4.2. 処罰等

①管理者：情報漏えいを起こした当事者に対し、処罰等を行うか検討する。

社則の処罰規定に基づき、処罰を行う。

4.3. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。

②実務担当：再発防止策を実施し、周知する。。

図 46　C2 手順：メールや FAX の誤送信、Web での誤公開対応

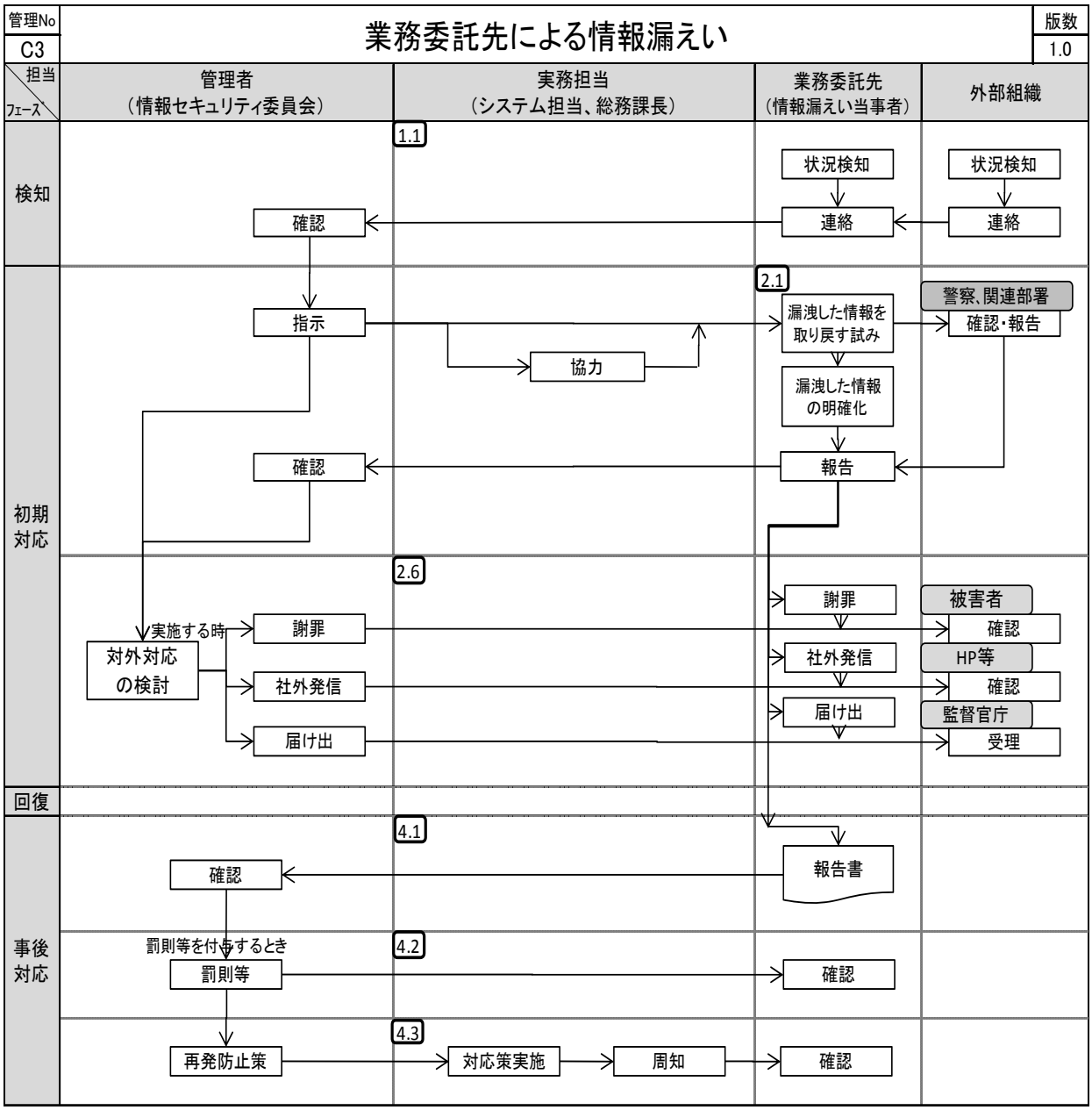


図 47　C3 フロー：業務委託先による情報漏えい対応

C3解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】業務委託先に預けた重要な情報が漏えいしたときは、委託元の監督不十分と見なされる。業務委託先と連絡を取り合い、対外対応について検討し、最終的には委託先に対して訴訟等の検討をおこなう。

【事例】

1 顧客へのダイレクトメールの印刷を委託した業者が顧客情報を漏えいした。
2 基幹システムの保守委託をしているベンダがバックアップデータを遠隔地に保管しようと持ち出し、紛失した。
3 基幹システム改造時に、開発委託ベンダが開発作業を再委託し、再委託先が機密情報を情報漏えいをした。

【対応】

1. 検知
   1.1. 検知・連絡
      ①情報漏えい当事者（委託先）:（委託先が情報漏えいを起こしてしまったとき）委託元の管理者に連絡する。
      ③顧客:情報が漏えいしているのに気付いたとき、組織に連絡がある（ことがある）。
      ④管理者:情報漏えいの連絡を確認する。

2. 初期対応
   2.1. 当事者の初期対応
      ①管理者:当事者、実務担当に指示を出す。
         漏えい当事者への指示:情報漏えいの初期対応実施の指示。
         実務担当への指示:漏えい当事者の対応に協力する。（同時に対応内容を監視・監督する。）
      ②情報漏えい当事者:漏えいした情報を取り戻す試みを実施。
      ③情報漏えい当事者:漏えいした情報の明確化を実施。
      ④情報漏えい当事者:管理者に報告する。

   2.6. 対外対応
      ①管理者、情報漏えい当事者:（漏えいした情報が顧客情報のとき）顧客への謝罪を行う。
         被害者（漏えいしてしまった顧客情報の顧客）に経緯を含め謝罪する。
      ②管理者、情報漏えい当事者:（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。
         社外発信（HP掲載）について検討し、必要に応じて実施する。
      ③管理者、情報漏えい当事者:（漏えいした情報が個人情報のとき）監督官庁への届出を行う。
         届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復（なし）

4. 事後対応
   4.1. 報告
      ①漏えい当事者:情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。
   4.2. 処罰等
      ①管理者:情報漏えいを起こした当事者に対し、処罰等を行うか検討する。
         委託契約などに基づき、罰則を検討する。
   4.3. 再発防止
      ①管理者:報告書等を元に、再発防止策を検討する。
      ②実務担当:再発防止策を実施し、周知する。

図 48　C3 手順：業務委託先による情報漏えい対応

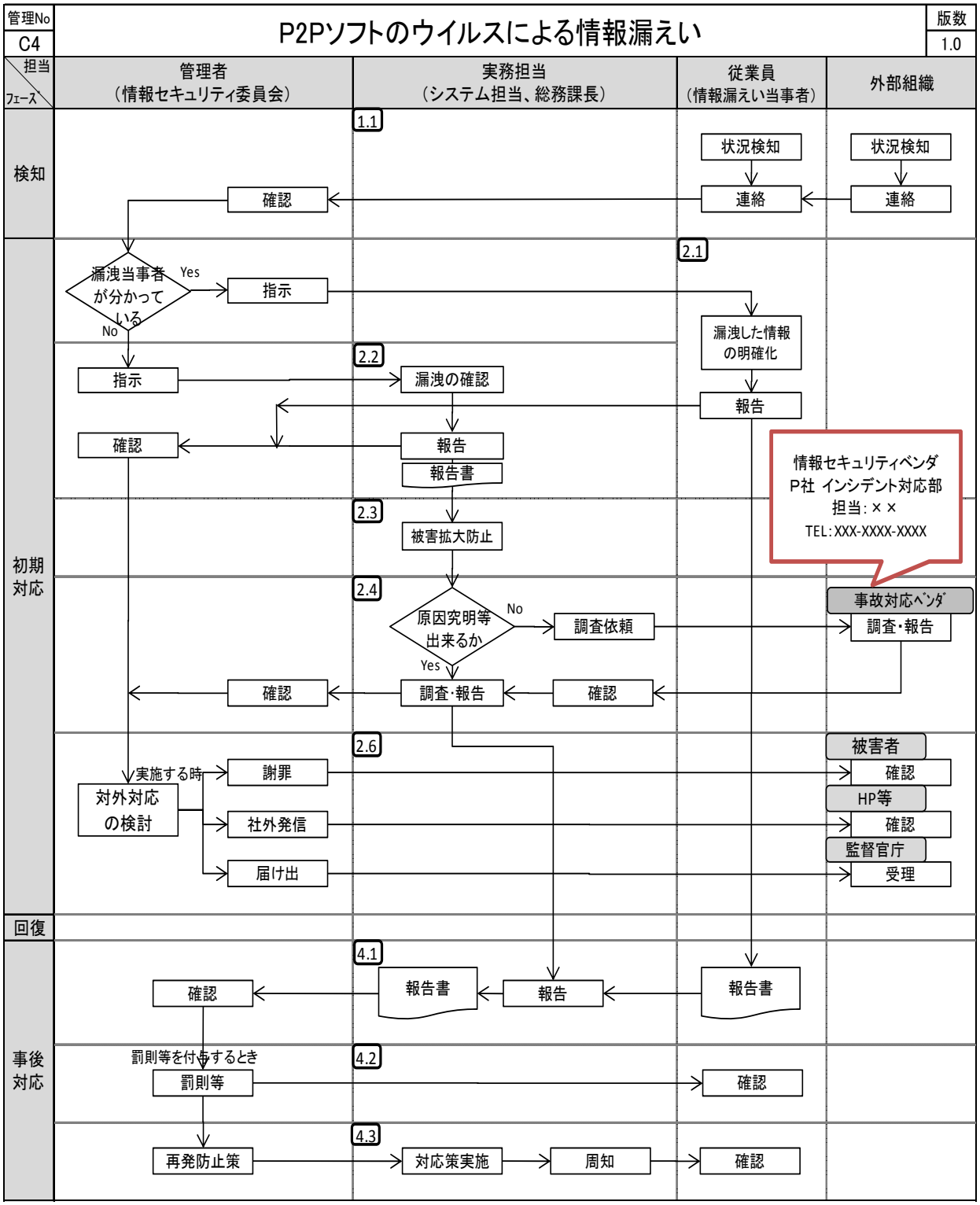


図 49　C4 フロー：　P2P ソフトのウイルスによる情報漏えい対応

C4解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】P2Pソフト（Winny、Share等）の暴露ウイルスに感染したことによりPC内の情報をネット上に公開された場合、漏えいした情報を確認し、当事者が不明な場合は探し出すことを検討し、対外対応について検討する。

【事例】

1 従業員が重要な情報を持ち帰り、自宅のPCがWinnyウイルスに感染していたことでPC内の情報が公開された。

2 会社のクライアントPCにShareをインストールし、これに暴露ウイルスが感染し、PC内の情報が公開された。

【対応】

1. 検知

1.1. 検知・連絡

①情報漏えい当事者：（自分で情報漏えいに気がついたとき）管理者に連絡する。

③顧客：情報が漏えいしているのに気付いたとき、組織に連絡がある（ことがある）。

④管理者：情報漏えいの連絡を確認する。

2. 初期対応

2.1. 当事者の初期対応

①管理者：漏えい当事者が分かっている場合、当事者に指示を出す。

②情報漏えい当事者：漏えいした情報にどのようなものがあったか明確にする。

③情報漏えい当事者：管理者に報告する。

2.2. 問題の切り分け

①管理者：情報漏えい当事者が不明な場合、実務担当に指示を出す。

情報漏えいの確認、漏えい元の調査を指示する。

②実務担当：情報漏えいか確認し、管理者に報告する。

連絡を受けた情報漏えい場所を確認し、本当に情報漏えいが発生しているか確認する。

「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。

③管理者：情報漏えいに関して、報告を受ける。

漏えいの状況についての報告を受け、漏えい当事者からも事実関係を把握する。

2.3. 被害拡大の防止

①実務担当：情報漏えいした情報・状況により、被害拡大が防止できる対策があれば実施する。

※現状難しい

2.4. 情報漏えい元、情報漏えい原因の調査

①実務担当：情報漏えいした情報・状況により、情報漏えい元、情報漏えい原因を調査する。

自社で原因究明ができない場合は、事故対応ベンダに調査依頼をする。

②実務担当：調査結果を管理者に報告する。

③管理者：調査報告を受ける。（場合により、対外対応の検討に取り入れる。）

2.6. 対外対応

①管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。

被害者（漏えいしてしまった顧客情報の顧客）に経緯を含め謝罪する。

社外発信（HP掲載）について検討し、必要に応じて実施する。

②管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。

届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復　（なし）

4. 事後対応

4.1. 報告

①漏えい当事者、実務担当：情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。

②管理者：報告書の受理とその他の事後対応（最終的な状況の社外発信等）。

4.2. 処罰等

①管理者：情報漏えいを起こした当事者に対し、処罰等を行うか検討する。

社則の処罰規定に基づき、処罰を行う。

4.3. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。

②実務担当：再発防止策を実施し、周知する。

図 50　C4 手順： P2P ソフトのウイルスによる情報漏えい対応

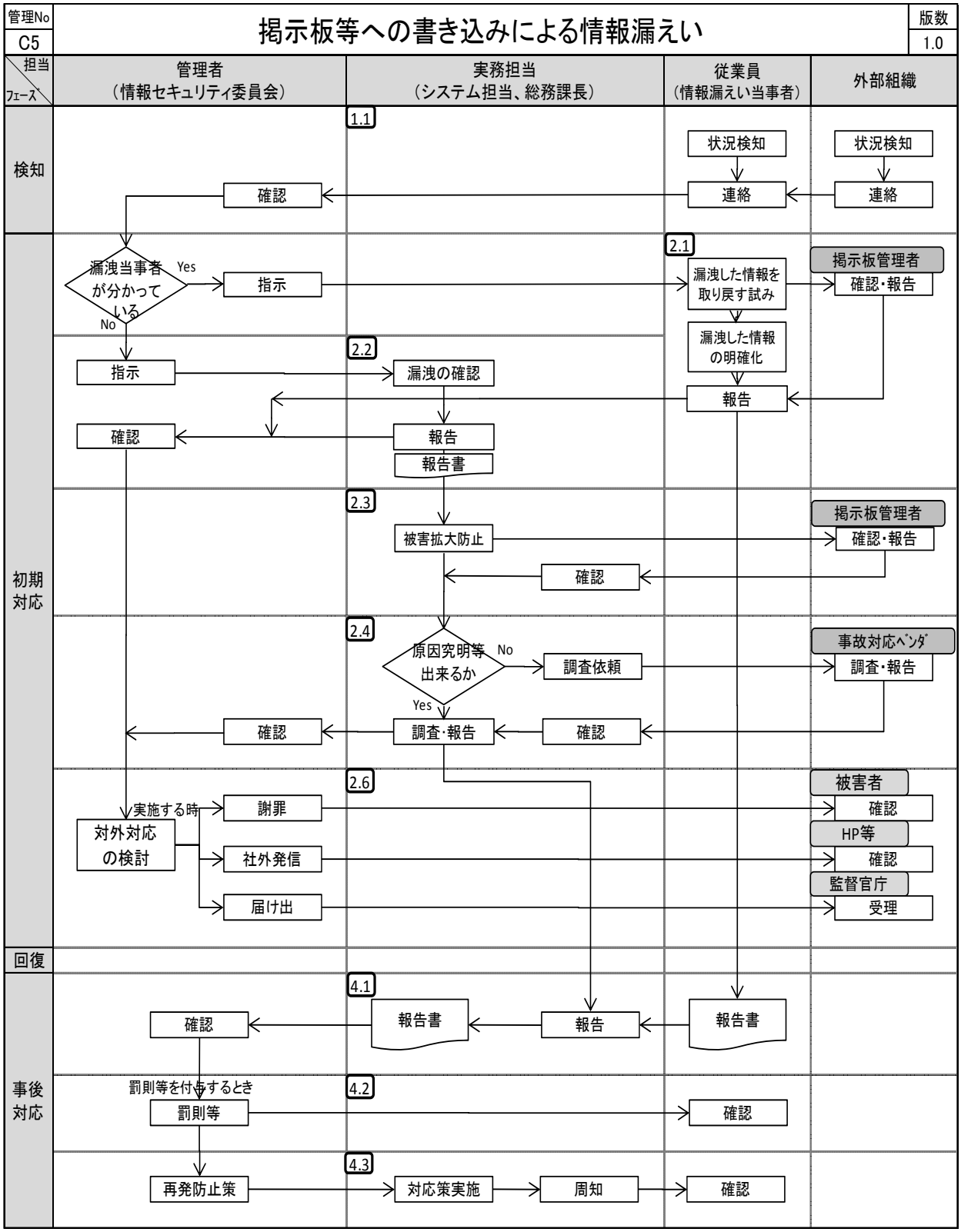


図 51　C5 フロー：掲示板等への書き込みによる情報漏えい対応

C5解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】従業員がインターネット上の掲示板やブログ等への書き込みにより、重要な情報が漏えいしたとき、漏えいした情報を確認し、当事者が不明な場合は探し出すことを検討し、対外対応について検討する。

【事例】

1 Webサイトの掲示板に会社の機密情報が書き込まれていた。
2 従業員が自分のブログの中で、自社の機密情報を暴露していた。

【対応】

1. 検知
   1.1. 検知・連絡
      ①情報漏えい当事者：（自分が情報漏えいをしてしまった場合）管理者に連絡する。
      ③顧客：情報が漏えいしているのに気付いたとき、組織に連絡がある（ことがある）。
      ④管理者：情報漏えいの連絡を確認する。

2. 初期対応
   2.1. 当事者の初期対応
      ①管理者：情報漏えい当事者が分かっている場合（紛失、盗難 等）、当事者に指示を出す。
      ②情報漏えい当事者：掲示板管理者に登録したデータの削除依頼を実施。
      ③情報漏えい当事者：（情報の紛失等の場合）紛失した情報にどんなものがあったか明確にする。
      ④情報漏えい当事者：管理者に報告する。

   2.2. 問題の切り分け
      ①管理者：情報漏えい当事者が不明な場合、実務担当に指示を出す。
         情報漏えいの確認、漏えい元の調査を指示する。
      ②実務担当：情報漏えいか確認し、管理者に報告する。
         連絡を受けた情報漏えい場所を確認し、本当に情報漏えいが発生しているか確認する。
         「情報セキュリティ事故発生報告書」を起票し、状況を記入。これをもとに管理者に報告する。
      ③管理者：情報漏えいに関して、報告を受ける
         漏えいの状況についての報告を受け、漏えい当事者からも事実関係を把握する。

   2.3. 被害拡大の防止
      ①実務担当：情報漏えいした情報・状況により、被害拡大が防止できる対策があれば実施する。
         掲示板管理者に登録したデータの削除依頼を実施する。

   2.4. 情報漏えい元、情報漏えい原因の調査
      ①実務担当：情報漏えいした情報・状況により、情報漏えい元、情報漏えい原因を調査する。
         自社で原因究明ができない場合は、事故対応ベンダに調査依頼をする。
      ②実務担当：調査結果を管理者に報告する。
      ③管理者：調査報告を受ける。（場合により、対外対応の検討に取り入れる。）

   2.6. 対外対応
      ①管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。
         被害者（漏えいしてしまった顧客情報の顧客）に経緯を含め謝罪する。
         社外発信（HP掲載）について検討し、必要に応じて実施する。
      ②管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。
         届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復　（なし）

4. 事後対応
   4.1. 報告
      ①漏えい当事者、実務担当：情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。
      ②管理者：報告書の受理とその他の事後対応（最終的な状況の社外発信等）。
   4.2. 処罰等
      ①管理者：情報漏えいを起こした当事者に対し、処罰等を行うか検討する。
         社則の処罰規定に基づき、処罰を行う。
   4.3. 再発防止
      ①管理者：報告書等を元に、再発防止策を検討する。
      ②実務担当：再発防止策を実施し、周知する。

図 52　C5 手順：掲示板等への書き込みによる情報漏えい対応

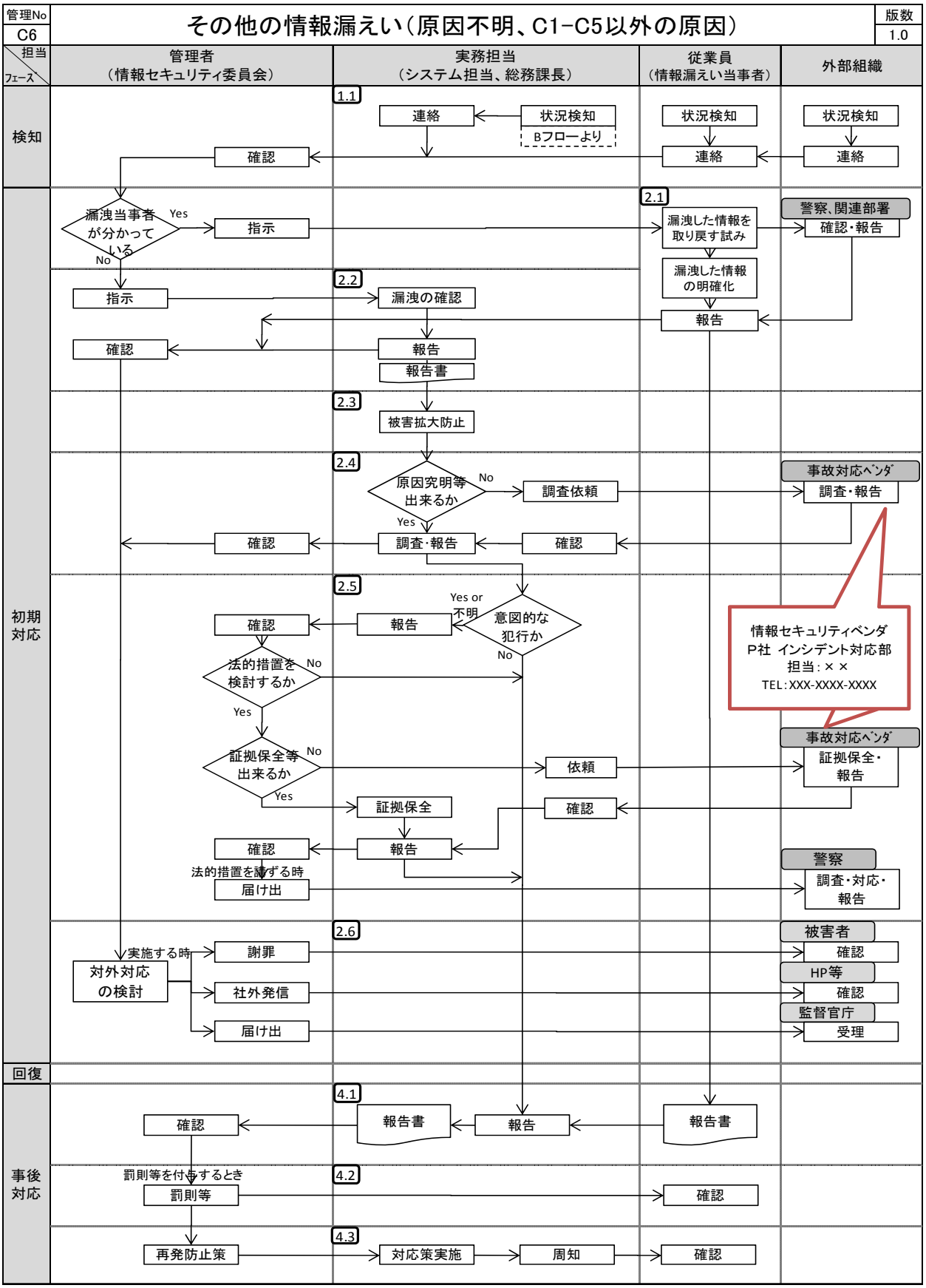


図 53　C6 フロー：その他の情報の漏えい対応（原因不明、C1-C5 以外の原因）

C6解説

【対象情報】　重要な情報（別途 重要な情報リスト用意）

【概要】重要な情報が漏えいしたときは、その事実を確認し被害拡大防止、原因調査を行う。また、意図的な犯行の場合は法的措置を検討し、顧客情報の場合は対外対応を検討する。

【事例】

1 従業員が顧客情報を盗み出し、競合会社や名簿販売業者に売っていた。
2 競合会社が、自社で開発中の商品とほとんど同様の商品を先に発売した。
3 名簿業者に組織の会員情報が売られていた。

【対応】

1. 検知

1.1. 検知・連絡

①情報漏えい当事者：（自分で情報漏えいに気がついたとき）管理者に連絡する。
②実務担当：情報漏えいを検知した場合、管理者に連絡する。（Bフロー対応時、情報漏えいが確認された場合も含む）
③顧客：情報が漏えいしているのに気付いたとき、組織に連絡がある（ことがある）。
④管理者：情報漏えいの連絡を確認する。

2. 初期対応

2.1. 当事者の初期対応

①管理者：情報漏えい当事者が分かっている場合（紛失、盗難 等）、当事者に指示を出す。
②情報漏えい当事者：漏えいした情報を取り戻す試みを実施する。
③情報漏えい当事者：漏えいした情報にどんなものがあったか明確にする。
④情報漏えい当事者：管理者に報告する。

2.2. 問題の切り分け

①管理者：情報漏えい当事者が不明な場合、実務担当に指示を出す。
②実務担当：情報漏えいか確認し、管理者に報告する。（情報漏えい時には「情報セキュリティ事故発生報告書」起票）
③管理者：情報漏えいに関して、報告を受ける。

2.3. 被害拡大の防止

①実務担当：情報漏えいした情報・状況により、被害拡大が防止できる対策があれば実施する。

2.4. 情報漏えい元、情報漏えい原因の調査

①実務担当：情報漏えいした情報・状況により、情報漏えい元、情報漏えい原因を調査する。
　自社で原因究明ができない場合は、事故対応ベンダに調査依頼をする。
②実務担当：調査結果を管理者に報告する。
③管理者：調査報告を受ける。（場合により、対外対応の検討に取り入れる。）

2.5. 意図的犯行時の対応

①実務担当：意図的な犯行による情報漏えいが疑われるときは、管理者に報告をする。
②管理者：意図的な犯行による情報漏えいが疑われるときは、法的措置を検討するか判断する。
③実務担当：意図的な犯行による情報漏えいが疑われるときは、証拠保全を行う。
　自社で証拠保全ができない場合は、事故対応ベンダに証拠保全を依頼する。
④管理者：調査報告を受け、法的措置を講ずるか判断する。
　法的措置を講ずる場合は、警察に証拠とともに届け出る。

2.6. 対外対応

①管理者：（漏えいした情報が顧客情報のとき）顧客への謝罪、HP等での社外発信を行うか検討する。
　被害者（顧客情報が漏えいしてしまった顧客）に謝罪する。
　社外発信（HP掲載）について検討し、必要に応じて実施する。
②管理者：（漏えいした情報が個人情報のとき）監督官庁への届出を行う。
　届出について検討し、必要に応じて経産省担当窓口に届け出る。

3. 回復　（なし）

4. 事後対応

4.1. 報告

①漏えい当事者、実務担当：情報セキュリティ事故の内容を「情報セキュリティ事故最終報告書」にまとめ、管理者に提出する。
②管理者：報告書の受理とその他の事後対応（最終的な状況の社外発信等）。

4.2. 処罰等

①管理者：情報漏えいを起こした当事者に対し、処罰等を行うか検討する。
　従業員の場合は、社則の処罰規定に基づき処罰を行い、委託業者の場合は、委託契約に基づき罰則を検討する。

4.3. 再発防止

①管理者：報告書等を元に、再発防止策を検討する。
②実務担当：再発防止策を実施し、周知する。

図 54　C6 手順：その他の情報漏えい対応（原因不明、C1-C5 以外原因）

【付録１】情報システム事故受付表

管理番号	受付日	報告者	事故種別	情報資産名	事故概要	受付者	影響範囲	対応要否	事故原因	事故対応者	対応概要	対応完了日	検証者	検証完了日	備考
0001	2011/4/1	報告者	A. 障害	ショッピングサイト	ショッピングサイトにアクセスできない。	受付者	5. 顧客	要	DDoS攻撃によりWebサーバが過負荷状態になったため。	事故対応者	特定の攻撃に対するパケットフィルタリングを実施。警察署へ被害届を提出し、攻撃者の追跡を依頼。	2011/4/1	検証者	2011/4/1	

情報セキュリティ事故発生報告書

件名			
報告者 （所属・氏名）		報告日	年　月　日

下記事項のうち判明していることを迅速に報告すること。

事故発見者 （※）		発見日時	年　月　日　時頃
事故発生場所		発生日時	年　月　日　時頃
事故の種類	□システム障害（公開システム・社内共有システム・個人システム）		
	□外部からの攻撃（ウイルス感染・不正アクセス・改ざん・その他）		
	□情報漏えい （紛失・盗難・誤送信・誤公開・管理ミス・内部犯行・その他） （意図的要因・非意図的要因）　（発災当事者判明・発災当事者不明）		
影響範囲	□顧客　□全社　□複数部署　□単一部署　□個人		

（※）情報漏えいの場合は、発災当時者を記載し不明な場合は不明と記載すること。

対象資産 （媒体、範囲、量）		
事故の内容		
想定される原因		
想定される二次被害等影響		
初期対応	暫定措置	
	現在の状況	
復旧時期の見込み		
対応実施者		

情報セキュリティ事故経過報告書

件名			
報告者 （所属・氏名）		報告日	年　月　日
前回報告者 （所属・氏名）		前回報告日	年　月　日
報告事由	□誤報訂正		
	□新規事項判明		
	□その他（　　）		
報告事項			

情報セキュリティ事故最終報告書

件名			
報告者 （所属・氏名）		報告日	年　　月　　日

事故の概要	
事故の原因	
事故対応の経緯	
事故対応後の結果	
最終的な被害状況	
事故対応における問題点	
再発防止策および実施計画	

【付録５】参考 URL 集

- IPA「中小企業の情報セキュリティ対策ガイドライン」
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html
- 中小企業庁「中小企業 BCP 策定運用指針」
  http://www.chusho.meti.go.jp/bcp/
- 警察庁「DoS/DDoS 対策について」
  http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf
- IPA「情報セキュリティ安心相談窓口」
  http://www.ipa.go.jp/security/anshin/
- 特定非営利活動法人デジタル・フォレンジック研究会「証拠保全ガイドライン　第１版」
  http://www.digitalforensic.jp/eximgs/100405gijutsu.pdf
- IPA「情報漏えい対策のしおり」
  http://www.ipa.go.jp/security/antivirus/documents/5_roei_v3_2.pdf
- 消費者庁「個人情報の保護」
  http://www.caa.go.jp/seikatsu/kojin/

情報セキュリティ事故対応ガイドブック
（初版第一刷）

平成２３年３月

著作・発行　情報セキュリティ大学院大学
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-14-1
＜URL＞http://www.iisec.ac.jp/