情報漏洩対応マニュアル（サンプル）

目的
このマニュアルは、情報漏洩が発生した際に被害を最小限に抑え、適切な対応を行うための指針を提供することを目的としています。

適用範囲
本マニュアルは、全従業員が対象となります。情報漏洩の兆候を発見した場合、直ちに以下の手順に従って行動してください。

---

1. 発見・報告

- 情報漏洩を発見、またはその可能性がある場合は、すぐに担当部署（IT部門）へ報告します。
- 報告時には、漏洩の詳細（日時、影響範囲、関係するファイルやデータ）を明確に伝えてください。

---

2. 初動対応

- 情報漏洩が確認された場合、担当部署は対策本部を設置し、応急措置を実施します。
    - 漏洩が発生した端末をネットワークから切断
    - 不正プログラムが発見された場合、すぐに隔離
    - サーバへのアクセス権限の見直しを実施
- 二次被害を防ぐため、該当端末やサーバの物理的隔離を行い、さらに詳しい調査が行える状態にします。

---

3. 調査

- 初動対応が完了した後、調査を進めます。
    - 「5W1H」に基づいて、何が、いつ、どこで、なぜ漏洩したのかを整理
    - 必要に応じて外部の専門機関と連携し、原因を特定

---

4. 通知・報告・公表

- 情報漏洩の対象者（取引先、顧客、従業員）に対して、速やかに通知を行います。
    - 個別通知が難しい場合は、Webサイトやメディアでの発表を検討
    - 監督機関（IPAや警察など）への報告を忘れずに実施

---

5. 抑制措置・復旧

- IDやパスワードが漏洩した場合は、該当アカウントを停止し、再発行を行います。
- 漏洩した情報の拡散を防ぐため、セキュリティ体制を強化し、システムの脆弱性を修正。
- 可能な限りバックアップを用いてデータ復旧を進めます。

---

6. 事後対応

- 再発防止策を策定し、全従業員に対して改めてセキュリティ教育を実施します。
    - 新たなセキュリティポリシーの導入
    - サーバールームの物理的な施錠管理やアクセス制限の見直し
    - 定期的なセキュリティチェックの実施
- 経営層への報告と、必要に応じた内部者への処分を行います。