情報セキュリティインシデント対応計画（体制と手順書）
適用日：2025 年 11 月 01 日

1. 目的と体制

情報セキュリティインシデント（情報漏えい、不正アクセス、マルウェア感染、サービスの停止など）が発生した際に、被害を最小限に食い止め、迅速に復旧し、お客様や取引先、関係機関に対して適切な説明責任を果たすための体制と手順を定める。

1-2. インシデント対応体制（CSIRT/個人事業主版）

役割	担当者	連絡先/備考
インシデント対応責任者（IRL: Incident Response Leader）	竹内葵	全対応の最終決定と外部報告の窓口となる
技術担当者	竹内葵	技術的な調査、隔離、復旧措置を担当
対外連絡担当者	竹内葵	顧客、取引先、警察、弁護士などへの連絡調整を担当

1-3. 連絡先リスト（事前に準備）

項目	連絡先/担当者	備考
顧問弁護士		法的判断、賠償責任、外部公表文の確認など
サイバー保険会社		事故報告、専門業者（フォレンジック）の手配など
警察（サイバー犯罪相談窓口）		不正アクセス、犯罪行為の疑いがある場合
取引先/主要顧客		契約上の報告義務がある場合を想定
利用サービス/プロバイダ		クラウドサービスやホスティングサービスで事故が発生した場合

2. インシデント対応手順

インシデントが発生した場合、以下の 6 つのステップで対応を実施する。

ステップ 1：検知と初動対応（最も重要）

1　異常の検知: マルウェア感染の警告、システムログの異常、顧客からの情報漏えい指

摘など、異常の発生を認知する。
2　状況確認: 発生時刻、影響範囲（どの PC/サーバーか、どの情報か)、具体的な事象（データが消えた、見覚えのない通信があるなど）を速やかに記録する。
3　隔離（封じ込め）:

- 感染した PC/サーバーをネットワークから即座に切断する（LAN ケーブルを抜く、Wi-Fi を切る)。
- 不正アクセスを受けたアカウントのパスワードを直ちにリセットする。
- 隔離が必要な機器の電源は、フォレンジック調査の可能性があるため、原則として切らない。

ステップ 2：被害状況の調査と分析（原因特定）
1　フォレンジック調査: 必要に応じて、サイバー保険会社を通じて**専門の調査会社（フォレンジック）**を手配し、不正アクセスの経路、侵入された期間、窃取された情報の種類と量を特定する。
2　ログ分析: サーバー、OS、ネットワーク機器、セキュリティソフトのログを収集し、根本原因を特定する。
3　影響範囲の確定: どの顧客情報、機密情報が影響を受けたか、具体的な件数と内容を確定させる。

ステップ 3：復旧措置
1　根本原因の排除: 不正アクセスの経路やマルウェアを完全に排除する。
2　セキュリティ強化: 脆弱性へのパッチ適用、設定の強化、アクセス権限の見直しなど、再発防止のための措置を実施する。
3　データ復旧: 隔離措置により影響を受けなかったバックアップデータを用いて、システムやデータを復旧させる。

ステップ 4：対外連絡と報告（被害状況の確定後）
1　社外への報告:

- 取引先・顧客: 契約上の義務や信義に基づき、影響を受けた可能性がある範囲を速やかに報告する。この際、事実に基づかない推測は控える。
- 関係機関: 個人情報保護法に基づく重大な漏えい事態の場合、個人情報保護委員会に報告を行う。犯罪性が疑われる場合は警察に相談する。
- 保険会社: サイバー保険の請求に必要な手続きを行う。

2　**公表:** 必要に応じて、ウェブサイトなどで**公表文**を作成し、事故の経緯、対応状況、再発防止策を公表する（弁護士と相談の上、内容を確定)。

ステップ 5：再発防止策の策定と実施

1　原因分析: 調査結果に基づき、なぜインシデントが発生したのか（例：パスワードの管理不備、ソフトの更新遅れ）を明確にする。

2　再発防止策の実施: 根本原因に対して、技術的・組織的な対策（例：二要素認証の義務化、セキュリティ研修の実施）を策定し、実行する。

3　ポリシーの見直し: 既存の情報セキュリティポリシーを本インシデントの教訓を反映させて見直し、改定する。

ステップ 6：記録と完了

1　記録の保管: インシデント発生から完了までの全対応記録（ログ、調査報告書、対外連絡文書など）を一定期間保管する。

2　レビュー: 対応プロセス全体を振り返り、対応の有効性と改善点を確認する。