取扱注意

作成日　　年　月　日

[redacted]御中

# 情報セキュリティ診断報告書

当報告書は貴社にご記入いただいたヒアリングシートに基づいて作成しています。ヒアリングシートは弊社のこれまでの経験を基に作成しており、簡単な質問で評価ができるよう工夫したものですが、ヒアリングシートで触れていない範囲（一般的な施設のリスク）やより専門的な内容につきまして、十分な評価ができない場合もございますのでご了承ください。また、当報告書の記載内容は、貴社のセキュリティ管理上の重要事項が含まれますので、管理者以外の方への開示は避けるなど、取扱には十分ご注意ください。

## 1. 総合評価

判定ランク

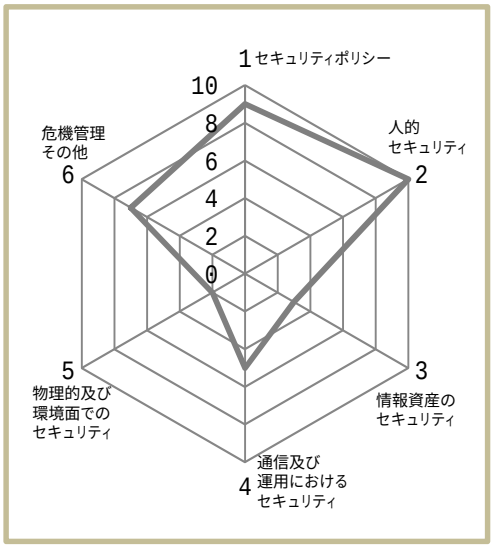
**B**

基本的なセキュリティ対策は整備されつつありますが、情報漏えい等に関するリスクは潜在しています。情報漏えい等の事故は、セキュリティ対策の弱い箇所が1つでも存在するとその箇所から発生する可能性があります。セキュリティが対策が脆弱な部分を中心に対策を実施し、継続的な見直しを行いながらセキュリティの維持・向上に取り組んでください。また、そのように万全のセキュリティ対策を実施していても、情報漏えい事故が起こらないとは限りません。万一事故が発生した際の備えとして、貴社が保有している情報資産の価値及び情報漏えいが発生した際に第三者に与える影響を考慮し、適切な賠償責任保険の加入をご検討ください。

判定ランクの説明
A：全体的にセキュリティ対策は整備されています。今後も継続的に見直しを実施し現状の維持と更なる向上に努めてください。
B：基本的なセキュリティ対策が整いつつありますが一部脆弱性が見受けられます。脆弱性の洗い出しを行い対策を実施してください。
C：セキュリティ対策の弱い部分が見られます。改めて詳細なリスク評価を行いそれに応じたセキュリティ対策をお勧めします。
D：全体的にセキュリティ対策が低いレベルにあり、危険な状態といえます。リスク対策の全体的な底上げが必要です。
E：セキュリティ対策への取組みがほとんどできていません。情報漏えいなどの事故が発生する危険が非常に高い状況で早急な対策が必要です。

## 2. 各項目評価

日本工業規格であるJIS Q27002（情報セキュリティマネジメントの実践のための規範）を基に情報漏えいを防止するためのセキュリティ対策の実施状況を以下の6つのカテゴリーで診断しています。




**1.セキュリティポリシー**
企業がセキュリティに対する取組方針を定めることは企業全体の運営に影響する非常に重要なポイントです。
（例：セキュリティポリシーの策定や監査体制の整備の有無）

**2.人的セキュリティ**
情報資産を守るには、すべての役職員がセキュリティに関する高い意識を持つことが重要です。
（例：従業員教育や誓約書の取り付けの有無等）

**3.情報資産のセキュリティ**
企業にとって重要な情報資産に対して技術的なセキュリティ対策を実施することは、不測の事態への備えになります。
（例：社外持ち出しデータの暗号化やパスワード設定の有無）

**4.通信及び運用におけるセキュリティ**
情報資産が最も危険にさらされる通信経路のセキュリティ強化のため、データ通信及び情報システムの運用面の対策が極めて重要です。
（例：ウィルス対策ソフトやOSの最新版導入の有無）

**5.物理的及び環境面でのセキュリティ**
情報システムの設備環境を整備するためのハード面の対策は、
ソフト面のセキュリティ対策の前提となる重要なポイントです。
（例：サーバールームの入退室管理の有無）

**6.危機管理その他**
完璧なセキュリティ対策はありません。不測の事態に遭遇した場合、迅速に対応することが被害を最小限にします。
（例：災害時のデータバックアップの有無）

## 3. セキュリティ対策のご提案

貴社にご記入いただいたヒアリングシートに基づき診断した結果、情報セキュリティ対策の更なる向上を図る上で重要と思われる3カテゴリーにつきまして、コメントを記載しました。今後の情報セキュリティ対策のご参考にしてください

### （1）情報資産のセキュリティ

・情報の取扱い（含む廃棄処理）の外部委託に関する管理強化
情報の取扱いや廃棄処理について、外部企業に委託している場合は、その取扱いに注意が必要です。外部委託する場合も、その管理責任は委託する側にありますので、万一委託先で漏洩事故が発生した場合には、委託元としての責任が問われることがあります。

・外部委託（受託）における機密保持・再委託禁止などの取り決め事項の整備推進
外部委託や受託の際に、機密保持や再委託の禁止など、十分な注意をした上で取り決め事項を決定する必要があります。万一の事故を未然に防ぐため、外部委託先との責任範囲を明確にし、外部委託先の業務を適時監査できるように契約上明記しておくことが必要です。

（事例）
システム開発業務を委託していた会社のアルバイトが個人情報を盗み、名簿業者に売却するという事故が発生しています。裁判の結果、委託元にもその責任が問われ損害賠償の支払いを命じられたケースがあります。

### （2）通信及び運用におけるセキュリティ

・機密情報に対するアクセス権限の制限強化
情報は必要な人が必要な時にだけアクセスできるようにすることがアクセス制御の基本的な考え方です。便利さとセキュリティは相反する概念といえますが、アクセス制御はセキュリティレベルを高めるためには有効な手段です。
機密情報に対するアクセス制御について、今一度ご確認ください。

・電子メールの暗号化推進
電子メールは、「はがき」と同様に、受信者の手元に届くまでの間に、第三者に内容を見られてしまう可能性があります。 そのため「重要な情報は電子メールで送らない」などの社内ルールを策定するなどの対策が必要です。電子メールのフィルタリングや暗号化が不十分な場合はご注意ください。

（事例）
電子メールの送信先を間違えたことによる個人情報の漏洩事故が発生しています。
電子メールを暗号化することで、そのような場合の情報漏洩を防止することができます。

### （3）物理的および環境面でのセキュリティ

・サーバー保管室等の施錠管理・入退室制限体制の整備強化
サーバー保管室等は通常無人であるため、施錠管理や入退室管理が不十分であると情報漏洩の危険性がきわめて高くなります。サーバー保管室や情報保管室など重要情報が保管されている場所は必ず施錠し、入退室が可能な人の制限および入退室記録を整備するなどの対策が必要です。

・再利用を不可能にする情報廃棄の徹底と廃棄記録による管理の推進
情報を活用している時点では、それが重要情報であるとの認識をもって取り扱いますが、廃棄の際にはその認識が薄れる可能性があります。情報の廃棄時には破壊・裁断・溶解などにより再利用ができないようにしたうえ、廃棄記録を保存することが重要です。

（アドバイス）
サーバー室等は、重要な情報が保存されているにもかかわらず、人目が少ないため第三者の侵入を発見し難い場所でもあります。そのためにも施錠管理・入退室記録などはセキュリティを保つために重要といえます。