

情報セキュリティ方針

1. 情報セキュリティ基本方針

昨今情報漏洩などのセキュリティ事件が相次いでおりますが、株式会社常光（以下、「当社」という）は、情報資産の重要性を認識し、情報セキュリティ対策を経営課題の最重要項目として捉え、情報セキュリティマネジメントを実施するために、情報セキュリティポリシーを策定するとともに、組織全体で情報セキュリティポリシーを遵守していくことに努めます。

2. 情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、当社のすべての情報資産に関連する人的・物理的・環境的リソースも含むものとする。

3. 情報セキュリティポリシーの適用者

当社の役員・従業員（正社員、パート社員、契約社員）など、当社の情報資産を利用するすべての者に適用する。

3. 1 経営陣の責務

経営陣は、情報セキュリティポリシーへの支持・支援を表明し、率先して情報セキュリティマネジメントを推進しなければならない。

3. 2 従業員の責務

従業員には、当社の情報資産の使用を認めるが、それは円滑な業務遂行の手段としての使用を認めることであり、私的利用を許可するものではない。従業員は情報資産を扱う上で、企業利益の維持・向上および顧客満足のために、情報セキュリティポリシーに同意し、遵守しなければならない。またこれに違反した者は、その結果について責任を負わなければならない。

3. 3 外部委託業者に対する対応

情報セキュリティポリシーの適用範囲内で行う作業を、外部委託業者に依頼する場合には、契約上で遵守すべきセキュリティ管理策を明確にし、セキュリティ事故時の責任に関しても明確にしなければならない。

4. 情報セキュリティポリシーの構成と位置付け

情報セキュリティポリシーは、「情報セキュリティ方針」、「情報セキュリティ対策標準」、「情報セキュリティ実施手順書」の3つの階層に分けて策定・管理される文書とする。

4. 1 情報セキュリティ方針

情報セキュリティ方針（以下、「方針」とする）は、情報セキュリティポリシーの最上位に位置する文書である。この文書は、当社の情報セキュリティマネジメントにおける方針を記述したものである。この文書に基づいて下層の文書を策定する。

4. 2 情報セキュリティ対策標準

情報セキュリティ対策標準（以下、「対策標準」とする）は、方針の下層に位置する文書である。この文書は、次に掲げる項目に分類される。

- ①情報セキュリティの運営基準
- ②情報の取り扱い基準
- ③情報システムの運用基準
- ④情報システムの開発・導入基準
- ⑤物理的セキュリティ対策基準
- ⑥外部委託基準
- ⑦情報セキュリティ監査基準
- ⑧情報資産の取り扱いに関わる法令等の遵守

4. 3 情報セキュリティ実施手順書

情報セキュリティ実施手順書（以下、「実施手順書」とする）は、対策標準の下層に位置する文書である。この文書は、対策標準で記述された文書をより具体的に明記する必要がある場合に作成する。

4. 4 既存の規程との関連

方針は、当社の社内規程・就業規則と同等の位置付けの文書とする。よって、この文書の改廃は所定の規程に準じて行うものとする。

4. 5 その他関連法規

情報セキュリティポリシーは、関連法規と照らして違反することの無いようにしなければならない。また、必要に応じて関連規格に遵守した管理策を導入しなければならない。

5. 情報セキュリティポリシーの公開対象者

方針は、従業員すべてを公開対象とする。したがって、一般には公表しない機密情報として取り扱わなければならない。以下、方針以外の文書は機密情報である。

6. 情報セキュリティポリシーの公開

情報セキュリティポリシーは機密文書として扱い、原則として、社外に公開してはならない。ただし、公開しなければ業務を遂行できない場合には、機密保持契約を締結した上で、公開を認める場合がある。

1 4. 執行期日

本方針は、2015年10月7日に取締役会にて承認され、2015年10月16日より施行する。

【参考文献】 情報セキュリティポリシーサンプル(0.92a 版)
NPO 日本ネットワークセキュリティ協会(JNSA) <http://www.jnsa.org/>

【実 施】 2015年10月16日

【改 定】