情報セキュリティポリシー

2017 年 11 月 1 日策定

目　次

株式会社軽井沢 IT 経営センター

1	組織的対策（基本方針）
適用範囲	当社全体

1. 情報セキュリティ基本方針

情報セキュリティ基本方針を以下のとおり定める。

＜情報セキュリティ基本方針＞

当社は IT 事業を中核としてお客様のニーズに応えてきました。今後も、お客様にご満足いただける製品・サービスを提供するために、高度情報化社会における情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ基本方針を定め、当社の情報セキュリティに対する取り組みの指針といたします。

1. 社内体制および情報セキュリティポリシーの整備

当社は、セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を社内の正式な規則として定めます。

2. リーダーシップにおける責任および継続的改善

当社の経営者は、本方針の遵守により、当社及びお客様の情報資産が適切に管理されるよう主導します。

3. 法令、契約上の要求事項の遵守

当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規範及びお客様との契約上のセキュリティ要求事項を遵守します。

4. 従業員の取組み

当社の従業員は、情報セキュリティの維持及び改善のために必要とされ知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

5. 違反及び事故への対応

当社は、情報セキュリティに関わる法令、規制、規範及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

2018 年 4 月 1 日

株式会社　軽井沢 IT 経営センター

代表取締役社長　高見　康昭

2. 個人番号及び特定個人情報の適正な取扱いに関する基本方針

個人番号及び特定個人情報の適正な取扱いに関する基本方針を以下のとおり定める。

＜個人番号及び特定個人情報の適正な取扱いに関する基本方針＞

1.関係法令・ガイドライン等の遵守

当社は、個人番号及び特定個人情報（以下「特定個人情報等」といいます。）の取り扱いに関し､「行政手続における特定の個人を識別するための番号の利用等に関する法律」(以下「マイナンバー法」といいます。）及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編)」、並びに「個人情報の保護に関する法律」(以下「個人情報保護法」といいます。）及び各省庁のガイドラインを遵守します。

2.利用目的

当社は、提供を受けた特定個人情報等を、以下の目的で利用します。

(1) 取引先様の特定個人情報等

・報酬、料金、契約金及び賞金に関する支払調書作成事務

(2) 株主様の特定個人情報等

・配当及び剰余金の分配に関する支払調書作成事務

(3) 当社の従業員等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出、申請・請求事務

・雇用保険・労災保険届出、申請・請求、証明書作成事務

(4) 当社従業員等の配偶者及び親族等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出事務

3.安全管理措置に関する事項

当社は、特定個人情報等の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために、別途「情報セキュリティポリシー４　マイナンバー対応」を定め、これを遵守します。

4.委託の取り扱い

当社は、特定個人情報等の取り扱いを第三者に委託することがあります。この場合、当社は、マイナンバー法及び個人情報保護法に従って、委託先に対する必要かつ適切な監督を行います。

5.継続的改善

当社は、特定個人情報等の取り扱いを継続的に改善するよう努めます。

6.特定個人情報等の開示

当社は、本人又はその代理人から、当該特定個人情報等に係る保有個人データの開示の求めがあったときは、次の各号の場合を除き、遅滞なく回答します。

・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合
・法令に違反することとなる場合

特定個人情報等の開示に関するお問合せ、および質問苦情等は下記までお願いいたします。

軽井沢 IT 経営センター

https://www.karuizawaitkeiei.jp/

2018 年 4 月 1 日

株式会社　軽井沢 IT 経営センター

代表取締役社長　高見　康昭

1	組織的対策
適用範囲	当社全体

1.情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、１２社内体制図の組織を設置する。

2.情報セキュリティ取組みの点検

情報セキュリティポリシーの実施状況について、適時点検を行う。

、点検結果に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- ➢情報セキュリティポリシーが有効に実施されていない場合、その原因の特定と改善
- ➢情報セキュリティポリシーに定められたルールが、新たな脅威に対する対策として有効でない場合は、情報セキュリティポリシーの改訂
- ➢情報セキュリティポリシーに定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティポリシーの改訂

3.情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。

【専門機関】

- ➢独立行政法人情報処理推進機構（略称：IPA）

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

- ➢JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

- ➢一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

- ➢個人情報保護委員会

http://www.ppc.go.jp/

2	人的対策
適用範囲	全従業員（役員、社員、派遣社員、パート・アルバイトを含む）

1. 雇用条件

従業員を雇用する際には秘密保持契約を締結する。

2. 取締役及び従業員の責務

取締役及び従業員は、以下を遵守する。

●取締役及び従業員は、当社が営業秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。

●取締役及び従業員は、当社の情報セキュリティ方針及び関連規程を遵守する。違反時には懲戒処分の対象とする。

3. 雇用の終了

●取締役及び従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。

●取締役及び従業員は、在職中に知り得た当社の営業秘密もしくは業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

4. 情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を立案する。

対象者：全従業員、派遣社員、パート・アルバイト

テーマ：以下は必須とする。

- 情報セキュリティポリシーの説明（入社時、就業時）

➢

3	情報資産管理
適用範囲	当社事業に必要で価値がある情報及び個人情報

1. 情報資産の管理

1.1 情報資産の特定と重要度の評価

当社事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、情報資産の機密性における重要度は、以下の基準に従って評価する。

機密性 2：極秘	法律で安全管理措置が義務付けられている 守秘義務の対象として指定されている 漏えいすると取引先や顧客に大きな影響がある
機密性 1：社外秘	漏えいすると事業に大きな影響がある
機密性 0：公開	漏えいしても事業に影響はない

1.2 情報資産の分類と表示

情報資産の重要度は以下の方法で表示する。

表示がない場合には　機密性１と判断し、　機密性２の場合はファイル名などに【機密性 2】を明記する

1.3 情報資産の管理責任者

情報資産の管理責任者は、取締役社長とする。

2. 情報資産の社外持ち出し

情報資産を社外に持ち出す場合には、以下を実施する。

- 極秘の場合は代表取締役の許可を得る。
- 屋外でネットワークへ接続して社外秘又は極秘の情報資産を送受信する場合は、暗号化通信で行う。

3. 媒体の処分

3.1 媒体の廃棄

社外秘又は極秘の情報資産を廃棄する場合は以下の処分を行う。

書類・フィルム	細断
USB メモリ・HDD・CD・DVD	破壊

4.バックアップ

4.1 バックアップ取得対象

バックアップ対象機器については取締役社長が指定する

4.2 クラウドサービスを利用したバックアップ

クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、以下のサービス要件を確認し、導入する。

＜サービス要件＞

- サービス提供者のサービス利用約款、情報セキュリティ方針が、当社の情報セキュリティポリシーに適合している。
- 当社事業所がある地域で発生する震災、水害等の影響を受けない地域の施設であること。

4	マイナンバー対応
適用範囲	特定個人情報（マイナンバーを内容に含む個人情報）

1. 総則

1.1 目的

本規程は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の適正な取扱いの確保に関し必要な事項を定めることにより、当社の事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

1.2 定義

本項における用語の定義は、次に定めるところによる。

個人情報：

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できることとなるものを含む。）をいう。

個人番号：

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「マイナンバー法」という。）第 2 条 5 項が定める住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

特定個人情報：

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

個人情報データベース等：

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」（平成 15 年政令第 507 号。以下「個人情報保護法施行令」という。）で定めるものをいう。

個人情報ファイル：

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」で定めるものをいう。

特定個人情報ファイル：

個人番号をその内容に含む個人情報ファイルをいう。

個人データ：

個人情報データベース等を構成する個人情報をいう。

保有個人データ:
個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして個人情報保護法施行令で定めるものをいう。
個人番号関係事務:
マイナンバー法第 9 条第 3 項の規定により個人番号利用事務（行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が同条第 1 項又は第 2 項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務）に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。
個人情報取扱事業者:
個人情報データベース等を事業の用に供している者（国の機関、地方公共団体、独立行政法人等及び地方独立行政法人を除く。）をいう。
本人:
個人番号によって識別され、又は識別され得る特定の個人をいう。
従業員:
当社の組織内にあって直接間接に当社の指揮監督を受けて当社の業務に従事している者をいう。具体的には、従業員のほか、取締役、派遣社員等を含む。
1.3 当社の責務
マイナンバー法その他の個人情報保護に関する法令及びガイドライン等を遵守するとともに、実施するあらゆる事業を通じて特定個人情報等の保護に努めるものとする。

2. 特定個人情報等の取り扱い
2.1 利用目的の特定
●特定個人情報等を利用できる事務の範囲を、社会保障、税及び災害対策に関する特定の事務に限定するものとする。
●利用に当たっては前項で定めた事務の範囲の中から、具体的な利用目的を特定した上で、利用するものとする。
●特定した利用目的を超えて利用する必要が生じた場合には、当初の利用目的と相当の関連性を有すると合理的に認められる範囲内で利用目的を変更して、本人に通知を行い、変更後の利用目的の範囲内で利用するものとする。

2.2 取得に際しての利用目的の通知等
●特定個人情報等を取得した場合は、あらかじめその利用目的を通知又は公表している場合を除き、速やかに、その利用目的を本人に通知し、又は公表するものとする。

●前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式等で作られる記録を含む。）に記載された当該本人の特定個人情報等を取得する場合その他本人から直接書面に記載された当該本人の特定個人情報等を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

●前 2 項の規定は、次に掲げる場合については、適用しない。

⑴利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

⑵利用目的を本人に通知し、又は公表することにより当社の権利又は正当な利益を害するおそれがある場合

⑶国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき

⑷取得の状況からみて利用目的が明らかであると認められる場合

2.3 取得の制限

●特定個人情報等を取得するときは、適法かつ適正な方法で行うものとする。

●マイナンバー法第 19 条各号のいずれかに該当する場合を除き、他人の特定個人情報等を収集しないものとする。

2.4 個人番号の提供の求めの制限

マイナンバー法第19条各号に該当して特定個人情報の提供を受けることができる場合を除くほか、他人に対し、個人番号の提供を求めないものとする。

2.5 本人確認

本人又はその代理人から個人番号の提供を受けるときは、マイナンバー法第 16 条の規定に従い、本人確認を行うものとする。

2.6 利用目的外の利用の制限

●「2.1 利用目的の特定」の規定により特定された利用目的の達成に必要な範囲を超えて、特定個人情報等を取り扱わないものとする。

●合併その他の事由により他の法人等から事業を継承することに伴って特定個人情報等を取得した場合は、継承前における当該特定個人情報等の利用目的の達成に必要な範囲を超えて、当該特定個人情報等を取り扱わないものとする。

●前 2 項の規定にかかわらず、次の各号のいずれかに該当する場合には、「2.1 利用目的の特定」の規定により特定された利用目的の範囲を超えて特定個人情報等を取り扱うことがで

きるものとする。

(1)マイナンバー法第 9 条第 4 項の規定に基づく場合

(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意があり、又は本人の同意を得ることが困難であるとき

2.7 特定個人情報ファイルの作成の制限

マイナンバー法第 19 条 11 号から 14 号までのいずれかに該当して特定個人情報を提供し、又はその提供を受けることができる場合を除き、個人番号関係事務を処理するために必要な範囲を超えて特定個人情報ファイルを作成しないものとする。

2.8 特定個人情報等の保管

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を保管しないものとする。

2.9 データ内容の正確性の確保

「2.1 利用目的の特定」により特定された利用目的の達成に必要な範囲内において、特定個人情報等を正確かつ最新の内容に保つよう努めるものとする。

2.10 特定個人情報等の提供

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を提供しないものとする。

2.11 特定個人情報等の削除・廃棄

個人番号関係事務を処理する必要がなくなった場合で、かつ、所管法令において定められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除するものとする。ただし、その個人番号部分を復元できない程度にマスキング又は削除した場合には、保管を継続することができるものとする。

2.12 特定個人情報等を誤って収集した場合の措置

- 従業者は、誤って特定個人情報等の提供を受けた場合、自ら当該特定個人情報等を削除又は廃棄してはならず、速やかに「3.1 事務取扱担当者・責任者」に定める事務取扱責任者に報告しなければならない。
- 前項の報告を受けた際、「5.3.4 個人番号の削除、機器及び電子媒体等の廃棄」に従って、当該特定個人情報等をできるだけ速やかに削除又は廃棄したうえで、その記録を保存するものとする。

2.13 安全管理措置

特定個人情報等の取り扱いに関し、「4.委託先の監督」及び「5.安全管理措置」に定める安全管理措置を講じるものとする。

3. 組織及び体制

3.1 事務取扱担当者・責任者

●別途定めるとおり、特定個人情報等を取り扱う事務の範囲を明確化し、明確化した事務において取り扱う特定個人情報等の範囲を明確にしたうえで、当該事務に従事する従業員（以下「事務取扱担当者」という。）を明確にするものとする。

●別途定めるとおり、前項により定められた各事務における事務取扱責任者を明確にするものとする。

●事務取扱責任者は、次に掲げる業務を所管する。

(1)特定個人情報等の利用申請の承認及び記録等の管理

(2)特定個人情報等を取り扱う保管媒体の設置場所の指定及び変更の管理

(3)特定個人情報等の管理区分及び権限についての設定及び変更の管理

(4)特定個人情報等の取扱状況の把握

(5)委託先における特定個人情報等の取扱状況等の監督

(6)特定個人情報等の安全管理に関する教育・研修の実施

(7)特定個人情報等管理責任者に対する報告

(8)特定個人情報等の安全管理に関する規程の承認及び周知

(9)事務取扱責任者からの報告徴収及び助言・指導

(10)特定個人情報等の適正な取扱いに関する事務取扱担当者に対する教育・研修の企画

(11)その他特定個人情報等の安全管理に関する事項

3.2 苦情対応

●特定個人情報等の取扱いに関する苦情（以下「苦情」という。）の対応について必要な体制整備を行い、苦情があったときは、適切かつ迅速な処理に努めるものとする。

●苦情対応の責任者は、代表取締役社長とする。

3.3 従業員の義務

●当社の従業者又は従業員であった者は、業務上知り得た特定個人情報等の内容をみだりに他人に知らせたり、不当な目的に使用したりしてはならない。

●特定個人情報等の漏えい、滅失もしくは毀損の発生又は兆候を把握した従業員は、その旨を事務取扱責任者に報告するものとする。

●本規程に違反している事実又は兆候を把握した従業者は、その旨を事務取扱責任者に報告するものとする。

●事務取扱責任者は、前 3 項による報告の内容を調査し、本規程に違反する事実が判明した場合には遅滞なく代表取締役に報告するとともに、関係部門に適切な措置をとるよう指示するものとする。

4.委託の取扱い

4.1 委託

特定個人情報等の取扱いの全部又は一部を当社以外の者に委託するときは、委託先において、マイナンバー法に基づき当社が果たすべき安全管理措置と同等の措置が講じられるか否かについてあらかじめ確認したうえで、原則として委託契約において、特定個人情報等の安全管理について委託先が講ずべき措置を明らかにし、委託先における特定個人情報の取扱状況を把握するものとする。

4.2 再委託

委託先が特定個人情報等の取扱いの全部又は一部を再委託する場合には、当社の許諾を得るものとする。また、再委託が行われた場合、当社は、委託先が再委託先に対して必要かつ適切な監督を行っているかについて監督するものとする。

5.安全管理措置

特定個人情報等の漏えい、滅失又は毀損の防止その他の特定個人情報等の安全管理のために、以下に定める措置を講ずるものとする。

5.1 組織的安全管理措置

特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じる。

5.1.1 組織体制の整備

安全管理措置を講ずるために、「3. 組織及び体制」に従い、組織体制を整備する。

5.1.2 取扱状況を確認する手段の整備

本規程に基づく運用状況を確認するため、以下の項目をシステムログ又は利用実績として記録する。

・特定個人情報ファイルの利用・出力状況の記録
・書類・媒体等の持出しの記録
・特定個人情報ファイルの削除・廃棄記録

5.1.3 情報漏えい等事案に対応する体制の整備

情報漏えい等の事案の発生又は兆候を把握した場合には、事務取扱責任者は「情報セキュリティポリシー」に定める安全管理措置に従って対応を行う。

5.1.5 取扱状況の把握及び安全管理措置の見直し

特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組むため、事務取扱責任者が、毎年 1 回、取扱状況を点検し、安全管理措置を見直す。

5.2 人的安全管理措置

特定個人情報等の適正な取扱いのために、「情報セキュリティポリシー２　人的対策」に従い人的安全管理措置を講じる。

5.2.1 従業者の監督・教育

特定個人情報等の安全管理のために、従業者に対する必要かつ適切な監督・教育を行うものとする。

5.3 物理的安全管理措置

特定個人情報等の適正な取扱いのために、「情報セキュリティポリシー６　物理的対策」の物理的安全管理措置を講じる。

5.3.1 特定個人情報等を取り扱う領域の管理

特定個人情報ファイルを取り扱う情報システムを管理するセキュリティ領域（以下「レベル〇領域」という。）及び特定個人情報等を取り扱う事務を実施するセキュリティ領域（以下「レベル〇領域」という。）を明確にし、「情報セキュリティポリシー６　物理的対策」に定める安全管理措置を講ずる。

5.3.2ＩＴ機器及び電子媒体等の盗難等の防止

管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講ずる。

5.3.3 電子媒体等を持ち出す場合の漏えい等の防止

特定個人情報等が記録された電子媒体又は書類等を社外に持ち出す場合、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講じる。

5.3.4 個人番号の削除、機器及び電子媒体等の廃棄

個人番号を削除又は廃棄する際には、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置に従って、復元できない手段で削除又は廃棄する。

5.4 技術的安全管理措置

特定個人情報等の適正な取扱いのために、以下の技術的安全管理措置を講じる。

5.4.1 アクセス制御

事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。

5.4.2 アクセス者の識別と認証

特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証するものとする。

5.4.3 外部の不正アクセス等の防止

情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するため、「情報セキュリティポリシー７．ＩＴ機器利用」「情報セキュリティポリシー８　ＩＴ基盤運用管理」に定める安全管理措置を講じる。

5.4.4 情報漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するため、「情報セキュリティポリシー７　ＩＴ機器利用」に定める安全管理措置を講じる。

6.特定個人情報等の開示、訂正等、利用停止等

6.1 特定個人情報等の開示等

本人から、当該本人が識別される特定個人情報等に係る保有個人データについて、書面又は口頭により、その開示（当該本人が識別される特定個人情報等に係る保有個人データを保有していないときにその旨を知らせることを含む。以下同じ。）の申出があったときは、身分証明書等により本人であることを確認のうえ、開示をするものとする。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

⑴本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

⑵当社の事業の適正な実施に著しい支障を及ぼすおそれがある場合

⑶他の法令に違反することとなる場合

開示は、書面により行うものとする。ただし、開示の申出をした者の同意があるときは、書面以外の方法により開示をすることができる。

特定個人情報等に係る保有個人データの開示又は不開示の決定の通知は、本人に対し、遅滞なく行うものとする。

6.2 特定個人情報等の訂正等

●本人から、当該本人が識別される特定個人情報等に係る保有個人データの内容が事実でないという理由によって当該特定個人情報等に係る保有個人データの内容の訂正、追加又は削除（以下「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該特定個人情報等に係る保有個人データの内容の訂正等を行うものとする。

●前項の規定に基づき求められた特定個人情報等に係る保有個人データの内容の訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知するものとする。

●前項の通知を受けた者から、再度申出があったときは、前項と同様の処理を行うものとする。

●前第２項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、

その理由を説明するよう努めるものとする。

6.3 特定個人情報等の利用停止等

●本人から、当該本人が識別される特定個人情報等に係る保有個人データが「2.6 利用目的外の利用の制限」の規定に違反して取り扱われているという理由又は「2.3 取得の制限」の規定に違反して取得されたものであるという理由によって、当該特定個人情報等に係る保有個人データの利用の停止又は消去（以下「利用停止等」という。）を求められた場合、又は「2.10 特定個人情報等の提供」の規定に違反して第三者に提供されているという理由によって、当該特定個人情報等に係る保有個人データの第三者への提供の停止（以下「第三者提供の停止」という。）を求められた場合で、その求めに理由があることが判明したときは、遅滞なく、当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止を行うものとする。ただし、当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止に多額の費用を要する場合その他の利用停止等又は第三者提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

●前項の規定に基づき求められた特定個人情報等に係る保有個人データについて、利用停止等を行ったときもしくは利用停止等を行わない旨の決定をしたとき、又は第三者提供の停止を行ったときもしくは第三者提供の停止を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。

●前項第 3 項及び第 4 項は本項に準用する。

5	アクセス制御及び認証
適用範囲	情報資産の利用者及び情報処理施設

1. アクセス制御方針

社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。

●特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

2. 利用者の認証

社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。

●利用者の認証に用いるアカウントは、利用者 1 名につき 1 つを発行する。

●複数の利用者が共有するアカウントの発行を禁止する。

3. 利用者アカウントの登録

利用者の認証に用いるアカウントは、代表取締役の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

4. 利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。

5. パスワードの設定

利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。

●8 文字以上で英数字の混在したパスワードを用いる（IPA 準拠）

●他者に知られないようにする。

6. 従業員以外の者に対する利用者アカウントの発行

当社の取締役又は従業員以外の者にアカウントを発行する場合は、代表取締役又の承認を得たうえで、秘密保持契約を締結する。

6 物理的対策

適用範囲	情報処理設備が設置される領域

1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル 1 領域	応接スペース・倉庫
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	ー
侵入検知	ー
来客用名札	着用不要
火災対策	ー

2. 関連設備の管理

情報機器に関連する設備は以下を設置する。

・ サーバーは施錠付き専用ラックに収納する。

3. セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

・ 複合機、プリンタに原稿、印刷物を放置しない。

4. 搬入物の受け渡し

郵便物及び宅配便の受取り・受け渡しは、以下を介して行う。

＜本社＞

オフィス内にて実施する

7	Ｉ Ｔ機器利用
適用範囲	業務で利用する情報処理設備･機器

1. ソフトウェアの利用

1.1 標準ソフトウェア

業務に利用するパソコンにソフトウェアを導入する場合は、代表取締役社長の許可を得たうえで導入する。

1.2 ソフトウェアの利用制限

会社は、利用者の業務に不要な機能をあらかじめ取除いて提供する。従業員は、業務に不要なシステムユーティリティやインストールされているソフトウェアを利用しない。

1.3 ソフトウェアのアップデート

従業員は、業務で使用するソフトウェアを最新の状態で利用する。最新の状態で利用する方法は「6.2 ソフトウェアのアップデート方法」を参照のこと。

1.4 ウイルス対策ソフトウェアの利用

従業員は、パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。

2. Ｉ Ｔ機器の利用

従業員は、業務に利用するパソコン・タブレット・スマートフォンには、ログインパスワードを設定する。利用するときには以下を実行する。

3. クリアデスク・クリアスクリーン

3.1 クリアデスク

クリアデスクを徹底する。

・　利用時以外には机上に放置しない。

3.2 クリアスクリーン

離席時に以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。

●退社時又は使用しないときにはパソコンの電源を切る。

4.インターネットの利用

インターネットを利用する際には以下を遵守する。

4.1 ウェブ閲覧

・　不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。

。

4.2 オンラインサービス

従業員は、インターネットで提供されているサービスを業務で利用する場合は、代表取締役社長の許可を得る。

4.3ＳＮＳの利用

・　当社の業務に関わる情報の書き込みは行わない。

4.4 電子メールの利用

従業員は、業務で電子メールを利用する際には以下を実施する。

＜禁止事項＞

・　業務に支障をきたすおそれがある使用。

・　私用電子メールサーバーへの接続。

・　私用メールアドレスへの転送。

4.5 ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分に注意し、3 添付ファイルを開く、又はリンクを参照するなどしない。

メールのテーマ	①知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容 ·新聞社や出版社からの取材申込や講演依頼 ·就職活動に関する問い合わせや履歴書送付 ·製品やサービスに関する問い合わせ、クレーム ·アンケート調査 ②心当たりのないメールだが、興味をそそられる内容 ·議事録、演説原稿などの内部文書送付 ·VIP 訪問に関する情報 ③これまで届いたことがない公的機関からのお知らせ ·情報セキュリティに関する注意喚起 ·インフルエンザ等の感染症流行情報 ·災害情報

	④組織全体への案内 ·人事情報 ·新年度の事業方針 ·資料の再送、差替え ⑤心当たりのない、決裁や配送通知（英文の場合が多い） ·航空券の予約確認 ·荷物の配達通知 ⑥IDやパスワードなどの入力を要求するメール ·メールボックスの容量オーバーの警告 ·銀行からの登録情報確認
差出人のメール アドレス	①フリーメールアドレスから送信されている ②差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
メールの本文	①日本語の言い回しが不自然である ②日本語では使用されない漢字（繁体字、簡体字）が使われている ③実在する名称を一部に含むURL が記載されている ④表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる（HTML メールの場合） ⑤署名の内容が誤っている ·組織名や電話番号が実在しない ·電話番号がFAX 番号として記載されている
添付ファイル	①ファイルが添付されている ②実行形式ファイル(exe/scr/cplなど)が添付されている ③ショートカットファイル(lnkなど)が添付されている ④アイコンが偽装されている ·実行形式ファイルなのに文書ファイルやフォルダーのアイコンとなっている ⑤ファイル拡張子が偽装されている ·二重拡張子となっている ·ファイル拡張子の前に大量の空白文字が挿入されている ·ファイル名にRLO4が使用されている

5.私有ＩＴ機器・電子媒体の利用

従業員個人が所有するパソコン、タブレット、スマートフォン、携帯電話等のＩＴ機器及びUSB メモリ、HDD、CD 等の電子媒体の業務利用は禁止する。

8	ＩＴ基盤運用管理
適用範囲	情報資産を扱うサーバー・ネットワーク等のＩＴインフラ

1. 管理体制

ＩＴ基盤の運用にあたり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、システム管理者である代表取締役社長が決定する。

1.1 ＩＴ基盤の情報セキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること。

1.1.1 サーバー機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバー機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にサーバー機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、システム管理者の許可を得て導入する。

1.1.2 サーバー機器に導入するソフトウェア

ＩＴ基盤で利用するサーバー機器に導入するソフトウェアは、システム管理者がソフトウェアを選定する。新規にソフトウェアを導入する場合は、システム管理者の許可を得て導入する。

1.1.3 ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にネットワーク機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、システム管理者の許可を得て導入する。

2. ＩＴ基盤の運用

規定なし

3. クラウドサービスの導入

ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、「6.5 クラウドサービス情報セキュリティ対策評価基準」を参照のこと。

4.脅威や攻撃に関する情報の収集
システム管理者は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて社内で共有する。

5.廃棄・返却・譲渡
システム管理者は、ＩＴ基盤で利用した機器を返却、廃棄、譲渡を行う場合は、内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し代表取締役社長の承認を得たうえ返却、廃棄、譲渡を行う。内部記憶媒体の破壊又はデータの完全消去を、外部に委託する場合は、破壊又はデータの完全消去を実行したことの証明書を取得する。

6.ＩＴ基盤標準
ＩＴ基盤で利用する機器及びソフトウェアの情報セキュリティ要件と、それに基づく当社標準を以下とする。
6.1 サーバー機器情報セキュリティ要件
なし
6.2ＩＴ基盤標準ソフトウェア
なし
6.3 標準ネットワーク機器
なし
6.4 ネットワーク機器情報セキュリティ要件
なし
6.5 クラウドサービス情報セキュリティ対策評価基準
●サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が、処理しようとする情報資産の重要度に照らして適切であること。

9	システム開発及び保守
適用範囲	当社が独自に開発及び保守を行う情報システム

1. 情報システムの開発

独自システムは存在しない

10	委託管理
適用範囲	情報資産を取り扱う業務の委託

1. 委託先の評価（クラウドサービスの利用を除く）

1.1 委託先評価基準

社外秘又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、下記の評価基準に基づいて評価する。

（委託先評価基準）

社内管理体制	①経営者による情報セキュリティ基本方針がある
	②情報セキュリティ管理責任者を置いている
	③情報セキュリティ対策を定める規定等を整備している
	④情報セキュリティ事故に対する対応手順がある
従業員の監督	⑤全ての従業者に情報セキュリティに関する教育を実施している
	⑥従業者から秘密保持に関わる誓約書等を取得している
オフィス内のセキュリティ	⑦顧客の情報を扱う領域への入退室を管理している
	⑧顧客の情報の保管について施錠管理を実施している
情報機器・媒体の取扱い	⑨機器・媒体の盗難防止措置を講じている
	⑩媒体の無断複製、不正持出しを防止する措置を講じている
	⑪媒体の移送、受け渡し時の保護措置を講じている
	⑫媒体の安全な消去、廃棄の手順を整備している
サーバー・パソコン等の管理	⑬業務で使用するサーバー・パソコンのウイルス対策を行っている
	⑭業務で使用するサーバー・パソコンは利用者認証機能を設定している
	⑮業務で使用するサーバー・パソコンに利用制限等を設け管理している

1.2 委託先の選定

評価結果に基づき委託先を選定し、代表取締役社長の承認を得る。

1.3 委託契約の締結

委託契約書には、下記に関する事項を明記する。

①当社の社外秘又は極秘の情報資産及び個人情報の守秘義務

②再委託についての事項

③事故時の責任分担についての事項

④委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項

⑤情報セキュリティ対策の実施状況に関する監査の方法とその権限
⑥契約内容が遵守されない場合の措置
⑦事故発生時の報告方法

1.4 委託先の評価
委託開始後には、1.1 委託先評価基準の委託先における実施状況について定期的に評価する機会を設ける。委託先における評価基準の実施に関して不備又は変更が認められた場合は、双方協議のうえ、対処を検討し、書面で合意する。
＜委託先評価の方法＞
- 委託先事業所に訪問して現場を観察する。
- 委託先の管理責任者にインタビューする。
- 委託先に書面で確認事項を通知し、実施状況について報告してもらう。

1.5 再委託
当社が委託する業務を、委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求める。報告には必要に応じて以下の提供を含め、当社の「1.1 委託先評価基準」「1.3 委託契約の締結」「1.4 委託先の評価」と同等の管理を再委託先に求めていることを確認し、情報セキュリティ責任者の承認を得たうえで再委託を認める。
- 委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
- 再委託先の選定基準
- 再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその証書の写し

11	情報セキュリティインシデント対応 ならびに事業継続管理
適用範囲	情報セキュリティ事故対応及び事業継続管理

1. 対応体制

情報セキュリティインシデントが発生した際には以下の体制で対応する。

最高責任者	代表取締役
一次対応者	発見者又はシステム管理者

2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	対応者
3	●顧客、取引先、株主、等に影響が及ぶとき ●個人情報が漏えいしたとき	代表取締役
2	事業に影響が及ぶとき	代表取締役
1	従業員の業務遂行に影響が及ぶとき	システム管理者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき	システム管理者

3. インシデントの連絡及び報告

レベル 1 以上のインシデントが発生した場合、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

最終対応者	緊急連絡先
代表取締役	別途掲示する

4. 対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	社外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

4.1 漏えい・流出発生時の対応

事故レベル	対応手順	対応者
3	①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。 ②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。	代表取締役社長
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は漏えい先を調査し、インシデント対応責任者に報告する。 ③システム管理者は社内関係者に周知する。	代表取締役社長
1	※情報漏えい・流出は全て事故レベル 2 以上	

4.2 改ざん・消失・破壊・サービス停止発生時の対応

事故レベル	対応手順	対応者
3	①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。 代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。	代表取締役
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。	システム管理者

1	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行する。 ④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑤書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する ⑥システム管理者は原因対策を実施する	システム管理者
0	発見者は発見次第、発生可能性のあるインシデントと想定される被害をシステム管理者に報告する。	システム管理者

4.3 ウイルス感染時の初期対応

従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③ウイルス対策ソフトの定義ファイルを最新版に更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。

⑦システム管理者に報告する。

4.5 届出及び相談

システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。

＜届出・相談先＞

独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)

➢ウイルスの届出

https://www.ipa.go.jp/security/outline/todokede-j.html

TEL: 03-5978-7518

E-mail : virus@ipa.go.jp

➢不正アクセスに関する届出

E-Mail : crack@ipa.go.jp

FAX : 03-5978-7518

➢情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html
TEL:03-5978-7509
E-mail：anshin@ipa.go.jp

5.情報セキュリティインシデントによる事業中断と事業継続管理
代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以下を定める。
5.1 想定される情報セキュリティインシデント
　インシデントによる事業の中断を想定する。
5.2 復旧責任者及び関連連絡先
　代表取締役社長
5.3 事業継続計画

必要に応じて復旧から事業再開までの計画を立案する。

12	社内体制図
適用範囲	当社の情報セキュリティ管理

1. 情報セキュリティのための組織

「1. 組織的対策」における「2. 情報セキュリティのための組織」を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。