もっと、わくわく！
あなぶきグループ

情報セキュリティ方針

1．当社は，不動産に関するあらゆる事業活動を通じて得た，お客様及びお取引先の情報並びに当社が保有する情報資産を漏洩，改ざん，破壊，紛失，不正アクセス等の脅威から守り，リスクを最小限に抑え，適切に保護することが当社の事業継続に関わる最重要課題として位置づける。

2．当社は，個人情報の保護を含む情報資産の機密性・完全性・可用性の維持，向上に万全を期し，社会とお客様の信頼に応えるため，「情報セキュリティのための方針群」「情報セキュリティ個別方針」を定め実施する。

情報セキュリティ方針はホームページ上などに公開し，一般の人の直接請求に各拠点で応じられるようにする。

情報セキュリティ方針群

1．情報セキュリティ目的
当社は，情報資産及び情報セキュリティの管理を適切に実施し，情報セキュリティ事故を未然防止し，その低減を目指す。

2．適用範囲
本方針の適用範囲は当社の保有する情報資産すべてとする。また，当社の保有する情報資産を第三者との間で共用する場合は，管理する。

3．情報セキュリティマネジメントマニュアルの周知
本方針実行のため，情報セキュリティマネジメントマニュアルを策定し，これを当社のすべての役員，全従業員および協力会社に周知する。情報資産を取扱う社員等は情報セキュリティの重要性について共通認識を保ち，社内規程及び情報セキュリティに関する法令等を順守する。もし，違反した場合は当社就業規則の罰則規定が適用される。

4．情報セキュリティの管理体制
情報セキュリティを適切に管理するために情報セキュリティ委員会を組織し，経営者を委員長，情報セキュリティ管理責任者及び各部署より個人情報処理担当者・情報セキュリティ委員を選任する。

5．情報資産の保護と管理
保有する情報資産を保護するため，法令等のほか本方針をはじめとする情報セキュリティマネジメントマニュアルに従って情報資産を管理し，また，取り扱うとともに適正かつ合理的な以下の３つの情報セキュリティ対策を講じる。

①人的セキュリティ対策
情報セキュリティに関する責任権限を明確にし，情報セキュリティマネジメントマニュアルを理解し， 実践するための教育・訓練を計画的に実施する。

②物理的セキュリティ対策
安全領域への不正立入り，損傷・盗難等から保護するため，入退室管理など物理的対策を講じる。

③技術的及び運用面でのセキュリティ対策
情報資産への不正アクセス等から適切に保護するため，情報資産へのアクセス制御，コンピュータウイルス対策を実施する。

6．事業継続リスクへの取組み
事業上の情報セキュリティ要求事項並びに識別された法的および規制要求事項に適したリスクアセスメントの方法を特定し実施する。

7．個人情報の保護
個人情報について，当社の定める個人情報保護規程および情報セキュリティマネジメントマニュアルに従い保護するとともに，情報セキュリティ管理責任者を置き適正な管理を実施する。

8．情報セキュリティ監査の実施
情報セキュリティマネジメントマニュアルが周知徹底されていることと情報資産が適正に管理されていることを継続的に監視するために，定期的に情報セキュリティ監査を実施する。

9．情報セキュリティ侵害時の対応
万が一情報セキュリティ侵害事故が発生した場合，その被害を最小限にとどめ，迅速な復旧を行うとともに再発防止に努める。

10. 法令等の順守
当社のすべての役員，全従業員および協力会社社員は，情報セキュリティに関する法令，その他規範および契約等の要求事項を順守する。

11. 継続的改善
当社は，情報セキュリティ方針に従い，情報セキュリティ管理の仕組みを継続的に見直し，その改善に努める。

情報セキュリティ個別方針

以下の情報セキュリティ個別方針を適用宣言書，情報セキュリティガイダンス，手順書集等に明記し，定期的にレビューする。

◆モバイル機器の方針 (A.6.2.1)
業務でのモバイル機器の利用は、当社が利用許可を出したものに限る。
利用に際しての注意事項を下記に示す。
1. 屋外での物理的安全性
2. 第三者による覗き見
3. 置き忘れ、紛失
4. 置き引きや車上荒らしなどの盗難
5. 業務外での利用禁止

◆アクセス制御方針 (A.9.1.1)
1. 適用範囲外のエリアとのネットワーク分離を確実にする。
2. 許可された者のみ、アクセス権限を付与する。
3. 特権ユーザは限られたユーザのみに制限する。
4. アカウント及びアクセス権限の登録・変更・削除の手順を明確に定め、運用する。
5. 従事する業務及び取り扱う情報資産分類に応じ、アクセス範囲を制限する。
6. アカウントの利用状況を定期的にチェックし、正しく管理する。

◆暗号による管理策の利用方針 (A.10.1.1)
1. 情報機器に機密データを保管する必要がある場合は、機密データの漏えいを防ぐため、暗号化やアクセス制御等の対策を講じる。
2. 機密情報を電子メールの添付ファイルで送信する場合は、暗号化を行う。

◆クリアデスク・クリアスクリーン方針 (A.11.2.9)
1. 帰宅時や長時間、離席する時は書類や可搬媒体を放置しない。
2. 重要な書類や可搬媒体は、セキュリティが確保された場所に保管する。
3. スクリーンセーバーは 10 分以内で設定し、パスワードロックをかける。
4. 終業時や休日、長期休暇時及び３０分以上の離席時には PC の電源を切る。
5. 定期的に作業場所の整理整頓を実施し、思わぬ情報漏えいの危険を排除する。

◆情報のバックアップ方針 (A.12.3.1)
1. 指定したサーバのデータやシステム領域等について、定期的にバックアップを行う。
2. バックアップが正常に実施されている事を、定期的に確認する。
3. バックアップのデータは、事業継続の観点を考慮し、異なる施設にて保管する。
4. バックアップしたデータを、リストアする手順を確立する。

◆情報転送の方針 (A.13.2.1)
1. インターネット経由にて情報を転送する場合は、セキュアな通信方式にて行う。
2. 機密情報を電子メールの添付ファイルで送信する場合は、暗号化を行う。
3. 公共の場では、機密情報は話さない。携帯電話では周りに注意を払って利用する。
4. FAX を使用する場合、送信前の番号確認及び送信後の到達確認を行う。
5. 取り扱いに慎重を要する重要な情報の印刷物について、放置を禁ずる。

◆セキュリティに配慮した開発のための方針 (A.14.2.1)
セキュリティに配慮した開発を推進する。

◆供給者関係のための情報セキュリティ方針 (A.15.1.1)
供給者など外部の関係者が自社の情報資産を利用したり、アクセスしたりする場合には当社の情報セキュリティ方針に従うことに合意し、機密保持契約書などを締結する。

※() 内は ISO27001 適用宣言書の管理策番号

ISMS 第2版：2021年4月1日

情報セキュリティ方針群・情報セキュリティ個別方針は，文書化して，DesknetsＮＥＯに保存し，社員の利用が可能な状態に置くものとする。

情報セキュリティマネジメントシステム　経営者　新宮　章弘

ISMS-D-100-(1)