社外秘

情報セキュリティマニュアル

制定／改訂日：　2025 年 12 月 3 日
版数：　2.4
文書番号：　AB-標準-250502
管理部門：　情報セキュリティ管理

承認	確認	作成
塩田	井上	岡

株式会社　アグ・ブレインズ・システム

目次

1　適用範囲

株式会社　アグ・ブレインズ・システム（以下、当社と称す）は、ISO/IEC 27001:2022「情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項」（以下、ISO/IEC 27001 とする）に従って情報セキュリティマネジメントシステム（以下、ISMS とする）を構築する。
本マニュアルは、ISO/IEC 27001 の要求事項に従って、当社の ISMS を確立し、実施し、維持し、かつ、継続的に改善する手順について定める。

当社の ISMS の適用範囲は、以下の通りとし、本マニュアルの 4.3 に従って決定する。

a)　業務上の適用範囲

システムエンジニアアウトソーシング事業、人材派遣事業

b)　組織的適用範囲

【組織図】を参照。

c)　物理的適用範囲

本社：　株式会社アグ・ブレインズ・システム
東京都大田区本羽田３－１－２０

【フロアレイアウト図】を参照。

d)　インターフェースと依存関係

【ネットワーク構成図】を参照。

2　適用規格

2.1　適用規格

JIS Q 27001:2023（ISO/IEC 27001:2022/Amd.1:2024）情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項

2.2　引用規格

JIS Q 27000:2019（ISO/IEC 27000:2018）情報技術−セキュリティ技術−情報セキュリティマネジメントシステム−用語

3　用語及び定義

この文書で用いる主な用語及び定義は、JIS Q 27000:2019 による。

4　当社の状況

4.1　当社及びその状況の理解

当社は，組織の目的に関連し，かつ，その ISMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定する。
その際，気候変動が関連する課題かどうかを決定する。

外部状況、内部状況について以下のとおり整理する。

適用範囲	詳細内容	課題
外部	顧客	情報セキュリティリスクに対する要求
	協力会社	コンプライアンスの徹底と内部統制
内部	従業員	情報セキュリティに対する継続的な意識強化、及びお客様作業遵守事項の徹底
	全体	情報資産の適切な管理 ISMS 活動推進と、継続的な改善活動の実施 ペーパーレス/省力化

【情報セキュリティ管理者】は、年 1 回、 7 月に外部及び内部の課題を決定し、明確にする。

4.2　利害関係者のニーズ及び期待の理解

組織は，次の事項を決定しなければならない。
a)　ISMS に関連する利害関係者
b)　それらの利害関係者の，関連する要求事項(気候変動に関するものも含む)
c)　それらの要求事項のうち，ISMS を通して取り組むもの

利害関係者のニーズ及び期待について以下のとおり整理する。

適用範囲	利害関係者	情報セキュリティに関する要求事項
外部	顧客	顧客が要求する情報セキュリティ事項への対応
	協力会社	情報セキュリティ関連ルールの順守 『お客様対応作業及び企業秘密取り扱いの遵守事項』の徹底
内部	従業員	情報セキュリティ関連ルールの順守 『お客様対応作業及び企業秘密取り扱いの遵守事項』の徹底
	全体	ISMS 活動推進と、継続的な改善活動の実施 規格要求事項に基づく適切な内部監査の実施、運営

【情報セキュリティ管理者】は、年 1 回、 7 月に利害関係者のニーズ及び期待を決定し明確にする。

4.3 ISMS の適用範囲の決定

当社は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定する。

この適用範囲を決定するとき，当社は，次の事項を考慮する。

a) **4.1** に規定する外部及び内部の課題

b) **4.2** に規定する要求事項

c) 当社が実施する活動と他の組織が実施する活動との間のインターフェース及び依存関係

ISMS の適用範囲は，文書化した情報として利用可能な状態にする。

当社は、「4.1　当社及びその状況の理解」に規定する外部及び内部の課題、「4.2　利害関係者のニーズ及び期待の理解」に規定する利害関係者の要求事項、当社が実施する活動と他の組織が実施する活動との間のインターフェース及び依存関係を考慮して、ISMS の適用範囲を「1　適用範囲」に規定する。

4.4 ISMS

当社は，この規格の要求事項に従って，必要なプロセス及びそれらの相互作用を含む，ISMS を確立し，実施し，維持し，かつ，継続的に改善する。

5 リーダーシップ

5.1 リーダーシップ及びコミットメント

トップマネジメントは，次に示す事項によって，ISMS に関するリーダーシップ及びコミットメントを実証する。

a) 情報セキュリティ方針及び情報セキュリティ目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。
b) 組織のプロセスへの ISMS 要求事項の統合を確実にする。
c) ISMS に必要な資源が利用可能であることを確実にする。
d) 有効な情報セキュリティマネジメント及び ISMS 要求事項への適合の重要性を伝達する。
e) ISMS がその意図した成果を達成することを確実にする。
f) ISMS の有効性に寄与するよう人々を指揮し，支援する。
g) 継続的改善を促進する。
h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう，管理層の役割を支援する。

5.2 方針

トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立する。

a) 組織の目的に対して適切である。
b) 情報セキュリティ目的（**6.2** 参照）を含むか，又は情報セキュリティ目的の設定のための枠組みを示す。
c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。
d) ISMS の継続的改善へのコミットメントを含む。

情報セキュリティ方針は，次に示す事項を満たす。

e) 文書化した情報として利用可能である。
f) 組織内に伝達する。
g) 必要に応じて，利害関係者が入手可能である。

(1) 情報セキュリティ方針の内容

当社が策定した情報セキュリティ方針は、【情報セキュリティ基本方針】を文書化した情報として維持する。

(2) 情報セキュリティ方針の周知

情報セキュリティ方針は、ホームページ、教育での周知により、従業員やその他関係者に伝達し、周知させる。定期的な状況確認により順守状況を確認する。

また、社外へはホームページに掲載し、利害関係者が必要に応じて入手可能な状態にする。

(3) 情報セキュリティ方針の見直しのタイミング

トップマネジメントは、情報セキュリティ方針が、社内外の変化に対して引き続き有効であるかを確認するために、マネジメントレビュー、及び社内外で重大な変化があった場合に見直しを行い、必要に応じて改訂する。

5.3 当社の役割、責任及び権限

トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権限が割り当てられ，組織内に伝達されることを確実にする。 トップマネジメントは，次の事項に対して，責任及び権限を割り当てる。 a) ISMS が，この規格の要求事項に適合することを確実にする。 b) ISMS のパフォーマンスをトップマネジメントに報告する。

トップマネジメントは、情報セキュリティに関連する役割に対して責任及び権限を、【組織の役割・責務一覧】に明確にし、当社内に伝達する。

6 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

ISMS の計画を策定するとき，当社は，**4.1** に規定する課題及び **4.2** に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定する。

a) ISMS が，その意図した成果を達成できることを確実にする。
b) 望ましくない影響を防止又は低減する。
c) 継続的改善を達成する。

当社は，次の事項を計画する。

d) 上記によって決定したリスク及び機会に対処する活動
e) 次を行う方法
    1) その活動の ISMS プロセスへの統合及び実施
    2) その活動の有効性の評価

当社は、「4.1　当社及びその状況の理解」で規定した課題及び「4.2　利害関係者のニーズ及び期待の理解」で規定した要求事項を考慮し、「6.1.2　情報セキュリティリスクアセスメント」及び「6.1.3　情報セキュリティリスク対応計画」に規定されている手順に従って、【情報資産リスクアセスメント表】及び【情報セキュリティリスク対応計画表】【情報セキュリティ目的達成計画表】でリスク及び機会、並びにそれらに対処する活動を明確にする。

6.1.2 情報セキュリティリスクアセスメント

当社は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用する。

a) 次を含む情報セキュリティのリスク基準を確立し，維持する。
    1) リスク受容基準
    2) 情報セキュリティリスクアセスメントを実施するための基準
b) 繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。
c) 次によって情報セキュリティリスクを特定する。
    1) ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。
    2) これらのリスク所有者を特定する。
d) 次によって情報セキュリティリスクを分析する。
    1) **6.1.2 c) 1)** で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
    2) **6.1.2 c) 1)** で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
    3) リスクレベルを決定する。

e) 次によって情報セキュリティリスクを評価する。
   1) リスク分析の結果と 6.1.2 a) で確立したリスク基準とを比較する。
   2) リスク対応のために，分析したリスクの優先順位付けを行う。

当社は，情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持する。

当社は、以下の手順に基づいて、情報セキュリティリスクアセスメントのプロセスを実施し、【情報資産リスクアセスメント表】に記録する。

I. 情報資産の洗い出し

当社に存在する情報資産を洗い出し、以下の項目を特定又は決定する。

- 分類
- 保管形態
- 利用を許容する範囲
- 管理責任者
- リスク所有者
- 保管場所
- 保管期間
- 廃棄方法

II. 情報資産の評価

「I. 情報資産の洗い出し」にて洗い出した情報資産について、以下の区分に基づいて機密性（C)、完全性（I)、可用性（A）を定量的な評価を行い、以下の論理式に基づいて資産価値を算出する。

① 機密性（C：Confidentiality）

評価値	レベル	定義
1	公開	情報が漏洩しても、ビジネスへの影響はほとんどない
2	社外秘	情報が漏洩した場合、ビジネスへの影響はプロジェクト内、部署内で対応可能
3	極秘	情報が漏洩した場合、ビジネスへの影響は深刻かつ重大であり全社的信用の失墜につながる

② 完全性（I：Integrity）

評価値	レベル	定義
1	低	内容に誤りや改ざんがあっても影響は非常に少ない
2	中	内容に誤りや改ざんがあった場合、業務・サービスに影響を及ぼす
3	高	内容に誤りや改ざんがあった場合、会社全体又は外部（顧客、取引先）に影響を及ぼす

③　可用性（A：Availability）

評価値	レベル	定義
1	低	・利用停止があっても影響ない
2	中	・1 日程度の利用停止が許容できる ・利用停止があった場合、業務・サービスに影響を及ぼす
3	高	・1 時間程度の利用停止が許容できる ・利用停止があった場合、会社全体又は外部（顧客、取引先）に影響を及ぼす

④　資産価値算出の論理式

{資産価値} ＝ {機密性の評価値} × {完全性の評価値} × {可用性の評価値}

III.　想定される脅威の特定

資産価値を決定した情報資産について、⑤に示す例を参考に想定される脅威を特定する。

⑤　想定されるリスクの例

分類	脅威の例
物理的損傷	火災、水害、汚染、機器・媒体の破壊・滅失、粉塵、腐食、凍結
自然事象	気候、地震、火山活動、気象現象、洪水
重要なサービスの喪失	空調や給水システムの故障、電力供給の停止、電気通信機器の故障
情報を危うくすること	危険にさらされている干渉信号の傍受、遠隔スパイ行為、盗聴、媒体・文書の盗難、機器の盗難、再利用又は廃棄した媒体からの復元、漏洩、信頼できない情報源からのデータ、ハードウェアの改ざん、ソフトウェアの改ざん
技術的な故障	機器の故障、機器の誤動作、ソフトウェアの誤作動、情報システムの保守に関する違反
認可されていない行為	海賊版又は（不正）コピーソフトウェアの使用、データの破壊、データの違法な処理
機能を危うくすること	使用時のミス（誤消去、紛失、パスワード忘却等）、権限の乱用、権限の詐称、アクションの拒否、要員の可用性に関する違反

IV.　脆弱性の特定

特定した想定される脅威から、⑥に示す例を参考に脅威に関連する脆弱性を特定する。

⑥　脆弱性の例

分類	脆弱性の例	関連するリスクの例
環境施設	ドア、窓などの物理的保護の欠如	盗難
	災害を受けやすい立地条件	洪水、地震、災害

ハードウェア	格納・保管の不備 （温湿度変化に影響を受けやすい等）	故障、誤作動、盗難
	記憶媒体のメンテナンス不足	故障、情報漏洩
	復旧方法の未整備	故障
	保管・管理手順の不備（持出しの際の手続きの不備等）	誤廃棄、紛失、盗難
ソフトウェア	アクセス制御の未整備（アクセス制限がされていない／不十分、取扱担当者が多い等）	情報漏洩、システムへの不正アクセス
	ソフトウェアのダウンロードの非制限	故障、情報漏洩、システムへの不正アクセス
	ライセンス管理の不徹底	情報漏洩、システムへの不正アクセス
	セキュリティパッチの未適用	情報漏洩、システムへの不正アクセス
電子データ	アクセス制御の未整備（アクセス権限が割り当てられていない／不十分、取扱担当者が多い等）	情報漏洩、システムへの不正アクセス
	バックアップの未整備（バックアップがされていない／不十分等）	故障
	量が多い	誤消去、情報漏洩
紙データ	保管体制の不備	情報漏洩
	アクセス制御の未整備（格納庫の未施錠等）	情報漏洩
	量が多い	紛失、誤廃棄
組織	情報セキュリティに対する役割分担の未整備	情報漏洩、システムへの不正アクセス、オペレーションミス
	情報セキュリティに対する監査体制の未整備	情報漏洩、システムへの不正アクセス、オペレーションミス

V. 現状の管理策の特定

現状、脅威の発生頻度や脆弱性を低減するために講じている管理策を特定する。

VI. 脅威の発生頻度の評価

脅威が発生する頻度（発生頻度）の定量的な評価を、⑦に示す区分に基づいて行う。

⑦ 発生頻度の区分

評価値	レベル	定義
1	低	通常では発生しない（3 年以内に 1 度も発生しない）
2	中	専門能力のあるものの不注意で発生する（1 年に 1 度程度発生する）
3	高	通常の状態で発生する（1 ヶ月に 1 度以上発生する）

VII. 脆弱性レベルの評価

脆弱性レベルの定量的な評価を、⑧に示す区分に基づいて行う。

⑧　脆弱性レベルの区分

評価値	レベル	定義
1	低	適切な対策を実施している。
2	中	ある程度の対策は実施している。
3	高	全く対策を講じていない。

VIII. リスク値の決定

上記にて、資産価値・発生頻度・脆弱性について評価した情報資産について、⑨に示す論理式に基づいて、リスク値の定量的な評価を行う。

⑨　リスク値算出の論理式

｛リスク値｝＝｛資産価値｝×｛発生頻度｝×｛脆弱性｝

IX. 情報セキュリティリスクの評価

算出したリスク値について、⑩に示すリスク受容基準と照らし合わせ、受容基準値未満だったものについては、リスクを受容するものとし、受容基準値以上のものについては、リスク対応計画を策定する。

⑩　リスク受容基準

リスク受容基準値：　２４

脅威の発生頻度						1	1	1	2	2	2	3	3	3
脆弱性レベル						1	2	3	1	2	3	1	2	3
CIA値の組合せ	1	1	1	資産価値	1	1	2	3	2	4	6	3	6	9
	1	1	2		2	2	4	6	4	8	12	6	12	18
	1	1	3		3	3	6	9	6	12	18	9	18	27
	1	2	2		4	4	8	12	8	16	24	12	24	36
	1	2	3		6	6	12	18	12	24	36	18	36	54
	2	2	2		8	8	16	24	16	32	48	24	48	72
	1	3	3		9	9	18	27	18	36	54	27	54	81
	2	2	3		12	12	24	36	24	48	72	36	72	108
	2	3	3		18	18	36	54	36	72	108	54	108	162
	3	3	3		27	27	54	81	54	108	162	81	162	243

6.1.3　情報セキュリティリスク対応

当社は，次の事項を行うために，情報セキュリティリスク対応のプロセスを定め，適用する。

a) リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する。

b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。

c) **6.1.3 b)** で決定した管理策を附属書 **A** に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。

d) 次を含む適用宣言書を作成する。
- 必要な管理策［**6.1.3** の **b)** 及び **c)** 参照］
- それらの管理策を含めた理由
- それらの必要な管理策を実施しているか否か
- 附属書 **A** に規定する管理策を除外した理由

e) 情報セキュリティリスク対応計画を策定する。

f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について，リスク所有者の承認を得る。

組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持する。

当社は、以下の手順に基づいて、情報セキュリティリスク対応のプロセスを実施する。

I.　情報セキュリティリスク対応の選択

「6.1.2　情報セキュリティリスクアセスメント」にてリスク評価を行った結果、リスク受容基準値を超えたものについて、以下の区分に基づいて、リスク対応を選択し、【情報資産リスクアセスメント表】に記録する。

対応策	対応内容
低減	管理策を採用し、リスク発生の可能性やリスクによってもたらされる影響を軽減する。
回避	リスクの発生可能性を根本的に無くす。例えば、書類による漏洩というリスクがあるならば、書類での業務をやめて、全て電子化してしまうといったものがこれに当たる。
移転	関連するリスクを、保険業・外部委託業者といった他の関係者へ移転すること。 例えば、情報セキュリティ保険に加入する、業務をアウトソーシングする、等。
受容	受容レベル基準を明確に満たす場合はリスクを受け入れる考え方。また、管理策を採用しても、新しい脅威が発生する場合や、リスクが残存してしまう場合もある。

II.　管理策の選択

リスク対応を実施することが決定したリスクに対して、講じる管理策を決定し、【情報資産リスクアセスメント表】に記録する。

III. リスク値の再決定

実施が決定した管理策について、その実施を想定して、脅威の発生頻度・脆弱性レベルを再評価し、リスク値を再算出する。

IV. 適用宣言書の作成

(1) 情報セキュリティ委員会は、①から④の事項を考慮して、【適用宣言書】を作成する。
   ① リスクアセスメントの結果、実装が必要だと判明した追加の管理策
   ② リスクアセスメントの結果に関わらず、当社の情報セキュリティ上、必須と考えられる基本的な管理策
   ③ 法的又は規制要求事項を満たすための管理策
   ④ お客様との契約上の要求事項を満たすための管理策

(2) 【適用宣言書】には、以下の内容を必ず含める。
   ① 必要な管理策
   ② ①の管理策が必要な理由
   ③ ①の管理策を実施しているか否か
   ④ ISO/IEC 27001:2022 附属書 A に規定する管理策を除外した理由

V. リスクアセスメント結果及び残留リスクの承認

リスクアセスメントの結果は、リスク所有者に報告し、リスク所有者によってリスクアセスメント結果及びリスク対応後に残留するリスクの受容について承認する。

VI. リスク対応計画の策定

リスクアセスメントの結果新たに講じる管理策、及び適用宣言書の作成時に必要であると決定した管理策の実施計画を策定し、【情報セキュリティリスク対応計画表】に記録する。

6.2 情報セキュリティ目的及びそれを達成するための計画策定

当社は，関連する機能及び階層において，情報セキュリティ目的を確立する。

情報セキュリティ目的は，次の事項を満たす。

a) 情報セキュリティ方針と整合している。
b) （実行可能な場合）測定可能である。
c) 適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。
d) これを監視する。
e) これを伝達する。
f) 必要に応じて，更新する。

g) 文書化した情報として利用可能な状態にする。

当社は，情報セキュリティ目的に関する文書化した情報を保持する。

当社は，情報セキュリティ目的をどのように達成するかについて計画するとき，次の事項を決定する。

h) 実施事項
i) 必要な資源
j) 責任者
k) 達成期限
l) 結果の評価方法

(1) 情報セキュリティ目的
情報セキュリティ管理者は情報セキュリティ目的及びその目的を達成するための計画を策定し、【情報セキュリティ目的達成計画表】を文書化した情報として保持する。

(2) 情報セキュリティ目的の周知
情報セキュリティ管理者は情報セキュリティ目的を、部門内に掲示し、伝達、周知する。

(3) 情報セキュリティ目的の見直しのタイミング
情報セキュリティ管理者はマネジメントレビューの結果を受けて、及び社内外で重大な変化があった場合に見直しを行い、必要に応じて改訂する。

6.3 変更の計画策定

当社が ISMS の変更の必要があると決定したとき，その変更は，計画的な方法で行う。

7 支援

7.1 資源

当社は，ISMS の確立，実施，維持及び継続的改善に必要な資源を決定し，提供する。

7.2 力量

当社は，次の事項を行う。

a) 組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。

b) 適切な教育，訓練又は経験に基づいて，それらの人々が力量を備えていることを確実にする。

c) 該当する場合には，必ず，必要な力量を身に付けるための処置を講じ，講じた処置の有効性を評価する。

d) 力量の証拠として，適切な文書化した情報を保持する。

当社は以下の手順に従って、教育及び訓練を実施する。

I. 力量

(1) 力量の明確化

情報セキュリティ管理者は、情報セキュリティパフォーマンスに影響のある業務に従事する従業員に必要な力量を【スキル管理表】に明確にする。

(2) 力量の確保

情報セキュリティパフォーマンスに影響のある業務に従事する従業員に必要な力量を確保するため、次の事項を実施する。

① 情報セキュリティパフォーマンスに影響がある業務には、【スキル管理表】に定める力量を有している従業員を割り当てる。

② 従業員が必要な力量を満たすため、教育訓練を実施する。

II. 教育・訓練

(1) 教育・訓練の計画

【情報セキュリティ管理者】は、毎年教育・訓練計画を作成し、【教育・訓練計画表】として策定する。

(2) 教育・訓練の実施

情報セキュリティ管理者は、作成した教育・訓練計画に基づき実施する。

(3) 教育・訓練の有効性評価

情報セキュリティ管理者は、教育・訓練の受講者に対し、理解度の確認を行うことで、教育・訓練の有効性を評価する。

(4) 教育・訓練の記録

【情報セキュリティ管理者】は、実施結果を【教育・訓練計画表】に記録し、トップマネジメントに報告する。

7.3 認識

当社の管理下で働く人々は，次の事項に関して認識をもつ。
a) 情報セキュリティ方針
b) 情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMS の有効性に対する自らの貢献
c) ISMS 要求事項に適合しないことの意味

当社は、当社の管理下で働く全ての要員が、下記の事項について認識をもつように、集合研修/e ラーニングを用いた教育を実施し、【教育・訓練計画表】で確実にする。

a) 情報セキュリティ方針（「5.2　方針」参照）
b) ISMS の有効性に対する自らの貢献
   ■ ISMS 活動を行うことにより、本人への信頼、スキルアップにつながり、ひいては当社への信頼を高め、価値を増大化し、事業に対する大きな貢献となる。
c) ISMS 要求事項に適合しなかった場合に起こりうる結果及びその重大性
   ■ セキュリティ行動に対する信頼を失うことは、技術者にとってのその他の価値を無きものにしてしまうほどの意味をもつ。ひいては当社の事業停止につながりえる。

7.4 コミュニケーション

当社は，次の事項を含む，ISMS に関連する内部及び外部のコミュニケーションを実施する必要性を決定する。
a) コミュニケーションの内容
b) コミュニケーションの実施時期
c) コミュニケーションの対象者
d) コミュニケーションの方法

当社は，ISMS に関連する内部及び外部のコミュニケーションを以下の通り実施する。

内部のコミュニケーション			
内容	実施時期	対象者	方法
ISMS 研修会	1 回/年	社員全員	集合研修、e ラーニング
内部監査	1 回/年	内部監査員、情報セキュリティ管理者、	対面

		トップマネジメント	
マネジメントレビュー	1 回/年	情報セキュリティ管理者、トップマネジメント	対面
インシデント報告	随時	社員、トップマネジメント	対面、オンライン会議

外部のコミュニケーション			
内容	実施時期	対象者	方法
NEC	随時	トップマネジメント	対面、オンライン会議　他

7.5　文書化した情報

7.5.1　一般

当社の ISMS は，次の事項を含む。
a)　この規格が要求する文書化した情報
b)　ISMS の有効性のために必要であると組織が決定した，文書化した情報

当社の ISMS に関する文書は、【文書管理台帳】に示す。

7.5.2　作成及び更新

文書化した情報を作成及び更新する際，当社は，次の事項を確実にする。
a)　適切な識別及び記述（タイトル，日付，作成者）
b)　適切な媒体（例えば，紙，電子媒体）
c)　適切性及び妥当性に関する，適切なレビュー及び承認

I.　形式・構成

紙又は電子媒体で作成するものとする。

II.　文書番号

文書番号は、【文書管理・採番ルール】に従う。

7.5.3　文書化した情報の管理

ISMS 及びこの規格で要求されている文書化した情報は，次の事項を確実にするために，管理する。

a)　文書化した情報が，必要なときに，必要なところで，入手可能かつ利用に適した状態である。

b)　文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用又は完全性の喪失からの保護）。

文書化した情報の管理に当たって，組織は，該当する場合には，必ず，次の行動に取り組む。

c)　配付，アクセス，検索及び利用

d)　読みやすさが保たれることを含む，保管及び保存

e)　変更の管理（例えば，版の管理）

f)　保持及び廃棄

ISMS の計画策定及び運用のために組織が必要と決定した外部からの文書化した情報は，必要に応じて識別し，管理する。

文書の発行者又は情報セキュリティ管理者は、文書化した情報を管理するために、該当する場合には次の事項を実施する。

(1)　発行・配布・アクセス

①　発行された文書は、共有フォルダに保管し、必要に応じて HP で従業員がアクセス可能とする。

②　許可された者以外が参照や更新ができないよう適切なアクセス制限を行う。

③　容易に検索し利用できるように、適切に分類し保管する。

(2)　保管・保存

①　紙媒体は、劣化や損傷及び紛失を防止するよう書庫などに保管する。

②　電子媒体は、誤って修正や削除が行われないように、適切なアクセス制限を行う。

(3)　変更管理

①　文書を変更した場合には、改訂歴表に変更の内容、改訂版の番号、日付などを記入して、最新版及び使用可能な版であることを明示する。

②　【文書管理台帳】を更新した上、ファイル名の改訂日や版番号等を変更する。

③　文書が変更された場合には、電子メールで速やかに関係者に周知する。

(4)　文書の廃棄

①　情報セキュリティ管理者が不要と判断した文書化した情報は、廃版として【文書管理台帳】を更新する。

②　文書が廃版となった旨、電子メールで速やかに関係者に周知する。

③　旧版を保持する必要がある場合は、旧版であることを明示して管理する。

8　運用

8.1　運用の計画及び管理

当社は，次に示す事項の実施によって，要求事項を満たすため，及び箇条 **6** で決定した活動を実施するために必要なプロセスを計画し，実施し，かつ，管理する。

－　プロセスに関する基準の設定

－　その基準に従った，プロセスの管理の実施

当社は，プロセスが計画どおりに実施されたという確信をもつために必要とされる，文書化した情報を利用可能な状態にする。

当社は，計画した変更を管理し，意図しない変更によって生じた結果をレビューし，必要に応じて，有害な影響を軽減する処置を講じる。

当社は，ISMS に関連する，外部から提供されるプロセス，製品又はサービスが管理されていることを確実にする。

プロセスが計画通りに実施されたという確信をもつために、【年間スケジュール】、【情報セキュリティリスク対応計画表】及び 【情報セキュリティ目的達成計画表】を文書化した情報として保持する。

8.2　情報セキュリティリスクアセスメント

当社は，あらかじめ定めた間隔で，又は重大な変更が提案されたか若しくは重大な変化が生じた場合に，**6.1.2 a)** で確立した基準を考慮して，情報セキュリティリスクアセスメントを実施する。

当社は，情報セキュリティリスクアセスメント結果の文書化した情報を保持する。

当社は、情報セキュリティリスクアセスメントの結果を、【情報資産リスクアセスメント表】に記録・保持する。

8.3　情報セキュリティリスク対応

当社は，情報セキュリティリスク対応計画を実施する。

当社は，情報セキュリティリスク対応結果の文書化した情報を保持する。

当社は、情報セキュリティリスク対応の結果を、【情報セキュリティリスク対応計画表】に記録・保持する。

9　パフォーマンス評価

9.1　監視、測定、分析及び評価

当社は，次の事項を決定する。

a)　監視及び測定が必要な対象。これには，情報セキュリティプロセス及び管理策を含む。

b)　該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法。
選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい。

c)　監視及び測定の実施時期

d)　監視及び測定の実施者

e)　監視及び測定の結果の，分析及び評価の時期

f)　監視及び測定の結果の，分析及び評価の実施者

当社は，この結果の証拠として，文書化した情報を利用可能な状態にする。

当社は，情報セキュリティパフォーマンス及び ISMS の有効性を評価する。

当社は、下記の表のとおり、情報セキュリティパフォーマンス及び ISMS の有効性を評価する。

監視・測定の対象	何をもって監視・測定・分析・評価を行うか	監視・測定の実施時期	監視・測定の実施者	分析・評価の実施時期	分析・評価の実施者
方針・目的の達成度 ISMS 運用の有効性評価	『情報セキュリティ目的達成計画表』 『年間スケジュール』	随時	情報セキュリティ管理者	年 1 回	情報セキュリティ管理者
ISMS の適合性	『内部監査チェックリスト』	年 1 回	内部監査員	年 1 回	内部監査員
リスク対応計画の実施状況	『情報セキュリティリスク対応計画表』	随時	情報セキュリティ管理者	年 1 回	情報セキュリティ管理者
インシデント	『是正処置報告書』	インシデント発生時	トップマネジメント	年 1 回	トップマネジメント
監査ログ	監査ログ	月 1 回	情報セキュリティ管理者	年 1 回	情報セキュリティ管理者、トップマネジメント
アクセス権	アクセス権一覧	年 1 回	情報セキュリティ管理者	年 1 回	情報セキュリティ管理者、トップマネジメント
資産の見直し	『情報資産リスクアセスメント表』	年 1 回	トップマネジメント	年 1 回	情報セキュリティ管理者、トップマネジメント

9.2 内部監査

9.2.1 一般

当社は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施する。

a) 次の事項に適合している。
   1) ISMS に関して，当社自体が規定した要求事項
   2) この規格の要求事項
b) 有効に実施され，維持されている。

9.2.2 内部監査プログラム

当社は，監査プログラムを計画し，確立し，実施し，維持する。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。

そ（れら）の内部監査プログラムを確立するとき，当社は，関連するプロセスの重要性及び前回までの監査の結果を考慮する。

当社は，次に示す事項を行う。

a) 各監査について，監査基準及び監査範囲を明確にする。
b) 監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。
c) 監査の結果を関連する管理層に報告することを確実にする。

当社は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にする。

当社は、以下の手順に基づいて、内部監査を実施する。

I. 監査基準

次のものを監査基準として、内部監査を実施する。

① ISO/IEC 27001:2022
② 識別された法令・規則及び契約上の要求事項
③ 当社が制定した情報セキュリティマニュアル、規程及び手順書

II. 内部監査員の選定

(1) 内部監査員は、次の条件を全て満たした者とする。
   ① 社外又は社内の内部監査研修を受講した者
   ② トップマネジメントが任命した者
(2) トップマネジメントは、内部監査員に、内部監査を実施させる。

III. 計画

(1) 内部監査員は、供給者も含め、トップマネジメント及び情報セキュリティマネジメントシステムに係わる全ての部門・機能を網羅した内部監査が実施できるように計画を策定し、【内部監査計画書】を作成する。少なくとも年 1 回、内部監査を実施するものとする。
(2) 内部監査員は、チームメンバーが所属する部門を自ら監査しないように配慮して、計画を策定する。
(3) 内部監査員は、監査の実施に先立ち、被監査部門に【内部監査計画書】にて事前通知する。
(4) 内部監査員は、監査の準備及び【内部監査チェックリスト】を作成し、トップマネジメントが承認する。

IV. 実施

(1) 内部監査は、必要な場合、下記の基準に基づいて評価を行う。

区分	定義
充実点	要求事項を超えている、又は、当該組織に効果的である充実していると評価するパフォーマンス、方法、技術などの優れた取組み
適合	要求事項を満たしており、マネジメントシステムの意図した結果を達成している
重大な不適合	意図した結果を達成するマネジメントシステムの能力に影響を与える不適合 a) 効果的なプロセス管理が行われているか、又は製品若しくはサービスが規定要求事項を満たしているかについて、重大な疑いがある。 b) 同一の要求事項又は問題に関連する軽微な不適合が幾つかあり、それらがシステムの結果であることが実証され、その結果重大な不適合となるもの
軽微な不適合	意図した結果を達成するマネジメントシステムの能力に影響を与えない不適合
観察事項	a) 不適合には該当しないが、放置しておくと不適合につながる可能性のある状況 b) 不適合には該当しないが、組織の効果的な運用の視点において改善の余地がある状況

(2) 【内部監査チェックリスト】に監査の記録をとる。

V. 報告

(1) 内部監査員は、監査の中で不適合を発見した場合、【是正処置報告書】を起票する。
(2) 内部監査員は、起票された【是正処置報告書】を用いて不適合として指摘した内容を被監査部門責任者に説明し、是正処置を指示する。
(3) 内部監査員は、監査結果に基づき、【内部監査報告書（情報セキュリティ）】を作成し、トップマネジメントに報告する。

VI. 内部監査における是正処置

内部監査で指摘され、【是正処置報告書】に示された不適合は、「10.2　不適合及び是正処置」に規定さ

れている手順に従い、是正処置を実施する。

9.3 マネジメントレビュー

9.3.1 一般

トップマネジメントは，当社の ISMS が，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，ISMS をレビューする。

トップマネジメントは年 1 回、情報セキュリティマネジメントシステム、情報セキュリティ方針及び情報セキュリティ目的の見直しを実施する。ただし、トップマネジメントが見直しの必要がある判断した場合は、臨時のマネジメントレビューを実施することができる。

9.3.2 マネジメントレビューへのインプット

マネジメントレビューは，次の事項を考慮する。 a) 前回までのマネジメントレビューの結果講じた処置の状況 b) ISMS に関連する外部及び内部の課題の変化 c) ISMS に関連する利害関係者のニーズ及び期待の変化 d) 次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック 1) 不適合及び是正処置 2) 監視及び測定の結果 3) 監査結果 4) 情報セキュリティ目的の達成 e) 利害関係者からのフィードバック f) リスクアセスメントの結果及びリスク対応計画の状況 g) 継続的改善の機会

情報セキュリティ管理者は、マネジメントレビューの実施に際して、上記 a) ～ g) の情報を【マネジメントレビュー議事録】に記録し、トップマネジメントに提出する。
また、【年間スケジュール】に、1 年の振り返り結果を記載しトップマネジメントに提出する。

9.3.3 マネジメントレビューの結果

マネジメントレビューの結果には，継続的改善の機会，及び ISMS のあらゆる変更の必要性に関する決定を含める。 当社は，マネジメントレビューの結果の証拠として，文書化した情報を利用可能な状態にする。

当社は、マネジメントレビューの結果を、【マネジメントレビュー議事録】に記録、保持する。

10　改善

10.1　継続的改善

当社は，ISMS の適切性，妥当性及び有効性を継続的に改善する。

当社は、継続的改善の一環として取り組まなければならない必要性があるかどうかを明確にするために、「9.1　監視、測定、分析及び評価」の結果、「9.2　内部監査」の結果及び「9.3　マネジメントレビュー」の結果を検討し、【是正処置報告書】に明確にし、保持する。

10.2　不適合及び是正処置

不適合が発生した場合，当社は，次の事項を行う。 a)　その不適合に対処し，該当する場合には，必ず，次の事項を行う。 　1)　その不適合を管理し，修正するための処置を講じる。 　2)　その不適合によって起こった結果に対処する。 b)　その不適合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置を講じる必要性を評価する。 　1)　その不適合をレビューする。 　2)　その不適合の原因を明確にする。 　3)　類似の不適合の有無，又はそれが発生する可能性を明確にする。 c)　必要な処置を実施する。 d)　講じた全ての是正処置の有効性をレビューする。 e)　必要な場合には，ISMS の変更を行う。 是正処置は，検出された不適合のもつ影響に応じたものとする。 当社は，次に示す事項の証拠として，文書化した情報を利用可能な状態にする。 f)　不適合の性質及びそれに対して講じたあらゆる処置 g)　是正処置の結果

当社は、以下の手順に基づいて、是正処置を実施する。

I.　不適合の識別

不適合	処置責任者	処置実施者
外部監査での指摘事項	トップマネジメント	トップマネジメント、情報セキュリティ管理者、指摘を受けた部門の部門推進者又は指摘を受けた担当者
内部監査での指摘事項	情報セキュリティ管理者	トップマネジメント、情報セキュリティ管理者、指摘を受けた部門の部門推進者又は指摘を受けた担当者
不適合の是正処置	情報セキュリティ管理者	トップマネジメント、情報セキュリティ管理者、不適合を発見又は指摘された担当者

苦情	情報セキュリティ管理者	トップマネジメント、情報セキュリティ管理者、不適合を発見又は指摘された担当者
その他マネジメントシステムに関わる不適合	情報セキュリティ管理者	トップマネジメント、情報セキュリティ管理者、不適合を発見又は指摘された担当者

II. 是正処置の実施手順

(1) 処置実施者は、外部監査、内部監査又はマネジメントレビューにおいて不適合が報告された場合、そこで起票された【是正処置報告書】又は不適合が記録された報告書にて、不適合の内容を確認する。
(2) 処置実施者は、不適合の根本的な原因を究明し、是正処置を立案、【是正処置報告書】に記録する。
(3) 処置責任者は、是正処置案を評価し、是正処置の実施を承認する。
(4) 処置実施者は、承認を得た是正処置を実施し、実施結果を【是正処置報告書】に記録、処置責任者に提出する。
(5) 処置責任者は、是正処置の有効性をレビューし、【是正処置報告書】に記録する。

III. 是正処置に関するその他事項

(1) とられる是正処置は、問題の大きさに対して適切な程度とする。その判断は処置責任者による。
(2) 是正処置の処置実施者は、実施した是正処置の中で、特に情報セキュリティマネジメントシステム文書（以下、ISMS 文書とする）の改定又は制定を必要とするもの、水平展開を必要とするものについては、処置責任者経由で文書管理部門に関係 ISMS 文書の改訂又は制定を起票する。
(3) 是正処置の情報は、情報セキュリティ管理者からマネジメントレビューに提出される。

〔制定・改訂履歴〕

版数	制定・改定日	制定又は改訂主旨	作成	承認
0.1	2025/3/9	ドラフト版	岡	塩田
0.2	2025/4/1	6.4 リスク分析・評価を全面改訂	岡	塩田
0.3	2025/4/4	全面改訂(ベース文書を変更)	岡	塩田
1.0	2025/7/11	初版	岡	塩田
2.0	2025/8/30	文書管理ルールについて改訂	岡	塩田
2.1	2025/10/14	1 適用範囲　a)業務上の適用範囲　の名称を厳格化	岡	塩田
		4.1　当社及びその状況の理解　気候変動に関連する課題として、ペーパーレス/省力化　を追加	岡	塩田
		8.1　9.1　9.3.2 に　「年間スケジュール」を追記	岡	塩田
2.2	2025/10/27	4.1 最新版で変更された「気候変動」に関する要求事項を記載。	岡	塩田
2.3	2025/11/18	7.2　力量　「教育・訓練実施記録」を「教育・訓練計画表」へ変更。	岡	塩田
2.4	2025/12/0312/3	7.5.3　文書化した情報の管理　発行責任者→発行者、保管責任者→情報セキュリティ管理者	岡	塩田