制定・改訂履歴

版数	制定/改訂日	制定 又は 改訂主旨	作成	承認
2.1	2025年10月14日	改版履歴を追加	岡	塩田
		秘密関連機器管理台帳を修正。電子媒体、秘密情報機器の持ち出し管理表とする。持出先を追加。秘密事項扱いの紙文書の持ち出し状況を修正。持出先を追加。	岡	塩田
		No5 私有PCについて「私用PCを利用する場合は、経営管理者の承認を得る。」を追加	岡	塩田
2.2	2025年10月27日	No.12 入館簿のマスタを変更	岡	塩田
2.3	2025年12月3日	No.24 許可ソフトを記載	岡	塩田

ABS情報セキュリティ運用ルール（2025年度版）

社外秘

No	規則	備考
1	~~業務の再委託を禁止する。~~	
2	NECグループが要求するセキュリティ対策を理解するため、お取引先様向け「お客様対応作業における遵守事項」を読み、熟知する。	
3	不適切な取り扱いによる情報漏えいやウイルス感染を防ぐために、構内外において取り外し可能な媒体*1の使用を禁止する。	*1 取り外し可能な媒体とは、コンピュータシステム等から取り外し、持ち運び可能な媒体（USBメモリ、取り外し可能なハードディスク、フラッシュメモリ、テープ、CD、DVD等）を指します。
4	紛失・盗難、ウイルス感染等による情報漏えいを防ぐため、秘密事項を格納する業務用のスマートデバイス*1に関して、以下のセキュリティ対策を行う。 ・ 自動的にロックされるように設定し、ロックの解除にはパスワード等を設定すること。 ・ 電話帳データを除き、スマートデバイスに業務情報を保存していないこと。 ・ ウイルス対策ソフトを導入すること （ただし、iOSのスマートデバイスはこの限 りではない）。	*1 スマートデバイスとは、スマートフォンやタブレット端末等の情報端末を指します。
5	私品による情報漏えい等を防ぐために、私有情報機器*1（PC 等）や取り外し可能な私有媒体*2に関して、以下のセキュリティ対策を行う。 ・ 私有情報機器*1（PC 等）や取り外し可能な私有媒体*2の業務利用を禁止する。やむを得ず私用PCを利用する場合は、経営管理者の承認を得る。 ・ 私有情報機器*1（PC 等）や取り外し可能な私有媒体*2への業務情報の保存*3を禁止する。 ・ 私有メールアドレスに業務情報を送信しないこと。 ・ 私有情報機器を業務端末に接続しないこと。	*1 情報機器とは、情報処理に用いるコンピュータ等の機器を指します。 *2 取り外し可能な媒体とは、コンピュータシステム等から取り外し、持ち運び可能な媒体（USBメモリ、取り外し可能なハードディスク、フラッシュメモリ、テープ、CD、DVD等）を指します。 *3 過去に取り扱った業務情報も対象とします。
6	情報漏えい等を防ぐために、社有のスマートデバイス*1に関して、以下のセキュリティ対策を行う。 ・ 端末に秘密情報を保存しないこと。端末への電話帳の登録は可とするが、 できる限り符号化すること。 ・ アプリケーションを利用する場合は、信頼できる提供元のアプリケーション、ファイル*2のみを取り扱うこと。 ・ OS・アプリケーションのパッチ適用やバージョンアップを迅速かつ確実に行うこと。 ・ OSの改造（root化、Jailbreak）を行わないこと。 ・ OS・アプリケーションのパッチ適用やバージョンアップを迅速かつ確実に行う こと。 ・ クラウドサービスを利用しないこと。 ・ 端末は、10分以内で自動的にロックされるように設定し、ロック解除のためのパスワードは、原則として、8文字以上の英数字を設定すること。また、可能であれば、盗難・紛失対策として、リモート消去の設定を行うこと。 ・ ウイルス対策ソフトを導入すること （ただし、iOSのスマートデバイスはこの限りではない）。 ・ 原則として、会社が推奨する端末のみ利用すること。 ・ イントラネットへの接続は、会社から許可された方法に従うこと。 ・ スマートデバイスを社外に持ち出す場合は、所定の手続きを経ること。 ・ ネックストラップや携帯電話ケースを利用し紛失対策を実施すること。 ・ 携帯電話内の不要な情報は常に削除すること。 ・ キャリアメールでは、従業員間の緊急連絡用等、最小限の用途に留め、秘密情報のやり取りは行わないこと ・ 返却時は、携帯電話に保存されているデータを確実に消去すること ・ 紛失・盗難時は、速やかな連絡、回線停止・解約等の手続き等を行うこと	*1 スマートデバイスセとは、 PC並みの機能を持つ携帯電話やPDA（携帯情報端末）の総称です。 PC同様にウェブページの閲覧、メール等の様々なインターネットサービスを利用できる他、ビジネスアプリケーションの利用も可能な 例） MEDIAS、LifeTouch、iPhone、iPad、BlackBerry 等 の機器を指します。 *2 「信頼できる提供元のアプリケーション」の選定基準例 信頼できる提供元のアプリケーションの選定は、以下を考慮して行う。 ・セキュリティの観点でアプリを確認しているマーケットや紹介サイトで扱われている ・端末上で「提供元不明のアプリ」の設定を有効にすることを求めない ・マーケット上の評判がよい、ダウンロード数が多い（ただし、単純に信用しない） ・アプリのサポート（アプリの更新や問い合わせへの対応）が継続されている なお、Androidアプリの選定にあたっては、上記に加えて、使用するアクセス権限（パーミッション）が必要最小限に留められているアプリであることも重要である。特に以下のパーミッションは、通信が発生し、情報漏えいをもたらす恐れがあるため、注意が必要で ・完全なインターネットアクセス ・SMSの受信 ・SMSメッセージの送信 ・電話番号発信
7	秘密事項の取り扱い方法を明確にするため、「NECグループ標準秘密指定の指針」を読み、熟知する。	

ABS情報セキュリティ運用ルール（2025年度版）

社外秘

No	規則	備考
8	秘密事項を特定するため、以下の秘密表示を行う。 ・自社で作成した書類に秘密事項を記載する場合は、各ページに秘密表示を行うこと。 ・NECグループ委託元を経由せずに直接入手した書類に秘密事項が記載されていた場合は、各ページに秘密表示を ・秘密事項を含む電子メールのサブジェクト(件名)もしくは本文に秘密表示を行うこと。 ・NECグループ委託元からの指示の有無にかかわらず、秘密表示を行うこと。	
9	紛失による情報漏えいを防ぐために、秘密事項の持ち出しは原則禁止とし、持ち出す場合は以下のような管理手順によって厳格に管理する。 ・秘密事項を持ち出す際、持ち出す情報が適切であることを管理者が確認の上、承認を得ること。 ・秘密事項を持ち出す際、持ち出す情報量が必要最小限であることを管理者が確認の上、承認を得ること。 ・秘密事項扱いの電子データを持ち出す場合、万一紛失した際持ち出し情報を特定できるよう、電子データを記録用フォルダにバックアップ*1すること。 ・秘密事項扱いの紙文書を持ち出す場合、万一紛失した際持ち出し情報を特定できるよう、台帳*2に持ち出し文書の情報を記録すること。 また、秘密事項の携行時に以下の事項を注意する。 ・必要最小限の情報に留め、目的地まで速やかかつ安全に運ぶこと。 ・事故が発生した場合に備えて持ち歩く情報の特定ができるようにしておく。 ・手提げ袋は原則として使用しないこと(材質が弱いため、運搬中の破損等のリスクがある)。 ・電車移動や車移動等で秘密事項を携行する際は、肌身離さず所持すること。 ・持ち歩く場合は飲酒しない。飲酒をする場合は持ち歩かない。	*1 電子データのバックアップとは、万一紛失した場合に、紛失情報を特定できるよう、持ち出し時に、持ち出す情報だけバックアップすることを指します。データの保全を目的としたバックアップではありません。 *2 本ファイルマスタの、「秘密事項扱いの紙文書の持ち出し状況」シートに記録すること。
10	残留データの漏えいを防ぐために、秘密事項に対する廃棄・返還管理*1し、廃棄・返還結果をNECグループ委託元に報 ・自社の個人環境から秘密事項を削除した結果の報告する。 ・自社の秘密事項の廃棄・回収結果を、委託元宛てに文書で報告する。 ・業務都合で当該案件の秘密事項を継続して保持する場合、委託元と相談の上、継続保持すべき情報を選定する。	*1 廃棄・返還管理とは、個人環境をはじめ自社内からの破棄、委託元への報告、継続保持の委託完了を管理することを指します。
11	部外者が秘密事項にアクセスできないよう、データに対するアクセス制御を漏れなく実施する。 ※ 以下の点を持ってアクセス制御(取り扱うデータに対するアクセス制御の設定、および、アクセス権限の管理)とす ・常時オフィスへの施錠をし、部外者のオフィスへの侵入を阻止する。 ・外部から、オフィス内のPCへのアクセスを許可しない。 ・全てのPCにユーザ名とパスワードの入力を要求するようにし、例えオフィス内に侵入してもデータにアクセスできな	
12	部外者の侵入を防ぐため、事務所では出入口を施錠及び入退を監視する。 ・出入口を常時施錠する。 ・事務所の入退出時に入退出記録*1を記入する。	*1 「250531-13_入館簿」に記録すること。
13	情報漏えい事故を防ぐため、サイバーセキュリティ攻撃*1に対して、セキュリティ対策を熟知する。 ・メール添付ファイルを不用意に開かない ・メール本文中にURLがあった場合、不用意にクリックしない ・HTMLメールを表示しない ・不審なメールはメールヘッダ情報を確認し、怪しいものは破棄する ・業務外でWebサイトを閲覧しない ・セキュリティパッチを速やかに適用する ・ネットワークドライブの割り当て設定を必要最小限にする ・重要なデータは定期的にバックアップする	*1 本項目で言うサイバーセキュリティ攻撃とは、コンピュータやインターネット等を利用して、標的のコンピュータやネットワークに不正に侵入して機密情報の搾取や破壊、改ざん等を行なったり、システムを機能不全に陥らせたりすることを指します。

ABS情報セキュリティ運用ルール（2025年度版）

社外秘

No	規則	備考
14	第三者による進入やウィルス感染を防ぐため、常に最新の状態に保つ[*1]等、情報システム（サーバ、PC等）の脆弱性を管理する。 ・ウイルス対策ソフトのパターンファイルを常に最新化する ・最新バージョンのOSやソフトウェアを利用する ・最新のパッチを適用する ・禁止ソフトウェアおよびアプリ[*2]は、業務で使用するPC、スマートデバイスにインストールおよび業務利用しない	*1 サポート切れのOSやソフトウェアをしようせず、最新のOSを使用し、最新のセキュリティパッチを運用する等を行う。 *2 P2Pソフトウェア、VPN/リモートアクセスソフトウェア、私有アカウントによるソフトウェア利用など 新規のソフトウェアやアプリを利用する場合は、情報セキュリティ責任者の許可を受けること。 ABS社有PCについては、7Zip、Zoom、Chrome　は許可するものとする。
15	電子メールの使用時は以下のような対策を行う。 ・送信する前に宛先アドレスが間違いないか確認する。 ・メールソフトのオートコンプリート機能で誤送信を発生させないようにする。 ・返信、転送する場合は、そのメールに送る必要のないアドレスや転送先に開示してはならない情報が含まれていないか確認する。（安易に「全返信」しない） ・初めてメールを送る相手の場合は、特に宛先のアドレスに間違いがないか確認する。 ・送信先と関係のないファイルを添付していないかを送信前に必ず開いて確認する。 ・他のお客様向けに作成したメール本文、ファイルを流用しない。 ・添付するファイル内の別シートや非表示部分、ファイルのプロパティに不要な情報がないか送信前に確認する。 ・メーリングリストを管理する者はリスト登録者を常に最新の状態にする。 ・送受信したメールは、その内容を確認し、リスクの高い秘密情報は速やかに消去する。 ・送受信したメールを保存する場合は、情報漏えい対策を講じ、用済み後は速やかに消去する。 ・私有メールアドレスは業務で使用しない。 ・送信する情報の重要度に応じた情報漏洩対策を講じる。 お客様情報はメール本文に記載せず、暗号化またはパスワード保護した添付ファイルに記載する パスワードは、事前に送付先と決めておく、または電話などの手段でファイルを添付したメールとは別に連絡する ファイルは添付せず、利用が認められているアクセス制限付の共有場所（サーバやストレージサービス、セキュアな	
16	FAXの使用時は以下のような対策を行う。 ・送信先に事前に電話し、テスト送信を行う。確認がとれた後にリダイアルで再度送信する。 ・確認済みの短縮ダイアルを使用する。その際、短縮ダイアルの押し間違いに注意する。 ・カタログや申し込み用紙等の印刷物に自部門等の電話番号、FAX番号を記載するときは、その番号で確実に着信（受信）できるか事前にテストする。	
17	インシデントによる影響を最小にするため、インシデント発生時の対応[*1]について熟知する。 ・事故に該当するか否かを含め、一人で判断せず、直ちに上司、自社業務責任者に報告する。 ・自社業務責任者を通じて直ちにNEC業務責任者に第一報を行う。 ・紛失・盗難の場合は警察、交通機関にも届けを出す。 ・入場証、操作認証用キー、スマートデバイス、携帯電話等は失効の手続きを行う。	*1 インシデント発生時は、予め決められた手順に従い、エスカレーション報告、初期対応、証拠の収集等を行います。

ABS情報セキュリティ運用ルール（2025年度版）

社外秘

No	規則	備考
18	セキュア開発を実施するため、以下の対応を行う。	
	① Webアプリケーションセキュリティ対策 SQLインジェクションやクロスサイトスクリプティング等、Webアプリケーションにおける一般的な脆弱性に対処する。	設計、レビュー時にチェック項目に入れること。
	② セキュアコーディング 脆弱性に繋がるような危険な関数の利用禁止等、セキュリティを考慮したコーディングを行う。	禁止する関数についてはプロジェクトごとに検討、決定すること。
	③ セキュリティテスト セキュリティ機能が期待どおりに動作すること、情報漏えい等のセキュリティ事故が発生しないかの観点でのテストを実施する。	. テスト時の項目に入れること。
	④ 脆弱性診断 製品・システム・サービスの動作を解析にすることにより、潜在する脆弱性を検出し、当該脆弱性に対処する。 網羅的に脆弱性を検出するために、一般的には診断ツールを利用する。	確認項目についてはプロジェクトごとに検討、決定すること。 所属するプロジェクトでツール利用が作成されている場合、それに準ずること。
	⑤ セキュアな運用・保守業務 セキュアな運用・保守業務を行うための手順を確立し、当該手順に基いて業務を行う。	確認項目についてはプロジェクトごとに検討、決定すること。
	⑥ 脆弱性情報収集・対処 公開されている脆弱性情報の中から、提供する製品・システム・サービスに関連する脆弱性情報のみを収集し、当該脆弱性を悪用した攻撃を受けないように対処(パッチ適用、バージョンアップ、回避策の実施、サポート切れ製品の利用不可)する。	確認項目についてはプロジェクトごとに検討、決定すること。
	⑦ セキュア開発・運用チェックリスト適用 NECが提供するチェックリストを活用して、セキュリティ対策の実施状況を確認する対策。	確認項目についてはプロジェクトごとに検討、決定すること。
	⑧ 外部サービスの利用制限 外部サービス(Amazon AWSやOffice 365のようなインターネットを介して利用可能なサービス)は原則利用不可とす	
	⑨ 納品前のマルウェア感染確認 委託元に納品する前に、納品物がマルウェアに感染していないことをウイルス対策ソフトで検査する。	
	⑩ 物理的セキュリティの確保 開発作業を行う場所に対して、セキュリティ事故が発生しないよう物理的な対策(入退室管理、キャビネの施錠管理など)を実施する。	お客様構内のルールに従うこと。
	⑪ 論理的セキュリティの確保 開発・運用に利用するサービス機器等に対して、セキュリティ事故が発生しないよう論理的な対策(アクセス制御、構成管理など)を実施する。	お客様構内のルールに従うこと。 ABSにおいては、ルーター以外は外部ネットワークに直接接続することを禁ずる。
	⑫ 海外への再委託 再委託は原則として禁止する。	
	⑬ アクセス権管理 特権アカウントは必要な特のみ有効化し、その他のアカウントのアクセス権についても必要最低限の権限を付与す	
	⑭ ログ管理 業務情報へのアクセスログを収集し、当該ログを定期的に分析して意図していない操作が行われていないかを確認	
	⑮ 持ち込み・持ち出し管理 私物の機器(PC、スマートフォンなど)の持ち込みや、業務用機器(PCなど)の不正な持ち出しを制限する。	
19	知的財産権の保護について認識する。 ・ 知的所有権の侵害等、違法行為となる恐れがあるファイルの配布、ダウンロードを行ってはいけない。 ・ 他社の保有する特許権を侵害してはならない。他社の保有する特許権に関わる取扱いについては管理者に確認す ・ 市販パッケージソフト及び無償ソフトウェア製品はその使用許諾契約を守って使用する。	

ABS情報セキュリティ運用ルール（2025年度版）

社外秘

No	規則	備考
20	社内で使用するパスワードについては以下を遵守する。（お客様環境でのパスワードは、お客様環境のルールに従う。） ① パスワードは英数字を含め8文字以上に設定する。 ② パスワードは秘密に保つ。 ③ パスワードを忘れたり、間違えたりした場合、再度新しいパスワードの発行を行う。 ④ パスワードの他人による流用が発覚した場合、パスワードが漏えいしたと疑われる場合、直ちにパスワードを変更 ⑤ IDとパスワードは同じものを使用してはならない。 ⑦ パスワードは、定期的(1回/1年)変更する。	