1.はじめに

本ガイドラインの目的、適用対象及び構成は、以下のとおりです。

(1)株式会社ナンバーワンソリューションズの従業員が、当社または当社顧客先に常駐して作業をする場合に、守っていただくべき情報セキュリティに関する具体的要件を示します。

(2)当社業務について再委託がある場合は、再委託先の会社及び従業員に対しても本ガイドラインを適用し、遵守させるものとします。また派遣契約にもとづく業務においても貴社の従業員が遵守すべき情報セキュリティに関する具体的要件は本ガイドラインに準じます。

2.当社業務において保護すべき情報等

当社業務において保護すべき対象となる機密情報は、以下に示すとおり、当社及び当社顧客が開示する全ての事実、データ及び情報のことであり、口頭、書面、電子情報等、その情報が媒体に記録されているか否かは問わないものとします。

(1)仕様書、設計書等の業務資料

(2)打合せの内容、指示事項等の業務上知り得た情報

(3)顧客名・プロジェクト名等の情報

(4)当社及び当社顧客から貸与する ID カード、入館証等

(5)業務で利用するユーザ ID・パスワード等

但し、次に該当する情報は対象外とします。

a)開示を受ける前に、既に公知であった、または保有していた情報

b)開示を受けた後に、公知になった情報

c)正当な権限を持つ第三者から機密保持義務を負うことなく開示された情報

d)独自に開発または取得した情報

3.情報セキュリティ管理体制の整備

(1)情報セキュリティの管理責任者をソリューション事業部長と定める。管理責任者は、当社業務における情報セキュリティに関して、必要となる対策の指示や社内の指導、緊急時の対応、事故後の指示等を全社的な立場で行うものとします。

(2)情報セキュリティに関する情報展開、教育の手順を定める。

4.情報セキュリティインシデントへの対応

4.1. 情報セキュリティインシデントの定義

本ガイドラインにおける「情報セキュリティインシデント」の定義は、以下のとおりとします。

(1)「情報セキュリティインシデント」は、情報セキュリティが損なわれる可能性がある事象全般を指します。

(2)「情報セキュリティインシデント」は、結果的に当社の事業運営に著しく悪影響を与えた場合、または対外的に大きな問題として扱われた場合は「情報セキュリティ事故」として扱います。

(3)「情報セキュリティ事故」は発生状況を踏まえて、情報セキュリティの管理責任者が判断します。

4.2.情報セキュリティインシデント発生時の対応

情報セキュリティインシデント発生時には、速やかに対応を行うようお願いします。

(1)情報セキュリティインシデントが発生した場合、またはその可能性がある場合は情報セキュリティの管理責任者と常駐先の管理職に速やかに連絡をする。

(2)情報セキュリティインシデントの経緯、原因、是正施策を情報セキュリティの管理責任者と常駐先の管理職の要求に応じて報告する。

(3)情報セキュリティインシデントが事故の扱いとなった場合には、是正施策の確認を受ける場合がある。

5.当社または当社顧客先での遵守事項

当社または当社顧客先に常駐して作業に従事する従業員が守るべき具体的な情報セキュリティ遵守事項を以下に示します。なお、当社顧客先に常駐する場合は、顧客指定のルールに従います。

5.1.PC の取り扱い

(1)業務用の PC は、業務目的以外で利用しない。

(2)業務には当社または当社顧客先貸与の PC を利用する。個人所有 PC を持ち込んで社内ネットワークに接続したり、機密情報を格納したりする等、業務に使用することは一切禁止とする。また、業務報告書等の社内資料を、個人所有 PC を用いて作成または社外へ送付する等も業務利用とみなして禁止とする。（個人 所有 PC を業務利用すると管理が行き届かず機密情報漏洩のリスクが高くなる）

(3)機密情報が格納された PC は、以下のいずれかの盗難/紛失対策を実施する。但し、当該 機能が無い場合、または業務都合により当社管理職の許可を得た場合はこの限りではない。

・BIOS パスワードの設定 ・HDD/SSD 暗号化もしくは HDD/SSD パスワードの設定

(4)ノート PC を長期間使用しない時は、施錠可能なキャビネット等へ保管、またはワイヤーロック等の物理的保護を施し、盗難・紛失に備える。

(5)共有フォルダを作成した場合は、関係者のみがアクセスできるよう適切に権限を設定する。OS インストール時にデフォルトで共有されるフォルダ（Windows の Users フォルダ等）にも注意する。

(6)「ごみ箱」フォルダは、最低 1 ヶ月に 1 回の間隔で定期的に空にする。

(7)離席時や無人の状態で起動している際は、操作されないように常時コンピュータのロック、ログオフのいずれかを行う。また、不正な操作や盗み見を防止するため、特に理由がない限り、パスワード付きスクリーンセーバを 10 分以内の不動作で起動する設定にする。

(8)業務用 PC にタブレット、スマートフォン、フィーチャーフォン等のモバイル端末を接続することは原則として禁止とする。業務上やむを得ない場合は管理職の許可を得る。なお、充電目的で業務用 PC に接続する行為も、誤解を招くため禁止とする。

5.2.パスワード管理

(1)パスワードは 8 文字以上に設定する。但し、文字数制限がある場合はこの限りではない。

(2)パスワードの文字の種類は英大文字、英小文字、数字、記号のうち 3 種類以上を使用する。

(3)以下のような他人から推測されやすい文字列をパスワードに含めない。□ユーザアカウント□自分の苗字□自分の名前□自分の生年月日

(4)外部の Web サイト等で使用しているパスワードを業務で使用しない。

(5)パスワードを紙に書いて保存しない。

(6)システムに入力したパスワードを Web ブラウザに記憶させない。

(7)パスワードを他人に教えない。また、パスワードをシステムに入力する時は、周りの環境に気を配り、他人に見られないようにする。

(8)パスワードを他人に知られた場合は、ただちに管理者に連絡し、パスワードを変更する。

5.3. ウイルス対策

(1)ウイルス対策ソフトは常駐設定し、常時スキャンできるように設定する。

(2)ドライブ全体のウイルスチェックを、最低 1 ヶ月に 1 回の間隔で実施する。(パターンファイルが 間に合わず、侵入を許したウイルスを炙り出すため)

(3)外部ネットワークに接続したモバイル機器や PC を社内ネットワークへ接続する時は、それまでア クセスした社外での設定を見直すとともに、ウイルス対策ソフトによってドライブ全体をチェックする。
(4)ウイルス感染を発見または、その恐れがある場合、対象機器のネットワークケーブルを直ちに抜き、被害の拡大を防止する。
(5)ウイルス対策ソフトによりウイルスを検知した場合、直ちに管理職へ連絡する。

5.4.ソフトウェアの管理

(1)OS・ソフトウェアのセキュリティ情報には常に注意を払い、セキュリティ修正パッチ等がメーカーより提供された場合は、業務上の支障がない限り直ちに適用する。サポートが終了し、セキュリティパッチが提供されなくなった OS・ソフトウェアをインストールしている PC は、原則として社内ネットワークへの接続を禁止とする。
(2)出所不明なソフトウェアや、内容に確信の持てないソフトウェアをダウンロードまたは実行しない。
(3)セキュリティ上の問題がないことを確認済みのソフトウェアでも、PC にインストールする際は、管理職の許可を得て行う。
(4)ファイル交換ソフト等、情報漏洩リスクの高いソフトウェアは PC へのインストールを禁止とする。業務の都合によりやむを得ず利用する必要がある場合は、管理職の許可を得る。
(5)ライセンスを所持していないソフトウェアはインストールしない。
(6)個人で購入したソフトウェアを社内の機器にインストールしない。

5.5.インターネットサービス利用

(1)インターネットは、業務目的以外で利用しない。
(2)機密情報をインターネット環境（SNS、掲示板、ブログ、オンラインストレージ等）へ私的に書き込み・格納・保管することは禁止とする。

5.6.電子メール利用

(1)電子メールは、業務目的以外で利用しない。
(2)機密情報は原則として電子メールで送信しない。ただし業務上、機密情報を含む内容を電子メールで送信する必要がある場合は、管理職の許可を得る。
(3)電子メールに機密情報を含むファイルを添付する際には、暗号化またはパスワード付にする等の漏え

い対策をとる。また、パスワードを同じメールに記載しない。パスワードの複雑性は、「5.2. パスワードの管理」に従う。

(4)送信時には、送信先のメールアドレスに間違いがないことを必ず再確認する。また、使用しているメールソフトに送信前確認機能がある場合、当該機能を有効にする。

(5)宛先の選択ミスを防ぐため、アドレス帳はグループ分けに留意し、アドレス名称は日本語名称を用いる等、識別しやすくする。また、業務異動等により不要となったアドレス情報は削除する。

(6)意図しない宛先の入力を防止するため、宛先入力の補完機能（オートコンプリート機能）を使用しない。

(7)外部の電子メールサービス(Web メール含む)を利用しない。ただし業務上利用する必要がある場合は、管理職に相談する。

(8)メール受信時に、信頼できない ActiveX、Java 及び JavaScript 等のコードが自動的に実行されないよう、HTML メールの表示機能を使用しない。業務上やむを得ない場合は管理職の許可を得る。

(9)チェーンメール及びスパムメール(広告メール)には応対しない。

(10)安全性が確認されていない、送信元不明のメールや添付されたファイルは安全だと判明するまで展開しない。

5.7.チャット利用

(1)当社または当社顧客が環境を提供するチャットは、原則として業務目的以外で利用しない。

(2)管理職の許可のなくチャットサーバを社内ネットワーク上に構築しない。

(3)チャネルへの投稿は、チャネルに参加しているメンバ全てに内容が伝わるため、機密情報を、その機密情報へのアクセス権限がない人がいるチャネルに投稿しない。投稿前には、投稿先、内容に誤りがないことを確認する。

(4)投稿時に、不適切な表現（嫌がらせ、ハラスメント、恐喝、誹謗・中傷等）を含めない。また、文章については、丁寧さを心がけるようにする。

5.8.現場入館証・ID の取り扱い

(1)入館証・ID は、機密情報の漏えいに繋がる重要な資産であることを認識し、紛失しないよう細心の注意 を払う。

(2)通勤時等、屋外で携行する際は以下のいずれかを実施する。

●ネックストラップにて首から提げた状態で胸ポケットまたは上着の内ポケットに格納する等落とさないための工夫をする。

●ファスナー等により密閉できる鞄のポケットに格納し、鞄は可能な限り身体から離さない（財布、定期券、携帯電話等と同じポケットに格納すると、取り出し時に落下する可能性があるため、入館証・IDと他の所持品は、可能な限り別のポケットに格納する）。但し、飲酒する場合、鞄ごと紛失するリスクに配慮し、本方法は原則として禁止とする。

●その他、容易に身体から離すことができない方法を用いて携行する。各常駐先にて状況に応じた携行方法を定めている場合は、その携行方法を遵守する。

(3)屋内での着用時はネックストラップを用いるなど、紛失しないよう十分注意を図る。

(4)カードフォルダー本体、ネックストラップとカードフォルダーの接続部分の破損、劣化状況に日頃より留意し、不具合のある場合は直ちに補修または交換を行う。

(5)休日等、必要のない場合は持ち歩かない。

(6)紛失した場合、またはその可能性がある場合は、直ちに報告する。（紛失した入館証が悪用されることで、不正侵入される可能性がある）

(7)その他、入退館・入退室に使用するための物（カード、鍵等）も入館証と同様、紛失しないように 取り扱う。

5.9.オフィス内の管理

(1)機密に関わる会話は、近隣に漏洩しないよう密閉された会議室を利用したり小声で行なったりする等、注意する。

(2)機密情報が含まれる文書を関係者以外の者が閲覧可能な場所に掲示しない。

(3)印刷物をプリンタ・コピー機上に放置しない。

(4)機密情報の入った書類や媒体、及び持ち出しが容易な機器を机上や机の周囲に放置しない。机上は常に整頓しておく。

(5)機密情報の入った書類や媒体は必要に応じて施錠可能な引き出しやキャビネットに収納する。

(6)会議室やレビュールームにおけるホワイトボード等への書き込みは、使用後に消去してから退去する。

5.10.リムーバブルメディアの取り扱い

(1)個人所有のリムーバルメディア（コンピュータから容易に着脱可能な記憶媒体。CD や DVD、USB メモリ、リムーバブルハードディスク等を指す）を業務用 PC に接続する等、業務に利用することは原則として禁止とする。

(2)機密情報を記録したリムーバルメディアは、施錠して保管する等、紛失や盗難に合わないように管理を行う。

(3)USB メモリは業務で使用しない。業務上必要な場合は、管理職の許可を得て使用する。

(4)不要になったリムーバルメディアは、フォーマットできるものは物理フォーマットし、その後読み取れないようにシュレッダーにかける、傷をつける、寸断する等の対策を行う。

5.11.機密情報の持ち出し管理

(1)機密情報を勤務先事業所外へ持ち出すことは原則として禁止とする。自宅での作業を目的とした持ち出しはいっさい原則として禁止とする。

(2)業務都合により機密情報を持ち出す可能性がある場合は、第一に持ち出さなくても済む方法を検討する。やむを得ず持ち出す場合は、管理職へ申請し、許可を得る。持ち出し情報は、紛失・盗難 リスクを考慮し最小限とする。

(3)持ち出し前の注意事項

①機密情報を機器に格納して持ち出す際は、申請外の情報が格納されていないことを確認する。

②モバイル端末や PC、及びリムーバブルメディアで機密情報を持ち出す際には、原則として暗号化対策を施す。

③機器の持ち出し時は、持ち出す前にウイルス対策ソフトによってドライブ全体をチェックすることがのぞましい。また持ち出し機器を顧客先ネットワークに接続する場合はチェックを実施する。

④万一、持ち出し情報を紛失・盗難した場合、影響範囲が特定できるよう、持ち出し機器に格納した機密情報のバックアップ、ファイル一覧等を取得しておく。

(4)持ち出し中の注意事項

①持ち出し中の移動時は、持ち出した機器や媒体が第三者から認識されづらい方法、かつ身体から離さない方法で持ち運ぶ。（肌身離さないことで紛失や盗難を回避する）

②業務目的以外の場所への無用な立ち寄りを行わない。

③公共の場では機密に関わる作業を行わない。やむを得ず、作業を実施する場合、覗き見等による漏洩が起きないように注意する。

④可能な限り公共無線 LAN は利用しない。

(5)持ち出し完了時の注意事項

①持ち出し完了時、持ち出し情報を漏れなく持ち帰ったか（もしくは提出したか）を自ら確認した後、管理職に報告する。

5.12.顧客情報の保護

(1)顧客業務に従事する際は、本ガイドラインのみでなく、顧客が当社に提示しているセキュリティに関する遵守事項を必ず当社の技術部門に確認する。

(2)自社への報告書等、自社の文書において、顧客名・プロジェクト名・機器名・システム名等、顧客の機密情報を特定できる固有名称は「A 社」、「B システム」等伏せ字を利用する。また、固有名称だけでなく、顧客の機密情報を特定できる表現を使用しない。正式な文書だけでなく、ヒアリングメモ 等、正式な資料ではないものについても同様とする。

(3)やむを得ず顧客名やプロジェクト名を特定できる名称を利用する場合は、電子ファイルを暗号化・ パスワード付きにする等、当該情報を機密情報として、厳重に取り扱う。

5.13.業務情報の消去・廃棄

(1)担当業務の終了時は、業務情報消去の要否を確認の上、必要であれば消去する。

(2) PC、記憶媒体を廃棄する際は、以下のいずれかの処置を実施する。

●機器のメーカーが提供する手順による情報の消去

●データ消去アプリケーションによる情報の消去（最低 3 回以上の全体書き込み）

●記憶媒体の物理フォーマットによる情報の消去

(3)機密情報が含まれる書類を破棄する時は、必ずシュレッダーにかける。

5.14.情報セキュリティインシデント発生時の対応

(1)情報セキュリティインシデントが発生した場合、またはその可能性がある場合は、直ちに管理職に連絡する。

(2)情報セキュリティインシデント発生時の連絡先を常時確認できるようにしておく。

(3)情報セキュリティインシデント発生に際しては、影響範囲や原因の特定等を行うために、当該情報・機器等の保全を実施する。例えば、以下のような対応が挙げられる。

●インターネット環境での情報漏洩の場合、運営会社へ連絡し当該情報の保全を依頼する。

●ファイル交換ソフトによる情報漏洩の場合、漏洩元 PC の電源が入っていない場合は起動しない。

（ログ等の上書きを防ぐ）

●メール誤送信の場合、送信メールを削除しない。

7.情報セキュリティ遵守状況の確認への協力

本ガイドラインの遵守状況等を確認するために実施する以下の活動に協力をお願いします。

(1)情報セキュリティへの取り組み状況に関するアンケートへの回答。

(2)各事業所における実地ヒアリングへの対応。

(3)当社や常駐先にて実施する情報セキュリティに関する点検作業に対する貴社従業員の参加。