

2 . 安全管理措置について

- ・電気通信事業者は、個人情報の取扱い等に関して安全管理措置を講ずる必要があります。



ここでは、一般的な安全管理のための注意を説明します。

必要な安全管理措置

No. _____

- ・個人情報へのアクセスの管理
- ・個人情報の持ち出し手段の制限
- ・外部からの不正なアクセスの防止のための措置
- ・個人情報の漏えい等（漏えい、滅失またはき損）の防止
- ・その他個人情報の安全管理のための必要かつ適切な措置

会社では、「情報通信ネットワーク安全・信頼性基準」等の基準を活用した安全管理措置がとられていますので、その内容をよく確認し、これに従うようにしましょう

2 - 1 オフィスでの安全管理

- ・ オフィスでは、不審者の侵入を防止するため、施錠の管理や社員証の常時携帯を心がけましょう。
- ・ 来訪者や配達業者、見知らぬ人がいた場合には、用件を確認し、オフィスへの立ち入りは、必ず付き添うようにしましょう。



オフィスでの入退室時の注意事項

No. _____

- ・ オフィス内のドアやキャビネットの施錠は盗難や紛失等から防ぐため、確実に行うようにし、開けっ放しにしないでください。
- ・ 業務で利用する重要資料は、机上に放置したりせず、施錠できる場所に保管するようにしてください。 また重要資料が入ったフォルダボックスを机の下などに置くようなことはしないでください。
- ・ 社員証は、常に携帯し必要な時に提示できるようにしておき、紛失した場合には、 直ちに上司・管理者に報告するようにしてください。
- ・ 宅配や郵便などは、原則、職場の入り口で対応し、やむを得ず来訪者をオフィス内に入室させる場合には、 必ず従業者が付き添うようにしてください。



ケーススタディ - 11

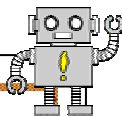


オフィス内での安全管理対策について、あなたが不適切だと思う行動はどれですか？

新入社員がオフィスのドアを開けたまま外出しようとしていたので、必ず閉めるよう注意した。

派遣契約が終了した派遣社員には、契約期間終了時に直ちに社員証やIDカードを回収するようにしている。

制服を着用している宅配業者には、入退室権限が設定されている部屋も含めてオフィスを自由に出入りすることを認めている。



注意事項

オフィス内のその他の物理的対策について

- ・来訪者などが出入りできる共有スペースでは、個人情報などの重要情報を取扱う作業は慎むようにしてください。またやむを得ず来訪者とオフィス内での打ち合わせを実施する際には、情報の漏えいに十分注意して行ってください。
- ・会議室などのような場所で来訪者と打ち合わせ中に、昼食で一時中断するような場合でも、会議室等が施錠できる環境の場合は施錠し、その鍵を他の人に預けたりしないようにしてください。
- ・サーバ室等の専用の部屋を設けた場合には、定められた手順や手続きに従って行動するようにしてください。執務時間外や昼休み・休憩時に勝手にサーバ室へ入ることのないようにしてください。
- ・ノートパソコンは、盗難等の被害から守るために施錠管理できる場所に保管するか、もしくはワイヤーロックでつなぐようにしてください。



ケーススタディ-11の答え：

入退室権限が設定されている部屋に、部外者の自由な入退室をさせることがないようにしてください。

2 - 2 オフィスでの注意点

- ・電気通信事業者のオフィス内には、様々な多くの個人情報があります。情報の内容や重要度に応じて、適切な取扱いを心がけましょう。



No. _____

各種情報の取扱い時における注意点

- ・情報の取扱い時には、社内規程やマニュアルに従い、安全に取扱うようにしてください。
- ・お客様の通信履歴、利用明細、発信者情報、位置情報、不払い情報、電話番号情報等の取扱いについては、より一層の注意が必要です。
- ・電子ファイルの取扱いについては、情報の重要度に応じて作成、修正、閲覧、複製、削除できる権限者を決めておく必要があります。同様に紙資料の取扱いについても保管場所や閲覧場所を特定しておく必要があります。
- ・また重要な紙資料や電子媒体は、施錠できるキャビネットへ保管し、廃棄時においても社内規程やマニュアルに従い確実に廃棄するようにしてください。



ケーススタディ - 12



情報の取扱いについて、あなたが適切だと思う行動はどれですか？

すべての資料に、個人情報と同じ一番管理が厳しい「厳秘」を記載している。

資料の取扱いは、扱う人が独自で判断して取扱うようにしている。

個人情報などの重要な情報の取扱いについて、不明な点は上司・管理者に確認するようにしている。

- ・ オフィス内での情報保護に努め、机上の整理整頓や会話に留意して行動するようにしましょう。



オフィスでの注意点（日常の振る舞い・行動について）

No. _____

- ・ 個人情報などの重要な情報が含まれている資料を机上や会議室等に放置しないでください。またそのような状況を見つけた場合には、周囲への確認を行うとともにオフィス内で注意喚起を促すようにしてください。
- ・ 仕事中に離席する際には、個人情報などの重要情報が机上にないかどうか確認を行うとともに、パソコンには一定時間内にパスワード付きのスクリーンセーバが作動するよう設定するか、又はログオフを行い、盗み見防止の対策を実施するようにしてください。
- ・ 業務に関する会話は、周囲に配慮して行い、エレベータ内や階段の踊り場では話さないようにしてください。 また必要であれば、声の漏れが無い会議室などで行うようにしてください。



ケーススタディ - 13

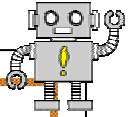


オフィス内での行動として、あなたが不適切だと思うものはどれですか？

帰宅時に一番最後の退出者であったため、コピー機に印刷物が放置されていないかどうか確認した。

オフィスには、個人情報漏えい防止の標語やポスターを貼り、セキュリティ意識の向上に努めている。

業務委託先にお客様リストを送る際、担当者の住所が分からなかったため、ホームページに記載されている本社住所に郵送した。



注意事項

オフィスでの行動、その他の一般的な注意事項について

- ・ F A X送受信時やプリンタ出力時には、放置することなく速やかに回収してください。またF A X送信時には誤送信していないかどうか確認しておく必要があります。
- ・ 電話で情報のやり取りを行う際は、相手方にも注意を呼びかけ、情報の漏えいを防止する必要があります。
- ・ 打ち合わせで使用したホワイトボードは、利用後には必ず消すようにしてください。
- ・ 契約書等の重要資料の受け渡しは、直接手渡しするか、郵送であれば「親展」と記載し配達記録をつけておくとういでしょう。
- ・ 従業員が所有する私物の持ち込みは、好ましくありません。やむを得ない場合には、社内規程やマニュアルに従ってください。また持ち込んだ電子機器や電子媒体に関しては、必ずウィルスチェックを行うようにしてください。



ケーススタディ-12の答え：

個人情報などの重要な情報の取扱いについて、不明な場合は自己で判断せず、上司・管理者に問合せを行うようにしてください。なおオフィスには様々な情報が在るため、一律に厳しい取扱いを表示することは、情報利用の観点から妥当ではありません。

ケーススタディ-13の答え：

お客様リストのような重要書類を送る場合は、事前に届けるべき人（担当部署）を確認して確実に送達されるようにしなければなりません。宛先が不明の場合、紛失のおそれがありますので、事前に確認するようにしてください。

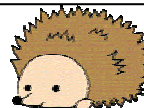
2 - 3 情報の持ち出し時の注意

- ・ 個人情報などの重要情報を持出そうとする場合には、持出しが認められたものかどうかをまず確認してください。
- ・ 持ち出す際には、必ず事前に承認を得るとともに外出時には、盗難や紛失に注意しましょう。



個人情報の漏えい事件・事故発生の原因の多くに、個人情報を持ち出したときの不適切な行動が挙げられています。情報の持ち出し時には、オフィス内と比べて盗難・紛失の被害にあう可能性が高まりますので、情報の安全性を確保する上でも、より一層の注意が必要です。

< 注意 >



- ・ 持出しが認められているかどうか確認してください。
- ・ 情報の持ち出し、外出時にどのような対策をすれば、盗難・紛失のリスクを回避できるか考えてください。
- ・ 盗難・紛失による情報漏えい事件を引き起こした場合、会社やあなた自身にどのような影響を及ぼすか持ち出すことが本当に必要かどうか、考えてください。



ケーススタディ - 14

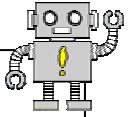


個人情報などの重要情報を持ち出した際の行動として、あなたが適切だと思う行動はどれですか？

車の中は施錠できる環境なので、重要な情報は持ち歩かずに車内に保管している。

外出時は、持ち出した資料が要るかどうか、喫茶店や公園など落ち着ける場所で確認している。

重要情報が入ったUSBメモリやノートパソコンを持ち出す際には、必ず暗号化やパスワード設定等の措置を施している。



情報を持ち出す際の手順について

個人情報等の重要な情報を持ち出す際には、社内規程やマニュアルに従って適切な行動をとるようにしてください。下記には、一般的な持ち出し手順を記述しています。

個人情報が含まれた機器や媒体をやむを得ず持ち出す際には

- ・ 事前に上司・管理者に申請し承認を得るようにしてください。
- ・ 電子媒体やノートパソコンを持ち出す際には、必ず暗号化やパスワード設定、データの分散化等のセキュリティ対策を施すようにしてください。
- ・ 外出時には、盗難や紛失に注意して、常に「手元から離さない」ようにしてください。
- ・ 外出先から帰社した際には、持ち出した情報が全て揃っているか確認を行い、足りない場合は直ぐに上司・管理者に報告してください。
- ・ また外出中に盗難や紛失の被害にあった場合には、直ちに上司・管理者に報告を行い指示を仰ぎ、最寄りの警察署に届け出るようにしてください。

注意事項

情報の持ち出し時の紛失・盗難以外の脅威について

盗難・紛失以外に、最近の個人情報の漏えい原因の中には、スパイウェアやWinnyを介して個人情報に漏えいした事例が数多く報告されています。情報の持ち出し時は常に漏えいする危険でいっぱいです。不特定多数が利用するインターネットカフェやウィルス対策ソフトが最新化されていない私物パソコンでの情報のやりとりは、厳に慎むべきです。



ケーススタディ-14の答え：

USBメモリやノートパソコンを持ち出す際には、情報漏えいのリスクが軽減できるよう暗号化やパスワード設定等の安全管理対策を施す必要があります。特に、USBメモリは大容量・小型化に伴い、紛失するとその影響は甚大なため十分な注意が必要です。

2 - 4 情報システムの利用 (1) インターネット

- ・私的な目的のために会社のインターネットを利用してはいけません。
- ・「ちょっとぐらい」などの安易な考えで、怪しいサイトを閲覧したり、不用意な情報の書き込みはしないでください。



インターネット利用時の注意事項



- ・インターネットの私的利用は禁止されています。業務と関係の無いウェブサイトの閲覧は控えるようにしてください。
- ・ウェブサイトで検索や閲覧をする際には、怪しいウェブサイトへのアクセスはしないでください。スパイウェア等の不正プログラムが仕掛けられ、知らないうちに情報が外部に送信されるおそれがあります。
- ・またウェブサイト閲覧中に意味不明な画面が出たり、警告する画面が表示された場合には、直ぐに利用を中止するようにしてください。
- ・インターネットを通じての情報の発信や掲示板への書き込みには、社会的責任、又は法的責任を負うことを常に意識してください。また不用意な情報の発信や書き込みは、社会全体に大きな影響を与えることを認識してください。



ケーススタディ - 15



会社のインターネットを利用する際の行動として、あなたが不適切だと思う行動はどれですか？

業務で活用できるフリーウェアのソフトを見つけたので、上司・管理者の正式な許可を得た上で、ダウンロードして利用した。

正式な許可は得ていないが、幅広い情報を得るため、インターネットの掲示板を有効に活用して、情報交換している。

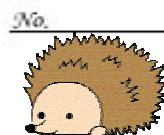
利用中に意味不明な画面が突然、表示されたので直ぐに利用を中止し、上司・管理者にその旨報告した。

2 - 4 情報システムの利用 (2) 電子メール

- ・業務目的以外で会社の電子メールを利用しないでください。
- ・個人情報等が含まれている資料を電子メールで送るには、細心の注意が必要です。やむを得ず送る場合には、暗号化や添付ファイルにパスワード設定を行うなどの対策を実施するようにしてください。



電子メール利用時の注意事項



- ・業務に関係ない目的で電子メールを利用しないでください。
- ・送信内容や宛先をよく確認して誤送信がないように注意してください。
- ・複数の送信先に送る場合には、お互いに面識がない場合もありますので、メールアドレスが表示されないBCC機能を使うなどの配慮が必要です。
- ・個人情報が含まれている資料を電子メールで送る場合は、細心の注意が必要です。送信する場合には、必ず暗号化や添付ファイルにパスワード設定を行う等のセキュリティ対策を実施するようにしてください。
- ・スパムメール等の不審なメールの添付ファイルや怪しいメールの内容に記述されたリンク先は絶対に開かないでください。悪意のあるプログラムが仕掛けられ、知らないうちに情報が外部に送信されるおそれがあります。



ケーススタディ - 16



電子メールを利用する際の行動として、あなたが適切だと思う行動はどれですか？

特定の人宛のメールでも、できるだけCC機能を利用して、関係者全員が情報共有できるようにしている。

業務多忙だからといって、受信した電子メールを自宅で利用しているパソコンには、転送しないようにしている。

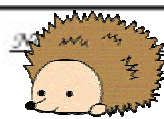
メーリングリストへの参加や登録は個人の判断で行うようにしている。

2 - 4 情報システムの利用 (3) ハード及びソフトウェア

- ・業務で利用するパソコンやソフトは、私的に改造したり、私的な目的のためにソフトウェアをダウンロードしてはいけません。また自宅で使用している機器などは、無断で持ち込んではいけません。



ハードウェア・ソフトウェア利用時の注意事項



- ・業務で利用するパソコンを無断で改造したり、無線LAN等の機器を勝手にネットワークに接続してはいけません。
- ・私物機器の持ち込みは、好ましくありません。やむを得ない場合には、社内で定められた規則に従ってください。また持ち込んだ機器をネットワークに接続する際は、セキュリティ対策がとられているかどうか上司・管理者による確認を受けてください。
- ・業務以外で、私的な目的のためにソフトウェアをダウンロードしたり、私物のソフトウェアを持ち込んではいけません。
- ・上司・管理者から指示されたソフトウェアのアップデートやセキュリティパッチの適用は、速やかに実施するようにしてください。



ケーススタディ - 17



パソコンの取扱いに関して、あなたが不適切だと思う行動はどれですか？

私物パソコンの持ち込み時は、確認を受けなければならないため、余分なソフトウェアは一旦削除して、後ほどインストールし直した。

余っていた無線LANの機器があったので、上司・管理者への確認をもとに暗号化などの必要なセキュリティ対策を実施した上で利用した。

使っていないパソコンを再利用する際は、OSやソフトウェアの修正プログラムを適用し、上司・管理者の確認を受けてから利用する。

2 - 4 情報システムの利用 (4) ID・パスワード

- ・ID・パスワードは他人に知られないように適切に管理し、注意事項を守って正しく利用しましょう。



ID・パスワード利用時の注意事項



- ・ID・パスワードは個人管理です。モニターや壁に付箋を使って貼り付けないで、管理ツールや安全な場所で管理するようにしてください。
- ・ログイン用に与えられた初期パスワードは速やかに変更してください。また生年月日や内線番号など他人に分かりやすいような設定や過去に使ったパスワードを再設定してはいけません。
- ・不正なアクセスを防止するため、設定したパスワードは定期的に変更するようにしてください。
- ・他人のID・パスワードを使って情報を閲覧したり、データを抽出することは不正アクセス禁止法で禁止されています。またID・パスワードの貸し借りは、セキュリティの確保が困難になるため、絶対にしないでください。



ケーススタディ - 18



ID・パスワードの利用について、あなたが適切だと思う行動はどれですか？

ID・パスワードは忘れやすいので、いつも目のつくところに貼り付けている。

同一部署全員で同一のID・パスワードを使用している。

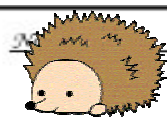
初期に設定されたパスワードがIDと同一であったため、直ぐに変更した。

2 - 4 情報システムの利用 (5) 共有ファイル、アクセス制限等

- ・ 共有ファイルサーバに保管する資料は、上司及び管理者の指示に従い、定期的な情報の整理やデータのバックアップを行うようにしましょう。
- ・ 重要な情報システムを利用する際には、許可された範囲内で利用するようにしましょう。



共有ファイルサーバ利用時の注意事項



- ・ 共有ファイルサーバは、業務の効率化や情報共有のために利用し、私的な趣味の動画や画像は保存しないでください。また上司・管理者の許可無く共有ファイルサーバの移動、削除、複製はしないでください。
- ・ データの保存領域に限りがあるため、上司・管理者と確認して、定期的に情報の削除、移動、及び統一等のメンテナンスを行うようにしてください。

情報システム利用に関する注意事項

- ・ 上司・管理者の指示に従い、アクセス制限された範囲で利用してください。また上司・管理者は、従業員が利用するメールの送受信履歴やインターネット及びシステムへのアクセスログを取得して定期点検・指導を行う場合もありますので、従業員もこの点検・指導に協力するようにしてください。



ケーススタディ - 19



情報システムの利用について、あなたが適切だと思う行動はどれですか？

個人情報が含まれたデータベースから必要な情報のみを参照しようと思ったが、今後も必要と思い、個人のパソコンにも記録しておいた。

個人情報などの重要データの紙出力は紛失する場合もあるため、極力USBメモリに記録するようにしている。

業務上やむを得ず個人情報が入ったデータをCD-Rに記録する際には、複数に分割して記録して、それぞれ単独では復元できないような措置を施している。

ケーススタディの解答



ケーススタディ-15の答え：

インターネットを活用して情報の発信や受信を行うことについて、社会的な責任や法的責任を負っていることを常に意識してください。この場合正式な許可を得るか、もしくは内部規程（マニュアル）に従って行動してください。



ケーススタディ-16の答え：

最近、自宅でWinnyを利用しているパソコンからウィルス感染による機密情報が漏えいした事例が報告されています。自宅に転送することは、原則禁止されていますので注意してください。



ケーススタディ-17の答え：

著作権法上、ソフトウェアのコピーは禁止されている場合があります。また私物パソコンの持ち込みは、事前に十分な確認を受けるとともに、確認後に余分なソフトを再インストールすることは絶対にしないでください。

ケーススタディ-18の答え：

初期パスワードの付与ルールを知っている者が不正なアクセスを行うおそれがありますので、直ぐに変更しなければなりません。また共有パスワードに設定することで、だれがいつアクセスしたのか解析が困難になり、パスワードを第三者に教えることで、不正アクセスの原因にもつながるため注意が必要です。



ケーススタディ-19の答え：

個人情報などの重要情報を外部メディア（CD等）に記録する場合には、細心の注意を払う必要があります。また選択肢の他にパスワード設定や暗号化を施すことも有効な対策の一つです。



2 - 5 コンピュータウィルス対策

- ・コンピュータウィルスやスパイウェアなど悪意のあるプログラムによる情報漏えいが、多数報告されています。情報漏えいを未然に防ぐため、コンピュータウィルス対策の重要性を理解して適切な対策を実施しましょう。
- ・Winnyの使用はやめましょう。



コンピュータウィルス及びスパイウェア対策の重要性について

- ・コンピュータウィルスにより、一度外部のネットワーク（インターネット）に流出した情報は、回収することが困難です。このような事態にならないためにもコンピュータウィルス対策は重要です。
- ・これまで情報漏えいを起こした人の多くが、「自分は大丈夫だ」や「ほんの少しの間だけ」と言う意識の人達でした。パソコンを利用している限り、ウィルス感染などの脅威は常に身近に存在していることを認識してください。
- ・Winnyなどの業務に関係の無いソフトを利用し、ウィルス感染から情報の漏えいを引き起こしてしまう行動は、お客様から極めてセキュリティ意識が低いと判断され、会社にとって社会的信頼を失いかねません。

ケーススタディ - 20

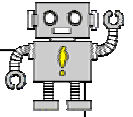
コンピュータウィルス感染などの脅威を回避するための行動として、あなたが不適切だと思う行動はどれですか？

怪しいメールの添付ファイルは、開かないようにする。

ウィルス対策ソフトは、常に起動して自動的に最新版への更新を行えるよう設定し、定期的にウィルスチェックを行うようにする。

Winnyさえ使わなければ大丈夫なので、Winnyだけ利用しないでいる。





コンピュータウィルス対策について

コンピュータウィルス対策は組織として統一した対策をとらなければ意味がありません。社内規程やマニュアル等に従って適切な行動をとるようにしてください。下記には、一般的なコンピュータウィルスへの予防対策を記述しています。

一般的なコンピュータウィルスへの予防対策

- ・サーバだけでなく、個人で利用するパソコンにもコンピュータウィルス対策ソフトを導入するようにしてください。
- ・またウィルス対策ソフトは、常時起動させ、定義ファイル（パターンファイル）を最新版に更新するなど新種又は亜種のウィルスがないかチェックできるようにしてください。
- ・メールの送受信や添付ファイル、並びにインターネットからダウンロードしたファイルは、開く前に必ずウィルスチェックを行ってください。
- ・上司・管理者による許可を得た機器、又はUSBメモリやCD - Rなどの記憶媒体を利用する場合にも、必ず事前にウィルスチェックの確認を受けるようにしてください。

注意事項

スパイウェアについて

スパイウェアはコンピュータウィルスとは異なり、自己増殖機能を持っていませんが、最近では巧妙な手口で情報を盗み出す事例も報告されています。ファイルの名前やアイコン、ファイルを添付したメールの内容がいくらかもっともらしい内容でも「.exe」や「.pif」などの拡張子が付いているファイルは危険ですから開かないようにしてください。



ケーススタディ-20の答え：

Winny以外のファイル交換ソフトでも、ウィルス感染によって情報が漏えいすることがあります。業務に不必要なファイル交換ソフトはインストールしないようにしましょう。

2 - 6 個人情報保護への意識向上

- ・個人情報の漏えい被害にあわないため、また知らないうちに加害者にならないようにするため、一人ひとりが積極的にセキュリティ意識を高めていきましょう。



No. _____

個人情報保護への意識向上の重要性

- ・いくら技術的に十分な個人情報保護の対策をしていても、たった一人の誤った行動により一般社会の目から組織のセキュリティレベルが低いと判断される場合があります。
- ・「ついうっかり」や「自分は大丈夫」と言う判断ミスや軽率な行動は、就業規則や社内規程の違反行為に該当する場合がありますので、日頃から自らの行動と照らし合わせてチェックや再確認をしておく必要があります。
- ・個人情報の保護や情報セキュリティに関する監査には、業務の一環と捉えてできる限り協力し、また必要な教育や研修についても率先して参加するようにしてください。



ケーススタディ - 2 1

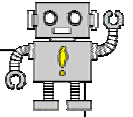


個人情報保護への取り組みとして、あなたが適切だと思う行動はどれですか？

業務に支障がある個人情報保護関係の社内規程やマニュアルは、守る必要がない。

退職予定者に対しても業務で得た情報がセキュリティ上問題となる場合もあるので、退職前から注意喚起を行い相互確認を実施している。

内部規程は、難しい用語ばかりでよくわからないため、その都度個人の判断に基づいて行動している。



個人情報保護への取組みについて

個人情報保護への取組みは、従業員一人ひとりが適切に運用していくことが重要です。下記には個人情報保護への意識を高めるために重要となる点を記述しています。

社内規程やマニュアル閲覧時において

- ・ 不明な点や実際の業務にあてはまらない場合には、そのまま放置しないで同僚や上司・管理者と意見交換を行うようにしてください。

個人情報の保護に関する教育において

- ・ 個人情報保護に関する教育においては、情報に接する全ての人が個人情報の取扱いにおける重要性を深く認識しておく必要があります。したがって派遣社員やパート社員でも個人情報に関わることが想定できるため、率先して教育を受けるよう努めてください。

注意事項

退職後の情報の取扱いについて

在職時に利用していた機密情報を別の第三者に提供することは、法律に抵触する場合があります。情報資産を保護するため、退職後においても守秘義務は継続されることが一般的ですので、相互に確認しておく必要があります。



ケーススタディ-2 1の答え：

過去に起きた事例の中に退職者による情報漏えい事件も報告されています。情報資産に接する全ての人は情報セキュリティの重要性について理解しておく必要があります。