パソコン／ネットワーク使用時のガイドライン

ＪＡ新潟厚生連

第１版　Ｈ１２.４.１
第２版　Ｈ２４.４.１
第３版　Ｈ２７.７.１
第４版　Ｈ２８.７.１

はじめに

近年、パソコンの普及とネットワークの進展により情報の流通が加速されつつあります。情報は自由に制約なく流通することが大切で、積極的な情報発信は、これからますます重要になってきます。一方それとともに、個人が情報を発信する際のモラルや責任も重要になってきます。

本ガイドラインは、本会のコンピュータ（以下、パソコン）とネットワークを使用する際の知的財産管理、ネットワークセキュリティ、法律・倫理等に関して適切に行動するための基本的なルールをまとめたもので、これにより適切なパソコン使用を図ることを目的としています。

なお、本ガイドラインはパソコンを以下のように使用する場合を想定しています。

(a) スタンドアロンで使用する場合
(b) 本会内のネットワーク（以下、本会内ネットワークという）および本会から貸与されたユーザ ID 等を用いてネットワーク上に構築されたシステムを使用する場合
(c) インターネットに接続しているネットワークとそのシステム、メールアドレス等を使用する場合

本ガイドラインは本会従業員に適用します。

本ガイドラインの各条項についての解説は、添付の「パソコン／ネットワーク使用時のガイドライン（解説編）」を参照してください。

＜パソコン／ネットワーク使用時のガイドライン＞

1. 使用目的

(1) 本会内のパソコンやネットワークは業務目的で活用する。
(2) 本会内のパソコンやネットワーク上の情報はすべて業務上のものと見なされる。

2. ソフトウェアの入手と使用

(1) 市販ソフトは、開封契約等の使用許諾条件に従って使用し、開封契約等で認められている以外のコピーをしてはならない。
(2) フリーソフトやシェアウェアを使用する時は、その使用条件を守る。
(3) 本会内ネットワークに接続しているパソコンには、無断でソフトウェアをインストールしてはならない。

3. セキュリティ

(1) 本会内ネットワークで流通している情報は、公開情報を除き、原則として本会外に開示してはならない。
(2) 本会内ネットワークの使用者は、自分のユーザＩＤのパスワードを使用者個人の責任で管理する。自分のユーザＩＤを他人に貸したり、一つのユーザＩＤを複数人で共有しない。
(3) 本会の秘密情報を本会内ネットワークの外に送信したり、フロッピーや USB メモリ、モバイルパソコン等の可搬記憶媒体に格納して持ち出す場合には、必要に応じて情報を暗号化する。送信先が本会外の場合には、事前に秘密保持契約を結び、秘密表示をする。
(4) 暗号化した情報を復元する鍵は、不慮の事故に備えて第三者が復元できるよう上司（幹部職員）などに預託する。
(5) 暗号化を復元する鍵を預託された者は、その鍵が破壊・改ざん・漏洩しないよう管理をし、業務上必要な場合以外預託された鍵で復元してはならない。
(6) 記憶媒体を廃棄する場合は、内容を消去あるいは媒体を破壊したうえで廃棄する。

4. コンピュータウイルス対策

(1) 自分の使用するパソコンがコンピュータウイルスに感染しないよう予防するとともに、他のパソコンにも感染させないようチェックする。
(2) コンピュータウイルスの感染を確認した場合は、すみやかにウイルス駆除、通知等の処置を行う。

5. 著作権

著作物については例外を除き基本的に著作権が存在する。これはインターネット上の記事や画像、プログラム等のデータも含まれる。著作物は許諾されている範囲内で使用すること。

6. 法律・倫理

パソコン／ネットワークを使用する際にも、以下の行為をしない。

(a)　業務上知り得た情報を私的な利益のために用いる行為
(b)　公序良俗に反する行為
(c)　他人の財産・プライバシーを侵害する行為
(d)　他人を誹謗・中傷するなど、名誉を毀損する行為
(e)　その他法律・倫理に反する行為

7. パソコン・ソフトウェア資産の管理

パソコン・ソフトウェア資産の管理について、以下のとおり運用する。

(1)　パソコン設置部署には最低１人以上の管理者を配置する。
(2)　パソコン設置部署ごとにパソコンの利用方針や利用規則を順守する誓約書を作成し、設置部署と各施設の総務課でそれぞれ保管する。
(3)　パソコンにインストールされている有償ソフトウェアについては、管理台帳を作成し適正に管理する。
(4)　毎年１回内部監査を実施し、管理台帳の点検を行う。
(5)　マイクロソフト社製品（OS を除く）を購入する場合、ボリュームライセンスで購入する。
(6)　ライセンス関係を証明する資料は保証書類と共に適正に保存・管理する。

＜付則＞

1. 本ガイドラインは、平成１２年４月１日より施行する。
　　〃　　平成２４年４月１日改訂する。
　　〃　　平成２７年７月１日改訂する。
　　〃　　平成２８年７月１日改訂する。

2. 本ガイドラインの取扱部門は、本部総務部電算課とする。

【添付資料】

パソコン／ネットワーク使用時のガイドライン（解説編）

ここでは「パソコン／ネットワーク使用時のガイドライン」の各条項について解説してあります。

1. 使用目的

(1) 本会内のパソコンやネットワークは業務目的で活用する。

本会内のパソコンやネットワークは、本会内の日常業務を効率的に行うためのツールですので、業務目的で積極的に活用してください。業務で使用するユーザＩＤやメールアドレス等も同様の理由で本会従業員に配布されているものですので、これらを業務と無関係な目的で使用しないでください。

(2) 本会内のパソコンやネットワーク上の情報はすべて業務上のものと見なされる。

本会内のパソコンや本会内ネットワークおよび業務で使用するユーザＩＤやメールアドレスは、本会が所有・管理し、本会内の業務を効率的に行うためのものであり、従業員個人のプライバシーの保護や通信の秘密を保証するものではありません。本会は、本会内のパソコンやネットワーク上の情報を、作成者・送信者・受信者の了解なしに、いつでも調査・使用・開示することができます。

私的情報に関して、プライバシーを確保し、通信の秘密を保つための最善の方法は、他の人に見られたくないような私的情報を本会内のパソコン上に蓄積したり、本会内ネットワーク上で送受信しないことです。

これらの設備やユーザＩＤ等は業務目的で使用するものではありますが、従業員個人のプライバシーの保護や通信の秘密を保証するものではないという原則を了解したうえで、業務外の電子メールの送受信や業務外のデータ（個人用のカレンダー・住所録・スクリーンセーバー等）の作成・保存など、業務に支障がなく必要最小限の範囲で、これらの設備やユーザＩＤ等を使用することができます。ただし、この場合は以下の事項を守ってください。

(a)　業務の遂行に支障を与えないこと
(b)　本ガイドラインや他の本会内規程に反しないこと
(c)　本会に損害や責任を生じさせるような形で使用しないこと
(d)　所属長の指示があるときは、その指示に従うこと

2. ソフトウェアの入手と使用

(1) 市販ソフトは、開封契約等の使用許諾条件に従って使用し、開封契約等で認められている以外のコピーをしてはならない。

開封契約とは、市販のソフトを購入すると添付されている使用許諾条件のことで、一般に、製品のパッケージまたはプログラムＣＤの入った封筒を開封することによって契約が成立したとみなす契約形態をいいます。開封契約では一般に、「このソフトウェアは１台のパソコンのみで使用できます」といった著作権がユーザに許諾している範囲が書かれています。

プログラムは著作者として、著作権法により保護されています。そのため、著作権

者の許諾なしにプログラムを複製したり改変したりすると、著作権侵害になります。例えば、開封契約で認められた範囲を超えてコピーしてしまうと、開封契約に反し、また著作権侵害になります。

市販ソフトを使用するときには、開封契約等購入契約で認められている以上のコピーをせず、使用するパソコンの台数分のソフトを必ず購入してください。また、ライセンスパックのように、１本の媒体から複数台のパソコンにインストールすることを許諾しているものもあります。このような場合も、インストールする台数は、契約で認められている範囲内としなくてはなりません。

(参考)　ライセンスパックとは？

企業ユーザ向けに、プログラム媒体やマニュアルは１セットだけ提供し、10 台、50 台といったまとまった台数分のインストールを許諾する販売形態があります。

(2) フリーソフトやシェアウェアを使用する時は、その使用条件を守る。

フリーソフトやシェアウェアは、ネットワーク等を通して配付され、手軽に入手することができます。フリーソフトは一般に、複製、配付、改造が自由（フリー）で無償（プライスフリー）で使用することができます。また、シェアウェアもフリーソフトとほぼ同じ条件で配付されていますが、その開発にかかる費用を使用者にもシェア（分担）してもらうために、使用者に対価の支払いを要求しています。

フリーソフトやシェアウェアを入手した時に添付されている使用条件を確認し、その使用条件の範囲で使用してください。

市販ソフトと同様に、フリーソフトやシェアウェアも著作権法により保護されていますので、著作権者が許諾している範囲を超えた使用は著作権侵害になる可能性もあります。したがって、使用条件を守って使用しなければなりません。

(3) 本会内ネットワークに接続しているパソコンには、無断でソフトウェアをインストールしてはならない

本会内ネットワークに接続されているパソコンには、業務で使用する様々なシステムがインストールされています。プログラムには相性があり、新たにソフトウェアをインストールすることでその業務システムの動作に影響を与える可能性を否定できないため、無断でインストールすることはやめてください。

3. セキュリティ

(1) 本会内ネットワークで流通している情報は、公開情報を除き、原則として本会外に開示してはならない。

ネットワークの普及により情報の流通が容易になったため、情報を共有する一人ひとりが責任をもって情報を適切に取り扱うことが重要になってきました。本会内ネットワーク上にはさまざまな情報がありますが、これらのほとんどが本会外秘・関係者外秘の情報です。本会では本会内ネットワークにおける情報の流通を迅速に行うことを優先し、これらの情報の提供・入手の際に本会外秘か否かの判断をする手続きを不要にしています。そのため、本会内ネットワークを使用する全員が、ネットワーク上の情報は原則としてすべて本会外秘の情報として扱い、これらを本会外に公開してはならないという共通認識をもっておくことが大切です。本会内ネットワークの外および他社に情報を開示する場合は、その秘密性をあらためて確認し、どのような形で開示するかを決定しなければなりません。本会の秘密情報であるが本会外に開示可能と判断した場合は３項（3）に従ってください。

なお、公開情報とは、本会内のものであると本会外のものであるを問わず、カタロ

グ、パンフレット、ニュースリリース等により、一般に公開されている情報をいいます。

(2) 本会内ネットワークの使用者は、自分のユーザＩＤのパスワードを使用者個人の責任で管理する。自分のユーザ ID を他人に貸したり、一つのユーザ ID を複数人で共有しない。

自分のパスワードを外部の人間に見破られ、そのパスワードで本会内ネットワークへアクセスされれば、自分自身の問題だけでは済みません。いったん外部の人間がパスワードを破ると、本会ネットワーク内の情報全体が本会外に漏れてしまうことになりかねません。このように、ネットワーク上のデータは外部に漏れても気づきにくいのが特徴です。

もし、パスワードが破られたことに気づいた場合には、すぐに施設長に連絡してください。

パスワード破りに対抗し、本会内ネットワークのセキュリティを守るためには、各自パスワードを管理することが重要です。具体的には以下の点について注意してください。

(a) 他人が連想できないようなパスワードをつける
アカウント名や有名人の名前のように誰でも連想できるようなパスワードは、本会内ネットワークに侵入しようとするものにとって、格好の標的です。独自で考えたパスワードをつけてください。

(b) 自分のパスワードを他人に教えない
他人にユーザ ID やパスワードを教えて業務を代行してもらうことは論外として、自分のパスワードをメモしてパソコンの横に貼り付けておくなど、自分のパスワードを他人が見える所に書き留めておくことも、他人にパスワードを知られる原因になります。このような行為は避けてください。

(c) 一つのユーザ ID を複数人で共有しない
複数人で行っている業務で一つのユーザ ID を取得し、そのユーザ ID とパスワードを共有することは他人にパスワードを知られる原因になりますので、このような行為は避けてください。

(d) アクセスログの通知されるものについてはそれを参照し、不明なアクセスがないかどうか確認する

(e) 不正アクセスと思われる事象を検出した場合は、速やかに当該システムの管理者に連絡する

(f) ユーザ ID を使用しなくなった場合は、速やかに当該システムの管理者に連絡し、ユーザ ID を停止してもらう
使用しなくなったユーザ ID を放置することは、ユーザ ID の不正使用のもとになります。

(3) 本会の秘密情報を本会ネットワークの外に送信したり、フロッピーや USB メモリ、モバイルパソコン等の可搬記憶媒体に格納して本会外に持ち出す場合には、必要に応じて情報を暗号化する。送信先が本会外の場合には、事前に秘密保持契約を結び、秘密表示をする。

ネットワークを使って秘密情報を送信することは、距離に関係なくタイムリーに送れるなど便利な反面、送信途中で第三者に秘密が漏れる危険性も高くなります。また、フロッピーや USB メモリ、モバイル用のパソコンに秘密情報を格納して本会外に持ち出す場合も、紛失などによる同様の危険があります。

関係者外秘など高度な安全性が要求される秘密情報を本会内ネットワークの外に送信したり、フロッピーやUSBメモリ、モバイルパソコン等の可搬記憶媒体に格納して本会外に持ち出す場合には、情報暗号化してください。

また、本会の秘密情報を外部に送信する場合には、事前に送信先と秘密保持契約を締結してください。やむを得ない場合には、以下の事項を明記したうえで秘密情報を送信してください。

- その資料を第三者に開示、提供しないこと
- 使用目的以外に使用しないこと
- 使用期間終了後は本会に返却または破棄すること

さらに、その情報が秘密であることを示すために、送信するファイルのできるだけ先頭に近い部分に、「（本会名）秘密情報」または「(本会名）ＣＯＮＦＩＤＥＮＴＩＡＬ」の秘密表示などをしたうえで送信してください。

(4) 暗号化した情報を復元する鍵は、不慮の事故に備えて第三者が復元できるよう上司（幹部職員）などに預託する。

暗号化は情報を安全に保存する方法の一つですが、本人以外解読できなくなるため、その本人に不慮の事故が発生した場合、業務に支障をきたすことにもなりかねません。したがって、暗号化機能を使用する場合は、その暗号を復元するための鍵を上司（担当幹部職員）などの第三者に預託することにより、緊急時にも第三者が復元できるようにしてください。

(5) 暗号化を復元する鍵を預託された者は、その鍵が破壊・改ざん・漏洩しないよう管理し、業務上必要な場合以外預託された鍵で復元してはならない。

暗号化された情報を復元する鍵を預託された者は、その鍵が他人にアクセスされることのないよう、預託された鍵を暗号化したり、預託された鍵を格納したファイルにパスワードを付けるなどしてその鍵が漏洩しないよう厳重に管理してください。鍵を預託された者が暗号化された情報を復元する場合は、業務上必要な場合のみとしてください。

(6) 記憶媒体を廃棄する場合は、内容を消去あるいは媒体を破棄したうえで廃棄する。

本会外秘情報が格納された記憶媒体（HDD、ＭＯ、ＦＤ等）を不用意に廃棄するとそこから情報が漏洩する危険があります。記憶媒体を廃棄する場合は、記憶媒体に格納されたデータを完全初期化により消去あるいは媒体を物理的に破棄し読むことができない状態にしたうえで廃棄してください。

4. コンピュータウイルス対策

(1) 自分の使用するパソコンがコンピュータウイルスに感染しないよう予防するとともに、他のパソコンにも感染させないようチェックする。

コンピュータウイルスは大変種類が多く、毎日大量の新種ウイルスも生まれており、そのすべてを完全にチェックすることは不可能です。しかし、コンピュータウイルスに感染すると、その種類によってはパソコンが動かなくなったりファイルが壊れたりと様々な障害を引き起こし、またネットワークや外部媒体を介して他のパソコンにも伝染し被害を拡大させる可能性があるため、限りなく感染しないような対策が必要となります。コンピュータウイルスはプログラムやデータを媒介して感染するものがほとんどです。必ず以下の対策を行ってください。

(a)　アンチウイルスソフトを導入し、リアルタイムスキャンを有効にする。また、

定期的にウイルス定義ファイルを最新化する。

(b) インターネットからファイルをダウンロードしたり、USB メモリ等の外部媒体を使用する際には、アンチウイルスソフトにより事前にスキャンを行いウイルス感染していないことを確認する。

(c) 見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する。特に実行形式の添付ファイルはむやみにクリックしない。

(d) 外部からパソコンを持ち込んで勝手にネットワークに接続しない。

(e) P2P ファイル共有ソフト（Winny、Share 等）を使用しない。

(f) 怪しいインターネットサイトを閲覧しない。

(2) コンピュータウイルスの感染を確認した場合は、すみやかにウイルス駆除、通知等の処置を行う。

コンピュータウイルスは種類によってはネットワークを介して伝染する場合があります。このため、感染が確認された場合は速やかに LAN ケーブルをはずし、ネットワークから切り離してください。その後、当該システムの管理者に連絡して感染の経緯について報告すると共に周辺の使用者にも警告を行い、ウイルス感染源も含めてウイルス駆除の処置を行ってください。ネットワークへの再接続はウイルスの完全排除を確認できた後になります。

7. パソコン・ソフトウェア資産の管理

ソフトウェアには利用に関してライセンスの制限があります。ライセンスの範囲を超えた利用については、不正利用となり処罰の対象となりかねないため十分注意して運用してください。

(1) パソコン設置部署には最低１人以上の管理者を配置する。

適正なソフトウェア管理のため、パソコン設置部署には最低１人以上の管理者を配置してください。

管理者は、自部署において不適正なソフトウェア管理がされないように、自部署職員への当ガイドライン周知を行うなど管理を徹底してください。

(2) パソコンの利用方針や規則を順守する誓約書をパソコン設置部署と各施設の総務課でそれぞれ保管する。

各施設の総務課にてパソコンの利用方針や利用規則についての誓約書を作成し、パソコン設置部署と各施設の総務課でそれぞれ保管してください。

誓約書は当ガイドラインを順守した内容で作成し、職場代表者の氏名記入・押印をしてください。

(3) パソコンにインストールされている有償ソフトウェアについては、管理台帳を作成し適正に管理する。

有償ソフトウェアについては、著作権上の問題から適正に管理する必要があります。以下のとおり管理台帳の作成、運用をしてください。

(a) 各施設で購入した部門システム、インターネット、スタンドアロンを対象とする。（病院情報システムおよび健診システム、人事給与・財務会計システムのパソコンは本部で一括管理とするため各施設では作成不要。私物や業者等の持込パソコンは対象外）

(b) 管理台帳を作成し、各施設の総務課で管理する。

台帳作成時に記入したハードウェア本体には、識別するために任意の表示シール（ラベル）を添付し、未記載のものと完全に区別する。識別ラベルには記載日・設置部署・識別番号等を記載するものとする。購入や移設、移管、廃棄など変更があった場合はその都度台帳に記載し、ラベルにも適用する。

(c)　従来からある本会の固定資産台帳についてはそのままの運用とする。

(4) 毎年1回内部監査を実施し、管理台帳の点検を行う。

毎年1回7月31日を応当日として内部監査を実施し、管理台帳の点検を行ってください。点検後、管理台帳を本部総務部電算課へ提出してください。本部にて全施設分を取り纏めてマイクロソフト社に報告します。（報告はマイクロソフト社製品のみ）

(5) 今後マイクロソフト社製品（OSを除く）を購入する場合、ボリュームライセンスで購入する。

覚書による取決め（マイクロソフト社からの指示）により、今後マイクロソフト社製品（OSを除く）はボリュームライセンスで購入してください。パソコン購入の際にプレインストールされているものを購入したり、店頭でパッケージを購入したりしないようご注意ください。

【参考　ライセンス種別について】

マイクロソフト社製品のライセンスには以下の3種類があります。

・ボリュームライセンス　…　大量導入する場合向けの使用権。
1つのメディア（CD等）からライセンス購入数分だけパソコンにインストール可能。
ライセンス保有証明はメディアではなく証書の保管による。また、マイクロソフト社にも購入履歴が残る。

・パッケージ　…　一般に市販されているパッケージ製品。原則、製品1本につき1台のパソコンにのみインストール可能。
ライセンス保有証明には購入時の製品一式（CD、箱、説明書等）を保管しておく必要がある。

・プレインストール　…　パソコン購入時に最初からインストール済みのもの。そのパソコンでしか使用できない。

なお、ライセンス保有証明には、パッケージと同様、製品一式の保管が必要になりますのでご注意ください。

(6) ライセンス関係を証明する資料は保証書類と共に適正に保存・管理する。

ライセンス関係を証明する資料（プロダクトキー等）は保証書類とともに保管場所を明確に定め、各施設の総務課により管理を徹底してください。

どのパソコンの資料か特定できるように、保管をしてください。

＊補足＊　システム管理者について

本会では様々なシステムが利用されているが、管理者については以下のように定義する。

1）システム管理者

システムやパソコン、ネットワークについては、その系統によって以下のように管理する。

① 本会内ネットワーク上のシステム

- 医療情報系システムについては、本部総務部電算課が管理する
- 総務系システムについては、本部事業部が管理する
- 本会内ネットワークについては、本部総務部電算課が管理する

② 施設側で整備したシステム

- 施設側で整備した以下のようなシステム等については、施設長が管理する。
  (ア) インターネット環境、レセプト電算請求環境
  (イ) その他、施設で個別に整備したシステム・パソコン

2）ユーザ ID 管理者

ユーザ ID やメールアドレスについては、それぞれのシステムの使用環境を勘案し以下のように管理する。

① 本会内ネットワーク上のシステム

- 本会共通で使用するグループウェアのユーザ ID については、対象が限定されることから、本部総務部電算課が管理する
- 医療情報系システムのユーザ ID および使用権限の範囲については、従業員の配属就業状況による判断が必要なことから、施設長が管理する
- 総務系のシステムのユーザ ID については、使用者が限定されることから、本部事業部が管理する

② 施設側で整備したシステム

- 施設側で整備したシステムやパソコンのユーザ ID、メールアドレス等については、施設長が管理する