情報セキュリティハンドブック

your security
hand book

Version 1.0

２０２１年９月

２０２１年９月

IT Professor

IT 部

秘 Confidential

your security
hand book

1．はじめに

ハンドブックの目的

このハンドブックは、あなたと会社の情報セキュリティ水準の向上を目的としています。
高水準の情報セキュリティを実現するためには、会社で共に働く従業員ひとりひとりの協力が必要です。したがって、情報セキュリティに関する問題や疑問が生じた際、このハンドブックをいつでも参照できるようにしてください。

コミュニケーションルート

あなたは日々の業務のなかで、ときには解決できない、または判断に迷う場合があります。
その場合の問題や疑問を解決するため、情報セキュリティに関する相談窓口が用意されています。また、日々の業務は、「IT ヘルプデスク」や「FAQ」を通じてサポートしていきます。

- 情報セキュリティ管理体制
- helpdesk@it-professor.jp

2．情報資産

あなたが守る情報資産

あなたとあなたの同僚が日々の仕事のなかで触れるものはすべて大切な会社の資産です。これら重要な資産は、各組織や担当する仕事により様々な形で存在しています。このハンドブックでは、あなたと会社を守るための情報セキュリティの基本的な内容が説明されています。

あなたが日々の仕事のなかで大切に守らなければならない情報資産をこのハンドブックにメモしてください。このハンドブックを活用することで、常にあなたと会社を守ってください。

守るべき情報資産	備　考

3．あなたの会社での仕事

あなたの日常業務

会社を取り巻く環境は日々変化しています。
社会的には個人情報やプライバシーへの関心が高まるなか、情報漏洩や不正アクセスなどの事件・事故が発生しています。また、企業活動を行っていくうえで、社会倫理や法律上の新しい課題が生じてきています。
私たちは、このような状況のなかで改めて日々の業務内容を点検し、セキュリティの観点から情報を適切に保護し、利用していく必要があります。

日常業務での情報セキュリティのチェックポイント

あなたは、あなたと会社の大切な資産を保護するため、日常業務のなかで次の事柄を守って業務を行ってください。

- ＩＤとパスワードは、大切に管理してください。
- 社内の情報システムは、業務目的のみに使用してください。
- インターネットは、業務目的のみに利用してください。
- ソフトウェア等の著作物は、決められた手続きを経て入手し利用してください。
- パソコンは、必要なときのみログオンし他人からの不正利用を防止してください。
- 情報は、利用目的と重要度に応じて安全な保管をしてください。
  また、不要な情報は、安全・確実な廃棄を行ってください。
- 電子メールは、送信するまえに伝達する相手と内容を確認してください。
  また、情報の重要度に応じた安全な情報伝達に努めてください。

なお、チェックポイント毎にどんな脅威やリスクがあるのか、またどうすれば安全に情報を活用できるのかについて解説しています。
あなたは、あなたの日常を点検し、情報セキュリティ水準の向上に協力してください。
もし、あなたの周囲で正しい運用が行われていない場面を見かけることがあれば、上司や同僚に相談するなど、注意を促し、あなたと会社を守ってください。

３．１　ＩＤとパスワードの管理

ＩＤとパスワードの意義

ＩＤはあなたと他人を識別するために、パスワードはあなたであることを証明するために付与されています。
したがって、ＩＤとパスワードには、あなたと会社の資産を保護する重要な鍵の役目があります。

あなたと会社の脅威となること

ＩＤとパスワードを気軽に教えることやパソコンに貼ることは、あなたのＩＤとパスワードが不正に利用され、重要なデータの改ざんや、重要なデータの持ち出しが行われる危険があります。

あなたと会社の財産を守るために

あなたは、あなたの家族・財産を守るために自宅の鍵を大切に管理するのと同じく、あなたと会社を守るためにＩＤとパスワードは大切に管理してください。
ＩＤとパスワードを安全に管理するためには、定期的にパスワードを変更することや、他人が推測できないパスワードを使うことが有効です。
また、緊急時など何らかの事情でＩＤとパスワードを他人に教えた場合は、パスワードを変更して下さい。

３．２　私的使用の禁止

情報資産の私的使用の禁止

インターネットや電子メールを含む社内の情報システムは、会社の重要な資産です。あなたが社内の情報システムを利用して扱う情報は、あなたと会社の企業活動の成果であり、すべて大切な会社の資産です。

したがって、あなたは業務目的以外でこれら情報資産を私的に使用することは出来ません。また、個人所有の機器から社内情報システムの利用は禁止されています。会社貸与の携帯電話・端末を使って下さい。

あなたと会社の脅威となること

インターネットや電子メールを含む社内の情報システムの私的使用は、同僚の仕事と会社の成果に悪影響を及ぼす原因になります。

インターネットでは、どこからの訪問者かを特定することができます。私的な使用によるクレームであっても、会社は対応を求められることになります。また、電子メールについても同様です。

あなたと会社の財産を守るために

あなたが情報を保護し、利用するためには各組織・業務毎に定められた業務手順やマニュアルなどに従ってください。

もし、社外に持ち出す必要がある場合は、あなたの上司に利用目的を説明し、承諾を受ける必要があります。

３．３　不正コピーの禁止

ソフトウェアについて

あなたが仕事をするため利用するソフトウェアは、それを作成した個人や企業の許可なく、複製や配布、転載することができません。

あなたと会社の脅威となること

ソフトウェアの使用許諾契約書にある条件を超えた使用は、知的財産権の侵害にあたります。

したがって、購入した数量を超えたインストールやインストール媒体（DVD など）をコピーし、自宅に持ち帰るなどの行為をしてはいけません。

あなたと会社の財産を守るために

正当に取得したソフトウェアであることを証明できるように、使用許諾契約書（ライセンス証明書）は、適切に保管しておく必要があります。

あなたが会社で使用するソフトウェアは、必ず上司とソフトウェア管理責任者の承諾のもと、会社で決められた手続きを経て購入してください。

あなたが業務目的でインストール媒体を使用する場合は、あなたの上司やソフトウェア管理責任者の承認を得てください。また、不正行為や紛失を防止するためにソフトウェア管理責任者の指示に従ってください。

個人のソフトウェアと著作物

個人が所有するソフトウェアを会社で使用することは禁止されています。

また、インターネットなどから取得可能なフリーソフトやデータ（画像や音声も含む）を使用することは、知的財産権を侵害するおそれがあります。これらを業務で利用する場合はソフトウェアの取扱と同じ対応が必要です。

３．４　パソコンの利用

ログオン

パソコンや社内の情報システムは、ＩＤとパスワードで保護されており、あなたが利用するために最初に行うことはＩＤとパスワードでログオンすることです。
これは、情報セキュリティ水準を維持するために最も重要なことです。

あなたと会社の脅威となること

来客や電話、打合せなどにより、あなたがパソコンや情報システムからログアウトせず一時的に離席した場合、あなたと会社の大切な資産が不正に利用されるおそれがあります。その結果、重要なデータの改ざんや持ち出しが行われるかもしれません。
また、ネットワーク共有を利用することは、あなたやあなたの同僚とデータを共有するなど大変便利です。しかし、共有フォルダのアクセス権限の設定が適切になされていない場合は、意図しないデータの変更や消失が起こるかもしれません。

あなたと会社の財産を守るために

あなたが仕事で、パソコンや社内の情報システムを使う場合は、次のことを守りましょう。

- 業務に利用するときのみ、ログオンしてください。離席するなど一時的に使用しない場合は、ログアウトしてください。スクリーンセーバーにパスワードを設定することも有効です。
- ネットワーク共有する場合は、業務上必要な人だけがアクセスできるようにしてください。必要に応じて、あなたの上司やアクセス権限設定責任者に相談してください。
- 重要なデータは万一に備えバックアップを取っておきましょう。
- コンピュータウィルスの加害者・被害者にならないために、ウイルス検知駆除ソフトは常に起動しておきましょう。

３．５　電子メールを利用した情報の伝達

気持ちよいコミュニケーションにはマナーが大切

あなたは、業務目的のため、あなたの同僚や顧客、取引先との連絡や情報の交換に電子メールを使用します。コミュニケーションツールとして積極的に活用することは大切ですが、決められたルールやマナーを守り使用することが大切です。

あなたと会社に脅威となること

送信相手をよく確認しなかったために、誤って別の人に送信してしまうことは、重要なデータを社外に漏らしてしまうことになります。また、あなたの大切な顧客のメールアドレスを他人に教えてしまうなど、大切な顧客に迷惑をかけることになります。
身元が不確かな相手からメールの添付ファイルを不用意に開いてしまうと、コンピュータウィルスに感染する危険があります。

安全なコミュニケーションを実現するために

電子メールは業務目的のみに利用しますが、より安全なコミュニケーションをするために、必要に応じてあなたの上司に相談してください。
あなたは、次のことに注意すれば、より安全な伝達を行えます。

- 電子メールで送っても良い情報であるか確認します。必要に応じて、あなたの上司に同報（CC）もしくは転送を行ってください。
- 送る情報の取扱を事前に上司と相談してください。送る情報が重要であればあるほど情報の取扱を相手に正確に伝える必要があります。
- 送信する前に、もう一度相手のメールアドレスを確認してください。
- 社内や顧客、取引先などから誤ってあなた宛にメールがきてしまった場合は、送信者に知らせ、受け取った情報の処置について確認してください。
- 身元が不確かな相手から送られてきた場合は、不用意に返信せず、メールを削

除してください。

３．６　インターネット

インターネットの適切な利用

あなたは、情報収集などの業務目的にのみ、インターネットを利用できます。

あなたと会社に脅威となること

インターネットは、様々な人や企業が利用またはホームページの開設をしています。あなたの不用意なアクセスは、コンピュータウィルスを社内に意図せず持ち込む危険があります。性的・差別的コンテンツを閲覧するなどの行為は、あなたの同僚へのハラスメント行為につながります。

また、電子掲示板や SNS への書き込みは、あなたと会社の重要な情報が流出してしまう恐れがあることから行ってはいけません。

安全に利用するために

あなたは、より安全にインターネットを利用するために、次のことに気をつけてください。判断に迷う場合は、あなたの上司に相談してください。

- 業務上必要な情報の閲覧のみに利用してください。発言や掲示板への書き込みなどは行ってはいけません。
- 不用意なダウンロードは行わないでください。業務上必要な場合は、あなたの上司やソフトウェア管理責任者に相談してください。
- インターネットにある情報を利用する場合、使用条件を確認し、知的財産権等の侵害にあたらないことを確認してください。

３．７　情報の保管と廃棄

安全な保管

あなたは、電子化された情報を業務上の利用目的や情報の重要度に応じて安全な状態で保管し、利用してください。

あなたと会社に脅威となること

ソフトウェアのインストール媒体（DVD など）を机のうえに放置することは、盗難や不正コピーの原因になります。

また、記録媒体の情報を消去せず廃棄することは、大切な情報の漏洩などの原因になります。

あなたと会社の財産を守るために

あなたは、電子化された情報を安全に利用するために、次のことに気をつけてください。判断に迷う場合は、あなたの上司や電子化情報取扱責任者に相談してください。

- 重要な情報や万一に備えたバックアップのデータは、外付け HDD や USB フラッシュメモリーなどに保存し、施錠できる場所に保管すると安全です。また、情報の内容や保管期限などをラベルに記入して貼付することは、紛失防止とともに適切な管理が行えます。
- 業務上の必要性から社外にデータを持ち出す場合は、必ずあなたの上司の承諾を受けてください。

情報の廃棄

業務上不要となった情報は、速やかに消去する必要があります。

外付け HDD や USB フラッシュメモリーのデータは、消去したつもりでも特殊なツールにより復元することが可能です。情報漏洩の危険がありますので、磁気媒体を再利用、廃棄する際は、次のように安全な対応を行ってください。

- 磁気媒体は、データの重要性に関係なく、必ずデータの消去し、再利用を行ってください。
- 重要なデータを保存していた磁気媒体は、ディスクシュレッダーを利用するなど再利用できないように処置してください。

・ パソコンなどハードウェアを廃棄する場合は、会社により決められた手続きを経て、廃棄してください。

4．参考

4．1　関連規定と規約

情報セキュリティを守るうえで、関連する社内規定等には次のものがあります。

名称	備　考
情報セキュリティポリシー	情報システムを円滑で安全に利用するための情報セキュリティ活動の基本的な方針が示されています。
電子化情報取扱基準	電子化された情報の適切な保護と利用を行うために、重要度に応じたデータの区分、取扱、保護の基準がまとめられています。
アクセス権限管理基準	業務で利用する情報システムやその資源を守るためのアクセス権限の設定と管理基準がまとめられています。
物理的セキュリティ対策基準	情報システムを安全に設置し、利用するため、物理的破壊や盗難などの保護に関する基準がまとめられています。
ネットワーク接続基準	社内ネットワークへの不正侵入、情報漏洩、破壊を防止するための社外との接続方法と基準がまとめられています。
ソフトウェアライセンス保護基準	ソフトウェアの不正利用を防止するため、ソフトウェアの適切な導入、使用ならびに管理する基準についてまとめられています。
コンピュータウィルスウイルス対策基準	コンピュータウィルスの侵入、感染、拡大を防止するための基準と運用方法がまとめられています。
外部委託時の情報セキュリティ管理基準	情報資産の取り扱いを外部委託する場合に、必要な基準がまとめられています。
インターネット情報サービスセキュリティ対策基準	インターネット公開サービスの設計、構築、運用および検査について、必要な基準がまとめられています。
情報資産モニタリング基準	情報資産を不適切な利用、漏洩、盗難、改ざん、破壊等から保護するためのモニタリングについてまとめられています。

４．２　情報セキュリティ管理体制

情報セキュリティ水準の向上を目的に次の体制が用意されています。
あなたが業務を行うなかで、これは情報セキュリティ上問題にあたらないかと思う場面があるかもしれません。あなたが相談することで不利益が生じることはありませんので、あなたの上司や同僚、または準備された相談窓口に相談してください。そうすることで、問題が提起され、あなたと会社は改善のために一歩前進することができます。

名称	役　割
電子化情報取扱責任者	電子化された情報（データ）の把握、情報の機密レベルに応じたアクセス権限、配布・保管方法など取扱を明確にするとともに、適切な管理に努める役割を担います。
アクセス権限設定責任者	主管するシステムや共有サーバ毎にアクセス権限設定仕様などルールを取り決めます。また、定期的にパスワードの運用状況を把握し、適切な指導を行う役割を担います。
ソフトウェア管理責任者	ソフトウェアの使用状況の把握や保管を行い、不正コピーの防止、台帳などを使用しライセンスや媒体を適切に管理する役割を担います。
コンピュータウィルス対応責任者	コンピュータウィルスの侵入、感染、拡大を防止する対策を管理する役割を担います。
利用者（あなた）	情報セキュリティポリシーを理解し、守ります。 問題や疑問が生じた場合は、関係する責任者に連絡します。

５．ハンドブックの最新版

このハンドブックの最新版は、IT 部ヘルプデスク掲示板に掲載されています。